Miskolci Egyetem
Gépészmérnöki és Informatikai Kar

Szakdolgozat

Blokkláncok fejlődése témában

Készítette: Dobozi Botond
Szak: Programtervező Informatikus
Neptun-kód: HYS4P5

Témavezető: Dr. Karácsony Zsolt
Beosztás: egyetemi docens

Miskolc, 2025

Tartalomjegyzék

1. fejezet

Bevezetés

A blokklánc-technológia az elmúlt évtized egyik legjelentősebb digitális innovációjává vált, amely alapjaiban formálta át a pénz, a bizalom és a digitális adatkezelés fogalmát. Eredetileg a Bitcoin kriptovaluta működését biztosító infrastruktúraként jelent meg, mára azonban jóval túlmutat az egyszerű fizetési rendszereken, és olyan területeken is meghatározóvá vált, mint a pénzügyi szolgáltatások, az ellátási láncok, a szerződéskezelés vagy akár a közigazgatás. A technológia iránti fokozódó érdeklődés nemcsak a piaci szereplők, hanem a tudományos világ figyelmét is felkeltette, mivel egy olyan újfajta, decentralizált adatkezelési modellt kínál, amely a bizalmat a résztvevők hálózatára és a kriptográfiai elvekre alapozza, nem pedig egyetlen központi szereplőre.

A blokkláncok fejlődése szorosan összefonódik a digitális pénz és a kriptográfia történetével. A Bitcoin 2008-as megjelenése mérföldkő volt, mivel az első olyan, széles körben ismert rendszer, amely képes volt központi elszámoló fél nélkül, nyilvános hálózaton biztonságosan kezelni a tranzakciókat. A Bitcoin-bányászat, mint konszenzusmechanizmuson alapuló folyamat, nemcsak a hálózat biztonságát garantálta, hanem gazdasági ösztönzőkkel is ellátta a résztvevőket. Ezzel létrejött egy újfajta ökoszisztéma, ahol a technológiai, gazdasági és játékelméleti szempontok szorosan összekapcsolódnak. A kezdeti időszakot így elsősorban a kriptovaluták és a bányászat köré szerve-

ződő innovációk jellemezték.

A blokklánc-technológia következő nagy ugrását az okosszerződések megjelenése jelentette, különösen az olyan platformoknak köszönhetően, mint az Ethereum. Az okosszerződések lehetővé teszik, hogy a felek közötti megállapodások feltételei programkód formájában, automatikusan végrehajtódjanak a blokkláncon, ezáltal csökkentve a közvetítők szerepét és a visszaélések lehetőségét. Ezzel a blokklánc kilépett a pusztán pénzügyi alkalmazások világából, és általános célú, decentralizált alkalmazásplatformmá vált. A technológia fejlődése során új konszenzusmechanizmusok (például a Proof of Stake) és új típusú hálózatok (nyilvános, magán- és konzorciumi blokkláncok) jelentek meg, amelyek különböző használati esetekhez igazodnak.

A jelen kor kihívásai – így a digitális biztonság, az átláthatóság, az adatvédelem és az automatizálás iránti igény – tovább növelik a blokkláncok jelentőségét. Egyre több iparág keresi azt, miként tudná kihasználni a technológia olyan sajátosságait, mint a megmásíthatatlan tranzakciós napló, a decentralizált irányítás vagy a programozható pénzügyi logika. Ugyanakkor a blokkláncok elterjedését számos kihívás is kíséri, többek között a skálázhatóság, az energiafelhasználás, a szabályozási kérdések és a felhasználói biztonság problémái. Ezek a tényezők jól mutatják, hogy a blokklánc még fejlődő, dinamikusan változó technológiai terület, amely egyszerre rejt magában komoly lehetőségeket és kockázatokat.

Jelen dolgozat célja, hogy bemutassa a blokkláncok fejlődését a kezdetektől a Bitcoin-bányászaton keresztül az okosszerződésekig, áttekintve a technológia kialakulását, legfontosabb mérföldköveit és a mögötte álló konszenzusmechanizmusokat. Emellett részletesen foglalkozik a blokkláncok jelenlegi és jövőbeli felhasználási területeivel, különös tekintettel arra, hogyan alakíthatják át a gazdasági és társadalmi folyamatokat. A bevezető fejezetet követően a dolgozat először a technológia történeti és elméleti hátterét ismerteti, majd a különböző blokklánc-megoldások működését és konszenzusmechanizmusait elemzi, végül pedig áttekinti a gyakorlati alkalmazásokat és a várható fejlődési irányokat.

2. fejezet

Elméleti alapok – pénz, kriptográfia, decentralizáció

A dolgozat elméleti részében először a pénz, a decentralizáció és a kriptográfia fogalmait tekintjük át, mivel a blokklánc-technológia ezek metszetében helyezkedik el. A pénz és az érték közgazdasági megközelítése rávilágít arra, milyen funkciókat kell egy pénzszerű eszköznek betöltenie, és miben tér el ettől a kriptovaluták működése. A centralizált és decentralizált rendszerek összehasonlítása segít megérteni, miért jelent újdonságot egy olyan pénzügyi és adatkezelési modell, amely nem egy központi szereplőre, hanem egy elosztott hálózatra épül. A kriptográfia bemutatása pedig azért elengedhetetlen, mert a blokklánc biztonságát, a tranzakciók hitelességét és a felhasználók azonosítását – vagy éppen pseudonimitását – a modern kriptográfiai eljárások teszik lehetővé. E három terület rövid áttekintése teremti meg azt az elméleti alapot, amelyre a későbbi fejezetekben a Bitcoin, a blokkláncok és az okosszerződések részletes bemutatása épül.

2.1. A pénz és az érték fogalma röviden

A pénz legegyszerűbb meghatározása szerint a társadalomban általánosan és azonnal felhasználható csere- és fizetési eszköz. Átadásával lehet javakat és szolgáltatásokat megvásárolni, illetve adósságokat törleszteni.[1]

Az érték hétköznapi szóhasználatban mindaz, ami valaki számára jelentős, fontos, lényeges valamilyen szempontból. Beszélünk anyagi értékekről (lakás, ékszer, autó stb.) és szellemi értékekről (barátság, békesség, szeretet stb.). Meghatározott – erkölcsi, kulturális, esztétikai stb. – értékek általános és alapvető tájékozódási mértéket (mércét) tartalmaznak azon esetekben, amikor különböző cselekvési alternatívák között kell választani.[2]

A pénzhez szorosan kapcsolódik az érték fogalma. Közgazdasági szempontból az érték sokszor a hasznossággal, illetve a szűkösséggel függ össze: egy jószág annál értékesebb, minél nagyobb hasznosságot nyújt a fogyasztó számára, és minél korlátozottabb a rendelkezésre álló mennyisége. A pénz önmagában többnyire nem rendelkezik közvetlen fogyasztási hasznossággal (különösen a digitális pénz esetében), értékét az adja, hogy más javakra és szolgáltatásokra váltható.

Az érték kérdése a digitális korban új megvilágításba került. A kriptovaluták és a blokklánc-technológia megjelenésével olyan digitális, nem állami pénzformák jelentek meg, amelyek értékét nem központi banki szabályozás vagy állami garancia, hanem algoritmusok, kriptográfiai szabályok és a hálózat résztvevőinek konszenzusa határozza meg. A szűkösség ebben az esetben nem fizikai tulajdonság, hanem programkód által rögzített paraméter. Ezzel a pénz és az érték fogalma elmozdul a hagyományos, intézményalapú modellből egy decentralizált, bizalom- és technológiaalapú modell irányába, amelynek megértése kulcsfontosságú a blokkláncok fejlődésének vizsgálatához.

[1] Bácskai Tamás – Huszti Ernő – Simon Péterné: *A pénz*. Budapest: Kossuth, 1974.
[2] Dr. Poór Ferenc: Érdek, értékfelfogás.

2.2. Kriptográfia – a kódolás tudománya

Maga a kriptográfia egy görög eredetű szó (kriptos = eltitkolt, graphein = írni), mely alatt egészen a 70-es évekig elsősorban az üzenetek titkosításának módszereit értették. Jelentése azonban mára kibővült:

> „A kriptográfia azoknak a matematikai eljárásoknak, algoritmusoknak, biztonsági rendszabályoknak kutatását, alkalmazását jelenti, amelyek elsődleges célja az információnak illetéktelenek elől való elrejtése."[3]

A kriptográfia a blokklánc-technológia alapja: enélkül a blokklánc nem tudna biztonságosan működni. A rendszerben a világ jelenleg ismert egyik legbiztonságosabb kódolási módszereit használják, ezért a tranzakciók hamisítása gyakorlatilag lehetetlen.

A blokkláncokban elsősorban a nyilvános kulcsú kriptográfia és a kriptográfiai hash függvények a legfontosabb eszközök. Minden felhasználó egy privát–nyilvános kulcspárral rendelkezik: a privát kulcsot titokban tartja, ezzel írja alá digitálisan a tranzakcióit, a nyilvános kulcsból képzett cím pedig azonosítja őt a hálózatban. A hash függvények gondoskodnak arról, hogy a blokkok egymáshoz legyenek láncolva, és ha valaki utólag megpróbálna módosítani egy már rögzített adatot, annak a hash-értéke azonnal megváltozna, így a manipuláció könnyen észrevehetővé válik.

Fontossága a blokkláncok világában megkérdőjelezhetetlen, hiszen egyszerre biztosítja a hitelesítést, az adatintegritást és a felhasználók (pontosabban: pseudonim) anonimitását. Hagyományos pénzrendszerek esetén az általunk végzett, valamint fogadott tranzakciókat ugyan le tudjuk ellenőrizni, de ehhez egy harmadik félre (bankra, pénzintézetre) kell támaszkodnunk. Blokkláncok esetében azonban nincs szükség központi szereplőre: a hálózat minden tagja ugyanahhoz a főkönyvhöz fér hozzá, bárki tranzakciói visszakövethetők a

[3]IT biztonsági fogalomtár: `https://www.fogalomtar.hu`

kezdetekig, miközben az ügyletek mögötti természetes személy kiléte rejtve marad, csak a kriptográfiai azonosító jelenik meg. Ez a sajátos kombináció – nyilvános, átlátható főkönyv és kriptográfián alapuló pseudonimitás – a blokklánc-technológia egyik legfontosabb újítása.

2.3. Centralizált és decentralizált világ

A mai pénzügyi és informatikai rendszerek többsége centralizált: egy központi szereplő (bank, állam, nagyvállalat) határozza meg a szabályokat, vezeti a nyilvántartást és hagyja jóvá a tranzakciókat. Előnye, hogy jól szervezhető és hatékony, ugyanakkor sérülékeny a „single point of failure" problémája miatt: ha a központi rendszer leáll, hibázik vagy támadás éri, az egész szolgáltatás megbénulhat, és az adatok is veszélybe kerülhetnek.[4]

A decentralizált modell ezzel szemben az irányítást és az adatkezelést sok, egymástól független résztvevő között osztja meg. Ilyen példák a peer-to-peer (P2P) hálózatok – például a BitTorrent –, ahol a felhasználók közvetlenül egymással osztanak meg adatokat központi szerver nélkül.[5] A blokklánc-technológia ugyanezt az elvet alkalmazza a tranzakciós főkönyvre: a nyilvántartást nem egy adatbázis-szerver, hanem a hálózat számos csomópontja tartja fenn, és a résztvevők egy konszenzusmechanizmus alapján döntenek arról, mi tekinthető érvényes állapotnak. Ez ellenállóbbá teszi a rendszert hibákkal, támadásokkal és cenzúrával szemben.[6]

A gyakorlatban jelenleg egy hibrid állapotban vagyunk: a legtöbb hétköznapi szolgáltatás továbbra is centralizált, miközben gyorsan terjednek a decentralizált megoldások (kriptovaluták, DeFi, DAO-k, Web3-projektek), ahol a közösség nagyobb beleszólást kap az irányításba. Ezzel párhuzamosan a szabályozói környezet is alakul: az Európai Unió például a MiCA-rendelet (Regulation (EU) 2023/1114) révén igyekszik egységes keretet adni a kriptoeszköz-

[4] https://www.geeksforgeeks.org/system-design/comparison-centralized-decentralized-and-distri
[5] https://www.britannica.com/technology/BitTorrent
[6] https://www.geeksforgeeks.org/system-design/comparison-centralized-decentralized-and-distri

piacnak, úgy, hogy egyszerre védje a befektetőket és teret engedjen az innovációnak.[7]

2.4. A kriptovilág indulása

A kriptovilág indulásának időpontját jóval a Bitcoin megjelenése előtt kell keresnünk. Egészen az 1980-as évek végéig kell visszautaznunk az időben, amikor Timothy C. May amerikai informatikus és kriptográfus megfogalmazta, majd a kilencvenes évek elején ismertté tette „The Crypto Anarchist Manifesto" című kriptoanarchista kiáltványát. May már ekkor nagyon pontosan leírta, hogy a számítógépes hálózatok és az internet terjedésével milyen szerepe lesz a kriptográfiának:

> „Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact in a totally anonymous manner."
> (Timothy C. May, *The Crypto Anarchist Manifesto*, ∼1988/1992)

Magyarul: a számítógépes technológia a küszöbén áll annak, hogy lehetővé tegye az egyének és csoportok számára a teljesen anonim kommunikációt és interakciót. May víziója szerint a kriptográfia alapjaiban fogja megváltoztatni az állam szabályozó szerepét, az adóztatást, az információ feletti kontrollt és a bizalom természetét.

A következő fontos mérföldkő 1993, amikor megszületett „A Cypherpunk's Manifesto", a Cypherpunk-kiáltvány, amely egy amerikai matematikus és programozó, Eric Hughes nevéhez köthető. Ő már pontosan lefektetett néhány olyan elvet, amely közvetlenül befolyásolja azt, ahogyan ma internetezünk és digitális szolgáltatásokat használunk. Hughes rámutatott, hogy a magánszféra nem azonos a titkolózással: a magánszféra lényege az, hogy az

[7] `https://eur-lex.europa.eu/hu/legal-content/summary/european-crypto-assets-regulation-mica.html`

egyén maga dönthesse el, kinek, mikor és mennyit fed fel magából. Szavaival élve: „privacy is the power to selectively reveal oneself to the world", vagyis a magánszféra a szelektív önfeltárás képessége.

Hangsúlyozza azt is, hogy a magánszférát nem az állam vagy a vállalatok fogják megvédeni helyettünk: „We must defend our own privacy if we expect to have any. We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography...". A Cypherpunkok tudatosan olyan technológiákat (anonim rendszerek, kriptográfia, elektronikus pénz) akartak építeni, amelyekkel az emberek ténylegesen megvédhetik magánszférájukat az elektronikus korban.[8]

A kriptovilág indulása természetesen konkrét technikai kísérletekkel is járt. Az első név, akit ezzel kapcsolatban érdemes megemlíteni, Nick Szabo, magyar származású amerikai jogász és informatikus, aki a kilencvenes évek végén dolgozta ki *bit gold* nevű koncepcióját. A bit goldból soha nem lett ténylegesen használt kriptovaluta, de Szabo volt az elsők egyike, aki a digitális pénz kapcsán megfogalmazta és kezelni próbálta az úgynevezett *double-spending* problémát. A „kettős költés" azt jelenti, hogy ugyanazt a digitális pénzegységet valaki jogosulatlanul többször próbálja elköteni; Szabo javaslata már elosztott nyilvántartásban gondolkodott, banktól függetlenül.

Ha visszaugrunk néhány évet az időben, David Chaum 1989-ben alapított cége, a DigiCash hozta létre az *ecash* nevű elektronikus készpénzrendszert, amely a kilencvenes években sokak figyelmét felkeltette. A DigiCash nem blokklánc-alapú kriptovaluta volt, hanem központi szereplő (a cég és a vele szerződő bankok) által működtetett, kriptográfián alapuló e-pénzmegoldás: erős, kétkulcsú titkosítást használt, és anonim, készpénzszerű tranzakciókat tett lehetővé. Centralizált működése, az üzleti modell és a szabályozási környezet miatt azonban a vállalat végül 1998-ban csődbe ment, így a rendszer nem terjedt el széles körben.

Ezek a törekvések stabil alapot adtak Wei Dai kínai származású informatikusnak, aki 1998-ban megalkotta a *b-money* nevű rendszert. A b-money-t

[8]Eric Hughes (1993): *A Cypherpunk's Manifesto.*

inkább egy korai, elméleti kriptodeviza-ötletnek tekinthetjük: olyan digitális pénzt képzelt el, amelyet számítógépek munkájával lehet „előállítani”, nagyjából abban az értelemben, ahogy ma a bányászatot értjük. Maga az a gondolat, hogy a gépek számítási kapacitását használjuk fel ilyen „digitális munkára”, már 1997-ben megjelent Adam Back Hashcash nevű spam-szűrő rendszerében, de a b-money ezt a szemléletet vitte tovább egy pénzrendszer irányába. A b-money végül soha nem valósult meg működő hálózatként, többek között azért, mert akkor még nem volt meg az a blokklánc-technológiai háttér, amelyre később a Bitcoin épült.

Összességében látható, hogy a kriptovilág nem a semmiből született: May, Hughes, Chaum, Szabó, Wei Dai és társaik mind egy-egy darabját rakták le annak a gondolati és technológiai alapnak, amire később a modern kriptodevizák épültek. Ezek a korai próbálkozások ugyan többnyire nem jutottak el a széles körű gyakorlati használatig, mégis megmutatták, hogy létezhet bankoktól és államoktól független, digitális pénz. A következő fejezetben azt vizsgálom meg, hogyan jelent meg erre a háttérre építve a Bitcoin, és miben hozott valódi áttörést.

3. fejezet

A Bitcoin megszületése és fejlődése