Kriptovaluták elméleti háttere

Ladóczki Bence
docens
Távközlési és Mesterséges Intelligencia Tanszék (TMIT)
Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar (VIK)
ladoczki.bence@vik.bme.hu

2026. november 3.

1 DeFi hitelezési protokollok: Morpho és társai

Az AMM-ekhez hasonlóan a hitelezési protokollok is a decentralizált pénzügyek (DeFi) alapvető részei. A betétes eszközt helyez el egy okosszerződésben; a hitelfelvevő pedig egy másik eszközt vesz kölcsön. A kölcsönt általában fedezettel kell biztosítani, és a fedezet értékének nagyobbnak kell lennie az adósságénál. A kamatot a protokoll szabályai számítják ki, jellemzően attól függően, hogy a betétek mekkora részét vették már kölcsön.

Kihasználtság és kamat. Jelölje A az adott eszközből a piacra befizetett teljes mennyiséget, B pedig a vissza nem fizetett kölcsönök teljes mennyiségét. A piac kihasználtsága az alábbi hányados:

$$U = \frac{B}{A}, \qquad 0 \le U \le 1. \tag{1}$$

Ha például $U = 0{,}8$, akkor a befizetett eszközök 80%-át kölcsönadták. Az $U = 1$ érték azt jelenti, hogy az adott eszközből minden betét ki van kölcsönözve; ilyenkor új befizetés vagy visszafizetés nélkül a betétesek nem tudják kivenni a kölcsönadott mennyiséget.

Az egyszerűsített kamatmodellben a hitelfelvevők évesített kamata a kihasználtságtól függ. A modell a U^* értéknél vált enyhe emelkedésről meredekebb emelkedésre:

$$r_b(U) = \begin{cases} r_0 + \dfrac{U}{U^*} m_1, & U \le U^*, \\[2ex] r_0 + m_1 + \dfrac{U - U^*}{1 - U^*} m_2, & U > U^*. \end{cases} \tag{2}$$

Itt $r_b(U)$ a hitelfelvevő évesített kamatlába, r_0 az alapkamata, U^* a kihasználtsági fordulópont, m_1 az első szakaszban hozzáadódó kamatemelkedés, m_2 pedig a fordulópont fölötti további kamatemelkedés. A modellben $0 < U^* < 1$; az egyenlet a fordulópontnál folytonos, és a felső szakasz meredekebb lehet. A magas kihasználtságra adott magasabb kamat mérsékelheti az új kölcsönök iránti keresletet, és ösztönözheti a betéteket, de nem

garantálja, hogy minden betétes azonnal ki tudja venni az eszközét. Minden kamatot és kamatemelkedést tört alakban kell behelyettesíteni; például évi 5% kamatot 0,05 alakban.

Jelölje r_s a betétes évesített kamatlábát, ϕ pedig a kamatból a protokollnál maradó hányadot, ahol $0 \leq \phi \leq 1$. A közös likviditási alapra használt egyszerű közelítés:

$$r_s \approx U\, r_b(U)(1-\phi). \tag{3}$$

Azért szerepel benne U, mert csak a kölcsönadott betétek után fizetnek kamatot; a protokollnál maradó hányadot pedig nem kapják meg a betétesek. Ez szemléltető képlet: a tényleges kamatszámítás protokollonként és piaconként eltérhet, a jutalmak és a kamatos kamat hatása pedig nincs benne.

Fedezet és kényszerértékesítés. A protokoll a fedezet és az adósság értékét közös elszámolási egységben, például dollárban hasonlítja össze. Több fedezeti eszközt kezelő piacon jelölje C_i az i-edik fedezet dollárértékét, LT_i pedig annak kényszerértékesítési küszöbét arányként, 0 és 1 között. Az i index a fedezettípusokat különbözteti meg. Jelölje D az összes fennálló tartozás dollárértékét; hitel esetén $D > 0$. Az egészségi mutató:

$$\mathrm{HF} = \frac{\sum_i C_i LT_i}{D}. \tag{4}$$

Az összeg a különböző fedezetek értékét a hozzájuk tartozó küszöbbel súlyozza. Ha $\mathrm{HF} > 1$, a pozíció a küszöb fölött van; ha $\mathrm{HF} < 1$, a protokoll szabályai szerint kényszerértékesíthetővé válik. Egyetlen fedezeti eszköznél a képlet egyszerűsödik: $\mathrm{HF} = C\,LT/D$, ahol C a fedezet értéke és LT annak kényszerértékesítési küszöbe [1]. Az egészségi mutató nem százalék, hanem dimenzió nélküli arány; az 1 fölötti érték biztonsági tartalékot jelez.

A maximális hitel/fedezet arányt LTV jelöli; ez 0 és 1 közötti arány. Egy fedezeti eszköz esetén az induláskor felvehető hitelre az alábbi korlát vonatkozik:

$$D \leq \mathrm{LTV} \cdot C. \tag{5}$$

Az LTV és az LT nem feltétlenül azonos: az előbbi a hitelfelvétel megengedett felső határa, az utóbbi pedig azt jelzi, mikor válik a már fennálló pozíció kényszerértékesíthetővé. A Morpho elkülönített piacain használt LLTV a kényszerértékesítési hitel/fedezet arány felső határa, szintén 0 és 1 közötti érték. Itt C az egyetlen elfogadott fedezet értéke, D a kölcsön értéke, és a pozíció addig nem érheti el a kényszerértékesítési határt, amíg $D \leq \mathrm{LLTV} \cdot C$.

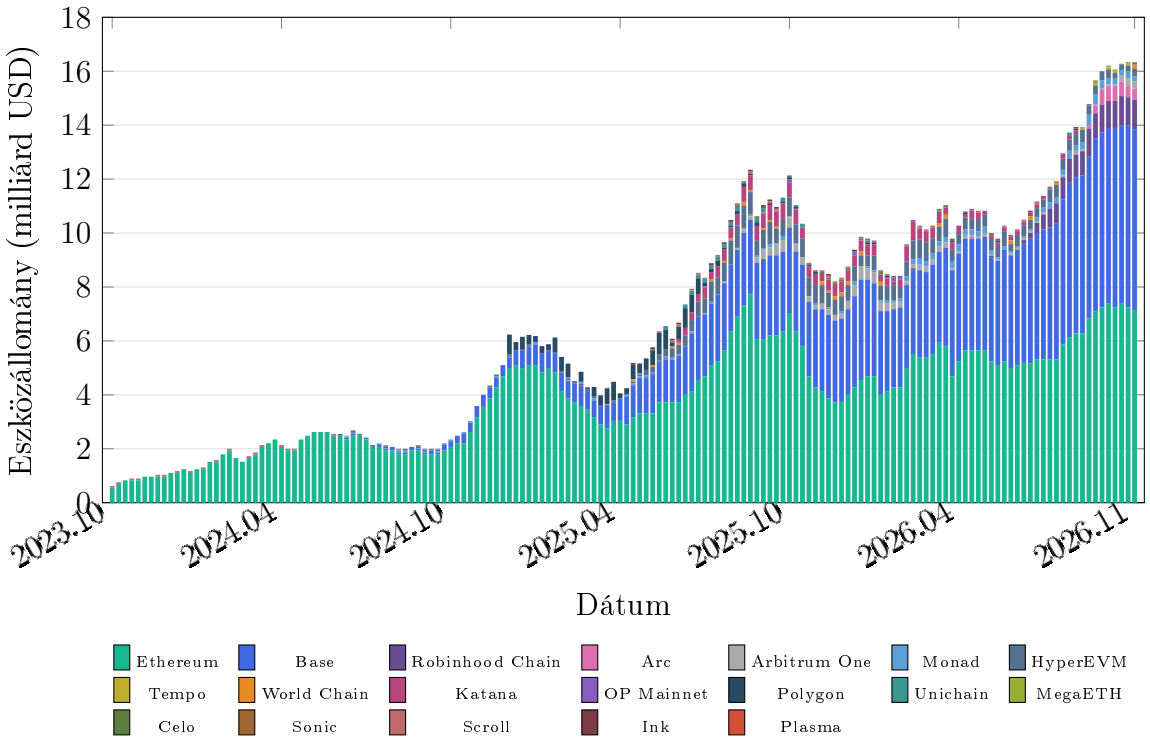
Kényszerértékesítéskor egy másik hálózati szereplő visszafizeti az adósság egy részét, és cserébe a fedezetből a visszafizetett összegnél nagyobb értékű részt kap. A különbség a kényszerértékesítési jutalom; ez ösztönzi a szereplőket, hogy a veszélyes pozíciókat időben rendezzék. A fedezet értékének hirtelen esése, a hibás árfolyamadat vagy a hálózat torlódása azonban azt eredményezheti, hogy a fedezet már nem elég az adósság teljes visszafizetésére.

Közös likviditási alapok és elkülönített piacok.

- **Közös likviditási alap.** Az azonos kölcsöneszköz betétei és kölcsönei egy közösen használt piac részei. Többféle fedezet is elfogadható, de a piac szabályai és kockázati korlátai közösek. Az Aave V3 ilyen hitelezési rendszer: a felhasználó több eszközt is betétbe helyezhet fedezetként, miközben a kamatlábak eszközönként változnak. A Compound V3 piacai egy megadott kölcsöneszköz köré épülnek, a hitelhez pedig az adott piacon engedélyezett fedezeti eszközök használhatók [2].

- **Elkülönített piac.** Minden piac egy kölcsöneszközt és egy fedezeti eszközt kapcsol össze, saját árfolyam-forrással, kamatszámítási szabállyal és kényszerértékesítési hitel/fedezet aránnyal. A Morpho Blue piacainak szabályai a létrehozás után nem változtathatók meg, és minden piac külön kezeli a saját kockázatát. A piacokat engedély nélkül létre lehet hozni, de a kockázati paraméterek kiválasztására a Morpho irányítása által jóváhagyott értékkészlet vonatkozik [3].

Morpho Blue piacaira épülnek a *Morpho Vaults* betétgyűjtő szerződések. Egy betétgyűjtő több elkülönített piac között oszthatja szét a felhasználók eszközeit. A kockázati kezelő határozza meg, mely piacokat használhatja a betétgyűjtő, és milyen korlátok között oszthatja el a tőkét. Ez egyszerűsíti a betétes dolgát, de nem szünteti meg a kockázatot: a betétesnek a betétgyűjtő szabályaiban és a kockázati kezelő döntéseiben is meg kell bíznia [4]. A Morpho hálózatonkénti heti TVL-alakulását az ábra szemlélteti.



1. ábra: A Morpho heti átlagos, hálózatonkénti zárolt értéke (TVL), 2023. október 30. és 2026. november 2. között.

Morpho közvetlen hitelező–hitelfelvevő illesztése. A Morpho korábbi optimalizáló rendszere az Aave vagy a Compound közös likviditási alapjára épült. Először megpróbálta közvetlenül egymáshoz illeszteni a betétesek és hitelfelvevők igényeit; csak az illesztetlen összegek kerültek a hátterében álló közös likviditási alapba. Ha az illesztett rész kamatlábát külön modellként írjuk le, akkor:

$$r_m = \theta r_b + (1-\theta) r_s, \qquad 0 \le \theta \le 1. \tag{6}$$

Itt r_m a közvetlenül illesztett összeg évesített kamata, r_b a hitelfelvevői kamat, r_s a betétesi kamat, θ pedig azt mutatja, hol helyezkedik el az illesztett kamat a két kamat között. Így az illesztett rész után a hitelfelvevő kevesebbet fizethet, a betétes pedig többet kaphat,

mint a mögöttes likviditási alapban. Ez a korábbi rendszer nem azonos a ma használt Morpho Blue elkülönített piacaival; a Morpho Optimalizáló rendszereinek működését a Morpho irányítása fokozatosan leállította [5, 6].

Példák és kockázatok. Az Aave V3 és a Compound V3 közös likviditási alapokra épülő hitelezési rendszerek; a Morpho Blue elkülönített piacokat, a Morpho Vaults pedig több ilyen piac között elosztó betétgyűjtőket kínál. Az Euler V2, a Silo, a Fluid, a Venus és a JustLend szintén hitelezési protokollok, de a piacaik szabályai és felépítése eltérhetnek. Ezeknél a rendszereknél nincs egyetlen állandó betéti hozam: a kamat a kereslettel, a kihasználtsággal, a piaci szabályokkal és az esetleges jutalmakkal együtt változik.

A fő kockázatok a fedezet árának esése; a hibás vagy késve frissülő árfolyam-forrás; a nagy kihasználtság miatt átmenetileg elérhetetlenné váló betét; a kényszerértékesítés során felmerülő árhatás és hálózati díj; az okosszerződés hibája; valamint az elkülönített piac vagy betétgyűjtő rosszul megválasztott szabályai. A fedezet és a kényszerértékesítési szabályok csökkentik a veszteség esélyét, de nem garantálják, hogy minden adósság teljes egészében visszafizethető lesz.

Hivatkozások

[1] Aave, *Frequently Asked Questions: Health Factor and Liquidations*. https://aave.com/faq

[2] Aave, *Aave V3 Overview*, Aave Documentation. https://www.aave.com/docs/aave-v3/overview

[3] Morpho, *Variable Rate Market (Morpho Blue)*, Morpho Documentation. https://docs.morpho.org/learn/concepts/blue/

[4] Morpho, *Curator*, Morpho Documentation. https://docs.morpho.org/learn/concepts/curator/

[5] Morpho, *Morpho Optimizer Yellow Paper*. https://yellowpaper.morpho.org/

[6] Morpho, *Terms of Use*, Morpho Protocols. https://morpho.org/terms-of-use