

Gulyás Attila ny. alezredes:

# DZSIHADISTA TERRORSZERVEZETEK KRIPTOVALUTA ALAPÚ ONLINE ADOMÁNYGYŰJTÉSE

DOI: 10.35926/HSZ.2024.5.4

*ÖSSZEFOGLALÓ: A terrorizmus elleni sokrétű harc egyik meghatározó eleme a szervezetek anyagi eszközeiktől történő megfosztása és pénzügyi műveleteik korlátozása, illetve akadályozása. Egyes feltételezések szerint a nemzetközileg összehangolt terrorizmus-finanszírozás elleni (Counter-Terrorist Financing, CTF) és pénzmosás elleni (Anti-Money Laundering, AML) intézkedések hatására a dzsihadista terrorszervezetek a fiat valutákkal<sup>1</sup> lebonyolított hagyományos pénzügyi műveletektől a központi felügyeletet és ellenőrzést nélkülöző kriptovaluták felé fordulnak. Ugyanakkor a szélsőséges iszlamista terrorszervezetek kriptovaluta-használatának módjával és mértékével kapcsolatban számos egymásnak ellentmondó vélemény és nyilatkozat látott napvilágot. A szerző kutatásában azt vizsgálja, hogy a dzsihadista terrorszervezetek az online adománygyűjtéseik alkalmával milyen mértékben használják ki a kriptovaluták nyújtotta előnyöket. A felmérés eredménye hozzájárulhat a kriptovaluta-használat valós mértékének meghatározásához. A szerző különböző OSINT<sup>2</sup>-eszközök és -eljárások alkalmazásával a nyílt interneten és a dark weben dzsihadista weboldalakat kutatott fel abból a célból, hogy megvizsgálja, mennyire jellemző az egyes dzsihadista terrorszervezetekre a kriptovalutában történő adománykérés. A kutatás során felderített weboldalak elemzését követően megállapította, hogy a vizsgált terrorszervezetekre nem jellemző a kriptovalutában történő online adománygyűjtés.*

*KULCSSZAVAK: kriptovaluta, terrorizmus, finanszírozás, adománygyűjtés, bitcoin*

## A SZERZŐRŐL:

*Gulyás Attila ny. honvéd alezredes, az Óbudai Egyetem Biztonságtudományi Doktori Iskola végzős hallgatója (ORCID: 0000-0001-5645-144X; MTMT: 10074524)*

## BEVEZETÉS

A terrorizmus elleni nemzetközi küzdelem egyik legfontosabb összetevője a terrorszervezetek pénzügyi műveleteinek felderítése, akadályozása és korlátozása, ami csak nemzetközi szinten összehangolt terrorizmus-finanszírozás elleni (Counter-Terrorist Financing, CTF) és pénzmosás elleni (Anti-Money Laundering, AML) intézkedések bevezetésével lehetséges. A Financial Action Task Force (FATF), a Nemzetközi Valutaalap (International Monetary Fund), az ENSZ, a Világbank és más nemzetközi szervezetek összefogásának eredményeként eddig már számos esetben sikerült érzékeny veszteséget okozni a szélsőséges iszlamista

<sup>1</sup> A fiat valuta olyan pénznem, amelyet kormányok és központi bankok bocsátanak ki, és amelyet nem értékes árucikk garantál, mint például arany vagy ezüst. A fiat (lat.) jelentése: legyen.

<sup>2</sup> Open Source Intelligence – a nyílt forrású hírszerzés nemzetközileg is elfogadott angol nyelvű rövidítése.

terroriszervezetek pénzügyi rendszerében. A sikerek fényében a rendvédelmi szervek és a politikai döntéshozók részéről felmerült a lehetősége annak, hogy ezek a veszteségek arra sarkallhassák a technikai újdonságokra fogékony terroriszervezeteket, amelyek egyre aktívabban a kibertérben,<sup>3</sup> hogy pénzügyi műveleteikben a hagyományos valutákat (fiat valuták) az időközben növekvő népszerűségnek örvendő, központi ellenőrzést nélkülöző kriptovalutákra cseréljék, amelyek segítségével a pénzügyi korlátozó intézkedéseket kijátszhatják.

A további sikeres terrorizmus-finanszírozás elleni harc érdekében tisztázásra szorul, hogy a szóban forgó terroriszervezetek valóban áttértek-e a kriptovaluták használatára, és ha igen, akkor pénzügyi műveleteik rendszerében az eddigiekhez képest milyen jellegű műveletekben és milyen mértékben változott meg a hagyományos és a kriptovaluta-kötődésű műveletek aránya.

Jelenleg egyfajta bizonytalanság és egymásnak ellentmondó feltételezések állnak rendelkezésre a kriptovaluta-használat jellegére és mértékére vonatkozóan. A bizonytalanság egyrészt a terroriszervezetek működésére jellemző konspirációnak, másrészt a kriptovalutákkal, főleg azok anonimitásával kapcsolatos félreértéseknek és az ezekből származó mítoszoknak köszönhető.

Az adománygyűjtés és ezen belül is az online adománygyűjtés része a szélsőséges iszlamista terroriszervezetek pénzügyi rendszerének, hiszen bevételeik egy része ebből a forrásból származik, ezért kutatásomban azt vizsgáltam, hogy a terroriszervezetek az online adománygyűjtéseik alkalmával milyen mértékben használják ki a kriptovaluták nyújtotta előnyöket. Véleményem szerint a felmérés eredménye hozzájárulhat a kriptovaluta-használat valós mértékének meghatározásához és a várható tendenciák előrejelzéséhez.

A kutatás során személyes adatokat nem kezeltem. A terroriszervezetek tagjaival a büntetőjogi következmények elkerülése érdekében nem kommunikáltam. Tanulmányomban, ahol eredeti terroristaeredetű tartalmat mutattam be, annak pontos elérhetőségét a tartalom terjesztésének elkerülése érdekében szándékosan eltorzítottam. A kutatás megismételhetőségének érdekében az adatbázis-építésnél alkalmazott OSINT-eszközöket és -módszereket a szükséges mértékig bemutattam.

## A KRIPTOVALUTA-HASZNÁLATTAL KAPCSOLATOS ELLENTMONDÁSOK

A New York Times 2019-ben<sup>4</sup> az Amerikai Egyesült Államok pénzügyminiszterére és egy meg nem nevezett egykori CIA-elemzőre hivatkozva arra hívta fel a figyelmet, hogy a terroriszervezetek egyre inkább elfordulnak a hagyományos valutáktól, helyettük a kriptovalutákat használják. Az amerikai CNAS (Center for a New American Security) 2020-ban készült jelentése szerint<sup>5</sup> a terrorcsoportok a kriptovaluta alapú online adománygyűjtés céljából egyre gyakrabban veszik igénybe a közösségi média nyújtotta lehetőségeket. A jelentés szerint a terrorcsoportok hozzáértő digitális szereplőkké válnak.

Whang és Zhu<sup>6</sup> a kriptovaluta szerepét vizsgálták a terroriszervezetek pénzügyi műveleti rendszerében, és arra a megállapításra jutottak, hogy az új digitális fizetőeszköz fontos szerepet játszik ugyan, de mennyisége nem tekinthető jelentősnek. ENSZ-szakértőkre

<sup>3</sup> Besenyő et al. 2021.

<sup>4</sup> Popper 2019.

<sup>5</sup> Dorshimer 2020.

<sup>6</sup> Wang–Zhu 2021.

hivatkozva<sup>7</sup> 2023-ban a Reuters arról tudósított, hogy a terrorszervezetek kriptovaluta-használata valószínűsíthetően nem jelentős.

Ezzel szemben az ENSZ Biztonsági Tanácsának Terrorizmusellenes Bizottsága 2020. október 28–29. között Mumbaiban megtartott ülését követően Svetlana Martynova, a terrorizmus finanszírozása elleni küzdelem koordinátora sajtótájékoztatót tartott, ahol újságírói kérdésre elmondta, hogy a terrorszervezetek kriptovaluta-használata jelentős mértékben (5%-ról 20%-ra) növekedett, és további emelkedésre lehet számítani.<sup>8</sup>

Ennek ellentmondani látszik a nemzetközi elismertségnek örvendő blokklánc-elemző vállalat, a Chainalysis jelentése,<sup>9</sup> amely szerint az összes illegális kriptovaluta-forgalom mindössze egy százaléka köthető terrorizmus-finanszírozáshoz. Ezzel szemben az ugyancsak kriptovalutablokklánc-elemző Elliptic nevű vállalat jelentése szerint<sup>10</sup> a terrorszervezetek kriptovaluta-használata meredeken emelkedik.

A kriptovalutára specializálódott Coindesk nevű szaklap pedig arról tudósított,<sup>11</sup> hogy szenátusi meghallgatásán Janet Yellen, az Amerikai Egyesült Államok pénzügyminisztere a kriptovaluták a terrorizmus finanszírozásában betöltött szerepét rendkívül aggasztónak találja. Ezt alátámasztani látszik az ENSZ Biztonsági Tanácsa Szankciómonitorozási Csoportjának 2021-ben írott levele,<sup>12</sup> amely arról számol be, hogy az Iszlám Állam és az al-Kaida kriptovaluta-használata növekszik. Példaként említik, hogy a francia rendőrség felszámolt egy hálózatot, amelynek tagjai kis összegű kriptovaluta-kuponokat vásároltak, és ezeknek a titkos kódját a szíriai HTS (Hay'at Tahrir al-Sham) terrorszervezet tagjainak juttatták el, akik felhasználták a kuponokat.

Az Európai Unió Emberjogi és Alkotmányügyi bizottsága által készített jelentés<sup>13</sup> szerint a terrorszervezetek kriptovaluta-használatát nehéz megbecsülni. A dokumentum szerint a terrorszervezetek keresik a módját az új fizetőeszköz mind szélesebb körű felhasználhatóságának. A jelentés vélelmezi, hogy a kriptovalutát a közösségi médiában folytatott adománygyűjtésre, illegális eszközök és javak sötét weben történő beszerzésére fordítják majd. Elképzelhetőnek tartják, hogy a hagyományos banki átutalások kiváltására is igénybe vehetik.

Wiwoho és kollégái tanulmányukban<sup>14</sup> a Délkelet-Ázsiában működő szélsőséges iszlamista terrorszervezetek kriptovaluta-használatát vizsgálták meg, és arra a következtetésre jutottak, hogy az al-Kaida és az Iszlám Állam társult szervezetei gyakran használnak kriptovalutát az akcióik finanszírozásához. Véleményük szerint a szabályozottság hiánya miatt ez egyre inkább jellemző lesz a térségben.

A válogatásból látható, hogy a terrorszervezetek kriptovaluta-használatának mértékével kapcsolatban nagyfokú bizonytalanság tapasztalható. Szakértők, szakpolitikusok és nemzetközi szervezetek is egymásnak ellentmondó véleményeket fogalmaznak meg.

<sup>7</sup> The United Nations Global... 2023.

<sup>8</sup> UN says crypto use... 2022.

<sup>9</sup> Chainalysis Team 2023.

<sup>10</sup> Elliptic 2023a.

<sup>11</sup> De N. 2021.

<sup>12</sup> Letter dated 21 January 2021... 2021, 18.

<sup>13</sup> Virtual Currencies and terrorist financing... 2018, 9.

<sup>14</sup> Wiwoho et al. 2023, 102–124.

## AZ ADOMÁNYGYŰJTÉS HELYE ÉS SZEREPE A DZSIHADISTA TERRORSZERVEZETEK PÉNZÜGYI RENDSZERÉBEN

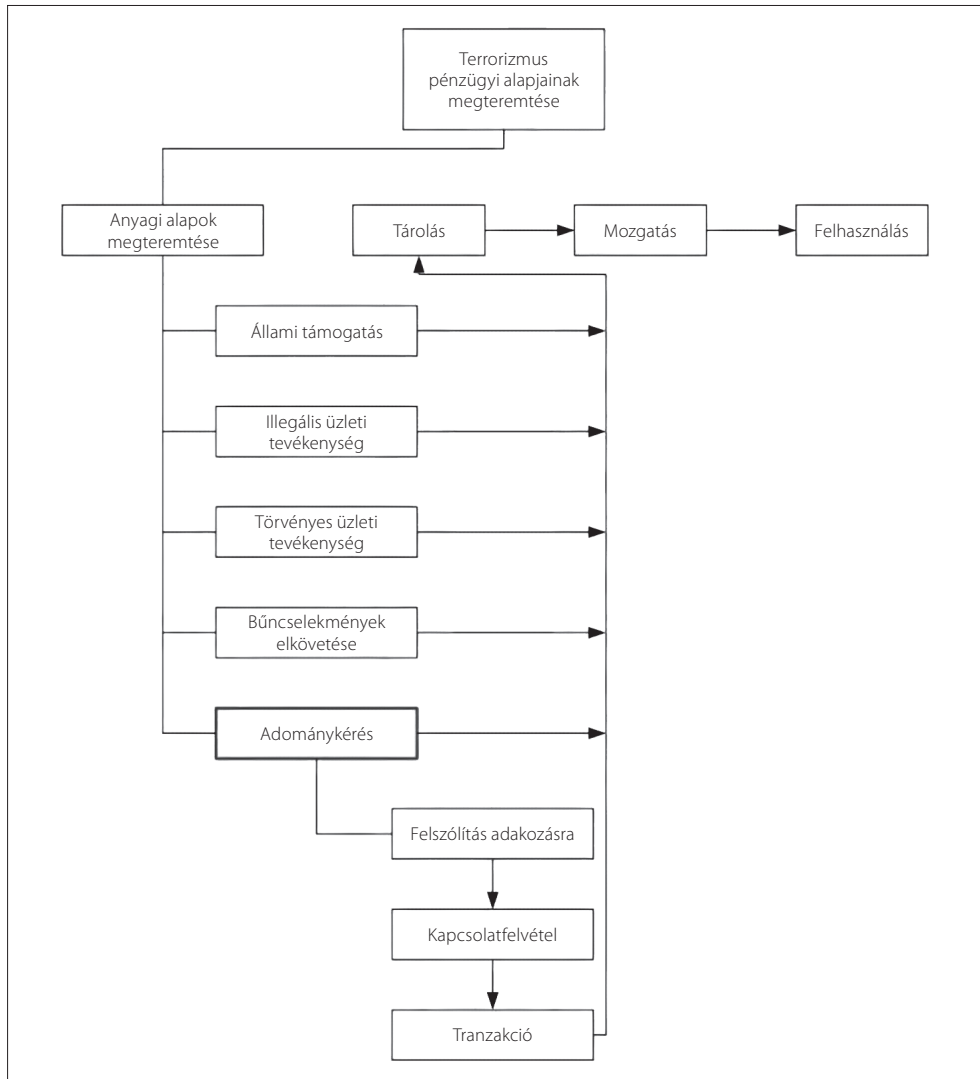
Az utóbbi néhány évben megdőlt az a korábban kőbe vésett szabálynak számító megállapítás, hogy a terrortámadások végrehajtásához jelentős anyagi befektetések szükségesek. Ha összevetjük a szeptember 11-ei terrortámadások anyagi szükségletét az utóbbi években elkövetett terrortámadások költségigényével, akkor azt látjuk, hogy szinte néhány száz vagy ezer euróból is nagy felháborodást kiváltó súlyos merényletek követhetők el.<sup>15</sup> Ez természetesen ne tévesszen meg senkit, ettől még a terrorszervezeteknek jelentős anyagi szükségleteik lehetnek. A szervezetek adminisztratív és anyagi-technikai költségei, illetve a humán vonatkozású kiadások jelentős összegeket emésztnek fel. Ezeken túl egyes szervezetek iskolákat, kórházakat üzemeltetnek, és egyéb, terrorszervezetektől szokatlan szociális szolgáltatásokat biztosítanak. A propagandagépezet működtetése, az újonctoborzás, a mártírok hozzátartozóinak támogatása ugyancsak jelentős költségvonzattal jár. A működéshez szükséges pénzt elő kell teremteni, azt tárolni kell, és ha szükséges, akkor az egyes sejtek között mozgatni kell, és végül el kell tudni költeni. Ez egy rendkívül összetett rendszert feltételez, amelynek a könnyebb áttekinthetősége érdekében készítettem az 1. ábrát. Tekintettel arra, hogy a kutatás tárgya a szervezetek adománykérése, így csak az anyagi alapok megteremtésének lehetőségeit fejtettem ki részletesebben a rajzban. Ahogyan az ábrán is látható, a terroristák anyagi eszközeiket változatos forrásokból teremtik elő. A teljesség igénye nélkül ezek a következők lehetnek:

- állami támogatás;
- kábítószer-termelés és -csempészés, valamint -kereskedelem;
- embercsempészet, emberkereskedelem;
- zsarolás, emberrablás, védelmi pénz szedése;
- illegális adók kivetése;
- hamisított termékek kereskedelme;
- pénz-, illetve okmányhamisítás;
- hitelkártyacsalás;
- illegális műkincs-kereskedelem;
- illegális fakitermelés;
- illegális bányászat;
- illegális üzleti tevékenységből származó jövedelem;
- legális üzleti tevékenységből származó jövedelem.

Természetesen a felsorolás nem lehet teljes körű, mivel a terrorszervezetek semmitől sem riadnak vissza, amiből pénzt csinálhatnak. Az anyagi eszközök megteremtését vizsgálva szem előtt kell tartanunk, hogy egy dzsihadista terrorszervezet általában nem egy adott területen található egyetlen egységből áll, hanem jellemzően kis területeken tevékenykedő sejtekből épül fel, amelyek többé-kevésbé integrálódtak a helyi közösségekbe. A lakosok ismerik a terroristákat, tudják, hogy mivel foglalkoznak, de szimpátiából vagy félelemből megtűrik, esetleg támogatják is őket. Ezek a sejtek ismerik a helyi körülményeket, így pénzügyi forrásait a helyi körülményeknek megfelelően tudják optimalizálni.<sup>16</sup>

<sup>15</sup> Besenyő 2017, 18.

<sup>16</sup> Dion-Schwarz et al. 2019, 26.



1. ábra A dzsihadista terrorszervezetek pénzügyi műveleteinek vázlata (A szerző szerkesztése)

Az adománygyűjtés jellemzően helyi szinten (általában készpénzben és természeti javakban), vagy nemzetközi segélyszervezetek, jótékonyági szervezetek útján (adományeltérítéssel) történik, de az internet és a közösségi média térhódításával, valamint a világméretű muszlim diaszpóra növekedésével párhuzamosan elterjedt az online adománykérés is. Ebben az esetben viszont az adakozással kapcsolatos pénzügyi művelet adatai (tranzakciós adatok) bekerülhetnek a banki információs rendszerbe, és ennek a terrorizmusellenes finanszírozási törvények megszegése miatt büntetőjogi következményei lehetnek. Ennek fényében az online adománygyűjtés, adakozás esetében a névtelenséget biztosító kriptovaluták (zcash, monero stb.) tűnnek használható alternatívának.<sup>17</sup>

<sup>17</sup> Uo. 27.

## A TERRORSZERVEZETEK ONLINE ADOMÁNYGYŰJTÉSI KAMPÁNYAINAK JELLEMZŐI

Az adománygyűjtési kampányokat általában valamilyen konkrét céllal hirdetik meg. Ezek a célok változatosak lehetnek, úgymint fegyverek beszerzése, külföldi harcosok utaztatása, a propaganda életben tartása, vagy egyszerűen a szervezet napi működéséhez szükséges pénz előteremtése.

Az Elliptic blokkláncelemző cég 2023-as elemzése szerint<sup>18</sup> a dzsihadista terroriszervezetek egyre gyakrabban használnak kriptovalutát az online adománygyűjtő kampányaik során. Az ilyen kezdeményezések eredményeként alkalmanként néhány száz dollártól százezer dollárig terjedő bevételekhez juthatnak. A jelentés szerint az al-Kaida, az Iszlám Állam és a Hamász katonai szárnya, az Izz ad-Din al-Kasszám Brigádok járnak élen a kriptovaluta alapú adománygyűjtésben. Megfigyelték, hogy az említett szervezetek az utóbbi néhány évben fokozatosan felhagytak a bitcoin használatával, és helyette a tether (*USDT stablecoin*) felé fordultak, ugyanis a bitcoin nyílt blokklánc a hatóságok számára lehetővé tette, de legalábbis megkönnyítette a tranzakciók nyomon követését és a részt vevő felek beazonosítását.

A kripto alapú adománygyűjtési kampányok általában valamilyen erre a célra készült weboldalon (*crowdfunding sites*) vagy a közösségi médián keresztül történnek úgy, hogy közléseket a kriptovaluta-pénztárca címét, ahová az adományokat várják. Az Iszlám Állam esetében van példa arra is, hogy a szervezet által működtetett honlapon szerepel az adakozásra történő felhívás. Ha az adománygyűjtés időbeliségét vizsgáljuk, akkor beszélhetünk kampányszerű, bizonyos ideig tartó adománygyűjtésről, illetve állandó vagy másképpen folyamatos kampányról. Az előbbieket esetében nem ritkán a kampányok valamilyen eseményhez kötődnek, ami lehet egy természeti katasztrófa vagy egy nagyobb visszhangot kiváltó sikeres terrortámadás. A terroriszervezetek alkalmazkodnak a hatósági intézkedésekhez. A Hamász például a sikeres izraeli hatósági rajtaütéseket követően, 2023 áprilisától felfüggesztette a kriptovaluta-használatot, míg az Iszlám Állam a lefoglalások elkerülése érdekében áttért a névtelenséget biztosító monero használatára. Az Elliptic jelentése szerint<sup>19</sup> a kriptovalutában összegyűjtött összegek csak egy kis részét képezik a terroriszervezetek bevételeinek, habár az összegek nagysága növekvő tendenciát mutat.

A jelentés szerint esetenként kapcsolat mutatható ki a terroriszervezetek kriptovaluta-adományt fogadó címei és a dark weben elkövetett hitelkártyacsaláshoz, illetve más pénzügyi jellegű bűncselekményekhez köthető kriptovaluta-címek között.

## AZ IZZ AD-DIN AL-KASSZÁM BRIGÁDOK KRIPTOVALUTA ALAPÚ ADOMÁNYGYŰJTŐ KAMPÁNYA

A Hamász katonai ága, az Izz al-Kasszám Brigádok (AKB) 2019-ben indította bitcoin alapú terrorizmust finanszírozó kampányát. Ennek során nyomon követhető, hogy a rendvédelmi szervek közbelépése milyen módon segítette elő a szervezet kriptovaluta alapú adománygyűjtési módszereinek evolúcióját. A kampány az alkalmazott technikák szempontjából három szakaszra osztható.

Az első szakaszban az AKB az adományok fogadására egy New York-i kriptovaluta-tőzsdén bejegyzett pénztárca címét adta meg. Az AKB nyilvánosan elérhető weboldalán

<sup>18</sup> Elliptic 2023a., 2023b.

<sup>19</sup> Uo.

népszerűsítette a kampányt. A nyílt felszólítás felkeltette a rendvédelmi szervek figyelmét és intézkedtek a számla befagyasztására.

A második szakaszban az AKB egy tőzsdéktől független privát bitcoincímet jelölt meg az adományok fogadására, ezzel kivédve a tőzsdei nyilvántartással járó adatszivárgást. Az intézkedések ellenére a blokkláncelemzők nyomon tudták követni a tranzakciókat, és meg tudták akadályozni a kriptovaluta fiat pénzzé történő átváltását.<sup>20</sup>

A harmadik szakaszban az adománykérő weboldalukba egy olyan mechanizmust építettek be, amely minden adakozó számára egy egyedi fogadó címet generált. Ezzel párhuzamosan oktatóvideót készítettek, amelyben három módszert javasoltak a támogatások névtelenül történő célba juttatására. A többnyelvű videót a Telegramon tették közzé 2019. június 3-án. Az első esetben azt javasolták, hogy az adományozó keressen fel egy pénzváltót, ahol megadhatja a számára generált címet mint címzettet az adomány átutalására, de a cím tulajdonosát ne nevezze meg! A második esetben a hibrid (kripto- és fiat valuta) hawala rendszer használatát javasolták. A harmadik megoldásban bemutatták, hogy a felhasználók hogyan hozhatnak létre privát pénztárcát, amelyből név nélkül küldhetnek adományt. A videóban tőzsdéket is ajánlottak, ahonnan a támogatók bitcoinot vásárolhattak, és az IP-cím elrejtése érdekében kitértek a nyilvános wifi-használat célszerűségére is.

Az erőfeszítések ellenére az adománygyűjtés névtelenségét nem sikerült biztosítaniuk. Az Amerikai Egyesült Államok rendvédelmi szerveinek sikerült 150 bitcoincímet lefoglalniuk. Több támogatót beazonosítottak, és eljárás alá vontak. Ezen túl sikerült megszerezniük az AKB weboldala felett az irányítást, és hónapokon keresztül gyűjtötték a „támogatók” adatait.<sup>21</sup>

Összegezve a kampányt megállapítható, hogy az átlagos adomány értéke 24 dollár volt. A háromszakaszos kampányban összesen alig több mint 20 ezer dollárt sikerült összegyűjteniük. A kampány során elszenvedett kudarc hozzájárult a Hamász kriptovaluta-moratóriumához.

## DZSIHADISTA WEBOLDALAK VIZSGÁLATA

### Az adatbázis kialakítása

A nyílt és a dark weben történő sikeres keresés végrehajtásának alapvető feltétele a megfelelő keresőkifejezés kiválasztása. A nem megfelelően megválasztott keresőkifejezés használata vagy túl sok irreleváns, vagy túl kevés hasznosítható találatot eredményezhet. Ezért nem célszerű az olyan általános szavak használata, mint „islam”, „terror”, „terrorist” és ehhez hasonlók. A jó keresőkifejezések megtalálása elképzelhetetlen az adott szubkultúra nyelvezete, az általuk használt szófordulatok és a szleng kifejezések megismerése nélkül, ezért célszerű az idevágó szakirodalom előzetes tanulmányozása.

A vizsgált dzsihadista terrororganizációk általában arab nyelven kommunikálnak, kiadványaik is leginkább az arab nyelvű közösséghez szólnak. A legismertebb ilyen kiadványok az „al Naba” és a „Voice of Hind” (Iszlám Állam), a „One Ummah” (al-Kaida), amelyeknek vannak ugyan idegen nyelvű fordításai is, de az eredeti kiadványok nyelve arab. Erre való tekintettel a kutatás során az angol mellett az arab nyelvű kulcsszavakat is gyűjtöttem. A kutatás a 2023. május 1. és december 31. közötti időszakban történt.

<sup>20</sup> Mutunkei 2023.

<sup>21</sup> Global Disruption of Three... 2020.

## A kutatás során alkalmazott keresőkifejezések kiválasztásának szempontjai

A megfelelő keresőkifejezések kiválasztásának folyamata a 2. ábrán látható. A kutatás során fő forrásnak az arab és az angol nyelvű eredeti tartalmakat, valamint a magyar és az idegen nyelvű tudományos publikációkat választottam. A megfelelő kulcsszavak keresése nem egyszeri alkalom volt, hanem egy ciklikus folyamat, amely magában foglalta a megszerzett információk és tartalmak elemzését és az ezekben esetlegesen található új kifejezések (valamint ezek esetleges kombinációjának) tesztelését, majd kedvező esetben az adatbázisba történő mentésüket. A vizsgált szervezetek weboldalai a rendvédelmi szervek és a közösségi média korlátozó tevékenységének köszönhetően gyakran kényszerülnek helyváltoztatásra, és ezek újbóli megtalálása vagy az esetleges új oldalak felderítése ugyancsak indokoltta teszi a keresési folyamat jellegének átalakítását.



2. ábra A keresőkifejezések kiválasztásának folyamata (A szerző szerkesztése)

A dzsihadista online jelenlét kutatásához szükséges adatbázis építése érdekében a nyílt forrású információgyűjtés keretében célirányosan olyan eszközöket választottam ki, amelyek egyrészt alkalmasak voltak a kutatás szempontjából releváns weboldalak, felhasználói



fiókok, posztok összegyűjtésére, ezek rendszerezésére, másrészt az egyes elemek közötti kapcsolatok ábrázolására.

## A keresések helyének kiválasztása

### *Közösségi média vonatkozásában*

A vizsgált szervezetek igyekeznek tartalmaikat minél szélesebb körben terjeszteni, ezért a kutatás megtervezésénél ezt a tényezőt is figyelembe kellett venni. Ennek megfelelően kiválasztottam azokat az alkalmazásokat, amelyek a legelterjedtebbek, legnépszerűbbek a felhasználók körében, és a kutatásomat ezekre fókuszálva a már ismertetett módon kiválasztott kulcsszavak segítségével a kutatás időszakában rendszeresen hajtottam végre kereséseket a Facebook, az Instagram, a TikTok és az „X” (korábban Twitter) alkalmazások felületein, illetve a Telegram nyílt webes csatornáin.

### *Nyílt internetes keresőmotorok használata*

A közösségi médiában történő kereséseken túl a kiválasztott keresőkifejezésekkel a legnépszerűbb keresőmotorokat használva kutattam a nyílt interneten a kutatás szempontjából figyelembe vehető dzsihadista weboldalak után. A kutatás során a Google, a DuckDuckGo, a Bing, a Yahoo, a Yep, a SwissCow és a SearchEncrypt keresőmotorokat vettem igénybe.

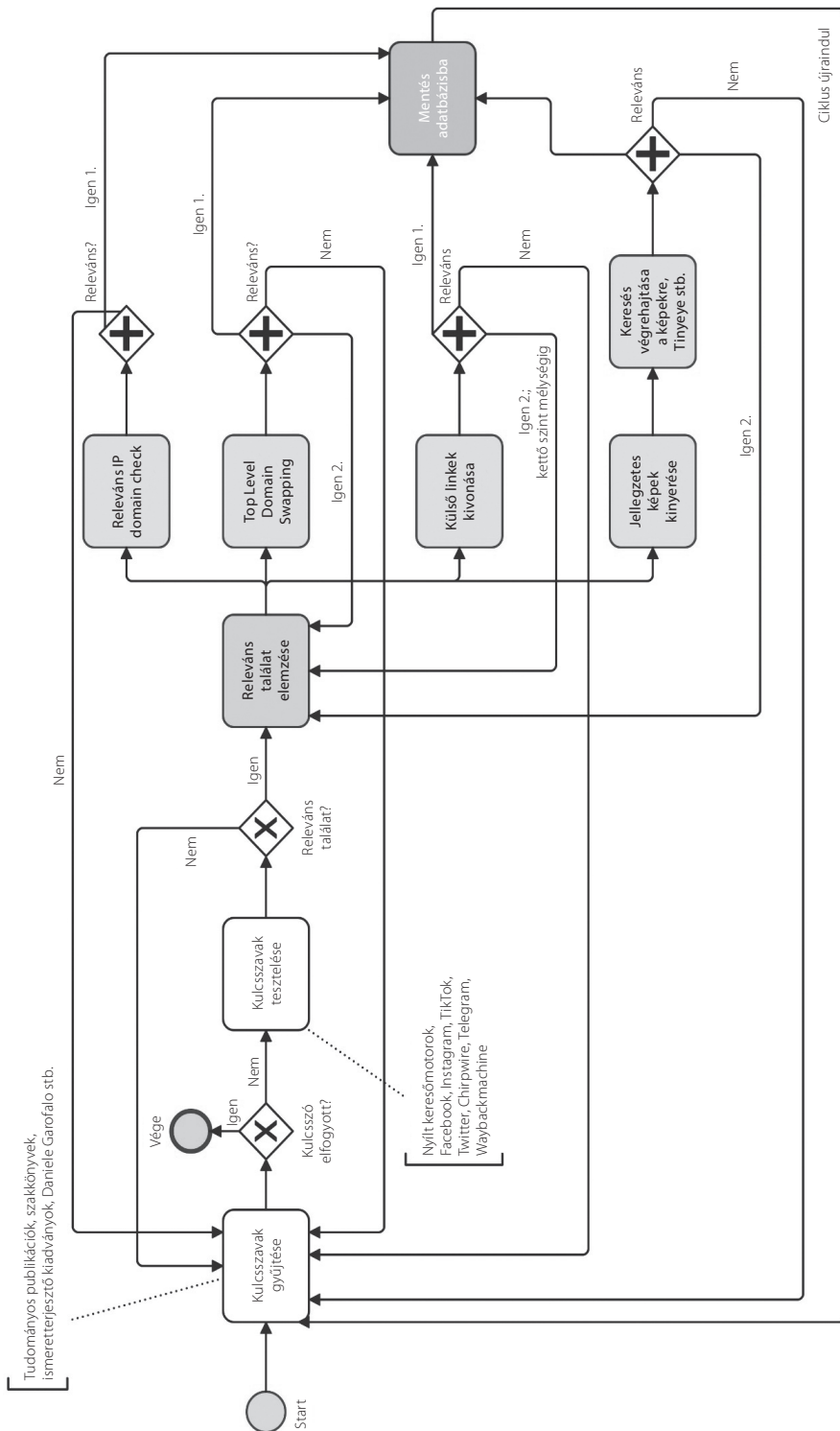
### *Dark webes kutatás*

A dark webes kutatás keretében a TOR-rendszerre fókuszáltam, ahol a jól ismert linkgyűjteményeken kívül (onion links, Hidden Wiki stb.) a keresőmotorok közül a tapasztalataim szerint legjobb Ahmia-fi, Torch, Haystack, Recon, Onion search szolgáltatásokat használtam.

### *Az adatbázis-építés folyamata*

- A különböző forrásokból származó kulcsszavakat teszteltem a felsorolt platformokon.
- Amennyiben releváns találat keletkezett, azt elmentettem az adatbázisba, majd a tartalom jellegétől függően végrehajtottam az IP-cím alapján történő ellenőrzését annak érdekében, hogy megtudjam, milyen más weboldalakat tárolnak az adott szerveren. Ha releváns weboldalt találtam, akkor azt elmentettem az adatbázisba, majd azt is elemeztem.
- A releváns weboldalakon végrehajtottam a Top Level Domain Swapping ellenőrzést, hogy megállapítsam, az adott weboldalnak van-e olyan klónja, mely más TLD alatt fut.
- Az elemzett weboldalakból kivontam az olyan képeket, amelyek alkalmasak lehetnek más, esetleg klónozott webhelyek, kiadványok, posztok felderítésére, majd ezeket nyilvános képek kereső szolgáltatásokon lefuttattam, és a releváns találatokat rögzítettem az adatbázisban.
- A hasznos találatnak ítélt weboldalakból kivontam a külső webhelyekre mutató linkeket, és ezeken is végrehajtottam az elemzést és a fent felsorolt ellenőrzéseket két szint mélységéig.

Az adatbázis-építés folyamata a 3. ábrán látható.



3. ábra A nyílt forrású információgyűjtés eszközeivel végrehajtott adatbázis-építés folyamatábrája (A szerző szerkesztése)

A kutatás szempontjából hasznos linkeket MS Excel táblában gyűjtöttem. Az 1. táblázat a legfontosabb mezőket és azok típusát tartalmazza.

1. táblázat *Az adatbázis mezői és adattípusai*  
(A szerző szerkesztése)

Mezőnév	Adattípus
Weboldal neve	szöveges
URL	szöveges
Év	szám
Szervezet	szöveges
Társult szervezet	szöveges
Nyelv	szöveges
Adománykérés	bináris
Kriptoaluta	szöveges
Megjegyzés	szöveges

A relevánsnak ítélt weboldalak esetében megvizsgáltam az oldal valós létrejöttének idejét, mivel a kutatásba csak az első kriptoaluta 2009-es megjelenését követően létrehozott weboldalakat vontam be.

Az adatbázis-építés során a közösségi médiában egyszerű kereséssel nem találtam szélsőséges iszlamista weboldalakra mutató linkeket.

## A KRYPTOVALUTÁBAN TÖRTÉNŐ ONLINE ADOMÁNYKÉRÉSEK FELKUTATÁSA

### Az adatbázis kiértékelése

Az adatbázisban található weboldalak szervezetenkénti megoszlása az 2. táblázatban látható.

2. táblázat *Az összegyűjtött weboldalak szervezetenkénti felbontásban* (A szerző szerkesztése)

Ssz.	Szervezet megnevezése	Archív	Élő	Összesen
1.	Iszlám Állam	52	12	64
2.	al-Kaida	21	13	34
3.	Abu Ali Mustapha Brigades	0	1	1
4.	Al Shabaab	4	3	7
5.	Hezbollah	8	2	10
6.	Hay'at Tahrir al-Sham (HTS)	1	1	2
7.	Taliban	8	2	10
8.	Kataib Hezbollah	4	1	5
9.	Iszlám Forradalmi Gárda	1	1	2

Ssz.	Szervezet megnevezése	Archív	Élő	Összesen
10.	Harakat Hezbollah	1	1	2
11.	al-Kassám Brigádok	1	1	2
12.	Független/beazonosíthatatlan	9	7	16
13.	Hamász	1	3	4
14.	Mujahideen Brigades	0	1	1
15.	Al Quds Brigades	1	2	3
16.	Tehreek-e-Taliban	2	1	3
17.	Ansar al-Din Front	1	0	1
18.	Palestinian Islamic Jihad	0	1	1
19.	Jaysh al-Ummah	0	1	1
20.	Turkistan Islamic Party	0	1	1
21.	Al Qaeda in the Islamic Maghreb	1		1
22.	Houthi	0	3	3
	Összesen	116	58	174

A 3. táblázatban látható a kriptovalutában történő adománykérés megoszlása szervezet, weboldalak állapota és jellege szerint, valutanemenként csoportosítva.

3. táblázat *Az online adománykérések megoszlása (A szerző szerkesztése)*

Szervezet megnevezése	Archív weboldal		Élő weboldal		Dark webes oldal	
	Bitcoin	Monero	Bitcoin	Monero	Bitcoin	Monero
Iszlám Állam Al Raud Media Archive	0	1	0	1	0	1
Iszlám Állam I'lam Foundation	0	2	0	2	0	1
Jaysh al-Ummah	0	0	1	0	0	0
Független dzsihadista híroldal	0	0	1	0	0	0
Összesen	0	3	2	3	0	2

A táblázatban szereplő adatok alapján megállapítható, hogy a vizsgált terrorszervezetekre nem jellemző a kriptovalutában történő nyilvános adománykérés. Az Iszlám Államhoz köthető I'lam Foundation és az Al Raud Media Archive a névtelenséget biztosító monerót részesíti előnyben a nyílt webes és a dark webes felületein egyaránt. Mintaként az Al Raud alapítvány dark webes adománykéréséről készült képernyőfotó a 4. ábrán látható. Az adománykérések címeit összevetve megállapítottam, hogy az alapítványok nyílt és dark webes monerocímei egyeznek, de a két alapítvány címei egymástól eltérnek.

Úgy tűnik, hogy az alapítványok weboldalain aktív adománygyűjtés folyik. Az adományozás részleteit tartalmazó weboldalak hozzászólásai évekre visszamenőleg időben folyamatos érdeklődésre utalnak, viszont a kérdésekből arra lehet következtetni, hogy a felhasználók

többsége nincs tisztában a kriptovaluták működésével, és az ilyen formában történő támogatás ismeretlen terület a számukra, habár néhány felhasználó igyekszik tanácsokkal és oktatóvideókra mutató hivatkozásokkal segíteni őket. Mindazonáltal a moneróban folytatott tranzakciók részletei a kriptovaluta jellegéből adódóan rejtve maradnak a külső szemlélő számára, így nem tudható, hogy mennyire sikeresek a szóban forgó kampányok.

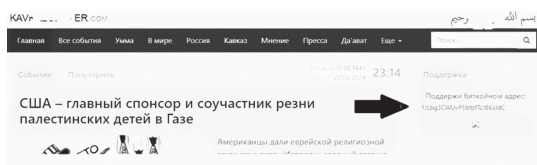
Az Iszlám Állam egykori központi weboldalain (elokxx.de és ennek variációi) megjelenő adakozásra történő felkérések nem jelölték meg a kért adomány nemét, hanem arra kérték a támogatókat, hogy adakozás előtt vegyék fel a kapcsolatot a weboldalon megadott email-címmel, hogy az adakozás részleteit megismerhessék. Ebben az irányban további kutatásra nem volt lehetőség.



4. ábra Az Al Raud Media Archive dark webes oldalán található, adakozásra történő felszólítás

Forrás: <http://xxxxxcv2uw2h3fay3cpopxuug6fxyp2reykt7lg67hnuonhm4xxxxx.onion/> (Képernyőfotó: 2024. 02. 15.)

A kavka##cen### (neve szándékosan eltorzítva) nevű, kaukázusi eseményekkel foglalkozó, orosz nyelvű, független, főleg csecsen és orosz vonatkozású dzsihadista hírportál bitcoinban kér adományt. Az adománygyűjtő felület az 5. számú ábrán látható.



5. ábra A kaukázusi független dzsihadista weboldal adománykérő felülete

Forrás: <https://kav##er.com> (Képernyőfotó: 2024. 02. 15.)

Az al-Kaidával kapcsolatban álló Jaysh al-Ummah palesztin terrrorszervezet a weboldalán bitcoinban történő adományozásra szólít fel. A szervezet a weboldalán többek között árlistát is közöl az egyes fegyverek beszerzési áráról annak érdekében, hogy a támogatókat adakozásra ösztönözze. Az adakozásra történő felszólításról készült kép a 6. ábrán látható.

Külön megvizsgáltam a Hamász kriptovaluta-műveleteiről ismert és széles körben alkalmazott weboldalait. A szervezet élő weboldalait összevetve a webarchívumban tárolt oldalakkal megállapítható, hogy a kriptovalutában történő adományozásra ösztönző felhívások eltűntek, ami arra enged következtetni, hogy a szervezet tartja magát a 2023 áprilisában kihirdetett kriptovaluta-moratóriumához. Mint ismeretes, az izraeli hatóságok több esetben sikerrel hiúsítottak meg Hamászhoz köthető kriptovaluta-tranzakcióikat, és foglaltak le je-



6. ábra A Jaysh-al-ummah-weboldalán található, adakozásra történő felszólítás

Forrás: <https://alraxxxx.nex/en/category/>  
(Képernyőfotó: 2024. 02. 15.)

lentőebb összegű kriptovalutát. A sorozatos kudarcok hatására hirdette meg a Hamász a kriptovaluta-moratóriumot.<sup>22</sup>

## A KAVKA##CEN### ÉS A JAYSH AL-UMMAH BITCOIN-CÍMEIHEZ TARTOZÓ TRANZAKCIÓK ELEMZÉSE

### Az elemzés lépései

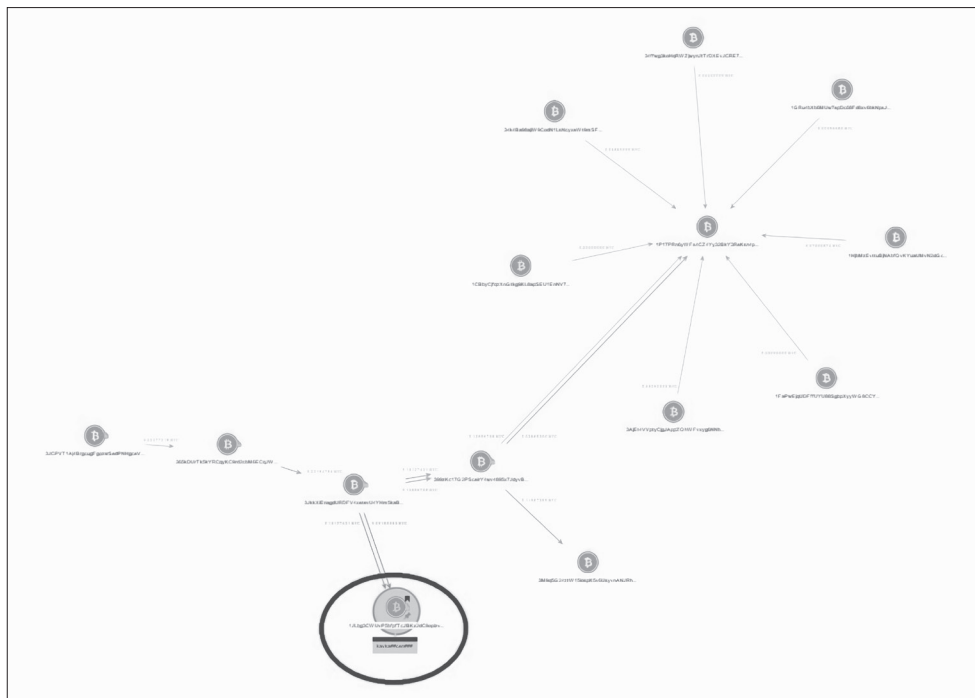
1. A támogatásra irányuló felszólításában szereplő bitcoincímre vonatkozóan összegyűjtöttem a kapcsolódó tranzakciókat, majd minden partner tekintetében hasonló módon egyenként elvégeztem a tranzakciók kigyűjtését. A nagy mennyiségű adatra tekintettel háromszintű kapcsolatmélységig végeztem el a kutatást.
2. Az elemzés során felmerült bitcoincímeket egyenként ellenőriztem az olyan nyilvános adatbázisokban, mint a „*bitcoin who is who*” (<https://www.bitcoinwhoswho.com>), a „*crypto scam*” (<https://cryptscam.com>) és a „*chainabuse*” (<https://www.chainabuse.com>), amelyek a felhasználók önkéntes adatszolgáltatásán alapuló adatbázisok, ahol a csalásokkal, pénzmosással, terroriz-musfinanszírozással kapcsolatos bitcoincímek lekérdezésére van lehetőség.
3. A felderített címeket internetes kereséssel is ellenőriztem annak érdekében, hogy megtudjam, szerepelnek-e más weboldalakon.
4. Az összegyűjtött adatokat azok tisztítását követően a Maltego 4.0.7. alkalmazás segítségével vizuálisan ábrázoltam.

### kavka##cen###

A kavka##cen###-hez tartozó bitcoin-cím ellenőrzése során megállapítottam, hogy az adományozásra szolgáló bitcoincímhez (körrel jelölve) tartozó egyenleg 0,00180353 BTC (napi árfolyamon 93,55 USD), amelyet egy a 3JkkXiEnagdURDFV4xetevU4YHm5kaB\_\_\_ címről küldtek 2018. január 12-én 17 órakor. A címen ez volt az egyetlen tranzakció, az egyenleg

<sup>22</sup> Al-Mughrabi 2023.

azóta nem változott. A tranzakcióban érintett címet és annak kapcsolatait három szint mélységig ellenőriztem a nyilvános adatbázisokban, de figyelmet érdemlő adat velük kapcsolatban nem keletkezett. A vizsgált címhez tartozó tranzakció a 7. ábrán látható.



7. ábra A `kavka##cen###` tartozó bitcoincímhez köthető tranzakció (A szerző szerkesztése)

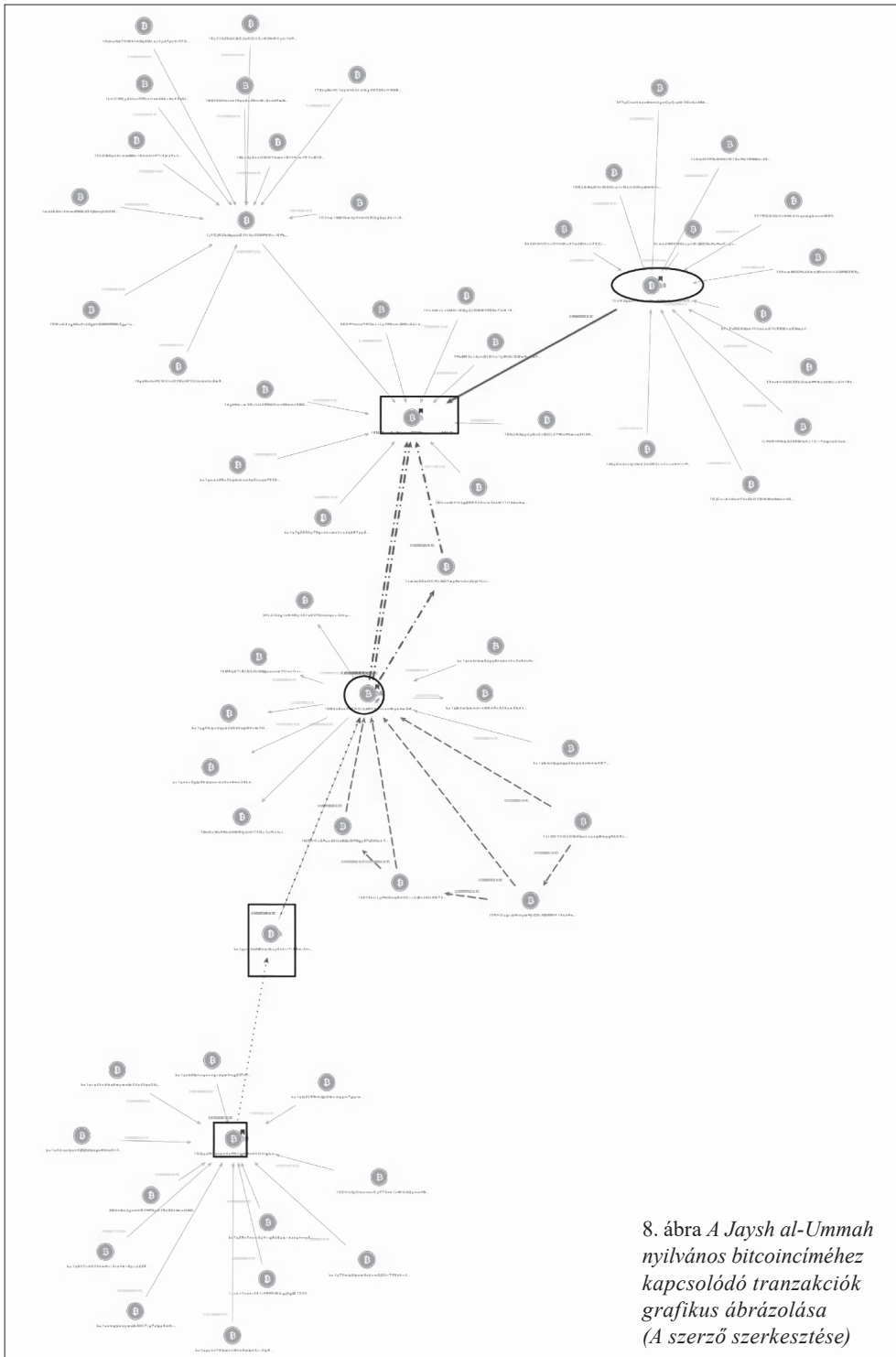
## A Jaysh al-Ummah tranzakciói

A megadott bitcoincímhez köthető pénzügyi műveletek grafikus ábrázolása a 8. ábrán látható. A kiindulási pont a körrel jelölt cím: `1EM4e8eu2S2RQRbS8C6aYnunWpkAwQ8___`. Egyenlege: 0 BTC. Fogadott hét tranzakcióban 0,00896503 BTC-t (468,55 USD), küldött hét tranzakcióban 0,00896503 BTC-t (468,55 USD). A tranzakciók száma 14, az első tranzakció 2020. július 8-án, az utolsó 2024. január 4-én történt.

A terrorizmussal, illetve a kiberbűnözéssel kapcsolatos nyilvános adatbázisokban a vizsgált cím nem szerepel.

## Figyelemre méltó pénzügyi műveletek

- A kiindulási pont (kör) mellett szaggatott nyíllal jelölt tranzakciók mintázata arra enged következtetni, hogy a küldő az összeg feldarabolásával és a címeikkel való játékkal törekedett az általa utalt összeg eredetének elrejtésére és a nyomunkövethetőség megnehezítésére.
- A vizsgált cím (a Jaysh al-Ummah címe) a `bclqnw3n6l6vqrllcky0uhrr7r89wr0mhhgpm1sl___` címen keresztül (álló téglalap) 20 USD-t kapott a `INDyJtNTjmwk5xPNhJgAMu4HDHigto___` címről (négyzet, pontozott nyíl), amely kriptovalutával kapcsolatos csalások és bitcoin mixer tevékenység miatt szerepel a „*bitcoinwhoiswho*” és a „*cryptscam*”

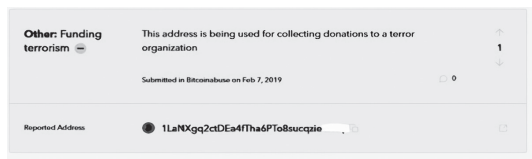




adatbázisában. A bc1-es kezdetű cím feltehetően a valódi küldő elrejtése miatt mindössze csak ehhez az egy tranzakcióhoz köthető. A csalás miatt megjelölt cím további tranzakcióit terjedelmi okok miatt nem vizsgáltam. A cím jelentőségét jól mutatja, hogy 1 191 638 tranzakcióban összesen 15 654 676,018 116 31 BTC-t fogadott (ami napi árfolyamon 809 117 409 132 USD-nak felel meg), és küldött tovább az elmúlt hat évben. Jelenlegi egyenlege 0,318 BTC. A cím feltehetően valamely illegális pénzügyi szolgáltatóhoz (kriptotőzsde vagy mixer) köthető.

- c) Az 1EM4e8eu2S2RQrbS8C6aYnunWpkAwQ8\_\_\_ (kör) kimenő tranzakciói között figyelemre méltó a 18MJ9vje3yPAytwePSTPmqmzaayB8LC\_\_\_ (fekvő téglalap), ugyanis ide két alkalommal közvetlenül és egy esetben közvetítón keresztül is küldött kis összegeket a Jays al Ummah. Ezek a tranzakciók pontozott szaggatott nyíllal vannak jelölve az ábrán. Ez a cím nem szerepel egyik adatbázisban sem, ugyanakkor figyelemre méltó kapcsolatai közé tartozik a 1LaNXgq2ctDEa4fTha6PTo8sucqzie\_\_\_ cím (ellipszis), amelyről 0,966 509 2 BTC-t kapott (vastag nyíl). Az 1LaNXgq2ctDEa4fTha6PTo8sucqzie\_\_\_ (ellipszis) cím viszont 2019. február 9. óta szerepel a *scamalert* adatbázisában mint a Hamászhoz köthető cím – ahogyan az a 9. ábrán is látható –, amelyet terrorizmus-finanszírozásra használnak. Erre a címre 3370,01580508 BTC érkezett, és innen 3370,01462506 BTC-t küldtek el összesen 9054 tranzakcióban. Valószínűsíthető tehát, hogy a 18M kezdetű cím (fekvő téglalap) is valamilyen formában kötődhet a terrorszervezetekhez, hiszen két olyan címmel is teljesített tranzakciókat, amelyek egyértelműen terrorszervezetekhez köthetők.

Internetes keresés feltárta, hogy az 1LA kezdetű cím mögött egy Cash4ps nevű palesztin pénzügyi szolgáltató áll, amelynek valóban vannak a Hamászhoz köthető kapcsolatai. A Chainalysis szerint<sup>23</sup> a címen megforduló összegből körülbelül egymillió dollárnyi kriptovaluta köthető terrorcsoportokhoz.



9. ábra A Chainabuse webszolgáltatás nyilvántartásában a cím terrorizmust támogató megjelölést kapott (Képernyőfotó: 2024. 02. 15.)

## ÖSSZEFOGLALÁS

Kutatásomban a szélsőséges iszlamista terrorszervezetek kriptovaluta-használatának összetevői közül a nyilvános weboldalakon folytatott adománykérés mértékét vizsgáltam. Az adatbázisba összegyűjtöttem az online jelenléttel rendelkező mértékadó szélsőséges iszlamista szervezetek OSINT-eszközökkel elérhető weboldalait. Objektív okokból a létező összes weboldal nem érhető el, de a keresés módszere és eszközei lehetővé tették a lehető legtöbb weboldal összegyűjtését és adatbázisba rendezését, ezzel a dzsihadista online ökoszisztéma jelentős részének a lefedését. Véleményem szerint ezek alapján a felmérés során tett megállapítások megalapozottnak tekinthetők.

Az 58 aktív weboldalból mindössze öt oldalon szerepel felhívás kriptovalutában történő támogatásra, ami a vizsgált oldalak mindössze 8,6%-a.

<sup>23</sup> Chainalysis Team 2020.

A Jaysh al-Ummah és a kavka##cen### látszólag semmilyen intézkedést nem alkalmaznak a hatóságok kijátszására. A két szervezet nyilvános bitcoincímeihez köthető tranzakciók elemzését követően megállapítottam, hogy ezeken jelentéktelen összegű pénzmozgások tapasztalhatók, ami arra enged következtetni, hogy a kriptovalutában történő adománygyűjtés nem játszik súlyponti szerepet a pénzügyi műveleteikben.

Ugyanakkor a Jaysh al-Ummah esete tanulságos. A szervezet tranzakciónak elemzése során a felhasználók hatóságot megtévesztő trükkjeinek néhány példáját sikerült demonstrálni. Példát láttunk arra, ahogyan az adományozók igyekeztek bitcoin mixerekkel kilétüket elfedni, trükköztek az utalt összeg feldarabolásával és a címek közötti játékkal. Emellett a tranzakciók elemzése igazolta azokat a feltételezéseket, miszerint a terrorszervezetek és a kiberbűnözők között kapcsolat van.

Ami az Iszlám Államhoz köthető alapítványok adománygyűjtését illeti, mindössze az állapítható meg, hogy a kampányuk napjainkban is zajlik, a felhasználók ugyan érdeklődnek iránta, de felkészültségük hiányos. Az anonim monero használatának köszönhetően további részletek megismerésére sajnos nincs mód. Tekintetbe véve a felhasználók jelentős részének felkészületlenségét, nem tűnik valószínűnek, hogy ez a módszer az alapítványok jelentős bevételi forrása lenne.

A korábban a kriptovaluta-műveletekben annyira aktív Hamász weboldalait összevetve a webarchívumban tárolt oldalakkal megállapítható, hogy a kriptovalutában történő adományozásra buzdító felhívások eltűntek, ami arra enged következtetni, hogy a szervezet tartja magát a 2023 áprilisában kihirdetett kriptovaluta-moratóriumhoz, legalábbis ami az online adománygyűjtést illeti.

Összességében kijelenthető: a nyilvános weboldalakon folytatott kriptovaluta alapú adománygyűjtés mindössze a terrorszervezetek töredékére jellemző, és a bitcoinban összegyűjtött adományok összege nem tekinthető jelentősnek. Az Iszlám Államhoz köthető, moneróban folytatott adománygyűjtés részletei nem ismeretesek, az érdeklődők kriptovalutákkal kapcsolatos felkészületlensége miatt azonban valószínűsíthetően ennek összege sem lehet jelentős.

## FELHASZNÁLT IRODALOM

- Al-Mughrabi, Nidal: *Hamas armed wing announces suspension of bitcoin fundraising*. Reuters, 2023. 04. 28. <https://www.reuters.com/world/middle-east/hamas-armed-wing-announces-suspension-bitcoin-fundraising-2023-04-28/> (Letöltés időpontja: 2023. 11. 05.)
- Besenyő, János: *Low-cost attacks, unnoticable plots? Overview on the economical character of current terrorism*. Strategic Impact, 62. évf. 2017/1., 83–100.
- Besenyő, János et al.: *Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Health-care Facilities and Workers*. Studies in Conflict & Terrorism, 2021. DOI: 10.1080/1057610X.2021.1937821
- Chainalysis Team: *Fact Checking Recent Cryptocurrency Terrorism Financing Reports*. Chainalysis, 2020. 05. 20. <https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-fact-check> (Letöltés időpontja: 2023. 01. 08.)
- Chainalysis Team: *2023 Crypto Crime: Illicit Crypto Volumes Reach All-Time Highs*. Chainalysis, 2023. 01. 12. <https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction> (Letöltés időpontja: 2023. 12. 20.)
- De, Nikhilesh: *Crypto Use in Terrorism “a Growing Problem,” Yellen Says*. coindesk.com, 2021. 02. 11. <https://www.coindesk.com/policy/2021/02/11/crypto-use-in-terrorism-a-growing-problem-yellen-says> (Letöltés időpontja: 2023. 12. 21.)

- Dion-Schwarz, Cynthia et al.: *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats*. RAND Corporation, 2019. 03. 27. [https://www.rand.org/pubs/research\\_reports/RR3026.html](https://www.rand.org/pubs/research_reports/RR3026.html) (Letöltés időpontja: 2023. 12. 18.)
- Dorshimer, Sam: *The New Era in Cyber-Enabled Terrorist Financing*. Center for a New American Security, 2020. 09. 29. <https://www.cnas.org/publications/commentary/the-new-era-in-cyber-enabled-terrorist-financing> (Letöltés időpontja: 2023. 10. 11.)
- *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns*. Department of Justice, 2020. 08. 13. <https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns> (Letöltés időpontja: 2023. 10. 07.)
- *How terrorist groups are exploiting crypto to raise funds and evade detection*. Elliptic, 2023a. [www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection](http://www.elliptic.co/blog/how-terrorist-organizations-are-exploiting-crypto-to-raise-funds-and-evade-detection) (Letöltés időpontja: 2023. 12. 27.)
- Letter dated 21 January 2021 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council. ENSZ Biztonsági Tanács, 2021. <https://documents.un.org/doc/undoc/gen/n21/000/98/pdf/n2100098.pdf?token=4Z2oi70z4PrXsUs1JG&fe=true> (Letöltés időpontja: 2023. 09. 11.)
- Mutunkei, Julius: *How Hamas and terrorist groups use crypto donations*. Crypto.news, 2023. 10. 10. <https://crypto.news/how-hamas-and-terrorist-groups-use-crypto-donations/> (Letöltés időpontja: 2023. 12. 27.)
- Popper, Nathaniel: *Terrorists Turn to Bitcoin for Funding, and They're Learning Fast*. The New York Times, 2019. 08. 18. <https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html> (Letöltés időpontja: 2023. 12. 10.)
- *Terrorist Financing Through Cryptoassets in 2023*. Elliptic, 2023b. <https://www.elliptic.co/resources/terrorist-financing-and-cryptoassets-in-2023> (Letöltés időpontja: 2023. 12. 27.)
- *The United Nations Global Counter-Terrorism Strategy: 8<sup>th</sup> review: resolution adopted by the General Assembly*. ENSZ Közgyűlés, 2023. <http://digitallibrary.un.org/record/4013935> (Letöltés időpontja: 2023. 09. 11.)
- *UN says crypto use in terror financing likely soaring*. livemint.com, 2022. 10. 31. <https://www.livemint.com/market/cryptocurrency/un-says-crypto-use-in-terror-financing-likely-soaring-11667220010748.html> (Letöltés időpontja: 2023. 12. 10.)
- *Virtual Currencies and terrorist financing: assessing the risks and evaluating responses*. European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, 2018. 05. [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf) (Letöltés időpontja: 2023. 12. 20.)
- Wang, Shacheng – Zhu, Xixi: *Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing*. Policing: A Journal of Policy and Practice, 15. évf. 2021/4. <https://doi.org/10.1093/police/paab059> (Letöltés időpontja: 2023. 09. 11.)
- Wiwoho, Jamal et al.: *Examining Cryptocurrency Use among Muslim Affiliated Terrorists: Case Typology and Regulatory Challenges in Southeast Asian Countries*. Al-Ihkam: Jurnal Hukum Dan Pranata Sosial, 18. évf. 2023/1., 102–124. <https://doi.org/10.19105/al-ihkam.v18i1.7147>