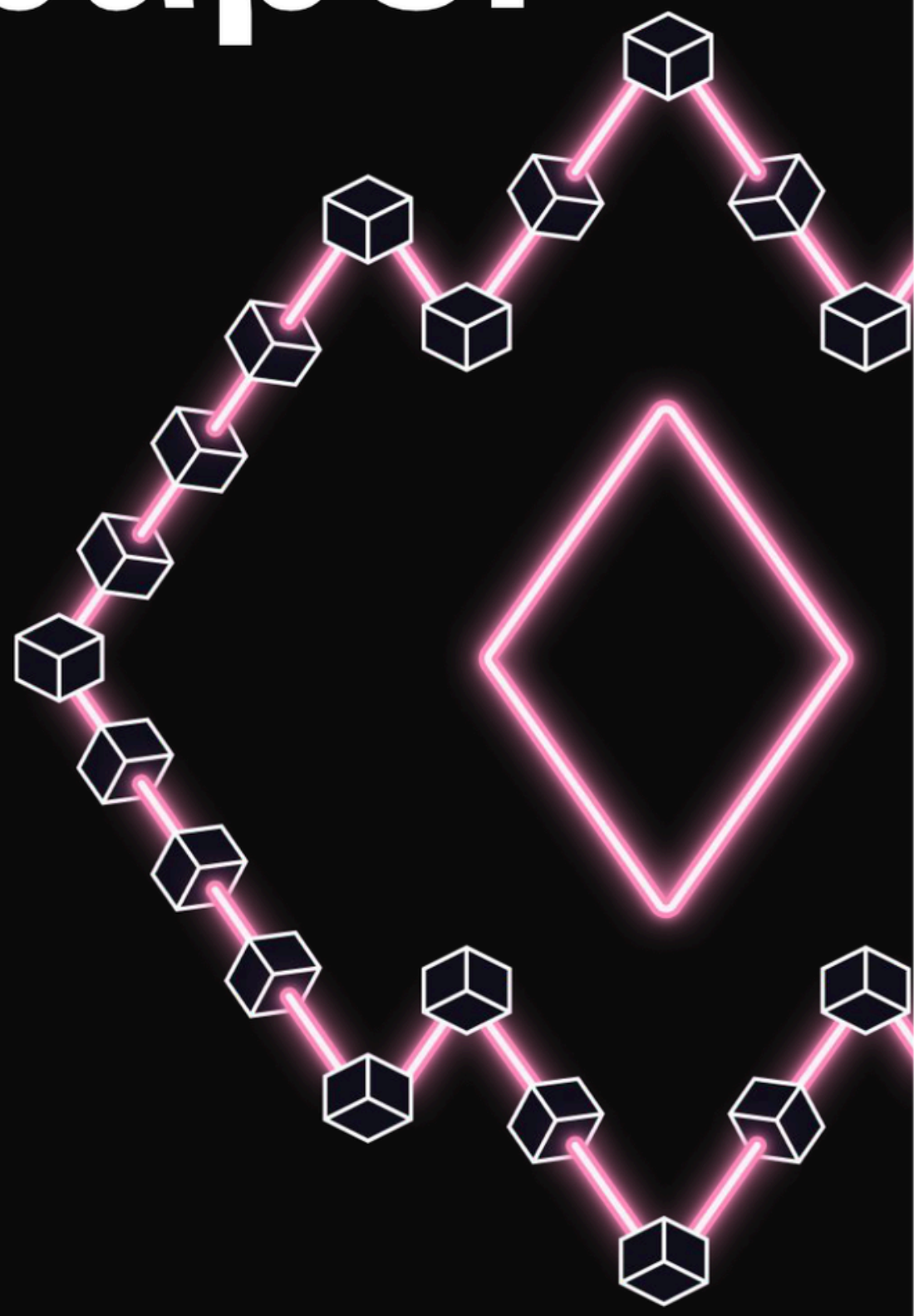
Mosaic chain

Mosaic Chain Whitepaper



Fordította: **Halasi Adél**

Mosaic Galaxy Ambassador

Tartalomjegyzék

Fogalomtár 5

Absztrakt 11

Bevezetés 12
- Motiváció 12
- Tervezési elvek 13
- Főbb hozzájárulások 14

Rendszeráttekintés 15
- Mi a Mosaic Chain? 15
- Hálózati érettség és bevezetési állapot 16
- Szerepkörök és eszközök áttekintése 17

Architektúra 18
- Protokoll- és runtime-architektúra 18
- Fő on-chain modulok 19
- Explorer, indexelés és külső interfészek 20
- Hálózatok és konfigurációs felületek 21

Konszenzus és validator készletmechanika 23
- Konszenzus áttekintése 23
- Sessionek és aktív készletrotáció 25
- Validator-részhalmaz kiválasztás 26
- Operatív működési eredmények 27

NFT-alapú részvétel, staking és gazdasági biztonság 29
- Miért NFT-k a validator jogosultságokhoz? 29
- Validator NFT-k (PoS és DPoS) 30
- Delegation NFT-k (Delegator NFT-k) 31
- Staking szerződések 32
- Jutalmak és díjak (mechanikai szint) 33
- Slashing, Chilling és biztonsági mechanizmusok 34

Protokollkiterjesztések és natív termékek 36
On-chain validator reputációs rendszer (Mosaic Trust Score) 36
Programozható Staking Vaultok 39
Cross-chain hozamirányítás XCM-en keresztül (Mosaic Yield Bridge) 44

Tokenomika (MOS) 48
A MOS felhasználási területei (MOS utility) 48
Kínálat és denominációk 48
Kibocsátási és jutalmazási modell 50
Vesting és Vesting-to-Freeze 51
Staking Incentive Pool 52

Governance és frissítések 53
Az irányítás hatóköre 53
Forkless frissítések 54

Interoperabilitás 55
Kapcsolat a Polkadottal 55
Parachain státusz és végrehajtási modell 55
XCM irányelvek 56

Validator OS és üzemeltetés 58
Mi a Validator OS? 58
Onboarding folyamat 59
Megbízhatóság és karbantartás 60

Biztonsági megfontolások 62
Kulcskezelés és felhasználói biztonság 62
Gazdasági biztonsági modell 63
Operatív biztonság 64

Roadmap 65

Fogalomtár

Blockchain és infrastruktúra

Aura (Authority Round)
A Substrate ökoszisztémában alkalmazott Proof-of-Authority (PoA) alapú blokkgyártási konszenzusmechanizmus, amely előre meghatározott validatorrotáció alapján határozza meg a blokk-előállítás sorrendjét és időzítését.

BABE (Blind Assignment for Blockchain Extension)
A Polkadot blokkgyártási konszenzusmechanizmusa, amely véletlenszerű validator-kiválasztáson alapuló slot-allokációval biztosítja a decentralizált blokk-előállítást.

GRANDPA (GHOST-based Recursive Ancestor Deriving Prefix Agreement)
A Polkadot finalizációs protokollja, amely gyors és determinisztikus blokkfinalitást biztosít a Relay Chain és a parachainek számára.

Blockchain state / Chain state
A blockchain aktuális teljes állapota, amely magában foglalja az account-egyenlegeket, runtime-adatokat, staking információkat, smart contract állapotokat és egyéb protokollszintű adatstruktúrákat.

Collator
Parachain-specifikus node-operátor, amely tranzakciókat gyűjt össze, candidate blockokat állít elő, majd azokat validációra továbbítja a Relay Chain validatorai számára.

Consensus engine
A blockchain konszenzusmechanizmusát megvalósító rendszerkomponens, amely koordinálja a blokkgyártást, validációt és finalizációs folyamatokat.

Fork
A blockchain történetének szétválása eltérő protokollszabályok vagy konszenzusállapotok következtében.

Forkless upgrade
Olyan protokollfrissítési mechanizmus, amely lehetővé teszi a runtime módosítását láncszakadás (fork) nélkül, közvetlen on-chain frissítéssel.

Mainnet
A protokoll éles, valós gazdasági értékkel működő blockchain hálózata.

Devnet
Fejlesztési és tesztelési célokra fenntartott hálózati környezet, amely lehetővé teszi új funkciók és protokollmódosítások validálását éles üzembe helyezés előtt.

Runtime
A blockchain on-chain végrehajtási környezete, amely a protokoll üzleti logikáját, állapotátmeneteit és működési szabályait kezeli.

Runtime upgrade
A blockchain runtime-jának on-chain frissítése, amely lehetővé teszi a protokoll logikájának módosítását hard fork nélkül.

Session
Időalapú működési periódus, amely alatt egy meghatározott validatorhalmaz felelős a blokkgyártásért és konszenzusműveletekért.

Session keys
A validatorok által blokkgyártásra és konszenzusműveletekre használt operációs kriptográfiai kulcsok.

Slot
Előre meghatározott blokkgyártási időablak, amely során egy kijelölt validator jogosult blokk előállítására.

Substrate
A Parity Technologies által fejlesztett moduláris blockchain framework, amely egyedi blokkláncok és runtime-ok fejlesztését teszi lehetővé.

Validator
A blockchain konszenzusmechanizmusában részt vevő node-operátor, amely blokkok validálásáért, előállításáért és a hálózat biztonságának fenntartásáért felelős.

Validator set
Az adott időszakban aktív konszenzusparticipációra jogosult validatorok összessége.

Waiting pool
Azon validatorok állapota vagy halmaza, amelyek megfelelnek a részvételi követelményeknek, de aktuálisan nem részei az aktív validator setnek.

NFT, staking és gazdasági modell

Delegation NFT
A Mosaic Chain ökoszisztémában olyan NFT-alapú staking instrumentum, amely delegált stakingpozíciót és névleges MOS-értéket reprezentál. A Delegation NFT lehetővé teszi, hogy a delegatorok stake-et kapcsoljanak DPoS validatorokhoz, miközben a pozíció feltételei és értéke on-chain módon nyomon követhetők.

Delegator
Olyan hálózati résztvevő, aki saját MOS tokenjeit vagy Delegation NFT-jét validatorhoz delegálja staking jutalmak megszerzése érdekében. A delegator nem üzemeltet validator node-ot, de gazdasági szerepet vállal a hálózat biztonságának támogatásában.

DPoS (Delegated Proof-of-Stake)
Olyan Proof-of-Stake alapú konszenzusmodell, amelyben a tokenholderök validatorokat támogatnak delegált stake-kel. A Mosaic Chain DPoS-jellegű modellje a validatorok és delegatorok közötti gazdasági kapcsolatot staking szerződéseken és NFT-alapú részvételi instrumentumokon keresztül kezeli.

PoS (Proof-of-Stake)
Olyan konszenzusmechanizmus, amelyben a hálózati résztvevők stake-elt tokenek révén vesznek részt a konszenzusban és a hálózat biztonságának fenntartásában.

PoA
Olyan konszenzusmodell, amelyben előre meghatározott, jogosultsággal rendelkező szereplők vesznek részt a blokkgyártásban.

Permission NFT
Validatorrészvételi jogosultságot reprezentáló NFT-alapú protokollobjektum a Mosaic Chain ökoszisztémában.

Staking
Olyan mechanizmus, amely során a hálózati résztvevők tokeneket zárolnak a konszenzus és a hálózati biztonság támogatása érdekében jutalmakért cserébe.

Staking contract
On-chain szerződéses kapcsolat, amely validator és delegator közötti staking- és jutalommegosztási viszonyt reprezentál.

Slashing
Gazdasági büntetési mechanizmus, amely validatorhibák, rosszindulatú működés vagy protokollsértések esetén csökkenti a stakelt eszközök értékét.

Chilling
Validator ideiglenes inaktiválási mechanizmusa, amely során a validator átmenetileg kikerül az aktív blokkgyártási és kiválasztási folyamatból.

Unbinding
Validatorhoz kötött stake vagy NFT kapcsolat megszüntetése és leválasztása.

Rebinding
Korábban leválasztott stake vagy NFT új validatorhoz történő hozzárendelése.

Treasury
On-chain közösségi pénzügyi alap, amely a protokoll fejlesztésének, ökoszisztéma-finanszírozásának és governance által jóváhagyott kezdeményezések támogatásának forrásait kezeli.

Vesting
Időalapú tokenfelszabadítási mechanizmus, amely meghatározott ütemezés szerint teszi elérhetővé a tokeneket.

Vesting-to-Freeze
Olyan tokenkezelési modell, amelyben a vesting alatt álló tokenek staking célra felhasználhatók, ugyanakkor továbbra is transzferkorlátozás alatt maradnak.

Yield
Stakingből vagy protokollmechanizmusokból származó hozam vagy jutalom.

Yield routing
Olyan mechanizmus, amely lehetővé teszi stakinghozamok vagy protokolljutalmak más alkalmazásokba, stratégiákba vagy pénzügyi rendszerekbe történő automatikus irányítását.

XCM és interoperabilitás

XCM (Cross-Consensus Messaging)
A Polkadot ökoszisztéma natív trustless cross-chain kommunikációs protokollja, amely lehetővé teszi az üzenetküldést és eszközátvitelt parachainek között.

Cross-chain
Eltérő blockchain hálózatok közötti kommunikációt, adatcserét vagy eszközmozgást lehetővé tevő működési modell.

Relay Chain
A Polkadot központi koordinációs és konszenzusrétege, amely shared securityt és finalitást biztosít a csatlakozó parachainek számára.

Parachain
A Relay Chainhez kapcsolódó önálló blockchain, amely a Polkadot shared security és interoperabilitási infrastruktúráját használja.

Bridge
Különböző blockchain hálózatokat összekötő infrastruktúra vagy protokollréteg, amely cross-chain eszközmozgást és kommunikációt tesz lehetővé.

Trustless
Olyan rendszerarchitektúra, amely működéséhez nem igényel központi bizalmi szereplőt vagy harmadik felet.

Hálózat és operáció

Air-gapped device
Olyan eszköz, amely fizikailag leválasztott minden külső hálózati kapcsolatról a maximális biztonság érdekében.

NAT (Network Address Translation)
Hálózati címfordítási technológia, amely lehetővé teszi több eszköz számára közös nyilvános IP-cím használatát.

Node
A blockchain hálózathoz csatlakozó szoftveres csomópont, amely részt vesz a hálózati kommunikációban, adatfeldolgozásban vagy konszenzusban.

Peer-to-peer (P2P)
Decentralizált hálózati kommunikációs modell, amelyben a node-ok közvetlenül kommunikálnak egymással központi szerver nélkül.

RPC (Remote Procedure Call)
Kommunikációs interfész, amely lehetővé teszi külső alkalmazások számára blockchain node-ok funkcióinak elérését és használatát.

Telemetry
Node- és hálózati állapotmonitoring rendszer, amely működési, teljesítmény- és diagnosztikai adatokat gyűjt.

UPS (Uninterruptible Power Supply)
Szünetmentes tápegység, amely áramkimaradás esetén biztosítja a node-ok folyamatos működését.

VPN (Virtual Private Network)
Titkosított hálózati kapcsolati réteg, amely biztonságos kommunikációt biztosít nyilvános hálózatokon keresztül.

WASM / WebAssembly
Sandboxolt, platformfüggetlen végrehajtási környezet, amelyet a Substrate-alapú blockchain runtime-ok futtatására használnak.

Governance és biztonság

Governance
On-chain döntéshozatali rendszer, amely meghatározza a protokoll fejlesztésével, paramétereivel és treasury-kezelésével kapcsolatos folyamatokat.

Committee-based governance
Olyan governance modell, amelyben meghatározott bizottságok vagy kijelölt szereplők vesznek részt a döntéshozatali folyamatokban.

Token-weighted voting
Olyan szavazási mechanizmus, amelyben a résztvevők szavazati súlya a birtokolt vagy stake-elt tokenmennyiség alapján kerül meghatározásra.

Supermajority
Minősített többségi döntéshozatali modell, amely meghatározott arányú — például kétharmados — jóváhagyást követel meg.

Security budget
A staking és tokenérték által biztosított teljes gazdasági biztonsági kapacitás, amely a hálózat támadásokkal szembeni ellenállóképességét támogatja.

Defense-in-depth
Többrétegű biztonsági modell, amely egymást kiegészítő védelmi mechanizmusok alkalmazásával csökkenti a rendszerkockázatot.

Seed phrase
Kriptográfiai helyreállító kulcsszólista (mnemonic phrase), amely lehetővé teszi wallet-ek és privát kulcsok visszaállítását.

Two-factor authentication (2FA)
Kétfaktoros hitelesítési mechanizmus, amely több egymástól független azonosítási módszer használatával növeli a biztonságot.

Absztrakt

A Mosaic Chain egy Substrate-alapú blokklánc, amelyet kifejezetten Web3 pénzügyi és privacy-first alkalmazások támogatására terveztek anélkül, hogy kompromisszumot kellene kötni a teljesítmény, a biztonság vagy a decentralizáció terén. A hálózat egy NFT-alapú részvételi modellt vezet be, amelyben a validator jogok on-chain NFT-ként jelennek meg, lehetővé téve az átlátható és átruházható részvételt, miközben a hálózat biztonságát egyértelműen meghatározott stake-értékekhez köti. Annak érdekében, hogy elkerülje azokat a skálázhatósági szűk keresztmetszeteket, amelyek akkor jelentkeznek, amikor több ezer validatornak kell folyamatosan koordinálnia egymással, a Mosaic Chain egy session-alapú konszenzusmodellt alkalmaz, amely rotációs elven választja ki az aktív validator készletet, miközben hosszabb időtávon egy jóval nagyobb validator populáció számára is lehetőséget biztosít a részvételre.

Operatív szempontból a Mosaic Chain a Validator OS rendszerrel együtt működik, amely egy célzottan fejlesztett, plug-and-play validator operációs rendszer. Ez szabványosítja a node-ok telepítését, kapcsolódását, frissítését és monitorozását, ezáltal csökkenti az üzemszünetek és konfigurációs hibák kockázatát. Az eredmény egy olyan hálózat, amely a validator szerepkört szélesebb körben elérhetővé kívánja tenni az üzemeltetők számára, miközben gyors blokkgyártást és kiszámítható hálózati működést biztosít. Jelen whitepaper részletesen ismerteti a protokoll alaparchitektúráját, a konszenzus- és validator kiválasztási mechanikát, az NFT-alapú staking modellt és annak biztonsági tulajdonságait, a MOS token felhasználási és gazdasági modelljét, a Validator OS működését, valamint a Polkadot ökoszisztémán belüli interoperabilitási irányokat.

Bevezetés

Motiváció

A decentralizált pénzügyi rendszerek rendkívül szigorú követelményeket támasztanak az őket kiszolgáló infrastruktúrával szemben. Míg az általános célú számítási platformokon az időszakos késleltetések vagy átmeneti inkonzisztenciák sok esetben elfogadhatók, addig a pénzügyi alkalmazások kiszámítható finalitást, erős gazdasági biztonsági garanciákat, valamint alacsony belépési küszöböt igényelnek mind az üzemeltetők, mind a végfelhasználók számára.
A megakadt vagy késleltetett tranzakciók pénzügyi környezetben elfogadhatatlanok; a DeFi protokollok kockázati modellje alapvetően eltér a közösségi alkalmazások vagy IoT-hálózatok működésétől. Ezek a követelmények egy célzottan tervezett blokklánc létrehozását indokolják az általános célú platformokra épülő megközelítésekkel szemben.

Ezzel párhuzamosan a decentralizáció gyakorlati megvalósítását továbbra is jelentősen korlátozza a validator infrastruktúra üzemeltetésének összetettsége. A legtöbb proof-of-stake hálózat esetében a validatoroknak bonyolult telepítési folyamatokon kell végigmenniük, több account között kell kezelniük a kulcsokat, manuálisan kell monitorozniuk az uptime-ot, valamint off-chain csatornákon keresztül kell koordinálniuk a szoftverfrissítéseket. Ennek eredményeként a validator készletek jellemzően technikailag magasan képzett üzemeltetők kezében koncentrálódnak, gyakran néhány nagy cloud szolgáltató infrastruktúráján. Ez a koncentráció gyengíti azokat a decentralizációs garanciákat, amelyeket a proof-of-stake rendszerek eredetileg biztosítani kívánnak.

A Mosaic Chain egyszerre kívánja kezelni mindkét problémát. Egy Substrate-alapú runtime környezetet biztosít, amelyet pénzügyi alkalmazásokra optimalizáltak: kiszámítható blokkidőkkel, on-chain staking eszközökön keresztül érvényesíthető gazdasági biztonsággal, valamint egy validator operációs rendszerrel, amely a node-üzemeltetés technikai küszöbét szakértői szintről plug-and-play hardveres megoldássá csökkenti. A hálózatot eleve úgy tervezték, hogy több ezer validator működését támogassa anélkül, hogy mindegyiküknek minden konszenzuskörben részt kellene vennie, ezáltal egyszerre megőrizve a decentralizáció szélességét és a blokkgyártás hatékonyságát.

A Mosaic Chain mögött álló tervezési filozófia szerint a pénzügyi célú blokklánc-infrastruktúrák jelentős előnyt nyernek a célzott optimalizációból. Az általános célú láncok egyszerre számos felhasználási területet szolgálnak ki — például gaming, közösségi média, IoT vagy supply chain alkalmazásokat — ezért tervezési kompromisszumaik is ezt a sokoldalúságot tükrözik. Egy kizárólag pénzügyi alkalmazásokra épített lánc ezzel szemben más prioritásokat választhat: a maximális átviteli teljesítmény helyett a kiszámítható blokkidőket, a smart contract expresszivitás helyett a gazdasági biztonság átláthatóságát, valamint a hardverskálázás helyett a validator hozzáférhetőségét helyezi előtérbe. Ezek a kompromisszumok nem univerzálisan helyesek, ugyanakkor pontosan megfelelnek annak a területnek, amelyet a Mosaic Chain kiszolgál.

Tervezési elvek

A Mosaic Chain architektúráját **öt alapvető tervezési elv** határozza meg, amelyek a protokoll minden rétegében irányadó szerepet töltenek be.

Elsőként: a hálózat célja a decentralizáció skálázása a teljesítmény romlása nélkül. A hagyományos konszenzusprotokollok alapvető feszültséggel szembesülnek: minél több validator vesz részt a rendszerben, annál nagyobb kommunikációs többletterhelés keletkezik, ami csökkenti az átviteli teljesítményt és növeli a késleltetést. A Mosaic Chain ezt a problémát session-alapú validator rotációval oldja meg, amely alkalmassá teszi egy nagy, több mint 2400 validatorból álló populáció működését, miközben sessionenként egy kompakt, körülbelül 200 validatorból álló aktív készlet biztosítja a hatékony blokkgyártást.

Második alapelvként a validálási folyamatnak operatív szempontból is hozzáférhetőnek kell lennie. A validator node-ok üzemeltetésének „expert-only” jellege nem pusztán felhasználói élménybeli probléma, hanem a decentralizáció strukturális akadálya. A Validator OS egységes operációs rétegként kezeli a telepítést, konfigurációt, kapcsolódást, monitorozást és szoftverfrissítéseket, ezáltal csökkenti a hibás konfigurációk kockázatát és mérsékli a részvétel technikai belépési küszöbét.

Harmadik alapelvként a biztonsági ösztönzőknek on-chain módon átláthatónak és kikényszeríthetőnek kell lenniük. A validator jogok explicit névleges értékkel rendelkező NFT-ként történő reprezentációja, valamint a delegáció MOS-token staking szerződéseken vagy opcionálisan Delegation NFT-ken keresztüli kezelése alkalmassá teszi, hogy a részvételi jogok és a gazdasági biztonsági kötelezettségek transzparens, auditálható és protokollszinten érvényesíthető formában jelenjenek meg. A stake-értékek, jutalékfeltételek, slashing szabályok és részvételi jogosultságok on-chain kerülnek rögzítésre, nem pedig átláthatatlan off-chain megállapodások formájába**n.**

Negyedik alapelvként a protokollnak támogatnia kell a forkless frissítéseken keresztüli folyamatos fejlődést. A pénzügyi infrastruktúrák nem engedhetik meg maguknak a hard forkokkal járó működési zavarokat és koordinációs költségeket. A Substrate forkless runtime upgrade mechanizmusa lehetővé teszi, hogy a Mosaic Chain fejlessze üzleti logikáját, módosítsa paramétereit és új funkciókat vezessen be anélkül, hogy a validatoroknak manuálisan új szoftvert kellene telepíteniük vagy chain split kockázatával kellene számolniuk.

Ötödik alapelvként a protokollnak egyértelmű interoperabilitási útvonalat kell biztosítania a cross-chain assetek és üzenetküldés számára. A Polkadot ökoszisztéma parachainjeként a Mosaic Chain natívan hozzáfér az XCM infrastruktúrához, amely trustless cross-chain kommunikációt tesz lehetővé a hagyományos bridge architektúrákhoz kapcsolódó biztonsági kockázatok nélkül.

Főbb hozzájárulások

A Mosaic Chain számos olyan egyedi tervezési megoldást vezet be, amelyek megkülönböztetik a meglévő blokklánc-platformoktól.

NFT-alapú validator részvételi jogosultságok.
Ahelyett, hogy a validator státuszt egy bináris on-chain jelzőként vagy egyszerű account-egyenlegként reprezentálná, a Mosaic Chain a részvételi jogokat explicit névleges értékkel rendelkező NFT-ként kezeli. Ez a megközelítés hordozhatóvá teszi a validator jogokat — a binding szabályok figyelembevételével —, auditálhatóvá teszi azokat, valamint jóval összetettebb funkcionalitást biztosít a hagyományos staking modellekhez képest.
Az NFT-modell explicit on-chain részvételi jogosultságokat vezet be PoS és DPoS Validator NFT-k segítségével. A delegáció történhet közvetlenül MOS-token staking szerződéseken keresztül, vagy opcionálisan Delegation NFT-k alkalmazásával, amennyiben átruházható, névleges értékkel rendelkező instrumentumra van szükség. Ez egyszerre biztosít egyszerű delegációs lehetőséget a MOS token számára, miközben fejlettebb on-chain instrumentumstruktúrákat is kialakít ott, ahol erre valódi igény mutatkozik.

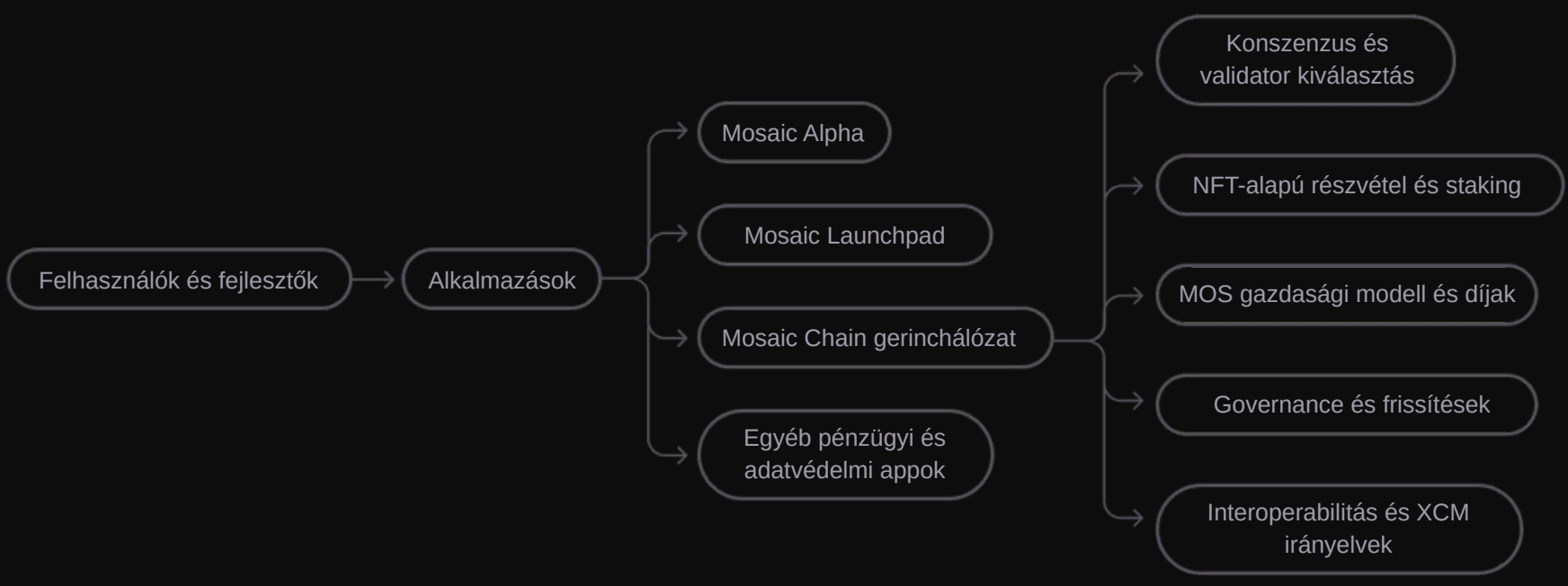
Session-alapú validator rotáció nagyméretű validator populáció mellett.
A továbbfejlesztett bucket selection algoritmus támogatja, hogy egy több mint 2400 validatorból álló hálózat időben kiegyensúlyozott módon vehessen részt a működésben, miközben sessionenkéntt egy körülbelül 200 validatorból álló aktív készlet biztosítja a konszenzusfolyamat hatékony működését. A szimulációk közel egyenletes kiválasztási eloszlást mutatnak heti időtávokon, ugyanakkor elegendő varianciát hagynak a kiszámíthatóság csökkentése érdekében.

A Validator OS, mint szabványos operációs réteg.
Ahelyett, hogy a validatorok működését külső tényezőként kezelné, a Mosaic Chain egy kifejezetten erre a célra kifejlesztett, Debian-alapú operációs rendszert biztosít, amely a validator teljes életciklusát szabványosítja — a hardver telepítésétől kezdve a folyamatos karbantartásig. Ez a tervezési döntés az üzemeltetési megbízhatóságot protokollszintű kérdésként kezeli, nem pedig utólagos szempontként.

Rendszeráttekintés

Mi a Mosaic Chain?

A Mosaic Chain egy egyedi fejlesztésű Substrate runtime környezet, amelyet kifejezetten pénzügyi fókuszú ökoszisztémák számára optimalizáltak. A Parity Technologies által fejlesztett Substrate keretrendszerre épül, amely örökli annak moduláris, pallet-alapú architektúráját. Ez az architektúra elkülöníti egymástól a konszenzuslogikát, az alkalmazási logikát és a kriptográfiai host funkciókat, amelyek egymással kombinálható komponensekként működnek együtt. A runtime WebAssembly (Wasm) formátumba fordítva kerül tárolásra on-chain, lehetővé téve a forkless frissítéseket validator koordináció vagy szoftver-újratelepítés nélkül.



A jelen dokumentumban ismertetett alapprotokoll alkotja a Mosaic ökoszisztéma „gerinchálózatát”. Ez magában foglalja a konszenzusmechanizmust és a validator kiválasztási algoritmust, az NFT-alapú staking és delegációs rendszert, a MOS token gazdasági modelljét, a Validator OS operációs réteget, valamint a Polkadot relay chainnel való interoperabilitási interfészt. Ezek az összetevők együtt biztosítják azt az infrastruktúraréteget, amelyre olyan pénzügyi alkalmazások épülnek, mint a Mosaic Alpha — egy decentralizált portfóliókezelő platform — vagy a Mosaic Launchpad, amely Web3-alapú fundraising megoldásként működik. Mivel a felhasználóbarát működés és a könnyű hozzáférhetőség kiemelt prioritást élvez, a Mosaic Explorer egyben elsődleges frontend felületként is szolgál a legtöbb validator és delegator munkafolyamat számára. Működését a 3.3-as fejezetben ismertetett decentralizált indexing stack támogatja.

A gerinchálózati infrastruktúra és az alkalmazási réteg tudatosan különválasztásra került. A Mosaic Chainre épülő pénzügyi alkalmazások öröklik az alapréteg biztonsági, finalitási és interoperabilitási tulajdonságait anélkül, hogy ezeket újra kellene implementálniuk. Maga az alapréteg ezzel párhuzamosan minimalista és stabil kialakítású, ahol az új funkciók bevezetése elsősorban a 6. fejezetben ismertetett kiterjesztési mechanizmusokon keresztül történik, nem pedig a protokollmag közvetlen módosításával.

Hálózati érettség és bevezetési állapot

A Mosaic Chain több különálló környezetben működik annak érdekében, hogy támogassa az iteratív fejlesztést és a biztonságos éles üzembe helyezést. A devnet környezetet runtime frissítések, paramétermódosítások és operatív folyamatok validálására használják kontrollált körülmények között, együttműködő vállalatokkal és DAO-kkal közösen, a Paseo hálózaton. A mainnet jelenti az éles hálózati környezetet, ahol a MOS token, a validator részvételi jogosultságok és a protokollösztönzők már valós gazdasági feltételek mellett működnek.

2026. február 16-i állapot szerint a mainnet hálózati telemetria a publikus státusz dashboard alapján az alábbi főbb mutatókat jelentette:

- **Összes validator száma:** 2 027
- **Aktuális blokk:** 1 662 769
- **Node-egészségügyi állapot** (összes jelentő node: 1 945):
  - **Chain:** 1 928 egészséges, 17 hibás
  - **Indexer:** 1 770 egészséges, 175 hibás
  - **Admin**: 1 937 egészséges, 8 hibás

A validator életciklus-állapot ebben az időpontban azt mutatja, hogy a validator részvételi instrumentumok túlnyomó többsége aktív állapotban van, míg kisebb részük chilled állapotú, illetve csak minimális számú faulted státusz fordul elő. Ez összhangban áll egy olyan operatív hálózat működésével, amely nagyléptékű onboarding folyamat mellett is stabil blokkgyártást képes fenntartani. A dashboard emellett valós idejű bontásban jeleníti meg a validator- és delegator-oldali részvételi instrumentumokat, valamint a session részvételi állapotokat — például az aktuális aktív készletet, a várólistán lévő vagy sessionen kívüli validatorokat —, ezáltal folyamatos átláthatóságot biztosítva a hálózati részvétel időbeli eloszlásáról.

Funkcionális szempontból a whitepaperben ismertetett alapprotokoll már implementálásra került és működik a mainnet környezetben. Ez magában foglalja a session-alapú blokkgyártást, a validator életciklus- és jogosultsági modellt, a Validator OS onboarding és operációs folyamatait, valamint a staking és részvételkezeléshez szükséges on-chain interfészeket is. Mivel a hálózati szintű mutatók folyamatosan változnak, a dokumentumban szereplő valamennyi kvantitatív adat időbélyeggel ellátott pillanatfelvételként értelmezendő, amennyiben nincs ettől eltérően jelezve.

Szerepkörök és eszközök áttekintése

A Mosaic Chain protokoll **négy elsődleges szerepkört** és az ezekhez kapcsolódó on-chain eszközöket határozza meg. Ezen szerepkörök és az általuk használt instrumentumok megértése alapvető fontosságú a protokoll további működésének értelmezéséhez.

A **validatorok** olyan node-okat üzemeltetnek, amelyek blokkokat állítanak elő és részt vesznek a konszenzusfolyamatban. Minden validatornak rendelkeznie kell egy Validator NFT-vel — PoS vagy DPoS típussal —, amely biztosítja a részvételi jogosultságot, valamint meghatározza az adott validatorhoz tartozó névleges stake-értéket. A validatorok slashing büntetés alá esnek üzemszünet vagy protokollsértés esetén, míg a jutalmazásuk a hálózati részvételük arányában történik.

A **delegatorok** olyan MOS token tulajdonosok, akik további stake biztosításával támogatják a validatorokat. A delegáció on-chain staking szerződéseken keresztül valósul meg, amelyek rögzítik a stake mennyiségét, a jutalékrátát és a minimális staking időszakot. A delegatorok a hozzájárulásuk arányában részesülnek jutalomban, a validator jutalékának levonása után. A felhasználói élmény javítása érdekében a jutalmakat nem szükséges manuálisan lehívni: azokat egy on-chain háttérfolyamat automatikusan kiosztja és újrakamatoztatja minden session lezárását követően. A delegáció kétféle módon történhet: (1) MOS tokenek közvetlen delegálásával staking szerződéseken keresztül; (2) Delegation NFT-k használatával, ahol az explicit névleges értékek átruházható on-chain stake instrumentumként működnek. Fontos hangsúlyozni, hogy a Delegation NFT-k használata opcionális: a delegatorok Delegation NFT kibocsátása nélkül is delegálhatnak MOS tokeneket. A Delegation NFT-k elsősorban olyan esetekben kerülnek alkalmazásra, amikor a delegator explicit névleges értékkel rendelkező, instrumentumszerű pozíciót és nagyobb on-chain kompozabilitást (más on-chain rendszerekkel való összeépíthetőséget) kíván létrehozni.

A **MOS token** a Mosaic Chain natív eszköze. Elsődleges elszámolási egységként szolgál tranzakciós díjak, staking jutalmak, delegációk, treasury- és alapkezelési döntésekhez kapcsolódó proposal letétek, valamint — egy későbbi frissítést követően — tokenalapú governance szavazások és runtime frissítések során.
A maximális kínálat rögzített: 2 000 000 000 MOS.

A **Validator NFT-k és Delegator NFT-k** olyan on-chain instrumentumok, amelyek részvételi jogosultságokat és stake-kötelezettségeket reprezentálnak. A hagyományos, egyenlegalapú staking modellekkel szemben az NFT-alapú megközelítés explicit módon jeleníti meg ezeket a jogosultságokat, átruházhatóvá teszi őket — a kötelező szabályok figyelembevételével —, valamint integrálhatóvá a szélesebb on-chain állapottérbe. Minden NFT rendelkezik egy MOS-ban denominált névleges értékkel, amely közvetlenül hozzájárul a hálózat gazdasági biztonságához.

Architektúra

Protokoll- és runtime-architektúra

A Mosaic Chain a Substrate architektúrájának hagyományos felépítését követi, amely világosan elkülöníti egymástól a node-réteget és a runtime-réteget. Ez a szétválasztás alapvető jelentőségű a protokoll frissítési modellje és operatív működése szempontjából.

A node-réteg azokat az összetevőket foglalja magában, amelyek natív szoftverként futnak a validator hardvereken. Ide tartozik a peer-to-peer hálózati stack — libp2p alapokon —, a konszenzusmotor, amely koordinálja a blokkgyártást és a finalizációt, valamint az állandó adattárolási réteg, amely fenntartja a blokklánc állapotát. A node-réteg kezeli a peer-felderítési folyamatokat, a tranzakciók hálózaton belüli propagációját, a külső kliensektől érkező Remote Procedure Call (RPC) kéréseket, valamint interfészként szolgál a runtime felé az állapotátmenetek végrehajtásához.



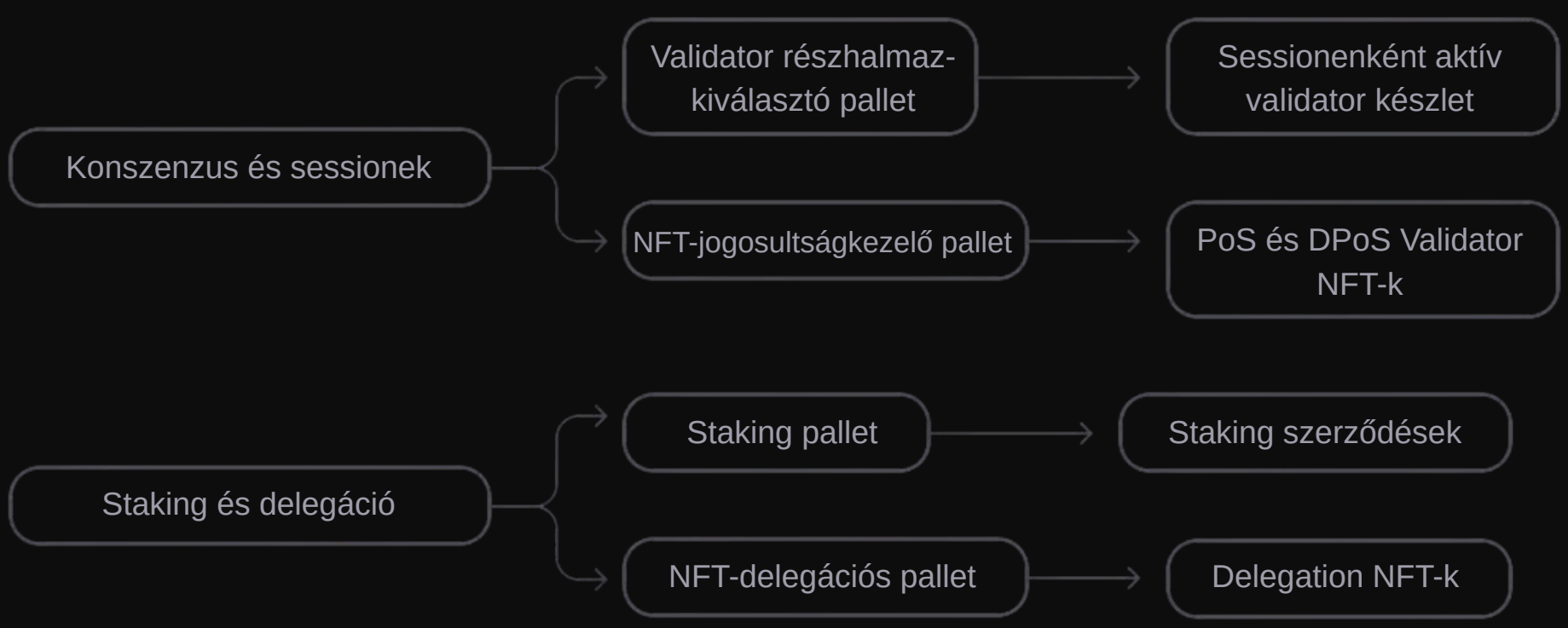
A runtime-réteg definiálja a blokklánc üzleti logikáját: az állapotátmeneteket szabályozó mechanizmusokat, az account-egyenlegeket, a staking műveleteket, az NFT-életciklus kezelését és minden egyéb on-chain műveletet. Kritikus jelentőségű, hogy a runtime WebAssembly (Wasm) formátumba fordítva kerül tárolásra magának a chain state-nek a részeként. Amikor egy validator új blokkot állít elő, a tranzakciók validálásához és alkalmazásához mindig az aktuális on-chain runtime kerül végrehajtásra. Ez az architektúra teszi lehetővé a forkless frissítéseket: egy governance-jogosultsággal jóváhagyott runtime frissítés egy on-chain tranzakción keresztül kerül alkalmazásra, majd minden validator automatikusan az új logikát kezdi futtatni a következő blokktól kezdődően, manuális szoftverfrissítés nélkül.

A node-réteg és a runtime-réteg szétválasztása egyúttal egy világos biztonsági határvonalat is létrehoz. A node-réteg natív kódként működik, közvetlen hozzáféréssel a rendszererőforrásokhoz — például a hálózati kapcsolatokhoz, adattároláshoz és kriptográfiai host funkciókhoz —, míg a runtime egy sandboxolt WebAssembly környezetben fut, kontrollált host-funkció hozzáféréssel. Ez a sandboxolt működés biztosítja, hogy a runtime logika ne férhessen hozzá közvetlenül a node-szintű állapotokhoz, illetve ne sérthesse azok integritását, továbbá hogy az alkalmazási logikában bekövetkező hibák ne veszélyeztethessék a hálózati vagy adattárolási rétegek stabilitását. Egy pénzügyi fókuszú lánc esetében — ahol a runtime hibák költsége közvetlen gazdasági értékben mérhető — ez az izoláció kiemelten fontos.

A runtime palletekből épül fel, amelyek moduláris komponensek, hasonlóan a hagyományos szoftverfejlesztés során használt könyvtárakhoz vagy csomagokhoz. Minden pallet egy meghatározott funkcionális területet kezel saját adattárolással, eseményekkel, hibakezeléssel és hívható függvényekkel. A palletek jól definiált trait interfészeken keresztül képesek egymással együttműködni és egymásra épülni, lehetővé téve a kompozabilitást szoros összekapcsolás nélkül. Ez a modularitás teszi lehetővé a Mosaic Chain számára, hogy egyes protokollfunkciókat hozzáadjon, módosítson vagy lecseréljen anélkül, hogy az nem kapcsolódó rendszerelemek működését zavarná.

Fő on-chain modulok

A Mosaic Chain runtime-ja két fő palletkategória köré szerveződik: a konszenzushoz kapcsolódó palletek, amelyek a hálózat alapvető biztonsági infrastruktúráját alkotják, valamint az alkalmazási logikát biztosító palletek, amelyek a decentralizált alkalmazások működését támogatják.



NFT-Permission Pallet. Ez a pallet a standard pallet-nfts frameworkre épül, és a Permission NFT-k létrehozását, tulajdonkezelését, attribútum-hozzárendelését és teljes életciklusát kezeli. Támogatja új Permission NFT-k kibocsátását, az NFT-k validator accountokhoz történő binding és unbinding műveleteit, valamint az NFT-k chilling és unchilling állapotkezelését, amelyek ideiglenesen letiltják vagy újraengedélyezik azok konszenzusban való részvételét. A pallet garantálja azt az invariánst, hogy kizárólag megfelelően bound állapotú NFT-k jogosíthatnak fel node-okat blokkgyártásban való részvételre.

Staking pallet. Ez a pallet biztosítja a MOS tokenek és NFT-k staking és unstaking műveleteinek alapvető funkcionalitását. Kezeli a delegatorok és validatorok közötti staking szerződések teljes életciklusát, érvényesíti a minimális staking időszakokat és mennyiségeket, feldolgozza a jutalékszámításokat, valamint együttműködik a slashing mechanizmussal. A staking pallet kezeli továbbá a „kick” műveletet is, amely biztosítja, hogy a validator meghatározott feltételek mellett eltávolítson delegatorokat.

NFT-Delegation Pallet. Ez a pallet olyan Delegation NFT-k kezeléséért felel, amelyek további stake-et reprezentálnak MOS-ban denominált névleges értékkel, valamint maximális session-részvételi korláttal. Kezeli a meghatározott névleges értékű és részvételi időtartamú Delegation NFT-k kibocsátását, azok DPoS (delegációt támogató) validatorokhoz történő binding folyamatát, a szerződés lejáratakor történő unbinding műveleteket, valamint az arányos slashing végrehajtását abban az esetben, ha a kapcsolódó validator büntetés alá kerül. A pallet tartalmaz egy automatikus lejárati logikát is, amely aktiválódik, amikor egy bound delegáció eléri a konfigurált maximális session-számot.

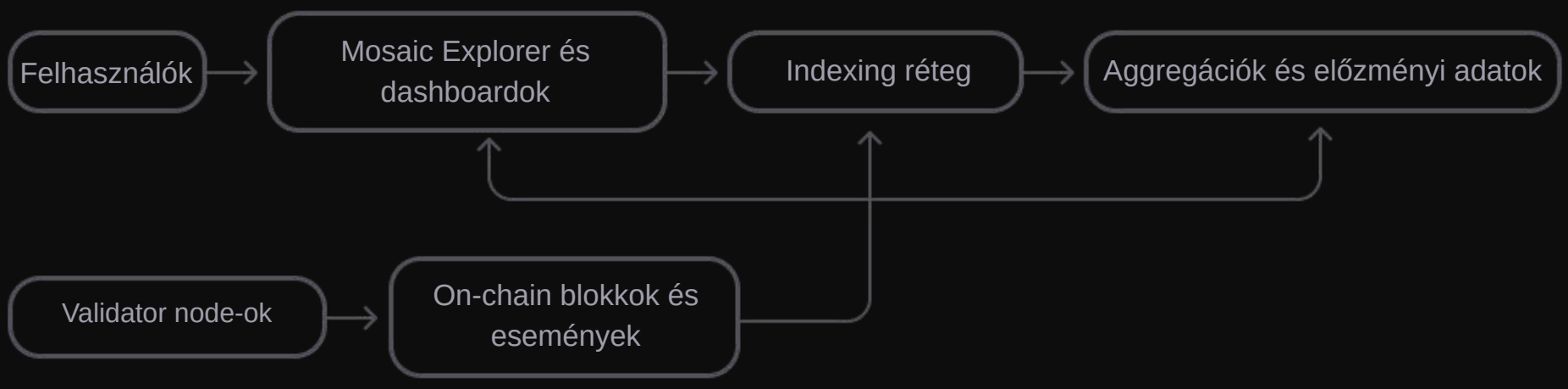
Validator-Subset-Selection Pallet. Ez a pallet valósítja meg azt a továbbfejlesztett bucket selection algoritmust, amely meghatározza, hogy mely validatorok kerülnek be az egyes sessionek aktív készletébe. Kezeli az egyes validatorok bucket állapotát, kiszámítja a kiválasztási eredményeket a sessionhatárokon, valamint dinamikusan igazítja a sessionek hosszát a kiválasztott validatorok számához. Ez a pallet testesíti meg on-chain formában a 4. fejezetben részletesen ismertetett kiválasztási mechanizmust.

A projekt a Mosaic Chain GitHub tárolóján keresztül nyílt forráskódúvá tette a runtime alapvető komponenseit (github.com/Mosaic-Chain/mosaic-chain) annak érdekében, hogy támogassa az auditálhatóságot és a közösségi hozzájárulásokat.

Explorer, indexelés és külső interfészek

A Mosaic Explorer egyszerre szolgál blokklánc-explorerként és elsődleges operációs interfészként validatorok és delegatorok számára. Működését egy több technológiára épülő, decentralizált indexing infrastruktúra támogatja, amely valós idejű hozzáférést biztosít az on-chain adatokhoz.

A Mosaic Chain minden node-ja kettős szerepet tölt be: egyrészt részt vesz a konszenzusfolyamatban blokkok előállításával és validálásával, másrészt egyidejűleg továbbítja az on-chain adatokat az indexing réteg felé, amely a frontend interfészek működését kiszolgálja. Ez az architekturális megközelítés biztosítja, hogy az explorer és más frontend rendszerek adatellátása ne függjön központosított indexer szolgáltatástól. Ehelyett az adatáramlás eredendően decentralizált módon működik, ahol minden node hozzájárul a teljes adatinfrastruktúra fenntartásához.



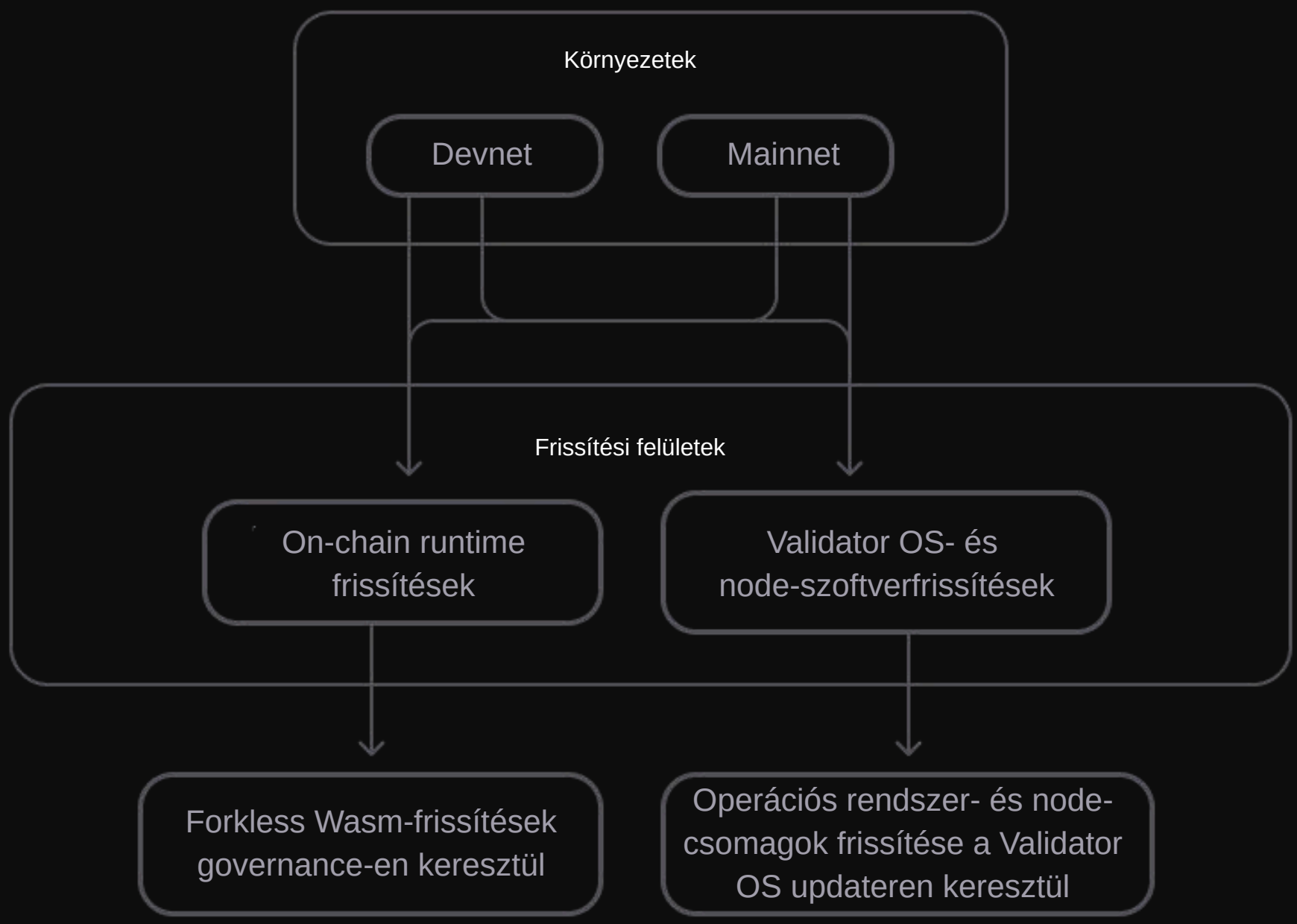
Az indexer olyan hatékony adatlekérdezési képességeket biztosít, amelyek túlmutatnak azon, amit egy teljes node felé irányított közvetlen RPC-hívás nyújtani képes. Míg egy full node elsősorban az aktuális állapotra vonatkozó lekérdezések kiszolgálására alkalmas, addig az indexer olyan származtatott és historikus adatstruktúrákat tart fenn, amelyeket kifejezetten az explorer, a validator dashboardok és a wallet interfészek lekérdezési mintázataihoz optimalizáltak. Ide tartoznak például az aggregált staking statisztikák, a történeti jutalomelosztások, a validator teljesítménymutatók és a session-részvételi rekordok.

A validator frontend dedikált vezérlőfelületet biztosít a node-üzemeltetők számára. Valós idejű monitorozást kínál a node-egészségügyi állapotokról, teljesítménymutatókról, staking státuszokról, jutalékbeállításokról és blokkjutalom-előzményekről. A publikus frontend ezzel párhuzamosan intuitív felületet nyújt bármely felhasználó számára a blokklánc-adatok böngészéséhez, a validator teljesítmények elemzéséhez és az alapvető hálózati információk eléréséhez. Mindkét interfész egy gateway-rétegen keresztül működik, amely a kéréseket a megfelelő backend szolgáltatások felé irányítja. A nagy mennyiségű olvasási műveletet és historikus lekérdezéseket az indexer szolgálja ki, míg az élő láncállapot-lekérdezések és tranzakcióbeküldések gateway-en keresztül elérhető RPC node-okon keresztül történnek. Ez az architektúra nagy teljesítményű adat-hozzáférést biztosít anélkül, hogy a frontend rendszereknek közvetlenül egyedi validator node-okat kellene célozniuk.

Hálózatok és konfigurációs felületek

A Mosaic Chain több különálló hálózati környezetben működik, amelyek eltérő célokat és konfigurációkat szolgálnak ki. A devnet fejlesztési és tesztelési környezetként funkcionál, ahol az új runtime funkciók, paramétermódosítások és operatív folyamatok validálása történik a mainnet telepítést megelőzően.

A mainnet jelenti az éles hálózati környezetet, ahol a valódi MOS tokenek, Validator NFT-k és a hálózathoz kapcsolódó gazdasági következmények működnek.



A devnet és a mainnet között eltérő konfigurációs paraméterek működhetnek, többek között a sessionek hossza, a slashing büntetések súlyossága, a minimális staking mennyiségek, a validator részhalmaz mérete, valamint különböző biztonsági küszöbértékek. A devnet jellemzően lazább paraméterezéssel működik annak érdekében, hogy támogassa a gyors iterációt és tesztelést, míg a mainnet paraméterei már a produkciós környezet biztonsági és stabilitási követelményeihez igazodnak.

A protokoll két, egymástól elkülönülő frissítési mechanizmussal rendelkezik. A runtime frissítések az on-chain üzleti logikát módosítják — beleértve a palleteket, paramétereket és állapotátmeneteket —, és a korábban ismertetett forkless frissítési mechanizmuson keresztül kerülnek telepítésre. Ezzel szemben az operációs rendszer- és node-szoftverfrissítések a node-réteget és a Validator OS környezetet érintik, valamint a 10. fejezetben ismertetett Validator OS frissítési rendszeren keresztül kerülnek terjesztésre. A két frissítési útvonal egymástól független: egy runtime frissítés nem igényel Validator OS frissítést és egy Validator OS frissítés sem követel meg runtime módosítást. Ez a szétválasztás biztosítja, hogy a lánclogika változásai és az operatív szoftverkarbantartás egymástól független ütemezésben történhessenek anélkül, hogy koordinációs szűk keresztmetszetek alakulnának ki.

Konszenzus és validator készletmechanika

Konszenzus áttekintése

A Mosaic Chain blokkgyártáshoz Proof of Authority (PoA) modellt alkalmaz — egy módosított Aura implementáció formájában —, amelyet egy NPoS-stílusú gazdasági modell egészít ki a validator jogosultságok, delegációk, jutalmazás és slashing kezelésére. A staking- és delegációs modell koncepcionálisan hasonló a Polkadot Nominated Proof of Stake (NPoS) rendszeréhez, ugyanakkor a Mosaic a validator jogosultságokat és stake-kötelezettségeket Permission NFT-k formájában reprezentálja, valamint bucket-alapú validator részhalmaz-kiválasztási algoritmust alkalmaz annak érdekében, hogy egy nagyméretű validator populáció rotációs módon vehessen részt a konszenzusfolyamatban egy kompakt aktív készleten keresztül.

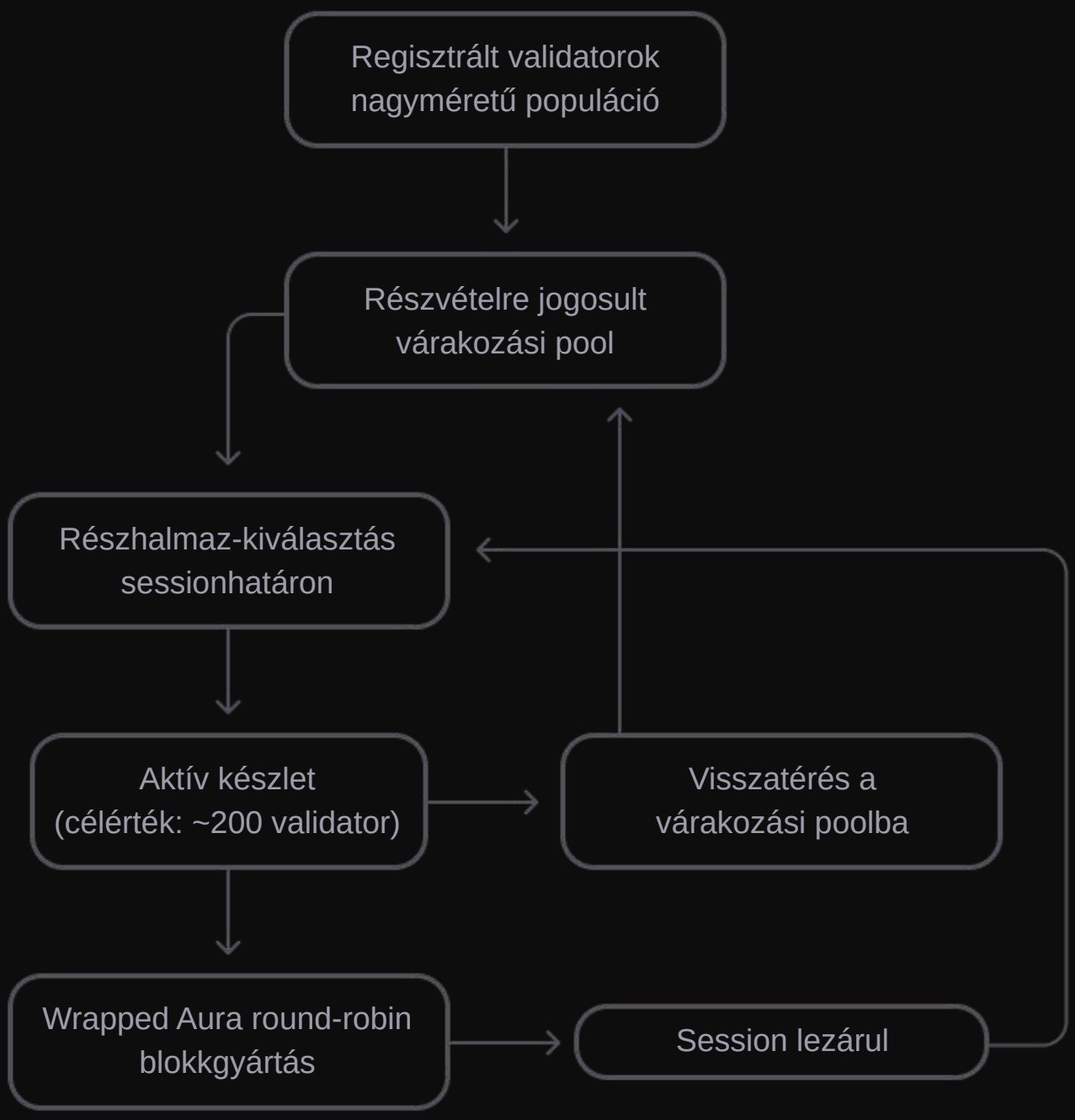
A konszenzusmechanizmus által kezelt alapvető kihívás két kívánatos tulajdonság közötti egyensúly megteremtése: a széles körű részvétel biztosítása — vagyis minél több validator hozzájárulása a decentralizációhoz; valamint a hatékony blokkgyártás fenntartása — gyors, kiszámítható finalitással és alacsony kommunikációs többletterhelés mellett.
A hagyományos konszenzusprotokollok megkövetelik, hogy minden validator minden egyes konszenzuskör során üzeneteket váltson egymással, ami olyan kommunikációs komplexitást eredményez, amely kvadratikusan növekszik a résztvevők számával. Egy több mint 2400 validatort célzó hálózat esetében, 6 másodperces blokkidő mellett, ez a megközelítés gyakorlatilag nem lenne fenntartható.

A Mosaic Chain ezt a problémát úgy oldja meg, hogy elkülöníti a teljes validator populációt az aktuálisan aktív validator készlettől. Egy adott időpillanatban a teljes hálózat több, mint 2400 regisztrált validatorból állhat, amelyek mindegyike rendelkezik bound Validator NFT-vel és szinkronizált node-dal. Ugyanakkor sessionenként csupán körülbelül 200 validator vesz részt aktívan a konszenzusfolyamatban. Ez az aktív készlet minden sessionhatárnál rotálódik, biztosítva, hogy idővel minden validator méltányos lehetőséget kapjon blokkok előállítására és jutalomszerzésre, miközben a sessionenként kommunikációs többletterhelés kezelhető szinten marad.

A blokkgyártást az aktív készlet egy módosított Aura (Authority Round) konszenzusmechanizmuson keresztül végzi. Az Aura egy egyszerű és hatékony konszenzusprotokoll, amelyben a validatorok előre meghatározott sorrendben váltják egymást a blokkgyártás során. Az aktív készlet minden validatorához meghatározott időslotok tartoznak, amelyek során jogosult blokkot előállítani. Ez a determinisztikus kiosztás kiküszöböli a proof-of-work rendszerekre jellemző energiafelhasználást és probabilisztikus finalitást, miközben kiszámítható, 6 másodperces blokkidőt biztosít.

A „wrapped” megjelölés arra utal, hogy a Mosaic Chain Aura implementációja a standard Aura protokollra épülő egyedi kiterjesztéseket tartalmaz. Ezek a kiterjesztések integrálják a validator részhalmaz-kiválasztási mechanizmust, az NFT-alapú jogosultsági rendszert, valamint a sessionkezelési logikát közvetlenül a konszenzusmotor működésébe. Az eredmény egy olyan konszenzusmechanizmus, amely megőrzi az Aura egyszerűségét és hatékonyságát, miközben támogatja a Mosaic Chainre jellemző validator rotációs, gazdasági biztonsági és operatív hozzáférhetőségi funkciókat.

Érdemes megvizsgálni, hogyan viszonyul ez a megközelítés az alternatív modellekhez. A tisztán NPoS-alapú rendszerek — például a Polkadot relay chainje — stake-súlyozott választási algoritmusokat alkalmaznak az aktív validator készlet meghatározására, ami összetett jutalomelosztási és nominátor–validator igazítási mechanizmusokat eredményez. Számos PoA-alapú hálózat ezzel szemben fix és viszonylag kis validator készlettel működik, ami korlátozza a decentralizáció kiterjeszthetőségét. A Mosaic Chain a PoA-alapú blokkgyártást egy NPoS-stílusú delegációs gazdasági modellel kombinálja, miközben nagyméretű, regisztrált validator populációt tart fenn. Az aktív készletek rotációját a bucket selection algoritmus határozza meg, amely a méltányos részvételt helyezi előtérbe, miközben megőrzi egy kompakt aktív készlet operatív hatékonyságát.



Sessionek és aktív készletrotáció

A Mosaic Chain időkezelése elkülönített sessionekre épül, amelyek egyenként körülbelül egyórás időtartamot fednek le. Egy session az aktuális aktív validator készlet teljes blokkgyártási ciklusát reprezentálja. Az egyes sessionek határán a validator részhalmaz-kiválasztási algoritmus lefut, meghatározza a következő aktív készletet, majd az új validator készlet megkezdi a blokkgyártást a következő session során.

A session életciklusa a következőképpen működik. Az aktuális session lezárásakor a validator-subset-selection pallet kiértékeli az összes jogosult validator bucket állapotát, majd előállítja a következő sessionre kiválasztott validatorok listáját. Minden sessionhatárnál a lánc aktiválja a korábban queue-ba helyezett validator készletet, miközben egyidejűleg kiszámítja és sorba állítja a következő részhalmazt is. A sessionek időtartama dinamikusan kerül meghatározásra a kiválasztott validatorok számának egész számú többszöröseként annak érdekében, hogy kiegyensúlyozott round-robin slotkiosztás valósuljon meg. Ennek eredményeként minden kiválasztott validator azonos számú blokkgyártási slotot kap sessionenként — tipikusan egyet körönként —, nem pedig pontosan egyetlen slotot.
A kiválasztott validatorok a várakozási állapotból aktív státuszba lépnek át, míg az előzőleg aktív validatorok visszakerülnek a várakozási poolba.

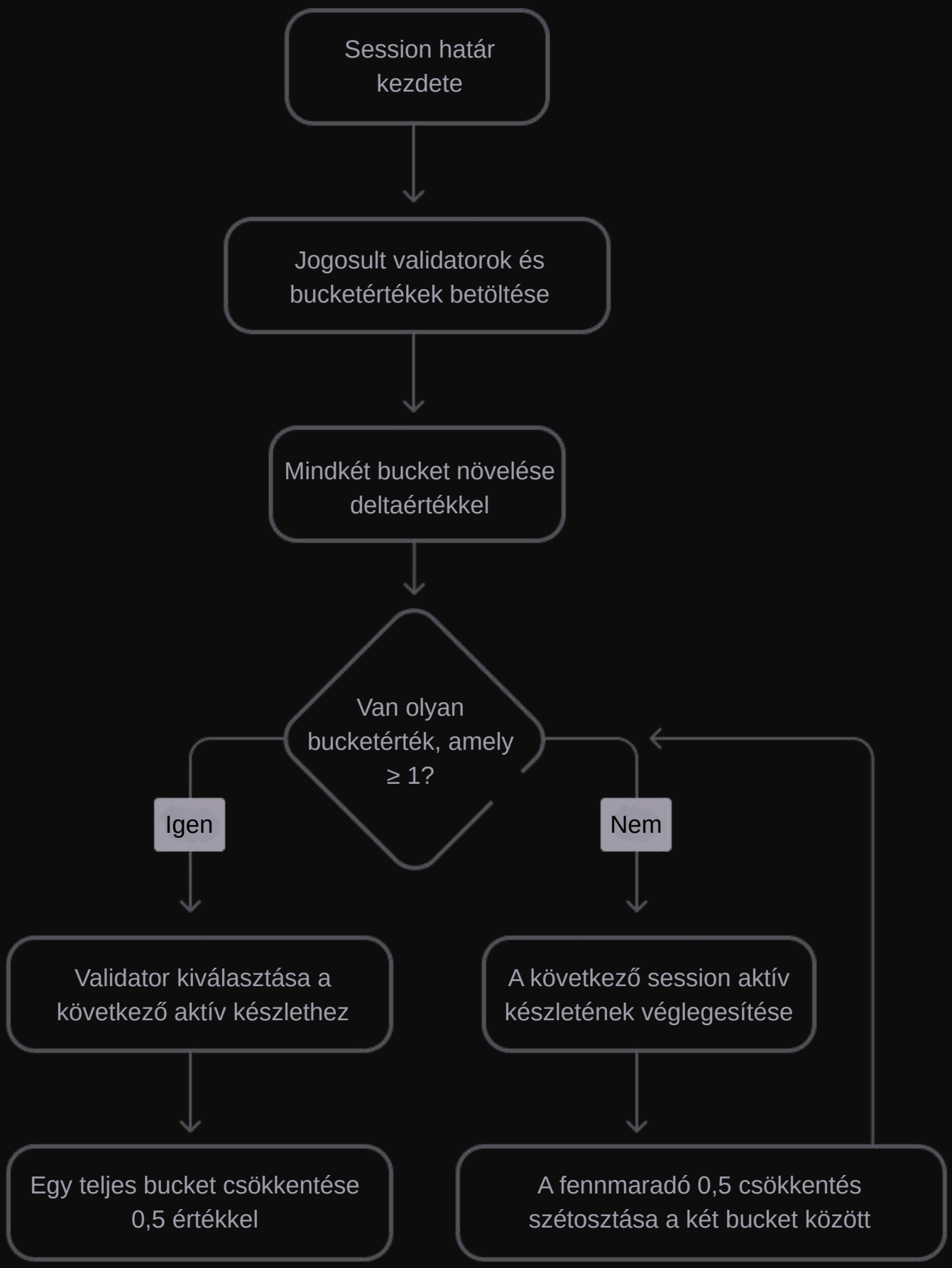
Ez a session-alapú rotáció több fontos tulajdonságot biztosít. Először is garantálja az időbeli méltányosságot: kellően hosszú időtávon minden jogosult validator megközelítőleg azonos számú kiválasztást kap. Másodszor, kiszámíthatatlanságot biztosít: a bucket selection algoritmus randomizált jellege megnehezíti annak előrejelzését, hogy egy adott session során mely validatorok lesznek aktívak, ezáltal csökkentve a célzott támadási felületeket. Harmadszor, operatív egyszerűséget nyújt, mivel az aktív validator készlet a teljes session időtartamára rögzített marad, kiküszöbölve a session közbeni validatorcserék komplexitását.

Az egyórás session időtartam tudatos egyensúlyt teremt a rotáció gyakorisága és az operatív stabilitás között. A rövidebb sessionek gyakoribb rotációt — és ezáltal finomabb méltányosságot — biztosítanának, ugyanakkor növelnék az átállásokból származó terhelést és csökkentenék a validatorok számára rendelkezésre álló blokkgyártási időt. A hosszabb sessionek mérsékelnék az átállási terhelést, viszont növelnék annak az időablakát, amely alatt egy kompromittált aktív készlet kárt okozhatna, valamint csökkentenék a méltányosság granularitását. Az egyórás session idő — körülbelül 200 fős aktív validator készlettel kombinálva — normál működési körülmények között azt eredményezi, hogy minden kiválasztott validator sessionenként hozzávetőlegesen egy blokkot állít elő, miközben egy teljes session nagyjából egy óra alatt zárul le.

Mosaic Chain

Validator-részhalmaz kiválasztás

A validator részhalmaz-kiválasztási mechanizmus felelős annak meghatározásáért, hogy az egyes sessionek konszenzusfolyamatában mely validatorok vehetnek részt. A mechanizmusnak három alapvető követelménynek kell megfelelnie: **méltányosság** — minden validator közel azonos gyakorisággal kerüljön kiválasztásra hosszabb időtávon; **kiszámíthatatlanság** — a következő session aktív készlete ne legyen előre meghatározható publikus információk alapján; **stabilitás** — az aktív készlet mérete maradjon közel a körülbelül 200 validatoros célértékhez sessionenként.



A Mosaic Chain egy továbbfejlesztett bucket selection algoritmust alkalmaz annak érdekében, hogy biztosítsa ezeket a tulajdonságokat. Az algoritmus működése a következő.

Minden validatorhoz két bucket tartozik, amelyek mindegyike egy-egy, egymástól független, 0 és 1 közötti egyenletes eloszlású véletlen értékkel inicializálódik. Minden kör— vagyis session határ — során valamennyi bucket értéke növelésre kerül a következő képlet alapján: subset_size / (2 * number_of_validators) ahol a subset_size az aktív készlet célmérete, míg a number_of_validators az összes jogosult validator száma. Azok a validatorok, amelyek legalább egyik bucketjükben elérik vagy meghaladják az 1,0 értéket, kiválasztásra kerülnek a következő session aktív készletébe. A kiválasztást követően a validator egyik teljes bucketértéke 0,5-tel csökken, míg a fennmaradó 0,5 csökkentés egyenletesen oszlik el a validator két bucketje között.

Ez a kétbucketes mechanizmus kedvező statisztikai tulajdonságokkal rendelkező kiválasztási viselkedést eredményez. Az 1 000 validatorral és 200-as célzott aktív készletmérettel végzett szimulációk — többnapos időablakokon vizsgálva — közel egyenletes kiválasztási eloszlást mutatnak időben, miközben elegendő randomizációt biztosítanak a kiszámíthatóság csökkentése érdekében. A gyakorlatban az algoritmus az aktív készlet méretét szorosan a célérték körül tartja, miközben biztosítja, hogy egyetlen validator se kerüljön tartósan előnybe vagy hátrányba a kiválasztási lehetőségek tekintetében, összehasonlítható időintervallumokon belül. Ez támogatja a Mosaic Chain alapvető célkitűzését: egy sessionenként kompakt aktív készlet fenntartását a hatékony blokkgyártás érdekében, széles körű részvétellel párosítva egy jóval nagyobb validator populációban.

Az algoritmus által létrehozott részhalmazméretek megközelítőleg binomiális eloszlást követnek, 250-es átlagértékkel és 13,8-as empirikus szórással, amely hatékonyan közelíthető Gauss-eloszlással. Ez azt jelenti, hogy az aktív készlet mérete enyhén ingadozik a célérték körül, ugyanakkor előre jelezhető tartományon belül marad, biztosítva az egyenletes hálózati átviteli teljesítményt a sessionek között.

Operatív működési eredmények

Normál működési körülmények között a konszenzusmechanizmus 6 másodpercenként állít elő új blokkot, miközben az egyes sessionek körülbelül 200 validatorból álló aktív készlete óránkénti rotációban cserélődik. A hálózathoz újonnan csatlakozó validatorok egy regisztrációs folyamaton mennek keresztül — amelyet a 10. fejezet ismertet részletesen —, majd bekerülnek a várakozási poolba, ahol jogosulttá válnak a későbbi sessionek során történő kiválasztásra.

A hálózatból kilépő validatorok önkéntesen chilled állapotba helyezhetik NFT-jüket, amely eltávolítja őket a kiválasztásra jogosult validatorok várakozási pooljából a jövőbeni sessionek tekintetében. A chilling azonban nem távolít el visszamenőlegesen egy validatort az aktuális sessionből, és amennyiben a validator már korábban queue-ba került, még részt vehet a következő sessionben is, mielőtt a chilling hatása a további kiválasztások során érvénybe lépne.

A konszenzusmechanizmus együttműködik a slashing és chilling rendszerrel — amelyet az 5.6-os fejezet ismertet részletesen — annak érdekében, hogy kezelje a validatorok hibás vagy szabálytalan működését. Amennyiben egy aktív validator offline állapotba kerül a számára kijelölt blokkgyártási slot során, az adott slot kihagyásra kerül, a validator pedig slashing büntetésben részesül. Ha egy validator account elegendő számú szabálysértést halmoz fel az automatikus chilling aktiválásához, a protokoll chilled állapotba helyezi a validator NFT-t — amely funkcionálisan megegyezik egy manuális chilling művelettel. Ettől a pillanattól kezdve a validator kizárásra kerül a jövőbeni kiválasztásokból, miközben az aktuális sessionben — és amennyiben korábban már queue-ba került, potenciálisan a következő sessionben is — még részt vehet. Az aktív készlet többi validatora ettől függetlenül normál módon folytatja a blokkgyártást; a kihagyott slotok enyhe késedelmet okoznak, de nem eredményeznek tartós blokkgyártási leállást.

Az átmeneti kapcsolódási problémákkal küzdő validatorok számára a protokoll egy 72 sessionből álló slacking időszakot definiál. Az unbinding folyamat a delegator tranzakciójának időpontjában kerül előkészítésre, majd a session periódus végén hajtódik végre. A slacking periódus elsődleges célja a korai kilépés elleni védelem biztosítása: amennyiben egy validator a slacking időszaknál hosszabb ideig marad chilled állapotban, miközben a delegator minimális staking periódusa még nem telt le, a delegator a fennmaradó zárolási idő ellenére is végrehajthatja az unbinding műveletet és újradelegálhatja tokenjeit. Ez a konstrukció figyelembe veszi, hogy a rövid ideig tartó üzemszünetek az operatív működés természetes részét képezhetik — különösen otthoni infrastruktúrán működő validatorok esetében —, miközben továbbra is szankcionálja a tartós megbízhatatlanságot, amely veszélyeztetheti a hálózat biztonságát.

NFT-alapú részvétel, staking és gazdasági biztonság

Miért NFT-k a validator jogosultságokhoz?

A validator részvételi jogosultságok NFT-ként történő reprezentálása — a hagyományos, egyenlegalapú staking modellek alkalmazása helyett — tudatos architekturális döntés, amely mögött több fontos megfontolás áll. A legtöbb jelenlegi proof-of-stake hálózatban a tokenbirtoklás és a validator státusz közötti kapcsolatot teljes mértékben protokollszintű könyvelés közvetíti: a validator tokeneket köt le, a staking pallet nyilvántartja a lekötött összeget, a konszenzusmechanizmus pedig ebből a staking állapotból határozza meg a részvételi jogosultságot. Ez a megközelítés funkcionálisan működőképes, ugyanakkor átláthatatlan: a staking kapcsolatok a protokoll adattárolási struktúráiban jelennek meg, nem pedig önálló, vizsgálható, átruházható vagy más instrumentumokkal kombinálható on-chain objektumokként.
A Mosaic Chain NFT-alapú modellje ettől alapvetően eltérő megközelítést alkalmaz azáltal, hogy a validator jogosultságokat első osztályú on-chain eszközként kezeli. Ennek a tervezési döntésnek három elsődleges indoka van.

Explicit jogosultságkezelés. Az egyenlegalapú staking rendszerekben a tokenegyenleg és a validációs jogosultság közötti kapcsolat implicit módon létezik, és olyan protokollszabályok határozzák meg, amelyek a résztvevők számára nem minden esetben egyértelműek. Az NFT-modell explicit módon teszi láthatóvá a jogosultságokat: egy validator kizárólag akkor vehet részt a konszenzusfolyamatban, ha rendelkezik megfelelően bound állapotú Validator NFT-vel. Ez a bináris feltétel egyszerűen ellenőrizhető, könnyen értelmezhető és on-chain módon egyértelműen kikényszeríthető.

Hordozhatóság és kompozabilitás. A Validator NFT-k olyan on-chain eszközök, amelyek — a binding szabályok figyelembevételével — átruházhatók, amennyiben az NFT éppen nem vesz részt aktívan a konszenzusfolyamatban. Ez a hordozhatóság alkalmassá teszi másodlagos piacok kialakulását a validator jogosultságok számára, támogatja a validator infrastruktúrák különböző hardverek vagy üzemeltetők közötti áthelyezését, valamint megalapozza a jövőbeni kompozabilitást más on-chain instrumentumokkal.

Átlátható stake-reprezentáció. Minden Validator NFT rendelkezik egy MOS-ban denominált névleges értékkel, amely azt a minimális stake-kötelezettséget reprezentálja, amelyet az adott validator a hálózat biztonságának fenntartásához biztosít. Ez a névleges érték első osztályú on-chain attribútumként jelenik meg, nem pedig származtatott számítás eredményeként, ezáltal az egyes validatorok gazdasági biztonsághoz való hozzájárulása azonnal láthatóvá válik a delegatorok, governance-résztvevők és külső megfigyelők számára.

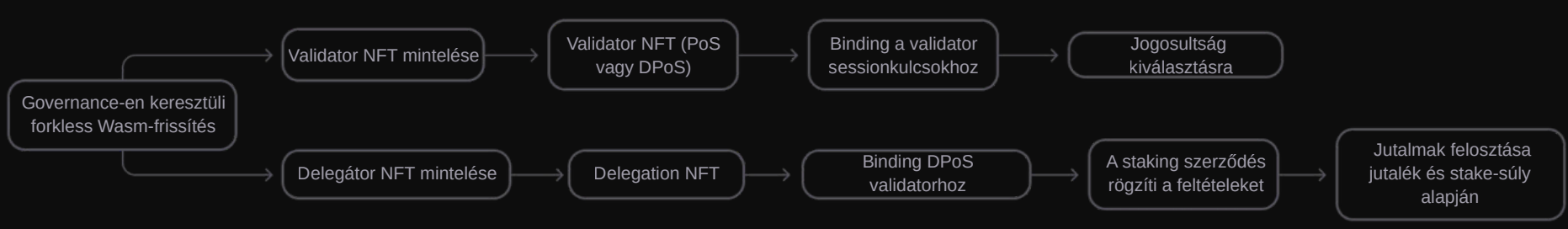
Validator NFT-k

A Validator NFT-k két különböző típusban léteznek, amelyek eltérő szerepet töltenek be a konszenzus- és staking modellben.

A PoS (Proof of Stake) NFT-ket olyan validatorok birtokolják, amelyek kizárólag saját self-stake felhasználásával vesznek részt a konszenzusfolyamatban. Egy PoS NFT jogosultságot biztosít tulajdonosának validator node üzemeltetésére és a blokkgyártási rotációban való részvételre. A PoS NFT névleges értéke a validator saját stake-kötelezettségét reprezentálja. Fontos tulajdonság, hogy a PoS validatorok az NFT kezdeti névleges értékén túl nem növelhetik tovább self-stake pozíciójukat, ezáltal a rendszer megakadályozza a stake koncentrációját és fenntartja a kiszámítható biztonsági modellt.

A DPoS — vagyis delegációt támogató — NFT-ket olyan validatorok birtokolják, amelyek saját self-stake mellett más MOS token tulajdonosoktól származó delegált stake-et is elfogadnak. Bár a Mosaic Chain konszenzusmotorja PoA-alapú — Aura-alapú slotrotációval —, a „DPoS” megnevezés ebben a kontextusban a delegációt támogató validator jogosultság rövidített formája az NPoS-jellegű gazdasági modellen belül. A standard PoS NFT által biztosított jogosultságokon túl a DPoS NFT lehetővé teszi, hogy a validator staking szerződéseket kössön olyan delegatorokkal, amelyek Delegation NFT-ket birtokolnak. Egy delegációt támogató validator teljes stake-állománya a validator saját stake-jének — vagyis az NFT névleges értékének —, valamint az adott validatorhoz bound állapotban kapcsolódó összes delegált stake összegéből áll.

A Validator NFT-k binding és unbinding szemantikája kritikus szerepet játszik a protokoll biztonsági modelljében. Egy Validator NFT-t a konszenzusfolyamatban való részvétel előtt egy meghatározott validator node-hoz kell bound állapotban kapcsolni — amelyet a validator sessionkulcsai azonosítanak. Bound állapotban az NFT nem ruházható át és nem módosítható, biztosítva ezzel, hogy a validator identitása és stake-kötelezettsége az aktív részvétel során stabil maradjon. Az unbinding folyamat megköveteli, hogy a validator először chilled állapotba kerüljön — vagyis önként kilépjen a jövőbeni kiválasztásokra jogosult validatorok várakozási pooljából —, valamint megvárja az összes aktív staking szerződés lezárását. Ez a mechanizmus megakadályozza a stake hirtelen kivonását a hálózat biztonsági költségvetéséből.



Delegation NFT-k (Delegator NFT-k)

A Mosaic Chainen történő delegáció nem igényel Delegation NFT-ket. A delegatorok közvetlenül, staking szerződéseken keresztül is delegálhatnak MOS tokeneket. A Delegation NFT egy opcionális instrumentum, amelyet olyan esetekben alkalmaznak, amikor a delegator egy delegációs pozíció átruházható, explicit névleges értékkel rendelkező reprezentációját kívánja létrehozni.

A Delegation NFT-k átruházható, időben korlátozott staking instrumentumokat reprezentálnak, amelyek hozzáférést adnak a MOS token tulajdonosok számára, hogy validator node üzemeltetése nélkül járuljanak hozzá a hálózat biztonságához. Minden Delegation NFT rendelkezik egy MOS-ban denominált névleges értékkel, valamint egy maximális részvételi időtartammal, amely a validatorhoz történő binding után sessionszámban kerül meghatározásra. A Delegation NFT-k részvételi instrumentumként elsősorban a kezdeti befektetési időszak során kerülnek kibocsátásra, ezt követően pedig átruházással szerezhetők meg. A névleges érték és a maximális sessionszám az NFT attribútumait képezik; a tipikus delegatorok a mindennapi staking tevékenység részeként általában nem bocsátanak ki új Delegation NFT-ket. A standard felhasználói folyamat során a MOS token tulajdonosok staking szerződéseken keresztül delegálnak. A Delegation NFT-ket elsősorban olyan esetekben használják, amikor instrumentumszerű pozíció létrehozására van szükség. Az NFT ezt követően egy staking szerződésen keresztül — amelyet az 5.4-es fejezet ismertet részletesen — egy meghatározott delegációt támogató validatorhoz kerül bound állapotba. A binding megtörténte után a Delegation NFT stake-je hozzájárul az adott validator teljes biztosítéki állományához, ezáltal növelve annak súlyát a hálózat gazdasági biztonsági modelljében. A részvételi időszak számítása nem a kibocsátás, hanem a binding pillanatában kezdődik meg, világos időbeli keretet biztosítva a delegációs kötelezettségvállalás számára.

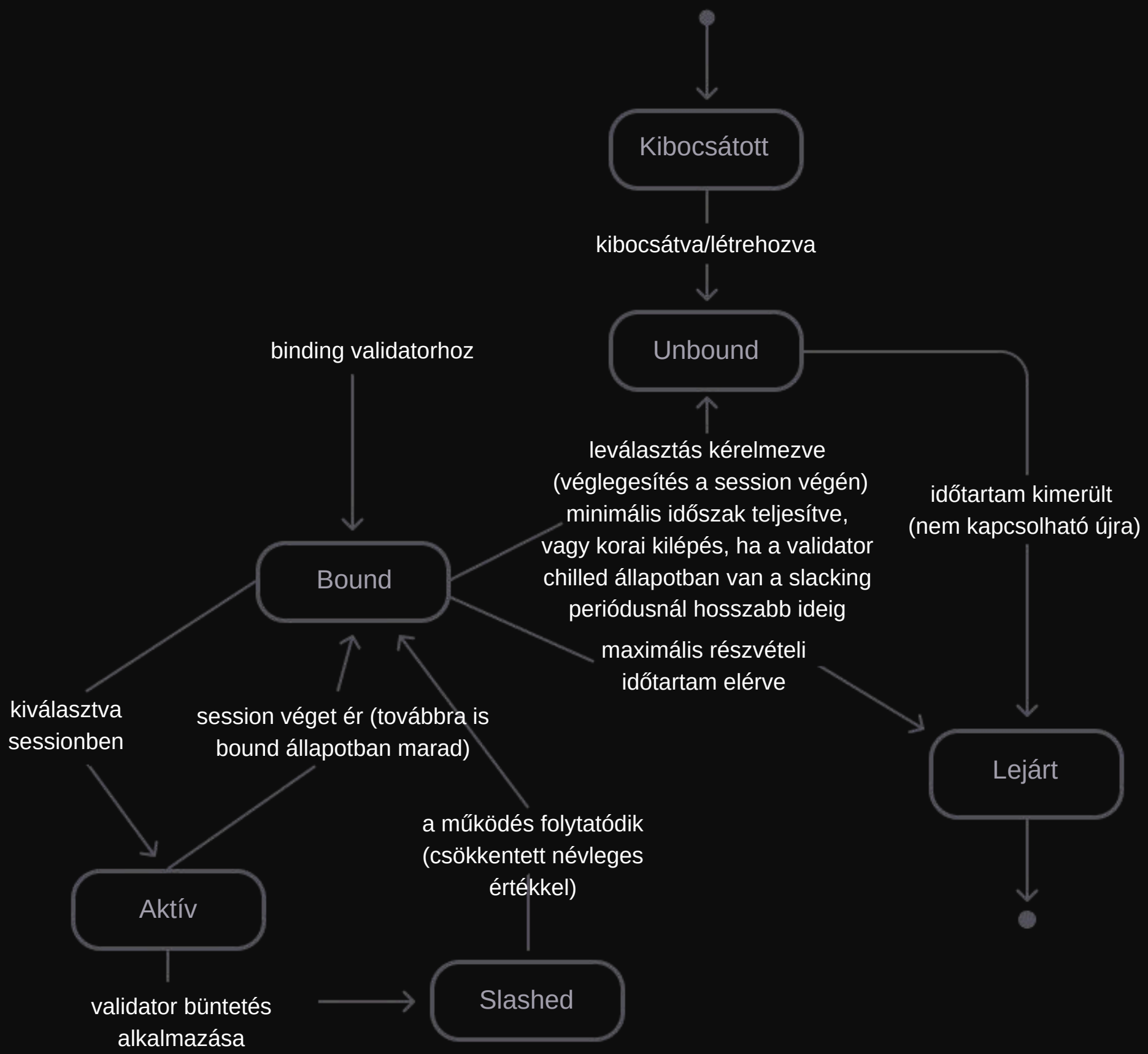
Bound állapotban a Delegation NFT ugyanazon slashing feltételek alá tartozik, mint az a validator, amelyet támogat. Amennyiben a validator szabályszegést követ el vagy büntetésben részesül, az adott validatorhoz bound állapotban kapcsolódó valamennyi Delegation NFT névleges értéke arányosan csökken. Ez a megosztott kockázati modell biztosítja, hogy a delegatorok gazdasági ösztönzői összhangban maradjanak a validator minőségének értékelésével és delegációik megbízható üzemeltetők közötti elosztásával, ezáltal hozzájárulva a validator készlet általános egészségéhez.

A minimális staking időszak lejártát követően a Delegation NFT leválasztható a validatorról. Ettől függetlenül maga a Delegation NFT akkor is lejárhat, amikor eléri a maximálisan konfigurált részvételi időtartamot. A lejárt Delegation NFT-k nem válthatók vissza MOS tokenre, és nem fizetnek vissza „névleges értéket” a tulajdonos számára. Amennyiben egy delegator MOS tokeneket is stakingelt a kapcsolódó staking szerződés keretében, ezek a tokenegyenlegek a staking szerződés unbinding szabályait követik, valamint tükrözik a delegált stake-re alkalmazott esetleges slashing hatásokat is.

Az unbinding folyamat lépcsőzetesen működik: a delegator tranzakciójának beküldésekor indul el, majd a session végén kerül véglegesítésre. A slacking periódus különösen a korai kilépés elleni védelem szempontjából releváns: amennyiben egy validator a slacking időszaknál hosszabb ideig marad chilled állapotban, miközben a minimális staking időszak még érvényben van, a delegator a fennmaradó zárolási idő ellenére is végrehajthatja az unbinding műveletet.

Staking szerződések

Amikor egy delegator egy Delegation NFT-t egy DPoS validatorhoz bind állapotban kapcsol, a rendszer létrehoz egy on-chain staking szerződést, amely rögzíti a delegációs kapcsolat feltételeit. Minden staking szerződés az alábbi paramétereket határozza meg.



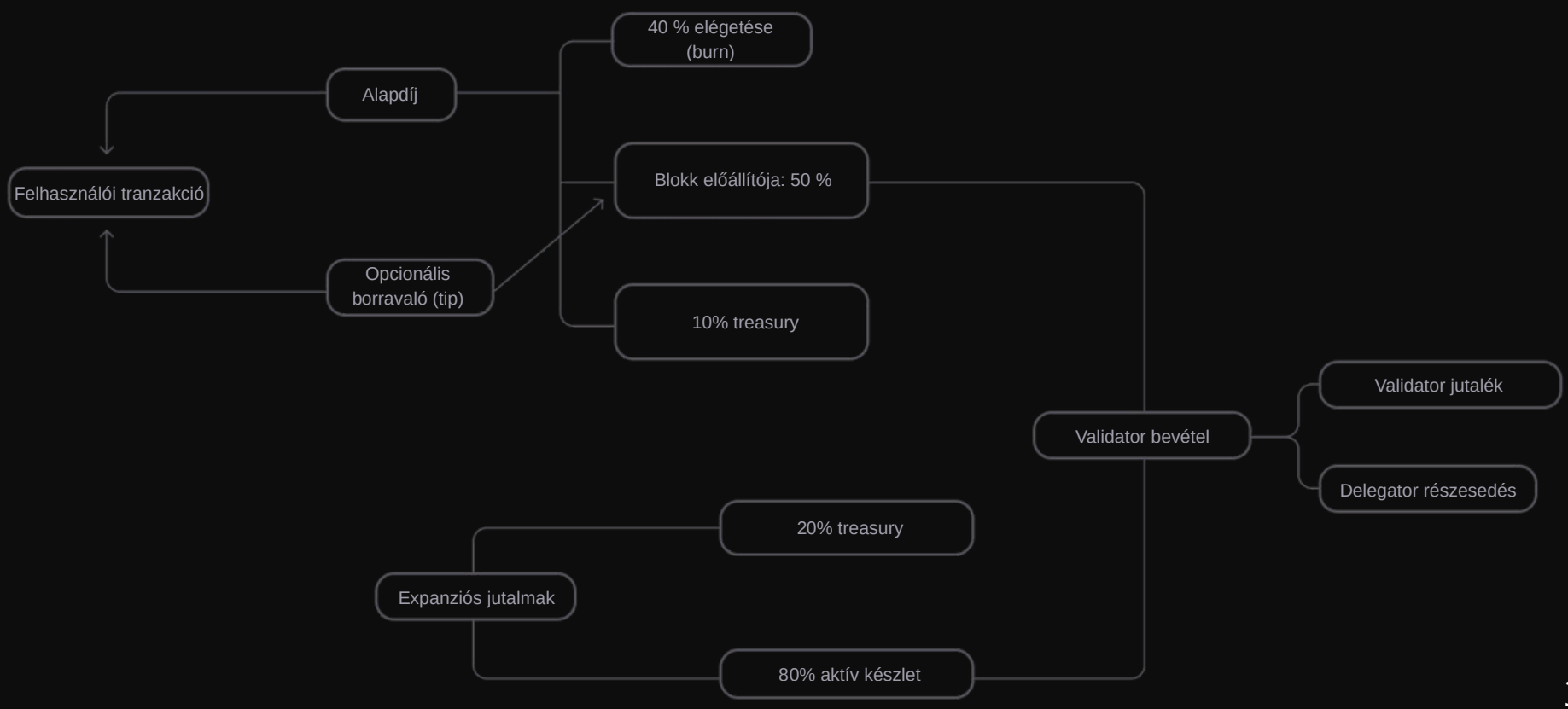
A stake összege biztosítható MOS tokenek formájában, a Delegation NFT névleges értékeként, vagy ezek kombinációjaként, a delegator által preferált instrumentumstruktúrától függően.
A MOS tokenek delegálásához nem szükséges Delegation NFT használata. A validator által meghatározott jutalékráta — globális minimuma 1% — határozza meg azt a jutalomrészt, amelyet a validator megtart, mielőtt a fennmaradó összeget kiosztaná a delegatorok között.
A minimális staking időszak meghatározza, hogy egy delegációnak mennyi ideig kell aktív állapotban maradnia, mielőtt a delegator végrehajthatná az unbinding műveletet. A globális minimum 28 nap — vagyis 672 session —, ugyanakkor az egyes validatorok ennél hosszabb időszakot is előírhatnak. A globális minimális staking mennyiség 50 MOS, és ugyanez a minimum vonatkozik a meglévő delegációk növelésére — vagyis a top-up műveletekre — is.

A staking szerződések működését több fontos viselkedési szabály szabályozza.
Amennyiben egy delegator további stake-et ad egy meglévő szerződéshez, a szerződés feltételei és zárolási periódusa újraindul, megakadályozva ezzel azt, hogy az inkrementális stake-hozzáadások megkerüljék a minimális staking időszakot.
Minden validator legfeljebb 1 000 aktív staking szerződéssel rendelkezhet, ami korlátozza a jutalomelosztási számítások számítási terhelését. Egyetlen validator sem halmozhat fel a teljes MOS kínálat 5%-ánál nagyobb kombinált self-stake és delegált stake állományt.
Ez a korlátozás megakadályozza a túlzott stake-koncentrációt, valamint mérsékli egyetlen validator esetleges hibás működésének gazdasági következményeit.

Ezeket a korlátozásokat a protokoll a staking pallet szintjén érvényesíti, így validatori vagy delegatori műveletekkel nem kerülhetők meg. Az 5%-os felső korlát fontos rendszerszintű kockázatkezelési elem: biztosítja, hogy még egyetlen validator teljes kompromittálódása esetén is legfeljebb a hálózat gazdasági biztonságának korlátozott része sérülhessen.

Jutalmak és díjak (mechanikai szint)

A Mosaic gazdasági biztonsági modelljét két egymást kiegészítő ösztönzőáram erősíti: a konszenzusmunkáért fizetett protokollkibocsátás („expanzió”), valamint a felhasználók által erőforrás-felhasználásért és priorizációért fizetett tranzakciószintű díjak.



A tranzakciók mindegyike egy MOS-ban denominált díjkeretet határoz meg, amely a mért végrehajtási erőforrás-felhasználásból (gas), valamint egy opcionális tipből áll. Az alapdíjat a runtime determinisztikus módon számolja fel a végrehajtás pillanatában; a tip egy felhasználó által meghatározott prioritási díj, amely sürgősséget jelez abban az esetben, amikor a blokkhely korlátozottan áll rendelkezésre.

Az alapdíjak elosztását a protokollszint érvényesíti: az alapdíj (gas) 40%-a elégetésre (burn) kerül, 50%-a a blokk előállítójához (az aktív validatorhoz/collatorhoz, aki a blokkot létrehozza) kerül, 10%-a pedig az on-chain kincstárba. A borravaló (tip) teljes egészében — 100%-ban — a blokkgyártót illeti. A burn tranzakció-végrehajtás során történik, ezáltal csökkentve a tényleges forgalomban lévő tokenkínálatot. A treasurybe érkező bevételek a treasury accountban halmozódnak fel, és a Mosaic költségvetési- és burn-folyamatai szabályozzák őket, amelyeket a Tokenomika fejezet ismertet részletesen. Mivel az elosztási logikát maga a runtime érvényesíti, a díjelosztás transzparens, auditálható, és nem támaszkodik láncokon kívüli, off-chain megállapodásokra.

A validatorok így egy olyan bevételi struktúrával rendelkeznek, amely alapdíjakból, tipbevételekből és expanziós jutalmakból épül fel. A delegatorok a validator jutalékával csökkentett validatori bevételekből részesednek pro rata alapon, közvetlen kapcsolatot teremtve a tranzakciós átviteli teljesítmény, a blokkgyártás minősége és a hálózat hosszú távú biztonsága között.

Slashing, Chilling és biztonsági mechanizmusok

A slashing és a chilling a protokoll elsődleges biztonsági mechanizmusai, amelyek a validatorok megbízhatóságát biztosítják egy nagyméretű, rotálódó aktív készletben. A slashing on-chain gazdasági büntetést alkalmaz üzemszünet vagy protokollsértés esetén, míg a chilling eltávolítja a validator Permission NFT-jét a kiválasztásra jogosult poolból — önkéntes vagy automatikus módon — annak érdekében, hogy az ismétlődő hibák ne rontsák a hálózat teljesítményét.

Mi vált ki büntetést? (üzemszünetek és protokollsértések)
A Mosaic Chain két fő kategóriát különböztet meg: a rendelkezésre állási hibákat és a protokollsértéseket. Minden validatornak minden session során be kell küldenie egy „I’m online” szívverés-tranzakciót. Az aktív validatoroknak ezenfelül legalább egy blokkot is elő kell állítaniuk a kiválasztott session során. E követelmények nem teljesítése üzemszünetnek minősül, és slashing büntetést vonhat maga után. A protokollsértések közé olyan műveletek tartoznak, amelyek veszélyeztetik a konszenzus integritását — például érvénytelen blokkok előállítása vagy egyéb runtime-szabályok megsértése.

Mi kerül büntetésre? (validator stake + delegált stake)
A slashing a validator Permission NFT névleges értékére, valamint az adott validatorhoz delegált teljes stake-állományra alkalmazandó. Ez magában foglalja a Delegation NFT-k névleges értékét, valamint a staking szerződéseken keresztül delegált MOS tokeneket — és adott esetben más támogatott eszközöket is. A slashing célja az ösztönzők összehangolása: a validator közvetlen gazdasági veszteséget szenved, míg a delegator a támogatott validator kockázatával arányosan osztozik a veszteségen.

Jelenlegi slashing ráta és alkalmazási részletek.
Az alapértelmezett slashing ráta 0,1%, amely mainnet környezetben ideiglenesen 0,0001%-ra csökkentett értéken működik. A validator Permission NFT névleges értéke slashing hatálya alá esik. A Delegation NFT-k névleges értékei szintén slashingre kerülnek; egy adott szerződésen belül az NFT névleges értékének csökkentése először a legrégebben delegált Delegation NFT-re kerül alkalmazásra, majd innen halad tovább addig, amíg a teljes slashing összeg levonásra nem kerül.
Ez a sorrendiség biztosítja, hogy a később delegált NFT-k megőrizzék eredeti névleges értéküket, ezáltal potenciálisan fenntartva másodpiaci értéküket. A szerződés keretében delegált valamennyi eszköz ugyanazon slashing esemény hatálya alá tartozik.

Automatikus chilling működés és küszöbértékek.
Az első hibás működés slashing büntetést eredményez, azonban nem helyezi automatikusan chilled állapotba a validatort. Amennyiben a validator a következő aktív session során sikeresen blokkot állít elő, állapota visszaáll normál működésre.
Ha a validator közvetlenül az előző slashing eseményt követően ismét slashing büntetésben részesül, a protokoll automatikusan chilled állapotba helyezi a validatort, lehetőséget biztosítva az üzemeltető számára a konfigurációs vagy kapcsolódási problémák javítására, mielőtt újra belépne a kiválasztási poolba.

Slacking periódus és korai kilépési védelem delegatorok számára.
A protokoll 72 sessionből álló slacking periódust biztosít türelmi időként az átmeneti problémák kezelésére. Amennyiben a validator ezen időablakon belül nem áll vissza normál működésre, a delegatorok szabadon megszüntethetik staking szerződésüket az adott validatorral — vagyis megkerülhetik a fennmaradó zárolási periódust — annak érdekében, hogy stake-jüket egy megbízhatóbb validatorhoz delegálhassák át. Ezek a paraméterek a mainnet érettségének növekedésével várhatóan tovább fejlődnek. A csökkentett mainnet slashing ráta célja, hogy elkerülje az aránytalan veszteségeket a nagyléptékű onboarding és operatív finomhangolási időszak alatt, azzal az elvárással, hogy a slashing ráta később fokozatosan közelíthet az alapértelmezett értékhez, ahogy a validator készlet stabilizálódik.

Minimális staking mennyiség.
A globális minimális staking mennyiség 50 MOS, és ugyanez a minimum vonatkozik a további delegációkra — vagyis a top-up műveletekre — is. Ez a küszöbérték csökkenti az alacsony értékű („dust”) szerződésekből származó terhelést, miközben a delegáció továbbra is elérhető marad a kisebb tokenbirtokosok számára.

Protokollkiterjesztések és natív termékek

Az előző fejezetek a Mosaic Chain éles működésű gerinchálózatát ismertették: a konszenzust, a staking rendszert, a validator működést és az interoperabilitást. A jelen fejezet olyan protokollszintű funkciókat mutat be, amelyek a forkless runtime-frissítési mechanizmuson keresztül kerülnek bevezetésre. Minden funkció közvetlenül a meglévő on-chain primitívekre épül, és a jelenlegi protokoll képességeiben meglévő konkrét hiányosságokat kezeli. A funkciókat úgy tervezték, hogy egymástól függetlenül is telepíthetők legyenek, ugyanakkor architekturálisan kiegészítsék egymást, és kombinált működésük során még nagyobb funkcionalitást biztosítsanak.

On-chain validator reputációs rendszer (Mosaic Trust Score)

Probléma. A Mosaic Chainen a delegatorok jelenleg az Explorerben megjelenített nyers metrikák alapján választanak validatort: uptime százalék, jutalékráta, teljes stake-mennyiség és session-részvételi statisztikák alapján. Ezek a metrikák informatívak, ugyanakkor széttagoltak. Egy delegatornak két validator összehasonlításához több különböző időhorizonton kell manuálisan elemeznie az eltérő adatpontokat, miközben nem áll rendelkezésre szabványosított módszer az általános megbízhatóság értékelésére. Jelentős MOS-pozíciókat kezelő intézményi delegatorok számára ez a manuális értékelési folyamat nem skálázható. Egy natív, protokollszintű minőségi jelzés hiánya továbbá korlátozza a 6.2-es fejezetben ismertetett staking vault stratégiák működését is, amelyek automatizált delegációs döntésekhez géppel olvasható megbízhatósági bemenetet igényelnek.

Tervezési modell. A Mosaic Trust Score egy összetett, on-chain reputációs mutató, amelyet egy új Reputation Pallet számol ki, és első osztályú attribútumként tárol minden Validator NFT-n. A score egy 0 és 1 000 közötti egész szám, amely minden sessionhatárnál újraszámításra kerül az előző 672 session — megközelítőleg 28 nap — adatainak felhasználásával. Ez a gördülő időablak elegendően hosszú ahhoz, hogy kisimítsa az elszigetelt incidenseket, ugyanakkor elég rövid marad ahhoz, hogy tükrözze a közelmúltbeli viselkedésváltozásokat. Egy validator, amely hónapokon keresztül megbízhatóan működött, de az elmúlt két hét során romló teljesítményt mutatott, a jelenlegi időablakon belül a score fokozatos csökkenését fogja tapasztalni.

A score három súlyozott bemeneti kategóriából épül fel.
A blokkgyártási megbízhatóság (40%-os súly) azt méri, hogy a validator az aktív készletben eltöltött időszak alatt a számára kiosztott slotok hány százalékában állított elő sikeresen blokkot. A validator maximális pontszámot akkor kap ebben a komponensben, ha minden kiosztott blokkgyártási slotot teljesít; a kihagyott slotok arányosan csökkentik a score értékét.

A rendelkezésre állás és válaszkészség (35%-os súly) azt követi nyomon, hogy a validator node-ja elérhető és megfelelően szinkronizált állapotban volt-e a sessionhatárok idején, a peer-to-peer egészségmonitorozási réteg jelentései alapján. Ez a komponens olyan kapcsolódási hibákat rögzít, amelyek nem feltétlenül eredményeznek kihagyott blokkokat, ugyanakkor az infrastruktúra sérülékenységére utalnak.

A szabálysértési előzmények (25%-os súly) a validatorokat a gördülő időablakon belüli slashing előzményeik alapján büntetik. Minden slashing esemény csökkenő súlyú büntetést alkalmaz: a közelmúltbeli szabálysértések nagyobb súllyal számítanak, mint a régebbiek. A csökkenési függvény úgy került kalibrálásra, hogy egyetlen kisebb szabálysértés büntetési súlya körülbelül 336 session — vagyis két hét — elteltével megközelítőleg 50%-kal csökkenjen.

A számítás teljes egészében on-chain módon, a Reputation Pallet keretein belül történik, a már meglévő staking-, session- és slashing palletek által rögzített adatok felhasználásával. Nincs szükség off-chain oracle-ökre, indexer lekérdezésekre vagy külső adatforrásokra. A pallet a blokkgyártási rekordokat a session palletből olvassa ki, a rendelkezésre állási állapotokat a node-egészségügyi jelentési rendszerből, a szabálysértési rekordokat pedig a slashing palletből. Minden bemeneti adat normalizálásra kerül egy 0–1 000 közötti részpontszámmá, majd a fent meghatározott fix súlyozással kombinálódik a végső összesített score előállításához. A súlyok governance útján módosítható paraméterek, lehetővé téve a közösség számára, hogy a hálózat prioritásainak változásával eltérő hangsúlyt helyezzen a blokkgyártási megbízhatóságra, a rendelkezésre állásra vagy a szabálysértési előzményekre.

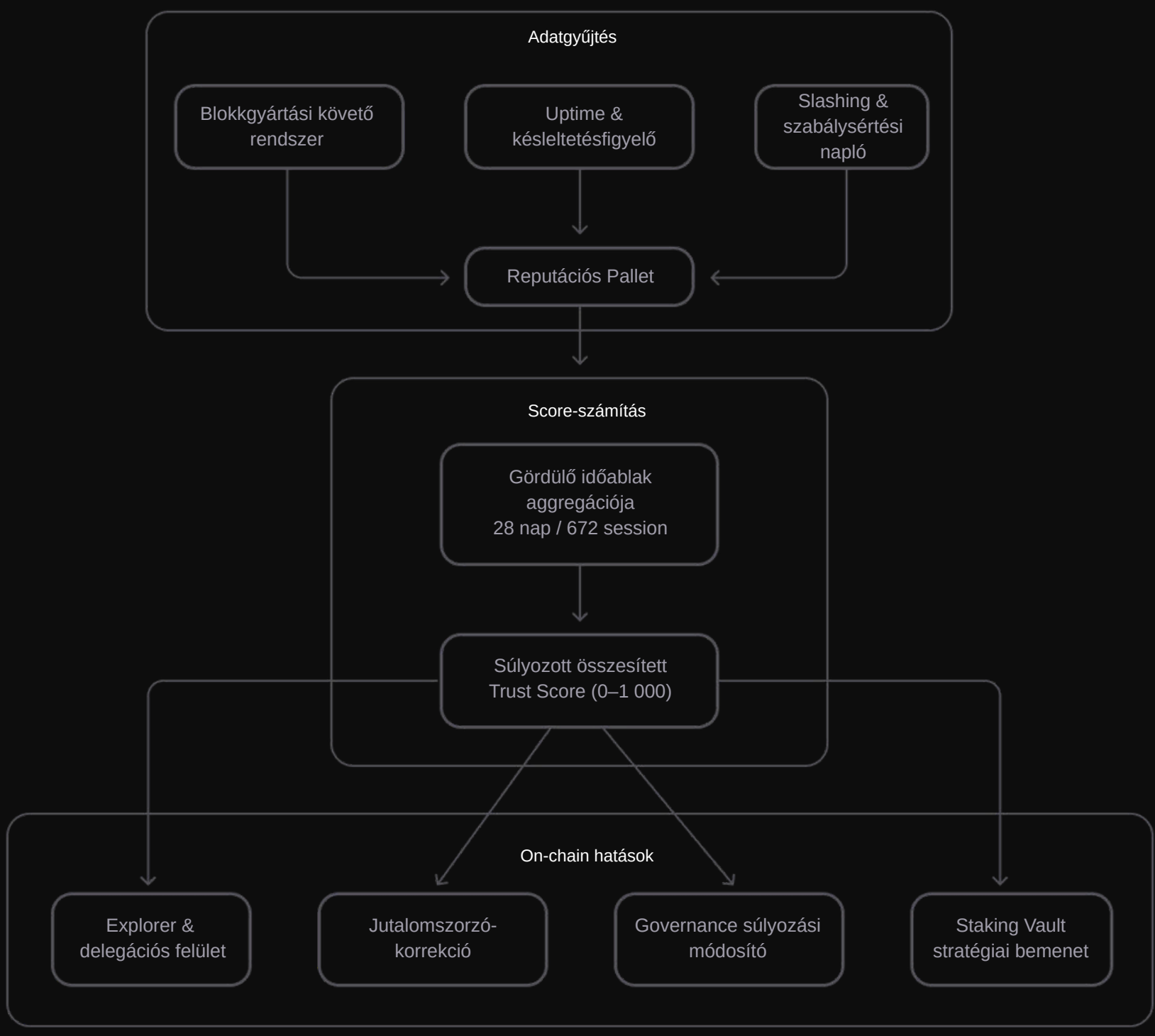
On-chain primitívek. A Reputation Pallet egy perzisztens adattárolási térképet (ValidatorTrustScores) vezet be, amely validator accountok szerint indexelve tárolja az aktuális összesített score-t és az egyes komponensek részpontszámait. Egy második adattárolási térkép (ReputationHistory) a gördülő időablak nyers bemeneti pillanatképeit őrzi meg, lehetővé téve a pallet számára a score-ok inkrementális frissítését a sessionhatárokon anélkül, hogy minden alkalommal teljes újraszámításra lenne szükség.
A pallet egy kizárólag olvasható RPC-metódust (reputation_trustScore) is biztosít, amelyen keresztül a külső kliensek bármely validator aktuális score-ját lekérdezhetik, továbbá minden sessionhatárnál kibocsát egy TrustScoreUpdated eseményt, amely tartalmazza a validator accountot és az új score értékét. A score ezenfelül módosítható NFT-attribútumként is tárolásra kerül a Validator NFT-n az NFT-Permission Pallet attribútuminterfészén keresztül, ezáltal ugyanúgy lekérdezhetővé válik, mint más NFT-tulajdonságok.

Gazdasági és biztonsági hatások. A Trust Score visszacsatolási kapcsolatot hoz létre a validator viselkedése és a gazdasági eredmények között. A kezdeti bevezetési szakaszban a score kizárólag információs célokat szolgál: megjelenik az Explorerben, valamint elérhető a staking vault szerződések számára, ugyanakkor közvetlenül nem módosítja a jutalomszámításokat.

Egy későbbi szakaszban — governance szavazáshoz kötve — a protokoll bevezethet egy jutalomszorzót, amely a validator jutalmakat egy szűk sávon belül (például 0,95×–1,05× között) módosítja a Trust Score alapján. Ez a szorzó szándékosan korlátozott tartományban működne annak érdekében, hogy megakadályozza a jutalmak túlzott koncentrációját a magas pontszámú validatorok között, amely veszélyeztetné a méltányos részvételi modellt. A score emellett természetes bemenetet biztosít a 6.2-es fejezetben ismertetett programozható staking vaultok számára is, lehetővé téve olyan automatizált stratégiák kialakítását, amelyek a stake-et következetesen megbízható üzemeltetők felé irányítják át.

Hibamódok és kockázatcsökkentés. Az elsődleges kockázat a score manipulálása. Egy validator megpróbálhatná mesterségesen javítani score-ját azzal, hogy stratégiai módon chilled állapotba kerül azokban az időszakokban, amikor gyenge teljesítményre számít, ezáltal kizárva a kedvezőtlen adatokat a gördülő időablakból. A pallet ezt úgy mérsékli, hogy az availability komponensben a túl gyakori chilling negatív jelzésként jelenik meg: azok a validatorok, amelyek rendszeresen chilled és aktív állapot között váltanak, alacsonyabb rendelkezésre állási részpontszámot kapnak. A gyakorisági küszöbérték úgy került kalibrálásra, hogy a legitim karbantartási időablakok — például gördülő periódusonként egy vagy két alkalom — ne járjanak büntetéssel.
Egy második kockázat az úgynevezett „rich get richer” dinamika kialakulása, amelyben a magas score-ral rendelkező validatorok aránytalanul nagy mennyiségű delegációt vonzanának, csökkentve a decentralizáció mértékét. A korlátozott jutalomszorzó és az egy validatorra vonatkozó 5%-os stake-korlát strukturálisan mérsékli ezt a koncentrációs hatást. Végül a 28 napos gördülő időablak azt eredményezi, hogy egy újonnan onboardolt validator kezdetben alacsony vagy alapértelmezett score-ral indul addig, amíg elegendő operatív előzményt nem halmoz fel. A pallet ezt úgy kezeli, hogy az új validatorok számára semleges, 500-as alapscore-t rendel nulla helyett, elkerülve ezzel a cold-start büntetést, miközben továbbra is teljesítményalapú működést követel meg a magasabb score eléréséhez.

Interoperabilitási kapcsolódási pontok. A Trust Score-ok a standard RPC interfészen, valamint NFT-attribútumként is elérhetők, így bármely on-chain vagy off-chain rendszer számára hozzáférhetők. Más parachaineken működő cross-chain alkalmazások XCM-en keresztül lekérdezhetik a Mosaic validatorok Trust Score értékeit annak érdekében, hogy megalapozott döntéseket hozzanak arról, mely Mosaic validatorokra támaszkodjanak cross-chain műveletek során. A score formátuma — vagyis a dokumentált komponenssúlyokkal rendelkező 0–1 000 közötti egész érték — úgy került kialakításra, hogy Mosaic-specifikus kontextus nélkül is értelmezhető maradjon, megkönnyítve a harmadik féltől származó dashboardokkal, analitikai platformokkal és cross-chain aggregátorokkal történő integrációt. A governance mechanizmus továbbra is teljes kontrollt gyakorol a komponenssúlyok, a gördülő időablak hosszának és a semleges alapscore meghatározása felett, biztosítva ezzel, hogy a reputációs rendszer a hálózat validator készletének növekedésével és az operatív mintázatok fejlődésével együtt újrakalibrálható maradjon. A jövőbeni iterációk további bemeneti jelzéseket is bevezethetnek — például földrajzi diverzitási mutatókat vagy kliensszoftver-diverzitási metrikákat —, feltéve, hogy ezek megbízható harmadik fél általi attestáció nélkül, tisztán on-chain módon verifikálhatók maradnak.



Programozható Staking Vaultok

Probléma. A Mosaic Chain jelenlegi staking modellje manuális és statikus működésű. A delegator egy Delegation NFT-t vagy MOS tokeneket bind állapotban kapcsol egy meghatározott validatorhoz, jutalmakat szerez, majd időszakosan újraértékeli a delegációját. Amennyiben a validator teljesítménye romlik, a delegatornak ezt észlelnie kell, döntést kell hoznia a beavatkozásról, el kell indítania az unbinding tranzakciót, ki kell várnia a minimális staking periódust vagy feloldási időszakot, majd újra kell delegálnia egy másik validatorhoz. Minden ilyen lépés aktív felügyeletet, on-chain tranzakciókat, valamint kapcsolódó díjakat és időzítési korlátozásokat igényel. Több validator között megosztott pozíciókkal rendelkező delegatorok esetében ez a fenntartási terhelés jelentőssé válik. A megszerzett jutalmak ráadásul tétlenül maradnak mindaddig, amíg a delegator manuálisan újra nem stake-eli azokat, így elmarad a kamatos újrabefektetés hatása.

Ennek eredményeként a Mosaic Chainen történő delegáció — a legtöbb proof-of-stake hálózathoz hasonlóan — a résztvevők többsége számára „beállít és elfelejt” jellegű tevékenységgé válik, ami nem optimális tőkeallokációhoz és gyengébb hálózati biztonsághoz vezet, amikor stake marad tartósan alulteljesítő validatoroknál.

Tervezési modell. A Programozható Staking Vaultok olyan on-chain smart contractok, amelyek MOS befizetéseket fogadnak delegatoroktól, majd előre definiált staking stratégiákat hajtanak végre automatikusan. Minden vault egy stratégiai konfiguráció alapján működik, amelyet a vault létrehozója — vagy a vault típusától függően maga a delegator — határoz meg a telepítés során. A vault szerződés kezeli a letétbe helyezett MOS tokeneket, a stratégiai szabályoknak megfelelően különböző validatorok között delegál, valamint a delegator nevében menedzseli a delegációs szerződések teljes életciklusát: binding, unbinding, jutalomgyűjtés, újradelegálás és kamatos újrabefektetés.

Három alapvető stratégiai primitív támogatott, amelyek egyetlen vaulton belül kombinálhatók is.

A rebalance primitív a vault teljes stake-állományát validatorok között osztja újra az egyes sessionhatárokon a célallokációs súlyok alapján. Amennyiben egy vault például három validator között 40/30/30 arányú elosztást céloz meg, és az aktuális allokáció eltér egy konfigurálható küszöbértéknél — alapértelmezetten 5%-nál — nagyobb mértékben, a vault unbinding műveletet indít a túlsúlyozott validatoroknál, majd újradelegálja a stake-et az alulsúlyozott pozíciókhoz.

A compound primitív automatikusan újra stake-eli a megszerzett jutalmakat a sessionhatárokon. Ahelyett, hogy a jutalmak külön egyenlegként halmozódnának fel, a vault arányosan hozzáadja őket a meglévő delegációs pozíciókhoz, ennek eredményeként idővel növelve az effektív hozamot. A compound művelet gyakorisága konfigurálható: történhet minden session során, meghatározott számú sessionenként, vagy akkor, amikor az összegyűlt jutalmak meghaladnak egy előre meghatározott küszöbértéket.

A migrate primitív figyeli a vault delegációs készletében szereplő validatorok Trust Score értékeit (6.1-es fejezet), és automatikusan stake-migrációt indít, amennyiben valamely validator score-ja egy konfigurálható minimumszint alá csökken. A migráció tiszteletben tartja a minimális staking periódust: az unbinding folyamat queue-ba kerül, majd a lehető legkorábbi engedélyezett időpontban végrehajtódik, ezt követően pedig a felszabadult stake a legmagasabb score-ral rendelkező, még nem használt jogosult validatorhoz kerül újradelegálásra.

On-chain primitívek. Egy új Vault Pallet kezeli a staking vaultok teljes életciklusát. A pallet bevezet egy VaultConfig adattárolási struktúrát, amely rögzíti a stratégiai paramétereket, a célzott validator készletet, az allokációs súlyokat, a Trust Score minimumküszöbét, a compound gyakoriságát és a rebalance küszöbértéket. Minden vault egy egyedi on-chain accounttal rendelkezik, amely a vault létrehozási tranzakciójából származik, és ez a vault account tartja a befizetett MOS tokeneket. A pallet extrinsic műveleteket biztosít vault létrehozására (create_vault), befizetésekre (deposit_to_vault), kifizetésekre (withdraw_from_vault), valamint stratégiai frissítésekre (update_strategy). A kifizetésekre olyan értesítési időszak vonatkozik, amely megegyezik a vault aktív delegációs szerződései közül a leghosszabb minimális staking periódussal, megakadályozva az azonnali likviditáskivonást, amely megzavarhatná az aktív delegációkat.

A sessionhatárokon a Vault Pallet on_session_end hookja kiértékeli az összes aktív vaultot a stratégiai paraméterek alapján. A pallet beolvassa a jelenlegi delegációs állapotot a Staking Palletből, a Trust Score értékeket a Reputation Palletből, valamint a függő jutalmakat a jutalomelosztási alrendszerből. Ezt követően kiszámítja a szükséges műveletsorozatot — rebinding, unbinding, compound és migrate műveleteket —, majd automatikusan végrehajtja azokat a sessionváltás során.

Ez a kötegelt végrehajtási modell biztosítja, hogy a vaultműveletek ne okozzanak állapotinkonzisztenciát a sessionök közben. Az egyes vaultokra jutó számítási terhelést az adott vault delegációs készletében szereplő validatorok maximális száma korlátozza, amely 20-ban van maximalizálva annak érdekében, hogy a sessionhatárokon jelentkező terhelés előre kiszámítható maradjon.

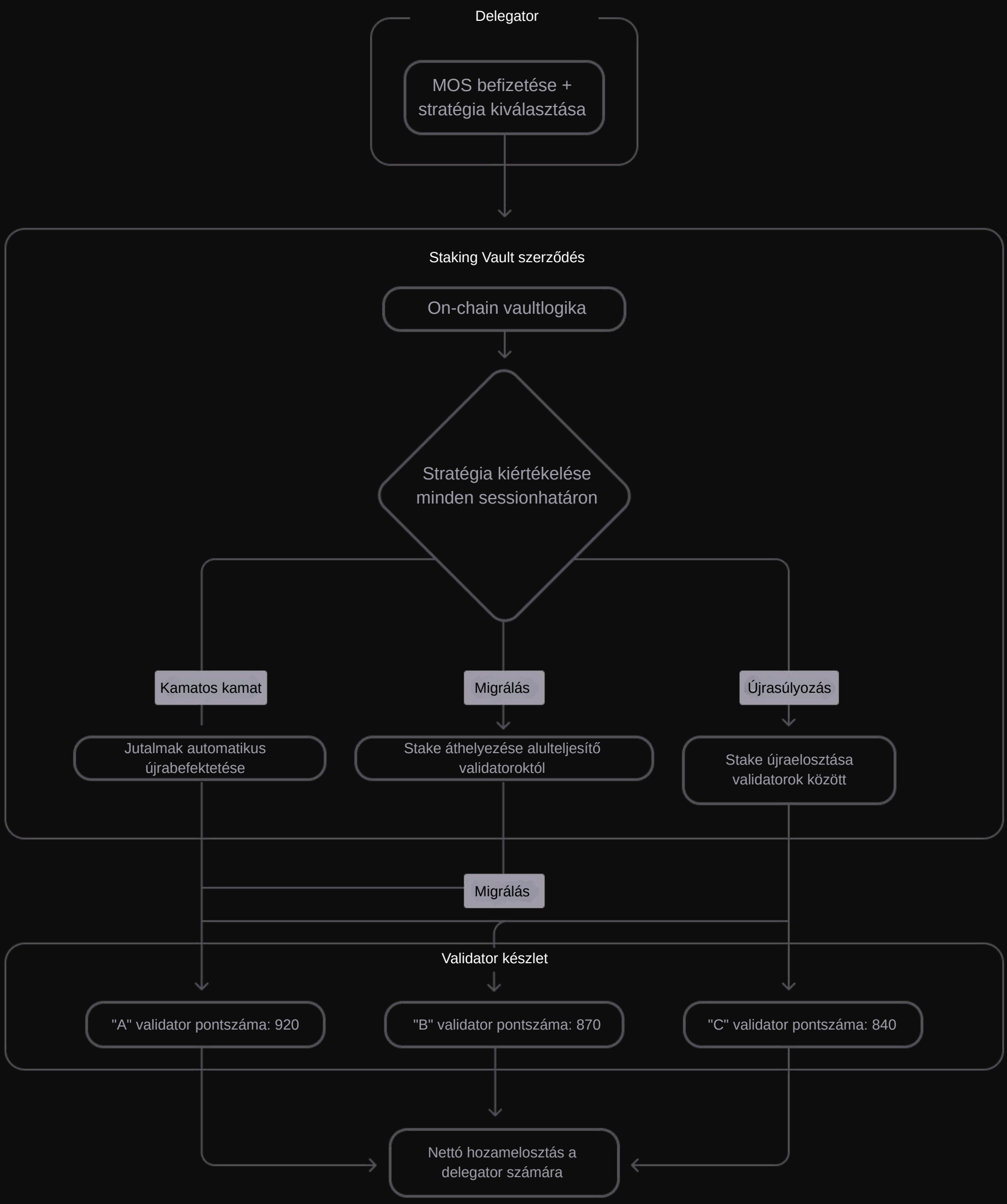
Gazdasági és biztonsági hatások. A staking vaultok két módon javítják a hálózat biztonságát. Először is az automatikus kamatos újrabefektetés révén idővel növelik az effektíven stakingelt tokenkínálatot anélkül, hogy ehhez a delegatorok aktív részvételére lenne szükség, ezáltal növelve a konszenzustámadások gazdasági költségét. Másodszor, az alulteljesítő validatoroktól történő automatikus stake-migráció révén közvetlen gazdasági következményt teremtenek a gyenge validatori működés számára, amely gyorsabban érvényesül, mint a delegatorok manuális reakciói. Azok a validatorok, amelyek magas Trust Score értéket tartanak fenn, megtartják a vaultokon keresztül delegált stake-et; amelyek elveszítik ezt a minőséget, stake-vesztést szenvednek el. Ez piacszerű nyomást gyakorol az operatív minőség fenntartására, kiegészítve a slashing rendszer protokollszintű büntetéseit.

A vaultmodell emellett az ökoszisztéma résztvevőinek egy új kategóriáját is bevezeti: a vaultstratégát. A stratégák meghatározott paraméterkonfigurációkkal hoznak létre vaultokat, majd azokat nyilvános befizetések számára elérhetővé teszik, miközben stratégiai díjat kapnak — vagyis a vault által generált jutalmak kis százalékát. Ez versenypiacot hoz létre a staking stratégiák minősége körül, ahol a stratégák ösztönözve vannak olyan allokációs szabályok kialakítására, amelyek maximalizálják a kockázattal korrigált hozamot. A stratégiai díjat a Vault Pallet on-chain módon érvényesíti, és még a jutalmak delegatorok közötti elosztása előtt levonásra kerül.

Hibamódok és kockázatcsökkentés. Az elsődleges kockázat az összehangolt migrációs viselkedés. Amennyiben több vault hasonló Trust Score küszöbértékeket használ, egy népszerű validator score-jának átmeneti csökkenése egyszerre nagyszámú unbinding műveletet válthat ki, olyan láncreakciót idézve elő, amely destabilizálhatja a validator stake-pozícióját, és potenciálisan továbbterjedhet a delegatorokra is.
A pallet ezt sessionenkénti migrációs korláttal kezeli: egyetlen session során legfeljebb a validator teljes delegált stake-állományának 10%-a migrálható ki, így az átrendeződés több session alatt, fokozatosan történik.
Egy második kockázatot a hibás stratégiai konfigurációk vagy contracthibák jelentenek. Mivel a vaultstratégiák automatikusan futnak minden sessionhatáron, egy rosszul konfigurált stratégia ismétlődően mozgatná a stake-et validatorok között, szükségtelen tranzakciós költségeket generálva. A pallet ezt minimális rebalance-időköz alkalmazásával kezeli — alapértelmezetten 24 session, vagyis megközelítőleg egy nap —, valamint egy értékelési ciklusonként meghatározott maximális churn-rátával, amely korlátozza ezt a viselkedést.
A vaultonkénti 20 validatoros felső korlát tovább szűkíti az egyetlen vault sessionhatár-logikájához kapcsolódó számítási felületet.

Interoperabilitási kapcsolódási pontok. A staking vaultok kompozábilis módon integrálhatók a 6.3-as fejezetben ismertetett yield routing funkcióval. Egy vault konfigurálható úgy, hogy a compound jutalmak egy részét a Yield Routeren keresztül irányítsa tovább ahelyett, hogy teljes egészében újra stake-elné őket, lehetővé téve olyan vaultok létrehozását, amelyek a staking hozamot cross-chain DeFi stratégiákkal kombinálják.
A vaultállapot — beleértve a teljes befizetési állományt, az aktuális allokációkat és a történelmi teljesítményt — lekérdezhető a standard RPC interfészen keresztül, lehetővé téve harmadik féltől származó portfóliókövető és analitikai platformok számára, hogy a vaultpozíciókat közvetlen stakingpozíciók mellett jelenítsék meg.

Mosaic Chain



Cross-chain hozamirányítás XCM-en keresztül (Mosaic Yield Bridge)

Probléma. A MOS stakelők jelenleg egy bináris döntési helyzettel szembesülnek: vagy staking jutalmakért zárolják tokenjeiket, vagy likviden tartják azokat más parachaineken elérhető DeFi-részvétel céljából. Ez a tőkehatékonysági probléma általánosan jelen van a proof-of-stake hálózatokban. A stakelt tokenek biztosítják a hálózat biztonságát, ugyanakkor nem tudnak egyidejűleg hozamot termelni hitelezési protokollokban, likviditási poolokban vagy más DeFi primitívekben olyan parachaineken, mint az Acala, Moonbeam vagy Astar. A liquid staking derivatívák (LSD-k) részben kezelik ezt a problémát, azonban új ellenoldali kockázatokat vezetnek be, külső protokollokba vetett bizalmat igényelnek, valamint összetett árfolyam-eltérési dinamikát hoznak létre a derivatíva és az alapul szolgáló eszköz között. Egy olyan pénzügyi fókuszú lánc számára, amely az átlátható gazdasági biztonságot és az on-chain transzparenciát helyezi előtérbe, a hozamok külső, harmadik fél által működtetett LSD-protokollokon keresztüli irányítása ellentmond a tervezési filozófiának.

Tervezési modell. A Mosaic Yield Bridge egy protokollszintű funkció, amely lehetővé teszi a stakelők számára, hogy stakingpozíciójuk konfigurálható részét más Polkadot parachaineken elérhető, ellenőrzött DeFi hozamlehetőségekbe irányítsák át XCM használatával, trustless cross-chain kommunikáción keresztül.
A mechanizmus nem oldja fel a stakingelt tokeneket a hagyományos értelemben. Ehelyett a Yield Router Pallet egy szintetikus receipt tokent (yMOS) bocsát ki, amely az átirányított részt reprezentálja, miközben az alapul szolgáló MOS továbbra is a hálózat gazdasági biztonsági költségvetésének részeként marad elszámolva.
A receipt token nem átruházható és nem kompozábilis — kizárólag számviteli artefaktumként létezik a Yield Router Palleten belül, nem pedig kereskedhető derivatívaként.
A routing folyamat a következőképpen működik. Egy aktív stakingpozícióval rendelkező stakelő meghatározza, hogy stakingelt MOS-állományának mekkora részét kívánja átirányítani — a protokoll által kikényszerített, legfeljebb 30%-os felső korlát figyelembevételével —, majd kiválaszt egy célzott hozamlehetőséget a governance által fenntartott whitelistből.
A Yield Router Pallet ellenőrzi, hogy a stakelő fennmaradó, nem átirányított stake-je továbbra is meghaladja-e a minimális staking küszöböt. Ezt követően kibocsátja a megfelelő yMOS receipt tokent, majd XCM-transzfert indít a meghatározott MOS-mennyiséggel a cél parachain irányába.
A cél parachainen az átutalt MOS a kiválasztott DeFi protokollba kerül befizetésre — például egy Moonbeam-en működő lending poolba, egy Acala likviditási poolba vagy egy Astar staking dApp szerződésbe — egy előre konfigurált XCM-programon keresztül, amely kódolt formában tartalmazza a befizetési utasításokat.

Amikor a stakelő vissza kívánja hívni az átirányított tőkét, vagy a hozamlehetőség futamideje lejár, a Yield Router XCM-en keresztül withdrawal műveletet kezdeményez. A cél parachain visszaküldi a tőkét és a felhalmozott hozamot a Mosaic Chainre. A Yield Router Pallet ezt követően burneli a yMOS receipt tokent, jóváírja a visszaérkezett MOS-t — az eredeti tőkét és a hozamot — a stakelő accountján, majd a stakelő dönthet: a hozam újrastakeléséről, másik opportunitybe történő átirányításról vagy a funds kivonásáról.
A stakelő eredeti stakingpozíciója a teljes folyamat során érintetlen marad; a receipt token kizárólag annak biztosítására szolgál, hogy a stakingelt egyenleg biztonsági célból ne legyen kétszer elszámolható.

On-chain primitívek. A Yield Router Pallet több új adattárolási struktúrát vezet be.
A YieldOpportunityRegistry tárolja a governance által jóváhagyott cél parachainek, protokollok és XCM-programok whitelistjét, valamint az ezekhez tartozó kockázati tier-besorolást és maximális routingkapacitást.

A RoutedPositions adattérkép minden stakelő aktív routingpozícióját nyilvántartja:
az átirányított összeget, a célzott opportunityt, a yMOS receipt azonosítót, valamint a routing időbélyegét.

A PendingSettlements queue kezeli a visszahívási folyamat során éppen folyamatban lévő XCM-transzfereket. A pallet extrinsic műveleteket biztosít: routing műveletekhez (route_to_yield), visszahíváshoz (recall_from_yield), valamint vészhelyzeti visszahíváshoz (emergency_recall).

Emellett kizárólag governance által használható extrinsic műveleteket is tartalmaz a hozamlehetőségek whitelistjének kezelésére (add_yield_opportunity, remove_yield_opportunity, update_risk_tier).

Gazdasági és biztonsági hatások. A Yield Bridge növeli a MOS stakelők effektív tőkehatékonyságát anélkül, hogy csökkentené a hálózat biztonságát. Mivel az átirányítható MOS mennyisége legfeljebb a stakelő pozíciójának 30%-a lehet, a stakingelt MOS legalább 70%-a minden időpillanatban teljes mértékben a konszenzusbiztonságot támogatja.
A yMOS receipt token nem átruházható jellege megakadályozza a liquid staking tokeneket gyakran érintő derivatívadinamikák kialakulását: nincs másodpiaca a yMOS tokennek, nincs depegkockázat és nincs tőkeáttételes útvonal.

A 30%-os felső korlát governance által módosítható paraméter, amely szigorítható, ha a hálózat biztonsági költségvetésének erősítésére van szükség, vagy lazítható, amennyiben a teljes stakingállomány növekszik.

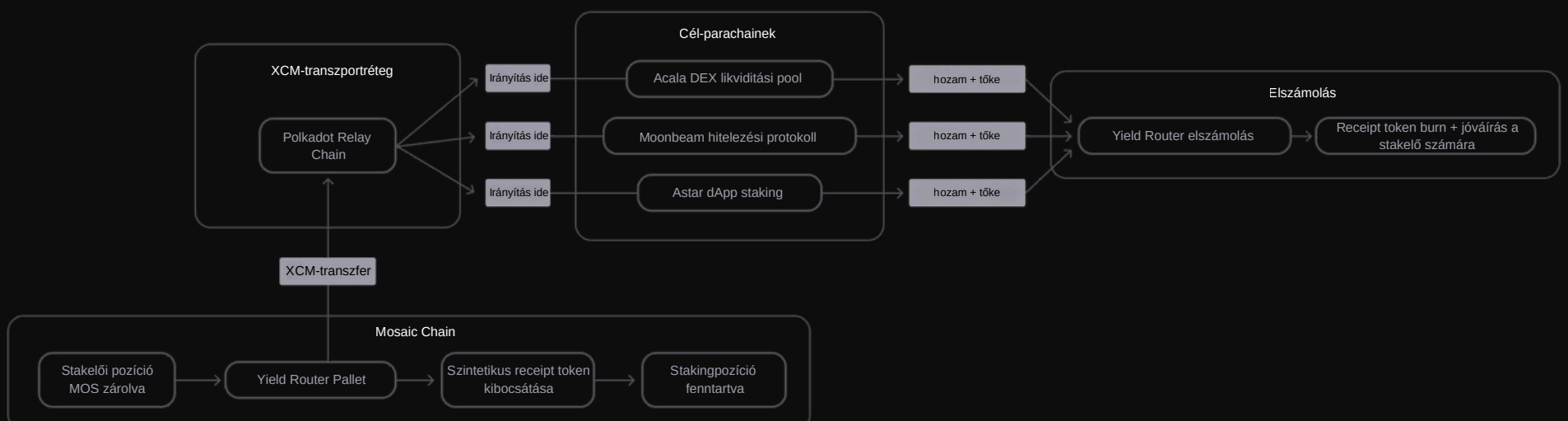
A tágabb Polkadot ökoszisztéma szempontjából a Yield Bridge tőkeáramlási csatornát hoz létre a Mosaic Chain stakingbázisa és más parachaineken működő DeFi protokollok között. Ez növeli a célprotokollok teljes zárolt likviditását (TVL), miközben a MOS stakelők számára diverzifikált hozamforrásokat biztosít.
A díjstruktúra a protokollszintű díjak egy kis részét — alapértelmezetten a hozam 2%-át — a Mosaic treasurybe irányítja, új bevételi forrást teremtve, amely a cross-chain DeFi aktivitással együtt növekszik.

Hibaüzemmódok és kockázatkezelés. A legsúlyosabb kockázat a cél parachainen futó smart contract hibája. Amennyiben az a DeFi protokoll, amelybe a MOS befizetésre kerül, exploit áldozatává válik, az átirányított funds elveszhetnek. Az elsődleges védelmi mechanizmust a governance által kezelt whitelist jelenti. Csak olyan protokollok kerülhetnek fel a whitelistre, amelyek: formális biztonsági auditon estek át, legalább egy minimális ideig — alapértelmezetten hat hónapig — incidensmentesen működtek, valamint megfelelő biztosítási vagy biztonsági modullal rendelkeznek.
Minden whitelistelt opportunity egy kockázati tier-besorolást kap (alacsony, közepes vagy magas), amely meghatározza a maximális routingkapacitását. A magas kockázatú opportunityk összességében kevesebb átirányított MOS-t fogadhatnak.
Az emergency_recall extrinsic governance által aktiválható mechanizmust biztosít arra az esetre, ha sérülékenységet észlelnek: ilyenkor a rendszer kényszerített módon visszavonhatja a MOS-t a célprotokollból, megkerülve a normál visszahívási folyamatot.
Az XCM üzenetküldési késedelmek vagy hibák kezelését a PendingSettlements queue végzi, amely konfigurálható időközönként újrapróbálja a sikertelen transzfereket, majd governance szintű figyelmeztetést generál, ha a retry-kimerülési küszöb elérésre kerül.

Interoperabilitási kapcsolódási pontok. Ez a funkció eredendően cross-chain működésű, és teljes mértékben a Polkadot XCM infrastruktúrájára épül. A Yield Router minden whitelistelt opportunityhez olyan XCM-programokat hoz létre, amelyek kódolt formában tartalmazzák a befizetési, withdrawal és vészhelyzeti visszahívási logikát, kifejezetten az adott célprotokoll működéséhez igazítva. Ezek az XCM-programok on-chain módon kerülnek tárolásra, és auditálhatók.
Ahogy a Polkadot XCM képességei fejlődnek — például az XCMv4 hibakezelési és díjbecslési fejlesztéseivel —, a Yield Router XCM-programjai governance útján frissíthetők anélkül, hogy a core pallet logikáját módosítani kellene.
A Staking Vaultokkal (6.2-es fejezet) való integráció támogatja az automatizált hozamirányítást a vaultok compound stratégiájának részeként: egy vault konfigurálható úgy, hogy a compound jutalmak meghatározott részét a Yield Bridge-en keresztül irányítsa tovább ahelyett, hogy teljes egészében újra stake-elné azokat, ennek révén a vault befizetői kombinált staking- és DeFi-hozamkitettséget kapnak.

A jelen fejezetben ismertetett három funkció — vagyis a vaultstratégiákat vezérlő Trust Score rendszer, a delegációt és compound műveleteket automatizáló vaultok, valamint a tétlen tőke cross-chain irányítását biztosító Yield Bridge — együtt egy vertikálisan integrált staking infrastruktúrát alkot, amelyet külső, harmadik fél által működtetett protokollokkal nehéz reprodukálni.

Bár minden funkció önállóan is működőképes, együttes hatásuk egy olyan, a Mosaic Chain protokolljába natívan integrált tőkemenedzsment-rendszert hoz létre, amely jelentősen növeli a staking infrastruktúra hatékonyságát és automatizálhatóságát.



Tokenomika (MOS)

A MOS felhasználási területei (MOS utility)

A **Mosaic Coin** (MOS) a Mosaic Chain hálózat natív tokenje, amely alapvető értékhordozóként szolgál valamennyi protokollszintű művelet során. A MOS öt jól elkülöníthető funkcionális szerepet tölt be az ökoszisztémán belül.

Tranzakciós díjak. Valamennyi on-chain művelet — beleértve az átutalásokat, staking tranzakciókat, governance műveleteket és smart contract interakciókat — MOS felhasználását igényli a számítási és adattárolási költségek fedezésére. A díjmodell biztosítja, hogy a hálózati erőforrások hatékony módon kerüljenek allokálásra, valamint hogy a spam- és szolgáltatásmegtagadási (DoS) támadások gazdasági költséggel járjanak.

Staking és biztonság. A MOS tokenek stake-ként kerülnek zárolásra a validatorok által — NFT névleges értékeken keresztül, — valamint a delegatorok által — Delegation NFT-k és staking szerződések használatával — a hálózat biztonságának biztosítása érdekében. A stakingelt MOS teljes értéke alkotja a hálózat gazdasági biztonsági költségvetését, amely meghatározza a konszenzusmechanizmus megtámadásának gazdasági költségét.

Jutalmak. A blokkjutalmak és a tranzakciós díjak egy része a validatorok és delegatoraik között kerül szétosztásra a hálózat biztonságának fenntartásáért cserébe. A jutalmazási mechanizmus ösztönzi a tisztességes részvételt, és szankcionálja azokat a működési mintázatokat, amelyek veszélyeztetik a hálózat megbízhatóságát.

Governance. A tokenalapú, súlyozott on-chain governance egy jövőbeni runtime-frissítés keretében kerül bevezetésre. Jelenleg a MOS proposal deposit mechanizmusként működik, miközben a protokollal és az alapokkal kapcsolatos döntéseket kijelölt on-chain bizottságok (collective-ek) hozzák meg, amelyek kétharmados (2/3) szupermajoritással hagyják jóvá a javaslatokat.

Treasury. A blokkjutalmak és tranzakciós díjak egy része az on-chain treasurybe áramlik, amely az ökoszisztéma fejlesztését, marketingtevékenységeket, biztonsági auditokat és egyéb, governance által jóváhagyott kezdeményezéseket finanszíroz.

Kínálat és denominációk

A MOS maximális kínálata rögzített: összesen 2 000 000 000 token. Ezt a határértéket a protokollszint érvényesíti, és kizárólag governance által jóváhagyott runtime-frissítéssel módosítható. A MOS legkisebb oszthatatlan egysége (a Bitcoin satoshijához vagy az Ethereum wei egységéhez hasonlóan) a tile, ahol: 1 MOS = 10^18 tile. Valamennyi on-chain egyenleg, stakingmennyiség és díjszámítás tile-szintű pontossággal működik.

Definíciók (kínálati fogalmak)
Az egyértelműség érdekében a Mosaic Chain az alábbi kínálati definíciókat használja:

- **Pretokenek:** onboarding folyamat során kiosztott tokenek (időalapú vesting mellett).
- **Premined:** az induláskor kibocsátott tokenek a pretokenek nélkül.
- **Total supply:** valamennyi kibocsátott token összessége — függetlenül attól, hogy zárolt vagy feloldott állapotban vannak-e.

A „circulating supply” a már kibocsátott, de nem zárolt tokenek mennyiségét jelenti, a staking incentive poolt nem számítva. A „max supply” az elméleti maximális tokenkínálatot jelöli.
A Token Generation Event (TGE) azt a sessiont jelenti, amelytől kezdve a blokkjutalmak felhalmozása megkezdődik.

Hálózati időkonstansok. A Mosaic Chain célzott blokkideje 6 másodperc, egyórás sessionekbe szervezve. E feltételek mellett egy on-chain év 5 259 600 blokkot jelent.

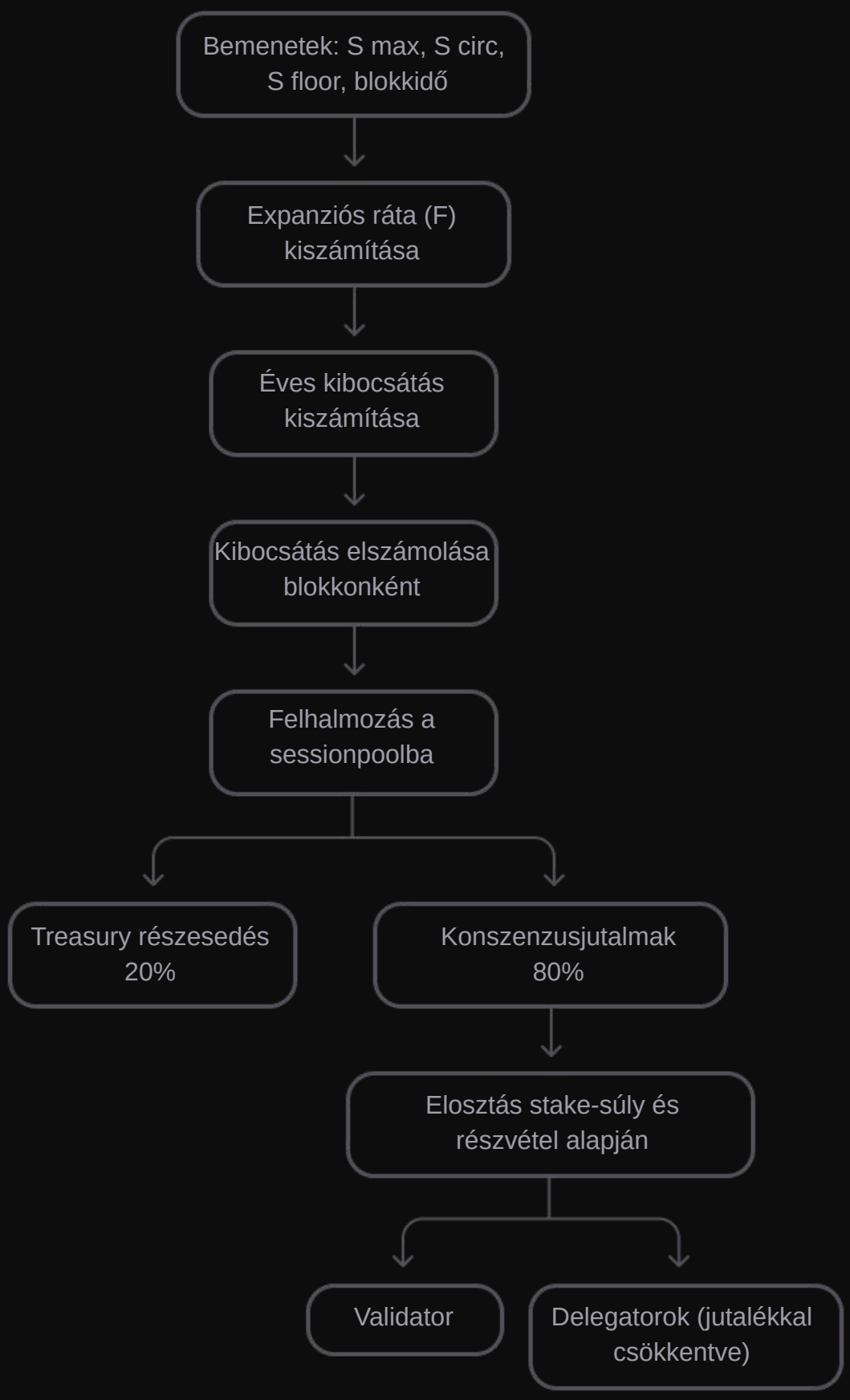
Előre kibocsátott (premined) token-allokáció: Az induláskor kibocsátott (mintelt) tokenek (a pretokeneket nem számítva) az alábbi kategóriák között kerülnek felosztásra:

Cél	Mennyiség (MOS)
Staking ösztönző (Staking Incentive)	~500 000 000
Pretokenek	~100 000 000
Kincstár (Treasury)	10 000 000
Fejlesztés és Innováció	24 000 000
Pénzügyi és likviditási alapok	20 000 000
Marketing és közösségépítés	20 000 000
Csapat és tanácsadói támogatás	8 000 000
Biztonság és megfelelőség	4 000 000
Oktatás és dokumentáció	2 400 000

A teljes tokenkínálat minden időpillanatban magában foglalja az összes kibocsátott tokent — függetlenül attól, hogy azok zárolt, vesting alatt álló, stakingelt vagy szabadon forgalomban lévő állapotban vannak-e. A circulating supply nem tartalmazza a vesting ütemezésekben zárolt tokeneket, valamint a staking incentive poolt sem. Ezek a megkülönböztetések fontosak a hálózat gazdasági dinamikájának és a piacon ténylegesen rendelkezésre álló likviditás pontos értékeléséhez.

Kibocsátási és jutalmazási modell

A Mosaic Chain korlátozott maximális kínálatra épülő kibocsátási modellt alkalmaz, amely kezdetben inflációs szakaszban működik, majd a circulating supply maximális kínálathoz történő közelítésével fokozatosan aszimptotikusan nullához tartó kibocsátási rátára áll át.



6 másodperces célzott blokkidő (egy on-chain év alatt 5 259 600 blokk) mellett a protokoll az expanziót egy átlagos blokkjutalom-függvényként határozza meg. Legyen a max_supply a maximális MOS-kínálat, a circulating_supply pedig a forgalomban lévő tokenmennyiség (100 000 000 MOS minimumértékkel).

Az expanziós faktor definíciója:

F = 12,5 × sqrt((max_supply − max(circulating_supply, 100 000 000)) / (max_supply − 100 000 000))

Mivel a jutalmak minden session során az aktuálisan aktív validatorkészlet alapján kerülnek kiosztásra, a protokoll sessionkorrekciót alkalmaz, amely figyelembe veszi a kötött validatorok számát (B) és az aktív validatorok számát (A). Egy adott session korrigált jutalmazási rátája arányos a (B × F / A) értékkel, miközben a teljes sessionkifizetés a session hosszával (L) skálázódik. Minden session végén az aktív validatorok jutalmat kapnak az előző session során előállított blokkok után.

Az egyes sessionek kibocsátási pooljából a protokoll egy fix részt — T = 20% — a treasury számára különít el. A fennmaradó 80% konszenzusjutalomként kerül kiosztásra az aktív validatorkészlet számára.
A konszenzusjutalmak az aktív validatorok között az effektív kötött stake és a részvételi arány alapján kerülnek szétosztásra (például blokk-előállítás és rendelkezésre állás alapján). Ezt követően minden validator a saját jutalmait stake-súly alapján továbbosztja delegatorai között, a validator által meghatározott jutalék levonása után.
Ahogy az expanzió idővel csökken, a biztonság finanszírozása fokozatosan a díjalapú bevételi modell és a protokollszintű hasznosság irányába tolódik el, csökkentve a tokenhígulástól való függést, miközben a hálózat növekedési szakaszában továbbra is kiszámítható ösztönzőket biztosít.

Vesting és Vesting-to-Freeze

Pretokenek és vesting. A pretokenek onboarding folyamat részeként kerülnek kiosztásra, és nem azonnal válnak hozzáférhetővé, hanem egy vesting ütemezés szerint, időben elosztva kerülnek felszabadításra. A vesting periódus hossza az allokált mennyiségtől függ, és jellemzően körülbelül 2–4 év között mozog, egy olyan formula alapján meghatározva, amely még az onboarding megkezdése előtt kerül rögzítésre on-chain módon.

Vesting-to-Freeze (stakingelhető zárolt eszközök). A Mosaic Chain lehetőséget biztosít arra, hogy a még vesting alatt álló pretokenek zárolt MOS tokenekké kerüljenek átalakításra, amelyek az eredeti vesting ütemezés végéig továbbra is zárolva maradnak. Ezek a zárolt tokenek szabadon stakingelhetők, azonban a vesting periódus lezárultáig nem használhatók átutalásokra vagy egyéb célokra. Ez a mechanizmus biztosítja a résztvevők számára, hogy hozzájáruljanak a hálózat biztonságához és staking jutalmakat szerezzenek anélkül, hogy ezzel növelnék a circulating supply mennyiségét.

Staking Incentive Pool

A Mosaic Chain staking incentive poolt alkalmaz a hosszú távú staking magatartás ösztönzésére. A Token Generation Event (TGE) után a staking incentive jutalmak várhatóan évente egyszer válnak lehívhatóvá, a negyedik évtől a nyolcadik év végéig.
Minden egyes kifizetés során a staking incentive pool előre meghatározott része kerül kiosztásra a jogosult stakelők között egy olyan score alapján, amely a stake méretével és a stakingben eltöltött idővel arányosan növekszik.
A lehívott incentive jutalmak egyéves vesting ütemezés mellett kerülnek jóváírásra, és stakingelhető zárolt eszközökké (stakable frozen assets) alakíthatók.

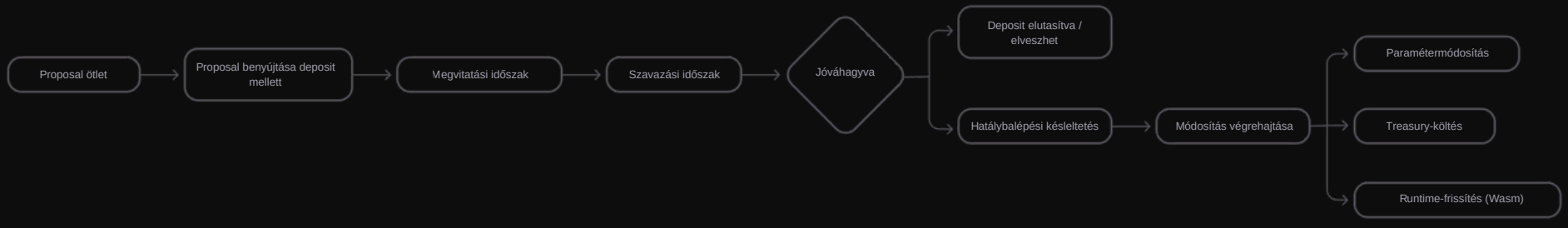
Mivel az incentiveelosztás paraméterei idővel változhatnak, az egyes kifizetések pontos időzítése és összege governance-paraméterezett módon kerül meghatározásra.

Governance és frissítések

Az irányítás hatóköre

A Mosaic Chain governance rendszere jelenleg bizottságalapú működésre épül. A MOS tulajdonosai jelenleg nem vesznek részt közvetlen tokenalapú on-chain szavazásban a protokollparaméterek, treasury-költések vagy frissítések szabályozására. Ehelyett a MOS proposal deposit mechanizmusként szolgál, miközben a javaslatokat kijelölt on-chain bizottságok (collective-ek) értékelik és hagyják jóvá. A token-súlyozott governance egy jövőbeni runtime-frissítés részeként kerül bevezetésre (a roadmapben Governance 1.0 néven hivatkozva). A dokumentum készítésének időpontjában a nyílt, token-súlyozott governance még nem érhető el a Mosaic Chainen.

A paramétermódosítások olyan protokollkonstansok változtatásait foglalják magukban, mint: a sessionhossz, a minimális stakingösszeg, a jutalékráták, a slashing százalékok, valamint a validator-kiválasztási célértékek.Ezek a paraméterek közvetlenül befolyásolják a hálózat működését és gazdasági modelljét. A jelenlegi modell szerint a paramétermódosítások MOS deposit mellett proposal formájában kerülnek benyújtásra, majd az illetékes bizottság kétharmados (2/3) szupermajoritással hagyja jóvá őket a hatálybalépés előtt.



A treasury- és alapkezelési mechanizmus szabályozza a blokkjutalmakból és tranzakciós díjakból befolyó források felhasználását. A finanszírozási javaslatoknak tartalmazniuk kell: az igényelt összeget, a tervezett felhasználási célt, valamint egy MOS depositot.
A Mosaic treasury rendszere dedikált alapokat és egy külön alapkezelő bizottságot is támogat; minden egyes alapot saját governance bizottsága irányít, nem pedig tokenalapú szavazás.
Egy proposal akkor kerül elfogadásra, amikor az illetékes governance bizottság eléri a szükséges kétharmados (2/3) szupermajoritást. Ezt követően az igényelt összeg a jelenlegi spending periódus végén válik lehívhatóvá (28 nap / 672 session).
A treasury- és alapegyenlegek aktív felhasználásának ösztönzésére az inaktív egyenlegek konfigurálható ütemezés szerint periodikus burn mechanizmus alá eshetnek.

A runtime-frissítések biztosítják, hogy a governance folyamat új vagy módosított on-chain logikát telepítsen. Mivel a runtime Wasm bytecode formájában on-chain tárolódik, egy sikeres governance szavazás által jóváhagyott runtime-frissítés automatikusan életbe lép egy meghatározott blokkmagasságnál.
Ez a mechanizmus biztosítja, hogy a protokoll új képességekkel bővüljön, hibákat javítson és alkalmazkodjon a változó követelményekhez anélkül, hogy hard forkok koordinációs költségeit vagy közösségmegosztó kockázatait vállalnia kellene.

A governance modell többfázisú proposal-életciklust alkalmaz, amely magában foglalja: a deposit melletti benyújtást, a felülvizsgálati időszakot, a kétharmados (2/3) szupermajoritást igénylő bizottsági szavazást, valamint a hatálybalépési időszakot, amely pufferidőt biztosít a jóváhagyás és az implementáció között. Ez a többlépcsős folyamat egyensúlyt teremt a gyors reagálóképesség és az elővigyázatosság között, biztosítva, hogy a jelentős protokollmódosítások megfelelő ellenőrzés mellett történjenek meg, miközben a hálózat fokozatosan áttér a jövőbeni token-súlyozott governance modellre.

Forkless frissítések

A Substrate-ből örökölt forkless frissítési mechanizmus a Mosaic Chain egyik legfontosabb architekturális tulajdonsága egy pénzügyi fókuszú blockchain esetében. A hagyományos blockchain-frissítések hard forkokon keresztül történnek, amelyek jelentős off-chain koordinációt igényelnek: minden validatornak le kell töltenie és telepítenie kell az új szoftvert egy szűk időablakon belül, és azok a validatorok, amelyek nem frissítenek időben, fennakadhatnak egy inkompatibilis chain fork állapotán. Ez a folyamat lassú, működési szempontból kockázatos, és fragmentálhatja a hálózati közösséget.

A Mosaic Chain forkless frissítései ettől eltérő módon működnek. A blockchain runtime-logikája WebAssembly bytecode formájában kerül tárolásra a chain state-en belül. Amikor egy runtime-frissítést a hálózat governance jogosultsággal rendelkező szerve (jelenleg bizottságalapú governance) jóváhagy, az új Wasm bináris on-chain tranzakcióként kerül benyújtásra. Miután ezt a módosítást a relay chain finalizálta, és egy rövid biztonsági időablak eltelt, valamennyi validator automatikusan az új runtime-ot kezdi futtatni, mivel a konszenzusszabályok előírják, hogy a validatoroknak mindig a legfrissebb on-chain runtime-verziót kell végrehajtaniuk. Nincs szükség szoftverletöltésre, manuális telepítésre vagy koordinált frissítési időablakra.

Ez a frissítési mechanizmus közvetlen hatással van a pénzügyi alkalmazások szempontjából kritikus biztonsági tulajdonságokra. Megszünteti az aszinkron validatorfrissítésekből eredő chain split kockázatát. Biztosítja, hogy minden résztvevő mindig ugyanazokat a protokollszabályokat hajtsa végre. Emellett megvalósítja a kritikus problémák gyors kezelését is, mivel a hibajavítások ugyanazon governance- és frissítési folyamaton keresztül telepíthetők anélkül, hogy meg kellene várni egy manuális frissítési ciklus lefutását a teljes validatorkészleten.

A Mosaic Chain konzervatív biztonsági megközelítést alkalmaz a frissítések kezelésében. A runtime-módosítások alapos tesztelésen mennek keresztül devnet környezetben, mielőtt mainnet proposal formájában benyújtásra kerülnének. A governance folyamat megvitatási és hatálybalépési időszakokat is tartalmaz, amelyek lehetőséget biztosítanak a közösség számára a javasolt módosítások értékelésére. A visszafelé kompatibilitás kiemelt prioritást élvez, és az állapotmigrációk (amennyiben szükségesek) a frissítési tranzakció részeként kerülnek végrehajtásra. Bár a teljes rollback nem automatizálható triviális módon, technikailag megvalósítható ugyanazon governance mechanizmuson keresztül abban az esetben, ha egy telepített frissítés problémásnak bizonyul.

Interoperabilitás

Kapcsolat a Polkadottal

A Mosaic Chain a Substrate keretrendszerre épül, és a Polkadot ökoszisztémán belül működik. A Polkadot egy Layer 0 blockchainként funkcionál, amely megosztott biztonságot és interoperabilitási infrastruktúrát biztosít az összekapcsolt Layer 1 láncok (parachainek) számára. A bridge-alapú interoperabilitási modellekkel szemben — ahol minden lánc saját biztonsági modellt tart fenn, és cross-chain kommunikáció során megbízható közvetítőkre támaszkodik — a Polkadot relay chain modellje alapvetően eltérő biztonsági architektúrát biztosít: a parachain blokkokat a Polkadot saját validatorkészlete validálja és finalizálja, ezáltal garantálva, hogy a cross-chain üzeneteket a teljes Polkadot hálózat gazdasági biztonsága fedezi.

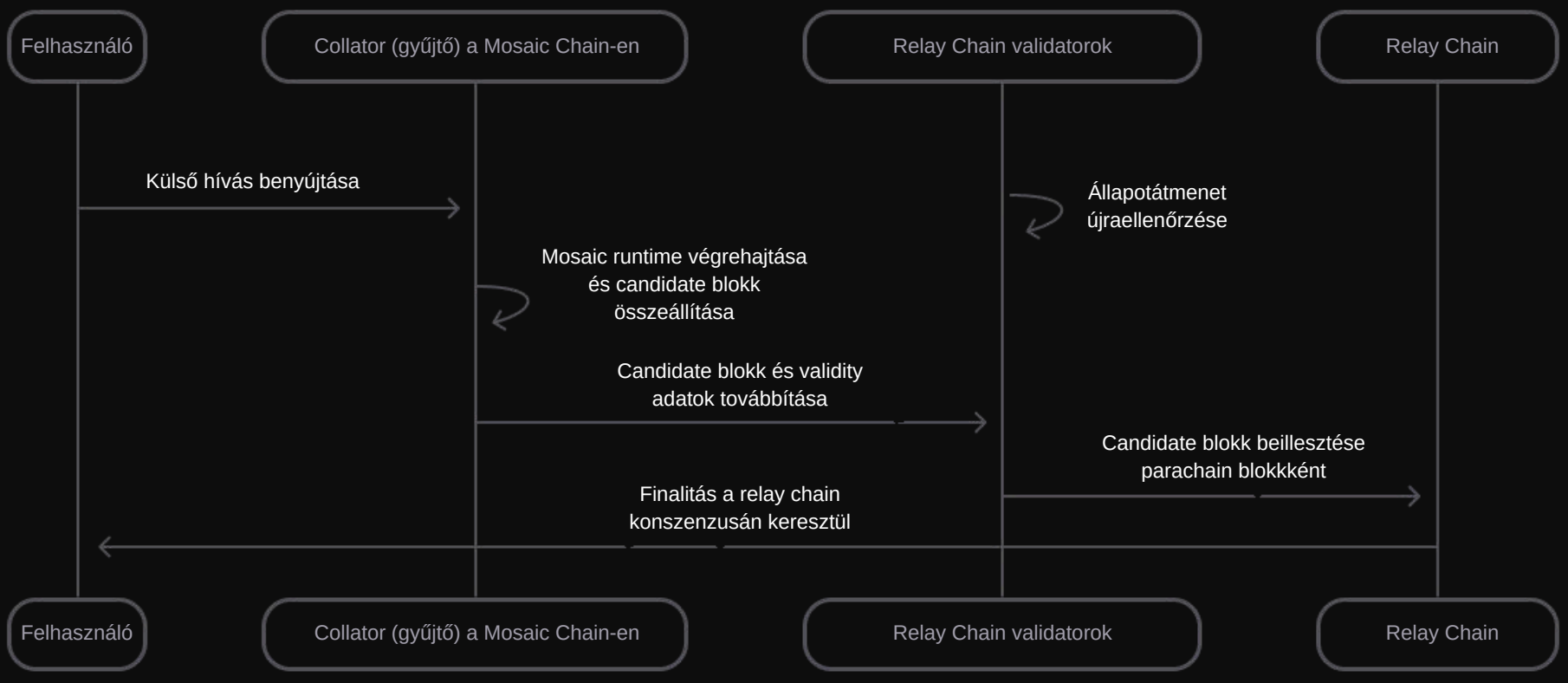
A Mosaic Chain számára ez a kapcsolat több konkrét előnyt biztosít. A skálázhatóság részben a relay chain architektúrára kerül kiszervezésre: parachainként csatlakozva a Mosaic Chain egy olyan megosztott hálózat részévé válik, amely a tranzakció-végrehajtást több blockchain között osztja szét, megakadályozva, hogy bármely egyedi parachain önálló szűk keresztmetszetté váljon.
A finalitást a Mosaic Chain a Polkadot GRANDPA finalizációs mechanizmusából örökli, amely a hagyományos önálló láncoknál lényegesen erősebb probabilisztikus garanciákat biztosít. A biztonságot tovább erősíti a Polkadot megosztott biztonsági modellje, amely az összes parachain gazdasági biztonságát közös poolban kezeli ahelyett, hogy minden láncnak önállóan kellene kiépítenie saját biztonsági infrastruktúráját.

A Mosaic Chain parachain slotot nyert, és továbbra is a Polkadot ökoszisztémán belül működik, követve a protokoll fejlődésével együtt érkező változásokat. Ez az ökoszisztémaszintű integráció biztosítja, hogy a Mosaic Chain részesüljön a relay chain infrastruktúra folyamatos fejlesztéseiből — beleértve a skálázhatósági fejlesztéseket, governance-frissítéseket és új cross-chain kommunikációs képességeket.

Parachain státusz és végrehajtási modell

Parachainként működve a Mosaic Chain elkülöníti a lokális végrehajtást a globális finalitástól. A Mosaic saját validatorüzemeltetői collatorként működtetik a parachain infrastruktúrát: fenntartják a teljes Mosaic state-et, összegyűjtik a felhasználói tranzakciókat (extrinsic-eket), végrehajtják azokat a Mosaic runtime-on, majd candidate blokkokat állítanak össze.

Minden candidate blokkhoz a collator előállítja a kapcsolódó validity adatokat (state transition witness) is, amelyek szükségesek ahhoz, hogy a Polkadot relay chain validatorai ellenőrizni tudják az állapotátmenetek helyességét. A relay chain validatorai újra végrehajtják a candidate blokk state transitionjeit; amennyiben azok érvényesnek bizonyulnak, a blokk bekerül a Relay Chainbe, és a Polkadot konszenzusmechanizmusán keresztül finalitást kap (BABE a blokk-előállításhoz, GRANDPA a finalitáshoz).



Ez a modell megosztott biztonságot biztosít: a Mosaic saját runtime-szabályait érvényesíti, miközben a Relay Chain finalitása gazdasági és kriptográfiai szempontból rendkívül nehézzé teszi a finalizált Mosaic blokkok visszafordítását. A Mosaic permissioning és NPoS-stílusú bonding mechanizmusai határozzák meg, hogy mely operátorok jogosultak collatorként működni, valamint hogyan történik a blokk-előállítási jogosultságok rotációja; a Polkadot biztosítja a finalitási és biztonsági réteget.

A parachain-végrehajtás horizontális skálázhatóságot és interoperabilitást is lehetővé tesz. A Mosaic a Polkadot Cross-Consensus Messaging (XCM) protokollján keresztül képes üzeneteket és eszközöket cserélni más parachainekkel és a Relay Chainnel, lehetővé téve, hogy a Mosaic-natív alkalmazások értéket és hívásokat irányítsanak a teljes Polkadot ökoszisztémán keresztül megbízható közvetítők használata nélkül.
A runtime-frissítések governance útján, on-chain Wasm-frissítésekként kerülnek telepítésre, lehetővé téve a végrehajtási logika forkless fejlődését, miközben megőrzik a lánctörténetet és a Relay Chaintől örökölt biztonsági garanciákat.

XCM irányelvek

A Polkadot Cross-Consensus Messaging (XCM) protokollja biztonságos, trustless kommunikációt tesz lehetővé a parachainek között. Az XCM egy üzenetformátum és utasításkészlet, amely lehetővé teszi, hogy eltérő konszenzusmechanizmusokat használó blockchainek üzeneteket és eszközöket cseréljenek anélkül, hogy centralizált bridge-ekre, megbízható oracle-ökre vagy többszereplős aláírási rendszerekre támaszkodnának.
Ez megszünteti azt a rendszerszintű kockázatot, amely a hagyományos bridge-megoldások feltörései és sérülékenységei miatt már dollármilliárdos veszteségekhez vezetett.

A Mosaic Chain számára az XCM két kategóriájú cross-chain interakciót tesz lehetővé. Az eszköztranszferek támogatják, hogy a MOS tokenek és más, a Mosaic Chainen lévő eszközök más Polkadot parachainekre kerüljenek átküldésre, illetve onnan fogadásra kerüljenek — beleértve olyan meghatározó ökoszisztéma-szereplőket, mint a Hydration, Bifrost, Acala, Moonbeam és Astar. Ez a képesség különösen fontos egy pénzügyi fókuszú lánc esetében, mivel a DeFi-alkalmazások működése alapvetően a likviditásra épül, és a cross-chain eszközáramlások jelentik a parachain ökoszisztémákba belépő és onnan kilépő likviditás elsődleges mechanizmusát.
A cross-chain üzenetküldés biztosítja, hogy a Mosaic Chainen futó smart contractok más parachaineken hajtsanak végre műveleteket — és fordítva —, ezáltal olyan kompozábilis pénzügyi alkalmazásokat téve lehetővé, amelyek több láncon átívelően működnek.

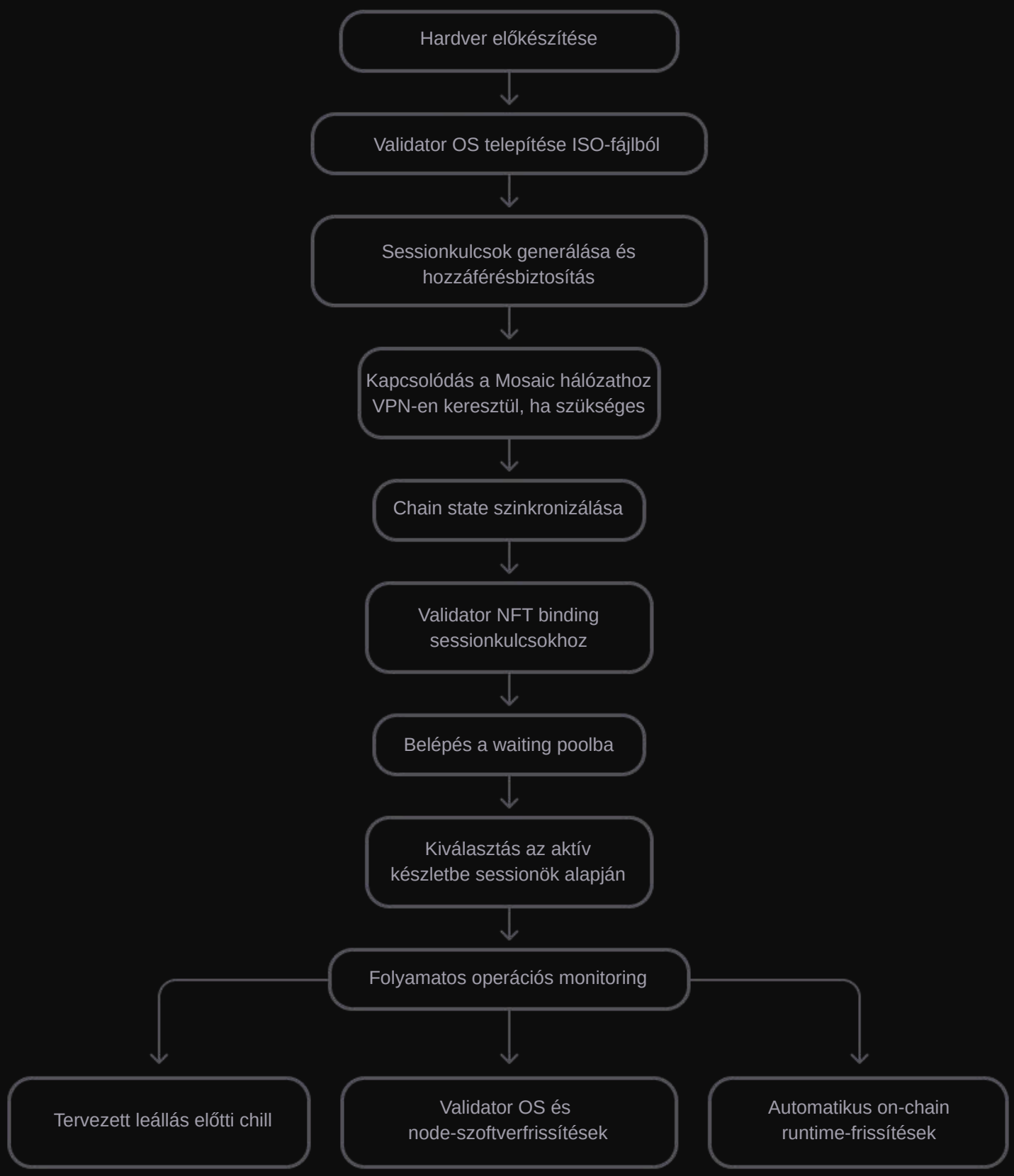
Az XCM biztonsági modellje minőségileg eltér a hagyományos bridge-rendszerekétől. A tradicionális bridge-architektúrák jellemzően multisignature sémákra, oracle-hálózatokra vagy optimista verifikációs periódusokra támaszkodnak a cross-chain üzenetek hitelesítéséhez. E megközelítések mindegyike olyan bizalmi feltételezéseket és támadási felületeket vezet be, amelyek a gyakorlatban már számos alkalommal kompromittálódtak. Az XCM ezzel szemben a relay chain saját validatorkészletére támaszkodik a cross-chain üzenetek ellenőrzéséhez, örökölve a teljes Polkadot hálózat gazdasági biztonságát. Egy pénzügyi fókuszú lánc esetében — ahol az áthelyezett eszközök jelentős értéket képviselhetnek — ez a trustless biztonsági modell nem pusztán kényelmi funkció, hanem alapvető követelmény.

A Mosaic Chain jelenlegi XCM implementációjának hatóköre konzervatív megközelítést követ, és a megbízható alapfunkcionalitás kialakítására összpontosít. A Mosaic Chain és más Polkadot parachainek közötti eszköztranszferek jelentik a kezdeti képességet. A governance által jóváhagyott frissítési folyamaton keresztül a jövőben további képességek fejleszthetők és telepíthetők, többek között: programozható cross-chain contracthívások, cross-chain likviditási pooling, valamint olyan parachainekkel való integráció, amelyek kiegészítő pénzügyi infrastruktúrát biztosítanak.
A roadmap tartalmazza a MOS tokenek nagyobb külső hálózatok — például Ethereum és Solana — felé történő bridge-elését is, kezdetben ökoszisztéma-bridge-eken keresztül, majd később natív XCM képességekkel, ahogy a Polkadot külső bridge-infrastruktúrája érettebbé válik.

Validator OS és üzemeltetés

Mi a Validator OS?

A Validator OS egy célzottan fejlesztett, Debian-alapú Linux disztribúció, amelyet a Mosaic Chainen futó validator node-ok teljes működési életciklusának szabványosítására és egyszerűsítésére terveztek. A general-purpose operációs rendszerekkel szemben — ahol a validator szoftvert manuálisan kell telepíteni, konfigurálni és karbantartani — a Validator OS előre konfigurált környezetet biztosít, amely valamennyi szükséges komponenst, biztonsági mechanizmust és operációs eszközt előre telepítve tartalmaz.



A rendszer ISO image formájában kerül terjesztésre, amely USB-meghajtóra írható (minimum 16 GB), és közvetlenül használható a validator hardver formázására és konfigurálására. Az operációs rendszer tartalmazza a teljes Mosaic Chain node-szoftvert, a peer-to-peer kapcsolódáshoz szükséges hálózati konfigurációt (beleértve a NAT mögötti node-ok számára biztosított Mosaic VPN-t), a monitoring- és telemetriai infrastruktúrát, valamint az automatizált frissítési mechanizmusokat. Az első üzembe helyezést követően nincs szükség külön letöltésekre vagy csomagtelepítésekre.

A Validator OS mögötti tervezési filozófia célja, hogy csökkentse a validatorrá válás operációs belépési küszöbét, miközben a szabványosított eszközkészlet révén javítja a megbízhatóságot. Ahelyett, hogy feltételezné, hogy minden validatorüzemeltető professzionális rendszergazda, a Mosaic egy célzottan fejlesztett, Debian-alapú disztribúciót biztosít, amely a node-ot, a hálózati komponenst, a monitoringrendszert és a frissítési eszközöket egyetlen irányított, reprodukálható munkafolyamatba csomagolja.
A Validator OS nyílt forráskódúként kerül kiadásra, így független szereplők saját alternatív verziókat is létrehozhatnak és karbantarthatnak. Ez elkerüli azt a sérülékeny monokultúrát, amelyben egyetlen operációsrendszer-szintű hiba az egész hálózatot érinthetné, miközben továbbra is biztosít egy ajánlott „golden path” konfigurációt a legtöbb operátor számára.

Onboarding folyamat

A validator onboarding folyamata egy tudatosan kialakított, szekvenciális munkafolyamatot követ annak érdekében, hogy minden validator node megfelelően konfigurált és biztonságosan előkészített állapotban csatlakozzon a hálózathoz. A folyamat bizonyos szakaszai szándékosan szigorúak, mivel a kulcskezeléssel kapcsolatos hibák később már nem korrigálhatók.

A folyamat a hardver előkészítésével kezdődik. A minimális specifikációkat teljesítő számítógép szükséges (Intel Core i5-12400 vagy egyenértékű CPU, 32 GB DDR4 RAM, 2×1 TB NVMe SSD, vezetékes internetkapcsolat legalább 30–40 Mbps sávszélességgel és ideálisan 50 ms alatti késleltetéssel), előre telepített operációs rendszer nélkül. A Validator OS ISO image USB-meghajtóra kerül kiírásra, majd a rendszer az USB-ről bootolva megkezdi a telepítési folyamatot.

A telepítő formázza a célgép adattárolóit, telepíti az operációs rendszert és valamennyi validatorszoftvert, konfigurálja a hálózati stacket, valamint létrehozza a kezdeti biztonsági beállításokat. Az operációs rendszer telepítését követően a node-üzemeltetőt egy lépésről lépésre felépített regisztrációs folyamat vezeti végig, amely magában foglalja:
a sessionkulcsok generálását, a kétfaktoros hitelesítés konfigurálását, a Mosaic VPN-hez való csatlakozást peer discovery céljából, valamint a blockchain state hálózatról történő szinkronizálását.

Az onboarding folyamat utolsó lépése a Validator NFT bindingja a node sessionkulcsaihoz. Ez az on-chain tranzakció hivatalosan jogosult validatorként regisztrálja a node-ot, és amint a node teljesen szinkronizált állapotba kerül, bekerül a waiting poolba, ahonnan a validator subset selection algoritmus jövőbeni aktív készletekbe választhatja be.

A hálózat decentralizációs tulajdonságainak megőrzése érdekében bizonyos konfigurációk a javasolt működési modellben kifejezetten nem támogatottak. Ilyennek számít: több validator futtatása ugyanazon fizikai gépen, több validator üzemeltetése ugyanazon fizikai helyszínen, validatorok telepítése VPS-szolgáltatásokba vagy azonos szolgáltató infrastruktúrájára, valamint validatorok hosztolása ugyanabban a szerverparkban.
Ezeket a konfigurációkat a protokoll nem tiltja közvetlen technikai ellenőrzésekkel; ehelyett a hálózat monitorozza, hogy a validatorkészlet milyen mértékben követi ezeket az ajánlásokat a decentralizációs állapot felmérése érdekében, miközben lehetőséget hagy olyan legitim speciális esetekre, ahol a szigorú tiltás érvényes felhasználási helyzeteket akadályozna.

A Mosaic VPN szolgáltatás egy kiegészítő komponens, amely az otthoni környezetből működő validatorok egyik gyakorlati problémáját kezeli. Számos lakossági internetkapcsolat Network Address Translation (NAT) mögött működik, és nem biztosít nyilvánosan routolható IP-címet, amely hagyományosan szükséges a peer-to-peer hálózati kapcsolatokhoz.
A Mosaic VPN lehetővé teszi, hogy a NAT mögött működő validator node-ok biztonságosan kapcsolódjanak a hálózat többi node-jához anélkül, hogy az operátornak port forwardingot, statikus IP-címeket vagy más fejlett hálózati konfigurációkat kellene beállítania.
Ez a szolgáltatás integrált része a Validator OS-nek, és automatikusan konfigurálásra kerül az onboarding folyamat során.

A hardverkövetelmények szándékosan mérsékeltek és könnyen elérhetők. Az ajánlott specifikációk — egy fogyasztói kategóriás Intel Core i5 processzor, 32 GB RAM és két darab 1 TB-os NVMe SSD — általánosan elérhető, kereskedelmi forgalomban kapható komponensekkel teljesíthetők, töredékéért azoknak a költségeknek, amelyeket az intenzívebb hardverigényű hálózatok megkövetelnek.
A két SSD-ből álló konfiguráció redundanciát biztosít a chain storage réteg számára anélkül, hogy vállalati szintű RAID hardverre lenne szükség. Az otthoni működésre helyezett hangsúly — kombinálva a hozzáférhető hardverkövetelményekkel — támogatja a projekt decentralizációs célját: a validatorok földrajzilag diverzifikált eloszlását a professzionális adatközpontokba történő koncentráció helyett.

Megbízhatóság és karbantartás

A validatorok folyamatos karbantartása két egymástól független frissítési csatornán keresztül történik. Az operációs rendszer és a node-szoftver frissítései a Validator OS beépített frissítési mechanizmusán keresztül kerülnek telepítésre, amely automatikusan tölti le a frissítéseket a Mosaic Chain repositoryiból.

Ezek a frissítések magukban foglalhatnak: biztonsági javításokat, teljesítmény-optimalizációkat, hálózati stack frissítéseket, valamint a node-szoftver új verzióit.
Azok a haladó felhasználók, akik a manuális kontrollt részesítik előnyben, letilthatják az automatikus frissítéseket, és saját maguk kezelhetik rendszereiket.
A szoftverstack a standard Substrate node-konvenciókat követi, és várhatóan egyre nagyobb mértékben válik nyílt forráskódúvá, ahogy az egyes komponensek fokozatosan publikálásra kerülnek.

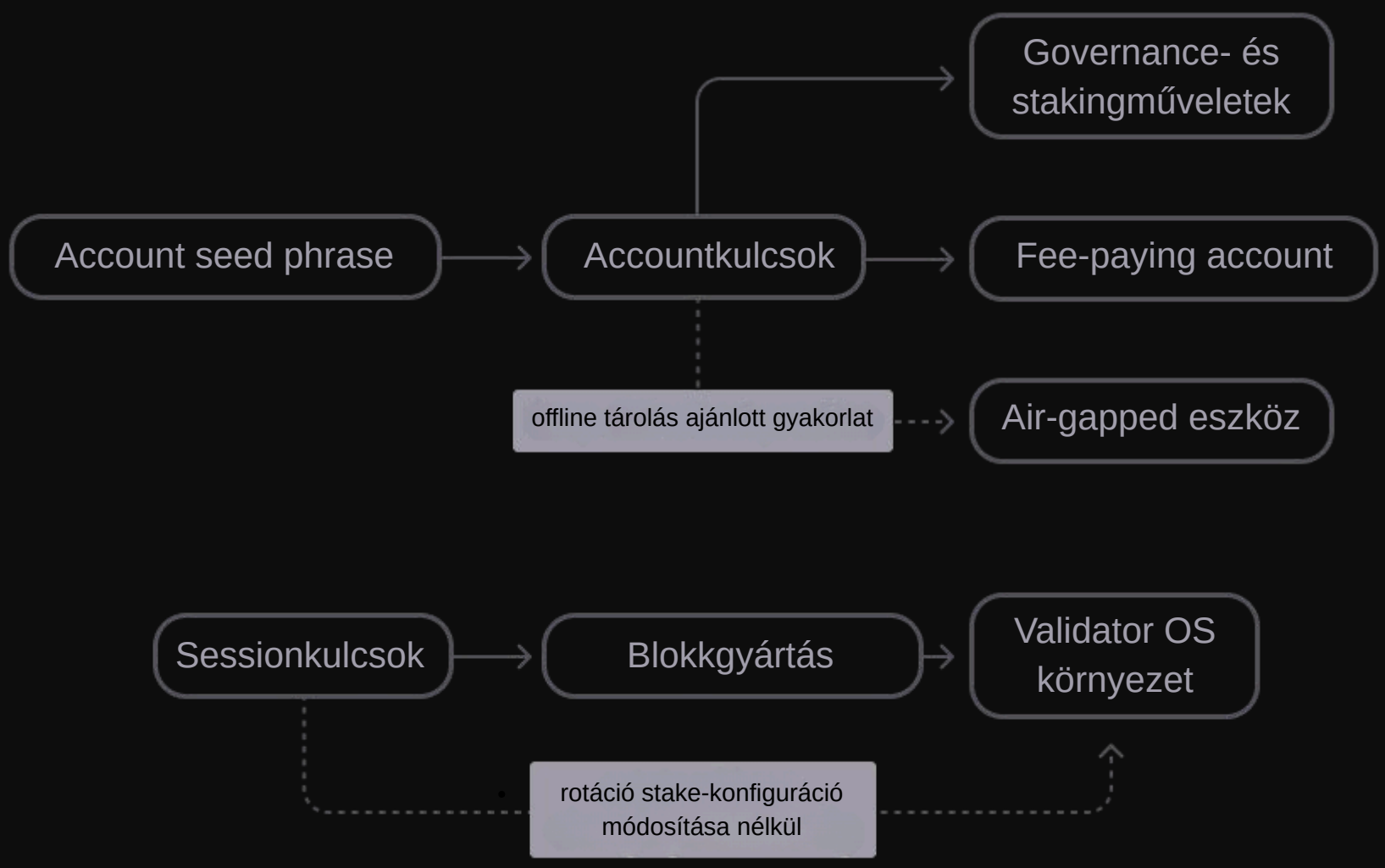
A runtime-frissítések — ahogy a 8.2-es fejezet is ismerteti — ettől függetlenül, az on-chain forkless frissítési mechanizmuson keresztül működnek. A validatoroknak nincs szükségük semmilyen manuális beavatkozásra ahhoz, hogy a runtime-frissítések életbe lépjenek; az új runtime automatikusan alkalmazásra kerül a konszenzusmotor által, amint az upgrade tranzakció megjelenik a chain state-ben.

A validator-karbantartás ajánlott gyakorlatai közé tartozik a proaktív chilling a tervezett leállások előtt (hardverkarbantartás, hálózati módosítások vagy fizikai áthelyezés esetén), a tartalék áramellátás (UPS) és hálózati redundancia fenntartása a nem tervezett kiesések megelőzése érdekében, továbbá annak rendszeres ellenőrzése, hogy a monitoring- és telemetriai rendszerek megfelelően működnek-e.
Szintén kiemelten fontos a biztonságos hitelesítőadat-kezelés gyakorlata — különösen a seed phrase-ek esetében, amelyek elvesztésük esetén visszaállíthatatlanok. A Validator OS frontend valós idejű rálátást biztosít: a node állapotára, a szinkronizációs státuszra, a staking teljesítményre, valamint a jutalomelőzményekre, ezáltal lehetővé téve az operátorok számára, hogy még azelőtt észleljék és kezeljék a problémákat, mielőtt azok slashing büntetésekhez vezetnének.

Biztonsági megfontolások

Kulcskezelés és felhasználói biztonság

A Mosaic Chain standard publikus kulcsú kriptográfiát használ a fiókhitelesítéshez és a tranzakciók aláírásához. Minden account egy seed phrase-ből (mnemonic) származik, amely az account eszközei és műveletei feletti végső jogosultsági forrásként szolgál.
A biztonsági modell a seed phrase biztonságos megőrzésének teljes felelősségét a felhasználóra hárítja: nincs helyreállítási mechanizmus elveszett seed phrase esetén, és nincs visszavonási lehetőség kompromittálódott seed phrase esetén sem.
Ez a kriptográfiai modell alapvető tulajdonsága, nem pedig olyan korlátozás, amely szoftverfrissítésekkel kezelhető lenne.



A validatorüzemeltetők számára a kulcskezelés további biztonsági dimenziókkal rendelkezik. A blokkgyártáshoz használt validator sessionkulcsok elkülönülnek a stakinghez és governance-műveletekhez használt accountkulcsoktól. Ez a szétválasztás biztosítja a validatorok számára a sessionkulcsok rotálását anélkül, hogy staking-konfigurációjuk módosulna, miközben csökkenti a magas jogosultságú accountkulcsok kitettségét a validator node operációs támadási felületének.
Ajánlott gyakorlat az accountkulcsok különálló, air-gapped eszközön történő generálása és kezelése, míg a sessionkulcs-generálás a Validator OS környezeten belül maradjon.

A felhasználóknak és validatoroknak szigorú accountszétválasztást kell fenntartaniuk: az operációs accountok (napi tranzakciókhoz és fee-fizetéshez használva), valamint a magas értékű accountok (nagy stakingpozíciókhoz és governance-műveletekhez használva) között. Ez a gyakorlat korlátozza egy esetleges kulcskompromittálódás hatókörét, és többrétegű védelmet biztosít mind a technikai támadásokkal, mind az operációs hibákkal szemben.

Gazdasági biztonsági modell

A Mosaic Chain gazdasági biztonsága a validatorok és delegatorok által stake-elt MOS teljes értékére épül. Egy olyan támadónak, aki a konszenzus manipulálására törekszik, a teljes stake-állomány kellően nagy részét kellene kontrollálnia, ami közvetlen gazdasági költséget jelent a hálózat teljes stake-elt értékével arányosan.
A slashing mechanizmusok biztosítják, hogy a rosszindulatú viselkedés ne csupán veszteségessé, hanem a támadó tőkéjére nézve ténylegesen destruktívvá váljon, olyan elrettentő modellt létrehozva, amely a hálózat által védett értékkel arányosan skálázódik.

A hálózat biztonsági költségvetése — vagyis a stakingen keresztül kockáztatott teljes érték — határozza meg egy konszenzustámadás költségét. Mivel a Mosaic blokkgyártáshoz PoA-modellt használ NPoS-jellegű delegációs gazdasági modellel kombinálva, egy támadónak vagy elegendő stake-et kellene felhalmoznia ahhoz, hogy jelentős befolyást szerezzen (vagy kontrollálja a permission alapú részvételi jogokat), vagy elegendő számú validator operátort kellene kompromittálnia ahhoz, hogy uralja az aktív készlet többségét.
A sessionalapú rotációs mechanizmus tovább nehezíti a célzott kompromittálást: mivel az aktív készlet minden session végén változik, és egy randomizált algoritmus határozza meg, a támadó nem tudja előre megjósolni, mely validatorok lesznek aktívak egy jövőbeli session során. Emiatt a teljes validatorpopuláció jelentős részét kellene kompromittálnia, nem csupán egyetlen aktív készlet egy részét.

A protokoll gazdasági modellje több strukturális védelmi mechanizmust is tartalmaz a koncentrációs kockázatok ellen. Az 5%-os validatoronkénti stake-korlát megakadályozza, hogy bármely szereplő domináns stake-pozíciót halmozzon fel egyetlen validatoron keresztül. A sessionalapú rotáció biztosítja, hogy még a maximális stake-kel rendelkező validatorok se rendelkezzenek folyamatos blokkgyártási jogosultsággal, ezáltal korlátozva bármely validator kompromittálódásának hatását.
A delegációs modell — miközben növeli a teljes stake-elt értéket — a monitoring felelősségét is szétosztja a delegatorok között, akik gazdaságilag motiváltak a validatorok minőségének értékelésében.

A diverzifikáció különösen fontos a jelentős MOS-pozíciókat kezelő delegatorok számára. Mivel a slashing mind a validator saját stake-jére, mind a delegált stake-re alkalmazandó, a teljes pozíció egyetlen validatorhoz történő delegálása koncentrált kockázatot jelent.
A protokoll staking szerződéses struktúrája — amely validatoronként 1 000 szerződésben és a teljes kínálat 5%-ában maximalizálja a stake-et — ösztönzi ugyan a diverzifikációt, de azt egyéni delegatorszinten nem kényszeríti ki.
A delegatoroknak a delegációs döntések meghozatalakor értékelniük kell: a validator uptime-előzményeit, a jutalék mértékét, valamint az operációs transzparenciát.
A Mosaic Explorer nyilvános hozzáférést biztosít ezekhez a metrikákhoz, lehetővé téve a megalapozott delegációs döntéshozatalt.

Operatív biztonság

A validator node-ok biztonsági modellje a defense-in-depth elvet követi. A Validator OS egy megerősített alapkonfigurációt biztosít, amely minimalizálja a támadási felületet: a validator node-ok kizárólag egyetlen célra (validációra) szolgálnak, és nem használhatók más programok vagy szolgáltatások futtatására.
A hálózati kapcsolódást a Mosaic VPN kezeli, amely biztonságos peer-to-peer kapcsolatokat biztosít még NAT mögött vagy nyilvános IP-cím nélkül működő node-ok számára is.
A kétfaktoros hitelesítés védi a validator adminisztrációs felületét.

A gyakori hibaforrások és azok mitigációs mechanizmusai a következők: nem tervezett leállások (UPS és hálózati redundancia által mitigálva), hibás konfigurációk (a Validator OS szabványosítása által mitigálva), kompromittálódott hitelesítő adatok (account- és sessionkulcsok szétválasztásával mitigálva), valamint hardverhibák (a dual-SSD storage konfigurációval és a chain syncből vagy cserehardverből történő helyreállítás lehetőségével mitigálva).
A protokoll slashing mechanizmusa úgy került kalibrálásra, hogy büntesse a tartós megbízhatatlanságot anélkül, hogy aránytalanul szankcionálná az izolált incidenseket, figyelembe véve, hogy a teljes operációs hibamentesség sem technikailag nem garantálható, sem gazdaságilag nem ésszerű elvárás.

Roadmap

Kattints ide a roadmap megtekintéséhez

