MULTIVERSUM

HERE TO STAY

WHITE PAPER v 1.0.6

Business | Technical

Hungarian

19.02.2018

Authors: Multiversum Team

www.multiversum.io

A miénken kívül, még megszám-lálhatatlanul sok univerzum van, és ezek határtalan nagyságuk ellenére is úgy mozognak, mint a benned lévő atomok.

Bhagavata Purana 6.16.37

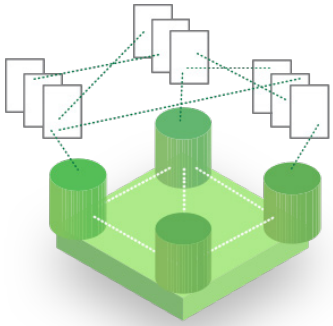
Multiversum
Identitás és küldetés

A cryptovaluták úttörője, a Bitcoin, az összes klónjával és elágazásával együtt első generációs blokláncoknak tekinthetőek, amik proof-of-work algoritmuson alapszanak, a tranzakciók hitelesítéséhez.
A második generáció, az Ethereum vezetésével lehetségessé vált intelligens szerződésekkel, valóban heterogénebb, és könnyebb tokenizációt engedélyez.
Mind a két szerkezet rendkívül alacsony energia hatékonysággal és közepesnél alacsonyabb blokk visszaigazolási sebességgel és blokkonkénti tranzakcióval bír.
A harmadik generáció célja a skálázhatósággal, sebességgel és energiafogyasztással kapcsolatos problémák megoldása, különböző megközelítéseket és technikákat alkalmazva, mint például a Proof of Stake algoritmus, off-chain routing, graph-chains és a teljes vagy részleges centralizáció.
A negyedik generáció messze túlmegy ezeken, gyorsabb és könnyebb skálázhatóságot elősegítő megoldásokat elérve, és ugyanakkor próbál versenyképessé válni üzleti szemszögből; az adatok egyszerű láncai nem elég rugalmasak ahhoz, hogy kielégítsék a vállalati környezet szükségeit, amelyben összetett adatszerkezeteket kell rendezni táblákban (mint a relációs adatbázisokban).
Ugyanakkor, azokat a szerkezeteket igazolni kell és módosíthatatlanná kell tenni block chain alapú technikákkal, növelve az átláthatóságukat és biztonságukat.
Más szavakkal, a negyedik generációs blochchain előrehozza ezt a technológiát egy komplett elsődleges termelési alkalmazássá, és kibővíti a jelenlegi üzlet orientált kínálatot az adat tárolást, alkalmazás decentralizálást, átláthatóságot, biztonságot, megbízhatóságot tekintve.
Multiversum összetett adat rendezést kínál, ahelyett, hogy az adatokat szekvenálja, lánc elválasztást és újra egyesítést a nagyobb mértékű skálázhatóság és párhuzamosság érdekében, és a proof of integrity koncepciót (vagyis a szerverkód titkosítási bizonyítéka-cryptographic proof of server code) a létező proof of work és proof of stake megoldások helyett.
Továbbá, a multiversumra jellemző lesz az ERC20/ERC23 integráció, lehetővé téve más, különböző megoldásokból származó coinoknak és tokeneknek, hogy a láncunkban legyenek és oda-vissza ugyanúgy, közjegyzői szolgáltatásokkal, mint egy külső megerősítési módszer.
Közben, ezekkel az innovációkkal együtt, biztosan hasznul veszünk majd számos jó megoldást, amit a kollégák már beágyaztak az idő során.

Multiversum

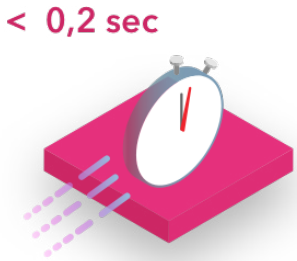
Negyedik generációs összefüggő blockchain

Miért a multiversum a 4.0 blockchain?



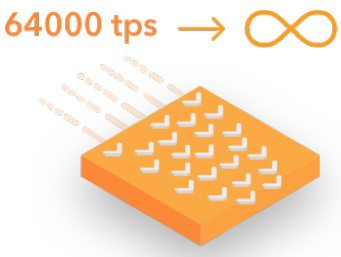
Összefüggő blockchain

Egy vadonatúj blockchain, ami különböző típusú adatokat jelenít meg multidimenzionális struktúrában.



Tranzakció sebesség

0.2 másodpercnél kevesebb idő alatt az összegek átmennek a walletok között, beleértve a tranzakciók biztonságos érvényesítését. A világ leggyorsabbjai között van.



Tranzakció áteresztőképesség

Páratlan skálázhatóság: 64,000 Tps-ig (1000 Tps/mag) egy 64 magos szerveren. Támogatja a 64+ magos technológiákat.

Proof of Integrity

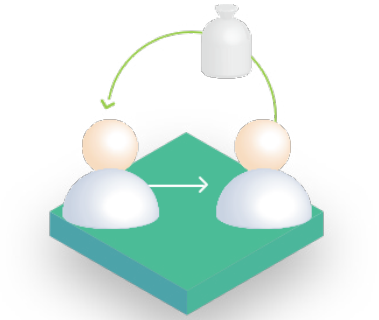
PoS(proof of stake) cserélve lesz PoI-re.
(Proof of Integrity: cryptographic proof of server code).

Következő generációs tárca

Élvonalbeli biztonság az elérhetőségben és az összegek küldése biometric inputokkal.

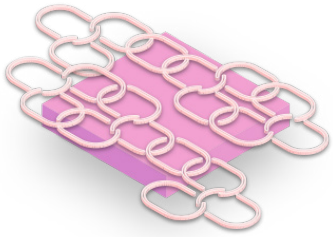
Környezetbarát

A multiversum tranzakcióinak jelntéktelen költségei lesznek
és a 0-hoz közeli ökológiai lábnyoma.



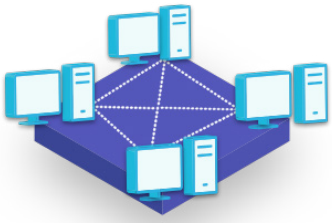
Rollback

Lehetséges rollback aktiválása a multiversumon lévő tokenekre.



Osztható láncok

Erőforrás optimalizálás a csomópontok között a lánc elválaszthatóságával.



Helyreállítási csomópontok elosztása

Az MTV csomópontok szétszóródtak az egész világon a páratlan rugalmasságért, a megbízhatóságért és katasztrófa utáni helyreállításért.

Nyilvános prezentáció

A blockchain jelenlegi fejlettségi szintje

A blockchain jelenség vezető szereplői közös vonásokban osztoznak : egyedülálló biztonság és megbízhatóság. Ugyanakkor ezért nagy árat kell fizetni : feldolgozása rengeteg energiát igényel, elfogadhatatlan méretű környezetszennyezést okoz, magas tranzakciós költségekkel jár és emellett a rendszert lassúság jellemzi. Ez aligha elfogadható a technológia jelenlegi fejelettségi szintje mellett és nem nyújt kézenfekvő technikai megoldást a modern pénzügyi és kereskedelmi felhasználáshoz.
A lassú futási időt a vízszintes skálázhatóság hiánya okozza. A számítási teljesítmény növelését csakis új processzorok hozzáadásával teszik, a régiek újra cserélése helyett. Másik oka a blockchain jelenlegi biztonsági rendszerének velejárója. Úgy tervezték, hogy megakadályozzon bárkit a clusterek tulnyomó részének elfoglalásától, azzal, hogy másoknak nem megtérülő befektetéssé teszi a számítási energia és/vagy költség függvényében. (PoW and PoS)
Ezenkívül, a jelenlegi blockchainek csak adategységek állapotváltozásainak egyszerű láncolatai. Az adatok jelenlegi állapotának kimutatása, a lánc teljeskörű átkutatását igényli. Ami a rendszer még ennél is nagyobb mértékű lassulásához és erőforrásigényhez vezet.
Ez az egyszerű megoldás nem teszi megfelelővé a blockchaint tudományos és ipari célokra. A bonyolult adatrendszerekre irányuló szükségletek egyre nagyobb kihívásnak bizonyulnak.
Ráadásul, a biztonsági intézkedések megállnak egy bizonyos adatszint felett, így nem garantálva a felhasználók biztonságát. Lehetetlenné téve ezzel az ellopott, elveszett coin-ok és token-ek visszaszerzését, még akkor is, ha azok a láncon helyezkednek el, miközben az ártó szándékú felhasználók nem kerülnek kitiltásra.
Végül, a kriptovaluták egy másik probléméja a tördelés és az inhomogenitás. Nem képesek kommunikálni egymással, egymástól független környezetben működnek.

A Multiverzum és blokklánc globális adaptálása

A multiverzum technológia kitolja a tradicionális blokklánc jelenlegi határait, azzal hogy, erősíti az adat réteget, önellenőrző és szétosztott struktúrájú rendezett adat entitásokon keresztül, amelyek szimbolikus linkeken keresztül mind kapcsolatban állnak egymással.
Ez a technológia rakta le az alapköveit egy decentralizált és szétosztott, koherens, önellenőrző tranzakciókból álló rendszernek: a multiverzum blokkláncnak.
Multiverzum lehetővé teszi, a létező egyszerű blokklánc adatmodell helyett, egy Relációs Kripto Adatbázis (egy előrehaladott, rendezett adat raktározási megoldás) létrejöttét, amely képes nem csak egyszerű adattipusok, hanem egymással összefüggésben álló, bonyolult gráfokba rendeződő adatsorozatok kezelésére is. A relációk így már első rangú szereplői lesznek a blokkláncnak és kriptografikus metódusok által biztosítottak lesznek.
Mindegyiknek, amikor státusz változtatás kerül kérelmezésre, meglesz a saját al-lánca, ami az eredeti ágból származik, és ami az operáció végeztével visszacsatlakozik, hogy érvenyesítetté váljon.
Tehát a Multiverzum egy továbbfejlesztett blokklánc technológia, amely egyedülálló megoldásokat kínál az előzőleg megvizsgált kellemetlenségeken való felül kerekedésre, kripto-érvényesítő és szétosztó technikák készletének segítségével, amelyek minden körülményre megfelelőek: legyen az adminisztratív, ipari, pénzügyi vagy kormányzati.
A Multiversum egyik fő célja, hogy minden pillanatban, az elérhető legkifejlettebb produktumot kínálja az egész piac számára: ez az AGILIS szoftverfejlesztési metodológia elsajátításával érhető el.
Az AGILIS metodológia drasztikus csökkentést jelent a projekt kezdeti tervezésének részvételében, a projekt fejlesztése közben szerzett tapasztalatok későbbi legcélravezetőbb módon való felhasználásanak érdekében, amely az elejétől fogva szinte megjósolhatatlan új lehetőségekre és egyben veszélyekre hívja fel a figyelmet, eredményezve a legjobb praktikák használatát, és a nem megfelelőek hátrahagyását.
Az AGILE egy megalapozott szoftverfejlesztési standard, ami készteti a fejlesztőket, a termék tulajdonosokat és a befektetőket, hogy rugalmasnak és könnyen a piaci igényekhez igazíthatónak tekintsék a projekt feladatkörét. Továbbá, egy ilyen rohamosan fejlődő területen mint a szoftver, 6 hónapos kutatást és 1 éves implementációt követően kiadni egy olyan terméket amely a 18 hónappal azelőtti piac kiszolgálására készült, egy olyan termék kiadását jelenti amely idejétmúlt, valószínűleg konkurencia által már megoldott problémákra igyekszik választ adni, illetve képtelen megoldást biztosítani az újabb kihívásokra.
AGILE, ehelyett, mindig a leginnovatívabb termékek piacra dobására ad lehetőséget.

Gyorsaság és Technológia

Az egyik erőssége ezen technológiának valóban a sebesség, köszönhetően a különböző tranz-

akciók egyidőben történő futtatásának, és a szétválasztó-újraegyesítő mechanizmusnak. Ezek a tulajdonságok nagyobb horizontális skálázási lehetőséget és tranzakció feldolgozási kapacitást biztosítanak, számítási teljesítményt hozzáadva a már meglévőhöz, minden csomópontot kiemelve ezzel, a teljesítmény érdekében.

Horizontális Skálázhatóság

Multiversum két specifikus tulajdonságból húz hasznot a rendszerhatékonyság maximalizálásának érdekében:
A fő lánc képes optimalizálni struktúráját azáltal, hogy automatikusan több alláncra hasad, a kért forrásoknak és adatfolyamoknak megfelelően, párhuzamosítva ezzel a munkát több szálon és csomóponton át.
Ez a lánc-hasadási folyamat a munkaterhelés normalizációjáig tart, amikor is, szintén automatikusan, a lánc újra eggyé válik.
Ez mind attól a technikától válik lehetővé, hogy a lánc minden blokkja kettő különböző alláncot képes kettő különböző beérkező hivatkozásról érvényesíteni.
Adat szabdalás, vagyis, egy technika amely adat szétosztást engedélyez több csomópont között.
Adott az ABC adat sorozat és három Cluster csomópont; az adat szétosztás a következőképpen fest:
- AB
- BC
- CA

Ez a parcellázás gyorsabb tranzakció feldolgozást tesz lehetővé, mert az adat lekérések csak az allánc csomópontjaira vannak hatással, optimalizálva minden lépést.
Még egy rendkívül fontos tulajdonsága a technológiánknak a Magasabb Elérhetőség : annak az esélye, hogy egy csoport típusra hagyatkozunk, amely biztosítja a szolgáltatások további működését még akkor is, ha esetleg néhány csomópont a hálozaton belül leáll.
Az előző példát használva (A,B és C csomópontok), ha C kikapcsol, A és B továbbra is tökéletesen működőképes marad, így biztosítva a szolgáltatás folytonosságát bármiféle adat veszteség nélkül, egészen addig amíg a csomópontokból 50%+1 darab működőképes állapotban van.
Így, több csomópont meghibásodása esetén, a csoport autonóm módon újrarendezi az adat szétoszlást kommunikálva minden csomóponttal, a teljes operáció talpraállásáig.

Környezet

Ráadásul a Multiversum környezet barát: az egyik fő célunk, hogy csökkentsük a szükséges számítási erőt a kriptográfiai érvényesítéshez, ennek érdekében elkerülve a bányásza-

tot (proof of work), az erő és az erőforrások hatalmas pazarlását.
Ez az idejétmúlt technika helyett, implementáljuk a Proof of Integrity-t, egy olyan protokolt, ami úgy végzi el a kriptográfiai érvényesítést, hogy ellenőrzi a szoftver hitelességét, ami megszünteti a tranzakció minden fennmaradását.

Adatkezelés

Multiverzum a kripto-relációs adatbázissal könnyedén felépíti adatok összekapcsolásának korlátai nélkül.
Minden tárcának több állapota lesz, és egy személyhez (felhasználóhoz) lesz kötve; minden új tárca állapot változás két adatmezőt foglal majd magába:
az előző állapotot, az érvényesítés ellenőrzéséért.
az utolsó tranzakcióra mutató link (vagy az utolsó főlánc linkre)
szóval ismert lesz az új állapot változás linkjének eredete
A változás után, a tranzakciós módosítás hozzá lesz adva és a módosított láncszem újra kapcsolódni fog a főlánchoz.
Így az új tranzakció két hasht fog tovább vinni: egyet az állapot linktől, egyet pedig az előző tranzakcióból, ezúton minden művelet érvényesíti majd a tranzakcióhoz tartozó előző műveleteket.
Ez a fejlett megoldás, amely képes kezelni összetett adat forgatókönyveket, lehetővé teszi az embereknek, hogy bármiféle alkalmazást implementáljanak a technológiánkon, biztosítva világszerte intézményes, állami, pénzügyi és ipari diffúziót, az egész blockchain univerzumot egy lépéssel előrébb hozva.

MULTIVERSUM

HERE TO STAY

Unique Features !

Crypto relational DB
Autovalidating Complex Data structures

Divisible/Re-joinable chains
(Parallel Work)

Sharding data
(Parallel Work)

Minimal ecological footprint

Reciprocal chain confirmation
(Interoperability with other BC)

Advanced API offer

Native off-chain adapter for own ERC20
(Interoperability with other BC)

Java, Spring and Javascript
(Libraries for Integration)

Freezable wallets
(User Security)

Proof of Integrity
(Protocol Innovation)

Biometric Data integration as Electronic Signature seed
(User Security)

Double Access Lock
(Structural Security)

Reverse Access Denial
(Structural Security)

Rollback
(User Security)

Self managing Crypto-Cluster

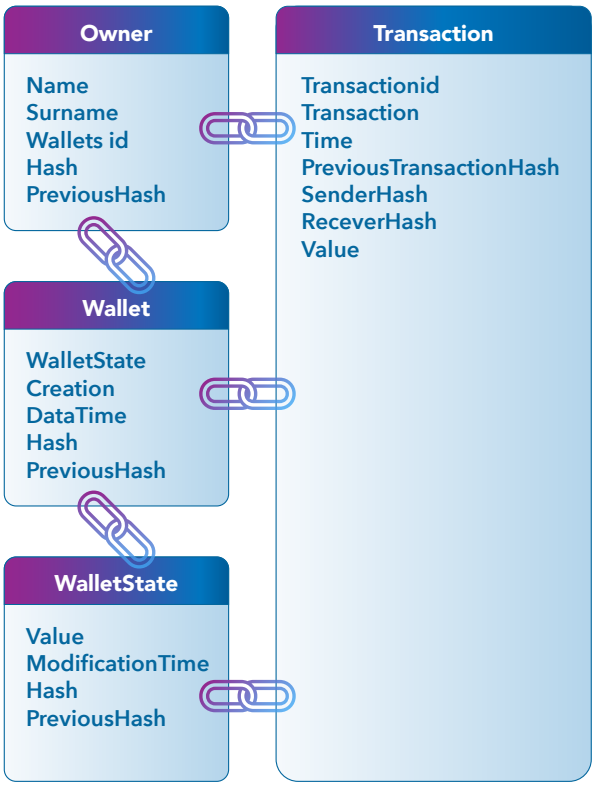
Native on chain adapter for own ERC20
(Interoperability with other BC)

ERC23
(Interoperability with other BC)

A Multiversum Küldetés

A multiverzum célja egy generáció előrelépés a blockchain világában és Egyedi értékesítési pontként az alábbi célkitűzéseket tettük :

1. Egy önazonosító, összetett adatrendszerekkel ellátott, relációs kriptoadatbázis létrehozása
2. A rendszer jelenlegi terhelésére alapozott szétválasztható/újraillleszthető láncok
3. Adattördelés (Párhuzamos munka)
4. Fejlett API
5. Biztonsági visszaállítás (Felhasználóbiztonság)
6. Fagyasztható tárcák (Felhasználóbiztonság)
7. Biometrikus adatok felhasználása az elektronikus aláírás magjainak
8. ERC 23 (átjárhatóság más blockchainekkel)
9. Natív, láncon kívüli fogadók, saját ERC20/ERC23 (átjárhatóság más blockchainekkel)
10. Natív, láncon kívüli fogadók, vendég ERC20/ERC23 (átjárhatóság más blockchainekkel)
11. Proof of Integrity (Innovációs Protokkol)
12. Kétszeri-hozzáféréses zár (Struktúrális Biztonság)
13. Kölcsönös hozzáférés megtagadása (Struktúrális Biztonság)
14. Reciprokális láncmegerősítés(átjárhatóság más blockchainekkel)
15. Java, Spring és Javascript integrálása
16. ACID modell
17. Tranzakciós modell
18. SQL-szerű nyelv



1. Egy önazonosító, összetett adatrendszerekkel ellátott, relációs kriptoadatbázis létrehozása

A Multiversum hivatásának tekinti az ipari és intézményi területeken való igénybevételt, ahol az adatokat összetett struktúrákban tároljuk, lehetetlen, hogy hatékonyan és rendezetten egyetlen láncként kezeljük őket.

A célunk, hogy mi legyünk az első kriptorelációs kriptoadatbázis a piacon, decentralizálva vagy egyszerűen szétosztva ha szükséges.

A lehetőség a láncolható egységek megvalósításából ered: technológiánkban az elsődleges lánc képes másodlagosokká osztódni, amelyek különböző egységek csoportjait és feljegyzéseket tartalmaznak.

Majd ezek az egységek újra összeállnak az utolsó fázisukban és a megfelelő változtatások után a fő lánc utolsó elemébe kapcsolódnak, ezzel újra egészet alkotva. A láncolható felület előre feltételez egy olyan rekordfélét, ami kettő- vagy több hash-t tartalmaz az előző rekordokból. Nem cask egy, hanem több alláncot azonosítva így.

A Multiversumnál szabványos végrehajtást alkalmazunk, ami Versum Coin által használt, az egységek amik együttesen léteznek a láncon négy csoportra tagolódnak : Felhasználó, Tárca, Tárca állapot, Tranzakció, egymáshoz kapcsolódva reciprokálisan megerősítve önmagukat.

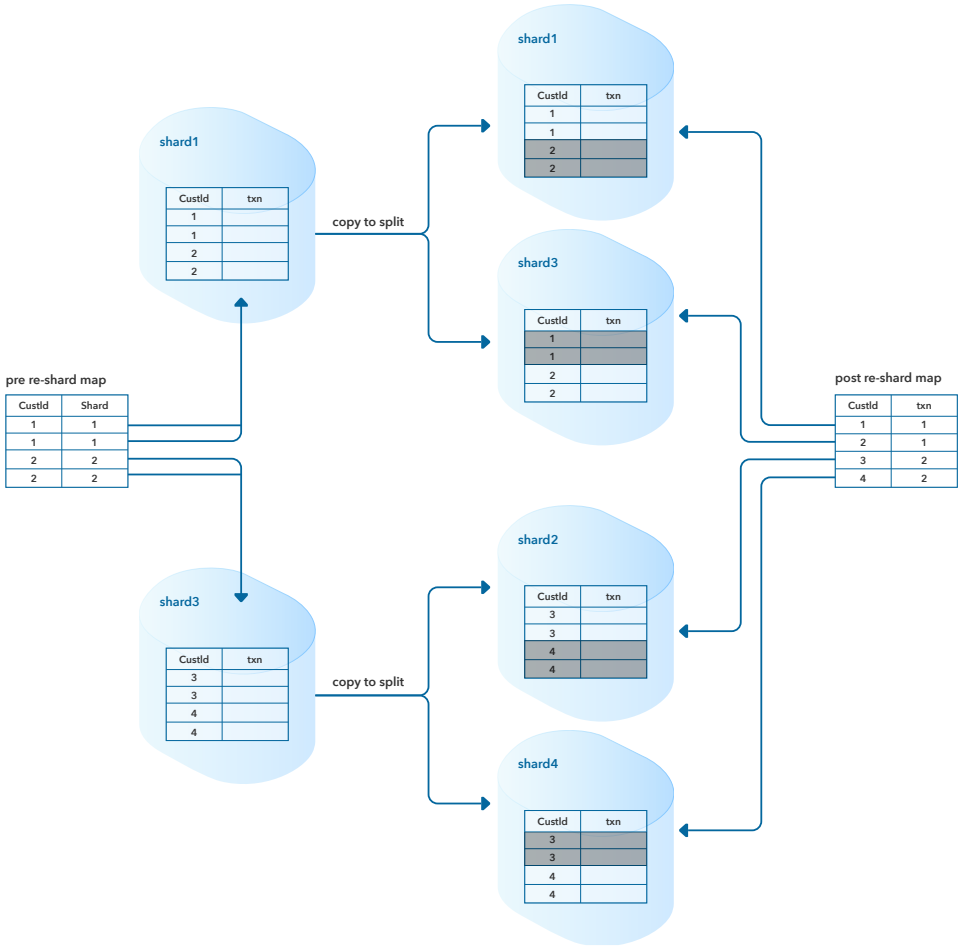
2. Szétválasztható / újraillleszthető láncok, a rendszer jelenlegi munkaterhelésére

alapozva(Párhuzamos Munka)

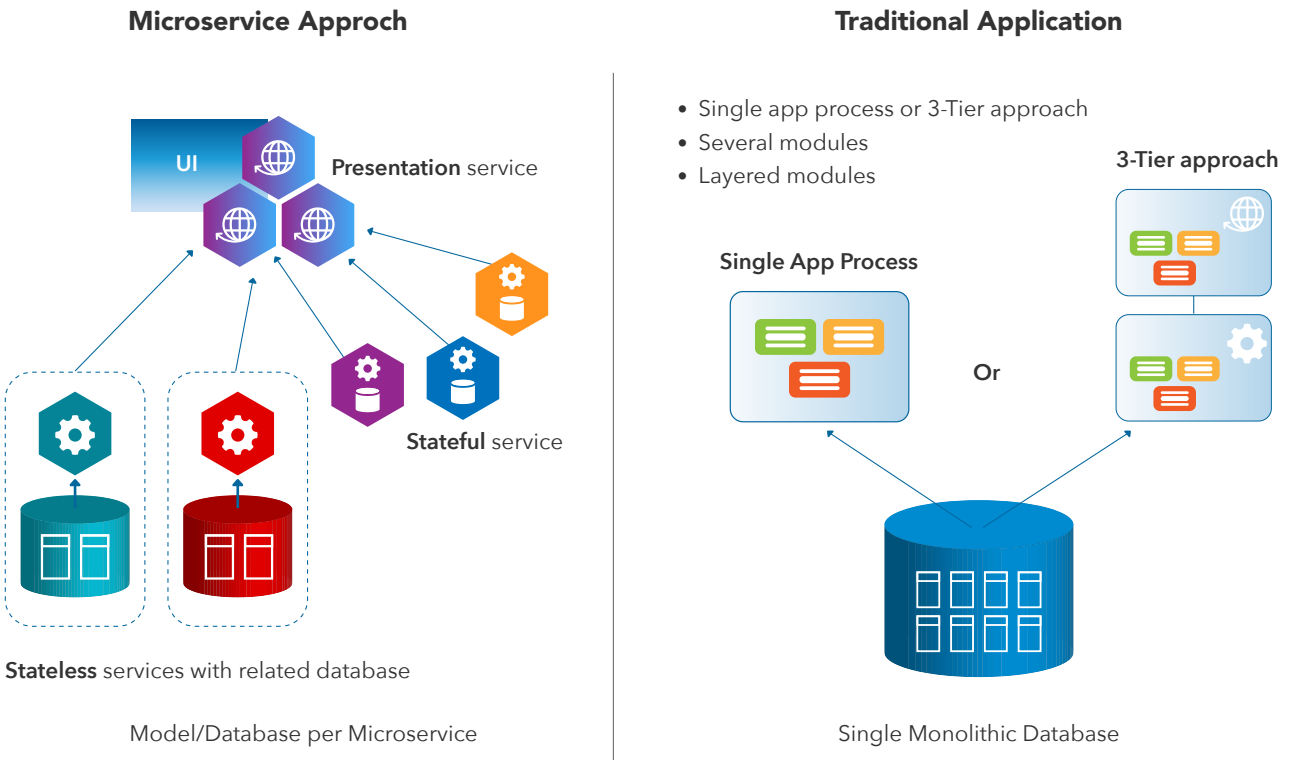
Az a képesség, amelyik lehetővé teszi, hogy egy adott láncszemtől több másikat is elválasszunk és újraegyesítsük őket,technikailag utat enged a munkaterhelés-elemzésnek, ez a clusterre mutat, illetve arra a szükségre, hogy az elsődleges láncot két másodlagos láncá válasszuk (hogy lehetőleg továbbá is szétválljanak), amikor nagy számban hajtódnak végre tranzakciók. Amint a munkaterhelés újra lecsökkent, a meglévő alláncok enegedélyt kapnak, hogy visszacsatolódjanak és érvényesüljenek. Ez a működési elv lehetőséget ad a párhuzamos munkára, miközben biztonságot garantál a tranzakció feljegyzésének.

3. Adattördelés (Párhuzamos munka)

Minden egyes csomópont tartalmazni fogja az összes láncadatot vagy a lánc adatainak egy töredékét. Amikor az adattördelés szükséges, az irányító csomópontok speciális adatfelosztási módokat állítanak be, annak érdekében, hogy ezzel optimalizálják a saját felosztásukat a jelenlegi munkaterhelés függvényében. Figyelembe véve a jelenleg elérhető technológiát, a megbízhatóság és a strapabírás mindig biztosítva lesz, még a cluster egyes részeinek hirtelen elvesztése esetén is, azáltal, hogy minden esetben a csomópontok 50%+1 része fennmarad. Ezek a csomópontok képesek arra, hogy egy részleges cluster összeomlás esetén újraterjeszkedjenek és újrarendezzék az adatszerkezeteket, azért,



hogy képesek legyen egy újabb részleges cluster összeomlás minnél hamarabbi elbírására. A 2. és 3. módszer által, a Multiversum blockchain fokozott párhuzamos munka végzésére képes és nagy adattördelési kapacitással bír, ez vízszintes skálázhatóságot eredményez, fokozott biztonságot, könnyebb elérhetőséget, rendszerszintű ellenállóképességet, minden hibalehetőség hiányát és önvisszaállítást katasztrófa esetén is.



4. Mikroszolgáltatás struktúra és fejlett API kínálata

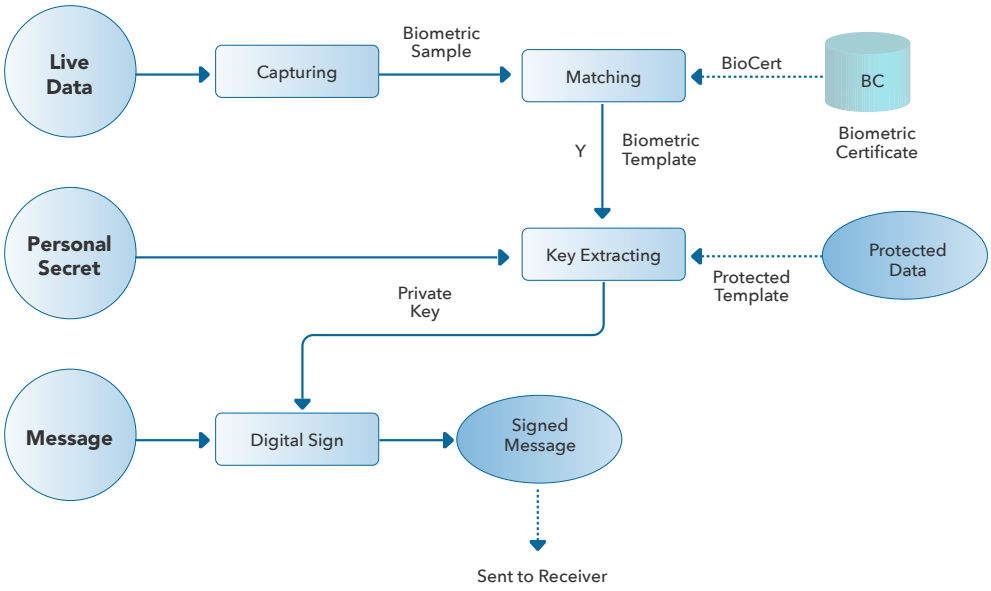
Egy mikroszolgáltatásokra és szerver nélküli modellekre alapozott platformon fejlesztett rendszerként, a Multiversum képes lesz arra, hogy fejlett biztonságot és modern API funkcionalitásokat biztosítson, mindkét struktúrán alkalmazkodóképes legyen.

5. Biztonsági visszaállítás

Technológiánk egy tranzakciós környezetben, lehetővé teszi a nemkívánatos műveletek visszaállítását, azaz visszaállít egy korábbi fázist a hitelesítés és a lánc érvényesítésének megbontása nélkül, különböző tranzakciós visszatérési pontok implementálásával. Ennek a korábbi tranzakciós visszaállítási állapotok készletének implementálása ad teret. Ez a funkció engedélyezhető, opcionálisan minden tokenre és alkalmazásra, amit a Multiversum blockchain kínál.

6. Fagyasztható tárcák (Felhasználó biztonság)

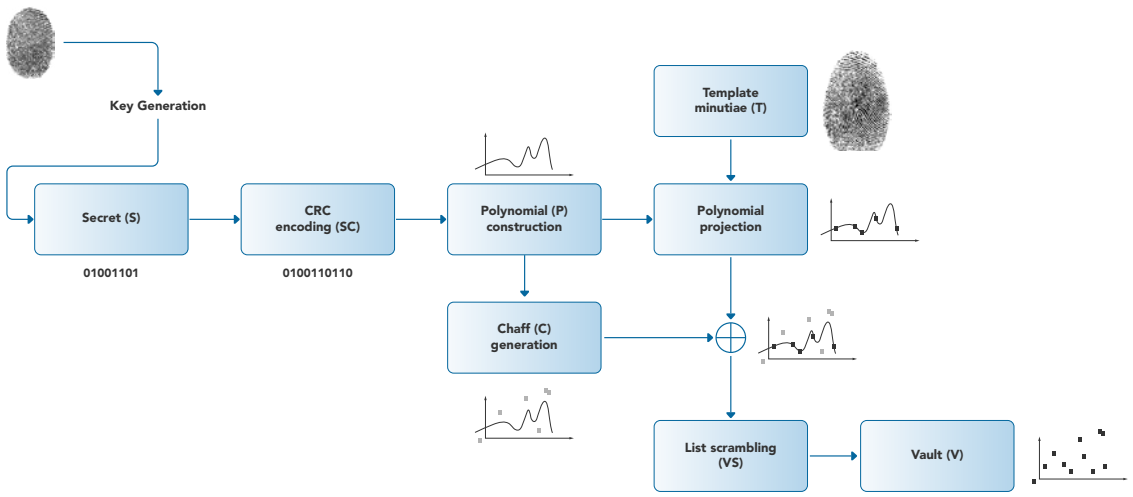
Esélye, hogy egy tárca fagyasztása lehetőséget implementáljon, törvénytelen vagy gyanús cselekedetek esetén, a használhatóságát megvizsgálva az üzleti logika oldalán.
Szabadalmazott alkalmazások, beépítve a Multiversum blockchainbe, opcióként implementálhatják ezt a funkciót, ha igényelt.



Biometric Digital Key Generation Framework

7. Biometrikus adatok felhasználása az elektronikus aláírás magjainak

Je-Gyeong Jo, Jong-Won Seo and Hyung-Woo Lee kutatási munkája nyomán, a Multiversum csapata felméri a biometrikus adatok, mint ujjlenyomat, retina olvasó és grafometrikus aláírás lehetőségét, egy aszimetrikus kriptográfiai kulcs forrásának és a felhasználó eredeti személyiségének garanciájának.
Értékelni fogják a titkosított adatok biztonságát, és a használhatóságot jogi viták érvényesítésénél.
Továbbá biometrikus adatokat fognak használni Androidon, IOS és más platform alkalmazásain, a felhasználó biztonság kivitelezésében.



Fuzzy Vault Scheme for Biometric Digital Key Protection

8. ERC23 felület (átjárhatóság más blokkláncok között)

A Verzum implementálja az ERC23 felületet, ami visszamenőlegesen kompatibilis az ERC20 felülettel, így garantálja az átjárhatóságot más láncokkal.

```
int totalSupply();
int balanceOf(String walletId);
boolean transfer(String receiverWalletId, int value);
boolean transferFrom(String senderWalledId, String receiverWalletId, int value);
boolean approve(String spenderWalledId, int _value);
int allowance(String walletId, String spenderWalledId);
boolean Transfer(String senderWalledId, String receiverWalletId, int value);
boolean Approval(String walletId, String spenderWalledId, int _value);
```

9. Natív, láncon kívüli adapter szabadalmazott ERC20/ERC23-hoz (átjárhatóság más blokkláncok között)

A Multiverzum ki fog fejleszteni egy natív adaptert, hogy lehetővé tegye a befele és kifele történő forgalmat a sajat érméi és más, nem saját láncok között.

10. Natív, láncon kívüli adapter külső ERC20/ERC23-hoz (átjárhatóság más blokkláncok között)

A Multiverzum ki fog fejleszteni egy natív adaptert, hogy lehetővé tegye a befele és kifele történő nem saját láncokról származó érmék forgalmát a saját láncán.

Integrity

11. Integrity - Teljesség

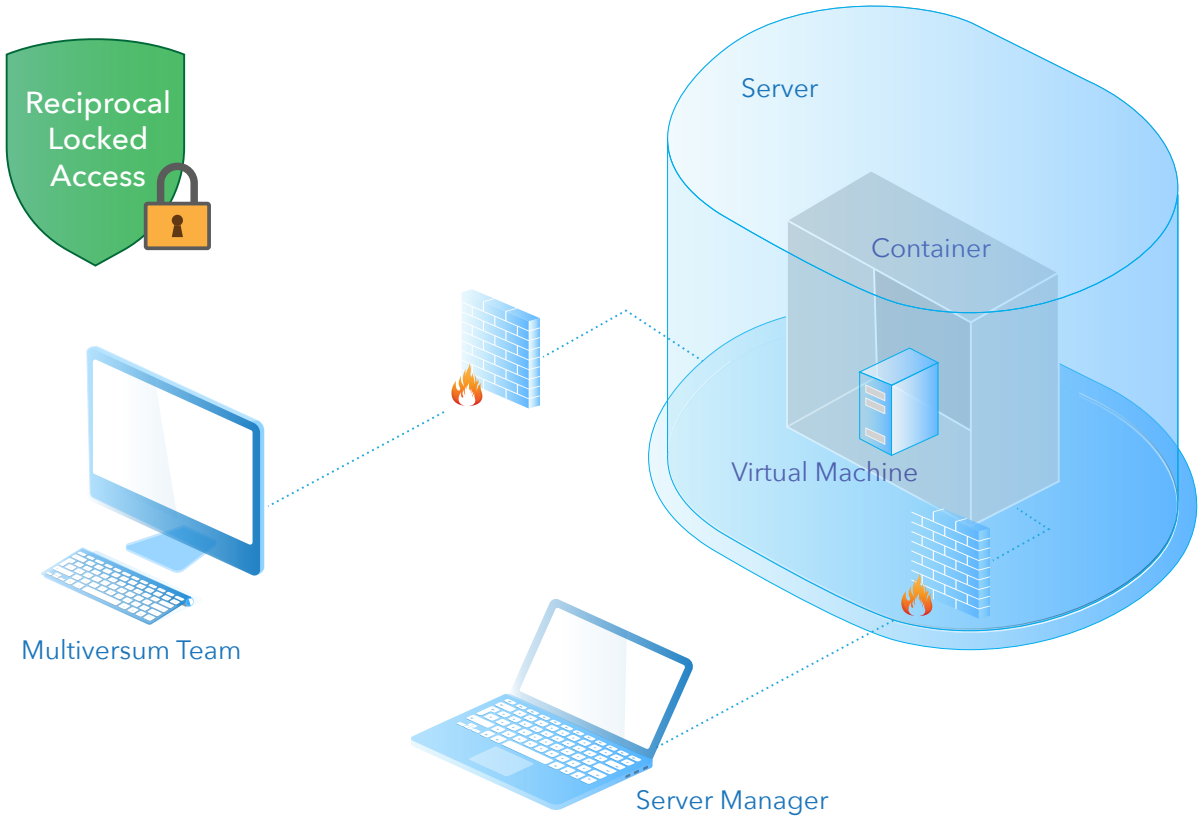
Egy új megoldásként az Proof of work/Elvégzett Munka Bizonyíték illetve Proof of stake/ Részesedési Bizonyíték protokollok helyett, a Multiverzum bevezeti a Teljességi Bizonyíték protokollt: egy olyan algoritmus csoportot, amelyek képesek kriptografikus módon hitelesíteni egy csomópont érvényességét és a csomópontok többsége által adott válaszok uniformitását. A hitelesítés egy véletlenszerűen kiválasztott "mag" érték ellen zajlik, kombinálva egy külső komponens által a szoftverből kiszámolt ún. "hash" értékkel (a külső komponens védett a kód visszafejtés ellen, és a kommunikáció védett csatornán történik), és a tranzakciós adattal. Ahhoz, hogy egy tranzakció érvényes legyen, a fenti kalkuláció eredményének ugyanannak az értéknek kell lennie az összes csomóponton, az adott tranzakcióra nézve.

Ez a folyamat figyelemre méltóan kevés számítási teljesítményt igényel, megelőzi a más blokk érvényesítő protokollokra tipikusan jellemző energiapazarlást, további szerketeti biztonságot ad, és nem alapszik sem a statisztikai, sem a Bizánci Konszenzus modelleken, amelyek kis csoportokban meglehetősen sebezhetőek.

Access Denied

12. Dupla Hozzáférési Zár (Szerkezeti biztonság)

A csomópontok biztosított Virtuális Konténerekben kerülnek szétosztásra, így a belépési adatok (felhasználónév, jelszó) nem lesznek elérhetők a gazda gép operátora számára, kizárva a hozzáférést; így a biztonság a Linux Biztonság legjobb gyakorlatain alapszik, pl. SeLinux vagy más disztribúciók. Mindeközben, ha valakinek megszerezné a vendég gép belépési adatait, továbbra sem tudna hozzáférni, hiszen nem tud belépni a gazda gépre ami a csomópontot futtatja. A csomópont így tulajdonképpen egy dupla hozzáférési zár által van bebiztosítva.



13. Kölcsönös hozzáférés megtagadása (Struktúrális Biztonság)

A 12. pontban leírt hozzáférési zár magába foglal egy kölcsönös kizárást a csomópont hozzáféréshez, mind a gazda gép működtetőinek és mindazoknak, akik majd a csomópont hitelesítő adatait birtokolják; ez biztosítja, hogy minden csomópont, ami nem közvetlen a Multiversum által irányított, hiteles és elérhetetlen akárki számára, tulajdonképpen önálló és izolált külső emberi beavatkozásoktól. Három alapvető összetevő lesz szétosztva a konténeren belül az operációs és a biztonsági rendszereken felül: Multiversum szerver összeállított kód, egy igazolás asszimetrikus kulccsal hitelesíteni a Multiversum clustert, a 11. pontban leírt komponens, ami felelős a kiszolgáló kód hash, igazolás, felelős mag és tranzakciós adat alapján felelős számításáért.

Esetleg további opcionális biztonsági technikákat implementálnak, mint pl. automatikus frissítés a konténer hozzáférési igazolványokról, egy random jelszóval az összeállítási szakasz ideje alatt, megelőzés képpen, hogy senki se nyerhessen hozzáférést. Ez a mechanizmus esetleg a cluster elérési igazolásokhoz is adaptálva lesz.

14. Reciprokális láncmegerősítés(átjárhatóság más blockchainekkel)

Multiversum tanulmányozza egy külső lánc integráló komponens megvalósíthatóságát, ami képes tárolni más blokkláncok állapotát (tokenek váltásához) ezzel további érvényesítést és bizalmat nyújtva.

Ugyanez a technika használható, hogy Multiversum megossza a saját állapot érvényesítését más blokkláncoknak, kiszervezve a hitelesítését.

Egy specifikus felületet nyújt ehhez a funkcióhoz, amit szükséges népszerűsíteni már létező és jövőbeli blockchain megoldások között.

Ennek egy szerver nélküli összetevő lenne az alapja, ami elérhető a konténer összerakása után is, hogy lehetővé tegye az adapterek befogadását más láncok felé.

15.Java, Spring és Javascript integrálása

Multiversum csúcskategóriájú felületeket kínál funkcionális könyvtárakban csoportosítva Java, Javascript és valószínűleg más mainstream nyelvek számára, ezáltal technológiánk könnyedén adaptálható vállalkozási és ipari szinteken.

Fejlesztve lesznek integrációs modulok keretekkel, mint a Spring. Az ilyen könyvtárak megkönnyítik a Multiversum integrációját szabadalmazott megoldásokba, mind privát láncokba és hivatalos MainNetbe.

16. ACID model

A Multiverzum kielégíti az ACID paradigmát: ez a rövidítés kihangsúlyozza a tranzakciók által igényelt logikai tulajdonságokat.
Ahhoz, hogy egy biztonságos tranzakciós modell jöjjön létre, a következő tulajdonságokat kell implementálni:
Atomicitás: Egy tranzakció nem osztható több részre a végrehajtásában, és a végrehajtásnak mindenképpen teljesnek vagy semmisnek kell lennie; részleges végrehajtás nem megengedett.
Consistency: Bármely tranzakciónak az adatbázist egyik érvényes állapotból a másikba kell juttatnia. Az eltárolt adatnak mindenképpen érvényesnek kell lennie az adott szabályrendszernek megfelelően.
Izoláció: A tranzakciók végrehajtásának teljesen elszigetelt módon kell megtörténnie: egy esetleges hibás tranzakció semmilyen mértékben nem befolyásolhatja a többi éppen végrehajtodó tranzakciót.
Durabilitás: Nevezik még perzisztenciának is, lényege, hogy ha egyszer egy tranzakció megtörtént, az eredmény semmiképp sem veszhet el, legyen bármiféle rendszer összeomlás, hiba, vagy áramkimaradás.

17. Tranzakciós Modell

A Multiverzum az adatokat tranzakcionális modell szerint tárolja, azaz biztosítja, hogy vagy az összes, vagy semennyi adat sem kerül tárolásra az al-láncokról, igy kényszerítve ki minden egyes végrehajtott tranzakció következetességét és az adatok teljességét.

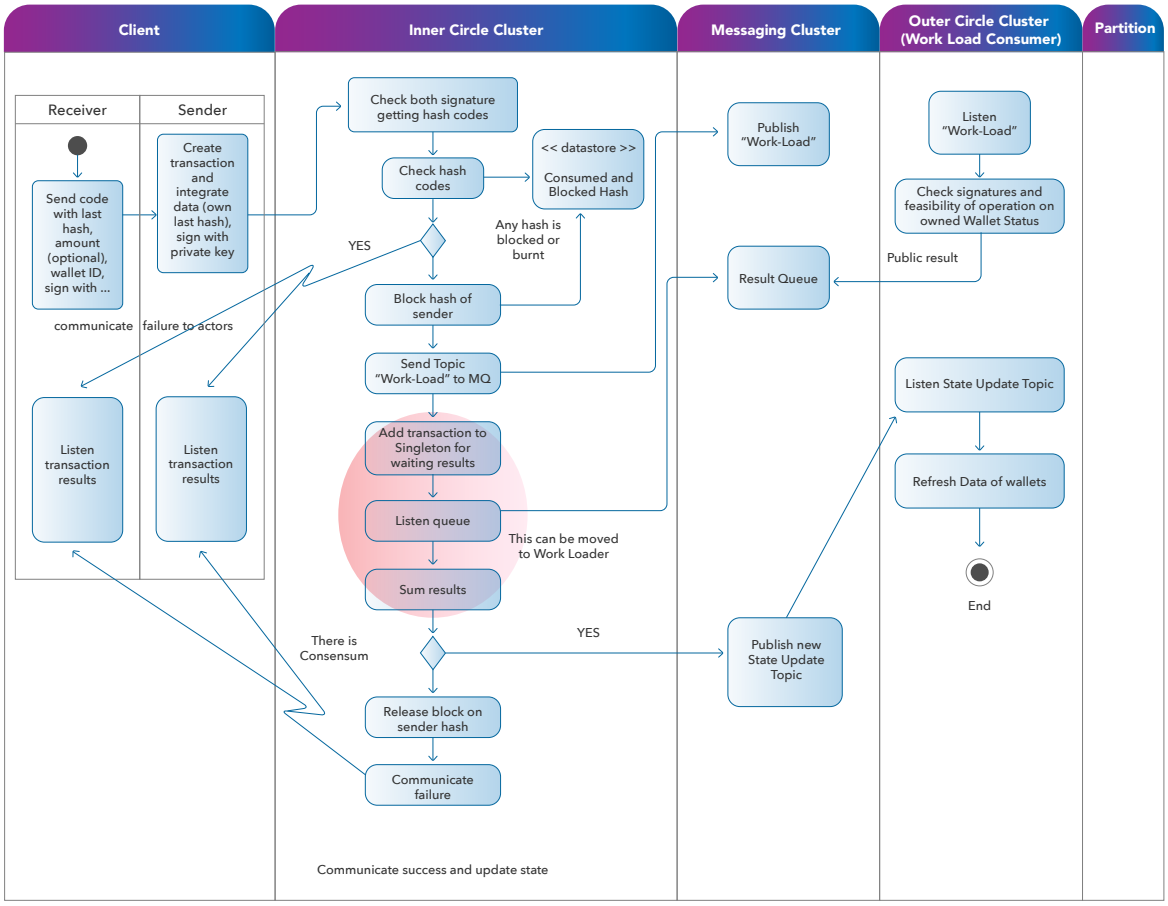
18. SQL-szerű nyelv

Hogy egyszerűbbé tegyük a Kripto-Relációs Adatbázisunkon alapuló alkalmazások fejlesztését és enyhítsük a más technológiákhoz viszonyított tanulási görbét, a Multiverzum tartalmazni fog egy SQL alapú szintaxist az alapvető tárolási funkciók alkalmazásához.

19. Teljes adatfolyam útvonal

A tranzakciók elfogadási, vezérlési, érvényesítési és tárolási folyamatai a következő egyszerűsített séma alapján fognak zajlani:
A privát kulccsal aláírt tranzakció és a szükséges adatok egy REST klienshez futnak be; a REST kliens elküldi az a tranzakciót egy koordinációs csoport vezér csomópontjához, ami pedig továbbitja a feladatokat a különböző csomópontokra egy saját koordinációs protokoll alapján; A csomópontok először ellenőrzik az adatok teljességét, az aláírás hitelességét, a források meglétét, a már felhasznált hash-eket, továbbá, hogy naprakész-e a tárca állapota, blokkolt-e a tárca vagy a felhasználó;
Bármely más művelet ugyanezzel a küldő ID-val blokkolva van a volatilis memoriában, mi-

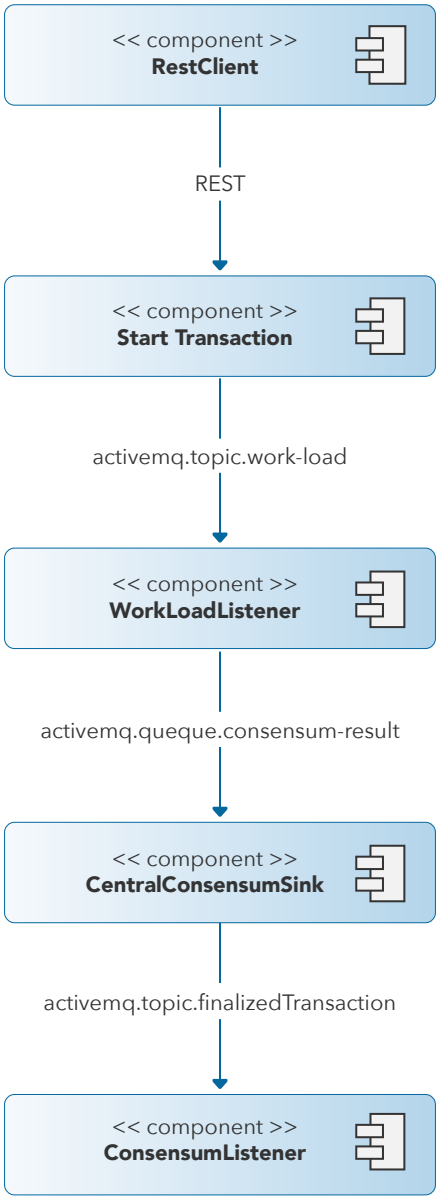
közben a különböző adatmezők inicializálásra kerülnek (mint például hivatkozás az előző tranzakciókra, időbélyeg és előző hash);
A tranzakció ezután továbbítódik egy üzenetküldési rendszerre, aminek a protokollja később kerül definiálásra
(AMPQ a bevezetés idejére, MQTT és egyéb protokollok később) és ezzel párhuzamosan szétosztásra kerülnek a dolgozó csomópontok között;
A dolgozó csomópontok megerősítik az érdeklődésüket a kérés feldolgozása iránt (lehetséges, hogy hiányoznak szükséges adatok, éppen elfoglaltak, illetve egyéb feltételeket is

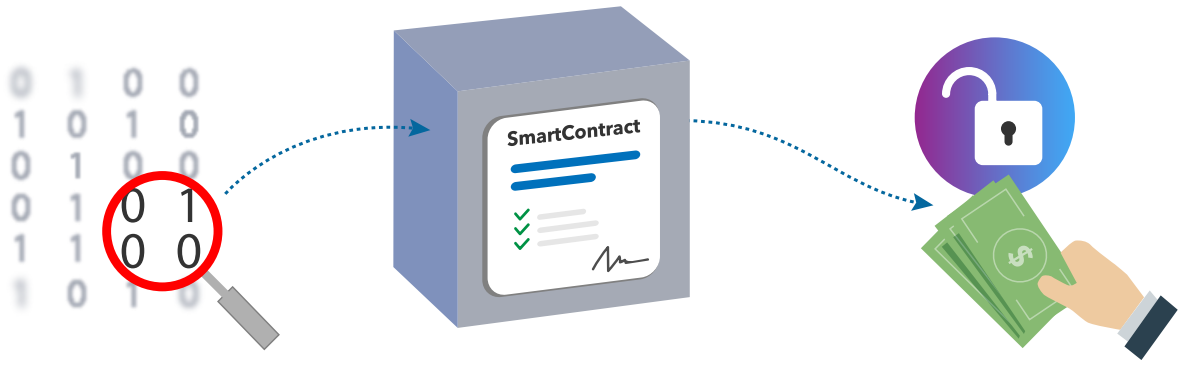


ki kell értékelni), majd ezután létrehozzák az új tárca állapotot, felállítják a korábbi hash-eket a hivatkozott tranzakciókból, majd iktatják ezeket. Hozzáadódik a Teljességi Bizonyíték eredménye; Kiszámítódik a tranzakciós hash; A dolgozó csomópontok bejegyzik a tranzakciót a memóriába, majd elküldenek egy szavazatot a koordinációs csomópontok felé egy üzenetküldési rendszeren keresztül, összegyűjtve az eredményeket; Ha a szavazatok és a hash-ek koherenciát mutatnak, a koordinációs csomópontok eltárolják a tranzakciót és az új tárca állapotokat, majd szétsugározzák a szavazat érvényességét egy további üzenetküldési rendszer segítségével. Ezután a dolgozó csomópontok szintén eltárolják a tranzakciót és a tárca változásokat.
A folyamat ismertetésének ezzel vége.

Logikus adat folyam

Részletes folyamatleírás





Okos szerződések

Habár a Multiverzum hisz az okos szerződések továbbfejlesztésére tett javaslatok fontosságában, jelen írás keletkezésének idejében, úgy döntött - amennyiben nem történik változtatás a kutatási területeket illetően -, hogy nem deríti fel ezt a lehetőséget. Ezek alapján várhatóan azt az Open Source technológiát fogjuk alkalmazni ezen a területen, amely az igényeinket a legjobban kielégíti.

Infrastruktúra

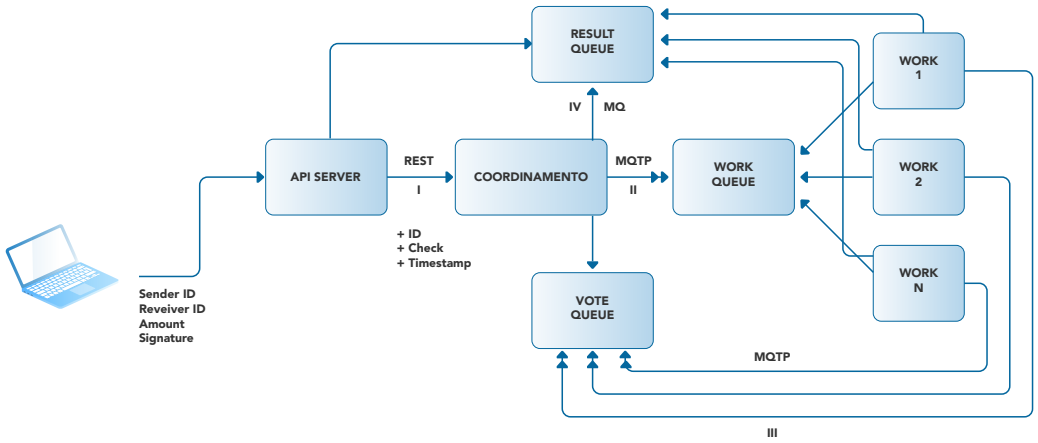
A Multiverzum infrastruktúráját úgy terveztük meg, hogy biztosítsa a rugalmasságot és az elérhetőséget. Ezt úgy értük el, hogy olyan csomópont csoportokat fejlesztettünk ki, amelyek képesek önműködő módon szerepeket kiosztani maguk között, a technológiai specifikációknak megfelelően, amelyek a következők:

- Számítási teljesítmény
- Memória méret
- Reciprokális késlekedés
- Lánc adat teljesség
- Gép elérhetőség
- Kétségek a Teljességi Bizonyítékot illetően

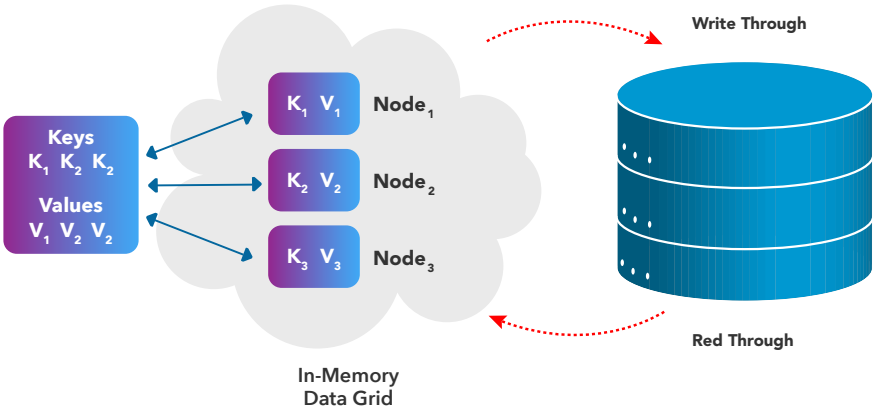
A csomópontok a következő szerepeket vehetik fel:

- Kliens csomópontok
- Koordinációs csomópontok
- Üzenetküldő csomópontok
- Dolgozó csomópontok
- Tároló csomópontok
- Biztonsági mentési csomópontok

Bármely csomópont, amely képes egy érvényes igazolás felmutatására, regisztrálhat a há-



lózaton és szerepet kaphat.
Egy vagy több csomópont összeomlása esetén, a hálózat képes automatikus módon újraosztani a feladatokat, optimalizálva a különböző szerepeket.
JVM-en belüli osztott cache elérhető lesz mint memórián belüli adatbázis, ami a következőket teszi lehetővé:
Keresztülolvasás, azaz adatolvasási kérések direktben a volatilis memóriában futnak, mielőtt a fizikai memóriából olvasnának

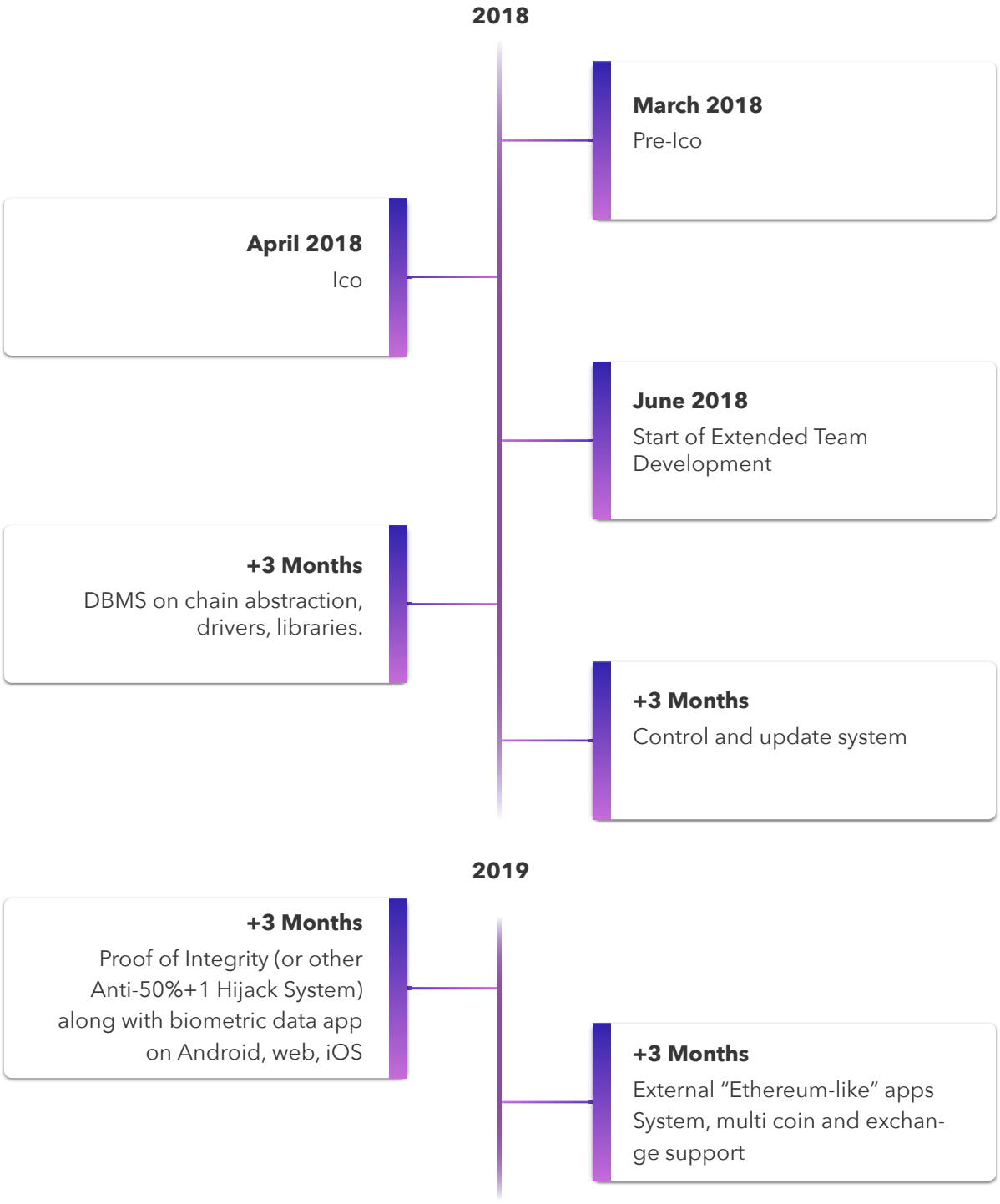


Keresztülírás, azaz az adatok az optimális teljesítmény elérése érdekében először a volatilis memóriába kerülnek, mielőtt egy tömeges behelyezés keretében fizikailag tárolódnak

Megjegyzések a biztonságot illetően

A fejlesztés során díjakat fogunk felajánlani azoknak, akik sebezhetőséget fedeznek fel és előállnak megoldási javaslatokkal.

Technical Road Map

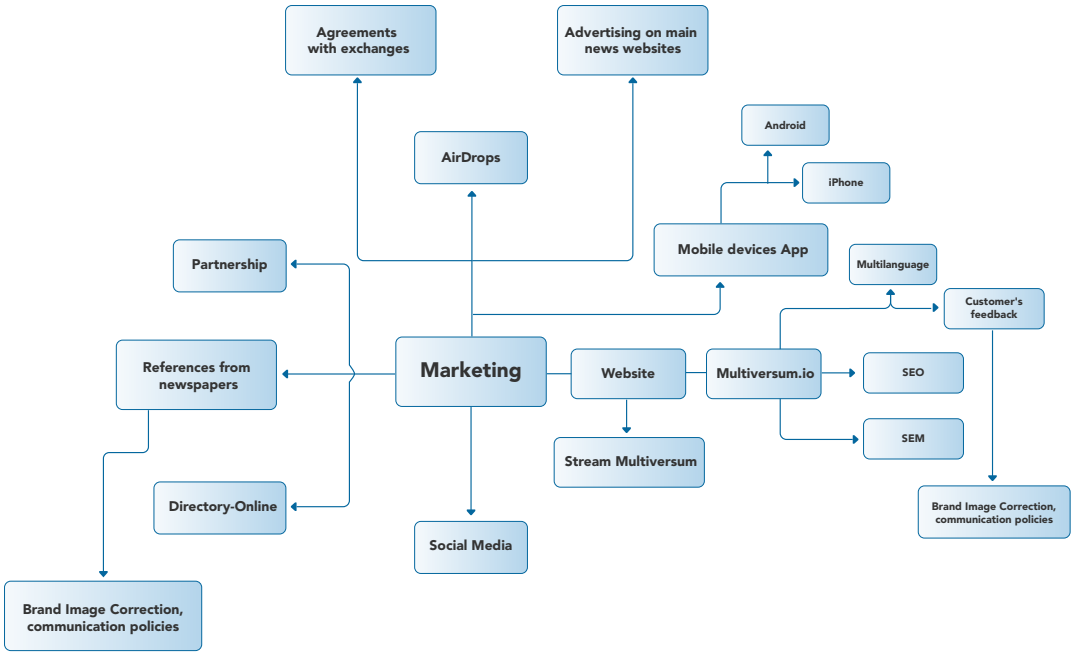


Marketing terv

A folyamatosan változó IT piacon, frissíteni fogjuk a stratégiánkat, kommunikációs technikánkat és a vállalat küldetését, szem előtt tartva, hogy értéket képviseljünk az ebben érdekelteknek és biztosítsuk a helyén való egyensúlyt a rövid és hosszú távú irányítási logikában.

A terv kulcspontjai:

- Vállalat küldetés
- Üzleti célok
- Üzleti stratégiák
- Üzlet aktivitásának portfolioja



Az egyik fő eszköz a Social Media Marketing lesz: szociális hálón folytatott kampányok, hogy növeljük a márkaismertséget, megtaláljuk a potenciális fogyasztókat, kontaktokat generáljunk, és kiépítsük a kapcsolatot a fogyasztókkal.
A Social Media Stratégiáink különböző cselekvésekből állnak, amelyek mind egy tervnek a részei, kezdve a különböző csatornák kezelésére és megfigyelésére alkalmas eszközök haasználatával és közösség fejlesztéssel, összpontosítva a tartalom, kölcsönhatások és taktikák hatékonyságának értékelésére az elért eredmények alapján.

Az univerzumot fedő elemek rétegei mind tízszerese az előttelévőnek, és az összes univerzum egymásbafürtözve olyan, mint az atomok egy hatalmas kombinációban.

Bhagavata Purana 3.11.41

MULTIVERSUM

HERE TO STAY