MULTIVERSUM

HERE TO STAY

WHITE PAPER v 1.0.5

Zakelijk Technisch

Nederlands

06.02.2018

Authors: Multiversum Team

www.multiversum.io

Er zijn een oneindig aantal universums naast deze, en ondanks dat ze ongelimiteerd groot zijn, bewegen ze zoals de atomen in jou.

Bhagavata Purana 6.16.37

Contents

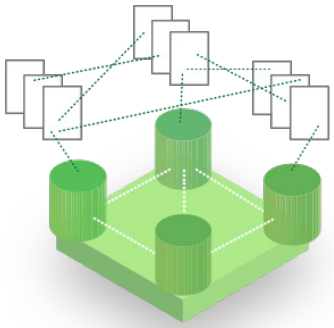
Identiteit en missie Multiversum

Bitcoin is de pionier onder de cryptocurrencies. Samen met al zijn verschillende klonen en takken die gebaseerd zijn op het Proof of Work algoritme voor transactie validaties worden beschouwd als de eerste generatie blockchains (grootboeken).
De tweede generatie, waarbij Ethereum de leider is onder de blockchains met de mogelijkheid tot smart-contracten, zijn meer heterogeen. Dit vereenvoudigt het omzetten van activa in tokens, oftewel tokenisatie.
Beide bouwwerken hebben een extreem lage energie efficiëntie en tevens een gemiddelde tot lage blokvalidatiesnelheid en aantal transacties per blok. Het doel van de derde-generatie blockchains is om problemen op het gebied van schaalbaarheid, snelheid en het energieverbruik op te lossen.
Dit wordt gedaan aan de hand van verschillende benaderingen en technieken zoals het Proof of Stake validatie algoritme, off-chain routing, graph-chains en volledige of gedeeltelijke centralisatie.
De vierde generatie gaat zelfs veel verder dan dit en bereikt snellere en meer schaalbare oplossingen. Ook probeert deze generatie tegelijkertijd concurrerend te worden vanuit een zakelijk perspectief. Eenvoudige ketens van gegevens zijn niet voldoende om te voldoen aan de behoeften van de bedrijfsomgeving, waarbij complexe datastructuren moeten worden georganiseerd (zoals in relationele databases).
Tegelijkertijd moeten deze structuren worden gevalideerd en bestendig worden gemaakt met technieken op basis van blockchains. Hierdoor nemen de traceerbaarheid en veiligheid toe. In andere woorden maakt de vierde generatie blockchains deze technologie tot een complete primaire productieapplicatie. Het zorgt ervoor dat het huidige bedrijfsgerichte aanbod uit te breiden is in gegevensopslag, decentrale toepassingen, controle, veiligheid en betrouwbaarheid.
Multiversum biedt een complexe data organisatie (in plaats van data ordening, splitsing van ketens of het opnieuw verbinden) om grotere schaalbaarheid en parallellisme mogelijk te maken. Het concept van Proof of Integrity validatie (oftewel cryptografisch bewijs van integriteitsvalidatie) in plaats van de bestaande Proof of Work of Proof of Stake oplossingen.
Tevens zal Multiversum voorzien zijn van ERC20/ERC23 integratie waardoor munten en tokens van andere oplossingen in onze keten kunnen worden gehost en vice versa. Notariële diensten zullen hierbij als een externe beveiligingsmethode worden gebruikt. Ondertussen zullen we, samen met deze innovaties, gebruik maken van verschillende goede oplossingen die in de loop van de tijd door onze collega's zijn geïmplementeerd.

Multiversum

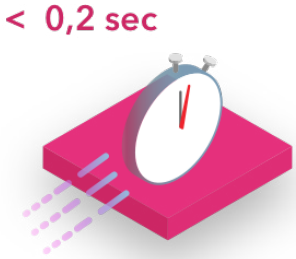
De vierde generatie relationele blockchain

Waarom is Multiversum de 4.0 Blockchain?



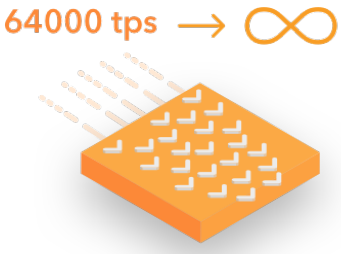
Relationele Blockchain

Een geheel nieuwe Blockchain die verschillende soorten gegevens bevat en zich bevindt in een multidimensionale structuur.



Transactie snelheid

Geldmiddelen kunnen In minder dan 0.2 seconden worden overgemaakt tussen portefeuilles met de zekerheid van een veilige validatie van de transacties. Hiermee is Multiversum een van de snelste ter wereld.



Transactie doorvoer

Ongeëvenaarde schaalbaarheid: tot 64.000 Tps (1000 Tps/core) op een 64 cores-server.

Bewijs van integriteit

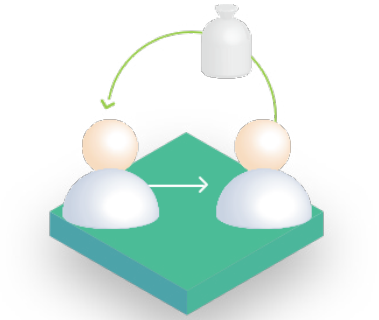
PoS (Proof of Stake) wordt vervangen door PoI (Proof of Integrity).

Next Generation Wallet

Baanbrekende beveiliging in toegang en geld-transfers met biometrische invoer.

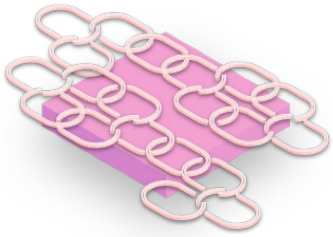
Eco-vriendelijk

De kosten van een Multiversum transactie zijn onbeduidend en er is vrijwel geen ecologische voetafdruk.



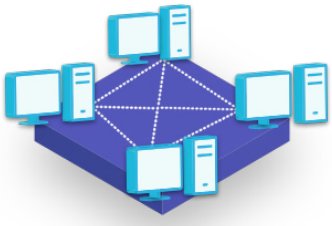
Rollback

Operationele Rollback kan geactiveerd worden op door Multiversum gehoste tokens.



Deelbare ketens

Optimalisatie van bronnen tussen knooppunten dankzij scheidbaarheid.



Toewijzing van herstelknooppunten

MTV-knooppunten zijn verspreid over de hele wereld voor betrouwbaarheid en wereldwijd nood-herstel.

Publieke presentatie

Huidige blockchain is State of the Art

De hoofdrolspelers van het Blockchain fenomeen delen een gemeenschappelijke kenmerk, namelijk een bijzonder hoge mate van veiligheid en betrouwbaarheid. Tegelijkertijd betalen we hiervoor in termen van grote verwerkingscapaciteit, onacceptabele vervuiling, hoge transactiekosten en traagheid. Deze factoren geven nauwelijks de huidige technologische vooruitgangsnormen weer en geven slechts een schappelijk technisch antwoord op moderne financiële en commerciële use cases.
Deze traagheid wordt veroorzaakt door het ontbreken van horizontale schaalbaarheid[1]. Dit wil zeggen dat de toename van de berekening-capaciteit is verkregen door processors toe te voegen in plaats van deze te vervangen voor snellere versies. Een andere oorzaak van deze traagheid is inherent aan het huidige Blockchain veiligheid-mechanisme. Dit mechanisme is ontworpen om te voorkomen dat iemand de meerderheid van de clusters overneemt. Door het heel duur te maken is dit erg moeilijk te realiseren in termen van rekenkracht en/of kosten (Proof of Work[2] and Proof of Stake[3]).
Bovendien zijn huidige Blockchains eenvoudige combinaties van enkele veranderingen in de status van data eenheden. Het reconstrueren van de werkelijke toestand van deze eenheden houdt in dat een scan van de gehele keten nodig is. Dit zorgt voor een nog grotere vertraging in het systeem- en bronnengebruik.
Deze vereenvoudiging maakt Blockchains ontoereikend voor wetenschappelijke en industriële doeleinden omdat de eisen met betrekking tot datastructuren buitengewoon complex kunnen worden. Verder stoppen beveiligingsmaatregelen op gegevensniveau. Dit betekent onder andere dat de veiligheid van gebruikers niet kan worden gegarandeerd. Ook is het onmogelijk om gestolen munten en tokens te herstellen, zelfs als ze zich in de keten bevinden. Daarnaast kunnen kwaadwillende accounts niet worden geblokkeerd.
Tot slot zijn fragmentatie en homogeniteit onder cryptocurrencies die niet met elkaar kunnen communiceren en leven in niet-gerelateerde universums een probleem.

Wereldwijde acceptatie van Multiversum Blockchain

De Multiversum technologie duwt de traditionele blockchain verder dan zijn huidige limieten. Dit wordt gerealiseerd door de gegevenslaag te verbeteren via zelfverificatie en gedistribueerde structuren van georganiseerde data eenheden die onderling verbonden zijn door symbolische koppelingen.
Deze technologie vormde de basis voor een gedecentraliseerd en gedistribueerd system van samenhangende zelf-controlerende transacties, oftewel het Multiversum Blockchain. Multiversum staat, in plaats van het bestaande eenvoudige model voor blockchain, de creatie toe van een Relationele Crypto Database (een geavanceerde en georganiseerde oplossing voor gegevensopslag). Deze database kan niet alleen een enkel gegevenstype aan maar is zelfs in staat om een reeks gegevens gegroepeerd in grafieken van complexe datastructuren die aan elkaar gerelateerd zijn te verwerken. Relaties worden nu gezien als eersteklas burgers in de blockchain en worden verzekerd door cryptografische methodes.
Wanneer er om een verandering van status wordt gevraagd, kan ieder van hen splitsen in een eigen sub-keten van de oorspronkelijke tak. Vervolgens zullen deze na de operatie weer samenkomen om geldig te worden verklaard.
Daarom is Multiversum een geëvolueerde blockchain-technologie die unieke functies biedt omtrent het overwinnen van eerder geanalyseerde ongemakken met een verzameling aan cryptovalidatie en distributietechnieken geschikt voor elke omgeving: administratief, industrieel, financieel en overheid.
Een van de belangrijkste doelen van Multiversum is om de markt op ieder moment het meest geëvolueerde product dat beschikbaar is te bieden. Dit kan gerealiseerd worden door het toepassen van een AGILE[4] softwareontwikkelingsmethode.
De AGILE methodologie betekent een drastische vermindering van de aanvankelijke betrokkenheid bij het projectontwerp. Dit komt de valorisatie van de ervaringen die zijn aangetroffen tijdens de projectontwikkeling ten goede. Het toont aan dat kansen en bedreigingen op voorhand nauwelijks voorspelbaar zijn. Vervolgens is het van belang de beste werkwijzen te belonen en de inadequate werkwijzen achter je te laten.
AGILE is een gevestigde standaard voor softwareontwikkeling die ontwikkelaars, producteigenaren en investeerders aanspoort om project scope[5] te overwegen en te zien als flexibel en eenvoudig aanpasbaar aan marktbehoeften. In een snel evoluerende sector als software, betekent het vrijgeven van een product na een studie van zes maanden en een jaar van implementatie dat in feite een verouderd product wordt aangeboden. Het product werd achttien maanden geleden ontwikkeld onder de toen geldende behoeftes in de markt. Dit houdt in dat het product enkel antwoord kan geven op verouderde

problemen die inmiddels misschien zijn opgelost door concurrenten en een gebrek aan antwoorden heft op zojuist gemaakte uitdagingen.

AGILE daarentegen, biedt de kans om tegen de tijd van levering het meest innovatieve product op de markt te bieden.

Snelheid en technologie

Een van de sterkste punten van deze technologie is inderdaad snelheid. Dit dankzij het vermogen om verschillende transacties parallel uit te voeren en het split-rejoin mechanisme van onze Blockchain. Deze functies zorgen voor een grotere horizontale schaalbaarheid en een verhoging van de capaciteit om transacties te verwerken. Dit wordt bereikt door rekenkracht toe te voegen aan de al bestaande, waardoor iedere knoop prestatiewijs telt.

Horizontale schaalbaarheid

Multiversum profiteert van twee specifieke functies om de efficiëntie van het systeem te optimaliseren:
1- De hoofdketen kan zijn structuren optimaliseren door zichzelf op te splitsen in meerdere subketens. Volgens gevraagde bronnen en datastromen is het werk evenredig verdeeld over draden en knooppunten. Dit proces van keten-splitsing wordt uitgevoerd tot de werklast weer is teruggekeerd tot normaal, en wanneer de keten nog steeds onafhankelijk is zal deze weer een geheel worden. Dit alles is mogelijk dankzij een techniek die elke blok in de keten in staat stelt om twee verschillende subketens van twee verschillende inkomende links te valideren.
2 – Data Sharding[6], in andere woorden een techniek die gegevensdistributie tussen meerdere knooppunten mogelijk maakt. Ter illustratie, in geval van een ABC-gegevensreeks en drie kloosterknooppunten zal de gegevensdistributie er als volgt uitzien:

AB

BC

CA

Deze onderverdeling maakt een hogere verwerkingssnelheid van transacties mogelijk, aangezien gegevensvragen alleen van invloed zijn op subketen-knooppunten, waarbij elke stap wordt geoptimaliseerd.
Een ander uiterst belangrijk kenmerk van onze technologie is High Availability[7]: de mogelijkheid

om te vertrouwen op een clustertype dat de continuïteit van services garandeert, zelfs in het geval van het stil liggen van sommige knooppunten in het netwerk.
In het bovenstaande voorbeeld (A-, B- en C-knooppunten), zou C offline moeten gaan terwijl A- en B- nog steeds volledig operationeel zouden moeten blijven. Hierdoor is continuïteit van de dienstverlening mogelijk, zonder enige vorm van gegevensverlies. 50% + 1 van de knooppunten blijft actief.
Op deze manier zal het cluster in geval van een storing met meerdere knooppunten de gegevensdistributie zelfstandig reorganiseren en communiceren met elk knooppunt tot het bereiken van volledig operationeel herstel.

Milieu

Multiversum is eco-vriendelijk: een van onze hoofddoelen is het verlagen van de rekenkracht die nodig is voor cryptografische validatie. Hierdoor wordt mijnbouw (Proof of Work), wat een enorme verspilling van kracht en middelen is, vermeden.
In plaats van het gebruiken van deze verouderde techniek implementeren we Proof of Integrity, een protocol dat cryptografische validatie uitvoert door de authenticiteit van de software na te kijken die elke persistentie van de transactie oplost.

Data management

Multiversum, met zijn crypto-relationele database, kan de koppeling van gegevens gemakkelijk en zonder beperkingen structureren. Elke portefeuille heeft een reeks states en wordt gekoppeld aan een persoon (gebruiker) en een nieuwe portestatuswijziging bevat twee gegevensvelden:

- De vorige state, om de validatie te controleren
- Een link naar de laatste transactie (of naar de laatste hoofdkettinglink) zodat de herkomst van de nieuwe state change link bekend is. Na de wijziging wordt de verandering van de transactie toegevoegd en keert de gewijzigde statuslink terug naar de hoofdketen.

Om deze reden neemt de nieuwe transactie twee hashes over: één van de statuslink en één van
de vorige transactie. Op deze manier zullen alle bewerkingen de vorige handelingen valideren die gerelateerd aan de transactie zelf.
Deze geavanceerde oplossing die in staat is om complexe datascenario's te beheren, zal mensen in staat stellen om elke vorm van toepassing op onze technologie te implementeren. Dit zal leiden tot een verspreiding van wereldwijde institutionele, overheids-, financiële en industriële mogelijkheden waarmee het gehele blockchain-universum een stap vooruit kan zetten.

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

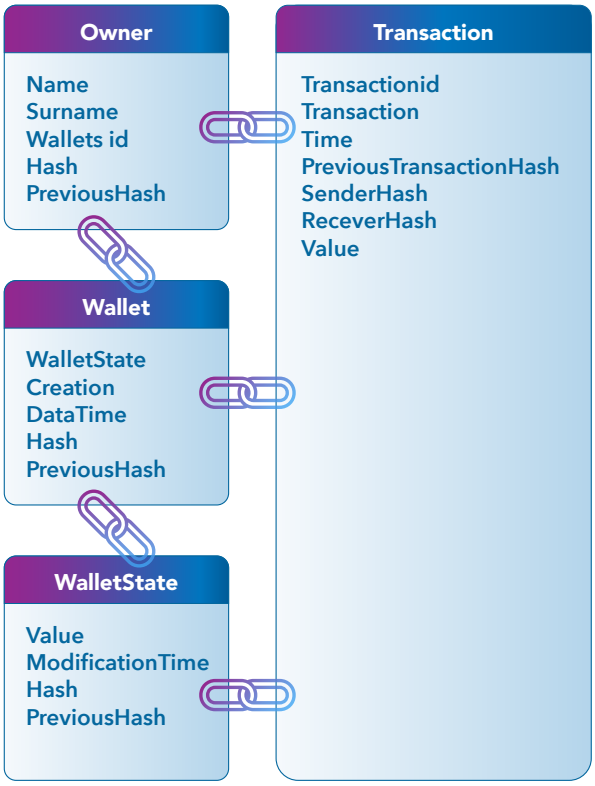
Native on chain adapter for own ERC20
(Interoperability with other BC)

ERC23
(Interoperability with other BC)

De missie van Multiversum

Multiversum streeft naar een generationele stap vooruit in de blockchain-wereld en USP (Unieke verkoop proposities) stellen we de volgende doelstellingen voor:

1. Realisatie van een Crypto-Relationele DB met zelf-validerende Complexe Gegevens Structuren
2. Deelbare/opnieuw koppelbare ketens op basis van de huidige systeembelasting (Parallel werk)
3. Sharding van gegevens (Parallel Werk)
4. Geavanceerd API aanbod
5. Rollback (Gebruikersveiligheid)
6. Bevriesbare portefeuilles (Gebruikersveiligheid)
7. Integratie van biometrische gegeven als startpunt voor elektronische handtekeningen
8. ERC23 interface (Interoperabiliteit met andere BC)
9. Oorspronkelijke off-chain adapter voor eigen ERC20/ERC23 (Interoperabiliteit met andere BC)
10. Oorspronkelijke off-chain adapter voor eigen ERC20/ERC23 gasten (Interoperabiliteit met andere BC)
11. Bewijs van integriteit (Protocol innovatie)
12. Dubbel toegangsslot (Structurele veiligheid)
13. Reverse Access Denial (Structurele veiligheid)
14. Bevestiging van wederzijdse keten (Interoperabiliteit met andere BC)
15. Integratie voor Java, Spring en Javascript
16. ACID model
17. Transactioneel Model



1. Realisatie van een Crypto-Relationele DB met zelf-validerende complexe gegevensstructuren

Multiversum richt zich voornamelijk op industrieel en institutioneel gebruik. Dit zijn sectoren waar gebruik wordt gemaakt van gegevens met complexe structuren en waarbij het onmogelijk is om deze op een efficiënte en gewone manier weer te geven via een eenvoudige keten.

We hebben als doel gesteld om de eerste relationele crypto database op de markt te worden en zullen gedecentraliseerd zijn of gewoonweg gedistribueerd.

Dit vermogen komt voort uit het ontwerp van ketenbare eenheden: in onze technologie kan een primaire ketting opsplitsen in secundaire ketens, met verschillende series aan eenheden en

records.

Deze eenheden zullen zich opnieuw bij hun laatste aanhoudende state weer verenigen en zullen, na de nodige aanpassingen, weer opnieuw aansluiten bij de laatste schakel van de primaire keten en zo weer een geheel worden. De "ketenbare" interface veronderstelt een soort van record die twee of meer hashes omvat van de vorige records, waarbij niet alleen één maar meer subketens worden gevalideerd.

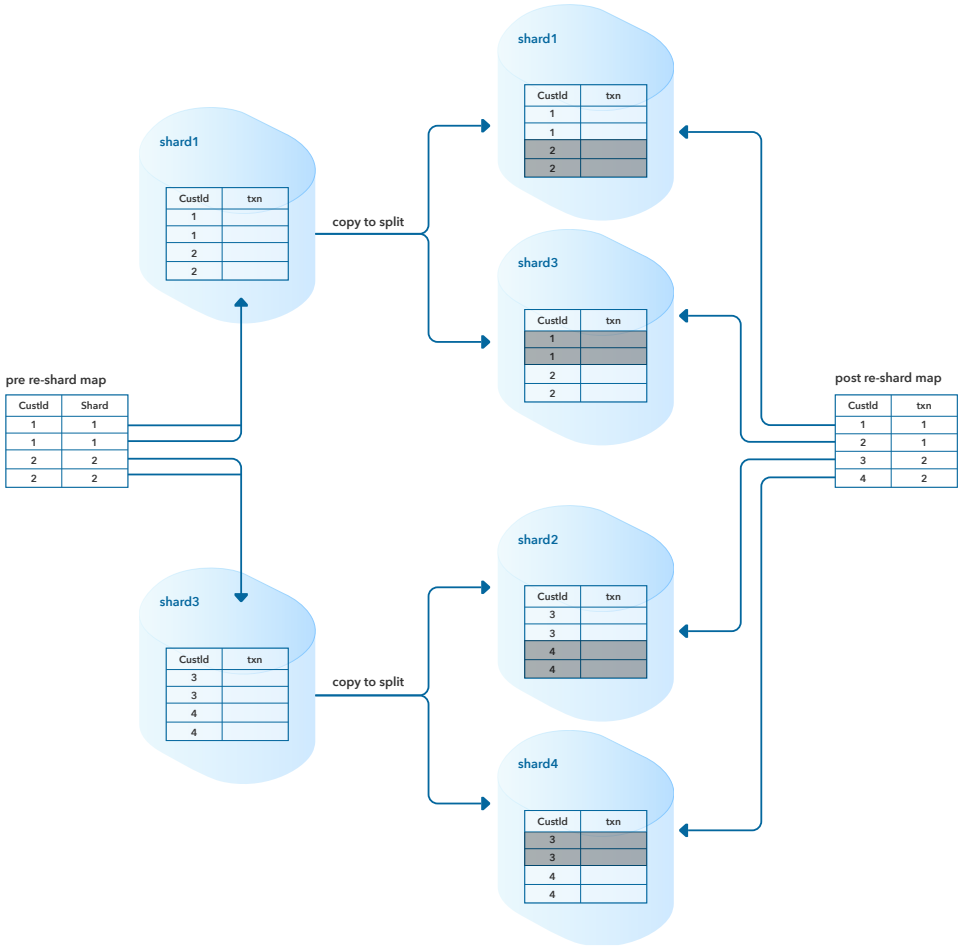
In de standaardimplementatie van Multiversum, die wordt gebruikt voor Versum munten, be-

horen de naast elkaar bestaande en ketenbare eenheden tot vier tabellen: Gebruiker, Portefeuille, Staat van portefeuille en Transactie. Deze zijn allen aan elkaar gerelateerd en wederzijds bevestigend.

2. Deelbare/opnieuw koppelbare ketens op basis van de huidige systeembelasting (Parallel werk)

Hetzelfde vermogen om meerdere links af te leiden van een gegeven link en terug te koppelen, stelt de technologie in staat om werklast-analisten te gebruiken. Deze zullen aangeven wanneer het noodzakelijk is voor het cluster om de primaire keten in twee secundaire ketens te splitsen (en zich mogelijk voor onbepaalde tijd opnieuw te splitsen) wanneer een hoge vraag naar transacties is. Zodra de werklast weer gedaald is, kunnen meerdere, vooraf bestaande subketens teruggekoppeld en gevalideerd worden. Dit mechanisme is in staat tot parallel werk terwijl tegelijkertijd de veiligheid van de transactie records wordt behouden.

3. Sharding van gegevens (Parallel Werk)

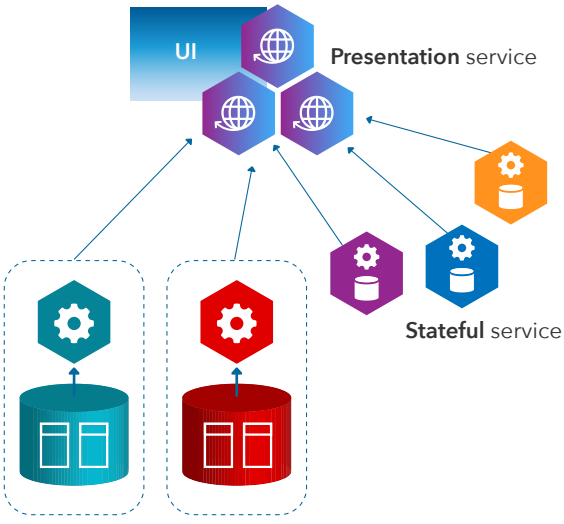


Elk knooppunt bevat de volledige of slechts een deel van gegevens van de keten. Wanneer sharding van gegevens nodig is, zullen coördinerende knooppunten specifieke wijzes van gegevensverdeling instellen, om hun eigen distributie op basis van de huidige werkbelasting te optimaliseren. Volgens de High Availability techniek zullen betrouwbaarheid en persistentie altijd verzekerd zijn. Zelfs in het geval van onverwachts verlies van een deel van het cluster, op voorwaarde dat minstens 50% + 1 van de knooppunten het overleeft.
Deze knooppunten kunnen na een gedeeltelijke clustercrash de gegevensstructuren opnieuw distribueren en reorganiseren om zo mogelijk een andere gedeeltelijke clustercrash te kunnen weerstaan.
Door middel van bovenstaande technieken 2 en 3 zal een Multiversum blockchain een verbeterd en evenwijdig proces hebben. Daarnaast zal er een verbetering te zien zijn in sharding van gegevens, wat weer leidt tot horizontale schaalbaarheid, verhoogde veiligheid, hoge beschikbaarheid, systeembestendigheid, afwezigheid van een enkel storingspunt[8] en zelfherstel na calamiteiten.

4. Microdienst-structuur en geavanceerd API aanbod

Multiversum is ontwikkeld aan de hand van een platform die gebaseerd is op zowel Microdiensten[9] en Serverloze modellen[10] waardoor het mogelijk is om geavanceerde, veilige en moderne API functionaliteiten aan te bieden die toepasbaar zijn op beide samenstellingen.

Microservice Approch

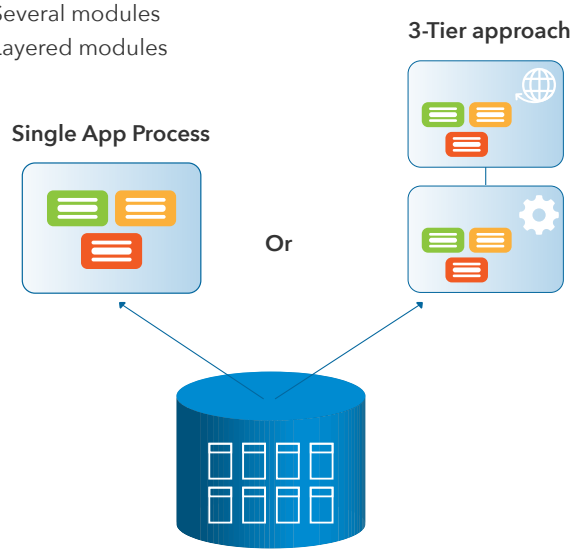


Stateless services with related database

Model/Database per Microservice

Traditional Application

- Single app process or 3-Tier approach
- Several modules
- Layered modules



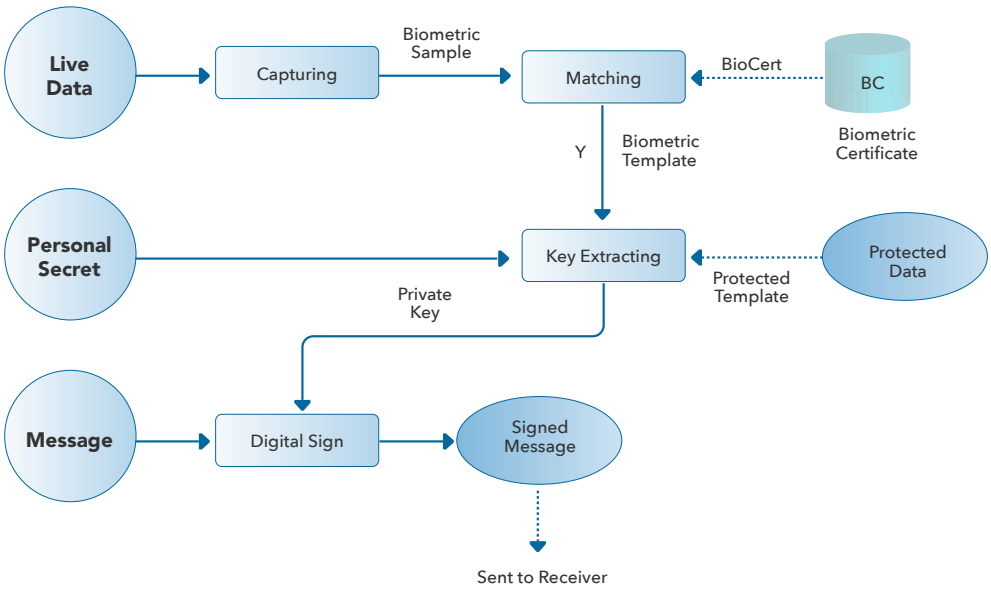
Single Monolithic Database

5. Rollback (Gebruikersveiligheid)

In een transactionele context zal onze technologie het mogelijk maken om rollbacks te maken van ongewenste operaties, in andere woorden een vroege toestand (state) herstellen zonder de geloofwaardigheid van ketenvalidatie te verstoren, door het implementeren van een reeks transactieherstellende states. Deze functie kan optioneel worden ingeschakeld voor alle tokens en applicaties die worden gehost op de Multiversum-blockchain.

6. Bevriesbare portefeuilles (Gebruikersveiligheid)

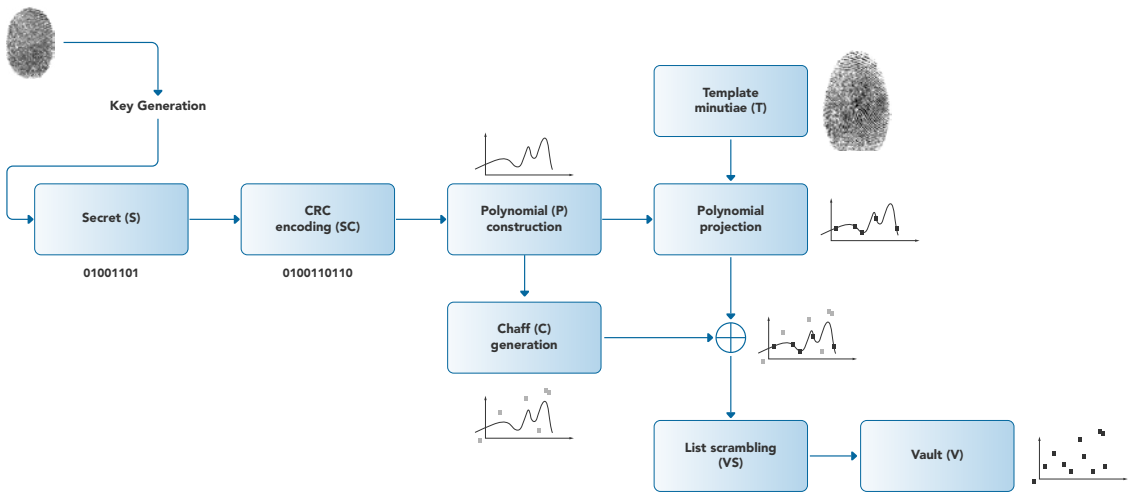
De mogelijkheid tot een functie voor het bevriezen van portefeuilles in geval van onwettige of verdachte activiteiten zal worden geïmplementeerd nadat de haalbaarheid ervan aan de Business Logic-kant is bestudeerd. Eigen applicaties, gebouwd op Multiversum blockchain, hebben de optie om deze functie desgewenst te implementeren.



Biometric Digital Key Generation Framework

7. Integration of biometric data as a seed for Electronic Signature

Vanuit het oogpunt van het door Je-Gyeong Jo, Jong-Won Seo en Hyung-Woo Lee's on-



Fuzzy Vault Scheme for Biometric Digital Key Protection

derzoekswerk[11] , beoordeelt het Multiversum team de haalbaarheid van het gebruik van biometrische gegevens. Voorbeelden hiervan zijn vingerafdrukken, irisscans en grafometrische handtekeningen. Deze worden gebruikt als bron voor asymmetrische, cryptografische sleutels om de authenticiteit van de identiteit van de ondertekenaar te garanderen.
Veiligheid van gecodeerde gegevens en hun gebruik ter validatie in juridische argumenten worden geëvalueerd. Bovendien worden biometrische gegevens gebruikt op Android, IOS en andere platforms en toepassingen voor het beheren van de gebruikersveiligheid.

8. ERC23 interface (Interoperability with other blockchains)

Versum munten worden ontwikkeld ter uitvoering van ERC23 interface, dat achterwaarts overeenstemmend is met ERC20[12] om te zorgen voor interoperabiliteit met andere ketens.

```
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. Oorspronkelijke off-chain adapter voor eigen ERC20/ERC23 (Interoperabiliteit met andere BC)
Multiversum ontwikkelt een eigen adapter waarmee de inkomende en uitgaande stroom van zijn eigen munten en penningen aan niet-gepatenteerde ketens wordt toegestaan.

10. Oorspronkelijke off-chain adapter voor eigen ERC20/ERC23 gasten (Interoperabiliteit met andere BC)
Multiversum ontwikkelt een eigen adapter waarmee de inkomende en uitgaande stroom van munten en penningen van niet-gepatenteerde ketens naar eigen keten wordt toegestaan.

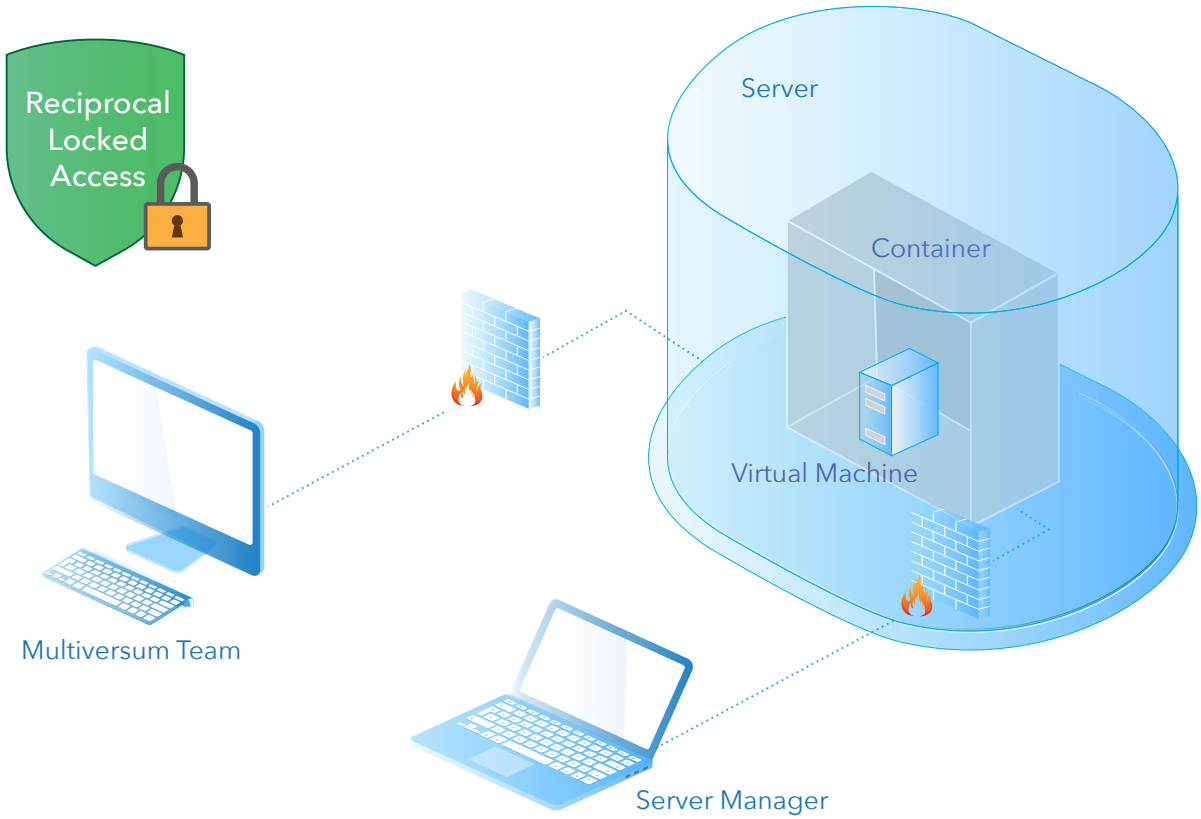
Integriteit

11. Bewijs van integriteit (Protocol innovatie)
Als een oplossing voor het vervangen van Proof of Work en Proof of Stake in alle verschillende vormen, komt Multiversum met Proof of Integrity. Dit is een set van algoritmes die in staat zijn om de cryptografische geldigheidsduur van een samengesteld knooppunt te verifiëren en de uniformiteit van de reactie van de meerderheid van de knooppunten te verifiëren. De keuring wordt gedaan tegen een willekeurige see-challenge. Dit wordt gecombineerd met de hash en berekend door een externe component (beschermd tegen reverse engineering, en communiceren met knooppunt-software via een gecodeerd kanaal) van de software zelf en met transactiegegevens. Met het oog op het valideren van een transactie, waarbij de uitkomst van deze berekening hetzelfde moet zijn voor een specifieke transactie, op elk knooppunt.
Deze procedure vereist een opmerkelijk lagere rekenkracht, waardoor afvalstoffen die typerend zijn andere blokvalidatie (PoW, PoS, DpoS) oplossingen worden voorkomen.
Het is voorzien van structurele veiligheid, die niet gebaseerd zijn op statistische modellen of Byzantijnse Consensus[13] modellen, deze zijn tamelijk kwetsbaar in kleine cluster

Toegang geweigerd

12. Dubbel toegangsslot (Structurele veiligheid)

Knooppunten worden gedistribueerd in beveiligde virtuele containers, met referenties die niet beschikbaar zijn voor de Host machine operator, deze verhindert toegang; daarom wordt de veiligheid verwezen naar Linux Security[14] Best Practices, zoals bijvoorbeeld SeLinux en/of andere pakketten. Wanneer iemand Guest-machine referenties heeft, is het voor hem nog steeds niet mogelijk om toegang te verkrijgen. De hostmachine die het betreffende knooppunt runt, weigert toegang. Het knooppunt is zogezegd beveiligd door een dubbel toegangsslot



13. Reverse Access Denial (Structurele veiligheid)

Het toegangs slot dat beschreven is bij punt 12 zorgt voor een wederzijdse uitsluiting van knooppunt toegang tot zowel host machine-operators en iemand die beschikt over de inloggegevens van knooppunten. Dit zorgt ervoor dat elk knooppunt dat niet rechtstreeks beheerd wordt door Multiversum authentiek en ontoegankelijk is en dus eigenlijk zelfstandig en geïsoleerd van extern menselijk ingrijpen. Er zijn drie fundamentele componenten die naast operationeel systeem en veiligheid worden verdeeld binnen een container: een door een Multiversum Server samengestelde code, een certificaat met asymmetrische sleutel ter authenticatie van een Multiversum cluster, een element reeds beschreven bij punt 11) die verantwoordelijk is voor de challenge berekening gebaseerd op server code hash, certificaat, challenge startpunt en transactiegegevens. Extra optionele beveiligingstechnieken kunnen worden ingevoerd, zoals een geautomatiseerde updatefunctie van containertoegang met een willekeurig wachtwoord tijdens de samenstelling fase, om te voorkomen dat iedereen toegang heeft. Dit mechanisme kan worden aangenomen voor een cluster toegangscertificaat.

14. Bevestiging van wederzijdse keten (Interoperabiliteit met andere BC)

Multiversum bestudeert de haalbaarheid van een externe component van de ketenintegratie waarbij het mogelijk is om states van andere blockchains op te kunnen slaan (uiteindelijk in ruil voor tokens) om zo in extra validatie en vertrouwen te voorzien.
Deze zelfde techniek kan worden gebruikt door Multiversum om zijn eigen state-validatie te delen met andere blockchains om zo verificatie uit te besteden.
Een specifieke interface wordt verleend voor deze functionaliteit, die weer gepromoot onder bestaande en toekomstige blockchain uitvoeringen.
Deze functie is gebaseerd op een serverloze component die ook toegankelijk is na het samenvoegen van een container voor het inbegrepen van adapters voor andere ketens.

15. Integratie voor Java, Spring en Javascript

Multiversum biedt high-end interface die gegroepeerd zijn in functionele bibliotheken voor Java, Javascript en mogelijk andere populaire talen waardoor onze technologie gemakkelijker kan worden overgenomen op zowel bedrijfs- als institutioneel niveau. Integratiemodules met Frameworks, zoals Spring[15] zullen ook worden ontwikkeld. Dit soort bibliotheken zullen de integratie van Multiversum in gepatenteerde oplossingen vergemakkelijken, zowel in privé ketens als officiele MainNet ketens.

16. ACID-model

Multiversum zal voldoen aan het ACID-model[16], deze afkorting legt de nadruk op de logische eigenschappen die zijn vereist voor transacties. Om te zorgen voor een veilig transactiemodel, moet de technologie voldoen aan de volgende eigenschappen:
Atomiciteit: Een transactie is niet deelbaar in zijn uitvoering en de uitvoering daarvan moet worden voltooid of nul zijn, gedeeltelijke uitvoeringen zijn niet toegestaan.
Consistentie: Elke transactie brengt de database vanaf een geldige staat naar de andere. Blijvende gegevens moeten geldig zijn volgens alle gedefinieerde regels.
Isolatie(afzondering): Iedere transactie moet worden uitgevoerd op een geïsoleerde manier: het mogelijke mislukken van een transactie mag niet in de weg staan van andere samenvallende transacties.
Duurzaamheid: Ook wel persistentie, staat erop dat zodra een transactie is aangegaan het resultaat niet kwijt wordt geraakt. Om welke reden dan ook (crashes, fouten, stroomuitval).

17. Transactioneel model

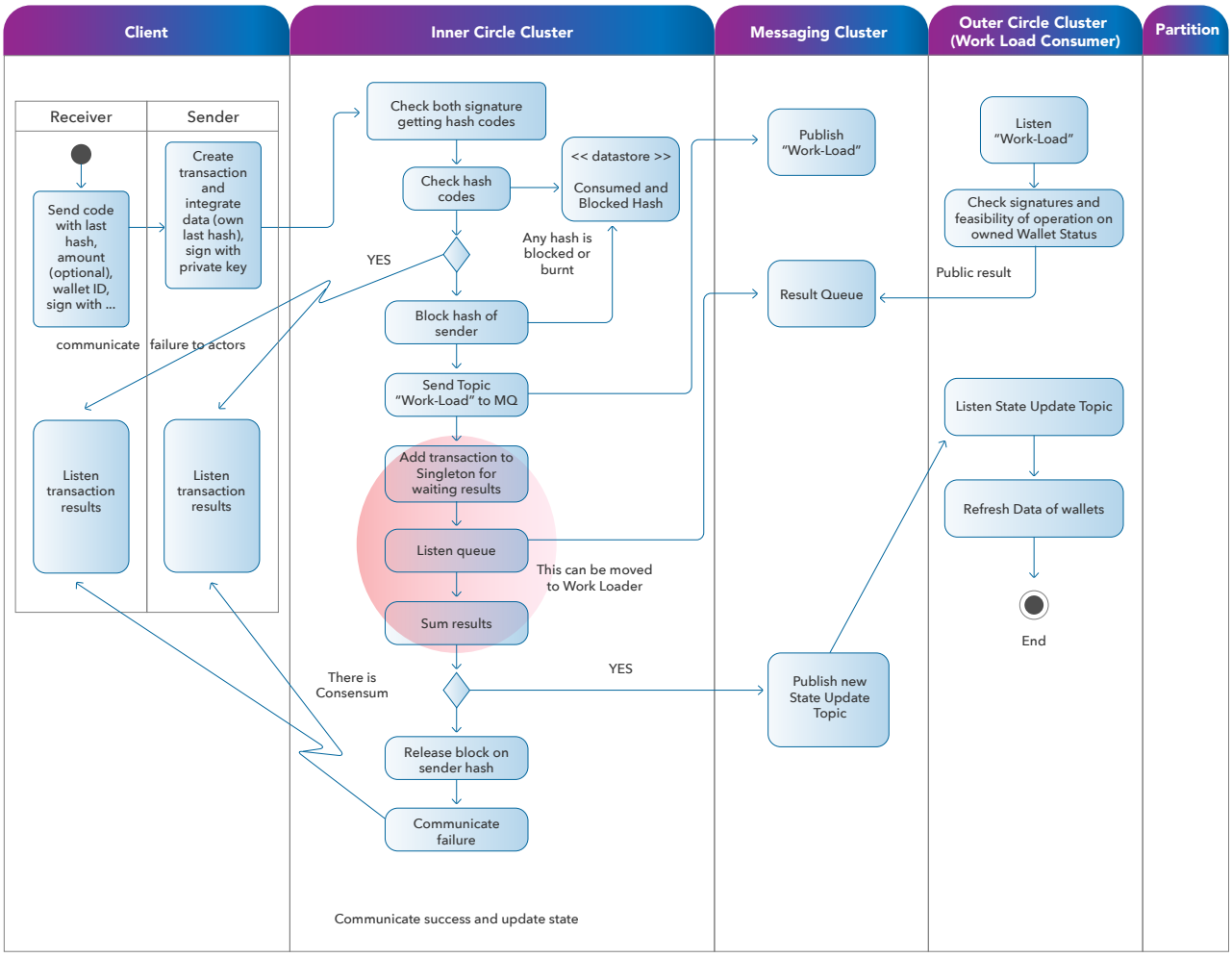
Multiversum zal transactiegegevens blijven behouden in een Transactioneel model[17]. Dit model zorgt ervoor dat alles van deze gegevens of helemaal niets van deze gegevens die verwikkeld zijn op verschillende sub-ketens worden aangehouden en gehandhaafd voor volledigheid van de gegevens.

18. SQL-achtige taal

Om de ontwikkeling van applicaties gebaseerd op onze Crypto-Relationele database technologie te vereenvoudigen en de leercurve te vergemakkelijken ten opzichte van bestaande technologieën zal Multiversum voorzien zijn van een SQL-gebaseerde[18] syntaxis voor persistente opslagfuncties (CRUD).

19. Full Route Data Flux

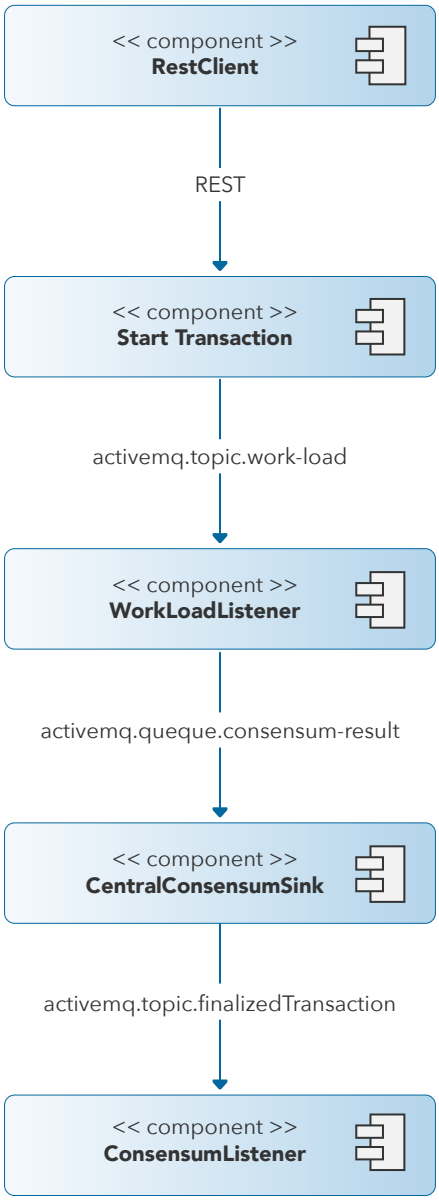
De processen van acceptatie, controle en validatie van de vasthoudendheid van een transactie vindt plaats met de volgende schematische en vereenvoudigde procedure:
de transactie is verzonden naar REST-cliënt, met haar noodzakelijke gegevens, ondertekend met privé-sleutel;
de REST-client stuurt de transactie naar een leidend knooppunt van coördinerende clusters: het splitst de werkzaamheden via knooppunten met een protocol voor de coördinatie van patenten;
Er wordt een eerste controle van de gegevens met betrekking tot volledigheid, handtekeningen, fondsbeschikbaarheid, al gebruikte hashes, daadwerkelijke wallet states, geblokkeerde mapjes en/of gebruikers uitgevoerd.
Een eventuele aanvullende bewerking van Sender ID is nu vergrendeld in het tijdelijke geheugen, terwijl specifieke gegevensvelden worden afgerond (zoals bij eerdere transacties waarnaar gelinkt kan worden, tijdstempel en vorige hash);

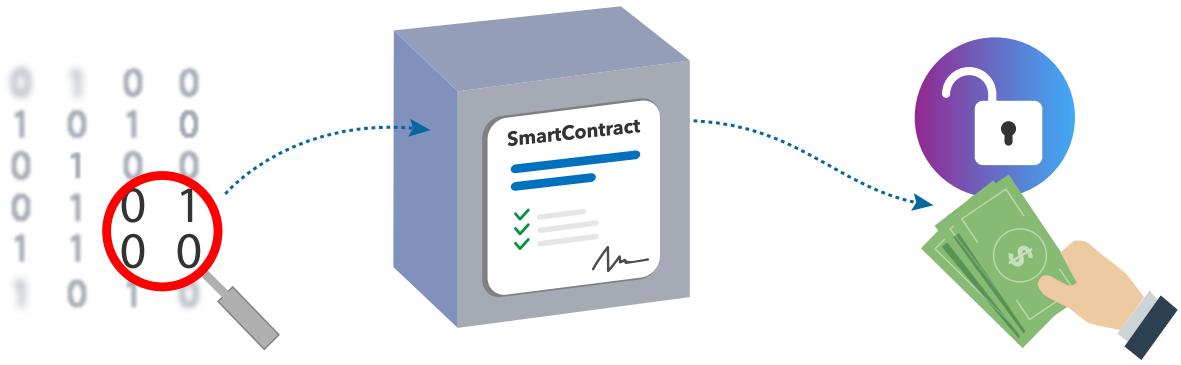


De transactie wordt verzonden naar een Topic Message Queue[19] met een protocol dat moet worden gedefinieerd
(AMQP voor de pilot, MQTT en anderen worden gedefinieerd) en evenwijdig gedistribueerd worden naar werk-knooppunten.
Werk-knooppunten zien toe in hun belang voor het verwerken van de aanvraag (er kunnen noodzakelijke gegevens missen, ze kunnen bezet zijn of er zijn andere oorzaken die moeten worden geëvalueerd) en gaan te werk om een nieuwe portefeuille state te ontwikkelen, herstellen in verband staande hashes van vorige gekoppelde transacties en voegen deze toe aan het rekeningoverzicht. Het resultaat van Proof of Integrity is nu toegevoegd, Transactie hash wordt berekend.
Werk-knooppunten registreren de transactie op het geheugen en sturen een vote door naar coördinerende knooppunten via een Message Queue waardoor resultaten worden verzameld.
Wanneer votes en hashes samenhangend zijn, zullen coördinerende knooppunten vasthoudend zijn met betrekking tot de transactie en nieuwe portefeuille-states. Ze zullen dan alle hashes van eerdere states verbranden en geldigheid van votes uitzenden via een extra Topic Message Queue systeem. Werk-knooppunten zullen ook vasthoudend zijn bij transacties en wijzigingen in portefeuille states. Einde van een best case full route scenario.

Logic data flux

Processtroom in detail





Slimme contracten

Multiversum gelooft in het belang van het aanbieden van verbeterde Slimme Contracten[20] voor iedereen. Op het moment van schrijven heeft Multiversum besloten om deze mogelijkheid niet te onderzoeken, tenzij er een aanpassing komt in het onderzoeksbereik. Daarom zijn we aan het kijken om Open Source in te voegen in de Multiversum technologie omdat deze het beste in onze behoefte voorziet, om uiteindelijk geïmplementeerd te worden als referentie volgens zijn licentiemodel.

Infrastructuur

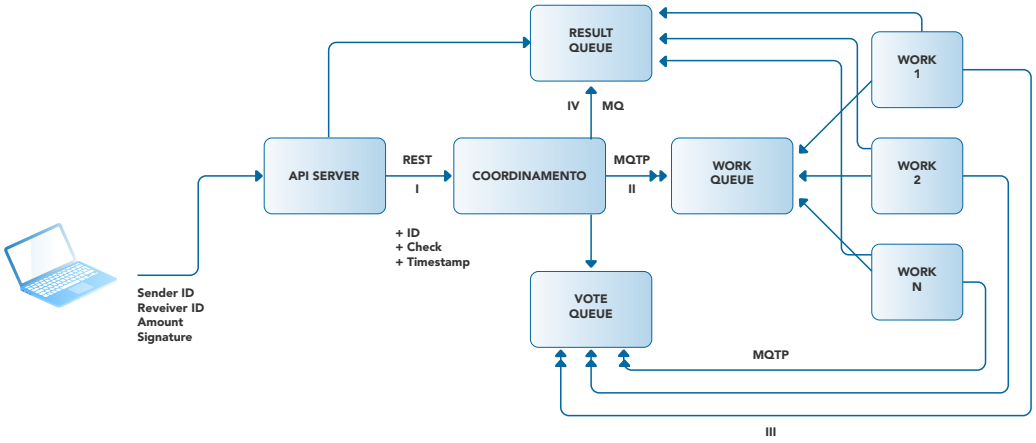
Multiversum infrastructuur is ontworpen om veerkracht en bereikbaarheid (reachability)[21] te garanderen. Deze doelstelling is bereikt door knooppunt-clusters te ontwikkelen die in staat zijn om zelf hun leden te kiezen op basis van specifieke rollen die gebaseerd zijn op technische specificaties van de verschillende knooppunten, waaronder:

- Berekening van capaciteit
- Geheugencapaciteit
- Wederzijdse latentie (onzichtbaarheid)
- Volledigheid van keten gegevens
- Betrouwbaarheid van machines
- Twijfels over Proof of Integrity

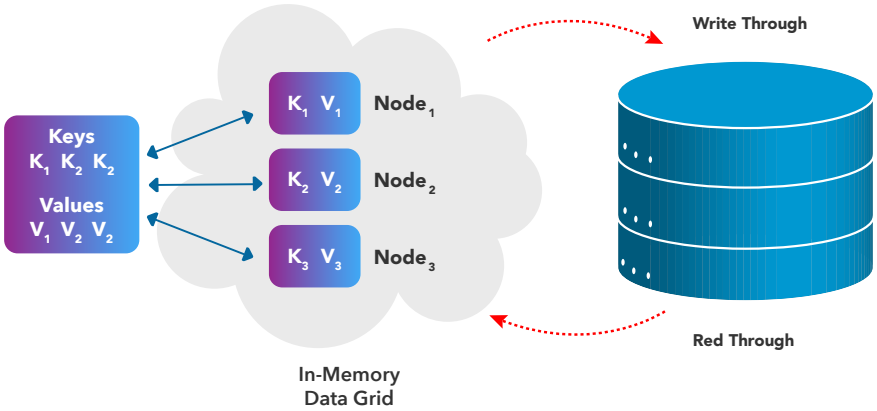
Knooppunten zullen dan een of meer rollen hebben:

- Client knooppunten
- Coördinerende knooppunten
- Seinende knooppunten
- Werk knooppunten
- Vasthoudende knooppunten
- Backup knooppunten

Ieder knooppunt die een geldig certificaat kan aantonen, zal de mogelijkheid hebben zich te kunnen inschrijven voor het cluster en zal een rol kunnen bemachtigen.
In geval van botsing tussen een of meerdere knooppunten kan het cluster zelfstandig een nieuwe taakverdeling inrichten voor het optimaliseren van rollen.



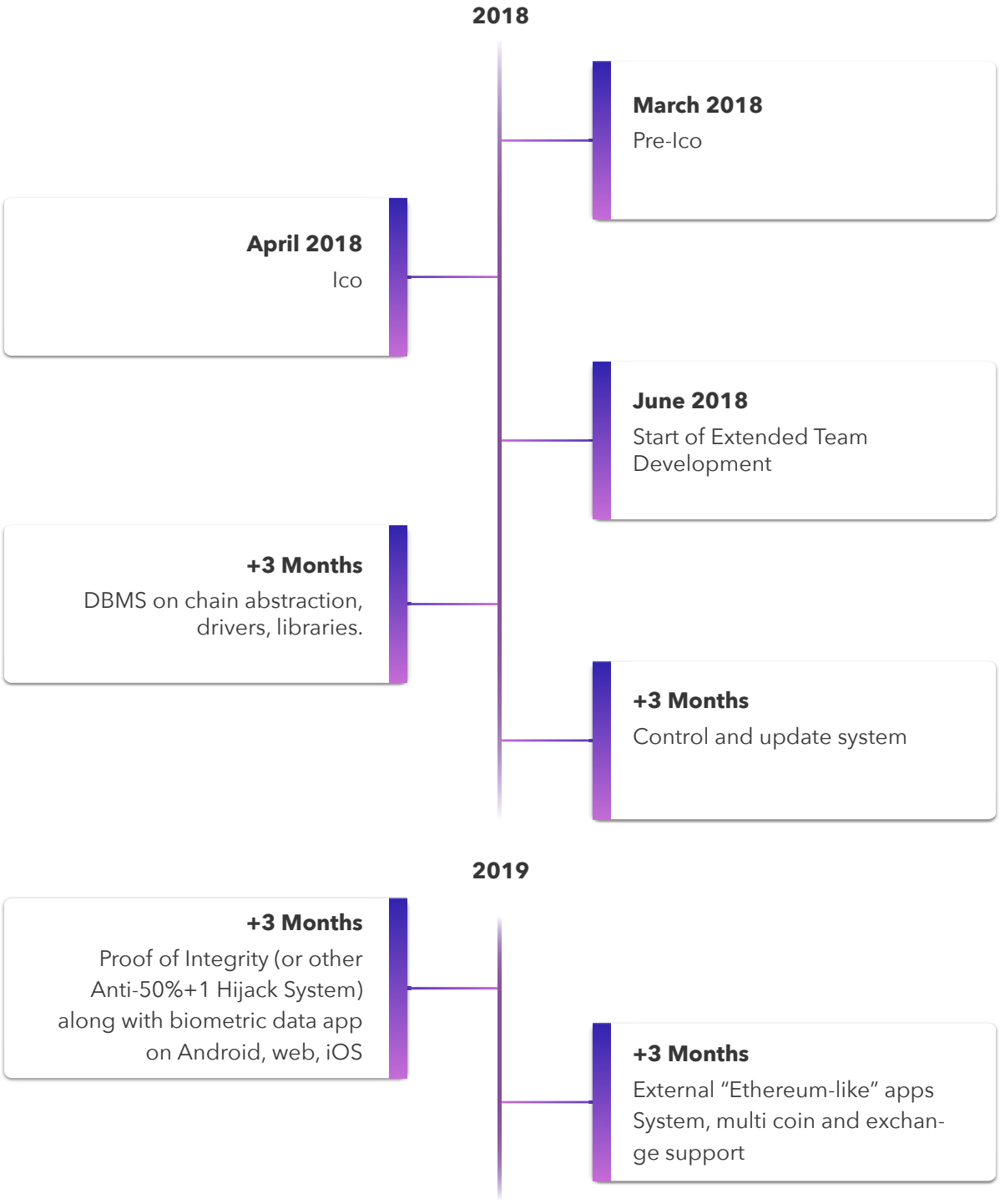
Componenten van shared-cache intra JVM[22] zullen dienen als geheugendatabase waardoor het mogelijk is om 'door te lezen', ook wel read-through. In andere woorden betekent dit het lezen van datavragen die direct uitgevoerd worden op een tijdelijk geheugen voordat het omgezet wordt naar fysiek geheugen.
Door-schrijven, oftewel Read-through, is het laden van data op tijdelijk geheugen voordat het wordt wordt gebruikt voor massale invoering om data aan te houden voor optimale prestaties.



Notities omtrent veiligheid

Tijdens de ontwikkeling zullen er 'hackers-premies' worden uitgeloofd aan ontwikkelaars die zwaktes vertonen zodat het mogelijk is om een geldige oplossing te vinden.

Technical Road Map



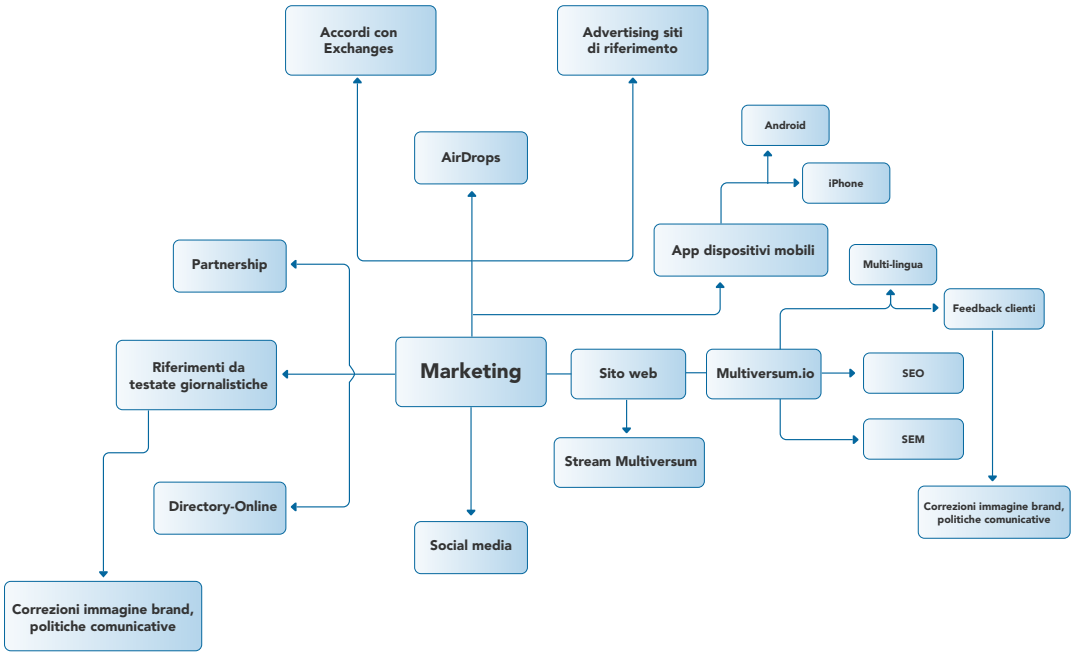
Referenties

1 https://en.wikipedia.org/wiki/Scalability#Horizontal_and_vertical_scaling
2 https://en.wikipedia.org/wiki/Proof-of-work_system
3 https://en.wikipedia.org/wiki/Proof-of-stake
4 https://en.wikipedia.org/wiki/Agile_software_development
5 https://en.wikipedia.org/wiki/Scope_(project_management)
6 https://en.wikipedia.org/wiki/Shard_(database_architecture)
7 https://en.wikipedia.org/wiki/High-availability_cluster
8 https://en.wikipedia.org/wiki/Single_point_of_failure
9 https://en.wikipedia.org/wiki/Microservices
10 https://en.wikipedia.org/wiki/Serverless_computing
11 http://goo.gl/CVBzJd Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint"
12 https://en.wikipedia.org/wiki/ERC20
13 https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
14 https://en.wikipedia.org/wiki/Security-Enhanced_Linux
15 https://en.wikipedia.org/wiki/Spring_Framework
16 https://en.wikipedia.org/wiki/ACID
17 https://en.wikipedia.org/wiki/Models_of_communication#Transactional_Model
18 https://en.wikipedia.org/wiki/SQL
19 https://en.wikipedia.org/wiki/Message_queue#Standards_and_protocols
20 https://en.wikipedia.org/wiki/Smart_contract
21 https://en.wikipedia.org/wiki/Reachability
22 https://en.wikipedia.org/wiki/Java_virtual_machine

Marketing strategie

Omdat we actief zijn op de altijd veranderende IT-markt, zullen we onze strategie, communicatie technieken en missie waar mogelijk updaten.Zo hopen we waarde te kunnen creëren voor onze aandeelhouders en de juiste balans te garanderen tussen lange- en korte termijn management. De belangrijkste punten van ons plan zijn:

- Missie
- Zakelijke doelstellingen
- Zakelijke doelstellingen
- Zakelijk portfolio van activiteiten



Social media marketing zal een van de belangrijkste middelen zijn die we gaan inzetten: we zullen campagnes uitvoeren op sociale netwerken om merkbekendheid te vergroten, potentiële klanten te identificeren, contacten te genereren en belangrijke relaties op te bouwen met klanten.

Onze social media strategen zullen diverse acties opzetten die onderdeel zijn van een strategisch plan, beginnend met het managen en monitoren van kanalen waarbij gebruik wordt gemaakt van hulpmiddelen en het ontwikkelen van de gemeenschap. Hierbij wordt gefocust op inhoud en interactie, de efficiëntie wordt getoetst aan de hand van behaalde resultaten.

De lagen van elementen die het universum bedekken zijn ieder tien keer dikker dan de voorgaande, en alle universums bij elkaar gevoegd lijken op een gigantische atoomcombinatie.

Bhagavata Purana 3.11.41

MULTIVERSUM

HERE TO STAY