MULTIVERSUM

HERE TO STAY

WHITE PAPER v 1.0.6

Business | Technical

German

13.02.2018

Authors: Multiversum Team

www.multiversum.io

**Es gibt außer unserem Universum noch unzählige andere,
und obgleich sie unendlich groß sind,
bewegen sie sich in Dir wie Atome.**

Bhagavata Purana 6.16.37

Multiversum
Identität und Mission

Als Pionier der Kryptowährungen ist Bitcoin, mit all seinen verschiedenen Klonen und Forks, die den Proof of Work-Algorithmus zur Transaktionsvalidierung nutzen, die erste Generation der Blockchain.

Die zweite Generation, in der Ethereum erstmals Smart-Contract-fähige Blockchains eingführt hat, ist heterogener strukturiert und erlaubt eine leichtere Tokenisierung von Vermögenswerten.

Beide Architekturen haben eine extrem niedrige Energieeffizienz und mittlere bis niedrige Werte für die Geschwindigkeit von Blockvalidierung und Transaktionen pro Block.

Das Ziel der dritten Generation der Blockchain-Lösungen ist es, Probleme hinsichtlich Skalierbarkeit, Geschwindigkeit und Energieverbrauch zu lösen mit Hilfe verschiedener Ansätze und Techniken wie Proof of Stake-Validierungsalgorithmen, Off-Chain-Routing, Graph-Chains und vollständiger oder partieller Zentralisierung.

Die vierte Generation geht weit darüber hinaus und erreicht schnellere und besser skalierbare Lösungen, um so aus geschäftlicher Sicht wettbewerbsfähig zu werden;
Einfache Datenchains sind nicht flexibel genug, um den Anforderungen einer Unternehmensumgebung gerecht zu werden, in der komplexe Datenstrukturen in Tabellen, wie relationalen Datenbanken, strukturiert werden müssen.

Gleichzeitig müssen diese Strukturen mit Hilfe von Blockchain-basierter Technik validiert und unveränderlich gemacht werden, um Rückverfolgbarkeit und Sicherheit zu gewährleisten.

Mit anderen Worten bietet die vierte Generation der Blockchain diese Technologie als komplette Anwendung für die Primärproduktion und erweitert das aktuelle Business-orientierte Angebot in Bezug auf Daten-Storage, Anwendungsdezentralisierung, Auditing, Sicherheit und Zuverlässigkeit.

Multiversum bietet komplexe Datenorganisation anstelle von Datensequenzierung;

Chainaufspaltungen und Wiedervereinigungen, um größere Skalierbarkeit und Parallelität zu ermöglichen, und Proof of Integrity-Validierung (Nachweis von Integritätsvalidierung - d. h. kryptographischer Nachweis des Servercodes) anstelle der bislang genutzten Proof of Work- oder Proof of Stake-Lösungen.

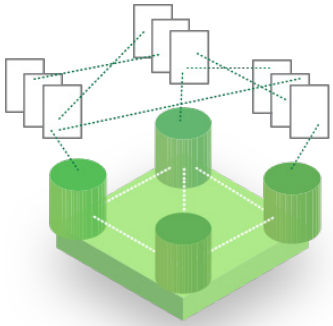
Darüber hinaus wird Multiversum über eine ERC20 / ERC23-Integration verfügen, die es ermöglicht, Coins und Tokens anderer Dienste in unserer Chain zu hosten wie auch umgekehrt unsere Coins und Tokens auf anderen Chains zu hosten, mit notariellen Diensten als externer Bestätigungsmethode.

Zusätzlich zu diesen Innovationen werden wir noch weitere gute Lösungen anwenden, die unsere Kollegen bereits im Laufe der Zeit umgesetzt haben.

Multiversum

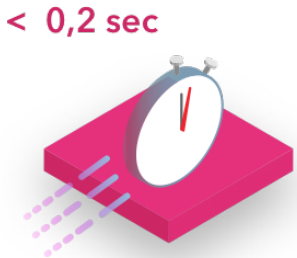
Die relationale Blockchain der 4. Generation

Warum ist Multiversum die Blockchain 4.0?



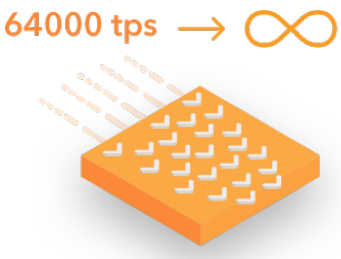
Relationale Blockchain

Ein brandneuer Typ von Blockchain, die verschiedene Arten von Daten nutzt und diese in einer multidimensionalen Struktur miteinander in Beziehung setzt.



Transaktionsgeschwindigkeit

In weniger als 0,2 Sekunden werden Finanzmittel zwischen Wallets übertragen, bei gleichzeitiger sicherer Validierung der Transaktionen. Dies macht Multiversum zu einem der schnellsten Transaktionsysteme der Welt.



Transaktionsdurchlauf

Unübertroffene Skalierbarkeit: Bis zu 64.000 Tps (1000 Tps / Core) auf einem 64-Core-Server. 64+ Core-Technologien werden unterstützt.

Integritätsnachweis

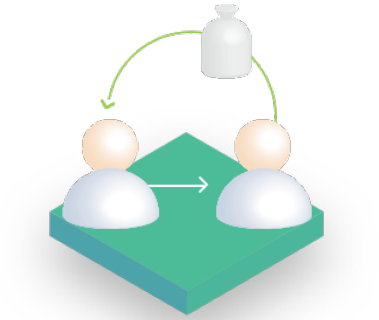
PoS (Proof of Stake) wird ersetzt durch PoI (Proof of Integrity: kryptographischer Nachweis des Server-Codes).

Wallet der nächsten Generation

Modernste Sicherheit beim Zugang und Geldtransfer durch biometrische Eingaben.

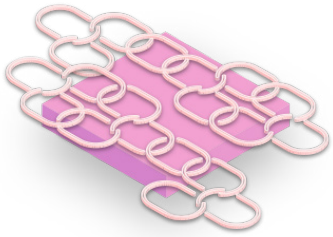
Umweltfreundlich

Eine Multiversum-Transaktion wird unbedeutende Kosten haben und nahezu keinen ökologischen Fußabdruck hinterlassen.



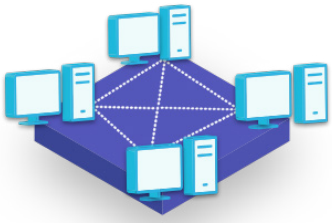
Rollback

Optionales Rollback kann auf Multiversum-gehosteten Token aktiviert werden.



Teilbare Chains

Ressourcenoptimierung zwischen Nodes durch Kettentrennbarkeit.



Recovery Nodes Verteilung

MTV-Nodes sind global gestreut für unübertroffnene Widerstandsfähigkeit, Zuverlässigkeit und Global Disaster Recovery.

Öffentliche Präsentation

Gegenwärtiger Stand der Blockchain-Technologie

Die Hauptfiguren des Blockchain-Phänomens haben ein gemeinsames Merkmal: sie sind bemerkenswert sicher und zuverlässig. Den Preis hierfür zahlen wir in Form von gewaltiger Rechenleistung, inakzeptabler Verschmutzung, hoher Transaktionskosten und Langsamkeit, die kaum dem aktuellen technologischen Fortschritt entsprechen und somit schwerlich angemessen auf die Bedürfnisse moderner finanzieller und kommerzieller Anwender eingehen können.

Diese Langsamkeit wird durch das Fehlen horizontaler Skalierbarkeit1 verursacht, d. h. indem eine Steigerung der Rechenkapazität lediglich durch Hinzufügen zusätzlicher Prozessoren erreicht wird, statt diese durch schnellere Versionen zu ersetzen.

Ein weiterer Grund für diese Langsamkeit ist der derzeitige Blockchain-Sicherheitsmechanismus, der verhindern soll, dass jemand die Mehrheit der Cluster übernimmt, indem die hierfür benötigten Rechenleistungen und / oder Kosten in die Höhe getrieben werden. (Proof of Work2 und Proof of Stake3).

Darüber hinaus sind aktuelle Blockchains einfache Verkettungen von einzelnen Datenentitätszuständen und ihren Veränderungen. Rekonstruktion der tatsächlichen Zustände dieser Entitäten impliziert einen ganzen Kettenscan, was zu noch größerer Systemverlangsamung und Ressourcenverbrauch führt.

Diese Vereinfachungen machen Blockchains für wissenschaftliche und industrielle Zwecke ungeeignet, da hier die Anforderungen an Datenstrukturen extrem komplex werden können.

Darüber hinaus hören die Sicherheitsmaßnahmen auf der Datenebene auf, ohne die Nutzersicherheit gewährleisten zu können: es ist unmöglich, verlorene oder gestohlene Münzen und Wertmarken zurückzuerhalten, selbst wenn sie sich an der Kette befinden, oder bösartige Accounts zu blockieren.
Ein weiteres Problem ist schließlich die Fragmentierung und Inhomogenität der Kryptowährungen, die nicht in der Lage sind, miteinander zu kommunizieren und in nicht verwandten Universen leben.

Multiversum und globale Blockchain-Akzeptanz

Die Multiversum-Technologie treibt die traditionelle Blockchain über ihre aktuellen Grenzen hinaus, sie verbessert die Datenschicht durch selbstüberprüfende und verteilte Strukturen von organisierten Daten-Entitäten, die durch symbolische Links miteinander verbunden sind.

Diese Technologie bildet die Grundlage für ein dezentrales und verteiltes System kohärenter und selbstüberprüfender Transaktionen: Multiversum Blockchain.

Multiversum ermöglicht anstelle des einfachen Datenmodells bestehender Blockchains die Erstellung einer relationalen Crypto-Datenbank, einer fortschrittlichen und organisierten Datenspeicherlösung. Diese Crypto-Datenbank kann nicht nur einen einzelnen Datentyp verarbeiten, sondern eine Reihe von Daten, die in komplexen, miteinander verwandten Graphen gruppiert sind. Diese Datenstrukturen, die miteinander in Beziehung stehen, sind jetzt First-Class-Citizen der Blockchain und werden durch kryptographische Methoden abgesichert.

Jede dieser Relationen wird bei Aufforderung auf Statusänderung in eine eigene Unterkette von der Hauptkette abgespalten und, nach vollzogener Operation, wieder mit dieser vereint, um erneut validiert zu werden.

Somit ist Multiversum eine weiterentwickelte Blockchain-Technologie, die dank ihrer einzigartigen Funktionen die zuvor analysierten Nachteile überwindet, und Krypto-Validierung und Verteilungstechniken für jeden Bedarf bietet: Verwaltung, Industrie, Finanzen und Behörden.

Eines der Hauptziele von Multiversum ist es, dem Markt jederzeit das bestentwickelte Produkt anbieten zu können. Dies wird ermöglicht durch Anwendung von AGILE4-Softwareentwicklungsmethodik.

Die AGILE-Methodik bedeutet eine drastische Reduzierung des anfänglichen Engagements im Projektdesign zugunsten der Valorisierung von Erfahrungen während der Projektentwicklung, in welcher Chancen und Risiken erst sichtbar werden, die im Voraus kaum abzuschätzen sind, und belohnt somit die besten Verfahren, während die unzulänglichen aufgegeben werden können. AGILE ist ein etablierter Softwareentwicklungsstandard und drängt Entwickler sowie Produkteigner und Investoren, den Projektumfang5 als flexibel und leicht an die Marktbedürfnisse anpassbar zu betrachten.

In einem sich mit so rasanter Geschwindigkeit veränderndem Sektor wie Software ein Produkt vorzustellen, das schon sechs Monate Studien und ein Jahr Implementierung hinter sich hat, bedeutet, ein obsoletes Produkt vorzustellen, das auf Marktbedürfnisse von vor achtzehn Monaten reagiert, die in der Zwischenzeit womöglich von Wettbewerbern bedient werden konnten und welches nicht auf aktuelle, neue Herausforderungen reagieren kann.

AGILE dagegen bietet die Chance, dem Markt jederzeit das innovativste Produkt anzubieten.

Geschwindigkeit und Technologie

Eine der grössten Stärken dieser Technologie ist Geschwindigkeit, dank des Split-Rejoin-Mechanismus unserer Blockchain und der Fähigkeit, verschiedene Transaktionen parallel auszuführen.

Diese Funktionen ermöglichen eine größere horizontale Skalierbarkeit und erhöhen die Transaktions-Verarbeitungskapazität. Durch die resultierende erhöhte Rechenleistung kann jeder Node volle Leistung bringen.

Horizontale Skalierbarkeit

Multiversum profitiert von zwei spezifischen Funktionen zur Maximierung der Systemeffizienz:

1. Die Hauptchain ist in der Lage, ihre Strukturen zu optimieren, indem sie sich autonom in mehrere Unterchains aufteilt, je nach angeforderten Ressourcen und Datenströmen, und

so die Arbeit über mehrere Ausführungsstränge und Nodes parallelisiert.
Dieser Chain-Split-Prozess wird bis zur Normalisierung der Arbeitsbelastung ausgeführt, woraufhin sich die Chain, ebenfalls autonom, wieder in eins zusammenfügt.
Dies ist möglich aufgrund einer Technik, die es jedem Block der Chain ermöglicht, zwei verschiedene Unterchains von zwei verschiedenen eingehenden Links zu validieren.
2. Daten Sharding6, d. h. eine Technik, die eine Verteilung von Daten zwischen mehreren Nodes erlaubt.
Bei einer ABC-Datenreihe und drei Cluster-Nodes haben wir eine Datenverteilung wie folgt:

AB

BC

CA

Diese Unterteilung ermöglicht eine höhere Verarbeitungsgeschwindigkeit von Transaktionen, da sich Datenabfragen lediglich auf Subchain-Nodes auswirken, und so jeder Schritt optimiert wird.
Ein weiteres äußerst wichtiges Merkmal unserer Technologie ist High Availability7: die Chance sich auf einen Cluster-Typ zu verlassen, der die Kontinuität der Dienste selbst im Falle des Herunterfahrens einiger Nodes im Netzwerk gewährleistet.
Um beim vorherigen Beispiel zu bleiben (A, B und C Nodes): Sollte C offline gehen, bleiben A und B davon unberührt komplett operabel und können so eine ununterbrochene Funktion ohne Verlust von Daten sicherstellen, vorausgesetzt, es bleiben 50% + 1 aller Nodes funktionsfähig.
Auf diese Weise reorganisiert der Cluster im Falle eines Ausfalls mehrerer Nodes autonom die Datenverteilung und kommuniziert mit jedem Node bis zur vollständigen Wiederherstellung des Betriebs.

Umwelt

Multiversum ist auch umweltfreundlich: Eines unserer Hauptziele ist, die benötigte Rechenleistung für die kryptografische Validierung zu verringern um Mining (Proof of Work) zu vermeiden, welches eine riesige Verschwendung von Energie und Ressourcen darstellt.
Anstelle dieser veralteten Technik implementieren wir den Integritätsnachweis (Proof of Integrity), ein Protokoll, das kryptografische Validierung durch Überprüfung der Authenti-

zität der Software ablaufen lässt, über die jede Persistenz der Transaktion läuft.

Datenmanagement

Multiversum kann dank seiner krypto-relationalen Datenbank Daten leichter strukturieren, ohne Begrenzung von Datenverknüpfung.
Jedes Wallet hat eine Reihe von Zuständen und wird mit einer Person (Nutzer) verknüpft.
Die Änderung des Walletstatus umfasst zwei Datenfelder:
-Den vorherigen Zustand, um die Validierung zu überprüfen.
-Einen Link zur letzten Transaktion (oder zum letzten Hauptchainlink), um die Provenienz des neuen Statuswechsels anzuzeigen.
Nach der Statusänderung wird die Transaktionsänderung hinzugefügt und der Link für den geänderten Status wird wieder der Hauptchain beigefügt.
Hierbei erbt die neue Transaktion zwei Hashes: einen aus der Statusverknüpfung,und einen aus der vorherigen Transaktion.
Auf diese Weise validieren alle Operationen die vorhergegangenen, die mit derselben Transaktion verknüpft sind.

Diese fortschrittliche Lösung, die in der Lage ist, komplexe Datenszenarien zu verwalten, wird es den Menschen ermöglichen, jede Art von Anwendung auf unserer Technologie einzubetten und so eine weltweite Verbreitung in Institutionen, Ämtern, Finanz- und Industrieanbietern zu erzielen, die das gesamte Blockchain-Universum einen Schritt nach vorne bringt.

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

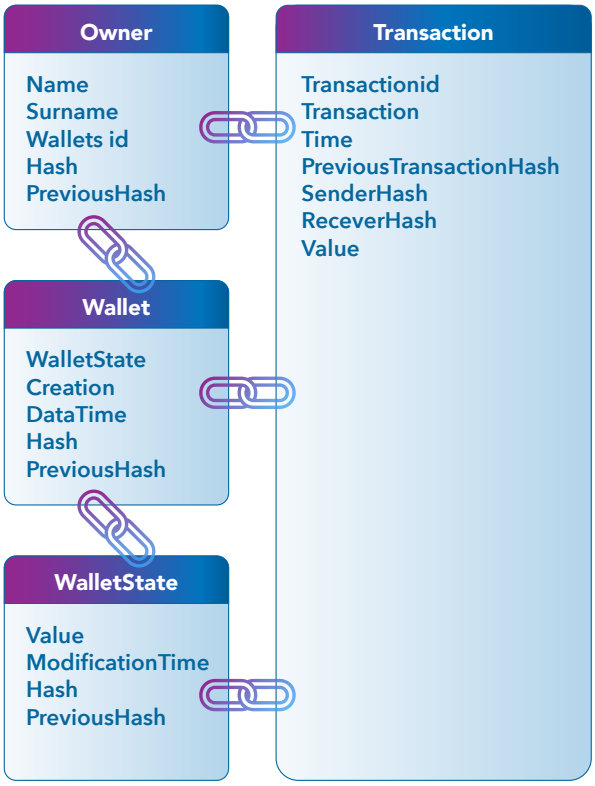
Native on chain adapter for own ERC20
(Interoperability with other BC)

ERC23
(Interoperability with other BC)

Multiversum - Unsere Mission

Unser Ziel als Multiversum ist es, die Welt der Blockchains um eine Generation nach vorne zu bringen. Als Alleinstellungsmerkmale bieten wir folgende Zielstellungen:

1. Erlangen einer krypto-relationalen DB mit selbstvalidierenden komplexen Datenstrukturen
2. Teilbare / wiedervereinigbare Chains basierend auf der jeweils aktuellen Systemauslastung (Parallel Work)
3. Daten-Sharding (Parallelarbeit)
4. Erweitertes API-Angebot
5. Rollback (Nutzersicherheit)
6. Freezable Wallets (Nutzersicherheit)
7. Integration von biometrischen Daten als Seed der elektronischen Signatur
8. ERC23-Schnittstelle (Interoperabilität mit anderen Blockchains)
9. Native Off-Chain-Adapter für den eigenen ERC20 / ERC23 (Interoperabilität mit anderen Blockchains)
10. Native Off-Chain Adapter für ERC20 / ERC23-Gäste (Interoperabilität mit anderen Blockchains)
11. Proof of Integrity - Nachweis der Integrität (Protokollinnovation)
12. Doppelzugriffssperre (strukturelle Sicherheit)
13. Umgekehrte Zugriffsverweigerung (Strukturelle Sicherheit)
14. Gegenseitige Chainbestätigung (Interoperabilität mit anderen Blockchains)
15. Integration für Java, Spring und Javascript
16. ACID Modell
17. Transaktionsmodell
18. SQL-ähnliche Sprache



1. Erlangen einer krypto-relationalen DB mit selbstvalidierenden komplexen Datenstrukturen

Multiversum ist besonders auf industrielle und institutionelle Nutzung ausgerichtet.
Dies sind Kontexte, in denen wir Daten mit komplexen Strukturen vorfinden, die unmöglich effizient und normiert mit einer einfachen Chain dargestellt werden können.
Wir wollen die erste relationale krypto-relationale Datenbank auf dem Markt werden, dezentral oder aufgeteilt, wo nötig.
Die Fähigkeit hierzu leitet sich aus der konzeptuellen Verbindung von verketteten Entitäten (Einheiten) ab: In unserer Technologie ist eine primäre Chain in der Lage, sich in sekundäre Chains aufzuteilen, die verschiedene Sätze von Entitäten(Einheiten) und Protokollen enthalten.
Diese Entitäten fügen sich in ihrem letzten persistierenden Zustand wieder zusammen, um nach den notwendigen Modifikationen sich wieder an das letzte Glied der primären Chain anzuhängen und so wieder ein Ganzes mit dieser zu bilden.
Die „chainfähige“ Schnittstelle setzt eine Art von Datensatz voraus, der zwei oder mehr Hashes der vorherigen Datensätze enthält. Validiert wird nicht nur eine, sondern mehrere Unterchains.
Die Multiversum-Standard-Implementierung, die von Versum-Coins verwendet wird, ba-

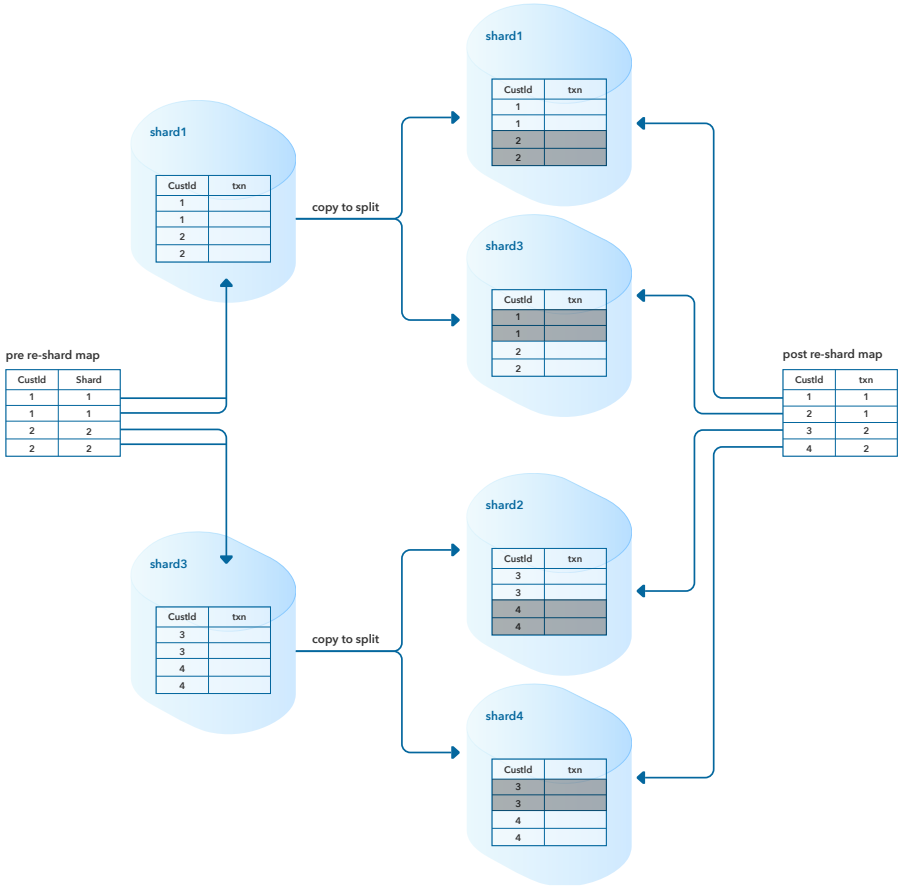
siert auf Chainable-Entitäten(Einheiten), die auf einer Chain koexistieren und zu vier Tabellen gehören: Nutzer, Wallet, Wallet-Status, Transaktion. Diese Entitäten sind miteinander verbunden und bestätigen sich gegenseitig.

2. Teilbare / wiedervereinigbare Chains basierend auf der aktuellen Systemauslastung (Parallel Work)

Die gleiche Fähigkeit, mehrere Links von einem einzelnen abzuleiten und sie wieder zu verbinden, erlaubt der Technologie die Verwendung von Workload-Analysatoren, die dem Cluster die Dringlichkeit aufweisen, die Primär-Chain in zwei Sekundär-Chains aufzuteilen (und sich möglicherweise unbegrenzt weiter zu teilen), wenn eine hohe Anforderung von Transaktionsausführungen auftritt. Sobald der Workload nachgelassen hat, können mehrere bereits existierende Unterchains zurückverlinkt und validiert werden. Dieser Mechanismus ermöglicht paralleles Arbeiten bei gleichzeitiger Sicherstellung der Transaktionsprotokolle.

3. Daten Sharding (Parallelarbeit)

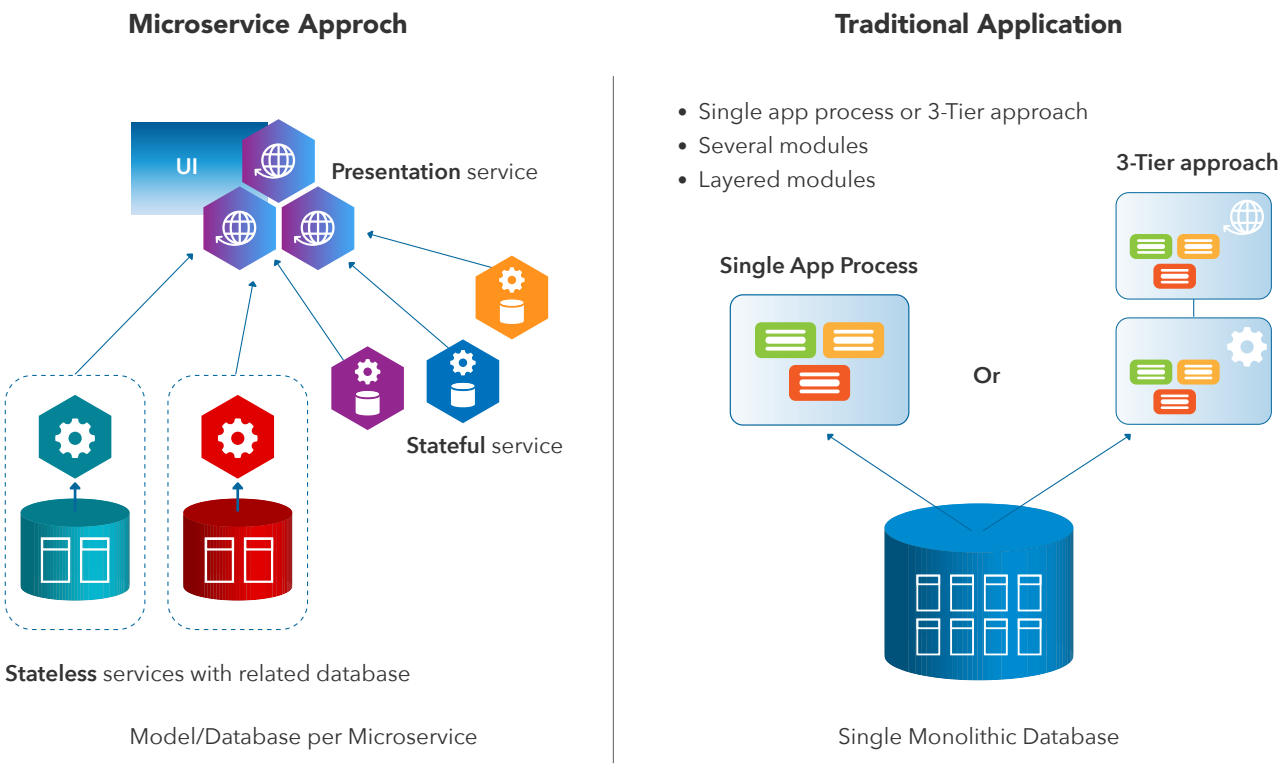
Jeder Node enthält die gesamten Chaindaten oder nur einen Teil der Chain.
Wenn Datensharding erforderlich ist, legen Koordinator-Nodes bestimmte Datenpartitionsmodi fest, um die eigene Distribution entsprechend der aktuellen Auslastung zu optimieren.



Gemäß der Hochverfügbarkeitstechniken wird Zuverlässigkeit und Beständigkeit immer gewährleistet, auch im Falle eines plötzlichen Verlustes eines Teils des Clusters, sofern mindestens 50% + 1 der Nodes überleben.
Diese Nodes können nach einem partiellen Cluster-Crash die Datenstrukturen neu verteilen und reorganisieren, um so schnell wie möglich einem weiteren partiellen Cluster-Crash entgegentreten zu können.
Mit den Techniken 2 und 3 erreicht Multiversum Blockchain eine verbesserte Kapazität für paralleles Arbeiten und Daten-Sharding; d.h. horizontale Skalierbarkeit, erhöhte Sicherheit, hohe Verfügbarkeit, Systemstabilität, Fehlen eines Single Point of Failure8 sowie autonome Disaster Recovery.

4. Microservice Struktur und Advanced API Angebot

Entwickelt auf einer Plattform basierend auf Microservices9 und Serverless-Modellen10, wird Multiversum in der Lage sein, erweiterte sichere und moderne API-Funktionalitäten anzubieten und sich beiden Strukturen anzupassen.



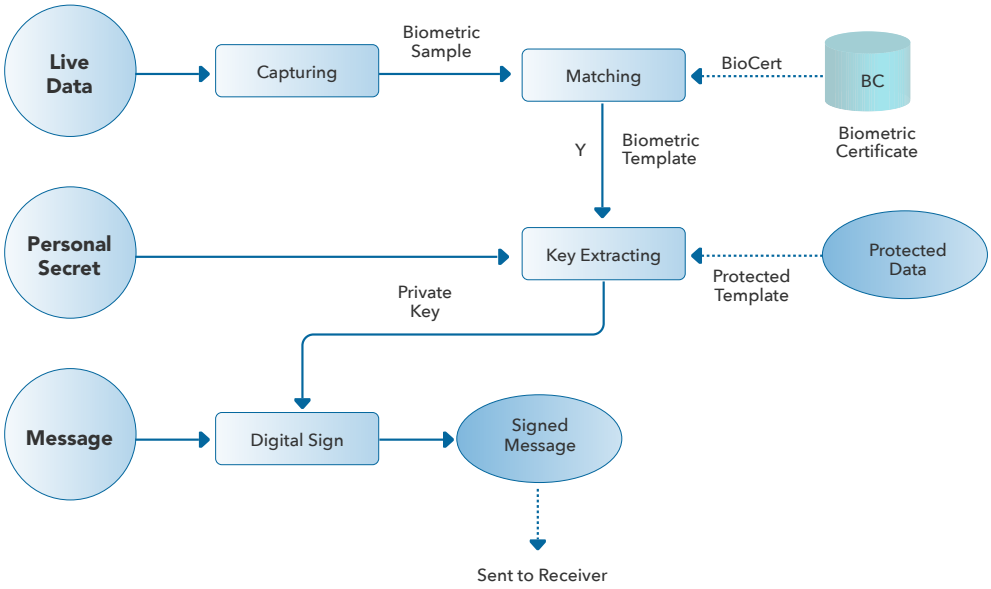
5. Rollback (Nutzersicherheit)

Unsere Technologie wird im Kontext von Transaktionen Rollbacks von unerwünschten

Operationen ermöglichen; d. h. Wiederherstellung eines vorherigen Zustandes, ohne die Bestätigung der Chain-Validierung durch Implementierung einer Reihe von Transaktionswiederherstellungsstatus zu stören. Diese Funktion kann optional aktiviert werden für alle Token und Anwendungen, die auf der Multiversum Blockchain gehostet werden.

6. Freezable Wallets (Nutzersicherheit)

Die Möglichkeit, eine Wallet-Freezing-Funktion im Falle von rechtswidrigen oder verdächtigen Aktivitäten einzubeziehen, wird implementiert werden, nachdem die Prüfung der Durchführbarkeit auf der Geschäftslogik-Seite abgeschlossen ist. Proprietäre Anwendungen, die auf der Multiversum-Blockchain basieren, können diese Funktion, falls gewünscht, implementieren.

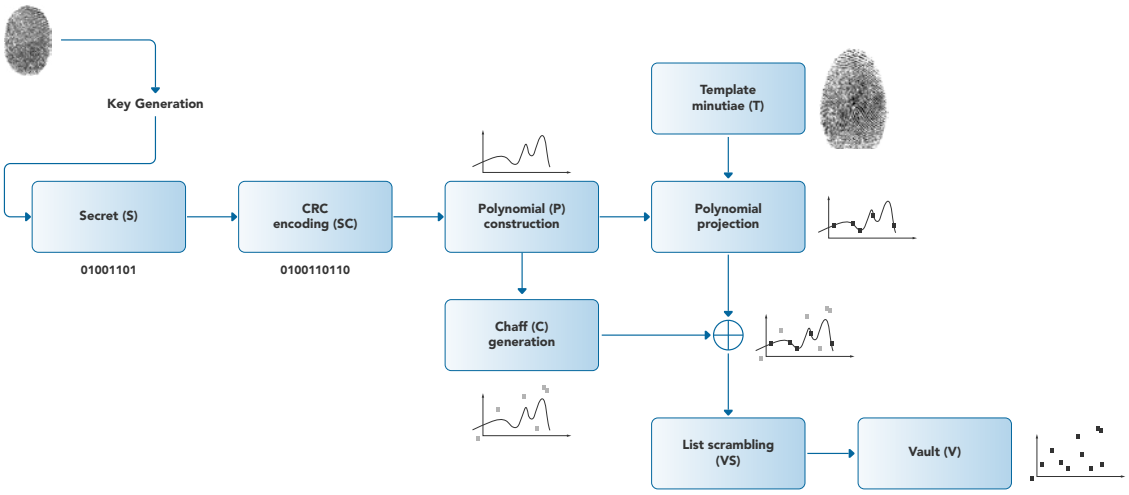


Biometric Digital Key Generation Framework

7. Integration biometrischer Daten als Seed für die elektronische Signatur

Ausgehend von Forschungarbeiten von Je-Gyeong Jo, Jong-Won Seo und Hyung-Woo Lee11 prüft das Multiversum-Team die Umsetzbarkeit der Nutzung biometrischer Daten wie Fingerabdrücke, Netzhautscans und graphometrischer Signaturen als asymmetrische

Schlüssel, um die Identität des Unterzeichnenden nachzuweisen.
Die Sicherheit verschlüsselter Daten und ihrer Verwendung als Validierung in juristischen Auseinandersetzungen wird evaluiert.
Darüber hinaus werden biometrische Daten für Android, IOS und Applikationen anderer Plattformen verwendet, um die Nutzersicherheit zu verwalten.



Fuzzy Vault Scheme for Biometric Digital Key Protection

8. ERC23-Interface (Interoperabilität mit anderen Blockchains)

Versum-Münzen werden mit dem ERC23-Interface entwickelt, die abwärtskompatibel mit ERC2012 ist, um die Interoperabilität mit anderen Chains zu gewährleisten.

```
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. Native Off-Chain-Adapter für proprietäre ERC20 / ERC23 (Interoperabilität mit anderen Blockchains)
Multiversum wird einen nativen Adapter entwickeln, der ein- und ausgehenden Münzfluss der eigenen Münzen und Token zu nicht-proprietären Chains ermöglicht.

10. Native Off-Chain-Adapter für externe ERC20 / ERC23 (Interoperabilität mit anderen Blockchains)
Multiversum wird einen nativen Adapter entwickeln, der ein- und ausgehenden Münzfluss von Token von nicht-proprietären Chains auf seiner eigenen Chain ermöglicht.

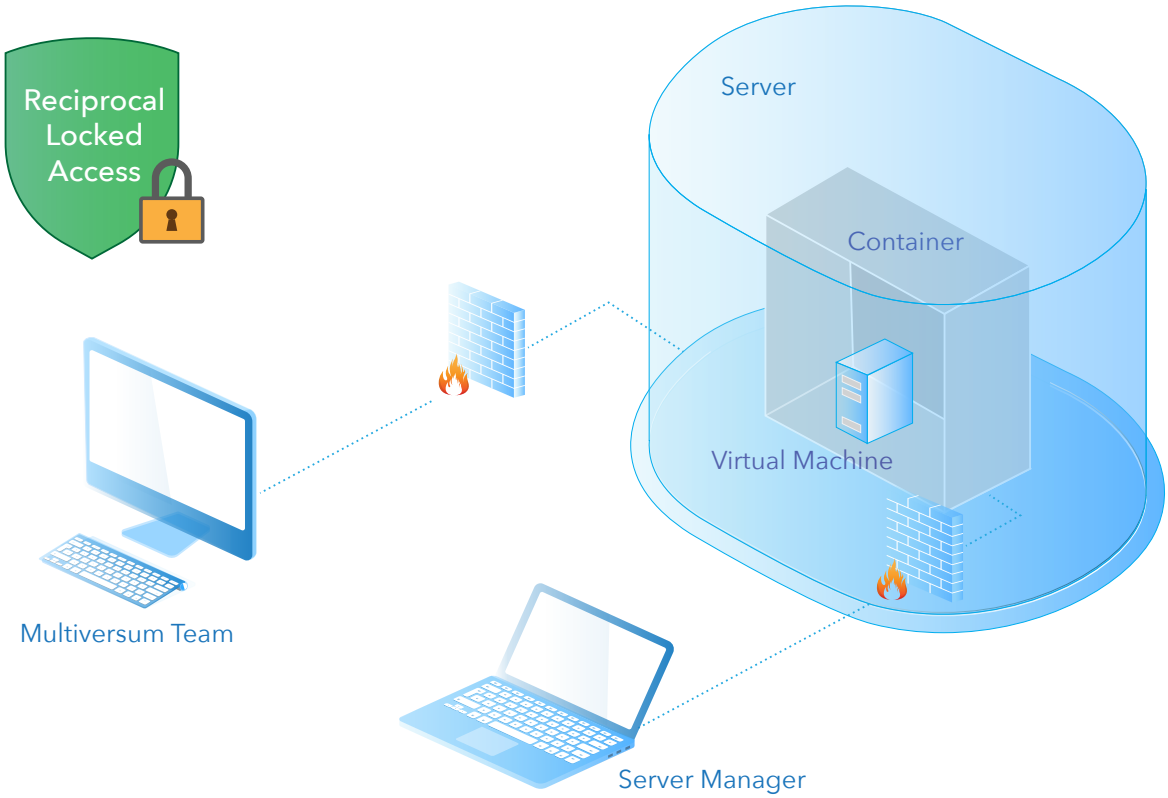
Integrity

11. Proof of Integrity (Protokollinnovation)
Anstelle der bisher üblichen Konsensmechanismen von Proof of Work und Proof of Stake in ihren verschiedenen Formen bietet Multiversum Proof of Integrity: eine Reihe von Algorithmen, die in der Lage sind, die kryptographische Validität einer kompilierten Node zu verifizieren und die Einheitlichkeit der Rückmeldungen der Mehrzahl der Nodes zu prüfen.
Diese Verifizierung erfolgt über eine zufallsgenerierte Challenge in Kombination mit einem Hash, erzeugt von externen Komponenten der Software selbst (Schutz vor Reverse Engineering, Kommunikation mit der Node-Software über verschlüsselte Kanäle) und Transaktionsdaten. Um eine Transaktion zu validieren, muss das Ergebnis dieser Berechnung für eine konkrete Transaktion auf jedem Node identisch sein.
Dieses Verfahren erfordert eine bemerkenswert geringere Rechenleistung, verhindert Verschwendung von Rechenleistung typisch für andere Blockvalidierungslösungen (PoW, PoS, DpoS) und schafft strukturelle Sicherheit, welche weder auf statistischen Modellen noch auf Byzantinischen Consensus13-Modellen basiert, die in kleinen Clustern ziemlich anfällig sind.

Access Denied

12. Doppelzugriffssperre (Strukturelle Sicherheit)

Nodes werden in gesicherten virtuellen Containern verteilt, mit Anmeldeinformationen, die nicht für den Host-Operator verfügbar sind; die Sicherheit wird gewährleistet über Linux Security14 Best Practices, wie beispiesweise SeLinux und / oder andere Pakete. Gleichzeitig wird Sorge dafür getragen, dass jemand, der Gastzugangsrechte zu der operierenden Maschine hat, keinen Zugang zu dem Host erhält, der den Node ausführt. Somit ist der Node durch eine Doppelzugriffssperre gesichert.



13. Umgekehrte Zugriffsverweigerung (Reverse Access Denial) (Strukturelle Sicherheit)

Die unter Punkt 12 beschriebene Zugriffssperre führt zu einer wechselseitigen Ausschlie-

ßung des Nodezugriffs sowohl für Betreiber der Host-Computer wie auch für Personen, die in Besitz von Node-Credentials kommen.
Dies stellt sicher, dass jeder Node, der nicht direkt von Multiversum verwaltet wird, authentisch ist und gegen jeden Zugriff geschützt, also im Grunde autonom und isoliert von externen menschlichen Eingriffen.
Zusätzlich zu operativen und Sicherheitssystemen werden drei grundlegende Komponenten innerhalb des Containers verteilt: ein durch den Multiversum Server kompilierter Code; ein Zertifikat mit einen asymmetrischen Schlüssel zur Authentifizierung beim Multiversum-Cluster; eine schon unter Punkt 11) beschriebene Komponente, welche Challenge-Berechnungen basierend auf dem Server-Hash ausführt; sowie Zertifikat, Challenge Seed und Transaktionsdaten.
Zusätzliche optionale Sicherheitstechniken können implementiert werden, wie beispielsweise ein automatisches Update von Zugangsdaten für Container mit einem zufälligen Passwort während der Kompilierungsphase, um zu verhindern, dass jemand darauf zugreift. Dieser Mechanismus könnte für Cluster als Zugangszertifikat übernommen werden.

14. Gegenseitige Chainbestätigung (Reciprocal Chain Confirmation) (Interoperabilität mit anderen Blockchains)

Multiversum wird die Machbarkeit einer externen Chain-Integrationskomponente untersuchen, die in der Lage ist, Zustände anderer Blockchains zu speichern (eventuell im Austausch von Token), um so zusätzlich Validierung und Vertrauen zu bieten.
Dieselbe Technik kann auch verwendet werden, um Multiversum zu ermöglichen, die eigene Status-Validierung mit anderen Blockchains zu teilen und so Verifikation quasi outzusourcen.
Für diese Funktionalität ist eine spezielle Schnittstelle vorgesehen, die auch unter bestehenden und zukünftigen Blockchain-Implementierungen gefördert werden müsste.
Ein solches Feature wird auf einer serverlosen Komponente beruhen, auf die auch nach der Zusammenstellung der Container zugegriffen werden kann, um die Aufnahme von Adaptern in andere Chains zu ermöglichen.

15. Integration mit Java, Spring und Javascript

Multiversum bietet High-End-Schnittstellen in funktionalen Bibliotheken für Java, Javascript und möglicherweise auch andere Mainstream-Sprachen an, die eine einfachere Übernahme unserer Technologie auf Unternehmens- und institutioneller Ebene ermöglichen.
Integrationsmodule mit Frameworks wie Spring15 werden ebenfalls entwickelt. Diese Art von Bibliotheken werden die Integration von Multiversum in proprietäre Lösungen erleichtern, sowohl in privaten Chains als auch im offiziellen MainNet.

16. ACID-Modell

Multiversum wird das ACID16-Paradigma erfüllen. Das Konzept hinter dieser Abkürzung betont die logischen Eigenschaften, die für Transaktionen als notwendig betrachtet werden.

Um ein sicheres Transaktionsmodell zu gewährleisten, muss die implementierte Technologie folgende Anforderungen erfüllen:

Atomarität (Atomicity):

Eine Transaktion ist in ihrer Ausführung nicht teilbar und ihre Ausführung muss abgeschlossen sein oder null betragen, Teilausführungen sind nicht erlaubt.

Konsistenzerhaltung (Consistency):

Jede Transaktion bringt die Datenbank von einem gültigen Zustand in einen anderen. Persistente Daten müssen gemäß allen definierten Regeln gültig sein.

Isolation (Isolation):

Jede Transaktion muss isoliert ausgeführt werden: der eventuelle Ausfall einer Transaktion darf sich nicht auf andere konkurrierende Transaktionen auswirken.

Dauerhaftigkeit (Durability):

Auch Persistent; diese legt fest, dass sobald eine Transaktion dauerhaft festgeschrieben ist, das Ergebnis nicht verloren gehen kann (etwa durch Abstürze, Fehler, Stromausfall).

17. Transaktionsmodell (Transactional Model):

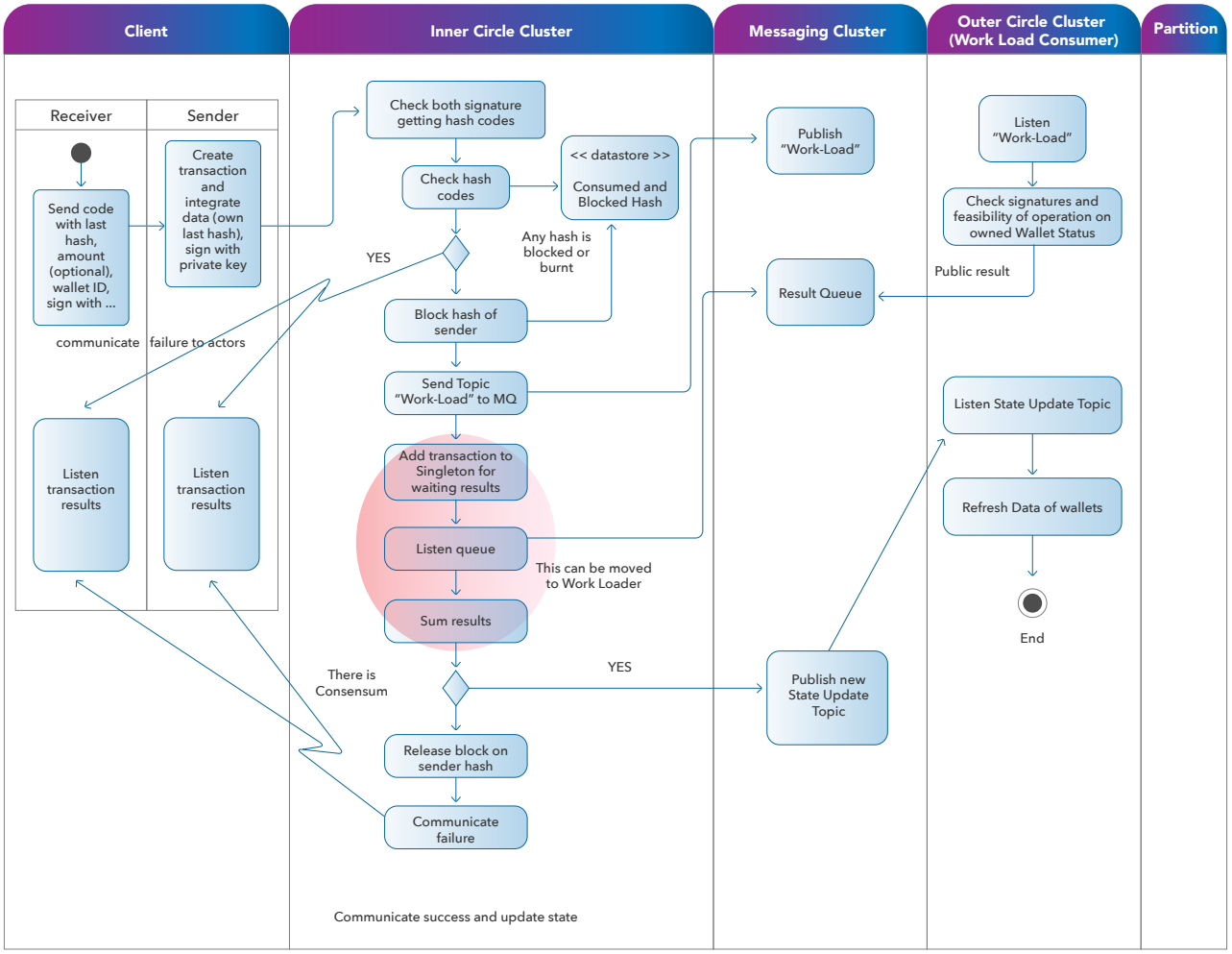
Multiversum bewahrt Transaktionsdaten in einem Transaktionalen17 Modell auf und stellt sicher, dass alle Daten, oder nichts davon in den beteiligten Unterchains beibehalten werden, um so Vollständigkeit der Daten und Kohärenz jeder ausgeführten Transaktion zu gewährleisten.

18. SQL-ähnliche Sprache (SQL-like Language):

Um die Entwicklung von Anwendungen basierend auf unserer Crypto-Relationalen Database-Technologie zu vereinfachen und die Lernkurve gegenüber bestehenden Technologien zu mildern, wird Multiversum über eine SQL-basierte18 Syntax verfügen, um standardmäßige Persistent-Storage-Funktionen (CRUD) zu verwenden.

19. Full-Route-Datenflux (Full Route Data Flux):

Die Prozesse der Annahme, Kontrolle, Validierung und Persistenz einer Transaktion läuft in folgendem schematisierten und vereinfachten Verfahren ab:
Die Transaktion wird mit den erforderlichen Daten an einen REST-Client gesendet und mit einem privaten Schlüssel signiert; Der REST-Client sendet die Transaktion an einen

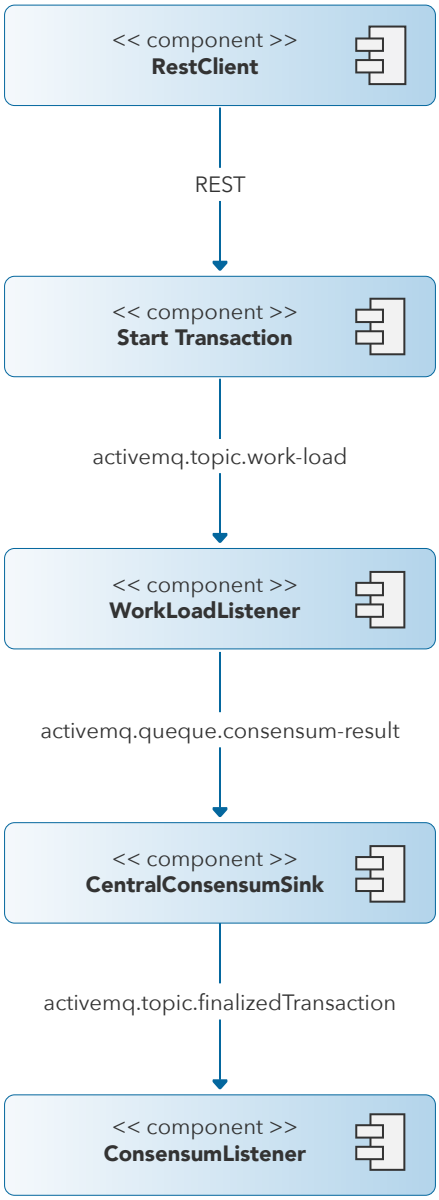


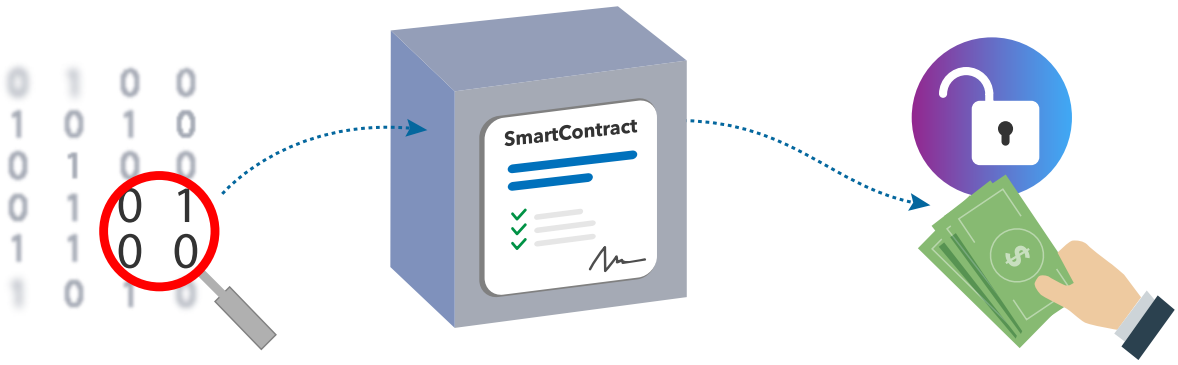
Leader-Node von Koordinationsclustern: dieser wiederum verteilt die Arbeit mittels eines proprietären Koordinationsprotokolls auf verschiedene Nodes;
Diese führen eine erste Überprüfung der Daten auf Vollständigkeit der Daten, Unterschrift

und Verfügbarkeit der Mittel durch, sowie auf vormals verwendete Hashes, Inactual Wallet States, blockierte Wallets oder Nutzer;
Jede zusätzliche Operation von der Sender-ID ist nun im flüchtigen Speicher gesichert, während spezifische Datenfelder abgeschlossen werden (wie vorherige, zu verknüpfende Transaktionen, Zeitstempel und vorherige Hashes);
Die Transaktion wird an ein Topic Message Queue19 mit einem Protokoll gesendet, das definiert werden muss
(AMQP für den Piloten, MQTT und andere noch zu definierende) und parallel die Arbeit auf die Nodes verteilt.
Worker-Nodes bestätigen ihr Interesse an der Verarbeitung der Anfrage (es könnten möglicherweise Daten fehlen, die Nodes könnten bereits beschäftigt sein, andere Bedingungen können noch auftreten), und schaffen daraufhin einen neuen Wallet-Status, stellen korrelierte Hashes früherer verknüpfter Transaktionen wieder her und fügen diese dem Transaktionsdatensatz hinzu.
Dann wird das Resultat des Proof of Integrity erfragt und der Transaktions-Hash berechnet;
Worker-Nodes registrieren die Transaktion im Speicher und senden ihr Votum an Koordinator-Nodes über eine Message Queue, wo die Ergebnisse gesammelt werden;
Wenn Voten und Hashes einheitlich sind, halten die Koordinatior-Nodes die Transaktion sowie den neuen Status des Wallets fest, vernichten die Hashes vorheriger Status und verbreiten die Abstimmungsgültigkeit über ein zusätzliches Topic Message Queue System.
Die Worker-Nodes schreiben nun ebenfalls die Transaktion und Veränderungen des Wallet-Statuses fest.
Ende des Best-Case-Szenarios für die vollständige Route.

Logischer Datenfluss

Detail des Prozessablaufs





Intelligente Verträge (Smart Contracts)

Multiversum glaubt an die Wichtigkeit, der Öffentlichkeit verbesserte Smart Contracts20 anbieten zu können. Aktuell wird diese Möglichkeit noch nicht konkret ausgelotet; dies gilt bis zu einer Ausweitung des Forschungsumfangs. Daher ist unser Ziel, in die Multiversum-Technologie diejenige Open-Source-Lösung zu integrieren, die unseren Anforderungen am besten gerecht wird, indem diese als Referenz gemäß ihres Lizenzmodelles implementiert wird.

Infrastruktur

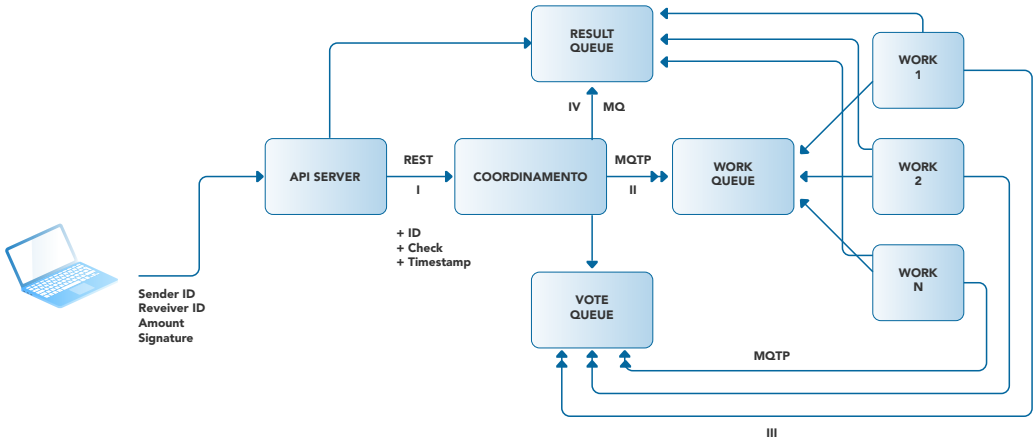
Die Multiversum-Infrastruktur ist darauf ausgelegt, Resilienz und Erreichbarkeit21 sicherzustellen. Dieses Ziel wurde erreicht über die Entwicklung von Node Clustern, die autonom den einzelnen Nodes spezifische Rollen zuweisen können, je nach technischer Ausrichtung des jeweiligen Node, wie z.B.:

- Rechenkapazität
- Speicherkapazität
- Gegenseitige Latenz
- Chaindaten-Vollständigkeit
- Maschinenzuverlässigkeit
- Zweifel am Integritätsnachweis / Proof of Integrity

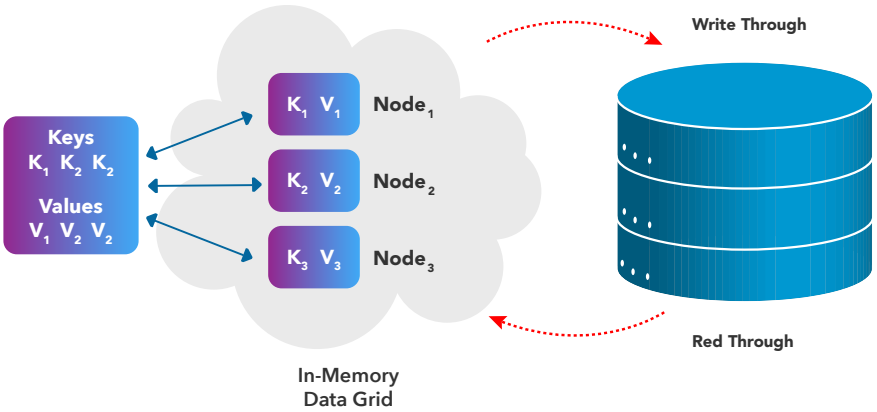
Nodes übernehmen dann eine oder mehrere Rollen:

- Clientnodes
- Koordinatornodes
- Nachrichtennodes
- Worker-Nodes
- Persistenznodes
- Sicherungsnodes

Jeder Node, der ein gültiges Zertifikat bereitstellen kann, kann sich beim Cluster registrieren und eine Rolle erhalten.
Im Falle eines Absturzes eines oder mehrerer Nodes kann der Cluster die Aufgaben autonom neu verteilen und optimieren.



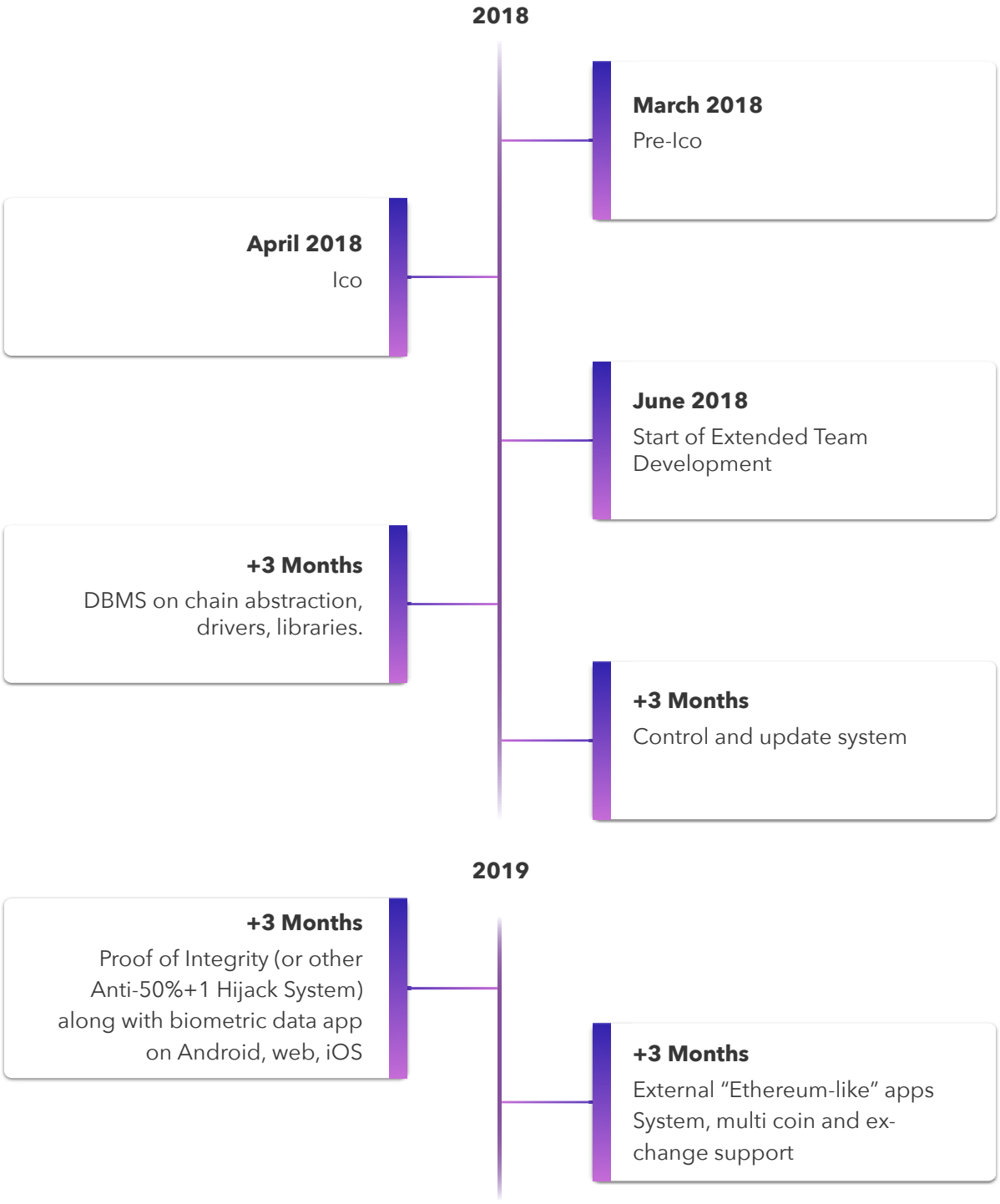
Komponenten des gemeinsam genutzten Caches intra JVM22 dienen als Speicherdatenbank und ermöglichen so:
Read-Through, d. h. Datenlese-Abfragen, die direkt im flüchtigen Speicher ausgeführt werden, bevor sie das physische Gedächtnis untersuchen.
Write-Through, lädt Daten im flüchtigen Speicher, bevor eine Masseninsertion der persistenten Daten ausgeführt wird, um die Leistung zu optimieren.



Hinweise zur Sicherheit

Während der Entwicklung bieten wir Entwicklern „Hacker's Bounties" bei Offenlegung von Schwachstellen und Vorschlägen einer wirksamen Lösung.

Technical Road Map

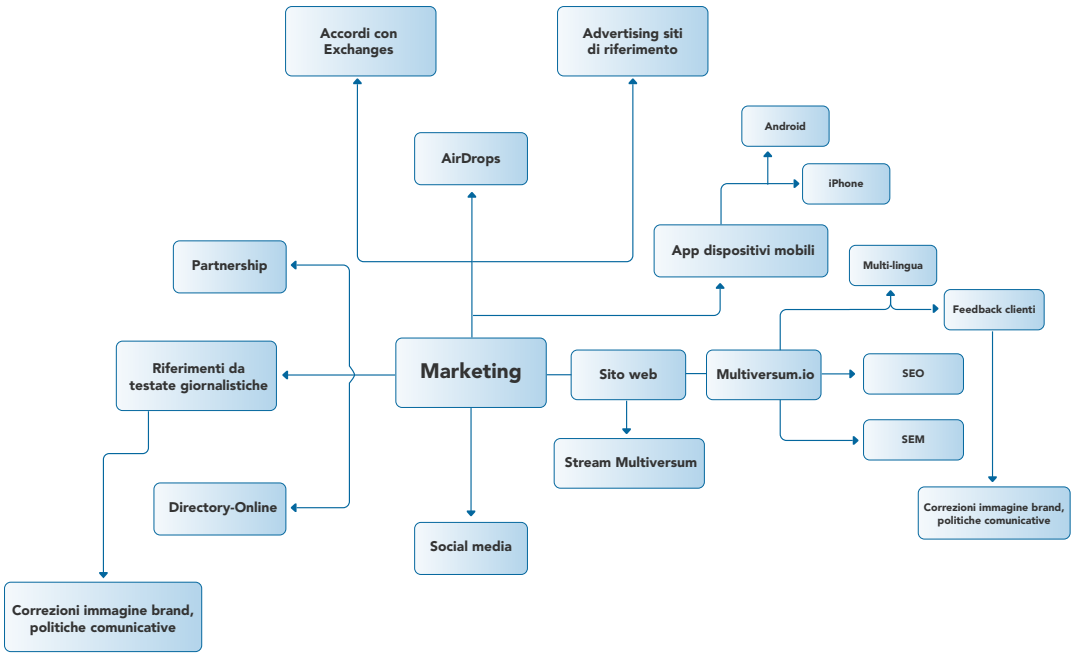


Marketing Strategie (Marketing Strategy)

Wir werden auf dem sich ständig verändernden IT-Markt unsere Strategie und Kommunikationstechniken und die Mission des Unternehmens entsprechend aktualisieren, mit Schwerpunkt auf der Schaffung von Mehrwert für die Anteilseigner und Sicherstellung eines angemessenen Gleichgewichts zwischen kurz- und langfristiger Managementlogik.

Die wichtigsten Punkte unseres Plans sind:

- Unternehmensphilosophie
- Geschäftsziele
- Geschäftsstrategien
- Portfolio der Geschäftsaktivitäten



Eines der wichtigsten Werkzeuge wird **Social Media Marketing** sein: Kampagnen in sozialen Netzwerken, um die Bekanntheit der Marke zu stärken, potentielle Kunden zu identifizieren, Kontakt herzustellen und bedeutsame Beziehungen zu Kunden zu schaffen. Unsere Social-Media-Strategen werden verschiedene Aktionen durchführen, die Teil einer einheitlichen Strategie sind; beginnend mit Management und Beobachtung von Kanälen durch spezielle Werkzeuge und Community-Entwicklung, mit Schwerpunkt auf Inhalten, Interaktion und Taktik-Effizienz-Einschätzung aufgrund erhaltener Ergebnisse.

Die Schichten aus Elementen, die die Universen umhüllen, sind jede zehnmal so dick wie die vorherige, und alle Universen, die traubenförmig zusammenhängen, erscheinen wie Atome in einer gewaltigen Verbindung.

Bhagavata Purana 3.11.41

MULTIVERSUM

HERE TO STAY