

MULTIVERSUM

HERE TO STAY

WHITE PAPER v 1.0.6

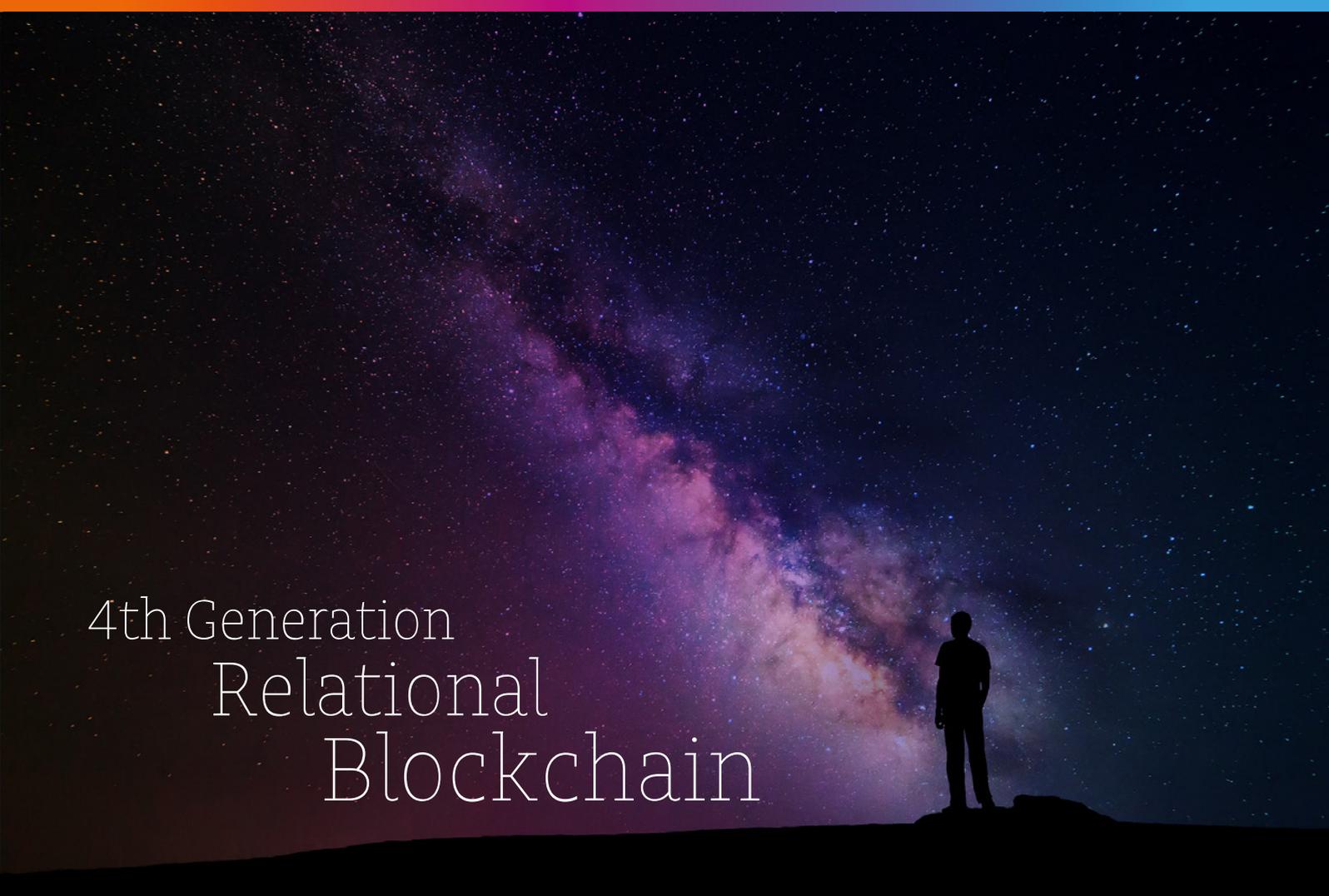
Business | Technical

Español

19.02.2018

Autores: Multiversum Team

www.multiversum.io



4th Generation
Relational
Blockchain



**Hay innumerables universos además
del nuestro, y aunque sean
infinitamente extensos, se mueven
como átomos dentro de Ti.**

Bhagavata Purana 6.16.37

Identidad y Misión de Multiversum

La primera generación de blockchain está constituida por las primeras monedas como el Bitcoin, basadas en Pruebas de Trabajo y sus diferentes clones y ramificaciones. Los BC de segunda generación son más heterogéneos, basados sobre el empleo de tokens como Ethereum y su ecosistema de soluciones.

Estas dos categorías se caracterizan por una bajísima eficiencia energética y un reducido número de transacciones. A la tercera generación pertenecen aquellos BC que han intentado proveer respuestas a la lentitud de las transacciones y a la incapacidad de ser escalables utilizando varios mecanismos: Prueba de Acción, ruta off chain, graphchain, centralización completa o parcial.

La cuarta generación, en cambio, se propone seguir dando respuestas a la lentitud del sistema; al mismo tiempo se pone objetivos de utilidad en el campo empresarial, cosa para la que una cadena desorganizada de datos que necesitan sistemas complejos de almacenamiento de datos organizados en tableros correlacionados (como las bases de datos relacionales) se prestan muy poco, pero al mismo tiempo en la que los datos se convalidan y refuerzan con la técnica de la blockchain. Es decir, es el intento de hacer desembocar esta tecnología en una verdadera utilidad productiva primaria.

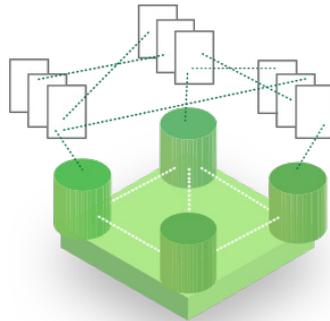
Multiversum ofrece la gestión organizada de los datos complejos en lugar de una sucesión simple de los datos, la divisibilidad de la cadena y unión para permitir el paralelismo y verificación de la factibilidad de la Prueba de Integridad (prueba criptográfica del código del servidor) en lugar de la Prueba de Trabajo.

Además se suman aparatos de interoperabilidad con otras cadenas (hospedando en nuestra cadena otras monedas y tokens y viceversa) y un servicio de notaría que funcione como validación externa. Mientras tanto, además de todas nuestras innovaciones, emplearemos ciertamente también algunas de las óptimas soluciones que nuestros colegas ya han implementado.

Multiversum

Blockchain Relacional de Cuarta Generación

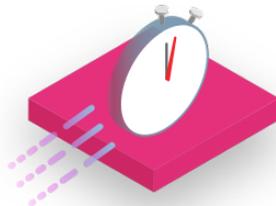
¿Por qué Multiversum es la Blockchain 4.0?



Blockchain Relacional

Una blockchain de nueva generación, que pasará del poder administrar un sólo tipo de datos en forma lineal a más tipologías de datos, relacionados entre ellos a través de identificativos, en una estructura multidimensional.

< 0,2 sec

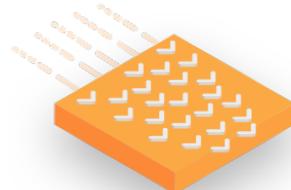


Velocidad de Transacción

En menos de apenas 0,2 segundos los fondos son transferidos de una cartera a otra cumpliendo todos los diferentes pasos que certifican su seguridad.

Está entre las blockchain más rápidas del mundo.

64000 tps → ∞



Cantidad de Transacciones

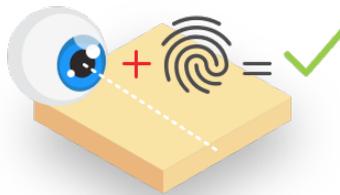
Hasta 64000 TPS en un servidor a 64 núcleos (1000 TPS por núcleo), soporte a sistemas de más de 64 núcleos - escalabilidad sin límites.

POI



Seguridad extrema de Transacción

Ya no existirá el concepto de POS (Proof of Stake, o Prueba de Acción):
qué será sustituida por la POI (Prueba de Integridad).



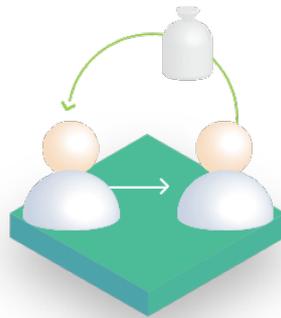
Cartera de Nueva Generación / Entrada Biométrica

Extrema seguridad en el acceso a la cartera y en el envío de los fondos
a través de entradas biométricas.



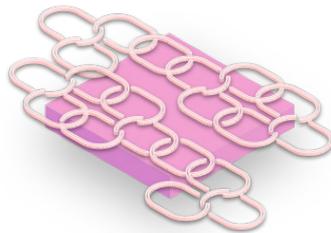
Amigable con el Medio Ambiente

Una transacción tendrá costos irrelevantes
y un impacto ambiental casi nulo.



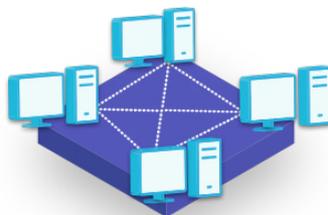
Rollback

El sistema de *rollback* será opcional y estará disponible en soluciones ad-hoc que puedan beneficiarse de esta función.



Cadenas que se pueden desdoblar

Optimización de la carga de trabajo con una distribución de los recursos entre los nodos disponibles gracias a la posibilidad de subdividir la cadena principal en más sub-cadenas.



Asignación de Nodos de Recuperación

La empresa Multiversum ha colocado nodos periféricos de Global Disaster Recovery en diferentes continentes.

Presentación al público

El Concepto de Multiversum y su uso en una escala Global

Multiversum es una tecnología que, modificando los aspectos pertinentes a la persistencia de los datos en la Blockchain a través de datos distribuidos que se auto verifican, organizados en entidades coherentes relacionadas entre ellos con enlaces simbólicos, revoluciona sus límites tradicionales, llevando, de hecho, a una nueva generación: la Blockchain 4.0.

En esta tecnología se basa un sistema descentralizado y distribuido de transacciones coherentes y que se verifican automáticamente: el Multiversum BC. Las Blockchain actuales se basan en una secuencia de transacciones que representan un único tipo de dato: pertinente a la transacción misma o a múltiples cadenas coexistentes y no firmemente coherentes entre sí, en la que los datos están organizados en blob conceptuales y atribuibles el uno al otro con dificultad y grandísimos costos computacionales.

Multiversum permite, en cambio, crear una Cripto Base de datos Relacional, una solución avanzada y organizada para el almacenamiento de los datos, que permite tener no un solo tipo de dato sino una serie de datos asociados en tableros en una estructura de datos complejos, relacionados el uno con el otro a través de un identificativo.

Cada uno de ellos, en el momento en que un estado cambie, tendrá una sub-cadena propia proveniente de un nodo ya certificado y se reunirá, para conseguir la certificación, con todo el resto de la cadena.

Multiversum es, por tanto, una tecnología Blockchain evolucionada que ofrece características únicas para solucionar estos problemas en un panorama de cripto validación y distribución, y que podrá ser usada en cualquier entorno: Administrativo, Industrial, Fi-

nanciero y Gubernamental. Uno de los objetivos principales de Multiversum es ofrecer al mercado, en todo momento, el producto más desarrollado disponible: eso será posible utilizando una metodología denominada AGILE.

Este enfoque nos permitirá entender las necesidades del mercado, durante y después de la fase de desarrollo, y de implementarla progresivamente, llegando a publicar el Main Net más desarrollado y completo disponible. Esta técnica de desarrollo, nos permite ofrecer el producto más moderno y actual del mercado.

Velocidad y Tecnología

Un punto fuerte de esta tecnología es indudablemente su velocidad, que se debe a la capacidad de poder procesar paralelamente diferentes transacciones. Esta característica permite tener una perfecta escalabilidad horizontal o sea la posibilidad de poder aumentar al infinito la capacidad de elaboración de las transacciones, añadiendo nuevos procesadores en lugar de reemplazar aquellos existentes, devolviendo cada nodo adicional útil para mejorar las prestaciones del entero sistema.

Escalabilidad Horizontal

Multiversum posee dos peculiaridades muy importantes que la hacen ser así de eficiente: La cadena es capaz de optimizar la misma estructura dividiéndose autónomamente en más sub-cadenas con base en los recursos requeridos y al flujo de datos, distribuyendo así el trabajo del cluster de procesadores de forma óptima entre los nodos dispuestos para la elaboración.

Esta subdivisión podrá ser efectuada infinitamente hasta la normalización de las cargas de trabajo, cuando, siempre de modo autónomo, la cadena volverá a ser una. Todo esto gracias a un aparato que permite a cada anillo convalidar dos cadenas diferentes de los dos diferentes eslabones anteriores.

La posibilidad de hacer el sharding de los datos: una técnica que permite la distribución de los datos entre más nodos. Imaginando de tener una serie de datos ABC y tres nodos del Cluster, tendremos una subdivisión de los datos dispuestos de la siguiente forma:

AB

BC

CA

Esta subdivisión permite una mayor velocidad de elaboración de las transacciones que pasarán a investigar los datos sólo en los nodos que las contendrán, optimizando cada paso.

Otra característica presente muy importante se llama High Availability, o Alta Disponibilidad: la posibilidad de basarse en una tipología de cluster que también garantiza continuidad de los servicios en caso de interrupción de algunos nodos de la red.

Utilizando el ejemplo anterior (nodos A., B y C) si C se interrumpiera, los nodos A y B quedarían completamente operativos, permitiendo la continuidad del servicio sin ninguna pérdida de datos mientras estén operativos al menos el 50% + 1 de los nodos totales.

El cluster, en esta situación, comunicando con todos los nodos, organizará autónomamente la distribución de los datos hasta el completo restablecimiento operativo.

Entorno

Multiversum además es amigable con el medio ambiente, porque se pone como objetivo la eliminación de la minería, un derroche de potencia de cálculo y energías inmensas, que sustenta la Prueba de Trabajo, a favor de un nuevo concepto, la Prueba de Integridad: un protocolo que verifica la veracidad y la autenticidad del software que solucionará cualquier persistencia de la transacción.

Gestión de los datos: Base de datos Relacional

Multiversum, con su Cripto Base de datos Relacional, puede estructurar fácilmente los datos sin límites en el tipo de enlaces.

Cada cartera tendrá una serie de estados (estados) y estará conectada a una persona (usuario); cada nuevo anillo de cambio del estado de la cartera incorporará dos cosas:

- el estado anterior, de manera tal de tener la validación del acto precedente;
- un enlace a la última transacción, o al último anillo de la cadena principal, mediante el cual se sabrá de dónde deriva el nuevo anillo del cambio de estado. Ocurrido este cambio, se añadirá la transacción de modificación y, con esta, se reunirá el anillo del estado modificado, que indicará la procedencia del enlace del nuevo cambio de estado. La nueva transacción, por tanto, heredará dos hashes: uno del anillo de estado, uno del anillo de la transacción anterior. De esta manera todas las operaciones convalidan las anteriores relacionadas a la transacción misma. Este sistema es tan complejo como avanzado, y permitirá implementar software en nuestra tecnología garantizando una difusión institucional, gubernamental, financiera e industrial, llevando todo el mundo de los Blockchain a un nivel superior.

En conclusión...

Este enfoque nos permitirá entender las solicitudes del mercado durante y después de la fase de desarrollo, e implementarlas progresivamente para publicar el MainNet más desarrollado y completo disponible. Lo será en ese entonces y también lo será en el futuro. Multiversum publicará inmediatamente un Piloto de Blockchain funcional y una APP propietaria como Cartera en versión Beta. En 6 meses los productos estarán completos y serán actualizados cotidianamente con base en las exigencias. Ninguna Blockchain posterior al BTC, en su lanzamiento, ha podido jactarse de tanto desarrollo anticipado. El valor del Coin y el Token no podrán sino beneficiarse de ello.

Análisis de la Vanguardia de las Blockchain

El Concepto de Multiversum y su uso en una escala Global

Actualmente, los actores principales del “fenómeno blockchain” se caracterizan por una notable robustez en materia de seguridad.

Frente a eso, tal seguridad implica una capacidad de cálculo enorme, polución, comisiones de las transacciones inaceptables y una lentitud incapaz de representar el progreso tecnológico actual, invalidando la posibilidad de dar una respuesta técnica creíble a los casos de uso financieros y comerciales modernos.

Tal lentitud es causada por la incapacidad de conseguir una escalabilidad horizontal, es decir, el aumento de la capacidad de cálculo que se obtiene mediante la simple adición de procesadores en lugar de su sustitución con versiones más veloces.

Un segundo motivo de escasa eficiencia proviene del mecanismo de seguridad de las blockchain actuales basadas en la Prueba de Trabajo y, menos frecuentemente, en la Prueba de Acción, que pasan por alto el riesgo de perder el control de la mayoría del cluster a causa de Sybil Attacks solicitando a los nodos una capacidad de cálculo artificialmente alta, lo que hace imposible una creación indiscriminada por el aumento de la dificultad. Además, las blockchain actuales son simples sucesiones de cambios de estado de entidades individuales de datos: la reconstrucción de los estados actuales, solicitando un barrido de la entera cadena, implica una ulterior lentitud del sistema y un derroche de recursos. Tal configuración además hace inadecuado el empleo de la tecnología blockchain en un contexto industrial y científico, entornos en los que las estructuras de datos

son extremadamente complejas.

La seguridad garantizada por las blockchain actuales concierne únicamente a los datos, pero no se extiende al usuario: es imposible, por ejemplo, recobrar monedas o token injustamente sustraídos, también en el caso de que hayan estado localizados en la cadena, o detener cuentas implicadas en actividades ilícitas. Un último problema es la total falta de homogeneidad e incomunicabilidad en el panorama de las múltiples criptomonedas: toda Blockchain, existiendo en un propio universo separado, resulta incapaz de relacionarse con las otras.

Metodología AGILE

Multiversum se propone utilizar la metodología AGILE durante el desarrollo del producto. Esta técnica presupone una drástica reducción del planeamiento inicial, en favor de la valorización de las experiencias conseguidas en el progreso de los trabajos, que evidencian oportunidades y peligros que de otro modo sería difícil identificar antes del lanzamiento, premiando las Mejores Prácticas y perjudicando los Métodos de Trabajo (modalidades operativas) inadecuados.

La metodología ÁGIL es el Estándar Industrial de la producción del software y sugiere a los desarrolladores, propietarios de producto e inversionistas que consideren flexible el objetivo del proyecto, para adaptarlo a la variación de las exigencias del mercado. Además, en un sector que evoluciona rápida y constantemente como el del software, proponer al mercado, después de un período típico de seis meses de estudio y un año de implementación, un producto nacido para satisfacer las exigencias de 18 meses antes, significaría ofrecer una solución anticuada, que no soluciona problemas actuales, que probablemente ya han sido superados por la competencia y ser incapaz de dar respuestas a los nuevos desafíos. AGILE, al revés, permite ofrecer al mercado el producto más innovador posible al momento de la entrega del proyecto.

MULTIVERSUM

HERE TO STAY

Unique Features !

Crypto relational DB

Autovalidating Complex
Data structures

Proof of Integrity

(Protocol Innovation)

Divisible/Re-joinable chains

(Parallel Work)

Biometric Data integration as Electronic Signature seed

(User Security)

Sharding data

(Parallel Work)

Double Access Lock

(Structural Security)

Minimal ecological footprint

Reverse Access Denial

(Structural Security)

Reciprocal chain confirmation

(Interoperability with other BC)

Rollback

(User Security)

Advanced API offer

Native off-chain adapter for own ERC20

(Interoperability with other BC)

Self managing Crypto-Cluster

Java, Spring and Javascript

(Libraries for Integration)

Native on chain adapter for own ERC20

(Interoperability with other BC)

Freezable wallets

(User Security)

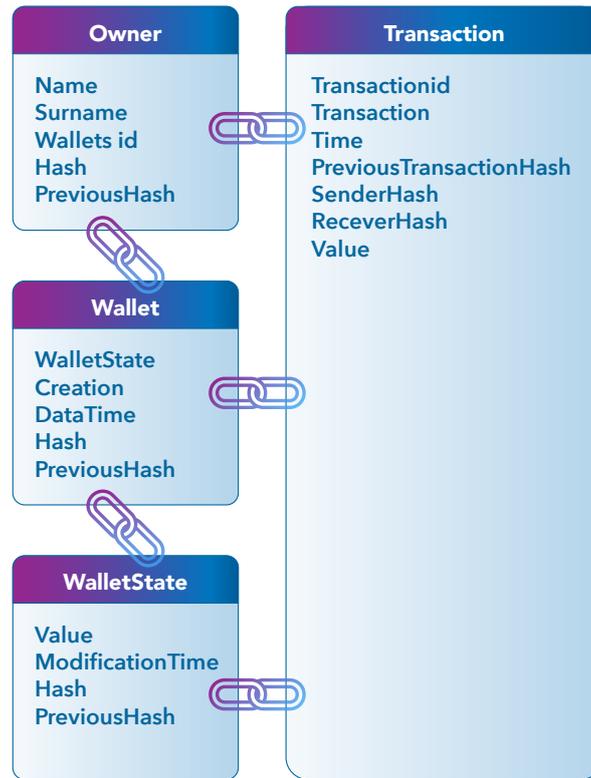
ERC23

(Interoperability with other BC)

Misión de Multiversum

Multiversum se propone estudiar soluciones para permitir un salto generacional en el mundo de las blockchain, en particular, como Unique Selling Points, se pone los siguientes objetivos:

1. Realización de una Base de Datos Cripto con Estructuras Complejas de Datos auto-convalidantes
2. Cadenas divisibles y reunibles en relación a la cantidad de trabajo necesario (Trabajo en Paralelo)
3. Sharding de los datos (Trabajo en Paralelo)
4. Oferta de una API Avanzada
5. Rollback (Seguridad del Usuario)
6. Carteras multi divisa congelables (Seguridad del Usuario)
7. Integración de los datos biométricos como entrada para la Firma Electrónica
8. Interfaz ERC23 (Interoperabilidad con otras Blockchain)
9. Adaptadores nativos off-chain para la propia ERC20/ERC23 (Interoperabilidad con otras Blockchain)
10. Adaptadores nativos off-chain para los huéspedes de la ERC20/ERC23 (Interoperabilidad con otras Blockchain)
11. Prueba de Integridad (Innovación del Protocolo)
12. Bloqueo Doble del Acceso (Seguridad Estructural)
13. Denegación del Acceso Inverso (Seguridad Estructural)
14. Confirmación Recíproca de Cadena (Interoperabilidad con otras Cadenas de Bloque)
15. Integración para Java, Spring y Javascript
16. Modelo ACID
17. Modelo Transaccional
18. Lenguaje SQL-like



1. Realización de una Base de Datos Cripto relacional con Estructuras Complejas de Datos

Multiversum tiene una fuerte vocación por su uso en contextos industriales, institucionales, públicos y empresariales: ambientes que requieren estructuras de datos complejas, imposibles de representar de manera eficiente y normalizada con una cadena simple.

Esta vocación se manifiesta con el deseo ser la primera base de datos cripto relacional a disposición del mercado, distribuida y opcionalmente descentralizada. Dicha primacía ha sido alcanzada partiendo de la conceptualización de entidad chainable. Éstas entidades permiten la implementación de una interfaz capaz de definir los métodos necesarios a un dato para que pueda ser insertado como un eslabón en la blockchain.

En el modelo conceptual existirá una cadena primaria a la que se enlazarán cadenas secundarias que representan entidades diferentes, que, a su vez, representan los records de un tablero.

Dichas entidades se enlazarán ulteriormente a su último estado de persistencia y después de las modificaciones necesarias se reunirán en el último eslabón de la cadena primaria que reunirá las dos cadenas. La interfaz "chainable" presupone: la grabación de múltiples eslabones de los que derivarse de nuevo, la grabación de los múltiples eslabones que derivan del individual y la de la validación de la presencia de tales datos, que actúa importando los hash de los eslabones emplazados en el cómputo del hash corriente.

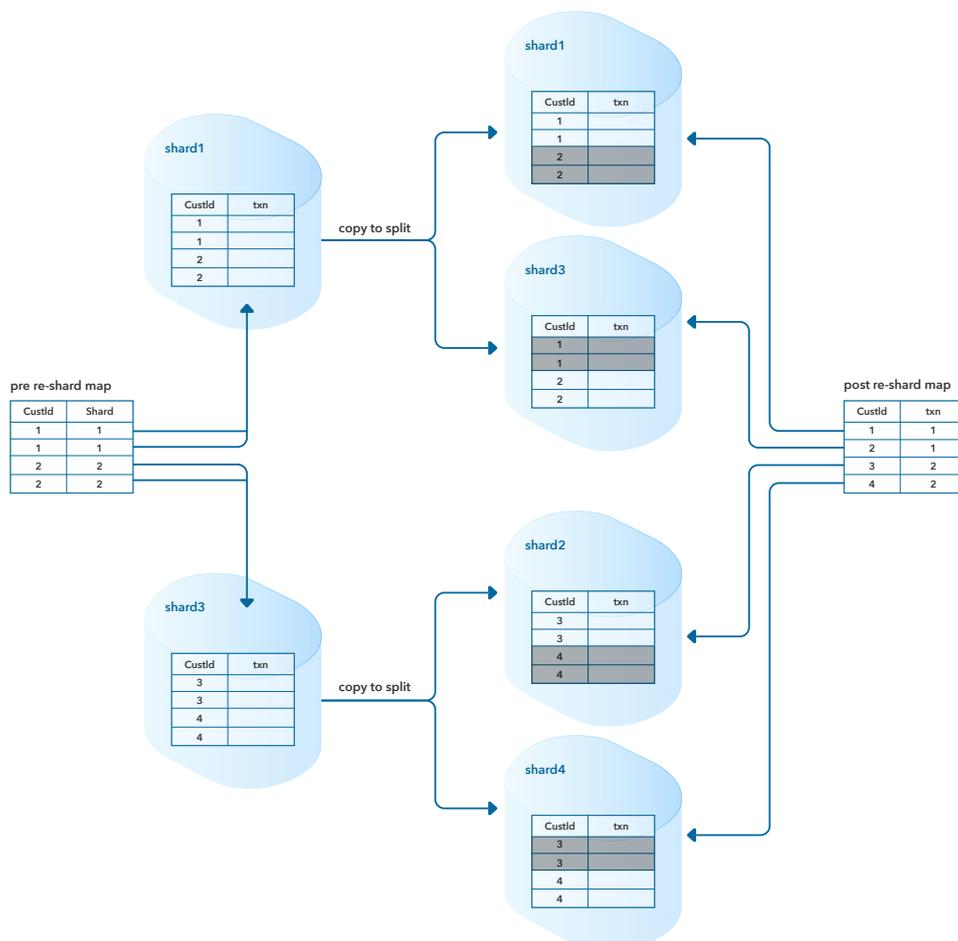
En la implementación de la tecnología Multiversum relativa a las monedas Versum, las entidades chainable que convivirán en la cadena pertenecerán a cuatro Tableros: Usuario, Cartera, Estado de la Cartera y Transacción, que se correlacionarán entre sí convalidándose recíprocamente.

2. Cadenas divisibles y reunibles en función de la cantidad de trabajo necesario (Trabajo Paralelo)

La capacidad de derivar múltiples eslabones a partir de uno y, sucesivamente, reunirlos deriva del empleo de analizadores de la carga de trabajo que, en presencia de un alto número de solicitudes de ejecución, señalarán al cluster la necesidad de dividir, infinitas veces, si es necesario, la cadena primaria de las transacciones en dos cadenas secundarias y, al reducirse la misma, exista forma de reunir las múltiples sub-cadenas anteriormente generadas. Este mecanismo permite el trabajo paralelo, lo que permite seguir ofreciendo tutela a la alteración de los registros de las transacciones.

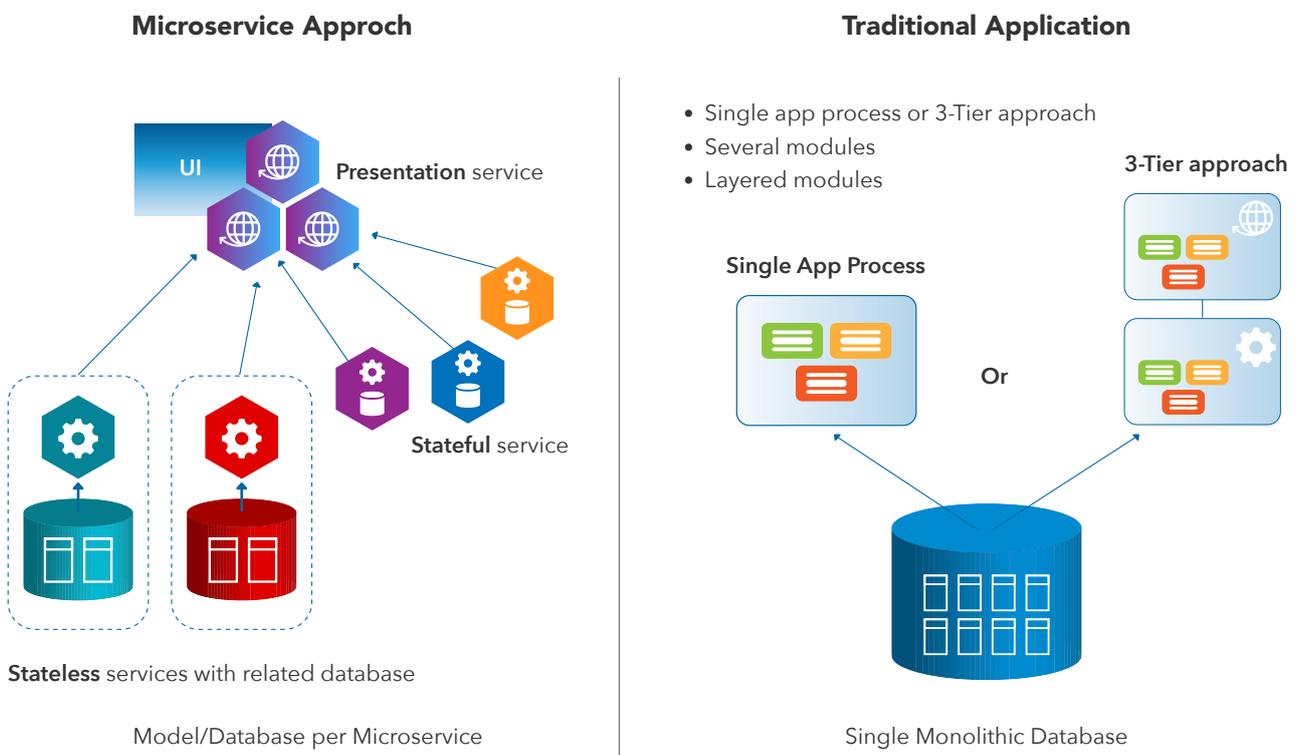
3. Sharding de los datos (Trabajo en Paralelo)

Cada nodo podrá tener en memoria todos los datos del blockchain o sólo una parte de ellos. En el caso de que se manifestara la necesidad de paralelizar los datos, los nodos



coordinadores establecerán las modalidades de subdivisión de manera tal de optimizar la distribución a través de parámetros de paralelización del cálculo y la Alta Disponibilidad, garantizando (siempre que el 50% +1 de los nodos quedará online) la disponibilidad de los datos incluso en caso de desaparición instantánea de una parte del clúster de persistencia. Tales nodos, en la fase siguiente al bloqueo parcial del clúster, serán capaces de redistribuir y reorganizar sus datos de forma independiente, de modo de poder afrontar una vez más un bloqueo parcial del clúster lo antes posible.

Los dispositivos descritos en este punto y en el anterior, permiten la capacidad de trabajo paralelo, es decir: escalabilidad horizontal, seguridad, alta disponibilidad, resistencia del sistema, falta de un único punto de falla¹⁰ y autorecuperación de desastre.



4. Estructura de microservicio y oferta de Advanced API

Multiversum, ha sido desarrollado sobre una plataforma basada en parte en Micro-servicios y en parte en el modelo Serverless, y también gracias a las API modernas, extensas y seguras, con características idempotentes, tendrá la capacidad de adaptarse a ambas estructuras.

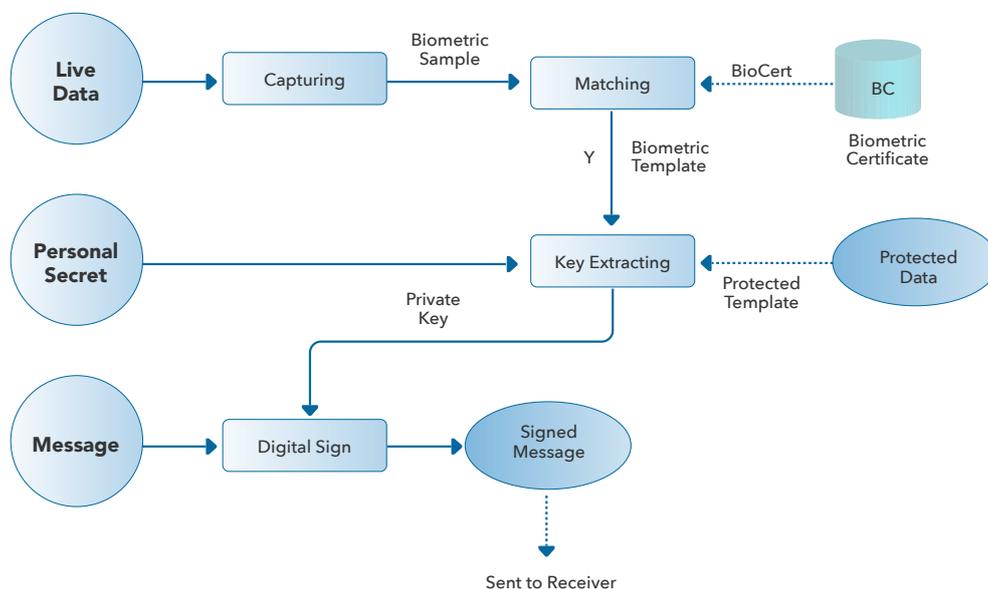
5. Rollback (Seguridad del Usuario)

La tecnología de Multiversum permite, en el contexto de una transacción, revertir las operaciones indeseadas, o bien restaurar un estado anterior sin afectar la credibilidad de la validación de la cadena, pero implementando nuevas transacciones programáticas para restaurar el Estado deseado.

Una vez evaluada la factibilidad desde el punto de vista de la Lógica de Negocios, será considerada la posibilidad de implementar en las monedas Versum esta funcionalidad y ampliarla con efecto retroactivo. En la cadena pública esta funcionalidad no será implementada, pero los casos de Uso patentados que hacen referencia a la tecnología Multiversum serán libres de implementarla.

6. Freezable wallets (Seguridad del Usuario)

Una vez evaluada la factibilidad desde el punto de vista de la Lógica del Negocio, será estudiada la posibilidad de implementar la congelación temporal de las monedas Versum de un portafolio como resultado de actividades ilícitas.

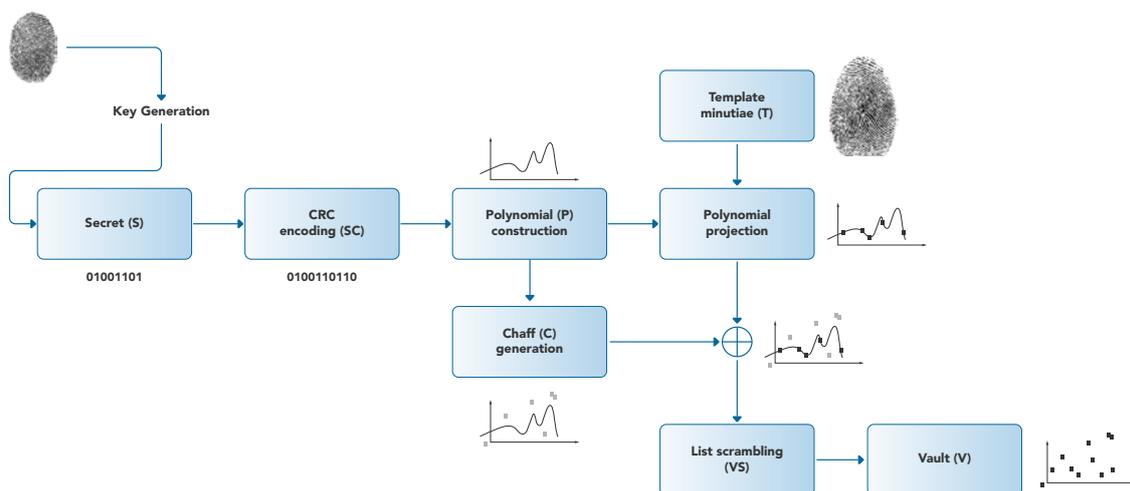


Biometric Digital Key Generation Framework

7. Integración de los datos biométricos como cimiento para la Firma Electrónica

Refiriéndose a los estudios de los profesores Je-Gyeong Jo, Jong-Won Seo y Hyung-Woo Lee del Hanshin University (República de Corea) y sintetizados en la publicación “Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint”, se estudiará la factibilidad del empleo de datos biométricos como huellas digitales, imagen del iris y firma grafométrica como fuente de la llave criptográfica asimétrica como garantía de la identidad del firmante de la transacción.

Para permitir el empleo de los datos biométricos encriptados en la fase de disputa legal, será evaluada la seguridad de la inserción. En cualquier caso, estos datos serán utilizados en las aplicaciones para Android e iOS.



Fuzzy Vault Scheme for Biometric Digital Key Protection

8. Interfaz ERC23 (Interoperabilidad con otras Blockchain)

Para garantizar la interoperabilidad con otras cadenas, las monedas Versum serán desarrolladas implementando la interfaz ERC23, versión avanzada y retrocompatible de ERC2014.

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

9. Adaptadores nativos off-chain por el propio ERC20/ERC23 (Interoperabilidad con otros Blockchain)

Para permitir la entrada y la salida de sus propias monedas y tokens en otras cadenas no propietarias, Multiversum desarrollará un adaptador nativo, comparándolo con un buffer que regulará la entrada y la salida de la cadena propietaria.

10. Adaptadores nativos off-chain para ERC20/ERC23 huéspedes (Interoperabilidad con otros Blockchain)

Para permitir la entrada y la salida de monedas y tokens no propietarias en su cadena, Multiversum desarrollará un adaptador nativo, comparándolo con múltiples buffer que regularán la entrada.



Integrity

11. Prueba de Integridad (Protocolo de Innovación)

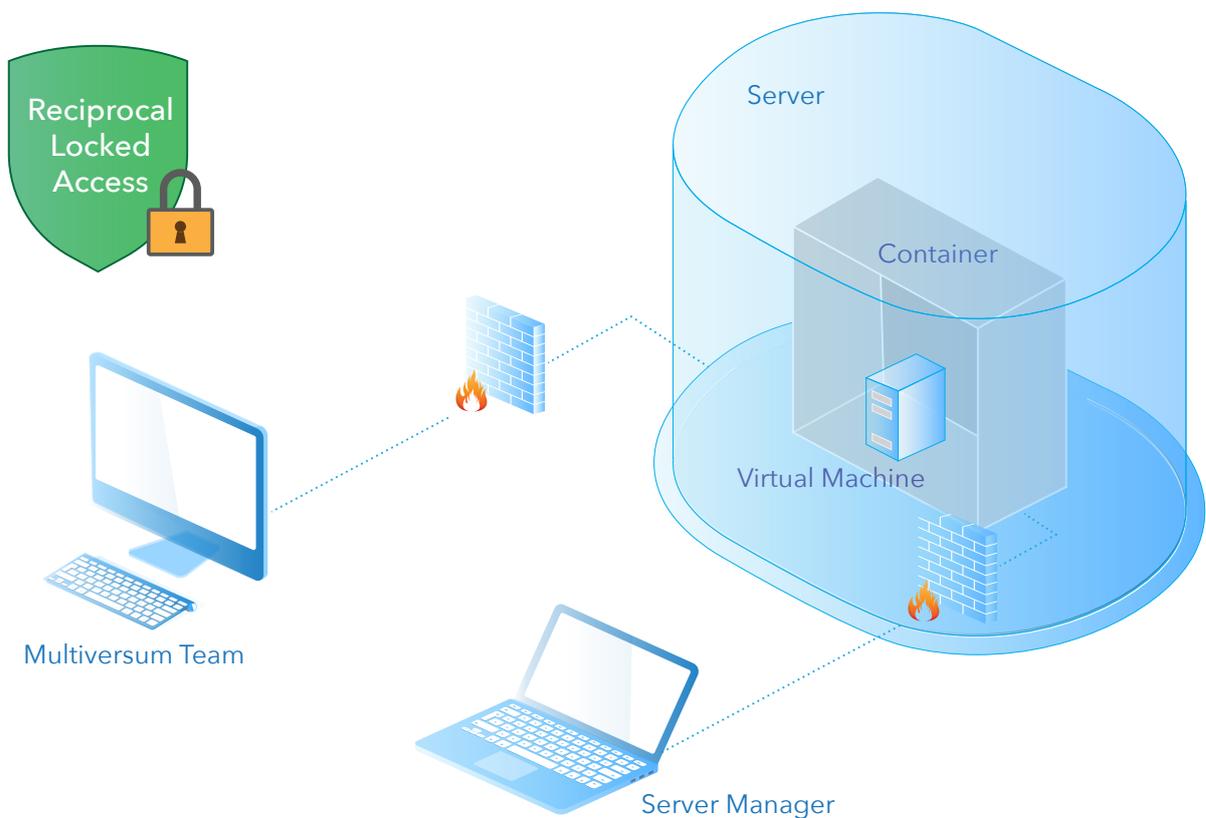
Como alternativa a la Prueba de Trabajo y a la Prueba de Participación en sus diversas formas, Multiversum introduce la Prueba de Integridad, que es un dispositivo de verificación criptográfica de la sinceridad del código del nodo compilado y de la uniformidad de respuesta de parte de la mayoría de los nodos con respecto a un simiente de desafío aleatorio, que, combinado al hash calculado por un componente externo, (no descompilable, protegido y comunicado con el software del nodo en un canal encriptado), del software mismo, y a los datos de la transacción, tiene que ser lo mismo en cada transacción individual para todos los nodos. Este proceso requiere una potencia de cálculo notablemente inferior y evita los desperdicios típicos de otros sistemas (PoW) PoS, DPoS,; además provee una seguridad mayor y real, no de tipo estadístico o de supuestos basado en el modelo del Consenso Bizantino, particularmente vulnerable en clúster de dimensiones reducidas.



Access Denied

12. Doble Acceso de Bloqueo (Seguridad Estructural)

Los nodos serán distribuidos en Contenedores Virtuales inaccesibles al operador de la máquina Host ya que están protegidos por credenciales no disponibles para el mismo operador. La seguridad, por lo tanto, está remitida a las mejores prácticas de la Seguridad Linux a través, por ejemplo, del paquete SeLinux y otros. Al mismo tiempo, incluso si alguien tuviera las credenciales de la máquina Invitada, en todo caso no podría acceder a ella, ya que no tendría acceso al equipo host en el que se ejecuta el nodo. El nodo, por lo tanto, está sujeto de hecho a un doble cierre para el acceso.



13. Denegación de Acceso Inverso (Seguridad Estructural)

El doble cierre discutido en el punto 12 implica un efecto de prevención recíproca en el acceso del nodo. Esto garantiza que los nodos no administrados directamente por Multi-

versum sean perfectamente auténticos e inaccesibles para cualquiera, fundamentalmente autónomos, y aislados de intervenciones humanas externas.

Además de los del Sistema Operativo y de la Seguridad, otros tres componentes fundamentales serán distribuidos en el Contenedor: el código compilado del Servidor Multiversum, un certificado con clave asimétrica para la autenticación en el clúster Multiversum y un componente ya discutido en el punto 11, responsable del cálculo del desafío basado en el hash del código del servidor, del certificado, de la simiente de desafío y de los datos de la transacción.

Además, este componente, será el único accesible al operador para verificar la sinceridad del código compilado del servidor que se ejecuta en la máquina, (quedan por verificar las desventajas). Otras funciones opcionales de seguridad podrán ser implementadas, como la posibilidad de cambiar automáticamente la contraseña de acceso al contenedor, mientras se está compilando, con una contraseña aleatoria desconocida, impedirá fin de evitar el acceso a cualquiera.

Tal mecanismo puede ser también implementado por el certificado de acceso al clúster.

14. Confirmación Recíproca de Cadena (Interoperabilidad con otras blockchain)

Multiversum verificará la factibilidad de un componente para registrar los estados de otras cadenas de modo de certificar su estado y reforzar mutuamente su credibilidad y la validación de las transacciones (eventualmente frente a un token). Por lo tanto, si se considera una solución deseable, este componente será implementado.

Multiversum desea utilizar la misma posibilidad de registrar periódicamente una transacción para poder compartir la responsabilidad de la verificación de un estado en otras cadenas.

Proveerá una interfaz especializada para la función y promoverá su implementación en nuevas cadenas. Este componente hará uso de un componente serverless al que también se puede acceder luego de la compilación del contenedor para permitir la adición de adaptadores a otras cadenas.

15. Integración para Java, Spring y JavaScript

Considerada su vocación de uso en entornos industriales, financieros, legales, públicos, administrativos y empresariales, Multiversum desea implementar una nueva capa de abstracción sobre las modalidades en base a su funcionamiento, ofreciendo interfaces de alto nivel recopiladas en librerías funcionales para Java, Javascript y opcionalmente para otros lenguajes principales.



También serán desarrollados módulos de integración a frameworks como Spring en un proyecto Spring Multiversum. Estas librerías facilitarán la integración de la tecnología Multiversum en soluciones patentadas, tanto en la creación de cadenas privadas, como en su acceso a la MainNet oficial.

16. Modelo ACID

Multiversum implementará un modelo definido ACID. El acrónimo deriva del inglés Atomicity, Consistency, Isolation, Durability (Atomicidad, Consistencia, Aislamiento y Durabilidad), e indica las propiedades lógicas que deben tener las transacciones.

Para que las transacciones funcionen correctamente en los datos es necesario que los mecanismos que las implementan satisfagan estas cuatro propiedades:

Atomicidad - la transacción es indivisible en su ejecución y su ejecución tiene que ser o completa o nada, no se admiten ejecuciones parciales;

Consistencia - cuando inicia una transacción, la base de datos se encuentra en un estado coherente, y cuando la transacción finaliza la base de datos tiene que estar en otro estado coherente, o bien no debe violar eventuales vínculos de integridad; por lo tanto no deben existir contradicciones (inconsistencia) entre los datos archivados en la DB;

Aislamiento - cada transacción debe ser ejecutada de modo aislado e independiente de las otras; la eventual falla de una transacción no debe interferir con otras transacciones en ejecución;

Durabilidad - llamada también persistencia, se refiere al hecho de que, una vez solicitado un commit work desde una transacción, los cambios realizados ya no deben perderse, para evitar que, en el periodo de tiempo comprendido entre el momento en que la base de datos se compromete a escribir las modificaciones y aquel en que las ha escrito efectivamente, ocurran pérdidas de datos debido a funcionamientos defectuosos.

17. Modelo Transaccional

Multiversum persistirá en los datos conectados a una transacción en un modelo “transaccional”, es decir, asegurándose que cada uno o ninguno de los datos sobre los múltiples subgrupos de monedas en algún momento se conviertan en persistentes, para garantizar la coherencia de cada transacción ejecutada y la integridad de los datos.

18. Lenguaje como SQL

Para garantizar la facilidad de composición de las consultas, Multiversum se basará en una sintaxis similar a la de SQL, utilizando un lenguaje parecido al estándar del sector. De este modo, la curva de aprendizaje de quien se acerca a este componente por primera vez, resulta bastante dulce.

19. Funcionamiento y Ruta Completa de Flujo de Datos

El proceso de aceptación, control, validación y persistencia de una transacción ocurre en la modalidad esquematizada y simplificada a continuación.

El mejor caso de ruta completa sigue este proceso:

La transacción es enviada a un cliente REST, se completa con los datos necesarios y se firma con una clave privada.

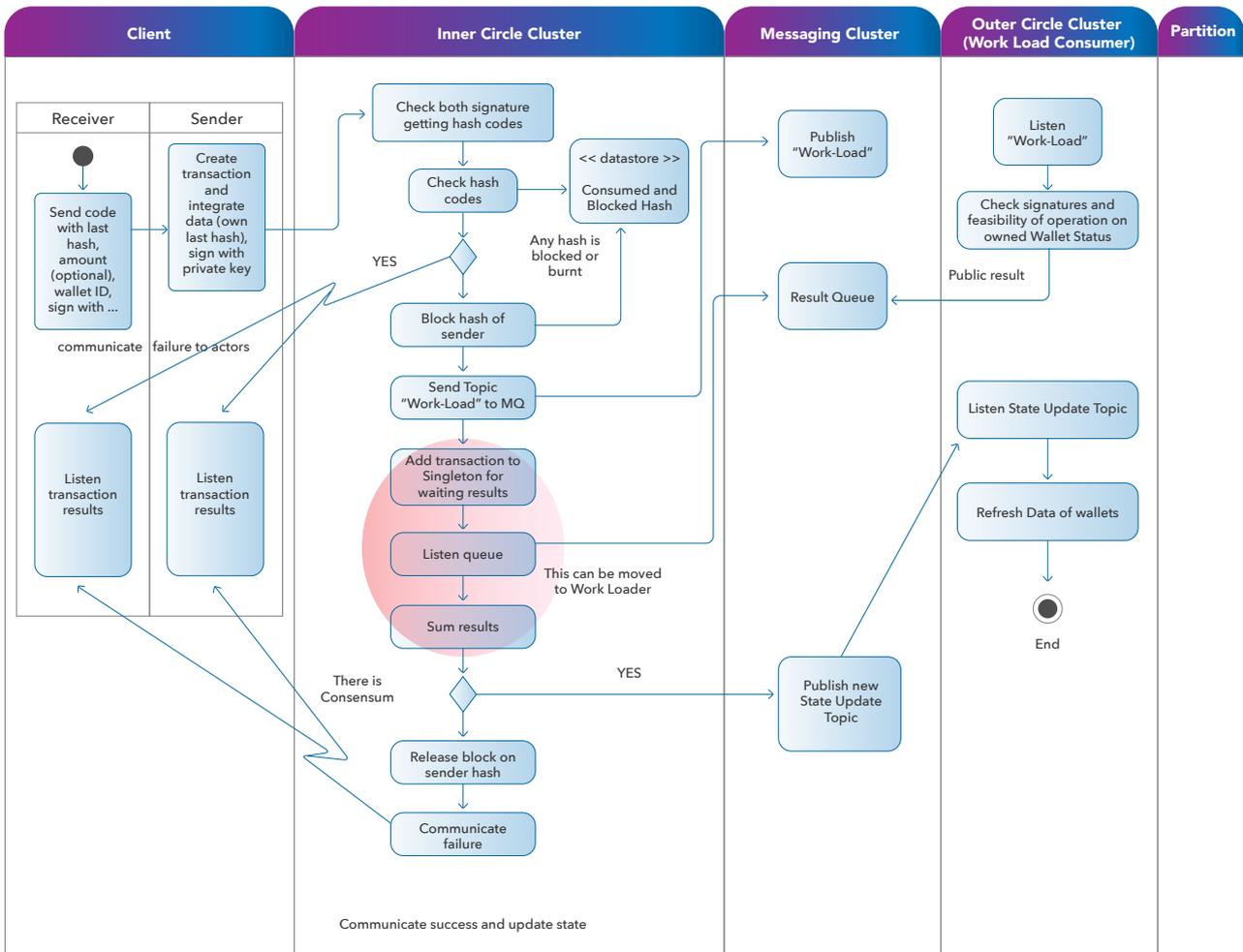
El Client REST comunica la transacción al Nodo Líder del clúster de coordinación: éste dividirá internamente el trabajo, gracias a un protocolo propietario, entre los nodos del clúster de coordinación, que harán un control preventivo de la integridad de los datos y firma, de la disposición de fondos para la transacción, de la presencia de hashes ya utilizados, de estados no actuales de los portafolios y portafolios o usuarios bloqueados.

Mientras tanto, bloquea temporalmente en la memoria volátil el empleo posterior del ID del remitente de la transacción y completa algunos datos, como la transacción anterior a la que se engancha, la marca de tiempo y hash anterior.

La transacción es enviada a un Topic Message Queue con protocolo por definir (en el Pilot en AMQP, para verificar MQTT u otros), y es distribuida paralelamente a los Nodos Trabajadores. Los Nodos Trabajadores verifican si están involucrados en su procesamiento (podrían no tener los datos necesarios, que tengan exceso de trabajo u otro por comprobar), y proceden a la creación del nuevo estado del portafolio, recuperando los hashes relacionados con transacciones anteriores y agregándolos al récord de la transacción. También es añadido el resultado de la Prueba de Integridad.

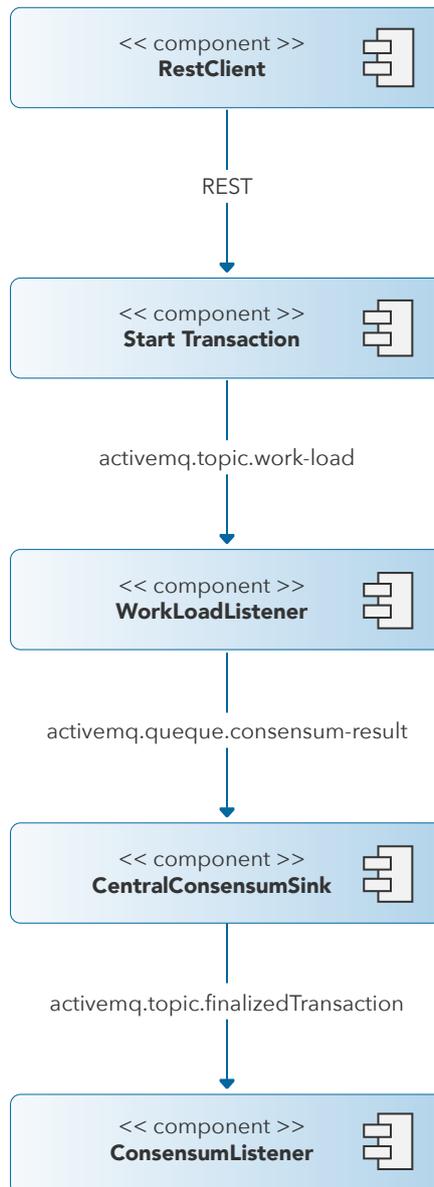
Finalmente, calculan, en el conjunto de datos, el hash de la transacción. Los Nodos Trabajadores registran en la memoria volátil esta transacción y envían un voto a los nodos coordinadores por un Message Queue que reúne todos los votos.

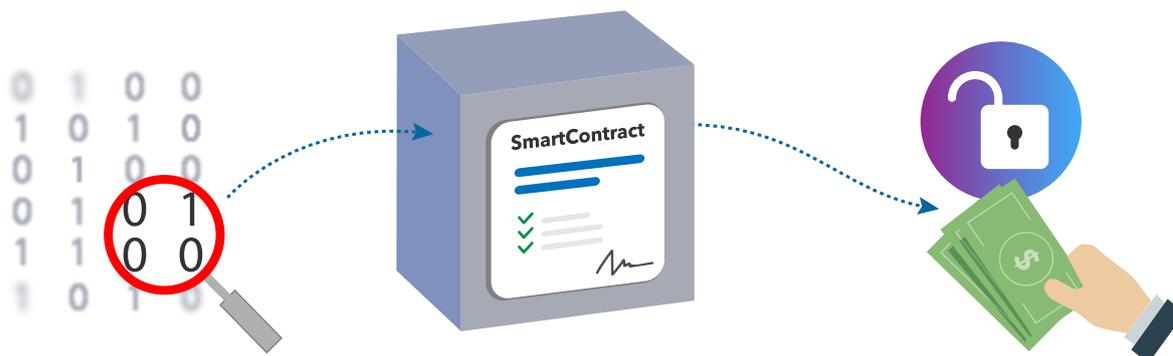
En caso de que los votos y hashes sean consistentes, los nodos de coordinación escriben de modo permanente sobre los mismos soportes las transacciones y nuevos estados del Portafolio, quemando los hashes de los estados anteriores y comunicando, con un sistema adicional de Topic Message Queue, que el voto es válido. En ese punto los Nodos Trabajadores persisten toda la operación. Fin del mejor caso de ruta completa.



Logic data flux

Detail of process flow





Contratos Inteligentes

Multiversum cree necesario proponer al público Contratos Inteligentes avanzados; al mismo tiempo ha decidido que por el momento, salvo una futura modificación de los ámbitos de su investigación, no se pondrá el objetivo de estudiar esta posibilidad, limitando su acción, con la modestia adecuada al entorno científico, a localizar la mejor solución de Código Abierto en el mercado y referirse a ella para su inclusión en su solución (compatiblemente con el modelo de licencia del proyecto al que hará referencia).

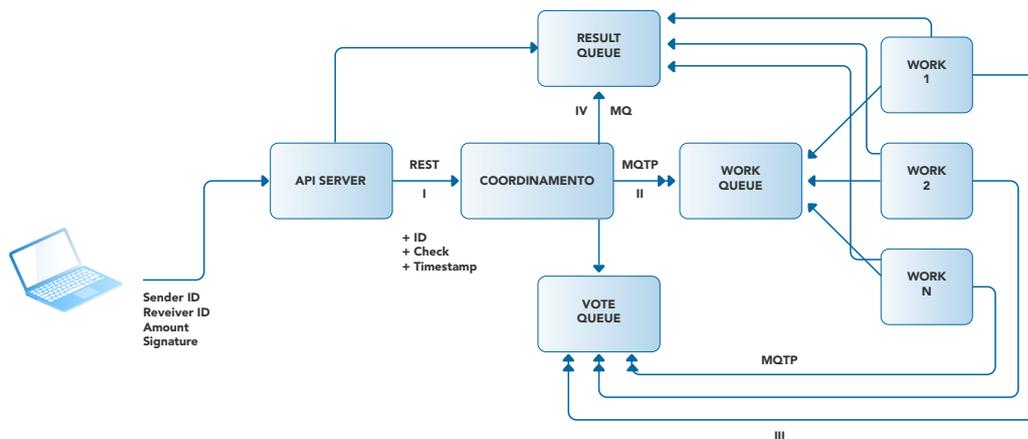
Infraestructura

Él infraestructura de Multiversum ha sido diseñada para garantizar la resiliencia y la alta disponibilidad. Este objetivo ha sido alcanzado desarrollando clusters de nodos capaces de auto-elegir a sus miembros para funciones específicas, con base en las características técnicas de cada nodo, entre las cuales:

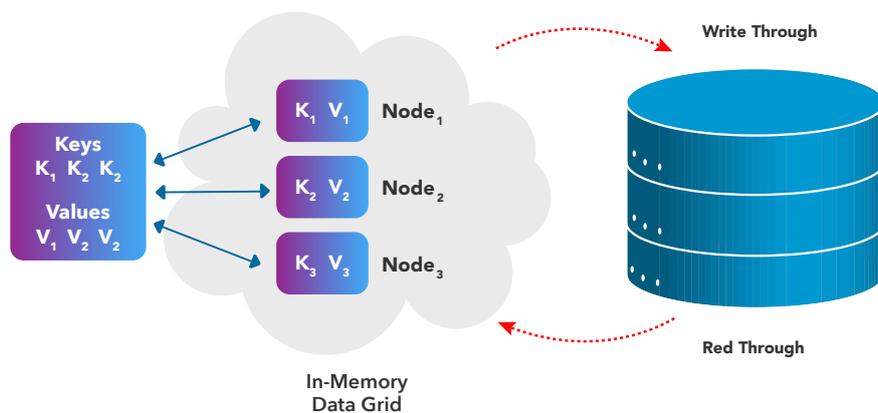
- Capacidad de cálculo
- Capacidad de memoria
- Velocidad de ping recíproco
- Integridad de los datos de las cadenas
- Fiabilidad de la máquina
- Dudas sobre la Prueba de Integridad

Los nodos podrán tener una o más funciones, entre las cuales:

- Nodos Clientes
- Nodos de coordinación
- Nodos de mensajería
- Nodos de trabajo
- Nodos persistentes
- Nodos de respaldo



Cualquier nodo capaz de demostrar que posee un certificado válido podrá registrarse en el clúster y obtener una función.
 En caso de falla de uno o más nodos el clúster podrá redistribuir autónomamente las tareas, optimizando los roles.

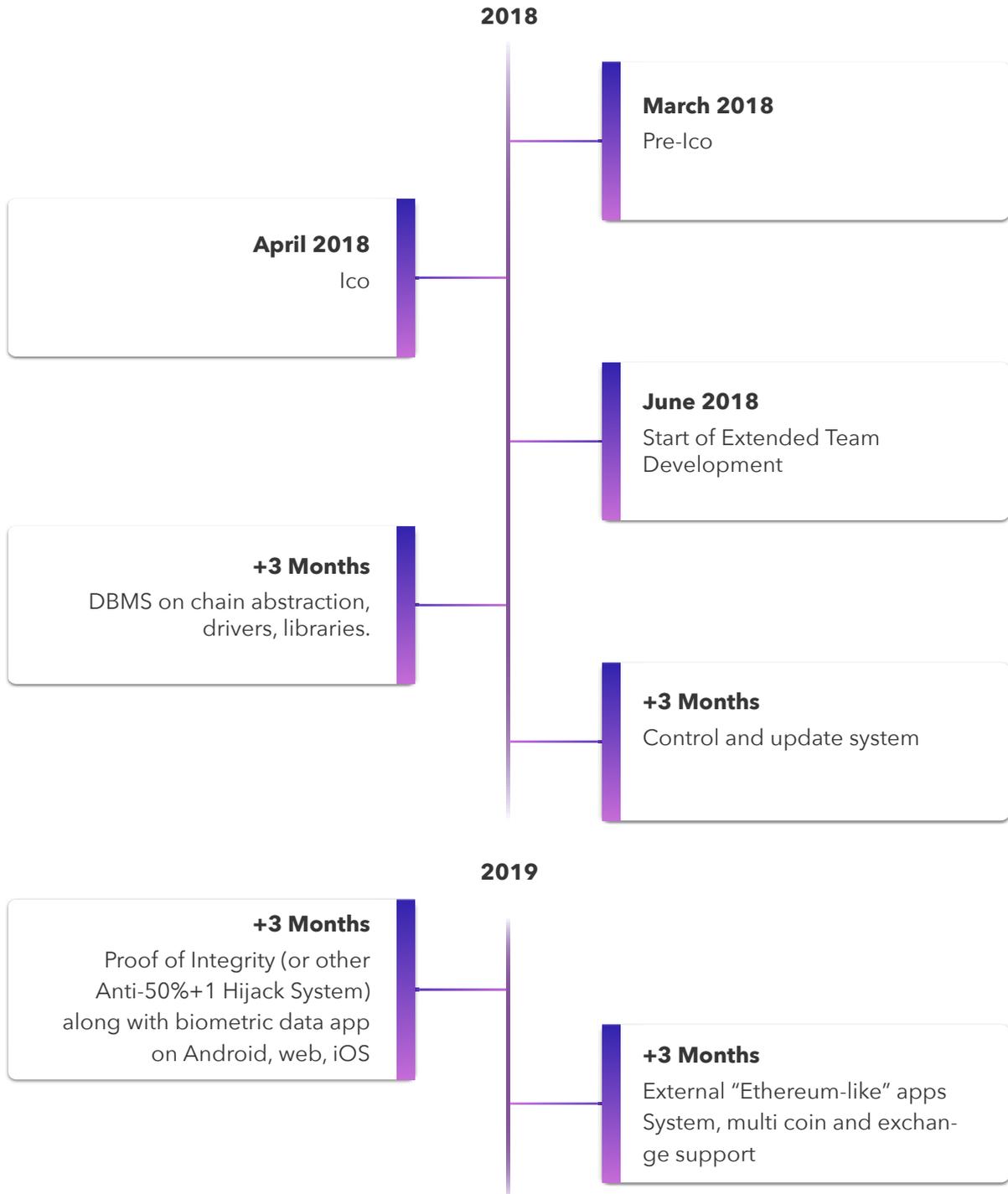


Habrán componentes de caché compartidos intra JVM como bases de datos de memoria, que permiten mecanismos de Read through: la búsqueda de los datos en la memoria volátil (si aquí no están presentes, en la física) y, sucesivamente, el *Write Through*: la acumulación de los datos en la memoria volátil y la inserción de masa en la física, para tener que esperar solamente una vez la finalización del *handshake* y overreadla sobrecarga de datos, obteniendo una optimización de las prestaciones (en el caso de transacciones individuales se ejecutarían repetidamente).

Notas sobre la seguridad

En el curso de la construcción se ofrecerán "recompensas de Hacker's" a quien encuentre vulnerabilidades y eventualmente proponga una solución adecuada.

Hoja de Ruta Técnica



La implementación completa llevará aproximadamente un año de trabajo para implementar el servidor de la Main Net por dos equipos de desarrolladores, un arquitecto de Software, dos desarrolladores de GUI, dos responsables de la seguridad, un Arquitecto de Negocios.

En los años siguientes el desarrollo continuará para permitir tener un producto enter-prise grade: a partir de el desarrollo continuo la moneda Versum ganará ventajas de credibilidad e imagen. La Main Net estará completa con todos los mecanismos de seguridad y de la lógica del producto enter-prise, pero no de los que hacen que la tecnología se integre fácilmente, ya que no son indispensables para su uso. El software será publicado constantemente para respaldar la credibilidad del proyecto y a la Prueba Net ofrecerá las nuevas características disponibles tan pronto como lo estén.

Estrategia de Mercadeo

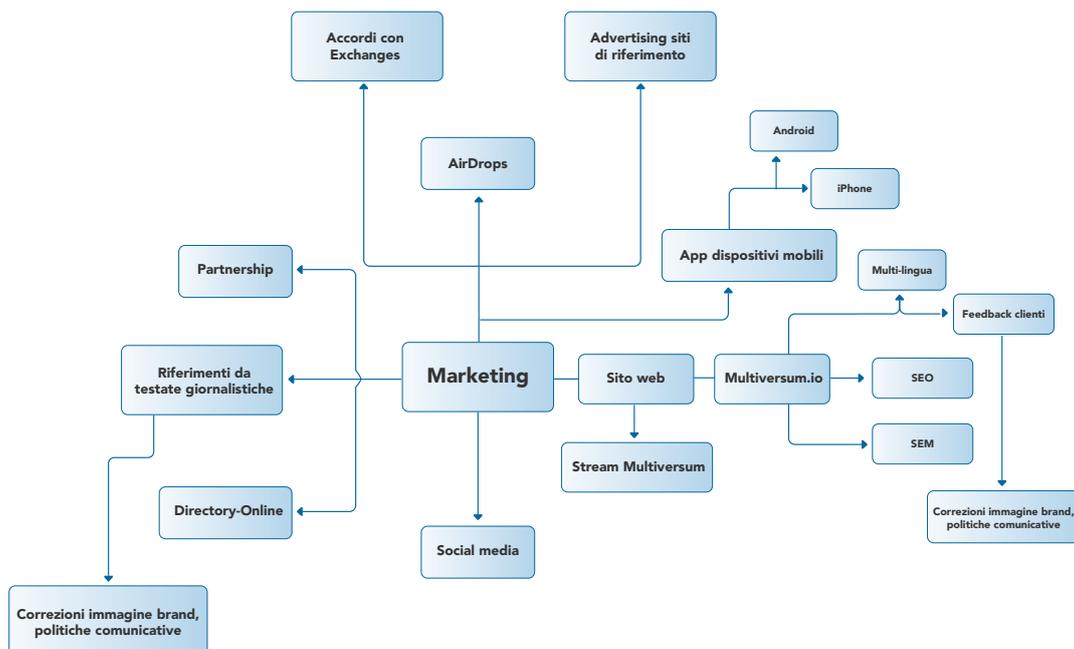
Hemos centrado la planificación de toda la organización de mercadeo partiendo de un contexto general para poder enfocarnos luego en aspectos específicos.

Comprenderemos todas aquellas actividades que permitirán la consecución de los objetivos, adoptando un enfoque global para toda la organización (desde la definición de la misión empresarial a la identificación de la estrategia más apropiada).

La estrategia empresarial será el reflejo de un entorno en continua evolución y la misión de la empresa será crear valor para las partes interesadas, asegurando el equilibrio entre lógicas de gestión a corto y largo plazo.

Las 4 componentes del plan son:

- Misión empresarial
- Estrategias empresariales
- Objetivos empresariales
- Portafolio de actividades empresariales



Mercadeo Social media Asociaciones Directorio-Online AirDrops iPhone Multi-lengua SEO SEM Retroalimentación clientes Correcciones de imagen de marca, políticas de comunicación dispositivos móviles con Aplicaciones Android Acuerdos con Intercambios Publicidad de sitios de referencia Correcciones de imagen de marca, políticas comunicativas Referencias de medios periodísticos Sitio web Multiversum.io Stream Multiversum

Uno de los instrumentos principales será el Mercadeo Social Media que es el conjunto de las actividades realizadas en las redes sociales para aumentar el conocimiento de la marca, identificar a potenciales consumidores, generar contactos y construir relaciones significativas con los clientes.

Implementaremos diversas acciones que son parte de un único plan estratégico, partiendo de la gestión y el monitoreo de los canales utilizando herramientas dedicadas y fortaleciendo a la comunidad a través del cuidado diario de los contenidos y la interacción, hasta el análisis de los resultados obtenidos y la verificación de la táctica aplicada en campo.

Cada una de ellas se refleja en las habilidades de nuestros Estrategas de Redes Sociales: la planificación estratégica, la definición y producción de la línea editorial, la interacción y el soporte con el mercado y el análisis de los resultados. plan, starting with the management and monitoring of channels using dedicated tools and community development, focusing on contents and interaction and tactics efficiency assessment based on obtained results.

Las capas de elementos que envuelven los universos son cada una diez veces más gruesas que la anterior, todos los universos, agrupados juntos, aparecen como átomos en una inmensa combinación.

Bhagavata Purana 3.11.41



MULTIVERSUM

HERE TO STAY