

MULTIVERSUM

HERE TO STAY

WHITE PAPER v 1.0.6

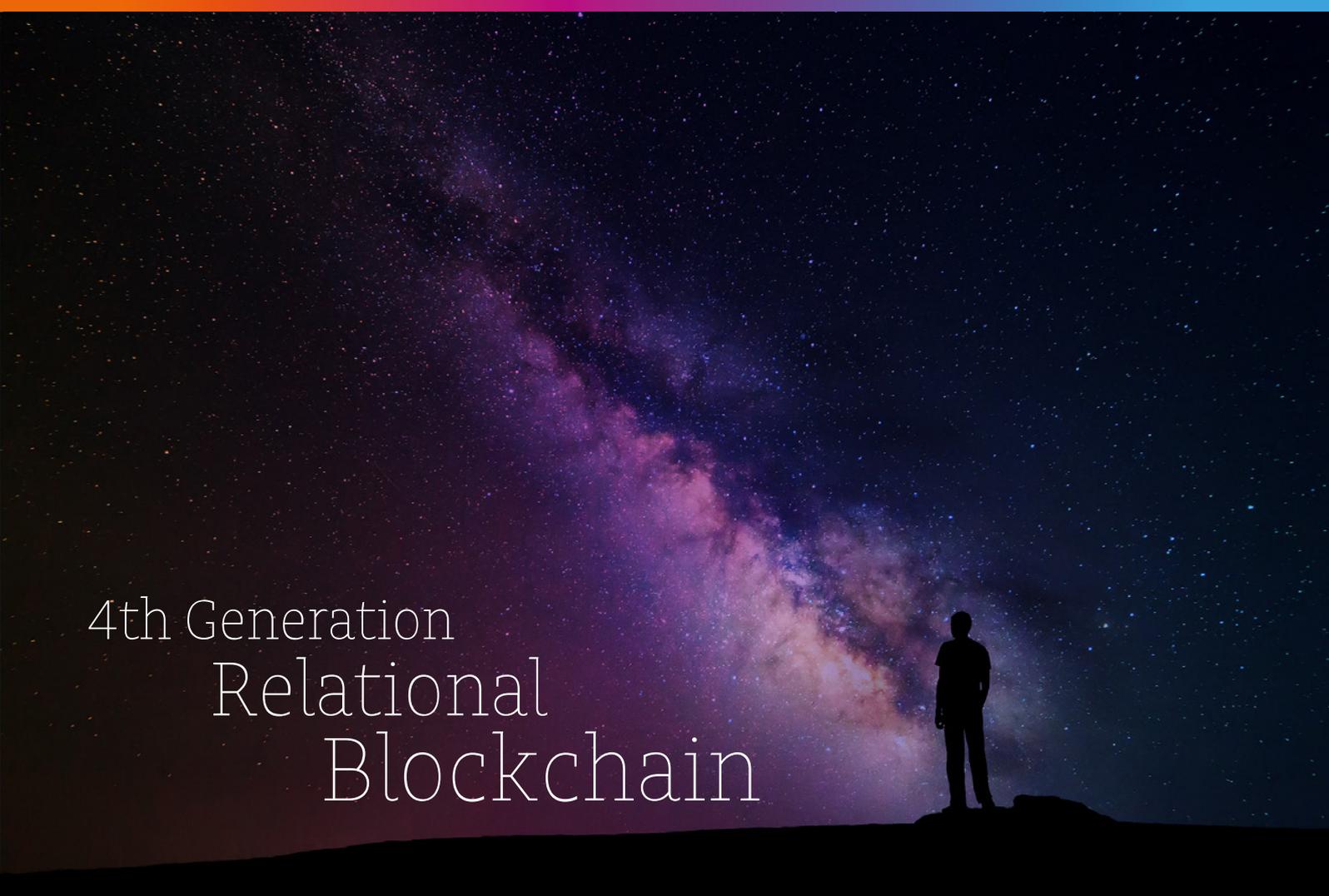
Business | Technical

French

13.02.2018

Authors: Multiversum Team

www.multiversum.io



4th Generation
Relational
Blockchain



**Il n'y a d'innombrables univers
différents du notre, bien qu'ils
soient infiniment étendus, ils
bougent comme des atomes en
vous.**

Le bhâgavata Purana 6.16.37

Contents

Multiversum Identity and mission	4
Multiversum	5
The 4th Generation Relational Blockchain	5
Public presentation	8
Current Blockchain State of the Art	8
Multiversum and blockchain global adoption	9
Speed and Technology	10
Horizontal Scalability	10
Environment	11
Data Management	11
The Multiversum Mission	13
1. Achievement of a Crypto Relational DB with self-validating Complex Data Structures	14
2. Divisible / re-joinable chains based on current system workload (Parallel Work)	14
3. Data sharding (Parallel Work)	15
4. Microservice structure and Advanced API offer	16
5. Rollback (User Security)	16
6. Freezable wallets (User Security)	17
7. Integration of biometric data as a seed for Electronic Signature	17
8. ERC23 interface (Interoperability with other blockchains)	18
9. Native off-chain adapter for proprietary ERC20/ERC23 (Interoperability with other blockchains)	18
10. Native off-chain adapter for external ERC20/ERC23 (Interoperability with other blockchains)	18
11. Proof of Integrity (Protocol Innovation)	19
12. Double Access Lock (Structural Security)	19
13. Reverse Access Denial (Structural Security)	20
14. Reciprocal chain confirmation (Interoperability with other blockchains)	21
15. Integration with Java, Spring and JavaScript	21
16. ACID model	22
17. Transactional Model	22
18. SQL-like Language	22
19. Full Route Data Flux	22
Logic data flux	24
Smart Contracts	25
Infrastructure	25
Notes on security	26
Technical Road Map	27
References	28
Pre-ICO and ICO	30
Pre-ICO	31
ICO	31
Token Distribution	32
Destination of contributions	33
Marketing Strategy	34
Disclaimer	36

Multiversum identité et Mission

La première génération de Blockchain est composée par les premières pièces comme Bitcoin, fondée sur la Proof of Work et de ses divers clones et fork.

Les Blockchains de la deuxième génération sont plus hétérogènes, basés sur l'utilisation de Token comme Ethereum et son écosystème de solutions.

Ces deux catégories sont caractérisées par la faible efficacité et faible nombre de transactions.

A la troisième génération appartiennent ces BC qui ont tenté de fournir des réponses à la lenteur et l'impossibilité d'être évolutif à l'aide de divers mécanismes :

Proof of Stake, off chain route, graphchain, centralisation complète ou partielle.

La quatrième génération, cependant, a l'intention de continuer à répondre à la lenteur du système ; en même temps, elle se fixe des objectifs d'utilisabilité dans le domaine de l'entreprise, chose à laquelle peu est préparé une chaîne de données désorganisée qui nécessite des systèmes de stockage de données complexes structurées en tables connexes (comme les Databases relationnelles), mais à en même temps dans lequel les données se valident et se renforcent avec la technique de la Blockchain. Autrement dit, la tentative de conduire cette technologie à une réelle utilité productive primaire. Multiversum offre une gestion organisée de données complexes au lieu de la simple succession de données, de la divisibilité de la Chain et de la réunion afin de permettre le parallélisme et vérifier la faisabilité du Proof of Integrity (preuve cryptographique du code du Server) au lieu du Proof of Work.

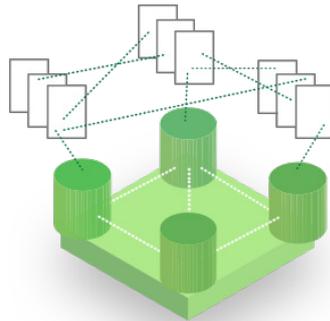
Ajout également d'appareils pour interagir avec les autres Chains (hébergement sur notre Chain d'autres Coins et Tokens et vice versa) et d'un service des notaires agissant comme une validation externe.

Pendant ce temps, en plus de toutes nos innovations nous utiliserons certainement des solutions déjà optimales que nos collègues ont mises en place

Multiversum

Block chaîne 4e génération relationnel

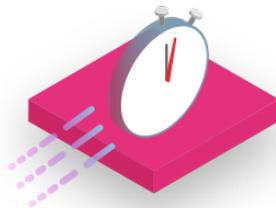
Pourquoi Multiversum est la Blockchain 4.0?



Relational Blockchain

Une Blockchain de nouvelle génération, qui passera de gérer un seul type de données linéairement à plusieurs types de données, liées entre elles par l'indicatif d'appel, dans une structure multidimensionnelle.

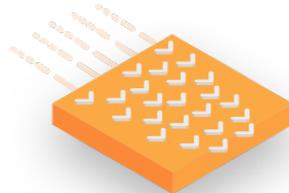
< 0,2 sec



Transaction Speed

En moins de 0,2 secondes les fonds sont transférés d'un Wallet à l'autre en effectuant toutes les étapes qui certifient la sécurité. Entre les Blockchains les plus rapides dans le monde.

64000 tps → ∞



Nombre de transactions

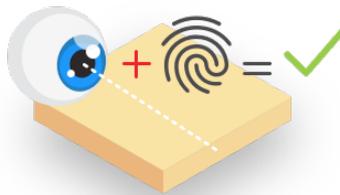
Jusqu'à 64000 TPS sur Server a 64 Core (1000 TPS par Core), support pour les systèmes avec plus de 64 Core - évolutivité sans limites.

POI



Sécurité extrême des transactions

Le concept de POS (Proof of Stake) n'existera plus :
Il sera remplacé par POI (Proof of Integrity).



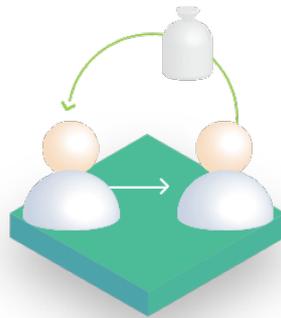
Wallet de nouvelle génération/Input biométrique

Sécurité extrême en accédant au Wallet et à l'envoi des fonds à travers
l'entrée biométrique.



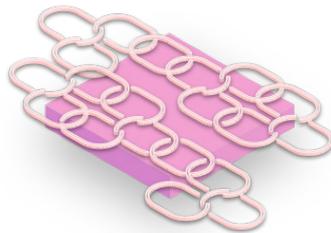
Respectueux de l'environnement

Une transaction aura des coûts insignifiants et presque
zéro impact sur l'environnement.



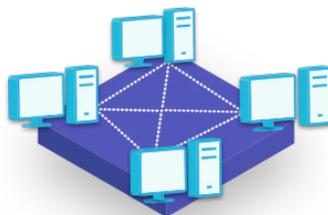
Rollback

Le système de Rollback sera facultatif et disponibles en solutions ad hoc qui peuvent bénéficier de cette fonctionnalité.



Chaînes divisibles

Réglage de la charge de travail avec une allocation de ressources étant disponibles grâce à la possibilité de fractionner la chaîne principale en plusieurs chaînes secondaires.



Répartition des Recovery Nodes

La société Multiversum a placé des nœuds périphériques de Global Disaster Recovery sur différents continents.

Présentation au public

Le concept de Multiversum et son utilisation à l'échelle mondiale

Multiversum est une technologie qui, en modifiant les aspects liés à la persistance des données dans la Blockchain par des données auto-vérifiées et distribuées, organisées en entités cohérentes liées entre elles par des liens symboliques, il révolutionne les limites traditionnelles, conduisant, en fait, à une nouvelle génération : la Blockchain 4.0.

Sur cette technologie est basée sur un system décentralisé et distribué de transactions cohérent et auto-vérifiée : BC Multiversum. Les Blockchain actuelles reposent sur une séquence d'opérations qui représentent un seul type de données : ou se rapportant à la transaction elle-même ou à de multiples chaînes coexistantes et pas fermement cohérentes les unes avec les autres, dans lequel les données sont organisées en blobs conceptuels et liées les unes aux autres avec d'énormes difficultés et des coûts de calcul. Multiversum permet de créer un Database Crypto relationnelle (une solution avancée et organisée de stockage de données) qui vous permet d'avoir non seulement un type de données, mais une série de données regroupées en tableaux dans une structure de données complexes, liées entre elles grâce à un identificateur.

Chacune d'elles quand un état changera, aura sa propre sous-chaîne qui viendra d'un nœud déjà certifié et sera réunie, pour obtenir la certification, avec le reste de la chaîne. Multiversum est donc une technologie Blockchain avancée qui offre des fonctionnalités uniques pour résoudre ces problèmes dans un panorama de validation et de distribution crypto, et peut être utilisée dans n'importe quel environnement: administratif, industriel,

financier et gouvernemental. L'un des principaux objectifs de Multiversum est d'offrir au marché à tout moment le produit le plus avancé disponible: cela sera possible en utilisant une méthode appelée AGILE.

Cette approche nous permettra de comprendre les demandes du marché, pendant et après la phase de développement, et de les mettre en œuvre progressivement, en arrivant à publier le Main Net le plus avancé et le plus complet disponible.

Cette technique de développement nous permet d'offrir le produit le plus moderne et le plus actuel sur le marché.

Vitesse et la technologie

Un point fort de cette technologie est certainement la rapidité, due à la possibilité de traiter différentes transactions en parallèle.

Cette fonctionnalité permet une évolutivité horizontale parfaite, c'est-à-dire la possibilité d'augmenter infiniment la capacité de traitement des transactions, en ajoutant de nouveaux processeurs au lieu de remplacer ceux existants, rendant chaque nœud supplémentaire utile pour améliorer les performances de tout le système.

L'évolution Horizontale

Multiversum peut profiter de deux fonctionnalités très importantes qui le rendent si efficace: La chaîne est capable d'optimiser sa structure en se divisant en plusieurs sous-chaînes en fonction des ressources requises et du flux de données, partageant ainsi le travail du cluster de processeurs de la meilleure façon entre les nœuds préparés pour le traitement.

Cette division peut être effectuée indéfiniment jusqu'à la normalisation des charges de travail, lorsque, de nouveau de manière autonome, la chaîne reviendra à être une. Tout cela grâce à un dispositif qui permet à chaque anneau de valider deux chaînes différentes des deux anneaux précédents différents.

La possibilité de faire Sharding des données: une technique qui permet la distribution de données dans plusieurs nœuds. Imaginant avoir une série de données ABC et trois nœuds du Cluster, nous aurons une subdivision des données ainsi disposées:

AB

BC

CA

Cette division permet une plus grande vitesse de traitement des transactions qui rechercheront des données à utiliser uniquement dans les nœuds qui les contiendront, en optimisant chaque

étape. Une autre caractéristique très importante est appelée High Availability: la possibilité de s'appuyer sur un type de cluster qui garantit la continuité des services même en cas d'interruption de certains nœuds du réseau. En utilisant l'exemple précédent (nœuds A, B et C), si C était interrompu, les nœuds A et B resteraient pleinement opérationnels, permettant une continuité de service sans perte de données jusqu'à ce qu'au moins 50% + 1 des nœuds soient opérationnels. Dans cette situation, le Cluster, en communiquant avec tous les nœuds, organisera de manière autonome la distribution des données jusqu'à leur récupération opérationnelle complète.

Environnement

Multiversum est également écologique, car il vise à éliminer le Mining, un gaspillage de puissance de calcul et une immense énergie, qui soutient le Proof of Work, en faveur d'un nouveau concept, le Proof of Integrity: un protocole qui vérifie la véracité et l'authenticité du logiciel qui résout toute persistance de la transaction.

Gestion des données : Database relationnelle

Multiversum, avec son Crypto Database relationnelle, peut facilement structurer des données sans limites dans le type de liens.

Chaque Wallet aura une série d'états (Statee) et sera connecté à une personne (User); tout nouvel anneau de changement dans l'état du Wallet incorporera deux choses: - l'état précédent, de manière à avoir la validation de l'acte précédent; - un lien vers la dernière transaction (ou vers le dernier anneau de la Main Chain), pour lequel nous saurons d'où provient le nouvel anneau du changement d'état.

Une fois ce changement survenu, la transaction de changement sera ajoutée et, à ceci, l'anneau de l'état modifié sera rejoint, ce qui indiquera l'origine de la connexion du nouveau changement d'état.

Par conséquent, la nouvelle transaction héritera de deux Hash: un de l'anneau d'état, un de l'anneau de transaction précédent.

De cette manière, toutes les opérations valident les précédentes liées à la transaction elle-même.

Ce système aussi complexe que perfectionné et nous permettra d'implémenter un logiciel sur notre technologie assurant une diffusion institutionnelle, gouvernementale, financière et industrielle, amenant l'ensemble du monde Blockchain à un niveau supérieur.

Analyse du State of Art de la Blockchain

À l'heure actuelle, les principaux acteurs du «phénomène blockchain» se caractérisent par une robustesse considérable en termes de sécurité.

Dans ce contexte, cette sécurité implique une énorme puissance de calcul, la pollution, des commissions de transactions inacceptables une lenteur incapable de représenter les progrès technologiques actuels, affectant ainsi la capacité de donner une réponse crédible en cas d'utilisation techniques commerciaux et financiers modernes.

Cette lenteur est due à l'impossibilité d'atteindre l'évolutivité horizontale, qui est l'augmentation de la capacité de calcul obtenue par la simple addition de processeurs au lieu de les remplacer par des versions plus rapides.

Une deuxième raison de la faible efficacité est inhérente au mécanisme actuel de sécurité blockchain basée sur la Proof of Work et, moins fréquemment, sur la proof of Stake, qui crée un risque de perdre le contrôle de la majorité du Cluster en raison du Sybil Attacks en exigeant des noeuds une capacité de calcul artificiellement élevée, rendant impossible la création indiscriminée par l'augmentation de la difficulté. En outre, les Blockchain actuelles sont des séquences simples de changements d'état d'entités de données individuelles: la reconstruction des états actuels, nécessitant d'une scansion de toute la chaîne, implique une lenteur supplémentaire du système et un gaspillage de ressources. Cette approche rend inadéquate la technologie blockchain dans un contexte industriel et scientifique, des environnements où les structures de données sont extrêmement complexes.

La sécurité garantie par les blockchain actuelles ne concernent que les données, elle

ne couvre pas l'utilisateur: il est impossible, par exemple, récupérer des Coin ou Token détournées, même si elles avaient été identifiées dans la Chain, ou bloquer des comptes impliqués dans des activités illégales. Un dernier problème est l'absence totale d'homogénéité et le manque de communication dans le monde des différents crypto-monnaie: chaque Blockchain existant dans son propre univers à part, il est incapable de communiquer avec les autres.

Méthodologie AGILE

Multiversum propose d'utiliser la méthodologie AGILE lors du développement du produit. Cette technique présuppose une réduction drastique de la conception initiale, en faveur de la valorisation des expériences acquises en cours de construction, mettant en évidence des opportunités et des dangers autrement difficiles à identifier ex ante, en récompensant Best Practices (pratiques exemplaires) et en pénalisant Ways of Working (modalité opérative) inadéquat.

La méthodologie AGILE est l'Industrial Standard de la production de logiciels et suggère aux développeurs, Product Owner et aux investisseurs de considérer la portée du projet de manière flexible, afin de l'adapter aux besoins du marché. Par ailleurs, dans un secteur en évolution rapide et constante tel que celui des logiciels, proposer au marché, après une période typique de six mois d'études et une année de mise en œuvre, un produit né pour répondre aux besoins de 18 mois auparavant, offrirait une solution obsolète, ce qui résout des problèmes non courants, probablement déjà surmontés par la concurrence et incapable de donner des réponses aux nouveaux défis. AGILE, au contraire, permet d'offrir au marché le produit le plus innovant possible au moment de la livraison du projet.

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)

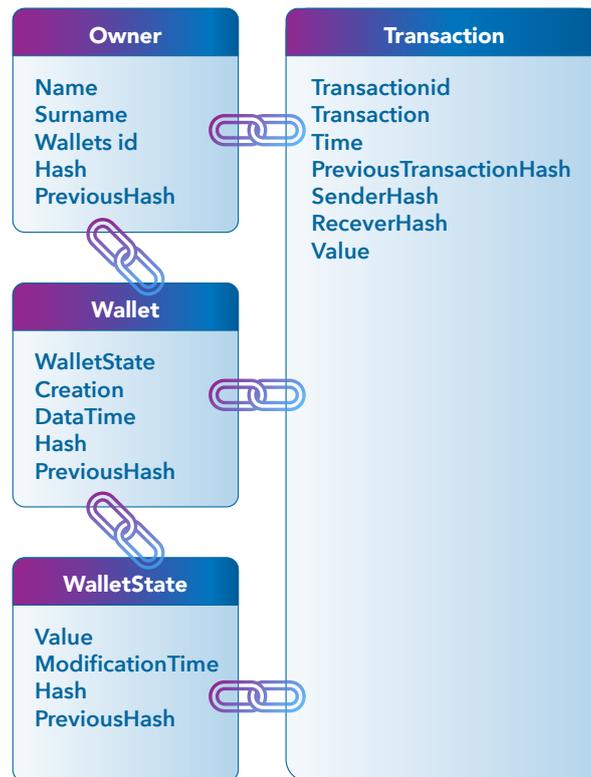
ERC23

(Interoperability with other BC)

Multiversum mission

Multiversum propose d'étudier des solutions pour permettre une évolution générationnelle dans le monde de la Blockchain, en particulier, en tant que Unique Selling Point, il se pose les objectifs suivants :

1. Implémentation d'une Database crypto-relationnelle avec des structures de données complexes auto-validantes
2. Chaînes divisibles et ré-assemblables par rapport à la quantité de travail requise (Parallel Work)
3. Sharding de données (Parallel Work)
4. Offre d'API avancée
5. Rollback (User security)
6. Wallet Multicurrency freezable (User Security)
7. Intégration des données biométriques comme Seed pour la signature électronique
8. Interface ERC23 (Interopérabilité avec d'autres Blockchains)
9. Adaptateurs natifs off-chain pour votre ERC20 / ERC23 (Interopérabilité avec d'autres Blockchains)
10. Adaptateurs natifs off-chain pour les clients ERC20 / ERC23 (Interopérabilité avec d'autres Blockchains)
11. Proof of Integrity (protocole d'innovation)
12. Double Access Lock (Structural Security)
13. Reverse Access Denial (Structural Security)
14. Reciprocal Chain Confirmation (Interopérabilité avec d'autres Blockchains)
15. Intégration pour Java, Spring et Javascript
16. Modèle ACID
17. Modèle transactionnel
18. Langage SQL-Like



1. Mise en œuvre d'un Crypto DB relationnelle avec des Structures de données complexes auto-validantes

Multiversum a une forte vocation pour une utilisation dans des contextes industriels, institutionnels, publics et entreprise : des environnements qui nécessitent des structures de données complexes qui sont impossibles à représenter de manière efficace et normalisée avec une simple chaîne.

Cette vocation se manifeste en voulant être la première base de données relationnelle cryptographique à s'offrir au marché, distribuée et éventuellement décentralisée. Cet enregistrement a été atteint à partir de la conceptualisation des entités chainables. Ces Entités permettent de mettre en œuvre une interface capable de définir les méthodes nécessaires à une donnée pour être insérée en anneau dans une blockchain.

Dans le modèle conceptuel, il y aura une chaîne primaire à laquelle les chaînes secondaires seront connectées, représentant des entités de types différents, qui, à leur tour, représenteront les enregistrements d'une table.

Ces entités se connecteront à leur dernier état de persistance et après les changements nécessaires se rencontreront dans le dernier maillon de la chaîne primaire qui rejoindra les deux chaînes.

. L'interface « chainable » signifie: l'enregistrement de plusieurs anneaux à partir duquel dérivent de nouveaux, l'enregistrement des multiples anneaux qui dérivent de l'individu,

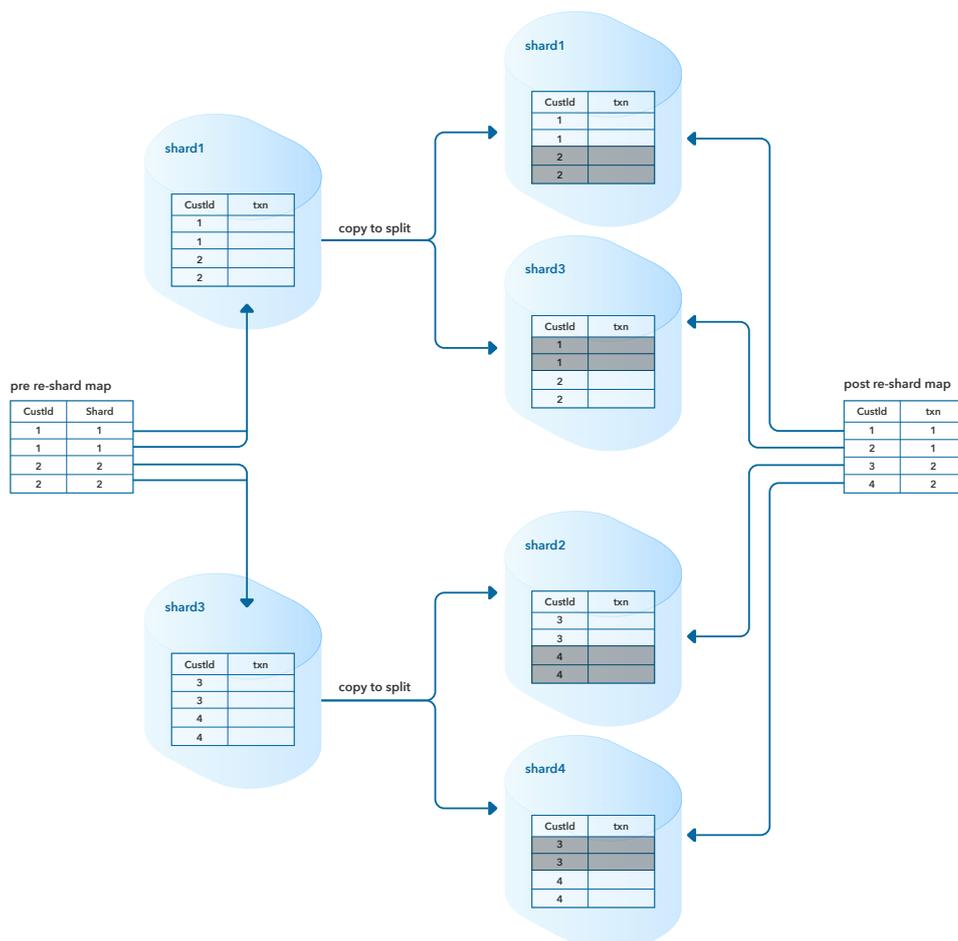
et celle de la validation de la présence de telles données, qui agit par l'importation de hachage des cycles mentionnés dans le calcul de l'actuel hash.

Dans la mise en œuvre de la technologie Multiversum pour les pièces Versum, les entités chaînables qui coexisteront sur la chaîne appartiendront à quatre tables: User, Wallet, Wallet State et Transaction, qui se corrèleront entre elles et se valideront mutuellement.

2. Chaînes divisibles et ré-assemblables en fonction de la quantité de travail requise (travailler en parallèle)

La capacité de dériver plusieurs anneaux d'un et de les rassembler ensuite provient de l'utilisation d'analyseurs de charge de travail qui, en présence d'un grand nombre de demandes d'exécution, signalent au Cluster la nécessité de dédoubler (pour des temps infinis, si nécessaire) la chaîne primaire des transactions en deux chaînes secondaires et, sur la réduction de la même, permettront de rejoindre les multiples sous-chaînes précédemment générées. Ce mécanisme permet un travail parallèle, en continuant à offrir une protection contre l'altération des registres de transactions.

3. Données Sharding (travail parallèle)



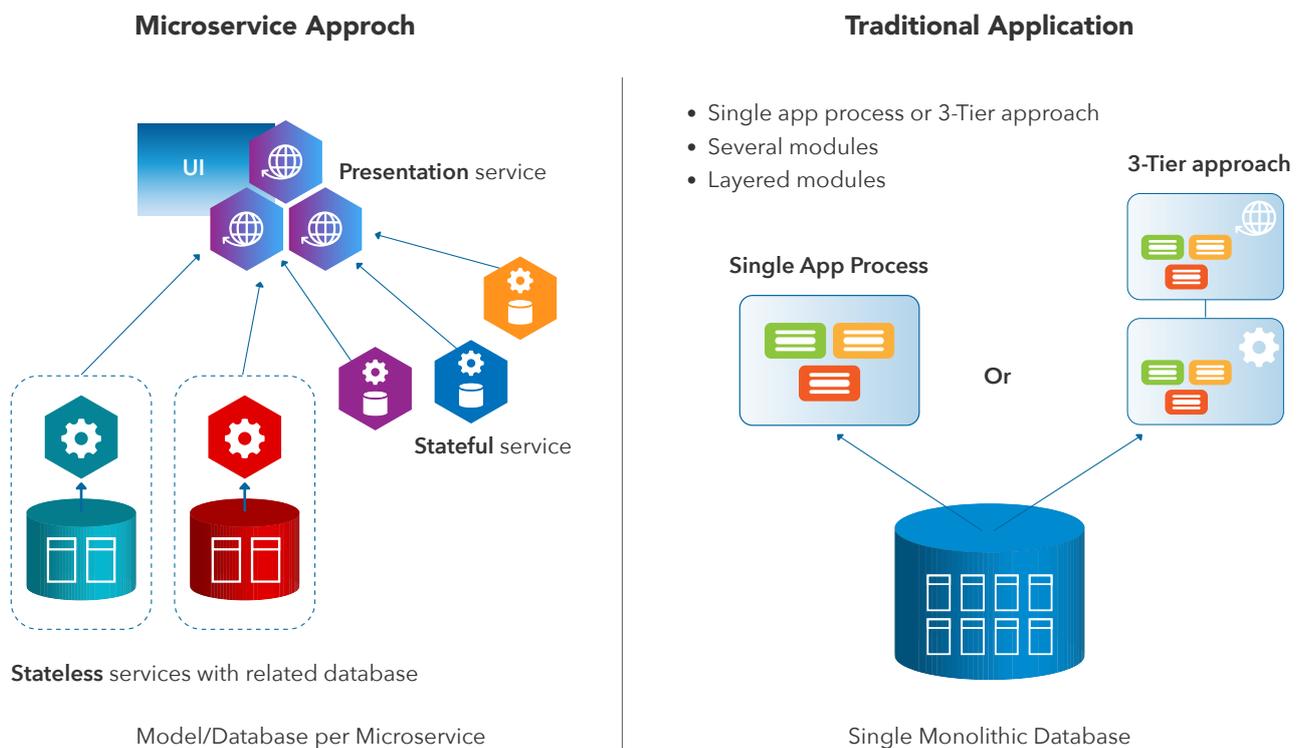
Chaque nœud peut avoir en mémoire toutes les données de la blockchain ou juste une partie de celle-ci. en cas de necessite de paralléliser les données, les nœuds de coordination établiront les modalités de subdivision afin d’optimiser la distribution à travers les paramètres de parallélisation du calcul et de High Availability, assurant (jusqu’à 50% +1 des nœuds resteront en ligne) la disponibilité des données même en cas de disparition instantanée d’une partie du Cluster de persistance.

Ces nœuds, dans la phase qui suit le crash partiel du Cluster, sera en mesure de redistribuer et de réorganiser leurs données de manière autonome, de sorte qu’il puisse à nouveau faire face à un autre crash partiel du Cluster dès que possible.

Les dispositifs décrits dans ce point et dans le précédent accordent la capacité de travail parallèle, donc: évolution horizontale, sécurité, high availability, résilience du système, Absence de single point of failure 10 et récupération auto-sinistre.

4. Structure microservice et offre d’API avancées

Multiversum, ayant été développé sur une plateforme basée en partie sur Microservices 11 et en partie sur le modèle Serveless^{1 2} et aussi grâce à des API modernes, étendues et sécurisées, avec des fonctionnalités d’égales puissances, aura la capacité de s’adapter aux deux structures.



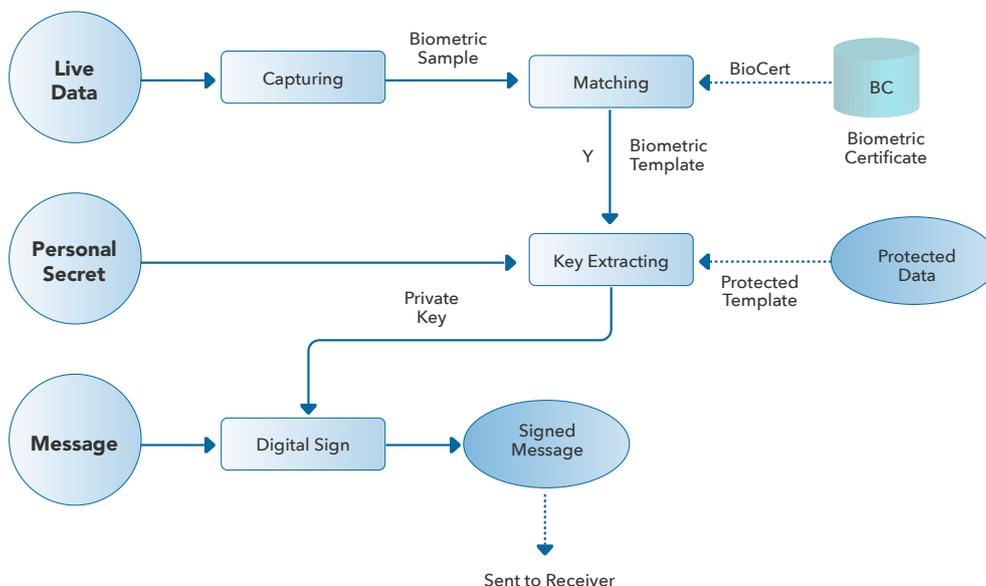
5. Rollback (sécurité de l'utilisateur)

La technologie Multiversum permet, dans le cadre d'une transaction, d'effectuer le rollback des opérations non désirées, c'est-à-dire restaurer un état antérieur sans affecter la crédibilité de la validation de la Chain, mais implémenter de nouvelles transactions programmables pour restaurer le statut souhaité.

Une fois la faisabilité du point de vue de Business Logic est évaluée, la possibilité d'implémenter cette fonctionnalité dans les coins Versum et de l'étendre avec effet rétroactif sera considérée. Dans la Chain publique, cette fonctionnalité ne sera pas mise en œuvre, mais les cas d'utilisation exclusifs faisant référence à la technologie Multiversum seront libres de l'implémenter.

6. Freezable wallets (User Security)

Une fois que la faisabilité a été évaluée du point de vue du Business logic, la possibilité de mettre en œuvre le gel temporaire des coin Versum d'un Wallet suite à des activités illégales sera étudiée.

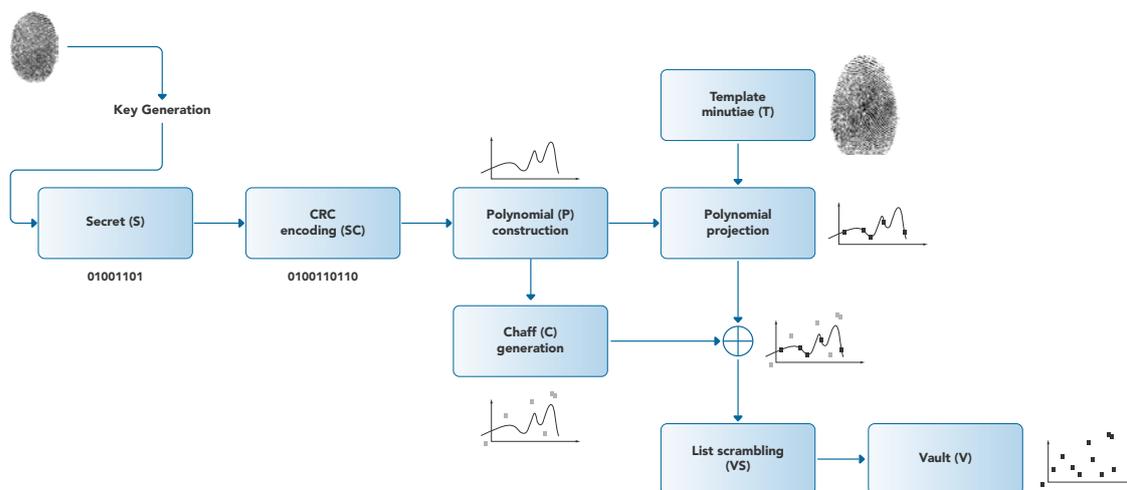


Biometric Digital Key Generation Framework

7. intégration des données biométriques comme semence pour la Signature électronique

Rappelant les études des professeurs Je-Gyeong Jo, Jong-Won Seo et Hyung-Woo Lee de l'Université Hanshin (République de Corée) et résumées dans la publication « Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint [13], nous étudierons la faisabilité l'utilisation de données biométriques telles que les empreintes digitales, l'image de l'iris et la signature graphométrique comme source de la clé cryptographique asymétrique pour garantir l'identité du signataire de la transaction.

Pour permettre l'utilisation de données biométriques cryptées dans la phase de contestation juridique, la sécurité de l'insertion sera évaluée. Dans tous les cas, ces données seront utilisées dans des applications pour Android et iOS.



Fuzzy Vault Scheme for Biometric Digital Key Protection

8. ERC23 Interface (interopérabilité avec d'autres chaînes de bloc)

Pour garantir l'interopérabilité avec d'autres Chains, les Coins Versum seront développées en implémentant l'interface ERC23, une version avancée et rétrocompatible de ERC201 4

```
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. Adaptateurs natifs off-chain pour votre ERC20 / ERC23 (Interopérabilité avec d'autres Blockchains)

Pour permettre l'entrée et la sortie de leurs propres Coins et Tokens sur d'autres Chain non propriétaires, Multiversum développera un adaptateur natif, en l'associant à un buffer qui régulera l'entrée et la sortie de la chain propriétaire.

10. Adaptateurs natifs off-chain pour les invités ERC20 / ERC23 (Interopérabilité avec d'autres Blockchains)

Pour permettre l'entrée et la sortie de Coins et de Tokens des non propriétaires sur sa Chain, Multiversum développera un adaptateur natif, en le combinant avec de multiples buffer qui réguleront son entrée.



Integrity

11. Proof of Integrity (Protocol Innovation)

Comme alternative à la Proof of work et à la Proof of Stake sous ses diverses formes, Multiversum introduit la Proof of integrity, qui est un dispositif de vérification cryptographique de la sincérité du code du noeud compilé et de l'uniformité de réponse de la majorité des noeuds par rapport à un challenge seed aléatoire, qui, avec le hash calculé par un composant externe (non décompilé, protégé et communiquant avec le software du noeud dans un canal crypté) du software lui-même, et aux données de transaction, doit être le même dans chaque transaction pour tous les noeuds. Ce processus nécessite beaucoup

moins de puissance de calcul et évite le gaspillage typique des autres systèmes (PoW, PoS, DPoS); elle fournit également une sécurité plus grande et plus réelle, et non un type statistique ou suppositoire basé sur le modèle du Consensus byzantin, particulièrement vulnérable dans les Cluster de tailles réduites.

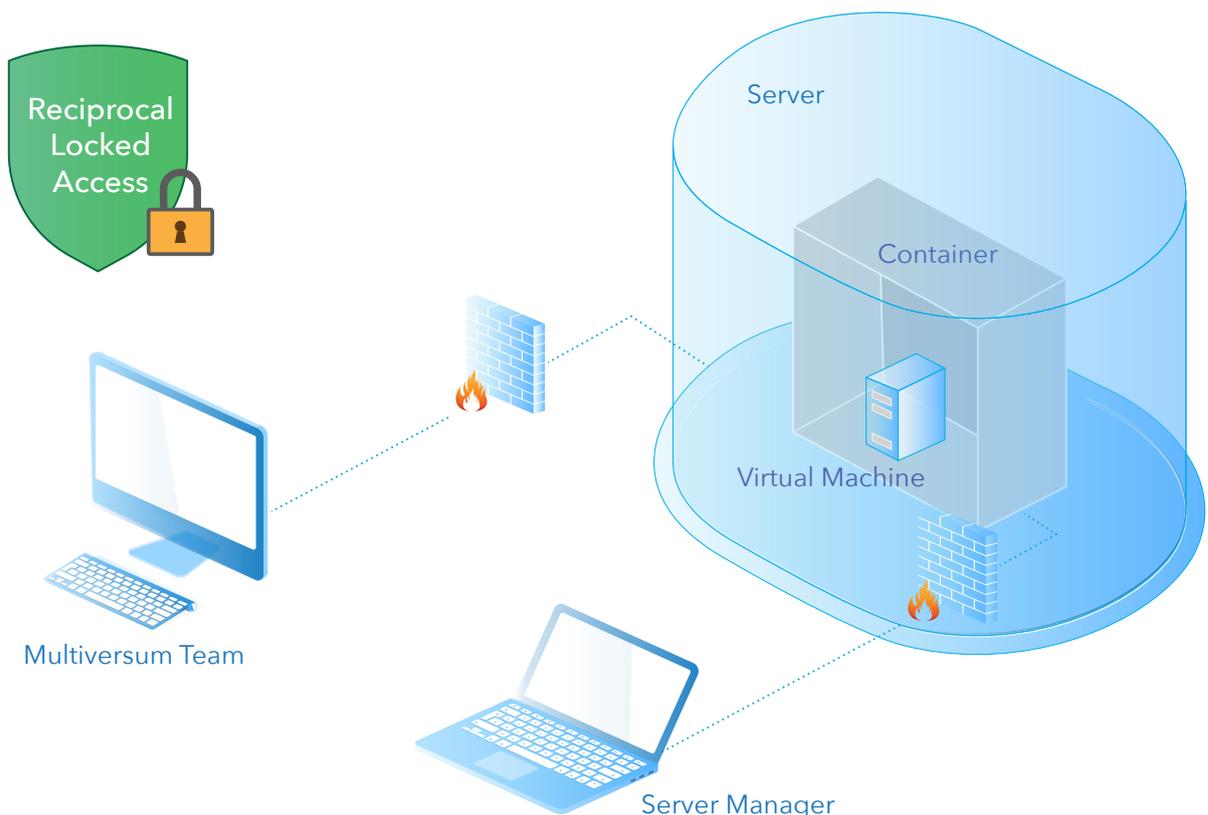


Access Denied

12. Verrouillage double accès (sécurité structurelle)

Les nœuds seront distribués dans des conteneurs virtuels inaccessibles à l'opérateur de la machine host car ils sont protégés par des informations d'identification qui ne sont pas disponibles pour l'opérateur lui-même. La sécurité est donc confiée aux Best Practices de la sécurité Linux à travers, par exemple, le paquet SeLinux15 et/ou autres.

En même temps, même si quelqu'un avait les informations d'identification de la machine Guest, il ne pourrait pas y accéder, n'ayant pas accès à la machine host sur lequel le nœud est en cours d'exécution. Le nœud est donc effectivement soumis à une double fermeture d'accès.



13. Reverse Access Denial (Structural Security)

La double fermeture discutée au point 12 implique un effet de forclusion réciproque à l'accès au nœud. Cela garantit que les nœuds non gérés directement par Multiversum sont parfaitement authentiques et inaccessibles à quiconque, fondamentalement autonomes et isolés des interventions humaines externes.

En plus de l'exploitation et le système de sécurité, trois éléments clés seront distribués dans le Container: le code compilé du serveur Multiversum, un certificat avec une clé asymétrique pour l'authentification dans le Cluster Multiversum et un élément discuté au paragraphe 11, responsable du calcul du challenge basé sur le Hash du code serveur, du certificat, du challenge seed et des données de transaction.

De plus, ce composant sera le seul accessible à l'opérateur pour vérifier la sincérité du code compilé du serveur qui s'exécute sur la machine (les Downsides restent à vérifier).

D'autres fonctionnalités de sécurité supplémentaires peuvent être implémentées, telles que la possibilité de modifier automatiquement le mot de passe d'accès au Container, pendant qu'il est compilé, avec un mot de passe aléatoire inconnu, afin d'empêcher l'accès à quiconque.

Ce mécanisme peut également être implémenté pour le certificat d'accès au cluster.

14. Reciprocal chain confirmation Interopérabilité avec d'autres blockchains)

Multiversum vérifiera la faisabilité d'un composant pour enregistrer le statut d'autres Chain afin de certifier leur statut et de renforcer mutuellement la crédibilité et la validation des transactions (éventuellement face à un Token). Si elle est considérée comme une solution souhaitable, cette composante sera ensuite mise en œuvre.

Multiversum aimerait utiliser la même possibilité pour enregistrer périodiquement une transaction afin de pouvoir partager la responsabilité de vérifier un statut sur d'autres Chain. Il fournira une interface spécialisée à la fonction et favorisera sa mise en œuvre sur de nouvelles Chain. Ce composant utilisera un composant serverless accessible ultérieurement à la compilation du Container pour permettre l'ajout de Adapters vers autres chaînes.

15. Intégration de Java, Spring et JavaScript

Considérant sa vocation pour une utilisation dans les environnements industriels, financiers, juridiques, publics, administratifs et d'entreprise, Multiversum souhaite implémenter

ter un layer d'abstraction supplémentaire sur son fonctionnement, offrant des interfaces de haut niveau collectées dans des bibliothèques fonctionnelles pour Java, Javascript et optionnellement pour d'autres langues mainstream.

Des modules d'intégration à des frameworks tels que Spring seront également développés dans un projet Spring Multiversum. Ces bibliothèques faciliteront l'intégration de la technologie Multiversum dans des solutions propriétaires, à la fois dans la création de chain privées et dans leur accès au MainNet officiel.



16. ACID model

Multiversum implémentera un modèle défini ACID¹⁷. L'acronyme est dérivé de l'anglais **Atomicity, Consistency, Isolation, Durability** et indique les propriétés logiques que les transactions doivent avoir.

Pour que les transactions fonctionnent correctement sur les données, les mécanismes qui les implémentent doivent satisfaire à ces quatre propriétés: **atomicité** - la transaction est indivisible dans son exécution et son exécution doit être complète ou nulle, les exécutions partielles ne sont pas autorisées; **cohérence** - lorsqu'une transaction commence, la base de données est dans un état cohérent, et lorsque la transaction se termine, la base de données doit être dans un autre état cohérent, c'est-à-dire qu'elle ne doit pas violer les contraintes d'intégrité; par conséquent, aucune contradiction (incohérence) ne doit apparaître entre les données stockées dans la base de données; **isolement** - chaque transaction doit être exécutée de manière isolée et indépendante des autres; toute défaillance d'une transaction ne doit pas interférer avec d'autres transactions en cours d'exécution; **durabilité** - également appelée persistance, fait référence au fait qu'une fois qu'un travail de validation a été demandé à une transaction, les modifications apportées ne doivent plus être perdues, pour éviter que, dans la période entre le moment où la base de don-

nées s'engage à écrire les changements et celui dans lequel il les a réellement écrits, les pertes de données dues à des dysfonctionnements se produisent.

17. Model Transactional

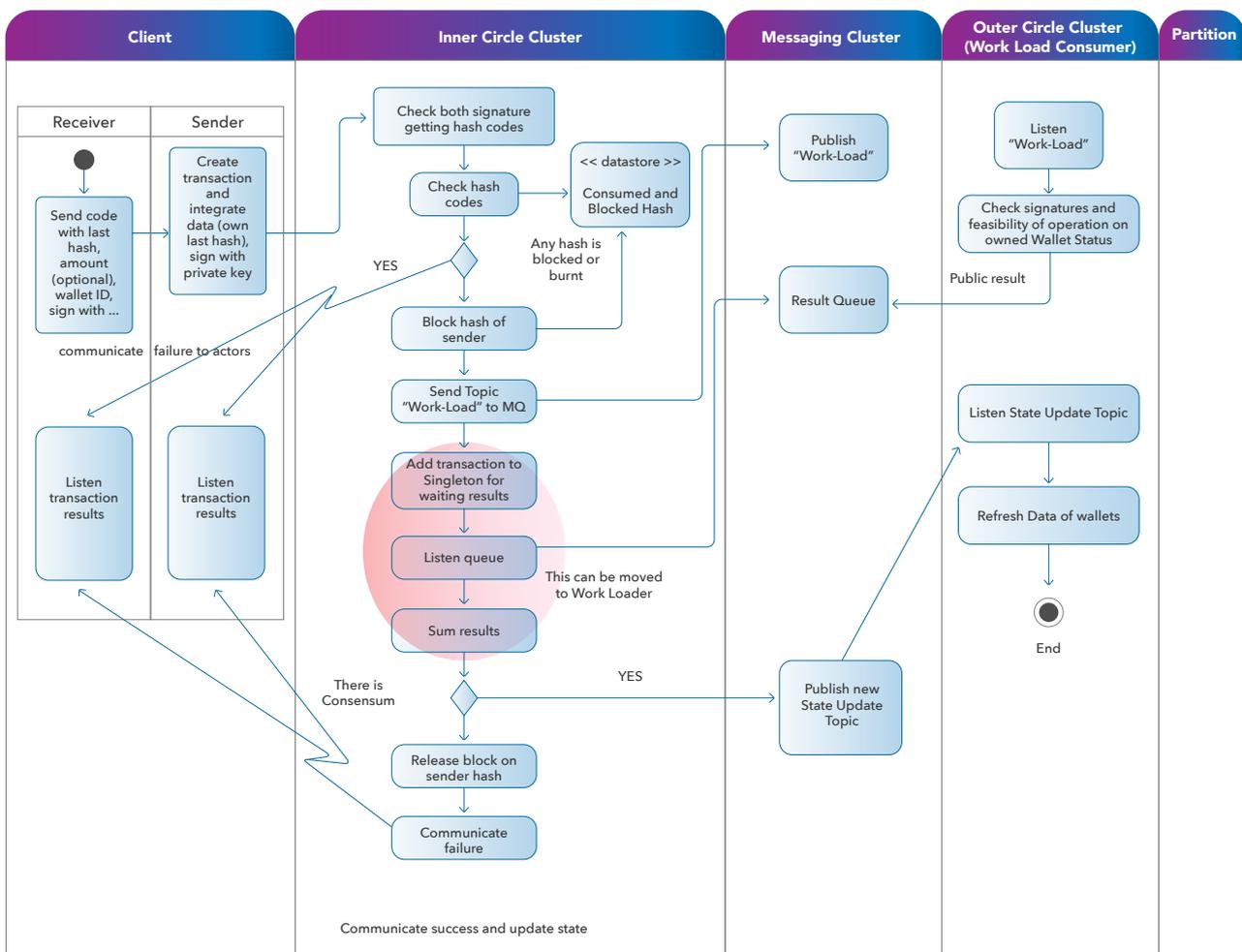
Multiversum persiste les données relatives à une transaction dans un modèle « transactionnel » 18, c'est-à-dire faire en sorte que chacune ou aucune des données sur plusieurs sous-chaînes concernées soient rendu persistantes, afin d'assurer la cohérence de chaque transaction et l'exhaustivité des données.

18. Language SQL like

Pour assurer la facilité de composition des requêtes, Multiversum sera basé sur une syntaxe similaire à SQL19, en utilisant un langage similaire à l'industrie standard. De cette façon, la courbe d'apprentissage de ceux qui approchent cette composante pour la première fois est plutôt douce.

19. Fonctionnement et Full Route Data Flux

Il verrou temporairement dans la mémoire volatile l'utilisation ultérieure de l'identifiant de l'expéditeur de la transaction et compléter certaines données, telles que la transaction précédente à laquelle crochet, timestamp et hash précédent.



La transaction est envoyée à une Topic Message Queue avec un protocole à définir (dans le Pilot en AMQP, à vérifier MQTT ou autres) et distribué en parallèle avec les Worker Nodes.

Les Worker Nodes vérifient qu'ils sont impliqués dans le traitement (ils peuvent ne pas avoir les données nécessaires, sont surchargés ou autrement) et procèdent à la création du nouveau statut du Wallet, récupérant les hash liés aux transactions précédentes et les ajoutant à la transaction. Le résultat de la Proof of Integrity est également ajouté.

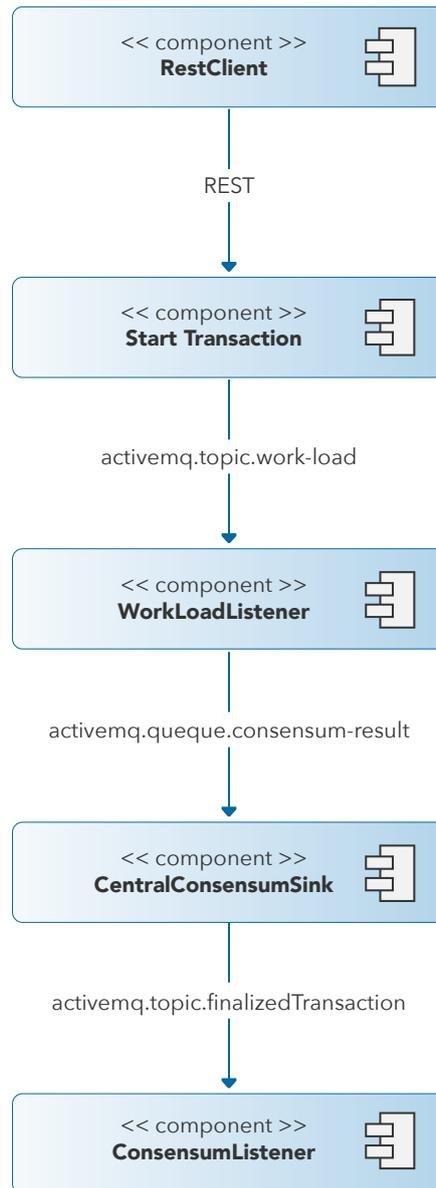
Enfin, ils calculent le hash de transaction sur l'ensemble de données.

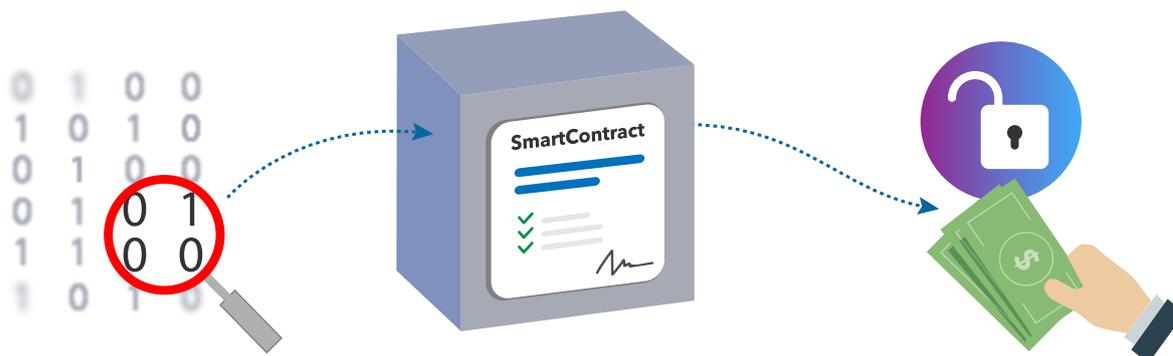
Les Worker Nodes enregistrent cette transaction dans une mémoire volatile et envoient un vote aux nœuds coordinateurs via Message Queue qui rassemble tous les votes.

Si les votes et hash sont cohérents, les nœuds de coordination écrivent en permanence sur leurs supports les transactions et les nouveaux statuts du wallet, brûlant le hash des états précédents et en communiquant avec un système supplémentaire de Topic Message Queue, que le vote est valide. À ce stade, les Worker Nodes persistent toute l'opération. Fin du best case full route.

Logic data flux

Detail of process flow





Smart Contracts

Multiversum estime qu'il est nécessaire de proposer au public Smart Contracts²¹ évolué; en même temps il a décidé que, pour l'instant, à moins d'une modification future des champs de sa recherche, l'objectif d'étudier cette possibilité, en limitant son action, avec la modestie appropriée à l'environnement scientifique, d'identifier la meilleure solution Open Source sur le marché et s'y référer pour son inclusion dans sa solution (compatible avec le modèle de licence du projet auquel il se réfèrera).

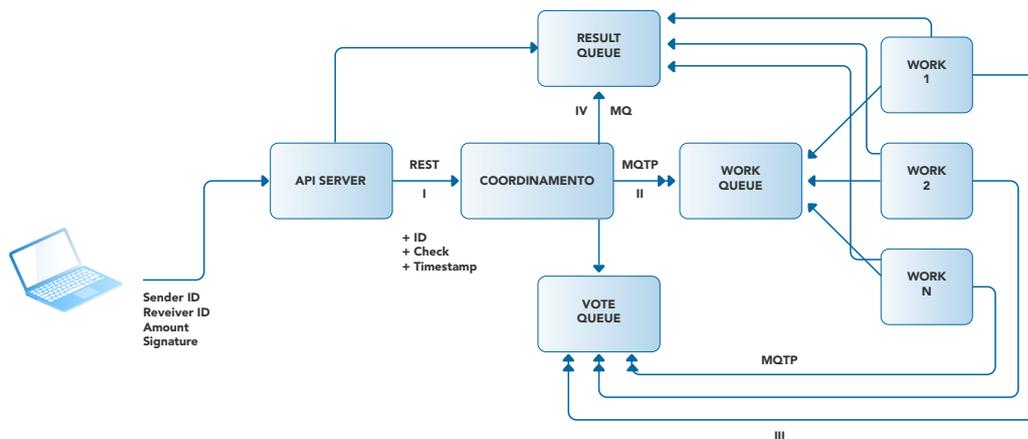
Infrastructure

L'infrastructure Multiversum a été conçue pour assurer la résilience et high availability. Cet objectif a été atteint en développant des clusters de nœuds capables d'auto-élire leurs membres à des fonctions spécifiques, en fonction des caractéristiques techniques de chaque nœud, parmi lesquelles:

- Capacité de calcul
- Capacité de mémoire
- Vitesse de ping mutuelle
- Complétude des données de chaîne
- Fiabilité de la machine
- Doutes sur la preuve d'intégrité

Les nœuds peuvent avoir une ou plusieurs fonctions, parmi lesquelles:

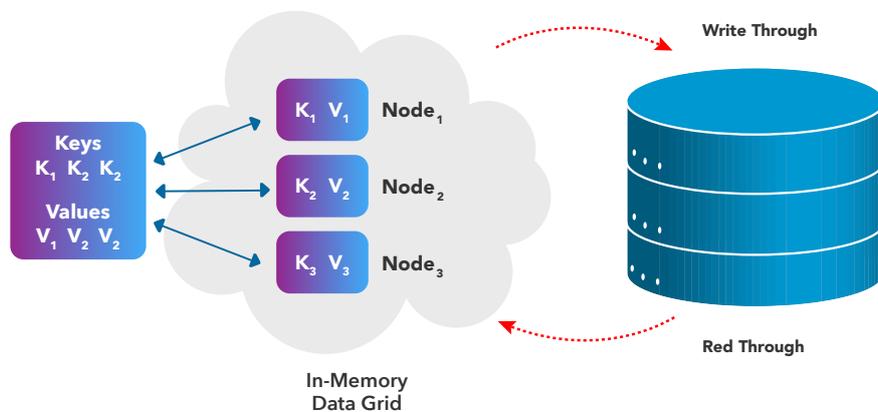
- Nœuds clients
- Nœuds de coordination
- Nœuds de messagerie
- Nœuds de travail
- Nœuds persistants
- Nœuds de backup



Tout nœud pouvant démontrer qu’il possède un certificat valide peut s’enregistrer auprès du cluster et obtenir une fonction

En cas de crash d’un ou plusieurs nœuds, le cluster pourra redistribuer de manière autonome les tâches, optimisant ainsi les rôles.

Il y aura des composants de cache partagés JVM partagés tels que memory database, qui permettent des mécanismes Read through: la recherche de données en mémoire volatile

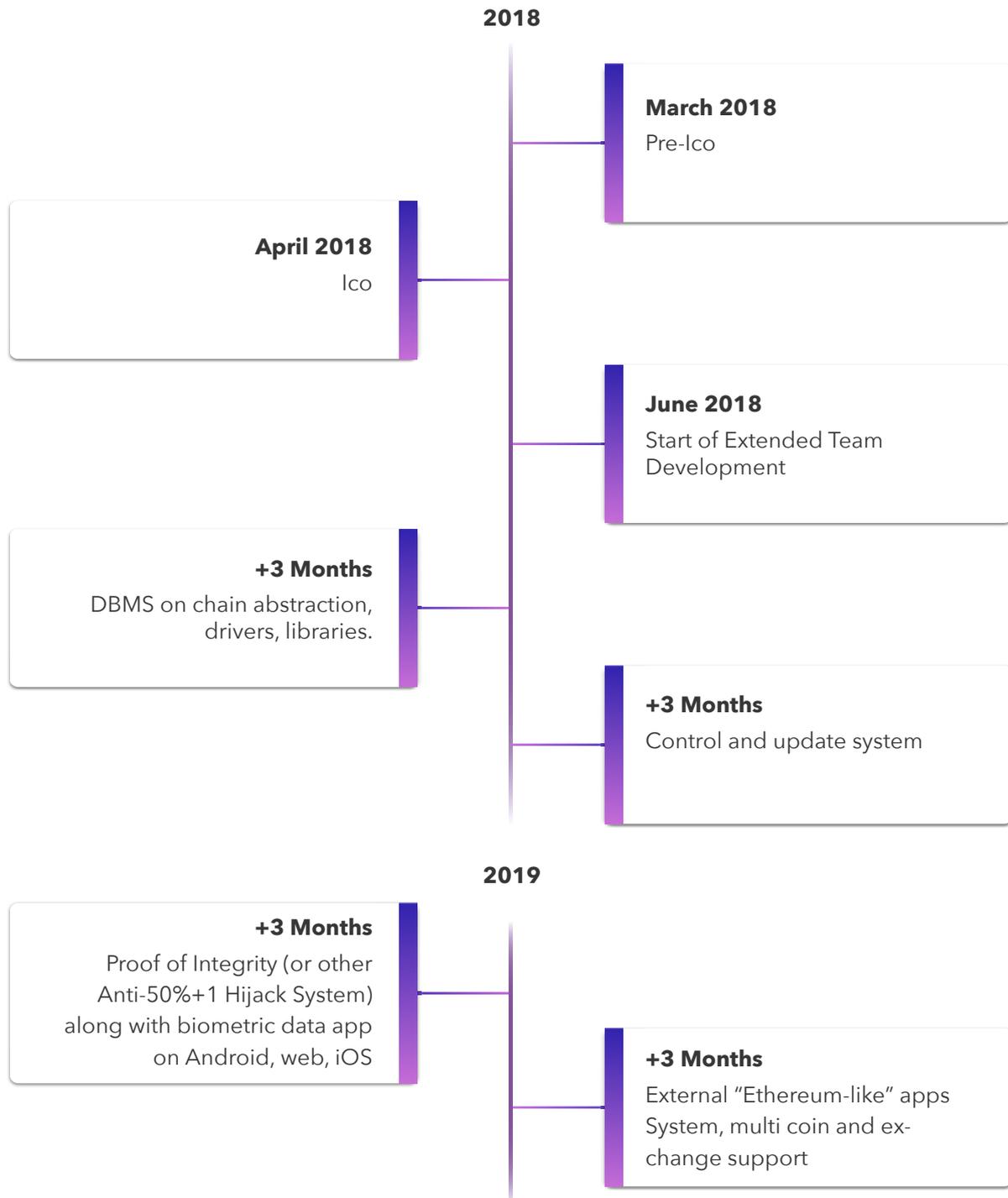


(si non présente, dans la physique) et, ensuite, Write Through: l’accumulation de données en mémoire volatile et l’insertion de masse dans le physique, pour ne pas devoir attendre l’achèvement de l’handshake et le data overhead une fois seulement, obtenant une optimisation des performances (dans le cas des transactions individuelles, elles seraient exécutées à plusieurs reprises).

Consignes de sécurité

En cours de réalisation, on offrira des «Hacker’s bounties» à ceux qui trouveront des vulnérabilités et proposeront éventuellement des remèdes approprié.

Road Map technique

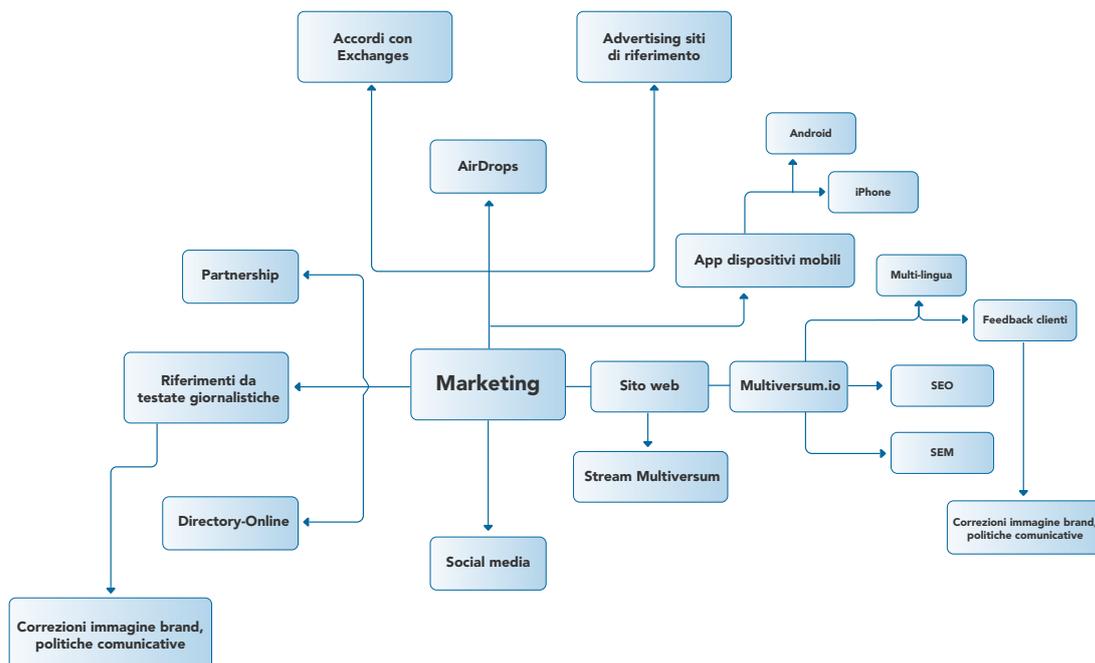


L'implémentation complète prendra environ une année de travail pour déployer le serveur du réseau principal pour deux équipes de développement, un architecte logiciel, deux développeurs d'interface graphique, deux responsables de la sécurité, un Business Architect. Dans les années suivantes le développement continuera à permettre d'avoir un produit de qualité d'entreprise: à partir de ce développement continu, le coin Versum gagnera des avantages de crédibilité et d'image. Le réseau principal sera complet avec tous les mécanismes de sécurité et la logique du produit d'entreprise, mais pas ceux qui rendent la technologie facilement intégrée, car elle n'est pas indispensable pour son utilisation. Le software sera publié en permanence pour soutenir la crédibilité du projet, et le Test Net offrira les nouvelles fonctionnalités disponibles dès qu'elles seront disponibles.

Stratégie de marketing

Nous avons concentré la planification de l'ensemble de l'organisation marketing en partant d'un contexte général pour ensuite nous concentrer sur des aspects spécifiques. Nous comprendrons toutes ces activités qui permettront la réalisation des objectifs, en adoptant une approche globale pour l'ensemble de l'organisation (à partir de la définition de la mission de l'entreprise à l'identification de la stratégie la plus appropriée). La stratégie de l'entreprise sera le reflet d'un environnement en constante évolution et la mission de l'entreprise sera de créer de la valeur pour les parties intéressées, en assurant l'équilibre entre la logique de gestion à court et à long terme. Les 4 composantes du plan sont:

- Mission de l'entreprise
- Objectifs d'entreprises
- stratégies d'entreprise
- Portefeuille activités d'entreprises



L'un des principaux outils sera le Social Media Marketing qui est l'ensemble des activités menées sur les réseaux sociaux pour accroître la notoriété du brand, identifier les consommateurs potentiels, générer des contacts et construire des relations significatives avec les clients. Nous réaliserons plusieurs actions qui font partie d'un plan stratégique unique, à partir de la gestion et surveillance des réseaux sociaux à l'aide d'outils dédiés et en renforçant la communauté par le soin quotidien des contenus et des interactions, jusqu'à l'analyse des résultats obtenus et la vérification des tactiques mise en place. Chacun d'entre eux se reflète dans les compétences de nos Social Media Strategists: la planification stratégique, la définition et la production de la ligne éditoriale, l'interaction et le soutien au marché et l'analyse des résultats.

Les couches d'éléments qui enveloppent les univers sont chacune dix fois plus épaisses que la précédente, tous les univers, regroupés, apparaissent comme des atomes dans une immense combinaison.

Le bhagavata Purana 3.11.41



MULTIVERSUM

HERE TO STAY