

# MULTIVERSUM

HERE TO STAY

**WHITE PAPER v 1.0.6**

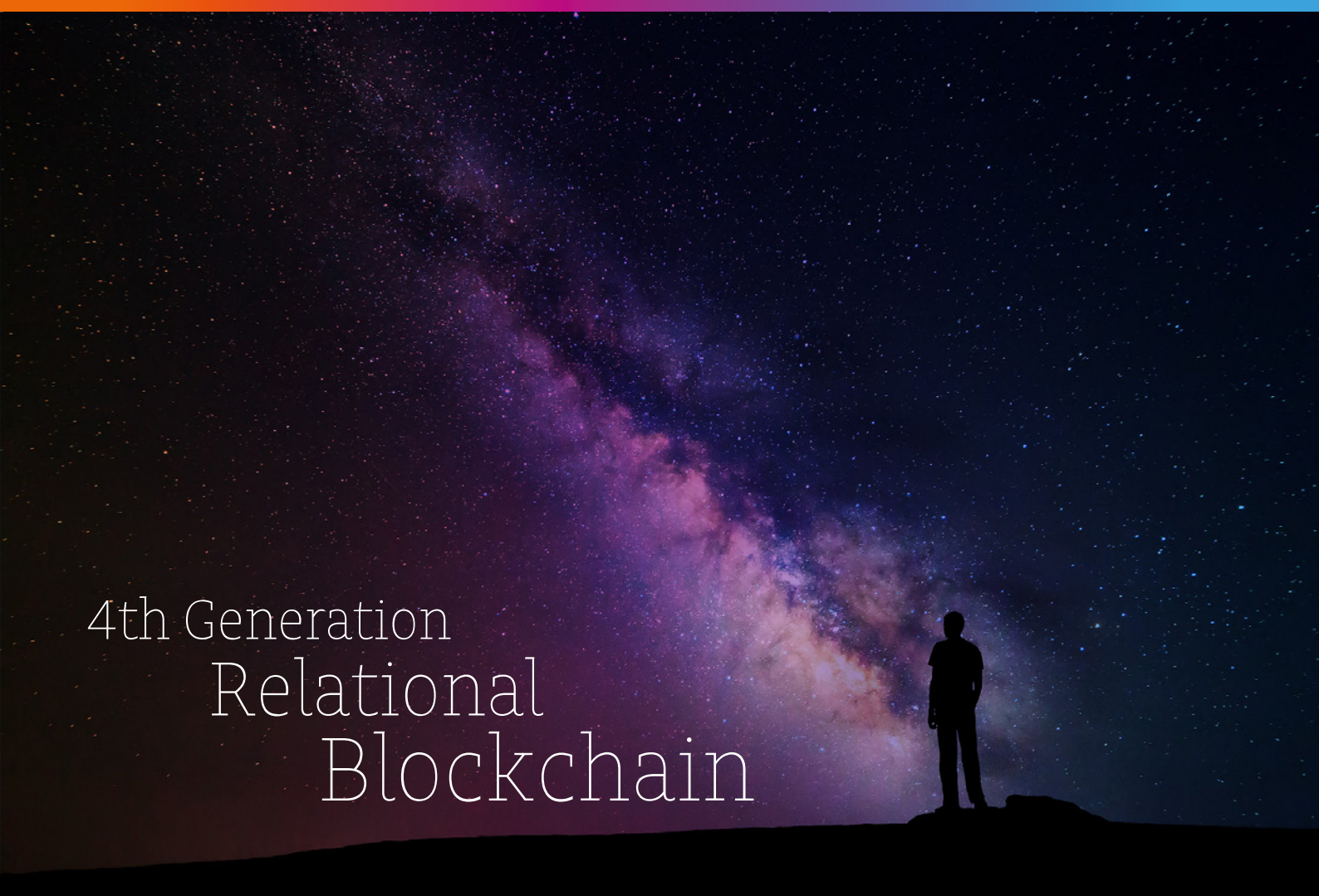
Business | Technical

Italiano

19.02.2018

Autori: Multiversum Team

[www.multiversum.io](http://www.multiversum.io)



4th Generation  
Relational  
Blockchain



**Ci sono innumerevoli universi  
oltre al nostro, benché siano  
infinitamente estesi,  
si muovono come atomi in Te.**

Bhagavata Purana 6.16.37

# Contenuti

<b>Multiversum Identità e Mission</b>	<b>4</b>
<b>Multiversum Blockchain Relazionale di Quarta Generazione</b>	<b>5</b>
<b>Presentazione al pubblico</b>	<b>8</b>
Il Concetto di Multiversum ed il suo utilizzo su scala Globale	8
Velocità e Tecnologia	9
Scalabilità Orizzontale	9
Ambiente	10
Gestione dei dati: Database Relazionale	10
In conclusione...	10
<b>Analisi dello State of Art delle Blockchain</b>	<b>11</b>
Metodologia AGILE	12
<b>Missione di Multiversum</b>	<b>14</b>
1. Realizzazione di un Crypto relational DB con Complex Data Structures autoconvalidanti	15
2. Catene sdoppiabili e ricongiungibili in funzione della quantità di lavoro necessaria (Parallel Work)	16
3. Sharding dei dati (Parallel Work)	16
4. Struttura microservice e offerta di Advanced API	17
5. Rollback (User Security)	17
6. Freezable wallets (User Security)	18
7. Integrazione dei dati biometrici come seed per l'Electronic Signature	18
8. Interfaccia ERC23 (Interoperabilità con altre Blockchain)	19
9. Adattatori nativi off-chain per il proprio ERC20/ERC23 (Interoperabilità con altre Blockchain)	19
10. Adattatori nativi off-chain per ERC20/ERC23 ospiti (Interoperabilità con altre Blockchain)	19
11. Proof of Integrity (Protocol Innovation)	20
12. Double Access Lock (Structural Security)	20
13. Reverse Access Denial (Structural Security)	21
14. Reciprocal chain confirmation (Interoperabilità con altre blockchain)	22
15. Integrazione per Java, Spring and JavaScript	22
16. ACID model	23
17. Modello Transactional	23
18. Linguaggio SQL like	23
19. Funzionamento e Full Route Data Flux	23
Logic data flux	25
Smart Contracts	26
Infrastructure	26
Note sulla sicurezza	27
Road Map Tecnica	28
References	29
<b>Marketing Strategy</b>	<b>30</b>
<b>Disclaimer</b>	<b>32</b>

# Multiversum Identità e Mission

La prima generazione di blockchain è costituita dalle prime coin come Bitcoin, basate su *Proof of Work* ed i suoi vari cloni e fork.

Le BC di seconda generazione sono più eterogenee, basate sull'uso di token come Ethereum e il suo ecosistema di soluzioni.

Queste due categorie sono caratterizzate da bassissima efficienza energetica e ridotto numero di transazioni.

Alla terza generazione appartengono quelle BC che hanno provato a fornire risposte alla lentezza delle transazioni e alla incapacità di essere scalabili utilizzando vari meccanismi: Proof of Stake, off chain route, graphchain, centralizzazione completa o parziale.

La quarta generazione, invece, si ripropone di continuare a dare risposte alla lentezza del sistema; contemporaneamente si pone obiettivi di utilizzabilità in campo aziendale, cosa alla quale poco si appresta una catena disorganizzata di dati che necessitano di sistemi di storage di dati complessi organizzati in tabelle correlate (come i database relazionali) ma al tempo stesso in cui i dati si convalidano e rafforzano con la tecnica della blockchain. Ovvero è il tentativo di far sfociare questa tecnologia ad una vera utilità produttiva primaria. Multiversum offre la gestione organizzata dei dati complessi al posto della semplice successione dei dati, divisibilità della chain e ricongiunzione per permettere il parallelismo, e verifica della fattibilità del *Proof of Integrity* (prova crittografica del codice del server) al posto del *Proof of Work*.

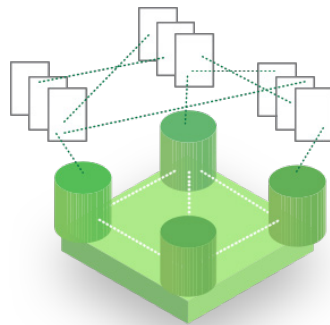
Inoltre si aggiungono dispositivi di interoperabilità con altre chain (ospitando sulla nostra chain altre coins e tokens e viceversa) ed un servizio di notariato che funga da convalida esterna.

Intanto, oltre a tutte le nostre innovazioni, adopereremo certamente anche alcune delle soluzioni già ottimali che i nostri colleghi hanno implementato.

# Multiversum

## Blockchain Relazionale di Quarta Generazione

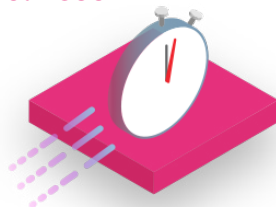
*Perché Multiversum è la Blockchain 4.0 ?*



### Blockchain Relazionale

Una blockchain di nuova generazione, che passerà dal poter gestire un solo tipo di dati in modo lineare a più tipologie di dati, relazionati tra loro tramite identificativo, in una struttura multidimensionale.

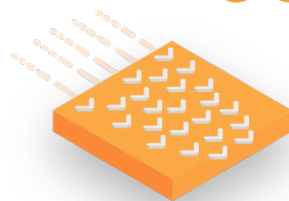
<0.2 sec



### Velocità di Transazione

In meno di soli 0,2 secondi i fondi vengono trasferiti da un wallet all'altro compiendo tutti i vari passaggi che ne certificano la sicurezza. Tra le più veloci blockchain al mondo.

64000 TPS → ∞



### Quantità di Transazioni

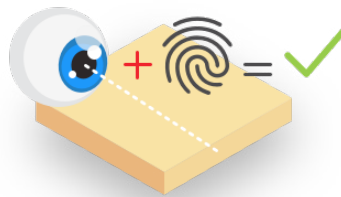
Fino a 64000 TPS su server a 64 core (1000 TPS per core), supporto per sistemi a più di 64 core - scalabilità senza limiti.

POI



## Sicurezza estrema di Transazione

Non esisterà più il concetto di POS (Proof of Stake):  
verrà sostituito da POI (Proof of Integrity).



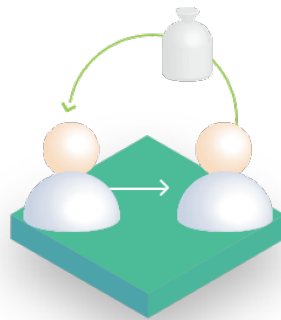
## Wallet di nuova Generazione / Input Biometrico

Estrema sicurezza nell'accesso al wallet  
e nell'invio dei fondi mediante input biometrico.



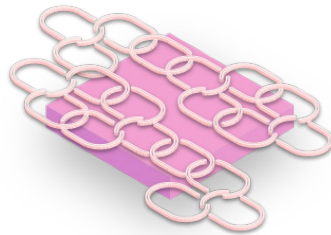
## Eco-Friendly

Una transazione avrà costi irrilevanti e impatto ambientale quasi nullo.



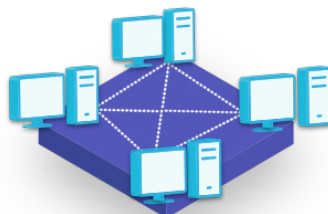
## Rollback

Il sistema di rollback sarà opzionale e disponibile in soluzioni ad-hoc che potranno trarre beneficio da questa funzione.



## Catene Sdoppiabili

Ottimizzazione del carico di lavoro con una ripartizione delle risorse tra i nodi disponibili grazie alla possibilità di suddividere la main chain in più sub-chains.



## Allocazione di Recovery Nodes

L'azienda Multiversum ha collocato nodi periferici di Global Disaster Recovery in diversi continenti.

# Presentazione al pubblico

## Il Concetto di Multiversum ed il suo utilizzo su scala Globale

Multiversum è una tecnologia che, modificando gli aspetti attinenti alla persistenza dei dati nella Blockchain attraverso dati auto-verificanti e distribuiti, organizzati in entità coerenti relazionate tra loro da link simbolici, ne rivoluziona i tradizionali limiti, portando, di fatto, ad una nuova generazione: la Blockchain 4.0.

Su questa tecnologia si basa un sistema decentralizzato e distribuito di transazioni coerenti e auto-verificanti: Multiversum BC. Le attuali Blockchain si basano su una sequenza di transazioni che rappresentano un unico tipo di dato: o attinente alla transazione stessa o a molteplici catene coesistenti e non saldamente coerenti tra loro, in cui i dati sono organizzati in blob concettuali e riconducibili l'uno all'altro con difficoltà e costi computazionali enormi.

Multiversum consente, invece, di creare un Crypto Database Relazionale (una soluzione di stoccaggio dei dati avanzata e organizzata) che permette di avere non un solo tipo di dato, ma una serie di dati riuniti in tabelle in una struttura di dati complessi, relazionati l'uno con l'altro attraverso un identificativo.

Ognuno di essi, nel momento in cui cambierà uno stato, avrà una sua sub-catena che proverrà da un nodo già certificato e si ricongiungerà, per ottenere la certificazione, con tutto il resto della catena.

Multiversum è, pertanto, una tecnologia Blockchain evoluta che offre features uniche per risolvere questi problemi in un panorama di cripto validazione e distribuzione, e potrà essere usata in qualsiasi ambiente: Amministrativo, Industriale, Finanziario e Governativo. Uno degli obiettivi principali di Multiversum è offrire al mercato, in ogni momento, il prodotto più evoluto disponibile: ciò sarà possibile utilizzando una metodologia denominata AGILE.

Questo approccio ci permetterà di capire le richieste di mercato, durante e dopo la fase di sviluppo, e di implementarle progressivamente, arrivando a pubblicare la Main Net più evoluta e completa disponibile.

Questa tecnica di sviluppo, ci permette di offrire il prodotto più moderno e attuale sul mercato.



## Velocità e Tecnologia

Un punto di forza di questa tecnologia è sicuramente la velocità, dovuta alla capacità di poter processare differenti transazioni parallelamente.

Questa caratteristica permette di avere una perfetta scalabilità orizzontale, ossia la possibilità di poter aumentare all'infinito la capacità di elaborazione delle transazioni, aggiungendo nuovi processori invece di sostituire quelli esistenti, rendendo ogni nodo aggiuntivo utile a migliorare le prestazioni dell'intero sistema.

## Scalabilità Orizzontale

Multiversum può godere di due peculiarità molto importanti che lo rendono così efficiente: La chain è in grado di ottimizzare la propria struttura dividendosi autonomamente in più sub-chain in base alle risorse richieste e al flusso di dati, ripartendo così il lavoro del cluster di processori nel modo ottimale tra i nodi disposti all'elaborazione.

Questa suddivisione potrà essere effettuata all'infinito fino alla normalizzazione dei carichi di lavoro, quando, sempre in modo autonomo, la chain tornerà ad essere una.

Tutto questo grazie ad un dispositivo che permette ad ogni anello di convalidare due differenti chain dei due differenti anelli precedenti.

La possibilità di fare lo sharding dei dati: una tecnica che permette la distribuzione dei dati in più nodi.

Immaginando di avere una serie di dati ABC e tre nodi del Cluster, avremo una suddivisione dei dati così disposta:

- AB
- BC
- CA

Questa suddivisione permette una maggior velocità di elaborazione delle transazioni che andranno a ricercare i dati da utilizzare solo nei nodi che le conterranno, ottimizzando ogni passaggio.

Un'altra caratteristica presente molto importante si chiama High Availability: la possibilità di basarsi su una tipologia di cluster che garantisce continuità dei servizi anche in caso di interruzione di alcuni nodi della rete.

Utilizzando l'esempio precedente (nodi A, B e C), se si interrompesse C, i nodi A e B rimarrebbero completamente operativi, permettendo la continuità del servizio senza alcuna perdita di dati finché saranno operativi almeno il 50% + 1 dei nodi totali.

Il cluster, in questa situazione, comunicando con tutti i nodi, organizzerà autonomamente la distribuzione dei dati fino al completo ripristino operativo.

## Ambiente

Multiversum è inoltre eco-friendly, perché si pone come obiettivo l'eliminazione del mining, uno spreco di potenza di calcolo ed energie immenso, che sostiene il Proof of Work, a favore di un nuovo concetto, il Proof of Integrity: un protocollo che verifica la veridicità e l'autenticità del software che va a risolvere ogni persistenza della transazione.

## Gestione dei dati: Database Relazionale

Multiversum, col suo Crypto Database Relazionale, può facilmente strutturare i dati senza limiti nel tipo di collegamenti.

Ogni wallet avrà una serie di stati (states) e sarà collegato ad una persona (user); ogni nuovo anello di cambiamento dello state del wallet andrà ad incorporare due cose:

- lo state precedente, in maniera tale da avere la convalidazione dell'atto precedente;
- un collegamento all'ultima transazione (o all'ultimo anello della main chain), per cui si saprà da dove deriva il nuovo anello del cambio di stato.

Avvenuto questo cambiamento, verrà aggiunta la transazione di modifica e, a questa, si ricongiungerà l'anello dello state modificato, che indicherà la provenienza del collegamento del nuovo cambio di stato.

La nuova transazione, pertanto, erediterà due hash: uno dall'anello di stato, uno dall'anello della transazione precedente.

In questa maniera tutte le operazioni convalidano quelle precedenti relazionate alla transazione stessa.

Questo sistema è tanto complesso quanto avanzato, e permetterà di implementare software sulla nostra tecnologia garantendo una diffusione istituzionale, governativa, finanziaria e industriale, portando tutto il mondo delle Blockchain ad un livello superiore.

## In conclusione...

Questo approccio ci permetterà di capire le richieste del mercato durante e dopo la fase di sviluppo, e di implementarle progressivamente arrivando a pubblicare la MainNet più evoluta e completa disponibile.

Lo sarà in quel momento e lo sarà anche in futuro.

Multiversum rilascerà immediatamente un Pilot di Blockchain funzionante ed un APP Wallet proprietario in versione Beta. Nel giro di 6 mesi i prodotti saranno completi e verranno aggiornati quotidianamente in base alle esigenze.

Nessuna Blockchain posteriore a quella di BTC, all'uscita, ha potuto vantare tanto sviluppo precorso. Il valore della Coin e del Token non potranno che beneficiarne.

# Analisi dello State of Art delle Blockchain

Allo stato attuale, gli attori principali del “fenomeno blockchain” sono caratterizzati da una notevole robustezza in materia di sicurezza.

A fronte di ciò, tale sicurezza comporta capacità di calcolo enormi, inquinamento, commissioni delle transazioni inaccettabili ed una lentezza incapace di rappresentare il progresso tecnologico attuale, inficiando la possibilità di dare una risposta tecnica credibile agli use cases finanziari e commerciali moderni.

Tale lentezza è causata da incapacità di ottenere scalabilità orizzontale<sub>1</sub>, ovvero l'aumento della capacità di calcolo ottenuta dalla semplice aggiunta di processori invece che dalla loro sostituzione con versioni più veloci.

Un secondo motivo di scarsa efficienza è insito nel meccanismo di sicurezza delle blockchain attuali basato sul Proof of Work<sub>2</sub> e, meno frequentemente, sul Proof of Stake<sub>3</sub>, che ovidio al rischio di perdere il controllo della maggioranza del cluster a causa di Sybil Attacks<sub>4</sub> richiedendo ai nodi una capacità di calcolo artificialmente alta, rendendone impossibile una creazione indiscriminata attraverso l'aumento della difficoltà<sub>5</sub>. Inoltre, le blockchain attuali sono semplici successioni di cambi di stato di singole entità di dati: la ricostruzione degli stati attuali, richiedendo una scansione dell'intera catena, comporta ulteriore lentezza del sistema e spreco di risorse. Tale impostazione rende oltretutto inadeguato l'impiego della tecnologia blockchain in un contesto industriale e scientifico, ambienti dove le strutture di dati sono estremamente complesse.

La sicurezza garantita dalle blockchain attuali riguarda solo i dati, ma non si estende all'utente: è impossibile, ad esempio, recuperare coins o token indebitamente sottratti, anche qualora fossero stati individuati nella chain, o bloccare account coinvolti in attività illecite. Un ultimo problema è la totale disomogeneità e incomunicabilità nel panorama delle diverse criptovalute: ciascuna Blockchain, esistendo nel proprio universo separato, risulta incapace di relazionarsi con le altre.

## Metodologia AGILE

Multiversum si ripropone di utilizzare la metodologia AGILE, durante lo sviluppo del prodotto. Questa tecnica presuppone una drastica riduzione della progettazione iniziale, in favore della valorizzazione delle esperienze ottenute in corso d'opera, che evidenziano opportunità e pericoli altrimenti difficilmente individuabili ex ante, premiando *Best Practices* (migliori prassi) e penalizzando *Ways of Working* (modalità operative) inadeguate.

La metodologia AGILE è l'*Industrial Standard* della produzione del software e suggerisce a sviluppatori, *product owners* ed investitori di considerare flessibile lo scope, del progetto, per adattarlo alla variazione delle esigenze del mercato. Inoltre, in un settore in rapida e costante evoluzione come quello del software, proporre al mercato, dopo un periodo tipico di sei mesi di studio ed un anno di implementazione, un prodotto nato per rispondere alle esigenze di 18 mesi prima, significherebbe offrire una soluzione obsoleta, che risolve problemi non attuali, probabilmente già superati dalla concorrenza e incapace di dare risposte alle nuove sfide. AGILE, al contrario, permette di offrire al mercato il prodotto più innovativo possibile al momento della consegna del progetto.

# 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)

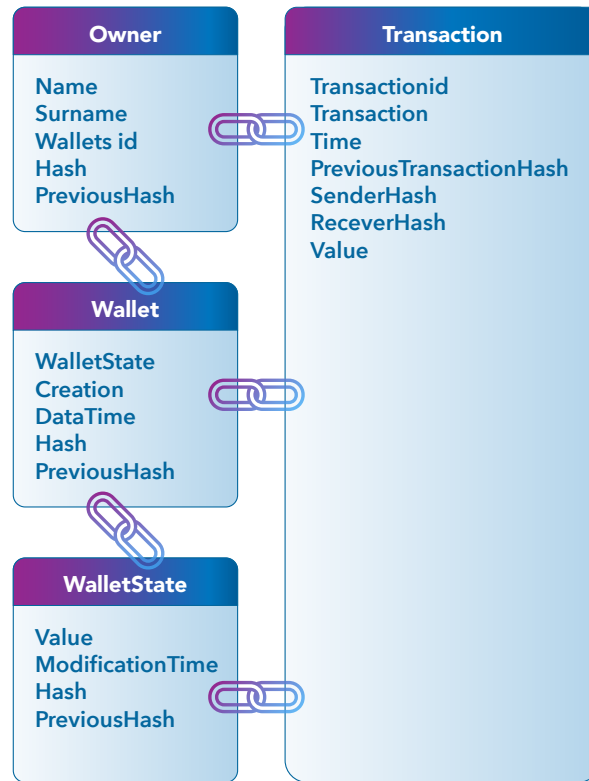
### **ERC23**

(Interoperability with other BC)

# Missione di Multiversum

Multiversum si propone di studiare soluzioni per permettere uno step-up generazionale nel mondo delle blockchain, in particolare, come Unique Selling Points, si pone i seguenti obiettivi:

1. Realizzazione di un Crypto Relational DB con Complex Data Structures autoconvalidanti
2. Catene sdoppiabili e ricongiungibili in relazione alla quantità di lavoro necessaria (Parallel Work)
3. Sharding dei dati (Parallel Work)
4. Offerta di Advanced API
5. Rollback (User Security)
6. Wallet multicurrency congelabili (User Security)
7. Integrazione dei dati biometrici come seed per l'Electronic Signature
8. Interfaccia ERC23 (Interoperabilità con altre Blockchain)
9. Adattatori nativi off-chain per il proprio ERC20/ERC23 (Interoperabilità con altre Blockchain)
10. Adattatori nativi off-chain per ERC20/ERC23 ospiti (Interoperabilità con altre Blockchain)
11. Proof of Integrity (Protocol Innovation)
12. Double Access Lock (Structural Security)
13. Reverse Access Denial (Structural Security)
14. Reciprocal Chain Confirmation (Interoperabilità con altre Blockchain)
15. Integrazione per Java, Spring and Javascript
16. Modello ACID
17. Modello Transactional
18. Linguaggio SQL-like



### 1. Realizzazione di un Crypto relational DB con Complex Data Structures autoconvalidanti

Multiversum ha una forte vocazione per l'impiego nei contesti industriali, istituzionali, pubblici ed enterprise: ambienti che richiedono strutture di dati complesse, impossibili da rappresentare in maniera efficiente e normalizzata con una semplice chain.

Questa vocazione si manifesta col voler essere il primo crypto database relazionale ad offrirsi al mercato, distribuito e opzionalmente decentralizzato. Tale primato è stato raggiunto partendo dalla concettualizzazione di *entità chainable*. Tali Entità permettono di implementare un'interfaccia capace di definire i metodi necessari ad un dato per poter essere inserito come anello in una blockchain.

Nel modello concettuale esisterà una catena primaria alla quale si collegheranno catene secondarie rappresentanti entità di tipo diverso, che, a loro volta, rappresentano i *records* di una tabella.

Tali entità si collegheranno ulteriormente al loro ultimo stato di persistenza, e dopo le modifiche necessarie si riuniranno nell'ultimo anello della catena primaria che ricongiungerà le due catene.

L'interfaccia "chainable" presuppone: la registrazione di molteplici anelli dai quali derivarne di nuovi, la registrazione dei molteplici anelli che derivano dal singolo, e quella della convalida della presenza di tali dati, che agisce importando le hash degli anelli citati nel computo della hash corrente.

Nell'implementazione della tecnologia Multiversum relativa alle coins Versum, le *chainable*

entities che conviveranno sulla chain apparterranno a quattro Tabelle: User, Wallet, Wallet State e Transaction, le quali si correleranno le une con le altre convalidandosi reciprocamente.

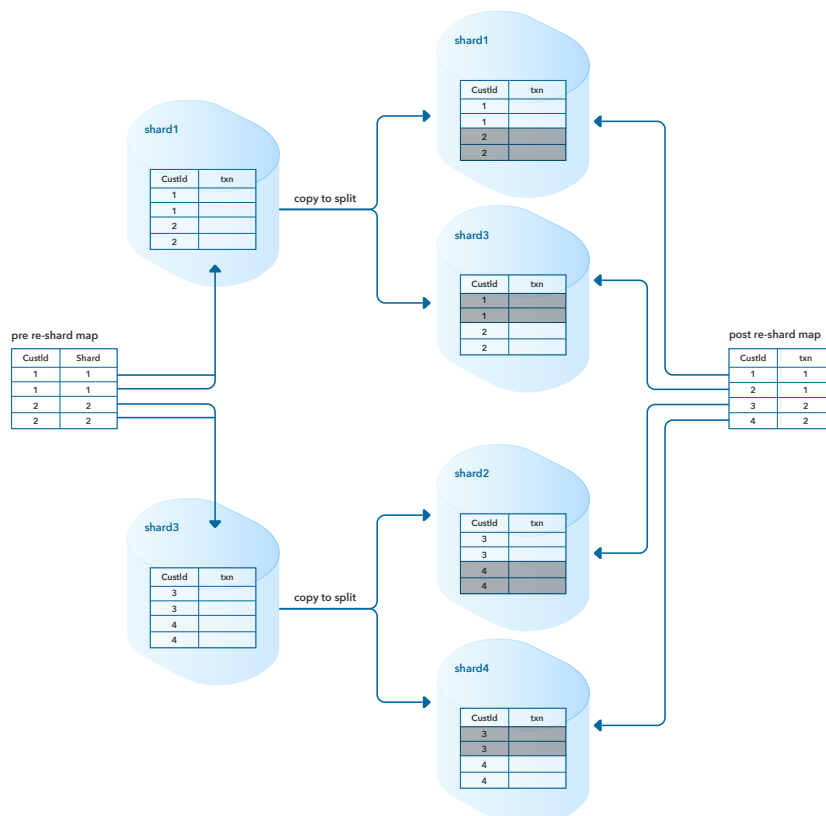
## 2. Catene sdoppiabili e ricongiungibili in funzione della quantità di lavoro necessaria (Parallel Work)

La capacità di derivare molteplici anelli da uno e, successivamente, riunirli deriva dall'impiego di analizzatori del carico di lavoro che, in presenza di un alto numero di richieste d'esecuzione, segnaleranno al cluster la necessità di sdoppiare (per infinite volte, se necessario) la catena primaria delle transazioni in due catene secondarie e, al ridursi della stessa, daranno modo di ricongiungersi alle molteplici sub-chains precedentemente generate. Questo meccanismo permette il lavoro parallelo, continuando ad offrire tutela dall'alterazione dei registri delle transazioni.

## 3. Sharding dei dati (Parallel Work)

Ogni nodo potrà avere in memoria tutti i dati della blockchain o solo una parte di essi. Nel caso si manifestasse la necessità di parallelizzare i dati, i nodi coordinatori ne stabiliranno le modalità di suddivisione in maniera tale da ottimizzarne la distribuzione attraverso parametri di parallelizzazione del calcolo e *High Availability*, garantendo (finchè il 50% +1 dei nodi resterà online) la reperibilità dei dati anche in caso di istantanea scomparsa di una parte del cluster di persistenza.

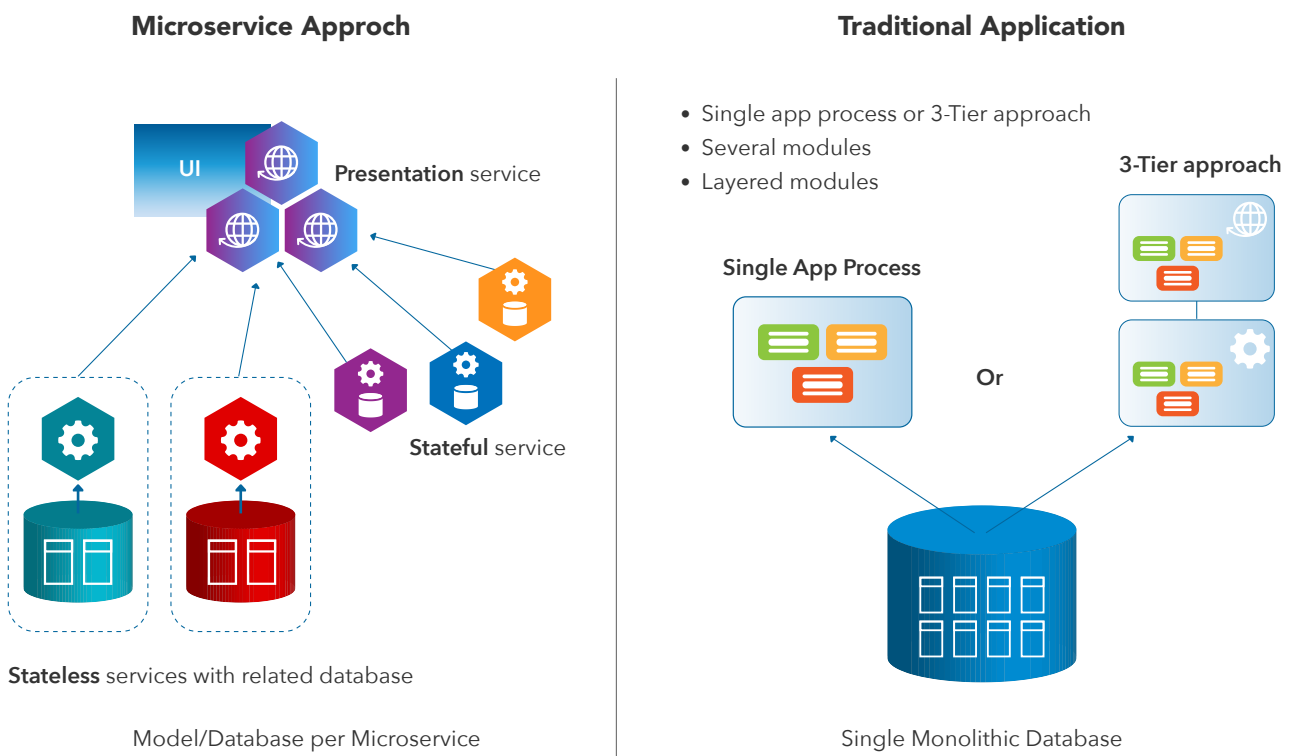
Tali nodi, nella fase successiva al crash parziale del cluster, saranno in grado di ridistribui-





re e riorganizzare i propri dati autonomamente, in modo da poter affrontare nuovamente un ulteriore crash parziale del cluster il prima possibile.

I dispositivi descritti in questo punto e nel precedente concedono la capacità di lavoro parallelo, quindi: scalabilità orizzontale, sicurezza, *high availability*, resilienza del sistema, mancanza di un single point of failure<sub>10</sub> e *self disaster recovery*.



#### 4. Struttura microservice e offerta di Advanced API

Multiversum, essendo stato sviluppato su una piattaforma basata in parte su Microservices<sub>11</sub> e in parte sul modello Serverless<sub>12</sub>, ed anche grazie ad API moderne, estese e sicure, con caratteristiche idempotenti, avrà la capacità di adattarsi ad entrambe le strutture.

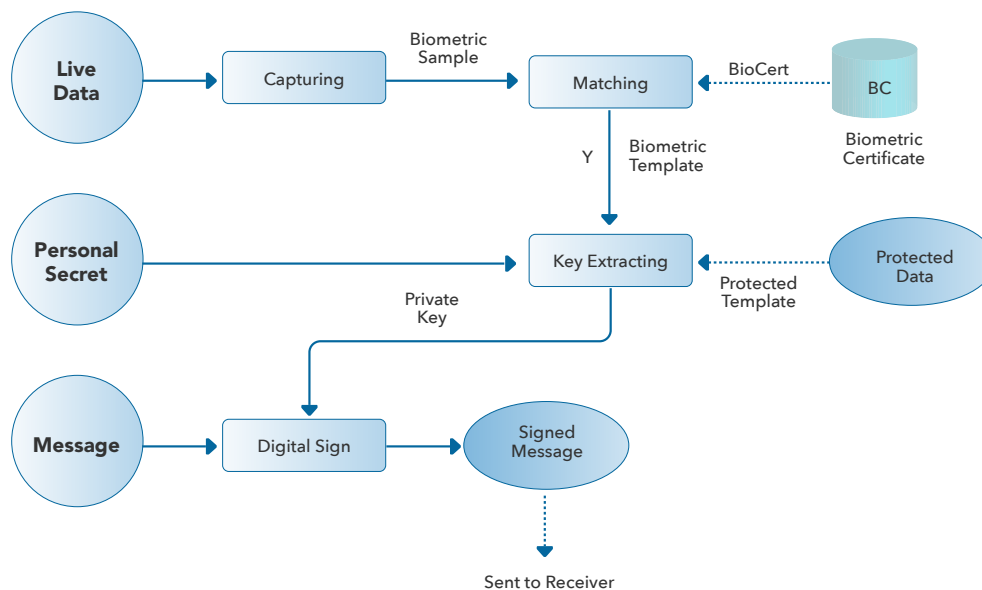
#### 5. Rollback (User Security)

La tecnologia di Multiversum permette, nel contesto di una transazione, di effettuare rollback di operazioni indesiderate, ovvero ripristinare uno stato precedente senza intaccare la credibilità della convalida della chain, ma implementando nuove transazioni programmatiche di ripristino dello Status desiderato.

Una volta valutata la fattibilità dal punto di vista della *Business Logic*, sarà considerata la possibilità di implementare nelle coins Versum tale funzionalità e ampliarlo con effetto retroattivo. Nella chain pubblica questa funzionalità non verrà implementata, ma *Use cases* proprietari che si rifanno alla tecnologia Multiversum saranno liberi di implementarla.

## 6. Freezable wallets (User Security)

Una volta valutata la fattibilità dal punto di vista della *Business Logic*, sarà studiata la possibilità di implementare il congelamento temporaneo delle coin Versum di un wallet in seguito ad attività illecite.

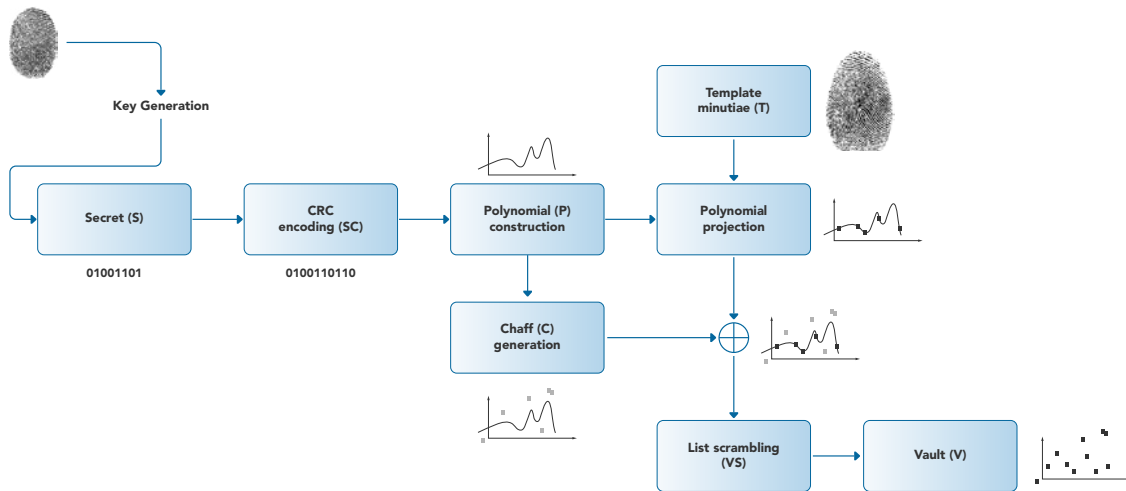


Biometric Digital Key Generation Framework

## 7. Integrazione dei dati biometrici come seed per l'Electronic Signature

Rifacendosi agli studi dei professori Je-Gyeong Jo, Jong-Won Seo e Hyung-Woo Lee della Hanshin University (Repubblica di Corea) e sintetizzati nella pubblicazione "Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint"<sup>13</sup>, si studierà la fattibilità dell'impiego di dati biometrici come impronte digitali, immagine dell'iride e firma grafometrica come sorgente della chiave crittografica asimmetrica a garanzia dell'identità del firmatario della transazione.

Per permettere l'utilizzo dei dati biometrici crittati in fase di contestazione giuridica, ne sarà valutata la sicurezza dell'inserimento. In ogni caso, questi dati saranno utilizzati nelle applicazioni per Android ed iOS.



Fuzzy Vault Scheme for Biometric Digital Key Protection

## 8. Interfaccia ERC23 (Interoperabilità con altre Blockchain)

Per garantire l'interoperabilità con altre chain, le coin Versum saranno sviluppate implementando l'interfaccia ERC23, versione evoluta e retrocompatibile di [ERC20](#)<sub>14</sub>.

```

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. Adattatori nativi off-chain per il proprio ERC20/ERC23 (Interoperabilità con altre Blockchain)

Per permettere l'entrata e l'uscita dei propri coins e tokens su altre chain non proprietarie, Multiversum svilupperà un adattatore nativo, accostandolo ad un buffer che ne regolerà l'ingresso e l'uscita dalla chain proprietaria.

## 10. Adattatori nativi off-chain per ERC20/ERC23 ospiti (Interoperabilità con altre Blockchain)

Per permettere l'entrata e l'uscita di coin e token non proprietari sulla sua chain, Multiversum svilupperà un adattatore nativo, accostandolo a molteplici buffer che ne regoleranno l'ingresso.



## Integrity

### 11. Proof of Integrity (Protocol Innovation)

Come alternativa alla *Proof of Work* e alla *Proof of Stake* nelle sue varie forme, Multiversum introduce la *Proof of Integrity*, ovvero un dispositivo di verifica crittografica della sincerità del codice del nodo compilato e dell'uniformità di risposta da parte della maggioranza dei nodi rispetto ad un *challenge seed* casuale, che, unito all'hash calcolato da un componente esterno (non decompilabile, protetto e comunicante con il software del nodo in un canale criptato) del software stesso, e ai dati della transazione, deve essere il medesimo in ogni singola transazione per tutti i nodi. Tale processo richiede una potenza di calcolo notevolmente inferiore ed evita gli sprechi tipici di altri sistemi (PoW, PoS, DPoS); fornisce inoltre una sicurezza maggiore e reale, non di tipo statistico o suppositivo basata sul modello del Consenso Bizantino, particolarmente vulnerabile in cluster di dimensioni ridotte.



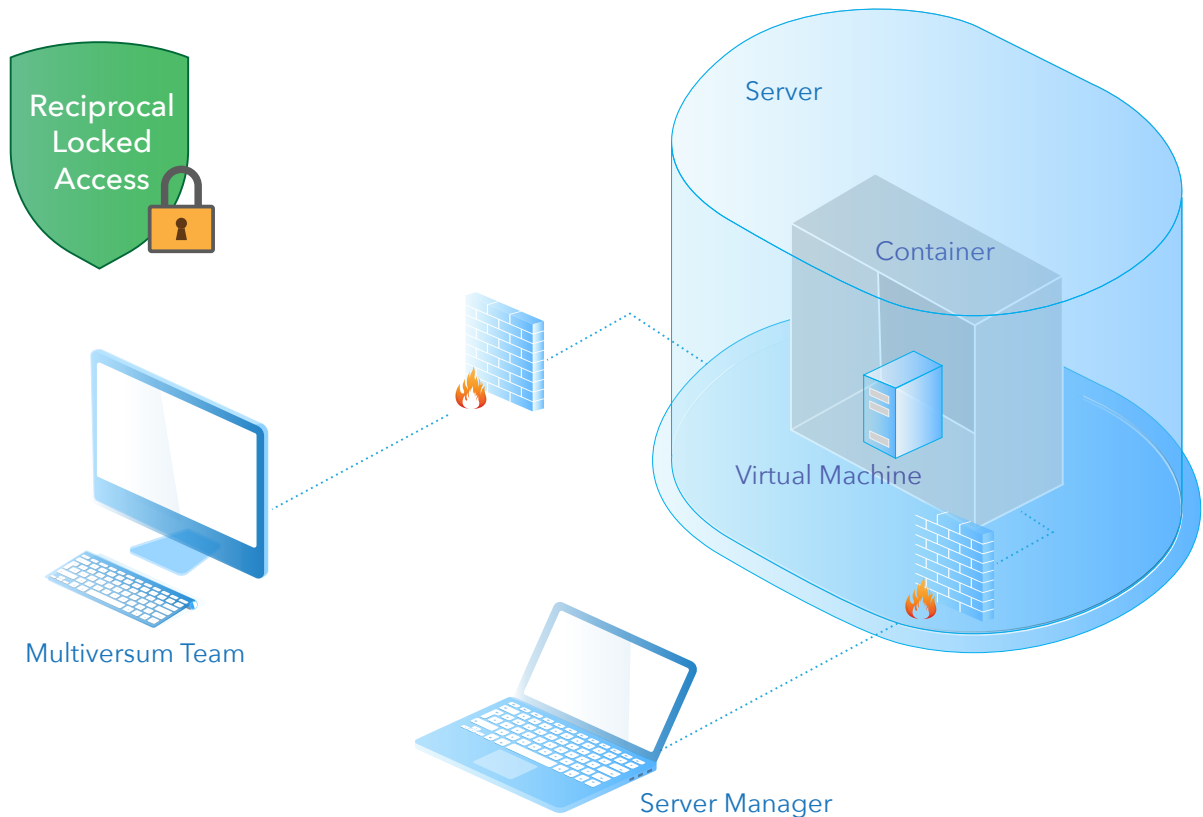
## Access Denied

### 12. Double Access Lock (Structural Security)

I nodi verranno distribuiti in Container Virtuali inaccessibili all'operatore della macchina Host poiché protetti da credenziali non disponibili all'operatore stesso. La sicurezza viene, pertanto, demandata alle *best practices* della Sicurezza Linux attraverso, ad esempio, il pacchetto [SeLinux<sub>15</sub>](#) e/o altri.

Allo stesso tempo, se anche qualcuno fosse in possesso delle credenziali della macchina Guest, non sarebbe comunque in grado di accedervi, non avendo accesso alla macchina host su cui il nodo gira.

Il nodo, pertanto, è sottoposto di fatto ad una duplice chiusura all'accesso.



### 13. Reverse Access Denial (Structural Security)

La doppia chiusura discussa al punto 12 comporta un effetto di reciproca preclusione all'accesso del nodo. Questo garantisce che i nodi non gestiti direttamente da Multiversum siano perfettamente autentici e inaccessibili a chiunque, fondamentalmente autonomi, e isolati da interventi umani esterni.

Oltre a quelli del Sistema Operativo e della Sicurezza, altri tre componenti fondamentali saranno distribuiti nel Container: il codice compilato del Server Multiversum, un certificato con chiave asimmetrica per l'autenticazione nel cluster Multiversum ed un componente già discusso al punto 11, responsabile del calcolo del challenge basato su hash del codice del server, del certificato, del challenge seed e dei dati della transazione.

Tale componente, inoltre, sarà l'unico accessibile all'operatore per verificare la sincerità del codice compilato del server che gira sulla macchina (restano da verificare i *downsides*).

Ulteriori funzionalità opzionali di sicurezza potranno essere implementate, come la possibilità di cambiare automaticamente la password di accesso al container, mentre viene compilato, con una password casuale sconosciuta, così da impedire l'accesso a chiunque. Tale meccanismo può essere implementato anche per il certificato di accesso al cluster.

#### 14. Reciprocal chain confirmation (Interoperabilità con altre blockchain)

Multiversum verificherà la fattibilità di un componente per registrare stati di altre chain in modo da certificarne lo stato e rafforzarne vicendevolmente la credibilità e la convalida delle transazioni (eventualmente a fronte di un token). Se reputata una soluzione desiderabile, tale componente verrà, quindi, implementato.

Multiversum desidera avvalersi della medesima possibilità di registrare periodicamente una transazione al fine di poter condividere la responsabilità della verifica di uno stato su altre chains. Fornirà un'interfaccia specializzata alla funzione e promuoverà la sua implementazione su nuove chain.

Tale componente si avvarrà di un componente *serverless* accessibile anche in un momento successivo alla compilazione del *container* per permettere l'aggiunta di adapters verso altre catene.

#### 15. Integrazione per Java, Spring and JavaScript

Considerata la sua vocazione all'uso in ambienti industriali, finanziari, legali, pubblici, amministrativi ed enterprise, Multiversum vuole implementare un ulteriore layer di astrazione sulle modalità alla base del suo funzionamento, offrendo interfacce di alto livello raccolte in librerie funzionali per Java, Javascript ed opzionalmente per altri linguaggi mainstream.



Saranno sviluppati anche moduli di integrazione a frameworks come Spring<sub>16</sub> in un progetto Spring Multiversum.

Tali librerie faciliteranno l'integrazione della tecnologia Multiversum in soluzioni proprietarie, sia nella realizzazione di chain private, che nel loro accesso alla MainNet ufficiale.

## 16. ACID model

Multiversum implementerà un modello definito ACID<sub>17</sub>. L'acronimo deriva dall'inglese **Atomicity, Consistency, Isolation, Durability** (Atomicità, Consistenza, Isolamento e Durabilità) ed indica le proprietà logiche che devono avere le transazioni.

Affinché le transazioni operino in modo corretto sui dati è necessario che i meccanismi che le implementano soddisfino queste quattro proprietà:

**atomicità** - la transazione è indivisibile nella sua esecuzione e la sua esecuzione deve essere o completa o nulla, non sono ammesse esecuzioni parziali;

**consistenza** - quando inizia una transazione, il database si trova in uno stato coerente, e quando la transazione termina il database deve essere in un altro stato coerente, ovvero non deve violare eventuali vincoli di integrità; perciò non devono verificarsi contraddizioni (inconsistenza) tra i dati archiviati nel DB;

**isolamento** - ogni transazione deve essere eseguita in modo isolato e indipendente dalle altre; l'eventuale fallimento di una transazione non deve interferire con altre transazioni in esecuzione;

**durabilità** - detta anche persistenza, si riferisce al fatto che, una volta richiesto un commit work da una transazione, i cambiamenti apportati non dovranno essere più persi, onde evitare che, nel lasso di tempo intercorso tra il momento in cui la base di dati si impegna a scrivere le modifiche e quello in cui le ha effettivamente scritte, si verifichino perdite di dati dovuti a malfunzionamenti.

## 17. Modello Transactional

Multiversum persisterà i dati collegati ad una transazione in un modello "transazionale"<sub>18</sub>, ovvero assicurandosi che ciascuno o nessuno dei dati sulle molteplici sottocatene coinvolte siano resi persistenti, al fine di garantire la coerenza di ogni transazione eseguita e la completezza dei dati.

## 18. Linguaggio SQL like

Per garantire facilità di composizione delle query, Multiversum si baserà su una sintassi simile a quella SQL<sub>19</sub>, usando un linguaggio simile a quello standard del settore. In questo modo la *learning curve* di chi si avvicina a questo componente per la prima volta risulta piuttosto dolce.

## 19. Funzionamento e Full Route Data Flux

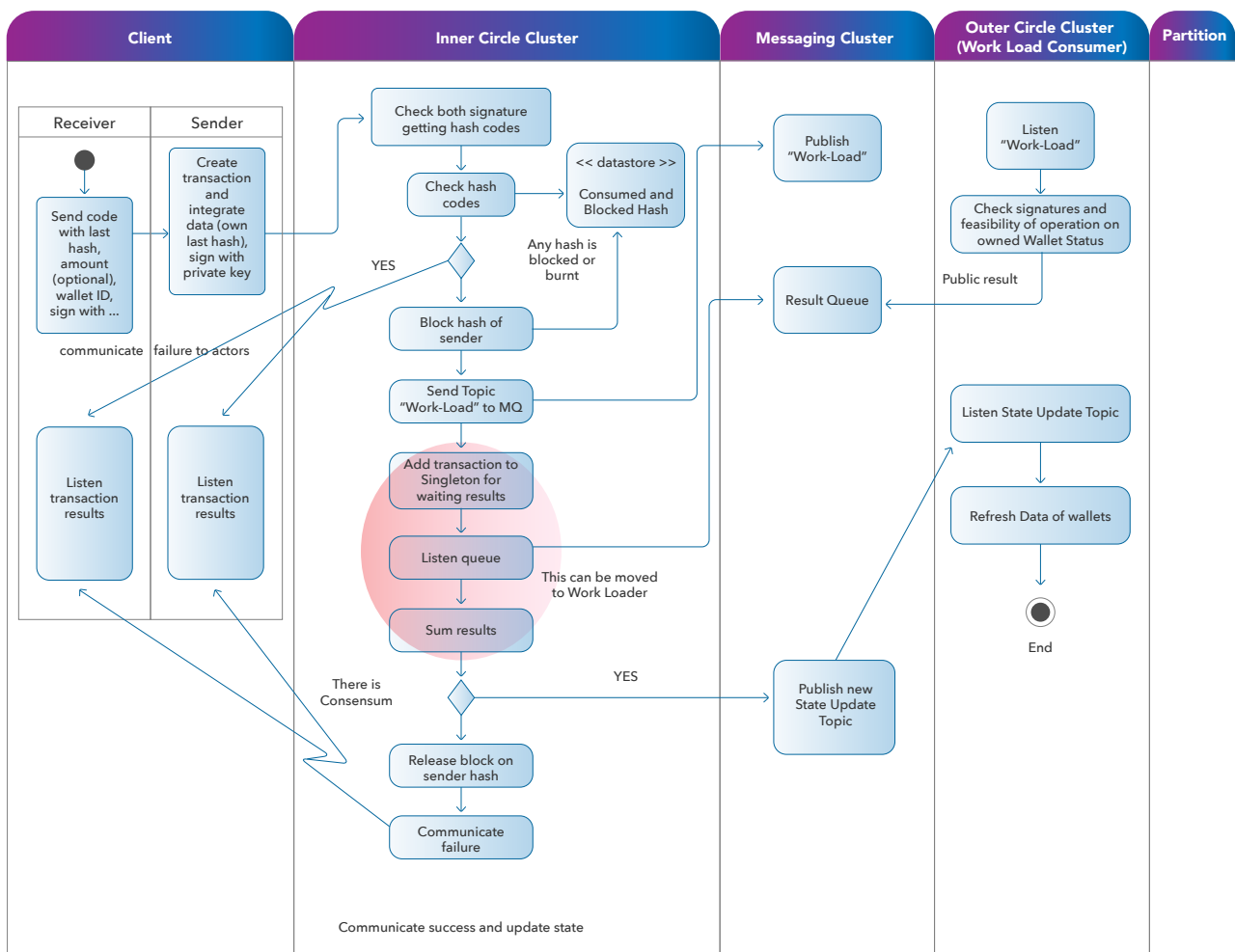
Il processo di accettazione, controllo, convalida e persistenza di una transazione avviene nella modalità schematizzata e semplificata di seguito.

Il *best case full route* segue questo iter:

La transazione viene inviata ad un client REST, completa dei dati necessari e firmata con chiave privata.

Il Client REST comunica la transazione al *Leader Node* del cluster di coordinamento: questo spartirà il lavoro internamente, grazie ad un protocollo proprietario, tra i nodi del cluster di coordinamento, che faranno un controllo preventivo della completezza di dati e firma, della disposizione di fondi per la transazione, della presenza di hash già usati, di stati non attuali dei wallets e di wallets o utenti bloccati.

Nel mentre, blocca temporaneamente in memoria volatile l'uso ulteriore dell'id del mit-



tente della transazione e completa alcuni dati, come transazione precedente alla quale agganciarsi, timestamp e hash precedente.

La transazione viene inviata ad una Topic Message Queue<sub>20</sub> con protocollo da definire (nel Pilot in AMQP, da verificare MQTT o altri) e distribuita parallelamente ai *Worker Nodes*.

I *Worker Nodes* verificano di essere coinvolti nel processarla (potrebbero non avere i dati necessari, essere già oberati di lavoro, o altro da appurare) e procedono alla creazione



del nuovo stato del wallet, recuperando gli hash correlati alle transazioni precedenti e aggiungendoli al record della transazione. Viene aggiunto anche il risultato della *Proof of Integrity*.

Infine, calcolano, sul complesso di dati, l'hash della transazione.

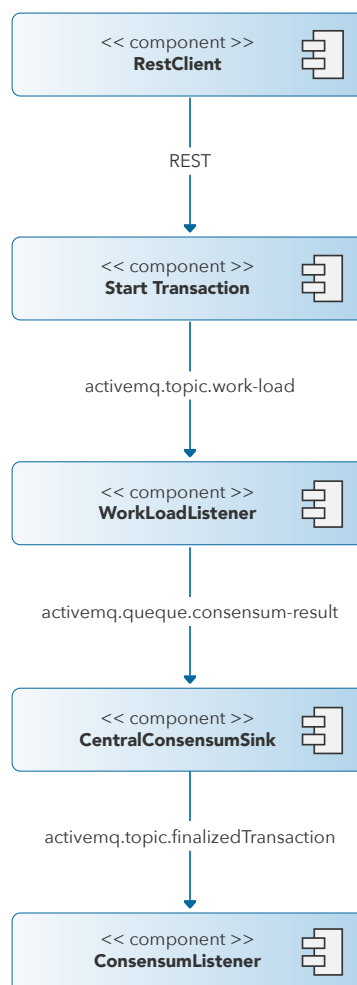
I *Worker Nodes* registrano nella memoria volatile questa transazione e mandano un voto ai nodi coordinatori attraverso una Message Queue che raccoglie tutti i voti.

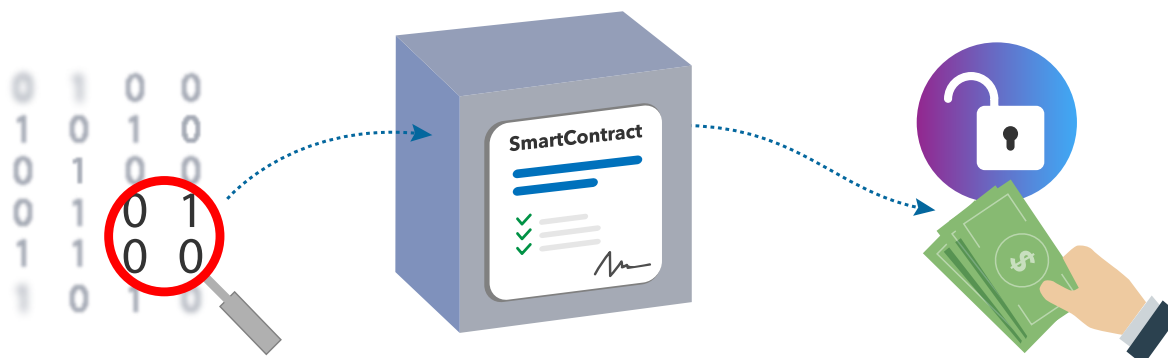
In caso voti e hash siano coerenti, i nodi di coordinamento scrivono in modo permanente sui propri supporti le transazioni e nuovi stati del wallet, bruciando gli hash degli stati precedenti e comunicando, con un ulteriore sistema di Topic Message Queue, che il voto è valido. A quel punto i *Worker Nodes* persistono l'intera operazione.

Fine del best case full route

## Logic data flux

*Detail of process flow*





## Smart Contracts

Multiversum ritiene necessario proporre al pubblico Smart Contracts<sub>21</sub> evoluti; contestualmente ha deciso che per il momento, salvo una futura modifica degli scopes della propria ricerca, non si porrà l'obiettivo di studiare questa possibilità, limitando la propria azione, con la modestia consona all'ambiente scientifico, ad individuare la soluzione Open Source migliore sul mercato e rifarsi ad essa per la sua inclusione nella propria soluzione (compatibilmente col modello di licenza del progetto al quale farà riferimento).

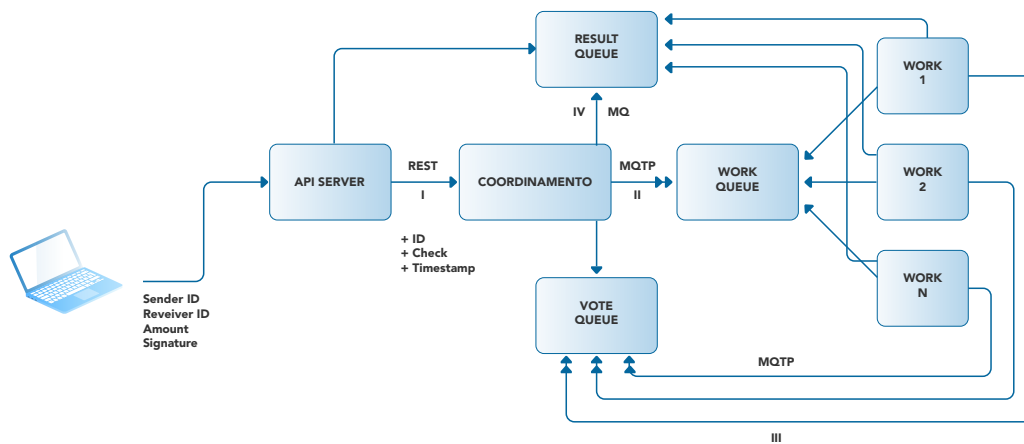
## Infrastructure

L'infrastruttura di Multiversum è stata progettata per garantire resilienza ed *high availability*. Tale obiettivo è stato raggiunto sviluppando cluster di nodi in grado di auto eleggere i propri membri a funzioni specifiche, in base alle caratteristiche tecniche di ciascun nodo, tra le quali:

- Capacità di calcolo
- Capacità di memoria
- Velocità di ping reciproca
- Completezza dei dati delle chain
- Affidabilità della macchina
- Dubbi sulla Proof of Integrity

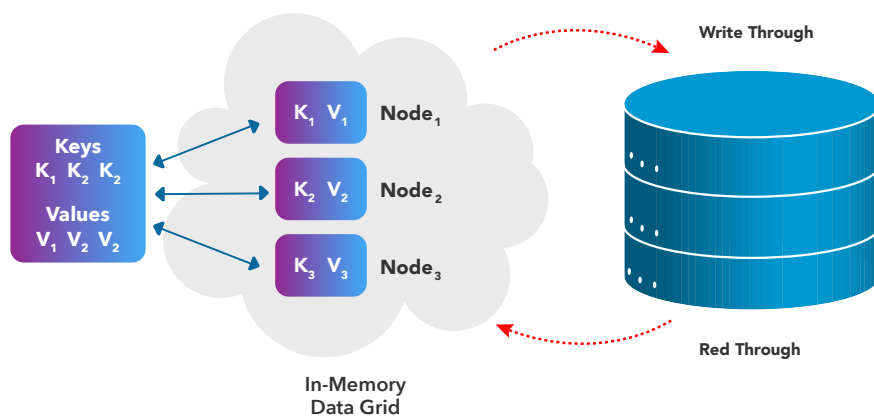
I nodi potranno avere una o più funzioni, tra le quali:

- Nodi Client
- Nodi di coordinazione
- Nodi di messaggistica
- Nodi di lavoro
- Nodi di persistenza
- Nodi di backup



Qualunque nodo in grado di dimostrare di possedere un certificato valido potrà registrarsi al cluster e ottenere una funzione.

In caso di crash di uno o più nodi il cluster sarà in grado di ridistribuire autonomamente gli incarichi, ottimizzando i ruoli.

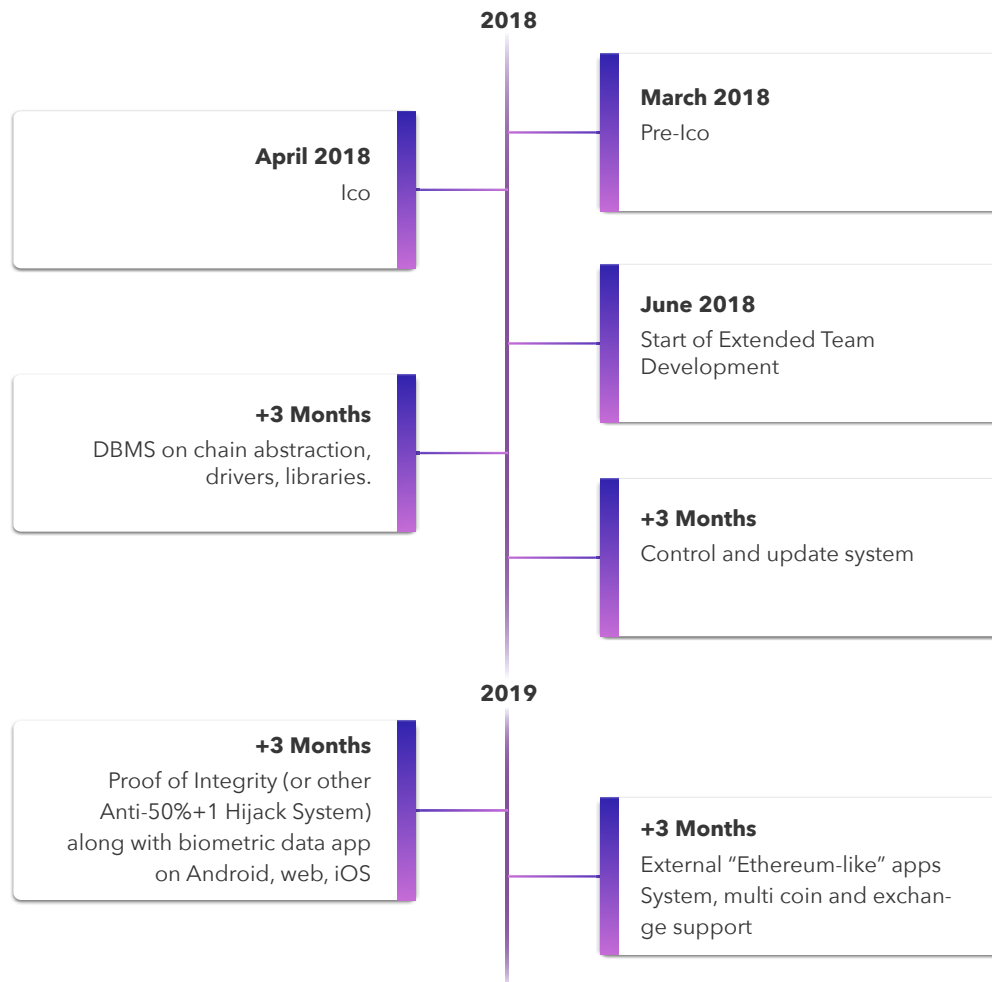


Saranno presenti componenti di cache condivisa intra JVM come memory database, che consentono meccanismi di *Read through*: la ricerca dei dati nella memoria volatile (se qui non presenti, in quella fisica) e, in seguito, il *Write Through*: l'accumulo dei dati nella memoria volatile e l'inserimento di massa in quella fisica, in modo da dover attendere il completamento dell'handshake e il data overhead soltanto una volta, ottenendo un'ottimizzazione delle prestazioni (nel caso di singole transazioni sarebbero stati eseguiti ripetutamente).

## Note sulla sicurezza

In corso di realizzazione verranno offerti "Hacker's bounties" a chi saprà trovare vulnerabilità ed eventualmente proporre un rimedio adeguato.

## Road Map Tecnica



L'implementazione completa richiederà circa un anno di lavoro per il deployment del server della Main Net per due team di sviluppatori, un architetto del Software, due GUI developer, due responsabili della sicurezza, un Business Architect.

Negli anni successivi lo sviluppo continuerà per permettere di avere un prodotto enterprise grade: da quel continuo sviluppo la coin Versum trarrà vantaggi di credibilità ed immagine.

La Main Net sarà completa di tutti i meccanismi di sicurezza e della logica del prodotto enterprise, ma non di quelli che rendono la tecnologia facilmente integrabile, in quanto non indispensabili per il suo utilizzo. Il software sarà pubblicato costantemente a supporto della credibilità del progetto, e la Test Net offrirà le nuove features disponibili appena queste saranno disponibili.

## References

- 1 [https://en.wikipedia.org/wiki/Scalability#Horizontal\\_and\\_vertical\\_scaling](https://en.wikipedia.org/wiki/Scalability#Horizontal_and_vertical_scaling)
- 2 <https://it.wikipedia.org/wiki/Proof-of-work>
- 3 <https://it.wikipedia.org/wiki/Proof-of-stake>
- 4 [https://en.wikipedia.org/wiki/Sybil\\_attack](https://en.wikipedia.org/wiki/Sybil_attack)
- 5 <https://en.bitcoin.it/wiki/Difficulty>
- 6 [https://it.wikipedia.org/wiki/Metodologia\\_agile](https://it.wikipedia.org/wiki/Metodologia_agile)
- 7 [https://en.wikipedia.org/wiki/Scope\\_\(project\\_management\)](https://en.wikipedia.org/wiki/Scope_(project_management))
- 8 [https://en.wikipedia.org/wiki/Persistence\\_\(computer\\_science\)](https://en.wikipedia.org/wiki/Persistence_(computer_science))
- 9 [https://en.wikipedia.org/wiki/High-availability\\_cluster](https://en.wikipedia.org/wiki/High-availability_cluster)
- 10 [https://en.wikipedia.org/wiki/Single\\_point\\_of\\_failure](https://en.wikipedia.org/wiki/Single_point_of_failure)
- 11 <https://en.wikipedia.org/wiki/Microservices>
- 12 [https://en.wikipedia.org/wiki/Serverless\\_computing](https://en.wikipedia.org/wiki/Serverless_computing)
- 13 <http://goo.gl/CVBzJd>
- 14 <https://en.wikipedia.org/wiki/ERC20>
- 15 [https://it.wikipedia.org/wiki/Security-Enhanced\\_Linux](https://it.wikipedia.org/wiki/Security-Enhanced_Linux)
- 16 [https://it.wikipedia.org/wiki/Spring\\_framework](https://it.wikipedia.org/wiki/Spring_framework)
- 17 <https://en.wikipedia.org/wiki/ACID>
- 18 [https://en.wikipedia.org/wiki/Models\\_of\\_communication#Transactional\\_Model](https://en.wikipedia.org/wiki/Models_of_communication#Transactional_Model)
- 19 <https://en.wikipedia.org/wiki/SQL>
- 20 [https://en.wikipedia.org/wiki/Message\\_queue#Standards\\_and\\_protocols](https://en.wikipedia.org/wiki/Message_queue#Standards_and_protocols)
- 21 [https://en.wikipedia.org/wiki/Smart\\_contract](https://en.wikipedia.org/wiki/Smart_contract)

# Marketing Strategy

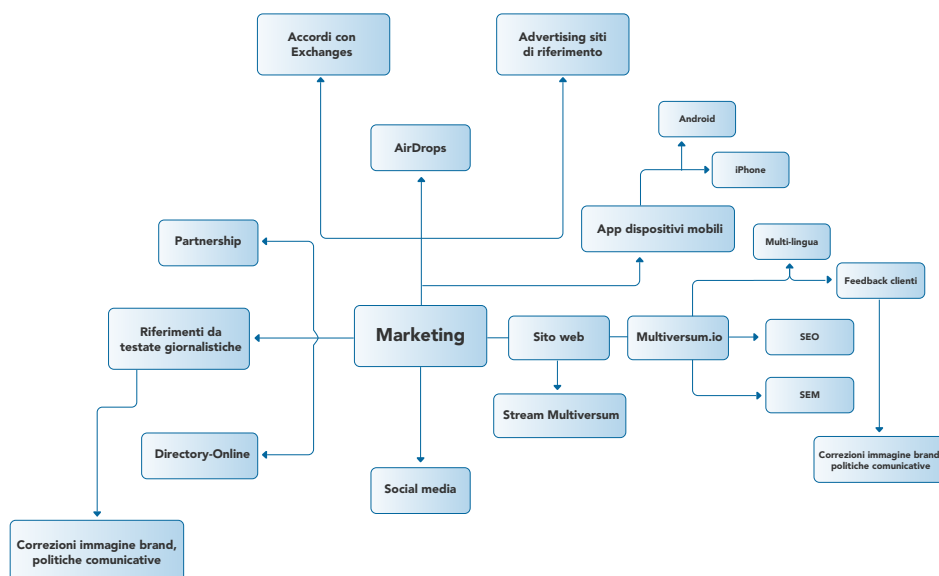
Abbiamo focalizzato la pianificazione dell'intera organizzazione del marketing partendo da un contesto generale per poter poi effettuare un focus su aspetti specifici.

Comprenderemo tutte quelle attività che permetteranno il conseguimento degli obiettivi, adottando un approccio globale per l'intera organizzazione (dalla definizione della missione aziendale all'individuazione della strategia più appropriata).

La strategia aziendale sarà il riflesso di un ambiente in continua evoluzione e la missione dell'impresa sarà quella di creare valore per gli stakeholder, assicurando equilibrio tra logiche gestionali di breve e lungo termine.

Le 4 componenti del piano sono:

- Missione aziendale
- Strategie aziendali
- Obiettivi aziendali
- Portafoglio attività aziendali



Uno degli strumenti principali sarà il **Social Media Marketing** che è l'insieme delle attività condotte sui social network per aumentare la consapevolezza del brand, identificare potenziali consumatori, generare contatti e costruire relazioni significative con i clienti.

Realizzeremo diverse azioni che sono parte di un unico piano strategico, partendo dalla gestione e il monitoraggio dei canali utilizzando strumenti dedicati e il rafforzamento della community attraverso la cura quotidiana dei contenuti e l'interazione, fino all'analisi dei risultati ottenuti e la verifica della tattica messa in campo.

Ciascuna di esse si rispecchia nelle competenze dei nostri Social Media Strategists: la pianificazione strategica, la definizione e produzione della linea editoriale, l'interazione e il supporto con il mercato e l'analisi dei risultati.

**Gli strati di elementi che avvolgono gli universi sono ognuno dieci volte più spesso del precedente, tutti gli universi, raggruppati insieme, appaiono come atomi in una immensa combinazione.**

Bhagavata Purana 3.11.41



MULTIVERSUM

HERE TO STAY