

# MULTIVERSUM

HERE TO STAY

**WHITE PAPER v 1.0.6**

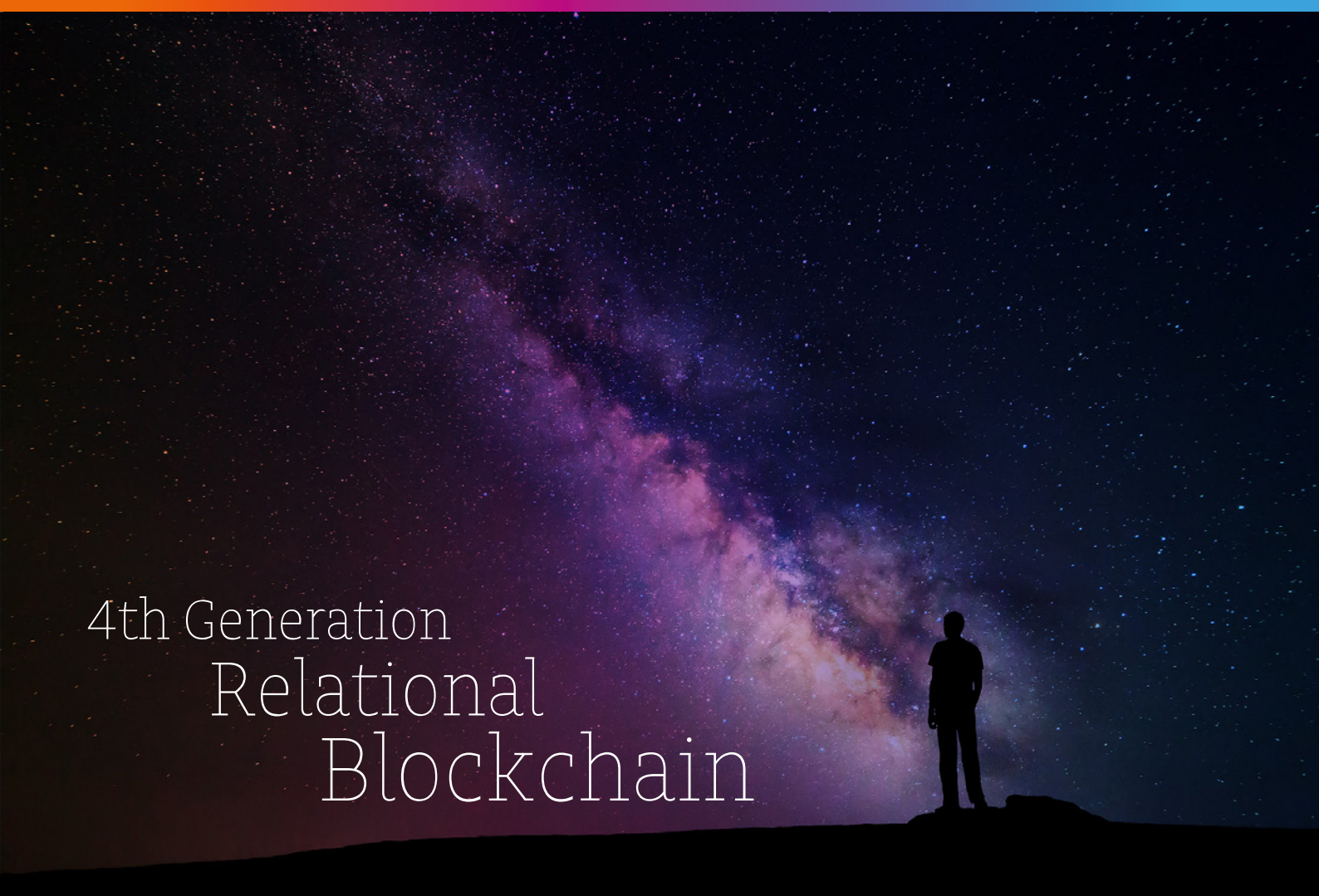
Business | Tehnička

Srpski

19.02.2018

Autori: Multiversum Team

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



4th Generation  
Relational  
Blockchain



**Postoje beskonačni svemiri  
osim našega, iako su  
beskonačno prošireni, oni se  
kreću poput atoma u vama.**

Bhagavata Purana 6.16.37

# Identitet i misija Multiversuma

Prva generacija Blockchaina se sastoji od prvih moneta kao što je Bitcoin, koje se temelje na dokazu o radu i sa svojim raznim duplikatima i forkovima.

Druga generacija Bitcoina su više heterogene, koja se baziraju na korištenju tokena kao što je Ethereum i njegov sustav rješenja.

Ove dvije kategorije karakterizira vrlo niska energetska učinkovitost i smanjeni broj transakcija.

Trećoj generaciji Bitcoina pripadaju oni BC koji su probali da ponude odgovore na sporost transakcija i na nemogućnost nadogradivosti pomoću raznih mehanizama: Proof of Stake, off chain route, graphchain, potpuna centralizacija ili djelomična.

Četvrta generacija, umjesto svih tih mehanizama, nudi se da daje odgovore na sporost sistema; u međuvremenu si postavlja ciljeve u upotrebi na području poslovanja tvrtke, na što se malo obrača jedan lanac podataka koji je neorganiziran i koji treba sisteme pohrane podataka koji su složeni u povezane tablice (kao što su relacijske baze podataka) ali u isto vrijeme u kojem se podaci potvrđuju i pojačavaju sa tehnikom Blockchaina. Istovremeno rečeno to je pokušaj da se ova tehnologija pretvori u pravi primarni produktivni rad. Multiversum nudi organizirano upravljanje složenim podacima umjesto jednostavnoga slijeda podataka, raspodjeljivost lanaca i ponovno povezivanje kako bi se omogućio paralelnost, i provjera izvedivosti *Proof of Integrity* (kriptografski dokaz kod poslužitelja) umjesto *Proof of Work*.

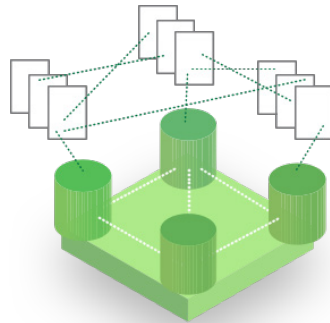
Osim toga istovremeno se kombiniraju interoperabilnost sa drugim lancima (hosting na našem lancu drugih lancaca, kovanica žetona i obrnuto) i uslugu javnoga beležnika koji služi kao validacija procesa.

U međuvremenu sigurno ćemo usvojiti neke od rešenja koja su već ponuđena i usvojena od naših kolega.

# Multiversum

## Četvrta generacija relacijskog Blockchaina

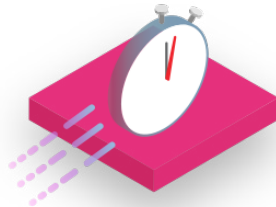
Zašto je Multiversum Blockchain 4.0?



### Relacijski Blockchain

Lanac nove generacije, koji će preći da može upravljati samo jedan tip podataka u linearnom načinu u više vrsti podataka, koji su međusobno povezani između sebe preko identifikacije, u jednoj multistrukturanoj dimenziji.

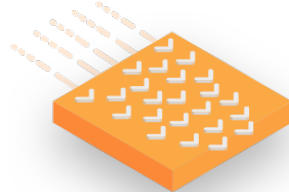
< 0,2 sec



### Brzina transakcije

U manje od 0,2 sekundi investicijski fondovi se mogu prenjeti sa jednoga novčanika na drugi ispunjavajući sve korake koji potvrđuju sigurnost. Lanac koji je jedan od najbržih na svijetu.

64000 tps → ∞



### Količina tranzakcija

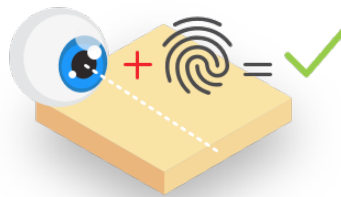
Do 64000 TPS na serveru od 64 kora (1000 TPS za kor), podrška za sisteme koji imaju više od 64 kora – skalabilnost bez granica.

POI



## Ekstremna sigurnost u transakciji

Neće postojati više koncept POS (Proof of Stake – Dokaz o udjelu):  
Biti će zamjenjen sa POI (Proof of Integrity – Dokaz integriteta).



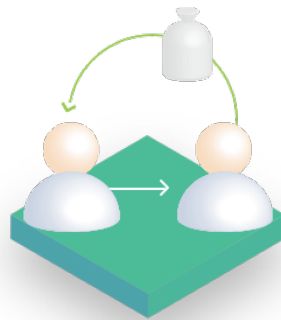
## Novčanik nove generacije / Biometrijski ulaz

Ekstremna sigurnost pri pristupu novčaniku i slanju fondova preko  
biometrijskog ulaza.



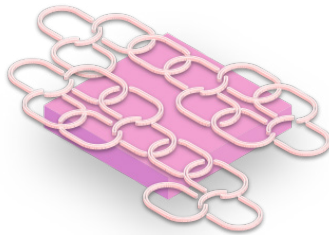
## Eco-Friendly

Jedna transakcija će imati beznačajne troškove i utjecaj na okoliš je gotovo ravan nuli.



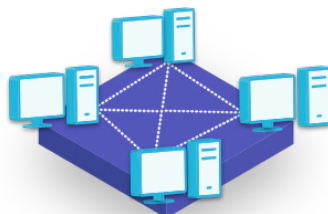
## Rollback - povratak na staro

Sistem povratka na staro je kao opcija I bit će dostupan u rješenjima ad-hoc koji će imati koristi od ove funkcije.



## Podjeljivi čvorovi

Optimizacija radnoga opterećenja sa podjelom sredstava između dostupnih čvorova zahvaljujući mogućnosti podjele glavnoga čvora na manje sub-lance.



## Smještaj čvorova za oporavak

Tvrtka Multiversum je smjestila periferijske čvorove Global Disaster Recovery (Globalne Katastrofalne Oporavke) na različite kontinente.

# Predstavljanje publici

## Koncept Multiversuma i njegova upotreba na svetskoj razini

Multiversum je tehnologija koja, mjenjajući one aspekte koji se odnose na upornosti podataka u Blockchainu kroz samoprovjeru podataka i distribuciju podataka, koji su organizirani zajedno u zajednici i povezani u simboličkoj vezi, revolucionira tradicionalne granice, što dovodi zapravo novoj generaciji: **Blockchain 4.0**.

Ova tehnologija temelji se na decentraliziranom i distribuiranom sustavu usklađivanja dosljednih transakcija i koje se automatski potvrđuju: Multiversum BC. Aktualni Blockchainovi se temelje na sekvenciji transakcija koje predstavljaju jedan tip podataka: ili se odnose na samoj transakciji ili na više pratećih lanaca i ne čvrsto povezanih jedni sa drugima, pri čemu su podatci organizirani u konceptijskim blobovima i koji su povezani jedni s drugima sa poteškoćama i sa ogromnim računarskim troškovima. Multiversum međutim dopušta kripto relacijske baze podataka (jedno rješenje za pohranu podataka koja je napredna i organizirana) koji omogućuje da imaju ne samo jednu vrstu podataka, ma i niz podataka prikupljenih u tablicama u složenoj strukturi podataka, povezanih jedni s drugima putem ID-a.

Svaki ID, u vrijeme kada se promjeni jedan status, imati će vlastiti pod-lanac koji će pokazati već kod ovjerenenog čvora, te će ponovno spojiti za dobivanje garancije sa ostatkom lanca.

Multiversum je stoga napredna Blockchain tehnologija koja nudi jedinstvene značajke za rješavanje ovih problema u panorami kripto valjanosti i distribucije i moći će se koristiti u bilo kojem okruženju: administrativne, industrijska, financijske i vladi.

Jedan od glavnih ciljeva Multiversuma je ponuditi na tržište, u bilo koje vrijeme proizvod koji je najviše razvijen na raspolaganju: to će biti moguće uz pomoć metodologije koja se zove AGILE.

Ovaj pristup će nam omogućit da razumijemo zahtjeve tržišta, za vrijeme i nakon faze razvoja, i provesti ih progresivno, dolazeći do objavljivanja Main Neta koji će biti najrazvijeniji i najkompletniji dostupan na tržištu.

Ova tehnologija razvoja omogućuje nam da ponudimo proizvod koji je najmoderniji i najaktualniji na tržištu.

## Brzina i tehnologija

Jaka točka ove tehnologije je svakako brzina, zbog mogućnosti obrade različitih operacija u paraleli.

Ova karakteristika omogućuje da imaju savršen horizontalnu skalabilnost, odnosno mogućnost da se može neograničeno povećati kapacitet obrade transakcija, dodavajući nove procesore umjesto zamjene postojećih, što svaki novi čvor čini učinkovitim za poboljšanje učinkovitost cjelokupnog sistema.

## Horizontalna skalabilnost

Multiversum može uživati u dvije vrlo važne značajke koje ga čine jako učinkovitim:

- Lanac je u stanju optimizirati svoju strukturu podjele djeleći se automatski u skladu sa zahtjevima i resursima za protok podataka, djeleći tako posao clustera na optimalan način između čvorova raspoređenih za obradu. Ova podjela se može izvršavati do beskonačnosti sve do normalizacije opterećenja rada, kada, uvijek na samostalan način čvor se vrati da bude jedan. Sve to zahvaljujući uređaju koji omogućuje da svaki prsten može potvrditi dva različita lanca od dva prijašnja različita prstena.
- Prilika za obavljanje podataka (load shading) : tehnika koja omogućuje distribuciju podataka na više čvorova.

Zamislimo da imamo niz ABC podataka i tri Cluster čvora, imat ćemo podjelu podataka na sljedeći način:

- AB
- BC
- CA

Ovakva podjela omogućuje veću brzinu obrade transakcija koje će tražiti podatke za korištenje samo u čvorovima koji ih sadrže, optimizirajući tako svaki protok podataka.

Još jedna prisutna i važna značajka se zove High Availability: mogućnost da se temelji na vrsti klustera koji osigurava kontinuitet usluga, čak i u slučaju prekida pojedinih čvorova u mreži.

Koristeći prijašnji primjer (čvorovi a, B i C), ako je C prekinut, čvorovi A i B ostaju kompletno operativni, omogućujući kontinuitet usluge, bez ikakvog gubitka podataka sve do kada budu operativni do najmanje 50% + 1 od kompletnih čvorova.

Kluster, u ovoj situaciji, komunicirajući sa svim čvorovima, automatski će organizirati distribuciju podataka do potpunog oporavka.



## Okoliš

Multiversum je ekološki, jer ima za cilj uklanjanje mininga, spreka snage u računanju i ogromne energije, koja podupire Proof of Work (dokaz o radu), u korist novog koncepta, Proof of integrity (dokaz o integritetu): protokol koji provjerava istinitost i autentičnost softvera koji je potreban da riješi bilo koju upornost transakcije.

## Upravljanje podacima: relacijska databasa

Multiversum, sa svojim kripto relacijskom bazom podataka, može lako strukturirati podatke bez ijednoga ograničenja vrsta veza.

Svaki novčanik će imati niz stanja (States), te će biti spojeni na osobu (korisnika); Svaki novi mjenjački prsten od stanja novčanika će uključivati dvije stvari:

- prijašnje stanje, kako bi imali vrednovanje ranijeg čina;
- link koji je povezan na najnovije transakcije (ili zadnju kariku u glavnom lancu), za koji će se znati od kuda dolazi novi prsten u u mjenjačkoj funkciji.

Kada dođe do te promjene biti će dodana transakcije uređivanja i, uz to, pridružit će se prsten promjenjenog stanja, koji će pokazati podrijetlo ovoga povezivanja i promjene stanja.

Nova transakcija će nasljediti haša (Hash) : jedan od prstena stanja, jedan prsten od prijašnje transakcije.

Na ovaj način sve operacije potvrđuju one prijašnje koje su povezane sa samom transakcijom.

Ovaj sustav je kompleksan kao što je napredan, te će dopustiti dograđivanje softwera na našoj tehnologiji garantirajući institucionalnu difuziju, vladinu difuziju, industrijsku i finansijsku difuziju, dovodeći sav svijet Blockchaina na viši stupanj.

## U zaključku...

Takav pristup omogućit će nam da razumijemo zahtjeve tržišta za vrijeme i nakon faze razvoja i progresivnu implementaciju koja će postepeno doći do objavljivanja MainNeta (Glavne mreže) koji je više razvijen i potpuno dostupan.

Bit će tako u tom momentu i u budućnosti.

Multiversum će odmah objaviti Pilot od Blockchaina (Probni Blockchain) koji će funkcionirati i APP Vlasnički Novčanik u Beta verziji. U roku od šest mjeseci proizvodi će biti ažurirani svakodnevno prema potrebama.

Niti jedan Blockchain koji je kasniji od BTC-a, na izlasku na tržište, bi se mogao pohvaliti tako velikim razvojem. Vrijednost coina i tokena može imati samo koristi od toga.

# Analiza State of Art Blockchainova

Trenutačno glavni čimbenici "blockchain fenomena" karakteriziraju znatna robustnost u smislu sigurnosti.

U tom kontekstu, takva sigurnost vodi do mogućnosti ogromnih računanja, zagađivanja, neprihvatljivih transakcija i sporosti koja je u nemogućnosti da predstavlja trenutni tehnološki napredak, čime utječe na mogućnost da daju tehnološki vjerodostojane odgovore za moderne finacijske i trgovačke slučajeve.

Takva je sporost uzrokovana nemogućnošću postizanja vodoravne skalabilnosti<sup>1</sup>, što je povećanje računalnih kapaciteta dobivenih jednostavnim dodavanjem procesora umjesto da ih zamijeni bržim verzijama.

Drugi razlog slabe učinkovitosti se nalazi u sigurnosnom mehanizmu aktualnih Blockchaina koji se temelje na Proof of Work<sub>2</sub> (Dokazu o radu) i, rjeđe korištenih Proof of Stake<sub>3</sub>, što uklanja rizik od gubitka kontrole nad većinom clustera zbog Sybil Attacks<sub>4</sub> zahtijevajući od čvorova umjetno stvaranje visokih računalnih kapaciteta, čineći ih u nemogućnost neselektivnog stvaranja kroz povećanje poteškoća<sub>5</sub>. Nadalje, aktualni Blockchainovi su jednostavne sekvence promjena pojedinih entiteta podataka: obnova aktualnih stanja, koja zahtijevaju skeniranje cijelog lanca, i time čineći daljnje usporavanje sustava i gubitak resursa. Ova postavka čini neadekvatnim korištenje tehnologije blockchaina u industrijskom i znanstvenom kontekstu, okruženja u kojima su strukture podataka izrazito složene.

Sigurnost koju pružaju trenutačni Blockchain uređaji odnosi se samo na podatke, ali se ne odnosi na korisnika: na primjer, nemoguće je dobiti coins ili tokene koji su biti neopravdano oduzeti iako su individuירani u lancima -chainovima ili blokirati račune uključene u protuzakonite aktivnosti. Konačni problem je ukupni nedostatak homogenosti i nedostatka komunikacije u panorami različitih krypto valuta: svaki Blockchain, koji postoji u svom vlastitom zasebnom svemiru, rezultira nesposoban da se poveže d drugima.

## Metodologija AGILE

Multiversum namjerava koristiti tehniku AGILE, dtijekom razvoja proizvoda. Ova tehnika pretpostavlja drastično smanjenje početnog dizajna, u korist valorizacije iskustava dobivenih tijekom rada, koje ističu mogućnosti i opasnosti koje su inače teško identificirati *ex ante*, nagrađivajući *Best Practices* (najbolje prakse) i kažnjavanje *Ways of Working* neadekvatnog (načina rada).

AGILE metodologija je Industrijski standard za proizvodnju softvera i sugerira razvojnim programerima, vlasnicima proizvoda i investitorima razmatranje opsega projekta – scope, kako bi se prilagodila promjenama tržišnih potreba. Štoviše, u sektoru koji brzo i stalno evolviraju, poput softverskog sektora, ponuditi na tržište nakon određenog razdoblja koji tipično traje šest mjeseci studija i godinu dana provedbe, proizvod rođen za odgovor prema potrebama 18 mjeseci prije, tako da bi to značilo nuditi zastarjelo rješenje, koje rješava probleme koji nisu aktualni, vjerojatno već prevladani od strane konkurenata i ne mogu dati odgovore na nove izazove. AGILE, naprotiv, omogućuje da se proizvod ponudi na tržište što je inovativnije u momentu kada je projekt isporučen.

# 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)

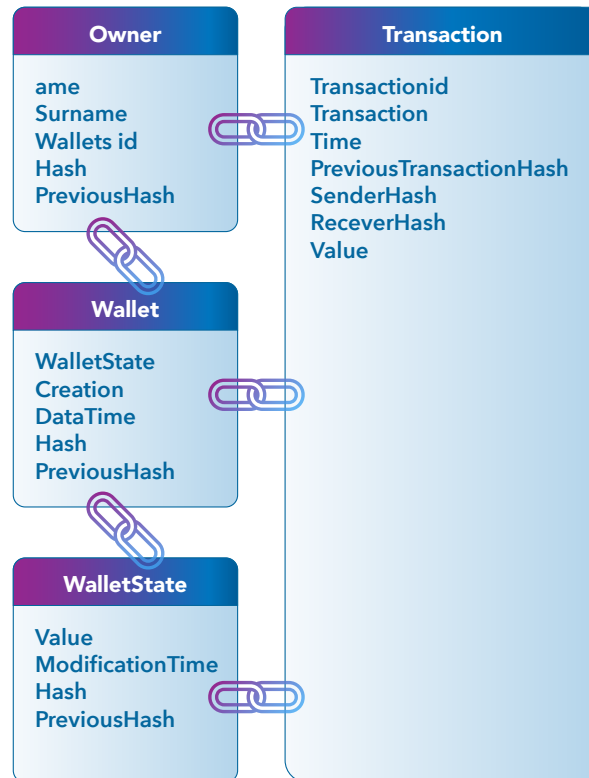
### **ERC23**

(Interoperability with other BC)

# Misija Multiversuma

Multiversum ima za cilj istražiti rješenja koja omogućuju generacijski napredak u svijetu blockchaina, *Unique Selling Points*, i postavlja si sljedeće ciljeve:

1. Realizacija Crypto relacijskog DB sa samo provjerom valjanosti kompleksne strukture podataka
2. Lanci koji se mogu duplirati i spajati prema potrebnoj količini posla (Parallel Work)
3. Sharding podataka (Parallel Work)
4. Mikrostrukturalna struktura i napredna ponuda API
5. Rollback (Sigurnost korisnika)
6. Freezable wallets (Sigurnost korisnika)
7. Integracija biometrijskih podataka kao seed za elektronički potpis
8. Sučelje ERC23 (mogućnost povezivanja sa drugim Blockchainovima)
9. Nativni izvanredni adapter za vlastiti ERC20/ERC23 (mogućnost povezivanja sa drugim Blockchainovima)
10. Nativni izvanredni adapter za posjetitelje ERC20/ERC23 (mogućnost povezivanja sa drugim Blockchainovima)
11. Proof of Integrity (Protok inovacije)
12. Double Access Lock (strukturna sigurnost)
13. Reverse Access Denial (strukturna sigurnost)
14. Recipročna potvrda lanca (mogućnost povezivanja sa drugim Blockchainovima)
15. Integracija sa Javom, Springom i JavaScriptom
16. ACID model
17. Transakcijski model
18. Jezik kao SQL like
19. Funkcioniranje i Full Route Data Flux



## 1. Realizacija Crypto relacijskog DB sa samo provjerom valjanosti kompleksne strukture podataka

Multiversum ima snažan odaziv za korištenje u industrijskim i institucionalnim kontekstima, javnosti i poduzećima: okruženja koja zahtijevaju složene strukture podataka, koje su u nemogućnosti da učinkovito predstavljaju i normaliziraju jednostavnim lancem.

Ovaj odaziv se očituje tako što želi biti prvi glas kripto relacijske baze podataka koja se ponuđuje na tržište, distribuira i opcionalno decentralizira. Ovaj je rekord postignut počevši od konceptualizacije lančanih entiteta. Takvi entiteti dopuštaju implementirati sučelje sposobno za definiranje metoda potrebnih da bi podaci mogli biti umetnuti kao prsten u blok-lanac.

U konceptualnom modelu bit će primarni lanac na koji će se lanci povezati sekundarni predstavnici različitih vrsta, koji zauzvrat predstavljaju zapise tablice.

Ti entiteti će se povezati dalje sa svojim posljednjim postojanjem, i poslije nužne promjene će se ujediniti u zadnji prsten glavnoga lanca koji spaja dva sub-lanca.

"Lančano" sučelje pretpostavlja: registraciju višestrukih prstenova iz kojih ih će se izvući novi prstenovi, registracija višestrukih prstenova koji proizlaze iz jednoga, i provjeru i potvrđivanje takvih podataka, koji djeluje uvozom haševa već prije spomenutih prstenova u haš koji se trenutno koristi.

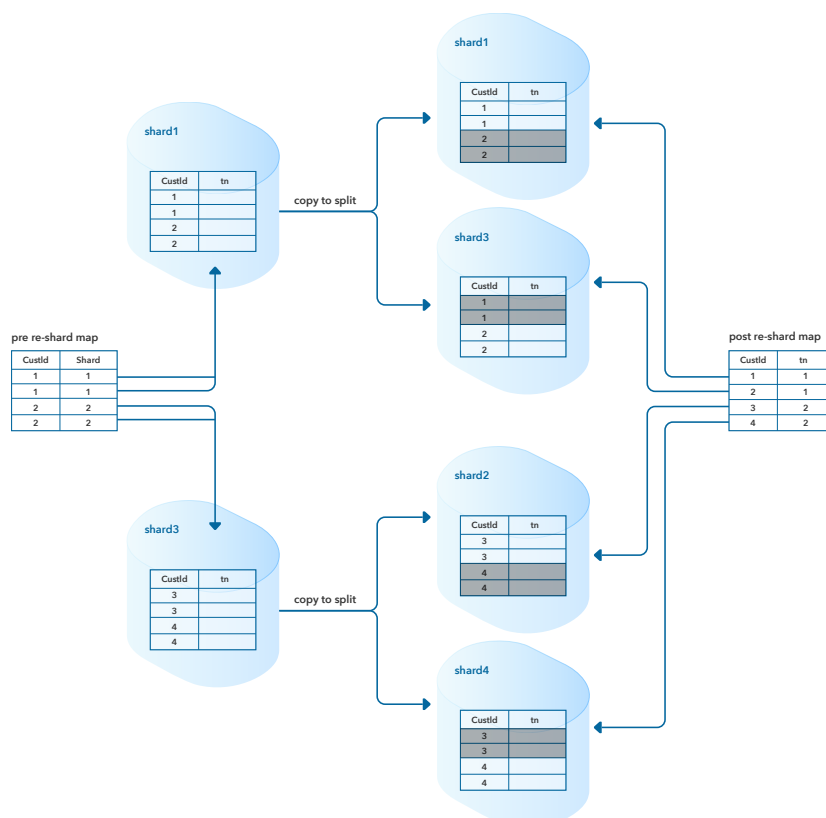
U provedbi Multiversum tehnologije za Versum coins, lančani entiteti koji će koegzistirati na lancu, pripadati će u četiri tablice: Korisnik, Novčanik, Wallet State i transakcija, koji će se međusobno povezati i potvrđivati.

## 2. Lanci koji se mogu duplirati I spajati prema potrebnoj količini posla (Parallel Work)

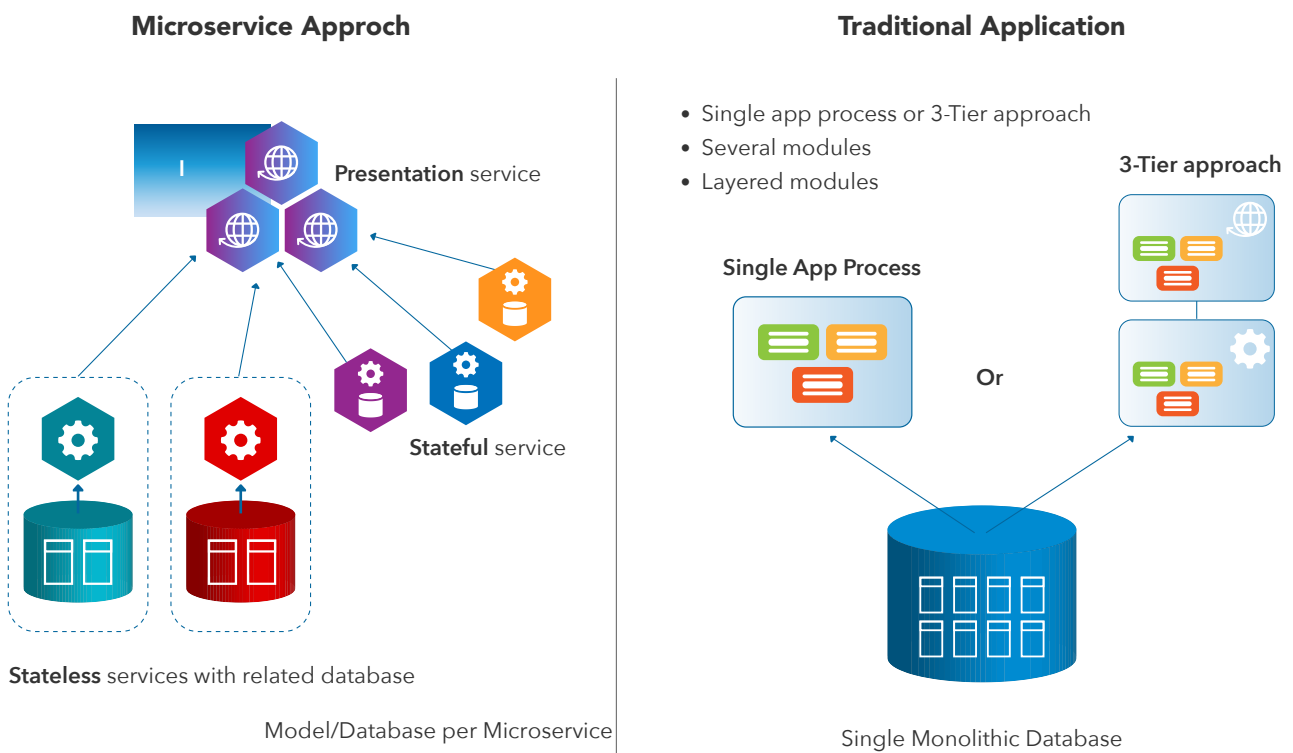
Sposobnost za izvođenje višestrukih prstenova od jednoga i njihovo povezivanje potječe od upotrebe analizatora radnog opterećenja koji, u prisutnosti velikog broja zahtjeva izvršenja, će izvješćivat klasteru potrebu podjele (bez vremenskih granica i vremena, ako je potrebno) primarni lanac transakcija u dva sekundarna lanca, a na kraju isto će omogućiti ponovno povezivanje s većim brojem pod-lanaca koji su bili prije generirani. Ovaj mehanizam omogućava paralelni rad, i dalje pruža zaštitu dnevnka transakcija.

## 3. Sharding podataka (Parallel Work)

Svaki čvor može imati u memoriji sve podatke blockchaina ili samo dio njih. Ako se pojavi potreba za paralelizacijom podataka, koordinirajući čvorovi će utvrditi metode podjele na takav način da optimiziraju distribuciju s obzirom na parametre paralelizacije izračuna i *High Availability*, (visoke dostupnosti), osiguravajući (čak 50% +1 čvorova ostat će na mreži) dostupnost podataka čak i u slučaju trenutnog nestanka clustera upornosti. Ti čvorovi, u fazi nakon djelomičnog pada klastera, moći će se redistribuirati i samostalno reorganizirati svoje podatke, tako da je u stanju ponovno riješiti daljnji djelomični sudar klastera što je prije moguće.



Uređaji opisani u ovoj točki I u prethodnoj dopuštaju mogućnost paralelnog rada dakle: horizontalna skalabilnost, sigurnost, visoka dostupnost, *high availability*, otpornost sustava, nedostatak *single point of failure*<sub>10</sub> (jedinственe točke neuspjeha) i *self disaster recovery* (samostalni oporavak).



#### 4. Mikrostrukturalna struktura i napredna ponuda API

Multiversum, razvijen na platformi koja se temelji dijelom na Microservicesu<sub>11</sub>, i djelomično na modelu poslužitelja Serverlessa<sub>12</sub>, zahvaljujući suvremenim, proširenim i sigurnim API-jimas karakteristikama, imat će imati sposobnost da se prilagodi obama strukturama.

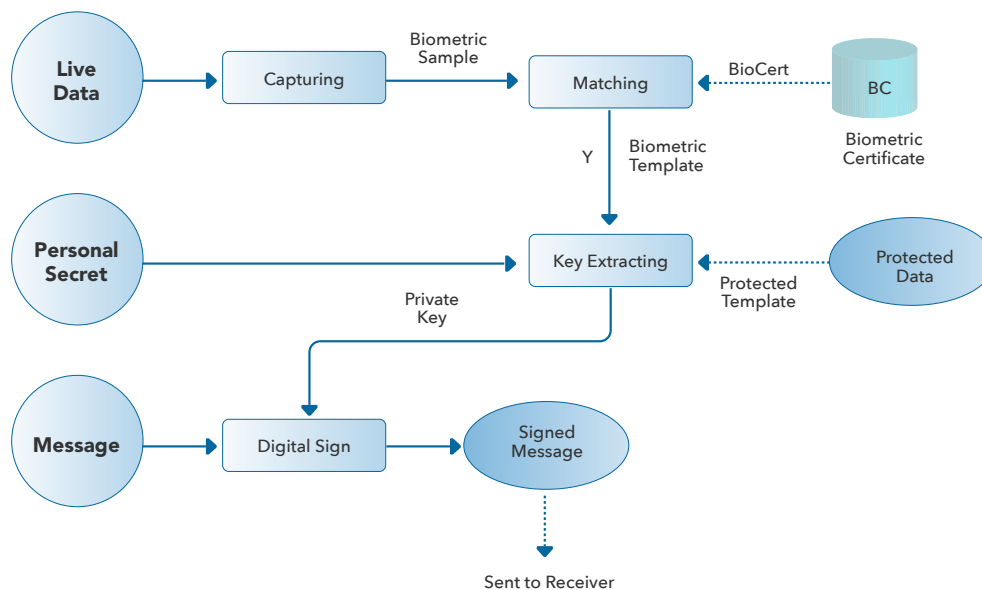
#### 5. Rollback (Sigurnost korisnika)

Multiversum tehnologija omogućuje, u kontekstu transakcije, vratiti se unatrag od neželjenih operacija ili vraćanje prethodnog stanja bez utjecaja na vjerodostojnost valjanosti lanca, ali i provođenje novih programskih transakcija za vraćanje željenog statusa. Nakon što je izvedivost ocijenjena sa stajališta poslovne logike, ona će se smatrati mogućnost implementacije ove funkcionalnosti u novčiće Versum i širenje efektom retroaktivno. U javnom lancu ova funkcionalnost neće biti implementirana, ali Use cases vlasnici koji se odnose na Multiversum tehnologiju bit će slobodni da ga implementiraju.



## 6. Freezable wallets (Sigurnost korisnika)

Nakon procijene izvedivost od strane bazirane na *Business logic* - poslovnoj logici, proučavati će se mogućnost provedbe privremenog zamrzavanja Versum koina u jednom novčaniku koji su posljedica i rezultat nezakonitih aktivnosti.

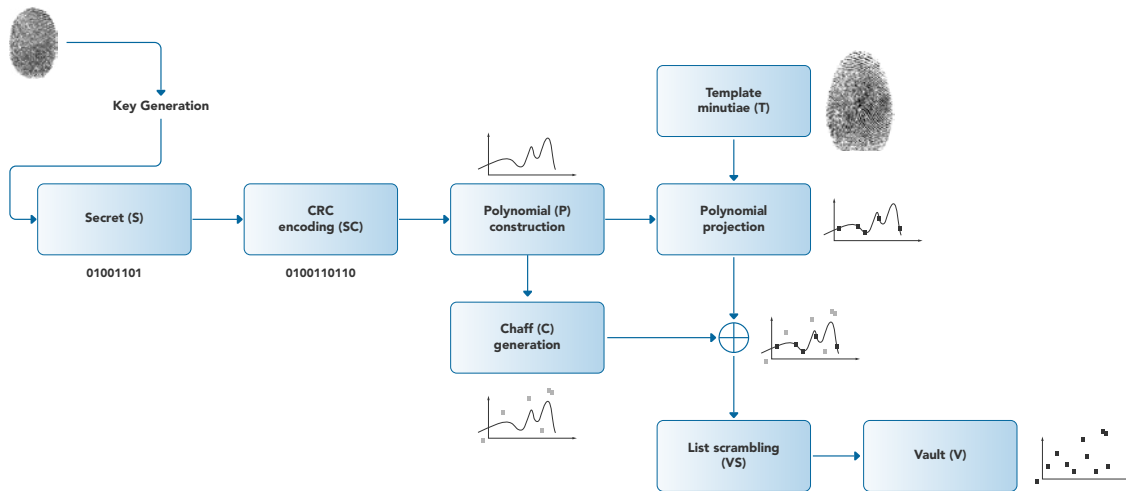


Biometric Digital Key Generation Framework

## 7. Integracija biometrijskih podataka kao seed za elektronički potpis

Pozivajući se na studije profesora Je-Gyeong Jo, Jong-Won Seo i Hyung-Woo Lee iz Sveučilište Hanshin (Republika Koreja) i sažeto u publikaciji "Biometric Digital Signature Key Generation and Cryptography Communication Based on Finger-print"<sup>13</sup>, sproučit ćemo izvedivost korištenja biometrijskih podataka kao što su otisci prstiju, slike irida očiju i grafometrijski potpis kao izvor asimetričnog kriptografskog ključa koji će jamčiti identitet potpisnika transakcije.

Da bi se omogućila uporaba šifriranih biometrijskih podataka u fazi pravnog ispora, biti će procijenjena sigurnost unoošenja podataka. U svakom slučaju, ti će se podaci moći upotrebljavati u aplikacijama za Android i iOS.



Fuzzy Vault Scheme for Biometric Digital Key Protection

## 8. Sučelje ERC23 (mogućnost rada sa drugim Blockchainovima)

Kako bi se osigurala mogućnost rada s drugim lancima, Versumov coin će se razviti implementiranjem sučelja ERC23, napredna i kompatibilna inačica 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. Adapteri off-chain za vlastite ER20/ERC23 (mogućnost rada s drugim Blockchainovima)

Da bi se omogućilo ulazak i izlazak vlastitih koina i tokena na druge ne-vlasničke lance, Multiversum će razviti prirodni prilagodnik – adapter koji će ga uskladiti s buferom koji će regulirati ulaz i izlaz iz vlastitog lanca.

## 10. Nativni izvanredni adapteri za ERC20/ERC23 domaćine (mogućnost rada s drugim Blockchainovima)

Kako bi omogućio ulazak i izlazak neovlaštenih coinsa i tokena na svoj lanac, Multiversum će razviti nativni adapter, kombinirajući ga s višestrukim puferima koji će regulirati njegov unos i izlaz na vlastitom lancu.



## Integrity

### 11. Proof of Integrity (Protok inovacije)

Kao alternativaaalla *Proof of Work* (dokazivanju o radu) i *Proof of Stake* (Dokaz o stanju) u svojim različitim oblicima Multiversum uvodi *Proof of Integrity* (dokaz o integritetu), koji je kriptografski uređaj za provjeru iskrenosti koda kod sastavljenog čvora i uniformnosti odgovora većine čvorova s obzirom na slučajni *challenge seed* koji zajedno s hašom kojeg izračunava vanjska komponenta (ne dekompilirati, zaštićuje i komunicira s softverom čvora u enkriptiranom kanalu) samog softvera i podataka o transakciji, mora biti isti u svakoj pojedinačnoj transakciji za sve čvorove. Ovaj proces zahtijeva znatno manju računalnu snagu i izbjegava trošak koji je tipičan za druge sustave (PoW, PoS, DPoS); ona također pruža veću i stvarniju sigurnost, a ne statističku ili supozitorsku vrstu temeljenu na modelu bizantskog konsenzusa, posebno osjetljivima i ranjivima u malim skupinama.



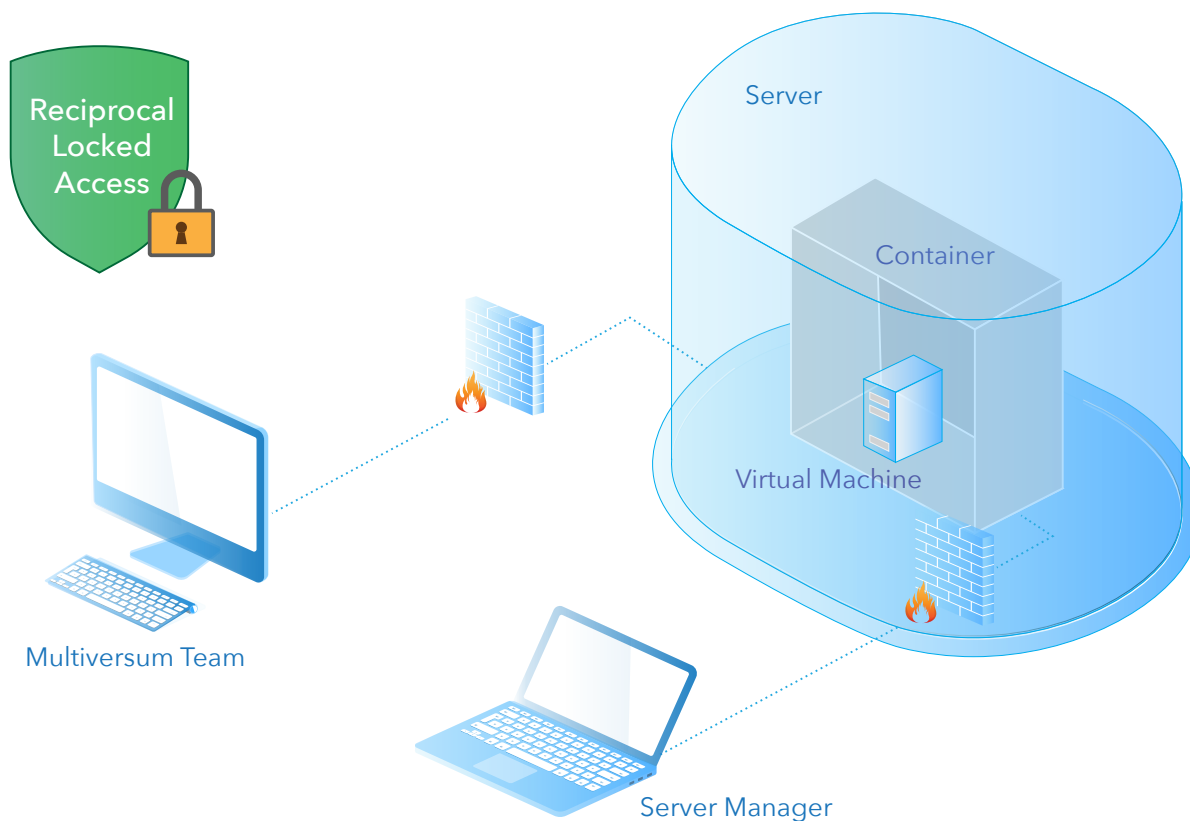
## Access Denied

### 12. Double Access Lock (strukturna sigurnost)

Čvorovi će se distribuirati u virtualnim kontejnerima koji su nedostupni operateru host računala jer su zaštićeni vjerodajnicama koje nisu dostupne samom operatoru. Sigurnost je stoga povjerena najboljim praksama i Linux sigurnosti putem, primjerice, paketa SeLinux<sub>15</sub> i/ili drugih.

Istodobno, čak i ako je netko imao vjerodajnice gostnog stroja, ne bi mu mogao pristupiti, a da ne imati pristup stroju domaćina na kojem je čvor pokrenut.

Čvor je, stoga, učinkovito podvrgnut dvostrukom zatvaranju za pristup.



### 13. Reverse Access Denial (strukturna sigurnost)

Dvostruko zatvaranje koje je razmatrano u točki 12 podrazumijeva učinak međusobnog isključivanja kod pristupa čvoru. To osigurava da čvorovi koji nisu izravno upravljani od strane Multiversuma budu savršeno autentični i nedostupni svima, čvorovi koji su temeljno autonomni i izolirani od vanjskih ljudskih činioca.

Osim sigurnosti operacijskog sustava i sigurnosti ostale tri ključne komponente će biti distribuirane u Container - spremnik: prikupljenih kodova Servera Multiversum, potvrdu s asimetričnim ključ za provjeru autentičnosti u Multiversum klusteru i komponent koji je već raspravljan u paragrafu 11, odgovoran o kalkuliranju challenge koji su bazirani na hašu poslužiteljskog koda, certifikata, challenge seed i podataka o transakciji.

Ova komponenta će biti jedina na raspolaganju operatoru koji će je koristiti za testiranje o iskrenost koda koji je sastavljen od servera koji funkcionira na stroju (ostaju da se provjere mane – downsides).

Dodatne sigurnosne značajke mogu se dodavati i povećati kao što je sposobnost da se automatski promijeni lozinka za pristup Containeru – spremniku dokle se ispunjava, sa slučajnom lozinkom tako da bi se spriječio pristup svakome.

Ovaj se mehanizam može provesti i za potvrdu o pristupu klasteru.

## 14. Recipročna potvrda lanca (mogućnost povezivanja sa drugim Blockchainovima)

Multiversum će provjeriti izvedivost komponente za snimanje stanja drugih lanaca u sustavu kako bi potvrdio svoj status i međusobno ojačao vjerodostojnost i provjeru valjanosti transakcija (eventualno kod tokena). Ako se smatra poželjnim rješenjem, ova komponenta biti stoga implementirana.

Multiversum želi koristiti istu mogućnost periodičnog snimanja transakcije u svrhi kako bi mogli dijeliti odgovornost za provjeru statusa ostalih lanaca. Ona će osigurati specijalno sučelje za funkciju i promicati će njegovu provedbu na novim lancima.

Ova će se komponenta koristiti bez poslužitelja - serverless koji će biti dostupan u sljedećem trenutku ispunjavanja containera koji služe za dodavanje drugih adapteras prema drugim lancima.

## 15. Integracija sa Javom, Springom i JavaScriptom

S obzirom na vokaciju za korištenje u industrijskim, financijskim, pravnim, javnim, administrativnim i poduzeća, Multiversum želi provesti daljnji sloj apstrakcije o modalitetima rada, nudeći sučelja na visokoj razini prikupljenih u funkcionalnim knjižnicama za Java, Javascript i po želji sa ostalim jezicima mainstreama.



Također će se razviti moduli integracije u framework poput Springa u projektu Spring Multiversum.

Te će knjižnice olakšati integraciju Multiversum tehnologije u vlastita rješenja, kako u stvaranju privatnih lanaca, tako i u njihovu pristupu službenom Main Netu.

## 16. ACID model

Multiversum će implementirati definirani model ACID<sub>17</sub>. Akronim dolazi od engleskog termina **Atomicity, Consistency, Isolation, Durability** (Atomičnost, Dosljednost, Izolacija i Izdržljivost) i ukazuje na logična svojstva koja moraju imati transakcije. Da bi transakcije ispravno radile na podacima, potrebno je da mehanizmi koji ih implementiraju ispunjavaju ova četiri svojstva:

- **Atomičnost** - transakcija je nedjeljiva u njegovu izvršenju i njezino izvršenje mora biti ili potpune ili nevažeće, djelomična izvršenja nisu dopuštena;
- **Dosljednost** - kada transakcija počne, baza podataka je u dosljednom stanju, npr. kada transakcija završi, baza podataka mora biti u drugom dosljednom stanju, to jest ne smije prekršiti nikakva ograničenja integriteta; stoga ne smije biti proturječnosti (nedosljednosti) između podataka pohranjenih u DB;
- **Izolacija** - svaka transakcija mora biti izvršena izolirano i neovisno o drugih; svaki eventualni neuspjeh transakcije ne smije ometati druge transakcije koje se izvode;
- **Trajnost** - koja se naziva i upornost, odnosi se na činjenicu da kada se jednom napravi commit transakcije, izmjene se ne smiju više izgubiti, kako bi se to izbjeglo, u vremenskom razdoblju između vremena kada se baza podataka obvezuje da napiše sve varijacije i trenutka u kojem su efektivno napisane, da dođe do gubitaka podataka zbog kvarova ili lošeg rada.

## 17. Transakcijski model

Multiversum će ustrajati na držanju podataka povezanih s transakcijom u "transakcijskom"<sub>18</sub>, modelu tj. Osiguravajući da se svaki ili nijedan podatak o uključenim višestrukim pod-lancima su ustrajani kako bi se zajamčila dosljednost svake provedene transakcije i cjelovitost podataka.

## 18. Jezik kao SQL like

Kako bi se osigurala jednostavnost sastavljanja upita, Multiversum će se temeljiti na sintaktičkoj analizi sličnoj SQL<sub>19</sub>, koristeći jezik sličan onome koji se koristi u standardnoj industriji. Na taj način *learning curve* - krivulja učenja onih koji prvi put pristupaju ovoj komponenti prilično su lagana.

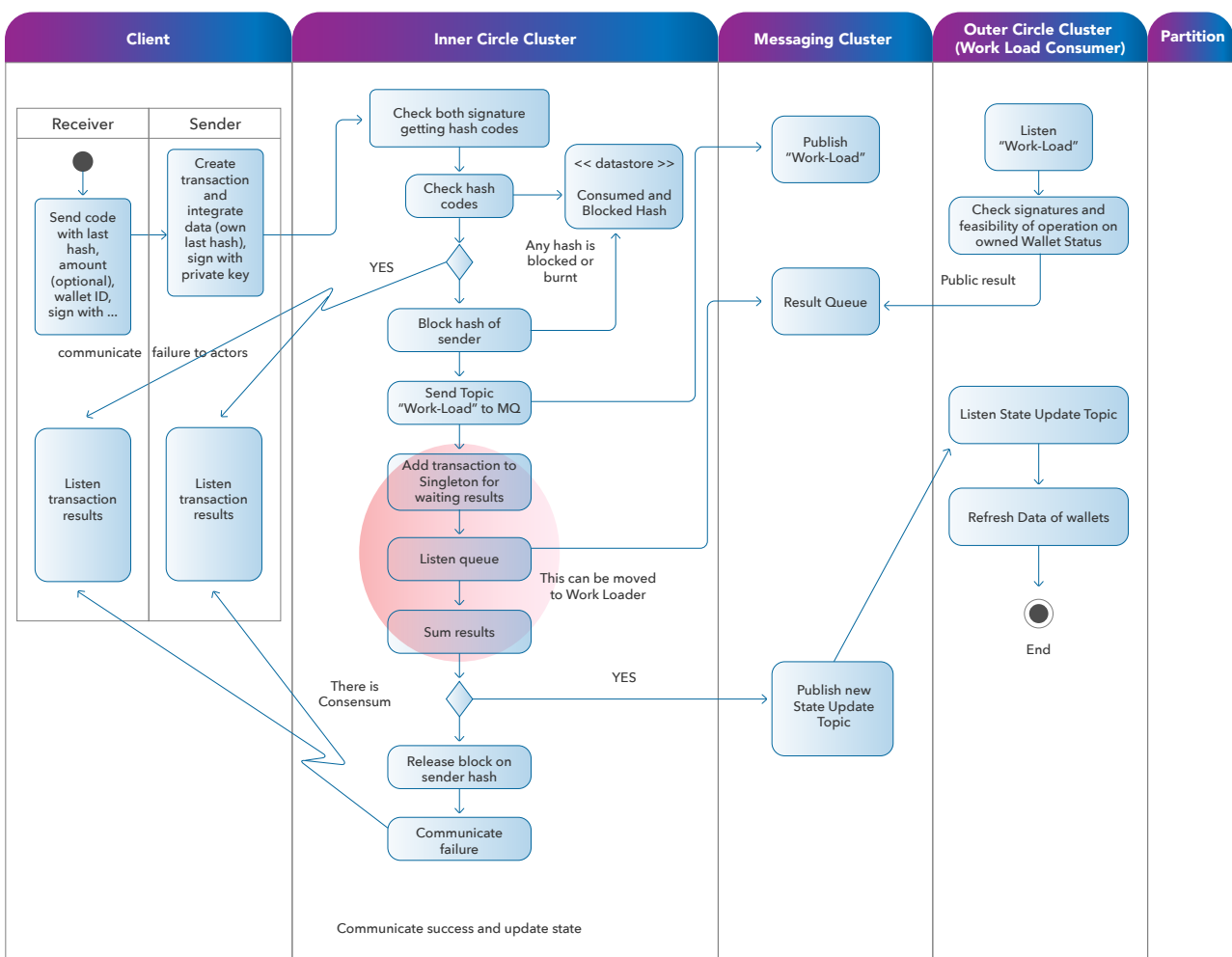
## 19. Funkcioniranje i Full Route Data Flux

Proces prihvaćanja, kontrole, provjere i ustrajanja transakcije odvija se u pojednostavljenom i skematiziranom obliku koji slijedi u nastavku.

Il *best case full route* slijedi ovaj put:

Transakcija se šalje klijentu REST, zajedno s potrebnim podacima i sa potpisanim privatnim ključem.

REST klijent prenosi transakciju čvoru voditelja cluster koordinacije: voditelj Clustera će dijeliti posao unutar, zahvaljujući vlastitom protokolu, između čvorova clustera za koordinaciju, koji će prethodno provjeriti cjelovitost podataka i potpis, mogućnost sredstava za transakciju, prisutnost već korištenih haševa, ne-trenutni status novčanika i novčanika ili blokiranih korisnika.



U međuvremenu, privremeno blokira u letećoj memoriji daljnju uporabu id-a pošiljaoca transakcije e upotpunjava neke podatke, kao što je prijašnja transakcija sa kojom se treba spojiti, timestamp – vremenski pečat i prijašnji haš - hash.

Transakcija se šalje na Topic Message Queue<sub>20</sub> sa protokolom koji će biti definiran (u Pilot u AMQP, koji treba provjeriti MQTT ili drugi) i distribuiran paralelno sa *Worker nodes* radnim čvorovima.

Work nodes potvrđuju da su uključeni u njegovu obradu (oni možda nemaju podatke koji su potrebni, mogu biti opterećeni a radom ili se treba istražiti nešto drugo) i nastavljaju sa stvaranjem novog statusa novčanika, nadoknaditi haševe koji su vezani uz prethodne transakcije i dodajući ih u zapisnik o transakciji.

Dodaje se i Proof of Integrity.

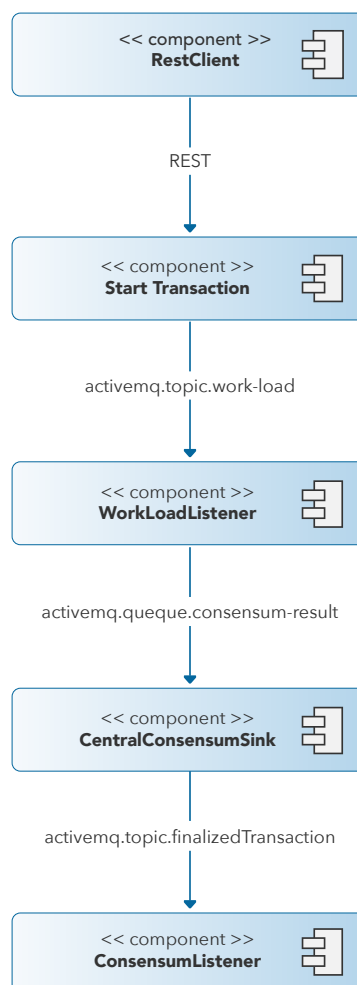
Konačno, oni izračunavaju bazirajući se na svim podacima hašh transakcije. Worker nodes bilježe ovu transakciju u nestabilnim memorijama i šalju ocjene na čvorove koordinatora kroz niz poruka koji prikupljaju sve ocjene.

U slučaju da su ocjene i hašovi dosljedni, koordinacioni čvorovi pišu na trajni način na svoje nosače transakcije i nova stanja novčanika, spaljajući prijašnje haševe i komunicirajući, s dodatnim sustavom Topic Message Queue da je ocjena valjana. Na kraju tog cijelog procesa Worker Nodes pišu da cijela transakcija postoji i dalje.

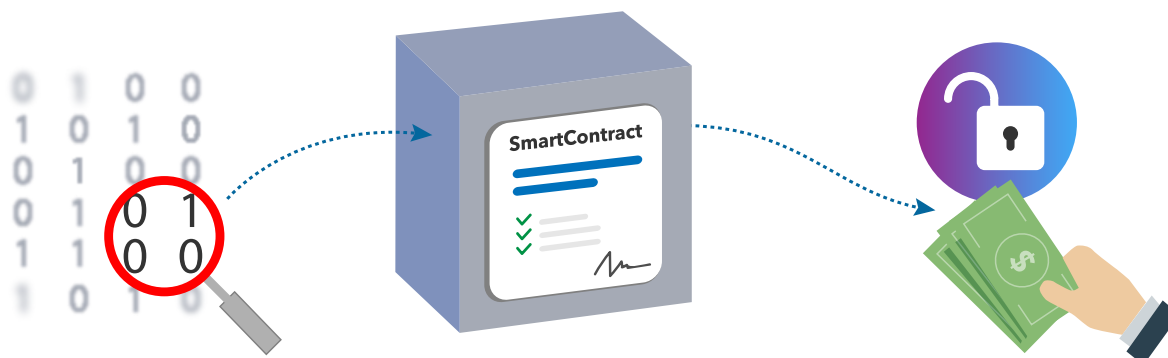
Kraj Best case full road.

## Logic data flux

*Detail of process flow*







## Smart Contracts

Multiversum smatra potrebnim predložiti javnosti pametno razvijene ugovore Smart Contracts<sub>2,1</sub>; istodobno je odlučio da trenutačno, osim ako u budućnosti bude bilo izmjena opsega njegova istraživanja, neće si zacrtati kao cilj da prouči tu mogućnost, ograničavajući njegovo djelovanje, s skromnošću prikladnom znanstvenom okruženju, i identificirati najbolje Open Source rješenje na tržištu i uputiti se na nju radi uključivanja u njegovo rješenje (kompatibilno s modelom licence za projekt na koji će se odnositi).

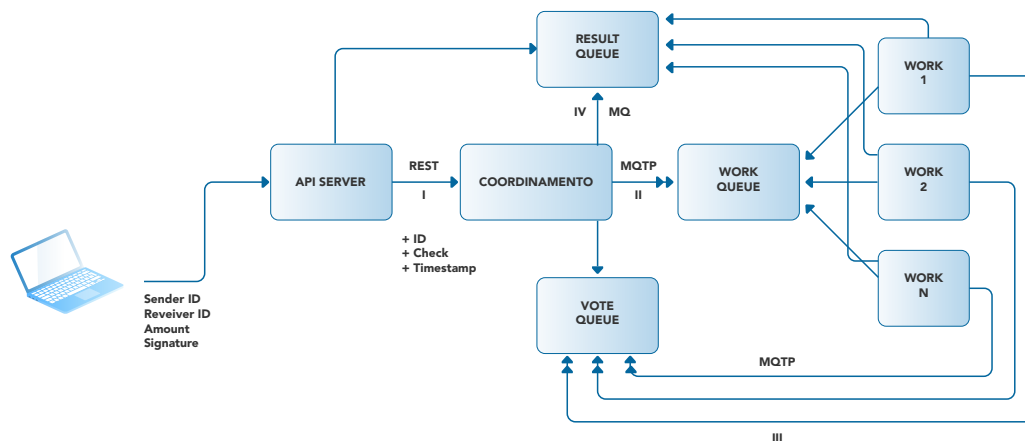
## Infrastruktura

Infrastruktura Multiversuma je dizajnirana kako bi se osigurala otpornost i visoka dostupnost (*high availability*). Ovaj je cilj postignut razvojem clustera čvorova sposobnih samostalno odabrati svoje članove specifičnim funkcijama, koje se temelje na tehničkim karakteristikama svakog čvora, među kojima:

- Kapacitet izračunavanja
- Kapacitet memorije
- Međusobna ping brzina
- Potpunost lančanih podataka
- Pouzdanost stroja
- Sumnje o Proof of Integrity

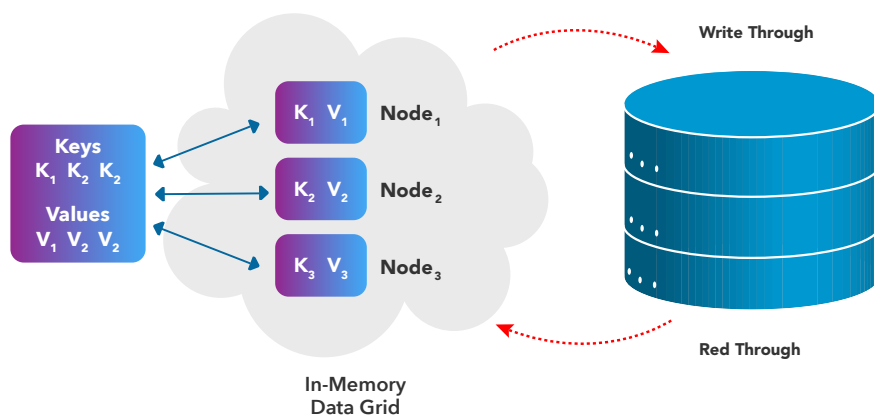
Čvorovi mogu imati jednu ili više funkcija, među kojima:

- Čvorovi klijenata
- Koordinacijski čvorovi
- Čvorovi za razmjenu poruka
- Radni čvorovi
- Trajni čvorovi
- Sigurnosni čvorovi (backup čvorovi)



Svaki čvor koji može dokazati da ima valjanu potvrdu može se registrirati uz cluster i dobiti jednu funkciju.

U slučaju sudara jednog ili više čvorova, cluster će biti u stanju autonomno preraspodijeliti zadatke, optimizirajući uloge.

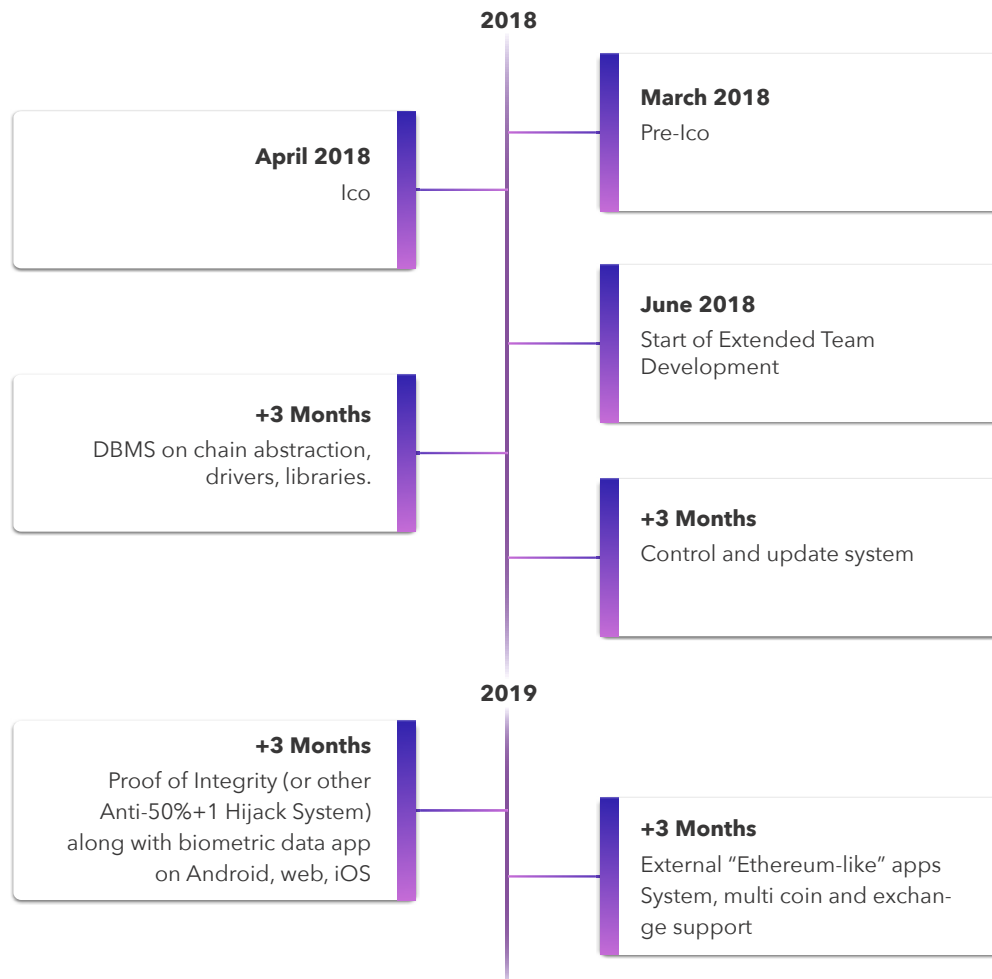


Bit će prisutni komponenti zajedničke predmemorije- cache unutar JVM-a kao baze memorijskih podataka, koji dopuštaju čitanje mehanizama – **Read Through**: traženje podataka u letećoj memoriji (ako ovdje nije prisutan, u fizičkom) i, kasnije, **Write Through**: akumulacija podataka u letećoj memoriji i umetanje u velikom broju u fizičku, tako da se mora čekati dovršetak handshakea i podaci overheada samo jednom, dobivajući optimizaciju performansi (u slučaju pojedinačnih transakcija, oni bi bili izvršeni u više navrata).

## Sigurnosne napomene

U izgradnji će se ponuditi "Hacker's bounties" za one koji će biti u stanju naći ranjivosti i eventualno predložiti odgovarajući odgovor (lijeak).

## Tehnička Road Map



Puno izvršenje zahtjevat će oko jedne godine za deployment servera Glavnog Neta za dva razvojna tima, arhitekta softvera, dva GUI developera, dva menadžera odgovornih za sigurnost, jednog poslovnog arhitekta .

U narednim godinama razvoj će omogućiti da se ima veliki proizvod tvrtke (enterprise grade): od tog kontinuiranoga razvoja, coin Versum će zadobiti prednosti kredibiliteta i imidža.

Glavna će mreža biti kompletna sa svim svojim sigurnosnim mehanizmima i logikom poduzetničkog proizvoda, ali ne onima koje tehnologije čine lako integrirane jer nije neophodan za njegovo korištenje. Softver će biti objavljen stalno i ažuriran kako bi podržao vjerodostojnost projekta, u Test Net će ponuditi devet značajki koje će biti dostupne čim budu objavljene.

## Bibliografija

- 1 [https://en.wikipedia.org/wiki/Scalability#Horizontal\\_and\\_vertical\\_scaling](https://en.wikipedia.org/wiki/Scalability#Horizontal_and_vertical_scaling)
- 2 [https://en.wikipedia.org/wiki/Proof-of-work\\_system](https://en.wikipedia.org/wiki/Proof-of-work_system)
- 3 <https://en.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://sh.wikipedia.org/wiki/Agilni\\_razvoj\\_softvera](https://sh.wikipedia.org/wiki/Agilni_razvoj_softvera)
- 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://en.wikipedia.org/wiki/Security-Enhanced\\_Linux](https://en.wikipedia.org/wiki/Security-Enhanced_Linux)
- 16 [https://en.wikipedia.org/wiki/Spring\\_framework](https://en.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)

# Marketinška strategija

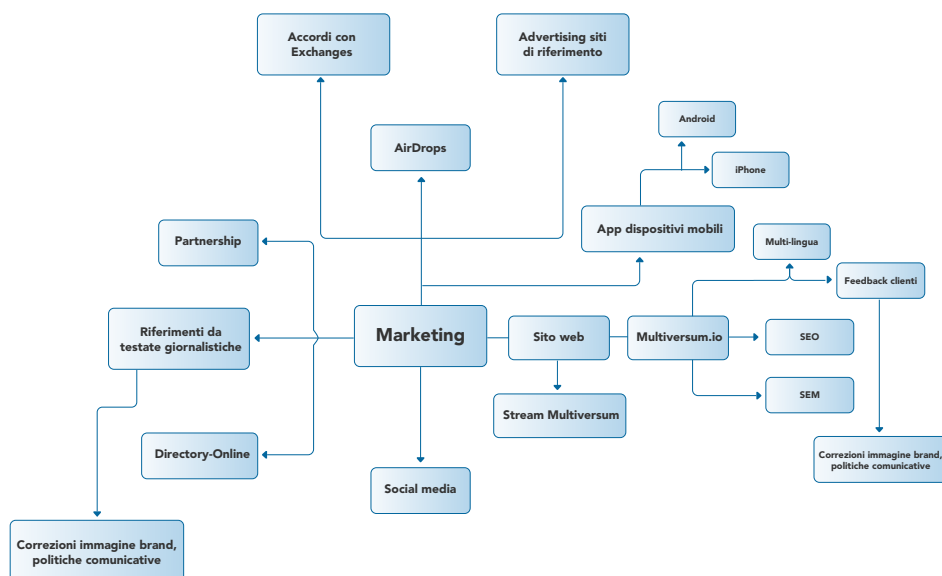
Usredotočili smo se na planiranje cjelokupne marketinške organizacije počevši od općeg konteksta kako bismo se zatim usredotočili na specifične aspekte.

Razumijet ćemo sve one aktivnosti koje će omogućiti postizanje ciljeva, usvajajući globalni pristup prema cijeloj organizaciji (počevši od definicije misije tvrtke sve do prepoznavanja najprikladnije strategije).

Strategija tvrtke bit će odraz okruženjakoji se stalno mjenja i misija tvrtke bit će stvaranje vrijednosti za dioničare, osiguravajući ravnotežu između kratkoročne i dugoročne logike upravljanja.

4 komponente plana su:

- Misija tvrtke
- Poslovni ciljevi
- Strategija tvrtke
- Novčanik poslovnih aktivnosti



Jedan od glavnih alata bit će **Social Media Marketing** koji zajedno sa aktivnostima koje se provode na društvenim mrežama kako bi se povećala svijest o brandu, prepoznala potencijalne potrošače, generirala kontakte i izgradila smislene odnose s kupcima.

Izvršit ćemo različite akcije koje su dio jednog jedinog strateškog plana, počevši od upravljanja i praćenja kanala koristeći se sa instrumentima koji su im namjenjeni i jačanja zajednice kroz svakodnevnu skrb o sadržaju i interakciji sve do konačne analize dobivenih rezultata i provjere strateške taktike koja je provedena.

Svaka od njih se ogledava u vještinama naših Social Media Strategist (stratega socijalnih medija): strateškog planiranja, definiranja i produkcije redakcije, interakcije i podrške s tržištem i analizom rezultata.

**Slojevi elemenata koji  
obuhvaćaju svemir svaki su deset  
puta deblji od prethodnog, svi se  
svemiri, grupirani zajedno,  
pojavljuju kao atomi u ogromnu  
kombinaciju.**

Bhagavata Purana 3.11.41



MULTIVERSUM

HERE TO STAY