MULTIVERSUM

HERE TO STAY

Sách trắng (whitepaper: tài liệu, báo cáo hướng dẫn) phiên bản 1.0.5

Thương mại - Kỹ thuật

06/02/2018

Tác giả: Đội ngũ Multiversum

www.multiversum.io

Bên cạnh vũ trụ này có hàng sa số những vũ trụ khác, và dù vô hạn nhưng chúng vẫn vận hành như những nguyên tử trong Ta.

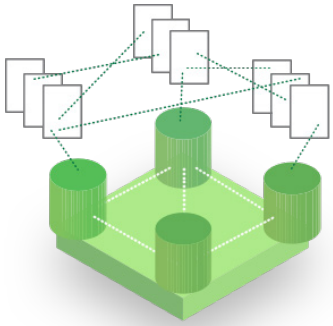
Bhagavata Purana 6.16.37

Multiversum
Nhân dạng và nhiệm vụ

Tiên phong trong lĩnh vực tiền tệ ảo, Bitcoin, cùng với đó là nhiều clone và fork của chính nó dựa trên thuật toán Proof of Work (PoW) cho việc hợp thức transaction (giao dịch tiền ảo), được xem như là blockchain thế hệ đầu tiên.
Thế hệ thứ 2, với Ethereum dẫn đầu blockchain-sử-dụng-smart-contracts, thay vào đó đã đồng nhất hơn, cho phép token hoá dễ dàng tài sản.
Cả 2 công trình đều có hiệu quả năng lượng cực kỳ thấp, tốc độ hợp thức block trung bình thấp và transaction mỗi block.
Giải quyết vấn đề về khả năng mở rộng, tốc độ, và tiêu thụ năng lượng là mục đích của giải pháp blockchain thế hệ thứ 3, sử dụng các cách tiếp cận lẫn kỹ thuật khác nhau như hợp thức thuật toán Proof of Stake (PoS), routing không trực tiếp, đồ thị chuỗi, và tập trung hoá một phần hay toàn bộ.
Thế hệ thứ 4 đi xa hơn nữa vấn đề này, với việc hoàn thành nhanh hơn, giải pháp có khả năng mở rộng hơn và đồng thời cố gắng để trở nên cạnh tranh về mặt thương mại; các chuỗi dữ liệu đơn giản không đủ linh hoạt để thoả mãn yêu cầu trong môi trường đoàn thể, mà ở đó các cấu trúc dữ liệu phức tạp cần được tổ chức theo bảng (như trong cơ sở dữ liệu quan hệ).
Đồng thời, những cấu trúc này cần được hợp thức và không bị ảnh hưởng với các kỹ thuật dựa trên blockchain, tăng cường khả năng truy gốc và bảo mật.
Nói cách khác, thế hệ blockchain thứ 4 mang đến công nghệ này để hoàn thiện ứng dụng sản xuất căn bản, và mở rộng đề nghị hướng về thương mại hiện hành xét về mặt lưu trữ giữ liệu, phi tập trung hoá ứng dụng, kiểm toán, bảo mật và độ tin cậy.
Multiversum đề nghị tổ chức dữ liệu phức thay vì dùng chuỗi dữ liệu, chia tách hay nối lại chuỗi (chain) để cho phép khả năng mở rộng và quan hệ song song lớn hơn, và hợp thức khái niệm Proof of Integrity (PoI - minh chứng cho tính nguyên vẹn) (ví dụ bằng chứng cryptographic của server code) thay vì giải pháp thuật toán PoW hoặc PoS đang hiện hành.
Hơn nữa, Multiversum sẽ đặc trưng tích hợp ERC20/ERC23, cho phép coin và token từ những nguồn khác tham gia vào dây chuyền của chúng tôi và ngược lại, với dịch vụ công chứng cũng như phương pháp xác nhận bên trong.
Trong lúc đó, cùng với những cải tiến này, chúng tôi chắc chắn sẽ sử dụng nhiều giải pháp tuyệt vời mà đồng nghiệp của chúng tôi đã sử dụng trong suốt thời gian qua.

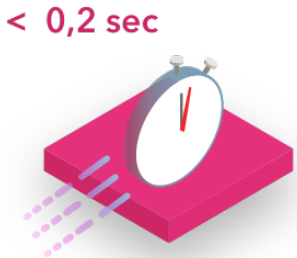
Multiversum
Blockchain thế hệ thứ 4

Tại sao nên chọn lựa Multiversum Blockchain 4.0?



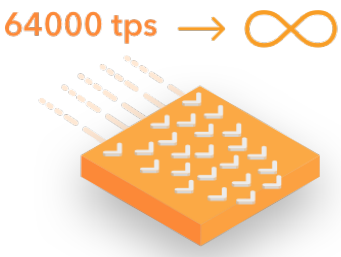
Blockchain tương quan

Một loại blockchain mới đặc trưng với nhiều loại dữ liệu, quan hệ trong một cấu trúc đa chiều.



Tốc độ transaction

Trong khoảng thời gian ít hơn 0.2 giây, quỹ sẽ được chuyển qua wallet (ví điện tử), bao gồm cả xác nhận bảo mật transaction. Thuộc vào loại nhanh nhất trên thế giới.



Thông lượng Transaction

Khả năng mở rộng tốt nhất: lên tới 64000 Tps (1000 Tps/core) trên một server có đến 64 core.

Proof of Integrity

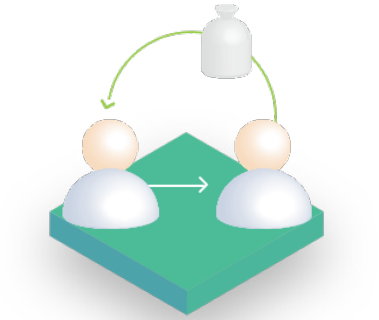
PoS (Proof of Stake) sẽ được thay thế bằng PoI (Proof of Integrity).

Wallet thế hệ tiếp theo

Đi đầu về bảo mật trong việc tiếp cận và thuyên chuyển các quỹ với nhập liệu sinh trắc học.

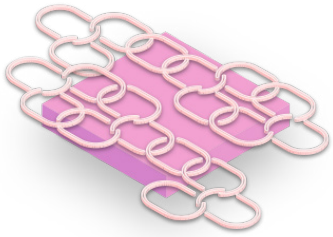
Eco-friendly

A Multiversum transaction will have insignificant costs and next to zero environmental footprint.



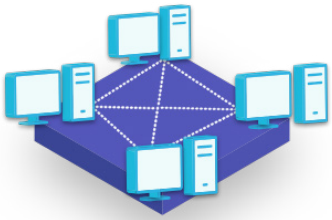
Rollback

(thao tác lùi cơ sở dữ liệu về trạng thái cũ nhằm mục đích khôi phục dữ liệu)
Rollback tuỳ chọn có thể được kích hoạt thông qua Multiversum token.



Các chuỗi phân chia được

Tối ưu hoá tài nguyên giữa các node do chuỗi có khả năng phân chia.



Phân phối node phục hồi

MTV node phân phối khắp thế giới nhằm mục đích ổn định và phục hồi nếu sự cố toàn cầu xảy ra.

Thuyết trình công khai

Blockchain hiện hành tiên tiến nhất

Những đặc tính hàng đầu của hiện tượng Blockchain đều có một điểm chung: cực kỳ an toàn và đáng tin cậy. Đồng thời, chúng ta đã phải trả giá khi xét tới việc xử lý năng lượng khổng lồ, gây ô nhiễm không thể chấp nhận, mức phí transaction cao và sự chậm chạp trong transaction, những điều khó mà có thể đại diện cho tiêu chuẩn tiến bộ kỹ thuật hiện tại, và đưa ra những câu trả lời về mặt kỹ thuật phù hợp cho những trường hợp tài chính hiện đại và tiêu dùng thương mại.
Sự chậm chạp này được tạo ra do thiếu sót trong phát triển về bề ngang, ví dụ như việc gia tăng công suất tính toán đạt được chỉ bằng cách thêm vào nhiều bộ xử lý thay vì thay thế chúng với những bộ xử lý nhanh hơn. Một nguyên nhân khác nằm ở cơ chế an ninh cố hữu của blockchain hiện hành, được thiết kế để phòng ngừa bất kỳ người nào chiếm lấy phần lớn cluster bằng cách khiến cho việc sử dụng trở nên tốn kém về cả mặt năng lượng và chi phí (thuật toán Proof of Work và Proof of Stake).
Hơn nữa, những blockchain hiện hành là những chuỗi đơn giản của những sự thay đổi trong trạng thái thể dữ liệu đơn; tái cấu trúc các trạng thái thật của những thể dữ liệu này ngụ ý rằng phải scan toàn chuỗi, từ đó dẫn đến hệ thống bị trì trệ hơn nữa và tốn nhiều tài nguyên hơn.
Ngoài ra, việc đo lường bảo mật dừng lại ở mức dữ liệu không đảm bảo sự an toàn cho người sử dụng, khiến cho việc phục hồi coin bị mất hoặc bị ăn cắp trở nên hầu như là không thể cho dù kể cả khi chúng đã được xác định vị trí trong chuỗi, hoặc kể cả khi chặn các tài khoản nhiễm mã độc.
Cuối cùng, một vấn đề khác đó là sự phân mảnh và tính không đồng nhất giữa cái tiền ảo, dẫn tới việc không thể giao thiệp giữa các tiền ảo với nhau và tồn tại trong những vũ trụ không liên quan đến nhau.

Multiversum và chấp nhận blockchain toàn cầu

Công nghệ Multiversum thúc đẩy blockchain truyền thống vượt ngưỡng giới hạn hiện tại bằng cách nâng cao lớp dữ liệu thông qua việc tự xác minh và các cấu trúc được phân phối của các thể dữ liệu được tổ chức, liên kết thể dữ liệu này tới thể khác thông qua các link biểu tượng.
Công nghệ này đã đặt ra nền móng cho hệ thống phi tập trung và phân phối của các transaction thống nhất sử dụng tự xác minh: Multiversum blockchain.
Multiversum, thay vì sử dụng mẫu dữ liệu đơn của blockchain hiện hành, cho phép việc tạo ra cơ sở dữ liệu quan hệ mật (Relational Crypto Database - một giải pháp lưu trữ giữ liệu được tổ chức và dữ liệu cao cấp), mà có thể giải quyết không chỉ một loại dữ liệu đơn mà còn cả các chuỗi dữ liệu được nhóm lại trong các biểu đồ cấu trúc dữ liệu phức tạp liên quan tới dữ liệu khác. Những mối quan hệ bây giờ được xem như là những công dân hạng nhất của blockchain và được đảm bảo bởi phương pháp cryptographic.
Mỗi chuỗi dữ liệu, khi được yêu cầu thay đổi trạng thái, sẽ phân tách chuỗi ngầm của chính nó từ nhánh gốc, rồi sau đó sẽ nối trở lại sau khi tiến hành xong, để hợp thức.
Do đó Multiversum chính là một kỹ thuật blockchain tiến hoá, mang đến những nét đặc trưng duy nhất để khắc phục những bất tiện đã được phân tích trước đó, với những kỹ thuật tập hợp, hợp thức mật và phân phối phù hợp với mọi môi trường: Hành chính, Công nghiệp, Tài chính và Chính phủ.
Một trong những mục tiêu chính của Multiversum đó là mang lại cho thị trường, mọi lúc, sản phẩm tân tiến nhất có sẵn: điều này sẽ là có thể khi thực hiện phương pháp phát triển phần mềm AGILE.
Phương pháp AGILE ngụ ý việc giảm mạnh sự tham gia đến giai đoạn thiết kế ban đầu nhằm nâng cao giá trị kinh nghiệm gặp phải trong suốt quá trình phát triển dự án, cho thấy cơ hội và thách thức khó có thể dự đoán được, trao thưởng các vấn đề hay nhất và bỏ lại những vấn đề không thích hợp.
AGILE là một tiêu chuẩn phát triển phần mềm được thiết lập và thúc đẩy các nhà phát triển, các chủ sản phẩm và các nhà đầu tư để xem xét phạm vi dự án linh hoạt và sẵn sàng thích nghi với nhu cầu thị trường. Hơn thế nữa, trong một phân khúc phát triển nhanh chóng như phần mềm, đưa ra sản phẩm sau 6 tháng nghiên cứu và một năm thực nghiệm, khi nó được thai nghén để phù hợp với nhu cầu thị trường của 18 tháng trước, đồng nghĩa với việc đề nghị một sản phẩm lỗi thời trả lời cho những vấn đề lỗi thời, điều đó có thể được giải quyết bởi những công ty cạnh tranh và thiếu phản hồi cho những thách thức vừa mới được tạo ra.
AGILE, thay vào đó, tạo ra cơ hội để đưa đến cho thị trường sản phẩm tân tiến nhất tại ngay chính thời điểm giao nhận.

Tốc độ và công nghệ

Một trong những điểm mạnh của công nghệ này là nó thực sự nhanh chóng, nhờ vào khả năng chạy nhiều transaction khác nhau một cách song song và cơ chế tách-ghép với công nghệ block-chain của chúng tôi. Những đặc điểm này cho phép việc mở rộng phát triển theo bề ngang, và tăng cường khả năng tiến hành transaction mà thêm năng lượng tính toán vào công nghệ có sẵn, mỗi node đều được tính đến, hiệu năng tốt nhất.

Mở rộng phát triển theo bề ngang

Multiversum mang lại ích lợi từ 2 đặc điểm cụ thể để tối đa hoá hiệu quả hệ thống:
1- Chuỗi chính có thể tối ưu hoá cấu trúc của nó bằng cách chia tách tự động thành nhiều chuỗi ngầm, theo như tài nguyên và nguồn dữ liệu được yêu cầu, song song hoá công việc thông qua nhiều thread và node.
Quá trình tách-chuỗi này được tiến hành cho tới lúc bình thường hoá khối lượng công việc, khi chuỗi nối trở lại một cách tự động.
Tất cả những điều này đều có thể bởi vì công nghệ cho phép mỗi khối (block) của chuỗi hợp thức 2 chuỗi ngầm khác từ 2 đường link sắp đến khác.
2- Sharding (tiến trình lưu trữ dữ liệu qua nhiều bản ghi) dữ liệu, ví dụ như một kỹ thuật cho phép phân phối dữ liệu giữa nhiều node.

Cho một dãy dữ liệu ABC và 3 cluster node, chúng ta sẽ có dữ liệu phân phối như sau:

AB

BC

CA

Sự phân chia này cho phép tốc độ tiến hành transaction cao hơn, vì truy vấn dữ liệu sẽ gây tác động mỗi node chuỗi ngầm, tối ưu hoá từng bước.
Thêm một đặc điểm cực kỳ quan trọng khác nữa trong công nghệ của chúng tôi đó là Tính Sẵn sàng Cao (High Availability): cơ hội dựa vào loại cluster đảm bảo tính liên tục của dịch vụ kể cả trong trường hợp một số node bị shutdown ngay trong mạng.
Sử dụng ví dụ trước (A, B và node C), giả sử C bị offline (đứt mạng), node A và node B sẽ vẫn còn hoạt động hoàn toàn, cho phép dịch vụ tiếp tục mà không có bất kỳ sự mất mát về dữ liệu nào, đến mức chỉ cần 50% + 1 node tiếp tục hoạt động.
Cách này, trong trường hợp nhiều node bị hỏng, cluster vẫn tự động tái tổ chức phân bố dữ liệu giao tiếp với mỗi node, cho tới khi hoàn toàn phục hồi hoạt động

Môi trường

Multiversum cũng thân thiện với môi trường: một trong những mục đích chính của chúng tôi là giảm thiểu năng lượng tính toán cần thiết cho việc hợp thức cryptographic vì thế tránh được tình trạng mining (Proof of Work), một sự lãng phí năng lượng và tài nguyên khổng lồ.
Thay vì công nghệ lỗi thời này, chúng tôi đang tiến hành Proof of Integrity, một giao thức thi hành hợp thức cryptographic bằng cách kiểm tra tính xác thực của phần mềm mà giải quyết mỗi transaction bền vững.

Quản trị dữ liệu

Multiversum, với Dữ liệu cơ sở Quan hệ Mật (Crypto-Relational Database) của chính nó có thể dễ dàng cấu trúc mà không cần giới hạn link dữ liệu.
Mỗi wallet sẽ có một dãy trạng thái và sẽ được liên kết với một người (user), và sự thay đổi mới trong trạng thái wallet sẽ bao gồm 2 vùng dữ liệu:
trạng thái trước đó, để kiểm tra tính hợp thức.
một đường link kết nối tới lần transaction cuối cùng (hoặc tới link của chuỗi chính cuối cùng)
vì thế mà nơi phát sinh trạng thái mới sẽ được nhận biết.
Sau khi thay đổi, việc điều chỉnh transaction sẽ được thêm vào mà trạng thái sau khi điều chỉnh của nó tái tham gia vào chuỗi chính.
Do đó, transaction mới sẽ được kế thừa 2 mã hash (mã băm): một cái từ link trạng thái, cái còn lại từ transaction trước đó, và theo cách này, tất cả hoạt động sẽ hợp thức những transaction trước đó liên kết với chính transaction đó.
Phương án tân tiến này, có thể quản lý được cả những trường hợp có dữ liệu phức tạp, sẽ cho phép mọi người thực hiện bất kỳ ứng dụng nào với công nghệ của chúng tôi, đảm bảo sự phổ biến cả thế giới về hành chính, chính phủ, tài chính và công nghiệp, đưa đến cả một vũ trụ blockchain với một bước đệm về phía trước.

MULTIVERSUM

HERE TO STAY

Unique Features !

Crypto relational DB
Autovalidating Complex Data structures

Divisible/Re-joinable chains
(Parallel Work)

Sharding data
(Parallel Work)

Minimal ecological footprint

Reciprocal chain confirmation
(Interoperability with other BC)

Advanced API offer

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

Java, Spring and Javascript
(Libraries for Integration)

Freezable wallets
(User Security)

Proof of Integrity
(Protocol Innovation)

Biometric Data integration as Electronic Signature seed
(User Security)

Double Access Lock
(Structural Security)

Reverse Access Denial
(Structural Security)

Rollback
(User Security)

Self managing Crypto-Cluster

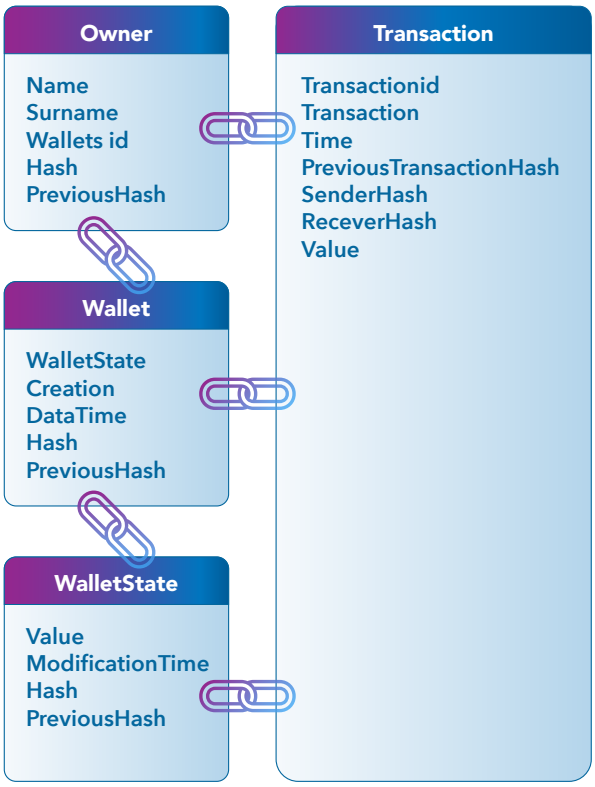
Native on chain adapter for own ERC20
(Interoperability with other BC)

ERC23
(Interoperability with other BC)

Nhiệm vụ Multiversum

Multiversum hướng tới bước tiến mang tính thế hệ trong thế giới blockchain, và như Lợi điểm bán hàng độc đáo (Unique Selling Points – ưu thế khác biệt của một sản phẩm hay thương hiệu so với đối thủ cạnh tranh), chúng tôi đề xuất các mục tiêu sau:

1. Đạt được Crypto Relational DB với cấu trúc dữ liệu phức tự hợp thức
2. Phân chia/Tái nhập chuỗi dựa trên khối lượng công việc trong hệ thống hiện hành (Làm việc song song)
3. Sharding dữ liệu (Làm việc song song)
4. Đề nghị API tân tiến
5. Rollbacks (Bảo mật người dùng)
6. Đóng băng wallet (Bảo mật người dùng)
7. 7Tích hợp dữ liệu sinh trắc học giống như seed cho chữ ký điện tử
8. Giao diện ERC23 (Khả năng tương tác với các blockchain khác)
9. Adaptor mở rộng không trực tiếp cho chính ERC20/ERC23 (Khả năng tương tác với các blockchain khác)
10. Adaptor mở rộng không trực tiếp cho ERC20/ERC23 khách (Khả năng tương tác với các blockchain khác)
11. Proof of Integrity (Giao thức cải tiến)
12. Khoá truy cập đôi (Bảo mật có cấu trúc)
13. Từ chối truy cập ngược (Bảo mật có cấu trúc)
14. Xác nhận chuỗi tương hỗ (Khả năng tương tác với các blockchain khác)
15. Tích hợp cho Java, Spring và Javascript
16. Mẫu ACID
17. Mẫu transaction
18. SQL - giống như ngôn ngữ



1. Đạt được Crypto Relational DB với cấu trúc dữ liệu phức tự hợp thức

Multiversum có một thiên hướng mạnh mẽ tới việc sử dụng trong công nghiệp và hành chính, các bối cảnh mà trong đó chúng tôi sở hữu dữ liệu với cấu trúc phức tạp, không thể được đại diện được theo một cách hiệu quả thông thường với chuỗi đơn giản.

Chúng tôi hướng tới việc trở thành dữ liệu cơ sở quan hệ mật đầu tiên trên thị trường, phi tập trung hoá hoặc đơn giản chỉ là phân phối nếu cần.

Khả năng này xuất phát từ việc khái niệm hoá các thể chuỗi: trong công nghệ của chúng tôi, một chuỗi cơ bản có thể chia ra thành các chuỗi thứ cấp, bao gồm nhiều nhóm thể và bản ghi.

Những thể này sẽ tái nhập ở trạng thái tồn tại cuối của chúng, sau khi việc điều chỉnh được yêu cầu, chúng sẽ tái nhập một lần nữa đến link cuối của chuỗi cơ bản, trở thành một thể lần nữa. Giao diện "có thể nối chuỗi" giả định một loại bản ghi bao gồm 2 hoặc nhiều hơn mã hash của những bản ghi trước, hợp thức không chỉ một mà nhiều chuỗi ngầm khác.

Trong việc thực hiện tiêu chuẩn Multiversum, được sử dụng với Versum coin, các thể "có thể nối chuỗi" cộng sinh trong chuỗi sẽ thuộc về 4 bảng: User (người dùng), Wallet, Trạng thái Wallet, Transaction, liên quan đến một thể khác và chúng tự xác nhận tương hỗ.

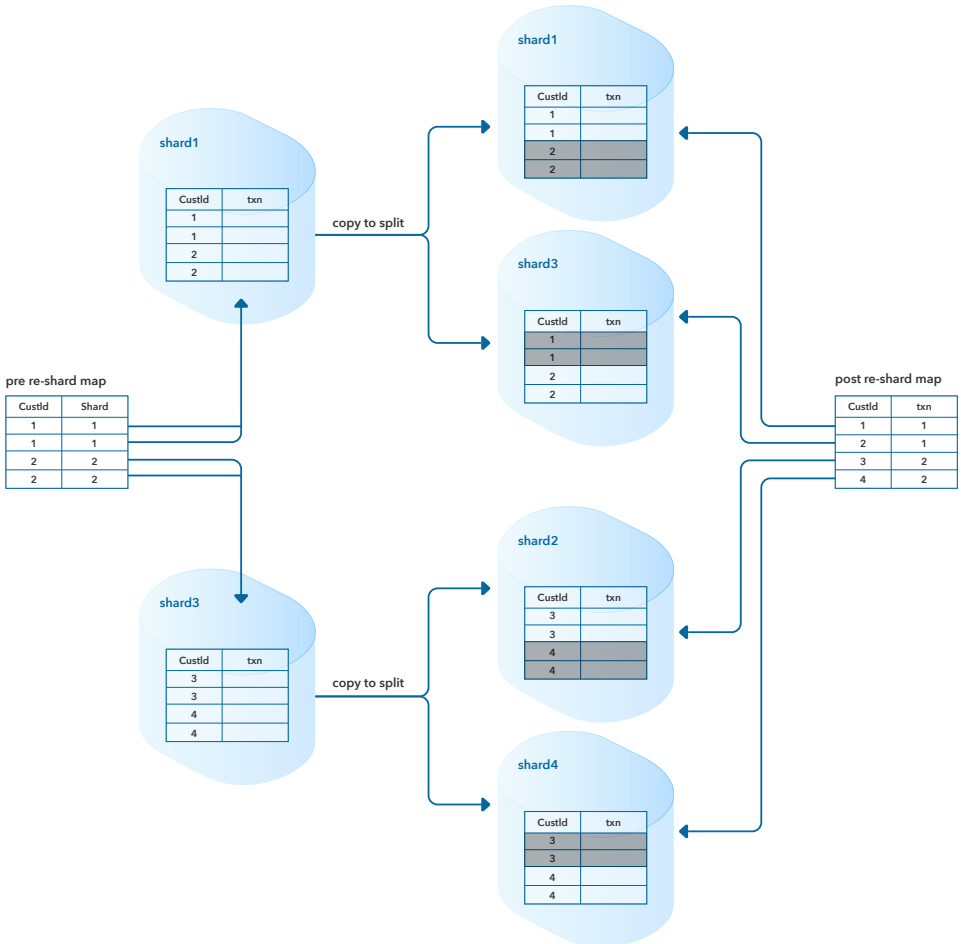
2. Phân chia/Tái nhập chuỗi dựa trên khối lượng công việc trong hệ thống hiện hành (Làm việc song song)

Khả năng tương tự bắt nguồn nhiều link từ một link được đưa ra và nối chúng lại cho phép

công nghệ sử dụng các máy phân tích khối lượng công việc mà chỉ ra sự cần thiết của việc phân tách chuỗi chính thành 2 chuỗi thứ cấp (và chắc chắn có thể phân tách chúng lần nữa) khi một yêu cầu cao trong việc tiến hành transaction diễn ra. Một khi khối lượng công việc dừng lại lần nữa, nhiều chuỗi ngầm tồn tại từ trước được cho phép kết nối lại và được hợp thức. Cơ chế này cho phép làm việc song song trong khi vẫn giữ được tính an toàn tới bản ghi của transaction.

3. Sharding dữ liệu (Làm việc song song)

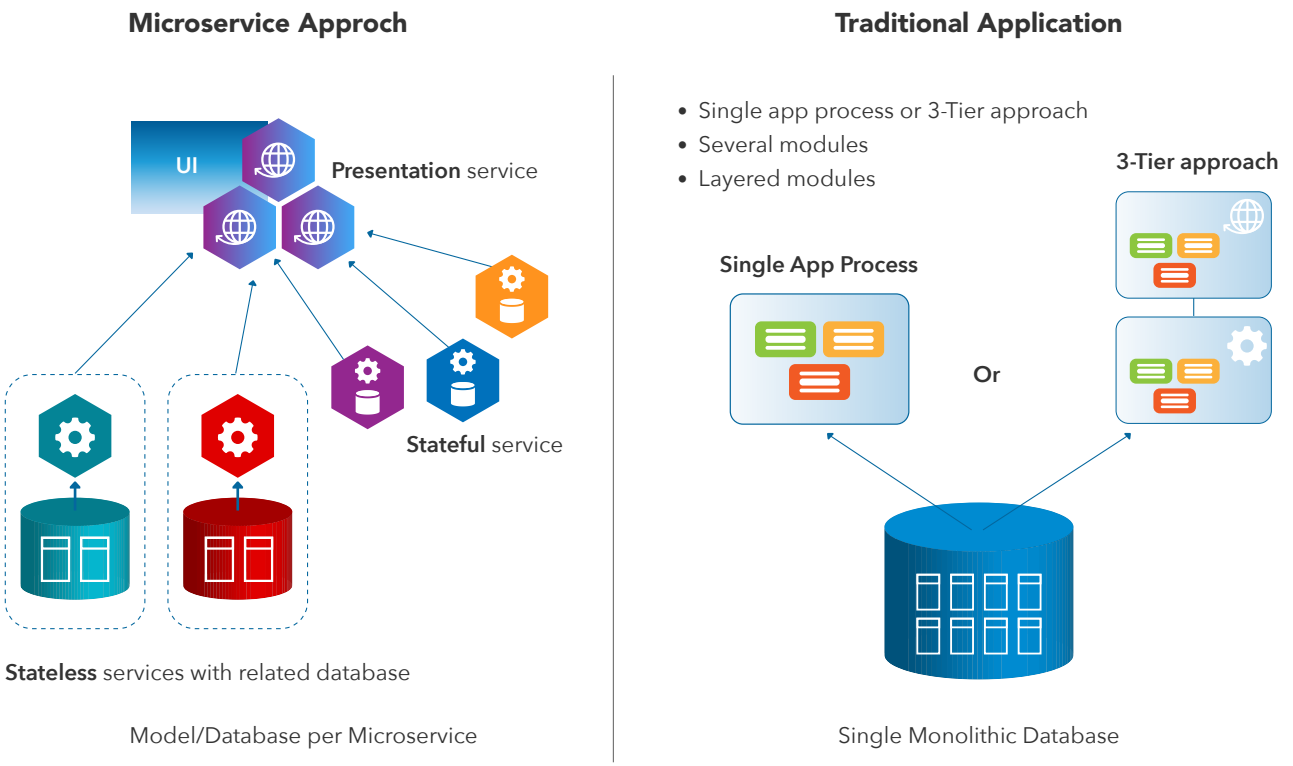
Mỗi node sẽ chứa cả chuỗi dữ liệu hoặc chỉ một phần của chuỗi.
Khi Sharding dữ liệu được cần tới, các coordinator node sẽ thiết lập các chế độ tham gia vào dữ liệu cụ thể, nhằm tối ưu hoá khả năng phân phối của chúng theo như khối lượng công việc hiện hành. Theo như các kỹ thuật cao có sẵn, độ tin cậy và độ bền vững sẽ luôn luôn được đảm bảo, kể cả trong các trường hợp một phần cluster bị mất đột ngột, ví như tối thiểu 50%+1 số node tồn tại. Những node này, sau khi cluster bị crash, sẽ có thể tái phân phối và tái tổ chức cấu trúc dữ liệu để có thể đương đầu được với lần crash cluster tiếp theo nhanh nhất có thể.
Bằng những phương tiện kỹ thuật 2 và 3, Multiversum blockchain sẽ đề cao làm việc song song và khả năng sharding dữ liệu, đồng nghĩa với khả năng phát triển theo bề ngang,



bảo mật được tăng cường, khả năng sẵn sàng cao, khả năng hồi phục của hệ thống, sự biến mất của việc hỏng một điểm (a single point of failure) và khả năng tự phục hồi sau sự cố.

4. Cấu trúc Microservices (cấu trúc nhiều dịch vụ nhỏ) và đề nghị API tân tiến

Đã phát triển trên nền tảng dựa trên Microservices và Các mẫu Không server (Serverless models), Multiversum sẽ có thể cung cấp bảo mật tiên tiến, các chức năng API hiện đại và để thích ứng với cả 2 kiểu cấu trúc.

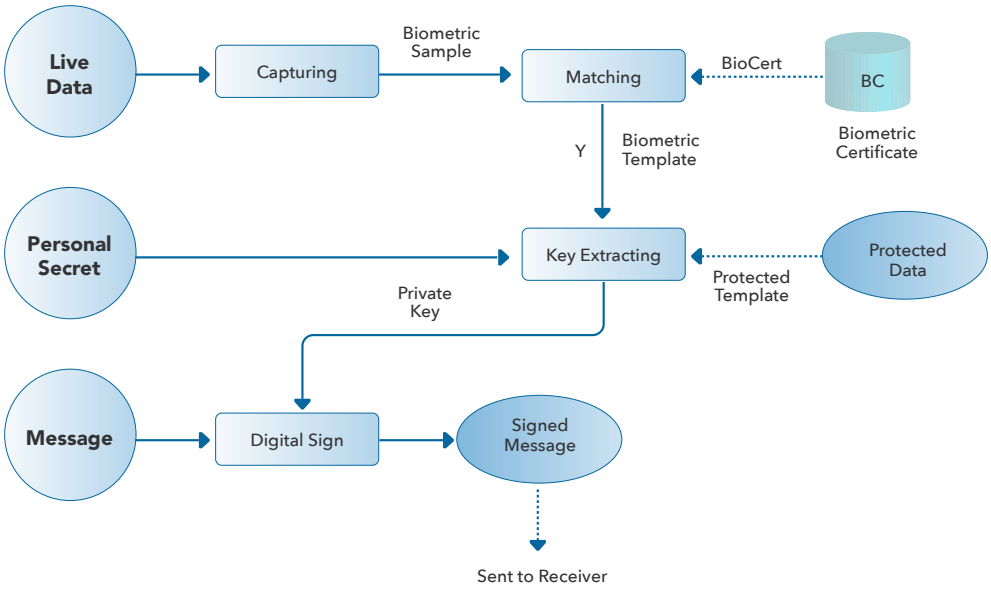


5. Rollback (Bảo mật người dùng)

Công nghệ của chúng tối, trong bối cảnh liên quan đến transaction, sẽ cho phép rollback những hoạt động không mong muốn, ví dụ như phục hồi trạng thái trước đó mà không làm giảm độ tin cậy của hợp thức chuỗi, bằng cách tiến hành một nhóm trạng thái hồi phục transaction. Đặc trưng này có thể được cho phép tuỳ ý với tất cả token và ứng dụng được khởi tạo trong Multiversum blockchain.

6. Đóng băng wallet (Bảo mật người dùng)

Khả năng bao gồm việc đóng băng wallet trong trường hợp có hoạt động bất hợp pháp hoặc đáng ngờ sẽ được thực hiện sau khi đã nghiên cứu tính khả thi về mặt Business Logic. Những ứng dụng độc quyền, được xây dựng trên Multiversum blockchain, sẽ có lựa chọn để tiến hành đóng băng nếu muốn.

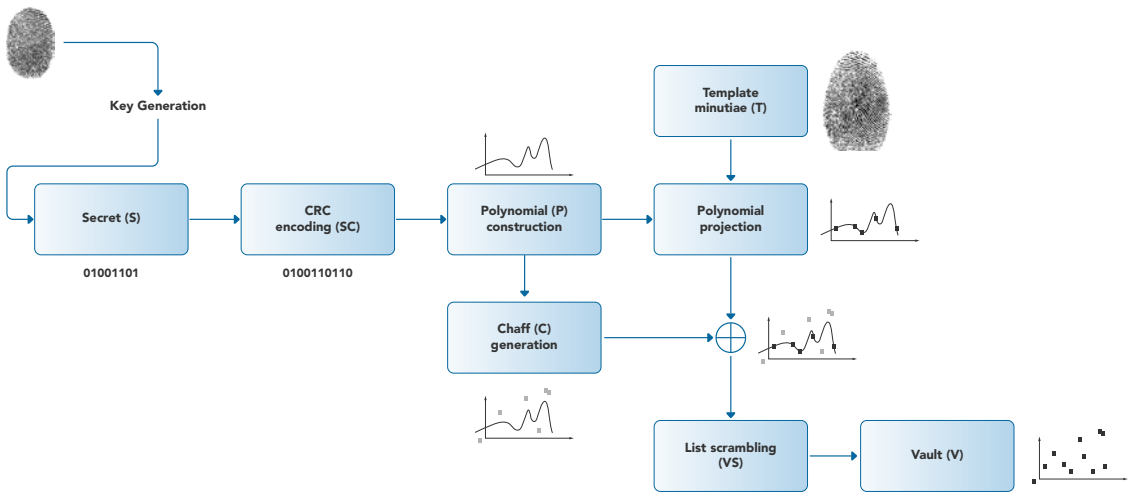


Biometric Digital Key Generation Framework

7. Tích hợp dữ liệu sinh trắc học giống như seed cho chữ ký điện tử

Bắt đầu từ nghiên cứu được hoàn thiện bởi công trình của Je-Gyeong Jo, Jong-Won Seo và Hyung-Woo Lee, đội ngũ Multiversum sẽ đánh giá tính khả thi của dữ liệu sinh trắc học giống như dấu vân tay, scan võng mạc và chữ ký cá nhân như là nguồn key cryptographic bất đối xứng để đảm bảo tính xác thực của nhân dạng người dùng.

Sự an toàn của dữ liệu đã được mã hoá và cách dùng của chúng như việc hợp thức trong luận cứ luật pháp sẽ được đánh giá. Hơn thế nữa, dữ liệu sinh trắc học sẽ được sử dụng trong Android, IOS và những ứng dụng có nền tảng khác để quản lý bảo mật người dùng.



Fuzzy Vault Scheme for Biometric Digital Key Protection

8. Giao diện ERC23 (Khả năng tương thích với các blockchain khác)

Versum coin sẽ được phát để triển tiến hành giao diện ERC23, tương thích phiên bản cũ với ERC20 để đảm bảo khả năng tương thích với các chuỗi khác.

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

9. Adapter mở rộng không trực tiếp thiết kế riêng cho ERC20/ERC23 độc quyền (Khả năng tương tác với các blockchain khác)

Multiversum sẽ phát triển một adapter thiết kế riêng cho phép các dòng nội bộ và ngoại bộ của chính các coin và token đến các chuỗi không sở hữu.

10. Adapter mở rộng không trực tiếp thiết kế riêng cho ERC20/ERC23 ngoài (Khả năng tương tác với các blockchain khác)

Multiversum sẽ phát triển một adapter thiết kế riêng để cho phép cái dòng nội bộ và ngoại bộ của coin và token từ chuỗi không sở hữu trong chuỗi của chính nó.

Integrity

11. Proof of Integrity (Giao thức cải tiến)

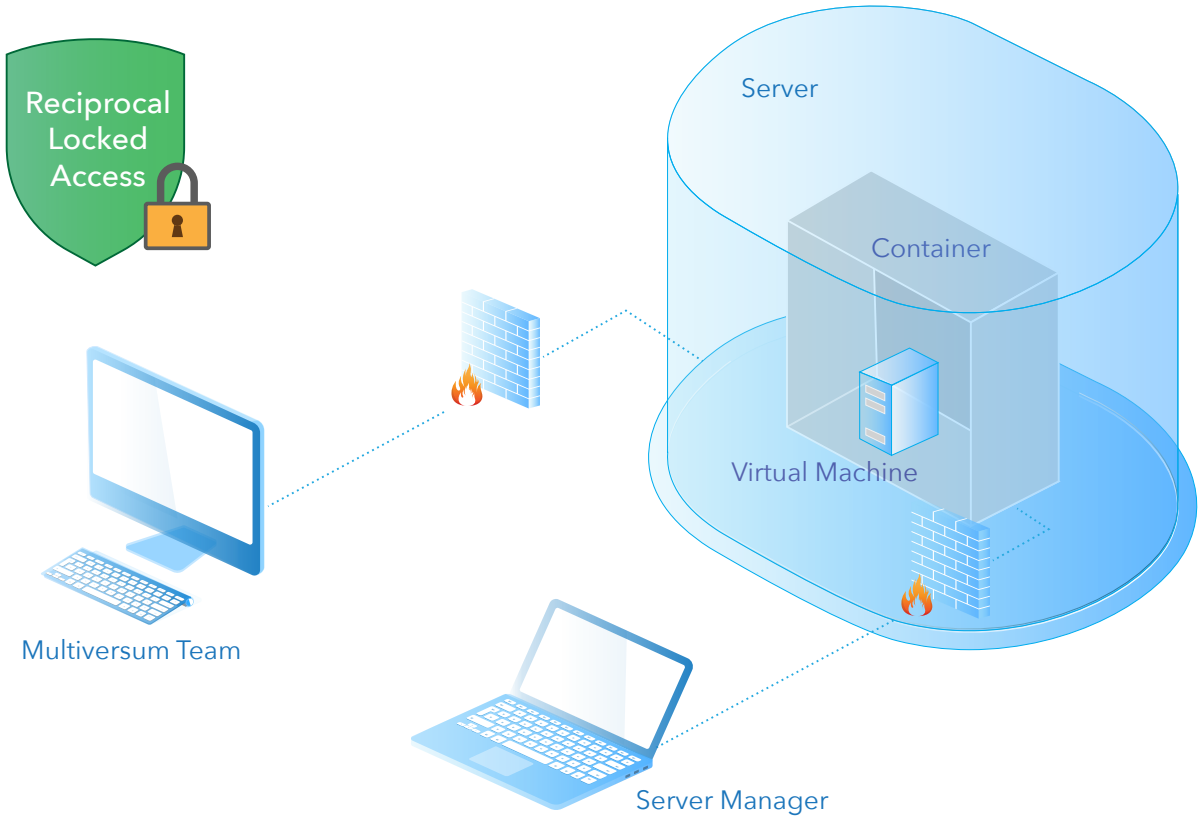
Như là một giải pháp để thay thế giao thức Proof of Work và Proof of Stake trong nhiều trường hợp, Multiversum đề xuất Proof of Integrity: một nhóm các thuật toán có thể xác thực tính hợp thức cryptographic của một node được tổng hợp và sự thống nhất phản hồi từ phần lớn các node. Sự xác thực được hoàn tất trước thách thức về seed ngẫu nhiên, được kết hợp với mã hash đã được tính toán bởi cấu phần ngoài (được bảo vệ từ công nghệ nghịch đảo, và giao tiếp với node phần mềm thông qua kênh đã được mã hoá) của chính phần mềm đó và với dữ liệu transaction. Để hợp thức transaction, kết quả tính toán phải là cùng loại trong một transaction cụ thể, trên mỗi node.

Quy trình này yêu cầu năng lượng tính toán cực kỳ thấp, ngăn được sự thất thoát năng lượng máy tính điển hình trong những giải pháp hợp thức blockchain khác (như PoW, PoS, DpoS), cung cấp bảo mật có cấu trúc, không dựa trên mẫu số liệu hay mẫu Byzatine Consensus, một mẫu khá dễ bị tấn công trong những cluster nhỏ.

Access Denied

12. Khoá truy cập đôi (Bảo mật có cấu trúc)

Các node sẽ được phân phối trong Container Ảo (Visual Containers), với credential không có sẵn tới bộ phận vận hành Máy chủ, ngăn ngừa truy cập; vì thế an ninh được đề cập tới Mô thức Bảo mật Linux Tốt nhất (Linux Security Best Practices), như, ví dụ, SeLinux và/hoặc các gói khác. Trong khi đó, nếu ai đó có credential máy Khách, anh ta sẽ vẫn không thể có quyền truy cập vào đó, không thể truy cập máy chủ chạy node đó. Node này, hiển nhiên, đã được bảo mật bởi khoá truy cập đôi.



13. Đảo ngược từ chối truy cập (cơ cấu bảo mật)

Khoá truy cập (miêu tả tại mục 12) đòi hỏi bài trừ đối ứng của node truy cập tới cả người vận hành máy chủ và cả người sở hữu những node credential; điều này đảm bảo rằng mỗi node không trực tiếp quản lý bởi Multiversum là xác thực và không thể truy cập bởi bất cứ ai, về cơ bản là kể cả tự động hoặc tách biệt khỏi sự tác động bên ngoài của con người. Ba thành phần cơ bản sẽ được phân phối trong container bên cạnh Hệ thống Vận hành và các hệ thống an toàn: Multiversum server tổng hợp code, chứng nhận khoá bất đối xứng để xác thực tới Multiversum cluster (một thành phần đã miêu tả tại mục 11) mà chịu trách nhiệm cho sự tính toán thách thức dựa trên server code hash, chứng nhận, challenge seed và cả dữ liệu transaction.

Kỹ thuật bảo mật tuỳ chọn thêm vào có thể được tiến hành, như là tự động cập nhật container, truy cập credential với mật khẩu ngẫu nhiên trong suốt giai đoạn tổng hợp, để ngăn ngừa bất cứ ai truy cập. Cơ chế này có thể được sử dụng cho việc chứng thực truy cập cluster.

14. Xác nhận chuỗi tương hỗ (kiểm tra tương tác với những blockchain khác)

Multiversum sẽ nghiên cứu tính khả thi của hợp thành chuỗi tích hợp ngoài để có thể lưu trữ trạng thái của những blockchain khác (cuối cùng là trong việc trao đổi token), cung cấp thêm sự hợp lệ cũng như tín nhiệm.

Kỹ thuật tương tự cũng có thể được sử dụng để Multiversum chia sẻ xác nhận trạng thái hợp lệ của chính nó đến những blockchain khác, kiểu như xác nhận "thu hút ngoài" (out-sourcing)

Một giao diện cụ thể sẽ được cung cấp cho chức năng này. Giao diện này cũng cần được xúc tiến giữa các blockchain đang hiện hành và cả việc thực hiện các blockchain tương lai. Đặc điểm này sẽ dựa vào cấu phần không có server, có thể được truy cập sau khi sắp xếp container, cho phép bao gồm adapter đến những chuỗi khác.

15. Tích hợp với Java, Spring và Javascript

Multiversum sẽ cung ứng các giao diện cao cấp được nhóm lại trong thư việc chức năng Java, Javascript và có thể là cả những dòng ngôn ngữ lập trình chính thống khác, cho phép chúng ta chấp nhận kỹ thuật dễ dàng hơn ở mức độ doanh nghiệp cũng như tổ chức cơ quan.

Module tích hợp với framework như Spring cũng sẽ được cung cấp. Loại thư viện này sẽ tạo điều kiện thuận lợi cho việc tích hợp Multiversum với giải pháp độc quyền, cả trong chuỗi cá nhân lẫn MainNet chính thức.

16. Mẫu ACID

Multiversum sẽ thoã mãn mô hình ACID. Cụm viết tắt này nhấn mạnh đặc tính lô-gic được yêu cầu trong transaction.

Để chắc chắn rằng mẫu transaction được đảm bảo, công nghệ thực hiện cần đáp ứng các đặc điểm sau:

Atomicity (nguyên tử): transaction không thể chia tách việc việc thực hiện lệnh, và lệnh trong transaction phải một là được thực hiện hoàn toàn trọn vẹn, hai là không được thực hiện. Việc thực hiện chỉ một phần lệnh là không được cho phép.

Consistency (nhất quán): Bất cứ transaction nào cũng sẽ mang dữ liệu từ trạng thái có hiệu lực sang trạng thái khác. Dữ liệu thường xuyên được truy cập phải hợp lệ theo như các quy tắc đã được định sẵn.

Isolation (riêng biệt): Mỗi transaction phải được tiến hành riêng biệt: lỗi ngẫu nhiên phát sinh trong một transaction sẽ không ảnh hưởng tới các transaction đang tiến hành khác.

Durability (Bền vững): còn được gọi là persistence, đảm bảo chắc chắn rằng một khi transaction được tiến hành, kết quả không thể bị mất vì bất cứ lý do gì (lỗi crash, lỗi khác, mất điện)

17. Mẫu transaction

Multiversum sẽ nắm giữ dữ liệu trong mẫu transaction, đảm bảo rằng tất cả hoặc không có dữ liệu nào trong quan hệ đa chuỗi ngầm sẽ được giữ nguyên, thực thi tính liên kết của những transaction được thực hiện và tính trọn vẹn của dữ liệu.

18. SQL - giống như một ngôn ngữ

Để đơn giản hoá sự phát triển của ứng dụng dựa trên công nghệ cơ sở dữ liệu quan hệ mật (Crypto-relational Database technology) và để parabol hoá đường cong học tập đối lập với công nghệ hiện tại, Multiversum sẽ tập trung vào cú pháp dựa trên SQL để sử dụng các chức năng tiêu chuẩn trong tài nguyên lưu trữ tồn tại độc lập (CRUD)

19. Dòng dữ liệu full route

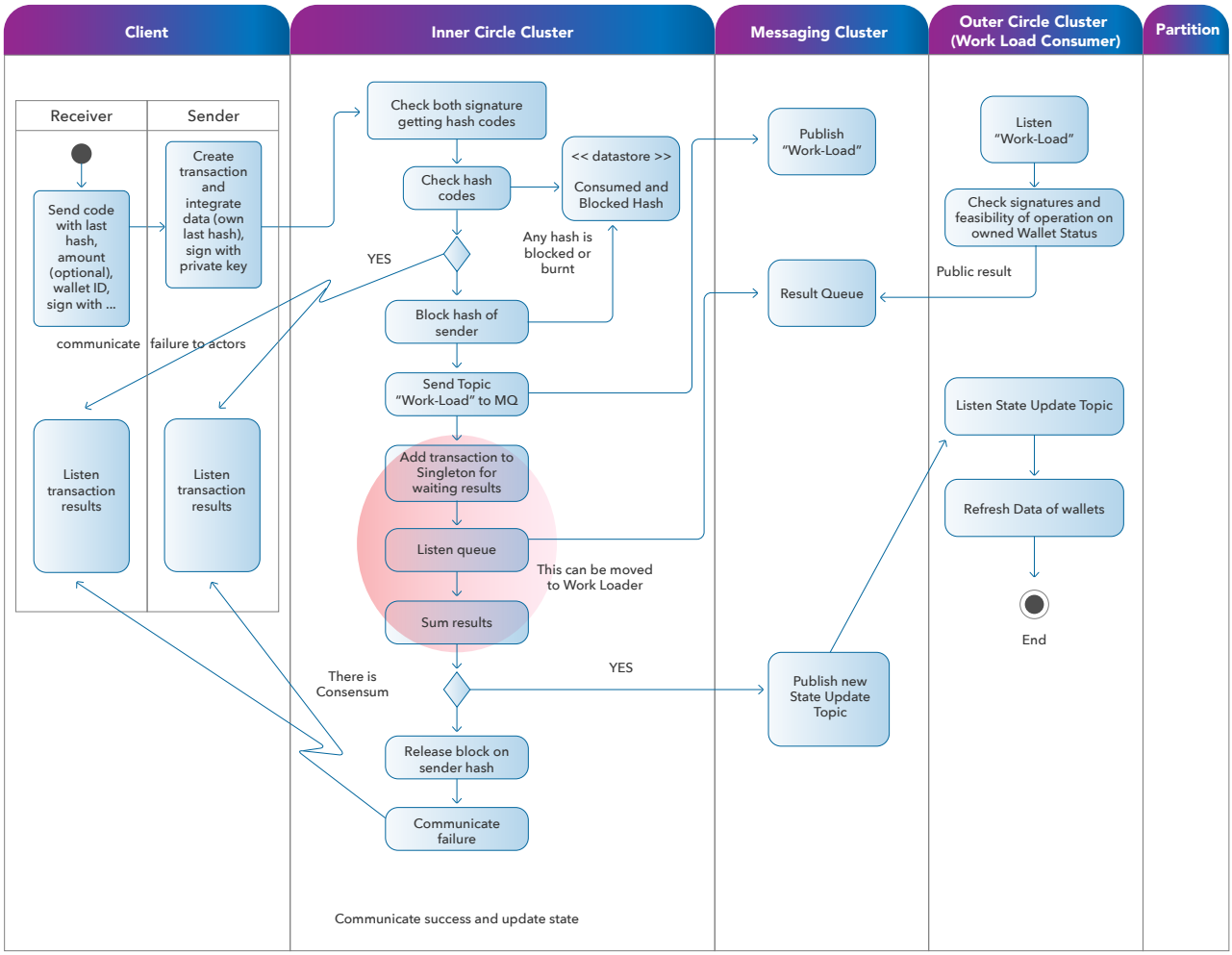
Các quá trình chấp nhận, điều khiển, xác nhận và sự bền vững của một transaction diễn ra với những quy trình được khái quát và đơn giản hoá như sau:

Transaction được gửi tới REST client, với những dữ liệu cần thiết, đăng ký với key cá nhân;

REST client gửi transaction tới leader node thuộc coordination cluster, Multiversum sẽ phân tách công việc thông qua node với giao thức kết hợp độc quyền;

Chúng sẽ đầu tiên chạy kiểm tra hoàn thiện dữ liệu, dấu hiệu, nguồn lưu trữ có sẵn, các

mã hash đã được sử dụng, tình trạng wallet ảo hoặc người sử dụng;
Bất cứ các hoạt động phụ nào bắt nguồn từ ID của người gửi bây giờ sẽ bị khoá trong bộ nhớ khả biến, trong khi các trường dữ liệu cụ thể được hoàn tất (giống như transaction trước đó liên kết với timestamp và mã hash trước);
Transaction được gửi tới Topic Message Queue với giao thức mà phải được xác định (AMQP cho pilot, MQTT và những giao thức khác để xác nhận) và được phân phối song song với các worker node.

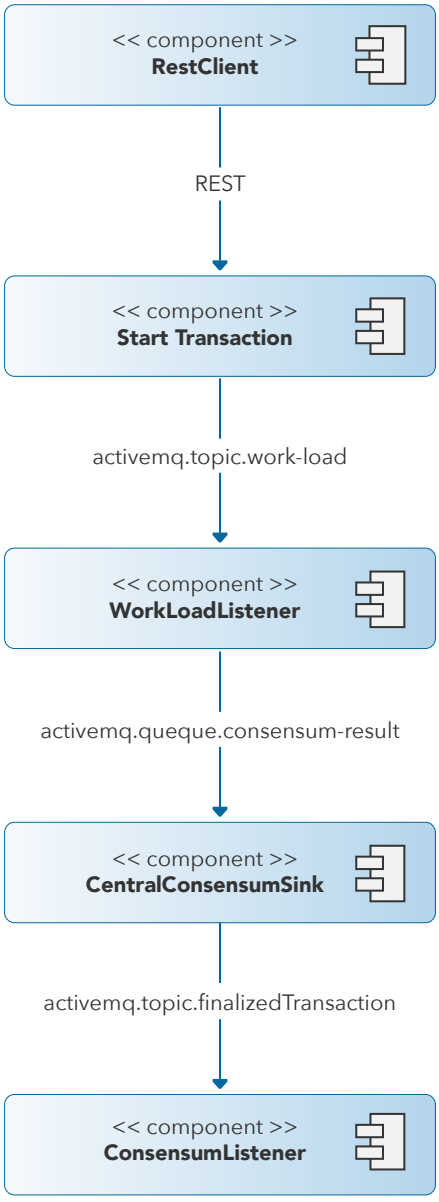


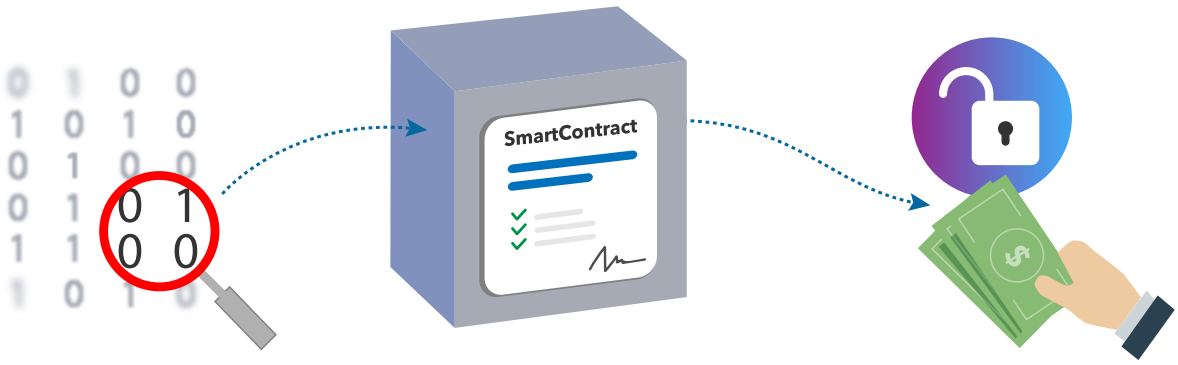
Worker node xác nhận sự quan tâm của chúng trong quá trình thực hiện yêu cầu (chúng có thể đang thiếu các dữ liệu cần thiết, đang bận và có các điều kiện được đánh giá khác) và đi đến việc khởi tạo tình trạng wallet mới, phục hồi các mã hash liên quan thuộc transaction liên kết trước đó và thêm chúng vào bản ghi của transaction. Kết quả chứng thực tính nguyên vẹn bây giờ được thêm vào;

Mã hash đã được tính toán;
Worker node đăng ký transaction trong bộ nhớ và gửi một vote tới coordinator nodes thông qua Message Queue, thu thập kết quả;
Nếu vote và hash thống nhất, coordination node sẽ tiếp tục giữ transaction và bất cứ trạng thái mới nào của wallet, huỷ bỏ bất cứ mã hash nào trước đó và truyền tin chứng thực với hệ thống Topic Message Queue phụ. Worker node bây giờ cũng sẽ tiếp tục giữ transaction và những sự thay đổi trong tình trạng wallet;
Kết thúc tốt nhất trong trường hợp full route

Logic data flux

Detail of process flow





Smart Contracts

Multiversum tin vào sự quan trọng trong việc đề nghị bản giao thức Smart Contracts đã được cải thiện một cách công khai, nhưng vào thời điểm của bài viết này, trừ khi có sự điều chỉnh trong quy mô nghiên cứu, còn không Multiversum chưa quyết định khám phá khả năng này. Vì thế, chúng tôi đang tìm kiếm bao gồm cả trong chính công nghệ Multiversum giải pháp cho Mã nguồn Mở, thứ phù hợp nhất với nhu cầu của chúng ta, để tiến hành tham khảo theo như mẫu cấp phép.

Cơ sở hạ tầng

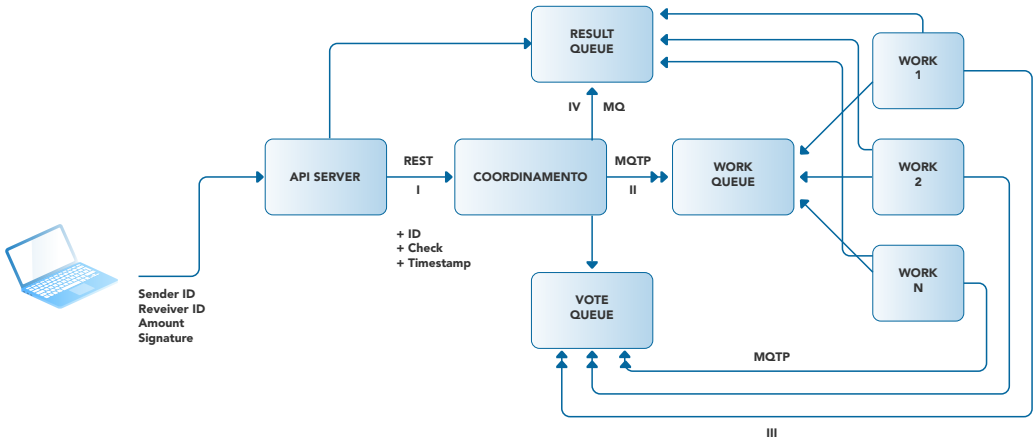
Cơ sở hạ tầng của Multivesum được thiết kế để đảm bảo tính phục hồi nhanh và tính năng "với" (reachability). Nhiệm vụ này đã được hoàn tất trong việc phát triển các khối node mà có thể tự chọn nhiệm vụ cụ thể cho các thành viên của chúng, theo mỗi khía cạnh kỹ thuật của node:

- Công suất tính toán
- Sức chứa bộ nhớ
- Khả năng tương hỗ tiềm tàng
- Sự hoàn thiện chuỗi dữ liệu
- Độ tin cậy của máy móc
- Sự hoài nghi về minh chứng cho tính nguyên vẹn (proof of integrity)

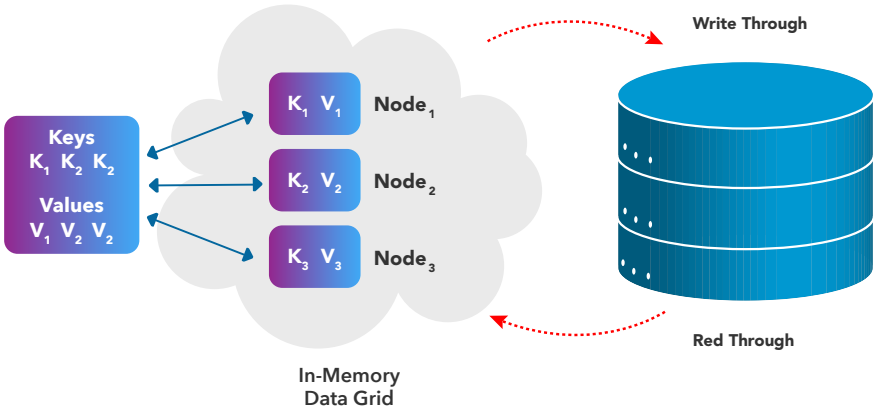
Node sau đó sẽ có một hoặc nhiều các vai trò sau:

- Client node
- Coordination node
- Messaging node
- Work node
- Persistence node
- Back up node

Mỗi node cung cấp xác nhận chứng thực sẽ có thể đăng ký cluster và đảm nhận một vai trò.
Trong trường hợp một hay nhiều node bị crash, cluster sẽ được phân phối các nhiệm vụ một cách tự động thông qua việc tối ưu vai trò.



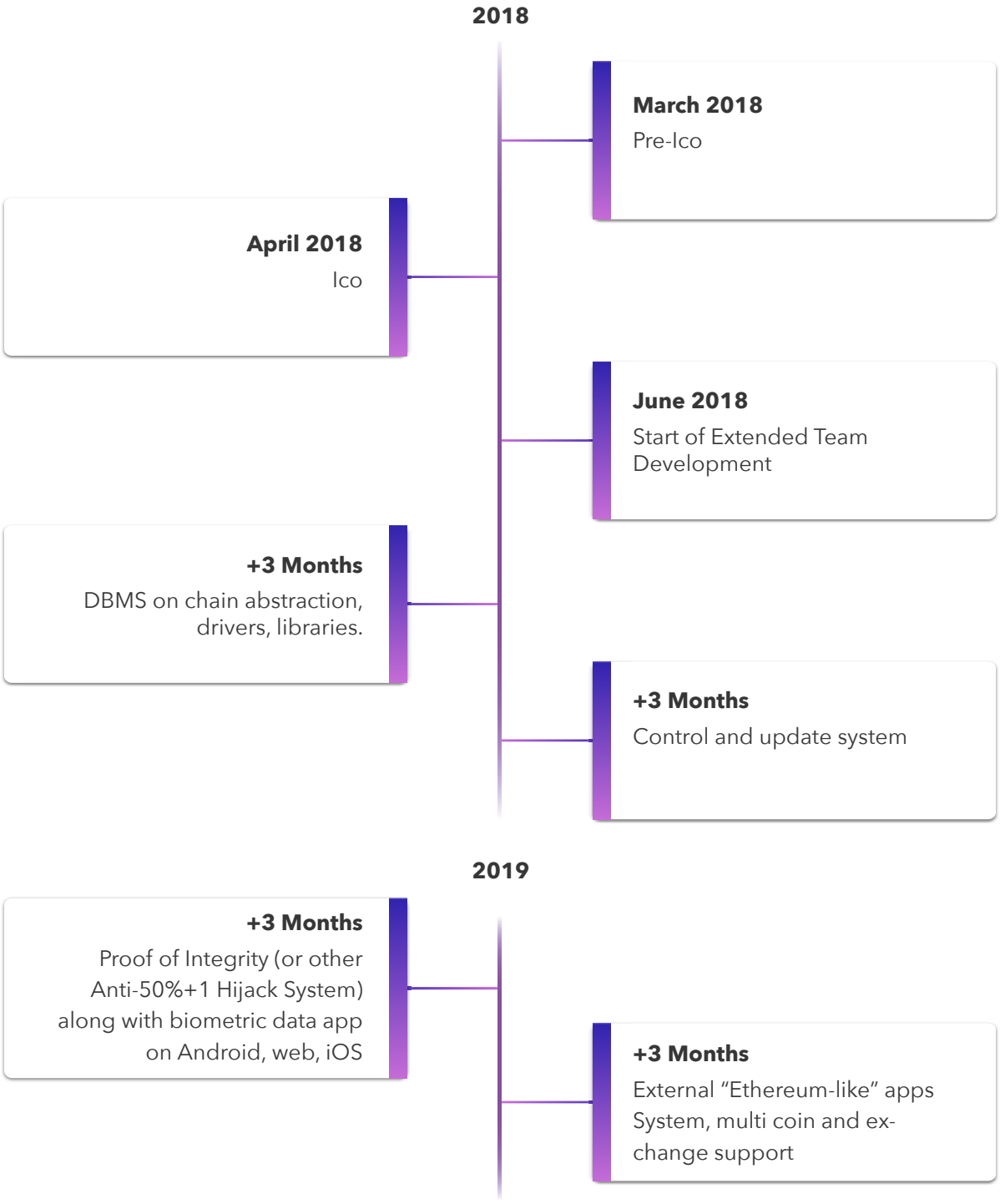
Các thành phần của cache dùng chung thông qua JVM sẽ ở đó như bộ nhớ cơ sở dữ liệu, cho phép:
Read through, ví dụ như việc truy vấn đọc dữ liệu thực hiện trực tiếp trong bộ nhớ khả biến trước khi đưa vào bộ nhớ vật lý.
Write though, tải dữ liệu lên bộ nhớ khả biến trước khi tiến hành chèn hàng loạt vào dữ liệu đang lưu giữ để tối ưu hoá năng suất.



Tính bảo mật ở node

Trong suốt quá trình phát triển, "tiền thưởng hacker" (bounty) sẽ được trao cho các nhà phát triển phát hiện được chỗ hổng và có thể đề xuất được giải pháp hợp lệ.

Technical Road Map



References

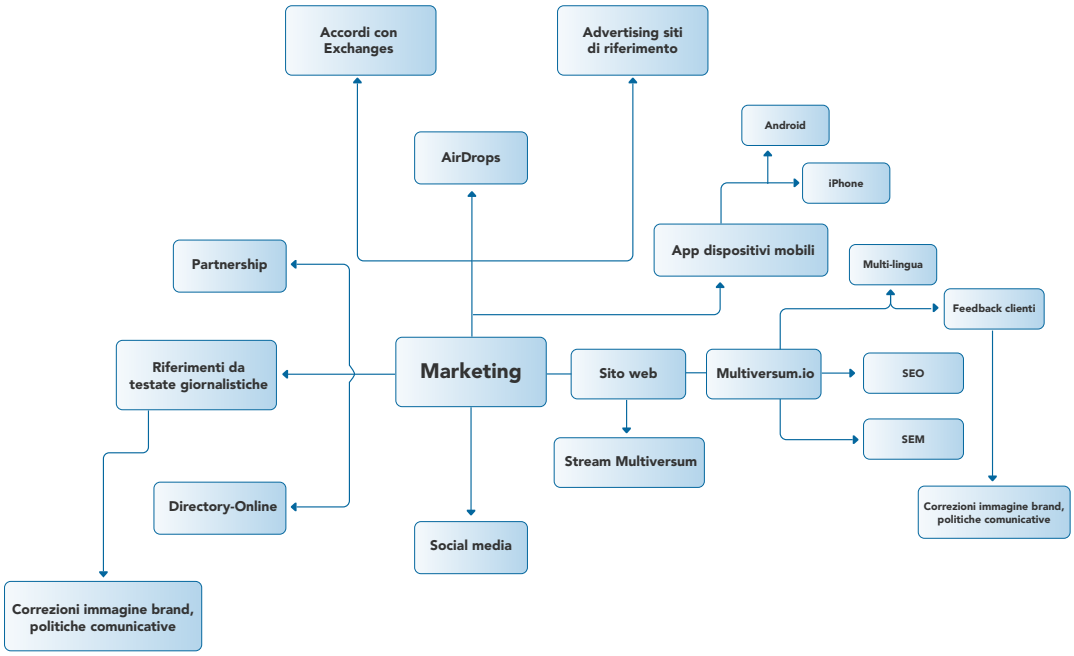
1 https://en.wikipedia.org/wiki/Scalability#Horizontal_and_vertical_scaling
2 https://en.wikipedia.org/wiki/Proof-of-work_system
3 https://en.wikipedia.org/wiki/Proof-of-stake
4 https://en.wikipedia.org/wiki/Agile_software_development
5 https://en.wikipedia.org/wiki/Scope_(project_management)
6 https://en.wikipedia.org/wiki/Shard_(database_architecture)
7 https://en.wikipedia.org/wiki/High-availability_cluster
8 https://en.wikipedia.org/wiki/Single_point_of_failure
9 https://en.wikipedia.org/wiki/Microservices
10 https://en.wikipedia.org/wiki/Serverless_computing
11 http://goo.gl/CVBzJd Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint"
12 https://en.wikipedia.org/wiki/ERC20
13 https://en.wikipedia.org/wiki/Byzantine_fault_tolerance
14 https://en.wikipedia.org/wiki/Security-Enhanced_Linux
15 https://en.wikipedia.org/wiki/Spring_Framework
16 https://en.wikipedia.org/wiki/ACID
17 https://en.wikipedia.org/wiki/Models_of_communication#Transactional_Model
18 https://en.wikipedia.org/wiki/SQL
19 https://en.wikipedia.org/wiki/Message_queue#Standards_and_protocols
20 https://en.wikipedia.org/wiki/Smart_contract
21 https://en.wikipedia.org/wiki/Reachability
22 https://en.wikipedia.org/wiki/Java_virtual_machine

Chiến thuật Marketing

Tiến hành trong thời điểm thị trường IT đang bấp bênh, do đó chúng tôi sẽ cập nhật chiến lược, kỹ thuật giao tiếp và nhiệm vụ của công ty, chú trọng vào tạo ra giá trị cho những cổ đông và đảm bảo sự cân bằng phù hợp nguyên lý quản lý ngắn hạn và dài hạn.

Những điểm chính trong kế hoạch của chúng tôi là:

- Nhiệm vụ công ty.
- Mục tiêu kinh doanh.
- Chiến lược kinh doanh.
- Danh mục vốn đầu tư của hoạt động kinh doanh.



Một trong những công cụ chính sẽ là Truyền thông qua Mạng Xã Hội (Social Media Marketing): các chiến dịch đã tiến hành trên mạng xã hội để tăng cường nhận thức về nhãn hiệu, nhận diện khách hàng tiềm năng, tạo quan hệ và xây dựng những mối quan hệ đầy ý nghĩa với khách hàng.

Những nhà chiến lược Marketing thông qua Mạng xã hội của chúng tôi sẽ tiến hành thực hiện nhiều hành động mà thuộc kế hoạch chiến lược đơn lẻ, bắt đầu với quản trị và các kênh quan sát, sử dụng các công cụ tinh tế và sự phát triển cộng đồng, tập trung vào nội dung, tương tác và chiến thuật, đánh giá hiệu quả dựa trên kết quả thu nhận được.

Mỗi lớp nguyên tố bao bọc vũ trụ đều dày hơn mười lần so với lớp trước đó, và tất cả các vũ trụ tạo thành một khối cùng nhau và xuất hiện như những nguyên tử trong một tập hợp khổng lồ.

Bhagavata Purana 3.11.41

MULTIVERSUM

HERE TO STAY