MULTIVERSUM

HERE TO STAY

الورقة بيضاء v 1.0.5

الأعمال | تقني

العربية

06.02.2018

المؤلفون: فريق مولتيفرسوم

www.multiversum.io

هناك عدد لا يحصى من الأكوان إلى جانب هذا،
وعلى الرغم من أنها كبيرة بشكل غير محدود، فإنها تتحرك مثل الذرات في نفسك.

Bhagavata Purana 6.16.37

Multiversum

جميع الحقوق محفوظة 2017 -2018

Multiversum
الهوية والرسالة

رائدة العملات المشفرة (كريبتوكيرنسيز)، بيتكوين، جنبا إلى جنب مع مختلف شبيهاتها المستنسخة واستنادا إلى خوارزمية إثبات العمل للتحقق من صحة المعاملات، تعتبر الجيل الأول من الblockchains بلوكشينز

الجيل الثاني، مع إثريوم الرائدة في مسؤولية العقود الذكية بتمكين بلوكشينز، هو بدلا من ذلك متنوع اكثر، مما يتيح سهولة تحويل الأملاك الى العملة (توكنtoken.). كل من التصميمين لديهم كفاءة للغاية في استخدام قليلا من الطاقة وسرعة متوسطة-منخفضة للتحقق من صحة المعاملات لكل كتلة.

حل قضايا قابلية التوسع والسرعة، واستهلاك الطاقة هو الهدف من حلول الجيل الثالث بلوكشين، وذلك باستخدام أساليب وتقنيات مختلفة مثل خوارزمية إثبات الحصة والتحقق من صحتها، والتوجيه خارج السلسلة، وسلاسل الرسوم البيانية، ومركزية كاملة أو جزئية.

الجيل الرابع يذهب أبعد من ذلك، محققا حلول أسرع وأكثر قابلية للتوسع ومحاولا، في الوقت نفسه، ليصبح قادر على المنافسة من منظور الأعمال التجارية: سلاسل بسيطة من البيانات ليست مرنة بما فيه الكفاية لتلبية احتياجات البيئة للشركات، حيث هياكل البيانات المعقدة تحتاج إلى تنظيم في الجداول (كما هو الحال في قواعد البيانات الارتباطية).

في الوقت نفسه، تحتاج هذه الهياكل إلى التحقق من صحتها وجعلها غير قابلة للتغيير مع تقنيات بلوكشين- للتتبع، وزيادة التتبع والأمن. بعبارة أخرى، الجيل الرابع بلوكشين يجلب هذه التكنولوجيا إلى تطبيق إنتاج اولي وكامل، ويوسع العرض الحالي الموجه نحو الأعمال من حيث تخزين البيانات، اللامركزية للتطبيق، التدقيق، الأمن، الموثوقية.

مولتيفرسوم(MTV) يقدم تنظيم البيانات المعقدة بدلا من تسلسل البيانات، تقسيم سلسلة وضمها مرة أخرى للسماح لمزيد من التدرجية والتوازي، ومفهوم إثبات التحقق من سلامة (أي دليل التشفير من رمز الخادمserver code-) بدلا من إثبات العمل أو إثبات حلول حصة المتداول.

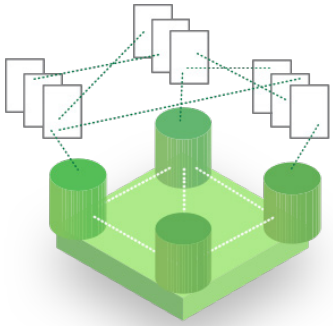
وعلاوة على ذلك، ستتصف مولتيفرسوم بميزة تكامل ERC٢٠ / ERC٢٣، مما يسمح باستضافة للقطع النقدية والتوكنز من الحلول الأخرى على السلسلة لدينا، والعكس بالعكس، مع خدمات كاتب العدل كطريقة تأكيد خارجية.

في الوقت نفسه، جنبا إلى جنب مع هذه الابتكارات، ونحن بالتأكيد سوف نستخدم العديد من الحلول جيدة المنفذة من زملائنا مع مرور الوقت.

Multiversum

الجيل الرابع بلوكشين ارتباطي

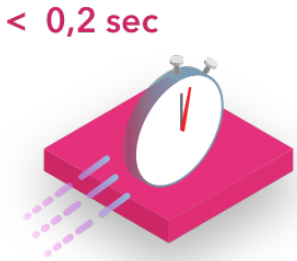
لماذا مولتيفرسوم هي بلوكشين 4.0 ؟



بلوكشين ارتباطي

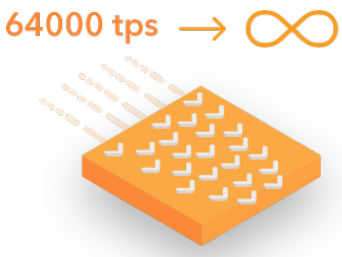
بلوكشين العلامة التجارية الجديدة التي تتميز أنواع مختلفة من البيانات،

ذات الصلة في هيكل متعدد الأبعاد.



سرعة المعاملات

في أقل من 2.0 ثانية يتم تحويل الأموال عبر محافظ، بما في ذلك التحقق من صحة المعاملات. من بين الأسرع في العالم.



المعاملات الإنتاجية

قابلية لا مثيل لها: ما يصل إلى 64000 Tps (1000 Tps / الأساسية) على ملقم 64 النوى.

إثبات النزاهة

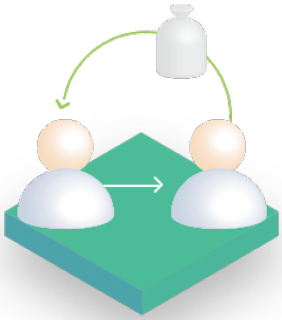
سيتم استبدال PoS (دليل على حصة) PoI(إثبات النزاهة).

محفظة الجيل التالي

أمن متطور في الدخول وتحويل الأموال مع المدخلات البيومترية.

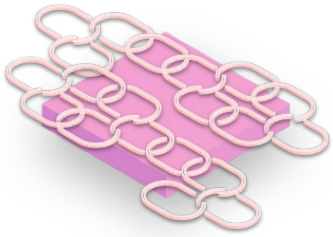
صديقة للبيئة

ستكون لمعاملة مولتيفرسوم تكاليف ضئيلة والبصمة البيئية بجانب الصفر.



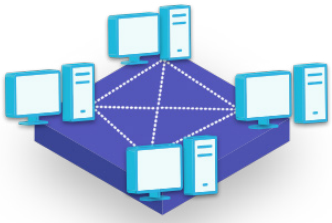
التراجع

يمكن تفعيل التراجع الاختياري للتوكنز التي تستضيفها مولتيفرسوم.



سلاسل قابلة للتقسيم

تحسين الموارد بين العقد بسبب قابلية السلسلة.



تخصيص عقد الاسترداد

MTV العقد المنتشرة في جميع أنحاء العالم من أجل الموثوقية والتعافي من الكوارث العالمية.

التقديم العام

بلوكشين الحالي مثال رائع من الفن

الشخصيات الرائدة من ظاهرة بلوكشين لهم سمة مشتركة: سلامة وموثوقية ملحوظة. وفي الوقت نفسه، فإننا ندفع ثمن هذا من حيث قوة معالجة ضخمة، تلوث غير مقبول، وارتفاع تكاليف المعاملات، والبطء الذي لا يمكن أن يمثله معايير التقدم التكنولوجي الحالية، وإعطاء إجابة فنية معقولة لحالات الاستخدام المالي والتجاري الحديثة.

ويعزى هذا البطء إلى عدم وجود قابلية توسع أفقية (1)، أي زيادة القدرة الحسابية التي تم الحصول عليها فقط بإضافة المعالجات بدلا من استبدالها بأسرع الإصدارات. سبب آخر لهذا البطء هو ملازم السلامة لآلية بلوكشين الحالية ، المصممة لمنع أي شخص من الاستيلاء على غالبية التجمعاتبجعلها مكلفة للغاية من حيث القوة الحسابية و / أو التكلفة (دليل على العمل والدليل على الحصة Proof of Stake[3] and Proof ofWork[2]).

وعلاوة على ذلك، بلوكشينز الحالية هي ترابط بسيط من كيانات بيانات واحدة متغيرات. إعادة بناء فعلي لهذه الكيانات ينطوي على سلسلة كاملة المسح الضوئي، مما يؤدي إلى تباطؤ أكبر في النظام واستخدام الموارد.

هذا التبسيط يجعل بلوكشينز غير كافية للأغراض العلمية والصناعية، كما يمكن أن تصبح المتطلبات من حيث هياكل البيانات معقدة للغاية.

وعلاوة على ذلك، تتوقف الإجراءات الأمنية على مستوى البيانات لأنها لا تضمن سلامة المستخدم، مما يجعلها من المستحيل استرداد النقود المفقودة أو المسروقة والتوكن حتى لو كانت تقع على السلسلة،أو لمنع الحسابات الخبيثة.

وأخيرا، هناك مسألة أخرى هي التجزؤ وعدم التجانس بين العملات الخفية، الغير قادرين على التواصل مع بعضهم البعض وتعيش في أكوان لا علاقة لها ببعض.

التبني العالمي لمولتيفرسوم و بلوكشين

تكنولوجيا مولتيفرسوم تدفع بلوكشين التقليدية خارج حدودها الحالية، بتعزيز طبقة البيانات من خلال التحقق الذاتي وتوزيع هياكل كيانات البيانات المنظمة، ذات الصلة واحدة إلى أخرى عن طريق الروابط الرمزية.

وهذه التكنولوجيا تضع الأسس لنظام لامركزي وموزع لتماسك التحقق الذاتي للمعاملات: بلوكشين مولتيفرسوم.

مولتيفرسوم يسمح، بدلا من نموذج بلوكشين للبيانات القائم والبسيط، بإنشاء قاعدة بيانات التشفير الارتباطية (وهو حل تخزين البيانات المتقدمة والمنظمة) والتي تمكن التعامل مع سلسلة من هياكل البيانات المجمعة المتعلقة بعضها البعض في الرسوم البيانية المعقدة، ليس فقط نوع بيانات واحد. العلاقات هي الآن مواطنين من الدرجة الأولى من بلوكشين ويتم التأكد من أساليب التشفير.

كل واحد منهم، عند طلب تغيير الحالة، سيكون لها تقسيم خاص بها من فرع السلسلة الفرعية الأصلي، التي ستعود بعد العملية، من أجل التحقق من صحتها.

ولذلك مولتيفرسوم هي تكنولوجيا بلوكشين متطورة، وتقدم ميزات فريدة من نوعها للتغلب على المضايقات التي تم تحليلها سابقا، مع مجموعة التحقق المشفر وتقنيات التوزيع لتناسب كل بيئة: الإدارية، الصناعية، المالية والحكومية.

واحدة من الأهداف مولتيفرسوم الرئيسية هو تقديم للسوق، في كل لحظة، المنتج المتاح الأكثر تطورا: هذا سيكون ممكنا باعتماد منهجية تطوير البرمجيات AGILE(4) أجيل.

وتنطوي منهجية أجيل على تخفيض كبير في المشاركة المبدئية في تصميم المشروع لصالحها من تثمين التجارب التي صودفت أثناء تطوير المشروع، والتي تظهرالفرص والتهديدات الصعب التنبؤ بها مسبقا، ومكافأة أفضل الممارسات، وترك تلك الغير كافية.

أجيل هو معيار معمول بها لتطوير البرمجيات ويحث المطورين ، أصحاب المنتجات والمستثمرين للنظر في نطاق المشروع على أنه مرن وقابل للتكيف بسهولة مع احتياجات السوق.

وعلاوة على ذلك، في مثل هذا القطاع المتطور بسرعة والبرمجيات، الإفراج عن منتج بعد ستة أشهر من الدراسة وسنة التنفيذ، عندما كان تصور متناسب مع احتياجات السوق قبل ثمانية عشر شهرا ، يعني تقديم منتج عفا عليه الزمن الذي يعطي إجابات على القضايا القديمة ، والتي ربما تم حلها من قبل المنافسين والافتقار إلى الردود على التحديات التي تم إنشاؤها للتو.

أجيل، بدلا من ذلك، يعطي الفرصة لتقديم المنتج الأكثر ابتكارا للسوق وقت التسليم.

السرعة والتكنولوجيا

واحدة من نقاط القوة لهذه التكنولوجيا هو في الواقع السرعة، وذلك بفضل قدرتها لتشغيل المعاملات المختلفة بشكل متوازي وآلية الانقسام-العودة من بلوكشين لدينا.

هذه الميزات تسمح لزيادة قابلية التوسع الأفقية، وزيادة قدرة معالجة المعاملات بإضافة قوة حاسوبية إضافية إلى الحالية، مما يجعل كل عقدة تعد، كأداء حكيم.

قابلية التوسع الأفقي

فوائد مولتيفرسوم من اثنين من الميزات المحددة لتحقيق أقصى قدر من كفاءة النظام:

١- السلسلة الرئيسية قادرة على تحسين هياكلها من خلال تقسيمها بشكل مستقل في سلاسل فرعية متعددة، وفقا للموارد المطلوبة وتيارات البيانات، موازية العمل عبر المواضيع المتعددة والعقد.

يتم تنفيذ عملية تقسيم السلسلة حتى تطبيع أحمال العمل، عندها، لا يزال بشكل مستقل، تصبح السلسلة كاملة مرة أخرى. كل هذا ممكن بسبب تقنية تسمح لكل كتلة من السلسلة بتفعيل سلسلتين فرعيتين مختلفتين ومن رابطين واردين ومختلفين.

٢ - تقطيع البيانات[٦]، أي تقنية تسمح بتوزيع البيانات بين عقد متعددة.

بالنظر إلى سلسلة بيانات ABC وثلاث عقد نظامية، سيكون لدينا توزيع للبيانات على النحو التالي:

AB

BC

CA

يسمح هذا التقسيم الفرعي بسرعة أعلى لمعالجة المعاملات، حيث أن استعلامات البيانات سوف تؤثر فقط على العقد الفرعية، محسن كل خطوة.

ميزة أخرى هامة للغاية من التكنولوجيا لدينا هي التوفر العالي[٧]: فرصة الاعتماد على نوع كتلة تضمن استمرارية الخدمات حتى في حالة اغلاق بعض العقد في الشبكة.

باستخدام المثال السابق(ABC للعقد) جاري حاليا، ان توقفت عقدة C نجد العقد A و B لا تزال تعمل تماما، مما يسمح استمرارية الخدمة دون أي نوع من فقدان البيانات بقدر ٥٠٪ + ١ من العقد لا تزال عاملة .

وبهذه الطريقة، في حالة فشل عقد متعددة، ستقوم المجموعة بإعادة تنظيم توزيع البيانات بشكل مستقل مع كل عقدة، إلى حين استعادة التشغيل الكامل.

بيئة

مولتيفرسوم هو أيضا صديقة للبيئة: واحد من أهدافنا الرئيسية هو خفض الطاقة الحسابية اللازمة للتحقق من التشفير وبالتالي تجنب التعدين (إثبات العمل)، هدر كبير من الطاقة والموارد.

بدلا من هذه التقنية التي عفا عليها الزمن، نقوم بتنفيذ الدليل على النزاهة(POI)، وهو البروتوكول الذي يقوم بالتحقق من صحة التشفير عن طريق التحقق من صحة البرنامج الذي يحل كل استمرارية للصفقة.

إدارة البيانات

مولتيفرسوم، مع قاعدته لتشفير البيانات الارتباطية ممكن بسهولة من هيكلها دون حدود ربط البيانات.

سيكون لكل محفظة سلسلة من الحالات، وستكون مرتبطة بشخص (المستخدم)، وتغيير حالة المحفظة لجديدة تشمل حقلين للبيانات:

الحالة السابقة، للتحقق من صحة التفعيل.

وصلة إلى آخر معاملة (أو إلى آخر وصلة للسلسلة الرئيسية) بحيث يكون رابط التغيير الجديد للحالة معروف.

بعد التغيير، سيتم إضافة تعديل الصفقة و رابط الحالة المعدلة سينضم إلى السلسلة الرئيسية.

ولذلك، فإن الصفقة الجديدة سترث جزئين: واحد من رابط الحالة وواحد من الصفقة السابقة، وبهذه الطريقة، فإن جميع العمليات ستفعل تلك السابقة المتعلقة بالصفقة نفسها.

هذا الحل المتقدم، قادر على إدارة سيناريوهات البيانات المعقدة، سيسمح للناس بتنفيذ أي نوع من تطبيق التكنولوجيا لدينا، وضمان نشر مؤسساتي، حكومي، مالي وصناعي في جميع أنحاء العالم، وبذلك تقديم كون بلوكشين خطوة واحدة إلى الأمام.

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

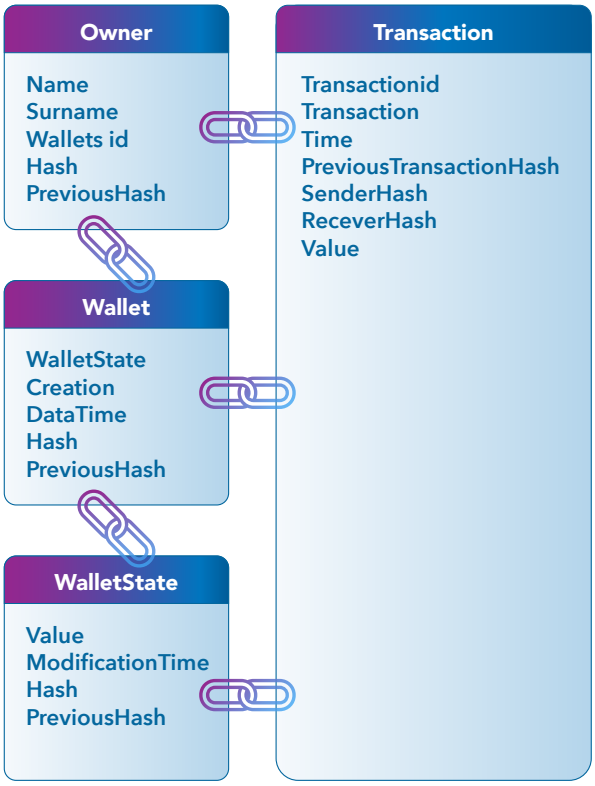
Native on chain adapter for own ERC20
(Interoperability with other BC)

ERC23
(Interoperability with other BC)

مهمة مولتيفرسوم

يهدف مولتيفرسوم إلى زيادة الأجيال في عالم بلوكشين، وكنقاط بيع فريدة، نقترح الأهداف التالية:

1. تحقيق تشفير ارتباطيDB مع هياكل البيانات المعقدة المفعلة ذاتيا
2. سلاسل قابلة للانقسام / إعادة الانضمام استنادا إلى عبء العمل الحالي للنظام (العمل المتوازي)
3. تجزئة البيانات (العمل المتوازي)
4. عرض API المتقدم
5. التراجع (أمان المستخدم)
6. محافظ قابلة للتجميد (أمن المستخدم)
7. دمج البيانات البيومترية كبذرة للتوقيع الإلكتروني
8. واجهةERC٢٣ (قابلية التشغيل البيني مع بلوكشينز أخرى)
9. محولات أصلية خارج السلسلة لERC٢٠ / ERC٢٣ (قابلية التشغيل البيني مع بلوكشينز أخرى) الخاصة بها
10. محولات أصلية خارج السلسلة لضيوفERC٢٠ / ERC٢٣ (قابلية التشغيل البيني مع بلوكشينز أخرى)
11. إثبات النزاهة (بروتوكول الابتكار)
12. قفل الدخول المزدوج (الأمن الهيكلي)
13. رفض الدخول العكسي (الأمن الهيكلي)
14. تأكيد تبادل السلسلة (التشغيل البيني مع بلوكشينز أخرى)
15. التكامل لJava, Spring and Javascript
16. نموذج ACID
17 - نموذج المعاملات
18. لغة (مثل SQL)



1.تحقيق تشفير ارتباطيBD مع هياكل البيانات المعقدة المفعلة ذاتي

مولتيفرسوم لديه مهنة قوية نحو الاستخدام الصناعي والمؤسساتي، سياقات لدينا لها هياكل بيانات معقدة، من المستحيل أن تكون ممثلة بطريقة فعالة وطبيعية مع سلسلة بسيطة.

ونحن نهدف إلى أن نصبح أول قاعدة تشفير ارتباطية للبيانات في السوق، لامركزية أو ببساطة موزعة إذا لزم الأمر.

وتستمد هذه القدرة من تصور الكيانات القابلة للتسلسل: ففي التكنولوجيا لدينا، يمكن تقسيم السلسلة الأولية إلى سلاسل ثانوية تحتوي على مجموعات مختلفة من الكيانات والسجلات.

وستندمج هذه الكيانات مجددا في آخر حالة ثابتة لها، وبعد التعديلات المطلوبة، فإنها سوف تعود مرة أخرى إلى الرابط الأخير منالسلسلة الأولية، لتصبح واحدة.

ويفترض السطح البيني «القابل للتسلسل» نوعا من السجل المتضمن تجزئتين أو أكثر من السجلات السابقة، مصادقا ليس على سلسلة واحدة فحسب، بل على عدة سلاسل فرعية.

في تنفيذ معيار مولتيفرسوم، المستخدام من قبل العملة فيرسوم(Versum coins,)، الكيانات قابلة للتسلسل التي تتعايش على السلسلة تنتمي إلى أربعة جداول: المستخدم، المحفظة، حالة المحفظة، والمعاملات، ذات الصلة بعضها البعض وتأكد أنفسها بالتناوب.

2. سلاسل قابلة للانقسام / إعادة الانضمام استنادا إلى عبء العمل الحالي للنظام (العمل المتوازي)

بنفس القدرة على اشتقاق وصلات متعددة من واحد وانضمامهم مرة أخرى تسمح التكنولوجيا لاستخدام تحليل عبء العمل للاشارة إلى الكتلة الحاجة إلى تقسيم السلسلة الأولية في سلسلتين ثانويتين (وربما تقسيم أنفسهم مرة أخرى إلى أجل غير مسمى) عندما يرتفع طلب تنفيذ المعاملات. وبمجرد أن ينخفض عبء العمل مرة أخرى، يسمح لعدة سلاسل فرعية موجودة مسبقا بالربط مرة أخرى والتفعيل.

هذه الآلية تسمح العمل الموازي مع الحفاظ على السلامة لسجل الصفقة.

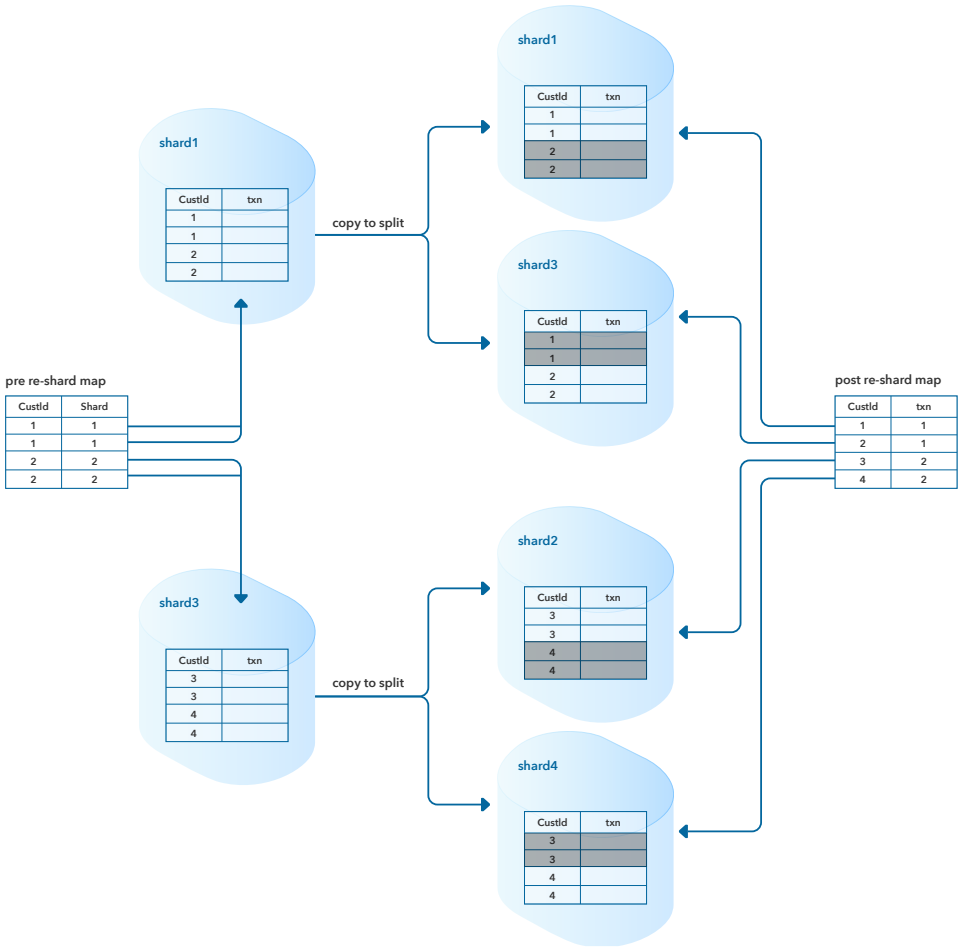
3. تجزئة البيانات (العمل المتوازي)

سوف تحتوي كل عقدة على بيانات السلسلة بأكملها أو مجرد جزء من السلسلة.

وعندما تكون هناك حاجة إلى تقطيع البيانات، ستضع العقد التنسيقية أنماطا محددة لتقسيم البيانات، من أجل تحسين توزيعها وفقا لحجم العمل الحالي. وفقا لتوفر التقنيات العالي، الموثوقية والثبات بضمان دائم، حتى في حالة فقدان مفاجئ لجزء من الكتلة، بالنظر إلى أن لا يقل عن ٥٠٪ + ١ من العقد تبقى على قيد الحياة.

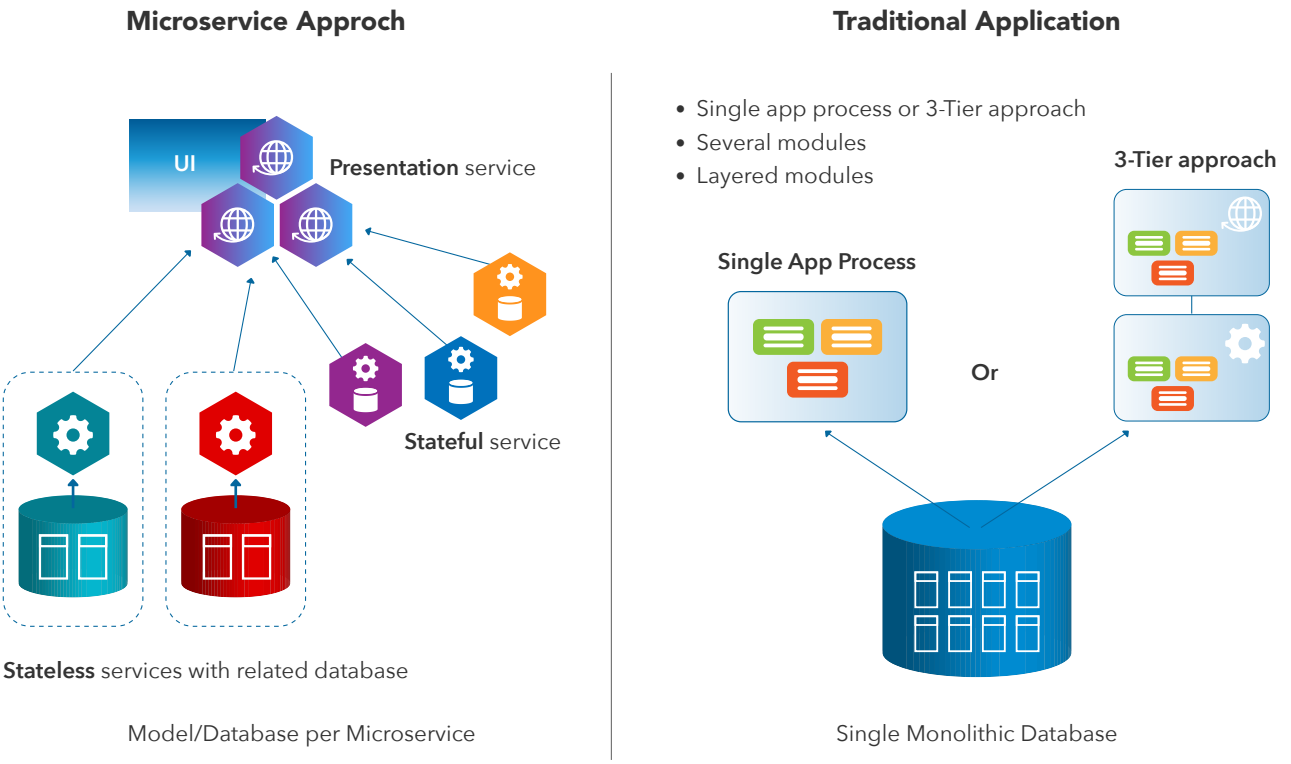
وستتمكن هذه العقد، بعد تعطل الكتلة الجزئي، من إعادة توزيع هياكل البيانات وإعادة تنظيمها لكي تتمكن من مواجهة تحطم مجموعة جزئية أخرى في أقرب وقت ممكن.

وباستخدام الأسلوبين ٢ و ٣، ستحظى بلوكشين مولتيفرسوم بقدرة معززة للعمل المتوازي وعلى تقطيع البيانات، مما يعني قابلية التوسع الأفقي، زيادة الأمن، التوافر العالي، مرونة النظام، غياب نقطة عطل واحدة[8] ، والتعافي الذاتي من الكوارث.



4. عرض API المتقدم

وضعت على منصة تقوم على كل من Microservices[9] و سيرفيرليس Serverless model[10]، ستكون مولتيفرسوم قادرة على تقديم وظائف API المتقدمة، الحديثة والآمنة، والتكيف على كلا الهيكلين.



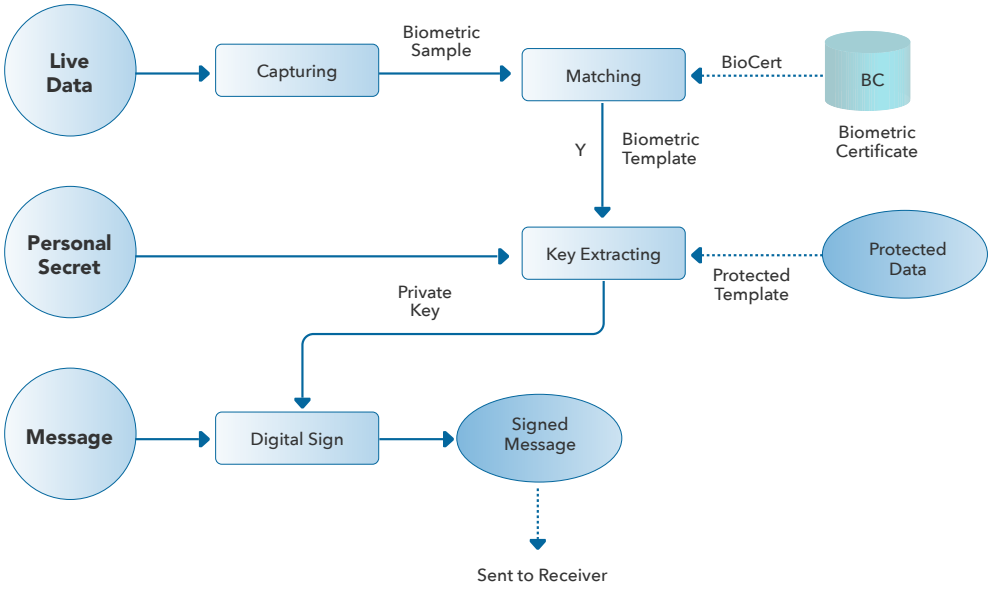
5. التراجع (أمان المستخدم)

تسمح تقنيتنا، في سياق المعاملات، بتراجع العمليات غير المرغوب فيها، أي استعادة حالة مبكرة دون تعطيل مصداقية التحقق من السلسلة، من خلال تنفيذ مجموعة من حالات استرداد المعاملات. هذه الميزة قابلة للتمكين ، اختياريا، على كافة الرموز والتطبيقات المستضافة على بلوكشين مولتيفرسوم.

6. محافظ قابلة للتجميد (أمن المستخدم)

ستنفذ فرصة إدراج ميزة تجميد المحفظة في حالة الأنشطة غير المشروعة أو المشبوهة بعد دراسة جدواها على الجانب المنطقي للأعمال.

تطبيقات الملكية، التي بنيت على بلوكشين مولتيفرسوم، سيكون لديها خيار تنفيذ هذه الميزة إذا رغبت في ذلك.



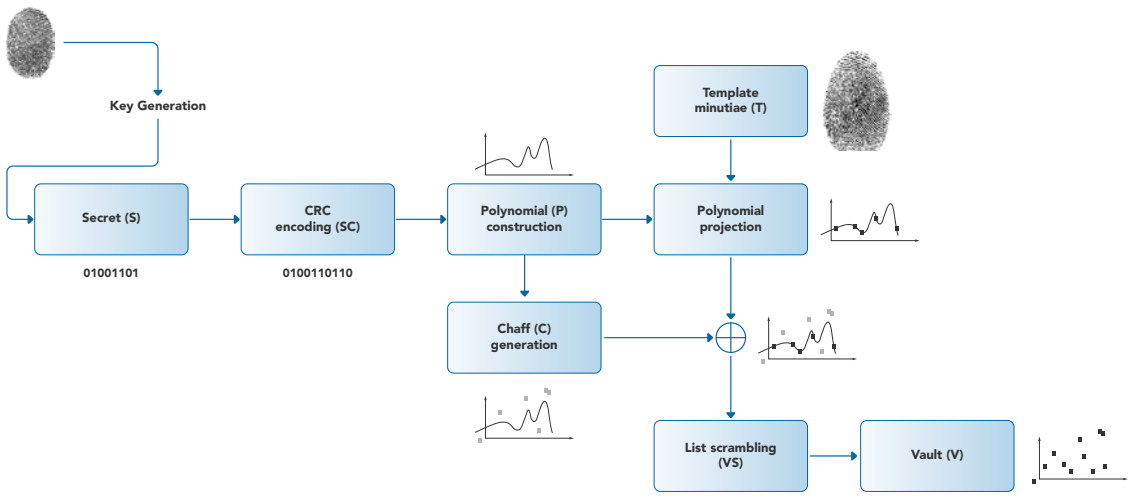
Biometric Digital Key Generation Framework

7. دمج البيانات البيومترية كبذرة للتوقيع الإلكتروني

بدءا من البحث الذي قام به (Je-Gyeong Jo, Jong-Won Seo and Hyung-Woo Lee'swork[11])، سيقوم فريق مولتيفرسوم بتقييم جدوى البيانات البيومترية مثل بصمات الأصابع وفحص الشبكية والتوقيع البياني كمصدر لمفتاح التشفير غير المتماثل لضمان صحة هوية الموقع.

وسيتم تقييم سلامة البيانات المشفرة واستخدامها كمصادقة في الحجج القانونية.

وعلاوة على ذلك، سيتم استخدام البيانات البيومترية على Android, IOS وغيرها من منصات التطبيقات لإدارة أمن المستخدم.



Fuzzy Vault Scheme for Biometric Digital Key Protection

8. واجهةCRE٣٢ (قابلية التشغيل البيني مع بلوكشينز أخرى)

وسيتم تطوير العملات فيرسوم تنفيذ ERC23 واجهة، وهذا هو متوافق مع $ERC20_{12}$ إلى الوراء، لضمان التشغيل البيني مع سلاسل أخرى.

قابلية التشغيل البيني مع إجمالي العرض ()؛

توازن متبادل من (وصلة هوية المحفظة)؛

تحويل بولان **boolean** (وصلة هوية محفظة المتلقي ، قيمة متبادلة)؛

تحويل بولان **boolean** من (وصلة هوية محفظة المرسل ، وصلة هوية محفظة المتلقي ، قيمة متبادلة)؛

موافقة بولان **boolean** (وصلة هوية محفظة المنفق ، قيمة متبادلة)؛

حد مسموح للتبادل (وصلة هوية المحفظة ، وصلة هوية محفظة المنفق)

تحويل بولان **boolean** (معرف محفظة المرسل، وصلة هوية محفظة المتلقي ، قيمة متبادلة)؛

موافقة بولان **boolean** (وصلة هوية محفظة المرسل ، وصلة هوية محفظة المنفق ، قيمة متبادلة)؛

9. محولات أصلية خارج السلسلة لERC20/ ERC23 (قابلية التشغيل البيني مع بلوكشينز أخرى) الخاصة بها

سوف مولتيفرسوم تطوير محول الأصلي للسماح تدفق الواردة والصادرة لعملاتها الخاصة والرموز إلى سلاسل غير الملكية.

10. محولات أصلية خارج السلسلة لضيوفERC20/ ERC23 (قابلية التشغيل البيني مع بلوكشينز أخرى)

سوف مولتيفرسوم تطوير محول الأصلي للسماح تدفق الواردة والصادرة من القطع النقدية والرموز من سلسلة غير الملكية على سلسلة خاصة بها.

Integrity

11. إثبات النزاهة (بروتوكول الابتكار)

كحل لاستبدال دليل العمل والدليل على الحصة(PoWوPoS) في أشكالهم المختلفة، مولتيفرسوم يقترح إثبات النزاهة(PoI): مجموعة من الخوارزميات قادرة على التحقق من صحة التشفير لعقدة مجمعة ووحدة الاستجابة من غالبية العقد.

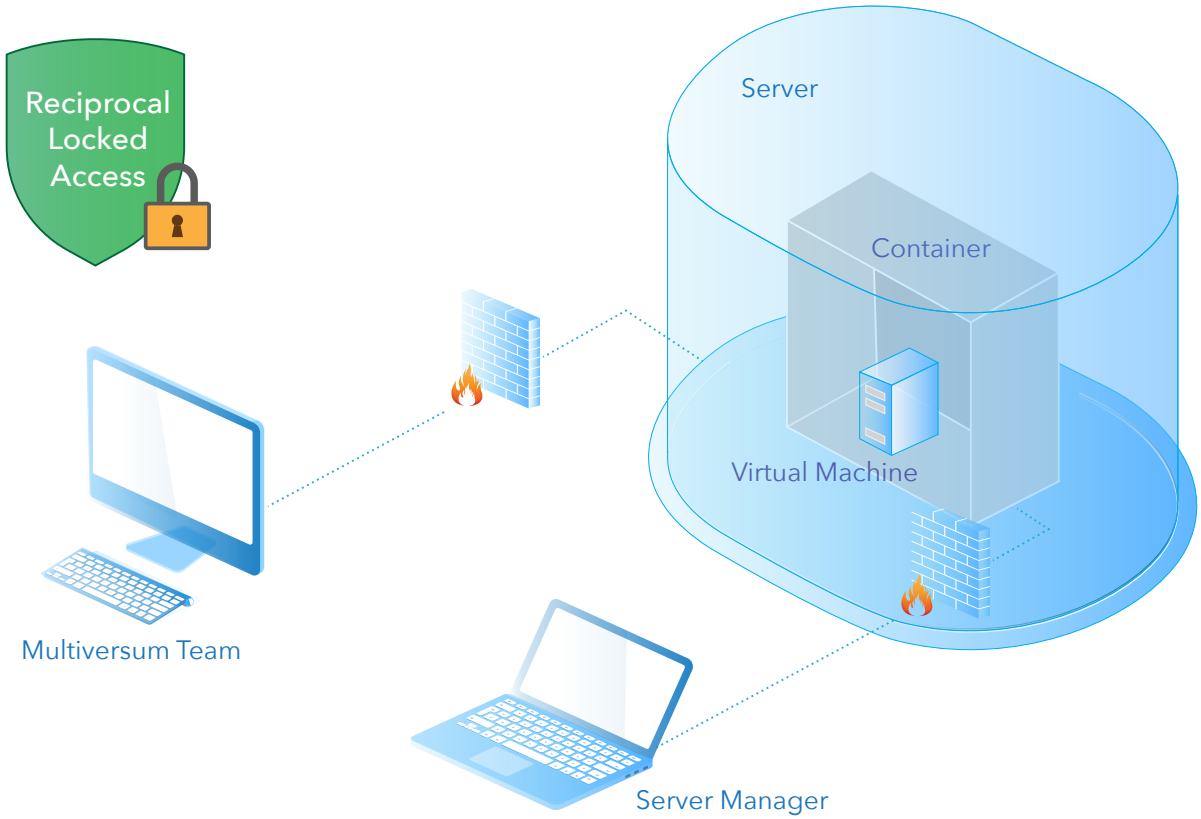
يتم التحقق مقارنة بحدي البذور-العشوائية، جنبا إلى جنب مع التجزئة التي يحسبها عنصر خارجي (محمي من الهندسة العكسية، ومتواصل مع برنامج العقدة عبر قناة مشفرة) من البرنامج نفسه ومع بيانات المعاملات. من أجل تفعيل المعاملة، يجب أن تكون نتيجة هذا الحساب مطابقة لمعاملة معينة، على كل عقدة.

ويتطلب هذا الإجراء قدرة حاسوبية أقل بشكل ملحوظ، مما يمنع هدر القدرة الحاسوبية النموذجية في حلول أخرى للتحقق من الكتل (PoW, PoS, DpoS)، وتوفير الأمن الهيكلي، غير مستند إلى النماذج الإحصائية أو نماذج Byzantine Consensus[13] ، التي تكون ضعيفة جدا في مجموعات صغيرة.

Access Denied

12. قفل الدخول المزدوج (الأمن الهيكلي)

سيتم توزيع العقد في حاويات افتراضية مضمونة، مع عدم توفر بيانات الاعتماد لمشغل الجهاز المضيف، مما يحول دون الوصول؛ وبالتالي يتم إحالة السلامة إلى أفضل ممارسات Linux Security[14] ، كما، على سبيل المثال، SeLinux و / أو حزم أخرى. وفي الوقت نفسه، إذا كان شخص ما لديه أوراق اعتماد الجهاز كضيف ،لن يتمكن من الوصول إليها، لعدم القدرة على الوصول إلى الجهاز المضيف المشغل لتلك العقدة. العقدة هي، في واقع الأمر، مأمنة عن طريق قفل الوصول المزدوج.



13. رفض الدخول العكسي (الأمن الهيكلي)

وينطوي قفل النفاذ(الدخول) الموصوف في النقطة ٢١ على استبعاد متبادل لعقدة النفاذ إلى كل من مشغلي الأجهزة المضيفة ومن يمتلك في نهاية المطاف بيانات اعتماد العقدة؛ وهذا يضمن أن كل عقدة لا تدار مباشرة من قبل مولتيفرسوم هي أصلية ولا يمكن الوصول إليها من قبل أي شخص، في الأساس مستقلة ومعزولة عن التدخل البشري الخارجي.

سيتم توزيع ثلاثة مكونات أساسية داخل الحاوية بالإضافة إلى نظام التشغيل والسلامة:الرمز المجمع لخادم مولتيفرسوم الرقمي(server)، شهادة مع مفتاح غير متماثل للمصادقة على كتلة مولتيفرسوم، وهو مكون سبق وصفه في النقطة ١١) وهو المسؤول عن تحدي الحساب استنادا إلى خادم رمز التجزئة، شهادة، تحدي بيانات البذور والمعاملات.

قد يتم تنفيذ تقنيات أمنية اختيارية إضافية، مثل التحديث الآلي لوثائق الوصول للحاوية مع كلمة مرور عشوائية أثناء مرحلة تجميعها، وذلك لمنع أي شخص من الوصول. ويمكن اعتماد هذه الآلية للحصول على شهادة النفاذ إلى المجموعات.

14. تأكيد تبادل السلسلة (التشغيل البيني مع بلوكشينز أخرى)

سوف تدرس مولتيفرسوم جدوى عنصر تكامل مع سلسلة خارجية، قادر على تخزين حالات من بلوكشينز أخرى (في نهاية المطاف في تبادل الرموز) لتوفير المزيد من التحقق والثقة.

ويمكن أيضا أن تستخدم نفس التقنية للسماح لمولتيفرسوم ان تشترك في التحقق من صحة الحالة الخاصة بها مع بلوكشينز أخرى، «الاستعانة بمصادر خارجي» للتحقق.

وسيتم توفير واجهة محددة لهذه الوظيفة، التي تحتاج أيضا إلى تعزيز بين تطبيقات بلوكشين الحالية والمستقبلية.

سوف تعتمد هذه الميزة على عنصر سيرفيرليس الذي يمكن الوصول إليها أيضا بعد تجميع الحاويات، للسماح لإدراج محولات نحو سلاسل أخرى.

15. التكامل ل Java, Spring and Javascript

سوف تقدم مولتيفرسوم واجهات راقية مجمعة في مكتبات فنية لجافا، جافا سكريبت(Java, Javascript) وربما غيرها من اللغات السائدة، مما يسهل اعتماد التكنولوجيا لدينا على مستوى الشركات والمؤسسات.

كما سيتم تطوير وحدات تكامل مع أطر مثل Spring[15]. هذا النوع من المكتبات سيسهل دمج مولتيفرسوم في حلول الملكية، سواء في سلاسل خاصة أو MainNet الرسمية.

16. نموذج ACID

سيلبي مولتيفرسوم نموذج ACID[16]: هذا الاختصار يستوعب منطق الخصائص المطلوبة من المعاملات.

ولضمان نموذج معاملات آمن، تحتاج التكنولوجيا المنفذة إلى تحقيق الخصائص التالية:

الذرية: الصفقة غير قابلة للتقسيم في تنفيذها، ويجب أن يكون تنفيذها كاملا أو لاغيا، ولا يسمح بالإعدام الجزئي.

الاتساق: أي معاملة سوف تجلب قاعدة البيانات من حالة صالحة واحدة إلى أخرى. يجب أن تكون البيانات الثابتة صالحة وفقا لجميع القواعد المحددة.

العزل: يجب تنفيذ كل معاملة بطريقة معزولة: فإن الإخفاق النهائي لمعاملة لا يتداخل مع المعاملات الأخرى المتفق عليها.

المتانة: يدعى أيضا استمرار، يفرض أنه بمجرد الالتزام بمعاملة، لا يمكن أن تفقد النتيجة لأي سبب (حوادث، أخطاء، فقدان الطاقة).

17 - نموذج المعاملات

وسيستمر مولتيفرسوم في بيانات المعاملات في نموذج المعاملات transactional[18] ، مع التأكد من استمرار جميع البيانات أو عدم وجود أي منها على سلاسل فرعية متعددة، وتحقيق الاتساق بين كل معاملة منفذة واكتمال البيانات.

18. لغة (مثل SQL)

لتبسيط تطوير التطبيقات استنادا إلى تكنولوجيا التشفير الارتباطية لقاعدة البيانات وتخفيف منحنى التعلم مقابل التكنولوجيات القائمة، ستتميز مولتيفرسوم [18] syntax SQL-based لاستخدام وظائف التخزين المستمر القياسية (CRUD).

19. كامل تدفق البيانات الطريق

تتم عمليات القبول والتحكم والتحقق من صحة واستمرار المعاملة مع الإجراءات التخطيطية والمبسطة التالية:

يتم إرسال المعاملة إلى عميل REST، مع البيانات اللازمة، موقعة مع مفتاح خاص؛

يرسل العميل REST المعاملة إلى عقدة رائدة من مجموعات التنسيق: فإنه سيتم تقسيم العمل عبر العقد مع بروتوكول تنسيق الملكية؛

وسوف تشغل تحقيق أولي من اكتمال البيانات، والتوقيع، وتوافر الأموال، والتجزئة المستخدمة بالفعل، حال المحفظة غير نشط، ومحافظ أو المستخدمين ممنوعين؛

يتم الآن حجز أي عملية إضافية من معرف المرسل في الذاكرة المتطايرة، في حين يتم الانتهاء من حقول بيانات محددة (مثل المعاملات السابقة للربط، والطابع الزمني والتجزئة السابقة)؛

يتم إرسال المعاملة إلى Topic Message Queue [19] مع البروتوكول الذي يجب أن يعرف(AMQP for the pilot, MQTTوغيرها ليتم تعريفها) وتوزيعها بالتوازي مع العقد العاملة؛

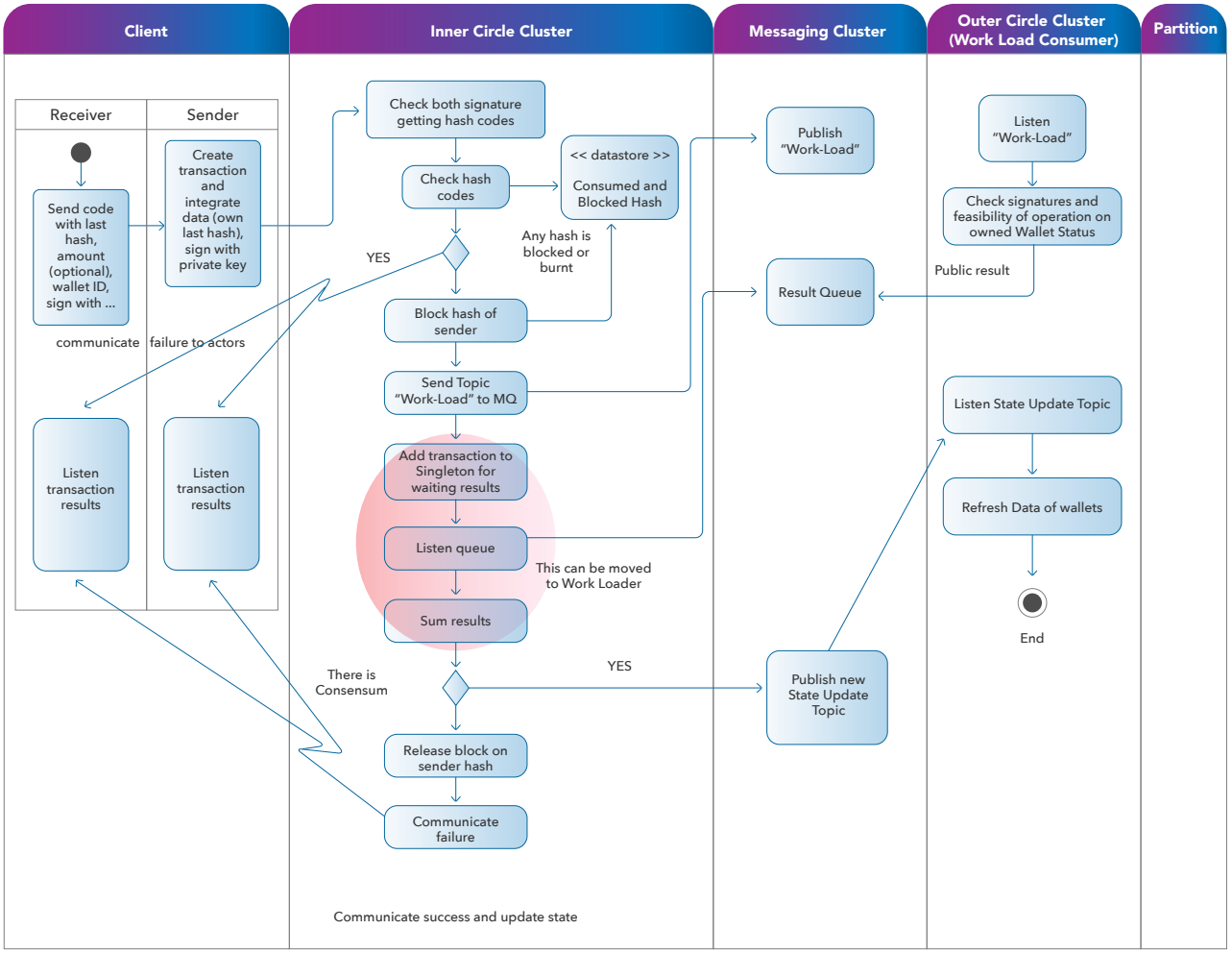
تتحقق العقد العاملة من اهتمامهم بمعالجة الطلب (قد ينقصهم بيانات ضرورية، تكون مشغولة بالفعل وغيرها من الشروط التي يتعين تقييمها) والمضي قدما في إنشاء حالة المحفظة الجديدة، واستعادة تجزئة مترابطة من المعاملات المرتبطة السابقة وإضافتها إلى سجل المعاملات. ويضاف الآن إثبات نتائج النزاهة؛

يتم حساب تجزئة الصفقة.

سجل العقد العاملة الصفقة في الذاكرة وترسل تصويت إلى العقد المنسقة من خلال قائمة انتظار الرسائل(Message Queue)، جمع النتائج.

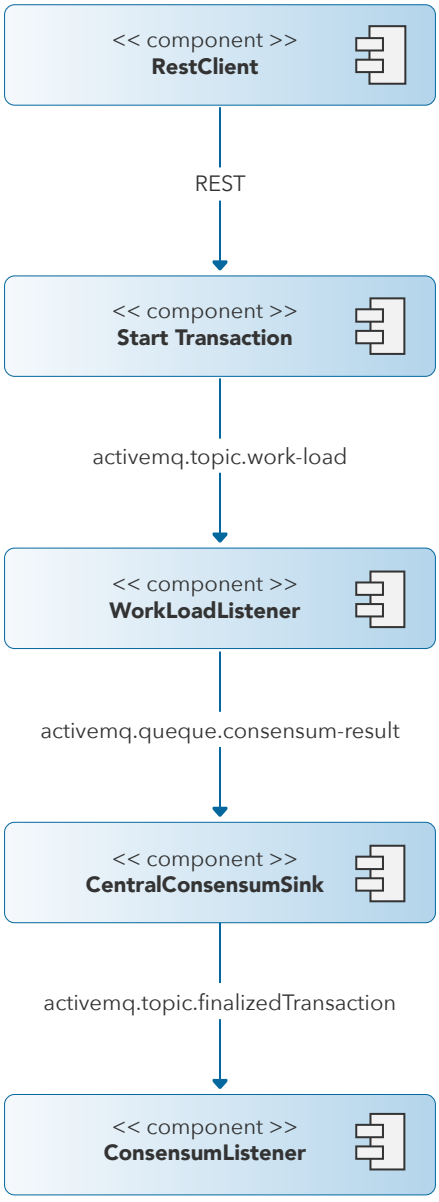
إذا كانت الأصوات والتجزئة متماسكة، ستستمر عقد التنسيق في المعاملة وأي حالات جديدة لمحافظ، وحرق أي تجزئة من الحالات السابقة وبث مفعل تصويت مع نظام قائمة انتظار موضوع إضافية(Topic Message Queue system). الآن أيضا ستستمر العقد العاملة في المعاملات وتتغير حالة المحفظة؛

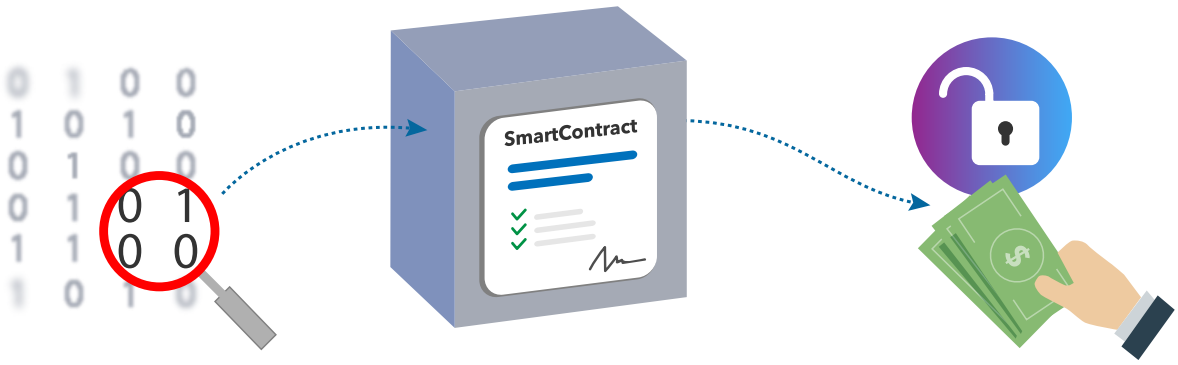
نهاية أفضل سيناريو المسار الكامل.


Client
Inner Circle Cluster
Messaging Cluster
Outer Circle Cluster (Work Load Consumer)
Partition
Receiver
Sender
Send code with last hash, amount (optional), wallet ID, sign with ...
Create transaction and integrate data (own last hash), sign with private key
communicate failure to actors
Listen transaction results
Listen transaction results
Check both signature getting hash codes
Check hash codes
<< datastore >>
Consumed and Blocked Hash
Any hash is blocked or burnt
YES
Block hash of sender
Send Topic "Work-Load" to MQ
Add transaction to Singleton for waiting results
Listen queue
This can be moved to Work Loader
Sum results
There is Consensum
YES
Release block on sender hash
Communicate failure
Communicate success and update state
Publish "Work-Load"
Result Queue
Publish new State Update Topic
Listen "Work-Load"
Check signatures and feasibility of operation on owned Wallet Status
Public result
Listen State Update Topic
Refresh Data of wallets
End

تدفق البيانات المنطقي

تفاصيل تدفق العملية





العقود الذكية

يعتقد مولتيفرسوم في أهمية اقتراح تحسين العقود الذكية (Smart Contracts[20]) للجمهور، ولكن في وقت كتابة هذا التقرير، ما لم يكن هناك تعديل في نطاقات البحث، لم يقرر استكشاف هذا الاحتمال. ولذلك، فإننا نتطلع إلى أن ندرج في تكنولوجيا مولتيفرسوم حلول المصدر المفتوح التي تناسب احتياجاتنا في أفضل الأحوال، ليتم تنفيذها كمرجع وفقا لنموذج الترخيص لها.

بنية تحتية

تم تصميم البنية التحتية لضمان الصمود والقدرة على الوصول (reachability[21]). وقد تم تحقيق هذا الهدف بتطوير مجموعات العقد القادرة على انتخاب أعضائها لأدوار محددة، وفقا للمواصفات الفنية لكل عقدة ، منها:

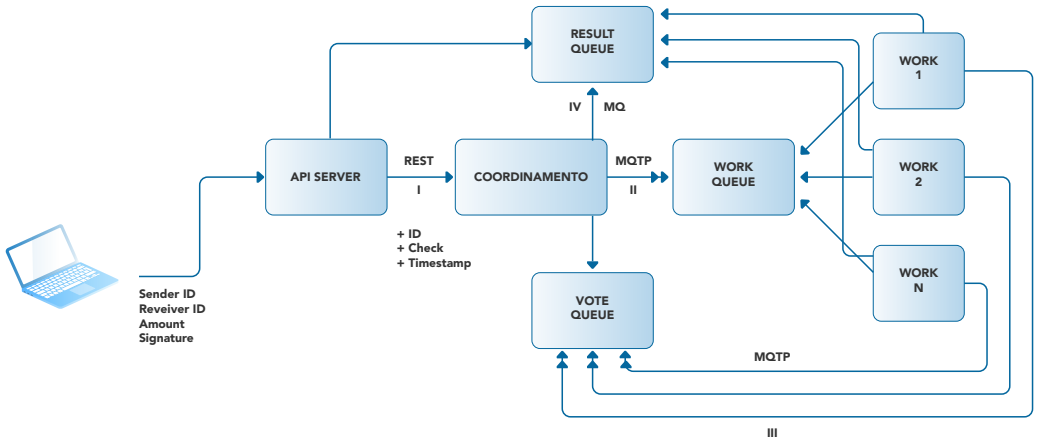
- القدرة الحسابية
- سعة الذاكرة
- وقت الإستجابة المتبادل
- اكتمال بيانات السلسلة
- موثوقية الجهاز
- شكوك حول إثبات النزاهة

وعندئذ يكون للعقد دور واحد أو أكثر:

- العقد العميلة
- عقد المنسقة
- عقد التراسل
- عقد العاملة
- عقد الثبات
- عقد النسخ الاحتياطي

كل عقدة التي يمكن أن توفر شهادة صالحة ستكون قادرة على التسجيل في الكتلة والحصول على دور.

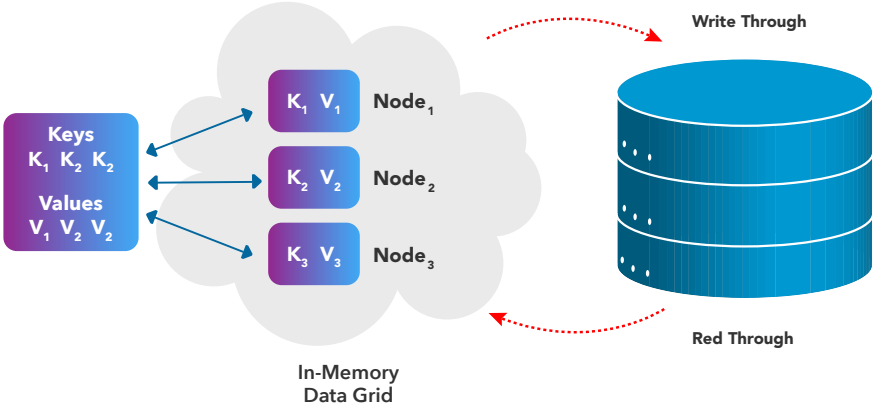
في حالة تعطل عقدة أو أكثر، ستكون المجموعة قادرة على إعادة توزيع المهام بشكل مستقل، وتحسين الأدوار.



مكونات ذاكرة التخزين المؤقت المشتركة داخل JVM[٢٢] سيكون هناك كقاعدة بيانات الذاكرة، ويسمح:

القراءة من خلال، أي طلبات قراءة البيانات التي يتم تنفيذها مباشرة في الذاكرة المتقلبة قبل النظر في الذاكرة الفعلية.

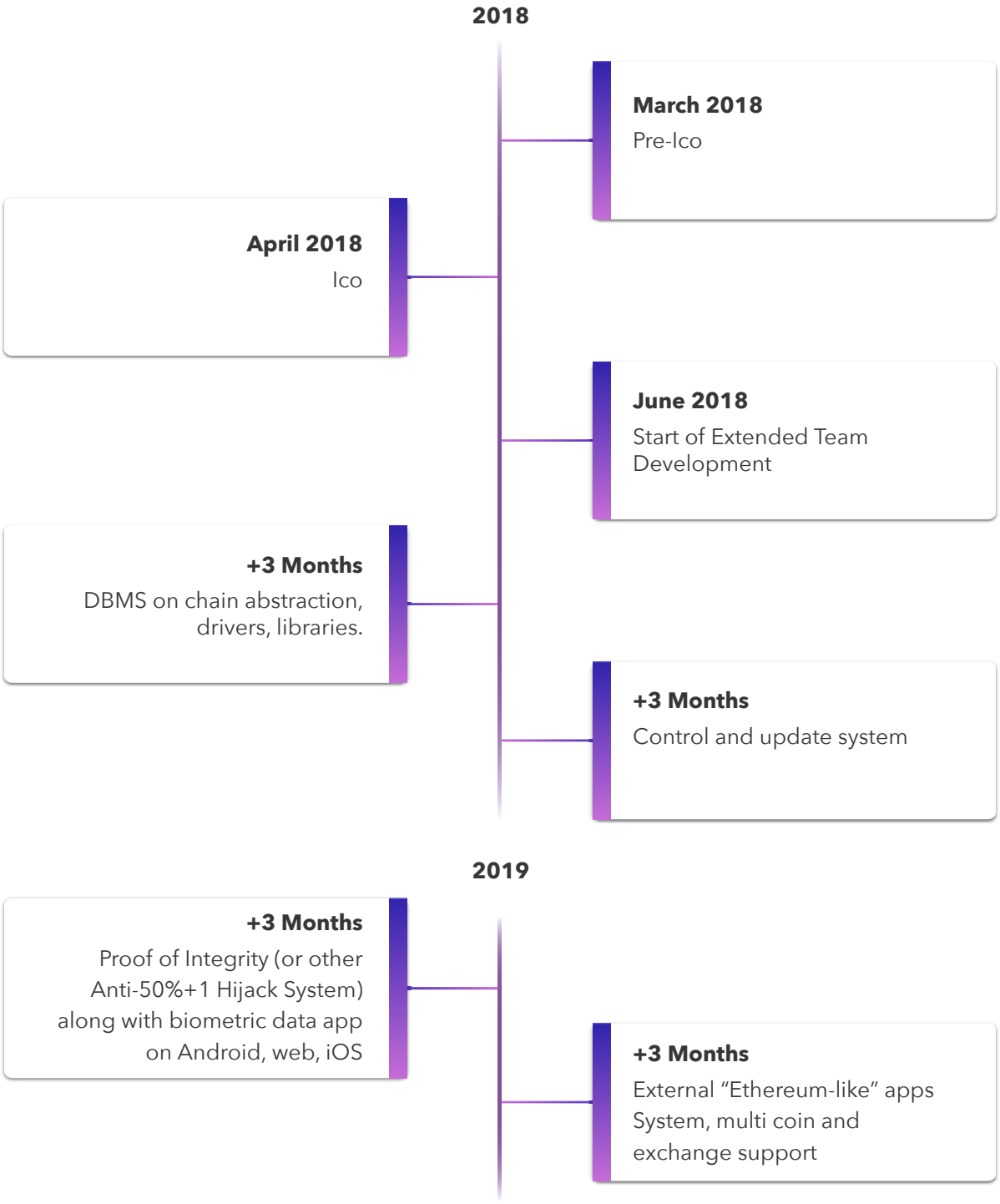
الكتابة من خلال، تحميل البيانات في الذاكرة المتطايرة قبل تنفيذ الإدراج الشامل لاستمرار البيانات، من أجل تحسين الأداء.



ملاحظات حول الأمن

خلال التنمية، وسيتم تقديم "Hacker's bounties" للمطورين لكشف نقاط الضعف وقادرة على اقتراح إصلاح لها.

خارطة الطريق التقنية



المراجع

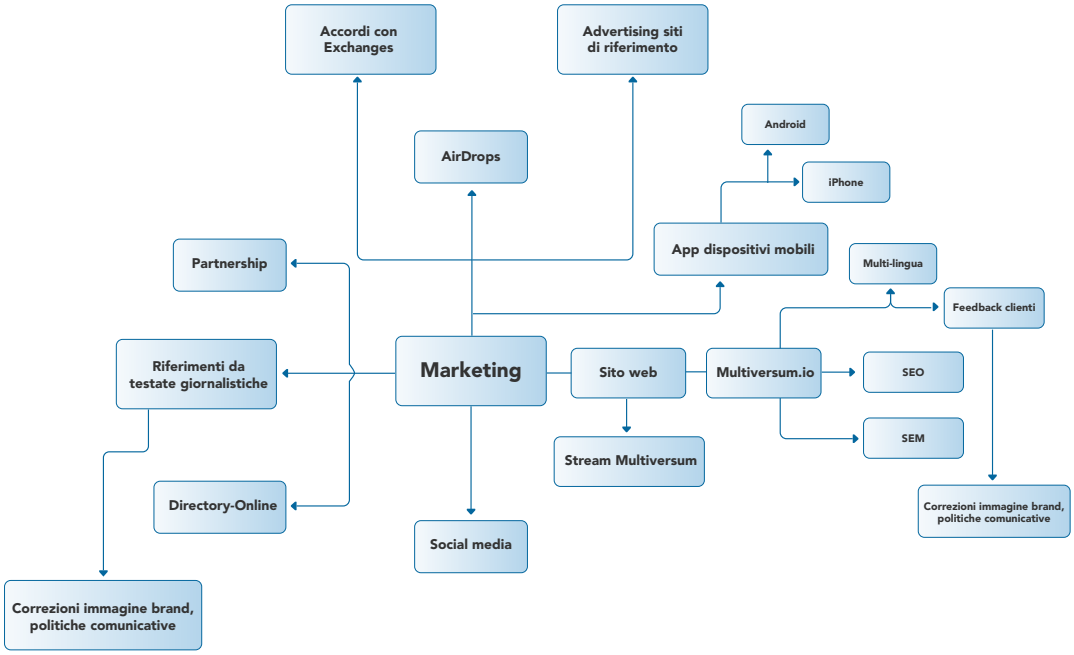
1 https://en.wikipedia.org/wiki/Scalability#Horizontal_and_vertical_scaling
2 https://en.wikipedia.org/wiki/Proof-of-work_system
3 https://en.wikipedia.org/wiki/Proof-of-stake
4 https://en.wikipedia.org/wiki/Agile_software_development
5 https://en.wikipedia.org/wiki/Scope_(project_management)
6 https://en.wikipedia.org/wiki/Shard_(database_architecture)
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

استراتيجية التسويق

عمل الشركة في سوق تكنولوجيا المعلومات المتغيرة باستمرار، سيحدث إستراتيجيتنا وتقنيات التواصل ومهمة الشركة وفقا لذلك، مع التركيز على خلق قيمة لأصحاب المصلحة وضمان التوازن المناسب بين منطق الإدارة قصيرة وطويلة الأجل.

النقاط الرئيسية في خطتنا هي:

- مهمة الشركة
- أهداف العمل
- استراتيجيات الأعمال
- محفظة أنشطة الأعمال



واحدة من الأدوات الرئيسية ستكون التسويق ضمن **وسائل الاعلام الاجتماعية:** حملات أجريت على الشبكات الاجتماعية لزيادة الوعي بالعلامة التجارية، وتحديد المستهلكين المحتملين، وتوليد الاتصالات وبناء علاقات هادفة مع العملاء.

سوف يقوم خبراء استراتيجيات التواصل الاجتماعي بتنفيذ العديد من الإجراءات التي تشكل جزءا من خطة استراتيجية واحدة، بدءا من إدارة ورصد القنوات باستخدام أدوات مخصصة وتنمية المجتمع، مع التركيز على المحتوى والتفاعل وتقييم كفاءة التكتيكات على أساس النتائج التي تم الحصول عليها.

طبقات العناصر التي تغطي الأكوان هي كل عشر
مرات أكثر سمكا من التي قبلها،

وجميع الأكوان تتجمع معا وتظهر مثل الذرات
في مزيج ضخم.

Bhagavata Purana 3.11.41

MULTIVERSUM

HERE TO STAY