الورقة البيضاء التقنية

(يمكن إضافة بعض التفاصيل)

نظام مالي لامركزي

كردتس

إصدار 1.5/ 15.9.2017

المحتويات

ملخص

منصة كريديتس هو النظام المالي اللامركزي للتفاعل المباشر بين المشاركين على مبادئ نظير لنظير (P2P). منصة توسع إمكانات استخدام الخدمات المالية على أساس الدفتر المحاسبي الموزع، العقود الذكية ذاتية التنفيذ، وعملة كريديتس الرقمية. يهدف النظام إلى توحيد جميع المشاركين في موقع واحد، تزويدهم بمنصة لإنشاء واستخدام الخدمات المالية؛ حيث يمكن للجميع تقديم الخدمة واستخدامها معاً. بفضل نظام تكنولوجي جيد التحديد ومتوازن، تقدم منصة كريديتس حلا تقنيا جديدا ونموذجا مفاهيميا جديدا لتفاعل المشاركين في الشبكات من أجل تطوير الخدمات المالية اللامركزية الحديثة.

المقدمة

ترتيب الند للند الكامل لأنظمة تقديم الخدمات التي تسمح بتشكيل الخدمات المالية: تحويل الأموال، تبادل العملات والقيمة، الائتمان والتمويل وغيرها من الخدمات المباشرة بين المشاركين. يتم توفير كل شيء دون وسطاء إضافيين، وفقا لمبدأ - واحد من المشاركين المساويين – للمشاركين الآخرين في النظام. نتيجة لذلك، يحصل الجميع على أرخص وأسرع وأفضل الخدمات.

العالم يتحرك نحو التفاعل المباشر بين الناس على مبادئ الند للند - متكافئة. التطور حدث! يتضح ذلك بوضوح من خلال الانقلاب في وسائل الإعلام: حتى التسعينات، كانت الصحف والمجلات والتلفزيون هي المزود الرئيسي للمعلومات. اليوم، قادة الرأي والمدونين، الموجودين على قنوات يوتيوب والشبكات الاجتماعية، يتم استثمار الأموال في حملة التمويل الجماعي ومرحلة الإيكو، ويتم تخزين المعلومات في أنظمة سحابية لامركزية.

ربما كانت الصناعة المالية إحدى الصناعات القليلة التي تتخلف عن الركب، والتي تقاوم إدخال اللامركزية والتفاعل المباشر بين المشاركين. على الرغم من أنه من الناحية الفنية، من الأسهل بكثير إنشاء خدمات مالية لا مركزية أكثر من إنشاء مركبات غير مأهولة.

هناك حاجة إلى بيئة تكنولوجية مقابلة لإنشاء نظام للمنتجات والخدمات المالية اللامركزية استنادا إلى الدفتر المحاسبي الموزع:

1. سرعة تنفيذ عالية (بالثواني)، جنبا إلى جنب مع القدرة على التعامل مع عدد كبير من المعاملات في وقت واحد (مئات الآلاف في الثانية الواحدة) بتكلفة منخفضة لكل معاملة (للمدفوعات الصغيرة والمعاملات الغير نقدية).

2. تطوير نظام حيث يتم الجمع بين جميع المشاركين والبنود اللازمة للخدمات المالية اللامركزية النوعية: إضفاء الطابع الشخصي للمستخدمين، معرفة عميلك، مركز تاريخ الائتمان، مراكز تسوية الأموال النقدية، السحب والصرف للعملات الرقمية و ما إلى ذلك.

هذه هي المهمتين الكبيرتين والأساسيتين التي تعوق حاليا تطوير المنتجات المالية بين الأنداد.

نقدم لكم حلا لهذه المهام، نفذناه بمساعدة النظام المالي كريديتس.

كريديتس منصة لامركزية تقنية مفردة يمكنها الجمع بين جميع المشاركين في الخدمات المالية، بأمان وبسرعة تنفيذ جميع المعاملات باستخدام مبادئ الدفتر المحاسبي الموزعة. التنفيذ دون تدخل طرف خارجي للعقود الذكية ومبادئ نظام التصويت الفدرالي توفر فرصا غير محدودة لجميع المشاركين لإنشاء تفاعلات فريدة للمنتجات المالية المختلفة. المنصة تفتح سوقا ضخماً جديداً وإمكانات جديدة لاستخدام مشاريع بلوكشين والخدمات في القطاعات المالية وغيرها التي لا يمكن استخدامها سابقا بسبب السرعة وقيود تكلفة المعاملات.

1. دفتر الشبكة المحاسبي

تعريفات

1 - النظام عبارة عن مجموعة من عقد الشبكة اللامركزية التي تقوم بالمعالجة، حفظ المعاملات، تنفيذ وتأكيد شروط العقود الذكية،وتجهيز الطلبات من أنظمة الطرف الثالث، وتوفير بيانات المعلومات عند الطلب.

2. عقدة الشبكة هي جهاز كمبيوتر حيث يتم تثبيت عميل شبكة كاملة، متصلا بنظام معروف، يتحقق من المعاملات و يكتبها في الدفتر المحاسبي.

3. الدفتر المحاسبي هو قائمة المعاملات التي أكدها النظام و خزنها على جميع عقد الشبكة.

4. الصفقة هي بند النظام، تدل على طلب لأداء طريقة العقد الذكي أو أي إجراء على الشبكة وتسجيل النتائج في نظام بلوكشين.

5. العقد الذكي هو بند النظام، بروتوكولات الكمبيوتر التي تسهل، تتحقق أو تضمن الالتزام لشروط التفاعل. وعادة ما يكون لديهم واجهة مستخدم وغالبا ما يحاكي منطق العلاقات التعاقدية. والممتلكات الرئيسية للعقد الذكي هي اللامركزية واستقلاليته عن المصدر المركزي.

6. نموذج العقد الذكية هو رمز البرنامج المسئول عن حساب نتيجة عمل شروط العقد الذكي وتسجيلها في الدفتر المحاسبي.

7 - الطرف المتعاقد هو المشارك النهائي في الشبكة ومستخدم النظام.

عقد الشبكة

نحن نستخدم عدة أنواع من العقد، اعتمادا على هدفها لبناء شبكة لامركزية على أساس حرية الوصول واتصال العقدة:

1. العقدة المشتركة (ОУ) هي العقدة المشاركة في التحقق من المعاملة من أجل الصلاحية ولكن لديها الحد الأدنى من عامل الثقة. تعتبر أيضا مرشحة لدور عقدة موثوق بها والعقدة للمعالجة الحالية في الدورة القادمة من اختيار دور العقدة في الشبكة.

2. عقدة موثوق بها (ДУ) هي العقدة المشاركة في التحقق من المعاملات ولها أقصى عامل ثقة (1)، تعتبر مرشحة لدور العقدة للمعالجة الحالية والعقدة المشتركة. لا يمكن أن تصبح هذه العقدة موثوق بها خلال عدد محسوب رياضيا من دورات الاختيار والتصويت بين العقد. الحساب الرياضي يعتمد على عدد العقد وتعقيد الشبكة.

3. العقدة الرئيسية (ГУ) للشبكة هي العقدة المشاركة في التحقق والمسئولة عن إضافة المعاملات إلى كتلة الدفتر المحاسبي للمعاملات. هذه العقدة لا يمكن أن تصبح موثوقة أو عقدة المعالجة الحالية خلال عدد محسوب رياضيا من دورات التصويت، والتي يتم حسابها رياضياً بالاعتماد على عدد العقد وتعقيد الشبكة.

يستخدم النظام عامل ثقة - قيمة رقمية كسرية مطلقة من 0 إلى 1، معبرا عنها في المصطلحات الرياضية لعدد العقد الموثوقة الأكثر من 1 إلى العدد الإجمالي للعقد في الشبكة. لا يمكن أن يتجاوز الحد الأقصى لعدد العقد الموثوقة 50٪ من عقد الشبكة.

آخر كتلة محفوظة

الدفتر المحاسبي المشترك للكتل (كرب) هو حالة متزامنة من الدفتر المحاسبي المعروف كلياً للتجمعات والكتل في جميع عقد النظام.

من خلال محتويات كتلة الدفتر المحاسبي، نريد تحقيق وحدة من المعلومات المخزنة التي تحتوي على رمز تجزئة الكتلة السابقة وقائمة من البيانات المتعلقة بهذا الدفتر المحاسبي مع عدد المرتبطة بها من الكتل السابقة. عند استلام كتلة من عقدة أخرى، فإنه يأخذ مكانه في الدفتر المحاسبي المعروف للكتل وفقا للعدد. هذا يوفر عرض النطاق الترددي للشبكة. أثناء المزامنة، يتم فحص رقم الكتلة أولا. إذا كانت الكتلة مفقودة في هذه العقدة، يتم تنزيلها وحفظها.

نتيجة لذلك، فإن النظام في أي وقت يحتوي على أحدث نسخة للدفتر المحاسبي. نسميها آخر دفتر محاسبي (LR). يتم إنشاؤها تلقائيا من قبل العقدة المسئولة عن تشكيل دفتر محاسبي عند التوصل إلى توافق في الآراء. يتم إرسال هذه الكتلة إلى جميع عقد النظام من أجل الحفاظ على توحيد جديد لحالة الدفتر المحاسبي في جميع عقد النظام.

ترتبط كل عقدة مع جميع العقد الأخرى في الشبكة ويتبادلوا باستمرار كتل جديدة مع المعاملات معهم، وذلك للحفاظ دائما على المعلومات ذات الصلة. تشكل جميع الكتل مجموعة من المعاملات التي تنتظر إضافتها إلى الدفتر المحاسبي. في الوقت نفسه، يُنشئ كل خادم مجموعات مفترضة من المرشحين لخوادم أخرى ومجموعة معاملات مقترحة. يتم اتخاذ قرار عند التحقق، بحيث يتم إضافتها إلى الدفتر المحاسبي.

نتيجة لذلك، فمن الممكن تخزين بيانات الدفتر المحاسبي عدة مرات على خوادم متعددة - عقد النظام، وجميع المعلومات محمية. كلما زادت العقد في النظام، كلما زادت موثوقيتها و استقلالها.

تزامن العقد

يتم إطلاق كل عقدة جديدة ومزامنتها بعد تحديد المفهوم والتحقق من الثقة الشاملة. لتحسين معدل معالجة المعلومات، يتم التعامل مع جميع العمليات في وقت واحد، بشكل مستقل عن بعضها البعض. إذا لم يكن هناك متغيرات واردة، ثم يتم إنشاء مخزن دفتر محاسبي فارغ - يتم حجز مساحة في ذاكرة الوصول العشوائي لمزيد من الوصول المُبسّط. في حالة عدم توفر الدفتر المحاسبي المطلوب، يتم إرسال طلب إلى العقد الموثوقة لتلقي جميع المعاملات التي تم إجراؤها لحساب متزامن.

إذا كانت متغير الإدخال هدف يميز المعاملة، يتم بعدها بدء البحث في كافة مؤشرات التزامن قيد التشغيل. ينتج عن العملية رمز رقمي - رقم الموضع في الدفتر المحاسبي للعقدة الموثوق به لموضوع مؤشر الترابط الحالي أو الرقم الخطأ إذا كانت القيمة أقل من الصفر. إذا انتهت طريقة مؤشر الترابط مع خطأ اتصال، عندها ينتهي مؤشر الترابط تماما.

2. توافق الشبكة

الإجماع في كريديتس هو طريقة لاتخاذ القرارات الجماعية. بهدف تطوير حلول نهائية مقبولة لجميع عقد الشبكة.

مقارنة الإجماع

تعريف مبادئ الدفتر المحاسبي اللامركزية لمقارنة أنواع مختلفة من الإجماع:

- توافر دفتر محاسبي (العقد يمكنها كتابة البيانات في الدفتر المحاسبي وقراءتها منه في أي وقت).
- قابلية التعديل من قبل جميع عقد الشبكة المشاركة؛
- تناسق جميع عقد النظام (جميع العقد تُرى كنسخة متطابقة تماما للدفتر المحاسبي، والتي يتم تحديثها بعد التغييرات).
- مقاومة الفصل (إذا أصبحت العقدة الواحدة غير قابلة للتشغيل، فإن هذا لا يؤثر على تشغيل الدفتر المحاسبي بأكمله).

مقارنة المتغيرات	إثبات العمل و إثبات التوافق المحددين في كردتس	مبدأ إثبات العمل PoW	مبدأ إثبات التوافق PoS
مبدأ تعريف العقدة التي تولد الكتلة	حساب الدالة الرياضية. تأكيد تخزين آخر نسخة دفتر محاسبي.	إجراء حساب تكراري للدالة الرياضية، مع تعقيد متفاوت	البحث عن أقصى تجمع بين المشاركين (العقد المتنافسة).
حملة 51%	على غير المرجح، لأنه من الضروري أن يكون الدفتر المحاسبي كامل في الموارد وقوة حسابية للحساب، ويتم اختيار العقد الموثوقة بشكل فعال.	محتملة ، لكن ستكون مكلفة للغاية من حيث استخدام الموارد.	محتملة ، لكن مكلفة، بسبب الحاجة إلى زيادة الكتلة والتجمع لشخص معين.
التعويض عن العمل المنجز في الموقع لإضافته إلى الدفتر المحاسبي/ بلوكشين.	يحسب تلقائيا، متعتمداً على العمولة لكل عملية.	يقدم حل لتعدين الكتلة.	يقدم حل لتعدين الكتلة.

مفهوم عقدة الشبكة الرئيسية

جميع عقد الشبكة لامركزية ولا أحد منها له الأولوية. مطلوب تحديد عقدة شبكة من شأنها معالجة قائمة انتظار المعاملات المخزنة في عقد شبكة مختلفة. بعد ذلك، يجب إدخال كتلة عمليات تم إنشاؤها حديثا في الدفتر المحاسبي.

منصة كريديتس تستخدم بروتوكول موحد خاص بها لزيادة سرعة معالجة المعاملات، لتوفير الأمن الكامل لتخزين البيانات ومعالجتها ونقل المعاملات. يستند البروتوكول على حساب وظيفة رياضياً لجميع معاملات الدفتر المحاسبي، تطبيق مبادئ إثبات العمل. يحدد بدقة تخزين أحدث نسخة للدفتر المحاسبي والبرمجيات في هذه العقدة (إثبات القدرات)، من خلال حساب المجموع الاختباري لقيم المحتويات - رمز التجزئة. يتم تحديد حجم الملفات أيضا، و إثبات أنه الأحدث، نسخة حديثة ورمز التجزئة لأحدث المعاملات المسجلة في النظام.
لتصبح عقدة الشبكة الرئيسية، تبحث العقدة عن قيمة الدالة المجزأة التي يحسبها استنادا إلى الدفتر المحاسبي المخزن أخيراً. نحن ننظم بيئة تنافسية سليمة بين عقد الشبكة لإتاحة الفرصة لتصبح العقدة الرئيسية؛ لإنشاء وتخزين دفتر محاسبي جديد.
بعد حساب الدالة والحصول على النتيجة، يتم إرسالها إلى كل عقد الشبكة للتحقق. تحتوي النتيجة على الطابع الزمني للحساب والقيمة استنادا إلى حساب وظيفة ملفات الدفتر المحاسبي والبرمجيات. تتلقى جميع العقد القيمة المحسوبة، تقارن وقت الحساب المخصص للبحث عن خادم الشبكة الرئيسي، التحقق منه و تأكيد عامل الثقة للعقدة، وتؤكد أيضا فرصتها للمشاركة في المنافسة - لتصبح عقدة الشبكة الرئيسية.

بعد الحصول على موافقة من جميع عقد الشبكة، يتم تشكيل قائمة من العقد التي تحسب بشكل صحيح قيمة الدالة وتحتوي على الطابع الزمني. العقدة التي حصلت على النتيجة الصحيحة، وقد وافقت في أسرع وقت، تصبح عقدة الشبكة الرئيسية في هذه اللحظة.
يتم استخدام مفهوم خوارزمية SHA2 لحساب مجموع التجزئة للملف.
يتم بناء وظائف مجزأة لفصيلة SHA2 على أساس هيكل Merkle-Damgard.
الرسالة الأولى بعد الإضافة تنقسم إلى كتل، وتنقسم كل كتلة إلى 16 كلمة. الخوارزمية تمرر كل كتلة رسالة من خلال دورة من 64 أو 80 تكرار (جولات). في كل تكرار، يتم تحويل كلمتين، وتحدد بقية الكلمات وظيفة التحويل. يتم تلخيص نتائج كل عملية كتلة. المجموع هو قيمة الدالة المجزأة. مع ذلك، يتم تهيئة الحالة الداخلية استنادا إلى نتائج معالجة الكتلة السابقة. لذلك، فإنه من المستحيل معالجة الكتل بشكل مستقل وتلخيص النتائج.

معدات عقد الشبكة

نسعى جاهدين لبناء منصة مع أسرع خصائص ممكنة لمعالجة المعاملات ، لذلك نقترح استخدام حافز مادي للحفاظ على عقد الشبكة في أفضل حالة: معدات خادم ذات الأداء العالي وعرض النطاق ترددي للانترنت عالي.
كتعويض مادي، سوف يحصل مالك عقدة الشبكة الرئيسية على مكافأة بعملة كريديتس من عدد من العمولات لكل معاملة من دفتر المحاسبة المعالج. وباقي ال (½) مخصص لميزانية تطوير المشروع الشاملة لدعم المستخدم، الميزات الحالية، وتطوير منتجات جديدة. يمكن تغيير النسبة المئوية، وكذلك فصلها إلى نظام تشكيل معدل من خلال التصويت الاتحادي من قبل عقد الشبكة، بعد عرض العملة الأولي لمدة ثلاث سنوات على الأقل.
نتيجة لذلك، فإننا نشجع مالكي الخادم على إبقاء هذا الخادم على أعلى مستوى من الأداء والحفاظ على قناة اتصال عالية الجودة وعالية السرعة.

بناء المشورة والإجماع

نتيجة لذلك، لدينا عقدة الشبكة الرئيسية المحددة من قبل جميع العقد. المهام الرئيسية للعقدة الرئيسية هي: الحصول على المعاملات في حالة المرشح لإضافتها إلى الدفتر المحاسبي من جميع العقد، معالجتها، بناء الدفتر المحاسبي الأخير ذو الصلة وإرسال دفتر محاسبي تم بناؤه حديثا إلى جميع العقد الشبكة. عملية معالجة المعاملات وبناء دفتر محاسبي أخير ذو صلة هي بالتحديد البحث عن حل إجماعي. نتيجة بناء دفتر محاسبي أخير ذو الصلة هو الحل الإجماعي.
يمكن تقسيم العملية كاملة إلى المراحل التالية:
1. البحث عن عقدة الشبكة الرئيسية.
2 - بناء العقد الموثوقة؛
3. تلقي قائمة المعاملات وبناء قائمة من المرشحين بالإضافة إلى الدفتر المحاسبي.
4. معالجة قائمة المرشحين، التصويت على العقد (العقد الموثوق بها والمعروفة لديها عوامل الوزن المختلفة (عامل الثقة).
5. إزالة من قائمة المرشحين من المعاملات غير المؤكدة التي لم يتم التحقق منها أو التي تحتوي على تأكيد سلبي.
6 - وضع قائمة بالمعاملات المؤكدة التي ستضاف إلى الدفتر المحاسبي؛
7. إضافة المعاملات إلى الدفتر المحاسبي مع الطابع الزمني ورمز التجزئة للكتلة التي تحتوي على الصفقة؛
8. إرسال الكتلة مع المعاملات إلى جميع عقد الشبكة. عند استلامها، يتم إضافتها إلى سجلات جميع العقد.

بناء و إجراء الدفتر المحاسبي

يمكن وصف العملية كاملة في التسلسل التالي:
1. المستخدم النهائي للشبكة في النظام يُنشئ معاملة.
2. عند استيفاء جميع شروط العقد الذكي المحدد فيه، يبدأ المستخدم بإجراء (المعاملة) من خلال استدعاء الطريقة المطلوبة باستخدام برنامج المنصة.
3. لمتابعة المبادئ الأساسية للبلوكشين، جوهر المصادقة يتتبع التزامن وثبات أحدث إصدار للدفتر المحاسبي.
4. في وقت بناء الإجماع، يتم تجميع جميع المعاملات التي يتم استلامها خلال الدورة في المجموعة.
5. يتم تعيين عدد إلى الكتلة، تتألف من الطابع الزمني ،معرف عقدة يُحوّل إلى رمز التجزئة، ومن ثم يتم وضع كتلة في وحدة التوافق.
6. بعد تجميع القائمة البيضاء للمرشحين، ليس فقط تجزئة المعاملة تُكتب في الدفتر المحاسبي، ولكن أيضا تجزئة الكتلة، ليصدّق دائما المصدر على أساس ذلك.
7. هذه التجزئة هو نوع من التوقيع للكتلة و الذي أنشأ هذه الكتلة مع المعاملات.
8. بعد بناء توافق الآراء باستخدام خوارزمية البحث الاتحادية، يتم تمرير المعاملات المضافة إلى الكتلة إلى جوهر المصادقة ليتم كتابتها في الدفتر المحاسبي.

المعاملات الغير مدرجة في السجل

يتم وضع علامة على المعاملات غير المدرجة في قائمة المعاملات الجاهزة على أنها مرفوضة. يتم عرض المعلومات حول هذا على الفور في مكان المرسل (البادئ) للمعاملة.
تبقى المعاملات غير المدرجة في الدفتر المحاسبي في مجموعة المرشحين ويتم تخزينها في عقد الشبكة. جميع المعاملات الجديدة التي يتلقاها الخادم في وقت توافق الآراء تصل أيضا هناك، ثم تبدأ عملية البحث من جديد. تسمح هذه العملية الدورية المستمرة للشبكة بإجراء المعاملات لفترة قصيرة نسبيا من الوقت مع الحفاظ على درجة عالية من الموثوقية والأهمية للمعلومات.

3. معالجة المعاملات

المعاملات

المعاملة هي الحد الأدنى لوحدة النظام التي تعلم المنصة بتنفيذ أساليب العقد أو التحويلات المباشرة بين الحسابات دون إنشاء عقد الذكية، تليها وضع النتيجة في شبكة الأنداد.

بناء المشورة

يستخدم النظام نموذجا اتحادياً لبناء توافق في الآراء - التصويت لعقد المصادقة الموثوق بها، وأيضا خوارزمية بناء توافق في الآراء - خوارزمية لتمرير التشغيل الآلي للحالة المحدودة. توافق الآراء يعمل عن طريق دورات (خطوات وقتية)، في خطوة زمنية، يتم استخراج المعاملات ووضعها في تجمع (نسق بُعدي واحد). بعد وضعه في التجمع، يتم إرسال جميع المعاملات إلى العقد الموثوقة من أجل الحصول على رد. إذا تم تلقي الرد، بعدها يمكن إرسال المعاملة المُضافة ، إلى دفتر الأستاذ من هذا المصادقة. بعد ذلك، يتم إرسالها إلى أداة التحقق التالية في الشبكة. عند بناء المشورة - في نهاية السلسلة حيث يتم تأكيد قانونية النقل بشكل كامل، يتم إرسال المعاملة إلى التحقق من صحتها مع علامة للكتابة و الاحتفاظ بالدفتر المحاسبي.

معالجة المعاملات

لتحقيق الطبيعة اللامركزية للنظام، يجب أن يكون لكل خادم مخزن دفتر محاسبي وأيضا أن يكون معالج بالكامل من جميع المعاملات.
يستخدم النظام مفهوم جوهر النظام. من خلال الجوهر، نريد معالجة البيانات التي تؤدي مهمة إنتاج محددة، بغض النظر عن توافر وقابلية التشغيل من مكونات النظام المتبقية. كل أساس، عند الإدخال، في وقت تنفيذ المهمة، يتلقى قائمة من المتغيرات للمعالجة. ودائما يحصل على نتيجة في الإخراج - إيجابية، أي حالة أخرى أو خطأ. نتيجة لذلك، فإن أساس النظام يحتوي دائما على رمز الاستجابة، بالإضافة إلى مجموعة البيانات الرئيسية. هذا الهيكل مطلوب لأعلى سرعة ممكنة لكل عملية، والتي يجب أن تعمل بشكل مستقل عن بعضها البعض.

هيكل الدفتر المحاسبي

لتحقيق أداء مهم للدفتر المحاسبي، لكن في الوقت نفسه، دون المساس بالأمن، نقترح استخدام قاعدة بيانات دفتر محاسبي دون بناء شجرة ميركل من رمز التجزئة للكتلة السابقة و نتيجة الصفقة.

شجرة ميركل (TTH) هو نوع من وظيفة التجزئة المستخدمة للتحقق من سلامة البيانات، للحصول على معرف فريد للسلسلة، واستعادة التسلسل. تنقسم البيانات إلى أجزاء صغيرة - كتل التي يتم تجزئتها بشكل فردي باستخدام تجزئة ورق تايغر، ثم يتم احتساب ورق التايغر المُجزأ من كل زوج من التجزئة واحد مقابل واحد. إذا لم يكن للتجزأة قرين، بعدها يتم

نقلها إلى سلسلة جديدة دون تغيير. بعدها، يتم احتساب تجزأة التايغر المُجزأة مرة أخرى في سلسلة لكل زوج. يكرر هذا الإجراء حتى يكون هناك تجزئة واحدة متروكة.

عندما يتم تشغيل الدفتر المحاسبي باستخدام أشجار ميركل، سرعة معالجة المعاملات تكون منخفضة جدا، والحمولة على موارد الحوسبة عالية جدا. في رأينا، هذا ليس استخداما منطقياً لتخزين البيانات.

هيكل الدفتر المحاسبي لكريديتس

نحن نقترح أن نستغني عن أشجار ميركل و نستخدم معاملات الدفتر المحاسبي في نظام كريديتس؛ مع كل إدخال يتكون من رمز التجزئة لكتلة الصفقة لإضافتها إلى قائمة المرشحين بالإضافة إلى الدفتر المحاسبي. أيضا، يحتوي الإدخال على معرف العقدة والطابع الزمني عندما تم إنشاؤه. يحتوي مدخل الدفتر المحاسبي على اتجاه المعاملة، والحسابات الأولية والنهائية، ونوع الكتابة، وعدد وحدات الكتابة، ونوع الإيداع، وعدد وحدات الإيداع. هذا المبدأ يزيد من سرعة معالجة المعاملات، ويزيد من تعقيد تغيير الدفتر المحاسبي الغير شرعي ويستبعد التغييرات المحتملة في إدخال الدفتر المحاسبي بعد فوات الأوان.

حجم الكتلة

وحدة الوقت هي دورة البحث عن العقد الرئيسية والموثوق بها، ويتم احتساب وقت الدورة اعتمادا على تعقيد الشبكة. لكل وحدة من الوقت، تحتوي الشبكة على المعاملات N التي تم إنشاؤها ونقلها للمعالجة إلى الشبكة من نهاية الدورة السابقة، حتى بداية الدورة التالية، للحصول على وضع "المرشح ليتم إضافته إلى الدفتر المحاسبي." يتم وضع المعاملات المختارة من الشبكة N على الكتلة. حجم الكتلة يعتمد على عدد المعاملات فيها.

البحث عن المشاركين في المعاملة

كريتدس شبكة أنداد يمكن تمثيلها كرسم بياني، مع حسابات المستخدمين على شكل قمم والعديد من المعاملات الممكنة في شكل حدود موجهة التي تربط اثنين من القمم (حساب). بما أن جميع الحدود لها قمة مبدئية وقاعدة طرفية، يمكنك دائما إنشاء رسم بياني موجه (orgraph).

إذا أخذنا الشروط التالية لتحديد الهوية:

- أي معاملة لديها دائما مرسل ومستقبل؛
- أي قمة (حساب) يمكن دائما أن يكون متصلا بقمة أخرى مع هامش موجه (المعاملة).
- أي قمة في الرسم البياني (حساب) لديها عدد محدود من الحدود الموجهة (المعاملات الواردة والصادرة).

في ما يتعلق بما سبق، يمكننا القول أن أورغراف orgraph يحتوي على المسار المطلوب لتحقيق شروط الصفقة اللازمة وبناء سلسلة بسيطة. نظرا لأنه هو تسلسل محدود من القمم، حيث يتم توصيل كل قمة (باستثناء الأخيرة) إلى القمة المقبلة في التسلسل بواسطة الهامش.

قناة نقل البيانات

كل قناة اتصال بين عقدة الشبكة الرئيسية والعقدة المشتركة لشبكة كريديتس عبارة عن مؤشر ترابط منفصل (تعدد العلامات)،حيث يتم إرسال البيانات بشكل مشفر عند تنفيذ المعاملة.
لضمان أمن الشبكة، يتم نقل كافة البيانات بين عقد المصادقة في نموذج مشفر، وكل اتصال بين العقد يكون منخفض المستوى استنادا إلى مكتبة الشبكة. في حالة حدوث نقل البيانات مع وجود خطأ، يجب أن يتم قطع مؤشر الترابط تلقائيا، يتم وضع الإدخال المقابل للكتابة إلى نظام التسجيل ثم إلى ملف السجل. يتم نقل البيانات من خلال المتغيرات التي تم وصفها. يتم تشفير البيانات المرسلة باستخدام خوارزمية متماثلة RC4. وبما أن هذه الخوارزمية تعمل تحت مفتاح سري معروف، يتم نقل هذا المفتاح عند إنشاء اتصال بين العقد ويتم إرساله بشكل مشفر وفقا لخوارزمية Diffie-Hellman.

خوارزمية RC4، مثل أي تيار شفرات، تم بناؤه على أساس مولد بت pseudo-random. يتم كتابة المفتاح في مساهمة المولد، ويتم قراءة بت pseudo-random في الناتج. يمكن أن يكون طول المفتاح من 40 إلى 2048 بت. ولدى البتات المتولدة توزيع موحد.
خوارزمية Diffie-Hellman يسمح لطرفين بتلقي المفتاح السري المعروف باستخدام قناة غير محمية من الاستماع من خلالها ولكن محمية من تغيير قناة الاتصال. يمكن استخدام المفتاح المستلم لتبادل الرسائل باستخدام التشفير المتماثل.
تستند الخوارزمية على تعقيد حساب اللوغاريتمات المنفصلة. في ذلك، كما هو الحال في العديد من الخوارزميات الأخرى بالمفتاح العمومي، الحسابات تنفذ قياس مودولو إلى عدد رئيسي كبير معين P.
أولا، يتم اختيار عدد طبيعي معين A، أصغر من P، بطريقة خاصة. إذا كنا نريد تشفير قيمة X، بعدها نحسب
.Y = AX mod P
وأنه من السهل حساب Y بوجود X. المشكلة العكسية لحساب X من Y معقدة نوعا ما. ويسمى الأس X بالضبط اللوغاريتم المنفصل Y. هكذا، مع معرفة مدى تعقيد حساب اللوغاريتم المنفصل، يمكن نقل الرقم Y علنا على أي قناة اتصال، نظرا لأن المقياس الكبير P تكون القيمة الأولية X مستحيل حسابها و التقاطها. تستند خوارزمية Diffie-Hellman لتوليد مفتاح على هذه الحقيقة الرياضية.
ترتبط أي إجراءات في النظام إلى الطابع الزمني، عدد من الكتلة السابقة، تسجيل الدخول للمستخدم، ومعرف العقد الذكي. هذا يسمح بالبحث عن التكرارات عند التنفيذ. إذا تم العثور على تكرار، بعدها نأخذ الصفقة الأولى من التجمع، والباقي تعتبر غير شرعية.

الإجراء في النظام

الإجراء في النظام هو معاملة تميز أبسط نقل للقيمة من حساب إلى حساب أو نقل نتيجة طريقة العقد إلى جهة المصادقة، للبحث اللاحق عن حل في النظام الفرعي للبحث المتفق عليه.

من أجل منع الازدواجية في المعاملة لنفس الكتلة بنفس المعرف، يقبل النظام اتفاقا بأن المعاملة الحقيقية الصحيحة هي التي جاءت أولا إلى النظام المصادقة الفرعي للمعالجة. بما أنه تم تسجيله بالفعل في نظام المصادقة بأن المعاملة قد تمت بالفعل من الحساب الجاري ولا توجد قيم متبقية في الحساب لإجراء المعاملة، لا يمكن العثور على اتفاق بالرأي. وهكذا، يتم حل مشكلة الضياع المضاعف.
عند تنفيذ المعاملة، يتم استلام المعلومات إلى جهة المصادقة وتأكيدها، يتم توزيع المعلومات حول تغيير حالة الدفتر المحاسبي تلقائيا إلى جميع العقد من قائمة موثوق بها، وبعد ذلك تتم مزامنة الدفتر المحاسبي.
من أجل أن يكون دائما معاملات الدفتر المحاسبي حديثة بين جميع العقد الموثوق بها لعقدة المصادقة الحالية، فمن الضروري مزامنة الصفقة التي وصلت حديثا في الدفتر المحاسبي لجميع العقد في كل مرة. لحل هذه المشكلة، ينبغي استخدام منفذ منفصل للمزامنة (إذا كان هناك مثل هذه الفرصة). هذه الفرصة سوف تزيد من سرعة معالجة المعلومات الواردة إلى جوهر المصادقة بسبب توزيع الحمل على المنفذ. يتم تنفيذ موضوع التزامن دائما، الذي يعتبر دوري. أولوية تخصيص ذاكرة الوصول العشوائي وحمولة وحدة المعالجة المركزية (باستخدام دورات وحدة المعالجة المركزية) هو أقل من المتوسط. تخزن الذاكرة آخر 1000 عملية وحالة الحسابات الخاصة بهم (في شكل مشفر باستخدام خوارزمية متزامنة)، وهذا يزيد من سرعة الاستجابة للطلبات من عقد المصادقة الأخرى.

إضافة معاملة للتحقق

تُستدعى إضافة المعاملات إلى الدفتر المحاسبي فقط من النظام الفرعي للمصادقة المباشرة بعد بناء توافق الآراء وتجميع قائمة بيضاء نتيجة للعمليات المحفوظة في الدفتر المحاسبي. ومن المستحيل استدعاء أنظمة طرف ثالث، من أجل تحسين الأمن.
العوامل الواردة - الهجف الذي يميز المعاملة. القيمة الناتجة ResultValue 0>
- يتم إلغاؤ التنفيذ مع خطأ، القيمة الناتجة هي رمز خطأ ممكن / 0 < ResultValue- تم تنفيذ الدالة دون أخطاء، النتيجة هي عدد المدخلات في الدفتر المحاسبي.
العامل الوارد - الهدف الذي يحتوي على التسمية الفريدة للمعاملة، المرسل، المستلم، القيمة المنقولة، مراسلات القيمة، القيمة المطلوبة، مقدار القيمة المنقولة، مقدار القيمة المطلوبة ومعلومات النظام الأخرى التي يمكن يتم تغييرها إذا لزم الأمر.

تكلفة المعاملات

يستخدم النظام عملة كريديتس، التي تخدم:
- كوسيلة داخلية للدفع لاستخدام النظام.
- تبادل العملات المختلفة داخل النظام.
- تبادل القيم المختلفة داخل النظام.
- إنشاء ومعالجة العمليات بموجب عقود ذكية.
- شراء معلومات من مصادر الطرف الثالث للخدمات داخل النظام.

تكلفة الصفقة يمكن أن تختلف اعتمادا على تحميل الشبكة، على مستخدم معين للنظام، والتي يمكن نظريا أن توجه تدفقاً ضخماً من المعاملات في وقت الذروة معينة. نقترح استخدام طريقة المواد والتأثير على مستخدمي النظام للتحكم في تحميل الشبكة.
سيتم تحديد تكلفة أداء المعاملات في السنوات الثلاث الأولى لتشغيل النظام بشكل فردي لأنواع مختلفة من المعاملات والعمليات. في المستقبل، سيتم تطوير خوارزمية للتوليد التلقائي لتكلفة المعاملة.

4. العقود الذكية

المقدمة

العقد الذكي في نظام كريديتس هو خوارزمية إلكترونية تصف مجموعة من الشروط التي يمكن من خلالها ربط الإجراءات والأحداث في العالم الحقيقي أو الأنظمة الرقمية.
لتنفيذ عقود ذكية ذاتيا، بيئة لامركزية التي تستبعد تماما العامل البشري تكون مطلوبة، و لتستخدم نقل تكلفة العقد الذكي، مطلوب عملة رقمية مستقلة عن السلطة المركزية.

الكيانات

عقد ذكي في كريديتس يتكون من الكيانات التالية:
1- الممتلكات (المتغيرات العامة) - كيان النظام الذي يخزن البيانات العامة اللازمة لعمل العقد في نظام كريديتس.
2. الطريقة هي كيان نظام كريديتس المسئولة عن مراقبة منطق وتسلسل الإجراءات عند إجراء المعاملة (الإجراءات بموجب العقد).
المشاركون في نظام كريديتس يوقعوا العقود الذكية باستخدام استدعاء الطريقة التي تعدل خصائص العقد، من خلال إطلاق عمليات للتحقق من الامتثال للشروط والتنسيق.
يبدأ سريان العقد الذكي بعد توقيع الطرفين. لضمان الوفاء الآلي بالالتزامات، فإن بيئة الوجود تتطلب أتمتة لتنفيذ شروط العقد. هذا يعني أن العقود الذكية يمكن أن توجد فقط ضمن بيئة لديها إمكانية الوصول دون عراقيل إلى التعليمات البرمجية القابلة للتنفيذ لعناصر العقد الذكية.
يجب أن يكون لجميع شروط العقد وصف رياضي ومنطق واضح للتنفيذ. وبالتالي، فإن المبدأ الرئيسي للعقد الذكي هو الأتمتة الكاملة وموثوقية العلاقات التعاقدية بين الطرفين.

نموذج العقد الذكي

نموذج التعاقد الذكي كريديتس هو كيان النظام المسئول عن الامتثال للمنطق وتسلسل الإجراءات خلال المعاملة (الإجراءات بموجب العقد).
يتم وصف منطق وتسلسل الإجراءات من خلال رمز البرنامج (وحدة) تحتوي على الأوامر؛ التنفيذ المتسلسل يسمح للحصول على النتيجة المرجوة. يمكن لهذه التعليمات البرمجية التعامل مع أوامر النظام (على سبيل المثال، أمر التعيين) وأوامر المستخدم (وظائف مكتوبة بشكل منفصل) وخصائص العقد (المتغيرة بشكل ثابت أو ديناميكيا المتغيرات المتاحة من أي طريقة العقد)، ونماذج من أي عقد طرف ثالث آخر المتاحة فقط لمالك العقد المتصلة (الطرف الثالث). لمزيد من التعميم، يتم توفير التطوير في لغات البرمجة النصية (على سبيل المثال، جافا سكريبت).

نموذج (رمز البرنامج) يسمح باستخدام جميع مشغلي لغة البرمجة النصية (الأوامر) المستخدمة على نطاق واسع (التخصيص، القفزات المشروطة وغير المشروطة)، إنشاء وظائف وإجراءات (الفرعية)، اتصال مكتبات الطرف الثالث.

آلة التنفيذ الظاهري

يتم تنفيذ نموذج العقد لنظام كريديتس في البيئة الافتراضية للنظام (الجهاز الظاهري، ويشار إليها فيما يلي باسم VM).
عندما يتم استدعاء طريقة لعقد معين، VM يخصص منطقة الذاكرة ويُحمّل عقد البيتيكود bytecode فيها والذي يحتوي على الأساليب والمتغيرات المُبتدأ بها (أو إعادة التعريف عند استدعاء نماذج العقد الأخرى). VM يبدأ بمعالجة نموذج بيتيكود bytecode ، في وقت التشغيل، يتم تحميل المتغيرات والرمز في منطقة الذاكرة الخاصة به، ويتم تنفيذ الأوامر تباعا، يتم نقل نتائجها إلى شبكة الأنداد لوضع لاحق في الدفتر المحاسبي.
البادئ لطريقة التنفيذ هو المستخدم للنظام، الذي أطلقت نيابة عن هذا النموذج.

القيمة
عملة كريديتس الرقمية هي أيضا مؤشر على قيمة مصطلح وحدة العقد لمقارنة وحدتين مختلفتين تماما وبناء توافق في الآراء عند تنفيذ أو قبول العقد من قبل الطرفين. بدلا من تسجيل كل قيمة منفصلة / الجمع، عملة كريديتس الرقمية بمثابة باقة لتنفيذ تحويلات القيمة. هذا ممكن لأن أي قيمة يمكن أن تكون سلسة فيما يتعلق بعملة كريديتس، وهو ما يعني أن أي قيمة يمكن أن تكون سلسة فيما يتعلق بأي قيمة أخرى.

تنفيذ شروط العقد الذكي

مدة العقد في نظام كريديتس هي قيم حقول نشطة (فحص) المطلوبة لإغلاق (إكمال) العقد.
تحقيق شروط العقد الذكية هو إجراء عندما يتم فحص الحقول النشطة (المطلوبة) للحصول على قيمة مكافئة مرغوبة.
هناك ثلاث طرق ممكنة لإيجاد حل للوفاء بشروط العقد:
1 - يبرم العقد بين طرفين أو أكثر لنقل القيمة. وفي هذه الحالة، يكون الوفاء بالعقد هو توفير التكلفة المعادلة للقيمة للطرف المتحول من الطرف المتلقي.
2. يتم إبرام العقد بين الطرفين لتحويل القيمة، ولكن يجب أن يتم السداد عند الوفاء بعدد معين من الشروط (على سبيل المثال، تسليم القيمة إلى الطرف المتلقي).
3 - يوضع في النظام نظام لتحويل قيمة واحدة إلى قيمة أخرى مع تكلفتها في شكل ائتمانات. في هذه الحالة، يبدأ النظام الأساسي بالبحث عن أقصر مسار ممكن لتبادل قيمة واحدة لأخرى من خلال التحويل في عقود أخرى. يمكن تقديم أي إبرام للعقد في معاملة واحدة أو في عدة معاملات، مما سيتيح فرصة لجمع الكمية المطلوبة من وحدات القيمة لإتمام العقد.

مصادر البيانات

للحصول على عمل سليم ومطابق تماما، التحقق من وتوفير معلومات إضافية، لإيجاد حل أكثر توازنا وأفضل، تستخدم كريديتس موفري بيانات طرف ثالث. تعزى الحاجة إلى إدخال مصادر بيانات إضافية في النظام إلى عدم كفاية المعلومات العامة عن طرف أو عدة أطراف متعاقدة (على سبيل المثال، الحصول على المركز الائتماني للمقترض لاتخاذ قرار بإصدار الائتمان).
للعمل مع أنظمة معلومات الطرف الثالث، يمكن للمنصة استدعاء مجمّع التكامل، عن طريق الوصول البعيد الذي يولد طلب لنظام طرف ثالث (الموقع) في شكل لعرض البيانات على أساس مدفوع للمشاركين للنظام مع الدفع في شكل عملة كريديتس.
يتم إرسال الطلب في نموذج مشفر إلى الموانئ والعناوين التي تقدمها نظم المعلومات الأخرى غير تلك القياسية. يمكن أن تكون نتيجة الطلب أي رد على الخدمة التي تحتوي على المعلومات الضرورية لاتخاذ قرار، أو رمز خطأ يميز استحالة تلقي الاستجابة المطلوبة والخطوات الممكنة للقضاء على الخطأ.

5 - خطة التنفيذ

الخطة الفنية لتنفيذ المشروع

	S1	S2	S3	S4	S5
	ما قبل مرحلة ألفا	مرحلة ألفا	النسخة التجريبية	إصدار المرشح	الإصدار
التخزين ، الإجماع و اتفاق الآراء عن المصادقة متعددة المراحل	مصادقة باستخدام عامل واحد : تنفيذ التصميم	مصادقة متعددة العوامل:تصميم تنفيذ مبدأ إثبات العمل و إثبات القدرة	تهيئة مصادقة متعددة العوامل	-	-
تخزين البيانات	دفتر محاسبي لامركزي،تنفيذ تخزين NoSQL	تاريخ MessagePack	-	دعم بلوكشين	-
آلة كردتس الافتراضية	تصميم وتنفيذ	الدمج بالنظام الاقتصادي	تهيئة	فحص الأخطاء	-
نظام الطرف الثالث	-	تصميم و تنفيذ	دمج بكامل النظام	-	تحسين
واجهة المحرك	تخصيص رسمي و عوامل التصميم الأساسية	دمج المنطق ببلوكشين	المنطق الأمثل	-	-
المحفظة	تخصيص رسمي للمحفظة	-	اختبار تطبيق تصميم خبرة المستخدم UX	-	محافظ مكتبية ، محافظ نظام أندرويد و نظام آيفون
واجهة برمجة التطبيقات RPC & REST	تخصيص رسمي	مستكشف بلوكشين	-	مستكشف طرف ثالث	-
واجهة المستخدم	تنفيذ	تصميم ويب خبرة المستخدم UX	-	-	-

العملة الرقمية كردتس

بعد إطلاق إصدار النظام، سيتم إصدار مبلغ ثابت من 1000000000 كريديتس. سيتم تبادلها بتوكنز ERC20 القياسية، الصادرة في بيع التوكن الأولي. سيتم تبادلها بسعر صرف ثابت: 1 توكن معياري ERC20 = 1 وحدة مقدية لكريديتس.