

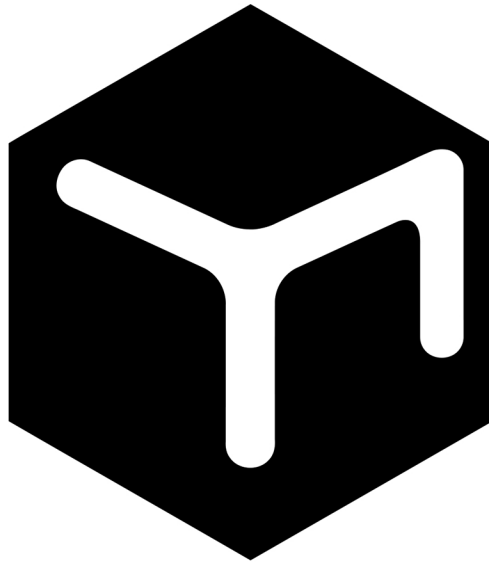
Relictum Pro

Blockchain 5.0

Decentralized Ledger Technology

Yellowpaper

version 2.05.21.ru-2



Relictum Pro

Blockchain 5.0

Global platform covering all the aspects
of human life in a distributed registry

With the use of HYPERNET technology based
on peer-to-peer peering networks

Relictum Pro

ملخص

Relictum Pro يمثل أحدث جيل من بلوكتشين من

Blockchain 5.0.

المتضمن للشروط الأساسية والكافية اللازمة لضمان

عمل الجيل الرابع من blockchain حيث :

1. هايبر نت - شبكة رباعية الأبعاد لتبديل القنوات الافتراضية.
2. سلسلة تنظيمية متعددة (عقود - ذكية) مع منافذ لحظية.
3. منصة عالمية لإضفاء الطابع الرسمي على جميع الأحداث في المجالات الاقتصادية والأنشطة اليومية للبشر والدول
4. سرعة تسليم الرسالة (حزمة) إلى كل عقدة من 100,000 TPS / ثانية.
5. دوائر ديناميكية.
6. هرمية ادوار العقد
7. تجديد الشبكة.
8. استبعاد الغموض .
9. قابلية التوسع. يختلف في أن محفظة الملفات الثنائية متطابقة تماماً.
10. توزيع التخزين. حتماً ، هناك حاجة إلى إنشاء توزيع للتخزين ، لأن التجزئة البسيط لأحداث التوقيع الرقمي لا يضمن تخزين المحتوى نفسه والتزويد اللاحق بالوثيقة في شكل خاص ومشارك.
11. تزامن مع الوقت .
12. باستخدام مولد الرقم العشوائي المثالي على أساس (الحصول على البيانات (قراءات - الطاقة المنخفضة لكل بكسل انبعاث راديو خلفي (تقدير كمي).
13. يجب التحقق من تكامل الملف الثنائي ، سواء في الوضع الثابت أو تحميله في الذاكرة ، بواسطة موارد خارجية.
14. ثلاثة مستويات لاختيار سلامة الدارة. لتلقي تجزئة ، تجزئة كاملة ، تجزئة على فترات ، و المجموع الاختباري.

المحتوى

6	مقدمة
7	الوظيفية
7	1. الملف
8	2. سلسلة من كتل
9	3. توزيع التخزين
11	مبدأ التواصل. بروتوكول الشبكة
11	1. الملك
11	2. المستوى Z الجنرالات
11	3. مستوى - P العقدة العادية
12	4. مستوى - L العقدة الخفيفة
13	5. مستوى - S العقدة الخاصة
13	6. مستوى O - زلة العقدة
13	7. العقدة السحابية
14	جدول وظائف أنواع العقدة
15	هندسة الدارة
16	مجال التطبيق
16	الحقوق
16	التأمين
16	المالية
16	الطب
16	اللوجستية
16	مشاكل سوق التذاكر
16	الهيدروكربونات
17	الرمز وتصنيفه
17	وسائل الدفع
17	رمز المنفعة
17	أصول الاستثمار الرقمي
17	رمزية الأصول
17	الرموز
17	بنية النظام (المعمارية)
18	المراحل الرئيسية لتشغيل الشبكة
19	خوارزمية التشفير
19	وضع التسجيل
19	أهداف شبكة بلوكتشين
19	المستودع (الوظيفة)
20	الصيغ والتنفيذ
20	مثال للتعيين
21	مولد الصيغة شبه العشوائية والحصول على سلاسل التجزئة

21	1. توليد قيمة ابتدائية للسلسلة
21	2. توليد العنصر التالي للصف
	GenP [byte] ،
	نتيجة التوليد
21	3. الحصول على تجزئة الخط الوسيطة
	Nth
22	تجنب الأخطاء الكامل لسلسلة الكتل
22	مكرتك العقد الذكي
23	التحقق من سلامة العقدة
	1. وحدة للتحقق من سلامة كتل سلسلة
	كاملة
23	2. وحدة للتحقق من سلامة كتل سلسلة
	من الجميع
	المعاملات الخاصة
24	3. وحدة لفحص الملف الثنائي المحلي
24	(الأصلي) القابل للتنفيذ
25	4. تشغيل البرنامج المساعد
	الحصول على سلسلة التجزئة
25	المرحلة الأولى
25	المرحلة الثانية
25	المرحلة الثالثة
26	المرحلة الرابعة
26	المرحلة الخامسة
26	القائمة
27	

مقدمة

نقدم منصة – IaaSB ذات بنية تحتية في شكل خدمة ، حيث B محفظة .

قيمة - جميع الأحداث التي يتم إنشاؤها بواسطة الشخص و التي تحدد قيمته ومقاومة الوصول غير المصرح به للمعلومات.

Relictum Pro هي أول خدمة بلوكتشين عالمية تقدم فرصة لتحقيق الاستخدام الأمثل للمعدات الحديثة مع أساس عظيم للمستقبل.

السمات الرئيسية تشمل:

1. الاستقلال عن النقل. أي لا حاجة لاستخدام شبكة الإنترنت ، يمكنك استخدام WiFi ، Bluetooth ، شبكات الهاتف ، اتصالات الألياف البصرية ، وحتى نقل المعلومات من خلال محرك أقراص فلاش USB أو الشبكات الضوئية الكمية الواعدة.

2. الاستقلال عن نوع العميل (جهاز رفيع ، أو سميك ، مركز بيانات وأجهزة الضغط على زر المحمول) ، حيث يوجد أي نوع من نظم التشغيل.

3. TPS قريب من سمك قنوات Masternode.

4. لديها توزيع 100 ٪. لفترة محدودة من الوقت ، خلال يوم واحد من blockchain شبكة تشغيل الشبكة التشغيل تصل إلى 100000 مرة أي من العقد التي تقبل حلول للشبكة بالكامل. يرتبط تفويض بروتوكول السلطة مع مولد رقم عشوائي مشتق من خلفية بقايا انبعاث الراديو ، كأفضل وصف لمنحنى توزيع غاوسي الطبيعي

5. تنظيم العقد الذكية المكرنة.

6. توافر دوائر ديناميكية لتخزين البيانات الديناميكية على سبيل المثال للركب الوجستية المتكررة للعقود الذكية

7. باستخدام ترقيم التجزئة للسلاسل من نهاية إلى نهاية لضمان القضاء على النزاعات لفترة طويلة

8. توزيع التخزين. التفتت والتمييز وضع البيانات الرقمية على أجهزة المستخدم ، الذي يحتوي على عقدة

9. توفر خوارزمية نقل الكتل عبر الشبكة إلى كل عقدة دورة كاملة ، عندما تتلقى جميع العقد هذه البيانات: 100 ٪ - (ناقص) السكون (الصيغة)

10. العقدة يمكن لها الخروج من الانزلاق فقط عند اكتماله التهيئة مع تأكيد ملزمة للسداد ، و استلام التجزئة ، والتحقق من التجزئة ، والتحقق من الملف الثنائي بواسطة مورد خارجي مع سلاسل ضخ كاملة.

وظيفي

عقدة (حافظه)



ع.ذ.ص. - عنصر الذكاء الاصطناعي

تتكون العقدة من ثلاثة كيانات:

1. محفظة.
2. سلاسل الكتل.
3. توزيع التخزين.
1. **الحافظة :**
- ملف ثنائي يحتوي على العناصر التالية:
1. إدارة العقد.
2. المستكشف.
3. مولد العقود الذكية.
4. إنشاء IO.
5. مولد الرموز.

6. المعاملات الوظيفية لجميع أنواع العملات.
7. درشة خاصة.
8. تغيير العملة.
9. التشخيص الذاتي.
10. تحديث الموارد.
11. الحماية ضد الأنهيبار.
12. ملزمة للسداد.
13. وحدة الاتصالات مع مورد خارجي للخروج من وضع الانزلاق.
14. وحدة التهيئة API.
15. وحدة التهيئة SDK.
16. وحدة تهيئة منخفضة المستوى API (المقبس).
17. وحدة العمل مع توزيع التخزين.
18. وحدة إذن.
19. وحدة القياس الحيوي Biohesh.
20. وحدة تزامن الوقت (تشغيل على مدار الساعة)
21. وحدة لتلقي البيانات من مصدر بيانات خارجي حيث بقايا الإشعاع في شكل تطبيع ثلاثي الأبعاد على البطاقة الرقمية.
22. وحدة قفل الوضع. تستخدم لمنع الوصول غير المصرح به إلى كل من الملف الثنائي والجزء من ملف التطبيق الذي تم تنزيله.
23. وضع علامة وحدة التشخيص الذاتي.
24. وحدة التدمير الذاتي. في حال وجود أي تباين للجزء الحرجة التي تؤدي إلى تغليف البرامج داخل التطبيق الذي يزيل كل شيء من الموارد ، بما في ذلك بيانات مصادقة المستخدم.

2. سلاسل الكتل :

1. سلسلة الكتل عبارة عن مصفوفة n ثلاثية الأبعاد للسلاسل مع العقود الذكية التي تحكمها آلية توقيع التجزئة للسلاسل مع تأكيد إلزامي ووضعها في السلسلة الرئيسية من كل معاملة.
2. يتراوح حجم كل كتلة من 120 إلى 300 بايت. في الوقت نفسه ، يتم ترقيم كل كتلة بشكل مستمر في مصفوفة n -الأبعاد.
3. يتم تنظيم البنية التحتية الارتباط لهذه الكتل على النحو التالي. الطريقة التي يحدث بها استرداد البيانات من النهاية إلى البداية. إنه كذلك النتائج في المعلومات لحظية تقريبا البيانات في مصفوفة n الأبعاد. على سبيل المثال: للحصول على قوائم لجميع معاملات العملة المشفرة التي تنتقل من آخر مرجع إلى أوله، هذه القائمة تحصل بصورة لحظية، متجاوزة الكتل الوسيطة بسبب تر

قيم الكتل في المصفوفة. انها تسمح بتحليل أي بيانات في blockchain محليا ؛ لبناء الرسومات. إيجاد طرق لتقاطع البيانات ؛ و لإدارة عقود ذكية ديناميكية. حساب تحليلات البيانات محرف وتقريبية و وظيفة استقراء لحساب التوقعات لفترة طويلة بما فيه الكفاية

4. وجود كتل ديناميكية.

5. يمكن لكل مالك عقدة إنشاء قاعدة بيانات خاصة به. للتفاعل مع الكتل الديناميكية (العقود الذكية). في قاعدة البيانات هذه يمكن التخزين ، على سبيل المثال ، مظهر الطرف المقابل وهلم جرا. أيضا ، ديناميكية ذكية يمكن تطبيق العقود على أنها مفصلية عقود ذكية.

3. توزيع التخزين

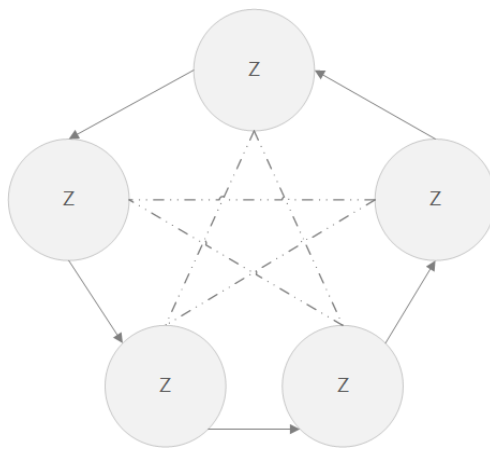
1. يجب حيازة عقد ذكي لتوزيع التخزين و تأكيد صاحب الحافظة على استخدام موارد آلة الحوسبة.
2. الحد الأدنى للكمية المخصصة للبيانات هو 200 ميجابايت. الحد الأقصى- غير محدود.
3. تهيئة توزيع التخزين في الحافظة يسمح للمالك للكسب على عدد المكالمات إلى قاعدة بيانات توزيع التخزين.
4. توزيع التخزين يستقبل البيانات كما هي (في شكل مجموعة من بايت) ولا يتحكم في محتويات قاعدة البيانات. ويتم الاعتناء بمحتويات قاعدة البيانات من قبل Noda ، و الذي يضع تخزين البيانات متباينة عبر الشبكة بالكامل.
5. يمكن أن يكون لكل عنصر بيانات طول مختلف ، من 1 بايت إلى الحد الأقصى لقيمة تسجيل الكمبيوتر (264)
6. يتم تخزين المعلومات حول قطعة بايت في عقد ذكي (سلسلة) توزيع التخزين
7. يحدث تكرار قطع تسلسل البايت مرارا وتكرارا على العقد المختلفة للقضاء على فقدان البيانات.
8. يمكن لمالك البيانات التي تم وضعها في وحدة التخزين الموزعة وضع الملف بالكامل في قاعدة البيانات الخاصة به في محفظته ، سواء المشفرة والمشاركة.
9. البيانات المخزنة في المستودع لها حالة من عرض البيانات المفتوحة إلى القطع المختلطة بالفسيفساء. قد تكون البيانات مشاركة أو خاصة.

10. عند تهيئة مستند جديد ، يتم إجراء فحص لموضوعية وموثوقية البيانات لاستبعاد البريد العشوائي.

11. وضع بيانات في موزع تخزين يتم احتسابه مقابل استبعاد البريد العشوائي.

مبادئ التواصل. بروتوكول الشبكة:

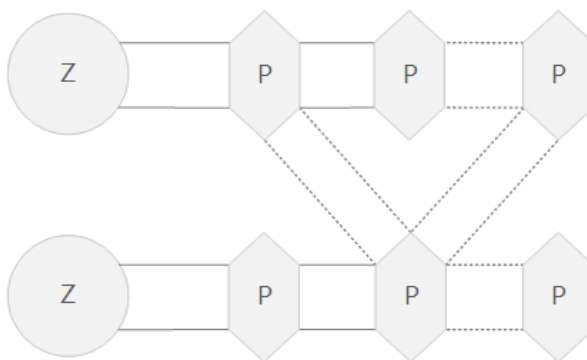
1. الشبكة لديها 5 مستويات:
1. الملك.
2. مستوى - Z الجنرالات.
3. P المستوى - العقدة المعتادة.
4. L مستوى العقدة الخفيفة.
5. S مستوى العقدة الخاصة.
6. O مستوى العقدة المنزلقة.
7. العقدة العادية.
2. مستوى Z (الجنرالات) (مستوى الصفر)



(1) اي منهم مالك لكن غير معروف.

(2) جميع Z تعمل ككمبيوتر واحد مع

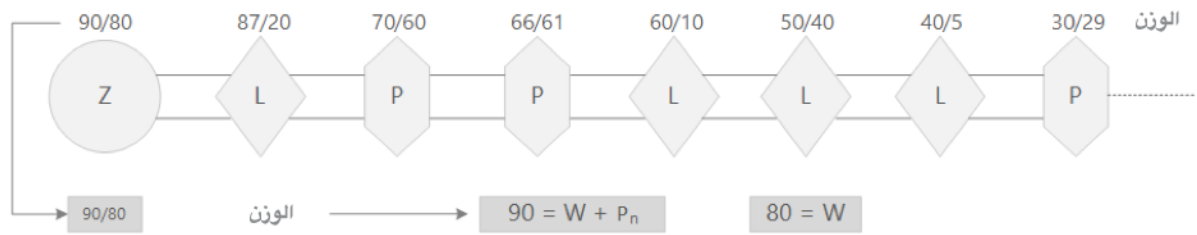
3. مستوى P (مستوى الطاقة) من عقدة المستوى الأول



سلاسل Z-P.

نقل CC
(تبادل قنوات)

4. مستوى L (العقدة السهلة) المستوى الثاني



حيث

W- الوزن الحالي للعقدة

P_n - نتيجة الصيغة

$$P_n = G_p [R]$$

حيث

G_p مولد الأرقام العشوائية الزائفة

R اختيار من بقايا تطبيعها إلى المدى (1-100%)

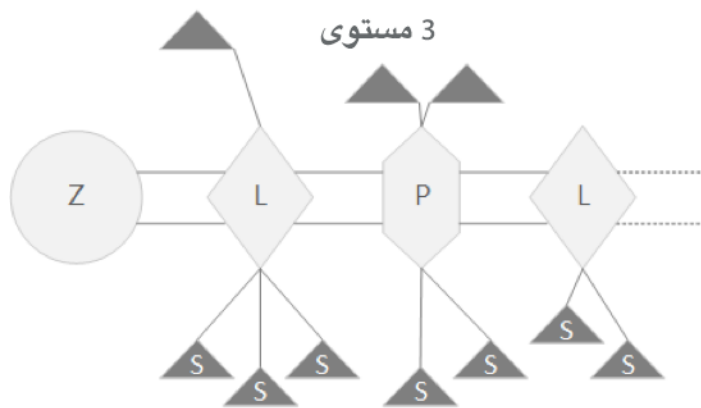
صيغة الوزن (الحالية + ديناميكية)

$$W_d = W + G_p [R_n]$$

G_p الرقم في مجموعة R_n

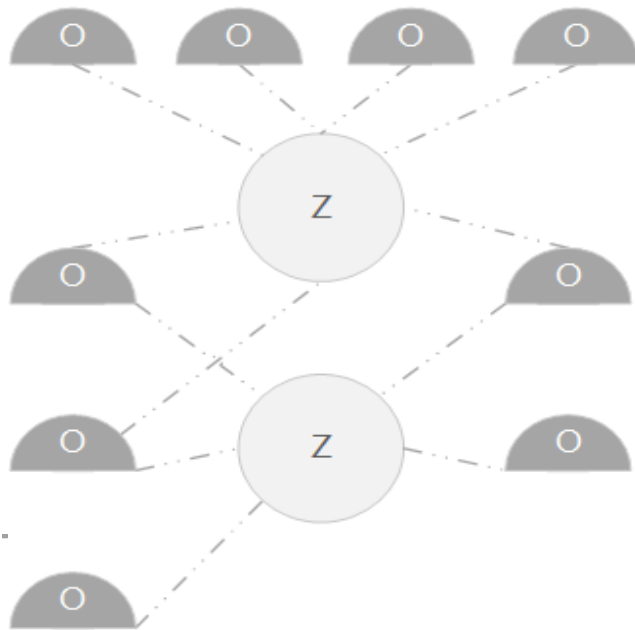
حيث n هو رقم تجديد الشبكة.

5. S (عقدة ذاتية) = عقدة خاصة









1. المعاملات الخاصة
2. العقد المحددة
(فقط معاملاتهم)
3. إذن التخزين معطيات توزيع
مرافق التخزين

6. O (عقدة غير متصلة) = عقدة الانزلاق



1. محاولة الاتصال
- عقدة Z.
2. الحصول على عنوان اتصالات (IP).
3. تحقق النزاهة الموارد المحلية.
4. تحقق السداد.
5. مزامنة التجزئة.

جدول وظائف نوع العقدة

0	1	2 W IP	3	4	5	6	7	8
0		+	+	+	+	+	+	-
1		+	+	+	+	+	+	-
2		±	±	+	+	+	+	-
3		-	±	+	+	+	+	-
4		±	-	-	-	-	-	+
5		-	-	-	+	-	-	+
								
								

0. رقم
1. الابهام
2. الأبيض IP
3. تصبح عامة
4. تصبح ملكا

5. بدء المعاملات
6. المشاركة في التصويت
7. الأرباح
8. تقييد التقييم

هندسة الدارة

S	سلسلة الماستر	1.
S	سلسلة الذكية 1	2.
S	سلسلة الذكية 2	
S	سلسلة الذكية N	
D	سلسلة ديناميكية	3.
	سلسلة ديناميكية 2	
	سلسلة ديناميكية 3	
D4	تتزامن سلسلة	مع العقد غير المكتملة التوازن
D5	سلسلة زمنية	ت حسب على مدار الساعة
D6	سلسلة التخزين	سلسلة العقد الذكية توزيع التخزين
D7	معلومات سلسلة	الحالة حول حالة جميع العقد في الشبكة

S - العقدة القياسية
D - العقدة الديناميكية

مجال التطبيق

الحق في:

القيمة ، والتدرجية ، والقدرة على تحمل التضخم والحوافز لاستخدامها

التأمين:

تعظيم الاستفادة من نموذج دفع أقساط التأمين
تخفيض أو القضاء على المخاطر الاحتمالية
الدفع التلقائي للأقساط باستخدام العقود الذكية
تحسين خدمة العملاء

لمالية :

تحسين آلية تحديد الهوية
تقليل المخاطر بين الأطراف المقابلة
الشفافية الكاملة لعملية تقديم الخدمة
معاملات سريعة عبر الحدود

الطبية :

تبسيط حفظ السجلات الطبية الإلكترونية
كفاءة جمع وإدارة البيانات من الأجهزة الطبية
شفافية تتبع سلسلة التوريد الدوائية
تحديث التأمين الصحي
عقد ذكي متعددة (التسليم)

الخدمات اللوجيستية:

كفاءة تتبع البضائع ، انخفاض احتمال الخسارة
انخفاض وقت التسليم
شفافية المعلومات اللوجستية
زيادة النطاق الترددي في سلسلة التوريد

مشاكل سوق التذاكر :

التزوير
التخمين

الهيدروكربونات:

فرص صناعة النفط والغاز Blockchain توفر تقنية
لحل مشاكل النقل عبر الحدود ، حجم كبير
المعاملات ، وتدفق وثيقة معقدة.

الرمز وتصنيفه

الرمز ، باعتباره التزامًا رقميًا ، يمكن تصنيفه على النحو التالي:

وسائل الدفع :

إنه مماثل للنقد التقليدي

رمز الأداة المساعدة:

ويضمن تشغيله. blockchain يستخدم كوقود داخل نظام

أصول الاستثمار الرقمي:

الأصول الرقمية التي لديها دعم قانوني الحقيقي ، وليس
العالم الرقمي

الأصول المشفرة :

الالتزام الرقمي بالتبادل لمنتج أو خدمة حقيقية

Tokenomika:

مجموعة من القواعد والنماذج الاقتصادية التي توفر
عمل مشروع اقتصادي يعتمد على الرموز.

النموذج الاقتصادي:

وصف رسمي لمختلف الظواهر الاقتصادية و
العمليات

بنية النظام (المعمارية)

كمهندس نظام يستخدم AGT ك (لعبة حساب نظرية)
الذي يضمن الانتهاء غير المشروط للمعاملات قبل الصفقة التالية.
يستخدم ايضا ك إثبات التتابع وإثبات المنفعة - دليل على العمل وإثبات الفائدة ، مما يؤدي إلى تسهيل غير
مشروط لاستخدام العقد من قبل قانون الألعاب النظرية.

الصفقة القادمة. تستخدم أيضا إثبات التتابع وإثبات المنفعة - دليل على العمل وإثبات فائدة ، مما يؤدي إلى تسهيل غير مشروط لاستخدام العقد من قبل نظرية قانون اللعبة.

المراحل الرئيسية للشبكة

وضع التجديد (التغييرات في الطوبولوجيا ، وتغيير) السلطة. طوبولوجيا البناء.

التجديد دائماً أو بناءً على طلب القراءة أو الكتابة (في النهاية قراءة أو كتابة الطلبات). إذا كانت الشبكة في وضع الخمول ، ثم التجديد يحدث في مهلة.

في هذا الوضع ، تتوقف الشبكة عن معالجة الطلبات (القراءات والسجلات) وعقد الشبكة (العقد) تحليل ، عدد (عمل الدورة السابقة – الوقت لمعالجة الكتلة ، سرعة الوصول (سرعة قنوات الاتصال المعاملات التي تمت معالجتها).

وفقاً لنتائج هذا التحليل يتم تصنيف طوبولوجيا الشبكة الفريدة (التسلسل الهرمي ، تصنيف) لما يليدورة. RCS اختيار الملك يحدث بشكل عشوائي بناءً على خوارزمية توقف الدائرة العشوائية ، (خوارزمية فريدة من نوعها) من بين الجنرالات في بداية وضع التجديد.

خوارزمية RCS هي لعبة مثل "الصخرة ، ورقة ، مقص". خلال الفترة المحددة لإنتاج حسابات متسلسلة (الحصول على بيانات عشوائية من الجدول الحالي للخلفية الموثوقة للانبعاث الراديوي).

عند انتهاء الوقت المحدد ، واختيار الملك. يأتي اختيار الجنرالات من أعلى العقدة التي حصلت عليها الصيغة صفحة رقم 4

$Wd = W + Gp [Rn]$ (العدد الذي يعتمد على تحميل الشبكة. في كل دورة ، يتم تحديث الجنرالات. (لا يمكنك أن تكون جنرال لدورتين في صف واحد). يحسب الملك (يتحقق ، يوافق) كل وحدة جديدة ويبدأ المعاملات المجمعة من قبل الجنرالات في الدورة السابقة.

بعد التحقق من كل كتلة من قبل الجنرالات ، تنتقل الكتل أسفل الشبكة إلى جميع العقد. يتم احتساب طوبولوجيا الشبكة الجديدة (التسلسل الهرمي) والموافقة عليها من قبل الملك في نهاية الدورة الحالية ويتم توزيعها عبر الشبكة من العقدة إلى العقدة ، وفقاً لطوبولوجيا كل دورة على الفرع المناسب .

على هذا النظام الأساسي ، مع المعالجة التلقائية للبيانات لا توجد هنا ديموقراطية

خوارزمية التشفير

إنها خوارزمية SHA-1 مع التحويل اللاحق إلى طريقة الانتقال الملكية ، والتي تستخدم خطأ Overflow غير المشخص للتجزئة في اتجاه واحد.

وضع التسجيل

أي عقدة التي تلقت معلومات للكتابة إلى blockchain يمر على أنها شبكة ، والملك يشكل كتلة بناء على المعلومات الواردة ، يكتب إلى blockchain ويتم نقل الكتل النهائية لجميع الجنرالات.

أهداف كتل الشبكة

- يمكن لأي عقدة الاتصال بهذه الشبكة المفتوحة بالكامل من أي مكان
- طوبولوجيا الشبكة تعزز المفصل الفعال باستخدام الشبكة.
- تأمين حيادية الشبكة من الابتكار على مستوى الشبكة.
- دائما مفتوحة وقابلة للتطوير.
- توجيه فعال وديناميكي.
- آلية التقييم (أتمتة عملية الحساب مع باستخدام آلية محاسبة رمزية ، كرسوم للمحافظة و التوس ، وتحسين اتصالات الشبكة والشبكة ، ونقل الأصول البيانات وتحفيز العقد المشاركة.
- تصميم وبناء شبكة الجيل القادم blockchain.

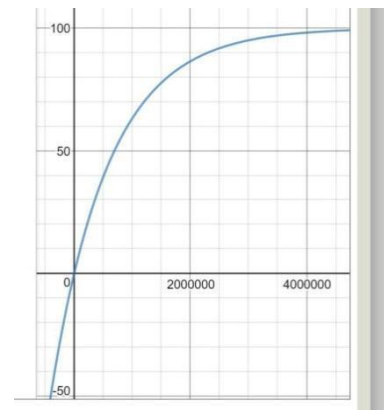
المستودع (الوظائف)

المستودع للعقدة (وضع السكون) التي لا تتعامل مع أداء الشبكة أو لسبب ما قطع الاتصال عودة العقد من المستودع عقدة الانفصال (البحث عن الجودة)

الصيغ والتتفيذ

دالة تعمل على إبطاء نمو وزن **Relict coin** (التكلفة) عند اللانهاية ولا تسمح لها بتجاوز التكلفة القصوى المحددة مسبقًا (الانبعاثات ، الوزن ...) $\% 100 =$ معادلة الزيادة في تكلفة **Relict coin** إلى 100 وحدة (%) ، على سبيل المثال دليل على عقد التعدين الذكي Mining للوقت:

$$y = -100e^{(-0.00082x)} + 100$$



أدناه هو الرابط للتحقق من الرسم البياني الصيغة:

http://www.yotx.ru/#!1/3_h/ubWwch@2cHBwf7Rgzhf23/aP9g/2DfT0qt7W9uHRysrW9sHkAODg5gO3u70K2Dg/2DfRINu7Fzyng83WI8bl1e7O5v7QMG

مثال التعدين Mining

$$\begin{aligned} \text{TicS} &= \text{TicL} + \text{TicD} \\ \text{AmC} &= -100e^{(-0.00082\text{TicS})} + 100 \\ \text{AmD} &= \text{AmC} - \text{AmL} \\ \text{AmD} &= \text{SUM}(\text{APn}) \\ \text{TicD} &= \text{SUM}(\text{TDn}) \\ \text{APn} &= (\text{TDn}/\text{TicD}) * \text{Amd} \end{aligned}$$

حيث :

1 Tic = 24Hour
AmL - Last Amount
AmC - Current Amount

AmD - delta - SUM {TickL->TikC} جميع العملات للفترة
 APn - مقدار كل فترة
 ADn - delta
 TicL - Last Tick
 TDn - delta Tick Nod (كل عقدة)
 TSn - Sum All Ticks Nod
 TicD - delta - SUM {TickL->TikC} كل العلامات للفترة

مولد الصيغة شبه العشوائية والحصول على سلاسل التجزئة

1. يتم إنشاء قيمة البداية للسلسلة:

```
ep = ep=15436757;
ep=abs(sin(ep));
ep=ep*429496729;
```

2. توليد العنصر التالي للصف

النتيجة-GenP[byte]
 توليد
 gran=255;
 ep=abs(sin(ep));
 ep=ln(7)/ln(ep);
 ep=ep*10;
 ep=ep-trunc(ep);
 GenP=trunc(ep*gran);

3. الحصول على عنصر تجزئة السلسلة الوسيطة-S. s[byte]. سلسلة الرموز. التجزئة [255] عبارة عن صفيف بايت. رقم z لعنصر الصفيف [Hesh]. ط-رقم عنصر صفيف السلسلة

في حالة الطول (الأطوال (Hash)) <length (، تتم إضافة 0 [byte] إلى s إلى طول الحالة (ق)) = length (تجزئة) دورة

؛inc (z)

؛GenP (ep) + ord (s [i])) ،inc (Hash [z]

في حالة (Hash)) <length (z ،

تعيين 1 ، مما يؤدي إلى التعديل

z (متوسط) عنصر التجزئة

تُستخدم قيم المولد شبه العشوائي للحصول على قيم عشوائية تمامًا من مصفوفة الأوزان الخاصة بالإرسال الراديوي في الخلفية

تجنب الأصطدام الكامل بسلاسل الكتل

في التجزئة ، يتم استبدال وحدات البايت الأربع الأولى بقيمة عدد الرقم الحالي كتلة السلسلة الرئيسية.

هذا يعني أن 2147483647 المعاملات مضمونة لاستبعاد الاصطدامات.

لكل سلسلة من العقود الذكية ، يتم إنشاء رمز مميز واحد (لكل مالك) بقيمة اسمية N

لكل سلسلة من العقود الذكية ، يتم إنشاء رمز مميز واحد

بحد أقصى N

(لكل مالك) بقيمة اسمية 9223372036854775807).

مفصلية العقد الذكي

الطريقة الأمثل لحساب مفصلية العقد الذكي (

(tokenomics

حساب مفصلية العقد الذكي مع الأحداث المتوسطة (حاجز)

خيارات العقد الذكية :

L - الطول (بالأمتار ، الروابط ، الحلقات ، ذبذبات الموجة (عدد الفترات)
(خطوات ، الخ

$T(L)$ - الوقت المستغرق في مرور الطول بالكامل ، مع مراعاة التوقيات
في نقاط التفقيش

T_n - الوقت n الجزئي

R_n - تصنيف (موثوقية النقطة n)

G_n - هو نتيجة لمولد تغيير التصنيف العشوائي الزائف عند نقطة n

W_n - تأثير المعلومات الخارجية على كل مرحلة

G_n - عامل أمان نقطة التفقيش

S_n هي القيمة المحسوبة لمعدل التغلب على L_n .
من الضروري حساب الارتباطات مع الأحداث الأخرى للكتل السابقة واستقراء الأحداث المستقبلية
وحساب موثوقية الركبتين. ، الذي يتيح لك اختيار مسار مختلف ، على سبيل المثال ، عندما تكون نقطة
التفقيش مشغولة (مشكلة التقاطعات).

Z - الموثوقية على طول الطريق. لكتلة واحدة

$$T(L) = \sum (T_n * R_n * G_n * W_n * G_n)$$

$$T_n = T_n * R_n * G_n * W_n * G_n$$

$$S_n = L_n / T_n$$

$$S = S_n / n$$

$$Z = S / L \text{ مع } Z = 1 \text{ (الموثوقية الكاملة).}$$

يمكنك أيضا حساب رتبة ضعيفة وغيرها من المعالم لمحللون عندما يكون عدد الكتل < 17 ، نستخدم طريقة أصغر الوحدات و + يمكن اعتباره عنصر عقد ذكي من الذكاء الاصطناعي (الدراسة الذاتية التحليل الذاتي).
على سبيل المثال ، يمكن استخدامه للتحكم في إشارات المرور

التحقق من سلامة العقدة

1. وحدة للتحقق من سلامة كتل سلسلة كاملة.

الصيغة:

التحقق من الحفاظ على الحالة خلال السلسلة ، بدءًا من العنصر الثاني

$$h(B_{n-1}) = H_n \text{ مع } n [1..BlockCount-1]$$

حيث،

h - كتلة التجزئة

H_n - كتلة

B_n - كتلة N

إذا لم يتم استيفاء الحالة ، تعتبر الدائرة تالفة ويحدث حدث إعادة التشغيل للدائرة بأكملها.

2. وحدة للتحقق من سلامة كتل سلسلة من جميع المعاملات الخاصة بـ

الصيغة:

التحقق من الحفاظ على الحالة خلال السلسلة ، بدءًا من العنصر الثاني.

$$h(B_{n-1}) = H_n$$

حيث،

h - كتلة التجزئة

H_n - التجزئة في كتلة

B_n - كتلة N

إذا لم يتم استيفاء الحالة ، تعتبر الدائرة تالفة وتحدث

حدث إعادة تشغيل السلسلة

3. وحدة للتحقق من السلامة المحلية (الأصلية) ملف ثنائي قابل للتنفيذ.

A1 - التحقق من اسم (خارجي)

A2 - تاريخ إنشاء التحقق من (خارجي)

A3 - التحقق من موقع الإطلاق (محلي)

A4 - فحص حجم (خارجي)

A5 - ملف تجزئة الاختيار نفسه (خارجي)

A6 - التحقق من الربط إلى الغدة (محلي)

الصيغة:

$$h(A1, A2, A4, A5)$$

حيث،

h - تجزئة سلسلة المتغيرات

A - متغير سلسلة من نوع سترنج

النتيجة h تتطلب تأكيد تكامل الملفات الفريدة عبر شبكة من العقد الأخرى بناءً على طلب العقد الذكي

إذا لم يتم استيفاء شرط التأكيد الذي يبلغ (9) دقائق ، فسيتم اعتبار العقد تالفة ، مما يؤدي إلى إخلاء التطبيق تمامًا ورفض خدمة الشبكة.

4. عند بدء تشغيل ملف ثنائي قابل للتنفيذ ، يقوم بتحميل وتشغيل مكون إضافي يعمل بشكل منفصل عن البرنامج الرئيسي. في هذه الحالة ، ينتظر البرنامج الرئيسي تأكيد المصادقة (في انتظار مفتاح الجلسة).

للحصول على مفتاح الجلسة ، ينفذ المساعد الخطوة 3 ويرسل $h(A1, A2, A4, A5)$ إلى الشبكة.

بعد التحقق من الإقرار بالدقيقة (9) للسلسلة الديناميكية للعقد العشوائية ، تقوم الشبكة بإرسال مفتاح جلسة جديد للبرنامج الرئيسي. تتم كتابة مفتاح الجلسة أيضاً في السلسلة الديناميكية لجميع العقد. وبالتالي ، تتغير حالة العقدة من SLEEP إلى ONLINE.

- البرنامج المساعد نفسه هو ملف فريد تم إنشاؤه بواسطة الشبكة (عند الطلب) متى بدء البرنامج الرئيسي.
- عند بدء التشغيل ، يتحقق البرنامج المساعد من مزامنة وقت الشبكة و الجهاز الذي يعمل عليه.
- البرنامج المساعد يعمل لمدة 1-2 ثواني. إذا خلال هذا الوقت لم يرسل $h(A1, A2, A4, A5)$ عنئذ يتم إغلاق جميع البرامج عن طريق الخطأ.
- عند إعادة تشغيل نفس المكون الإضافي ، ستستجيب الشبكة مع حدوث خطأ ، لأن المكون الإضافي لم يعد فريداً.
- يتم تحديد تفرد المكون الإضافي من خلال تجزئة ملف المكون الإضافي المسجل في السلسلة الديناميكية لجميع العقد الرئيسية.

الحصول على سلسلة التجزئة

الحصول على سلسلة التجزئة $f(x(l))$ (التجزئة) من السلسلة L

المرحلة 1 - يتم حساب دالة sha1 القياسية (مع تعديلات صغيرة) نتيجة لذلك ، نحصل على $f(X(L))$ بأبعاد 20 بايت.

المرحلة 2 - تحويل $f(X(L))$ إلى 32 عدد بايت باستخدام التحويل بايت مع الجمع

تحويل البايت مع الجمع:

اكتب

```
Tsb32=array[1..32+1] of byte;
for i:=1 to HashLength do sb[i]:=sb[i]+sb[i+1]+i*i;
حيث  $f(X(L))=sb$ 
```

في هذه الحالة ، يتم استخدام حظر وقائي للجهاز لخطأ تجاوز سعة خلية المعالج.
على سبيل المثال:

```
var a,b:byte;
a:=255;
b:=1;
a:=a+b;
```

النتيجة: $a=0$;

مثل هذه العملية توفر الموارد بشكل كبير ، ليست هناك حاجة لإجراء عمليات فحص وحسابات إضافية.

المرحلة 3

عدد قليل من القفزات فوق الحاجز 255

```
inc(b,sb[i])
inc(sb[i],b)
```

حيث b عبارة عن خلية بايت

المرحلة 4

يتم استخدام دالة إضافة البايت للتجزئة الناتجة $f(X(L))$ مع سلسلة المصدر L .

```
inc(sb[k],ord(s[i]));
```

حيث $k(1..32), i(1..length(L))$

المرحلة 5

يجب إجراء المرحلة 3 لإزالة الإجراء العكسي في المرحلة 4.

قائمة

(Pascal)

```
function ShaM_Bin(s:string):THash;
const HashLength = 32;
    MagicByte =*****;
var i,k,L:integer;b:byte;
    sb:Tsb32;
    SHA1Digest:TSHA1Digest;
begin
    SHA1(s,SHA1Digest);
    k:=1;
    L:=20;
    for i:=1 to L do sb[i]:=SHA1Digest[i-1];
    for i:=L+1 to HashLength do sb[i]:=$0;
    for i:=HashLength-L to HashLength do inc(sb[i],SHA1Digest[i-HashLength-L]);
    *****=MagicByte;
    for i:=1 to HashLength do sb[i]:=sb[i]+sb[i+1]+i*i;
    b:=0;
    for k:=1 to 4 do begin
        for i:=1 to HashLength do inc(b,sb[i]);
        for i:=1 to HashLength do inc(sb[i],b);
    end;
    k:=1;
    L:=length(s);
    for i:=1 to L do begin
        inc(sb[k],ord(s[i]));
        inc(k);if k>HashLength then k:=1;
    end;
    for i:=1 to HashLength do ShaM_Bin[i]:=sb[i];
    //result:=SHAMDigestToHex(sb);
end;
```