# نظرة عامة عن مشروع Nervos

**1. الغرض من هذا المقال**

تتكون شبكة Nervos من عدد من البروتوكولات والابتكارات. الكبيرة من المهم أن يكون لديك وثائق سهلة وواضحة لتثقيف مجتمع الكربتو وتقديم مشروع بلغة ميسرة للفهم ). لأننا ، نشعر أن من مهم جدا أن نساعد مجتمعاتنا على فهم ما نحاول تحقيقه ، والمشاريع التي قمنا بها ، وكيف توصلنا إلى الى فكرة بناء مشروع مثل هدا .

نبدأ هذا المستند بفحص تفصيلي للمشكلات التي تواجهها Blockchain بشكل عام والحلول الحالية التي تحاول حلها. نأمل أن يوفر هذا المقال الضروري لقرائنا لفهم منطقنا الخاص حول أفضل السبل للتعامل مع هذه التحديات ، وقرارات الأساسية الخاصة بنا. نقدم بعد ذلك جولة تفصيلية عالية المستوى لجميع أجزاء شبكة Nervos ، مع التركيز على كيفية عملها معًا لفهم الرؤية الشاملة للشبكة.

**2. خلفية المشروع**

تعد قابلية التوسع والاستدامة وقابلية التشغيل البيني من بين أكبر التحديات التي تواجهها بلوك تشين مفتوحة المصدر. بينما تدعي العديد من المشاريع أن لديها حلولاً لهذه المشاكل ، من المهم أن نفهم من أين تأتي هذه المشاكل وأن نضع الحلول في سياق تحسين تقنية بلوك تشين بصفة عامة .

**2.1 قابلية التوسع**

كانت بلوك تشين البتكوين أول blockchain مفتوحة المصدر ، تم تصميمها للاستخدام كنقد إلكتروني من طرف الى طرف اول تطبيق عملي لتقنية جديدة و معقدة . ثم ظهرت بعد دلك بلوك تشين Ethereum [2] وهي ب لوك تشين جديدة أتت بخصائص ومميزات مختلفة مع المزيد من حالات الاستخدام ممكنة أيضا طرحت منصة حوسبة لامركزية للأغراض العامة. ومع ذلك ، فإن كلا النظامين يفرضان قيودًا على قدرات المعاملات الخاصة بهما - تحدد Bitcoin حجم الكتلة الخاص بها وتحد Ethereum حد الغاز الخاص بها. هذه خطوات ضرورية لضمان اللامركزية على المدى الطويل ، ولكنها أيضًا تحد من قدرات كلا النظامين.

اقترح مجتمع blockchain العديد من حلول قابلية التوسع في السنوات الأخيرة. بشكل عام ، يمكننا تقسيم هذه الحلول إلى فئتين: الاشتغال على السلسلة او التوسيع خارج السلسلة.

تهدف حلول التوسع على السلسلة عملية الإجماع وإنشاء بلوكشين ذات إنتاجية أصلية تنافس الأنظمة المركزية. لا تستخدم حلول التوسع خارج السلسلة سوى blockchain كأصل آمن ومنصة تسوية ، مع نقل جميع المعاملات تقريبًا إلى الطبقات الأخرى لتقليل الضغط على الطبقات الرئيسية مع تزايد الاستخدام العام لشبكات

**2.1.1 التحجيم على السلسلة باستخدام Blockchain واحد**

الطريقة الأكثر سهولة لزيادة إنتاجية blockchain هي زيادة المعروض من مساحة الكتلة. مع وجود مساحة كتلة إضافية ، يمكن تدفق المزيد من المعاملات عبر الشبكة ومعالجتها. كما أن زيادة المعروض من مساحة الكتلة استجابةً للطلب المتزايد على المعاملات يسمح أيضًا ببقاء رسوم المعاملات منخفضة.

تتبنى Bitcoin Cash (BCH) هذا النهج لتوسيع نطاق شبكة الدفع من نظير إلى نظير. بدأ بروتوكول Bitcoin Cash بحد أقصى 8 ميجابايت ، والذي تم زيادته لاحقًا إلى 32 ميجابايت ، والذي سيستمر في الزيادة إلى أجل غير مسمى مع زيادة الطلب على المعاملات. للإشارة ، بعد تنفيذ Bitcoin (BTC) بشكل منفصل تحديث في أغسطس 2017 ، يسمح بروتوكول Bitcoin الآن بمتوسط ​​حجم كتلة يبلغ حوالي 2 ميغابايت.

في نطاق توضيح اكثر  إذا قام 7.5 مليار شخص بإنشاء معاملتين على السلسلة يوميًا أي بلوك تشين ، فستتطلب من الشبكة إنتاج كتل بحجم 26 جيجابايت كل 10 دقائق ، مما يؤدي إلى معدل نمو blockchain يبلغ 3.75 تيرابايت في اليوم اي 1.37 بيتابايت أي فوق 1 كوادرليون و في السنة [3]. تعد متطلبات التخزين والنطاق الترددي هذه معقولة لأي خدمة سحابية اليوم.

ومع ذلك ، يؤدي تقييد تشغيل العقدة في بيئة و في ظل هده البيانات إلى هيكل شبكة واحد قابل للتطبيق ويفرض تنازلات في الأمان (سيزداد معدل تفرع blockchain مع زيادة متطلبات نقل البيانات عبر الشبكة) ، بالإضافة إلى اللامركزية (سيؤدي عدد العقدة الكامل إلى زيادة يتم تخفيضها مع زيادة تكلفة المشاركة بالإجماع).

من وجهة نظر اقتصادية ، فإن حجم الكتلة المتزايد باستمرار يخفف من ضغط الرسوم الذي يشعر به المستخدمون. أظهر تحليل شبكة Bitcoin أن الرسوم تظل ثابتة حتى تمتلئ الكتلة بنسبة 80٪ ، ثم ترتفع أضعافًا مضاعفة [4].

على الرغم من أن وضع عبء تكاليف الشبكة المتنامية على مشغليها قد يبدو قرارًا معقولاً ، إلا أنه قد يكون قصير النظر لسببين:

* يؤدي إلغاء رسوم المعاملات إلى إجبار عمال المناجم على الاعتماد بشكل أساسي على التعويض من إصدار العملة الجديدة (مكافآت الكتلة). ما لم يكن التضخم جزءًا دائمًا من البروتوكول ، سيتوقف إصدار العملة الجديدة في النهاية (عند الوصول إلى الحد الأقصى الإجمالي للعملة الرقمية ، ولن يتلقى المعدِّنون مكافآت كتلة ولا رسوم معاملات كبيرة. سيؤثر التأثير الاقتصادي لهذا الأمر بشكل كبير على نموذج أمان الشبكة.
* تصبح تكلفة تشغيل عقدة كاملة باهظة الثمن. هذا يزيل قدرة المستخدمين العاديين على التحقق بشكل مستقل من تاريخ ومعاملات blockchain ، مما يجبر الاعتماد على مزودي الخدمة مثل التبادلات ومعالجات الدفع لضمان سلامة blockchain. ينفي مطلب الثقة هذا عرض القيمة الأساسية لشبكات البلوك شين العامة غير المصرح بها كنظير إلى نظير وأنظمة موزعة غير موثوقة.

تواجه المنصات المحسّنة لتكلفة المعاملات مثل Bitcoin Cash منافسة كبيرة من سلاسل الكتل الأخرى (المرخصة وغير المصرح بها) ، فضلاً عن أنظمة الدفع التقليدية. سوف تتكبد قرارات التصميم التي تعمل على تحسين الأمان أو مقاومة الرقابة التكاليف المرتبطة وبالتالي تزيد من تكلفة استخدام النظام الأساسي. مع الأخذ في الاعتبار المشهد التنافسي ، بالإضافة إلى الأهداف المعلنة للشبكة ، فمن المحتمل أن تكون التكاليف المنخفضة هي الهدف الشامل للشبكة ، على حساب أي اعتبارات أخرى.

يتوافق هذا الهدف مع ملاحظاتنا حول استخدام شبكة المعاملات. لا يبالي مستخدمو هذه الأنظمة بالمقايضات المهمة طويلة المدى لأنهم لن يستخدموا الشبكة إلا لفترة قصيرة. بمجرد استلام سلعهم أو خدماتهم وتسوية مدفوعاتهم ، لم يعد لدى هؤلاء المستخدمين أي قلق بشأن التشغيل الفعال للشبكة. يتضح قبول هذه المقايضات في الاستخدام الواسع النطاق لتبادلات الأصول المشفرة المركزية ، فضلاً عن سلاسل الكتل الأكثر مركزية. تحظى هذه الأنظمة بشعبية في المقام الأول بسبب ملاءمتها وكفاءتها في المعاملات.

اتبعت بعض منصات العقود الذكية أساليب مماثلة لتوسيع نطاق إنتاجية blockchain ، مما يسمح فقط لمجموعة محدودة من "أجهزة الكمبيوتر الفائقة" المصادقة بالمشاركة في عملية الإجماع والتحقق من صحة blockchain بشكل مستقل.

على الرغم من أن الحلول الوسط فيما يتعلق باللامركزية وأمن الشبكة تسمح بمعاملات أرخص وقد تكون ملائمة لمجموعة من المستخدمين ، إلا أن نموذج الأمان طويل الأجل المخترق وحاجز التكلفة للتحقق بشكل مستقل من المعاملات والتركيز المحتمل لمشغلي العقدة وترسيخها يقودنا إلى نعتقد أن هذا ليس نهجًا مناسبًا لتوسيع نطاق سلاسل الكتل العامة.

**2.1.2 التدرج على السلسلة من خلال سلاسل متعددة**

يمكن تحقيق scaling على السلسلة من خلال سلاسل متعددة من خلال التجزئة ، كما هو موجود في Ethereum 2.0 ، أو سلاسل الأخرى التي تعمل بنفس نظام ، كما هو موضح في Polkadot. تقسم هذه التصميمات بشكل فعال الحالة العامة ومعاملات الشبكة إلى سلاسل متعددة ، مما يسمح لكل سلسلة بالوصول بسرعة إلى إجماع محلي ، ولاحقًا لشبكة كاملة للوصول إلى إجماع عالمي من خلال إجماع "Beacon Chain" أو "Relay Chain". هما نوعين جديدين من اثبات الحصة

تسمح هذه التصميمات للسلاسل المتعددة باستخدام نموذج أمان مشترك ، مع السماح بإنتاجية عالية ومعاملات سريعة داخل الأجزاء (Ethereum) أو شبه السلاسل (Polkadot). على الرغم من أن كل من هذه الأنظمة عبارة عن شبكة من سلاسل الكتل المترابطة ، إلا أنها تختلف فيما يتعلق بالبروتوكولات التي تعمل على كل سلسلة. في Ethereum 2.0 ، يعمل كل جزء بنفس البروتوكول ، بينما في Polkadot ، يمكن لكل سلسلة بارزة تشغيل بروتوكول مخصص ، تم إنشاؤه من خلال إطار عمل framework

في هذه البنى متعددة السلاسل ، كل dApp (أو مثيل dApp) يتواجد فقط في سلسلة واحدة. على الرغم من أن المطورين اليوم معتادون على القدرة على بناء dApps التي تتفاعل بسلاسة مع أي dApp آخر على blockchain ، فإن أنماط التصميم ستحتاج إلى التكيف مع البنى الجديدة متعددة السلاسل. إذا تم تقسيم dApp عبر أجزاء مختلفة ، فستكون هناك حاجة إلى آليات للحفاظ على مزامنة الحالة عبر مثيلات مختلفة من dApp (الموجودة على أجزاء مختلفة). بالإضافة إلى ذلك ، على الرغم من إمكانية نشر آليات الطبقة 2 للتواصل السريع عبر الأجزاء ، فإن المعاملات عبر الأجزاء تتطلب إجماعًا عالميًا وإدخال و زمن للانتقال للتأكيد.

مع هذه المعاملات غير المتزامنة ، تنشأ مشكلة "القطار والفندق" سيئة السمعة. عندما يجب أن تكون معاملتان ذريتين (على سبيل المثال حجز تذكرة قطار وغرفة فندق على جزأين مختلفين) ، فإن الحلول الجديدة مطلوبة. تقدم Ethereum عقد "yanking" ، حيث يتم حذف عقد تابع على جزء واحد ، يتم إنشاؤه على جزء ثان (يحتوي على عقد تابع آخر) ، ويتم بعد ذلك تنفيذ كلتا العمليتين على الجزء الثاني. ومع ذلك ، لن يكون العقد المنزوع متاحًا على الجزء الأصلي ، مما يؤدي إلى ظهور مشكلات قابلية الاستخدام ، ويتطلب مرة أخرى أنماط تصميم جديدة.

للتقاسم مزاياها وتحدياتها. إذا كان من الممكن أن تكون القطع مستقلة حقًا وكانت الاحتياجات المشتركة في الحد الأدنى ، فيمكن للبلوكشين توسيع نطاق إنتاجيتها خطيًا عن طريق زيادة عدد القطع. هذا هو الأنسب للتطبيقات المستقلة التي لا تتطلب حالة خارجية أو تعاونًا مع تطبيقات أخرى.

يمكن أن تكون البنية المُقسمة مشكلة بالنسبة للتطبيقات التي تم تطويرها من خلال تكوين تطبيقات "لبنة بناء" معًا (يُعرف هذا باسم "مشكلة القابلية للتركيب"). تعتبر القابلية للتركيب ذات أهمية خاصة في مجال التمويل اللامركزي (DeFi) ، حيث تميل المنتجات الأكثر تقدمًا إلى البناء فوق منتجات كتل البناء الأخرى.

في ملاحظة أكثر تقنية ، تتطلب التجزئة عادةً "1 + N" topology, ، حيث تتصل سلاسل one meta-chain، مما يؤدي إلى إدخال حد أعلى على عدد الأجزاء التي يمكن أن تدعمها السلسلة one meta-chain دون أن تواجه مشكلات في قابلية التوسع.

نلاحظ قيمة كبيرة في حالة عالمية موحدة ، مما يسمح لنظام بيئي للتطبيقات المترابطة بالظهور والمطورين للابتكار على الحواف ، على غرار استخدام مطوري الويب للمكتبات للمخاوف ذات المستوى الأدنى وواجهات برمجة التطبيقات المفتوحة لتكامل الخدمة. يتم تمكين تجربة تطوير أبسط بكثير عندما لا يضطر المطورون إلى التفكير في التزامن (في نقل الأصول عبر الأجزاء أو تمرير الرسائل) ، بالإضافة إلى تجربة مستخدم فائقة ، ناتجة عن الاتساق في الاهتمامات المعمارية لتفاعلات على blockchain.

نحن ندرك أن التجزئة هي حل قابل للتوسع واعد (لا سيما للتطبيقات الأقل ارتباطًا) ، ولكننا نعتقد أنه من المفيد أن يكون لديك تصميم يركز على الحالة الأكثر قيمة على blockchain واحد ، مما يسمح بالتركيب. مع هذا التصميم ، يتم استخدام أساليب القياس خارج السلسلة للسماح بإنتاجية أعلى.

**2.1.3 التحجيم خارج السلسلة من خلال الطبقة 2**

في بروتوكولات الطبقة 2 ، تعمل blockchain للطبقة الأساسية كطبقة تسوية (أو التزام) ، بينما تقوم شبكة الطبقة الثانية بتوجيه أدلة التشفير التي تسمح للمشاركين "بتلقي" العملة المشفرة. يتم تأمين جميع أنشطة الطبقة الثانية بشكل مشفر بواسطة blockchain الأساسي ويتم استخدام الطبقة الأساسية فقط لتسوية المبالغ التي تدخل / تخرج من شبكة الطبقة الثانية ، ولحل النزاعات. تعمل هذه التصاميم دون تفويض الوصاية (أو خطر فقدان) الأموال وتمكين المعاملات الفورية شبه المجانية.

توضح هذه التقنيات كيف يمكن استخدام مخزن لشبكة القيمة مثل Bitcoin للمدفوعات اليومية. المثال الأكثر شيوعًا لحل الطبقة 2 في الممارسة العملية هو قناة الدفع بين العميل والمقهى. لنفترض أن أليس تزور مقهى بيتكوين كل صباح. في بداية الشهر ، تودع الأموال في قناة دفع Lightning فتحتها مع المقهى. أثناء زيارتها كل يوم ، توقع بشكل مشفر حق المقهى في الحصول على بعض الأموال ، مقابل قهوتها. تحدث هذه المعاملات على الفور وهي تتم بشكل تام من نظير إلى نظير ، "خارج السلسلة" ، مما يسمح بتجربة عملاء سلسة. قناة Lightning غير موثوقة ، يمكن لـ Alice أو المقهى إغلاق القناة في أي وقت ، مع أخذ الأموال المستحقة عليهم في ذلك الوقت.

تقنيات قنوات الدفع مثل Lightning ليست سوى مثال واحد على أسلوب التوسع خارج السلسلة ؛ هناك العديد من التقنيات الناضجة التي يمكنها توسيع نطاق إنتاجية blockchain بأمان بهذه الطريقة. بينما تتضمن قنوات الدفع اتفاقيات خارج السلسلة لتوجيه الأرصدة بين طرفين ، فإن قنوات الشبكة تتضمن اتفاقيات خارج السلسلة لمعاملة بين المشاركين في القناة. يمكن أن يكون هذا التعميم أساسًا للتطبيقات القابلة للتطوير والغير موثوق بها واللامركزية. يمكن استخدام قناة حالة واحدة بواسطة تطبيقات متعددة ، مما يسمح بمزيد من الكفاءة. عندما يكون أحد الأطراف جاهزًا للخروج من القناة ، يمكنه إرسال إثبات التشفير المتفق عليه إلى blockchain ، والذي سيقوم بعد ذلك بتنفيذ انتقالات الحالة المتفق عليها.

السلسلة الجانبية هي بناء آخر يسمح بزيادة الإنتاجية ، على الرغم من ذلك عبر مشغلي blockchain من الأطراف الثالثة الموثوق بهم. من خلال ربط ثنائي الاتجاه إلى blockchain بإجماع موثوق وغير موثوق به ، يمكن نقل الأموال ذهابًا وإيابًا بين السلسلة الرئيسية والسلسلة الجانبية. يسمح هذا بكمية كبيرة من المعاملات الموثوقة على السلسلة الجانبية ، مع تسوية صافية لاحقًا على السلسلة الرئيسية. تتمتع معاملات السلسلة الجانبية برسوم قليلة وتأكيد سريع وإنتاجية عالية. على الرغم من أن السلاسل الجانبية تقدم تجربة متفوقة في بعض الجوانب ، إلا أنها تتنازل عن الأمان. ومع ذلك ، هناك قدر كبير من البحث في السلاسل الجانبية غير الموثوقة ، والتي يمكن أن توفر نفس تحسينات الأداء دون المساس بالأمان.

مثال على تقنية السلسلة الجانبية غير الموثوقة هي البلازما (التي تمت تغطيتها في 5.4) ، وهي بنية سلسلة جانبية تستفيد من جذر الثقة في blockchain مع إجماع عالمي واسع. تقدم سلاسل البلازما نفس التحسينات في الأداء مثل السلاسل الجانبية المركزية ، ولكنها تفعل ذلك مع تقديم ضمانات أمنية. في حالة ما إذا كان مشغل سلسلة البلازما ضارًا أو معطلاً ، يتم تزويد المستخدمين بآلية تسمح لهم بسحب أصول السلسلة الجانبية بأمان إلى السلسلة الرئيسية. يتم ذلك بدون تعاون مشغل سلسلة البلازما ، مما يوفر للمستخدمين الراحة في معاملات السلسلة الجانبية ، فضلاً عن أمان طبقة البلوكشين من الطبقة الأولى.

يسمح التحجيم خارج السلسلة باللامركزية والأمان وقابلية التوسع. من خلال نقل كل شيء باستثناء معاملات التسوية والنزاعات خارج السلسلة ، يتم استخدام الإجماع العالمي المحدود للبلوك تشين بكفاءة. يمكن تنفيذ بروتوكولات الطبقة 2 المتنوعة بناءً على متطلبات التطبيق ، مما يوفر المرونة للمطورين والمستخدمين. مع إضافة المزيد من المشاركين إلى الشبكة ، لا يتأثر الأداء ويمكن لجميع الأطراف مشاركة مع الضمانات الأمنية التي يوفرها توافق مع الطبقة الأولى.

**2.2 الاستدامة**

يمثل الحفاظ على التشغيل طويل الأجل لـ blockchain العامة المستقلة وغير المالكة تحديًا كبيرًا. يجب أن تكون الحوافز متوازنة بين أصحاب المصلحة المتنوعين ويجب تصميم النظام بطريقة تسمح بتشغيل الشبكة الكاملة على نطاق واسع وإمكانية التحقق العام. يجب أن تظل متطلبات الأجهزة معقولة ، مع دعم شبكة عالمية مفتوحة.

بالإضافة إلى ذلك ، بمجرد تشغيل blockchain العامة ، من الصعب جدًا تغيير القواعد الأساسية التي تحكم البروتوكول. منذ البداية ، يجب تصميم النظام ليكون مستدامًا. في هذا الصدد ، أجرينا جردًا شاملاً للتحديات في بناء بلوكشين مستدامة ومفتوحة المصدر .

**2.2.1 اللامركزية**

واحدة من أكبر التهديدات طويلة الأجل التي تواجهها شبكات بلوك تشين العامة هي العائق المتزايد باستمرار المشاركة المستقلة والتحقق من المعاملات ، وهو ما ينعكس في تكلفة تشغيل الشبكة الكاملة. تسمح الشبكة الكاملة للمشاركين في blockchain بالتحقق بشكل مستقل من الحالة / السجل على السلسلة ، وإخضاع المعدنين أو المدققين للشبكة للمساءلة عن طريق رفض توجيه الكتل غير الصالحة. مع زيادة تكلفة العقد الكاملة وتراجع أعدادها ، يضطر المشاركون في الشبكة بشكل متزايد إلى الاعتماد على مشغلي الخدمات المحترفين لتوفير كل من التاريخ والحالة الحالية ، مما يؤدي إلى تآكل نموذج الثقة الأساسي لشبكات البلوكشين المفتوحة وغير المرخصة.

لكي تتمكن العقدة الكاملة من مواكبة تطور blockchain ، يجب أن يكون لديها إنتاجية حسابية كافية للتحقق من صحة المعاملات ، وإنتاجية النطاق الترددي لتلقي المعاملات ، وسعة التخزين لتخزين الحالة العالمية بأكملها. للتحكم في تكلفة تشغيل العقدة الكاملة ، يتعين على البروتوكول اتخاذ تدابير لربط الإنتاجية أو نمو السعة لجميع هذه الموارد الثلاثة. ربطت معظم بروتوكولات blockchain معدل نقل البيانات الحسابي أو النطاق الترددي الخاص بها ، لكن القليل منها ربط نمو الحالة العالمية. مع نمو هذه السلاسل في الحجم وطول العملية ، ستزداد تكاليف تشغيل العقدة الكاملة بشكل لا رجعة فيه.

**2.2.2 النماذج الاقتصادية**

بينما كان هناك الكثير من الأبحاث حول بروتوكولات الإجماع في السنوات الأخيرة ، تركز النماذج الاقتصادية الحالية لبروتوكولات الطبقة الأولى بشكل أساسي على الحوافز والعقوبات لضمان توافق الشبكة ، وتستخدم الرموز الأصلية في الغالب لدفع رسوم المعاملات أو لتلبية متطلبات Staking التي توفر مقاومة ضد هجوم Sybil.

نعتقد أن النموذج الاقتصادي المصمم جيدًا يجب أن يتجاوز عملية الإجماع ويضمن أيضًا استدامة البروتوكول على المدى الطويل. على وجه الخصوص ، يجب تصميم النموذج الاقتصادي بالأهداف التالية:

* يجب أن يكون للشبكة طريقة مستدامة لتعويض مقدمي خدمات الاثبات (عادةً عمال المناجم أو المدققون) ، مما يضمن بقاء الشبكة آمنة بشكل مستدام
* يجب أن يكون للشبكة طريقة مستدامة للحفاظ على عوائق منخفضة للمشاركة ، وضمان بقاء الشبكة لامركزية بمرور الوقت
* يجب تخصيص موارد الشبكة العامة بشكل فعال وعادل
* يجب أن يكون لرمز البلوك تشين الأصلي قيمة جوهرية

**2.2.3 تحليل نموذج البيتكوين الاقتصادي**

يحدد بروتوكول Bitcoin حجم الكتل ويفرض وقت كتلة ثابت. هذا يجعل معدل نقل النطاق الترددي للشبكة موردًا نادرًا يجب على المستخدمين تقديم عطاءات عليه من خلال رسوم المعاملات. لا يسمح Bitcoin Script بالحلقات ، مما يجعل طول البرنامج النصي تقريبًا جيدًا لتعقيده الحسابي. بشكل عام ، يُترجم الطلب المتزايد على مساحة الكتلة إلى رسوم معاملات أعلى للمستخدمين. بالإضافة إلى ذلك ، كلما زاد عدد المدخلات أو المخرجات أو الخطوات الحسابية المتضمنة في المعاملة ، زاد المبلغ الذي سيدفعه المستخدم أيضًا في رسوم المعاملة.

تأتي القيمة الجوهرية للبيتكوين بالكامل تقريبًا من العلاوة النقدية (رغبة المجتمع في التعامل معها على أنها نقود) وعلى وجه الخصوص ، الرغبة في الاحتفاظ بها كمخزن للقيمة. نظرًا لأن دخل المُعدِّن مقوم بـ BTC ، يجب أن يظل هذا التصور ثابتًا حتى يكون نموذج Bitcoin الاقتصادي مستدامًا. بمعنى آخر ، نموذج أمان Bitcoin دائري - يعتمد على الاعتقاد الجماعي بأن الشبكة آمنة بشكل مستدام وبالتالي يمكن استخدامها كمخزن نقدي للقيمة.

يحدد الحد الأقصى لحجم كتلة Bitcoin بشكل فعال حاجز المشاركة في الشبكة - فكلما انخفض الحد الأقصى لحجم الكتلة ، كان من الأسهل على غير المحترفين تشغيل العقد الكاملة. حالة Bitcoin العالمية هي مجموعة UTXO الخاصة بها ، مع معدل نموها أيضًا محددًا بشكل فعال بحد حجم الكتلة. يتم تحفيز المستخدمين على إنشاء واستخدام UTXOs بكفاءة ؛ إنشاء المزيد من UTXO يترجم إلى رسوم معاملات أعلى. ومع ذلك ، لا توجد حوافز لتشجيع الجمع بين UTXOs وتقليل حجم الحالة العالمية ؛ بمجرد إنشاء UTXO ، سيحتل الحالة العالمية مجانًا حتى يتم إنفاقه.

يعد النموذج الاقتصادي القائم على رسوم المعاملات في Bitcoin نموذجًا عادلًا لتخصيص معدل نقل البيانات ، وهو المورد النادر الذي يفرضه البروتوكول. إنه نموذج اقتصادي مناسب لنظام الدفع من نظير إلى نظير ، ولكنه خيار ضعيف لمتجر حقيقي لمنصة القيمة. مستخدمو Bitcoin الذين يستخدمون blockchain لتخزين القيمة يدفعون رسوم المعاملات مرة واحدة فقط ، ولكن يمكنهم بعد ذلك احتلال الحالة إلى الأبد ، ويتمتعون بالأمان المستمر الذي يوفره عمال المناجم ، المطلوب منهم القيام باستثمارات مستمرة في الموارد.

تتمتع Bitcoin بإجمالي العرض الثابت وإصدارها الجديد عبر مكافآت الكتلة سينخفض ​​في النهاية إلى الصفر. قد يتسبب هذا في مشكلتين:

أولاً ، إذا استمرت Bitcoin في النجاح كمخزن للقيمة ، فستستمر قيمة الوحدة لـ BTC في الزيادة ، كما ستزداد القيمة الإجمالية التي تؤمنها الشبكة (مع انتقال المزيد من القيمة النقدية إلى الشبكة). يجب أن تكون منصة تخزين القيمة قادرة على زيادة ميزانيتها الأمنية مع زيادة القيمة التي تحميها بمرور الوقت ، وإلا فإنها تدعو المهاجمين إلى مضاعفة الإنفاق وسرقة أصول الشبكة.

عندما تكون تكلفة كسر أمان البروتوكول أقل من الربح الذي يمكن أن يكسبوه بالتصرف بأمانة ، فإن المهاجمين سيهاجمون دائمًا. هذا مشابه لمدينة يتعين عليها زيادة إنفاقها العسكري مع زيادة الثروة داخل المدينة. بدون هذا الاستثمار ، سيتم مهاجمة المدينة ونهبها عاجلاً أم آجلاً.

مع وجود مكافآت الكتلة ، فإن Bitcoin قادرة على توسيع نطاق الأمان إلى القيمة الإجمالية التي تخزنها - إذا تضاعف سعر Bitcoin ، فإن الدخل الذي يحصل عليه المعدنون من مكافآت الكتلة سيتضاعف أيضًا ، وبالتالي يمكنهم تحمل إنتاج ضعف معدل التجزئة ، مما يجعل الشبكة ضعف تكلفة الهجوم.

ومع ذلك ، يتغير هذا عندما تنخفض مكافآت الكتلة المتوقعة إلى الصفر. سيتعين على عمال المناجم الاعتماد كليًا على رسوم المعاملات ؛ لن يتناسب دخلهم مع قيمة أصل Bitcoin بعد الآن ، ولكن سيتم تحديده من خلال طلب المعاملات على الشبكة. إذا لم يكن الطلب على المعاملات مرتفعًا بما يكفي لملء مساحة الكتلة المتاحة ، فسيكون إجمالي رسوم المعاملات ضئيلًا. نظرًا لأن رسوم المعاملات هي وظيفة طلب مساحة الكتلة بشكل صارم ومستقلة عن سعر Bitcoin ، فسيكون لذلك تأثير عميق على نموذج أمان Bitcoin. لكي تظل Bitcoin آمنة ، يجب أن نفترض طلب معاملات متسق وفائض السعة ، والذي يتناسب أيضًا مع سعر Bitcoin. هذه افتراضات قوية جدا.

ثانيًا ، عندما تتوقف مكافآت الكتلة التي يمكن التنبؤ بها ، يزداد التباين في الدخل لكل كتلة لعمال المناجم ، ويوفر حوافز للمعدنين للتشعب ، بدلاً من تطوير blockchain. في الحالة القصوى ، عندما تكون مجموعة أعضاء المنجم فارغة ويتلقون كتلة محملة بالرسوم ، فإن حافزهم هو تفكيك السلسلة وسرقة الرسوم ، بدلاً من تطوير السلسلة وإنتاج كتلة بدون دخل محتمل [5]. يُعرف هذا باسم تحدي "قنص الرسوم" في مجتمع Bitcoin ، والذي لم يتم العثور على حل مُرضٍ له بعد ، دون إزالة سقف البيتكوين الثابت.

**2.2.4 تحليل النموذج الاقتصادي لمنصات العقود الذكية +**

يواجه النموذج الاقتصادي النموذجي لمنصات العقود الذكية المزيد من التحديات. دعنا نستخدم Ethereum كمثال. تسمح البرمجة النصية لـ Ethereum بالحلقات ، وبالتالي فإن طول النص لا يعكس التعقيد الحسابي للبرنامج النصي. هذا هو السبب في أن Ethereum لا تحدد حجم الكتلة أو إنتاجية النطاق الترددي ، ولكن الإنتاجية الحسابية (المعبر عنها في حد كتلة الغاز).

لتسجيل معاملاتهم على Ethereum blockchain ، يقوم المستخدمون بالمزايدة على تكلفة الحساب التي يرغبون في دفعها في رسوم المعاملات. يستخدم Ethereum مفهوم "الغاز" كقياس للتكلفة الحسابية المسعرة في ETH ، ويضمن التحكم في معدل "سعر الغاز" أن تكلفة كل خطوة من الحساب مستقلة عن تحركات أسعار الرمز الأصلي. تأتي القيمة الجوهرية لرمز ETH من موقعه كرمز دفع لمنصة الحساب اللامركزية ؛ إنها العملة الوحيدة التي يمكن استخدامها للدفع مقابل الحساب على Ethereum.

يتم تمثيل الحالة العالمية لـ Ethereum مع ثلاثي الحالة الخاص بـ EVM ، وهي بنية البيانات التي تحتوي على الأرصدة والحالة الداخلية لجميع الحسابات. عندما يتم إنشاء حسابات جديدة أو قيم تعاقدية ، يتوسع حجم الحالة العامة. تتقاضى Ethereum كميات ثابتة من الغاز لإدخال قيم جديدة في مخزن الشبكة الخاص بها وتقدم "راتب غاز" ثابتًا يعوض تكاليف الغاز في المعاملة عند إزالة القيم.

لا يتطابق نموذج التخزين "الدفع مرة واحدة ، وشغل إلى الأبد" مع هيكل التكلفة المستمر لعمال المناجم والعقود الكاملة ، ولا يوفر النموذج أي حافز للمستخدمين لإزالة الحالة طواعية أو إزالة الحالة عاجلاً. نتيجة لذلك ، شهدت Ethereum نموًا سريعًا في حجم الشبكة. يؤدي حجم الحالة الأكبر إلى إبطاء معالجة المعاملات ورفع تكلفة تشغيل العقود الكاملة. بدون حوافز قوية لإيضاح المعاملات ، هذا اتجاه لا بد أن يستمر.

على غرار Bitcoin ، يعد تسعير الغاز المدفوع بالطلب في Ethereum نموذجًا عادلًا لتخصيص إنتاجيتها الحسابية ، وهي المورد النادر للمنصة. يخدم النموذج أيضًا غرض Ethereum كنظام حساب لامركزي. ومع ذلك ، فإن نموذج رسوم التخزين الشبكة لا يتطابق مع اقتراحها المحتمل كشبكة لامركزية أو منصة تخزين الأصول. بدون تكلفة لتخزين الحالة طويل الأجل ، سيكون من مصلحة المستخدمين دائمًا احتلال جزء من مساحة الشبكة إلى الأبد مجانًا. بدون ندرة سعة تخزين الشبكة، لا يمكن إنشاء سوق ولا ديناميكيات العرض والطلب.

على عكس Bitcoin ، التي تحدد حد حجم الكتلة في بروتوكولها الأساسي ، تسمح Ethereum للمعدنين بضبط حد كتلة الغاز ديناميكيًا عند إنتاجهم للكتل. عمال المناجم الذين لديهم أجهزة متطورة ونطاق ترددي كبير قادرون على إنتاج المزيد من الكتل ، والسيطرة بشكل فعال على عملية التصويت هذه. ينصب اهتمامهم على تعديل حد غاز الكتلة لأعلى ، ورفع مستوى المشاركة وإجبار عمال المناجم الأصغر على الخروج من المنافسة. هذا عامل آخر يساهم في ارتفاع تكلفة تشغيل العقدة الكاملة بسرعة.

منصات العقود الذكية مثل Ethereum هي منصات متعددة الأصول. أنها تدعم إصدار ومعاملات جميع أنواع الأصول المشفرة ، وعادة ما يتم تمثيلها على أنها "توكنز". كما أنها توفر الأمان ليس فقط لرموزها الأصلية ، ولكن لقيمة جميع أصول التشفير على النظام الأساسي. يشير مصطلح "مخزن القيمة" في سياق متعدد الأصول إلى خاصية الحفاظ على القيمة التي تفيد كل من الرموز المميزة الأصلية للمنصة وأصول التشفير المخزنة على النظام الأساسي.

بفضل مكافآتها الضخمة ، تمتلك Bitcoin نموذجًا اقتصاديًا ممتازًا لـ "مخزن القيمة". يحصل عمال المناجم على مكافأة ثابتة مقومة بعملة البيتكوين ، وبالتالي يرتفع دخلهم جنبًا إلى جنب مع سعر البيتكوين. لذلك ، فإن النظام الأساسي لديه القدرة على زيادة الإيرادات لعمال المناجم لزيادة الأمن مع الحفاظ على نموذج اقتصادي مستدام.

بالنسبة للمنصات متعددة الأصول ، يصبح الوفاء بهذا المطلب أكثر صعوبة ، لأنه يمكن التعبير عن "القيمة" بأصول مشفرة تتجاوز الرمز المميز الأصلي. إذا زادت قيمة الأصول المشفرة التي يتم تأمينها بواسطة النظام الأساسي ، لكن أمان الشبكة لم يزداد ، يصبح من المربح مهاجمة عملية الإجماع الخاصة بالمنصة لمضاعفة إنفاق الأصول المشفرة المخزنة على النظام الأساسي.

لكي تعمل منصة العقود الذكية متعددة الأصول كمخزن للقيمة ، يجب وضع الحوافز المناسبة لمواءمة النمو في قيمة أصول الشبكة مع أمانها الأساسي. أو بعبارة أخرى ، يجب أن يكون الرمز المميز للنظام الأساسي بمثابة التقاط جيد لقيمة الأصول الإجمالية للمنصة. إذا كانت القيمة الجوهرية للرمز الأصلي للمنصة مقصورة على دفع رسوم المعاملة ، فسيتم تحديد قيمتها فقط من خلال طلب المعاملة ، بدلاً من طلب تخزين الأصول.

يجب أن تعتمد منصات العقود الذكية التي لم يتم تصميمها لتعمل كمخزن ذي قيمة على العلاوة النقدية للرمز الأصلي (رغبة الأشخاص في الاحتفاظ بالرموز بما يتجاوز قيمتها الجوهرية) لدعم أمانها المستمر. يكون هذا ممكنًا فقط إذا كانت إحدى الأنظمة الأساسية تهيمن على ميزات فريدة لا يمكن العثور عليها في مكان آخر ، أو تتنافس مع الآخرين من خلال تقديم أقل تكلفة ممكنة للمعاملات.

تتمتع Ethereum حاليًا بمثل هذه الهيمنة ويمكنها بالتالي الحفاظ على علاقتها النقدية. ومع ذلك ، مع صعود المنصات المنافسة ، تم تصميم العديد منها لـ TPS الأعلى وتوفير وظائف مماثلة ، فإنه سؤال مفتوح حول ما إذا كان الاعتماد على قسط نقدي وحده يمكن أن يحافظ على أمان منصة blockchain ، خاصةً إذا لم يتم تصميم الرموز الأصلية صراحةً أو تصديقها ليكون المال. علاوة على ذلك ، حتى إذا كان بإمكان النظام الأساسي توفير ميزات فريدة ، يمكن استخراج قسطها النقدي بعيدًا عن طريق واجهة المستخدم من خلال مقايضات فعالة (من المحتمل جدًا عندما يأتي الاعتماد الجماعي لـ blockchain أخيرًا). سيحتفظ المستخدمون بأصول مألوفة لديهم ، مثل Bitcoin أو العملات الرقمية المستقرة ، ويحصلون على رموز النظام الأساسي في الوقت المناسب لدفع رسوم المعاملات. في كلتا الحالتين ، فإن أساس النظام الأساسي

يجب أن توفر الأنظمة الأساسية متعددة الأصول من المستوى الأول أمانًا مستدامًا لجميع أصول التشفير التي تقوم بتأمينها. بعبارة أخرى ، يجب أن يكون لديهم نموذج اقتصادي مصمم لمتجر ذي قيمة.

**2.2.5 تمويل تطوير البروتوكول الأساسي**

شبكات بلوك تشين مفتوحة المصدر هي بنية تحتية عامة. يتطلب التطوير الأولي لهذه الأنظمة قدرًا كبيرًا من التمويل ، وبمجرد تشغيلها يتطلب صيانة وترقيات مستمرة. بدون وجود أشخاص مخصصين لصيانة هذه الأنظمة ، فإنهم يتعرضون لخطر الأخطاء الكارثية والتشغيل دون المستوى الأمثل. لا توفر بروتوكولات Bitcoin و Ethereum آلية معينة لضمان تمويل التطوير المستمر ، وبالتالي تعتمد على المشاركة المستمرة للشركات ذات الاهتمامات المتوافقة مفتوحة المصدر.

كانت عملة داش أول مشروع يستخدم صندوق الخزانة لضمان تمويل التطوير المستمر في البروتوكول. مع دعم تطوير البروتوكول بشكل مستدام ، يقدم هذا التصميم حلاً وسطًا فيما يتعلق باستدامة قيمة العملة المشفرة. مثل معظم سندات الخزانة blockchain ، يعتمد هذا النموذج على التمويل القائم على التضخم ، مما يؤدي إلى تآكل قيمة الحيازات طويلة الأجل.

تستخدم شبكة نيرفوس نموذج خزينة يوفر تمويلًا مستدامًا للتنمية الأساسية. تأتي أموال الخزانة من التضخم المستهدف لحاملي الرموز قصيرة الأجل ، في حين يتم تخفيف آثار هذا التضخم لأصحاب العقود طويلة الأجل. مزيد من المعلومات حول هذه الآلية موصوفة في فقرة (4.6).

**2.3 قابلية التشغيل البيني**

تعد قابلية التشغيل البيني عبر blockchain موضوعًا تتم مناقشته كثيرًا ، وقد تم اقتراح العديد من المشاريع على وجه التحديد لمواجهة هذا التحدي. من خلال المعاملات الموثوقة عبر البلوكشين ، يمكن تحقيق تأثيرات الشبكة الحقيقية في الاقتصاد اللامركزي.

كان أول مثال على قابلية التشغيل البيني blockchain هو التبادل بين Bitcoin و Litecoin. أصبح التبادل غير الموثوق به لـ Bitcoin مقابل Litecoin والعكس ممكنًا ليس من خلال آليات البروتوكول ، ولكن من خلال معيار تشفير مشترك (على وجه التحديد استخدام وظيفة التجزئة SHA2-256).

وبالمثل ، يسمح تصميم Ethereum 2.0 بالتوصيل البيني للعديد من سلاسل القطع ، وجميعها تعمل بنفس البروتوكول وتستخدم نفس أساسيات التشفير. سيكون هذا التوحيد ذا قيمة عند تخصيص البروتوكول للاتصال بين الأجزاء ، ولكن لن يكون Ethereum 2.0 قابلاً للتشغيل المتبادل مع سلاسل الكتل الأخرى التي لا تستخدم نفس أساسيات التشفير.

تذهب شبكات البلوكشين مثل Polkadot أو Cosmos إلى أبعد من ذلك ، مما يسمح للكتل التي تم إنشاؤها بنفس الإطار (Cosmos SDK لـ Cosmos و Substrate لـ Polkadot) بالتواصل والتفاعل مع بعضها البعض. توفر هذه الأطر للمطورين بعض المرونة في بناء البروتوكولات الخاصة بهم ، وتضمن توفر بدائل تشفير متطابقة ، مما يسمح لكل سلسلة بتحليل كتل بعضها البعض والتحقق من صحة المعاملات. ومع ذلك ، يعتمد كلا البروتوكولين على الجسور أو "مناطق الربط" للاتصال بشبكات البلوكشين التي لم يتم إنشاؤها باستخدام أطر عمل خاصة بها ، مما يوفر طبقة إضافية من الثقة. للتوضيح: على الرغم من قيام Cosmos و Polkadot بتمكين "شبكات blockchains" ، لم يتم تصميم شبكات Cosmos و Polkadot لتكون قابلة للتشغيل المتبادل مع بعضها البعض.

قد تحتاج اقتصاديات التشفير للشبكات عبر السلاسل إلى مزيد من الدراسة أيضًا. بالنسبة إلى كل من Cosmos و Polkadot ، يتم استخدام الرموز المميزة الأصلية للتخزين ورسوم الحوكمة والمعاملات. إذا وضعنا جانباً ديناميكيات العملات المشفرة التي قدمها Staking ، والتي لا يمكن أن تعطي وحدها قيمة جوهرية للرمز الأصلي (تمت مناقشته في 4.2.4) ، فإن الاعتماد على المعاملات عبر السلاسل لالتقاط قيمة النظام البيئي يمكن أن يكون نموذجًا ضعيفًا. على وجه الخصوص ، تعد المعاملات عبر السلاسل نقطة ضعف ، وليست قوة في الشبكات متعددة السلاسل ، تمامًا كما أن المعاملات عبر الأجزاء هي نقطة ضعف في قواعد البيانات المُقسمة.  . هناك ميل طبيعي للتطبيقات التي تحتاج إلى التفاعل مع بعضها البعض للانتقال في النهاية إلى نفس blockchain لتقليل النفقات العامة عبر السلسلة ،

تستفيد الشبكات عبر السلاسل من تأثيرات الشبكة - فكلما زادت السلاسل المترابطة في الشبكة ، زادت قيمة الشبكة ، وزادت جاذبيتها للمشاركين الجدد المحتملين في الشبكة. من الناحية المثالية ، سيتم التقاط هذه القيمة من خلال الرمز المميز الأصلي واستخدامها لزيادة تشجيع نمو الشبكة. ومع ذلك ، في شبكة الأمان المجمعة مثل Polkadot ، تصبح التكلفة الأعلى للمشاركة في الشبكة رادعًا للشبكة لتحقيق المزيد من القيمة. في شبكة غير متصلة بشكل محكم مثل Cosmos ، إذا افترضنا نفس الطلب على المعاملات عبر السلسلة ورسومها ، فإن التكلفة العالية للمشاركة في الـ Staking تقلل العائد المتوقع للمصادقين ، مما يثبط المزيد من المشاركة في الـ Staking.

من خلال نهجها متعدد الطبقات ، تعد شبكة Nervos أيضًا شبكة متعددة السلاسل. من الناحية بناء والتصميم ، يستخدم Nervos نموذج الخلية وجهازًا افتراضيًا منخفض المستوى لدعم التخصيص الحقيقي وأساسيات التشفير التي أنشأها المستخدم ، مما يتيح إمكانية التشغيل البيني عبر سلاسل الكتل غير المتجانسة (تمت تغطيتها في 4.4.1). من الناحية الاقتصادية المشفرة ، تركز شبكة Nervos على القيمة على سلسلة ترفع هذه الآلية ميزانية أمان الشبكة مع ارتفاع القيمة الإجمالية التي تؤمنها الشبكة. تم تناول هذا بالتفصيل في (4.4).

**3. المبادئ الأساسية لشبكة نيرفوس**

شبكة Nervos عبارة عن شبكة متعددة الطبقات تم إنشاؤها لدعم احتياجات الاقتصاد اللامركزي. هناك العديد من الأسباب التي تجعلنا نعتقد أن النهج متعدد الطبقات هو الطريقة الصحيحة لبناء شبكة blockchain. هناك العديد من الاساسيات المعروفة في بناء أنظمة blockchain ، مثل اللامركزية مقابل قابلية التوسع ، والحيادية مقابل التوافق ، والخصوصية مقابل الانفتاح ، وتخزين القيمة مقابل تكلفة المعاملة ، وسلامة الشبكة مقابل تجربة المستخدم. نعتقد أن كل هذه النزاعات تنشأ بسبب محاولات معالجة المخاوف المتعارضة تمامًا باستخدام blockchain واحد.

نعتقد أن أفضل طريقة لبناء نظام لا تتمثل في بناء طبقة واحدة شاملة ، ولكن بدلاً من ذلك لفصل الاهتمامات ومعالجتها في طبقات مختلفة. من خلال القيام بذلك ، يمكن أن تركز blockchain من الطبقة الأولى على كونها بنية تحتية عامة آمنة ومحايدة ولا مركزية ومفتوحة ، بينما يمكن تصميم شبكات الطبقة الثانية الأصغر خصيصًا لتناسب سياق استخدامها بشكل أفضل.

في شبكة Nervos ، بروتوكول الطبقة 1 (قاعدة الشبكة واساس قوتها ) هي طبقة مخصصة للحفاظ على القيمة للشبكة بأكملها. إنه نموذج مستوحى من Bitcoin من الناحية الفلسفية وهو عبارة عن blockchain مفتوح وعام ويقوم على خاصية إثبات العمل ، تم تصميمه ليكون آمنًا إلى أقصى حد ومقاوم للرقابة ، ليكون بمثابة حارس لامركزي للقيمة والأصول المشفرة. تستفيد بروتوكولات الطبقة الثانية من أمان blockchain من الطبقة الأولى لتوفير قابلية التوسع غير المحدودة والحد الأدنى من رسوم المعاملات ، وتسمح أيضًا بالمقايضات الخاصة بالتطبيقات فيما يتعلق بنماذج الثقة والخصوصية.

فيما يلي المبادئ الأساسية التي أدت إلى تصميم شبكة نيرفوس:

* يجب أن تكون blockchain مستدامة ومتعددة الأصول والطبقات مصممة اقتصاديًا لتكون مخزنًا للقيمة.
* تقدم Layer 2 أفضل خيارات القياس ، مما يوفر إمكانيات معاملات غير محدودة تقريبًا ، وتكاليف أقل للمعاملات وتجربة مستخدم محسنة. يجب تصميم سلاسل الكتل من الطبقة الأولى لتكمل حلول الطبقة الثانية ، لا أن تتنافس معها.
* يعد إثبات العمل طريقة مقاومة لهجمات Sybil أمرًا ضروريًا لكتل ​​الطبقة 1.
* يجب أن توفر blockchain للطبقة 1 نموذج برمجة عام للبروتوكولات التفاعلية وقابلية التشغيل البيني blockchain ، والسماح للبروتوكول بأن يكون قابلاً للتخصيص إلى أقصى حد وسهل الترقية.
* لتخصيص الموارد بشكل أفضل وتجنب "مأساة الانهيار " ، يجب أن يكون للتخزين نموذج ملكية واضح ودقيق. لتقديم مكافآت متسقة طويلة الأجل لعمال المناجم (بغض النظر عن طلب المعاملة) ، مع تكلفة مستمرة.

**4. قاعدة المعارف المشتركة نيرفوس**

**4.1 نظرة عامة**

يتم تعريف "المعرفة العامة" على أنها المعرفة التي يعرفها الجميع أو الجميع تقريبًا ، عادةً بالإشارة إلى المجتمع الذي يُستخدم فيه المصطلح. في سياق blockchain بشكل عام ، وشبكة Nervos بشكل خاص ، تشير "المعرفة العامة" إلى حالة تم التحقق منها من خلال الإجماع العالمي والمقبولة من قبل الجميع في الشبكة.

تسمح لنا خصائص المعرفة العامة بالتعامل الجماعي مع العملة المشفرة المخزنة في سلاسل الكتل العامة كأموال. على سبيل المثال ، تعتبر أرصدة وتاريخ جميع العناوين على Bitcoin معرفة شائعة لمستخدمي Bitcoin ، لأنهم قادرون على نسخ سجلات ومعاملات بشكل مستقل ، والتحقق من الحالة شبكة ومعرفة حتى اول تأكيد لأول شبكة ، ومعرفة أن أي شخص آخر يمكنه فعل الشيء نفسه. تتيح هذه المعرفة العامة للأشخاص إجراء معاملات نظير إلى نظير تمامًا دون الثقة في أي طرف ثالث.

تم تصميم قاعدة المعرفة العامة نيرفوس (CKB) لتخزين جميع أنواع المعرفة العامة ، وليس يقتصر على المال. على سبيل المثال ، يمكن لـ CKB تخزين أصول التي يحددها المستخدم ، مثل الرموز المميزة القابلة للاستبدال وغير القابلة للاستبدال ، بالإضافة إلى سجلات المعاملات القيمة التي توفر الأمان لبروتوكولات الطبقة العليا ، مثل قنوات الدفع (5.2) وسلاسل الالتزام (5.4) ).

تعد كل من Bitcoin و Nervos CKB أنظمة تخزين وتحقق شائعة. تخزن Bitcoin حالتها العالمية كمجموعة UTXO ، وتتحقق من انتقالات الحالة من خلال قواعد مشفرة ونصوص مضمنة في المعاملات. يقوم Nervos CKB بتعميم بنية بيانات Bitcoin وقدرات البرمجة النصية ، ويخزن الحالة العالمية كمجموعة من الخلايا النشطة القابلة للبرمجة ، ويتحقق من انتقالات الحالة من خلال البرامج النصية التي يحددها المستخدم وتورايخ كاملة والتي يتم تشغيلها في جهاز افتراضي.

بينما يتمتع Nervos CKB بقدرات تعاقدية ذكية كاملة مثل تلك الخاصة بـ Ethereum وغيرها من الأنظمة الأساسية ، فإن نموذجها الاقتصادي مصمم للحفاظ على المعرفة العامة ، بدلاً من الدفع مقابل الحساب اللامركزي.

**4.2 الإجماع**

يحظى توافق ناكاموتو (NC) الخاص بالبتكوين بقبول جيد نظرًا لبساطته وانخفاض تكاليف الاتصال به. ومع ذلك ، يعاني NC من عيبين:

1) إنتاج و معالجة المعاملات بعيدة عن أن تكون مرضية لانها بطيئة جدا ، و

2) أنها عرضة لهجمات التعدين الأناني ، حيث يمكن للمهاجمين الحصول على مكافآت كتلة إضافية عن طريق الانحراف عن السلوك المحدد للبروتوكول.

بروتوكول إجماع CKB هو أحد أشكال NC مع رفع من حد أدائها ومقاومة التعدين الأنانية مع الحفاظ على مزاياها. من خلال تحديد وازالة عوائق امام انتقال كتلة NC ، يدعم بروتوكولنا فترات كتلة قصيرة جدًا دون التضحية بالأمان. لا يؤدي الفاصل الزمني للكتلة المختصرة إلى زيادة الإنتاجية فحسب ، بل يقلل أيضًا من زمن انتقال تأكيد المعاملة. من خلال دمج جميع الكتل الصالحة في حساب واحد بدون صعوبات ، لم يعد للتعدين الأناني مربحًا في بروتوكولنا.

**4.2.1 زيادة الإنتاجية**

يزيد Nervos CKB من إنتاجية الكثل عن طريق خاصية إجماع إثبات العمل بخوارزمية إجماع مشتقة من إجماع ناكاموتو. تستخدم الخوارزمية معدل الكثل اليتيمة في مصطلح blockchain ، الكتل اليتيمة عبارة عن كتل يتم تعدينها في وقت واحد ككتلة أخرى ولكن لا تقبلها blockchain. في معظم الأحيان ، يرجع ذلك إلى عدم وجود كتل كافية تم إنشاؤها من تلك الكتلة حتى تتعرف الشبكة عليها على أنها أطول مفترق طرق. يتجاهل blockchain Bitcoin الكتل اليتيمة ؛ ومع ذلك ، قد تستخدمها سلاسل الكتل الأخرى لأغراض مختلفة. في blockchain (النسبة المئوية للكتل الصالحة التي ليست جزءًا من السلسلة الأساسية) كقياس للاتصال عبر الشبكة.

يستهدف البروتوكول معدلًا ثابتًا للكثل اليتيمة استجابةً لمعدلة مهمة ك ، كلما تم تقليل من الكتل اليتيمة يؤدي (زيادة معدل إنتاج الكتل) وعندما يتجاوز معدل الكتل اليتيمة عتبة محددة ،يتم (تقليل معدل إنتاج الكتل).

يسمح هذا باستخدام إمكانيات النطاق الترددي للشبكة بالكامل. يشير معدل الأيتام المنخفض إلى أن الشبكة متصلة جيدًا ويمكنها التعامل مع نقل بيانات أكبر ؛ ثم يزيد البروتوكول من الإنتاجية في ظل هذه الظروف.

* + 1. **القضاء على Propagation Bottleneck لتكاثر الكتل**

يعتبر Propagation Bottleneck في أي شبكة blockchain هو انتشار الكتلة. يزيل بروتوكول إجماع Nervos CKB مشكل Propagation Bottleneck لانتشار الكتلة عن طريق تعديل تأكيد المعاملة إلى عملية من خطوتين: 1) اقتراح 2) الالتزام.

يجب أولاً اقتراح الصفقة في "منطقة الاقتراح" للكتلة (أو أحد أعمامها). سيتم بعد ذلك الالتزام بالمعاملة إذا ظهرت في "منطقة الالتزام" الخاصة بالكتلة ضمن نافذة محددة بعد اقتراحها. يزيل هذا التصميم Propagation Bottleneck لانتشار الكتلة ، حيث سيتم بالفعل استلام المعاملات الملتزمة الخاصة بالكتلة الجديدة والتحقق منها بواسطة الجميع في العقد عند اقتراحها.

**4.2.3 التخفيف من هجمات التعدين الأناني**

يعد التعدين الأناني أحد أهم الهجمات الأساسية على إجماع ناكاموتو. في هذا الهجوم ، يكتسب عمال المناجم الخبثاء مكافآت كتلة غير عادلة من خلال تعمد إخفاء الكتل عن قصد عن الآخرين.

يلاحظ الباحثون أن فرصة الربح غير العادلة متجذرة في آلية عمل الخاصة بإجماع ناكاموتو ، والتي تتجاهل الكتل المعزولة حسب قوة الحوسبة للشبكة. هذا يؤدي إلى انخفاض صعوبة التعدين ومكافآت كتلة بمتوسط ​​الوقت أعلى.

يدمج بروتوكول إجماع Nervos CKB كتل العم في جدول الصعوبات التي يجب حلها أولا لبد من فهم كتلة العم هي كتلة لم يتم تعدينها في السلسلة . يمكن استخراج كتلة واحدة فقط والاعتراف بها على أنها أساسية في blockchain. الكتل المتبقية هي كتل عم. عندما يقوم اثنان أو أكثر من عمال المناجم بإنتاج كتل في نفس الوقت تقريبًا ، يتم إنشاء كتل عمومية.

كتل العم تشبه الكتل اليتيمة على Bitcoin ولكن لها اختلافات دقيقة مرتبطة ببروتوكول Ethereum. كتل العم هي كتل صالحة رفضتها الشبكة. يتقاضى عمال المناجم رواتبهم مقابل إنتاج كتلة عم ، على عكس الكتلة اليتيمة ، حيث لا يحصل عمال المناجم على مكافأة.

، مما يجعل التعدين الأناني لم يعد مربحًا. هذا صحيح بغض النظر عن استراتيجية الهجوم أو مدته ؛ لا يستطيع عامل المناجم الحصول على مكافآت غير عادلة من خلال أي مزيج من التعدين الصادق والأناني.

يوضح تحليلنا أنه من خلال عملية تأكيد المعاملة المكونة من خطوتين ، يتم أيضًا التخلص من التعدين الأناني بحكم الواقع عبر نافذة زمنية محدودة للهجوم.

للحصول على فهم مفصل لبروتوكول الإجماع الخاص بنا ، يرجى قراءة [هنا](https://github.com/nervosnetwork/rfcs/blob/master/rfcs/0020-ckb-consensus-protocol/0020-ckb-consensus-protocol.md) .

**4.2.4 إثبات العمل** PoW  **مقابل إثبات الحصة** PoS

إن أنظمة إثبات العمل (PoW) وإثبات الحصة (PoS) كلاهما عرضة لتركيزات القوة ، ومع ذلك فإن خصائص الأنظمة توفر حقائق تشغيل مختلفة جدًا لمن هم في السلطة.

يتكبد تعدين إثبات العمل (PoW) نفقات في العالم الحقيقي يمكن أن تتجاوز عائدات التعدين دون إشراف دقيق على التكلفة. يُطلب من من هم في السلطة أن يظلوا مبتكرين وأن يتبعوا استراتيجيات عمل سليمة وأن يواصلوا الاستثمار في البنية التحتية ليظلوا مهيمنين. تخضع معدات التعدين وعمليات تجمع التعدين والوصول إلى الطاقة الرخيصة للتغيرات من الابتكار التكنولوجي. من الصعب الحفاظ على احتكار الثلاثة على مدى فترات طويلة من الزمن.

في المقابل ، تتم مكافأة منشئي الكتل في أنظمة PoS بطريقة حتمية ، بناءً على المبلغ المحصن ، بمتطلبات رأس مال تشغيلي منخفضة للغاية. مع نمو النظام ، سينمو تأثير المزايا الطبيعية المقدمة للشركات والأفراد أولاً. في نظام PoS ، من الممكن أن تتركز الطاقة في أيدي عدد قليل من المتحمسين. على الرغم من أن أنظمة إثبات العمل لديها مشكلة مماثلة مع تركيز التعدين ، فإن تكلفة البقاء في السلطة في نظام PoS أقل بكثير.

بالإضافة إلى ذلك ، يتمتع مدققو PoS بقدرة فريدة واحدة: التحكم في مجموعة المدققين . قبول المعاملة التي تسمح للمدقق بالانضمام إلى مجموعة الإجماع في أيدي المدققين الموجودين. سيكون من الصعب اكتشاف جهود التواطؤ للتأثير على المدقق الذي تم تعيينه من خلال الرقابة على المعاملات وأمر التلاعب ، فضلاً عن صعوبة المعاقبة. على العكس من ذلك ، فإن المشاركة بالإجماع في أنظمة إثبات العمل مفتوحة حقًا ولا تخضع لهيكل السلطة الحالي. لا يتم إعطاء المزايا للمشاركين الأوائل للنظام.

فيما يتعلق بالاقتصاد الرمزي ، في حين يُعتقد أن Staking يمكن أن يجذب رأس المال الذي يتطلع إلى كسب عائد (وبالتالي زيادة الطلب على الرمز المميز الأصلي) ، فإن هذه ليست الصورة الكاملة. ستشهد جميع مشاريع نقاط البيع (PoS) في نهاية المطاف استقرار معدل الرهان الخاص بها ، وعندئذٍ سيكون دخول رأس المال وخروجه من مجموعة رأس المال المربوط هو نفسه تقريبًا. لن تؤدي آلية Staking في حد ذاتها إلى زيادة الطلب على الرمز المميز الأصلي. بعبارة أخرى ، على الرغم من أن تقديم Staking يوفر طلبًا على الرمز الأصلي في المرحلة الأولية من المشروع (مع ارتفاع معدل Staking) ، لا يمكن أن يوفر Staking وحده طلبًا طويل الأجل على الرمز المميز الأصلي ، وبالتالي لا يمكن أن يكون كذلك القيمة الجوهرية الوحيدة للرمز الأصلي.

يمتلك حاملو الرموز طويلة الأجل في نظام PoS 3 خيارات: يمكنهم 1) إدارة البنية التحتية وتشغيل عقدة التحقق من الصحة بأنفسهم لتلقي إصدار جديد ، 2) تفويض الرموز المميزة الخاصة بهم إلى طرف ثالث والثقة في سلامتها وبنيتها التحتية ، أو 3 ) تخفف قيمة الرموز الخاصة بهم من خلال الإصدار المستمر. لا يعتبر أي من هذه الخيارات جذابًا بشكل خاص لمالكي الرموز طويلة الأجل والموجهة نحو القيمة.

نعتقد أن المشاركة غير المصرح بها من PoW هي شرط للبنية التحتية في أساس النشاط الاقتصادي العالمي. الهدف الرئيسي للطبقة 1 هو ضمان أن تكون blockchain لامركزية وآمنة ومحايدة قدر الإمكان. بينما تلعب أنظمة PoS دورًا في الاقتصاد اللامركزي ، إلا أنها في رأينا لا تفي بمتطلبات الطبقة 1 المفتوحة واللامركزية حقًا.

**4.2.5 إثبات وظيفة العمل**

يمكن اقتراح كتل Nervos CKB بواسطة أي عقدة ، بشرط أن تكون 1) الكتلة صالحة ؛ و 2) وان يقوم مقدم الطلب بحل لغز صعب حسابيًا يسمى إثبات العمل. يتم تعريف لغز إثبات العمل من حيث الكتلة المقترحة ؛ هذا يضمن أن حل اللغز يحدد بشكل فريد للكتلة.

يتطلب إثبات عمل Bitcoin العثور على رقم صحيح بحيث تفي نتيجة تطبيق دالة تجزئة على رأس الكتلة بمستوى معين من الصعوبة. بالنسبة إلى Bitcoin ، يتم تكرار دالة التجزئة مرتين SHA2–256. في حين أن SHA2 كان اختيارًا جيدًا للبيتكوين ، فإن الشيء نفسه لا ينطبق على العملات المشفرة التي تليها. تم تطوير كمية كبيرة من الأجهزة المخصصة لتعدين البيتكوين ، والتي يبقى جزء كبير منها في وضع الخمول ، بعد أن أصبحت قديمة بسبب تحسينات الكفاءة.

العملة المشفرة الجديدة التي تستخدم نفس لغز إثبات العمل ستجعل هذا الجهاز المهمل مفيدًا مرة أخرى. يمكن استئجار حتى الأجهزة الحديثة وإعادة تصميمها لتعدين عملة جديدة. سيكون من الصعب للغاية التنبؤ بتوزيع طاقة التعدين لعملة مستندة إلى SHA2 وعرضة للتغييرات المفاجئة والكبيرة. تنطبق هذه الحجة أيضًا على التحسينات الخوارزمية المصممة لـ SHA2 ، والتي تم تطويرها لجعل حساب البرنامج للوظيفة أرخص أيضًا.

بالنسبة للعملات المشفرة الجديدة ، من المنطقي تحديد لغز إثبات العمل من حيث الوظيفة التي لم يتم استخدامها بعد من قبل العملات المشفرة الأخرى. بالنسبة لـ Nervos CKB ، قطعنا خطوة إلى الأمام واخترنا تعريفها من حيث وظيفة إثبات العمل التي لا يمكن أن تكون موضوع تحسين سابق لأوانه ، لأنها جديدة.

ومع ذلك ، فإن عدم التوفر المقصود لأجهزة التعدين هو الحال فقط في البداية. على المدى الطويل ، تعد عمليات نشر أجهزة التعدين المخصصة مفيدة ، مما يزيد بشكل كبير من تحديات مهاجمة الشبكة. لذلك ، بالإضافة إلى كونها جديدة ، فإن الوظيفة المثالية لإثبات العمل لعملة رقمية جديدة هي أيضًا بسيطة ، مما يقلل بشكل كبير من حاجز تطوير الأجهزة.

الأمن هو الهدف الثالث الواضح للتصميم. في حين يمكن استغلال ثغرة معروفة من قبل جميع عمال المناجم على قدم المساواة ، وسوف تؤدي فقط إلى صعوبة أكبر ، يمكن أن تؤدي إحدى الثغرات غير المكشوف عنها إلى تحسين التعدين الذي يوفر للمكتشف (المكتشفين) ميزة تفوق حصتهم في قوة التعدين المساهمة. أفضل طريقة لتجنب هذا الموقف هو تقديم حجة قوية على عدم التعرض للخطر.

**4.2.6 خاصية Eaglesong**

Eaglesong هي وظيفة تجزئة جديدة تم تطويرها خصيصًا لإثبات عمل Nervos CKB ، ولكنها مناسبة أيضًا في حالات الاستخدام الأخرى التي تتطلب وظيفة تجزئة آمنة. كانت معايير التصميم كما هو مذكور أعلاه تمامًا: الابداع والبساطة والأمان. أردنا تصميمًا كان في نفس الوقت جديدًا بما يكفي ليشكل خطوة صغيرة إلى الأمام للعلم ، وكذلك قريبًا بدرجة كافية من التصاميم الحالية لتقديم حجة أمنية قوية.

تحقيقًا لهذه الغاية ، اخترنا إنشاء مثيل لهيكل (كما هو مستخدم في Keccak / SHA3) مع تبديل مبني من عمليات ARX (الإضافة ، والتناوب ، و xor) ؛ تستند حجة أمنها على استراتيجية المسار العريض (نفس الحجة الكامنة وراء AES).

على حد علمنا ، تعتبر Eaglesong أول وظيفة تجزئة (أو وظيفة ، لهذه المسألة) التي تجمع بنجاح بين مبادئ التصميم الثلاثة.

يمكنك قراءة المزيد عن Eaglesong  [هنا](https://medium.com/nervosnetwork/the-proof-of-work-function-of-nervos-ckb-3cc8364464d9) .

**4.3 نموذج الخلية**

يستخدم Nervos CKB نموذج الخلية ، وهو بناء جديد يمكن أن يوفر العديد من مزايا نموذج الحساب (المستخدم في Ethereum) ، مع الحفاظ على ملكية الأصول وخصائص التحقق القائمة على الإثبات لنموذج UTXO (المستخدم في Bitcoin).

يركز نموذج الخلية على الحالة. تحتوي الخلايا على بيانات عشوائية ، والتي قد تكون بسيطة ، مثل مبلغ الرمز المميز والمالك ، أو أكثر تعقيدًا ، مثل الرمز الذي يحدد شروط التحقق لنقل الرمز المميز. ينفذ جهاز الحالة في CKB البرامج النصية المرتبطة بالخلايا لضمان سلامة انتقال الحالة.

بالإضافة إلى تخزين البيانات الخاصة بها ، يمكن للخلايا الرجوع إلى البيانات في خلايا أخرى. يسمح ذلك بفصل الأصول المملوكة للمستخدم والمنطق الذي يحكمها. هذا على عكس منصات العقود الذكية القائمة على الحسابات ، حيث تكون الحالة ملكية داخلية لعقد ذكي ويجب الوصول إليها من خلال واجهات عقد ذكية. في Nervos CKB ، الخلايا هي كائنات حالة مستقلة مملوكة ، ويمكن الرجوع إليها وتمريرها مباشرة. يمكن للخلايا التعبير عن "أصول محتملة" ، تنتمي إلى مالكيها (تمامًا مثل UTXO هي أصول يمكن تحملها لمالكي Bitcoin) ، مع الإشارة إلى خلية تحمل منطقًا يضمن سلامة انتقالات المعاملات

معاملات نموذج الخلية هي أيضًا أدلة حالة على الانتقال. تتم إزالة خلايا إدخال المعاملة من مجموعة الخلايا النشطة وتتم إضافة خلايا الإخراج إلى المجموعة. تشكل الخلايا النشطة الحالة العامة لـ Nervos CKB ، وهي غير قابلة للتغيير: بمجرد إنشاء الخلايا ، لا يمكن تغييرها.

تم تصميم نموذج الخلية ليكون قابلاً للتكيف ومستدامًا ومرنًا. يمكن وصفه كنموذج UTXO معمم ويمكن أن يدعم الرموز المميزة التي يحددها المستخدم والعقود الذكية وبروتوكولات الطبقة 2 المتنوعة.

لفهم أعمق لنموذج الخلية ، يرجى الاطلاع [هنا](https://medium.com/nervosnetwork/https-medium-com-nervosnetwork-cell-model-7323fca57571) .

**4.4 آلة افتراضية**

في حين أن العديد من مشاريع blockchain من الجيل التالي تستخدم WebAssembly كأساس لجهاز افتراضي blockchain ، يتضمن Nervos CKB خيار التصميم الفريد لجهاز افتراضي (CKB-VM) استنادًا إلى مجموعة تعليمات RISC-V.

RISC-V عبارة عن بنية مجموعة تعليمات RISC مفتوحة المصدر تم إنشاؤها في عام 2010 لتسهيل تطوير أجهزة وبرامج جديدة ، وهي مجموعة تعليمات خالية من حقوق الملكية ومفهومة على نطاق واسع ومدققة على نطاق واسع.

لقد وجدنا العديد من المزايا لاستخدام RISC-V في سياق blockchain:

* الاستقرار: تم الانتهاء من مجموعة التعليمات الأساسية RISC-V وتجميدها، فضلاً عن تنفيذها واختبارها على نطاق واسع. تم إصلاح مجموعة تعليمات RISC-V الأساسية ولن تتطلب تحديثًا أبدًا.
* مفتوح ومدعوم: يتم توفير RISC-V بموجب ترخيص BSD ومدعوم من قبل مجمعين مثل GCC و LLVM ، مع تطبيقات لغة Rust and Go قيد التطوير. تضم مؤسسة RISC-V أكثر من 235 منظمة عضو تعزز تطوير مجموعة التعليمات ودعمها.
* البساطة والقابلية للتوسعة: مجموعة تعليمات RISC-V بسيطة. مع دعم الأعداد الصحيحة 64 بت ، تحتوي المجموعة على 102 تعليمات فقط. يوفر RISC-V أيضًا آلية معيارية لمجموعات التعليمات الموسعة ، مما يتيح إمكانية الحوسبة المتجهة أو الأعداد الصحيحة 256 بت لخوارزميات التشفير عالية الأداء.
* تسعير دقيق للموارد: يمكن تشغيل مجموعة تعليمات RISC-V على وحدة معالجة مركزية فعلية ، مما يوفر تقديرًا دقيقًا لدورات الجهاز المطلوبة لتنفيذ كل تعليمات وإبلاغ أسعار موارد الجهاز الظاهري.

CKB-VM عبارة عن جهاز افتراضي RISC-V منخفض المستوى يسمح بحساب مرن وكامل. من خلال استخدام تنسيق ELF المطبق على نطاق واسع ، يمكن تطوير نصوص CKB-VM بأي لغة يمكن تجميعها لتعليمات RISC-V.

**4.4.1 جهازCKB-VM والية نموذج الخلية**

بمجرد نشرها ، تكون البلوكشين العامة الحالية ثابتة بشكل أو بآخر. تتضمن ترقية العناصر الأساسية ، مثل أساسيات التشفير ، تعهدات متعددة السنوات أو ببساطة غير ممكنة.

يأخذ CKB-VM خطوة إلى الوراء ، وينقل العناصر الأولية التي تم إنشاؤها مسبقًا في أجهزة ظاهرية مخصصة إلى الخلايا الموجودة أعلى الجهاز الظاهري. على الرغم من أن نصوص CKB منخفضة المستوى أكثر من العقود الذكية في Ethereum ، إلا أنها تحمل فائدة كبيرة تتمثل في المرونة ، مما يتيح منصة وأساسًا متجاوبًا للاقتصاد اللامركزي المتقدم.

يمكن للخلايا تخزين التعليمات البرمجية القابلة للتنفيذ والإشارة إلى الخلايا الأخرى على أنها تابعة . يتم تنفيذ جميع الخوارزميات وهياكل البيانات تقريبًا كنصوص CKB مخزنة داخل الخلايا. من خلال الحفاظ على الجهاز الظاهري بسيطًا قدر الإمكان وتفريغ تخزين البرنامج في الخلايا ، يكون تحديث الخوارزميات الرئيسية بسيطًا مثل تحميل الخوارزمية في خلية جديدة وتحديث الموجودة.

**4.4.2 تشغيل الأجهزة الافتراضية الأخرى على CKB-VM**

بفضل الطبيعة منخفضة المستوى لـ CKB-VM وتوافر الأدوات في مجتمع RISC-V ، من السهل تجميع الأجهزة الافتراضية الأخرى (مثل EVM الخاص بـ Ethereum) مباشرةً في CKB-VM. هذا له العديد من المزايا:

* يمكن بسهولة نقل العقود الذكية المكتوبة بلغات متخصصة تعمل على أجهزة افتراضية أخرى لتشغيلها على CKB-VM. (بالمعنى الدقيق للكلمة ، سيتم تشغيلهم على جهاز VM الخاص بهم والذي تم تجميعه للتشغيل داخل CKB-VM.)
* يمكن لـ CKB التحقق من انتقالات حالة تسوية المنازعات لمعاملات الطبقة 2 ، حتى إذا تمت كتابة قواعد انتقالات الحالة للتشغيل في جهاز افتراضي غير CKB-VM. هذا هو أحد المتطلبات الرئيسية لدعم السلاسل الجانبية للأغراض العامة للطبقة 2 غير الموثوقة.

للحصول على إرشادات تقنية حول CKB-VM ، يرجى الاطلاع [هنا](https://medium.com/nervosnetwork/an-introduction-to-ckb-vm-9d95678a7757) .

**4.5 النموذج الاقتصادي**

الرمز الأصلي لـ Nervos CKB هو "بايت المعرفة العامة" ، أو CKByte للاختصار. تخول CKBytes حامل الرمز المميز لشغل جزء من إجمالي تخزين الحالة في blockchain. على سبيل المثال ، من خلال الاحتفاظ بـ 1000 CKBytes ، يكون المستخدم قادرًا على إنشاء خلية بسعة 1000 بايت أو خلايا متعددة بإضافة سعة تصل إلى 1000 بايت.

يؤدي استخدام CKBytes لتخزين البيانات على CKB إلى إنشاء تكلفة فرصة لمالكي CKByte ؛ لن يكونوا قادرين على إيداع CKBytes المشغولة في NervosDAO لتلقي جزء من الإصدار الثانوي. يتم تسعير CKBytes في السوق ، وبالتالي يتم توفير حافز اقتصادي للمستخدمين للإفراج الطوعي عن تخزين الشبكة لتلبية الطلب المرتفع للحالة المتوسعة. بعد قيام المستخدم بإصدار تخزين الحالة ، سيحصل على كمية من CKBytes مكافئة لحجم الحالة (بالبايت) التي كانت بياناته تشغلها.

يسمح النموذج الاقتصادي لـ CKB بإصدار العملة الأصلية من أجل نمو الشبكة، والحفاظ على حاجز منخفض للمشاركة وضمان اللامركزية. نظرًا لأن CKBytes أصبحت موردًا نادرًا ، يمكن تسعيرها وتخصيصها بكفاءة أكبر.

سيحتوى العرض المتداول الخاصة بشبكة Nervos على 33.6 مليار CKBytes ، سيتم حرق 8.4 مليار منها على الفور. يتضمن الإصدار الجديد من CKBytes جزأين - الإصدار الأساسي والإصدار الثانوي. يقتصر الإصدار الأساسي على إجمالي العرض المحدود (33.6 مليار CKBytes) ، مع جدول إصدار مشابه لعملة البيتكوين. تنخفض مكافأة الكتلة إلى النصف تقريبًا كل 4 سنوات ، حتى تصل إلى 0 إصدار جديد. تُمنح جميع الإصدارات الأساسية لعمال المناجم كحوافز لحماية الشبكة. الإصدار الثانوي له معدل إصدار ثابت يبلغ 1.344 مليار CKBytes سنويًا وهو مصمم لفرض تكلفة الفرصة البديلة لشغل التخزين على البلوك تشين بعد توقف الإصدار الأساسي ، سيكون هناك إصدار ثانوي فقط.

يتضمن Nervos CKB عقدًا ذكيًا خاصًا يسمى NervosDAO ، والذي يعمل بمثابة "مأوى التضخم" ضد تأثيرات الإصدار الثانوي. يمكن لمالكي CKByte إيداع الرموز الخاصة بهم في NervosDAO والحصول على جزء من الإصدار الثانوي الذي يعوض تمامًا الآثار التضخمية من الإصدار الثانوي. بالنسبة لحاملي التوكنات طويلة الأجل ، طالما قاموا بإغلاق الرموز المميزة الخاصة بهم في NervosDAO ، فإن التأثير التضخمي للإصدار الثانوي يكون اسميًا فقط. مع تخفيف آثار الإصدار الثانوي ، فإن هؤلاء المستخدمين يحتفظون فعليًا برموز محدودة الحد الأقصى مثل Bitcoin.

أثناء استخدام CKBytes لتخزين الحالة ، لا يمكن استخدامها لكسب مكافآت إصدار ثانوية من خلال NervosDAO. هذا يجعل الإصدار الثانوي ضريبة تضخم ثابتة ، أو "إيجار الشبكة" يفرض هذا النموذج الاقتصادي رسوم تخزين تتناسب مع مساحة ووقت شغل المساحة . إنه أكثر استدامة من نموذج "الدفع مرة واحدة ، وشغل إلى الأبد" الذي تستخدمه المنصات الأخرى ، وهو أكثر جدوى وسهولة في الاستخدام من حلول الإيجار الأخرى التي تتطلب مدفوعات صريحة.

يتم تعويض عمال المناجم بمكافآت الكتلة ورسوم المعاملات. بالنسبة لمكافآت الكتلة ، عندما يقوم عامل منجم بتعدين كتلة ، فإنه سيحصل على مكافأة الإصدار الأساسي الكاملة للكتلة ، وجزءًا من الإصدار الثانوي. يعتمد الجزء على مدى توفر مساحة التخزين ، على سبيل المثال: إذا تم استخدام نصف جميع الرموز المميزة الأصلية لتخزين الحالة ، فسيحصل عامل التعدين على نصف مكافأة الإصدار الثانوي للكتلة. يتم تضمين معلومات إضافية حول توزيع الإصدار الثانوي في القسم التالي (4.6). على المدى الطويل ، عندما يتوقف الإصدار الأساسي ، سيستمر عمال المناجم في الحصول على دخل "إيجار الشبكة " المستقل عن المعاملات ، ولكنه مرتبط باعتماد قاعدة المعرفة العامة Nervos.

على سبيل المقارنة ، يمكن اعتبار CKBytes على أنها أرض ، في حين يمكن اعتبار الأصول المشفرة المخزنة على CKB بمثابة منازل. الأرض مطلوبة لبناء منزل ، و CKBytes مطلوبة لتخزين الأصول على CKB. مع زيادة الطلب على تخزين الأصول على CKB ، يرتفع الطلب على CKBytes أيضًا. مع ارتفاع قيمة الأصول المخزنة ، ترتفع قيمة CKBytes أيضًا.

تم تصميم Nervos CKB لترجمة الطلب على العديد من الأصول إلى طلب على أصل واحد ، واستخدامه لتعويض عمال المناجم لتأمين الشبكة.

لمزيد من الشرح التفصيلي عن النموذج الاقتصادي ، يرجى الاطلاع [هنا](https://github.com/nervosnetwork/rfcs/blob/master/rfcs/0015-ckb-cryptoeconomics/0015-ckb-cryptoeconomics.md) .

**4.6 الخزينة**

الجزء من الإصدار الثانوي الذي لا يذهب إلى 1) عمال المناجم أو 2) حاملي العملات على المدى الطويل الذين لديهم رموز مقفلة في NervosDAO ، سيذهب إلى صندوق الخزانة. للتوضيح: إذا تم استخدام 60٪ من CKBytes التي تم إصدارها لتخزين الحالة وتم إيداع 30٪ من CKBytes في NervosDAO ، سيحصل عمال المناجم على 60٪ من الإصدار الثانوي ، وسيحصل NervosDAO (أصحاب المدى الطويل) على 30٪ من الإصدار الثانوي ، وسيذهب 10٪ من الإصدار الثانوي إلى الخزينة.

سيتم استخدام صندوق الخزانة لتمويل البحث والتطوير المستمر للبروتوكول ، بالإضافة إلى بناء النظام البيئي لشبكة نيرفوس. سيكون استخدام أموال الخزينة مفتوحًا وشفافًا ومتسلسلًا ليراه الجميع. مقارنة بنموذج تمويل الخزانة القائم على التضخم ، فإن هذا النموذج لا يخفف من حاملي الرموز طويلة الأجل (الذين قاموا بإيداع الرموز الخاصة بهم في NervosDAO). يتم اشتقاق تمويل تطوير البروتوكول بشكل صارم من تكلفة الفرصة البديلة لحاملي الرموز قصيرة الأجل.

لن يتم تنشيط الخزانة فور إطلاق الشبكة الرئيسية لقاعدة المعرفة العامة نيرفوس. بموافقة المجتمع ، سيتم تنشيطه باستخدام هارد فورك لاحقًا ، فقط بعد أن استنفدت مؤسسة نيرفوس صندوق النظام البيئي ، المتضمن في مجموعة جينيسيس. قبل تفعيل الخزانة ، سيتم حرق هذا الجزء من الإصدار الثانوي.

**4.7 الحوكمة**

الحوكمة هي كيفية تنظيم المجتمع أو المجموعات داخله لاتخاذ القرارات. يجب أن يشارك كل طرف ذي صلة لديه مصلحة في النظام في هذه العملية. فيما يتعلق بـ blockchain ، لا ينبغي أن يشمل ذلك فقط المستخدمين ، والمالكين ، وعمال المناجم ، والباحثين ، والمطورين ، ولكن أيضًا مقدمي الخدمات مثل المحافظ ، والبورصات ، ومجمعات التعدين أيضًا. لدى مجموعات أصحاب المصلحة المختلفة اهتمامات متنوعة ويكاد يكون من المستحيل مواءمة حوافز الجميع. هذا هو السبب في أن حوكمة blockchain موضوع معقد ومثير للجدل. إذا اعتبرنا blockchain تجربة اجتماعية كبيرة ، فإن الحوكمة تتطلب تصميمًا أكثر تعقيدًا من أي جزء آخر من النظام. بعد عشر سنوات من التطور ، ما زلنا لم نحدد أفضل الممارسات العامة أو العمليات المستدامة لحوكمة blockchain.

تدير بعض المشاريع الحكم عبر "ديكتاتور خير مدى الحياة" (مثل لينوس تورفالدس إلى لينكس). نحن ندرك أن هذا يجعل المشروع عالي الكفاءة ومتماسكًا وجذابًا أيضًا: فالناس يحبون الأبطال ؛ ومع ذلك ، فإن هذا يتعارض مع اللامركزية ، القيمة الأساسية لـ blockchain.

تكلف بعض المشاريع لجنة متميزة خارج السلسلة بسلطة اتخاذ القرار بعيدة المدى ، مثل ECAF (منتدى التحكيم الأساسي EOSIO) على EOS. ومع ذلك ، تفتقر هذه اللجان إلى القوة الأساسية لضمان التزام المشاركين بقراراتهم ، والتي كان من الممكن أن تلعب دورًا في قرار إغلاق ECAF في وقت سابق من هذا العام.

تذهب بعض المشاريع ، مثل Tezos ، إلى أبعد من ذلك ، وتنفذ حوكمة على السلسلة لضمان التزام جميع المشاركين بالتصويت على القرارات. يؤدي هذا أيضًا إلى تجنب أي آثار للخلاف بين المطورين وعمال المناجم (أو مستخدمي العقدة الكاملة). لاحظ أن الحوكمة على السلسلة تختلف عن التصويت البسيط على السلسلة ، إذا حصلت الميزة أو التصحيح المقترح على عدد كافٍ من الأصوات من خلال الحوكمة على السلسلة ، فسيتم تحديث رمز السلسلة تلقائيًا ، ولن يكون لدى المعدنين أو العقد الكاملة أي وسيلة لذلك السيطرة على هذا التغيير. يتبنى Polkadot نهجًا أكثر تعقيدًا للحوكمة على السلسلة ، باستخدام مجلس منتخب ، وعملية الاستفتاء للتصويت المرجح بالحصص وآليات التحيز الإيجابي / السلبي لحساب نسبة إقبال الناخبين.

ومع ذلك ، على الرغم من وضوحها ، إلا أن الحوكمة عبر السلسلة في الممارسة ليست أنيقة كما هي مقدمة.  ، تعكس الأصوات فقط مصلحة حاملي الرموز ، بينما تتجاهل ببساطة جميع الأطراف الأخرى. ثانيًا ، يعد معدل التصويت المنخفض مشكلة طويلة الأمد في كل من عالم blockchain والعالم الحقيقي. كيف يمكن أن تكون النتائج في مصلحة الأغلبية إذا كان صوت الأقلية فقط؟ أخيرًا ولكن الأهم من ذلك ، يجب دائمًا اعتبار الهارد فورك كملاذ أخير لجميع أصحاب المصلحة. نظرًا لتوافر البيانات الممتاز الذي يوفره النسخ المتماثل الواسع لـ blockchain بدون إذن ، يجب أن يكون الابتعاد عن السلسلة الحالية مع الاحتفاظ الكامل بالبيانات ودون انقطاع خيارًا دائمًا. لا يمكن تنفيذ الهارد فورك من خلال الحوكمة على السلسلة.

لا توجد حتى الآن إجابات قابلة للتطبيق على أسئلة الحوكمة ، لذلك بالنسبة لشبكة نيرفوس ، سنتخذ نهجًا متطورًا. نتوقع أن يتطور المجتمع بشكل عضوي في الأيام الأولى وبمرور الوقت ، حيث يتم تعدين المزيد من الرموز ، ويصبح التعدين أكثر توزيعًا ، ويشارك المزيد من المطورين ، وستصبح مسؤوليات الحوكمة تدريجية أكثر لامركزية. على المدى الطويل ، ستدير الإدارة المجتمعية عملية ترقية البروتوكول وتخصيص الموارد من الخزانة.

تم تصميم Nervos CKB لتكون بنية تحتية مستقلة لامركزية يمكن أن تستمر لمئات السنين ، مما يعني أن هناك بعض الأشياء التي تتطلب بذل قصارى جهدنا كمجتمع للحفاظ على صحتها ، بغض النظر عن كيفية تطور هذه الشبكة. الثوابت الثلاثة الأساسية هي:

* جدول الإصدار ثابت تمامًا ، وبالتالي لن يتغير أبدًا.
* لا يجوز العبث بالحالة / البيانات المخزنة في الخلايا.
* لن يتم تغيير دلالات النصوص الموجودة.

تعد الحوكمة القائمة على المجتمع للبلوكشين مجالًا جديدًا للغاية وهناك العديد من التجارب الجارية الجديرة بالاهتمام. نحن ندرك أن هذا ليس موضوعًا تافهًا ، وأن الوقت مطلوب للدراسة والمراقبة والتكرار بشكل كامل للوصول إلى النهج الأمثل. نحن نتبع نهجًا متحفظًا للحوكمة المجتمعية على المدى القصير ، مع الحفاظ على التزامنا الكامل بهذا الاتجاه على المدى الطويل.

**5. نظرة عامة على حلول الطبقة الثانية**

**5.1 ما هي الطبقة 2؟**

تُعرَّف الطبقة 1 من شبكة blockchain بالقيود. لا تقدم blockchain من الطبقة الأولى المثالية أي تنازلات بشأن الأمان واللامركزية والاستدامة ، ومع ذلك ، فإن هذا يخلق تحديات تتعلق بقابلية التوسع وتكاليف المعاملات. تم تصميم حلول الطبقة الثانية على قمة بروتوكولات الطبقة 1 ، مما يسمح بنقل الحساب خارج السلسلة بآليات للاستقرار بشكل آمن في طبقة block 1 blockchain.

هذا مشابه للتسوية الصافية في النظام المصرفي اليوم أو الإيداعات التنظيمية التي تفرضها هيئة الأوراق المالية والبورصات. من خلال تقليل كمية البيانات التي تتطلب إجماعًا عالميًا ، يمكن للشبكة أن تخدم عددًا أكبر من المشاركين وتسهل نشاطًا اقتصاديًا أكثر مما كانت ستتمكن من القيام به بخلاف ذلك ، مع الحفاظ على خصائص اللامركزية.

يعتمد مستخدمو الطبقة الثانية على الأمان الذي يوفره blockchain للطبقة الأولى ، ويستخدمون هذا الأمان عند نقل الأصول بين الطبقات أو تسوية نزاع. تشبه هذه الوظيفة نظام المحاكم: لا يتعين على المحكمة مراقبة جميع المعاملات والتحقق منها ، ولكنها تعمل فقط كمكان لتسجيل الأدلة الرئيسية وتسوية النزاعات. وبالمثل ، في سياق blockchain ، تسمح طبقة blockchain من الطبقة الأولى للمشاركين بالتعامل خارج السلسلة ، وفي حالة وجود خلاف يوفر لهم القدرة على تقديم أدلة تشفير إلى blockchain ومعاقبة عدم الأمانة.

**5.2 قنوات الدفع والولاية**

يتم إنشاء قنوات الدفع بين طرفين يتعاملان كثيرًا. إنها توفر تجربة دفع فورية منخفضة لا يمكن للمعاملات التي تتم مباشرة على blockchain العالمية توفيرها. تعمل قنوات الدفع بشكل مشابه لعلامة تبويب الشريط - يمكنك فتح علامة تبويب مع نادل والاستمرار في طلب المشروبات ، ولكن فقط قم بتسوية علامة التبويب ودفع المبلغ النهائي عندما تكون مستعدًا لمغادرة الشريط. أثناء تشغيل قناة الدفع ، يتبادل المشاركون رسائل تحتوي على التزامات تشفير لأرصدةهم ويمكنهم تحديث هذه الأرصدة لعدد غير محدود من المرات خارج السلسلة ، قبل أن يكونوا مستعدين لإغلاق القناة وتسوية الأرصدة مرة أخرى على blockchain.

يمكن أن تكون قنوات الدفع أحادية الاتجاه أو ثنائية الاتجاه. تتدفق قنوات الدفع أحادية الاتجاه من الطرف "أ" إلى الطرف "ب" ، على غرار مثال علامة تبويب الشريط أعلاه. يقوم الطرف "أ" بإيداع الحد الأقصى للمبلغ الذي قد ينفقه مع الطرف "ب" ، ثم يقوم بالتوقيع ببطء على الأموال أثناء تلقيهم السلع أو الخدمات.

تعد قنوات الدفع ثنائية الاتجاه أكثر تعقيدًا ، ولكنها تبدأ في إظهار نطاق الاحتمالات لتقنيات الطبقة الثانية. في قنوات الدفع هذه ، تتدفق الأموال ذهابًا وإيابًا بين الأطراف. يسمح ذلك "بإعادة موازنة" قنوات الدفع ويفتح إمكانية الدفع عبر القنوات من خلال طرف مقابل مشترك. يتيح ذلك لشبكات قنوات الدفع ، مثل شبكة Lightning Network الخاصة ببيتكوين. يمكن تحويل الأموال من الطرف "أ" إلى الطرف "ب" بدون قناة مباشرة بينهما ، طالما أن الطرف "أ" يمكنه العثور على مسار عبر وسيط مع اتصالات مفتوحة لكلا الطرفين.

مثلما يمكن لقنوات الدفع توسيع نطاق المدفوعات عبر السلسلة ، يمكن للقنوات الحكومية توسيع نطاق أي معاملات على السلسلة. بينما تقتصر قناة الدفع على إدارة الأرصدة بين طرفين ، فإن قناة الشبكة هي اتفاق على حالة معينة ، مما يتيح كل شيء من لعبة الشطرنج غير الموثوق بها إلى التطبيقات اللامركزية القابلة للتطوير.

على غرار قناة الدفع ، يفتح الطرفان قناة ويتبادلان التوقيعات المشفرة بمرور الوقت ويقدمان الحالة النهائية (أو النتيجة) لعقد ذكي على السلسلة. سيتم بعد ذلك تنفيذ العقد الذكي بناءً على هذا الإدخال ، وتسوية المعاملة وفقًا للقواعد المشفرة في العقد.

"قناة الشبكة المعممة" هي بناء شبكة قوي ، مما يسمح لها بدعم انتقالات متعددة عبر عقود ذكية متعددة. هذا يقلل من تضخم الحالة المتأصل في بنية "قناة واحدة لكل تطبيق" ويسمح أيضًا بالتعامل السهل مع القدرة على استخدام قنوات الحالة التي فتحها المستخدمون بالفعل.

**5.3 السلاسل الجانبية**

السلسلة الجانبية عبارة عن blockchain منفصل متصل بـ blockchain غير موثوق به (سلسلة رئيسية) مع ربط ثنائي الاتجاه. للاستفادة من السلسلة الجانبية ، يرسل المستخدم الأموال إلى عنوان محدد على السلسلة الرئيسية ، ويغلق هذه الأموال تحت سيطرة مشغلي السلسلة الجانبية. بمجرد تأكيد هذه المعاملة ومرور فترة الأمان ، يمكن إرسال دليل إلى مشغلي السلسلة الجانبية يوضح بالتفصيل إيداع الأموال. سيقوم المشغلون بعد ذلك بإنشاء معاملة على السلسلة الجانبية ، وتوزيع الأموال المناسبة. يمكن بعد ذلك إنفاق هذه الأموال على السلسلة الجانبية برسوم منخفضة وتأكيد سريع وإنتاجية عالية.

العيب الرئيسي للسلاسل الجانبية هو أنها تتطلب آليات أمنية إضافية وافتراضات أمنية. إن أبسط إنشاءات السلسلة الجانبية ، وهي سلسلة جانبية متحدة ، تضع الثقة في مجموعة متعددة التوقيعات من المشغلين. على منصات العقود الذكية ، يمكن ضبط نماذج الأمان باستخدام حوافز رمزية أو ألعاب اقتصادية للترابط / التحدي / القطع.

بالمقارنة مع حلول التوسع للأغراض العامة الأخرى خارج السلسلة ، فإن السلاسل الجانبية أسهل في الفهم والتنفيذ. بالنسبة لأنواع التطبيقات التي تسمح بإنشاء نموذج ثقة مقبول لمستخدميها ، يمكن أن تكون السلاسل الجانبية حلاً عمليًا.

**5.4 سلاسل الالتزام**

في سلاسل الالتزام [6] ، مثل البلازما [7] ، يتم إنشاء سلسلة الطبقة 2 التي تعزز جذر الثقة في طبقة 1 blockchain (سلسلة الجذر) مع إجماع عالمي واسع. سلاسل الالتزام هذه آمنة ؛ في حالة ما إذا كان مشغل السلسلة ضارًا أو غير فعال ، يمكن للمستخدمين دائمًا سحب أصولهم من خلال آلية على سلسلة الجذر.

عامل سلسلة الالتزام موثوق به لتنفيذ المعاملات بشكل صحيح ونشر تحديثات دورية لسلسلة الجذر. في ظل جميع الظروف ، باستثناء هجوم رقابي مطول على سلسلة الجذر ، ستظل الأصول في سلاسل الالتزام آمنة. على غرار السلاسل الجانبية الموحدة ، تقدم تصميمات سلسلة الالتزام تجربة مستخدم فائقة مقارنة بسلاسل الكتل غير الموثوق بها. ومع ذلك ، فإنهم يفعلون ذلك مع الحفاظ على ضمانات أمنية أقوى.

يتم تأمين سلسلة الالتزام من خلال مجموعة من العقود الذكية التي تعمل على سلسلة الجذر. يقوم المستخدمون بإيداع الأصول في هذا العقد ومن ثم يقوم مشغل سلسلة الالتزام بتزويدهم بأصول في سلسلة الالتزام. سينشر المشغل بشكل دوري الالتزامات لسلسلة الجذر ، والتي يمكن للمستخدمين استخدامها لاحقًا لإثبات ملكية الأصول من خلال أدلة Merkle ، "خروج" ، حيث يتم سحب أصول سلسلة الالتزام إلى سلسلة الجذر.

يصف هذا المفهوم العام لتصميمات سلسلة الالتزام ، وهي أساس عائلة البروتوكولات الناشئة بما في ذلك البلازما. يقدم المستند التعريفي التمهيدي الخاص بالبلازما [7] الذي أصدره فيتاليك بوتيرين وجوزيف بون في عام 2017 رؤية طموحة. على الرغم من أن جميع سلاسل Plasma تعتمد حاليًا على الأصول ، ولا يمكنها تخزين سوى ملكية الرموز القابلة للاستبدال وغير القابلة للاستبدال (والتحويلات) ، إلا أن تنفيذ الكود غير الموثوق به (أو العقود الذكية) يعد مجالًا نشطًا للبحث.

**5.5 حسابات خارج السلسلة يمكن التحقق منها**

يوفر التشفير أداة مصممة على ما يبدو لتناسب ديناميكيات التحقق عبر السلسلة باهظة الثمن والحساب غير المكلف خارج السلسلة: أنظمة الإثبات التفاعلية. نظام الإثبات التفاعلي هو بروتوكول يضم اثنين من المشاركين ، المُثبِّت والمحقق. من خلال إرسال الرسائل ذهابًا وإيابًا ، سيوفر المُثبِّت معلومات لإقناع المدقق بأن ادعاءً معينًا صحيحًا ، بينما سيفحص المدقق ما يتم تقديمه ويرفض الادعاءات الكاذبة. يتم قبول الادعاءات التي لا يمكن للمدقق رفضها على أنها صحيحة.

السبب الرئيسي لعدم قيام المدقق بالتحقق من الادعاء بسذاجة من تلقاء نفسه هو الكفاءة - من خلال التفاعل مع Prover ، يمكن للمدقق التحقق من الادعاءات التي قد تكون باهظة التكلفة للتحقق من خلاف ذلك. يمكن أن تأتي فجوة التعقيد هذه من مجموعة متنوعة من المصادر: 1) قد يقوم المدقق بتشغيل أجهزة خفيفة الوزن يمكن أن تدعم فقط الحسابات المحددة بالمساحة أو المحددة بالوقت (أو كليهما) ، 2) قد يتطلب التحقق الوصول إلى تسلسل طويل من عدم التحديد 3) قد يكون التحقق مستحيلاً لأن المدقق لا يمتلك معلومات سرية معينة.

في حين أن سرية المعلومات المهمة هي بالتأكيد عاملاً مقيدًا مناسبًا في سياق العملات المشفرة ، فإن تكلفة التحقق عبر السلسلة هي عامل مقيد أكثر صلة في سياق قابلية التوسع ، لا سيما على النقيض من الحسابات الرخيصة نسبيًا خارج السلسلة.

في سياق العملات المشفرة ، تم توجيه اهتمام كبير نحو zk-SNARKs (المعرفة الصفرية ، الحجج المختصرة غير التفاعلية للمعرفة). تدور هذه العائلة من أنظمة الإثبات غير التفاعلية حول الدائرة الحسابية ، والتي تشفر حسابًا تعسفيًا كدائرة من الإضافات والمضاعفات على مجال محدود

البراهين zk-SNARK ذات حجم ثابت (مئات البايتات) ويمكن التحقق منها في وقت ثابت ، على الرغم من أن كفاءة أداة التحقق هذه تأتي بتكلفة: يلزم إعداد موثوق وسلسلة مرجعية منظمة ، بالإضافة إلى العمليات الحسابية القائمة على الاقتران (منها لا تزال صلابة التشفير الملموسة موضع قلق).

توفر أنظمة الإثبات البديلة مقايضات مختلفة. على سبيل المثال ، ليس لدى Bulletproofs أي إعداد موثوق به وتعتمد على افتراض اللوغاريتم المنفصل الأكثر شيوعًا ، ومع ذلك لديها أدلة لوغاريتمية الحجم (على الرغم من أنها لا تزال صغيرة جدًا) وأدوات التحقق من الوقت الخطي. توفر zk-STARKs بديلاً لـ zk-SNARKs من حيث قابلية التوسع ، دون إعداد موثوق به وتعتمد فقط على افتراضات التشفير الصلبة ، على الرغم من أن البرهان الناتج ذو حجم لوغاريتمي (وكبير جدًا: مئات الكيلو بايت).

في سياق النظام البيئي متعدد الطبقات للعملات المشفرة مثل شبكة Nervos ، توفر البراهين التفاعلية القدرة على تفريغ العمليات الحسابية الباهظة الثمن من جانب المُثبِّت إلى الطبقة 2 بينما تتطلب فقط عملًا متواضعًا من جانب المُحقق من الطبقة 1. يتم التقاط هذا الحدس ، على سبيل المثال ، في بروتوكول ZK Rollup [8] في Vitalik Buterin: يجمع المرحل غير المرخص المعاملات خارج السلسلة ويقوم دوريًا بتحديث جذر Merkle المخزن في السلسلة. كل تحديث جذر يرافقه zk-SNARK الذي يوضح أنه تم تجميع المعاملات الصالحة فقط في شجرة Merkle الجديدة. يتحقق العقد الذكي من الإثبات ويسمح بتحديث جذر Merkle فقط إذا كان الإثبات صالحًا.

يجب أن يكون البناء الموضح أعلاه قادرًا على دعم انتقالات الحالة الأكثر تعقيدًا بما يتجاوز المعاملات البسيطة ، بما في ذلك DEX والرموز المتعددة والحسابات التي تحافظ على الخصوصية.

**5.6 النموذج الاقتصادي لحلول الطبقة الثانية**

بينما توفر حلول الطبقة الثانية قابلية توسع رائعة ، فإن اقتصاد المميز لهذه الأنظمة قد تشكل تحديات في التصميم.

قد يتضمن اقتصاد الرمز المميز من الطبقة الثانية تعويضًا عن البنية التحتية الحيوية (مثل المدققين وأبراج المراقبة) ، بالإضافة إلى تصميم الحوافز الخاصة بالتطبيقات. تميل البنية التحتية الحرجة للطبقة 2 إلى العمل بشكل أفضل مع نموذج اشتراك قائم على المدة. في شبكة Nervos ، يمكن تنفيذ هيكل التسعير هذا بسهولة من خلال طريقة الدفع على أساس تكلفة الفرصة البديلة من CKB. يمكن لمقدمي الخدمات تحصيل رسوم على "ودائع" مستخدميهم من خلال NervosDAO. يمكن لمطوري الطبقة الثانية بعد ذلك تركيز النماذج الاقتصادية الرمزية على الحوافز الخاصة بتطبيقاتهم.

بطريقة ما ، نموذج التسعير هذا هو بالضبط كيف يدفع المستخدمون مقابل تخزين على شبكة CKB أيضًا. إنهم يدفعون بشكل أساسي رسوم اشتراك لعمال المناجم من خلال توزيع مكافآت التضخم الخاصة بهم الصادرة عن NervosDAO.

**6. شبكة نيرفوس Nervos**

**6.1 الطبقة الأولى كمخزن للقيمة متعدد الأصول**

نعتقد أنه يجب بناء blockchain من الطبقة الأولى كمخزن للقيمة. لضمان اللامركزية على المدى الطويل ، يجب أن تستند إلى إثبات إجماع العمل pow مع نموذج اقتصادي مصمم على التخزين على الشبكة ، بدلاً من رسوم المعاملات. تعد قاعدة المعرفة المشتركة (CKB) دليلاً على وجود مخزن blockchain قائم على العمل ومتعدد الأصول وقيمته مع كل من البرمجة والنماذج الاقتصادية المصممة.

CKB هي الطبقة الأساسية لشبكة Nervos ، مع أعلى درجات الأمان وأعلى درجة من اللامركزية. يأتي امتلاك الأصول ومعاملاتها على CKB بأعلى تكلفة ، ومع ذلك يوفر تخزين الأصول الأكثر أمانًا ويمكن الوصول إليه في الشبكة ويسمح بأقصى قدر من التوافق. يعتبر CKB هو الأنسب للأصول عالية القيمة والحفاظ على الأصول طويلة الأجل.

قاعدة المعارف المشتركة هي أول blockchain من الطبقة الأولى تم تصميمه خصيصًا لدعم بروتوكولات الطبقة 2:

* تم تصميم CKB لاستكمال بروتوكولات الطبقة 2 ، مع التركيز على الأمان واللامركزية ، بدلاً من تداخل أولويات الطبقة 2 مثل قابلية التوسع.
* يصمم CKB سجل المعاملات الخاص به ، بدلاً من الحسابات. الخلايا هي في الأساس حالة قائمة بذاتها يمكن الرجوع إليها بالمعاملات وتمريرها بين الطبقات. يعد هذا مثاليًا للهندسة ذات الطبقات ، حيث تكون الخلايا المشار إليها والتي يتم تمريرها بين الطبقات عبارة عن أجزاء من الكثلة ، بدلاً من الحسابات.
* تم تصميم CKB كآلة تحقق منفعة العامة ، بدلاً من محرك الحساب. يسمح ذلك لـ CKB بالعمل كمحكمة تتحقق من انتقالات ومعاملات خارج السلسلة.
* يتيح CKB للمطورين إضافة أساسيات تشفير مخصصة بسهولة. هذا يثبت مستقبل CKB ، مما يسمح بالتحقق من البراهين الناتجة عن مجموعة متنوعة من حلول الطبقة 2.

تهدف Common Knowledge Base إلى أن تكون البنية التحتية لتخزين المعرفة المشتركة الأكثر قيمة في العالم ، مع نظام الطبقة 2 الأفضل في فئته والذي يوفر معاملات blockchain الأكثر قابلية للتطوير والأكثر كفاءة.

**6.2 مقياس استخدام حلول الطبقة الثانية**

من خلال هيكلها متعدد الطبقات ، يمكن لشبكة Nervos التوسع في الطبقة 2 لأي عدد من المشاركين ، مع الحفاظ على الخصائص الحيوية للامركزية والحفاظ على الأصول. يمكن لبروتوكولات الطبقة الثانية الاستفادة من أي نوع من التزام الطبقة الأولى ، مما يتيح مرونة كبيرة وإبداعًا في تصميم أنظمة المعاملات لدعم قاعدة مستخدمي الطبقة الثانية المتزايدة. يمكن لمطوري الطبقة الثانية اختيار المقايضات الخاصة بهم فيما يتعلق بنماذج الإنتاجية والنهائية والخصوصية والثقة التي تعمل بشكل أفضل في سياق تطبيقاتهم ومستخدميهم.

في شبكة Nervos ، تُستخدم الطبقة 1 (CKB) للتحقق من الحالة ، بينما تكون الطبقة 2 مسؤولة عن إنشاء الكثل . تعد قنوات الشبكة والسلاسل الجانبية أمثلة لتوليد الشبكة ، ومع ذلك يتم دعم أي نوع من أنماط إنشاء التحقق ، مثل مجموعة توليد إثبات المعرفة الصفرية. تعمل المحافظ أيضًا في الطبقة 2 ، حيث تقوم بتشغيل ، وتولد حالة جديدة وتقدم انتقالات الحالة إلى CKB للتحقق من صحتها. تعتبر المحافظ في شبكة Nervos قوية جدًا ، مع سيطرة كاملة على انتقالات الكثل.

السلاسل الجانبية صديقة للمطورين وتوفر تجربة مستخدم جيدة. ومع ذلك ، فهم يعتمدون على صدق المدققين. إذا تصرف المدققون بشكل ضار ، فإن المستخدمين معرضون لخطر فقدان أصولهم. توفر شبكة Nervos مكدس سلسلة جانبية مفتوح المصدر وسهل الاستخدام لإطلاق سلاسل جانبية على CKB ، والتي تتكون من إطار عمل blockchain Proof-of-Stake يسمى "Muta" وحل سلسلة جانبية يعتمد على ذلك يسمى "محور عصبي".

موتا هو إطار عمل blockchain عالي الأداء وقابل للتخصيص بدرجة كبيرة مصمم لدعم إثبات الحصة وإجماع BFT والعقود الذكية. يتميز بإنتاجية عالية وزمن وصول منخفض إجماع BFT "Overlord" ، ويدعم العديد من الأجهزة الافتراضية بما في ذلك CKB-VM و EVM و WASM. يمكن استخدام أجهزة افتراضية مختلفة في سلسلة واحدة من سلسلة Muta blockchain في وقت واحد ، مع إمكانية التشغيل البيني عبر الأجهزة الافتراضية. يقلل موتا بشكل كبير من حاجز المطورين لبناء بلوكشين عالي الأداء ، مع السماح بأقصى قدر من المرونة لتخصيص بروتوكولاتهم.

Axon هو حل كامل تم إنشاؤه باستخدام Muta لتزويد المطورين بسلسلة جانبية جاهزة على رأس Nervos CKB ، مع أمان عملي ونموذج اقتصادي رمزي. تستخدم حلول Axon CKB لحفظ الأصول بشكل آمن ، واستخدام آلية الحوكمة القائمة على الرمز المميز لإدارة مدققي السلسلة الجانبية. سيتم أيضًا تضمين بروتوكولات عبر السلسلة للتفاعلات بين سلسلة جانبية Axon و CKB ، وكذلك بين سلاسل Axon الجانبية. مع Axon ، يمكن للمطورين التركيز على إنشاء التطبيقات ، بدلاً من بناء البنية التحتية والبروتوكولات عبر السلاسل.

كلا من موتا وأكسون يخضعان حاليًا لتطوير كبير. سنقوم بفتح مصدر الأطر قريبًا ، وستكون RFC لكل من Muta و Axon في الطريق أيضًا.

تعد بروتوكولات الطبقة الثانية مجالًا مزدهرًا للبحث والتطوير. نتوقع مستقبلًا تكون فيه جميع بروتوكولات الطبقة 2 موحدة ومتفاعلة بسلاسة. ومع ذلك ، فإننا نقر بأن حلول الطبقة 2 لا تزال في مرحلة النضج ، وغالبًا ما نواصل دفع حدود ما يمكنهم فعله ، بالإضافة إلى إيجاد المقايضات المقبولة لديهم. لقد رأينا حلولًا واعدة مبكرة ، ولكن لا يزال هناك الكثير من الأبحاث التي يجب إجراؤها حول موضوعات مثل قابلية التشغيل البيني والأمان والنماذج الاقتصادية في تصميمات الطبقة الثانية.

**6.3 الاستدامة**

من أجل الاستدامة على المدى الطويل ، تفرض قاعدة المعارف المشتركة نيرفوس تكلفة على التخزين على السلسلة وتوفر حوافز للمستخدمين لمسح تخزينهم في الشبكة. تحافظ الكثلة المقيدة على متطلبات المشاركة الكاملة للعقدة منخفضة ، مما يضمن إمكانية تشغيل العقد على أجهزة منخفضة التكلفة. تزيد المشاركة القوية الكاملة للعقدة من اللامركزية وبالتالي الأمن.

من خلال فرض تكلفة "إيجار على الشبكة " المتناسبة مع الوقت على تخزين الشبكة ، تخفف قاعدة المعرفة العامة نيرفوس مأساة و المشاكل التي يواجهها العديد من سلاسل الكتل في نموذج "الدفع مرة واحدة ، التخزين إلى الأبد". توفر آلية الإيجار الشبكة هذه ، التي يتم تنفيذها من خلال "التضخم المستهدف" ، تجربة مستخدم سلسة مع فرض تكلفة على تخزين الشبكة.

يمكن استهداف تكلفة ايجار هذه لأن المستخدمين يمتلكون مساحة الإجماع التي تشغلها بياناتهم. يتضمن هذا النموذج أيضًا آلية أصلية للمستخدمين لإزالة حالتهم من مساحة الإجماع. إلى جانب الحوافز الاقتصادية للإيجارات الشبكة، يضمن هذا أن حجم الشبكة سيتحرك دائمًا نحو الحد الأدنى من البيانات المطلوبة من قبل المشاركين في الشبكة.

كما أن الشبكة المملوكة للأفراد تقلل بشكل كبير من تكاليف المطورين. بدلاً من مطالبتهم بشراء CKBytes لمتطلبات الحالة لجميع مستخدميهم ، يتعين على المطورين فقط شراء عدد كافٍ من CKBytes لتخزين رمز التحقق المطلوب بواسطة تطبيقهم. سيستخدم كل مستخدم الخلايا الخاصة به لتخزين الرموز الخاصة به وسيكون مسؤولاً بالكامل عن أصوله.

أخيرًا ، يوفر الإيجار االشبكة و مكافأة مستمرة لعمال المناجم من خلال إصدار رمز جديد. يحفز هذا الدخل المتوقع عمال المناجم على تطوير blockchain ، بدلاً من جمع الكتل المربحة لأخذ رسوم المعاملات.

**6.4 حوافز متوافقة**

تم تصميم النموذج الاقتصادي لقاعدة المعارف المشتركة لمواءمة الحوافز لجميع المشاركين في النظام البيئي.

تم إنشاء Nervos Common Knowledge Base بشكل صريح للحفاظ على القيمة بشكل آمن ، بدلاً من رسوم المعاملات الرخيصة. سيؤدي هذا النموذج الحرج إلى جذب المستخدمين ذوي القيمة ، على غرار مجتمع مستخدمي Bitcoin ، بدلاً من وسيط مستخدمي التبادل.

تميل حالات استخدام التبادل الوسيط إلى دفع شبكة blockchain دائمًا نحو المركزية ، سعياً لتحقيق كفاءة أكبر ورسوم منخفضة. بدون دخل كبير من الرسوم لمشغلي البنية التحتية الذين يؤمنون الشبكة (عمال المناجم أو المدققون) ، يجب تمويل الأمن من خلال التضخم النقدي ، أو ببساطة يعاني من نقص التمويل. يعد التضخم النقدي ضارًا لأصحاب المصلحة على المدى الطويل ، كما أن نقص التمويل الأمني ​​يضر بأي صاحب مصلحة في الشبكة.

ومع ذلك ، فإن مستخدمي متجر القيمة لديهم مطالب قوية لمقاومة الرقابة وأمن الأصول. إنهم يعتمدون على عمال المناجم لتوفير ذلك ، وبدورهم يعوضونهم عن دورهم. في متجر لشبكة القيمة ، يكون لهذه الأطراف مصالح متوائمة.

من خلال مواءمة حوافز جميع المشاركين ، يمكن لمجتمع Nervos الموحد أن ينمو ، ومن المتوقع أيضًا أن يكون النظام الاقتصادي المتوافق للشبكة مقاومًا لكل التحديات.

**6.5 التقاط وتوليد القيمة**

لكي تظل أي blockchain آمنة مع زيادة قيمة الأصول التي يتم تأمينها بواسطة النظام الأساسي ، يجب أن يكون لدى النظام آلية لالتقاط القيمة مع نمو قيمة الأصول المضمونة. من خلال الشبكة المقيدة ، يجعل CKB مساحة التخزين موردًا نادرًا وبأسعار السوق. مع زيادة الطلب على تخزين الأصول على الشبكة ، من المتوقع أن يقوم النظام بتعويض عمال المناجم بشكل أفضل عن تأمين هذه الأصول.

كمنصة للحفاظ على القيمة ، يتم تحديد القيمة الجوهرية لـ CKB كمنصة من خلال مقدار الضمان الذي يوفره للأصول التي يحتفظ بها. مع ارتفاع قيمة الأصول المضمونة ، فإن آلية الحصول على القيمة للنموذج الاقتصادي CKB قادرة تلقائيًا على رفع ميزانية أمان CKB لجذب المزيد من موارد التعدين ، مما يجعل النظام الأساسي أكثر أمانًا. هذا ليس مهمًا فقط لجعل النظام الأساسي مستدامًا ، ولكنه يوفر أيضًا مسارًا للنمو للقيمة الجوهرية للمنصة - نظرًا لأن النظام الأساسي يصبح أكثر أمانًا ، فإنه يصبح أيضًا أكثر جاذبية للأصول ذات القيمة الأعلى ، مما يؤدي إلى زيادة الطلب. من الواضح أن هذا مرتبط بالقيمة الإجمالية الإجمالية التي ستنتقل في النهاية إلى مساحة blockchain.

مع مرور الوقت ، نتوقع أن يزداد الطلب على لـ CKB. سيتم استخدام CKBytes لتخزين الأصول عالية القيمة والأصول منخفضة القيمة ستنتقل إلى blockchain المتصلة بـ CKB ، مثل السلاسل الجانبية للطبقة 2. بدلاً من تأمين الأصول بشكل مباشر ، يمكن استخدام CKB كجذر ثقة لتأمين النظام البيئي لسلسلة جانبية كاملة من خلال ، على سبيل المثال ، بضع مئات من البايتات ، مما يدعم منحنى الطلب على مساحة التخزين: على غرار قطعة صغيرة من الأرض تزيد كثافتها الاقتصادية بشكل كبير من خلال دعم ناطحة سحاب.

أخيرًا ، من خلال تصميم NervosDAO ووظيفة "مأوى التضخم" ، سيحتفظ حاملو الرموز طويلة الأجل دائمًا بنسبة مئوية ثابتة من إجمالي الإصدار ، مما يجعل الرمز الأصلي نفسه مخزنًا قويًا للقيمة.

**6.6 سد الفجوة التنظيمية**

تسمح سلاسل الكتل غير المسموح بها باللامركزية الكاملة في إصدار الأصول والمعاملات. هذا ما يجعلها ذات قيمة ، ولكنها أيضًا سبب عدم توافقها مع الأنظمة المالية والقضائية في العالم الحقيقي.

يوفر ظهور بنية متعددة الطبقات الفرصة لإنشاء أجزاء متوافقة مع التنظيمات من blockchain غير منظم وغير مصرح به. على سبيل المثال ، يمكن للمستخدمين تخزين أصولهم اللامركزية على الطبقة 1 ، والتمتع بالملكية المطلقة لهذه الأصول ، ويمكنهم أيضًا معالجة الأعمال التجارية الواقعية على الطبقة 2 ، حيث يخضعون لقيود تنظيمية وقانونية.

خذ على سبيل المثال بورصات العملات المشفرة - أصدرت دول مثل اليابان وسنغافورة تراخيص للتبادلات وأنشأت متطلبات تنظيمية. يمكن لبورصة متوافقة أو فرع من بورصة عالمية بناء سلسلة تجارية من الطبقة الثانية ، واستيراد هويات المستخدمين وأصولهم ، ومن ثم إجراء الأعمال القانونية وفقًا للمتطلبات التنظيمية المحلية.

أصبح إصدار ومعاملات الأصول في العالم الحقيقي ممكنًا في إطار بناء blockchain متعدد الطبقات. يمكن أن تتدفق الأصول في العالم الحقيقي إلى النظام الإيكولوجي blockchain من خلال سلسلة جانبية منظمة من الطبقة 2 إلى blockchain من الطبقة الأولى غير المرخصة ، مما يسمح لهذه الأصول بالوصول إلى أكبر نظام بيئي للخدمات المالية القابلة للتكوين واللامركزية.

في المستقبل ، من المتوقع أن تستخدم شبكة نيرفوس أيضًا سلاسل وتطبيقات من الطبقة الثانية كأساس لاعتماد المستخدمين على نطاق واسع ، بالتعاون مع الشركات الرائدة في هذا المجال.

**مراجع**

[1] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". 31 Oct 2008, <https://bitcoin.org/bitcoin.pdf>

[2] Vitalik Buterin. "Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform". Nov 2013 <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>

[3] With an average Bitcoin transaction size of 250 bytes: (2 \* 250 \* 7,500,000,000) / (24 \* 6) = 26,041,666,666 byte blocks (every 10 minutes); 26,041,666,666 \* (24 \* 6) = 3,750,000,000,000 bytes (blockchain growth each day); 3,750,000,000,000 \* 365.25 = 1,369,687,500,000,000 bytes (blockchain growth each year)

[4] Gur Huberman, Jacob Leshno, Ciamac C. Moallemi. "Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System". Bank of Finland Research Discussion Paper No. 27/2017. 6 Sep 2017, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3032375>

[5] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, Arvind Narayanan. "On the Instabiliity of Bitcoin Without the Block Reward". Oct 2016, <https://www.cs.princeton.edu/~smattw/CKWN-CCS16.pdf>

[6] Lewis Gudgeon, Perdo Moreno-Sanchez, Stefanie Roos, Patrick McCorry, Arthur Gervais. "SoK: Off The Chain Transactions". 17 Apr 2019, <https://eprint.iacr.org/2019/360.pdf>

[7] Joseph Poon, Vitalik Buterin. "Plasma: Scalable Autonomous Smart Contracts". 11 Aug 2017, <https://plasma.io/plasma.pdf>

[8] Vitalik Buterin. "On-chain scaling to potentially ~500 tx/sec through mass tx validation". 22 Sep 2018, <https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477>