إتفاق سايتو: إصلاح إخفاقات السوق في البيتكوين

ديفيد لانكشاير وريتشارد باريس

٢٤ ديسمبر/ كانون الأول ٢٠٢٠
الإصدار ٤.٠.١

ترجمة فيصل الرميحي

نبذة مختصرة

تعمل سايتو على إصلاح مشكلات العمل الجماعي التي تعيق التوسع في سلاسل الكتل (Blockchains) لإثبات العمل (Proof of work) وإثبات الحصة (Proof of stake) من خلال ربط دفتر الحسابات الدوري (Circular ledger) بآلية اتفاق (Consensus) تحفز تحصيل رسوم المعاملات وتقاسمها. ستدفع الشبكة الناتجة ليس فقط للتعدين (Miners) والتخزين الاستثماري (Staking)، ولكن لجميع الأنشطة التي تساهم بقيمة اقتصادية للشبكة. في هذه العملية، تقضي سايتو بشكل كامل على نظام الأغلبية من بين الهجمات الأخرى.

تدفع سايتو عقد البنية التحتية (Infrastructure nodes) التي تواجه المستخدم من خلال آلية اتفاق مفتوحة. ونظرًا لأن هذا النهج يتوسع بشكل طبيعي، فإنه يحفّز معالجة كميات كبيرة من البيانات ويمكن استخدامه لبناء إصدارات لامركزية من العديد من الخدمات كثيفة البيانات. على سبيل المثال، عمليات تبادل البيانات غير القابلة للتسويق وتطبيقات المصادقة وتحقيق الدخل والسجلات الرئيسية الموزعة الآمنة من هجمات الوسطاء (MITM) وقنوات الدفع وغيرها.

من الناحية الاقتصادية، يمكن فهم سايتو على أنها حل لخلق اسواق حرة تقدم منفعة عامة. يصحح التصميم مشاكل العمل الجماعي المتأصلة في آليات إثبات العمل وإثبات الحصة، بحيث يتنافس الأشخاص الساعون للربح لجلب الأموال إلى الشبكة مما يسمح بقابلية التوسع (Scalability) إلى الحد الذي تكون فيه أجهزة الشبكة الأساسية هي التي تفرض قيودًا على نمو سلسلة الكتل بدلاً من القيود الاقتصادية. نعتقد أن الحد العملي لسلسلة كتل سايتو اليوم هو في حدود ١٠٠ تيرابايت من البيانات في اليوم الواحد، وسوف يدفعنا التقدم في سعة التوجيه إلى مستوى البيتابايت في غضون عشر سنوات من الآن.

يصف القسم التالي بإيجاز المشكلات الاقتصادية التي يجب حلها من أجل بناء سلسلة كتل قابلة للتطوير و التوسع. توضح الأقسام التالية كيف تحل سايتو هذه المشكلات وتصف تنفيذ هذه الأساليب.

١. المشكلة

لا تكمن مشكلة توسيع نطاق سلسلة الكتل في طبقة تقنية الشبكة: حيث أنه في وقت كتابة هذا التقرير، كانت مراكز البيانات في جميع أنحاء العالم تنفذ محولات شبكة ٤٠٠ جيجابت في الثانية بينما أصبحت اتصالات الـ ١٠٠ جيجابت في الثانية قياسية حتى في مرافق تحديد المواقع ذات المستوى الأدنى. إذا كانت لدينا الموارد الكافية لدفع ثمن المعدات اللازمة، فلا يوجد ما يمنعنا من الناحية الفنية من بناء سلسلة كتل لا مركزية ومفتوحة لتكون مثل العمود الفقري للإنترنت.

ما يحد من نمو الشبكة هو التحدي المتمثل في دفع المال الكافي للشبكة. في الماضي، تخلص غير الاقتصاديين من هذا القيد، وذلك بزعمهم أنه طالما أن شخصًا ما يكسب المال من الشبكة، فسوف يدفع جميع التكاليف اللازمة لدعمها. لكن هذا ليس صحيحًا، نظرًا لأن شبكات إثبات العمل وإثبات الحصة تعانيان من إخفاق كبير في السوق وهما: مأساة المشاع (Tragedy-of-the commons) والتي تؤدي إلى تضخم سلسلة الكتل ثم انهيارها ومشكلة الراكب المجاني (Free-rider) التي تؤدي إلى نقص في البنية التحتية للشبكة التي تواجه المستخدم والإفراط في توفير الأنشطة المدفوعة مثل التعدين والتخزين. لا تسبب تلك المشاكل إعاقة كبيرة عندما تكون الشبكة على نطاق صغير، لكنهما تسببان إعاقة كبيرة عندما يزداد سعر تكلفة الشبكة وسعة التخزين الاستثماري.

هل توجد بدائل أخرى؟ في مواجهة الحاجة إلى الدفع مقابل البنية التحتية للشبكة غير المدفوعة، يطرح علماء الكمبيوتر هذه المشكلة في السوق. كما يعرف الاقتصاديون منذ فترة الستينيات، فإن مطالبة القطاع الخاص بتمويل البنية التحتية الغير القابلة للاستبعاد تتطلب أن تغلق في مكان ما في النموذج الاقتصادي. يجب بالضرورة على الشركات ان تدفع مقابل تحصيل الرسوم وإغلاق الوصول إلى الرسوم التي تتلقاها. يؤدي التدفق المتحكم في الأموال داخل سلسلة الكتل إلى تقويض انفتاح طبقة الإتفاق (Consensus layer).

الحل الوحيد القابل للتطبيق هو القضاء على إخفاقات السوق هذه على مستوى الحوافز (Incentive level). وقبل فهم الحل، يجب رؤيته بوضوح. القضايا الرئيسية لهذا الحل هي:

تنشأ مشكلة مأساة المشاع من وجود دفتر الحسابات الدائم (Permanent ledger)، والذي يشجع العُقَد على قبول الدفع اليوم مقابل العمل الذي يمكن تفريغه للآخرين غدًا. يؤدي هذا إلى تضخم سلسلة الكتل وإلى سوء تسعير المعاملات، حيث يمكن للمستخدمين دفع رسوم لا تعكس التكلفة الحقيقية لمعاملاتهم للشبكة ككل. حقيقة إن هذه مشكلة أساسية وقد توقف نهج ساتوشي "بعدم الاهتمام" عن كونه قابلاً للتطبيق في الشبكات التي تعمل على نطاق اقتصادي واسع.

يتطلب القضاء على مشكلة مأساة المشاع أن تتحمل جميع العُقَد التي تضيف معاملات إلى سلسلة الكتل تكلفة معالجة هذه المعاملات طالما أنها تظل على سلسلة الكتل. من الناحية العملية، يتطلب هذا آلية السوق لتحديد سعر تخزين البيانات على السلسلة بدقة. كما يتطلب أيضًا القضاء على زحف سلسلة الكتل أو تأجيل تحصيل الرسوم بحيث يتم سداد المدفوعات بمرور الوقت حيث تستمر العُقَدة في القيام بالعمل المطلوب للدفع. تم شرح حلنا لهذه المشكلة في القسم ٢.

أما بالنسبة لمشكلة الراكب المجاني فهي أصعب قليلا. فهي تنشأ في سلاسل الكتل حيث يتم الدفع مقابل نوع معين من العمل (مثل التعدين والتخزين الاستثماري) على حساب الأنشطة الضرورية الأخرى. يحفز عدم التوافق هذا المشاركين على إنفاق المزيد على تلك الأعمال وتقليل الإنفاق على غيره من الأشياء. في فضاء سلسلة الكتل ، ينتج عن هذا "حرية وصول وركوب مجاني" للمعدّنين والمستثمرين عبر التخزين لأولئك الذين يقومون بالعمل غير المدفوع الأجر المتمثل في تحصيل الرسوم أو تطوير التطبيقات أو دعم الشبكة التي تواجه المستخدم. تزداد المشكلة مع توسع الشبكة مما يجعل الفخ أمرًا لا مفر منه: أي مُعدّن بيتكوين ينفق نسبة أقل من إيراداته على التجزئة (Hashing) من نظرائه الأكثر إيثارًا (Altruistic peers) سيفقد حصته في السوق حتى يستسلم أيضًا.

في الاقتصاد، يتمثل الحل النموذجي لمشكلة الراكب المجاني في القضاء على خاصية "عدم الاستبعاد" المرتبطة بأي سلعة أو خدمة: أي قصر فوائدها على أولئك الذين يدفعون تكاليفها. في فضاء سلسلة الكتل، من المستحيل القيام بذلك دون تدمير انفتاح الشبكة. غالبًا ما يعالج علماء الكمبيوتر المشكلة عن طريق إضافة برمجيات وسيطة وقائية ، مثل احاطة مدفوعات الإتفاق (Consensus payments) بحلقات تصويت مغلقة والتي تكون بدورها عرضة لهذه الهجمات أيضا. لا تستطيع لعبة jiggery-pokery هذه أن تحل هذه المشاكل الاقتصادية أبدًا: فالأسواق قوية بما يكفي لتقويض هذه الهياكل لأنها تحفزها بالأساس.

بدون حلنا لهذه المشكلة، تنحصر الخيارات بين شبكة لا يمكنها التوسع لأنها لا تستطيع الدفع مقابل عمليات الشبكة، أو شبكة تتوسع ولكنها تفقد الانفتاح وعدم الثقة والاكتفاء الذاتي الاقتصادي الذي يجعل تقنية سلاسل الكتل في الأساس اختراعًا مفيدًا. لا يعتبر أي من النهجين مفيدًا لبناء سلاسل كتل منفتحة على نطاق واسع.

يتطلب الحل النظري لمشكلة الراكب المجاني القضاء على إمكانية الانتفاع المجاني: وذلك بإصلاح هيكل الحوافز الأساسي بحيث يتم الدفع للمشاركين مقابل توفير ما تحتاجه الشبكة بالفعل. نظرًا لأن سلاسل الكتل تتطلب تكلفة هجوم قابلة للقياس الكمي ، فإن هذا يتطلب القضاء على "التعدين " و "التخزين الاستثماري" والتحول إلى شكل مختلف من العمل يقيس العُقَد ويدفعها بما يتناسب مع "القيمة" التي توفرها للشبكة بدلاً من مبلغ التجزئة أو التخزين الاستثماري التي يقومون بها.

هذا يتطلب منّا إيجاد طريقة جديدة لقياس القيمة ثم دفع العُقَد بما يتناسب مع مقدار المساهمة التي تساهم بها. يتطلب تحقيق ذلك استنباط مقياسنا "للعمل" من رسوم المعاملات التي يدفعها المستخدمون. إن توجيه رسوم المعاملات إلى الشبكة هو العمل الذي يجب أن تشجعه شبكتنا. يمكن حث العُقَد الصادقة (Honest nodes) على القيام بهذا العمل بحصة من الرسوم المحصلة. تصبح صعوبة في هذا الحال، هي إيجاد كيفية ضمان أن هذه الآلية تحافظ على خصائص تكلفة الهجوم، بحيث لا يتمكن المهاجمون من إنفاق أموالهم لمهاجمة الشبكة، واستعادتها مرة أخرى في حلقة مفرغة. تحدد آلية الأمان الموضحة في القسم ٣ طريقة تقنية لإنجاز ذلك.

٢. إصلاح مشكلة مأساة المشاع (Tragedy-of-the commons)

تعمل سايتو على حل مشكلة زحف سلسلة الكتل عن طريق السماح للعُقد في الشبكة بحذف أقدم الكتل (Blocks) في دفتر الحسابات على فترات زمنية يمكن التنبؤ بها. طول الفترة محدد في قوانين الإتفاق. الحالة القصوى - سلسلة الكتل مصممة للتعامل مع حركة المرور العالمية لتطبيقات تبادل المفاتيح الموزعة - قد يكون لها فترة قصيرة تصل فقط إلى ٢٤ ساعة.

كما تعمل سايتو على تحديد التالي: أنه بمجرد خروج الكتلة من الفترة الحالية، لم تعد مخرجات المعاملات غير المنفقة (UTXO) قابلة للإنفاق. ولكن يجب إعادة تضمين أي UTXO من تلك المجموعة التي تحتوي على ما يكفي من الرموز لدفع رسوم إعادة البث في الكتلة التالية. يقوم منتجي الكتل بذلك عن طريق إنشاء معاملات "إعادة البث التلقائي للمعاملات" (ATR) التي تتضمن بيانات المعاملة الأصلية، ولكن لديها UTXO جديدة تمامًا وقابلة للإنفاق. بعد فترتين ، يمكن لمنتجي الكتل حذف جميع بيانات الكتلة، على الرغم من أنه قد يتم الاحتفاظ بتجزئة الرأس المكونة من ٣٢ بايت لإثبات الاتصال مع كتلة التكوين الأصلية.

تعمل آلية "إعادة البث التلقائي للمعاملات" ATR على إصلاح مشكلة مأساة المشاع بشكل كامل، مما يجعل من المستحيل أن

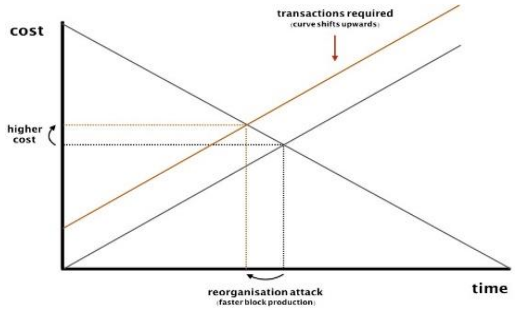
تنمو سلسلة كتل بشكل كبير بحيث تصل لحد الانهيار. المفتاح هو التأكد من أن "رسوم إعادة البث" التي تدفعها معاملات ATR"إعادة البث التلقائي للمعاملات" هي مضاعف إيجابي لمتوسط الرسوم المدفوعة من خلال المعاملات الجديدة على مدار الفترة السابقة. مع توسع سلسلة الكتلة ووجود مساحة أقل للمعاملات الجديدة المتاحة، تؤدي المنافسة في السوق إلى زيادة الرسوم المدفوعة من المعاملات الجديدة. يؤدي هذا إلى زيادة الرسوم المدفوعة من المعاملات القديمة ويزيد من كمية البيانات التي يتم ترتيبها بواسطة سلسلة الكتلة. ويصل السوق إلى حالة توازن حيث تتم إزالة البيانات القديمة من السلسلة بنفس وتيرة إضافة البيانات الجديدة.

إن اكتشاف السوق للتكلفة الحقيقية لمعالجة سلسلة الكتلة هو أحد الآثار الجانبية لهيكل الحوافز هذا، والذي يعمل من خلال القضاء على الحوافز التي يتعين على منتجي الكتل المحفزة الذين يضيفون بيانات غير مربحة إلى السلسلة. تتجنب هذه الآلية المشاكل مع المطورين الذين يقومون بتشفير المتغيرات الاقتصادية وتمنع أي أشكال خفية للركوب المجاني والتي توجد عادة في سلاسل أخرى (حذف البيانات على السلسلة، ورفض تخزين أو مشاركة الكتل التاريخية) حيث يتم الحذف بهدف توفير المال. تختفي جميع أشكال الغش هذه لأن العُقَد التي لا تخزن سلسلة الكتلة بالكامل غير قادرة على إنتاج كتل جديدة، لأنها لا تعرف المدفوعات التي يجب إعادة بثها.

في حين أن هذا من شأنه أن يجنبنا مشكلة نمو سلسلة الكتل الخاص بنا بشكل كبير جدًا بحيث يكون من الصعب على عقد الشبكة تخزينه، فهو أيضا يضمن إمكانية تسعير المساحة على سلسلة الكتل بشكل دقيق للغاية حتى مع اقتراب أوقات التخزين إلى الما لا نهاية، مما يساعد على إصلاح مأساة المشاعات. لا يحصل على أموال للعقد الموجودة في شبكة نظير إلى نظير التي تدفع مقابل جميع الأنشطة المتنوعة التي تحافظ على عمل الشبكة. وللتمكن من حل هذه المشكلة، فإننا نحتاج إلى آلية توافق جديدة.

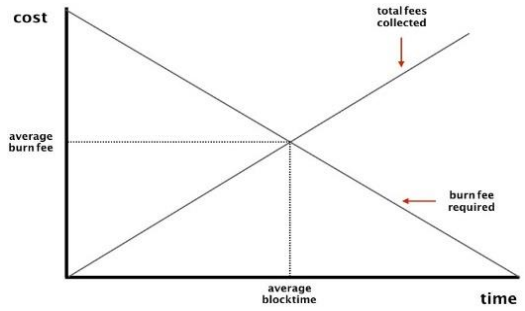
٣. القضاء على الراكب المجاني(Free-rider)

في سايتو، يمكن لأي عقدة إنشاء كتلة في أي وقت بشرط أن يكون لديها ما يكفي من "عمل التوجيه" (Routing work) في مجموعة الذاكرة الخاصة بها. يعتمد مقدار "عمل التوجيه" المطلوب لإنتاج كتلة على مدى سرعة اتباع الكتلة لسابقتها: تزيد قواعد الاتفاق من القيمة فور العثور على الكتلة وتبدأ في إنقاصها تدريجيًا حتى تصل إلى الصفر. نظرًا لأن منتجي الكتل سيصدرون الكتل بمجرد أن تصبح مربحة، يتم تحديد وتيرة إنتاج الكتلة من خلال المقدار الإجمالي لـ "عمل التوجيه" الذي تولده الشبكة.



الشكل ١: منحنى رسوم الحرق

يستمد سايتو عمل التوجيه من رسوم المعاملة المدمجة في كل معاملة. إن استخدام مقياس العمل هذا لإنتاج الكتل يجعل مهاجمة الشبكة أمر مكلف للغاية، لأن تقديم مطالبات حول الوقت تكلف أموالًا كثيرة. يمكن أن نرى من الشكل ٢ أنه من المستحيل على المهاجمين إنتاج كتل بوتيرة أسرع من السلسلة الرئيسية ما لم يكن لديهم وصول إلى مجموعة أكبر من رسوم المعاملات.



الشكل ٢: تكلفة رسوم الحرق للمثل

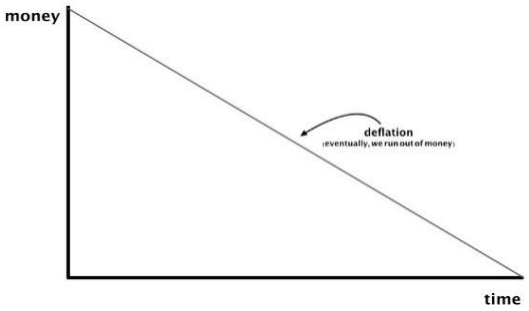
لتأمين تلك الآلية، تمتلك سايتو عقد توجيه (Routing nodes) تقوم بتوقيع المعاملات بشكل مشفّر أثناء انتشارها عبر الشبكة. تحدد قواعد الاتفاق أن مقدار "عمل التوجيه" الذي توفره المعاملة لأي عقدة يسقط مع عدد القفزات في مسار التوجيه الخاص بها، وأن المعاملات لا توفر أي عمل توجيه قابل للاستخدام للعقد التي ليست في مسار التوجيه (Routing path) الخاص بها. العمل المستخدم لإنتاج الكتل هو الجمع والمشاركة الفعّالة لرسوم الشبكة الواردة.

طالما لا يوجد دفع مقابل إنتاج الكتلة، فإن هذا النظام يوفر أمانًا مشابهًا لعملة البيتكوين: يمكن دائمًا تحديد تكلفة الهجوم ويجب على المهاجمين إنفاق أموالهم الخاصة لمهاجمة السلسلة. يتيح ذلك للمستخدمين الانتظار بالرغم من الحاجة إلى العديد من التأكيدات لتلبية متطلبات الأمان الخاصة بهم. على سبيل

[١] العديد من المشاكل الأساسية المتعلقة بآليات إثبات العمل وإثبات الحصة تنبع من هذا القرار. وبغض النظر عن هجوم واحد وخمسين بالمائة (the fifty-one percent attack)، لاحظ الطريقة التي يتم بها استخدام قيود جانب العرض في الأسواق الخارجية (أي منحنى العرض غير المرن لقوة التجزئة أو رأس المال) لفرض "قيود التكلفة" على المهاجمين. لا يزيل هذا التصميم فقط أي قدرة لسلسلة الكتل على تنظيم أمانها الخاص، ولكن الأرباح المتاحة في الأسواق الخارجية تؤدي بالضرورة وبشكل حتمي إلى سلعة وظيفة العمل وتسطيح منحنى العرض للعمل في السوق الخارجية.

المكافأة، يمكن للشبكة زيادة مقدار "عمل التوجيه" اللازم لإنتاج الكتلة للحفاظ على وقت الكتلة (Block time) ثابتًا مع نمو حجم المعاملات، بحيث يتناسب الأمان مع حجم الرسوم.

تكمن المشكلة الرئيسية في هذا النهج في عواقب مطالبة الشبكة بحرق رأس المال لإنتاج الكتل:



الشكل ٣: انكماش رسوم الحرق بمرور الوقت

يتطلب تجنب الانهيار الانكماشي إعادة الرموز المميزة (Tokens) إلى شبكتنا. لكن سايتو لا يمكنه ببساطة منح الرسوم مباشرة لمنتجي الكتل: من شأن ذلك أن يسمح للمهاجمين باستخدام الدخل من كتلة واحدة لتوليد أعمال التوجيه اللازمة لإنتاج الكتلة التالية. يُفضل تقسيم المدفوعات بين العُقَد المختلفة، ولكن طالما أن منتجي الكتل لديهم أي تأثير على من يحصل على الرسوم، يمكن للمهاجم المتمرس أن يتعامل مع الشبكة أو ينفذ هجمات طاحنة تستهدف آلية إصدار الرمز المميز (Token-issuing).

يتطلب حل هذه المشكلة قلب الحل الكلاسيكي لإثبات العمل. في البيتكوين، تجعل قواعد الاتفاق إنتاج الكتل أمرًا مكلفًا للغاية، حيث يتم تسليم الرسوم إلى منتج الكتلة. ويهدف هذا إلى ضمان أن يكون إنتاج الكتل أمرًا مكلفًا ولكن في الواقع يضمن أن هناك دائمًا ظروفًا تكون الهجمات في ظلها مربحة.[1] في سايتو يكون الحل هو عكس ذلك تمامًا. حيث تكون المشكلة الرئيسية في تأمين آلية الدفع: ضمان أن تكون المدفوعات متناسبة مع العمل بغض النظر عمن ينتج الكتل. يتم بعد ذلك الاستفادة من تكلفة الهجوم التي تنشئها آلية بهذه الخاصية لتصبح تكلفة إنتاج الكتلة.

نطلق على الآلية التي تحقق ذلك "التذكرة الذهبية". تدفع هذه الآلية العقد الصادقة بسبب تحصيلهم على الرسوم بغض النظر عمن ينتج الكتل. الحيلة هي سحب هذا بطريقة تضمن دائمًا وجود تكلفة قابلة للقياس الكمي لمهاجمة النظام. الحل العملي هو إعادة المعاملات إلى الشبكة من خلال عملية لا يمكن لأي لاعب في الشبكة التلاعب بها دون إنفاق أموال على الهجوم أكثر بكثير مما يمكنهم الاستفادة من تحصيل المدفوعات. يتم وصف تفاصيل التنفيذ في القسم التالي.

٤. التذكرة الذهبية (Golden Ticket)

عندما تقوم أحد العُقَد بإنتاج كتلة، فإنها قد تجمع الفرق بين مقدار "عمل التوجيه" المتضمن في كتلتها ومقدار عمل التوجيه المطلوب لإنتاج الكتلة. لم يتم إجراء أي مدفوعات أخرى.

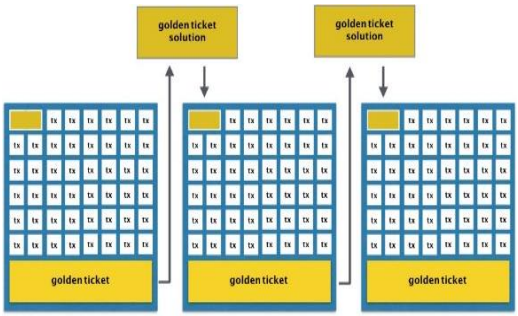
يتطلب فتح هذه المدفوعات أن تحل الشبكة لغزًا حسابيًا نسميه "التذكرة الذهبية" (Golden ticket). يتطلب هذا اللغز معرفة عملية تجزئة الكتلة، لكي نتمكن من حلها ولا يمكن حسابها بشكل مسبق. يشاهد المعدّنين على الشبكة الكتل أثناء إنتاجها ويبدأون عملية تجزئة الكتلة بحثًا عن حل. وفي حال تمكنوا من إيجاد المعاملة، فإنهم يقوموا بنشرها مرة أخرى في الشبكة كمعاملة عادية لدفع الرسوم.

من الممكن تضمين حل واحد فقط في أي كتلة، كما يجب كذلك تضمين هذا الحل في الكتلة التالية حتى يتم اعتباره صالحًا. إذا تم انتهاك هذه الشروط أو إذا لم يتم حل "التذكرة الذهبية"، فبكل بساطة، لن يتم تخصيص الأموال التي لم يتم دفعها في الكتلة السابقة. يتراجعون إلى الخلف في سلسلة الكتل ويسقطون من السلسلة في النهاية، وعند هذه النقطة يتم إعادة جمع الأموال المفقودة من خلال طبقة الإتفاق (Consensus layer). وإعادة توزيعها في النهاية كجزء من المكافأة المستقبلية للكتلة.

في حالة العثور على حل في الوقت المناسب، يتم تحرير الرسوم غير المخصصة للشبكة؛ وينقسم بين الشخص الذي وجد الحل عن طريق التعدين، وبين عُقَدة عشوائية في شبكة التوجيه من نظير إلى نظير (Peer-to-peer routing network). يتم تحديد عقدة التوجيه المحظوظة باستخدام متغير عشوائي مصدره حل الشخص الذي يقوم بعملية التعدين، مع جعل فرصة كل عقدة توجيه للفوز طبيعية لتكون متناسبة مع "عمل التوجيه" (Routing work) العام الذي ساهمت به في حل الكتلة.

عندما يتم توجيه المعاملات إلى الشبكة، يمكن ملاحظة أن إجمالي المطالبات المتعلقة بالدفع المضمنة فيها (مجموع عمل التوجيه المتاح لجميع العُقَد في مسار التوجيه) ينمو بينما حجم العمل المتاح لإنتاج كتلة (مقدار عمل التوجيه المتاح لعقد محددة) يتناقص. المهاجمون الذين يستخدمون المعاملات الصادقة لإنتاج الكتل يضعون أنفسهم في مأزق دفع الفرق.

نطلق على عملية تقسيم الدفع بين من يقومون بعملية التعدين والموجّهين (Routing nodes)، اسم "paysplit" للشبكة. تم ضبطه على ٠.٥ افتراضيًا (النصف لمن يقومون بعملية التعدين، والنصف الآخر إلى أجهزة التوجيه) ولكن يمكن تعديله كما هو موضح في القسم أدناه. يمكن تصور نظام التذكرة الذهبية على النحو التالي:



الشكل ٤ : نظام التذكرة الذهبية

يتمتع هذا النظام بالعديد من المزايا الرئيسية على آليات إثبات العمل وإثبات الحصة. الأهم من ذلك، هو أن سايتو يوزع صراحة الرسوم على العُقَد التي تخدم المستخدمين، وتجمع المعاملات وتنتج الكتل، وتقوم بذلك بما يتناسب مع القيمة التي تقدمها هذه الجهات الفاعلة للشبكة ككل. تتنافس عقد الشبكة للوصول إلى تدفق المعاملات المربح إلى الداخل، وسيسعد بتمويل أي أنشطة تطويرية لازمة لجذب المستخدمين إلى الشبكة. وتجدر الإشارة إلى أن الخدمات التي تقدمها العُقَد الطرفية لجذب استخدام سايتو يمكن أن تشمل البنية التحتية العامة التي تحتاجها سلاسل الكتل الأخرى.

هذا من شأنه أن يعتبر تحولاً أساسياً. عندما تحدد سلاسل الكتل الأخرى بشكل صريح الأنشطة التي لها قيمة، يتيح سايتو للمستخدمين الإشارة إلى الخدمات التي توفر القيمة من خلال تسعير الرسوم، بينما تحدد الشبكة من يستحق الدفع. يحفّز سايتو أيضًا تقديم القيمة بشكل فعّال للمستخدمين. ومن خلال الدفع مقابل القيمة بدلاً من مجموعة فرعية من أنشطة الشبكة، فإنه يوفر الطريقة الوحيدة لضمان أن تظل شبكة الاكتفاء الذاتي مفتوحة ومستقلة اقتصاديًا على نطاق واسع.

آلية اتفاق سايتو هي أيضًا "آمنة مرتين" أكثر من إثبات العمل وإثبات الحصة. تقوم العُقَد الصادقة بتوجيه المعاملات إلى منتجين الكتل وتكسب الرسوم في المقابل. لكن المهاجمين يقعون في شباك فخ ٢٢ (Catch-22): لا يجب عليهم فقط إنفاق نفس القدر من الرسوم مثل الشبكة الصادقة لإنتاج سلسلة تنافسية، ولكن يجب أيضًا مطابقة مئة بالمئة من ناتج التعدين للعثور على حلول تذاكر ذهبية كافية لاستعادة أموالهم. حتى إذا نجح المهاجمون في شن هجمات لإعادة تدوير الرسوم ، فلا يزال يتعين عليهم إنفاق مئة بالمئة من دخلهم على عملية التجزئة (Hashing).

يحقق الإصدار الأساسي من نظام سايتو أمانًا للرسوم بنسبة مئة بالمئة، مما يقضي على هجوم واحد وخمسين بالمئة تمامًا. يصف القسم ٥ تعديلاً على هذه الآلية يزيد من مستوى الأمان إلى أكثر من مئة بالمئة ويضمن أن المهاجمين يخسرون الأموال في جميع الأحوال. بغض النظر عن التطبيق المستخدم، تختفي المشاكل الاقتصادية الناتجة عن الآليات التي تعتمد على منحنيات العرض الخارجية: يعمل التعدين كدالة تكلفة خالصة بدلاً من وظيفة صعوبة وتظل سلسلة الكتل آمنًا حتى إذا أصبح منحنى العرض لقوة التجزئة (Hash power) مسطحًا بشكل كامل.

٥.الأمن المتقدم لـ POWSPLIT

من الممكن زيادة تكاليف الهجوم بما يتجاوز مئة بالمئة من العائدات المتاحة من خلال آلية "powsplit". لاحظ أنه في تطبيق سايتو العادي مع شريحة دفع ثابتة (Paysplit) تبلغ ٠.٥، تقوم الشبكة تلقائيًا بضبط صعوبة التعدين بحيث يتم العثور على حل واحد لكل كتلة، في المتوسط. نظرًا لأن المعدّنين لا يمكنهم التحكم في التباين الذي يتم العثور على الحلول فيه، فقد ينتهي الأمر بصعوبة الشبكة إلى أن تكون أقل في المتوسط من المطلوب لتحقيق الأمان الأمثل.

آلية "powsplit" من شأنها القضاء على تلك المشكلة عن طريق تعديل صعوبة عملية التعدين بحيث يتم العثور على حل واحد في كل عدد "ن" من الكتل (N- blocks) في المتوسط. عندما يتم تضمين مثل هذا الحل في سلسلة الكتل، إذا لم تحتوي الكتلة السابقة على تذكرة ذهبية، يتم تجزئة المتغير العشوائي (Random variable hashing) المستخدم لاختيار عقدة التوجيه الفائزة (Winning routing nodes) مرة أخرى لتحديد فائز من الكتلة التي لم يتم حلها والتي سبقتها أو من جدول المحتفظين بالأموال لدعم المشروع (Table of stakers) كما هو موضح أدناه. يمكن تطبيق حد أعلى للتكرار العكسي لأغراض عملية، نظرًا لأن سلسلة الكتل الدائري سوف تستعيد أي أموال لم يتم دفعها.

لكي يصبح المستخدمون أحد مستثمري التخزين (Stakers) في الشبكة، يبث المستخدمون معاملة تحتوي على UTXO منسق بشكل خاص. تتم إضافة تلك الـ UTXO إلى قائمة "مستثمرين التخزين المعلقين" (Pending stakers list) عند إدراجها في الكتلة. بمجرد دفع جدول مستثمرين التخزين الحالي (Current staking table) بالكامل، يتم نقل جميع UTXO المعلق إلى جدول الاحتفاظ بالأموال الحالي. لتجنب الهجمات الخانقة على آلية التخزين، من الحكمة أن نمنع مستثمرين التخزين من الانسحاب أو إنفاق UTXO حتى يتلقوا الدفع.

يجب أن تكون النسبة المئوية لإيرادات الشبكة المخصصة لعقد التخزين الاستثماري متناسبة مع نصيبها من مبلغ الرسوم المدفوعة إلى الخزانة بواسطة آلية التخزين الاستثماري خلال الجولة السابقة. يمكن وضع حدود على حجم تجمعات مستثمرين التخزين (Staking pools) للحث على المنافسة بين المحتفظين بالأموال إذا كان ذلك الأمر مرغوبًا فيه أو منع المستخدمين من إرسال رسائل غير مرغوب فيها إلى آلية الاحتفاظ بالأموال على أمل ثني من يحتفظون بالأموال

الصادقين عن المشاركة. في الحالات العادية، ستمنع آلية سلسلة الكتل الحلقية و"إعادة البث التلقائي للمعاملات" المتسللين من شن هجمات البريد العشوائي حيث أن UTXO المتعددة ستدفع جميعًا رسوم إعادة البث.

لضمان استمرارية عمل النظام، يجب على منتجي الكتل الذين يعيدون بث UTXO إلى أن يحددوا في "إعادة البث التلقائي للمعاملات" الخاصة بهم إلى ما إذا كانت النواتج (Outputs) المحددة نشطة في تجمعات مستثمرين التخزين(Staking pools) الحالية أو المعلقة. يمكن تضمين تمثيل تجزئة (Hash representation) لحالة جدول الاحتفاظ بالأموال في كل كتلة في شكل التزام للسماح للعقد بالتحقق من دقة جدول الاحتفاظ بالأموال، لكن آلية "إعادة البث التلقائي للمعاملات" ستسمح نظريًا لجميع العُقَد بإعادة بناء حالة احتفاظ بالأموال في فترة واحدة على أقصى تقدير.

يمكن تعديل صعوبة عملية التعدين لأعلى إذا تم العثور على كتلتين تحتويان على تذاكر ذهبية في صف واحد أو لأسفل إذا تم العثور على كتلتين بدون تذاكر ذهبية على التوالي. يمكن لتكلفة عقابية مماثلة أن تخنق عائد مستثمرين التخزين إذا تم العثور على كتلتين متتالية بدون تذاكر ذهبية (يتم حجب مبلغ متزايد باستمرار من إيرادات التخزين). نشجع المهتمين بالرياضيات البحتة على الرجوع إلى أوراقنا البحثية حول هذا الموضوع. تكلفة مهاجمة شبكة سايتو باستخدام هذه الآلية ترتفع بشكل ملحوظ فوق مئة بالمئة.

٦. الأمن المتقدم لـ PAYSPLIT

هناك العديد من التعديلات على آلية paysplit التي يمكن استخدامها لزيادة تكاليف الهجوم. في حين أن إصدار سايتو الذي يتم إطلاقه للإنتاج لا يتضمن هذه الآلية، فمن الممكن إضافة نظام تصويت ديناميكي إلى سايتو والذي يمكن أن يسمح بعملية paysplit ديناميكيًا. يصف هذا القسم التحسين النظري الذي يسمح بعملية الدفع paysplit التي ستعمل وفقًا لافتراضات معينة حول عقلانية الشبكة.

يؤدي تطبيق هذا النظام إلى تعديل الكتل بحيث تتضمن تصويتًا لزيادة أو تقليل أو تثبيت عملية paysplit للشبكة. يمكن بعد ذلك تعديل حلول التذاكر الذهبية بحيث تحتوي على تصويت مماثل حول صعوبة وظيفة إنتاج التذكرة الذهبية. يتم تحديث متغيرات الاتفاق للشبكة عندما وفقط عندما يتم حل التذاكر الذهبية وإدراجها في سلسلة الكتل.

يمكن أن يؤدي تعديل عملية paysplit إلى تغيير توزيع الرسوم بين عقد التوجيه والمعدّنين في الوقت الفعلي. هذا يسمح للشبكة بالوصول إلى التوازن الأمثل بدلاً من التوازن التعسفي. لمنع هذا التوازن من عكس تفضيلات عقد التوجيه والتعدين فقط، نوصي بالسماح للمستخدمين على الشبكة بتمييز معاملاتهم بعملية تصويت paysplit المثلى أيضًا: في حالة حدوث معاملة من إنشاء المستخدم على مثل هذا التصويت، فقد يتم تضمينه فقط في الكتلة التي تصوت في نفس الاتجاه. وبالتالي، فإن المستخدمين الذين يتخذون جانبًا في الصراع المستمر بين أجهزة التوجيه والمعدّنين يضحون بموثوقية وسرعة تأكيد المعاملة، لكنهم يكتسبون تأثيرًا هامشيًا على كيفية تخصيص الشبكة للرسوم. يقوم المستخدمون الذين يقومون بالتصويت أيضًا بحجب رسومهم من العُقَد التي تصوت بشكل مختلف عنهم.

في ظل الظروف التي يُظهر فيها المشاركون في الشبكة عقلانية محدودة، تدفع آلية paysplit إلى النقطة التي يكون فيها الأمان المقدم هو الأمثل لجميع المشاركين بالنظر إلى تكلفة تحصيل الرسوم الإضافية. اتفاقيات دي توكفيل تؤمّن التوازن: يمكن لأي لاعبين في بنية الشبكة الثلاثية (أجهزة التوجيه، والمعدّنون، والمستخدمون) أن يتعاونوا معًا لإعادة توزيع الدخل paysplit إلى المثالية المرغوبة. بينما نترك البحث في هذه الآلية للمستقبل، فإن تجربة فكرية مفيدة تستكشف كيف يتدهور أمان هذا النظام المكون من ثلاثة لاعبين إلى مستوى أمان من فئة البيتكوين فقط مع اقتراب paysplit من القيم القصوى.

٧. ملاحظات إضافية حول أمن الشبكة

يحل تصميم سايتو العديد من المشكلات التي طال أمدها من الملاحظة. يتم تقليل هجمات التخزين لأن العُقَد التي تشارك في توجيه المعاملات تزيد من الإيرادات من خلال إيجاد مسار التوجيه الأكثر كفاءة في الشبكة. تشجع المنافسة على تقاسم الرسوم بدلاً من اكتنازها . يتيح توفر معلومات التوجيه في الكتل أيضًا للمشاركين التحقق من أن أقرانهم ينشرون معاملاتهم بأمانة بدلاً من تكديسها.

نظرًا لأن إضافة القفزات إلى أي مسار توجيه يقلل بالضرورة من ربحية التوجيه لكل عقدة في المسار، يتم أيضًا التخلص من هجمات sybil. توفر الكتل المعلومات اللازمة للمشاركين لتحديد وإلغاء هجمات sybil في شبكات نظير إلى نظير الخاصة بهم. وتضمن الضغوط التطورية أنها تطهرها: العُقَد الأضعف التي تسمح لنفسها بالتعامل معها سوف تجد نفسها مطرودة من الشبكة بسبب الضغوط التنافسية بمرور الوقت.

تخدم شبكة التوجيه أيضًا آلية دفاعية فريدة. يمكن لعقد التوجيه في سايتو زيادة تكلفة الهجوم في الوقت الفعلي من خلال رفض توجيه المعاملات إلى المهاجمين، مما يجبر المهاجم على زيادة اعتماده على محفظته الخاصة لتمويل إنتاج الكتلة. تدافع هذه الآلية أيضًا عن سايتو ضد الهجمات الخفية مثل تسييل تدفقات المعاملات وتوجيه الوصول المغلق.

كملاحظة أخيرة، نلاحظ أن "ثلاثية القابلية للتوسع" (Scalability trilemma) التي غالبًا ما يتم الدفاع عنها كقانون أساسي من سلسلة الكتل غير موجودة في تصميم سايتو.

هناك العديد من التكوينات الواضحة للشبكة التي يمكن أن تؤدي فيها رسوم إعادة التوجيه من المعدّنين إلى عقد التوجيه في نفس الوقت إلى زيادة الإنتاجية واللامركزية وأمن الشبكة في وقت واحد.

٨. الملخص

تعتبر المشاكل الأساسية التي تؤثر على توسيع نطاق سلسلة الكتل هي مشاكل اقتصادية بحتة. يعمل سايتو على إصلاح هذه المشكلات، مما يسمح لنا ببناء سلسلة كتل قابلة للتوسع (Scalable blockchain) بشكل كبير من خلال ضمان تدفق المدفوعات إلى العُقَد التي تنفق الأموال على البنية التحتية للشبكة.

سيجد أولئك الذين يتدفقون على التفاصيل الفنية لشبكة سايتو ما لا يقل عن سبعة ابتكارات رئيسية مضمنة في تقنية سلسلة الكتل: إعادة البث التلقائي للمعاملات، ورسوم الحرق، ونظام التذاكر الذهبية، و paysplit و powsplit، وتذاكر N-block الذهبية، آلية تصويت آمنة، وسلسلة التوقيعات المشفرة التي تسمح لسلسلة الكتل بتحديد ومكافأة العُقَد المنتجة في شبكة التوجيه.

تم تأمين حماية براءات الاختراع على هذه التقنيات ونرحب بالاتصال من المشاريع الأخرى لسلسلة الكتل التي تتطلع إلى دمج واحدة أو أكثر من هذه الطرق في شبكاتهم الخاصة. نشجع القراء أيضًا على زيارة موقعنا على الويب (Https: // saito.io) والذي يتضمن واجهة لشبكة العمل وخارطة طريق تحدد خطط التطوير المستقبلية والبرامج التعليمية التي يمكن أن تساعد أي شخص على البدء في إنشاء تطبيقات سايتو اليوم.