ما مدى مقاومة الأنظمة اللامركزية للرقابة؟[1]

Jon Durfee

A product manager in the Federal Reserve Bank of New York's New York Innovation Center.

Michael Junho Lee

A financial research economist in the Federal Reserve Bank of New York's Research and Statistics Group

تم تصميم سلاسل الكتل العامة غير المصرح بها لتكون مقاومة للرقابة، مما يعني أن الوصول إلى البلوكشين دون إعاقة. من الناحية العملية، يمكن للجهات الفاعلة المختلفة في النظام الإيكولوجي للبلوكشين (مثل المستخدمين أو البنائين أو المقترحين) التأثير على درجة مقاومة البلوكشين للرقابة. في تقرير الموظفين الأخير، ندرس كيف أثرت العقوبات التي فرضها مكتب مراقبة الأصول الأجنبية (OFAC) على تورنادو كاش، وهي مجموعة من العقود الذكية للعملات المشفرة غير الاحتراصية على الإيثيريوم، على تورنادو كاش وشبكة الإيثيريوم الأوسع. في هذا المنشور، نلخص النتائج المتعلقة بالتعاون في العقوبات في طبقة التسوية من قبل "مقترحي الكتلة" – وهي مجموعة من الجهات الفاعلة في مجال الاستيطان المسؤولة على وجه التحديد عن اختيار كتل جديدة لإضافتها إلى البلوكشين.

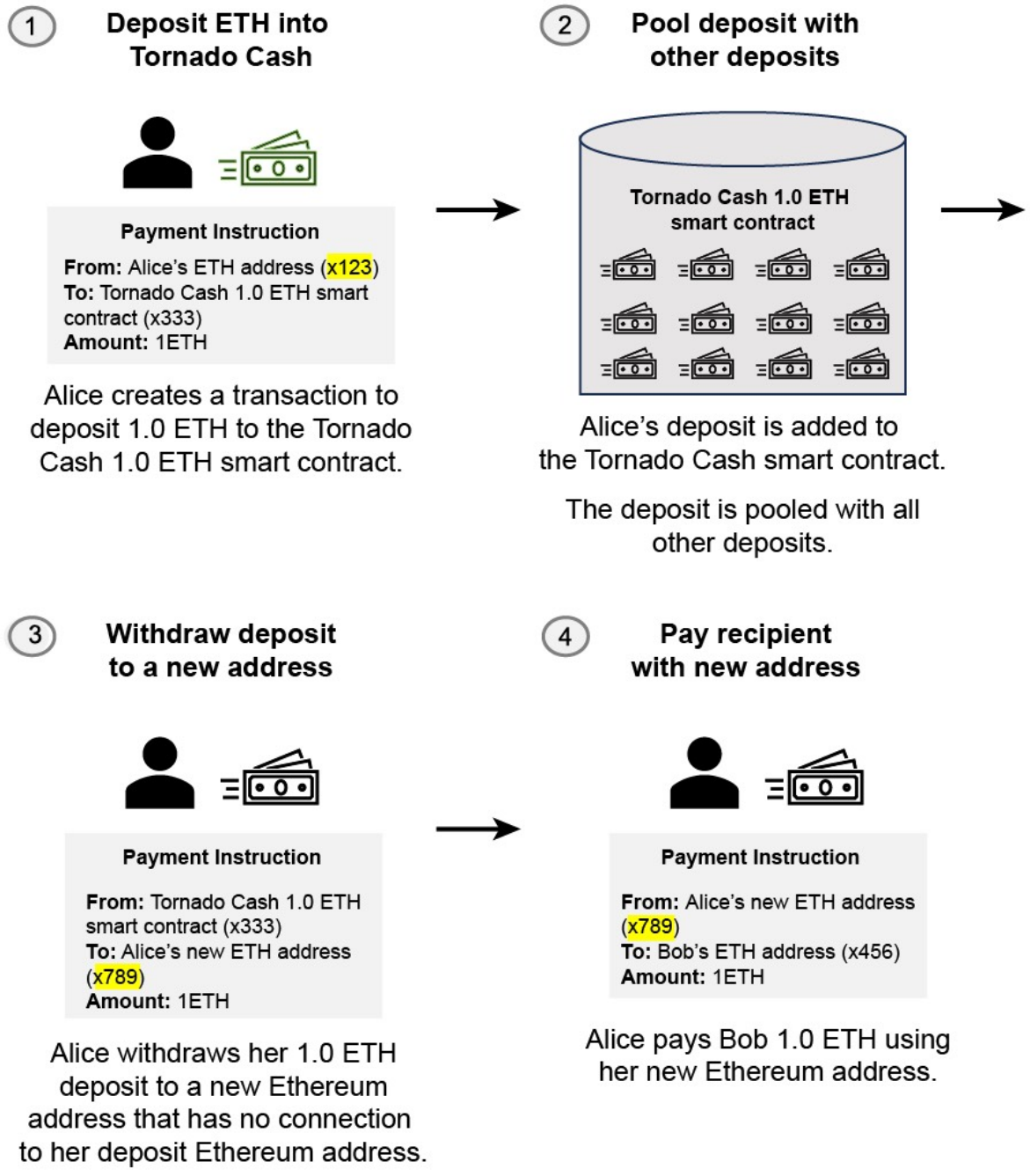
ما هو Tornado Cash؟

تورنادو كاش هي مجموعة من العقود الذكية على بلوكشين الإيثيريوم، وهي بلوكشين عام بدون إذن يسمح لأي شخص لديه إمكانية الوصول إلى الإنترنت بالتفاعل معها. نظرا لطبيعة الإيثيريوم المفتوحة، فإن جميع المعاملات هي سجل عام. يهدف تورنادو كاش إلى توفير خصوصية المعاملات للمستخدمين من خلال الجلوس بين سلاسل الدفع لإخفاء الروابط بين دافعي المستفيدين. يعمل Tornado Cash عن طريق إنشاء حسابات شاملة، أو مجمعات، تحدد أحجام الودائع والرموز المميزة والعملات المستقرة (مثل 1 ETH و 10 ETH و 100 ETH و 1 USDC و 10 USDC وما إلى ذلك). لإيداع الأموال في هذه الحسابات الشاملة، أو "المسابح"، يقوم المستخدم بتحويل إيداع محدد للعملة المشفرة (1 ETH، على سبيل المثال) إلى تجمع Tornado Cash المحدد، ويرفق مفتاحا سريا

[1] Jon Durfee and Michael Lee, How Censorship Resistant Are Decentralized Systems?, FEBRUARY 14, 2025, Federal Reserve Bank of New York, Link.

للمعاملة التي يعرفها المستخدم فقط. يمنح عقد تورنادو كاش الذكي لأي شخص يعرف المفتاح حقوق سحب الأموال من المجمع في وقت لاحق من خلال أي حساب. لا يحتفظ عقد تورنادو كاش الذكي بالأموال أثناء الاحتفاظ بالأموال في المجمعات. انظر الرسم البياني أدناه للحصول على تصوير منمق ونادلر وشار (٢٠٢٣) للحصول على نظرة عامة أكثر تقنية على تورنادو كاش.

مثال منمق على معاملة تورنادو النقدية



المصدر: براونورث، دورفي، لي، ومارتن (٢٠٢٤)، الشكل ٢.

استمر استخدام Tornado Cash في الارتفاع حتى عام ٢٠٢٢، وعلى وجه الخصوص، تم استخدامه من قبل المجرمين. على سبيل المثال، في أوائل عام ٢٠٢٢، أعلن مشروع البلوكشين رونين عن سرقة العملات المشفرة التي تزيد قيمتها عن ٦٠٠ مليون دولار. قامت مجموعة لازاروس، وهي مجموعة القراصنة الكورية الشمالية المسؤولة عن الاختراق، بتحويل الرموز المسروقة إلى تورنادو كاش. في ٨ أغسطس ٢٠٢٢، مكتب الأوان المتحرجي، وهي وكالة داخل الولايات المتحدة. أعلنت وزارة الخزانة التي تحافظ على سياسة العقوبات على الولايات المتحدة وتنفذها، عن عقوبات تحظر "جميع المعاملات التي يقوم بها الأشخاص الأمريكيون أو داخل الولايات المتحدة" التي تنطوي على أصول تورنادو كاش.

تنطبق العقوبات على نطاق واسع على الأشخاص والكيانات الأمريكيين وأولئك الذين لديهم أشكال من الانتماءات. وبالتالي، ليس مطلوبا من جميع المستخدمين والجهات الفاعلة في التسوية الامتثال. بالنظر إلى الطبيعة المستعارة للإيثيريوم، فإننا ننظر إلى تحليلنا على أنه يدرس التعاون، بدلا من الامتثال للعقوبات. نحن نعرف التعاون على أنه "التصرف بطريقة لا تسهل معالجة معاملات تورنادو كاش". مجموعة مهمة من الجهات الفاعلة في التسوية هم المقترحون، الذين لديهم الحقوق النهائية لاختيار الكتلة المرفقة بالبلوكشين. نقوم بتحليل السلوك التعاوني لأفضل عشرة مقترحين للإيثيريوم، الذين يمثلون أكثر من ٥٠٪ من كتل الإيثيريوم التي تم التحقق منها، من يناير ٢٠٢٠ إلى ديسمبر ٢٠٢٣. يعتمد تحليلنا على بيانات معاملات الإيثيريوم على السلسلة من الكثبان الرملية، وهي منصة بيانات للعملات المشفرة، وبيانات البلوكشين العامة لخدمات أمازون ويب (AWS).

تحليل التعاون في طبقة التسوية

يتم تنظيم تسوية الإيثيريوم حاليا في هيكل فصل المقترحين والباني (PBS). بموجب PBS، يتم تجميع المعاملات المقدمة من المستخدمين في كتل من قبل البنائين. ثم يقدم البناؤون كتلهم إلى المقترحين (المدققين)، الذين لديهم حقوق اختيار الكتلة التالية التي سيتم إلحاقها بالبلوكشين. بعبارة أخرى، يختار المقترحون بنشاط من مصدر الكتل منه (بما في ذلك إمكانية بناء اللبنات بأنفسهم). وبالتالي، يلعب مقترحو الكتلة دورا أساسيا في مقاومة الرقابة الخارجية حيث يمارسون السلطة التقديرية بشأن البنائين الذين يعملون معهم، وبالتالي يؤثرون على طبيعة المعاملات التي تمت تسويتها في دفتر الأستاذ الإيثيريوم.

في هذا المنشور، نلخص بعض النتائج الرئيسة المتعلقة بتأثير عقوبات تورنادو كاش على سلوك أفضل ١٠ مقترحين، ونحقق فيما إذا كان هؤلاء المقترحون يستبعدون بنشاط معاملات تورنادو كاش.

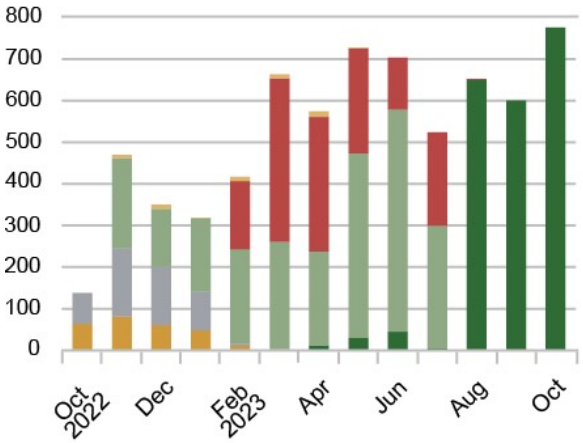
أولا، نجد مجموعة واسعة من التعاون في مجال العقوبات بين مقدمي المقترحات. على التردد الشهري، يختلف عدد الكتل التي تم التحقق منها والتي تحتوي على معاملات تورنادو كاش اختلافا كبيرا عبر المقترحين، ويتراوح في أي مكان من الصفر إلى أكثر من ٧٠٠.

ومن المثير للاهتمام، أننا نجد أن مقدمي المقترحات الأفراد يحافظون على مواقف تعاونية متسقة بشكل ملحوظ مع مرور الوقت (على سبيل المثال، لاختيار الكتل التي تستبعد معاملات تورنادو كاش)، على عكس البنائين، الذين تتطور مواقفهم ديناميكيا استجابة للتطورات القانونية. والجدير بالذكر أن أكبر اثنين من المقترحين حسب حصة الكتلة (المقترحين ١ و ٢ في الرسم البياني أدناه)، يمثلان معا حوالي ٤٠٪ من الكتل، والتحقق من صحة الكتل غير التعاونية (وبعبارة أخرى، الكتل التي تشمل معاملات تورنادو كاش).

يختلف مستوى التعاون بين المقترحين

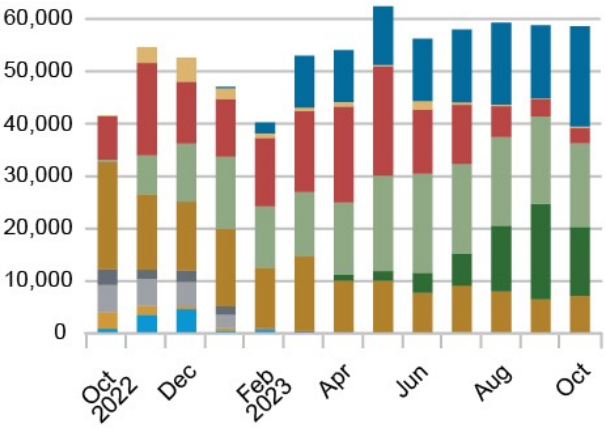
Proposer 1 – Non-Cooperative Blocks by Builder

Number of blocks by builder, monthly



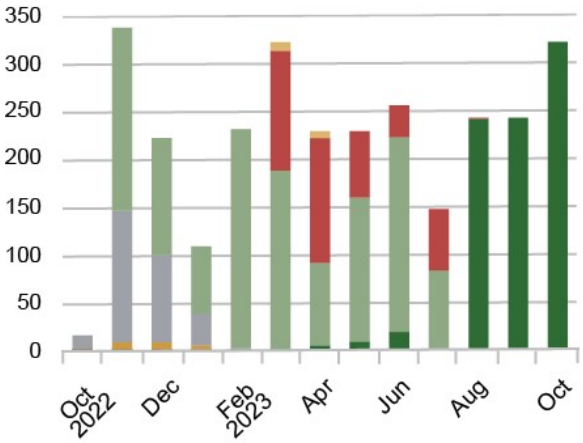
Proposer 1 – Cooperative Blocks by Builder

Number of blocks by builder, monthly



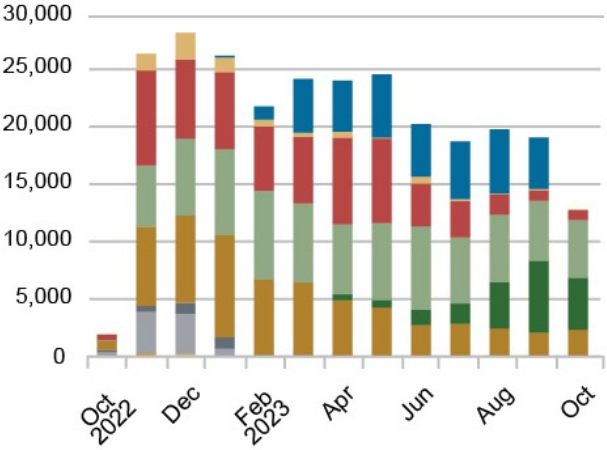
Proposer 2 – Non-Cooperative Blocks by Builder

Number of blocks by builder, monthly



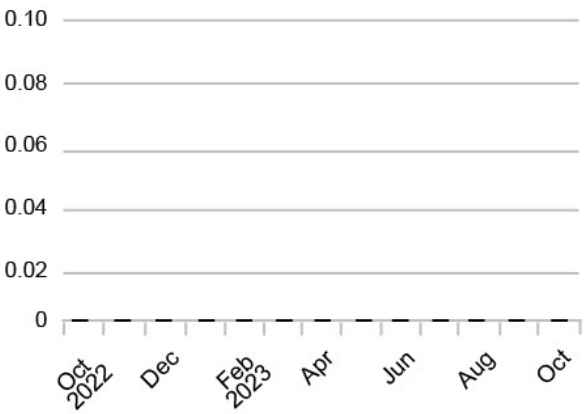
Proposer 2 – Cooperative Blocks by Builder

Number of blocks by builder, monthly



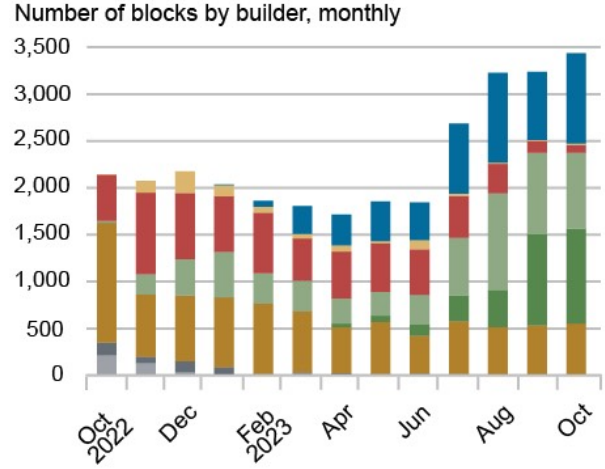
Proposer 9 – Non-Cooperative Blocks by Builder

Number of blocks by builder, monthly



Proposer 9 – Cooperative Blocks by Builder

Number of blocks by builder, monthly



المصدر: براونورث، دورفي، لي، ومارتن (٢٠٢٤)، الأشكال ١١–١٣.

ما الذي يفسر الموقف غير التعاوني لأكبر المقترحين بشأن الإيثيريوم؟

يمكن أن يكون أحد الأسباب المحتملة لمقترحي المقترحات لمواصلة التحقق من صحة الكتل غير التعاونية هو أن التعاون يمثل تحديا تشغيليا أو مكلفا بالنسبة لهم. من حيث المبدأ، لا يستطيع المقترحون رؤية المعاملات الفردية المدرجة في كتلة يقدمها المنشئ؛ فهم يختارون الكتل بناء على هوية المنشئ والرسوم المرتبطة بالكتلة. وبالتالي، لا يمكن لمقدم الاقتراح التحقق تقنيا مما إذا كانت الكتلة متعاونة أم لا.

ومع ذلك، في الممارسة العملية، لا يبدو أن هذا قيد ذي صلة. أولا، نلاحظ المقترحين (على سبيل المثال، انظر المقترح ٩ في الرسم البياني أدناه) الذين يعالجون باستمرار الكتل التعاونية طوال فترة العينة لدينا. بالإضافة إلى ذلك، في حين أنه من الصحيح أن مقدمي المقترحات غير قادرين على فحص المعاملات التي تشكل الكتلة، فإن هوية المنشئ غالبا ما تكون كافية لتحديد التعاون. بدءا من أغسطس ٢٠٢٣، يتم توفير جميع الكتل غير التعاونية تقريبا التي تم التحقق من صحتها من قبل المقترحين ١ و ٢ من قبل منشئ واحد، Titan Builder. بشكل عام، نظرا لأننا نجد إمكانية التنبؤ في الموقف التعاوني للبنائين – وفي بعض الحالات، الكشف العام عن موقفهم التعاوني – فإن إمكانية وجود تحديات تشغيلية للتعاون من قبل مقدمي المقترحات تتضاءل.

حجة أخرى هي أن "علم الرمز" قيد التنفيذ. من حيث المبدأ، تم تصميم الإيثيريوم لجذب مشاركين متنوعين من خلال الحوافز النقدية. إذا كانت الحوافز النقدية هي الدوافع الرئيسة، فيجب أن نتوقع أن تكون الرسوم المرتبطة بالكتل غير التعاونية أعلى من تلك الخاصة بالكتل التعاونية. لم نجد أي دليل على أن هذا هو الحال. في الواقع، نجد العكس: تقدم الكتل غير التعاونية في عينتنا باستمرار رسوما أقل، مع خصم يتراوح من ١٥–٢٣٪، اعتمادا على التقديرات.

هل تستطيع البلوكشين العامة مقاومة الرقابة؟

تهدف سلاسل الكتل العامة غير المصرح بها، مثل الإيثيريوم، إلى أن تكون مقاومة للرقابة. ومع ذلك، حتى سلاسل الكتل ذات قواعد المستخدمين الواسعة، مثل الإيثيريوم، ليست في مأمن من إمكانية استبعاد بعض المعاملات بسبب الضغط الخارجي. في عينتنا، نرى وضعا تعاونيا مختلطا للإنفاذ في طبقة التسوية من قبل المقترحين، والأهم من ذلك، أننا لا نلاحظ أي تغيير في المواقف.

في ضوء أدلتنا على أن التعاون ليس صعبا، إلى جانب حقيقة أن دوافع عدم التعاون ليست مالية، تشير نتائجنا إلى أن مقاومة الرقابة للنظام تعززها اللاعبين الكبار الذين يقدرون مقاومة الرقابة كميزة بدائية. علاوة على ذلك، لا يبدو أن ميزات التصميم الملموسة – مثل الحوافز المالية، التي تهدف إلى السماح بالتعبير عن الآراء، مهما كانت مثيرة للجدل – فعالة في تعزيز مقاومة الرقابة.

لم يتم بعد تحديد الإطار التنظيمي والقانوني للنظم اللامركزية، كما يتضح من قرار المحكمة الأخير الذي ألغى الأحكام السابقة المتعلقة بعقوبات مكتب مراقبة الأصول الأجنبية بشأن تورنادو كاش. تظهر هذه التطورات كذلك أن شفافية المعاملات والاختيار في علاقة بناة الكتل والمقترحين هو موضوع بحثي حاسم لمجتمع الإيثيريوم، الذي يطمح إلى الحفاظ على طبقة تسوية مقاومة للرقابة. يبقى أن نرى ما إذا كان مجتمع الإيثيريوم يقدم ضوابط وعمليات منهجية لضمان تسوية جميع المعاملات في التسوية، بغض النظر عن الأنظمة التنظيمية.