# CashWeb: بروتوكول متكامل مع العملات المشفرة لأنظمة الرسائل الموزعة المقاومة للبريد المزعج والنشر-الاشتراك

Chancellor Shammah
shammah.chancellor@proton.me
https://t.me/TheLotusNetwork

٢١ فبراير ٢٠٢٦
الإصدار 1.1

ملخص

نقدم CashWeb، مجموعة بروتوكولات شاملة تدمج الآليات الاقتصادية القائمة على العملات المشفرة مع بنية تحتية موزعة للرسائل لتمكين التواصل المقاوم للبريد المزعج دون إشراف مركزي. يوظف البروتوكول آلية مبتكرة للإحراق للتعبير (burn-to-speak) لمكافحة البريد المزعج، حيث يُرفق مُرسِلو الرسائل مدفوعات مشفرة صغيرة قابلة للتحقق الكتابي دون الحاجة إلى وسطاء موثوقين. نُقدم مواصفات رسمية لثلاثة مكونات أساسية: (1) بروتوكول إثبات الدفع (POP) الذي يربط القيمة على السلسلة بالأفعال خارج السلسلة، (2) الرسائل الموزعة مع إدارة هوية تشفيرية، و(3) نظام نشر-اشتراك للبث القائم على المواضيع. يُثبت تحليلنا الاقتصادي أن آلية الإحراق تحقق ردعاً أمثل ضد البريد المزعج مع الحفاظ على إمكانية الوصول للتواصل المشروع. تستثمر بنية النظام المعايير الويبية الراسخة (HTTP/2، WebSockets) والأوليات التشفيرية لتمكين التكامل السلس مع البنية التحتية القائمة. يُظهر التحليل النظري أن البروتوكول يحقق مقاومة البريد المزعج بتكاليف تتناسب تناسباً دون خطي مع حجم الشبكة، فيما يُثبت النشر التجريبي الجدوى العملية لتطبيقات الرسائل الفورية.

## ١ مقدمة

### ١.١ مشكلة المركزية

يكشف تطور بروتوكولات التواصل عبر الإنترنت عن توتر جوهري بين اللامركزية وسهولة الاستخدام. صُمِّمت الأنظمة الأولى كـUsenet ?? وSMTP ?? وXMPP ?? كشبكات موزعة تتيح التواصل النظير-إلى-نظير دون سلطات مركزية. غير أن بنية التكلفة غير المتماثلة المتأصلة في هذه البروتوكولات --- حيث يتحمل المستقبلون تكاليف معالجة الرسائل بينما تبقى تكاليف الإرسال ضئيلة --- أفرزت حوافز اقتصادية للإساءة دفعت المستخدمين في نهاية المطاف نحو المنصات المركزية.

بحلول عام 2020، بلغ تركيز البنية التحتية للاتصالات مستويات غير مسبوقة: سيطرت كل من جوجل وأبل ومايكروسوفت مجتمعةً على 85% من حصة سوق عملاء البريد الإلكتروني ?، في حين أفادت فيسبوك بأكثر من ملياري مستخدم وخدمت Gmail 5.1 مليار حساب نشط ?. هذه المركزية، وإن وفرت الراحة للمستخدمين، أدخلت مخاطر منهجية تشمل الرقابة والمراقبة ونقاط الفشل المفردة التي تضر بالرؤية الأصلية للتواصل الإنترنتي الموزع.

### ٢.١ آليات مكافحة البريد المزعج الاقتصادية

التحدي الجوهري في أنظمة الرسائل اللامركزية هو منع البريد المزعج دون تصفية مركزية. تعتمد المقاربات التقليدية إما على التكاليف الحسابية (Hashcash ?) أو أنظمة السمعة التي تستلزم التحقق من الهوية المستمر. رغم توفير هذه الآليات قدراً من الحماية، إلا

أنها تعاني من قيود جوهرية: لا يتوسع إثبات العمل الحسابي جيداً مع تسريع الأجهزة الحديثة، وتُنشئ أنظمة السمعة حواجز أمام المستخدمين الجدد مع بقائها عرضة لهجمات السيبل.

يُتيح ظهور شبكات العملات المشفرة، ولا سيما بيتكوين ?، نهجاً جديداً: آليات إثبات الدفع الاقتصادية التي تتحقق من صحة الرسائل عبر الإثبات التشفيري لإتلاف القيمة بدلاً من العمل الحسابي. هذا النهج الذي تصوره فيني أصلاً ? بوصفه ``إثبات العمل القابل لإعادة الاستخدام''، يمكن الآن تطبيقه دون وسطاء موثوقين باستخدام شبكات العملات المشفرة اللامركزية.

### ٣.١ المساهمات

تقدم هذه الورقة CashWeb، مجموعة بروتوكولات شاملة تعالج مشكلة المركزية عبر ثلاث مساهمات رئيسية:

١. بروتوكول إثبات دفع رسمي: نُحدد بروتوكولاً تشفيرياً كاملاً لربط معاملات العملات المشفرة على السلسلة بأفعال الرسائل خارج السلسلة، مما يتيح آليات مكافحة البريد المزعج القابلة للتحقق دون الحاجة إلى أطراف موثوقة.

٢. تصميم بنية تحتية موزعة: نقدم بنية قابلة للتوسع تجمع خوادم المفاتيح لإدارة الهوية وخوادم التتابع لتوجيه الرسائل، مُصمَّمة لدعم أحجام المعاملات اللازمة للتبني الواسع مع الحفاظ على اللامركزية.

٣. تحليل الأمان الاقتصادي: نقدم تحليلاً نظرياً يُثبت أن آليات معدل الإحراق المناسبة تحقق مقايضات مثلى بين ردع البريد المزعج وإمكانية وصول المستخدمين الشرعيين، مع حدود رسمية على تكاليف الهجوم واحتمالات نجاحه.

البروتوكول مُصمَّم للنشر على شبكة Lotus للعملات المشفرة ?، سلسلة إثبات عمل بدعم أصلي لمخرجات OP_RETURN ذات القيمة وسياسة نقدية تكيفية كما هو مُحدد في ?. Lotus يعمل حالياً، CashWeb يوفر بروتوكول طبقة التطبيقات المُكمِّل للمنظومة الاقتصادية. يستثمر البروتوكول المعايير الويبية الراسخة ويحافظ على التوافق مع البنية التحتية الإنترنتية القائمة. توفر تجربة النشر مع الشبكة الاجتماعية Stamp تحققاً مبكراً من المقاربة الجوهرية.

هذه الورقة هي الثالثة في سلسلة. تُرسي ? الأساس النظري: في أي نظام إجماع بلا إذن، يكون الإنفاق الأمني في التوازن مرتبطاً بالقيمة المتوقعة المعرضة للخطر، ويجعل إثبات العمل هذا الإنفاق قابلاً للقراءة على مستوى البروتوكول عبر إشارة عمل مكشوفة تنافسياً. تطور ? التداعيات على السياسة النقدية، مُحددةً آلية حلقة مزدوجة خالية من الوسطاء تستخدم إشارة العمل لإصدار ذيل تكيفي والإحراق للتعبير كمصرف داخلي للعرض. تُحدد الورقة الحالية آلية الإحراق للتعبير كاملةً كبروتوكول رسائل موزع. ومن ثمَّ يؤدي الإحراق للتعبير دوراً مزدوجاً عبر المنظومة: ردع البريد المزعج على طبقة التطبيقات وإدارة العرض النقدي الداخلي على مستوى البروتوكول.

### ٤.١ تنظيم الورقة

يستعرض القسم ?? الأعمال ذات الصلة في آليات مكافحة البريد المزعج والرسائل الموزعة. يُؤسِّس القسم ?? نموذج النظام وافتراضات التهديد. يوفر القسم ?? المواصفات الرسمية للبروتوكولات الأساسية. يُحلل القسم ?? الخصائص الاقتصادية وضمانات مقاومة البريد المزعج. يفحص القسم ?? خصائص الأمان ومقاومة الهجمات. يناقش القسم ?? اعتبارات النشر العملي. يقدم القسم ?? نتائج التقييم النظري والتجريبي.

## ٢ الخلفية والأعمال ذات الصلة

### ١.٢ آليات مكافحة البريد المزعج الاقتصادية

لاستخدام الحوافز الاقتصادية في منع البريد المزعج تاريخ ثري في بحوث الأنظمة الموزعة. اقترح دورك وناور ? أول مرة اشتراط إثبات عمل حسابي لإرسال البريد الإلكتروني، مُطبَّقاً في Hashcash ? عبر أحاجي البادئة الأولية لتجزئة SHA-256. رغم سلامة

المقاربات الحسابية نظرياً، إلا أنها تعاني من قيود عملية: (1) تتباين تكلفة الحوسبة تبايناً كبيراً عبر الأجهزة المختلفة مُفرِزةً عدم إنصاف، (2) يمكن للASIC الحديث والGPU المُسرَّع حل الألغاز بمعدلات تفوق الأجهزة الاستهلاكية بمراتب، (3) يستلزم مستوى الصعوبة الأمثل تعديلاً مستمراً مع تطور القدرات الحسابية.

اقترح لوري وكلايتون ؟ أنظمة إثبات عمل تستخدم دوال كثيفة الذاكرة لتقليل مزايا الأجهزة، لكن هذه المقاربات لا تزال تستلزم إنفاقاً طاقوياً كبيراً وتُنشئ حواجز للأجهزة محدودة الموارد. المقاربات البديلة القائمة على السمعة ؟ تستلزم أنظمة هوية مستمرة تتعارض مع أهداف الخصوصية وتُنشئ حواجز عالية للمستخدمين الشرعيين الجدد.

### ٢.٢ التحكم في الوصول القائم على العملات المشفرة

يُتيح ظهور شبكات العملات المشفرة القابلة للبرمجة آليات اقتصادية أكثر تطوراً. اقترح ميلر وآخرون ؟ استخدام بيتكوين للمدفوعات الصغيرة المجهولة، لكن مقاربتهم تستلزم بروتوكولات تفاعلية لا تتوسع لتطبيقات الرسائل. توفر الأبحاث الأخيرة حول قنوات الدفع ؟ وقنوات الحالة ؟ آليات للمدفوعات الصغيرة منخفضة الكمون، لكن اشتراط القنوات المُموَّلة مسبقاً يُنشئ حواجز قابلية الاستخدام.

تختلف مقاربتنا باعتمادها على إتلاف القيمة غير القابل للاسترداد (``الإحراق") بدلاً من نقل القيمة، مُلغيةً الحاجة إلى بنية تحتية لدفع المستقبِل مع الحفاظ على حوافز اقتصادية قوية ضد الإساءة.

### ٣.٢ أنظمة الرسائل الموزعة

تُوازن معماريات الرسائل الموزعة بين مزايا اللامركزية ومتطلبات قابلية التوسع العملية. يُثبت XMPP ؟ جدوى الرسائل الفورية الموزعة، لكنه يفتقر إلى آليات مكافحة البريد المزعج الاقتصادية. يوفر Matrix ؟ رسائل موزعة حديثة مع تشفير شامل، لكنه يعتمد على مزودي هوية مركزيين ويفتقر إلى آليات مكافحة البريد المزعج بما يتجاوز تحديد المعدل.

تشمل أنظمة الرسائل الأخيرة القائمة على سلسلة الكتل Status ؟ وSession ؟، التي توفر إدارة هوية لامركزية لكنها لا تعالج مشاكل الحوافز الاقتصادية المُحرِّكة للمركزية. تدمج مقاربتنا الآليات الاقتصادية مباشرةً في تصميم البروتوكول لمعالجة هذه الانحرافات في الحوافز الجذرية.

## ٣ نموذج النظام والمعمارية

### ١.٣ المشاركون في الشبكة

تتألف شبكة CashWeb من أربعة أنواع من المشاركين:

تعريف ١ (المشاركون في الشبكة). ليكن $\mathcal{U} = \{u_1, u_2, \ldots, u_n\}$ مجموعة المستخدمين، $\mathcal{R} = \{r_1, r_2, \ldots, r_m\}$ مجموعة خوادم التتابع، $\mathcal{K} = \{k_1, k_2, \ldots, k_\ell\}$ مجموعة خوادم المفاتيح، و$\mathcal{T} = \{t_1, t_2, \ldots, t_p\}$ مجموعة مواضيع النشر-الاشتراك.

المستخدمون ($u_i \in \mathcal{U}$): المشاركون الطرفيون الذين يُرسِلون الرسائل ويستقبلونها. يتحكم كل مستخدم في محفظة عملة مشفرة ويمكنه توليد إثباتات دفع تشفيرية. يتفاعل المستخدمون مع الشبكة عبر برامج العميل التي تدير مواد المفاتيح ومعاملات الدفع.

خوادم التتابع ($r_i \in \mathcal{R}$): خوادم موزعة تخزن الرسائل المشفرة وتُحيلها نيابةً عن المستخدمين. تتحقق خوادم التتابع من إثباتات الدفع قبل قبول الرسائل، مُوفِّرةً الخط الدفاعي الأول ضد البريد المزعج. لا تتمكن من الوصول إلى محتوى الرسائل بسبب التشفير الشامل.

خوادم المفاتيح ($k_i \in \mathcal{K}$): خوادم موزعة تحتفظ بسجل عالمي لمفاتيح المستخدمين العامة والبيانات الوصفية المرتبطة بها. تُتيح خوادم المفاتيح للمستخدمين اكتشاف خوادم التتابع وإنشاء قنوات تواصل آمنة دون الحاجة إلى تواصل مسبق.

المواضيع ($t_i \in \mathcal{T}$): قنوات مُسمَّاة في نظام النشر-الاشتراك تُتيح التواصل البثي. المواضيع لامركزية --- يمكن لأي مستخدم إنشاء موضوع ويمكن لأي خادم تتابع نشر رسائل الموضوع استناداً إلى قوائم المشتركين.

### ٢.٣ نموذج التهديد

نأخذ بعين الاعتبار بيئة عدائية بيزنطية حيث قد يخرف المشاركون عشوائياً عن مواصفات البروتوكول. يتضمن نموذج التهديد:

مهاجمو البريد المزعج: خصوم يحاولون إرسال كميات كبيرة من الرسائل غير المرغوب فيها لتعطيل التواصل أو إهدار موارد الشبكة. نفترض أن المهاجمين يمتلكون موارد حسابية ومالية كبيرة لكن منتهية.

مهاجمو سيبل: خصوم يُنشئون أعداداً كبيرة من الهويات المزيفة لتضخيم قدرتهم على إرسال الرسائل أو التلاعب بأنظمة السمعة.

مهاجمو البنية التحتية للشبكة: خصوم يتحكمون في خوادم التتابع أو المفاتيح وقد يحاولون الرقابة أو تحليل حركة المرور أو هجمات الحجب.

المهاجمون الاقتصاديون: خصوم يحاولون التلاعب بالآليات الاقتصادية، بما في ذلك هجمات إعادة تدوير الرسوم حيث يستعيد المهاجمون الأموال المُحرقة عبر السيطرة على التعدين أو التحقق.

نفترض أن شبكة العملات المشفرة الأساسية (مثلاً بيتكوين، Lotus) توفر ضمانات أمانية قياسية تشمل عدم قابلية المعاملات للتغيير ومقاومة هجمات الإنفاق المزدوج. لا نأخذ بعين الاعتبار الهجمات على شبكة العملات المشفرة نفسها.

### ٣.٣ مبادئ التصميم

يلتزم تصميم البروتوكول بعدة مبادئ رئيسية:

الأمان الاقتصادي: ينبغي أن تنبثق حماية مكافحة البريد المزعج من الحوافز الاقتصادية لا من الحواجز الحسابية أو الإشراف المركزي، مما يضمن أن تكون الهجمات مُكلِفة باهظة بينما يظل الاستخدام المشروع ميسور التكلفة.

الخصوصية بالتصميم: ينبغي أن تظل محتويات الرسائل وأنماط التواصل خاصةً بالأطراف الثالثة، بما في ذلك مزودو البنية التحتية للشبكة.

قابلية التوسع الموزعة: ينبغي أن يدعم النظام التبني على النطاق العالمي عبر المعمارية الموزعة مع الحفاظ على خصائص اللامركزية.

التوافق العكسي: ينبغي أن يتكامل البروتوكول مع البنية التحتية الإنترنتية القائمة وأطر التطوير لتقليل حواجز التبني.

## ٤ مواصفات البروتوكولات الأساسية

### ١.٤ بروتوكول إثبات الدفع (POP)

يُتيح بروتوكول إثبات الدفع التحقق التشفيري من أن مقداراً محدداً من العملة المشفرة قد أُحرق (دُمِّر بصورة دائمة) مرتبطاً بفعل معين خارج السلسلة. خلافاً لأنظمة الدفع التقليدية التي تنقل القيمة بين أطراف، ينشئ بروتوكول POP إثباتاً قابلاً للتحقق لإتلاف القيمة لا يمكن استرداده أو إنفاقه مرتين.

تعريف ٢ (بروتوكول إثبات الدفع). بروتوكول *POP* هو ثلاثي $(\text{Setup}, \text{Commit}, \text{Verfiy})$ حيث:

- $\text{Setup}(1^\lambda) \to pp$: يُولِّد معاملات عامة لمعامل الأمان $\lambda$.
- $\text{Commit}(sk, m, v) \to (\pi, \tau)$: بمعطيات المفتاح السري $sk$ والرسالة $m$ والقيمة $v$، يُخرج الإثبات $\pi$ والمعاملة $\tau$.
- $\text{Verfiy}(\pi, \tau, m, v) \to \{0, 1\}$: يتحقق من أن المعاملة $\tau$ تُحرق القيمة $v$ ومرتبطة تشفيرياً بالرسالة $m$.

#### ١.١.٤ بناء المخرج غير القابل للإنفاق

قبل تحديد الخوارزمية، نُعرِّف الأولية الأساسية:

تعريف ٣ (العنوان غير القابل للإنفاق / مخرج OP_RETURN). بقيمة التزام مُكوَّنة من 32 بايت $h_m$، يُشير $\text{UnspendableAddress}(h_m)$ إلى برنامج المخرج $\langle h_m \rangle$ OP_RETURN. مخرج المعاملة ذو القيمة $v$ المُرسَل إلى هذا البرنامج مُدمَّر إثباتاً: (أ) مخرجات

OP_RETURN غير صالحة بالإجماع كمدخلات إنفاق، لذا لا يمكن لأي طرف بناء معاملة إنفاق صالحة؛ (ب) تُصنِّف العقد المتوافقة هذه المخرجات بوصفها معفاة من *UTXO*، مُزيلةً القيمة نهائياً من التداول. حمولة *SHA-256* ذات 32 بايت تقع ضمن حد بيانات OP_RETURN البالغ 80 بايت، تاركةً مجالاً لمعرِّف بروتوكول 4 بايت وحقل إصدار.

تدعم شبكة Lotus، الهدف المقصود للنشر لCashWeb، مخرجات OP_RETURN ذات قيمة غير صفرية بموجب قاعدة الإجماع، مما يجعل ما سبق البناءَ الأساسي. للسلاسل التي تحظر مخرجات OP_RETURN ذات القيمة غير الصفرية (السياسة القياسية لبيتكوين)، يُرسِل البناء البديل $v$ إلى عنوان $\text{P2PKH}(\text{Hash160}(0\text{x}0000\ldots00 \| h_m))$: عنوان P2PKH صالح صياغياً لا يوجد له مفتاح خاص، محققاً عدم قابلية الإنفاق باحتمالية لا عدم قابلية الإنفاق المُنفَّذ بالإجماع.

### ٢.١.٤ البناء

يستثمر بناء بروتوكول POP لدينا مخرجات OP_RETURN في المعاملات على غرار بيتكوين لتضمين بيانات الالتزام مع ضمان إتلاف الأموال:

**Algorithm ١** بناء إثبات الدفع

**Require:** الرسالة $m$، مقدار الإحراق $v$، المفتاح السري للمستخدم $sk$
**Ensure:** الإثبات $\pi$ والمعاملة $\tau$

$pk \leftarrow \text{DerivePublic}(sk)$
$h_m \leftarrow \text{Hash}(m \| pk \| \text{Timestamp}())$
$addr_{burn} \leftarrow \text{UnspendableAddress}(h_m)$
$\tau \leftarrow \text{CreateTransaction}(sk, v, addr_{burn}, h_m)$
$\sigma \leftarrow \text{Sign}(sk, \tau \| m)$
$\pi \leftarrow (\tau, \sigma, m, v, pk)$
return $\pi, \tau$

يضمن البناء عدة خصائص جوهرية:

عدم القابلية للاسترداد: الأموال المُرسَلة إلى $addr_{burn}$ غير قابلة للإنفاق إثباتاً لأن العنوان مشتق من تجزئة لا تتوفر لها صورة أولية معروفة.

الفرادة: كل زوج رسالة-دفع يُنتج التزاماً فريداً لا يمكن إعادة استخدامه لرسائل مختلفة.

قابلية التحقق: يستطيع أي طرف التحقق من الإثبات بفحص المعاملة على سلسلة الكتل والتحقق من التوقيعات التشفيرية.

## ٢.٤ إدارة الهوية وتسجيل المفاتيح

يحتفظ المستخدمون في CashWeb بهويات مستعارة قائمة على التشفير بالمفتاح العام. تتألف كل هوية من زوج مفاتيح $(sk, pk)$ حيث يعمل المفتاح العام كمعرِّف عالمي للمستخدم.

### ١.٢.٤ تسجيل الهوية

تُسجَّل الهويات الجديدة مع شبكة خوادم المفاتيح عبر البروتوكول التالي:

### ٢.٢.٤ تدوير المفاتيح والاسترداد

يدعم البروتوكول تدوير المفاتيح لتمكين الاسترداد من اختراق المفتاح أو فقدانه. يمكن للمستخدمين التسجيل المسبق لمفاتيح الاسترداد أو استخدام اشتقاق المفاتيح الهرمي المحدد للتدوير السلس:

**Algorithm ٢** تسجيل الهوية

**Require:** زوج مفاتيح المستخدم $(sk, pk)$، عنوان خادم التتابع $addr_{relay}$، رسم التسجيل $v_{reg}$
**Ensure:** سجل الهوية في شبكة خوادم المفاتيح

$metadata \leftarrow \{\text{“}relay\text{”} : addr_{relay}, \text{“}timestamp\text{”} : \text{Now}()\}$
$(\pi_{reg}, \tau_{reg}) \leftarrow \text{POP.Commit}(sk, metadata, v_{reg})$
$record \leftarrow (pk, metadata, \pi_{reg})$
do $k_i \in \mathcal{K}$ keyserver each for
Send$(record, k_i)$
for end

**Algorithm ٣** تدوير المفاتيح

**Require:** زوج المفاتيح الحالي $(sk_{old}, pk_{old})$، زوج المفاتيح الجديد $(sk_{new}, pk_{new})$، رسم التدوير $v_{rot}$
**Ensure:** تحديث سجل الهوية

$rotation\_msg \leftarrow (pk_{old}, pk_{new}, \text{Now}())$
$\sigma_{old} \leftarrow \text{Sign}(sk_{old}, rotation\_msg)$
$\sigma_{new} \leftarrow \text{Sign}(sk_{new}, rotation\_msg)$
$(\pi_{rot}, \tau_{rot}) \leftarrow \text{POP.Commit}(sk_{new}, rotation\_msg, v_{rot})$
$update \leftarrow (pk_{old}, pk_{new}, \sigma_{old}, \sigma_{new}, \pi_{rot})$
do $k_i \in \mathcal{K}$ keyserver each for
Send$(update, k_i)$
for end

## ٣.٤ الرسائل الموزعة مع الإحراق للإرسال

يدمج بروتوكول الرسائل الأساسي تسليم الرسائل التشفيري مع الحماية الاقتصادية من البريد المزعج. تُشفَّر الرسائل شاملياً وتتضمن إثبات دفع لإظهار التزام المُرسِل.

**Algorithm ٤** بروتوكول إرسال الرسائل

**Require:** المفتاح العام للمستقبِل $pk_{recv}$، محتوى الرسالة $content$، مقدار الإحراق $v_{msg}$
**Ensure:** تسليم الرسالة إلى خادم تتابع المستقبِل

$(pk_{sender}, sk_{sender}) \leftarrow \text{GetUserKeys}()$
$relay_{recv} \leftarrow \text{KeyserverLookup}(pk_{recv})$
$k_{shared} \leftarrow \text{ECDH}(sk_{sender}, pk_{recv})$
$msg_{encrypted} \leftarrow \text{Encrypt}(k_{shared}, content)$
$message \leftarrow (pk_{sender}, pk_{recv}, msg_{encrypted}, \text{Timestamp}())$
$(\pi_{msg}, \tau_{msg}) \leftarrow \text{POP.Commit}(sk_{sender}, message, v_{msg})$
$delivery\_req \leftarrow (message, \pi_{msg})$
$\text{HTTPPost}(delivery\_req, relay_{recv})$

### ١.٣.٤ التحقق من الرسائل وتخزينها

تتحقق خوادم التتابع من الرسائل الواردة قبل التخزين:

## ٤.٤ النشر-الاشتراك مع الإحراق للبث

يمتد نظام النشر-الاشتراك ليشمل البث القائم على المواضيع. يمكن للمستخدمين الاشتراك في المواضيع واستقبال جميع الرسائل المنشورة فيها، مع تحديد أولوية الرسالة بمقدار الإحراق.

**Algorithm ٥** التحقق من الرسائل بواسطة خادم التتابع

**Require:** طلب تسليم الرسالة $delivery\_req = (message, \pi_{msg})$

**Ensure:** قبول الرسالة أو رفضها

$(message, \pi_{msg}) \leftarrow delivery\_req$

$(pk_{sender}, pk_{recv}, msg_{encrypted}, timestamp) \leftarrow message$

**if** POP.Verfiy$(\pi_{msg}, message) \neq 1$ **then**

  **return** "مرفوض: إثبات دفع غير صالح"

**end if**

**if** BurnAmount$(\pi_{msg}) < v_{min}$ **then**

  **return** "مرفوض: مقدار الإحراق غير كافٍ"

**end if**

StoreMessage$(message, \pi_{msg})$

**return** "مقبول"

تعريف ٤ (الاشتراك في موضوع). الاشتراك في موضوع هو ثلاثي $(u_i, t_j, r_k)$ يشير إلى أن المستخدم $u_i$ يشترك في الموضوع $t_j$ عبر خادم التتابع $r_k$.

**Algorithm ٦** بث رسالة الموضوع

**Require:** معرِّف الموضوع $topic\_id$، محتوى الرسالة $content$، مقدار الإحراق $v_{broadcast}$

**Ensure:** توزيع الرسالة على جميع مشتركي الموضوع

$(pk_{sender}, sk_{sender}) \leftarrow$ GetUserKeys()

$topic\_msg \leftarrow (pk_{sender}, topic\_id, content,$ Timestamp())

$(\pi_{broadcast}, \tau_{broadcast}) \leftarrow$ POP.Commit$(sk_{sender}, topic_msg, v_{broadcast})$

$broadcast\_req \leftarrow (topic\_msg, \pi_{broadcast})$

**for** $r_i \in \mathcal{R}$ **do** server relay each

  SendToRelayIfSubscribers$(broadcast_req, topic_id, r_i)$

**for end**

تتضمن آلية البث الترتيب القائم على الأولوية وتحديد المعدل استناداً إلى مقادير الإحراق:

## ٥ التحليل الاقتصادي وخصائص مكافحة البريد المزعج

### ١.٥ اقتصاديات معدل الإحراق وتحليل التوازن

تعتمد فاعلية آلية الإحراق للتعبير على تحديد معدلات إحراق تجعل هجمات البريد المزعج غير مجدية اقتصادياً مع الحفاظ على إمكانية الوصول للمستخدمين الشرعيين. نُنمذج هذا كمسألة توازن نظرية للألعاب، اتباعاً لإطار الردع الأمثل لبيكر (؟)، مُمتداً إلى البيئة اللامركزية حيث يُطبَّق الإنفاذ عبر الإثبات التشفيري لإتلاف القيمة.

تعريف ٥ (تكلفة هجوم البريد المزعج). لمهاجم يحاول إرسال $N$ رسالة بريد مزعج بمقدار إحراق $B$ لكل رسالة، إجمالي تكلفة الهجوم هو:

$$C_{attack}(N, B) = N \cdot B + C_{operational}(N)$$

حيث $C_{operational}(N)$ تمثل التكاليف الحسابية والبنية التحتية.

تعريف ٦ (منفعة المستخدم الشرعي). منفعة المستخدم الشرعي من إرسال رسالة بمقدار إحراق $B$ هي:

$$U_{legit}(B) = V_{communication} - B - C_{friction}(B)$$

حيث $V_{communication}$ هي القيمة المستمدة من تسليم الرسالة بنجاح و$C_{friction}(B)$ تمثل تكاليف سهولة الاستخدام.

Algorithm ٧ ترتيب أولوية رسائل الموضوع

Require: مجموعة رسائل الموضوع $M = \{m_1, m_2, \ldots, m_k\}$ بمقادير إحراق $\{v_1, v_2, \ldots, v_k\}$

Ensure: جدول تسليم رسائل مُرتَّب حسب الأولوية

$priority\_queue \leftarrow$ EmptyQueue()

do $m_i \in M$ message each for

$priority_i \leftarrow f(v_i)$ حيث $f$ دالة رتيبة تصاعدياً

Insert$(priority_queue, m_i, priority_i)$

for end

do BandwidthAvailable() and NotEmpty$(priority_queue)$ while

$m_{next} \leftarrow$ PopMax$(priority_queue)$

DeliverMessage$(m_{next})$

while end

معدل الإحراق الأمثل $B^*$ يُعظِّم تبني المستخدمين الشرعيين مع تقليص جدوى البريد المزعج. للحصول على شكل قابل للمعالجة، نُحدد الأشكال الدالية:

تعريف ٧ (دالة الرفاه الاجتماعي). نُعرِّف:

$$W(B) = U_0 - \alpha B - \frac{D\sigma}{B},$$

حيث $U_0 > 0$ هي قيمة كل رسالة للمستخدم الشرعي التمثيلي، $\alpha > 0$ هي تكلفته الهامشية للإحراق، $D > 0$ هي الضرر الاجتماعي لكل رسالة بريد مزعج، و$\sigma > 0$ هي حجم البريد المزعج عند تكلفة إحراق وحدة. يلتقط الحد $\alpha B$ التراجع في فائض المستخدم الشرعي من ارتفاع الإحراق؛ يلتقط الحد $D\sigma/B$ إجمالي ضرر البريد المزعج، الذي يتناقص كـ$1/B$ في إطار اقتصاديات مُرسِل البريد المزعج العقلاني.

في ظل هذا التحديد، معدل الإحراق الأمثل هو:

$$B^* = \sqrt{\frac{D\sigma}{\alpha}},$$

مُوازِناً الردع والإمكانية في شكل مغلق.

مبرهنة ٨ (معدل الإحراق الأمثل). يُحقق معدل الإحراق الأمثل $B^*$:

$$\frac{\partial}{\partial B}\left[\sum_{i=1}^{n} U_{legit}^{i}(B) - \alpha \cdot E[N_{spam}(B)]\right] = 0$$

حيث $\alpha$ تمثل التكلفة الاجتماعية للبريد المزعج و$E[N_{spam}(B)]$ هو العدد المتوقع لرسائل البريد المزعج عند معدل إحراق $B$.

برهان. الوجود. عند $B \to 0$، يصبح البريد المزعج غير مُقيَّد و$W(B) \to -\infty$. عند $B \to \infty$، يُصبح المستخدمون الشرعيون خارج نطاق الوصول و$W(B) \to -\infty$. بما أن $W$ دالة مستمرة، يوجد حد أقصى داخلي بموجب نظرية القيمة المتطرفة على أي فترة مضغوطة تحتوي الحد الأقصى.

الشرط من الرتبة الأولى. عند الحد الأمثل الداخلي $B^*$، ينطبق الشرط المذكور مباشرةً بالاشتقاق.

الوحدانية تنطبق في ظل الافتراض الإضافي بأن $W(B)$ مقعَّرة بصرامة، الذي ينطبق حين تكون منفعة المستخدم الشرعي مقعَّرة في $B$ وحجم البريد المزعج محدب في $1/B$ --- افتراضات قياسية في أدبيات الردع الأمثل (?). □

### ٢.٥ قياس مقاومة سيبل

توفر آلية الإحراق مقاومة متأصلة لسيبل لأن كل هوية تستلزم التزاماً اقتصادياً لا مجرد عمل حسابي:

قضية ٩ (حدود هجوم سيبل). لمهاجم بميزانية $\mathcal{B}$، يكون الحد الأقصى لعدد هويات سيبل مُقيَّداً بـ:

$$N_{sybil} \leq \frac{\mathcal{B}}{v_{reg} + k \cdot v_{msg}}$$

حيث $v_{reg}$ هو رسم تسجيل الهوية و$k$ هو العدد المتوقع لرسائل كل هوية.

يُثبت هذا الحد أن هجمات سيبل تتناسب خطياً مع ميزانية المهاجم لا بموارده الحسابية، موفراً ضمانات مقاومة يمكن التنبؤ بها.

### ٣.٥ منع هجمات إعادة تدوير الرسوم

اعتبار أمني جوهري هو منع المهاجمين من استعادة الأموال المُحرقة عبر السيطرة على بنية تحتية التعدين أو التحقق. نُعالج ذلك عبر الإحراق الجزئي للرسوم:

تعريف ١٠ (آلية الإحراق الجزئي للرسوم). لكل معاملة ذات رسوم $F$، تُحرق نسبة $\beta \in (0, 1]$ بينما يُدفع الباقي $(1-\beta)F$ للمعدِّنين:

$$B_{total} = B_{explicit} + \beta \cdot F$$

حيث $B_{explicit}$ هو مقدار الإحراق الصريح و$F$ هو رسم المعاملة.

المعامل $\beta$ مشترك مع إطار السياسة النقدية التكيفية في ?، حيث يعمل نسبة إحراق الرسوم ذاتها في آنٍ واحد كآلية انكماش داخلي للعرض. وهكذا يتحد الدور المضاد للبريد المزعج والدور النقدي هيكلياً: ثابت بروتوكول واحد $\beta$ يوفر كلاً من أرضيات تكلفة الهجوم على مستوى التطبيق وإدارة العرض على مستوى النقد.

مبرهنة ١١ (مقاومة إعادة تدوير الرسوم). في ظل آلية الإحراق الجزئي للرسوم، يمكن لمهاجم يسيطر على نسبة $\mu$ من قوة التجزئة استعادة ما يصل إلى $\mu(1-\beta)$ من تكاليف هجومه على أقصى تقدير، مما يضمن بقاء صافي تكلفة الهجوم موجباً لـ$\mu < \beta$.

تحليل التوازن. تُعطي المبرهنة ?? شرطاً كافياً ($\mu < \beta$) لبقاء صافي تكلفة الهجوم موجباً. يعتمد هل يُحقق $\mu$ التوازني في لعبة التعدين هذا الشرط على العوائد النسبية للتعدين مقابل البريد المزعج. يُقارن معدِّن-مهاجم بين ربح التعدين الأمين (يتناسب مع $\mu$) وربح البريد المزعج (يتناسب مع حجم الرسائل، مُقيَّد ببنية تحتية المهاجم). بما أن التعدين الأمين يتناسب مع $\mu$ والبريد المزعج لا يتناسب، فإن المعدِّنين الكبار لديهم حافز أقل نسبياً للبريد المزعج مقارنةً بالصغار. يُشير ذلك إلى أن شرط $\mu < \beta$ يُعزِّز نفسه ذاتياً في الأنظمة النموذجية لقيم $\beta$ معقولة، وإن كان البرهان الرسمي يستلزم تحديداً صريحاً لدوال تكاليف التعدين والبريد المزعج --- مُؤجَّل للعمل المستقبلي.

### ٤.٥ الاستجابة للسعر بلا وسطاء

يحقق البروتوكول استقرار السعر دون وسطاء خارجيين بتحديد جميع المعاملات بوحدات العملة المشفرة مع السماح للمشاركين في السوق بتعديل مقادير الإحراق استناداً إلى تقييمات القيمة الخارجية:

قضية ١٢ (الاستجابة للسعر). مع ارتفاع السعر الخارجي للعملة المشفرة بعامل $\gamma$، سيُخفِّض المستخدمون العقلانيون مقادير إحراقهم بنحو $1/\gamma$، محافظين على تكاليف ثابتة مُقيَّمة بالفيات دون تغيير البروتوكول.

تُتيح هذه الآلية التكيف التلقائي مع تغيرات الأسعار الخارجية دون استلزام مدخلات وسيط أو قرارات حوكمة. خاصية اللا-وساطة متطلب تصميم مشترك مع الإطار النقدي التكيفي في ?؛ وقابلية قراءة الإنفاق الأمني لإثبات العمل التي تُتيح التصميم النقدي بلا وسطاء مُؤسَّسة في ?.

## ٦ تحليل الأمان

### ١.٦ الخصائص الأمانية التشفيرية

يوفر البروتوكول ضمانات أمانية تشفيرية قياسية:

مبرهنة ١٣ (سرية الرسائل). في ظل افتراض *Decisional Dffiie-Hellman*، محتوى الرسائل غير قابل للتمييز حسابياً عن العشوائي بالنسبة للخصوم الذين لا يملكون وصولاً إلى المفاتيح الخاصة للمُرسِل أو المستقبِل.

مبرهنة ١٤ (عدم إنكار الدفع). في ظل افتراض عدم قابلية التوقيعات الرقمية للتزوير، لا يستطيع الخصوم تزوير إثباتات الدفع دون وصول إلى المفتاح الخاص للدافع.

مبرهنة ١٥ (صحة الهوية). في ظل افتراض مقاومة التصادم لدالة التجزئة وعدم قابلية التوقيعات للتزوير، لا يستطيع الخصوم انتحال هوية المستخدمين الشرعيين دون وصول إلى مفاتيحهم الخاصة.

### ٢.٦ الأمان الاقتصادي ضد الخصوم العقلانيين

نُحلل الأمان ضد المهاجمين ذوي الدوافع الاقتصادية:

مبرهنة ١٦ (عدم ربحية هجوم البريد المزعج). لهجمات بريد مزعج حيث القيمة المستخرجة لكل رسالة ناجحة هي $v_{spam}$ واحتمال النجاح هو $p_{success}$، تكون هجمات البريد المزعج غير مربحة حين:

$$B > \frac{v_{spam} \cdot p_{success}}{1 - \beta\mu}$$

حيث $\beta$ نسبة الإحراق و$\mu$ نسبة قوة التعدين للمهاجم.

يوفر ذلك حدوداً ملموسة لاختيار المعاملات لضمان الأمان الاقتصادي.

### ٣.٦ ضمانات الخصوصية وإخفاء الهوية

رغم عدم توفير CashWeb إخفاءً تاماً للهوية (المفاتيح العامة تعمل كمعرِّفات مستمرة)، يوفر عدة حمايات خصوصية:

خصوصية محتوى الرسائل: جميع الرسائل مُشفَّرة شاملياً، مانعةً خوادم التتابع والمفاتيح من الوصول إلى المحتوى.

خصوصية أنماط التواصل: خوادم التتابع لا ترى إلا الرسائل المشفرة لمستخدميها المستضافين، مُقيِّدةً تحليل حركة المرور العالمي.

عدم ربط الأسماء المستعارة: يمكن للمستخدمين توليد أسماء مستعارة متعددة دون الكشف عن الروابط بينها، موفِّرةً إدارة هوية مجزَّأة.

قيود خصوصية البيانات الوصفية. خصوصية المحتوى لا تعني خصوصية البيانات الوصفية. معاملات الإحراق مرئية علناً على سلسلة الكتل؛ خادم تتابع يرصد سلسلة الكتل وحركة رسائله الواردة في آنٍ واحد يمكنه ربط توقيتات معاملات الإحراق بأوقات وصول الرسائل، مُحتمِلاً ربط هوية الدافع بالمُرسِل المستعار. تعلم خوادم المفاتيح إضافةً الخريطة من المفتاح العام إلى عنوان خادم التتابع. يوفر النظام خصوصية المحتوى وهوية المُرسِل المستعار، لكنه لا يوفر عدم الربط الكامل ضد خصم يتواطأ مع خادم التتابع أو المفاتيح. ينبغي للمستخدمين الذين يحتاجون إلى ضمانات إخفاء هوية أقوى التوجيه عبر شبكة خلط أو طبقة إخفاء مماثلة متعامدة مع هذا البروتوكول.

### ٤.٦ المرونة أمام هجمات التحالف

نأخذ بعين الاعتبار الهجمات من تحالفات المشاركين الخبثاء في الشبكة:

قضية ١٧ (توفر خادم التتابع في ظل تواطؤ جزئي). في ظل الشروط: (أ) يحتفظ المستخدمون باتصالات مع $k \geq 2$ من خوادم التتابع مُختارة باستقلالية؛ (ب) كل خادم تتابع خبيث باحتمال $f < 1/2$ باستقلالية؛ (ج) الخوادم الخبيثة تسقط الرسائل صامتةً: احتمال فشل التسليم لا يتجاوز $f^k$، ويقل عن الهدف $\delta$ لـ $k \geq \log(1/\delta)/\log(1/f)$.

ضمانات الاتفاق البيزنطي الرسمية (الأمان والحيوية تحت $f < 1/3$ عقدة بيزنطية) تنطبق على شبكة خوادم المفاتيح في ظل افتراضات *BFT* القياسية (?).

ملاحظة كمون خادم المفاتيح. يُحدث إجماع *BFT* عبر خوادم مفاتيح موزعة جغرافياً كموناً متأصلاً في الرحلة ذهاباً وإياباً --- نموذجياً 50--500 ملي ثانية لمجموعة موزعة عالمياً، مع حاجة إلى جولات متعددة للنهائية. تنتشر تسجيلات المفاتيح وتحديثاتها في شبكة خوادم المفاتيح خلال ثوانٍ. هذا مقبول لإدارة الهوية (التسجيل غير متكرر) لكنه يُقصي ضمانات إلغاء المفاتيح الآنية.

مبرهنة ١٨ (مقاومة تحالف خوادم المفاتيح). تحافظ شبكة خوادم المفاتيح على التوفر والاتساق طالما أقل من $1/3$ من خوادم المفاتيح أمينة، باستخدام تقنيات التسامح مع الأخطاء البيزنطية القياسية.

## ٧ اعتبارات التطبيق

### ١٠٧ صيغ رسائل البروتوكول وواجهات برمجية

يستثمر CashWeb مخازن البروتوكول ? لتسلسل الرسائل المهيكل وواجهات HTTP الـRESTful للتواصل الشبكي. تشمل صيغ الرسائل الرئيسية:
تسجيل الهوية:

```
IdentityRegistration message {
    bytes public_key = 1;
    string relay_address = 2;
    ProofOfPayment proof = 3;
    int64 timestamp = 4;
}
```

الرسالة المشفرة:

```
EncryptedMessage message {
    bytes sender_key = 1;
    bytes recipient_key = 2;
    bytes encrypted_content = 3;
    ProofOfPayment burn_proof = 4;
    int64 timestamp = 5;
}
```

إثبات الدفع:

```
ProofOfPayment message {
    bytes transaction_id = 1;
    bytes signature = 2;
    uint64 burn_amount = 3;
    bytes commitment_data = 4;
}
```

### ٢٠٧ اقتصاديات خادم التتابع وحوافزه

يجب أن تكون خوادم التتابع مستدامة اقتصادياً مع الحفاظ على خصوصية المستخدم. يتضمن النموذج الاقتصادي:
مصادر الإيرادات:

- رسوم تسجيل المستخدمين الجدد
- خدمات مميزة اختيارية (تخزين متزايد، تسليم أولوي)
- مشاركة رسوم المعاملات (لخوادم التتابع التي تشارك في التعدين)

هيكل التكاليف:

- تكاليف تخزين الرسائل المشفرة
- تكاليف النطاق الترددي لتسليم الرسائل
- التكاليف الحسابية للتحقق من الدفع

الديناميكيات التنافسية: يمكن للمستخدمين الانتقال بين خوادم التتابع باستخدام الواجهة البرمجية القياسية، مُفرِزاً ضغطاً سوقياً للتسعير التنافسي وجودة الخدمة.

### ٣.٧ إدارة الإحراق على الجانب العميلي وتجربة المستخدم

يجب على عملاء المستخدمين استخلاص تعقيد إدارة العملات المشفرة مع الحفاظ على الأمان:

الاختيار التلقائي لمقدار الإحراق: يمكن للعملاء تطبيق الاختيار التلقائي لمقدار الإحراق استناداً إلى:

- أولوية الرسالة (الرسائل العاجلة تستخدم معدلات إحراق أعلى)
- علاقة المستقبِل (إحراق أعلى للاتصال الأول)
- ازدحام الشبكة (تعديل ديناميكي استناداً إلى أوقات التسليم المُلاحَظة)

تكامل المحفظة: تكامل سلس مع محافظ العملات المشفرة عبر واجهات موحَّدة، بدعم لمعماريات المحافظ الحضنية وغير الحضنية.

حماية الخصوصية: يتضمن برنامج العميل حمايات مدمجة ضد تحليل حركة المرور وهجمات التوقيت عبر تجميع الرسائل والتأخيرات العشوائية.

### ٤.٧ التكامل مع البنية التحتية القائمة

البروتوكول مُصمَّم للنشر التدريجي جنباً إلى جنب مع أنظمة التواصل القائمة:

بوابة البريد الإلكتروني: يمكن جسر رسائل CashWeb إلى/من البريد الإلكتروني التقليدي عبر خدمات بوابة تعالج عمليات العملات المشفرة.

تكامل الويب: مكتبات JavaScript تُتيح التكامل المباشر لCashWeb في تطبيقات الويب عبر اتصالات WebSocket.

دعم الجوّال: حزم تطوير برامج جوّال أصلية توفر تطبيقات موفِّرة للبطارية مع إدارة مفاتيح مناسبة للبيئات الجوّالة.

## ٨ نموذج التهديد وتحليل الهجمات

### ١.٨ هجمات البريد المزعج والحجب

هجمات البريد المزعج المباشرة: يحاول الخصوم إرسال كميات كبيرة من الرسائل غير المرغوب فيها. تجعل آلية الإحراق هذا الهجوم مُكلِفاً: إرسال $N$ رسالة بريد مزعج بمقدار إحراق أدنى $B_{min}$ يكلف على الأقل $N \cdot B_{min}$.

هجمات استنزاف الموارد: يحاول الخصوم إغراق خوادم التتابع بطلبات معالجة الرسائل. يُقيِّد اشتراط الدفع حجم الهجوم، فيما يمكن لخوادم التتابع تطبيق تحديد معدل إضافي استناداً إلى مقادير الدفع.

هجمات استنزاف التخزين: يُرسِل الخصوم رسائل مدفوعة شرعية لملء تخزين خادم التتابع. يمكن لخوادم التتابع تطبيق سياسات إدارة التخزين بما في ذلك الحذف التلقائي للرسائل القديمة وطبقات التخزين المميزة.

### ٢.٨ الهجمات الاقتصادية

هجمات إعادة تدوير الرسوم: يحاول الخصوم الذين يسيطرون على بنية تحتية التعدين استعادة الأموال المُحرقة عبر رسوم المعاملات. يُقيِّد آلية الإحراق الجزئي للرسوم (القسم ??) الاستعادة بـ$\mu(\beta - 1)$.

هجمات سيبل: يُنشئ الخصوم هويات مزيفة كثيرة لتضخيم قدرة الهجوم. كل هوية تستلزم التزاماً اقتصادياً عبر رسوم التسجيل، مُنشِئةً تناسباً خطياً بين ميزانية الهجوم وسعة سيبل.

التلاعب بالسوق: يحاول الخصوم التلاعب بأسعار العملات المشفرة للتأثير على اقتصاديات الإحراق. يجعل التصميم الحالي من الوسطاء النظام مستجيباً لكن غير معتمد على التلاعب بالأسعار الخارجية.

### ٣.٨ هجمات البنية التحتية

رقابة خادم التتابع: خوادم التتابع الخبيثة ترفض تسليم الرسائل من مُرسِلين بعينهم. يمكن للمستخدمين اكتشاف الرقابة عبر تأكيدات التسليم والانتقال إلى خوادم تتابع بديلة.

التلاعب بخادم المفاتيح: يحاول الخصوم نشر معلومات هوية مزيفة. اشتراطات التوقيع التشفيري تمنع انتحال الهوية، فيما توفر شبكة خوادم المفاتيح الموزعة مرونة ضد اختراق خادم فردي.

تجزئة الشبكة: يحاول الخصوم عزل المستخدمين أو الخوادم عن الشبكة الأشمل. توفر المعمارية الموزعة مسارات تواصل متعددة، فيما توفر شبكة العملات المشفرة آلية تنسيق عالمية.

### ٤.٨ هجمات الخصوصية

تحليل حركة المرور: يرصد الخصوم حركة مرور الشبكة لاستنتاج أنماط التواصل. يحمي التشفير الشامل محتوى الرسائل، فيما يمكن للعملاء استخدام التوجيه البصلي أو تقنيات مماثلة للحماية الإضافية.

هجمات التوقيت: يُقارِن الخصوم أوقات الإرسال والاستقبال لتحديد علاقات التواصل. يمكن للعملاء تطبيق تأخيرات عشوائية وتجميع رسائل لتقليل الارتباط الزمني.

تحليل المدفوعات: يُحلِّل الخصوم معاملات سلسلة الكتل لربط المدفوعات بالرسائل. استخدام عناوين جديدة لكل معاملة إحراق وخلط معاملات مناسب يمكنه توفير خصوصية إضافية.

## ٩ التقييم والمناقشة

### ١.٩ نتائج التحليل النظري

يُثبت تحليلنا النظري عدة خصائص رئيسية:

قياسية مقاومة البريد المزعج: تتناسب تكلفة هجمات البريد المزعج خطياً مع حجم الهجوم، موفِّرةً ضمانات حماية يمكن التنبؤ بها. بمعدل إحراق أدنى $B_{min} = \$0.01$ لكل رسالة، يكلف إرسال مليون رسالة بريد مزعج على الأقل $10,000، عدا التكاليف التشغيلية.

إمكانية الوصول للمستخدمين الشرعيين: لمعدلات إحراق في نطاق $0.01 - $10 لكل رسالة، يظل الحاجز الاقتصادي ضئيلاً للمستخدمين الشرعيين (مماثل لتكاليف الرسائل القصيرة) مع توفير ردع جوهري للبريد المزعج.

فوائد أثر الشبكة: مع تزايد تبني الشبكة، تزداد قيمة الرسائل المشروعة بسرعة أكبر من كفاءة هجوم البريد المزعج، مُفرِزةً تغذية راجعة إيجابية لنمو النظام.

### ٢.٩ المقارنة مع الأنظمة القائمة

يُقارن الجدول ?? CashWeb مع مقاربات مكافحة البريد المزعج والرسائل القائمة:

| النظام | لامركزي | مكافحة البريد المزعج | الخصوصية | قابلية التوسع |
|---|---|---|---|---|
| البريد الإلكتروني (SMTP) | جزئي | ضعيف | ضعيف | عالي |
| Hashcash | نعم | متوسط | جيد | ضعيف |
| Matrix | جزئي | ضعيف | جيد | متوسط |
| Signal | لا | جيد | ممتاز | متوسط |
| CashWeb | نعم | جيد | جيد | عالي |

جدول ١: مقارنة أنظمة الرسائل عبر الخصائص الرئيسية

### ٣.٩ تجربة التطبيق

توفر الشبكة الاجتماعية Stamp تجربة نشر مبكرة لمفاهيم CashWeb. مواصفات البروتوكول في هذه الورقة هي الإتمام الرسمي لمعمارية جُرِّبت فيها الآليات الأساسية --- الإحراق للتعبير والتتابع الموزع وهوية خادم المفاتيح --- بشكل نموذجي في Stamp. تشمل ملاحظات النشر:

قبول المستخدم: يتكيف المستخدمون مع الرسائل القائمة على الإحراق دون احتكاك ملحوظ حين تظل مقادير الإحراق دون نحو 0.05$ لكل رسالة. المبالغ الأعلى تُنتج تردداً ملحوظاً للتواصل غير الرسمي.

تقليص البريد المزعج: متطلبات الإحراق الاقتصادية تردع البريد المزعج الآلي فعالياً، تكلفة كل رسالة تُدخل أرضيةً تتجاوز العائد المتوقع لحملات البريد المزعج النموذجية.

تكاليف البنية التحتية: يتناسب استهلاك موارد خادم التتابع تقريباً خطياً مع عدد المستخدمين في الاختبار الأولي. يُضيف التحقق من إثبات الدفع حملاً حسابياً معتدلاً نسبياً لتوجيه الرسائل الأساسي --- تهيمن عليه عمليات البحث في حالة سلسلة الكتل لا التحقق التشفيري.

هذه الملاحظات غير رسمية ومن نشر على نطاق صغير. تُؤكد صلاحية المقاربة لكنها لا تحل محل معايير الأداء الصارمة على نطاق واسع.

### ٤.٩ القيود والمقايضات

تنطوي مقاربة CashWeb على عدة مقايضات متأصلة:

الحواجز الاقتصادية: رغم ضآلة مقادير الإحراق للمستخدمين الشرعيين، قد تُنشئ حواجز للمستخدمين في المناطق المحرومة اقتصادياً. يمكن للعمل المستقبلي استكشاف معدلات إحراق متدرجة أو آليات إثبات قيمة بديلة.

الاعتماد على العملات المشفرة: يستلزم النظام الوصول إلى شبكات العملات المشفرة، مما قد يُقيِّد التبني في المناطق ذات الوصول المقيَّد أو بين المستخدمين غير المرتاحين للعملات المشفرة.

تعقيد الاسترداد: تستلزم سيناريوهات فقدان المفاتيح إجراءات استرداد أكثر تعقيداً من الأنظمة المركزية التقليدية، مما قد يُفرز تحديات في سهولة الاستخدام للمستخدمين غير التقنيين.

### ٥.٩ التوسعات المستقبلية والتطبيقات

يوفر بروتوكول CashWeb أساساً لتوسعات عديدة:

أنظمة السمعة: درجات سمعة المستخدم القائمة على تغذية راجعة من الرسائل المستقبَلة يمكن أن تُتيح تعديلات ديناميكية لمعدل الإحراق وتصفية محسَّنة للبريد المزعج.

أسواق المحتوى: يمكن توسيع آلية الإحراق إلى مدفوعات صغيرة للمحتوى، مُتيحةً نماذج اقتصادية جديدة لمشاركة المعلومات وتوزيع الوسائط.

تواصل إنترنت الأشياء: التواصل الآلي بين الأجهزة مع الدفع التلقائي يمكن أن يُتيح تطبيقات إنترنت الأشياء الجديدة حيث تدفع الأجهزة مقابل موارد النطاق الترددي والمعالجة.

الشبكات الاجتماعية اللامركزية: يوفر نظام النشر-الاشتراك بنية تحتية لمنصات الوسائط الاجتماعية اللامركزية كلياً مع توافق الحوافز الاقتصادية.

## ١٠ خاتمة

قدمنا CashWeb، مجموعة بروتوكولات شاملة تعالج مشاكل الحوافز الاقتصادية الجذرية المُحرِّكة للمركزية في أنظمة التواصل الإنترنتي. عبر المواصفات الرسمية لآليات مكافحة البريد المزعج بالإحراق للتعبير وتصميم البنية التحتية الموزعة وتحليل الأمان الاقتصادي، نُثبت أن تكامل العملات المشفرة يمكنه استعادة الرؤية الأصلية للتواصل الإنترنتي اللامركزي مع توفير مقاومة متفوقة للبريد المزعج مقارنةً بالمقاربات القائمة.

يوفر تأكيد البروتوكول على آليات مكافحة البريد المزعج الاقتصادية لا الحسابية ولا التنظيمية عدة مزايا: ضمانات حماية يمكن التنبؤ بها وقابلية التوسع للنشر العالمي والمقاومة لسباقات التسليح التقنية التي تعترض المقاربات الحسابية. تُؤكد تجربة التطبيق مع الشبكة الاجتماعية Stamp الجدوى العملية للمقاربة.

ينبغي للعمل المستقبلي التركيز على تقليص الحواجز الاقتصادية للمستخدمين المحرومين وتحسين سهولة إدارة المفاتيح واستكشاف التطبيقات بما يتجاوز الرسائل إلى مسائل التواصل والتنسيق الأخرى التي تعاني من ضغوط مركزية مماثلة.

الهدف الغائي لـCashWeb ليس الابتكار التقني فحسب، بل استعادة سيادة المستخدم على التواصل الرقمي --- تمكين العودة إلى مبادئ الإنترنت التأسيسية اللامركزية وتمكين المستخدم مع معالجة الحقائق الاقتصادية التي أدت إلى المركزية الأصلية.