□□□□□□□: संघीय स्पैम-रोधी संदेश और प्रकाशन-सदस्यता प्रणालियों के लिए क्रिप्टोकरेंसी-एकीकृत प्रोटोकॉल

□□□□□□□ □□□□□□□□□□
shammah.chancellor@proton.me
https://t.me/TheLotusNetwork

२१ फ़रवरी २०२६
□□□□□□□ 1.1

सारांश

हम □□□□□□□ प्रस्तुत करते हैं, एक व्यापक प्रोटोकॉल सूट जो केंद्रीकृत मॉडरेशन के बिना स्पैम-प्रतिरोधी संचार सक्षम करने के लिए क्रिप्टोकरेंसी-आधारित आर्थिक तंत्रों को संघीय संदेश अवसंरचना के साथ एकीकृत करता है। प्रोटोकॉल एक नवीन "बर्न-टू-स्पीक" स्पैम-रोधी तंत्र का उपयोग करता है जहाँ संदेश प्रेषक छोटे क्रिप्टोकरेंसी भुगतान संलग्न करते हैं जो क्रिप्टोग्राफिक रूप से सत्यापन योग्य हैं लेकिन विश्वसनीय मध्यस्थों की आवश्यकता नहीं है। हम तीन मुख्य घटकों के लिए औपचारिक विशिष्टताएँ प्रदान करते हैं: (1) एक भुगतान-प्रमाण (□□□) प्रोटोकॉल जो ऑन-चेन मूल्य को ऑफ-चेन क्रियाओं से जोड़ता है, (2) क्रिप्टोग्राफिक पहचान प्रबंधन के साथ संघीय संदेश, और (3) विषय-आधारित प्रसारण के लिए एक प्रकाशन-सदस्यता प्रणाली। हमारा आर्थिक विश्लेषण प्रदर्शित करता है कि बर्न तंत्र वैध संचार के लिए पहुँच बनाए रखते हुए स्पैम के विरुद्ध इष्टतम अवरोध उत्पन्न करता है। सिस्टम आर्किटेक्चर मौजूदा अवसंरचना के साथ निर्बाध एकीकरण सक्षम करने के लिए स्थापित वेब मानकों (□□□□/2, □□□□□□□□□□) और क्रिप्टोग्राफिक प्रिमिटिव का लाभ उठाता है। सैद्धांतिक विश्लेषण दर्शाता है कि प्रोटोकॉल नेटवर्क आकार में उपरैखिक रूप से स्केल होने वाली लागतों के साथ स्पैम प्रतिरोध प्राप्त करता है, जबकि अनुभवजन्य परिनियोजन रियल-टाइम संदेश अनुप्रयोगों के लिए व्यावहारिक व्यवहार्यता प्रदर्शित करता है।

1 परिचय

1.1 केंद्रीकरण की समस्या

इंटरनेट संचार प्रोटोकॉल के विकास से विकेंद्रीकरण और उपयोगिता के बीच एक मूलभूत तनाव प्रकट होता है। □□□□□□ ??, □□□□ ??, और □□□□ ?? जैसी प्रारंभिक प्रणालियाँ केंद्रीय प्राधिकरणों के बिना पीयर-टू-पीयर संचार सक्षम करने वाले संघीय नेटवर्क के रूप में डिज़ाइन की गई थीं। हालाँकि, इन प्रोटोकॉलों में निहित असममित लागत संरचना—जहाँ संदेश प्रसंस्करण लागत प्राप्तकर्ताओं द्वारा वहन की जाती है जबकि भेजने की लागत नगण्य रहती है—ने दुरुपयोग के लिए आर्थिक प्रोत्साहन उत्पन्न किए जो अंततः उपयोगकर्ताओं को केंद्रीकृत प्लेटफ़ॉर्मों की ओर ले गए।

2020 तक, संचार अवसंरचना का एकाग्रीकरण अभूतपूर्व स्तर पर पहुँच गया: □□□□□, □□□□□, और □□□□□□□□□ ने सामूहिक रूप से 85% ईमेल क्लाइंट बाजार हिस्सेदारी को नियंत्रित किया ?, जबकि □□□□□□□ ने 2 अरब से अधिक उपयोगकर्ताओं की रिपोर्ट की और □□□□□ ने 1.5 अरब सक्रिय खातों की सेवा की ?। यह केंद्रीकरण, उपयोगकर्ता सुविधा प्रदान करते हुए, सेंसरशिप, निगरानी, और एकल-विफलता बिंदुओं सहित प्रणालीगत जोखिम प्रस्तुत करता है जो वितरित इंटरनेट संचार की मूल दृष्टि से समझौता करते हैं।

1.2 आर्थिक स्पैम-रोधी तंत्र

विकेंद्रीकृत संदेश प्रणालियों में मूलभूत चुनौती केंद्रीकृत फ़िल्टरिंग के बिना स्पैम रोकथाम है। पारंपरिक दृष्टिकोण या तो गणनात्मक लागतों (?) या प्रतिष्ठा प्रणालियों पर निर्भर करते हैं जिनके लिए स्थायी पहचान सत्यापन आवश्यक है। जबकि ये तंत्र कुछ सुरक्षा प्रदान करते हैं, इनमें महत्वपूर्ण सीमाएँ हैं: गणनात्मक कार्य-प्रमाण आधुनिक हार्डवेयर त्वरण के साथ खराब रूप से स्केल होता है, और प्रतिष्ठा प्रणालियाँ नए उपयोगकर्ताओं के लिए प्रवेश बाधाएँ उत्पन्न करती हैं जबकि हमलों के प्रति संवेदनशील रहती हैं।

क्रिप्टोकरेंसी नेटवर्क, विशेष रूप से ?, के आगमन से एक नया दृष्टिकोण सक्षम होता है: आर्थिक भुगतान-प्रमाण तंत्र जहाँ संदेश प्रामाणिकता गणनात्मक कार्य के बजाय मूल्य विनाश के क्रिप्टोग्राफिक प्रमाण के माध्यम से सत्यापित होती है। यह दृष्टिकोण, मूल रूप से ? द्वारा “पुनः प्रयोज्य कार्य प्रमाण” ( ) के रूप में प्रस्तावित, अब विकेंद्रीकृत क्रिप्टोकरेंसी नेटवर्क का उपयोग करके विश्वसनीय मध्यस्थों के बिना कार्यान्वित किया जा सकता है।

1.3 योगदान

यह पेपर प्रस्तुत करता है, एक व्यापक प्रोटोकॉल सूट जो तीन प्राथमिक योगदानों के माध्यम से केंद्रीकरण समस्या का समाधान करता है:

1. औपचारिक भुगतान-प्रमाण प्रोटोकॉल: हम ऑन-चेन क्रिप्टोकरेंसी लेनदेन को ऑफ-चेन संदेश क्रियाओं से जोड़ने के लिए एक पूर्ण क्रिप्टोग्राफिक प्रोटोकॉल निर्दिष्ट करते हैं, जो विश्वसनीय पक्षों की आवश्यकता के बिना सत्यापन योग्य स्पैम-रोधी तंत्र सक्षम करता है।

2. संघीय अवसंरचना डिज़ाइन: हम पहचान प्रबंधन के लिए कीसर्वर और संदेश रूटिंग के लिए रिले सर्वर को संयोजित करने वाली एक स्केलेबल आर्किटेक्चर प्रस्तुत करते हैं, जो विकेंद्रीकरण बनाए रखते हुए व्यापक अपनाने के लिए आवश्यक लेनदेन मात्रा का समर्थन करने के लिए डिज़ाइन की गई है।

3. आर्थिक सुरक्षा विश्लेषण: हम सैद्धांतिक विश्लेषण प्रदान करते हैं जो प्रदर्शित करता है कि उचित बर्न-दर तंत्र स्पैम अवरोध और वैध उपयोगकर्ता पहुँच के बीच इष्टतम ट्रेड-ऑफ प्राप्त करते हैं, हमले की लागत और सफलता संभावनाओं पर औपचारिक सीमाओं के साथ।

प्रोटोकॉल को क्रिप्टोकरेंसी नेटवर्क ? पर परिनियोजन के लिए डिज़ाइन किया गया है, जो ? में निर्दिष्ट मूल्य-वाहक `OP_RETURN` आउटपुट और अनुकूली मौद्रिक नीति के लिए मूल समर्थन के साथ एक प्रूफ-ऑफ-वर्क चेन है। वर्तमान में परिचालन में है; आर्थिक स्टैक को पूर्ण करने वाला एप्लिकेशन-लेयर प्रोटोकॉल प्रदान करता है। प्रोटोकॉल स्थापित वेब मानकों का लाभ उठाता है और मौजूदा इंटरनेट अवसंरचना के साथ संगतता बनाए रखता है। सोशल नेटवर्क के साथ परिनियोजन अनुभव मुख्य दृष्टिकोण का प्रारंभिक सत्यापन प्रदान करता है।

यह पेपर एक श्रृंखला में तीसरा है। ? सैद्धांतिक आधार स्थापित करता है: किसी भी अनुमतिरहित सहमति प्रणाली में, संतुलन सुरक्षा व्यय जोखिम पर अपेक्षित मूल्य से आबद्ध है, और प्रूफ-ऑफ-वर्क विशिष्ट रूप से इस व्यय को प्रतिकूल रूप से प्रकट कार्य संकेत के माध्यम से प्रोटोकॉल-पठनीय बनाता है। ? मौद्रिक नीति निहितार्थ विकसित करता है, एक ओरेकल-मुक्त दो-लूप तंत्र निर्दिष्ट करता है जो अनुकूली पूँछ उत्सर्जन के लिए कार्य संकेत और अंतर्जात आपूर्ति सिंक के रूप में बर्न-टू-स्पीक का उपयोग करता है। वर्तमान पेपर बर्न-टू-स्पीक तंत्र को एक संघीय संदेश प्रोटोकॉल के रूप में पूरी तरह निर्दिष्ट करता है। फलस्वरूप, बर्न-टू-स्पीक स्टैक भर में दोहरी भूमिका निभाता है: एप्लिकेशन लेयर पर स्पैम अवरोध और प्रोटोकॉल लेयर पर अंतर्जात मौद्रिक आपूर्ति प्रबंधन।

1.4 पेपर संगठन

खंड ?? स्पैम-रोधी तंत्रों और संघीय संदेश में संबंधित कार्य की समीक्षा करता है। खंड ?? हमारा सिस्टम मॉडल और खतरे की धारणाएँ स्थापित करता है। खंड ?? मुख्य प्रोटोकॉल की औपचारिक विशिष्टताएँ प्रदान करता है। खंड ?? आर्थिक गुणों और स्पैम प्रतिरोध गारंटियों का विश्लेषण करता है। खंड ?? सुरक्षा गुणों और हमले प्रतिरोध की जाँच करता है। खंड ?? व्यावहारिक परिनियोजन विचारों की चर्चा करता है। खंड ?? सैद्धांतिक और अनुभवजन्य मूल्यांकन परिणाम प्रस्तुत करता है।

2 पृष्ठभूमि और संबंधित कार्य

2.1 आर्थिक स्पैम-रोधी तंत्र

वितरित सिस्टम अनुसंधान में स्पैम रोकथाम के लिए आर्थिक प्रोत्साहनों के उपयोग का समृद्ध इतिहास है। □□□□□ और □□□□ ? ने पहले ईमेल भेजने के लिए गणनात्मक कार्य-प्रमाण की आवश्यकता का प्रस्ताव किया, जिसे □□□□□□□□ ? में □□□-256 हैश प्रीइमेज पहेलियों के माध्यम से कार्यान्वित किया गया। सैद्धांतिक रूप से ध्वनि होने के बावजूद, गणनात्मक दृष्टिकोण कई व्यावहारिक सीमाओं से ग्रस्त हैं: (1) गणना की लागत विभिन्न हार्डवेयर में नाटकीय रूप से भिन्न होती है, जिससे असमानता उत्पन्न होती है, (2) आधुनिक □□□□ और □□□ त्वरण उपभोक्ता हार्डवेयर की तुलना में परिमाण के क्रम से तेज़ पहेलियाँ हल कर सकते हैं, और (3) इष्टतम कठिनाई स्तर के लिए गणनात्मक क्षमताओं के विकसित होने पर निरंतर समायोजन की आवश्यकता होती है।

□□□□□□ और □□□□□□□ ? ने हार्डवेयर लाभ कम करने के लिए मेमोरी-हार्ड फ़ंक्शन का उपयोग करने वाले कार्य-प्रमाण प्रणालियों का प्रस्ताव किया, लेकिन ये दृष्टिकोण अभी भी महत्वपूर्ण ऊर्जा व्यय की मांग करते हैं और संसाधन-बाधित उपकरणों के लिए बाधाएँ उत्पन्न करते हैं। वैकल्पिक प्रतिष्ठा-आधारित दृष्टिकोण ? को स्थायी पहचान प्रणालियों की आवश्यकता होती है जो गोपनीयता लक्ष्यों के साथ संघर्ष करती हैं और वैध नए उपयोगकर्ताओं के लिए उच्च प्रवेश बाधाएँ उत्पन्न करती हैं।

2.2 क्रिप्टोकरेंसी-आधारित अभिगम नियंत्रण

प्रोग्रामेबल क्रिप्टोकरेंसी नेटवर्क का उद्भव अधिक परिष्कृत आर्थिक तंत्र सक्षम करता है। □□□□□ □□ □□. ? ने अज्ञात माइक्रोपेमेंट के लिए □□□□□□ का उपयोग करने का प्रस्ताव किया, लेकिन उनका दृष्टिकोण इंटरएक्टिव प्रोटोकॉल की आवश्यकता है जो संदेश अनुप्रयोगों के लिए स्केल नहीं करते। भुगतान चैनलों ? और स्टेट चैनलों ? पर हालिया कार्य कम-विलंबता माइक्रोपेमेंट के लिए तंत्र प्रदान करते हैं, लेकिन पूर्व-वित्त पोषित चैनलों की आवश्यकता उपयोगिता बाधाएँ उत्पन्न करती है।

हमारा दृष्टिकोण मूल्य हस्तांतरण के बजाय अपुनर्प्राप्य मूल्य विनाश (“बर्निंग”) का उपयोग करके भिन्न है, प्राप्तकर्ता भुगतान अवसंरचना की आवश्यकता को समाप्त करते हुए दुरुपयोग के विरुद्ध मजबूत आर्थिक प्रोत्साहन बनाए रखता है।

2.3 संघीय संदेश प्रणालियाँ

संघीय संदेश आर्किटेक्चर व्यावहारिक स्केलेबिलिटी आवश्यकताओं के साथ विकेंद्रीकरण के लाभों को संतुलित करते हैं। □□□□ ? संघीय रियल-टाइम संदेश की व्यवहार्यता प्रदर्शित करता है, लेकिन आर्थिक स्पैम रोकथाम तंत्रों का अभाव है। □□□□□□ ? एंड-टू-एंड एन्क्रिप्शन के साथ आधुनिक संघीय संदेश प्रदान करता है, लेकिन केंद्रीकृत पहचान प्रदाताओं पर निर्भर करता है और दर सीमाओं से परे स्पैम-रोधी तंत्रों का अभाव है।

हालिया ब्लॉकचेन-आधारित संदेश प्रणालियों में □□□□□□ ? और □□□□□□□ ? शामिल हैं, जो विकेंद्रीकृत पहचान प्रबंधन प्रदान करते हैं लेकिन केंद्रीकरण को बढ़ावा देने वाली आर्थिक प्रोत्साहन समस्याओं का समाधान नहीं करते। हमारा दृष्टिकोण इन मूलभूत प्रोत्साहन असंरेखणों को संबोधित करने के लिए आर्थिक तंत्रों को सीधे प्रोटोकॉल डिज़ाइन में एकीकृत करता है।

3 सिस्टम मॉडल और आर्किटेक्चर

3.1 नेटवर्क प्रतिभागी

□□□□□□ नेटवर्क चार प्रकार के प्रतिभागियों से बना है:

परिभाषा 1 (नेटवर्क प्रतिभागी). माना $\mathcal{U} = \{u_1, u_2, \ldots, u_n\}$ उपयोगकर्ताओं का समुच्चय है, $\mathcal{R} = \{r_1, r_2, \ldots, r_m\}$ रिले सर्वरों का समुच्चय है, $\mathcal{K} = \{k_1, k_2, \ldots, k_\ell\}$ कीसर्वरों का समुच्चय है, और $\mathcal{T} = \{t_1, t_2, \ldots, t_p\}$ प्रकाशन-सदस्यता विषयों का समुच्चय है।

उपयोगकर्ता ($u_i \in \mathcal{U}$): अंतिम प्रतिभागी जो संदेश भेजते और प्राप्त करते हैं। प्रत्येक उपयोगकर्ता एक क्रिप्टोकरेंसी वॉलेट नियंत्रित करता है और भुगतान के क्रिप्टोग्राफिक प्रमाण उत्पन्न कर सकता है। उपयोगकर्ता क्लाइंट सॉफ़्टवेयर के माध्यम से नेटवर्क के साथ इंटरएक्ट करते हैं जो मुख्य सामग्री और भुगतान लेनदेन प्रबंधित करता है।

रिले सर्वर ($r_i \in \mathcal{R}$): संघीय सर्वर जो उपयोगकर्ताओं की ओर से एन्क्रिप्टेड संदेश संग्रहीत और अग्रेषित करते हैं। रिले सर्वर संदेश स्वीकार करने से पहले भुगतान प्रमाण सत्यापित करते हैं, जो स्पैम रक्षा की पहली पंक्ति प्रदान करते हैं। एंड-टू-एंड एन्क्रिप्शन के कारण उनके पास संदेश सामग्री तक पहुँच नहीं है।

कीसर्वर ($k_i \in \mathcal{K}$): वितरित सर्वर जो उपयोगकर्ता सार्वजनिक कुंजियों और संबद्ध मेटाडेटा का वैश्विक रजिस्ट्री बनाए रखते हैं। कीसर्वर उपयोगकर्ताओं को पूर्व संपर्क की आवश्यकता के बिना रिले सर्वर खोजने और सुरक्षित संचार चैनल स्थापित करने में सक्षम करते हैं।

विषय ($t_i \in \mathcal{T}$): प्रकाशन-सदस्यता प्रणाली में नामांकित चैनल जो प्रसारण संचार सक्षम करते हैं। विषय विकेंद्रीकृत हैं—कोई भी उपयोगकर्ता विषय बना सकता है और कोई भी रिले सर्वर सदस्यता सूचियों के आधार पर विषय संदेशों को प्रसारित कर सकता है।

3.2 खतरा मॉडल

हम एक बाइज़ेंटाइन प्रतिकूल वातावरण पर विचार करते हैं जहाँ प्रतिभागी प्रोटोकॉल विशिष्टताओं से मनमाने ढंग से विचलित हो सकते हैं। हमारे खतरे के मॉडल में शामिल हैं:

स्पैम हमलावर: प्रतिपक्षी जो संचार बाधित करने या नेटवर्क संसाधन बर्बाद करने के लिए बड़ी मात्रा में अनचाहे संदेश भेजने का प्रयास करते हैं। हम मानते हैं कि हमलावरों के पास महत्वपूर्ण लेकिन सीमित गणनात्मक और वित्तीय संसाधन हैं।

□□□□□ हमलावर: प्रतिपक्षी जो संदेश भेजने की क्षमता बढ़ाने या प्रतिष्ठा प्रणालियों में हेरफेर करने के लिए बड़ी संख्या में नकली पहचान बनाते हैं।

नेटवर्क अवसंरचना हमलावर: प्रतिपक्षी जो रिले सर्वर या कीसर्वर नियंत्रित करते हैं और सेंसरशिप, ट्रैफिक विश्लेषण, या सेवा-अस्वीकृति हमलों का प्रयास कर सकते हैं।

आर्थिक हमलावर: प्रतिपक्षी जो आर्थिक तंत्रों में हेरफेर करने का प्रयास करते हैं, जिसमें शुल्क पुनर्चक्रण हमले शामिल हैं जहाँ हमलावर खनन या सत्यापनकर्ता नियंत्रण के माध्यम से जले हुए फंड पुनर्प्राप्त करते हैं।

हम मानते हैं कि अंतर्निहित क्रिप्टोकरेंसी नेटवर्क (जैसे, □□□□□□□, □□□□□□) लेनदेन अपरिवर्तनीयता और दोहरे-खर्च हमलों के प्रतिरोध सहित मानक सुरक्षा गारंटी प्रदान करता है। हम क्रिप्टोकरेंसी नेटवर्क पर ही हमलों पर विचार नहीं करते।

3.3 डिज़ाइन सिद्धांत

प्रोटोकॉल डिज़ाइन कई प्रमुख सिद्धांतों का पालन करता है:

आर्थिक सुरक्षा: स्पैम-रोधी सुरक्षा गणनात्मक बाधाओं या केंद्रीकृत मॉडरेशन के बजाय आर्थिक प्रोत्साहनों से उत्पन्न होनी चाहिए, यह सुनिश्चित करते हुए कि हमले अत्यधिक महंगे हो जाएँ जबकि वैध उपयोग किफायती रहे।

डिज़ाइन द्वारा गोपनीयता: संदेश सामग्री और संचार पैटर्न नेटवर्क अवसंरचना प्रदाताओं सहित तृतीय पक्षों के लिए निजी रहने चाहिए।

संघीय स्केलेबिलिटी: सिस्टम को विकेंद्रीकरण गुण बनाए रखते हुए संघीय आर्किटेक्चर के माध्यम से वैश्विक पैमाने पर अपनाने का समर्थन करना चाहिए।

पश्चगामी संगतता: प्रोटोकॉल को अपनाने की बाधाओं को कम करने के लिए मौजूदा इंटरनेट अवसंरचना और विकास फ्रेमवर्क के साथ एकीकृत होना चाहिए।

4 मुख्य प्रोटोकॉल विशिष्टताएँ

4.1 भुगतान-प्रमाण (□□□) प्रोटोकॉल

भुगतान-प्रमाण प्रोटोकॉल क्रिप्टोग्राफिक सत्यापन सक्षम करता है कि एक विशिष्ट मात्रा में क्रिप्टोकरेंसी एक विशेष ऑफ-चेन क्रिया के संबंध में जलाई (स्थायी रूप से नष्ट) की गई है। पार्टियों के बीच मूल्य स्थानांतरित करने वाली पारंपरिक भुगतान प्रणालियों के विपरीत, □□□ प्रोटोकॉल मूल्य विनाश का सत्यापन योग्य प्रमाण बनाता है जिसे पुनर्प्राप्त या दोहरे-खर्च नहीं किया जा सकता।

परिभाषा 2 (भुगतान-प्रमाण प्रोटोकॉल). □□□ प्रोटोकॉल एक टपल (□□□□□, □□□□□□, □□□□□□) है जहाँ:

- □□□□□$(1^\lambda) \to pp$: सुरक्षा पैरामीटर λ के लिए सार्वजनिक पैरामीटर उत्पन्न करता है।
- □□□□□□$(sk, m, v) \to (\pi, \tau)$: गुप्त कुंजी sk, संदेश m, और मूल्य v दिए जाने पर, प्रमाण π और लेनदेन τ आउटपुट करता है।
- □□□□□□$(\pi, \tau, m, v) \to \{0, 1\}$: सत्यापित करता है कि लेनदेन τ मूल्य v जलाता है और संदेश m से क्रिप्टोग्राफिक रूप से जुड़ा हुआ है।

4.1.1 अव्ययनीय आउटपुट निर्माण

एल्गोरिदम निर्दिष्ट करने से पहले, हम मुख्य प्रिमिटिव परिभाषित करते हैं:

परिभाषा 3 (अव्ययनीय पता / □□_□□□□□□ आउटपुट). एक 32-बाइट प्रतिबद्धता मूल्य h_m दिए जाने पर, □□□□□□□□□□□□□□□□ आउटपुट स्क्रिप्ट ***OP_RETURN*** $\langle h_m \rangle$ को दर्शाता है। इस स्क्रिप्ट को मूल्य v भेजा गया एक लेनदेन आउटपुट सत्यापनीय रूप से नष्ट हो जाता है: (□) ***OP_RETURN*** आउटपुट व्यय इनपुट के रूप में सहमति-अमान्य हैं, इसलिए कोई भी पक्ष वैध व्यय लेनदेन नहीं बना सकता; (□□) अनुपालन नोड ऐसे आउटपुट को □□□□-मुक्त के रूप में चिह्नित करते हैं, स्थायी रूप से मूल्य को परिचलन से हटाते हैं। एक 32-बाइट □□□-256 हैश पेलोड 80-बाइट ***OP_RETURN*** डेटा सीमा के भीतर फिट होता है, जो 4-बाइट प्रोटोकॉल पहचानकर्ता और संस्करण फ़ील्ड के लिए स्थान छोड़ता है।

□□□□□□□ के इच्छित परिनियोजन लक्ष्य, □□□□□ नेटवर्क, सहमति नियम द्वारा गैर-शून्य-मूल्य OP_RETURN आउटपुट का समर्थन करता है, जो उपरोक्त को प्राथमिक निर्माण बनाता है। उन चेनों के लिए जो गैर-शून्य-मूल्य OP_RETURN आउटपुट प्रतिबंधित करती हैं (मानक □□□□□□□ नीति), एक वैकल्पिक निर्माण v को पते □2□□□(□□□□160(**0x0000...00**$\|h_m$)) पर भेजता है: एक वाक्यगत रूप से वैध □2□□□ पता जिसके लिए कोई निजी कुंजी मौजूद नहीं है (चूँकि □□□□160 का प्रीइमेज खोजना गणनात्मक रूप से अव्यावहारिक है)। यह प्राथमिक निर्माण की सहमति-प्रवर्तित अव्ययनीयता के बजाय संभाव्य अव्ययनीयता प्रदान करता है।

4.1.2 निर्माण

हमारा □□□ प्रोटोकॉल निर्माण फंड विनाश सुनिश्चित करते हुए प्रतिबद्धता डेटा एम्बेड करने के लिए □□□□□□□-शैली के लेनदेन में □□_□□□□□□ आउटपुट का लाभ उठाता है:

□□□□□□□□□ 1 भुगतान-प्रमाण निर्माण

□□□□□□□: संदेश m, बर्न राशि v, उपयोगकर्ता गुप्त कुंजी sk
□□□□□□: प्रमाण π और लेनदेन τ
$pk \leftarrow$ □□□□□□□□□□□□□□(sk)
$h_m \leftarrow$ □□□□$(m \| pk \|$ □□□□□□□□□□$())$
$addr_{burn} \leftarrow$ □□□□□□□□□□□□□□□□□□□□(h_m)
$\tau \leftarrow$ □□□□□□□□□□□□□□□□□□□□$(sk, v, addr_{burn}, h_m)$
$\sigma \leftarrow$ □□□□$(sk, \tau \| m)$
$\pi \leftarrow (\tau, \sigma, m, v, pk)$
□□□□□□ π, τ

निर्माण कई महत्वपूर्ण गुण सुनिश्चित करता है:

अपुनर्प्राप्यता: $addr_{burn}$ पर भेजे गए फंड सिद्ध रूप से अव्ययनीय हैं क्योंकि पता बिना ज्ञात प्रीइमेज वाले हैश से व्युत्पन्न है।

अद्वितीयता: प्रत्येक संदेश-भुगतान जोड़ी एक अद्वितीय प्रतिबद्धता उत्पन्न करती है जिसे विभिन्न संदेशों के लिए पुनः उपयोग नहीं किया जा सकता।

सत्यापनीयता: कोई भी पक्ष ब्लॉकचेन पर लेनदेन की जाँच करके और क्रिप्टोग्राफिक हस्ताक्षरों को मान्य करके प्रमाण सत्यापित कर सकता है।

4.2 पहचान प्रबंधन और कुंजी पंजीकरण

□□□□□□ में उपयोगकर्ता सार्वजनिक-कुंजी क्रिप्टोग्राफी पर आधारित छद्मनाम पहचान बनाए रखते हैं। प्रत्येक पहचान में एक कुंजी जोड़ी (sk, pk) होती है जहाँ सार्वजनिक कुंजी उपयोगकर्ता के वैश्विक पहचानकर्ता के रूप में कार्य करती है।

4.2.1 पहचान पंजीकरण

नई पहचान निम्नलिखित प्रोटोकॉल के माध्यम से कीसर्वर नेटवर्क के साथ पंजीकृत होती हैं:

□□□□□□□□□ 2 पहचान पंजीकरण

□□□□□□□: उपयोगकर्ता कुंजी जोड़ी (sk, pk), रिले सर्वर पता $addr_{relay}$, पंजीकरण शुल्क v_{reg}
□□□□□□: कीसर्वर नेटवर्क में पहचान रिकॉर्ड
$metadata \leftarrow \{\text{“}relay\text{”} : addr_{relay}, \text{“}timestamp\text{”} :$ □□□$()\}$
$(\pi_{reg}, \tau_{reg}) \leftarrow$ □□□.□□□□□□□$(sk, metadata, v_{reg})$
$record \leftarrow (pk, metadata, \pi_{reg})$
□□□ □□□□ □□□□□□□□□□ $k_i \in \mathcal{K}$ □□
  □□□□$(record, k_i)$
□□□ □□□

4.2.2 कुंजी रोटेशन और पुनर्प्राप्ति

प्रोटोकॉल कुंजी समझौते या हानि से पुनर्प्राप्ति सक्षम करने के लिए कुंजी रोटेशन का समर्थन करता है। उपयोगकर्ता पुनर्प्राप्ति कुंजी पूर्व-पंजीकृत कर सकते हैं या निर्बाध रोटेशन के लिए पदानुक्रमिक नियतात्मक कुंजी व्युत्पत्ति का उपयोग कर सकते हैं:

□□□□□□□□□ 3 कुंजी रोटेशन

□□□□□□□: वर्तमान कुंजी जोड़ी (sk_{old}, pk_{old}), नई कुंजी जोड़ी (sk_{new}, pk_{new}), रोटेशन शुल्क v_{rot}
□□□□□□: अद्यतन पहचान रिकॉर्ड

$rotation\_msg \leftarrow (pk_{old}, pk_{new}, \square\square\square())$
$\sigma_{old} \leftarrow \square\square\square\square(sk_{old}, rotation\_msg)$
$\sigma_{new} \leftarrow \square\square\square\square(sk_{new}, rotation\_msg)$
$(\pi_{rot}, \tau_{rot}) \leftarrow \square\square\square.\square\square\square\square\square\square(sk_{new}, rotation\_msg, v_{rot})$
$update \leftarrow (pk_{old}, pk_{new}, \sigma_{old}, \sigma_{new}, \pi_{rot})$
□□□ □□□□ □□□□□□□□□□ $k_i \in \mathcal{K}$ □□
  □□□□$(update, k_i)$
□□□ □□□

4.3 बर्न-टू-सेंड के साथ संघीय संदेश

मुख्य संदेश प्रोटोकॉल क्रिप्टोग्राफिक संदेश वितरण को आर्थिक स्पैम-रोधी सुरक्षा के साथ एकीकृत करता है। संदेश एंड-टू-एंड एन्क्रिप्टेड हैं और प्रेषक प्रतिबद्धता प्रदर्शित करने के लिए भुगतान-प्रमाण शामिल करते हैं।

□□□□□□□□□ 4 संदेश भेजने का प्रोटोकॉल

□□□□□□□: प्राप्तकर्ता सार्वजनिक कुंजी pk_{recv}, संदेश सामग्री $content$, बर्न राशि v_{msg}
□□□□□□: प्राप्तकर्ता के रिले सर्वर को वितरित संदेश

$(pk_{sender}, sk_{sender}) \leftarrow \square\square\square\square\square\square\square\square\square\square()$
$relay_{recv} \leftarrow \square\square\square\square\square\square\square\square\square\square\square\square\square\square\square\square(pk_{recv})$
$k_{shared} \leftarrow \square\square\square\square(sk_{sender}, pk_{recv})$
$msg_{encrypted} \leftarrow \square\square\square\square\square\square\square(k_{shared}, content)$
$message \leftarrow (pk_{sender}, pk_{recv}, msg_{encrypted}, \square\square\square\square\square\square\square\square\square\square())$
$(\pi_{msg}, \tau_{msg}) \leftarrow \square\square\square.\square\square\square\square\square\square\square(sk_{sender}, message, v_{msg})$
$delivery\_req \leftarrow (message, \pi_{msg})$
□□□□□□□□□$(delivery\_req, relay_{recv})$

4.3.1 संदेश सत्यापन और संग्रहण

रिले सर्वर संग्रहण से पहले आने वाले संदेशों को सत्यापित करते हैं:

□□□□□□□□□ 5 रिले सर्वर द्वारा संदेश सत्यापन

□□□□□□□: संदेश वितरण अनुरोध $delivery\_req = (message, \pi_{msg})$
□□□□□□: संदेश स्वीकृत या अस्वीकृत

$(message, \pi_{msg}) \leftarrow delivery\_req$
$(pk_{sender}, pk_{recv}, msg_{encrypted}, timestamp) \leftarrow message$
□□ □□□□.□□□□□□□$(\pi_{msg}, message) \neq 1$ □□□□
  □□□□□□ "अस्वीकृत: अमान्य भुगतान प्रमाण"
□□□ □□
□□ □□□□□□□□□□□$(\pi_{msg}) < v_{min}$ □□□□
  □□□□□□ "अस्वीकृत: अपर्याप्त बर्न राशि"
□□□ □□
□□□□□□□□□□□□□□$(message, \pi_{msg})$
□□□□□□ "स्वीकृत"

4.4 बर्न-टू-ब्रॉडकास्ट के साथ प्रकाशन-सदस्यता

प्रकाशन-सदस्यता प्रणाली विषय-आधारित प्रसारण का समर्थन करने के लिए संदेश प्रोटोकॉल का विस्तार करती है। उपयोगकर्ता विषयों की सदस्यता ले सकते हैं और उन विषयों पर पोस्ट किए गए सभी संदेश प्राप्त कर सकते हैं, जिसमें संदेश प्राथमिकता बर्न राशि द्वारा निर्धारित होती है।

परिभाषा 4 (विषय सदस्यता). एक विषय सदस्यता एक टपल (u_i, t_j, r_k) है जो दर्शाता है कि उपयोगकर्ता u_i रिले सर्वर r_k के माध्यम से विषय t_j की सदस्यता लेता है।

□□□□□□□□□ 6 विषय संदेश प्रसारण

□□□□□□□: विषय पहचानकर्ता $topic\_id$, संदेश सामग्री $content$, बर्न राशि $v_{broadcast}$
□□□□□□: सभी विषय सदस्यों को वितरित संदेश

$(pk_{sender}, sk_{sender}) \leftarrow$ □□□□□□□□□□□□()
$topic\_msg \leftarrow (pk_{sender}, topic\_id, content,$ □□□□□□□□□□())
$(\pi_{broadcast}, \tau_{broadcast}) \leftarrow$ □□□.□□□□□□□$(sk_{sender}, topic\_msg, v_{broadcast})$
$broadcast\_req \leftarrow (topic\_msg, \pi_{broadcast})$
□□□ □□□□ □□□□□ □□□□□□ $r_i \in \mathcal{R}$ □□
  □□□□□□□□□□□□□□□□□□□□□□□□□□□□□$(broadcast\_req, topic\_id, r_i)$
□□□ □□□

प्रसारण तंत्र में बर्न राशि के आधार पर प्राथमिकता-आधारित संदेश क्रम और दर सीमा शामिल है:

□□□□□□□□□ 7 विषय संदेश प्राथमिकताकरण

□□□□□□□: बर्न राशियों $\{v_1, v_2, \ldots, v_k\}$ के साथ विषय संदेशों का समुच्चय $M = \{m_1, m_2, \ldots, m_k\}$
□□□□□□: प्राथमिकताकृत संदेश वितरण अनुसूची

$priority\_queue \leftarrow$ □□□□□□□□□□□()
□□□ □□□□ □□□□□□□□ $m_i \in M$ □□
  $priority_i \leftarrow f(v_i)$ जहाँ f एकदिष्ट वर्धमान है
  □□□□□□□$(priority\_queue, m_i, priority_i)$
□□□ □□□
□□□□□ □□□□□□□□□$(priority\_queue)$ □□□ □□□□□□□□□□□□□□□□□□□□□() □□
  $m_{next} \leftarrow$ □□□□□□□$(priority\_queue)$
  □□□□□□□□□□□□□□□□(m_{next})
□□□ □□□□□

5 आर्थिक विश्लेषण और स्पैम-रोधी गुण

5.1 बर्न-दर अर्थशास्त्र और संतुलन विश्लेषण

बर्न-टू-स्पीक तंत्र की प्रभावशीलता ऐसी बर्न दरें स्थापित करने पर निर्भर करती है जो स्पैम हमलों को आर्थिक रूप से अव्यावहारिक बनाती हैं जबकि वैध उपयोगकर्ताओं के लिए पहुँच बनाए रखती हैं। हम इसे एक गेम-थियोरेटिक संतुलन समस्या के रूप में मॉडल करते हैं, □□□□□□ (?) के इष्टतम अवरोध ढाँचे का अनुसरण करते हुए, एक विकेंद्रीकृत सेटिंग में विस्तारित जहाँ प्रवर्तन मूल्य विनाश के क्रिप्टोग्राफिक प्रमाण के माध्यम से कार्यान्वित होता है।

परिभाषा 5 (स्पैम हमले की लागत). प्रति संदेश बर्न राशि B के साथ N स्पैम संदेश भेजने का प्रयास करने वाले हमलावर के लिए, कुल हमले की लागत है:

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

जहाँ $C_{operational}(N)$ गणनात्मक और अवसंरचना लागतों का प्रतिनिधित्व करता है।

परिभाषा 6 (वैध उपयोगकर्ता उपयोगिता). बर्न राशि B के साथ एक संदेश भेजने से एक वैध उपयोगकर्ता की उपयोगिता है:

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

जहाँ $V_{communication}$ सफल संदेश वितरण से प्राप्त मूल्य है और $C_{friction}(B)$ उपयोगिता लागतों का प्रतिनिधित्व करता है।

इष्टतम बर्न दर B^* स्पैम व्यवहार्यता को न्यूनतम करते हुए वैध उपयोगकर्ता अपनाने को अधिकतम करती है। एक सुगम रूप प्राप्त करने के लिए, हम कार्यात्मक रूप निर्दिष्ट करते हैं:

परिभाषा 7 (सामाजिक कल्याण फ़ंक्शन). परिभाषित करें:

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

जहाँ $U_0 > 0$ एक प्रतिनिधि वैध उपयोगकर्ता के लिए प्रति संदेश मूल्य है, $\alpha > 0$ बर्न की उनकी सीमांत लागत है, $D > 0$ प्रति स्पैम संदेश सामाजिक क्षति है, और $\sigma > 0$ इकाई बर्न लागत पर स्पैम मात्रा है। αB पद उच्च बर्न से वैध-उपयोगकर्ता अधिशेष में कमी को दर्शाता है; $D\sigma/B$ पद कुल स्पैम क्षति को दर्शाता है, जो तर्कसंगत स्पैमर अर्थशास्त्र के तहत $1/B$ के रूप में घटता है।

इस विशिष्टता के अंतर्गत, इष्टतम बर्न दर है:

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

बंद रूप में अवरोध और पहुँच को संतुलित करना। उच्च सामाजिक स्पैम क्षति D या उच्च स्पैम प्रवृत्ति σ उच्च B^* की मांग करती है; निम्न वैध-उपयोगकर्ता सीमांत लागत α भी B^* बढ़ाती है।

प्रमेय 8 (इष्टतम बर्न दर). इष्टतम बर्न दर B^* संतुष्ट करती है:

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

जहाँ α स्पैम की सामाजिक लागत का प्रतिनिधित्व करता है और $E[N_{spam}(B)]$ बर्न दर B पर स्पैम संदेशों की अपेक्षित संख्या है।

प्रमाण. अस्तित्व। जब $B \to 0$, स्पैम अप्रतिबंधित है और $W(B) \to -\infty$। जब $B \to \infty$, वैध उपयोगकर्ता मूल्य से बाहर हो जाते हैं और $W(B) \to -\infty$। चूँकि W सतत है, अधिकतम वाले किसी भी सघन उपअंतराल पर चरम मूल्य प्रमेय द्वारा एक आंतरिक अधिकतम मौजूद है।

प्रथम-क्रम शर्त। एक आंतरिक इष्टतम B^* पर, कथित शर्त अवकलन द्वारा संतुष्ट होती है।

अद्वितीयता अतिरिक्त धारणा के अंतर्गत प्राप्त होती है कि $W(B)$ कड़ाई से अवतल है, जो तब संतुष्ट होती है जब वैध उपयोगिता B में अवतल है और स्पैम मात्रा $1/B$ में उत्तल है—इष्टतम अवरोध साहित्य में मानक धारणाएँ (?)। □

5.2 □□□□□ प्रतिरोध परिमाणीकरण

बर्न तंत्र अंतर्निहित □□□□□ प्रतिरोध प्रदान करता है क्योंकि प्रत्येक पहचान को केवल गणनात्मक कार्य के बजाय आर्थिक प्रतिबद्धता की आवश्यकता होती है:

प्रस्ताव 9 (□□□□□ हमले की सीमाएँ). बजट $\mathcal{B}$ वाले हमलावर के लिए, □□□□□ पहचान की अधिकतम संख्या निम्न द्वारा सीमित है:

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

जहाँ v_{reg} पहचान पंजीकरण शुल्क है और k प्रति पहचान अपेक्षित संदेशों की संख्या है।

यह सीमा प्रदर्शित करती है कि □□□□□ हमले गणनात्मक संसाधनों के बजाय हमलावर के बजट के साथ रैखिक रूप से स्केल होते हैं, अनुमानित प्रतिरोध गारंटी प्रदान करते हैं।

5.3 शुल्क पुनर्चक्रण हमला रोकथाम

एक महत्वपूर्ण सुरक्षा विचार खनन या सत्यापन अवसंरचना के नियंत्रण के माध्यम से हमलावरों को जले हुए फंड पुनर्प्राप्त करने से रोकना है। हम आंशिक शुल्क बर्निंग के माध्यम से इसे संबोधित करते हैं:

परिभाषा 10 (आंशिक शुल्क बर्न तंत्र). शुल्क F वाले प्रत्येक लेनदेन के लिए, एक अंश $\beta \in (0, 1]$ जलाया जाता है जबकि शेष $(1 - \beta)F$ खनिकों को भुगतान किया जाता है:

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

जहाँ $B_{explicit}$ स्पष्ट बर्न राशि है और F लेनदेन शुल्क है।

पैरामीटर β ? में अनुकूली मौद्रिक नीति ढाँचे के साथ साझा किया गया है, जहाँ समान शुल्क बर्न अंश एक साथ एक अंतर्जात आपूर्ति अपस्फीति तंत्र के रूप में कार्य करता है। स्पैम-रोधी और मौद्रिक भूमिकाएँ इस प्रकार संरचनात्मक रूप से एकीकृत हैं: एकल प्रोटोकॉल स्थिरांक β एप्लिकेशन-लेयर हमले-लागत तल और मौद्रिक-लेयर आपूर्ति प्रबंधन दोनों प्रदान करता है।

प्रमेय 11 (शुल्क पुनर्चक्रण प्रतिरोध). आंशिक शुल्क बर्न तंत्र के तहत, नेटवर्क हैश पावर के अंश μ को नियंत्रित करने वाला हमलावर अपनी हमले लागत का अधिकतम $(1 - \beta)\mu$ पुनर्प्राप्त कर सकता है, यह सुनिश्चित करते हुए कि $\mu < \beta$ के लिए शुद्ध हमले की लागत सकारात्मक रहती है।

संतुलन विश्लेषण। प्रमेय ?? एक पर्याप्त शर्त ($\mu < \beta$) देता है कि शुद्ध हमले की लागत सकारात्मक रहे। खनन खेल में संतुलन μ इस शर्त को संतुष्ट करता है या नहीं, यह खनन बनाम स्पैमिंग के सापेक्ष रिटर्न पर निर्भर करता है। एक खनिक-स्पैमर ईमानदार खनन लाभ (μ के समानुपाती) की तुलना स्पैम लाभ (संदेश मात्रा के समानुपाती, हमलावर अवसंरचना द्वारा सीमित) से करता है। चूँकि ईमानदार खनन μ के साथ स्केल होता है और स्पैम नहीं करता, बड़े खनिकों के पास छोटे खनिकों की तुलना में स्पैम करने के लिए अपेक्षाकृत कम प्रोत्साहन है। यह सुझाव देता है कि उचित β के लिए विशिष्ट व्यवस्थाओं में $\mu < \beta$ शर्त स्व-प्रवर्तक है, हालाँकि एक औपचारिक प्रमाण के लिए खनन और स्पैमिंग लागत कार्यों की स्पष्ट विशिष्टता की आवश्यकता है—भविष्य के कार्य के लिए स्थगित।

5.4 ओरेकल-मुक्त मूल्य प्रतिक्रियाशीलता

प्रोटोकॉल बाह्य ओरेकल के बिना मूल्य स्थिरता प्राप्त करता है, सभी पैरामीटरों को क्रिप्टोकरेंसी इकाइयों में अंकित करके जबकि बाजार प्रतिभागियों को बाहरी मूल्य मूल्यांकन के आधार पर बर्न राशि समायोजित करने की अनुमति देता है:

प्रस्ताव 12 (मूल्य प्रतिक्रियाशीलता). जैसे-जैसे क्रिप्टोकरेंसी की बाहरी कीमत γ कारक से बढ़ती है, तर्कसंगत उपयोगकर्ता अपनी बर्न राशि लगभग $1/\gamma$ से कम करेंगे, प्रोटोकॉल परिवर्तनों के बिना स्थिर फिएट-अंकित लागत बनाए रखते हैं।

यह तंत्र ओरेकल इनपुट या शासन निर्णयों की आवश्यकता के बिना बाहरी मूल्य परिवर्तनों के लिए स्वचालित समायोजन सक्षम करता है। ओरेकल-मुक्त गुण ? के अनुकूली मौद्रिक ढाँचे के साथ साझा एक डिज़ाइन आवश्यकता है; □□□ सुरक्षा व्यय की पठनीयता जो ओरेकल-मुक्त मौद्रिक डिज़ाइन संभव बनाती है ? में स्थापित की गई है।

6 सुरक्षा विश्लेषण

6.1 क्रिप्टोग्राफिक सुरक्षा गुण

प्रोटोकॉल मानक क्रिप्टोग्राफिक सुरक्षा गारंटी प्रदान करता है:

प्रमेय 13 (संदेश गोपनीयता). निर्णायक □□□□□-□□□□□□ धारणा के तहत, प्रेषक या प्राप्तकर्ता निजी कुंजियों तक पहुँच के बिना प्रतिपक्षियों के लिए संदेश सामग्री यादृच्छिक से गणनात्मक रूप से अप्रभेद्य है।

प्रमेय 14 (भुगतान गैर-अस्वीकृति). डिजिटल हस्ताक्षरों की जाली-असंभाव्यता के तहत, भुगतानकर्ता की निजी कुंजी तक पहुँच के बिना प्रतिपक्षियों द्वारा भुगतान प्रमाण जाली नहीं किए जा सकते।

प्रमेय 15 (पहचान प्रामाणिकता). हैश फ़ंक्शन की टकराव प्रतिरोधकता और हस्ताक्षरों की जाली-असंभाव्यता के तहत, प्रतिपक्षी उनकी निजी कुंजियों तक पहुँच के बिना वैध उपयोगकर्ताओं का प्रतिरूपण नहीं कर सकते।

6.2 तर्कसंगत प्रतिपक्षियों के विरुद्ध आर्थिक सुरक्षा

हम आर्थिक रूप से प्रेरित हमलावरों के विरुद्ध सुरक्षा का विश्लेषण करते हैं:

प्रमेय 16 (स्पैम हमले की लाभहीनता). स्पैम हमलों के लिए जहाँ प्रति सफल संदेश निकाला गया मूल्य v_{spam} है और सफलता की संभावना $p_{success}$ है, स्पैम हमले लाभहीन हैं जब:

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

जहाँ β बर्न अंश है और μ हमलावर की खनन शक्ति अंश है।

यह आर्थिक सुरक्षा सुनिश्चित करने के लिए पैरामीटर चयन के लिए ठोस सीमाएँ प्रदान करता है।

6.3 गोपनीयता और गुमनामी गारंटी

जबकि □□□□□□ पूर्ण गुमनामी प्रदान नहीं करता (सार्वजनिक कुंजी स्थायी पहचानकर्ता के रूप में कार्य करती हैं), यह कई गोपनीयता सुरक्षाएँ प्रदान करता है:

संदेश सामग्री गोपनीयता: सभी संदेश एंड-टू-एंड एन्क्रिप्टेड हैं, रिले सर्वर और कीसर्वर को सामग्री तक पहुँच से रोकते हैं।

संचार पैटर्न गोपनीयता: रिले सर्वर केवल उनके होस्ट किए गए उपयोगकर्ताओं के एन्क्रिप्टेड संदेश देखते हैं, वैश्विक ट्रैफिक विश्लेषण को सीमित करते हैं।

छद्मनाम अनलिंक करने योग्यता: उपयोगकर्ता उनके बीच संबंध प्रकट किए बिना कई छद्मनाम उत्पन्न कर सकते हैं, विभाजित पहचान प्रबंधन प्रदान करते हैं।

मेटाडेटा गोपनीयता सीमाएँ। सामग्री गोपनीयता का अर्थ मेटाडेटा गोपनीयता नहीं है। बर्न लेनदेन ब्लॉकचेन पर सार्वजनिक रूप से दृश्यमान हैं; एक रिले सर्वर जो ब्लॉकचेन और अपने स्वयं के आने वाले संदेश ट्रैफिक दोनों का अवलोकन करता है, बर्न लेनदेन समय को संदेश आगमन समय के साथ सहसंबंधित कर सकता है, संभावित रूप से भुगतानकर्ता पहचान को छद्मनाम प्रेषक से जोड़ता है। कीसर्वर अतिरिक्त रूप से सार्वजनिक कुंजी से रिले सर्वर पते की मैपिंग जानते हैं। सिस्टम सामग्री गोपनीयता और छद्मनाम प्रेषक पहचान प्रदान करता है, लेकिन मिलीभगत रिले-सर्वर या कीसर्वर प्रतिपक्षी के विरुद्ध पूर्ण अनलिंक करने योग्यता नहीं। मजबूत गुमनामी गारंटी की आवश्यकता वाले उपयोगकर्ताओं को इस प्रोटोकॉल के लिए ऑर्थोगोनल एक मिक्सनेट या समान गुमनामीकरण परत के माध्यम से रूट करना चाहिए। यह वर्तमान डिज़ाइन की एक ज्ञात सीमा है; मजबूत गोपनीयता गुण भविष्य के कार्य के लिए छोड़े गए हैं।

6.4 गठबंधन हमलों के लिए लचीलापन

हम दुर्भावनापूर्ण नेटवर्क प्रतिभागियों के गठबंधन द्वारा हमलों पर विचार करते हैं:

प्रस्ताव 17 (आंशिक मिलीभगत के तहत रिले सर्वर उपलब्धता). शर्तों के तहत: (□) उपयोगकर्ता स्वतंत्र रूप से चुने गए $k \geq 2$ रिले सर्वरों से कनेक्शन बनाए रखते हैं, (□□) प्रत्येक रिले सर्वर स्वतंत्र रूप से $f < 1/2$ संभावना के साथ दुर्भावनापूर्ण है, (□□□) दुर्भावनापूर्ण सर्वर संदेश चुपचाप गिराते हैं: वितरण विफलता की संभावना अधिकतम f^k है, $k \geq \square\square\square(1/\delta)/\ \square\square\square(1/f)$ के लिए लक्ष्य δ से नीचे गिरती है।

औपचारिक बाइज़ेंटाइन समझौता गारंटी (मानक □□□ धारणाओं (?) के तहत $f < 1/3$ बाइज़ेंटाइन नोड के साथ सुरक्षा और जीवंतता) कीसर्वर नेटवर्क पर लागू होती हैं। रिले लेयर को उपलब्धता की आवश्यकता है, स्थिरता की नहीं; अतिरेक वितरण पर्याप्त है।

कीसर्वर विलंबता नोट। भौगोलिक रूप से वितरित कीसर्वरों में □□□ सहमति अंतर्निहित राउंड-ट्रिप विलंबता उत्पन्न करती है—वैश्विक वितरित सेट के लिए आमतौर पर 50–500 □□, अंतिमता के लिए कई राउंड की आवश्यकता होती है। कुंजी पंजीकरण और अपडेट इसलिए कीसर्वर नेटवर्क में सेकंड के क्रम पर प्रचारित होते हैं। यह पहचान प्रबंधन के लिए स्वीकार्य है (पंजीकरण अनिच्छित है) लेकिन रियल-टाइम कुंजी निरसन गारंटी को रोकता है। रिले सर्वरों को नए पंजीकृत कुंजियों पर भरोसा करने से पहले एक छोटी अनुग्रह अवधि लागू करनी चाहिए, और उच्च-मूल्य या प्रथम-संपर्क इंटरेक्शन के लिए कुंजी ताज़गी जाँच लागू करनी चाहिए।

प्रमेय 18 (कीसर्वर गठबंधन प्रतिरोध). कीसर्वर नेटवर्क उपलब्धता और स्थिरता बनाए रखता है जब तक $f < 1/3$ कीसर्वर ईमानदार हैं, मानक बाइज़ेंटाइन दोष सहिष्णुता तकनीकों का उपयोग करते हुए।

7 कार्यान्वयन संबंधी विचार

7.1 प्रोटोकॉल संदेश प्रारूप और □□□

□□□□□□□ संरचित संदेश क्रमांकन के लिए □□□□□□□□ □□□□□□□ ? और नेटवर्क संचार के लिए □□□□□□□ □□□□ □□□ का लाभ उठाता है। मुख्य संदेश प्रारूपों में शामिल हैं:

पहचान पंजीकरण:

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

एन्क्रिप्टेड संदेश:

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

भुगतान का प्रमाण:

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

7.2 रिले सर्वर अर्थशास्त्र और प्रोत्साहन

रिले सर्वरों को उपयोगकर्ता गोपनीयता बनाए रखते हुए आर्थिक रूप से टिकाऊ होना चाहिए। आर्थिक मॉडल में शामिल है:

राजस्व स्रोत:

- नए उपयोगकर्ताओं से पंजीकरण शुल्क
- वैकल्पिक प्रीमियम सेवाएँ (बढ़ा हुआ संग्रहण, प्राथमिकता वितरण)
- लेनदेन शुल्क साझाकरण (उन रिले सर्वरों के लिए जो खनन भी करते हैं)

लागत संरचना:

- एन्क्रिप्टेड संदेशों के लिए संग्रहण लागत
- संदेश वितरण के लिए बैंडविड्थ लागत
- भुगतान सत्यापन के लिए गणनात्मक लागत

प्रतिस्पर्धी गतिशीलता: उपयोगकर्ता मानक □ □ □ का उपयोग करके रिले सर्वरों के बीच माइग्रेट कर सकते हैं, प्रतिस्पर्धी मूल्य निर्धारण और सेवा गुणवत्ता के लिए बाजार दबाव बनाते हैं।

7.3 क्लाइंट-साइड बर्न प्रबंधन और □ □

उपयोगकर्ता-सामना करने वाले क्लाइंट को सुरक्षा बनाए रखते हुए क्रिप्टोकरेंसी प्रबंधन की जटिलता को अमूर्त करना चाहिए:

स्वचालित बर्न राशि चयन: क्लाइंट निम्न के आधार पर स्वचालित बर्न राशि चयन कार्यान्वित कर सकते हैं:

- संदेश प्राथमिकता (अत्यावश्यक संदेश उच्च बर्न दरों का उपयोग करते हैं)
- प्राप्तकर्ता संबंध (प्रथम संपर्क के लिए उच्च बर्न)
- नेटवर्क भीड़ (देखे गए वितरण समय के आधार पर गतिशील समायोजन)

वॉलेट एकीकरण: मानकीकृत इंटरफ़ेस के माध्यम से क्रिप्टोकरेंसी वॉलेट के साथ निर्बाध एकीकरण, कस्टोडियल और नॉन-कस्टोडियल वॉलेट आर्किटेक्चर दोनों का समर्थन करता है।

गोपनीयता सुरक्षा: क्लाइंट सॉफ़्टवेयर में संदेश बैचिंग और यादृच्छिक देरी के माध्यम से ट्रैफिक विश्लेषण और समय हमलों के विरुद्ध अंतर्निहित सुरक्षाएँ शामिल हैं।

7.4 मौजूदा अवसंरचना के साथ एकीकरण

प्रोटोकॉल मौजूदा संचार प्रणालियों के साथ वृद्धिशील परिनियोजन के लिए डिज़ाइन किया गया है:

ईमेल गेटवे: □□□□□□□ संदेशों को क्रिप्टोकरेंसी संचालन संभालने वाली गेटवे सेवाओं के माध्यम से पारंपरिक ईमेल से/के लिए ब्रिज किया जा सकता है।

वेब एकीकरण: □□□□□□□□□□ लाइब्रेरी □□□□□□□□□ कनेक्शन के माध्यम से वेब अनुप्रयोगों में सीधे □□□□□□□ एकीकरण सक्षम करती हैं।

मोबाइल समर्थन: नेटिव मोबाइल □□□ मोबाइल वातावरण के लिए उचित कुंजी प्रबंधन के साथ बैटरी-कुशल कार्यान्वयन प्रदान करते हैं।

8 खतरा मॉडल और हमला विश्लेषण

8.1 स्पैम और □□□ हमले

प्रत्यक्ष स्पैम हमले: प्रतिपक्षी बड़ी मात्रा में अनचाहे संदेश भेजने का प्रयास करते हैं। बर्न तंत्र इस हमले को महंगा बनाता है: न्यूनतम बर्न राशि B_{min} के साथ N स्पैम संदेश भेजने में कम से कम $N \cdot B_{min}$ खर्च होता है। स्पैम लाभदायक होने के लिए, हमलावरों को प्रति सफल संदेश $V > B_{min}$ मूल्य निकालना होगा, जो अधिकांश स्पैम श्रेणियों के लिए असंभव है।

संसाधन समाप्ति हमले: प्रतिपक्षी संदेश प्रसंस्करण अनुरोधों के साथ रिले सर्वरों को अभिभूत करने का प्रयास करते हैं। भुगतान आवश्यकता हमले की मात्रा को सीमित करती है, जबकि रिले सर्वर भुगतान राशि के आधार पर अतिरिक्त दर सीमा लागू कर सकते हैं।

संग्रहण समाप्ति हमले: प्रतिपक्षी रिले सर्वर संग्रहण भरने के लिए वैध भुगतान किए गए संदेश भेजते हैं। रिले सर्वर पुराने संदेशों की स्वचालित हटाने और प्रीमियम संग्रहण स्तरों सहित संग्रहण प्रबंधन नीतियाँ लागू कर सकते हैं।

8.2 आर्थिक हमले

शुल्क पुनर्चक्रण हमले: खनन अवसंरचना नियंत्रित करने वाले प्रतिपक्षी लेनदेन शुल्क के माध्यम से जले हुए फंड पुनर्प्राप्त करने का प्रयास करते हैं। आंशिक शुल्क बर्न तंत्र (खंड ??) पुनर्प्राप्ति को $(1 - \beta)\mu$ तक सीमित करता है जहाँ β बर्न अंश है और μ हमलावर की हैश पावर अंश है।

□□□□□ हमले: प्रतिपक्षी हमले क्षमता बढ़ाने के लिए बड़ी संख्या में नकली पहचान बनाते हैं। प्रत्येक पहचान को पंजीकरण शुल्क के माध्यम से आर्थिक प्रतिबद्धता की आवश्यकता होती है, हमले के बजट और □□□□□ क्षमता के बीच रैखिक स्केलिंग बनाता है (प्रस्ताव ??)।

बाजार हेरफेर: प्रतिपक्षी बर्न अर्थशास्त्र को प्रभावित करने के लिए क्रिप्टोकरेंसी कीमतों में हेरफेर करने का प्रयास करते हैं। ओरेकल-मुक्त डिज़ाइन सिस्टम को बाहरी मूल्य हेरफेर के लिए उत्तरदायी लेकिन निर्भर नहीं बनाता है।

8.3 अवसंरचना हमले

रिले सर्वर सेंसरशिप: दुर्भावनापूर्ण रिले सर्वर विशिष्ट प्रेषकों से संदेश वितरित करने से इनकार करते हैं। उपयोगकर्ता वितरण पुष्टिकरण के माध्यम से सेंसरशिप का पता लगा सकते हैं और वैकल्पिक रिले सर्वर पर माइग्रेट कर सकते हैं।

कीसर्वर हेरफेर: प्रतिपक्षी झूठी पहचान जानकारी प्रकाशित करने का प्रयास करते हैं। क्रिप्टोग्राफिक हस्ताक्षर आवश्यकताएँ प्रतिरूपण को रोकती हैं, जबकि वितरित कीसर्वर नेटवर्क व्यक्तिगत सर्वर समझौते के विरुद्ध लचीलापन प्रदान करता है।

नेटवर्क विभाजन: प्रतिपक्षी उपयोगकर्ताओं या सर्वरों को व्यापक नेटवर्क से अलग करने का प्रयास करते हैं। संघीय आर्किटेक्चर कई संचार पथ प्रदान करता है, जबकि क्रिप्टोकरेंसी नेटवर्क एक वैश्विक समन्वय तंत्र प्रदान करता है।

8.4 गोपनीयता हमले

ट्रैफिक विश्लेषण: प्रतिपक्षी संचार पैटर्न अनुमान करने के लिए नेटवर्क ट्रैफिक की निगरानी करते हैं। एंड-टू-एंड एन्क्रिप्शन संदेश सामग्री की रक्षा करता है, जबकि क्लाइंट अतिरिक्त सुरक्षा के लिए प्याज रूटिंग या समान तकनीकों का उपयोग कर सकते हैं।

समय हमले: प्रतिपक्षी संचार संबंध पहचानने के लिए संदेश भेजने और प्राप्त करने के समय को सहसंबंधित करते हैं। क्लाइंट समय सहसंबंध कम करने के लिए यादृच्छिक देरी और संदेश बैचिंग लागू कर सकते हैं।

भुगतान विश्लेषण: प्रतिपक्षी भुगतानों को संदेशों से जोड़ने के लिए ब्लॉकचेन लेनदेन का विश्लेषण करते हैं। प्रत्येक बर्न लेनदेन के लिए ताज़े पते का उपयोग और उचित लेनदेन मिश्रण अतिरिक्त गोपनीयता प्रदान कर सकता है।

9 मूल्यांकन और चर्चा

9.1 सैद्धांतिक विश्लेषण परिणाम

हमारा सैद्धांतिक विश्लेषण कई मुख्य गुणों को प्रदर्शित करता है:

स्पैम प्रतिरोध स्केलिंग: स्पैम हमलों की लागत हमले की मात्रा के साथ रैखिक रूप से स्केल होती है, अनुमानित सुरक्षा गारंटी प्रदान करती है। प्रति संदेश $B_{min} = \$0.01$ की न्यूनतम बर्न दर के लिए, 10 लाख स्पैम संदेश भेजने में परिचालन ओवरहेड को छोड़कर कम से कम $\$10,000$ खर्च होता है।

वैध उपयोगकर्ता पहुँच: प्रति संदेश $\$0.01$ - $\$0.10$ की बर्न दर के लिए, वैध उपयोगकर्ताओं के लिए आर्थिक बाधा न्यूनतम रहती है (संदेश लागत के तुलनीय) जबकि पर्याप्त स्पैम अवरोध प्रदान करती है।

नेटवर्क प्रभाव लाभ: जैसे-जैसे नेटवर्क अपनाना बढ़ता है, वैध संदेश का मूल्य स्पैम हमले दक्षता से तेज़ बढ़ता है, सिस्टम विकास के लिए सकारात्मक प्रतिक्रिया उत्पन्न करता है।

9.2 मौजूदा प्रणालियों से तुलना

तालिका ?? मुख्य गुणों में की मौजूदा स्पैम-रोधी और संदेश दृष्टिकोणों से तुलना करती है:

प्रणाली	विकेंद्रीकृत	स्पैम-रोधी	गोपनीयता	स्केलेबिलिटी
( )	आंशिक	खराब	खराब	उच्च
	हाँ	मध्यम	अच्छा	खराब
	आंशिक	खराब	अच्छा	मध्यम
	नहीं	अच्छा	उत्कृष्ट	मध्यम
	हाँ	अच्छा	अच्छा	उच्च

तालिका 1: मुख्य गुणों में संदेश प्रणालियों की तुलना

9.3 कार्यान्वयन अनुभव

सोशल नेटवर्क अवधारणाओं के साथ प्रारंभिक परिनियोजन अनुभव प्रदान करता है। इस पेपर में प्रोटोकॉल विशिष्टता एक आर्किटेक्चर का औपचारिक समापन है जिसके मुख्य तंत्र—बर्न-टू-स्पीक, संघीय रिले, कीसर्वर पहचान— में प्रोटोटाइप किए गए थे। परिनियोजन टिप्पणियों में शामिल हैं:

उपयोगकर्ता स्वीकृति: उपयोगकर्ता बर्न-आधारित संदेश के लिए अनुकूल होते हैं जब बर्न राशि लगभग 0.05 प्रति संदेश से नीचे रहती है। उच्च राशियाँ आकस्मिक संचार के लिए ध्यान देने योग्य संकोच उत्पन्न करती हैं।

स्पैम कमी: बर्न आवश्यकताएँ प्रभावी ढंग से स्वचालित स्पैम को रोकती हैं; प्रति संदेश आर्थिक लागत एक मंजिल प्रस्तुत करती है जो विशिष्ट स्पैम अभियानों के लिए अपेक्षित रिटर्न से अधिक है। पैमाने पर एक उत्पादन परिनियोजन में व्यवस्थित माप भविष्य के अनुभवजन्य कार्य के लिए स्थगित है।

अवसंरचना लागत: रिले सर्वर संसाधन खपत प्रारंभिक परीक्षण में उपयोगकर्ता संख्या के साथ लगभग रैखिक रूप से स्केल होती है। भुगतान प्रमाण सत्यापन मूल संदेश रूटिंग में मामूली गणनात्मक ओवरहेड जोड़ता है—क्रिप्टोग्राफिक सत्यापन के बजाय ब्लॉकचेन स्टेट लुकअप द्वारा प्रभुत्व।

ये टिप्पणियाँ अनौपचारिक हैं और एक छोटे पैमाने के परिनियोजन से हैं। वे दृष्टिकोण को व्यवहार्य के रूप में सत्यापित करती हैं लेकिन पैमाने पर कठोर प्रदर्शन बेंचमार्किंग का विकल्प नहीं हैं।

9.4 सीमाएँ और ट्रेड-ऑफ

□□□□□□ दृष्टिकोण में कई अंतर्निहित ट्रेड-ऑफ शामिल हैं:

आर्थिक बाधाएँ: जबकि वैध उपयोगकर्ताओं के लिए बर्न राशि न्यूनतम है, वे आर्थिक रूप से वंचित क्षेत्रों में उपयोगकर्ताओं के लिए बाधाएँ उत्पन्न कर सकती हैं। भविष्य के कार्य में स्लाइडिंग-स्केल बर्न दरें या वैकल्पिक मूल्य-प्रमाण तंत्र की खोज हो सकती है।

क्रिप्टोकरेंसी निर्भरता: सिस्टम के लिए क्रिप्टोकरेंसी नेटवर्क तक पहुँच की आवश्यकता होती है, जो प्रतिबंधित पहुँच वाले क्षेत्रों में या क्रिप्टोकरेंसी के साथ असहज उपयोगकर्ताओं के बीच अपनाने को सीमित कर सकता है।

पुनर्प्राप्ति जटिलता: कुंजी हानि परिदृश्यों में पारंपरिक केंद्रीकृत प्रणालियों की तुलना में अधिक जटिल पुनर्प्राप्ति प्रक्रियाओं की आवश्यकता होती है, जो गैर-तकनीकी उपयोगकर्ताओं के लिए उपयोगिता चुनौतियाँ उत्पन्न कर सकती हैं।

9.5 भविष्य के विस्तार और अनुप्रयोग

□□□□□□ प्रोटोकॉल कई विस्तारों के लिए आधार प्रदान करता है:

प्रतिष्ठा प्रणालियाँ: प्राप्त संदेश फीडबैक के आधार पर उपयोगकर्ता प्रतिष्ठा स्कोर गतिशील बर्न दर समायोजन और बेहतर स्पैम फ़िल्टरिंग सक्षम कर सकते हैं।

सामग्री बाजार: बर्न तंत्र सामग्री माइक्रोपेमेंट तक विस्तारित हो सकता है, सूचना साझाकरण और मीडिया वितरण के लिए नए आर्थिक मॉडल सक्षम करता है।

□□□ संचार: स्वचालित भुगतान के साथ मशीन-टू-मशीन संचार नए इंटरनेट ऑफ थिंग्स अनुप्रयोग सक्षम कर सकता है जहाँ उपकरण बैंडविड्थ और प्रसंस्करण संसाधनों के लिए भुगतान करते हैं।

विकेंद्रीकृत सोशल नेटवर्क: प्रकाशन-सदस्यता प्रणाली आर्थिक प्रोत्साहन संरेखण के साथ पूरी तरह से विकेंद्रीकृत सोशल मीडिया प्लेटफ़ॉर्म के लिए अवसंरचना प्रदान करती है।

10 निष्कर्ष

हमने □□□□□□ प्रस्तुत किया है, एक व्यापक प्रोटोकॉल सूट जो इंटरनेट संचार प्रणालियों में केंद्रीकरण को बढ़ावा देने वाली मूलभूत आर्थिक प्रोत्साहन समस्याओं को संबोधित करता है। बर्न-टू-स्पीक स्पैम-रोधी तंत्रों की औपचारिक विशिष्टता, संघीय अवसंरचना डिज़ाइन, और आर्थिक सुरक्षा विश्लेषण के माध्यम से, हम प्रदर्शित करते हैं कि क्रिप्टोकरेंसी एकीकरण मौजूदा दृष्टिकोणों की तुलना में बेहतर स्पैम प्रतिरोध प्रदान करते हुए विकेंद्रीकृत इंटरनेट संचार की मूल दृष्टि को पुनर्स्थापित कर सकता है।

प्रोटोकॉल का गणनात्मक या नियामक स्पैम-रोधी तंत्रों के बजाय आर्थिक पर जोर कई फायदे प्रदान करता है: अनुमानित सुरक्षा गारंटी, वैश्विक परिनियोजन के लिए स्केलेबिलिटी, और गणनात्मक दृष्टिकोणों को प्रभावित करने वाली प्रौद्योगिकी हथियार दौड़ के प्रतिरोध। □□□□□ सोशल नेटवर्क के साथ कार्यान्वयन अनुभव दृष्टिकोण की व्यावहारिक व्यवहार्यता को मान्य करता है।

भविष्य के कार्य को वंचित उपयोगकर्ताओं के लिए आर्थिक बाधाओं को कम करने, कुंजी प्रबंधन उपयोगिता में सुधार, और मैसेजिंग से परे अन्य संचार और समन्वय समस्याओं के लिए अनुप्रयोगों की खोज पर ध्यान केंद्रित करना चाहिए जो समान केंद्रीकरण दबावों से पीड़ित हैं।

□□□□□□ का अंतिम लक्ष्य केवल तकनीकी नवाचार नहीं है, बल्कि डिजिटल संचार पर उपयोगकर्ता संप्रभुता की बहाली है—मूल केंद्रीकरण को बढ़ावा देने वाली आर्थिक वास्तविकताओं को संबोधित करते हुए इंटरनेट के विकेंद्रीकरण और उपयोगकर्ता सशक्तिकरण के संस्थापक सिद्धांतों पर वापसी सक्षम करना।