quantus

क्वांटम-सुरक्षित, एन्क्रिप्टेड धन

प्रकाशित
21 मार्च 2026

संस्करण
0.3.3

वर्गीकरण
public

यह व्हाइटपेपर केवल सूचनात्मक उद्देश्यों के लिए प्रस्तुत किया गया है और किसी प्रतिभूति, निवेश या वित्तीय उत्पाद की बिक्री का प्रस्ताव, खरीद के प्रस्ताव का आग्रह या सिफारिश नहीं है। पाठकों को निवेश निर्णय लेने से पहले अपनी स्वयं की उचित जाँच करनी चाहिए और योग्य पेशेवरों से परामर्श करना चाहिए। Quantus Network यहाँ दी गई जानकारी की सटीकता या पूर्णता के संबंध में कोई प्रतिनिधित्व या वारंटी नहीं देता।

विषय - सूची

01

परिचय

क्वांटम खतरा

पारंपरिक ब्लॉकचेन क्रिप्टोग्राफ़िक रूप से प्रासंगिक क्वांटम कंप्यूटरों (CRQC) से अस्तित्वगत खतरे का सामना करते हैं। ब्लॉकचेन की क्रिप्टोग्राफ़िक नींव डिस्क्रीट लॉगरिदम समस्या (DLP) की कठिनता पर निर्भर करती है, और क्वांटम एल्गोरिदम, विशेष रूप से शोर का एल्गोरिदम, DLP को शास्त्रीय कंप्यूटरों की तुलना में घातीय रूप से तेज़ी से हल कर सकता है। यह भेद्यता प्रतिद्वंद्वियों को सार्वजनिक कुंजियों से निजी कुंजी निकालने में सक्षम बना सकती है, जिससे वे लेनदेन जाली बना सकें और संवेदनशील वित्तीय डेटा को डिक्रिप्ट कर सकें।

> सक्रिय क्वांटम-प्रतिरोधी अपग्रेड के बिना, खरबों डॉलर की क्रिप्टो अर्थव्यवस्था ऐसे हमलों से अचानक अवमूल्यन का जोखिम उठाती है।

अनूठा मूल्य प्रस्ताव

लैटिन शब्द से जिसका अर्थ «कितना» है, उसके नाम पर Quantus Network क्वांटम-सुरक्षित अर्थ में निजी, स्केलेबल धन सक्षम करता है। Quantus सामान्य स्मार्ट कॉन्ट्रैक्ट प्लेटफ़ॉर्म नहीं है। कुछ अत्यधिक परिष्कृत व्यंजनों वाले रेस्तरां की तरह, Quantus यह प्रदान करता है:

— सभी लेनदेन के लिए पोस्ट-क्वांटम हस्ताक्षर

— पीयर कनेक्शन सुरक्षित करने के लिए पोस्ट-क्वांटम हस्ताक्षर और एन्क्रिप्शन (ML-DSA और ML-KEM)

— स्केल करने के लिए पोस्ट-क्वांटम ज़ीरो-नॉलेज प्रूफ

— चोरी को रोकने और गलतियों से उबरने के लिए उच्च सुरक्षा खाते

— पते सत्यापित करने में आसानी के लिए मानव-पठनीय चेक-फ़्रेज़

निजी, क्वांटम-सुरक्षित, स्केलेबल धन पर ध्यान केंद्रित करने का निर्णय उद्योग के लिए CRQC द्वारा पेश खतरे और Bitcoin की इन चुनौतियों को संबोधित करने में असमर्थता से उत्पन्न होता है।

02

ब्लॉकचेन के लिए क्वांटम खतरा

क्वांटम कंप्यूटिंग की मूल बातें

क्वांटम कंप्यूटर सुपरपोज़िशन और उलझाव जैसे सिद्धांतों का उपयोग करके ऐसी गणनाएँ करते हैं जो शास्त्रीय मशीनों के लिए अथक हैं। शास्त्रीय बिट्स के विपरीत, जो 0 या 1 होते हैं, क्यूबिट एक साथ कई अवस्थाओं में हो सकते हैं, जिससे कुछ समस्याओं के लिए घातीय समानांतरता मिलती है। यह क्षमता ब्लॉकचेन वित्त को संरेखित करने वाली क्रिप्टोग्राफ़िक प्रणालियों के लिए अस्तित्वगत जोखिम पैदा करती है, क्योंकि क्वांटम हार्डवेयर के लिए विकसित एल्गोरिदम अधिकांश सार्वजनिक-कुंजी क्रिप्टोग्राफ़ी की सुरक्षा धारणाओं को कमजोर करते हैं।

शोर का एल्गोरिदम, 1994 में पीटर शोर द्वारा प्रस्तुत, बड़े पूर्णांकों के गुणनखंडन और क्वांटम कंप्यूटर पर डिस्क्रीट लॉगरिदम समस्या को हल करने के लिए बहुपद-समय विधि प्रदान करता है। यह किसी फ़ंक्शन की अवधि खोजने के लिए क्वांटम फूरियर ट्रांसफ़ॉर्म (QFT) का उपयोग करता है, जिससे RSA या दीर्घवृत्तीय वक्र क्रिप्टोग्राफ़ी (ECC) जैसी योजनाओं के आधार पर ट्रैपडोर फ़ंक्शनों को कुशलता से उलटने की अनुमति मिलती है। ब्लॉकचेन वित्त के लिए, इसका अर्थ है कि पर्याप्त शक्तिशाली क्वांटम कंप्यूटर (~2,000 लॉजिकल क्यूबिट अनुमानित [6][7][8][9]) वाला हमलावर बहुपद समय $O(n^3)$ में सार्वजनिक कुंजियों से निजी कुंजी निकाल सकता है: एक अत्यधिक त्वरण जो रातोंरात कमजोर प्रणालियों को अप्रचलित कर देता है। [1]

ग्रोवर का एल्गोरिदम, लव ग्रोवर द्वारा 1996 में प्रस्तावित, असंरचित खोज के लिए द्विघात त्वरण प्रदान करता है, खोज समय को $O(n)$ से $O(\sqrt{n})$ संचालन तक कम करता है। यद्यपि यह असममित क्रिप्टोग्राफ़ी के लिए शोर जितना विनाशकारी नहीं है, ग्रोवर हैश

फ़ंक्शन और AES एन्क्रिप्शन जैसे सममित प्रिमिटिव को प्रभावित करता है, प्रभावी रूप से सुरक्षा स्तर को आधा कर देता है (उदा., 256-बिट कुंजी क्वांटम हमलों के खिलाफ 128 बिट्स की तरह व्यवहार करती है)। इस हमले को क्रिप्टोग्राफ़िक योजना बदलने के बजाय सुरक्षा बिट्स दोगुना करके कम किया जाता है। इसके अतिरिक्त, ग्रोवर का द्विघात त्वरण उच्च क्यूबिट और गेट आवश्यकताओं के कारण अव्यावहारिक है, अरबों क्रमिक संचालन की आवश्यकता होती है सीमित समानांतरता के साथ, जिससे भविष्य के हार्डवेयर पर भी वास्तविक दुनिया में उलटफेर असंभव हो जाता है। [2]

चार खतरे की श्रेणियाँ

01 - डिजिटल हस्ताक्षर जाली बनाना

शोर का एल्गोरिदम अधिकांश ब्लॉकचेन में उपयोग किए जाने वाले ECC-आधारित हस्ताक्षरों को सीधे खतरे में डालता है (उदा., Bitcoin की secp256k1 वक्र), जिससे प्रतिद्वंद्वियों को उपयोगकर्ताओं का रूप धारण करने और धोखाधड़ी वाले लेनदेन को अधिकृत करने की अनुमति मिलती है। ऐसी क्षमता ब्लॉकचेन की सबसे बुनियादी विशेषता की गंभीर विफलता होगी।

02 - ज़ीरो-नॉलेज प्रणालियों में झूठे प्रमाण जाली बनाना

कई ज़ीरो-नॉलेज प्रूफ, जैसे गोपनीयता-केंद्रित वित्त के लिए zk-SNARKs में, प्रतिबद्धताओं के लिए दीर्घवृत्तीय-वक्र पेयरिंग के माध्यम से डिस्क्रीट लॉगरिदम कठिनता पर निर्भर करते हैं। शोर अमान्य प्रमाण बनाने में सक्षम हो सकता है जो वैध दिखें, जिससे हमलावर नए सिक्के बना सकता है या लेयर 2 (L2) की स्थिति जाली बना सकता है।

03 - गुप्त जानकारी डिक्रिप्ट करना

क्वांटम हमले Zcash या Monero जैसे गोपनीयता प्रोटोकॉल में कमजोर सार्वजनिक-कुंजी योजनाओं द्वारा संरक्षित एन्क्रिप्टेड डेटा को उजागर कर सकते हैं। वे वित्तीय

प्रोटोकॉल में p2p संचार को भी डिक्रिप्ट कर सकते हैं, संवेदनशील धन विवरण प्रकट कर सकते हैं और लक्षित चोरी सक्षम कर सकते हैं।

04 - हैश फ़ंक्शन उलटना

ग्रोवर का एल्गोरिदम SHA-256 जैसे हैश पर प्रीइमेज हमलों को तेज कर सकता है, जिनका उपयोग प्रूफ़-ऑफ़-वर्क और पता निर्माण में होता है, लेकिन यह सबसे कम चिंताजनक खतरा है। कई पोस्ट-क्वांटम क्रिप्टोग्राफ़िक योजनाएँ हैश-आधारित निर्माण शामिल करती हैं क्योंकि पर्याप्त बड़े डाइजेस्ट के साथ हैश पर्याप्त सुरक्षित माने जाते हैं।

पोस्ट-क्वांटम क्रिप्टोग्राफ़ी में स्केलिंग चुनौतियाँ

यद्यपि पोस्ट-क्वांटम क्रिप्टोग्राफ़ी (PQC) क्वांटम खतरों के खिलाफ आवश्यक सुरक्षा प्रदान करती है, यह इन एल्गोरिदम के अंतर्निहित डिज़ाइन के कारण महत्वपूर्ण स्केलिंग बाधाएँ पेश करती है। दीर्घवृत्तीय वक्र योजनाओं के विपरीत, जो संक्षिप्त गणितीय संरचनाओं पर निर्भर करती हैं, PQC प्रिमिटिव को शास्त्रीय और क्वांटम दोनों प्रतिद्वंद्वियों के खिलाफ सुरक्षा बनाए रखने के लिए बड़े पैरामीटर चाहिए। इसके परिणामस्वरूप सार्वजनिक कुंजी, निजी कुंजी और हस्ताक्षर काफ़ी बड़े हो जाते हैं, अक्सर परिमाण के क्रम तक। निम्न तालिका 128-बिट पोस्ट-क्वांटम सुरक्षा स्तर पर ML-DSA के लिए विशिष्ट आकार दर्शाती है 256-बिट ECDSA जैसे शास्त्रीय समकक्षों की तुलना में: [10]

एल्गोरिदम	सार्वजनिक कुंजी	निजी कुंजी	हस्ताक्षर
ML-DSA-87 (Dilithium)	**2,592 बाइट**	**4,896 बाइट**	**4,627 बाइट**
ECDSA (256-बिट)	**32 बाइट**	**32 बाइट**	**65 बाइट**

128-बिट पोस्ट-क्वांटम सुरक्षा स्तर पर आकार। स्रोत: Open Quantum Safe Project [10]

जैसा दिखाया गया है, ML-DSA हस्ताक्षर ECDSA समकक्षों की तुलना में 70 गुना से अधिक बड़े हो सकते हैं, और सार्वजनिक कुंजियाँ 80 गुना से अधिक बड़ी। अन्य PQC परिवार इसे बढ़ाते हैं: SPHINCS+ जैसी हैश-आधारित योजनाएँ 41 KB तक के हस्ताक्षर उत्पन्न कर सकती हैं, जबकि आकार-अनुकूलित जाली वेरिएंट जैसे FALCON अभी भी शास्त्रीय आकारों से काफ़ी अधिक गुणक पर हैं।

ब्लॉकचेन संदर्भों में, ये बढ़े हुए आकार प्रणालीगत स्केलिंग मुद्दों में जुड़ जाते हैं। बड़े हस्ताक्षर व्यक्तिगत लेनदेन को फुलाते हैं, प्रति सेकंड लेनदेन (TPS) कम करते हैं क्योंकि ब्लॉक तेज़ी से भरते हैं और सत्यापन में अधिक समय लगता है। यह पीयर-टू-पीयर (P2P) संचार को भी तनाव देता है, बैंडविड्थ और प्रसार में देरी बढ़ाता है, जो प्रूफ़-ऑफ़-वर्क जैसे सर्वसम्मति तंत्र में नेटवर्क फोर्क या अनाथ ब्लॉकों के जोखिम को बढ़ा सकता है। भंडारण आवश्यकताएँ भी प्रभावित होती हैं, उच्च नोड परिचालन लागत और भागीदारी में बाधाएँ, विशेष रूप से संसाधन-सीमित उपयोगकर्ताओं या सत्यापनकर्ताओं के लिए।

> **नोट**
>
> इन स्केलिंग चुनौतियों को भविष्य में सभी ब्लॉकचेन को संबोधित करना होगा। उदाहरण के लिए, यदि अधिकतम ब्लॉक आकार नहीं बढ़ाया जाता है तो `Bitcoin` में `1 TPS` से कहीं कम होगा।

03

प्रवासन संकट

समन्वय की समस्या

Bitcoin की रूढ़िवादी संस्कृति प्रोटोकॉल परिवर्तनों का विरोध करती है। कोई भी PQC अपग्रेड प्रवासन समयसीमा, संभावित सिक्का जब्ती और ब्लॉक आकार वृद्धि जैसे विवादास्पद मुद्दों पर सर्वसम्मति माँगेगा। यदि समुदाय सहमत भी हो, हर उपयोगकर्ता को अपने सिक्के नए क्वांटम-सुरक्षित पतों पर ले जाने होंगे। प्रवासन के लिए हर क्रिप्टो धारक की कार्रवाई चाहिए, जिनमें से कई ने अपने वॉलेट तक पहुँच खो दी है या खतरे से अनजान हैं।

ये मुद्दे हर सार्वजनिक ब्लॉकचेन के लिए मौजूद हैं, लेकिन Bitcoin के लिए अद्वितीय रूप से कठिन हैं क्योंकि स्पष्ट नेतृत्व की कमी है और तकनीकी अवसादन की दार्शनिकता।

खोए हुए सिक्कों की समस्या

अनुमान है कि $250 अरब से $500 अरब तक का Bitcoin खोई कुंजियों, मृत धारकों या भूले वॉलेटों के कारण स्थायी रूप से अप्राप्य है। [3] ये सिक्के प्रवासित नहीं किए जा सकते और क्रिप्टोग्राफ़िक रूप से प्रासंगिक क्वांटम कंप्यूटर (CRQC) बनाने के लिए सार्वजनिक इनाम के रूप में काम करते हैं। क्वांटम हमलावर प्रवासित नहीं की गई सार्वजनिक कुंजियों से निजी कुंजी निकालेंगे और संभवतः अरबों डॉलर BTC बाज़ार में डंप करेंगे।

> एकमात्र तकनीकी समाधान के लिए सख्त अंतिम तिथि चाहिए जो अप्रवासित सिक्कों को जमा कर दे: एक राजनीतिक असंभवता।

ऐसी अंतिम तिथि के बिना, परिणाम यह होगा कि अप्रवासित सिक्के चुराए और बेचे जाएँगे, बाज़ार ध्वस्त होगा और नेटवर्क में विश्वास नष्ट होगा।

प्रवासन समयरेखा की समस्या

पोस्ट-क्वांटम हस्ताक्षर वर्तमान Bitcoin हस्ताक्षरों से 20 से 80 गुना बड़े हैं। मौलिक वास्तुकला परिवर्तन के बिना, Bitcoin का थ्रूपुट पहले से सीमित क्षमता के एक अंश तक गिर जाएगा।

मान लें Bitcoin राजनीतिक और तकनीकी चुनौतियाँ हल कर लेता है, स्वयं प्रवासन में महीने या साल लगेंगे। हर धारक को कम से कम एक लेनदेन भेजना होगा ताकि धन क्वांटम-सुरक्षित पते पर जाए। कई पहले परीक्षण लेनदेन भेजेंगे। फूले हुए PQC हस्ताक्षर थ्रूपुट को दबाते हुए, नेटवर्क महीनों या सालों तक कतार का सामना करता है जबकि क्वांटम-संवेदनशील सिक्के खुले रहते हैं।

> **QUANTUS का उत्तर**
>
> ये संचित चुनौतियाँ मौजूदा चेन पर क्वांटम सुरक्षा जोड़ना असाधारण रूप से कठिन बनाती हैं। `Quantus Network` इसे पहले दिन से चेन में क्वांटम सुरक्षा बनाकर बचाता है।

04

quantus network वास्तुकला

आधार

Quantus Network Substrate पर बना है, एक ब्लॉकचेन SDK जिसे Parity Technologies ने विकसित किया, Ethereum और Polkadot के पीछे की टीम। Substrate अत्यधिक मॉड्युलर है, जिससे घटकों को आसानी से बदला जा सकता है ताकि हम Quantus को अनूठा बनाने वाली चीज़ों पर ध्यान दें।

Quantus Substrate को बेहतर बनाता है:

— पोस्ट-क्वांटम हस्ताक्षर योजनाओं के लिए समर्थन जोड़कर

— p2p नेटवर्किंग सुरक्षा को पोस्ट-क्वांटम बनाकर

— उपयोगकर्ता-नियंत्रित लेनदेन प्रतिवर्तनीयता जोड़कर

— सभी डेटा प्रकारों को फ़ील्ड-तत्व सीमाओं के साथ संरेखित करके डेटाबेस को zk-अनुकूल बनाकर

पोस्ट-क्वांटम क्रिप्टोग्राफ़िक प्रिमिटिव

Quantus Network लेनदेन और नेटवर्क संचार की सुरक्षा सुनिश्चित करने के लिए NIST-मानकीकृत PQC का उपयोग करता है क्वांटम खतरों के खिलाफ। लेनदेन अखंडता के केंद्र में **ML-DSA** (मॉड्यूल-जाली-आधारित डिजिटल हस्ताक्षर एल्गोरिदम, पहले CRYSTALS-Dilithium के नाम से जाना जाता था) है, एक जाली-आधारित हस्ताक्षर योजना जिसे सुरक्षा, दक्षता और कार्यान्वयन में आसानी के संतुलन के लिए चुना गया। ML-DSA LWE और SIS जैसी समस्याओं की कठिनता का उपयोग करता है

मॉड्यूल जालियों पर, शास्त्रीय और क्वांटम दोनों हमलों के प्रति मजबूत प्रतिरोध प्रदान करता है, शोर के एल्गोरिदम सहित। [4]

लेनदेन हस्ताक्षरों के लिए, Quantus **ML-DSA-87** एकीकृत करता है, पैरामीटर सेट जो उच्चतम सुरक्षा स्तर प्रदान करता है (NIST सुरक्षा स्तर 5, 256-बिट शास्त्रीय और 128-बिट क्वांटम सुरक्षा के समकक्ष) संभावित क्रिप्टोएनालिटिक सफलताओं से बचाने के लिए जाली समस्याओं में। यह विकल्प सावधानी को प्राथमिकता देता है, क्योंकि जाली क्रिप्टोग्राफ़ी अपेक्षाकृत नई है और शास्त्रीय योजनाओं की तुलना में कम युद्ध-परीक्षित है। बड़े पैरामीटर जाली क्रिप्टोएनालिसिस में संभावित प्रगति के जोखिम कम करते हैं, जो अभी भी छोटे कुंजी आकारों को नरम लक्ष्य छोड़ देंगे।

विचार किए गए विकल्प

ML-DSA को FN-DSA (Falcon) जैसे विकल्पों पर चुना गया क्योंकि FN-DSA की अधिक कार्यान्वयन जटिलता (उदा., फ़्लोटिंग-पॉइंट संचालन, ब्लॉकचेन-अनुकूल नहीं), विनिर्देश में नियतात्मक कुंजी निर्माण की कमी और विकास के समय गैर-अंतिम स्थिति।

SLH-DSA जैसी हैश-आधारित विकल्प उनके और भी बड़े हस्ताक्षर (17 KB से अधिक) के कारण नहीं चुने गए। क्रिप्टो-चपलता (विभिन्न हस्ताक्षर योजनाएँ बदलने की क्षमता) Substrate में निर्मित है, इसलिए भविष्य में परिस्थितियों की माँग पर ये विकल्प जोड़ना अपेक्षाकृत सरल है।

यद्यपि ML-DSA-87 बड़ी कुंजियाँ और हस्ताक्षर उत्पन्न करता है, ये Quantus के प्रारंभिक चरण के नेटवर्क में प्रबंधनीय हैं, जहाँ भंडारण अभी तक अड़चन नहीं है, और ज़ीरो-नॉलेज प्रूफ के माध्यम से वर्महोल पते जैसे अनुकूलन स्केलिंग संबोधित करेंगे।

कार्यान्वयन के तकनीकी विवरण के लिए QIP-0006 देखें।

libp2p - क्वांटम-सुरक्षित नेटवर्किंग

Quantus Network पीयर-टू-पीयर (P2P) नोड संचार को सुरक्षित करता है ML-DSA को प्रमाणीकरण के लिए और एन्क्रिप्शन के लिए **ML-KEM** (मॉड्यूल-जाली-आधारित कुंजी एनकैप्सुलेशन मैकेनिज़्म, पहले CRYSTALS-Kyber) के संयोजन से। यह एकीकरण PQC को libp2p स्टैक तक विस्तारित करता है, क्वांटम प्रतिरोध के लिए मुख्य घटकों को संशोधित करता है: पीयर पहचान के लिए ML-DSA-87 हस्ताक्षर और परिवहन सुरक्षा के लिए ML-KEM-768 (क्वांटम-प्रतिविरोधी साझा रहस्यों के लिए अतिरिक्त KEM संदेश के साथ Noise हैंडशेक विस्तारित करना)। [5]

P2P परत को अक्सर क्वांटम-सुरक्षा विश्लेषण में नज़रअंदाज़ किया जाता है। पीयर प्रमाणीकरण महत्वपूर्ण है, लेकिन पीयर स्तर पर हमलावर सबसे बुरा नोड का रूप धारण करके अमान्य संदेश भेज सकता है, जिससे सेवा से इनकार हो सकता है। यह हमला पहले से कम है क्योंकि ब्लॉकचेन मॉडल में नोड्स आम तौर पर अविश्वसनीय होते हैं और हमले का पता चलने पर आसानी से कुंजी बदल सकते हैं। इसी तरह, P2P संचार डिक्रिप्ट करने से हमलावर को सीमित लाभ (उदा., लेनदेन पथ ट्रैक करना, प्रॉक्सी या Tor से कम), और अधिकांश डेटा वैसे भी ऑन-चेन सार्वजनिक हो जाता है।

फिर भी, P2P परत को क्वांटम-सुरक्षित करना छिपकर सुनने, मध्यस्थ हमलों और क्वांटम डिक्रिप्शन से बचाता है, यह सुनिश्चित करता है कि नोड गॉसिप, ब्लॉक प्रसार और अन्य नेटवर्क इंटरैक्शन निकट भविष्य में गोपनीय और छेड़छाड़-रहित रहें।

तकनीकी विवरण के लिए QIP-0004 देखें।

pqc स्केलिंग - वर्महोल पते

पोस्ट-क्वांटम क्रिप्टोग्राफ़ी में अंतर्निहित स्केलिंग चुनौतियों का समाधान करने के लिए, Quantus Network एक नवीन एकत्रित पोस्ट-क्वांटम हस्ताक्षर योजना पेश करता है जिसे **«वर्महोल पते»** कहा जाता है। यह प्रणाली Plonky2 प्रूफिंग सिस्टम (मूलतः

STARKs) के माध्यम से उत्पन्न ज़ीरो-नॉलेज प्रूफ (ZKP) का उपयोग करती है ताकि शेष सत्यापन ऑफ-चेन हो, जिससे चेन एक ही संक्षिप्त प्रूफ सत्यापित कर सके बिना व्यक्तिगत हस्ताक्षर संसाधित किए। वर्महोल पते एक प्रूफ के साथ बड़ी संख्या में लेनदेन सत्यापित करने देते हैं, सार्वजनिक इनपुट (उदा., nullifiers, स्टोरेज रूट, निकास पते और राशि) प्राथमिक सीमक बन जाते हैं। यह प्रति-लेनदेन भंडारण माँग को लगभग 256 अतिरिक्त बाइट प्रति लेनदेन तक कम करता है, किसी भी ज्ञात PQC हस्ताक्षर योजना से कहीं छोटा।

योजना की क्वांटम सुरक्षा FRI (फास्ट रीड-सोलोमन इंटरैक्टिव ओरेकल प्रूफ) के माध्यम से प्रतिबद्धताओं के लिए सुरक्षित हैश फ़ंक्शन **Poseidon2** के उपयोग से आती है, SNARKs में आमतौर पर उपयोग किए जाने वाले क्वांटम-संवेदनशील दीर्घवृत्तीय-वक्र पेयरिंग के बजाय।

इसके अतिरिक्त, प्रमाणीकरण रहस्य Poseidon2 के पीछे छिपे रहते हैं। चूँकि सुरक्षित हैश फ़ंक्शन केवल ग्रोवर के एल्गोरिदम से द्विघात रूप से कमजोर होते हैं, टूटते नहीं, हैश प्रीइमेज प्रूफ ZK संदर्भों में हल्के पोस्ट-क्वांटम हस्ताक्षर के रूप में काम कर सकते हैं, SPHINCS+ जैसी हैश-आधारित योजनाओं के समान।

क्लाइंट / प्रूवर प्रवाह

उपयोगकर्ता एक नमक को गुप्त के साथ जोड़कर दोहरा-हैश करके प्रमाणित रूप से अखर्च योग्य पता बनाते हैं:

```
H(H(salt|secret))
```

यह संरचना झूठे सकारात्मक (उदा., सरल-हैश सार्वजनिक कुंजी को अखर्च योग्य पते से भ्रमित करना) रोकती है क्योंकि Substrate में (और सामान्यतः) ब्लॉकचेन पते सार्वजनिक कुंजी का सरल हैश होते हैं जो निजी कुंजी से किसी बीजगणितीय संक्रिया से

प्राप्त होते हैं, सुरक्षित हैश से नहीं। संरचना की सुरक्षा इसलिए सुरक्षित हैश की प्रीइमेज-ऑफ़-प्रीइमेज खोजने तक सिमट जाती है। इस पते पर भेजे गए टोकन प्रभावी रूप से जल जाते हैं। वे खर्च नहीं किए जा सकते क्योंकि प्राप्तकर्ता पते के लिए निजी कुंजी मौजूद नहीं है। ये सिक्के पुनः मिंट किए जा सकते हैं बिना आपूर्ति बढ़ाए।

प्रत्येक स्थानांतरण के लिए एक TransferProof स्टोरेज ऑब्जेक्ट बनाया जाता है, विवरण जैसे वैश्विक अद्वितीय स्थानांतरण गिनती। उपयोगकर्ता का वॉलेट हाल के ब्लॉक हेडर की स्टोरेज रूट से इस TransferProof की पत्ती तक Merkle-Patricia-Trie (MPT) स्टोरेज प्रूफ उत्पन्न करता है। डबल-स्पेंड रोकने के लिए nullifier गणना की जाती है:

```
H(H(salt | secret | global_transfer_count))
```

एग्रीगेटर प्रवाह

कोई भी पक्ष (क्लाइंट, माइनर या तीसरा) Plonky2 पुनरावृत्ति से कई प्रूफ एकत्र कर सकता है, प्रूफ का वृक्ष बनाता है जहाँ प्रत्येक मूल प्रूफ संतानों को सत्यापित करता है, संतान प्रूफ के सार्वजनिक इनपुट एकत्रित:

— Nullifiers अपरिवर्तित पारित होते हैं

— निकास पते डिडुप्लिकेट होते हैं

— ब्लॉक हैश लिंक सिद्ध होते हैं फिर सबसे हाल के को छोड़कर छोड़ दिए जाते हैं

— डुप्लिकेट निकास पतों की राशियाँ जोड़ी जाती हैं

चेन / सत्यापक प्रवाह

नेटवर्क एकत्रित प्रूफ सत्यापित करता है: ब्लॉक हैश चेन पर है और हाल का है, nullifier अद्वित्व (डबल-स्पेंड रोकने के लिए), और प्रूफ वैधता। ZK सर्किट स्टोरेज प्रूफ सही होना,

nullifier गणना, पते की अखर्च योग्यता, इनपुट और आउटपुट के बीच शेष मिलान और ब्लॉक हेडर लिंकेज लागू करता है।

`plonky2` क्यों

— पहले से ऑडिट किया गया

— पोस्ट-क्वांटम

— कोई विश्वसनीय सेटअप नहीं

— कुशल प्रूफ/सत्यापन

— निर्बाध प्रूफ एकत्रण

— Rust-मूल कार्यान्वयन

— Substrate के no-std वातावरण के साथ संगत

> ### प्रदर्शन
>
> पुनरावर्ती प्रूफ 170 मिलीसेकंड में पूर्ण होते हैं संक्षिप्त आकार के साथ (प्रति एकत्रित प्रूफ 100 KB)। 5 MB ब्लॉक और सभी लेनदेन एक ही आउटपुट की ओर जाने के इष्टतम मामले में, वर्महोल पते एक ब्लॉक में ~153,000 लेनदेन पैक कर सकते हैं (4.9 MB / प्रति nullifier 32 बाइट): ~685 कच्चे ML-DSA लेनदेन (प्रत्येक 7.3 KB, 5 MB) पर 223x सुधार।

सुरक्षा नोट्स

संभावित जोखिमों में सर्किट/सत्यापन कार्यान्वयन दोषों से मुद्रास्फीति बग शामिल हैं, हालाँकि यदि पुनः-मिंटेड सिक्के शून्य-भेज पतों के शेष से अधिक हों तो यह आर्थिक रूप से पता चल सकता है। उपयोगकर्ता वैकल्पिक रूप से प्रकाशित करके सिद्ध कर सकते हैं कि पता वर्महोल है पहला हैश बिना गुप्त प्रकट किए। सत्यापन लेनदेन हस्ताक्षरित नहीं हैं,

इसलिए विफल लेनदेन के माध्यम से सेवा से इनकार को वित्तीय साधनों के बिना कम किया जाना चाहिए। टोकन आपूर्ति गणना बनी रहती है, क्योंकि पुनः-मिंट नए सिक्कों की तरह दिखते हैं लेकिन जलाने के माध्यम से अधिकतम आपूर्ति गारंटी बनाए रखते हैं।

अधिक तकनीकी विवरण के लिए QIP-0005 देखें।

सर्वसम्मति तंत्र

Quantus Network प्रूफ़-ऑफ़-वर्क (PoW) सर्वसम्मति एल्गोरिदम का उपयोग करता है जो Bitcoin सर्वसम्मति के वांछनीय गुण संरक्षित करता है जबकि ZK-प्रूफ प्रणालियों के साथ अनुकूलता सुधारता है **Poseidon2** के साथ SHA-256 बदलकर।

महत्वपूर्ण: यह परिवर्तन क्वांटम सुरक्षा के लिए नहीं किया जाता। SHA-256 जैसी क्रिप्टोग्राफ़िक हैश फ़ंक्शन क्वांटम एल्गोरिदम, विशेष रूप से ग्रोवर, से कमजोर होते हैं लेकिन नष्ट नहीं होते। कुछ पोस्ट-क्वांटम हस्ताक्षर योजनाएँ इस कारण सुरक्षित हैश को बुनियादी ब्लॉक के रूप में उपयोग करती हैं।

Poseidon2 Poseidon हैश फ़ंक्शन का परिष्करण है। SHA-256 जैसी पारंपरिक हैश वाली गणनाओं के लिए SNARKs या STARKs बनाना अक्सर Poseidon की तुलना में लगभग 100 गुना अधिक गेट चाहता है, जो पूरी तरह बीजगणितीय फ़ंक्शन पर निर्भर करता है फ़ील्ड तत्वों पर, बिट-स्तर संचालन के बजाय।

हम Poseidon2 और Plonky2 दोनों के लिए **गोल्डीलॉक्स फ़ील्ड** का उपयोग करते हैं। गोल्डीलॉक्स फ़ील्ड का क्रम अहस्ताक्षरित 64-बिट पूर्णांक में फिट होता है, जिससे ध्वनिता से समझौता किए बिना दक्षता बढ़ती है।

05

धन संरक्षण

क्रिप्टोकरेंसी कुंजियों के प्रबंधन में कई जोखिम हैं। अधिकांश टाले जा सकते हैं।

प्रतिवर्तनीय लेनदेन

Quantus Network उपयोगकर्ता-कॉन्फ़िगर करने योग्य प्रतिवर्तनीय लेनदेन प्रदान करता है। प्रेषक एक समय खिड़की निर्धारित करते हैं जिसमें वे आउटगोइंग स्थानांतरण रद्द कर सकते हैं। यह चोरी को रोकता है और अंतिमता बलिदान किए बिना त्रुटियाँ सुधारता है। प्रणाली टाइमस्टैम्प के साथ संशोधित Substrate «scheduler» पैलेट का उपयोग करती है। वॉलेट प्रेषक के लिए (रद्द बटन के साथ) और प्राप्तकर्ता दोनों के लिए उलटी गिनती दिखाते हैं।

प्रतिवर्तनीय लेनदेन ऑन-चेन प्रवर्तन के माध्यम से विकेंद्रीकरण बनाए रखते हुए नवीन सुरक्षा प्रोटोकॉल सक्षम करते हैं।

अधिक तकनीकी विवरण के लिए QIP-0009 देखें।

चेक-फ़्रेज़

Quantus Network «चेक-फ़्रेज़» पेश करता है, ब्लॉकचेन पतों के लिए क्रिप्टोग्राफ़िक रूप से सुरक्षित मानव-पठनीय चेकसम। पता हैश करके BIP-39 म्नेमोनिक सूची से यादगार शब्दों की छोटी श्रृंखला उत्पन्न होती है। चेक-फ़्रेज़ टाइपो, छेड़छाड़ और पता विषाक्तता हमलों से बचाते हैं। 50,000 पुनरावृत्ति कुंजी व्युत्पन्न फ़ंक्शन इंद्रधनुष तालिका हमलों को महंगा बनाता है। बड़े लेनदेन के लिए, उपयोगकर्ताओं को अभी भी पते के प्रत्येक अक्षर की जाँच करनी चाहिए।

अधिक तकनीकी विवरण के लिए QIP-0008 देखें।

उच्च सुरक्षा खाते

कोई भी खाता सभी आउटगोइंग स्थानांतरणों पर अनिवार्य प्रतिवर्तन अवधि के साथ «उच्च सुरक्षा खाते» में उन्नत किया जा सकता है। नामित **गार्जियन** (हार्डवेयर वॉलेट, मल्टीसिग या विश्वसनीय तीसरा पक्ष) प्रतिवर्तन अवधि के दौरान संदिग्ध लेनदेन रद्द कर सकता है, धन प्रेषक या प्राप्तकर्ता के बजाय गार्जियन को भेजकर। यह ऑप्ट-इन सुविधा एक बार सक्रिय होने के बाद स्थायी है, चोरों को इसे बंद करने से रोकती है।

गार्जियन चेन किए जा सकते हैं: उच्च सुरक्षा खाते का गार्जियन स्वयं अपने गार्जियन वाला उच्च सुरक्षा खाता हो सकता है। यह संयोज्य पदानुक्रम बनाता है जहाँ प्रत्येक गार्जियन की सुरक्षित खाते पर श्रेष्ठ अनुमतियाँ होती हैं। डिज़ाइन उपयोगकर्ताओं को अनधिकृत गतिविधि का पता लगाने और प्रतिक्रिया करने का समय देता है बिना वैध स्थानांतरणों की अंतिमता से समझौता किए।

अधिक तकनीकी विवरण के लिए QIP-0011 देखें।

कुंजी पुनर्प्राप्ति

कई क्रिप्टो संपत्तियाँ मालिकों के साथ कब्र में चली गईं। Quantus Network पुनर्प्राप्ति पता निर्दिष्ट करने का सरल तरीका प्रदान करता है जो किसी भी समय आपके धन खींच सकता है, निश्चित विलंब के अधीन। इस दौरान, मालिक कुंजी तक पहुँच होने पर पुनर्प्राप्ति अस्वीकार कर सकता है। यह सुविधा उत्तरजीविता सक्षम करती है: उपयोगकर्ताओं के पास ऑन-चेन वसीयत है बिना अदालत या औपचारिक एस्टेट।

hd-lattice

पदानुक्रमित नियतात्मक (HD) वॉलेट उद्योग मानक हैं ब्लॉकचेन के लिए, एक बीज वाक्यांश से सभी कुंजियों का बैकअप, प्रति क्रिया मैनुअल बैकअप की तुलना में सुरक्षा और सुविधा बेहतर। Dilithium जैसी जाली योजनाओं के लिए इसे अनुकूलित करने में दो चुनौतियाँ:

— HMAC-SHA512 आउटपुट सीधे जाली निजी कुंजी नहीं बना सकते, जो कुछ गुणों वाले रिंग से नमूना लिए गए बहुपद हैं।

— गैर-कठोर कुंजी व्युत्पत्ति दीर्घवृत्तीय वक्र जोड़ पर निर्भर करती है, जालियों में अनुपस्थित (सार्वजनिक कुंजियाँ किसी बीजगणितीय संक्रिया के तहत बंद नहीं)।

Quantus Network पहले बिंदु को HMAC आउटपुट को एन्ट्रॉपी के रूप में उपयोग करके संबोधित करता है ताकि नियतात्मक रूप से निजी कुंजी बनाई जा सके, स्वयं कुंजी के रूप में नहीं। दूसरा बिंदु कम महत्वपूर्ण है और अनुसंधान का खुला प्रश्न रहता है कि क्या जाली क्रिप्टोग्राफ़ी इसे हल करने के लिए अनुकूलित की जा सकती है।

अधिक तकनीकी विवरण के लिए QIP-0002 देखें।

06

टोकनोमिक्स और शासन

Quantus Network बदलते वातावरण में मौजूद है और हम नहीं मान सकते कि पहली कोशिश में सब सही होगा। इसलिए हम एक सरल प्रारंभिक बिंदु चुनते हैं और शासन प्रणाली को नई जानकारी मिलने पर परिवर्तन करने देते हैं। यह डिज़ाइन ब्लॉकचेन को जीवित संस्था बनाता है जो अपने वातावरण के अनुकूल हो सकती है। विशेष रूप से, Substrate शासन प्रक्रिया विभिन्न नोड ऑपरेटरों के बीच न्यूनतम समन्वय के साथ चेन में गहरे परिवर्तन की अनुमति देती है।

ब्लॉक पुरस्कार

Quantus Network Bitcoin की तरह सरल टोकनोमिक्स मॉडल का उपयोग करता है। अधिकतम आपूर्ति **21,000,000 सिक्के** है और सरल ह्यूरिस्टिक प्रति ब्लॉक पुरस्कार निर्धारित करता है:

```
block_reward = (max_supply - current_supply) / co
```

यह ह्यूरिस्टिक चिकनी घातीय घटती वक्र बनाता है जैसे block_reward current_supply में योगदान करता है, जो अगले ब्लॉक पर गणना block_reward कम करता है। शुल्क या अन्य से कोई भी जल current_supply कम करता है और अनिवार्य रूप से ब्लॉक पुरस्कार बजट का हिस्सा बन जाता है। स्थिरांक इस तरह चुना गया है कि, बिना किसी जलने के, लगभग 30 वर्षों में 99% सिक्के जारी हों।

निवेशक आवंटन

Quantus Network निवेशकों की सहायता से बना जिन्होंने इसे वित्तपोषित करने में बड़ा जोखिम उठाया। निजी निवेशक 4 वर्ष की वेस्टिंग अनुसूची के अधीन हैं, टीम की

तरह। सार्वजनिक बिक्री के निवेशक पहले दिन से पूरी तरल होंगे। सार्वजनिक बिक्री में एकत्रित धन टोकन के साथ मिलाए जाएँगे और तरलता (DEX, CEX और मार्केट मेकर) के लिए उपयोग होंगे। ये निवेशक आवंटन साथ ही तरलता एकमात्र «प्री-माइन» होंगे। शेष टोकन को माइन करके अस्तित्व में लाना होगा।

यदि सार्वजनिक बिक्री के दौरान अधिकतम 10% से कम बिकता है, तरलता टोकन में समानुपातिक कमी होगी और शेष ब्लॉक पुरस्कारों के माध्यम से माइनरों को जारी होगा।

कंपनी आवंटन

टीम को बिना सफलता की गारंटी के नई तकनीकी बनाने के जोखिम के लिए क्षतिपूर्ति करने के लिए, लगभग चार वर्षों तक ब्लॉक पुरस्कार का एक हिस्सा कंपनी को जाता है। इससे कंपनी के लिए कुल आपूर्ति के लगभग **15%** की वेस्टिंग अनुसूची de facto मिलती है।

उस बिंदु के बाद, ब्लॉक पुरस्कार में कंपनी का हिस्सा टोकन धारक वोट के अनुसार बंद, समायोजित या पुनर्निर्देशित किया जा सकता है।

लेनदेन शुल्क

लेनदेन प्रकार	शुल्क संरचना	गंतव्य
मानक	निश्चित शुल्क	माइनर
प्रतिवर्तनीय (उच्च सुरक्षा)	आयतन पर 1%	जलाया गया
ZK एकत्रित	आयतन पर 0.1%	50% माइनर / 50% जलाया गया

बिना-फोर्क अपग्रेड

Quantus Network Substrate रनटाइम अपग्रेड के माध्यम से «बिना-फोर्क» अपग्रेड का समर्थन करता है, जिससे ब्लॉकचेन की मुख्य तर्क («रनटाइम») बिना हार्ड फोर्क के विकसित हो सकती है जो नेटवर्क को विघ्नित करे या समुदाय विभाजित करे। यह ऑन-चेन शासन जनमत संग्रह के माध्यम से हासिल होता है, जहाँ अनुमोदित प्रस्ताव रनटाइम स्वैप सक्रिय करते हैं — मौजूदा WASM कोड ब्लॉब को एक ब्लॉक में नए से प्रतिस्थापित करना, स्थिति और संचालन की निरंतरता सुनिश्चित करना। यह मार्ग निष्क्रियता और जोखिम कम करता है, समुदाय को वास्तविक उपयोग सुधार प्रकट करने पर प्रोटोकॉल को पुनरावृत्त रूप से परिष्कृत करने सशक्त बनाता है।

जैसे-जैसे समुदाय समय के साथ प्रणाली में विश्वास बढ़ाता है, रनटाइम बदलने की शक्ति काफ़ी कम कर दी जाएगी हमले की सतह सीमित करने के लिए, यदि दुर्भावनापूर्ण अभिनेता अपग्रेड प्रक्रिया पर नियंत्रण प्राप्त कर ले।

शासन प्रणाली

Quantus Network Substrate के माध्यम से Polkadot के OpenGov से अपना शासन ढाँचा विरासत में लेता है। टोकन धारक **विश्वास वोटिंग** के माध्यम से भाग लेते हैं, जहाँ वे वोट के भार को बढ़ाने के लिए विभिन्न अवधियों के लिए संपत्ति लॉक करने पर सहमत होते हैं। यह प्रवर्धन 1x (बिना लॉक) से 6x (अधिकतम लॉकअप) तक हो सकता है। यह डिज़ाइन प्रतिबद्धता से प्रभाव जोड़कर दीर्घकालिक संरेखण को प्रोत्साहित करता है।

प्रस्ताव कई वोटिंग ट्रैक में वर्गीकृत होते हैं जिन्हें «उत्पत्ति» कहा जाता है। प्रत्येक उत्पत्ति के अनुकूल पैरामीटर होते हैं जैसे अनुमोदन सीमा (उदा., उच्च प्रभाव परिवर्तनों के लिए सुपरमेजॉरिटी), स्पैम विरुद्ध न्यूनतम जमा, तैयारी/लागू अवधि और निर्णय समयसीमा

ग्रिडलॉक रोकने के लिए। यह बहु-ट्रैक डिज़ाइन विविध जनमत संग्रह समानांतर संसाधित करने देता है, रूटीन ट्रेजरी खर्च से महत्वपूर्ण रनटाइम अपग्रेड तक।

तकनीकी सामूहिक तकनीकी विशेषज्ञों का क्यूरेटेड समूह है जो तत्काल तकनीकी मामलों का प्रस्ताव, समीक्षा या व्हाइटलिस्ट करने के लिए विशेष निकाय के रूप में कार्य करता है, समर्पित ट्रैक के माध्यम से तेज़ करते हुए समुदाय की निगरानी बनाए रखता है।

Quantus इस प्रणाली को बिना संशोधन अपनाता है लेकिन प्रारंभिक चरणों में जटिलता से बचने के लिए न्यूनतम सेटअप से शुरू करता है। प्रारंभ में, केवल तकनीकी सामूहिक ट्रैक सक्रिय है, जिसका उपयोग प्रोटोकॉल अपग्रेड या पैरामीटर समायोजन जैसे बाध्यकारी, उच्च-विशेषाधिकार निर्णयों के लिए होगा।

बाद में, Quantus गैर-बाध्यकारी समुदाय वोट ट्रैक जोड़ सकता है लागू न करने योग्य विषयों पर भावना जाँचने के लिए, जैसे सुविधा सुझाव या पारिस्थितिकी सर्वेक्षण। जब कंपनी नेटवर्क DAO को सौंप देगी तो यह प्रणाली बाध्यकारी हो जाएगी। यह चरणबद्ध दृष्टिकोण भविष्य के शासन वोट के माध्यम से नेटवर्क को जैविक रूप से विकसित होने देता है बिना शुरुआत में अनावश्यक जटिलता उपयोगकर्ताओं पर लादे।

07

रोडमैप

2026 तक वर्तमान रोडमैप, परिवर्तन के अधीन।

heisenberg inception
दिसंबर 2024

वित्तपोषण सुरक्षित, Substrate चुना गया।

resonance alpha
जुलाई 2025

सार्वजनिक टेस्टनेट, Dilithium हस्ताक्षर, प्रतिवर्तनीय लेनदेन।

schrödinger beta
अक्टूबर 2025

सुविधाएँ पूर्ण, ऑडिट के लिए तैयार।

dirac beta
नवंबर 2025

PoW Poseidon2 में बदला, ऑडिट संबोधित।

planck beta
जनवरी 2026

उच्च सुरक्षा खाते, मल्टीसिग, हार्डवेयर वॉलेट, ZK एकीकरण।

bell mainnet
Q2 2026

मेननेट लॉन्च।

fermi upgrade
Q4 2026

ZK प्रूफ एकत्रण अवसंरचना।

08

जोखिम

Quantus Network बनाने में अंतर्निहित जोखिम हैं।

कार्यान्वयन समस्याएँ

सॉफ़्टवेयर तर्क में दोष गंभीर विफलता का कारण बन सकते हैं यहाँ तक कि सर्वोत्तम डिज़ाइन की प्रणालियों में भी।

nist एल्गोरिदम चयन समस्याएँ

चयनित पोस्ट-क्वांटम मानकों में संभावित दोष या बैकडोर (उदा., ML-DSA, ML-KEM) जो मानकीकरण के बाद सामने आ सकते हैं। सबसे बुरे मामले में, ऐसे दोष हमलावर को सार्वजनिक से निजी कुंजी निकालकर हस्ताक्षर जाली बनाने देंगे, जो चेन की विनाशकारी विफलता मोड होगी। यदि ऐसे दोष सार्वजनिक हों, Quantus Network नए एल्गोरिदम पर अपग्रेड कर सकता है, लेकिन यदि दुर्लभ रूप से शोषण हो तो कभी पता न चले।

क्वांटम कंप्यूटिंग समयरेखाएँ

क्वांटम सफलताएँ अपेक्षा से बहुत बाद आ सकती हैं, PQC की आवश्यकता देरी से; इसके विपरीत, गुप्त विकास (उदा. सरकारों द्वारा) अचानक खतरे पैदा कर सकता है यदि ब्लॉकचेन समुदाय तेज़ी से अपडेट न करे।

अन्य विचार

सामान्य अपनाने की बाधाएँ, वित्त/ब्लॉकचेन में नियामक अनिश्चितता, और क्रिप्टो पारिस्थितिकी तंत्र की अंतर्निहित अस्थिरता।

09

संदर्भ और आगे पढ़ने के लिए

[1] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509. https://doi.org/10.1137/S0097539795293172

[2] Grover, L.K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-Eight Annual ACM Symposium on Theory of Computing*, 212-219. https://doi.org/10.1145/237814.237866

[3] Chainalysis. (2024). *The Chainalysis 2024 Crypto Crime Report*. https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction/

[4] National Institute of Standards and Technology. (2024). *FIPS 204: Module-Lattice-Based Digital Signature Standard (ML- DSA)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

[5] National Institute of Standards and Technology. (2024). *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*. U.S. Department of

Commerce. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

[6] Häner, T., Jaques, S., Naehrig, M., Roetteler, M., & Soeken, M. (2020). Improved quantum circuits for elliptic curve discrete logarithms. *arXiv:2002.12480*. https://arxiv.org/abs/2002.12480

[7] Gidney, C., & Ekerå, M. (2021). *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*. *arXiv:1905.09749*. https://arxiv.org/abs/1905.09749

[8] Aggarwal, D., et al. (2021). Assessment of Quantum Threat To Bitcoin and Derived Cryptocurrencies. *ePrint IACR*. https://eprint.iacr.org/2021/967.pdf

[9] Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017). Quantum resource estimates for computing elliptic curve discrete logarithms. *arXiv:1706.06752*. https://arxiv.org/abs/1706.06752

[10] Open Quantum Safe Project. (n.d.). ML-DSA | Open Quantum Safe. Retrieved January 29, 2026, from https://openquantumsafe.org/liboqs/algorithms/sig/ml-dsa.html