Quantus Network Whitepaper

लेखक: Christopher Smith | **अंतिम अपडेट:** 14 जनवरी 2026

परिचय

क्वांटम खतरा

पारंपरिक ब्लॉकचेन क्वांटम कंप्यूटिंग के आगमन से अस्तित्व के खतरे का सामना कर रहे हैं। ब्लॉकचेन की क्रिप्टोग्राफिक नींव डिस्क्रीट लॉगरिदम प्रॉब्लम (DLP) की कठोरता पर निर्भर करती है, और क्वांटम एल्गोरिदम, विशेष रूप से शोर (Shor's), शास्त्रीय कंप्यूटरों की तुलना में DLP को तेजी से हल कर सकते हैं। यह भेद्यता क्वांटम-विरोधियों को सार्वजनिक कुंजी से निजी कुंजी प्राप्त करने में सक्षम बना सकती है, जिससे उन्हें लेनदेन को जाली बनाने और संवेदनशील वित्तीय डेटा को डिक्रिप्ट करने की अनुमति मिल सकती है।

इसका परिणाम एक विनाशकारी सिस्टम विफलता है। सक्रिय क्वांटम-प्रतिरोधी अपग्रेड के बिना, खरबों डॉलर की क्रिप्टो अर्थव्यवस्था ऐसे हमलों से अचानक अवमूल्यन का जोखिम उठाती है।

> 💡 **TIP**
> **Quantus इसे ठीक करता है।**

अनूठा मूल्य प्रस्ताव

"कितना" के लिए लैटिन शब्द के नाम पर, Quantus Network स्केलेबल, क्वांटम-सुरक्षित धन संरक्षण प्रदान करता है। Quantus एक स्मार्ट कॉन्ट्रैक्ट प्लेटफॉर्म नहीं है। इसके बजाय, बिना मेनू वाले हाई-एंड रेस्तरां की तरह, Quantus किसी भी अन्य chain की तुलना में कम संख्या में चीजों को बेहतर करने पर केंद्रित है।

विशेष रूप से, Quantus उपयोग करता है:

- सभी लेनदेन के लिए पोस्ट-क्वांटम signature
- पीयर कनेक्शन सुरक्षित करने के लिए पोस्ट-क्वांटम signature और एन्क्रिप्शन (ML-DSA और ML-KEM)
- अन्य ब्लॉकचेन के लिए एक पोस्ट-क्वांटम Bridge और क्वांटम-सुरक्षित रैप्ड सिक्के बनाना
- स्केल करने के लिए पोस्ट-क्वांटम zero-knowledge-proofs
- चोरी को रोकने और गलतियों से उबरने में सक्षम बनाने के लिए उच्च सुरक्षा खाते
- आसान पता सत्यापन के लिए मानव-पठनीय check-phrases

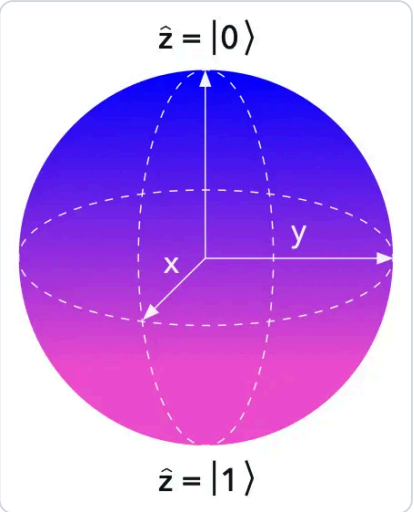
यह लक्षित दृष्टिकोण उपयोगकर्ताओं को आत्मविश्वास के साथ धन संरक्षित करने के लिए सशक्त बनाता है, क्वांटम खतरों को अवसरों में बदल देता है।

> 💡 **TIP**
> Quantus आपके भाग्य के लिए भविष्य-सुरक्षित किला है।

ब्लॉकचेन के लिए क्वांटम खतरा

क्वांटम कंप्यूटिंग की मूल बातें

क्वांटम कंप्यूटर शास्त्रीय मशीनों के लिए असाध्य गणना करने के लिए सुपरपोजिशन और उलझाव (entanglement) जैसे सिद्धांतों का लाभ उठाते हैं।



शास्त्रीय बिट्स के विपरीत, जो या तो 0 या 1 होते हैं, क्वांटम बिट्स (qubits) एक साथ कई अवस्थाओं में मौजूद हो सकते हैं, जो कुछ समस्याओं के लिए घातीय समानता को सक्षम करते हैं। **यह क्षमता ब्लॉकचेन वित्त को रेखांकित करने वाली क्रिप्टोग्राफिक प्रणालियों के लिए अस्तित्वगत जोखिम पैदा करती है, क्योंकि क्वांटम हार्डवेयर के लिए विकसित एल्गोरिदम अधिकांश सार्वजनिक-कुंजी क्रिप्टोग्राफी की सुरक्षा मान्यताओं को कमजोर करते हैं।**

शोर का एल्गोरिदम (Shor's Algorithm)

पीटर शोर द्वारा 1994 में पेश किया गया, बड़े पूर्णांकों के गुणनखंड और क्वांटम कंप्यूटर पर डिस्क्रीट लॉगरिदम समस्या को हल करने के लिए एक बहुपद-समय विधि प्रदान करता है। संक्षेप में, यह किसी फ़ंक्शन की अवधि खोजने के लिए क्वांटम फूरियर ट्रांसफॉर्म (QFT) का फायदा उठाता है, जो RSA या एलिप्टिक कर्व क्रिप्टोग्राफी (ECC) जैसी योजनाओं के आधार पर ट्रैपडोर कार्यों के कुशल उलट की अनुमति देता है।

ब्लॉकचेन वित्त के लिए, इसका मतलब है कि पर्याप्त शक्तिशाली क्वांटम कंप्यूटर (अनुमानित ~2,300 लॉजिकल क्विबिट) वाला हमलावर बहुपद समय $O(n^3)$ में सार्वजनिक कुंजी से निजी कुंजी प्राप्त कर सकता है। यह एक अत्यधिक गति-अप है, जो कमजोर प्रणालियों को रातोंरात अप्रचलित बना देता है।

ग्रोवर का एल्गोरिदम (Grover's Algorithm)

1996 में लव ग्रोवर द्वारा प्रस्तावित, असंरचित खोज समस्याओं के लिए द्विघात गति प्रदान करता है, जिससे अवर्गीकृत डेटाबेस में एक विशिष्ट वस्तु खोजने का समय $O(n)$ से $O(\sqrt{n})$ संचालन तक कम हो जाता है। यह क्वांटम हस्तक्षेप के माध्यम से लक्ष्य अवस्था के आयाम को पुनरावृत्त रूप से बढ़ाकर काम करता है। हालांकि असममित क्रिप्टोग्राफी के लिए शोर की तरह विनाशकारी नहीं है, **ग्रोवर का प्रभाव हैश कार्यों और AES एन्क्रिप्शन जैसे सममित प्रिमिटिव पर पड़ता है, प्रभावी रूप से सुरक्षा स्तर को आधा कर देता है** (उदाहरण के लिए, एक 256-बिट कुंजी क्वांटम हमलों के खिलाफ 128 बिट्स की तरह व्यवहार करती है)।

प्रभावशाली होने के बावजूद, इस हमले को क्रिप्टोग्राफिक योजना को बदलने के बजाय केवल सुरक्षा बिट्स को दोगुना करके कम किया जाता है। इसके अतिरिक्त, ग्रोवर का द्विघात त्वरण इसके उच्च क्विबिट और गेट आवश्यकताओं के कारण अव्यावहारिक है, जिसके लिए अनुक्रम में अरबों संचालन की आवश्यकता होती है, सीमित समानता के साथ, भविष्य के हार्डवेयर पर भी वास्तविक दुनिया के उलटफेर के लिए इसे अक्षम बनाता है।

ब्लॉकचेन वित्त के लिए क्वांटम कंप्यूटिंग के खतरों को चार क्षेत्रों में वर्गीकृत किया जा सकता है:

डिजिटल signature को जाली बनाना

शोर का एल्गोरिदम सीधे अधिकांश ब्लॉकचेन (जैसे, बिटकॉइन का secp256k1 कर्व) में उपयोग किए जाने वाले ECC-आधारित signature को खतरे में डालता है, जिससे विरोधियों 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 एक महत्वपूर्ण विफलता का प्रतिनिधित्व करेगी।

जीरो-नॉलेज सिस्टम में झूठे सबूत बनाना

कई जीरो-नॉलेज प्रूफ, जैसे कि गोपनीयता-केंद्रित वित्त के लिए zk-SNARKs में, प्रतिबद्धताओं के लिए एलिप्टिक-कर्व पेयरिंग के माध्यम से डिस्क्रीट लॉगरिदम कठोरता पर भरोसा करते हैं; शोर अमान्य सबूतों के निर्माण को सक्षम कर सकता है जो मान्य दिखाई देते हैं, जो हमलावर को नए सिक्के बनाने या लेयर-2s (L2s) की स्थिति को गलत साबित करने की अनुमति दे सकता है।

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। यह वित्तीय प्रोटोकॉल में p2p संचार को भी डिक्रिप्ट कर सकता है, संवेदनशील धन विवरण प्रकट कर सकता है और लक्षित चोरी को सक्षम कर सकता है।

हैश कार्यों को उलटना

ग्रोवर का एल्गोरिदम SHA-256 जैसे हैश पर प्रीइमेज हमलों को तेज कर सकता है, जिसका उपयोग प्रूफ-of-work और पता निर्माण के लिए किया जाता है, लेकिन यह सबसे कम चिंताजनक खतरा है। कई पोस्ट-क्वांटम क्रिप्टोग्राफिक योजनाएं हैश-आधारित निर्माणों को शामिल करती हैं क्योंकि हैश को पर्याप्त बड़े डाइजेस्ट के साथ पर्याप्त सुरक्षित माना जाता है।

पोस्ट-क्वांटम क्रिप्टोग्राफी में स्केलिंग चुनौतियां

जबकि पोस्ट-क्वांटम क्रिप्टोग्राफी (PQC) क्वांटम खतरों के खिलाफ आवश्यक सुरक्षा प्रदान करती है, यह इन एल्गोरिदम के अंतर्निहित डिजाइन के कारण महत्वपूर्ण स्केलिंग बाधाओं को पेश करती है। एलिप्टिक कर्व योजनाओं के विपरीत, जो कॉम्पैक्ट गणितीय संरचनाओं पर भरोसा करते हैं, PQC प्रिमिटिव को शास्त्रीय और क्वांटम दोनों विरोधियों के खिलाफ सुरक्षा बनाए रखने के लिए बड़े मापदंडों की आवश्यकता होती है। इसके परिणामस्वरूप काफी बड़ी सार्वजनिक कुंजी, निजी कुंजी और signature होते हैं, जो अक्सर परिमाण के आदेशों द्वारा होते हैं।

निम्न तालिका 128-बिट पोस्ट-क्वांटम सुरक्षा स्तर पर ML-DSA के लिए विशिष्ट आकारों को 256-बिट ECDSA जैसे शास्त्रीय समकक्षों की तुलना में दर्शाती है:

एल्गोरिदम	सार्वजनिक कुंजी आकार (बाइट्स)	निजी कुंजी आकार (बाइट्स)	signature आकार (बाइट्स)
ML-DSA-87 (Dilithium)	2,592	4,896	4,627
ECDSA (256-बिट)	32	32	65

जैसा कि दिखाया गया है, ML-DSA signature ECDSA समकक्षों की तुलना में 70 गुना से अधिक बड़े हो सकते हैं, और सार्वजनिक कुंजी 80 गुना से अधिक बड़ी हो सकती है।

अन्य PQC परिवार इसे और बढ़ाते हैं: SPHINCS+ जैसी हैश-आधारित योजनाएं 41 KB तक के signature उत्पन्न कर सकती हैं, जबकि आकार-अनुकूलित जाली वेरिएंट जैसे FALCON अभी भी शास्त्रीय आकारों से काफी अधिक हैं।

ब्लॉकचेन संदर्भों में, ये बढ़े हुए आकार प्रणालीगत स्केलिंग मुद्दों में बदल जाते हैं। बड़े signature व्यक्तिगत लेनदेन को बढ़ाते हैं, प्रति सेकंड लेनदेन (TPS) को कम करते हैं क्योंकि ब्लॉक तेजी से भरते हैं और सत्यापन के लिए अधिक समय की आवश्यकता होती है। यह पीयर-टू-पीयर (P2P) संचार को भी तनावपूर्ण बनाता है, बैंडविड्थ की मांग और प्रसार में देरी को बढ़ाता है, जो प्रूफ-of-work जैसे सर्वसम्मति तंत्र में नेटवर्क फोर्क्स या अनाथ ब्लॉकों के जोखिम को बढ़ा सकता है। भंडारण आवश्यकताएं भी प्रभावित होती हैं, जिससे उच्च नोड परिचालन लागत और भागीदारी के लिए बाधाएं आती हैं, विशेष रूप से संसाधन-विवश उपयोगकर्ताओं या सत्यापनकर्ताओं के लिए।

इन स्केलिंग चुनौतियों को भविष्य में सभी ब्लॉकचेन द्वारा संबोधित करना होगा। उदाहरण के लिए, यदि अधिकतम ब्लॉक आकार नहीं बढ़ाया जाता है, तो बिटकॉइन में 1 TPS से बहुत कम होगा।

Quantus Network आर्किटेक्चर

पोस्ट-क्वांटम क्रिप्टोग्राफिक प्रिमिटिव

Quantus Network क्वांटम खतरों के खिलाफ लेनदेन और नेटवर्क संचार की सुरक्षा सुनिश्चित करने के लिए **NIST-मानकीकृत PQC** प्रिमिटिव का उपयोग करता है। लेनदेन अखंडता के मूल में **ML-DSA (Module-Lattice-based Digital Signature Algorithm**, जिसे पहले CRYSTALS-Dilithium के रूप में जाना जाता था) है, जो सुरक्षा, दक्षता और कार्यान्वयन में आसानी के संतुलन के लिए चुनी गई एक जाली-आधारित हस्ताक्षर योजना है। **ML-DSA मॉड्यूल जाली पर लर्निंग विद एरर्स (LWE) और शॉर्ट इंटीजर सॉल्यूशन (SIS)** जैसी समस्याओं की कठोरता का लाभ उठाता है, जो शोर के एल्गोरिदम सहित शास्त्रीय और क्वांटम दोनों हमलों के लिए मजबूत प्रतिरोध प्रदान करता है।

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

विकल्प

ML-DSA को FN-DSA (Falcon) जैसे विकल्पों पर चुना गया था क्योंकि:

- FN-DSA की अधिक कार्यान्वयन जटिलता (जैसे, फ्लोटिंग-पॉइंट संचालन की आवश्यकता, जो ब्लॉकचेन-अनुकूल नहीं हैं)
- इसके विनिर्देश में नियतात्मक कुंजी निर्माण की कमी
- विकास के समय इसकी गैर-अंतिम स्थिति

SLH-DSA जैसे हैश-आधारित विकल्पों को उनके और भी बड़े हस्ताक्षर आकार (17 KB से अधिक) के लिए खारिज कर दिया गया था। क्रिप्टो-चपलता (विभिन्न हस्ताक्षर योजनाओं में अदला-बदली करने में सक्षम होना) सबस्ट्रेट में बनाया गया है, इसलिए भविष्य की तारीख में इन विकल्पों को जोड़ना अपेक्षाकृत आसान है, यदि परिस्थितियां मांग करती हैं।

जबकि ML-DSA-87 के परिणामस्वरूप बड़ी कुंजियाँ और signature होते हैं, ये Quantus के शुरुआती चरण के नेटवर्क में प्रबंधनीय हैं, जहाँ भंडारण अभी तक एक अड़चन नहीं है, और जीरो-नॉलेज प्रूफ के माध्यम से वर्महोल एड्रेस (wormhole addresses) जैसे भविष्य के अनुकूलन स्केलिंग को संबोधित करेंगे।

कार्यान्वयन के बारे में तकनीकी विवरण के लिए QIP-0006 देखें।

LibP2P

Quantus Network प्रमाणीकरण के लिए ML-DSA और एन्क्रिप्शन के लिए ML-KEM (Module-Lattice-based Key Encapsulation Mechanism, जिसे पहले CRYSTALS-Kyber के रूप में जाना जाता था) के संयोजन का उपयोग करके पीयर-टू-पीयर (P2P) नोड संचार को सुरक्षित करता है।

यह एकीकरण PQC को libp2p नेटवर्किंग स्टैक तक विस्तारित करता है, क्वांटम प्रतिरोध के लिए मुख्य घटकों को संशोधित करता है: पीयर पहचान के लिए ML-DSA-87 signature और परिवहन सुरक्षा के लिए ML-KEM-768 का उपयोग करना (क्वांटम-प्रतिरोधी साझा रहस्यों के लिए एक अतिरिक्त KEM संदेश के साथ Noise हैंडशेक का विस्तार करना)।

क्वांटम-सुरक्षा विश्लेषण में P2P परत की अक्सर उपेक्षा की जाती है। साथियों का प्रमाणीकरण महत्वपूर्ण है, लेकिन पीयर स्तर पर हमलावर जो सबसे बुरा कर सकता है वह है नोड का रूप धारण करना और अमान्य संदेश भेजना, जिसके परिणामस्वरूप सेवा से इनकार (DoS) हो सकता है। यह हमला पहले से ही इस तथ्य से कम हो गया है कि ब्लॉकचेन मॉडल में नोड्स आम तौर पर अविश्वसनीय होते हैं और यदि हमले का पता चलता है तो नोड्स आसानी से अपनी कुंजियाँ बदल सकते हैं। इसी तरह, P2P संचार को डिक्रिप्ट करने से हमलावर को सीमित लाभ मिलता है (जैसे, लेनदेन पथों को ट्रैक करना, प्रॉक्सी या Tor द्वारा कम किया गया), और अधिकांश डेटा वैसे भी ऑन-चेन सार्वजनिक हो जाता है।

फिर भी, P2P परत को क्वांटम-सुरक्षित करना ईव्सड्रॉपिंग, मैन-इन-द-मिडल हमलों और क्वांटम डिक्रिप्शन से बचाता है, यह सुनिश्चित करता है कि नोड गॉसिप, ब्लॉक प्रसार और अन्य नेटवर्क इंटरैक्शन निकट भविष्य के लिए गोपनीय और छेड़छाड़-प्रूफ बने रहें।

कार्यान्वयन के बारे में तकनीकी विवरण के लिए QIP-0004 देखें।

PQC स्केलिंग

पोस्ट-क्वांटम क्रिप्टोग्राफी में निहित स्केलिंग चुनौतियों का समाधान करने के लिए, **Quantus Network "वर्महोल एड्रेस" (Wormhole Addresses) नामक एक अभिनव एकत्रित पोस्ट-क्वांटम हस्ताक्षर योजना पेश करता है।** यह प्रणाली प्लोंकी 2 (Plonky2) सिद्ध प्रणाली (मूल रूप से STARKs) के माध्यम से उत्पन्न जीरो-नॉलेज प्रूफ (ZKPs) का लाभ उठाती है ताकि बैलेंस सत्यापन को ऑफ-चेन ले जाया जा सके, जिससे चेन व्यक्तिगत signature को संसाधित किए बिना एक कॉम्पैक्ट सबूत को सत्यापित कर सके।

वर्महोल एड्रेस एक सबूत के साथ बड़ी संख्या में लेनदेन के सत्यापन को सक्षम करते हैं, सार्वजनिक इनपुट (जैसे, नलफायर, स्टोरेज रूट, निकास पते और मात्रा) प्राथमिक सीमित कारक बन जाते हैं। यह प्रति-लेनदेन भंडारण मांगों को **प्रति लेनदेन लगभग 256 अतिरिक्त बाइट्स तक कम कर देता है, जो किसी भी ज्ञात PQC हस्ताक्षर योजना से बहुत छोटा है।**

योजना की क्वांटम सुरक्षा SNARKs में आमतौर पर उपयोग किए जाने वाले क्वांटम-कमजोर एलिप्टिक-कर्व पेयरिंग के बजाय, FRI (Fast Reed-Solomon Interactive Oracle Proofs) के माध्यम से प्रतिबद्धताओं के लिए सुरक्षित हैश फ़ंक्शन Poseidon2 के उपयोग से प्राप्त होती है।

इसके अतिरिक्त प्रमाणीकरण रहस्य Poseidon2 के पीछे छिपे हुए हैं। चूंकि सुरक्षित हैश फ़ंक्शन केवल ग्रोवर के एल्गोरिदम द्वारा द्विघात रूप से कमजोर होते हैं, टूटे नहीं, हैश प्रीइमेज प्रूफ ZK संदर्भों में हल्के पोस्ट-क्वांटम

signature के रूप में काम कर सकते हैं, जो SPHINCS+ जैसी हैश-आधारित योजनाओं के समान है।

क्लाइंट / प्रोवर फ्लो

उपयोगकर्ता एक रहस्य के साथ जुड़े नमक (salt) को डबल-हैशिंग करके एक प्रमाणित रूप से खर्च न करने योग्य पता उत्पन्न करते हैं:

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

यह निर्माण झूठी सकारात्मकता को रोकता है (उदाहरण के लिए, एक एकल-हैश सार्वजनिक कुंजी को खर्च न करने योग्य पते के रूप में समझना) क्योंकि सबस्ट्रेट (और आम तौर पर) ब्लॉकचेन पते सार्वजनिक कुंजी के एकल हैश होते हैं, जो निजी कुंजी से कुछ बीजगणितीय संचालन के माध्यम से प्राप्त होते हैं, न कि सुरक्षित हैश के माध्यम से। इसलिए निर्माण की सुरक्षा एक सुरक्षित हैश के प्रीइमेज-ऑफ-ए-प्रीइमेज को खोजने के लिए कम हो जाती है। इस पते पर भेजे गए टोकन प्रभावी रूप से जला दिए जाते हैं। उन्हें खर्च नहीं किया जा सकता क्योंकि उन्हें प्राप्त करने वाले पते के लिए कोई निजी कुंजी मौजूद नहीं है। इसलिए इन सिक्कों को आपूर्ति फुलाए बिना फिर से बनाया (re-minted) जा सकता है।

प्रत्येक हस्तांतरण के लिए, एक TransferProof स्टोरेज ऑब्जेक्ट बनाया जाता है, जिसमें एक अद्वितीय वैश्विक हस्तांतरण गणना जैसे विवरण होते हैं। उपयोगकर्ता का वॉलेट हाल के ब्लॉक हेडर के स्टोरेज रूट से इस TransferProof के लिए लीफ तक एक मर्कल-पेट्रीसिया-ट्री (MPT) स्टोरेज प्रूफ उत्पन्न करता है।

एक नलफायर (nullifier) की गणना की जाती है:

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

रिटेंशन के लिए वॉलेट सीड से नियतात्मक रूप से प्राप्त रहस्य के साथ डबल-स्पेंड को रोकने के लिए।

एग्रीगेटर फ्लो

कोई भी पक्ष (क्लाइंट, माइनर, या थर्ड-पार्टी) प्लोंकी 2 के रिकर्सन का उपयोग करके कई सबूतों को एकत्रित कर सकता है, सबूतों का एक पेड़ बना सकता है जहां प्रत्येक मूल सबूत बाल सबूतों का सत्यापन है, बाल सबूतों के सार्वजनिक इनपुट एकत्रित किए गए हैं:

- नलफायर अपरिवर्तित गुजरते हैं
- निकास पते डुप्लिकेट किए जाते हैं
- ब्लॉक हैश जुड़े हुए साबित होते हैं और फिर सबसे हाल के को छोड़कर सभी को छोड़ दिया जाता है
- डुप्लिकेट निकास पतों के लिए मात्राओं को संक्षेप में प्रस्तुत किया जाता है यह रिकर्सन पदानुक्रमित एकत्रीकरण का समर्थन करता है, ऑन-चेन डेटा को काफी कम करता है।

चेन / सत्यापनकर्ता फ्लो

नेटवर्क निम्नलिखित की जाँच करके एकत्रित सबूत को सत्यापित करता है:

- ब्लॉक हैश ऑन चेन और हाल ही में है
- नलफायर विशिष्टता (डबल-स्पेंड को रोकने के लिए)
- सबूत की वैधता

ZK सर्किट लागू करता है:

- स्टोरेज प्रूफ शुद्धता
- नलफायर गणना सटीकता
- पता खर्च न करने की क्षमता
- इनपुट और आउटपुट के बीच बैलेंस मिलान
- ब्लॉक हेडर लिंकेज

प्लोंकी 2 को निम्नलिखित कारणों से चुना गया था:

- पहले से ही ऑडिट किया गया
- पोस्ट-क्वांटम
- कोई विश्वसनीय सेटअप (trusted setup) नहीं
- कुशल सिद्ध/सत्यापन
- निर्बाध सबूत एकत्रीकरण
- रस्ट-नेटिव कार्यान्वयन
- सबस्ट्रेट के no-std वातावरण के साथ संगत

प्रदर्शन हाइलाइट्स में शामिल हैं:

170 मिलीसेकंड में रिकर्सिव प्रूफ और कॉम्पैक्ट आकार (प्रति एकत्रित सबूत 100 KB), बड़े पैमाने पर थ्रूपुट लाभ सक्षम करते हैं।

5 MB ब्लॉक और एक ही आउटपुट पर जाने वाले सभी लेनदेन के साथ एक इष्टतम मामले में, **वर्महोल एड्रेस एक ही ब्लॉक में ~153,000 लेनदेन पैक कर सकते हैं** (4.9 MB / प्रति नलफायर 32 बाइट्स), जो ~685 कच्चे ML-DSA लेनदेन (5 MB / प्रत्येक 7.3 KB) पर 223 गुना सुधार है।

सुरक्षा नोट

संभावित जोखिमों में दोषपूर्ण सर्किट/सत्यापन कार्यान्वयन से मुद्रास्फीति कीड़े शामिल हैं, हालांकि यह आर्थिक रूप से पता लगाने योग्य होगा यदि फिर से बनाए गए सिक्के शून्य-भेजने वाले पतों के बैलेंस से अधिक हो जाते हैं। उपयोगकर्ता वैकल्पिक रूप से रहस्य को प्रकट किए बिना पहला हैश प्रकाशित करके साबित कर सकते हैं कि एक पता वर्महोल है। सत्यापन लेनदेन अहस्ताक्षरित हैं, इसलिए विफल लेनदेन के माध्यम से सेवा से इनकार को गैर-वित्तीय रूप से कम करने

की आवश्यकता है। टोकन आपूर्ति गणना बनाए रखी जाती है, क्योंकि फिर से टकसाल नए सिक्कों के रूप में दिखाई देते हैं लेकिन जलने के माध्यम से अधिकतम आपूर्ति गारंटी बनाए रखते हैं।

कार्यान्वयन के बारे में अधिक तकनीकी विवरण के लिए QIP-0005 देखें।

सर्वसम्मति तंत्र

Quantus Network एक प्रूफ-of-work (PoW) सर्वसम्मति एल्गोरिदम का उपयोग करता है जो SHA-256 को Poseidon2 के साथ बदलकर ZK-प्रूफ सिस्टम के साथ अनुकूलता में सुधार करते हुए बिटकॉइन के सर्वसम्मति एल्गोरिदम के वांछनीय गुणों को संरक्षित करता है।

महत्वपूर्ण रूप से, यह परिवर्तन क्वांटम सुरक्षा के लिए नहीं किया जा रहा है। SHA-256 जैसे क्रिप्टोग्राफिक हैश फ़ंक्शन क्वांटम एल्गोरिदम, विशेष रूप से ग्रोवर द्वारा कमजोर किए जाते हैं लेकिन नष्ट नहीं होते हैं। कुछ पोस्ट-क्वांटम हस्ताक्षर योजनाएं इसी कारण से बिल्डिंग ब्लॉक के रूप में सुरक्षित हैश का उपयोग करती हैं।

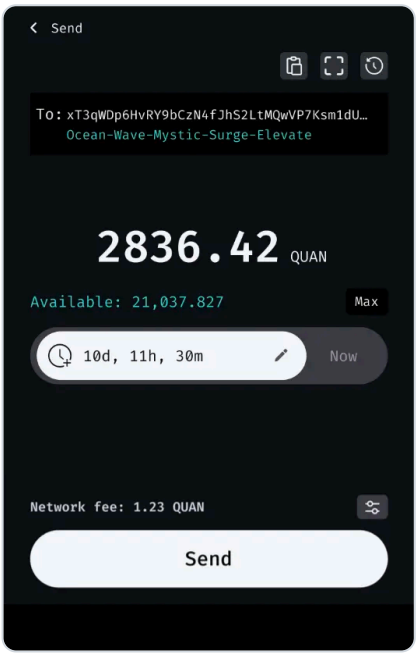
Poseidon2 पोसिडोन हैश फ़ंक्शन का एक शोधन है। SHA-256 जैसे पारंपरिक हैश कार्यों से जुड़े गणनाओं के लिए SNARKs या STARKs बनाना अक्सर पोसिडोन का उपयोग करने की तुलना में लगभग 100 गुना गेट्स की आवश्यकता होती है, जो बिट-स्तरीय संचालन के बजाय पूरी तरह से फील्ड तत्वों पर बीजगणितीय कार्यों पर निर्भर करता है। हम दक्षता को अधिकतम करने के लिए Poseidon2 और Plonky2 दोनों के लिए गोल्डिलॉक्स फील्ड का उपयोग करते हैं।

धन संरक्षण

क्रिप्टोकरेंसी कुंजियों के प्रबंधन में कई जोखिम हैं। उनमें से अधिकांश टालने योग्य हैं। Quantus Network चेन में ही उपयोग में आसानी का निर्माण करता है, जिससे गैर-विशेषज्ञों को मन की शांति के साथ लेनदेन करने में सक्षम बनाया जा सकता है।

प्रतिवर्ती लेनदेन (Reversible Transactions)

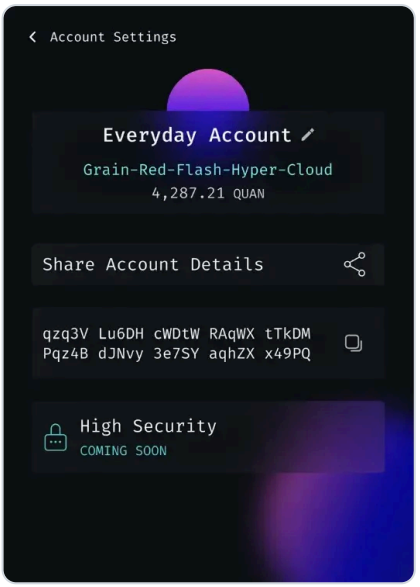
Quantus Network उपयोगकर्ता-कॉन्फ़िगर करने योग्य प्रतिवर्ती लेनदेन प्रदान करता है, जिससे प्रेषकों को एक समय विंडो सेट करने में सक्षम बनाया जा सकता है जिसके दौरान वे बाहर जाने वाले हस्तांतरण को रद्द कर सकते हैं, ब्लॉकचेन की मुख्य अपरिवर्तनीयता का त्याग किए बिना चोरी की रोकथाम और त्रुटि सुधार को बढ़ाते हैं। एक संशोधित सबस्ट्रेट "शेड्यूलर पैलेट" का लाभ उठाते हुए जो सहज देरी के लिए टाइमस्टैम्प का उपयोग करता है, सिस्टम क्लाइंट को एक सरल इंटरफ़ेस के माध्यम से हस्तांतरण शेड्यूल करने की अनुमति देता है, प्रेषक (रद्द करें बटन के साथ) और प्राप्तकर्ता (रद्द न होने पर पूरा होने का संकेत) दोनों के लिए वॉलेट में उलटी गिनती प्रदर्शित करता है। यह वाणिज्य के लिए त्वरित अंतिमता को उन उपयोगकर्ताओं के लिए लचीलेपन के साथ संतुलित करता है जो गलतियाँ करने के बारे में चिंतित हैं या एस्क्रो सेवा के बिना सद्भावना जमा करना चाहते हैं।



प्रतिवर्ती लेनदेन ऑन-चेन प्रवर्तन के माध्यम से विकेंद्रीकरण को बनाए रखते हुए उपन्यास सुरक्षा प्रोटोकॉल के लिए एक शक्तिशाली बिल्डिंग ब्लॉक बनाते हैं।

अधिक तकनीकी विवरण के लिए QIP-0009 देखें।

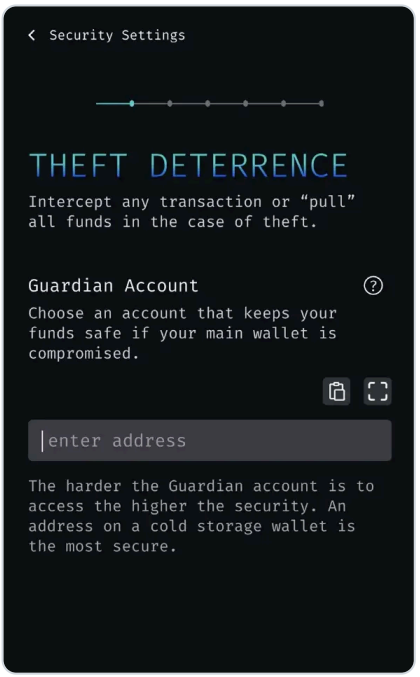
Check-Phrases



Quantus Network "check-phrases" पेश करता है, जो ब्लॉकचेन पते और मानव सत्यापन की आवश्यकता वाले अन्य डेटा के लिए एक क्रिप्टोग्राफिक रूप से सुरक्षित मानव-पठनीय चेकसम है। **BIP-39 निमोनिक सूची से यादगार शब्दों का एक छोटा अनुक्रम उत्पन्न करने के लिए पते को हैश करके, check-phrases त्वरित, त्रुटि-मुक्त अखंडता जांच सक्षम करते हैं, जो टाइपो, छेड़छाड़ और एड्रेस पॉइजनिंग (address poisoning) जैसे हमलों से बचाते हैं।** यह उपकरण उपयोगकर्ताओं को हस्तांतरण के दौरान कटे हुए डिस्प्ले या कमजोर चेकसम पर भरोसा किए बिना आत्मविश्वास से पते सत्यापित करने की अनुमति देता है। यह सुनिश्चित करने के लिए कि दिए गए चेकसम के लिए इंद्रधनुष तालिका (rainbow table) बनाना बहुत महंगा है, 50,000 पुनरावृत्ति कुंजी व्युत्पत्ति फ़ंक्शन का उपयोग किया जाता है। बेशक, बड़े लेनदेन के लिए, उपयोगकर्ताओं को अभी भी शुद्धता के लिए पते के हर अक्षर की मैन्युअल रूप से जांच करनी चाहिए।

अधिक तकनीकी विवरण के लिए कृपया QIP-0008 देखें।

उच्च-सुरक्षा खाते



Quantus Network किसी भी खाते को "उच्च-सुरक्षा खाते" में अपग्रेड करने की क्षमता प्रदान करता है जो सभी बाहर जाने वाले हस्तांतरण पर अनिवार्य उलट अवधि लागू करता है, जिससे हार्डवेयर वॉलेट, मल्टीसिग, या यहां तक कि उपयोगकर्ता द्वारा चुने गए विश्वसनीय-तृतीय-पक्ष जैसे नामित "अभिभावक" (guardian) खाते को उलट अवधि के दौरान विशेष रूप से संदिग्ध लेनदेन रद्द करने की अनुमति मिलती है, जिससे धन प्रेषक या प्राप्तकर्ता के बजाय अभिभावक को भेजा जाता है। यह ऑप्ट-इन, स्थायी सुविधा प्रतिवर्ती हस्तांतरण पर आधारित है, जहां उपयोगकर्ता सक्रियण पर देरी और इंटरसेप्टर निर्दिष्ट करते हैं, जिससे चोरों को इसे अक्षम करने से रोका जा सकता है।

इंटरसेप्टर स्वयं अपने अभिभावक के साथ एक और उच्च-सुरक्षा खाता हो सकता है, जो कंपोजेबल पदानुक्रम को सक्षम करता है जहां प्रत्येक अभिभावक के पास उस खाते के लिए बेहतर अनुमतियां होती हैं जिसकी वह रक्षा करता है। यह डिज़ाइन पारंपरिक वित्त के अदालत-आदेशित उलटफेर की नकल करता है लेकिन उपयोगकर्ता नियंत्रण के साथ। यह उच्च-मूल्य वाले खातों के लिए सुरक्षा और सुविधा को संतुलित करता है, वैध प्रवाह के लिए ब्लॉकचेन अंतिमता से समझौता किए बिना अनधिकृत गतिविधि का पता लगाने और प्रतिक्रिया देने के लिए समय देता है।

अधिक तकनीकी विवरण के लिए QIP-0011 देखें।

कुंजी रिकवरी

कई क्रिप्टो-भाग्य उनके मालिकों के साथ कब्र में चले गए हैं। Quantus Network एक रिकवरी पता निर्दिष्ट करने का एक सरल तरीका प्रदान करता है जो एक निश्चित देरी के अधीन किसी भी समय आपके धन को निकाल सकता है। इस दौरान, मालिक रिकवरी से इनकार कर सकता है यदि उनके पास कुंजी तक पहुंच है। यह सुविधा उत्तरजीविता को सक्षम बनाती है: उपयोगकर्ताओं के पास अदालतों या संपदाओं की आवश्यकता के बिना ऑन-चेन वसीयत होती है।

HD-Lattice

पदानुक्रमित नियतात्मक (HD) वॉलेट ब्लॉकचेन के लिए उद्योग मानक हैं, जो उपयोगकर्ताओं को सभी कुंजियों के लिए एक बीज वाक्यांश (seed phrase) का बैकअप लेने की अनुमति देते हैं, जिससे प्रति क्रिया मैन्युअल बैकअप की तुलना में सुरक्षा और सुविधा में सुधार होता है।

इसे डिलिथियम जैसी जाली योजनाओं के अनुकूल बनाने में दो चुनौतियाँ शामिल हैं:

- HMAC-SHA512 आउटपुट सीधे जाली निजी कुंजियाँ नहीं बना सकते हैं, जिन्हें अस्वीकृति नमूनाकरण (rejection sampling) के माध्यम से "अच्छे आधार" बहुपद की आवश्यकता होती है।
- गैर-कठोर (non-hardened) कुंजी व्युत्पत्ति एलिप्टिक कर्व जोड़ पर निर्भर करती है, जो जाली में अनुपस्थित है (सार्वजनिक कुंजियाँ किसी भी बीजगणितीय संचालन के तहत बंद नहीं होती हैं)।

Quantus Network HMAC के आउटपुट को निजी कुंजी को नियतात्मक रूप से बनाने के लिए एन्ट्रॉपी के रूप में उपयोग करके पहली समस्या का समाधान करता है, न कि निजी कुंजी के रूप में। दूसरी समस्या कम महत्वपूर्ण है और एक खुला शोध प्रश्न बनी हुई है कि क्या जाली क्रिप्टोग्राफी को इसे संबोधित करने के लिए अनुकूलित किया जा सकता है।

अधिक तकनीकी विवरण के लिए QIP-0002 देखें।

टोकनमिक्स और गवर्नेंस

Quantus Network एक बदलते परिवेश में मौजूद है, और हम यह नहीं मान सकते कि हम पहली कोशिश में ही सब कुछ सही कर लेंगे। इस कारण से, हम एक सरल प्रारंभिक बिंदु चुनते हैं और गवर्नेंस सिस्टम को नई जानकारी प्राप्त होने पर परिवर्तन करने की अनुमति देते हैं। यह डिज़ाइन ब्लॉकचेन को एक जीवित इकाई बनाता है जो अपनी इच्छा से अपने पर्यावरण के अनुकूल हो सकता है। विशेष रूप से, सबस्ट्रेट गवर्नेंस प्रक्रिया विभिन्न नोड-रनर के बीच न्यूनतम समन्वय के साथ चेन में गहरे बदलाव की अनुमति देती है।

ब्लॉक रिवॉर्ड्स

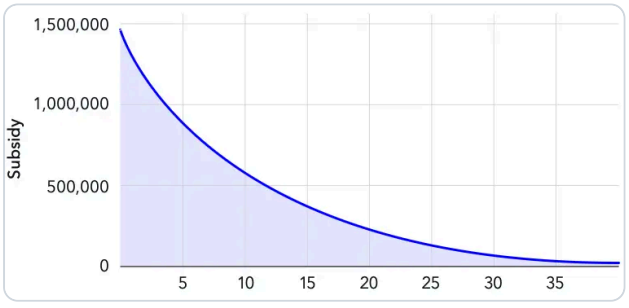
Quantus Network बिटकॉइन की नकल करते हुए एक सीधा टोकनमिक्स मॉडल नियोजित करता है। 21,000,000 सिक्कों की अधिकतम आपूर्ति है और एक सरल अनुमानी प्रत्येक ब्लॉक के इनाम को निर्धारित करता है।

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

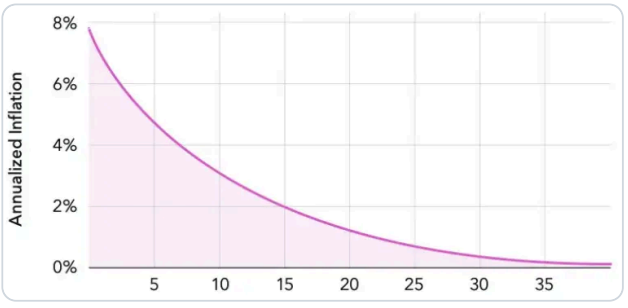
यह अनुमानी एक चिकनी घातीय क्षय वक्र बनाता है क्योंकि block_reward current_supply में योगदान देता है जो अगले ब्लॉक में गणना किए गए block_reward को कम करता है।

फीस या अन्यथा से कोई भी जलना current_supply को कम करता है और अनिवार्य रूप से ब्लॉक पुरस्कारों के बजट का हिस्सा बन जाता है। स्थिरांक को चुना जाता है ताकि, किसी भी जलने की अनुपस्थिति में, 99% सिक्के लगभग 40 वर्षों में उत्सर्जित हो जाएंगे।

ब्लॉक रिवॉर्ड्स / वर्ष



मुद्रास्फीति / वर्ष



निवेशक आवंटन

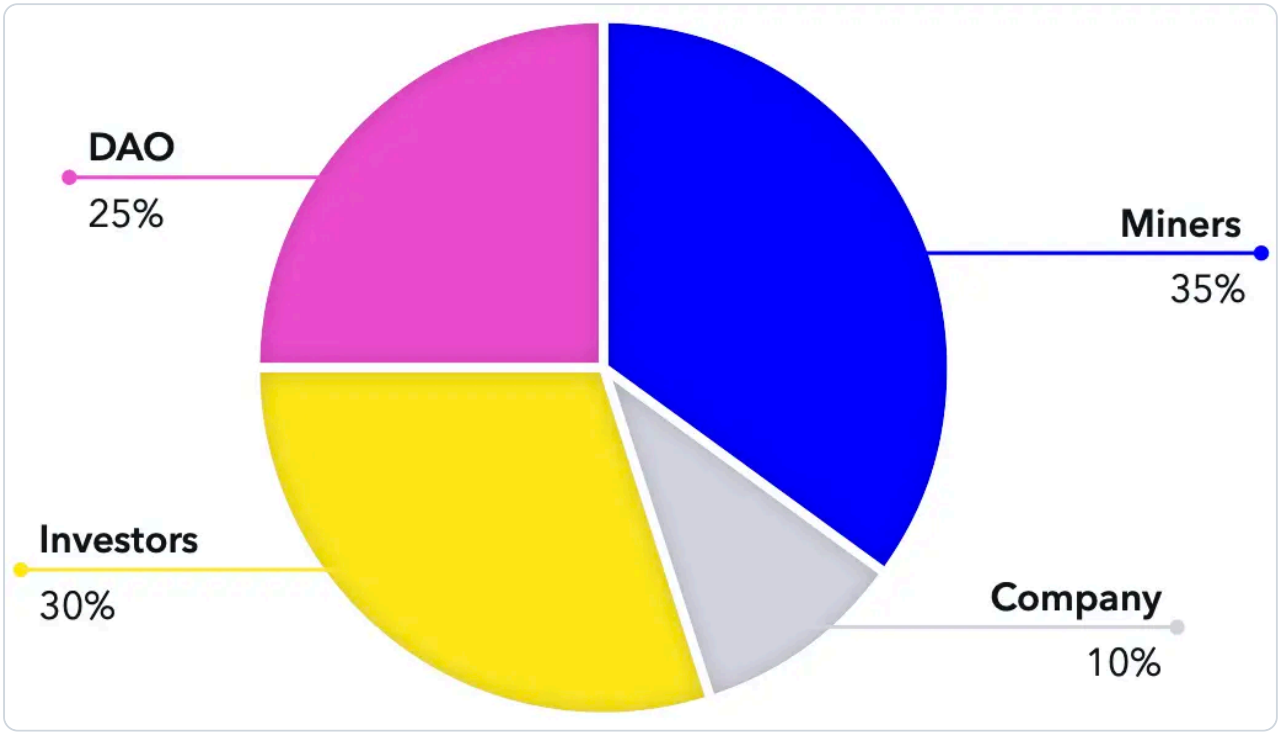
Quantus Network एंजेल निवेशकों की मदद से बनाया गया था जिन्होंने इसे वित्तपोषित करने में बड़ा जोखिम उठाया था। निवेशक-लॉकअप (investor-lockups) द्वारा बनाई गई आपूर्ति ओवरहैंग से बचने के लिए, हम सभी निवेशकों, सार्वजनिक और निजी, को पहले दिन तरल बना रहे हैं। यह आवंटन एकमात्र "प्री-माइन" होगा। अन्य सभी टोकन को अस्तित्व में लाने के लिए माइन किया जाना होगा। सार्वजनिक बिक्री की सफलता के आधार पर यह हिस्सा कुल आपूर्ति का 20-30% प्रतिनिधित्व करेगा।

कंपनी आवंटन

सफलता के वादे के बिना नई तकनीक बनाने का जोखिम उठाने के लिए टीम को क्षतिपूर्ति करने के लिए, हम ब्लॉक पुरस्कारों को दो हिस्सों में विभाजित करेंगे। पहला आधा माइनर को जाएगा। लगभग चार वर्षों के लिए दूसरा आधा कंपनी को जाएगा। यह कंपनी को कुल आपूर्ति का लगभग 10% का वास्तविक निहित (vesting) कार्यक्रम देता है। इस दौरान, खनिकों को नए टकसाल वाले सिक्कों की समान मात्रा मिलती है।

उस बिंदु के बाद, कंपनी के ब्लॉक पुरस्कारों के हिस्से को टोकन धारकों द्वारा शासित खजाने में पुनर्निर्देशित किया जाएगा, जो अनिवार्य रूप से एक DAO बनाएगा।

अनुमानित आपूर्ति आवंटन



लेनदेन शुल्क

मानक लेनदेन में एक शुल्क होगा जो खनिकों को जाता है, जो लेनदेन को शामिल करने के लिए प्रोत्साहन प्रदान करता है। उच्च-सुरक्षा खातों से उलट लेनदेन पर 1% का वॉल्यूम-आधारित शुल्क लिया जाएगा जो विभाजित है, आधा खनिक को जाता है और आधा जला दिया जाता है, जो भविष्य के सुरक्षा बजट में जाता है। zk एकत्रीकरण प्रणाली के माध्यम से जाने वाले लेनदेन पर भी 0.1% का वॉल्यूम-आधारित शुल्क लगेगा, जिसे खनिक, सबूत एग्रीगेटर और एक जलने के बीच विभाजित किया जाएगा।

फोर्कलेस अपग्रेड

Quantus Network सबस्ट्रेट के रनटाइम अपग्रेड के माध्यम से "फोर्कलेस" अपग्रेड का समर्थन करता है, जिससे ब्लॉकचेन के मुख्य तर्क ("रनटाइम") को हार्ड फोर्क्स के बिना विकसित होने की अनुमति मिलती है जो नेटवर्क को बाधित कर सकते हैं या समुदाय को विभाजित कर सकते हैं। यह ऑन-चेन गवर्नेंस जनमत संग्रह के माध्यम से प्राप्त किया जाता है, जहां अनुमोदित प्रस्ताव एक रनटाइम स्वैप को ट्रिगर करते हैं, अनिवार्य रूप से मौजूदा WASM कोड ब्लॉब को एक ही

ब्लॉक में एक नए के साथ बदल देते हैं, जिससे स्थिति और संचालन की निरंतरता सुनिश्चित होती है। यह अपग्रेड पथ डाउनटाइम और जोखिमों को कम करता है, समुदाय को प्रोटोकॉल को पुनरावृत्त रूप से परिष्कृत करने के लिए सशक्त बनाता है।

गवर्नेंस सिस्टम

Quantus Network सबस्ट्रेट के माध्यम से पोलकाडॉट के OpenGov सिस्टम से अपने गवर्नेंस ढांचे को विरासत में मिला है। टोकन धारक दोषसिद्धि मतदान (conviction voting) के माध्यम से भाग लेते हैं, जहां वे अपने वोट के वजन को बढ़ाने के लिए अलग-अलग अवधि के लिए अपनी संपत्ति को लॉक करने के लिए सहमत होते हैं। यह प्रवर्धन 1x (कोई लॉक नहीं) से 6x (अधिकतम लॉकअप) तक हो सकता है। यह डिज़ाइन प्रतिबद्धता के साथ प्रभाव को जोड़कर दीर्घकालिक संरेखण को प्रोत्साहित करता है।

प्रस्तावों को "ओरिजिन्स" (origins) नामक कई वोटिंग ट्रैक में वर्गीकृत किया गया है। प्रत्येक ओरिजिन में अनुमोदन सीमा (जैसे, उच्च-प्रभाव वाले परिवर्तनों के लिए सुपरमेजॉरिटी), स्पैम को रोकने के लिए न्यूनतम जमा, तैयारी/प्रवर्तन अवधि और गतिरोध को रोकने के लिए निर्णय समयसीमा जैसे अनुरूप पैरामीटर हैं। यह मल्टी-ट्रैक डिज़ाइन नियमित ट्रेजरी खर्चों से लेकर महत्वपूर्ण रनटाइम अपग्रेड तक विविध जनमत संग्रहों के समानांतर प्रसंस्करण की अनुमति देता है।

तकनीकी कलेक्टिव तकनीकी विशेषज्ञों का एक क्यूरेटेड समूह है जो तत्काल तकनीकी मामलों को प्रस्तावित करने, समीक्षा करने या श्वेतसूची में डालने के लिए एक विशेष निकाय के रूप में कार्य करता है, सामुदायिक निरीक्षण बनाए रखते हुए उन्हें एक समर्पित ट्रैक के माध्यम से तेज करता है।

Quantus बिना किसी संशोधन के इस प्रणाली को अपनाता है लेकिन अपने शुरुआती चरणों में जटिलता से बचने के लिए एक न्यूनतम सेटअप के साथ शुरू होता है। प्रारंभ में, केवल तकनीकी कलेक्टिव ट्रैक सक्रिय है, जिसका उपयोग प्रोटोकॉल अपग्रेड या पैरामीटर ट्वीक्स जैसे बाध्यकारी, उच्च-विशेषाधिकार निर्णयों के लिए किया जाएगा।

बाद में हम गैर-बाध्यकारी सामुदायिक वोट ट्रैक पेश करेंगे जो गैर-प्रवर्तनीय विषयों पर भावना को मापने के लिए है, जैसे कि फीचर सुझाव या पारिस्थितिकी तंत्र चुनाव। यह प्रणाली तब बाध्यकारी हो जाएगी जब कंपनी नेटवर्क को DAO को सौंप देगी।

यह चरणबद्ध दृष्टिकोण नेटवर्क को भविष्य के गवर्नेंस वोटों के माध्यम से व्यवस्थित रूप से विकसित होने की अनुमति देता है बिना शुरुआत में अनावश्यक जटिलता के उपयोगकर्ताओं पर बोझ डाले।

रोडमैप

Heisenberg Inception

दिसंबर 2024

फंडिंग सुरक्षित, सबस्ट्रेट चुना गया

Resonance Alpha

जुलाई 2025

पब्लिक टेस्टनेट, डिलिथियम सिग्नेचर, प्रतिवर्ती लेनदेन

Schrödinger Beta

अक्टूबर 2025

सुविधाएँ पूर्ण, ऑडिट के लिए तैयार

Dirac Beta

नवंबर 2025

PoW को **Poseidon2** में बदला गया, ऑडिट संबोधित

Planck Beta

जनवरी 2026

उच्च सुरक्षा खाते, मल्टीसिग, हार्डवेयर वॉलेट

Bell Mainnet

Q1 2026

मेननेट लॉन्च

Fermi Upgrade

Q2 2026

ZK एकत्रीकरण

जोखिम

Quantus Network बनाने में अंतर्निहित जोखिम हैं।

- **कार्यान्वयन के मुद्दे:** सॉफ्टवेयर लॉजिक में खामियां सबसे अच्छी तरह से डिजाइन की गई प्रणालियों में भी गंभीर विफलताएं पैदा कर सकती हैं।
- **NIST एल्गोरिदम चयन मुद्दे:** चयनित पोस्ट-क्वांटम मानकों (जैसे, ML-DSA, ML-KEM) में संभावित खामियां या बैकडोर जो मानकीकरण के बाद उभर सकते हैं। सबसे खराब स्थिति में, ऐसी खामियां हमलावर को सार्वजनिक से निजी कुंजी प्राप्त करके signature को जाली बनाने की अनुमति देंगी, जो चेन के विनाशकारी विफलता मोड का प्रतिनिधित्व करती हैं। यदि ऐसी खामियां सार्वजनिक की जाती हैं, तो Quantus Network को एक नए एल्गोरिदम में अपग्रेड किया जा सकता है, लेकिन यदि ऐसी खामियों का कम उपयोग किया जाता है तो उन्हें कभी खोजा नहीं जा सकता है।
- **क्वांटम कंप्यूटिंग समयरेखा:** क्वांटम सफलताएं प्रत्याशित की तुलना में बहुत बाद में आ सकती हैं, जिससे PQC की आवश्यकता में देरी हो सकती है; इसके विपरीत, गुप्त विकास (जैसे सरकारों द्वारा) अचानक खतरों का कारण बन सकता है यदि ब्लॉकचेन समुदाय तेजी से अपडेट करने में विफल रहता है।
- **अन्य विचार:** सामान्य अपनाने की बाधाएं, वित्त/ब्लॉकचेन में नियामक अनिश्चितताएं, और क्रिप्टो पारिस्थितिकी तंत्र की अंतर्निहित अस्थिरता।

समापन

QUANTUS

हम खुले प्रोटोकॉल, प्रूफ-ऑफ-वर्क और संप्रभु स्वामित्व की शक्ति में विश्वास करते हैं। क्वांटस नेटवर्क ऐप, डेस्कटॉप और मोबाइल पर उपलब्ध है, जो उपयोगकर्ताओं को डिजिटल संपत्ति स्टोर करने, नए ब्लॉक माइन करने और मध्यस्थों के बिना एक निष्पक्ष वित्तीय भविष्य में भाग लेने देता है।

हम पारदर्शिता, गोपनीयता और सुरक्षित, स्व-कस्टोडियल टूल के माध्यम से व्यक्तियों को सशक्त बनाने के लिए प्रतिबद्ध हैं।