Abstract

With recent significant improvements to several quantum computing paradigms, the vague danger of quantum attackers breaking traditional encryption methods has become real and pressing.

Quip Network is a quantum computing base layer designed to protect participants from quantum threat vectors on each network where the participant already transacts, and to form decentralized physical infrastructure for quantum computing workloads. The goal of the Quip Network is to offer a seamless, turn-key solution to secure client digital assets against threats from the advent of quantum computers, and to socialize the price of the quantum computing attack that can steal your keys. These initial quantum computing jobs are easily verifiable by network participants with classical computers, and form a seed community to unify the various quantum computing architectures under one virtual machine and language standard. Users of the Quip Network - wallets, protocols, retail, and institutions - can easily integrate the Quip Protocol into their existing chains and wallets to achieve post-quantum security as an extra layer of defense for their digital assets, and to accelerate their hash mining or intent calculations.

The Quip Network emphasizes both post-quantum and classical security, fully portable and native network deployments, procedural transparency with composability, and complete token fungibility across networks. The network relies on Quantum Unit Interlock Pathways (“QUIPs”), which can link together to create arbitrary contracts and value cascades simultaneously and atomically on multiple networks. A quorum of validators provides additional assurances in case of block reorganizations on interlocked chains, batches together complex transactions, and creates incentives for quantum cluster operators to execute jobs alerting the public to vulnerabilities in commonly used cryptographic primitives.

Introduction

Quantum computing threat vectors are imminent. Over the past few years, there has been a steady stream of results published by quantum computing researchers demonstrating significant increases in physical qubit counts, tremendous reductions in error rates, and other substantial improvements to practical computing factors relevant to real-world deployments[1,2,3,4]. These improvements taken as a whole paint a compelling picture that the first quantum computers capable of compromising widely used cryptographic algorithms, like ECC256 or RSA2048, will arrive before the end of the decade.

The incredible coherence values of superconducting qubit architectures like Google’s Willow chip[5], the startling clock speeds of Riken’s fusion-based photonics platform[6], and the scalability of Microsoft’s topological Majorana chip[7] represent significant leaps forward in the capabilities of contemporary quantum processing units. We are rapidly approaching a cost of attack of less than 4% of the value held in the largest Bitcoin wallets. Indeed, the marginal cost of an attack on

RSA2048 for a well-equipped quantum computing lab is estimated to approach $20,000[8,9], and the cost of an attack on ECC256 is likely even lower[10,11].

Unfortunately, broad adoption of post-quantum cryptography has lagged behind the accelerating scale of the threat, and few agents in the world are prepared for quantum attackers. While Bitcoin's pay-to-quantum-resistant-hash proposal has recently seen some small activity, the specification remains undecided with little consensus on the best path forward[12]. Similarly, the discussions on Ethereum offering solutions for EVM networks is likewise lacking in detail and serious agreement, with no further development on any of the EVM L2s or appchains[13]. These approaches remain reactive rather than proactive, leaving room for grievous harm to users who might be caught unaware and unprepared.

Many skeptics point out that P2PKH transactions on Bitcoin remain secure as long as the new public key is not disclosed with a payment transaction, however these users are not protected against block reorganization attacks made possible by quantum computers, and few users maintain sufficient operational discipline to maintain the integrity of their undisclosed public key.

Advocates for delaying adoption of post-quantum commitments claim that other targets are more likely to take priority over cryptocurrency addresses, and such advocates will often proclaim that a swift upgrade will deploy upon discovery of a viable quantum attack[14]. However, we find this argument unconvincing, as quantum attackers can collect many keys at once and hide their activity among legitimate transactions, while many such large targets have immense incentives to keep any compromise a secret. Further, the deployment of a chain upgrade closes its eyes to the possibility of a rewind attack through a chainwide block reorganization which impacts significantly more wallets than a single private key.

Exacerbating matters, traditional financial firms and certificate authorities show similar vulnerabilities to cryptocurrency networks, relying on insecure algorithms that provide guarantees sufficient only for classical computing. The Hudson Institute estimates that over $3.3 trillion in value hangs in the balance as financial contagion threatens to expand damages from the first quantum victim to the rest of the free market[15].

Challenges & Opportunities in Post-quantum Readiness
Any serious attempt to rectify the lackluster adoption of these necessary upgrades must grapple with the challenges that have hindered uptake in previous post-quantum protocols:

Key Considerations	The Solution Must…
Initial costs of a quantum computing attack filter viable targets down to very large wallets, and larger post-quantum signatures create significant negative externalities.	be adoptable in part or in whole by individuals without any requirements for change to the underlying protocols.
Clients do not wish to give up any capabilities of their assets for post-quantum security or	use native primitives on each network and maintain external interfaces of standard user

otherwise split liquidity.	accounts while staying post-quantum secure.
There is a huge risk associated with moving locked funds onto a less secure ledger.	provide the same security guarantees wherever the client chooses to transact.

Introducing QUIP: Four Pairs of Key Properties

For the above reasons, we propose the Quip Network, a new post-quantum communication protocol that represents the golden path that brings every transaction network into a future secure from quantum attackers while universalizing client liquidity so the locked value can be deployed to any approved contract on any network.

In order to ensure the successful adoption of the standard, the Quip Network must exhibit four pairs of properties: post-quantum and classically secure, native and portable, transparent and composable, liquid and bondable.

1. **Post-quantum and Classically Secure**

   While there are many proposed post-quantum algorithms, none have been battle-tested by actual quantum attackers, and some may even remain vulnerable to attacks via classical computing methods.

   For this reason, the Quip architecture should wrap a battle-tested cryptographic primitive such as ECC with a post-quantum primitive such as WOTS+[16], so the end user can benefit from both layers of security. Where possible, the protocol should give the user choice over the post-quantum algorithm that wraps the classical primitive.

2. **Native and Portable**

   Consumers do not want to move funds to yet another transaction network, as splitting the client's liquidity across multiple networks reduces the leverage and capabilities available to that client. Additionally, a client does not want to lose post-quantum security because they migrated their funds from one transaction network to another.

   Wherever possible, the Quip architecture should empower clients to remain on the protocols where they already hold funds while still receiving the benefit of post-quantum security, even when a Turing-complete smart contract language is not available. Furthermore, once the client has locked funds on one chain, they should be able to withdraw equivalent value on another chain at the minimum shared clock cycle.

3. **Transparent and Composable**

   Bridging funds between chains and executing cross-chain intents is a convoluted and error-prone process. Many oracular and bridging protocols rely on decentralized validator networks to monitor the latest state on source and destination networks, where

malicious nodes can be slashed for any perfidy. Such protocols are vulnerable to cartels, require significant resources to support new network deployments, and remain opaque to the end-user in the event of defection.

In contrast, the Quip architecture should prioritize transparency for the direct participants in the transaction, who may reveal all the information required to unwrap a post-quantum signature offline if they so wish. This process should be isolated, asynchronous, and concurrent, and should support the arbitrary composition of functions on dissimilar protocols, such that the outputs of a function on one network can be coerced into the inputs of arbitrary functions on the second network.

4. **Liquid and Bondable**

   Splitting liquidity is an enormous problem for consumers in the cryptocurrency industry, where clients must maintain balances on multiple chains in order to transact. Building on the difficulties of cross-chain intents, there are few resources that can bond funds on one-chain to deploy equivalent capital on another in an atomic and verifiable fashion.

   Ultimately, the Quip architecture should enable a process whereby any funds on any chain can be wrapped in a post-quantum signature and used as collateral or consideration for equivalent value on any other chain.

QUIP: The Quantum Unit Interlock Pathway

The Quantum Unit Interlock Pathway (“QUIP”) is the basic primitive building block of the Quip Network. Each QUIP is a secure lockbox or vault which protects user funds with a post-quantum signature. The algorithms generating the signature have no known vulnerabilities to quantum computing attackers. Beyond its role in safeguarding assets, the QUIP plays a crucial part in maintaining the integrity and functionality of the Quip Protocol.

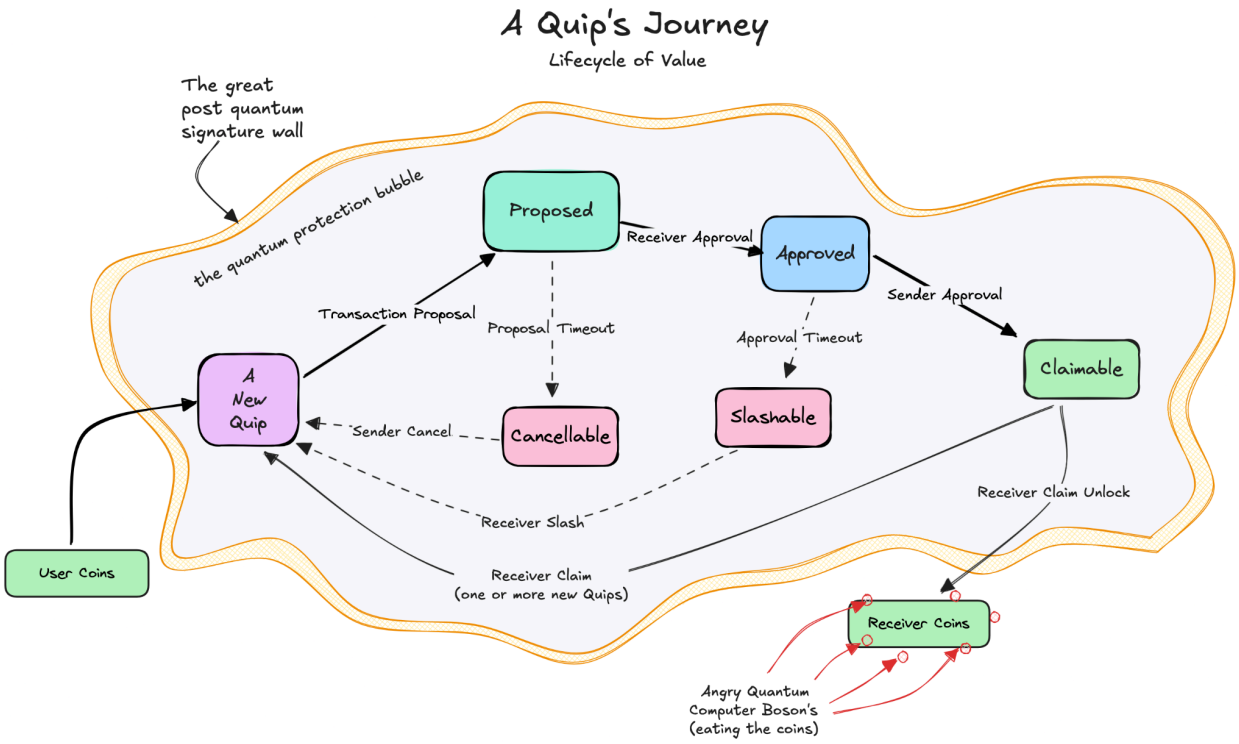
QUIPs start with a user deposit on any blockchain into a QUIP-enabled smart contract. This action creates a QUIP transaction input, which can be used across the entire Quip Network. This deposit pairs the user’s classical wallet with information that can be used to uniquely generate a compatible post-quantum wallet.

In its simplest form, the user can withdraw their funds from a QUIP by signing a transaction with their post-quantum wallet and sending the post-quantum signature to a QUIP-enabled smart contract with their classical wallet. This action could be easily integrated into existing wallets using an extension, such that the post-quantum wallet is hidden within the normal operations of the user’s everyday wallet. The user can also split funds in a QUIP by sending a signed split transaction to the contract, such that some balance is sent to a receiver, and the remaining assets are then shifted to a new QUIP address owned by the sender.

QUIPs provide the ultimate protection for anyone worried about quantum computers. While funds are inside the QUIP they are safe even in the advent of a quantum zero day attack. An

enterprising quantum attacker will be unable to provide the necessary post-quantum signature, which means they cannot provide a valid classical hash to the host transaction network, and thus they cannot create a valid QUIP transaction to remove the funds from the wallet. This guarantee holds true even if they can break the host transaction network's consensus or steal funds from classical unprotected wallets.

The Quip Lifecycle



A user creates a QUIP when they deposit funds to a QUIP-enabled smart contract or QUIP-enabled wallet. At any time, the user can transfer the QUIP to another owner using a regular cryptocurrency transaction. The QUIP also has three additional states that enable programmability:

1. *Propose* - A proposed QUIP signals that a user is ready to conduct a transaction
2. *Approve* - An approval accepts the proposal and enables changes to the network state
3. *Claim* - A claim executes the approved changes to the network state

When multiple parties exchange QUIPs, there are also two timeout cases:

1. *Cancellable proposal timeout* - A user can cancel a proposed QUIP once an initial timer expires with no counterparty matching the proposal. This resets the QUIP state.
2. *Slashable approval timeout* - If a user has approved a matching proposal and a second timer expires without all parties' approval, any approver can slash QUIPs belonging to the delinquent parties.

QUIPs provide post-quantum secure environments to execute arbitrary transactions between as many participants as the proposers wish to include. This programmability is essential to meet the expectations of users of existing protocols, and can be integrated across transaction networks in a bridgeless experience, and executed fully peer-to-peer or via a trustless, managed service.

The Virtuous Quip

The QUIP is an incredibly dynamic and effective building block:

1. Every transaction enforces ACID (Atomicity, Consistency, Isolation, and Durability) principles. They either complete or they do not.
2. The protocol supports staking, swaps, flash loans, mixnets, zero-knowledge proofs, dark pools, voting, delegation, and any other process dreamable with boolean logic.
3. Each deposit requires no custody or lockup on any one transaction network.
4. Transaction resolution is independent and secure without need for any additional consensus mechanism or validator set.
5. Exchange of funds requires no oracles or cross-chain messaging.
6. Post-quantum guarantees are agnostic to the network consensus model and cryptographic architecture.
7. Clients need only rely on the chains to validate transactions: no state comparisons, intermediate networks, or zero knowledge proofs are necessary to perform the needed validations, beyond those required by the host network consensus model.

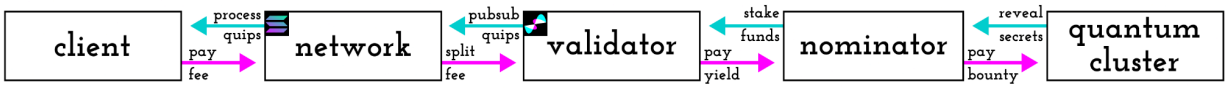
QUIPs represent a paradigm shift in blockchain security and interoperability. By enabling quantum-secure, cross-chain transactions without sacrificing functionality or requiring network-wide upgrades, QUIPs elegantly form a future-proof foundation for digital assets. This revolutionary primitive protects trillions in value from quantum threats while maintaining complete compatibility with existing blockchain infrastructure.

Beyond security, QUIPs unlock unprecedented possibilities for institutional adoption and innovation with the ability to seamlessly move assets across transaction networks while maintaining quantum protection[17]. They enable new forms of cross-chain communication, universal liquidity and shared flow, and heretofore unseen applications. For the first time, institutions can secure their assets against quantum attacks while maintaining full access to the entire digital asset ecosystem.

As quantum computing advances accelerate, QUIPs stand ready to safeguard the future of digital infrastructure everywhere. This elegant solution bridges the gap between quantum security and decentralized computing networks, establishing a new standard for institutional-grade decentralized ledger infrastructure that will shape the next generation of online and financial services.

The Quip Network and Value Chain

While QUIPs can be created and executed on a peer to peer basis, significant additional value will be created given a public index of all the active quips on various networks. As such, we endeavor to form the Quip Network, comprising several parties who collaborate to make the world a safer place to transact:



Payor	Payee	Service
Client	Transaction Network	Store & Process QUIPs
Transaction Network	Quip Network Validators	PubSub QUIP Commitments
Quip Network Validators	Nominators	Endorses via Staked Assets
Nominators	Quantum Clusters	Proves Cost of Attack

Clients

Clients come in many shapes and sizes, from retail to institutional, as lenders, traders, insurers, and end-users of the underlying protocol. To take advantage of a QUIP, they simply pay fees for the necessary computation and storage on the underlying transaction network and the QUIP extension will determine any additional fee retained by the protocol. Wallet providers and treasury management solutions may wish to integrate QUIPs as a secure add-on for their clients, in order to streamline the process of forming and executing more complex QUIP exchanges.

Institutions may wish to employ QUIPs as a second layer of security on their cold storage funds, or else integrate QUIPs directly into low volume hot wallet transactions that touch more sensitive and valuable assets. Even transaction networks with highly sensitive contracts, such as Ethereum's validator staking contract that holds more than 45% of all ETH, may wish to integrate a QUIP directly into the contract or designated withdrawal address so that stakers can rest secure in the knowledge their funds are safe.

Transaction Networks

Transaction networks don't have to explicitly form partnerships with the Quip Network, as any deployer can post a QUIP-enabled smart contract or cryptographic primitive to any sufficiently sophisticated network. However, protocols and traditional payment rails may wish to subscribe to the Quip Network's validators and create a plan for restoring a canonical chain state in the event of a significant reorganization by a quantum attacker.

If the Quip Validators are unable to show that certain accepted post-quantum signatures are still included in the heaviest block or tip of any network, it is a signal that the network may have been compromised by a quantum attacker. Such an eventuality can be planned for, and the miners or validators can adopt a set of criteria for rejecting chain states that do not include recent QUIP commitments.

Validators

In addition to the developers and the foundation, the Quip Network will employ Nominated Proof of Stake Validators to maintain and upgrade services for any transaction network that has not yet implemented post-quantum security, and to provide automation to individual depositors and clients who do not wish to directly manage the Quip Protocol on a peer-to-peer basis. There will be two types of nodes in the Quip Network who will receive the QUIP token for participating in the protocol:

1. *Validator Nodes*
   A full node, these infrastructure providers maintain indices of all proposed quips and process messages and transactions between willing counter-parties in return for QUIP. They can aggregate together multiparty quip transaction signatures and batch the processing for cost savings, provide mixnet or privacy-preserving functionality, and execute other post-quantum multi-party computation services. In return for locking up funds on target networks to facilitate liquidity and collateral, these node providers receive yield in the form of network fees on the indexed networks, as well as QUIP emissions.

2. *Canary Nodes*
   A lite node, these infrastructure providers maintain only a limited subset of the available quips and track the current state of the host transaction network to ensure that the quip has not been orphaned by a block reorganization or other malicious attack on consensus. These records can be used by host networks as a canonical checkpoint in case of a rewind attack by a quantum attacker, and can improve the security of the underlying transaction network. In return for storing and attesting the presence of quips on the host network, these node providers receive fees from the attestations, as well as QUIP emissions. Additionally, these nodes can validate quantum computing workloads for additional QUIP emissions.

For enterprising node providers with insufficient funds to meet the minimum bond required of a trusted validator, they can accept stakes from nominators and share yield from validation.

Nominators

Nominators can supply funds to validators with insufficient capital to meet the minimum stake, and can restake the coupon and yield tokens as collateral for further Quip Network activity.

An added bonus of the validator and nominator staking structure is that node providers can choose the post-quantum algorithms that they trust most to protect their own funds, and nominators can choose the validators using the post-quantum algorithms they trust most.

This stakers' collective choice of post-quantum algorithm will provide an implicit betting market on the safety, storage, and throughput tradeoffs of each paradigm, which can incentivize quantum attackers to prove that any given post-quantum algorithm is flawed. The protocol will provide a built-in emissions mechanism, where a quantum attacker can reveal the private information necessary to earn QUIP token from the protocol by showing the prices at which ECC256 can be broken, and signaling that quantum supremacy has arrived.

Quantum Clusters

Arguably one of the most important participants in the network, these enterprising cryptographers, computer scientists, and datacenter operators can earn automated bug bounties for showing that existing cryptography and protocols are now insecure to contemporary methods. By using vulnerabilities in classical and post-quantum algorithms to reveal private keys, or by accelerating hash mining to execute 26% attacks against Nakamoto Consensus, they can earn QUIP when validators and nominators prove that the attack was valid.

This activity creates a more resilient ecosystem of decentralized services, and will increase demand for the security guarantees provided by the Quip Network and the remaining secure algorithms. The more any one algorithm is preferred by the validators, the larger incentive remains for a quantum cluster provider to claim their pro rata share of the stake.

These jobs are only the first stage as the results are easily verifiable to validators with classical computers, but the network will evolve to provide similar verifiable quantum workloads of all kinds, from hash mining acceleration to intent solving and from AI tensor math to protein folding.

Developers

The core of any good open source protocol, the developers are the lifeblood and innovative soul of all decentralized networks everywhere. The Quip Network will form a foundation and ecosystem development organization to ensure developers have the resources they need to deploy quips on the networks of their choice and to earn QUIP tokens for their efforts.

The foundation will be empowered to increase the adoption of post-quantum secure algorithms, and to deploy an ISO 20022 compliant view of all transaction networks with particular focus on cryptocurrency ecosystems. This will enable developers to create transactions on any chain with any wallet type and supported signature scheme, and to gain access to liquidity and clientele on networks normally incompatible with their preferred ledger or consensus model.

The Quip Network will also develop a unifying standard and virtual machine for various quantum computing architectures, so that developers can write one contract and see results on any available worker with any supported architecture.

Conclusion

The quip primitive and its associated network functions represent a step change in how we think about and prepare for a post-quantum world. It is our sincere hope that the work described here provides an optional upgrade path that eases the transition to post-quantum security for the most vulnerable wallets without further encumbering their associated networks or cash flows. It is of paramount importance that wallets holding significant funds can be defended from quantum attackers, and that the tools exist to ensure that they can continue to transact unmolested on their favorite networks.

Having addressed this core weakness in existing network designs, we envision the Quip Network will become a standard for inter-blockchain and classical payment rail communication protocols, unify the underlying architectures of quantum computing providers, and pave the way for a unified messaging and transaction layer that does not discriminate between endpoints or clients: post-quantum and classically secure, native and portable, transparent and composable, liquid and bondable. The process of getting there won't be quick by any means, but you can certainly bet your money it'll be Quip.

References

1. Bluvstein, D., Evered, S.J., Geim, A.A. et al. Logical quantum processor based on reconfigurable atom arrays. Nature 626, 58–65 (2024). https://doi.org/10.1038/s41586-023-06927-3
2. Putterman, H., Noh, K., Hann, C.T. et al. Hardware-efficient quantum error correction via concatenated bosonic qubits. Nature 638, 927–934 (2025). https://doi.org/10.1038/s41586-025-08642-7
3. King, Andrew D. et al. Beyond-classical computation in quantum simulation. Science 0, eado6285 (2025). https://doi.org/10.1126/science.ado6285
4. Main, D., Drmota, P., Nadlinger, D.P. et al. Distributed quantum computing across an optical network link. Nature 638, 383–388 (2025). https://doi.org/10.1038/s41586-024-08404-x
5. Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. Nature 638, 920–926 (2025). https://doi.org/10.1038/s41586-024-08449-y
6. Kawasaki, A., Ide, R., Brunel, H. et al. Broadband generation and tomography of non-Gaussian states for ultra-fast optical quantum processors. Nat Commun 15, 9075 (2024). https://doi.org/10.1038/s41467-024-53408-w
7. Microsoft Quantum Collaboration. Roadmap to fault tolerant quantum computation using topological qubit arrays. arXiv:2502.12252 [quant-ph] (2025). https://doi.org/10.48550/arXiv.2502.12252
8. Gidney, C., Ekerå, M.: How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. Quantum 5, 433 (2021) https://doi.org/10.22331/q-2021-04-15-433
9. Parker, E., Vermeer, M. J. D. Estimating the Energy Requirements to Operate a Cryptanalytically Relevant Quantum Computer. arXiv:2304.14344v1 (2023). https://doi.org/10.48550/arXiv.2304.14344

10. Hyeonhak, K., Hong, S. New Space-Efficient Quantum Algorithm for Binary Elliptic Curves using the Optimized Division Algorithm. (2023). https://doi.org/10.48550/arXiv.2303.06570
11. Garn, M., Kan, A. Quantum resource estimates for computing binary elliptic curve discrete logarithms. arXiv:2503.02984 [quant-ph] (2025). https://doi.org/10.48550/arXiv.2503.02984
12. cryptoquick et al. BIP-360 Pay to Quantum Resistant Hash. Github (2025). https://github.com/bitcoin/bips/pull/1670
13. p_m et al. Tasklist for Post Quantum Eth. Eth Research. (2025). https://ethresear.ch/t/tasklist-for-post-quantum-eth/21296/5
14. Buterin, V. How to Hard Fork to Save Most Users Funds in a Quantum Emergency. Eth Research. (2024). https://ethresear.ch/t/how-to-hard-fork-to-save-most-users-funds-in-a-quantum-emergency/18901
15. Herman, A., Butler, A. Prosperity at Risk: The Quantum Computer Threat to the US Financial System. Hudson Institute (2023). https://www.hudson.org/technology/prosperity-risk-quantum-computer-threat-us-financial-system
16. Hülsing, A. WOTS+ Shorter Signatures for Hash-Based Signature Schemes. Cryptology ePrint Archive, Paper 2017/965 (2017). https://doi.org/10.1007/978-3-642-38553-7
17. Gugger, J. Bitcoin–Monero Cross-chain Atomic Swap. Cryptology ePrint Archive, Paper 2020/1126 (2020) https://eprint.iacr.org/2020/1126.pdf