PRESS RELEASE

Quantum Resistant Ledger Launches Blockchain Network

New decentralized, open source blockchain network is already resistant to blockchain's most existential threat: quantum computing

British Virgin Islands -- **June 26, 2018** -- The QRL Foundation is proud to announce The Quantum Resistant Ledger (QRL), a distributed ledger resistant to both traditional and quantum computing attacks. For the past year, QRL has been developing their test network and has recently completed a security audit undertaken by cybersecurity company Red4Sec. With their newly launched network, the QRL blockchain will be powered by the quantum (plural quanta), as the base currency unit, with transaction fees paid and calculated through a fraction of the quantum called a Shor. It will retain the established currency code $QRL.

Current cryptographic standards found in blockchain are strong enough to make the compromising of wallet private keys by traditional computers extremely difficult and unlikely, with the same odds as winning the Powerball lottery several times over. Quantum computing will render the current cryptographic standards used in the signature schemes of blockchains largely permeable. Companies like Google and IBM are currently working on projects that could see quantum computing surpass traditional supercomputing in the near future, with Google declaring itself close to quantum supremacy as recently as March.

Additionally, government agencies and watchdogs have been sounding the alarm in regards to current cryptographic standards and quantum computing. In 2016, the NSA released a statement discussing the permeability of elliptic curve cryptography in the face of quantum computing. ECDSA, the most common cryptographic algorithm used to secure blockchain signature schemes, is a type of elliptic curve cryptography.

“At our core, we are a quantum-resistant blockchain; more secure and future-oriented than other blockchains out there today,” said Adam Koltun, Lead Business Strategist for The Quantum Resistant Ledger. “If a person or organization wants to build a secondary-layer application on top of a blockchain, then QRL’s rock-solid security and open source orientation makes us an ideal platform.”

Unlike other blockchains and cryptocurrencies, QRL utilizes a type of hash-based signature scheme known as the Extended Merkle signature scheme, or XMSS. Unlike ECDSA, the cryptography standard favored by today’s most popular blockchain networks, XMSS is resistant to a sufficiently powerful quantum computer running Shor's algorithm.
In addition to providing a post-quantum cryptographic standard and open-source base-layer protocol upon which secondary layer applications may be built, the QRL project will be pursuing smart contract integration and feasibility in the upcoming weeks and months. Additionally, QRL will introduce the Ephemeral Data Messaging Layer which will allow communication using the QRL blockchain in the months following launch.

Looking further forward, the QRL project plans on pursuing Proof-of-Stake as the governance and distribution method for the blockchain. Hopes are to integrate Proof-of-Stake in the first year after launch.

About the Quantum Resistant Ledger

The Quantum Resistant Ledger (QRL) is cryptography with longevity, a post-quantum secure blockchain featuring a stateful signature scheme and unparalleled security. Unlike other blockchains and cryptocurrencies, QRL utilizes a type of hash-based signature scheme known as the Extended Merkle signature scheme, or XMSS. The QRL blockchain hosts its own native cyrptocurrency, $QRL. For more information, please visit https://theqrl.org/.