BlockTower Research Competition

Disclaimer: I, Adam Thiesen, am a small holder of $QRL as a hedge against future quantum computing. I have attempted to make this report as unbiased as possible, and I will not be trading QRL for 30 days prior or after submission of this report.

Additionally: On the day of submission the QRL market cap fell just below $20m to 18.5m after trading above $20m for several weeks. I realize that this was a strict project rule, and understand if disqualification occurs. However, I hope that BlockTower understands the volatile nature of these currencies and will still consider this submission.

Abbreviations:
XMSS: eXtended Merkle Signature Scheme. Merkle tree used to efficiently create many key pairs at generation.
OTS: One-time signature. A theoretically helpful attribute that protects private key cryptography from quantum resistance by avoiding reuse of public and private keys.
NIST: National Institute of Standards and Technology. Helps to lead a verify innovation, including quantum security.
Quanta: The Standard unity of one QRL coin of 105m total.
QRL: Quantum Resistant Ledger, the network and blockchain.
DeFi: Decentralized Finance.

1. Investment Thesis Summary

The defining feature of the Quantum Resistant Ledger is its use of both XMSS and one-time cryptographic signatures in the attempt to provide quantum security. Bitcoin currently uses ECDSA digital key cryptography which is potentially vulnerable to quantum computing[1]; this issue is exacerbated by the re-use of public and private keys. The XMSS and one-time signatures provide quantum security because of the inherent stateful nature of blockchains; this security has been confirmed by the NIST[2].

The Quantum Resistant Ledger has technically strong, audited code[3] along with a secure blockchain setup. In biology there is a phrase stating that "function follows form", and this applies to QRL as well. The blockchain requires many different key pairs and longer signatures, therefore blocks are larger, and transactions are slower as each block can hold only a finite amount of data. Slower, more expensive transactions inherently reduce the velocity of the asset, increase friction, and indirectly motivates users to hold. Combining this low velocity with a scheduled exponential decay mining reward and a hard cap of 105m Quanta means that the

[1] Mavroeidis et al., "The Impact of Quantum Computing on Present Cryptography."
[2] Allen, "Request for Public Comments on Stateful Hash-Based Signatures (HBS)."
[3] Matier, "Red4Sec Security Audit Concludes; a Summary," 4.

supply of QRL is continually constricted. This constricted supply causes price to increase reflexively as demand increases. The function of QRL as an extremely secure store of value and settlement layer follows its form as a "bulky" and slow blockchain.

Storylines and schelling points for digital assets are crucial for both project marketing as well as price discovery. For QRL the schelling point will be as *the* quantum resistant blockchain. This storyline will be compounded because a common trait of early digital currency investors is an affinity for technology and economics. Additionally, these same groups tend to be more open to radical future technology that fundamentally changes current paradigms. Based on their interests, these feverish "early adopters" will begin to think strongly about the prospects of quantum computing. The lindy effect implies that these individuals will then most likely converge on the most time-tested proof of work chain: the Quantum Resistant Ledger.

Currently QRL is only listed on Upbit (the South Korean exchange) and Bittrex International, making purchasing difficult for US investors. I would advise investors not to invest in QRL until *after* the completion of the impending bull market. I believe that deploying capital away from Bitcoin during this run would come with more risks than benefits. Therefore, I am advising a target entrance of 2021 to 2022 (or the beginning of the next bear market), and an exit by 2026 with QRL either trading at 0.01 BTC or $20. The total addressable market of off shore bank accounts is ~$21T[4], therefore I am suggesting that QRL could hold .01% of the offshore bank account market at its peak. This is not including sovereign individuals (or the unbanked) using QRL as a personal bank account.

For large holders of Bitcoin, I am proposing that they would be willing to place 1/100th of their Bitcoin stored wealth into QRL as a hedge against quantum computing. The market cap for QRL at $20 in 2026 would be about $1.5B, which I believe is again conservative as a secure quantum computing hedge for those with a low time preference.

2. People

The official QRL team is located in Zug, Switzerland; this specific location could have positive legal and regulatory implications. Jug has been seen as an ICO safe haven[5], although there is uncertainty regarding just how accepting Switzerland will be of cryptocurrencies. The QRL team consists of 15 members[6], including these contributors: Michael Kolenbrander (technical solution architect and core developer), Adam Koltun (leader of business development), Leon Groot Bruinderink (PhD student in post quantum cryptography, providing information on theoretical quantum computing), Kaushal Kumar Singh (blockchain developer),

[4] "Super Rich Hide $21 Trillion Offshore, Study Says."
[5] Ozelli, "Why Switzerland Is Becoming a 'Crypto Nation' with a Flourishing ICO Market."
[6] *Contribute to TheQRL/Theqrl.Org Development by Creating an Account on GitHub*.

Juan Leni (lead architect and senior consultant), and JP Lomas (full stack developer). The team therefore is filled with a diverse set of talented engineers, designers, and cryptographers.

The QRL blockchain was originally contrived by Peter Waterland, who previously worked as a practicing medical doctor. He became interested in the cryptocurrency space around 2012 and was an early investor and evangelist for Ethereum. Over the years Peter gained an increased passion for quantum computing and its potential threat against blockchains. Around 2016, he decided to create a blockchain whose sole purpose would be to protect against this black swan event.

While the team and founders are important, the true strength of these blockchain projects lies in the open source development. There are currently 29 developers on the QRL GitHub, of which 5 "core" developers make approvals on pull requests. The developers with these permissions include: "cyyber", "surg0r", "jplomas" (a former medical doctor himself and co-partner with Peter Warland), "jleni" and "scottdonaldau". There have been 61 total contributors to the QRL codebase through GitHub, and there have been 3,462 total commits, including the most recently merged commit on May 28 of this year.

Once the code is implemented a blockchain network must prove its security through mining and active nodes. The current hash rate of QRL is only at 59.71 MH/s; for reference Bitcoin currently has a hash rate of 60,000,000 TH/s—about 12 orders of magnitude greater. The 'Hero Miners' pool currently holds 71.45% of the hash rate, followed by miningocean.org at 28.9%; smaller pools including qrlpool.org, fairpool.xyz, qrlmining.info, supportqrl.com, and qrlpool.com make up the small remaining fractions of mining organizations[7]. While most of these mining groups are solely QRL evangelists, about 40% of the miners on the QRL network mine by using the nicehash algorithms. With nicehash anyone can purchase or sell computing power to put towards mining. QRL miners use the *cryptonightv7* mining software which is a standard proof of work mining algorithm meant to be "inefficiently computable on GPU, FBGA, and ASIC architecture"[8]. Equally as important to mining is the number of nodes or peers in the network; recently there have been between 16-20 total active QRL nodes, showing how the early nature of the network[9].

Overseeing the network is the QRL foundation, which is a non-profit that supports and funds research and development for quantum resistant blockchains. However, it seems that this foundation has not been completely developed. There is no clear way to donate to the foundations, and there is no public auditing of the foundation, or explanation about where money has been spent. This may not be malicious, it could simply mean that the team is too focused on building the actual blockchain and network to devote time to a foundation. The true QRL

[7] *Contribute to TheQRL/Theqrl.Org Development by Creating an Account on GitHub*.
[8] "CryptoNight V7 Coins and Mining Pools | WhereToMine."
[9] "QRL Block Explorer."

foundation probably lies within the vibrant and passionate Discord community of which there are 4929 members. The Discord contains interesting channels including quantum computing news, mining, development, as well as general discussions. QRL team members work as moderators in these channels and are helpful in answering any questions.

The official website of the network is extremely informative and contains a 'blockchain explorer', an extensive API for interested developers and information about the XMSS and one-time signature structure. Additionally, the website provides summaries of the external audits that the team has solicited. These code audits were run by the *red4sec* and *x41-Dsec* groups. The red4sec team has a proven history in blockchain audits and has worked with Neo and Nano in addition to QRL[10], while x41-Dsec is a proven security research team that has helped to find vulnerabilities and assist with cryptographic security in prominent companies.

3. Market Information

The QRL project began as an ICO and erc-20 token in April of 2017, raising $4,000,000 in token sales[11]. Subsequently, the main net for QRL launched on June 26, 2018. There has been no lockup schedule as the network is a full-fledged proof of work blockchain. During the genesis block 65m Quanta were minted, with 13m going to the QRL foundation. The total supply of QRL is hard capped at 105m Quanta, or 5x the supply of Bitcoin. At this time there are ~68,399,400 in existence (including cold storage, "lost" coins).

Importantly for stock to flow models and microeconomic principles the emission schedule for QRL will be an exponential decay of the ~38m remaining Quanta over 200 years. The average block time is one minute, and currently coinbase rewards yield about 6.09 Quanta per block.

The current market cap is $18.53m, although this has been fluctuating in both directions with recent market volatility. On Bittrex International, the only exchange that QRL trades on that has been verified by Messari Crypto, there is an average daily volume of $20,000-30,000[12]; currently quite low making it difficult to both accumulate and liquidate positions.

The all-time high for the QRL/BTC pair is .0003318 on 01/16/18. The all-time high in BTC/USD is $3.36 on 01/10/18. The current price in BTC is .00002915, and the current price in USD is $0.34. Therefore, if looking in relative market cycles, now is probably not a terrible time to buy (but again I warn against this).

[10] Matier, "Red4Sec Security Audit Concludes; a Summary."
[11] "The Quantum Resistant Ledger (QRL) - ICO Rating and Details | ICObench."
[12] "Messari - Crypto News, Pricing, and Research."

QRL's main competitor for price and market cap is the IOTA digital currency, which also claims to be quantum resistant due to a one-time signature scheme. IOTA does not use blockchain technology but instead uses a mechanism called Tangle to confirm transactions and prevent double spends. IOTA uses interesting technology, however the network is attempting to integrate micropayments within the "internet of things" and is not aiming to be a store of value or settlement layer. Therefore, while IOTA may be quantum resistant, I do not believe that it is a competitor for QRL's total addressable market cap.

Currently QRL is only listed on Bittrex International and Upbit.com. However, according to the QRL discord and medium posts, "finding a new exchange is a top priority". Until then QRL can only be obtained through mining or over the counter markets for US citizens. This is a critical reason why investors should wait before entering into a QRL trade. QRL will eventually have to be added to a more United States friendly exchange, or investors will have to wait for reliable decentralized exchanges.

The technical analysis for QRL looks promising in terms of QRL/USD as the chart is printing higher lows after the extended 90% drawdown. Additionally, QRL seems to have found strong support at $0.26 and has touched this area three times since a large price increase on May 13/14. However, against Bitcoin, the chart does not look strong at all and is currently in a downtrend. Therefore, I would advise against purchasing Quanta at the current time, especially while Bitcoin is making such strong advances. Even more extreme, I would caution against investing in QRL during this entire bull run. I believe that there are other coins and networks that will pump harder and gain more than QRL in the next year.

While looking at charts and macro data can be useful, one can also gain insights from "on chain" data. QRL wallets generate new key pairs for each transaction, but addresses can continually and securely be reused. Consequently, it is quite straightforward to track the biggest and most influential holders in the network. To give investors the full knowledge of a future investment, I will identify some of these wallets here. Currently, the Bittrex hot wallet holds a sizable (and slightly worrisome?) percentage of all Quanta in existence at about 12.5 million[13]. Another large wallet belongs to the QRL team from the main net genesis block. This wallet currently holds about 6.5m coins; however I believe that the foundation holds more coins in cold storage as some wallets received large amounts of QRL on the day of the genesis block and having been holding since. On that note there seems to be many "cold storage" wallets of QRL that have not been transferred for months at a time. This makes sense as QRL has ledger support, as well as functioning web and mobile wallets, making safe storage fairly user friendly.

Litecoin has experienced recent success despite a lack of development, and the reasons for this are the same reasons that QRL will utilize to attract users and holders. These attributes include proven security over a period of time, as well as a strong schelling point and storyline.

[13] "QRL Block Explorer."

This is why I recommend waiting to invest in QRL. Trust and certainty in the QRL proof of work blockchain will only increase over the years. Additionally, as discussions around quantum computing become more prevalent, more people will help to grow the QRL network and market. QRL daily exchange volume will most likely correlate strongly with time as the average investor becomes exposed to the prospects of quantum computing.

4. Regulatory

As referenced earlier QRL performed an ICO from May 1st 2017 to May 24th 2017, raising $4,000,000. This is a concern as there has recently been regulatory uncertainty surrounding ICOs[14]. However, QRL transitioned to a main net proof of work blockchain in June 2018, and this network is most likely "sufficiently decentralized" to avoid being labelled a security.

Recently, trading QRL on Bittrex has been suspended for American customers, however trading is still available on Bittrex International (available to international customers). The reason for the geofencing has not been stated, and this delisting occurred along with the wave of mass delistings for Bittrex that have transpired over the past few weeks[15].

QRL is definitively a public blockchain, and while this is worrisome for some cypherpunks, it could also help QRL to be viewed more favorably by governments and other regulatory bodies. Private blockchains, or blockchains with privacy guarantees, have recently seen increased regulation internationally[16].

Therefore, given that QRL is most like sufficiently decentralized, with a functioning proof of work blockchain that is public and auditable, I believe that QRL will have safer harbor against regulation relative to ERC-20 tokens and other more centralized digital assets.

According to moderator and full-time team member "@Puck342" disclosed on the QRL Discord the team has not come under any legal issues for their ICO or ERC-20 token distribution.

5. Confirming and Disconfirming Evidence

One case of disconfirming evidence for the QRL thesis would be if NIST decides that XMSS is not truly quantum secure. In this case investors should immediately begin searching for another blockchain hoping to achieve quantum resistance and security.

[14] "Kik Interactive Inc."
[15] "Bittrex Set to Block US Residents from 32 Crypto Assets - The Block."
[16] Seth, "Japan's FSA Bans Private Cryptocurrencies."

However, if quantum experimentation keeps progressing at a steady rate and if NIST continues to verify XMSS, then this would strongly support my QRL thesis. In this case greater numbers of technologists would start to think about Quantum computing at scale and start looking for "secure" Quantum Resistant Blockchains. Word would spread to savvy investors and people looking for safe wealth storage that the Quantum Resistant Ledger is an ideal store of value.

Even if other blockchains begin to implement quantum secure cryptographic systems, I still believe that QRL will benefit from the lindy effect. With blockchains and wealth storage alike trust and security are the most important attributes, and QRL will most likely have both in a few years. Additionally, as more Quantum Resistant blockchains arise more attention will be given to QRL, which may be seen as the standard for quantum resistance.

Another aspect to watch for over the next few years is whether QRL decides to transition to Proof of Stake, or a hybrid proof of work and proof of stake system. With complete quantum resistance in mind the team initially hoped to build a true proof of stake blockchain but realized the difficult engineering needed. If the team decides to transition completely to proof of stake at some point in the future, perhaps once another network has proven its security, then this would certainly alter the investment thesis for QRL. The tradeoffs would be that the Lindy effects and trust would be decreased, while quantum resistance and "holding" or friction would increase. This is not a doomsday scenario, but is something to keep in mind.

In the case that QRL continues as a proof of work blockchain, investors would be wise to monitor the network hash rate. The QRL hash rate should be much stronger to truly prevent a 51% attack, especially if serious wealth is stored using this blockchain. A strong increase in hash rate would certainly trigger a buy signal for those interested in quantum security.

Ultimately, investors should keep a keen eye to the quantum computing space in general, and realize that QRL may be setting the initial standard for a quantum secure blockchain.

6. Downside Scenarios

There are a few downside scenarios for investors to be aware of over the next couple of years before entering into this trade. To begin, there is always a risk when holding alt coins over long periods of time as developers might abandon the project or the coins may simply fade into obscurity.

Additionally, quantum resistance at a scale to "break" ECDSA private and public key cryptography may never come to fruition; or at least may not occur over the next ten years. IT is often said that "there is no difference between being early and being wrong", and this could ring

true for QRL as well. However, according to Neven's law which states that quantum computing will advance exponentially, this is becoming less and less likely[17].

Even if quantum computing is sufficiently powerful, NIST could adjust their analysis and declare that XMSS is not truly quantum secure. Even worse, if the XMSS tree is broken not just theoretically but also in practice or on the live network, then this would be catastrophic for QRL. The probability of these scenarios happening, especially before Bitcoin is potentially proven to be quantum insecure is sufficiently low. However, if either case does come to fruition then QRL would lose much, if not all, of its value and an exit position should be agreed upon immediately.

With its low hash rate the QRL network is certainly susceptible to 51% attacks as well. If this were to happen over the next few years the perception of trust and security associated with QRL would be greatly compromised. If an extended 51% attack were to occur then this thesis would be deemed invalid, and positions should be exited.

Lastly, Bitcoin could fork to a more quantum secure key system sometime in the future. This would require users to transfer all wallet funds to new quantum secure wallets and addresses. While there may be some lost funds, and price may take a hit for a period of time, Bitcoin would probably survive even the worst dark swan quantum event. In this case, QRL would lose value against Bitcoin, but may still hold value as a quantum hedge.

[17] "A New 'Law' Suggests Quantum Supremacy Could Happen This Year - Scientific American."

References

"A New 'Law' Suggests Quantum Supremacy Could Happen This Year - Scientific American." Accessed June 30, 2019. https://www.scientificamerican.com/article/a-new-law-suggests-quantum-supremacy-could-happen-this-year/.

Allen, Thelma A. "Request for Public Comments on Stateful Hash-Based Signatures (HBS)." Text. NIST, February 4, 2019. https://www.nist.gov/news-events/news/2019/02/request-public-comments-stateful-hash-based-signatures-hbs.

"Bittrex Set to Block US Residents from 32 Crypto Assets - The Block." Accessed June 29, 2019. https://www.theblockcrypto.com/tiny/bittrex-set-to-block-us-residents-from-32-crypto-assets/.

Contribute to TheQRL/Theqrl.Org Development by Creating an Account on GitHub. HTML. 2018. Reprint, The Quantum Resistant Ledger, 2019. https://github.com/theQRL/theqrl.org.

"CryptoNight V7 Coins and Mining Pools | WhereToMine." WhereToMine.io. Accessed June 29, 2019. https://wheretomine.io/algorithms/cryptonight-v7-coins.html.

"Kik Interactive Inc.," n.d., 49.

Matier, Jack. "Red4Sec Security Audit Concludes; a Summary." *The Quantum Resistant Ledger* (blog), June 24, 2018. https://medium.com/the-quantum-resistant-ledger/red4sec-security-audit-concludes-a-summary-563ecfe04c75.

Mavroeidis, Vasileios, Kamer Vishi, Mateusz D. Zych, and Audun Jøsang. "The Impact of Quantum Computing on Present Cryptography." *International Journal of Advanced Computer Science and Applications* 9, no. 3 (2018). https://doi.org/10.14569/IJACSA.2018.090354.

"Messari - Crypto News, Pricing, and Research." Accessed June 29, 2019. https://messari.io/.

"Mining Pools List." Accessed June 29, 2019. https://miningpoolstats.stream/.

Ozelli, Selva. "Why Switzerland Is Becoming a 'Crypto Nation' with a Flourishing ICO Market: Expert Take." Cointelegraph, February 18, 2018. https://cointelegraph.com/news/why-switzerland-is-becoming-a-crypto-nation-with-a-flourishing-ico-market-expert-take.

"QRL Block Explorer." Accessed June 29, 2019. https://explorer.theqrl.org/.

Seth, Shobhit. "Japan's FSA Bans Private Cryptocurrencies." Investopedia. Accessed June 29, 2019. https://www.investopedia.com/news/japans-fsa-bans-private-cryptocurrencies/.

"Super Rich Hide $21 Trillion Offshore, Study Says." Accessed June 30, 2019. https://www.forbes.com/sites/frederickallen/2012/07/23/super-rich-hide-21-trillion-offshore-study-says/#7130a6d06ba6.

"The Quantum Resistant Ledger (QRL) - ICO Rating and Details | ICObench." Accessed June 29, 2019. https://icobench.com/ico/the-quantum-resistant-ledger.

https://icobench.com/ico/the-quantum-resistant-ledger
https://miningpoolstats.stream/quantumrl
https://www.nicehash.com/about
https://medium.com/the-quantum-resistant-ledger/red4sec-security-audit-concludes-a-summary-563ecfe04c75
https://www.x41-dsec.de/

https://red4sec.com/en
https://www.theblockcrypto.com/tiny/bittrex-set-to-block-us-residents-from-32-crypto-assets/
https://explorer.theqrl.org/
https://www.nist.gov/news-events/news/2019/02/request-public-comments-stateful-hash-based-signatures-hbs

MESSARI CRYPTO