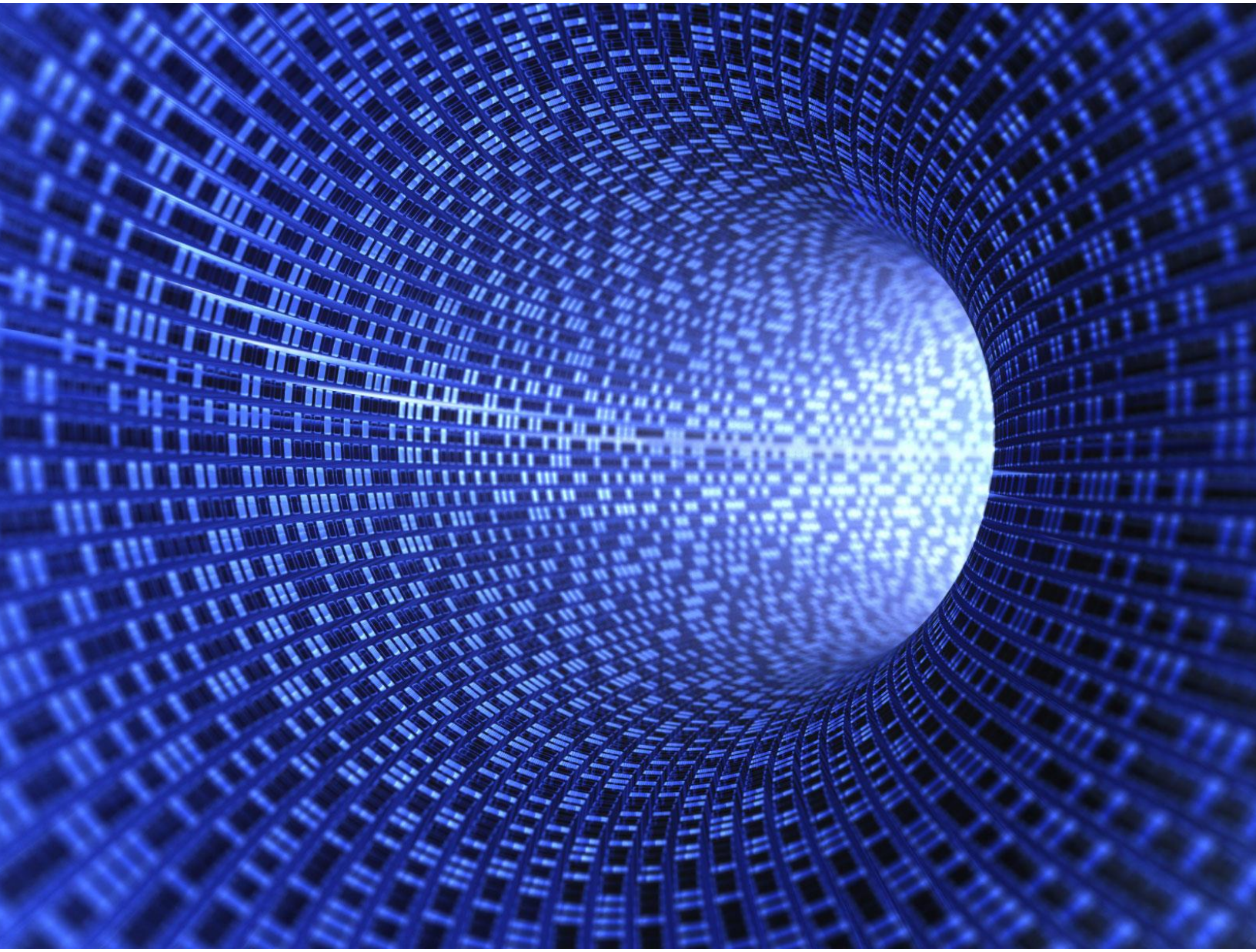
QUANTUM 1NET



# Cryptography for a Post-Quantum World

## Addressing the Security Challenges Ahead

WHITE PAPER

# Introduction

The RSA cryptography platform is now 40 years old. While it has served well in securing the Internet and digital communications, its days are numbered due to the unyielding advance of Moore's law and the emergence of quantum computing. Significant effort and resources are being employed by hackers to crack RSA and other forms of encryption.

The rise of quantum computing makes cracking RSA and various other forms of encryption feasible in the near future. Classical computers use binary bits, which have a value of either zero or one. Strings of these zeroes and ones translate into data, but the nature of the bit means only one calculation can be done at a time. However, with quantum computing, each quantum bit (called a *qubit*) can both be a zero and one at the same time. This difference means quantum computers can store vastly more data, and do many more calculations per second, making them perfect for code breaking applications.

With these quantum computing technologies on the cusp of a breakthrough making the technology ready to crack existing methods of encryption, the time to act is now. Once RSA is cracked, mission critical applications like HTTPS, credit and debit card processing, and government systems face the immediate risk of compromise. The chaos resulting from such a hack would be totally disruptive to the social and economic framework of daily life.

This is why we are developing a quantum generated, key secured data transmission platform called Quantum1Net. Leveraging quantum computing, we are able to provide a level of complexity in cryptographic key generation that is not possible by traditional means. We expect quantum computing to play a key role in the future of encryption.

# ICO

To support our efforts, Quantum1Net is launching two token types: an initial convertible Silver Token in February 2018 without quantum key encryption, and a later limited release quantum key encrypted Gold Token in July 2018. Silver token holders will be able to convert their holdings at a discount. The full deployment of the Gold Token and Quantum1Net is currently slated for January 2019.

More on the specifics of the ICO and the effort are detailed throughout this paper.

# The End of RSA Encryption

For four decades, electronic communications have been secured by a method known as RSA, named for the three researchers that developed the method: Ron Rivest, Adi Shamir, and Leonard Adleman. The process works due to the difficulty in factoring very large numbers. It takes a large amount of computing power both to produce and then factor these numbers, something that Is all but impossible with traditional computing techniques.[1]

The difficulty in doing so was illustrated in a 2009 study. Researchers found that a 768-bit (232 digit) number took hundreds of machines and nearly two years to crack, while a 1024-bit RSA key takes nearly a thousand times as long[2], and that's the lowest bit RSA key type currently used.

This means that it's impractical to even attempt to hack RSA encryption keys simply due to the amount of resources necessary to do so, and the so called "factoring problem" is the reason why a 40-year-old encryption strategy remains popular to this day. Hackers look to work fast, but RSA hacking is a slow and laborious process.

RSA security depends on the limits of traditional computing while technology is rapidly advancing and the emergence of quantum computing urgently necessitates a new encryption strategy. Far less resources and time would be necessary to crack even the strongest RSA keys with quantum computing. Quantum computing empowers the first credible threat to RSA encryption since its inception.

[1] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126.
[2] Kleinjung; et al. (2010-02-18). "Factorization of a 768-bit RSA modulus" (PDF). International Association for Cryptologic Research. Retrieved 2017-11-05.

# Quantum Computing

So, what is quantum computing?

The Traditional computers work by storing data in a string of *bits*, which either hold a value of 0 or 1. Long strings of bits store information, but at any one time that bit can only have one value or another, so only one calculation can be done at one time. Quantum computing works differently. It is based on the unique behavior of subatomic particles to be able to exist in more than one state at a time.

This allows quantum bits, called *qubits*, to store massive amounts of information while at the same time requiring less energy to do so. The result are computers able to run much more complex calculations, and far faster than a traditional computer.[3]

## *Quantum Computing and Code Breaking*

While quantum computers will have a positive effect on the technology industry, their power also presents an immediate security issue. RSA depends on the complexity of factorization of large numbers to keep data encrypted. Due to its architecture, quantum computing becomes an immediate solution to this problem.

Since qubits can have multiple states at the same time, called superposition of states, allowing for many more computations, quantum computers become a logical code breaking mechanism. Work is already underway, and the NIST expects a quantum computer capable of breaking RSA-2048 in a matter of hours by 2030 to be buildable at a cost of approximately one billion dollars.[4]

While that seems a long way off (and expensive), the actual point where RSA might be broken could be much sooner. If someone wants to pay the money, it's likely a computer could be built that could crack RSA in a matter of weeks or months well within the next decade. It is very difficult to say precisely when it will occur – or who might do it yet the ultimate occurrence of large scale quantum computing remains a near certainty

It will be expensive to do, but without our current encryption methods changing the value of the result would be priceless to who ever accomplishes it.

[3] Beall, A. (2017-03-23). "Inside the weird world of quantum computers." Wired UK. Retrieved 2017-11-05.
[4] NIST (2016-04). "Report on Post-Quantum Cryptography" (PDF). National Institute of Standards and Technology. NIST-IR-8105 (draft). Retrieved 2017-11-05.

# The NSA and Quantum Computing

Quantum computing has gained the attention of the top U.S. spy agency. Documents leaked by the former NSA contractor Ed Snowden in 2014, indicated that the agency was funding an $80 million project aiming to build "a cryptologically useful quantum computer."[5] NSA officials hoped that such a machine would enable them to dramatically improve digital spying efforts.

From the documents, it appears as if the NSA was no closer to a workable quantum computer than others, however it was keeping pace with some of the leading quantum computing labs worldwide. How their work is progressing or if they're any closer to success is unknown.

In 2016, it mentioned the risk in a Q&A document intended for those working with sensitive data. "There is growing research in the area of quantum computing, and enough progress is being made that NSA must act now," it wrote.[6] How it was going to act, the NSA was unsure of itself. It admitted no quantum-computer resistant cryptography method existed, so it was only able to recommend algorithms "believed to be safe from attack by a large quantum computer."

The NSA in other words is no less prepared for encryption in the post-quantum area than the rest of the industry. The race is on to figure out a new encryption method. *MIT Technology Review* points out that cracking today's keys would take a quantum computer with hundreds of millions of qubits. We're currently only capable of a quantum computer of about 2,000 qubits[7], so there's time to figure out the problem.

Luckily, a new method is now being developed that will shield us from the eventual failure of RSA-based encryption. That involves Quantum1Net and the new Quantum Encryption Key.

# Quantum1Net's Mission

Innovation is what drives the Quantum1Net team, we are determined to create incredibly powerful technology, make it accessible, relevant, and ultimately personal. Quantum1Net's mission is to create technology that enables and empowers. We have designed a product so secure that you don't need to worry now or in the future about the security of your data. We are introducing an unparalleled level of technical innovation, combined with a system design that connects with the user to provide critical security, ease of use, and peace of mind.

Each year, Quantum1Net plans to reinvest around 20% of its revenue into research and development of new network security solutions to improve transmissions options for people around the world suffering from insecure data transmission. This will make Quantum1Net a significantly research-intensive enterprise.

[5] Rich, S. and B. Gellman. (2014-01-02). "NSA seeks to build quantum computer that could crack most types of encryption." Washington Post (web). Retrieved 2017-11-05.
[6] Simonite, T. (2016-02-03). "NSA Says It 'Must Act Now' Against the Quantum Computing Threat." MIT Technology Review. Retrieved 2017-11-05.
[7] Gibney, E. (2017-01-24). "D-Wave upgrade: How scientists are using the world's most controversial quantum computer." Nature (web). Retreived 2017-11-05.

# Company Overview

Quantum1Net and its incorporated affiliates were created in 2017 to design; manufacture, and market, secure data communication for personal computing, mobile, and satellite transmissions. The Company provides a range of services and related network security solutions for third-party digital content and applications.

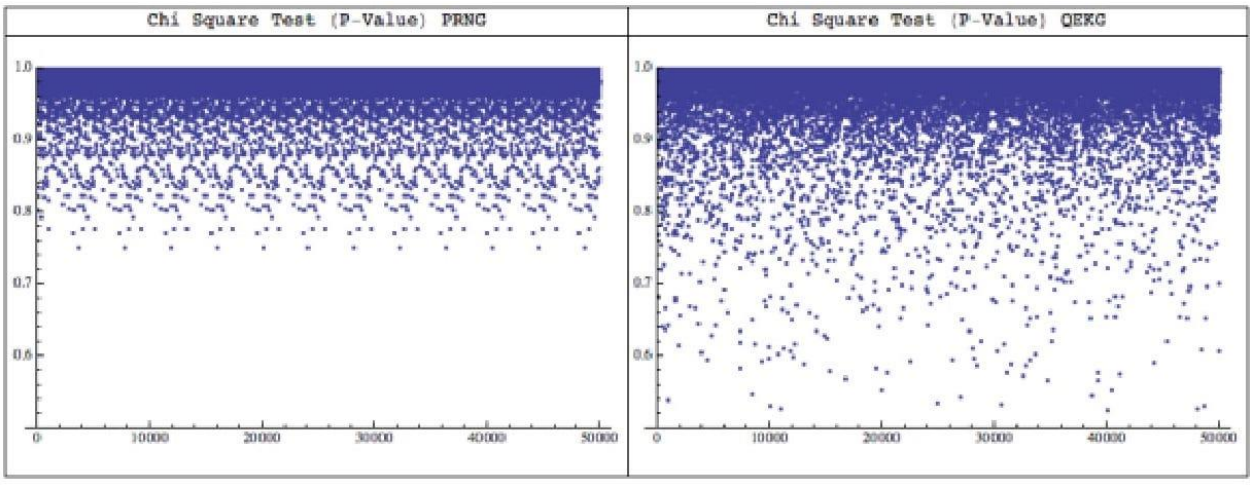
Most of our recent effort has focused on quantum encryption, and work on the *Quantum Encryption Key*, next described.

# The Quantum Encryption Key

The Quantum Encryption Key Generator is the heart of Quantum1Net's encryption strategy. To review, generating a random multi-digit number from which mathematical properties are derived in the case of RSA its prime factorization. There is one main issue however, the random generators used are only pseudo-random (commonly referred to as PRNGs), so an RSA key is pseudo-random. Tests have shown that PRNGs exhibit a repetitive pattern of behavior when selecting so called "random numbers." This pattern means that with enough results, a prediction can be made for future number selections. Thus, PRNGs aren't truly random.

Quantum1Net instead relies on a Quantum Encryption Key Generator (QEKG). Because of the properties of quantum computers itself, tests have shown that even in large samples, the numbers selected follow no pattern thus no predictive algorithm can be derived.

The graph below shows our results for a test of both a PRNG and QEKG on a sample 20,000 bit in length 50,000 times. Using a PRNG, after 50,000 tests it is apparent visually that data is predictive even after the first 10,000 or so attempts. With QEKG however that is not the case. Look at the bottom portion of the graph where the dots are more disperse. Unlike the PRNG graph, in the QEKG graph there is no apparent pattern to their locations.



*Entropy distribution of 50,000 samples 20,000 bits in length generated by PRNG (left) and QEKG lab prototype (right).*

This is possible with a one-qubit quantum optical device; meaning exceptionally large (and expensive) quantum computers are unnecessary to produce quantum encryption keys. We utilize a process known as quantum entanglement in such a way that it produces multiple sets of correlated random numbers so that combining two or more sets can only derive the entire encryption key. While a broader discussion of this process is beyond the scope of this paper, this behavior makes random numbers truly random.

The pattern-like behaviors of PRNGs make *quantum computing* attacks against not only RSA but also other public-key algorithms like Diffie-Hellman and elliptic curve cryptography utilizing Shor's or algorithm or its derivatives effective. Since a QEKG key is produced in a random non-algorithmic manner, systems using these generators will be impervious to such attacks.

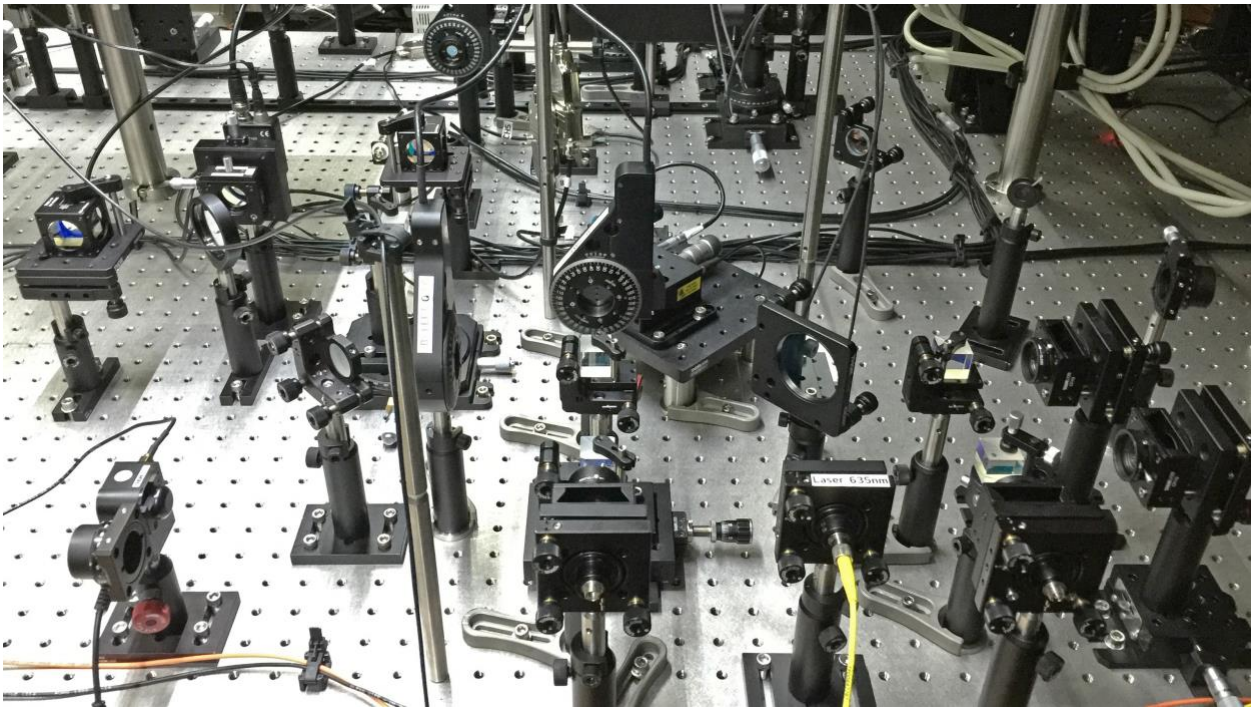
Therefore, the race is on to ensure that a practical real-world system is in place using the QEKG, which is precisely what Quantum1Net is currently working to accomplish.

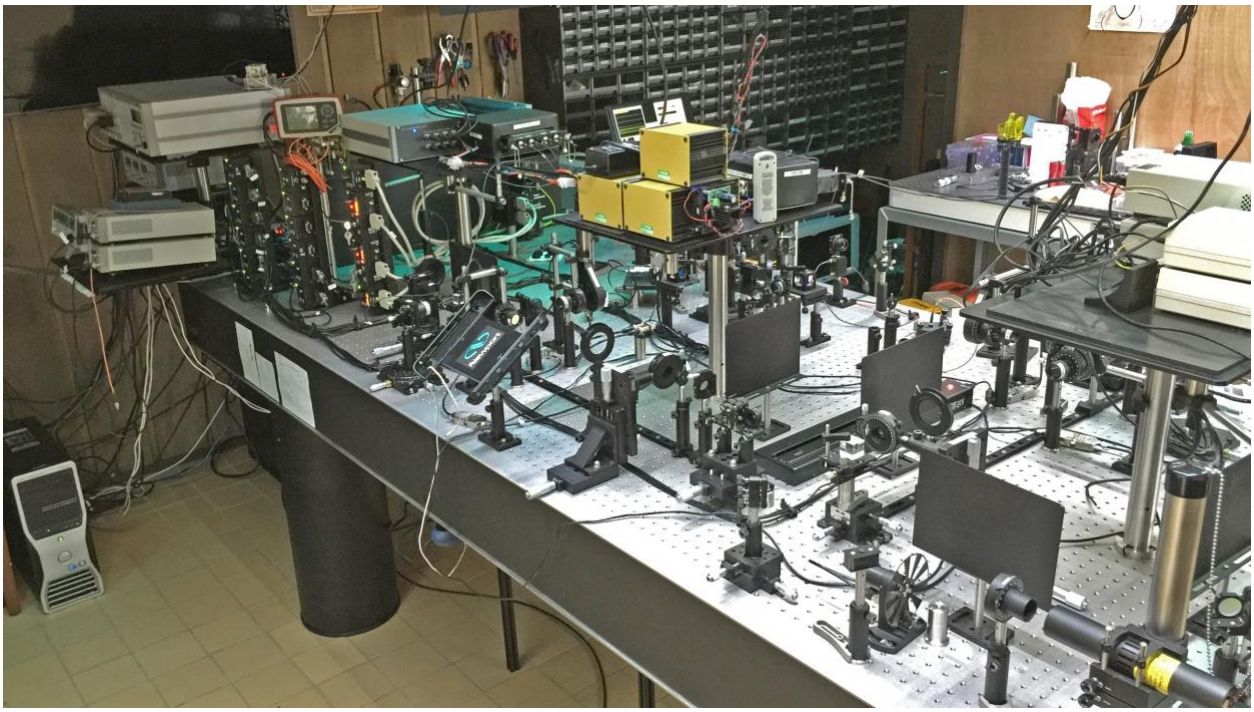
## Quantum1Net Prototype

The laboratory prototype of Quantum1Net's Quantum Random Number Generator, which has been in development since 2014, is based on a one-qbit optical device, that uses four photon detectors and time-to-digital (TDC) converter to generate sets of perfect random numbers with timestamps. The quantum device consists of an entangled photons source, and linear optical elements, which sets the quantum system to the desired state. Two configurations have been developed to generate sets of 4 and 6 elements respectively. The output of the TDC is the temporary queue, from which sets of unique random numbers or encryption keys can be requested, creating a real time, on demand encryption and decryption system.

The transaction data (text or binary) is encrypted using combination of encryption keys and multidimensional Cellular Automata, making quantum-computing algorithms, such as Shor's factorization algorithm for which RSA is vulnerable, ineffective.

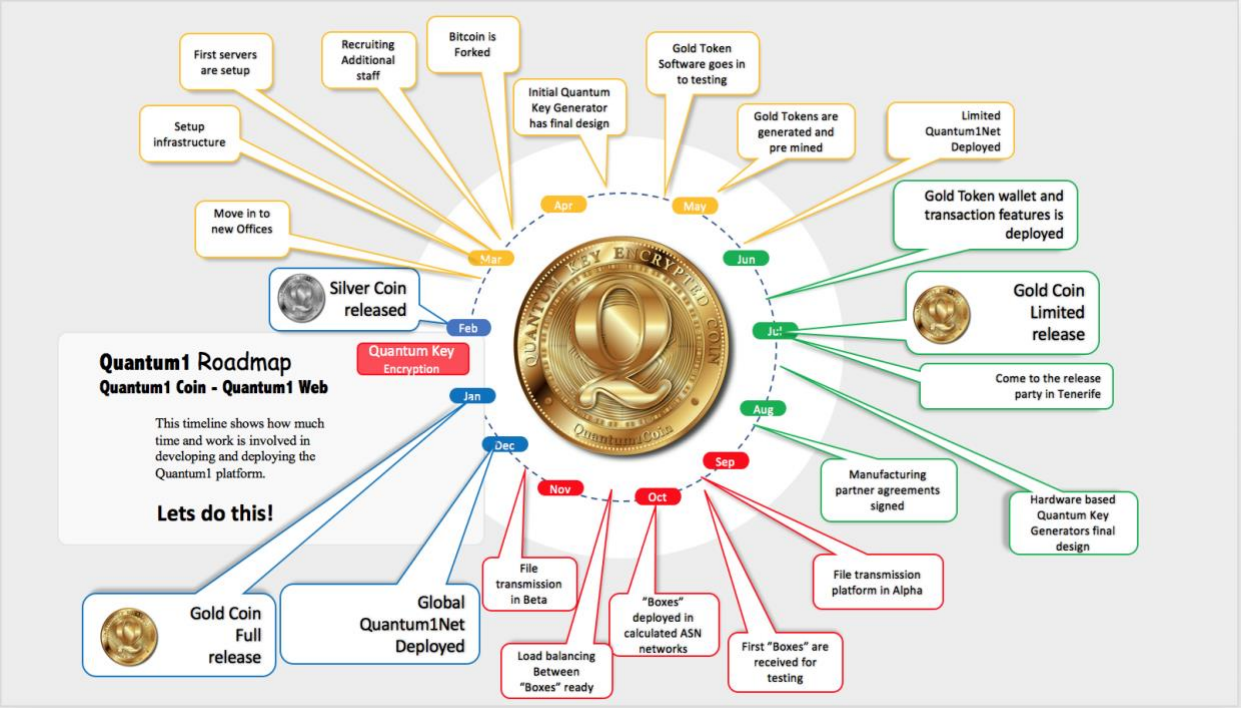
Quantum nature of the Quantum1Net's key generator ensures that the keys are produced can be processed with very little computing overhead.



# Quantum1Net Roadmap

Our plans are to fund our efforts through an initial custom Ethereum token offering, followed by a later Bitcoin token offering. Our second Bitcoin-based offering will use Quantum1Net's QEKG, as it will be released following the limited release of Quantum1Net next year.




## *Development and Release Track*

Quantum1Net expects to continue development through the first part of 2018. The hiring of additional developers in March 2018 should allow us to finalize development of the initial QEKG the following month, supporting a limited Quantum1Net deployment in May. The final design for the hardware-based Quantum Key Generation should be complete in July, followed by the signing of manufacturing partners by the end of Summer 2018.

Fall of 2018 is when we fully expect to start racing towards a global Quantum1Net launch in January of 2019. We expect the 'alpha' version of the Quantum1Net file transmission platform initially during September, and a beta version in November 2018. The release version is likely to be completed the following month, which paves the way for the global Quantum1Net release targeted for Q1 2019.

## *Funding/ICO Track*

Important to our efforts are our planned Ethereum and Bitcoin ICOs starting in early 2018. Our convertible custom Silver Ethereum token is slated for a February 2018 ICO. Funding here will be used to "seed" the project, and allow us to expand our development team to build out

Quantum1Net. This is followed by a limited Gold Token release in July, and a full release in January 2019 alongside Quantum1Net's global debut.

# Quantum1Net Tokens

Our token offerings play a key role in the success of Quantum1Net. As a startup, we'd rather not have our token buyers sit and wait. Thus, the decision has been made to offer convertible tokens just hours after our initial token sales end. As mentioned previously, the early convertible token release funds development efforts, while our second token offering will show proof-of-concept of Quantum1Net, as those tokens will be protected by quantum encryption techniques.

# ICO Timeline

### *First Token Sale: Silver Convertible Token (February 2018)*

Our first token sale is squarely aimed at giving Quantum1Net the necessary funding it needs to meet our January 2019 full release of our platform on time. It supports both our move to new offices to help centralize development as well as hire additional developers to hit our May 2018 goal for a limited release of Quantum1Net.

We will cap the sale at €15 million, and base this initial sale on Ethereum. These tokens will not come with our quantum encryption; however, they will be convertible at a 20% discount during the second token sale in July 2018.

### *Second Token Sale: Gold Token Restricted Sale (July 2018)*

As stated previously, initial investors of our first token sale will have the opportunity to convert their Silver Tokens converted to Gold Tokens during this second sale. We will also give our prior investors the opportunity to convert before the public sale, which will be capped at a value of €18 million. Unlike the first token, the Gold Token will be both based on Bitcoin *and* include the QEK that Quantum1Net is based on.

### *Third Token Sale: Gold Token Open Sale (January 2019)*

Our third sale is scheduled for January 2019, and will occur shortly after the planned global public release of Quantum1Net by the end of 2018. This sale funds Quantum1Net for the long-term as we expand and market Quantum1Net's use outside of crypto currencies to parties who stand to be the most affected by the failure of public-key based encryption.

As a thank you to investors who both held a Silver Token and converted it to a Gold Token during our initial offering in July, a discount of 5% will be offered to those that choose to participate in this offering as well. This funding round is capped at €200 million.

Through these three rounds of funding and the associated caps set, Quantum1Net is confident that our ambitious timeline is indeed achievable. While quantum computing is still in its infancy

and challenges do remain, the past several years has brought about significant progress to the point where developing such a network is now possible.

# Potential Risks

As with any token sale, the purchase of such tokens does carry a high degree of risk, including but not limited to the risks described below. Before choosing to invest, it is recommended that participants carefully weigh all information and risks, and specifically the following risk factors:

### *Technological Risks*

Quantum1Net is based on quantum computing, which in and of itself is a nascent technology. While researchers have made great strides in working towards development of a quantum computer that is useable, significant hurdles remain. While Quantum1Net believes that most of the issues currently plaguing quantum computing will resolve themselves in a matter of years, we cannot say or guarantee a specific timeline.

Additionally, Quantum1Net relies on technology itself to work. We can offer no assurances that issues with technology used may prevent token holders from using their tokens. While Quantum1Net by its nature is extremely secure, we also cannot assure users that use of ICO tokens may not be adversely affected by a third-party attack, whether to Quantum1Net's servers or elsewhere.

### *Regulatory Risks*

Blockchain and crypto currency are new, and largely unregulated. Several jurisdictions have already begun the process of regulating – and in some cases banning – the acquisition of ICO tokens. The investor is responsible for ensuring that their participation in the Quantum1Net ICO complies with applicable local laws. We also reserve the right to modify the sale and/or tokens to ensure compliance on our end with any new regulation. At this time, Quantum1Net believes that its ICO offerings comply with any necessary laws and best practices.

In addition to regulatory issues, ICO token holders also hold sole responsibility for paying any taxes required by their local law whether at the time of purchase or due to any future law.

### *Economic Risks*

As with any investment, success of the ICO and the company at large are subject to economic conditions. Investors' participation in the ICO is seen as an acceptance of that risk. As crypto currency is fairly new, volatility in the Bitcoin (and initially Ethereum) markets will also play a role in the valuation of Quantum1Net tokens.

In addition to these key risks, the Quantum1Net ICO may also be affected by other circumstances outside its control including but not limited to war, states of emergency, acts of nature, and other unforeseen events.

# Our Leadership Team

Quantum1Net is led by a worldwide team with a more than a half-century of combined experience in data science, technology, and data informatics. The team has successfully worked together on multiple startups and deployed global products. Quantum1Net is led by:

- **CEO Mattias Bergstrom**, inventor and tech executive with two decades of experience in the industry. He has developed multiple Internet protocols in the last 20 years and hold more the 60 patent claims in the field of networking.
  He personally invented and founded Voddler, a groundbreaking Video on Demand solution, and System73 a live broadcast system for the Internet. A native of Stockholm, Sweden, Mattias, currently resides in Tenerife, Spain.
- **CTO Stan Miasnikov**, who leads Quantum1Net's encryption work. Stan's experience spans 25 years, including working at Corel, Flex, and OpenTV. Stan's work experience also includes time with Project 1701A, LLC a company that worked to make quantum computing a reality. A native of St. Petersburg, Russia, he currently resides in Palo Alto, California.
- **Mats Jagmalm**, the company's crypto currency and finance expert. Mats' experience as a data scientist makes him uniquely qualified for work in crypto currency, and his understanding of how the crypto-markets work will guide our ICO process and ensure its success for both the company and its investors. Mats, was born in Linkoping, Sweden and currently resides in Stockholm.
- **Thomas Olofsson**, our security expert. Thomas has nearly two decades of experience in security, and most recently worked at Threat Finder, a company working to utilize AI and machine learning to identify threats to organizations. He currently resides in London.
- **Joseph Fernandez**, an astro and computational physicist. Joseph helps Quantum1Net understand the complexities of quantum computing. He is currently pursuing his PhD in astrophysics from Liverpool John Moores University. He currently resides in Wallasey, UK.

And our marketing team:

- **Andreas Tibblin**, whose experience in video will help explain Quantum1Net to our website visitors and interested parties in video form. He is the director of Tibblin Film, a Stockholm-based production house that has credits in TV commercials and shows, as well branded content, video game trailers and music videos. He resides in Stockholm.
- **Michael Johnson** has been a Director/Producer of film, television, as well as an innovator of highly successful media distribution, branding, and convergence projects, globally for over 30 years. He is a New York native and the recipient of three New York Art Directors One Show Awards, and currently resides in Hong Kong.

Stan and Mattias worked together at OpenTV in California in 1998-2000, while Mats and Mattias worked together at Telia Research and at Voddler in 1996 and 2006 respectively, and Joseph and Mattias at System73. Michael also is a veteran of Voddler.

Together, our team has the experience to run a professional startup, the skills to scale globally, and the work ethic to answer the problem of encryption in a post-quantum world.

**Contact information:**

General Information: info@Quantum1Net.com

Press Information: press@Quantum1Net.com