WHITEPAPER

HELPING THE CRYPTO WORLD TO SURVIVE IN THE POST QUANTUM COMPUTER ERA



ABOUT US

Arqit is a decentralised application of open source blockchain technology designed to facilitate a quantum safe business ecosystem.

As we enter the era of Quantum Computing existing encryption algorithms are likely to be compromised. The threat, which may crystallise within a few years, compromises all blockchain and internet systems.

Arqit is designed to serve the needs of customers with complex and large-scale use cases who will need built in protection against quantum attack. It allows businesses to create quantum secure blockchain systems of their own.

The Arqit blockchain is based on open source distributed ledger code called Corda built for enterprise applications by over a hundred institutions collaborating globally. To this, we have added distributed governance, fees and token mechanics to facilitate the creation of distributed autonomous organisations. This allows for, scale, speed and flexibility while incorporating quantum key distribution technology.

Arqit is engaged in a collaborative project with a number of organisations to build a global Satellite QKD ("S-QKD") system whereby quantum keys are transmitted to ground by satellites using quantum photon generators and down-converted into one-time pad keys on the ground. These keys are regarded as provably secure and can be used to encrypt and decrypt data using a variety of algorithms. Quantum keys cannot be transmitted at distances exceeding approx 150km by any method other than satellite. These quantum safe keys are embedded into the Arqit blockchain to protect elements of identity and communications. The S-QKD system element is being built by a highly experienced and credible team of developers, business leaders and investors in collaboration with corporations like BT plc and Qinetiq plc and the World leading scientists of the European Space Agency.

Arqit is also growing partnerships with the blockchain community to sponsor research into the post quantum algorithms for encryption and digital signatures.

By taking a lead in QKD and collaborating widely with the community in post quantum encryption, Arqit will play a role in helping blockchain business systems to become more secure and widely used.

BACKGROUND

Quantum computing is developing at pace, and some, like Google believe it will reach "quantum supremacy" (when quantum computers out-perform conventional supercomputers), very soon. Shor's algorithm and Grover's algorithm will allow Quantum computers to break many forms of existing encryption once Quantum Computers have reached a suitable level of scale whereby enough qubits (the quantum equivalent of a silicon gate) can be controlled. The blockchain revolution could be destroyed before it has properly executed its aims. This leaves us with two questions:

- When will this happen?
- How long do we want our current data and communications to be secure for?

If we say that quantum computers will break, say, ECC or RSA in n years – what is n? Around 1000 qubits are needed to break 160-bit ECC, or 2000 qubits for 1024-bit RSA keys. Since large-scale investment in Quantum projects by Google, Microsoft and many governments has accelerated through 2018, with Google announcing a 72-qubit quantum computer, the consensus suggests that n might be at the lower end as little as 5 years.

Many possible values of n are within the time frame of corporate data retention policies. In any case, data can be captured or stolen today, stored and decrypted later. This leads to the conclusion that we need to do something now about how we secure our data and digital identities.

WHAT IS AT RISK?

Blockchain technologies have two distinctive uses for digital signature cryptography, to validate and authorize transaction records and to validate the blocks in the blockchain. They additionally use conventional network protocols such as TLS to encrypt communications, verify identity of servers and possibly clients too. All these cryptographic algorithms are at risk from Quantum Cryptography.

Current blockchain systems commonly use an elliptic curve (ECDSA) signature to validate and authorize transaction records. Shor's algorithm will compromise this ECDSA signature, allowing fraudulent impersonation. In the case of a crypto-currency, this could lead to funds being fraudulently transferred.

Quantum computers using Grover's algorithm can also attack the cryptographic hash used to verify blocks. However, this is not so serious as the ECDSA challenge; rather than a complete compromise, hashes are effectively reduced to half their length. So, a quantum attack on a 256-bit hash would be comparable to a non-quantum attack on a 128-bit hash, or in other words hashes need to be doubled in length for the same strength.

The TLS (https) network protocol uses similar authentication and digital signatures, as well as algorithms for the negotiation of encryption keys, all of which are vulnerable to quantum attack. The consequence would be that network identities and transactions could be fraudulently forged by quantum computers, as well as transactions being monitored through broken encryption.

TLS commonly uses symmetric AES encryption once keys have been exchanged, and this can be attacked by Grover's algorithm, which may halve the effective key size. So, a quantum attack on AES-256-bit would be comparable to a non-quantum attack on AES-128.

A simple analysis of the threats is below[1]:

CRYPTOGRAPHIC ALGORITHM	TYPE	PURPOSE	IMPACT FROM LARGE-SCALE QUANTUM COMPUTER
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Other elements of network communications like HTTP and DNS are also compromised.

WHAT CAN WE DO ABOUT THIS?

Significant efforts are being deployed around the World in creating quantum resistant algorithms using a variety of techniques (lattice based, multivariate, hash-based, error-correcting code based, supersingular elliptic curve isogeny). Many of these still have practical challenges in deployment, such as the need to transfer large sizes of keys (several megabits). As with any new cryptographic algorithm, there are challenges in creating a secure implementation, and any new algorithm is at risk from mathematical or computational breakthroughs.

An alternative is to use technologies immune from such attacks. Quantum key distribution relies upon Heisenberg's uncertainty principle to transmit a block of secret data, in such a way that the receiver will detect any attempts at interception. After discarding any compromised portions, the sender and receiver will share an identical block of secret data, which they know has not been intercepted.

That secret data could be used as a "one-time pad" to encrypt another message. One-time pad encryption is provably secure and cannot be broken by new mathematical algorithms nor quantum computers. The main difficulty with using one-time pads is the need to securely distribute the keys, which must be at least as long as the messages to be encrypted and must be destroyed after using only once. Quantum key distribution is a good match for distributing one-time pad keys for this purpose.

1 https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

ARQIT DAPP

There are elements of the problem that Arqit will address immediately, elements that are evolving and elements requiring research. In addition to the issues that Arqit solves in key distribution, Arqit will support the development of new quantum resistant algorithms as part of the portfolio of solutions to make the blockchain community and the underlying telecoms infrastructure that it relies upon progressively safer. The elements of the offering are in several parts.

i. The Infrastructure

The Arqit blockchain will be deployed using an open source distributed ledger built by original Bitcoin core developers in collaboration with over 100 institutions, called Corda. It provides a transaction graph of discretely shared states similar to Bitcoin's UTXO model. The system was designed to be representative of real-world, multi-stage, business flows and to model complex processes.

Nodes provide consensus in Arqit. They can be a single node or a pool of 'distrusting' nodes, either fully validating or just checking for double-spends.

The team has added a number of important features to make the system conducive to building decentralized enterprise applications (DApps):

- Governance, so we can fund, build and run further decentralised autonomous organisations ("DAOs").
- Incentivisation, to encourage and reward participation in the sub-business networks those Dapps run on.
- A set of ready-made financial tools and APIs to enable the rapid creation of decentralised applications including tokens and accounts.

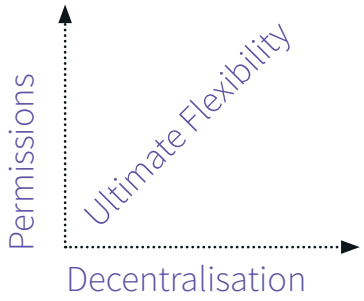
The crucial innovations which are now in TestNet form are DAOs and Metering.

The DAOs are designed to:

- Facilitate funding, building and organising decentralised apps
- Encapsulate
  - Governance (raising issues, voting)
  - Marshalling changes to the system
  - Economics (who pays for what, how proceeds are distributed)
- Can avoid the need for a centralised company

The Metering System is also novel:

- It incentivizes parties to run nodes that can receive payments for transaction authorization – providing a business model for networks and Dapps
- It facilitates PAYGO and customized structures
- It can provide Invoicing and dispute resolution



Chorum Combines:

- The best elements of blockchains for Ultimate Flexibility
- An open source platform with a large global developer bases
- The Scale of Enterprise Class Distributed ledgers
- Quantum Safe Security

Therefore, Arqit provides the important benefits of decentralised information, transactions, authorisations and smart contracts. It applies what we call Appropriate Decentralisation in the form of nodes. Any party can bid to become a node, with varying levels of identity and authority and commensurate incentivisation through fee levels. At the top of the chain are Quantum nodes as described above.

Arqit is expected to be suitable for those applications where marketplaces are disintermediated and large numbers of companies and individuals are brought together to create scaled transaction systems which require a degree of identity and regulatory compliance. Arqit will market its capabilities to communities wishing to establish new DAOs in wide variety of activity areas and will create broad business ecosystem

ii. Quantum Nodes and Quantum Enhanced Identity

Most blockchain systems are now incorporating some form of identity, even if it is just in the form of the KYC and AML required from investors in a Token Generating Event. Many blockchain systems for scaled enterprise use are moving towards the use of Blockchain Nodes – i.e. some form of Node with higher than average authority – in order to optimize a decentralised network's ability to scale. Those Nodes therefore have a requirement for high levels of trust.

Some Arqit Nodes will be equipped with QKD. Initially, these QKD equipped nodes will be able to identify, and securely communicate with, other QKD equipped nodes. Later, it is hoped that QKD keys can be used with new forms of public verification that will replace compromised PKI. These Nodes are therefore highly trusted and Quantum secure.

The QKD elements of these Nodes could also have a role to play in providing infrastructure for other blockchain systems, acting as complementary Nodes for other people's blockchain systems for any variety of purposes. Thus, a truly collaborative and efficient mechanism to extend security at low cost. Projects using Arqit can access Quantum Nodes through delivery of Arqit tokens.

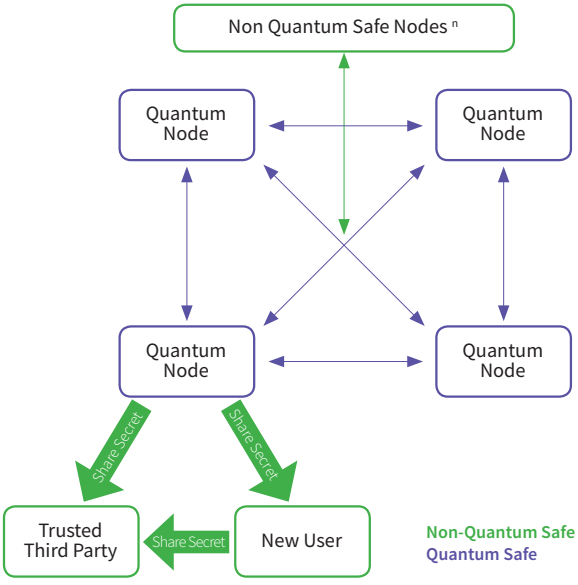
In Diagram 1, a group of Quantum Safe Nodes can be seen communicating directly with one another in pairwise quantum authenticated communications. Each Node is established on the network with a seed key, and grows keys from this seed. Every Node has the identity key of every other Node, and thus pairs of nodes wishing to communicate are able to identify one another, select a one-time pad key to use to communicate directly in a verifiably secure channel. For blockchain applications that do not require later auditability of transactions through passing data to third parties, a hash of these one-time pad keys can also be used to securely sign transactions.

As described more fully below, Arqit allows participants to bid to become Nodes, authorising transactions. Some may choose to be quantum safe, others may not. Those Nodes which are quantum safe can command potentially higher fees on the network and can also be trusted within certain applications with those tasks where provable quantum security is regarded as essential.

In the Post Quantum World, ECC and RSA will be compromised and any system, blockchain or otherwise using X.509 PKI certificates to prove digital identity will be broken by Shor. But also hash based signature schemes may potentially become more vulnerable that at present.

We need a way to generate trusted identity in a post quantum world. There will be many solutions proposed, and Arqit has one of them.

Diagram 1: Quantum Safe Ledger



In the diagram it can be shown that new participants in a project are able to access Nodes which are Quantum Safe, and to be certain of that Quantum Safety through an initial referral from a Trusted Third Party.

That Trusted Third Party will certificate the user as a result of some previous transaction. There will be a wide range of Certificate Authorities in the Blockchain World. It could be the user's Blockchain KYC provider, or a phone company, a financial service provider, or another blockchain provider with trusted transaction heritage and a range of identifiers embedded within the user's device.

ArQit

Rather than trying to maintain a unique identity/identifier, this approach creates a new relationship identifier for each relationship. These identifiers are derived from other existing identifiers using a one-way hash function. That means it is possible to prove that an identifier was used to generate a new derived relationship identifier, but without that original identifier, it's not feasible to trace back from that derived identifier to the original identifier. Due to this property, two relationship identifiers cannot be correlated together, except by using other supporting information, thus helping preserve privacy. This approach is used by the Austrian government's citizen smartcard, to ensure that different government departments cannot correlate identifiers, without the permission of the citizen.

This derivation of new identifiers can be repeated indefinitely, producing a tree of pseudonymous identifiers.

Through the Trust App to be built by Arqit as part of this project, the user contacts the Trusted Third Party and gives to him a secret, a one-time hash generated from the Identifier. The Trusted Third Party passes the Secret onto the Quantum Node. The communication channel between the TTP and the Quantum Node is itself protected by QKD. The Quantum Node now initiates a channel with the new user and passes the secret to him. Cross Checking the Secret, upon confirmation the New User now knows that it is safe to initiate transactions with the node, and in doing so is now gaining the benefit of working with a Quantum Safe node. The Quantum Safe Node and the new users now transact based on the hash of a QKD one-time pad and their shared secret, and grow further keys as needed from this key.

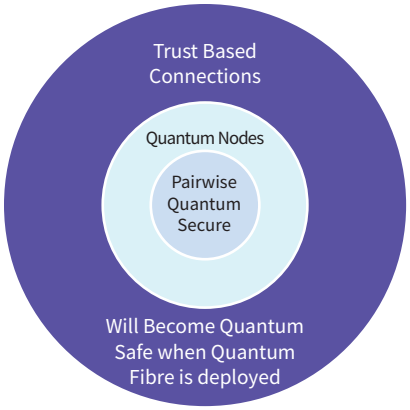
This system solves the problem of, in a post quantum World where RSA/ECC are broken, a user cannot know whether the blockchain node he is connecting to for the first time is real or an imposter.

Arqit will encourage and incentivise a wide range of blockchain systems and supporting technology and service provides to bid to become Quantum Node providers. Partner tokens will be allocated to early partners to enable them to acquire the QKD service and then they will be incentivised by transaction fees from Arqit network and subsequent networks that will use the Quantum Nodes and open source ledger.

Quantum Encryption cannot solve all of the problems posed by the threat posed by Quantum Computers. The two primary evolutions required for full protection are:

1. Deployment of Quantum Metro fibre. Whilst QKD satellite will ALWAYS be needed for long-haul key distribution, in the local loop, quantum capable fibre will eventually become ubiquitous, and this will enable all participants to use QKD to secure blockchain interactions, fed by satellite in the long haul segment. But this involves significant time and investment from telcos
2. The development of Quantum signatures

It is therefore important to acknowledge that in the 3-7 year run up to the arrival of a Universal Quantum Computer, we will generate waves of increasing quantum security within our infrastructures, with each enhancement adding incrementally more security.



In the first iteration there are three layers of security guaranteed. In the inner circle, those applications where both communicating parties have S-QKD can be assured of Provable Security – this stops malicious nodes being part of the inner circle. This should include inter-crypto exchange communications.

In the middle layer, we have a network of Quantum enhanced nodes. Not all nodes in a blockchain system can or will be quantum safe, but the existence of a core infrastructure either provides for a certain essential subset of tasks to be probably secure, or grants a statistical level of security to the network that is higher than otherwise.

In the outer circle are trust based communications using Trusted Third Parties and Shared Secrets to connect users into Quantum Safe Nodes for onboarding. Eventually with the arrival of Quantum Metro Fibre, this cohort will become fully quantum Safe, as will all non-quantum nodes.

iii. Advanced Research Sponsorship

The encryption journey always has two components - the key and the encryption algorithm. Arqit's quantum keys need to work in tandem with post quantum algorithms for encryption and signature.

Whilst Arqit has a definitive solution for the replacement of Public Private Key encryption for those users able to host a receiver, a pathway to deliver this to the mass market via Metro Fibre, and a solution for rendering identity certification more secure, it does need to promote research to create and test a Quantum Digital Signature scheme which can generate quantum secure signatures that work in every blockchain application. Quantum Signature schemes such as those proposed by E.O. Kiktenko et al[2] are suitable for applications where participants can engage in Pairwise QKD protected communications, storing signed transactions bilaterally that do not require onward transmission to unknown third parties. However, this is too limited to be considered useful in many public blockchain systems and so a more comprehensive solution is required. Arqit has been considering new forms of Quantum Signature for Blockchain and will lead a public Research theme accordingly.

2 https://arxiv.org/pdf/1705.09258.pdf Quantum-secured blockchain E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, A.S. Trushechkin, R.R. Yunusov, Y.V. Kurochkin, A.I. Lvovsky and A.K. Fedorov

Arqit proposes to use its funds to sponsor and act as a focal point for this research. Thus, token owning members can propose and receive token funding for research, testing and vote on which algorithms they wish the funding to be applied to. The aim is for algorithms to be developed that are adopted widely by the blockchain industry and therefore the research must generate consensus along the way. Arqit is open to partner with all open source research projects.

iv. Promoting Quantum Security in Telecoms Infrastructure

It is not enough that blockchain systems protect their own infrastructure. It is essential for the blockchain industry that the Tier 1&2 telcos who deliver our messages make their own infrastructure secure. The telcos also have a need generally to protect their own systems and those of their customers. Since the Arqit token community has contributed to the establishment of the technology, telcos using the technology for other applications are also invited to do so. This becomes an important part of token economics, and we hope that as a result of adoption for their own needs, these telcos will host fully functioning quantum safe Arqit blockchain nodes for the benefit of the community.

Arqit distribution model sees telcos contribute to the community in two forms:

1. Telcos secure a right to distribute in a given country through the purchase of five yearly Master Distribution Rights (“MDRs”). Telcos will sell the product to their own customers, as well as making it available to secure blockchain nodes. It is essential that price stability in the distribution channels are delivered and that confusing competition is minimised. This system achieves that aim. Telcos secure these rights by staking a winning number of tokens in an auction. The tokens are held in escrow for the duration of their exclusivity rights.

2. Telcos are incentivised to host quantum safe nodes.

Telcos who wish to be MDRs in a country must buy an MDR for that country. This gives them the exclusive rights to sell to other distributors in that country as well as to sell direct to customers, who will mainly be large enterprise and institutional organisations. Telcos are obligated to sell to qualifying junior distributors on a fair and equal access basis.

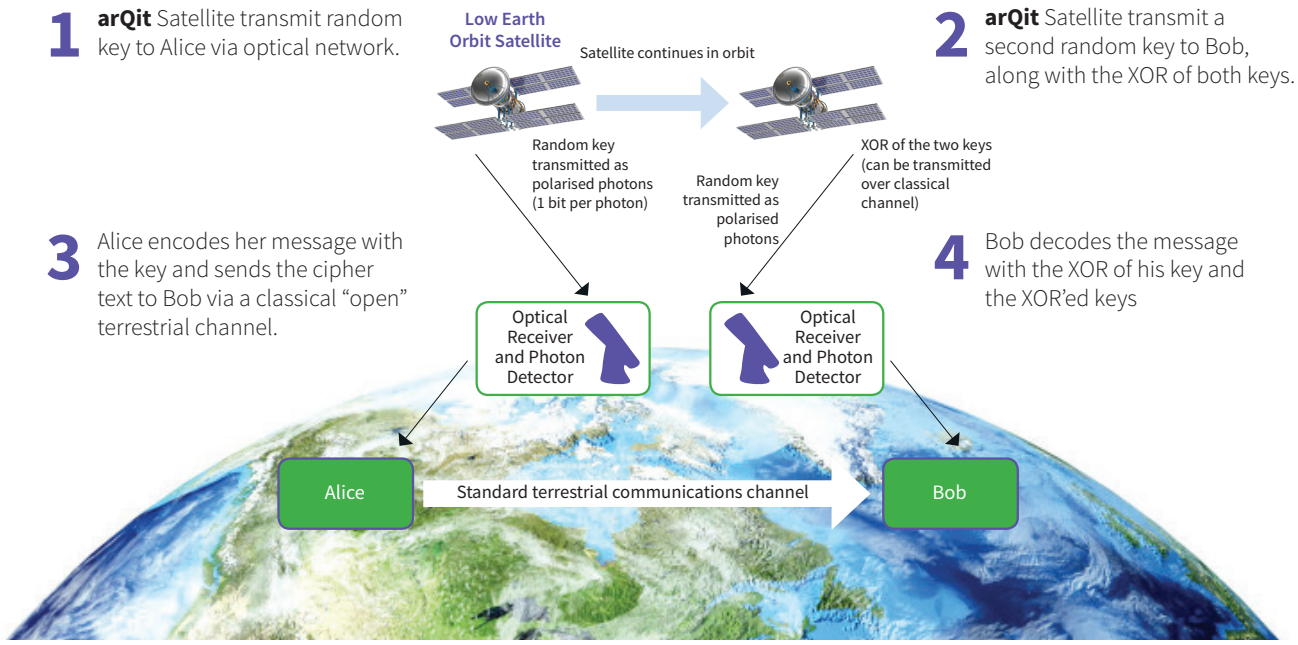
In order to buy a national franchise, a telco must bid a number of tokens in a competitive process. The telco must acquire the tokens the marketplace and deliver them into a secure ecrow account on the Arqit blockchain for the duration of the rights period. At the expiration of a five-year franchise, the bidding process is repeated.

Once a telco owns a national Master Distribution Right it pays Arqit Ltd for units of service in fiat or tokens as it wishes.

BT is a partner in the proposed European Space Agency project team with responsibility for defining and demonstrating the telco use-case within the project. We expect to announce more telcos joining shortly.

QUANTUM KEY DISTRIBUTION – HOW IT WORKS

Quantum Key Distribution uses the quantum properties of photons to encode data, transmitted through a laser to a receiver. Our example counterparties, Alice and Bob receive the same set of photonic data from which they create a common symmetric key through post processing, in effect a one-time pad and use it in an algorithm to encrypt their communications. The key is processed to keep it secret from Arqit. If Eve intercepts the transmission (however improbable it might seem to intercept a laser beam form space) the "No Cloning" rule demonstrates that it is impossible to view then send on the quantum data. QKD at distances over approximately 150Km is only possible by satellite. So, whilst quantum fibre networks will be used on the local loop (there must be no active components or amplification on the fibre), satellite will be used for long distance key sharing.



Thus, quantum key distribution is "Provably Secure". It offers a demonstrable means of ensuring "unconditionally secure" key exchange that, when coupled with quantum resistant cryptographic algorithms, allows two parties to communicate across the Internet with absolute confidence. Since it is not based on mathematical coding, it is not possible to create "trap doors", in fact even Arqit does not know the contents of the keys that Alice and Bob use. As such, the system is entirely free from all forms of interference.

Arqit network will see it first pair of satellites deployed in 2020, which will facilitate a global service. Since the satellites are low Earth Orbiting in a polar orbit they overpass all areas of Earth +-60° several times a day, providing buffering of quantum keys onto a key storage module at the receiver.

Additional satellites will be deployed as the volume of customers' orders increase.

In the development phase, Arqit and BT will also test the direct connection of the satellite QKD receiving ground stations to fibre links to evaluate the potential for low cost key distribution for use by consumers and businesses.

CAPITAL PARTNERS

Arqit is the Not For Profit Company established in Singapore to create the Arqit Blockchain and to turn the management functions over to the resulting DAO, with ongoing support from an administrative office.

Arqit Limited is a sister company created to act as a financing and operations vehicle for the satellite element of the system. That company has arranged a variety of sources of capital. it will provide a portion of its system resources at cost price on an arms-length basis to Arqit.

The initial Arqit Limited system is partly funded by the European Space Agency ("ESA"). ESA is one of the World's leading independently governed supranational scientific research organisations and is responsible for many great leaps forward in scientific understanding for the benefit of humanity. ESA is intending to partly fund the Arqit network deployment with up to €33 million of R&D funding with the first phase of contract agreed.

Arqit Ltd has received Venture Capital Funding from Notion Capital and Seraphim Capital.

PARTNERS

The founding Arqit consortium includes:

Qinetiq Plc - The Prime Contractor for construction of spacecraft.

BT plc - Partner for ground service and customer requirements.

QT Labs - A spin out form Academy of Sciences Austria, led by Dr Rupert Ursin, the global authority in S-QKD.

Fraunhofer Institute for Applied Optics and Precision Engineering IOF - The pre-eminent German not for profit academic research and development institute specialising in quantum optical engineering.

Arqit wishes as many blockchain systems to be quantum safe as possible, so a partner budget is available for other blockchain systems to create their own quantum safe nodes using the Arqit service. A number of partners are expected to announce shortly.

TOKEN ECONOMICS

The Arqit tokens, called ARQ will be delivered to members of the Arqit ecosystem in two ways:

1. As a Fee for operating a node which authorises transactions, including certificating users onto the system. Initially the transactions are those related to the market in ARQ tokens. But as more organisations choose to create DApps on the Arqit blockchain, the use of nodes will rise as will theri demand. The fee paid to a node operator will be entirely set my market supply and demand factors. A Budget is set aside to provide those Node Operators who hold the 20 largest stakes to receive free of charge S-QKD systems. It is expected that Quantum safe nodes will command higher fees.
2. A fee paid to fund research in post quantum algorithms. A budget of 5% of the tokens is established for this purpose. Proposals will be voted upon by the network and fees will be payable on delivery of the research.

ARQ will be paid in to the system by:

1. New DAOs wishing to use the node system
2. Telcos staking ARQs

In both areas pricing will be set by supply and demand.

TOKEN GENERATING EVENT

Arqit will launch a Token Generating Event for donors interested in becoming members of Arqit token ecosystem.

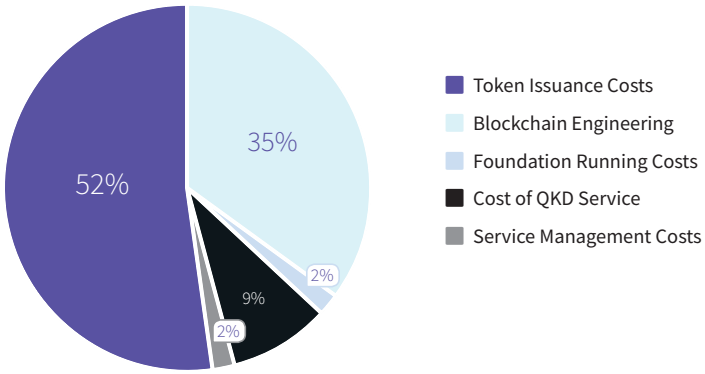
Arqit token has utility in several ways:

- Incentivises users to establish and run quantum nodes
- Incentivises Trusted Third Parties to certificate users onto Quantum Nodes
- Allows other blockchain systems to access to Quantum Nodes
- Incentivises Community to participate in Post Quantum Signature Research
- Used to distribute services to make underlying telecoms infrastructure secure

The proceeds of the TGE will be used to

- The build out and launch the Arqit Blockchain combining the Distributed Ledger and QKD technologies to provided quantum secure identity certification
- Purchase of sufficient QKD service to support the ledger deployment
- The management of the Arqit Research and Partner Programme

Funds are deployed over a three year period to build out the service, thereafter the token economy covers all costs.



45% of the tokens will be issued to investors. 20% will be retained to incentivise employees and advisers. 35% will be retained to incentivise Community participants and research sponsorship.

There will be no further tokens issued.

Arqit Will use Anti Money Laundering software tools to ensure best in class compliance. KYC is built into the model.

TEAM

Richard Crook, Chief Engineer
Leads a team of engineers and innovators looking at emerging technologies and their applications. 20-year career in investment banking technology, specialising in the building of financial ledgers and regulatory reporting for the largest financial service institutions.

Ben Wyeth, Distinguished Engineer
20 years' experience in agile, grid-based pricing and the last 2 years on distributed ledger technologies.

Farzad Pezeshkpour, Distinguished Engineer
Technical lead, systems engineer, of more than 20 years of experience in Finance, Gaming, and Defence, has been working with distributed ledgers for the past 2 years.

Mark Simpson, Distinguished Engineer
20 years' experience as a software engineer in the financial services industry. He has been active in the Ethereum, Hyperledger, Fabric and R3 Corda open source projects including contributing code and speaking at a number of events.

David Bestwick, CTO
Astrophysicist, winner of the Arthur C Clarke Prize, and architect of Arqit QKD system

Dr Lee Boland, R&D Director, Arqit
Space engineer, former Head of R&D Surrey Space.

David Williams
Former CEO of Avanti, a $1bn space start up. UK Growth Company Entrepreneur of the Year 2008.

Jack Blockley, Chief Token Officer
Cyber Security Entrepreneur, Launched Trusteer in Europe and sold to IBM.

Adam Hall, CFO
Experienced technology and media agency CFO.

Andrew Yeomans, CISO
Former Head of Security Engineering, Commerzbank and Lead Application Security Architect, Lloyds Bank.

Tim Grant, Adviser
CEO DrumG, DLT pioneer. Named in Lattice80 Top 100 blockchain influencers
https://www.lattice80.com/lattice80-blockchain-100-report/

Barry Childe, Adviser
Distinguished Engineer, Director Innovation at a HSBC. Leading DLT Development expert, Named in Lattice80 Top 100 blockchain influencers
https://www.lattice80.com/lattice80-blockchain-100-report/

Prof Rupert Ursin, Adviser
Assistant Professor of Quantum Optics, Academy of Sciences Vienna. Globally acknowledged expert in Free Space Quantum Key Distribution.

Dr D Williams, Adviser
Executive Director, CSIRO. Formerly Director of EUMETSAT.

Katherine Courtney, Adviser
Former CEO UK Space Agency.

Nick Miles, Adviser
Leading Public Relations Entrepreneur, Founder of Montfort.

Stephen Chandler, Investor
Managing Partner, Notion Capital.

Mark Boggett, Investor
Managing Partner, Seraphim Space Ventures.

ArQit