Whitepaper

Helping the Crypto World to Survive in the Post Quantum Computer Era

Contents

Disclaimer

IMPORTANT: YOU MUST READ THE FOLLOWING DISCLAIMER AND THE SECTION ENTITLED "IMPORTANT INFORMATION" IN FULL BEFORE CONTINUING

The sale of the Arqit tokens (the "**Token Sale**"), the exchange medium of the Arqit platform to be developed by Arqit Limited, a company incorporated in the United Kingdom of Great Britain and Northern Ireland and/or its affiliate(s) (collectively, the "**Project Group**") as detailed in this Whitepaper is only intended for, made to or directed at, only persons who are not Excluded Persons (as defined herein), and may be acted upon only by such persons. Moreover, this Whitepaper is not, is not intended to be and should not be construed to be, a prospectus or offer document of any sort and is not intended to and should not be construed to constitute an offer of shares or securities of any form, units in a business trust, units in a collective investment scheme or any other form of investment, or a solicitation for any form of investment in any jurisdiction. No regulatory authority has examined or approved of any of the information set out in this Whitepaper. This Whitepaper has not been registered with any regulatory authority in any jurisdiction.

The focus of this Whitepaper is on the Project and the Token Sale. You may have received, be in possession of or perused this Whitepaper together with the following documents:

1.   document entitled "*Helping the Crypto World to Survive in the Post Quantum Computer Era*" published in July 2018, and accessible at www.arqit.io (the "**Litepaper**");
2.   document entitled "*Proposition for Partners*" published in July 2018, and accessible at www.arqit.io (the "**Partner Proposition**");
3.   document entitled "*The Need for Satellites within a Global Network for QKD*" published in July 2018, and accessible at www.arqit.io (the "**QKD Technical Paper**"); and
4.   document entitled "*An Introduction to Cordite*" published in July 2018, and accessible at www.arqit.io (the "**Cordite Technical Paper**"),

which contain additional important (related) information about the Arqit project (or, the "**Project**"), including the Arqit platform, the Arqit tokens and their functions. This Whitepaper, the Litepaper, the Partner Proposition, the QKD Technical Paper, the Cordite Technical Paper, and such other documents as may be published by the Project team in relation to the Project, each as may be amended, modified, or supplemented from time to time (hereinafter collectively referred to as the "**Project Documents**") are intended to be read in conjunction with one another for the purpose of any proposed purchase of Arqit tokens. For the avoidance of doubt, the Project Documents are subject to all disclaimers, restrictions, notices, and legal provisions contained in this Whitepaper.

By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), you represent and warrant to the token vendor of the Token Sale (the "**Token Vendor**") that:

1.   you are not an Excluded Person;
2.   you have read the entirety of this Whitepaper and understand the risks entailed in your purchase of Arqit tokens;
3.   you agree to be bound by the limitations and restrictions described herein; and
4.   you acknowledge that this Whitepaper has been prepared for delivery to you so as to assist you in making a decision as to whether to purchase Arqit tokens.

Without limiting the generality of the foregoing, the offer and sale of the tokens have not been and will not be registered under the US Securities Act of 1933 (the "**Securities Act**") or with any securities regulatory authority of any state or other jurisdiction of the United States of America (the "**US**"). The Arqit tokens are being offered and sold outside the US in accordance with Regulation S under the Securities Act ("**Regulation S**"), and may not be offered and sold or delivered within the US or to, for the account or benefit of, US Persons (as defined in Regulation S).

Background

Arqit is a quantum safe blockchain designed to support a large enterprise ecosystem of users and projects.

Quantum computing is developing at a tremendous pace, and some believe the technology involved 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 number of years – what is n? Around 1,000 qubits are required to break 160-bit ECC, or 2,000 qubits for 1,024-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, and could be as low as five 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, and 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 authorise 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 as well. All these cryptographic algorithms are at risk from quantum computers.

Current blockchain systems commonly use an elliptic curve (ECDSA) signature to validate and authorise transaction records. Shor's algorithm will compromise this ECDSA signature, allowing

4

fraudulent impersonation. In the context of cryptocurrency, 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 as serious as the ECDSA challenge; rather than a complete compromise, hashes are effectively reduced to half their length. In other words, 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 likely 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 could be attacked by Grover's algorithm, which may halve the effective key size. Therefore, 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:

CRYPTOGRAPHIC ALGORITHM	TYPE	PURPOSE	IMPACT FROM LARGE-SCALE QUANTUM COMPUTER
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	Hash	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 (such as lattice based, multivariate, hash-based, error-correcting code based, super-singular elliptic curve isogeny). Many of these still face practical challenges in deployment, such as the need to transfer large sizes of keys (which could be up to several megabits). As with any new cryptographic algorithm, there are challenges in creating secure implementation, and any new algorithm is at risk from mathematical or computational breakthroughs.

An alternative is to use technologies immune from such attacks. QKD relies upon Heisenberg's uncertainty principle to transmit a block of secret data, in such a way that

5

ArQit

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. Onetime pad encryption is provably secure and cannot be broken by new mathematical algorithms or 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 a single use. QKD is a good match for distributing one-time pad keys for this purpose.

The Arqit blockchain

There are elements of the problem that the Arqit project will address immediately, elements that are evolving and other elements that require research. In addition to the issues that the Arqit project solves in key distribution, the Arqit project will support research into 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 Arqit project are in several parts.

i. The Infrastructure

The Arqit blockchain is deployed using an open source distributed ledger code called "Corda", which was built by original Bitcoin core developers in collaboration with over 100 institutions. 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. It was further enhanced by Richard Crook *et al* with features making it suitable for the creation of distributed autonomous organisations ("DAOs"). The current iteration is called Cordite (further information on which may be accessed at: https://docs.cordite. foundation/overview/).

Nodes provide consensus in the Arqit blockchain. They can be a single node or a pool of "distrusting" nodes, either fully validating or just checking for double-spending of tokens. The Cordite platform is being deployed for the first time in the Arqit blockchain, which will serve, along with the quantum safe elements, as a platform for the creation of other business blockchains in future. It has a number of important features to make the system conducive to building decentralised enterprise applications ("DApps"):

- Governance, to enable the funding, establishment, and running of DAOs.

6

- Incentivisation, to encourage and reward participation in the sub-business networks on which the DApps operate.
- A set of ready-made financial tools and APIs to enable the rapid creation of decentralised applications including tokens and accounts.
- DAOs and Metering (as elaborated below).

The Metering system:

- Incentivises parties to run nodes that can receive payments for transaction authorisation – providing a business model for networks and DApps

- Facilitates PAYGO and customized structures

- Can provide invoicing and dispute resolution

Therefore, the Arqit blockchain provides the important benefits of decentralised information, transactions, authorisations and smart contracts. It applies what is commonly referred to as "Appropriate Decentralisation" in the form of nodes. Any party can bid to become a node, with varying levels of identity and authority, corresponding incentivisation through the payment of fees to such nodes.
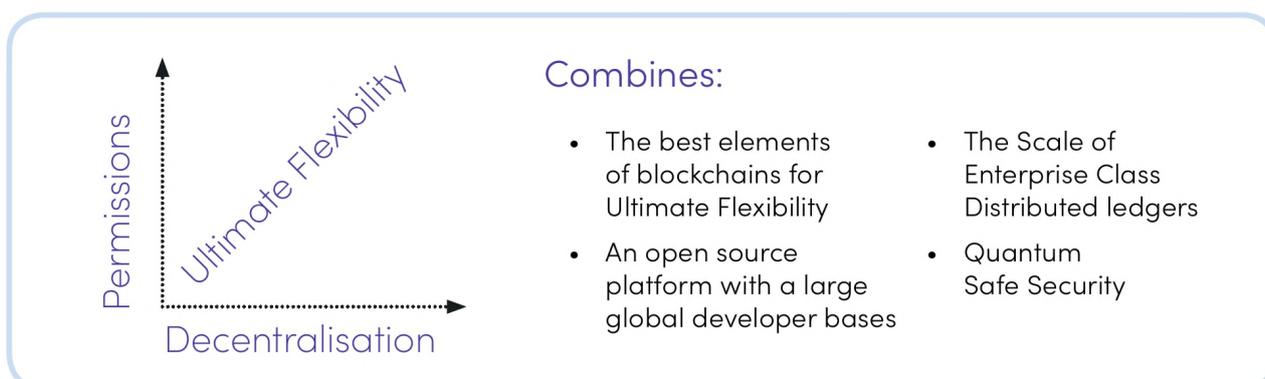
The Arqit blockchain is expected to be suitable for those applications where marketplaces are disintermediated and large numbers of companies and individuals are brought together to create scaled transaction systems which require a degree of identity and regulatory compliance. The Arqit blockchain will market its capabilities to communities wishing to establish new DAOs in a wide variety of activity areas and will create a broad business ecosystem. Eight such projects are working with us to launch their own systems using the Arqit nodes so we expect to see a flourishing ecosystem.

ii. Quantum Nodes and Quantum Enhanced Identity

Most blockchain systems are now incorporating some form of identity verification, typically in the form of know-your-client ("**KYC**") and anti-money laundering ("**AML**") procedures required of token issuers in a token generating event. Many blockchain

systems for scaled enterprise use are moving towards the use of blockchain nodes – which are nodes which have more authority than average nodes – in order to optimise a decentralised network's scalability. 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. Subsequently, it is envisaged that QKD keys can be used with new forms of public verification that will replace compromised PKI. These nodes would therefore be 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 blockchain systems for any variety of purposes. In this way, the nodes would function as a truly collaborative and efficient mechanism to enhance security at low cost.

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 and 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 may also be used to securely sign transactions.

As described more fully below, the Arqit blockchain allows participants to run nodes and authorise transactions. Some may choose to be quantum safe, others may not. Nodes which are quantum safe may command potentially higher fees on the Arqit blockchain 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 likely be compromised and any system, blockchain or operating on X.509 PKI certificates to prove digital identity will be broken by Shor. Hash based signature schemes may also potentially become more vulnerable.

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

Diagram 1: Quantum Enhanced Ledger
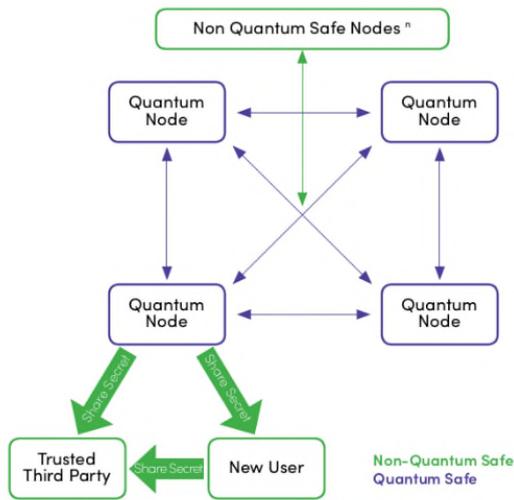
In Diagram 1 it can be shown that new participants in a project are able to access nodes which are quantum safe, which quantum safety is verified through an initial referral from a "Trusted Third Party".

That Trusted Third Party will verify the user as a result of a previous transaction. There will be a wide range of verification authorities in the blockchain world. It could be the user's

blockchain KYC provider, or a phone company, a financial provider with trusted transaction heritage, or even a range of identifiers embedded within the user's device.

Rather than trying to maintain a unique identity/identifier, the above approach creates a new relationship identifier for each relationship. These identifiers are derived from other existing identifiers using a one-way hash function. This means that it is possible to prove that an identifier was used to generate a new derived relationship identifier, but without that original identifier, tracing the original identifier through the derived identifier would not be possible. Due to this characteristic, two relationship identifiers cannot be correlated together, except by using other supporting information, thus achieves the aim of maintaining privacy. This approach is used by the Austrian government's citizen smartcard, to ensure that different government departments would not be able to 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 hash to the quantum safe node. The communication channel between the Trusted Third Party and the quantum node is itself protected by QKD. The quantum node now initiates a channel with the new user and passes the secret hash to him. After cross checking and confirming the secret hash, the new user will then know that it is safe to initiate transactions with the node, and thus benefitting from 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 hash, and grow further keys as needed from this key.

9

ArQit

This system solves the problem for a user in a post quantum world where RSA and ECC are no longer secure enough such that the user is able to identify whether the blockchain node to which he is connecting for the first time is real or not.

The Arqit blockchain is intended to encourage and incentivise a wide range of blockchain systems and supporting technology and service providers to bid to become quantum node providers. Arqit tokens will be allocated to such early technology and service providers to enable them to acquire the QKD service; should they choose to function as a quantum node, they will be able to earn transaction fees from the Arqit blockchain and subsequent networks that utilise the quantum nodes and open source ledger.

Quantum encryption cannot solve all of the problems posed by quantum computers. The two primary evolutions required for full protection are:

1. Deployment of quantum metro fibre. Whilst S-QKD 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.
2. The development of quantum signatures.

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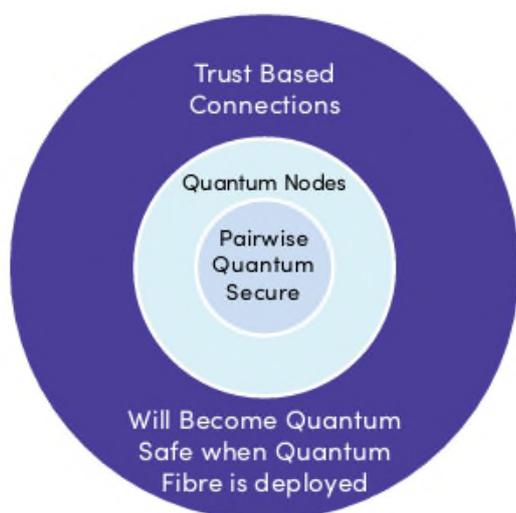
In the middle layer, we have a network of quantum enhanced nodes. Not all nodes in a blockchain system can or will be quantum safe, but the existence of a core infrastructure either provides for a certain essential subset of tasks to be provably secure, or grants a statistical level of security to the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

In the outer circle are trust based communications using Trusted Third Parties and shared secret hashes to connect users to quantum safe nodes for onboarding. With the eventual 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 has two components - the key and the encryption algorithm. The quantum keys of the Arqit blockchain need to work in tandem with post quantum algorithms for encryption and signature.

The Arqit project will promote research into encryption algorithms to partner its key system and 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* are suitable for applications where participants can engage in Pairwise QKD protected communications, and store 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. The Arqit project has been considering new forms of quantum signature for blockchain and will lead a public research theme accordingly. The Arqit project will to use a portion of its reserve tokens to sponsor and act as a focal point for this research. In this regard, holders of Arqit tokens may propose and receive funding in the form of Arqit tokens for research and testing, as well as vote on the research projects to which funding ought to be applied. The aim is for research projects to be developed such that they are adopted widely by the blockchain industry. Therefore, the research must generate consensus amongst Arqit token holders. The Arqit project is open to partnering with all open source research projects.

iv. Promoting Quantum Security in the Telecommunications Infrastructure

It is not enough that blockchain systems protect their own infrastructure. It is essential for the blockchain community that the Tier 1&2 telephone companies ("**telcos**") who deliver our messages ensure the security of their telecommunications infrastructure. The telcos

11

ArQit

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 QKD system, telcos using the technology ought to repay the contributions of the Arqit token holders. This is an important part of the Arqit token economics. As a result of adoption of the QKD system for their own needs, we expect these telcos will also host fully functioning quantum safe Arqit blockchain nodes for the benefit of the community.

Telcos contribute to the community and Arqit token holders in two ways:

1. Telcos secure a right to distribute the underlying Arqit QKD technology 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. Telcos which hold the MDRs for a jurisdiction will be granted the exclusive rights to distribute and sell the QKD product to other distributors in the relevant jurisdiction as well as to sell directly to customers, who will mainly be large enterprise and institutional organisations. Telcos will obligated in the MDR Agreement to sell to qualifying junior distributors on a fair and equal access basis. It is essential that there is price stability in the distribution channels, and that confusing competition is minimised. This system achieves that aim. Telcos secure the MDRs by staking the highest number of tokens in an auction. A minimum bidding price in Arqit tokens will be set for the MDRs of each jurisdiction. The Arqit tokens staked to win the MDRs will be held in escrow for the duration of the grant of exclusive MDRs. An MDR holder will be then able to make payment to Arqit Limited for units of QKD service in fiat or tokens as it wishes.
2. To incentivise and encourage telcos to be early adopters of the Arqit blockchain and to host quantum safe nodes, reserve Arqit tokens may be awarded to such early participants.

BT plc 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

QKD uses the quantum properties of photons to encode data, which is 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, which is in effect a one-time pad, and use it in an algorithm to encrypt their communications. The key is kept secret from Arqit Limited. If Eve intercepts the transmission (however improbable it might seem to intercept a laser beam form space) the "No Cloning" rule demonstrates that it would be impossible to view and thereafter send on the quantum data. QKD at distances over approximately 150 kilometres 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), satellites will be used for long distance key sharing.
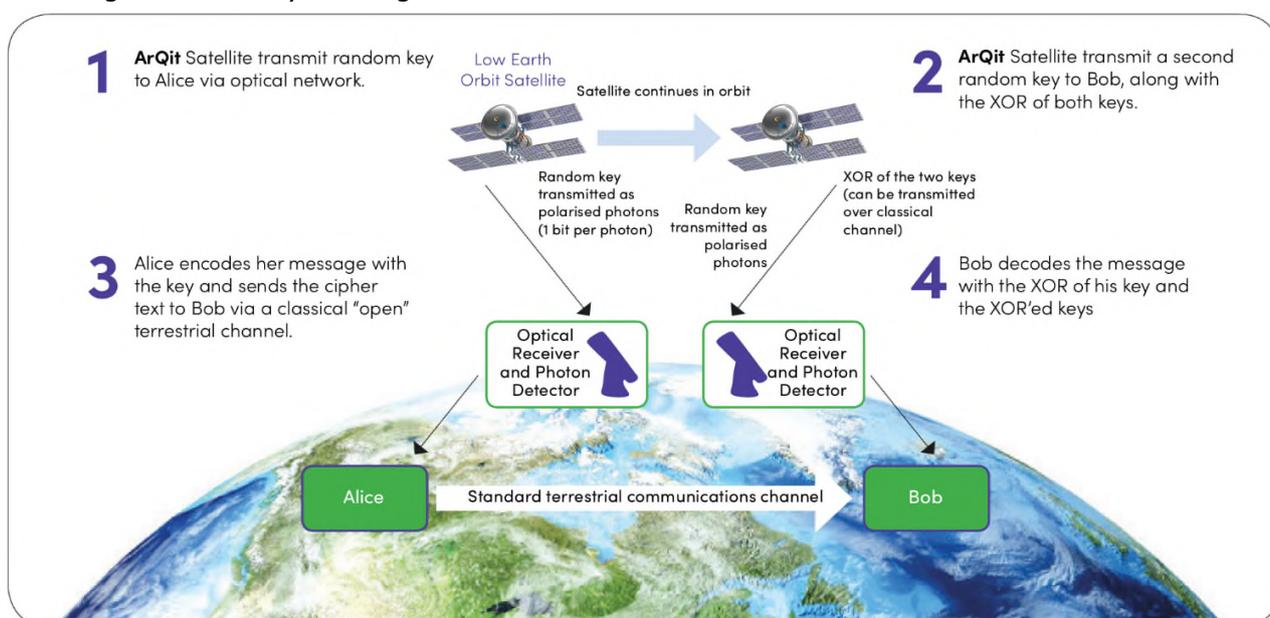
Thus, QKD is "provably secure". It offers a demonstrable means of ensuring "unconditionally secure" key exchange that, when coupled with quantum resistant cryptographic algorithms, allows two parties to communicate across the Internet with provable security. Since QKD is not based on mathematical coding, it is not possible for a state or corporate actor to create "trap doors"; in fact, even Arqit Limited would not know the contents of the keys that Alice and Bob use. As such, the system is free from all forms of interference.

Arqit Limited intends to deploy its first pair of satellites in 2020, which will facilitate a global service. Since the satellites are in a polar low Earth 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 may be deployed as the volume of customers' orders increase.

In the development phase, Arqit Limited and BT plc 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

A company to be incorporated in Singapore with the proposed name of "Arqit Pte. Ltd." ("**Arqit Singapore**") is the not-for-profit company established in Singapore to develop the Arqit Blockchain and to turn the management functions over to the resulting DAO, with ongoing support from an administrative office. The registered name of Arqit Singapore may be subject to change.

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 Singapore.

The initial Arqit system is to be partly funded by the European Space Agency. The European Space Agency 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. The European Space Agency is intending to partly fund the Arqit network deployment with significant research and development funding with the first phase of contract agreed.

Arqit Limited has received venture capital funding from Notion Capital and Seraphim Capital.

Partners

The Arqit Limited consortium includes:

QinetiQ Space – The Prime Contractor for construction of spacecraft

BT plc – partner for ground service and customer requirements.

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.

European Space Agency   A funding and technical partner to the Arqit project

ArQit

A number of further partners are expected to announce shortly.

Tokens

A token generating event will be launched for participants interested in becoming participants of the Arqit token ecosystem through use of the Arqit token.

A public sale of Arqit tokens will be announced on the Arqit website upon completion of the private sale.

Arqit tokens perform the following functions:

- Incentivises users to buy, establish and run nodes and quantum nodes
- Incentivises Trusted Third Parties to verify users onto quantum nodes
- Allows other blockchain systems to access to quantum nodes
- Incentivises community to participate in post quantum research
- Used to distribute services to make underlying telecoms infrastructure secure

Opportunity for Node Operators

Node Operators earn fees in tokens in two ways

1. For authorising transactions
2. For providing high quality infrastructure

It is important to the Arqit business ecosystem and the projects that will follow that a strong cohort of nodes is established early and that these nodes are operated to a high standard. Therefore, 15% of the Arqit tokens are reserved for payment to the first cohort of 2,200 Nodes to be established for the proprietary system established by Arqit called "Proof of Performance".

The Proof of Performance fees apply to all node operators. Node operators acquire the right to operate nodes immediately by staking ARQ tokens as below and will operate as soon as the Main net is launched. There are two types of nodes, base and quantum Nodes. Node operators which have staked Arqit tokens to qualify to be a quantum node will be able to operate as a base node, until the QKD system is installed at the relevant node.

AQTs	Base Node	Quantum node
Staking Fee	1,100,000	11,000,000
Node Cap for PoP Rewards	2,000	200
PoP Fee per month	22,917	229,167

The reserve tokens are applied to reward nodes over a four year period. Once the reserve tokens for Proof of Performance have been exhausted, fees awarded will be determined entirely by supply and demand based on the work that is performed by the relevant node, and not based on the number of Arqit tokens staked. Subject to demand, Arqit may consider releasing further reserve Arqit tokens to reward nodes beyond the aforementioned initial 2,200 nodes.

When new projects launch their own blockchain systems using the Arqit node system, they will have good statistics available to them to demonstrate the quality of node operators.

Proceeds and Allocations

The proceeds of the TGE will be used to:

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

33% of the tokens will be issued to investors. 23% will be retained to incentivise employees and advisers. 15% are reserved for Node operator fees. 24% will be retained to incentivise infrastructure partners and 5% for research sponsorship.
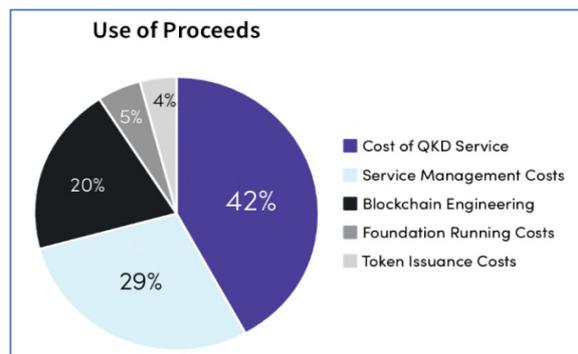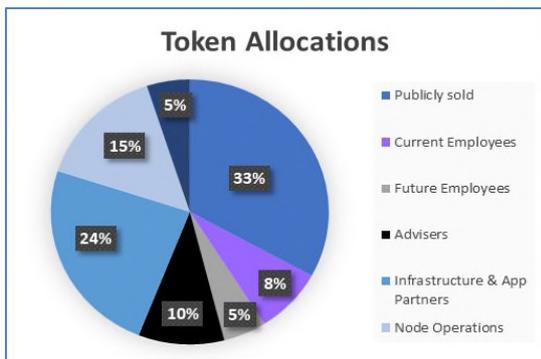
Team

David Bestwick, CEO. Astrophysicist, satellite engineer, and architect of Arqit QKD system. Former CTO of Avanti, a $1bn fleet of high frequency telecommunication satellites. David has designed astrophysics experiments and space implementations for 30 years, at Marconi, Vega then Avanti. He is founder and originator of the Arqit concept and holds several related patents.

Richard Crook, Chief Engineer Led a team of engineers and innovators a RBS 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. Was an early contributor to the architecting of the R3 Corda system and designed and implemented Cordite.

Dr Lee Boland, R&D Director Space engineer, former Head of R&D Surrey Satellites, Europe's pre-eminent small satellite manufacturer.   Over 20 years of experience in the space sector working in both government and industry. Chair of the Engineering Steering Board. Significant experience across numerous small satellite missions covers technical engineering through the entire lifecycle, from space mission concept design to build and in-orbit operations.   In government, for the UK Space Agency, represented the UK in the Horizon 2020 Space Programme Committee as well as roles in the UK Space Technology Advisory Committee, UK Space European Affairs Group, UK Space Propulsion Working Group, Climate Data from Space Stakeholder Group, and European Space Ag Harmonisation Advisory Group.

Prof Rupert Ursin, Chief Quantum Scientist Prof. Dr. Rupert Ursin, Austrian Academy Sciences Vienna is a globally acknowledged expert in Free Space Quantum Key Distribution. Contributed to the experimental implementation of the Chinese Mici satellite project. Holds the World Record for longest distance Quantum Free Spa communication. Dr Ursin Leads a team from Academy of Sciences who will man Quantum science and research elements for the Arqit project.

Dr Thomas Scheidl, Quantum Scientist Thomas is a World leader in working in the fiel space quantum communication under real-world conditions since 13 years and has be for a number of implementation projects. Most recently, he has been the leader of the in the Austrian-Chinese collaboration, successfully accomplishing the first-ever

ArQit

demonstration of space-to-ground quantum key distribution involving the Chinese quantum science satellite "Micius" and an optical ground receiver in Graz (Austria).

Dr Fabian Steinlechner, Quantum Scientist Fabian is an expert in quantum communications and one of the world leaders in the development of ultra-bright and high-quality entangled photon sources tailored to the specific requirements in free-space quantum communication experiments.

Dr Thomas Herbst, Quantum Scientist Thomas Herbst is an expert in quantum communication and free-space optical communication. He took part in the international cooperation between the Chinese Academy of Sciences and the Austrian Academy of Sciences, building the European receiving modules for the Chinese quantum communication satellite.

Dipl. Ing. Matthias Fink, Quantum Scientist Matthias Fink has a profound knowledge about single photon experiments involving free-space links through turbulent atmosphere and is an expert on quantum optics. He was actively involved in international collaboration with China and has significant field experience due to several experiments at the Canary Islands.

Farzad Pezeshkpour, Distinguished Engineer Farzad 'Fuzz' Pezeshkpour has more than 20 years of experience as a computer scientist and systems engineer with hands-on experience with blockchain technologies since 2013. He has been working Corda and a member of the Corda Technical Advisory Council. He is working on Cordite as a core developer for the DGL token ledger, and Braid, a cross-platform RPC library for Corda. Fuzz led the development of a government sponsored project for nation-wide payments of benefits using distributed ledger technology. Fuzz developed distributed animation and games engines before he joined RBS financial markets in 2001, where he was the principle architect and engineer for an award winning FX Options trading and risk management suite (SystemX). Fuzz moved to run a new technology function in Deutsche Bank for core risk services, before returning to RBS to head architecture and engineering in Risk, overseeing the design and engineering of counterparty credit-risk and market-risk systems across front-office and back-office.

Jack Blockley, Chief Revenue Officer Jack is a serial entrepreneur with a successful 19 year leadership record in the Financial Services and Cyber Security sectors. As the founder and CEO of Geneva Partners, he has helped launch a series of successful cyber start-ups into the European marketplace. During the past 15 years, Jack has created over $1bn of shareholder value through acquisition of portfolio companies, including the launch of Trusteer in Europe which was then sold to IBM.

Andrew Yeomans, CISO Andrew has over 20 years' experience of Information Security and the Finance industries, having been Domain Architect for Application Security and Lead Architect at

Lloyds Banking Group, and Head of Security Engineering at Commerzbank London (formerly Dresdner Kleinwort investment bank).

Andrew was on the management board of the Jericho Forum, an international information security thought-leadership group dedicated to defining ways to deliver effective IT security solutions that will match the increasing business demands for secure IT operations in our open, Internet-driven, globally networked world. Andrew is also is a member of the Executive Advisory Board of the ISSA UK chapter.

Prior to this, Andrew led IBM's European technical sales for Internet security. He is co-author of "Java Network Security", the first book to cover secure multi-tier Java applications. He has worked with UNIX and Open Source software since 1985, and managed and ran IBM's Scientific and Technical Computing group's UNIX network.

Adam Hall, CFO Experienced and commercially focused CFO with successful start-up and SME experience. M&A experience includes three successful trade sales and the co-founding of Avanti Communications Plc.

David Williams, Chairman Former CEO and founder of Avant.   David was a banker financing telecoms and media businesses before co-founding Avanti. Raising $1bn, the company deployed a fleet of geostationary satellites which delivered highly resilient communications to government and telecoms customers. Won and successfully deployed the homeland security network in the UK and served dozens of governments and telcos around EMEA. Received the Queens Award for Exports in 2016 and UK Growth Company Entrepreneur of the Year 2008.

Adviser Team

Tim Grant, Adviser CEO DrumG. Tim Heads DrumG which is developing Blockchain applications for the Financial Services industry. He was previously Head of R3 Labs, developing the early R3 product and applications.   Prior to this he was a Managing Director at UBS Bank.   Named in Lattice80 Top 100 blockchain influencers

Barry Childe, Adviser Barry Childe has more than 35 years' experience specialising in the monetisation of innovative digital technology solutions for Banks. Recently this focus has been Blockchain, A founder member of the R3 Blockchain consortium in 2014 and a named creator of the Corda platform and Certified Corda Developer, Barry has lead HSBC's Global Blockchain program since 2014. In that time Barry has delivered a number of world first Blockchain, Cyber and High

19

Performance computing projects including Voltron, VoltronONE on Corda and WE.Trade consortium application with IBM. He also worked on Project Ubin with the Monetary Authority of Singapore and the HKTFP project with the HKMA. In total over a 100 projects and engagements have been completed in the three year period across HSBC.

Since 2014 Barry was been the technical lead for the HSBC Group Applied Innovation & Strategic Investments team, providing technical and commercial support to a range of investments totalling beyond $100m. Barry has held CTO, CTA and Head of IT, Head of HPC positions at a number of Banks, including Nordea Bank, Westpac, TD Securities, RBS, Gemstone, VMWare, Barclays Capital and HSBC during his career. In 2015 Barry was named in the inaugural list of 9 HSBC Distinguished Engineers. In 2017 Barry's team won the Innovation Award for HSBC's Blockchain work at the Banker awards and in 2018 he was named in <u>Lattice 80's Top 'Blockchain Industry leaders to watch' list</u>.

<u>Dr D Williams, Adviser</u> Dr Williams leads the data-focused research, development and digital capability of Australian national science agency CSIRO, and is a member of the Executive Team. He has stewardship of a range of business lines and national facilities including the quantum and blockchain programmes as well as Astronomy and Space Science, the Australia Telescope National Facility, Marine National Facility, Australian Animal Health Laboratory, Australian Collections, Information, Management and Technology and Data 61.

Prior to joining CSIRO in 2014, Dr Williams was Chairman of the European Space Agency (ESA), leading the 20-nation council executive body that oversaw the ESA. During this same period Dr Williams was also Chief Executive of the United Kingdom Space Agency responsible for developing the strategic vision for UK space, securing bilateral arrangements with various countries, and establishing national facilities in Harwell, England.

Dr Williams holds BSc degree and a PhD from the University of Reading, served as a Member of the Global Climate Observing Committee, was elected Member of the International Academy for Astronautics in 2012, and is now a non-executive director of AARNET.

<u>Katherine Courtney, Adviser</u> Katherine was Chief Executive of the UK Space Agency - where she opened the UK market to Satellite launch, spaceflight and spaceport operators (creating new commercial growth opportunities for the UK economy); established UK leadership of the European Space Agency's Telecoms and, Navigation and Earth Observation programmes; and inspired a future generation of scientists and engineers through Major Tim Peake's highly successful Principia Mission to the International Space Station. She also initiated the agency's first Quantum encryption Programme.

Katherine's early career was spent developing new products and services in the global telecoms industry as a senior executive with major multinational corporations and a series of start-up companies.

She moved to the public sector in 2003 to lead the UK Government's National Identity Scheme Programme and then went on to lead a number of other flagship programmes including Universal Credit, Growth Vouchers, Business Growth Service and UK Small Business Commissioner - steering four cross-cutting pieces of legislation through Parliament.

She holds a Masters of Business Administration from London Business School.

Mark Simpson, Distinguished Engineer Mark has over 20 year of experience as a software engineer in financial services industry across retail, corporate and markets business lines. Mark has been working with blockchain platforms since early 2016, initially building a pioneering digital wallet application on Hyperledger fabric. He then contributed to the Emerald, a distributed clearing & settlement on Ethereum. Over the past three years Mark has been focused on building blockchain projects for syndicated lending, letters of credit and invoice financing . Mark is the lead developer on the metering code in the Cordite open source project. Mark has built high performance front office trading systems in C++ and lead the development of the first Equities Algorithmic trading platforms at ABN AMRO. He has architected and developed several front and middle office systems for Equity Derivatives as well as migrating the pricing and risk to a compute grid.

Ben Wyeth, Distinguished Engineer Ben has over 20 years of experience as a tech lead and developer building bespoke software systems. He wrote the initial Ethereum contract in Emerald a distributed clearing & settlement system and his results on tuning Ethereum were published widely in 2016. Ben worked on the FCA's mortgage reporting project - Maison and has contributed code to open source Corda. Most recently he has been the lead developers on the digital mutual in Cordite. Ben worked in consulting for 10 years at Andersen and Thoughtworks and then spent 11 years at RBS initially in grid based pricing of RBS' interest rate derivatives and credit portfolios, where he was tech lead on a team with a 40k node grid doing 250k compute hours each night. Ben spent the last 3 years specialising in Distributed Ledgers and other forms of emerging technology at RBS.

Stephen Chandler, Investor Stephen is the Co-founder and Managing Partner of Notion Capital, the leading venture capital firm, and a board director of / adviser to numerous high-potential B2B tech companies. He is an entrepreneur, investor and company builder, with over 20 years' experience in forming, funding, running, advising and investing in hyper-growth tech businesses. Part of the founding management team of over ten businesses, including leading cyber-security player MessageLabs (sold to Symantec in 2008 for $700m), with involvement in dozens more, Stephen has

helped a number of leading tech companies to develop and execute winning market strategies, either as an external professional advisor, a non-executive director or as a member of their senior leadership team. He sits on the board of Tradeshift, the tech 'Unicorn' which is a member of Hyperledger's governing board and a pioneer user of blockchain for supply chain payments as well as several other leading data, fintech and/or cyber companies (e.g. GoCardless, Panaseer, Dealflo and Paddle), often increasingly leveraging distributed ledger technologies in their offerings.

James Bruegger, Adviser James is the Chief Investment Officer and co-founder of the Seraphim Space Fund – the world's first venture capital fund focused on the Space Sector. James is one of the most active investors globally in new satellite constellations, having invested in the likes of Spire (www.spire.com) and Iceye (www.iceye.com) who between them have raised in excess of $150m in funding. James is also the co-founder of Seraphim Space Camp – the world's first accelerator focused on the Space Sector. Over the last 18 years, James has started, advised and invested in 40+ companies in UK, Europe, US and Asia. Prior to joining Seraphim Capital (a UK-based visionary deep-tech venture capital fund manager) in 2006, James spent a number of years working in M&A for Deloitte, advising private equity funds and corporates on more than $4.5billion worth of acquisitions. He holds a first class degree in History from University College London where he specialised in the history of science and medicine.

Nick Miles, Adviser Nick is one of the most experience PR advisers in London. Currently serving as Chairman of Montfort Communications, he was previously both founder and Chairman of M Communications and Financial Dynamics.

IMPORTANT INFORMATION

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

The Project Documents in its current form are circulated by the Token Vendor for general information and to invite feedback only on the Project, the Arqit platform, the Arqit tokens and their functions, and the Token Sale as presently conceived, and is subject to review and revision by the directors of the Token Vendor and/or advisors of the Token Vendor. Please do not replicate or distribute any part of the Project Documents without this section in accompaniment. The information in the Project Documents, including information set forth below, may not be exhaustive and no part of the Project Documents is intended to create legal relations with a recipient of the Project Documents or to be legally binding or enforceable by such recipient against the Token Vendor. An updated version of the Project Documents may be published at a later date and to be announced by the Token Vendor in due course.

PLEASE READ THIS SECTION AND THE FOLLOWING SECTIONS ENTITLED "DISCLAIMER OF LIABILITY", "NO REPRESENTATIONS AND WARRANTIES", "REPRESENTATIONS AND WARRANTIES BY YOU", "CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS", "THIRD PARTY INFORMATION AND NO CONSENT OF OTHER PERSONS", "TERMS USED", "NO ADVICE", "NO FURTHER INFORMATION OR UPDATE", "RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION", "NO OFFER OF INVESTMENT OR REGISTRATION" AND "RISKS AND UNCERTAINTIES" CAREFULLY.

IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

While we make every effort to ensure that any material in the Project Documents is accurate and up to date, such material in no way constitutes the provision of professional advice. The Token Vendor does not guarantee, and accepts no legal liability whatsoever arising from or in connection with, the accuracy, reliability, currency, or completeness of any material contained in the Project Documents. Potential purchasers of Arqit tokens should seek appropriate independent professional advice prior to relying on, or entering into any commitment or transaction based on, material published in the Project Documents, which material is published purely for reference purposes alone.

The Arqit tokens are proprietary cryptographic tokens developed and issued by the Token Vendor to function as the native utility token used in the Arqit platform as the means of value exchange and to power the Arqit platform.

The Project Documents do not constitute or form part of any opinion or any advice to purchase, sell or otherwise transact in Arqit tokens and the fact of presentation of the Project Documents shall not form the basis of, or be relied upon in connection with, any contract or decision to purchase Arqit tokens.

No Arqit token should be construed, interpreted, classified or treated as enabling, or according any opportunity to purchasers to participate in or receive profits, income, or other payments or returns arising from or in connection with the Token Vendor, the Project Group, the Arqit platform, the Arqit tokens, or the proceeds of the Token Sale, or to receive sums paid out of such profits, income, or other payments or returns.

No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the Arqit tokens, and no cryptocurrency other than those provided for in the Project Documents or other form of payment is to be accepted on the basis of the Project Documents.

Any agreement as between the Token Vendor and you as a purchaser, and in relation to any sale and purchase, of Arqit tokens is to be governed only by a separate document setting out the terms and conditions (the "**Token Sale Terms**") of such agreement. In the event of any inconsistencies between the Token Sale Terms and the Project Documents, the former shall prevail.

There are risks and uncertainties associated with the Token Vendor, the Project Group, the Project, the Arqit tokens, the Arqit platform, and the Token Sale. Please refer to the section entitled "Risks and Uncertainties" set out at the end of the Project Documents.

The Project Documents, any part thereof and any copy thereof must not be taken or transmitted to any jurisdiction where distribution or dissemination of the Project Documents is prohibited or restricted.

No part of the Project Documents is to be reproduced, distributed or disseminated without including this section and the following sections entitled "Disclaimer of Liability", "No Representations and Warranties", "Representations and Warranties By You", "Cautionary Note On Forward-Looking Statements", "Third Party Information and No Consent of Other Persons", "Terms Used", "No Advice", "No Further Information or Update", "Restrictions On Distribution and Dissemination", "No Offer of Investment or Registration", and "Risks and Uncertainties".

Disclaimer of Liability

To the maximum extent permitted by the applicable laws, regulations and rules, the Token Vendor shall not be liable for any direct, indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on the Project Documents or any part thereof by you.

No Representations and Warranties

The Token Vendor and/or the Project Group does / do not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in the Project Documents.

Representations and Warranties by you

By accessing and/or accepting possession of any information in the Project Documents or such part thereof (as the case may be), you represent and warrant to the Token Vendor and the Project Group as follows:

(a)   you agree and acknowledge that the Arqit tokens do not constitute shares or securities of any form, units in a business trust, units in a collective investment scheme or any other form of regulated investment or investment product in any jurisdiction;

(b)   you are not:

      (i)   a U.S. Person (as defined in Regulation S under the U.S. Securities Act of 1993, as amended);

      (ii)   if you are an individual, a person who is a citizen of, domiciled in, resident of, or physically present / located in a jurisdiction stipulated in Annex 1 hereto ("**Excluded Jurisdiction**");

      (iii)   if you are a body corporate, a body corporate :

            (aa)   which is incorporated or organised in, or operates out of, an Excluded Jurisdiction, or

24

(bb) which is under the control of one or more individuals who is/are citizen(s) of, domiciled in, residents of, or physically present / located in, an Excluded Jurisdiction; and/or

(iv) an individual or body corporate which is otherwise prohibited or ineligible in any way, whether in full or in part, from participating in any part of the transactions contemplated in the Token Sale Terms,

(collectively, "**Excluded Persons**");

(c) you are fully aware of and understand that you are not eligible and you are not to purchase any Arqit tokens if you are an Excluded Person;

(d) you agree and acknowledge that the Project Documents do not constitute prospectuses or offer documents of any sort and are not intended to constitute an offer of shares or securities of any form, units in a business trust, units in a collective investment scheme or any other form of regulated investment or investment product in any jurisdiction, or a solicitation for any form of regulated investment or investment product, and you are not bound to enter into any contract or binding legal commitment and no cryptocurrency other than those provided for in the Project Documents or other form of payment is to be accepted on the basis of the Project Documents;

(e) you agree and acknowledge that no Arqit token should be construed, interpreted, classified or treated as enabling, or according any opportunity to, Arqit token holders to participate in or receive profits, income, or other payments or returns arising from or in connection with Token Vendor, the Project Group, the Arqit tokens or the proceeds of the Token Sale, or to receive sums paid out of such profits, income, or other payments or returns;

(f) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in the Project Documents, no action has been or will be taken by the Token Vendor to obtain such approval under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of the Project Documents to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;

(g) you agree and acknowledge that the Project Documents, the undertaking and/or the completion of the Token Sale, or future trading of Arqit tokens on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of the Token Vendor, the Project, the Arqit tokens, the Token Sale, and the Arqit platform;

(h) the distribution or dissemination of the Project Documents, any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to the Token Vendor;

(i) you agree and acknowledge that in the case where you wish to purchase any Arqit tokens, Arqit tokens are not to be construed, interpreted, classified or treated as:

(i) any kind of currency other than cryptocurrency;

(ii) debentures, stocks or shares issued by the Token Vendor, the Project Group, or any other person or entity;

(iii) rights, options or derivatives in respect of such debentures, stocks or shares;

(iv) rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

(v) securities;

25

      (vi)   units or derivatives of units in a business trust;

      (vii)   units in a collective investment scheme; or

      (viii)   any form of regulated investment or investment product;

(j)   you are legally permitted to participate in the Token Sale and all actions contemplated or associated with such purchase, including the holding and use of Arqit tokens;

(k)   the amounts that you use to purchase Arqit tokens were not and are not directly or indirectly derived from any activities that contravene the laws and regulations of any jurisdiction, including anti-money laundering laws and regulations;

(l)   if you are a natural person, you are of sufficient age and capacity under the applicable laws of the jurisdiction in which you reside and the jurisdiction of which you are a citizen to participate in the Token Sale;

(m)   you are not obtaining or using Arqit tokens for any illegal purpose;

(n)   none of:

      (i)   you;

      (ii)   any person controlling or controlled by you;

      (iii)   if you are a privately-held entity, any person having a beneficial interest in you; or

      (iv)   any person for whom you are acting as agent or nominee in connection with this Token Sale,

is a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure.

A "senior foreign political figure" is defined as a senior official in the executive, legislative, administrative, military or judicial branch of a government (whether elected or not), a senior official of a major political party, or a senior executive of a foreign government-owned corporation, and includes any corporation, business or other entity that has been formed by, or for the benefit of, a senior foreign political figure.

A "immediate family" of a senior foreign political figure typically includes such figure's parents, siblings, spouse, children and in-laws.

A "close associate" of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with such senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of such senior foreign political figure;

(o)   if you are affiliated with a non-U.S. banking institution ("**Foreign Bank**"), or if you receive deposits from, make payments on behalf of, or handle other financial transactions related to a Foreign Bank, you represent and warrant to the Token Vendor that:

      (i)   the Foreign Bank has a fixed address, and not solely an electronic address, in a country in which the Foreign Bank is authorised to conduct banking activities;

      (ii)   the Foreign Bank maintains operating records related to its banking activities;

      (iii)   the Foreign Bank is subject to inspection by the banking authority that licensed the Foreign Bank to conduct its banking activities; and

(iv)   the Foreign Bank does not provide banking services to any other Foreign Bank that does not have a physical presence in any country and that is not a regulated affiliate;

(p)   you have such knowledge and understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology so as to be able to evaluate the risks and merits of the Project, the Arqit tokens, and the Arqit platform, and correspondingly any purchase of the Arqit tokens;

(q)   you are fully aware and understand that in the case where you wish to purchase any Arqit tokens, there are risks associated with the Token Vendor, the Project Group, the Project, the Arqit tokens, the Arqit platform and the Token Sale;

(r)   you bear the sole responsibility to determine what tax implications purchasing Arqit tokens may have for you and agree not to hold the Token Vendor or any other person involved in the Token Sale liable for any tax liability associated with or arising therefrom;

(s)   you agree and acknowledge that neither the Token Vendor nor the Project Group is liable for any direct, indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on the Project Documents or any part thereof by you;

(t)   you waive the right to participate in a class action lawsuit or a class wide arbitration against the Token Vendor and/or any person involved in the Token Sale and/or with the creation and distribution of Arqit tokens or the Arqit platform; and

(u)   all of the above representations and warranties are true, complete, accurate and non-misleading from the time of your access to and/or acceptance of possession the Project Documents or such part thereof (as the case may be).

Cautionary Note on Forward-Looking Statements

All statements contained in the Project Documents, statements made in press releases or in any place accessible by the public and oral statements that may be made by the Token Vendor, the Project Group, or their respective directors, executive officers or employees acting on behalf of the Token Vendor or the Project Group (as the case may be), that are not statements of historical fact, constitute "forward-looking statements". Some of these statements can be identified by forward-looking terms such as "aim", "target", "anticipate", "believe", "could", "estimate", "expect", "if", "intend", "may", "plan", "possible", "probable", "project", "should", "would", "will" or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding the Token Vendor, the Project Group, and/or the future outlook of the industry which the Token Vendor and the Project Group are in are forward-looking statements. These forward-looking statements, including but not limited to statements as to the Token Vendor, the Project Group and other matters discussed in the Project Documents regarding the Token Vendor and the Project Group are matters that are not historic facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may have an impact or adversely affect the Token Vendor and/or the Project Group, the Project, the Arqit platform, or the use of the Arqit tokens. These factors include, amongst others:

(a)   changes in political, social, economic and stock or cryptocurrency market conditions, and the regulatory environment in the countries in which the Project Group conducts its business and operations;

(b)   the risk that the Project Group may be unable to execute or implement the Project;

(c)   changes in interest rates and exchange rates of fiat currencies and cryptocurrencies;

27

(d)   changes in the anticipated growth strategies and expected internal growth of the Project Group and the Project;

(e)   changes in fees payable to the Project Group in connection with its businesses and operations or on the Project;

(f)   changes in the availability and salaries of employees who are required by the Project Group to operate its business and operations;

(g)   changes in preferences of users of the Arqit platform;

(h)   changes in competitive conditions under which the Project Group operates, and the ability of the Project Group to compete under such conditions;

(i)   changes in the future capital needs of the Project Group and the availability of financing and capital to fund such needs;

(j)   war or acts of international or domestic terrorism;

(k)   occurrences of catastrophic events, natural disasters and acts of God that affect the businesses and/or operations of the Project Group;

(l)   other factors beyond the control of the Token Vendor and/or the Project Group; and

(m)   any risk and uncertainties associated with the Token Vendor, the Project Group, the Project, the Arqit tokens, the Arqit platform and the Token Sale.

All forward-looking statements made by or attributable to the Token Vendor, the Project Group, or persons acting on behalf of the Token Vendor and/or the Project Group, or relating to the Arqit platform are expressly qualified in their entirety by such factors. Given the risks and uncertainties that may cause the eventual outcome to be materially different from that expected, expressed or implied by the forward-looking statements in the Project Documents, undue reliance must not be placed on these statements. These forward-looking statements are applicable only as of the date of the Project Documents.

The Token Vendor, the Project Group, and/or any other person do not represent, warrant, and/or undertake the contents in those forward-looking statements, and the eventual outcome may differ materially from those anticipated in these forward-looking statements.

Nothing contained in the Project Documents is or may be relied upon as a promise, representation or undertaking relating to the Token Vendor and/or the Project Group, or the Arqit platform.

Further, the Token Vendor and the Project Group each disclaims any responsibility to update any of those forward-looking statements or publicly announce any revisions to those forward-looking statements to reflect future developments, events or circumstances, even if new information becomes available or other events occur in the future.

Third Party Information and No Consent of Other Persons

The Project Documents include information obtained from various third party sources ("**Third Party Information**"). The consent of the publishers of the Third Party Information has not been sought for the inclusion of the Third Party Information in the Project Documents and such publishers are therefore not liable for the Third Party Information. While the Token Vendor and the Project Group have taken reasonable action to ensure that the Third Party Information have been included in their proper form and context, the Token Vendor, the Project Group, and/or their respective directors, executive officers, and employees acting on its behalf, have not independently verified the accuracy, reliability, completeness of the contents, or ascertained any applicable underlying assumption, of the relevant Third Party Information. Consequently, the Token Vendor, the Project

28

Group, and/or their respective directors, executive officers, and employees acting on their behalf do not make any representation or warranty as to the accuracy, reliability or completeness of such information and shall not be obliged to provide any updates on the same.

Terms used

To facilitate a better understanding of the Arqit tokens being offered for purchase by the Token Vendor, and the businesses and operations of the Project Group, certain technical terms and abbreviations, as well as, in certain instances, their descriptions, have been used in the Project Documents. These descriptions and assigned meanings should not be treated as being definitive of their meanings and may not correspond to standard industry meanings or usage.

Words importing the singular shall, where applicable, include the plural and *vice versa* and words importing the masculine gender shall, where applicable, include the feminine and neuter genders and *vice versa*. References to persons shall include corporations.

No Advice

No information in the Project Documents should be considered to be business, legal, financial or tax advice regarding the Token Vendor, the Project Group, the Project, the Arqit tokens, the Arqit platform, or the Token Sale. You should consult your own legal, financial, tax or other professional advisor regarding the Token Vendor, the Project Group, the Project, the Arqit tokens, the Arqit platform, and the Token Sale. You should be aware that you may be required to bear all risks of any purchase of Arqit tokens for an indefinite period of time.

None of the advisors engaged by the Token Vendor and/or the Project Group has made or purports to make any statement in the Project Documents or any statement upon which a statement in the Project Documents is based and each of them makes no representation regarding any statement in the Project Documents and to the maximum extent permitted by law, expressly disclaims and takes no responsibility for any liability to any person which is based on, or arises out of, any statement, information or opinions in, or omission from, the Project Documents.

No Further Information or Update

No person has been or is authorised to give any information or representation not contained in the Project Documents in connection with the Token Vendor, the Project Group, the Project, the Arqit tokens, the Arqit platform, or the Token Sale and, if given, such information or representation must not be relied upon as having been authorised by or on behalf of the Token Vendor and/or the Project Group. The Token Sale shall not, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of the Token Vendor and/or the Project Group or in any statement of fact or information contained in the Project Documents since the date hereof.

Restrictions on Distribution and Dissemination

The distribution or dissemination of the Project Documents or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of the Project Documents or such part thereof (as the case may be) at your own expense and without liability to the Token Vendor and/or the Project Group.

Persons to whom copies of the Project Documents have been distributed, disseminated, or provided access to or who otherwise have the Project Documents in their possession, shall not circulate it to any other persons, reproduce or otherwise distribute the Project Documents or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

No Offer of Investment or Registration

Arqit tokens are not intended to be and should not be construed to constitute shares or securities of any form, units in a business trust, units in a collective investment scheme or any other form of regulated investment or investment product in any jurisdiction. The Project Documents do not constitute prospectuses or offer documents of any sort and are not intended to and should not be construed to constitute an offer of shares or securities of any form, units in a business trust, units in a collective investment scheme or any other form of investment, or a solicitation for any form of investment in any jurisdiction. No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the Arqit tokens and no cryptocurrency (other than those provided for in the Project Documents) or other form of payment is to be accepted on the basis of the Project Documents.

THE TOKEN SALE (AS REFERRED TO IN THE PROJECT DOCUMENTS) IS INTENDED FOR, MADE TO OR DIRECTED AT ONLY PERSONS WHO ARE NOT EXCLUDED PERSONS. ACCORDINGLY, YOU ARE NOT ELIGIBLE AND YOU ARE NOT TO PURCHASE ANY ARQIT TOKENS IN THE TOKEN SALE IF YOU ARE AN EXCLUDED PERSON.

No regulatory authority has examined or approved of any of the information set out in the Project Documents. No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of the Project Documents does not imply that the applicable laws, regulatory requirements or rules have been complied with.

Risks and Uncertainties

Prospective purchasers of Arqit tokens should carefully consider and evaluate all risks and uncertainties associated with the Token Vendor, the Project Group, the Arqit tokens, the Project, the Arqit platform, and the Token Sale, and all information set out in the Project Documents and the Token Sale Terms prior to any purchase of the Arqit tokens. If any of such risks and uncertainties develop into actual events, the business, financial condition, results of operations and prospects of the Project, the Arqit platform, the Token Vendor and/or the Project Group could be materially and adversely affected. In such cases, the value or the trading price of the Arqit tokens may be indirectly impacted.

Please refer to the risks and warnings set out in the Token Sale Terms before deciding to purchase Arqit tokens. It should be noted the aforementioned list of risks and warnings is not exhaustive. Accordingly, prospective purchasers should not place undue reliance on these statements.

ANNEX 1
Excluded Jurisdictions

1. The People's Republic of China (which for the purpose of this Whitepaper shall exclude the Hong Kong Special Administrative Region of the People's Republic of China, the Macau Special Administrative Region of the People's Republic of China, and the Republic of China (Taiwan))

2. US

3. Democratic People's Republic of Korea[#^]

4. Democratic Republic of the Congo[^]

5. Eritrea[^]

6. Ethiopia[#]

7. Iran[#^]

8. Libya[^]

9. Pakistan[#]

10. Somalia[^]

11. Serbia[#]

12. Sri Lanka[#]

13. South Sudan[^]

14. Sudan[^]

15. Syria[#^]

16. Trinidad and Tobago[#]

17. Tunisia[#]

18. Yemen[#^]

19. Any jurisdiction in which the Token Sale is prohibited, restricted or unauthorised in any form or manner whether in full or in part under the Laws, regulatory requirements or rules in such jurisdiction

[#] *Jurisdictions with strategic anti-money laundering / counter-financing of terrorism deficiencies most recently identified by the Financial Action Task Force at <http://www.fatf-gafi.org/countries/#high-risk>*

[^] *Jurisdictions in which designated individuals and entities are identified by the MAS for the purposes of regulations promulgated under the Monetary Authority of Singapore Act (Chapter 186) of Singapore, the United Nations Act (Chapter 339) of Singapore or the Terrorism (Suppression of Financing) Act (Chapter 325) of Singapore*