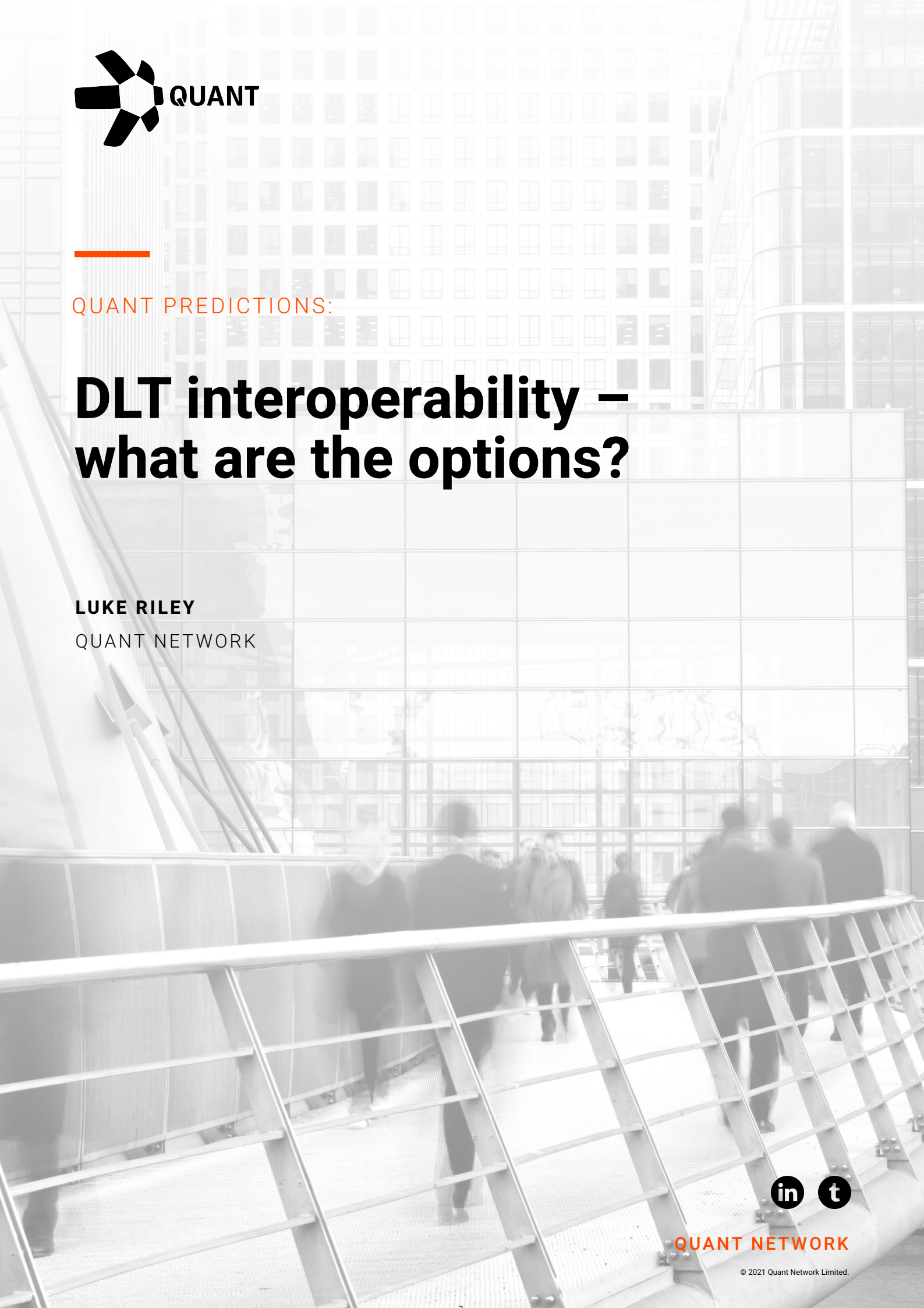
QUANT

QUANT PREDICTIONS:

DLT interoperability – what are the options?

LUKE RILEY
QUANT NETWORK



QUANT NETWORK

Contents

Foreword

This report was originally a submission to the UK All Party Parliamentary Group (APPG) on Blockchain. On February 23rd, 2021, the APPG held an evidence session in Parliament on Blockchain interoperability and scalability.[1] Quant Network was invited to provide evidence to the session. Dr Luke Riley, Head of Innovation at Quant, attended and as part of this evidence submission, he presented a detailed analysis investigating different approaches to DLT interoperability. The following is the evidence that was submitted.

[1] www.biginnovationcentre.com/event/interoperability-scalability-and-sustainability/

Executive Summary

Nowadays distributed ledger networks (DLNs) do not exist in silos. They increasingly need to be connected to external resources such as legacy systems, distributed filestores and other distributed ledger networks. To perform these connections, developers need to utilise a distributed ledger technology (DLT) interoperability solution to solve issues regarding standardised resource integration and data translation methods.

There are a few possible DLT interoperability solutions, each fitting into one of the following three DLT interoperability categories as defined by the World Economic Forum (WEF): (1) cross authentication (2) oracles and (3) API gateways. In this paper we describe the three categories and provide a comparison between them focusing on features such as resilience, decentralisation, and user connections.

Our comparison concludes that the API gateway categorisation is the leading approach. This is because (a) API gateways are built on proven technology (b) they can easily combine distributed ledger technology with non-distributed ledger technologies (c) they can provide fine-grained user access controls and (d) they can be utilised by cross authentication or oracle applications to provide more resilience to their deployments.

We conclude this report by describing how Quant's Overledger DLT API Gateway product stands out as the pre-eminent solution in this category through its use of cross-DLT data standardisation and ease of DLN integration, all of which improve the speed of DLT application deployment.

The necessity of distributed ledger interoperability standardisation

DLT is rapidly evolving yet still very new. Even though there are many different DLT implementations, the ability of these implementations to work together is very limited. This presents a huge barrier to adoption. The many advantages of using a DLT must be balanced against the technical complexity of operating it, as well as the strategic implications of using a DLT if it is a struggle to connect with other DLTs (let alone connect to other technologies like distributed databases, distributed file stores and legacy IT systems). Currently, from a technical point of view, most DLT implementations require experts with niche skills, particularly in smart contract languages, cryptography and DLT data structures. This means that application development requires expensive consultants or staff with specific skillsets – skillsets which cannot be easily redeployed to other projects as business needs evolve.

To ease this process, the distributed ledger industry must move towards standardisation with a specific focus on interoperability. There already are, and will continue to be, many distributed ledger technologies, including many different distributed ledger networks (DLNs) utilising the same technology. Currently, some DLNs are connected using the interoperability approaches defined in the next section, yet inevitably more will need to be connected to break down further data siloes. Additionally, DLT cannot exist completely separate to other technologies (e.g. distributed databases, distributed stores, IoTs and legacy systems) and so interoperability standards need to incorporate these concerns.

At a high level, we can split distributed ledger interoperability standardisation concerns into two main topics:

1. **Integration:** How can multiple distributed ledger (and other) technologies connect?
2. **Data translation:** How can request and response data from multiple distributed ledger (and other) technologies be combined into an understandable format?

Distributed Ledger Technology integration interoperability categorisations and comparisons

At Quant, we subscribe to the DLT integration interoperability categories defined by the World Economic Forum (WEF)[2] In this section we will briefly introduce them and then perform a detailed comparison between them. We will highlight that we believe the API gateway categorisation is the superior interoperability approach, due to the fact this category is based on proven technology, can easily connect different technology types, can handle many user connections, and can provide fine-grained user access controls.

WEF DLT interoperability category 1: cross authentication

This interoperability category is the most decentralised of the three categories. It requires separate authorisation on each side of the interoperability connection. Examples include:

Hashlocking: for example, used to atomically swap assets across distributed ledgers.

DLT-relayers: these are distributed ledger communication protocols that act as a layer between other distributed ledgers. They are designed for the exchange of different types of messages between these networks. Two DLT-relayer examples are Polkadot and Ethereum 2.0.

WEF DLT interoperability category 2: oracles

Oracles allow distributed ledgers to connect to external data resources (which may be another distributed ledger). Oracles are therefore orchestration layers, connected to different resources, which perform various actions according to on-chain and off-chain pre-defined bespoke rules. Some oracles not only pass information from an external data resource to smart contracts but also send data from the distributed ledger back to the external resources. There is usually a single oracle to perform each task, but occasionally there can be a collection of oracles performing the same task (in a permissioned or permissionless manner). Smart contract logic then states how consensus of data is achieved between multiple inputs recorded by different oracles. An example of an oracle system is Chainlink.

WEF DLT interoperability category 3: API gateway

An API provides access to a server and the resources it is connected to. An API gateway provides organised access to many underlying API resources, simplifying requests to the underlying resources to improve the user experience. A DLT API gateway can have shared end points across distributed ledger networks, standardised DLT data objects, and can compress many DLT actions into one endpoint. A leading example is Quant's Overledger API.

[2] Approaches to Interoperability Section, World Economic Forum, https://widgets.weforum.org/blockchain-toolkit/interoperability/

WEF DLT interoperability: Category comparison

Note that in the following discussion, DLT-relayers are discussed as the primary cross-authentication interoperability model, as the other WEF listed options for this category (e.g. hash locks and notary schemes) perform only limited interoperability functionality (e.g. just asset swapping or data time stamping respectively).

To evaluate and compare the different integration interoperability categorisations, we focused on the following properties:

Proven technology: DLT-relayers (such as Polkadot and Ethereum 2.0) are not yet proven technology. It is true that they have been in development for many years, but there is yet to be a stable implementation running in a high load environment for a considerable time period. As of writing, the most popular DLT-relayer examples, Polkadot and Ethereum 2.0, have only recently established their beacon chain (that is the chain which will be used to connect other chains). On the other hand, API gateways have a long proven record with thousands of implementations around the world to connect users to all types of resources. Finally, for oracles, even though it is true that data feed technology is established, data feeds from one distributed ledger network to another and back, has again yet to have a proven implementation running for a considerable time-period.

Combining different technologies: Many interoperability applications will want to connect to multiple technology types, such as permissioned and permissionless DLTs, distributed databases, distributed filesystems and of course legacy systems. If this is the case, a DLT-relayer cannot be chosen for this type of interoperability application as by definition DLT nodes cannot directly introduce a probabilistic element into their logic (and a direct connection from a distributed ledger to another resource would introduce a probabilistic element as the other resource cannot be guaranteed to always be available). But we do note that DLT-relayers **may in the future** be able to connect to non-DLT technology through a middleware bridge.

Decentralisation method: As stated by World Economic Forum (WEF), the three different models have different decentralisation properties. For DLT-relayers, they can be fully decentralised if a permissionless DLN design is used. For oracles, there are two different levels of permissions. Firstly, who can be an oracle depends on the network permissions (oracles need to have read and write access to the underlying DLNs). Secondly, as oracles place their data into smart contracts, the functions of these smart contracts may have additional attached permissions (e.g. user access controls). Whereas API gateways use more generally established user access control methods defined by the operator running the API gateway. When API gateways are used, the amount of decentralisation is dependent on the number of separate API gateways run by different stakeholders.

How users interact: Users not running the interoperability software need a way to interact with it. For DLT-relayers, users either need to be provided direct access to relayer nodes (which is a security risk as nodes can have sensitive functions) or the users need to be provided access to DLT-relayer nodes through an API gateway model. For non-oracle users, they can interact with the on-chain oracle smart contracts (again requiring an API gateway), or they can interact with the off-chain oracle instance (in a manner resembling an API gateway). Finally, for the API gateway itself, users interact through the API using standard elements like REST.

Resilience: The resilience of DLT-relayers is dependent on the consensus protocols they run, particularly the consensus protocol of the connecting chain (sometimes known as the beacon chain). Each consensus protocol has limits on the percentage of malicious nodes that it can handle, and therefore the resilience of the entire network is dependent on the number of nodes in the network. For the oracle design, the more oracles feeding data about the same topic, the more resilient the system will be (as long as a method to solve Sybil attacks has been implemented and data quality control aspects are in place). Whereas an API gateway's resilience will come from the number of instances running and its load balancing capabilities.

Interoperability Option	Proven Tech	Can combine different technologies	Decentralisation method	How users interact	Resilience
DLT-Relayers	No	No	Dependent on network permissions	Direct node connection or through API gateway	Depends on number of nodes in network
Oracles	Not in terms of DLN to DLN	Yes	Dependent on network and smart contract permissions	Connect to oracle's on-chain or off-chain elements	Depends on number of oracles
API Gateway	Yes	Yes	Access controlled by API gateway operator	Connect to API	Depends on number of API gateway instances, and number of API gateway connected nodes

Distributed Ledger Technology data translation interoperability considerations

Providing a generic data object framework for a fast-moving and open technology like DLT is a complex task, but already standard bodies have formed for this reason. We would like to highlight the ongoing ISO/TC 307 standardisation work (and the BSI DLT UK mirror committee DLT/1), established by Quant's CEO Gilbert Verdian in 2015. Today, there are 57 countries and organisations that are involved in ISO/TC 307, actively working together to standardise the technology, some aspects of which directly relate to data object standardisation (e.g. the ontology and taxonomy deliverable ISO/DTS 23258). Additionally, there is an emerging IETF standard Open Digital Asset Protocol (ODAP[3]), which includes identification of data objects stored on DLTs using a standardised URL format. ODAP therefore provides standardised and straightforward addressing of data assets.

At Quant we think of data translation interoperability considerations in the following two sections:

- **Common data objects:** where developers would have one format for common DLT objects such as transaction, smart contract, account, node, current state record, etc. Therefore, developers could read common data objects from different distributed ledger (and related) technologies in the same style.

- **Common interaction method:** Additionally, developers would perform common functionalities, such as build transaction, send transaction, add account, etc. on different distributed ledger (and related) technologies in the same manner.

In terms of the three integration interoperability categorisations defined in the previous section, we at Quant believe that the DLT API gateway model is the only reasonable way to provide a common data object and interaction model for users across DLTs. Briefly, this is because the purpose of the connecting chain (in the DLT-relayer category) is to allow cross-chain transactions not to provide a top-level common interface. And for the oracle category, different data feeds only provide the necessary translation to allow relevant external data to be placed in one specific distributed ledger. In the final section we discuss at a high level how Quant's Overledger system integrates these standards.

[3] The Open Digital Asset Protocol (ODAP) https://tools.ietf.org/html/draft-hargreaves-odap-00

For context, data translation for different DLTs is a complex task as data on DLTs can be formatted in vastly different manners. But the main data format differentiators are heavily influenced by the following distributed ledger technology properties:

- **Accounts or UTXO-based storage architectures:** Each distributed ledger has an associated state. The state is uniquely indexed either by userID/address (accounts-based) or via unspent transaction output reference (UTXO-based). This storage architecture indexing style subsequently affects the transaction formatting. Examples of accounts-based DLTs are Ethereum, Hyperledger Fabric and the XRP Ledger. Examples of UTXO-based DLTs are Bitcoin, Litecoin Corda.

- **User defined Turing complete smart contracts:** Each DLT can choose to allow user defined smart contracts written in a Turing complete language[4] or not. Examples of user defined Turing complete smart contract DLTs are Ethereum, Corda and Hyperledger Fabric. Examples of DLTs not allowing this are Bitcoin and the XRP Ledger.

- **Permissioned or permissionless DLN:** Each DLT can be deployed as a permissioned or permissionless distributed ledger network, but some are more appropriate for one domain over the other. DLTs like Corda, Hyperledger Fabric and Hyperledger Besu (which is Ethereum based), provide more authentication features as they were initially designed to be deployable in permissioned networks. These authentication features require additional request and response considerations.

[4] Note that even though some DLTs will allow smart contracts to be written in a Turing complete language, there will still be computational restrictions placed on this code (e.g. block computation limit), meaning that these DLTs are sometimes referred to as implementing "near Turing complete" code.

Quant's Overledger DLT API Gateway

e. Two-way asset transfers: Tokenised assets can be moved from one DLN to another DLN and back again, using a token lock, mint and burn process.

f. Single ledger token to multi ledger token transformation: A tokenised asset originally created on a single DLN can be transformed into a multi ledger token (and back again if required).

g. Multi ledger meta transactions: Transactions can be broadcast on different DLNs with the same data payload. This data payload can include aspects like hashes of off-chain data, as well as additional signatures, from a National Institute of Standards and Technology (NIST) approved and/or quantum secured signature scheme.

h. Linked transactions: Transactions in different DLNs can grouped together, tracking their process and replayed if required.

Conclusion

In this report we have described the main DLT interoperability categories and compared them. We have described why Quant believe that the API gateway category is the leading one and have detailed why Quant's Overledger is the pre-eminent instance of this model.

We know that over time there will be increasing demand for DLT interoperability solutions and therefore Quant is well placed to provide an enterprise grade and DLT standardised product for this burgeoning market.

LUKE RILEY

HEAD OF INNOVATION

After completing a PhD in Computer Science at the University of Liverpool, Luke moved on to King's College London, where he developed the college's online DLT module and played a key role in EPSRC DLT funded projects for voting system and consensus protocol development. Today, Luke leads Quant's R&D group, where he has made a vital contribution to shaping the company's unique technology by developing interoperability applications for atomic swaps, cross chain asset transfers, payment channel hubs and multi-ledger tokens. He also plays an essential part in helping Quant lead DLT standardisation and developing generic DLT APIs and re-useable data objects. Through Quant, Luke is also involved with ISO technical DLT committees and IEFT DLT proposals.

Visit our website to see how you can benefit from Overledger's ground-breaking technology.

www.quant.network

Registered Offices

U.K
20-22 Wenlock Road,
London,
N1 7GU,
United Kingdom

Switzerland
Dammstrasse 16,
6300 Zug,
Switzerland

Company No 09798383

Visit our website