QUANT

Bridge to the future

Achieving asset portability with confidence

October 2023

Unless there is easy and seamless connectivity between different tokenised asset types on multiple different platforms, the full benefits of tokenisation will not be realised.

Yet providing this interoperability has proved a major obstacle.

One promising solution is the concept of the blockchain bridge.

While bridges can also introduce high cost and risk, recent developments mean that they can be made accessible, secure and cost-effective to implement.

Dr Luke Riley, Head of Innovation at Quant, provides an overview of the benefits of bridges and how they can be effectively deployed.

Tokenisation:
The future of finance

Ever since blockchain technology first captured the public imagination some fifteen years ago, it has promised to transform the financial world. With every year that passes, new and innovative use cases emerge, and the technology attracts more and more users. Although the precise timeframe remains a matter of debate, most experts agree that mass adoption is 'just around the corner'.

The driving force of this growth is multidimensional. Although there may be many applications of blockchain technology, both inside and outside of the financial sector, one of the principal reasons for its success is its ability to leverage the massive benefits of tokenisation: the process of digitally representing assets and liabilities on a blockchain to record information such as their attributes, status, transaction history, and ownership. It is a process which has created new types of asset classes and players, and which offers a wide range of significant benefits compared to traditional assets, such as open access, transparency, and reduced transactional friction and cost.

"Citi forecasts $4-5 trillion of tokenised digital securities by 2030."

In March 2023, Citi issued a report that estimated the tokenisation market in global illiquid assets, from real estate to artwork would reach approximately $16 trillion, or nearly 10% of global GDP, by 2030. The benefits of tokenisation are so significant that the liquid markets – such as funds and commodities – are projected to reach $4-5 trillion by the same year.

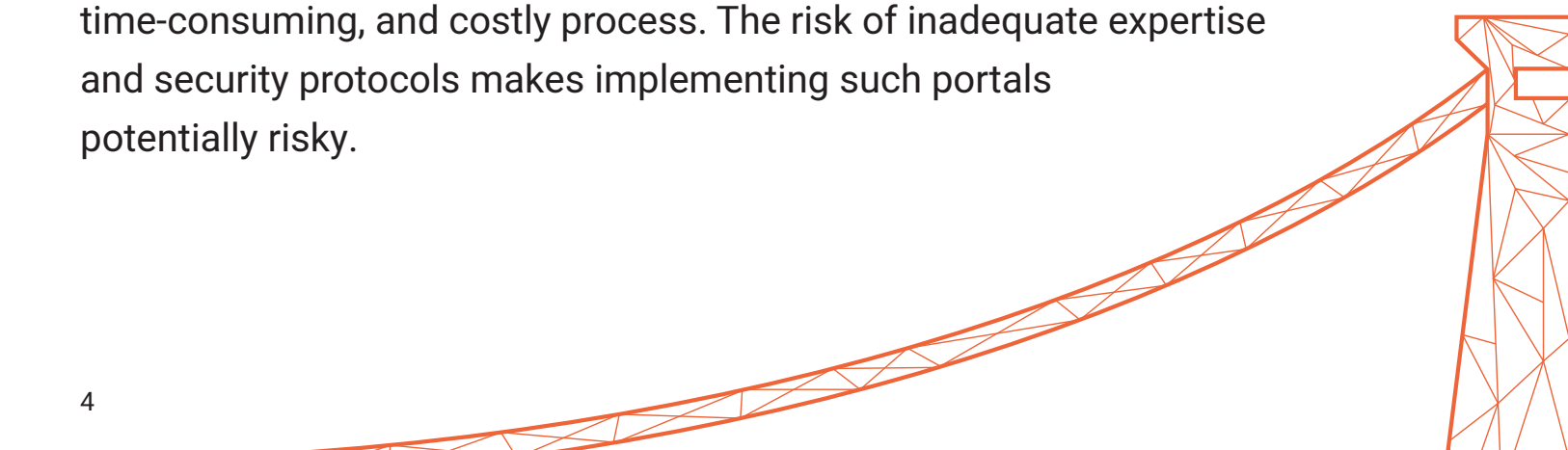
Most experts and leading financial institutions agree that tokenisation has begun to revolutionise the financial world, and is likely to trigger the mass adoption of blockchain.

A key challenge

Before the benefits of tokenisation can be unlocked, some important challenges must be overcome. One of these challenges, arguably the most critical, derives from the history and fundamental nature of blockchain itself. This is the issue of interoperability. Following the appearance of Bitcoin in 2009, different types of blockchain soon emerged, each developed in isolation, without regulation or standards. The result was that different blockchains could not connect to each other, effectively creating an ecosystem based on 'walled gardens', which has led to inefficient and fragmented markets with smaller-scale liquidity pools.

Obviously, a solution was required: a way to interconnect platforms. This would deliver massive benefits, such as opening assets to new pools of both institutional and individual investors, allowing assets to move between trading venues with ease. It would also create an environment perfectly suited to stablecoins and central bank digital currencies, as well as blockchain-native currency and payment mechanisms.

However, such a solution was not easy to find. The lack of a common language and disparate architectures meant that creating a secure and seamless connection between blockchains was, and still is, a complex, time-consuming, and costly process. The risk of inadequate expertise and security protocols makes implementing such portals potentially risky.



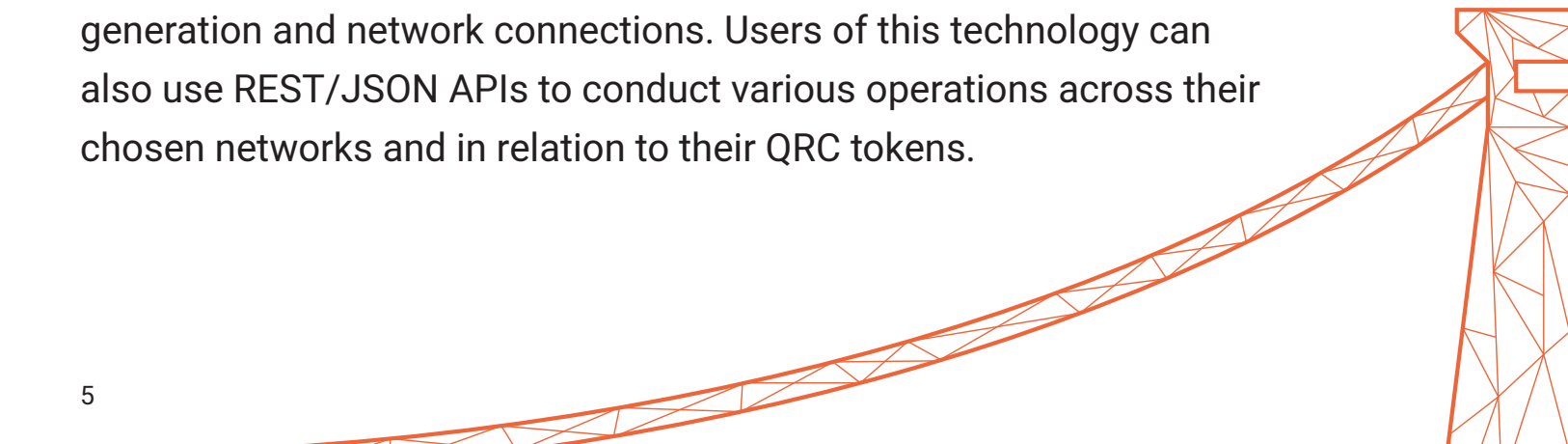
The journey to interoperability

Quant's founder, Gilbert Verdian, was among the first to recognise that blockchain interoperability would be a significant step forward, and the importance of standards. For this reason, in 2015, he spearheaded the Blockchain ISO Standard TC307, which has since become an international effort by 53 countries working together to standardise the technology.

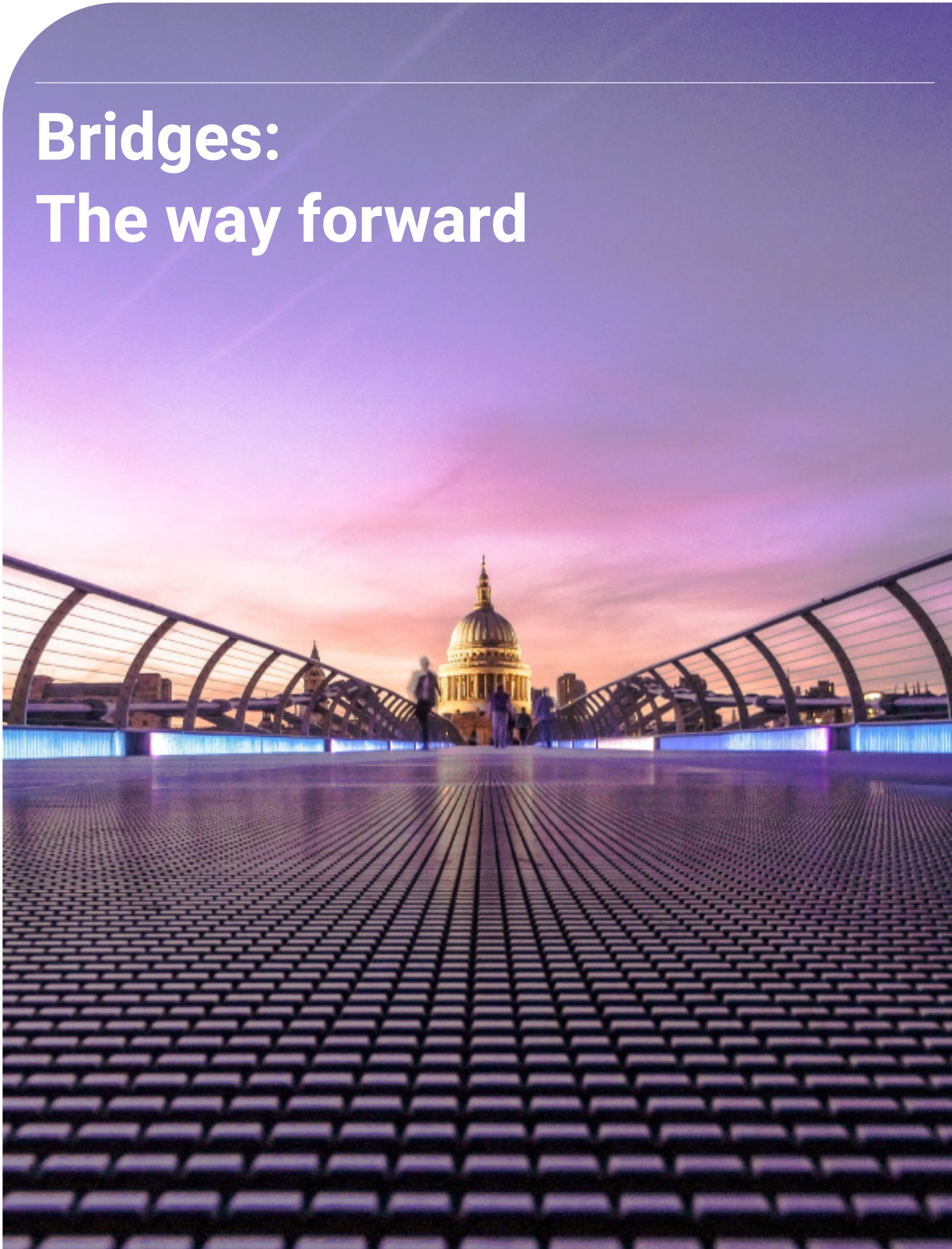
It was Gilbert's involvement with this initiative which gave rise to the concept of Overledger, the world's first blockchain-agnostic API gateway, and other Quant innovations, such as chain-agnostic smart contracts, called QRCs.

Based on Ethereum's ERC rules for fungible and non-fungible tokens, Quant's QRC smart contracts function like their Ethereum standard counterparts, but while ERC tokens are designed for deployment on the Ethereum network, QRC tokens are blockchain agnostic and work across multiple distributed ledger technologies. They can be implemented on public or private blockchains to enable complex operations between different distributed ledger technologies.

Today, Overledger is also offered as a platform, providing a simple user interface with preset attributes and functionality for smart contract generation and network connections. Users of this technology can also use REST/JSON APIs to conduct various operations across their chosen networks and in relation to their QRC tokens.



Bridges:
The way forward



Over recent years, the concept of the blockchain bridge – a connection that moves tokens from one blockchain to another – has emerged as another key component of interoperability. These work by moving a digital asset and its associated information – a token, stablecoin, cryptocurrency or NFT – from one blockchain to another.

All bridges are composed of off-chain services and on-chain elements. One way to build a bridge is for the bridge service to control one address on each blockchain. When a token is received by the 'exit' address on the origin blockchain, the bridge service uses its 'entrance' address on the destination blockchain to create a corresponding token.

Once the corresponding token has been created, depending on the features of the original token, it can either be deleted (burned) or kept in escrow while the corresponding token on the destination chain exists. If the original token remains in escrow, the bridge should allow owners of the corresponding token on the destination chain to reclaim the original tokens by trading in the duplicate version.

In this scenario, it is the bridge's responsibility to ensure that the corresponding tokens on the destination chain are backed 1:1 by the tokens in the escrow of the origin chain.

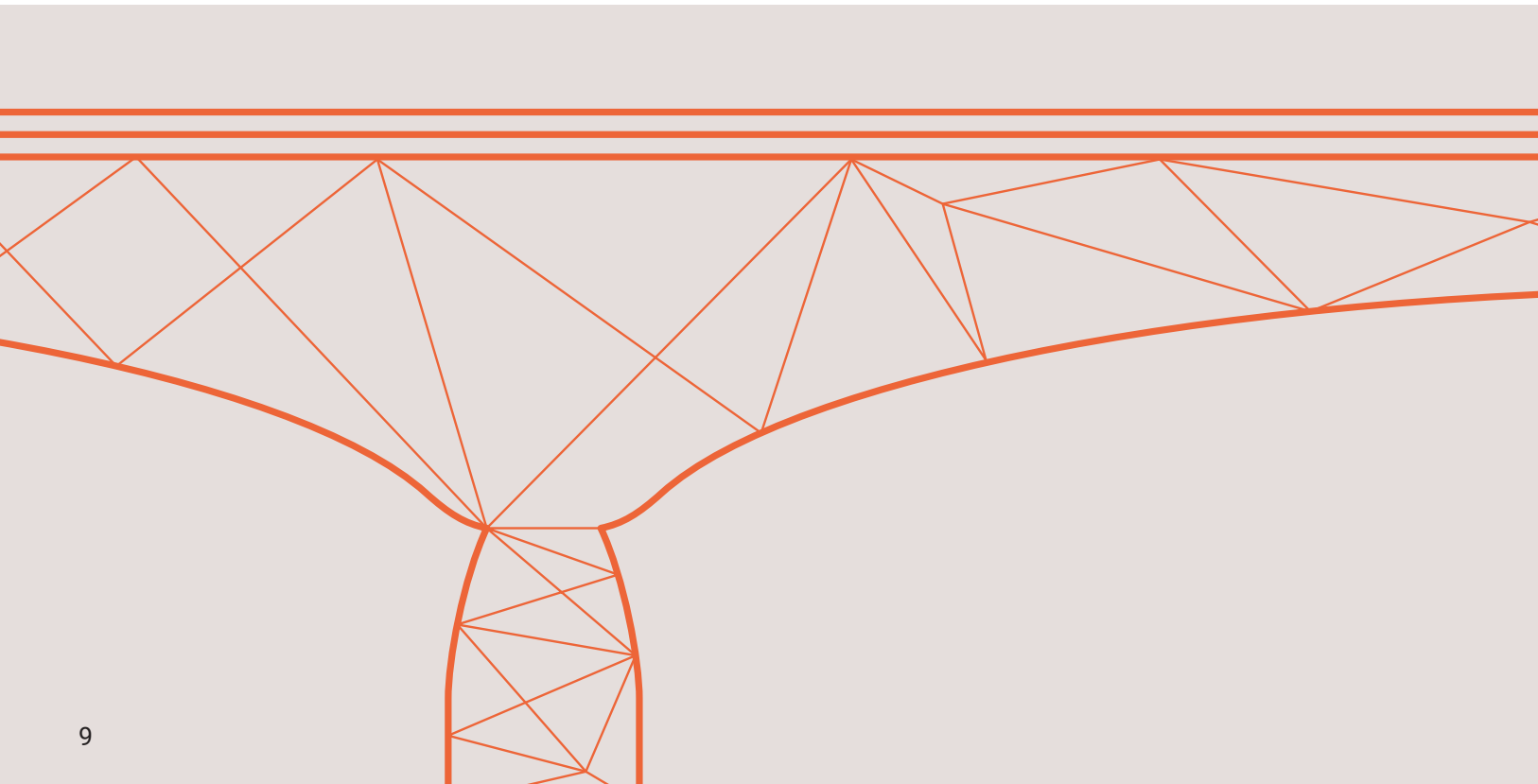
Bridges can use smart contracts (on networks that support them) in order to make their program logic more transparent. There are pros and cons to this approach. On the one hand, transparent code can increase trust in bridges, potentially even when the bridge service operators are anonymous. On the other, code deployed in smart contract form is difficult to upgrade, so any bug found by anyone (as the bridge code is now openly accessible) can be exploited immediately, potentially for large financial gain.

"The design choices of bridges depend on the type of asset they are intended to transfer, the network and security assumptions."

Ultimately, the design choices for bridges depend on a combination of factors, including the type of assets they are intended to transfer, which DLT networks they connect, and the trust and security assumptions in place. This last point raises a key question: are such bridges secure? And the answer is: 'they can be'. Consistently secure and easy-to-deploy blockchain bridges are available - and I'll explain those below – but first, let's look at the main approaches to bridge design.

Key bridge design considerations

There are several important issues to consider when designing a blockchain bridge.



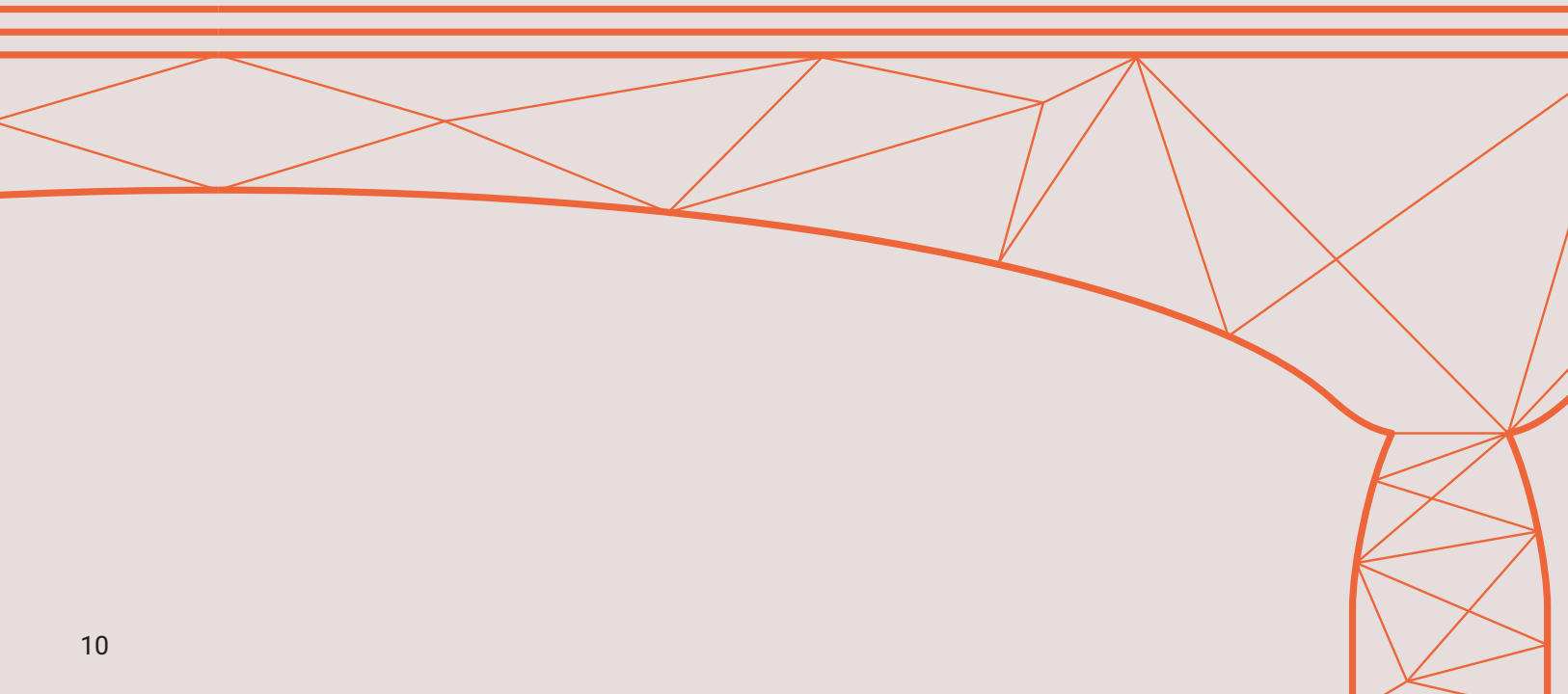
1 Bridge asset transfer flow

Before establishing a bridge, it is important to decide how to handle the tokens.

Two options are available: lock and mint flow, and burn and mint flow. The former requires the tokens to be kept in escrow on the origin chain while they exist on the destination chain, whereas the latter deletes them from the origin chain after adding them to the destination chain. Using a lock and mint flow approach is more complex and carries higher security risks, as the bridge must continually ensure a 1:1 peg of tokens in escrow and on the destination chain.

However, this technique may be necessary if the token on the origin chain cannot be replicated. Take, for example, a bridge moving a digital currency to another chain. This must deploy the lock and mint flow approach, as digital currency can only be created according to a strict algorithm unrelated to any bridges.

Given the security advantages of burn and mint flow, Quant recommends its use whenever possible.



2 Bridge ownership

A key secondary question is: who should be responsible for operating the bridge?

There are three options:

1. **A single organisation**
2. **Multiple organisations**
3. **Anyone**

When choosing a bridge design, it is important to consider the trust assumptions of its tokens. If the token has a function or action that can only be performed by a single organisation or a permissioned set of organisations, then a single or multiple organisational bridge would be appropriate. However, if the token in question has no particular whitelist for any function, then an open (permissionless) bridge, where anyone can join as an operator, is potentially more suitable. It is important to note, however, that permissionless bridges rely on game-theoretic incentives for correct behaviour, which usually requires economically rational users. Single or multi-organisational bridges, where you know the bridge operators, offer liability safeguards for users if an issue arises during a cross-chain transfer.

When choosing a bridge design, it is important to consider the trust assumptions of its tokens.

3 Bridge on-chain elements

Another major design issue is how to organise the bridge's on-chain elements.

For instance, should smart contracts be used or should the bridge use only private key-controlled addresses? In both cases, a related question is: should the bridge implement a multi- or threshold signature scheme (i.e. require multiple signatures from different entities before an action can take place)? This approach is commonly used when the bridge is controlled by multiple organisations, but it can also increase security when the bridge is controlled by a single organisation. In contrast, open bridges are not appropriate for multi-signature or threshold signature schemes, as it is usually impossible to identify all the parties operating the bridge.

Instead, open bridges include a 'challenge period'. Here, when one bridge operator claims that a cross-chain transfer request has occurred, and the related tokens need to be created on the destination chain, the other bridge operators are given a defined time period in which they can challenge that assumption before the actual transfer takes place.

Open bridges are not appropriate for multi-signature or threshold signature schemes, as it is usually impossible to identify all the parties.

Bridge risk

While there are several types of bridges, each with its own advantages and disadvantages, there is one common characteristic that all of them share: vulnerability.

At first glance, the idea that blockchains can be susceptible to attack may seem implausible. After all, DLTs – a family which includes blockchain – are inherently and exceptionally robust due to their distributed and decentralised nature. To perform a successful attack, you would need to strike most nodes on the network simultaneously (a so-called 'majority attack'). Because such hacks are usually (depending on network size) extremely costly, requiring a massive amount of energy and computational power on proof-of-work blockchain networks, they are generally unfeasible and very rare.

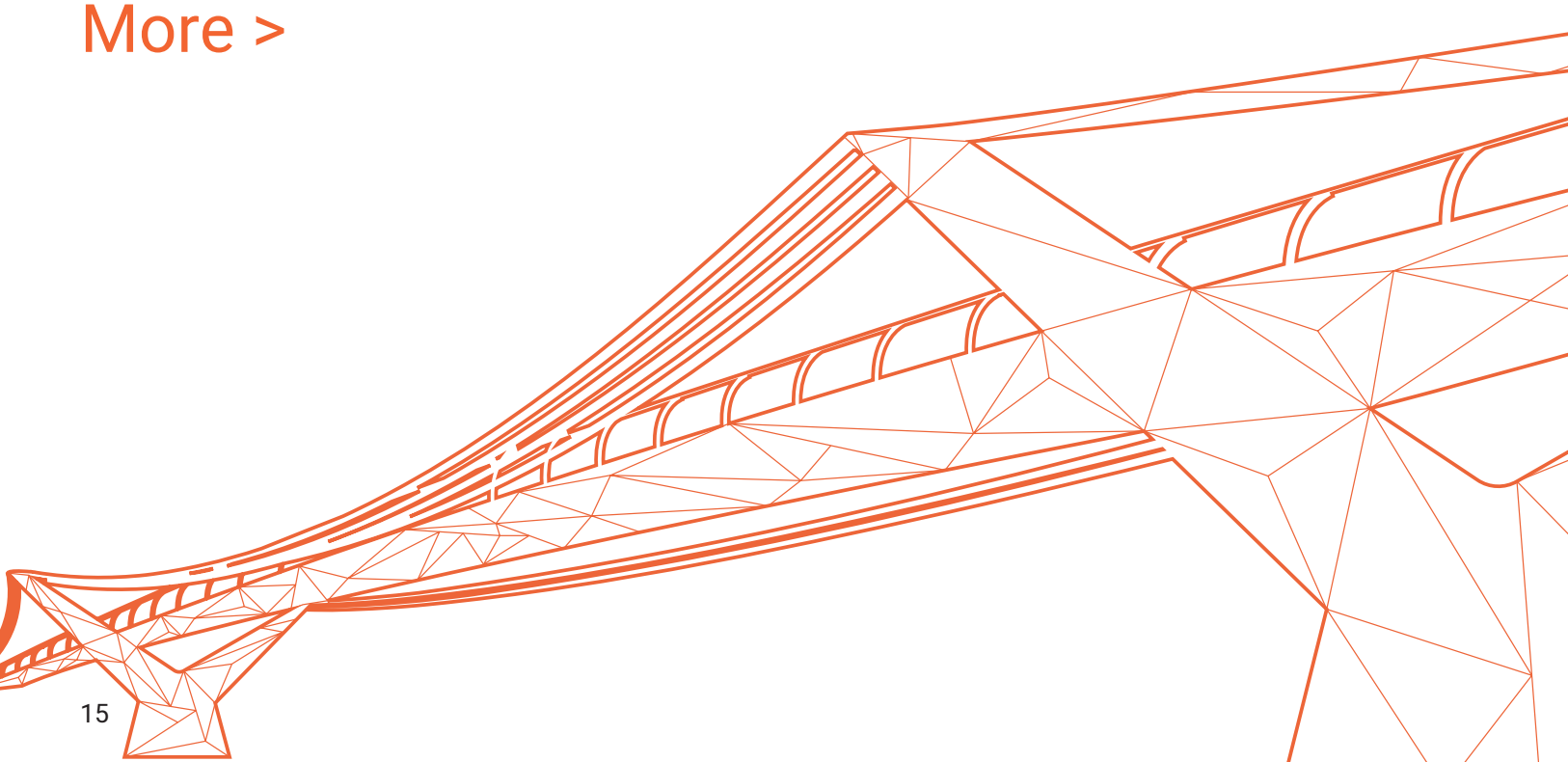
Bridge vulnerability exists because bridges have fewer participants and operators than major blockchain networks. This is most obvious where the bridge uses smart contracts as the code for them is often written by a small number of developers, and might not be thoroughly checked, tested or validated by experienced third-party experts, leaving its connected assets exposed to potential exploitation. The reality of this kind of threat was illustrated in February 2022, when an attack was made on the bridge between the Solana and Ethereum networks, resulting in a loss of about $375 million. Unfortunately, there are many other examples.

Overledger bridges

Overledger is the world's first blockchain platform that interconnects not only blockchains but also legacy networks to DLT and facilitates the creation of internet-scale multi-chain applications.

Overledger provides enterprise-grade security and an easy-to-use interface that enables users to issue, connect and monitor assets and develop applications on any blockchain without blockchain expertise.

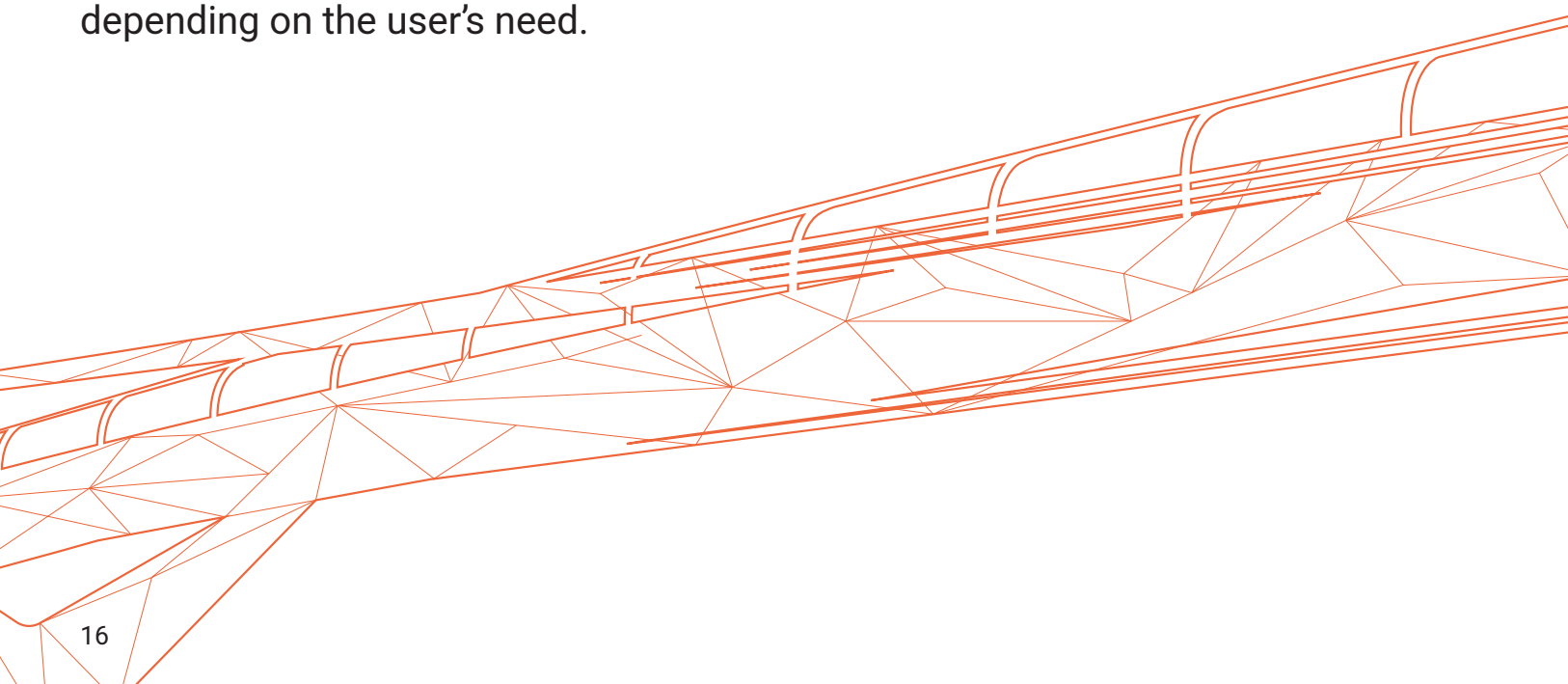
More >



There are several approaches to bridge design. For now, we will focus on one approach that is the basis of a proven bridging solution from Quant, developed in collaboration with the Internet Engineering Task Force and Massachusetts Institute of Technology. Offering a highly-secure way to connect blockchains, the secure asset transfer protocol bridge uses a standardised compliant interface and data model which eliminates the need to apply bespoke implementations for each DLT. This is thanks to each SATP bridge having gateways which are connected to the chosen DLT networks and open to interaction from its authorised users, directly and irrespective of the DLT being integrated.

The approach taken with these bridges is the burn and mint technique, briefly discussed earlier. As mentioned, this approach allows only one version of a token to exist at any time, as the token is burned on the origin chain and simultaneously minted on the destination chain. As no escrow address is required on the origin chain, it also removes the risk of the single storage of the funds being attacked by hackers.

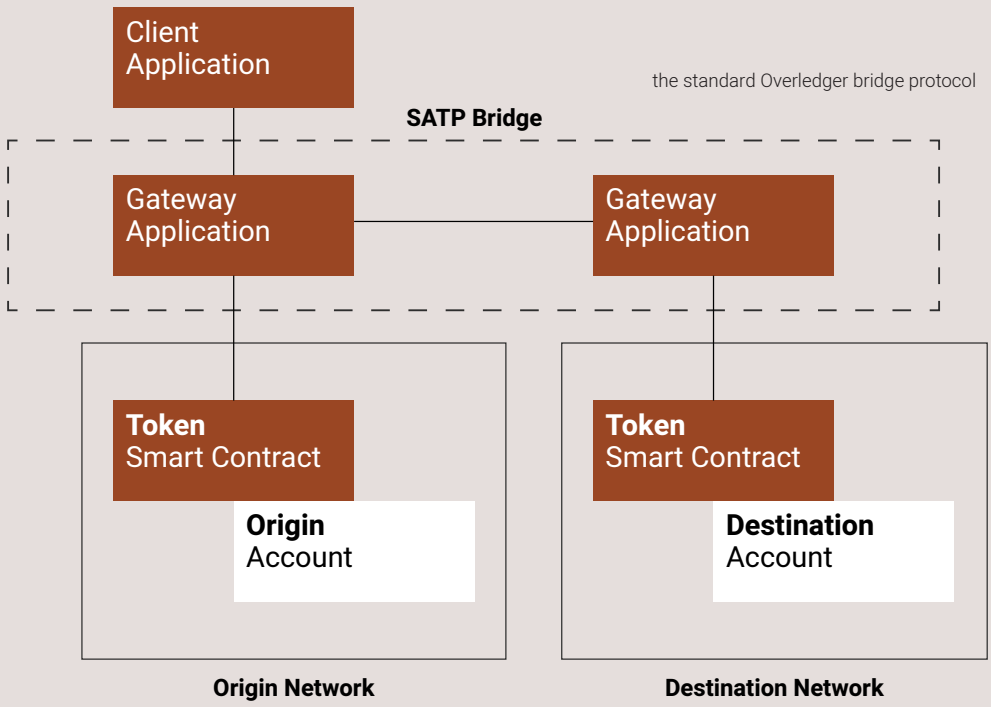
Overledger Platform deploys such bridges without smart contracts by default, but Overledger bridges can also be built with smart contracts, depending on the user's need.



Key characteristics of Overledger bridges

While burn and mint is a commonly-used approach to bridges, it is made particularly effective and easy to deploy through Overledger's pioneering and proven interoperability technology and underlying chain-agnostic smart contracts. The key characteristics of Overledger bridges are:

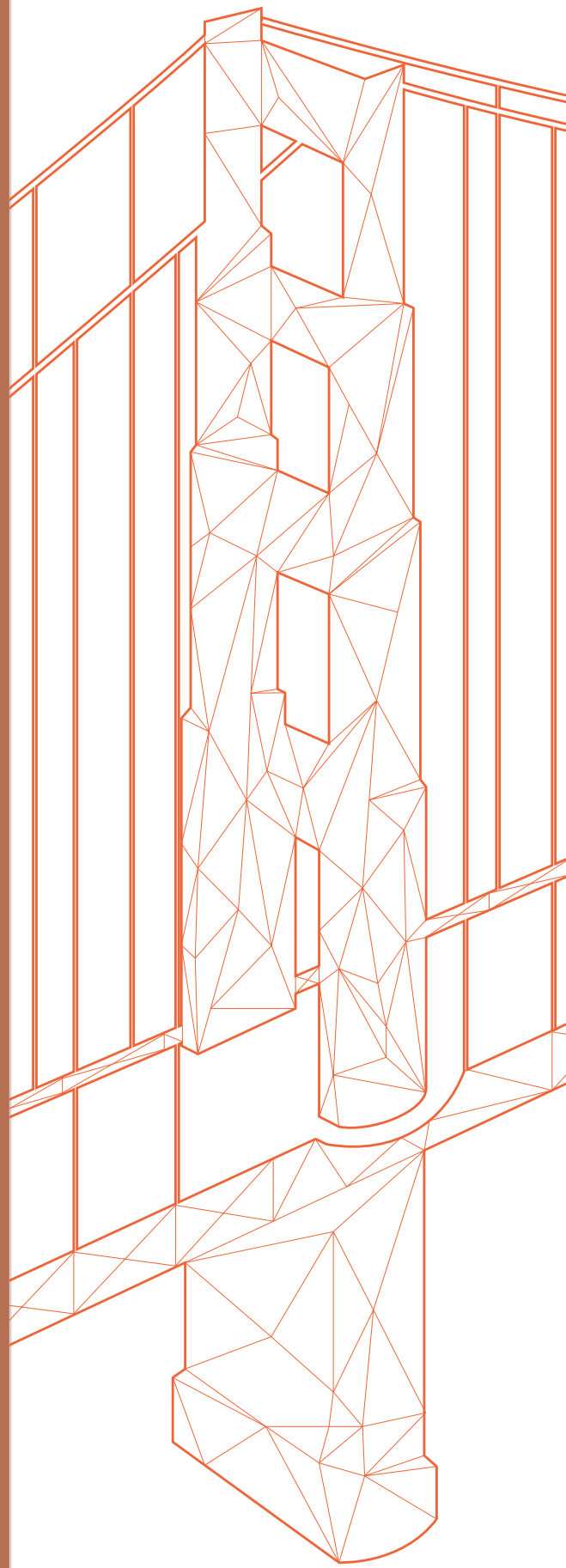
1. They work with different DLTs and networks.
2. They interact with Overledger APIs to provide a standardised gateway and messaging interface.
3. They offer atomic asset transfer, which avoids double spending.
4. They are auditable, allowing third-parties to verify when, where and by whom the asset transfer was initiated, as well as providing real-time confirmation of an asset transfer phase.



By combining the SATP approach with Overledger APIs, the generic interoperability aspect of SATP bridges has been expanded, providing standardised integration to popular blockchain networks for the creation of gateway applications that are agnostic to the underlying DLT.

The benefits of Overledger bridges

- **Interoperability:** Overledger provides channels for easy collaboration between financial institutions and clients.
- **Ease-of-use:** No need for expert blockchain developers. Overledger flows provide a code-free way of reducing friction and enabling new opportunities for innovation.
- **Security:** Overledger uses burn & mint design and a secure messaging protocol in addition to externally validating smart contracts.
- **Resilience:** Overledger bridges are built by experts led by a team with experience in critical national infrastructure and governments.
- **Programmable:** With expertly coded gateways, Overledger ensures the reliability and security of asset transfers.
- **Future-proof:** Overledger makes digital assets secure and fit for multiple blockchains, now and in the future.



The Overledger bridge flow

As a key feature of the Overledger Platform, the bridge flow is an easy-to-use user interface that generates interoperable assets, such as smart tokens and bridges. In the case of bridges, the connection between two networks can be created in minutes with little user input and zero coding.

Overledger bridges can be used to connect Quant Flex or Vari smart tokens to any chain for various use cases, including:

Digital currencies such as CBDCs and commercial stablecoins.

Alternative assets, carbon credits, funds and bonds.

Unique assets, such as collectables, vouchers and tokenised real state.

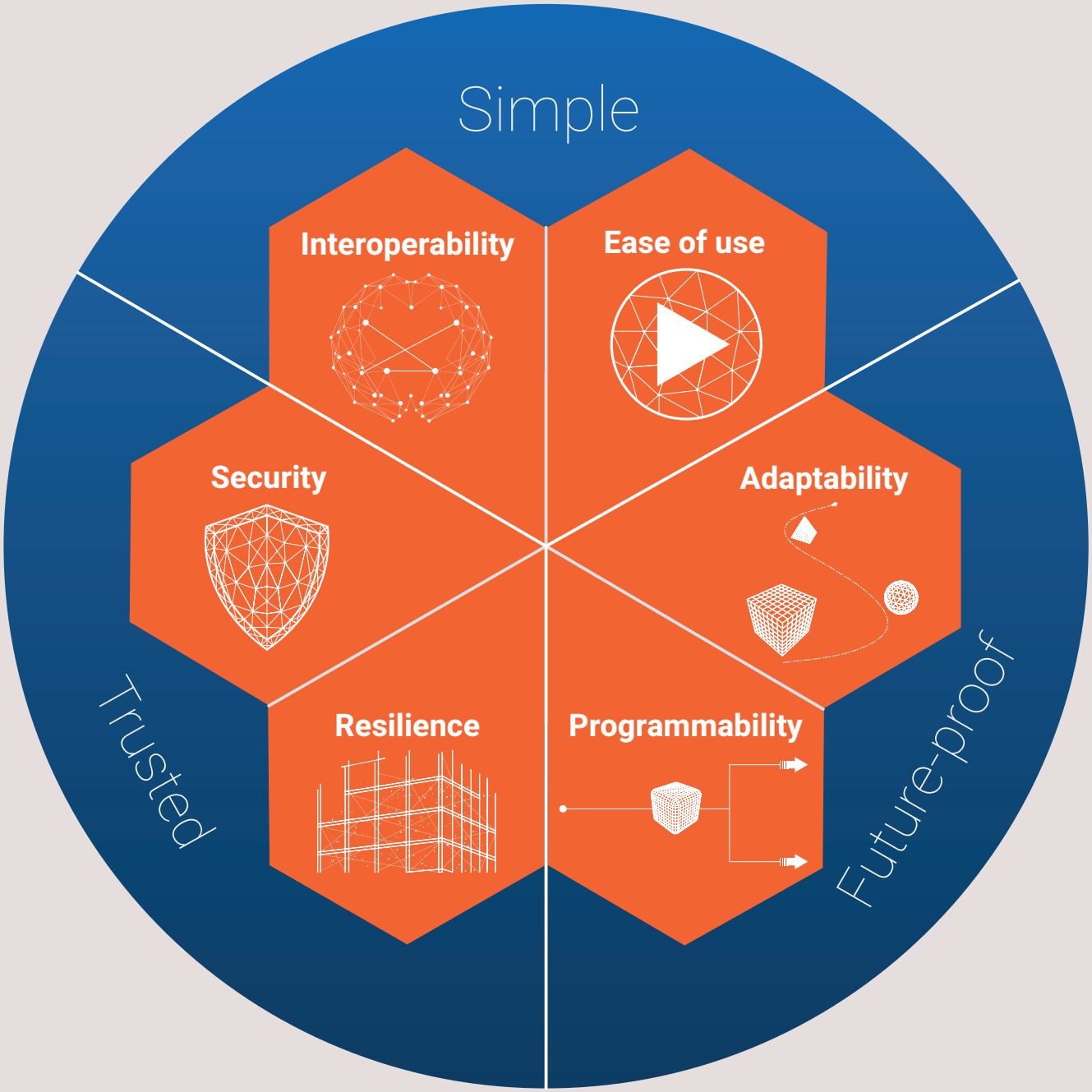
The Quant way forward

Bridges are a key component of DLT interoperability. Initially used for cross-chain asset transfers, they now have a growing role in cross-chain data transfer, as well as cross-chain asset exchange.

Quant is taking a long-term and business-focused view with its approach to bridges – we are confident that SATP bridges will greatly affect the market, particularly when linking two permissioned DLT networks (for use cases such as CBDCs or supply chain networks). This is because the limited number of organisations that can operate nodes in permissioned networks makes SATP bridges more impactful in this context. When connecting two permissioned DLT networks, for example, there might be no organisations running nodes in both networks (which is a requirement of a traditional bridge). And even if there are a small number of organisations running nodes in both networks, they might not be technically or legally able to run a bridge across both chains. With SATP bridges, however, any organisation connected to either network can be selected to run that side of the bridge, and the SAT protocol, in combination with legal agreements, can align both of these organisations to run the bridge correctly.

Furthermore, SATP bridges can also be effective in connecting two permissionless DLT networks or connecting a permissioned DLT network to a permissionless DLT network. This is because SATP bridges are a natural environment to enforce KYC and regulation, which may increasingly become a requirement in certain jurisdictions to protect users from issues such as bridge hacks or malicious actors.

Quant is leading the creation of the industry's best practice in interoperability with a development framework built around the following key pillars: making blockchain simple, ensuring trust, and preparing for the future. From these principles, come the elements of Quant's DNA.



1. Interoperability solved.

At Quant, we are working towards solving the issue of blockchain interoperability and creating networks that connect tokenised money, value and assets. To achieve this, we formed ISO/TC 307 and created Overledger, which is the first API gateway that enables legacy systems to access all blockchain networks.

2. Ease of use out of the box.

Overledger now underpins some of the world's most demanding blockchain-based use cases and is now offered as a SaaS enterprise-grade platform that is low-code and API-based. Overledger enables the building of applications in any mainstream coding language, the issuance of tokens and the creation of secure bridges across networks in minutes and with just a few clicks.

3. Security guaranteed.

Our CEO has over 20 years of cybersecurity experience, including government roles and private sector experience at Mastercard, Vocalink, and HSBC. At Quant, we prioritise security with tamper-proof smart contracts validated by third-party specialists.

4. Resilience by design.

We prioritise resilience in our technology to protect against risk, at the same time as helping our clients seize opportunities in a volatile world. Our leadership team has experience in financial services, enterprises, and government, understanding the needs of large, regulated businesses.

5. Programmability embedded.

Tokenised money offers granular control over its behaviour, allowing you to program your tokens to behave as desired even after deployment. This makes future money smarter, more useful, and more purposeful.

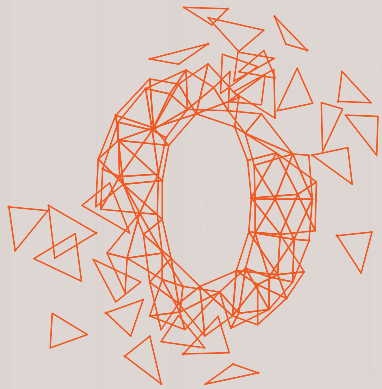
6. Adaptability built in.

Adaptability is a key element of our DNA because we know the digital asset you create, the blockchain you choose, and the smart contract you program today might no longer be a perfect fit in the future.

Further reading

- **The Bank of England**, April 2023: Innovation in payments and money by Sir Jon Cunliffe >
- **Boston Consulting Group**, August 2022: Relevance of on-chain asset tokenisation in 'crypto winter' >
- **Citi**, March 2023: Money, tokens and games >
- **CoinDesk**, April 2023: Tokenisation of real-world assets a key driver of digital asset adoption says Bank of America >
- **Finance Magnates**, May 2023: The potential of blockchain technology in revolutionising payment systems >
- **Investment Week**, May 2023: Tokenisation will revolutionise the 100-year-old fund structure says Calastone >
- **Ledger Insights**, May 2023: Brazilian CBDC to enable banks to tokenise balance sheets >
- **Mastercard**, Q2 2023: The future of payments >

Talk to one of our experts to discover the power of bridging with Quant and how Overledger can transform your business and help it thrive in the new blockchain economy.



QUANT

To learn more about Overledger, visit our website >

Contact us at GetOverledger@quant.network

The foundation of the blockchain economy.