A Future of Finance Round Table

The interoperability problem: how can it be solved?

In partnership with

kima

Future of Finance

Kima is a blockchain-based solution for facilitating value transfer transactions across disparate ecosystems by connecting multiple ledgers (public and private) and traditional bank accounts to settle transactions and transmit messages. Financial institutions and developers can embed Kima into their apps, providing users with a highly secure and capital-efficient way to seamlessly transfer assets across chains and interact with bank accounts. This approach addresses the interoperability and fragmentation challenges of financial apps. By efficiently and securely connecting ledgers and bank accounts, Kima eliminates the need to rely on smart contracts throughout the interoperability process, offering a new standard in financial transactions.

For more information, go to www.kima.finance.

The lack of interoperability between blockchain networks, and between blockchain networks and traditional financial markets, has emerged as one of the two main obstacles to the growth of tokenised assets in terms of both scale and scope. To improve understanding of the nature of the problem, and identify solutions, Kima Finance hosted a private discussion between ten industry experts representing the interests of regulators, banks, exchanges, financial market infrastructures and technology vendors. This is an edited account of the discussion.

Executive Summary / Key Points Discussed:

1. Interoperability Challenges:

The digital technology landscape is fragmented, with over 1,000 blockchain protocols and a plethora of digital assets, leading to significant market fragmentation. For digital asset investors, this fragmentation complicates asset portability and increases transaction costs.

2. Impact on Financial Markets:

Interoperability is crucial for enabling efficient transactions across multiple markets and asset classes. The current lack of interoperability hinders the diffusion of innovation and the development of network effects in tokenized asset markets.

3. Potential Solutions in the Industry:

Various technical solutions exist, such as bridges, swaps, sidechains, and API gateways, but they are often uncoordinated.

Unified ledgers, or common platforms, have emerged as promising long-term solutions, offering interoperability by design. These platforms would integrate different types of digital assets and facilitate seamless transactions.

4. Kima's Solutions:

Unified Interoperability Platform: Kima provides an API-based open protocol that facilitates value transfer transactions across disparate ecosystems. By connecting multiple ledgers (both public and private) and traditional bank accounts, Kima enables seamless transactions and message transmission.

Eliminating Smart Contract Reliance: Kima's architecture does not rely on smart contracts, which are often vulnerable to malicious attacks. Instead, it uses a secure and efficient method to connect ledgers and bank accounts, addressing the security and fragmentation challenges of financial applications.

Capital Efficiency and Security: Financial institutions and developers can easily embed Kima into their applications, offering users a highly secure and capital-efficient way to transfer assets across chains and interact with bank accounts.

5. Regulatory and Governance Considerations:

Direct regulatory intervention to impose interoperability standards is unlikely. Unified ledgers pose complex technical and governance challenges that need to be resolved for successful implementation.

6. Market Dynamics:

A transition period with multiple coexisting interoperability solutions is expected. The development of open protocol networks akin to existing Internet protocols (e.g., TCP/IP) could provide a radical solution, though regulated institutions may struggle with trust in such systems.

Digital technology has low barriers to entry. Any developer with a laptop and access to GitHub can write and distribute an application through the Internet. So it is not surprising that companies, technologies and versions of technologies proliferate in computing at a rate that would be uneconomic in any physical industry.

As a computing and Internet technology, blockchain is no exception to this relatively low cost of investment. There are more than 1,000 distinct layer one blockchain protocols in existence. These host an even wider variety of digital assets. On 24 July 2024, Coinmarketcap recorded 10,011 separate coins and utility tokens traded on 705 separate spot exchanges. There are another 108 cryptocurrency derivative exchanges. The numbers of instruments and exchanges increase all the time.

For investors, interoperability means portability

For investors in digital assets, even these ever-rising numbers under-estimate the fragmentation of the markets they confront. They must consider not only centralised and decentralised cryptocurrency and utility token exchanges and derivatives exchanges, but traditional assets traded on stock exchanges and fixed income trading platforms, the long-established futures and options exchanges and the new breed of specialist security and fund tokens exchanges that have emerged around the world.

Even the simplest investment strategy ("buy cheap, sell dear") depends on the ability to transact efficiently across multiple markets and asset classes. Investors need to move funds seamlessly between digital and traditional asset classes, creating alpha by selling over-valued assets and buying under-valued ones, and using one set of assets to collateralise exposures to another.

In short, investors need cash and financial assets to be portable. Operationally, that portability depends on the ability to exchange data about the assets using common data formats and communication protocols.

For investors, low friction data exchange is what interoperability means. Most industries meet the data exchange challenge by universal adoption of uniform standards. Shipping container standards (ISO standard 55.180.10) that specify the height, width and length of a container, so they can be locked together on a ship and transported on a lorry, are the classic example.

Digitalised financial markets have developed such standards, but they are fragmented between the back office (SWIFT), the front office (FIX) and the derivatives markets (FpML). These functional and asset class silos are exacerbated by digital technology vendors, now including blockchain vendors, that try to take ownership of a market by creating proprietary standards that make it

difficult for other companies in the industry to compete for their customers and take a share of the value they create.

Interoperability is a new version of an old problem

This multiplication of blockchain protocols is entirely consistent with the history of digital technology since the 1980s. It was then that the vertically integrated model of computing – in which processors, memory, software, hardware and even maintenance were sold as single, integrated packages – broke down. Technology vendors started to specialise in operating systems, databases, storage and other functionalities. Specialised applications replaced integrated systems.

Ever since, buyers of digital technology applications have wrestled with a dilemma. Either they must integrate the various applications themselves or they must purchase an integration product or service from a third party.

But integrating applications within a firm is only one aspect of the problem. The need for interoperability between firms, and between firms active in financial markets reliant on digital technology, is a variant of this fundamental structural feature of the modern computing industry.

To trade, settle and safekeep assets in financial markets, banks, brokers and asset managers need to exchange the data they have stored in their proprietary computer systems about the same assets and transactions. To settle purchases and sales, the various parties must agree that a purchase and sale has taken place.

Blockchain protocols are building new market and asset class silos

One of the principal claims of blockchain technology is that it can eliminate this process of "reconciliation" by sharing a single set of information with all parties to a transaction. Ironically, however, blockchain technology has instead reproduced the silos of traditional digital technologies. For example, to trade a token issued on Ethereum, or use an application hosted on Ethereum, it is necessary to join the Ethereum system. The same is true of other blockchain protocols.

This lack of interoperability between blockchain protocols limits the diffusion of innovations. Developers use smart contracts to execute the workflows that turn ideas into new products and services, but a smart contract that works on one blockchain protocol will not necessarily interact successfully with a smart contract on another blockchain protocol. To be fully composable, smart contracts need to be interoperable.

These limitations place significant constraints on the ability of digital or tokenised asset markets to extend their scope and scale, by trapping activity (including innovation) in closed networks and making it difficult for network effects to develop.

Token innovation, issuance and trading activity is taking place in isolated pockets. This makes it difficult for investors to support new products and services and, in most cases, even buy or sell a digital asset at all without affecting its price. This is a consequence of the fragmentation of liquidity between silos.

These siloes have developed for hard commercial reasons. Developers of blockchain protocols want to capture all the value they create for themselves, in the same way that the centralised platform technologies that emerged from the Dot Com era at the turn of the century – Amazon, Facebook (Meta), Netflix, Spotify, Apple, Google and Roblox - monopolise (or "oligopolise") on-line retailing, social media, streaming, apps, search and gaming.

Traditional financial institutions have endorsed this effect by building closed blockchain networks of their own. Both investment and custodian banks have built tokenisation platforms designed to protect their existing client bases from erosion by competitors. Regulators – in the United States at least – have strengthened this by discouraging banks from launching or participating in public blockchains that are open to all-comers.

The fragmentation of blockchain-based markets is unlikely to persist

This balkanised environment represents a convenient alliance of public and private interests, but it may prove unstable. Certainly, value in Web 2.0 (which is characterised by closed platforms owned by firms that monetise data) accrued to centralised platforms. But value in Web 3.0 (which is premised on open platforms owned by users trading peer-to-peer) cannot obviously follow the same path. In principle, value in Web 3.0 should accrue to the services, such as wallet providers or exchanges or custodians, that support open, decentralised networks that scale and expand their scope precisely because they are open and decentralised.

This implies that interoperability must occur eventually at the network level, because networks cannot scale and expand their scope without interoperability, and without scale and scope they cannot generate value.

That interoperability will generate value is evident already in one of the few blockchain projects to have delivered a return. By making its tokenised deposit available as a settlement asset on the Broadridge distributed ledger repo (DLR) platform, J.P. Morgan effectively made a blockchain platform interoperable with traditional asset markets and payments systems, generating measurable capital and liquidity savings for users of the services.

Buy-side firms – whose engagement with tokenised assets is crucial to growth – are reinforcing the case for interoperability. At present, asset managers are obliged to interact with separate infrastructures for traditional and digital assets. Connectivity between digital and traditional markets, even via standardised application programme interfaces (APIs) designed specifically to facilitate the exchange of data between systems, is complicated and expensive.

These costs are amplified by the lack of interoperability between the token markets and the cash markets. Tokens are bought and sold for cash, and fiat currency is not yet available on blockchain networks.

As a result, payment versus payment in fiat currency or delivery of tokens versus payment in fiat currency is impossible. The lack of fiat currencies in digital form on blockchain means that less-than-satisfactory alternatives, such as Stablecoins, must be used as cash substitutes to move between networks.

For as long as issuers of tokens and investors in tokens are obliged to maintain dual infrastructures and use traditional payment systems to receive or pay cash, the frictional costs of transferring

value on blockchain networks will inhibit adoption of tokens. Interoperability is the obvious solution, and asset managers are looking to technology vendors and service providers to deliver it.

Solutions to the lack of interoperability include technical workarounds as well as technical standards

A range of technical solutions to the lack of interoperability are now available. They include "bridges" (in which digital assets can be "minted" or "locked" on one blockchain and "burned" or "unlocked" on another), "swaps" (in which digital assets are exchanged via automated market-makers, or AMMs), "sidechains" (bi-lateral links between blockchains), cross-chain communication protocols ("routers" or "connectors") and abstraction layers and API "gateways" that enable legacy systems to communicate with blockchain networks as well as blockchain networks with each other.

A number of initiatives are also under way to devise digital data and communications standards for the blockchain industry. The most ambitious follow the established path of inviting the various parts of the industry to agree a sets of standard data formats and communication protocols and then press for their adoption throughout the industry.

As in other industries, this work is taking place under the auspices of the International Organisation for Standardisation (ISO), whose Technical Committee 307 (ISO/TC307) is working on the standardisation of various aspects of blockchain technology, including an interoperability framework.[1]

Many other bodies are engaged in similar work. In fact, the Global Blockchain Council has identified 63 separate organisations engaged with the development of technical standards for blockchain.

Among the most important is the Internet Engineering Task Force (IETF), the body for responsible for developing standards for the Internet, because blockchain is an Internet technology.

A technical working group of the IETF is developing, among other things, a base architecture and protocol for secure asset transfers between nodes on the Internet (a Secure Asset Transfer Protocol, or SATP), for which blockchain networks are the principal use case.

Simultaneously, the International Token Standardisation Association (ITSA) is developing the International Token Identification Number (ITIN), a token equivalent of the International Securities Identification Number (ISIN) to identify tokens wherever they trade. ITSA is also working on an

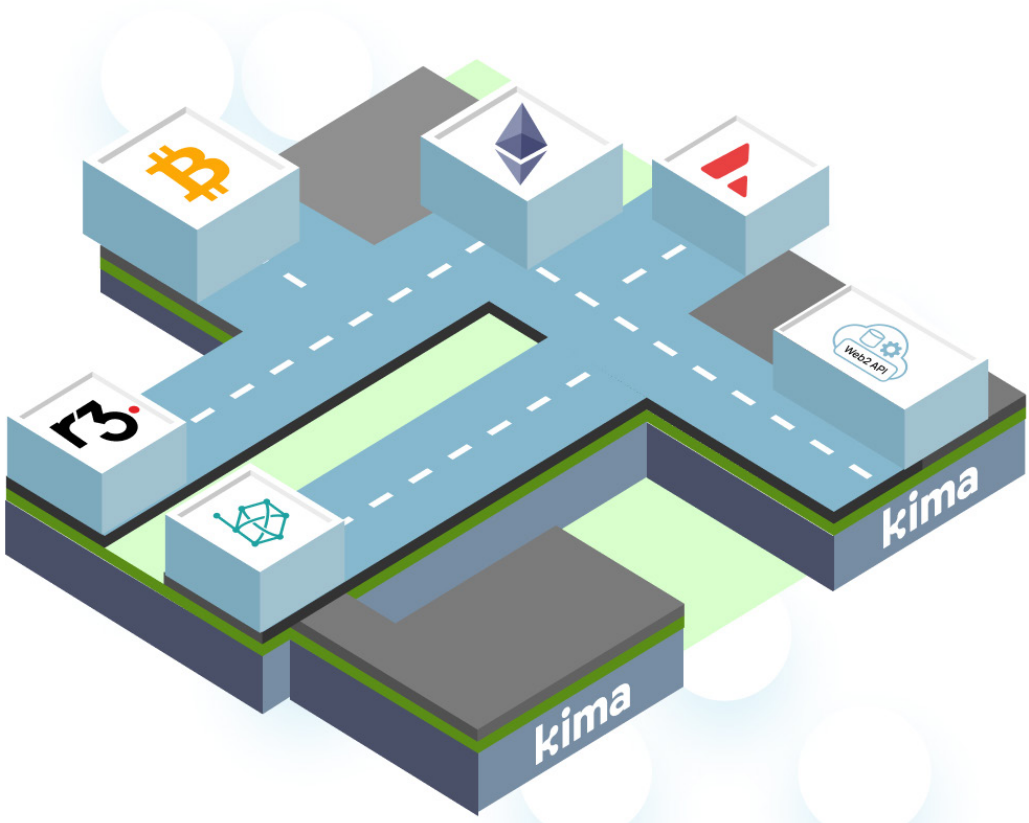
1. https://gbbcouncil.org/gsmi/technical-standards/

International Token Classification (ITC) framework for classifying tokens by their economic, technological and legal characteristics.

The World Wide Web Consortium (W3C) has set up a Blockchain Community Group to develop message format standards for blockchain based on ISO20022, the common data standards for financial messages developed by ISO Technical Committee 68 (TC 68).

These initiatives have similar methods and objectives but are not well coordinated. Indeed, the proliferation of interoperability methods is at risk of creating a lack of interoperability between interoperability solutions.

This lack of consistency might appear to argue for the more rigorous application of standards. But standards themselves have, as the experience of traditional financial markets proves repeatedly, a tendency to proliferate.



Neither regulation nor financial incentives can overcome the interoperability conundrum

Which is why some market participants argue for regulatory intervention to impose a single global standard, or at least a set of global standards that are compatible with functional or local variations. However, neither global nor national regulators are likely to regard mandatory adoption of a particular set of standards as a viable solution.

What central banks and financial market infrastructures (FMIs) can do is encourage adoption by using particular standards themselves, which then become the easiest way of interacting with the central bank or FMI. Even then, there will be resistance on grounds of cost, as SWIFT has found with the ISO 20022 standard. This is already obliging FMIs to continue to support previous versions of standards.

This disappointing experience has persuaded some market participants to conclude that any interoperability scheme that necessitates the replacement of existing methods of data exchange is bound to fail. Logically, adoption will always be deferred if the costs and risk of change appear to outweigh the benefits, and any innovation that requires wholesale changes to existing systems will fail that test.

This presents advocates of interoperability with a chicken-and-egg conundrum. The benefits of interoperability depend on scaling and scope expansion through network effects, which in turn depend on interoperability. By definition, the benefits of scalability, expansion of scope and network effects cannot be captured by a single company.

For example, individual banks have proved that they can generate internal economies by using tokenised deposits to settle payments in-house between corporate clients. But the real value of using tokenised deposits depends on inter-operability.

If banks can exchange tokenised deposits issued by another bank for tokens of their own, clients of one bank could pay clients of another bank using tokenised deposits. Tokenised deposits would take off as a method of payment, central banks could settle net token balances between banks in central bank money the same way that they settle net payments balances between banks today, and all banks and their customers would benefit.

In principle, this model of interoperability can be extended to cross-border as well as domestic payments. Indeed, the Bank for International Settlements (BIS) has already completed one project (Project Mariana) and is leading another (Project Agorá) to explore how tokenised commercial bank

deposits can be integrated with tokenised central bank money to make wholesale cross-border payments faster and cheaper.

A unified ledger may be the best solution to the problem of interoperability

Importantly, Project Agorá aims to build on the "unified ledger" or "common platform" concept proposed by the BIS in June 2023.[2] This envisaged a new type of FMI that combines central bank money and tokenised commercial deposits and other types of privately issued and managed tokenised assets (such as security tokens and tokenised funds) and uses APIs to link multiple ledgers into a single "programmable platform."

Project Agorá is not the only initiative that is developing the idea of a "unified ledger" or "common platform." The International Monetary Fund (IMF) has endorsed the idea of X-C, a multi-currency programmable platform for settling cross-border transactions.[3]

The Monetary Authority of Singapore (MAS) has published, in conjunction with five commercial banks, an outline of a "global layer one" FMI, shared by banks, that would host interoperable tokenised asset applications, smart contracts and digital identities. [4]

The Regulated Liability Network (RLN), originally conceived by a group of industry practitioners, also proposes a shared blockchain infrastructure.[5]

Unified ledgers or common platforms of this kind offer interoperability by design. In other words, all forms of digital money and digital assets, all forms of transfer of value, all types of digital wallets in which assets are stored, and all the applications by which digital assets are staked or lent or borrowed, would conform to a common data model.

Effectively, common platforms promise interoperability through the standardisation of token issuance, trading, safekeeping and servicing.

2. "Blueprint for the future monetary system: improving the old, enabling the new," in Bank for International Settlements, Annual Economic Report, 20 June 2023, pages 85-118.

3. International Monetary Fund, A Multi-Currency Exchange and Contracting Platform, by Tobias Adrian, Federico Grinberg, Tommaso Mancini Griffoli, Robert M. Townsend and Nicolas Zhang, 4 November 2022.

4. GL1, Global Layer One: Foundation Layer for Financial Networks, June 2024.

5. The Regulated Liability Network: Digital Sovereign Currency, White Paper, 15 November 2022.

This is what Ethereum offers already, and it is why the Ethereum protocol currently dominates token issuance and trading. But Ethereum remains a privately owned silo without access to central bank money and the trust in central bank money that reassures banks, brokers and asset managers that it is safe to participate in the token markets. A public version, underpinned by central bank money, would overcome those limitations. However, a shared public blockchain infrastructure must overcome several challenges.

Technical, ownership and governance challenges posed by unified ledgers

The first is technical. Because blockchains are not just ledgers but virtual computers, unifying ledgers means verifying the "state" (the information stored in the memory of the computer) of the decentralised computers that make up the blockchain network.

In practice, a "unified ledger" based on blockchain technology will rely on the blockchain to aggregate the "blocks" of data from the decentralised computers and resolve any discrepancies between the blocks to present the true "state" of the various ledgers.

Technically, this is different from the reconciliation of data between the different systems controlled by market participants. Blockchain is a mechanism for resolving data discrepancies automatically, instead

of using back-and-forth messages to reconcile the discrepancies. Regulated financial institutions such as banks are uncomfortable with the loss of control over data that reliance on blockchain implies.

Which is why the second challenge unified ledgers must overcome is how they are governed. The preference of regulated financial institutions for private or permissioned blockchains is obviously incompatible with a shared public infrastructure. So it is not surprising that public institutions, such as the BIS, the IMF and the MAS, have led discussions about the idea of a unified ledger. Even the RLN, though it is conceived and led by private sector institutions, has involved central banks as observers and participants.

The case for public sector involvement is strongest in cases of market failure, and the inability of market forces to increase the scale and scope of tokenisation can be read as an argument for public action.

In one field where blockchain technology is being tested – namely, cross-border payments – regulators have already identified the relatively high costs, slow speeds, lack of transparency and limited access to services as symptoms of market failure. It is reasonable to conclude that the development of unified ledgers will also be driven by the public sector.

Several existing ownership and governance structures provide precedents. A number of FMIs, in both the payments and securities markets, have divided ownership of an infrastructure from its operation. CLS, a limited purpose bank for settling foreign exchange transactions set up by central banks after the market failed to resolve Herstatt Risk, offers another model. It is owned by 69 banks but regulated separately by the Federal Reserve. Fnality, a blockchain-based infrastructure that uses tokenised cash to settle transactions, is owned by 20 regulated financial institutions but is led by independent management.

The radical option of relying on open protocol networks

A radical option is to dismiss ownership and governance questions as irrelevant to blockchain networks. Blockchain can be seen as a protocol network akin to email (where the Simple Mail Transfer Protocol (SMTP) provides the standard for exchanging emails) or the worldwide web (where the Hypertext Transfer Protocol (HTTP) renders websites) or the Internet (where the Transmission Control Protocol/Internet Protocol (TCP/IP) provide the rules and procedures to connect devices).

The SMTP, HTTP and TCP/IP protocols are free to use, not owned or governed by any one firm or organisation and, above all, generate network effects of the kind tokenisation requires to scale. In theory, a blockchain protocol that stored value and used smart contracts to transfer value could operate in a similar ungoverned and unowned way and generate similar network effects because anybody who complied with the protocol could communicate with anybody else who complied with the protocol.A suggestive analogue exists already. The Byzantine fault tolerant (BFT) consensus algorithms in blockchain networks that blockchains use to achieve consensus on the validity of transactions continue to operate even if some of the nodes in the network are faulty or malicious. BFT algorithms are not regulated, owned or governed by anybody but can be implemented by anybody. Users who want to join a blockchain network where BFT algorithms are used simply implement the protocol.

Unfortunately, regulated institutions are likely to struggle to trust self-governing systems of this kind, especially if counterparts were not subject to KYC checks. But the principal objection to self-governing protocols is that they are unlikely to emerge from the present dispensation.

Protocols such as SMPT and TCP/IP work because they focus on narrow areas that are not subject to competition. The siloed but competing nature of blockchain protocols today is an unpromising environment in which to develop open protocols for tokens.

However, the idea of complying with a set of rules and being able to communicate with anybody else who complies with the same set of rules, can be rescued. Kima Network provides a service by which native assets on any blockchain network can be abstracted to the Cloud. This enables native assets, which exist only as data objects on a blockchain, to move between otherwise closed networks. Customers of the service need only comply with the rules of the Kima Cloud, in the same way as users of the Internet comply with the TCP/IP protocol.

Conclusion

There is an urgent need to solve the lack of interoperability between blockchains and between blockchains and traditional markets because it is – along with the absence of fiat currency on-chain in digital form - one of the two main obstacles to the growth of the token markets. As long as the token markets are limited in scope and scale, issuers and investors will be denied the lower costs and higher returns that tokenisation promises.

Technical workarounds are available. Multiple bodies are working on the standardisation of the technical means by which data is exchanged. But interoperability is more than a technical issue. It encompasses regulatory and legal issues too. The cryptography behind digital wallets, for example, is open source and so publicly available, but cryptography standards vary between jurisdictions.

Unified ledgers, which have emerged as the most promising long-term solution to the lack of interoperability, are posing questions of ownership and governance to which the solutions are not yet obvious.

Even if those questions are resolved, it will take time for unified ledgers to be built and start operating. So the token industry faces a long transition, in which multiple interoperability solutions will co-exist. These solutions must themselves interoperate, and in ways that solve present problems without compromising the ideal future state.

Transitions of this kind require institutions to change. If they change at different speeds, that will likely make the problem of interoperability worse in the short term. Some market participants and their customers are bound to attach a higher value to friction than to interoperability.

Regulators will see some benefits in lack of interoperability. After all, if every asset can inter-operate seamlessly with every other asset, it will create new risks to financial stability, and foster demand for circuit-breakers that suppress interoperability.

If progress towards interoperability does prove to be slow, it will be worth remembering two things. First, that interoperability is important only because valuable propositions have emerged and matured, and their owners recognise they now need interoperability to scale.

Secondly, that interoperability is about innovation as well as expanding scale and extending scope. It is already uncovering new value propositions, such as cheaper and faster cross-border payments, and will unveil more that are presently regarded as too hard to solve or altogether invisible.

Summary of Key Points

- The low investment costs associated with digital technology and the Internet create a structural bias to fragmentation, from which blockchain suffers.
- Fragmentation inhibits the growth of scale and scope in tokenised assets issued on to blockchains because liquidity is low and transaction costs are high.
- Despite its claims to eliminate data reconciliation processes, blockchain in finance has followed traditional finance in trapping activity in closed siloes.
- The siloes are unlikely to endure, because the creation of value depends on network effects, which in turn depend on interoperability.
- The reluctance of asset managers to bear the cost of interacting with multiple infrastructures is increasing the pressure for interoperability solutions.
- Technical solutions and standards initiatives are numerous and poorly coordinated, risking a lack of interoperability between interoperability solutions.
- Direct regulatory intervention to impose interoperability standards is superficially appealing but unlikely to happen.
- Interoperability is trapped in a loop, in which the adoption of interoperability depends on network effects, which depend on interoperability.
- The introduction by public initiative of unified ledgers that solve the market failure through interoperability by design are the most promising path forward.
- Unified ledgers pose complex questions of technical operation and ownership and governance that must be solved before they can be successful.
- A radical alternative to unified ledgers is to rely on the emergence of an open protocol network akin to the TCP/IP and SMTP protocols.
- A compromise is an abstraction layer for digital assets on different blockchain protocols, accessible by anybody who complies with a set of rules.
- Although interoperability is needed urgently to secure the benefits of tokenisation, regulators will continue to attach importance to friction.
- Multiple solutions will coexist throughout a lengthy transition, creating a need for interoperability between interoperability solutions.
- Interoperability matters because valuable propositions exist already and need to scale and because interoperability will in time uncover still more.


Future of
Finance