OMFIF
Public Blockchain
WORKING GROUP

Driving public blockchain integration in banking

Evolving from experimental infrastructure into viable components of the financial system

APTOS Hedera MINSAIT ripple Stellar

OMFIF
Public Blockchain
WORKING GROUP

OMFIF

Official Monetary and Financial Institutions Forum
6-9 Snow Hill, London, EC1A 2AY
T: +44 (0)20 700 27898

enquiries@omfif.org

omfif.org

ABOUT OMFIF

With a presence in London, Washington and New York, OMFIF is an independent forum for central banking, economic policy and public investment – a neutral platform for best practice in worldwide public-private sector exchanges.

AUTHOR

Lewis McLellan, Head of Content, Digital Monetary Institute

OMFIF PROJECT TEAM

Sarah Moloney, Editorial Director

Simon Hadley, Director of Production and Development Planning

Janan Jama, Content Editor

Ophelia Mather, Marketing Coordinator

Ben Rands, Director of Operations and Marketing

DIGITAL MONETARY INSTITUTE

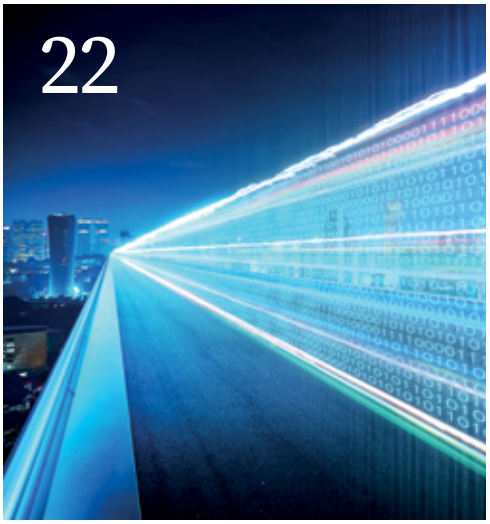
Katie-Ann Wilson, Managing Director

John Orchard, Chairman

Folusho Olutosin, Commercial Director

Max Steadman, Senior Programme Manager

Contents



Summit, In person, London, 19-20 May 2026

The Digital money summit 2026 represents an unparalleled opportunity for stakeholders across government, central banking, financial services and technology to connect and collaborate. Together, we will capitalise on innovations in digital money and push the industry towards practical actions for an inclusive, secure and regulated digital financial future.

OMFIF
DIGITAL MONEY
SUMMIT 2026

GET TICKETS

Constructing a consensus on blockchain

A shared understanding between technologists, financial services professionals and regulators is crucial to develop an innovation-forward policy framework that also protects the integrity of financial markets.

By Lewis McLellan, Head of Content, Digital Monetary Institute at OMFIF.

THE bitcoin blockchain is more than 15 years old and the application of the underlying technology to the world of finance has been widely discussed for well over a decade. While adoption is growing, blockchain has not yet been widely integrated. Its proponents have been advocating that, as well as allowing the introduction of new asset classes, blockchain can provide a new infrastructure for traditional financial instruments.

In that context, experts have argued that using blockchain-based tokens representing TradFi instruments – tokenisation – will improve settlement speed, reduce counterparty risk and enable programmable liquidity management. This process has already begun, with investment funds creating tokens representing ownership of their funds and others issuing tokenised bonds and other securities.

Tokenisation of capital markets and real-world assets is, as yet, small business, but it is set to grow rapidly, with McKinsey forecasting between $1.9tn and $4tn by 2030, Citi predicting $4tn-$5tn and Boston Consulting Group expecting $9.4tn.

However, the complex regulatory frameworks under which banks operate mean that they face challenges in adopting blockchain technology that other market participants do not. Banks are at the heart of the financial system and, until they can offer the suite of capital markets services that make them such important facilitators, the market for blockchain-based assets will struggle for maturity.

Under the Donald Trump administration in the US, the attitude towards blockchain is changing. The political will now is to ease the path for banks to make use of blockchain, which requires new rules to be drawn up to govern the way in which banks interact with new technology.

The Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency have issued new guidance on how commercial banks can interact with blockchain-based assets, which other jurisdictions may look to emulate.

Internationally, the picture is less clear. Many regulators still view blockchain architecture with scepticism and have regulatory frameworks that could make it challenging for banks to interact either with cryptoassets, or with tokenised versions of traditional assets.

Ideally, rules on how banks treat a technology should be set with some reference to a global standard. Since capital markets operate internationally, if one national framework is out of step with the global consensus, it risks compromising the flow of capital.

While the continued safe, orderly functioning of capital markets remains paramount, improvement is only possible if participants can experiment and engage with new systems. Balancing the tension between facilitating this innovation and protecting financial stability is the central challenge for regulators in this field. It can only happen with close and constructive dialogue between both sides.

OMFIF's Digital Monetary Institute has partnered with Aptos Labs, Hedera, Minsait (Indra Group), Ripple and the Stellar Development Foundation to present this report. These institutions, together with OMFIF, met with six key financial and bank regulators for open, in-depth discussions of the challenges involved in regulating the use of public blockchain at commercial banks.

These discussions are part of the process of constructing a shared understanding between technologists, financial services professionals and regulators. This understanding is crucial to develop a policy framework that both allows innovation to flourish and protects the integrity of financial markets.

OMFIF is indebted to the working group participants and to the regulators and bankers who participated in the meetings.

'Since capital markets operate internationally, if one national framework is out of step with the global consensus, it risks compromising the flow of capital.'

Function over form in financial infrastructure

As public blockchains emerge as a transformative force in financial infrastructure, regulators face the challenge of creating effective oversight without stifling innovation.

THIS is a time of immense dynamism, both in the rich innovation in products and tooling of blockchains, and in the pace with which traditional finance is adopting the infrastructure.

It is perhaps not surprising that regulations have not all kept pace with technical developments. However, it is vital that regulations adapt to ensure that innovation can flourish and standards are preserved in financial markets.

Open and decentralised blockchains in finance represent a novel architecture and given their transformative potential and specific structures, they have prompted a unique regulatory response. Eschewing the traditional technology-agnostic approach, regulators have drawn lines around public blockchains and the assets transacted on them and highlighted them as particularly dangerous. This attitude among regulators prevents the market from properly testing and determining the value that blockchains offer financial markets.

In a space where both technology and terminology are evolving quickly, this report begins by establishing the definitions and concepts that regulators should bear in mind when designing regulation.

Next, we shine a spotlight on the Basel Committee on Banking Supervision's standards for Prudential Exposure to Crypto-Assets, which provides a perfect example of regulatory guidance that hampers innovation and adoption by drawing too prescriptive a line around specific blockchain architectural choices.

We argue that regulation of financial infrastructure should not specify a particular architecture but rather focus on a set of functions and standards that the technical systems underpinning it must be able to support.

We break down those areas: accountability and governance, operational resilience, settlement finality, throughput and fee stability, asset control, confidentiality, validator screening and interoperability.

Finally, we explore the role that regulators can play in promoting innovation in blockchain, through labs, sandboxes and the promotion of interoperable design.

Throughout the report, we feature thought leadership from the working group members, introducing distinctive features of the blockchains they support or, in the case of Minsait (Indra Group), highlighting the importance of shared technical standards.

'It is vital that regulations adapt to ensure that innovation can flourish and standards are preserved in financial markets.'

POLICY RECOMMENDATIONS

Regulation of the blockchain technology underpinning financial infrastructure should not specify architectural choices but should instead focus solely on ensuring that the features and functionality required to maintain the integrity of financial markets are delivered.

Accountability/governance: The controls and responsibilities that regulators need to enforce can be exercised through regulations on issuers of tokenised securities and other operators of regulated financial services on the blockchain.

Operational resilience: Public blockchains typically exhibit extremely high resilience, but regulated institutions that leverage blockchain technology for financial infrastructure for regulated financial instruments should have fall-backs in place to ensure business continuity.

Asset control: Regulators should mandate that blockchains used as financial infrastructure enable regulated token issuers to implement controls to meet their regulatory obligations, such as white-listing for know-your-customer requirements, freezes, clawbacks and transfers.

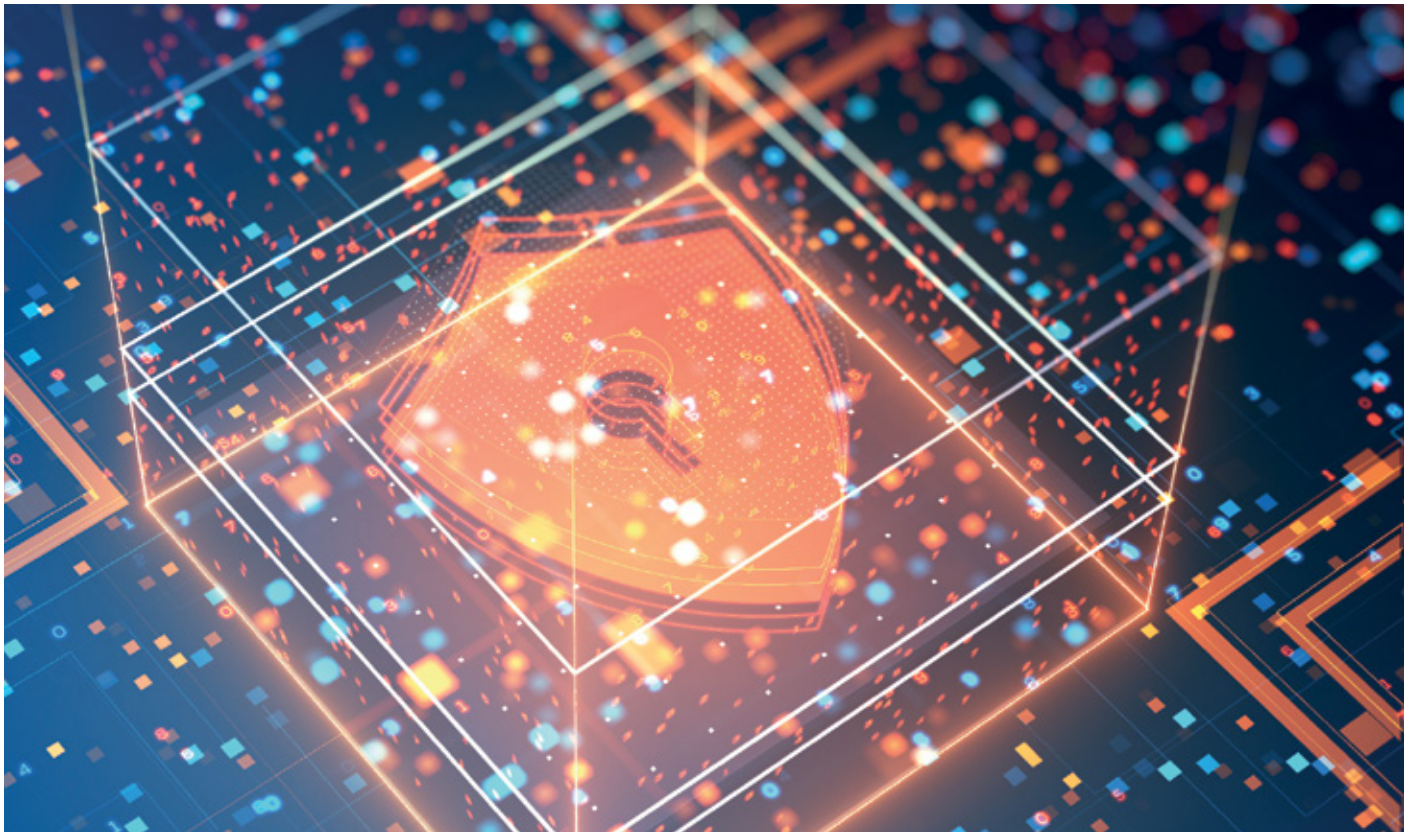
Settlement finality: Regulators should mandate that transactions in regulated financial instruments on blockchains are technically settled quickly and finally, fulfilling also the requirements for legal settlement.

Confidentiality: Regulators should consider ways that regulated financial instruments can transact in ways that protect users' confidentiality without compromising banks' ability to detect unlawful transactions.

Interoperability: Regulators should promote infrastructure for regulated financial instruments that enables seamless cross-chain migration of assets, improving resilience and liquidity.

Throughput and fee stability: Infrastructure for regulated financial instruments must be able to comfortably support peak levels of traffic, even accounting for increased traffic made possible by reduced transaction costs.

Validator considerations: Regulators should make clear whether financial institutions have any responsibility to know the composition of the community of validators.



Key findings

- Many regulations designate public blockchains as risky technologies but, frequently, these designations relate to risks exhibited only by particular protocols, not all public blockchains.
- The Basel Committee on Banking Supervision's rules on prudential exposure to cryptoassets impose such stringent capital requirements on public blockchains that several regulators are opting not to implement them.
- While the blockchain protocols themselves are unsuitable sites for regulatory oversight, banks and service operators making use of blockchains can be regulated to ensure appropriate standards are maintained.

Regulating public blockchains

The decentralised nature of public blockchains has unsettled some regulators, but though regulating the protocols themselves is not feasible, regulators can still impose requirements via regulations on the operators that use them.

BLOCKCHAIN regulations are sometimes flawed because they treat blockchains as homogeneous, or do not understand the nuanced distinctions between different kinds of blockchains.

With three types of blockchain – public permissionless, public permissioned and private – it is important to note, however, that not all regulators recognise these categories. The Basel Committee on Banking Supervision treats public blockchains as synonymous with permissionless, and private blockchains as synonymous with permissioned in its 'prudential treatment of crypto-asset exposure' document, referring to 'a public ('permissionless') ledger' and 'a private ('permissioned') ledger'.

This ignores the existence of public, permissioned blockchains as a category distinct from private, permissioned blockchains. It also overlooks the existence of public, permissionless blockchains whose consensus mechanism prevents anonymous or malicious actors from becoming validators.

Private blockchains control who can participate or build on the network via a consortium or set of approved parties. This means that the infrastructure has a centralised governance structure that allows it to make unilateral decisions.

'Distributed technology and decentralised governance are separate concepts and just because a network has one does not mean the other will be present.'

Public blockchains are typically open, allowing anyone to build on them and transactions to be visible to the whole network. Governance on public chains is built to be decentralised, since validators and/or token holders can participate in the governance process.

Permissioned blockchains only allow entities that have been given permission by privileged members of the network to participate in validating transactions. Permissionless blockchains allow anyone to become a validator (although some impose a minimum stake or other requirements).

Using these definitions, the public and permissioned category emerges, referring to chains on which anyone can build and view transactions, but to become a validator requires permissioning.

DISTINGUISHING BETWEEN CATEGORIES

Most in the blockchain industry favour public blockchains both for their openness and their high standards of resilience and cybersecurity. The crypto industry overwhelmingly makes use of these protocols, and many in the financial industry that have adopted blockchain technology also favour this type. But the regulators the working group spoke with observed that the nature of some regulations on banks makes using these protocols more complicated. Accordingly, to date, banks have had to build some of their experimental blockchain infrastructure on private blockchains.

Private blockchains more closely resemble traditional, centralised methods of record-keeping and therefore require less adjustment from users. However, they risk creating a walled garden where services can only be provided by privileged entities and lack the defining features of blockchain technology. This harms competition since smaller entities risk exclusion as they cannot create their own networks. Losing the dynamic ecosystem of builders that public networks benefit from can also harm resilience and security. If many private chains proliferate, this risks fragmenting liquidity, since it replicates existing centralised structures.

Settlement infrastructure platforms can only become truly valuable if a critical mass of market participants is onboard. With private networks, this can be challenging since it requires competitors to use each other's systems. Though this is not impossible, it may be that a public framework for common use is more readily adopted. However, such systems are challenging for banks to use at present due to regulations.

There is a great deal of research on the relative merits of different types of blockchains for different use cases. This report will not add to it. Blockchain users should be able to decide on the architecture that best suits their needs. We intend instead to challenge the assertion that public blockchains cannot exhibit the necessary qualities for regulated financial activities, and that they therefore need special regulation.

The distinctions between public and private and permissionless and permissioned are true when discussing the basic architecture of a given chain. However, technological progress has blurred the characteristics associated with the terms. New protocols and features have emerged that give many blockchains a set of characteristics that means they no longer fit into the categories of this simple taxonomy.

Part of the reason for this is the emergence of Layer 2 protocols, including sidechains, rollups and subnets. Although these work differently from each other, they aim to improve the throughput of the network by processing transactions away from the main chain, and to implement specific rules for a given use case.

While these are popular for some public networks like Ethereum, many modern Layer 1 blockchains have incorporated the functionality that Layer 2s and subnets seek to provide natively to their Layer 1 protocol. This means they can achieve the same effects without creating additional layers that may introduce centralisation or other risks that could compromise the integrity of the underlying protocol.

Given this technological progress, these distinctions are no longer informative when it comes to determining the functionality of a given chain. Accordingly, they are not sufficiently robust to be the basis of regulation.

It is also worth distinguishing between distributed technology and decentralised governance. Distributed technology refers to infrastructure supporting a network being diverse in location, technology stack and ownership. Decentralised governance refers to the concept of decision-making and consensus-building on the network requiring a consensus of participants, with no single entity having control. It is possible for a network with

distributed technology to have centralised governance, perhaps because a participant has amassed enough control to overrule the rest of the network.

Distributed technology and decentralised governance are separate concepts and just because a network has one does not mean the other will be present. Both have benefits – distributed technology brings operational resilience, while decentralised governance brings integrity and freedom from abusive control – and both must be protected by design features in order to persist.

BASEL AND CAPITAL REQUIREMENTS

Perhaps the single most obstructive piece of regulatory guidance for bank interaction with public blockchains and cryptoassets is contained within the Basel Committee on Banking Supervision's publication on the 'prudential treatment of crypto-asset exposures'. These standards are set to be implemented in January 2026. In the time since the document was first drafted in 2022, blockchain technology has advanced – as has regulators' understanding of the distinctions between different types of risk. However, these standards, known as SCO60, remain the Basel Committee's position.

In the document, the BCBS establishes four types of cryptoassets: types 1a, 1b, 2a and 2b. The problem stems from the definition of type 2b, which is defined as: 'All other crypto-assets (i.e. tokenised traditional assets, stablecoins and unbacked crypto-assets that fail to meet the classification conditions and fail the Group 2a hedging recognition criteria)', which receives a 1,250% risk weighting.

This punitive risk weighting was intended to deter institutional participation in what was initially perceived as a volatile and risky asset class by making them too expensive from a capital perspective for banks to hold. Whether this is warranted in the case of speculative investments in the crypto market is a matter for debate. However, the definition of type 2b includes any asset on a blockchain for which not all participants are traceable. In effect, this includes all assets on public blockchains other than a small number that satisfy hedging recognition criteria. The risk weighting therefore treats asset and technology risks equally.

To meet one of the BCBS's classifications, the following requirements must be met: 'All key elements of the network must be well-defined

'Since the Basel Committee exists to create a level playing field, the standards they recommend are only worthwhile if widely adopted.'

such that all transactions and participants are traceable. Key elements include: (i) the operational structure (whether there is one or multiple entities that perform core function(s) of the network); (ii) degree of access (whether the network is restricted or open); (iii) technical roles of the nodes (including whether there is a differential role and responsibility among nodes); and (iv) the validation and consensus mechanism of the network (i.e. whether validation of a transaction is conducted with single or multiple entities)'.

A requirement that all transactions and participants on a network are traceable will mean that any assets represented by tokens on public, blockchains will fall into type 2b. This will include bonds with triple-A credit ratings from issuers like the European Investment Bank and stablecoins like USDC, when (as they almost invariably are) they are issued on public, blockchains. This is despite the fact that their issuers are adhering to the standards set by their regulators. Holding these assets should not impact a bank's capital position.

While some regulators may have concerns about operational resilience and the makeup of validator communities, these concerns do

'If the BCBS is to carry weight, it must implement rules with which the national competent authorities are sufficiently comfortable to implement.'

not impact the prudential risk posed by a given asset and therefore should not be expressed through restrictive prudential standards.

The finance community has expressed concerns around the BCBS standards. In August 2025, a community of financial services associations including the Association for Financial Markets in Europe, Institute of International Finance and International Swaps and Derivatives Association, requested that the Basel Committee pause implementation of the 'prudential standards for crypto-asset exposure' and consider redesigning them.

The letter highlighted that several jurisdictions have already implemented guidance that conflicts with the Basel Committee standard and that others will decline to follow them. The group calls for the BCBS to 'eliminate the distinction between permissioned and permissionless ledgers', arguing that 'there should be no ex-ante distinction between permissioned and permissionless ledgers. The focus of regulatory supervision and treatment should be on the risk of the asset itself, not the attributes of the underlying ledger'.

IMPLEMENTATION DOUBTFUL AND VARIED

Since the Basel Committee exists to create a level playing field, the standards it recommends are only worthwhile if widely adopted. If the BCBS is to carry weight, it must implement rules with which the national competent authorities are sufficiently comfortable to implement.

The Basel Committee comprises some 28 jurisdictions and a uniform approach has yet to emerge. Although the European Union is applying the Basel Committee rules via Capital Requirements Regulation III, in its draft Regulatory Technical Standards, the European Banking Authority says that the approach that the classification conditions CRR III will use follow the Markets in Crypto-Assets distinction and may differ from those of the BCBS regime.

The report from the EBA states: 'The crypto-asset exposures classification specified in Article 501d of CRR 3 is based on MiCA and does not differentiate the token's riskiness based on the underlying type of technology or governance model of any distributed ledger. Also, the draft RTS does not incorporate any criteria around blockchain technology to determine the classification of the tokens and the capital treatment. The EBA note here that the Basel classification conditions for crypto-asset exposures might result in a different classification for some of these exposures compared to the transitional CRR 3 regime which incorporates elements of MiCA and the BCBS regime.'

Despite this encouraging framing, the reality on the ground in key EU jurisdictions is shaping up differently. Regulated institutions report that publications from the EBA and their national competent authorities do not provide the level of clarity they need when it comes to the capital treatment of bonds natively issued on public, permissionless blockchains.

Meanwhile, the US has said that it has no intention of adopting the Basel rules on cryptoasset exposure in their current form, which is likely to give its banks a head start in designing products and services for tokenised assets on public blockchains. China is expected to retain its existing domestic restrictions. India has made no moves towards implementing the Basel standards. While Hong Kong is expected to implement the Basel framework, the Hong Kong Monetary Authority generally assesses the suitability of a given blockchain arrangement for regulated activity on a case-by-case basis and acknowledges that technological development may mean that specific capital treatments are subject to review. The UK is still in a period of consulting and data gathering to determine how it will calibrate its rules. While Switzerland has broadly adopted the Basel III framework, the specifics of exposure to cryptoassets are not yet finalised.

At present, with several Basel Committee constituent countries making no moves to implement standards that are scheduled to come into force in January 2026, we are moving towards a world where each country, responding to domestic pressure from banks, will design their own prudential rules for cryptoasset exposure. If the Basel Committee eventually redesigns SCO60, then it will face an uphill battle in persuading its members to harmonise their disparate rules, rather than running ahead and providing standards to shape the formation of those rules.

A level playing field is vital for fair competition between banks across jurisdictions. Without the Basel Committee's rules to establish a common framework for guidance, there is an incentive for national regulators to implement looser standards, encouraging regulatory arbitrage and endangering financial stability.

Stellar

Rethinking blockchain categories

'The public-or-private and permissionless-or-permissioned categorisations have outlived their utility.'

We must move beyond the 'public, permissionless' and 'private, permissioned' categories, writes Marcelo Prates, policy director at the Stellar Development Foundation.

IN July 2025, two years after the Markets in Crypto-Assets Regulation was enacted in the European Union, the GENIUS Act was signed into law in the US. The increased legal certainty brought by these two landmark laws renewed the interest of regulated entities in digital assets.

These entities are now pondering in more detail how to enter the digital asset space. After the tokenisation of cash with stablecoins, what comes next in the tokenisation journey? And if they issue assets on-chain, what kind of controls do they need to have over these assets?

Before getting to these questions, regulated entities should look at where to issue digital assets. Among many options now available, which blockchain is best suited for the issuance of regulated assets?

The analysis should go beyond the supposedly straightforward distinctions between 'public and private' or 'permissionless and permissioned'. These overly simplified categorisations have blurred relevant differences among blockchains and led to dismal results.

The international standard developed by the Basel Committee on Banking Supervision for banks' exposures to cryptoassets is a case in point. As the standard heavily relies on the binary construct of 'public (permissionless)' and 'private (permissioned)' ledgers, it has an unjustified bias against what it calls 'public (permissionless) ledgers'.

The current text of the standard could lead financial supervisors to treat tokenised assets, like securities, as riskier than their traditional non-tokenised counterparts, especially if issued on 'public (permissionless) ledgers'. This approach would, in turn, impose a highly punitive capital requirement on banks: for each $1 held in tokenised securities, banks would have to add $1 in capital.

Blockchain was devised as a decentralised platform for users to send payments directly to each other without going through a trusted intermediary. This open model with distributed power was later labelled 'public blockchain'. The idea was to mark a contrast with some incoming alternatives that used blockchain technology to create closed networks, dubbed 'private blockchains', promising a more controlled environment for enterprise use.

Although open and decentralised blockchains have evolved into different types, the 'public-or-private' distinction has lingered, overlooking the increasing diversity within the 'public blockchain' group.

To avoid this oversight, any blockchain comparative analysis should start by assessing who controls the network: is it centralised around a single party or a group of selected organisations? Or is the network open and decentralised?

From a risk-management perspective, the more concentrated the power over the network, the easier it is to pinpoint a controller, but the higher the risk of single points of manipulation, failure or attack. The more decentralised the network, the harder it is to map accountability, but the more accessible, interoperable and resilient it tends to be.

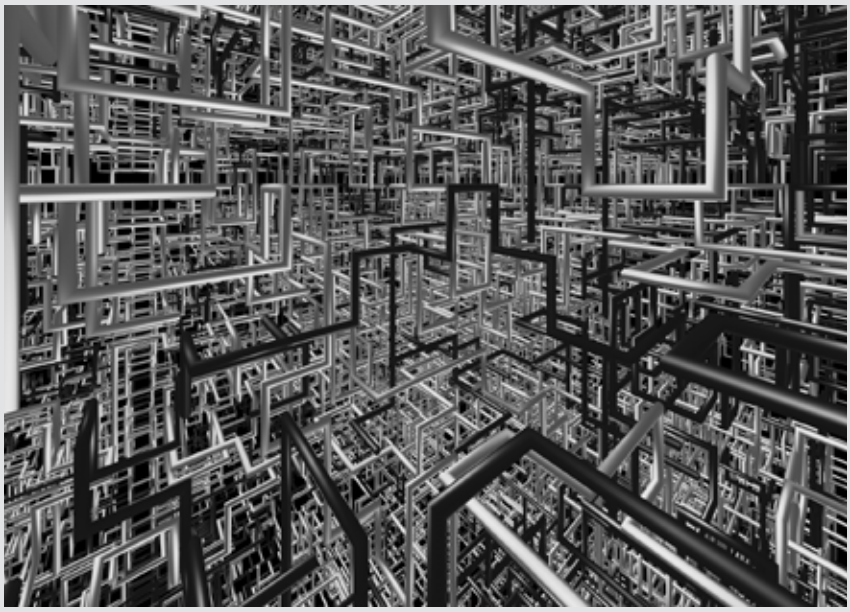
While the decentralised governance model may not follow traditional accountability structures, it introduces new ways to mitigate risks and achieve the safety and stability expected from any financial infrastructure.

It has to be clear that decentralisation, rather than denoting an absence of control, means that no individual party can exert control over the network. The development and maintenance of an open blockchain are spread across multiple parties.

Validators, nodes, developers and asset issuers have incentives to keep each other in check and ensure that the network operates according to the internal rules embedded in its protocol and that changes are implemented only after collective approval.

However, understanding who controls the network isn't enough. How decisions are made, especially on decentralised networks, is also a crucial factor. As open blockchains achieve decentralisation in different ways, it matters to examine their governance and decision-making processes, particularly when it comes to validating transactions.

Here again, for the sake of simplicity, another binary distinction appeared. The term 'permissionless' purports to describe



'As open blockchains achieve decentralisation in different ways, it matters to examine their governance and decision-making processes.'

open blockchains that allow anyone to join the network and freely compete to enter the transaction validation process. On the other hand, 'permissioned' refers to open blockchains that anyone can still join, but only a few are chosen by a central entity or group to take part in transaction validation.

In the face of these two opposing categories, a bias against 'permissionless' blockchains emerged. If anyone can 'join and participate', then nodes in North Korea could be engaging in transaction validation, and transaction fees might be paid to validators located in sanctioned jurisdictions. Should it then follow that no regulated entity should issue tokens on so-called 'public, permissionless' blockchains? Not really.

The current reality of open and decentralised blockchains is more diverse than the one suggested by these rigid categories. Take the Stellar network. Unlike proof-of-work and proof-of-stake networks, which rely on the assumption that economic incentives will suffice to keep validators honest, Stellar is built on proof-of-agreement.

On the Stellar network, participation in transaction validation isn't based on computational power and energy (PoW/mining) or token accumulation (PoS/staking) but on the reputation of the entities running the selected nodes.

The Stellar consensus mechanism achieves this result not by reintroducing centralisation at the validation level to control who can be a validator (so-called 'permissioned validators') but by designing a decentralised selection process based on mutual trust.

As in other open and decentralised blockchains, anyone can run a Stellar node. But a new node can only become a validator and participate in the transaction validation process if at least some of the already established validators add it to their trusted set of validators. As a consequence, Stellar validators are a set of known entities that trust each other.

This design prevents anonymous or malicious actors from becoming block producers. Untrusted nodes, no matter how powerful their computers are or how much money they have, cannot force their way into the validation process.

The only way to maliciously influence the Stellar network is to somehow convince a majority of existing validators to trust the attacker – a far higher bar than simply buying tokens or investing computation power and energy.

Moreover, validator nodes on Stellar don't compete for rewards or receive financial incentives when they process transactions. They each participate in the validation process to reach a network-wide agreement about the validity of transactions.

This feature brings neutrality to the Stellar blockchain since no validator financially benefits from the number of transactions being validated on the network. It also greatly reduces the incentives for validators to reorder or rush transactions submitted for validation – engaging in maximal extractable value, front-running or manipulation – as they don't seek fee maximisation.

Unlike other protocols, transaction fees charged on Stellar exist to curb network abuse, like spamming, and are eventually burned instead of going to validators. No one, much less criminal or sanctioned entities, receives transaction fees on Stellar.

While still open and decentralised, Stellar offers the promised benefits of 'private blockchains' without the risks of other 'public blockchains'. In this sense, Stellar is in a category of its own, demonstrating how inadequate the current blockchain labels are.

The public-or-private and permissionless-or-permissioned categorisations have outlived their utility. They're now a source of confusion and flawed regulatory outcomes. It's time to move past them and build a more accurate and useful analytical framework focused on key blockchain features, like network control, governance, settlement finality, efficiency, interoperability and asset controls.

Key findings

- Regulators can ensure standards appropriate to infrastructure of regulated financial activity are maintained through guidance and requirements on operators and users.
- These requirements will vary slightly between jurisdictions based on the priorities of local regulators, but generally should focus on delivering stability, resilience and deterministic settlement.
- The ability to restrict who can hold a regulated financial instrument is another key feature that financial market infrastructure must be able to provide. However, this permissioning can happen at the token level, rather than the protocol level.

Functionality requirements

Regulated financial activity can only take place on infrastructure that is capable of exhibiting certain standards. Defining these standards and assessing that they are present will be a core responsibility of regulators as the rails of financial markets evolve.

AMONG regulators' most important responsibilities is ensuring that the stability, security and integrity of financial markets are not compromised. If a new technology emerges to provide the rails for financial assets, then regulators must ensure that it achieves certain standards of stability. It must also facilitate their ability to supervise financial markets activity and, when appropriate, enforce their decisions.

Regulators have had concerns that public blockchains are incompatible with these requirements. Thanks to technological progress, this may no longer be the case. Testing this requires regulators to make a clear statement of the requirements they expect of the infrastructure used for regulated financial services. The key elements of those standards are laid out in this chapter, along with ways in which public blockchain architecture can fulfil these requirements.

GOVERNANCE STABILITY

With some blockchains, especially those that rely on proof-of-work, disagreements among validators or token holders over network rules, the blockchain can lead to a split or 'fork' into two separate versions of the blockchain. In the context of regulated finance, any risk that creates confusion around which version of a token represents a security is untenable and must be mitigated.

While this might have historically been a concern for some regulators, no major regulated asset, like stablecoins or tokenised securities, have been issued on PoW blockchains. Public blockchains that are typically issued for such instruments have technical governance features that make hard forks much less likely. When they do occur, it is usually the result of a planned migration and therefore takes place without disruption.

OPERATIONAL RESILIENCE

In capital markets, outages and downtime of core infrastructure can be enormously costly, making a high standard of operational resilience essential. Many public blockchains maintain extremely high levels of uptime because the decentralised nature of the infrastructure eliminates single points of failure or attack. However, failures remain a possibility, and any regulated financial institution making use of a public blockchain must have a contingency plan to ensure business continuity in the event of an unforeseen outage.

One possible solution is the inclusion of a so-called catastrophe clause in the legal documentation attached to an instrument that provides the ability to fall back on traditional methods in the event of a problem.

Another potential requirement should be the existence of a back-up chain onto which tokenised assets can be ported in the event of a failure of the original chain. In the event of a blockchain's catastrophic failure – either because of a network's governance decision or exploiting a technical vulnerability – the issuer of an asset could burn the original blockchain tokens and create new tokens representing the same assets and distribute them to the original holders. Similar business continuity features should also be required when a bank engages with a centralised technology provider, where the technology itself could fail or an issue could present itself with the vendor.

While this is achievable from a technical perspective, provided certain interoperability standards are maintained, policy must also be designed to ensure that it is legally possible. Thus, it is important that blockchain-based asset licensing is not specific to a particular blockchain but to its issuer.

ASSET CONTROL

The original promise of the bitcoin blockchain was a peer-to-peer transaction network and censorship-resistant ownership without intermediaries. Like cash transactions, it is impossible or extremely difficult for law enforcement to prevent people transacting in bitcoin even if the transactions are criminal.

For regulated financial instruments, this framework will not be appropriate. There is a series of controls that regulated asset issuers, infrastructure operators and other licenced intermediaries will need to be able to apply. These controls stem primarily from the token design choices. Many public blockchains have permissioned token standards available to empower regulated institutions to meet their regulatory and business objectives.

One of the main token standards is ERC-3643 – an open-source standard for permissioned tokens on Ethereum Virtual Machine chains. Alternatives exist that vary slightly depending on the blockchain protocol in use, but the unifying factor is that permissioned tokens can only be held by users that comply with certain conditions and that this functionality is not limited to private or permissioned chains. Many modern blockchain equivalents have their own native token standards that can achieve similar results, which give issuers a large menu of options to issue tokens with features that meets their specific regulatory or business needs.

Regulated institutions that issue tokens representing traditional financial products typically have to find ways to meet their anti-money laundering requirements and there is a variety of tools available to institutions to meet these important obligations. In certain circumstances, issuers may be able to revoke a user's ability to transact in a token or freeze and even claw back tokens in the event of sanctions or insolvency. It should also be possible to restrict transactions during given periods like blackouts.

In the event of insolvency proceedings or a court order ruling a transaction as unlawful, it should also be possible to enforce the transfer

'Any regulated financial institution making use of a public blockchain must have a contingency plan to ensure business continuity in the event of an unforeseen outage.'

'The benefits of public blockchain stem from openness. The value only emerges if assets are free to move from chain to chain and between blockchains and traditional financial systems.'

of tokens from one wallet to another, and to burn or mint new tokens. This power will also be important if it becomes necessary to migrate tokens from one chain to another if a chain becomes compromised.

Intermediaries should be able to claw back or reverse transactions in the event of errors. It should also be possible to make transfers conditional on the fulfilment of certain conditions, enabling tokens to be temporarily held in escrow.

Intermediaries like exchanges need to be able to handle events like stock splits or conversion of assets like contingent convertibles from bonds to equity. They must also be able to impose 'circuit-breakers', halting trading in the event of crises. Regulators must be able to oversee trading and to give law enforcement agencies the power to seize assets in certain conditions.

CONFIDENTIALITY

Payments on the bitcoin blockchain enjoy a blend of transparency and confidentiality. They are transparent because payments activity is visible to the network, but they are confidential because bitcoin can be used pseudonymously. This confidentiality is limited, because when one sells bitcoin and transfers the proceeds to a bank account, then a bitcoin address can be attached to an identity, but bitcoin transactions in themselves are pseudonymous.

In regulated finance, neither this limited confidentiality nor this unlimited transparency are viable. Holders of securities will need to have completed a know-your-customer process to ensure that they are not prohibited from doing so.

Some degree of transparency is necessary so that regulators, law enforcement agencies and those responsible for monitoring markets for suspicious activity can protect the integrity of financial markets. Tools like those provided by blockchain analytics firms, such as Chainalysis and TRM Labs, have helped law enforcement agencies track illicit payments made on blockchains. However, in financial markets, some degree of confidentiality is also important.

There are good reasons for regulated financial institutions not to wish for their entire trading activity to be known to their counterparties and the market more generally. Trading activity, particularly for large accounts, can be market-moving information and a degree of privacy from counterparts is therefore an important feature of capital markets infrastructure.

Solutions for this are emerging. EY has made the code for its Project Nightfall – a Layer 2 solution on Ethereum – available in the public domain. Nightfall uses zero-knowledge rollups to allow counterparties to transact privately without revealing all their details to the rest of the network.

SETTLEMENT FINALITY

A necessary quality of settlement infrastructure is the ability to provide absolute clarity on when a transaction is settled. With the bitcoin blockchain, settlement finality is probabilistic. Each new block contains some subset of the eligible transactions. When it is accepted, the other transactions that were left out of the winning block must be resubmitted. However, it is possible that a fork created when two miners both complete valid blocks may spawn a longer chain causing some transactions that were previously included to be undone.

As each block is completed, settlement becomes progressively more final and unlikely to be reversed. This means that transactions are only ever final in the sense that the possibility of the chain of blocks in which they exist being overtaken by another chain is vanishingly small. This is a consequence of the PoW consensus mechanism.

Other blockchain consensus mechanisms have been developed that negate this concern. Most blockchains today don't rely on PoW and offer a relevant degree of 'deterministic finality', in the sense that transactions are either confirmed and added to a block that will then be put on the blockchain or are rejected and fail.

When only one block is added to the blockchain at a time, with no simultaneous blocks being created, all transactions in the block are immediately final and irreversible. The key consideration then is how long it takes from the moment a transaction is confirmed and added to a block to the moment when the block is put on the blockchain.

However, it is important to remember that technical finality is not sufficient. It is essential that legal finality of settlement be explicitly separated from, and treated as equally important as, technical settlement. Legal settlement can only be declared by an institution empowered to do so through

'Regulators must be able to oversee trading and to give law enforcement agencies the power to seize assets in certain conditions.'

regulation. Accordingly, if public blockchain capital markets infrastructure is to successfully achieve widespread adoption, then regulators must implement policies that enable blockchain-based infrastructure to legally determine settlement. A lack of precision or consistency here may result in disagreements, particularly in the event of insolvencies when attempting to claw back assets.

INTEROPERABILITY

The benefits of public blockchain stem from openness. The value only emerges if assets are free to move from chain to chain and between blockchains and TradFi systems. The tokens that represent ownership of regulated assets must be able to move between chains seamlessly, whether through cross-chain bridges or swaps. This will improve liquidity by ensuring that assets are not tied to a specific chain and the community of people using it.

Achieving this is difficult because many blockchain developers are working on standards for specific protocols to give them a competitive advantage. This can result in fragmentation, which makes seamless communication between protocols difficult.

Solutions are already emerging to the technical challenge of interoperability. Circle, which issues the world's second largest stablecoin, USDC, has developed the Cross-Chain Transfer Protocol, enabling USDCs to move between trusted chains seamlessly and securely. Other solutions, like those offered by interoperability providers like LayerZero have also made important contributions to creating

a robust solution for cross-chain transfers.

Regulators around the world have identified that fragmentation as a result of a lack of easy cross-chain transfers is a risk. The risk will be lessened if the industry is able to coalesce on shared technical standards. While the industry may come to this result on its own – the emergence of open-source token standards like ERC-3643 is testament that this is possible – regulators can help the process by encouraging the industry to collaborate in defining common technical standards.

For regulated financial infrastructure, it may be appropriate for regulators to demand that tokenised securities trade only on protocols that adhere to certain standards of openness. This would ensure that the asset's liquidity is not compromised and that the option to port to another chain is present, avoiding vendor lock-in.

THROUGHPUT AND FEE STABILITY

An early challenge to the use of public blockchains in wholesale settlement is that they were unable to deliver the transaction throughput necessary for institutional capital markets. This was primarily a feature of the bitcoin blockchain, which was designed to process around seven transactions per second.

At times of higher demand, this results in higher transaction fees. Unpredictable fees and delays in settlement would certainly not be desirable features for capital markets infrastructure. However, for modern chains designed for institutional use, capacity limits are less of an issue. Many modern chains can support thousands of transactions per second at far lower costs.

VALIDATOR SCREENING

Regulators should focus on the validator communities that support permissionless blockchains. The distributed consensus that keeps public blockchains secure relies on the existence of a diverse and distributed community of validators.

On the bitcoin blockchain, these validators are known as miners. Miners search for a solution to the SHA-256 algorithm and compete to produce a valid block and earn rewards and transaction fees. This is the PoW consensus mechanism.

Many newer blockchains use proof-of-stake, in which validators stake their own native tokens or are delegated tokens to stake as collateral. Each takes a turn proposing a new block, which is checked and reviewed by other validators before being broadcast to the rest of the network. The work this requires earns validators fees known as 'validator rewards'.

Validators are not intermediaries and never hold or transmit tokens on behalf of blockchain users. Regulatory attempts to impose requirements on validator communities that make them responsible for preventing money laundering or illicit transactions are misguided. Validators play a neutral role: simply protecting the security of the network and ensuring no invalid transactions (such as double spending) are entered. Issuers of assets can choose to screen who can transact, but the settlement layer's neutrality should not be compromised.

In permissionless blockchains, participants do not need permission to become validators. But many blockchains have technical requirements that validators must satisfy before being able to validate transactions. In the case of the bitcoin blockchain, the validator community certainly contains sanctioned elements. From the perspective of regulators, this introduces a potential concern: because validators earn fees, some might consider them counterparties.

There are two possible responses to this. The first is to challenge the idea that the validator community should be considered counterparties in the traditional sense. Since the validator community is distributed, it is not a legal entity. Therefore, it cannot be a party to a contract even if it receives a fee. Since it cannot be party to a contract, it cannot be a counterparty and therefore banks can transact with the network without it being considered a counterparty relationship.

This is a legal argument and regulators around the world will come to their own conclusions. Perhaps some will take this view, but others may feel that, whether or not a validator community constitutes a counterparty, they do not want the fees from facilitating the trading of regulated financial instruments to go to a community that contains unsavoury elements.

For regulators who take this view, it may be helpful to be able to demonstrate that a validator community does not contain sanctioned elements. Many public blockchains are capable of doing this, either through permissioning entry to the validator community, allowing users to select a subset of validators or through ensuring validators are known to each other.

APTOS

Scaling trust with blockchain infrastructure

'Unlike many blockchains where transactions are processed sequentially, Aptos enables 'parallel execution' where multiple transactions are executed simltaneously.'

Jon Sabol, associate general counsel at Aptos Labs, speaks with OMFIF about creating compliant blockchain infrastructure purpose-built for institutional adoption.

OMFIF: You represent Aptos Labs. Can you tell us what that is?
Jon Sabol: Aptos Labs, founded in 2022, is the core development team building the Aptos blockchain – a next-generation, high-performance, proof-of-stake Layer 1 blockchain. Aptos Labs also builds applications and developer tools for the blockchain and has its roots in the Libra and Diem projects at Meta – where much of the founding team worked previously – and has attracted significant venture capital support from VCs such as a16z and Multicoin Capital, as well as leading financial institutions such as Tiger Global, Apollo and Franklin Templeton.

OMFIF: You said 'high-performance' to describe Aptos. In what respect? Is this about throughput?
JS: Yes, throughput is a big part of it. Since Aptos had its roots in a project intended to enable billions of Instagram, Facebook and WhatsApp users to transact on-chain, the technical capacity to deliver speed at scale was built in from the start. Unlike many blockchains where transactions are processed sequentially, Aptos enables 'parallel execution' where multiple transactions are executed simultaneously. Parallel execution – and other novel technological advances – enables Aptos to process more than 20,000 transactions per second, unlocking use cases that would not otherwise be possible on a blockchain.

Additionally, Aptos employs a novel smart contract programming language called Aptos Move, which offers unmatched power and flexibility for blockchain development and was designed with safety and security as a priority.

OMFIF: What about transaction fees? Those are charged in the underlying token. Is there a risk of volatility and cost fluctuation?
JS: Gas fees on Aptos are typically a fraction of a penny, making even microtransactions economically viable. While these can fluctuate, this low price has been consistently maintained and it's low enough that even if the costs increased by a factor of 10, network transaction fees are still not going to be prohibitive, particularly compared to other networks where gas fees can be a limiting factor.

OMFIF: You mentioned institutions and brands using Aptos. Can you give some examples?
JS: There are currently hundreds of projects live on Aptos. Within financial services, some of these include BlackRock's Buidl Fund, Franklin Templeton's OnChain US Goverment Money Fund and Apollo's Diversified Credit Securitize Fund (ACRED), which gives holders access to Apollo's global credit strategies. Additionally, the world's largest stablecoins have launched natively on Aptos, which has played a pivotal role in Aptos' ecosystem growth, with more than $1bn in native stablecoins on Aptos.

OMFIF: For regulated institutions that are launching on Aptos, there has to be some functionality around who can or can't hold assets and how they're transferred. How does that work?
JS: Regulated financial institutions that issue tokens on Aptos or any other blockchain must meet their existing compliance requirements – which often includes controlling who can hold their assets, how those assets are transferred and under what conditions. Aptos has the tools in place to support those needs.

The network's Fungible Asset standard permits issuers to implement role-based access (mint, burn, freeze, claw-back among others) and allows regulated institutions to embed compliance logic – know-your-customer attestations, travel-rule messaging or limits – directly in the asset. There's a lot of flexibility built into the Aptos platform.

OMFIF: What about confidentiality? Blockchains are typically transparent, but there's good reason for regulated institutions to not want their customer information shared publicly.
JS: Regulated financial institutions and their customers often expect confidentiality when transacting. But public blockchains, by design, are open, revealing a transaction's key details and making it challenging for regulated financial and enterprise-grade use cases to adopt the technology.

A new feature being explored – Aptos Confidential Transactions – would make a user's transaction amounts confidential to the public, opening up the space for developers to build compliant, confidential use cases. Sender and recipient information would still be visible publicly, and the token issuer would have the ability to nominate an auditor that would have access to all transaction information while ensuring certain sensitive transaction information remains confidential.

Hedera

Permissioning as protection

'It is wrong to assume that distributed technology will always lead to decentralised decision-making.'

Isadora Arredondo, global policy director at Hedera, speaks to OMFIF about empowering financial market infrastructure and the specific features of a permissioned blockchain compared to others.

OMFIF: You represent Hedera, which is the only public, permissioned chain in the working group. Could you break down what that means?
Isadora Arredondo: Well, the public component is something that Hedera has in common with all the other chains in this group. It refers to the fact that the infrastructure is open for anyone to build on and audit. This system of permissioned governance with auditable consensus will build more public trust than a purely closed (private) system. This is essential to the success of a global distributed ledger technology platform. Hedera's code base is also fully open source.

OMFIF: What about the permissioned component? How does that distinguish Hedera from the other chains?
IA: Permissionless chains allow anyone to join the community that operates nodes that validate transactions. They are also anonymous. Historically, open source software developers have recognised the value of maintaining a single baseline of code and ensuring that the best ideas from the community are included for the benefit of the whole. However, when combining an open source project with a protocol token, the traditional incentive structure is turned upside down. The DLTs that have been most widely adopted are also those that had historically split the most. Probabilistic finality, common in traditional blockchain where transactions can theoretically be reversed, introduces unacceptable risk and operational inefficiencies for critical financial market infrastructure.

The majority of public ledgers are not mathematically final. Instead they rely on a growing list of blocks containing transactions, leading to probabilistic finality. The older a block is in the history of blocks, the harder it is for an attacker to reverse that block. Most public ledgers specify how deep a block needs to be to be considered effectively final, but it's never 100% final – it's probabilistic. A determined attacker, with the appropriate financial means could theoretically change the course of history. This dynamic causes uncertainty, vulnerabilities to centralised control and has directly impeded the adoption of public ledgers by mainstream markets.

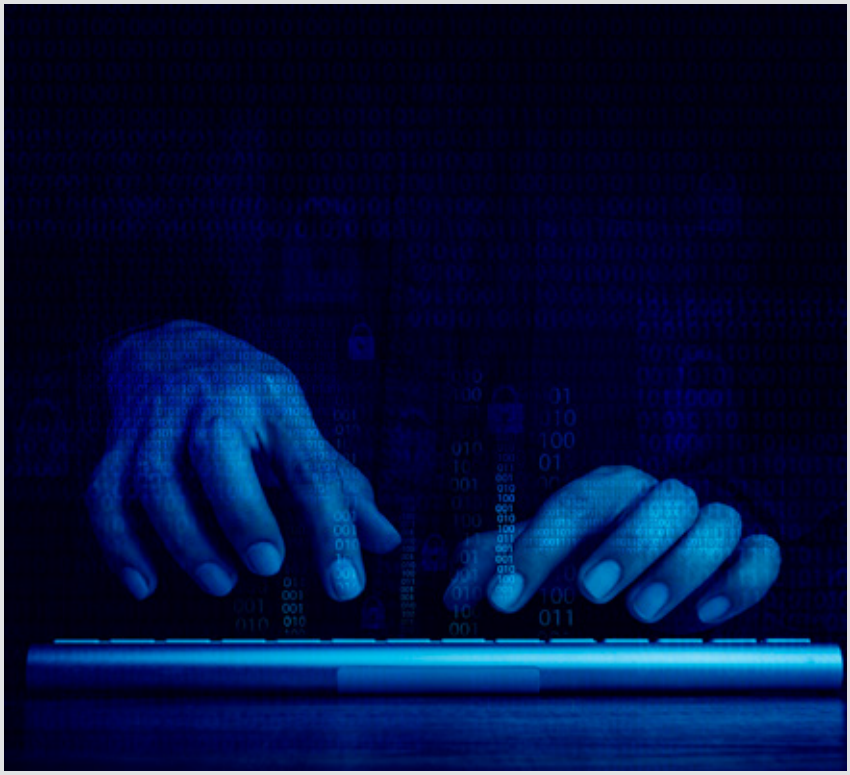
Hedera is different. Our governance and consensus algorithm ensures the platform will not fork into a competing platform and token. Finality on our network is deterministic.

OMFIF: What about decentralised governance?
IA: Most DLTs were designed with the objective of reducing market participants and end users' exposures to some of the vulnerabilities that stem from relying on centralised intermediaries and infrastructure. The idea of distributing technology and building peer-to-peer consensus is to foment democratic governance of online digital marketplaces. However, it is wrong to assume that distributed technology will always lead to decentralised decision-making.

Hedera will not fork. Forking as a result of community dissent can be as damaging as reverting transactions. Hedera operates a permissioned set of consensus nodes run by Fortune 500 organisations, dependable Web3 organisations and universities. Each node must periodically publish a hash of its state for other nodes to verify. Reverting transactions would result in an inconsistent state, which would result in the node being excluded from consensus in the first instance. The Hedera Council would then reconsider the node operator's membership.

Every public ledger depends on a majority of nodes being honest – this is the nature of Byzantine fault tolerance. It is always possible that a majority of nodes colludes to change history, most likely at a heavy financial cost. Knowing that Hedera is operated by mature and publicly known Fortune 500 organisations that change over time significantly reduces the likelihood of collusion.

Furthermore, Hashgraph, which underpins the Hedera network, treats every transaction in its own right and when that transaction has



'A determined attacker, with the appropriate financial means could theoretically change the course of history.'

reached consensus, it is considered 100% final. Given each transaction is 100% final, a malicious operator would not be able to reverse the course of history on Hedera.

OMFIF: Don't permissionless chains also achieve this? What makes the permissioned conception different?
IA: If consensus is achieved through the allocation of compute, or through staking reserves, then the security is essentially that it becomes prohibitively expensive for a single actor to compromise the integrity of the chain. But it is not impossible that a validator or group of validators starts to collude and, in doing so, amasses enough compute or stakes enough resources that the record that the chain maintains can be compromised. When that happens, you get all sorts of problems like possible forks to the chain, or improper transactions being validated.

In addition to its accountable governance, Hedera's Hashgraph consensus algorithm is leaderless: its strength is that it achieves true democratic, Asynchronous Byzantine Fault Tolerance consensus without sacrificing throughput or scale. Hedera doesn't have a single block producer or leader node – a node that is responsible for creating and proposing a block to the community of nodes. A single block producer, elected by the network and known to the public is a natural target for a denial-of-service attack. An attacker could direct its attack at each subsequent block producer, thus preventing the network from producing new blocks overall – this without 'skin in the game' since no cryptocurrency owned by the attacker is at risk.

Our fixed transaction fees are equally distributed across the network, removing the incentive to manipulate transactions. On Hedera, this means there is no maximal extractable value, no front-running and no sandwich trading. All nodes have to work together to achieve consensus on the order of transactions – no small cohort of nodes is able to cheat.

If you take any distributed consensus algorithm, they all have one basic job they must all do – and that is gossip transactions throughout the network. For Hashgraph to work, all we need to do is add a few bytes to each gossiped message. There is no additional communication required between nodes. Just gossip your messages and include a few extra bytes on each message and we can independently and deterministically resolve the order of transactions and their timestamps. Then we get technical finality.

OMFIF: Why do you specify from a technical perspective?
IA: Technical settlement is obviously an important feature for blockchains, but we also have to remember that settlement is a legal construct. It's not enough to simply receive an asset in a wallet. Financial market infrastructure has to be empowered by regulators to declare that settlement has been achieved and cannot be reversed. It's important to remember that blockchains are providing the technical architecture and the frameworks to support regulated financial activity are built on top of this.

Although the governance of blockchains is necessarily decentralised, we have to support activities that require some centralisation. While regulating public blockchains is practically impossible and not necessarily desirable, we need to support regulated entities in their journey of understanding the risks involved, the tools at their disposal and their responsibilities when it comes to using public blockchains. These support frameworks are an important component of any blockchain that wants to be a suitable host for regulated financial activity.

Key findings

- Blockchains should not be regulated as financial infrastructure nor as a third-party service provider, because they cannot be counterparties to a contract.
- By offering guidance on risk management frameworks, regulators can help make it easier for banks to adopt the technology. By setting standards on interoperability, regulators can help the market to coalesce around a single format.
- Sandboxes are a useful way of regulators testing the capabilities of new infrastructure in safe environments to ensure that they can deliver the features necessary for regulated financial activity.

The road to acceptance

Regulators can help to promote the adoption of public blockchain technology in capital markets in optimal, sustainable ways.

THE appropriate criteria for assessing what types of infrastructure can provide capital markets settlement are assessments on its ability to deliver technical features. However, even when the technical features are demonstrably present, ensuring the regulatory framework is adapted to account for their specificities is not an easy task. New technologies can introduce new risks. These risks must be acknowledged and mitigated. Where risks remain, the appropriate legal response must be identified.

For conventional financial market infrastructures, this regulatory framework rests on the fact that they are centralised and therefore operated by organisations with statutory responsibilities.

Public blockchains are decentralised and therefore do not fit easily into existing schema of responsibility. For many regulators, addressing this challenge will require a new approach. Typically, the handle for ensuring robustness, security and probity is through legal liability. With decentralised entities like blockchains, it is difficult or impossible to identify a directly liable individual or organisation.

The appropriate response to this is that blockchains themselves are not intended to function as financial market infrastructure. The protocols are simply a technology, akin to physical ledger books. The books are technology, not financial market infrastructure. They are deployed by regulated institutions who provide financial market infrastructure.

'The core breakthroughs required for public blockchains to provide the settlement infrastructure for capital markets have already been made. The challenge now is integration.'

Similarly, blockchains offer technological solutions, which should not therefore be regulated as a piece of financial market infrastructure and, in any case, do not have the sites for liability that would make this possible.

Blockchains can also not be considered an outsourced function, because this would require there to be a third-party service provider. Typically, arrangements with third-party service providers involve contracts. For public blockchains, this is unlikely to be the case since anyone can build on a public blockchain protocol and does not require a contractual relationship with the blockchain to do so.

The UK's Financial Conduct Authority seems comfortable with this situation. Its consultation paper 25/25 highlights that it may be difficult to apply general outsourcing requirements to permissionless distributed ledger technology and says: 'To avoid restricting the use of permissionless DLTs, we propose that such use should not be treated as an outsourcing arrangement under SYSC 8.1.1.' Although the FCA specifies permissionless DLTs, we anticipate that this will be applied more broadly to include public, permissioned chains.

Since blockchains are general-purpose technology, regulating them directly as financial market infrastructure is the wrong approach, but that does not mean regulators are powerless to enforce standards of resilience, security and neutrality on the regulated institutions that leverage the technology.

Crucially, the FCA's language does not absolve firms making use of public blockchains from risk management responsibility. They are still expected to 'evaluate their internal operational controls for permissionless DLTs, following the operational resilience framework'. Some Layer 1s have labs and deployment foundations that, although they will not function as counterparties, can offer technical support and guidance for regulated institutions adopting the technology. Regulators should feel empowered to guide banks in setting appropriate risk management standards for working with public blockchains, just as they did when commercial banks began migrating their data to public cloud infrastructure from on-premises servers. Banks can be required to implement risk management standards even on services that are not provided by a traditional third party.

Regulated issuers of tokenised securities can still meet their regulatory obligations by leveraging token, wallet or account standards that deliver the requisite controls to meet their obligations. They can also be required to prevent their asset operating or being transacted on any exchange or platform that does not adhere to appropriate requirements, including anti-fraud and market abuse regulations.

INTEGRATION REMAINS A CHALLENGE

The core breakthroughs required for public blockchains to provide the settlement infrastructure for capital markets have already been made. The challenge now is integration. While all the functions are technically feasible, the process of testing them and tuning them to meet the exacting standards of regulated financial markets is almost as difficult.

The public sector must play a role here. Just as determining settlement is a legal function as much as a technical one, the public sector will set the standards expected of the settlement infrastructure for regulated financial instruments. Part of their responsibility will be to clearly define their expectations of what features and functions such infrastructure should have.

This report has laid out the broad areas that these expectations should cover. Industry groups like the Global Blockchain Business Council have published detailed guidance on specific areas.

As well as setting expectations and standards, regulators need to design testing frameworks, labs and sandboxes to trial solutions, prove that they work and develop a clear, quick roadmap towards unfettered use. Initiatives like the European Union's DLT Pilot Regime and the UK's Financial Conduct Authority's Digital Securities Sandbox will be an important step towards building a shared understanding of the capabilities of the technology for regulated finance.

For the financial community, risk management principles are key when embracing a new technology. Regulators and central banks should work with industry experts to come up with a series of risk management questions to ensure that banks are able to effectively perform their due diligence on public blockchain protocols with which they wish to interact.

Finally, establishing shared standards for interoperability will give private sector market participants the confidence to invest in the time and expertise necessary to develop their systems without being concerned about the possibility that they are wasting resources on a standard that will not be widely used. If the public sector takes an active hand, discussing with experts in the private sector, they can help the industry to coalesce around shared standards.

MINSAIT

The missing piece of the fragmentation problem

Interoperability will not come from a single dominant platform. It will depend on aligning technology, law and oversight to link diverse digital asset ecosystems, writes Vivian Clavel Díaz, head of open banking and digital currency initiatives at Minsait (Indra Group).

'Without common standards, failures can cascade, leaving regulators and market participants uncertain about outcomes and accountability.'

THE financial system is rapidly moving towards a digital-first model, where value exists as data on secure networks or through tokenised representations. This transition delivers efficiency and automation but also introduces a critical risk: fragmentation.

Networks, tokens and legal frameworks rarely interoperate seamlessly. Semantic inconsistencies compound the problem. Tokens that appear similar can carry differing rights, transfer restrictions or compliance obligations, preventing automated processing and trapping liquidity. Entitlement fragmentation adds a further layer: some ledgers confer ownership directly, while others merely reflect positions elsewhere. Misaligned systems disrupt settlement and escalate disputes.

Fragmentation is therefore a structural risk. Without common standards, failures can cascade, leaving regulators and market participants uncertain about outcomes and accountability.

The early internet faced similar challenges. The Defense Advanced Research Projects Agency's initial networks were fragmented, until open collaboration produced shared protocols like Transmission Control Protocol/Internet Protocol. This process, built around the Request for Comments framework, wasn't smooth – commercial interests clashed and the transition was disruptive. But the result was a universal, scalable foundation.

Digital finance needs a similar approach. The incentives are misaligned, with private networks competing for users, regulators seeking control and different jurisdictions enforcing conflicting rules. Still, the lesson holds: interoperability won't emerge organically. It must be built through developing deliberate, co-operative standards.

Consistency, transparency and industry leadership

The goal should not be to impose a single universal token standard. Instead, the industry needs a meta-protocol – a common legal and technical framework that allows different token models to communicate.

Machine-readable asset schemas are key. These schemas define an asset's properties, settlement rules and relevant legal references in a structured format. With this shared 'language', networks can automatically verify asset validity, reconcile positions and enforce compliance across platforms.

The Internet Engineering Task Force's Secure Asset Transfer Protocol shows how gateways can move tokens between networks while checking pre-agreed rules. A broader meta-protocol could extend this concept, connecting diverse systems without forcing them to abandon their native designs or governance.

This requires a shared responsibility model. Industry participants build and maintain the technical infrastructure, while regulators and standards bodies define the overarching rules.

Two answers to 'who owns what?'

The legal dimension is equally important. In representational models, the ledger is merely a mirror of an external register, requiring constant reconciliation. Constitutive models make the ledger itself the source of truth, enabling seamless transfers and automation – but only if strict legal safeguards are in place.

Jurisdictions are beginning to test ledger-native registers. Spain's Entity Responsible for Enrollment and Registration framework, for instance, gives distributed ledger technology-based records the same legal standing as traditional systems, with regulated entities ensuring accuracy and finality.

This creates a trade-off: achieving legal certainty often means introducing centralised accountability, which clashes with the decentralisation ethos of many blockchain systems. Policy-makers and industry leaders must confront this tension directly.

Code into contracts, contracts into law

Tokenised assets are moving from experimental projects to core components of financial infrastructure. To scale safely, the industry must solve both semantic and entitlement fragmentation.

Machine-readable asset profiles can standardise how tokens are understood by systems and regulators. Clear entitlement models define who owns what, under what rules. Together, these form the foundation for genuine, auditable interoperability.

This is not a one-time technical fix; it is a long-term strategy requiring open standards, clear laws and coordinated oversight. By building this foundation now, the financial industry can replace today's patchwork of bespoke systems with a mature, integrated digital economy.

DMI OMFIF Digital Monetary Institute

BECOME A MEMBER

Get in touch to join our exceptional network and shape the future of money and capital markets

For more information, please contact:
Folusho Olutosin, Commercial Director
Digital Monetary Institute
Folusho.Olutosin@omfif.org

ripple

Retooling the public blockchain ecosystem

'With a public blockchain, anyone can participate, avoiding silos and creating a much more diverse and vibrant set of developers building solutions and tooling for them.'

Matthew Osborne, policy director, Europe, at Ripple speaks to OMFIF about regulatory obligations and concerns on public ledgers.

OMFIF: You're representing Ripple. What is Ripple and what does it do?
Matthew Osborne: Ripple is the leading digital assets infrastructure provider to financial institutions. We have several different products. First, there is our payments network, which is powered by crypto, specifically the XRP token. Second, we have a custody solution, which is software that institutions can use to securely custody digital assets. Then we have Ripple USD, which is our US dollar stablecoin with a market cap approaching $900m. It is regulated by the New York State Department of Financial Services and it's available globally, subject to local regulation. Most recently, we've announced that we're purchasing a prime broker, Hidden Road, so we will be able to offer both crypto and traditional brokerage services through that. Finally, we work with partners to support the tokenisation of assets on the XRP Ledger.

OMFIF: Tell us more about the XRP Ledger.
MO: The XRP Ledger was one of the first distributed ledgers. It was launched over 13 years ago. It's been operating continuously since then without any major outages or security failures. From the start, it was designed to be suitable for institutional use.

It's a public permissionless ledger meaning that anyone can view the transactions on the network, anyone can build applications on the network and anyone can participate in validating transactions.

OMFIF: Institutions must require some flexibility around that to comply with regulatory obligations?
MO: There can certainly be occasions when regulated financial institutions need to be able to apply elements of permissioning, even if the underlying ledger is permissionless. So, for example, a stablecoin issued on XRPL can have a level of permissioning applied directly to the token so that it can only be held by whitelisted wallets.

Or you can permission a whole domain – perhaps a trading or lending platform. That can be built on XRPL, and the whole application can have permissioning applied to it so that, for instance, only individuals that have completed a know-your-customer process can participate.

OMFIF: Regulators sometimes express concerns about regulated finance on public ledgers. Are these warranted?
MO: There certainly was a time a few years ago when there was scepticism about public blockchains. That is starting to change. Regulators and financial institutions are starting to recognise that not all public and permissionless blockchains are the same.

The functionality around being able to control or screen validator communities was a major one – we've already discussed that functionality. Another major concern was around probabilistic settlement, where transactions on some chains could theoretically be undone after settling. That is not an issue for many chains though, including XRPL, on which the settlement is deterministic, which is a key requirement for financial markets.

OMFIF: But if you get these benefits with private chains, why not use them?
MO: With a public blockchain, anyone can participate, avoiding silos and creating a much more diverse and vibrant set of developers building solutions and tooling for them. It's a really valuable ecosystem that supports innovation. It also potentially opens up the largest community for participants, which offers the best liquidity.

OMFIF: Are regulators sometimes concerned that decentralised governance will lead to unpredictable changes in how the ledger functions?
MO: The XRPL Foundation has a constitution under French law that governs how the ledger operates. It can be amended, but only certain participants can propose these amendments and there are rules about how those become accepted.

If regulators or those looking to build on the XRPL are concerned, I'd advise them to speak to Ripple and learn about how this process works. Regulators and market participants need to work together to adapt the technology for regulated use. We're big supporters of sandboxes where use cases can be explored in low-risk environments, so we'd encourage them to take an open attitude.

Driving public blockchain integration in banking

Be part of the working group

Although the benefits of blockchain for the financial industry are increasingly well understood, making use of public permissionless blockchains can still pose regulatory challenges for banks. Momentum is building to overcome the regulatory challenges preventing public blockchain adoption in the US, and we expect other countries to follow suit.

But if this process is to happen both quickly and safely, regulators and decision-makers at traditional institutions must understand the capabilities of public blockchain protocols in order to establish an effective policy framework. This means exploding some of the myths around public blockchains, demonstrating that they can provide a robust, scalable infrastructure for financial markets and identifying areas where existing regulations might prevent the adoption of blockchain infrastructure.

This working group will have the opportunity to be a key input for policy-makers during a time of dynamic policy formation. Members will be able to assert the robustness of public permissionless infrastructure and highlight their role as safe, responsible participants in the transformation of capital markets.

OMFIF
Public Blockchain
WORKING GROUP

omfif.org/pbwg

OMFIF

Public Blockchain

WORKING GROUP

Company Number: 7032533. ISSN: 2398-4236