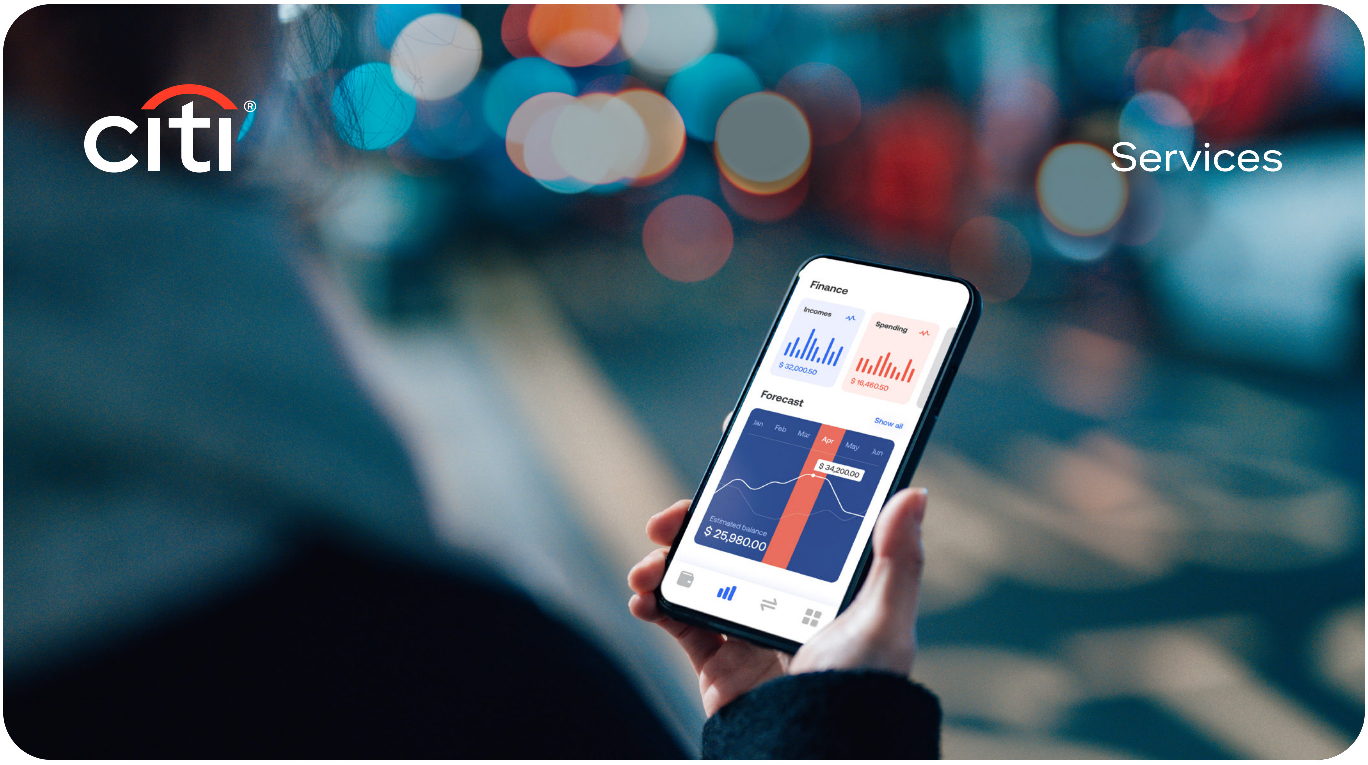


Ready Layer 1

A General-Purpose State Machine* for the Financial Sector

Introduction

In traditional finance, regulated financial firms and Financial Market Infrastructures (FMIs) use secure electronic messaging systems to exchange structured data pertaining to a wide range of financial transaction types. Coordination of financial transactions between firms is conducted through the messaging paradigm. Each institution updates its own books and records based on messages from clients and counterparties.

The development of blockchain technology presents the financial industry with an alternative paradigm based on 'tokenization'. Proponents believe that when financial instruments are tokenized they can be held and exchanged directly between participants more efficiently than can be achieved through current messaging systems alone.

This sets up a testable hypothesis that the 'tokenization' paradigm is superior to the prevailing 'messaging' paradigm.

'Tokenization' means different things to different groups. Adherents to the founding ideology of cryptocurrencies and public blockchains advocate for alternatives to sovereign currencies that would be censorship resistant and would have anonymous peer-to-peer transactions without central issuers or intermediaries.

This 'strong' form of tokenization needs to be modified for the regulated financial sector because several features could be said to be inconsistent with the current state of major jurisdictions' applicable regulatory regimes. It is not obvious that a technology developed as a radical alternative to traditional finance represents its future. A modified form of the tokenization thesis needs to be clearly articulated – one that could arguably fall within the prevailing regulation.

This article isolates a potentially compliant form of the tokenization thesis. This can be tested to determine whether there is a case for the industry to move beyond the current 'messaging' paradigm.

The analysis suggests that the 'messaging' paradigm might be augmented by a general purpose 'state machine'. The messaging paradigm generally does not provide participants with unambiguous, authoritative knowledge of the status of a financial transaction throughout its lifecycle. A tokenized system might provide that capability as well as support multi-asset and programmable operations.

The financial industry has already created secure, structured messaging as a general-purpose layer that serves thousands of firms on a global basis. Broad industry consensus would need to be achieved to build out a general-purpose tokenization capability (or state machine) to complement the existing messaging layer. This consensus can only be formed through a clear demonstration of the modified tokenization thesis, followed by concerted industry action to execute against any common vision that might emerge.

* The term state machine is a concept used in designing computer programs or digital logic. A state machine is any device storing the status of something at a given time. (Techopedia)

The Messaging Paradigm

In the traditional financial system, each regulated financial firm hosts financial instruments as liabilities and assets on its balance sheet. These instruments are varieties of claim. Deposits are claims on the institution; hence they are liabilities. The institution has assets in the form of claims against borrowers for the repayment of principal and interest and claims against the nation’s balance sheet in the form of government debt instruments.

When the financial system is built on a network of interlinked balance sheets, a core function is to know exactly who owes what to whom. The traditional financial system is a machine for keeping track of claims as they move from one balance sheet to another.

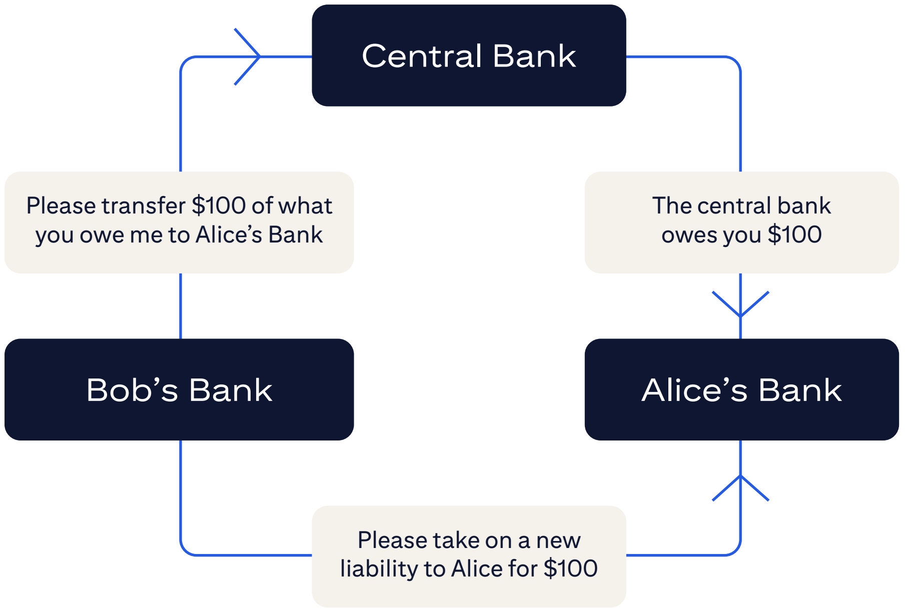
The books and records of an individual institution are maintained on proprietary databases running on data centers operated by each firm. Zoom out and consider the traditional finance ‘database of money’: thousands of institutions, each a self-contained balance sheet and a self-contained island of record keeping.

When institutions transact on behalf of clients, they send messages to one another. These can be bilateral messages through secure messaging infrastructures, or they can be routed through clearing houses that direct messages between multiple firms. The ultimate purpose of these messages is to transfer claims, to update the separate books and records – the balance sheets - of each institution that is party to a transaction.

When people speak of ‘sending money’, it prompts an image of something tangible moving; yet that’s not how payments work. A better way to understand payments is to think of them as transfers of claims from one balance sheet to another.

Illustration

A payment from Bob to Alice is a liability transfer from Bob’s bank to Alice’s bank. At the beginning of a payment, Bob’s bank owes him $100. At the end of the payment, Alice’s bank owes her $100. The claim has moved from one balance sheet to another.

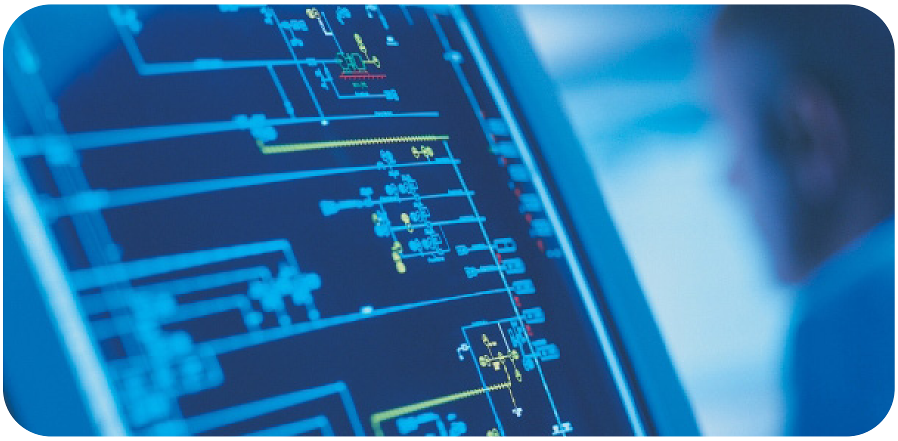

Central Bank
Please transfer $100 of what you owe me to Alice’s Bank
The central bank owes you $100
Bob’s Bank
Alice’s Bank
Please take on a new liability to Alice for $100

Alice’s bank will only accept an incremental liability if they receive a matching asset; so Bob’s bank will send a message to the central bank to facilitate an inter-bank transfer, and Alice’s bank will reflect the transfer of value to Alice’s account. This too is a transfer of claims. At the beginning of the transaction, the central bank owes Bob’s bank $100. At the end of the transaction the central bank owes Alice’s Bank $100.

In the payment of $100 from Bob to Alice, several messages have been sent, but only for the purpose of updating the records of claims on three balance sheets: Bob’s bank, Alice’s bank, and the central bank.

Traditional finance keeps track of constantly moving claims across a great global archipelago of thousands of individual firms, each updating its own balance sheet based on messages from its customers and other firms. As long as we have a world of many thousands of separate regulated institutions it will always be thus: financial transactions boil down to the synchronized updating of multiple separate balance sheets.

If the core function of the financial system is to keep track of who owes what to whom, then the question is whether the messaging paradigm is the best way to run the financial services railroad. Since the advent of blockchain technology, an alternative has appeared.



The ‘Strong’ Tokenization Thesis

The development of cryptocurrencies and public blockchains presents an alternative model for the transfer of value over electronic networks. The aim of crypto maximalists is to leverage strong tokenization in order to create an ‘internet of value’ where all kinds of tokenized digital assets can be transacted peer-to-peer on 24*7, resilient and secure networks that are self-governing due to the inbuilt economic rewards. Within the ‘strong’ tokenization thesis there are a number of design principles that warrant closer inspection.

Design Principle	Purpose
Trustlessness	An economic system can be built that does not rely on centralized authorities or intermediaries
Non-sovereign currency	A global form of digital money can be created that is not subject to debasement by nation states
Commodity forms of money	Avoid reliance on centralized issuers and intermediaries
Censorship resistance	Allow people to transact securely on an anonymous, peer-to-peer basis without risk of interdiction
Tokenomics	The system is self-sustaining through inbuilt rewards for participants ensuring the security of the system
Permissionless innovation	Provide open platform for new economic models to be built upon

This vision is not based on the network of balance sheets and transferable claims that comprise the world of traditional finance - it is the antithesis of that paradigm. The machinery of cryptocurrency is meant to provide an alternative to the world of trusted issuers and intermediaries.

What then is the logic that suggests the application of blockchain to traditional finance? Might it be an instinctual reaction by incumbents to co-opt a disruptive technology, or might there be a deeper synthesis between these two worlds that appear so different at first sight?

The answer emerges through the modification of the ‘strong’ tokenization thesis into something that might be consistent with the rules that govern regulated financial services. We can only uncover this modified thesis by casting off several inapplicable features of cryptocurrency and public blockchain.

> If the core function of the financial system is to keep track of who owes what to whom, *then the question is whether the messaging paradigm is the best way to run the financial services railroad.*

Stripping Back 'Strong' Tokenization

Regulated financial firms should operate within a set of laws or rules set by nation states and/or international bodies. These laws or rules generally create perimeters enclosing a 'controlled domain' within which a regulated financial firm may operate or carry out regulated activities or services. These 'perimeters' may change over time but in the current state, several attributes of 'strong' tokenization might be considered as inapplicable to regulated financial services.

'Strong' Tokenization Feature	Reason for inapplicability
Non-sovereign medium of exchange	Nation states consider sovereign currency to be an important instrument of self-determination and generally do not encourage substitutes that might undermine monetary policy.
Commodity forms of money	Credit forms of money represent the liability side of risk-taking balance sheets that drive economic growth. Unbacked cryptocurrencies are typically commodity forms of money that do not share this benefit.
Proof of work consensus mechanism	Achieving trustless consensus, which can sometimes require extravagant energy usage, is not required within a network of trusted regulated firms.
Anonymous transactions	Regulated financial firms must know their customers and provide data about transactions to combat financial crime. Compliance with Sanctions screening, Know-Your-Customer (KYC), anti-money laundering (AML), Travel Rule, etc., is not consistent with anonymous transactions.
Censorship resistance	Regulated financial firms operate in compliance within rules and regulations from national and supranational bodies including sanctions screening and AML measures.
Peer-to-peer transactions	Most regulated financial instruments are claims on an institution and their respective balance sheets need to be updated with each transaction. Bearer instruments are generally discouraged within a regulated environment due to the heightened financial crime risk.
Tokenomics	Regulated institutions need to comply with applicable laws (including laws relating to securities) and generally may not be keen to support the operation of FMIs through the creation of cryptocurrencies for sale to private individuals through cryptocurrency exchanges.

Proponents of the strong tokenization thesis would be aghast at the exclusion of these foundational features. One might wonder whether there is anything remaining of the tokenization thesis if these features are cast aside. However, even after stripping out these elements, there are potentially valuable features of tokenization that could be adopted by the regulated financial system. These are found by asking the question: what do blockchains do better than traditional finance?

The Modified Tokenization Thesis

While regulated financial firms might not quickly embrace anonymous peer-to-peer transactions over trustless networks that consume vast amounts of electricity, there are attributes of blockchain that might be usefully adopted by the formal financial system.

Beneficial Blockchain Feature	Description
Always-on operation	While blockchains operate 24*7, few traditional financial systems are always on. The largest traditional markets like foreign exchange (FX), money market, securities and derivatives, are bound within time windows. It might be argued that the nature of the 21st Century digital economy is 24*7 and that a financial system working on 'banking days' with 'cut off times' needs to be modernized. Adoption of blockchain might be one way to align the opening hours of the financial system with the digital economy.
Multi-asset operation	Traditional financial systems are built based on silos, which are special purpose systems for a subset of financial instruments. A Real Time Gross Settlement (RTGS) system only knows central bank money in one currency. A Central Securities Depository (CSD) only knows dematerialized securities in one legal jurisdiction. By contrast, blockchains have the potential to support the abstract representation of arbitrarily many digital assets on the same substrate. This could open new opportunities to settle transactions on a multi-asset basis on a common infrastructure.
State machine	Blockchains provide the participants to a transaction with unambiguous cryptographic proof of the state of the transaction. Shared clarity on the status of a transaction could ease reconciliation and remove breaks from traditional financial processes.
Programmability	The traditional financial system is not programmable in the sense that one cannot write computer code against it. In 'Turing complete' blockchains it is possible to write code in the form of smart contracts that can manipulate the multiple kinds of digital assets that exist on the network. This could lead to the creation of more flexible and more innovative financial services.
Resilience and security features	Distributed common infrastructure could provide the financial system with greater resilience than the current set up in which each firm runs its own proprietary infrastructure. Every transaction on blockchains is secured by strong cryptography and some public blockchains have proven themselves resistant to hacking over long periods of time.

This list of potentially important blockchain benefits available to the traditional financial system would appear to fall within the perimeters of the current state of major jurisdictions' applicable regulatory regimes. Subject to further legal and/or regulatory analysis to be considered, arguably, we would have the basis of a modified tokenization thesis that could be tested against the prevailing paradigm. A tokenized regulated financial system may therefore be a possibility and the potential benefits of such a system can be articulated.

The potential benefit of moving to the tokenization paradigm is in the *spirit of previous technological revolutions that moved from special purpose to general purpose technology.*

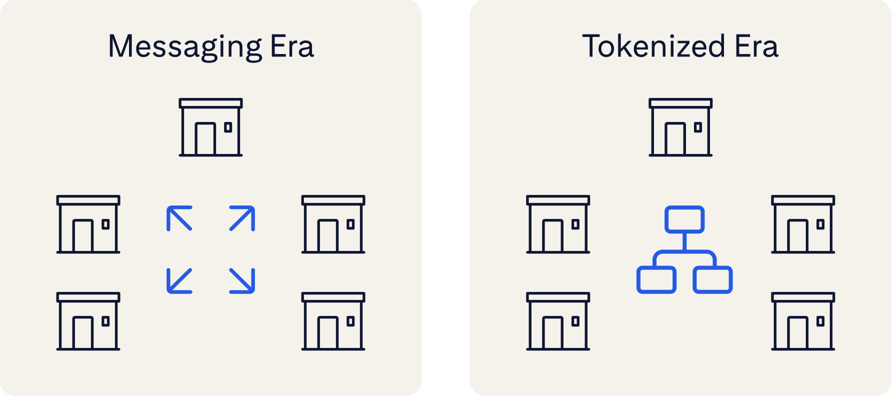
Tokenization Versus Messaging

So far, we have outlined the nature of the traditional financial system as one based on separate balance sheets recorded on separate databases. Claims on these balance sheets are transferred through messaging and settlement arrangements, with most financial transactions requiring updates to the separate balance sheets of each participating institution.

The development of cryptocurrencies and blockchains presents a different paradigm. The original 'strong' vision may not fall within the perimeters of the current state of major jurisdictions' applicable regulatory regimes, but there is a modified form of tokenization that could be considered.

What is interesting about this modified tokenization thesis when compared to the messaging paradigm? In the messaging paradigm, all the value is stored at the edges of the network, in the balance sheets of the institutions. There is no money or value in the messaging networks that connect the institutions.

In the tokenization paradigm, the value would be stored and transferred on the network itself. That network would operate 24*7, it would be programmable, distributed, and multi-asset.



The potential benefit of moving to the tokenization paradigm is in the spirit of previous technological revolutions that moved from special purpose to general purpose technology. There was a time when calculators could only perform arithmetical operations. The invention of general-purpose computers by Alan Turing represented the next stage in evolution – computers can perform arithmetic and do many more things besides.

This gives a sense of what proponents of tokenization believe to be the step change that might be coming to the traditional financial system: less silos, less cost, better resilience, greater security and most importantly a new wave of innovation.

The modified tokenization thesis can be tested, and the industry will have the luxury of choice between incremental improvements to the messaging paradigm and the creation of a new set of tokenized rails. In fact, these two worlds might prove to be complementary.

General Purpose Industry State Machine

There is a common root between the traditional financial system and the world of tokenization, even in its strong form. That root is 'who owns what'.

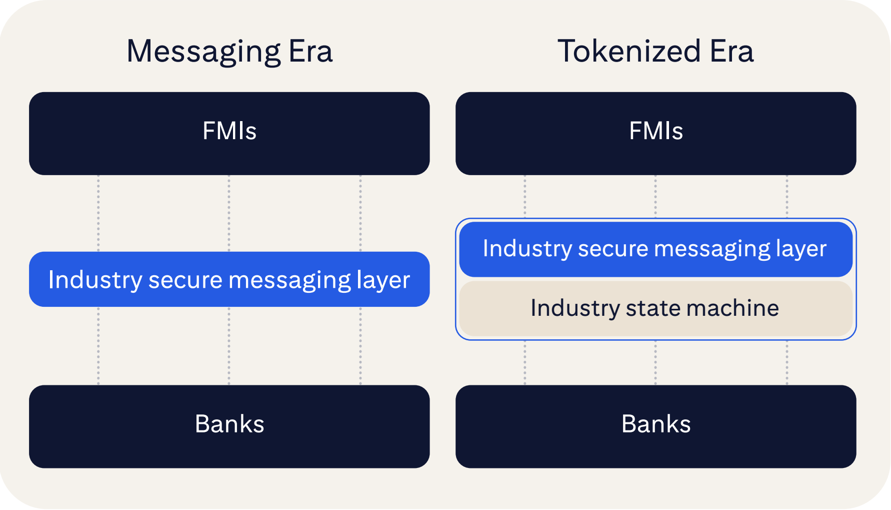
- **TRADITIONAL FINANCE:** regulated firms need to keep track of claims as they move from one balance sheet to another across separate institutions.
- **TOKENIZATION:** ownership of digital assets is tracked on the immutable ledger with every transaction movement secured by public/private keys.

Whether one thinks that finance should be built on the balance sheets of financial institutions, or on a trustless network where native digital assets are transacted without institutions, the heart of either system is an unambiguous record of ownership.

It may be that tokenization and blockchains could augment this foundational function of traditional finance better than messaging alone. Blockchains might point to the opportunity to add a new layer to the global financial system: a general-purpose state machine.

Blockchains are state machines – they are ways of keeping track of ownership as digital assets pass from one address to another. At present, there is no widely adopted general purpose utility available to all financial institutions that performs this role.

The presence of an industry state machine for regulated financial services is an intriguing possibility. In the messaging era we have secure, structured electronic messaging as an industry utility. What if there were a utility that gave the financial system an unambiguous record of the status of all kinds of financial transactions?



Such a utility would abstract the management of 'state' out of each individual institution, just as messaging has been abstracted out of bilateral connections and individual use-cases.

An industry state machine would be complementary to secure structured messaging because while connected, these layers do different things. The messaging layer needs to manage large data payloads that need to be transported from one institution to another. The state machine should not be encumbered by all this data. It only keeps track of transaction state throughout its lifecycle.

The potential benefits of such a utility can be thought of in the following way. If you want to organize a dinner party with 10 people, is it easier to manage that through email, or through a group chat? Most would agree that the latter is easier, but why? In the group chat the participants can see the current state of the arrangements, something which is much harder to see through bilateral messaging.

The potential development of an industry state machine arises from a close examination of the tokenization thesis and its modification to suit the structure of regulated finance. First it is necessary to strip back the strong form of tokenization into a proposition that is consistent with regulated financial services. The modified form of the thesis reflects on the remaining attributes of blockchains that might improve traditional finance: 24*7 operation, multi-asset capabilities and programmability. From this analysis we begin to focus into what functions blockchains might perform better than the prevailing messaging paradigm and find that the answer might be in the maintenance of state.

Applying this notion back to the regulated financial system, the suggestion is made that a general-purpose state machine available to FMIs and financial institutions around the world might provide the greatest scale of benefits, unlocking a wave of innovation through the provision of a new utility that complements existing messaging solutions.

Ready Layer 1

Financial institutions have been experimenting with blockchains for some time and there are several implementations in live production. To date there has not been adoption of blockchain technology in financial services by hundreds or thousands of firms.

A world of tokenized financial instruments will require such a scale of adoption, but this can only happen if there is broad industry consensus on what we are solving for.

Some experiments have demonstrated that blockchains can be used to support a given 'use-case'. Often this result is not surprising because blockchains that are 'Turing complete' are just computers, so they can emulate the same processing that already takes place on a different kind of computer. Such experiments only validate something that is already known and need not be reiterated, which is that one Turing machine can do the same work as another.

Mass adoption of tokenization requires the creation of an industry state machine – the adoption of a financial services Layer 1, or base protocol that facilitates interoperability.

Understanding how this might emerge requires another act of triage:

Industry Choice	Considerations
Public/Permissionless versus Private/Permissioned	When financial institutions use blockchains for record keeping, an outsourcing is going on. It may be more challenging for public blockchains to meet the requirements of Third-Party Risk Management (TPRM) than Private/Permissioned alternatives. The emergence of public blockchains that could address TPRM could change the dynamic.
One versus multiple providers	An industry utility could emerge through agreement across a critical mass of firms agreeing on a common technology. Alternatively, each firm/subset of firms could choose their own blockchain technology and bridges would need to be created between these islands.
To run a node or not	In a world of multiple blockchains, firms need to decide when to run nodes. In the current state of play, many firms choose to API into hosted nodes, perhaps undermining the notion of distributed ledger technology.

If public/permissionless blockchains are off limits for the time being and each firm chooses its own private/permissioned technology, then we are in a world of negative network effects. It becomes less likely that firms will run nodes as they will be in a position of having to pick a technological winner.

One way out of this bind would be through the emergence of a 'virtual Layer 1'. This would require interlinking of different private/permissioned blockchains in such a way that the resulting network acts as if it were a single technology from the perspective of the participants. The vendors in such an arrangement would enjoy positive network effects as the success of any participating vendor would grow the network.

Another option is for the emergence of industry consensus that there really is a missing layer to the global financial system. The benefits of industry utilities for secure, structured messaging are obvious in retrospect, but if we were to embark on such a project today it might fall foul of questions like, 'how do we avoid vendor lock in?'

The traditional financial services industry is at an inflection point. It can continue to incrementally improve the messaging paradigm while continuing to experiment with blockchain technology in a fragmented manner. Alternatively, it could attempt to articulate the tokenization thesis clearly as it applies to regulated firms and ask the question, is there a missing layer to the system? If there is industry agreement on where the gap is, there might follow industry action to fill it.

Tony McLaughlin

Author

Tony McLaughlin is responsible for Emerging Payments and Business Development in Citi's Treasury and Trade Solutions (TTS) business within Citi Services. He works on the future of money and the product-market fit between regulated finance and the modern digital economy.

His core interest is to ensure that Citi solutions and the wider regulated financial industry meet the emerging payment and settlement needs of digital native commerce:

https://icg.citi.com/icghome/what-we-think/treasury-and-trade-solutions/insights/strategies-for-three-sided-markets

He provides insights on the future of digital payments to Governments, Regulators, Fintechs, Big Techs, Multi-national Corporates and Financial Institutions and is the originator of the 'Regulated Liability Network' concept that explores the application of shared ledger technology to the sovereign currency system:

https://regulatedliabilitynetwork.org/

He joined Citi in 2004 and has been Cash Management Head for Asia Pacific based in Hong Kong and the Global Transaction Services Head for the United Kingdom, spearheading Citi's engagement with large public sector clients and payment aggregators. Tony was responsible for the design and development of ABN AMRO's Third Party Continuous Linked Settlement (CLS) offering, core electronic banking platform and Transactional Foreign Exchange solution.

At HSBC Holdings, he fulfilled a global strategy role for the Payments and Cash Management business, helping to set the five-year strategy. Before that he was a Senior Product Manager for Barclays Bank with responsibility for electronic collections products including International Direct Debits.

Contact: tony.mclaughlin@citi.com

Linkedin: https://www.linkedin.com/in/tony-mclaughlin-7b627a3/

Services
citigroup.com/global/businesses/services