Beyond Public Versus Private:
Connectivity and Control Within Regulatory Guardrails with Canton

(Working Paper)

January 2024

Manoj Ramia
General Counsel, Digital Asset

Tokenization promises billions of dollars in cost savings by improving settlement efficiency. But recent regulatory statements make clear that (1) for the benefits of tokenization to be fully realized, the blockchain network on which an asset is tokenized must provide ***connectivity*** *through an interconnected and interoperable network of networks and (2) for a tokenized asset to retain the same capital treatment as it has in non-tokenized form (and avoid a punitive capital charge), the blockchain network on which an asset is tokenized must provide* ***control*** *over key functionality of the tokenized asset.*

This requirement for both connectivity and control, however, does not fit within the public-versus-private blockchain dichotomy that dominates discussions around tokenization. To date, public blockchains have leveraged permissionless architectures to provide connectivity but at the expense of control. At the same time, private blockchains provide control but at the expense of connectivity. Either option requires a tradeoff between connectivity and control. Neither option is suitable if the benefits of tokenization are to be fully realized without impacting capital treatment. In light of this, the pursuit of tokenization—to improve settlement efficiency and gain billions of dollars in cost savings—seems quixotic.

However, with the Canton Network, public networks are no longer limited to permissionless networks; the public-versus-private blockchain dichotomy loses its relevance and the tradeoff between connectivity and control that was assumed to be inevitable in blockchain no longer needs to be made. Instead, with the Canton Network—a public, permissioned network—banks can be part of an interconnected and interoperable network of networks while still controlling key functionality of tokenized assets, allowing the benefits of tokenization to be fully realized while also allowing tokenized assets to retain the same capital treatment they have in non-tokenized form (and avoid a punitive capital charge).

1. Tokenization promises to improve settlement efficiency and save billions of dollars *only if* assets are tokenized using blockchain technology that enables *connectivity* through an interoperable network of networks.

Bank regulators are turning their attention to tokenization. The benefits are too big to ignore. As Acting Comptroller of the Currency, Michael Hsu, stated in a speech in June 2023:

> **The greatest promise for blockchain technology today may lie in its potential to improve settlement efficiency through tokenization of real-world assets** and liabilities on trusted blockchains. . . . Typically, there is a lag between when the terms of a transaction, such as price and quantity, are agreed upon and when all of the transaction components are performed, and obligations are fully discharged. That lag is due to the multiple entities and multiple steps that are typically needed for reconciliation and verification.

> Tokenization of real-world assets and liabilities has the potential to **improve settlement efficiency** by minimizing those lags and **thereby reducing the associated frictions, costs, and risks**. . . . With tokenization, the instruction, transaction, and settlement can theoretically be collapsed into a single step, removing those frictions—**provided, of course, that the technology is interoperable** with central bank money and real-world settlement systems.
>
> Some have estimated that tokenization of real-world assets could **save 35 to 65 percent across the settlement value chain**, including, for instance, **cost savings of up to $5 billion for equity-post trading**. (emphasis added).

Tokenization, however, does not happen in a vacuum (or a silo). Assets that are tokenized on a blockchain network that does not have any other participants, or that is not interoperable, are effectively dropped into silos where none of the benefits of tokenization can be realized. Settlement efficiency cannot be improved if there is no one to settle a transaction with.

Rather, as General Manager of the Bank of International Settlements, Agustin Carstens, noted in a speech on tokenization in November 2023:

> To harness the full benefits of tokenisation, we need all the components to work together seamlessly. The key here is to guarantee that **all the digital assets networks are interconnected and interoperable**. . . . The best way to knit together transactions and operations among markets and financial services is to bring them onto shared programmable platforms[,] . . . **a network of networks** that would allow various components of the financial system **to work seamlessly together**. (emphasis added).

Thus, tokenization promises tremendous benefits but *only if* assets are tokenized on interoperable networks.

2. Tokenized assets will retain the same capital treatment as they had prior to tokenization (and not incur punitive capital charges) *only if* assets are tokenized using blockchain technology that gives banks *control* over key functionality of the tokenized assets.

Though the connectivity of a blockchain network is important, banks cannot hold assets that have been tokenized on just any blockchain network if the assets are to retain the same capital treatment as they had prior to tokenization. Bank regulators have begun to make clear that the choice of technology impacts the regulatory treatment of tokenized assets. (For an in-depth discussion of this emerging regulatory framework, see *Uneven Terrain: Drawing a Regulatory Perimeter Around a Rapidly Evolving Digital Asset Landscape*, March 2023 (Selected as a "Must Read" paper for DC Fintech Week 2023).)

Most notably, the Basel Committee's December 2022 standards on the prudential treatment of "cryptoasset" exposures afford tokenized assets the same capital treatment as the non-tokenized form of the asset *only if* certain classification conditions are met. Among these is a classification condition that focuses on the functionality of the tokenized asset, requiring that "[t]he functions of the cryptoasset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are designed and operated to sufficiently mitigate and manage any material risks." The Basel Committee elaborates on these risks related to functionality as follows: "The functions of the cryptoasset, such as issuance, validation, redemption and transfer of the cryptoassets,

and the network on which it runs, do not pose any material risks that could impair the transferability, settlement finality or, where applicable, redeemability of the cryptoasset." In addition:

> All key elements of the network must be well-defined such that all transactions and participants are traceable. Key elements include: (i) the operational structure (ie whether there is one or multiple entities that perform core function(s) of the network); (ii) degree of access (ie whether the network is restricted or un-restricted); (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 (ie whether validation of a transaction is conducted with single or multiple entities).

Accordingly, the functionality of a tokenized asset, including the functionality of its underlying blockchain network, will determine whether the tokenized asset receives the same capital treatment as the non-tokenized form of the asset. If not, the tokenized asset will be treated the same as ordinary crypto and receive a 1,250% risk weighting.

Finally, even if all of the classification conditions are satisfied so that the tokenized asset receives the same capital treatment as the non-tokenized form of the asset, the Basel Committee's standards give regulators the discretion to nonetheless add an "infrastructure risk add-on" that "authorities can activate based on any observed weaknesses in the infrastructure on which cryptoassets are based."

While the Basel Committee's December 2022 standards make clear that the choice of blockchain technology matters when tokenizing traditional assets, the standards do not specify the implications of specific technology choices. Notably, the committee stated that it "will continue to reflect on whether the risks posed by cryptoassets [including tokenized assets] that use permissionless blockchains can be sufficiently mitigated to allow," in the case of tokenized assets, the same capital treatment as received by the non-tokenized form of the asset.

The Basel Committee completed this reflection in its December 2023 consultative document, concluding that an asset tokenized on a permissionless blockchain network should *not* get the same capital treatment as the non-tokenized form of the asset. Instead, assets tokenized on permissionless blockchain networks will be treated the same as ordinary crypto and receive a punitive 1,250% risk weighting. The committee reached this conclusion after determining "that the use of permissionless blockchains gives rise to a number of unique risks, some of which cannot be sufficiently mitigated at present." Specifically:

> Some of the most significant risks stem from the networks' reliance on third parties to carry out basic operations. Banks have limited ability to conduct due diligence and oversight over those third parties or prevent potential disruptions to the network. Similar analysis applies to political, policy, and legal risks, AML/CFT risks, and risks around settlement finality, privacy, and liquidity.

Accordingly, the committee will *not* "allow for the inclusion of cryptoassets [including tokenized assets] that use permissionless blockchains in Group 1 [which enables a tokenized asset to receive the same capital treatment as the non-tokenized form of the asset]," and these assets will instead be in Group 2, which receives a 1,250% risk weighting.

Reading the language above on the risks of permissionless networks together with the December 2022 prudential standards' discussion of risks to be accounted for regarding the functionality of tokenized assets and their underlying networks, the Basel Committee's concerns regarding permissionless networks appear to boil down to a concern over banks' resulting loss of control over key functionality

of tokenized assets such as control over who validates transactions, control over to whom a party is connected (impacting AML/CFT), and control over who sees what data when permissionless networks are used.

The Fed's February 2023 "policy statement" regarding participation in "crypto-asset" activities by certain of its regulated banks echoes this concern. While the policy statement "presumptively prohibits" these banks from holding "crypto-assets" (what we commonly think of as crypto) as principal, this prohibition does not generally apply to tokenized assets. Instead, a tokenized asset is afforded the same regulatory treatment as the non-tokenized form of the asset. However, this can change—and the tokenized asset may be treated the same as a "crypto-asset"—"[t]o the extent transmission using distributed ledger technology and cryptographic techniques changes the risks of a traditional asset (for example, through issuance, storage, or transmission on an open, public, and/or decentralized network, or similar system) . . . ." So for the Fed, as with the Basel Committee, the type of blockchain network on which an asset is tokenized matters. And while the Fed does not dive as deeply as the Basel Committee into discussing the specific risks raised by specific blockchain technologies, it is reasonable to surmise that the Fed is driven by the same concerns around permissionless networks, and the resulting loss of control over key functionality of tokenized assets, as the Basel Committee even though the Fed makes a broader reference to "open, public, and/or decentralized networks."

Finally, Acting Comptroller Hsu, in the speech quoted in section 1, is highly critical of public blockchains but—importantly—the key reasons for his (justifiably) harsh view are due to what he refers to as "trustlessness"—which can be thought of as network participants' delegation of key functionality to unknown third parties—and the permissionless nature of today's public blockchains —". . . the non-permissioned nature of public blockchains makes them attractive to criminals and others engaged in illicit finance, and full compliance with anti-money laundering rules is extremely difficult . . . .". Thus, the trustless and permissionless nature of today's public blockchains makes them unsuitable, in his view, for tokenization. In contrast, he praises "trusted" blockchains, which are "easily permissioned, making full compliance with AML rules achievable."

These regulatory statements show clearly that the choice of technology matters when looking to tokenize assets. For the Basel Committee, the Fed, and the OCC, the pivotal question to ask is whether using a particular blockchain technology to tokenize assets can introduce new risks and make the risk profile of the underlying asset worse than if it had not been tokenized. The Basel Committee (particularly with its December 2023 consultative document) drills down on exactly how and why the choice of technology can impact risk, making clear that central to this question of risk is *control*: how is control over key functionality of a tokenized asset (including control over who validates transactions, control over to whom a party is connected, and control over who sees what data) impacted by the underlying blockchain network? And this concern over control is shared by Acting Comptroller Hsu, as demonstrated by his preference for trusted, rather than trustless, blockchain networks. If a financial institution cannot control certain key functionality of a tokenized asset due to characteristics of the underlying blockchain network—specifically with permissionless networks—then using that blockchain network to tokenize assets can introduce new, unacceptable risks that would rightfully require harsher capital treatment for the tokenized assets.

But, as discussed in section 1, we also cannot lose sight of *connectivity*: without connectivity, the benefits of tokenization cannot be realized. Accordingly, for banks to realize the benefits of tokenization while retaining the same capital treatment for the relevant assets that they have today, banks will require a blockchain network that provides *both* control *and* connectivity.

3. The old dichotomy of "public" versus "private" blockchains.

Preserving control over key functionality while still leveraging the cross-institutional connectivity that blockchain promises has been a challenge. "Public" blockchains to date have also been permissionless, and thus have provided connectivity at the expense of control. "Private" blockchains provide control but no connectivity.

Inherent in the choice over whether to use a public or a private blockchain network—and the perceived tradeoff required between control on the one hand and connectivity on the other—is the assumption that all public blockchain networks are permissionless. Until the Canton Network, this assumption had been correct because public blockchains to date have only been able to offer connectivity by leveraging permissionless architectures.

Specifically, today's public, permissionless blockchains enable everyone to connect to everyone else by delegating key functionality to any number of unknown third parties. Moreover, because everyone on these public networks is in possession of the entire ledger for the network, every participant is able to see all of the data on that ledger, resulting in a complete loss of privacy. The resulting loss of control introduced by the permissionless nature of these public networks—including loss of control over who validates transactions, loss of control over to whom a party is connected (impacting AML/CFT), and loss of control over who sees what data—is a non-starter for any regulated financial institution looking to tokenize assets; it has justifiably drawn the scrutiny of the Fed and the OCC and warrants harsh treatment under the new Basel prudential standards.

Efforts to mitigate this loss of control in these public permissionless networks through so-called "layer 2" chains or application specific sidechains such as Polygon CDK appear to solve the control issue but at the expense of connectivity. While a layer 2 affords users some increased measure of control (but not complete control) over key functionality, it comes at the expense of data persisting outside of the main ledger, creating a new silo within which data needs to be reconciled; this clearly defeats the purpose of using blockchain technology. Moreover, by needing to connect into a public permissionless chain, these layer 2 chains nonetheless still present the same concerns as using the public permissionless chain itself because of the resulting loss of control over key functionality; any gains in control prove to be illusory. And efforts to overcome the limitations of these layer 2 chains through bridges introduce additional complexity and security risks without creating true interoperability.

The other way to reduce the control challenges of public permissionless blockchain networks has been to create a private blockchain network. But this simply amplifies the drawbacks of layer 2 chains. A small island is created where participants enjoy siloed connectivity with shared control over key functionality and data. While this is more palatable to regulators from a control perspective, an island is still an island and shared control is not full control. Moreover, the number of participants and types of use cases are inherently limited, providing only limited connectivity and thus limited benefit, with any benefits negated if a central operator is employed, as reconciliation is then required and the benefits of blockchain are lost.

Thus, if we were to exhaust our options with either the public or private blockchains available today, pursuing tokenization, and hoping to realize the benefits discussed at the outset of this paper, would seem quixotic. Only with *both* connectivity *and* control can tokenization have a transformative impact on the financial system. Unfortunately, until the launch of the Canton Network, blockchain technologies to date have only provided *either* connectivity *or* control, but not both.

We have been stuck with this tradeoff between connectivity and control because most blockchains today—whether public or private—suffer from the same fundamental design flaw: they replicate the *entire* ledger across all parties on a network, creating a single global ledger. This inherently results in

a loss of control over key functionality as everyone in the network is in possession of everyone else's information and, with public networks, each participant has effectively ceded control over key functionality to any number of unknown third parties.

4. The Canton Network: moving beyond the public-versus-private dichotomy by providing *both* connectivity *and* control through a public yet permissioned, privacy-preserving network of networks.

Canton (the name refers to Switzerland's cantonal, federalist governance structure) is a blockchain protocol that takes a unique approach to creating a global ledger among network participants that enables *both* connectivity *and* control.

This is possible because while other blockchain networks have their ledgers as their focal point, with the Canton Network, the network applications and participants are the focal point. Applications on the Canton Network are coded in Daml, a smart contract language that enables assets to be modeled in the context of rights and obligations and allows for workflows to be defined with granular permission over who sees what data and thus who is in possession of what data.

The Canton blockchain protocol leverages this granular permissioning to adopt a segmented data model where each participant on the Canton Network is only in possession of, and can only see, the data it is permissioned to see by a given Daml application, and each participant has *full control* over to whom it connects. At the same time, the Canton blockchain protocol ensures that the data stored and controlled by each participant is synchronized across all participants—without sharing that data with, or making it visible to, other participants—by creating a "virtual" global ledger: "The Canton protocol guarantees that the virtual ledger provides integrity, privacy, transparency, and auditability. The ledger is logically global, even though physically, it runs on segregated and isolated [nodes] that are not aware of each other."

When we talk about the Canton Network, we simply mean the universe of Daml applications that are capable of being discovered by a node in the network. Any node which is permissioned to join an application can do so, and any connection that is made across applications can happen, *only* to the extent application operators *choose* to permission such actions. As a result, the Canton Network creates a network of connectivity that is public in the sense that anyone can participate, yet also permissioned, by allowing participants to maintain control over key functionality, including control over who validates transactions, control over to whom a party is connected (impacting AML/CFT), and control over who sees what data.

This is not a novel idea. Canton is conceptually similar to the design of the Internet. The Internet is a network of networks, each permissioned according to its own controls. The Internet is public—anyone can access the network and anyone can discover public facing websites—but it is not permissionless. Each website or "application" is strictly permissioned. So it may be possible to navigate through your browser to a bank's website and log-in with your personal credentials, but it is not possible to discover all of the bank's customers' account balances.

Accordingly, though anyone can in theory participate in the Canton Network—much like anyone can connect to the Internet—the Canton Network is *not* permissionless because each participant in the network exercises complete control over its network activities, including which parties will validate its transactions, to whom it connects, and which parties can see what data. This ensures that participants tokenizing assets on the Canton Network have complete control over key functionality.

(In that same vein, while Canton Network participants can choose to connect to each other directly, they can also choose to connect to each other through common infrastructure. The first common

infrastructure for the Canton Network—the Global Domain, which is currently in its "testnet" phase—is intended to serve as decentralized, organizationally neutral infrastructure for participants on the Canton Network. Importantly, given the control offered by Daml and Canton, *the use of the Global Domain is entirely optional*; parties are free to bypass the Global Domain and connect to each other directly for regulatory or other reasons. The Global Domain is simply one, *optional*, component of the Canton Network, providing a convenience to network participants. Importantly, the existence of the Global Domain does not impact control over key functionality, including control over who validates transactions, control over to whom a party is connected, and control over who sees what data; this control is specified and preserved within a given Daml application and, as mentioned, the Global Domain can always be bypassed in favor of direct connections between participants.)

Like the Swiss federalist governance structure from which it takes its name, the Canton Network is not one monolithic network or ledger where everyone is connected to everyone else, where everyone is in possession of a global ledger, where all data is visible to everyone, and participants are forced to cede control over key functionality, all of which are the case with public blockchain networks that are also permissionless. Nor is it a closed system limited to a single use case and with limited connectivity like many private blockchain networks. Instead, it is a collection of Daml applications running on the Canton blockchain protocol that *choose* to connect to each other—it is *an interconnected and interoperable network of networks*—where each participant remains in control over key functionality, including control over who validates transactions, control over to whom a party is connected (impacting AML/CFT), and control over who sees what data. With this architecture, the Canton Network allows banks to realize the benefits of tokenization while avoiding the fatal flaws of permissionless networks that concern the Basel Committee.

5. Conclusion: The Canton Network—providing *both* connectivity *and* control with a public, permissioned network.

With the Canton Network, public networks are no longer limited to permissionless networks; the public-versus-private blockchain dichotomy loses its relevance and the tradeoff between connectivity and control that was assumed to be inevitable in blockchain no longer needs to be made. Instead, with the Canton Network—a public, permissioned network—banks can be part of an interconnected and interoperable network of networks while still controlling key functionality of tokenized assets, allowing the benefits of tokenization to be fully realized while also allowing tokenized assets to retain the same capital treatment they have in non-tokenized form (and avoid a punitive capital charge).