Canton Coin: A Responsible Approach to Digital Tokens[1]

To enhance interoperability on the Canton Network, Digital Asset has created the technology for an optional decentralized synchronizer for the Canton Network that includes a native utility token to pay synchronizer traffic fees and that can be minted by participants that provide infrastructure or applications for the synchronizer.

The first instance of this decentralized synchronizer technology is being deployed by leading market participants and is called the Global Synchronizer, and its utility token is called Canton Coin.

The Global Synchronizer is being deployed by market participants only after Digital Asset has spent ten years developing the underlying Daml and Canton technologies—and proving out the viability of these technologies through in-production use cases that process trillions of dollars in value—and only after almost a year of extensive testing by the market participants anchoring it.

The Global Synchronizer is not controlled by Digital Asset or by any of the market participants anchoring the Global Synchronizer. The Global Synchronizer is decentrally operated and governed by the market participants anchoring it; each market participant anchoring it independently operates an instance of the Global Synchronizer software and its consensus mechanism establishes an official output when at least two-thirds of these participants reach the same result. Governance will be coordinated through a new, independent entity under the Linux Foundation called the Global Synchronizer Foundation. And Digital Asset has made the synchronizer and token technologies available open source through the Hyperledger Foundation under Splice Labs.

Unlike other digital tokens, Canton Coin is not being sold in any initial coin offering. And Canton Coin is not issued by Digital Asset or by any market participant anchoring the Global Synchronizer. Instead, participants operating nodes connected to the Global Synchronizer will be able to mint Canton Coin in exchange for providing either infrastructure or applications for the Global Synchronizer. Canton Coin is designed so that its value will increase only if third parties develop and operate useful applications for the Global Synchronizer. Without these third party applications, Canton Coin will not have any value no matter the efforts of Digital Asset.

I.
Digital Tokens to Date—"Tokens First, Technology and Use Cases Later"

We are fifteen years from when Bitcoin first introduced a new paradigm for digital value transfer. Unfortunately, in that span of time, we have seen very few meaningful uses of digital (*i.e.*, native) tokens. Instead, false promises of technological revolution have jaded many observers and rightly drawn the scrutiny of regulators and policymakers. In the rush to push out digital tokens, it seems that many projects forgot two fundamental prerequisites for digital tokens to provide real value: technological readiness and the ability to solve real problems.

Instead, we have been given digital tokens that rely on immature technological foundations and that are unmoored from real world use cases. Rather than provide real world utility, they have simply served as regulatorily arbitraged capital raising vehicles. Unsurprisingly, these tokens have as a result been subject to rampant speculation and, in many cases, served as vehicles for fraud. "Tokens first,

[1] By Manoj Ramia, General Counsel, Digital Asset. Paper updated as of July 1, 2024.

technology and use cases later" has, at best, been an ineffective strategy for creating real-world value and, at worst, allowed bad actors to replay some of the most egregious episodes from financial history.

Use cases need to come first. And for better or worse, the potential use cases for natively digital value transfer are plenty. The financial system is saddled with inefficiencies. Information remains siloed both among and within institutions, resulting in data that remains unsynchronized across institutions. As a result, transaction settlement remains dependent on costly and slow reconciliation among participants. And though assets are now recorded on electronic ledgers, they remain as static ledger entries, and manual processes are required to issue assets and settle transactions. Only by demonstrating real potential to tackle these challenges can digital value transfer and its enabling technology—blockchain—have any longevity.

The right blockchain network can eliminate these myriad inefficiencies, resulting in tremendous cost savings and reduced risk, by enabling data to be synchronized across participants and automating critical workflows. And within these blockchain networks—when the technology is mature and the use cases have been proven out—digital tokens can provide real utility by enabling seamless value transfer and serving as a built-in mechanism to incentivize parties to operate applications and infrastructure.

II.
Digital Asset's Technology- and Use Case-First Approach

At Digital Asset, we recognized from the outset the importance of developing our technology and proving out use cases first. Digital Asset was founded in 2014 and our mission is to power connections across markets. Over the past ten years, we have diligently and methodically worked to develop our technology—our privacy-focused smart contract platform Daml and blockchain protocol Canton—to a mature state.

Daml enables the development of applications that model transactions in the context of rights and obligations, making it well-suited for applications that implement financial workflows.[2] While other blockchain application frameworks inherit the privacy properties of their underlying blockchain (*e.g.*, if the blockchain requires transparency for its integrity, then all data that runs through an application on that blockchain will be freely available to anyone who can connect to it), with Daml applications, integrity does not depend upon transparency and a developer can specify privacy rules for each unique piece of data that is handled in that application.[3]

Canton is a blockchain technology that takes a unique approach to distributing a ledger (its name is a reference to Switzerland's cantonal governance structure). Most blockchains today (including the Bitcoin and Ethereum blockchains) replicate the entire ledger across all parties in a network. Canton takes a different approach. With Canton, the entire ledger for a network of applications is *not* replicated across parties on the network and thus *not* publicly available. Instead, each user of a Daml application maintains a ledger of only the data it is permissioned to see by that Daml application.[4] The Canton protocol ensures that this data is valid and current.[5] As a result, everyone works from a unified ledger without being in possession of the entire ledger. Instead, each user is only in possession of their portion of the ledger. This is incredibly useful in financial workflows, where a unified ledger can eliminate costly reconciliation but where user application data nonetheless needs to be private. Canton enables the synchronization of data and transactions across independently operated applications and synchronizers, while implementing its unique privacy and control capabilities.

---

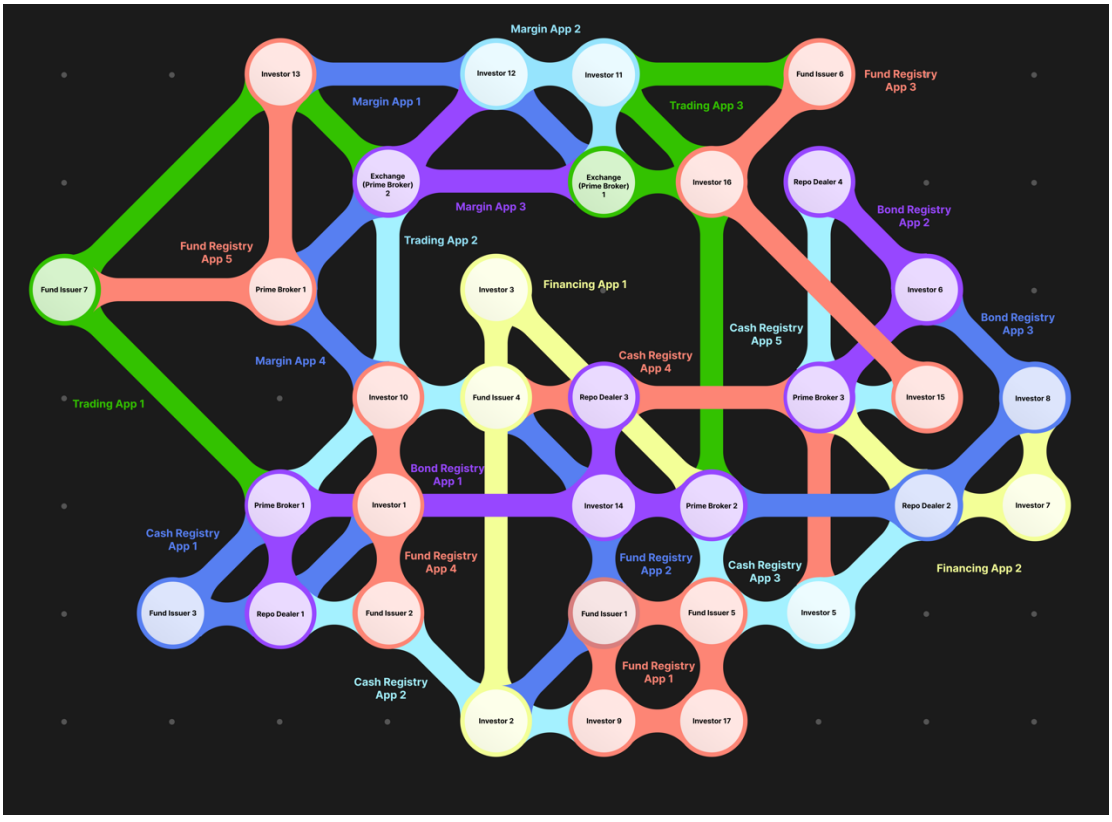
[2] https://docs.daml.com/concepts/ledger-model/ledger-daml.html#daml-defining-contract- models-compactly
[3] https://docs.daml.com/concepts/ledger-model/ledger-privacy.html#privacy
[4] https://docs.daml.com/concepts/glossary.html#private-contract-store
[5] https://docs.daml.com/concepts/glossary.html#virtual-global-ledger

Digital Asset has been unwaveringly focused on using these technologies to solve real problems. Daml and Canton are being used today in production systems at some of the world's leading financial institutions, enabling these institutions to reduce the issuance time of securities from days to seconds, reduce settlement risk, and increase efficiency. As just one example, Daml and Canton are being used to help process over $1.5 trillion of repo transactions per month, reducing millions in annual operating costs typically carried by market participants.

III.
The Canton Network

With our technology mature and with a demonstrated ability to solve real use cases, it was time to take the next step in our mission of powering connections across markets. On May 9, 2023, 30 institutions came together to announce the Canton Network.[6] The Canton Network—a public, permissioned blockchain network—is simply the universe of parties running Daml applications that can connect to each other through the Canton blockchain protocol. Market participants connected through the Canton blockchain protocol have the same control over key functionality they have today (allowing for strong privacy and permissioning) while benefiting from the real-time data synchronization and elimination of siloes that blockchain allows.

It is important to emphasize that the Canton Network is simply the universe of parties running Daml applications that are connected to each other through the Canton blockchain protocol; the Canton Network is not a single, monolithic network but rather a network of networks anchored by third-party applications. The figure below illustrates the Canton Network's application-centric, interconnected network-of-networks architecture:



[6] *Canton Network: A Network of Networks for Smart Contract Applications*, https://www.canton.network/whitepaper.

When two or more Daml applications want to connect to each other through the Canton blockchain protocol, what is needed is a mechanism for the data common to the applications to be synchronized in a privacy-preserving manner; this infrastructure is known as a Canton synchronizer. Synchronizers can be operated by any one of the parties seeking to interconnect their applications. However, there may be scenarios where none of the parties seeking to interconnect their applications is comfortable relying on any one party's synchronizer or otherwise seek to utilize a synchronizer provided by a third party.

IV.
Splice and Amulet: Technology for Decentralized Canton Synchronizers

A. Splice

To address this challenge, Digital Asset has developed the technology for a decentralized Canton synchronizer—"**Splice**." Admittedly, the term "decentralization" is often used in the blockchain space somewhat liberally and without precision. Here, however, we apply the label literally. A Splice decentralized synchronizer works as follows: third parties, each acting independently, operate an instance of the Splice decentralized synchronizer software on a node they control; these third parties are known as "**Super Validators**."

A Super Validator operating a Splice synchronizer node performs two functions. *First*, each Super Validator synchronizes all transactions that are processed through the synchronizer. "Synchronizing transactions" means ordering messages from nodes and applying a timestamp, and then collecting confirmations from nodes that they have validated the transaction, all without ever seeing the contents of those messages. *Second*, each Super Validator validates all Amulet token (described below) transactions (but does not validate any non-Amulet transactions) on the synchronizer. "Validating Amulet transactions" means confirming that the proposed transferor has sufficient tokens for the transfer and that the proposed transferee is a valid party as the intended transferee.

The Splice technology allows Super Validator nodes to configure the Canton blockchain protocol to perform all synchronization actions via byzantine-fault-tolerant consensus. This means that each Super Validator node automatically communicates with other Super Validator nodes until at least two-thirds agree on transaction order (for sequencing), confirmation (for validation on Amulet transactions), and any governance actions taken to change the Splice configuration. Accordingly, a transaction is sequenced, each Amulet transfer is validated, and each governance action is approved, when at least two-thirds of the Super Validators operating a given Splice configuration reach the same conclusion. Importantly, in performing its validation role, no Super Validator ever comes into possession of the token or otherwise stands in the middle of the transfer.

Thus, the Splice decentralized synchronizer technology is able to offer to Canton Network participants interoperability infrastructure that is not dependent on any single party. To ensure that decentralized synchronizers for the Canton Network can be developed without reliance on Digital Asset, the core code for Splice has been made available on an open source basis and is now maintained by Hyperledger Labs.[7]

B. Amulet

In constructing the architecture for Splice decentralized synchronizers, we saw a problem and an opportunity. In a decentralized system, incentivizing parties to participate, particularly by developing and operating applications or by operating infrastructure, can be challenging. (This problem is not new; credit card networks faced similar challenges in their early days and created incentives for

[7] https://github.com/hyperledger-labs/splice

participants to coalesce around a common set of standards and protocols and create a network of participants.) Moreover, without a native means of value transfer, it can be expensive to transact globally, across jurisdictions and foreign exchange lines. A native digital token could effectively address those problems. Accordingly, Splice includes the capability for a digital token, called "Amulet," which is also available through Hyperledger Labs as part of the Splice project.

Amulet tokens are generated through a minting protocol. Specifically, the token can be minted, according to the protocol rules, by each party operating a Super Validator node. In addition, parties that provide applications or other infrastructure for the synchronizer are also able to mint this token so long as they are operating what are called "validator" nodes.

The Amulet token utilizes a "burn-and-mint equilibrium" model. The four key features of this model are that (1) the minting of tokens is inflationary—the number of tokens minted continually increases over time, (2) fees for using the synchronizer (*e.g.*, the costs of utilizing a Super Validator) are "burned" (*i.e.*, removed from circulation) rather than transferred, (3) all fees on the synchronizer are denominated in USD, and (4) the token price is denominated in USD and can fluctuate based on market value.

To illustrate the burn-and-mint mechanism in action, consider the following example. If the fee to use the synchronizer is $0.01 per megabyte and the token-to-USD exchange rate is 100-to-1 (*i.e.*, the price of one token is $0.01), then a user will "burn" one token to cover the $0.01 fee. If there is a lot of demand to use a Splice synchronizer (*i.e.*, there are useful applications connected to it) and thus a lot of demand for the token, the token should increase in price and the token-to-USD exchange rate should decrease, leading to fewer tokens that need to be "burned" to pay that same $0.01 fee. Conversely, if there is not a lot of demand to use a Splice synchronizer (*i.e.*, there are not many useful applications connected to it), that should lead to a decrease in the price of the token and an increase in the token-to-USD exchange rate, leading to more tokens that need to be "burned" to pay the $0.01 fee.

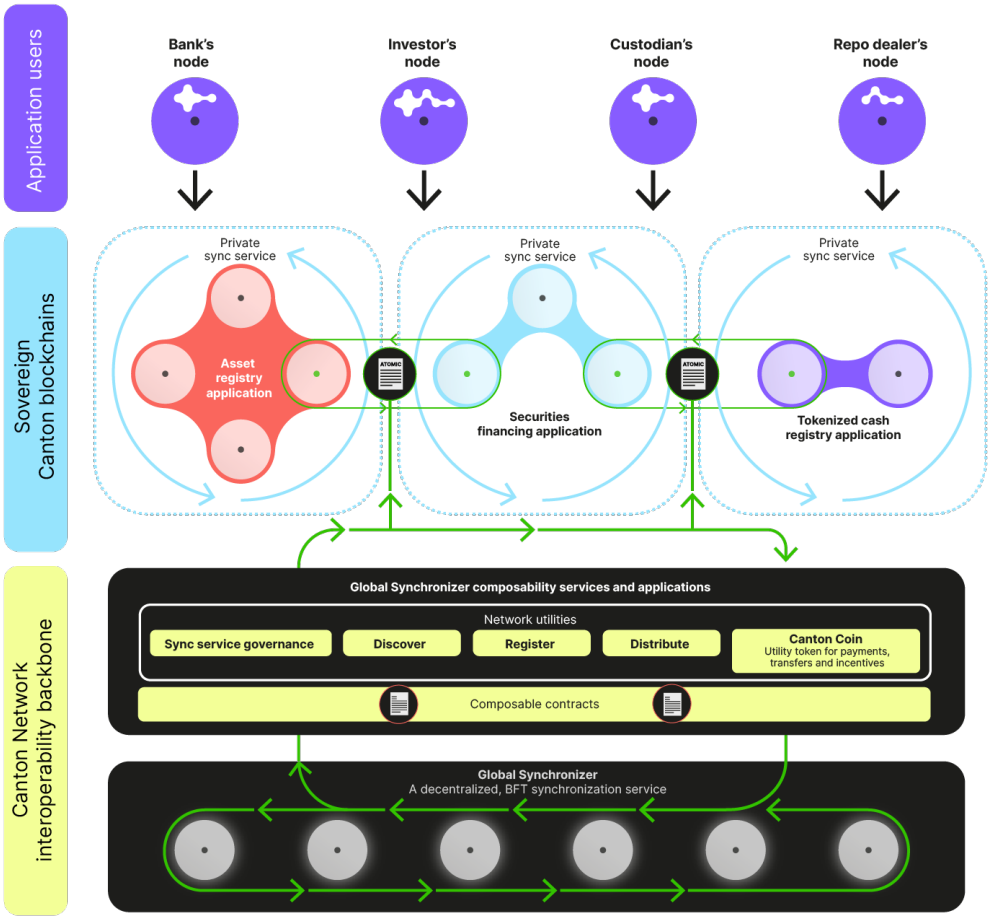
The upshot of this economic structure is twofold. *First*, the price of the token should reflect the true value of the network of applications connected to a Splice synchronizer over time because any speculative price swings will be dampened by fluctuations in the number of tokens that need to be "burned" to pay fees. And *second*, this model disincentivizes holding tokens purely for speculative reasons; because the supply of tokens will continually increase over time, unless tokens are removed from circulation via "burning" to pay fees, the constantly increasing supply of tokens will exert downward pressure on its price.

The operative parameters of the token—including the number of tokens to be minted over time, the timing and frequency of the intervals in which tokens can be minted, and the fees for using the synchronizer—are customizable for each implementation of a Splice synchronizer and are set by a vote of at least two-thirds of the Super Validators of a particular Splice synchronizer. Importantly, because fees are burned (and thus removed from circulation) rather than transferred to Super Validators, the Super Validators do not benefit from any particular value of fees (*i.e.*, the number of tokens each Super Validator can mint remains the same whether the fee is $0.01 or $100). In addition, the price of the token as denominated in USD will be set based on the median of the value provided by each Super Validator of a particular Splice synchronizer based on what each Super Validator understands to be the market price (but, importantly, this does not mean that any Super Validator acts to set any market price). The burn-and-mint mechanism disincentivizes the Super Validators from setting any of these parameters (number of tokens minted, fees, token price) at values that do not correspond to the actual demand for, and thus utility provided by, the network. If the values do not correspond to actual demand, then either too few or too many tokens will be burned, pushing the price of the token closer to a value reflective of its utility at a given fee structure.

V.
Splice and Amulet Implemented: The Global Synchronizer and Canton Coin

The Global Synchronizer is the first implementation of the Splice decentralized synchronizer technology. The Global Synchronizer entered its "TestNet" phase in August 2023 and entered "MainNet" (*i.e.*, processing live transactions) in June 2024. At the time it entered MainNet, thirteen parties were acting as Super Validators. This means that each of these thirteen parties have the right to independently operate an instance of the Global Synchronizer software, with the Global Synchronizer's consensus protocol determining the official output of the Global Synchronizer when at least two-thirds of the Super Validators reflect the same output. Accordingly, neither Digital Asset nor any other party operates or controls the Global Synchronizer. And just as importantly, the Global Synchronizer is not being jointly operated or controlled by the Super Validators and should not be thought of as such.

In this way, the Global Synchronizer is able to offer a reliable common infrastructure that is not dependent on any single party while enabling interoperability across connected Daml applications. The figure below shows how third-party applications can utilize the Global Synchronizer.



Use of the Canton Network's Global Synchronizer will always be optional; parties still retain the ability to connect and transact directly with each other by setting up their own private synchronizers (and may choose to do so as needed for regulatory or other reasons). And Daml smart contracts can be used to form multi-synchronizer workflows, allowing participants to utilize the most appropriate synchronizer for different legs of a transaction. Moreover, other parties may choose to set up their own

decentralized synchronizers utilizing the Splice open source codebase maintained by Hyperledger Labs.

And the Global Synchronizer will include the first deployment of Amulet, which will be called Canton Coin. Canton Coin is different from other digital tokens in a few key ways.

A. No Initial Coin Offering

First and foremost, Canton Coin is not being sold in any sort of initial coin offering. Instead, the primary way to obtain Canton Coin is by providing utility to the Global Synchronizer ecosystem. This can be done in one of three ways: operating a Super Validator, deploying a Daml application that connects to and uses the Global Synchronizer (each, an "**Application Provider**"), or operating a node that enables others to connect to the Global Synchronizer (each, a "**Validator**"). These parties will be able to mint Canton Coin through the Global Synchronizer's minting protocol (an implementation of the Amulet minting protocol described above) by performing their respective functions.

B. Digital Asset's Technology is Mature and Tested with Proven Use Cases

Second, unlike most digital tokens, which were launched in anticipation of, and as a mechanism to foster development of, a blockchain protocol and network infrastructure, Digital Asset has taken the opposite approach. We have already developed our blockchain protocol and network infrastructure. As discussed above, the foundational technologies for the Canton Network—Daml and Canton—have been in development by Digital Asset since 2014, and these technologies are already deployed today by some of the world's largest financial institutions. There is no question as to whether they are functioning and useful in the real world.

And the core technological infrastructure for the Global Synchronizer has also already been developed and is in such a sufficiently technologically mature state today that if Digital Asset were to stop making contributions to its codebase, the Global Synchronizer would still function. Notably, and as a testament to the Global Synchronizer's technological readiness, the "TestNet" version of the Global Synchronizer was made available in August 2023 and was used in late 2023 to support an unprecedented pilot program where 45 financial market participants came together to participate in 350 cross-application transactions, demonstrating the connectivity potential of the Canton Network for the capital markets industry.[8] The pilot demonstrated how multiple Canton instances can transactionally interoperate via the Global Synchronizer and execute cross-chain transactions without placing trust in a central operator, shared service providers, or competitors to exchange value between systems.

C. The Global Synchronizer is Operationally and Structurally Independent from Digital Asset

Third, in addition to being sufficiently technologically mature, the Global Synchronizer will also be *both* operationally *and* structurally independent from Digital Asset.

Operationally, the Global Synchronizer will *not* be operated by Digital Asset. Instead, as noted above, each Super Validator will independently operate an instance of the Global Synchronizer software and its actions will be mediated through the Global Synchronizer's consensus protocol.

To ensure that each Super Validator can carry its burden of operating its instance of the Global Synchronizer software, each of the Super Validators (including Digital Asset) has conducted extensive "practice" in the various aspects of operating the necessary software since TestNet was made available in August 2023, with the practices becoming significantly more intense in early 2024. And Digital

[8] https://www.canton.network/pilot-press-release

Asset has explicitly stated that it will not provide any support to the other Super Validators, further ensuring that the other Super Validators can operate the necessary software independently of Digital Asset.

Structurally, the Global Synchronizer will *not* be governed by Digital Asset. Any decision impacting the Global Synchronizer will instead require the approval of at least two-thirds of the Super Validators. This ensures that neither Digital Asset nor any other Super Validator can unilaterally make or block any decisions of the other Super Validators. The Super Validators have been operating under this decentralized governance protocol since late 2023 and have, as of July 1, 2024, voted on and approved over 20 proposals to improve the operation of the Global Synchronizer, including through code changes, configuration updates, and membership changes. Consequently, the Global Synchronizer entered "MainNet" after at least two-thirds of the Super Validators agreed to do so (the decision was in fact unanimous). Similarly, any new party seeking to become a Super Validator must obtain the approval of at least two-thirds of the then-existing Super Validators; neither Digital Asset nor any other Super Validator can unilaterally add a new Super Validator. To further ensure that the governance of the Global Synchronizer is truly independent of Digital Asset, it will be coordinated through an independent entity (not controlled by Digital Asset) called the Global Synchronization Foundation.

In addition, obtaining the software necessary to act as a Super Validator, Validator, or Application Provider will not require Digital Asset. Much of the core Daml and Canton code are already available on an open source basis. And, as noted above, the core code for the Global Synchronizer, including the code to enable Canton Coin functionality, will be available through the Hyperledger Foundation on an open source basis through the Splice project.

Finally, though certain of the software necessary to operate a Super Validator is proprietary and closed source, this software has been freely made available to each Super Validator on an irrevocable basis. Moreover, each Super Validator is permitted to distribute this software to any new Super Validator that is approved to join. And the source code for this proprietary software is being held in escrow and will be made available to the Global Synchronizer Foundation upon its formation. Together, this ensures that there is no dependency on Digital Asset for the Global Synchronizer to continue to operate and grow.

D. The Economic Model for Canton Coin is Designed to Disincentivize Price Speculation and Instead Encourage the Development of Useful Applications

Fourth and finally, Canton Coin implements Amulet's "burn-and-mint equilibrium" model, disincentivizing price speculation and instead incentivizing the development of useful applications for the Global Synchronizer. Specifically, as discussed above, if demand for the network is low, fewer tokens will be burned than minted, resulting in increased token supply and downward pressure on the price. The cheaper token will encourage network use and reassert upward pressure on the price, stabilizing it at a value reflective of utility. Conversely, if demand for the network is high, more tokens will be burned than minted, resulting in decreased token supply and upward pressure on the price. If the market price does not match the demand for the network, more tokens will be minted than burned and this inflation of supply should put downward pressure on the price, stabilizing it at a value reflective of utility.

The upshot of this economic structure is twofold. *First*, the price of Canton Coin should be reflective of the true value of the network over time because any speculative price swings will be dampened by fluctuations in the number of Canton Coins that need to be "burned" to pay fees. And *second*, this model disincentivizes holding Canton Coins purely for speculative reasons; because the supply of Canton Coins will continually increase over time, unless Canton Coins are removed from circulation

via "burning" to pay fees, the constantly increasing supply of Canton Coins will exert downward pressure on its price.

Moreover, the Canton Coin implementation of the Amulet model weights the minting distribution over the first ten years of the Global Synchronizer's operation equally between Application Providers on the one hand and Super Validators and Validators on the other hand.

Taken together, under this economic structure, Canton Coin will only be as valuable as the applications developed and operated by the Application Providers for the Global Synchronizer. Without these applications, Canton Coin will not have any value no matter the efforts of Digital Asset or any other Super Validator.

VI.
Canton Coin—A Responsible Approach to Digital Tokens

Ultimately, given the technological maturity of Daml and Canton, combined with their demonstrated ability to solve real problems, we developed the technology for Canton Coin because we genuinely believe that Canton Coin can serve as a true utility token for the Global Synchronizer, with its utility directly tied to the growth and utility of third-party applications that are connected to the Global Synchronizer. The solid technological foundation upon which the Global Synchronizer is built and the growing Canton ecosystem will encourage responsible use and serve as a strong counterweight to the speculative uses and abuses of other tokens because its value will grow only as third parties build useful applications that connect to the Global Synchronizer that enable meaningful value transfer.

***