Canton Coin (CC)
White paper

In accordance with Title II of Regulation (EU) 2023/1114 (MiCA)

N	Field	Content
0	Table of content	**Table of content** **2**

01	Date of notification	2025-09-09
02	Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The person seeking admission to trading of the crypto-asset is solely responsible for the content of this crypto-asset white paper.
03	Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omission likely to affect its import.
04	Statement in accordance with Article 6(5), points (a), (b), (c) of Regulation (EU) 2023/1114	The crypto-asset referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.
05	Statement in accordance with Article 6(5), point (d) of Regulation (EU) 2023/1114	false
06	Statement in accordance with Article 6(5), points(e) and (f) of Regulation (EU) 2023/1114	The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council. The crypto-asset referred to in this white paper is not covered by the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.
Summary		
07	Warning in accordance with Article 6(7), second subparagraph of Regulation (EU) 2023/1114	**Warning** This summary should be read as an introduction to the crypto-asset white paper. The prospective holder should base any decision to purchase this crypto-asset on the content of the crypto-asset white paper as a whole and not on the summary alone. The admission to trading of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and any such offer or solicitation can be

		made only by means of a prospectus or other offer documents pursuant to the applicable national law. This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to Union or national law.
08	Characteristics of the crypto-asset	**Summary of Characteristics of the crypto-asset** Canton Coin is the fungible, native utility token of the Canton Network's Global Synchronizer, the first decentralized and transparently governed interoperability service for the Canton Network. Canton Coin facilitates the transfer of value, provides incentives, and serves as payment for infrastructure costs on the Global Synchronizer. Rights and obligations of Canton Coin holders are subject to the Network's decentralized governance as described in "Governance" below. **Overview** Current smart contract networks suffer two constraints that significantly limit meaningful adoption by traditional financial institutions and other enterprises. First, they require every application to inherit the governance properties and the fully transparent privacy model of the underlying network. Second, applications compete for transaction throughput. The Canton Network is a smart contract network of networks that overcomes these limitations and enables each application provider to define their application's privacy, scaling, permissions, and governance, while being part of a broader decentralized public network. Accessibility and connectivity across subnets of the Canton Network will be supported by an infrastructure called the "Global Synchronizer", decentrally run by a group of "Super Validators". As part of the Global Synchronizer, the Super Validators launched a payment application called Canton Coin to facilitate the transfer of value, provide incentives, and serve as payment for infrastructure costs. Just as the Canton Network overcomes several of the key limitations holding back other networks from widespread enterprise adoption, Canton Coin is specifically designed to be compatible with an ecosystem used by regulated financial enterprises. **Motivation** The goal of the Super Validators is to build an ecosystem to foster and accelerate the creation of a "network of networks" of applications in regulated finance and other areas. A "backbone" infrastructure like the Global Synchronizer is an important part of doing so, but it is far from sufficient for starting an ecosystem. Networks acquire and deliver value through "network effects", where existing users and applications provide value to new users and applications, and vice versa. To incentivize the first users and applications to do something in the absence of that preexisting value, special mechanisms are needed to provide first-mover advantages. This includes the Super Validators themselves, which are providing the first services within this ecosystem, including the Global Synchronizer. Furthermore, ecosystems like the Canton Network benefit significantly from having both a means of transferring value, and publicly visible metrics for activity and use. To meet these needs, the Super Validators have included a payment and incentivization application in the launch of the Global Synchronizer's MainNet. The application is based on a token called Canton Coin, and each Super Validator independently runs an instance of the Canton Coin application. Canton Coin serves multiple purposes: 1. The Canton Coin application incentivizes all stakeholder groups to provide value, or more precisely utility, to the network. For example, third-party application providers can mint Canton Coin in return for offering their products and services via the Global Synchronizer, and Super Validators can mint

Canton Coin in return for running the network backbone.

2. The Canton Coin token provides an optional network-native mechanism to pay for network use. For example, the Super Validators operating the Global Synchronizer will allow the creation of transaction traffic balances across the Global Synchronizer using Canton Coin.

3. The Canton Coin token provides an optional network-native payment mechanism for application use. Any application provider can choose to charge application fees in Canton Coin. For example, the Canton Name Service, an application offering Validator name lookup and operated by the Super Validators operating the Global Synchronizer, will charge application fees in Canton Coin.

4. The Canton Coin token provides a public gauge of some aspects of network and application use. It gives visibility into the fees paid to different application providers as a proxy of the value that their applications provide to users.

5. The Canton Coin application provides an example of how to build public applications on the Canton Network.

Principles

Canton Coin is carefully designed to match the needs of a network and ecosystem for regulated finance, while at the same time allowing its users to achieve the goals stated under *Motivation* above. This is accomplished by following the set of key principles set forth below.

Reward Value to the Ecosystem

Canton Coin rewards utility provided by users of the Global Synchronizer. Canton Coin is not issued in exchange for investment. In contrast, most blockchain networks issue tokens in exchange for an investment in the developer of the network and in anticipation of future network value.

Most of a network's value comes from its users, assets, and applications. The bulk of Canton Coin can be minted by these stakeholder groups rather than just the Super Validators, again in contrast to most blockchain networks, where only "miners" can mine tokens.

Encourage Utility, Discourage Speculation

Infrastructure providers and application providers can mint Canton Coin only by providing utility to the network. There are no presales or special pools for "founders". Canton Coin could only be minted once the fully decentralized Global Synchronizer was running.

Furthermore, we avoid design choices that could lead to artificial scarcity or speculation bubbles. A stated goal, pursued through the "Burn Mint Equilibrium" mechanism explained below, is that an open market conversion rate for Canton Coin always tends to a point that matches the utility provided by the Global Synchronizer's ecosystem of users, infrastructure, and applications.

Optionality

Canton Coin is an optional token for users of the Global Synchronizer. This is in stark contrast to almost all other blockchain networks, where tokens are built into the protocol and cannot be avoided. For example, in Ethereum, Gas is paid in ETH as part of every transaction.

Participant node operators that want to connect to the Global Synchronizer *can* use Canton Coin to prepay their traffic directly, or they can arrange with a third party to set up a traffic balance (like a cell phone data plan paid in fiat currency) on their behalf. Canton participant nodes can then use the Global Synchronizer, with or without Canton Coin, by drawing down this traffic balance. Super Validators provide a small amount of transaction traffic for free, and any additional traffic is prepaid.

Besides serving as an optional method for purchasing transaction traffic, Canton Coin also provides an optional payment mechanism for application providers. Application providers can denominate their service fees in Canton Coin or in USD, and process these as Canton Coin payments via the Global Synchronizer.

Provide Signaling while Preserving Privacy

While most assets currently available on the Canton Network are private by default and visible to only the issuer, owner, and other permissioned parties, one of the design goals of Canton Coin is to provide public visibility of application use for those application providers who choose to share information about the volume of traffic their application processes. To this end, Canton Coin positions and transfers are publicly visible. These public transactions may be composed together with private transactions into a single atomic transaction. This composition does not alter the core privacy properties of the Canton protocol, and composed transactions preserve the privacy of all private sub-transactions (that is, the private, non-Canton Coin part of the transaction remains private).

Governance

All actions taken by Super Validators operating the Global Synchronizer, and Canton Coin application configurations and transactions, are subject to a ⅔ majority action of all Super Validators. This includes all parameters described in this paper, including the set of active Super Validators, the minting curve and rights split, fees, and protocol improvements.

High-Level Canton Coin Tokenomics

As discussed above, Canton Coins can only be minted in exchange for providing value to the network. This section covers how the ability to mint Canton Coin is made available to different users and roles over time, and what activities allow a user to mint Canton Coin and on what basis.

Roles

There are four main roles in the Canton Coin application:

1. User - anyone holding and transacting with Canton Coin via the Global Synchronizer. Users can choose to self-host participant nodes or use a participant node hosted by others.

2. Validator - a Canton participant node with the Canton Coin application installed. Validator nodes provide network access to users; validate both Canton Coin transactions and other installed applications' transactions, exclusively for the parties hosted on that participant node; and, in return, are able to mint Canton Coins.

3. Super Validator - a multi-component node, consisting of a Validator and also a Canton synchronizer node, that participates in the Global Synchronizer. Super Validator nodes validate every Canton Coin transfer via a ⅔ majority Byzantine Fault Tolerant (BFT) consensus; and offer the Name Service and a small number of other applications that support the Global Synchronizer and Canton Coin ecosystems.

4. Application Provider - A Validator operator that gives users, and their validator nodes, access to a Canton application that submits at least some portion of its transactions through the Global Synchronizer.

Minting Curve

Over the first ten years of operation of the Global Synchronizer, 100 billion Canton Coin can be minted, with availability split 50/50 between infrastructure providers and application providers. Following the first ten years, 2.5 billion Canton Coin can be minted yearly, with approximately 75% going to application providers and 25% going

to infrastructure providers.

The allocation of Canton Coin that can be minted by infrastructure providers is shared between Validators and Super Validators. Initially, this distribution will be biased towards bootstrapping the Super Validator network, as the Super Validators bear the costs of deploying and maintaining early infrastructure.

Over time, the allocation of Canton Coin that can be minted by Super Validators will decrease significantly after the first few years of the Global Synchronizer's operation. Five years after launch, the pool of Canton Coin that can be minted by Validators will be larger than the pool available to Super Validators.

The Canton Coin Minting Curve is below:

Canton Coin Minting Curve					
Years	Rate / Year	Total Minting	Application %	Validators %	SV %
0-0.5	40b	20b	15%	5%	80%
0.5-1.5	20b	20b	40%	12%	48%
1.5-5	10b	35b	62%	18%	20%
5-10	5b	25b	69%	21%	10%
10 yr Cumulative	10b	100b	50b	15b	35b
10+	2.5b	2.5b/yr	75%	20%	5%

09	Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability	N/A
10	Key information about the offer to the public or admission to trading	The Canton Foundation is seeking admission to trading of the Canton Coin token in the EU with a view to facilitating broad distribution and increased liquidity of the token to promote greater participation in the Canton Network. The token is expected to initially be listed in the EU on Kraken (i.e., on the EU crypto-asset trading platform operated by Payward Global Solutions Limited), and may also be listed on other crypto-asset trading platforms in the future.

Part I – Information on risks

I.1	Offer-Related Risks	**General Risk Factors Associated with Crypto-Asset Offerings** The admission to trading of crypto-assets, including Canton Coin, is subject to general risks inherent to the broader cryptocurrency market. **Market Volatility** The value of Canton Coin may experience substantial fluctuations driven by investor sentiment, macroeconomic developments, and market conditions. **Regulatory Risks**

		Changes in legislation, applicable laws, compliance requirements or the implementation of new regulatory frameworks could affect the availability, trading, or use of such assets.
		Security Risks
		The risk of exploitation, hacking or security vulnerabilities of the underlying protocol and/or contracts of the token leading to a loss.
		Reputational Risks
		The potential for damage to an organization's credibility or public trust, which can negatively impact stakeholder confidence and overall business viability.
I.2	Issuer-Related Risks	**No Issuer**
		Canton Coin is not issued by an identifiable entity and was not sold in any initial coin offering. Instead, participants operating nodes connected to the Global Synchronizer are able to mint Canton Coin directly from the protocol in exchange for providing either infrastructure or applications for the Global Synchronizer. Consequently, because Canton Coin has no identifiable issuer and is minted through the operation and use of a decentralized blockchain protocol, there is no issuer against which to seek any recourse.
I.3	Crypto-Assets-Related Risks	**Market Volatility**
		The crypto-asset market is subject to significant price volatility, which may affect the value of Canton Coin. Prices can fluctuate rapidly and unpredictably due to various factors, including market sentiment, economic indicators, technological developments, regulatory news, and macroeconomic trends. This high level of volatility may lead to sudden gains or losses and can impact the liquidity and tradability of the crypto-asset.
		Liquidity
		Liquidity refers to the ability to buy or sell a crypto-asset without causing significant price impact. Canton Coin may experience periods of low liquidity, meaning that it could be difficult to enter or exit positions at desired prices or volumes.
		Reduced liquidity may result from limited market participation, exchange restrictions, or broader market conditions. This can lead to increased price volatility, slippage, and difficulty in executing transactions.
		Cybersecurity & Technology Risks
		Risks arising from vulnerabilities in the blockchain technology used by the project or platforms. Example risks include smart contract exploits, compromise of platforms, forking scenarios, compromise of cryptographic algorithms.
		Custody & Ownership Risk
		The risk related to the inadequate safekeeping and control of crypto-assets *e.g.* loss of private keys, custodian insolvency leading to a loss.
I.4	Project Implementation-Related Risks	**Competition and Market Evolution**
		The blockchain sector is highly competitive. Other Layer-1 and Layer-2 networks (some backed by larger communities or resources) compete for the same user base and developers. If Canton Network fails to keep pace with technological advancements or to differentiate its offering, it could lose relevance, negatively impacting Canton Coin's utility and value.
		Adoption Risks
		The risk associated with the project not achieving its goals leading to lower than expected adoption, the impact leading to a reduced utility and value proposition.

I.5	Technology-Related Risks	**Smart contract risks**
		Canton Coin uses smart contracts to facilitate automated transactions and processes. While these contracts enhance efficiency and decentralization, they also introduce specific technical risks. Vulnerabilities such as coding errors, design flaws, or security loopholes within the smart contract code may be exploited by malicious actors. Such exploits could result in the loss of assets, unauthorized access to sensitive information, or unintended and irreversible execution of transactions.
		Blockchain Network Risks
		Canton Coin operates on a public blockchain infrastructure, which is maintained by a decentralized network of participants. The functionality and reliability of the crypto-asset are dependent on the performance and security of the underlying blockchain. Risks may include network congestion, high transaction fees, delayed processing times, or, in extreme cases, outages and disruptions.
		Additionally, vulnerabilities or failures in the consensus mechanism, attacks on the network, or protocol-level bugs could impact the operation and availability of Canton Coin.
		Risk of Cryptographic Vulnerabilities
		Technological advancements, such as quantum computing, could pose potential risks to cryptocurrencies.
I.6	Mitigation measures	**Technological Maturity**
		The Canton blockchain protocol is relatively mature compared to other blockchain protocols and is already in operation and is used by regulated financial market participants for live transactions.
		Open Source Codebase
		The core codebase for the Canton Network is all available on an open source basis under an Apache 2.0 license, enabling third parties to view and scrutinize the codebase for any vulnerabilities.
		Robust Decentralized Governance
		The Canton Network's decentralized public domain on which Canton Coin operates, the Global Synchronizer, is governed in a decentralized manner by multiple entities each acting independently, reducing the risk of a single point of failure. Misbehaving validators can be removed or slashed according to protocol rules, which helps mitigate consensus attacks. The on-chain governance mechanism allows the community to implement fixes or improvements if a vulnerability or critical issue is identified (subject to proposal and voting procedures), providing a path to mitigate unforeseen problems.
Part A - Information about the offeror or the person seeking admission to trading		
A.1	Name	Canton Foundation
A.2	Legal form	Non-stock corporation organized under the laws of the State of Delaware, United States of America
A.3	Registered address	548 Market Street, PMB 57274, San Francisco, California 94104-5401, United States of America
A.4	Head office	N/A
A.5	Registration Date	24 June 2024

A.6	Legal entity identifier	N/A
A.7	Another identifier required pursuant to applicable national law	SR# 20242961363
A.8	Contact telephone number	+1 814-359-6544
A.9	E-mail address	support@sync.global
A.10	Response Time (Days)	7 days
A.11	Parent Company	N/A
A.12	Members of the Management body	Melvis Langyintuo Executive Director 548 Market Street, PMB 57274 San Francisco, California 94104-5401 United States of America
A.13	Business Activity	The Canton Foundation's mission is to foster the development and growth of the Canton Network and facilitate its governance.
A.14	Parent Company Business Activity	N/A
A.15	Newly Established	Yes
A.16	Financial condition for the past three years	N/A
A.17	Financial condition since registration	The Canton Foundation was established on 24 June 2024 and therefore does not have historical financial data available for the past three years. The Foundation is funded by a combination of membership fees and Canton Coin rewards earned in connection with operating a Super Validator for the Global Synchronizer. The Foundation's financial resources are sufficient to support its current operations and limited business activities as described in A.13. The Foundation has no material outstanding liabilities, debts, or financial commitments and does not face any financial risks or uncertainties impacting its long-term sustainability.
Part B - Information about the issuer, if different from the offeror or person seeking admission to trading		
B.1	Issuer different from offeror or person seeking admission to trading	N/A – Canton Coin is not issued by an identifiable entity. Instead, participants operating nodes connected to the Global Synchronizer are able to mint Canton Coin directly from the protocol in exchange for providing either infrastructure or applications for the Global Synchronizer.
B.2	Name	N/A
B.3	Legal form	N/A

B.4	Registered address	N/A
B.5	Head office	N/A
B.6	Registration Date	N/A
B.7	Legal entity identifier	N/A
B.8	Another identifier required pursuant to applicable national law	N/A
B.9	Parent Company	N/A
B.10	Members of the Management body	N/A
B.11	Business Activity	N/A
B.12	Parent Company Business Activity	N/A

Part C- Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

C.1	Name	N/A
C.2	Legal form	N/A
C.3	Registered address	N/A
C.4	Head office	N/A
C.5	Registration Date	N/A
C.6	Legal entity identifier of the operator of the trading platform	N/A
C.7	Another identifier required pursuant to applicable national law	N/A
C.8	Parent Company	N/A
C.9	Reason for Crypto-Asset White Paper Preparation	N/A
C.10	Members of the Management body	N/A

C.11	Operator Business Activity	N/A
C.12	Parent Company Business Activity	N/A
C.13	Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	N/A
C.14	Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	N/A
Part D- Information about the crypto-asset project		
D.1	Crypto-asset project name	Canton Network
D.2	Crypto-asset name	Canton Coin
D.3	Abbreviation	CC
D.4	Crypto-asset project description	Current smart contract networks suffer two constraints that significantly limit meaningful adoption by traditional financial institutions and other enterprises. First, they require every application to inherit the governance properties and the fully transparent privacy model of the underlying network. Second, applications compete for transaction throughput. The Canton Network, a smart contract network of networks that overcomes these limitations and enables each application provider to define their application's privacy, scaling, permissions, and governance while being part of a broader decentralized public network. Accessibility and connectivity across subnets of the Canton Network will be supported by an infrastructure called the "Global Synchronizer", decentrally run by a group of "Super Validators". As part of the Global Synchronizer, the Super Validators will also launch a payment application called Canton Coin to facilitate the transfer of value, provide incentives, and serve as payment for infrastructure costs. Just as the Canton Network overcomes several of the key limitations holding back other networks from widespread enterprise adoption, Canton Coin is specifically designed to be compatible with an ecosystem used by regulated financial enterprises.
D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project	The Canton blockchain protocol was initially developed by Digital Asset Holdings, LLC ("Digital Asset"), a limited liability company organized under the laws of Delaware in the United States of America whose address is 107 Greenwich St., 17th Floor, New York, New York, 10006, United States of America. Digital Asset was founded in 2015, developed the Canton blockchain protocol, and led the launch of the network in 2024.

		The governance of the Canton Network is now overseen by the Canton Foundation, a non-stock corporation organized under the laws of Delaware in the United States of America whose address is 548 Market Street, PMB 57274, San Francisco, California 94104-5401, United States of America. Information on the Canton Foundation can be found at https://sync.global.
		The Canton Foundation oversees community and ecosystem growth, while Digital Asset and other contributors provide technical development and maintenance of the protocol.
		In addition to the Canton Foundation and Digital Asset, independent Super Validators, Validators, and developers worldwide contribute to the implementation and improvement of the Canton Network.
D.6	Utility Token Classification	false
D.7	Key Features of Goods/Services for Utility Token Projects	N/A
D.8	Plans for the token	Canton Coin is already used today by over 300 participants in the Canton Network's Global Synchronizer ecosystem to pay for traffic and application fees. The Canton Foundation is seeking admission to trading of the Canton Coin token in the EU with a view to facilitating broad distribution and increased liquidity of the token to promote greater participation in the Canton Network.
D.10	Planned Use of Collected Funds or Crypto-Assets	N/A
Part E - Information about the offer to the public of crypto-assets or their admission to trading		
E.1	Public Offering or Admission to trading	ATTR
E.2	Reasons for Public Offer or Admission to trading	The Canton Foundation is seeking admission to trading of the Canton Coin token in the EU with a view to facilitating broad distribution and increased liquidity of the token to promote greater participation in the Canton Network.
E.3	Fundraising Target	N/A
E.4	Minimum Subscription Goals	N/A
E.5	Maximum Subscription Goal	N/A
E.6	Oversubscription Acceptance	N/A
E.7	Oversubscription Allocation	N/A
E.8	Issue Price	N/A

E.9	Official currency or other crypto-assets determining the issue price	N/A
E.10	Subscription fee	N/A
E.11	Offer Price Determination Method	N/A
E.12	Total Number of Offered/Traded crypto-assets	N/A
E.13	Targeted Holders	ALL
E.14	Holder restrictions	None
E.15	Reimbursement Notice	N/A
E.16	Refund Mechanism	N/A
E.17	Refund Timeline	N/A
E.18	Offer Phases	N/A
E.19	Early Purchase Discount	N/A
E.20	Time-limited offer	N/A
E.21	Subscription period beginning	N/A
E.22	Subscription period end	N/A
E.23	Safeguarding Arrangements for Offered Funds/crypto-assets	N/A
E.24	Payment Methods for crypto-asset Purchase	N/A
E.25	Value Transfer Methods for Reimbursement	N/A
E.26	Right of Withdrawal	N/A
E.27	Transfer of Purchased crypto-assets	N/A

E.28	Transfer Time Schedule	N/A
E.29	Purchaser's Technical Requirements	N/A
E.30	Crypto-asset service provider (CASP) name	N/A
E.31	CASP identifier	N/A
E.32	Placement form	NTAV
E.33	Trading Platforms name	The token is expected to initially be listed in the EU on Kraken (i.e., on the EU crypto-asset trading platform operated by Payward Global Solutions Limited), and may also be listed on other crypto-asset trading platforms in the future.
E.34	Trading Platforms Market Identifier Code (MIC)	Kraken: PGSL
E.35	Trading Platforms Access	How investors can access the EU crypto-asset trading platforms on which the Canton Coin may be listed will vary depending on the requirements and terms and conditions of each platform. Investors should refer to relevant information provided by the relevant trading platform with respect to access and ability to transact in the Canton Coin via the platform.
E.36	Involved costs	The costs involved in relation to accessing the trading platforms on which the Canton Coin may be listed will vary depending on the relevant trading platform. Investors should refer to relevant information provided by the relevant trading platform with respect to access and transacting in the Canton Coin via the platform.
E.37	Offer Expenses	N/A
E.38	Conflicts of Interest	N/A
E.39	Applicable law	The applicable law governing the admission to trading of the Canton Coin on an EU crypto-asset trading platform, including any transactions effected in the Canton Coin by investors via the platform, will vary depending on the relevant trading platform. Investors should refer to the terms and conditions of the relevant trading platform.
E.40	Competent court	The competent court with respect to disputes or claims relating to the admission to trading of the Canton Coin on an EU crypto-asset trading platform, including any transactions effected in the Canton Coin by investors via the platform will vary depending on the relevant trading platform and the nature and location of the investor.
Part F - Information about the crypto-assets		
F.1	Crypto-Asset Type	Canton Coin is classified as a crypto-asset other than an asset referenced token or e-money token under MiCA, (EU) 2023/1114.
F.2	Crypto-Asset Functionality	Canton Coin serves multiple purposes: 1. The Canton Coin application incentivizes all stakeholder groups to provide value, or more precisely utility, to the network. For example, third-party application providers can mint Canton Coin in return for offering their products

		and services via the Global Synchronizer, and Super Validators can mint Canton Coin in return for running the network backbone.
		2. The Canton Coin token provides an optional network-native mechanism to pay for network use. For example, the Super Validators operating the Global Synchronizer will allow the creation of transaction traffic balances across the Global Synchronizer using Canton Coin.
		3. The Canton Coin token provides an optional network-native payment mechanism for application use. Any application provider can choose to charge application fees in Canton Coin. For example, the Canton Name Service, an application offering Validator name lookup and operated by the Super Validators operating the Global Synchronizer, will charge application fees in Canton Coin.
		4. The Canton Coin token provides a public gauge of some aspects of network and application use. It gives visibility into the fees paid to different application providers as a proxy of the value that their applications provide to users.
		5. The Canton Coin application provides an example of how to build public applications on the Canton Network.
F.3	Planned Application of Functionalities	All core functionalities are live.
A description of the characteristics of the crypto-asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article		
F.4	Type of white paper	OTHR
F.5	The type of submission	NEWT
F.6	Crypto-Asset Characteristics	See 08 above.
F.7	Commercial name or trading name	N/A
F.8	Website of the issuer	N/A
F.9	Starting date of offer to the public or admission to trading	Expected around 1 November 2025
F.10	Publication date	Expected around 1 October 2025
F.11	Any other services provided by the issuer	N/A
F.12	Language or languages of the white paper	English
F.13	Digital Token Identifier	N/A

F.14	Functionally Fungible Group Digital Token Identifier	N/A
F.15	Voluntary data flag	false
F.16	Personal data flag	true
F.17	LEI eligibility	N/A
F.18	Home Member State	Ireland
F.19	Host Member States	Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Iceland, Liechtenstein and Norway.
Part G - Information on the rights and obligations attached to the crypto-assets		
G.1	Purchaser Rights and Obligations	**Rights of Canton Coin Holders:** Canton Coin provides an optional network-native mechanism to pay for network use. For example, the Super Validators operating the Global Synchronizer allows the creation of transaction traffic balances across the Global Synchronizer using Canton Coin. Canton Coin also provides an optional network-native payment mechanism for application use. Any application provider can choose to charge application fees in Canton Coin. For example, the Canton Name Service, an application offering Validator name lookup and operated by the Super Validators operating the Global Synchronizer, charges application fees in Canton Coin. **Obligations of Canton Coin Holders:** There are no obligations imposed on Canton Coin holders. **Transferability and Trading:** Holders have the ability to transfer their Canton Coin tokens to others (on-chain) or to trade them on available markets at will. Ownership of Canton Coin carries with it the aforementioned access rights, and when a token is transferred, those rights pass to the new holder. The previous holder loses access once they no longer hold the token. This means all rights (which are usage rights) are fully transferable with the token.
G.2	Exercise of Rights and obligations	Holding, transferring or using Canton Coin for payments require no special procedures beyond having a compatible wallet.
G.3	Conditions for modifications of rights and obligations	All actions taken by Super Validators operating the Global Synchronizer, and Canton Coin application configurations and transactions, are subject to a ⅔ majority action of all Super Validators. This includes all parameters described in this paper, including the set of active Super Validators, the minting curve and rights split, fees, and protocol improvements.
G.4	Future Public Offers	N/A
G.5	Issuer Retained Crypto-Assets	N/A

G.6	Utility Token Classification	false
G.7	Key Features of Goods/Services of Utility Tokens	N/A
G.8	Utility Tokens Redemption	N/A
G.9	Non-Trading request	true
G.10	Crypto-Assets purchase or sale modalities	N/A
G.11	Crypto-Assets Transfer Restrictions	N/A
G.12	Supply Adjustment Protocols	See H.5 below.
G.13	Supply Adjustment Mechanisms	See H.5 below.
G.14	Token Value Protection Schemes	false
G.15	Token Value Protection Schemes Description	N/A
G.16	Compensation Schemes	false
G.17	Compensation Schemes Description	N/A
G.18	Applicable law	Canton Coin is not issued by an identifiable entity and was not sold in any initial coin offering. Instead, since the launch of the Global Synchronizer, participants operating nodes connected to the Global Synchronizer have been able to mint Canton Coin directly from the protocol in exchange for providing either infrastructure or applications for the Global Synchronizer. These participants are located in jurisdictions across the world. Thus, there is no single applicable law for Canton Coin.
G.19	Competent court	For the reasons stated in G.19, there is no single competent court for Canton Coin.
Part H – information on the underlying technology		
H.1	Distributed ledger technology	Canton Coin is implemented on the Canton blockchain protocol.
H.2	Protocols and technical standards	**Introduction** Several smart contract blockchain networks exist, but they all impose problematic constraints on assets and applications built on top of them. Specifically, on these

networks, (1) all assets and applications share all data permanently and publicly with all users, (2) interaction with assets and applications is all-or-nothing; application operators cannot easily control how different users interact with their applications, (3) applications compete for global network resources; application operators cannot independently scale or choose on which infrastructure to deploy. Furthermore, fees are interconnected and unpredictable, with increased usage in one application raising costs for all users.

In contrast, most of the world's assets are heterogeneous, and are governed by unique rules for how users and businesses transact with them. Operators of applications that interact with these assets need control over the privacy, scale, service availability, and infrastructure cost of their applications. As such, the limitations of existing blockchain networks prevent the onboarding of the bulk of the world's assets and processes into an interconnected network, reducing public blockchains' ability to build substantial network effects outside of crypto-native assets.

For illustration purposes, we contrast existing public blockchain networks with the most successful public network, the Internet. The Internet is a heterogeneous network hosting independently operated applications; e.g., Wikipedia is fully public and coexists with gated banking portals on the same public Internet. High-volume, low-value services co-exist on the same network as low-volume, high-value services. Each application provider has the sovereignty to control its application's unique permissions, fees, scale, service levels, and more. The Internet has unlimited horizontal scalability and grows with each application contributed to the network. As a service's traffic increases, the application provider adds resources; the growth of one service does not reduce the resources available to others. The heterogeneity of the applications found on the Internet helped it reach billions of users. Some users want to go to Wikipedia, and some want to access their banking portal; both go to the same place - the same Internet.

The lack of support for application heterogeneity in public blockchains has led to two significant negative outcomes. First, due to these networks' privacy limitations, only assets and data which can be part of the permanent public record are brought into public blockchains; we see experimentation with cryptocurrencies and non-fungible tokens (NFTs), but we don't see enterprises and governments bring traditional assets and records to public blockchains. Second, to overcome the contention on shared global resources, the bulk of application logic for blockchain applications is built 'off-chain' under the control of centralized application providers, meaning key functionality is operated off the shared network, negating the independent verifiability users expect of public blockchains.

Limitations of existing blockchain networks

Concretely, in Ethereum, and similar smart-contract networks, (1) data is fully transparent to anyone who can connect to the ledger, (2) there are strict, vertical limits on transaction capacity on layer 1, (3) layer 2s, rollups, and similar scaling channels lack transactional composability (4) issuers of assets forfeit control of that asset to a pool of pseudonymous validators. From a regulatory perspective, the data transparency and loss of control over assets make these networks unsuitable for use by financial institutions.

When smart contract applications hit transaction throughput limits, the results are catastrophic for the network and providers of smart contract applications on the network. For example, in 2017, Axiom Zen launched the wildly successful application CryptoKitties on the Ethereum network, exceeding 12% of all network transactions and causing massive network congestion. As a result, other applications on Ethereum at this time experienced very high fees and latencies. Following this, the company behind Axiom Zen built and commercialized a new blockchain, moving away from the network upon which it built its success, and fragmenting the market.

The scaling limitations of existing blockchains are not inherent to the synchronization of application data and state; the design of Canton avoids these limitations. Existing public blockchains force all applications through a single ordering service, even where this isn't necessary. But this bottleneck is not required; for example, the order of text messages in one messaging application should be independent of the order of a social network feed of another application. These two applications should have independent ordering mechanisms for their state. Likewise, a network of smart-contract applications should allow for a similar localization of transaction ordering.

However, ordering across these applications must also be possible, as necessary, to be an interoperable smart contract network. That requires a shared protocol to synchronize transactions composed across multiple applications. Current attempts to allow independent scaling with synchronization across applications, typically known as layer 2 protocols, rollups, and cross-chain bridges, add significant complexity and security problems, as evidenced by numerous recent hacks. In contrast, the Canton Network enables applications across multiple subnets to natively interoperate between them without requiring a layer 2 protocol or asset bridge.

Canton Network

The Canton Network is a network of networks for smart contract applications with heterogeneity and scalability properties similar to the Internet, giving application providers control over their applications.

Like existing blockchain networks, the Canton Network provides real-time synchronization of sensitive data across participants. It has the privacy of a private blockchain on a public network; applications on the Canton Network see a single public ledger. The Canton Network has an expressive smart contract language called Daml, which has programmable privacy built into every asset or piece of data. The Canton protocol allows each application to scale independently, increasing availability and keeping fees low.

Thus, the Canton Network fills a major gap in the public ledger space: it has smart contracts on a single virtual ledger, similar to Ethereum, Solana, Tezos, and many more, and it has built-in privacy with selective transparency, similar to the bitcoin lightning network and Zcash.

Daml

Daml is an open-source smart-contract language and framework designed to make it easy to develop, operate, and maintain multi-party applications in a way that preserves privacy and data consistency. More concretely:

1. Daml provides concepts to capture rules that govern real-world business transactions. This helps programmers focus on business logic only while avoiding common security pitfalls.

2. Daml allows to specify access and authorization policies within the smart contract code, making it easy to keep them in sync. Data is confidential by default, and access policies are easily defined so that the smart contract programmer can understand and maintain them effortlessly.

3. Daml supports application interoperability by enabling the composition of workflows into more complex ones, including when the workflows are already deployed across different applications on different networks. A party can unilaterally extend functionality by composing existing workflows into more complex ones. This ability for any party to extend functionality fosters organic growth of ledger usage and helps manage complexity. Daml enables the composition of workflows across a network of applications while maintaining the confidentiality and authorization requirements of each application.

4. Daml supports interoperability with other systems through integration

tooling, including auto-generation of bindings for common programming languages, bridges to other blockchains, and common standard and domain-specific libraries.

Contracts

Daml defines a contract as a codified agreement on a workflow between multiple parties on the network; these parties are called contract signatories. In addition, other parties may observe the contract; these are called contract observers. A party can be an individual entity signing with a private key or a consortium signing with a flexible multi-signature confirmation policy; as such, assets can be issued, and contracts can be signed by central parties, or consortiums.

Transactions

A contract is created as part of a transaction, making the contract active. A subsequent transaction may archive the contract, rendering it archived. To ensure consistency among network participants while maintaining each contract's privacy, we need transactions to exhibit two properties. First, we need a mechanism by which the different parties agree on the order of transactions to avoid diverging views. Second, various parties may be entitled to see distinct parts of the transaction based on the privacy definitions of the specific contracts; we call this sub-transaction privacy. Transactions must enable parties to have a partial view of the transaction, which they can verify, also known as a sub-transaction.

The state of active contracts is known as the Active Contract Set (ACS) and is derived from a transaction graph. Every transaction in the graph may archive and create contracts, referencing all contracts upon which it depends. New transactions are atomic changes appended to the end of the transaction graph. The transaction may consist of multiple sub-transactions, with different parties accessing different sub-transactions. As such, different parties observe a different subset of the global ACS.

This model is similar to the UTXO transaction model used in bitcoin and other public blockchains, with two notable differences:

1. No party sees the full transaction graph of the entire network; instead, each party sees a subset of the graph, also known as that party's view. This partitioning of the global transaction graph contrasts to other UTXO blockchains such as bitcoin and Cardano, in which every party can see the entire graph.

2. A transaction does not always archive referenced contracts. Whether a transaction archives an input UTXO or not depends on the application logic, and is defined in Daml using the keywords consuming and nonconsuming. This option to keep a referenced contract active is in contrast to bitcoin and others, in which referencing a UTXO always archives it.

Transactions are structured as trees; this enables workflows to compose: the trees of existing workflows become the subtrees of combined workflows. Each party can validate its subtree and ignore the rest of the transaction.

Said another way, the main difference between Canton's ledger model and that of other blockchains is that, in Canton, each party sees only a subset of the ACS and a subgraph of the global transaction graph, also known as the party's view. This party-specific view is always a valid ledger that can be verified locally by the party's node; a party need not trust any other party for verification. Upon receiving a transaction or sub-transaction, a party's node will verify three things: that the transaction is consistent with the party's view, that the transaction conforms with the logic written in the smart contracts, and that the transaction is properly authorized.

Beyond governing access control, we further utilize this partitioning of the ledger for parallel processing. Since transactions explicitly declare their dependencies, separate

infrastructures can process independent transactions in parallel; this allows the Canton Network to scale horizontally by adding capacity as network demand fluctuates.

This model poses two challenges:

1. We must ensure that different parties' views of the global ACS are consistent; in other words, for every contract, the various parties who see it must always agree on whether it is active or archived.

2. We need an application development model that makes it easy to work with these restrictive privacy controls. We will show how Daml achieves this.

Smart-contract language

Daml is a modern functional language featuring a static type system that can rule out many undesired behaviors and correctness errors at compilation time.

Developers define the data schema, workflow semantics, and transaction execution in contract templates. These are equivalent to object-oriented programming language class definitions and SQL database schemas. A template defines:

1. Arguments - data the contract stores

2. Choices - actions that parties can take on the contract. Choices are equivalent to methods in object-oriented programming classes or stored procedures in databases.

3. Authorization - signatories are parties who must authorize creating or archiving the contract; observers are other parties who can view the contract; controllers are parties who can take specific actions on the contract by exercising contract choices. A party can delegate its authority to another party to make particular choices. A party that delegates its authority sees whenever a transaction uses its authority.

4. Constraints - predicates that must hold for every contract of the template, denoted by the ensure keyword.

Example:

```
template Iou
  with
    issuer : Party
    owner : Party
    currency : Text
    amount : Decimal
  where
    ensure amount > 0.0
    signatory issuer, owner
    choice Transfer : ContractId Iou
      with newOwner : Party
      controller owner, newOwner
      do
        create this with owner = newOwner
```

By default, exercising a choice archives the contract. In the case of the Transfer choice above, it also creates a new contract with a new owner. As an improvement on

bitcoin's UTXO model and Cardano's eUTXO model, the developer can specify a choice as nonconsuming. Non-consuming choices do not archive the UTXO, thus reducing contention.

Daml's model of explicitly defining authorization enables manual intervention by a contract's stakeholders to rectify unexpected situations. Templates make it explicit where, how, and by whom intervention can happen during the execution, without requiring a priori knowledge of the exact type of intervention and without relaxing any security guarantees. Signatories can jointly agree to archive, upgrade, or create new contract instances as long as there is unanimous consent. If any of the signatory parties are consortiums, their consent is governed by the underlying consensus protocol of that party/consortium and may, for example, require a ⅔ supermajority instead of unanimous consent. Observers are parties entitled to be notified of, and can independently validate, any such changes but whose authorization is not required. All actions on contracts - their creation, archival, and calls to choices - are events in transaction trees and form a complete and non-repudiable audit log of all changes. This ability to change contracts post hoc, with the appropriate authorizations, enables application providers to upgrade data, processes, and operating procedures, due to unforeseen events. For example, to deal with regulatory or judicial decisions which require retroactive changes to business transactions.

Daml organizes templates in modules and packages. Packages can depend on other packages, including across applications which may be deployed to multiple networks. This ability to depend on packages across applications on different Canton subnets enables an open architecture, where parties can combine workflows with other parties like building blocks.

Ledger Model

Daml enables parties to exchange value (in the form of smart contracts) in a way that is unique among currently available technologies. A smart contract update is nothing more than an authorized and validated update to entries on a ledger. The fundamental challenge when trying to accomplish this update without a trusted, central intermediary is ensuring that the ledger entries reflecting the smart contracts are accurate and can be proven to a third party. A common approach to address this challenge is to decentralize the ledger among the parties on the network by requiring every party to hold and update a copy of the ledger for the entire network. A consensus mechanism is used to ensure accurate replication of the ledger to all parties. But this leads to networks devoid of privacy with hard caps on scalability.

Daml's ledger data model takes a different approach to address these privacy and scalability challenges. In Daml's ledger model, the ledger is not fully replicated among the parties; it is segmented according to privacy rules, and each party stores only its view, or shard, of the ledger. As a result, there is no ledger view common to all parties in the network. Instead, there is a ledger for each party that includes only the contracts of that party. As a result, instead of one ledger that all of the parties in the network must replicate, each party to a transaction updates its ledger to reflect that transaction. However, this creates a problem: if the record of smart contracts is spread across many ledgers, each visible to a certain party, then it would be difficult for any party on the network to know whether their smart contract is accurate.

Daml solves this problem by ensuring that each party's view is a subset of a single global, virtual ledger. In other words, conceptually, all parties of Daml ledgers perceive a single ledger while each party has read-access only to a subset of this ledger's state. This global ledger is virtual in the sense that it does not exist in any one data store. Since, conceptually, all users are reading from the same ledger, all users have a consistent view of any application state they share, for example, ownership of assets. The Canton protocol, described below, is the mechanism that ensures that the views of all properly functioning nodes in the network are consistent subsets of a single valid, global, virtual ledger. All of this is done while ensuring that no party sees or stores information to which it is not a party. As a result, parties can transfer digital

assets with the confidence that the party transferring the digital asset actually owns that asset while also being certain that no other party on the network will know of the transfer unless such party is explicitly permitted to do so.

Daml's fully decentralized and party-centric ledger model enables decentralization in one additional way – rather than being structured as a single network, Daml enables users to create their own subnets. A party can connect to a single or multiple subnets. And if a party is connected to multiple subnets, the Canton protocol can synchronize digital asset transactions across them. Thus, the Daml Ledger Model enables a network of networks. This design ultimately enables privacy, performance, and scalability in a decentralized environment.

Canton

Canton is an open-source privacy-enabled blockchain protocol.

Canton implements Daml's ledger model as described above. Canton currently supports the Daml language, though it can support any language with a similar hierarchical sub-transaction privacy model.

Network topology

Nodes in the Canton Network are called participant nodes. A user or company, represented in Daml as a Party, deploys one or more participant nodes; these participant nodes act on behalf of that Party. To transport data between nodes and determine the order of messages, each participant node connects to one or more private or public Canton Service Providers (CSP) which operate a Canton component called a synchronization domain ("sync domain"). Thus, connecting to sync domains allows a Party to transact with all other parties whose participant nodes are connected to a common sync domain. Anyone can become a CSP and deploy sync domains at will; reasons to deploy new sync domains may include increasing throughput, reducing latency, requiring data transport only through certain jurisdictions or certain blockchain networks, or other operational concerns. To promote privacy and net neutrality, data in transit over sync domains is encrypted, preventing CSPs from accessing message contents. Sync domains can be thought of as highly available, fault-tolerant messaging queues between participant nodes that sequence, timestamp, and serve encrypted messages to participant nodes. CSPs can be single entities or "virtual CSPs" in which a consortium of parties runs a distributed sync domain. At launch, the Canton Network will have at least one open virtual CSP (vCSP) that is run by a consortium and accepts connection requests from any participant node. Application providers can choose to use this open vCSP or any other CSP. As such, Canton creates a mesh network of composable Daml applications in which each application may make different tradeoffs between trust, access control, and operational complexity.

While single nodes have processing and storage limitations, the Canton Network has no intrinsic scaling bottlenecks: a participant node processes only its data and workflows, which different sync domains synchronize in parallel. Parties connect to any sync domains they choose as long as the CSP operating the sync domain accepts them. Open sync domains accept any well-formed requests to join. Canton enables a public network, in that anyone can deploy a Canton sync domain, thus becoming a CSP, for any reason. Sync domains are not silos: parties who share one or more common sync domains can compose higher-order workflows, including atomic transactions across multiple applications, processed via a sync domain selected by the applications. Contract signatories and observers control which sync domain will synchronize their contracts and can choose to reassign which sync domain sequences a given contract, avoiding sync domain lock-in or censorship

The Canton Network has no single centralized governance or policies for access and usage; each constituent node or subnet sets its own policies.

Data pruning

		Canton provides history-pruning and redaction capabilities for its log. Participant and sync domain operators can configure their nodes to store or prune historical cryptographic data, allowing them to trade-off between auditability and the ability to delete archived contracts to comply with right-to-forget regulations such as the European Union's General Data Protection Regulation (GDPR). Historical data can be moved to offline storage to retain full and immutable audit logs while reducing data storage costs and increasing sustainability of production environments. Canton nodes continuously exchange cryptographic commitment to their shared state, so parties remain secure against attempted repudiation by malicious or malfunctioning counterparties even when configured to prune historical data. Thus, individual node operators may trade off maintaining full and immutable historic auditability versus other operational and regulatory compliance requirements.
		Application composability
		In Canton, two or more applications can compose and rely on atomic transactions even if they are synchronized via different sync domains. Thus, for example, two central banks may each synchronize local currency transactions using country-local CSPs, while owners of these currencies can still atomically swap them in a cross-domain transaction.
		Global composability could be achieved, similar to other blockchains, by having a single global Canton synchronization sync domain that allows atomic composition of arbitrary workflows. However, having multiple sync domains is beneficial for multiple reasons. For example, companies and individuals may want more control over their network resources. A single global sync domain would impose a high communication latency for some or all participants. Multiple sync domains can help increase throughput: requests from different sync domains can be processed completely in parallel. There might also be operational concerns; for example, for critical workflows, a new sync domain with restricted access can be used. Finally, different sync domain operators may charge differently for their services. In the example above, transactions in each local currency would be processed completely within the jurisdiction of the central bank's country.
		However, having multiple sync domains opens up a new challenge of how to compose workflows across sync domains. In Daml, composing workflows specifically means that contracts synchronized via different sync domains can be used within a single transaction. Without such an ability, we would not truly solve the composability problem: this would create multiple siloed networks with a single sync domain each, instead of multiple subnets of a single interoperable network.
		Canton guarantees the atomicity of cross-subnet transactions. Since different sync domains have no common notion of ordering between the different sub-transactions that each sync domain processes, reconciling atomicity with resilience can become impossible. To overcome this, Canton allows cross-subnet transactions only whenever there exists at least one sync domain to which all transaction participants are connected. Contract changes required by the cross-subnet transaction are synchronized via this common sync domain. Furthermore, Canton makes it possible to change which sync domain provides the synchronization service for a contract. This synchronization reassignment marks a different sync domain as the new authority for ordering actions on the given contract.
H.3	Technology Used	The Canton Network is the network of networks spanned by all synchronization domains and their connected participant nodes. It is a global system of interconnected participant nodes, synchronization domain nodes and the private, semi-private, and public smart-contract applications deployed to these nodes.
		Canton Network users act in three main roles:
		1. Application Providers - application providers build and maintain smart-contract applications. They operate one or multiple participant nodes, application

backend infrastructure, and frontend web interfaces for those applications. Application providers optionally act as CSPs for their applications or they can use the service of other CSPs.

2. Application Users - most users interact with applications via application programmable interfaces (APIs) and web user interfaces (UIs). Users must have a participant node and can choose to operate their own participant nodes or use hosted nodes managed by others.

3. Canton Service Providers (CSPs) - infrastructure providers, who are typically also application providers, connect participant nodes by operating a Canton sync domain.

The Canton Network consists of multiple subnets. A Canton subnet is any one or more participant nodes that can transact with other participant nodes via one or more synchronization domain nodes.

The first decentralized synchronization domain is called the Global Synchronizer. Following its "TestNet" launch in June 2023, and extensive testing with market participants, the Global Synchronizer's "MainNet" subsequently went live in June 2024. The Global Synchronizer is decentrally operated by independent entities called Super Validators. The Global Synchronizer will be the first instance of a decentralized synchronization domain for the Canton Network but is not intended to be the only one. Third parties may set up their own decentralized Canton synchronization domains using the code available through Splice, a Hyperledger Lab.

All actions taken by Super Validators operating the Global Synchronizer, and Canton Coin application configurations and transactions, are subject to a ⅔ majority action of all Super Validators. This includes all parameters described in this paper, including the set of active Super Validators, the minting curve and rights split, fees, and protocol improvements.

Governance of the Global Synchronizer will be facilitated by the Canton Foundation, an independent entity managed by the Linux Foundation. The Canton Foundation will facilitate transparent governance and organizational neutrality in the operation of the Global Synchronizer.

The goal of the Super Validators is to build an ecosystem to foster and accelerate the creation of a "network of networks" of applications in regulated finance and other areas. A "backbone" infrastructure like the Global Synchronizer is an important part of doing so, but it is far from sufficient for starting an ecosystem. Networks acquire and deliver value through "network effects", where existing users and applications provide value to new users and applications, and vice versa. To incentivize the first users and applications to do something in the absence of that preexisting value, special mechanisms are needed to provide first-mover advantages. This includes the Super Validators themselves, which are providing the first services within this ecosystem, including the Global Synchronizer.

Furthermore, ecosystems like the Canton Network benefit significantly from having both a means of transferring value, and publicly visible metrics for activity and use.

To meet these needs, the Super Validators have included a payment and incentivization application in the launch of the Global Synchronizer's MainNet. The application is based on a token called Canton Coin, and each Super Validator will independently run an instance of the Canton Coin application.

| H.4 | Consensus Mechanism | **Proof-of-Stakeholder: Consensus with privacy**

Canton's primary goal is to provide consistent data across parties. In other words, Canton aims to achieve consensus amongst parties on the active contracts on which they are joint stakeholders, and on the validity of the transactions that led to this state. The standard approach to consensus is state machine replication, where all participants replicate the same global state. However, replicating the entire global |

		state is not acceptable for privacy and scalability reasons. Instead, Canton's proof-of-stakeholder consensus protocol is split into two layers of consensus. To achieve consistency along with privacy, the first consensus layer is a two-phase commit protocol that replicates each contract to the contract's stakeholders while concurrently enabling each stakeholder to validate the transaction. Conceptually, this can be thought of as having a replicated state machine for every subset of parties. For this first layer to commit transactions consistently, nodes must agree on the order in which conflicting transaction requests are applied to the ledger. Therefore, the second consensus layer is a sequencing protocol that receives encrypted transactions and determines a timestamp for each transaction. This sequencing layer can be run on a central CSP or, when connected to a virtual CSP's distributed sync domain, this sequencing protocol runs as a replicated state machine secured by a Byzantine Fault Tolerant (BFT) consensus algorithm. Thus, the virtual CSP determines a total order on transaction requests within a sync domain, and transaction processing is deterministic.
H.5	Incentive Mechanisms and Applicable Fees	**Burn-Mint Equilibrium** Canton Coin employs a burn-mint equilibrium mechanism, aiming to stabilize the conversion rate of Canton Coin around the intrinsic value it provides to network users. Token price is a function of supply and demand. As such, if supply is fixed and demand is volatile, the conversion rate becomes volatile. The burn-mint equilibrium mechanism is expected to allow total supply to adjust according to demand, thus reducing conversion rate volatility. Furthermore, under this mechanism, the conversion rate is expected to align, over the long run, with the utility value of the network.

The burn-mint mechanism works as follows:

1. Canton Network users use Canton Coin to pay fees denominated in United States Dollars (USD) as they use applications and infrastructure services.

2. Instead of paying fees directly to network infrastructure providers, all fees for using Canton Coin, and for creating a traffic balance on the Global Synchronizer, are burned by the user who submits the Canton Coin transaction. Thus, Canton Coin are retired from circulation, decreasing the token supply by the amount of real utility provided to network users (in USD). The users specify the application or infrastructure service for which they're burning fees.

3. In return for operating applications and network infrastructure, providers can mint new Canton Coin. Thus, the usage fee from user to provider is indirect via the burn-and-mint mechanism. Below, both fees and minting are described in more detail, as is the motivation for using this burn-and-mint mechanism.

4. As defined by the minting curve, the Canton Coin application creates a predetermined amount of Canton Coin that can be minted over time. At steady-state, the Canton Coin application allows the minting of 2.5 billion Canton Coin per year. Thus, the cumulative number of Canton Coin minted is always increasing. This is offset by the number of Canton Coin burned. Accordingly, network usage must burn 2.5 billion Canton Coin per year to keep the number of Canton Coin in circulation stable.

Fee Structure:

Canton Coin users pay two types of fees to use the Global Synchronizer and its Canton Coin application, detailed below. These fees are not paid to any other party directly; instead, users burn Canton Coin to cover these fees; this supports the Global Synchronizer's burn-mint equilibrium. While there are multiple fees described below, the design principle is simple: the fee structure looks to (1) increase the amount of coins burned as utility increases and vice-versa, (2) have similar total costs to the user as well-established payment systems, and (3) incentivize efficient usage of common

resources such that each Canton Coin owner pays for their fair share of the common resources they utilize.

1. Percentage transfer fees - A small percentage fee based on the amount of value transferred, with a regressive cost structure. Percentage transfer fees take inspiration from the fee structure and cost of existing cash payment networks.

2. Resource usage fees - Fees that cover the infrastructure costs of shared resources, regardless of the value transferred. These fees are calculated based on the amount of bandwidth and storage used, and the amount of time the storage is used as follows:

    a. Base transfer fee - A fee applied to every new coin contract record (UTXO) created in a Canton Coin transfer transaction. Most transactions incur at least two base transfer fees.

    b. Coin locking fees - A fixed fee for every holder of a lock on a coin record, since each additional signatory increases the load on the Super Validators.

    c. Holding fees - A fixed fee over time per separate coin contract (UTXO) per unit of time, regardless of the coin amount. This is paid by the coin holder and incentivizes users to merge coins or pay for any additional network storage the coin contracts (UTXOs) incur.

    d. Synchronizer traffic fee - Amount of traffic balance deducted to have a transaction synchronized via the Global Synchronizer. Traffic balance is denominated in megabytes and is required for transactions sequenced by the Global Synchronizer, whether or not a transaction uses Canton Coin. To set up a traffic balance for a given Validator node, someone must burn an equivalent value of Canton Coin, based on the current USD to Canton Coin conversion rate and the USD/MB price, and assign the resulting traffic balance to that Validator node. Note that traffic is non-transferable, and traffic balances cannot be converted back to Canton Coin. Traffic balances are designed to remain relatively small.

All fees are denominated in USD and settled in Canton Coin, based on a Canton Coin to USD conversion rate published on-chain, as part of the minting cycle every ten minutes. Super Validators operate the oracle that provides the on-chain conversion rate, which is computed by allowing every Super Validator to submit a proposed conversion rate at any time. An automated calculation then publishes the median of the proposed conversion rates at the start of each minting cycle.

Minting Structure

The minting curve defines how to split the total amount of Canton Coin available for minting.

There are four scenarios under which Canton Coin can be minted:

Application providers can mint Canton Coin for operating valuable services on the network. The total pool of Canton Coins that can be minted by application providers, as defined by the minting curve, is split among application providers relative to the value each application provider's application provides to the network. To calculate that value the Canton Coin application inputs the total amount of Canton Coin fees burned by users when using the application. Each application provider is subject to some minting caps, described below, to avoid gaming and arbitraging.

Validators can mint Canton Coin for "Coin usage" based on the value of Canton Coin transfers initiated by users of the Validator. Each Validator is subject to caps on the number of Canton Coins it can mint this way to avoid gaming and arbitraging.

Validators can mint Canton Coin for node uptime, or "liveness". If Validators do not

mint all available Canton Coin for Canton Coin usage (as described in the paragraph above) in a given minting cycle, the remaining Canton Coins can be minted for liveness by dividing the remaining Validator mints across all the active Validators. This creates an incentive for Validators to be ready to host potential users of new applications and use cases. As activity picks up, the allocation of Canton Coin minted by Validators that facilitate network activity overtakes the minting due to liveness, so passive Validator nodes will stop being eligible to mint Canton Coin. The number of Canton Coins that can be minted for liveness per Validator is capped to avoid first movers being incentivized to resist new joiners.

Super Validators can mint Canton Coin for running a node in the Global Synchronizer. The total pool of Canton Coins that can be minted by Super Validators is defined by the minting curve and is split among Super Validators relative to the efforts each Super Validator has made or committed to make to grow the network, as determined and agreed by ⅔ of the Super Validators. These weighted Super Validator allocations are part of the BFT network configuration.

Featured Applications and Minting Caps

Minting caps exist to prevent network users from arbitraging and gaming the Canton Coin application without adding value to the network. To avoid this gaming scenario, we distinguish between "featured" and "unfeatured" applications.

All applications are unfeatured initially, meaning the rewards they can mint are capped. This cap can be lifted by the Super Validators with a ⅔ majority vote by marking the application as a "featured application", indicating that they consider the application to be providing real utility to the network.

Featured application providers may mint up to 100x more Canton Coin than was burned as fees in Canton Coin transfers coordinated by their applications. This creates an incentive for application providers to build featured applications early on and provide high value to the network. As more featured applications gain usage, their providers will mint all Canton Coins available to application providers as defined by the minting curve, thus splitting available rewards between the different applications and reducing the effective multiplier they can reach.

Unfeatured application providers cannot arbitrage the incentive system by creating a high volume of transfers between parties they control. They may mint at most 80% of their fees back as Canton Coin. This ensures that application providers are disincentivized from wasting network resources without providing real utility to network users as a whole.

As an example, if an unfeatured application user pays $100 in fees to the application and in the process of this transfer burns $1 worth of Canton Coin, the application provider will receive $99 in fees and be eligible to mint up to $0.8, whereas a featured application provider would be able to mint up to $100 worth of Canton Coin, assuming there are enough coins in this round to reach the cap, as defined by the minting curve.

H.6	Use of Distributed Ledger Technology	false
H.7	DLT Functionality Description	false
H.8	Audit	false
H.9	Audit outcome	N/A

Part J - Information on the suitability indicators in relation to adverse impact on the climate and other environment-related adverse impacts

S.1	Name	Canton Network
S.2	Relevant legal entity identifier	N/A
S.3	Name of the crypto-asset	Canton Coin
S.4	Consensus Mechanism	See H.4 above.
S.5	Incentive Mechanisms and Applicable Fees	See H.5 above.
S.6	Beginning of the period to which the disclosure relates	2025-08-28
S.7	End of the period to which the disclosure relates	2025-08-28
Mandatory key indicator on energy consumption		
S.8	Energy consumption (per year) in kWh	131115.18805
Sources and methodologies		
S.9	Energy consumption sources and methodologies	Data provided by CCRI; all indicators are based on a set of assumptions and thus represent estimates; methodology description and overview of input data, external datasets and underlying assumptions available at: https://carbon-ratings.com/dl/whitepaper-mica-methods-2024 and https://docs.mica.api.carbon-ratings.com. We do not account for any offsetting of energy consumption or other market-based mechanism as of today
S.10	Renewable energy consumption (share of energy from renewable generation resources) in %	29.07
S.11	Energy intensity (energy used per validated transaction) in kWh	0.00096
S.12	Scope 1 DLT GHG emissions – Controlled (per year) in t CO_2eq	0
S.13	Scope 2 DLT GHG emissions –	60.18187

	Purchased (per year) in t CO$_2$eq	
S.14	GHG intensity (emissions per validated transaction) in kg CO$_2$eq	0.00044
Sources and methodologies		
S.15	Key energy sources and methodologies	Data provided by CCRI; all indicators are based on a set of assumptions and thus represent estimates; methodology description and overview of input data, external datasets and underlying assumptions available at: https://carbon-ratings.com/dl/whitepaper-mica-methods-2024 and https://docs.mica.api.carbon-ratings.com. We do not account for any offsetting of energy consumption or other market-based mechanism as of today.
S.16	Key GHG sources and methodologies	Data provided by CCRI; all indicators are based on a set of assumptions and thus represent estimates; methodology description and overview of input data, external datasets and underlying assumptions available at: https://carbon-ratings.com/dl/whitepaper-mica-methods-2024 and https://docs.mica.api.carbon-ratings.com. We do not account for any offsetting of energy consumption or other market-based mechanism as of today.