Central Bank Digital Currency

Principles for Technical Implementation

Darrell Duffie,[1] Graduate School of Business, Stanford University
Kelly Mathieson, Chief Client Experience Officer, Digital Asset
Darko Pilav, Director of Client Experience Engineering, Digital Asset

April 2021

Executive Summary

This document provides a high level overview of some principles of Central Bank Digital Currency (CBDC) and key factors supporting those principles that should be considered when choosing and implementing a technology to support CBDC. In this paper, we discuss:

- *Critical distinctions between CBDC and crypto assets, traditional and digital currency, and tokenization and digitization.*
- *Benefits for the Central Bank, policy makers, consumers, markets and institutions.*
- *Technology factors to consider prior to CBDC inception.*
- *Why interoperability is critical and must be considered from the start.*
- *Key advances in central bank ledger functionality, such as name-on-register protections, improved B2B settlement mechanisms, and B2C payment options.*
- *Protection of privacy while safeguarding compliance.*
- *How to create an effective foundation for CBDC with a smart contract application framework and digital ledger.*

The challenge of creating and implementing CBDC is large and complex, requiring a thoughtful approach and technology solutions that not only address current challenges but also facilitate future innovation and support yet-to-be known requirements and opportunities. The ability to start small, facilitate wide adoption, evidence controls, and maintain flexibility to maximize growth are essential. This paper particularly emphasizes the key requirements of privacy protection and interoperability.

Digital Asset has undertaken extensive explorations of the technical aspects of CBDC, most recently presenting our approach at the OECD Policy Forum in November 2020. Digital Asset introduced an interoperability functionality, showing how CBDC can tie into any reasonably foreseeable workflow. Digital Asset has open sourced the code to make it broadly accessible and to reduce the risk of multiple CBDCs running on incompatible, siloed platforms.

[1] Darrell Duffie received no compensation or other consideration for his collaboration on this paper.

Table of Contents

1.0 Introduction

As businesses and the lives of consumers become increasingly digitized, the drive for efficient digital solutions intensifies. New technologies such as smart contracts and distributed ledger solutions could solve long-standing banking and financing challenges, where complex transactions are handled on aging infrastructure using outdated business processes, and with information silos that hinder the ability to swiftly capture and analyze data.

From simple retail payments to sophisticated cross-border institutional transactions, attention is turning to smarter ways to move money quickly, track it carefully and prevent fraud. Central banks are exploring options for upgrading banking and payment technologies while preserving privacy and controls. Government entitlement programs can also be better expedited.

Digital currency offers the potential to address these challenges. This will take more than establishing the digital currency. It will also be necessary to modernize processes and policies, to ensure that the Central Bank's ledger is equipped to handle, issue, and manage a digital form of currency, and that access to the ledger is defined with rights, permissions, and controls that are necessary to govern currency issuance, distribution, and circulation.

1.1 Defining Central Bank Digital Currency (CBDC)

A CBDC is a digital form of currency backed by a central bank with legal tender status, meaning it can be used to settle debts or meet financial obligations. Importantly, we largely agree with the Central Bank of Sweden (Section 3.2) February 2021 that CBDC should not be a bearer instrument, in order to ensure that digital payments are between known entities and include Office of Foreign Assets Control (OFAC) checks.

Central banks will generally choose to issue CBDC **in addition** to conventional cash. The Central Bank retains control over the money supply because it would manage CBDC creation and destruction. CBDC should not be forgeable and its authenticity should be easily verified. It should be efficient to store and easily transferable. Owners should have an expectation of privacy. The Central Bank (issuer or supervisory authority) should be in a position to monitor compliance with anti-money laundering and other legal limits on payments, but privacy should otherwise be protected. Notably, the provider of the technology infrastructure and any entity not party to the transaction should not have access to transaction details, except as expressly authorized by the authorities for compliance purposes and disclosed to users.

Digital currency, unlike cash, is not a bearer instrument, and should not be conflated with cryptocurrency (often referred to as tokenization). Cryptocurrencies, because they are freely transferable bearer assets, are ill suited as CBDCs. A widely available cryptocurrency would run on a public ledger, thus making a substantial amount of data publicly available.

A digital currency supports some key desirable properties for a CBDC:

- Transferable, but with rights that are programmable - allowable actions that can be set by smart contracts.
- Ownership is known and can be restricted - to conform with Know Your Customer (KYC), Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT) and other compliance requirements.
- Data access is controlled - only the participants to a transaction can see the information relevant to them.
- Portable across any ledger - allowing the Central Bank to retain flexibility in terms of capabilities and choice of service providers, in both the short and long term.

Our view is that CBDC should support both retail and wholesale activities, over time. Therefore, for the purposes of this paper, we are not considering private ledgers or fully anonymous solutions because the former would place restrictions on participation while the latter provides no traceability or opportunity for controls and regulatory oversight.

Additional resources on digitization and tokenization

Beyond Tokenization - Overview of the challenges a tokenized solution would face in supporting complex transactions and how those challenges can be overcome with digital currency and smart contracts. (January 2020)

1.1.1 Required Properties of a CBDC Solution

CBDC must be easy to use but also exchangeable as an element of complex financial transactions. To realize its full potential, a CBDC should have the following properties:

High levels of privacy: A CBDC solution must guarantee fine-grained privacy controls. Transaction details should be accessible on a strict need-to-know basis.

Boundless horizontal scalability: A CBDC solution must be able to cope with an ever-increasing throughput of transactions. This calls for unrestricted horizontal scaling capabilities. The processing of transactions must be highly parallelizable.

Use case extension and integration: Beyond replacing the existing payment infrastructure, it must be possible to seamlessly integrate CBDC into other processes and workflows.

Infrastructure interoperability: Since it is unlikely that different countries will decide on the same infrastructure, a CBDC should interoperate across different technical infrastructures in order to reap the benefits of frictionless FX transactions. But even for domestic payments, the applications that are integrating into the CBDC ecosystem need not run on the Central Bank's own infrastructure, and should interoperate across commercial banks and payment providers. Therefore, infrastructure interoperability is needed to ensure that the CBDC solution is more than a like-for-like replacement of the existing payment system.

A CBDC with these properties could be utilized in complex transactions such as:

- The purchase and sale of securities, commodities, real estate, and other regulated activities for which ownership rights are restricted and rights, obligations, and exposures must be clear to all participants.
- Transactions for which not all steps or participants are necessarily visible to other participants on the blockchain or ledger (e.g. preventing competitors from viewing an institution's investment activity, or unauthorized persons from viewing an individual's personal financial transactions).
- Transactions for which transparency of ownership is sufficient for the purposes of meeting requirements for KYC, AML, and CFT.
- Activities requiring that records are kept and controlled by regulated entities that are recognized by law and have legal enforcement rights (e.g., property transfers). Similarly, activities for which access to change records or effect transfers must be restricted to appropriate parties only.

In the design and approach to CBDC that we envision, the ability to manage these activities with more controls, nuance, sophistication, and transparency will be critical to public trust and Central Bank oversight.

1.2 Market Drivers for CBDC Exploration

Support for the concept of digital currencies is gaining momentum. Payment-system innovations such as Libra (now Diem), Sweden's prospective e-Krona, China's immensely successful mobile payment services Alipay and WeChat Pay, and China's Digital Currency Electronic Payment System (DC/EP) have captured the attention of experts and non-experts alike. These innovations and the significant frictions associated with conventional bank-railed payments, especially in the United States, have caused many expert commenters to heighten expectations for more efficient payment systems, especially over the prospect of an effective CBDC. Many central banks have responded with CBDC research and development programs, according to BIS surveys, January 2021. Increasingly, the limits of aging, weakly connected information systems are stressed to keep up with compliance demands that involve knowing your customer, being able to prevent unauthorized or fraudulent transactions, and restricting access to funds for bad actors. Investors seek better ways to reduce counterparty risk with trading partners and depositories.

With global supply chains and voluminous wholesale and retail cross-border payments, there are increasing demands for rapid and safe payments. Currently, international transactions and poor payment processes create undue friction in commerce and involve annoyingly high fees for consumers. Settlement risk remains a costly concern. Existing technology constraints necessitate reliance on trusted third parties (e.g., escrow service providers), adding another layer of time, complexity, and expense to cross-border activities.

The global pandemic accelerated digitization. Economic stimulus programs highlighted the need to distribute funds rapidly and, in some cases, to set parameters for the use of funds (e.g., supplemental nutrition assistance, housing, or retraining). Heightened cybersecurity concerns call for improvements in transparency and the ability to embed safeguards.

A CBDC simplifies and - in some cases, removes - these challenges. A well designed digital currency can be authenticated and tracked, rely on smart contracts to verify transactions, and utilize complex business logic to address different financial activities. These features reduce and may even remove reliance on third parties, creating additional efficiencies throughout the transaction chain.

1.3 Costs and Benefits of Introducing Digital Currencies

A CBDC is a significant undertaking. The assurance of safety, operational reliability, privacy, and efficient payments are substantial responsibilities. Failures could be costly and could fall at the feet of the Central Bank, impinging on its reputation. The technology implementation of a CBDC should provide the Central Bank with flexibility in how to handle, delegate, or assign such responsibilities. One possible approach would be a two-tier system. In the first tier, the Central Bank provides the system of record for all consumer accounts and positions. In the second tier, the Central Bank delegates authorities to banks and other payment service providers allowing them to offer access and services to their customers, and to perform KYC, AML, and other regulatory requirements.

The object of paramount importance is the single system of record - the Central Bank ledger, with a single golden source of data and the ability for permissioned participants in the CBDC ecosystem to view, access, and act on those data. Critical to this architecture are interoperability capabilities, allowing the different systems of the Central Bank, banks and other payment service providers to have a common, fully synchronized view of the current state of the Central Bank ledger. Payment service providers, however, are permissioned to view only the essential data regarding their own customers. With these properties - a single system of record and interoperability - the current challenges of duplicated data and constant reconciliations across the separate records of participants can be removed.

Such an approach requires a technology with expressive and fine-grained permission delegations and privacy rules. Models such as the two-tier approach above, as well as hybrids that align broader roles and responsibilities to central banks, become possible. These technology properties allow banks and other payment service providers to act on behalf of their customers on the Central Bank ledger for specific actions, as agreed with their customers. The Central Bank remains the sole issuer and governs the system of record of CBDC positions. The Central Bank sets standards for the use of

CBDC (such as interoperability requirements) and could potentially be the regulator of the payment service providers, which could be commercial banks and authorized fintech firms, as is the case with China's DC/EP.

A further concern is the potential impact of a widely used CBDC on commercial banks, which currently have substantial payment and deposit franchises that might suffer adverse impacts. Disruption of existing payment arrangements can be viewed negatively or positively, given weaknesses in the service quality and costs of many bank-railed payment systems.

The main benefits of a CBDC are the prospect of much-improved payment efficiency and increases in financial inclusion. The transfer of money - whether peer to peer, customer to business, business to business, across banks, and potentially internationally - would become more straightforward, faster, and cheaper. This is so mainly because payments would involve fewer intermediate systems and fewer profit-taking service providers along the payment path. CBDC payments would be available instantly, around the clock. The introduction of a CBDC would permit the Central Bank to extend its ledger to a broader group of participants, including under- or un-banked consumers. This can especially improve the welfare of lower income households, who might otherwise have weak access to the economy or suffer from extremely high payment fees.

Users of a CBDC could realize additional benefits:

- More transparency, including real-time payment and account information.
- Reduced depository risk, as Central Bank-issued CBDC would remove consumer concerns about individual bank solvency or limits on bank deposit protections.
- When implemented correctly, improved privacy protections. For example, transactions would not be visible to those involved in preceding or following transfers, except as desired and arranged.

The introduction of CBDC would give businesses the option to settle transactions directly at the Central Bank, allowing access to funds more quickly and easily. Other advantages would include:

Frictionless wholesale payments between counterparties, wherein money is automatically transferred if and only if all steps of the transaction are successful and the conditions of the contract have been met. The result is increased settlement efficiency and certainty.

Enhanced settlement, covering both settlement and subsequent lifecycle events, by employing a common data model within or across markets, automated lifecycle events, and mutualized workflows across parties. The result is increased settlement transparency and lower operating cost and risk.

Significant risk reduction for counterparties and depositories, with synchronized protocols guaranteeing that data are reliably shared with entitled parties in real time, accurately. Compliance monitoring and regulatory requirements can be built into the workflows, providing real-time, continuous oversight.

Various Liquidity Saving Mechanisms developed for any anticipated Real Time Gross Settlement solution can be more easily implemented (such as those proposed by Rodney J. Garratt in *An Application of Shapley Value Cost Allocation to Liquidity Savings Mechanisms*, July 2019).

Some of the advantages of a CBDC can also be achieved with new fast bank-railed payment systems, such as the FedNow system under development in the United States. While this is a clear step forward toward faster and continually available payments, fast payment systems continue to rely mainly on banks for the provision of payment services and to use bank deposits as the medium of payments. Although a fast payment system could potentially increase competition among banks for payment and deposit services, this is not assured. For example, commercial banks would retain the incentive to maintain a "walled garden" around their customers. Moreover, there is not yet much prospect that bank deposits will be redesigned with the "smart" features of digital currencies that we have described and will detail in the next section.

2.0 Designing a Technology Approach for CBDC

Conversations about digital currency often begin at the end - with discussions about potential technology stacks or distributed ledger options. Centralized databases or existing payment rails also come under review, raising important downstream questions of adoption, extension, and interoperability.

Locking into a specific ledger provider restricts new solutions to a particular infrastructure or set of features even before they begin to take shape. This matters, because many ledger providers:

- Lack the granular privacy and authorization controls necessary to build critical market infrastructure.
- Cannot seamlessly connect to other ledgers and infrastructures.
- Lack horizontal scalability and set an upper limit on the number of possible transactions.
- Have poor trust properties and cannot effectively deal with malicious participants. To provide security, they are strongly permissioned and "locked down," limiting participation to privileged, vetted users.

These restrictions run against the flexibility required of an effective Central Bank ledger and digital currency.

2.1 Foundational Considerations

Central banks will want to embed flexibility and interoperability from the start. Given the proliferation of infrastructures, interoperability will be critical. If different central banks decide on non-interoperable ledger providers, new technology silos will replace old ones and large opportunities for efficiencies will be lost.

Any approach should be considered with an eye toward future-proofing: allowing for the broadest possible set of uses and greatest flexibility to expand as opportunities arise. This includes looking downstream to equitable adoption, allowing users to choose how they interact with the CBDC and to avoid commitment to a particular technology.

Key considerations of a ledger implementation include:

- Data integrity. No user or entity is able to change data without the authorization of its owners.
- Sub-transaction level privacy. Data minimization is the maxim. Even within a complex transaction, every entity will have access only to data that they own or are allowed to observe - even if this means that they see only a part of a transaction.
- Ability to model and enforce multi-party agreements. The modeling language should allow custom tailoring, so as to allow the capture of rights and obligations in multi-party agreements.
- Focus on Day 2 operations. Management, deployment, and monitoring, including comprehensive metrics and logs, are necessary for any systemically important market function. Entities operating such infrastructures or utilities must have access to established, 24x7 global support.
- Suitability to scale across multiple data centers. Integration with current SDDC (software-defined data center) infrastructure is necessary to allow for use across public, private, and/or hybrid environments.

Given the potential complexity associated with the deployment of a CBDC, it is likely that most CBDC programs will start small and grow as new adopters come on board or new solutions are identified. Over time, a central bank's needs may change, necessitating a switch of ledger partners or the ability to work across multiple ledger partners.

2.2 The Value a Smart Contract Application Platform Brings to a Central Bank Digital Ledger

The creation of CBDC allows the Central Bank to extend its ledger to a broader group of participants, including consumers who may be under- or un-banked, while still retaining control over the money supply and over who is permissioned to transact on the digital ledger. To be successful, the digital ledger should be implemented using a smart contract application platform that allows rules and permissions to be embedded within the CBDC and facilitates connections with a broad range of technology providers, existing institutions, and infrastructures.

A digital CBDC ledger, running on a smart contract application platform, reduces depository counterparty risk for the consumer, improves business-to-business settlement mechanisms, and modernizes and accelerates domestic and international payment options.

The Daml smart contract application platform provides the necessary foundation to meet these objectives. With Daml, a provider can develop the underlying business logic once, then run it on multiple infrastructures or even across ledgers. Key features include:

> **Capacity to create multi-party solutions** that transform silos into synchronized networks with guaranteed, consistent data. This allows the provider to focus on its use case, develop functional and non-functional requirements, and test them up front.
>
> **The ability to simplify complex workflows across infrastructure(s)**, eliminating boundaries through integration with both traditional databases or enterprise-scale distributed ledger technology (DLT).
>
> **A unique way to model and execute essential interactions**, such that business logic is separated from systems code and the language is easy for business experts to understand and technologists to use.
>
> **One layer that sits across multiple applications** to simplify individual processes. Data are extracted to create a single source of truth that can be used simultaneously across multiple applications, while combining common tasks to create efficiencies.
>
> **Built-in capabilities to include agreements, signatories, privacy, rights, and more**, with components that are flexible and can be built up front, added later, or incorporated as discrete modules to be used in certain scenarios. Daml provides the framework to model and establish discrete rights and permissions.

Daml supports a breadth of potential applications of CBDC, giving the Central Bank the flexibility to start with specific use cases and then expand without being constricted by the limitations of a particular ledger provider or infrastructure partner.

2.2.1 Support for Core CBDC Features

Daml's component approach delivers strong, secure data governance, workflow, data modeling protocols, and business interactions.

- Traceability by authority. Daml naturally supports auditing and tracking transactions, storing data and contracts (to the lowest level of identification) along with the history of each transaction. The set of observers of a Daml contract can be customized to allow for more transparency and visibility.
- Closer control of ownership by authority. The authority can control who can

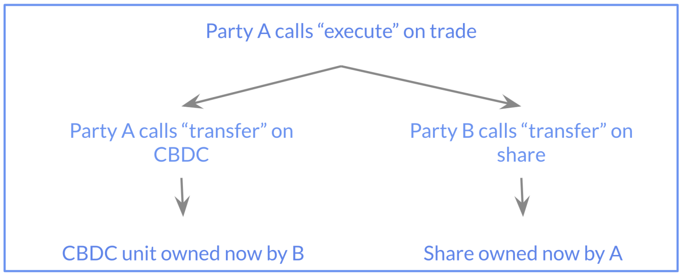
hold money at a programmatic level, for example, to comply with restricted lists (e.g., OFAC).

- Transaction safety. For simple or complicated transactions, Daml can establish specific rules for money transfers. The transactions are then executed atomically, so that for a successful transaction, all steps must be successful.
- Interoperability. Using a common language and protocol, Daml would permit a CBDC system to bridge different ledgers and technologies. (See Section 3.2, page 12.)

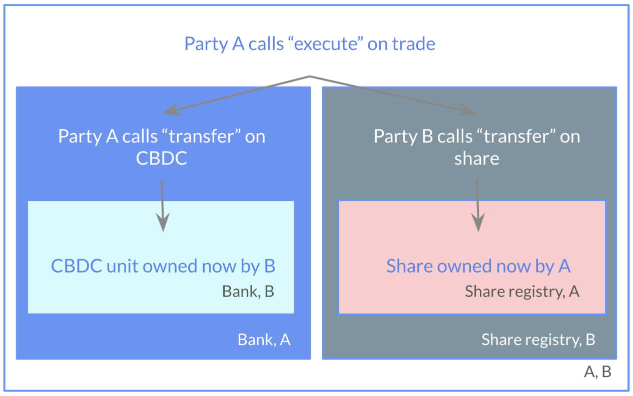
2.2.2 Efficiencies and Safeguards

For the Central Bank, Daml's key features simplify the development of a CBDC and increase efficiency while providing important safeguards and transparency:

- Common data and processes can be extracted to simplify highly complex, multi-step, multi-party workflows, making it convenient and safe for day-to-day business.
- Rights and obligations are defined and enforced using built-in business roles and fine-grained permissions. This ensures that information is shared with those who need to know it, when they need to act on it.
- Existing legal concepts can be digitized for efficiency, providing additional safeguards.
- Assets are extremely safe with Daml. Developed by cryptography experts, Daml's declarative security model minimizes accidental data leakage, hacks, and break-ins.


Party A calls "execute" on trade
Party A calls "transfer" on CBDC
Party B calls "transfer" on share
CBDC unit owned now by B
Share owned now by A

Example: Integrating CBDC money in a share trade workflow between parties. Party A transfers its CBDC money to party B in exchange for shares. The CBDC operator should not be aware of the share transfer, and the share operator should not be aware that the transfer was paid with CBDC.


Party A calls "execute" on trade
Party A calls "transfer" on CBDC
CBDC unit owned now by B
Bank, B
Bank, A
Party B calls "transfer" on share
Share owned now by A
Share registry, A
Share registry, B
A, B

Example: Different parts of a trade workflow are visible on a need-to- know basis. Each box is labeled with those parties who must be able to see the particular sub-transaction. For example, the CBDC transfer is not visible to the share registry, and the share transfer is not visible to the Central Bank, while A and B see the entire transaction.

Figure 3. Two examples of how Daml smart contracts work within a trade workflow.

3.0 Future-proofing

Given the extensive interactions of central banks with other institutions, individuals, and jurisdictions, a digital currency should freely support financing, trade, and commerce, whether at home or across borders. The necessary level of interoperability requires protocols that can span different technologies, which in turn requires the systems to be able to "speak" to compatible ledgers.

3.1 Daml-driven Interoperability

We believe that seamless and built-in interoperability is the only way for CBDCs to reach their full potential, and that true interoperability includes four key elements:

Multi-ledger technology: The ability to deploy and connect digital currency systems across disparate networks regardless of the underlying IT infrastructure. Top among the challenges is deciding which technology to use - distributed ledger technology (DLT), centralized database, or existing payment rails. Riding on the back of this issue is the requirement for compatibility with other CBDCs, since there will be no single master ledger and because some CBDCs may not use DLT. Ensuring that a CBDC is compatible with other CBDCs is a critical first step to preventing the CBDC from hitting a dead end in cross-border applications.

Cross-ledger atomicity: If one leg of a transaction fails, all legs fail. By ensuring atomicity, systems can achieve payment versus payment and delivery versus payment without the risk of handing over goods when the payment leg fails and without the need for a central bank to act as an escrow.

Data privacy: Almost all non-Daml blockchains lack the basic properties of privacy, leaking transaction information to the world. Some chains have addressed some of the privacy concerns but lack the ability to guarantee their privacy mechanisms when transacting across chains. A CBDC solution should feature privacy within as well as across ledgers.

Composable extensibility: This property is the ability to dynamically add new applications and to connect to other networks easily. Without composable extensibility, companies will likely reinvent the wheel when future technologies arise or when there is a need to deploy future use cases to the same infrastructure. Since it would be impossible to predetermine all potential uses for CBDC, the design of the currency should allow new uses to be created without requiring changes to the initial implementation. Thus, extensibility is critical to ensuring the ongoing effectiveness of the digital currency.

3.2 Interoperability Using the Canton Protocol

Canton is an interoperability protocol that is the next generation of Daml ledger integration. Canton allows for interaction among different ledger technologies including databases, permissioned or open blockchains, and hardware enclaves.

Canton extends Daml's ability to write a distributed application independent of the platform on which it will eventually run. With Canton, Daml workflows can be run across multiple platforms, making them interoperate even when the original platform owners had not included this capability.

In combination, Daml and Canton solve many of the immediate challenges inherent to creating and mobilizing CBDC, while also leaving the door open to future needs and expansion.

3.3 Canton Features

Daml works with a growing number of major enterprise blockchains as well as centralized databases and other systems. Digital Asset has used its deep knowledge of each of those technologies and their different privacy mechanisms to create the Canton interoperability protocol, which sits beneath the Daml smart contract language.

As a Daml ledger interoperability protocol, Canton's embedded synchronization guarantees that data are reliably shared only with entitled parties, and in a correct manner, even in the presence of malicious actors.

Canton can be extended without friction to new parties, ledgers, and applications, building on other applications without requiring a central managing entity or global consensus within the network.

Canton offers:

- Global composability. Different Daml-based ledger instances can operate using the Canton synchronization protocol.

- Data privacy. Canton is built around the principle of data minimization and the right to forget, enabling compliance with laws, regulations, and global standards such as General Data Protection Regulation (GDPR).
- Integrity. Canton's synchronization protocol ensures that a participant's ledger remains in a valid state, and that a corrupted state never occurs.
- Horizontal scalability. Canton has no upper bound on transaction throughput. The throughput scales linearly with the employed hardware.

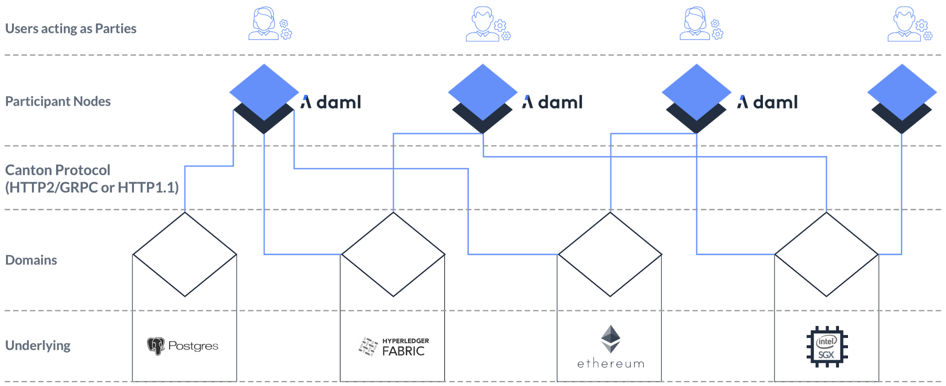


Figure 5. Canton allows multiple Daml-based leger instances to connect to different underlying domains and ledgers, while remaining constantly synchronized.

Additional resources on interoperability and the Canton protocol

Digital Asset Demos 4 Key Properties of Interoperability - Demo showing how wholesale and retail applications of CBDCs can interoperate across Hyperledger Fabric, Ethereum, and a traditional Postgres database, making CBDCs compatible regardless of the underlying technology. (November 2020, OECD Blockchain Policy Forum)

"Central Bank Digital Currencies" Technology Properties: We need Interoperability and More - Discussion of how application composability provides the technology underpinning for atomic settlement, sub-transaction privacy, and security, and how a CBDC system can be extended across participants using the Canton protocol. (July 2020)

Digital Asset Shapes Future of Interoperable Applications - Overview of 2021 market and segment expansion based on interoperability with infrastructure and ledger providers. (February 2021)

Elements of Canton - A short explanation of how Canton works. (February 2020)

Canton Reference Demo - Overview showing what Canton offers in terms of application composability, network interoperability, privacy, and regulatory compliance, and how Canton differs from existing solutions. (2021)

A Structured Semantic Domain for Smart Contracts - Extended abstract that reviews how additional structure yields a more secure programming model for smart contracts and allows for distributed implementations with better confidentiality, privacy, and scalability properties. (April 2019)

Canton: A Private, Scalable and Composable Smart Contract Platform - White paper providing a detailed overview of how Canton implements Daml's built-in models of authorization and privacy while also resolving issues of scalability and interoperability common to other platforms. (February 2020)

Canton Documentation - User information including documentation, tutorials, user manual, and an in depth review of architecture. (2021)

4.0 How CBDC Can Foster Efficiency and Innovation

By leveraging a CBDC's structure and functionality, programmable government ledgers can protect data, streamline processes, and reduce fraud, waste, and abuse while simultaneously increasing trust and accountability. Consumers, businesses, and governments can share resources over a secure distributed ledger, mitigating single points of failure and protecting sensitive citizen and government data.

Government Benefits Balance controls and compliance, to help the government set benefit parameters and manage use, and to provide citizens with greater convenience and certainty of receipt. *Real-world example: controlled stimulus payments*	**Government Processes** Streamline processes across agencies, with auditable workflows and multi-agency applications *Real-world example: budget allocations and contract approvals*
Supply Chain Management Reduce complexity by managing data across multiple (often untrusted) parties, and reducing risk-prone manual paperwork, one up-one down visibility, and long execution times *Real-world example: streamlined procurement and payments*	**Financial Market Resiliency** Enhance the efficiency of and ability to provide oversight on financial market processes *Real-world example: interbank payments*

Figure 6. Real-world examples showing potential use cases for CBDC.

5.0 Conclusion

The size and scope of financial markets and the high recent rate of flux in payment system design make any discussion of CBDC necessarily complex. Given the myriad challenges and impacts of introducing CBDC, designing such a system calls for prioritizing flexibility and interoperability, allowing use cases to expand over time and reducing potential limitations on reach or effectiveness. Central banks are properly worried about getting "painted into a corner." At the same time, security and privacy remain paramount, while allowing authorities to monitor the legality of transactions.

Daml and Canton offer central banks the chance to model and test digital currencies and to explore potential use cases, while allowing for the creation of contracts that can be extended and used across one or more ledgers, blockchains, or existing hardware when the time is right. Daml gives central banks the ability to start small and to maintain control while exploring and updating the eventual designs of CBDCs.

A successful CBDC should be able to work seamlessly across multiple institutions, access platforms, and borders. Interoperability is crucial. Digital Asset has created a demo and open sourced its implementation, showing some key features including interoperability.

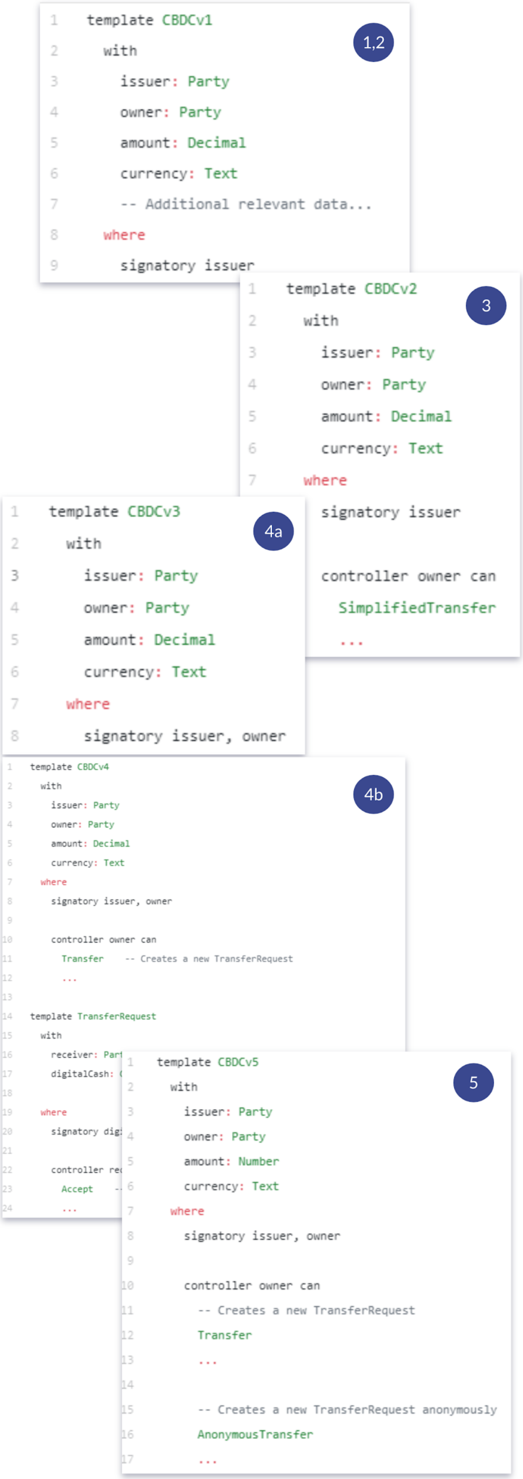
The objective of allowing a CBDC to tie into a wide range of workflows, and to reach its potential of transforming cross-border and domestic payments in both wholesale and retail markets, have led Digital Asset to make its interoperability functionality broadly available. The goal is to avoid the substantial risk of CBDCs being deployed on different, incompatible platforms.

By making this interoperability functionality available for public consumption, Digital Asset hopes to broaden the conversation about CBDC and allow more market participants to get involved.

Appendix - Technical Details

1. **Ensuring the Central Bank controls the volume of CBDC**, with rights and transparent trust relationships that support the creation and destruction of digital currency. Each Daml contract representing CBDC records the party that issues it.
2. **Proving authenticity and making it impossible to counterfeit CBDC**, since each Daml contract has verifiable signatories. Using digital signatures, if each issuer is mentioned in the contract and declared a signatory, no other party can create a contract representing CBDC without the issuer's consent.
3. **Providing transferability, similar to physical cash.** Each owner can be set up for 'simplified transfer', allowing them to exercise that choice only if they say who the receiver should be. Transfers happen atomically, meaning that all steps complete successfully or none of them do. In a simple transfer:
   a. the old contract is archived, effectively marking it as inactive
   b. The simplified transfer is executed, creating a new contract where the receiver is the rightful owner of the CBDC
5. **Supporting (a) consensual ownership and (b) transferability in financial transactions**, to ensure that the money belongs to the owner and the recipient must consent to the transfer. Consent is critical as owning money usually comes with responsibilities, such as taxes. To fix this, the issuer is added as the owner and added to the list of signatories (so can initiate a transfer). Once the receiving party accepts, all authorizations are collected and the transfer can be settled. Importantly, each contract can only be used for one transfer, preventing double spending.
6. **Allowing configurable privacy,** so that the parties to the transaction know only that step of the transaction - not what came before or what will happen next. For example, when you pay for something at a store, the merchant doesn't know where the money comes from and you don't know where it will go next. And if you pay in cash, the merchant may not even know the identity of the purchaser. Daml supports privacy with sophisticated modeling:
   a. Visibility rules guarantee that the chain of owners isn't disclosed to subsequent owners.
   b. Sub-transaction privacy ensures that parties only see the parts of the transaction in which they participate - even in a complex transaction.
   c. Parties can be promoted to be observers of a contract.

Where a payer requests a transfer and a receiver accepts it, a 'Anonymous Transfer' can be created to protect the privacy of both parties without sacrificing the integrity of the transactions or its permissions. Atomicity ensures that all steps must complete successfully or the transaction does not take place.



```
template CBDCv1
  with
    issuer: Party
    owner: Party
    amount: Decimal
    currency: Text
    -- Additional relevant data...
  where
    signatory issuer
```

```
template CBDCv2
  with
    issuer: Party
    owner: Party
    amount: Decimal
    currency: Text
  where
    signatory issuer

    controller owner can
      SimplifiedTransfer
      ...
```

```
template CBDCv3
  with
    issuer: Party
    owner: Party
    amount: Decimal
    currency: Text
  where
    signatory issuer, owner
```

```
template CBDCv4
  with
    issuer: Party
    owner: Party
    amount: Decimal
    currency: Text
  where
    signatory issuer, owner

    controller owner can
      Transfer    -- Creates a new TransferRequest
      ...

template TransferRequest
  with
    receiver: Part
    digitalCash: (

  where
    signatory digi

    controller rec
      Accept    --
      ...
```

```
template CBDCv5
  with
    issuer: Party
    owner: Party
    amount: Number
    currency: Text
  where
    signatory issuer, owner

    controller owner can
      -- Creates a new TransferRequest
      Transfer
      ...

      -- Creates a new TransferRequest anonymously
      AnonymousTransfer
      ...
```