# Central Bank Digital Currency

As the world moves toward digital-first experiences, the inefficiencies underpinning how businesses and consumers transact - in particular the way banks and financial institutions operate across internal and external systems - will remain problematic due to inaccessible data, complex operations, and unclear workflows.

New solutions such as distributed ledger technology and smart contracts may hold the key to solving long-standing banking and financing challenges, where complex transactions are handled on aging infrastructure, and the ability to capture and analyze data is hindered by information silos. From simple retail to sophisticated cross-border transactions, it has never been more important to move money quickly, track it carefully, and prevent fraud.

As a result of this need for more efficient monetary systems, Digital Currency is at the forefront of innovation discussions by Central Banks.

## Defining digital currency

Central bank digital currency (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. Central banks would issue CBDC in addition to or in lieu of cash. As with cash, the creation and destruction of money remain controlled by the monetary authority; its authenticity can be verified; it is transferable with transactions agreed by all participating parties; and owners have privacy. However, unlike physical currency, CBDC is highly efficient to store and use for transactions.

From a systemic standpoint, replacing physical currency with CBDC would allow central banks more control over exerting monetary policy and ensuring financial stability: For example, the supervising authority could also establish the rules for how funds are used. The transfer of money across banks and country boundaries would become more straightforward, as CBDC ownership records are updated at the Central Bank and different bank systems don't need to interact to facilitate payments.

Clearer, faster, and more transparent recordkeeping, and a single source of truth would make fraud or money laundering easier to identify and prevent. At the same time, reducing time and cost could spur innovation across payments and financial services.

Consumers benefit as well. Since CBDC is the central bank's liability, they would not have to rely on their bank to remain solvent for their money to be safe. Additional benefits include:

- Lower costs due to reduced transaction fees.
- Cheaper and quicker digital payments.
- More transparency about what their money is used for and what risk/reward profile they've accepted.
- Continued privacy protections, as details of their transactions would not be visible to those involved in preceding or following exchanges.
- Access for the unbanked or underserved, enabling those who don't have bank access or can't afford a bank account to have a CBDC account.

## Separating tokenization from digitization

Digital currency is often conflated with crypto currency when, in fact, digitization and tokenization are two very different things. Let's define the key differences.

| Tokenization (e.g., cryptocurrency) | Digitization (e.g., digital currency) |
|---|---|
| Digital cash | Digital assets |
| Freely transferable | Programmable transfer rights |
| Anyone can hold | Restricted ownership |
| Pseudonymous owners | Known owners |
| All data public to everyone | Data limited to stakeholders |
| Locked into one ledger | Portable across any ledger |

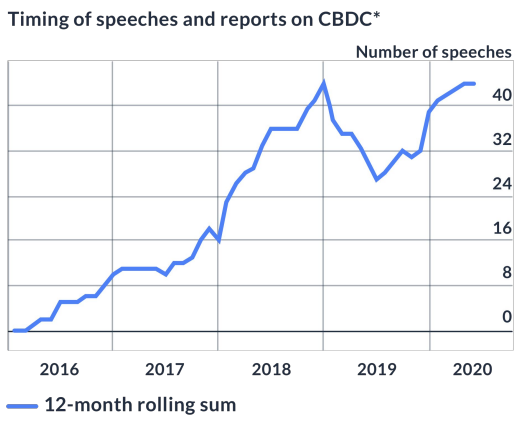
## Understanding market drivers

Support for digital currency is gaining momentum, with transactions that are more global and a financial services industry that is increasingly aware of interdependencies between systems.

The heightened regulatory agenda of the last two decades has uncovered limitations of aging, unconnected systems even as more importance is placed on knowing your customer, being able to prevent unauthorized or fraudulent transactions, and restricting access to funds for bad actors.

With global supply chains and individual transactions crossing borders, the provision of goods and services relies upon rapid payments and safe transactions. While essential, the need to involve trusted third parties adds layers and time to these activities.

**Central banks representing a fifth of the world's population reported that they were likely to issue CBDCs very soon.***




*Source: BIS; 12-month moving sum of the count of central bankers' speeches resulting from a case-insensitive search for any of the followin gwords/phrases: CBDC, central bank digital currency, digital currency and digital money

Introducing CBDC simplifies and in some cases, removes these challenges. A digital currency can be authenticated and tracked, rely on smart contracts to verify transactions, and utilize complex business logic to address different financial activities.

## Designing an approach

Often, conversations about digital currency jump right to potential technology stacks or distributed ledger options. But locking into a ledger provider, no matter how expert, means the new solution is restricted to a particular infrastructure or set of features - even before it begins to take shape.

This matters, because some ledger providers:

- Lack horizontal scalability and set an upper limit on the number of possible transactions;
- Have poor trust properties and cannot deal with malicious participants (to provide security, they are strongly permissioned, limiting participation to privileged, vetted users).

These restrictions are in direct opposition to the flexibility required of any useful currency.

But the sheer proliferation of ledger providers presents another challenge: if different central banks decide on different ledger providers, aren't new versions of technology silos being created and larger opportunities for efficiencies lost?

Any approach should be considered with an eye towards future-proofing, i.e, allowing for the broadest possible set of uses and greatest flexibility to expand as opportunities arise. This includes looking downstream to adoption, which must be equitable (users should be able to choose how they interact with the CBDC and not have to invest in a particular technology).

Given the potential complexity of rolling out CBDC, it's likely that most programs will start small but 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 distributed ledger partners.

## Identifying potential partners

Rather than narrowing the scope, consider starting with smart contracts and developing business logic that can run on multiple infrastructures or across ledgers. Digital Asset's core technology platform - Daml - is a platform for developing multi-party applications and leverages smart contract technology. Daml simplifies multi-party workflows and integrates with both traditional databases or enterprise-scale distributed ledger technology (DLT).

## Introducing Daml-driven CBDC

Daml provides a unique way to model and execute essential interactions. By separating business logic from systems code, the language is easy for business experts to understand and for technologists to use.

Daml creates a layer that sits across multiple applications, simplifying individual processes by connecting historically siloed information. It extracts data to create a single source of truth that can be used simultaneously across multiple applications, while combining common tasks to create efficiencies.

Daml gives offers built-in flexibility to include agreements, signatories, privacy, rights and more. The components can be built up front, added later, or incorporated as discrete modules to be used in certain scenarios. With the ability to model and establish discrete rights and permissions, Daml supports the following core features of CBDC:

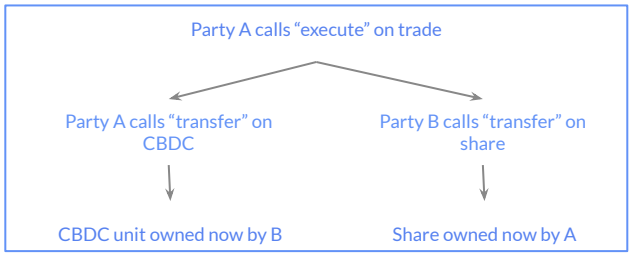
- **Trackability by authority**. Daml naturally supports auditing and tracking transactions, storing contracts (by ID) along with the history of each transaction. Observers of a Daml contract can be customized to allow for more transparency and visibility.
- **Closer control of ownership by authority.** The authority can control who owns money at a programmatic level: for example, to comply with restricted lists (e.g. OFAC).
- **Transaction safety.** Whether a transaction is simple or complicated, Daml can establish specific rules for money transfers that must be met atomically (e.g., all steps must be successful) for the transaction to occur.
- **Interoperability.** Using a common language and protocol, Daml would permit a CBDC system to bridge different ledgers and technologies.

*See Canton, p 4*

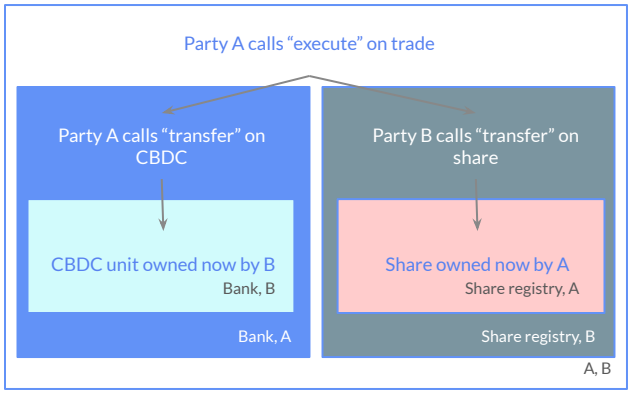
Daml's component approach delivers strong, secure data governance, workflow, data modeling protocols, and business interactions.

**Central banks reap significant benefits with Daml**

- Common data and processes can be extracted to simplify even the most complex, 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 recreated but digitized for efficiency, providing additional safeguards.
- Assets are safe with Daml. Developed by cryptography experts, Daml's declarative security model puts a stop to accidental data leakage, hacks, and break-ins.




*Example: Integrating CBDC money in a share trade workflow between parties. Party A transfers its CBDC money to party B in exchange for some 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.*




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

## Future-proofing with Canton

Given the extensive interactions of Central Banks with other institutions, individuals, and jurisdictions, it's essential to create a digital currency that can be freely used to support financing, trade, and commerce, whether at home or across borders. That level of interoperability requires using protocols that span different technologies, which in turn, requires the systems to speak to compatible ledgers.

**Canton**, a privacy-enabled distributed ledger that is enhanced when deployed with complementary blockchains, synchronizes any Daml-enabled blockchain or database. Canton allows for interaction among different ledger technologies including databases, permissioned or open blockchains, and hardware enclaves. It also makes Daml applications portable between different synchronization technologies, unlocking new users, new assets, and markets.

Canton extends Daml's ability to write a distributed application independent of the platform it will run on. With Canton, Daml workflows can run across multiple platforms and interoperate, even when the original platform owners didn't add this capability. Using 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.

At its core, Daml is a smart contract language and tooling mechanism that defines schema, semantics, and execution of transactions between distributed parties, and when layered with Canton, embeds critical interoperability functionality between systems while sharing data with entitled parties in a way that is always correct.

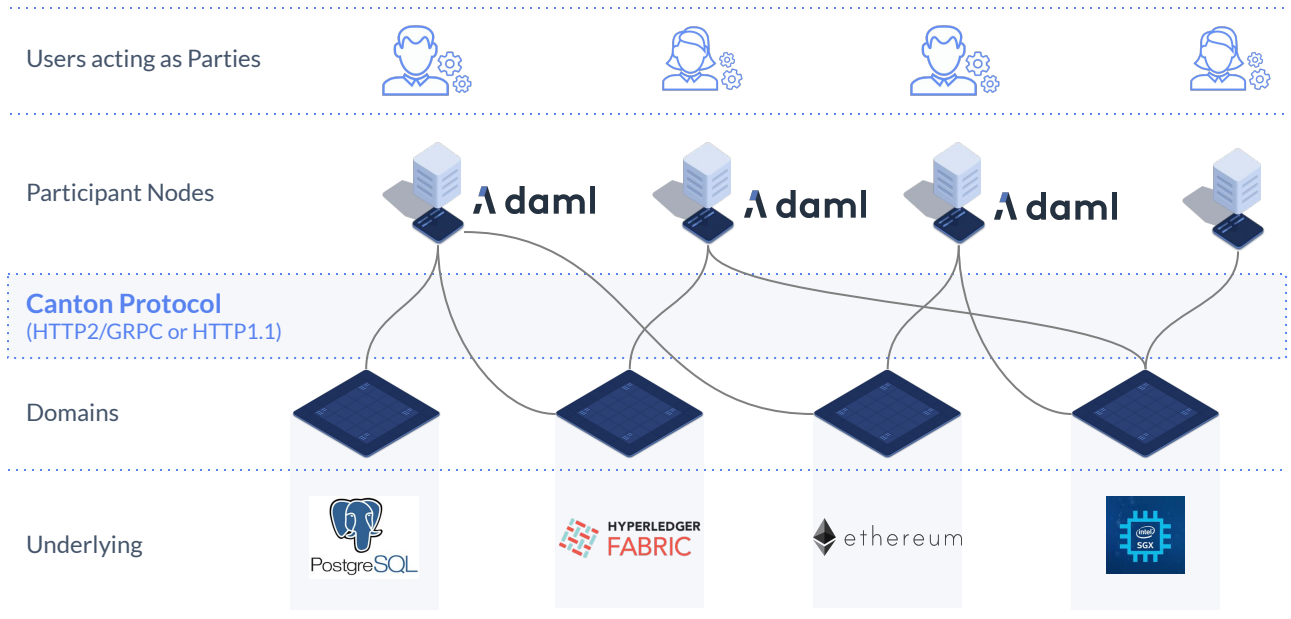
Canton can be extended without friction to new parties, ledgers and applications, building on other applications without requiring a central managing entity or global consensus within the network.

### Global composability
Different Daml-based ledger instances can interoperate using the Canton synchronization protocol

### Privacy and GDPR compliance
Canton is built around the principle of data minimization and the right to forget

### Integrity
Canton's synchronization protocol ensures your ledger is always in a valid state, and a corrupted state never occurs.

### Horizontal scalability
Canton has no upper bound on how many transactions per second it can process.



## Unlocking new possibilities with CBDC

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

### Government Benefits

Balance controls help the government set benefit parameters and manage use, and provides 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 eliminate 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 FX payments**

## Conclusion

The size and scope of financial markets and impact of changes to currency make any discussion on CBDC complex. Given the myriad of challenges and impact of introducing CBDC, designing such a system will require maximum flexibility and interoperability, allowing use to expand over time and precluding artificial limitations on reach or effectiveness. At the same time, security and privacy remain paramount to safeguard financial transactions and adhere to regulatory requirements.

Daml and Canton offer Central Banks the chance to model and test digital currency, and explore potential use cases, while creating clear 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 maintain control as they explore the important questions inherent in any currency decisions.

### Unlock innovation today

We welcome the chance to help you explore the opportunities that Daml and Canton can unlock.

### About Digital Asset

Digital Asset is a software and services provider that helps enterprises build economic value through interconnected networks. The company designs and delivers technology that reshapes legacy systems and workflows into efficient, secure, and interconnected applications. Daml, our core technology, is a platform for building multi-party applications. It extracts and simplifies business processes to make data accessible and optimizes workflows using smart contracts. Leading organizations across financial services, insurance and healthcare partner with Digital Asset to create new multi-party solutions that transform disparate silos into synchronized networks.

**Learn more and view additional case studies at**
https://digitalasset.com, or

Download the SDK and view our capital markets reference applications at https://daml.com

Connect with us on Twitter: @digitalasset @damldriven

Set up a call or meeting by contacting us at sales@digitalasset.com

## Appendix: The Technical Details

1. **Ensuring the monetary authority 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.

1,2

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

3

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

    controller owner can
      SimplifiedTransfer
      ...
```

4a

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

4b

```
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 dig

    controller re
      Accept    -
      ...
```

5

```
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
      ...
```