

WHITE PAPER

Achieving Uniformity of Tokenized Money Through Smart Contracts

Exploring the programmatic
interaction between CBDCs,
tokenized deposits, and stablecoins.



FIREBLOCKS IS A MASTERCARD
CBDC PARTNER PROGRAM MEMBER



 **Fireblocks**

Executive Summary

The uniformity of money is a simple concept that we often take for granted. It says that \$10 should be worth \$10, no matter how we spend it. In a world where people rely less on banknotes issued by central banks and where digital currencies are proliferating, preserving the uniformity of money has become a key motivation for central banks considering their own digital currencies.

In this paper, we explore how to preserve the uniformity of money in a world of digital assets. We contribute to the debate around privately and publicly issued digital currencies and relate them to the different forms of money that exist today.

We consider a vibrant and diverse digital asset ecosystem in which:

- ▲ The central bank issues a digital currency (CBDC) as a backing asset
- ▲ Commercial banks can issue fractionally-backed tokenized deposits, and
- ▲ Fintechs can issue fully-backed stablecoins.

We then illustrate a model of free convertibility between the fractionally-backed tokenized deposits and the fully-backed stablecoins, governed by rules set by the central bank, such that the consumer doesn't notice the difference.

Rather than simply offering a theoretical model, we also present the smart contract logic to make it operational and show through video demonstrations how this can be achieved today. It leverages the Fireblocks infrastructure, upon which countless projects operate at scale in the crypto asset industry. It also benefits from the knowledge and experience gained through a number of strategic financial services projects, helping to define the state-of-the-art in tokenized money, which we describe in more detail in the Foreword.

Although it is described as a wholesale CBDC for simplicity, the model is general enough to accommodate a retail CBDC held in a consumer wallet alongside tokenized deposits and stablecoins. Privacy is not addressed in depth, but we offer some considerations for extending this model to address privacy concerns directly in future work.

This paper should embolden central banks considering issuing CBDCs on the blockchain and help commercial banks understand their role in the future of money while preserving the valuable competition offered by non-bank fintechs.



VARUN PAUL

Senior Director for Central Bank Digital Currencies

Fireblocks

Foreword

About Fireblocks

The Fireblocks mission is to enable every business to easily and securely support digital assets and cryptocurrencies. Its digital custody, transfer, and settlement platform enables businesses to manage digital asset operations and build innovative businesses on the blockchain. Its multi-layer security approach eliminates single points of failure and insulates digital assets from cyberattacks, internal collusion, and human error, making it an ideal solution for companies looking to maximize security in their digital asset technology stack.

As a technology provider, Fireblocks offers critical infrastructure for a wide range of recognized institutions and cutting-edge startups looking to build out digital asset operations, including gaming companies, fintechs, banks, and FMIs. Its commitment to delivering a secure, easy-to-use, and scalable solution for emerging market entrants and use cases such as stablecoin issuance, NFT treasury management, and digital asset payments has established it as a leader in the blockchain infrastructure space. Fireblocks is widely considered one of the most secure custody technology solutions available, and its technology has become widely adopted by financial institutions such as BNY Mellon, SIX Digital Exchange, ANZ Bank, and Checkout.com.

Fireblocks is the most scaled and battle-tested digital asset platform in the market. As of November 2023, Fireblocks is trusted by over 1,800 institutional clients globally. It has secured over \$4 trillion in digital assets and its clients have created more than 130 million wallets using the platform.

In September 2023, Fireblocks announced its acquisition of BlockFold, a smart contract development and consulting firm specializing in advanced tokenization projects for financial institutions. Integrating BlockFold enriches Fireblocks' tokenization capabilities and ongoing innovation, enabling tier-1 financial institutions to bring more advanced tokenization projects into production as the market matures and evolves.

The State-of-the-Art in Tokenized Money

This section summarizes the strategic projects, through which Fireblocks is helping to define the state-of-the-art in tokenized money.



Australia and New Zealand bank issued the first Australian Dollar stablecoin, “A\$DC” in March 2022¹

Australia and New Zealand (ANZ) bank developed its stablecoin as a fully-backed payment token tied to the value of an Australian Dollar. It was initially designed to facilitate internal treasury operations before being used to demonstrate the transfer of value to a client and, more recently, used to purchase tokenized carbon credits on a public permissionless chain.



National Australia Bank executes multi-currency stablecoin cross-border settlement on Ethereum in March 2023²

National Australia Bank (NAB) developed its cohort of stablecoins and deployed its first seven currencies on Ethereum Mainnet in December 2022. These stablecoins are fully-backed liabilities of the bank. For example, its AUDN stablecoin is tied to the Australian Dollar.

In March 2023, NAB executed the world’s first intra-bank cross-border settlement using three of its seven stablecoins on Ethereum. The NAB eco-system of smart contracts leverages novel governance features, including system-wide emergency response and layered access control. The NAB eco-system of smart contracts is considered state-of-the-art for a bank-issued stablecoin.



Tel Aviv Stock Exchange’s Project Eden, launched in June 2023^{3,4}

Tel Aviv Stock Exchange (TASE) issued a payment token representing Israeli Shekels, while the Israeli Accountant General at the Israeli Ministry of Finance, in collaboration with TASE, created a digital government bond. In total, 12 banks, five domestic and seven international, participated in a traditional government bond auction via Bloomberg before the asset was issued and settled in real time on a permissioned blockchain.

Project Eden demonstrated the settlement of the tokenized government bond with tokenized shekel. It is widely considered to be one of the most advanced projects by a systemically important Financial Market Infrastructure (FMI) and represents the state-of-the-art for atomic settlement of financial instruments on a traditional exchange.

Bank for International Settlements Innovation Hub's (BIS IH) Project Mariana, published in June 2023⁵

Project Mariana investigated the viability of automated market makers (AMMs) improving the effectiveness, safety, and transparency of FX trading and settlement, eliminating some of their associated risks in FX markets. It explored a scenario in which central banks in France, Singapore, and Switzerland operated different blockchains. For this reason, the project also implemented bespoke domestic and international bridging with a fully qualified control framework, allowing the central banks to maintain full control over their respective central bank digital currencies (CBDCs), both native (domestic) and bridged (international).

Brazilian Central Bank's DREX CBDC Pilot, June 2023⁶

The Brazilian Central Bank announced the parameters of its CBDC pilot in June 2023. The central bank articulated its vision for a wholesale CBDC, including for the settlement of government bonds; and for a retail CBDC to build on the success of the real-time payments system, Pix, and offer programmable payments. In Brazil, the CBDC will co-exist alongside fractionally-backed digital liabilities issued by banks and fully-backed digital liabilities issued by non-bank payment institutions. Preserving Know Your Customer (KYC) rules means that liabilities issued by a financial institution can only be held by their customers. The intention of this setup is to preserve many of the features of today's financial system, while offering additional functionality and improved efficiency.

DIGITALX

DigitalX real-world asset tokenization of residential real estate, launched in July 2023⁷

DigitalX, in collaboration with Bricklet, launched a tokenized real estate offering, allowing for partial equity to be held in a tokenized fund and closing a financing gap in the housing market. Prospective homeowners get access to capital to fund their deposit on a new home, while investors in the fund receive a yield, which is derived from rent paid by the borrowers.

DigitalX also implemented an on-chain fund-of-fund architecture, allowing for highly flexible composability in terms of included asset classes and portfolio structure.

HSBC's e-HKD pilot, September 2023⁸

Building on its role as a distributor of Hong Kong Dollars, HSBC conducted a hypothetical e-HKD pilot with the Hong Kong University of Science and Technology (HKUST). Two hundred HKUST students and teachers participated in a one-week pilot to demonstrate the real-world use of a Hong Kong Dollar CBDC for retail payments and loyalty rewards on campus. In doing so, it illustrated the value of a retail CBDC even in a tiered distribution model.

“

In search of economic stability, there is a growing demand from businesses, consumers, and governments to reduce their reliance on a single currency or economy. The landscape is evolving rapidly with the emergence of CBDCs and stablecoins, each representing the goals and priorities set forth by their issuing bodies. These trends denote a larger shift to a diversified world economy, where many types of currencies, whether decentralized or state-issued, live alongside each other. As a result, a “basket of currencies” approach in global finance will likely evolve, requiring mechanisms of interactions between stablecoins, central bank digital currencies (CBDCs), cryptocurrencies, and fiat currencies.

Governments have sped up their exploration of CBDCs to increase efficiency, decrease transaction costs, and speed up settlement times. But the continued and future operation of CBDC and stablecoin networks – which will be integral to the financial system of tomorrow – will require the expansion of resilient and secure cloud-based infrastructures, regardless of whether the architecture is centralized or based on a distributed ledger template. Fireblocks’ report showcases the latest developments and innovations in this field, illustrating how it may look as the tokenization of money through smart contracts becomes a reality.

**MICHAEL GREENWALD**

Senior Executive and Global Lead for Digital Assets and Financial Innovation
Amazon Web Services

Table of Contents

09	Introduction
14	The Economic And Regulatory Framework
17	The Model: A Simplified Digital Monetary System
19	The Smart Contracts Describing The Model
25	Illustrative Flows Of Funds Between Customers
31	Considerations and Extensions Around Privacy
34	Conclusion

Introduction

This paper illustrates the uniformity of money in a world of digital assets. It adds to the debate around privately and publicly issued digital currencies and the different backing models in the monetary system today. It features a model of convertibility between fractionally-backed tokenized deposits issued by banks and fully-backed stablecoins issued by fintechs or non-banks. It includes high-level smart contract code and illustrative flows to explain how this interoperability is achieved in practice, and is accompanied by video demonstrations to show how this all comes together on the Fireblocks platform.

The Uniformity of Money

The uniformity of money is a simple concept that we often take for granted. It says that **\$10 should be worth \$10**, whether we use a banknote, a bank transfer, a debit card, or any other payment method. It's the idea that consumers shouldn't have to worry about the different ways in which they operate or the different entities they rely on. They should be freely interchangeable and should all work as equivalent forms of money when we want to use them.

The Evolution of Digital Assets To Date

Digital Assets are Hitting the Mainstream

Developments in the digital asset industry have caught the attention of every part of the financial system. In response to investor demand, the biggest banks and asset managers in the world have sought to offer access to crypto assets.^{9,10} Meanwhile, declines in crypto prices and speculative activity over the past 18 months have created space for corporates and financial institutions to focus on the utility offered by digital

assets. Some of the largest corporations in the world, including Starbucks and Nike, are using non-fungible tokens (NFTs) to revolutionize brand loyalty. Others are exploring token-gated access to live events, including concerts and football matches.¹¹

Digital Representations of Money are Proliferating

To access and interact with digital assets efficiently means paying with digital forms of money. In the face of cryptocurrency volatility, privately-issued stablecoins have served as the gateway (on- and off-ramp) between traditional money and the digital asset ecosystem. Stablecoins have provided a stable store of value between transactions, and adoption has grown rapidly. It is estimated that stablecoins were used to settle more than \$7 trillion in 2022.¹²

However, recent events have called into question the credibility of stablecoins, not least the collapse of Terra's algorithmic stablecoin but also the temporary de-pegging of Circle's USDC and Tether's USDT in times of market stress.^{13,14}



In response, banks have shown interest in stepping into the fold, offering to bring trust and credibility to the space as regulators start to define the rules more clearly. Banks in Australia, such as ANZ, have issued fully-backed Australian Dollar stablecoins, and there is increasing interest in tokenized deposits issued as a commercial bank liability, much like commercial bank money today.

Unlike fully-backed stablecoins, which ultimately lock up or drain liquidity from the banking system, tokenized deposits can enable credit creation and support economic growth. However, the recent collapse of Silicon Valley Bank in the U.S. and Credit Suisse in Switzerland has highlighted the inherent risks of commercial bank money in a fractional reserve banking system.

Central Banks See a Role for CBDCs

According to the Bank for International Settlements (BIS), around 90% of central banks around the world are exploring or actively developing their own CBDCs.¹⁵ Most major central banks have come to accept that digital assets are here to stay and have the potential to improve the financial system. Many also recognize that if stablecoins, NFTs, and other digital assets continue to proliferate, central banks must adapt to meet their duty to the public.



90%

of central banks around the world are exploring or actively developing their own CBDCs.

16%

of central banks consider it likely that they will have a wholesale CBDC within the next three years.

Many are considering wholesale CBDCs, in part because today's regulation requires financial assets to be settled in central bank money, so there is a need to keep up with the emerging tokenization of financial assets. But they also recognize the potential efficiencies that could be achieved by upgrading the technology at the core of the financial system without really affecting consumers. According to the BIS, 16% of central banks consider it likely that they will have a wholesale CBDC within the next three years.

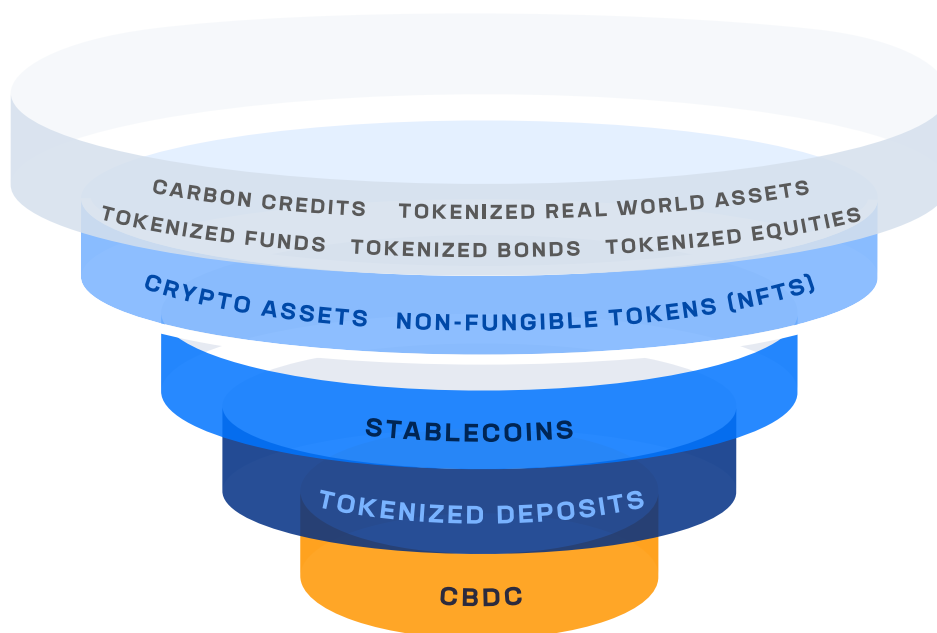
Retail CBDCs are politically more sensitive because they open up debates about how the central bank should and should not interact with the population, especially in an age where people are increasingly concerned about privacy. Despite these challenges, some central banks see it as their public duty to provide money in the form of retail CBDCs, in part to preserve the uniformity of money as spending moves away from banknotes into privately issued forms of money and towards a future of digital assets. The BIS survey suggests that 18% of central banks could have a retail CBDC within the next three years.

In truth, CBDCs, tokenized deposits and stablecoins are all just different forms of money, each with pros and cons, serving different purposes in the financial system. In a healthy and vibrant digital asset ecosystem, **these different forms of tokenized money will exist alongside one another**, providing consumer choice and financial system resilience. They will each find their most useful purpose, just as e-money exists alongside commercial bank money and central bank money today.

The Future of Digital Money

CBDCs issued as a liability of the central bank will be the ultimate “risk-free” asset in an economy, just as central bank money is today. They will likely serve as the fundamental unit of account in the digital asset ecosystem. Meanwhile, stablecoins may allow for programmability or be better suited for cross-border use cases, leveraging the blockchain’s ability to transcend national borders. Tokenized deposits could enable banks to continue to play their role in intermediating saving and borrowing, thereby creating credit and allocating it effectively. Together, all of these forms of money will enable consumers and investors to interact with the digital asset ecosystem of the future.

CBDCs at the Heart of a Vibrant Digital Asset Ecosystem



An Interoperable System of Digital Currencies

The concept of interoperability between different forms of tokenized money is not new. **In June 2023, the DREX Pilot in Brazil** started to explore how banks might issue tokenized deposits alongside non-bank payment institutions issuing stablecoins, each with different backing models reflecting their respective regulatory regimes and settled using a wholesale CBDC. The DREX proposals heavily informed the model presented in this paper.

In November 2022, the Regulated Liability Network (RLN) thesis described how the sovereign currency system comprises the liabilities of central banks and the liabilities of regulated private issuers (commercial banks and e-money issuers).¹⁶ It proposed that all the elements of today's sovereign currency system could be upgraded to digital and represented on a single ledger. It explored the potential for a (global) FMI with a shared ledger to make central bank money interoperable with commercial bank money, e-money, and regulated stablecoins in a digital system, just as they are today. However, some argue that this concept of a single FMI and shared ledger is too difficult to coordinate. History shows it can take many years to agree on and implement a single standard, as recently illustrated by the rollout of the ISO 20022 messaging standard. Unlike the RLN thesis, this paper is the first of its kind to explore how the same outcome of interoperability can be achieved with a minimal degree of coordination.

In June 2023, the BIS proposed a similar concept of a unified ledger as a new type of FMI to achieve the singleness of money and support tokenization.¹⁷ The concept of a unified ledger is attractive, but again, it can only succeed if everyone agrees on a single infrastructure. Although it recognizes the importance of public-private collaboration to minimize friction and realize the benefits of tokenization, it overlooks the role of non-banks and stablecoins in the future of money.

Other work has focused on cross-border interoperability to explore whether digital assets can address the significant costs and delays associated with cross-border payments – widely recognized as the largest inefficiencies in the global financial system. The BIS's project Mariana explores interoperability (bridges) between blockchains in different jurisdictions.¹⁸ Meanwhile, Swift's experiment with Chainlink's CCIP demonstrates the value of interoperability between blockchains to facilitate cross-border payments.¹⁹ Although this paper focuses on interoperability in a domestic context, a natural extension could include an externally sourced foreign exchange rate or enable interaction with an automated market maker.

The Economic And Regulatory Framework

Fractional Reserve Banking

Most financial systems around the world are built on the premise of fractional reserve banking. In a fractional reserve banking system, banks intermediate between savers and borrowers in the economy. Savers earn interest for depositing funds with banks. Banks can lend those funds out to borrowers, charging interest for the privilege, and banks earn a profit (the net interest margin) from the difference between the lending rate and the saving rate. Every loan issued by a bank creates new deposits somewhere in the banking system as the recipient deposits the funds (even temporarily) into a bank account. Those deposits are used for new loans, and the cycle continues. In this way, banks can be said to create money.

Fractional reserve banking is an inherently risky business because the banks have a mismatched balance sheet. On any given day, if a majority of savers turned up to a bank asking for their deposits back, the bank would not have enough liquid assets available to meet those demands on that day. And if some of the bank's loans turn sour, it may never be able to repay all savers in full.

However, reallocating funds between savers and borrowers is essential for a healthy economy. It enables productive businesses to access finance for growth opportunities and households to smooth their consumption in the face of variable income. Meanwhile, it enables people with excess funds to earn a return. Banks compete for deposits by offering attractive interest rates to savers and can earn greater profits if they maintain the net interest margin. Banks are also incentivized to allocate credit to the most productive uses to maximize their profits – they will be able to charge higher interest rates to borrowers taking on risky projects, but they carry a higher likelihood of default, and too many defaults will create a hole in their balance sheet and risk of insolvency. Banks are well-incentivized to find the right balance between the two.

Regulation

The profit incentive can still encourage excessive risk-taking, particularly if the bank underestimates the inherent risks in high-return investment projects. The potential difference in the maturity of saving and borrowing can also put the bank in a risky position. Due to the critically important nature of this credit intermediation function, regulators have set rules to manage these risks.

Supervisors regularly monitor their business models and strategies, and regulators impose a number of limits to safeguard the system. One example is the capital ratio, which requires the bank to retain around 5-15% of equity to absorb losses in the value of the bank's assets, including loans. In addition, there are liquidity requirements to ensure that the bank has a sufficient amount of highly liquid assets to return funds to savers if many call on their funds in a short period of time.

These safeguards help to protect the financial system, particularly ordinary customers, from this inherently risky business that banks carry out.

Deposit Guarantees

This setup enhances financial stability but, could not eliminate the risk of a run on the bank. For example, if a bank looks like it has made some poor lending decisions, it can dip into these buffers to ensure its continued survival. But if there is a perception that there are insufficient funds to cover all depositors (insolvency), savers are incentivized to pull their funds out, knowing that the last ones to act are more likely to lose their funds. The drying up of new funding exacerbates the bank's balance sheet mismatch and becomes a self-fulfilling problem. To counter that risk, governments create depositor protection schemes that insure deposits, usually up to a certain limit, so that customers have a reduced incentive to pull their funds out.

Resolution Regimes

Ultimately, there remains a risk that a given bank's liabilities could exceed its assets, leading to its failure. To protect customers and the broader economy, regulators rely on a resolution regime to wind up a bank's operations and ensure continuity of access to customer deposits. Recently, these regimes have created living wills for systemically important banks.

Implications

The banking system has a unique role in credit allocation and supporting economic growth. The service it provides is inherently risky, and through bitter experience of failures, regulators have developed rules to mitigate those risks, especially because they are so important to the system.

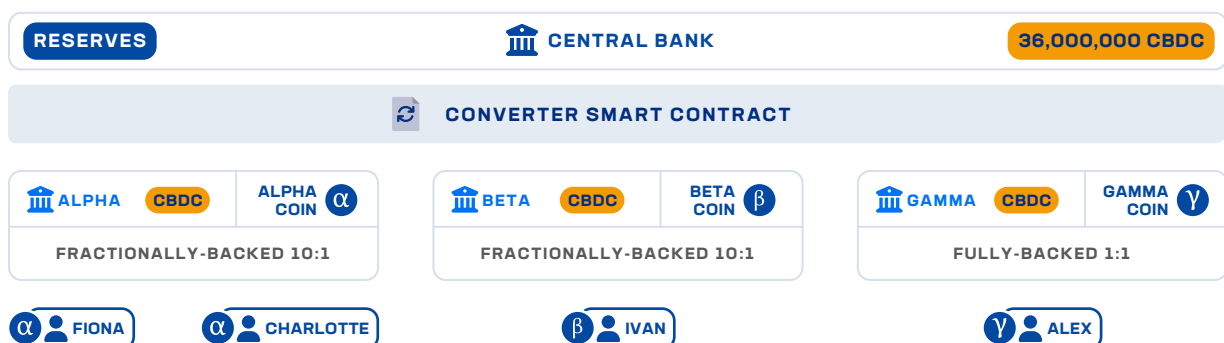
However, this regulatory regime is costly, not least for the banks that pay for the privilege of being supervised and regulated. That creates very significant barriers to entry and can make the banking system uncompetitive, which is why regulators are keen to promote competition from non-bank fintechs offering payment services.

Many countries have created e-money regimes to support a different, much less risky business model. E-money providers can offer accounts to customers, but customer funds must be deposited in segregated accounts at a regulated bank. In this way, the funds are bankruptcy-remote and protected by depositor protection schemes, up to a limit. E-money providers cannot offer interest on these funds and they cannot lend money. They also don't earn a net interest margin and therefore tend to focus on offering outstanding user experience for payments. This is arguably a less lucrative business model but is also less costly to operate.

The Model: A Simplified Digital Monetary System

We start with a simplified digital monetary system. For the purposes of this illustration, it is a closed economy with a single national currency. The central bank is responsible for authorizing and regulating banks, and has a credible regulatory regime that supports a fractional reserve banking system, as described in the previous section. The financial system also benefits from competition from non-bank fintechs, who are allowed to offer payment services to consumers. These fintechs or payment service providers are not permitted to perform maturity transformation and therefore do not present the same degree of risk to the financial system. Like the e-money regime that exists in many countries, customer deposits held by these fintechs must be fully-backed and bankruptcy-remote from the fintech in order to protect the consumer.

In this model, we have two banks, **ALPHA** and **BETA**, and a non-bank fintech, **GAMMA**. Each has a set of customers. We highlight two customers of **ALPHA** (**FIONA** and **CHARLOTTE**), one customer of **BETA** (**IVAN**) and one customer of **GAMMA** (**ALEX**).



Each institution is allowed to issue digital tokens, **ALPHA COIN**, **BETA COIN** and **GAMMA COIN** respectively. The monetary system is governed by a Central Bank that issues a wholesale CBDC.

Although we focus on a wholesale CBDC for simplicity, the model can be generalized to include a retail CBDC that could be held in customer wallets alongside **ALPHA COIN**, **BETA COIN** and **GAMMA COIN**. Most central banks that are considering retail CBDCs also intend to implement holding limits to allow for retail CBDCs to exist alongside privately issued digital money.

Consistent with e-money regimes, the digital tokens offered by **GAMMA** serve as a pure payment token. They are fully-backed by the wholesale CBDC. This 1:1 backing with a CBDC is hard-coded into the smart contract and helps to address the primary challenge around proof of reserves faced by today's most popular stablecoins.

Because of the comprehensive regulatory regime applied to banks, and the desire to preserve a fractional reserve banking model, **ALPHA** and **BETA** are allowed to issue fractionally-backed digital tokens. We assume a fixed ratio of 10:1 for mathematical simplicity in this model and to align broadly with bank capital ratios.

This programmatically guaranteed backing model is the main policy innovation in this paper. It codifies the credibility of the tokens issued by banks and non-banks and provides a clear and transparent illustration of the implications of banking regulation.

This setup is intended to mimic the existing monetary system in that commercial banks, under the supervision of a central bank/regulator can create commercial bank money, while e-money providers can offer payment services but do not create money. Financial systems that are overly reliant on banks have proved to be less competitive and less resilient to financial shocks. At the other extreme, an excess of customer funds in e-money accounts would drain the financial system of credit and is therefore undesirable. This regime attempts to balance these extremes to ensure equivalent outcomes for the consumer, while offering diversity and choice.

Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations require each of these financial institutions to identify customers they interact with and this prevents non-customers from holding the coins they have issued. To ensure the institutions can continue to comply with these regulations, the CBDC is used as a settlement asset here, in the same way that central bank money is used to settle outstanding balances between banks at the end of each business day.

The Smart Contracts Describing The Model

Context

A smart contract is a piece of code on a blockchain platform. It defines rules, conditions, and functions, like any other software. However, it is their self-executing nature that sets smart contracts apart.

When certain conditions specified in the smart contract's code are met and verified on the blockchain, the contract automatically triggers the pre-programmed actions. These actions could involve transferring digital assets between parties, updating data on the blockchain, or executing complex multi-step processes.

Standards like Ethereum Request for Comment 20 (ERC-20) play a crucial role in the blockchain ecosystem by providing a common framework and rules for creating and interacting with tokens on the Ethereum platform.²⁰ They improve interoperability and ease of adoption. With this objective in mind, we have adopted the ERC-20 token standard for all fungible tokens (units of account) within our model.

The following section describes how our model of a simplified Digital Monetary System is implemented at the smart contract level. It highlights the standards used as well as the governance and design considerations needed to achieve the goal of uniformity between different forms of tokenized money.

Design

The primary goal is to design a set of smart contracts that ensure tokens with different backing ratios are interchangeable and behave according to a set of pre-programmed rules to preserve uniformity of value. For example, the transfer of \$100 from a fractionally-backed unit of account must yield \$100 for the recipient regardless of whether the recipient holds that \$100 in a fractionally-backed or fully-backed unit of account.

In terms of the unit of account, the model uses two types:

A BACKING ERC-20

This can be thought of as central bank money (i.e., M0 or Wholesale CBDC), but could also be a liability issued by a consortium.

A FRACTIONALLY BACKED ERC-20

This smart contract is designed to be backed fractionally by the backing ERC-20.

Backing ratio: $0 < X \leq 100$

The backing ratio is defined and locked in upon deployment of the smart contract.

The model places no requirements on the **backing ERC-20** other than ERC-20 compliance. To this end, the model can use either a new ERC-20 implementation or an existing ERC-20 implementation (i.e., USDC) as a backing unit of account.

The **fractionally-backed ERC-20** token is created with the following details:

- ▲ Name
- ▲ Symbol
- ▲ Backing ERC-20
- ▲ Reserve Address (used for inter-token transfers/conversion)
- ▲ The backing fraction (e.g. 0.1 for 10% backing, 1.0 for 100% backing)

The **fractionally-backed ERC-20** smart contract does not implement the minting or burning functions that are commonly available in ERC-20 implementations, because this is not aligned with the backing nature of the token. Rather, the intent of the fractionally backed smart contract is to facilitate the transfer of tokens according to the backing fraction. Instead, the smart contract implements the **deposit** and **withdraw** functions, where the **deposit** is the action of depositing a specified amount of the backing token and stating the intended recipient of the face value **fractionally-backed ERC-20**.

```
function deposit(address to, uint256 amount) public onlyRole(ISSUER_ROLE) {
    uint256 mintAmount = amount * 1 ether / backingFraction;
    backingToken.transferFrom(_msgSender(), address(this), amount);
    _mint(to, mintAmount);
}
```

From the snippet above, we can also see that the **deposit** function is controlled by the **ISSUER_ROLE**, which is held by a very select set of addresses. In our illustrative case, the holders of this role are limited to the Treasury EOA (External Owned Address) and the Converter Smart Contract (see below for more detail).

The **withdraw** function is implemented in 2 guises; one implementation enacts a withdrawal, where the face value of the backed ERC-20 is burned, and the **fractionally-backed ERC-20** is transferred to the caller. This implementation is typically used by the bank or fintech to transfer funds.

```
function withdraw(uint256 amount) public onlyRole(ISSUER_ROLE) {
    uint256 backingAmount = amount * backingFraction / 1 ether;
    backingToken.transfer(_msgSender(), backingAmount);
    _burn(_msgSender(), amount);
}
```

A second implementation of the **withdraw** function is a delegated withdrawal, where the withdrawal is enacted on behalf of a third party. This implementation is used by the Converter Smart Contract. We use the default ERC-20 allowance mechanism to realize this function.

```
function withdrawFrom(address account, uint256 amount) public onlyRole(ISSUER_ROLE)
{
    uint256 backingAmount = amount * backingFraction / 1 ether;
    backingToken.transfer(_msgSender(), backingAmount);
    _spendAllowance(account, _msgSender(), amount);
    _burn(account, amount);
}
```

Once we have a plurality of **fractionally-backed ERC-20** tokens informed by a shared backing ERC-20 token, we have the building blocks to help us move closer to the uniformity of tokenized money.

Intra-token transfers (e.g., move **ALPHA COIN** from **FIONA** to **CHARLOTTE**) require no custom consideration. **Inter-token transfers** (e.g., send **ALPHA COIN** from **FIONA** and deliver **BETA COIN** to **IVAN**) require withdrawal from the source coin, supplementing from reserve for a shortfall (if any) to reach face value of the transfer and then deposit the destination coin, with a surplus (if any) being placed in reserve.

In service of this, the model implements a Converter Smart Contract controlled by the provider (i.e., a central bank). The Converter Smart Contract is designed as a public good in that it is not profit seeking. The only fee incurred in using the Converter Smart Contract is the gas of the underlying network (for gas-driven networks).

The Converter Smart Contract guarantees inter-token transfers are atomic in nature and will always yield face value equivalence. This Converter Smart Contract is the workhorse of this model and the main smart contract innovation offered by this paper.

At the heart of the conversion process we employ the following illustrative processing:

```
uint256 withdrawBackingAmount = amount * fromERC20.backingFraction() / 1 ether;
uint256 depositBackingAmount = amount * toERC20.backingFraction() / 1 ether;

uint256 fromReserveShortfall = amount - withdrawBackingAmount;
uint256 toReserveSurplus = amount - depositBackingAmount;
fromERC20.withdrawFrom(msg.sender, amount);
if ( fromReserveShortfall > 0 ) {
    backingToken.transferFrom(fromERC20.backingReserveAddress(), address(this),
    fromReserveShortfall);
}

backingToken.approve(address(toERC20), depositBackingAmount);
toERC20.deposit(recipient, depositBackingAmount);
if ( toReserveSurplus > 0 ) {
    backingToken.transfer(toERC20.backingReserveAddress(), toReserveSurplus);
}
```

The flow illustrated above is, in effect, executing exchange settlement on a per-transaction basis. This is key to the operating assumption that the face value being transferred is matched in the backing ERC-20 per transaction.

To control which **fractionally-backed ERC-20** tokens can operate in the ecosystem, the Converter Smart Contract makes available a registry of tokens allowed to engage in conversion.

```
mapping (FractionalBackedERC20 => bool) stablecoinRegistry;
```

The interplay between each institution's reserve account, their respective coins, and the pre-configured allowances is a critically important part of the configuration. The Converter Smart Contract needs sufficient allowance to withdraw from the reserve to achieve both symmetric and asymmetric conversion uniformity.

Additionally, we need to revisit the **ISSUER_ROLE** discussed earlier. To achieve uniformity in conversion, the Converter Smart Contract must hold the **ISSUER_ROLE** in terms of both the delegated withdrawal and deposit required.

At a glance the control dimensions are:

ATTRIBUTE	α ALPHA COIN	β BETA COIN	γ GAMMA COIN
Backing	CBDC	CBDC	CBDC
Backing	Yes	Yes	Yes
Coin ISSUER_ROLE members	Alpha Treasury EOA & Converter Smart Contract	Beta Treasury EOA & Converter Smart Contract	Gamma Treasury EOA & Converter Smart Contract
Reserve	Alpha Reserve EOA	Beta Reserve EOA	Gamma Reserve EOA
Reserve Allowance	Converter Smart Contract	Converter Smart Contract	Converter Smart Contract

Governance

From a governance and controls perspective, our model has three personas: the central bank, the bank/fintech, and the end users. The end users have no escalated privileges in this context.

The bank/fintech has privileges allowing it to hold the backing currency and having the role of **ISSUER_ROLE** for their respective fractionally-backed ERC-20s.

The central bank has escalated privileges spanning the mint and burn of the backing currency and participation therein. Over and above these privileges, the central bank controls the Converter Smart Contract, which maintains the curated set of **fractionally-backed ERC-20s** that are allowed to execute uniform transfers.

This is referred to as the registry of **fractionally-backed ERC-20s**, and the central bank holds the **REGISTRY_ADMIN_ROLE**, enabling it to curate eligible smart contract deployments.

The model requires that **fractionally-backed ERC-20** make their backing currency available via the **backingToken** attribute. The **backingToken** attribute signals the backing token of the **fractionally-backed ERC-20** (the CBDC for the purposes of this illustration). For uniformity of tokenized money to be applicable, the

respective **fractionally-backed ERC-20s** must be backed by the same token (i.e., the CBDC). The Converter Smart Contract uses this, in combination with the caller (the central bank for our purposes), to allow for addition to and removal from the participating **fractionally-backed ERC-20** registry.

The following is an illustrative implementation of the registry curation functions:

```
mapping (FractionalBackedERC20 => bool) stablecoinRegistry;

function registryAdd(FractionalBackedERC20 stablecoin) public
onlyRole(REGISTRY_ADMIN_ROLE) {
    require(stablecoin.backingToken() == backingToken, "FractionalBackedConvert:
ERC20 backingToken must match backingToken");
    stablecoinRegistry[stablecoin] = true;
}

function registryRemove(FractionalBackedERC20 stablecoin) public
onlyRole(REGISTRY_ADMIN_ROLE) {
    stablecoinRegistry[stablecoin] = false;
}
```


Illustrative Flows Of Funds Between Customers

Starting Balances

Let us assume that the financial system starts with 36 million CBDC denominated in the country's national currency, distributed evenly across the three financial institutions. Each financial institution holds 10 million in a Treasury (primary) account and 2 million CBDC in a Reserve account, which serves as a float.

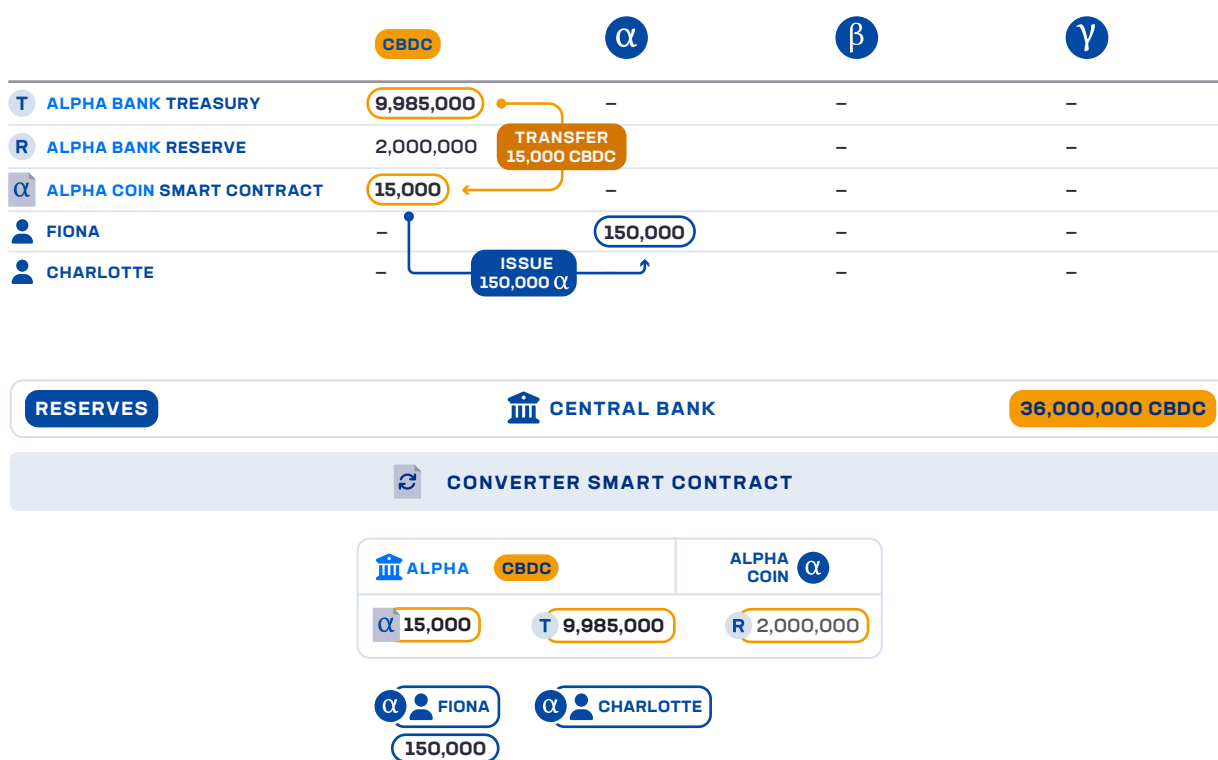
Both the Treasury and Reserve accounts are held and controlled by the financial institution. But the Converter Smart Contract has access to the Reserve accounts, as described in the previous section. The Reserve accounts can be considered equivalent to the reserves that the financial institution holds at the Central Bank in today's system.

	CBDC	α	β	γ
T ALPHA BANK TREASURY	10,000,000	-	-	-
R ALPHA BANK RESERVE	2,000,000	-	-	-
α ALPHA COIN SMART CONTRACT	15,000	-	-	-
FIONA	-	-	-	-
CHARLOTTE	-	-	-	-
T BETA BANK TREASURY	10,000,000	-	-	-
R BETA BANK RESERVE	2,000,000	-	-	-
β BETA COIN SMART CONTRACT	-	-	-	-
IVAN	-	-	-	-
T GAMMA BANK TREASURY	10,000,000	-	-	-
R GAMMA BANK RESERVE	2,000,000	-	-	-
γ GAMMA COIN SMART CONTRACT	-	-	-	-
ALEX	-	-	-	-
TOTAL CENTRAL BANK LIABILITY	36,000,000			

Deposit to Fiona

- ▲ At the start of the day, **FIONA**, a customer of **ALPHA BANK**, decides to convert 150,000 of the deposits she holds at **ALPHA BANK** into **ALPHA COIN**.
- ▲ To do this, **ALPHA BANK** transfers and locks 15,000 CBDC into the **ALPHA COIN** smart contract in order to mint (issue) 150,000 worth of **ALPHA COIN** according to the rules set out by the Central Bank, which it then deposits into **FIONA**'s wallet.



Because **ALPHA BANK** only has to lock up one tenth of the value in the **ALPHA COIN** smart contract, it retains the remaining nine-tenths on its balance sheet and can use those funds for lending. In this way **ALPHA BANK** can still create money in this model.



Fiona to Charlotte

- ▲ **FIONA** wants to transfer 25,000 to **CHARLOTTE**.
- ▲ She initiates the transfer and sends 25,000 **ALPHA COIN** to Charlotte's wallet.

As this is a simple transfer that takes place within the same bank, there is no change to the CBDC balances of the financial institutions nor of the amount locked in the **ALPHA COIN** smart contract.

	CBDC	α	β	γ
T ALPHA BANK TREASURY	9,985,000	-	-	-
R ALPHA BANK RESERVE	2,000,000	-	-	-
α ALPHA COIN SMART CONTRACT	15,000	-	-	-
 FIONA	-	125,000	TRANSFER 25,000 α	
 CHARLOTTE	-	25,000		



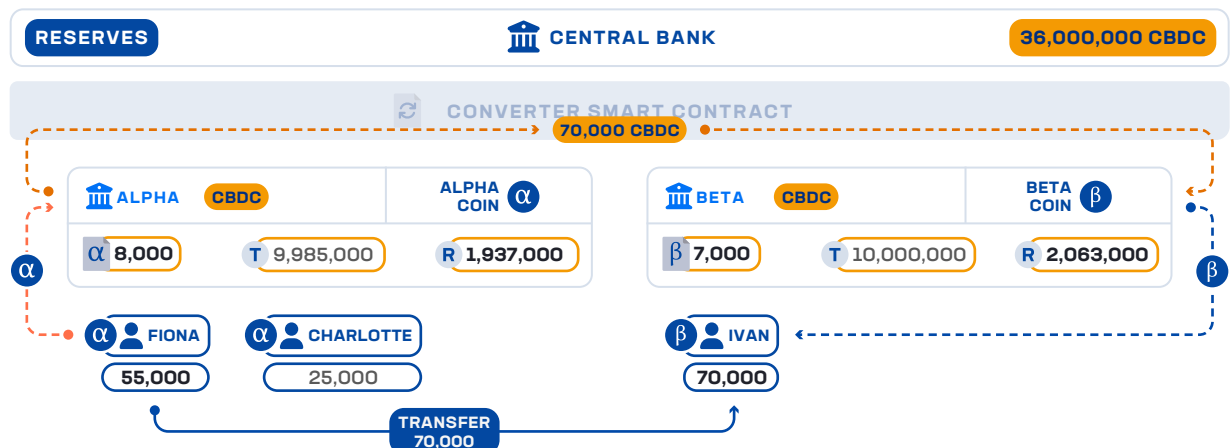
Fiona to Ivan

- ▲ FIONA wants to transfer 70,000 to IVAN.
- ▲ IVAN is not a customer of ALPHA BANK and, therefore, cannot hold ALPHA COIN.

	CBDC	α	β	γ
T ALPHA BANK TREASURY	9,985,000	-	-	-
R ALPHA BANK RESERVE	1,937,000	-	-	-
α ALPHA COIN SMART CONTRACT	8,000	-	-	-
α FIONA	-	55,000	-	-
α CHARLOTTE	-	25,000	-	-
T BETA BANK TREASURY	10,000,000	-	-	-
R BETA BANK RESERVE	2,063,000	-	-	-
β BETA COIN SMART CONTRACT	7,000	-	-	-
β IVAN	-	-	70,000	-

Annotations:

- Transfer of 7,000 CBDC from Alpha Bank Reserve to Beta Bank Reserve.
- Transfer of 63,000 CBDC from Alpha Bank Reserve to Beta Bank Treasury.
- Burn of 70,000 α from Fiona's wallet.
- Issue of 70,000 β to Ivan's wallet.



- ▲ FIONA initiates the transfer by instructing ALPHA BANK to burn the 70,000 ALPHA COIN in order to release 7,000 CBDC (1:10 backing) to the Converter Smart Contract.
- ▲ The Converter Smart Contract has permission to pull the 63,000 CBDC shortfall (nine-tenths) from ALPHA BANK'S Reserve account.
- ▲ The full complement of 70,000 CBDC is sent to BETA BANK.
- ▲ BETA BANK locks 7,000 CBDC in the BETA COIN smart contract, allowing it to mint (issue) 70,000 BETA COIN according to the rules set by the Central Bank, which it deposits into IVAN'S wallet, as per FIONA'S request.
- ▲ BETA BANK keeps the surplus of 63,000 (nine-tenths) CBDC in its Reserve account.

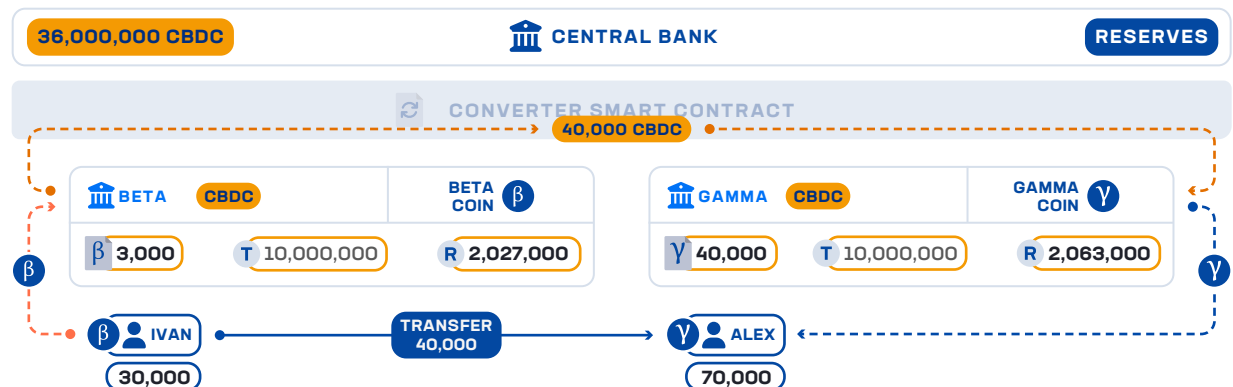
Following this symmetric transfer between banks, the banking system as a whole remains the same size. But **ALPHA BANK** now has a smaller balance sheet, while **BETA BANK** has expanded its deposit base from which it can issue additional loans, thus preserving a given bank's incentive to collect deposits in today's financial system.

Ivan to Alex

- ▲ **IVAN** wants to transfer 40,000 to **ALEX**.
- ▲ **ALEX** is not a customer of **BETA BANK** and, therefore, cannot hold **BETA COIN**.
- ▲ **IVAN** initiates the transfer by instructing **BETA BANK** to burn 40,000 **BETA COIN** in order to release 4,000 CBDC (1:10 backing) to the Converter Smart Contract.
- ▲ The Converter Smart Contract has permission to pull the shortfall of 36,000 CBDC (nine-tenths) from **BETA BANK'S** reserve account.
- ▲ The Converter Smart Contract sends the 40,000 CBDC to **GAMMA FINTECH**.
- ▲ Because Gamma's stablecoin must be fully backed, it locks the full 40,000 CBDC in the **GAMMA COIN** smart contract in order to mint (issue) the 40,000 **GAMMA COIN** and then deposits them into **ALEX'S** wallet, as per **IVAN'S** request.

Following this asymmetric transfer, **GAMMA'S** reserve is unchanged, but the banking system has lost 36,000 of reserves, and there is a reduction of credit creation capacity in the economy. This mimics the impact of customers switching from bank deposits to e-money in today's financial system.

	CBDC	α	β	γ
T BETA BANK TREASURY	10,000,000	-	-	-
R BETA BANK RESERVE	2,027,000	-	-	-
β BETA COIN SMART CONTRACT	3,000	-	-	-
IVAN	-	-	30,000	-
T GAMMA BANK TREASURY	10,000,000	-	-	-
R GAMMA BANK RESERVE	2,000,000	-	-	-
γ GAMMA COIN SMART CONTRACT	40,000	-	-	-
ALEX	-	-	-	40,000
TOTAL CENTRAL BANK LIABILITY	36,000,000			



Considerations and Extensions Around Privacy

The model presented here does not consider privacy in any real depth, but privacy is a top priority for most central banks. Commercial banks and other financial intermediaries would be unwilling to interact with an infrastructure that revealed their balances and transactions to their competitors. In times of stress, there are arguments for central banks being able to act as the lender of last resort privately in order to stabilize, rather than to exacerbate a precarious situation.

More importantly, many central banks know that, given a choice, the public will only adopt a retail CBDC that guarantees their privacy. In a world of surveillance and big data, people are highly sensitized to the idea that governments could use this new technology to monitor their activity and restrict how they spend their money. Once an obscure four-letter acronym, CBDCs have become highly politicized in a number of countries around the world.²¹

Central banks like the Bank of England have made clear they have no interest in having access to personally identifiable information and transaction data, not least because of the operational and compliance implications that go with it.²² These central banks have also drawn a distinction between privacy and anonymity, noting that they could never implement a completely anonymous payment token, as it would break the rules in the financial system that seek to prevent money laundering and terrorist financing. In response to this nuanced message, conspiracy theories abound, speculating about what central banks and governments could do with the data.

“

Many central banks will attempt to reassure the public by reminding them of the privacy protections that are enshrined in law. But some will be bold enough to propose technological solutions that give individuals greater control of their data in a way that can both enable identification and enhance privacy.

Part of the challenge likely stems from the notion that blockchains are designed as shared ledgers and are transparent, as a foundational principle; the fact that digital currencies also enable “programmability” only adds to the skepticism. To address concerns over privacy and control, central banks therefore have to go to great lengths to reassure people, both through legislation and design.

As an example, some concerns can be addressed through the design, by maintaining the role of intermediaries in the financial system – to monitor transactions, prevent fraud and terrorist financing, and manage customer complaints. That creates a degree of separation between the individual and the state, but that separation is weakened if the central bank can still observe every transaction on a single ledger. Many central banks will attempt to reassure the public by reminding them of the privacy protections that are enshrined in law. But some will be bold enough to propose technological solutions that give individuals greater control of their data in a way that can both enable identification and enhance privacy.

Extending the Model in this Paper for Privacy

The model in this paper makes the simplifying assumption that everything takes place on one blockchain. It can then use a whitelist in the **ALPHA COIN**, **BETA COIN**, and **GAMMA COIN** smart contracts respectively to ensure that the banks and fintech in this model only interact with known customer wallets and thereby adhere to KYC rules.

A natural extension in the digital asset ecosystem would be to allow each entity to deploy and manage its own sub-chain. The Central Bank would own and maintain one sub-chain, on which it would interact with the intermediaries. **ALPHA BANK** would own and maintain a sub-chain to interact with its customers, as would **BETA BANK** and **GAMMA FINTECH**. This would help to ensure that **BETA BANK** has no visibility of the transactions taking place in Alpha’s ecosystem, for example. It would also help to ensure an additional degree of separation, such that the central bank has no way of observing transactions taking place in the **ALPHA BANK** blockchain, thus protecting the privacy of **ALPHA BANK’S** customers.

Technologies Designed to Enhance Privacy

Cutting-edge technologies such as zero-knowledge proofs can provide an additional degree of privacy. Through encryption of wallet addresses and transaction details, these technologies can protect individuals' identity and transactions from others on the blockchain while also enabling the sharing of specific information with the recipient or their wallet provider to comply with regulations.

Zero-knowledge proofs could also support the development of a powerful type of privacy-enhancing digital identity. By combining a form of on-chain digital identity with these zero-knowledge proof technologies, individuals would be able to reveal parts of their identity and relevant data to counterparties they wish to interact with and as required by law, while hiding their identity and data from everyone else. That differential data sharing is arguably the definition of privacy.

These technologies are not yet battle-tested or available at scale. But digital currencies that can harness these technologies will be able to enhance individual privacy, while complying with the rules in the financial system. That could be a highly valuable proposition for individuals in the near future.

Conclusion

This paper has explored the programmatic interaction between CBDCs, tokenized deposits, and stablecoins. It has illustrated a practical way to achieve uniformity of tokenized money through smart contracts.

It describes roles for:

- ▲ The central bank, which issues a digital currency (CBDC) as a backing asset;
- ▲ Commercial banks, which can issue fractionally-backed tokenized deposits; and
- ▲ Fintechs, which can issue fully-backed stablecoins.

It then illustrates a model of free convertibility between the fractionally-backed tokenized deposits and the fully-backed stablecoins, governed by rules set by the central bank, such that the consumer doesn't notice the difference.

It leverages the Fireblocks infrastructure, upon which countless projects operate at scale in the digital asset and crypto industry, but it is by no means exclusive. It also benefits from the knowledge and experience gained through a number of strategic financial services projects, helping to define the state-of-the-art in tokenized money.

It should **embolden central banks** that are exploring CBDCs to build them on the blockchain and harness the programmatic benefits of this rapidly developing technology.

It should **help commercial banks** understand their role in the future of money and enable them to start developing tokenized deposits now, with a view to how they could interact with CBDCs in the future.

It should **empower fintechs** to continue innovating, while positioning their role in the future digital asset ecosystem.

We remain in the early stages of CBDC development around the world. In the hands of the decision makers at central banks, commercial banks, and fintechs, the ideas presented in this paper should take us one step closer to the future of money.

Endnotes

- 1 <https://media.anz.com/posts/2022/03/anz-completes-landmark-stablecoin-payment>
<https://media.anz.com/posts/2023/april-/anz-and-grollo-partner-to-trade-tokenised--australian-carbon-cre>
- 2 NAB News: NAB completes world first with cross border stablecoin transaction
- 3 Fireblocks blog: project eden technical perspective
- 4 PRnewswire: tel aviv stock exchange and the israeli ministry of finance successfully completed the project eden proof of concept issuing a government digital bond on a dedicated blockchain platform
- 5 Project Mariana: CBDCs in automated market-makers
- 6 Reuters: Brazil announces pilot digital currency seeking to leverage financial services
- 7 Market Herald: DigitalX launches asset reference token fund
- 8 <https://hkust.edu.hk/news/research-and-innovation/hkust-and-hsbc-conduct-one-week-hypothetical-e-hkd-pilot>
- 9 <https://www.bnymellon.com/us/en/about-us/newsroom/press-release/bny-mellon-launches-new-digital-asset-custody-platform-130305.html>
- 10 <https://www.forbes.com/advisor/investing/cryptocurrency/spot-bitcoin-etf/>
- 11 <https://www.forbes.com/sites/digital-assets/2023/07/07/how-companies-like-starbucks-and-nike-are-innovating-with-web3-customer-loyalty-programs/>
- 12 <https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-3ae>
- 13 <https://www.coindesk.com/markets/2023/03/11/usdc-stablecoin-depins-from-1-circle-says-operations-are-normal/>
- 14 <https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/>
- 15 <https://www.bis.org/publ/bppdf/bispap136.pdf>
- 16 <https://regulatedliabilitynetwork.org/wp-content/uploads/2022/11/The-Regulated-Liability-Network-Whitepaper.pdf>
- 17 <https://www.bis.org/publ/arpdf/ar2023e3.htm>
- 18 https://www.bis.org/publ/othp_mariana.pdf
- 19 <https://www.swift.com/news-events/press-releases/swift-unlocks-potential-tokenisation-successful-blockchain-experiments>
- 20 <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>
- 21 <https://www.coindesk.com/policy/2023/07/17/ron-desantis-promises-to-ban-cbdcs-if-elected-president/>
- 22 <https://www.bankofengland.co.uk/speech/2023/october/jon-cunliffe-speech-at-the-economics-of-payments-xii-conference>

About Fireblocks

Fireblocks is an enterprise-grade digital asset security platform for moving, storing, and issuing digital assets. Fireblocks enables financial institutions to securely build, run and scale digital asset operations through the Fireblocks Network and MPC-based Wallet Infrastructure.

The company has secured the transfer of over \$4 trillion in digital assets and offers a unique insurance policy that covers assets in storage & transit.

To see Fireblocks in action reach out to info@fireblocks.com.

Learn more at [Fireblocks.com](https://fireblocks.com).

\$4T

DIGITAL ASSETS
SECURELY TRANSFERRED

1,000s

INSTITUTIONAL CUSTOMERS

24/7

GLOBAL
CUSTOMER SUPPORT

