A 2024 Primer for Digital Money

Authors

Andreas Park

University of Toronto

Jona Stinner

Witten/Herdecke University

GLOBAL RISK INSTITUTE

DECEMBER 2023

A 2024 Primer for Digital Money

Andreas Park, University of Toronto
Jona Stinner, Witten/Herdecke University

Overview

This primer is the third part of a series of explainers for the emerging world of digital finance; the first was on crypto-asset trading, the second covered crypto-asset credit markets. This primer discusses digital money in particular privately-issued stablecoins – representations of a fiat currency on a blockchain – and central bank-issued digital money. We describe the different forms of this new type of money, how they are created and by whom, how they maintain their stability (or not), and what risks and opportunities emerge from their increasing proliferation.

What is digital money?

Money in the digital age exists in various electronic forms: bank deposits or balances in payment apps like Paypal or WeChatPay are electronic ledger entries in the databases of the respective institutions. There are also peer-to-peer cryptocurrencies, such as Bitcoin, that store registries in a decentralized blockchain. This report covers digital money that operates on platforms outside of the existing banking system but that represent traditional fiat currencies.

We are interested in two types: government or central-bank-issued digital money, commonly referred to as central bank-issued digital currency (CBDC), and non-government-issued or generated digital money, typically called stablecoins.

A CBDC is a liability of the central bank, like cash or reserves (in the U.S., these are deposits in so-called Fed master accounts). A privately issued stablecoin is a digital representation of a fiat currency that is backed by existing assets, most commonly commercial bank deposits or high-value liquid assets such as short-term treasuries or repurchase agreements (repos). The primary objective of a stablecoin is to maintain a 1:1 peg to a fiat currency.

Beyond the conventional backing arrangement in fiat currencies, some recent variations include stablecoins representing fractional ownership of a Treasury bill, which pays interest. In other cases, the stablecoin strives to maintain a price peg to specific assets such as gold, a diversified basket, or cryptoassets and thus resembles a tokenized asset. Finally, there have been some attempts to develop unbacked stablecoins, relying on an algorithmic monetary policy. However, all attempts thus far have proven unsuccessful due to inherent flaws in their design. To date, a functional algorithmic stablecoin remains elusive (we are, however, unaware of a conclusive mathematical proof showing that they are impossible).

From a broader perspective, economists categorize various types of money. Given the differences in designs, issuance, and backing arrangements, CBDC and stablecoins would add differently to these categories. The monetary base, or M0, comprises bills or cash in circulation and commercial bank reserves held at the central bank. A more comprehensive measure of money in an economy is M1, which includes demand deposits held at commercial banks. A newly-issued CBDC would add to M0, whereas a privately-issued fiat-backed stablecoin would represent existing assets and thus does not even add to M1.

There are additional subtleties: commercial bank deposits are claims on the specific bank where the deposit resides (sometimes also called "inside" money). These deposits carry inherent risk compared to cash, as the issuing institution may face failure. A notable achievement of central banks is persuading the public to perceive these various forms of money as the same. Functionally, commercial bank deposits are fungible across banks from the users' perspective, but payments within the banking system necessitate a realignment of the internal ledgers between banks.

A stablecoin operating on ledgers outside the realm of traditional banking, such as a blockchain, represents a claim on the issuing company, which may fail. Stablecoins issued by different entities are separate assets and not fungible – they are traded in an open market, and their relative exchange rate may not be 1:1.

Types of Stablecoins

Stablecoins exhibit two primary structures: fully/over-collateralized, or under-/un-collateralized. To simplify the exposition, we will refer to these as "backed" and "unbacked." In the case of a backed stablecoin, users initiate a deposit and, in return, receive tokens. In contrast, unbacked stablecoins generate tokens through a specific, often algorithmic, mechanism.

Backed stablecoins can be centrally created, typically off-chain, by a specific entity, or decentralizedly generated on-chain through a smart contract. Conditional on the nature of the collateral, assets are held in off-chain custody (e.g., fiat currencies) or on-chain within a non-custodial smart contract (e.g., cryptoassets).

Fiat-backed centrally-issued stablecoins

The most widely known fiat-backed, centrally issued stablecoins are: USDT, issued by Tether Inc., and USDC, issued by Circle Inc. The underlying principle is straightforward: for every stablecoin in circulation, the issuer maintains an equivalent amount of dollars in a bank account or other high-quality asset, such as very short-term treasuries or overnight repos for which duration risk is negligible.[1]

These stablecoins can be issued in pull or push transactions: in the former, a customer makes a deposit and receives funds in return. In the latter, the issuer creates the tokens, sells them on the open market, and deposits the proceeds in high-quality assets. Notably, no stablecoin issuer currently possesses a reserve account with a central bank, and securing sufficiently safe backing assets poses a non-trivial challenge.

For example, the collapse of Silicon Valley Bank (SVB) in March 2023 reveals the vulnerability of traditional bank deposits. At the time of SVB's collapse, Circle, in a bid for transparency, disclosed that 77% of its holdings were in 3-month or shorter U.S. Treasury Bills at BNY Mellon, a trusted custodial services provider. The remaining funds were held in cash deposits with Customers Bank, BNY Mellon, SVB, and Signature Bank. Following FDIC's closure of SVB and Signature, Circle relocated its deposits from these two banks to BNY Mellon and outsourced its asset management to Blackrock.

Stablecoin issuers capitalize on interest earned from the collateral, often without transferring these earnings to stablecoin holders. This renders stablecoin issuance a very profitable business in an

[1] Loosely, duration risk refers to the risk that pertains to the market price of a fixed income asset. For instance, a 3-month U.S. treasury has no risk of default, but an increase in interest rates would lower the market value of this asset. If the stablecoin issuer has to sell this asset, they may incur a loss that may cause the stablecoin to be undercollateralized.

environment with positive rates. A recent innovation in this area is the stablecoin USDM, which represents fractional ownership of a T-bill, with interest being distributed to depositors.

Centralized, backed stablecoins are issued by firms that are subject to regulatory oversight. In theory, various regulators could have jurisdiction over U.S.-based stablecoin issuers. This includes the Federal Reserve, due to their connection to treasury markets; the Office of the Comptroller of the Currency, which might categorize stablecoins as "new" money; or the Securities and Exchange Commission (SEC), viewing stablecoins as a form of money market fund and, consequently, a security.[2] As far as we know, in practice, U.S.-based stablecoin issuers are regulated by relevant state regulators in the same way as payment providers.[3]

Decentralized and Backed Stablecoins

Asset-backed, decentralized stablecoins utilize blockchain-based algorithms (also called smart contracts) to allow users to create stablecoins upon depositing collateral. In what follows, we refer to the MakerDAO Protocol to exemplify the fundamental architecture.

The native stablecoin of the Maker protocol is called DAI. Each DAI token represents a claim against an over-collateralized loan,, and a distinct incentive mechanism aims to keep its price at 1 USD. DAI is held in cryptocurrency wallets and is supported on most popular blockchains, such as Ethereum.

To "mint" new DAI, a user enters a Collateralized Debt Position (CDP) by depositing cryptoassets into a smart contract known as a vault. The contract determines the rules for creating and liquidating this de facto loan. It details factors such as the quantity of DAI generated based on the deposited amount and its quality, as well as the associated interest payments.

CDPs require over-collateralization of typically 150% to safeguard against price fluctuations in the volatile collateral asset. So-called price oracles continuously provide the collateral value in a numeraire, which is then cross-referenced with the CDP in DAI to maintain stability. Collateral remains locked within the contract until its release upon repayment, which simultaneously triggers the destruction (or burning) of the initially minted amount of DAI. The Maker protocol accepts a range of assets for DAI creation, including various cryptoassets, real-world assets, and liquidity deposits in platforms like UniSwap.[4]

Similar to DeFi lending protocols, the Maker protocol uses a process to settle and liquidate deposits or vaults with insufficient collateral values.[5] Unlike lending platforms such as Compound and Aave, MakerDAO auctions off the collateral from low-collateral vaults. It is important to stress that vaults become eligible for liquidation well before the loan is "underwater" (i.e., when the loan value exceeds the value of the collateral) – just as margin traders receive margin calls early.

[2] It is difficult to see that the latter approach of classifying stablecoins as securities is productive and useful unless the goal is to prevent the usage of them. Stablecoins commonly do not provide any interest or earnings, which is typically an intuitive pre-requisite for an asset being an investment contract. It is also not clear how a stablecoin issuer could comply with prospectus requirements, given that stablecoins can be exchanged peer-to-peer and held in self-custody. Overall, stablecoins are fundamentally payments tools.

[3] Some payment providers actually issue stablecoins, such as Paypal.

[4] The parameters of the Maker protocol are governed by the decentralized-autonomous organization of MKR token holders. Important voting rights of the tokens holders comprise decisions on the assets, which are accepted for creating DAI, and interest rates such as the stability fee and savings rate.

[5] An introduction into the mechanics of DeFi lending protocols is provided in Park & Stinner (2023).

Table 1: Types of Stablecoins

The table provides an overview over the main types of stablecoins, based on the issuance mechanisms that we detail in the main text. This list is illustrative and not exhaustive, as there are numerous stablecoins with hybrid formats, such as FRAX, AMPL, or ESD, combining several of the above characteristics.

	Collateralization	Collateral Asset	Issuance	Transparency	Pegging Mechanism	Examples
Central issuance	Fully collateralized	Typically fiat currencies (sometimes commodities)	Off-chain	Limited and periodic disclosure of reserve assets	Arbitrage	USDT, USDC, BUSD, TUSD
Decentralized issuance via loans	Over-collateralized	Primarily crypto- and tokenized assets	On-chain	Full real-time disclosure via blockchain	Arbitrage, interest rates	DAI, FEI
Algorithmic issuance	Implicit; typically under-collateralized	Primarily (related) crypto-assets	On-chain	Full disclosure via blockchain	Arbitrage, elastic supply	UST/LUNA, TRON

The evolution of the DAI liquidation mechanism demonstrates the self-correcting nature within the crypto space. In March 2020, a sudden 40% decline in ETH's value triggered numerous DAI vault liquidations. However, due to network congestion and a shortage of DAI (needed to settle debts in a liquidation auction), DAI traded at a premium, causing the liquidation process to falter. MakerDAO responded by modifying its protocol, introducing the "Peg Stability Module." This smart contract allows users to exchange USDC stablecoins for DAI tokens instantaneously. In May 2021, when markets saw a similar decline as in 2020, the DAI liquidations worked as intended.

The Peg Stability Module also established a direct pricing link between USDC and DAI: over the weekend of March 11-12, 2023, when the future of SVB depositors was uncertain, the USDC coin fell to around $.95 per USDT due to concerns surrounding Circle's deposit with SVB. During this period, DAI continued to trade on par with USDC and thus at a 5% discount to USDT.

Unbacked Decentralized Algorithmic Stablecoins

For a decentralized, algorithmic stablecoin, a smart contract manages the money supply and creates arbitrage incentives to keep the exchange rate of the coin close to the intended peg. Such a stablecoin is inherently self-referential and has the flavor of a perpetual motion machine.

It is, therefore, difficult not to think of these as 'magic internet money' no project has survived for more than a few months, leaving too many holding the bag. One of the most recent collapses was the stablecoin UST, built on the Terra blockchain. However, this is not the first time a stablecoin has disappeared, with other projects such as Iron, Neutrino, or Basis Cash suffering similar fates. However, no mathematical result proves the impossibility of an algorithmic stablecoin, and in a related paper, we describe conditions and constraints such that such a stablecoin can be considered to be implicitly backed.

The underlying algorithm must handle two distinct scenarios, one of which is relatively straightforward to manage while the other presents a challenging task. If the stablecoin price rises above 1 USD, the protocol or, rather, its users will print and sell more coins, diluting the coin's value and causing the price to decline. This is the easy part of the monetary policy.

The difficult part is when the stablecoin's price drops below 1 USD. In this scenario, coins must be withdrawn from circulation, and the market must be convinced that this process itself is not destroying the overall value of the remaining tokens in circulation. We will discuss the mechanism of a prominent example, the Terra network's UST, in detail below to illustrate the envisioned idea and its pitfalls. An illustrative breakdown of key characteristics distinguishing the three types of stablecoins is provided in Table 1.

Determining the Stability of Stablecoins

The core premise of a stablecoin is that, at all times, one coin consistently equals one unit of the target currency. However, coins are traded in the open market, and prices may fluctuate because of demand and supply imbalances. A robust arbitrage mechanism is crucial for a stablecoin peg to succeed, compelling the market price back toward the intended value.

We make three assumptions to simplify the exposition: First, the stablecoin aims to maintain parity with the U.S. Dollar. Second, the issuer commits to swap collateral for newly generated coins or redeem existing coins at a 1:1 ratio. Third, the issuer of an undercollateralized stablecoin can create new tokens at will. As before, we discuss the cases of collateralized/backed and under-collateralized/unbacked stablecoins and further distinguish between centralized and decentralized issuance.[6]

The fundamental premise of any arbitrage mechanism relies on the ability to instantly purchase an asset for a lower price than one can sell it for, ensuring a *risk-free* profit.

Stablecoin arbitrage is straightforward when the stablecoin's price exceeds 1 USD. The stablecoin is now overpriced. Irrespective of whether the stablecoin is over- or under-collateralized, an arbitrageur would simply exchange dollars for the stablecoin at a 1:1 rate with the issuer and subsequently sell it at a price p>1 USD. The arbitrageur's actions should raise the demand for the fiat currency relative to the stablecoin and depress the stablecoin's price.

The situation becomes more intricate when the stablecoin trades for less than a dollar. The stablecoin is now underpriced. An arbitrageur would buy stablecoins in the open market for less than a dollar and then exchange these at the issuer for dollars.

For a centralized, collateralized stablecoin, this mechanism is seamless when deposits entirely back the stablecoin. Problems may arise when the issuer has invested the initial cash in less liquid assets, whose abrupt conversion impacts the assets market price. Such liquidations potentially cause short-term price dislocation and, in extreme cases, under-collateralization. The sudden liquidation of the stablecoin's collateral can also disrupt traditional markets.

In the case of a centralized, under-collateralized stablecoin, the issuer can use whatever collateral they have to pay for the redemptions. This mechanism, however, only works if the price adjusts

[6] For context: historically, there have been many cases where a country's central bank tries to peg its currency to a foreign one, often to simplify and support trade with that country or the global economy. Usually, the central bank is worried about its currency dropping. To prevent this, peg-supporting central banks would stand ready as a purchaser of last resort of its own currency at the target rate. This defense, however, is only effective as long as the central bank has the necessary reserves. For all practical purposes, a pegged currency, therefore, has the flavour of an under-collateralized stablecoin.

quickly enough so that the demand for collateral conversion diminishes before the issuer exhausts its collateral reserves. If the issuer runs out of collateral, there is no mechanism to support or raise the price other than the market.

Decentralized, over-collateralized stablecoins do not have fiat reserves and must rely on an indirect mechanism to maintain the stablecoin-to-USD peg. The Maker protocol, for example, employs two key strategies: First, arbitrageurs would create or redeem DAI from circulation if the market price deviates from the peg. Consider DAI exceeding the one-dollar mark. Arbitrageurs are motivated to collateralize 1 USD of assets to generate a CDP worth 1 DAI and sell it to the market. This action increases DAI supply, naturally driving down its price. Conversely, if DAI trades below the peg, users are incentivized to retire a CDP to obtain collateral worth 1 USD per DAI, reducing its quantity. This process relies on adequate collateral value to cover outstanding DAI. As outlined above, this posed significant challenges during periods of heightened volatility, prompting various improvements in the mechanism's design.

Second, interest rates are pivotal in counterbalancing medium- to long-term demand fluctuations. The so-called "stability fee" applies to all open CDPs as effective interest on the loan. Maker's savings mechanism allows users to deposit DAI into a smart contract and earn interest at the "savings rate." This deposit yield is funded by the borrower interest payments. Changes in the interest rates are conducted on a weekly basis, incentivizing the minting or redemption of DAI when it is inexpensive or costly.

Blockchain-based stablecoins lack the ability to supply the currency they are pegged against directly. The issue-redemption mechanism based on over-collateralization with cryptoassets (including fiat-collateral backed stablecoins) removes the need for the extra step of exchanging a cryptoasset for the pegged currency.

Unbacked, algorithmic stablecoins operate without explicit collateral, relying instead on a monetary policy involving the minting or burning of a related token that functions as quasi-collateral. The architecture and peg mechanism of these coins are notably complex. To illustrate the concept, we describe the Terra network's stablecoin UST and its collapse in simplified terms below.

The Case of the Stablecoin UST in the Terra Network

The Terra network consisted of two tokens: LUNA, its internal cryptocurrency, and UST, its stablecoin. A pegging smart contract facilitated the exchange between LUNA and UST tokens according to a set of rules aiming to deliver a 1:1 peg of UST to the USD. Notably, the contract conducted the exchange at the prevailing market rate for LUNA tokens in dollars - not UST. Users could generate UST by sending LUNA tokens to the pegging smart contract, where the contract "destroyed" LUNA tokens from circulation and issued newly minted UST. Conversely, users could exchange UST tokens for LUNA tokens at the USD rate, with UST tokens being removed from circulation while new LUNA tokens were created.

To understand the envisioned arbitrage mechanism, suppose p(UST)>USD, and there is no triangular arbitrage between the LUNA token, USD, and UST. Therefore, one has to pay fewer UST than dollars to buy a LUNA token. An arbitrageur could borrow USD, purchase UST, exchange UST for LUNA, sell the acquired LUNA tokens to the contract for UST, and then sell the obtained UST back for USD.

Now suppose p(UST)<USD, and again, assume there is no triangular arbitrage. Now, one has to pay more UST than dollars to buy a LUNA token. An arbitrageur could borrow USD, use it to buy UST, exchange UST with the contract against LUNA, and then sell LUNA for USD. Each operation should increase the demand for the under-valued currency, ideally bringing the price back to the peg. An example of each arbitrage process is provided in Box 1.

Example of Triangular Arbitrage with LUNA, UST, and USD

Suppose UST trades above the reference currency USD with p(UST)=2xUSD, p(LUNA)=p(UST)=2USD. The arbitrageur borrows 2 USD, buys 1 UST, spends 1 UST to buy 1 LUNA, exchanges it with the pegging contract for 2UST, sells the 2UST for 4 USD, repays the loan of 2 USD, and pockets an arbitrage profit of 2 USD.

Now suppose UST trades below USD with p(UST)=0.5x USD, p(LUNA)=p(UST)=0.5USD. The arbitrageur borrows 1 USD, buys 2 UST, spends 2 UST to buy 4 LUNA against the peg contract (because it is priced at the USD), and then exchanges the 4 LUNA tokens in the open market for 2 USD.

However, there is a problem with the second aspect: the process puts downward pressure on the price of the implicit collateral, the LUNA token, for two reasons. First, open market sales create price pressure as they remove liquidity. Second, the exchange of UST to LUNA involves minting new tokens, thus creating a dilution that devalues existing owners' LUNA tokens.

While this mechanism might function as intended during minor deviations and infrequent conversions, it poses challenges at scale. The first component of the mechanism involves a temporary price pressure, akin to what we expect from the liquidation of crypto-backed stablecoin vaults. The second effect, however, permanently lowers the value of holdings of existing LUNA tokens. If these LUNA holders sell their tokens, they further devalue the coin's value, making it even harder to convince the market that redemptions are sufficiently valuable. If these sales sufficiently deplete liquidity, the price of LUNA may experience a further rapid decline, thereby disrupting the arbitrage mechanism and potentially triggering a "death spiral." In principle, arbitrage actions will follow *whenever* UST drops below its peg, creating dilution and depressing the price of the LUNA token relative to the USD. A lower price for the LUNA token, however, means that more LUNA tokens need to be minted, which further depresses the price, and so on.

In principle, minting new LUNA tokens transfers value from existing LUNA holders to those that redeem UST. Therefore, the collective value of the network serves as the collateral. The drop in the price of LUNA itself is not a problem, provided there is sufficient network value to transfer to satisfy UST redemptions. To understand the possible unraveling, it is therefore instructive to consider the case of the LUNA/UST/Terra collapse.

Most of the Terra network's activity revolved around a single application: the Anchor protocol. This DeFi lending platform enticed UST depositors with nearly 20% interest rates. At its zenith, Anchor held roughly 70% of the circulating supply of UST, establishing itself as one of the leading DeFi lending protocols by deposits. However, there was minimal borrowing within the protocol, and it was unclear how the significant deposit returns would be generated. In retrospect, it appears that the primary objective of the Terra blockchain was to mint UST tokens, subsequently deposited into the Anchor protocol, fostering unsustainable returns - a pattern that bore similarities to a Ponzi scheme.

Ultimately, in May 2022, a substantial withdrawal of funds from Anchor caused two issues. First, it instilled doubts regarding Anchor's long-term viability and, given its pivotal role within Terra, cast shadows on the overall value of the Terra network. Second, the funds were moved to the Curve protocol, a commonly used stablecoin exchange that serves as the main reference price. The outflow's size caused a drop in UST's price on Curve, triggering UST redemptions for LUNA. This downward trajectory in LUNA's price, coupled with diminishing trust in the network's viability, catalyzed the initiation of a death spiral affecting the prices of both UST and LUNA tokens.

Terra's collapse shares many features with the collapse of pegged fiat currencies, as observed in the 1997 Asian Crisis or the various Peso crises. For instance, fiat-pegged currencies are also under-collateralized, and the peg may fail if a central bank runs out of reserves. Our takeaway is that a functioning algorithmic stablecoin is likely elusive.

For a more detailed description of the collapse of the Terra network, we refer the reader to Lui et al. (2023) and Briola et al. (2023). d'Avernas et al. (2023) explore the possibility of an algorithmic stablecoin's stability under limited commitment theoretically.

Usage of Stablecoins

Before discussing applications for stablecoins, we need to address some complications in using a stablecoin on a public blockchain like Ethereum. Blockchain operations require validators to execute computations. Transferring stablecoins between addresses necessitates a function call to the stablecoin's smart contract, for which users must pay in the native cryptocurrency. Hence, users must hold a small amount of native cryptocurrency to use stablecoins for payments, a complication that potentially discourages everyday use.

Small complications and frictions can deter the adoption of any payment tool – an early example is the first-ever CBDC that the Bank of Finland issued in the early 1990s, for which minimal fees and inconveniences hindered uptake (Yadav et al., 2023).

However, there is ongoing work by wallet providers to streamline the process. For instance, stablecoin providers themselves may develop sponsored wallets where the software arranges the payment of network fees. Another innovation involves SIM cards for cell phones featuring integrated crypto wallets, addressing know your customer (KYC) concerns and enabling network payments via cell phone bills, solving multiple issues simultaneously.

Stablecoins serve diverse purposes across both traditional finance and blockchain ecosystems, offering users fast and efficient transactions. First, stablecoins can be employed similarly to other payment methods, contingent upon the counterparty's willingness to accept them, considering the aforementioned complications.

Second, stablecoins present a clear alternative for users in nations reliant on the U.S. dollar as a "shadow" currency, providing a convenient and more trusted store of value. In the developing world, people commonly receive remittance payments from relatives and friends employed as workers in other countries. Such remittances are typically sent in stronger Western currencies like the U.S. dollar or Euro. Stablecoins have the potential to substantially reduce fees and delays associated with traditional cross-border transactions. Additionally, recipients of remittances might opt to use foreign stablecoins directly, bypassing the need for local currency conversions.

Third, efficiency gains facilitated by stablecoins extend to traditional institutions when stablecoins are used for international funds transfers. Research by Liao and Caramichael (2022) demonstrates

that end-users may significantly reduce fees, with funds reaching recipients within seconds, revolutionizing the speed and cost efficiency of international transfers.

In the realm of blockchain networks, stablecoins are used in several different ways. Cryptocurrencies like Bitcoin, while excelling in decentralization and security, suffer from volatility due to their fixed supply and speculative nature. Stablecoins, however, are stable by design and allow straightforward commercial transactions in well-understood units of account. Users of the ecosystem who keep their funds in stablecoins have the option to use the continuous trading capabilities of blockchain networks and do not have to rely on centralized platforms such as cryptocurrency exchanges.

Stablecoins enable programmable payments within the blockchain landscape, fostering various functionalities and applications. In the current landscape, stablecoins are a cornerstone of decentralized finance applications. Additionally, stablecoins would remain a necessary ingredient for a world in which traditional assets are tokenized and traded on public blockchains.

Central Bank-Issued Digital Currencies

A central bank-issued digital currency (CBDC) would be a liability of the central bank, and it would add a third kind of M0 money to the existing two, cash and reserves.

There are two types of CBDC: wholesale and retail/general purpose CBDC. The former are available only for a select set of institutions such as commercial, chartered banks, other countries' central banks and international organizations such as the Bank for International Settlements (BIS) and the International Monetary Fund. A retail CBDC would be available for the general population. For the remainder of this primer, we will focus on retail CBDCs.

Exploring the diverse design options for CBDCs exceeds the scope of this primer but might be covered in a future explainer. Briefly, a central bank has four choices for the issuance and transfer organization of CBDCs: i) a centralized system managed internally; ii) outsourcing to commercial banks in parallel with inter-bank payment systems; iii) a hybrid model involving banks, payment service providers, and the central bank together operating the system; or iv) issuing CBDCs as a new token on a public blockchain. Notably, the first three are essentially substitutes, whereas a blockchain-issued CBDC complements any other approach.

Each approach has advantages and disadvantages, and they present separate risks. Again, we only point to some features and raise questions relevant to the design choice rather than providing a comprehensive discussion.

- *Abuse risk:* CBDCs may be used by criminals and terrorists and central banks will have an interest in ensuring that their money cannot be used for illicit activities, in particular, not *at scale*.
- *Resiliency:* as a payments system, a CBDC needs to be available 24/7/365 and cannot be down. Neither can funds be lost by system glitches. As a structurally essential infrastructure, a CBDC system would be a target for state-sponsored or terrorist cyber-attacks.
- *General availability:* as a public good, a state must decide the breadth of its CBDC mandate. The minimal requirement is that the CBDC does not systematically exclude a portion of the population from using it. A maximalist approach is to require that a CBDC is available and usable by every citizen within a country without exception at any time. For digital money, this poses challenges when the usage of the money requires electricity and internet connectivity. Yet offline payments add new abuse risks. Therefore, can and should the CBDC be used offline?

- *The business case:* Why issue the CBDC? What problem does it solve? Is there a sufficient user base? What features are essential for a CBDC from the user's perspective?
- *Privacy:* Who is allowed to view CBDC transmissions? How identifiable are individuals (who have a right to privacy) and businesses (who have a right to secrecy), and under what circumstances? Are there limits to the usage?
- *Onboarding:* How do people obtain CBDCs? Is there a KYC process? Who gets to use CBDCs and who is excluded? Foreign nationals? Minors? Are CBDCs portable across borders and usable outside of their country of origin?

As a general guideline, a centralized system offers speed and efficiency, yet it might cater to only a limited set of use cases. On the other hand, a blockchain-based issuance might offer broader capabilities but could grant the central bank less control over the system.

Considering the attributes of a CBDC, it is almost inevitable that tokenized versions of any closed-system CBDC would eventually circulate on public blockchains. Forward-thinking governments might opt to either authorize private providers or introduce their own tokens rather sooner than later.

As a pure payment tool, CBDCs may displace some of the private, electronic payment volume, which will affect financial institutions' profits as well as monetary policy pass-through. In a recent paper, Niepelt (2023) argues that CBDC would provide liquidity more efficiently than deposits and that the optimal share of CBDC in payments would exceed that of deposits.[7] However, payment markets are complex, and because of externalities, the welfare impact of an increase in competition is not at all obvious.[8]

The BIS and the central banks of France, Singapore, and Switzerland recently ran a pilot study ("Project Mariana") to assess the potential benefit of an international exchange system that would run on a public blockchain. The conversion of currencies was arranged via automated market makers with liquidity as established by the project participants. This proof-of-concept project did not use stablecoins but was based on wCBDCs (i.e., wholesale CBDCs available only to financial institutions) that were issued specifically for this project and that were built on a particular token standard. Central banks and their main partners, large financial institutions, arguably solve a different set of problems: individual people want to transfer funds safely, fast, and at low cost. Financial institutions and central banks have additional constraints and concerns. Indeed, the BIS described the project's architecture as balancing "central banks' domestic need for oversight and autonomy with financial institutions' interest in efficiently holding, transferring, and settling wCBDC across borders."

[7] Niepelt, D (2023), 'DP18444 Money and Banking with Reserves and CBDC', CEPR Discussion Paper No. 18444. CEPR Press, Paris & London. https://cepr.org/publications/dp18444 forthcoming *Journal of Finance*.

[8] See, for instance, Wang (2023) https://luluywang.github.io/PaperRepository/payment_jmp.pdf. The problem is as follows: in our current payments markets, customers choose the payments means and merchants (most commonly) accept whichever payment tool customers bring. Card issuers try to incentivize the use of the payment tool that is most profitable to them, often by offering the customer a benefit option. Card issuers finance these benefits via the fees that they charge merchants, and merchants recover the fee by raising prices. When a new payment tool enters the market, card issuers may react by increasing the benefits of card usage with off-setting higher charges on merchants which, on balance could force the merchant to raise prices further. Depending on the structure of the market, the entry of a competitor may therefore worsen welfare. The key insight is that one needs to carefully analyze platform externalities when implementing competition policy.

The Market for a CBDC and what we can learn from Toronto's A La Cart Program

In a free society, the state cannot force its citizens to use a particular payments tool, and the success of a CBDC as a payments tool will therefore be determined solely by the market. The concern is that instead of focussing on the success of the CBDC in the marketplace, the government bureaucracy focusses on government needs and concerns and creates an overregulated and constrained product that the market rejects.

An illustrative cautionary tale is the City of Toronto's A La Cart food truck program. Back in 2008, much of North America saw a boom in food trucks; the popular movie "Chef" nicely captures that vibe. At the time citizens and businesses pressured Toronto's city council to expand its licences beyond hot dog stands.

The city bureaucracy engaged in an elaborate process of developing regulations, licencing requirements and, most importantly, even designing the only acceptable cart model itself by a committee of the health, fire, licencing and economic development offices. The result was a cart and a set of operational rules that ticked all the boxes from the city's regulators.

The program turned out to be an abject disaster: only half the available licences were taken up; within two years, all vendors had given up, and most were struggling for years to unload their debts. The cart itself and the rules were entirely unusable for the vendors and did not allow them to offer a product that people wanted.

There are many lessons here. First and foremost, regulators, economists, central bankers, and other technocrats are unlikely to understand the yet to be established market for CBDCs, and a product that is designed to hit all the regulators' wishes will therefore likely fail badly.

Very simply put: the key to cash's success as a payments tool is that it is ultimately flexible. It has no restrictions and thus allows the market to determine its best use, and it is maximally easy to use. Much of the discussion around CBDC design features is concerned with AML rules, programmability (which, sadly, is often discussed in the context of restrictions and limited functionality), and limits to ownership and payment amounts. Moreover, just as with food trucks, incumbent payments providers also worry about their bottom line.

Markets teach humility, and technocrats (ourselves included) are best-served by showing utmost humility. *Any* usage and access restriction, and *any* functional complication can cause a "perfectly" designed CBDC to fail in the market of payments. Governments likely have only one shot at introducing a CBDC.

Without success in the marketplace, there is no point in introducing a CBDC. The smartest approach to guarantee success in the marketplace is to introduce a maximally flexible tool and to worry about regulatory restrictions later.

Stablecoins, Tokenization and Financial Stability

As open, borderless value management infrastructures, blockchains have obvious advantages over the current closed and siloed financial system. One opportunity that many traditional financial institutions have been looking at in the recent past is the tokenization of existing assets. A fiat-backed stablecoin is, in fact, a prime example of a tokenized asset.[9]

The availability of tokenized assets on public networks offers significant advantages: it introduces new business and investment tools, enhances collateral management practices, broadens access to potential investors globally, and enables investors worldwide to participate in the most promising ventures.[10]

Widespread tokenization of existing assets and their trading would also require the availability of large quantities of stablecoins, at least if the exchange happens on a decentralized infrastructure. In contrast to traditional markets, where transfers among institutions are often netted out on blockchains transfers require that the funds change hands for each trade.[11],[12]

As of early October 2023, approximately $125 billion in USD-backed stablecoins circulate within the market, supporting roughly $1 trillion in monthly crypto trading volume. Comparatively, the World Federation of Securities Exchanges estimates that the monthly global equity trading volume in Q1 of 2023 was around $10 trillion. Transitioning a relevant portion of this trading volume to public blockchains would require a substantial increase in the available volume of stablecoins.

Of course, stock trading accounts only for a tiny fraction of all finance transactions. Other markets such as bonds, options, or FX are orders of magnitude larger, not to mention regular retail transactions. Presently, deposits at commercial banks in the U.S. hover around $17T.[13] In optimistic scenarios where trillions in volume migrate to blockchains (as highlighted in a Goldman Sachs article), the demand for stablecoins might absorb a substantial portion of these commercial bank deposits. In fact, today, stablecoin issuers already rank as the 16th largest "foreign" purchaser of short-maturity U.S. treasuries.

There are two considerations. First, in the current setup, stablecoins are created by private firms in exchange for other assets. As trading transitions to decentralized platforms and capital to stablecoins, a portion of deposits may shift within the banking system to the custodians of stablecoin issuers. However, if these deposits circulate more rapidly through the banking system due to significant creation and redemption activities by stablecoin issuers, it could introduce new risks in traditional finance. The velocity of these deposits might deter banks from utilizing them for balance sheet lending, potentially negatively impacting the overall credit available in the economy.

---

[9] Malinova and Park (2022) analyze the necessary processes and the challenges involved in the tokenization of stocks and bonds. There are also several articles in the popular press describing how traditional financial institutions such as JP Morgan Goldman Sachs, and Blackrock are exploring and pursuing asset tokenization; see this article in Forbes or this analysis from McKinsey.

[10] As shown by Malinova & Park (2023), moving to automated market making may save investors around 30% of transactions costs. Applied to a tokenized world, to obtain these savings there would have to be a sufficient supply of capital in the form of stablecoins, about 2-5% of aggregate market capitalization.

[11] It is possible to arrange exchanges of assets directly without having to go through case – e.g., investors could exchange a tokenized version of Tesla directly for a tokenized version of Microsoft but looking at the history of finance, its hard to imagine asset trading would not use a numeraire like the USD to denominate all trades.

[12] It is technologically possible to arrange trades more efficiently, and there are protocols that develop tool for netting. For instance, series of back-and-forth transactions can be arrange in so-called roll-ups.

[13] See https://fred.stlouisfed.org/series/DPSACBW027SBOG.

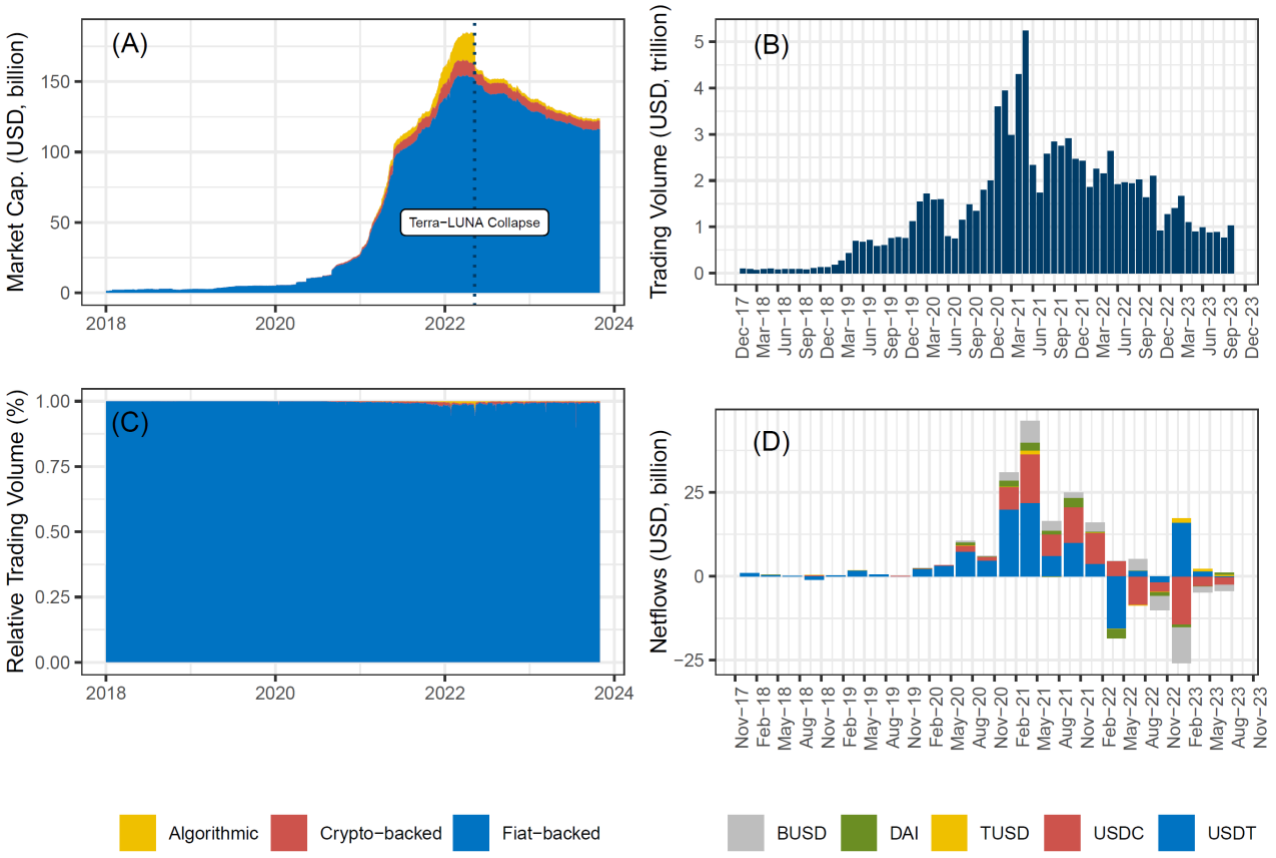

Figure 1: Market Capitalization and Trading Volume of Stablecoins

The figure depicts the daily market capitalization (panel A), monthly trading volume (panel B), and relative trading volumes across the three major peg-mechanism (panel C) of the 50 largest stablecoins by circulating supply. Panel (D) shows the quarterly netflows for the five largest stablecoins. Netflows are defined as the change in the circulating supply of tokens (inflows minus outflows).

Data Source: https://coinmarketcap.com/api/

Second, it is likely that there would be a strong international demand for dollar stablecoins to support a worldwide tokenized asset trading system, which leads to further dollarization.

Holders of stablecoins can typically sell their tokens on the open market or redeem them directly from the issuer for cash. Because stablecoins are linked to the traditional financial world, there is a mild concern that a sudden rush of redemption requests could destabilize traditional markets as issuers liquidate their positions to meet the redemption demand. This scenario could occur if the stablecoin is not fully backed, perhaps because a high-quality asset unexpectedly defaulted. However, so far, there has been no evidence that stablecoins present a stability risk to the banking sector. If anything, the causality goes in the other direction. As previously mentioned, the crisis around Signature Bank and SVB highlighted that large stablecoin-linked deposits might be vulnerable if the depositary institution faces financial distress.

A separate question is the oversight of stablecoin providers. The safest stablecoin provider would be one that has the ability to back its tokens with reserves. Such a setup would eliminate any

inherent counterparty of redemption risks of private stablecoins, making them viable for low-margin trades, such as bonds, where even the tiniest risk affects pricing. However, a stablecoin issuer that issues only reserve-backed tokens would effectively be a narrow bank, a concept that U.S. regulators are uncomfortable with because such entities are ineffective for monetary policy transmission and merely collect interest. An alternative view is that a stablecoin backed by reserves is a de-facto CBDC, albeit a synthetic one.

In practice, stablecoin providers back their tokens using existing assets, including bank deposits. The collapse of SVB showed that this exposes stablecoin providers to the risks of the banking system. When SVB faced uncertainty, Circle Inc., a stablecoin issuer with around $5B at SVB, experienced a 5% drop in the value of its USDC token, roughly matching the size of its deposit. Put differently, SVB's troubles spread to them. If stablecoin providers play a significant role in supporting widespread tokenization, their collapse or even a sudden loss of confidence could trigger severe consequences.

According to their reserve disclosure, Circle has significantly consolidated its backing assets since the SVB episode, relying largely on overnight repos, assets known for their high security and short-term nature, nearly equivalent to cash reserves. However, as stablecoin demand and thus supply grows, this shift mirrors a trend toward stablecoin providers like Circle, resembling a narrow banking model.

However, even though significantly more stablecoins would be required in a world with widespread asset tokenization, these stablecoins can also be created *decentrally* using systems similar to the Maker platform. Namely, a stablecoin like USDC is a de-facto tokenized version of a high-quality liquid asset (HQLA). When the same HQLA exists in tokenized form, the collateralized stablecoin can be created directly on-chain, and there is no need for an intermediary like Circle.

The bottom line is that an expansion of asset tokenization would create an increased demand for stablecoins. The proliferation of stablecoins requires careful thought, not only for supervising issuer risks but also for managing deposits, backing assets, cross-institutional creation/redemption of stablecoins, and their impact on balanced lending. The optimal management is likely an empirical question.

Terrorism, Corruption, Crime, Money-Laundering, and Digital Finance

We center our discussion on the key implications of digital money proliferation for money laundering and illicit transactions.

Any payment instrument can be used to fund illicit activities. The problem that governments likely worry most about is *scale*. Namely, physical payments like cash, gold, or bearer bonds have the advantage that they are largely anonymous, but they are hard to use at scale, and moving physical items of value is risky.

Sending funds electronically through the financial world is obviously more efficient, but governments across the world have enacted laws that make it increasingly difficult for criminals and terrorists to move funds through the international banking system. Financial institutions' own internal monitoring plays a crucial role in curtailing the ability of criminals and terrorists to access and abuse the international banking system.

However, when individuals have direct control over their money either for token-CBDCs or with decentralized, digital peer-to-peer payments, no third party like a bank can do the monitoring as

part of their normal business activities. Enforcing AML rules in such a world requires a different paradigm, bringing state monitoring very close to individuals. Having a clarifying conversation about a transaction or payment behavior with a stern law enforcement officer is a whole different matter than talking to a banker who wants one's business.[14] In addition, in a digital world, the monitoring and investigating of all payment activities by the state would likely have to be done systematically.

A lot can go wrong with the intense monitoring of financial transactions, and it is an open question whether the public will tolerate such behavior by the state. False positives would impose significant, life-changing legal (and emotional) costs on citizens and could cause a far-reaching erosion of social cohesion and trust in the state because an allegation of money laundering in the U.S. would likely be coupled with a charge for wire fraud, both of which constitute serious crimes. In the case of CBDCs, intense state monitoring is particularly risky: false positives could erode trust in the currency and the central bank, with possibly catastrophic consequences for society. In conclusion, the balance between stringent monitoring and preserving public trust remains a critical challenge in the evolution of digital currencies.

Conclusion

This primer has introduced and discussed two innovative forms of digital money. First, stablecoins, distinguished by their peg, issuance, and backing mechanisms, represent privately generated currencies aiming to maintain parity with fiat currencies. Second, central bank digital currencies (CBDCs) expand upon existing money forms like cash and central bank deposits by introducing a digital element accessible to banks or consumers, depending on the specific design.

CBDCs provide high legitimacy and price stability due to their central bank backing. Stablecoins may leverage enhanced usability and benefits provided to users as usage incentives. Usability is key in the adoption of both concepts, perhaps conflicting with regulators seeking stringent KYC/AML processes. Both concepts could significantly impact traditional balance-sheet lending by withdrawing deposited money from banks, affecting the savings-investment cycle.

The future development of stablecoins hinges on the ability of issuers to provide a seamless user experience and robustness to shocks (which may emerge in traditional finance or the blockchain ecosystem) while navigating regulatory scrutiny. Depending on the design, CBDC may revolutionize central banks operations but require careful consideration due to potential tradeoffs in privacy, regulatory oversight, central control, and usability.

[14] Presently, one's financial institution acts as a buffer between a customer and the monitoring authorities and most people likely do not worry about AML/CFT as they are rarely affected. If ever a question about a transaction would come up, most people can clarify matters by talking to their banker. There is an important caveat: customers that are involved in illicit activity are a risk to a bank because banks face billion dollar fines if they don't notice and should have. Customers that get caught by their bank's automated AML system are a risk for the bank, guilty or not. The New York Times recently ran a story that described how businesses and individuals alike get increasingly caught by these systems.

© 2023 Global Risk Institute in Financial Services (GRI). This "A 2024 Primer for Digital Money" is a publication of GRI and is available at www.globalriskinstitute.org. The views, and opinions expressed by the authors, are not necessarily the views of GRI. Permission is hereby granted to reprint the "A 2024 Primer for Digital Money" on the following conditions: the content is not altered or edited in any way and proper attribution of the authors and GRI is displayed in any reproduction. ***All other rights reserved.***

References

Briola, Antonio, David Vidal-Tomás, Yuanrong Wang, Tomaso Aste (2023). Anatomy of a Stablecoin's failure: The Terra-Luna case, *Finance Research Letters,* **51**, https://doi.org/10.1016/j.frl.2022.103358.

Buterin, Vitalik and Illum, Jacob and Nadler, Matthias and Schär, Fabian and Soleimani, Ameen. (2023) Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium https://ssrn.com/abstract=4563364

d'Avernas, Adrien and Maurin, Vincent and Vandeweyer, Quentin, Can Stablecoins Be Stable? (2022). University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2022-131, *Proceedings of the EUROFIDAI-ESSEC Paris December Finance Meeting* 2022, Available at SSRN: https://ssrn.com/abstract=4226027

Goldfeder, S., Kalodner, H., Reisman, D., and Narayanan, A. (2017). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. *arXiv*. https://doi.org/10.48550/arXiv.1708.04748

Liao, G. Y., & Caramichael, J. (2022). Stablecoins: Growth Potential and Impact on Banking. *International Finance Discussion Paper*, (1334). https://doi.org/10.17016/ifdp.2022.1334

Liu, Jiageng and Makarov, Igor and Schoar, Antoinette, Anatomy of a Run: The Terra Luna Crash (2023). MIT Sloan Research Paper No. 6847-23, SSRN: https://ssrn.com/abstract=4416677

Makarov, I., & Schoar, A. (2021). Blockchain Analysis of the Bitcoin Market. *NBER Working Paper Series*, *29396*. https://doi.org/10.3386/w29396

Malinova, K., & Park, A. (2023). Learning from DeFi: Would Automated Market Makers Improve Equity Trading? *SSRN Electronic Journal*.

Malinova, Katya and Park, Andreas, Tokenized Stocks for Trading and Capital Raising (2023). Available at SSRN: https://ssrn.com/abstract=4365241

Niepelt, D. (2022). Money and Banking with Reserves and CBDC. Universitaet Bern, Departement Volkswirtschaft., forthcoming Journal of Finance. https://ideas.repec.org/p/ube/dpvwib/dp2212.html

Park, A., & Stinner, J. (2023). A 2023 Primer for Crypto Credit Markets. *Global Risk Institute Paper Series*, (August). Retrieved from https://globalriskinstitute.org/publication/a-2023-primer-for-crypto-credit-markets/