

Shaping the Future of Digital Currencies

February 2021

Abstract

The digital currencies powering the financial system of the future are likely to come in a variety of different versions. Some will be issued by central banks (what we currently call central bank digital currency, or CBDC), but others may be issued by the private sector and backed by central bank liabilities. As policymakers become more familiar with the pros and cons of issuing a digital currency (essentially the *why*), it's natural that they will begin to turn their attention towards *how* a digital currency could be issued. Although there is still some debate as to whether digital currencies necessarily need to be issued using blockchain-based technology, the following report will, nonetheless, provide a detailed description of how a digital currency, either issued by a central bank or backed by a central bank liability, could be issued on the Celo blockchain.

Recognizing that there is no “one-size-fits-all” solution that will appeal to all central banks, this report will highlight two potential options for issuance: 1) a public/private partnership where a central bank digital currency is issued on a permissioned network, affording the central bank full authority over issuance, governance, and access and 2) an innovative twist on the indirect approach of a privately-issued digital currency backed by a central bank liability, offering substantial benefits related to access, liquidity, efficiency, and transparency. Additionally, the report makes a valuable contribution towards the discussion of interoperability, offering unique insights into the creation of bridges connecting public and private blockchains together.

Acknowledgements

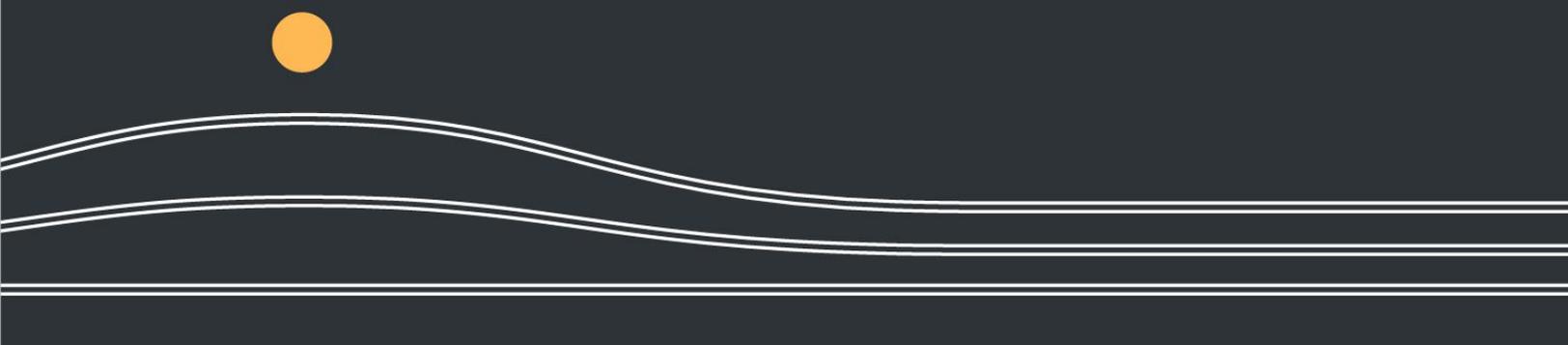
The following report was produced by cLabs, Inc, one of the teams working on the Celo protocol. The author of the report was Ezechiel Copic (ezechiel@clabs.co), with valuable feedback and insights from the following people: Bruno Batavia, Claire Belmont, Anjeza Beja, Cody Born, Niall Coffey, Robin Darbyshire, Sonja Davidovic, Markus Franke, Masaru Itatani, Sep Kamvar, John Kiff, Taylor Lahey, Jake Leraul, Carmen Li, Brynly Llyr, Klaus Loeber, Marek Olszewski, Marcelo Prates, Jai Ramaswamy, Rene Reinsberg, Anca Bogdana Rusu, Daniel Sanches, Kenneth Sullivan, and Natalya Thakur.

Any questions and comments about the report can be directed to: policy@clabs.co

Table of Contents

Exploring Innovative Digital Currency Frameworks	4
Creating money in the current system	5
Implementing a new system of digital currencies	7
Laying the groundwork for what’s possible on Celo	10
Building a Permissioned Public/Private CBDC Network	11
Configuring a private network environment	12
Establishing the CBDC Celo environment	13
Defining governance on the platform	14
Understanding interoperability and the importance of bridges	15
Distributing CBDC to retail end users	17
Highlighting the advantages of issuing a centralized, permissioned CBDC on Celo	18
Introducing an Innovative Twist on the Indirect Approach to Private DC-CB	20
Questioning the status of central bank reserves	21
Considering additional issues raised by the IMF model	21
Proposing an alternative “on-chain” option backing Private DC-CB	22
Addressing the issue of central bank liabilities	24
Highlighting the advantages of a Private DC-CB	25
Appendix	27
Interoperability	27
Privacy	29
Transaction Fees	30
Monetary Policy Implications	31

Exploring Innovative Digital Currency Frameworks



Not long ago, the idea of a “central bank digital currency” (or CBDC)¹ was a rather obscure notion that garnered little attention. As cryptocurrencies, such as Bitcoin, began to rise in prominence, some pioneering central bankers began to wonder what the world would look like if traditional banknotes were to become digitized as well. Initially, the research on CBDC was largely academic, and mostly focused on the potential implications that such digital assets could have on monetary policy and financial stability.

Then came the announcement of Facebook’s Libra project (now Diem) in June 2019. This event caused a seismic shift within the central bank community regarding CBDC. What was once an interesting “thought experiment” about the future of money, became an existential debate on the validity of the traditional payments system, as central bankers contemplated the challenge of competing against giant technology companies, with billions of dedicated users.

Despite concerns about Libra, central banks understand that to build a secure and innovative financial system for the future there needs to be a constructive partnership between the public and private sectors. Indeed, the digital currencies powering the financial system of the future are likely to come in a variety of different versions. Some will, of course, be issued by central banks (what we currently call CBDC), but others may be issued by the private sector and backed by central bank liabilities. In fact, these two examples mirror the current system of central bank money (banknotes) and commercial bank money (deposits).

¹ Although concerns related to the “currency” status of CBDC have been raised by the IMF and others, the “CBDC” term will be used in this report, given its ubiquitous nature. Nonetheless, the author would like to thank Niall Coffey of Avoca Global Advisors (and formerly the Federal Reserve Bank of New York) for his suggestion to revise the term to central bank digital money (or CBDM).

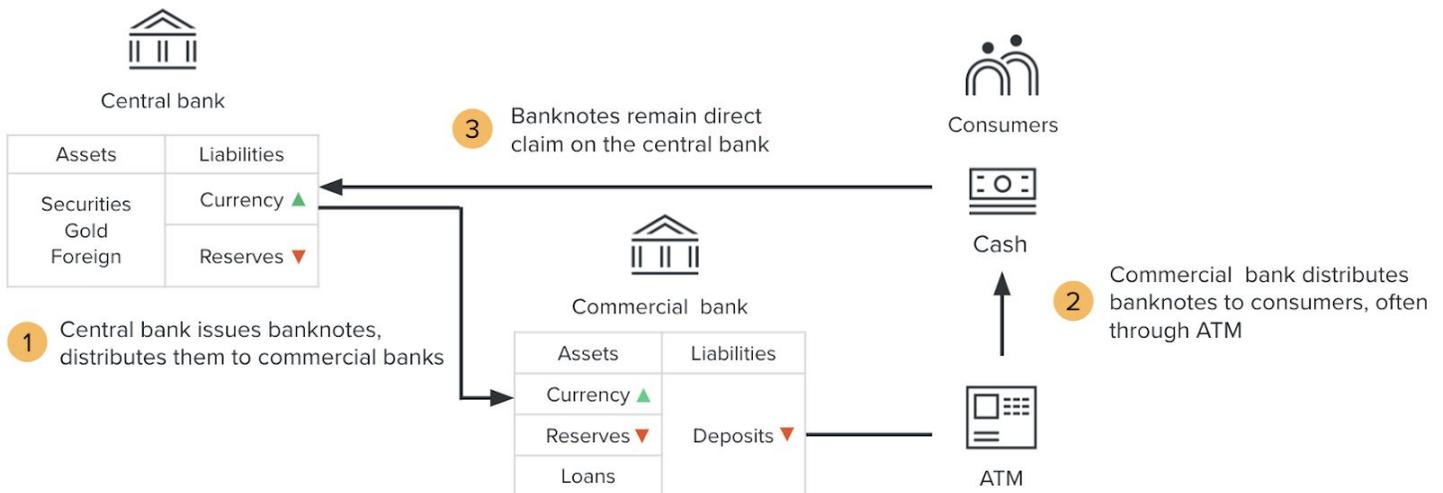
As policymakers become more familiar with the pros and cons of issuing a digital currency (essentially the *why*), it's natural that they will begin to turn their attention towards *how* a digital currency could be issued. However, before diving into the possible ways in which digital currencies could be implemented, it's important to understand how money is currently created.

Creating money in the current system

Understanding how money is currently created is vitally important when it comes to thinking about potential frameworks for creating money in the future. Although there are certainly many great resources available for learning about the creation of money, the work by Auer and Böhme² is particularly useful when thinking about this concept with respect to the potential creation of digital currencies.

When thinking about the creation of money, it's helpful to assess the impact such issuance has on the balance sheets of the key stakeholders in the financial system. For example, Chart 1 highlights the impact that issuing physical banknotes has on the system.³ To start, a central bank is responsible for issuing the physical banknotes that people use on a daily basis (this can also be referred to as “cash” or “currency in circulation”). Once issued, these banknotes remain a liability of the central bank.

Chart 1: Balance Sheet Assessment of Public Banknotes



Note (▼) Central bank debits commercial bank's reserve account with the central bank to pay for banknotes, thus overall reserves decline. Additionally, commercial bank debits consumer's deposit account to pay for banknotes obtained through ATM. Decline in reserves is offset by (▲) increase of currency in circulation. Furthermore, commercial bank holdings of currency as an asset increases, insofar as they do not distribute all of the currency received from the central bank onto their customers.

² Auer, R and R Böhme (2020), “CBDC architectures, the financial system, and the central bank of the future”, VoxEU.

³ Note: Charts 1-5, are based on the work of Auer and Böhme, and have been modified to include additional details.

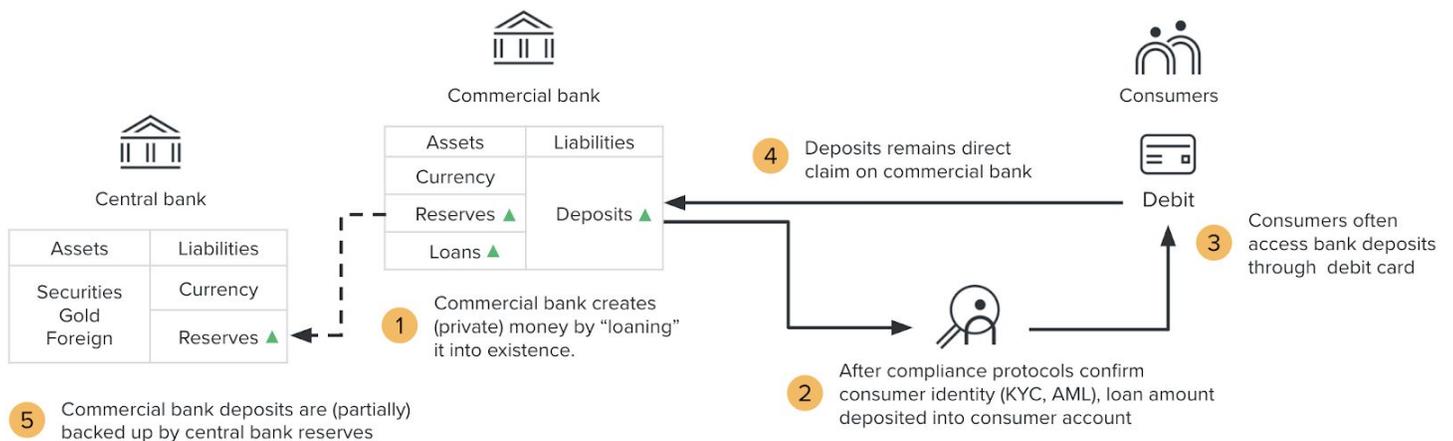
Although the central bank issues banknotes, it typically does not distribute these notes to the end consumers. In a “two-tiered” financial system, the central bank issues banknotes and distributes them to commercial banks. The commercial bank effectively “buys” the banknotes, which appear as an asset on its balance sheet, and the central bank debits the commercial bank’s reserve account at the central bank equal to the amount of banknotes distributed.

A commercial bank then makes these banknotes available to its customers, often through ATM machines. When a customer withdraws the banknotes from the ATM, the commercial bank debits that customer’s account at the bank by the amount of banknotes that were disbursed. Importantly, even though the banknotes may have been obtained by consumers from their respective commercial bank, the banknote itself still remains a liability of the central bank.

Central banks, however, are not the only ones that create money in today’s financial system. As Chart 2 illustrates, commercial banks also create money by loaning it into existence. Specifically, when a commercial bank agrees to loan a consumer money they credit the consumer’s deposit account with the loan amount. These deposits, which consumers often access through the use of a debit card, remain a liability on the commercial bank’s balance sheet, while the loans extended to consumers serve as an asset for the bank.

In order to support the financial stability of the system, commercial banks are usually required to back up these deposit liabilities with reserves held at the central bank. These reserves, typically representing a small percentage of outstanding deposits, are used in case the commercial bank goes bankrupt.⁴

Chart 2: Balance Sheet Assessment of Private Money



Note (▲) The issuance of loans by the commercial bank increases loan assets for the bank, and also increases deposit liabilities, as the funds being loaned are deposited into the consumer’s account with the commercial bank. Additionally, commercial banks typically have to hold a certain percentage of their deposits as reserves with the central bank, so an increase in deposits will also require an increase in reserves held at the central bank.

⁴ This is where “fractional banking” originates, as the money created by commercial banks is backed up by a fraction of reserves held at the central bank. This is distinct from the idea of a “narrow bank”, where all deposits are backed up one-for-one by central bank reserves.

Implementing a new system of digital currencies

The current creation of money provides an important perspective with regards to the liability of money. Banknotes are issued by the central bank, and thus remain a liability of that institution. Meanwhile, commercial bank deposits are essentially private money partially backed up by central bank reserves. These distinctions are also represented in the current research focused on digital currencies.

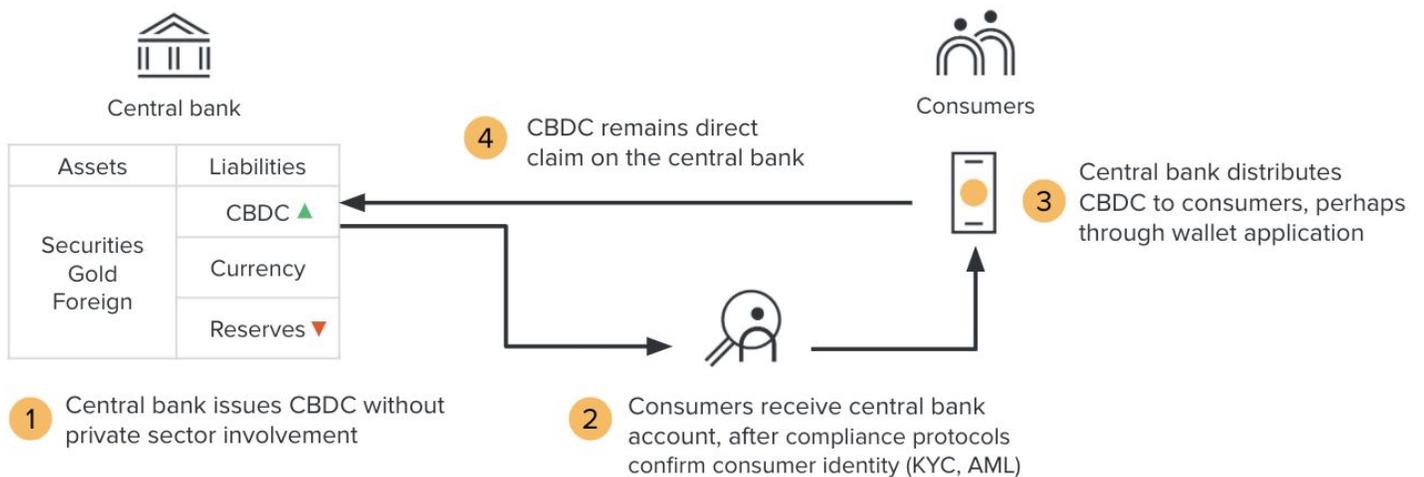
The most prominent is the idea of a central bank digital currency (CBDC). But the very definition of a CBDC requires that it be issued by a central bank to ensure that it remains a direct central bank liability. Of course, like private money today, there can also be privately-issued digital currencies that are backed-up by central bank liabilities. The following examples represent the most prominent options currently being discussed within the central banking community:⁵

Public CBDC

The first option, and most straightforward one, would be for the central bank to issue a CBDC without any private sector involvement (as depicted in Chart 3). This is referred to as “Direct CBDC” by Raphael Auer (BIS), and essentially means the central bank would be directly responsible for all aspects of the CBDC, including: issuance, distribution, technology, customer service, and compliance. This option is referred to as “Public CBDC” throughout this document to highlight that all aspects of the CBDC are the responsibility of the public sector (e.g. central bank).

Described as the “most radical departure from the existing system,” Auer and Böhme note such an architecture is unlikely to come to fruition as it “marginalises private sector involvement” and disintermediates the commercial banking sector.

Chart 3: Balance Sheet Assessment of Public CBDC



Note (▼) Central bank debits consumer’s reserve account with the central bank to pay for CBDC, thus overall reserves decline. Decline in reserves is offset by (▲) increase of CBDC in circulation.

⁵ Research by the BIS and IMF, as well as specific central banks, such as Banco Central do Brasil and the Bank of England, helped lay the foundation for ways digital currencies can be implemented. Please see John Kiff’s [website](#) for a comprehensive list of Retail CBDC

Public/Private CBDC

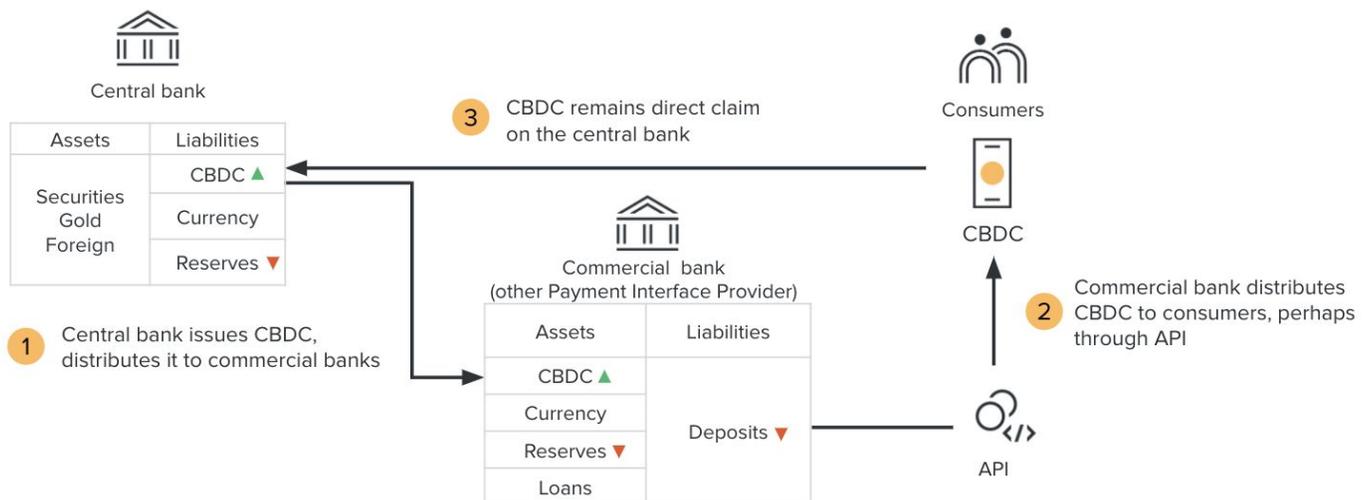
The second option would still result in a central bank-issued CBDC, but would also require private sector involvement to help with various aspects including: distribution, customer service, and technology development. Given the public and private sector involvement, this option is termed “Public/Private CBDC” in this document to highlight the public issuance and private distribution of the CBDC.

There are different levels of public/private sector involvement being proposed. For example, the Bank of England (BOE) proposed a “platform model,” whereby the central bank issues the CBDC and maintains control of the core ledger, while private sector institutions, referred to as “Payment Interface Providers” by the BOE, are responsible for on-boarding customers and providing overlay services.⁶

Under this option, also supported by Marcelo Prates⁷ of Banco Central do Brasil, consumers could have (pseudonymous) accounts directly with the central bank that would be facilitated by the Payment Interface Providers, which would be responsible for maintaining the full account profile of consumers on their respective networks. The BIS proposed a similar option, referred to as a “hybrid model”, which also has private sector involvement, but does not specifically advocate for consumers to have direct access to the central bank core ledger.

Nonetheless, the defining feature of these variations is the public/private sector collaboration. Similar to how physical banknotes are currently issued (see Chart 1 above), a public/private CBDC (as illustrated in Chart 4) would be issued by the central bank and made available to consumers through a wallet application or Application Programming Interface (API) developed by private sector firms. Importantly, CBDC in this option would remain a direct liability of the Central Bank.

Chart 4: Balance Sheet Assessment of Public/Private CBDC



Note (▼) Central bank debits commercial bank's reserve account with the central bank to pay for CBDC, thus overall reserves decline. Additionally, commercial bank debits consumer's deposit account to pay for CBDC obtained through API. Decline in reserves is offset by (▲) increase of CBDC.

⁶ Bank of England. “Central Bank Digital Currency: Opportunities, Challenges, and Design.” March 2020.

⁷ Prates, Marcelo. “The Big Choices when Designing Central Bank Digital Currencies.” *Coindesk*. October 2020.

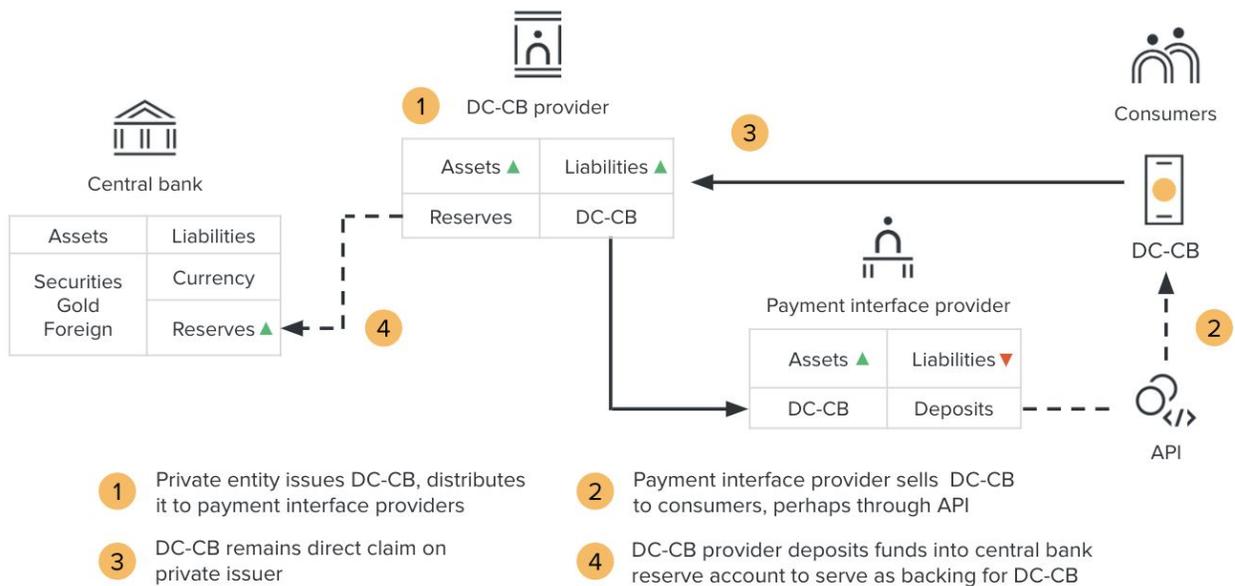
Private DC-CB

The final option involves the issuance of a digital currency by a private sector firm that is backed up, on a one-for-one basis, with a central bank liability. Since this option is not directly issued by a central bank, it is not typically viewed as being a central bank digital currency (CBDC). Instead, this option is referred to as “Private DC-CB” in this document to highlight that it’s a privately issued digital currency (DC) backed by a central bank liability (CB).⁸ It should be noted that Private DC-CB is conceptually similar to “electronic money” (or e-money) in that both act as privately-issued electronic stores of monetary value. Whereas e-money may or may not be directly (and/or fully) backed by central bank assets, Private DC-CB (as conceived here) is explicitly backed, one-for-one, by a central bank liability.

The idea of a Private DC-CB (as illustrated in Chart 5 below) is essentially the same as the private money option that currently exists (see Chart 2 above). Indeed, private money today is digitized in the sense that a consumer’s commercial bank deposits are available electronically, and through the use of applications like PayPal, funds can be transferred from one account to another.

The difference, however, is that since all transactions are governed by the blockchain protocol, holders of Private DC-CB can send this digital currency to anyone, regardless of whether or not they possess a commercial bank account. Indeed, like publicly-issued banknotes today, Private DC-CB is a peer-to-peer transaction that doesn’t necessarily require the authorization of a third party (such as the issuing institution or the distributing payment interface provider).

Chart 5: Balance Sheet Assessment of Private DC-CB



Note (▼) Payment interface provider debits consumer’s deposit account to pay for DC-CB, thus overall deposits decline. Meanwhile, (▲) DC-CB provider deposits funds received from the sale of DC-CB into central bank reserve account, thus overall reserves increase.

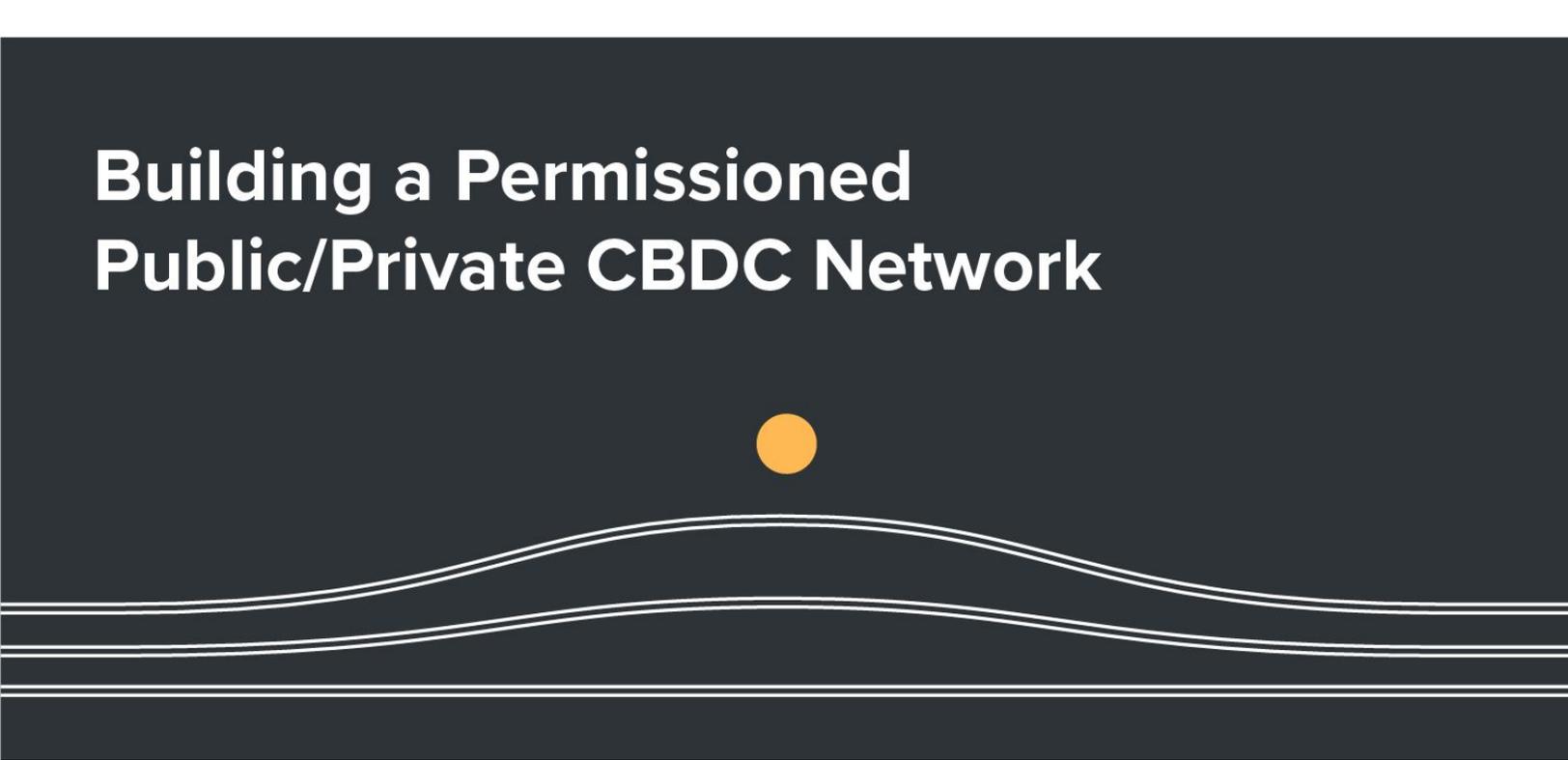
⁸ This option has also been referred to by the IMF as a “Synthetic CBDC”. However, many central banks would not consider this model to be a true “CBDC” since it is not issued directly by a central bank. As such, this version will be referred to as “Private DC-CB” in this document. Of note, the BIS refers to this framework as an “indirect architecture”.

Laying the groundwork for what's possible on Celo

Although there is still some debate as to whether digital currencies necessarily need to be issued using blockchain-based technology, the following report will, nonetheless, provide a detailed description of how a digital currency, either issued by a central bank or backed by central bank liabilities, could be issued on the Celo blockchain. Recognizing that there is no “one-size-fits-all” solution that will appeal to all central banks, this report, produced by cLabs (one of the companies working on Celo), will highlight two potential options for issuance that are currently being discussed within the broader central banking community.

The first section below provides details of how a Public/Private CBDC could be issued on a permissioned network, where the central bank retains full authority over issuance, governance, and access. The second section offers an innovative twist on the indirect approach of Private DC-CB, highlighting how a digital currency could be issued on a permissionless basis, and backed by a central bank liability. An appendix is also included to share details on issues common to both ends of the spectrum, including interoperability, privacy, and transaction fees.

Building a Permissioned Public/Private CBDC Network



Central banks are conservative and cautious, by nature. As the guardians of a country's financial system, they understandably want to make sure that any environment used for CBDC issuance is secure and resilient. Additionally, they will strive to deploy CBDC that is interoperable with traditional payment networks, thus causing as little disruption for consumers as possible.

For these reasons, and others, most central banks are likely to prefer a CBDC approach that affords them exclusive authority over key rules and functions of the CBDC network, such as issuance, governance, and overall network access. Many will also seek to maintain the current two-tiered financial system, in which commercial institutions are used to distribute money to the broader population.

As such, a recent report by the Bank of England, in which they incorporate these requirements into a “platform model” or “layered architecture” approach, has gained prominence within the central bank community.⁹ Under this approach, a core set of rules and functionalities are effectively governed by the central bank within a permissioned network, and “Payment Interface Providers” are granted access to this private network. These payment interface providers would be “private sector firms that would manage all the interaction with users of CBDC and provide overlay services that extend the functionality of CBDC”. Such activities include: distribution, customer onboarding, and regulatory compliance.

To help central bank policymakers better understand how this “platform model” approach can be achieved, this section highlights how the Celo protocol can be configured in such a way as to afford central banks the security and privacy of a

⁹ Bank of England. “Central Bank Digital Currency: Opportunities, Challenges, and Design.” March 2020.

traditional network, while also leveraging Celo’s public blockchain technology to enhance the user experience and provide access to decentralized financial (DeFi) applications. Within the context of establishing a permissioned network to create Public/Private CBDC, the following important topics will be discussed in this section: configuration, deployment, governance, interoperability, and distribution.

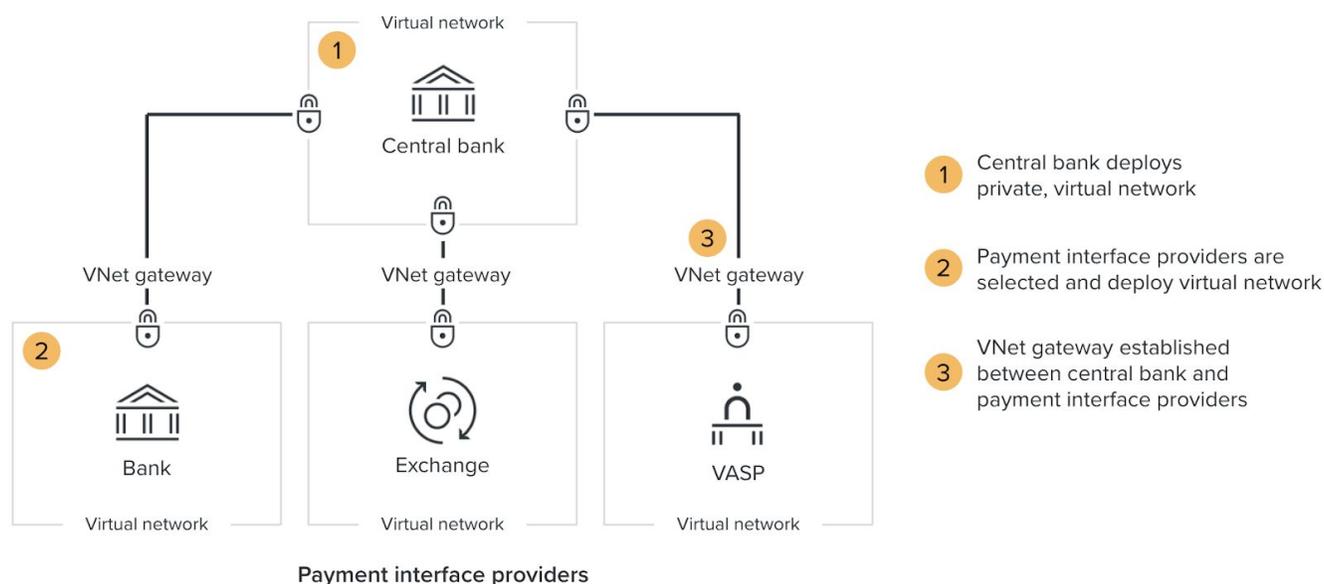
Configuring a private network environment

The process starts with the deployment of a secure and private virtual network (or environment). The network could be developed internally by the central bank or by a third-party system integrator (SI) or independent software vendor (ISV)¹⁰ on behalf of the central bank. Importantly, the central bank is free to choose how they would like to deploy this secure network, with additional technical support and documentation available from numerous parties working on the platform.¹¹

To ensure the central bank retains optionality, all Celo technology is open source, under common licenses. This prevents vendor lock-in, and provides a low barrier for adoption from a legal and business perspective. After deploying its virtual network, the central bank decides which private firms will serve as payment interface providers and be granted access to the network (see Chart 6).

Presumably, central banks will choose regulated entities within their jurisdiction -- such as banks, exchanges, and virtual asset service providers (VASPs) -- to fill this role. Once selected, these payment interface providers deploy their own virtual networks and connect to the central bank via VNet Gateways¹², ensuring secure communication across virtual networks.

Chart 6: Virtual Network Deployment



¹⁰ Examples of available virtual network providers include Microsoft’s Azure and Amazon AWS.

¹¹ Alternatively, cLabs can work directly with the central bank to deploy the secure network, if preferable.

¹² VNet Gateways allow each member of the network to connect their virtual private networks (VPN) together to have both the defense in depth that a VPN provides with the inter-organization communication that is required for a reliable blockchain network.

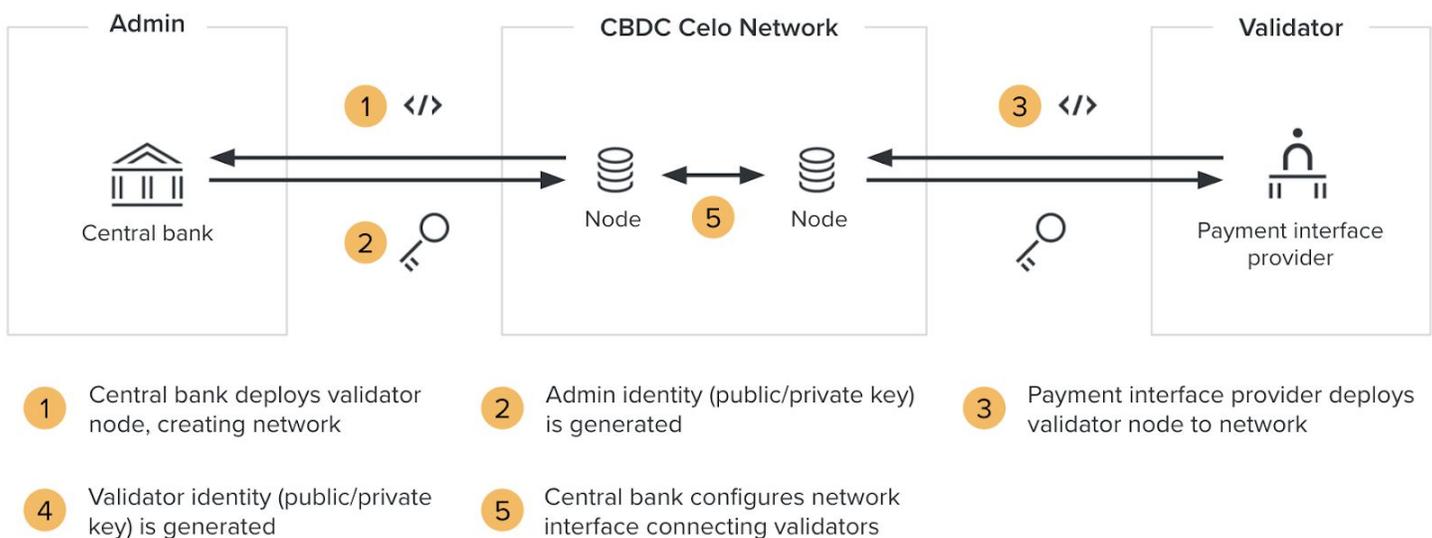
Establishing the CBDC Celo environment

Once the central bank deploys its secure, virtual network and provides gateway connections to its selected payment interface providers, the next step involves establishing the CBDC Celo environment. When CBDC is first deployed on Celo it defines two specific roles: admin and validator.

The central bank will typically serve as the admin, allowing it to establish the rules surrounding governance, access, issuance, and distribution, for example. Notably, admins have the ability to add/remove validators, as well as other admins.¹³ The payment interface providers selected by the central bank will likely serve as validators, meaning they will participate in consensus and help validate all transactions on the blockchain. Once a quorum of validators reach agreement on a transaction, that decision is final. The simplicity of this approach makes it easy to initially stand up and configure a network. The upgradable governance of CBDC on Celo also makes it easy to customize and update these rules over time.

The creation of the CBDC Celo Network begins when the central bank deploys a validator node¹⁴, after which an admin identity (public/private key) is generated (see Chart 7 below). The private key associated with this activity is generated in a cloud Hardware Security Module (HSM), which keeps the key secure and provides a traditional access control model. This HSM-based private key can be used for validation, governance processes, and submitting transactions to the blockchain, among other activities.

Chart 7: Creating a CBDC Celo Network



¹³ Although the central bank will retain total authority over the Public/Private CBDC network, they may wish to delegate some admin responsibilities (such as supervision) to other regulatory agencies.

¹⁴ Generally speaking, a “node” is simply computer software used by validators to connect to a specific blockchain in order to validate the transactions and/or produce blocks. A node will typically run a dedicated virtual machine and may have an identity represented by a private key that is used to sign transactions.

Once the central bank completes the deployment, the payment interface providers are able to deploy validator nodes of their own to the network, which will generate unique validator identity keys. After all validator nodes have been deployed, the central bank configures the CBDC Celo Network interface to allow inbound connections from all validator nodes, thus creating a validator set.

Defining governance on the platform

After the CBDC Celo Network is deployed and the validator set established, the central bank is ready to “issue” the CBDC and define the rules by which the digital currency will be governed. Governance on the Celo platform is defined via smart contracts, which provide unambiguous, auditable rules that can be upgraded over time by the network admin (e.g. the central bank).

The default CBDC smart contract¹⁵ affords the central bank the ability to “mint” (create) CBDC. Once issued, the CBDC is sent to the central bank’s address (e.g. account) that was generated when the CBDC Celo Network was deployed. As the network admin, the central bank can also “burn” (destroy) any CBDC it holds.

The CBDC smart contract also affords network participants (including payment interface providers and end users) the ability to transfer digital currency to other participants. Importantly, due to the programmable nature of the smart contract, the CBDC can be programmed in such a way that limits the amount available for transfer based on the user’s profile. For example, payment interface providers may be allowed to transfer large amounts of CBDC amongst themselves, because they would be regulated entities, and thus pose limited concern for anti-money laundering (AML) or combating the financing of terrorism (CFT) compliance. Conversely, a central bank may wish to place more restrictions (e.g. daily/monthly transaction limit amounts) on end users as they may be more lightly supervised.

Indeed, the central bank can customize its CBDC smart contract in myriad ways, related not only to transaction limits, but also with respect to whether its CBDC carries an interest rate or the creation of CBDC-related derivative products, to name just a few options. It should be noted that defining the business logic of CBDC related to the governance of monetary issuance and stability issues typically occurs in what is referred to as the “application layer” (see Chart 8 on the following page).¹⁶

Additionally, there exists a “consensus layer” where the central bank determines which entities can produce and validate blocks on the network. As noted earlier, the payment interface providers selected by the central bank -- and governed by

¹⁵ The use of “contract” in this instance refers to computer code written to define the rules by which the digital currency is governed (including issuance and distribution). An interpretation of the legal merits of such a “contract”, is beyond the scope of this paper. A recent IMF report (“[Legal Aspects of CBDC: Central Bank and Monetary Law Considerations](#)”) has begun to consider such merits.

¹⁶ The use of “application” in this instance should not be confused with applications (or “apps”) that are software programs used on smartphones or mobile devices.

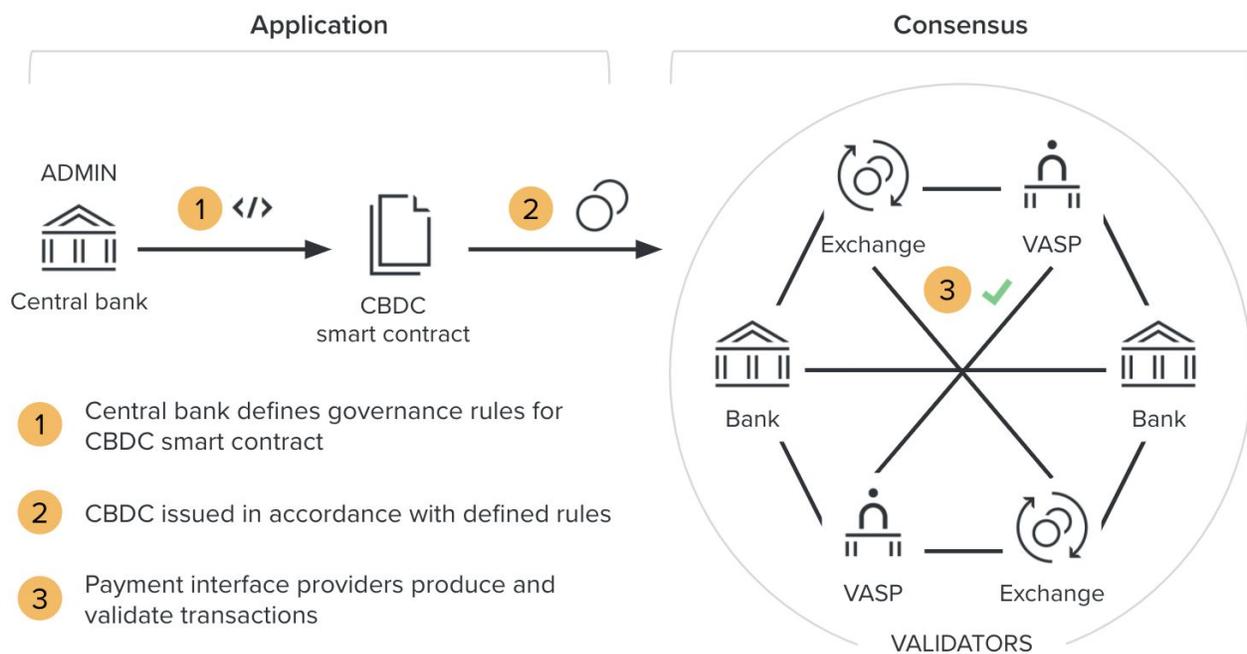
an admin list -- serve as network validators, confirming the validity of transactions on the network and helping to maintain consensus.¹⁷

Understanding interoperability and the importance of bridges

Before moving on to describe how CBDC could be distributed on the Celo Network,¹⁸ it's important to pause and discuss the importance of interoperability¹⁸ and the role it plays with respect to distribution. In a recent report by the Official Monetary and Financial Institutions Forum (OMFIF)¹⁹, 60% of central bank respondents expressed concern that interoperability would encumber progress on CBDC issuance. Importantly, 43% admitted they are currently only focused on strictly domestic CBDC use cases. But the issue of interoperability affects not only domestic use cases, but also cross-border payments that would potentially require interoperability with other CBDC systems.

Perhaps the most helpful way of thinking about interoperability is through the concept of creating bridges. Broadly speaking, with respect to digital currency platforms, a bridge provides a mechanism to move assets from one consensus network to another. When a user is bridging from one network to another there are essentially two options: a trusted option, wherein a user is required to trust a third-party regarding the validity of a transaction, and a trustless option, wherein such trust is not necessary as the validity of a blockchain transaction is verified by inspecting the underlying code source.

Chart 8: Network Layers



¹⁷ Celo uses Istanbul Byzantine Fault Tolerance consensus. This consensus algorithm provides instant finality, which decreases transaction latency and simplifies the transaction submission process.

¹⁸ The focus of “interoperability” in this report is related to the connection of various different network systems (both public and private). Please see the Appendix for more details on interoperability.

¹⁹ OMFIF and IBM. “Retail CBDCs: The Next Payments Frontier.” 2019.

To better understand the difference between these two options, let's use our current example where a central bank decides to issue CBDC on its own private network. In the trusted version (similar to the Bank of England design mentioned earlier), the central bank issuing CBDC allows private sector payment interface providers access to its core ledger through an API (application programming interface) -- thus effectively creating a "trusted" bridge between the parties. The central bank grants access to regulated entities, trusting them to act responsibly, while the payment interface providers are trusting that the CBDC received from the central bank is valid and the blockchain on which the CBDC is issued is up-to-date.

Similarly, when payment interface providers distribute the CBDC to their customers (e.g. consumers and merchants), another trusted bridge is needed -- likely in the form of an API-based wallet application granting customers access to the payment interface provider's network. Again, these consumers and merchants are trusting that the CBDC received from their payment interface provider is valid and the blockchain on which the CBDC is issued is up-to-date. Additionally, any third-party service providers wishing to build applications on the network (such as a saving or lending application) will need to be regulated in much the same way that payment interface providers and end users are, to ensure some level of trust.

As this example shows, there is a significant amount of trust that needs to be built for this type of system to function properly. Additionally, this approach has the potential to introduce additional legal friction and security risks. In fact, one of the biggest issues faced by permissioned networks is this idea of scaling trust -- growing the number of members beyond a certain limit becomes increasingly difficult. And this issue is only exasperated when considering the potential need for cross-border payment interoperability. A network may be able to grow steadily within a given country, where regulation and legal standards are shared, but the same network may be unable to incorporate participants from other countries, where different operating models and legal standards are used.

Instead of relying on trust, Celo solves the interoperability problem through the use of trustless bridges. Thanks to some key innovations on Celo -- including the use of epoch-based synching, BLS signature aggregation, and zero-knowledge SNARK proofs²⁰ -- the state of a Celo blockchain, whether it's permissioned and private or permissionless and public, can be verified immediately, without the need to trust a third party.

This "Celo Bridge" provides trustless reach from the central bank all the way to end customers on mobile devices. For example, this technology can be used domestically to bridge the central bank's private network to that of a public network, where end users can access the CBDC without needing to trust centralized APIs operated by payment interface providers. Additionally, the Celo Bridge can be used to support cross-border payments, by bridging permissioned

²⁰ Please see the "Interoperability" section of the Appendix for more detailed information on Celo's innovative technology used to create trustless bridges.

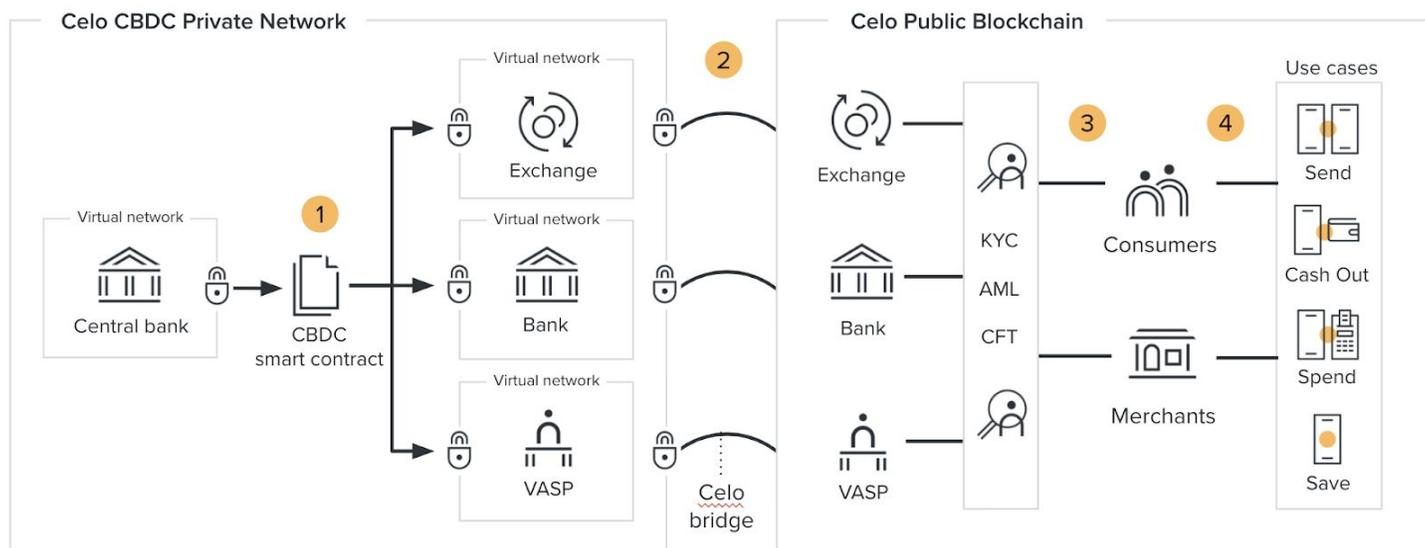
CBDC networks from two or more countries together. Indeed, the Celo Bridge model provides a scalable solution to reaching millions of users without relying upon trusted intermediaries to verify the validity of transactions.

Distributing CBDC to retail end users

Returning to the subject of distributing CBDC to retail end users (such as consumers and merchants), it's likely that the central bank will prefer to use a two-tier distribution model. This model is similar to the current financial system whereby a central bank distributes banknotes to commercial banks, who then distribute this money to their customers.²¹

After the Celo CBDC Network has been deployed, the central bank is free to transfer CBDC to any one of its payment interface providers, using the CBDC contract (see Chart 9). Assuming the payment interface provider has a reserve account at the central bank, any CBDC sent to it will be offset by an equal amount of fiat currency debited from the provider's reserve account at the central bank.

Chart 9: Distribution Model



- 1 Central bank transfers CBDC to payment interface provider using CBDC smart contract
- 2 Payment interface provider uses Celo bridge to transfer CBDC to Celo Public Blockchain
- 3 Payment interface provider sends CBDC to end user after KYC protocol compliance
- 4 End users have myriad use case options for CBDC, including spending, saving, and cashing out

²¹ If a central bank prefers to distribute CBDC directly (similar to the “Public CBDC” model highlighted earlier), the CBDC Celo Network can certainly accommodate such an arrangement. However, for the sake of the current example, we will assume that a central bank wants to maintain the current two-tier distribution model and pursue a “Public/Private CBDC”.

Upon receipt, a payment interface provider can then use the Celo Bridge (as discussed above) to transfer the CBDC from the private central bank network to an account on Celo's public blockchain. Once the CBDC is available on the public blockchain, the payment interface provider can make it available to any of its customers (in exchange for fiat currency), upon completion of all necessary "know your customer" (KYC) compliance protocols.

With the CBDC available on the Celo public blockchain, end users will be afforded myriad ways in which to utilize the CBDC on the network, including the ability to send it to others, use it to pay for goods and services at authorized merchants, and even take advantage of decentralized financial applications (e.g. DeFi apps) that allow them to save or borrow CBDC. Additionally, both merchants and consumers have the ability to transfer this CBDC back to their payment interface provider at any time, in exchange for fiat currency.

It should be noted the CBDC smart contract on the public blockchain can be governed by different rules than the CBDC available on the private network. As noted earlier, accounts on the Celo public blockchain can have much lower daily transaction limits compared to those available on the permissioned network, thus providing additional assurances that compliance protocols are being met.

Highlighting advantages of issuing a permissioned CBDC on Celo

For those central banks looking to issue a CBDC in a permissioned fashion, the Celo protocol offers the unique advantage of affording a central bank the security and privacy of a traditional network, while also leveraging Celo's public blockchain technology to enhance the user experience and provide access to decentralized financial (DeFi) applications. Additionally, the consensus algorithm used by the protocol provides near instant transaction finality, decreasing latency and simplifying the transaction submission process.

The open-sourced nature of the Celo blockchain also prevents vendor lock-in, provides a low barrier for adoption from a legal and business perspective, and allows the central bank authority over the governance, access, issuance, and distribution of the CBDC. Importantly, governance on the Celo platform is defined via smart contracts, which provide unambiguous, auditable rules that can be customized and upgraded over time by the central bank.

The programmable nature of CBDC on Celo affords central banks the ability to vary transaction limits based on user profiles. For example, accounts on the Celo Public Blockchain can have lower daily transaction limits compared to those available on the permissioned network, thus providing additional assurances that AML/CFT compliance protocols are being met. Additional options, such as demurrage fees and cash back rewards can also be programmed into the CBDC,

affording central banks a new channel for the transmission of monetary policy, whereby the velocity of CBDC can be tracked and influenced.²²

Finally, the issue of interoperability is addressed on the Celo platform through the use of trustless bridges. Using innovative technology, the state of a Celo blockchain, whether it's permissioned and private or permissionless and public, can be verified immediately, without the need to trust a third party. These "Celo Bridges" provide trustless reach from the central bank all the way to end customers on mobile devices.

Domestically, bridges can be built from the central bank's private network to those of public networks, affording end users the ability to utilize CBDC in useful DeFi applications that allow them to spend, save, or borrow CBDC, for example. Internationally, the Celo Bridge can also be used to support cross-border payments, by bridging permissioned CBDC networks from two or more countries together. Indeed, the Celo Bridge model provides a scalable solution to reaching millions of users without relying upon trusted intermediaries.

²² For more detailed information on the monetary policy implications of issuing CBDC on Celo, please check out the ["Influencing the Velocity of Central Bank Digital Currencies"](#) whitepaper by the cLabs team.

Introducing an Innovative Twist on the Indirect Approach to Private DC-CB



In contrast to the Public/Private CBDC version, the Private DC-CB option offers a unique way of creating a digital currency backed by a central bank liability in a permissionless environment. As noted earlier, the International Monetary Fund (IMF) introduced the concept of a “synthetic” central bank digital currency (sCBDC) when Tobias Adrian and Tommaso Mancini-Grifolli published their Fintech Note on “The Rise of Digital Money” in 2019. The IMF’s approach was to establish a public/private partnership to create a sCBDC by allowing a private e-money provider to hold central bank reserves.

The original idea is that any digital currency issued by an e-money provider would be done on a one-for-one basis with central bank reserves, which would be protected against creditors should the e-money provider go bankrupt. In essence, the IMF was creating a situation whereby e-money providers would be turned into narrow banks and focused solely on facilitating payment transactions.

In this scenario, the central bank would provide access to a reserve account and settlement services, but all other functions (including due diligence, technology development, customer service, etc.) would remain the responsibility of the e-money provider. As such, the IMF argued that “sCBDC is thus a far cheaper and less risky model of CBDC for central banks, relative to the full-fledged model”.

The idea of essentially using central bank reserves as collateral for the outstanding digital currency issued by an e-money provider is an intriguing idea. However, there are a number of issues with this approach that need to be considered and, according to a recent BIS report,²³ such a framework could not strictly be considered a CBDC due to the fact that it would not be issued by a

²³ Bank for International Settlements. “Central Bank Digital Currencies: Foundational Principles and Core Features”. October 2020..

central bank. This section will examine these issues in detail and outline a different approach to creating a Private DC-CB, instead of a synthetic CBDC, that may satisfy the concerns of the BIS and other central banks.

Questioning the status of central bank reserves

At the heart of the BIS's objection to the IMF's approach is the belief that the end user of the digital currency would not hold a claim on the central bank. It's unclear if the BIS is questioning the status of reserves as a legal claim on the central bank, or if they are concerned that any legal claim afforded to the digital currency provider holding its funds in a central bank account would not pass through to the end-user, should the provider go bankrupt. Nonetheless, without this central bank liability, any digital money issued by a private provider, and backed by central bank reserves, does not meet the definition of a CBDC, according to the BIS.²⁴

The report further notes that in addition to not meeting the CBDC definitional requirements, such digital currencies also lack “key features of central bank money” -- namely, they are motivated by profit objectives, rather than public policy objectives. Thus, they lack neutrality and inclusiveness, and may potentially lead to “concentration and monopolies or fragmentation”.

Finally, the BIS cites concerns around liquidity as yet another difference between CBDC and the “narrow-bank”-like money created using the IMF's approach. Essentially, the argument rests, again, on the idea that central bank reserves may not constitute a central bank liability (at least with regards to the end user). If underlying demand increases, a central bank could create additional liabilities, at short notice, in response to this demand, thus providing liquidity. But since a digital currency provider must match the funds it creates with reserves held at the central bank, they effectively are unable to add liquidity, according to this logic.

Considering additional issues raised by the IMF model

Aside from the issues raised by the BIS, concerns around efficiency, transparency, and access should also be considered. The fact that central bank reserves are “off-chain” assets -- meaning they are not on a blockchain, and thus require a custodian to safeguard and process the funds -- may not be as integral to the definition of a CBDC as the issue of legal liability, but it's vitally important, nonetheless, to the operational efficiency of a digital currency.

Requiring an “on-chain” digital currency to transform its assets into “off-chain” collateral impairs the efficiency of the system as this collateral must be processed by a third party, which often creates time lags. These time lags, combined with the fact that central bank reserves currently are not always accessible on a 24/7/365 basis, could create asset-liability mismatches.²⁵

²⁴ Auer and Böhme note that backing privately-issued digital currency with central bank reserves poses the added burden of determining the legitimate owner should the issuer go bankrupt, which may result in “lengthy and costly legal processes with uncertain outcomes.”

²⁵ Traditional asset liability management (or balance sheet management) in the context of banks is typically concerned with the mismatch between deposits and loans in terms of liquidity and duration or term structure. A similar mismatch (liquidity and term structure) exists between traditional assets and digital currencies, and should be considered if traditional assets are used for digital currency collateral.

Off-chain assets also reduce transparency. Data on central bank reserve holdings are not available to the general public. As such, the average user will not be able to confirm that the digital currency in circulation is, in fact, backed up by an equivalent amount of central bank reserves. Obviously, there is a stronger sense of security knowing that the reserves are held at the central bank instead of a commercial bank. Nonetheless, this arrangement still requires users to trust the central bank, limiting the transparency of the digital currency.

Indeed, the BIS report referenced concerns regarding the transparency of narrow bank money held at a central bank: “...concerns about the existence of the underlying matched funds could cause doubts on the value of the liabilities and result in users selling them at a discount to the par value of the currency.” If the underlying matched funds consisted of blockchain-based assets, instead of off-chain reserves, the “existence” of these funds would be easily verifiable.

Finally, access to central bank reserves could become an issue, especially for smaller digital currency providers. As noted in the IMF’s report, “[a]llowing e-money providers to hold central bank reserves would be a major policy decision”. In fact, it’s likely that such a decision would also require the changing of central bank legislation in many countries.

Typically, access to central bank reserves is limited to bank holding companies and international institutions.²⁶ Thus, legislation would need to be changed, allowing digital currency providers access, or such providers would need to turn themselves into banks. In either case, access would likely be limited to those providers that are large enough (or perhaps well connected enough) to gain access to central bank reserves.

Such a system could stifle innovation and give the perception that a central bank was arbitrarily choosing which providers received access to reserve accounts. Indeed, limiting access to central bank reserve accounts could further exacerbate the potential lack of neutrality and inclusiveness cited by the BIS, leading to an even greater concern for “concentration and monopolies or fragmentation”.

Proposing an alternative “on-chain” option backing Private DC-CB

Instead of referring to a privately-issued digital currency as a “synthetic CBDC,” and thus stirring a debate around the legitimacy of such nomenclature, it’s perhaps more productive to simply refer to this option as a Private DC-CB, as outlined earlier in the section on *Implementing a new system of digital currencies*.

²⁶ For example, according to the Federal Reserve Bank’s Operating Circular No. 1 (effective February 1, 2013) master accounts are reserved for financial institutions that are member banks, depository institutions, U.S. branch or agency of a foreign bank, or an Edge or agreement corporation, as defined in Section 25A or 25 in the Federal Reserve Act).

Furthermore, a more practical and efficient method of backing such a privately-issued digital currency with a central bank liability would be to replace (off-chain) central bank reserves with a (on-chain) central bank issued liability that could be purchased by digital currency providers, held in a trust, and used to back the issuance of digital currency on a one-for-one basis.

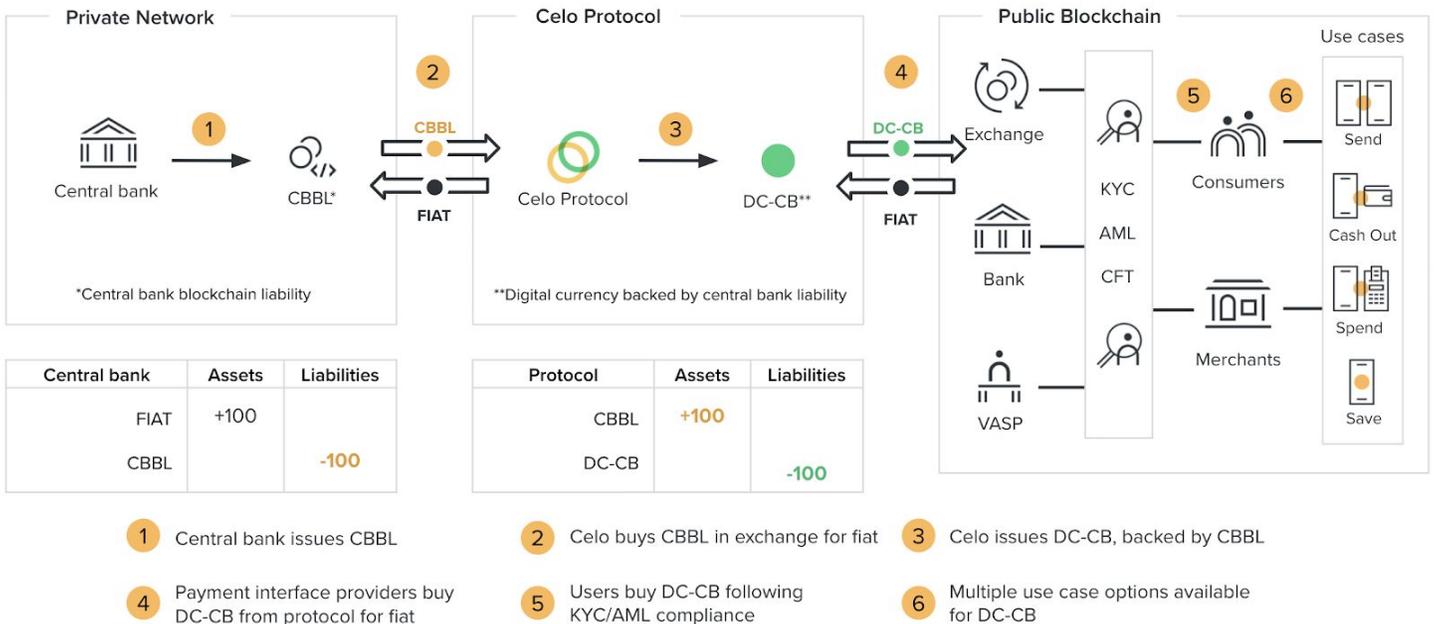
Such an asset could be thought of as a “central bank blockchain liability” (or CBBL) and would refer to an asset issued on a blockchain by a central bank that could be ring-fenced in the event of a bankruptcy by a digital currency provider. Such an asset would have the advantage of being both “on-chain” and a central bank liability, thus alleviating the two biggest concerns highlighted above.

Before going into a more detailed look at the advantages of this option vis-a-vis the central bank reserve model, it’s beneficial to provide an example of how the system could work. Let’s consider the following example, as illustrated in Chart 10.

Let’s assume a central bank issues 100 million of a CBBL. Concurrently, the Celo protocol issues 100 million of a digital currency pegged to the central bank’s unit of account (which we will call “DC-CB”) and uses the fiat proceeds to purchase 100 million of the CBBL from the central bank.

Distribution of DC-CB could be channeled from the issuance protocol through payment interface providers, such as banks, exchanges, and virtual asset service providers (VASPs), to ensure adherence to KYC/AML compliance protocols. Meanwhile, users would have access to myriad use cases and decentralized financial (DeFi) applications.

Chart 10: Alternative Private DC-CB model, with protocol distribution



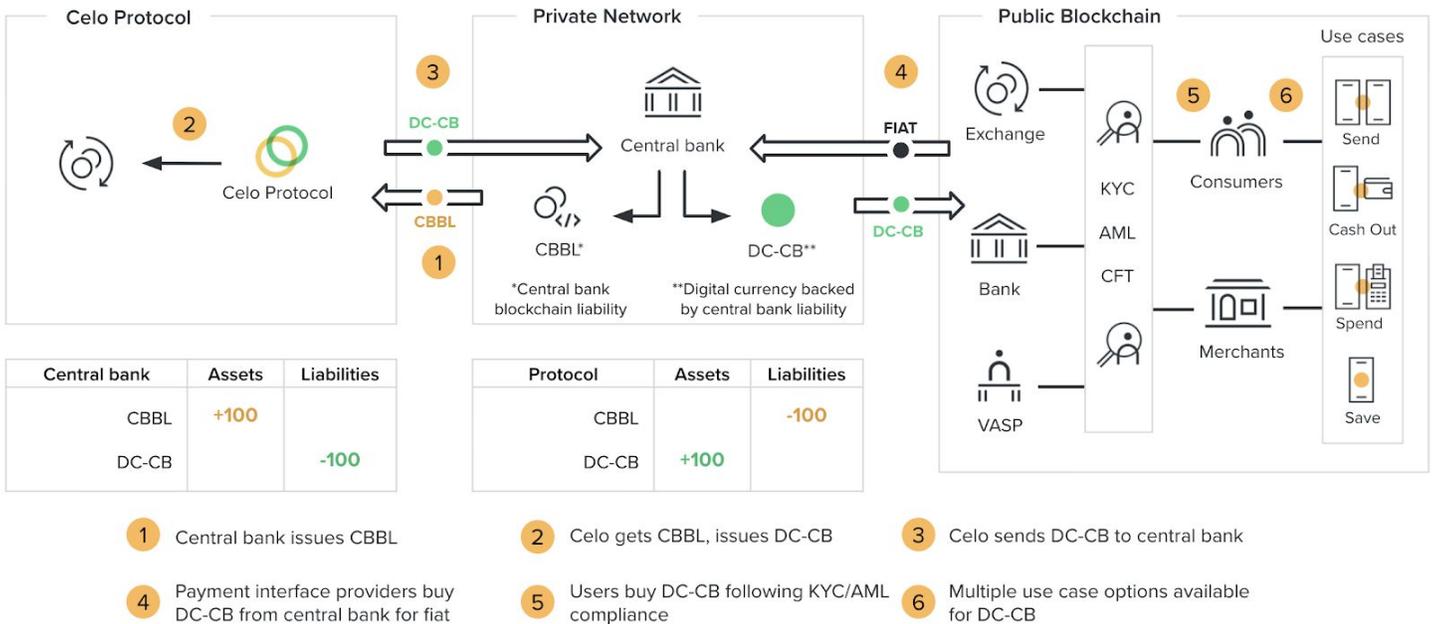
Alternatively, the distribution of DC-CB does not necessarily need to flow through the issuance protocol to the payment interface providers. Instead, the central bank could issue the CBBL and exchange it for the DC-CB with the protocol. In this instance, as illustrated in Chart 11 below, the central bank would have more control, as it would be able to distribute the DC-CB to authorized payment interface providers at its discretion.

Addressing the issue of central bank liabilities

As noted earlier, for a digital currency to be considered a “central bank digital currency” it must provide the holder of that digital currency with a legal claim against the central bank. In other words, a digital currency must be backed, one-for-one, by a central bank liability to be considered a CBDC. The BIS suggests that a digital currency backed by central bank reserves does not ultimately give the holder of that currency a legal claim against the central bank.

But the programmable nature of blockchain-based assets makes it possible to overcome this issue. When issuing the CBBL, a central bank would have full authority over the rules and regulations governing the asset. Therefore, it could be stipulated in a smart contract that, in the event a digital currency provider goes bankrupt, legal claim to the CBBL reverts to the holders of the digital currency (e.g. DC-CB). This would make the end users legal claim against the central bank explicit, and specific to the amount of DC-CB they are holding at the time of the bankruptcy.²⁷

Chart 11: Alternative Private DC-CB model, with central bank distribution



²⁷ Alternatively, an arrangement analogous to Federal Reserve notes issued in the early part of the 20th century that were redeemable in gold (or silver) could be devised. But in this case, DC-CB could be structured to be redeemable in the CBBL.

Regarding the issuance of a CBBL, it will, admittedly, require some amount of work on the part of the central bank. There are very few examples of blockchain-based assets available at the moment, but the World Bank's "bond-i" blockchain-based bond initiative could serve as a useful prototype. Importantly, the programmable nature of the blockchain would afford central banks the ability to issue CBBL to their exact specifications.

For example, such an asset could be issued on a central bank's private, permissioned network, giving the central bank authority over who has access to the CBBL. As with reserve accounts, central banks would be able to decide which digital currency providers are authorized to purchase the CBBL, presumably based on the providers ability to meet certain requirements.

Additionally, the central bank would be able to issue the asset in any amount it deems appropriate, and, importantly, they would be able to adjust issuance levels over time. As such, the central bank would effectively control the supply of DC-CB, since they control supply of the CBBL.

Finally, the rehypothecation of the CBBL could be forbidden, to ensure that the DC-CB is always collateralized on a one-for-one basis.

Highlighting the advantages of a Private DC-CB

Assuming a blockchain-based asset issued by a central bank could be considered a central bank liability, the ability to use such an asset to create a Private DC-CB issued by a digital currency provider could offer substantial benefits related to access, liquidity, efficiency, and transparency.

In the example above (in Chart 10), the process was simplified, and suggested that the entire issuance amount of 100 million of the CBBL would be purchased by the Celo protocol. But in reality, access to the CBBL does not need to be limited to just one digital currency provider. As noted earlier, central banks could decide which providers are authorized to purchase the CBBL, based on the ability to meet certain criteria. As such, a central bank could issue a CBBL in the amount of, for example, 1 billion and allow all authorized digital currency providers the ability to purchase a portion of the asset, with which to back up their digital currency.

Such a framework would provide a market-based approach to the creation of DC-CB, allowing central banks to remain neutral. All authorized digital currency providers would have access to the same high-quality collateral, allowing market participants to decide which provider(s) they prefer based on product offerings, user experience, customer service, etc. instead of on which provider(s) was able (or lucky enough) to get access to central bank reserves.

Indeed, this approach should help foster neutrality and inclusiveness, and alleviate concerns regarding the profit motivations of private digital currency providers. By controlling access to the CBBL, central banks can guard against monopolies or

fragmentation.²⁸ This framework can also help address liquidity issues, since the central bank is able to adjust CBBL issuance levels based on demand, allowing digital currency providers to modify their holdings of the central bank asset based on demand for their digital currency.

Let's return for a moment to our example above, where the central bank issues 1 billion worth of a CBBL and allows all authorized digital currency providers the ability to purchase part of the CBBL as collateral for the issuance of their digital currency. If there are five authorized providers in the system, and each of them purchases 100 million of the CBBL, there would still be an additional 500 million available. This could effectively serve as a liquidity buffer in the case that some (or all) of the digital currency providers needed to buy more of the CBBL to meet increased demand. Obviously, as the total amount outstanding increased towards the 1 billion mark currently issued, the central bank would need to decide whether they wanted to issue more of the CBBL or not. But this situation is not too dissimilar to the current way in which physical banknotes are managed, so central banks should be familiar with how to handle such circumstances.

Another advantage of using a blockchain-based asset as collateral for a Private DC-CB is the “on-chain” nature of the asset. Collateralizing an “on-chain” digital currency with an “on-chain” asset means that the collateral can be rebalanced at the same time as the underlying currency is minted or burned, which not only improves the efficiency of the system, but also helps prevent asset-liability mismatches. These efficiency gains would be impossible with “off-chain” central bank reserves, which require third-party processing.

Finally, using “on-chain” assets to collateralize the DC-CB also means that all aspects of the digital currency will be on the blockchain and thus fully transparent. Any user can audit the code to confirm that the total amount of currency issued is, in fact, backed up by a corresponding amount of collateral held in the form of a central bank blockchain liability. This ability to verify the existence of the underlying matched funds, should remove any doubt, and thus negate the possibility of the digital currency trading at a discount to par.

²⁸ In fact, commercial money currently created by traditional financial institutions is quite similar to Private DC-CB. The ability of commercial banks to loan money into existence, backed by central bank reserves, is not too dissimilar from the idea of private entities issuing digital currencies backed by central bank liabilities. Since central banks have largely been able to successfully guard against monopolies and fragmentation with respect to the profit objectives of traditional financial institutions, it's likely they will be able to do the same with digital currency providers.

Appendix

Whether the ultimate design of a digital currency is permissioned or permissionless, there are a few issues on the Celo platform common to both ends of the spectrum, including interoperability, privacy, and transaction fees.

Interoperability

Earlier, in the section on *Understanding interoperability and the importance of bridges* the concept of interoperability was introduced, including a brief discussion of the significance of bridges with respect to the Celo platform. Given how integral interoperability is to the success of digital currencies, a more detailed discussion highlighting the current challenges, as well as Celo's approach to overcoming these challenges, will be given in this section.

In order to understand the importance of interoperability, it's important to look at Bitcoin and Ethereum. As the last decade has unequivocally proven, Bitcoin is overwhelmingly popular, representing about 80% of the total market cap of cryptocurrencies. But its code base has a relatively narrow feature set and does not support smart contracts, which means that it doesn't support decentralized applications like DeFi available on Ethereum.

However, Bitcoin and Ethereum operate on two different, and distinct, blockchains. They only care about verifying transactions on their respective chains, which necessitates custom-built cross chain architecture to allow for the transfer of information between chains. In other words, a Bitcoin user needs access to a "bridge" between the two chains to take advantage of DeFi apps. But these bridges are very difficult to build in a decentralized, trustless environment.

In order to build a trustless bridge between Bitcoin and Ethereum, the protocol needs to verify the state of the chain to which it's connecting to ensure the accuracy and legitimacy of the transaction. But, the fact that blockchains have been growing steadily, makes it difficult for resource constrained devices (especially mobile devices) to do a full sync, and thus verify the state of the chain.

Over the past few years, the Bitcoin blockchain has increased significantly and is now more than 320 GBs of data (see Chart 12 on the following page). The Ethereum blockchain is even larger, at approximately 340 GBs. So if you want to create a bridge from Bitcoin to Ethereum you essentially have to recreate the

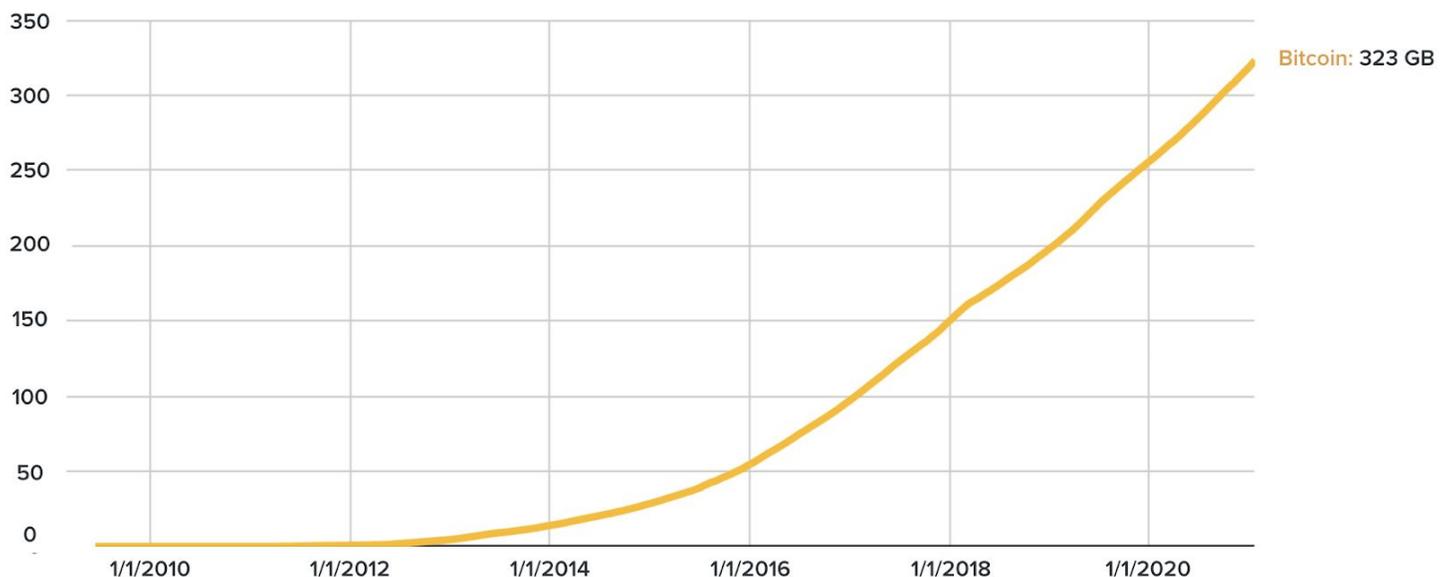
Bitcoin blockchain on Ethereum, which effectively doubles the size of the chain to more than 640 GBs.

Now, there are ways to reduce the data needs using a “Simple Payment Verification” technique, which essentially means that you only need to download the headers of a chain. Unfortunately, the amount of header data needed to sync in this fashion is still massive: 50 MB for Bitcoin, and 5.0 GB for Ethereum. Given the amount of data needed and the high transaction fees associated with Ethereum, it’s simply too expensive to maintain such a bridge.

As noted earlier, it’s highly likely that many central banks contemplating the issuance of CBDC are envisioning that it will be done on a private network. It’s also likely that this private network will not produce a significant amount of the decentralized apps (dApps) that provide utility for many people. As with Bitcoin, users of this CBDC will also desire a bridge to public blockchains like Celo and Ethereum, where they can access these dApps and use cases. But in order to do that, the issue of building bridges to create widespread interoperability still needs to be addressed.

In order to solve this problem, the team working on Celo developed an open-sourced light client called Plumo, which has made innovations in the use of epoch-based syncing, BLS signature aggregation, and zero-knowledge SNARKs to reduce the amount of data necessary to verify the state of a blockchain.

Chart 12: Blockchain size



Introducing Plumo, Celo's ultra-light client

To help address the issue of interoperability, Plumo introduces the concept of epochs, and limits validator elections to the last block of each epoch. This means that you can verify any header in any order within an epoch, and allows you to download only the last header of each epoch if you want to sync from the genesis block. At 5 second block times and 1 epoch per day, this reduces the amount of data that a light client has to download by 17,000 times.

Additionally, Plumo uses BLS signature aggregation to aggregate all of the signatures from each of the validators to a single constant sized multi-signature. This reduces the block size by roughly 10x, further improving light client performance.

Finally, Plumo uses zero-knowledge SNARK proofs, to compress the epoch syncing and BLS signature verification even more, down to a single 500 byte proof.

Ultimately, the innovations developed for the Celo protocol means the Plumo light client is 100k times lighter than Bitcoin, and 11 million times lighter than Ethereum -- making the idea of building bridges much more attainable and affordable.

Additionally, these innovations are helping to support the integration of tBTC with the Celo network. This integration effectively builds a bridge between the Bitcoin and Celo public blockchains, allowing users to simultaneously hold BTC and use it for any application (including DeFi) within the Celo ecosystem. And with the innovations developed in our light client, it also means that transactions between Bitcoin and Celo will be significantly faster and cheaper than Ethereum.

Privacy

Similar to Ethereum, accounts are pseudonymous on Celo networks. All value transfers are publicly visible to those who have access to the network, but information on the sender and recipient are limited to just the Celo addresses ("0xabcd...") used in the transaction. No further identifying information is available

on the blockchain. Additionally, traditional network-level access control remains the first form of transaction privacy.

To send a payment or payment request, the first step is to discover the address of the individual or institution with whom the transaction will be initiated. For an individual, a payment or payment request can be initiated using the recipient's mobile phone number. After submitting the individual's mobile number, he or she will receive a text prompting them to download the Celo wallet (called [Valora](#)), after which the public key associated with the newly created account will be securely (and privately) connected to the individual's mobile number, allowing them to finalize the transaction.

An institution, however, may wish to only be discoverable by a subset of other potential actors on the network. When an institution joins the network, their well-known public key certificate is used to communicate to the Celo ARKE service to establish a shared key with each of the potential recipients (also denoted by their public key certificate). With this shared key, the institution can share its payment address by encrypting it with the shared key and storing it in the ARKE cache. This is similar to the mechanism that is used to map phone numbers to addresses on the Celo public network.

The ARKE service allows message recipients to be addressed by their certificate subject or common name. ARKE verifies the recipient's certificate subject and certificate root and not the certificate public key, which allows the recipient to update their certificate over time and still send/receive messages using the certificate. The ARKE service is semi-decentralized which prevents any individual ARKE operator from accessing secret information or having the ability to censor requests.

Transaction Fees

Every blockchain network has limited block space and must allocate this space across all applications and participants. Public blockchains use a fee-based structure, paid in digital currency, to fairly distribute this space. Using space in a block consumes what is referred to as "gas," which is basically the time and energy used by validators to verify the transactions on the blockchain. The price of each unit of gas is referred to as the "gas fee" and equates to the price associated with each transaction.

Typically, on a permissionless blockchain, the sender is responsible for paying the gas fee. For permissioned networks this process can add unnecessary complexity. As such, the Celo network supports two gas-fee models: free-gas and paid-gas.

For central banks interested in implementing a CBDC on Celo using a permissioned network a free-gas model can be utilized, such that any entity which has access to this private network can submit transactions for free. This prevents

the hassle of first fauceting a wallet and relies upon traditional access control models to govern the block space.

In the paid-gas model, tokens are used to pay for gas in an approach similar to the Celo public network. This approach supports a governable list of tokens that can be used to pay for gas fees. This set can even be updated to include assets from other Celo networks (ex. USD, EUR).

Monetary Policy Implications

The potential impact that issuing a central bank digital currency could have on monetary policy is a very important (and complex topic) that has been the focus of countless reports. A thorough investigation of the monetary policy implications of issuing a CBDC on Celo is provided in a whitepaper published by the cLabs team focused on [“Influencing the Velocity of Central Bank Digital Currencies.”](#)

Aside from providing a more detailed understanding of the impact of a Celo-based CBDC on the financial system, the paper also goes into an in-depth discussion on the possible ways in which CBDC could be programmed on Celo to help influence the velocity of CBDC, giving the central bank a new channel for the transmission of monetary policy and helping to support economic growth and development.

