ISSUING CENTRAL BANK DIGITAL CURRENCY USING ALGORAND

ABOUT THE AUTHORS

Andrea Civelli

Senior Economist , Algorand, Inc

Andrea Civelli is a Senior Economist at Algorand and an Associate Professor in Economics at the Walton College of Business (University of Arkansas). His research interests focus on monetary policy transmission and inflation modeling, with a particular interest in the role of the banking sector and business loan supply in the propagation of macroeconomic shocks. His research has been published in numerous Economics and Financial journals. Andrea received a Ph.D. in Economics from Princeton University in 2010, and also held visiting positions at UT Austin and NC State University.

Co-Pierre Georg

Member of the Economic Advisory Council, Algorand Foundation

Co-Pierre Georg is an Associate Professor at the University of Cape Town and holds the South African Reserve Bank Chair in Financial Stability Studies. Co-Pierre's research interests focus on the nexus of financial innovation and financial stability. He obtained his PhD from the University of Jena in 2011 and has published both in finance and interdisciplinary journals. Co-Pierre has been a consultant at various central banks and held visiting positions at MIT, Oxford, Princeton, and Columbia University. Aside from being a Research Associate at the Oxford Martin School for the 21st Century, he is a Research Affiliate at the Columbia University Center for Global Legal Transformation. He serves on the Economic Advisory Council of the Algorand Foundation.

Pietro Grassano

Business Solutions Director, Europe at Algorand, Inc

Pietro Grassano is the Business Solutions Director – Europe at Algorand. At J.P. Morgan Asset Management from 2002 until 2019, Pietro has been Country Head for France since 2014: beforehand he had been Head of Sales for Italy and responsible for business in Greece. Before 2002, he held commercial functions at BNP Paribas Asset Management in Milan. He has more than 20 years of experience in the asset management sector. He was previously a consultant in the financial pole of Andersen Consulting. Pietro started his career in Brussels, in a commodities trading company. He holds a Master in Economics and Social Sciences (DES) from Bocconi University in Milan, and a baccalaureate in humanism (maturità classica) at the "Andrea Doria" High School in Novi Ligure. He is a proud supporter of the Torino Calcio football team.

Naveed Ihsanullah

Head of Engineering Research, Algorand, Inc

Naveed is VP of Engineering Research at Algorand where he focuses on future technology and features for Algorand's blockchain platform. He is a senior engineering leader and technologist with more than 20 years of experience and continues to be fascinated by distributed systems and performance. Most recently of Mozilla, Naveed was instrumental in designing and leading the Quantum Flow program that focused 400 engineers to double Firefox's performance in just one year. Naveed also led the adoption of new technologies across all the major browsers (Chrome, Safari, and Firefox) to close the performance gap with native applications. These technologies include WebAssembly, SIMD.js, and Shared Array Buffer. Naveed is also previously of Carbon Black (then Bit9) where his teams developed next-generation application security software and cloud-base software reputation services. Passionate about improving how enterprises use technology Naveed has consulted on large organizational level projects for Fortune 500 companies including Boeing Jeppesen.

0. EXECUTIVE SUMMARY

Estimates from the European Central Bank indicate that the total cost of retail payments in the EU is 139 Billion Euro, about 1% of GDP, half of which comes from cash alone. Globally, this percentage is likely higher, because the cost of cash distribution in emerging markets is much higher due to the high cost of extending cash distribution networks to underserved rural areas and largely manual nature of labor involved in distributing cash. At the same time, many central banks worldwide are overhauling their existing payments infrastructure to increase the efficiency and competitiveness of their financial services sector. With next-generation blockchains like Algorand, distributed ledgers have reached the technological maturity to serve as the critical infrastructure for a financial system of the future.

We believe that central bank digital currencies are the next natural step in the evolution of payment systems and that their design and implementation should be driven by six considerations.

1 - How to ensure trust in the new payment instrument?

The key challenge when issuing a CBDC is to create trust in the new payment instrument to ensure it maintains value at least as well as its physical counterpart. This is one of the main reasons why cash issuance is so expensive: trust in cash as a payment instrument requires the central bank to ensure that notes cannot be counterfeited and that the cash supply chain is secure. Counterfeiting CBDC issued on the distributed ledger is impossible thanks to the ledger's cryptographic primitives. By contrast, entries on centralized ledgers can be manipulated if the ledger's database is hacked or otherwise compromised. This additional cyber security risk and associated costs make centralized digital currencies inherently less efficient than digital currencies issued on a distributed ledger.

Transacting in cash has immediate settlement finality, at least if both counterparties are in the same physical location. The digital-analog of cash must, therefore, also have immediate settlement finality. Otherwise, the instrument would carry counterparty risk, again undoing some of the benefits of introducing a CBDC. While most blockchains do not have immediate settlement finality, Algorand's pure proof-of-stake protocol implements this natively. Instant settlement finality together with the additional monitoring capabilities central banks get when issuing a CBDC imply that a CBDC is at least as trustworthy as cash.

2 - How to achieve scalability for a seamless user experience?

Most blockchains to date, particularly those based on a proof-of-work algorithm like Bitcoin and Ethereum, have been plagued by scalability issues and an insufficient number of transactions per second to meet even the light loads placed on them today by early adopters. However, to reliably handle the transactions for a larger country with about 50 million CBDC users, each of which transact about two to three times per day, the CBDC would have to handle on average 1,500 transactions per second. This is a factor of one hundred more than the standard proof-of-work blockchains process today.

Scalability is key for a seamless user experience, which, in turn, is key for the adoption and acceptance of the new payment instrument. If users have to wait several seconds even for low-value transactions to clear, many essential use cases for cash will be inaccessible for a CBDC. Algorand is designed to scale and easily achieves several thousand transactions per second in a decentralized system.

3 - How to balance anonymity and accountability?

Privacy is a human right and a necessary condition for broad adoption of a CBDC. As such, it is paramount, particularly in the context of retail CBDCs, to balance this right carefully with the regulatory need to ensure transactions are KYC/AML compliant. This requires a layered approach to privacy with adjustable limits for fully private, partially private, and fully transparent transactions. Importantly, central banks must have full control over the thresholds between the different layers of privacy and be able to change these as necessary.

Algorand provides a flexible framework that allows governments and central banks to specify their own tiers of privacy and delegate, as needed, identity to authorized Identity Providers in their system using a combination of built-in features and powerful Layer-1 smart contracts. This layered approach to privacy is both practical and in stark contrast to the approach most private crypto assets have chosen, where there is no native notion of privacy. These blockchains instead rely on

pseudonymous addresses as a means of protecting user privacy, but this approach to privacy is in direct conflict with existing know your customer and anti-money laundering requirements. We believe that, rather than fixing this protocol flaw, it is better to design for privacy from the beginning. Algorand's permissioned blockchain for CBDC allows us to thread the privacy-compliance needle carefully.

4 - How to achieve full inclusivity?

For a payment instrument to be universally accepted and trusted, it needs to be available to everyone in a country. This is a significant challenge for central banks because smartphone penetration is far from perfect, even in the United States where it stands at about 80%, and even more so in emerging markets like India where smartphone penetration sits at around 37%. Consequently, any retail CBDC design must make provisions for users without smartphones.

Achieving full inclusivity faces two related challenges: identity and access. Especially – but not only – in emerging markets, users do not always have identity documents. Central banks issuing CBDC will have to seek broad stakeholder engagement to solve the digital identity challenge, amplified by the lack of access, the second challenge to full inclusivity.

Algorand embraces radical inclusivity, for example by facilitating the inclusion of users without smartphones. To enable access, solving identity is fundamental to scaling economic inclusivity. One of Algorand's core design principles is to create generalized and flexible tools that can be applied to many different problem sets. Algorand has worked with identity companies to create on-chain identity attestations. These attestations can be used inline with many emerging identity standards, such as W3C Decentralized Identifiers, so that identity can be portable across many different platforms.

In our recently published white paper [LINK], we outline solutions that we have designed to allow users with intermittent connectivity and without smartphones to be included on an entirely equal footing to users with good connectivity and smartphones, highlighting Algorand's focus on radical inclusivity for central bank digital currencies.

5 - How to guarantee interoperability?

The hardest part of designing new financial infrastructure is developing the protocols and processes in a robust and resilient way that is compatible not just with legacy systems but also with future requirements. In the ecosystem view adopted by Algorand, this work is front-loaded and has informed the fundamental design of our open-source blockchain technology. Algorand's "openness-by-design" architecture creates an ecosystem where the protocol facilitates the seamless interaction of various ecosystem partners (banks, e-money companies, payment providers, etc.).

Consequently, we have front-loaded the hard work of creating protocols and processes to allow a diverse set of ecosystem players to interact without any one party's ability to create barriers to entry. This is vastly different from other approaches, who effectively try to create walled gardens [LINK TO DEFINITION?]. Algorand has created an open platform that prevents capture by any private actor while giving central banks and government agencies full control over which users and use cases are allowed on the platform.

6 - How to incentivize competition?

The rise of private digital assets has set off a flurry of innovation among small startups, large banks, and big tech companies alike. Within Algorand's first year, the rapidly growing ecosystem had over 500 organizations join the tens of thousands of companies innovating in the broader digital asset space. To foster competition, an open system without barriers to entry is paramount. No walled garden solution can achieve this because, in such solutions, a provider can never commit not to create barriers to entry further down the line. The rules of a walled garden can be modified at any time by the solution provider. Algorand's open protocol enforced by decentralized validation ensures that any system built on our platform will always incentivize competition while curbing regulatory arbitrage. Only the collective wills of the authorized parties can choose to alter the rules of the system once established.

TABLE OF CONTENTS

1. INTRODUCTION

In 2012, the European Central Bank estimated that, in the EU, the total cost of retail payment instruments to society is about 1% of GDP (139B Euro), almost half being cash alone.[1] This percentage is likely a lower bound from a global perspective, as the price of cash in emerging markets is much higher. McKinsey's report highlights two reasons for this: the extension of cash distribution networks to underserved regions and the fact that cash distribution remains manual and is therefore labor-intensive.[2] In emerging markets, security concerns are amplified and add substantially to the cost of cash, both for central banks and commercial banks and for their customers. Despite incremental advancements to the existing central bank payment infrastructure, the cost of cash management shows no signs of change as cash continues to account for over 90% of all transactions in emerging markets. However, the advancements in speed, security and usability of blockchain technology has created the necessary platform for central banks to radically improve their cash management and distribution at scale.

Similar to the cost of cash management, the costs of foreign exchange operations for participants are high, even for the most basic transactions. These costs are mostly due to the lack of competition for cross-border payment services. These costs are concentrated in a handful of very large brokers as is the design of correspondent banking systems, where transaction validation and settlement must go through a long chain of intermediary domestic banks and the SWIFT cross-border confirmation system. For instance, a study by Hau et al. (2019) estimated forex fees as high as .5%, with large asymmetries between larger and smaller traders. Also, the SWIFT network is even more expensive. A report by the Financial Stability Board estimated that the typical fee for a $200 international remittance on the SWIFT network was 7% in 2019.[3] Another type of cost of the current settlement system is related to banks' liquidity and collateral management in the security markets. An estimate by Hartung et al. (2019) finds that holdings of high-quality liquid assets for collateralization can cost banks up to 50 basis points. This corresponds to approximately €13.5bn per year just for the holding of assets above the Basel III minimum requirements. Blockchains able to perform truly atomic transactions with immediate finality can substantially lower counterparty risk, reduce costs and enable more collateral to be put to work versus being allocated against securing transactions.

A critical requirement for the viability of central bank digital currencies is the inalterability of the core blockchain infrastructure, both now and in the future. Blockchains rely on modern cryptography to guarantee their security. New technologies on the horizon, such as quantum computers, may break the assumptions that many of today's blockchains are built on. This has the potential to expose end-users (citizens) to massive losses of value. Therefore, it is essential that a blockchain solution for CBDC is quantum resilient, a task that few blockchains organizations are well positioned to execute against today and in the future.

The Algorand blockchain provides the foundation for the future of economic exchange with global-scale performance on par with centralized solutions while also delivering the safety, security, and resilience that can only come from a truly decentralized system. Conceived of and built by an MIT team, led by Turing Prize-winning Professor Silvio Micali, Algorand is the world's first Pure Proof-of-Stake (Pure PoS) blockchain platform. Pure Proof-of-Stake refers to the system's ability to resolve transactions in a secure and expeditious manner. In blockchain parlance this is called, "Consensus." Algorand's novel consensus mechanism is designed to ensure that transactions are fast, instantly final, while ensuring that the blockchain never soft forks. Soft forking is when there is the possibility of two 'legitimate ledgers' existing in parallel. During a soft fork, network participants can append transactions, such as payments and cash distribution, to a fork of the chain that is ultimately deemed incorrect, thus negating all transactions that were appended to the 'wrong fork.' Thus preventing soft forking, among being fast, and secure are critically unique capabilities for a technology that provides the immutability essential for a CBDC. Additionally, thanks to Algorand's Research team leading the development and contribution to state-of-the-art in post-quantum cryptography, Algorand's blockchain will be safe and secure, even if quantum computer technology continues to make significant advances. Algorand has built the technical infrastructure for CBDCs to move from an experiment to real world implementation and scale to global adoption.

The CBDC model that we propose is a hybrid model, built on a private instance of the public Algorand blockchain in a two-tier retail system. In this model, central banks have full control over the CBDC. Simultaneously, licensed service providers (LSPs),

[1]Source: https://www.ecb.europa.eu/pub/pdf/scpops/ecbocp137.pdf

[2]Source: https://www.mckinsey.com/industries/financial-services/our-insights/attacking-the-cost-of-cash

[3]Source: https://www.fsb.org/wp-content/uploads/P090420-2.pdf

such as commercial banks, remittance providers, and other fintech companies, can facilitate distribution and transactions. This model also allows the central bank to delegate customer service responsibilities to institutions with that capability.

Compared to traditional bank accounts, a blockchain-based retail CBDC can reach a broader base of consumers, including those in the informal economy who might face difficulty opening a conventional bank account and who are, thus, unable to use digital services offered by banks. Compared to a traditional account-based digital currency, Algorand's proposed design will be simpler and more economical to implement and manage for central banks at scale.

Algorand's approach to retail CBDC proposes the creation of a retail digital asset similar in characteristics and purpose to cash that is issued and fully backed by the central bank as legal tender. This positioning allows for a widely accessible, easy-to-manage currency exchangeable by consumers and businesses in a peer-to-peer fashion. By adopting 'digital first' distribution, cash treasuries can be managed programmatically, significantly reducing the cost of cash management and providing standard interfaces to streamline foreign exchange through atomically swapping CBDCs that represent different fiat currencies.

It is worth mentioning that our proposed model will not destabilize existing systems. Being an open platform that is easily integrated via standard APIs, Algorand's infrastructure and network complements current systems and would be able to work alongside physical cash. As an example, Algorand's CBDC model can be fully integrated with local real-time gross settlement systems (RTGS) payment systems. Through Algorand's standards, such as asset creation and our transaction approval framework, a CBDC issued on Algorand's platform can programmatically receive instructions from the RTGS to issue the digital currency to service providers and the public.

Our approach to designing CBDC systems follows an open system design with the open-source Algorand blockchain at its core. Unlike many enterprise blockchain providers who effectively build a walled-garden and lock central banks to a single solution provider, the Algorand system is designed to have open APIs that foster competition and prevent vendor lock-in. By introducing competition, central banks are able to better serve their constituents by embracing innovative designs that ultimately drive the cost per transaction down. To be clear, open-source should not be interpreted as open-access. While anyone can develop applications that integrate with Algorand's standards, such as the 'Algorand Standard Asset,' each network, asset and application can implement 'Role Based Access Controls' ("RBAC"). These controls can determine, under what conditions is an entity/individual allowed to join the network, under what conditions can an entity/individual create an account and receive CBDC, and under what conditions can an entity/individual participate in financial applications, such as peer-to-peer lending and borrowing. These controls follow a defense in depth strategy and provide the Central Bank with a programmatic way of protecting their citizens while also fostering open innovation from the technology community.

To create a suitable environment for innovation, the network architecture consists of two networks, a pre-production betanet, which can be used by all institutions to program their products/services against a 'beta-CBDC' for end-to-end testing. After sufficient review, and approval from the Central Bank, and or review from the broader community, applications launched in betanet can be promoted and deployed to the Mainnet. To date Algorand's implementation of the model described above has involved collaboration with both local consortium partners and global technology companies collaborating to deliver a solution tailored to each country's specific characteristics and needs. By employing an open-source design, such as Algorand's, all participants benefit from open competition while adhering to systematic protections.

One of the defining characteristics of Algorand's standards is that they facilitate interoperability between a public and private Algorand network if the Central Bank so chooses. The Algorand Foundation has built and developed a Public and Permissionless blockchain network using the Algorand open-source code. The public and permissionless platform has developed a vibrant economy with over 600 organizations, millions of users and $12BN worth of assets available to its ecosystem. The private instance on which the CBDC will be issued will be fully interoperable with the Algorand Foundations network due to the same standards being employed in both networks. This interoperability provides central banks with the best of both worlds: complete control over the private networks validators, the geographic location of this infrastructure, while also facilitating a connection to the public domain for access to a broader ecosystem of other digital goods and services. By virtue of the two networks being interoperable, the central banks can utilize public infrastructure, such as current and future assets (e.g. stablecoins denominated in other currencies or other CBDCs) at their sole discretion. This unique capability provides central banks with a future proof path that ensures as new innovations continue to occur

that their CBDC will be benefit and be interoperable with all infrastructure connected to any Algorand network. In the same way that central banks can define the conditions by which an entity or organization can acquire their CBDC, they can also define the requirements for their CBDC to be transacted against other CBDCs. This is a unique value proposition that only Algorand's technology can provide to central banks.

The rest of this whitepaper is organized as follows:

Section 2: Designing Efficient CBDC
Outlines principles for designing efficient central bank digital currencies that Algorand has identified through our various CBDC projects.

Section 3: Economic Considerations when Issuing CBDC
Discusses economic implications when issuing a CBDC, from balance sheet and financial stability implications to monetary policy consequences.

Section 4: The Algorand Protocol
An overview of the Algorand protocol, including design principles and a high-level overview of the protocol itself.

Section 5: Issuing Retail CBDC with Algorand
Algorand's approach to issuing retail CBDC, including a detailed overview of relevant design considerations and examples of use cases facilitated by the Algorand platform. In particular, we present the critical use cases of issuing CBDC when connectivity is limited and adjustable privacy requirements for low- and high-value transactions.

Section 6: Issuing Wholesale CBDC with Algorand
Algorand's design approach to wholesale CBDC and the most relevant use cases; additional use cases are discussed in detail in Appendix A.

Section 7: Conclusion
Closing thoughts on why a hybrid CBDC model, built on a private instance of the open public Algorand blockchain in a two-tier retail system is a unique approach from enterprise and other providers.

2. DESIGNING EFFICIENT CBDC

Creating a central bank digital currency is the building of a new payments infrastructure. While not an unprecedented task—the introduction of electronic fund transfers in the United States in 1918 and the move from telegraph to telex to computer networks between 1960 and 1990 have many hallmarks of the current overhaul of national payment infrastructure – introducing a CBDC is more complicated than previous iterations of payment system innovations. Real-time gross settlement systems connect a relatively fixed set of counterparties, typically banks, and facilitate a small number of use cases. In contrast, many CBDC proposals include a much broader set of entities involved in the distribution of CBDC to the greater public. This extension is likely intended to improve the competitiveness of the financial system, but simultaneously increases the CBDC's implementation complexity.

Algorand's approach to CBDC has, therefore, been inspired not by the development of products but by the creation of general-purpose infrastructures like roads, railroads, harbors, bridges, and the Internet itself. We believe that, in particular, the history of the Internet provides a useful blueprint for the design of CBDC. For example, Clark (2018) outlines the "hourglass model" of the Internet structure with TCP/IP as the two common standards that implement the Internet as a packet transport system at the center. On top of the common standards is the highly diverse Internet experience, including all the possible applications such as the Web, email, video, and games. Below the common application standards are supporting physical transport technologies like broadband, wifi, ethernet, and cellular networks, which are also highly diverse. The private, permissioned Algorand blockchain achieves for central bank digital currencies what TCP/IP has achieved for the Internet: provision of a common standard for a plethora of user-facing applications and facilitation of a wide range of different deployments depending on the central bank's requirements.

On top of the hourglass are all the different applications that can be built on Algorand's technology. Section 4 provides details of the Algorand protocol features, facilitating the easy development of applications on top of the distributed ledger.

An extensive and rapidly growing ecosystem of applications building on the Algorand public blockchain is testimony to Algorand's ability to facilitate innovation. On the bottom of the hourglass, where in the Internet example there are different physical layers of network infrastructure, in the CBDC case there are other national real-time payment infrastructures. While most countries use RTGS systems, each country has specificities, both regulatory and technical, that are unique to them.

In that sense, a CBDC, like the Internet, is a piece of infrastructure, and it is useful to study proposals for CBDC designs in this light. Looking for high-level common denominators of all these infrastructures, we find at least three (see also Kasper (2015)):

1. The infrastructure needs to be **efficient** in the sense that it has to solve a real problem in a way that is both cost-effective and fit for purpose;
2. It needs to be **universally accessible**;
3. It needs to be **secure** for the user.

These principles naturally apply to existing RTGS payment systems as examples of a more general economic exchange infrastructure. However, to ensure they also apply to CBDC, two sets of considerations are essential: which design principles the CBDC follows, and its financial implications.

In this section, we focus on the first set of considerations, identifying six key points: (i) how to ensure trust in the new payment instrument and the central bank; (ii) how to achieve scalability for a seamless user experience; (iii) how to maintain the privacy of low-value transactions while ensuring full auditability for high-value transactions; (iv) how to achieve full inclusivity; (v) how to guarantee the interoperability of the system; and (vi) how to incentivize competition.

How to ensure trust in the new payment system.

The key challenge when issuing a CBDC is to create trust in the new payment instrument to ensure it maintains value at least as well as its physical counterpart. This is one of the main reasons why cash issuance is so expensive: trust in cash as a payment instrument requires the central bank to ensure that notes cannot be counterfeited and that the cash supply chain is secure. Counterfeiting CBDC issued on the distributed ledger is impossible thanks to the ledger's cryptographic primitives. By contrast, entries on centralized ledgers can be manipulated if the ledger's database is hacked or otherwise compromised. Eliminating cybersecurity risks will, therefore, be absolutely essential for centralized digital currencies. We believe that the additional cost of ensuring a centralized ledger's security offsets some of the efficiency gains of a central bank's digital currency issued on that platform.

Transacting in cash has immediate settlement finality. The digital-analog of cash must, therefore, also have immediate settlement finality. Otherwise, the instrument would carry counterparty risk, again undoing some of the benefits of introducing a CBDC. While most blockchains do not have immediate settlement finality—and some do not have settlement finality at all—Algorand's pure proof-of-stake protocol implements this natively.

Another advantage of a CBDC over cash is that it is much easier to monitor the circulation of CBDC and detect fraud. The ledger's transparent nature makes it possible for central banks to use sophisticated data analytics to detect irregularities and fraud.

How to achieve scalability for a seamless user experience

Most blockchains to date, particularly those based on a proof-of-work algorithm like Bitcoin and Ethereum, have been plagued by scalability issues and an insufficient number of transactions per second to meet even the light loads placed on them today by early adopters. However, to reliably handle the transactions for a larger country with about 50 million CBDC users, each of which transact about two to three times per day, the CBDC would have to handle on average 1,500 transactions per second. This is a factor of one hundred more than the standard proof-of-work blockchains process today.

Algorand is designed to scale and easily achieves several thousand transactions per second in a decentralized system. Decentralization is a function of the number of participants in the consensus protocol, hardware requirements, topography,

and the number of people who own a stake in the consensus protocol itself. Algorand, unlike other platforms, has decided that to run critical infrastructure, enabling decentralization at every level is key to avoiding single points of failure. For example, standardizing on a single type of GPU/CPU/ASIC/LSIC for your network infrastructure significantly increases the likelihood that your network will be susceptible to a particular hardware attack. Having a lower threshold for hardware ensures diversity in machines upholding the network and, therefore, mitigates the impact of any individual targeted vulnerability from taking down the whole system.

Scalability is key for a seamless user experience, which, in turn, is key for the adoption and acceptance of the new payment instrument. If users have to wait several seconds even for low-value transactions to clear, many essential use cases for cash will be inaccessible for a CBDC. However, most central banks' stated goalposts evaluating the issuance of retail CBDC is to find a payment instrument that can complement cash in circulation.

The flipside of scalability is the network structure. It is not difficult to have two computers next to each other and thereby to achieve a relatively high number of transactions per second. However, such a setup is not secure, with decentralization eliminating systematic risks and cybersecurity risks. Algorand has proven to be highly scalable even on a globally decentralized level with its MainNet and valuable experience designing systems that are both fully decentralized and highly scalable.

How to maintain privacy for low-value transactions while ensuring full auditability for high-value transactions

Privacy is a human right and a necessary condition for broad adoption. As such, it is paramount, particularly in the context of retail CBDCs, to balance this right carefully with the regulatory need to ensure transactions are KYC/AML compliant. This requires a layered approach to privacy with adjustable limits for fully private, partially private, and fully transparent transactions. Importantly, central banks must have full control over the thresholds between the different layers of privacy and be able to change these as necessary. Algorand does not impose a one-size-fits-all solution to this privacy/transparency continuum. Instead, Algorand provides a flexible framework that allows governments and central banks to specify their own tiers of privacy and delegate, as needed, identity to authorized Identity Providers in their system using a combination of built-in features and high performance/powerful Layer-1 smart contracts.

This layered approach to privacy is both practical and in stark contrast to the approach private crypto assets like Bitcoin and Ethereum have chosen, where there is no native notion of privacy. These blockchains instead rely on pseudonymous addresses as a means of protecting user privacy. This approach to privacy is in direct conflict with existing KYC/AML requirements. We believe that, rather than fixing this protocol flaw, it is better to design for privacy from the beginning. Our permissioned Algorand blockchain for CBDC allows us to thread the privacy-compliance needle carefully.

How to achieve full inclusivity

For a payment instrument to be universally accepted and trusted, it needs to be available to everyone in a country. This is a significant challenge for central banks because smartphone penetration is far from perfect, even in the United States where it stands at about 80%, and even more so in emerging markets like India where smartphone penetration sits at around 37%.[4]Consequently, any retail CBDC design must make provisions for users without smartphones. Achieving full inclusivity is crucial for retail CBDCs and wholesale CBDCs, depending on the use case (e.g., to ensure that all participants in a transaction comply with KYC/AML regulations).

Achieving full inclusivity faces two related challenges: identity and access. Especially – but not only – in emerging markets, users do not always have identity documents. In their 2016 paper "A Blueprint for Digital Identity," the World Economic Forum highlights the importance of building digital identity infrastructure for the future of financial infrastructure. Central banks issuing CBDC will have to seek broad stakeholder engagement to solve the digital identity challenge, amplified by the lack of access, the second challenge to full inclusivity.

With limited smartphone penetration and the resulting lack of digital identity, a substantial fraction of the population will not only struggle to transact using CBDC, but even to gain access to it. This is of particular importance for unbanked people

[4] See Newzoo Global Mobile Market Report 2019 – Light Version
Source: https://newzoo.com/insights/trend-reports/newzoo-global-mobile-market-report-2019-light-version/

in emerging markets. For no other group is this challenge as prevalent as for refugees. Algorand embraces *radical inclusivity*, e.g., by providing access to basic financial services for refugees, and facilitating the inclusion of users without smartphones. To enable access, solving identity is fundamental to scaling economic inclusivity. One of Algorand's core design principles is to create generalized and flexible tools that can be applied to many different problem sets. Algorand has worked with identity companies to create on-chain identity attestations. These attestations can be used inline with many emerging identity standards, such as W3C Decentralized Identifiers, so that identity can be portable across many different platforms. In working with companies such as FlexFinTx and Republic, all of the individual's personal and private information resides off-chain. Still, the account's ability to own a particular asset, e.g., a security, is published on-chain. With the attestation issued on-chain, asset issuers can enforce logic that requires these attestations to be presented at a particular moment in time, e.g., at time of purchase, or to be required as part of a routine compliance check, e.g., the address is still owned by an accredited investor. A practical example: If address ABC does not have an identity attestation token in their custody issued by an identity provider, then freeze the assets in their control, blocking any transactions of this asset or asset class until the attestation has been restored.

In Section 5, we outline solutions that we have designed to allow users with intermittent connectivity and without smartphones to be included on an entirely equal footing to users with good connectivity and smartphones, highlighting Algorand's focus on radical inclusivity for central bank digital currencies.

How to guarantee interoperability of the system

The hardest part of designing new financial infrastructure is developing the protocols and processes in a robust and resilient way that is compatible not just with legacy systems but also with future requirements. In the ecosystem view adopted by Algorand, this work is front-loaded and has informed the fundamental design of our open-source blockchain technology. Algorand's "openness-by-design" architecture creates an ecosystem where the protocol facilitates the seamless interaction of various ecosystem partners (banks, e-money companies, payment providers, etc.).

Consequently, we have front-loaded the hard work of creating protocols and processes to allow a diverse set of ecosystem players to interact without any one party's ability to create barriers to entry. This is vastly different from other approaches, notably by consulting firms and the Diem Association (formerly Facebook's Libra Association), who effectively make walled gardens. A "walled garden" is defined by technopedia as *"[...] a limited set of technology or media information provided to users with the intention of creating a monopoly or secure information system."*[5] Algorand has created an open platform that prevents capture by any private actor while giving central banks and government agencies full control over which users and use cases are allowed on the platform.

How to incentivize competition

The rise of private digital assets has set off a flurry of innovation among small startups, large banks, and big tech companies alike. Within Algorand's first year, the rapidly growing ecosystem had over 500 organizations join the tens of thousands of companies innovating in the broader digital asset space. A lot of this innovation, however, happens outside of the purview of existing regulatory bodies. Consequently, billions of euros worth of transactions are happening outside of official sight, and then settled to fiat. An official state-sponsored digital currency can allow much more of this digital innovation to happen "in the light of day."

To foster competition, an open system without barriers to entry is paramount. No walled garden solution can achieve this because, in such solutions, a provider can never commit not to create barriers to entry further down the line. The rules of a walled garden can be modified at any time by the solution provider. Algorand's open protocol enforced by decentralized validation ensures that any system built on our platform will always incentivize competition while curbing regulatory arbitrage. Only the collective wills of the authorized parties can choose to alter the rules of the system once established.

Lastly, creating a CBDC creates a more level playing field between traditional financial institutions and big tech companies. The BIS Report "Big tech in finance: opportunities and risks" outlines the challenge big tech companies pose to existing

[5] See https://www.techopedia.com/definition/2541/walled-garden-technology

financial institutions in an increasingly digital economy.[6] Big tech companies have a massive advantage over traditional financial institutions, and this advantage can translate into cheaper services outside existing regulatory frameworks. A CBDC will enable financial institutions to innovate more rapidly and compete on a more level playing field with the big tech companies.

3. ECONOMIC CONSIDERATIONS WHEN ISSUING CBDC

Balance Sheet Dynamics when Interbank Loans are Repaid Using a Real-Time Gross Settlement System

Before turning to the balance sheet implications when issuing a retail CBDC, it is instructive to look at the balance sheet of a simple economy when interbank transactions are settled via an RTGS system. One such method is shown in Figure 3-1, where we show the balance sheet for a central bank and two commercial banks explicitly. For simple interbank transactions, the balance sheet of firms, households, and the government are not affected and hence are omitted by us. Commercial banks have access to central bank reserves M, typically made available through open market operations, and Banks 1 and 2 hold reserves R1 and R2 with the central bank, respectively. We start our description when Bank 1 has already issued an interbank loan I to Bank 2, which Bank 2 intends to repay using the RTGS system.

Figure 3-2 shows the interbank loan I's actual repayment from Bank 2 to Bank 1. This reduces the interbank liability on Bank 2's balance sheet. This is only possible if an item on the asset side is reduced (or Bank 2 substitutes funding on the liability side, but in our example, this is not possible as there are no other sources of funding). The only available items are the reserves Bank 2 holds with the central bank. These are transferred by the central bank, which operates the RTGS system to Bank 1. Lastly, Bank 1's balance sheet has a reduced interbank asset position, which is compensated for by an increased reserve position with the central bank.

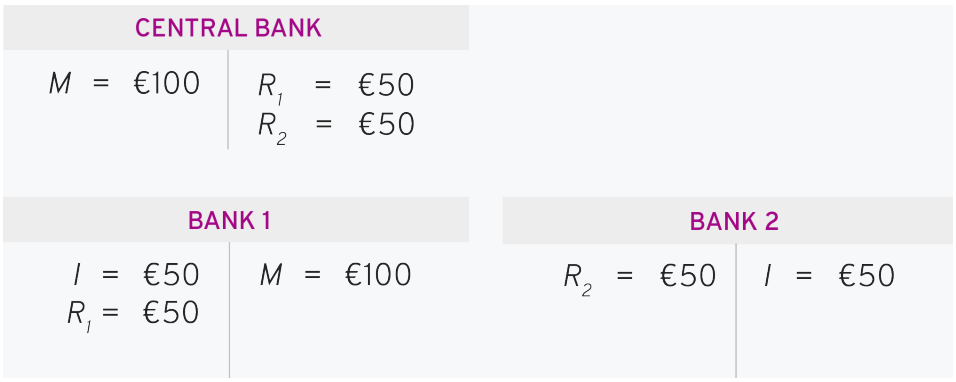


Figure 3-1: *A sample economy with a central bank and two commercial banks before the existing interbank loan I is repaid by Bank 2.*

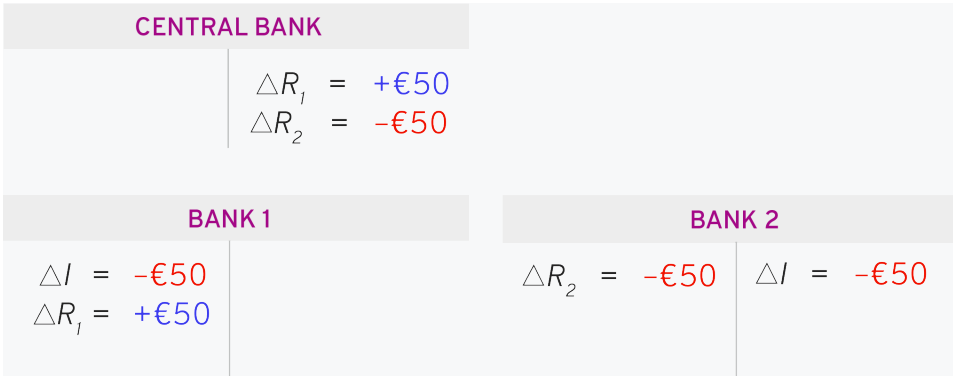


Figure 3-2: *A sample economy with a central bank and two commercial banks when Bank 2 repays the interbank loan to Bank 1. Using a RTGS system, this amounts to transferring reserves held at the central bank.*

Once all transactions are settled, Figure 3-3 shows the new balance sheet. Bank 1's balance sheet is as long as before, as is the central bank's, but the asset side's composition has shifted from interbank loans to reserves, which is reflected on the central bank's liability side.

[6] See https://www.bis.org/publ/arpdf/ar2019e3.htm

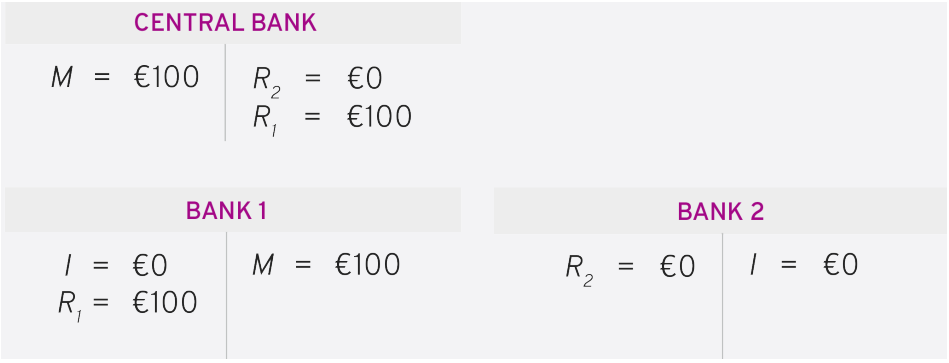


Figure 3-3: *A sample economy with a central bank and two commercial banks after Bank 2 has repaid the interbank loan to Bank 1.*

Balance Sheet Dynamics for Private Stablecoins

Next, we discuss how a private stablecoin would affect the balance sheet of the banking sector as a whole. For this, we now consolidate all banks in a banking sector entity. We introduce Libra as a dedicated entity and the non-bank sector (households, firms, and the government) as a reliable entity. Figure 3-4 shows the situation when Libra has launched and issued ΔC=50 units worth of tokens. Since a stablecoin would be pegged to, e.g., the euro, this amounts to EUR 50 worth of stable coin supply. These coins are demanded by the non-bank sector who uses existing deposits to pay for the coins. Hence, the issuance of coins amounts to a transfer of deposits between the non-bank sector and Libra. This is reflected in the banking sector's balance sheet, where the swap of deposits is recorded.

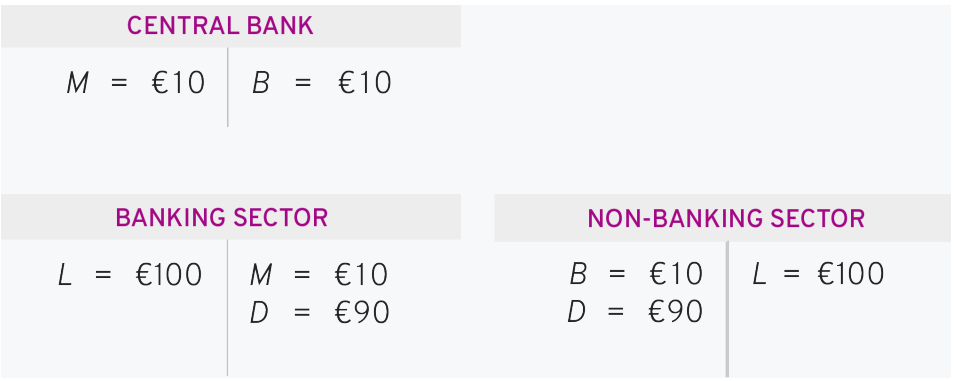


Figure 3-4: *A sample economy with a central bank, Libra, the Banking sector, and the Non-bank sector. The situation depicted shows the issuance of tokens by Libra.*

Stablecoins need to ensure that they are riskless to prevent "bank-run" such as scenarios where customers lose faith in the value of the stable coin and start running on it much as they would run on a bank. Therefore, the stablecoin must find highly-liquid and safe assets, such as government bonds. However, whenever Libra decides to reduce its deposit holdings and buy highly-liquid claims on the non-bank sector, this poses a risk for financial stability: when the deposit holdings are extensive, Libra could strongarm banks into selling their claims on the non-bank sector at a discount, incurring losses in the process. Thus, the issuance of coins would result in Libra holding considerable bargaining power towards the banking sector. When a sizable wholesale depositor like Libra decides to withdraw deposits, this could force banks into fire-sales and possibly trigger bank-runs.

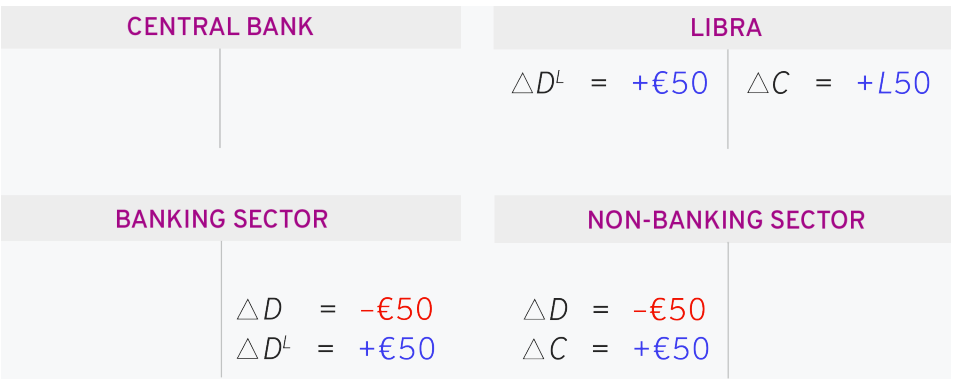


Figure 3-5: *A sample economy with a central bank, Libra, the Banking sector, and the Non-bank sector. The situation depicted shows what happens when the Non-bank sector decides to hold tokens.*

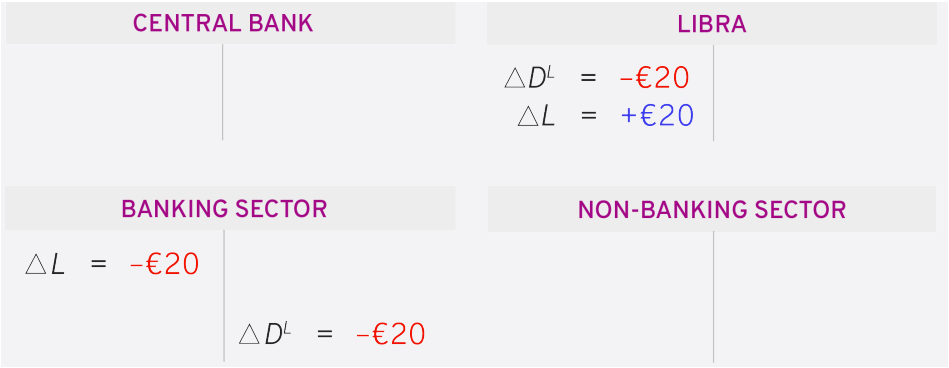


Figure 3-6: *A sample economy with a central bank, Libra, the Banking sector, and the Non-bank sector. The situation depicted shows what happens when Libra decides to reduce its deposit holdings and buy claims on the non-bank sector.*

The result of this dynamic is shown in Figure 3-6. The balance sheet of the Banking sector shrinks and there is disintermediation. At the same time, Libra would likely become a massive asset manager, depending on its tokens' demand. However, from a financial stability perspective, the banking sector's disintermediation might impair loan provision or even the monetary policy transmission channel's effectiveness. This is one of the reasons why central bankers have given private stablecoins only a lukewarm welcome.

Balance Sheet Dynamics for CBDC

The situation is different if the central bank issues the tokens directly in the form of a token-based retail CBDC. Figure 3-7 shows the status before the issuance of the CBDC. The central bank balance sheet also includes banknotes B, and the Banking sector has deposits D held by households, who finance their asset side, consisting of banknotes and deposits, with a loan from the Banking sector.

Figure 3-8 shows the issuance of tokens by the central bank. In this case, tokens are legal tender, and the EUR 20 worth of tokens have to be financed somehow. The central bank can now choose to offer additional funding to the banking sector in open market operations. However, the downside is that this would result in the central bank acquiring further claims on the Banking sector. Given that central banks carefully monitor individual banks' health and the entire system via micro-prudential supervision and macroprudential oversight, an existing framework is in place to manage these additional claims.

On the other hand, if the central bank decides to use the additional funds coming from the Non-bank sector to buy claims on the non-bank sector, this would be akin to the situation above, where the balance sheet of the Banking sector shrinks. The big difference now, though, is that the central bank is unlikely to use its additional bargaining power with the Banking sector when buying assets. Instead, the central bank can advise banks long in advance about its demand for private sector assets. This situation is shown in Figure 3-9. The central bank does not want to hold deposits, but if the Non-bank sector wants to buy CBDC, this might result in deposits being transferred to the central bank. To avoid such a situation, the central bank will then return the deposits to the banking sector, acquiring assets previously held by the Banking sector in return. This results in the central bank receiving claims on the non-bank sector. Traditionally, central banks do not hold claims on the non-bank sector on their balance sheet, but this might happen in exceptional circumstances. In this case, the central bank would have to have a policy for managing its non-bank sector assets portfolio.

Figure 3-7: *A sample economy with a central bank, the Banking sector, and the Non-bank sector. Depicted is the situation before the central bank issues a token-based CBDC.*

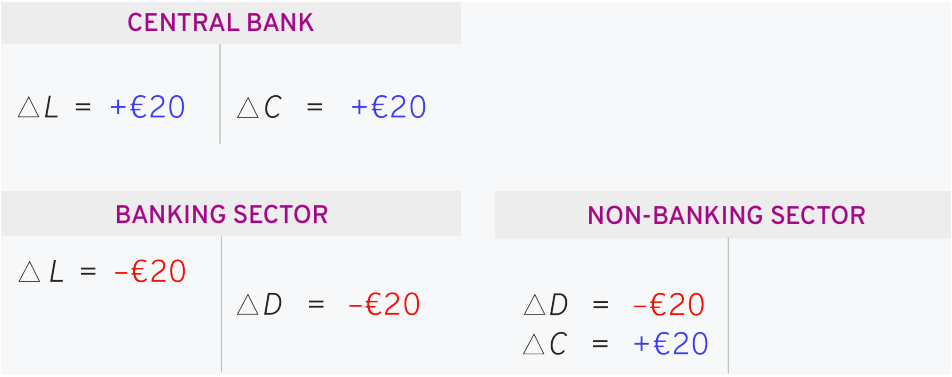


Figure 3-8: *A sample economy with a central bank, the Banking sector, and the Non-bank sector. Depicted is the situation after the central bank issues a token-based CBDC, which results in the central bank obtaining claims on the Banking sector via additional open market operations.*

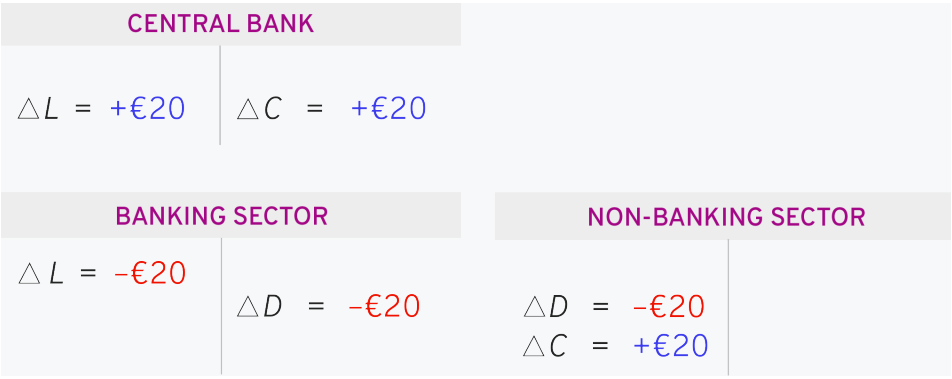


Figure 3-9: *A sample economy with a central bank, the Banking sector, and the Non-bank sector. Depicted is the situation after the central bank issues a token-based CBDC, which results in the central bank obtaining claims on the Non-bank sector instead of holding deposits.*

Monetary policy in a CBDC world

A growing body of theoretical literature has studied the impact of a retail CBDC on monetary policy. The lack of concrete implementations makes it difficult to define a CBDC model's standard features to be used as a baseline in a theoretical study. Hence, some of these works' conclusions may depend in part on the particular CBDC design assumptions made in that paper. In this section, we discuss some of the contributions of this literature and put them in relation to the main principles of the CBDC model we propose.

The first concern for central banking when a CBDC is issued is the effects on financial intermediation and banks' role in creating credit. Under a direct CBDC model, in which consumers can hold a deposit account with the central bank, central banks would compete with commercial banks for deposits. By subtracting deposits from private financial intermediaries, the introduction of a CBDC could jeopardize the maturity transformation process from deposits to loans traditionally conducted by private banks.

Fernandez-Villaverde et al. (2020) show that the set of investment allocations achieved under a CBDC regime in competition with commercial banks for deposits in normal no-panic conditions is equivalent to that under private financial intermediation. However, during a panic crisis, a credit system based on a CBDC offers more stability and deters runs. central banks would attract commercial banks' deposits, potentially dangerous for the banking sector and credit creation.

Brunnermeier and Niepelt (2019) also establish an equivalence result between monies with additional liquidity and payoff characteristics in terms of equilibrium allocations and prices. The introduction of a CBDC in their framework will not necessarily undermine credit provision or financial stability if the central bank accompanies the CBDC with an explicit commitment to serving as a lender of last resort and a pass-through policy for the substitution of bank funding via deposits by central bank funding. In this case, the central bank would act as a large depositor, eliminating the bad bank-run equilibria. By contrast, in a model with financially-constrained banks, Keister and Sanches (2019) show that CBDC crowds out bank deposits and introduces a liquidity premium on deposits. By increasing bank funding costs, CBDC would negatively affect the level of aggregate investment, although making the payment system more efficient and overall welfare higher.

Barrdear and Kumhof (2016) use a closed-economy Dynamic Stochastic General Equilibrium (DSGE) model in which a CBDC is introduced as a second monetary policy instrument. They show that a CBDC improves the central bank's ability to stabilize

the economy. Andolfatto (2018) uses an overlapping generations model instead to show that an interest-bearing CBDC does not necessarily lead to bank disintermediation. Still, banks will have to raise the rates paid on deposit to attract more deposits away from the CBDC. Finally, Gross and Schiller (2020) also study the disintermediation of the banking sector in a New Keynesian DSGE model, focusing on the interest rate policy of the CBDC and the interaction with the zero lower bound. They find that CBDCs crowd out bank deposits, but that a central bank can mitigate these effects by correcting the remuneration rate of CBDCs.

These results highlight the importance that broad architecture choices have for a successful implementation of a CBDC project. Limiting the disruption of the creation of bank deposits and bank credit and supporting investment and financial stability are key goals of any central bank. The CBDC model we propose guarantees the required flexibility to design and embed any supporting policy a central bank would need to achieve these goals. Moreover, our hybrid approach preserves a primary role for the banking sector in distributing CBDC and the daily management of retail CBDC activities, providing a direct and straightforward way to blend CBDC into the current financial and banking system.

The second strand of literature focuses on the international implications of CBDCs. Minesso Ferrari et al. (2010) introduced a CBDC in a two-country DSGE model. Their CBDC is a hybrid monetary asset used both as a means of payment and as a super-safe financial asset, which can pay a return, but it is not subject to any typical risk such as market risk or bank-run risk. The paper analyzes the transmission of shocks and optimal monetary policy in an economy with a CBDC with alternative designs. They define a modified UIP condition based on the CBDC remuneration rate and find two main results. First, the CBDC amplifies international linkages and the international transmission of shocks. Second, domestic CBDC reduces the autonomy of foreign monetary policy.

George et al. (2018) extend the work by Barrdear and Kumhof (2016) and study a small open economy DSGE model in which a CBDC is issued and used domestically, but not abroad. They focus on the welfare implications of a CBDC and the role of substitutability between CBDC and bank deposits. Their principal findings are that the overall welfare increases. The exchange rate is more stable when a CBDC with an adjustable remuneration rate is adopted, especially when foreign shocks are large. However, these gains depend on the degree of substitutability between bank deposits and CBDC.
Finally, Benigno et al. (2019) explore the effects of a privately-issued global cryptocurrency within a two-countries New Keynesian framework as well. They show that a worldwide cryptocurrency restricts monetary policy autonomy in each country by making monetary policy more synchronized. The classical Impossible Trinity (monetary policy autonomy, exchange rate flexibility, and financial openness) becomes even less reconcilable since monetary policies would ultimately lose their autonomy.

These results focus on the implications of two key aspects of the CBDC implementation in an open-economy setup: the flexibility of the return policy of a CBDC and its degree of substitutability with deposits. Potential benefits of a CBDC in an international context can come from the reduction of exchange rate volatility and welfare-improving effects. However, the main risk could be a loss in the autonomy of national monetary policy due to more substantial international spillovers. This area requires more analysis, especially to understand the implications of the introduction of multiple CBDCs simultaneously for the optimal design of a CBDC.

4. THE ALGORAND PROTOCOL

4.1 Background and Design Principles

Algorand is the brainchild of Turing, Gödel Prize, and RSA Prize winner Silvio Micali, a highly respected MIT professor, who helped invent many protocols that are the foundations of modern cryptography. He and a team of world-renowned cryptographers, technologists, researchers, and economists studied the first-generation blockchain. They found several shortcomings and stepped back to develop a blockchain that was purpose-built for both complex and simple financial applications — a next-generation blockchain that required no compromises on security, scalability, decentralization, or technical features, with advances in speed, reliability, and usability.

Algorand's Layer-1 general-purpose architecture enables ease of use and broad adoption with flexible governance. In common blockchain parlance, Layer-1 handles basic payments and the consensus protocol that ensures the validity of

those payments, while Layer 2 includes smart contracts and any other functionality not associated with the generation of new blocks. To increase compatibility, reduce security vulnerabilities, and advance the blockchain's efficiency, Algorand has chosen a different strategy - to implement key features, beyond block generation, in a high performing Layer-1.

Specifically, Algorand has implemented the creation of new assets (both fungible and non-fungible) and the execution of atomic transactions as Layer-1 primitives. Asset issuers can build their assets directly on these Layer-1 features instead of hand-coding their own. This design extends the world-class security audits and code reviews passed by Algorand's Layer-1 features to all assets issued on Algorand's platform. It also ensures that all third party asset issuers benefit from the same review and security testing as Algorand's native asset, thereby significantly reducing implementation effort and the errors associated with that work.

Issuers building their assets as Algorand Standard Asset (ASA) are assured their assets will be natively interoperable without the retooling of smart contracts, or the implementation of additional programming to ensure that balances are updated accordingly. Being implemented in Layer-1 ensures that if an application is designed to work with an Algorand Standard Asset it will work with all Algorand Standard Assets both past and future. Finally, implementation at Layer-1 enables Algorand to optimize performance in computation, storage and communication such that all ecosystem participants benefit from faster and cheaper transactions.

Algorand is purpose-built to enable sovereigns and enterprises to develier the next generation of financial products. A technology company dedicated to removing friction from financial exchange, Algorand is bridging the gap between legacy financial systems and the new OpenFi evolution by enabling the creation and exchange of value, building new financial tools and services, creating of new financial products, and providing responsible privacy models.

Algorand's approach provides less technical complexity, greater security, and fewer exploitable points between the applications and the platform, solving some of the most difficult real-world challenges. It is deployed today by corporations, governments, and nonprofits to create new financial offerings and business models that are re-inventing markets that otherwise wouldn't be possible.

4.2 The Algorand Protocol

The Algorand blockchain uses a decentralized Byzantine Agreement protocol that leverages pure proof-of-stake (Pure POS). This means that it can tolerate malicious users and achieve consensus without a central authority as long as a supermajority of the stake is in non-malicious hands. This protocol is very fast and requires minimal computational power per node, giving it the ability to finalize transactions efficiently.

The Algorand Consensus Protocol

Consensus refers to the way blocks are selected and written to the blockchain. Algorand uses a verifiable random function (VRF) described in our high-level documentation online to select leaders to propose blocks for a given round.[7] When a block is proposed to the blockchain, a committee of voters is selected to vote on the block proposal. If a majority of the votes are from honest participants, the block will be certified. What makes this algorithm Pure Proof-of-Stake is that members are chosen for these committees from the entire population of users, not some elite subset. Committees are made up of randomly selected accounts with voting power dependent on their online stake. Users with more tokens are more likely to be selected. This means higher stake accounts will most likely vote more often and participate more frequently in committees than accounts with less tokens. Using randomly selected committees allows the Algorand consensus protocol to have excellent performance while ensuring all users, even at world-scale, have a voice in the network's operations.

Consensus requires three steps to propose, confirm, and write the block to the blockchain. These steps are: 1) propose, 2) soft vote, and 3) certify vote. Each is described below, assuming the ideal case when there are no malicious users and the network is not partitioned (i.e., none of the network is down due to technical issues or from DDoS attacks). Note that all messages are cryptographically signed with the user's participation key and committee membership is verified using the VRF in these steps.

[7] See: https://developer.algorand.org/docs/algorand_consensus/

Block Proposal

In the block proposal phase, accounts are selected to propose new blocks to the network. This phase starts with every node in the network looping through each online account for which it has valid participation keys running Algorand's VRF to determine if the account is selected to propose the block. The VRF acts similarly to a weighted lottery where the number of Algos that the account has participated online determines the account's chance of being selected. Once an account is selected by the VRF, the node propagates the proposed block along with the VRF output, which proves that the account is a valid proposer. We then move from the proposed step to the soft vote step.

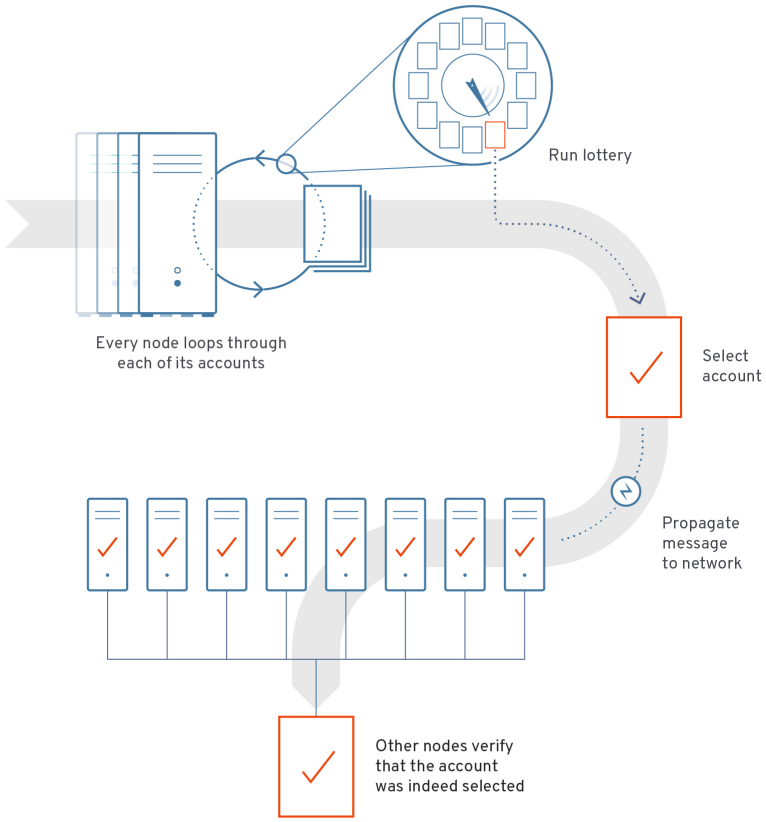
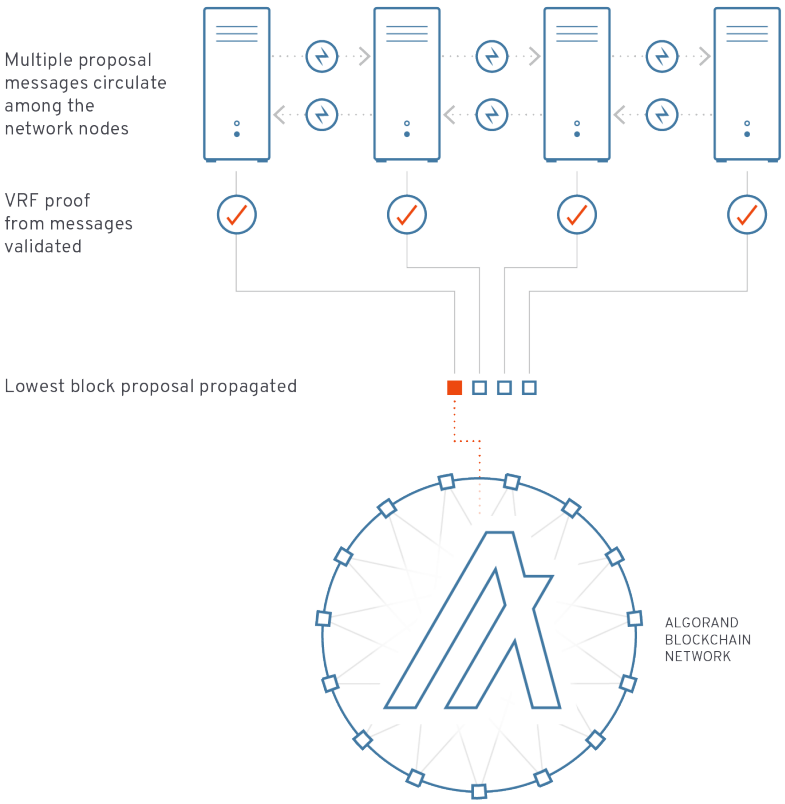


Figure 4-1: *Algorand block proposal.*

Source: https://developer.algorand.org/docs/algorand_consensus/

Soft Vote

The purpose of this phase is to filter the number of proposals down to one, guaranteeing that only one block gets certified. Each node in the network will get many proposal messages from other nodes. Nodes will verify the signature of the message and then validate the selection using the VRF proof. Next, the node will compare the hash from each validated winner's VRF proof to determine which is the lowest and will only propagate the block proposal with the lowest VRF hash. This process continues for a fixed amount of time to allow votes to be propagated across the network.



Each node will then run the VRF for every participating account it manages to see if they have been chosen to participate in the soft vote committee. If any account is chosen it will have a weighted vote based on the number of Algos the account has, and these votes will be propagated to the network. These votes will be for the lowest VRF block proposal calculated at the timeout and will be sent out to the other nodes along with the VRF Proof.

Figure 4-2: *Algorand soft vote Part 1.*
Source: https://developer.algorand.org/docs/algorand_consensus/

A new committee is selected for every step in the process and each step has a different committee size. This committee size is quantified in Algos. A quorum of votes is needed to move to the next step and must be a certain percentage of the expected committee size. These votes will be received from other nodes on the network and each node will validate the committee membership VRF proof before adding to the vote tally. Once a quorum is reached for the soft vote, the process moves to the certify vote step.

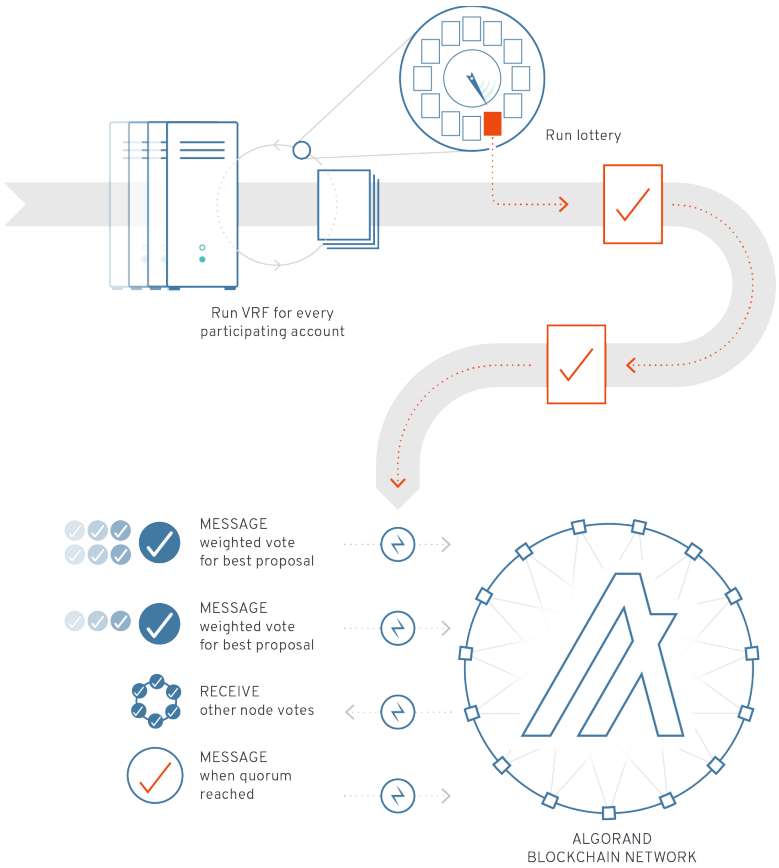


Figure 4-3: *Algorand soft vote Part 2*
Source: https://developer.algorand.org/docs/algorand_consensus/

Certify Vote

A new committee checks the block proposal that was voted on in the soft vote stage for overspending, double-spending, or any other problems. If valid, the new committee votes again to certify the block. This is done in a similar manner as the soft vote where each node iterates through its managed accounts to select a committee and to send votes. These votes are collected and validated by each node until a quorum is reached, triggering an end to the round and prompting the node to create a certificate for the block and write it to the ledger. At that point, a new round is initiated, and the process starts over.

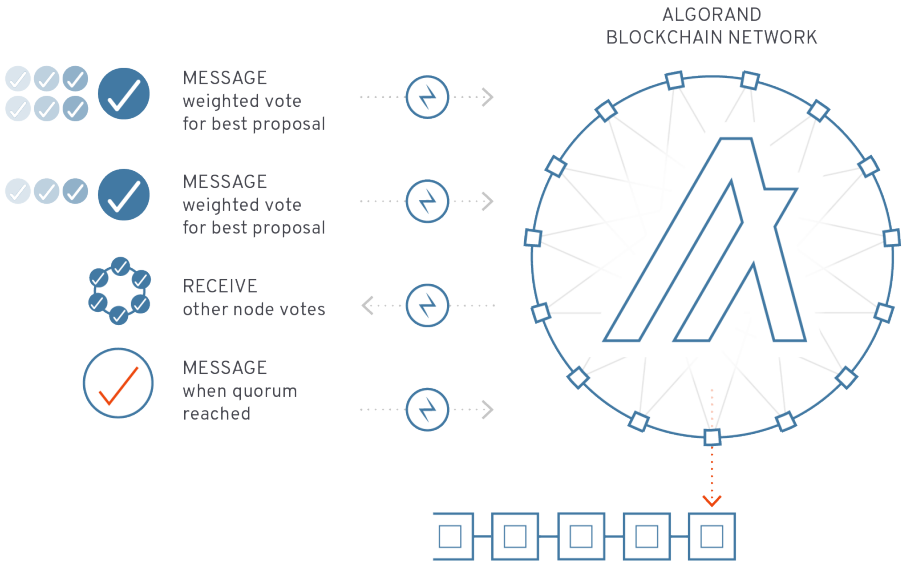


Figure 4-4: *Algorand certify vote*

Source: https://developer.algorand.org/docs/algorand_consensus/

5. ISSUING RETAIL CBDC WITH ALGORAND

We first turn to the opportunity of a retail CBDC issued using the Algorand protocol. We start this section by discussing a number of key design considerations for retail CBDC before turning to an extensive set of use cases Algorand has developed for this purpose. Most of these are discussed in detail in Appendix A, but we discuss the use cases of layered privacy and offline transactions in Section 5.2, given their importance for the success of retail CBDC projects.

5.1 Design Considerations for Retail CBDC

Taking the above design considerations into account, Algorand proposes a hybrid model built on a private instance of the Algorand blockchain: transactions occur on a decentralized ledger—the dedicated CBDC-Blockchain, as it will be called for this example—through electronic digital wallets in a two-tier retail system. The issuance and management of the CBDC will be fully controlled by the central bank, while distribution and transactions will be facilitated by Licensed Service Providers—including, but not limited to banks—and technology providers, respectively. Such a model would also encompass a situation where the central bank would issue the CBDC directly, i.e., without external licensed service providers. This could be done by creating a dedicated CBDC wallet and the supporting infrastructure. However, there are reputational concerns and most central banks will not have the capacity in house or the desire to issue CBDC directly.

A hybrid CBDC allows the central bank to delegate customer service responsibilities to dedicated and specialized organizations. While not envisaged as the normal mode of operation, in Algorand's model the central bank is also free to push currency directly to end-user wallets once end-users are onboarded. Bypassing financial intermediaries in this fashion can be advantageous to making monetary policy more effective during crises (e.g. natural disasters, financial crises) because money can be immediately given to consumers to stimulate the economy directly.

Algorand's CBDC is a retail digital token similar in characteristics and purpose to cash and private digital tokens, but issued and fully backed by the central bank as legal tender. In the "money flower" diagram of CBDC Types (Cœuré and Loh, 2018), which illustrates the position of the proposed model relative to other forms of physical and digital currency currently available to the public, the CBDC proposed by Algorand belongs to the subset "CB digital token (general purpose)". This positioning allows for a widely accessible, easy-to-manage currency that can be exchanged by consumers and businesses in a peer-to-peer fashion.

Compared to bank accounts, CBDC can reach a broader base of consumers, including those in the informal economy who might face difficulty in opening a traditional bank account and using digital services offered by banks. Compared to an account-based digital currency, it will be simpler and cheaper to roll out the CBDC on a blockchain and to manage retail transactions. The CBDC-Blockchain will hold end-user addresses, balances, and other details in an efficient and transparent manner as opposed to an account-based system controlled by financial institutions and their associated financial overheads.

Finally, Algorand's model will not destabilize existing systems because it will be working with them rather than against them. The Algorand CBDC model aims to fully integrate with the local payment system based on the national RTGS: it relies on the local RTGS to receive the payments necessary to issue the digital currency to service providers and the public. Algorand's CBDC design can also limit the risk of disintermediation of the bank sector. It includes the option to involve banks actively in the operational aspects of rolling out the currency and issue the CBDC against both ELT currency and cash.

Two-Tiered Distribution

Algorand proposes a two-tiered distribution model in which Licensed Service Providers—including banks — have two main functions:

1. Link end-users (i.e., consumers and businesses) and the central bank to facilitate and execute the issuance of CBDC: Licensed Service Providers will collect requests of CBDC from the public and use their accounts at the central bank and local RTGS to obtain CBDC in exchange for eligible forms of payments. Any form of payment is compatible with the model; we expect ELT through existing electronic funds transfer payment systems will be the most commonly used.

2. Provide gateway services to facilitate the distribution of CBDC to end-users: these services will include assistance in the activation and maintenance of digital wallets, identity verification, and know-your-customer procedures.

This type of solution reduces the burden that a central bank would face in a single-tier system where all the gateway services would have to be managed in-house by the central bank. It is also conveniently implemented within the already established local RTGS payment system because it fully relies on the same mechanism normally used by the central bank for its market interactions with the bank system.

The Algorand blockchain can accommodate both distribution systems. However, we see the two-tier model as preferable because it would not bypass the current central role the local RTGS plays in the payment system and easily includes banks in the distribution system. Working in a well-known framework enables higher efficiency and speed in the deployment of CBDC, and mitigates the impact of CBDC on the stability of the financial system.

A Token-Based Central Bank Digital Currency

The Algorand CBDC model is a token-based system leveraging the Algorand Standard Asset (ASA) atop the CBDC-Blockchain. In Section 4 we provide a full description of the blockchain itself. All users of this system will maintain control of their tokens via public and private key pairs. A user's public key identifies their wallet, which maintains that user's CBDC tokens. The private key, or spending key, enables the user to authorize transactions from their eWallet as payor to any valid payee in the system. The payee will be identified by their public key in the transfer transaction.

The way Algorand was built, ensures that CBDC tokens can never be minted or burned except by a specifically

authorized agency within the central bank following precise procedures. All users of the system other than a dedicated CBDC manager are able to transact freely according to the validation rules built into the CBDC token. Double spending and other erroneous or fraudulent transactions are impossible. Only well-formed transactions adhering to the rules of the system will be validated by the validators and permitted to go through. This design fundamentally facilitates the creation of trust in the new financial instrument, as does Algorand's immediate settlement finality.

A user may have any number of eWallets containing their supply of CBDC tokens. Onboarding into the system will be facilitated through authorized intermediaries, the Licensed Service Providers (LSPs). These LSPs are able to assist the user in the acquisition, installation, and setup of mobile wallet software and hardware. This includes mobile wallet software running on a smartphone such as an iPhone or a Google Android phone. Other devices and software may also exist, such as, but not limited to, feature phones and hardware wallets.

When issuing a CBDC, it is important to have designated partners who will assist existing financial services providers and the central bank with compliance verification, such as KYC/AML of the user, as appropriate for transacting with CBDC. If the user loses access to their device or to their signing keys, a LSP can also assist with the recovery process.

CBDC Issued as Legal Tender by the Central Bank Only

In the system envisioned by Algorand, the central bank will maintain full control of the issuing and management processes of the digital currency by interfacing directly with the CBDC-Blockchain. Therefore, the central bank will be the only entity with the authority to issue a legal tender and to expand or contract money supply. The CBDC will be issued exclusively by the central bank and "passed" to LSPs, which will be involved in managing individual users' accounts, distributing the CBDC to LSPs without access to the existing RTGS system, and distribution of the currency on the blockchain. This is particularly suitable in a situation where LSPs are both existing banks and new financial service providers.

The alternative scenario of banks and LSPs acting as issuing authorities (e.g. in a synthetic CBDC a la Adrian and Mancini-Griffoli (2019)) may limit the risk of disintermediation of the bank sector by involving the banks more directly in the creation of the CBDC, but it would make ensuring the effectiveness of the monetary policy decisions more difficult for the central bank because the control of the CBDC supply would be subject to banks' behavior. In some sense, it would be similar to a system in which banks issue private bank currency within the parameters specified by the central bank by using bank deposits to collateralize the issuance of CBDC. This type of solution could be implemented on traditional centralized digital platforms, however, and is not fully in the spirit of the DLT-based system proposed by Algorand.

From the technical perspective, the implementation of this alternative ("synthetic CBDC") system would be similar to the two-tier system Algorand proposes, but it would introduce an additional step requesting bank intercession in the distribution chain of the digital currency. We believe that a simpler model is preferable. Furthermore, the two-tier approach we propose is highly inclusive of the bank system.

CBDC Supply Limited As Determined by Applicable Monetary Policy

Ultimate control of the CBDC belongs to the central bank when deployed on the CBDC-Blockchain. The request for CBDC in the Algorand system relies on access to the national RTGS system on the central bank's authorization for release of the digital currency to the requestor. This access can be granted to banks and LSPs, or only to banks on behalf of an LSP that then connects to a bank in a two-tiered CBDC model.

All transactions and balances on the CBDC-Blockchain are visible to the central bank and other authorized entities. The central bank may limit the total quantity of CBDC to which LSPs have access based on information about those providers current holding or on a range of other factors.

CBDC holdings of individuals and businesses are easily monitored on the CBDC-Blockchain in a similar fashion. The central bank may use custom analytics or general purpose tools to inspect the disposition of CBDC balances and to impose limits and rules on individual wallets. A range of simple blockchain explorer tools exist that allow the central bank to search the full

blockchain transaction history. Differentiated policies, such as modulated interest rates or different maximum holdings per wallet, can also be implemented based on the amount of CBDC held in each wallet or on the level of AML clearance of an individual.

The Algorand blockchain allows central banks to inquire easily and to know the transaction history and current disposition of all CBDC held in any electronic wallet throughout the system. Smart contracts can be used to prevent transfers to a wallet exceeding a desired limit or to impose AML/CFT restrictions on specific individuals. The basic smart contracts provided by the Algorand blockchain under the name of Layer-1 Smart Contracts and the control options embedded in Algorand Standard Assets will be sufficient in their current form to support policy objectives.

Possibility of Issuing and Distributing CBDC to Commercial Banks Only, or to Commercial Banks as Well as to Licensed Service Providers.

The Algorand CBDC model does not require any Licensed Service Provider to have direct access to RTGS and central bank liquidity facilities in order to work. The architecture of our CBDC system allows for a staged deployment, and supports a partitioned system where transfer of CBDC from the central bank to the public end-users can be handled separately from CBDC interactions between end-users. The former mechanism can be independently designed and administered. Therefore, if desired or required by law, this issuance and distribution can easily be limited to banks only. It could be extended, gradually or rapidly, to other LSPs as the legal framework is updated.

Transactions between end-users occur directly on the Algorand blockchain. These are isolated and, therefore, are not impacted by additional mechanisms in place between the central bank and the end-user that are involved in CBDC distribution.

In our two-tier model, the issuance and distribution of new CBDC includes two steps:

1. Purchase of CBDC by end-users through LSPs: this first step requires integration with the local RTGS system.
2. Actual release of CBDC to end-users' wallets: this step takes place directly on the CBDC-Blockchain.

Restrictions to the access of CBDC facilities of the central bank can be easily imposed at step 1 of the process, as a license to operate in RTGS will be required. If a service provider cannot directly participate in the payment system, it will have to rely on a settling bank. In this case, the service provider will still be able to collect orders and payments from consumers and businesses and redirect them to the supporting bank.

Complementarity to Cash

In Algorand's system, CBDC is not expected or designed to fully replace cash. CBDC and cash can freely co-exist; they will always have equal value, and end-users can decide which type of currency to hold based on their own preference. The most common model will likely be the distribution of CBDC primarily as an exchange of electronic legal tender for CBDC as a conceptual device for explanation purposes. But, in our two-tier model, any qualifying form of payment could be accepted by the central bank to purchase CBDC.

As the CBDC is first introduced, consumers and businesses may prefer to use cash to purchase the digital currency. The central bank itself might want to impose explicit limitations on the types of accepted payments and restrict cash initially. However, other forms of value might be preferred by the central bank for exchanging to CBDC such as against bank accounts or government bonds. We could expect, then, at the initial phase of introduction, that CBDC would reduce cash holdings—for the benefit of increased deposit holdings— until a point of equilibrium between the two is achieved. This equilibrium will depend on the efficiency and cost-reduction in the payment system that CBDC achieves and on the ability of the bank sector to incorporate CBDC in the credit creation process.

CBDC as any other Central Bank Money from an Accounting Perspective

In Algorand's two-tier model, the central bank is the only entity able to issue CBDC, so it cannot be a liability of banks or of LSPs. CBDC is modeled from an accounting perspective exactly as any other type of central bank money, i.e., the same as central bank reserves and cash. The distribution of CBDC exclusively through authorized RTGS settling counterparties further guarantees this principle.

The release of CBDC by the central bank on the blockchain by means of the double-key system described in Appendix A also guarantees that nobody except the central bank will be able to issue any new currency. This principle, however, does not imply that banks or other financial intermediaries could not borrow CBDC from consumers and use it to supply credit, as is normally done with deposits. In this case, CBDC would technically classify as a liability for the bank, but in the form of standard borrowings.

Therefore, this principle has no particular impact on Algorand's system from a technical perspective. However, the decentralized nature of the Algorand blockchain has one particular advantage over any centralized ledger solution: with a centralized ledger (e.g., if the ledger is stored in a traditional database), the operator maintaining the ledger can change it at will, giving the operator the power to affect monetary policy by changing the supply of tokens. Thus, with such a solution, the central bank must maintain the ledger itself to retain control of monetary policy. In contrast, with Algorand's solution, the central bank remains the only authority able to control the token supply.

One-to-One Parity With Legal Tender

The two-tier system proposed by Algorand allows the central bank to fully control and set the conversion rate between CBDC and physical legal tender directly at the RTGS payment stage. The central bank enforces parity with legal tender as it is the sole entity empowered to "mint" and "burn" the CBDC supply (as it is true for the legal tender) and may do so in the appropriate fashion to ensure the one-to-one parity with the legal tender.

Orders of Magnitude Lower Fees or Free Transactions

The CBDC model proposed by Algorand includes very low transaction fees for end-users because it relies on Algorand blockchain technology. Currently, transaction fees are set at 1 milli-Algo per transaction on the Algorand MainNet (the equivalent of about half of a tenth of a cent of Euros at the August 2020 price of the Algo). The transaction fee will be denominated in CBDC legal tender on the CBDC-Blockchain but should be set similarly low. This transaction fee serves primarily to ensure the security of the CBDC-Blockchain from denial of service attacks. Similarly, the wallet app is freely available to people without any maintenance charge. Furthermore, transaction fees can be waived by the central bank in this permissioned Algorand blockchain environment, if desired.

In the distribution chain, banks could charge fees to final consumers to "load" CBDC to their eWallets. This is not a transaction cost per se, but it would affect the CBDC competitiveness. This service cost should be comparable to that of purchasing a rechargeable phone card, be built into the distribution authorization deal between the central bank and distributors, and driven down by competition among distributors.

Retail shops may charge additional fees for payments in CBDC, but this would not be due to any justifiable operational cost and would not be imposed by the CBDC-Blockchain. Such fees will be differentiated by the system from system-imposed fees. Fee padding by merchants will, therefore, be visible to the end user. This is an important difference from the POS-terminal fees usually charged by the conventional payment networks of credit and debit cards. In the Algorand blockchain, payments occur from wallet to wallet and are approved by the consensus protocol of the blockchain in a few seconds. Once a data connection is available, the only information required is the public address of the payee.

It is worth emphasizing that not only do merchants have negligible costs with a CBDC-Blockchain, but they also have no credit risk. In fact, in a payment system based on Algorand, all payees have no credit risk: everyone, including the payees themselves, can check that the payees got paid, with finality, within seconds of the payor authorizing the transaction.

Incentives to Promote the CBDC Use

The advantage of using a blockchain network to distribute CBDC to end-users instead of physically transferring cash to distribution points is highly significant in countries where the distribution system of cash is notably inefficient and expensive.

The solution proposed by Algorand is convenient in this respect. First, the cost of the technological infrastructure is relatively modest. Second, the two-tier model is designed to exploit the already-existing payment system of the local RTGS and the retail networks of multiple Licensed Service Providers. Third, there are negligible costs for end-users to manage their eWallets or fees related to the transaction activities.

Additionally, the open-system design of Algorand's approach positions the central bank to steward the CBDC while fostering open and inclusive innovation. Third parties can extend the features, power, and reach of this CBDC system, greatly increasing the currency's value with respect to traditional cash, and offering end-users services not previously accessible to them.

CBDC Ubiquity and Acceptance as Means of Payment by Businesses and Government

In the Algorand proposal, CBDC is a legal tender issued exclusively by the CB, and not by banks or any service provider. For this reason, it would be equivalent from a legal standpoint to any other form of currency in the country, and it must be accepted as a means of payment by all businesses, the government, and any other private user.

This CBDC, via the CBDC-Blockchain, will be easily and instantly available to all businesses and citizens across the nation, via freely available wallets that reside on users' smartphones, point-of-sale systems, computers, or even via low-cost hardware wallet fobs attached to users' keychains. Anyone with access to internet data may interact immediately with the CBDC-Blockchain through approved/authorized wallet software. The wallet software can make payments even where Internet access is asymmetric (e.g., only one party in an exchange has it). If no Internet is available, payments can be supported (with some restrictions) and cached until Internet data is available again. Given the importance of financial inclusion offline payments functionality is essential in the design of Algorand's CBDC-Blockchain

The CBDC-Blockchain, by its very nature as a highly decentralized and distributed pure-proof-of-stake system built on Algorand technology, will be incredibly robust and resilient to outages.

Algorand's CBDC Avoids Destabilization of the Financial Sector Risk and Provides Mechanisms for the Central Bank to Control CBDC Supply and Movement.

The risk of disintermediation of the bank sector due to a run to the CBDC can reduce the bank system's ability to provide credit to the economy. In the Algorand baseline model, CBDC is obtained directly in exchange for electronic legal tender from consumers. However, banks will maintain access to central bank reserves and their ability to offer deposits to consumers. So, the question of whether the demand for deposits remains the same is of primary importance.

The solution to this problem entails making deposits relatively more attractive than CBDC. There are a few options to achieve this goal. One option is for banks to increase the interest paid on deposits. Although feasible, this would decrease banks' profitability, with a potential destabilization of the bank system. A second option is a hard restriction on the convertibility of deposits to CBDC, with the central bank keeping CBDC facilities and reserves distinct and not convertible into each other, as proposed by Kumhof and Noone (2018). Although also feasible, this would introduce an artificial barrier between different forms of central bank money.

The third, in the case of the CBDC-Blockchain purely hypothetical option (given that CBDC shall be issued on par with ELT without interest), following a proposal by Bindseil (2020), is based on a two-tier remuneration system for CBDC holdings. In this model, a higher remuneration rate, r_1, is paid on small size CBDC holdings below a certain threshold set by the CB. A second remuneration rate, $r_2 < r_1$, would be paid on larger CBDC holdings in order to disincentivize consumers to convert large amounts of fiat currency into CBDC. Specifically, setting r_2 below the return rate paid on bank deposits—for instance, setting $r_2 < 0$—would also set the right incentives to avoid large flows of funds from bank deposits into CBDC. This case would also be perfectly consistent with an $r_1 = 0$, which implies no actual interest rate attached to the CBDC.

All options outlined above are easily implementable within Algorand's CBDC system. The Algorand blockchain already provides all the functionality necessary to implement the suggested solution. The opportunity to monitor eWallets and set thresholds for different remuneration rates is supported by Layer-1 Smart Contracts and can be easily embedded in the setup of an Algorand Standard Asset.

Enabling Innovation in Payments

The Algorand CBDC solution is based on an open-source distributed ledger infrastructure, which strongly supports and facilitates the development of decentralized applications (DApps) on the blockchain. Blockchain technology is ideal for the creation of a bottom-up ecosystem, where innovation is fostered by the network itself and by the participants in the ecosystem.

A large ecosystem of developers, applications, and innovative ideas are already focusing on using Algorand blockchain technology. They are using Algorand Standard Assets to model real-world, economic, and virtual assets in the blockchain space, and leveraging Layer-1 Smart Contracts to give these assets capabilities that do not require third-party intermediaries with their associated fees.

Extensive development support via online documentation and examples greatly facilitates onboarding of innovators and decreases time-to-market of their ideas. These solutions can be supported without any compromise to the CB's authority over the CBDC itself.

5.2 Examples of Use Cases for Retail CBDC Issued with Algorand

Spotlight: Issuing a CBDC When Connectivity is Limited

Blockchain technology, especially when built on Algorand's platform, is exceptionally resilient. If even one party in a transaction has connectivity, the transaction can safely go through. This is possible because the party with connectivity can act as a relay for the one without. Algorand messages and proofs are impossible to forge so if a properly signed transaction makes it into a block, the proof of that inclusion can be shown to the party without connectivity and be convincing, and goods or service can then be exchanged with complete trust.

When we are talking about disconnected, we mean truly offline - that is, neither party has a real-time connection back to the blockchain. The Algorand blockchain that the CBDC is built on acts as the trust mediator for all transactions. In the offline scenario, we need a replacement for this role. One approach we follow is to use Secure Hardware Enclaves built into most modern phones to stand in for the blockchain. It can vouch for the validity of a transaction and verify proof of sufficient funds when the wallet is offline.

The user of the CBDC would have a special offline account that is created for them by their wallet. This is in parallel to their regular online account. The user is in complete control of their regular online account. They can spend from it freely, add to its balance, and export the key so that that account can be used on other devices.

The offline account, however, is controlled only by the secure hardware on their wallet device (the mobile phone, a smart payment card, and a secure Universal Access Device as described in the interesting proposal of Barresi, Zatti (2020)). While connectivity exists, the wallet hardware will ensure some of the user's total account balance is in this special offline account as per the user's settings. For example, the user may have 1000 Euros in their normal account but have specified 250 Euros should be available even if connectivity does not exist. While the wallet is connected it will move 250 Euros from the user's account into this special hardware managed account. From the user's perspective, while online, they have all 1000 Euros and are free to spend it as they please.

When connectivity is lost and with it access to their main account on the blockchain, the user will still have access to the 250 Euros maintained by the secure hardware of the wallet.

In normal online usage the user signs his transaction to enable a payment and the validators on the blockchain will accept the payment after checking that enough balance exists in the user's account.

In the offline scenario the secure hardware will fulfill these roles and then signs the transaction with a special vendor key maintained by the secure hardware and completely inaccessible to the user. Any wallet in the CBDC system will know to accept this vendor signature as valid because it is coming from tamper proof hardware. A QR code or NFC would be enough to show proof of payment to the other party.

When either party has connectivity restored the transaction generated by the secure wallet will be reconciled with the blockchain using the usual rules. Double spending continues to be impossible. Value can never be created or destroyed in the CBDC except by itself using the central bank's special mint and burn transactions. These actions would typically only be used for economic control and require special privileges.

The secure hardware, as mentioned earlier, could be a smart phone. These are often expensive and may not be available to all. Algorand partners have expertise in the secure payment domain, however, and can create special smart payment cards at volume capable of operating in this role for around one Euro per device.

Spotlight: Privacy for Low-Value Transactions, Auditability for High-Value Transactions

Transaction traceability is already guaranteed in our blockchain-based system because all transfers are attributed to Public Keys. A Public Key serves as a proxy identity, however, and is not sufficient to identify the real world individual behind that key.

The Algorand platform's identity system is designed with flexibility in mind. We provide the essential primitives for the central bank to define nearly any identity and Privacy rules. Here is one system to give you an idea what is possible.

We can define three classes of scrutiny. These tiers can be based on transaction value, on a number of transactions in a certain amount of time, or on a variety of other details as defined by the central bank.

Let's imagine that all transactions over 2,000 Euros are subject to Direct Discovery, a process that allows for immediate and non-interactive revelation of the subject's real-work identity. The central bank and any other appropriate agencies, can inspect the transactor's identity at will. This would be our TIER 1 - High Value and Low Privacy.

For TIER 1 transactions discovery by the central bank is easy and automatic. Every such transaction will contain the encrypted real-world ID of the sender and receiver so the central bank can decrypt it at their leisure without involving any other parties.

TIER 2 contains the owners of transactions between 2,000 and 100 Euros. These must have their identity registered so regulatory agencies can request the identities if a situation arises that makes that relevant.

TIER 3 is low value and high privacy. Transactions below 100 Euros can be authorized by keys of this privilege. No identity registration is required at all. Only statistical discovery would be possible by analyzing the movement of money over time. We understand that users may be looking to avoid the scrutiny of higher TIER keys and their associated identity registration. TIER 3 can be designed such that structured payments are impossible so that bypassing the identity requirements cannot happen.

This is just one example of what an Identity and Privacy implementation can look like. The key point is that the Algorand CBDC provides a diverse set of low-level triggers, workflows, data, and controls so that nearly any Identity and Privacy system can be easily designed and implemented.

6. ISSUING WHOLESALE CBDC WITH ALGORAND

Algorand's approach to CBDC can also be easily adapted to accommodate a wholesale CBDC. We propose a wholesale CBDC model that leverages two of Algorand's strengths: CoChains and atomic swaps. The flexibility of Algorand's blockchain and its broad array of functionalities allows us to design a novel wholesale CBDC model which can coexist with, and not necessarily replace, any legacy RTGS system as well.

Design Overview

As for the retail case, the wholesale CBDC is also implemented on an Algorand CoChain, a permissioned instance of the Algorand blockchain platform. The digital representation of the currency will leverage the Algorand Standard Asset (ASA) functionality for easy, fast, and secure tokenization without the complexity of smart contracts. Algorand's blockchain technology uses a novel consensus algorithm based on pure proof-of-stake that is capable of global-scale performance, is competitive with centralised solutions, and provides safety, security, and resilience that only can come from a truly decentralized system. Algorand's network achieves the scalability necessary for a wholesale application.

The wholesale CBDC is created using advanced cryptographic principles such as multi-signature signing and authorization. These will ensure that the currency supply is always safeguarded at rest in the CBDC Vault and in transit during transactions. Additionally, because ASAs support powerful, role-based asset controls (including the ability to freeze assets, reverse transactions, and, of course, increase and decrease CBDC supply), a central bank is allowed to maintain full control of the CBDC and to ensure compliance with all prevailing regulations.

In the wholesale CBDC model, the participants in the national RTGS system are allowed to request and receive CBDC from the central bank and submit payments via the RTGS in exchange for CBDC. The central bank is able to execute transfers of CBDC immediately and directly to any entity in the CBDC CoChain, upon verification of the availability of the funds required by the payment. Algorand's blockchain transactions then take less than five seconds to finalize.

Any transaction made with CBDC on the CBDC CoChain is secured with advanced cryptography and duplicated redundantly by all the Nodes. Commercial banks do not hold CBDC themselves. They do hold the Private Spending Key of their respective Vault addresses. The Private Spending Keys can authorize transfers out of a bank's Vault address. Banks typically would use the wholesale CBDC to settle payments in security purchases and to post collaterals. True atomic swaps on the Algorand blockchain guarantee immediate finality of these transactions, regardless of the complexity and number of parties involved in an operation. But these are not the only use cases for our wholesale CBDC. The openness of Algorand's blockchain will allow the participants of the CBDC ecosystem to foster innovation by creating new financial products and services.

Wholesale CBDC for Security Settlements when Asset Digitalization Is Available

The main wholesale CBDC we propose can be characterized as a digital counterpart of a typical security trading system supported by a central bank. The CBDC is deployed on a CoChain of the Algorand platform where digital assets are created and also traded. Both payments in CBDC for the assets and settlements are fully finalized on the CoChain.

Digital assets are created through the Algorand Standard Asset (ASA) functionality. This type of digital asset can be a digital representation of a non-digital security or simply a digital asset originally created on the CoChain. For example, a digital asset could be a dematerialization of a physical asset implemented by a bank with the support of a Digital Security Depository (DSD), a service provider similar to a Central Security Depository (CSD), which arranges for the immobilization of the physical asset and also provides custody and key management services of the newly created digital asset.

Once a deal for the sale of the asset is reached between a seller bank and a buyer bank, the trade is ready for execution on the CoChain via an atomic swap transaction. The payment leg of the transaction is made in CBDC. Simultaneously, the digital asset is transferred from the seller's wallet to that of the buyer. This is the settlement leg of the transaction.

As banks participating in the digital security market use their RTGS Cash accounts to obtain the wholesale CBDC necessary to support their trades, exchanges are possible and finalized only if funds to pay for the digital assets are available in the buyer's wallet. Therefore, settlement is immediately guaranteed. The request for funds to cover asset purchases can be made in real-time as well, which is made possible by the technology of the Algorand blockchain and the rapidity of its consensus protocol which does not materially increase the time of execution of RTGS operations.

An interesting feature of our wholesale CBDC model is that pre-funded CBDC accounts on the blockchain would not force banks to use their liquidity to trade digital assets exclusively. Banks would be able to use the CBDC in their wallets in any other type of activity developed by the blockchain ecosystem as well, such as the creation of new financial services and products.

Wholesale CBDC for Security Settlements when Asset Digitalization Is Not Available

The Algorand wholesale CBDC model can easily accommodate a security exchange system in which the digitalization of listed assets is not possible. In this case, a seamless integration with a central bank's RTGS system for the settlement of security purchases would enhance the utility of Algorand's blockchain network as a payment infrastructure and support this kind of application. At the same time, banks would still have the opportunity to benefit from the adoption of the CBDC and from participation in the CBDC blockchain ecosystem.

The main feature of this solution is the creation of a new payment channel for security trading, powered by an instance of the Algorand blockchain. The wholesale CBDC is issued on this CoChain and banks hold their CBDC wallets on it. Digital wallets are used to receive CBDC from the central bank, and must be directly backed by a Cash Account at the national RTGS. Banks can then use their CBDC to make and receive payments when securities are purchased.

In this model, banks have to rely on traditional CSDs for management of their assets, the settlement mechanism, and accounting purposes. The only new element is the integration of the CBDC-CoChain with a centralized central bank Security Account System, which will be shared between the national RTGS and the CoChain. In this case, the exchange is clearly not fully atomic because the payment has to be finalized first, and the delivery of the security follows immediately after that. However, the payment on the Algorand CoChain is nearly instantaneous given the speed of the Algorand consensus protocol, while the delivery follows the same mechanisms and guarantees currently in place with conventional systems.

Wholesale CBDC for International Payments

The wholesale CBDC model we propose can be extended to include international payments on the Forex markets as well. Two cases are of interest, which are defined by whether the foreign CBDC is implemented on the Algorand blockchain as a native Algorand Standard Asset or on a different platform.

Foreign CBDC implemented on Algorand as a native Standard Asset

Let's assume that two CBDCs are issued by two central banks on their respective CoChains. The two currencies are not formally on the same blockchain, but they share the same underlying implementation which makes the exchange simple to implement by using a cross-chain atomic swap. Atomic swaps are one of the standard tools provided by the Algorand blockchain. In a cross-chain swap, Algorand MainNet works as a bridge in the exchange, ensuring a seamless transition of the two CBDCs from one bank's wallet to the other's.

This type of solution can be easily seen as an equivalent digital form of the traditional forex market, but in which the role of intermediaries and dealers is largely downsized. The two parties involved in the currency exchange reach an agreement and trade directly with each other on the blockchain in a decentralized fashion. This approach, especially due to the use of atomic swaps, has clear advantages in terms of cost reduction, and currency and counterparty risk management.

It is important to also note that the Algorand blockchain protocol would fully preserve the rules and attributes of a CBDC created on an Algorand CoChain in all the cross-chain representations of the original CBDC crossing Algorand-powered chains. Algorand allows the issuer of an ASA to set management rules for the corresponding ASA-based tokens, and ensures that such rules are enforced across Algorand-powered chains. This feature preserves the CBDC status of a digital currency across chains as well.

Foreign CBDC implemented on a non-Algorand based platform

Although a non-Algorand native CBDC makes an atomic swap more complicated, Algorand technology still allows for an atomic swap between the two CBDCs with some small operational modification. The CBDCs continue to live on their respective blockchains; however, the ownership is transferred to new accounts across blockchains. This solution requires both banks to have an account on both blockchains. If the foreign CBDC is implemented on a platform that supports

a time lock and has at least one hashing function in common with Algorand, then it is possible to swap the CBDCs atomically using a Hashed Time Lock Contract (HTLC). Although technically more advanced, HTLC contracts remain cheaper than those in the current Forex market and preserve the advantages of a decentralized trading system.

International Securities Settlement

The model for international payments can support the international settlement of traded digital securities as well. The model exploits the flexibility and speed of blockchain technology, but also shares some common features with the traditional correspondent banking system.

Let's assume a foreign CBDC is implemented on a non-Algorand platform which allows institutions to hold other private digital assets in their wallets. The settlement of an international trade of a digital asset can be implemented thanks to an Intermediary Link which will provide the services necessary to execute and complete the asset transaction. The Intermediary is a financial institution which holds multiple wallets on multiple blockchains for multiple currencies. The Intermediary also needs to have access, directly or indirectly, to both the domestic and foreign RTGS systems in order to be able to obtain their respective CBDCs.

The Intermediary facilitates the flow of payments from one bank to the other, collecting funds in one currency on one CBDC blockchain and releasing them in the second currency on the other platform. The intermediary also manages the dematerialization of the digital asset and its migration from one platform to the other. Although the overall transaction comprises two separate legs, it can be completed almost atomically with minimal counterparty risk for the seller of the digital asset and no risk for the buyer. The counterparty risk is, however, mitigated by the role of the Intermediary, which introduces a buffer in the transaction and the use of CBDCs for the payments which eliminates the need for any collateralization because the exchange occurs only if the funds are already secured.

Benefits for Foreign Exchange Markets of the Algorand's wholesale CBDC model

Algorand's open-source pedigree will enable the participants in the wholesale CBDC network to build unprecedented, innovative third party payment products without compromising the authority of the central bank or the system's performance and safety. The current system of foreign exchange is expensive for participants, in no small part due to the correspondent banking system and the lack of competition for cross-border payment systems. In contrast, the decentralized nature of Algorand's protocol enables substantial cost reduction and efficiency gains, thanks to capabilities that are unique to Algorand's protocol.

Identified benefits include the following:

1. Elimination of the need for traditional Forex dealers. This allows us to reduce the cost of FX transactions significantly, especially for lower value transactions. A recent study by Hau et al. (2019) finds that Forex dealers typically charge fees as high as .5% of the amount of the transaction to their customers, with large traders paying only a few basis points and smaller traders paying very large fees. Atomic swaps and transactions on the Algorand CoChain can be offered to all customer banks at a cost easily an order of magnitude smaller than the traditional fees paid by large traders.

2. Elimination of counterparty risk. The Atomic transaction executed on the Algorand blockchain is immediately finalized. Delays in settlement are not necessary and counterparty risks are eliminated.

3. Truly Atomic transfers remove counterparty risk, reducing the need for collateral. Algorand blockchain mathematically guarantees no forking, ensuring payments are final as soon as they are posted on the blockchain. The combination of atomic swaps and instant settlement finality enable Algorand to transact seamlessly with other CBDCs issued on an Algorand CoChain. For CBDCs issued on other blockchain protocols, Algorand's hashed time lock design ensures easy interoperability.

4. Even in the use cases in which an Intermediary across blockchain is involved, the Intermediary will face only limited currency conversion risk when it consolidates its balance sheets to a single accounting unit. However, not every transaction will necessarily require international ELT transfers. This will lead to an overall strong reduction of settlement delays and costs associated with the SWIFT system.

5. Full control of the wholesale CBDC is present at any point in time. The Algorand protocol is highly secure and scalable (up to 1,000 transactions per second in a public permissionless setting – higher throughput with same-region permissioned servers). This guarantees that a central bank issuing a CBDC on an Algorand CoChain will retain full control of the CBDC at any point in time, while being able to support a realistically high volume of trades, including for interoperability with other CBDCs.

6. Quasi-instantaneous FX transactions. Settlement of payment-versus-payment transactions also becomes virtually instantaneous thanks to the speed of the consensus protocol of Algorand which purposes and adds new blocks to the chain in less than five seconds.

7. Innovation within the financial system. The time consuming, complex, and expensive process of cross-border transactions is greatly simplified and expedited, especially for low-value transactions, which will deepen the integration of international financial markets. Furthermore, Atomic Swaps eliminate counterparty risk in financial transactions, reducing collateral requirements and facilitating new use cases

Benefits for Security and Liquidity Markets of the Algorand's wholesale CBDC model

Similar benefits can be expected for security markets and trading. The main advantage of Algorand's proposed solutions is a further simplification of banks' liquidity and collateral management in a system that guarantees, at the same time, extremely rapid settlement finality and the elimination of counterparty risk.

A huge improvement over legacy current systems is that a CBDC blockchain allows banks to trade digital assets as well as take part in the development of the CoChain ecosystem. An interesting feature of our wholesale CBDC model is that pre-funded CBDC accounts on the blockchain would not force banks to use their liquidity to trade digital assets exclusively. Banks would be able to use the CBDC in their wallets in any other type of activity developed by the blockchain ecosystem as well, such as the creation of new financial services and products. This means the opportunity to both build and take advantage of innovative bank-to-bank financial services and products that increase market efficiency and participation.

For instance, CBDC funds could be used to provide interbank loans. Smart contracts, at the same time, simplify the design and execution of the loan contracts. Similarly, the use of escrow accounts combined with the use of time locks provided by Algorand's technology, would enable banks to set up smart contracts for auto-collateralization procedures. Banks would not have to re-balance their CBDC accounts on a daily basis either, as done with traditional cash accounts, and would enjoy more flexibility in the management of capital requirements for trade.

The CBDC-CoChain framework could also facilitate interbank lending of funds in CDBC without directly relying on the supply of funds from the central bank. Banks could normally borrow from each other and use ASAs as collateral if necessary. A three-way form of auto-collateralization could also be easily devised and implemented on the blockchain in a completely secure and final way by using a multi-party settlement. For example, a lender bank would commit to provide the buyer bank atomically with the CBDC necessary to complete the trade, while the buyer bank would deposit the purchased asset in an escrow time-locked account as a collateral for the borrowed funds. The asset would be released to the lender bank's wallet if the buyer bank failed to repay the loan in time. In conclusion, we could expect an overall simplification of the liquidity management for banks actively involved in asset trading.

We expect these and other enabled innovations to lead to an increase in market participation. Banks will be free to trade assets more frequently and at lower cost, especially smaller banks, and even with foreign counterparties operating on different blockchains. Service providers of international security trading will be able to rely on the functionalities enabled by Algorand's state-of-the-art technology to reduce the settlement delays and costs associated with the SWIFT system. Finally, we expect our solution to strongly mitigate, if not completely eliminate, counterparty risks for internationally traded securities.

Digital assets and financial innovation

As mentioned before, one of the main advantages of the Algorand's protocol is that it enables financial innovation. The Algorand protocol is fully interoperable with other blockchain platforms which makes it easy for international financial

market participants to design and create digital securities on top of a wholesale CBDC system. This will significantly increase the competitiveness of national market players, in particular with regards to foreign competitors from the rest of the world. Algorand's seamless integration with other less performative blockchains through time-locked hashes, Algorand Standard Assets, and Atomic Swaps are powerful building blocks for novel, fully compliant financial instruments.

7. CONCLUSION

The Algorand blockchain is powerful financial technology that enables central banks to issue both wholesale and retail CBDC seamlessly . Our open-systems design approach prevents vendor lock-in and facilitates financial innovation on a level playing field. In this whitepaper, we reflect on the experience Algorand had participating in various CBDC projects around the globe. The value proposition of retail CBDCs is to include the 1.7 billion unbanked people globally and facilitate cheaper, easier, and more convenient transactions than cash. For wholesale CBDCs, the value proposition is that a CBDC can offer significant cost savings for market participants. The quantum-resilient Algorand blockchain is the ideal platform to realize these savings.

We propose a hybrid CBDC model, built on a private instance of the public Algorand blockchain, in a two-tier retail system. Central banks will always have full control over the CBDC, while distribution and transactions can be facilitated by licensed service providers, such as commercial banks, remittance providers, and other fintech companies. A blockchain-based retail CBDC can reach a broad base of consumers, including those without a traditional bank account. We propose the creation of a retail digital asset similar in characteristics and purpose to cash, issued and fully backed by the central bank as a legal tender.

Our approach to designing CBDC is very different from enterprise blockchain providers, who aim to build a walled-garden and achieve vendor lock-in. Algorand is designed to have open APIs which facilitates competition and prevents vendor lock-in. We believe that this open systems approach is the best design to empower central banks globally to issue retail and wholesale CBDC on our best-in-class blockchain platform.

References

- Tobias Adrian and Tomasso Mancini-Griffoli, (2019) "The Rise of Digital Money", IMF Fintech Notes 19/01.
- Barresi, R. G., and Zatti, F., (2020) "The Importance of Where Central Bank Digital Currencies Are Custodied: Exploring the Need of a Universal Access Device" (mimeo)
- Ulrich Bindseil, "Tiered CBDC and the financial system", ECB Working Paper No. 2351, (2020)
- Eva Kasper "A Definition for Infrastructure - Characteristics and Their Impact on Firms Active in Infrastructure"; PhD Thesis, LMU Munich, (2015). Obtained from https://d-nb.info/1071370057/34 . Accessed 2020-10-22
- Andolfatto, D. (2018), "Assessing the impact of central bank digital currency on private banks." Federal Reserve Bank of St. Louis Working Papers, 2018-25.
- Benigno, P., L. M. Schilling, and H. Uhlig (2019), "Cryptocurrencies, currency competition, and the impossible trinity." NBER Working Papers, 26214.
- Barrdear, J., and M. Kumhof (2016), "The macroeconomics of central bank issued digital currencies." Bank of England working papers, 605.
- Brunnermeier, M. K., and D. Niepelt (2019), "On the equivalence of private and public money", Journal of Monetary Economics, 106, 27-41.
- Fernandez-Villaverde, J., D. Sanchez, L. Schilling, and H. Uhlig (2020), "Central Bank Digital Currency: Central Banking For All?" Mimeo.
- A. George, T. Xie, and J. Alba (2018), "Central bank digital currency with adjustable interest rate in small open economies". Mimeo.
- Gross, J., and J. Schiller (2020), "A model for central bank digital currencies: Do CBDCs disrupt the financial sector?" Mimeo.
- Hau, H., P. Hoffmann, S. Langfield, and Y. Timmer (2019), "Discriminatory Pricing of Over-the-Counter Derivatives," IMF Working Paper 19/100.
- Hartung, G., Rutter, K., and Stroemer, G., (2019) "A solution for managing high-quality liquid assets: How distributed ledger technology can benefit the securities lending market", Journal of Securities Operations & Custody, Vol. 11, No. 4, pp. 282-291.
- Keister, T., and D. R. Sanches (2019), "Should central banks issue digital currency?" Working Paper 19-26, Federal Reserve Bank of Philadelphia.
- Kumhof, M. and C. Noone(2018) "Central bank digital currencies - design principles and balance sheet implications", BoE WP No. 725.
- Minesso Ferrari, M., , A. Mehl, and L. Stracca (2020), "Central bank digital currency in an open economy," Mimeo.

Appendix A – Additional Use Cases for Retail CBDC Issued on Algorand's Permissioned Private Blockchain

In this section we provide additional details of use cases for retail central bank digital currency issued using Algorand's technology stack.

Use Case 1-1: A central bank Issues a token-based CBDC

Use case description:

1. **As the central bank, I wish to design and create token-based CBDC securely using a secure internal process and store the CBDC in my secure electronic vault prior to distribution**

The design, operation, and security of the CBDC touches on national sovereignty. Ensuring that central banks maintain their authority as the ultimate agent in the CBDC system is therefore paramount in the design of CBDC solutions.

Algorand's open permissioned implementation of decentralized ledger technology offers a system that ensures the greatest safeguards of a central bank's sovereign powers. In a centralized system, such as a permissioned database, the gatekeeper of that system owns the data under their purview by merit of their absolute control. If their database records balances representing CBDC, then that gatekeeper can bypass any safeguards over the disposition of the currency—whoever operates the database controls what it records. If the gatekeeper is a third party administering the system and not the central bank, then the central bank's authority over that system is no longer absolute.

Centralized systems compromise on many elements of system design, such as indelible transparency, resilience, and security. Centralized solutions are also walled-gardens with gatekeepers. The rationalization for this approach is a belief that real performance requires centralization. The decentralized Algorand consensus protocol at the heart of the Algorand blockchain platform is designed, however, so that performance is not sacrificed, and global-scale payment processing for millions of users is attainable, nullifying a centralized approach's advantage.

Because the Algorand system is decentralized, and therefore has no central gatekeeper, it enables native issuance of CBDC as a liability of- and fully controlled by the central bank. Furthermore, because the Algorand system is open by design, with a well documented and defined extensibility framework, it incentivizes innovative and competitive products to be built on top of the CBDC without jeopardizing the central bank's authority.

A decentralized system enables startups and industry incumbents to participate easily while maintaining the central bank's full functional control over the money supply and over access criteria for participants. A centralized, walled-garden approach greatly restricts the emergence of novel ideas.

Those with final authority (e.g. the Governors) can directly oversee the day-to-day activities of the CBDC or, alternatively, delegate some authority over specific tasks to trusted subordinates or external parties using fine-grained access control that modern decentralized ledgers like the Algorand protocol facilitate.

Other decisions at this first stage of the CBDC creation include determining the maximum possible CBDC amount and smallest possible denomination. In the CBDC-Blockchain, all possible digital currency is created ahead of time and then released from the CBDC Vault into circulation as needed.

Creating CBDC with Algorand consists of instantiating a supply of an Algorand Standard Asset (ASA) currency *type* called CBDC on a permissioned instance of the Algorand blockchain. This blockchain instance is maintained by designated authorities in the country of issuance, including the central bank and potentially a consortium of members from the financial services industry. The currency thus created has a direct representation on Layer-1 of the blockchain, the layer where the core operations of the blockchain are executed, and, thus, provides the highest degree of security on the chain. Algorand Standard Assets support role-based access control functionality which allows the central bank to delegate the different management responsibilities of the system. For example, the central bank may decide that CBDC supply is

managed by a particular group of people within the bank. The central bank could assign this role to a multisignature address that includes all the people they have entrusted with minting and burning powers. The CBDC based on ASAs supports several powerful roles out-of-the-box. These include:

- The option to quarantine individuals and their eWallets for investigative purposes;
- The ability to authorize a transfer or reverse a transfer of CBDC for any eWallet where legal or other regulations require it;
- The ability to whitelist specific user addresses (eWallets) allowing only these individuals to transact in the CBDC.

CBDC built on Algorand Standard Assets can have additional "smart money" features such as tiered AML requirements for different sized transactions. These can be added at creation time by attaching sophisticated Algorand Layer-1 Smart Contracts (ASC1) to the CBDC. Regulatory needs and policies governing CBDC will evolve over time. Algorand's flexible infrastructure supports the governing ASC1 smart contract for the currency to be updated at any time without taking the currency and payment system offline.

Once the asset class is created, currency can be minted: CBDC can be moved into the central bank CBDC Vault "pre-distribution" address for storage and future circulation at the discretion of the CB.

The central bank will create this CBDC Vault where tokens will be stored by creating a multi-signature account on the blockchain. This type of account is highly secure and impossible to access without proper authorization. Its principal defense wall utilizes the world-leading encryption technology of the Algorand blockchain itself.

The central bank sets the total amount of digital tokens that are originally minted, and immediately issues a token creation transaction on the blockchain which transfers the tokens to the Vault. The central bank can also withdraw CBDC from circulation and back to the central bank CBDC Vault as necessary by implementing an appropriate set of policy tools.

Creating the entire maximum amount of CBDC at this stage is a requirement of the ASA design. It does not imply that the full amount must be in circulation. Any CBDC tokens in the central bank CBDC Vault are considered out of circulation and all query APIs and dashboards will adjust accordingly. The Algorand Standard Asset supports 2^{64} maximum tokens. Some of the tokens will need to be reserved for fractions of a unit of fiat currency, e.g. Euro. If, for example, accounting requirements require one-tenth of a cent of a Euro , then the central bank would be allowed to set more than 18,400 Trillion Euros at origination.

Storage doesn't mean actual storage of the tokens. The blockchain holds those balances redundantly on all the Nodes. Storage means the transfer of "pre-distribution" and "out-of-circulation" CBDC to the central bank CBDC Vault address. Storage has an operational component to it: protection of the Private Signing Keys that can create central bank CBDC Vault transactions. The central bank CBDC Vault Private Signing Keys may authorize transfers out of the central bank CBDC Vault. Their physical and operational security is paramount to ensuring that only appropriate transfers are created and signed.

The central bank will decide how to devolve authority in order to move currency into this Vault and out of it into circulation. For instance, it may choose to give authorization to the Governor and all Deputy Governors working in concert or to a quorum of them. This includes transactions such as adjusting supply of tokens in circulation according to the prevailing monetary policy stance. The Appendix describes the operational strategies related to central bank CBDC Vault key-management and its related technology in greater detail.

Once in the Vault, the CBDC can be released to the public over time according to the requests received by the central bank and the policy rules decided by the central bank.

Use Case 2-1: Distribute token-based CBDC to licensed entities

Use case description:

1. **As a commercial bank, I wish to order CBDC from the central bank and pay for it via the existing RTGS system.**
2. **As a licensed service provider, I wish to order CBDC from the central bank and pay for it via the existing RTGS system or via my sponsoring RTGS settlement bank.**

3. **As the central bank, I wish to transfer ownership of the CBDC ordered by commercial banks and/or licensed service providers to these entities as soon as payment has been received in the RTGS system.**

4. **As a commercial bank or licensed service provider, I wish to securely store the CBDC received from the central bank in my electronic vault.**

We will discuss the four parts of the use case in turn below.

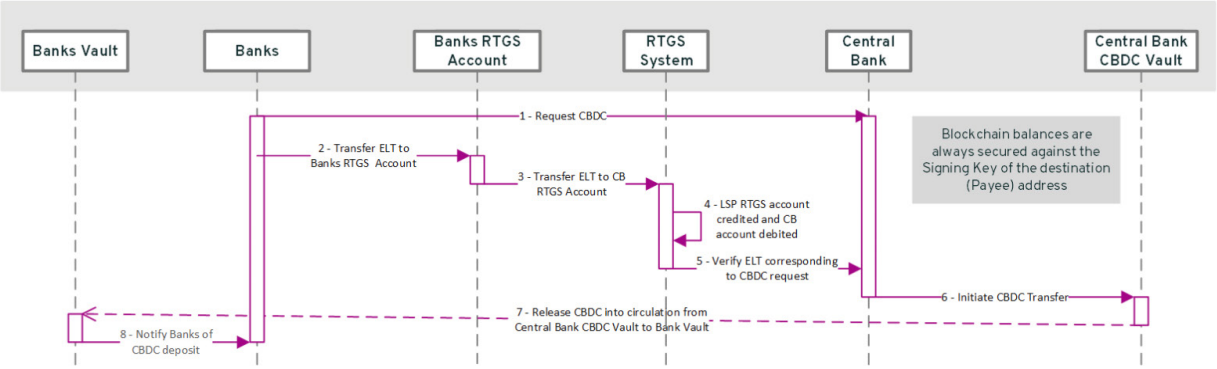


Figure UC2-1: *Sequence diagram for Use Case 2-1 (distribute a token-based CBDC to licensed entities).*

LSP: Licensed Service Provider role with access to RTGS system.
Banks: Existing Financial Institutions with access to RTGS system.
LSP/Bank Vault: Blockchain address that holds LSP/Bank's CBDC.
RTGS System: Real Time Gross Settlement system.
Central Bank CBDC Vault: Blockchain user and associated address that holds "out-of-circulation" CBDC.
ELT: Electronic Legal Tender.

UC2-1.1 – As a commercial bank, I wish to order CBDC from the central bank and pay for it via the RTGS system.

Commercial Banks and Licensed Service Providers (LSP) with RTGS access are treated functionally the same in our proposed system. Both are able to request CBDC via the central bank dashboard and submit payments via RTGS to receive CBDC. If an LSP does not have or does not desire access to RTGS payment infrastructure, they may request CBDC through an LSP or Bank with RTGS access to act as an intermediary.

The solution proposed by Algorand to issue and distribute CBDC to the public will require adding a simple operative and communication framework based on the Algorand blockchain protocol, interfaced with the current RTGS payment system.

We detail in Figure UC2-1 an illustrative example for the case of a generic Licensed Service Provider (LSP), which could be the provider of the blockchain technology itself with a direct access channel to RTGS, an affiliated entity of the technology provider, or any pre-existing bank.

In the model we envision, users would obtain CBDC in exchange for electronic legal tender (ELT) through an electronic fund transfer (EFT), or in exchange for cash. These transactions would be intermediated by an LSP. Once the LSP receives an order, it would transmit it to the central bank, pay for the CBDC via RTGS, and trigger the distribution of CBDC on the Algorand blockchain to the LSP Vault address. All exchanges, CBDC to cash or CBDC to ELT, will follow the same principle and flow, outlined below: the amount of fiat and digital currency exchanged in each transaction is exactly the same, since a perfect parity between the two would exist.

"Request CBDC" will require a communication system between the LSP and central bank dashboards. It could be a simple internet API connection, or an encrypted system, or a reserved phone line if preferred. This has to be defined based on the preferences of the central bank. The "Transfer ELT to LSP RTGS" step will require the LSP to have access to the RTGS payment system according to the current legal framework. In particular, the LSP will need a Reserves account at the central bank and must be authorized to settle this type of transaction. In the current specification this is no problem, as banks are envisaged

as LSPs. Note that access to the RTGS account is purely for settlement purposes, and Algorand's proposed system does not require that the LSP would have access to the central bank's open market or other liquidity operations. However, the proposed solution also does not explicitly preclude this possibility and therefore complies with the terms set out in the RFP.

At this point, the LSP can transfer funds from its account to the central bank's account. The central bank verifies that the payment was correctly executed and finalized, and the central bank dashboard can then approve the order and initiate the CBDC transfer. The issuance then instructs the blockchain to release the CBDC from the central bank CBDC Vault to the LSP Vault and from there to the eWallets of the individual final users.

UC2-1.2 — LSPs order CBDC from central bank and pay for it via RTGS system directly or via sponsoring RTGS settlement bank

LSPs with an RTGS account follow the workflow precisely as described in UC2-1.1 and diagrammed in Figure UC2-1.

For LSPs without a RTGS account, an additional step is added on either end of this workflow. The LSP requests CBDC through a RTGS settlement bank where it has an account. The Bank transfers ELT from the LSP's bank account to the central bank RTGS account. The central bank verifies the ELT from the RTGS settlement bank and releases CBDC from the central bank CBDC Vault to the Bank Vault. The Bank then transfers CBDC to the LSP Vault on the central bank-CBDC-Blockchain.

The transfer of funds from the LSP to the Bank is net-settled from the Bank RTGS account to the same account assuming the LSP has a bank account with the settling Bank.

UC2-1.3 — The central bank transfers CBDC to LSP/Bank Vault

The solution proposed by Algorand to issue and distribute CBDC to the public will require adding a simple operative and communication framework based on the Algorand blockchain protocol, interfaced with the current RTGS payment system. These workflows complement the existing central bank and RTGS infrastructure.

We describe here an illustrative example for the case of a generic Licensed Service Provider (LSP), which could be the provider of the blockchain technology itself with a direct access channel to RTGS, to an affiliated entity of the technology provider, or to any pre-existing bank. This design allows the addition of licensed service providers who are not banks to the system, should this be desired. But the system would also be fully functional if only banks could be LSPs.

In the model we envision, users would obtain CBDC in exchange for ELT through an EFT, or in exchange for cash. These transactions would be intermediated by an LSP. Once the LSP receives an order, it would transmit it to the CB, pay for the CBDC via the RTGS system, and trigger the distribution of CBDC on the Algorand blockchain to the LSP Vault address. All exchanges, CBDC-to-cash or CBDC-to-ELT, will follow the same principle and flow, outlined below: the amount of fiat and digital currency exchanged in each transaction is exactly the same, due to the parity between them.

"Request CBDC" will require a solution provider to build a communication system between the LSP and central bank dashboards. It could be a simple internet API connection, or an encrypted system, or a reserved phone line if preferred. This has to be defined based on the preferences of the CB. The *"Transfer ELT to LSP RTGS"* step will require the LSP to have access to the RTGS payment system according to the current legal framework. In particular, the LSP will need a Reserves account at the central bank and must be authorized to settle this type of transaction. Note that access to the RTGS account is purely for settlement purposes and that Algorand's proposed system does not require that the LSP have access to the central bank's open market or other liquidity operations. However, our solution also does not explicitly preclude these possibilities.

At this point, the LSP can transfer funds from its account to the central bank's account. The central bank verifies that the payment was correctly executed and finalized and the central bank dashboard can then approve the order and initiate the CBDC transfer. With this step, the issuing flowchart moves into the blockchain for the release of the CBDC from the central bank CBDC Vault to the LSP Vault and from there to the eWallets of the individual final users.

UC2-1.4 — A LSP or bank securely store CBDC in their vault

As mentioned in UC1-1, storage doesn't necessarily mean storage of the actual tokens. The blockchain holds those balances redundantly on all the Nodes. Storage is the transfer of CBDC from the central bank CBDC Vault address to the LSP/Bank Vault address. This storage has an operational component to it and that is protection of the Private Signing Keys that can create LSP Vault transactions. The Licensed Service Providers Private Signing Keys may authorize transfers out of the LSP Vault. Their physical and operational security are paramount to ensuring that only appropriate transfers are created and signed.

Use Case 2-2: Distribute token-based CBDC to consumers and businesses

This use case can be summarized as:

1. As a consumer or business, with or without a bank account, I wish to obtain CBDC from a commercial bank or a licensed service provider and store it securely in my eWallet or my personal electronic vault held at the commercial bank or licensed service provider.
2. As a consumer or business, I wish to offer cash and/or transfer funds (via EFT) from my bank account in exchange for CBDC.
3. As a consumer, I want to be able to receive my social grant payments from the government in CBDC directly into my eWallet or into my personal electronic vault held at a commercial bank or licensed service provider.

The use case is depicted in Figure below.

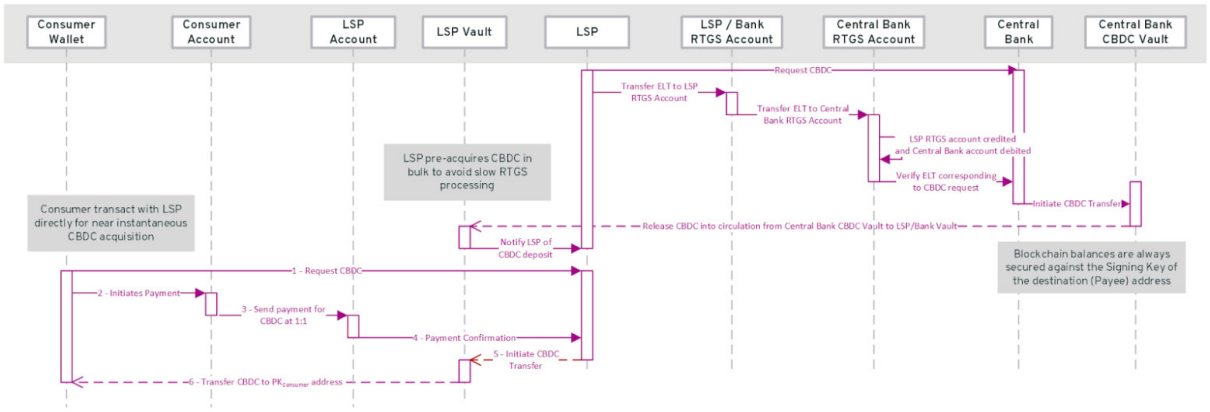


Figure UC2-2: *Sequence diagram of Use Case 2-2 (distribute a token-based CBDC to consumers and businesses).*

LSP: Licensed Service Provider role with access to RTGS system.
Banks: Existing Financial Institutions with access to RTGS system.
LSP/Bank Vault: Blockchain address that holds LSP/Bank's CBDC.
RTGS System: Real Time Gross Settlement system.
Central Bank CBDC Vault: Blockchain user and associated address that holds "out-of-circulation" CBDC.
ELT: Electronic Legal Tender.

UC2-2.1 — Consumer wishes to offer cash or EFT from my bank account for CBDC

The solution proposed by Algorand for the distribution of CBDC from the central bank Vault to end-user consumers and businesses is identical to the distribution of tokens to licensed based entities, UC2-1, with two primary extensions. The first extension is that the end-user has a communication and payment channel with the Licensed Service Provider to make CBDC requests and offer payments for the CBDC by e.g. cash and EFT. This payment is made 1:1 for the digital currency.

The second extension is that the end-user will receive their CBDC directly into their eWallet from the LSP Vault via the Algorand blockchain platform instead of via the central bank CBDC Vault. This is because many RTGS systems are high-value payment settlement systems that may not be optimized for instantaneous settlements of numerous low-value payments that are likely to come from end-users. The LSP may, therefore, acquire CBDC in bulk following the procedure already outlined in UC2-1 and fulfill these low-value requests directly. If an immediate low-value, high-volume settlement is available, the workflow can avoid a cache of CBDC in the LSP Vault and, instead, follow UC2-1 and settle with the RTGS system directly.

The key elements of the model we propose are as follows:

1. Any CBDC transaction involving final users (consumers and business) occurs on the private instance of the Algorand blockchain. As a service provider, Algorand facilitates the creation of eWallets for the final users through a simple phone app, which will be similar to the AlgoWallet app, called the CBDC-Wallet. KYC/AML, security, and identity/anonymity features as established by the central bank and other relevant regulatory authorities are embedded in this app. Other providers will be involved in the development of the wallet application as well as the necessary APIs, depending on local requirements.
2. Other providers with a capillary geographic network in the CBDC-issuing country, potentially including banks, can be involved in the operations related to the creation of the wallets. First, they could assist consumers onboarding into the system as necessary: creation of accounts and eWallets, identity verification, etc. Second, they could operate as terminals on the territory to facilitate CBDC requests from consumers and collect the payments in different forms to purchase the CBDC. As explained below, these payments are principally envisioned to be made by electronic transfers through the standard EFT system, but payments in other forms (including cash) for those consumers who don't have access to bank services are not excluded and Algorand has developed solutions in collaboration with a host of partners.

   Online orders, however, will be possible and probably the most common way to purchase new CBDC. In this case the payment would occur through credit card or existing banking channels. However, it could be fully implemented on the Algorand blockchain by allowing payments in crypto assets or other stable coins and CBDC that the central bank accepts into the central bank-CBDC-Blockchain platform as an asset.

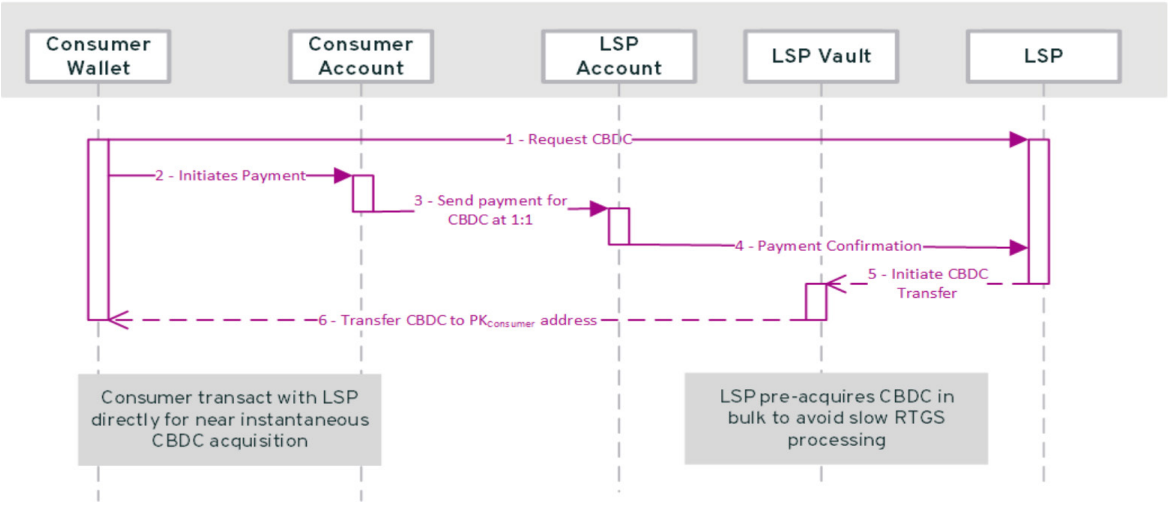


Figure UC2-2-focused: Sequence diagram of Use Case 2-2 (distribute a token-based CBDC to consumers and businesses) focused on a consumer requesting CBDC through LSP.

LSP: Licensed Service Provider role with access to RTGS system.
Banks: Existing Financial Institutions with access to RTGS system.
LSP/Bank Vault: Blockchain address that holds LSP/Bank's CBDC.
RTGS System: Real Time Gross Settlement system.
Central Bank CBDC Vault: Blockchain user and associated address that holds "out-of-circulation" CBDC.
ELT: Electronic Legal Tender.

The diagram above (Figure UC2-2–focused) illustrates the mechanism in play when a user, let's assume a Consumer, requests some CBDC through the LSP.

The Consumer uses a simple interface to place her order through the messaging communication system that connects the public to the LSP and the central bank dashboard. The interface could simply be integrated as a function in the same central bank-CBDC-Wallet application. At the same time, placing the order triggers the payment from the Consumer to the LSP. The interface is linked to a source of funds that the Consumer must provide and validate in advance, such as her bank account or PayPal account, from which the payment is withdrawn. The LSP account is then credited with the payment amount necessary to fulfill the order. This transfer of funds would occur via electronic legal tender.

As soon as a confirmation of the payment is received, the LSP initiates CBDC transfer from its own LSP Vault. The LSP Vault will transfer CBDC via the Algorand blockchain directly into the Consumer's Wallet.

It is important to reiterate the difference between the two layers involved in the distribution of the CBDC to the Consumer in this use case. The order of CBDC by the Consumer initiates two processes that take place in parallel on two independent channels. The first loop of effects entails traditional systems of payments such as the EFT, the ELT transfers, and the RTGS system payment system, which are all well-established mechanisms. The second loop of effects unfolds on the private instance of the Algorand blockchain, which represents a self-contained system but which will be fully integrated with and rely on the standard payment system. The messaging communication platform on the top of these two systems of effects works with their particular APIs and interfaces as a connecting junction between the different agents who must coordinate operations across multiple systems.

In principle, as briefly discussed above, the order and payment of CBDC by the Consumer could be completely realized on the private instance of the Algorand blockchain if the transfer of assets with different denominations is allowed. In this case, Consumer would "put" a standard asset with some recognized value onto the blockchain and a Smart Contract would allow Consumer and LSP to finalize a crypto-for-digital currency exchange. If the central bank CBDC-Blockchain is open only to central bank CBDC, Consumers could hold another wallet on the main Algorand blockchain, and the crypto-for-digital exchange could occur by Atomic Swap instead.

UC2-2.2 — Consumer obtains eWallet without a bank account

A Consumer can get onboard into the CBDC-Blockchain with minimal effort and resources. The only thing they require is a CBDC-Wallet issued from an authorized Wallet Provider. This Wallet may be software or hardware and will act as the Consumer's user-agent on the CBDC-Blockchain. Examples of these Wallets are iOS and Android applications which will be available to consumers. Additional Wallets can be web portals or even special purpose hardware wallets.

No bank account is required to gain access to a Wallet. Licensed Service Providers and Onboarding Partners can assist users with downloading and installing the mobile apps. They can also help with the initial and subsequent funding of the Wallets with CBDC by accepting cash or other payment methods and transferring CBDC to the users newly acquired Wallet.

UC2-2.3 — Receive social grants from government directly into eWallet

Government payments to a Wallet address are identical to any payment from one eWallet to another on the Algorand blockchain. Government entities would create and own a CBDC-Wallet and obtain CBDC from the central bank. Both these steps follow the procedures outlined in this use case: the government acquires CBDC via the RTGS system, possibly against an ELT transfer from the Treasury Department or against government bonds, and the government then transfers CBDC to consumers directly via blockchain. Once the government institutions have CBDC they will be able to transfer any Social Grant payments to a Consumer's registered CBDC-Wallet address as a normal transfer transaction.

Use Case 3-1: Transact in token-based CBDC using online channels

One of the most common use cases is the transaction of token-based CBDC using online channels. In more detail:

1. As a consumer or business, I wish to transact in CBDC with other consumers and/or businesses using online real-time channels provided by commercial banks or licensed service providers.
2. As a commercial bank or licensed service provider, I want to ensure interoperability with my counterparts in order to facilitate real-time transfer of value in CBDC between our respective customers.
3. As a consumer without a bank account, I wish to transact in CBDC with other consumers (with or without bank accounts) as well as with businesses.
4. As a consumer, I wish to freely exchange my CBDC for cash or, if I have a bank account, for commercial bank money (EFT).

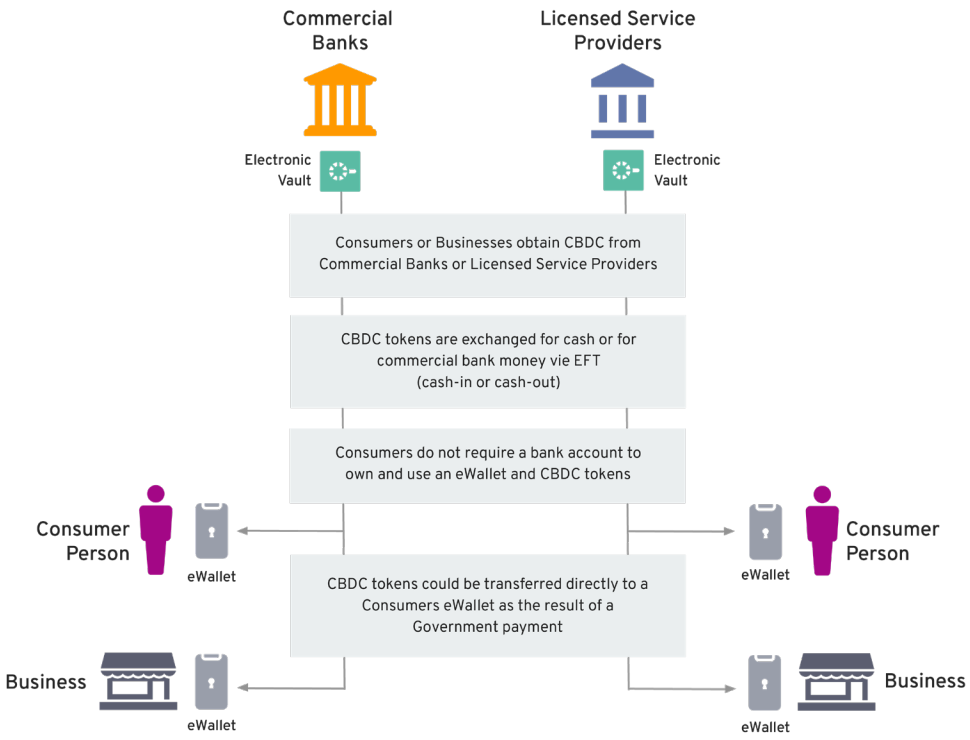


Figure UC3-1–***Schema**: Depiction of Use Case 3-1 (Transaction in token-based CBDC using online channels)*

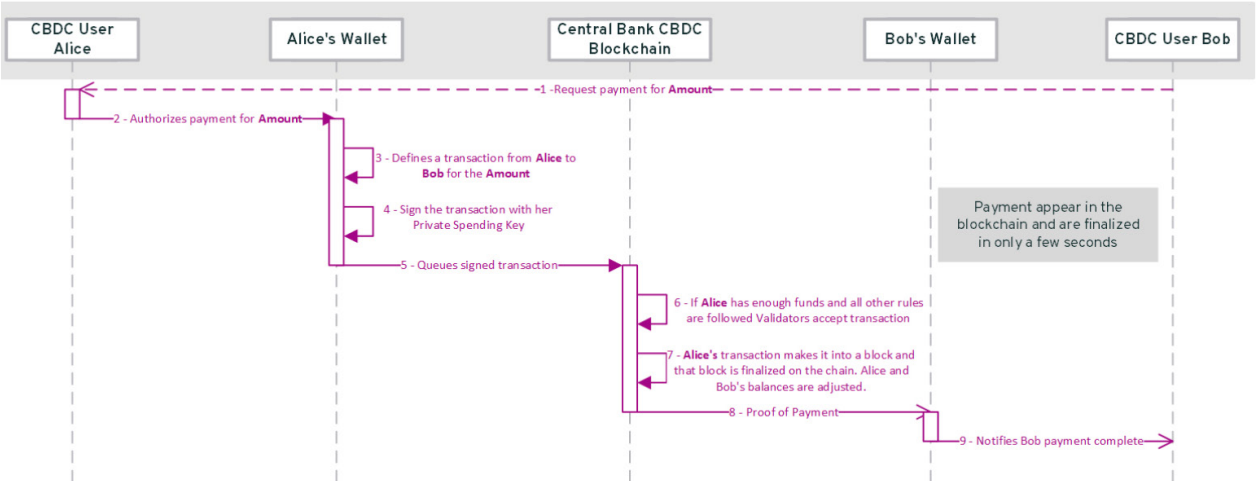


Figure UC3-1–***Sequence**: Sequence diagram for Use Case 3-1 (Transaction in token-based CBDC using online channels)*

CBDC User Alice and CBDC User Bob – Users of the CBDC-Blockchain. Bob wishes Alice to pay him AMOUNT in CBDC. Alice and Bob may be two Consumers, two Merchants, or any combination of users.

Alice's Wallet and Bob' Wallet – Business, Merchant or other end-user seeking to transact with CBDC using their Wallet as a user-agent. This electronic wallet user-agent holds the Private Spending Key to the end-users' CBDC.

CBDC-Blockchain – Public permissioned instance of the Algorand blockchain platform with an ASA representing CBDC.

UC3-1.1 — Consumer (or Business) transacts with other Consumers online real-time

In our model, all CBDC transactions occur on the private permissioned Algorand blockchain. Any CBDC transaction between consumers, businesses, banks, or even foreigners are executed from one blockchain address to another.

The Algorand blockchain functionalities would be used to support all the operations related to the CBDC transactions. Algorand's unique Pure Proof-of-Stake consensus protocol would verify the validity of each transaction, add it to a block, and extend the blockchain with the new validated block in seconds. Additionally, Smart Contracts can be used to verify the AML status of an end-user, impose policy rules on the wallets of end-users, suspend users from transacting, or even shut-down wallets in violation of any requirement, etc.

As an illustrative example, the diagram above describes the sequence of interactions of a CBDC transaction between a Consumer (Alice the Payor) and a Business (Bob the payee), a P2B transaction. The same logic, though, would apply for a transaction between two consumers, P2P, or two businesses, B2B.

A payment in CBDC from Alice to Bob is finalized in a few seconds, broadly following these steps:

1. Bob sends Alice a request for payment in CBDC;
2. Alice authorizes a payment from her wallet to Bob's: she defines a transaction from Alice to Bob for the amount of CBDC requested and signs the transaction with her Private Spending Key. Her wallet then puts the valid transaction in a queue for the CBDC-Blockchain;
3. The payment is entered onto the CBDC-Blockchain. That is, first, Alice's transaction is validated to ensure she has enough funds and that other rules are followed. Then, the transaction makes it into a validated block and Alice and Bob's balances are adjusted.
4. Bob is notified that the payment is complete.

In more detail:

Request for Payment

A Consumer wishes to purchase goods from a Store and wants to pay for it with her CBDC. The Wallet of the Consumer already contains enough CBDC, which was "pre-loaded" as described in UC2-2. The Store initiates the process by sending a request for payment from its business interface to the Consumer, indicating the amount of the payment and its eWallet address, this is point [1] in the diagram. This step can be automated with Near Field Communication (NFC) with the Payee's Point of Sale system or by scanning a Quick Response (QR) code.

Authorize Payment

The Payor sees the request on her interface and crafts a transaction for the appropriate amount from her own eWallet (with public key PK_{Payor}) to the Payee's eWallet (PK_{Payee}). The Payor's eWallet prevents the creation of a transaction when the Payor does not have sufficient CBDC. If everything is correct, the Consumer signs the transaction with her Private Spending Key (SK_{Payor}), and once the transaction is signed it cannot be altered by any means without invalidating it. The CBDC token payment is authorized, point [2] in the diagram.

Validation of Payment

At this point, the execution of the payment moves to the blockchain. The Consumer's eWallet submits the signed transaction to the system. Since the transaction is signed it can go through any number of 3rd party hands without concern that the contents will be tampered with. The consensus protocol verifies and validates the transaction, and the transfer of tokens is then securely finalized (point [7] in the diagram).

Algorand's Pure Proof of Stake (PPoS) consensus protocol uses a novel implementation of the Byzantine Agreement protocol to securely and decentrally propose and agree on new transactions and blocks that will be accepted by the system and extend the blockchain. The advanced cryptographic methods employed in PPoS allow it to propose and agree in seconds, easily supporting the transaction of millions of users. Once a block is agreed to by the system, the block, and all of the transactions inside of the block, are final and irrevocably committed. There is no possibility of a transaction, once agreed upon, being reversed, as is often the case in other blockchain using prior approaches to consensus.

Every participating authorized Node designated by the central bank to act as a Validator guarantees that the Payor is uniquely entitled to execute a transaction, that funds are available in her wallet, that double-spending is impossible, and that all other possible requirements have been fulfilled.

After finalization, a simple proof of transfer to any listeners such as the Payor and the Payee is provided by the blockchain. The Store's interface app can be programmed to receive this message and inform the Store that its eWallet has received the payment and that the purchase of the goods is complete (point [9]).

UC3-1.2 — Bank/LSP ensure interoperability with counterparts to facilitate real-time transfer of value in CBDC between their respective customers

Banks and Licensed Service Providers have a very minimal set of system requirements they must adhere to in order to ensure interoperability with their counterparts. These requirements are a) CBDC transactions occur on the Algorand blockchain as normal transfer transactions; b) payments between them are handled via existing ELT channels such as EFT; and c) payments between them and the central bank are accomplished by using the RTGS infrastructure. When these minimum requirements are satisfied, CBDC value transfers will be easy, fast, and final between their respective customers with the vast majority of the interaction taking place on the CBDC-Blockchain, bypassing the Banks and LSPs as intermediaries once CBDC acquisition has occurred yet preserving regulatory oversight as needed.

UC3-1.3 — Consumer without a bank account transact CBDC with other consumers with and without bank account

As briefly described in UC2-2, opening an eWallet on the CBDC-Blockchain does not require consumers to have a bank account. The key aspect of our distribution model of CBDC is that the LSP works as a liaison between the central bank and the final users, allowing for multiple LSP and different ways of delivery of the CBDC to the public to coexist. Specific characteristics of the business model of an LSP can be used or developed to tailor the distribution service to different modalities of payment. Although ELT payments could be preferred as a baseline method, paying in cash would also be possible. On the contrary, cash and CBDC are interchangeable from a value perspective. A partnership with providers such as specialized payment providers (e.g. for remittances), for instance, would facilitate the distribution of CBDC in exchange for cash to consumers with no access to bank services.

Moreover, transactions and payments can be finalized online through payment services provided by service providers and easily integrated into online shopping platforms. Mobile phones and the CBDC-Wallet app will provide a simple and fast portable form of payment, but other payment structures when users have limited access to the Internet or do not own mobile phones would be possible as well. We describe this situation in the next user case.

UC3-1.4 — Consumer freely exchanges CBDC for cash or, if they have a bank account, for commercial bank money (EFT)

CBDC is designed as legal tender. Any institution capable of exchange will, therefore, accept it in lieu of other forms of payment. Licensed Service Providers, Banks, and even end-users with cash reserves like Merchants can facilitate the exchange of CBDC for cash or for EFT. Consumers are not required to go back to their onboarding LSP to make this exchange. They are free to swap CBDC for cash/EFT with any institution that supports the exchange at any time. The process is straightforward. The Consumer issues a CBDC-Blockchain transaction to the exchange entity. Once proof of payment is received from the blockchain the exchange entity will provide cash or send EFT to the Consumer.