BIS Innovation Hub

Project Sela

An accessible and secure retail CBDC ecosystem

September 2023

BANK OF ISRAEL בנק ישראל بنك إسرائيل

HONG KONG MONETARY AUTHORITY
香港金融管理局

Contents

Acronyms and abbreviations

AE	access enabler
AML	anti money laundering
API	application programming interface
ATM	automated teller machine
AWS	Amazon web services
A2A	account-to-account
BIS	Bank for International Settlements
BoE	Bank of England
BoI	Bank of Israel
CA	certificate authority
CPMI	Committee on Payments and Market Infrastructures
CFT	countering financing of terrorism
CNAAT	cloud-native application protection platforms
DeFi	decentralised finance
DLT	distributed ledger technology
ECB	European Central Bank
e-HKD	Hong Kong dollar CBDC
FI	funding institution
FMI	financial market infrastructure
gRPC	general-purpose remote procedure calls
HKMA	Hong Kong Monetary Authority
HSM	hardware security module
IP	Internet protocol
KMaaS	key management as a service
KYB	know your business
KYC	know your customer
mTLS	mutual transport layer security
NIST	National Institute of Standards and Technology
PC	personal computer
PII	personally identifiable information
PoC	proof of concept
RBAC	roles-based access control
rCBDC	retail central bank digital currency
RTGS	real-time gross settlement
RTP	request-to-pay
SDK	software development kit
SOC	security operations centre
SME	small and medium-sized enterprises
SSL	secure sockets layer
TEE	trusted execution environment
TLS	transport layer security
UI	user interface
UNIDROIT	International Institute for the Unification of Private Law
2FA	two-factor authentication

1. Introduction

Central bank money forms the core of the global monetary system, providing a foundation of safety, neutrality, accessibility and integrity underpinned by the payment finality achieved via settlement on the central bank's balance sheet.[1] Currently, the public has access to only one form of central bank money – physical cash in the form of notes and coins. However, there is clear evidence of a decline in the use of physical means of payment as consumers shift to digital payments that are heavily reliant on private providers. As economies become increasingly digital, more and more central banks are exploring retail central bank digital currency, or rCBDC, and evaluating different designs.[2] An rCBDC represents a new, additional form of public money. Depending on its architecture, it can be accompanied by a central bank-operated payment system that should provide both the unique advantages of central bank money and support digital payments as a public good.

Designing a functional rCBDC platform presents several challenges for central banks. The central bank can play a critical role in operating the core of the system and ensuring sound money, liquidity and overall security. As retail payment needs are diverse and constantly evolving, one way to meet this demand is through a vibrant community of intermediaries that can foster competition, innovation and access. In their explorations, central banks are therefore contemplating many alternative designs for an rCBDC system. The questions that must be considered in these efforts include, notably, what is the most efficient division of tasks between the private and public sectors in the provision of the rCBDC platform and services? How can an rCBDC system promote access and competition, and foster innovation in payment services? Does increased access come at the cost of greater cyber security risks? And, lastly, can a well designed rCBDC system retain the desirable attributes of cash while also creating user experiences functioning as well as, or better than, today's payment systems? These are questions that Project Sela seeks to answer.

Project Sela is a joint experiment between the BIS Innovation Hub Hong Kong Centre, the Bank of Israel (BoI) and the Hong Kong Monetary Authority (HKMA). Sela leverages the BoI's ongoing work on its digital shekel project[3] and its cyber security expertise and the HKMA's learnings from Project Aurum and its ongoing work on Project e-HKD.[4,5] It is also supported by private sector service providers FIS and M10 Networks on the technology and core product, Clifford Chance on the legal analysis and Check Point Software Technologies on cyber security.

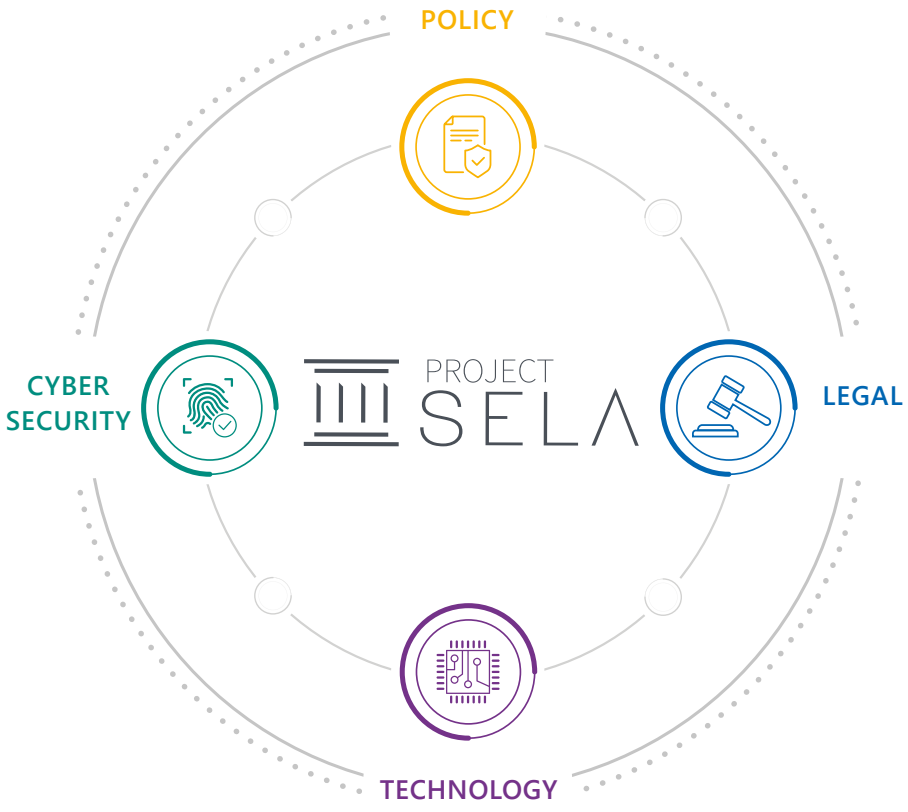
---

1. BIS (2022).
2. A recent BIS survey of 86 central banks found that 93% are actively exploring rCBDCs, with work on retail rCBDC more advanced than on wholesale -CBDC. See Kosse and Mattei (2023).
3. See www.boi.org.il/en/economic-roles/payment-systems/future-payment-methods/digital-shekel-cbdc/.
4. See BISIH (2022) and www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/central-bank-digital-currency/.
5. Project Sela does not reflect any policy decisions by the HKMA about a potential e-HKD or by the BoI about a potential digital shekel.

Sela tests the feasibility of an accessible and cybersecure rCBDC proof of concept (PoC). In doing so, it assumes that competition, innovation, access and cyber security are desirable properties of an rCBDC payments platform, and that these properties can be achieved through a public-private partnership that supports a vibrant ecosystem of private sector intermediaries. For this purpose, an rCBDC architecture was chosen where the central bank operates the retail ledger and provides rCBDC accounts for end users, while private intermediaries handle all customer-facing rCBDC services and obligations.

The building and evaluation of the Sela ecosystem was conducted through the lens of four key pillars – policy, legal, cyber security and technology (Graph 1). The policy workstream proposed that lowering the barriers to entry for intermediaries, with a view to diversifying the range of service providers, could serve as a catalyst for an accessible, competitive and innovative rCBDC ecosystem. One way this could be achieved is by the unbundling and efficient redistribution of rCBDC processes among different public and private actors in the ecosystem. In the Sela architecture, the central bank operates the rCBDC platform, providing instant settlement for all rCBDC transactions, and provides (via the platform) pseudo-anonymous accounts for end users. Private intermediary service providers perform all customer-facing services and compliance obligations, and end users control their rCBDC funds through self-generated private cryptographic keys.

Graph 1 – Project objectives and workstreams



These design features were then validated by the legal workstream. The unbundling of rCBDC processes and services in Sela gives rise to a new category of rCBDC payment service providers called access enablers (AEs). AEs provide all customer-facing rCBDC services but never take hold of, or control, the customer's rCBDC itself, nor do they need to hold liquidity on their own balance sheets to provide rCBDC services. rCBDC payments are thus settled directly on the central bank's balance sheet, free from credit risk. This could justify a lower financial regulatory standard for AEs and lead to a reduced entry barrier to providing rCBDC-based services, opening the doors to payment service providers distinct from those participating in the existing payments ecosystem.[6] This, in turn, could encourage competition, enabling more rCBDC use cases to be developed and providing the foundation upon which innovation can flourish.

When considering the cyber security of such a critical infrastructure, it is important to ensure that this enhanced access does not come at the cost of increased cyber security risks. In this regard, the cyber security workstream provided input on preventative measures that could be used in the Sela design to mitigate cyber security threats while not limiting overall access to the rCBDC platform. The outcomes of the policy, legal and cyber workstreams then fed into the technology workstream, which oversaw the building of the PoC.

Specifically, the Sela PoC aimed to:

1. Maximise access for end users and service providers by lowering the barriers to entry for intermediaries and foster competition and innovation in the private sector;

2. Mitigate cyber security threats by preventative software design;

3. Preserve the desirable attributes of cash, including absence of credit risk, wide accessibility, safety as a means of payment and store of value, provision of instant settlement, low cost operation and an appropriate level of privacy for end users vis-à-vis the central bank; and

4. Capture the benefits of digitalisation, such as providing frictionless and location-independent payment, instant liquidity, and programmability.

Other design criteria such as performance, scalability, offline and cross-border transactions are beyond the project's direct scope. No design decisions were made that prevent these functions from being supported.[7]

The next section describes the Sela ecosystem design. Sections 3, 4 and 5 outline the main policy, legal and cyber security considerations underpinning the Sela PoC build. Section 6 provides an overview of the PoC technical implementation architecture, including the ecosystem participants, components and the use case flows. The last section concludes with lessons learned and suggested next steps.

---

6. While a lower financial regulatory standard could be justified, there could be other requirements placed on AEs (eg security, governance etc) as part of a broader regulatory framework.

7. Furthermore, the policy and legal analyses focused on considerations related to the project objectives. Other considerations, such as rCBDC remuneration, bank disintermediation, monetary policy transmission etc, were all out of scope of the project.

2. Ecosystem design

The Sela PoC implemented an rCBDC ecosystem (Graph 2) where the activities related to rCBDC accounts are unbundled and redistributed among the different participants, namely:

i. A central bank that issues and redeems the rCBDC, operates the rCBDC ledger providing instant settlement for rCBDC transactions, provides pseudo-anonymous rCBDC accounts for end users and operates the real-time gross settlement (RTGS) system;

ii. Funding institutions (FIs) that manage end users' deposit accounts of private money and cash ATMs, and enable the conversion of rCBDC to and from bank deposits and cash;

iii. A new type of intermediary called an access enabler (AE) that facilitates all customer-facing rCBDC services (eg onboarding and know-your-customer (KYC) and know-your-business (KYB) checks, providing user access to the rCBDC system, endorsing and routing of user payment requests, compliance obligations, and implementation of any additional requirements mandated under the rCBDC platform rules) without "holding" end users' rCBDC or needing to hold liquidity on its own balance sheet; and

iv. End users who control their own rCBDC funds in wallet applications on their electronic devices (such as mobile phones), through sole authority over their cryptographic private keys.

Sela's PoC is a full-stack solution of the overall rCBDC ecosystem, including the rCBDC ledger and its connected infrastructures and participants. The core of the Sela PoC is an rCBDC ledger run by the central bank, which is a private, permissioned and account-based distributed ledger technology (DLT) system storing pseudo-anonymous and unique representations of each end user registered on the network and the corresponding account balances.[8] The rCBDC ledger is accompanied by a central bank-hosted rCBDC application outside the ledger providing business logic for the platform, such as coordinating with other components operated by the central bank. The PoC was also designed to be modular and to integrate into traditional payment infrastructures, such as a central bank-operated RTGS system, FI deposit accounts and ATMs to support the conversion of rCBDC to and from bank deposits and cash. These traditional infrastructures are connected to the rCBDC ledger and form part of the overall ecosystem, alongside new rCBDC components such as end user wallets and AE backend systems that together support baseline rCBDC functionality.

8. Although based on DLT, the DLT is assumed to be run by the central banks as a single operator. This leaves future scope to explore how the operations of the platform could be distributed among additional ecosystem participants if desirable.

Graph 2 – Project ecosystem

Sela's accessible and cybersecure rCBDC ecosystem PoC contributes to the work done by the central banking and digital payments community. The project is inspired by open banking and decentralised finance (DeFi) protocols as they support open access to financial data, end users holding their own funds and the unbundling of financial services. This will help to remove barriers and enable a more diverse and innovative ecosystem of service providers.[9]

9. A growing number of countries are introducing Open Banking initiatives (such as the EU's PSD2 Directive and Israel's Open Banking Standard) that give third-party providers access to customers' bank account information to offer services based on this access. Under Open Banking, financial services which were previously centralised and controlled by a single entity can now be decomposed and offered by different service providers. See www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html and www.boi.org.il/en/economic-roles/supervision-and-regulation/2527/implementation-of-an-open-banking-standard-in-israel/.

The project also builds on global central banks' CBDC explorations, such as the BoI's digital shekel, the Bank of England's (BoE) digital pound, and the European Central Bank's (ECB) digital euro, where private sector involvement in the rCBDC ecosystem is highlighted as key to supporting innovation, and where the roles and responsibilities are distributed amongst the central bank and supervised private sector intermediaries in the form of a public-private partnership. For example, the digital pound and digital euro initiatives outline an rCBDC ecosystem where the central bank issues the rCBDC, operates the central infrastructure and retains full control over settlement of retail transactions, while the private sector is responsible for all end user-facing tasks, playing a crucial role in offering innovative and user-friendly services. This ensures that "holding [the rCBDC] would mean holding a direct liability of a central bank"[10] at all times, as is the case with cash today, with the added benefit of private-sector payment services. The BoE deemed this rCBDC "platform" model "the most efficient mechanism to deliver the digital pound,"[11] with the goal to "to enable a diverse range of organisations to join the digital pound ecosystem to provide innovative services to consumers and households."[12]

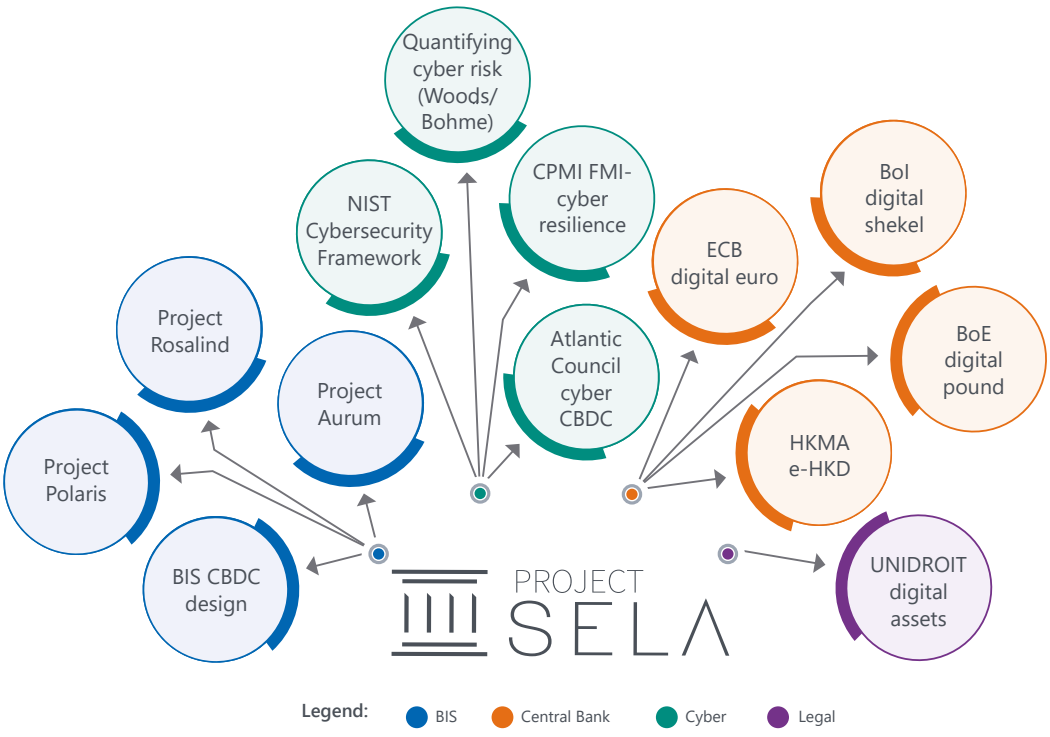
In the BoI's digital shekel draft model, payment services providers "will not develop a balance-sheet exposure", allowing a wide range of entities to provide rCBDC services, including "banks, credit card companies, fintech firms, or international or domestic technology and/or financial firms, provided that they meet the legal and regulatory requirements that the Bank of Israel and other authorities put in place."[13] Similarly in the Sela rCBDC architecture, while AEs provide all customer-facing operations, they never "hold" end users' rCBDC as end users hold their own rCBDC funds, FIs handle rCBDC conversion[14] and the central bank operates the retail ledger. Sela also builds on Rail 2[15] of the HKMA's Project e-HKD, which examines different rCBDC design and architectural issues, and supports the HKMA's efforts in promoting open banking, on top of the recent introduction of the Open API Framework for the Hong Kong Banking Sector in 2018.[16]

10. See ECB (2022).
11. See BoE (2023a).
12. See BoE (2023b).
13. See BoI (2021).
14. A distinction between FIs and other types of intermediary in the rCBDC ecosystem is also envisioned as part of the governance model currently being developed in the digital shekel project.
15. Project e-HKD, Hong Kong's rCBDC exploration, adopts a "three-rail approach" in paving the way for the possible issuance of an e-HKD in the future. See www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/research-and-applications/central-bank-digital-currency/.
16. See HKMA (2018).

In addition, Sela complements other BIS Innovation Hub projects on rCBDCs. For example, it builds on the learnings from Project Aurum, a technical rCBDC study conducted in collaboration with the HKMA that examined an architecture where the central bank operates only the wholesale ledger and commercial banks operate the retail ledger.[17] Project Sela instead tests the feasibility of an architecture where the central bank operates the retail ledger and aims to reduce the entry barriers for rCBDC to catalyse competition, innovation and user access. The project is also inspired by the innovative rCBDC use cases outlined in Project Rosalind, which focuses on an rCBDC application programming interface (API) layer.[18] In addition, Sela aims to extend the CBDC security and resilience framework of Project Polaris to practical learnings.[19,20]

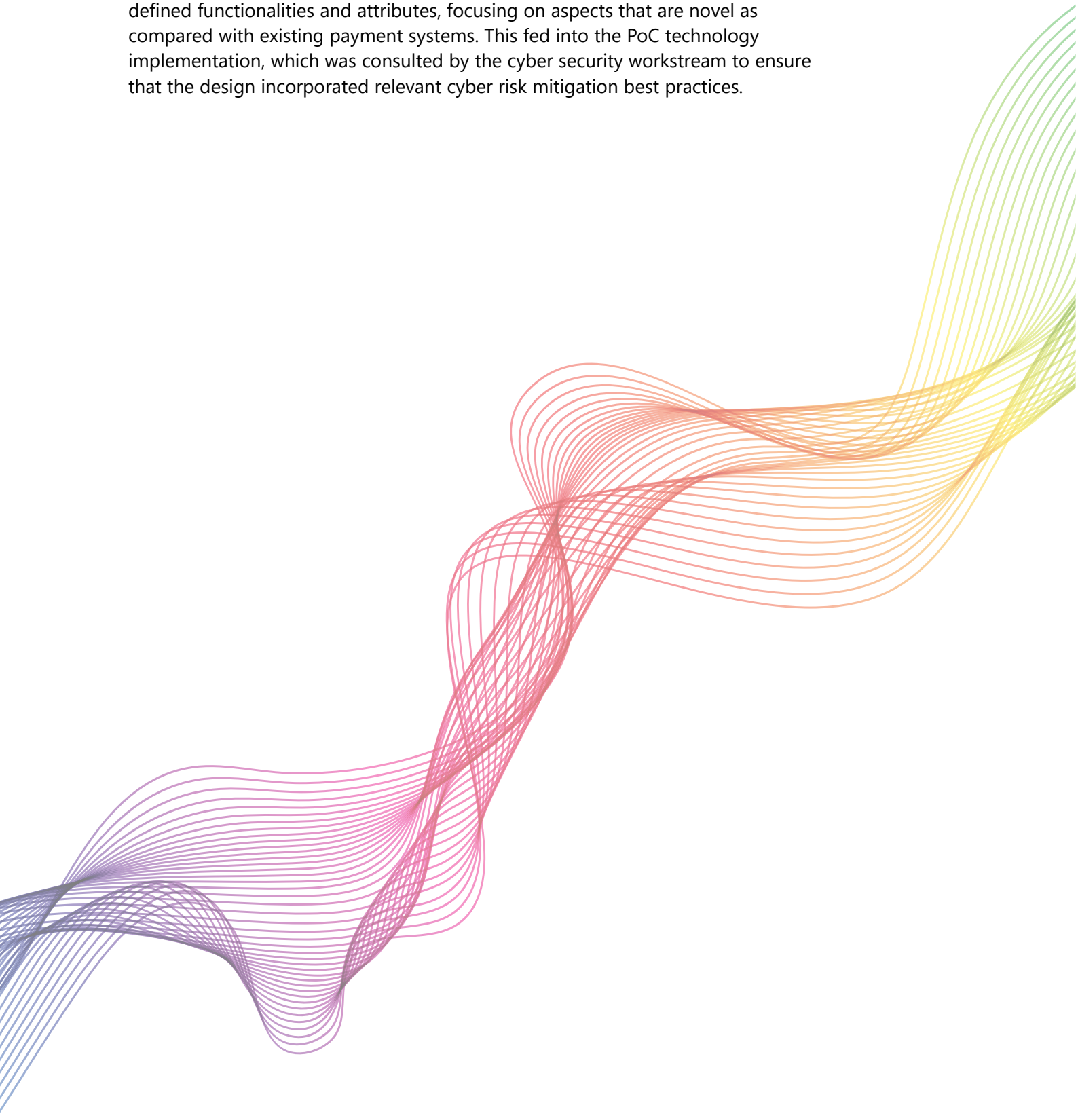
Sela is also informed by legal and cyber literature on, for example, the legal principles on digital assets from the International Institute for the Unification of Private Law (UNIDROIT), and cyber security and resilience frameworks for FMIs and CBDCs (eg from the Committee on Payments and Market Infrastructures (CPMI), The National Institute of Standards and Technology (NIST), the Atlantic Council and Woods and Böhme (2021)) – see Graph 3.

Graph 3 – Foundation of existing work and literature



17. See BISIH (2022).
18. See BISIH (2023a).
19. See BISIH (2023b).
20. For a recent review of the Innovation Hub's CBDC work, see BISIH (2023c).

The Sela ecosystem design is conducted through the lens of four key pillars – policy, legal, cyber security and technology/PoC implementation. To leverage the expertise of project participants, members were divided into four corresponding workstreams. Each workstream followed an agile process over the project's six-month time span. The first workstream led by policy experts from the participating central banks defined the functionalities and attributes that should characterise the rCBDC ecosystem PoC. The legal workstream then provided legal validation of the defined functionalities and attributes, focusing on aspects that are novel as compared with existing payment systems. This fed into the PoC technology implementation, which was consulted by the cyber security workstream to ensure that the design incorporated relevant cyber risk mitigation best practices.



3. Policy considerations

Guided by an overarching set of policy goals, the policy workstream identified the attributes that should characterise the rCBDC ecosystem. These high-level attributes fed into the requirements of the rCBDC architecture and subsequently the PoC build.

3.1 Unbundling and efficient distribution of activities in an rCBDC ecosystem

Central banks' rCBDC explorations aim to provide a public, trusted, accessible and secure monetary and payment infrastructure that can support users' increasingly digital payment needs. At the same time, retail customer-facing payment services have long been the purview of the private sector, which has come up with innovative and creative solutions to meet users' differing payment needs. Continued involvement of the private sector would enable constant innovation and new services that rely on the rCBDC platform, as private intermediaries would compete on user experience and value-added services. An rCBDC architecture should therefore continue to leverage the respective strengths of the public and private sectors, with each focusing on what they do best – the central bank on operating the core of the system by ensuring sound money, liquidity and overall security, and the private sector on using its creativity and ingenuity to serve customers.[21]

Furthermore, technological developments in the open banking and DeFi space have demonstrated the ability to disentangle financial services through open access to financial data and end users controlling their own funds. This would enable a more diverse and innovative ecosystem of service providers. A defining feature of the Sela ecosystem is the unbundling and redistribution of activities related to an rCBDC account among the main participants in the Sela architecture – the central bank, FIs, AEs and end users.[22] This division of responsibility among the participants should give rise to an open and competitive rCBDC ecosystem that could also provide some of the desirable attributes of cash in digital form in terms of providing a safe store of value, instant settlement and low-cost operation.

3.2 Lower barriers to entry allow a wider range of intermediaries to foster an innovative payment ecosystem

Competition spurs innovation. It is therefore important for an rCBDC system to enable a diverse and vibrant community of private sector intermediaries in the provision of rCBDC services. This can be done by reducing the barriers to entry for services providers in the rCBDC ecosystem. In Sela, the AEs are a key participant category: their role is designed to increase access to rCBDC services and develop innovative retail rCBDC payment solutions. While handling most customer-facing rCBDC services, AEs do not provide rCBDC accounts or need to manage consolidated records of retail transactions, as this is done by the central bank via the rCBDC platform (although AEs play a crucial role in masking sensitive personal information from the central bank – see Section 3.6). This removes a large

21. See Shin (2021).
22. While the AE and FI roles were unbundled for the conceptual architecture, nothing prevents an entity from performing both roles as a bundled service.

operational burden from AEs and can reduce their barriers to entry. Furthermore, AEs do not control end users' rCBDC funds (as these are held by the end users themselves), nor do they provide conversion services for end users to exchange their rCBDC to and from other forms of money – a service provided by the FIs (see Section 3.3), although facilitated by AEs. As such, AEs do not need to hold or control their own or customer funds at any point to support the provision of services.[23] AE-enabled rCBDC payments are settled on the central bank's balance sheet and are free from credit risk, in contrast to digital payments in traditional payment systems. This can result in lower liquidity costs for AEs and potentially greater liquidity efficiency in the entire system – see Box A for more details.

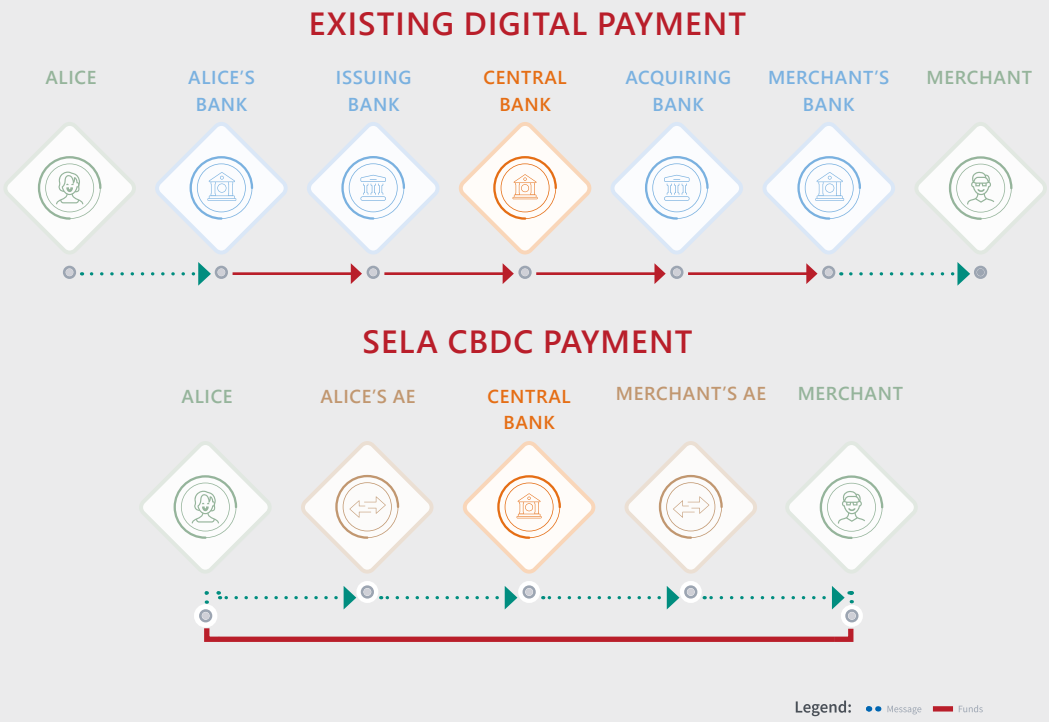
Taken together, these attributes of AEs could justify a lower regulatory standard in terms of financial requirements, and in turn a lower barrier of entry to providing rCBDC-based services. For example, AEs would not need to be subject to liquidity or capital requirements that are calculated, among other things, by reference to customer funds held.[24] The base financial regulatory requirements to become an AE should therefore be lower than those of most intermediaries in the current financial system (who are financially liable for their customers' funds). Lower entry barriers can enable wider participation in the provision of rCBDC services, compared with the existing payments market, to include, for example, SMEs, civil society and charitable organisations, e-commerce providers, community centres and technology companies, among others, supporting a more accessible, competitive and innovative ecosystem over time.

Payments through AEs versus via traditional intermediaries Box A

In existing systems, digital payments are made using claims on commercial intermediaries, who hold client funds on their balance sheets. Transferring funds creates a financial exposure on the balance sheets of the intermediaries involved and imposes risks and costs affecting both the intermediaries and the end users. Consider, for example, an end user, Alice, paying with a credit card to a merchant (Graph 4). The funds need to go from Alice's bank account to her card-issuing bank,[25] to the merchant's acquiring bank, to the merchant's bank account. Liquidity, counterparty and credit risks arise at each leg of the transaction as steps in the process do not take place instantaneously and intermediaries need to hold liquidity against their commitments to each other along the payment chain, imposing costs that are often passed on to the end user.

23. These entities are inspired by service providers seen in DeFi and open banking protocols, such as intermediaries serving customers with self-custody wallets and programmable protocols, payment initiation and account information service providers, and intermediaries in rCBDC designs explored by the central banking community, such as the BoE's digital pound.
24. This is not to say that AEs will not be subject to capital requirements, eg they will still need capital to meet their own operational needs. Furthermore, AEs would still need to be subject to a regulatory framework for things such as AML, cyber security and consumer conduct, and would need a licence from the central bank or any other designated regulator in order to offer rCBDC services and connect to the system. See Section 4 below for more details.
25. In the case that the card was not issued by the bank where Alice is managing her account. If the card is issued by her bank, "Alice's bank" and "the issuing bank" are the same entity.

Graph 4 – Existing digital payment vs Sela rCBDC payment



In Sela's architecture, while AEs help to route payment requests to and from the CBDC platform, the funds move instantaneously from Alice to the merchant (or any other type of payee) without ever "touching" the balance sheets of the AEs or any other intermediaries during an rCBDC payment. The involvement of the central bank in the rCBDC settlement process thus eliminates the need for AEs to hold collateral or liquidity against settlement risk during rCBDC transfers. As the corresponding funds remain solely on the central bank's balance sheet, the Sela rCBDC payment can be considered "credit risk-free". Furthermore, AEs do not need to hold their own rCBDC or cash reserves for the purposes of facilitating end users' exchange of cash and other forms of digital funds against rCBDC, as this is handled by FIs based on their existing central bank reserves (see Section 3.3), suggesting that liquidity costs for AEs are lower than those associated with other rCBDC configurations, where payment service providers need to maintain such reserves.[26] This could result in a reduction of total liquidity costs in the system if FIs need in any case to hold unremunerated reserves with the central bank (in which case rCBDC and cash holdings could count towards this requirement) and/or cash forms part of their reserve requirements (in which case their cash holdings to facilitate end users' exchange from rCBDC could fall under the same category).[27]

26. The liquidity savings of AEs in not needing to hold cash inventory to facilitate end users' exchange of cash from rCBDC can be roughly extrapolated from an initial assessment of the necessary cash inventory level of ATMs. Based on discussions with an ATM provider, around 5% of the relevant activity cycle in cash needs to be maintained at any given time. The cost of this depends on the alternative yield; eg at an alternative yield of 5%, the estimated cost is approximately 0.25% of the turnover. This is only an initial estimate and subject to change based on the volume and characteristics of the activity.
27. That said, a more rigorous economic analysis would be needed to assess whether it could result in meaningfully reduced liquidity costs in the entire system.

The Sela rCBDC PoC also offers additional support to assist AEs in their rCBDC services provision, such as developer tools to facilitate AEs' integration into the platform – see Section 5.2.2 for details. Central banks will also need to consider providing other technical support channels and sandboxes for AEs. This reduces the barriers to entry for AEs, removing the need to invest in these tools themselves, and can ensure a more consistent "out-of-platform" service across AEs, which will in turn lead to better services and lower costs for end users. At the same time, in providing these tools, central banks must avoid taking on undue risks and must ensure adequate supervision and regulation of the rCBDC ecosystem. For example, while developer tools facilitating AEs' AML/CFT regulations compliance can reduce their operational burden, they may create a liability for the central bank vis-à-vis the AML authorities or prevent the central bank from penalising any breach of AML/CFT regulations and should be avoided. Furthermore, a heavy-handed approach in supporting AEs may lead to AEs becoming overly dependent on central bank-provided developer tools. The key is to provide a solid foundation upon which AEs can develop their own creative and innovative value-added services, rather than to increase their reliance on the central bank.[28]

3.3 Singleness of money, access and financial inclusion

An rCBDC system should maintain the singleness of money in the economy, meaning that payments denominated in the sovereign unit of account will be settled at par, even if they use different forms of privately or publicly issued monies.[29] rCBDCs should therefore be interchangeable with other forms of regulated money in the economy, and FIs' role in the Sela ecosystem is crucial to achieving this goal.

FIs continue to play an important role in the Sela rCBDC ecosystem, similar to today's payment systems. Deposit accounts managed by FIs remain an important vehicle for end users in Sela to hold funds, make payments and save, and it is important to enable smooth interoperability between end user accounts at FIs and rCBDC. Sela does not aim to replace existing forms of regulated money, such as FI deposits, nor to introduce risks to financial stability by disintermediating regulated private entities, and design choices can be put in place to prevent this. For example, as many central banks have identified the need for holding limits to manage wider financial and monetary stability risks that may arise when introducing an rCBDC to the financial system,[30] an arbitrary holding limit was implemented in the Sela PoC.

28. For example, the digital euro's third progress report outlines a dual approach where a digital euro app provided by the Eurosystem with a homogenous look and feel facilitating a standardised approach to connecting end users to intermediaries would be provided alongside the option for intermediaries to build their own integrated solutions. This dual approach facilitates speedier digital euro adoption for new and smaller intermediaries by leveraging the Eurosystem app, while also leaving room for tailored value-added services and front-end solutions developed by intermediaries. See ECB (2023a).
29. See BIS (2023).
30. See, for example, BoE (2023a) and ECB (2023a).

For simplicity, it is assumed in Sela that FIs are commercial banks that hold accounts with the central bank in the RTGS system and settle obligations amongst each other on the central bank's balance sheet.[31] In today's payment systems, in order to exchange funds from a deposit account to central bank money (currently available only in the form of cash), customers would approach an ATM or a branch of their FI. In the Sela design, FI customers can exchange funds from their deposit accounts to rCBDC, or from rCBDC to their deposit accounts, seamlessly, on a 24/7/365 basis and from any geographic location (see Section 6.2.2 for a detailed flow of users exchanging FI deposits for rCBDC).

To ensure access and inclusion by all retail users in the economy, an rCBDC system must support the conversion of CBDC to and from cash for those with and without bank accounts. In Sela, customers can exchange cash to and from rCBDC through the ATMs operated by FIs, supporting interoperability between physical and digital central bank money. End users can convert cash to and from rCBDC at any FI-operated ATM even if they are not customers of the same FI or have no bank account whatsoever (eg are "unbanked"), so that rCBDC serves as a tool for financial inclusion. See Section 6.2.3 for a detailed flow of users exchanging cash for rCBDC. This interoperability between cash, FI customer deposits and rCBDC is supported by an rCBDC-bank reserves reconciliation mechanism between the FIs and the central bank, as outlined in Box B.

rCBDC-bank reserves reconciliation mechanism Box B

To support end users' conversion requests of rCBDC against cash and FI deposits on an ongoing basis, RTGS systems would need to operate 24/7 to reconcile corresponding falls and increases in an FI's reserve balances held at the central bank. In most jurisdictions, however, RTGS systems are not available all the time. Furthermore, they are not designed to support high-frequency, low-value retail transactions. As such, a loading and unloading mechanism that supports continuous availability of rCBDC is required. (See Section 6.2.1 for a detailed flow of FIs loading rCBDC against reserves.) When an end user requests a conversion of their FI deposits or cash into rCBDC (and vice versa), there needs to be a way to reconcile the corresponding fall (or increase) in the FI's reserve balance held at the central bank outside of RTGS operating hours. Project Sela explored three such reconciliation mechanisms: (i) net-based settlement/ account-to-account (A2A); (ii) a pre-funded model of tokenised central bank reserves; and (iii) a pre-funded model of rCBDC. The first two options are direct rCBDC distribution mechanisms, involving the central bank directly issuing/redeeming rCBDC into/from end users' wallets upon end users' requests.

31. In theory, FIs can be any entity that takes customer deposits and has access to the central bank balance sheet. Moreover, there may be institutions that offer deposit accounts but do not have direct access to the RTGS system, such as e-money institutions. For simplicity, the assumption in Sela is that all FIs hold accounts at the RTGS. However, the learnings of the project would hold without this assumption.

The third option, which was implemented in the PoC, is an indirect distribution model, where FIs pre-fund their rCBDC wallets and act as the distributor of rCBDC to support end users' requests.[32]

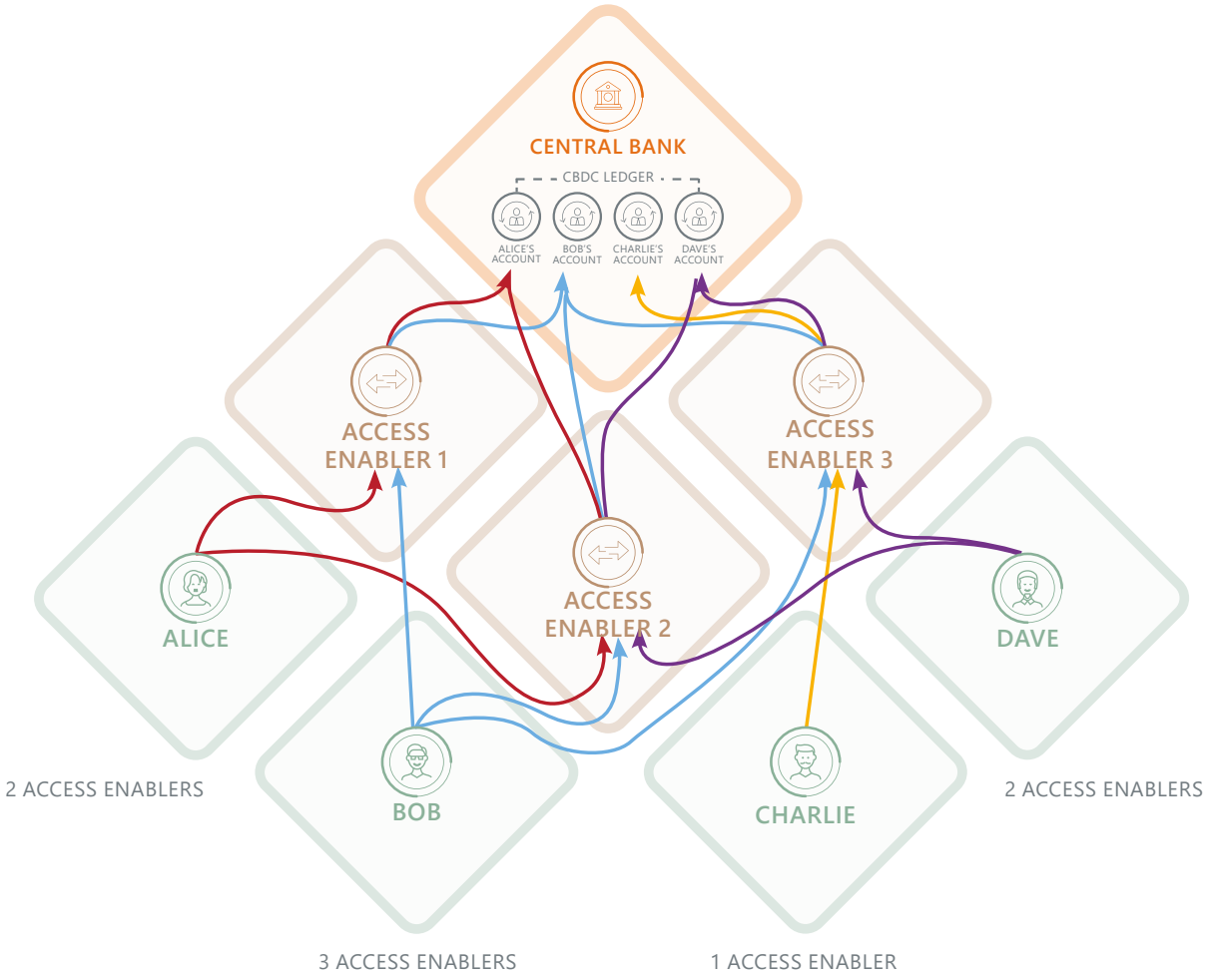
Since the rCBDC in Sela's architecture can be issued only by the central bank, to ensure 24/7 liquidity, all three reconciliation mechanisms involve some version of "pre-funding". The process by which rCBDC is distributed to customers through intermediaries would be more efficient than with physical cash, due to rCBDCs' digital nature. Customers currently access cash via commercial banks as opposed to directly from the central bank. To supply cash to their customers, commercial banks need to first "buy" cash from the central bank, where it is physically transferred from the central bank's vaults to the ATMs of commercial banks. If banks failed to accurately anticipate demand for cash in their ATMs, customers would not be able to quickly obtain their desired amount of central bank money as the movement of physical cash takes time. On the other hand, holding excess amounts of cash may result in liquidity as well as operational costs. In Sela, the efficiency of this distribution process could be significantly enhanced due to the digital nature of the central bank money, reducing the likelihood of intermediaries having insufficient rCBDC funds and lowering liquidity costs to meet customer demand. For example, in Sela's PoC, FIs can set watermarks to automatically load and unload rCBDC from the rCBDC system to better support liquidity and variations in end user demand for rCBDC.

3.4 Enhanced customer experience and programmability

A convenient and smooth customer experience is key to supporting the adoption and viability of an rCBDC platform. Users should be able to easily change between service providers, which should encourage competition in the rCBDC ecosystem and avoid intermediary lock-in. In Sela, a many-to-one mapping of AEs to users was chosen so that each end user can have multiple AEs specialising in different value-added services and switch between AEs without friction. Furthermore, each of an end user's AEs maps back to a single rCBDC account on the central bank's ledger, providing the simplicity of a single liquidity pool with the benefit of multiple service providers (Graph 5). However, a many-to-one mapping between AEs and end users raises challenging technical and user-experience design questions. For example, when an end user with multiple AEs has an incoming payment, which of its AEs accepts and screens the payment? In Sela, a few alternatives were considered, including (i) the payee being notified of an incoming payment and choosing which AE to accept it through; (ii) the payee's AEs competing to process an incoming payment; and (iii) the payee maintaining a default AE that processes all incoming payments. Each option has its own unique set of trade-offs and assessing which is optimal requires more in-depth user-experience research.

32. It is worth noting that the project setup may in the future absorb existing RTGS systems. This could occur if the rCBDC platform becomes the system of record between FIs themselves and the central bank (in addition to its rCBDC functionality). In Sela, FIs hold rCBDC solely for the purpose of enabling end users to exchange deposits and cash for rCBDC, similar to banks' holding of cash today. However, there is nothing in theory to stop banks from using their rCBDC holdings to make interbank payments, which today are done in the RTGS system, and in the future may be made through what is called "wholesale CBDC". Sela in fact lays the groundwork for a future where each jurisdiction has one CBDC system, used both for retail and wholesale. These different use cases may require different design characteristics, and the CBDC system may need to be adapted to these wholesale use cases. These considerations are out of the scope of Sela.

Graph 5 – Example of a possible end user-rCBDC account mapping



Restricting rCBDC accounts to one per end user can also help the central bank apply limits on individual holdings of rCBDC, among other scheme rules, as there is no need to reconcile individual holdings across multiple pools of liquidity. Holding limits for rCBDC could, however, complicate liquidity management and hinder the user experience. To support a smoother payment experience, an arbitrary holding limit accompanied by waterfall and top-up (reverse waterfall) functions were implemented in Sela – see Sections 6.2.5 and 6.2.6 for the detailed flows. These functions are a way of managing end users' rCBDC holdings. Under the waterfall mechanism, an end user's rCBDC holdings exceeding a pre-determined threshold will be automatically converted into its deposit held in a linked FI account. Similarly, under the top-up mechanism, rCBDC holdings below a pre-determined threshold will trigger automatic conversion of an end user's FI deposits to rCBDC.[33,34] It is important to note that the

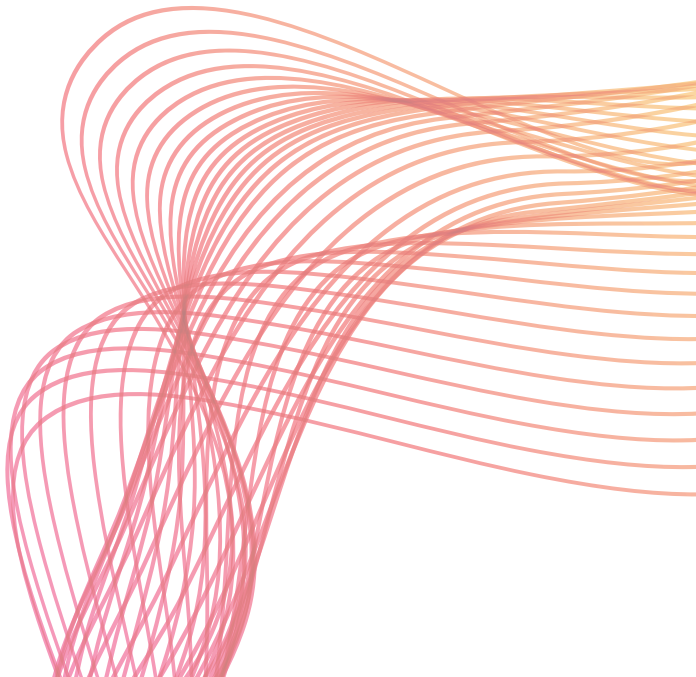
33. See ECB (2023b). For example, automatically converting rCBDC to deposits at a linked FI account if the end user's rCBDC balance exceeds a predetermined X amount.

34. Another challenge could be limitations in FIs' existing infrastructure in handling potentially large loads of conversion to and from rCBDC. One potential solution would be to allow FIs to hold separate customer deposit accounts on the ledger in the form of tokenised deposits; during waterfall, funds would then be converted from rCBDC to tokenised deposits on the same ledger. This is something that is out of scope of Project Sela but which could be explored in the future.

setup in Sela not only enables the enforcement of holding limits with a many-to-one mapping of AEs to end users, but it does so without compromising users' privacy from the central bank, assuming the existence of a unified individual identifier system (see Section 3.6 on proper data management and privacy for more details).

While end users in Sela control their own funds through sole authority over their private keys, a key/account recovery process was put in place so that users do not lose their funds if they lose their keys. Private keys are designed to provide a more convenient and secure experience on websites and applications, as compared with passwords. In the Sela rCBDC platform, private keys are used to validate user requests and are pivotal in verifying user identities and granting access to the application. Under normal circumstances, if an end user misplaces their private key, retrieving it can be a challenging task, and often entails loss of funds in the DeFi ecosystem – this is not a desirable customer experience and should not be an attribute of an rCBDC system. In Sela, the central bank can associate a new public key to an existing rCBDC account (similar to a new end user onboarding process) in the case of lost keys and revoke the old ones.

To reap the full benefits of payments digitalisation and enable a wide variety of rCBDC use cases, an rCBDC platform should ideally support the programmability of payments. It is generally considered that the introduction of programmable payment platforms could bring long-term benefits that far outweigh the short-term costs of investment and coordination efforts in shifting to new standards and procedures.[35] In Sela, preliminary programmability is supported through the movement of messages and transaction payloads between accounts (see Section 6.1.1.2 for more details), providing the building blocks for automation on the platform and for AEs to build value-added payment services on top of the rCBDC ledger. These value-added services can take many forms and serve many use cases, as illustrated in Project Rosalind, which explored private sector programmability.[36] One example is request-to-pay (RTP), where an end user sends a request to another user to be paid a specified amount. The message sent with the request can contain the appropriate transaction payload so that, once the payer receives the message, they can simply validate the content of the payload, sign and submit the payment. This function can be extended in the future to other types of transactions made available by the rCBDC ledger such as split, micro and conditional payments.



35. See BIS (2023).
36. See BISIH (2023a) for more details.

3.5 Regulation and countering illicit activity

An rCBDC system should support financial regulation aimed to mitigate illicit activity, while also protecting the privacy of end users. In existing frameworks, account providers such as commercial banks are typically financially liable for customer funds and responsible for account and payment-related services, including executing payment transactions, account balance checks, user onboarding with KYC/KYB procedures and transaction risk screening such as AML/CFT. In an rCBDC system, however, the account provider – the central bank – is not well placed to directly interact with retail customers, nor is it desirable from a privacy perspective as it would require the central bank to handle personally identifiable information (PII) and to perform the customer-facing operations discussed above.

Sela's AEs, who provide services to end users through direct access to the central bank, bear responsibilities such as customer due diligence and transaction screening. This relieves the central bank from taking on customer-facing obligations, while also ensuring that the rCBDC system adheres to AML/CFT requirements among other relevant financial regulation. A deep dive into what these responsibilities entail for AEs is out of scope for Project Sela as the detailed set of obligations is likely to vary across jurisdictions.[37] However, the expectation is that the ongoing supervision and enforcement of AE obligations would be achieved through a regulatory framework (see Section 4 for more details).

3.6 Proper data management and privacy to ensure trust and cyber security

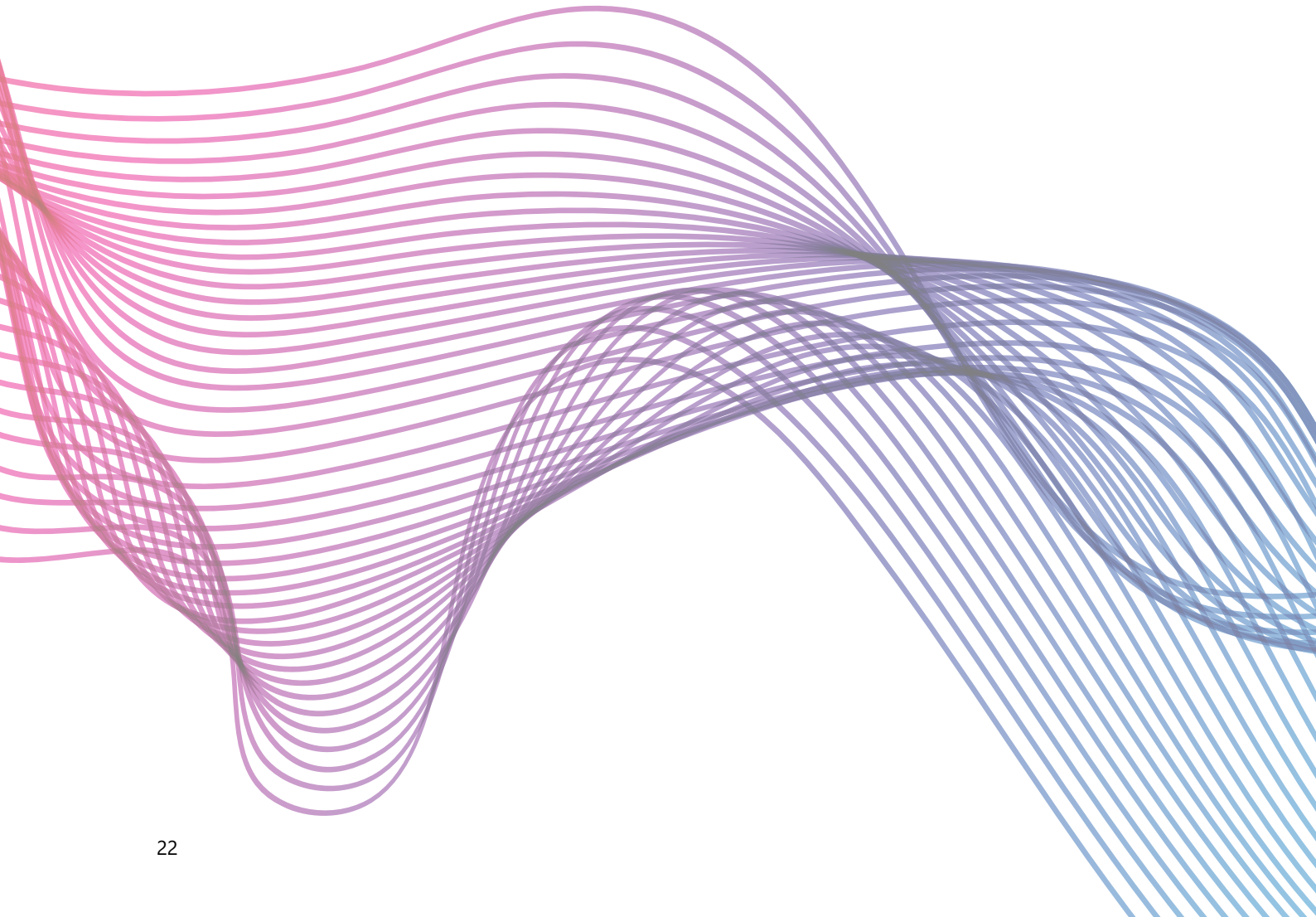
The rCBDC architecture explored in Sela sees the central bank providing real-time and instant settlement to anyone transferring rCBDC, meaning that all retail transactions are stored by the central bank on the rCBDC ledger. Although the central bank is not handling customer-facing operations, end user accounts are in fact provided by the central bank, which also ensures that each account on the ledger is mapped to a unique end user. While this distribution of responsibilities may serve to reduce the barriers to entry for intermediaries, the storage and processing of PII of individual persons by the central bank may not be desirable, for both privacy and cyber security considerations. As a critical financial market infrastructure, an rCBDC platform would need to safeguard the confidentiality, integrity and availability of its user data.[38]

37. More details about different technical approaches for detecting money laundering activities can be found in Project Aurora, see BISIH (2023d).

38. See CPMI and IOSCO (2016).

In Sela, AEs play a vital role in the rCBDC ecosystem in terms of protecting the privacy of retail users from the central bank, or any other centralised government authority, and preventing the data of all retail users from being concentrated in a single entity. While privacy was not in the direct scope of the project, obfuscated personal identifiers from a unified individual identifier system were used in Sela to prevent the central bank from having full visibility into end users' data while reaping the benefits of a single-retail-ledger model managed at the central bank. End users in Sela cannot interact directly with the rCBDC platform, but only through AEs who obfuscate users' PII using hash functions before requests are routed to the rCBDC platform. Obfuscated personal identifiers are then used by the CBDC platform to map end users to unique rCBDC accounts. PII is therefore distributed among AEs, rather than being concentrated at the central bank.

This framework assumes the availability of a unified digital ID or individual identifier system that allows the mapping of (obfuscated) unique identifiers of end users across multiple AEs to single rCBDC accounts. For jurisdictions without these unified ID systems in place, however, there may be practical challenges in achieving this unique rCBDC-account mapping, and enforcement of rCBDC scheme rules such as holding limits, while still protecting the privacy of end users from the central bank. End users could use different identifiers to apply for multiple rCBDC accounts, and the absence of a consolidated view to identify a user will make it difficult to detect. How to achieve this represents an interesting area for future research.



4. Legal considerations

With the key policy goals and attributes of the Sela rCBDC ecosystem identified in the policy workstream, their legal feasibility was evaluated to ensure that the design criteria are supported by a robust legal analysis. This section summarises the legal analysis underpinning the Sela PoC, focusing on aspects that are novel compared with existing payment systems. Notably, who is "holding" or "controlling" the rCBDC in the Sela ecosystem, and correspondingly, whether separating the functions of account provision (by the central bank), services provision (by the AEs) and holding of the funds (by the end user) can support the goals described in the policy section. Although there are important nuances that arise in the legal framework of individual jurisdictions, the legal analysis aims to be as jurisdiction-agnostic as possible while retaining sufficient levels of practicality to be applicable within jurisdiction-specific law.[39]

4.1 Definition of control

A key to achieving the objectives of Project Sela was the introduction of a new type of intermediary called an AE. The AE is never liable for returning customer funds and at no point in its provision of services does it have customer funds on its balance sheet. In practice, this means that an AE should never "hold" rCBDC for others or need to hold liquidity to provide rCBDC services to its users. However, as rCBDCs are non-corporeal (ie they have no "physical" form) and exist only as data packets on the rCBDC platform, it is crucial to determine in what circumstance an rCBDC is considered to be "held" (by the AEs or any other entity). Indeed, many jurisdictions are currently considering if and how a person or entity could be "holding" digital assets such as rCBDCs. While legal certainty surrounding the "holding" of digital assets will only be achieved through the development of relevant case law or specific legislation, published guidelines can provide useful reference.

39. A fundamental part of the legal analysis is underpinned by the UNIDROIT Principles on Digital Assets which are jurisdiction-neutral. They have been drafted using jurisdiction-agnostic terminology and are intended to be applied to any legal system or culture.

Notably, the UNIDROIT Principles on Digital Assets and Private Law[40] (which are jurisdiction-agnostic) provide a useful framework for assessing which entity in the Sela ecosystem is "holding" the rCBDC. The principles propose the concept of "control" in order to capture the notion of "holding" or "having" non-corporeal data objects.[41] Subject to certain exceptions and constraints, a person or entity should be regarded as having "control" of a digital asset if the relevant system (such as the rCBDC platform) confers on that person/entity the following (Graph 6):

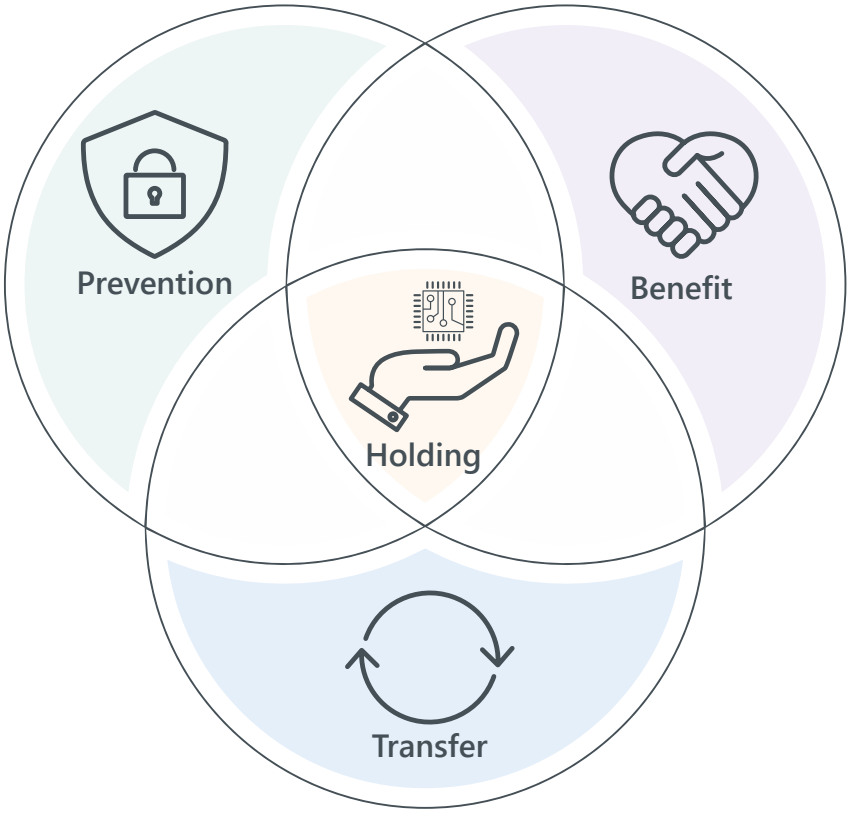
1. *the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset;*

2. *the ability to obtain substantially all the benefit from the digital asset; and*

3. *the exclusive ability to transfer these abilities to another person (ie to action a "change of control").*[42]

40. See UNIDROIT (2023).
41. We note that the UNIDROIT Principles apply only in respect of a defined category of "digital assets" that are capable of being "controlled".
42. See Principle 6 of UNIDROIT (2023).

Graph 6 – UNIDROIT test of control



4.2 Who controls the rCBDC in circulation?

In order to ascertain whether AEs in Sela are holding rCBDC for end users, we apply the UNIDROIT principles' test of control. The aforementioned three abilities determining "control" applied in Sela's context translate into having control over the cryptographic private key (allowing exclusive ability to prevent others from making payments and/or accumulating more rCBDCs), holding the rCBDC account and executing transfers and transactions, or taking responsibility for rCBDCs under a custodial arrangement. As AEs in the Sela architecture do not have access to end users' private cryptographic keys or to their rCBDC account, other than to view balances and endorse payment instructions, we consider that *they would not be legally holding the rCBDCs for end users*.

Furthermore, this lack of control over end users' rCBDC extends to AEs' regulatory obligations. For example, AE compliance with AML/CFT or sanctions legislation and the ability to refuse services to end users or reject specific payment instructions does not imply control or holding of rCBDCs. A refusal to act would be the result of the legal framework preventing all AEs from servicing the end users in such circumstances, rather than the ability of individual AEs. Fundamentally, the CBDC funds are not controlled by the AEs, the AEs merely control their provision of services to specific users.

If AEs do not hold end users' rCBDC in Sela, a natural question that follows is whether end users are holding their own rCBDC or if somehow the rCBDC is being held by central bank on behalf of the end users. In the Sela architecture, there is an argument to be made that end users may not have full control over their rCBDC, as rCBDC accounts are provided and operated by the central bank and the central bank can, in certain circumstances within the legal framework, influence an individual rCBDC account. For example, for users who lose access, central banks can recover rCBDC accounts by going through the appropriate offline key recovery procedures. This responsibility is placed with the central bank, rather than the AEs, as it could otherwise suggest some control of an AE over their end user's funds, which contradicts the key attribute of AEs that they cannot hold an end user's rCBDC. Despite a certain level of central bank control, the legal workstream took the view that the central bank would not have sufficient abilities to meet the UNIDROIT Principles' test for control. This is because the central bank's ability to influence individual CBDC balances is constrained to apply only in certain circumstances. When end users acquire CBDC, they accept these terms.[43] As such, end users in Sela retain control of their own CBDC.

In the absence of a legal provision that clarifies the above issue, the question of who holds the rCBDC will ultimately depend on the jurisdiction-specific levels of control the central bank exercises with respect to individual rCBDC balances on the platform. In either case, the availability of the rCBDC asset to the end user depends on the broader operation of the rCBDC platform.

4.3 Prudential framework considerations for AEs

The unique characteristics of AEs may warrant a tailored prudential regulatory framework that can build on existing frameworks for open banking or other non-custodial payment services.[44] Unlike banks, broker-dealers or traditional payment services providers, AEs would not hold funds for their customers or against customer payments, thereby eliminating the need for traditional liquidity or capital requirements tied to client financial exposures. Additionally, the ability of end users to have multiple AEs and easily switch between them suggests that the failure or downtime of a single AE may not impose as large an impact as if each user had only a single AE.

Nonetheless, AEs would still provide crucial services to end users as part of a national critical payment infrastructure, and therefore be subject to a regulatory framework. Individual jurisdictions would likely create bespoke regimes for AEs, considering the specific set of services they provide. The core focus of any prudential regulatory regime for AEs should be on ensuring a high standard of services provision and facilitating the smooth and continued operation of AEs.

---

43. According to the UNIDROIT Principles, the requirement for exclusive control can be relaxed, and control can be shared for convenience or security purposes or upon acceptance of the user.

44. See, for example, the European Bank Association's Final Report on Guidelines on revised Money Laundering and Terrorist Financing Risk Factors (www.eba.europa.eu/eba-publishes-final-revised-guidelines-money-laundering-and-terrorist-financing-risk-factors), De Nederlandsche Bank's view on transaction monitoring requirements for payment initiation services (www.dnb.nl/en/sector-information/open-book-supervision/open-book-supervision-sectors/payment-institutions/integrity-supervision/transaction-monitoring-requirements-for-payment-initiation-services-service-7/) and the Financial Conduct Authority's FCA's approach to Payment Services and Electronic Money (FCA (2017)).

Broadly, the project team considers that such a regime should include the following three sets of requirements:

a. **Systems and controls:** AEs should be subject to robust systems and controls requirements to ensure the reliability and security of their operations. This includes implementing adequate risk management systems, cyber security measures and internal controls. AEs should also have mechanisms in place to monitor and address any potential operational risks that could impact the provision of services to end users.

b. **Governance:** to promote effective oversight and accountability, AEs should be subject to comprehensive governance requirements. This may, for example, entail establishing a clear organisational structure with defined roles and responsibilities. AEs should also maintain policies and procedures that align with sound governance practices, such as compliance protocols.

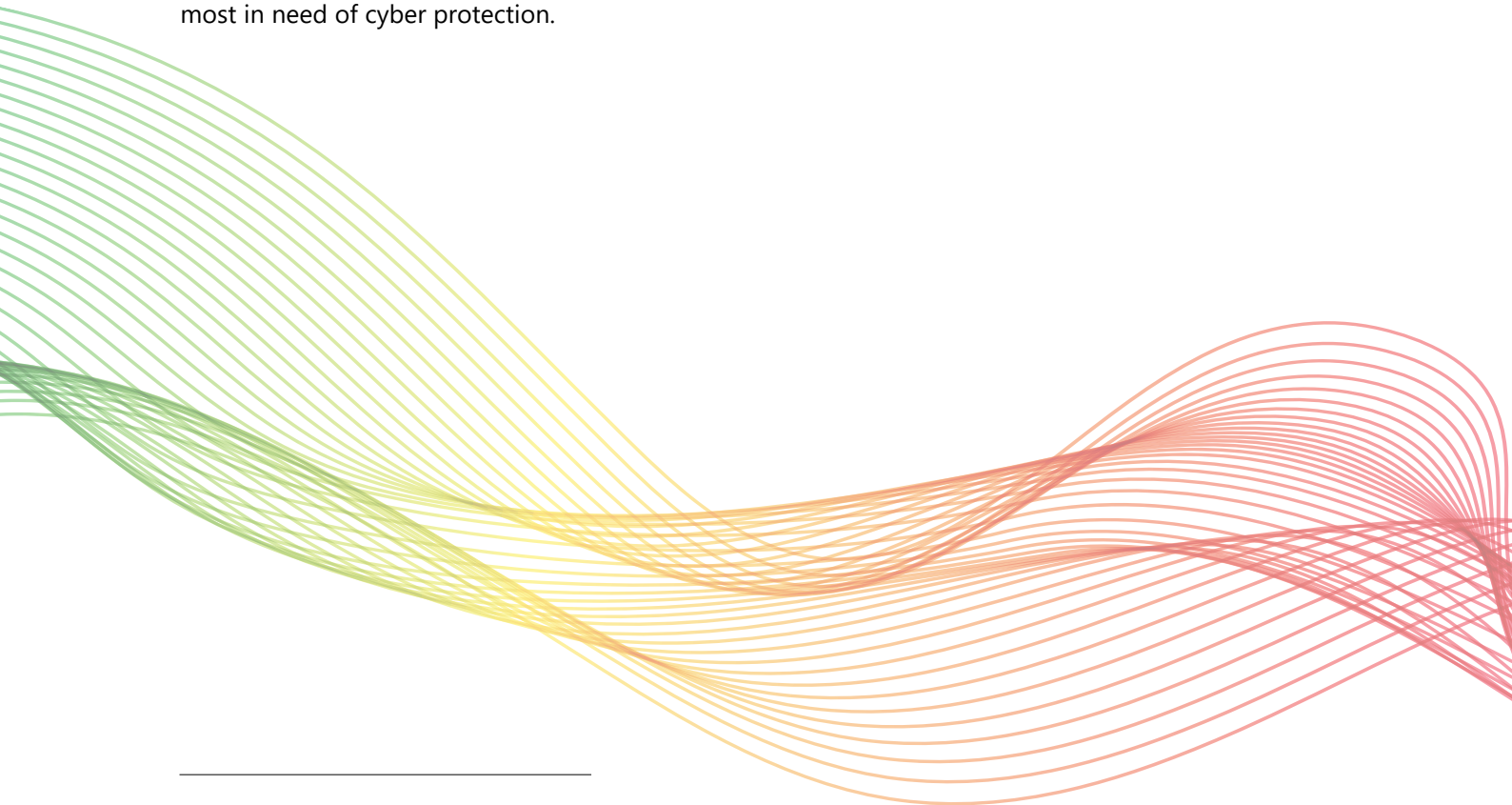
c. **Operational capital:** while AEs would not need to hold capital or liquidity that are calculated by reference to customer funds held, they should, like any other regulated entity that provides a critical service, maintain sufficient capital to ensure continued technical operation for a specified period. A potential approach could be to set capital requirements at the higher of a base amount, or the costs of operating the AE's business for a minimum specified period. This would ensure that AEs have the necessary financial resources to sustain their operations and provide the desired level of service for a sufficient amount of time, even if they need to shut down and have their customers transition to alternative providers.

The proposed core focus of a prudential regulatory regime for AEs balances the need for AML/CFT, technological soundness and customer protection procedures with the unique characteristics of these intermediaries. By focusing on systems and controls, governance requirements and operational capital provisions, this framework would ensure that end users can enjoy a similar standard of services in an rCBDC system as in the existing system.

5. Cyber considerations

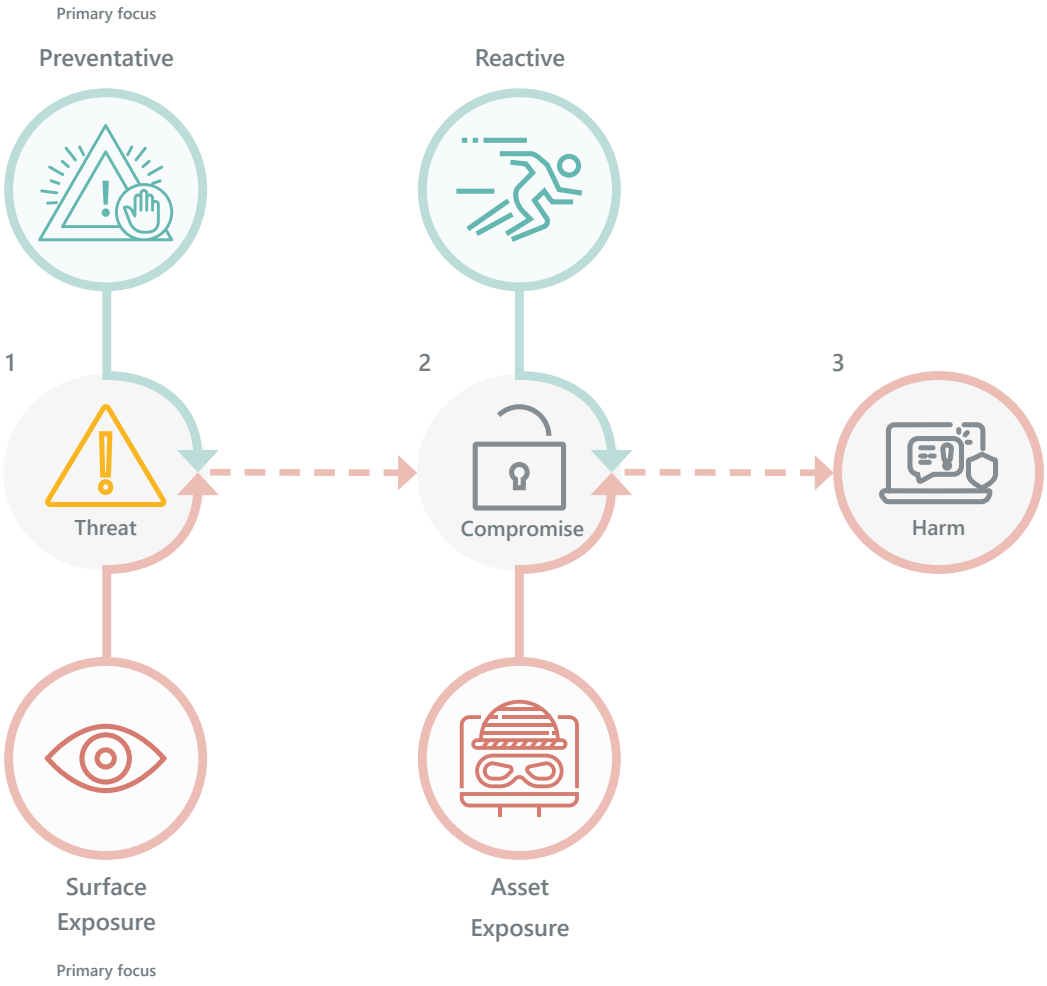
With increasing digitalisation, cyber security has become a top priority for critical infrastructure in financial markets.[45] Security risks may be particularly pronounced for novel rCBDC systems. Given the critical role that central banks play in the financial system, the large volumes of PII involved and the financial value stored on the system, an rCBDC platform can be an attractive target for hostile actors.[46] Perpetrators are wide and varied and can include anything from malicious end users, hackers and criminal organisations to nation state actors. Attacks could have far-reaching consequences, including general disruption or outage in the availability of services, loss of funds, compromise of sensitive data, counterfeiting or reputational damage to the central bank. Tailored frameworks such as the security and resilience framework outlined in Project Polaris provide useful references for assessing and mitigating these risks.[47]

Cyber risks may be even more pronounced in Sela's accessible architecture, as a system with wider access could increase exposure to cyber security threats and is conceivably harder to defend than one with limited access. The cyber security workstream consulted on how to ensure that a widely accessible system does not come at the expense of greater cyber security risk. Cyber security is a broad and complex topic with many dimensions, from hardware and software to social engineering. A complete cyber analysis within the project's six-month timespan was not feasible. The scope was therefore narrowed to best practices in application-level preventative design (Graph 7), focusing on the rCBDC platform components with the highest value and thus most in need of cyber protection.



45. CPMI and IOSCO (2016).
46. See BoE (2020) and Atlantic Council (2022).
47. See BISIH (2023b).

Graph 7 – Preventative cyber focus[48]



The most critical components in Sela's rCBDC ecosystem are the point of transaction settlement – the rCBDC ledger – and end users' rCBDC balances and the devices through which they access and authorise transactions on the platform. Components operated by the central bank in Sela such as the rCBDC ledger fall within the same cyber security perimeters as those in existing payment systems, where the central bank interacts only with financial institutions. In Sela, while the direct connections to the central bank are expanded to include a new type of intermediary (AEs), this represents an incremental step in the scale of direct connections compared with the exponential increase that would be needed if the central bank were to directly receive requests from all end user devices. Furthermore, a risk-oriented approach to

48. The causes and correlates of cyber harm can be broken down by different latent factors as detailed in a model for the quantification of cyber risk by Woods and Böhme (2020). Under this model, the evolution from a cyber threat to a compromise, and subsequently to real harm, is influenced by surface and asset exposure and interventions such as preventative and reactive security. These interventions, along with other measures that system operators can take to ensure security, are further expanded upon in the seven-step security and resilience framework of Project Polaris covering preventative measures, detection, containment, and recovery. In project Sela, we focus on preventative measures.

programmability was taken in Sela, limiting execution on the rCBDC ledger to mitigate cyber threats, and instead relying on the rCBDC platform's coordination of application logic executed at the AEs (a less mission-critical environment) through messages and transaction payloads. When considering the security of end user devices, Sela's architecture relies on existing standards and solutions in production-grade financial services application such as trusted execution environments (TEEs) for key storage and device protection.

Proper safeguarding of the rCBDC ledger and end user devices can leave little room for the layers in between these critical components to impact the cyber security apparatus of the platform. However, additional complexity in the communication channels between end users and the rCBDC platform – notably the presence of AE intermediaries – still represents potential for a larger attack surface. These risks are mitigated in Sela by AEs' inability to hold, or to initiate movement of, end user funds, ensuring minimal damage even in the event that an AE is compromised. Furthermore, flexibility and redundancy of user access through a one-to-many mapping to AEs enables users to move freely between them and reduces the impacts of service disruption at any individual AE. Finally, transaction data is distributed among an end user's different AEs, removing single pools of sensitive information outside the rCBDC ledger.

Sela's preliminary cyber security findings suggest that, through preventative design and the application of cyber security best practices, increased access does not necessarily come at the cost of greater cyber security risk. Special attention in Sela was placed on the design and use of authentication and authorisation structures, key management using hardware security modules (HSMs) and TEEs, and a risk-oriented decomposition of programmability. The following subsections describe how these measures were used in the PoC to provide preventative cyber security, concluding with some considerations surrounding deployment tools and existing services for implementation.

5.1 Authentication, 2FA, TLS and mTLS

While the concepts of authentication and authorisation are similar and often grouped together, their distinction is important in the context of Sela. Authentication refers to the process of verifying identity, while authorisation refers to the granting of permissions to access a resource.[48] With multiple participants and components interacting in an rCBDC system, understanding the trust nature of the relationships and allowing data to securely cross over these trust boundaries is critical to the overall system's cyber security.[49] Ensuring that each participant is communicating with the desired counterparty relies on strong authentication mechanisms, which can be tailored to allow for wider access in the rCBDC ecosystem without compromising cyber security.

48. See www.okta.com/identity-101/authentication-vs-authorization/.

49. A trust boundary can be thought of as line drawn through a program, with untrusted data on one side of the line and trusted data on the other. See https://web.archive.org/web/20110519233053 /https://www.owasp.org/index.php/Trust_Boundary_Violation.

In Sela's architecture, trust relationships are "chained" between the central bank, AEs and end users through overlapping authentication protocols (Graph 8). The rCBDC ledger authenticates AEs, which in turn authenticate end users. This supports wide access to the platform, as no single entity needs to authenticate all end users – a task that would be both operationally challenging and undesirable from a cyber security perspective to the extent that it would lead to a concentration of sensitive PII. It also preserves accountability by preventing malicious behaviour and cyber threats at each level. The AE can establish robust authentication mechanisms with its end users and identify and counter malicious activities with punitive measures. On the other hand, as there is no direct relationship between the central bank and end users, it would be difficult for the central bank to identify a malicious end user. However, because the central bank can establish robust authentication mechanisms with AEs (and identify, and take appropriate action, if an AE is compromised by, for example, revoking access to the platform), this establishes a flexible chain of trust to the end users that also supports wide access. The AE, on the other hand, has a direct relationship with the end user and can counter malicious activities with punitive measures.

The authentication protocol between AEs and end users should be implemented by a trusted authentication service provider, with a preference towards two-factor authentication (2FA). 2FA is a security process that requires users to provide two independent forms of identification for authentication, such as a password and a biometric identifier (eg face ID).[50] To enforce strong authentication protocols with end users, a requirement for AEs to implement commonly used 2FA service providers (which are sufficiently secure) can form part of the overall AE regulatory framework.

Once authenticated, the communication has end-to-end security over the network through a protocol called Transport Layer Security (TLS).[51] Communication between end user devices and AEs are secured through one-way TLS connections, and communication between AEs and the central bank is secured using mutual TLS (mTLS). TLS and mTLS protocols ensure that, through proper encryption, no machine can access resources that it has not been authenticated to access, which prevents "man-in-the-middle" and other cyber security attacks. That said, since TLS and mTLS protocols are not perfect and are constantly evolving with new vulnerabilities being detected, staying up to date on the latest TLS implementations is critical to ensuring cyber security effectiveness.[52]

---

50. Authentication elements are categorised as possession, knowledge or inherence. Possession refers to something you have, knowledge to something you know, and inherence to something you are. 2FA provides two out of the three factors and should come from separate sources.
51. For example, web services use the TLS protocol to secure all communications between servers and web browsers. See NIST (2019).
52. See NIST (2019).

5.2 Authorisation, HSMs, enclaves and TEEs

Authorisation in Sela is done directly between the end user and the rCBDC platform, providing trusted and non-repudiable transactions on ledger.[53] Only transactions initiated and signed by the correct end user are authorised by the rCBDC platform, verified by validating the presence of that user's signature on each transaction initiation request and ensuring the appropriate permissions. AEs also sign these transactions to indicate their endorsement after they have performed the necessary compliance checks. The design prevents AEs from moving an end user's funds without their approval and is the technical implementation that allows end users to hold their own rCBDC funds. This not only serves to support wide access by reducing entry barriers for AEs (through potentially less stringent capital and liquidity requirements), but it can also lead to a more secure rCBDC ecosystem as compromised AEs would not be able to move customer funds. Together with chained authentication, direct authorisation provides a secure and flexible system design that supports access.

Sela's architecture puts significant emphasis on the safekeeping of cryptographic key pairs for authorising and signing transaction requests. Two methods to securely store and use the keys of the different participants in the Sela ecosystem were explored in the PoC – HSMs for the central bank and FIs, and TEEs for end users. Keys are generated inside the respective modules, are used only within the module itself and require the rightful owner's authentication. A reference architecture implementation for enclaves for the AEs was part of the PoC's technical build, and HSMs were emulated (Graph 8).

5.2.1 HSMs

In Sela, the PoC emulated HSMs commonly used in enterprise systems to protect the central bank and FIs' cryptographic keys. These HSMs handle the encryption and decryption processes and create and verify digital signatures for authorisation. All transactions involving an HSM are logged to create an audit trail.

HSMs are specialised physical hardware devices used to store and manage cryptographic keys securely, and to provide a high level of protection against attacks such as key theft and tampering. These devices provide cryptographic keys for critical functions such as encryption, decryption and authentication, which are necessary for the use of applications, identities and databases. HSMs keep cryptographic functions separate from regular application operations. They can be plugin cards or embedded in other hardware such as smart cards, appliances and external devices, and can be connected to a network server or used as a standalone device offline. Furthermore, HSMs can be used concurrently to provide faster services for high throughput or low-latency applications. Since HSMs are hardware-dependent, they were not included in the scope of the current PoC.

53. In the context of cyber security, non-repudiation ensures that the sending party cannot deny the validity of a message due to the authenticity of the signature.

HSM devices are not always suitable for cloud environments. For example, cloud service providers may require customers to use HSMs hosted in their data centres, as using a device on premise can cause connectivity issues that introduce unwanted latency in the system. As such, Key Management as a Service (KMaaS) has emerged to secure encryption keys across different cloud environments. These services offer centralised, on-demand HSM-level tools without the need to provision hardware.[54] Sela used KMaaS services as part of the enclaves for AEs detailed in Section 5.2.2.

5.2.2 Enclaves

One possible way to ensure a baseline of secure functionality and to reduce intermediaries' entry barriers is to provide tamper-proof executable environments that have been tested and verified. For example, the central bank can, through executable environments, provide AEs with the ability to refresh their own cryptographic keys, enabling it to distribute functionality to AEs in a manner that is verifiable by the central bank. In Sela, key management embedded in an enclave was implemented in the PoC as an example of how the rCBDC system operator can provide tools to the intermediaries in the ecosystem to reduce their operational burden. Management of cryptographic keys is a necessary function common to all AEs and can be a potential barrier of entry to smaller payment service providers who lack the experience in managing the keys themselves. An enclave with key management logic that connects with AEs' private keys embedded within a KMaaS was provided to AEs in the PoC. This can reduce entry barriers, but also provide a baseline for key management across AEs that ensures flexible and adequate preventative cyber security measures are implemented as needed.

In the Sela architecture, we assume that AEs will be largely cloud-based. Enclaves were therefore implemented to provide key management for AEs using EC2 Nitro Enclaves (as deployment is done on AWS).[55] Enclaves are separate, hardened and highly constrained virtual machines. They provide secure local socket connectivity only with their parent instance, which in Sela's case is the AE rCBDC application – see Section 6.1.3.2 for more details. They have no persistent storage, interactive access or external networking, which means that users cannot connect the administrative console to an enclave directly, and the data and applications inside the enclave cannot be accessed by the processes, applications or users (root or admin) of the parent instance.[56] Enclaves can be thought of as a wrapper around a KMaaS with additional functionality.

A signature provided by an enclave presents an opportunity to streamline any software development kits (SDKs) or baseline sensitive functions at the AE backend level. AEs' private keys cannot be retrieved from the enclave. Enclaves integrate with the KMaaS (in this case AWS Key Management Service), where AEs' private keys can be generated by "burning" them into their unique enclave image.

---

54. Major cloud service providers, such as AWS, Google, IBM and Microsoft, offer cloud KMaaS products, along with smaller companies like Entrust and Thales.
55. Other cloud providers have similar solutions.
56. See https://docs.aws.amazon.com/enclaves/latest/user/nitro-enclave.html.

Enclaves also include cryptographic attestation for the software running in them, ensuring that only authorised code runs in the enclave.[57]

5.2.3 TEEs

In Sela, end user devices are equipped with TEEs – commonly used technology to enhance wallet security in mobile devices – to protect users' cryptographic keys and to handle the encryption and decryption processes. For example, even if an end user's mobile device is compromised, its keys cannot be used without the rightful owner's authentication with the device.[58] TEEs also create and verify digital signatures, and all transactions involving a TEE are internally logged to create an audit trail.

TEEs are secure areas of a device's hardware that are isolated from the main processor. They can help protect sensitive data and cryptographic keys from malware and other attacks.[59] While a TEE is separated from the device's primary processing environment, a trusted application running in a TEE can operate within a dedicated memory region.[60] Applications contained within a TEE are separated through software and cryptographic functions and can be configured to accept only authorised code. Although not completely free of vulnerabilities,[61] TEEs can help to prevent malicious actors from accessing a secret key or from compromising the execution instructions of the application.

While the implementation of a TEE varies depending on the use case, the fundamental concepts remain the same, focusing on trust, security and the isolation of sensitive data. TEE technology offers several essential services, such as (i) secure peripheral access, which allows direct access and protection of peripherals such as touchscreens, displays, fingerprint sensors, cameras, microphones and speakers; (ii) secure communication with remote entities, which allows secure data, communication and cryptographic operations (private and public keys for encryption are stored, managed and used only within the secure environment); and (iii) support of trusted device identity and authentication protocols, with some using roots of trust to enable the verification of a device's legitimacy by connected services in which it is attempting to enrol.

57. See https://docs.aws.amazon.com/kms/latest/developerguide/services-nitro-enclaves.html.
58. For example, even if a user's phone is stolen, the token that represents the user's credit card information on a smart wallet can only be accessed by logging into the phone – something that would need biometrics or a user-generated password.
59. See Project Polaris, BISIH (2023e).
60. It should be noted that TEEs are present in smartphone devices, but may not be present is simpler mobile devices.
61. See Munoz et al (2023).

5.3 Data management and encryption

5.3.1 Data management

As a critical retail payments infrastructure, an rCBDC system like Sela can involve the accumulation of large amounts of PII, and proper data management is paramount to safeguarding the cyber security of an rCBDC system. PII is generally considered to be the most sensitive form of data, and is defined as any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct (eg name, social security number, date and place of birth, mother's maiden name, biometric records) and indirect means (eg medical, educational, financial, and employment information).[62] Furthermore, PII data can be classified into many different categories based on their confidentiality and impact levels. Breaches involving PII can result in identity theft and blackmail for individuals, and loss of public trust, legal liability and remediation costs for organisations.

Protecting PII in a CBDC platform requires many different operational and privacy-specific safeguards and security controls. A few examples based on NIST recommendations[63] were considered in Sela's design:

1. ***De-identifying records*** *by removing enough PII such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. De-identified records can be used when full records are not necessary, such as for examinations of correlations and trends.*

2. *Taking into consideration the* ***location of PII****. When the PII is regularly transmitted or transported offsite, there are more opportunities to compromise the confidentiality of the PII.*

3. ***Providing transmission confidentiality*** *by encrypting the communications or by encrypting the information before it is transmitted.*

In Sela's architecture, the PII that is sent to the rCBDC ledger operated by the central bank, national identifiers, is de-identified by AEs using a hash function called *h().h()* is a one-way function[64] that takes as input the national identifier (ID) and returns *h(*ID*)* with no possibility of obtaining ID from *h(*ID*)*.[65] This preserves the privacy of the national ID holder from the central bank and provides a pseudo-anonymous account mapping of the end user to the rCBDC account.[66]

---

62. See www.dol.gov/general/ppii#:~:text=Personal%20Identifiable%20Information%20(PII)%20is,either%20direct%20or%20indirect%20means.
63. See NIST (2010).
64. A function f : {0,1}* → {0,1}* is one-way if f can be computed by a polynomial time algorithm, but any polynomial time randomised algorithm F that attempts to compute a pseudo-inverse for f succeeds with negligible probability.
65. If the number of possible IDs is sufficiently small, a brute force attack would be possible.
66. Pseudonymisation of data is defined as replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified. See Article 4(5) of the GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504.

Additionally, the hash function ensures that no two IDs map to the same hashed output, meaning that no two national identifiers map to the same account, providing the uniqueness of rCBDC accounts.[67] Storing a hashed version of a user's information on the rCBDC system does not, however, guarantee the full privacy of end users from the central bank and a live implementation would need to consider further measures to guarantee such full privacy.[68]

Measures were also taken in the Sela architecture to consider the location of the PII, including avoiding the concentration of PII in a single location and keeping the transmission of PII to a minimum. As AEs handle all customer-facing operations and end user authentication, PII is distributed and safeguarded across the various AEs of each end user. The central rCBDC ledger stores only pseudo-anonymous account identifiers and their related transaction histories, and no additional PII (such as information needed for KYC compliance) is sent to or stored in the rCBDC ledger. This avoids a central pool of PII data as a potential attack vector (Graph 8). Furthermore, the use of TLS and mTLS (as discussed above) ensures transmission confidentiality by securing and encrypting traffic/ communication over the rCBDC network.

5.3.2 Key cryptography

The Sela rCBDC platform uses Elliptic curve cryptography (ECC) algorithms for digital signatures and encryption for secure end-to-end communication. ECC is a type of public key cryptography based on the algebraic structure of elliptic curves over finite fields, used for digital signing, encryption and key exchange. Public key cryptography, also known as asymmetric cryptography, is a cryptographic protocol that uses a pair of mathematically related keys to perform various security functions.[69]

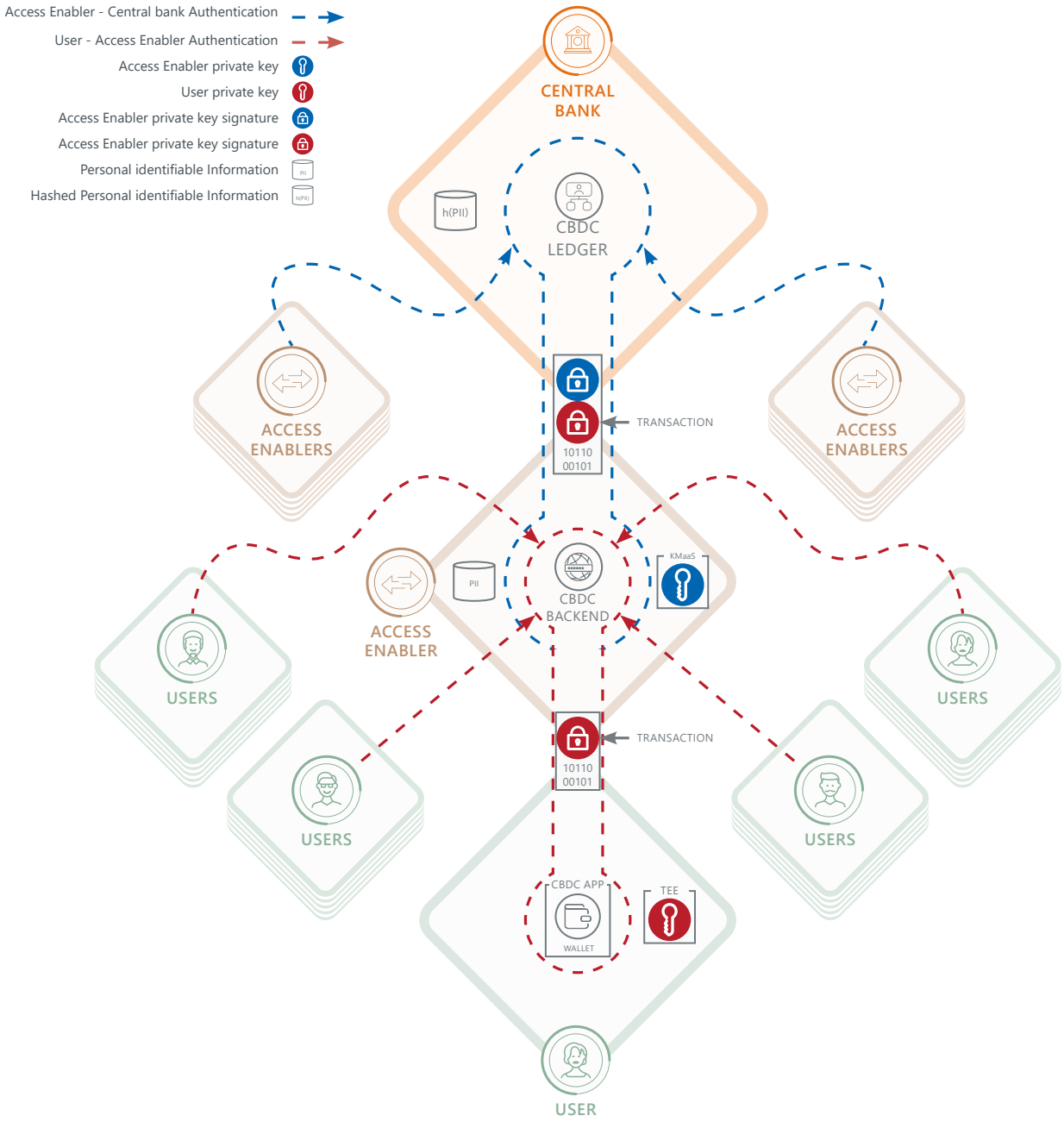
ECCs work by creating a private key from a secret number and a public key from deriving a point on an elliptic curve. Sela implements two different elliptic curves, P256 and the Edwards curve 25519, that provide signing schemes ECDSA and Ed25519 respectively. Both generate keys used to sign and verify digital messages. ECDSA is based on the prime 256-bit modulus, used for key exchange and digital signatures, and is recommended by NIST. Ed25519 is a different type of algorithm, and is used mostly for digital signatures, sometimes being considered more secure than P256. These schemes were chosen for compatibility with reference architectures for iOS- and Android-based devices.

---

67. Many functions qualify as hash functions, and each will render different outputs. It is therefore important to align on a common hash function across all the AEs. In the PoC a simple SHA256 hash function was used. Furthermore, as noted in Section 3, Sela assumes the existence of a unified national ID system.
68. Other privacy-enhancing technologies such as adding biometrics to the national ID or the use of zero knowledge proofs are an area for future exploration. See, for example, the privacy-enhancing technologies section of BoE (2023c), Project Tourbillon: www.bis.org/about/bisih/topics/cbdc/tourbillon.htm, and Phase 2.0 of Project Aurum (upcoming).
69. See more in NIST (2023).

In Sela, users generate their own cryptographic key pair during the onboarding process. Private keys are kept confidential, while public keys are shared with the rCBDC platform when onboarding. This provides an end-to-end ability to verify signatures between users, AEs and the central bank as the platform operator.

Graph 8 – Cyber security components



5.4 Programmability and cyber security

A key draw of digital payments is the wide range of potential use cases they can deliver through programmability. In Sela, a risk-oriented approach to programmability was taken, limiting direct execution on the rCBDC ledger to mitigate cyber threats, and instead relying on the rCBDC platform's coordination of application logic executed at the AEs through messages and transaction payloads.

The notion of programmability can be broken down into three distinct functions – automation, conditionality and composability. Automation refers to the ability to execute an action in a way that reduces human intervention, while conditionality refers to the ability of an executing code to contain complex conditional logical statements.[70] These conditional statements often rely on external data sources as inputs. Finally, composability is the ability of one logical code execution environment to trigger another, and can enable long chains of code execution that can pass parameters between each other to form long chains of executed logic. When considering these three subfunctions of programmability, special consideration was taken in Sela regarding whether and how to implement this logic and the appropriate division of responsibilities between the rCBDC ecosystem participants.

Having a general compute environment on the rCBDC ledger itself introduces a wide range of risks, as outlined in the Project Polaris analysis of recent attacks in the DeFi space.[71] This is because a general-purpose Turing-complete execution environment[72] provides the ability for a potential attacker to run any desired logic it wants and is harder to defend.[73] As a result, in Sela's architecture the rCBDC ledger does not support a general compute environment, effectively removing the ability of the ledger itself to run executable code. These execution environments instead reside with the AEs, who can provide the conditionality part of programmability as a service in a far less mission-critical environment and in a business application context that is more relevant for the end user. This has an additional computation and implementation benefit for the central bank, as it would otherwise require the central bank ledger to store a large volume of business logic, which could become prohibitively expensive to manage.

The Sela rCBDC ledger instead supports automation (in the form of automated event triggers between users) because of its relatively narrow and safe functionality and its prerequisite role for the subsequent functions of conditionality and composability. Sela's architecture enables messaging to be passed through the ledger between users in the form of actions. These actions allow users through their AEs to request the initiation of an action from another user. For example, an RTP function was implemented – see Section 6.2.7 for the detailed flow. In its simplest form, an RTP is a message from the payee requesting the payer to initiate a payment. The request itself can contain the actual unsigned message payload (already approved by the payee), which reduces the operational requirement on the payer, since all they need to do is sign the message and submit it to the rCBDC ledger for execution.

---

70. While most automation has some degree of conditionality in the form of a control loop (eg a tea kettle that stops heating water when the steam pressure causes a switch to flip the breaker), conditionality in our case refers to the ability of an executing code to contain complex conditional logical statements.
71. See Part 3 of BISIH (2023b).
72. In computability theory, a system of data-manipulation rules is said to be Turing-complete if it can be used to simulate any Turing machine within the unbound time and space. This is widely used as the definition of a general-purpose computer.
73. While a Turing-complete exploit can be extremely dangerous, this does not imply that a non-Turing-complete exploit would be less dangerous, only easier to defend against.

This messaging ability is arguably a first step to supporting simple automation programmability, in addition to the transaction settlement provided on ledger. With this, further work can be done on augmenting the platform with a limited scope for isolated conditional execution environments and, ultimately, composable ones.

5.5 General considerations

In addition to the application design considerations outlined above, the cyber security workstream also discussed other deployment-specific tools that, despite not being implemented in the PoC due to time constraints, are worthy of consideration. For one, network isolation of each component in the rCBDC ecosystem should be of high priority and can be supported using next-generation firewalls. In addition to the traditional internet protocol (IP) and port access list, these firewalls provide intrusion protection, anti-virus and file sandboxing, secure sockets layer (SSL) inspection and application controls, among others. These network firewalls can be deployed at the physical point of deployment or virtually.[74]

Furthermore, data stored on cloud data centres are critically important and a broad range of cloud-native application protection platforms (CNAAP) should be used to provide the appropriate protection. These include functions such as cloud security posture management to identify cloud configurations that do not match the company policy (eg an Amazon S3[75] bucket which is open publicly instead of being protected) and, to protect runtimes, a cloud workload protection platform such as containers, virtual machines and lambda functions.[76] These workload protections dynamically patch vulnerabilities over time and constantly monitor runtime behaviour. Web Application and API Protection is another example function, which can be used to provide schema validation and threat prevention based on API calls.

In addition, data layer protection tools can be used to guard sensitive data such as PII by enforcing control policies on where and how data are transported. Server endpoint protection can also be considered to provide phishing protection, zero-day protection, risk assessment, vulnerability and patch management, and ransomware protection.

While these measures can further enhance the protection of an rCBDC system, they may not alone be sufficient to prevent all threats. A security operations centre (SOC) that can aggregate potential threats and provide extended detection and response is often also needed to automate the investigation of issues and their appropriate handling. For example, if a suspicious IP address is found, it should be blocked in the firewall, in the cloud protection and in the endpoint protection service.[77] Together with the processes and cyber components described in the previous subsections, these additional measures can form part of an overall cyber security and resilience framework for an rCBDC system such as Sela.

---

74. For more details, see Check Point (2023).
75. See: https://aws.amazon.com/s3/.
76. See: https://aws.amazon.com/lambda/.
77. See: www.checkpoint.com/downloads/products/horizon-xdr-xpr-solution-brief.pdf.

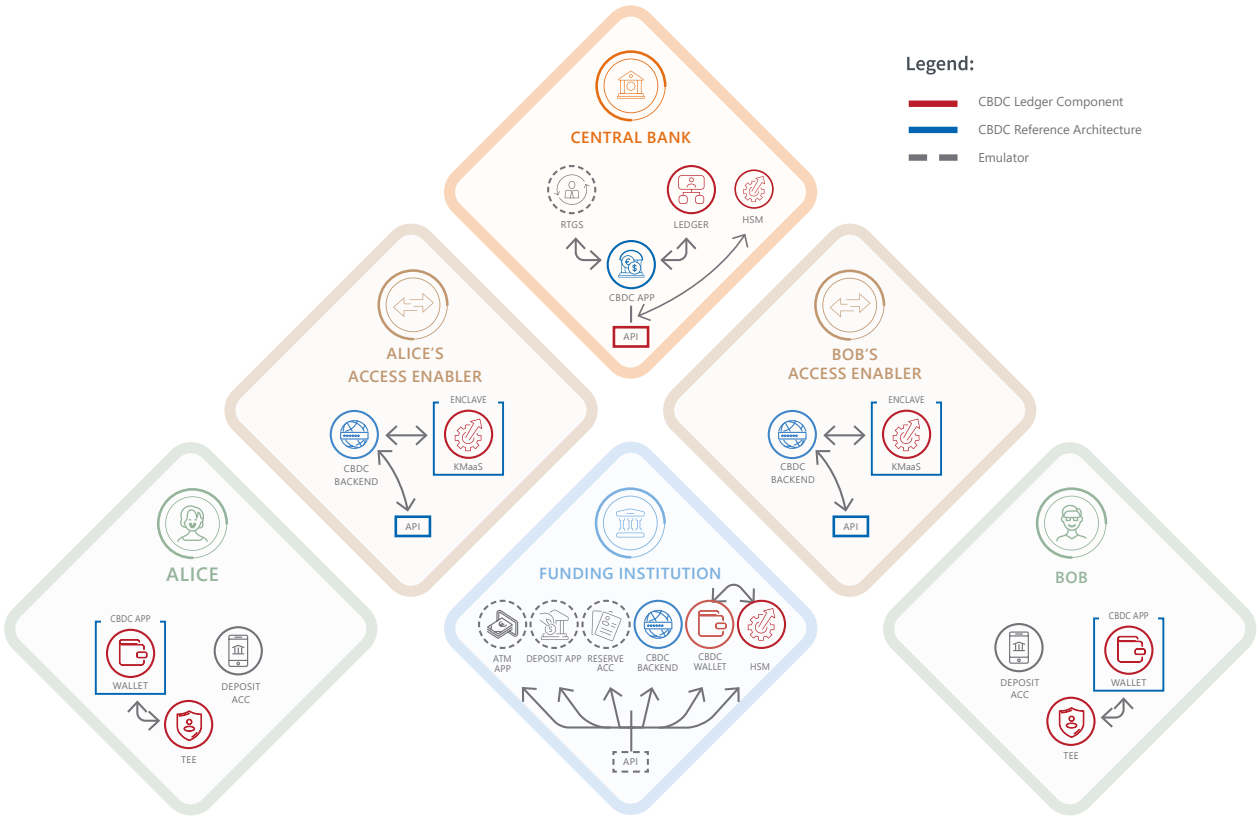
6. Technology: PoC implementation

Guided by the global rCBDC body of work and the considerations and outcomes of the policy, legal and cyber security workstreams described above, the technology workstream then built the PoC for Sela's accessible and cybersecure rCBDC ecosystem. The following section outlines the considerations of this final workstream and the PoC's technical implementation. It provides an overview of the ecosystem participants and components, and the detailed flows of rCBDC use cases.

6.1 rCBDC ecosystem participants and components

The main participants in the Sela ecosystem include (i) a central bank that operates the rCBDC ledger, the central-bank rCBDC application and the RTGS system; (ii) FIs that take consumer deposits and operate ATM networks; (iii) AEs that provide rCBDC services and wallets to end users through their own rCBDC backends; and (iv) end users who hold their own rCBDC through their mobile devices, or any other end factor such as a personal computer (PC) or a point-of-sale device etc (Graph 9).

Graph 9 – Participants and components



6.1.1 Central bank: rCBDC platform and RTGS system

The central bank plays a core role in the Sela architecture. First, it issues and redeems the rCBDC on the rCBDC platform that represents its direct liability. Second, it operates the rCBDC platform and provides real-time and instant settlement to anyone transferring rCBDC, meaning that all retail transactions are executed by the central bank on the rCBDC ledger. This ensures that, at all times, the rCBDC remains a claim on the central bank (and not on private sector intermediaries). The central bank also enables access to the platform for FIs and AEs and determines rules and governance requirements for participants. In addition to these new responsibilities, the central bank in Sela continues to act as an RTGS account provider to FIs (or other entities) that manage end users' deposits of private money.

6.1.1.1 rCBDC ledger

The rCBDC ledger run by the central bank forms the core of the Sela rCBDC platform PoC. It is a private, permissioned and account-based DLT system that stores a pseudo-anonymous and unique representation of each user registered on the network, along with a non-negative account balance. While the DLT in Sela's PoC is run centrally by the central bank, the operational role of running the ledger could be decentralised by, for example, allowing FIs or AEs to run nodes. Decentralisation may be desirable for operational or security reasons, but the trade-offs would need to be closely evaluated.

Transfers on the ledger are effectively account balance updates that conform to the rules of settlement in the ledger.[78] Any update to the state of the ledger is recorded as part of a new block, making it immutable and final. This forms the basis for the technical transaction finality that underpins legal transaction settlement on the ledger, ensuring real-time and instant settlement for every rCBDC transfer. Each transaction is initiated and digitally signed by the end user and endorsed by a digital signature of the user's AE. These signatures are stored on the ledger as part of the transaction to ensure non-repudiation of transactions and a form of central bank accountability to end users.

To support the scale and responsiveness of retail payments, the ledger supports over 450,000 transactions per second with subsecond latency on transactions.[79] It does so by using a variant of the PaLa consensus algorithm[80] that has been optimised for high throughput and low latency, and by keeping programmability largely outside the ledger (recall Section 5.4).

Management of permissions for participants on the ledger is conducted through a role-based access control (RBAC) system. Each role consists of a set of rules defining permissions on resources, such as accounts. For example, a central bank would have "create", "read" and "update" permissions on an AE account, meaning that it can manage AE administrative data, while an AE would have only the "read" permission on its own account.

---

78. For example, the amount debited from the payer's account must equal the amount credited to the payee's account.
79. See M10 (2021).
80. See Chan et al (2018).

Any attempt by an AE to change AE-related data, such as its own permissions, on the platform would fail since it does not have the proper permissions. Roles can be assigned to or revoked from a participant with a simple request. Once a role changes, the effect is immediate at all levels of the platform. As the RBAC system is part of the ledger, it has the same security guarantee as any other transaction on the ledger. Each change on the RBAC system is recorded permanently in a new block, which facilitates the auditing process of RBAC management.

In addition to providing transfer functionality (moving funds between accounts), the ledger also provides actions, which facilitate the movement of messages between accounts. Actions are effectively a payload with content defined by the initiating party[81] that is sent to individual accounts on the platform. Ecosystem participants with read access on an account can be automatically notified of any actions on that account. Actions allow subscribed entities to receive messages in real time relating to a certain account. They therefore provide the building blocks for automation on the platform and a way for the rCBDC system to enable AEs to coordinate events and provide multi-party services. The RTP example outlined in Section 3.4 shows how actions enable message transfer and automation to coordinate functions across different AEs.[82] See also Section 6.2.7 for the detailed RTP flow.

The ledger is written in the Rust programming language to provide performance, type safety and concurrency out of the box. API requests to the ledger are done via a RESTful APIs gateway, making integration easy and accessible, while internal messages between the various micros service components within the platform use the gRPC protocol.[83]

6.1.1.2 Central bank rCBDC application

The rCBDC application is hosted by the central bank outside the ledger and provides the business logic for the rCBDC platform. It coordinates between the rCBDC ledger, the external-facing API and other components operated by the central bank, such as the RTGS system. For example, it supports FI and AE onboarding, user account management, processing of rCBDC issuance and redemption requests and coordination of transactions between RTGS accounts and the rCBDC ledger.

This application allows authorised ecosystem participants, such as AEs and FIs (and other regulated and approved integrations), to send requests to the rCBDC ledger to, for example, create rCBDC accounts and issue and redeem rCBDC, through a RESTful interface and OAuth authentication mechanism. These messages are secured via Ed25519 or P256 cryptographic signatures verified within the ledger itself, and their exchange is coordinated via the internal gRPC message protocol. The application is also written in Rust, packaged as a docker container and deployed on an AWS environment with Kubernetes.

---

81. For example, ISO2022 formatting can be placed on message types.
82. Actions provide similar functionality to a distributed queue such as Kafka. Once an ID is subscribed to a stream, all actions that occur with at-least-once semantics for messages are provided without an external service. See: https://kafka.apache.org/.
83. See: https://grpc.io/.

6.1.1.3 RTGS system

To support the conversion of FI customer deposits and rCBDC, the RTGS system provides simple reserve accounts for FIs with access to the central bank's balance sheet, to convert their reserve balances to and from rCBDC. It therefore plays an important role in enabling fungibility between reserve balances and rCBDC in the Sela ecosystem.

6.1.2 FIs: deposit accounts and ATMs

FIs in the Sela architecture are financial institutions that manage deposits for end users and enable the conversion of bank deposits to and from rCBDC, ensuring interoperability between rCBDC and commercial bank money.

6.1.2.1 Commercial bank deposit accounts

The FI system includes client deposit accounts and a backend system to manage FI reserve accounts in the RTGS system at the central bank. The client deposit accounts provide an API that is used to coordinate functionality with other components of the ecosystem. For example, users through their AEs can make requests via this API to retrieve account data just as in open banking. The FI also has its own rCBDC account at the central bank which it uses to prefund rCBDC to enable fungibility between its customers' deposits, cash and rCBDC (recall Box B).

6.1.2.2 ATM network

FIs also manage the ATM network which, with the help of AEs in routing requests, provides fungibility between cash and rCBDC in the Sela PoC – see Section 6.3.3 for a detailed flow of users converting cash and rCBDC. ATMs also play an important financial inclusion role in the ecosystem by allowing users without bank accounts to convert rCBDC to and from cash. Together with the FI and RTGS systems, the ATM network supports the singleness of money and allows rCBDC to be interchangeable with other forms of money by facilitating the conversion of rCBDC against reserves, FI customer deposits and cash. The ATM application, through the AE and FI, makes requests to the rCBDC application backend and is secured using signed messages with a key stored in a notional hardware enclave built into the ATM itself.

The RTGS and FI systems and the ATM network are all emulators simulating the main functions of each system. These services are developed in the Rust development language and deployed via Docker containers with Kubernetes on AWS. They are enabled through an easy-to-use and exploratory interface that examines the data available for each participant in the ecosystem. Developed using the Retool[84] system, this interface tool provides views of the full data sets of each of the emulators mentioned above.

84. See https://retool.com/.

6.1.3 AEs: back and front-end rCBDC services

With direct access to the rCBDC platform, AEs handle all customer-facing rCBDC operations, including (i) submitting user onboarding requests to the platform after completing required KYC processes; (ii) endorsing/co-signing user transaction requests after completing the required AML/CFT screening; (iii) hashing sensitive user data before they are sent to the rCBDC platform; (iv) retrieving user account information; (v) providing secure authentication with the user; and (vi) facilitating secure authorisation with the rCBDC platform. Furthermore, AEs can notify users of any actions and transfers on their accounts, and coordinate transfers between users' FI deposits and their rCBDC wallet holdings through balance top-ups or waterfalls of excess funds (see Sections 6.2.5 and 6.2.6 for the detailed flows). It is important to note that AEs do not need to have their own rCBDC account to provide rCBDC services to their customers.

6.1.3.1 Front-end services – wallets

AEs provide rCBDC services to end users through wallets. Wallets are the client-side, front-end applications that provide the customer experience surrounding the rCBDC platform.[85] A wallet application is provided by an AE and paired with an AE's respective backend services. The wallet can be tailored to serve many use cases, including for individual retail use or merchant points-of-sale, as outlined in Project Rosalind. A key feature of the wallet application is how it creates, stores and manages end users' private keys. Upon installation, the wallet creates a unique private key in the TEE of the user's device (recall Section 5.2.3). The corresponding public key is then sent to the rCBDC platform during the user onboarding process. If the onboarding is successful, this public key is associated with the user account.

Importantly, the private key counterpart to the public key associated with the end user's rCBDC account is the only key that can sign transactions initiating payments on the ledger. This creates a direct trusted authorisation channel between the rCBDC ledger and the end user device, and ensures that only the end user, and not its AE(s), can move the rCBDC in its wallet (recall Section 5.2). This technical implementation ensures that AEs never hold or control end user funds (even if they are compromised), which is a key attribute defining AEs in the Sela ecosystem. Therefore, unlike the existing monetary system where custodial wallets are the standard in payment instruments, in Sela the rCBDC is, from a technical perspective, held by the end users themselves[86] through self-generated keys in wallets provided by AEs.

85. While the PoC assumed that end users access their wallets through their mobile devices, in a live implementation, they could be accessed through many different forms of devices.

86. See ECB (2023c).

The wallet application communicates primarily with the corresponding AE's rCBDC application backend services via the RESTful API interface, secured with messages cryptographically signed using a private key generated inside the device's TEE. The wallet is written in the Dart programming language using the Flutter framework and packaged as a native application as iOS and Android binaries.

6.1.3.2 Backend services – rCBDC application

Front-end client wallets offered by AEs are supported by the backend rCBDC application, which intermediates between the rCBDC ledger and user-oriented functionality. Through this backend application, AEs can provide programmable payment logic on top of the baseline functionality provided by the central bank. Additionally, these backend services can communicate with each other through the platform's messaging and payload functionality to coordinate between each other. For example, conditional coordinated execution logic such as recurring payments, micro payments, split payments and crowd-funding are a few of the possibilities.

This service is written in the Rust programming language, packaged as a docker container and tested in an AWS environment deployed with Kubernetes.

6.1.4 End users: user devices

End users include any individual or entity in the real economy with retail payment needs like individuals, businesses, merchants and government agencies.[87] Mobile devices (or any other relevant device such as a merchant's point of sale) provide end users with full control over their rCBDC (recall Section 4). This relies on the fact that the only key that can initiate transactions is generated and stored securely on a user's TEE. The private key is used to digitally sign instructions, which are then endorsed and co-signed by AEs before being sent to the rCBDC system for execution.

6.2 Use case flows

This section outlines the main functionalities built and tested in the PoC, including loading and unloading of rCBDC by FIs, exchange of FI deposits and cash to and from rCBDC, rCBDC payments between end users, and automated top-ups or waterfalls when wallet balances are too low or too high, respectively.

6.2.1 FI loading rCBDC against reserves

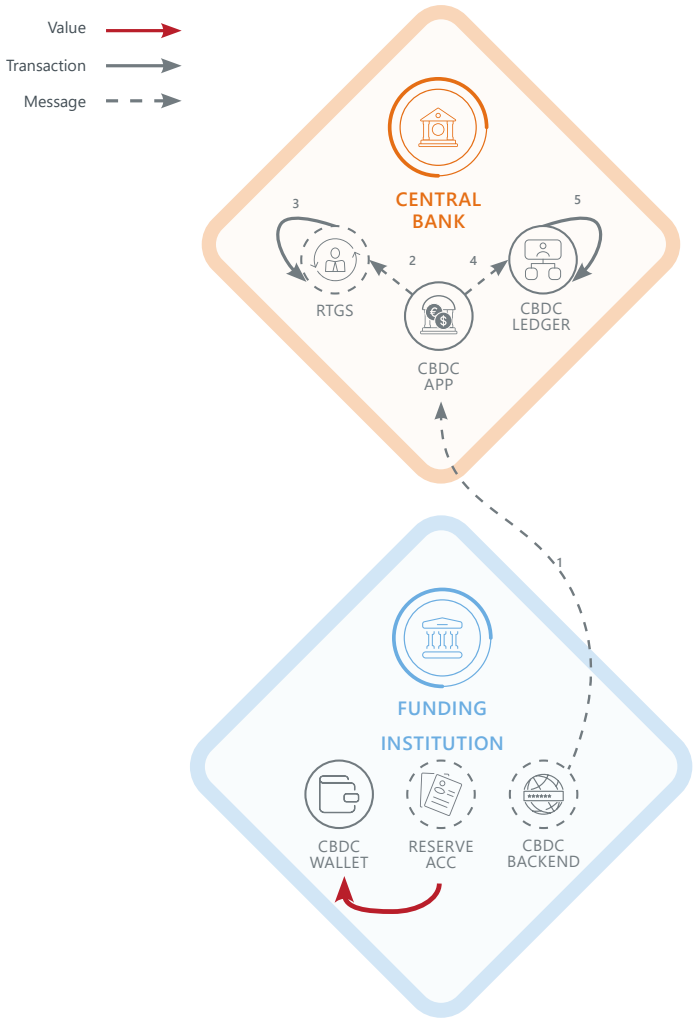
In order to support the conversion of Sela FI customers' deposit account balances to rCBDC, FIs need to first fund their own rCBDC wallets against reserves held at the central bank in the RTGS system.

87. This excludes wholesale users, such as participants with RTGS accounts at the central bank.

This rCBDC "loading" process begins with the FI requesting rCBDC from the central bank through the rCBDC app (step 1 in Graph 10.1). Next, the central bank's rCBDC app requests a transfer from the FI to the central bank's reserve account in the RTGS system (step 2). Once the transfer has been completed (step 3), the app instructs the rCBDC ledger to issue the equivalent amount in rCBDC to the FI's wallet (step 4). The rCBDC ledger executes the transaction by crediting the FI's balance (step 5). This sequence of actions results in the transfer of value from the FI's reserve account to its rCBDC wallet (red arrow).

The FI now has rCBDC funds in its wallet to support the conversion of its customers' deposit balances and end users' cash to rCBDC. This process can be automated with the FIs setting watermarks to automatically load rCBDC from the rCBDC system to better support liquidity and variations in end user demand for rCBDC. The "unloading" of the FI's rCBDC back to reserves follows roughly the reverse flow.

Graph 10.1 – FI loading rCBDC against reserves



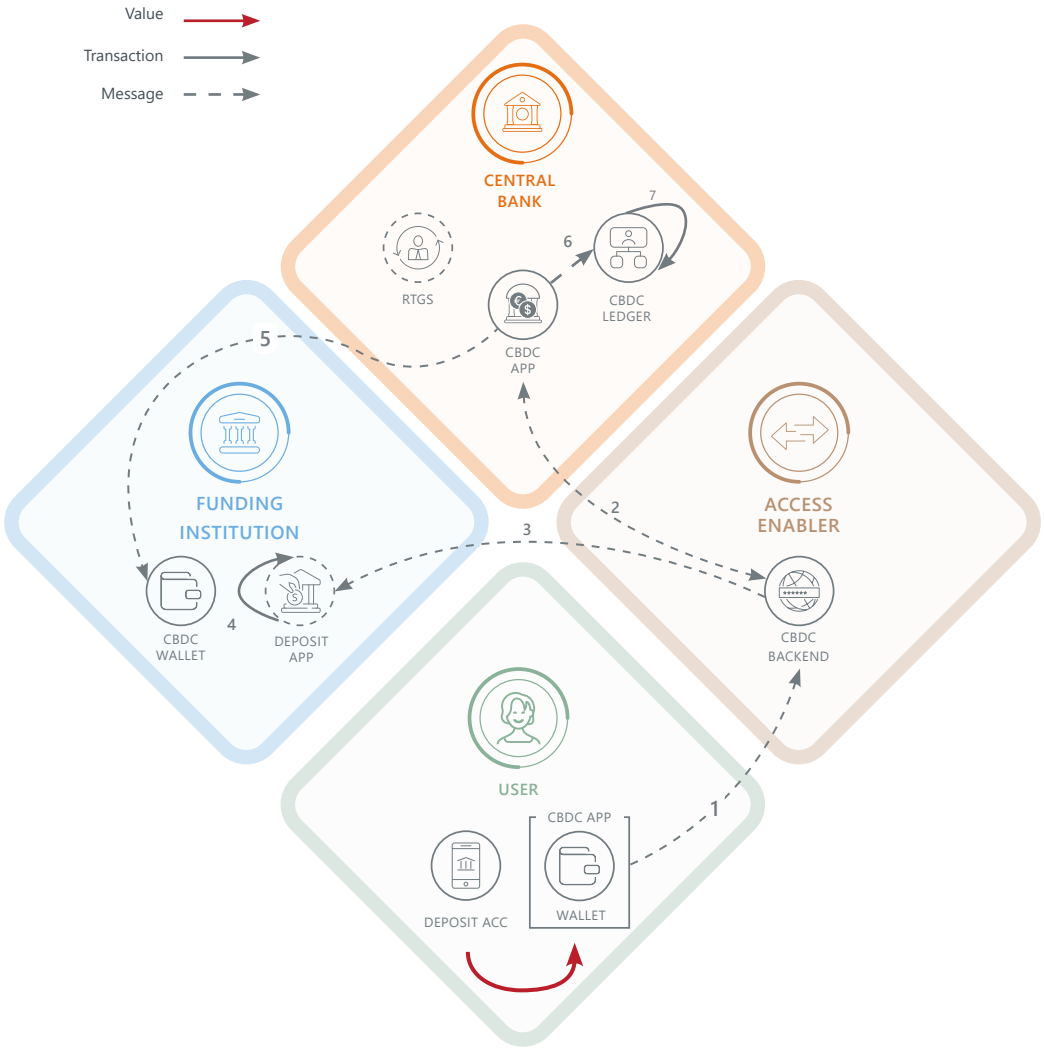
6.2.2 User converting deposits to rCBDC

Customers of FIs in the Sela architecture can easily convert between their deposits held at FIs and rCBDC, providing users with effective fungibility between rCBDC and FI deposits. This flow assumes that the end user has linked its bank account to its AE(s).

To exchange deposits for rCBDC, the user first requests rCBDC through one of its AEs in the rCBDC app (step 1 in Graph 10.2). The AE then checks the user's rCBDC account balance[88] and that the transaction would not bring the balance above the rCBDC holding limit (step 2) before requesting an exchange of FI deposits for rCBDC (step 3). The FI debits the user's deposit account (step 4) and then, through its own rCBDC wallet, requests a payment of the equivalent amount in rCBDC to the user's account (step 5). The rCBDC app then requests the ledger to debit the FI's rCBDC balance and credit the user's rCBDC balance (step 6). Finally, the debit and credit transactions are executed by the ledger atomically (step 7). This sequence of actions moves value from the user's FI deposit account to its rCBDC wallet (red arrow).

The conversion of rCBDC back to FI deposits follows roughly the reverse flow.

Graph 10.2 – User converting deposits to rCBDC



88. Before routing a request for the end user to convert deposits to rCBDC, an end user's AE needs to check the updated rCBDC account balance as the balance could be changed due to transactions submitted through another AE.

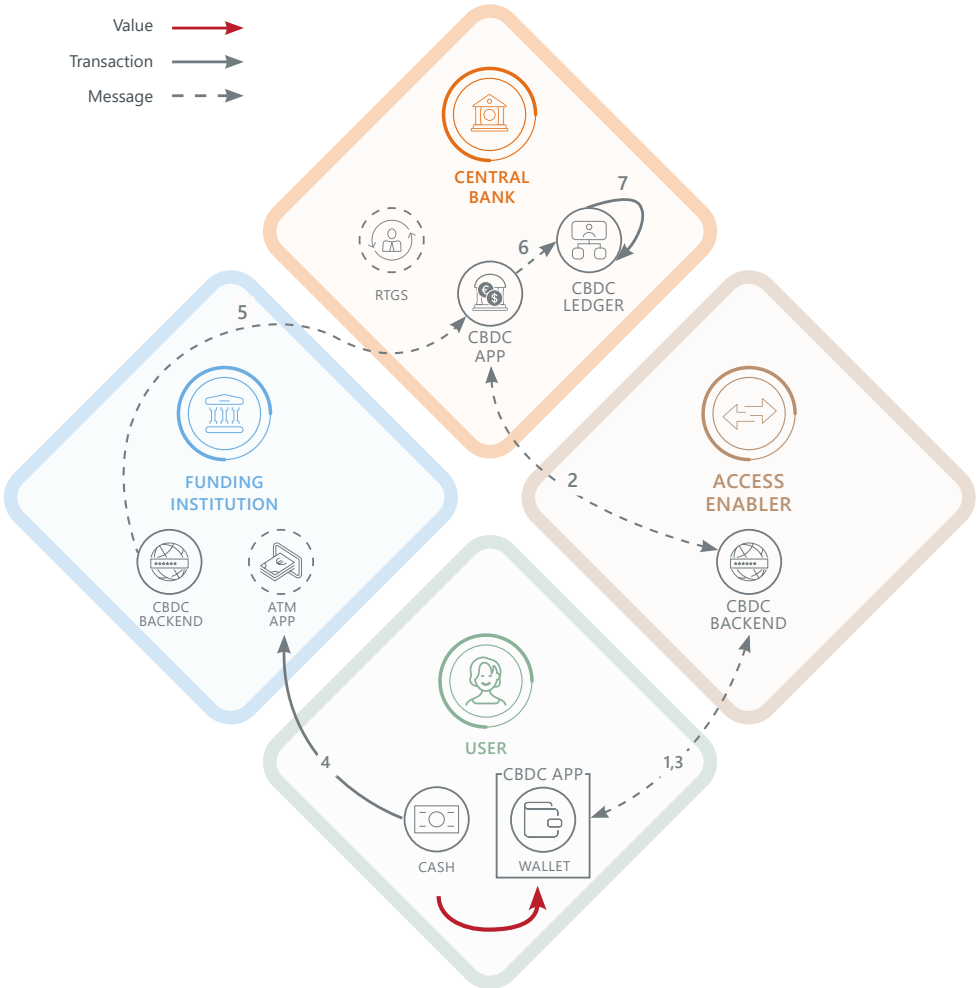
6.2.3 User converting cash to rCBDC

Similarly, end users can easily convert between cash and rCBDC using the ATMs operated by the FIs, providing users with fungibility between these two forms of money. This conversion can be done at any FI-operated ATM machine whether or not the end user is a customer of the same FI or any FI at all, making this conversion service available to anyone in the economy (including the unbanked) and supporting financial inclusion.

To exchange cash to rCBDC, the user first requests rCBDC through one of its AEs in the rCBDC app (step 1 in Graph 10.3). The AE then requests a one-time password (OTP) from the central bank (step 2) to link the cash-based transaction with the appropriate rCBDC wallet. The AE then relays the OTP back to the user (step 3). The user then approaches an ATM, enters the OTP and deposits the cash (step 4). The FI then, through its own rCBDC wallet, requests a payment of the equivalent amount in rCBDC to the user's account (step 5). The central bank's rCBDC app requests the ledger to execute the transaction (step 6) and finally, the debit and credit transactions are executed atomically (step 7). This sequence of actions moves value from cash held by the user to its rCBDC wallet (red arrow) and shows how a user, whether or not it has a relationship with the FI operating an ATM, can convert cash to rCBDC, easily and conveniently.

The conversion of rCBDC back to cash follows roughly the reverse flow.

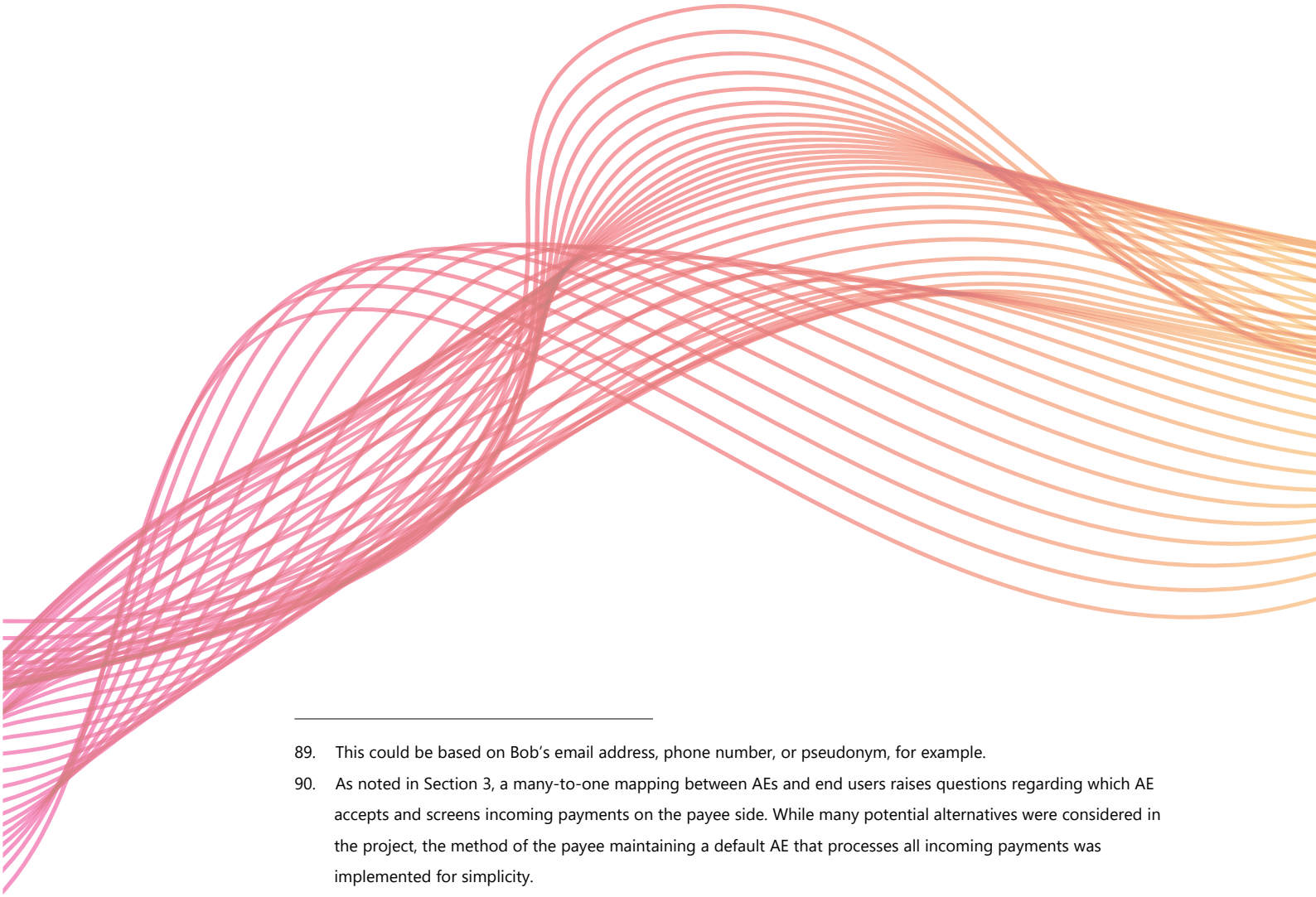
Graph 10.3 – User converting cash to rCBDC



6.2.4 rCBDC payment transfer

In contrast to existing systems, where digital payments often involve multiple intermediaries and financial exposure, in Sela's architecture an rCBDC payment moves funds instantly from payer to payee with the appropriate endorsement of their respective AEs. This flow shows how an end user, Alice, can pay another end user, Bob, assuming that Alice has Bob's unique address or address alias[89] and that Alice has sufficient funds in her rCBDC wallet to execute the payment.

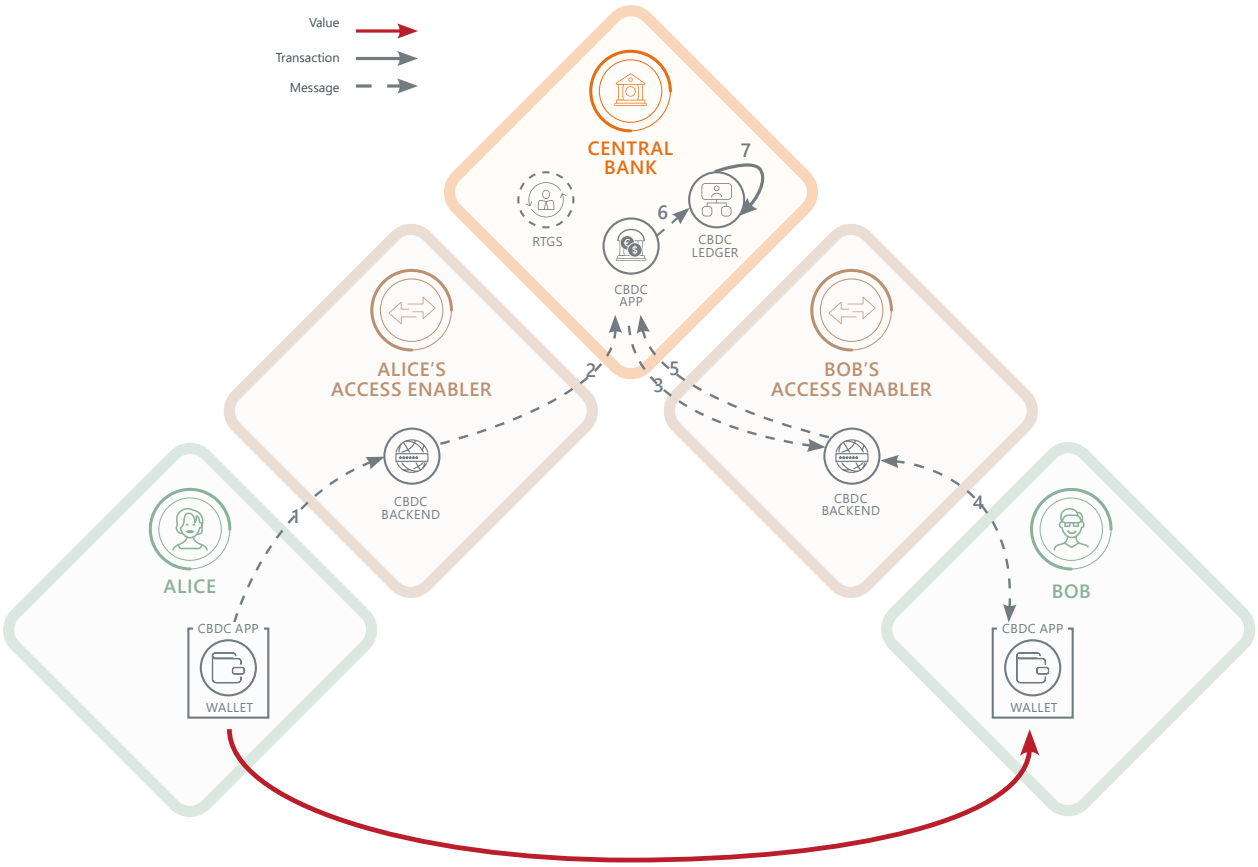
Alice first requests to make a transfer to Bob through one of her AEs (step 1 in Graph 10.4). Once the proper compliance processes have been completed by Alice's AE, it endorses the request by co-signing the transaction before submitting it to the rCBDC system (step 2). The system then notifies Bob's default AE for incoming payments of the intended transfer (step 3).[90] Bob's AE responds to the message and relays to Bob that there is a pending transfer for approval (step 4). Once Bob accepts the transfer, his AE relays it back to the rCBDC system (step 5). The system then atomically requests and executes a debit to Alice's rCBDC account and a credit to Bob's account (steps 6 and 7). This sequence of actions moves value from Alice's rCBDC wallet to Bob's rCBDC wallet (red arrow).



89. This could be based on Bob's email address, phone number, or pseudonym, for example.

90. As noted in Section 3, a many-to-one mapping between AEs and end users raises questions regarding which AE accepts and screens incoming payments on the payee side. While many potential alternatives were considered in the project, the method of the payee maintaining a default AE that processes all incoming payments was implemented for simplicity.

Graph 10.4 – User rCBDC payment transfer



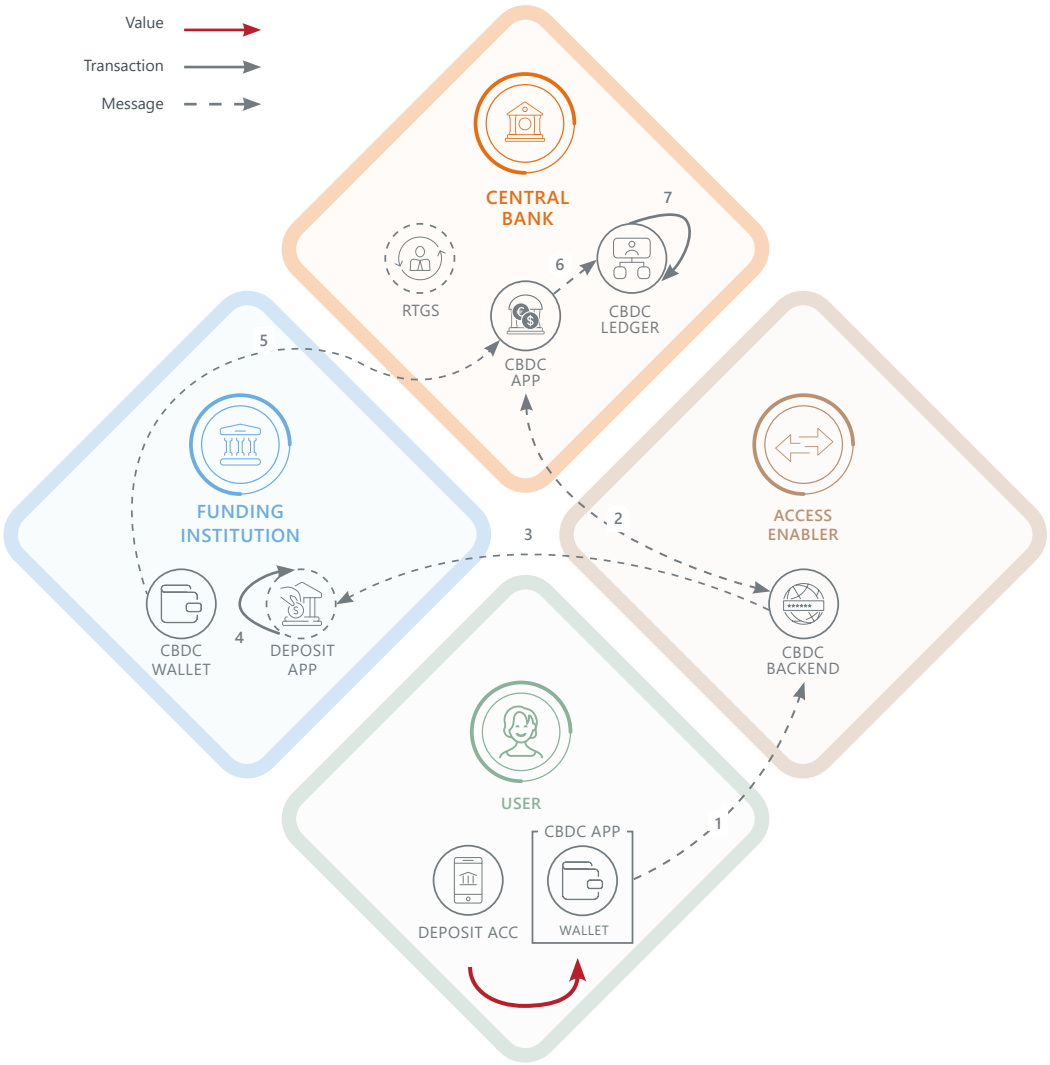
6.2.5 Top-up

A top-up is a transaction that increases an rCBDC wallet balance after it falls below a pre-determined lower bound. For example, suppose in the rCBDC payment outlined in Section 6.2.4 that the payer Alice does not have sufficient funds in her rCBDC wallet. If Alice has linked an FI account to her AE supporting her outgoing payment request and has provided the necessary consent and settings for this AE to trigger conversions with the FI on her behalf, the AE can initiate a top-up request to fund the payment.

Alice (the user in Graph 10.5) requests to make a transfer to Bob through one of her AEs (step 1). The AE first updates Alice's rCBDC account balance (step 2) and determines that Alice has insufficient rCBDC funds to execute the desired transaction. The AE then initiates an rCBDC top-up request to Alice's linked FI (step 3). The FI debits Alice's deposit account (step 4) and instructs the rCBDC platform to transfer rCBDC from its wallet to Alice's wallet (step 5). The rCBDC app instructs the ledger to execute the transaction, and the transaction takes place (steps 6 and 7). This sequence of actions moves sufficient value from Alice's FI deposit account to her rCBDC wallet (red arrow) to execute her requested outgoing payment to Bob. The outgoing payment then starts from here with step 2 in the rCBDC payment flow outlined in Section 6.2.4.

If Alice does not have a linked FI to support the top-up function, the transaction will not be endorsed by the AE and will fail to execute, accompanied by an error message sent to the user.

Graph 10.5 – User rCBDC account top-up

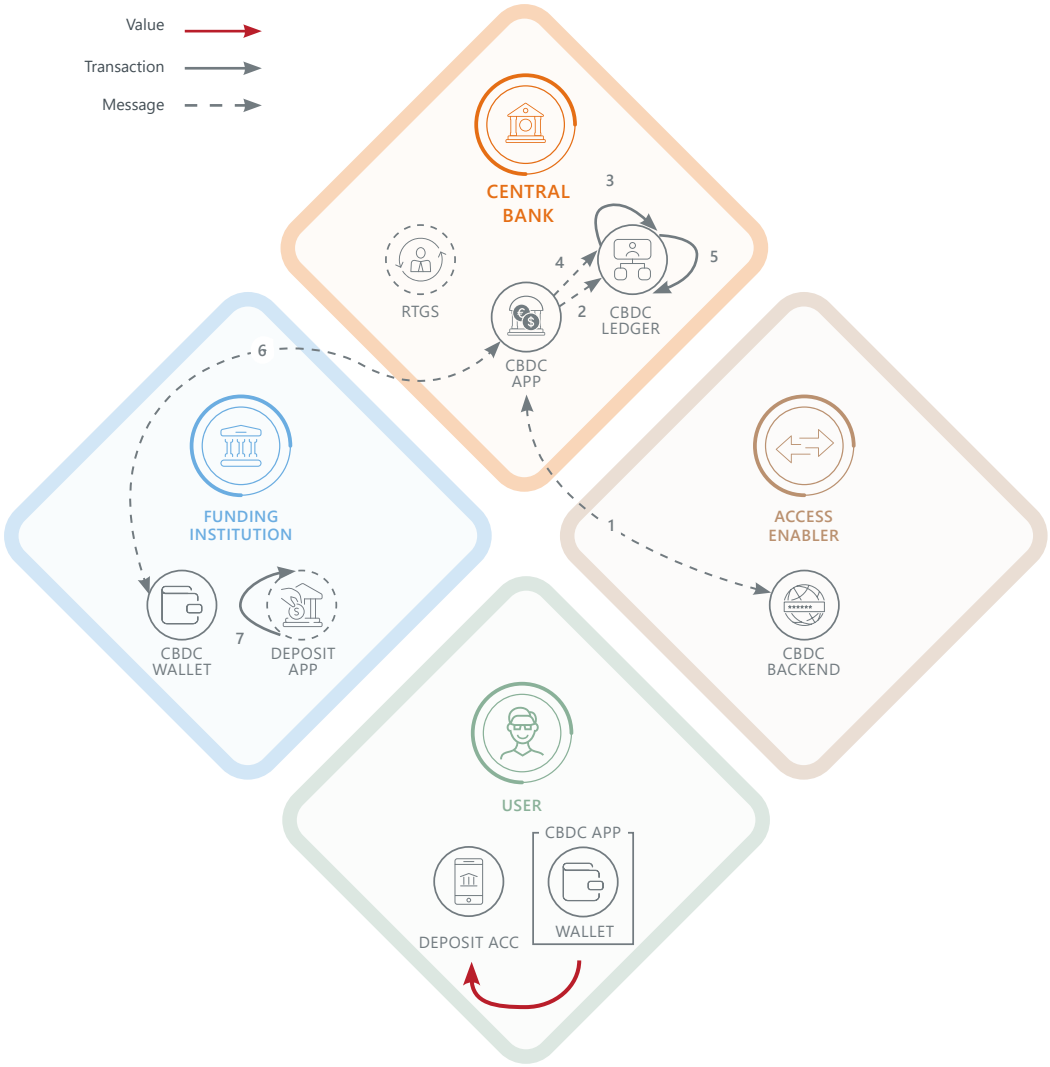


6.2.6 Waterfall

A waterfall is a transaction that re-routes an rCBDC wallet's funds in excess of a pre-determined upper bound to a different destination. This flow outlines a waterfall mechanism implemented in Sela whereby incoming payments bringing an end user's rCBDC wallet balance above a holding limit (determined by the central bank) can still be received by converting the excess rCBDC into deposits at a linked FI. For example, suppose in the rCBDC payment outlined in Section 6.2.4, that after the incoming payment from Alice, the payee Bob's rCBDC wallet balance will exceed the holding limit. If Bob has linked an FI account to his AE and has provided the necessary consent to the AE, this will automatically trigger a waterfall process to defund the excess rCBDC amount to Bob's deposit account at his FI by the rCBDC app at the central bank.

Bob (the user in Graph 10.6) is about to receive an incoming payment request from Alice that will make his total rCBDC wallet holdings exceed the holding limit. The rCBDC system notifies Bob's AE that there is an incoming payment. Bob's AE passes the notification on to Bob. Once he accepts the payment, the AE endorses his acceptance and shares the user's FI account information as a destination for the excess funds (step 1). The rCBDC app requests to execute the incoming payment from the rCBDC ledger, which in turn credits Bob's rCBDC account (steps 2 and 3). The rCBDC app, where the upper limit rules are defined, checks and identifies immediately that Bob's balance has exceeded the limit and initiates the waterfall action. The rCBDC app requests the initiation of rCBDC defunding, which is a transfer of rCBDC from Bob's wallet (with Bob's signing consent) to his FI's wallet (steps 4 and 5). Upon receiving the funds, the FI credits Bob's deposit account (steps 6 and 7). This sequence of actions moves value from Bob's rCBDC wallet to his FI deposit account (red arrow) through a waterfall process that is triggered after receiving a payment from Alice that exceeds Bob's rCBDC holding limit.

Graph 10.6 – User rCBDC account waterfall



If Bob does not have a linked FI to support the waterfall function, the transaction will not be endorsed by the AE and will fail to execute, accompanied by an error message sent to the user.

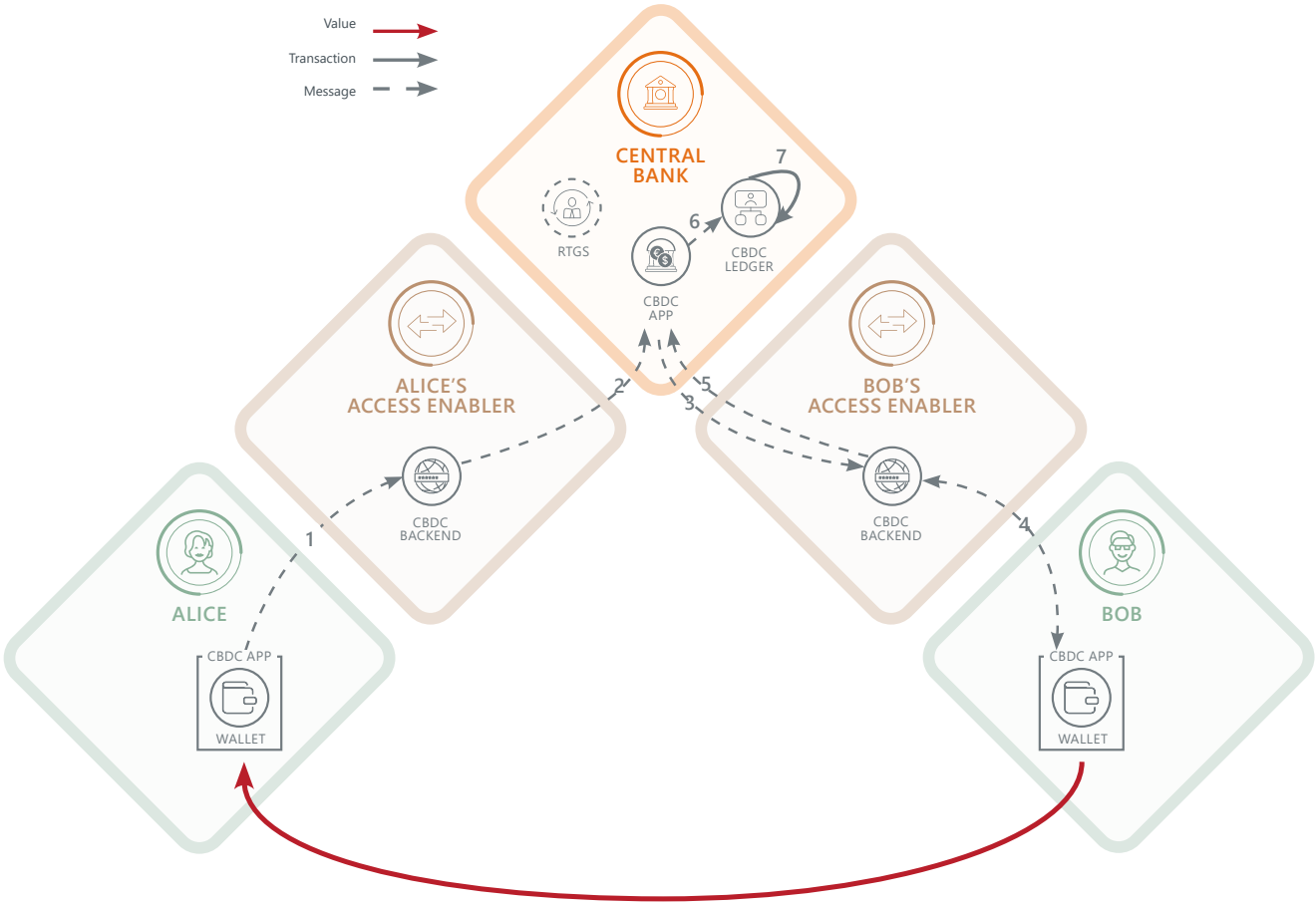
6.2.7 RTP

The Sela rCBDC platform supports automated triggering of payments, the first component of programmability (recall Section 5.4), by sending messages with payloads through the central bank's rCBDC app between rCBDC accounts. These "actions" can coordinate and trigger any actions available on the ledger. One example is an RTP function, where an action is sent from one user to another, requesting an rCBDC payment as a message along with the payment transaction itself as an accompanying payload. This flow can be generalised to include other forms of desired ledger functions.

Suppose, for example, that Alice wants to receive an rCBDC payment from Bob. Alice first sends a message with a request for payment from Bob to her AE (step 1 in Graph 10.7). Alice's AE runs the appropriate compliance checks, and once these are complete, endorses the request by co-signing and submitting it to the rCBDC system (step 2). This payment request now contains the payload for a payment from Bob to Alice co-signed by Alice and her AE. The rCBDC app then forwards the request to Bob's AE (step 3), who in turn forwards the request to Bob (step 4). Once Bob accepts, the AE endorses and responds to the rCBDC app (step 5). The rCBDC app then requests the rCBDC ledger to execute the transaction and the ledger validates that the correct signatures are present and executes the transaction (steps 6 and 7). This sequence of actions moves value from Bob's rCBDC wallet to Alice's rCBDC wallet (red arrow) through a request sent from Alice to Bob in the format of an RTP.

If more complex conditional transactions are made available through the rCBDC ledger, they can be triggered across end users using a similar design.

Graph 10.7 – Request to pay example of rCBDC action



7. Conclusion

The increasing digitalisation of the economy has prompted central banks around the world to explore retail central bank digital currencies, but designing a functional rCBDC system is a challenging task. Project Sela helps to address this challenge by providing learnings from the design and build of an accessible and cyber-secure rCBDC system PoC that aims to capture the benefits of cash while also preserving the desirable attributes of private-sector digital payments. The Sela PoC was informed by the project's four workstreams on policy, legal, cyber security and technology, and leveraged the strengths and expertise of the BIS Innovation Hub, the Bank of Israel, the Hong Kong Monetary Authority and selected private sector partners.

A key policy goal of the project was to promote an accessible, competitive and innovative rCBDC ecosystem that can serve a wide range of use cases. As such, an effort was made to lower the barriers to entry for rCBDC service providers and unbundle and efficiently redistribute rCBDC processes and services among public and private actors. Lower barriers to entry can allow a more diverse range of intermediaries to compete and develop creative ways to provide rCBDC services to a large user base. A novel type of intermediary, the AE, was designed to support this goal by providing all customer-facing rCBDC services without ever "holding" an end user's rCBDC (or needing to hold funds to service end users) at any point in the provision of their services. rCBDC payments facilitated by AEs are thus settled directly on the central bank's balance sheet, free from credit risk. While a tailored regulatory framework will probably be needed for this new type of intermediation, it may require less financial regulation, reducing friction and operational costs for payment service providers in the rCBDC ecosystem.

At the core of Sela's accessible and secure rCBDC PoC is a retail rCBDC ledger operated by the central bank that facilitates instant payment finality for transactions at scale. This ledger is directly connected to AEs, who intermediate between the rCBDC ledger and end users, and FIs, who manage end user deposits and ATM networks that enable the conversion of rCBDC to and from other forms of money in the economy. While end users hold their own rCBDC in the PoC design, AEs provide all client-facing and business-oriented functionality as well as certain compliance services such as KYC procedures and AML/CFT screening.

The project also explored design considerations to preventatively secure this rCBDC system, which could see greater vulnerability due to the increased access. This resulted in a PoC design that is grounded in (i) strong authentication and authorisation methods, supported by robust key management environments and secure communication channels that are flexible enough to accommodate wide access in the rCBDC ecosystem; (ii) proper data management of sensitive information, protecting the privacy of end users from the central bank and avoiding central pools of PII that can attract malicious actors; and (iii) automation as a building block for broader programmability, where the execution environment resides with intermediaries – a less mission-critical environment – rather than the rCBDC ledger. The measures implemented form only a small part of the multi-dimensional and complex cyber security measures needed to fully secure an rCBDC system.

Project Sela demonstrates that an rCBDC system with a central bank-operated retail ledger promoting access, competition and innovative payment services does not necessarily come at the cost of greater cyber security risk. Access to the rCBDC can be supported by a novel type of intermediary called an AE that, through lower barriers of entry, can increase competition and innovation in rCBDC payment services. Sela's findings show promise that, with careful preventative architecture design, cyber security risks can be mitigated.

The project also highlighted areas for future research. First, further work could assess the appropriate regulatory structure and business viability of an architecture like Sela's in increasing access. For example, incentive models for AEs in providing rCBDC services could build from existing regulations in the open banking space that allow payment service providers to leverage their existing infrastructure and end users' transaction data to create additional commercial offerings on top of basic rCBDC functions. Second, interoperability with existing payment systems such as the RTGS, fast payment systems and FI systems could be further explored, including the different reconciliation mechanisms between FI rCBDC and reserve balances, and upgrades to FI infrastructure to handle potentially large loads of conversion to and from rCBDC. Integration with additional payment components, such as those of e-money institutions and other existing payment service providers could also be considered.

Third, while the Sela platform supports automation as a preliminary part of programmability, further analysis into more advanced functionality (as illustrated in Project Rosalind) and the cyber security implications was left for future work. In addition, other privacy-enhancing technologies to safeguard users' privacy represent a promising area for future exploration; indeed, projects such as Tourbillon and Aurum are already leading this effort. Finally, additional work along other cyber security dimensions is needed. For example, evaluating the cyber security of Sela's design against active cyber attacks would help test Sela's existing design choices, identify gaps, and increase public confidence in the security of such an architecture in a production setting.

References

Atlantic Council (2022): *Missing Key: The challenge of cybersecurity and central bank digital currency,* June.

Bank for International Settlements (BIS) (2022): "The future monetary system", *Annual Economic Report 2022,* June, Chapter III.

——— (2023): "Blueprint for the future monetary system: improving the old, enabling the new", *Annual Economic Report 2023*, June, Chapter III.

Bank of England (BoE) (2020): "Central Bank Digital Currency: Opportunities, challenges and design", *Discussion Paper*, March.

——— (2023a): "Enabling innovation through a digital pound", *Quarterly Bulletin*, August.

——— (2023b): *The digital pound: a new form of money for households and businesses?*, February.

——— (2023c): "The digital pound", *Technology Working Paper*, February.

Bank of Israel (BoI) (2021): *A Bank of Israel Digital Shekel: Potential Benefits, Draft Model, and Issues to Examine*, May.

BIS Innovation Hub (BISIH) (2022): *Project Aurum: A Prototype for Two-Tier Central Bank Digital Currency (CBDC),* October.

——— (2023a): *Project Rosalind: Building API prototypes for retail CBDC ecosystem*, June.

——— (2023b): *Project Polaris, Part 2: A security and resilience framework for CBDC systems,* July.

——— (2023c): *Lessons learnt on CBDCs,* July.

——— (2023d): *Project Aurora: The power of data, technology and collaboration to combat money laundering across institutions and border*, May.

——— (2023e): *Project Polaris, Part 1: A handbook for offline payments with CBDC*, May.

Chan, T-H, R Pass and E Shi (2018): Pala: *A Simple Partially Synchronous Blockchain*, October.

Check Point (2023): *Network Security*, June.

CPMI and International Organization of Securities Commissions (CPMI-IOSCO) (2016): *Guidance on cyber resilience for financial market infrastructures*, June.

European Central Bank (ECB) (2022): *Progress on the investigation phase of a digital euro – second report*, December.

——— (2023a): *Progress on the investigation phase of a digital euro – third report*, April.

——— (2023b): *Digital euro glossary*, March.

——— (2023c): *Digital euro – Prototype summary and lessons learned*, May.

Financial Conduct Authority (FCA) (2017): P*ayment Services and Electronic Money – Our Approach,* September.

Hong Kong Monetary Authority (HKMA) (2018): *Open API Framework for the Hong Kong Banking Sector*, July.

International Institute for the Unification of Private Law (UNIDROIT) (2023): *Draft UNIDROIT Principles on Digital Assets and Private Law,* January.

Kosse, A and I Mattei (2023): "Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto", *BIS Papers*, no 136, July.

Munoz, A, R Rios, R Roman and J Lopez (2023): "A survey on the (in)security of trusted execution environments", *Computers & Security*, no 129.

M10 (2021): *M10 system throughput report.*

National Institute of Standards and Technology (NIST) (2019): *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,* August.

——— (2010): *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April.

——— (2023): *Digital Signature Standard (DSS)*, February.

Shin, H S (2021): "Central bank digital currencies: an opportunity for the monetary system", speech by the BIS's Economic Adviser and Head of Research at the Bank's Annual General Meeting, Basel, 29 June.

Woods, D and R Böhme (2021): "SoK: Quantifying Cyber Risk", *IEEE Xplore*, May.

Appendix: Project participants and acknowledgements

BIS Innovation Hub

Bénédicte Nolens, Hong Kong Centre Head

Daniel Eidan, Adviser and Solution Architect

Leanne (Si Ying) Zhang, Adviser

Jack Ho, Adviser

Bank of Israel

Yoav Soffer, Digital Shekel Project Manager

Amir Moshe, Economist, Digital Shekel Project

Nir Yaacobi, Economist, Digital Shekel Project

Gil Polak, CISO

Konstantin Vandyshev, Cyber Security Team

Tomer Mizrahi, CTO

Ovad Sabati, Analyst, Clearing Houses Operation Unit

Hong Kong Monetary Authority

Nelson Chow, Chief Fintech Officer

Yvonne Tsui, Senior Fintech Director

Michael Law, Fintech Director

Danny Chau, Fintech Director

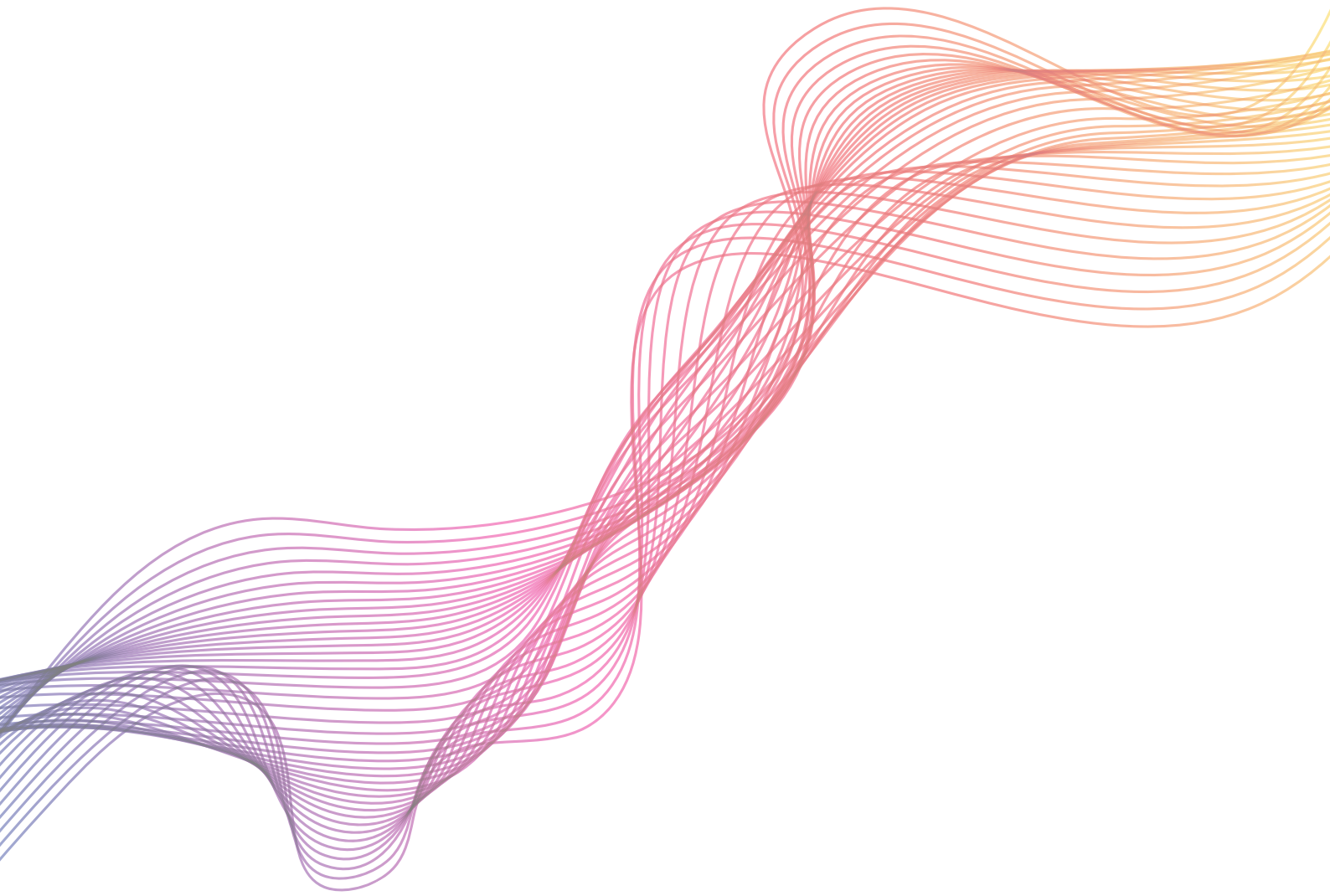
Frederick Cheung, Senior Associate Fintech Director

Luca Conti, Associate Fintech Director

Bernia Lee, Associate Fintech Director

Acknowledgements

We would like to thank Cecilia Skingsley, Ross Leckow, Morten Bech, Francesca Hopwood Road, Beju Shah, William Zhang, Codruta Boar, Jennifer Devlin, Ben Dovey, Hakan Eroglu, Italo Borssatto, John Tsz Hon Yuen and Andreas Adriano for their inputs to this report, and also our private sector partners Marten Nelson, Lucie Pra, Julia Demidova, Daniel Driscoll, Michael Wittner, Urvashi Sharma, Andres Sosa, Simon Gleeson, Diego Ballon Ossio, Anastasia Mikhaleva, Dan Karpati, Assaf Mendelson and Eran Nafusi for supporting this project.



ISBN 978-92-9259-688-0 (Online)