FEDERAL RESERVE BANK *of* NEW YORK

New York Innovation Center

PROJECT CEDAR

Phase One Report Technical Appendix

May 2023

NYIC

The content of this report reflects research of the New York Innovation Center and should not be interpreted to reflect any policies or directives of the Federal Reserve Bank of New York or the Federal Reserve System. Any views expressed in this report are those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of New York or Federal Reserve System.

Table of Contents

1 Background and Purpose

Project Cedar is the inaugural project of the New York Innovation Center (NYIC). The NYIC, a part of the Federal Reserve Bank of New York (New York Fed), bridges the worlds of finance, technology, and innovation. Established as part of a strategic partnership with the Bank for International Settlements Innovation Hub, the NYIC generates insights into high-value central bank-related opportunities through technical research, experimentation, and prototyping, to drive advancements in central banking and enhance the functioning of the global financial system.

In November 2022, the NYIC published its findings from Phase I of Project Cedar. This work investigated how improvements to cross-border payments might be enabled by new technologies such as blockchain and distributed ledgers (DLT). Specifically, the project considered a foreign exchange (FX) spot trade in which settlement occurred in simulated wholesale central bank digital currency (wholesale CBDC) enabled by DLT.

The purpose of this document is to provide supplementary technical detail to the November 2022 report. It is designed to be referenced in conjunction with that report and not as a standalone overview of the research.

This report aims to contribute to a broad and transparent dialogue about central bank digital currencies (CBDC) from a technical perspective. It is not intended to advance any specific policy outcome, nor to signal that the Federal Reserve will make any imminent decisions about the appropriateness of issuing a retail or wholesale CBDC, nor to indicate how one would necessarily be designed.

The content of this report should not be interpreted as reflecting any policies or directives of the Federal Reserve System or the Federal Reserve Bank of New York. Any views expressed in the report are those of the authors and do not necessarily reflect the views of the Federal Reserve Bank of New York or Federal Reserve System.

2 CBDC Research Landscape Detail

Project Cedar Phase I aims to contribute to a broader research landscape related to cross-border payments and wholesale CBDC. The section below highlights some existing projects within this landscape.

Project Jasper-Ubin: Project Jasper-Ubin was a collaboration between the Bank of Canada (BOC) and the Monetary Authority of Singapore (MAS) that concluded in May 2019.[1] The goal of this project was to allow atomic settlement for two legs of a transaction, where each leg is denominated in a different currency (CAD and SGD) and each central bank uses a different type of DLT platform (a Corda-based network in Canada and a Quorum-based network in Singapore). The project used a hashed timelock contract (HTLC) to achieve atomicity of settlement. The project was implemented successfully and demonstrated the ability to perform atomic transactions using this type of smart contract.

In contrast to Project Jasper-Ubin, the other projects described this section take the approach of setting up a joint DLT platform to facilitate cross-border transactions.

Project Inthanon-LionRock: Project Inthanon-LionRock is a collaboration between the Hong Kong Monetary Authority (HKMA) and the Bank of Thailand (BOT). Phase I achieved a proof-of-concept single platform built by technology vendor R3 on Corda that is designed to allow participants to conduct fund transfers and foreign exchange transactions on a peer-to-peer basis. Each central bank issues a wholesale CBDC on the single platform that can be used to facilitate settlement. Importantly, entities in a given jurisdiction have access to the wholesale CBDC of only that jurisdiction.

[1] See Bank of Canada and Monetary Authority of Singapore, "Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies," 2019, at https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf.

Phase 2 produced a prototype built by technology vendor ConsenSys on Hyperledger Besu. The prototype encompasses Thailand, Hong Kong, and two additional jurisdictions. Within the prototype, participating central banks are able to control the flow of their CBDC, monitor transactions and balances of their issued CBDC, utilize programmable levels of transaction privacy, and automate certain compliance functions. In its third phase, the project became mBridge, described in more detail below.

Project Jura: Project Jura was conducted by the Banque de France, the BIS Innovation Hub, and the Swiss National Bank in collaboration with a group of private sector firms. The goal of Project Jura was to perform the direct transfer of euro and Swiss franc wholesale CBDCs, as well as tokenized commercial paper, between French and Swiss commercial banks on a single DLT platform operated by a third party. In contrast to Project Inthanon-LionRock, the commercial banks in this project have access to both wholesale CBDCs. To retain critical controls for central banks, notably over their wholesale CBDC, the project makes use of subnetworks. Each central bank is the notary on its subnetwork and atomicity is achieved because a transaction occurs only if both notaries have validated the transaction.

The experiment was performed on the SDX platform, which uses R3's Corda as the underlying permissioned DLT platform.

Project Dunbar: Project Dunbar brings together the Reserve Bank of Australia, Central Bank of Malaysia, Monetary Authority of Singapore, and South African Reserve Bank with the Bank for International Settlements Innovation Hub to test the use of CBDCs for international settlements.

Project Dunbar worked with technology vendors R3 and Partior to develop prototypes on the distributed ledger technologies of Corda and Quorum, respectively. The prototypes proved the technical feasibility of implementing a shared multi-CBDC platform.

Project mBridge: Project mBridge is the third phase of Project Inthanon-LionRock. The BIS Innovation Hub Hong Kong Centre, the Digital Currency Institute of the People's Bank of China, and the Central Bank of the United Arab Emirates joined the HKMA and the BOT for this phase. Phase 3 involves further experimentation with design choices and technology trade-offs, and a future roadmap from prototype to a production-ready network that can serve the broader central banking community as a public good through open-sourcing.

3 Primary Research

Primary research was conducted to validate the working hypothesis related to the problem space and potential solution concept for an FX spot transaction. Interviews were conducted with a range of market participants to meet the following objectives:

1. Generate a deep understanding of the current state FX spot transaction process.
2. Augment an understanding of the New York Fed's internal process flow with that of its counterparties.
3. Evaluate the perceived value of the solution to the market.
4. Identify gaps in the current process and potential opportunities for future development.

Interviews were conducted with wholesale FX market participants spanning three categories: central banks, FX dealers, and non-bank liquidity providers. While transaction chains can involve many counterparties, most transactions across the market involve some subset of these parties, making their perspectives crucial in understanding the limitations of the current state. Additionally, these three types of counterparties represent distinct approaches to FX trading and settlement, so their input resulted in a diverse cross-section of data.

While the trading process varied across participants, takeaways from this research were largely applicable across the range of responses. Key takeaways are as follows:

1. The majority of interview participants experience a high degree of straight-through processing, given an industry-wide shift toward automation in recent years.
    - The trade matching and execution processes are highly automated, as market participants rely on industry solutions such as Bloomberg, Traiana, and SWIFT.
    - On the settlement side, the degree of automation depends on settlement type and accuracy of standard settlement instructions (SSIs).
2. Despite this high degree of straight-through processing, drivers of counterparty risk and long settlement times remain, such as lack of access to payment-versus-payment (PvP) settlement solutions.
    - Those interviewed expressed a preference for PvP settlement options, such as CLS, for trades that cannot be offset internally. The percentage of trades eligible for CLS settlement depended on the firm.
    - Where PvP mechanisms or internalization is not available, trades are often settled on a gross basis in which no netting takes place. Of the settlement options, this presents the greatest counterparty risk.
3. Given the credit risk involved in non-PvP settlement, some counterparties with lack of access to PvP solutions may experience limitations in FX market participation.
    - Counterparties settling on a gross basis tend to be non-CLS members, small to mid-size firms, and potentially representing emerging markets.

4. For transactions that do not benefit from straight-through processing, the T+2 settlement window is driven in part by delays in manual communications.
    - Where manual steps are required, email is the primary mode of communication between transaction participants.
    - These communications can be stalled, as many FX transactions involve parties operating across a range of time zones.
5. Participants were generally more enthusiastic about the potential value of atomic settlement than they were of instantaneous settlement.
    - There was recognition across participants that atomic settlement could substantially reduce the credit risk associated with a transaction. Participants placed high value on a solution that could establish certainty that a given transaction would settle.
    - Several participants expressed the desire for PvP settlement to be accessible for all counterparties. Given that the CLS solution is not universally accessible, an opportunity remains to develop a solution enabling PvP settlement agnostic of the counterparty.
    - The value of instantaneous settlement was not as clear across participants. Many identified a potential liquidity issue associated with instantaneous settlement, given the transaction and credit chains that exist across the FX market today.

Ultimately, the primary research validated the secondary research, which highlighted speed and access issues in wholesale cross-border payments. Based on both bodies of research, a future state solution should enable atomic settlement, access to a wider range of counterparties, and settlement taking place faster than T+2.

The research also highlighted a range of opinions on the value of instantaneous settlement in the FX market, with several participants highlighting potential negative impacts to liquidity should the market shift to an instantaneous settlement standard. However, many also highlighted that T+2 settlement may be an outdated market convention, with an optimal settlement time existing somewhere between instantaneous and T+1. It is important to note that PvP settlement can be implemented independently from instantaneous settlement, and that there may be value in allowing market participants to choose when the settlement of their trades takes place.[2] Additional research is required to validate these claims and assess market implications of this shift in settlement convention.

4 Phase I Scope

Project Cedar Phase I focused on demonstrating the potential of DLT to deliver instant and atomic settlement for an FX spot use case involving simulated wholesale CBDC. The sections below highlight the key goals for experimentation in Phase I and call out the significant topics or design choices that were not assessed as part of Phase I.

In Scope

Instant and atomic settlement: Testing functionality related to instant and atomic settlement was central to Phase I, as these attributes underpin many of the core value propositions of a wholesale CBDC (for example, reduced settlement times and reduced counterparty risk). Demonstrating this functionality in Phase I included the usage of a UTXO-based blockchain and HTLCs.

[2] See "What is Atomic Settlement?", Federal Reserve Bank of New York *Liberty Street Economics*, November 7, 2022, at https://libertystreeteconomics.newyorkfed.org/2022/11/what-is-atomic-settlement/.

Interoperability across a simulated multi-ledger ecosystem of homogeneous ledgers: For Phase I of Project Cedar, interoperability was defined as conducting a transaction across multiple wholesale CBDC ledgers representing individual currencies and monitoring performance under a test load. This model hypothesizes a future in which a USD wholesale CBDC ledger would need to interact with ledgers owned and operated by different entities across the broader financial system. In Phase I, the simulated ecosystem included eight ledgers of the same technical design. Successfully transacting across such an ecosystem represents validation of interoperability in a limited sense. Further research is required to better understand requirements related to interoperability.

Telemetry: Establishing telemetry and capturing performance data in Phase I of Project Cedar provided insight into whether instant settlement was achieved as defined. For example, measuring end-to-end transaction duration allowed for comparability against the success metric of settlement in fewer than thirty seconds. This data also provides a benchmark for future research.

Out Of Scope

This section highlights some of the specific issues relating to the FX transactions use case and simulated wholesale CBDC ledger that were considered out of scope for Phase I of Project Cedar. This list is not inclusive of all out-of-scope topics.

Scalability: While some data was collected with respect to system performance, scaling the system was not an objective. Phase I aimed to establish a baseline against which future performance improvements could be measured. Significant optimization work in Phase I beyond what was required to meet the established performance targets was outside of this scope.

Programmability: Programmability is a key research area for digital assets in general. In Phase I, sufficient programmability was implemented to enable HTLCs, and functionality beyond this was considered out of scope. Programmable functionality beyond this could present an interesting topic for future research.

Further extensions of interoperability: Phase I demonstrated interoperability across a simulated multi-ledger ecosystem as described above. Further extensions of interoperability considered out of scope in Phase I included transacting across ledgers based on differing technical designs and interaction with existing payment systems.

AML/CFT: The FX trade and settlement processes involve numerous steps to ensure the relevant due diligence has taken place for each trade, such as Office of Financial Assets Control (OFAC) sanctions list and anti-money laundering (AML) / countering the financing of terrorists (CFT) checks. These processes were out of scope for Phase I.

Policy: Policy choices are a key input to the design of a wholesale CBDC. The work of the NYIC is focused on the potential for new technologies to enable new capabilities or create more efficient systems. Therefore, efforts were made to minimize policy assumptions required in the design for Project Cedar Phase I.

Issuance: The type of wholesale CBDC issuance —for example, whether the domestic central bank issued native or synthetic wholesale CBDC, was out of scope for Phase I.

Privacy and Security: Privacy and security are critical topics in digital asset research. While they were out of scope for Phase I, they may present interesting topics for the NYIC's future research.

5 Design Choices

A wholesale CBDC system could be designed in many ways. For instance, Project Cedar Phase I considers a design based on DLT, but non-DLT solutions such as traditional databases could plausibly deliver similar benefits. The set of design choices described below represents one of many alternatives and aims to contribute to the broader ongoing dialogue of wholesale CBDC research.

Programming languages: Rust was selected as the primary programming language for development of the ledger used in Project Cedar Phase I. Rust offers benefits including memory safety, concurrency management, standardized tooling, and speed. Rust is favored as a systems programming language by security researchers, who have found that up to 70 percent of vulnerabilities in software arise from memory safety issues.[3] Using Rust to implement the simulated wholesale CBDC ledger structurally eliminates the source of many memory and security problems that can plague systems software. In addition to Rust, Python, JavaScript, and Go are used in different supporting components of the ledger used in Project Cedar Phase I.

Ledger data: Project Cedar uses an **unspent transaction output (UTXO)** accounting model as its wholesale CBDC data representation, which allows for greater potential for concurrent transaction processing.

Permission structure: The platform deployed for Project Cedar is a private **permissioned** blockchain network. This structure allows for the designation of different types of actors with permissions and entitlements and allows the Federal Reserve to maintain exclusive control over its USD wholesale CBDC ledger.

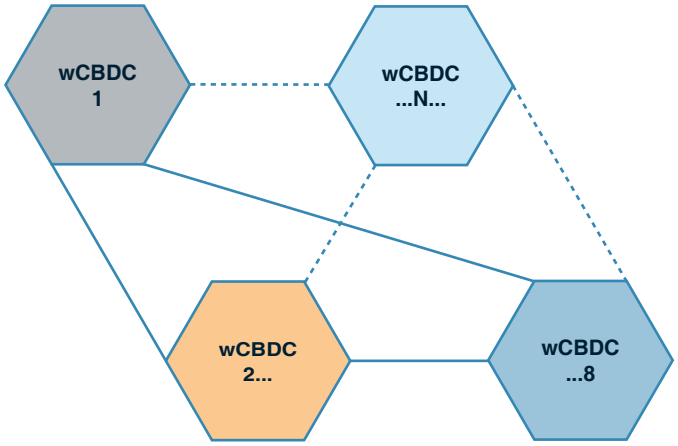
[3] See, for example, this Microsoft Security Response Center blog post, which notes that 70 percent of Microsoft Common Vulnerabilities and Exposures (CVE) are memory safety issues.

Ledger ecosystem: A fundamental design choice was to develop a **multi-ledger ecosystem** in which each ledger represents an individual currency. This design choice contrasts with other CBDC research that focuses on establishing a single multi-currency ledger. The rationale for this design choice was two-fold:

- **Security and resiliency of a wider currency of ecosystems:** Creating individual currency ledgers could improve resiliency by using separate systems with as little coupling as possible. This allows potential network issues to be localized and for unaffected ledgers to continue operating.
- **Flexibility:** Creating separate ledgers provides the owners or operators of the network with the flexibility to implement specific policy requirements that may not be portable to other networks and currencies.

This design choice requires that ledgers rely on certain common standards allowing for interoperability. The figure below denotes the ledger design of Project Cedar Phase I.

Figure 1. Multi-Ledger Wholesale CBDC Model



Consensus: The ledger is a private, permissioned blockchain network, that does not require proof-of-work consensus. Instead, the ledger is managed by a trusted operator, in this case, a central bank. This consensus model can be considered to be based on **proof-of-authority**, where a single server produces new blocks by attaching its signature and all other nodes only accept blocks with a correct signature.

Roles: Based on the permission structure, the ledger design offers two distinct roles: Validator and Participant. Validators are entitled to approve and timestamp batches of transactions (for example, blocks), proving their authority to do so by digitally signing the block. Participants can send transactions to the network and observe transactions that happen on the network. Participants receive blocks from the Validator through a peer-to-peer network and, after independently verifying the digital signature, apply the transactions in these blocks to their local state. In the testing approach, an additional role of Observer is distinguished that is effectively a Participant that does not actively transact, although it would have the permission to do so.

Hashed timelock contracts: HTLCs are used to enable interoperable and atomic settlement between two different currencies and ledgers. HTLCs consist of two components: a hashlock that is unlocked by a corresponding secret (or "pre-image") and a timelock that specifies the time window after which payment can be reclaimed.[4] Beyond the basic signature verification that any digital currency would support, HTLCs only require the ability to verify knowledge of the secret and to assert a transaction takes place after a certain deadline. They do not require rich statefulness or a highly expressive programming environment to implement, and nearly all ledger designs can implement them or an equivalent construction. Given these characteristics, HTLCs were selected to enable atomicity in Phase I.

[4] The secret or pre-image is a cryptographic proof used by one party to generate the hashlock and by the other to unlock the associated funds.

6 Design Components

Project Cedar's solution design consists of five key technical components, described below.

1. **Cedar Ledger** is the ledger infrastructure of the experiment, written in the programming language Rust. For each currency simulated in this prototype, a separate instance of the Cedar Ledger was run, servicing a fully separate ledger. While each currency is running the Cedar Ledger in Phase I, this design anticipates potential future work that could test different ledger technologies across the system.

2. **Cedar Agent** is responsible for carrying out the trade process and acts as a gateway providing information about the ledgers and basic wallet functionality for managing the user's funds. Cedar Agent is also written in Rust and interacts with the ledgers through remote procedure calls (RPCs) to the Cedar Ledger. In the Project Cedar prototype, FX transactions on the ledger are executed in the form of an atomic cross-chain swap.[5,6] When a transaction is initiated, the Cedar Agent provides the data required to exchange assets between parties and execute the on-chain process of the swap. After the setup is complete, the remainder of the trade is executed automatically and the funds from the other party are deposited into the user's wallet provided by the Cedar Ledger client.

3. **Cedar UI Backend** is an API server written in the programming language Go that serves as a medium for content and state external to the ledger that is required for the UI. The Cedar UI Backend is

[5] Remote procedure calls are used to request a service from another process without explicitly coding the details for the interaction.

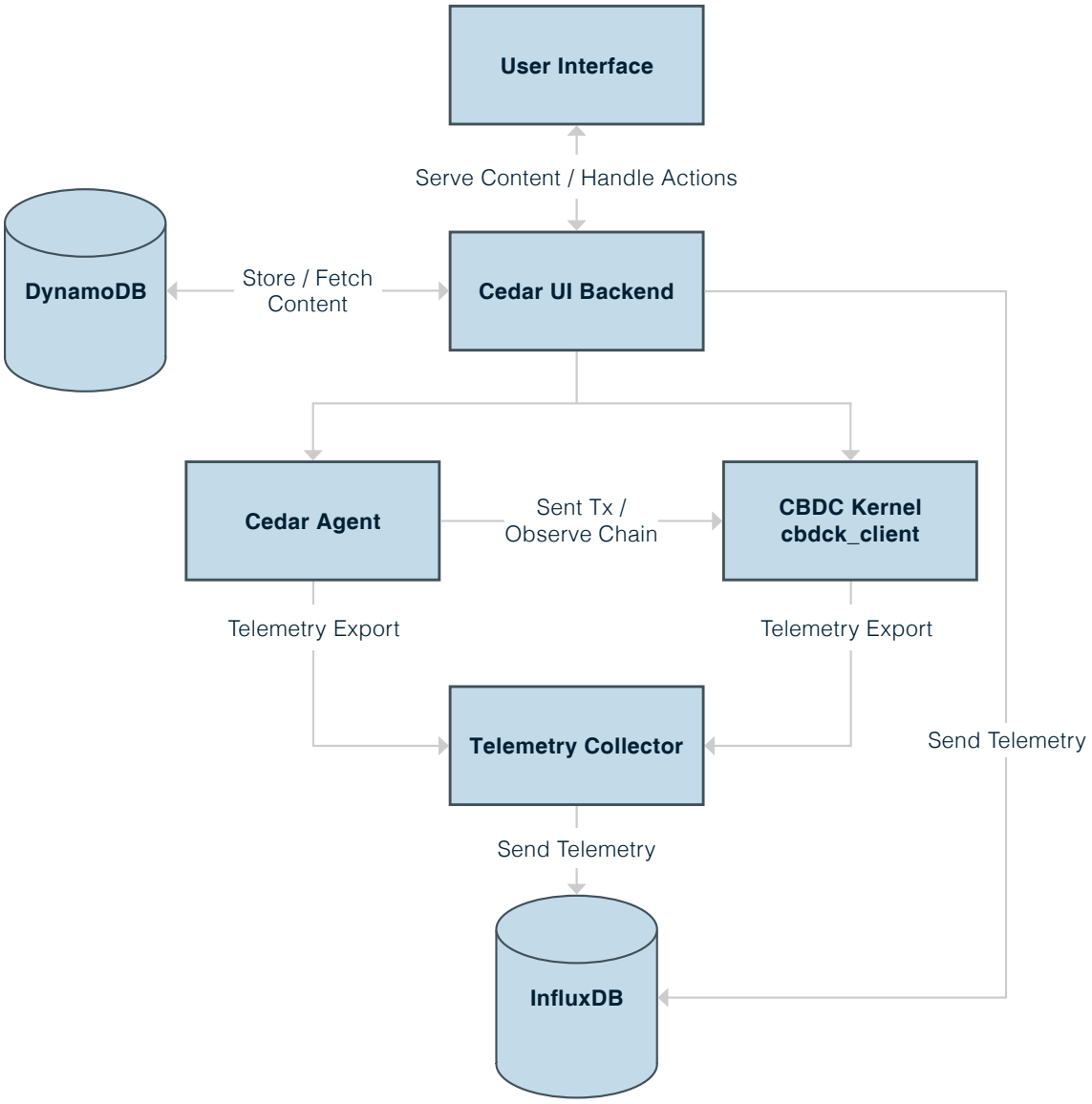
[6] An atomic cross-chain swap is a method of exchanging different digital currencies between participants in a system where either all or none of the assets associated with the transaction settle. The technical component that enables this in Project Cedar is a hashed timelock contract, which is further explained in the Solution Overview section of this report.

responsible for storing the state of the User Interface, connecting to the Cedar Agent to execute the atomic cross-chain swaps, and connecting to the Cedar Ledger to provide insight into the current state of the ledger (balances, for example). The Cedar UI Backend uses the Amazon Web Services (AWS) DynamoDB database for its persistent storage of trade details. The Cedar UI Backend also writes telemetry to the InfluxDB database, such that the performance of the system can be constantly monitored.

4. The **User Interface** is a web-based front-end tool using the React programming library that allows subject matter experts and other users to test and provide feedback on the prototype in a tangible way. It is designed to provide the minimal functions of a trading desk application, while being fully integrated with the underlying distributed ledger.

5. The **Telemetry Connector** subscribes to telemetry events published by the Cedar Ledger and the Cedar Agent over a ZeroMQ endpoint. When events like “SubmitTransaction” or “PublishBlock” occur inside these components, the Telemetry Connector will record the event in the time-series database (InfluxDB), which can then be queried for performance metrics parallel to the system’s operation.

Figure 2. Outline of System Component Interaction in the Project Cedar Prototype.



7 Infrastructure Components

The Project Cedar solution is built on the following foundational infrastructure components. Assessing alternative infrastructure was not in scope for Phase I.

- **AWS:** AWS is the cloud provider used in Project Cedar for rapidly spawning and terminating computing resources for conducting tests.
- **Terraform:** Terraform is an open-source infrastructure as code software tool created by HashiCorp. In Project Cedar, Terraform is used to deploy prototype and test resources on cloud providers by storing infrastructure as code, enabling the team to define, configure, and version infrastructure in a repeatable and scalable fashion.
- **Infux DB:** InfluxDB is a high-speed read and write database owned by Influx Data. In Project Cedar, it was used to collect various performance metrics involved in executing simulated trades at scale and present them for analysis. Some performance items could be collected directly from the underlying Linux operating system on which the services ran, but others were collected by exposing a metrics endpoint in Cedar Ledger. This took the form of a ZeroMQ endpoint that emitted timestamped messages corresponding to important events.

8 Solution Detail

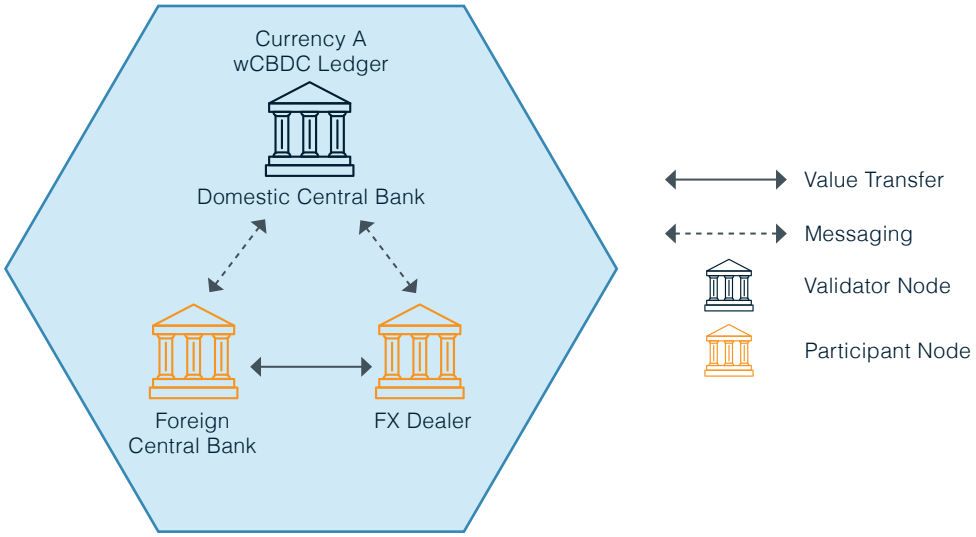
The Project Cedar Phase I solution was developed with the objective of enabling instant and atomic settlement through DLT, specifically in the context of a simulated FX spot transaction.

Phase I of Project Cedar aimed to build specific currency ledgers, each operated by its respective central bank. Within each currency ledger, the simulated domestic central bank operated validator nodes responsible for issuing its particular wholesale CBDC. At the request of a simulated foreign central bank

or participating FX dealer, the validator node may issue the requested funds to the requesting party, allowing the prototype to simulate transactions. Once the requested funds are successfully issued to the requesting party, the party may begin submitting wholesale CBDC transactions to the ledger. All transactions submitted are validated by the domestic central bank validator node and settled instantaneously and atomically.

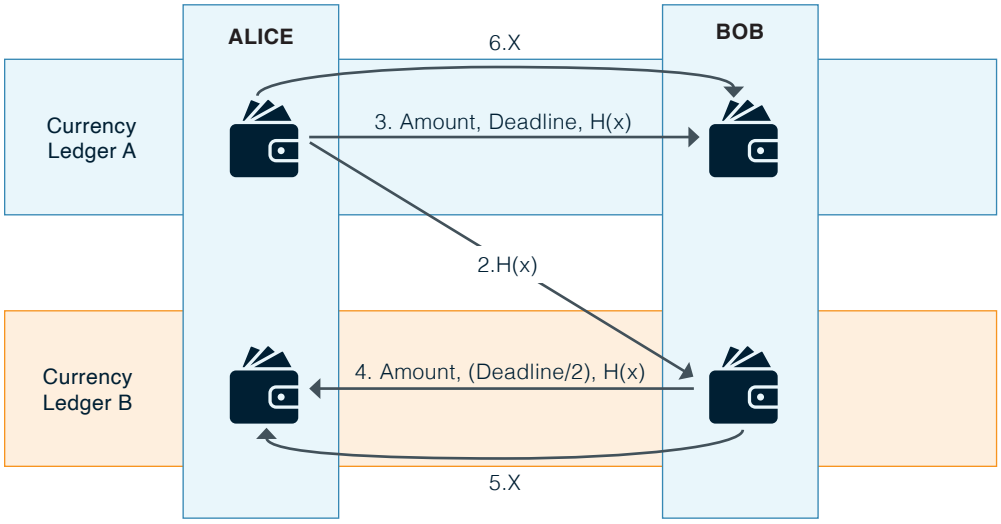
The diagram below represents how a hypothetical wholesale CBDC ledger, operated by the domestic central bank and leveraging the Project Cedar ledger design, would be set up for a transfer between two participants.

Figure 3. Hypothetical Wholesale CBDC Ledger



The core construction that enables settlement between two distinct currency ledgers is the HTLC. An HTLC cryptographically locks funds within a contract that the beneficiary of the payment must "unlock." In addition, the beneficiary must claim the funds prior to a defined deadline or the originator of the payment will be able to reclaim the funds. To settle the FX spot between two ledgers via HTLCs, an HTLC contract must be created on each respective currency ledger and bound by a common attribute (the pre-image, or secret), which enables the beneficiary to claim the funds locked in the HTLC. The figure below outlines the atomic swap process via HTLCs.

Figure 4. HTLC Atomic Cross-Chain Swap Process



HTLC Process Flow:

1. Alice and Bob agree on the trade details off-ledger (for example, counterparty, value, currency, FX rate).

2. Alice creates a secret x, a random character sequence, generates its hash, H(x), and provides H(x) to Bob.

3. Alice locks funds in an HTLC on Currency Ledger A that includes the amount, the hash, and the deadline.

4. Bob creates a corresponding HTLC on Currency Ledger B that includes the amount, the hash, and the deadline. However, Bob creates a shorter deadline on Currency Ledger B so that Alice can claim the funds on Currency Ledger B prior to Bob claiming his funds on Currency Ledger A and Bob is able to reclaim his funds before Alice is able to reclaim her leg of the transaction.

5. Alice claims the funds on Currency Ledger B by using the secret x she generated. This process reveals the secret to Bob.

6. Bob uses the secret revealed by Alice to claim the funds on Currency Ledger A.

Executing atomic transactions with HTLCs relies on certain assumptions and raises exception scenarios. For one, exchange of the hash and secret must be securely communicated off-chain. Additionally, because the claiming of funds is reliant on a secret, the loss of the secret will result in the entire swap not completing. Phase I did not include a comprehensive examination of these exceptions.

9 Testing Approach

Testing for Project Cedar Phase I focused on simulating the system through an automated test controller. The approach is described in the sections below.

Simulations: Simulations were deployed to determine whether the prototype met the established performance requirements and validated or invalidated the project's hypotheses. Metrics were captured via the established telemetry.

In every simulation, each currency is represented by a separate ledger containing three types of nodes with specific assigned functions.

- **Validator Node:** Each ledger is operated by a validator. This node simulates the role of the central bank, issuing its currency as simulated wholesale CBDC. It validates transactions coming from the network, produces signed blocks of validated transactions, and broadcasts those blocks to the network so that the central bank's signature can be validated and the ledger can be updated.
- **Observer Node:** Observers receive blocks passively from all central bank validator nodes and apply the changes to their local copies of the ledger state.
- **Participant Node:** Participants observe two ledgers in a similar way to the observers but are also transacting on these ledgers by executing the FX trades. They simulate the exchange of currency continuously at the speed allowed by the Cedar Agent's state machine or the main ledger, whichever allows less speed.

The table below highlights key results across three test scenarios. The scenarios were designed to assess the system's performance as it is scaled to include a broader number of simulated actors in the ecosystem. Each test scenario comprised a specific number of currencies (C), observers (O), and participants (P), as detailed below.

Table 1: Scenario Parameters

Scenario	Currencies	Observers	Participants
A	2	2	4
B	4	4	8
C	8	8	16

For each role in the system, EC2 virtual machines with the Cedar Ledger and Cedar Agent installed were deployed. For each simulation, the system ran for ten minutes, generating load and sending telemetry to the InfluxDB. After ten minutes, the processes were interrupted and the virtual machines were shut down. The entire cycle is repeated three times for each configuration.[7]

Results from individual runs may vary since the experiments ran on virtual machines, which share their system resources and networks with other clients of AWS, yielding slightly unpredictable performance. Repeating the experiment multiple times and averaging the results counters variability.

Testing Methodologies: In order to verify that the system performs correctly in a real-world setup, the system was deployed on Amazon EC2 instances in AWS.[8] Several distinct configurations were tested, including the configuration ultimately used for the prototype, providing insight into system performance across a range of conditions.

[7] InfluxDB is a time-series database that specializes in storing and aggregating real-time application metrics and resource monitoring for systems. In Project Cedar, InfluxDB is leveraged for metric collection, storage and retrieval for all of the metrics that are generated when running test runs. These metrics are then queried for analysis and compiled into the final performance results for Project Cedar. https://www.influxdata.com/

[8] https://aws.amazon.com/ec2/

The OpenCBDC Test Controller from the OpenCBDC project released by the MIT Digital Currency Initiative under the MIT License was modified and used to execute the tests.[9,10] This allowed for variation across the number of ledgers (currencies, for example) in use, the number of nodes following each of the ledgers, the amount and type of simulated load on the system, and the underlying compute resources (such as CPU, memory, and storage) available to the nodes.

Virtual Machine Configuration: The virtual machines used for the simulation testing are running Ubuntu Server 20.04 LTS and, unless otherwise specified, were of type m5.large (2 vCPUs, 8GB RAM), with a 20GB Elastic Block Store (EBS) disk.[11]

10 Targets And Metrics

Establishing baseline data for performance indicators was an objective of Phase I. Two minimum performance requirements were set:

1. **Speed:** Settlement in fewer than thirty seconds; this requirement stems from the instantaneous settlement objective and would represent a significant improvement from the current state settlement time of T+2 days.

2. **Throughput:** Settlement of greater than ten transactions per second for an individual wholesale CBDC ledger; this requirement was established based on estimates using SWIFT messaging data as a reference and reflecting current market volume.[12]

[9] https://github.com/mit-dci/opencbdc-tctl

[10] https://opensource.org/licenses/MIT

[11] https://aws.amazon.com/ebs/

[12] The SWIFT messaging system records approximately 46 million messages per day on average, with a peak of approximately 50 million. Subject matter experts estimate roughly 8-10 percent of those messages correspond to FX and that each transaction contains five to six messages. Assuming twenty four-hour availability translates to approximately ten transactions per second for an individual wholesale CBDC system.

In addition to the primary metrics of cross-chain swap latency and cross-chain swaps per second, supplementary metrics, described below, were selected to ensure a balanced view across the system. This enabled visibility into whether performance changes in one part of the system have a detrimental impact elsewhere.

Table 2: Phase I Supplementary Metrics

METRIC	DESCRIPTION
BLOCKS PER SECOND - MAIN LEDGER (AVERAGE/PEAK)	Number of blocks per second appended to the ledger over the total duration of the test cycle
BLOCK SIZE (AVERAGE/PEAK)	Size of the blocks over the test cycle in kB
MEMORY USAGE (AVERAGE/PEAK)	Amount of memory used by the software in MB
DISK I/O (AVERAGE/PEAK)	Amount of disk i/o used by the software in MB/s
TRANSACTION PROPAGATION (AVERAGE/PEAK)	Time it takes for a transaction to broadcast to all nodes in ms
BLOCK PROPAGATION (AVERAGE/PEAK)	Time it takes for a new block to propagate to all nodes in ms

Metrics were collected in a time-series database, InfluxDB. Integrating metrics capture into the prototype supports both the short-term simulation tests as well as the long-running prototype deployment.

Table 3 lists the collected events, Table 4 provides a further description of the fields used in the events, and Table 5 shows the tags used. Generic tags are automatically attached to every event.

Table 3: Collected Events

EVENT	FIELDS	DESCRIPTION
publish_block	block_id, num_txs block_slot, tps, bps, block_size	Emitted when a block producer makes a new block
confirm_transaction	transaction_id	Emitted when a node considers a transaction final, either by adding it to a block (for block producers) or when receiving it in a verified block (for other observers)
send_transaction	transaction_id	Emitted when a node submits a transaction to its peers
*r*eceive_transaction	transaction_id	Emitted when a node receives a transaction (for the first time) from one of its peers. Peers can learn about individual transactions, but this can also be triggered by the peer learning about the transaction in a block it received.
receive_block	block_id, block_slot, num_txs	Emitted when a block is received (for the first time) from one of its peers
verify_block	block_id, num_txs, verification_time	Emitted when a node has finished verifying a block
completed_swap	time_session_start, time_data_exchange, time_total	Emitted when the full process of an FX transaction has been completed
procstat	cpu_time_user, memory_data, read_bytes, write_bytes	Emitted every 10 seconds by Telegraf[3] with information about the Cedar Ledger's main process: how much CPU and Memory it uses, and how much storage I/O is happening
filecount	size_bytes	Emitted every 10 seconds by Telegraf[3] with the size of the Cedar Ledger's storage folder

Table 4. Field Descriptions

FIELD	DESCRIPTION
time	The nano-second precision time at which the event occurred
block_id	The unique ID of the block. Used to match publish_block and receive_block events to determine propagation times
block_slot	The slot of the block in the ledger. Ledgers start at block_slot 1 and each block has a sequentially incrementing block_slot.
tps	The current transactions per second at the time the block is published, calculated from dividing the number of transactions in the block by the seconds since the last block was published. These are the raw ledger transactions, not swap transactions (since each swap transaction consists of multiple ledger transactions)
bps	The current blocks per second at the time the block is published, calculated from the time since the last block was published
block_size	The serialized size of the block (in bytes)
transaction_id	The unique ID of the transaction. Used to match send_transaction and receive_transaction events to determine propagation times, and matching send_transaction and confirm_transaction to measure transaction latency.
num_txs	The number of transactions in a block

Table 5: Event Tags

TAG	DESCRIPTION	GENERIC
testrun_id	The ID of the test cycle that the event is a part of	Yes
testrun_role	The role of the current node within the test cycle's composition (For instance 'node-10'). Used to filter events that happened on a specific node in the network.	Yes
aws_region	The region in which the node that emitted the event was running	Yes
aws_instance_id	The ID of the instance on which the node that emitted the event was running	Yes
chain_label	The chain on which an event happened (transaction / block level events)	No
chain_labels	The chains between which the swap was conducted	No

11 Results

The results of running the simulation tests on the system are discussed below. The figures shown are the average across three runs with the given configurations. Each run simulated the system for ten minutes.

For reference, C/O/P in the tables below references currencies / observers / participants roles as described above.

Table 6 shows the matrix of our simulated setups, with the primary results.

Table 6: Primary Results for Phase I

TEST	PARAMETERS			CROSS-CHAIN SWAP LATENCY (in seconds)		CROSS-CHAIN SWAPS (per second)	
Scenario	Currencies	Observers	Participants	Mean	99th Percentile	Mean	Peak
A	2	2	4	9.05	14.54	10.91	33.27
B	4	4	8	8.52	12.84	18.78	47.20
C	8	8	16	8.96	15.86	37.53	98.93

As evidenced by the table, the system performs well within the set performance constraints of settling more than ten swaps per second and swaps completing within thirty seconds on average. Additionally, the global system throughput increases even as currencies are added, given that each currency operates on an individual ledger.

Currently, each currency pair is simulating a roughly equal volume in FX transactions. Given current system performance, doubling the number of currencies on the system will result in roughly double the number of swaps executed globally. In a real-world setting, different currency pairs will experience varying volumes. Modeling scalability across this variance was not in scope for Phase I of Project Cedar.

Additionally, test results from Phase I indicate that a modular ecosystem of ledgers has the potential for continued scalability and could be an area for further research and analysis. Test results show that as additional ledgers, participants, and observers are added to the system, the system performance remains stable. It should be noted that these early test results have not accounted for edge cases and different network configurations. Further analysis and testing would be required to draw any conclusions related to scalability.

Alongside these key results, additional metrics were gathered to gain more insight in respect to the prototype's performance. Tables 7-9 below provide this additional data.

Table 7: Block Propagation Time and Transaction Propagation Time

TEST	PARAMETERS			BLOCK PROPAGATION TIME (ms)		TRANSACTION PROPAGATION TIME (ms)	
Scenario	Currencies	Observers	Participants	Mean	99th Percentile	Mean	99th Percentile
A	2	2	4	593.92	16957.23	168.28	1549.50
B	4	4	8	549.85	22263.45	168.64	1486.06
C	8	8	16	686.09	13971.77	1071.44	6742.54

Table 8: Block Size and Blocks per Second

TEST	PARAMETERS			BLOCK SIZE (kB)		BLOCKS (per second)	
Scenario	Currencies	Observers	Participants	Mean	Peak	Mean	Peak
A	2	2	4	14.02	61.12	0.48	1.31
B	4	4	8	12.21	55.46	0.48	1.29
C	8	8	16	12.21	101.37	0.48	1.36

Table 9: CPU, Memory, and Disk I/O

TEST	PARAMETERS			CPU (percent)		MEMORY (MB)		DISK I/O (MB/s)	
Scenario	Currencies	Observers	Participants	Mean	Peak	Mean	Peak	Mean	Peak
A	2	2	4	13.16	32.43	173.00	341.18	4.38	11.39
B	4	4	8	13.15	29.42	178.14	308.04	4.25	9.91
C	8	8	16	16.72	57.40	205.96	448.09	4.97	11.29

12 Acronyms, Abbreviations, and Terms

ACRONYM OR TERM	DEFINITION
AML	Anti-money laundering
ATOMIC / ATOMICITY	Settlement that occurs simultaneously; funds are released by one party only in the event of release of funds by the other party
BIS	Bank for International Settlements
BLOCK PROPAGATION TIME	The time it takes for a block to reach the majority of the network
BLOCKS PER SECOND	Frequency at which a new block of verified transactions is emitted
BOC	Bank of Canada
BOT	Bank of Thailand
CAD	Canadian dollar
CBDCS	Central bank digital currencies
CFT	Countering the financing of terrorists
CLS	Continuous Linked Settlement
CPU	Percentage of CPU time being used by the Cedar Ledger; measured as a percentage of a single CPU[13]

[13] Since the simulation is running on 2vCPU machines, this number can go up to 200 percent.

DISK I/O	Disk i/o generated by the Cedar Ledger
FX	Foreign exchange
HKMA	Hong Kong Monetary Authority
HTLC	Hashed timelock contracts
INSTANTANEOUS SETTLEMENT	Exchange of assets between the counterparties of a transaction occurring in fewer than thirty seconds
LATENCY	Time between the submission of the transaction to the network and the confirmation of acceptance by the network
MAS	Monetary Authority of Singapore
MEAN	Mean across all measured datapoints in the course of the test run
MEMORY	Memory used by the Cedar Ledger
NYIC	New York Innovation Center
OFAC	Office of Foreign Assets Control
PEAK	Highest measured single datapoint over the course of the test run
POC	Proof-of-concept
SGD	Singapore dollar
SMART CONTRACT	A self-executing contract in which the terms of the agreement are reflected in lines of code and the code controls the execution of the contract based on whether those terms are met
SWAPS PER SECOND	Mean number of cross-chain swaps completed per second over the course of the test run
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TRANSACTION LATENCY	Time between a single ledger transaction being submitted and received back in a signed block
TRANSACTIONS PER SECOND	Number of ledger transactions verified per second[14]
TRANSACTION PROPAGATION TIME	Time it takes for a transaction to reach the majority of the network
UI	User Interface
UNSPENT TRANSACTION OUTPUT (UTXO)	A model for digital currency in which excess payment in a transaction is minted in the form of a new output, representing the leftover fraction from the original payment
WHOLESALE CBDCs	Wholesale central bank digital currencies
99%	99th percentile of the measured datapoints

[14] These are not the FX transactions, but individual ledger transactions. They reflect averages over individual ledger measurements, not across the entire system.