BIS Innovation Hub

Hong Kong SAR Centre

Inthanon-LionRock to mBridge

Building a multi CBDC platform for international payments

September 2021

HONG KONG MONETARY AUTHORITY
香港金融管理局

ธนาคารแห่งประเทศไทย
BANK OF THAILAND

中国人民银行
数字货币研究所
DIGITAL CURRENCY INSTITUTE
PEOPLE'S BANK OF CHINA

United Arab Emirates

مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

Abstract

This report sets out the take-aways of Project Inthanon-LionRock Phase 2 and introduces the scope of the third phase. Phase 2 achieved a prototype that enables three participating central banks to control the flow of their CBDC and to monitor transactions and balances of their issued CBDC, with programmable levels of transaction privacy and aspects of automated compliance. The prototype demonstrates a substantial increase in cross-border transfer speed from days to seconds, as well as the potential to reduce several of the core cost components of correspondent banking. It thereby demonstrates the potential of faster and lower cost cross-border transfers for participating jurisdictions. The benefits would be further increased for jurisdictions that do not benefit from a vibrant correspondent banking network. With the joining of 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, the project has evolved into Phase 3 and to this effect has been renamed mCBDC Bridge project or, in short, mBridge. 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. To achieve this, collaboration with the public and private sector will continue and trials will be conducted in a safe environment.

> Money is one of humanity's greatest inventions. It enables you to specialise in one profession instead of having to do everything by yourself or go through all the fuss of bartering goods. It brings the best out of every individual, according to individual capabilities. Money is, so to speak, the oil that makes the machinery work.[1]
>
> **Agustin Carstens**
> General Manager of the Bank for International Settlements

[1] See Translation of an interview with Mr. Agustin Carstens, General Manager of the BIS, in Basler Zietung, 25 June 2018. https://www.bis.org/speeches/sp180704a.htm .

Phase 2 prototype built in collaboration with:

On open-source enterprise Ethereum:

Special Thanks: Raphael Auer, Codruta Boar, Jon Frost, Henry Holden, Ben Dyson, Anneke Kosse, Thomas Lamar, Tara Rice, Takeshi Shirakami, and Thomas Nilsson.

Contents

Executive Summary **6**

1 Central bank journeys **10**

1.1 BIS Innovation Hub 10

1.2 Hong Kong Monetary Authority 11

1.3 Bank of Thailand 12

1.4 Digital Currency Institute of the People's Bank of China 13

1.5 Central Bank of the United Arab Emirates 15

2 Project overview **18**

2.1 Background 18

2.2 Vision 20

2.3 Goals and objectives 24

2.4 Functional scope 25

2.4.1 CBDC operations 25

2.4.2 Foreign exchange (FX) execution models 25

2.4.3 Accessibility 25

2.4.4 Liquidity management 25

2.4.5 Regulatory compliance 25

2.5 Non-functional scope 26

2.5.1 Scalability 26

2.5.2 System performance 26

2.5.3 System availability 26

2.5.4 Transaction privacy 26

3 Inthanon-LionRock Phase 2 **28**

3.1 Operating model 28

3.1.1 Speed 29

3.1.2 Costs 32

3.2 Technical solution 34

3.2.1 System architecture 34

3.2.2 Model design 38

3.3 Operational considerations 46

3.3.1 Deployment 46

3.3.2 Performance and resiliency 47

3.3.3 Data Privacy and protection 49

3.3.4 Disaster recovery 50

3.3.5 Cybersecurity 50

4 mBridge **52**
4.1 Phase 3 52
4.2 Governance 54
4.2.1 Steering committee 54
4.2.2 Technology sub-committee 55
4.2.3 Legal sub-committee 55
4.2.4 Policy sub-committee 55
4.2.5 Business sub-committee 55
4.3 Roadmap 56

5 Conclusion and next steps **58**

Annex 1 Terminology **62**
Project stages 62
Public-private key cryptography 63

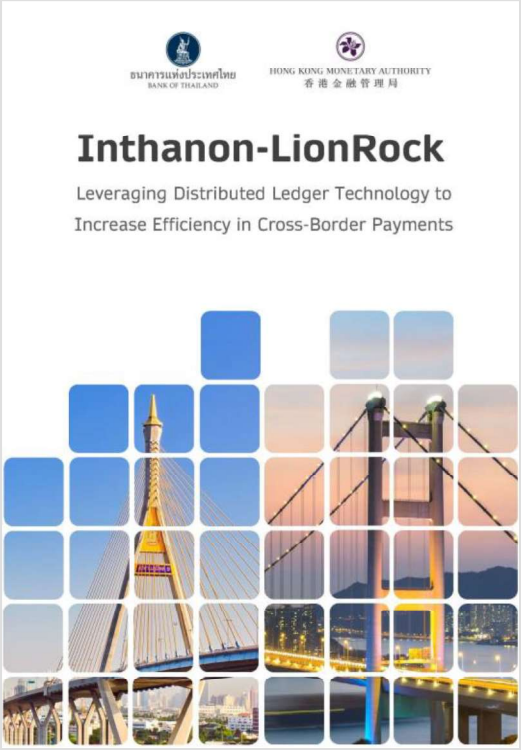
Annex 2 FX quote flow charts **65**
Request for quote 65
Off-bridge 66
Board rate 67

Annex 3 Project participants **68**
BIS Innovation Hub 68
Hong Kong Monetary Authority 68
Bank of Thailand 68
Digital Currency Institute of the People's Bank of China 69
Central Bank of the United Arab Emirates 70
Vendors 70

Executive Summary

With the signing by the Hong Kong Monetary Authority (HKMA) and the Bank of Thailand (BOT) of a joint memorandum of understanding (MOU) in May 2019, Project Inthanon-LionRock embarked on the first common platform for multiple CBDC settlement, corresponding to a BIS Model 3 arrangement based on a single multi-currency system.[2]

Project Inthanon-LionRock Phase 1 achieved a proof-of-concept (PoC) single platform built by R3 on Corda, designed to allow the participants of each network to conduct fund transfers and foreign exchange transactions on a peer-to-peer basis, thus reducing settlement layers. The platform also aimed to enhance banks' foreign currency liquidity management by adopting a multiple currency liquidity saving mechanism and incorporated streamlined compliance with local regulations. The findings of Phase 1 were published in January 2020.[3]



Source: Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020

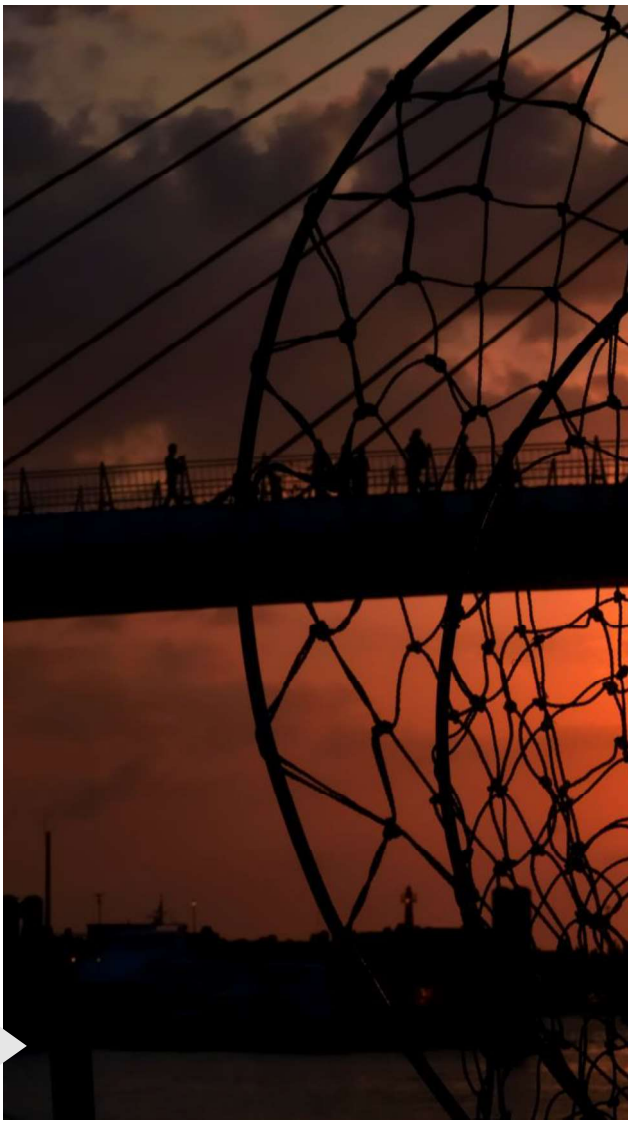
[2] See CPMI, BISIH, IMF and the WB, Joint report to the G20, Central bank digital currencies for cross-border payments, July 2021, https://www.bis.org/publ/othp38.pdf .

[3] See Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf .

Upon completion of Phase 1, the BOT and HKMA agreed to proceed further with joint applied technology research and cross-border fund transfer trials, in collaboration with participating banks and other relevant parties. The goals were to enhance the Phase 1 prototype to support CBDCs from other jurisdictions, to continue investigating different design trade-offs, and to explore business use cases and connections to other platforms. This took the shape of Project Inthanon-LionRock Phase 2, the findings of which are summarised in the present report.

The Project Inthanon-LionRock Phase 2 prototype (also referred to as the IL2 prototype) is built by ConsenSys on Hyperledger Besu. The prototype encompasses Thailand, Hong Kong and two additional jurisdictions. Participating central banks are able to control the flow of their CBDC on the prototype, monitor transactions and balances of their issued CBDC, utilise programmable levels of transaction privacy, and automate certain compliance functions. The operating model, technical solution and operational considerations are further explained in Section 3.

The prototype demonstrates a substantial improvement in cross-border transfer speed from multiple days to seconds, as well as the potential to reduce several of the core cost components of correspondent banking. It thereby demonstrates the potential of faster and lower cost cross-border transfers for participating jurisdictions. As explained in Section 2, the benefits would be further increased for jurisdictions that do not benefit from a vibrant correspondent banking network due to the retreat of correspondent banks.



With the joining of the BIS Innovation Hub (BISIH) Hong Kong Centre, the Digital Currency Institute (DCI) of the People's Bank of China (PBC) and the Central Bank of the United Arab Emirates (CBUAE) in February 2021, the project has now evolved into Phase 3 and to this effect has been renamed as the mCBDC Bridge project or, in short, mBridge.

Phase 3 involves further experimentation with design choices, technology trade-offs, and defining a future roadmap from prototype to an open-source, production-ready system. In Section 4 we include an overview of the current governance of the project, further objectives, and the scope of continued experimentation and trials that we are envisioning in the months ahead.

The overall goal of the project throughout these three phases remains unchanged: to design and iterate a new efficient cross-border payment infrastructure that improves on key pain points, including high cost, low speed, and operational complexities. Each of the phases of the project, including the current one, are set as agile experiments, in a safe environment, with due consideration of technological, policy, legal and business considerations. Each of the steps to date have led to incremental learnings that will contribute to the evolution from current prototype to pilot, becoming a minimum viable product (MVP) and, eventually, a production-ready network that can serve the broader central banking community as a public good through open-sourcing.

As concluded in Section 5, we are proud to continue taking steps towards the G20 mandate of creating cheaper, faster and more resilient cross-border payments and look forward to continuing to contribute to the international dimension of this work, including by welcoming more central banks to our agile and experimentation-driven journey founded on the principles of *do no harm, compliance and interoperability.*[4]

[4] See also Agustin Carstens, General Manager of the BIS, Central bank digital currencies: putting a big idea into practice, March 2021, https://www.bis.org/speeches/sp210331.pdf .

1 Central bank journeys

1.1 BIS Innovation Hub

The Bank for International Settlements (BIS) has long kept a close eye on fintech innovation. Witnessing the speed of change and the potential impact on central banking, we embarked in 2019 on a new journey – that of creating the BIS Innovation Hub (BISIH). The BISIH is the youngest member to the BIS family, yet in barely two years since its inception, it has accomplished a lot, tapping the talent and enthusiasm of its multidisciplinary team of regulators, economists, market practitioners and technology experts.

We started with defining our work program to focus on six themes: Supervisory technology (suptech) and Regulatory technology (regtech), Next-generation financial market infrastructures, Central Bank Digital Currency (CBDC), Open finance, Cyber security and Green finance. It comes as no surprise that CBDC is a standalone theme that we decided to focus our knowledge, expertise and creative energy towards, alongside a growing number of central banks that are rolling out prototypes and pilots. *How to best execute on CBDCs? Which pain points and use cases to focus on? How CBDCs can be interconnected and help make cross-border payments cheaper and faster? Which design choices to make?* are some of the most pressing, and hardest, technology questions facing central banks.

Central banks, embodying market stability, security and safety, cannot act in an ill-thought-through or rash manner. It is easy to move fast and break things. Not breaking things is more difficult. To do the latter, we need to move together. mBridge[3] is an integral part of this journey. Through it, the BISIH Hong Kong Centre is working with our central bank partners to iteratively improve the prototype. Next, we will extend collaboration with the private sector through further experimentation and trials in a safe environment.

Aside from mBridge, the BISIH is also furthering CBDC in a series of other projects across its centres. Project Aurum, the Latin word for gold, is also a partnership between the BISIH Hong Kong Centre and the Hong Kong Monetary Authority. It is the first retail CBDC project of the BISIH, and undoubtedly not the last.[6] In addition, the BISIH Swiss Centre is building on the foundations laid by project Helvetia to extend the exploration into project Jura, where the focus is on cross-border wholesale settlement for tokenised securities. Similarly, project Dunbar in the Singapore Centre explores multiple CBDCs.

In the coming months, the expansion of the BISIH to Frankfurt and Paris, London, Stockholm and Toronto, and our strategic partnership with the Federal Reserve Bank of New York, will provide further impetus to our CBDC work programme. Taken together, we believe that these explorations, each coming from different angles and exploring different design choices, will provide the BISIH, and with it the central banking community, a solid foundation to face the next stage of central banking – *that of digital money backed by the trust in central banks*.

Benoît Cœuré
Head of BIS Innovation Hub of the Bank for International Settlements

[5] See BISIH website https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm .
[6] See BISIH website https://www.bis.org/about/bisih/topics/cbdc/rcbdc.htm .

1.2 Hong Kong Monetary Authority

Hong Kong's robust financial infrastructure has been the cornerstone of the city's success as an international financial centre. To ensure that this status can endure in the decades ahead, and to secure our future for the generations to come, it is crucial that the city's infrastructure, especially our payment infrastructure, is proactively and continuously enhanced. Inspired by the considerable potential that Distributed Ledger Technologies (DLT) hold, the HKMA has been researching DLT-based CBDCs since 2017 to understand their benefits and possible applications.

Named after Hong Kong's most iconic mountain, the HKMA commenced Project LionRock in 2017 in collaboration with the three note-issuing banks[7] and the Hong Kong Interbank Clearing Limited.[8] This proof-of-concept project studied potential applications of CBDCs in Hong Kong and demonstrated the ability of CBDCs in handling large-value payments and delivery-versus-payment settlements.

In 2019, the HKMA decided to explore expanding the functionalities of the proof-of-concept to include cross-border transactions and FX settlements through collaboration with the Bank of Thailand in Project Inthanon-LionRock. A common platform that enabled real-time cross-border funds transfers between the participating banks on a peer-to-peer basis was developed.

Starting February 2021, the BISIH Hong Kong Centre, the Digital Currency Institute of the People's Bank of China (PBC) and the Central Bank of the United Arab Emirates joined the project – now called mBridge. We are pleased to set out our findings and areas for future research and development in this report, with a focus on driving to live and production usage.

In addition to the continued effort on wholesale CBDCs, the HKMA is also strengthening its research work to increase Hong Kong's readiness in terms of adopting CBDCs at the retail level. Together with the BISIH Hong Kong Centre, we started applied technology research and set up an internal cross-departmental working group to explore the prospect of issuing e-HKD. Meanwhile, the HKMA continues to support the PBC on the technical testing of e-CNY in Hong Kong for facilitating cross-border payments between Hong Kong and Mainland China.

Howard Lee
Deputy Chief Executive of the Hong Kong Monetary Authority

[7] Hong Kong's currency notes, except for $10 notes, are issued by commercial banks. Currently, there are three note-issuing banks in Hong Kong, namely The Hongkong and Shanghai Banking Corporation Limited, the Standard Chartered Bank (Hong Kong) Limited and the Bank of China (Hong Kong) Limited.
[8] Hong Kong Interbank Clearing Limited provides interbank clearing and settlement services to all banks in Hong Kong and operates a central clearing and settlement system for public and private debt securities on behalf of the HKMA.

1.3 Bank of Thailand

The Bank of Thailand (BOT) envisions the financial sector as being one of the key drivers behind Thailand's digital transformation, and CBDC as having the potential to become the foundation for the nation's digital financial system in the future. With this vision in mind, the BOT set out to conduct hands-on experimentation in collaboration with the private sector, to explore how emerging technologies can be used to better serve stakeholders and address long-standing pain points in our financial system, all the while providing the trust and protection of the central bank.

In 2018, Project Inthanon was initiated in collaboration with eight leading domestic banks to build a proof-of-concept DLT-based real time gross settlement system using wholesale CBDC. Upon the success of Project Inthanon's third phase, Project Inthanon-LionRock, which was conducted in collaboration with the Hong Kong Monetary Authority to explore the potential of a cross-border wholesale CBDC; we wished to scale our experimentation to include more currencies and jurisdictions to simulate real-world conditions as best as possible. We are therefore excited, to continue the joint experimentation with the BISIH Hong Kong Centre, the Hong Kong Monetary Authority, the Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates.

The BOT has also simultaneously expanded its CBDC focus to the corporate and retail level. In 2020, we partnered with two domestic firms to explore how CBDC could be used to reduce pain points in business payments, marking the first time the BOT expanded the scope of CBDC development to business users. A two-tier CBDC system prototype was successfully built and basic functionalities of CBDC were achieved. In addition, complex functionalities such as invoice tokenisation and programmable money were accomplished using smart contracts.

In the coming year, the BOT will also focus on the research and development of a publicly accessible retail CBDC. Our main objective in exploring retail CBDC is aimed at providing citizens with access to a digital form of central bank money, which is trustworthy and secure. In addition, the development of a retail CBDC will support a technology-led future financial sector and contribute to the development of more diverse and innovative financial services.

However, the design of CBDC for widespread usage will need to take into consideration safety and efficiency as well as implications on monetary policy, financial system stability, and the roles of financial institutions and the central bank. Thus, we intend to closely involve relevant stakeholders throughout the CBDC development process, to ensure that it is conducive to financial innovation in this era of digital transformation.

Vachira Arromdee
Assistant Governor of the Financial Markets Operations Group of the Bank of Thailand

1.4 Digital Currency Institute of the People's Bank of China

Given the economic evolution towards digital, starting as early as 2014, the People's Bank of China (PBC) set up a task force to analyse the possible development of CBDC. Focus areas included the issuance framework, critical technologies, circulation environment, and relevant international experience.

This was followed in 2016 by the establishment of the Digital Currency Institute (DCI). Since 2017, the PBC DCI added to its R&D strength, joining forces with the market, including several leading commercial banks, telecom operators, and payment service providers (PSPs). PBC DCI research is conducted in a prudent, safe, managed, innovative, and practical manner. This approach cumulated in the creation of the Chinese CBDC, which system was named as Digital Currency Electronic Payment (DCEP), and the currency later named as e-CNY.

The objectives of the e-CNY are as follows: improving central bank payment system efficiency; complementing the current retail payment service; securing the access to the central bank money, while providing the payment market participants with a level playing field; safeguarding monetary sovereignty; reducing the cost for physical cash issuance and management; and improving financial inclusion and privacy protection.

The e-CNY is positioned mainly as M0, in other words, a central bank liability to the public with legal tender like cash. It is backed 100 percent by reserves in PBC and is not anticipated to pay any interest to avert disintermediation risk.

The e-CNY adopts a two-tier system under which the PBC issues e-CNY to second-tier commercial institutions, which then circulate the e-CNY to the public. The second-tier commercial institutions include six commercial banks, three telecom operators, and two PSPs (in the name of their commercial bank entity). These commercial institutions take on responsibilities such as performing anti-money laundering controls, providing privacy protection, and investing in technology. More details are available in a paper recently published by the PBC.[9]

e-CNY is a hybrid system - compatible with token-based, account-based, and quasi-account-based systems. It is also characterized as "managed anonymity". In terms of "anonymity", the e-CNY wallet adopts a loosely coupled design and a tiered arrangement based on the know-your-customer (KYC) level - certain low-value, capped wallets can be opened merely by a mobile phone number, while high-value wallets require advanced KYC. Also, the safety of customers' personal information is achieved by encryption and tokenisation. In terms of "managed", the e-CNY system is designed to achieve compliance with international anti-money-laundering standards. It will leverage its technological capacity to identify suspicious transactions in a timely way pursuant to the relevant law and regulations.

[9] See PBC, Progress of Research & Development of E-CNY in China, July 2021, http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf .

The e-CNY pilot project is going smoothly. So far pilots have been running in 10 areas and the winter Olympics use cases in Beijing. A series of use cases covering catering, tourism, transportation, utility fees etc. have been explored. Payment methods such as QR code and tap-and-go have been well-supported and innovative services such as dual-offline payment and wearable device payment have been tested for safety and efficiency. The promotional activities in those pilot areas have shown to be popular among the citizens and have helped stimulate consumption, thereby benefitting the real economy.

The PBC is prudent yet open-minded about exploring the cross-border payment use case for CBDC, subject to the base *principles of do no harm, compliance and interoperability*.[10] Pursuant to this, the PBC guided the DCI to explore the feasibility of cross-border payments through trial pilots. The DCI has signed a memorandum with the Hong Kong Monetary Authority and successfully carried out the first stage of e-CNY cross-border payment technical testing. The participation of the PBC DCI in the mCBDC Bridge project follows the same philosophy of prudent testing and adherence to the three base principles.

Changchun Mu
Director-General of the Digital Currency Institute of the People's Bank of China

[10] See Changchun Mu, PBC, at BIS Innovation Summit 2021, https://www.youtube.com/watch?v=Dywea8d9YW4 .

1.5 Central Bank of the United Arab Emirates

With the global economy being more interconnected than ever and the increased volume of money flowing across borders, more efficient and effective methods of both domestic and cross-border fund transfers are needed. For decades, the high cost, inefficiencies, and delays around cross-border payments have been notorious pain points. Against this backdrop and underpinned by a robust commitment to drive the United Arab Emirates' digital transformation across the financial and banking sectors, the Central Bank of the United Arab Emirates (CBUAE) embarked on a journey in 2018 to explore the feasibility of developing cross-border payment infrastructures that would address these shortcomings.

CBUAE began this journey with its neighbours from the Gulf Cooperation Council (GCC) to jointly implement two cross-border multi-currency wholesale payment platforms developed on conventional payment infrastructures, including:

- **GCC Real Time Gross Settlement (RTGS) System:** in 2020, all GCC central banks worked together to launch a regional RTGS system to allow cross-border wholesale payments between GCC countries in their domestic currencies, with foreign exchange (FX) conversion support provided within the system.
- **Arab Regional Payment System:** The system, which went live in 2020, has the capability of processing cross-border payments for a number of eligible currencies without any FX conversion. The project, which covered all Arab countries in the Middle East and North Africa region, is led by the Arab Monetary Fund and overseen by a committee of central banks chaired by CBUAE.

In addition to implementing the two conventional cross-border payment infrastructures referenced above, in 2019, CBUAE also successfully completed a CBDC proof-of-concept study titled *Project Aber*[11] (the Arabic translation of the term Aber is "crossing boundaries"). In partnership with the Saudi Central Bank (SAMA), CBUAE explored the feasibility of a DLT solution for both domestic and cross-border fund transfers. Under *Project Aber*, the respective central bank is the sole issuer of its CBDC, which is only tokenised by and redeemed against the issuing central bank. The AED/SAR peg to the USD enables Project Aber to eliminate any FX variations, making it swift and efficient to settle cross-border transactions.

Project Aber is the first CBDC project adopting a dual-issued CBDC and a single network concept for cross-currency payments. Using this CBDC as a unit of settlement between commercial banks in the two countries prevents any FX conversion and FX settlement as well as the need for the payment-versus-payment (PvP) arrangement. In addition, it significantly eliminates inefficiencies in the existing correspondent banking payment methods, which often result in delays and trapped liquidity. What's more, the movement of funds is conducted in real-time, eliminating the requirement for a correspondent bank with a nostro account in each country. The project has also demonstrated the possibility of using CBDC for domestic inter-bank payments, in turn highlighting the potential of CBDC to be adopted as a back-up facility for domestic RTGSs, which, among others, can aid in mitigating and addressing the risk of cyber-attacks. In Project Aber, settlement finality and irrevocability are ensured by requiring a signature for all transactions. The initiative has demonstrated that the system is capable of providing settlement finality involving CBDC or token exchanges between participating parties.

[11] See CBUAE and SAMA, Project Aber report, https://www.centralbank.ae/sites/default/files/2020-11/Aber%20Report%202020%20-%20EN_4.pdf .

Project Aber was achieved through fruitful collaboration underpinned by valuable contributions from CBUAE and SAMA, as well as the participation of commercial banks, technology partners and development teams, reflecting the shared urgency to shape the application of DLT to overcome existing hurdles in cross-border transfers. Building on this momentum, CBUAE is looking forward to leveraging the experience gained thus far and participating in the mCBDC Bridge project, alongside its esteemed peer central banks. While the journey ahead certainly has its challenges, CBUAE believes that it will also reap great rewards.

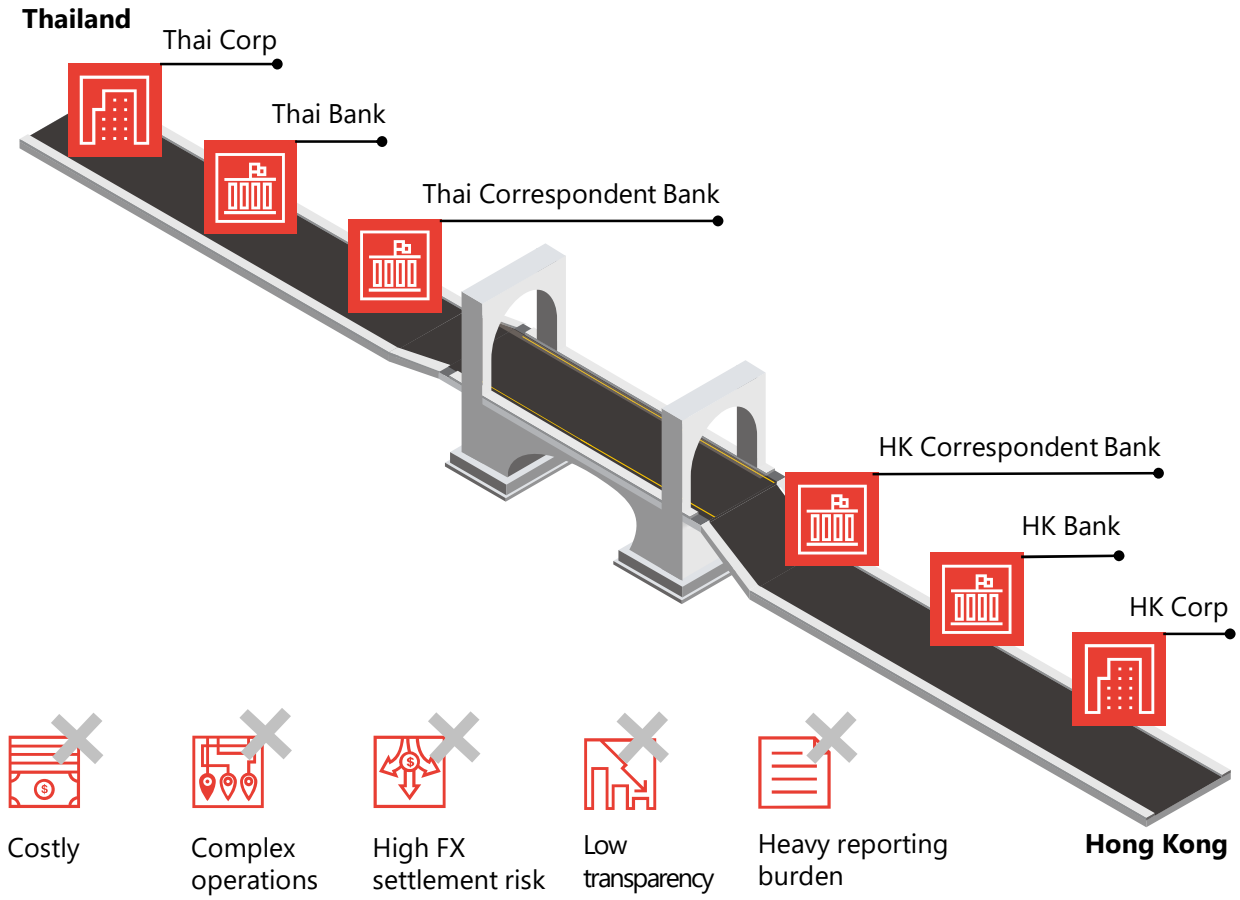
Saif Al Dhaheri
Assistant Governor – Strategy, Financial Infrastructure, and Digital Transformation of the Central Bank of UAE

2 Project overview

2.1 Background

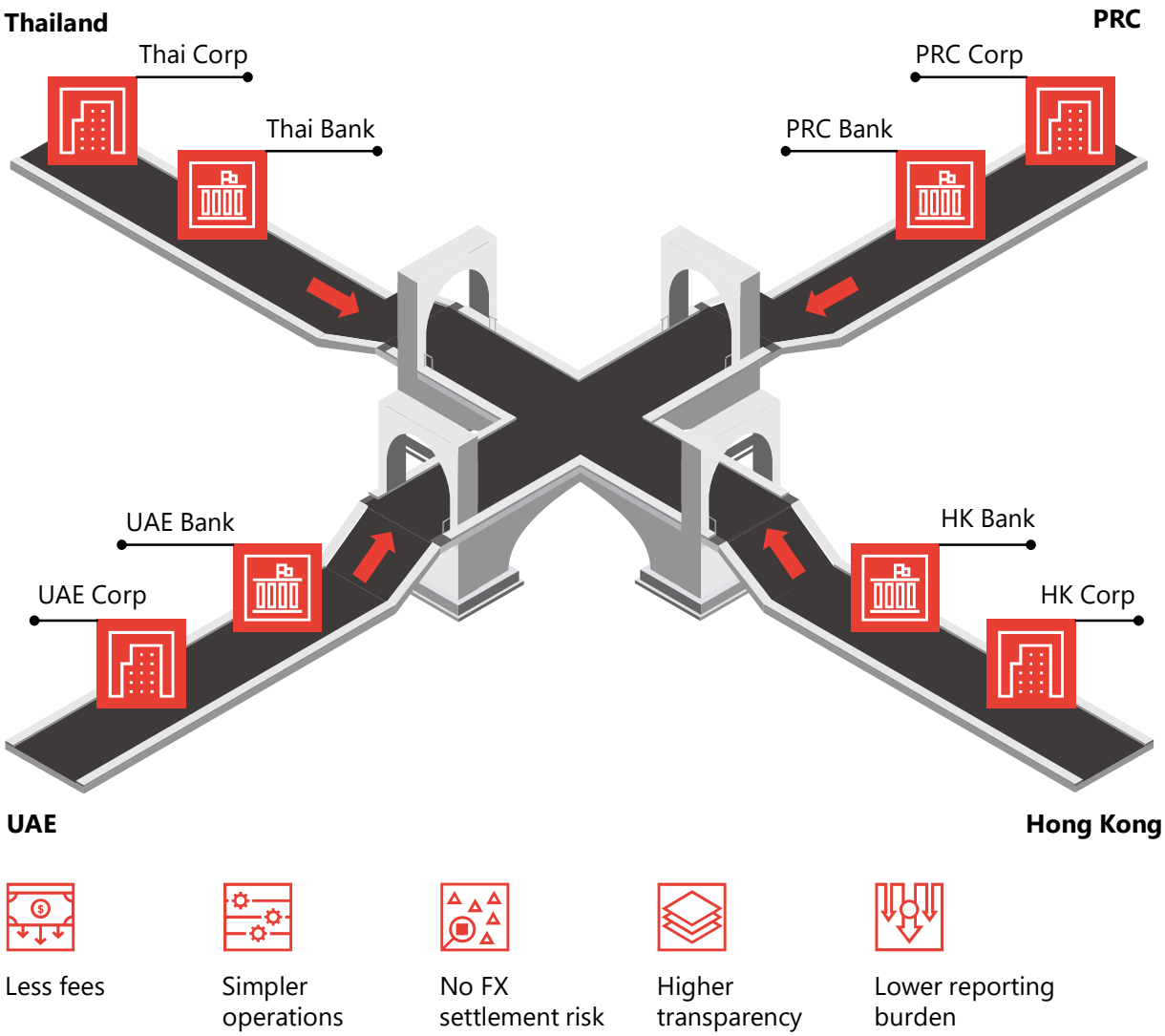
In the absence of multilateral solutions for cross-border payments, correspondent banks currently act as bridges, moving payments from one jurisdiction to another. To achieve this, they have built extensive correspondent banking networks and arrangements. While serving a critical economic role, these networks and arrangements also introduce more intermediary steps in the system, as correspondent banks are spread out across multiple time zones and different operating hours. This leads to increased operational complexity, possible bottlenecks and duplication. For example, know-your-customer (KYC) processes are repeated by every bank in the correspondent banking process flow. As illustrated in the published report of Inthanon-LionRock Phase 1 this in turn leads to higher cost and slower speed of cross-border payments. This process complexity also is paired with high FX settlement risk, low transparency and a high reporting burden.[12]

Existing mode of cross-border fund transfers and its pain points



[12] See Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf .

Inthanon-LionRock and mBridge Model



Source: Adapted from Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020

The G20 has made enhancing cross-border payments a priority.[13] As concluded in Rice et al (2020) *"Technological developments, as well as private and public sector initiatives, could help to reduce frictions in cross-border payments. Further monitoring and action are warranted to ensure that all countries enjoy access to safe, low-cost cross-border payment channels."*[14] Within this frame of mind, central banks have been increasingly experimenting with CBDCs and DLT as the foundation of a new type of payments infrastructure that has the potential to make cross-border payments faster, cheaper, and safer by reducing the risk and burden of intermediary banks.

[13] See CPMI, Enhancing Cross-border Payments Stage 1 report to the G20, April 2020, Enhancing Cross-border Payments: Stage 1 report to the G20 https://www.fsb.org/wp-content/uploads/P090420-1.pdf .
[14] See Tara Rice, Goetz von Peter and Codruta Boar, On the Global Retreat of Correspondent Banks, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003g.pdf .

2.2 Vision

Against this backdrop, the overall goal of the project throughout its phases remains unchanged: to design new efficient cross-border payment infrastructure that improves on key pain points, including high cost, low speed, and operational complexities.[15,16] The project supports the efforts of the G20 roadmap for enhancing cross-border payments, in particular the Building Block 19 on factoring an international dimension into the CBDC design. Action 1 of Building Block 19 concluded[17] that CBDCs can help to enhance cross-border payments when authorities coordinate internationally. To achieve the potential benefits for public welfare while preserving financial stability, further exploration of design choices and their macro-financial implications is essential.

[15] See also Bénédicte Nolens, BISIH Hong Kong Centre Head, at the MIT CEBRA High-Level Panel on CBDC and the future of payments, https://cbdcbgnews.com/2021/08/19/cebra2021-high-level-panel-cbdc-and-the-future-of-payments/ .
[16] See Raphael Auer, Giulio Cornelli and Jon Frost, BIS Working Papers No 880, Rise of the central bank digital currencies: drivers, approaches and technologies, August 2020, https://www.bis.org/publ/work880.pdf .
[17] See CPMI, BISIH, IMF and the WB, Joint report to the G20, Central bank digital currencies for cross-border payments, July 2021, https://www.bis.org/publ/othp38.htm . See also Raphael Auer, Philipp Haene and Henry Holden, Multi-CBDC arrangements and the future of cross-border payments, https://www.bis.org/publ/bppdf/bispap115.htm .

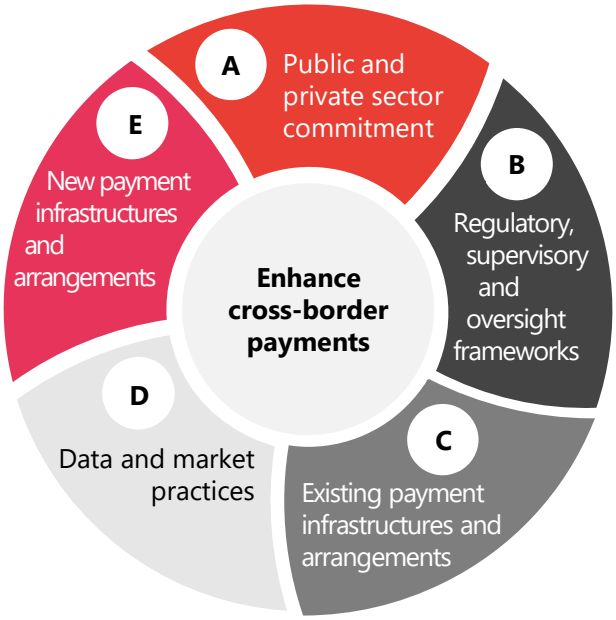
Roadmap to enhancing cross-border payments

1. Develop common cross-border payments vision and targets
2. Implement international guidance and principles
3. Define common features of cross-border payment service levels

A

4. Align regulatory, supervisory and oversight frameworks
5. Apply AML/CFT consistently and comprehensively
6. Review interaction between data frameworks and cross-border payments
7. Promote safe payment corridors
8. Foster KYC and identity information-sharing

B



C

9. Facilitate increased adoption of PvP
10. Improve (direct) access to payment systems
11. Explore reciprocal liquidity arrangements
12. Extend and align operating hours
13. Pursue interlinking of payment systems

D

14. Adopt a harmonised version of ISO 20022 for message formats
15. Harmonise API protocols for data exchange
16. Establish unique identifiers with proxy registries

E

17. Consider the feasibility of new multilateral platforms and arrangements for cross-border payments
18. Foster the soundness of global stablecoins arrangements
19. Factor an international dimension into CBDC designs

Source: Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20, July 2020[18]

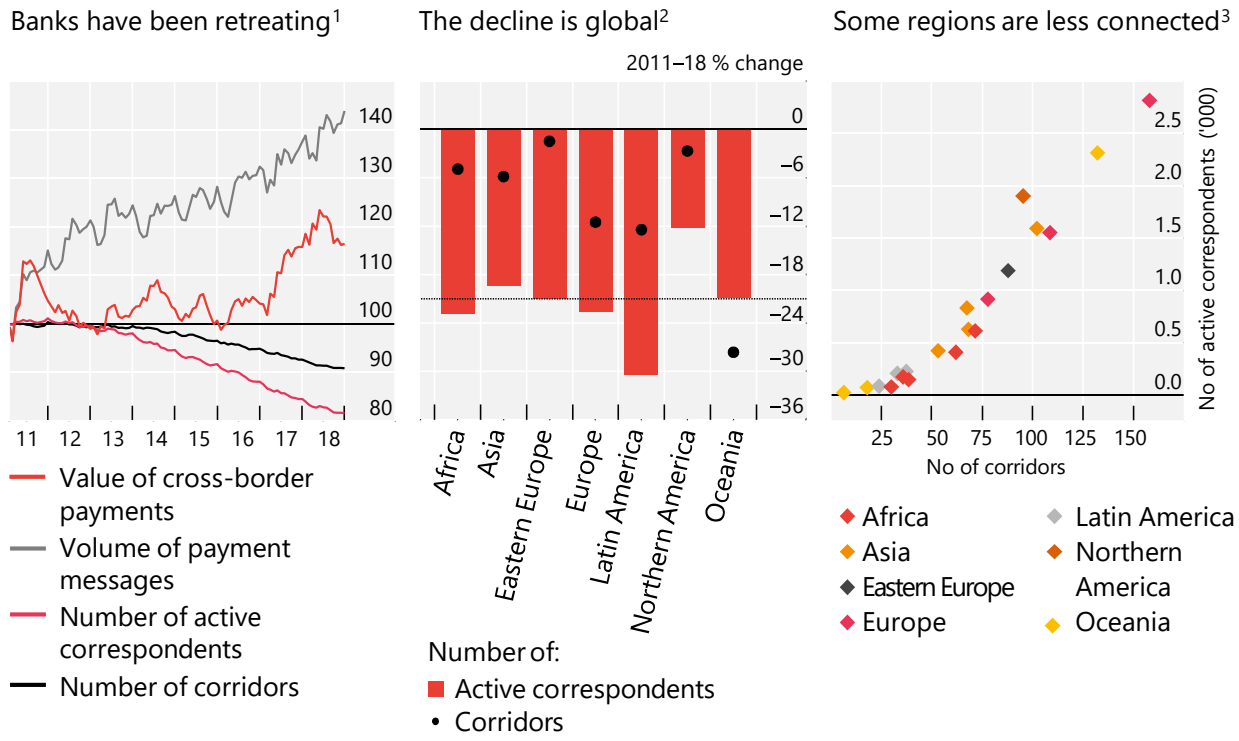
Each of the phases of the project, including the current one, are set as agile experiments in a safe environment with due consideration of technological, policy, legal and business considerations. Each phase has led to incremental learnings that will contribute to the evolution from prototype to pilot, to minimum viable product (MVP) and, ideally, a production-ready network.

If successful, an efficient, low cost, compliant and scalable multi-currency, multi-jurisdiction arrangement can provide a network of direct central bank collaboration, greatly increasing the potential for international trade flows and cross-border business at large.

[18] See CPMI, Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20, July 2020, https://www.bis.org/cpmi/publ/d193.htm .

The benefits of such new payment infrastructure could be even more significant for jurisdictions that currently lack an efficient correspondent banking network. Correspondent banks have been paring back their cross-border banking relationships for the past decade due to derisking.[19] Derisking occurs when global banks stop providing international payment services such as wire transfers, credit card settlements, and even hard foreign currency to a country's local banks. Without it, a bank (and therefore its clients, i.e., people and companies in that country) lose access to the global financial grid, leaving such countries with insufficient access to capital flows[20].

Correspondent banking landscape



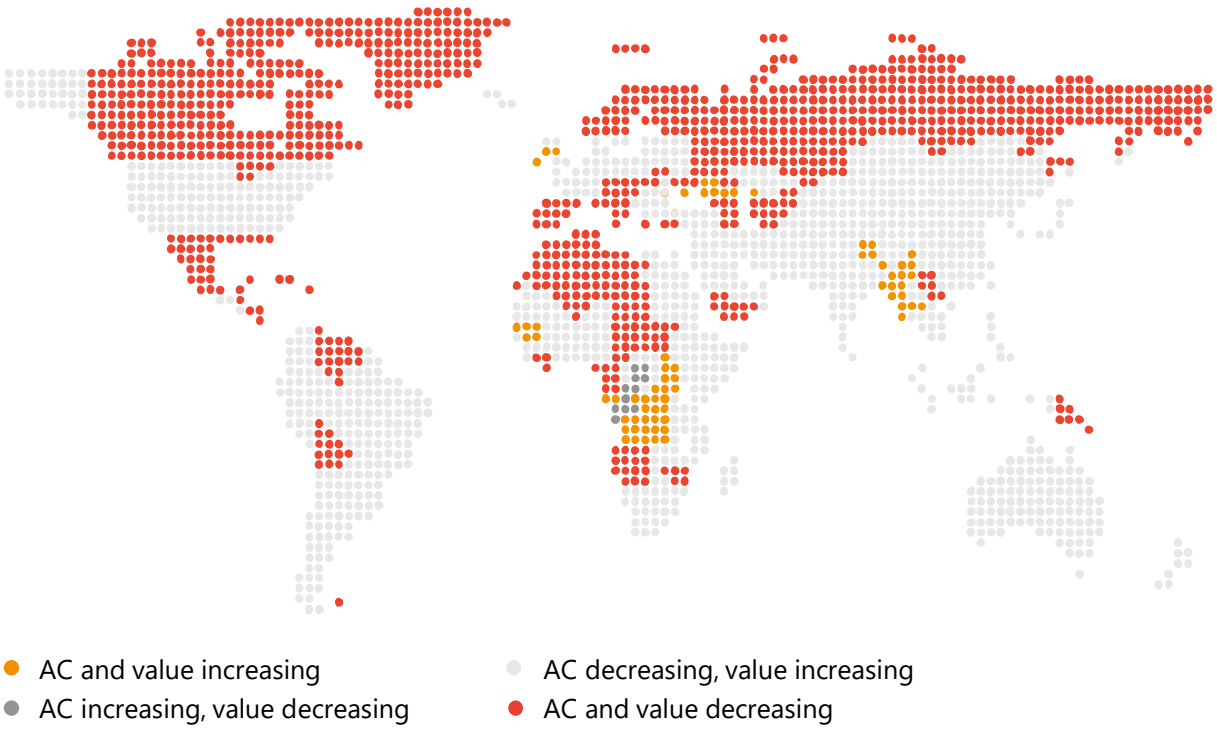
[1] Three-month moving averages.
[2] The black dotted line shows the average percentage change of active correspondents across regions.
[3] 2018 data. Correspondent banks that are active in several corridors are counted several times. Averages across countries in the following subregions: Africa: Eastern, Middle, Northern, Southern and Western; Asia: Central, Eastern, South-Eastern, Southern and Western; Eastern Europe; Europe: Northern, Southern and Western; Latin America: Caribbean, Central and South America; Northern America; Oceania: Australia and New Zealand, Melanesia, Micronesia and Polynesia. Source: SWIFT BI Watch, National Bank of Belgium

Source: On the Global Retreat of Correspondent Banks, BIS Quarterly Review, March 2020[21]

[19] See Tara Rice, Goetz von Peter and Codruta Boar, On the Global Retreat of Correspondent Banks, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003g.pdf .
[20] See Andreas Adriano, When Money can No Longer Travel, July 2017, https://www.elibrary.imf.org/downloadpdf/journals/022/0054/002/article-A012-en.pdf .
[21] See Tara Rice, Goetz von Peter and Codruta Boar, On the Global Retreat of Correspondent Banks, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003g.pdf .

Derisking in turn appears linked to the cost of doing business. In particular, banks are required by law to try to prevent the possibility of seemingly routine cross-border payments disguising money laundering, terrorism financing, tax evasion, and corruption proceeds. In most countries, regulation and enforcement of these requirements has become a lot more rigorous, as has enforcement of economic and trade sanctions. The necessary compliance structure can be so costly that correspondent banking, a large-scale low-margin service, could stop being profitable.[22] The retreat is broad-based but affects some countries more than others.[23] As noted in IMF research, in a limited number of countries, financial fragilities have been accentuated as their cross-border flows are concentrated through fewer correspondent banking relationships or maintained through alternative arrangements. These fragilities could undermine affected countries' long-run growth and financial inclusion prospects by increasing costs of financial services and negatively affecting bank ratings.[24]

Active correspondent (AC) banks vs. value of cross-border payments



The boundaries shown and the designations used in this map do not imply official endorsement or acceptance by the BIS. The graph crosses country-level data on active correspondents (ACs) with the value of payments sent or received over the same period, identified from SWIFT payment messages (see Box A). Individual countries appear in one of four colours, according to whether a positive/negative change in ACs was accompanied by a positive/negative change in the value of payments.

Source: SWIFT BI Watch, National Bank of Belgium; On the Global Retreat of Correspondent Banks, BIS Quarterly Review, March 2020[25]

[22] See Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf .
[23] See Rice, Tara and von Peter, Goetz and Boar, Codruta, On the Global Retreat of Correspondent Banks, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003g.pdf .
[24] See Andreas Adriano, When Money can No Longer Travel, July 2017, https://www.elibrary.imf.org/downloadpdf/journals/022/0054/002/article-A012-en.pdf .
[25] See Rice, Tara and von Peter, Goetz and Boar, Codruta, On the Global Retreat of Correspondent Banks, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003g.pdf .

2.3 Goals and objectives

mBridge Objectives

1

To explore different technologies and develop the prototype that can evolve to a pilot, MVP and production-ready solution.[26]

2

To test different technology configurations and design choices and evaluate and compare their trade-offs.

3

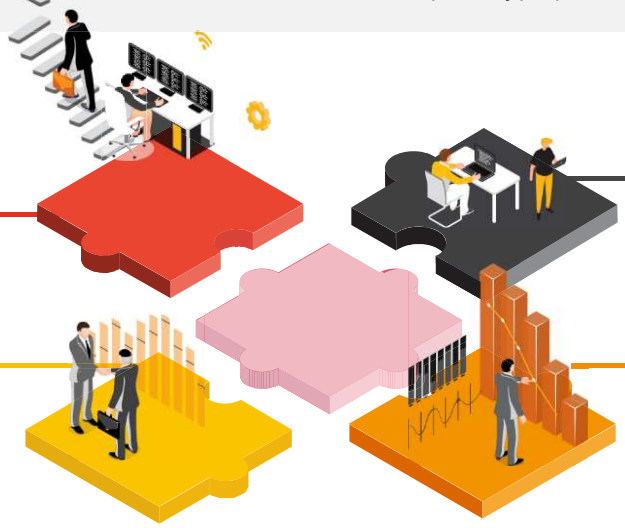
To define relevant business use cases for which the network could be deployed, including the policy considerations, legal implications, and other potential challenges.

4

To extend participation to additional jurisdictions, financial institutions, corporations and other relevant market participants.

5

To determine governance, policy, legal and technical requirements to make the prototype production-ready.



Inthanon-LionRock Objectives

1

A DLT enabled cross-border fund transfer PoC

2

Seamless connection between domestic and overseas payment networks

3

Improve settlement, liquidity and regulatory efficiency

4

Collaboration between Central banks and financial institutions through DLT infrastructure

[26] See the definitions in Annex 1.

2.4 Functional scope

The functional scope of the platform covers the following requirements:

2.4.1 CBDC operations

- Central bank participants can issue and redeem their CBDC.
- Commercial bank participants can submit peer-to-peer CBDC push payments.
- Payment versus payment (PvP)[27] can be achieved.

2.4.2 Foreign exchange (FX) execution models

- The platform can automatically match PvP transactions with the best available FX Board Rate and can achieve execution at the agreed rate.
- The platform also enables direct FX quotations through a Request for Quote function (RFQ) mechanism and can achieve execution of FX transactions at the agreed rate.
- In addition, the platform can ingest FX rates agreed bilaterally outside the platform (off-bridge Arrangement) and can achieve execution of FX transactions at the agreed rate.

2.4.3 Accessibility

- The platform can enable banks and exchanges run their own nodes on the ledger or interact with them through application programming interfaces (APIs).
- The platform can enable corporates and other participants to run their own nodes or interact with them through application programming interfaces (APIs).

2.4.4 Liquidity management

- The platform allows banks to queue transactions if there is not enough liquidity, deferring the execution of the transactions until there is sufficient liquidity.
- The platform initiates netting of queued transactions periodically at the individual central bank level using an automated Liquidity Saving Mechanism (LSM).

2.4.5 Regulatory compliance

- Central banks can monitor transactions executed on the system in their CBDC in real-time.
- Central banks can set currency threshold limits for end of day balances and can automatically reduce the balance of commercial banks at a specified rate if their holdings are above the threshold at the end of day, to comply with jurisdiction-specific regulations.
- Commercial banks can extract transaction information for compliance reporting, surveillance and analysis.

[27] See CPMI Glossary: payment versus payment (PvP) is a settlement mechanism that ensures that the final transfer of a payment in one currency occurs if and only if the final transfer of a payment in another currency or currencies takes place.

2.5 Non-functional scope

The technical design of the system covers the following requirements:

2.5.1 Scalability

- Ensure easy extension to include additional participants and jurisdictions.
- Allow flexibility for integration to different types of local settlement systems, such as Real Time Gross Settlement (RTGS), Faster Payment System (FPS) and other CBDC platforms.

2.5.2 System performance

- Establish a solution that can achieve efficient round trip fund transfer time.
- Enable high network throughput that scales linearly with respect to the number of participants.

2.5.3 System availability

- Operate continuously with Disaster Recovery Procedures (DRP) to support resumption of operations in the event of disruption.
- Establish a mechanism to operate continuously if a node fails during a multi-node operating process.

2.5.4 Transaction privacy

- Provide transaction privacy with respect to the participants to a transaction ensuring that the minimum required amount of information is shared between the counterparties.
- Ensure privacy of transactions from other network participants that are not part of the transaction, ensuring that other members of the network are not able to directly have access to, or infer, any sensitive information about the participants.
- Provide adequate transaction privacy from the network operator along with timely disclosure and compliance capabilities to any regulating entity on the network.

3 Inthanon-LionRock Phase 2

3.1 Operating model

Project Inthanon-LionRock corresponds to a Model 3 single platform multi-currency system (Table 1 and Auer et al (2020)).[28]

Potential improvements of different mCBDC arrangements to frictions in correspondent bank arrangements for cross-border payments

Potential improvements			
Frictions in cross-border payments	**Model 1 mCBDC arrangement based on compatible CBDC systems**	**Model 2 mCBDC arrangement based on interlinked CBDC systems**	**Model 3 Single mCBDC multi-currency system**
Legacy technology platforms	Compatible systems allow for efficiency gains in existing banking relations	A common clearing mechanism could reduce the number of relationships and provide economies of scale	A single system does not require such relations (however, a single system may add to operational costs)
Limited operating hours	CBDCs can be operate 24/7, eliminating any mismatch of operating hours		
Fragmented and truncated data formats	Compatible message standards allow payments to flow without data loss or manual intervention	The message standard (e.g. ISO 20022) adopted by the interlinkage would act to harmonise standards across systems	Single message standard across the system eliminates mismatches
Unclear FX rates and unclear incoming fees	Compatibility requirements for wallet providers could enable users to calculate fees and rates prior to a payment	Common calculation of rates and fees for transfers using any interlinkage would aid transparency	A single system would likely be designed to include options for FX conversion
Long transaction chains	CBDCs could settled instantly, reducing the need for status updates		
Complex processing of compliance checks	Compatible compliance regimes reduce uncertainty and costs	Interlinking systems do not impact multiple or conflicting compliance requirements	Single set of access requirements means compliance could be equivalent across the system

Source: Adapted from R Auer, P Haene and H Holden, "Multi-CBDC arrangements and the future of cross-border payments", BIS Papers, no 115, March 2021.

Source: Central bank digital currencies for cross-border payments, July 2021[29]

[28] See Raphael Auer, Philipp Haene and Henry Holden, Multi-CBDC arrangements and the future of cross-border payments, March 2021, https://www.bis.org/publ/bppdf/bispap115.htm .
[29] See CPMI, BISIH, IMF and the WB, Joint report to the G20, Central bank digital currencies for cross-border payments, July 2021, https://www.bis.org/publ/othp38.pdf .

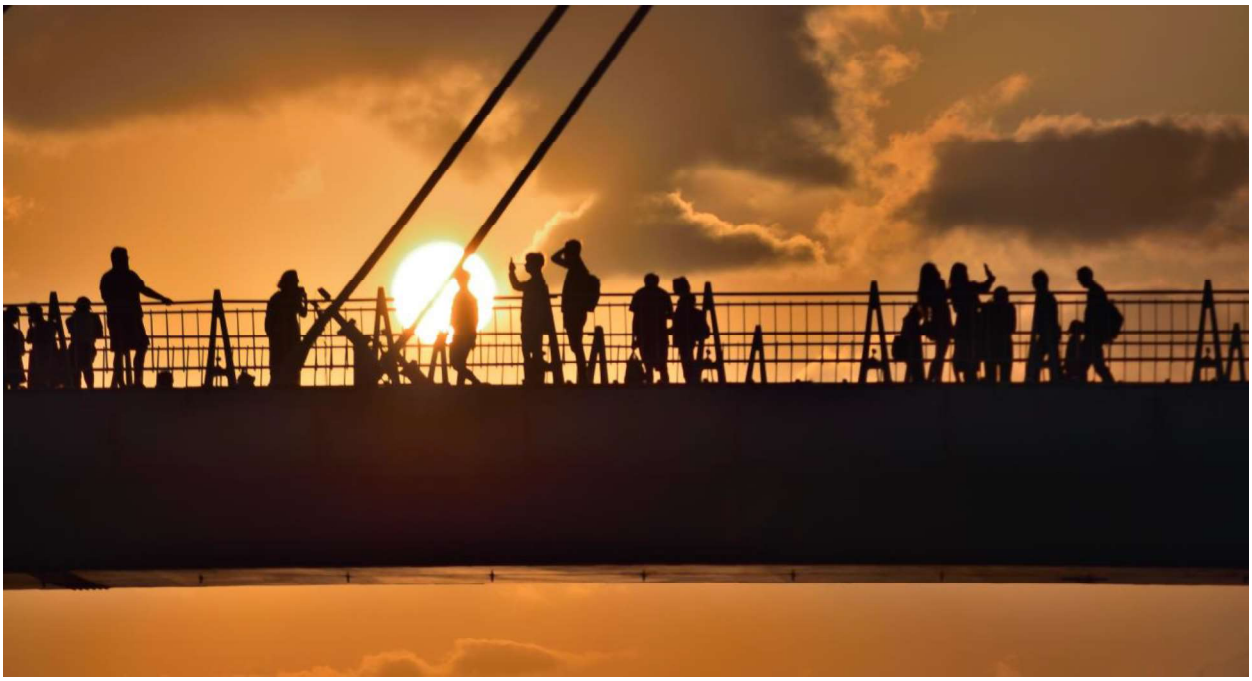
Upon completion of Phase 1, the BOT and HKMA agreed to proceed with further joint research work in Phase 2, including to enhance the prototype to support CBDCs of other jurisdictions, to continue investigating different design trade-offs, and to explore business cases and connections to other platforms, involving participation of non-bank entities in cross-border funds transfer trials. This took the shape of Project Inthanon-LionRock Phase 2 (IL2), the findings from which are summarised in the present report.

The IL2 prototype demonstrates substantial increase in transaction speed from multiple days to near real-time, as well as the potential to reduce by up to half several core components of correspondent banking costs, including nostro-vostro liquidity, treasury operations, compliance and FX. It thereby demonstrates the potential of faster and lower cost cross-border transfers for participating jurisdictions. The benefits would be further increased for jurisdictions that do not benefit from a vibrant correspondent banking network.

3.1.1 Speed

The results of IL2 estimate an approximate 80% reduction in transaction time. There is currently a 3-5 day delay between payment and settlement for a typical cross-border transaction processed via correspondent banking[30]. **The IL2 prototype demonstrates the potential to shorten these transactions from days to seconds.[31]**

Current Transaction Time	3-5 days
Estimated IL2 Transaction Time	2-10 seconds



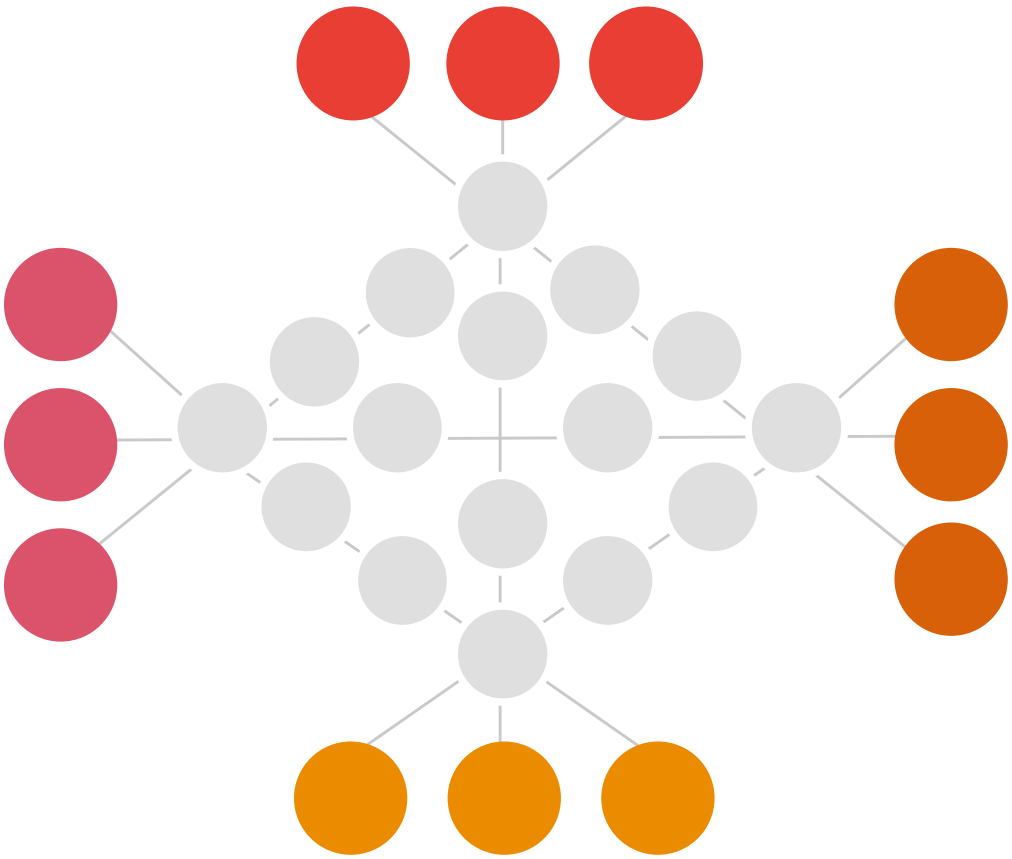
[30] See Bank of Thailand and Hong Kong Monetary Authority, Inthanon-LionRock Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments, January 2020, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf .
[31] Excluding any further operational steps specific to each bank's policies and procedures.

3.1.1.1 Current speed

The structure of correspondent banking is often depicted as a chain from the payer, through the intermediary banks, to the payee. The length of this chain varies depending on the location of the payer and payee and the correspondent banking relationships between them. A longer correspondent chain would increase the number of intermediaries, lengthening the overall transaction time. Since each correspondent can represent many payers and payees, the full network is a group of chains with branches at the ends. The nodes within the chain represent correspondent banks, while the nodes on the branches represent the payers and payees.

A notable effort to improve the speed of cross border payments is SWIFT gpi. SWIFT gpi messages can be sent and received in under five minutes and 92% of the payments are clearing within 24 hours.[32] In spite of this, the participant banks in the IL2 project indicated an average cross-border transaction could experience half to a full day delay at each intermediary correspondent bank. When taking into account manual processing, compliance checking, differences in time zones and operating hours for local settlement networks, the time between payment messages and settlement can often take up to 3-5 days. The correspondent banking model often presents further uncontrollable delays due to cross-border sanctions-related follow-ups, frequent internal investigations, and dispute resolutions.

Illustrative model of a correspondent banking network



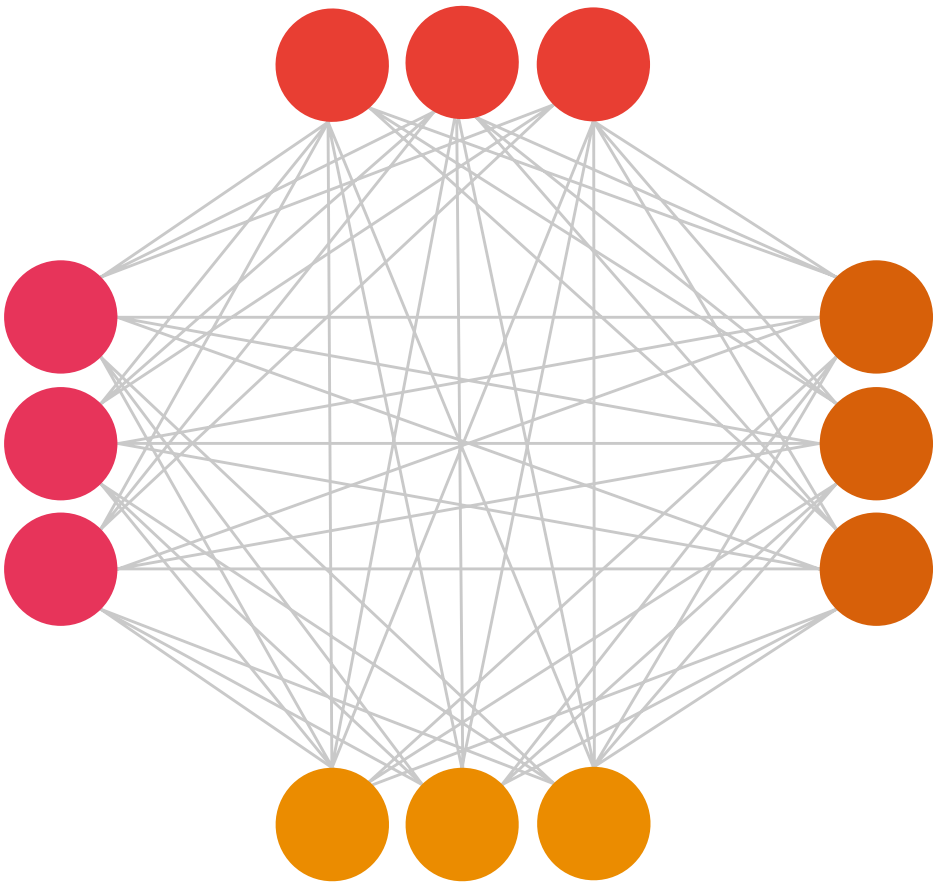
Source: Daniel Eidan, Adviser, BIS Innovation Hub, Hong Kong Centre

[32] See https://www.swift.com/news-events/news/swift-gpi-driving-payments-revolution .

3.1.1.2 Estimated speed

The IL2 prototype's use of DLT replaces the chain of intermediary banks presented in the correspondent banking model by directly linking payers and payees. Using this connectivity model, the solution synchronises transaction data across all counterparties and pushes repetitive back-office operations that are often duplicated by each party along the correspondent banking chain into an automated smart contract layer. These smart contracts can be applied to each process of the transaction lifecycle and automate routine treasury operations, reconciliations and confirmations, compliance validations, and settlement posting. The IL2 prototype reduces transaction times from an average of 3-5 days[33] to near real-time cross-border payment.[34]

Illustrative model of an mCBDC network



Source: Daniel Eidan, Adviser, BIS Innovation Hub, Hong Kong Centre

[33] ½-1 days × 2-3 intermediary banks + 1-2 days from time difference delays.
[34] Near real-time is defined as less than 10 seconds.

3.1.2 Costs

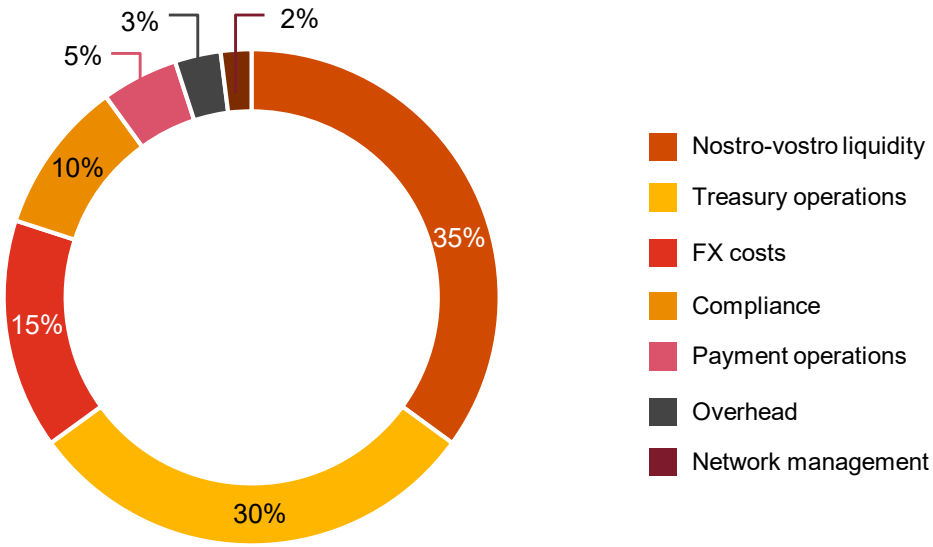
The IL2 prototype shows the potential to reduce the cost of cross-border payments in nostro-vostro liquidity, treasury operations, compliance, and FX by up to half.

3.1.2.1 Current cost

Costs associated with wholesale payments are difficult to measure and individual costs vary per bank and region. The average retail payment cost ranges from below 2% in Europe to over 7% in Latin America,[35] while the average global cost of sending remittances is 6.38% of the amount sent.[36] Bank participants in the IL2 project noted that transaction costs can vary depending on the size and volume of the payments, the customer's relationship with the bank, the size of the bank, and the receiving/sending jurisdictions. Based on this, transaction costs for a multi-million-dollar payment could be as low as 1%. Regardless, 1% of a such a high value payment is still a significant amount.

3.1.2.2 Estimated cost

Using data from McKinsey[37] combined with data obtained from participant banks in the IL2 project, PwC estimates that correspondent banking fees can be broken down as below:



The majority of the existing costs come from nostro-vostro liquidity management and treasury operations.

[35] See FSB, Targets for Addressing the Four Challenges of Cross-Border Payments, Consultative document, 2021, https://www.fsb.org/wp-content/uploads/P310521.pdf .
[36] See World Bank, March 2021, https://remittanceprices.worldbank.org/en .
[37] See McKinsey, A vision for the future of cross-border payments, https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/A%20vision%20for%20the%20future%20of%20cross%20border%20payments%20final/A-vision-for-the-future-of-cross-border-payments-web-final.ashx .

The IL2 prototype shows the potential to reduce the cost of cross-border payments in four of the components above:

1. To reduce **nostro-vostro liquidity costs**, the prototype manages liquidity across all participants algorithmically with a liquidity saving mechanisms. This minimises the need for correspondent banks to manually monitor and predict supply and demand of cross-border payments in order to prefund their foreign accounts. The prototype enables payers and payees to manage their own supply and demand by funding their own individual accounts. This represents a paradigm shift in the way adequate funding for cross-border payment is currently managed.

2. To reduce **treasury operation costs**, the prototype provides direct payment vs. payment (PvP) settlement for banks. In the current traditional model, the same back-office treasury operations must be repeated by banks along the correspondent banking chain. Such inefficiency will be greatly reduced by directly linking banks involved in the fund transfer. In addition, the settlement cycle is executed through smart contracts and as a consequence, the records are promulgated to each of the relevant participants. This eliminates record inconsistencies and reconciliation errors, thus reducing operating cost.

3. To reduce **FX costs** the prototype targets two cost sources, FX risk and exchange fees. It does so in three ways:

    a. Firstly, by representing the liability of the issuer as a bearer tokenised asset it tightly couples the payment obligation and settlement stages of the transaction into a single atomic transaction. This reduces the Herstatt risk[38] of each transaction to zero.

    b. Secondly, the solution's network topology ensures bilateral connectivity between counterparties. This reduces the number of necessary cross-border nostro accounts and the associated exchange fees.

    c. Thirdly, smart contracts on the platform could bring substantial automation and transparency to FX transactions. This can provide more efficient price discovery and less arbitrage in FX markets, while enabling participants to interface directly with more competitive FX markets. These efficiency gains can minimise the potential impact of foreign exchange risk and interest rate differentials, thus reducing the pricing of FX risk.

4. To reduce **compliance costs**, the prototype provides greater transparency and potential benefits of using smart contracts. The storage and updating of payment records is synchronized and made more transparent, helping to facilitate efficient compliance and reporting. It also helps in automating some pre-trade compliance and post-trade monitoring processes for banks and regulators.

Considering the above, PwC estimates that in a production environment the IL2 prototype may reduce the above costs of cross-border payments by up to 50%.

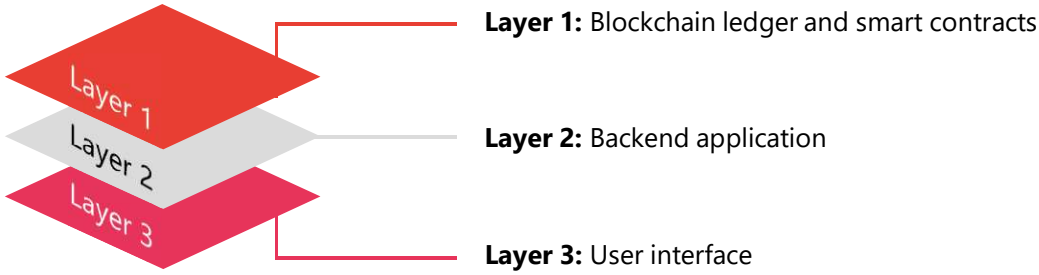
[38] Herstatt risk financial definition, https://financial-dictionary.thefreedictionary.com/Herstatt+risk .

3.2 Technical solution

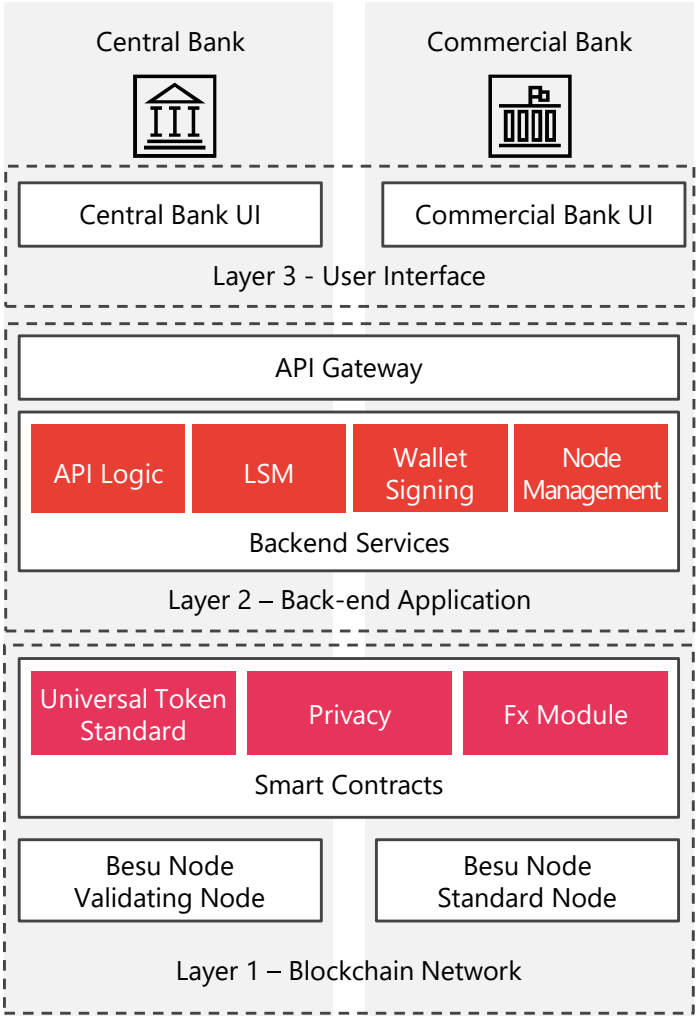
3.2.1 System architecture

The IL2 prototype is composed of three layers:

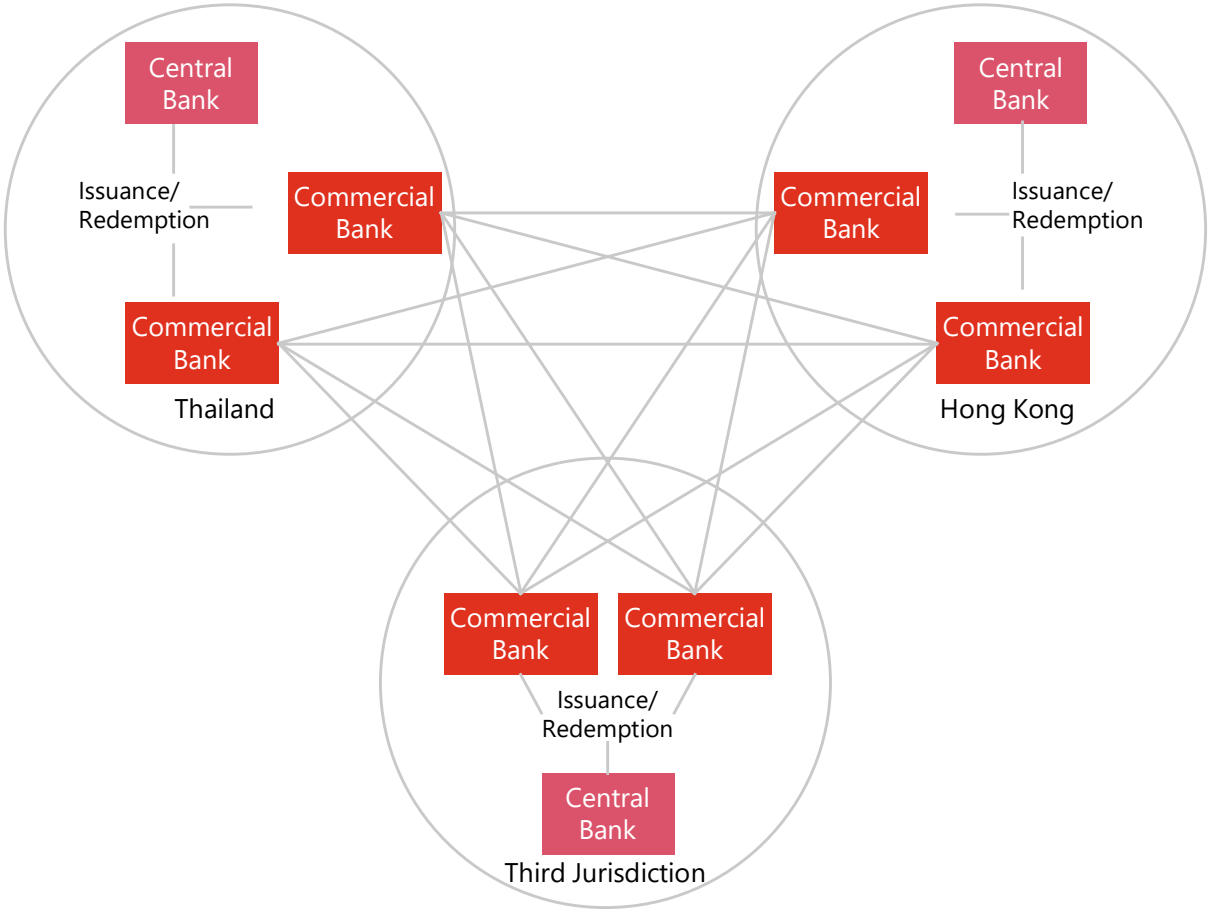
- **Layer 1** is the core layer. This layer contains the blockchain ledger where data persists and the smart contract logic that implements functionality is programmed.
- **Layer 2** is the backend application layer. This layer provides identity, access and routing functions into layer 1 along with wallet signing, key management, and off-ledger FX services.
- **Layer 3** is the front-end layer. This layer provides the interface into the core systems and can take on different forms depending on the end user and the desired functionality.



Illustrative model of IL2 prototype stack layers



Illustrative model of IL2 connectivity diagram



3.2.1.1 Layer 1 – The Blockchain network

The blockchain layer is the core of the IL2 prototype and is comprised of blockchain nodes and smart contracts. This layer provides the following functions:

- Smart contracts for issuance and redemption transactions
- Smart contracts for payment transactions
- Decentralised ledger block validation
- Maintenance of CBDC balances.

The IL2 prototype was built by ConsenSys on Hyperledger Besu, a permissioned Enterprise Ethereum blockchain. Hyperledger Besu was chosen, in line with the objective of technical experimentation, in order to assess how an Ethereum-inspired architecture could support the objectives of a single ledger multi-currency network. Features of Hyperledger Besu that were considered include privacy, flexible choice of the consensus mechanism, and support from the Hyperledger ecosystem and community.

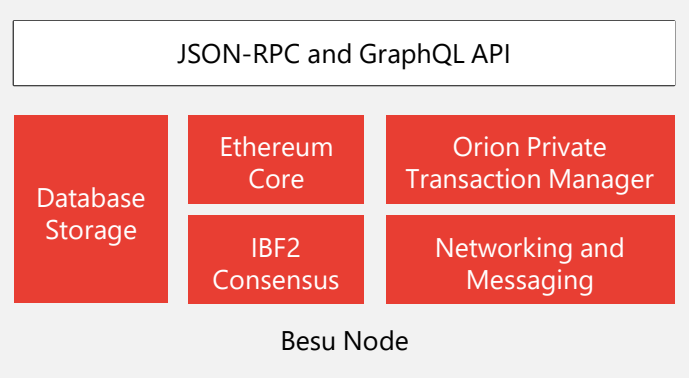
In the prototype, each central bank is assigned a validating node and each commercial bank participant is assigned a standard node. Both these types of nodes are further augmented with the Orion transaction manager. The transaction manager is responsible for enabling communication between other nodes in a private manner, such that all participants in the network are not able to see the data involved.

The settlement finality of CBDC transactions is achieved via a Proof of Authority (PoA) consensus protocol. PoA is a type of consensus protocol that can have different practical implementations. The Istanbul Byzantine Fault Tolerant 2 implementation (IBFT 2.0) was chosen for the IL2 prototype. IBFT 2.0 is an enterprise grade implementation suitable for handling a high volume of transactions and fast settlement finality.[39]

Using this consensus protocol, the validator nodes provide settlement finality to the participants in the network by publishing finalised transactions or blocks onto the blockchain. This ability to run the consensus protocol is what separates standard nodes from the validator nodes. The PoA consensus mechanism ensures that every transaction must be approved by two-thirds of the authorised validator nodes, regardless of their origin node, in order to finalise a transaction.

[39] See IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks, https://arxiv.org/pdf/1909.10194.pdf .

Node Type	Description
Validating Node	Allow the central banks to participate in the Proof of Authority (PoA) consensus mechanism, giving them the full ability to validate transactions within the network along with issuing and redeeming CBDC.
Standard Node	Used by commercial banks and other authorised participants to read and write information to the blockchain.
Orion Transaction Manager	• Encrypts outgoing private transactions and decrypts incoming private transactions from the associated Besu nodes using public/private key pairs. • Manages privacy groups between participants. • Provides peer-to-peer transactions among network participants.



Smart contracts are the way business logic is implemented on the blockchain. In the IL2 prototype all transactions are implemented through smart contracts. The open-source Universal Token standard[40] has been chosen to represent the CBDC asset in the prototype. Built and maintained by ConsenSys, the standard provides the flexibility to accommodate future functionality, such as embedded compliance or tokenised securities, and allows the platform to be interoperable with other networks that utilise common Ethereum token standards. More information on the Universal Token standard can be found in section 3.2.2.4.

3.2.1.2 Layer 2 – Backend application

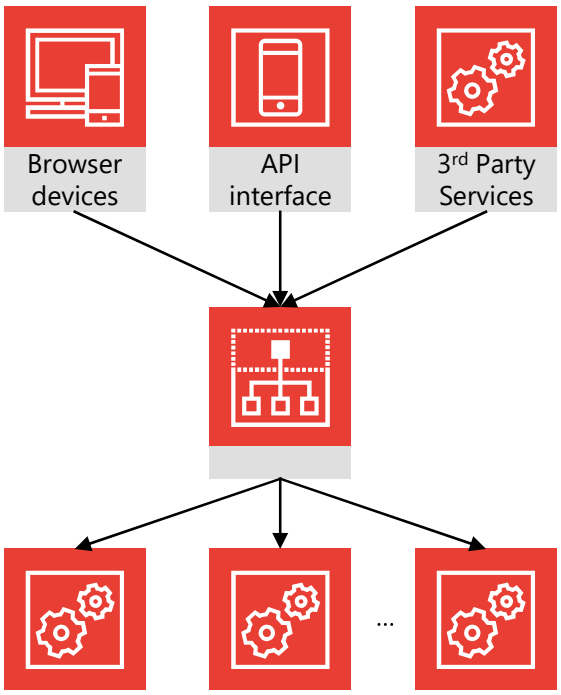
The backend application layer handles the identity and access management, and the API gateway to the blockchain and related services. Built in a microservices fashion, these services include wallet creation and management, transaction signing, FX swaps, queuing, and other services.

- API gateway for identity access management to nodes and identity mapping of user ID to public keys.
- Signing wallet service: Key management, wallet creation, transaction signing.
- Network node services:
  - Transaction preparation: calls issuance/redemption functions
  - Publishing transactions to blockchain
  - Provides ability to query blockchain for transaction status/history.
- FX mechanisms and account management, including liquidity savings mechanism.
- Regulatory features such as real-time monitoring, currency threshold and automatic reduction.

[40] See universal token: https://github.com/ConsenSys/UniversalToken .

3.2.1.3 Layer 3 – Frontend and user interfaces

The IL2 prototype is built to be accessible to users. Forms Syntron HK built an intuitive user interface (UI) that easily interacts with the underlying application. The UI connects securely with API that in turn connects with the underlying blockchain network. This enables user interfaces built for the prototype to be modular and contextual to their application environment, different user interfaces and API integrations can be made depending on the end users' preferences and operating environment.



Blockchain network

3.2.2 Model design

3.2.2.1 Access and Availability

There are three categories of participants that can access the IL2 prototype. This access is split into three categories - permissioned, private, and hierarchical - which enable updating, submitting, and viewing the ledger respectively. The type of access is dependent on the role of the participant within the network. The table below summarises the different roles and permissions assigned to each participant. We note that these permissions are implemented within the blockchain solution itself and not at the API or other access point level.

Design Choice	Feature	User Type	Summary
Updating the ledger	Permissioned	Central banks	Only trusted parties can validate transactions on the ledger. These parties could be nodes managed by the central bank or a trusted blockchain service provider. Having trusted validators reduces the computational resources necessary to securely validate transactions.
Submitting to the ledger	Private	Commercial Banks and Exchanges	A restricted list of parties can submit transactions to the ledger. The list of restricted participants is decided by the central bank and governing bodies.
Viewing the ledger	Hierarchical	Fintechs, Corporates, etc	Access to view the ledger is restricted into hierarchies. The central bank or regulatory bodies can have an extended view of all transactions while banks' and exchanges' views can be limited to their own transactions.

Additionally, the IL2 prototype is designed to support 24/7 payments with no planned downtime. Settlement on the prototype is reliant on a decentralized group of trusted validators as opposed to a centralized clearing house operation. This ensures that if a minimum number of validators are available on the network transactions can be settled at any time. Maintenance can also be done through continuous integration tools without disrupting the prototype's operations.

3.2.2.2 Settlement and settlement finality

A traditional payment transaction involves three distinct phases: payment, clearing, and settlement. Payment is defined as the agreement on the obligation to pay. Clearing entails the transmission, reconciliation and confirmation of transactions prior to settlement. And settlement, the discharge of the obligation. An important part of settlement is the concept of finality. Settlement finality is legally defined as the moment at which the transfer of an asset or financial instrument, or the discharge of an obligation, is irrevocable and unconditional and not susceptible to being unwound following the bankruptcy or insolvency of a participant.[41]

Settlement systems follow three main models.[42] The three models are: real-time gross settlement (RTGS), deferred net settlement (DNS), and hybrid. The IL2 prototype uses the hybrid model, implemented similar to the Euro Access Frankfurt (EAF2) algorithm, developed to support bilateral and multilateral net settlements in centralized queues. The hybrid model was selected as it targets the efficiency of RTGS but requires less liquidity.[43]

The three models are summarised in the table below:

Different models of settlement

Model	Overview	Benefits and Limitations
Real-time gross settlement (RTGS)	Provided the payer's account has sufficient funds, each payment is settled on a gross basis individually or on a net basis as a batch. If the payer has insufficient funds, the payment is either rejected or queued.	Settlements are immediate but requires greater liquidity to operate.
Deferred net settlement (DNS)	Netting and settlement take place after a specified period. Incoming and outgoing payments offset each other. Payments are settled periodically in batches.	Requires less liquidity to operate. Final settlement could experience delays. For instance, in a single batch of payments with other PSPs, the default of one PSP can affect all other payments in the batch. Payments from the defaulted PSP are removed and new net obligations have to be calculated.
Hybrid	Combines RTGS and DNS. For instance, if a payment is queued due to insufficient funds, an ad-hoc liquidity saving mechanism can be triggered that nets/offsets other payments.	Balance between speed and liquidity but more complexity could lead to greater coordination costs and risks.

[41] See Distributed ledger technology in payment, clearing and settlement Distributed ledger technology in payment, clearing and settlement (bis.org).
[42] See Bech and Hancock, Innovations in payments, BIS Quarterly report, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003.pdf .
[43] See Selected Issues in Mature Financial Systems: EMU, Banking System Performance, and Supervision and Regulation - IMF International Capital Markets September 1998--V. Selected Issues in Mature Financial Systems: EMU, Banking System Performance, and Supervision and Regulation.

Settlement finality is achieved via the IBFT2 enterprise grade proof of authority (PoA) consensus mechanism, where there is a group of validators providing approval. The IBFT2 algorithm offers several benefits:

- **Immediate block finality:** Only one block will be proposed at any given chain height. This removes the potential for the creation of forks and the possibility that a transaction will have to be undone.
- **Efficiency:** Compared to Proof of Work, proof of authority (PoA) consensus protocols are more efficient in regard to new block production and transaction throughput.
- **Forgery minimisation:** Validators must take turns to approve transactions and block creation, and over two-thirds of the validators must sign the block in order to publish it to the blockchain.
- **Byzantine fault tolerance (BFT):** Allows the network to continue to function and reach consensus despite any potential node failure. Note that a minimum of four validator nodes are required.

3.2.2.3 FX Conversion

The IL2 prototype implements three different mechanisms for foreign exchange: request for quote (RFQ), off-bridge deals, and board rate. This menu of FX mechanisms provides greater transparency and choice for the platform's participants when conducting FX trades promoting greater competitiveness for FX rates and transaction fees. The mechanisms are summarised in the table below:

Mechanism	Description
Request for Quote (RFQ)	Banks and corporate participants (e.g., commercial banks, corporates and exchanges) can conduct FX transactions by requesting quotes from other participants within the platform. These requests are initiated and responded to through a web user interface and supporting API. All transactions, however, are encrypted and executed through the platform's distributed ledger. Each RFQ is subject to a response expiry period set by the requestor.
off-bridge Arrangement	This mechanism allows banks and corporate participants to enter into FX transactions that are arranged outside of the platform. After the FX transaction details are negotiated and agreed among the participants, transaction details are then inputted into the platform and settled on blockchain inside the platform.
Board Rate	Banks and corporate participants in the platform can view via the web user interface and API board rates posted by other participants, and amount available for various pairs of CBDC currencies within the network. FX trades can then be performed at the board rate via a Smart Contract and recorded on the platform's distributed ledger.

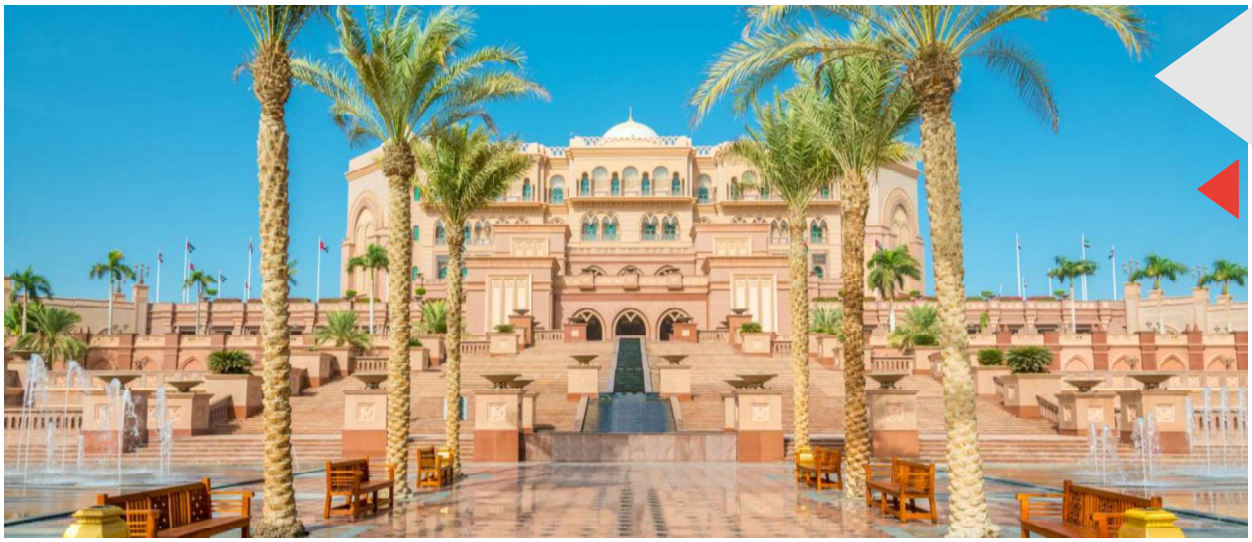
See Annex 2 for more details

3.2.2.4 Payment vs. Payment, tokenisation, and single ledger transactions

Payment vs Payment (PvP) is a settlement mechanism that ensures that the final transfer of a payment in one currency occurs, if and only if, the final transfer of a payment in another currency or currencies takes place.[44] Due to the structure of PvP transactions, they serve as an effective mechanism to eliminate principal risk. Principal risk plays a significant role in cross-border payments where the transaction participants reside in different regulatory jurisdictions. Due to this, enabling PvP payments is a core focus of this prototype.

Blockchain and distributed ledger technologies (DLT) enable cryptographically secure transaction chains. Very simply, this means that transactions on the network have mathematically guaranteed results. Due to this, these types of transaction chains are useful in the implementation of tokenised assets and liabilities. Tokenisation broadly can be defined as a digital representation of value that is not recorded in accounts.[45] With tokenised assets, parties can conduct exchange in a peer-to-peer fashion without the need for intermediate accounts. Through this, the platform is able to provide tokenised PvP transfers between different currencies and across different jurisdictions seamlessly. In the IL2 prototype, the PvP system involves multiple tokenised currencies on a single ledger. Central banks can issue their own tokenised CBDC liability on the prototype with no prerequisites on their domestic payment systems. The CBDC can only be used within the context of the network.

This tokenisation was done using the Universal Token standard developed by ConsenSys. Universal Token is a smart contract standard that extends the ERC-20 and ERC-1400 smart contract standards, some of the most popular token standards on the Ethereum blockchain. ERC-20 defines a set of functions that enable smart contracts to provide token-like functionality.[46] ERC-1400 extends the functionality of the ERC-20 contract and enables functions for regulatory compliance, fractional ownership, fungibility, and issuer forced transfers.[47] The Universal Token standard extends this further to provide finer-grain asset



[44] See CPMI Principles for financial market infrastructures: https://www.bis.org/cpmi/publ/d101a.pdf .
[45] See Bech and Hancock, On the future of securities settlement, BIS Quarterly Review, March 2020, https://www.bis.org/publ/qtrpdf/r_qt2003i.pdf .
[46] See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md .
[47] See https://github.com/ethereum/eips/issues/1411 .

controls needed for institutions, more flexibility to offer versatile use case support, and to accommodate delivery-versus-payment (DvP). The standard also allows for restricted usage based on the holder's identity, legal jurisdiction or asset type. For example, the prototype can be built to limit the number of tokens in a specific wallet, impose thresholds on transaction sizes or whitelist potential holders in secondary markets all via smart contracts in the blockchain layer.

Universal Token standard is an aggregation of other token standards defined as:

- ERC-20: fungible token standard,
- ERC-1410: differentiated ownership / transparent restrictions,[48]
- ERC-1594: on-chain restriction checking with error signalling, off-chain data injection for transfer restrictions and issuance / redemption semantics,[49]
- ERC-1643: document / legend management,[50] and
- ERC-1644: controller operations (force transfer).[51]

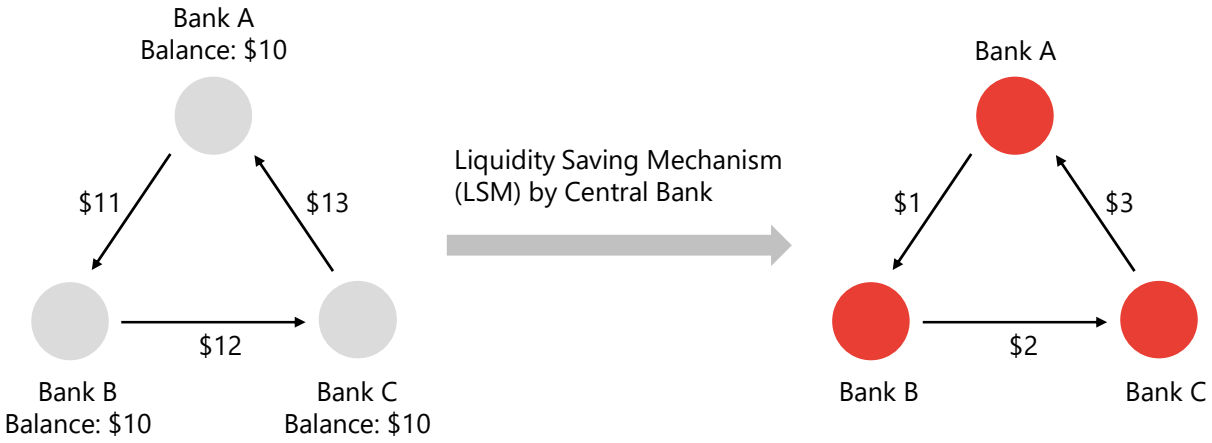
One of the benefits of a single ledger implementation, such that is used in the IL2 prototype, is that transfers between different tokens, issued by different central banks, do not require complex locking mechanisms. To effectively reduce counterparty or settlement risk, minimising the distinct and separate steps within a token transfer transaction is critical. For implementations that have tokens issued on separate ledgers, complex transactions, such as hash timelock contracts, must be constructed. Having such complex cross-ledger arrangement might introduce several possible failure points.[52] In theory, with a single ledger, the transaction model is simplified such that the transfer process can be truly atomic, where both legs of the transaction happen within one action and such that any failures for any part of the transaction will cause the entire transaction to fail.[53] In practice, the result of our prototype showed transactions are made more complex when privacy mechanisms are implemented in specific ways. More details on the privacy mechanism used here, privacy groups, is provided in Section 3.2.2.6. Succinctly, the provisioning of privacy groups to minimise transaction data disclosures inevitably introduces multi-ledger like behaviour and constraints that impede on the atomicity of multi asset transactions.

3.2.2.5 LSM

The adoption of the IL2 prototype depends on its ability to provide an advantage in terms of cost and speed of transactions compared to traditional methods. To support this increase in transaction speed, there must also be adequate liquidity within the network, otherwise gridlock would slow down the practical transaction time. A gridlock is a scenario where transactions are mutually awaiting each other in order to settle, see diagram on the next page.

[48] See https://github.com/ethereum/EIPs/issues/1410 .
[49] See https://github.com/ethereum/EIPs/issues/1594 .
[50] See https://github.com/ethereum/EIPs/issues/1643 .
[51] See https://github.com/ethereum/EIPs/issues/1644 .
[52] See https://www.bis.org/publ/qtrpdf/r_qt2003i.pdf .
[53] See definition of Atomic from McGraw-Hill Dictionary of Scientific & Technical Terms, https://encyclopedia2.thefreedictionary.com/Atomic+(computer+science) .

Simple Gridlock Example



The Liquidity Saving Mechanism (LSM) is used to resolve these gridlock situations. Each central bank is responsible for facilitating the LSM within their own currency (i.e., HKMA for HKD, BOT For THB, etc.). Transactions that lack liquidity and are gridlocked will be placed in the payer's queue awaiting the LSM settlement. The central bank will periodically and automatically initiate the LSM process.

The process contains four stages:

- **Detect:** The central bank asks banks to send in their pending transactions and balances for LSM planning calculations.
- **Plan:** After receiving the pending transactions and balances from the banks, the central node will calculate which transactions can be netted.
- **Propose:** With the results from the planning stage, the central bank will
  - Send instructions of netted positions to resolve the cyclical gridlock, or
  - Will inject liquidity in the situation of a transaction deadlock.
- **Execute:** Banks then execute the transfers.

Unprocessed transactions will be placed back into the queue for the next iteration of the LSM process.

Note that the LSM process can be triggered automatically at set intervals or manually on an ad-hoc basis. Algorithms and techniques for resolving gridlock can be incredibly complex and factor in a variety of other considerations and data points. This prototype, as in the previous phase, utilised a straightforward LSM model to prove and validate how an LSM can be implemented based on the Hyperledger Besu architecture. Due to the constraints of the privacy group implementation, the current LSM was unable to calculate an optimal netting solution when higher degrees of transaction privacy where guaranteed.

3.2.2.6 Transaction Privacy

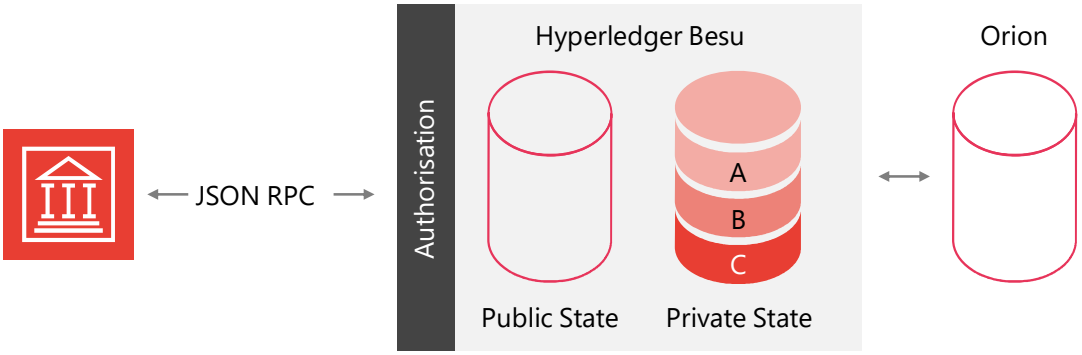
Transaction privacy can be thought of as having two main components: privacy of what and privacy from whom? From this perspective, the IL2 prototype focuses on two types of privacy offerings. The first is transaction privacy with respect to other network participants, meaning that when two participants on the prototype engage in a transaction, this transaction is kept private from non-participating members. The applies to issuance, redemption and PvP transactions. The second is transaction privacy with respect to the transaction validators. This means that when a transaction is submitted to the ledger for validation, the validating members of the network cannot learn any identifying information about the data within the transaction or the members of the transaction as a result of validating it.

[54] See Orion features have been merged with Tessera: https://docs.orion.consensys.net/en/latest/Tutorials/Migrating-from-Orion-to-Tessera/ .

To support this functionality, the prototype takes advantage of Hyperledger Besu's privacy groups. These groups are made of subsets of the participants on the network. The nodes maintain the public state for blockchain and a corresponding private state for each privacy group. To support this functionality each Besu node is paired with an Orion transaction manager.[54] The Orion transaction manager encrypts and distributes the private transaction to other private participant nodes. Privacy groups are created on demand with no limits to the number of groups in a network. Transactions within these groups do not involve any other participants on the network, except for the creation of a transaction hash to the main public chain. This hash is used by the transaction managers to provide data verification of the transaction. Smart contracts are used to manage and maintain group members and the owner of each group has the signing key to create and delete the group.

There are three types of privacy groups:

- **Public:** main group for all members,
- **Private:** between central bank and each commercial bank, and
- **Bilateral:** peer-to-peer between commercial banks with the central bank as needed.



To provide transaction privacy with respect to the verifying nodes, every token transfer on the blockchain contains a unique digital signature. These digital signatures are encrypted in a way that enables anonymous transaction verification and ensures that the verifying members of the network aren't exposed to any data contained within the transactions. Additionally, access to view transactions is hierarchically restricted. For example, a central bank or regulator can be provided access to all transactions within its jurisdiction, while a bank or exchange can be provided access to only the transactions they are a counterparty of.[55]

[55] See Annex 1 for Public-private Key Cryptography information.

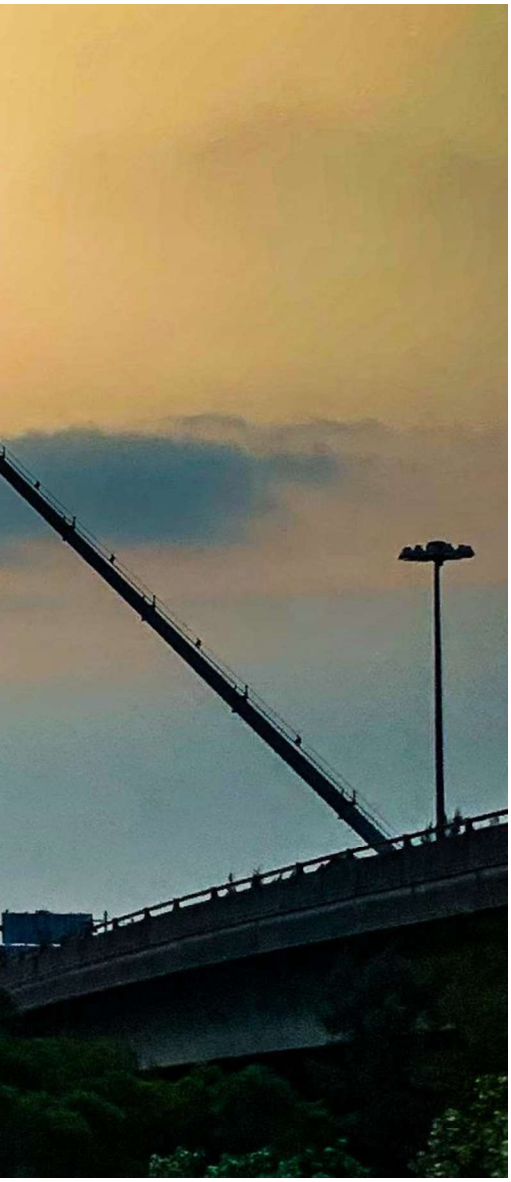
3.2.2.7 Currency controls and compliance

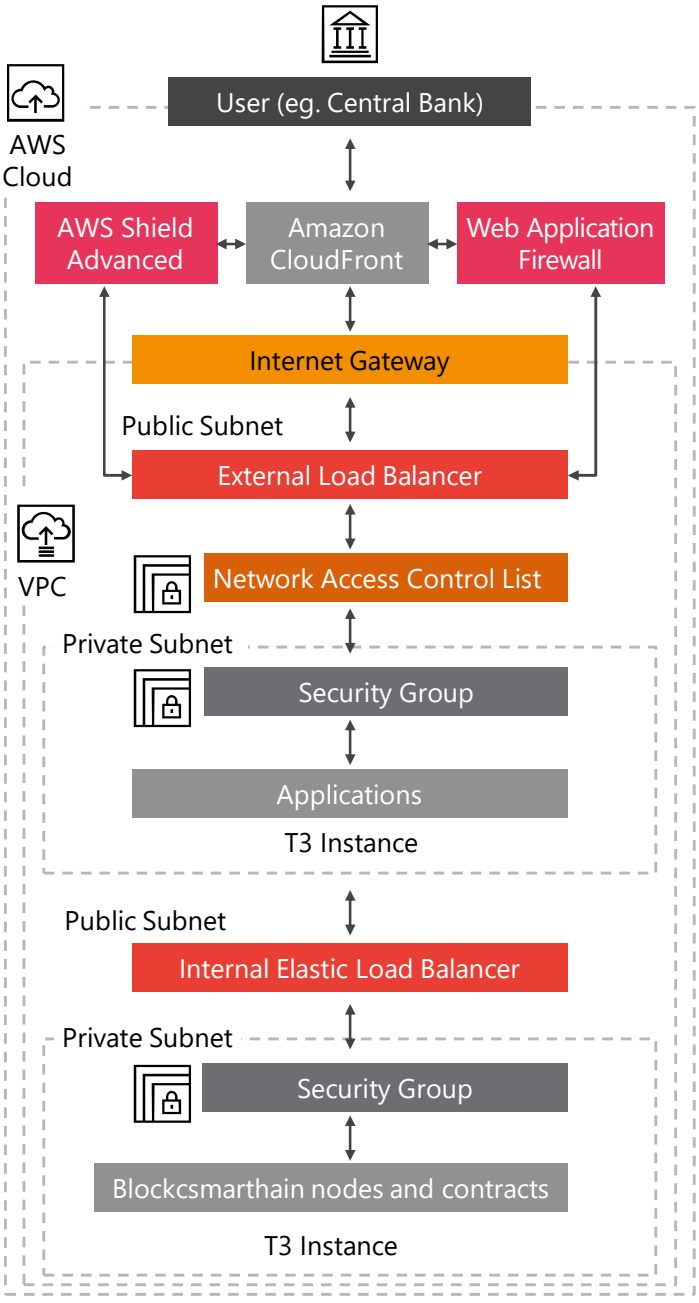
Central bank nodes are the only participants with the permission to execute transactions for issuance and redemption of currencies. This ensures that the IL2 prototype conforms to all currency controls implemented by the Central Bank. Along with this, the central banks are able to view transactions that use their issued currencies. Even in a cross-border FX transaction, the issuer of each currency maintains their ability to monitor their respective currency. This gives the central bank real time visibility into important metrics like overall money supply and the velocity of currency. For example, if a Thai bank holding Thai Baht conducts an FX trade with a Hong Kong bank for HKD. The BOT will be able to monitor the offshore Baht held by the Hong Kong Bank. Similarly, the HKMA will be able to monitor the offshore HKD held by the Thai bank. This ensures the ability to enforce and have real time monitoring of capital controls. It is important to note that these parameters can be set differently for different central banks respecting the unique circumstances within each region. For instance, Thailand's FX regulations do not allow for foreign banks to hold over 200 million outstanding Thai Baht at the end of each day. The IL2 prototype therefore allows for an auto-reduction mechanism to be performed if this threshold is breached.

3.3 Operational considerations

3.3.1 Deployment

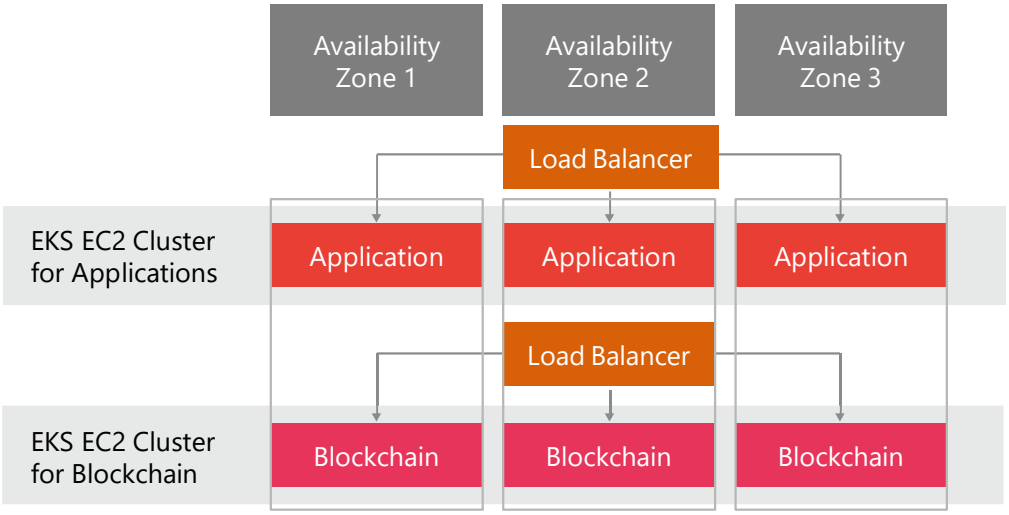
The IL2 prototype was deployed on a virtual private cloud architecture with multi-layer security. The blockchain network and applications are hosted within an AWS T3 instance protected by security group policies, which utilise private subnets further protected by access control lists. As the internet gateway will be the point of entry for bank participants on the cloud, all access will need to pass through CloudFront, which will be configured with AWS Shield Advanced for DDoS mitigation, with web application firewall protection. All application servers, including the blockchain nodes, were deployed in containers via Docker and managed by Kubernetes. Kubernetes played a key role in providing an ease of deployment for the multi-node and multi-server network, allowing for efficient management and usage of test networks. In addition, the automated deployment features of Kubernetes were utilised as part of the disaster recovery features.





3.3.2 Performance and resiliency

To avoid single point of failure, each jurisdiction is running at least four validators in total, where each validator is running a pair of nodes. A minimum of four validators is required by the IBFT 2.0 consensus mechanism and the paired nodes ensure that the two-thirds validation required by the IBFT 2.0 will be present if one of the validating nodes becomes unresponsive. Notably this setup becomes more resilient as more validating nodes are added to the network. However, trade-offs in performance need to be considered when increasing resiliency.



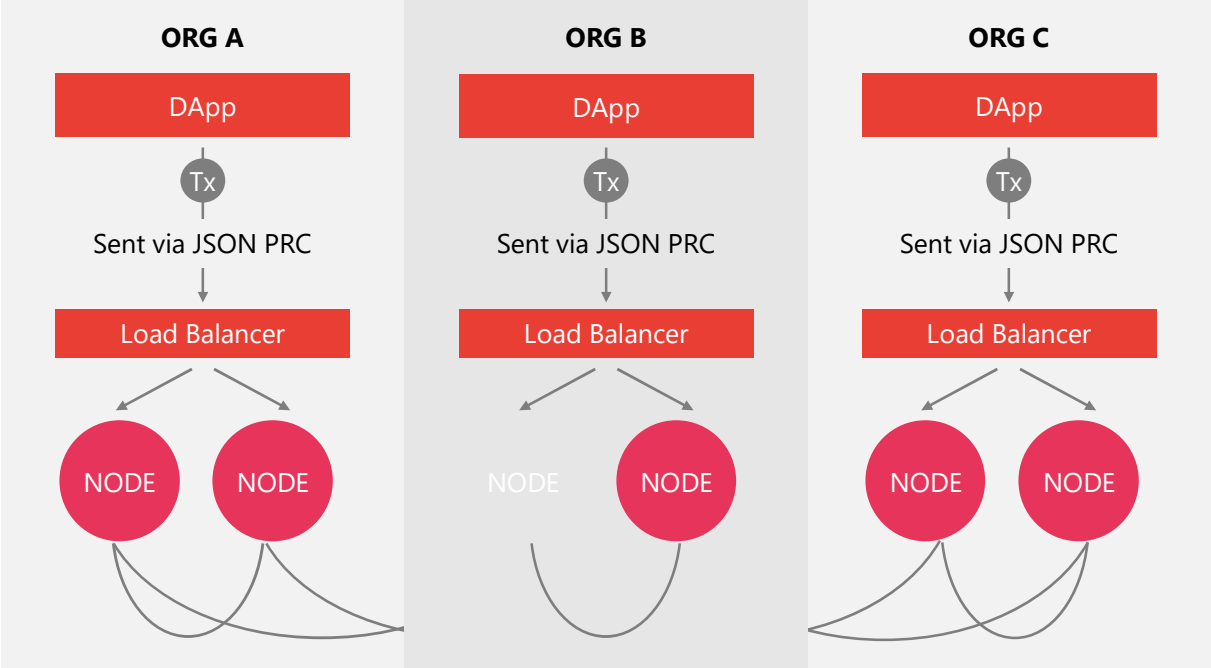
Along with resiliency tests, in-depth performance testing was conducted to evaluate the Hyperledger Besu platform.

The following tests were conducted:

- **Load Testing**: It is a general testing performed to determine how a system performs by transaction type as agreed among users, vendors and IT. It is concerned with achieving response times, throughput, and resource-utilisation levels that meet the performance objectives for the project or product.
- **Soak Testing**: It is testing the projected maximum load over an extended period of time. Soak testing focuses on system stability while the system is loaded with the projected maximum load over a long period of time.
- **Disaster Recovery Testing**: It is a general testing performed to support the disaster recovery and be able to restore/recover smoothly. The test was meant to ensure the product's ability to perform in chaotic conditions without a loss of core functions or data. It ensures a quick recovery after unforeseen, uncontrollable events.

Some of the initial results from these performance tests are detailed below:

- **Operational Efficiency and Scalability**: The system shows a competent liquidity management ability such that the transactions can be completed in a quicker and cost-effective manner than in conventional methods. It also demonstrates the scalability for supporting the expansion growth of transaction volumes and the number of jurisdictions and commercial banks within the jurisdiction.
- **Service Availability**: The system is tested for operational resilience with business continuity and redundancy coverage. To cope with various disaster scenarios, the platform service is fully resilient such that the transaction operations will be picked up by other nodes in the chain immediately with no data loss, whilst the service of the victim node can be resumed very quickly by leveraging the high-availability and resilience capability in the cloud architecture design (e.g., AWS EKS and persistent volume storage).



- **Network Latency**: To demonstrate the network latency by measuring the TPS, the applications and blockchain nodes have been hosted in a cloud provider data center based in Hong Kong and multiple load tests have been carried out in three different locations: Hong Kong, India and the UK. The result of the test illustrated that transactions are latency non-sensitive among different geographical locations.

Initial performance and resiliency testing were done to prove the initial features and base functionality are compatible with baseline expectations. The results of these tests provided good insight into where bottlenecks, limitations, and constraints may be on the path to production grade performance. To further refine these metrics and determine reliable quantifiable results will be part of the future phases of work.

3.3.3 Data privacy and protection

As the project progresses, data protection issues and their risks will be addressed for data in storage, transit and in use. For example, Hong Kong and Thailand have outlined how data is to be protected and handled in their respective Personal Data (Privacy) Ordinance and Personal Data Protection Act, with principles addressing the purpose of collection, usage, security, and disclosure. As more jurisdictions join, cross-border data flow and liabilities between all the participating jurisdictions will need to be examined, such as prohibition of data transfer to countries without adequate data protection standards or owner consent.

A data protection policy will be created outlining how data is to be classified, encrypted, protected physically, and destroyed, as well as how to handle data breach reporting, etc. Due diligence will be conducted with involved contractors and third-party vendors evaluating their own information security practices and service level agreements on the protection of data. Insurance that covers the platform and its participants regarding a data breach should be in place, where possible.

3.3.4 Disaster recovery

In future project stages, incident response, management procedures and escalation policies will be formalised. Drills that test disaster recovery and business continuity plans end-to-end should be conducted annually. Consideration should be given to various scenarios such as failure of IT equipment, natural disasters and human-related threats with procedures for failovers and backup systems. Contingency procedures should be in place for incidents where node shutdown is required. A recovery time objective has been proposed of a minute or less for a recovery test where a node or API fails.

3.3.5 Cybersecurity

As the prototype evolves to a production-ready system, a comprehensive approach to cybersecurity risk management is imperative to protect assets and maintain trust among the participants and user base. To do so the prototype will need to meet internationally recognised standards in security, such as the ISO 27000 series or the NIST Cybersecurity Framework. Participants will also be subject to their jurisdictional requirements, such as the HKMA's Cybersecurity Fortification Initiative and the BOT's Cyber Resilience Assessment Framework.


ANDAZ

4 mBridge

4.1 Phase 3

With the joining of the BISIH, the PBC DCI and the CBUAE,[56] the project has been renamed mBridge and entered its Phase 3. As noted in Section 1 to this report, the overall goal of the project throughout these three phases remains unchanged:

> To design new efficient cross-border payment infrastructure that improves on key pain points, including high cost, low speed, and operational complexities, while ensuring policy, regulatory compliance and privacy are appropriately integrated.

The objective of the Phase 3 is to continue iterating and improving the prototype, including exploring connectivity to standing core banking systems and future multi-party networks, testing out business use cases in international trade and beyond as proposed by participating banks, and deepening our study of policy, regulation, and legal requirements as applied to the system's architecture, design, and functionalities. While more detailed reports will follow as the project crosses new milestones, we explain in this section the current project governance, as well as the future roadmap.

Each of the phases of the project, including the current one, are set as agile experiments in a safe environment, with due consideration of technological, policy, legal, and business considerations. Each of the steps to date has led to incremental learnings that will contribute to the evolution from current prototype to pilot, becoming a minimum viable product (MVP) and, eventually, a production-ready network. Throughout this joint central banking collaborative journey under the auspices of the BIS, we adopt the following core principles:

- **First, do no harm:**[57] CBDC supplied by one central bank should continue to support the healthy evolution of the international monetary system. CBDC supplied by one central bank should not disrupt other central banks' currency sovereignty and their ability to fulfil monetary and financial stability mandates, and meanwhile should protect the legitimate rights of consumers such as data privacy and security and boost fair competition.
- **Second, compliance:** Cross-border payment arrangements with CBDC should have a sound legal system and a stable operation system, comply with the regulations and laws of the jurisdictions concerned, such as capital management and foreign exchange mechanisms. Information flow and fund flow could be synchronised, so as to facilitate the advancement of cross-border trade, bolster the development of real economy and meet the regulatory requirements for anti-money laundering and countering terrorist financing.

[56] See BIS press release: https://www.bis.org/press/p210223.htm .
[57] See also Agustin Carstens, Central bank digital currencies: putting a big idea into practice, March 2021, https://www.bis.org/speeches/sp210331.pdf .

- **Third, interoperability:** The development of CBDC should fully tap into the role of the existing infrastructures and leverage fintech so as to enable interoperability between CBDC systems of different jurisdictions as well as between CBDC systems and traditional payment systems. In the meanwhile, its development should contribute to the orderly development of the payment system and guard against market fragmentation.

These principles are to ensure that mBridge is compliant with the monetary sovereignty of the participating jurisdictions, accommodates the legal and regulatory requirements of each participating jurisdiction, supports interoperability with standing and future systems, enables each participating jurisdiction to create its own building blocks (referred to as the LEGO bricks approach), and empowers every jurisdiction to trial, pilot, and eventually enter production at its own pace.

4.2 Governance

The mBridge project governance is defined in a Charter that was agreed to at the onset of the project by the participating central banks and that will undoubtedly evolve as the project progresses. The Charter sets out the existence, scope, and governance of the Steering Committee and the four subcommittees.

4.2.1 Steering committee

The Steering Committee is chaired by the BIS Innovation Hub, Hong Kong Centre. It is comprised of senior representatives of the involved authorities. Its core objective is to achieve alignment on project direction, vision, and roadmap, including to achieve consensus on solution design and solution requirements, and to oversee and guide the work of the subcommittees.

The Steering Committee is supported by four subcommittees that formulate working level viewpoints, inputs and deliverables to execute on the project direction, vision and roadmap, including through conducting technological experimentation and trials.

4.2.2 Technology sub-committee

The Technology subcommittee is chaired by the PBC DCI. It is primarily comprised of members from participating central banks with technology or engineering backgrounds. Its objective is to offer a solution architecture that is scalable, accessible, extensible and compliant in order to serve the broader central banking community as a public good via open-sourcing.

4.2.3 Legal sub-committee

The Legal subcommittee is chaired by the HKMA. It is primarily comprised of members from the involved authorities with a legal and governance background. It coordinates legal documentation needed in respect to the project and formulates the processes for governance, risk, compliance, and dispute resolution. In addition, it examines legal and regulatory requirements relating to the business use cases proposed for trial.

4.2.4 Policy sub-committee

The Policy subcommittee is chaired by the BOT. It is primarily comprised of members from the involved authorities with a policy or economics background. It analyses central bank policy implications in the context of mBridge, including financial ecosystem considerations such as those linked to international trade, correspondent FX regulation, financial stability, and monetary policy transmission.

4.2.5 Business sub-committee

The Business subcommittee is chaired by the CBUAE. It is primarily comprised of members from the involved authorities and, to the extent they see fit, invitees of the private sector to be proposed by the involved authorities and to be approved by the Steering Committee. It focuses on detailed formulation of the business use cases and serves to obtain input from and secure collaboration with the private sector, each of which the Steering Committee deems necessary to achieve a production-ready system.

4.3 Roadmap

In keeping with the above, governance, legal, policy, and business concerns are catalogued, analysed, and prioritised with a focus on moving towards a production-ready system. While doing so, we expect to push the capabilities of DLT and CBDC in areas where results are not yet sufficiently advanced to support real world critical infrastructure requirements as well as policy and legal requirements.

Our future technology roadmap includes:

- Data privacy approaches for single ledger and multi-ledger solutions,
- FX liquidity management across multiple currencies,
- Performance and scalability to support fully operational payment volumes,
- Interoperability by vertically linking into core banking systems and payment providers,
- Interoperability by horizontally linking with other cross-border and domestic systems,
- Atomic transactions across multiple self-sovereign systems,
- Distributed gridlock resolution solutions, and
- Technical platform governance.

Our future policy, legal, and business roadmap includes:

- System requirements necessary to safeguard monetary and financial stability,
- Features to achieve compliance with jurisdiction-specific regulations and reporting requirements,
- Legal governance of the platform and designing contractual arrangements,
- Participation models and onboarding criteria for new central banks and participants,
- Inclusion of non-bank players, associated roles and scope of permissible activities, and
- Trials of business use cases with participating banks.

As these milestones are achieved further progress reports will be issued.

5 Conclusion and next steps

Accomplishments

Building on the experience of Inthanon-LionRock Phase 1, other work done by various central banks, and BIS research, we are proud to take another step towards the G20 mandate of creating cheaper, faster, and more resilient cross-border payments.

With the addition of the BISIH, CBUAE, and PBC DCI to the original Inthanon-LionRock participants, the HKMA and BOT, we have extended the geography of our work to include more regional borders, additional currencies, and more diversity in the cross-border business use cases. Furthermore, by building the Inthanon-LionRock Phase 2 (IL2) prototype on Ethereum's Hyperledger Besu blockchain, we continue to expand our hands-on experience with different software components and push the capabilities of DLT as a technical enabler for cross-border payments.

As illustrated in this report, with the IL2 prototype we have shown that DLT can significantly increase the speed, lower the cost and provide operational efficiencies and resiliency to complex cross-border payment flows. Our work further shows that innovative modular solutions can allocate liquidity, resolve gridlock, provide competitive FX, enforce compliance and regulatory oversight, and support the necessary future services.

However, it is worth noting the DLT implementation for IL2 still has several limitations. In particular, the reliance on Privacy Groups to preserve privacy across multiple jurisdictions does not allow for fully atomic PvP transactions. In addition, since there is no single entity or jurisdiction that can view the balance of all pending FX transactions; an optimal liquidity savings mechanism has yet to be found. Lastly, the scalability and performance of DLT in handling large transaction volumes will need to be assessed further if more jurisdictions or currencies are added onto the platform. Detailed risk governance procedures will also need to be created.

Nonetheless, our perspective on DLT-enabled infrastructure has matured and as a result, we have been able to deeply evaluate the subtle trade-offs inherent to multi-faceted solution features such as privacy, transparency, atomicity, access, and consensus protocols.

Next steps

With this progress in mind, there is still more work to be done developing the prototype into a production-ready solution. Within the mBridge governance structure, the subcommittees have already begun this work and will continue to build and evolve their efforts guided by the Steering Committee, chaired by the BIS. Legal, policy, governance, and business concerns are being catalogued, analysed, and prioritised for future research and development with a focus on driving to live and production usage.

Moreover, we continue to push the capabilities of DLT and CBDC in areas where results are not yet sufficiently advanced to support real world critical infrastructure requirements. In keeping with an agile approach, part of our journey will involve trials with market participants to further iterate and improve on the prototype and its functionalities.

Through international central bank collaboration and in keeping with building blocks 9, 17, and 19 of the Stage 2 reports to the G20, we will continue our progress towards designing multilateral solutions for cross-border payments that improve on key pain points, including high cost, low speed, and operational complexities.

We look forward to continuing to contribute to the international dimension of this work, including by welcoming more central banks to our agile and experimentation driven journey founded on the principles of *do no harm, compliance and interoperability*. As milestones are achieved, further progress reports will be issued.


望京SOHO

Annex

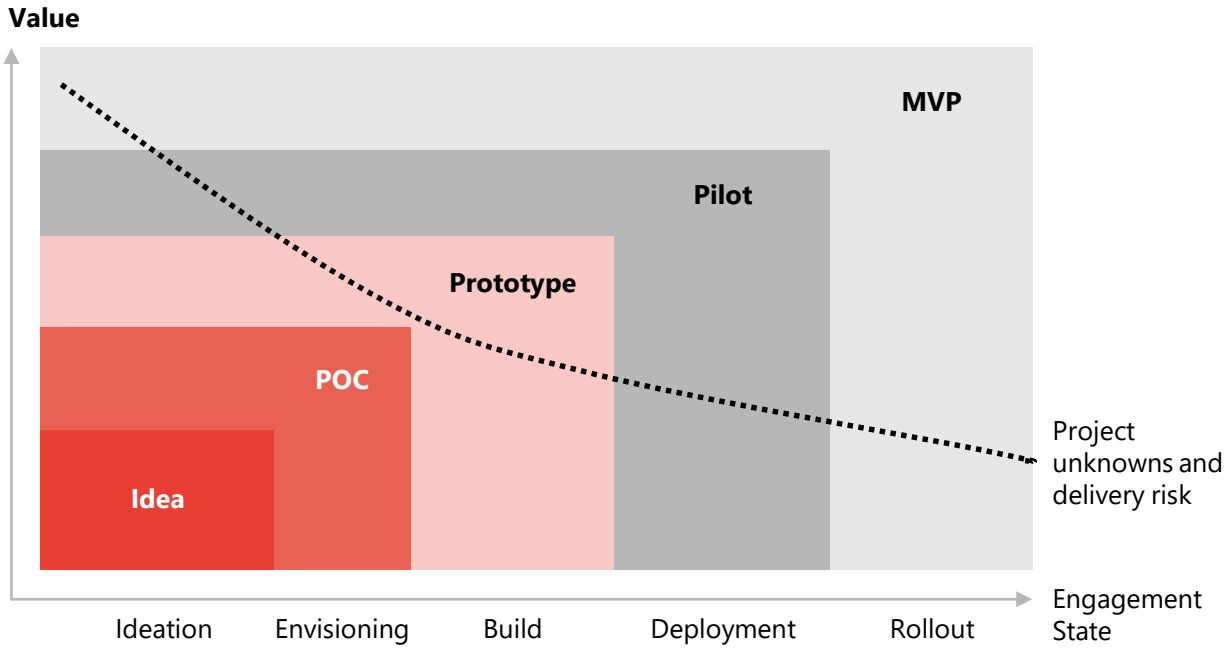
Annex 1 Terminology

Project stages

Proof-of-concept (PoC): A PoC is a method to test and validate a technology or approach within a limited time window. It typically has less functionality than a prototype. The experience and knowledge gained from a PoC informs on the feasibility of the product. A PoC is comparable to research when it is not clear whether an idea can be brought to life and whether to proceed with the development of the product.

Prototype: While a PoC focuses on one or just a few aspects of a product, a prototype is a working model of several aspects of the product. A prototype is comparable to a draft of a full product and is built to test the product's design, usability, and often functionality. While a PoC is typically used only internally, a prototype can also used to attract users. Furthermore, it forms a basis for a minimum viable product. While the main goal of a prototype is testing, building a prototype helps to get a preview at how real people interact with a product. The development team can gather users' feedback and make changes to the prototype or create a new one. Prototyping is also useful for idea generation.

Different technology-related outputs



Source: BISIH adaptation of Giblin et al (2021): Envisioning To Delivery – POC, Prototypes, Pilots and MVP

Pilot: Pilots are often used as the first stage of a new policy or service rollout. Rather than a test or experiment, pilots are a 'live' activity, usually with a small group of real users receiving the new service.

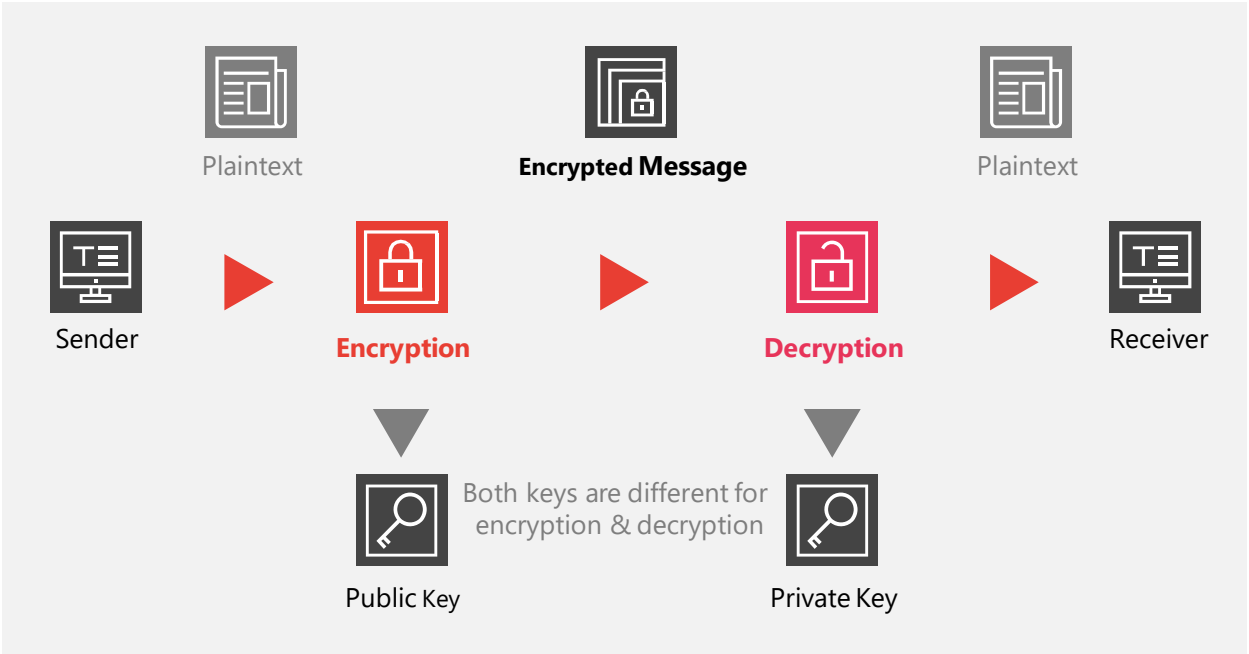
Minimum viable product (MVP): an MVP is a minimum version of a final product and is delivered to the market right away. It is typically simple, appealing, and bug-free. An MVP is a version of a product that has just enough features to stay viable. It only has the core functionality. Delivering an MVP to the market allows for immediate feedback on the product's value.

Public-private key cryptography

Public-private Key Cryptography (PKC) uses a pair of keys: a public key and a private key. The public key can be disseminated to any party without compromising security. Each party, however, holds their own private key in secret. Both keys are strings of alphanumeric symbols that are mathematically related to each other using a "one-way function". In PKC, a sender can input the receiver's public key into the one-way function to produce an encrypted message which can only be decrypted by the receiver's private key. Therefore, given a public key (that can be shared), a private key (that is secret), and a one-way function (that is common knowledge), two persons (sender A and receiver B) can transfer tokens in three steps:

1. **Signed instruction**: Sender A uses their private key and the one-way function to digitally sign a message to pay N number of tokens to receiver B. The digital signature is a string of alphanumeric symbols, akin to the public and private keys, but cannot be decrypted by anybody except sender A. Sender A broadcasts the message and the digital signature to validator nodes on the distributed ledger.

2. **Verification**: Validator nodes are third parties (or the receiver B themselves) whom sender A has shared their public key with. Validators receive sender A's message and digital signature. They then match sender A's public key with the digital signature to verify that sender A did in fact send the message.



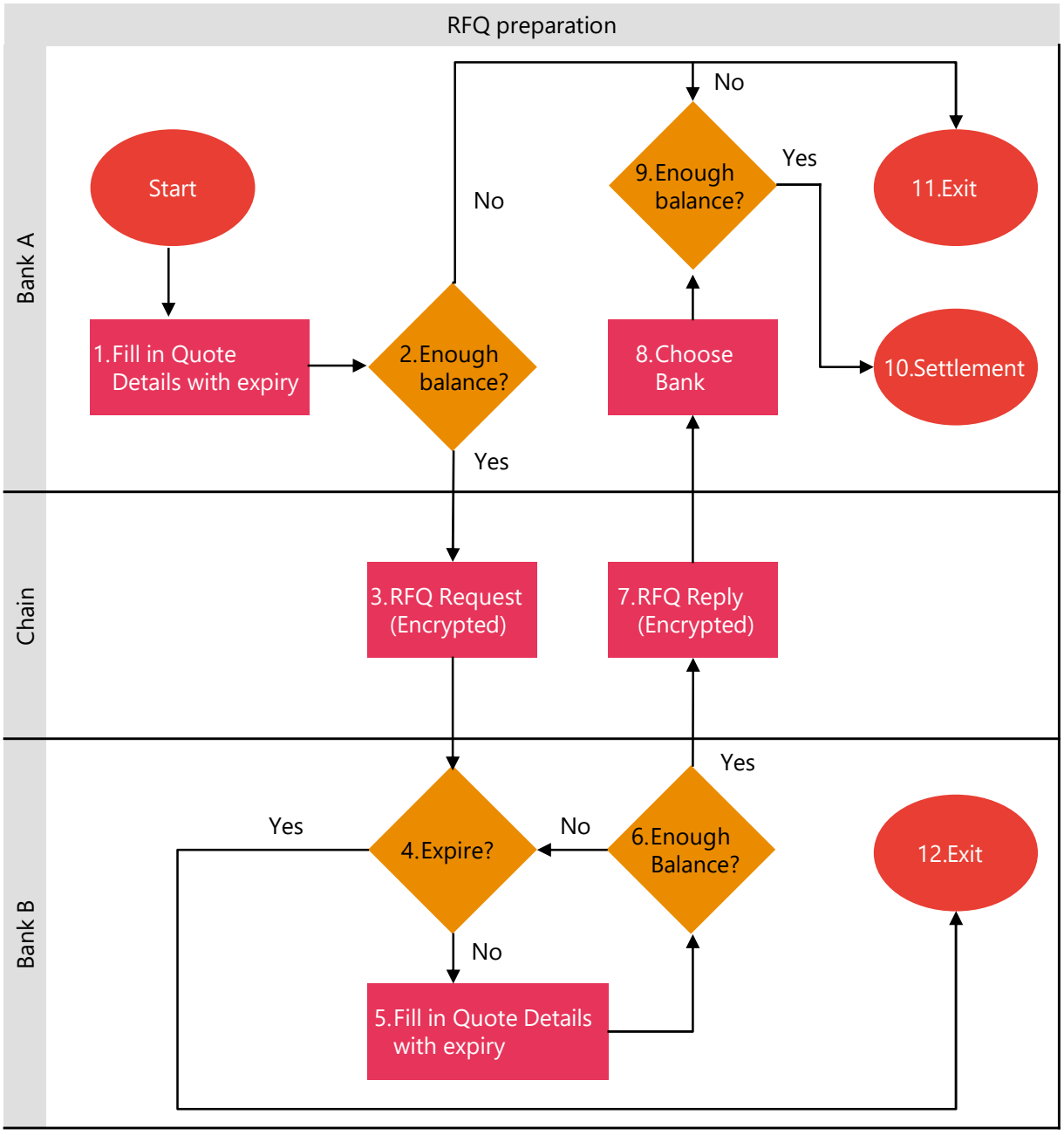
3. **Updating the ledger**:

   a. If the digital signature is verified, the payment message can be added to the ledger. Messages added to the ledger are then synchronised with the rest of the network to prevent double-spending between participants. To conclude the transfer, the digital tokens associated with sender A's public-private keys are destroyed and replaced with receiver B's public-private keys. This action is destructive with regards to sender A's information but constructive with regards to receiver B. This process ensures that only receiver B can initiate the next transfer of these tokens.

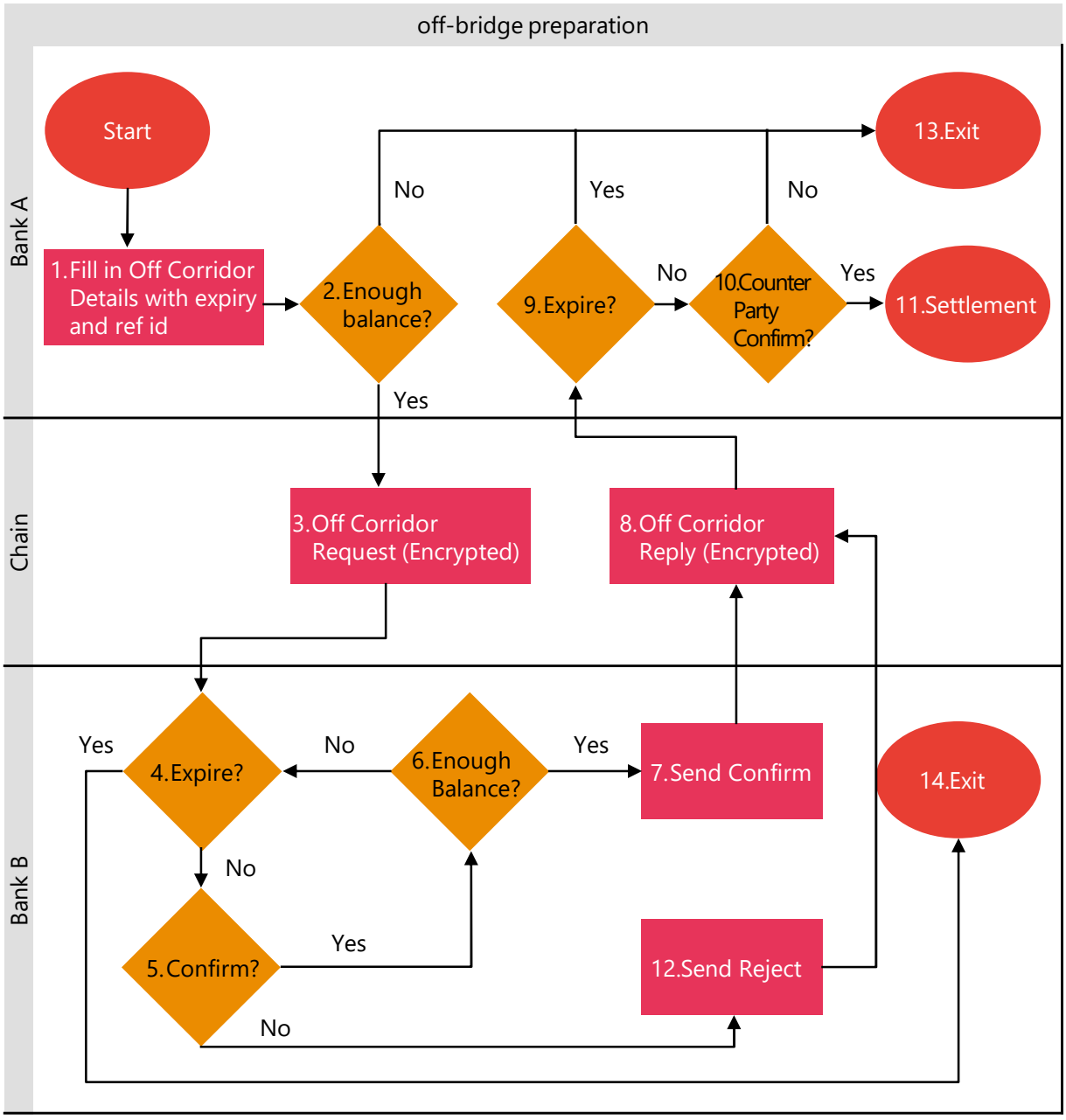
   b. If the digital signature is not verified (e.g. a person other than sender A sent the message), then the validator rejects the message and the transfer is not added to the ledger.

Annex 2 FX quote flow charts

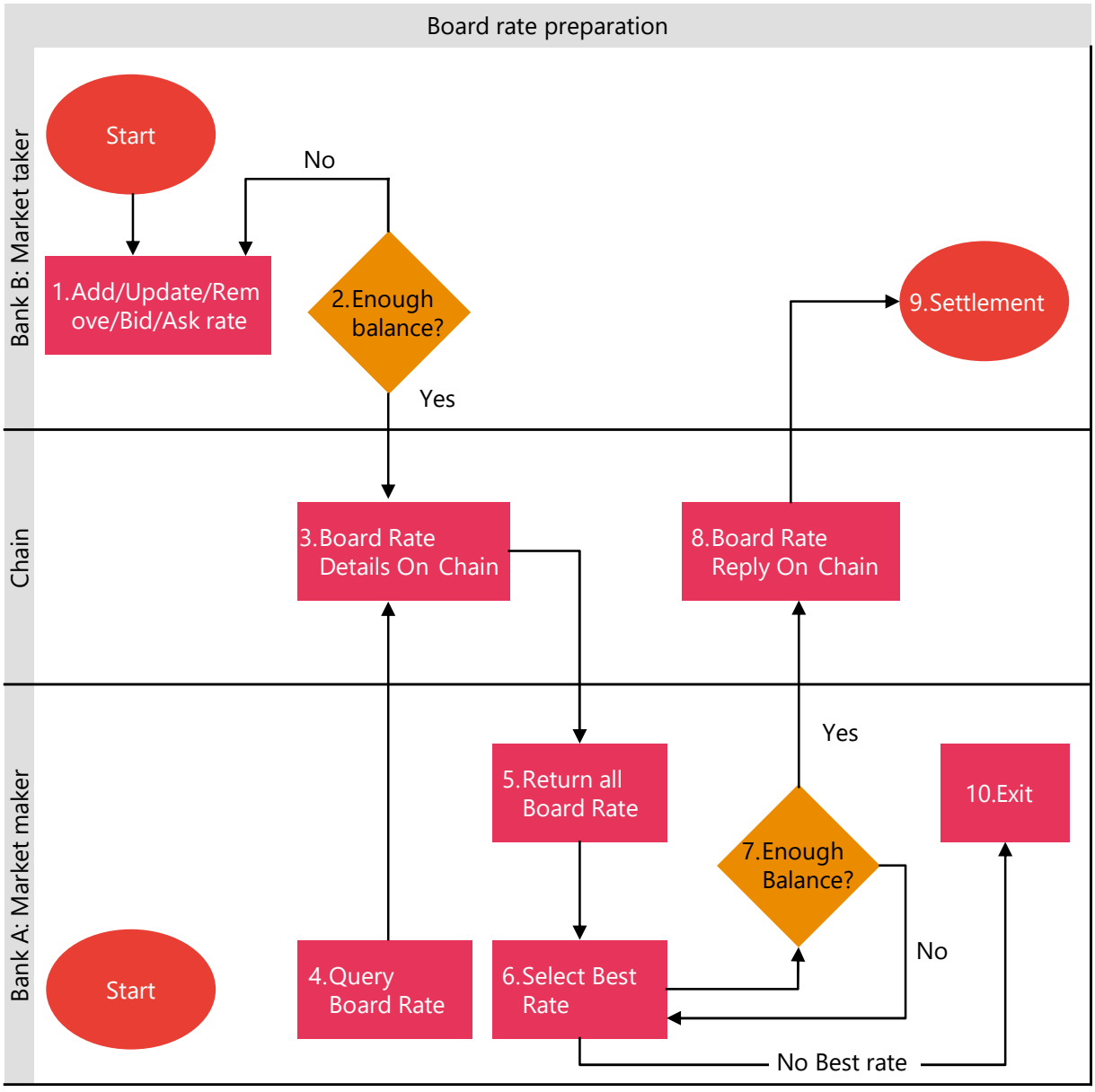
Request for quote



Off-bridge


off-bridge preparation
Bank A
Chain
Bank B
Start
1.Fill in Off Corridor Details with expiry and ref id
2.Enough balance?
No
Yes
13.Exit
9.Expire?
No
10.Counter Party Confirm?
No
Yes
11.Settlement
Yes
3.Off Corridor Request (Encrypted)
8.Off Corridor Reply (Encrypted)
Yes
4.Expire?
No
6.Enough Balance?
Yes
7.Send Confirm
14.Exit
No
5.Confirm?
Yes
12.Send Reject
No

Board rate


Board rate preparation
Bank B: Market taker
Chain
Bank A: Market maker
Start
No
1.Add/Update/Remove/Bid/Ask rate
2.Enough balance?
Yes
9.Settlement
3.Board Rate Details On Chain
8.Board Rate Reply On Chain
Yes
5.Return all Board Rate
10.Exit
7.Enough Balance?
No
Start
4.Query Board Rate
6.Select Best Rate
No Best rate

Annex 3 Project participants

BIS Innovation Hub

- Bénédicte Nolens, Hong Kong Centre Head
- Daniel Eidan, Adviser
- Asad Khan, Adviser
- Chaiwat Sathawornwichit, Adviser

Hong Kong Monetary Authority

- Colin Pou, Executive Director, Financial Infrastructure Department
- Nelson Chow, Chief Fintech Officer, Fintech Facilitation Office
- Brian Lam, Senior Manager, Fintech Facilitation Office
- Yvonne Tsui, Senior Manager, Fintech Facilitation Office
- Frederick Cheung, Manager, Fintech Facilitation Office

Bank of Thailand

- Vachira Arromdee, Assistant Governor, Financial Markets Operations Group
- Amporn Sangmanee, Assistant Governor, Internal Audit Group
- Thammarak Moenjak, Director, Financial Institutions Strategy Department
- Kasidit Tansanguan, Deputy Director, Office of Corporate Strategy
- Peerapong Thonnagith, Assistant Director, Digital Currency Team
- Sarun Youngnoi, Assistant Director, Digital Currency Team
- Witit Synsatayakul, Assistant Director, Foreign Exchange Strategy Unit
- Tunyathon Koonprasert, Senior Specialist, Digital Currency Team
- Tansaya Kunaratskul, Senior Specialist, Office of Corporate Strategy
- Pontakorn Mekintarangkoon, Developer, Digital Currency Team

Digital Currency Institute of the People's Bank of China

- Changchun Mu, Director-General
- Yuan Lyu, Deputy Director of Innovation Department
- Youcai Qian, Deputy Director of R&D II Division
- Ying Zhao, Team Leader of Legal and Compliance Team
- Shuang Zhang, Strategy Planning Team
- Zhan Zhang, Business Development Team
- Lin Su,Business Development Team
- Mingming Zhang, Business Development Team
- Mingyang Cai, Legal and Compliance Team
- Shiyue Sun, Business Development Team
- Zuorong Xia, Business Development Team
- Qingjie Chen, R&D II Team
- Yang Gao, R&D II Team
- Wenbo Wang, R&D II Team

Central Bank of the United Arab Emirates

- Saif Al Dhaheri, Assistant Governor – Strategy, Financial Infrastructure, and Digital Transformation of the Central Bank of UAE
- Shu-Pui Li, Advisor, The Governor Office
- Hafid Oubrik, Director of Payment Systems Operations and Development
- Junaid Ward, Assistant Director, Governor's Office
- Husam Habannakeh, Senior Manager of Banking Operation
- Salem Al Harmi, Banking operations

Vendors for Inthanon-LionRock Phase 2

- ConsenSys lead Charles d'Haussy, Managing Director APAC
- Forms HK lead Alex Chan, CEO
- PwC lead Gary Ng, Partner

Promoting global monetary and financial stability

This publication is available on https://www.bis.org

Picture credit: Ahmed, Musheer, FinStepAsia (P5, 7, 8, 17, 29, 45, 46, 70).