

INTHANON

Phase I

An application of Distributed Ledger Technology for a Decentralised Real Time Gross Settlement system using Wholesale Central Bank Digital Currency



BANK OF THAILAND







“Distributed Ledger Technology (DLT) has the potential to disrupt many different domains of financial services. Project Inthanon represents the collaborative effort between the Bank of Thailand and key industry players to explore and experiment the use of DLT in order to enhance efficiency and resiliency of the financial system. With a better understanding of DLT applications, we hope the project would lay a strong foundation for the future of Thailand’s financial sector.”

Dr. Veerathai Santiprabhob
Governor, Bank of Thailand

Foreword

The Bank of Thailand (BOT) has initiated Project Inthanon with the goal to assess potentials and applications of Distributed Ledger Technology (DLT) in the area of financial infrastructure. With collaboration from the leading industry players, Project Inthanon marks an important milestone in our effort to drive forward technological development for the Thai financial sector. The Project is divided into three phases. Phase I concentrates on building the fundamental payment infrastructure, whilst the applicability of DLT for other business solutions are further explored in the latter phases.

Building upon the bodies of work from other central banks' DLT projects, Inthanon Phase I aims to develop a proof-of-concept for a decentralised Real Time Gross Settlement system (RTGS) using tokenised Thai Baht on a distributed ledger. The proof-of-concept is expected to deliver key RTGS functionalities while demonstrating the distinctive benefits of DLT such as resiliency and privacy. Moreover, the Project's approach aims to encourage all participants to test the capabilities of DLT by collaboratively designing innovative solutions such as bond tokens and automated liquidity provision to improve the payment functions.

The Project's outcome reveals the potential of DLT for interbank payments and demonstrate the importance of collaboration and technological readiness of market participants as the benefits of DLT rely heavily on a strong network foundation. We believe Project Inthanon will encourage other financial institutions to further experiment and develop DLT for other use cases.

The BOT would like to extend our gratitude towards eight participating banks and our technology partner R3, who have contributed to the successful journey of Project Inthanon Phase I and the completion of this Report, which shares the objectives, approaches, technical findings, and insights from the Project.

We hope that the Report will provide a better understanding of the use of DLT applications on the payment system and insights to the future of Thai financial market as envisioned by Project Inthanon participants.

Mathee Supapongse
Deputy Governor, Bank of Thailand



Words from the Steering Committee



Bank of Thailand

The BOT has acknowledged of the rapid technological development in DLT which has been identified as a disruptive innovation adopted in many areas, particularly the financial sector. "Project Inthanon" is an important initiative of the BOT and key financial institutions in building a supportive financial technology ecosystem for learning and exploring DLT in order to innovate and develop key financial infrastructures.

Progressing in building a proof-of-concept system, we will push forward the collaborative approach for the enhancements of its capabilities in the next phases. This would help not only strengthen the network but also enhance the efficiency and productivity of the Thai economy.



Vachira Arromdee

Assistant Governor,
Financial Markets
Operations Group



Kukkong Ruckphaopunt

Executive Vice President,
Customer Service
Management,
Technology Division

Bangkok Bank Public Company Limited



As one of Southeast Asia's leading regional banks, Bangkok Bank is committed to exploring innovative technologies to provide better products and services for our diverse customer base. As Thailand's first member bank of R3 Consortium, we are delighted to embark upon a DLT journey with the Bank of Thailand and fellow Thai banks.

Project Inthanon provides an excellent opportunity to embrace Distributed Ledger Technology, commonly referred to as blockchain, to improve a key financial market infrastructure of the country. We look forward to sharing our experience to help forge better understanding and further local adoption of the disruptive technology.



Krung Thai Bank Public Company Limited

The real benefits behind the DLT is not directly as tools for financial system itself, but as a trusted, shared infrastructure between related multi-parties. Significant improvement of efficiency gained from lower cost of reconciliation, instant fraud prevention, high fault-tolerance, effective monitoring and auditing by regulators.

In order to truly achieve well-designed DLT, related parties including regulators must work together to reach the consensus on rules and governance body of the platform. In the age of disruption, development methodology such as Design Thinking and AGILE Development could be a wise choice.

As a state-owned bank, Krung Thai foresees that DLT is the important technology that will take financial industry into the age of distributed autonomous organization where banks are transparent and provide financial-as-a-service for the country.



Boonlerd Sinsombat

Senior Executive
Vice President,
Managing Director
Technology Group

Words from the Steering Committee



Voranuch Dejakaisaya

Chief Information and
Operations Officer

Bank of Ayudhya Public Company Limited



The economic implications of Blockchain / DLT have great potentials to disrupt the fundamental of National Financial Infrastructure.

With this belief, the Inthanon Project has been initiated by the Bank of Thailand, and is becoming a truly essential project for the country. The success of the project will encourage Thai Financial Institutions to go beyond just a collaborative experimentation of the Digital Currency in enabling new way of Interbank Settlement.

Krungsri is pleased to be the pioneer of the project and continue to support and take a lead in the digital innovation to uplift Thailand's economy by bringing in the best DLT Technology to serve customers.



Kasikornbank Public Company Limited

KBank is one of the leading pioneers in Thailand's Banking Industry in term of adopting DLT into real business operations. We have been committing ourselves in exploring and expanding our expertise to apply DLT in financial services.

Inthanon project is one of a kind in delivering powerful and creative collaborations among Thailand's financial institutions. Eight commercial banks and the Bank of Thailand have been working collaboratively in every step. We were thinking out of the box by consolidating user stories from all stakeholders designing the DLT framework, ultimately enhancing the liquidity of interbank payment transactions while protecting data privacy.



Silawat Santivisat

Senior Executive
Vice President,
Corporate and SME
Products Division Head



Pimolpa Suntichok

Senior Executive
Vice President,
Commercial Banking
Solutions

Siam Commercial Bank Public Company Limited



Project Inthanon is very crucial to the banking industry in this fast-moving technological environment to adopt the best-fit technology to better serve unique needs for Thai payment infrastructure. The project comes at the right time to address this. It is a true and remarkable collaboration between the regulator and commercial banks in exchanging knowledge and resources to achieve the shared-objectives to serve the country's infrastructure.

The outcome of Project Inthanon has demonstrated that DLT has not only increased efficiency but also reduced risks and overall costs in the financial ecosystem. It has given the team a strong encouragement to accelerate this initiative further to put in place a more robust, secure, and efficient country payment infrastructure.

Words from the Steering Committee



Thanachart Bank Public Company Limited

This is a great opportunity for Thanachart Bank to be a part of Project Inthanon that utilizes DLT in this project. The disruptive technology will change the current process from centralised to distributed which will transform Thai financial service system by eliminating intermediaries, increasing flexibility, safeguarding data privacy and enhancing resiliency.

Moreover, Thanachart Bank acquires knowledges from new working process, such as collaboration with other banks and BOT during Design Thinking session, to improve financial services and the national payment infrastructure.



Sutut Chitmonkongsuk

Chief Information and
Technology & Digital Officer



Parnkae Nandavisai

Managing Director
Head of Transaction Banking

Standard Chartered Bank (Thai) Public Company Limited



Standard Chartered Bank is pleased to be a part of Project Inthanon, a collaboration among commercial banks in Thailand and the Bank of Thailand. The collaboration in this Project evidences the Thai spirit of unity. The outputs of Project Inthanon Phase I preface the Project's subsequent phases that will set the stage for the next era of efficiency that Thailand's banking sector aims to achieve.



The Hongkong and Shanghai Banking Corporation Limited

HSBC is very honoured to be the international bank in Thailand represented in Project Inthanon Phase I; we look to leverage our involvement globally in other Central Bank Digital Currency projects having worked closely with Canada, Hong Kong, Singapore and now Thailand's regulator.

The collaborative nature of this initiative makes it a very interesting journey for all participants given the paradigm shift with distributed ledger technology. HSBC team included colleagues from Applied Innovation Hong Kong (which includes Kwok Ching TSUI and York Tsang) and Innovation Laboratory in Singapore, set up in partnership with the Monetary Authority of Singapore, as well as in Hong Kong.



Ai Chen Lim

Head of Global Liquidity
and Cash Management



Contents

Executive Summary	2
01 Introduction.....	3
1.1 Inthanon's Vision & Objectives.....	3
1.2 Project Approach	3
1.3 Phase I Scope	5
02 Background	7
2.1 Why Distributed Ledger Technology?	7
2.2 The Corda Platform	8
2.3 Other Central Bank Initiatives	9
03 Phase I Design	12
3.1 Architectural Design.....	12
3.2 Functional Design	13
04 Phase I Key Findings	25
4.1 Findings from Inthanon's Project Approach	25
4.2 Findings from the Proof-of-Concept	25
05 Next Steps and Future Works	28
5.1 Technical and Functional Features Build-outs	28
5.2 Legal and Regulatory Considerations	28
5.3 Operational Considerations	29
5.4 Looking forward to Phase II	29
06 Conclusion.....	30
07 Glossary	31
08 Appendix.....	32
8.1 Improving privacy of a decentralised LSM	32
8.2 Gridlock Resolution Algorithms	33
09 Acknowledgements	34



Executive Summary

The Bank of Thailand (BOT) seeks to position the Thai financial service industry at the forefront of DLT revolution. Named after the highest mountain in Thailand, Project Inthanon is a collaborative project initiated and led by the BOT to explore the potential of DLT for financial market infrastructure.

Launched in August 2018, Inthanon Phase I aims to achieve these key objectives: 1) to develop a collaborative network among Thai financial institutions for learning DLT and its applications for financial infrastructure enhancement, 2) to explore the capabilities of DLT and creating new designs by developing a proof-of-concept of decentralised Real Time Gross Settlement system (RTGS), and 3) to evaluate the impact of such design in both functionality and non-functionality aspects. This would also lead to the foundation for future consideration and improvement.

Project Inthanon is in partnership with R3 and a consortium of Thailand's financial institutions to build a proof-of-concept on Corda platform, a distributed ledger for enabling and managing financial contracts. The consortium is assembled in the project, consisting of Bangkok Bank Public Company Limited, Krung Thai Bank Public Company Limited, Bank of Ayudhya Public Company Limited, Kasikornbank Public Company Limited, Siam Commercial Bank Public Company Limited, Thanachart Bank Public Company Limited, Standard Chartered Bank (Thai) Public Company Limited, and The Hongkong and Shanghai Banking Corporation Limited.

Inthanon Phase I first experimented DLT for key payment functionalities consisting of cash tokenisation, decentralised fund transfers, payment queue management, and gridlock resolution. In addition, the project developed complex functionalities and enhanced architectural design from other previous central banks' projects.

One of achievements is the gridlock resolution architecture that can provide both privacy and atomicity properties. The design also succeeded to compromise between the optimised liquidity used and priority of transactions while gridlock resolution initiated. In addition, the innovative payment functions of bond tokenisation and automated liquidity provision were included in order to support banks liquidity in full 24/7 operating hours. This allows BOT to automatically provide liquidity to banks by allowing the use of bond token as a collateral if required. This automated liquidity provision also accomplished the property of atomicity by exchanging bond tokens and cash tokens simultaneously (Delivery-Versus-Payment) without any operator as an intermediary.

Given the results of these new functionalities tested, some improvements could be further explored. Project Inthanon will continue to leverage DLT capabilities to enhance the payment infrastructure in future phases. Phase II will explore the applications of DLT in the areas of bond tokens lifecycle and the atomic Delivery-versus-Payment (DvP) settlements, regulatory requirements related to non-residents, and fraud detection and prevention, while Phase III will extend functionalities of the proof-of-concept for cross-border payment and interoperability with other platforms and the legacy system.

The success of Inthanon Phase I reaffirms the importance of a cooperative network among stakeholders and a strong support from the authority in driving innovation and advancing the technology. The outcome of the project would not only help elevate Thailand's payment infrastructure, but also mark the key milestone of the overall financial market development.



01 Introduction

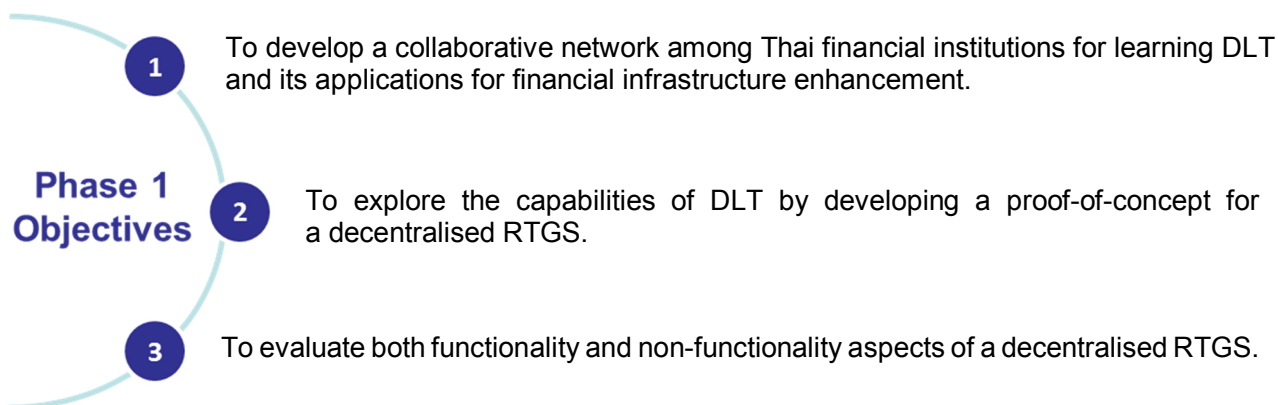
1.1 Inthanon's Vision & Objectives

1.1.1 Inthanon's Vision

The vision of Project Inthanon is to create an environment for the Thai financial services industry to collaborate and gain a better understanding of the characteristics of DLT through hands-on experiences. The decentralised RTGS for the interbank payment was chosen to be the first business case for the joint-learning initiative in Phase I. The feasibility, benefits, and trade-offs of DLT for an interbank payment system development will also be evaluated. Insights from the project are expected to provide a foundation of future development of the Thai payment system. The roadmap of Project Inthanon is divided into three distinct phases. The anticipated duration of each phase is approximately three months, to allow for technology development and reporting the findings.

1.1.2 Phase I Objectives

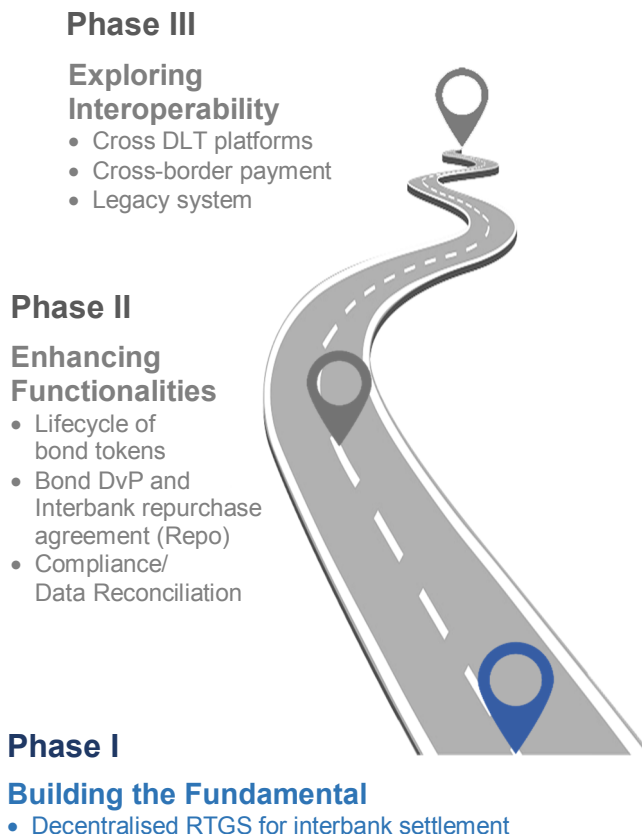
Phase I had three key objectives:



1.2 Project Approach

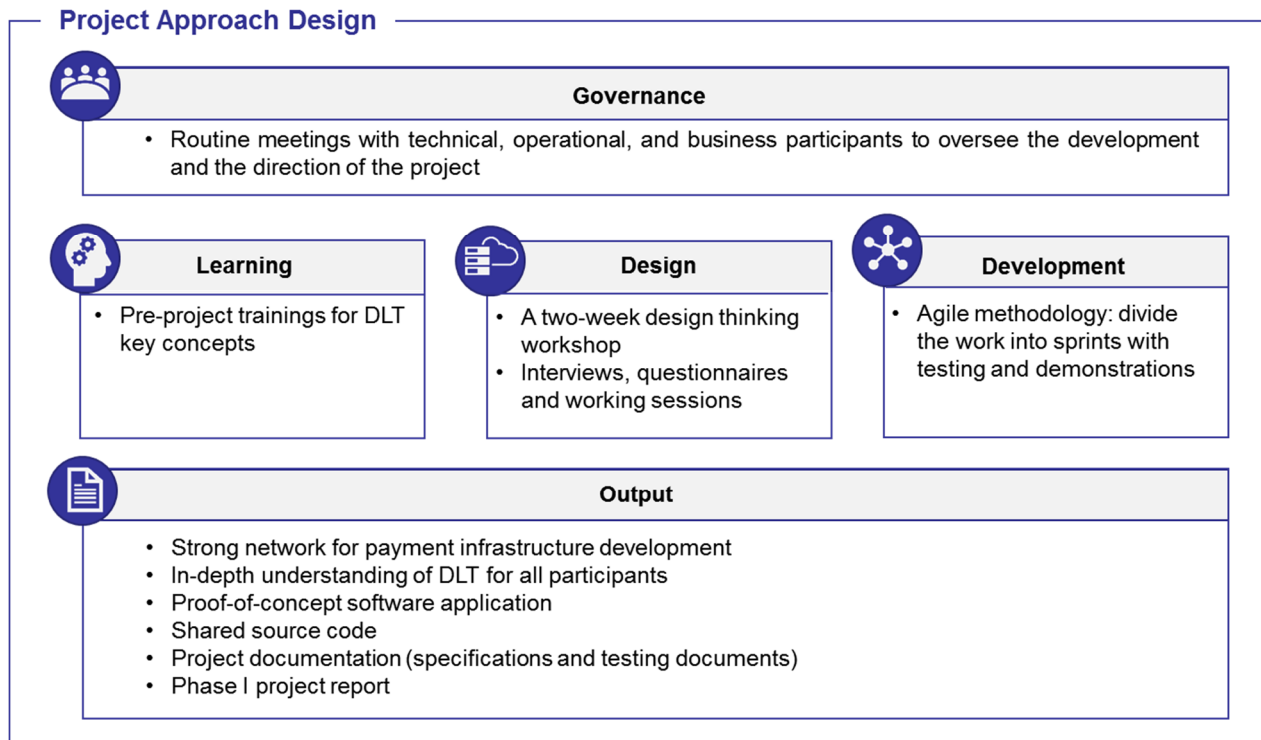
Project Inthanon is designed to accelerate the Thai financial services industry knowledge and understanding of the potential of DLT, and to drive the technology forward with innovative solutions tailored specifically to Thailand's financial service sector.

Figure 1: Roadmap of Inthanon



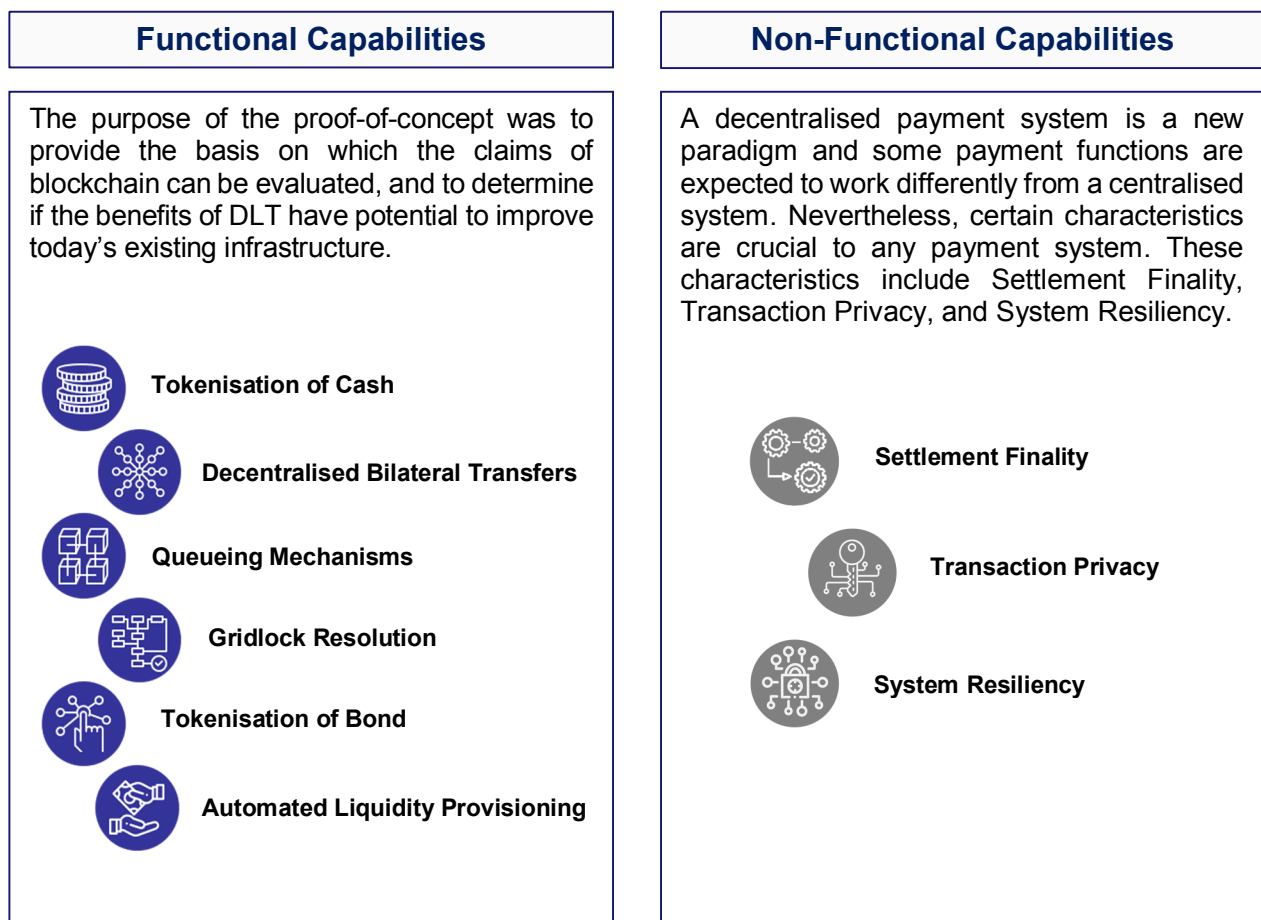
Two key principles of Project Inthanon's approach are 1) collaborative design and 2) shared development. The solution design process is carried out through a collective exercise involving all key stakeholders and is expected to facilitate learning throughout the duration of the project, and to produce problem-focused solutions rather than top-down prescribed solutions.

Figure 2: Inthanon's Project Approach Design



1.3 Phase I Scope

The scope for the Phase I proof-of-concept included:



1.3.1 Functional Capabilities



Tokenisation of Cash

The central bank node has an exclusive capability to issue and redeem (destroy) Thai Baht (THB) cash tokens used by parties on the network. The tokens should only be available for use by a whitelist of parties, those known and approved by the central bank to become part of the network.



Decentralised Bilateral Transfers

The decentralised payment network should be set up for participating nodes to make payments by transferring cash tokens to one another without relying on the central system operator. In Phase 1, the network consists of nodes from the eight participating banks and the BOT.



Queueing Mechanisms

Participants may temporarily have insufficient liquidity to make payments. As such, payment instructions become queued as obligations. Participants should be able to set priorities and manage their outgoing queues to serve their business and operations purposes.



Gridlock Resolution

There can be a situation where two or more queued obligations are resolvable with one or more net payments. This situation is known as a gridlock. Many existing RTGS have gridlock resolution mechanisms to resolve gridlocks through making net payments periodically in what is known as Liquidity Saving Mechanism (LSM).



Tokenisation of Bond

Bond tokenisation allows banks to effectively convert “real-world” bonds held at the Thai Securities Depository (TSD) into bond tokens on the Distributed Ledger system (DL system). Bond detokenisation is the reverse process. These tokenised bonds are used for the automated provision of liquidity when needed. This capability of having multiple tokenised assets would allow the leverage of DLT on the atomic DVP settlement which enhances the efficiency of the decentralised RTGS.



Automated Liquidity Provisioning

The Automated Liquidity Provisioning (ALP) is explored in Phase I to provide the liquidity when the ‘Urgent’ transaction has passed some certain period of time or the netting solution cannot be found during a gridlock cycle. The ALP is conducted by an automated intraday repo transaction between a participant requiring liquidity and the BOT, using a tokenised bond as the collateral asset. This functionality would be advantageous for facilitating around-the-clock settlements in the decentralised RTGS.



- an innovative function developed in Project Inthanon

1.3.2 Non-functional Capabilities

Non-functional aspects that are essential to any interbank settlement system were also evaluated for Phase I proof-of-concept.



Settlement Finality

During a transaction, there should be no ambiguity as to the ownership status of funds or an asset, at any point in time. Furthermore, once a transaction occurs, it should be irrevocable. This is the principle for any payment system, and is important for risk management, especially in the event where a payment participant becomes insolvent.



Transaction Privacy

It is important that the details of transactions are private to counterparties, and that unrelated parties should not be able to discover business-sensitive information. Under decentralised system with no central operator, this principle is particularly challenging since the responsibility for controlling a database in such platforms is shared among network participants. Thus, there exists a tradeoff between decentralising transfers and keeping transaction privacy. However, cryptographic techniques are heavily used for maintaining transaction privacy under the decentralised system.



System Resiliency

Resiliency is considered to be a key advantage of a decentralised system over a traditional one since the system does not rely on a central operator to navigate transactions. In a decentralised system, if a node is incapacitated, other nodes should still be able to function.

1.3.3 Out of Scope

Phase I proof-of-concept was not designed to be deployed as-is into a production environment. As such, some non-functional requirements to bring the system up to production grade as well as integrations of the Phase I proof-of-concept with external systems were not in scope for Phase I. For clarity, Phase I was not designed or built to be directly compared against BAHTNET system. In addition, messaging standards such as ISO20022 were not in the scope of Phase I.

02 Background

This chapter provides the main concepts of Distributed Ledger Technology (DLT) as well as its potential benefits when applied to the payment system. The second part of this chapter includes details on Corda, the platform experimented in Project Inthanon for developing the proof-of-concept, and the summary of similar DLT projects of other central banks.

2.1 Why Distributed Ledger Technology?

DLT, commonly referred to as 'blockchain technology' is a combination of technologies such as cryptography, consensus algorithms and smart contracts¹. These technical features allow digital assets and their values to be created and passed from party to party with guarantees that the assets are authentic and have not been copied or counterfeited, without needing a trusted third party to debit and credit accounts. Furthermore, the DL system does not rely on a central party to manage participating members' account balances or database but relies on the shared control among participants. However, there is no universal practice on database control in the DLT platforms. Some platforms replicate copies of ledgers among participants while others may restrict data sharing to just the related parties. In common, they prevent parties from spending the same digital asset more than once (prevent double-spending).

Several central banks have acknowledged the DLT capabilities of creating digital assets and transferring their values, which match the core fundamental of the payment system. In addition, DLT has potential to enhance cost savings, transactional traceability, and system resiliency. Thus, most central banks experimenting with DLT started with investigating the feasibility of implementing DLT with their Real Time Gross Settlement (RTGS) by building a proof-of-concept.

RTGSs are typically operational during office hours and used for high value transactions requiring immediate settlement. Most RTGSs are operated on centralised infrastructure, which is subject to risks such as a single-point-of-failure. The high-value nature of RTGS transactions requires that the system processes transactions seamlessly and efficiently to reduce ambiguity and risks in the financial market.

BAHTNET

The core RTGS in Thailand is known as 'BAHTNET' (Bank of Thailand Automated High-value Transfer Network). It facilitates large value interbank funds transfers, third party funds transfers for bank customers and the government, multilateral fund transfers, and settlements for cash leg of government bond trading, along with inquiry services.

One prerequisite to operate RTGS smoothly and efficiently is the ability to manage liquidity in the system. Specifically, in BAHTNET system, there are three major liquidity management mechanisms to accommodate intraday payments between participants as follows:

1) Payment Instruction Queueing to allow participants to input payment instructions while the participants have insufficient liquidity to make the payment. Queued payments are executed on a first-in-first-out basis once sufficient liquidity arrives in their accounts (preemptive FIFO). The queued payments can be reprioritised by the participants.

2) Gridlock Resolution to allow bilateral and multilateral queued payment instructions to execute if a netting solution can be found and does not result in any party becoming overdrawn. The gridlock resolution system uses algorithms to search for combinations of queued funds transfer orders that result in all participants having net positive balances, then executes these simultaneously.

3) Intraday Liquidity Facilities (ILF) which provide interest-free facilities to participants to help facilitate interbank payments by temporarily providing liquidity on BAHTNET against eligible collateral. When BAHTNET opens, the BOT provides intraday liquidity to the participants against the high-quality liquid collateral in the form of repurchase transaction. The minimum amount of collateral for this facility is required. At the end of the day, the participants have to buy back their collateral from the BOT. The BOT provides ILF on a fully collateralised concept in which the collateral is valued on a mark-to-market basis with appropriate haircuts.

¹ Smart Contracts are self-executing contracts in computer code which are embedded in DL network to automatically enforce rules and navigate interactions between nodes in the network.

Some characteristics of DLT that may be beneficial to the Thai financial services industry if applied to a payment system are identified as follows:

1) Atomic Delivery-vs-Payment Transactions (atomic DvP)

The interesting aspect of DLT for financial markets is the ability to record multiple asset types as tokens so they can be transacted simultaneously on the same ledger. This means that the system can provide atomic DvP settlement. This involves transferring ownership of two assets (or payments) simultaneously or not at all. The concept would be particularly useful for the delivery of financial securities against the payment of cash.

2) 24/7 Payment Operations

Tokenised assets can be transacted around-the-clock without the central bank needing to make debits and credits in its main ledger, as long as participating nodes are available and operational.

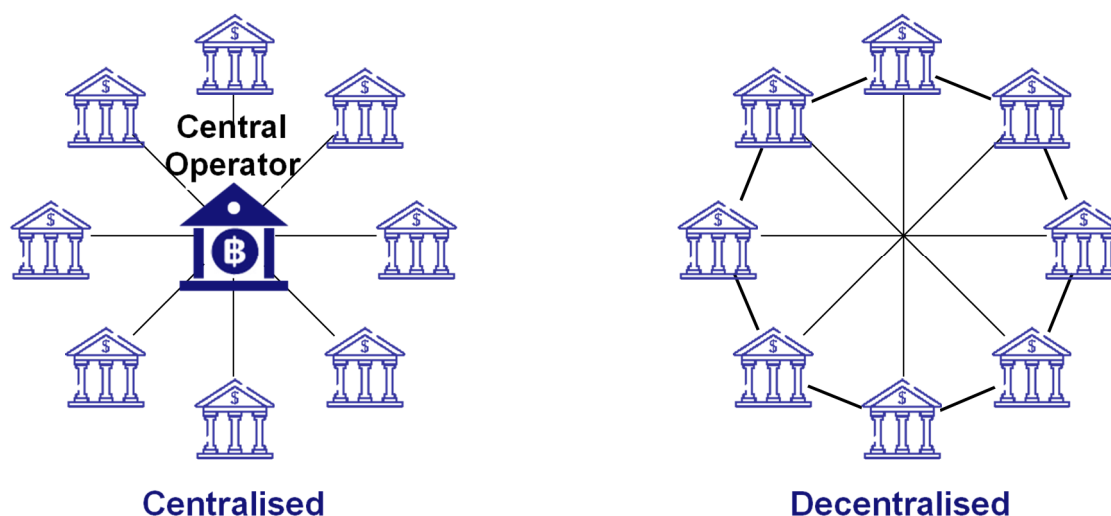
3) System Resiliency

A DL system may be considered more resilient than a centralised system owing to its decentralised nature and lack of a single-point-of-failure. This resiliency is important in a payment system that needs to have high availability as systemic failure has potentially catastrophic implications.

4) Automated Liquidity Provision

Currently, the process of adding intraday liquidity in BAHTNET via bond repurchase agreements are predetermined early in the day. Therefore, the amount of liquidity used is not at the optimum level during the day. With DLT, the process of injecting liquidity for participants with insufficient balances can be achieved automatically and around-the-clock using cash and bond tokens with reduced settlement risk.

Figure 3: Connection between Banks in Centralised vs. Decentralised System



2.2 The Corda Platform

Project Inthanon does not intend to compare different DLT platforms. Rather, the project aims to develop the proof-of-concept to test the capability of DLT for interbank payments and increase the understanding of DLT for project participants.

Corda was chosen as the platform for developing Project Inthanon's proof-of-concept. An overview of key features of Corda is provided in this section.

Corda is an open source distributed ledger platform built to record and manage contracts between mutually distrusting parties. Corda was built by R3 in collaboration with the world's largest financial institutions. It was designed to meet the rigorous requirements imposed by financial service regulators, conform to industry standards, and deliver on the promise of DLT. Corda is unique among blockchain platforms in that multiple Corda networks can join up to create a wider network with assets that can be transferred between them.

Corda distinguishes itself from other DLT platforms through several design characteristics to ensure that the platform could be used to solve real world problems found in any industry:

- Supports transactions between strictly regulated entities
- Allows counterparties to know each other's identity
- Protects privacy by not globally broadcasting transaction data
- Provides technical finality which could serve the creation of enforceable transactions
- Scales to support a global system of transactions

Corda addresses many of the challenges of building an enterprise-grade DL network with its unique point-to-point architecture where asset data is only sent to parties who need to see it – the sender and receiver of the asset. This allows Corda to achieve the openness of public networks while retaining the security and privacy characteristics of a private network.

Corda's privacy model is to send as little data to parties as possible to achieve the guarantees that the tokens being transacted are authentic and have not been copied. Unlike other DLT platforms that broadcast transaction data to multiple or all parties, Corda's transactions are created and confirmed between the sender and receiver, and a notary service confirms that the tokens have not been double-spent. The notary

service guarantees this by keeping track of transaction identifiers, without seeing the contents of the transactions themselves. Thus, Corda does not have a replicated ledger which contains the history of all transactions. However, assets can be traced back to the original of issuance through a chain of ownership, as Corda uses a "UTXO" (Unspent Transaction Output) model for creating a lineage of tokens, similar to that of Bitcoin.

2.3 Other Central Bank Initiatives







Central banks have been monitoring and exploring the potential impact of financial technology (fintech) and DLT for financial markets. As the technology develops, some central banks have set up units with specialist to understand the functionality and infrastructure that new technologies can bring to the ecosystem.

Central banks experiments have tended to follow a similar pattern: first investigating decentralised wholesale domestic payments, then extending the projects to explore tokenised assets such as bonds and equities for DvP transactions. Some central banks also eye on cross-border flows to explore DLT for international payments.

With regard to technology platforms, early experiments used a fork of public blockchain platform Ethereum, while later experiments have focused on various DLT platforms.

Project Inthanon builds on early lessons learnt from previous projects, adds some innovative capabilities, and localises the functionality to the Thai context.

Table 1: Summary of Other Central Bank DLT Initiatives on Payment System Made Public to Date.

Phase	Paper Published	Project Focus	DLT Platform Used
 Bank of Canada Project Jasper			
Phase 1	Mar. 2016	1.Create a wholesale interbank RTGS proof-of-concept on DLT Ethereum platform 2.Evaluate PFIMs against tokenised interbank payments	Ethereum
Phase 2	Dec. 2016	1.Rebuild original proof-of-concept on Corda 2.Build additional functionalities such as LSM	Corda
Phase 3	Oct. 2018	1.Integrate a liquidity savings mechanism for netting transactions 2.Examine DvP solutions for security settlement	Corda
 Monetary Authority of Singapore Project Ubin			
Phase 1	Aug. 2016	1.Build a proof-of-concept for domestic RTGS on a private Ethereum network. 2.Identify the non-technical implications of moving this into a production environment 3.Integrate DLT with existing RTGS in a test environment to automate tokenisation and detokenisation	Ethereum
Phase 2	Jul. 2017	1.Expand on the original proof-of-concept by incorporating LSMs 2.Understand how RTGS privacy can be ensured on DLT 3.Compare alternative DLT platforms	Quorum, Corda, Hyperledger Fabric
Phase 3	Nov. 2018	1.Explore different combinations of DLT for DvP between cash and Singapore government bonds 2.Test and examine solutions designed by Anquan Capital, Deloitte, and Nasdaq	Ethereum, Hyperledger Fabric, Chain, Quorum, Anquan
 Central Bank of Brazil			
Phase 1	Aug. 2016	1.Identify use cases and build a working prototype for the central bank using DLT 2.Identify realistic functionality and build a minimum proof-of- concept for RTGS system on DLT platform	Ethereum
Phase 2	Nov. 2016	1.Analyse competing blockchain platforms using the selected use case as a benchmark 2.Address the privacy issues identified in the previous phase	Corda
 European Central Bank & Bank of Japan Project Stella			
Phase 1	May. 2017	1.Build RTGS system on DLT, including LSM functions 2.Assess safety and efficiency of current system in DLT implementation	Hyperledger Fabric
Phase 2	Nov. 2017	1.Build DvP proof-of-concept on different DLT platforms 2.Identify the trade-off between network size and performance 3.Assess DLT capability for cross-chain securities settlement	Quorum, Corda, Hyperledger Fabric, Elements
 Hong Kong Monetary Authority Project Lionrock			
Phase 1	Aug. 2016	1.Identify use cases and build a working prototype for the central bank using DLT 2.Identify realistic functionality and build a minimum proof of concept for RTGS system on DLT platform	Corda
 South African Reserve Bank Project Khokha			
Phase 1	Feb. 2018	1.Build an RTGS proof-of-concept on DLT, exploring on privacy and scalability 2.Perform tests under a variety of deployment models in different locations 3.Assess a Quorum-based interbank payment system	Quorum



03 Phase I Design

This chapter provides the information on the design of the Phase I proof-of-concept from the architectural to functional aspects. Information about the innovative functionalities which were introduced to provide an alternative solution to the privacy concern arising from the previous central banks' works and to enhance the capability of the system is also summarised in this chapter.

3.1 Architectural Design

For Inthanon Phase I, the proof-of-concept was built on Corda open-source version 3.2. Each node - BOT, banks, and notary node- is hosted in individual Azure virtual machines. The key components for Corda's architectural design for Phase I are as follows:

1) Corda Distributed App (CorDApp)

Corda Distributed App (CorDApp) are distributed applications that run on the Corda platform. Each CorDApp is installed at the level of the individual node. The goal of a CorDApp is to allow nodes to reach agreement on updates to the ledger. CorDApp consists of an application program interface (API), flow, and contract.

2) Network Map Service

The network map is a list of the approved parties in the network and contains a mapping between real world identities and network IP addresses, as well as some other information.

3) Central Bank (BOT) Node

This node has two key functions:

- 1) As a monetary agent, this node
 - Creates and destroys cash tokens
 - Re-issues and destroys bond tokens
 - Provides intraday liquidity (cash tokens against bond tokens) via reverse repos with the participating banks and vice versa
- 2) As the Liquidity Saving Mechanism oracle node (LSM oracle node) that collects data of obligations (pending payments) and calculates gridlock resolutions.

In a production system, these functions can be split into different nodes if required.

4) Participating Bank Node

Banks store cash tokens and bond tokens in order to make payments with each other as well as performing repos with the central bank node.

5) Notary (Consensus Service)

The notary service in Corda serves to prevent double-spending within the network. Once the notary service is satisfied that a digital token has not been spent before, it issues a signature to indicate the transaction finality.

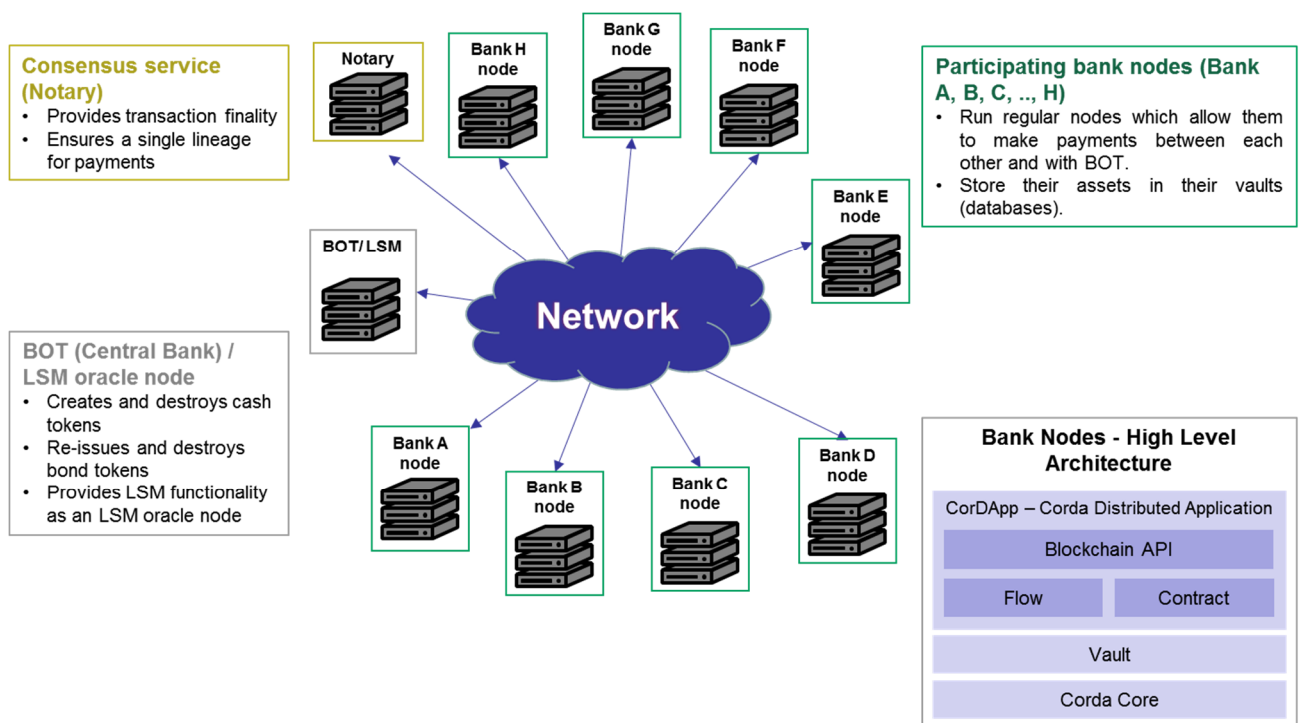
In Phase I, a 'non-validating' notary service was chosen, meaning that only transaction identifiers are sent to the notary, and so the notary does not know the contents of the transactions. Its only job is to prevent double-spending. Another type of notary is 'fully validating' where the full contents of each transaction are sent to it, which have privacy implications.

The notary service can be run either by the central bank or any independent party. It can also be implemented as a single node or multiple nodes that come to consensus using any consensus algorithms to remove a single-point-of-failure. In Phase I, the BOT runs a single node notary service.

Consensus algorithms

A consensus algorithm is a decision-making process of the network to achieve an agreement on the data value. Two popular consensus algorithms are Raft and Practical Byzantine Fault Tolerance (PBFT). Raft assumes that all parties are trustworthy, i.e. no one is trying to subvert the system by deliberately supplying false information to other parties or deliberately withholding information. PBFT assumes that parties may be hostile.

Figure 4: Inthanon Phase I Architectural Design



3.2 Functional Design

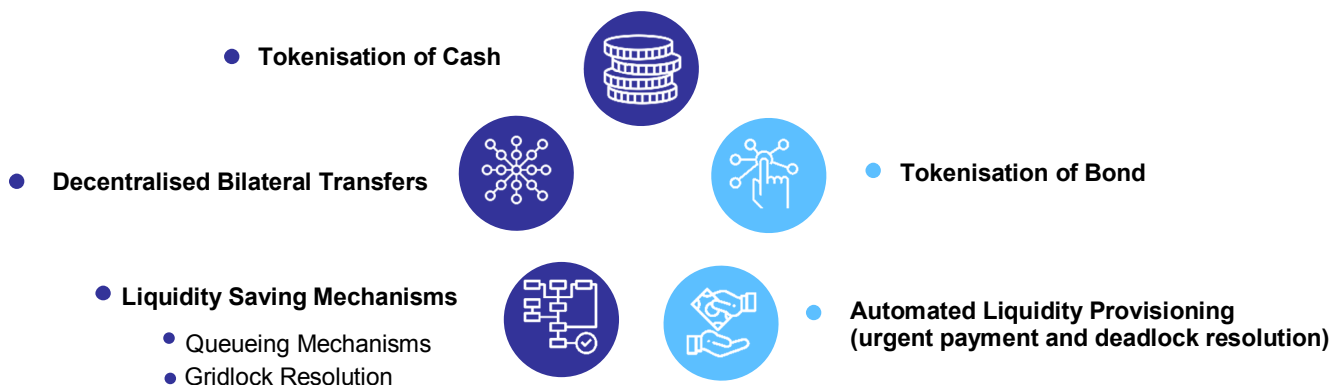
Inthanon Phase I explored the use of DLT to create cash tokens in order to perform payment functionalities on DL network, which include:

3.2.1 Tokenisation of Cash

In Inthanon, tokens were created by BOT and passed to a requesting participating bank, which can then send the tokens to other participating banks in the network without needing to instruct a third party to debit and credit account (peer-to-peer).

Figure 5: Phase I Standard and Innovative Payment Functionalities

Standard payment functionalities



Innovative solutions for payment functionalities

Tokenisation of Cash

Cash tokens are created by the BOT. In Phase I proof-of-concept's design, participants are required to convert their balances in the RTGS to cash tokens, just like a participant would convert their balances in the RTGS to physical banknotes.

The creation of cash tokens is entirely demand-driven. Tokens are created when participating banks instruct a fund transfer from their current accounts at BAHTNET to a specially created collateral account (omnibus account) at BAHTNET. Once the BOT recognises this balance transfer, it simultaneously creates cash tokens on the distributed ledger and sends them to the requesting bank. As a movement of cash balance is required at BAHTNET; this process may only be initiated during BAHTNET operating hours.

Detokenisation of Cash

This is a reversal of the cash tokenisation process. A participant who wishes to exchange cash tokens on the distributed ledger for balances at BAHTNET sends the cash tokens to BOT's node with a detokenisation request. The BOT approves the detokenisation request and permits a balance transfer in BAHTNET from the collateral account to the requesting bank's account.

Tokens vs Account Balances

Cash token is a central bank-issued money digitally issued as a token so it can function under the DL system. However, cash token is sometimes referred to as central bank digital currency or CBDC.

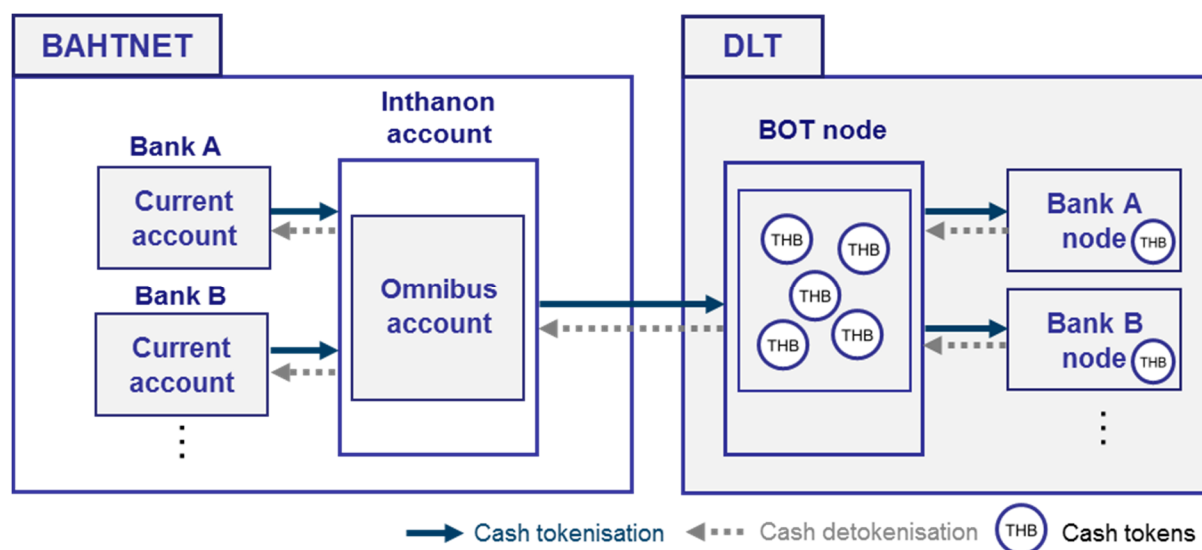
Nevertheless, digital money issued by the central banks has long been existing in a form of reserves deposited in banks' current accounts under the central banks in the RTGS. Since the money is held in accounts and the balances are controlled by the central banks in the central systems, the digital money is thus managed under account balances basis.

Whereas tokens represent the data stored on the servers of the money owner, they are similar to banknotes as a form of physical tokens issued by the central banks stored in the safety vaults at commercial banks. Tokens can be passed from one participant to another without instructing a central service to debit and credit accounts.

Zero Interest Cash

In the proof-of-concept, cash tokens bear zero interest, same as cash balances in the current accounts.

Figure 6: Illustration of Cash Tokenisation and Detokenisation Process



3.2.2 Decentralised Bilateral Transfers

A bank may wish to make a payment to another bank because of its own principal activities or being instructed by a customer. To do this, the sending bank sends payment instructions to make fund transfers to the receiving bank, and the amount should be settled given the sending bank has sufficient balances for the payment.

Under the centralised system, the central payment operator has a key role to validate all payment instructions for the network participants. However, in the decentralised system, the fund transfer is processed peer-to-peer with the sender and receiver validating and executing the payment without going through a third-party validator. A mechanism to ensure validity, security, and privacy of the fund transfers is therefore required for the payment settlement to be completed successfully.

Two of Corda's key features to ensure validity, security, and transaction privacy are:

1) Confidential Identity (CI): CI is used to obfuscate the identity of token holder by generating single-use public key and certificate per transaction. Both sender and receiver of a transaction create new public key identifier on the fly and tell each other about them in a certificate swap. Hence, CI consists of a public key and certificate. The tokens are then sent from one confidential identity to another. The identity is not resolvable to real-world identity by any other node on the network except the two who are transacting. This reduces the amount of intelligence that future owners of the token can gain when reviewing previous owners of the token.

2) Notary service²: The notary service's task is to prevent double-spending by attesting that for a proposed transaction, it has not already signed other transactions that consumes any of the proposed transaction's input states. Once the notary node validates that the transaction is not double-spent nor consumed by a prior transaction, it provides a signature over that transaction, which creates a point of settlement finality in the system.

When the sending bank initiates a payment to the receiving bank, a new CI is created particularly for the transaction. Two scenarios can occur:

Scenario 1: The sending bank has sufficient cash tokens for the payment:

When the sending bank has sufficient cash tokens, it creates a payment transaction which is digitally signed by the sender, the receiver and the notary node. After the transaction is signed by all three parties, the payment transaction is deemed to have successfully completed.

Scenario 2: The sending bank has insufficient cash tokens for the payment:

When the sending bank has insufficient cash tokens, it creates an obligation which is digitally signed by the sender and the receiver and the notary node. After the obligation is signed by all three parties, the obligation state is deemed as an active obligation, and then is put in both sender and receiver's queues. Only when the sending bank acquires sufficient cash tokens, the obligation follows the process in Scenario 1, and the obligation state is deemed to be a settled obligation.

3.2.3 Liquidity Saving Mechanisms

A bank requires sufficient liquidity to make gross payments. However, there is opportunity cost of holding zero-interest cash, so the bank tries to hold cash as little as necessary to fulfil its payments arising from its clients and its own activities. In addition, handling large value transactions in gross may lead to intraday liquidity shortage, hence, LSMs are introduced to enhance efficiency of liquidity management. LSMs allow these two functions:

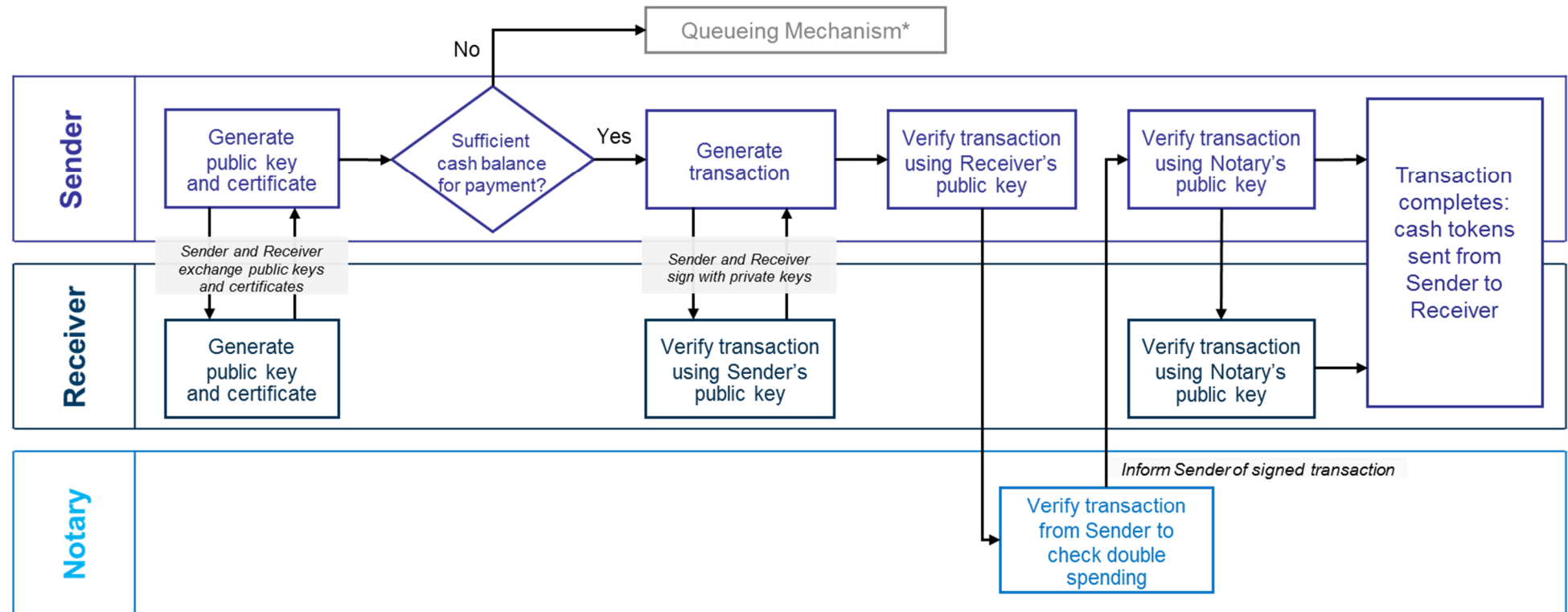
1) Queueing Mechanism allows payment instructions to be prioritised and reprioritised.

2) Gridlock Resolution settles payment through bilateral and multilateral netting opportunities.

LSMs exist in many centralised RTGS, and decentralised LSMs architectures have been explored in some previous central bank projects.

² Notary service in Corda network: <https://docs.corda.net/key-concepts-notaries.html>

Figure 7: Illustration of Decentralised Bilateral Transfer Process



* The details can be found in Phase I Design Chapter under the Queueing Mechanism section.

Queueing Mechanism

Participating banks may temporarily have insufficient liquidity to make payments. As such, payment instructions become queued as obligations. Once a bank obtains sufficient liquidity, the obligations will be settled in accordance with predetermined priorities.

1) Queue Management

A sending bank can manage its outgoing obligations by setting priorities, reprioritising or cancelling the obligations as needed. A receiving bank is able to monitor the information of incoming obligations (i.e. amount and sending bank's name) but not the priorities set by the sending bank.

2) Queue Priorities

Three levels of priorities can be assigned to the payment instructions: 'Urgent', 'High', and 'Normal'. The obligations can be reprioritised to higher or lower priorities. The key features of each priority are summarised in Figure 8.

Gridlock Resolution (GR)

Inthanon's gridlock resolution was designed and developed collaboratively by the Inthanon team based on findings from similar DLT projects of other central banks. The fully decentralised GR was successfully tested in the Project Ubin, but some privacy issues were partially compromised. The Inthanon team, therefore, attempts to put privacy issue on the top priority.

As a result, the GR process was redesigned to address the privacy concern by maintaining the centralised function for initiating, detecting and planning GR while the settlement process was still executed in a decentralised manner. The design incorporated the five key features:

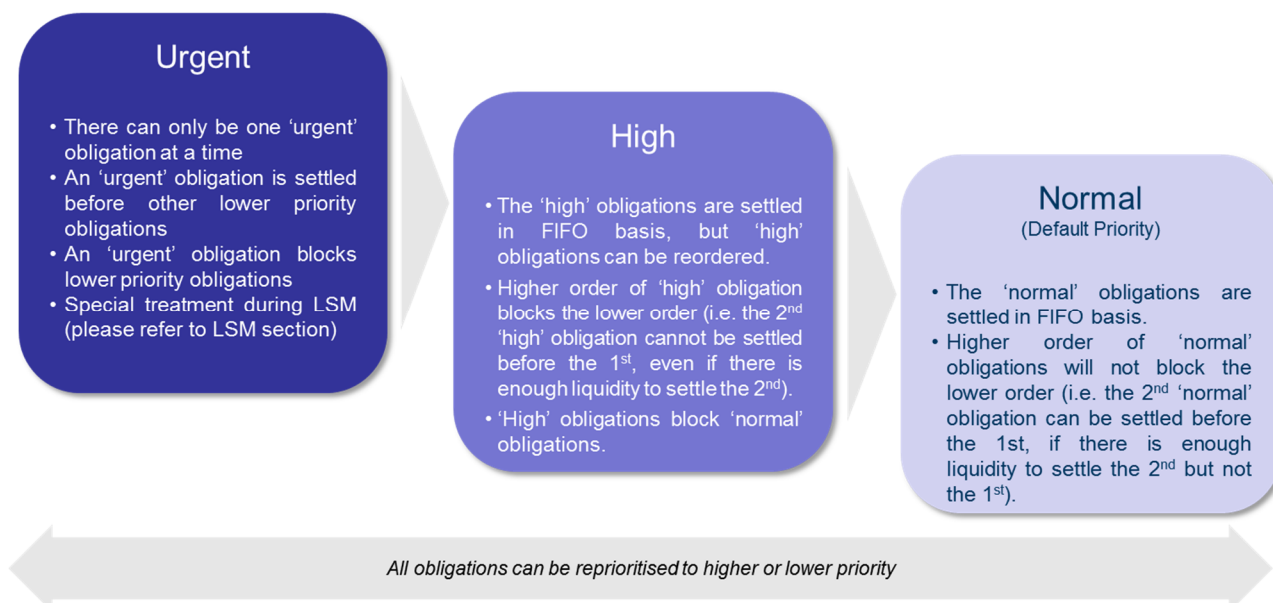
1) LSM oracle node: LSM oracle node's responsibility is to collect information from all nodes in the network, to plan a gridlock resolution if one exists, and then to propose it to parties on the network. Inthanon's design is to have BOT node act as LSM oracle node. Although this creates a point of centralisation and is susceptible to a single-point-of-failure problem, the only functionality that is lost if LSM oracle node becomes offline is an efficiency function (liquidity saving), while the ability to make bilateral payments remains.

Privacy issue in a decentralised GR

In the case of a decentralised GR, any party in the gridlock can initiate the gridlock resolution by requesting the neighbouring nodes to propagate a scan request to obtain available obligations in the outgoing queue. Then, the GR algorithm finds the resolvable netting solution. A gridlock initiator will see transaction details of the obligations. With Corda prototype, details of sender and receiver are anonymised, but not the transaction amount since it is required to figure out the optimal solution for the gridlock.

Revealing the transaction amount and ability to graph the network can lead to a privacy concern. The gridlock initiator is able to deduce the true identities of sender and receiver, although the attempt would be harder if there are many participating nodes involved in the gridlock.

Figure 8: Summary of key features for queue priorities



2) Confidential Identity³ (CI): A confidential identity is generated between the sender and receiver for every transaction in order to protect transaction privacy. It consists of a public key and certificate.

3) Resolution Identity (RI): A resolution identity is introduced in the gridlock resolution as an additional privacy-preservation solution. The RI is used as the identity for the netting payments to ensure that participating nodes cannot deduce the true identities of sender and receiver in the resolution transaction.

4) Well-Known Identity (WI): Generally, the LSM oracle node will not be able to know the true identity based on the CI solely. WI is the necessary key for LSM oracle node to resolve the true identity of the CI. WI is generated and sent by the sending bank together with the obligations.

5) Decentralised Net Payments: Participating bank nodes are responsible for executing net payments instructed by the LSM oracle node in case that a gridlock resolution exists.

Gridlock Resolution Process

The GR process is triggered by BOT node which serves as the LSM oracle node. There are four stages of the GR process: Detect, Plan, Propose, and Execute.

1) Detect

The LSM oracle node instructs all participating bank nodes to provide the following information:

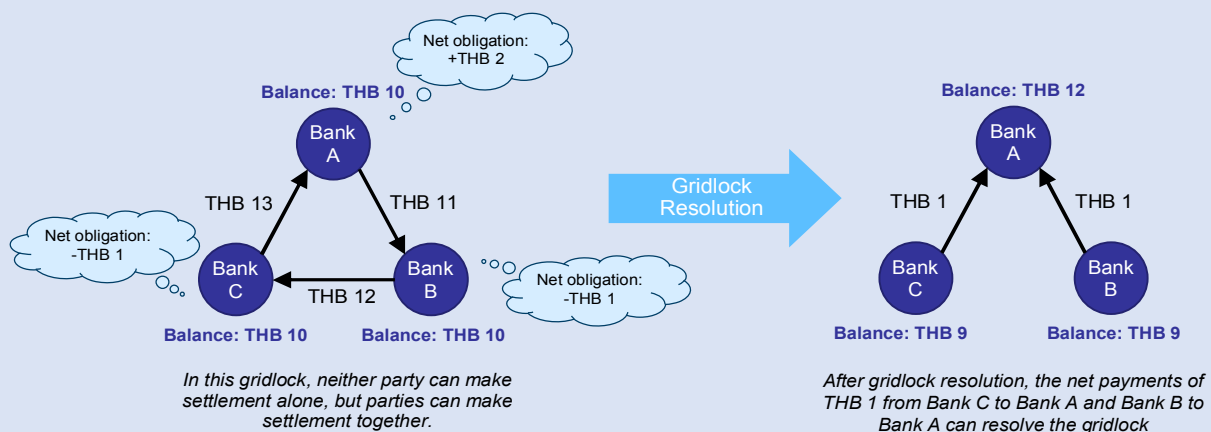
- Obligations with Confidential Identity
 - If the bank node has the 'Urgent' obligation, only 'Urgent' obligation is sent; or
 - If the bank node has no 'Urgent' obligation, the entire outgoing obligations are sent; or
 - If the bank node has no outgoing obligations, no obligation is sent.
- The total amount of cash tokens available
- The cash value of bond tokens available⁴
- Resolution Identity
- Well-Known Identity

The business rationale for adding an 'Urgent' obligation into GR is to give it the highest chance of settling as part of a netting cycle. If other obligations are also sent for solving a gridlock, there is less chance for the 'Urgent' obligation to be settled as part of the netting cycle.

Gridlock and Gridlock Resolution

- **Gridlock** is a group of obligations that cannot settle individually in gross due to insufficient liquidity, but two or more obligations are resolvable with one or more net payments.
- **Gridlock resolution** is an optimisation process to help resolve a gridlock situation. The system searches for a combination of obligations that can be netted, in which these obligations are executed simultaneously.

An example of gridlock and gridlock resolution



³ Refer to Inthanon's Functional Design - Decentralised Bilateral Transfer.

⁴ This cash value of bond tokens is adjusted with haircut.

2) Plan

The LSM oracle node uses the information obtained in Detect stage to derive a network graph of payment obligations by using CI together with WI, to plan the netting solution. In case the gridlock is irresolvable given available cash tokens, the system will trigger ALP process for deadlock resolution (the detail for ALP and LSM algorithm can be found in the ALP for Deadlock section).

3) Propose

The LSM oracle node proposes the netting solution to all involved bank nodes. Then, all involved bank nodes will respond back to the LSM oracle node.

To ensure privacy, the proposed instructions sent between bank nodes and the LSM oracle node in this stage are secured by RI.

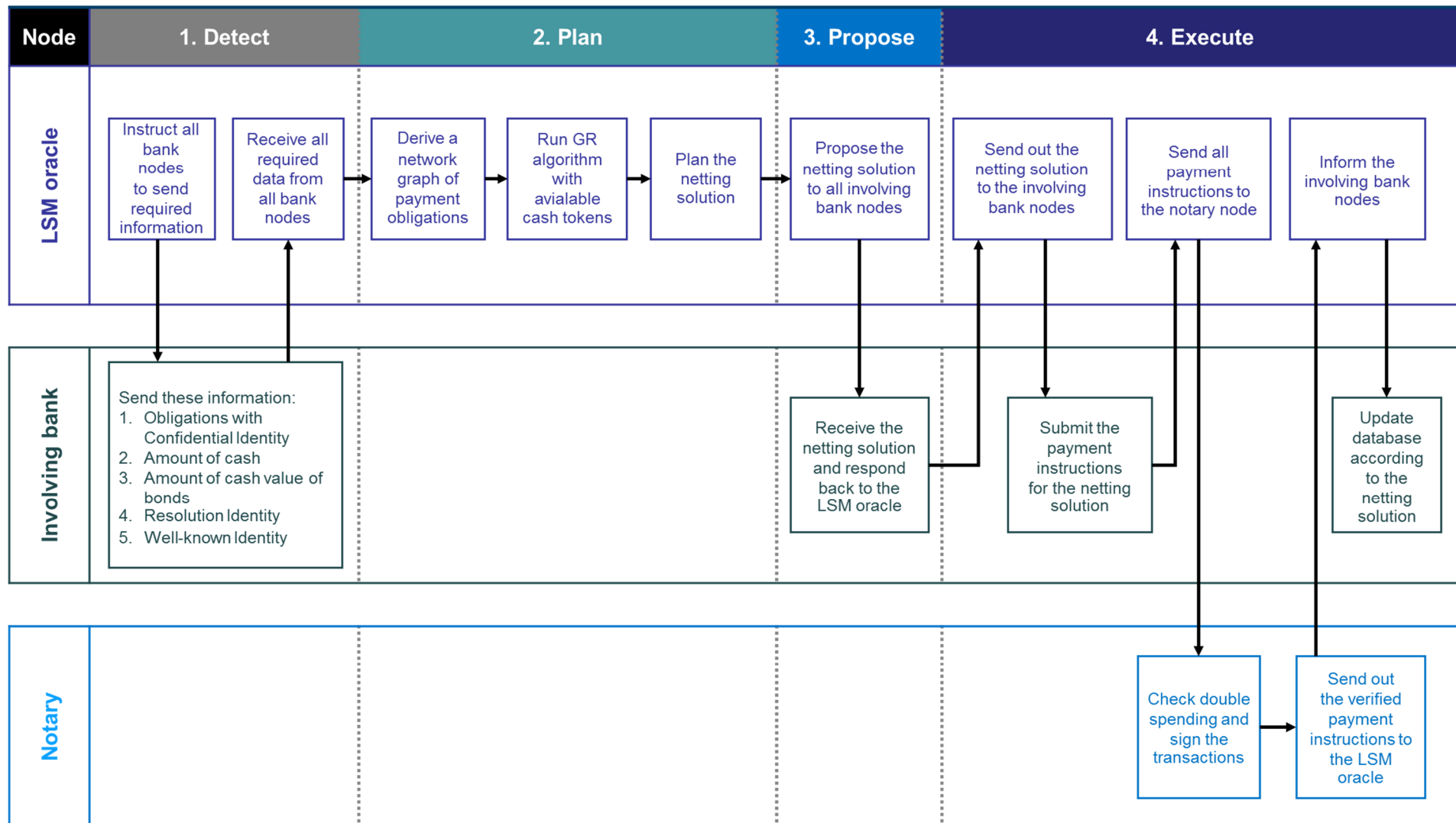
4) Execute

The LSM oracle node sends out the confirmed netting solution to all involved bank nodes. Upon receiving the netting solution, the involved bank nodes will submit the payment instructions for the netting solution to the LSM oracle node. The LSM oracle node then sends all payment instructions to the notary node to check on double-spending and sign these transactions. This is to ensure the finality of the atomic settlements. Then, the notary node will send out the verified payment to the LSM oracle node. In the final step, the LSM oracle node will inform all involved bank nodes to update on their database according to the netting solution.

Table 2: Summary of gridlock design

Project	GR Steps	
	Initiation, detection and planning	Execution (net payments)
Jasper	Centralised (Oracle node)	Centralised (Oracle node)
Inthanon	Centralised (Oracle node)	Decentralised (Involved node)
Ubin	Decentralised (Any node)	Decentralised (Involved node)

Figure 9: Illustration of Inthanon's GR process



3.2.4 Tokenisation of Bond

Banks with liquidity shortage is able to pledge their available assets to obtain additional liquidity. As the result, the concept of bond tokenisation was formed.

Bond tokens are representative of real-world bonds. Bond tokenisation is the process of converting eligible bonds to bond tokens on the DL system. Bond tokens serve as a tool for banks wishing to acquire additional cash tokens by automatically pledging the bonds for a repo with the BOT.

Bond Tokenisation

Currently, each bank holds bonds under BOT's account at TSD for the purpose of settlement and monetary operations. A bank manages its bonds in the BOT's account through BAHTNET system.

To create bond tokens on the DL system, banks have to instruct a bond transfer to a specially created collateral account at BAHTNET system. When the BOT recognises this bond transfer, it simultaneously creates bond tokens in the DL system and sends them to the requesting bank. This process can only be initiated during BAHTNET operating hours.

Bond Detokenisation

Banks can choose to detokenise the bond tokens in the DL system into the real-world bonds. This is a reversal of the bond tokenisation process. A participating bank who wishes to convert bond tokens on the DL system to real-world bonds sends a detokenisation request to the BOT. Then, the BOT approves the detokenisation request and transfer bond from the omnibus collateral account to the requesting bank's securities account in BAHTNET.

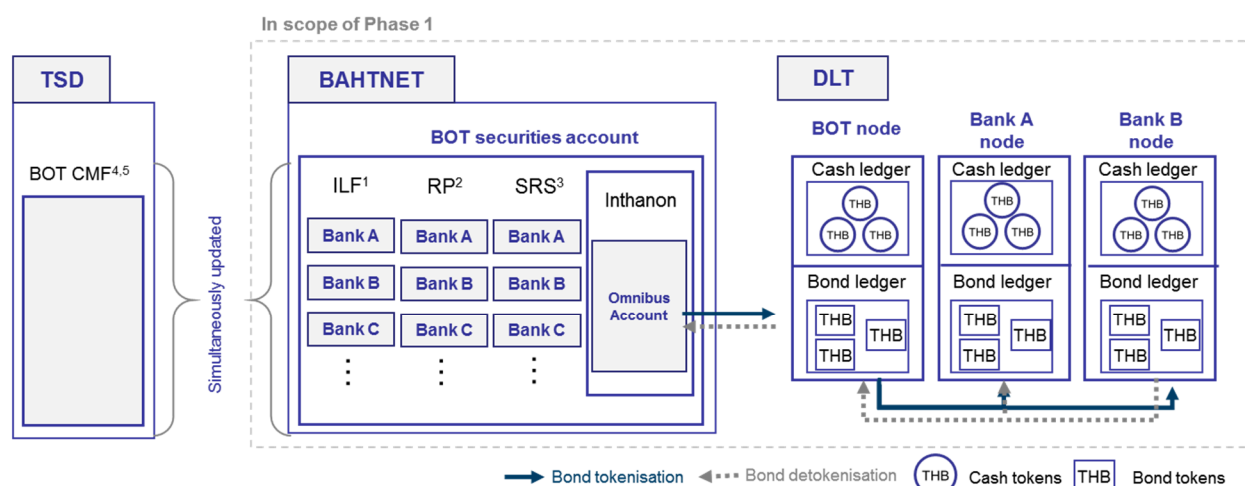
3.2.5 Automated Liquidity Provision

ALP is introduced in this project in order to increase efficiency of bond usages and to ensure that the transactions can be settled according to business needs.

Business Rationale of Automated Liquidity Provision

In current BAHTNET system, the BOT provides liquidity through ILF to banks for facilitating payment settlement. Banks are required to hold minimum eligible bonds to satisfy regulatory requirement for the ILF. As a result, there is an opportunity cost presented for the small banks who holds fewer eligible bonds in comparison to the large banks.

Figure 10: Illustration of bond tokenisation and detokenisation process



- ¹ Intraday Liquidity Facility, the securities account that provides participants intraday liquidity against eligible collaterals to support liquidity management.
² Repo, securities account for BOT's end-of-day lending facility
³ Securities Requirement for Settlement, the securities account to mitigate settlement risks resulting from net settlements.
⁴ Collateral management facilities account belongs to BOT. It is an omnibus account which BOT hold securities on behalf of the member banks.
⁵ Bonds in BOT CMF equal to sum of Bonds in ILF, RP, SRS and Inthanon in BAHTNET.

At the beginning of the day, banks obtain liquidity from repo transactions with the BOT. Due to abundant liquidity in the banking system, the RTGS runs smoothly and gridlock resolution mechanism is rarely used. Inthanon's proof-of-concept explored the alternative process called ALP to optimise the bonds used for obtaining intraday liquidity. The design of ALP is built upon the key capabilities of DLT: tokenisation and atomicity.

ALP Functionalities

ALP is the function which automatically injects additional liquidity for clearing outgoing obligations with an optimised use of bond tokens. The transaction under the ALP is conducted in the form of repo contract between a participating bank requiring liquidity and the BOT using tokenised bonds as collaterals. ALP serves two main roles:

1. Allowing banks to acquire on-demand liquidity automatically: this is to experiment liquidity injection to the payment system without the central bank manual intervention.

2. Enhancing efficiency of collateral usage for liquidity provision: ALP is designed to use bond tokens on a just enough basis. This would reduce opportunity cost of holding bonds in their ILF accounts and over pledging collateral for intraday liquidity.

ALP Process

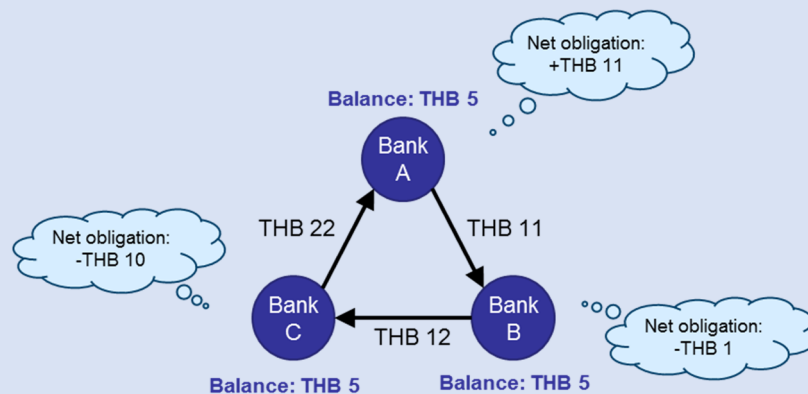
ALP can be triggered in two scenarios:

1. A bank has 'Urgent' obligation that is stuck for a certain period of time due to insufficient cash tokens.
2. The GR algorithm could not find a netting solution given available cash tokens (deadlock situation).

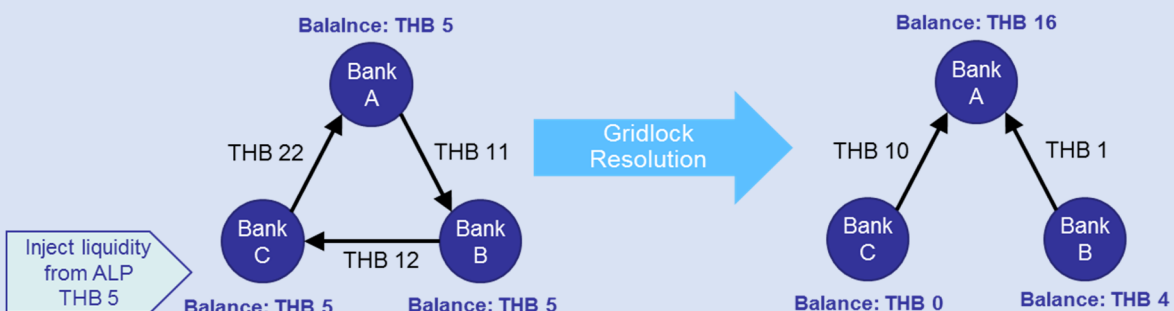
What is deadlock?

Deadlock arises when netting solution cannot be found by GR algorithm. In other words, a potential netting solution results in a negative net liquidity across of any participants unless additional liquidity is provided.

Example of a deadlock: neither party can make settlement individually, nor on the net basis. A deadlock requires injection of liquidity to resolve.



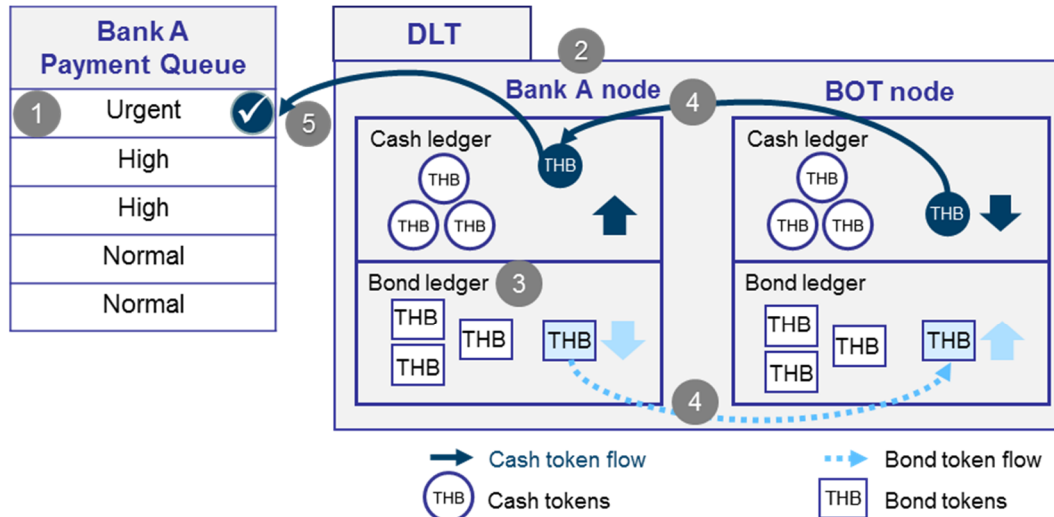
Example of a deadlock resolution: ALP inject liquidity so that all parties can make settlement.



1) ALP for Urgent Payment Obligation

'Urgent' is the highest priority of payment obligation which must be settled as soon as possible. If 'Urgent' payment obligation has been in the queue for a certain period of time, the ALP mechanism is triggered following these steps:

Figure 11: Illustration of automated liquidity provision for 'Urgent' payment obligation



- 1 Bank A's 'Urgent' payment obligation is stuck in outgoing queue for more than a certain period of time
 - 2 ALP is triggered. Bank A node calculates:
 - Shortfall amount of cash tokens sufficient to settle 'Urgent' payment obligation
 - Amount of bond tokens need to be converted to match the shortfall amount of cash tokens. Haircut rate and market prices are applied for the calculation.
 - 3 Bank A node checks the amount of bond tokens in its bond ledger
 - If there is insufficient bond tokens, no ALP is processed. Bank A node will repeat Step 2 for every certain period of time configured by ALP scheduler.
 - Otherwise, proceed to Step 4.
 - 4 Bank A enters a repo agreement with the BOT by transferring bond tokens from Bank A node to BOT node (first-leg repo). In return, Bank A node is credited with cash tokens from BOT node. The atomicity of the exchange between cash tokens and bond tokens is ensured and notarised by the notary node.
 - 5 With newly injected liquidity, Bank A node has sufficient cash tokens to settle 'Urgent' payment obligation.
- Once Bank A node acquires additional cash tokens sufficient to repay BOT node, Bank A node can manually close the repo and the process in Step 4 is reversed (second-leg repo). Penalties and interest charges for closing the repo after end-of-day, as well as partial buybacks are out of scope for Phase I proof-of-concept.

2) ALP for Deadlock

During the Plan stage of the GR process, when LSM oracle node detects a deadlock which can be resolved with additional liquidity, the ALP process is triggered following these steps:

Figure 12: Illustration of automated liquidity provision for deadlock

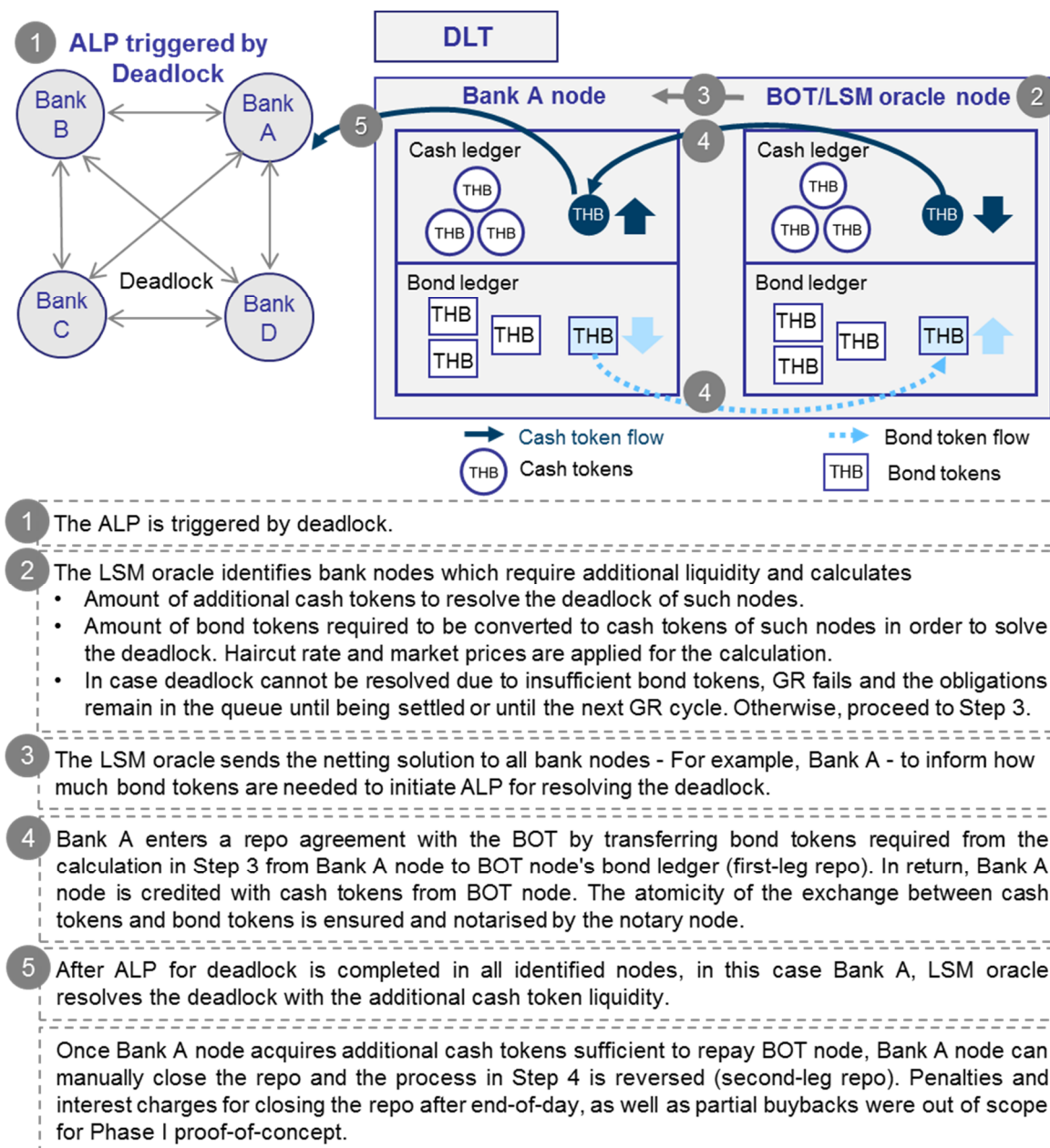
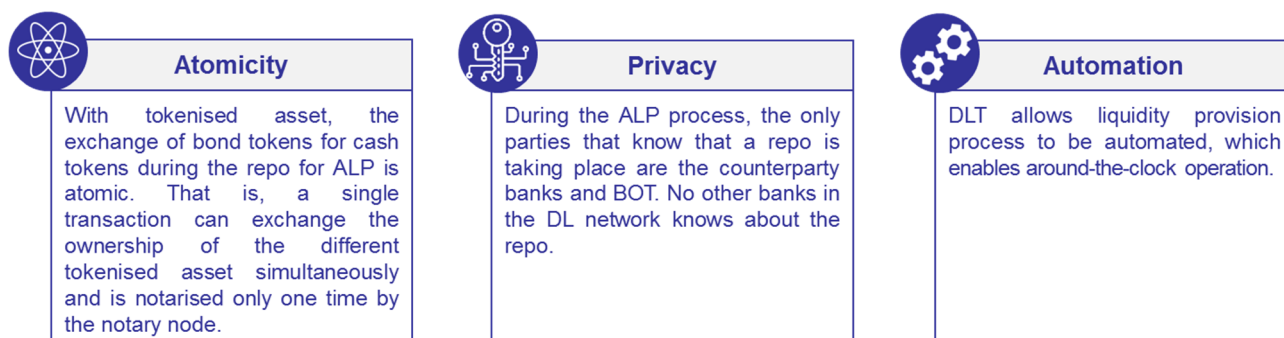


Figure 13: Key characteristics in the Inthanon's ALP



04 Phase I Key Findings

4.1 Findings from Inthanon's Project Approach

Throughout Project Inthanon, technical and business professionals from the BOT and the eight participating banks collaborated during design thinking workshops to define pain points, design solutions, and deliver the proof-of-concept.

By collaboratively discussing user journeys, problems were identified and discussed from both functional and non-functional perspectives. As a result of the problem-driven approach, the output of the workshops were 47 user stories for the functional designs. The user stories were divided into 4 sprints. Leveraging on the agile approach, development work was done at the beginning of each sprint and followed by functionality testing. With the contribution from the banks' developers, the proof-of-concept was successfully delivered within the 13-week timeframe.

This approach enabled participants to have a well-rounded view of the processes around RTGS. There was also a cross-organisational knowledge sharing and discussing on best practices that could be taken back to enhance their in-house operations.

Phase I proof-of-concept was built by Inthanon team including business subject matter experts and developers from the BOT and participating banks. Therefore, a solid insight into the fundamentals of decentralised payment system has been built up among a population of technical and operational professionals.

This project also helped the participants gain a better understanding of how DLT works and gave a clue into the future potential of how it could be adopted in Thailand.

4.2 Findings from the Proof-of-Concept

With Phase I proof-of-concept successfully delivered, key findings from both functionalities and non-functionalities were raised and specified by the project participants.

4.2.1 Functional Findings

Phase I proof-of-concept demonstrated DLT capabilities of achieving not only key payments functionalities existing in RTGS such as bilateral transfers and LSM, but also the automated liquidity provision using bond tokens. This highlighted the three key capabilities of DLT which show potentials for increasing flexibility of the RTGS:

1) *Tokenisation of Multiple Assets*

In Phase I, cash and bonds were tokenised, recorded and transacted on the same platform. This made the proof-of-concept particularly different from traditional single-asset based payment platforms.

2) *Atomicity of Delivery versus Payment (Atomicity of DvP)*

The proof-of-concept showed that asset tokens could be created and exchanged against one another simultaneously. This atomic DvP has potential to improve efficiency as settlement process can be simplified and intermediaries are no longer required.

3) *Around-the-Clock Operations*

Under the DL system, banks can settle in cash tokens around the clock and facilitate business during off-hours. This helps reduce the interbank credit risk that builds up during off BAHTNET operating hours.

4.2.2 Non-functional Findings

1) *Settlement Finality*

Settlement finality is the point in time at which an asset is considered to change ownership. Once a transaction is completed, the transfer must be irrevocable. Different DLT platforms differ in their approach to this. Some blockchain platforms with proof-of-work consensus mechanism (e.g. Bitcoin) never provide settlement finality, which makes settlement probabilistic rather than deterministic.

The proof-of-concept was able to provide the deterministic settlement finality by leveraging the notary service in Corda platform. In Corda, the notary service functioned to commit to settlement finality and irrevocability by providing a signature for any transaction. Upon receipt of

the notary signature, participants of the transaction were informed of the settlement, and the transactions were committed on the ledgers. The payment then became technically irrevocable.

2) Privacy

As mentioned earlier, there is a natural tradeoff between the decentralisation and privacy. However, DLT platforms differ in terms of privacy layer which it provides to participants such as data availability and accessibility. According to the previous projects of other central banks, the decentralised payments and privacy could be achieved. However, in a fully decentralised RTGS, privacy concern especially during LSM process remained a challenge.

Phase I proof-of-concept's design was effectively developed to ensure that privacy would not be compromised in any payment activities including the LSM process. Findings on privacy can be divided into two main parts, namely transaction privacy and LSM privacy.

- **Transaction privacy:** Given the Corda's approach, the proof-of-concept could ensure that the transactional information was sent and shared on a need-to-know basis and not to a whole global ledger as is the case with traditional blockchain platforms.

The notary provides a signature that attests that a token has not been already spent. However, it sees only a transaction identifier of the tokens which are being spent (a previous transaction hash and index number plus a Merkle tree⁵ of the transaction), without seeing the contents of those transactions. Therefore, while the notary service knows if a token has been spent or not, it does not know what the token represents, nor the sender, receiver, amounts, or even the asset type being transacted.

- **LSM privacy:** Project Inthanon considered various LSM models and ended up building a novel solution. In the proof-of-concept, privacy was completely safeguarded during the LSM process. By achieving this, the LSM oracle node and resolution identity features were built in the design to address the trade-offs between privacy and single-point-of-failure problem. As such, payment obligations were not shared to

unrelated parties unlike the decentralised LSM process⁶.

3) Resiliency

It is often noted that a DLT-based system offers higher resiliency than a traditional centralised system with a central server. For Project Inthanon, two types of resiliency were considered.

- **Data resiliency:** A traditional 'public' blockchain with a replicated ledger is resilient to data failures on any specific node. If any node loses all of its data, it can request an entire copy of the whole ledger from any of its neighbours. However, due to the privacy issues surrounding traditional blockchain platforms, Corda does not replicate all data to all parties, so each participating bank node and notary node must be responsible for its own data. In the proof-of-concept, control points were set during the workflows which automatically saved transaction details. In the case any node was down and then recovered, data could be resumed, and the transaction could continue.

- **Network resiliency:** For Phase I, the single notary model was chosen for the proof-of-concept, which constituted to a single-point-of-failure problem since the notary is necessary for settling transactions and ensuring settlement finality. Different results for each scenario are outlined below:

1) Bilateral transfers: if the notary failed, a transaction could not be settled. However, if one of the participating nodes failed, other active nodes could still continue their payment transfers between one another.

2) ALP: both BOT and the notary were critical components for ALP process. If BOT failed, ALP process could not be initiated. Whereas when the notary node failed, ALP transaction could not be settled.

3) GR: LSM oracle node, the notary node and the bank nodes were critical components for GR process. The results of different scenarios are summarised in *Table 3*.

⁵ A Merkle tree is a well-known cryptographic scheme that is commonly used to provide proofs of inclusion and data integrity. Merkle trees are widely used in peer-to-peer networks and blockchain systems.

⁶ Privacy for a decentralised system can be improved with the hardware-based privacy solutions. More information can be found in the Appendix.

Table 3: Summary of results from resiliency test during the GR process under different scenarios.

Down node	<u>Before GR initiated</u>	<u>During GR operates</u>
LSM oracle	GR could not be initiated. Bilateral transfers can be settled.	GR was paused until LSM oracle node resumed. Involved banks nodes became inactive.
Notary	GR could run, but netting solution could not be settled until the notary node resumed.	
Any banks	GR was paused at the Detect stage until the down node resumed.	GR failed.

Potential solutions and designs can be considered for the future phases to address the resiliency issue. For example, the multiple notary model and high availability of the notary and LSM oracle nodes can be implemented to mitigate the risk of a single-point-of-failure. In addition, time-out or cancellation mechanism can be added so that the active node can resume normal operations.

The chapter lays out Phase I key findings from both functional and non-functional aspects, which could be utilised in the next phases of Project Inthanon or become part of contribution for other payment projects including the next-generation of BAHTNET.

05 Next Steps and Future Works

As Phase I proof-of-concept already built, there are a number of areas including the readiness of financial industry and the complexity of deployment, that need to be explored to move the proof-of-concept towards a full production-grade system. Some non-exhaustive suggestions for future work are outlined below, although their inclusion does not constitute a commitment from the project to deliver them in future phases.

5.1 Technical and Functional Features Build-outs

1) Resiliency

The notary in Phase I was implemented as a single non-validating notary node, which represents a single-point-of-failure. A more resilient notary cluster could be designed and implemented as a Byzantine Fault Tolerant or other technique. The most appropriate consensus mechanism would need to be determined, as would the governance and ownership of the individual notary nodes.

2) Scalability

Phase I was built on Corda's open-source version, thus evaluating scalability of the system was not in the scope of Phase I proof-of-concept. However, as the technology develops and newer versions of DLT platforms are available, future work can include scalability by conducting a full end-to-end test for transaction throughput. In addition, in order to expand accessibility and increase a number of nodes in the system, the technical perspective of total number of nodes will also need to be assessed since some consensus algorithm's performance will degrade as the number of nodes increase. Moreover, from the cost-efficiency perspective, small participants may not be able to host their own nodes, thus a concept of proxy node or shared node may need to be explored.

3) GR Efficiency

A further study could be conducted with real payments data to discover the optimum time interval to run the GR.

4) Bond Lifecycle and More Token Types

Inthanon's proof-of-concept included tokens representing Thai government bonds with no life-cycle events. As a future step, tokens representing a wider range of bonds and other financial assets could be modelled, along with their range of life-cycle events. Moreover, bond prices for the bond tokens in the proof-of-concept were fixed, whereas bond prices should be updated automatically and in real-time whenever bond repurchase is initiated for ALP. Thus, a real-time data feeding from reliable sources should interface with the new system for bond repo calculations. Penalties for late delivery of the far leg of the repo transaction were not incorporated in the proof-of-concept and would need to be designed and modelled in future work.

5) Net Payments Arising from External Systems

The proof-of-concept in Phase I was not interoperable with other external net payment systems particularly Multilateral Fund Transfer (MFT), which is one of the critical services in the payment system. As a result, if the decentralised RTGS is aimed to be operationalised, this capability of such system to support these services must be ensured.

6) Cross-border Payments

With regard to currencies, Inthanon addressed only THB cash tokens issued by the BOT for domestic interbank payments. An obvious next step would be to explore cross border payments, both in THB and foreign currencies, to enhance operational efficiency. This potentially requires linkage or interoperability with other national payment systems.

5.2 Legal and Regulatory Considerations

Some key legal considerations should be further explored.

- **Legal status of THB tokens:** in case there is a policy to certify THB tokens as a legal tender, the Currency Act will need to be revisited.
- **Regulatory treatment on central bank-issued cash tokens:** this has to be clarified whether it could be treated as same as reserve money or physical banknotes since it may have implications on the liquidity regulatory compliance such as reserve requirements or liquidity coverage ratio.

- **Settlement finality:** this has to be clearly defined in both operational and legal aspect before pushing the proof-of-concept towards a production-grade system.

- **Highly Important Payment System:** in case the system falls under the characteristics of Highly Important Payment System under the Payment System Act, several relevant issues must be considered, including security standard of the system and the supervisory role of BOT.

5.3 Operational Considerations

Around-the-clock Operations

The Inthanon Phase I model explored and enabled 24/7 interbank payments in central bank-issued cash tokens with finality. Some operational issues regarding the around-the-clock operations would arise. These include:

- **Adjusting banks' operational procedures to support 24/7 features:** Around-the-clock operation would allow transactions to be made during off-operating hours. Therefore, this will have an impact on banks operational procedures in various aspects such as cash tokens and bond tokens management, customer handling etc. For example, with ALP, bond tokens might be automatically repurchased to support a payment during off hours, thus banks would need to add monitoring to ensure that they have sufficient liquidity for the repurchase leg of the repos and mitigate the associated risks.

- **Determining cut-off periods for ALP interest rate charged:** In a 24/7 system with no 'overnight' period, a snapshot would need to be taken at a particular point in time for the calculation of interest, or perhaps interest could be calculated and charged on a more granular basis, for example, hourly.

Roles of the Central Bank

In the decentralised RTGS, the traditional role of central banks as a monopoly supplier of liquidity shall remain unchanged. However, given the current design of the proof-of-concept, certain roles of central bank would be different or added.

- **As a notary:** instead of being a central operator, the central bank will act as a notary to prevent double-spending.

- **As a payment system regulator:** There is a natural governance role for the central bank to take a leading role in establishing and ensuring good governance.

5.4 Looking forward to Phase II

Phase II of Inthanon will have triple aims:

- 1) Modelling lifecycle of bond tokens, Bond DvP and Interbank Repo.
- 2) Exploring DLT for regulatory compliance related to third-party initiated interbank fund transfers.
- 3) Investigating DLT for improving transaction safety and the detection of certain types of financial fraud.

Lifecycle of bond tokens, Bond DvP and Interbank Repo

To leverage the bond tokens introduced in Phase I, Phase II aims for modelling lifecycle of bond tokens including coupon payments, inter-bank trading (DvP) and their final redemption. Interbank repos with bond tokens will also be explored.

Regulatory Compliance

Non-Thai residents having Thai Baht account opened with banks in Thailand are subjected to regulatory compliance; for example, a cap of 300 million baht at the end of the day per non-Thai resident across accounts hold within the Thai banking system.

This issue was major pain point identified by participants in Phase I and proposed to be a key area for exploration in Phase II.

Fraud Detection and Prevention

Currently, certain types of fraud are difficult for banks to detect before fraudulent payments have been made. Phase II will look at implementing a solution for these types of fraud that will work on a DLT-based system.

06 Conclusion

The Phase I proof-of-concept was successfully built by BOT, the eight participating banks and the technology partner, R3. The trainings and technical support received had promoted an educational collaboration between stakeholders. Design thinking technique which involved interviews, questionnaires and workshop sessions with the subject matter experts from the BOT and the banks enabled them to share their insights. This contributed to the development of user stories with enriched key payment functionalities for the proof-of-concept, which included cash tokenisation, queueing mechanisms, gridlock resolution mechanisms, bond tokenisation and automated liquidity provision.

With strategic collaboration among the stakeholders throughout the project, Phase I proof-of-concept demonstrated the potential of DLT for payment system adoption. From the design and development process to the integration and testing of the proof-of-concept, all relevant stakeholders were involved and held accountable for the successful delivery of the project's two main outcomes: 1) the proof-of-concept which reaffirmed DLT's potentials for payment system development and 2) collaborative learning outcome that helps enhancing technological knowledge and capability for the key financial market players.

Looking forward to the future phases, Project Inthanon is looking to test DLT's capabilities for other more complex payment functionalities. Based on the findings from Phase I proof-of-concept, Phase II will explore the application of DLT in the areas of bond tokens lifecycle, regulatory requirements related to non-residents, and fraud detection and prevention. For Phase III, the interoperability with the legacy system and other platforms will be experimented on both domestic and cross-border levels.

Project Inthanon Phase I has proven that it has not only raised the awareness of the disruptive technology among project participants, but also helped accelerate the technological capability and readiness of Thai financial system, which would be beneficial the Thai financial system development in the long run.

07 Glossary

Term	Description
ALP	Automated Liquidity Provisioning - the automatic repo of available bond tokens for cash tokens provided by BOT
API	Application Programming Interface
BAHTNET	The Bank of Thailand Automated High Value Transfer Network. Thailand's real time gross settlement system. ⁷
BOT	Bank of Thailand
CBDC	Central Bank Digital Currency
DLT	Distributed Ledger Technology
DvP	Delivery versus Payment
GR	Gridlock Resolution
ILF	Intraday Liquidity Facility
LSM	Liquidity Saving Mechanism
RTGS	Real Time Gross Settlement system
SME	Subject Matter Expert
THB	Thai Baht
TSD	Thai Securities Depository
Bond tokens	Tokens recorded on Corda that represent a claim on specific bonds held in custody by the BOT at the TSD
Cash tokens	Tokens recorded on Corda that represent a claim on an equivalent balance in BOT's collateral account at BAHTNET
Deadlock	Deadlock arises when a potential netting solution results in a negative net liquidity across of any participants, and so no resolution is possible unless additional liquidity is provided by one or more of the participants.
Gridlock	Gridlock is a formation of queues that can fulfil the requirement for payments to be settled individually.
Haircut	Discount applied by the buyer of repo on price of security which accounts for volatility in prices and opportunity costs that are related to the cash being given to the seller of the security.
Netting	When two parties (e.g. bank nodes) owe each other money, netting is the process of calculating a single payment that will satisfy the individual payments.
Repo	A sale-and-repurchase agreement. In Inthanon's case, the BOT is the lender of cash against assets provided by banks.

⁷ See <https://www.bot.or.th/English/PaymentSystems/PSServices/bahtnet/Pages/default.aspx>

08 Appendix

8.1 Improving privacy of a decentralised LSM

(contributed by Bangkok Bank PCL)

R3 is exploring Intel Software Guard Extensions (SGX) which are secure enclaves in hardware chips. SGX provides a way to offload sensitive data processing to remote untrusted machines in such a way that the operator of the hardware is unable to decrypt the data they are sent, but the data can still be calculated upon. Intel SGX would enhance privacy within the platform and could be a way to improve our privacy of a decentralised LSM.

SGX could help us delegate a job processing to the protected environment, called enclaves, in the CPU. The huge benefit from SGX is the protected environment to compute on private, encrypted data without revealing that data to the owner of the hardware. Consequently, SGX capable nodes can be used to establish an authenticated communication channel with each other by trusting in their enclave. Intel named this feature Remote Attestation (RA). RA can be used to exchange, and compute sensitive data then reveal only the result, but not the input, to the hardware owner.

Figure 14: Application partitioning (Image source: Intel⁸)

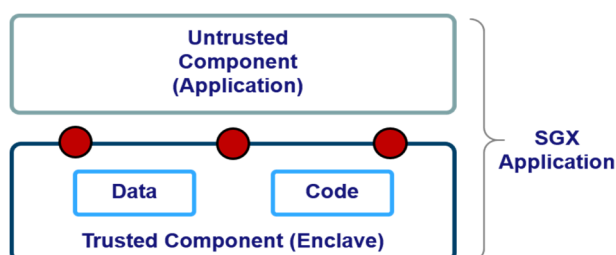
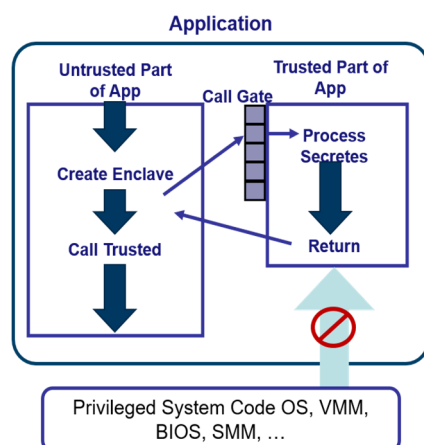


Figure 15: Runtime execution (Image source: Intel⁹)



Intel SGX opens up the possibility for more flexible application designs with less privacy exposure probability to Corda, possibly allowing a more fully decentralised LSM without sacrificing transactional privacy.

⁸ <https://software.intel.com/en-us/sgx/details>

⁹ <https://software.intel.com/en-us/sgx/details>

8.2 Gridlock Resolution Algorithms

The LSM algorithm aims to find a solution yielding highest obligations sum and number of urgent transactions. In case there are more than one solution yielding the same amount of highest obligations sum and number of urgent transactions, the algorithm will pick the first solution it found. Due to the fact that LSM algorithm applies both deterministic and probabilistic approach for speed of solving, the netting results may not be the global maximum obligation sum, particularly when there are large number of obligations in the queue.

There are five approaches for gridlock resolution in the proof-of-concept. Examples of each approach are described below.

Just

This is a deterministic approach to remove the outgoing obligation which is just enough to make the position become positive from the node having biggest negative position; or if there are no such obligations, remove the largest obligation.

1. Select the bank with the largest negative value in the ending position
2. Remove the outgoing transaction of the bank so that the value of ending position can be
 - a. Equal to 0, if not
 - b. Positive and closest to 0, if not
 - c. Negative and closest to 0
3. Repeat (1) until all values of ending position are non-negative

Greedy

This is a deterministic approach to remove the largest outgoing obligation from the node having biggest negative position.

1. Select the bank with the largest negative value in the ending position
2. Remove the largest amount of outgoing transactions of the bank
3. Repeat (1) until all values of ending position are non-negative

Random

This is a probabilistic approach to randomly choose any obligation.

1. Select the bank with the largest negative value in the ending position
2. Remove the outgoing transaction of the bank
3. Repeat (1) until all values of ending position are non-negative

Positive Random

This is a probabilistic approach to choose randomly among the obligations which can make the position become positive alone; or if there are no such obligations, choose the largest obligation.

1. Select the bank with the largest negative value in the ending position
2. Remove the outgoing transaction of the bank so that the value of ending position can be non-negative
3. Repeat (1) until all values of ending position are non-negative

Positive Counterparty Random

This is a probabilistic approach to choose the obligation which is paying to parties with positive position; or if there are no such obligations, choose random obligation.

1. Select the bank with the largest negative value in the ending position
2. Remove the outgoing transaction of the bank sending to a bank with non-negative value of ending position
3. Repeat (1) until all values of ending position are non-negative

09 Acknowledgements

Steering Committee

Name	Organisation
Vachira Arromdee	Bank of Thailand
Kukkong Ruckphaopunt	Bangkok Bank Public Company Limited
Boonlerd Sinsombat	Krung Thai Bank Public Company Limited
Voranuch Dejakaisaya	Bank of Ayudhya Public Company Limited
Silawat Santivisat	Kasikornbank Public Company Limited
Pimolpa Suntichok	Siam Commercial Bank Public Company Limited
Sutut Chitmonkongsuk	Thanachart Bank Public Company Limited
Parnkae Nandavisai	Standard Chartered Bank (Thai) Public Company Limited
Ai Chen Lim	The Hongkong and Shanghai Banking Corporation Limited

Project Management Team

R3

Name	Role
Aaron Seabrook	Project Director
Antony Lewis	Director of Research
Ben Tan	Solution Engineer

Wipro

Name	Role
Welawan Chansupat	Senior Business Development Manager
Chetan Ghadge	Domain Consultant - Financial Services
Harihara Subramanian	Domain Consultant - Financial Services
Anoop V Mathew	Domain Consultant - Financial Services
Pallavi Thakur	Subject Matter Advisor - Blockchain
Ashish Sinha	Architect - Blockchain
Hitarshi M Buch	COE Head - Blockchain
Srinivasan Sankaran	Developer - Blockchain
Divya Taori	Developer - Blockchain
Purnima Agrawal	Developer - Blockchain
Pranay Gandhi	Developer - Blockchain
Manish Sharma	Development Lead - UI

Chappuis Halder & Co.

Name	Role
Karnrawee Archavaditchai	Project Manager
Laurent Liotard-Vogt	Functional Project Manager
Guillaume Rico	Payment SME
Erynn Lee	Report Author
Cynthia Han	Report Author

Participating Banks

Bangkok Bank Public Company Limited

Name	Role
Pongbhoka Buddhi-baedlya	Business SME
Choopong Tanaphongsatorn	Business SME
Phusamita Charoenwattanaphokaew	Business SME
Sumeena Visavakul	Technical SME
Somboon Chiewcharnpipat	Technical SME
Suda Ua-areeesuksamarn	Technical SME
Thanapon Leelasethakoon	Developer

Krung Thai Bank Public Company Limited

Name	Role
Thanasak Wiradakun	Business SME
Jakkrit Klinsmith	Technical SME
Ohm Samkoses	Technical SME
Pornthep Prungarvut	Legal SME

Bank of Ayudhya Public Company Limited

Name	Role
Wirote Chuenratanakul	Business SME
Pongsit Vilailert	Business SME
Napawan Chiraporncharoensuk	Business SME
Sasin Phitsanuphan	Technical SME
Boonthep Techarungruangkit	Technical SME
Natpong Keadsem	Developer

Kasikornbank Public Company Limited

Name	Role
Manaviga Pinthongkham	Business SME
Suphot Butsarawong	Business SME
Sophit Visitkitjakarn	Business SME
Chatnapang Wuthiwatana	Business SME
Samanun Chotkiatikhun	Developer
Phootsadee Hongchinda	Developer

Siam Commercial Bank Public Company Limited

Name	Role
Nartruedi Punyaratabandhu	Business SME
Pratarnporn Viranuvatti	Business SME
Worapat Pilungasa	Business SME
Peerapon Suradaroonsri	Business SME
Chitchanok Thongsanga	Technical SME
Supatporn Kennedy	Developer

Thanachart Bank Public Company Limited

Name	Role
Apinya Assavavipas	Business SME
Ganikar Lertphuwong	Business SME
Malee Jongpaisalsakul	Business SME
Kaewkal Rajavallabhanusith	Technical SME
Patsakorn Rittitum	Developer

Standard Chartered Bank (Thai) Public Company Limited

Name	Role
Aramsri Choowongse	Business SME

The Hongkong and Shanghai Banking Corporation Limited

Name	Role
Prateek Dayal	Business SME
Anupong Troranison	Business SME
Saowaluck Boonmahanark	Business SME
Siripen Payubyupapong	Business SME
Adisorn Tanthaworn	Technical SME
Kwok Ching Tsui	Technical SME
York Tsang	Developer

Bank of Thailand

Name	Role
Mathee Supapongse	Project Chairman
Vachira Arromdee	Project Executive
Chantavarn Sucharitakul	Senior Advisor
Titanun Mallikamas	Senior Advisor
Amporn Sangmanee	Project Manager
Chayawadee Chai-anant	Project Advisor / Project Coordinator
Thammarak Moenjak	Project Advisor / Project Coordinator
Nidchanard Phulsanong	Project Advisor / Project Coordinator
Chananun Supadulya	Product Owner / Project Coordinator
Nuttathum Chutasripanich	Product Owner / Project Coordinator
Kasidit Tansanguan	Product Owner / Project Coordinator
Uraipun Boriruktungkul	Product Owner (Payment)
Pisak Kurusathian	Product Owner (IT)
Tuln Sermsiriviboon	Business Solution Design
Tansaya Kunaratskul	Business Solution Design
Premmanat Kanchanawila	Business Solution Design
Wuthinan Bangjing	Payment SME
Kanyarat Silakong	Payment SME
Nuntapun Bhensook	Payment SME
Worapol Tangkokiattikul	IT SME
Supagan Pulprapan	IT SME
Apichai Dokmai	IT SME
Ploypan Phrukampai	IT SME
Wasna Nimityongskul	Project Advisor
Ed Yampratoom	Project Advisor
Vanaporn Laksanasut	Project Advisor
Suchot Piamchol	Project Advisor
Pensiri Wangdan	Project Advisor
Bongkoj Isara	Project Advisor
Tuangporn Khawcharoenporn	Project Advisor
Bangonsri Rujiwasin	Project Advisor
Pumthan Chaichantipyuth	Project Advisor
Tippawan Teerathanon	Project Advisor
Aunshulee Horsombat	Project Advisor





Inthanon National Park, Chiang Mai

Disclaimer: This article, analysis, or research has been jointly conducted by the Bank of Thailand (BOT) together with eight participating banks in Project Inthanon for informational purposes only. The information used in this report is obtained from trustworthy sources. However, the BOT does not guarantee the completeness and accuracy of data provided in this report, and hence shall not be responsible nor accountable for any use, replication, or interpretation therein of the data, text, or views expressed in this report. The BOT retains the sole intellectual property of this report and reserves copyright of the information within this report. The reproduction, adaption, or public dissemination of the whole report or parts of it for commercial purposes is strictly prohibited unless written authorization from the BOT and the eight participating banks have been agreed and provided in advance.

Replication, quotation, or reference to any part of this report in articles, reports, or any other form of communication shall be conducted accurately without causing any misunderstanding or damage to the BOT and the eight participating banks and must acknowledge copyright ownership of the data to the BOT. The views expressed in this report are our own and do not represent those of the BOT or the eight participating banks. All errors are ours.