SCG

BANK OF THAILAND

DIGITAL VENTURES

Central Bank Digital Currency: The Future of Payments for Corporates

Leveraging Technology to Enhance Efficiency and Innovation in the Business Sector

Powered by

CONSENSYS

FOREWORD

In the belief that technology will bring unprecedented and impactful changes to society, the Bank of Thailand (BOT) sets a vision to pursue and facilitate the transformation of the Thai economy towards a digital era in which a safe and efficient payment system is a crucial component. Project Inthanon is one of the key initiatives in which the BOT explores the potential of Distributed Ledger Technology (DLT) in developing a digital currency, transforming the financial infrastructure, and fostering the ecosystem to digitally innovate. Beginning in August 2020, the BOT made a prominent step in the pursuit of this vision by expanding the scope of Project Inthanon, originally focused on interbank payments, to bring benefits to and support innovation in business sectors. The BOT together with the Siam Cement Group (SCG) and Digital Ventures Company Limited (DV) engaged in an experimental cross-platform project to explore how Central Bank Digital Currencies (CBDC) could be used for payment and settlement by the corporate sector. This partnership was formed with the vision that digital currencies will become a basis for future financial innovations, especially around the areas of programmable money, which will become building blocks for future business innovations.

In addition, the rising threat from private digital forms of money encourages central banks to explore the potential of central bank digital currencies and their implications on the financial landscape and financial stability.

Under this public-private sector collaboration, we successfully demonstrate how blockchain can enhance efficiency and support innovations. Our prototype shows that the supply chain financing industry can be transformed by smart contract features on blockchain which leads to greater market efficiency and more competitive funding costs for supplier firms. The prototype was able to seamlessly integrate with DV's commercial application, Blockchain Solution for Procure-to-Pay (B2P), to tackle some shortfalls of existing payment systems. The outcome demonstrates that CBDCs have the potential to be a game-changer that will transform the financial landscape and bring potential benefits to all participants along the supply chain.

We would like to take this opportunity to express our appreciation towards technology consultant ConsenSys for their worthwhile contributions and continuous support throughout the journey of the project. More importantly, we hope this project encourages communities to leverage insights and ideas for CBDC usage and to better understand the opportunities that the new technology has to offer.

Thammasak Sethaudom
The Siam Cement Public Company Limited

Mathee Supapongse
Bank of Thailand

Orapong Thien-ngern
Digital Ventures Company Limited

Contents

01 Executive Summary

This project is a joint initiative among the Bank of Thailand (BOT), Siam Cement Group (SCG) and Digital Ventures Company Limited (DV), with technical support from ConsenSys, to explore the potential benefits of using Central Bank Digital Currencies (CBDC) for payment in the business sector.

While CBDCs do not necessarily require the use of Distributed Ledger Technology (DLT), the BOT recognizes the need to explore its potential. In this experiment, the BOT, for the first time, introduces a blockchain-based digital form of central bank money for corporate payments, expanding the scope from the previous Project Inthanon which focused only on interbank payments. Our prototype is based on a two-tier system in which the central bank distributes CBDC through intermediaries before reaching end-users. This model preserves financial institutions' roles in monetary policy transmission mechanisms and utilizing existing resources and infrastructure.

Apart from successfully carrying out the basic payment functionalities of issuing, destroying, distributing, transferring CBDC and other related functions, the project also demonstrates complex functionalities, namely invoice tokenization and programmable money, by utilizing smart contracts. For invoice tokenization, the project successfully introduces supply chain financing on the CBDC network, with seamless integration with DV's Blockchain Solution for Procure-to-Pay (B2P), to enhance information sharing and transparency, allowing supplier firms to access liquidity from a broader lender base with more competitive funding costs.

For programmable money, we create a CBDC that can schedule conditioned payments and trade among parties. These tokens help enhance payment efficiency as conditions embedded in programmable money can be built into the CBDC to control how the token will be spent. This feature can also help improve the private sector's cash management processes.

From a technical perspective, six non-functionality requirements including finality, interoperability, privacy, resiliency, scalability, and security are assessed through many scenario tests. It is proven that resiliency is one of the strengths as the system deploys multiple validating nodes. However, it is worth noting that system scalability and performance will remain challenging issues if we aim to leverage blockchain as a core technology for a robust and large-scale infrastructure. In addition, although transactions on a typical blockchain are deliberately designed to be transparent among participants, one key requirement for financial transactions is that details of the transactions must be kept private to non-participating parties. Therefore, a cryptographic technique is employed to preserve transaction privacy with the sacrifice of system performance.

The success of the project reaffirms the importance of public-private collaboration in driving innovation and technology. The project's outcome sets the key milestone of developing CBDC for business and retail sectors that enables stakeholders to understand the potential of blockchain technology.

At this point in time, the BOT has not made any decision on whether and when to issue CBDC but the findings from this experiment will help the BOT make more informed decisions going forward.

02 Introduction

2.1 Background

The rapid development of technology is changing the way we think of money. DLT[1] has introduced the world to faster, cheaper and more efficient forms of digital currencies. CBDCs, in particular, have the potential to change the financial landscape and the way financial transactions are conducted across the business sector. It is for this very reason CBDCs have attracted the attention of central banks worldwide, including the BOT.

While CBDCs do not necessarily require the use of DLT, the BOT recognizes the need to explore its potential. In August 2018, the BOT initiated Project Inthanon, a collaborative project with eight leading commercial banks in Thailand, to explore the potential of DLT in enhancing wholesale payment efficiency. The project focused on multiple payment functionalities using CBDC such as interbank payment, cross-border funds transfer, bond tokenization with delivery-vs-payment (DvP)[2] properties. In addition, process automation using smart contracts helped improve post-trade operational efficiency, liquidity management, and transaction transparency.

At the same time, SCG and DV joined forces to build a novel supply chain solution, B2P. B2P brought all stakeholders in the supply chain network onboard, providing them with more automated solutions such as matching and verifying purchase orders, goods received, and invoices. In addition, participants can track approval and payment statuses in real-time, enhancing security and transparency throughout the entire procurement process.

The BOT sees CBDC as potential building blocks for supporting financial innovation in the business sector. Acting on this vision, this project brings together the BOT, SCG and DV to explore how CBDC could bring benefits to supply chain financing and business operations by utilizing smart contracts.

This project was developed using Hyperledger Besu, a blockchain platform supported by ConsenSys.

Blockchain for CBDC

Blockchain technology brings unique advantages to CBDC.

- **Decentralization**: Payment verification can be carried out without dependency on any single party.
- **Resiliency**: Storing transactional data across a network rather than in a central database helps support a resilient payment landscape.
- **Programmability and Innovation**: Smart contracts can be programmed into CBDC to enhance payment innovation and meet future payment demands in a digital economy.
- **Tokenization**: Blockchain technology can issue securities in tokenized form, including turning fiat-money into cash tokens. With this feature, the token will have a cash-like property in a digital form.
- **Data Integrity**: Due to its decentralized nature, there are no centralized data stores since data is recorded on a chain of nodes, making it more resistant to malicious changes by any single party.
- **Interoperability**: Serves as a building block for cross-border payment for central banks to work together in linking domestic CBDCs and setting cloud standards to support interoperability.

HYPERLEDGER BESU

Hyperledger Besu is an open-source Ethereum client designed with a modular architecture to meet the requirements of enterprise applications and projects.

Ethereum is a large open-source blockchain ecosystem and its implementations display a single, unified view of their network's stored ledger. This single ledger can support a large number of use cases, allowing the build-out of additional privacy and scalability solutions on top of the protocol without restrictions to ownership.

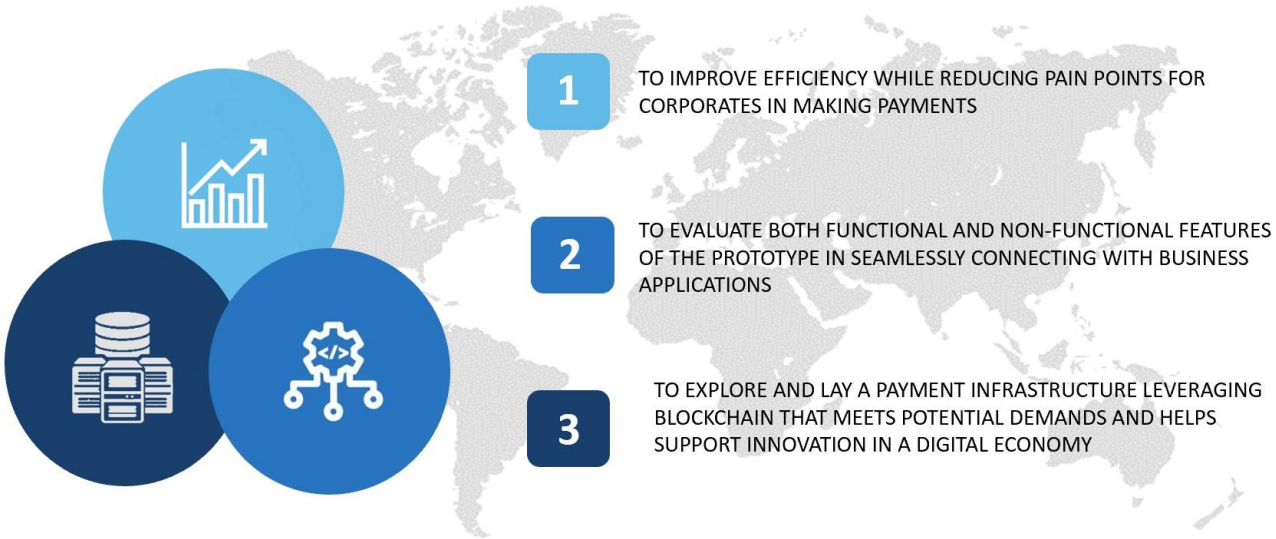
1/ Distributed ledger technology (DLT) is a system for recording the transaction in which the transactions and their details are recorded in multiple places without central data store. Blockchain is a type of DLT where transactions are recorded with an immutable cryptographic signature called a hash.
2/ DvP is a common form of settlement for securities. The process involves the simultaneous delivery of all documents necessary to give effect to a transfer of securities in exchange for the receipt of the payment.

2.2 Vision

Central banks across the globe have shown increasing interest in retail CBDC. Beginning with the exploration of utilizing wholesale CBDC to facilitate payments between financial institutions in Project Inthanon, the BOT now expands its attention to the corporate and retail level. This project is the first time in which the BOT introduces a new form of central bank money accessible by corporates. The project aims to engage stakeholders in envisioning the potential uses of CBDC in the real world, helping us lay a sound foundation for the country's digital financial infrastructure.

2.3 Objectives

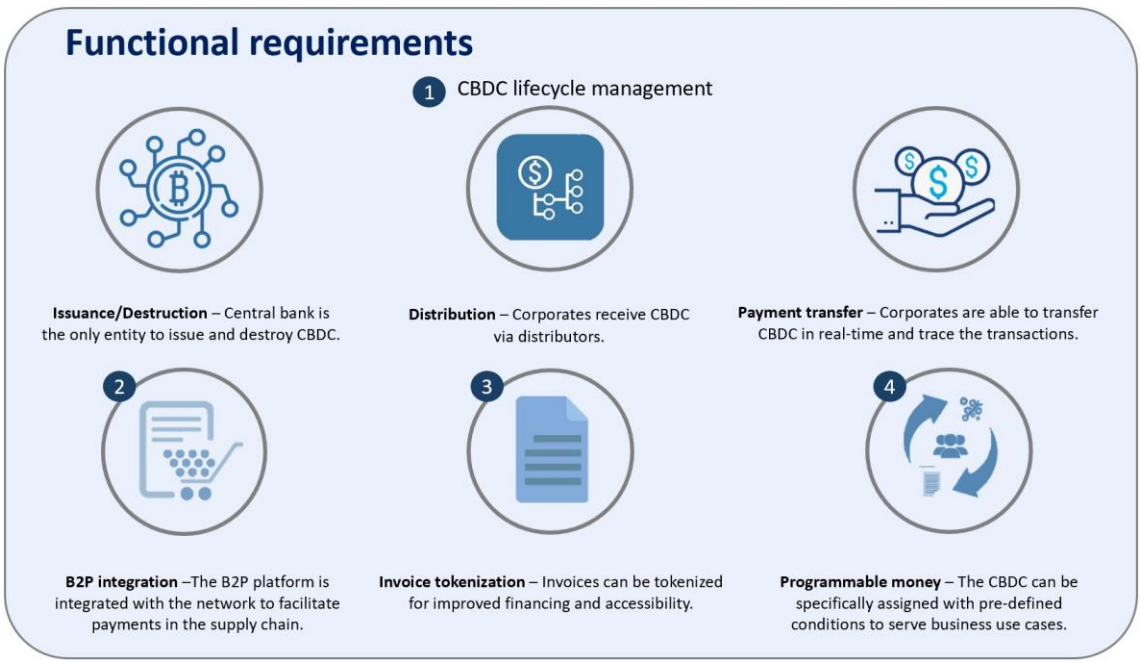
The BOT, SCG and DV see potential in connecting CBDC with business applications. Our project, a CBDC network prototype, is developed to meet the key objectives, as follows.

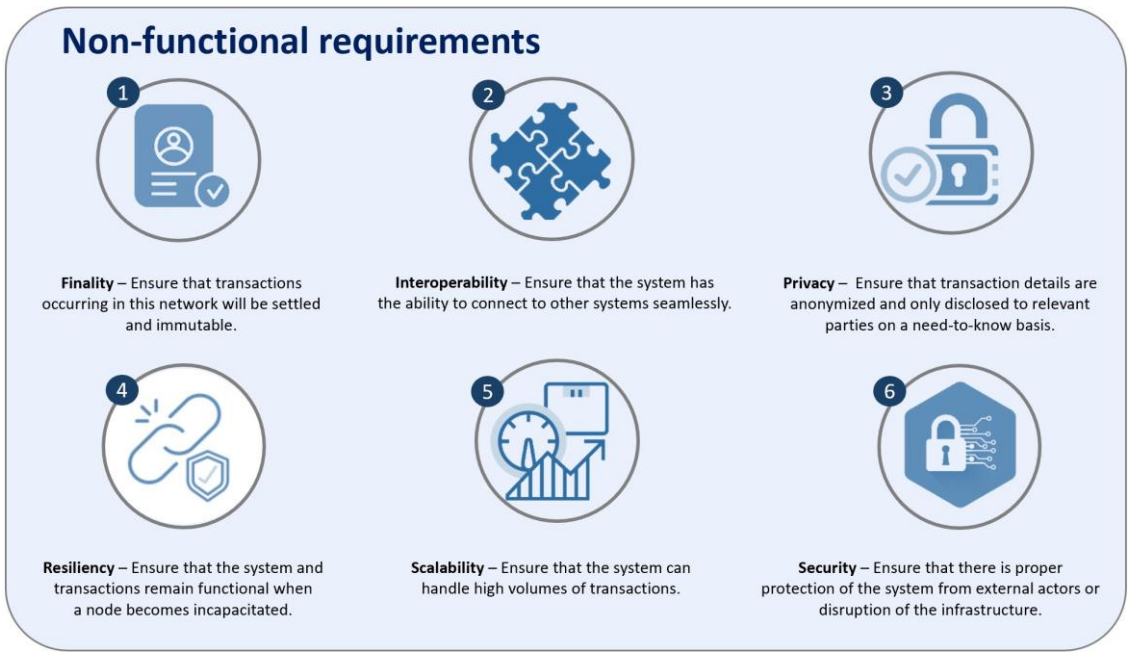


2.4 Scope

The four functional requirements of this project include (1) CBDC lifecycle management: issuance, destruction, distribution, and payment transfer, (2) B2P integration, (3) invoice tokenization, and (4) programmable money.

Additionally, six non-functional requirements, namely (1) finality, (2) interoperability, (3) privacy, (4) resiliency, (5) scalability, and (6) security are identified as key considerations during the solution design and development.



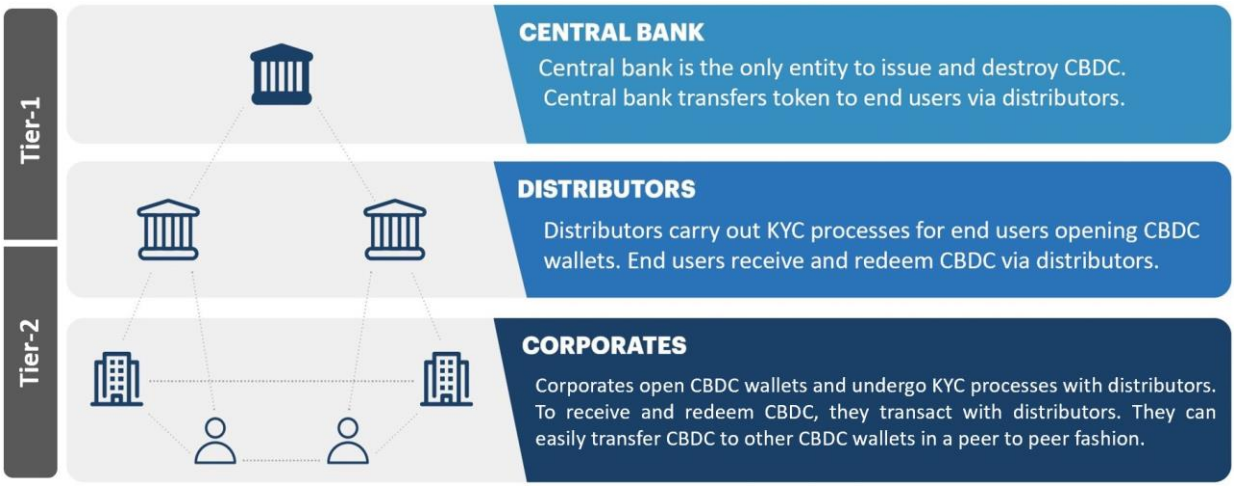


03 Architecture Design

3.1 Two-tier System and Roles in CBDC Network

One key question in the design of CBDC is the respective roles of the central bank and private sector in providing CBDC access to corporates. In a one-tier CBDC system, the central bank is responsible for the entire end-to-end process including customer onboarding, CBDC issuance, account-keeping, and transaction verification. Alternatively, the two-tier system utilizes intermediaries to distribute CBDC and conduct all customer-facing activities and services.

In this project, we opt for a two-tier CBDC design as this system preserves financial institutions' roles in monetary policy transmission mechanisms, utilizes existing resources and infrastructure, supports innovation and promotes competition through market-driven development. Financial institutions, such as commercial banks and payment service providers (PSPs), already possess fully-developed IT infrastructure applications and service systems, along with strong distribution channels, customer onboarding capabilities, and the abilities to provide more advanced financial services. Furthermore, as the public is accustomed to financial services being provided by commercial institutions, a two-tier system could also help boost public adoption of CBDC.



Central bank level: The central bank, as the sole CBDC issuer, is responsible for issuing, destroying and controlling CBDC in circulation.

Distributor level: Under a two-tier system, distributors such as commercial banks and PSPs are responsible for handling user-related and distribution operations, such as KYC[3] processes and exchanging CBDC and deposits. Hence, intermediaries are indispensable even though they are not responsible for the settlement and provision of transaction finality. Seamless interoperability with distributors' platforms is crucial for handling such operations.

Corporate level: To obtain a CBDC wallet, all users must verify their identities with distributors. Once users have their own wallets and receive CBDC from distributors, they can make transfers on a peer-to-peer and real-time basis.

3/ Know Your Customers (KYC) is the process of identifying and verifying the identity of the client when opening an account.

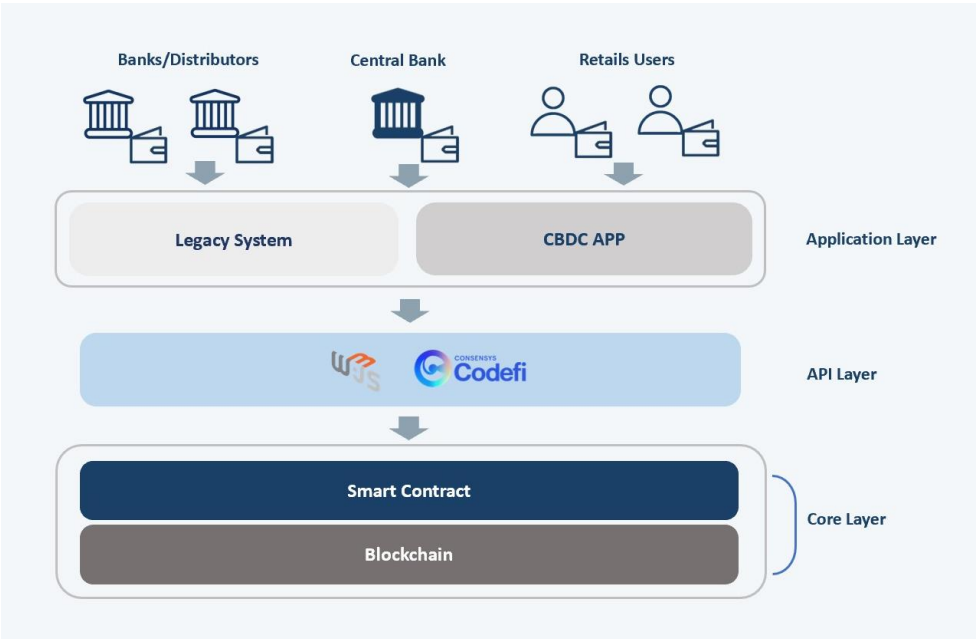
3.2 Overall Architecture

Core Layer is where data operation is carried out by receiving instructions from users through Application Programming Interfaces (API[4]) and managed on a peer-to-peer basis. In the core layer, there are two sub-layers which are the blockchain and smart contract layers.

1) Blockchain Layer is a network of computers that sends, executes, and stores transactions in a shared ledger in an orderly fashion. This creates a distributed database that records all the data, transactions, and other relevant information. Each computer in the network is called a node. Nodes are accountable for validating transactions, structuring them into blocks, and broadcasting them to the blockchain network. When a consensus is reached, a new block is committed to the blockchain network and each node then updates its local copy with the latest data.
2) Smart Contract Layer is the layer home to smart contracts[5] and underlying rules. This layer contains the codes and rules for execution. Business logic regarding tokens issuance, destruction, and access control will be interpreted into a computer program. Such programs are called smart contracts and will be executed when the pre-defined conditions are met.

API Layer enables applications to interact with the blockchain. For instance, an application can interact with blockchain nodes and smart contracts through APIs such as Web3.js[6] and Codefi[7] by ConsenSys.

Application Layer comprises applications and legacy systems that end-users use to interact with the blockchain network. User interfaces, frameworks, and scripts reside in this layer. We call applications that are designed to work with the blockchain network dApps[8].

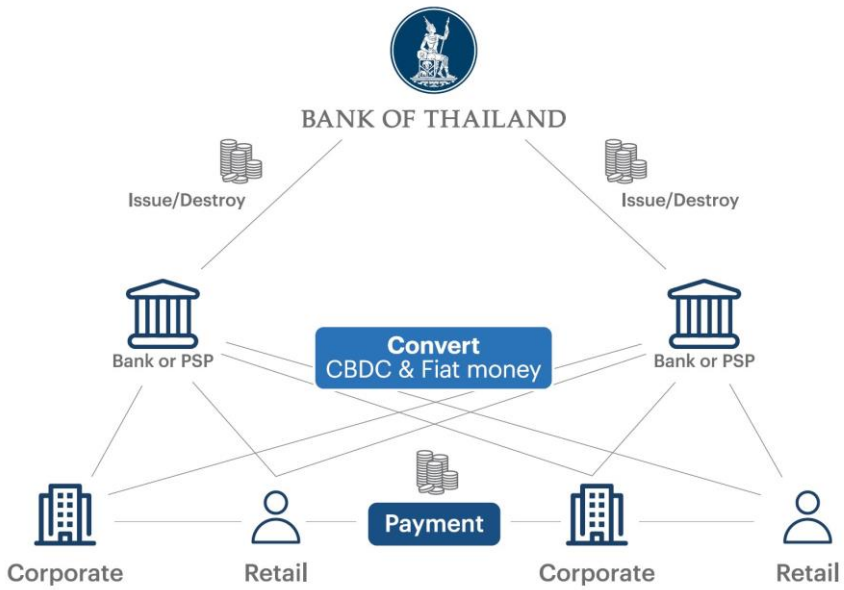


4/ Application Programming Interface (API) is a programming interface that defines interactions between applications. It defines available function calls that can be made, the required data formats and the conventions to follow, etc.
5/ Smart Contracts are computer codes which are embedded in the network to automatically enforce rules and navigate interactions between accounts in the network.
6/ Web3.js is a collection of libraries which allow the application to sign, send transactions, and communicate with smart contracts in the blockchain.
7/ Codefi Asset APIs, developed by ConsenSys, utilizing blockchain technology to optimize business processes and payments, digitize financial instruments, and build customized decentralized applications.
8/ dApps are decentralized applications developed to run on top of distributed ledger technology like blockchain. A decentralized application leverages smart contracts. The blockchain network is the back-end system for these applications and they often connect with the blockchain network via APIs.

04 Functional Scope and Key Findings

4.1 CBDC Lifecycle Management

In this prototype, the BOT is responsible for issuing, distributing to the first tier, which comprises commercial banks or PSPs. It is also responsible for destroying CBDC. Commercial banks or PSPs then distribute CBDC to the corporates in the second tier. Corporates can then use CBDC to make payments on a peer-to-peer and real-time basis.



4.2 CBDC Applications

Alternative payment for corporates

Background

At present, corporate payments are made through banks and processed in job scheduling and executed in batches. Given this, corporates face the following pain points;

1) Corporates are required to send payment instructions to banks within the cut-off time during business hours and several business days ahead of the actual settlement date.
2) There is a low level of traceability of transactions in existing payment channels. It is difficult for business operations to be aware of the transaction status including incoming and outgoing transactions for daily cash management.
3) Corporates typically use multiple banks for facilitating diverse business operations and risk management purposes. Therefore, they are required to handle various payment instruction formats from multiple banks for submitting payment transactions.

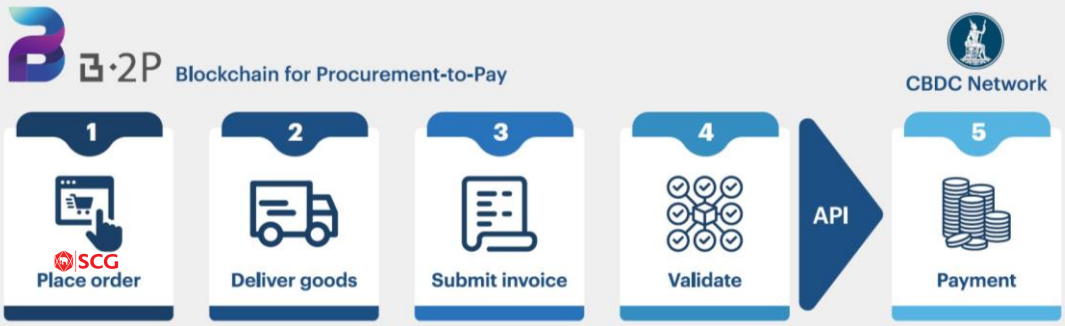
Solution and key findings

CBDC, as digital cash on hand that is readily transferable, can alleviate the burdens that corporates face on a regular basis. Through our design, corporates can exchange their deposits held at banks to obtain CBDC to hold in their wallets. They can then transfer and receive CBDC on a peer-to-peer and real-time basis in the same way people transact with cash in their daily lives.

Instead of integration with existing payment systems provided by banks, we experimented by allowing the B2P platform to connect with the CBDC network, to facilitate supply chain payments. Buyer (SCG), sellers (suppliers), and banks exchange trade documents over the platform while payments are settled through CBDC on demand, even during off-hours and holidays. Also, as CBDC is accessible by anyone within the network, it allows for traceability of transaction statuses and eliminates the need to handle multiple payment instruction formats.

However, for corporates to hold CBDC in their wallets means that they sacrifice the interest income earned on holding deposits. Therefore, we should not expect that CBDC payments will completely replace or act as a complete substitute for the banks' existing payment services. Instead, we envision CBDC payments to play a role alongside bank deposits and payments services.

B2P business payment workflow



1. The buyer (SCG) places an order to buy goods from a seller (supplier) company.

2. The seller delivers the goods to the buyer.

3. The seller sends an invoice to the buyer via the B2P platform.

4. The B2P platform validates the trade documents and the buyer confirms the payment.

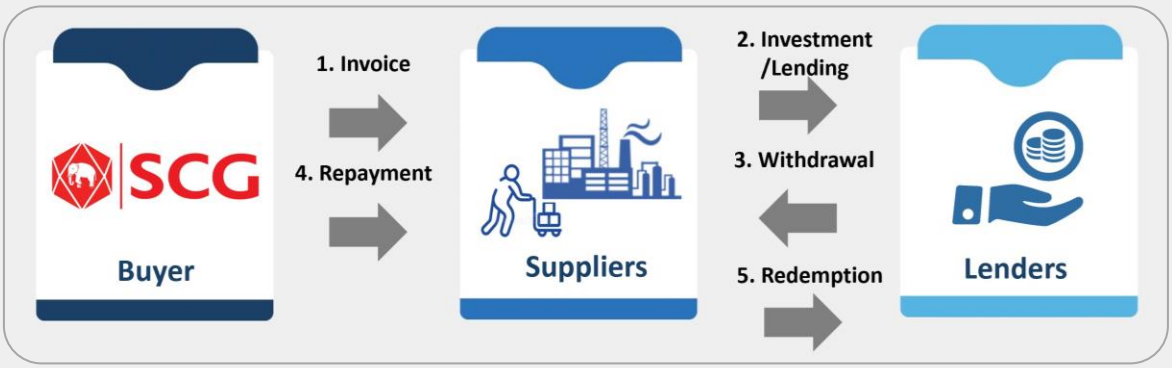
5. The B2P platform triggers a payment in the CBDC payment networks via API call to transfer CBDC, as provided by the CBDC payments network.

Supply chain financing and invoice tokenization[9]

Background

Leveraging blockchain technology, B2P provides buyers in the network with more automated procurement solutions, such as matching and verification of purchase orders, goods receipts, and invoices. Suppliers can post invoices as collateral to request financing from lenders on the B2P platform. One existing limitation is that the platform is currently open to a limited number of lenders. As a result, suppliers cannot access funding at competitive rates.

Invoice tokenization and financing workflow



1. After SCG submits an invoice to a supplier, the supplier can select the invoice for financing request on B2P platform.

- The invoice information e.g. invoice number, buyer (SCG) and supplier's information, amount, and due date, is sent to the supply chain financing decentralized application on the CBDC network for tokenization.
- The smart contract generates invoice tokens on the CBDC network. An invoice is represented by a certain number of tokens which is equal to the invoice value in Thai Baht.
- This invoice information is made publicly available on the supply chain financing application.

2. Any lender can view the invoice information in the application and select to buy the tokens at a discount rate.

- The lender can buy full or partial amount of the invoice value in the form of tokens.
- When the lender buys invoice tokens, the lender's wallet is connected to the application and a transaction will be executed to swap the lender's CBDC with invoice tokens.

3. Suppliers who make the financing request can obtain CBDC, which is the money from the lenders(s) who bought the invoice tokens, from the smart contract.

4. On the invoice due date, SCG pays the supplier.

5. The lender redeems the tokens from the supplier after the due date and earns interest.

9/ Please see Appendix #1: Blockchain and Tokenization

Solution and key findings

On the CBDC network, invoices are converted into tokens. Invoice tokens can attract a larger and more diverse array of lenders as funds can come from anyone who has access to the CBDC network. Equipped with traceability, divisibility, and immutability features, one invoice can be financed by several lenders while preventing double financing. Moreover, the ownership of invoice tokens can be transferred on the network. Ultimately, this tokenization process has the potential to help reduce suppliers' cost of funding and transform Thailand's supply chain financing.

Programmable Money

Background

Managing cash at branches for corporates has long been a pain point, as they require tedious internal procedures. The process typically entails heavy manual reconciliation of cash receipts, disbursements, and balances. Handling cash also inevitably entails some losses due to human error, fraud, and theft.

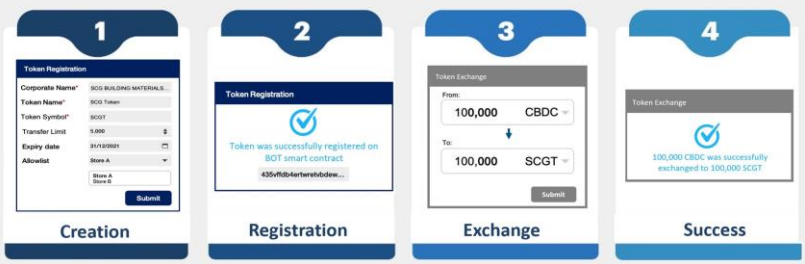
Solution and key findings

The adoption of CBDC is considered an appealing solution for addressing the aforementioned pain points as predefined conditions can be programmed into the CBDC. In this prototype, the CBDC programmable features included in the business logic are:

1. Allow/deny corporate list of who can send and receive the CBDC
2. Threshold amounts for senders
3. Time limit for usage within a particular period

Embedding such predefined conditions can help improve cash management efficiency. Businesses will be able to make, track and collect payments, which could then improve reconciliation processes, reduce costs associated with handling cash and losses from internal corruption or external theft.

Programmable money creation workflow



1. Any approved corporates can create programmable money in the form of custom tokens by providing the required information such as token name, symbol and specific payment conditions (e.g. transfer limit, expiry date, or specific recipients). which must be backed by CBDCs on the CBDC network. The smart contract generates the custom tokens on CBDC accordingly.

2. The approved corporate registers the custom tokens on the platform.

3. To obtain the tokens, the corporate needs to swap CBDC with these custom tokens.

4. The corporate can transfer these new custom tokens to the recipients if the payment conditions are met. Upon receiving custom tokens, they will be converted into CBDC automatically, and the custom tokens will be burned.

05 Non-functional Scope and Key Findings

5.1 Finality

In a blockchain, transaction finality refers to the moment when parties involved in a transaction consider the transaction to be completed. More specifically, this is the moment when it becomes impossible to revert or alter a transaction that has been added to the blockchain. Transaction finality models can be either deterministic (does not include elements of randomness) or probabilistic (transactions are not final but become more final over time as more blocks are added).

For this prototype, we have chosen the IBFT 2.0 Proof-of-Authority (PoA)[10] consensus mechanism which makes the finality deterministic. Once a transaction has been validated by the BOT blockchain network, this transaction cannot be reverted.

5.2 Interoperability

Interoperability refers to the intercommunication between two or more blockchain/distributed ledger systems. This can include event recognitions, asset moves/swaps, data transmission, or complex business logic spanning multiple ledgers. CBDC platform interoperability is guaranteed in different levels:

- Asset-level: The CBDC token is based on the Universal Token (the main token standard used in Codefi Assets API), which is interoperable with other ERC standards[11] and compatible with services currently supported by wallets and key custody solutions.
- Network-level: The prototype is based on Ethereum protocol using Hyperledger Besu, which makes it interoperable with any private Ethereum network and also with the Ethereum Mainnet[12].
- Application-level: For the CBDC platform to be interoperable with other applications, the open API layer must be standardized and well-designed to ensure seamless interoperability.

10/ The Proof-Of-Authority (PoA) is a consensus method that assigns a small and designated number of blockchain actors as validators to validate transactions or interactions with the network and to update its more or less distributed registry. Please see more information about the IBFT in 5.6 Resiliency section.

11/ An Ethereum Request for Comments (ERC) is a document that smart contract programmers using the Ethereum blockchain platform write and Ethereum-based tokens must comply with the rules in the documents.

12/ Ethereum mainnet is secured by the interaction of thousands of independent nodes run by individuals and miners. Anybody can set up a node on Ethereum mainnet.

5.3 Privacy

One of the most prominent features of blockchain is how data is verifiable yet still anonymous. Transactions can be fully validated and are open for inspection, but senders and recipients' transaction information is linked to pseudonyms instead of real names, which is called pseudo-anonymity. However, pseudo-anonymity may not be adequate for certain types of transactions. For instance, interbank transactions must be kept entirely confidential between participants. Failure to do so could harm the financial institutions' reputation and credibility. In a similar manner, corporates also prefer to keep their business transactions anonymous.

On the other hand, authorities prefer traceability and to know precisely who the senders and recipients are when necessary. The optimal level of privacy in CBDC is still debatable, as the balance between user preference and preventing fraudulent transactions must be carefully addressed.

As such, Aztec, a Zero-knowledge proof protocol[13], is introduced to enhance privacy settings from the typical blockchain. The prototype leverages Aztec so that only participants involved in the transfer can see the before and after token balances and the transfer values, but the validator can verify transfers' integrity.

In our prototype, the BOT as a regulator can potentially monitor all types of transactions. Transactions among participants are kept completely anonymous and can be seen by only the participants of that transaction and the BOT.

The outcome proves that by utilizing Aztec, privacy settings can be achieved on the blockchain. However, it is worth noting that a higher level of privacy has a negative impact on overall system performance. As such, applying privacy settings to the overall system would need to be carefully considered further.

[13/] Please see Appendix #2: Zero-knowledge proof

5.4 Security

For effective security on the blockchain, there are two key elements to take into consideration: network and data security.

Network Security

- Access Permissioning enables the prototype network to be designed and created as a permissioned network. This allows only approved nodes to connect to the network and perform only allowed actions (e.g. onboarding or identity requirements).
- Firewall must be configured to restrict network connections and allow only permitted participants

Data Security

- Encryption at rest prevents malicious actors who gain access to a node on a private network from reading its valuable data, by ensuring full encryption of the node database.
- Key management refers to storing, managing keys and signing blockchain transactions. On a blockchain, private keys are required for users to access accounts, sign and send transactions. Once your private key is lost, you can no longer access your account or send transactions. Hyperledger Besu does not support key management. The keys used to sign transactions are stored externally.

Additionally, more security configurations can be enhanced to secure nodes and integration points.

- Role-based Access Control defines roles and privileges to restrict system access to authorized participants.
- Log Management maintains transaction records amongst participants.
- Monitoring Tool allows for the monitoring of streaming activity and improper events.

Security			
Network Security		Data Security	
Access Permissioning	Firewall	Data Encryption	Key Management

5.5 Scalability

Scalability refers to the network size (number of participants) and the transaction volume (number of transactions) that can be managed on the network.

1) Network size

There are two kinds of network participants, namely network users and network administrators. Network users only need to own and manage non-validating nodes and thus are not participating in the blockchain consensus mechanism. There is no limit to the number of network users, as we can add as many non-validating nodes as needed. On the other hand, network administrators own and manage validating nodes and thus participate in the blockchain mechanism.

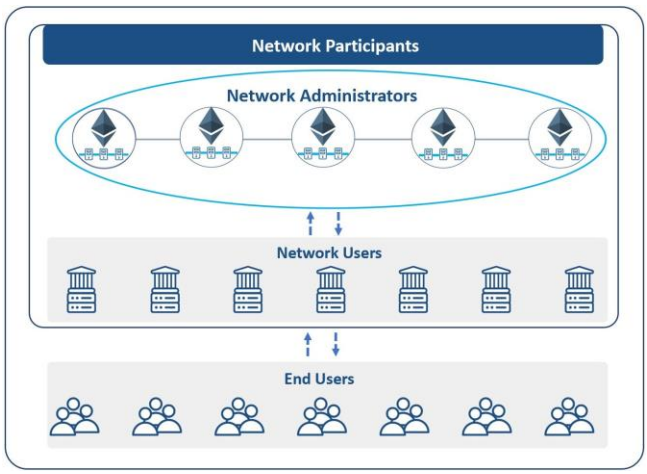
The recommended number of validating nodes is no more than 20 nodes due to technical constraints. As such, if there are more network participants willing to manage validating nodes, a rotation mechanism can be set up. Please note that CBDC end-users (i.e. corporates and households) are not network participants.

2) Transaction volume

The transaction volume is not capped by the network, but the overall network performance (measured by the number of transactions per second: TPS) relies on the time taken to process and confirm transactions. In this prototype, we decided to use a Rollup solution[14] supported by ConsenSys, to increase scalability and performance. The Rollup protocol is built on top of an existing blockchain system and processes transactions off-chain by grouping transactions into batches. Each batch will then be recorded on-chain as validity proof.

As this mechanism works on off-chain processing, on-chain smart contracts cannot interact directly with off-chain tokens and vice versa. Therefore, this increases the difficulty and complexity for developers when using the Rollup mechanism in developing applications.

Through testing, we find that the Rollup mechanism can significantly increase the TPS. The batch size can be configured to achieve optimal performance, manage transaction volume, and batch releases. However, there are some concerns regarding the batching technique as it will be processed and persisted on-chain only when the batch is full. This could result in a long waiting period when there is low transaction volume.



[14] Please see Appendix #3: Rollup Mechanism

5.6 Resiliency

Making systems resilient to ensure business continuity has become of paramount importance as more companies become digitalized and operations are increasingly being carried out on digital platform. It is proven that blockchain help enhance data resiliency as the system deploys multiple validating nodes. Therefore, the entire system will not be affected when one node is down. The system can then restore itself from an undesired malfunctioning situation.

In IBFT 2.0, there are validating nodes known as validators to verify transactions and blocks. Validators take turns to create the next block. Before inserting the block onto the chain, a super-majority (greater than 66%) of validators must first sign the block. IBFT 2.0 requires at least four validators to be Byzantine fault-tolerant. Byzantine fault tolerance is the ability for a blockchain network to function correctly and reach consensus despite nodes failing or propagating incorrect information to peers.

In our prototype, there are five validators deployed in the network. Consensus can be reached and the network can still properly function even if one validator becomes unresponsive. However, in the event two or more nodes down, consensus will no longer be reached in which case restoring the whole network to be active again may take some time due to the timeout mechanism[15].

[15] When all validators append the same block to the chain, the consensus protocol usually adds the block before reaching the timeout period. If the validators fail to add a block, then the process will be restarted and the timer will be reset. Moreover, the timeout period will double each time as the consensus fails to add a new block. In other words, the longer the network is inactive, the more time it takes to recover and validate the pending block until one of the validators becomes responsive.

06 Further considerations

There are a number of topics to consider further before any decision with regards to CBDC can be made, some of which are outlined below.

Business incentives for participants

In order to create a decentralized system, increase the attractiveness and shared value, commercial banks and other participants must see an upside in becoming a validator and distributor in the CBDC network. One possible incentive is to have accessibility to data in the blockchain. It is a fact that nowadays leveraging data insights and analytics is crucial for businesses to gain competitive advantages. Every business would like to get insights into such data as it can be analyzed and utilized towards identifying market trends and forming better business strategies. Also, a financial incentive for validator participants to actively participate, grow and secure the CBDC network can also be further explored. This could be in the form of CBDC revenue for services provided to the network along with transaction fee sharing.

Financial stability

There has been wide discussion on the possible ramifications of CBDC issuance on the broader economy and financial system, challenging central banks' abilities to conduct their key mandates of maintaining financial and monetary stability. For instance, the introduction of CBDC could lead to banking disintermediation and exacerbate "digital" bank runs, directly affecting the stability of the financial system. Clear risk-management guidelines and design principles for the CBDC system will need to be established to mitigate these risks. Setting a conversion limit between deposits or cash to CBDC, or paying lower interest rates on CBDC relative to bank deposits are examples of mechanisms that should be explored in further detail.

Data management and governance

"Data is the new oil". This quote emphasizes how valuable data is in the digital economy. Changing the way we spend, from transacting via physical cash to digital cash or CBDC, would generate unprecedented amounts of data. Therefore, the data stored on blockchains will become a precious asset. As such, data management and governance frameworks must be set up to ensure that data is managed effectively and consistently as well as guaranteeing data privacy and integrity. Creating sound policies on the use of data along with procedures to monitor usage and enforce policies on an ongoing basis is also required.

Legal frameworks

A robust legal framework for CBDC issuance will need to be thoroughly considered to mitigate legal and reputational risks for central banks. Firstly, banknotes and coins are currently the only two forms of Thai Baht currency recognized as legal tender by the Currency Act. This Currency Act may need to be revisited if the BOT is to issue CBDC and certify it as legal tender, a key attribute that would differentiate CBDC from other private digital money. Secondly, the BOT's authorized roles under the Bank of Thailand Act are to attain the objectives of maintaining monetary stability, financial institution system stability and payment systems stability. If the issuance of CBDC is to be an additional operation by the central bank to retain its capabilities to serve these key objectives, the Bank of Thailand Act may also need to be revisited. Possible amendments of the Payment Systems Act may also be needed, if CBDC is to be a national and systematically important payment infrastructure rendering the BOT's oversight; and also the Financial Institution Business Act, if financial institutions' CBDC holdings are to be counted towards liquidity asset and capital adequacy. Lastly, it will be necessary to design a framework around governance, standards and regulations to ensure that the CBDC is appropriately used, managed and operated.

Participation and accessibility

The CBDC platform is expected to be open to and inclusive of all corporates and their use cases. Therefore, a clear overall strategy of the CBDC system, robust governance structure, and adequate criteria guidelines will need to be established to allow for the onboarding of new participants and requirements. Corporates' financial health, reputation, cybersecurity practices and other relevant standards should be considered as a part of the onboarding process. In addition, risk mitigation measures will also need to be formed to ensure the safe and successful integration of the CBDC system with new and existing business platforms.

07 Conclusion

This project is the BOT's first experiment in introducing a new digital form of central bank money to corporates, in line with our vision of moving towards the broader digitization of money and a cashless society. Leveraging blockchain technology with the collaborative efforts of BOT, SCG, DV, and technology partner ConsenSys, a proof-of-concept has been successfully built to demonstrate the potential of blockchain technology adoption in payment systems for business sectors. The key findings from our prototype demonstrate that CBDC can achieve not only basic payment functionalities such as issuing, distributing, destroying, transferring CBDC but also more complex and innovative applications such as invoice financing and conditional payments. Such applications can help reduce existing pain points and enhance efficiency in financial services, and business operations.

The programmability feature through smart contracts will expand the capacity of what money can do, as it allows more innovative and customized applications to be implemented and tailored to suit business and individual needs. Moreover, it is proved that it is highly accessible for business applications as we successfully integrated the CBDC network with Blockchain Solution for Procure-to-Pay (B2P) developed by DV, with both being able to work seamlessly alongside each other.

From a technical perspective, blockchain is a technology that enables innovation, data transparency and resiliency in a way that has not existed in conventional systems. However, it is worth noting that system performance remains a challenging issue and there is much room for improvement before the system would be ready for a live environment. Moreover, since the CBDC will serve as a public good accessible by consumers nationwide, further research and experiments are certainly needed to elevate CBDC performance to its highest potential.

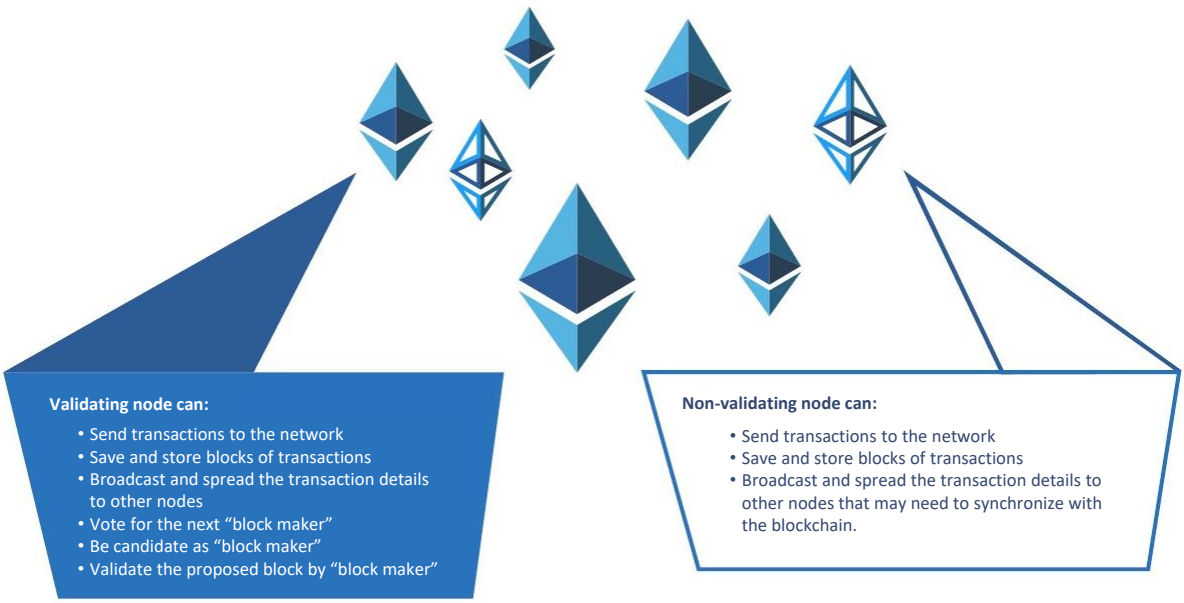
Beyond assessing technological capability, it is also necessary to conduct more comprehensive studies in other aspects as the introduction of CBDC to the general public would undoubtedly have far-reaching implications to the overall economic system. In addition to enhancing innovation for payments as we discovered in the project, the impact of CBDC on financial stability and the payment system as a whole would need to be taken into account and carefully assessed. Moreover, implementation costs at a full-production level, governance structures as well as legal and regulatory compliance are important issues that require further discussions and research. Thus, before any decisions can be made, the BOT would need to be certain that the net benefit of issuing CBDC would outweigh any potential risks, which is also dependent on dynamics of market development and unforeseeable challenges. We will continue engaging with stakeholders and monitor the development of digital currencies and technologies, not limited to blockchain, to ensure that our policy decisions are optimal.

08 Glossary

Term	Description
API	Application Programming Interface is a programming interface that defines interactions between applications. It defines available function calls that can be made, the required data formats and the conventions to follow, etc.
dApps	Decentralized applications developed to run on top of distributed ledger technology like blockchain leveraging smart contracts. The blockchain network is the back-end system for these applications and they often connect with the blockchain network via APIs.
DLT	Distributed ledger technology is a system for recording the transaction in which the transactions and their details are recorded in multiple places without central data store. Blockchain is a type of DLT where transactions are recorded with an immutable cryptographic signature called a hash.
DvP	Delivery versus Payment is a common form of settlement for securities. The process involves the simultaneous delivery of all documents necessary to give effect to a transfer of securities in exchange for the receipt of the payment.
ERC	An Ethereum Request for Comments (ERC) is a document that smart contract programmers using the Ethereum blockchain platform write and Ethereum-based tokens must comply with the rules in the documents.
Ethereum mainnet	Ethereum mainnet is secured by the interaction of thousands of independent nodes run by individuals and miners. Anybody can set up a node on Ethereum mainnet.
KYC	Know Your Customers is the process of identifying and verifying the identity of the client when opening an account.
PoA	The Proof-Of-Authority is a consensus method that assigns a small and designated number of blockchain actors as validators to validate transactions or interactions with the network and to update its more or less distributed registry. Please see more information about the IBFT in 5.6 Resiliency section.
Smart Contracts	Smart Contracts are computer codes which are embedded in the network to automatically enforce rules and navigate interactions between accounts in the network.

09 Appendix

Appendix #1: Blockchain and Tokenization



A blockchain is composed of blocks of data stored on nodes (which can be compared to small servers). All nodes are connected and constantly exchange the latest blockchain data with one another to stay up-to-date. They store, distribute and preserve the blockchain data that make it impossible to change, hack, or cheat system.

The Ethereum blockchain is based on two types of nodes: Validating nodes and Service nodes (Non-validator nodes).

The CBDC token is based on the Universal Token for Assets and Payment. The Universal Token smart contracts combine and enable all requirements needed:

- Control mechanisms, by offering a module for certificate checks, a module for allowlist checks and the possibility to force transfers.
- Reliability of participant registry, by providing a module to create token holds.
- Certainty of delivery-vs-payment (DvP) execution, by including token holds for atomic DvP, and HTLC (Hash Time Locked Contract) mechanism for non-atomic DvPs.
- Interoperability, by offering an ERC20 interface to remain compatible with the majority of existing tools and platforms.

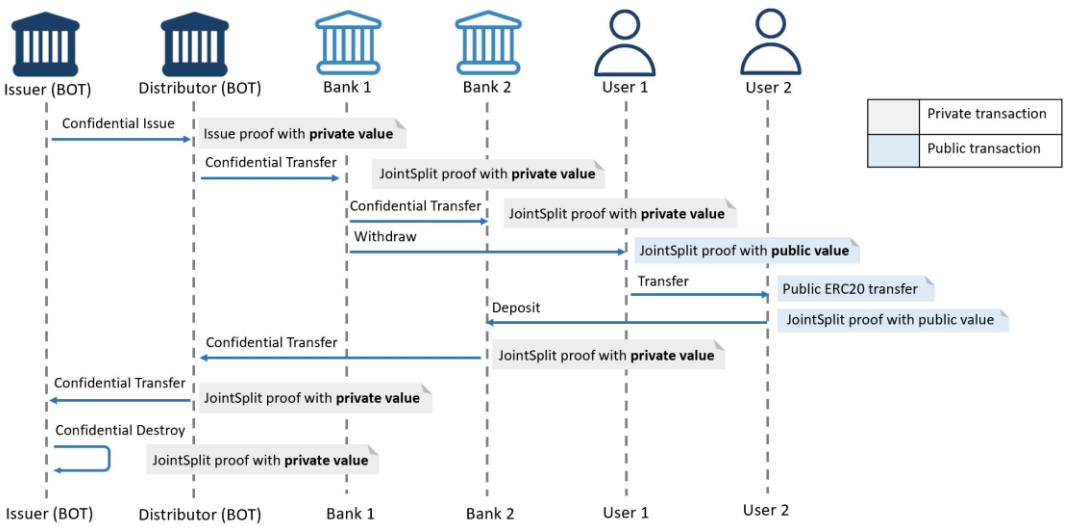
The listed features can be turned on and off during the token's life cycle. In addition, businesses can tokenize other assets and use CBDC for payment and settlement. This will increase interoperability for FinTech companies to create and provide more value-added financial services, stimulating competition and innovation.

Appendix #2: Zero-knowledge Proof

Zero-knowledge proof mechanisms have been explored to guarantee transaction privacy. The details of how they work are beyond the scope of this documentation, but a high-level summary is that Zero-knowledge proof leverages advanced cryptography to provide a trusted compute framework so that state transitions can happen with encrypted data and is verifiable by everybody in the network without knowing the real data. A global state is maintained by the entire network, making it possible for token use cases to ensure global mass conservation.

Technically, the protocol is a smart contract deployed on-chain. One advantage is that, as it is a layer-1 solution, it is possible to interact with other contracts and tokens on-chain. However, in order to transfer CBDC tokens privately, the tokens must first be converted into notes in the UTXO (Unspent Transaction Output) model and then transferred, causing some performance concerns.

Workflow: Issue, Deposit, Withdraw, Destroy, and Transfer CBDC



For the prototype, Zero-knowledge proof (using Aztec) has been chosen over Privacy Group (using Orion) because it allows a wider variety of use cases regarding the management of recipients receiving private transactions. When using the Besu Privacy Group mechanism, the prerequisite for sending a private transaction between two parties, A and B, is to have created a Private Group between A and B, before sending the private transaction. Whereas with the Zero-knowledge proof mechanism, a private transaction can be sent directly between parties A and B, without any prerequisite.

Appendix #3: Rollup Mechanism

Rollup mechanism is typically used to solve transaction speed performance and scaling difficulties. In terms of scalability, Rollup mechanism is widely considered to be the best solution by the crypto community. Rollups bundle or "roll-up" transactions into a single transaction and generate a cryptographic proof. This proof is then submitted on-chain, meaning that all state and executions are stored and performed "off-chain". The off-chain state and transactions can then be verified by the proofs stored on-chain, removing the burden of validation from the network and dramatically increasing the TPS.

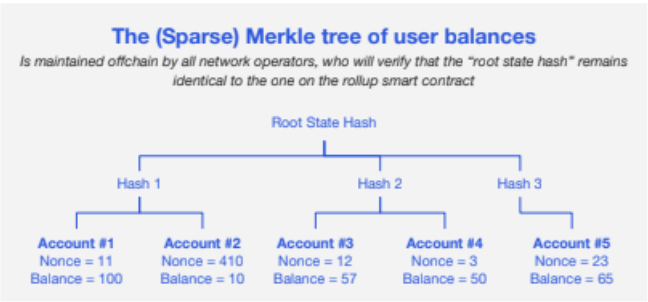
A Rollup Mechanism designed by ConsenSys was used in our prototype as it best matches our use case. The ConsenSys Rollup Mechanism allows for the state (in hash form) to be stored on a smart contract while storing the proofs on-chain. Each operator can then validate the transactions retrospectively by applying the proof to the off-chain state and generating a state hash, then submit this generated hash to the contract. If the hash is the same as the original hash mentioned above, a vote is added to the contract. Once more than 60% of operators vote in favor, the state is confirmed.

All user accounts are maintained in a unique rollup merkle tree.

Only the root state hash is recorded in the smart contract, while transactions are recorded in the **block payload**.

Each operator maintains his full own Merkle tree offchain

The operator generates **the proof** that the changes in the state correspond to actual valid transactions and sends it to the blockchain with the **root hash update** and the **executed transactions**



10 Acknowledgements

Steering Committee

Name	Organisation
Vachira Arromdee	Bank of Thailand
Thammasak Sethaudom	The Siam Cement Public Company Limited
Orapong Thien-ngern	Digital Ventures Company Limited

BANK OF THAILAND

Name	Role
Mathee Supapongse	Project Sponsor
Vachira Arromdee	Project Executive
Kasidit Tansanguan	Project Coordinator
Sarun Youngnoi	Project Coordinator

Name	Role
Premmanat Kanchanawila	Business SME
Tansaya Kunaratskul	Business SME
Tunyathon Koonprasert	Business SME
Tuln Sermsiriviboon	Business SME
Pisak Kurusathian	IT SME
Worapol Tangkokiattikul	Developer
Soranut Midtrapanon	Developer
Pontakorn Mekintarangkoon	Developer
Napat Pornchensunapong	Developer

SCG

Name	Role
Vilasinee Channarukul	Business Expert
Pimrat Vasinchai	Business Expert

DIGITAL VENTURES

Name	Role
Paisal Kiattananan	Product Manager
Pawinee Amonnuntarat	Project Manager
Apirak Boonsanong	Senior Developer
Jittawat Thanawatcharangkul	Senior Developer
Thanapong Sinsirimongkol	DevOps
Laikhram Jamjuntra	Developer
Ariya Lawanitchanon	Developer
Ugrit Wongkham	Developer
Natsha Panchanta	Business Analyst
Natthamon Pongchanchai	Business Analyst
Kawin Khanobthamcha	Automate Tester
Adinan Soseesuk	Automate Tester
Tharit Suebamornpimon	Automate Tester

CONSENSYS

Name	Role
Charles d'Haussy	Project Director
Dr. Arafet Ben Makhlouf	Project Manager & Technical Architect Lead
Patricia Yeung	Business Analyst
Pablo Valles	Technical Business Analyst
Nick Addison	Senior Developer (Privacy SME)
Liam McAweeney	Developer (Rollup SME)
Kanthesha Devaramane	Developer (Solidity SME)

SPECIAL THANKS

The BOT Digital Currency Team would like to express our gratitude to our senior executives for their insightful advice and constant support throughout the project.

BANK OF THAILAND

Dej Titivanich	Roong Mallikamas	Amporn Sangmanee
Daranee Saeju	Pornvipa Tangcharoenmonkong	Vanaporn Laksanasut
Suchot Piamchol	Thammarak Moenjak	Tuangporn Khawcharoenporn
Archari Supiroj	Chananun Supadulya	Anocha Sompannok

The Team would also like to extend special thanks to the ConsenSys team and ConsenSys' partner, Atato, for their meaningful assistance and development of the prototype.

CONSENSYS

Edmund To	Matthieu Saint Olive	Adrien Delaroche
Rafael Chiang Diaz	Bryan Combs	Sarah Carlson
Guillaume Le Saint (Atato)	Pongsabutra Viraseranne (Atato)	Pattaragorn Khunanupabkhun (Atato)

Contact Us

DigitalCurrencyTeam@bot.or.th

Digital Currency Team
Bank of Thailand