NATIONAL BANK OF CAMBODIA

Riel. Stability. Development.

PROJECT BAKONG

Next Generation Payment System

JUNE 2020

CONTENTS

Foreword

The National Bank of Cambodia ("NBC") is mandated to: (1) formulate, implement and monitor monetary and exchange rate policies; (2) regulate and supervise financial institutions; (3) oversee payment systems in the country; (4) enhance interbank payments aiming to maintain stability of the financial sector; and (5) contribute to high and sustainable growth.

With the promoting of a safe and efficient payment system being one of the bank's key priorities, several development initiatives had been undertaken over the past decades to uplift payment system capabilities, ranging from the National Clearing System ("NCS"), FAST system ("FAST") and Cambodian Shared Switch ("CSS"). The latest addition to the payments landscape is Project Bakong - a project that explores the use of an alternative technology platform to further enhance payment system in Cambodia. This Project was explored as part of effort to address the lack of interconnectivity and interoperability, and attain efficiencies (reduced cost, increased speed, and enhanced security) within the current payment system. It also aims to promote financial inclusion and ease Cambodian Riel ("KHR") cash payment.

As such, in 2016, NBC established a working group to explore the use of blockchain and distributed ledger technology ("DLT") in payment systems. By early 2017, the group had developed use-cases under the auspices of Project Bakong. The name Bakong comes from a prominent Khmer temple from 9th century whose architecture was replicated to build Cambodian Independent Monument in 1958. The logo of Bakong project is the outline of the temple's structure.

Within the same year, prototypes were developed during the second half of the year. In early 2018, the group evaluated the results of the prototype tests and continued to fine-tune business processes, system processes, and internal system integration. By mid-2018, a call for express of interest from the banking and financial institutions to participate in the project was announced for the first time. Several financial institutions participated in the demonstration and discussion of the project.

This report explains the rationale behind this project and provides an overview of the Project Bakong with regards to the choice of technology, the design feature and potential implications. A pilot test of the project with participating financial institutions is currently under way as a mean to examine the feasibility of the approach and identify potential issues before the official launch.

Phnom Penh, June 2020

1 Background

With the intention to harness the rapid advancement of new technological innovations, central banks have cautiously and prudently explored the degree to which blockchain technology can be harnessed, via research and experimentation. The use of blockchain technology to develop a central bank digital currency ("CBDC") has attracted attention of central bankers across the globe. While the digital currency, i.e. bitcoin, was first created in response to the financial crisis. Since then, several central banks around the globe have been exploring the introduction of CBDC, and new technological innovations arising from blockchain and distributed ledger technology ("DLT"). It is believed that such technologies will not only be capable of developing digital currencies, but also potentially unlock new possibilities with more efficiency. For developed countries, the introduction of CBDC is in line with the declining use of cash, while for developing countries it intends to promote financial inclusion and improve inefficiencies, especially in payment systems.[1]

Aiming to benefit from such technological innovation, the NBC is embracing blockchain technology for its national payment system to:

01

Address the issue of interconnectivity and interoperability across platforms of payment operators

02

Attain efficiency (lower cost, faster speed and more secure) in payment systems

03

Promote financial inclusion and

04

Ease KHR (Khmer Riel) cash payment

To address the above objectives and upgrade existing payment systems, in 2017, NBC had started to explore several alternative technologies including DLT and blockchain. Such efforts provide the NBC and the financial sector with an opportunity to explore new alternative payment and operation technologies which are more secure and resilient. The project was named Bakong, and Hyperledger Iroha was selected as the platform for DLT

[1] Central banks that respond to the diminishing cash usage and aim to resolve monopoly distortions and operational risk include for example the Bank of Canada, Central Bank of Norway (Norges Bank) and Bank of Sweden (Sveriges Riksbank), while others that aim to achieve financial inclusion are the Central Bank of the Bahamas, People's Bank of China, the Central Bank of Curaçao and Sint Maarteen, Eastern Caribbean Central Bank, the Central Bank of Senegal, the Central Bank of Tunisia and Central Bank of Uruguay (Mancini-Griffoli et al., 2018).

to run on, and the pilot test of the project is currently being carried out since July 2019. Bakong also assesses implications for the adoption of DLT for retail and wholesale payments in the financial sector in Cambodia.

As payment systems facilitate safe and secure transactions across the whole economy, NBC plays the crucial role of being a catalyst, an operator, and an overseer of payment systems. Currently, the NBC operates both the retail and wholesale payment systems. The initial adoption of those systems started since 2012, nonetheless since then new features, functions, and systems had been gradually added. Although the current payment systems have been gradually developing over the last decade, the interoperability of retail payments among banks as well as Payment Service Institutions ("PSI") remains a challenge. Currently, there is no Real Time Gross Settlement ("RTGS") between banks except for end-users, while interbank clearings and settlements take place twice daily. The usage of DLT in payment system represents an opportunity for Cambodia's payment systems to leapfrog the traditional mean of connecting all players and address many challenges all at once. Bakong brings all payment service providers into one system through an open API allowing users to transact peer to peer without transaction fees in real time and in a secured manner.

More importantly, access to financial services could be substantially expanded across the country:

01

Given the current high rate of mobile usage

02

Convenient to set up an account with Bakong application

03

High adoption of E-wallet and

04

Simplified Know your Customer ("KYC")

By having such electronic payment account/wallet users do not have to carry large amount of KHR banknote to pay for high-value transaction, which ultimately will ease KHR payment.

Given the above considerations, the NBC re-evaluates existing payment systems infrastructure and engages in the Project Bakong - a project to consider alternative technology platforms to create a next generation of payment system aimed at addressing financial inclusion, interoperability amongst players, and supporting the ease of payments in the local currency, while at the sametime doing so in safety and efficiency. The project is undertaken with the collaboration of SORAMITSU Co., Ltd (a technology company based in Japan) and domestic financial institutions interested in the project.

This report provides an overview of the Project Bakong covering key considerations toward the implementation of the project, the review of the technology for the project, the design features of the new payment system, and possible implications resulting from the adoption of the new system. The rest of the report is organized as follows: Section 2 reviews key considerations for the Project Bakong and Section 3 provides the details of Project Bakong. Section 4 discusses key observations and findings, while Section 5 draws the implication of the Project Bakong. Section 6 provides the conclusion.

2 Key Considerations for the Project Bakong

This section explains key considerations that lead NBC to explore and adopt DLT under the Project Bakong. The considerations include solutions to the challenges that the current payment system is faced with, the availability of alternative technology that has the potential to tackle those payment challenges and the recent experiment of and research into blockchain technology amongst central banks around the world. With the new DLT technology facilitating the current payment system, participants and end-users are brought into one platform, and thereby efficiency in payment is attained through an increase in speed, improved security, and elimination of transaction cost, while the issue of interconnectivity and interoperability could be resolved as banks and users share one common platform, i.e. Bakong DLT. While embracing modern technology, NBC also takes into consideration the promotion of financial inclusion and increase usage of local currency in the development of Project Bakong.

2.1. Payment System Landscape

2.1.1. Payment System

The payments landscape in Cambodia has evolved remarkably over the last decade thanks to sustainable economic growth, political stability, technological advancement, and the need for efficient and fast services. However, despite such developments, paper-based instruments in the form of cash and cheques still dominate over electronic payment instruments for retail and business payments. The dominant use of such paper-based instruments over the electronic ones stems from the conventional mindset of users. Such practices while being inconvenient and inefficient, also bear inherent risks such as counterfeit currency and fraudulent cheques. Therefore, promoting electronic payment has been a key priority for NBC to mitigate such risks and make payment more convenient and efficient to support the fast growing economy of the country.

In Cambodia, retail and large-value payment systems are operated by the NBC as it plays an important role as the heart of the country's economy when facilitating the flow of money for businesses and retail transactions. Disruption of a payment system can result in financial instability that can lead to financial crisis. Given this importance, according to the Law on the Organization and Conduct of the National Bank of Cambodia promulgated on 26 January 1996, the NBC is to perform three roles with regards to the payment system, namely a catalyst, an operator, and an overseer.

01

As a Catalyst

The NBC shall ensure that payment systems are on par with that of other similar economies, contribute to payment innovations, improve general speed of payments, coordinate efforts to prevent fragmentation, enable faster remittances and also facilitate financial inclusion.

02

As an Operator

The NBC shall facilitate both settlement and clearing services, operate the National Clearing House, promote efficiency use of payment system and financial relations with public entities.

03

As an Overseer

The NBC shall ensure the safety and efficiency of payment systems by formulating regulatory framework, monitoring and assessing financial risks and other risks, and maintaing trust in the domestic currency.

The National Clearing House ("NCH") is operated by NBC, and it consists of NCS, FAST and CSS. NCH's functions have been improved continuously since its establishment in 1994, with an upgrade to the full-fledged functions of a clearing house in 2012 - providing a more secure and efficient payment system. Each of the three systems facilitates different payment instruments. For instance, cheque and payment order are facilitated by NCS, while KHR interbank funds transfer and automated teller machine ("ATM") / point of sale ("POS") interoperability are facilitated by FAST and CSS, respectively. Of these, cheques and payment orders are the most popular payment instruments used in retail payment and business activities. By using cheques and payment orders, consumers can conduct an unlimited number of transactions in both Khmer Riel (KHR) and United States Dollar ("USD"). However, as settlements are only conducted twice daily and during business hours, banks are subject to settlement risks arising from the lag time between the transaction and settlement.

The NBC launched FAST in 2016 as a supplementary payment system to promote electronic payments. FAST allows electronic payment transactions and fund transfers in real time from bank account to bank account (irrespective of the banking entity) in KHR with a daily limit of 40 million KHR (10,000 USD equivalent). It is worth noting that while FAST allowed real time settlement for end-customers, interbank clearing and settlement still observe the NCH schedule, i.e. twice daily. As a backbone system, the NBC relies on banking institutions to create the users interface required with their customers to make the transactions convenient. Unfortunately, many institutions do not invest in mobile application that would facilitate such transaction, and customers would still need physically visit the participating banks or microfinance deposit-taking institutions ("MDI") to initiate payments or transfers, rendering the service as inconvenient and inefficient as before. NBC is therefore encouraging the participants to adopt FAST in their mobile and internet banking in order to make the system more convenient and less costly. Some participating banks have also started to adopt mobile and internet banking.

FAST, however did not address card payment connectivity. To address this challenge, in 2017 the NBC introduced CSS, a nationwide infrastructure for local debit card payment operated by ATM and POS machines, and a network for international gateway for payment system integration in the region. CSS aims to provide interconnectivity and interoperability amongst participating institutions, allowing them to save cost of the deployment of card payment network. CSS is made possible by adopting a national chip card specification with the NBC providing the switch to connect all card transactions within the country. Participation in FAST and CSS are compulsory for MDIs in the country.

For interbank large-value transactions, it can be made through online banking hosted by the NBC and this process removes paperwork by allowing participants to directly carry out transactions online. Since its establishment in 2016 online banking services are offered by 38 financial institutions including the national treasury department, which is in line with the government's efforts to digitize its revenue collection and budget expenditures. Settlement between members is made in real-time using their current accounts held at the NBC.

In addition, to promote interbank market transaction, the NBC introduced the NBC-Platform in 2017, supporting the growth of central bank security trading, foreign exchange dealing, and the discount window. The introduction of the system helps participants to better manage their treasury position with repo transaction and contributes to the conduct of the monetary policy, while the settlement of funds between participants is carried out in real-time.

Having seen lots of developments driven by technological advancement and the dominant use of paper-based instruments in retail payments, NBC introduces Project Bakong, a wallet based electronic currency operated on DLT, with public mobile application (eliminating the need for banks and PSIs to develop their own while allowing those with existing mobile application to easily integrate through open API), aiming to promote electronic payment and financial inclusion. Bakong processes payment and settlement transactions.

2.1.2 Payment Services

Apart from developing infrastructure, digital and electronic payment services provided by the private sector is also a key enabler to promote financial inclusion, as such, a conducive and transparent regulatory framework is required to support the growth of the sector. Broadening payment services and digital network is an important factor to promote access to finance, i.e. financial inclusion. In other words, adoption by households, and small and medium enterprises in the financial sector is an important element to support economic growth in the long term. One of NBC's principal responsibilities is to ensure that convenience, affordability, fairness, and safety features are met by engaging closely with relevant stakeholders without discriminating the types of institutions.

Currently, besides banking and financial institutions, there are other 24 PSIs operating on a standalone basis to provide services to the public. The range of services offered by these institutions are diverse but can be categorized into 4 main groups, namely:

According to data compiled by the NBC, mobile payment by banks and PSIs accounted for 22.9% of the gross domestic products ("GDP") in 2019. Money remittance within the country was equivalent to about 213% of GDP. Despite this remarkable achievement, the development of payment services in Cambodia still faces significant challenges. All PSIs are allowed by regulation to participate in the central infrastructure, but most institutions are still reluctant to do so and instead expand their services through their own investment in agent networks and points of sale. Access to a central infrastructure reaps a host of benefits including :

1. The expansion of payment types;
2. Increase in the number of users;
3. Eligible for liquidity support;
4. Access to interbank clearing and settlement.

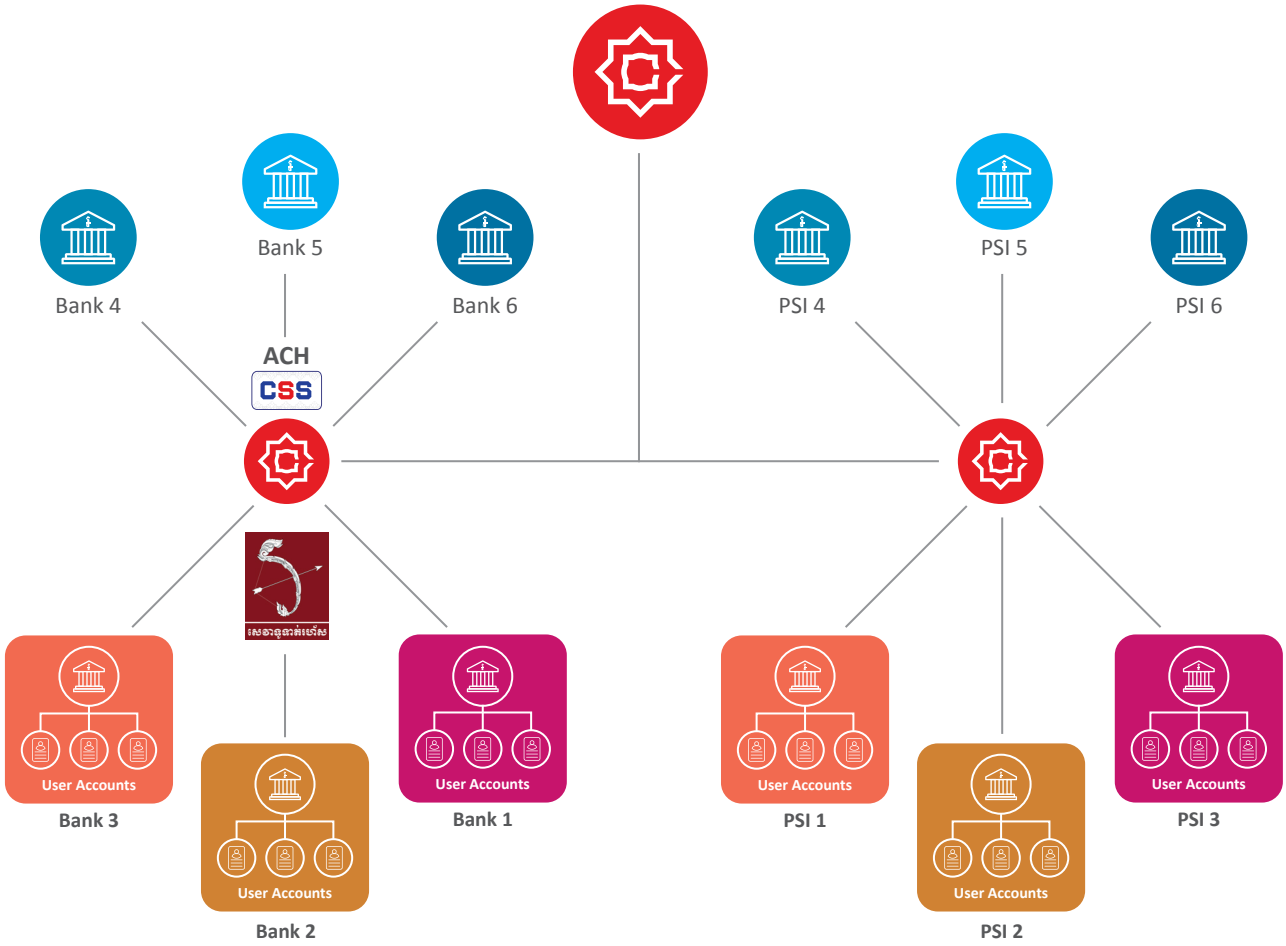
Another issue is that most transactions are carried out over the counter ("OTC"). A majority of the OTC transactions are money remittance and cash-out at agents. These transactions do not require consumers to have accounts which will undermine potential financial products in the future.

Therefore, with the introduction of Project Bakong, NBC aims to help consumers access finance more widely, efficiently and conveniently, as well as beneficial to financial institutions.

2.1.3 Efficiency Gain & Solution to Interconnectivity and Interoperability Problems

The adoption of Bakong will allow the public to enjoy value-added benefits at reduced costs. When customers transfer funds from their own banking account to Bakong account or vice versa, they will bear no costs as the transactions would be free of charge (Cost). On the other hand, Bakong clearing system reduces the processing cost and time compared to other retail payment systems that require clearing process between banks (Speed). For instance, in retail payments, there is a need to establish a clearing process between banks, and it is inevitable to incur expenses related to the establishment of a separate clearing house and pledging collateral for risk management in the clearing process. On the other hand, Bakong doesn't require this since there is a connection linked to peer-to-peer ("P2P") network by both payer and payee due to its decentralized nature and the platform proves resilient to cyber-attacks (Security). Since banks and individual users are now brought into one DLT platform both banks and users no longer face with interconnectivity and interoperability problems (see Figure 1 Interoperability of Bakong Platform).

Figure 1: Interoperability of Bakong platform



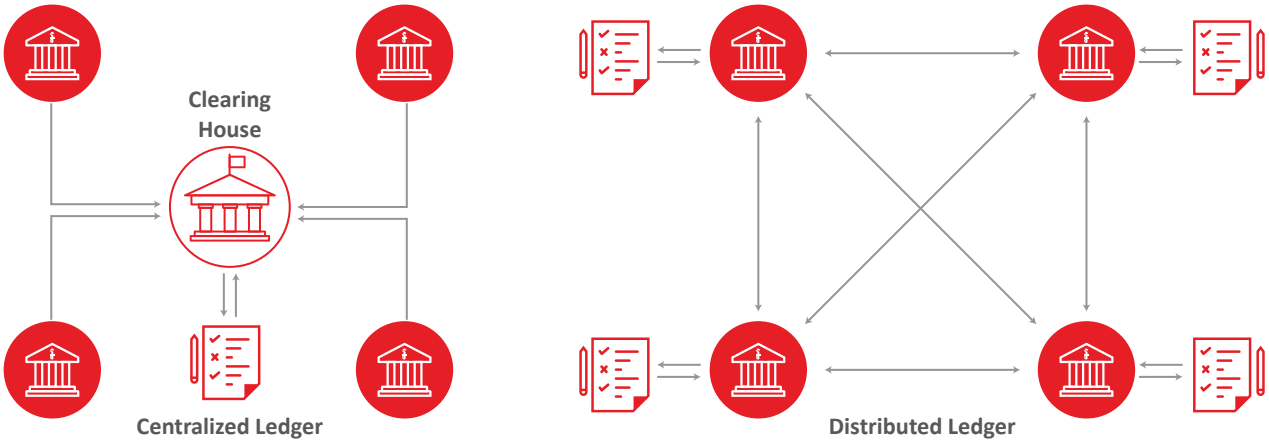
2.2. Technology Consideration

Blockchain and DLT are often discussed by financial institutions because they offer a promise to improve the efficiency of financial business practices. Since NBC adopted a permissioned distributed ledger, in which participation is not public and registration is needed, DLT was used as a platform for payment.

2.2.1 Distributed Ledger Technology

A distributed ledger can be thought of as a database that exists across several locations (see Figure 2 for distinction between centralized and distributed ledger and see Box 1 in the Annex for further exposition). Distributed ledgers consist of nodes on a network of equal peers that record, transmit, and synchronize transactional data in each node's electronic ledger, instead of keeping all data in a centralized data store. Because of increased resilience to distributed denial of service attacks and hardware failures, DLT has the potential to improve services offered by financial institutions while decreasing costs. DLT allows use of commodity hardware rather than specialized servers, resulting in cost savings. The redundancy of ledgers improves security, reliability, and integrity.

Figure 2: Centralized vs. Distributed Ledgers Schematic overviews of how centralized and distributed ledgers are structured show that the main difference is the lack of centralized clearing house

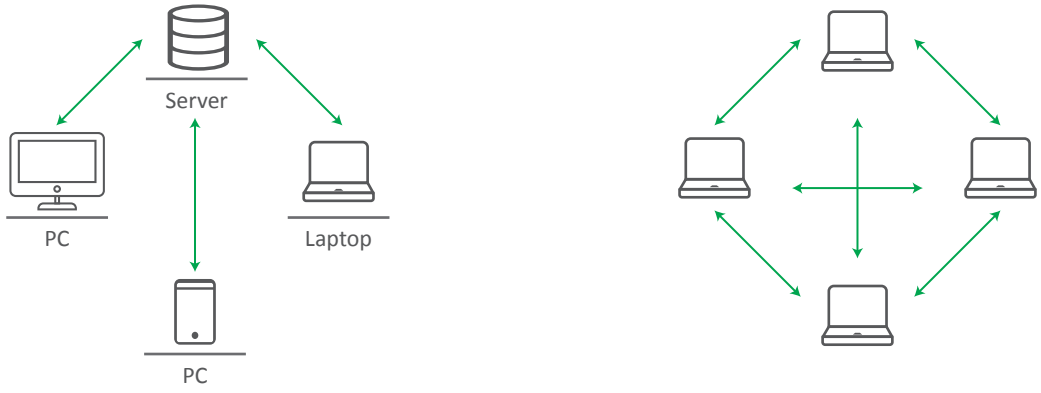


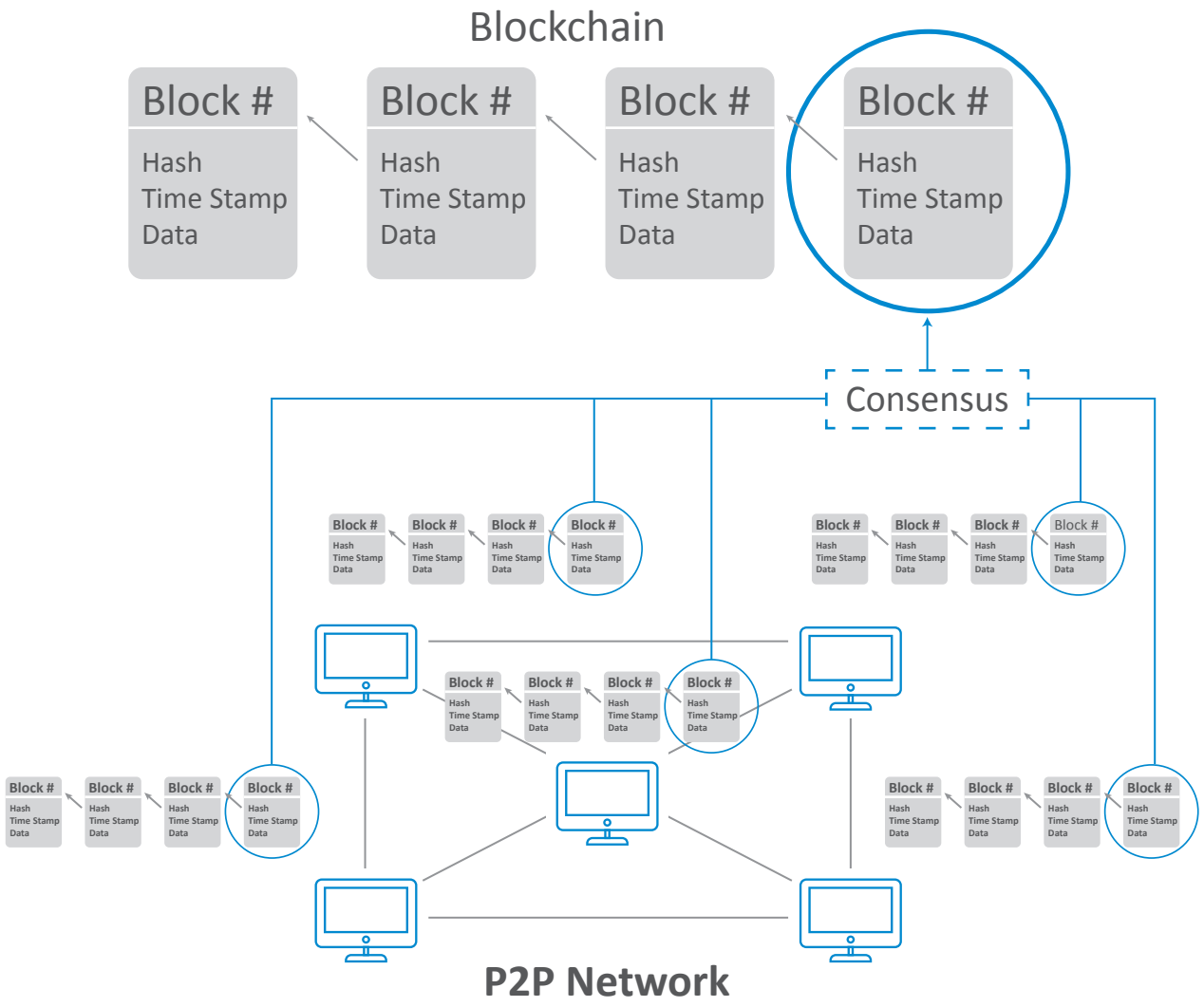
2.2.2 Blockchain Technology

Blockchain is a new technology that consists of an append-only distributed ledger. New entries are added by appending them to the end of the ledger's dataset and the ledger is built as a chronological chain of blocks, hence the name blockchain. Blockchain technology has many variations, but is typically considered as being:

1. a store of immutable (or at least tamper-evident) data;
2. decentralized; and
3. consensual.

Blockchain consists of blocks that contain a time-stamped set of transactions that are bundled together. Each new block is linked to a preceding block. Combined with cryptographic hashes, this time-stamped chain of blocks provides an immutable and tamper-evident record of all transactions in a network, from the genesis block until the last/most current block. In contrast with a traditional relational database where data can be deleted or modified, there are no administrator permissions within a blockchain that allow users to either delete or edit the recorded data.





The multiplicity of nodes negates the need for a pre-existing trust relationship and are connected through a peer-to-peer network. Each node will host the same exact copy of a blockchain ledger creating a decentralized structure. However, for such a structure to be useful, there must exist some mechanisms by which the nodes can mutually agree on the next valid block in the chain to be added. That mechanism is a consensus protocol.

The consensus protocol ensures that all nodes (entities that maintain the blockchain and (sometimes) process transactions) are synchronized with each other and agree to record legitimate sets of transactions. The effective design of a consensus mechanism is crucial for a blockchain in order to work correctly. Some of the deployed schemes for establishing such a distributed consensus include: Proof-of-Work, Proof-of-Stake, Proof-of-Importance, Proof-of-Capacity, Proof-of-Human-Work, Proof-of-Authority, and Proof-of-Elapsed-Time.

In addition to immutability, decentralization, and consensus, a blockchain network also has two additional key characteristics: (1) provenance; and (2) finality. Provenance is the quality that proof exists for the origin, history, and current status of a specific asset. Finality is the trait that proof exists with respect to the fact that only one instance of a specific asset is present in one location. In other words, there is insurance that a transaction results in one asset being transferred to one owner which all network participants with proper permissions can agree to be true. This is the solution to the problem commonly referred to as “double-spending.”

A blockchain can use smart contracts, or a set of rules that semi-autonomously govern a business transaction. A smart contract is stored on the blockchain and is automatically executed as part of a transaction. It should be noted that smart contracts here is from the standpoint of the use case of creating smart (i.e. digital) contractual relationships between parties, and not the technological standpoint (i.e. computer programs running on a blockchain, also called chaincode). In his work, Nick Szabo proposed smart contracts [1] as a mean to build on the complex social structures that have evolved over the last few millennia. Smart contracts provide a means to adapt modern law and regulation by incorporating observable, verifiable, private, and enforceable contracts that are written in code and operate according to defined rules. These smart contracts can be used to reduce fraud and make business processes more efficient.

By affording rights, or permissions, to the appropriate parties to monitor smart contract activity, automation of otherwise tedious processes can increase efficiency and reduce errors. A blockchain can be both permissionless and permissioned. A permissionless (public) blockchain entitles anyone to join the network. A permissioned (private) blockchain, requires a pre-verification of the participating parties which are made known to each other participant within the network. The choice between the two types is mainly driven by whether an application can ‘commoditize’ the trust. Bitcoin [2] and Ethereum are examples of permissionless blockchains which facilitate parties’ ability to transact without necessarily having to verify each other’s identity. On the other hand, inter-bank financial transactions are an ideal use case for permissioned blockchains. One would not want non-vetted companies participating in the network, able to access sensitive financial information.

Central Bank Use of Blockchain

Blockchain technology has gone through substantial deliberation in recent years within the financial and banking disciplines. It has drawn considerable attention from the public given its possibility of recording all financial transactions in a secure and verifiable decentralized (peer-to-peer) fashion, without intermediation by a third party to process transactions and without counterparty risk for trades of purely digital assets. In other words, the decentralization of these transactions, allows users to conduct financial transactions completely independently of control from either side. While the focus of blockchain applications to date has been to build ledgers of transactions involving virtual tokens (i.e. cryptocurrencies), potential use cases have gained increased curiosity in several fields. In a January 2016 report, Mark Walport, the UK government's chief scientific adviser, argued that blockchain technology could expand far beyond a trading tool: "Distributed ledger technologies have the potential to help governments collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods, and generally ensure the integrity of government records and services," the report concluded (Walport, 2016 p.6). Numerous central banks across the globe have begun working with blockchain and DLT experimentation in pursuit of increasing process efficiency and innovation.

Similarly, there have been many dialogues about "Central Bank Digital Currencies" or CBDCs, in which a joint report by the Bank for International Settlements (BIS) Committee on Payments and Market Infrastructures provides a definition of a CBDC as "a digital form of central bank money that is different from balances in traditional reserve or settlement accounts" [3]. At a regional level, Japan, China, and Singapore are actively engaged in blockchain research and experimentation. The Bank of Japan performed a joint experiment with the European Central Bank, exploring how DLT could be applied to process streamlining, particularly interbank settlement, through an effort known as Project Stella. The Monetary Authority of Singapore has worked on Project Ubin [4], which modernizes RTGS using digital Singaporean dollars for wholesale interbank settlement. Rather than focusing on the wholesale segment, People's Bank of China assessed the retail payments network and tested a prototype CBDC for the public.

At a global level, there is a mix of whole sale and retail areas of blockchain-based CBDC. Bank of Canada is widely known for its Project Jasper which models interbank wholesale payments; while the Swedish e-krona project by Sveriges Risk Bank was meant to develop the concept that the bank could issue retail CBDC (e-krona) to public consumers as a complement to cash. The Central Bank of the Bahamas announced a Payments System Modernization Initiative ("PSMI") where blockchain or other robust technology was required. Other publicly announced blockchain or DLT projects include Israel, Australia, Brazil, Russia, Estonia, United Arab Emirates, Kuwait, and Saudi Arabia.

Overall, key focal points of blockchain initiatives by central banks center around: i) retail transactions for the public, and ii) wholesale payments and settlements systems for interbank transactions. A research paper from the Bank of England discusses costs and benefits in relation to macroeconomic improvements resulting from central banks issuing digital currencies. Rather than focusing on the macroeconomic policy of CDBC, Project Bakong targets infrastructure modernization and responds to real demands that already exist for wider use of electronic means of payment by expanding access to financial services to people in the rural areas of the Kingdom.

The above review of the challenges in the payment system and services in Cambodia, alternative payment technology, i.e. blockchain and DLT, and the experiment of and research into blockchain as an alternative to current payment services among central banks around the globe lead NBC to identify several areas of benefits in the current payment system through adopting blockchain technology (i.e. Project Bakong).

2.3 Financial Inclusion

Financial Inclusion is a primary agenda of the NBC. One of the effective measures to promote financial inclusion is to ensure a cashless society where transactions could be performed digitally, and money transfer / mobile banking is accessible and affordable to every citizen. So far, this has been done by private sector players especially PSIs that have been paying much effort to introduce innovative products, that can better serve the market as a whole - people in urban areas as well as the unbanked through their large expansion of mobile and agent network. From the NBC statistic, the number of e-wallet account increase 64% from previous year to 5.22 million in 2019 while the number of deposit account reaches 7.62 million within the same period. On the other hand, money transfer by both banks and PSIs goes up to USD 57.99 billion in 2019 constituting 213% of the GDP. Such efforts could be further encouraged by the authorities through the developement of legal and physical infrastructures. Thus, Project Bakong has been introduced to address this by gathering all participants into one system where finance can be widely spread through their Bakong accounts that can be created through Bakong App installed in their smart phones. It is expected that the Bakong will have potential to bring those unbanked population into formal financial sector that could contribute to the reduction of poverty in Cambodia. With user friendly application and simplified KYC procedure, Bakong user are able to access Bakong channels for all banking transactions (i.e payments, remittances, credits and savings).

2.4 Cashless Payment and Ease of Local Currency

Cambodia is still considered as a highly dollarized economy while most of the transactions are still cash- based. This could hinder the effective implementation of monetary policy as well as payment system development. Thus, the NBC as the monetary and payment system authority, has developed the Bakong aimed at promoting the use of local currency and electronic payment in Cambodia.

The Bakong is developed with a feature that allows for real-time fund transfer and instant payment transaction and given its interconnectedness and interoperability among different payment service providers and the adoption of QR code payment, it provides more convenience and wider acceptance channel for Bakong users to make electronic payment at any merchant. In addition, with the possibility to link with bank accounts, customers are able to make fund transfer from Bakong accounts to their bank accounts and vice versa. As Cambodia consists of younger population, the introduction of modern payment system via QR code can be easily adopted. This would induce consumer to make electronic payment instead of using cash. Besides, the development of Bakong is expected to encourage the use of local currency in the sense that it facilitates the payment of high value transaction instead of using US Dollar. Furthermore, the Bakong can be utilized as a tool in promoting the use of local currency by providing advantages to transaction in Riel over those in US dollar.

3 Project BAKONG

3.1. Overview

Bakong started as early as 2017 where several alternative technologies and their applications in the payment system were explored and tested. As a result, DLT was selected as it was believed to be more efficient, reliable and resilient to cyber-attacks than the current payment systems, especially when connecting to payment service providers.

Project Bakong is designed as a new platform for a payment system that uses DLT to enhance efficiency (cost, speed and security) of the payment system. The nodes in Project Bakong core are installed in a closed-loop infrastructures that are located at the NBC, and they can be shared with participants through the payment gateway. Only individuals who register in the system can carry out their business transactions. The consensus transactions based on (2n+1) of (3n+1) nodes mechanism while “n” represent the number of nodes.

The implementation of Bakong would connect all financial institutions and payment service providers under single payment platform which will allow for fund transfers to be processed on real-time basis without the need of a centralized clearing house. Institutions that are current participants of FAST would be able to interface directly with Bakong without making changes to their existing infrastructure.

Bakong also provides an extended feature (P2P) which allows for end-users to perform real-time retail fund transfers using its all-in-one mobile payment and banking application. The application enables end users to transfer funds easily by scanning QR codes, keying in phone numbers, or just selecting from their contact list, as well as easily deposit funds to any accounts within the Bakong's network of participating banks.

The end users can download the application from the application store or market and register with their preferred participating banks or PSIs in order to have a Bakong account and participant's bank/institution account. The participating banks are responsible for performing KYC / Anti-Money Laundering ("AML") procedures for their end users, storing their information and managing their Bakong accounts.

The participating banks shall have a Bakong settlement account at NBC. End user's balance at Bakong account is considered as cash equivalent, and it should be recorded in the participant's Bakong settlement account at NBC. The balance is subject to update at the end of each business day.

Under Bakong, end users have two separate accounts for KHR and USD to allow for transactions in the respective currencies. A conversion or transfer from one currency to the other is not possible on the system. However, the participating banks can provide FX service to end users.

3.2. Design Features

To ensure smooth implementation of Project Bakong, the platform preserves most of the existing payment system features including FAST and is upgraded by using Hyperledger Iroha, a permissioned blockchain network, as a core system. Some other features include:

Bakong maintains existing user interfaces ("GUI"), Application programming interface ("API", and client module (gateway) of the current FAST system.

Bakong preserves existing business processes and authentication requirements such as user roles in the FAST system, utilizing Hyperledger Iroha's role based on access control permission system and native multi-signature capabilities to model business processes.

Bakong enables plug-and-play mode for participating in the new payment platform. Existing participants can join the platform without re-investing in system integration. Such application shows that the current FAST system is enhanced through the replacement of relational database by the permissioned blockchain network of Hyperledger Iroha nodes. This is a rather conservative use of blockchain technology, as it is mainly a change to the backend infrastructure in a way that will be invisible in many use cases.

However, by utilizing Hyperledger Iroha, the system offers several other key features as follows:

- Upon joining the Bakong network, the participant (registered institution) will receive a domain that allows him or her to create accounts for their customers (end users). Customers can access their accounts via the Bakong mobile or desktop apps or via a participant's custom app.
- The following applies to Bakong transactions:
  - transactions can be carried out in a decentralized manner (end users can conduct transactions directly with other end users in the same or with different participating institutions) where NBC performs the validation of the transactions within the permissioned blockchain network;
  - transaction can be done not only between Bakong accounts but also traditional bank accounts;
  - initiating and settling payment transactions are in real-time with settlement finality;
  - transaction time will drop to less than 5 seconds with high transaction throughput;
  - debiting the sender's balance and crediting to a receiver's balance in a single, automatically executed operation; and
  - payment transaction data are stored in distributed storage (Hyperledger Iroha blockchain network).

Since Bakong is built on top of the Hyperledger Iroha blockchain it preserves the privacy and finality of transactions. Transactions are validated using a Byzantine Fault Tolerant ("BFT") consensus algorithm that ensures consistency across the distributed ledger, resistance to transaction censorship and DDoS attacks, while avoiding double-spending and counter party risk in swapping digital assets. Transactions are transparent to validating nodes, which are run by the NBC as a central bank and a regulator, without disclosing identity of parties involved in performing the transaction. In this sense, Bakong requires participating institutions to manage KYC for their end users or clients. This segregated approach reinforces privacy of users and ensures the public's trust.

3.3 Bakong Architecture

3.3.1 Bakong Core

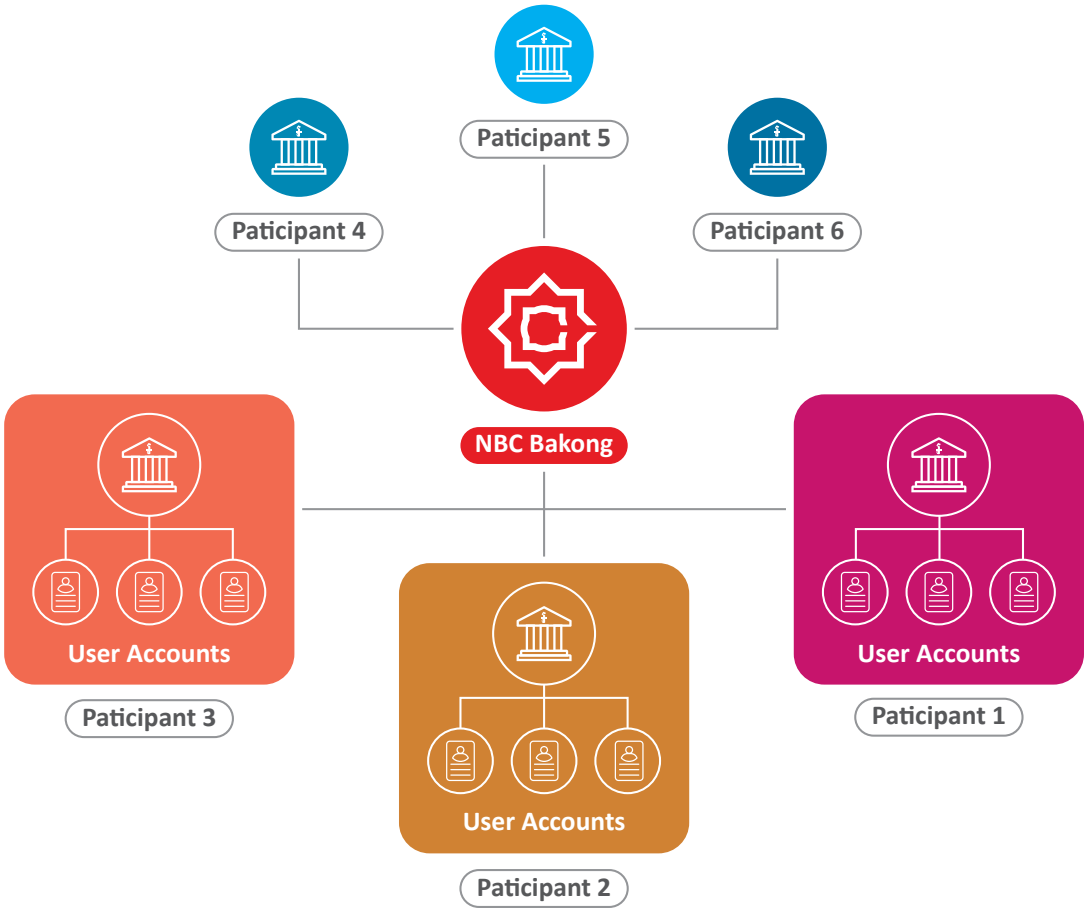
Bakong Core is the system containing the distributed ledger and transaction-processing capabilities. It consists of the following features:

- all transactions processed by the payment system are stored;
- transactions are stored in blocks, which are linked and secured using cryptography;
- each block has a hash pointer which serves as a link to a previous block, a timestamp, and transaction data;
- blockchains are inherently resistant to modification of data; and
- all ledger nodes have the same data and they validate all transactions.

3.3.2 Payment Gateway

Financial institutions that join Bakong are the participants. Each participant needs to register with NBC to obtain permission to join the network. After successful registration, participants will access the Payment Gateway, so their customers can create accounts under their domain (Figure 3). The Payment Gateway also allows financial institutions to monitor their users' transactions and to manage the users (accounts) within their institutions.

Figure 3: Bakong as a Backbone of Payment System



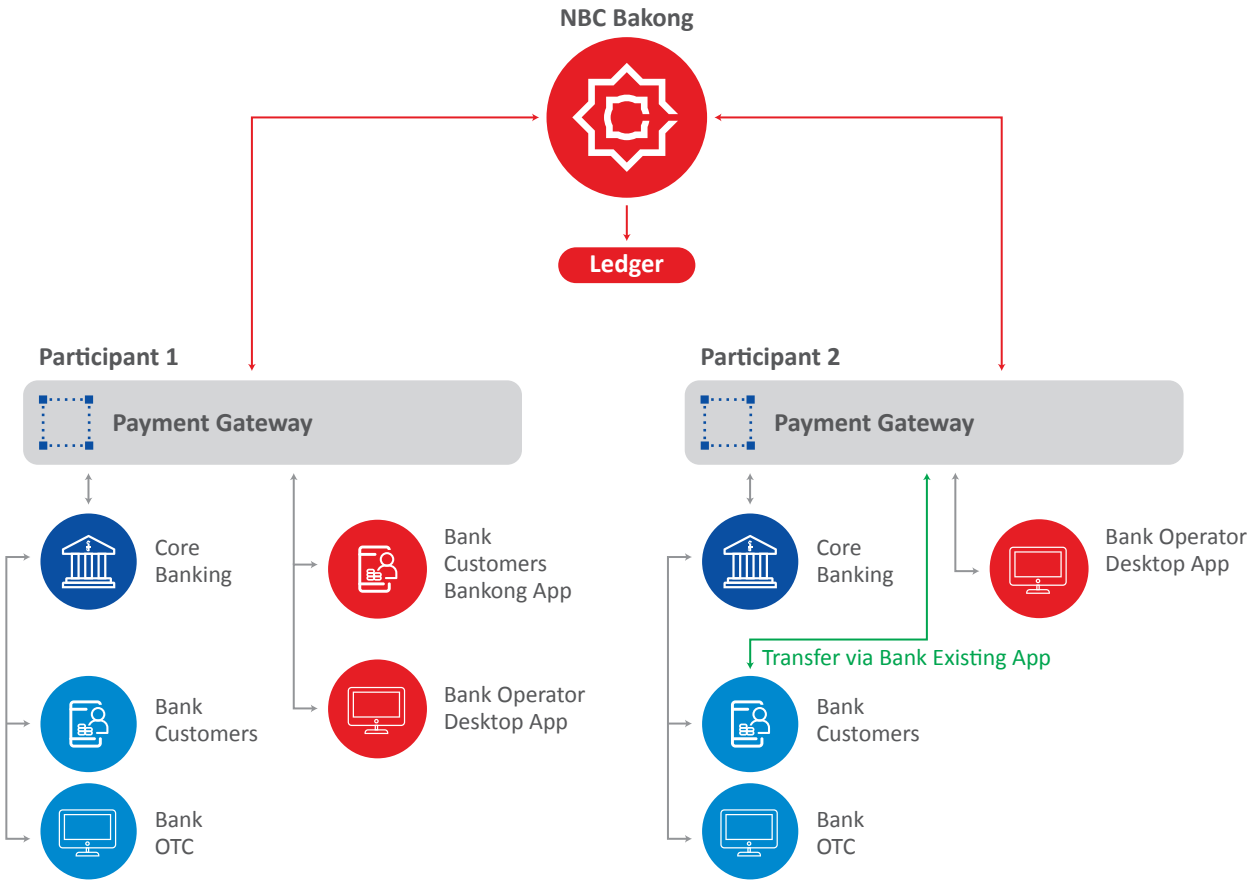
On the Bakong platform, each participant's Payment Gateway is a domain under Bakong Core, in which end users can create accounts under the participant's domain. The Payment Gateway also provides participants with a way to monitor the transactions conducted by their customers via accounts in their domain (but not unrelated transactions carried out by customers in other domains). The Payment Gateway is also a platform where participants can manage KYC operations and transaction limits. Although each participant has a respective Payment Gateway to join Bakong Core, their customers holding accounts under their domains can transact directly with other users in different domains.

As illustrated in Figure 3, with 6 participants joining Bakong system, Participants can transfer assets to their customers registered under their domain. Customers of each domain can make transactions within the same domain or across domains. All transactions submitted to the blockchain are validated by the nodes owned by NBC.

3.3.3 End Users

By joining the Bakong network, participants allow their customers to create accounts under their domains. To access their accounts, users can use either the desktop or mobile application provided by NBC (Figure 4). Participants who already have a mobile application can integrate with Bakong through an API provided by NBC.

Figure 4: Extended Feature of the Bakong



3.4 Transaction in Bakong

3.4.1 Participant Main Accounts

After joining the Bakong network, a participant should inform NBC of his or her Bakong main account which can be accessed via the desktop application. After NBC registers the participant's main account into Bakong system, the participant can use their main account to conduct transaction which includes transferring fund from/to the current account or settlement account at NBC as well as from/to other participants' Bakong accounts and current accounts.

3.4.2 End User Accounts

Once end users have created accounts with participating institutions, they are ready to carry out transactions but only up to a limited daily amount. If a user wants to increase his or her transaction limit, he or she needs to contact his/her participating institution to perform KYC and negotiate the increase of the limit. To receive funds, users notify payers or senders of their: (1) account ID; (2) phone number; or (3) QR code; following which, the senders or payers can send funds to their account immediately. While they have funds in their account, users can perform transactions such as send, pay, and deposit.

4 Key Observations and Findings

4.1 Transaction Finality

Settlement finality is an important component of consumer protection in the payments ecosystem, where fast speed of payments execution, raises challenges relating to consumer protection against fraud or errors. Such challenges primarily arise when cancelling, reversing or recalling any fraudulent or erroneous transactions. As such, settlement finality acts as a safeguard and guarantees that transfer orders which enter into such systems are also finally settled, regardless of whether the sending participant has become insolvent or transfer orders have been revoked while in transitory.

As such, the Bakong platform has a consensus mechanism to verify the validity of transactions and avoid double-spending. Where the validation nodes perform verification on a per-transaction basis and at the time of execution. Upon successful verification, the transaction record will be stored in the block distributed on the network. At that instance, the balance of the sender is debited, and the balance of the receiver is credited immediately. The transaction would be considered final, irrevocable and enforceable.

4.2 Scalability and Performance

Results of the technical test carried out by the Bakong Test Lab have shown that the new payment system run on the Bakong platform is highly efficient. Where the execution time for one transaction during a normal load was noted to take less than 5 seconds. In addition, transaction throughout is between 1,000 and 2,000 transactions per second (depending on the network size, hardware, and system characteristics and configuration), which is considerably higher than the number of transactions in other blockchain platforms. This suggests that there is potential for this project to scale.

4.3 Resiliency

Bakong platform is designed to be highly resilient to various forms of cyber-attacks. Depending on the consensus algorithm used in the system setup, transactions are processed normally, when the number of network nodes are unavailable due to machine failure, network interruption, among others. The number of nodes that can be temporarily unavailable depends on consensus algorithm and network size. New network nodes could be added, and existing nodes could be shut down or removed from the network while the system remains fully functional.

Additionally, as the Bakong account private key of each end user is stored in their individual device, only that particular end user knows his or her private key. Therefore, any cyber-attack on a particular IP address affects only the account using that IP address, but not the whole Bakong system. In case the account is compromised

the fund is transferred to another account, and user reports to their institution, which later requests NBC to block that account. This mechanism is a deterrence to hacking.

4.4 KYC and Privacy

Bakong uses a permissioned blockchain technology, where only authorized nodes can join the network. Transaction records are immutable but transparent amongst the nodes. On the network, only addresses are stored without disclosing the details of the end-users. Therefore, participating institutions are responsible for performing KYC/AML procedures on their clients. The customer's information is stored at the participant's system. Such mechanism segregates between personal and transactional information, which ensures confidentiality of end-users and trust on the platform.

4.5 Bakong Settlement System

Since Bakong can be made from Bakong Platform to a Bank Account or vice versa, there is a link to a settlement system for central bank money. It would also be possible to move Bakong in and out of the platform smoothly and safely so that there is control at each given point over how many Bakong there are in total on the platform. This would probably require transfers to and from Bakong Platform to be made instantly, which would mean that the platform also needs to have a connection to a Bakong Settlement System in the central bank money that implements instant payments. Payments that are made from Bakong Platform to a bank account or from a bank account to Bakong Platform would thus be settled immediately between the NBC and all participants in the Bakong Settlement System.

4.6 Standardized QR Code

To achieve interoperability and interconnectivity for Bakong platform, there must be a common standard usage which is consistent with the international standard to enable the platform to work safely and efficiently. Based on best international practice, Bakong will adopt EMV QR Code Payment that facilitates the worldwide interoperability and the acceptance of secured payment transactions by managing and evolving the EMV specifications and related testing processes. According to EMVCo, "adoption of EMV specifications, associated approval and certification processes promotes a unified international payment framework, which supports a range of advanced payment methods, technologies and acceptance environments" (EMVCo, 2019).

5 Possible Implications

Given the aforementioned business and technical specifications, there is potential implication that needs to be carefully considered. This section depicts the potential benefits and risks associated with the new upgraded payment system - Bakong.

5.1 Efficiency Gain

Since transaction on Bakong platform is carried out on a peer-to-peer basis and without centralized clearing house, time used for each transaction on the Bakong platform is similar to transaction time on other real-time payment system. Thus, cost is reduced, and time is saved as the transaction does not need clearing process between banks, which is an advantage over other retail payment systems because transactions on these payment systems require clearing process which must be conducted through a centralized clearing system. Importantly, investment in centralized clearing system infrastructures is not needed, while time between the initiation and the final settlement of the transaction is also substantially saved.

5.2 Financial Inclusion

Bakong will function as a mechanism of promoting cashless payment in a digital economy. The payment system will facilitate adoption amongst the unbanked population as financial access through Bakong platform is much more convenient than the current payment system. Given the design of the technology behind the Bakong platform, financial institutions may invest at low cost in Project Bakong to expand payment services via smart devices in order to promote access to financial services of the unbanked population. The Bakong initiative is also coincident with the interest of Cambodian youth in exploring new and advanced technology that offers low cost, secured, fast, and convenient payment services. Bakong is a vehicle for expanding access to financial services to the rural population with the expansion of agent banking and customized platform for agent to extend the services. Bakong focuses on infrastructure modernization to respond to the market demand and the customer behavior.

5.3 Monetary Policy

Project Bakong is likely to have moderate impact on the central bank's monetary policy and the financial stability because money in circulation will still be managed by the Central Bank provided that Bakong is pre-funded by fiat money through banking institutions and payment service institutions or agents. To have electronic money in Bakong account the customers must for example (1) first deposit cash in their accounts at financial institutions, open a Bakong account under the domain of that financial institution and transfer the money to the Bakong account or (2) open a Bakong account via the Bakong App under the domain of

any participant and make a direct cash deposit through any participant. Consequently, through Bakong the national bank can collect physical cash and create electronic money in the financial system. Doing so the national bank can conduct its monetary policy through the change in size of the electronic money in circulation. In addition, Project Bakong will also help the national bank to conduct foreign exchange policy to stabilize exchange rate as NBC can better forecast the demand of local and foreign currency using information stored in the Bakong system.

From the financial stability perspective, systemic risk of settlement will be mitigated since Bakong follows a pre-funded model where all participants must deposit in their Bakong settlement accounts before being able to make transactions. In addition, all transactions must be authorized, so inadequate balance in Bakong settlement account cannot be transacted.

5.4 The composition changes in the financial intermediation

Bakong will not eliminate intermediary function of banking institutions and payment service institutions since the design of Bakong is different from other platforms. It requires banking institutions and payment service institutions to review and manage customer information, conduct KYC procedure, and open bank account for customers to receive an authorization and account for accessing Bakong application. Therefore, transactions will be processed between Bakong and bank account.

5.5 The risk of bank run

With or without the presence of Bakong, the risk of bank run that may stem from operational management and other uncertainties within the banking and financial institutions remains. Depositors and investors could withdraw their money if they panic or feel insecure about bank solvency. With presence of Bakong, the conversion from cash to digital money affects the movement speed of money comparing with physical cash, so customers may move their electronic money speedily via Bakong from one institution to another, but the movement is subject to the maximum limit required by each financial institution or settlement account held at the central bank.

5.6 Cyber security

Cyber-security has been a priority issue among relative jurisdiction around the globe in order to mitigate or prevent the risk in financial sector particularly the payment infrastructure. Generally, almost every payment, clearing and settlement system comes with cyber threats such as malware and fraud. Such cyber threats create a challenge for Bakong payment, which is open to many participants and points of attack. Additionally, the ease for amount allowed to transact could possibly pose a potential risk of fraud. A healthy mitigation approach of cyber risk is required for implementing Bakong payment. The presence of risk management framework is uncertainty to ensure the safe in payment system in respond to the evolvement of technology. Because central bank plays a significant role in stimulating a smooth functioning of an economy, very robust requirements for reliability, scalability, and resilience are necessities. Central banks therefore typically have to be very rigorous operational requirements for introducing systems and services.

5.7 Other key risks

To mitigate credit and liquidity risks, Bakong was designed so that its operations are settled in near real-time before participant of the payee credits the funds in the account of its customer. As such, it does not extend credit nor overdrafts to its participant's accounts; transfers that do not have enough liquidity to be processed are queued until they can be processed.

According to Bank for International Settlement: "the speed and continuous availability of fast payments have an impact on operational risk, and due to their speed, any operational incident that results in the delay or interruption of fast payment services could be immediately observable by end users" (BIS, 2016 p.50).

As for operational risk, NBC is supported by a framework for the comprehensive management of risks that defines roles and responsibilities for the identification and management of risks, their assessment, and the establishment of its risk's tolerance policy, the basis on which to determine if controls are required to mitigate risks.

Measures of business continuation are in place to face various possible risk scenarios, and these measures comprise a redundant infrastructure, an alternate operation site, a remote operation scheme, and contingency operation procedures that permit a quick recovery of the system, even in a major event that impacts normal operation.

6 Conclusion

Given the technological considerations along with the multitude of operational/stress tests that went into the development of Bakong, NBC is positive that this new generation payment system using the blockchain/DLT technology is feasible. Without hampering the existing payment system and substantial investment by existing participants, an upgraded version of FAST with key design features proves sufficient to further explore the Project Bakong prior to introducing it to the general public. With regards to the caveats discussed above, the NBC acknowledges that there is a need to mitigate risks, while constantly evaluating the effectiveness and efficiency of the project. The NBC in collaboration with interested participants will strive to bring the effective and cyber-resilient payment system out of this project. As a next step, the NBC has started a pilot test with a first batch of 8 participating institutions and will continue to analyze the technology and business model of the Project Bakong. The pilot test has been completed by the second quarter 2019. Where appropriate, all participants have taken part in the second round of testing in the third quarter of 2019. Bakong will go live for the public in early 2020. A follow-up report on the outcome of the pilot test will be prepared and circulated among stakeholders of the project.

Bibliography

1. Alluva (2019). What is consensus in blockchain? Retrieved from https://www.quora.com/What-is-consensus-in-blockchain
2. Bank of Canada. (2017). Project Jasper – A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement, Ottawa: Bank of Canada
3. Bank for International Settlement (2016). Fast payments—Enhancing the speed and availability of retail payment, Committee on payments and market infrastructures, Basel: Switzerland
4. CPSS, A. (2003). Glossary of Terms Used in Payments and Settlement Systems. CPSS-Committee on Payment and Settlement Systems. URL: https://www.bis.org/cpmi/glossary_030301.pdf
5. ECB and BOJ (2018). STELLA – a joint research project of the ECB and BOJ: Securities Settlement Systems: Delivery-Versus-Payment in distributed ledger environment, European Central Bank and Bank of Japan
6. EMVCo, (2019). EMVCo The Basics. Retrieved from https://www.emvco.com/media-centre/press-room/emvco-the-basics/
7. Kumhof, M., & Noone, C. (2018). Central bank digital currencies-design principles and balance sheet implications.
8. MarketWatch (2019, March 7). The Bahamas, Project Sand Dollar: The Central Bank Identifies Preferred Technology Solutions Provider for Bahamas Digital Currency, [Press Release]. Retrieved from https://www.marketwatch.com/press-release/bahamas-project-sand-dollar-the-central-bank-identifies-preferred-technology-solutions-provider-for-bahamas-digital-currency-2019-03-07
9. MAS (2017). Project Ubin Phase2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies, Monetary Authority of Singapore: Singapore
10. N. Szabo, N. (1996). Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought, (16), 18.
11. Nakamoto, S. (2018). Bitcoin: A Peer-to-Peer Electronic Cash System [Electronic resource]. Bitcoin [Official website].
12. Zhang, Y., Han, Wei (2017). Report in Chinese publication Caixin written by By Zhang Yuzhe &Han Wei, https://www.caixinglobal.com/2017-01-26/pboc-set-to-be-first-to-issue-digital-bills-101049103.html
13. Sverige Riksbank. (2018). The Riksbank's e-krona Project Report 2, Sockholm: Sverige Riksbank
14. Walport, M. (2016). Distributed Ledger Technology: beyond block chain (A report by the UK Government Chief Scientific Adviser). UK Government.

Annex

Box 1. Blockchain and Distributed Ledger Technology – Background

Blockchain and distributed ledger technology (DLT) are generally considered as a mean to improve the efficiency of financial business practices. However, there is often confusion surrounding the differences between blockchain and DLT. The following sections explain the fundamentals of and differences between blockchain and DLT.

Distributed ledger Technology

A distributed ledger is, at its essence, a database that exists across several locations. Distributed ledgers consist of nodes on a network that are equal peers that record, transmit, and synchronize transactional data in each node's electronic ledger, instead of keeping all data in a centralized data store. Because of increased resilience to distributed denial of service attacks and hardware failures, DLT has the potential to improve services offered by financial institutions, while decreasing costs by allowing use of commodity hardware rather than specialized servers residing in highly available data centers.

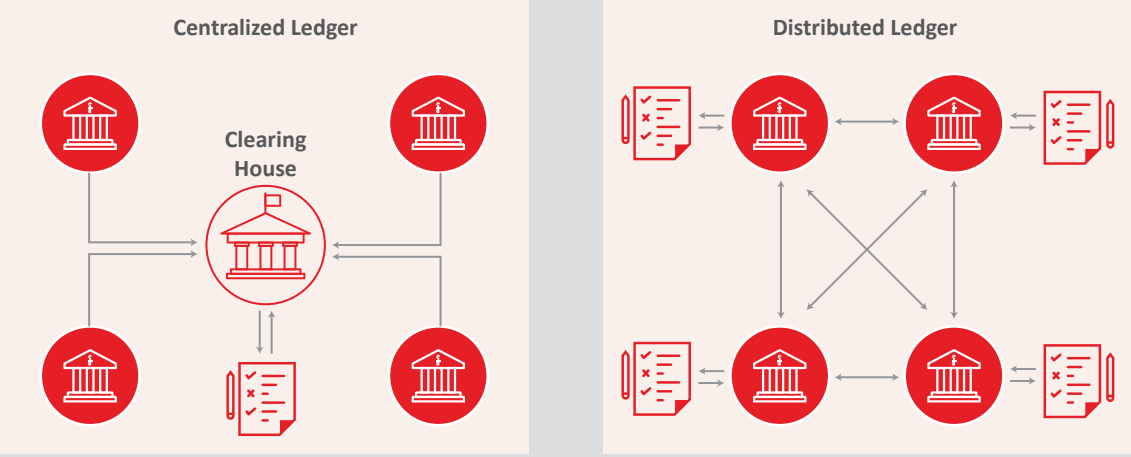


Figure 1a: Centralized vs. Distributed Ledgers Schematic overviews of how centralized and distributed ledgers are structured show that the main difference is a lack of a centralized clearing house.

Blockchain Technology

Blockchain is an ascending technology that consists of an append-only distributed ledger. New entries are added exclusively by appending them at the end of the ledger, the ledger is built as a chronological chain of blocks; hence its name. A blockchain technology is characterized as being (i) immutable, (ii) decentralized, and (iii) consensual, explained as follows. Blockchains consist of blocks that contain a time-stamped set of transactions that are bundled together. Each new block is linked to a preceding block. Combined with cryptographic hashes, this time-stamped chain of blocks provides a hopefully immutable and tamper-evident record of all transactions in a network, from the genesis block until the last/most current block. This is in contrast with a traditional relational database where data can be deleted or modified, there are no administrator permissions within a blockchain that allow for deleting or editing of the recorded data.

Figure 2a: Blocks of Data Forming a Blockchain in a blockchain, data are grouped into blocks that are then “linked” together using digital signatures on cryptographic hashes.

A blockchain comprises a set of nodes without a pre-existing trust relationship and are connected through a peer-to-peer network. Each node will host the exact copy of a blockchain that create a decentralized structure. But for such a structure to be useful there must exist some mechanism by which the nodes can mutually reach a consensus on the next valid block in the chain to be added. Alluva (2019) stated that “the consensus mechanisms are protocols that make sure all nodes (devices on the blockchain that maintains the blockchain and (sometimes) processes transactions) are synchronized with each other and agree on which transactions are legitimate and added to the blockchain.” These consensus mechanisms are crucial for a blockchain in order to correctly work. Some of the deployed schemes for establishing such a distributed consensus include: Proof of Work, Proof of Stake, Proof of Capacity, Proof of Human-Work, Proof of Activity and Proof of Elapsed Time.

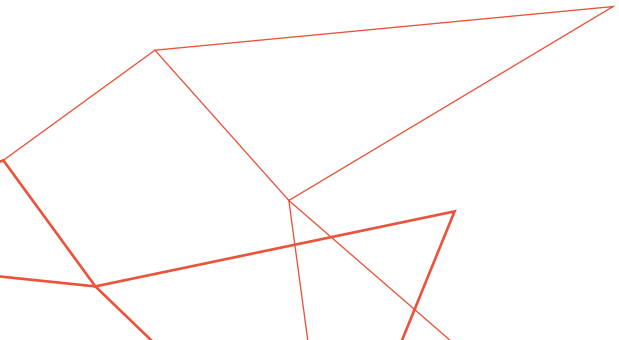
In addition to decentralization, consensus and immutability, a blockchain network also has two additional key characteristics: (iv) Provenance and (v) finality. Provenance comprises the support for participants of the network to know where the “asset” came from and how its ownership has changed over time; while finality refers to a single and shared ledger providing one unique place to support on and to determine the ownership of an asset or the completion of a transaction.

A blockchain can use smart contracts, which serve as agreements or a set of rules that govern a business transaction. A smart contract is stored on the blockchain and is automatically executed as part of a transaction. For example, a smart contract may define contractual conditions of insurance claim processing, which may be automatically executed when a medical expenses

transaction is executed. It should be noted that we discuss smart contracts from the standpoint of the use case of creating smart (i.e., digital) contractual relationships between parties, and not the technological standpoint (i.e., computer programs running on a blockchain, also called chaincode).

In his path-finding work, Nick Szabo proposed smart contracts [1] as a means to build on the complex social structures that have evolved over the last few millennia. One of the problems of moving more and more of the interactions between actors in a society into the digital realm is that traditional contractual agreements can break down, losing the advantages of the complex legal frameworks that have been created. Smart contracts are a way to take advantage of the social structures society has now, in a digital realm, by incorporating observable, verifiable, private and enforceable contracts that are written in code and operate according to defined rules. These smart contracts can be used to reduce fraud and make business processes more efficient.

A blockchain can be both permissionless or permissioned. Permission less (public) blockchain entitles anyone to join the network. A permissioned (private) blockchain, requires a pre-verification of the participating parties which are known to each other within the network. The choice between the two types is mainly driven by the whether an application can 'commoditize' the trust. Bitcoin [2] and Ethereum are examples of permissionless blockchain facilitating parties to transact without necessarily having to verify each other's identity. On the other hand, electronic health records, for example, is an ideal use case for permissioned blockchains. One would not want non-vetted companies participating in the network.



Box 2. Blockchain: Use Cases and Platforms

Blockchain technology has gained substantial deliberation in recent years from the financial / banking disciplines. The technology of blockchain attracted a considerable attention due to the possibility of recording all financial transactions in a secure and verifiable decentralized (peer-to-peer) fashion, without the rule from a third party to process transactions, which are then combined into blocks where each block contains a timestamp and is linked to a previous block. Once recorded, data can't be altered and the transactions history is combined into a chain structure without the possibility of additional branches of alternative transactions emerging or wedging into the middle of a chain. The decentralization of these transactions allows conducting financial transactions completely independently of control from either side.

While the focus of applications of blockchain applications in practice to date has been to build ledgers of transactions involving virtual tokens (i.e. cryptocurrencies), this technology has recently gained an increased curiosity in several diverse fields. In a January 2016 report, Mark Walport, the UK government's chief scientific adviser, argued that blockchain technology could expand far beyond a trading tool: "Distributed ledger technologies have the potential to help governments collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods, and generally ensure the integrity of government records and services," the report concluded (Walport, 2016 p.6). The impetus has now extended to the other domains, including the real-state, identity management, insurance, supply chain, healthcare, and government just to name examples.

Blockchain Platforms

- Ethereum

  Ethereum is an open-source and permissionless blockchain platform that lets anyone build and use decentralized applications that run on blockchain technology. It is designed for mass consumption versus restricted access (a typical requirement for privacy requirements in enterprise use-cases). Ethereum is known for its robust smart contract functionality and flexibility, it is used widely across multiple industry use cases, and it has the largest number of use-cases available today (50%+ in our sample set).

  Ethereum utilizes the Proof-of-Work (PoW) consensus protocol, which is energy intensive, has no guarantees about transaction finality, and can have latency issues. Though it is proposed to change the consensus algorithm to Proof-of-Stake (PoS) in the future, this will help only with energy use and the latency of block creation and not with guarantees about transaction finality.

- Corda

  R3 was launched in 2015 and currently comprises of world's largest financial institutions that has created an open-source distributed ledger platform known as Corda. It has grown to a network of more than 60 companies. Although Corda was originally built to serve banking

industry, recent use of Corda in sectors such as supply chain, healthcare, trade finance and government is now emerging. Corda has neither built-in token nor cryptocurrency, but it is a permissioned blockchain because Corda limits access to data within an agreement to only those permissioned, but not to everyone in the entire network. Corda's consensus system also accounts for the reality of the management of the complex financial agreements. Corda is also well known for its focus on interoperability ease of integration with legacy systems.

- Hyperledger Fabric

Hyperledger Fabric is an open-source, permissioned distributed ledger technology (DLT) platform, designed for enterprise use. Fabric utilizes a modular architecture, allowing flexibility for a large variety of use cases, with the potential trade-off of having a more complex system.

- Hyperledger Iroha

Hyperledger Iroha is a decentralized ledger (blockchain) platform created for enterprises and financial institutions to create highly performant systems that can scale to large numbers of concurrent users. The key features of Hyperledger Iroha are:

- Byzantine fault-tolerant consensus, via the YAC (Yet Another Consensus) algorithm
- Transaction finality
- Role-based account permission system
- Simple command execution environment
- Software development kits (SDKs) in a variety of languages to ease client development

The backbone of Hyperledger Iroha is a peer-to-peer network of validating peers, where all peers are considered equal. Unlike other systems, there is only one type of peer in Iroha— validating peers—simplifying the construction of systems incorporating Iroha and reducing points of failure.

Hyperledger Iroha uses a blockchain as the data structure to provide verifiable proof about the existence of transactions, and validating peers on the network participate in the block creation process. To create a block, either a time limit expires or the number of transactions in the pending queue reaches a predetermined threshold. When this happens, the crash-fault tolerant ordering service generates a block proposal and transfer it to the peers in the network. For each block proposal, there is a designated leader node who is determined based on the hash of the proposal, after each node verifies the transactions and creates a verified proposal. Each node sends their vote for a verified proposal to the leader of the consensus round and once a super majority of nodes vote for a proposal, then it becomes finalized and a commit message is broadcast to the network.

Hyperledger Iroha uses an account-based model, meaning that all users in the system must register a username that is associated with at least one public key. All validating peers with system level access have access to all data and privacy is provided through the pseudoanonymous nature of account user names. There is no limit on the number of usernames that an institution or user can register in Iroha, though for auditing purposes pre-determined and static usernames are likely to be a desideratum for many financial use cases.

Next Generation Payment System

website: bakong.nbc.org.kh

Bakong Bakongpayment info@bakong.nbc.org.kh