Can blockchain make a financial and information revolution?

Use cases of commercial projects at the National Bank of Cambodia and with Moscow Stock Exchange Group
**Who are we?**

<table>
<thead>
<tr>
<th>Logo</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Soramitsu](image) | Founded in 2016  
60+ people  
Offices in 5 countries |
| ![Hyperledger Iroha](image) | We are the creator of Hyperledger Iroha and an active member of the Linux Foundation’s Hyperledger Project; V1.0 released in May 2019 |
| ![NATIONAL BANK OF CAMBODIA](image) | We are implementing a payment system based on Hyperledger Iroha for the central bank and regulator of the Kingdom of Cambodia, targeted at 18 million retail users |
| ![D3ledger.com](image) | We are the technology provider to D3, a decentralized digital depository with the national CSDs of Slovenia and Russia |
| ![Polkadot](image) | We were chosen by the Web3 Foundation to create the C++ implementation of the Polkadot Runtime Environment |
| ![BCA](image) | We have worked on an implementation of digital, self-sovereign identity with BCA Group in Indonesia |
Mission: Create a better (& more efficient world) through decentralized technologies
Hyperledger Iroha v1 Release

- **Production-ready** Hyperledger Iroha V1.0 was released by Hyperledger in May 2019

- Initially contributed by Soramitsu

- Hyperledger Iroha passed security, stability and durability tests, and was verified that it can be used safely by financial institutions, enterprises, and governments
Hyperledger Iroha

Iroha is a permissioned blockchain that is created explicitly for digital asset and digital identity management.

Simple & Fast
Transaction finality achieved within 2 seconds, with thousands of transactions processed per second.

Mobile SDKs
iOS, Android, and JavaScript SDKs are provided to ease development of end-user applications.

Asset Management
Assets such as currencies, points, tickets, securities can all be managed using core functionality in Iroha.

Use case partners:

Development partners:
Some use cases of Hyperledger Iroha

**PoC**
- Regional currency at Smart city
- Smart contract insurance
- Self-sovereign identity
- Interoperability with Polkadot

**Commercial**
- Central Bank of Cambodia
  - New payment infrastructure
- Moscow Stock Exchange Group
  - Decentralized Digital Depository
- Indonesia Banking group
  - Self-sovereign identity
- Interoperability with other blockchains

**New economic system**

© 2019 SORAMITSU All Rights Reserved. These materials are to be used only for your present business purpose. Unauthorized copying or distribution to a third party without the consent of Soramitsu Co., Ltd. is strictly prohibited.
Key Features of Hyperledger Iroha
Commands in Hyperledger Iroha

Without writing code, asset, identity & supply chain management can be done using prepared commands in the data model. This eases development and increases reliability.
Commands in Hyperledger Iroha

**Peer**
- AddPeer

**Domains**
- CreateDomain

**Assets**
- CreateAsset
- AddAssetQuantity
- TransferAsset

**Account**
- CreateAccount
- AddSignatory
- RemoveSignatory
- SetQuorum

**Permissions**
- CreateRole
- AppendRole
- GrantPermission
- RevokePermission

---

**Diagram:**
- **Domain**
  - Peer
  - Multi assets
    - Assets
  - Account
    - Signatures
    - Role
  - Permissions
Creating a better world through decentralized technologies

Example: Twitter-Style App

Using Iroha’s account info, tweets can be stored associated with an account. This can be used to make a decentralized social media client, like twitter.

https://github.com/x3medima17/twitter
Decentralized Permission Model

Example of Role Decentralization

- Decentralized RBAC* permission model without single point failure
- Separation of three powers can be created to avoid concentration of authority
- Roles and permissions are set determined in the genesis block

*RBAC = Role Base Access Control
**Transaction privacy protection**

- Only authorized users can access the information
- Flexible permission for Commands and Queries done via RBAC permission model
- Each account has rights with respect to their multiple roles

**Domains**

- **Account**
  - admin
  - alice
  - bob

- **Role**
  - admin
  - user
  - money_creator

- **Permissions**
  - can_append_role, can_detach_role, can_create_role, can_add_asset_qty, can_add_peer, can_add_signatory, can_create_account, can_create_asset, can_create_domain, can_remove_signatory, can_set_quorum, can_transfer, can_receive, can_subtract_asset_qty
  - can_read_assets, can_get_roles, can_get_my_account, can_get_all_accounts, can_get_my_signatories, can_get_all_signatories, can_get_my_acc_ast, can_get_my_acc_detail, can_get_all_acc_ast, can_get_my_acc_txs, can_get_all_acc_txs, can_get_my_acc_ast_txs, can_get_all_acc_ast_txs, can_grant_add_signatory

*RBAC=Role Base Access Control
User Protection

In most blockchain systems, if you lose your private key, access will not be possible. In Hyperledger Iroha, GrantPermission can be used to safely change keys in the case of device loss.

1. AddSignatory
2. GrantPermission of signatory change
3. Lost Private Key
4. After identity verification, request to New signatory
5. Remove Old signatory
6. Add New signatory
7. Access
Retail Payments
New retail payment infrastructure in Cambodia

In April 2017, the National Bank of Cambodia and Soramitsu started to create a new payment infrastructure for the Kingdom of Cambodia using blockchain.
Bakong in the News

“The National Bank of Cambodia plans to introduce blockchain technology into the payment system by the end of 2019.”

“The most surprising thing about Cambodia's plan is the fact that it's going to be a large-scale development with more than 10 banks participating, not starting as an experimental program.”

https://www.weforum.org/agenda/2019/04/this-new-form-of-currency-could-transform-the-way-we-see-money/
Bakong Pilot Launch on July 17, 2019
Bakong: Mobile Payments (Retail Settlement System)

Blockchain platform is run by NBC as the central bank and regulator; only NBC has access to all transactions.

Commercial banks:
- run mobile API servers that provide access to the Bakong system; commercial banks can only monitor the transactions of their own users;
- desktop API and app to manage bank and branch accounts;
- integration with the Core Banking System via ISO20022 messaging.
New payment infrastructure: Mobile application

- Multi currency
- Send money to registered user
- Deposit money to existing bank account
- Display QR code others can scan
- Scan QR code to send money to

Creating a better world through decentralized technologies
New payment infrastructure: Desktop application

- Remittances between bank accounts, issuance of digital currency, etc.
- Requires supervisor approval by multi-signature.
- The financial institution monitors the user's transaction, then restrict suspicious transactions.
Self-Sovereign Identity
Digital Identity

Project Features:

- Supports customer on-boarding process for both new and existing customers
- Allow to share data between different business units through appropriate permissions
- Provides opportunity to audit any operation performed in any unit via Iroha blockchain
- Android & iOS applications for customers, web application for operators
Key Features of Digital Identity

- KYC — Registration with verified document
- Blacklisted customers
- Update document data
- Sharing requests
Problem 1: Customers have to perform KYC for each BCA company

- BCA
- CSfinance
- BCAfinance
- BCAinsurance
- BCAlife
- BCASyariah
- BCAsecurities
Problem 2: No group standard for identity

Customer has to provide information to each group company and opportunities are lost for selling new services.
How it works: BCA Digital Identity Project

A digital stamp of approval for the customer is shared with all group companies

Comes once, verified for all companies

Once verified, able to pass KYC automatically
BCA Digital Identity Project

• Eases on-boarding process for both new and existing BCA customers
• Allows to share the data between BCA companies, such as a customer’s documents, blacklist
• Provides opportunity to audit any operation in BCA companies using the Iroha blockchain
• Android & iOS applications for customers, web-application for operators in BCA companies
Decentralized Identifier (DID)

- DIDs are a proposal from the W3C to create globally unique identifiers using cryptography to generate proofs of data.

- https://w3c-ccg.github.io/did-spec

Sora Identity: Secure, Digital Identity on the Blockchain (2018)
Motivating Example: Putting it all together

A user with a bank account wants to open an account at a new bank and speed up verification of their identity.

1. A user registers their DID on the blockchain. PII are encrypted and backed up on the cloud.
2. User shares info with Bank A.
3. Bank A writes a verifiable claim about the data to the blockchain.
4. User shares info with Bank B.
5. Bank B reads the verifiable claim from Bank A on the blockchain.
6. Bank B receives data from Bank A to verify claims about the User.
Identity verification by face recognition

Selfie movie

Shoot ID card

OCR

Calculate face matching
Decentralized Digital Depository (D3)
D3 Ledger

D3 (Decentralized Digital Depository) is a decentralized infrastructure that enables institutionalized financial service providers, like banks or stock exchanges, to safely work with blockchain-based assets, such as tokenized securities, while ensuring full compliance with the existing regulatory framework.

https://d3ledger.com
D3 ledger network

- Bidirectional direct exchange with DVP (Atomic Swap) between Bitcoin and Hyperledger Iroha, Ethereum and Hyperledger Iroha achieved by sidechain

- Advantages for financial institutions are improving security, scalability, and reduction of handling fees
Services Offered by D3

Safekeeping
Digital assets safekeeping with multi-signature protection.

OTC settlement
Settlement of OTC trades using internal swap transactions of D3ledger.

Exchange trades settlement
Settlement of trades completed on the partnering exchanges.

Token generation
Generation of asset-backed tokens.
Interoperability activities with Polkadot

We were chosen by Web3 Foundation to create the C++ implementation of the Polkadot Runtime Environment (Kagome)

Sora
Decentralized
Autonomous Economy
Sora: A Decentralized Economic System
XOR: Solving the Problem of Allocation of Money in an Economy

Like all economies, Sora is comprised of actors who work to create their own goods and services.

By using Sora (XOR), these goods and services can contribute to the Sora economy and help build a decentralized world economic system.
The Tech

Sora, the decentralized autonomous economy, is being launched as the Sora Network. It was built using D3 Ledger technology, created along with the central securities depositories of Russia and Slovenia. D3 Ledger uses the Hyperledger Iroha blockchain, originally contributed to the Linux Foundation by Soramitsu.

XOR lives across multiple platforms and is not tied to any one technology. XOR is being launched on the Sora network using Hyperledger Iroha and D3 Ledger tech and can also be transferred to Ethereum as an Erc-20 token. In the future, support for Polkadot is also planned.
Contact

Phone: +81-3-6635-2705
t@soramitsu.co.jp
Makoto Takemiya