The world’s most secure identity information-based
blockchain platform
using the multi biometric authentication technology

SHIELDCURE Whitepaper (Ver1.0)

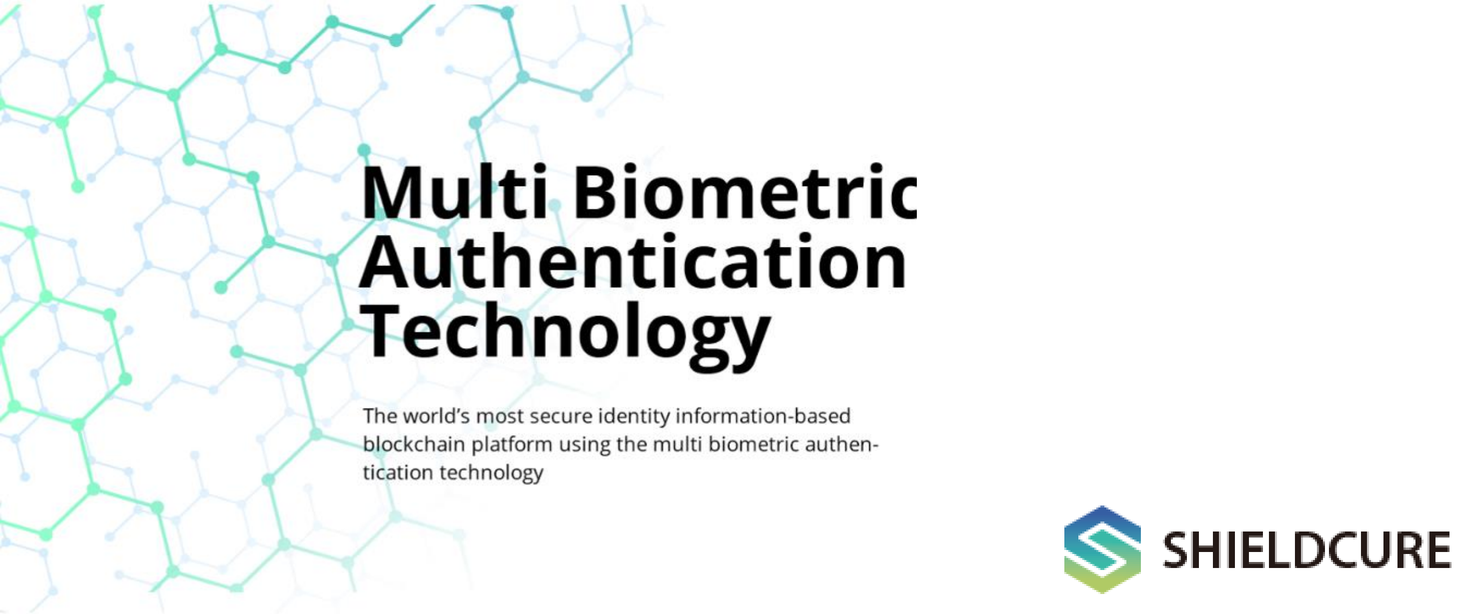
Table of Contents

1. Introduction

SHIELDCURE aims to build a reliable identity authentication service of the next-generation by using the multiple biometric recognition system in the blockchain environment. It pursues personalization of information and social utility and will take a step to build a Baas (Blockchain as a service) infrastructure that promotes exchanges of personal information and digital assets.

As an integrated IDENTITY information platform, SHIELDCURE guarantees the trust of the value information and assets, and serves as the hub of authentication and transaction for our affiliated Alliances by using ID COIN, the standard currency in our network. All information and assets, whose value is verified by ID COIN, will be traded in the SHIELDCURE Alliance ecosystem via ID Wallet equipped with DAMS (Digital Asset Management Service). The SHIELDCURE Alliance blockchain will be based on ID COIN with the characteristics and governance of each network maintained and interoperability among them ensured through compatibility.

The SHIELDCURE platform combines multiple biometric recognition technology with blockchain technology in order to build a new economic ecosystem where users can trade information and data easily and safely based on user authentication, transparency and integrity.


Multi Biometric
Authentication
Technology
The world's most secure identity information-based blockchain platform using the multi biometric authentication technology
SHIELDCURE

2. SHIELDCURE Technical View

2-1. ID Wallet Prototype

SHIELDCURE provides ID Wallet Prototype, an integrated cryptocurrency e-wallet with various features before the launch of SHIELDCURE Mainnet. Users are able to store different SHIELDCURE Alliance Tokens and ERC20 tokens in SHIEDCURE ID Wallet Prototype and send, exchange and trade them in the network.

SHIELDCURE plans to provide not only Hot Wallet in the form of an application but also Cold Wallet in a thumb drive armed with fingerprint recognition. All access and transactions related to e-wallet are made possible by biometric information and e-signature which minimizes the risk of leaking or exposing private keys and recovery keys.

The early model of SHIELDCURE’s integrated e-wallet application is under development with the aim to provide a service that allows users to easily experience the systematic combination of the real economy and cryptocurrency with the app in their personal devices. The application is compatible with the network built by a number of card companies and VAN/POS companies which enables users to use the payment systems the existing affiliates established with their e-wallet.

SHIELDCURE Multi-Crypto Currency Wallet
Provides users to control the different cryptocurrency
with an APP by mobile device

Key Features of SHIELDCURE e-Wallet

Access
Multi-
Cryptocurrencies
TOP
SECURITY
SECURED
P2P EXCHANGE

- ERC20 Tokens
- QRC Tokens
- Alliance Coins

- Apply Multi-Biometric Authentication
- Use bank grade security

- Exchange Multi-Cryptocurrency
- Digital Asset Management

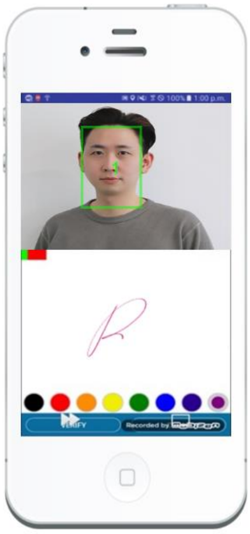
2-1-1. Multi Biometric Authentication

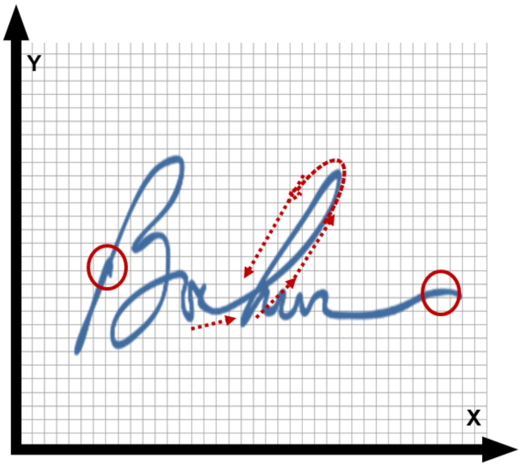
Based on the multiple biometric recognition system, SHIELDCURE ID Wallet provides stronger security and greater convenience than any other e-wallet. All authentication and access are done through an individual's biometric information, which minimizes the risk of illegal use or theft in case the person loses his or her device. This high reliability allows cryptocurrencies stored in ID Wallet to be distributed, exchanged, and used in decentralized transactions.

The multiple biometric recognition system uses a security solution application technology called "SmartSigncroSs," which supports multiple recognition features such as fingerprint recognition, manual signature, and have stronger security solutions than a single biometric authentication.
The "SmartSigncroSs" technology gets rid of the inconvenience of having to memorize or change your password and greatly increases reliability by recognizing one's unique physical features and the speed of writing a signature, and the tilt of your pen. These biometric data will be stored in blocks after being codified for de-identification using encryption and security technologies according to the principle of Least of Privilege (LoP) once the Mainnet is launched later on. It is to build a structure that prevents hackers from stealing or forging data using another device even if users lose their device.

In particular, the e-signature feature does not require a dedicated sensor available only for specific devices, and uses manual signature, which is biometric behavior, so users can enjoy the highest security technology by just installing a software program. When it comes to management of keys, users can use ID Wallet with Public Key Infrastructure (PKI)-based multi-factors such as fingerprint, face, and signature with their consent.

All these features significantly reduce the risk of hacking and greatly enhance anonymity and privacy in SHIELDCURE ID Wallet.





- Coordinate value
- Speed / Acceleration
- Time
- Pressure
- Color
- Direction
- Curvature
- Start and End points
- Number of Strokes
- Inclination

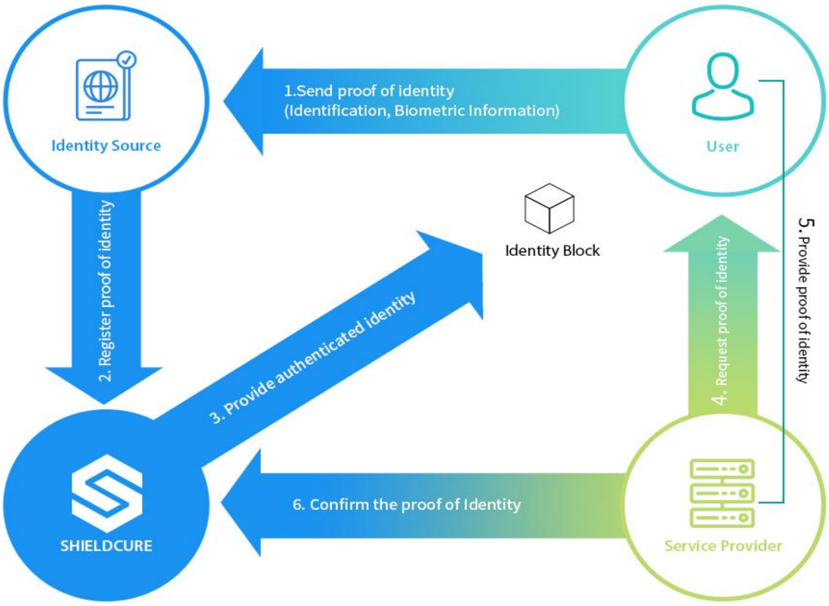
2-2. SHIELDCURE Blockchain

SHIELDCURE Blockchain, which is to be built soon, is a platform where various service items based on identity authentication are applied. At this stage, SHIELDCURE will release an official SHIELDCURE ID Wallet equipped with features such as on-line and off-line identity confirmation and Digital Asset Management Service (DAMS). In addition, we plan to expand the scope of the platform by providing commercialized blockchain services in various areas including finance, a share economy, production, distribution, and entertainment through Dapp.

SHIELDCURE Blockchain strengthens personal identification feature using an individual's biometric information, which enables users to use various services such as identity authentication, fitness, a shared economy, and IoT interworking. Furthermore, users themselves are able to manage and trade information they have and digital assets, which will be enabled by powerful access control and security configuration.

SHIELDCURE will develop its unique blockchain by applying Security & Privacy Act (SPA) with enhanced security and privacy and ID Smart Contract (ISC) with more enhanced features compared to previous smart contracts. In particular, SPA adopts stronger concepts of Security By Design and Role-Based Access Control (RBAC), and Blockchain as a service (Baas) based on identity authentication stability, security and extensibility.

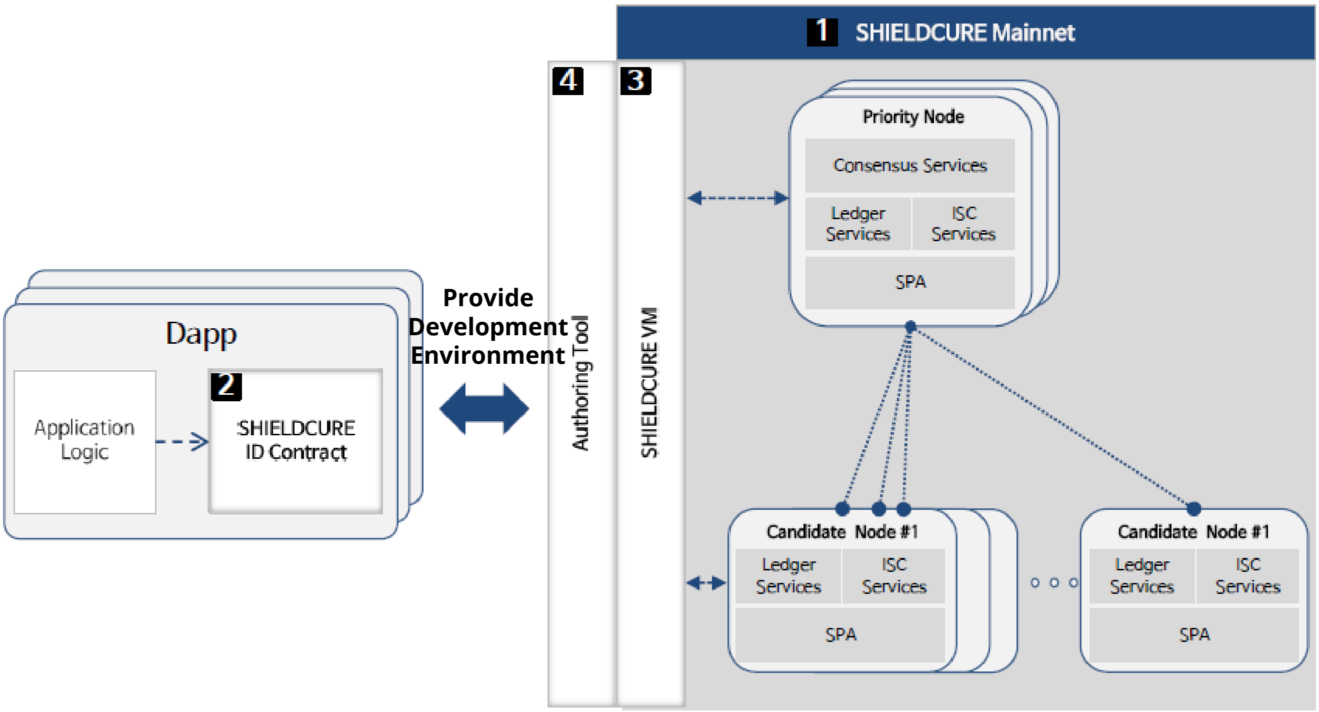
This makes it possible for SHIELDCURE to create a SHIELDCURE Alliance community with various cryptocurrencies and unstandardized blockchain ecosystems, and build an integrated, decentralized information platform which guarantees security and reliability. This new SHIELDCURE Alliance ecosystem will grow and enhance trust with Alliances, including certified verifiers. As more businesses join the Alliance, the value and influence of SHIELDCURE Alliance will be extended to a variety of business areas based on blockchain.


Identity Source
1.Send proof of identity
(Identification, Biometric Information)
User
Identity Block
2. Register proof of identity
3. Provide authenticated identity
4. Request proof of identity
5. Provide proof of identity
SHIELDCURE
6. Confirm the proof of Identity
Service Provider

2-2-1. Architecture

The structure of Mainnet and its main developments are the following:

(1) The Structure of SHIELDCURE Mainnet

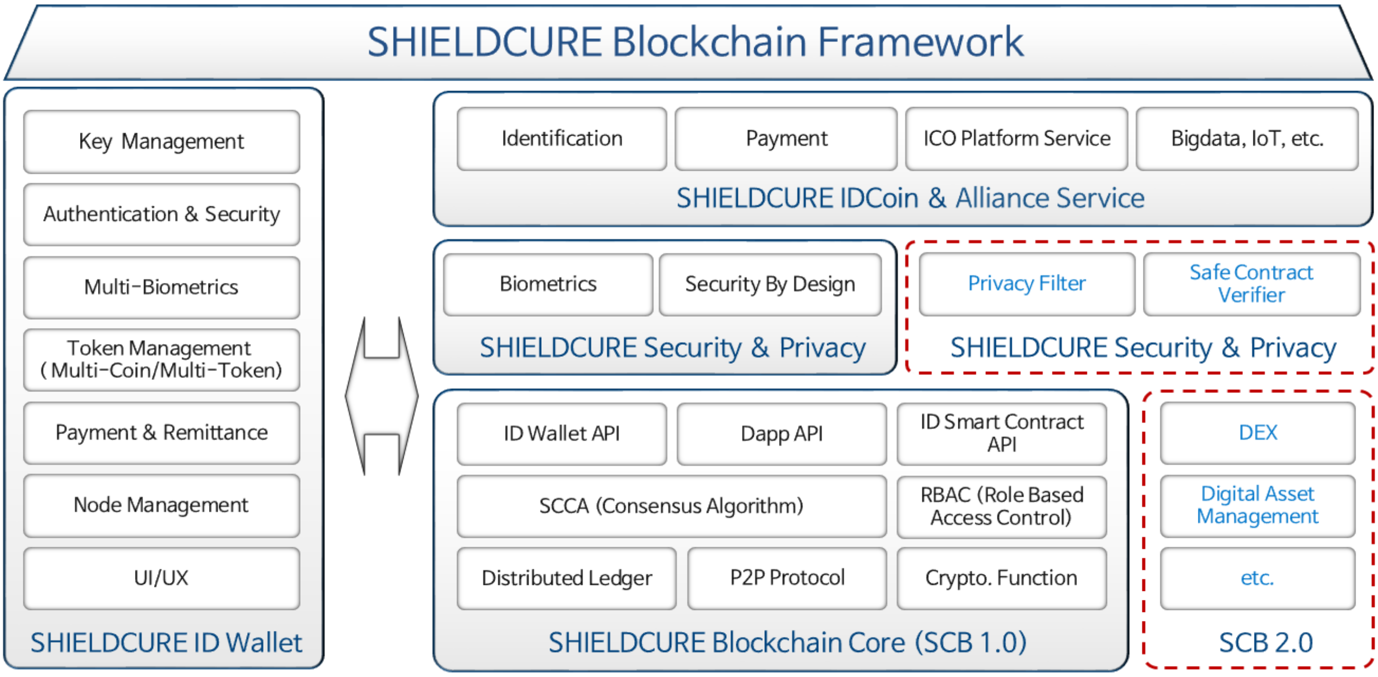


(2) SHIELDCURE Mainnet Development Scope

Development Items	Development Details	Description
Mainnet System	SCCA (ShieldCure Consensus Algorithm) consensus algorithm	Develops SHIELDCURE's own consensus algorithm (SCCA) based on Opos and the P2P process regarding consensus
	Build Priority Node and the Candidate Node environment	Develops Priority Node (Block Validators) and Candidate Node in accordance with consensus algorithm
	Block Creation and Transaction Process	Creates Hash algorithm-based Blocks and develops Transaction processing technology
	FIDO bio-authentication interworking	Designs FIDO authentication process and Develops interworking UI
ID Smart Contract	Develops Smart Contract-based ISC	Develops Smart Contract-based add functions and templates
	Develop Biz. Logic in accordance with ISC	Designs and Develops basic Biz. Logic of registration, authentication, and destruction needed for ISC and extended Biz. Logic
VM Development	Bytecode conversion and compiler development	Develops VM which is able to compile to bytecode by analyzing solidity augmented grammar
	Mainnet execution setting development	Develops a executable program and settings for distribution and execution of Mainnet

SHIELDCURE Mainnet Framework will be developed step-by-step based on SHIELDCURE ID Wallet and SHIELDCURE Blockchain Core (SCB) as the following:

(3) SHIELDCURE Mainnet Framework



SHIELDCURE Blockchain Framework

SHIELDCURE ID Wallet: Key Management; Authentication & Security; Multi-Biometrics; Token Management (Multi-Coin/Multi-Token); Payment & Remittance; Node Management; UI/UX

SHIELDCURE IDCoin & Alliance Service: Identification; Payment; ICO Platform Service; Bigdata, IoT, etc.

SHIELDCURE Security & Privacy: Biometrics; Security By Design

SHIELDCURE Security & Privacy: Privacy Filter; Safe Contract Verifier

SHIELDCURE Blockchain Core (SCB 1.0): ID Wallet API; Dapp API; ID Smart Contract API; SCCA (Consensus Algorithm); RBAC (Role Based Access Control); Distributed Ledger; P2P Protocol; Crypto. Function

SCB 2.0: DEX; Digital Asset Management; etc.

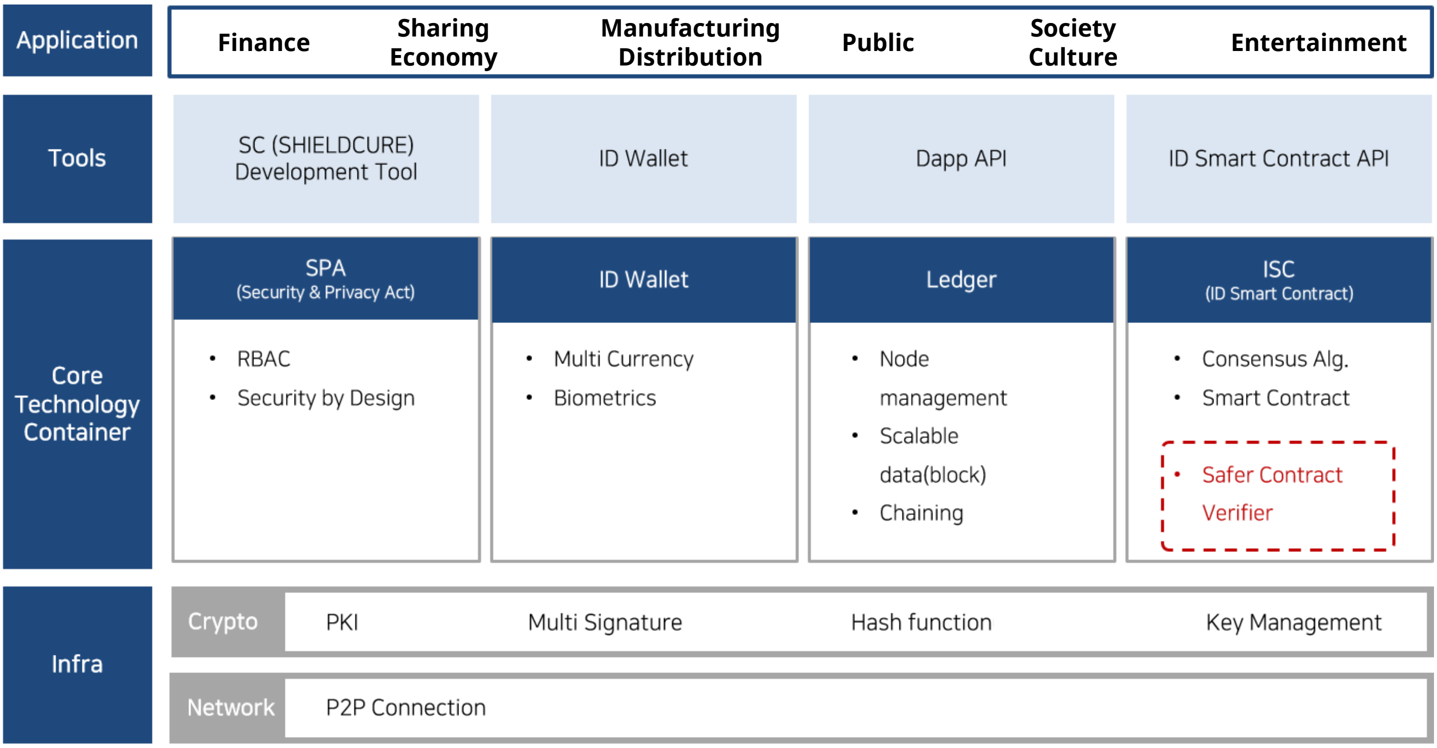
: Stage 2

❖ Stage 2 means advanced development phase

The logical architecture of SHIELDCURE Blockchain will be built on encryption and network capabilities based on application, tools offered to users or developers and four key technologies.

(4) SHIELDCURE Blockchain Logical Architecture

Stage 2



Application: **Finance**, **Sharing Economy**, **Manufacturing Distribution**, **Public**, **Society Culture**, **Entertainment**

Tools: SC (SHIELDCURE) Development Tool; ID Wallet; Dapp API; ID Smart Contract API

Core Technology Container:

SPA (Security & Privacy Act)	ID Wallet	Ledger	ISC (ID Smart Contract)
• RBAC • Security by Design	• Multi Currency • Biometrics	• Node management • Scalable data(block) • Chaining	• Consensus Alg. • Smart Contract • Safer Contract Verifier

Infra:

Crypto: PKI; Multi Signature; Hash function; Key Management

Network: P2P Connection

❖ DAMS(Digital Asset Management Service) is at a business development phase and will be updated soon

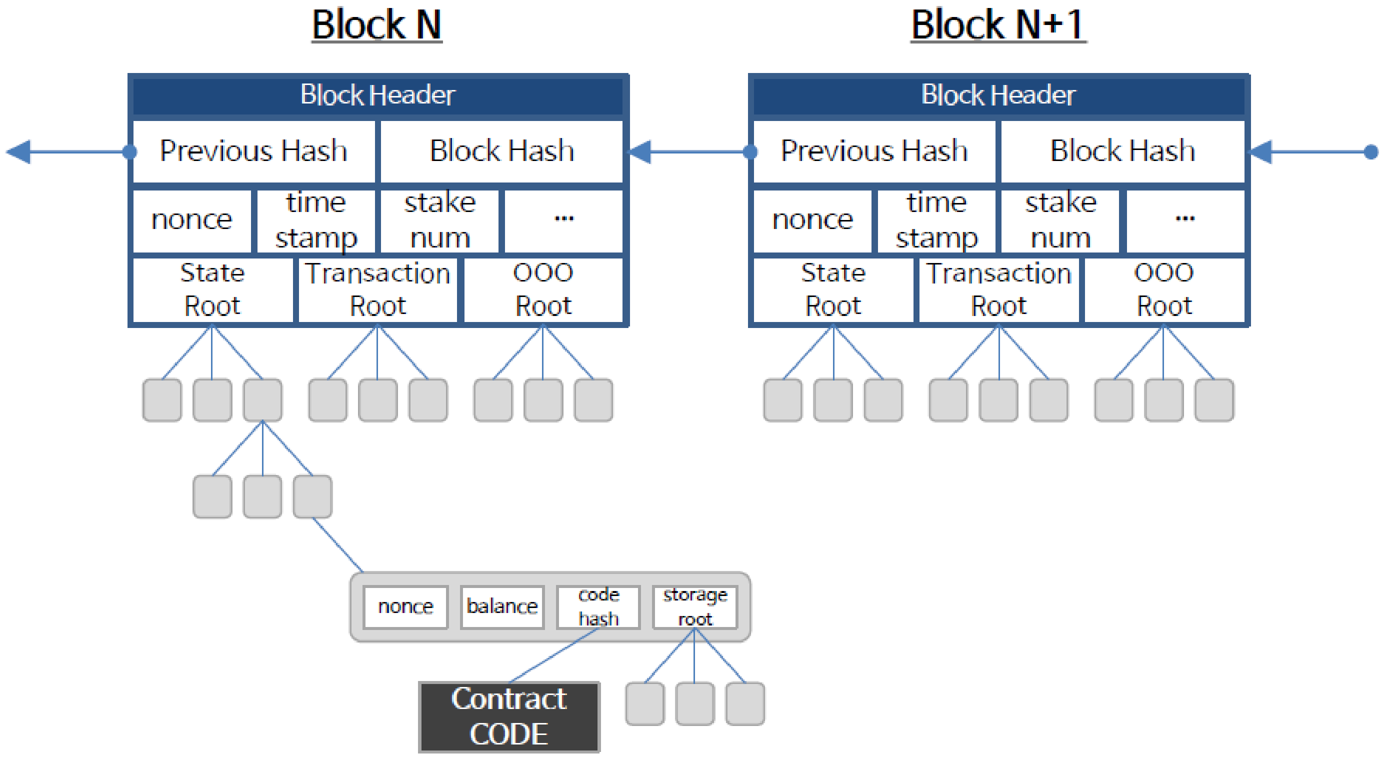
(5) SHIELDCURE Specifications and Characteristics

Stage 2

특성	사양	내용
Consensus Method	• SCCA (ShieldCure Consensus Algorithm)	• Compared to the other existing protocols, SCCA can handle transactions with exceptional speed per unit time, and differentiated SCCA model (stake + participation + No. of Nodes in the network + Node property (role)) will be used to strengthen the reliability of Delegated Nodes which has been a major issue in Delegated Proof of Stake (DPoS) method with in free transfer fees • When we build the overall blockchain with stability and extensibility, we analyze and reflect two main original methods; 1. RBAC, and 2. Security By Design.
Cryptography Algorithm	• Multi-Signature • Hash	• Supports multiple signatures based on PKI, Hash algorithm and key management feature
SPA (Security & Privacy Act)	• Security By Design • RBAC (Role Based Access Control)	• Builds a safe blockchain ledge with the three SC security mechanisms(R&R, SoD, LoP) and apply RBAC-based decentralized access control model ❖ R&R: Role and Responsibility SoD: Segregation of Duties LoP: Least of Privilege
	• De-Identification	• Plans to store and use de-identification data through filtering feature for sensitive or personal information
ISC (ID Smart Contract)	• SCGM (Smart Contract Generation Mechanism) • SCVM (Safer Contract Verifier Mechanism)	• We plan to guarantee compatibility and secure the legitimacy related to parsing • Also plan to verify the stability and validity of Smart Code
ID Wallet	• Multicurrency • Biometrics	• Various coins are managed and supported in one e-wallet • Provides Strong Authentication based on biometric recognition

(6) SHIELDCURE Ledger

SHIELDCURE Ledger will compose of the following:

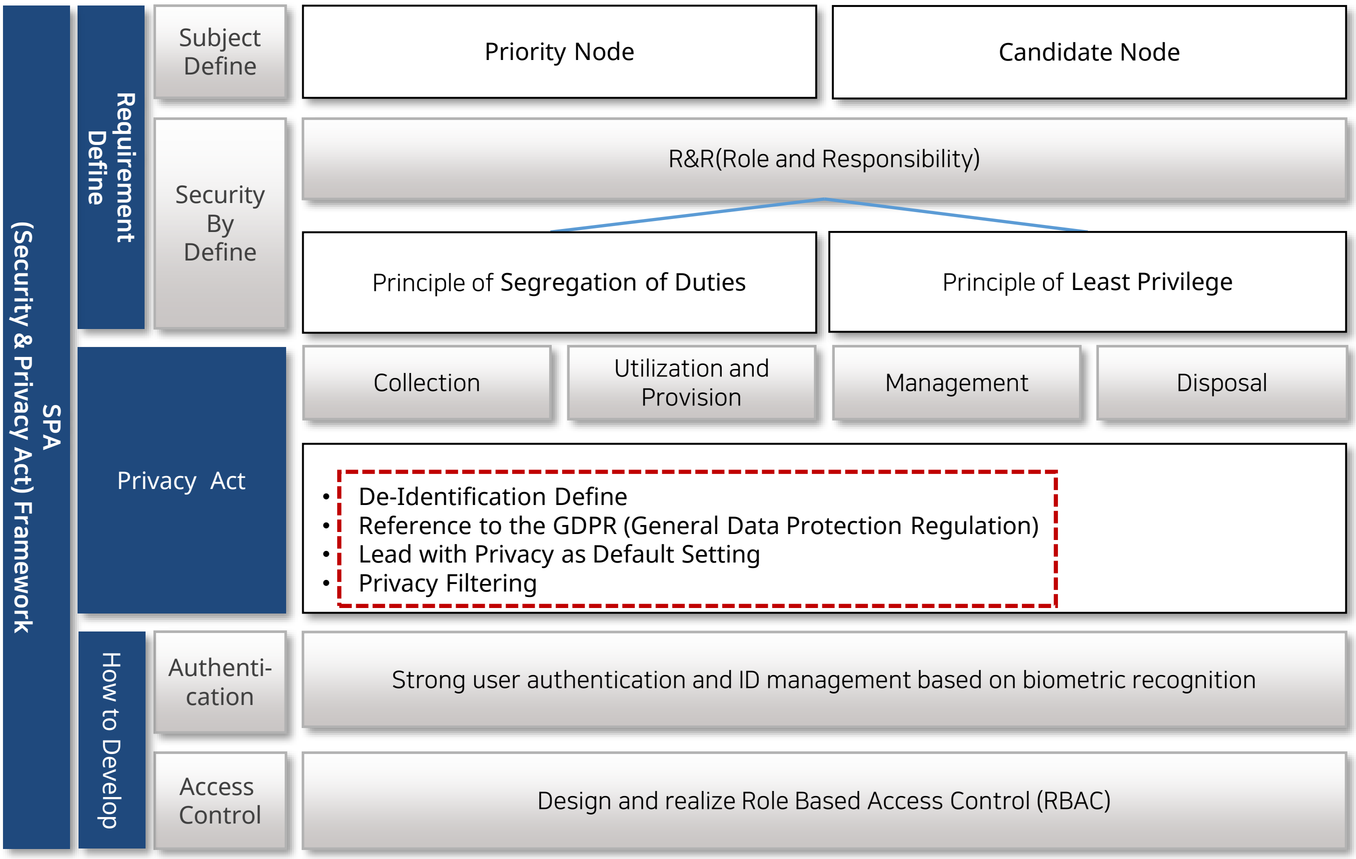


2-2-2. Core Technology

SHIELDCURE plans to make sure to take into account multi-faceted security risk factors like pre-requests, lifespan of personal information in Security By Design, which concerns protection of personal information, and build SPA with the following philosophy.

(1) Security & Privacy Act (SPA) Framework

Stage 2



SPA (Security & Privacy Act) Framework

Requirement Define

Subject Define

Priority Node

Candidate Node

Security By Define

R&R(Role and Responsibility)

Principle of Segregation of Duties

Principle of Least Privilege

Privacy Act

Collection

Utilization and Provision

Management

Disposal

- De-Identification Define
- Reference to the GDPR (General Data Protection Regulation)
- Lead with Privacy as Default Setting
- Privacy Filtering

How to Develop

Authentication

Strong user authentication and ID management based on biometric recognition

Access Control

Design and realize Role Based Access Control (RBAC)

(2) SPA Security Part

(2-1) Need for Security by Design and the measures to differentiate it

Once a block is designed and built, it is hard to change or destruct it by nature, so it is highly important to build a reliable block at first. Therefore, Security by Design is SHIELDCURE Mainnet’s key feature that should be prioritized for extensibility and compatibility based on integrity and transparency.

SHIELDCURE Mainnet uses the following two security measures to provide a more reliable platform than existing public blockchains, which lays the foundation for more stable service.

1. Building and applying RBAC (Role-Based Access Control)
2. Biometric Based on Consolidated Authentication

(2-2) How to apply Security by Design

We will apply the three security governance key policies (R&R, LoP, SoP) from the designing phase considering the consent and agreement issues of Smart Contract based on digital business at the initial node registration stage, and conflicts and solutions, which could arise in digital asset transactions.

1. Role & Responsibilities

We define the overall roles and responsibilities of nodes depending on their definition, purpose, property and regulation.

2. Least of Privilege

Least of Privilege is about giving the least privilege to each node when work is first assigned and grant more privilege later if needed. This is to prevent violation of security principles by nodes' mistake or abuse of privilege.

3. Separation of Duties

No node in the network is allowed to be given absolute privilege over the entire security system and work is assigned under least of privilege. It is to get rid of the risk of abuse of the system and resources, administrators' mistake or abuse of privilege.

An example of defining the roles of nodes in the network

Classification	Details
Priority Node	• Priority Node meets Delegated conditions and selected based on SHIELDCURE's verification methods • It makes important decisions on transactions and processes and helps nodes to discuss and reach an agreement.
Candidate Node	• Candidate Node is a basic node which consists the ledger in the blockchain network and selects Priority Node via voting. • It confirms the content in a block where Priority Node is registered and monitors blocks to see if there are any opaque administration, malicious action or fraud.

❖ SHEILDCURE verification method is under development taking into account qualitative and quantitative factors and will be updated soon

(2-3) Definition and advantages of RBAC (Role-Based Access Control) model

SHIELDCURE Mainnet applies Role-Based Access Control, or RBAC, which enhances reliability of delegated nodes in a way to effectively manage a number of nodes in a decentralized ecosystem like blockchain and control illegal access.

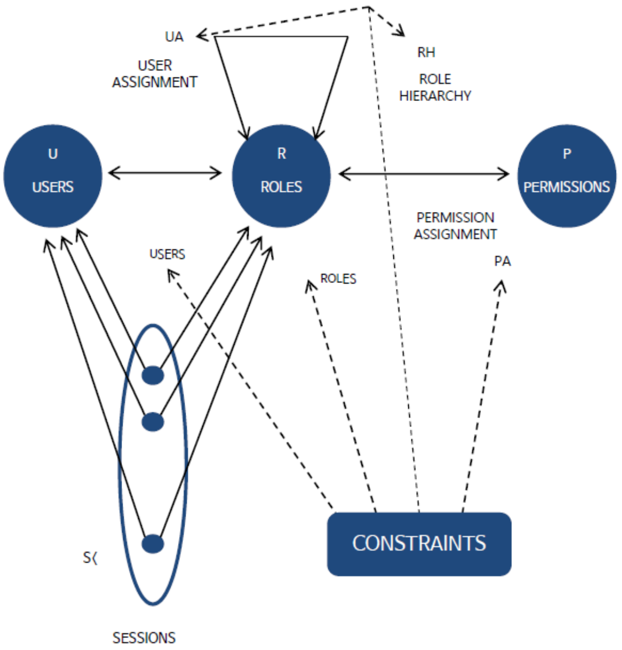
RBAC overcomes the weaknesses of Mandatory Access Control, which has low availability, or Discretionary Access Control, which is vulnerable to veiled attacks or when there are too many participants in a decentralized environment, and assign roles based on the networks' participants responsibilities. It promotes efficiency of management work when the function of the organization changes by allowing operations assigned to roles.

Also, RBAC is an privilege management method that can be used effectively in the connections between various business areas in the decentralized environment as it can control users' behavior actively or passively by firmly establishing Role Hierarchy, Relationship, and Constraint.

(2-4) Structure of RBAC (Role-Based Access Control) model:

Main rules of RBAC

1. Authorization: A user or a role can perform a series of operations that require permissions
2. Permissions: A permission is assigned to a command, a user, or a system.
3. Security attribute: An attribute is a value required for a process to perform its task
4. Permission profile: A set of security attributes that can be assigned to a user or a role
5. Role: A user designated for the execution of an application with permission



SHEILDCURE SPA will design best way to manage security risks such as change, forgery and fraud by setting permissions and constraints that designated nodes in security attributes and operations in advance under the rules of RBAC.

(3) SPA Privacy Part

(3-1) Need for de-Identification and measures to differentiate it – Stage 2:

Recently, it has become more important than ever before to protect and manage sensitive information related to personal information in the blockchain environment. This is one of the issues that should be taken into consideration when designing a blockchain based on the EU’s General Data Protection Regulation (GDPR) or the Private Information Protection Act in Korea, but it is difficult to find a blockchain model that actually considers it.

SHIELDCURE, which aims to realize direct ownership, management and trading of personal information and digital assets by utilizing biometric authentication and blockchain technology, focuses specifically on protection of personal and sensitive information, privacy and security. When personal information is analyzed, it is indiscriminately identified regardless of the analysis purpose, which often infringes on privacy. This problem is more severe in the case of a blockchain as it is almost impossible to discard or modify a block once it’s created.

On the SHIELDCURE platform, we want to apply de-identification by utilizing Privacy Filtering feature on sensitive information in stored data when providing personal information. In addition, we plan to apply a system that allows storing identity data in an off-chain or a separate DB (ID Block) in the side chain, and]registering only major transactions or access-setting data in the main chain.

(3-2) An example of using De-identification and Privacy Filtering – Stage 2:

1. The information whose data alone can identify an individual is deleted.

2. Remaining information will be processed further (deleted or changed) to make sure that the recipient of the information may never be able to identify the owner by combining it with public information

Pseudonymization

Replacing identifying characteristics with a label, in order to render identification of the data subject difficult.

Hong Gildong, 35-year-old, living in Seoul, going to Hankuk University
→Lim Ggeokjeong, in his 30s, living in Seoul, going to Gukje University

Aggregation

Showing the total value of data so that the value of each item is not visible

Lim : 180cm, Hong : 170cm, Lee : 160cm
→A total height of students major in physics : 510cm, Average height : 170cm

Data Reduction

Deleting unnecessary values among the values configured in the dataset or important values for the individual identification depending on the purpose of opening the data sharing

Hong Gildong, 35-year-old, living Seoul, going to Hankuk University
→ 35-year-old, living in Seoul
Resident registration number : 901206-1234567
→ Born in the 1990s, male

Data Masking

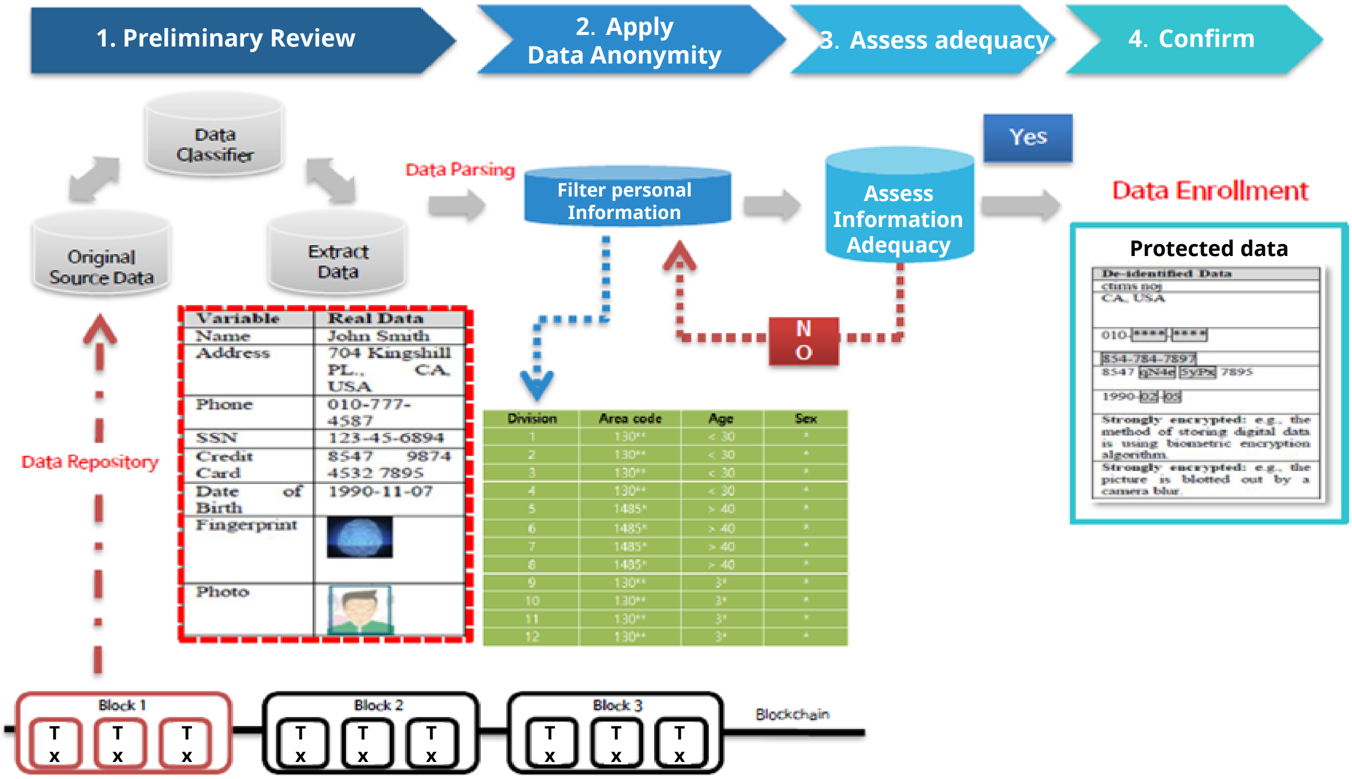
Preventing identification of individuals by hiding individual identifiers that are highly likely to contribute to identifying individuals

Hong Gildong, 35-year-old, living in Seoul, going to Hankuk University
→ Hong **, 35-year-old, living in Seoul, going to ** University

∗Source : National Information Society Agency

(3-3) Example of protecting personal information within the SHIELDCURE platform – Stage 2:

The following is a four-step application example that demonstrates that Privacy Filtering confirms de-identification before personal information is stored in a database or a block and sees if it is properly stored. This will be gradually expanded through the two-step quantitative development process of Mainnet.



Variable	Real Data
Name	John Smith
Address	704 Kingshill PL., CA. USA
Phone	010-777-4587
SSN	123-45-6894
Credit Card	8547 9874 4532 7895
Date of Birth	1990-11-07
Fingerprint	
Photo	

Division	Area code	Age	Sex
1	130**	< 30	*
2	130**	< 30	*
3	130**	< 30	*
4	130**	< 30	*
5	1485*	> 40	*
6	1485*	> 40	*
7	1485*	> 40	*
8	1485*	> 40	*
9	130**	3*	*
10	130**	3*	*
11	130**	3*	*
12	130**	3*	*

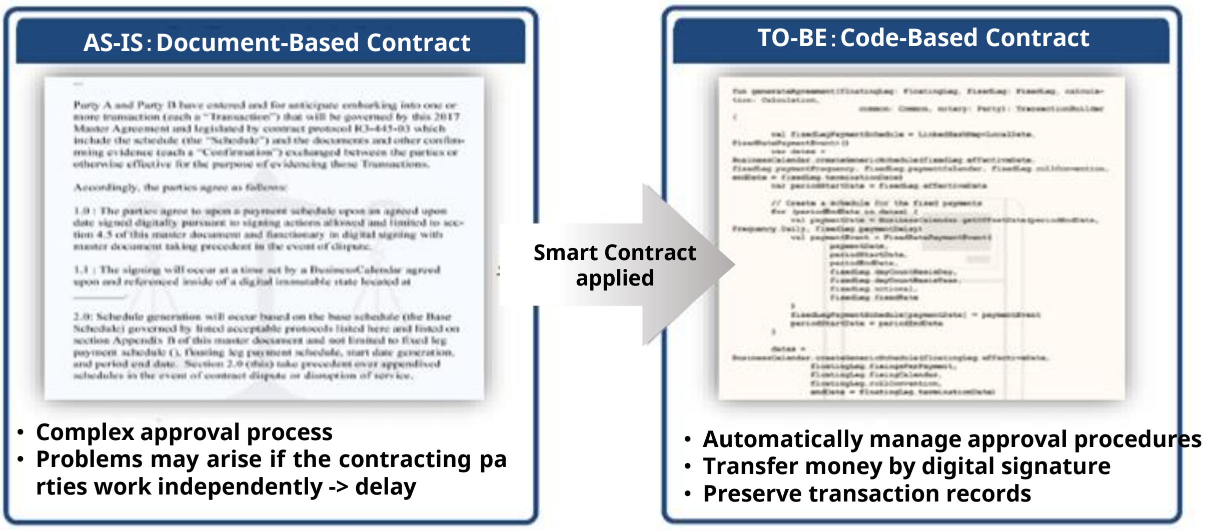
Protected data

De-identified Data
ctiuns noj
CA. USA
010-****-****
834-784-7897
8547 gN4e SyPx 7895
1990-02-05
Strongly encrypted: e.g. the method of storing digital data is using biometric encryption algorithm.
Strongly encrypted: e.g. the picture is blotted out by a camera blur.

(4) ISC (ID Smart Contract)

Smart Contract helps reduce the amount of duplicated work and provides automation support to deal with the approval and proceeding of transactions between the parties and to solve the problems such as delays and possible errors in frequent transactions. In addition, we are creating various business models through smart contract code design as well as simple contracts.

The SHIELDCURE platform uses its own smart contract, ID Smart Contract (ISC). We developed add functions, syntax and templates, and designed and developed a utility-type business logic model for registration, authentication, and destruction. By doing so, we can improve the extensibility of smart contracts so that many service providers can easily and quickly create various business models. ISC secures legality, compatibility, and parsing of ISC according to SCGM (Smart Contract Generation Mechanism) and SCVM (Safer Contract Verifier Mechanism), and verifies stability and validity of codes.



Party A and Party B have entered and for anticipate embarking into one or more transaction (each a "Transaction") that will be governed by this 2017 Master Agreement and legislated by contract protocol IC3-445-03 which include the schedule (the "Schedule") and the documents and other confirming evidence (each a "Confirmation") exchanged between the parties or otherwise effective for the purpose of evidencing these Transactions.

Accordingly, the parties agree as follows:

1.0 : The parties agree to upon a payment schedule upon an agreed upon date signed digitally pursuant to signing actions allowed and limited to section 4.5 of this master document and functionary in digital signing with master document taking precedent in the event of dispute.

1.1 : The signing will occur at a time set by a BusinessCalendar agreed upon and referenced inside of a digital immutable state located at ________

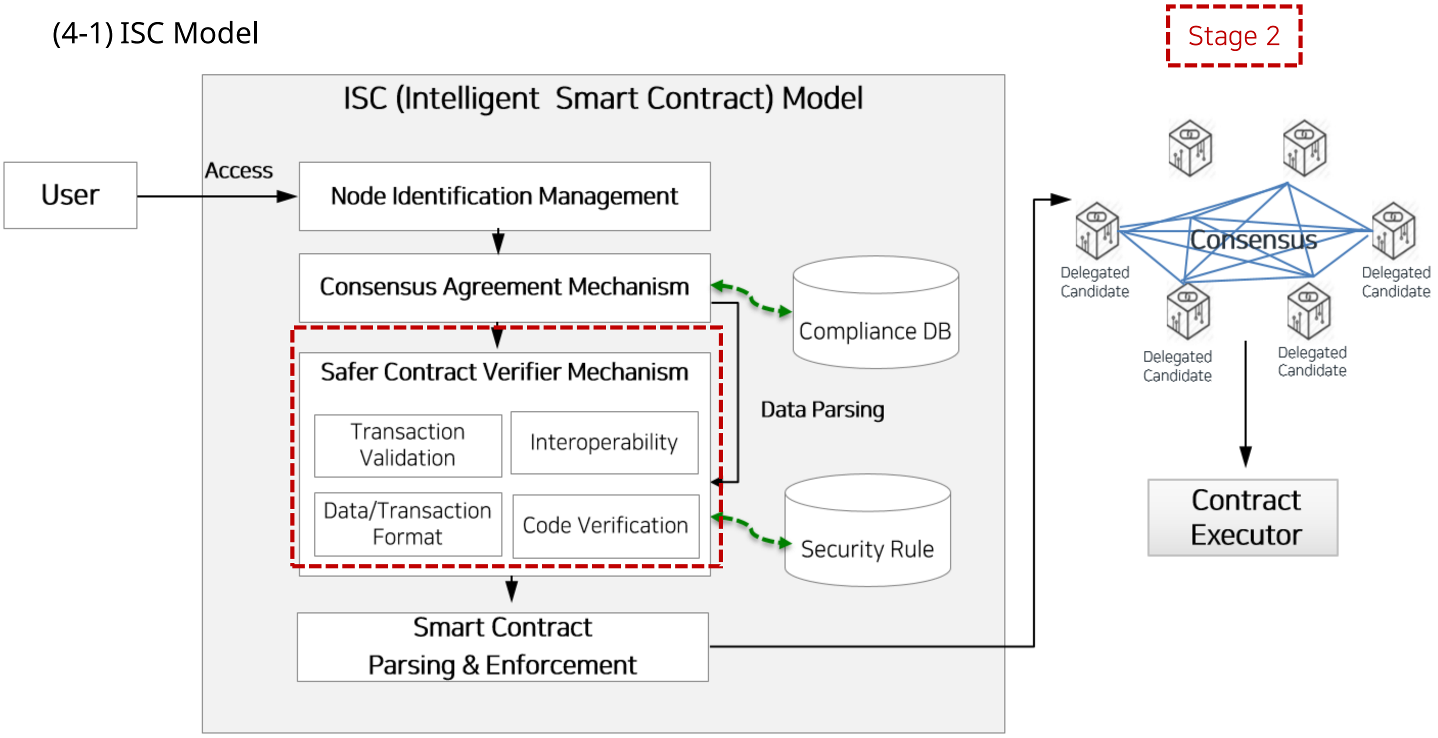
2.0: Schedule generation will occur based on the base schedule (the Base Schedule) governed by listed acceptable protocols listed here and listed on section Appendix B of this master document and not limited to fixed leg payment schedule (), floating leg payment schedule, start date generation, and period end date. Section 2.0 (this) take precedent over appendixed schedules in the event of contract dispute or disruption of service.

- Complex approval process
- Problems may arise if the contracting parties work independently -> delay

```
fun generateAgreement(floatingLeg: FloatingLeg, fixedLeg: FixedLeg, calcula-
tion: Calculation,
                              common: Common, notary: Party): TransactionBuilder
{

        val fixedLegPaymentSchedule = LinkedHashMap<LocalDate,
FixedRatePaymentEvent>()
        var dates =
BusinessCalendar.createGenericSchedule(fixedLeg.effectiveDate,
fixedLeg.paymentFrequency, fixedLeg.paymentCalendar, fixedLeg.rollConvention,
endDate = fixedLeg.terminationDate)
        var periodStartDate = fixedLeg.effectiveDate

        // Create a schedule for the fixed payments
        for (periodEndDate in dates) {
            val paymentDate = BusinessCalendar.getOffsetDate(periodEndDate,
Frequency.Daily, fixedLeg.paymentDelay)
            val paymentEvent = FixedRatePaymentEvent(
                    paymentDate,
                    periodStartDate,
                    periodEndDate,
                    fixedLeg.dayCountBasisDay,
                    fixedLeg.dayCountBasisYear,
                    fixedLeg.notional,
                    fixedLeg.fixedRate
            )
            fixedLegPaymentSchedule[paymentDate] = paymentEvent
            periodStartDate = periodEndDate
        }

        dates =
BusinessCalendar.createGenericSchedule(floatingLeg.effectiveDate,
                floatingLeg.fixingsPerPayment,
                floatingLeg.fixingCalendar,
                floatingLeg.rollConvention,
                endDate = floatingLeg.terminationDate)
```

- Automatically manage approval procedures
- Transfer money by digital signature
- Preserve transaction records

(4-1) ISC Model



(4-2) ShieldCure Consensus Algorithm (SCCA)

SHIELDCURE Mainnet analyzes and reflects the original concepts of Role-Based Access Control (RBAC) and Security By Design, which take stability and scalability into account, based on Delegated Proof of Stake (DPoS). The SHEILDCURE blockchain is able to process transactions at a rate faster than other existing protocols through its own SCCA (ShieldCure Consensus Algorithm). In order to solve the reliability issue of Delegated Node, which is frequently mentioned in DPoS, ShieldCure Evaluation Model (SEM) is applied, which comprehensively assesses participation, number of nodes, and node attributes.

(4-2-1) Implementation of ShieldCure Consensus Algorithm (SCCA)
(DPoS + RBAC + Security by Design)

1. SCCA Delegated Proof Method
- Direct democracy through member voting
- Verifying delegate's reliability
- Delegate monitoring feature

2. Priority Node (Block Validators) selected by the voting results of Candidate Nodes with Ledger

3. No. of Nodes in the network

4. Degree of participation

5. SHIELDCURE's unique credit rating based on roles and attributes assigned by SHIELDCURE

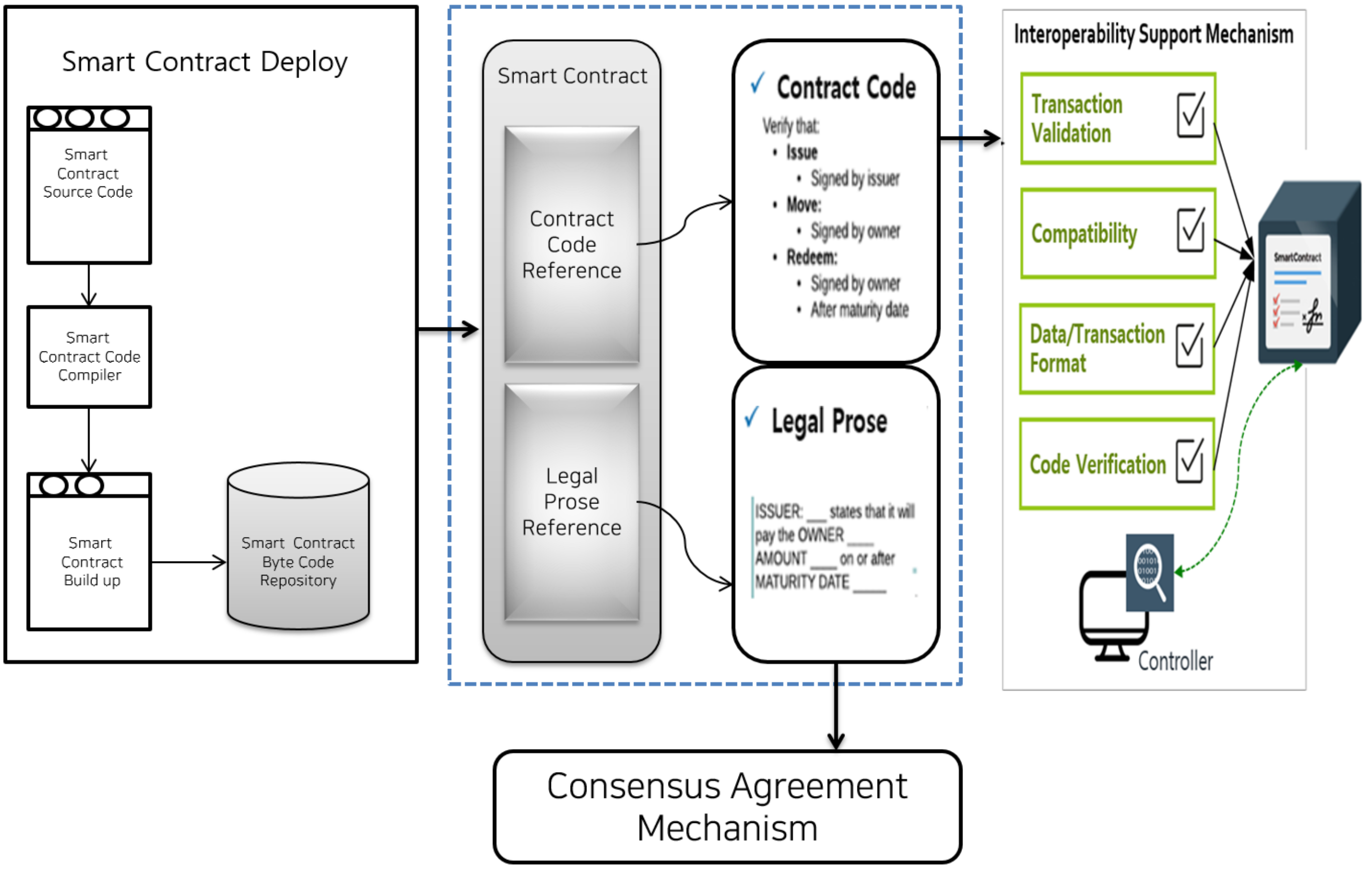
6. Candidate Node monitors the Priority Node's task and verifies other nodes.

(4-3) Safer Contract Verifier Mechanism – Stage2

Smart Contract Generation Mechanism (SCGM) and Safer Contract Verifier Mechanism (SCVM) are mechanisms to ensure ISC code reliability. They check interoperability so that the created ISC can operate in various environments, and verify the validity of execution codes and transactions, data format among others.

At the first stage of SCGM and SCVM development, we are developing a method for contracting parties to make an electronic contract with ISC template in the form of a standard contract and variables imported from HTML pages even if the parties cannot program. In the second stage, we will build features to verify data format, transaction format, code validity, and compliance with Secure Coding in order to prevent code errors that may be caused by input data during execution of ISC.

(4-3-1) Example of SCGM Flow



2-3 Technical Roadmap (v.1.0)

2018.2Q

- SHIEDLCURE TOKEN Generation
- Interface Biometric Authentication into ID Wallet
- UX design/Build ID Wallet Alpha Version
- Define Long Term Technical Roadmap
- User testing

2018.3Q

- Provide SHIELDCURE Token
- Build Dapp for ID Wallet
- Testing Multi-cryptocurrency ID Wallet
- Define Mainnet Development Scope
- Develop ID Wallet API

2018.4Q

- SHIELDCURE Mainnet Prototype (Beta Version)
- Release USB/Card Type Cold Wallet
- Release Multi-Cryptocurrency ID Wallet
- Design and Develop to SPA (Focus on Security)
- Smart Contract API
- Alliance Start up

2019.1Q

- Optimize to the SCCA(ShieldCure Consensus Algorithm)
- Develop P2P Exchange Beta version
- Stabilize/Expand ID Wallet

2019.2Q~

- Testing Mainnet (User Test/System Test)
- Release SHIELDCURE Mainnet 1.0
- Design and Develop to SPA (Focus on Privacy Act)
- Develop DAMS(Digital Asset Management Service)

3. SHIELDCURE Business View

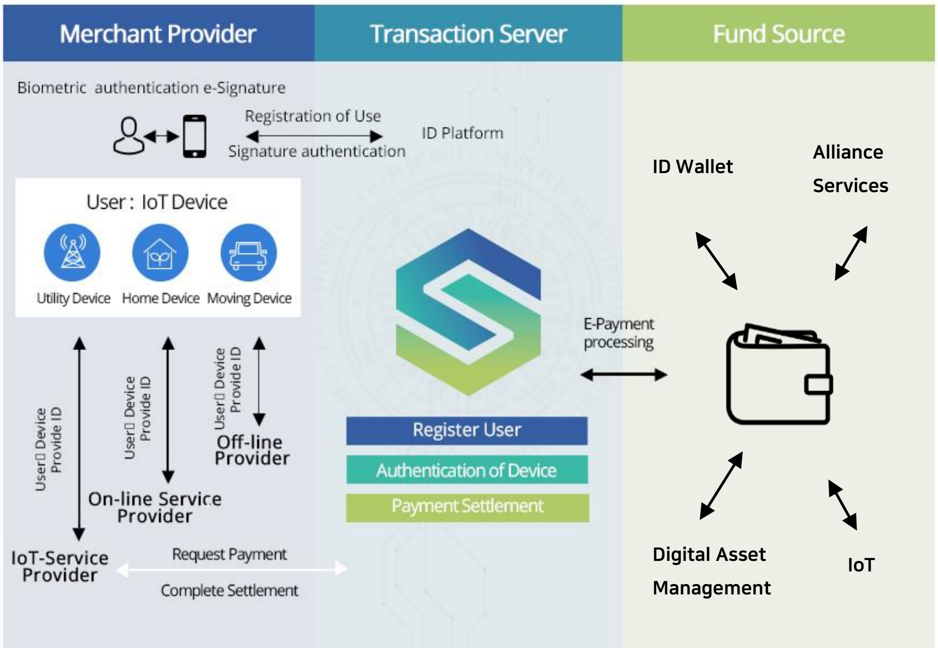
3-1. User Benefits

3-1-1. Enhance Security and Accessibility

Users use three factors - knowledge, possession and inherence- as a means to prove one's identity when accessing a service. Passwords based on knowledge can be forgotten and possessed keys can be lost. However, passwords based on biometric recognition which is inherent to oneself can never be leaked nor lost, and are convenient to use. SHEILDCURE replaces or integrates private keys with biometric recognition when accessing blockchain services provided by SHIELDCURE to minimize the exposure of private keys. As such, security will be strengthened compared to existing services, allowing users to more securely store and access information and digital assets.

3-1-2. Easy to use Wallet

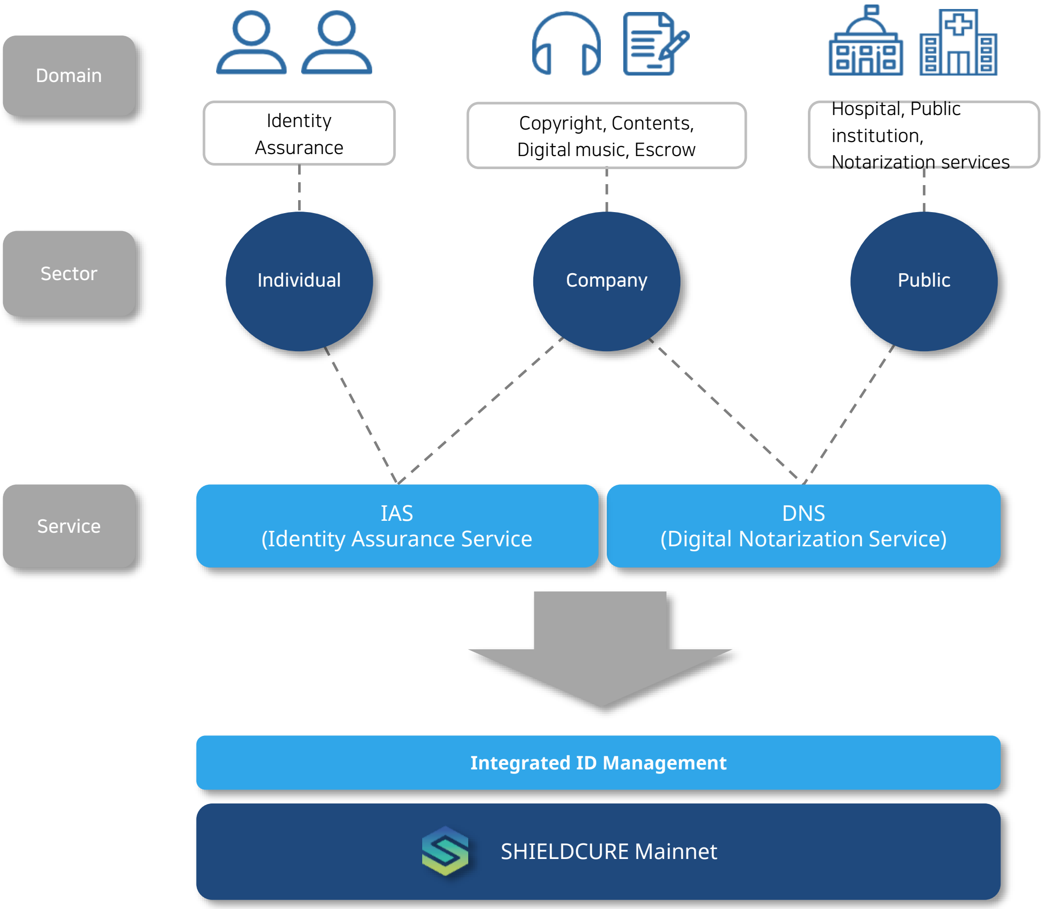
User needs have become diversified as the blockchain technology improves and various blockchain services are introduced. Users are expressing more and more desire to pursue convenience and services more valuable to oneself.
To meet such demands, SHIELDCURE provides ID Wallet in the form of an application which is designed considering 1) provision of information 2) clarity of information 3) availability and 4) interoperability.
Users can receive clear information and use an electronic wallet in the form of an app more easily and quickly. The electronic payment system will continuously be needed in the era of Internet of Things (IoT). SHIELDCURE aims to build an environment in which users can make payments with Utility, Wearable and Home Device using ID Wallet thanks to its interoperable nature.



3-1-3. Provide digital identity service

SHEILDCURE provides a blockchain-based digital identity assurance service. Individual users and service providers within the ecosystem can use an identity confirmation and verification service through Identity Assurance Service (IAS), and services providers and public institutions can use notarization services through Digital Notarization Service (DNS). IAS and DNS will be provided on the Service Layer in the SHIELDCURE Mainnet.

Existing systems required high operation costs and had centralized server problems but SHEILDCURE's blockchain-based identity assurance service will improve security and efficiency, and clarify some uncertain operational areas with decentralization. As SHEILDCURE provides an integrated identity management system, service providers and public institutions don’t have to build separate ones, thus can reduce costs.


Domain
Identity Assurance
Copyright, Contents, Digital music, Escrow
Hospital, Public institution, Notarization services
Sector
Individual
Company
Public
Service
IAS (Identity Assurance Service
DNS (Digital Notarization Service)
Integrated ID Management
SHIELDCURE Mainnet

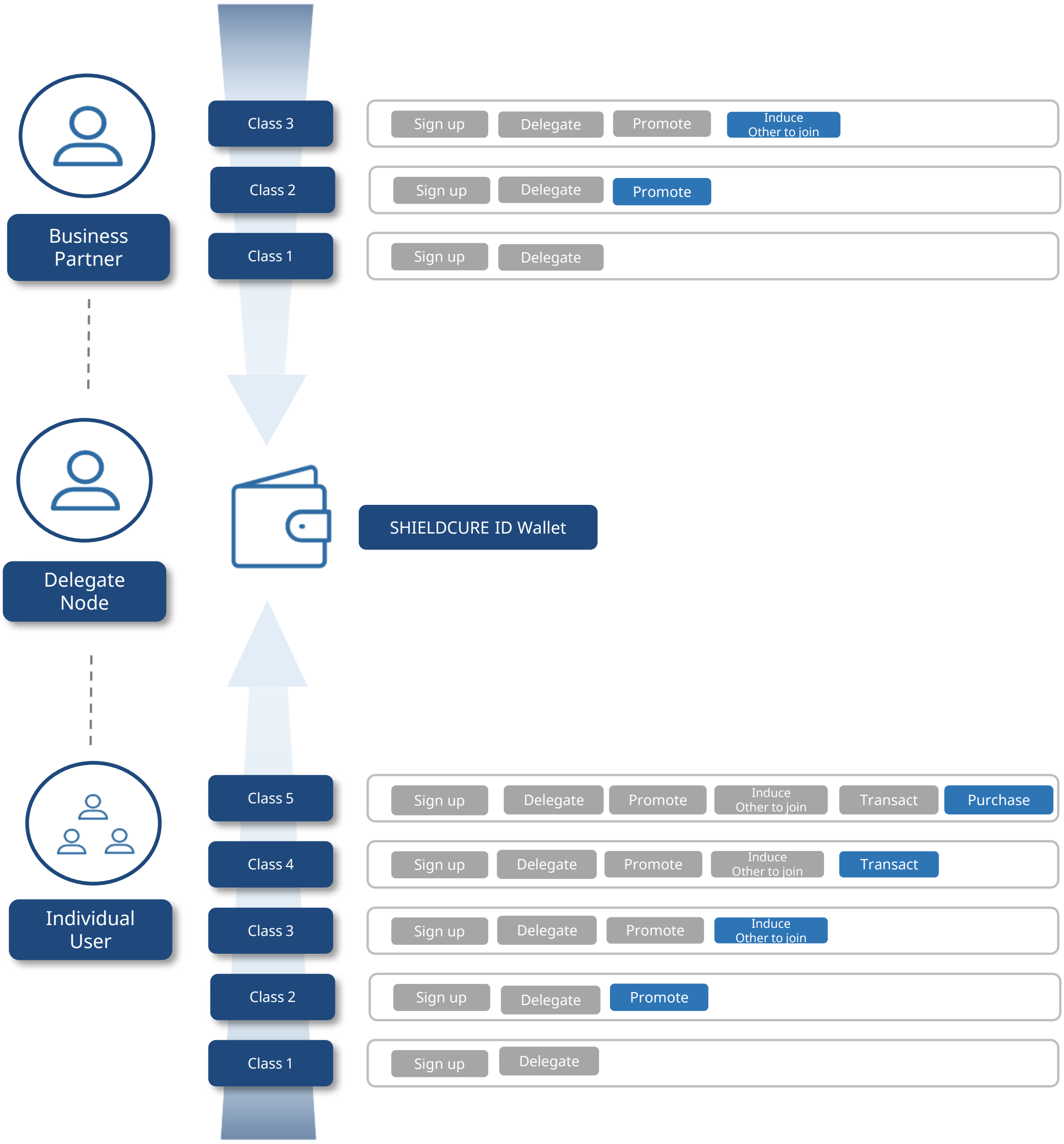
Identity Assurance Service (IAS)
Using Multi Factor Authentication Mechanism (MFAM), ISA assures users' identity with differentiated level of authentication methods from SIMPLE Authentication using ID/PW to STRONG Authentication based on multibiometric recognition.

Digital Notarization Service (DNS)
Cumbersome notarization services can become convenient and verified on the SHIELDCURE platform.

3-1-4. Interests / Rewards for ecosystem participants

Every participant within the SHEILDCURE ecosystem uses ID Wallet. Participants will be divided into different classes based on their role and what they do with their ID Wallet and each class will be given different amount of interests. For example, individual users who download ID Wallet, sign up and cast a vote to elect delegate nodes before trading assets will be given higher interests than the ones who just set up an account. It is an attempt to activate the use of ID Wallet by providing incentives to users with higher participation rate. Service providers, too, will be fallen into different classes and be given higher rewards if they provide diverse services or services to more users.
The range and amount of Interests and Rewards will be decided after going through simulations of various models. The selected model will be applied as the chart below.

.



4. Vision

4-1. To-be Model

SHEILDCURE Blockchain provides Blockchain as a Service (Baas) together with the Alliance based on identity authentication to ultimately build an information data economic ecosystem where information and data owned by individuals can be traded freely.

As the name of the project "SHEILDCURE" presents, security is at the center of SHEILDCURE and is the basis of various Bass built on top of identity authentication. SHEILDCURE Blockchain provides the following four major features:

1. Filtering feature for de-identification when collecting, using, providing and managing personal information to prevent possible data leakage

2. Strong identity confirmation feature based on biometric recognition and public key infrastructure (PKI)

3. Trust model applied with three major security governance mechanisms (R&R, SoD, LoP) and RBAC-style decentralized access control model considering Security By Design from the initial development stage of the blockchain

4. Data utilization feature with personal information guidelines in compliance with international legislation such as Europe’s General Data Protection Regulation (GDPR) and that of the OECD.

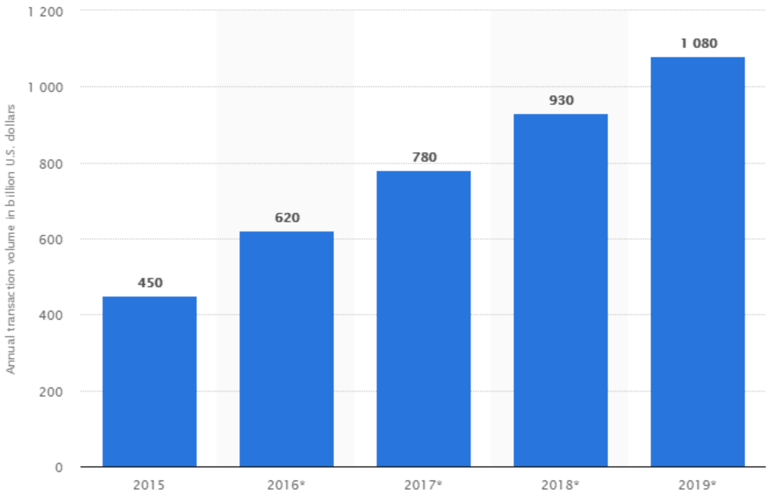
Using the aforementioned features, users can register and store personal information and assets that can only be accessed by the owner on the off-chain database for real-life usage, and allocating minimum amount of information needed to be shared on mainchain blocks such as major transactions, accessibility to data, and registration and access history. Service providers can reduce costs since they don’t have to build and manage their own security services by using the SHEILDCURE platform.

As users will be accessing the chain with device sensors in the era of IoT, the trustworthiness of privacy protection and information gathering are most important. Along with the trustworthiness of information and integrated confirmation of user, device and information provider using the blockchain, fast processing speed is also very much needed. SHEILDCURE Blockchain will build a safe gateway into the blockchain specialized in IoT in cooperation with various partners based on already secured trust.

DAMS with ID COIN will be a foundation for improving scalability of the SHEILDCURE platform as it connects the platform with the real economy based on identity authentication. When the official ID Wallet is released, owners of various digital assets, which are equipped with security function and registered after going through identity authentication, can freely trade their assets. SHEILDCURE plans to expand into digital finance by providing optimal transaction information through interworking with multi-exchanges and on- and off-line transactions through affiliated companies. Business models with specific detail will be disclosed through the official channel or paper later on.

4-2. Digital Asset Management Service (DAMS)

The Fintech industry encompassing Internet-only banks and easy payment services has grown rapidly around the world since the first introduction of Paypal thanks to the development of ICT technologies. The mobile transaction market, in particular, based on mobile devices is growing at a rapid pace and competition to become a dominant player in the market is getting fiercer and fiercer.



2015-2019 Total Revenue of Global Mobile Payments Market [Source: Statista, 2018]

Currently, there are Apple Pay, Android Pay and Samsung Pay in the market, which is continuously growing at a fast pace. Korea is also experiencing a radical change due to the spread of smartphones and biometric authentication technologies, and the competition among relevant companies. As of August, 2017, more than 10 trillion Korean won (KRW) was paid through Korea's five major easy payment service providers including Samsung Pay, Naver Pay and Kakao Pay. Payments made with easy payment services soared in 2017 to 57.9 billion KRW from 41 billion KRW in 2015 in terms of the average amount used on a daily basis. It can be analyzed that more and more customers who were used to the existing transaction system are switching to the service that allows easy payment on- and off-line without cumbersome process including verification by an official ID certificate. Payment service in the form of an electronic wallet is expected to garner more attention going forward as there will be more people using smartphones, more usage and various additional services introduced.

Recently, integration of cryptocurrencies and payment service is garnering much attention. Various companies are researching and developing blockchain and fintech technologies to allow digital assets to be used in real life. Companies such as Centra, Monaco and TenX have materialized a payment system with a debit card and an application. However, Centra was delisted recently as it was subjected to SEC investigation under the accusation of collecting illegal funds with false information. Some Korean offline retail stores and online companies such as We Make Price and With Innovation are attempting to build a payment system using cryptocurrencies based on the existing infrastructure.

However, there isn't a dominant payment system using cryptocurrencies that can be used in real life, so there will be a fierce competition among companies from various industries to gain the upper hand in the market. Easy payment service with cryptocurrency is more than just a service that provides a similar payment service but is a foundation of a separate ecosystem and is expected to become a new profit source for existing retail and IT companies.

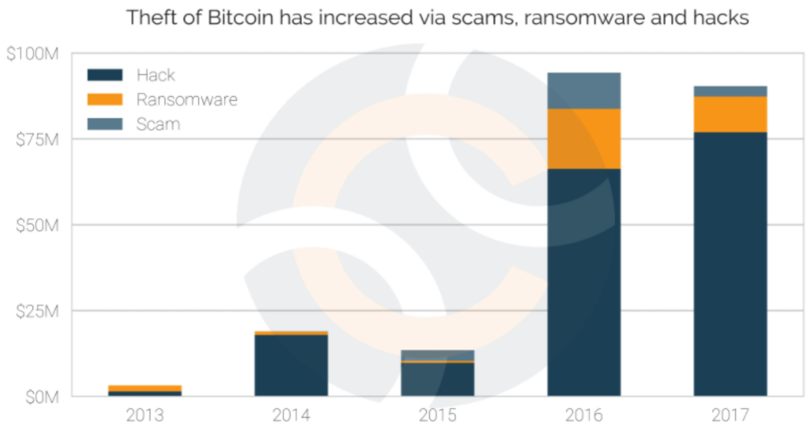
Using SHEILDCURE ID Wallet, participants can conveniently use their cyrptocurrency from their own device at affiliated stores both online and offline. The process will be carried out with the standard currency of the chain, IC Token.

The SHEILDCURE network is planned to form a partnership with VAN/POS companies which will allow real-life usage. It won't be that different from the existing mobile payment except that it is based on decentralized blockchain, so service providers will be able to support the payment with ID Token and users also can use the cryptocurrencies in their electronic wallet which are verified and selected by the SHEILDCURE Payment Policy as a means of payment, without having to upgrade their devices.

Just like P2P Exchange services, SHIELDCURE will provide information including the list of tokens that can be paid with, market prices, price changes compare to the previous day, completed or cancelled transactions and blocking function through the customer center, system monitoring function and back-up and authentication function through "fingerprint recognition devices" to increase the accessibility of users.

4-3. P2P Exchange

Existing exchanges lacked reliability due to their centralized nature.
Many cryptocurrency exchanges were attacked in 2017 and a total of 1.25 billion U.S. dollars (USD) were estimated to be lost when taking into account the loss incurred from the attacks conducted before and during 2017.



[Source : chainalysis , 2018]

Advantages of a decentralized exchange (DEX) that can solve the problems experienced by existing exchanges are surmised as below:

1. There is no central point in access and control.
The market isn't controlled by a single entity and the exchange is not supported by a single server.

2. Users manage funds.
There is no central hub controlling users' funds as there is no entity that owns DEX.

3. DEX can be integrated with hardware wallets.
When using a DEX that is integrated with a hardware wallet, users can personally send his funds to his hardware wallet using the exchange's smart contract.

SHEILDCURE ID Wallet provides a limited DEX based on ID Token on the SHEILDCURE Network. ID COIN will be airdropped after the launch of the Mainnet. SHEILDCURE Alliance Token and ERC20 tokens and others at an individual's wallet will be traded within the network on a P2P base with the exchange rate following the SHEILDCURE Exchange Rate Policy which is compatible with ID Token. Many independent tokens which were hard to be traded before the listing can be interchanged on the SHEILDCURE Network.

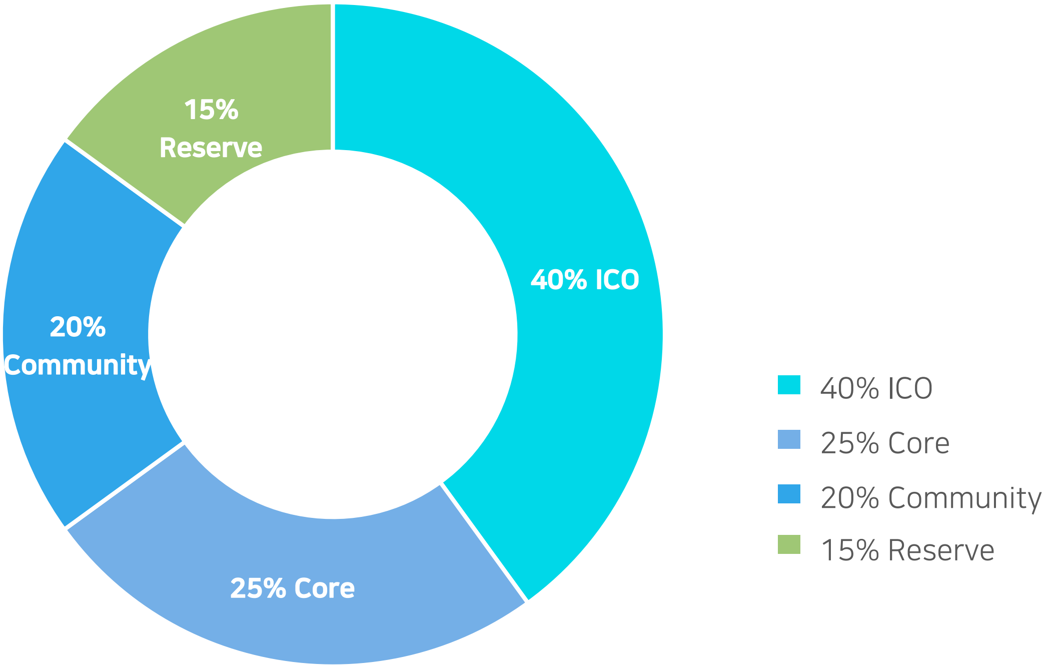
SHEILDCURE ID Wallet, which will be provided as an application, will provide information that allows exchanges and bidding with ID Token as the standard such as charts with various features (the list of coins, market prices, price changes compared to the previous day, and market cap).

Based on such information, users can check his or her transaction history and decide conditions of the trade or how much cryptocurrency he or she wants to trade. A chat room function between trading parties which will allow transaction requests and access is under development as well.

5. ICO Plan

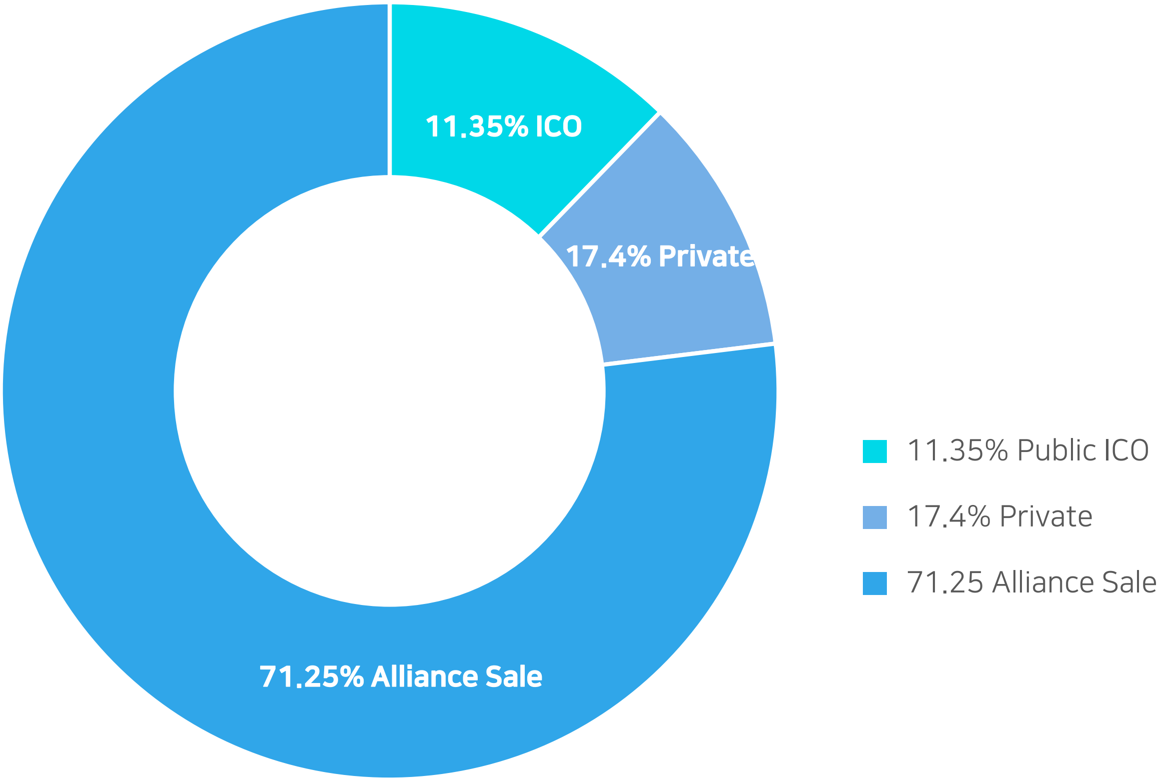
5-1. Distribution

SHEILDCURE project will issue 5 billion ID Tokens and 2 billion of them will be allocated for participants. The remaining tokens will be used for Mainnet development and core partners, and include a backup pile for building the Alliance ecosystem and restoration of the lost amount.



- ICO 40%
- CORE 25%
- COMMUNITY 20%
- RESERVE 15%

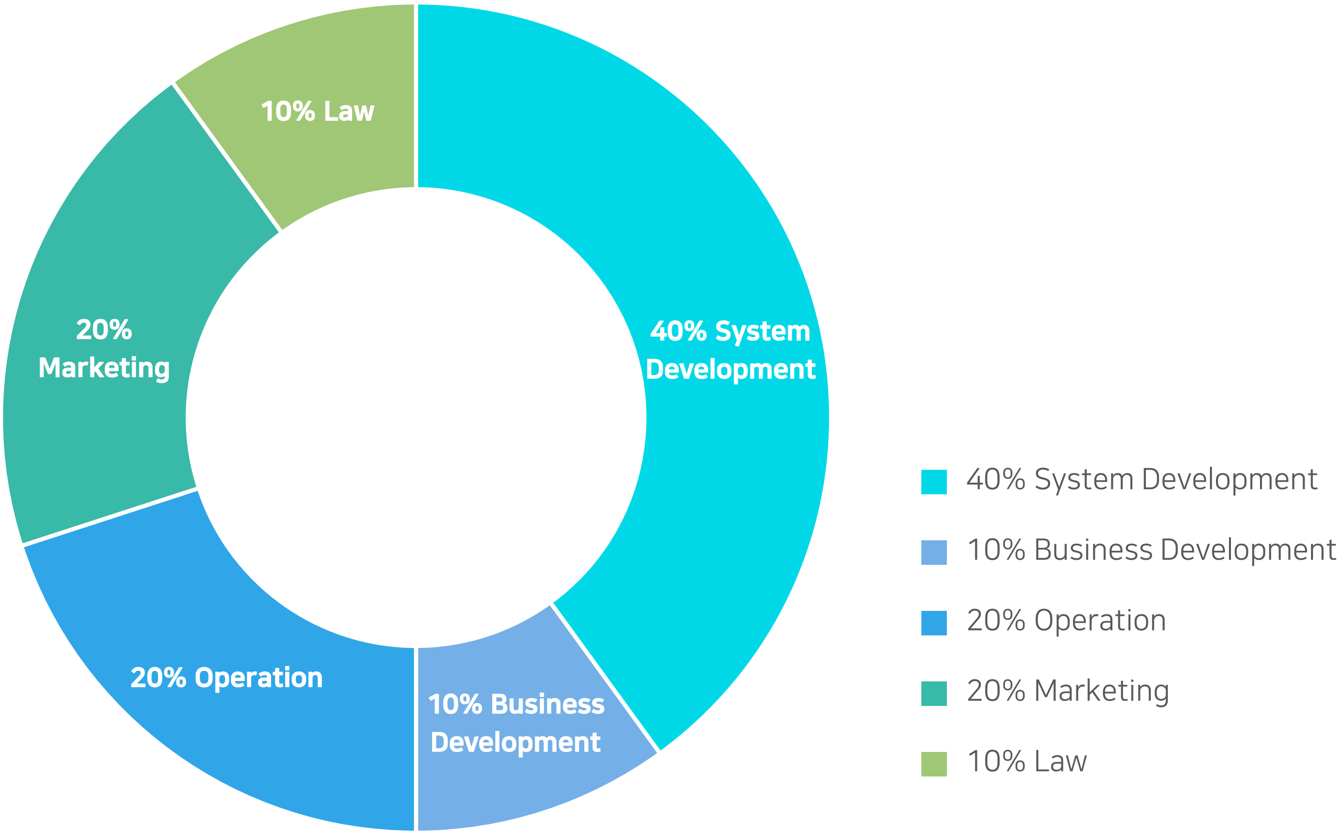
5-1-1. Crowdsale Distribution



A total of 2 billion ID for the ICO will be distributed as the following:

- PUBLIC ICO 11.35% (227 million IDs)
- PRIVATE 17.4% (348 million IDs)
- ALLIANCE SALE 71.25% (1.425 billion IDs)

5-1-2. Budget Allocation



5-2. Team & Advisor

FOUNDER

Taebong Kim

- CEO
- Chair of board of directors at KTB Global
- CEO of KTB Solution

James Jung

- CSO
- CEO of Golden Globiz
- LG CNS: Business Analyst, Director of B2B incubation

Cheolhwa Yu

- COO
- KTB Solution COO

ADVISOR

Hajin Jhun

- Chair of self-regulatory committee under Korea Blockchain Association

Dr. Alex Zhavoronkov

- Token CEO of Longenesis
- President of Insilico Medicine

Evan Caron

- CEO of Switch Coin

Dr. John Clippinger

- Prof. at MIT Media Lab

Eyal Oster

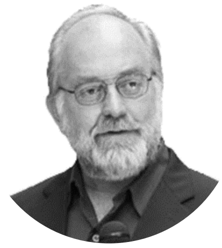
- CEO of Mobile Bridge

Dr. Jerome Glenn

- President of Millennium Project

Dr. Ben Goertzel

- Chair of Global AI Research Center



Thomas Frey

- President of De Vinci Research Center

ADVISOR

Mila Popovich

- President of Global Women in Blockchain

Youngsook Park

- Chair of The Millennium Project Korea (UN Future Forum)

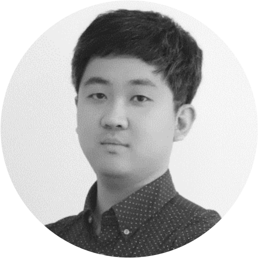
DEVELOPER

Shawn, Harmsen

- Senior Software Developer
- Swytch coin main developer

Dongwan Kim

- Blockchain Developer
- Mainnet Development



Teakwang Park

- Blockchain Developer
- Mainnet Development
- Security Specialist

Shinhaeng Oh

- Senior Software Developer
- Completed Doctoral Program in Computer Science and Engineering at Seoul National University
- Graduated from Korea Advanced Institute of Science and Technology with a bachelor's degree in Computer Science
- Public Service Agent at ATSolutions

Yoonsang Jung

- Senior Software Developer
- Graduated from Yonsei University with a bachelor's degree in Computer Science
- Developer at ATSolutions

Yonghun Lee

- Software Engineer
- Multi Biometric Authentication
- Multi Crypto Currency Wallet

MARKETING

Jaemin Ryu

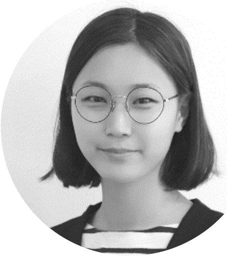
- Senior Marketing Director
- CEO of ALCO

Changhee Lee

- Strategic Planning Manager
- Business Developer

Seyeong Oh

- Blockchain Analyst
- Planning Manager



Jin Jang

- Blockchain Analyst
- Marketing Manager

7. Legal Issues

NOTICE

The SHEILDCURE Whitepaper is to provide information for those who have interests in the SHEILDCURE project. This whitepaper is not a guidebook or a proposal, and neither it is for attracting investment nor securities of a certain jurisdiction. ID Token explained in this whitepaper is not securities of any kind. The information written in this whitepaper wasn't screened nor approved by the regulation authorities, so measures in accordance with the rules and regulations of the jurisdiction will not be applied in case of a failure. As such, no individual can make a legally binding promise or contract regarding sales and purchase of tokens based on the whitepaper. Reproduction and distribution of information included in the whitepaper for any purpose is not allowed under any circumstance. The SHEILDCURE Foundation is not reliable for any indirect, special, collateral, consequential or other losses incurred based on the whitepaper. The SHEILDCURE Foundation and the distributors of the whitepaper have no obligation to give representations and warranties of any kind, thus bear no responsibilities.

STATEMENTS

All the information stated in the whitepaper is written by the SHEILDCURE Foundation and part of the information is future oriented. Such statements can be identified with the words such as "plans to," "is planned to," "is expected to," "will," "aims to," or any other similar phrases. However, these phrases are not the only identifiers for future-oriented contents. SHEILDCURE wrote the plan and prospect of the project based on forecasts of relevant technologies and business aspects. Such forecasts include expected results, achievements but at the same time entail unidentified risks, uncertainty and other factors. So, information included in the whitepaper is not a promise or statement of development process or guarantee of future achievements or rewards. Also, SHEILDCURE is not obliged to or responsible for updating contents in the whitepaper for disclosure.

RISK

Investors who are considering the purchase of ID Token mentioned in the whitepaper must thoroughly consider and evaluate the risk and uncertainty associated with the SHEILDCURE project. If any risk or uncertainty embedded in the whitepaper develops into an actual event, it may have an adverse impact on the business, finance and operation of the SHEILDCURE Foundation. But in such a case, you may lose partial or entire value or your ID Token.

6. Reference

[1] Nakamoto, Satoshi. Bitcoin: “A peer-to-peer electronic cash system”, URL: http://www.bitcoinorg/bitcoin.pdf, 2008

[2] Korea's Financial Services Commission, "Research on how to introduce blockchain technology into financial se ctor," 2016

[3] Jeong Jae-won, A Study on t he Systems, Technical Problems, and Solutions for Investigation of Crimes Abusin g Bitcoin, Seoul National University, master's thesis in digital forensic at Graduate School of Convergence Science and Technology, 2016

[4] Szabo, Nick. The idea of smart contracts. Nick Szabo’s Papers and Concise Tutorials, 1997

[5] Hwang Gyeong-rak, A Study on Bitcoin Mechanism Analysis in detail and improvement research, master's thes is in Information Security at Graduate School of International Affairs and Information Security, 2017

[6] Yang Hae-sul, A Study on The Blockchain-based Financial Information Service Model- focusing on transaction o f national housing bonds, doctoral thesis in Hoseo Graduate School of Venture, 2017

[7] Park Su-min, Design and application of reliable blockchain in digital business environment, master's thesis in C omputer Science at Sungshin Women's University, 2017

[8] Korean Society for Internet Information, Study on Applicability of Online Voting System Using Blockchain, Com missioned by Korean Civic Education Institute for Democracy, 2017

[9] Lee Bu-hyeong, Lim Eon-ju, Lee Jong-hyeok, Consensus Algorithm on Blockchain Platform, Korean Institute of Communications and Information Sciences, pp 386~387, 2017

[10] Miguel Castro and Barbara Liskov, “Practical Byzantine Fault Tolerance”, USENIX Technical Program - Paper - Proceedings of the Third Symposium on Operating Systems Design and Implementation, 1999

[11] Jae Kwon, “Tendermint: Consensus without Mining”

[12] https://tendermint.com/intro/consensus-overview

[13] DAYLI Financial Group (https://daylifg.blog.me/)

[14] Shin Dae-hye, Lee Jong-hyeob, Security of Smart Contract for Fintech, Korea information processing society r eview Vol.22 No.5, 2015

[15] Structure and Theory of Blockchain, Wikibooks

[16] https://litemap.net/

[17] Kang Min-hyeok, Park Min-gyeong, Kwon Tae-gyeong, User-centric Identity Management System Using Smar t Contract, Korean Institute of Communications and Information Sciences, 2018

[18] https://ethereum.stackexchange.com/

[19] http://samse.tistory.com/465, Executing Swarm to test Dapp

6. Reference

[20] Yu Hyeong-u, A study on performance improvement and implementation of electronic voting system using bl ockchain, master's thesis at Graduate School of Information and Communication Technology, Ajou University, 20 16

[21] Lee Ru-da, Electronic Voting Systems Using the Blockchain, master's thesis in Computer Science, Sangmyung University, 2017

[22] Yang Min-hui, A Design and Implementation of Health Insurance Condition Discount System Using Blockchain, master's thesis in Electronoics and Computer Engineering, Hanyang University, 2018

[23] Lee Sang-min, A Study on Copyright Protection Method of Digital Contents using Block Chain, master's thesis, Graduate School of Information Sciences, Soongsil University

[24] Lee Chan-hyeok, Design and Implementation of IoT Data Protection System using Block chain, master's thesis in Knowledge Information Enginnering, Ajou University, 2018

[25] Jaume Barcelo, "“User Privacy in the Public Bitcoin Blockchain." 2014

[26] Ahmed Kosba, “Hawk: The blockchain model of cryptography and privacy-preserving smart contracts”. Security and Privacy (SP), 2016 IEEE Symposium on, (2016) May22-26, San Jose, CA, USA, 2016

[27] Mustafa Al-Bassam , “SCPKI: A Smart Contract-based PKI and Identity System”, BCC '17 Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, 2017

[28] Jeong Han-jae, Design and Implementation of Blockchain Based Digital Identity Management System, Special ized Graduate school of Software, Soongsil University, 2017

[29] Gavin Wood, “Ethereum : A secure decentralized generalised transaction ledger.” Etheruem Project Yellow Paper, 2014

[30] Vitalik buterin, Ethereum white paper: a next generation smart contract & decentralized application platform, Ethereumm.org, 2014

[31] Xiaoqi Li, Peng Jiangm Ting Chen, Xiapu Luo, Xiapu Luo, Wen, “A survey on the security of blockchain systems, Future Generation Computer Systems”, 2017

[32] Alexnadra Covaci, “NECTAR : Non-Interactive Smart Contract Protocol using Blockchain Technology”

[33] https://www.ethereum.org

[34] David Cerezo Sanchez, “Private and Verifiable Smart Contracts on Blockchains”, https://eprint.iacr.org/2017/878.pdf, 2015

[35] Kim Gwamg-seok, Trend of four major fintechs and implications to financial industry, Institute for Informatio n and Communications Technology Promotion, Weekly Technology Trend, 2016

[36] Buchman, Ethan , “Tendermint: Byzantine Fault Tolerance in the Age of Blockchains”, In partial fullment of requirements for the degree of Master of Applied Science in Engineering Systems and Computing, 2016

6. Reference

[37] Chrysoula Stathakopoulou, “On Scalability and Performance of Permissioned Blockchain”, EuroSys Doctoral Workshop ’18, April 23, Porto, Portugal, 2018

[38] Signe Rusch, “High-Performance Consensus Mechanisms for Blockchains”, EuroDW’18, April 23, Porto, Portugal, 2018

[39] Alysson Bessani et al. “A Byzantine Fault-tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform”. In: Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. SERIAL ’17. 2017.

[40] Vitalik Buterin et al. Casper the Friendly Finality Gadget. 2017. url: http://arxiv.org/abs/1710.09437

[41] Yossi Gilad et al. “Algorand: Scaling Byzantine Agreements for Cryptocurrencies”. In: Proceedings of the 26th Symposium on Operating Systems Principles. SOSP ’17. 2017.

[42] National Law Information Center (http://www.law.go.kr)

[43] Chae Song-hwa, Research result of ICT R&D planning and analysis project by Ministry of Science and ICT(MSI T), 2017

The world's most secure identity information-based
blockchain platform
using the multi biometric authentication technology

SHIELDCURE Whitepaper (Ver1.0)