THEKEY MVP/Mainnet Technical Report
Of
Blockchain based Dynamic Multi-Dimension Identification

THEKEY Project Team, November 2018, Beijing, China

Table of Content

1. BACKGROUND

After the completion of the first phase MVP, THEKEY has accomplished the technical Proof of Concept of Blockchain based Dynamic Multi-dimension Identification (BDMI) Technology, and the “undeniable” and “unalterable” EA5 (e-authentication 5) level online Identity Verification (IDV) results were generated. At the same time, THEKEY has integrated IDV and digital wallets to form the Real Identity Wallet (RIW) for the first time in the world, which will play a significant role in anti-money laundering applications, therefore lays a solid foundation for the healthy development of cryptocurrency and the digital economy.

In our MVP/Testnet Progress Report, it’s stated that THEKEY Project will focus on improving the performance, efficiency and reliability of BDMI technology based on the first phase achievement, so as to be put into real-world application as soon as possible. In addition, we also decided to research on Secure Environment (SE) to support RIW, user data and program engines.

2. SOLUTIONS TO THE KEY ISSUES

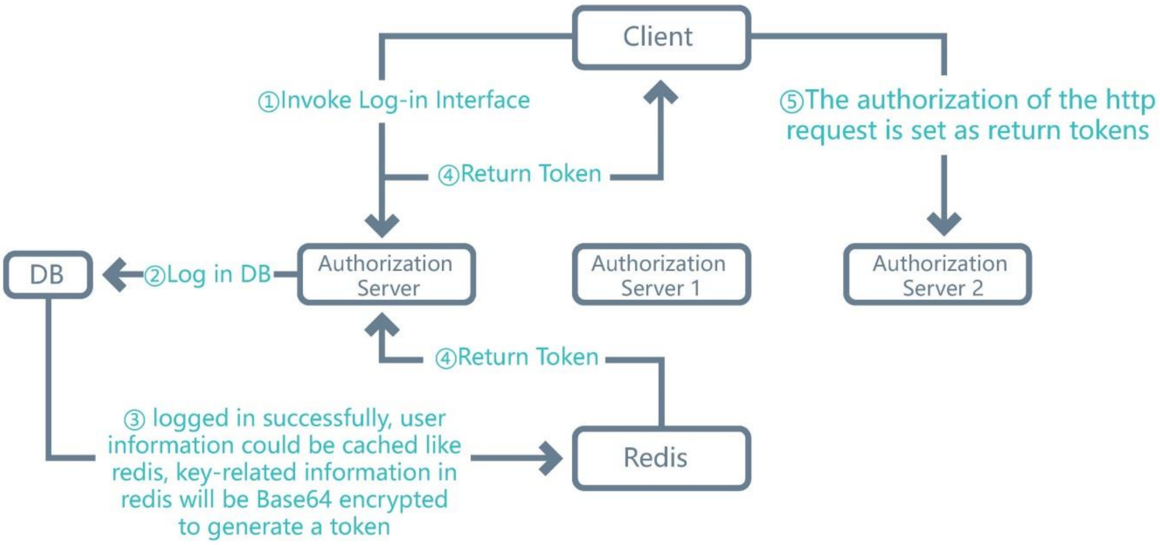
In regard to the issues mentioned in the MVP/Testnet Progress Report, we have conducted experiments and researches, focusing on improving BDMI capabilities, SE and multi-scenario applications, and worked out solutions and accomplished technical upgrades accordingly.

2.1 BDMI Capability Improvement

In order to improve BDMI capability, such as performance, efficiency and reliability, we have accomplished improvements as following:

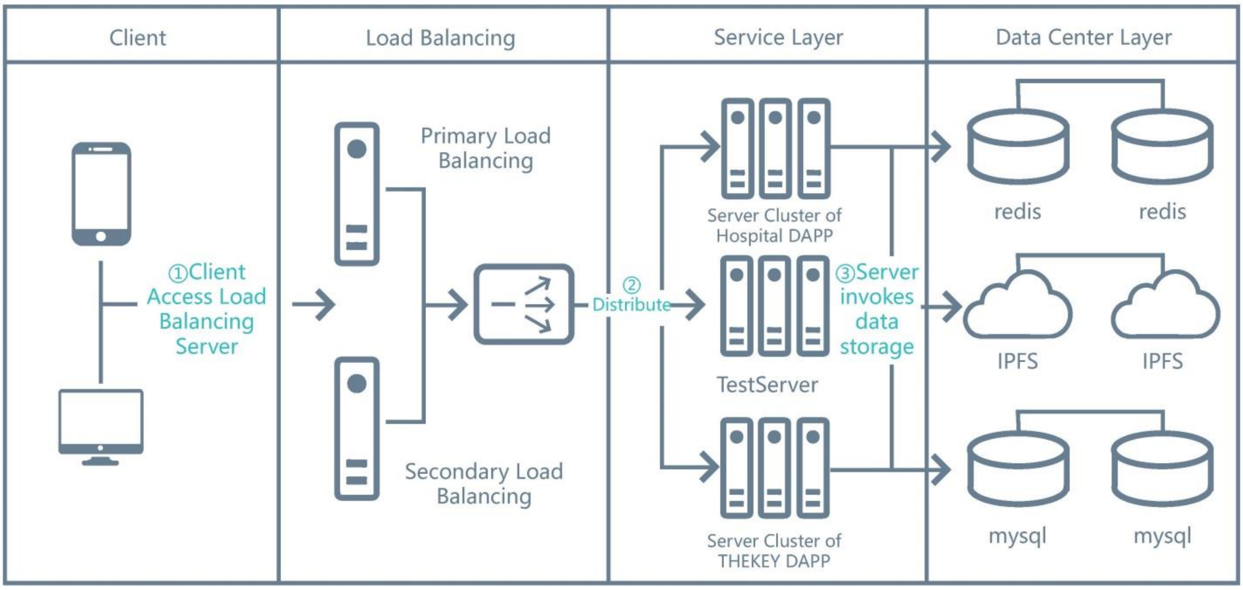
2.1.1 Technical Upgrades for Performance Improvement

The system performance is improved by implementing the authentication token to solve the on-chain high-concurrency problems. User logs in by username and password, and then the user information is stored in the cache, and the server receives the request to verify the username and the password. After the successful verification, the key related information in redis will be encrypted using Base64 to generate a token, which will be then sent to the user. The user saves the token (cookie or local Storage), and verification request when logging in will be sent to the server with the token. The server receives the request, verifies the token, and if it succeeds, it returns the data.


Client
①Invoke Log-in Interface
④Return Token
⑤The authorization of the http request is set as return tokens
DB
②Log in DB
Authorization Server
Authorization Server 1
Authorization Server 2
④Return Token
③ logged in successfully, user information could be cached like redis, key-related information in redis will be Base64 encrypted to generate a token
Redis

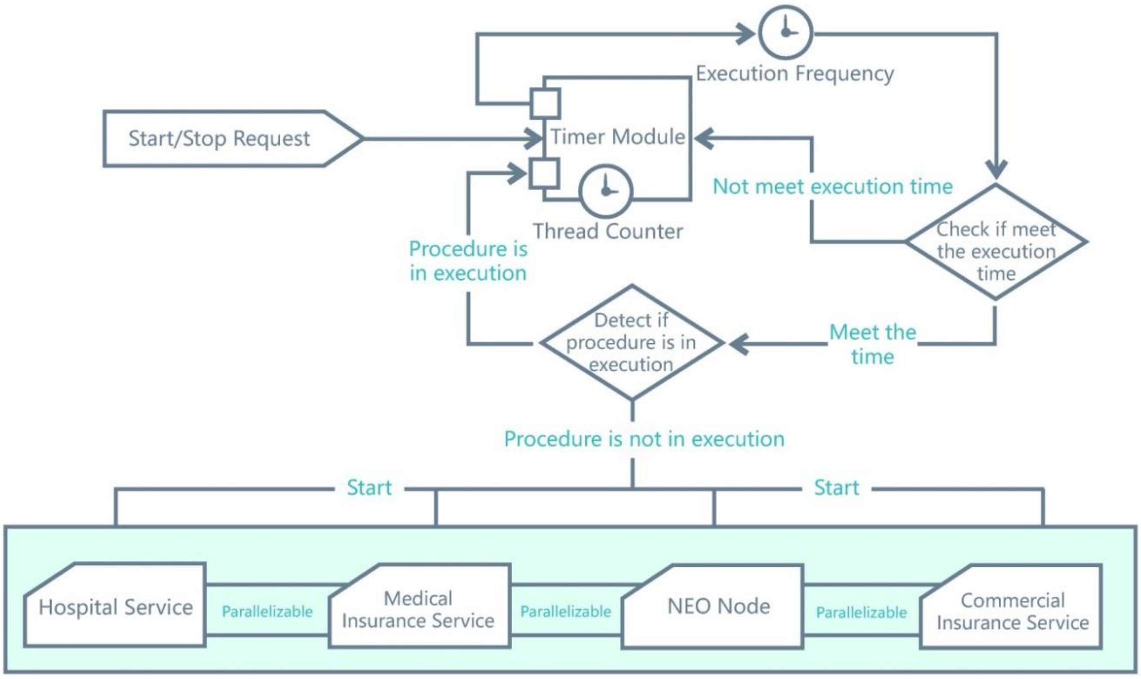
2.1.2 Technical Upgrades for Efficiency Improvement

The system efficiency is improved by optimizing the server deployment. When the user's request is sent to the server, the request is scheduled by Nginx to achieve load balancing. When the request enters the service layer, the logic is processed by the server, the information is then stored, and the results are returned. The Nginx server and load balancing strategy can greatly improve the system performance, allowing more users to join THEKEY Ecosystem and enhancing the user experience.



2.1.3 Technical Upgrade for Reliability Improvement

In avoidance of the defects and errors in software programming and the software execution failure caused by external factors, a daemon is embedded into blockchain nodes to ensure continuous availability and the system reliability. At the same time, the robustness testing of Smart Contract is conducted, including floating point errors prevention, infinite loops prevention, and output control. In addition, strategies for disaster recovery mechanism and backup mechanism of the database are developed in details.



2.1.4 Conclusions of the Test

BDMI Capability	Detailed Index	BDMI Phase 1	BDMI Phase 2
System Performance	Data Loss rate	0.4%	0.2%
	Task Amount per Unit Time	50+	200+
	Memory Usage Rate	15%	25%
	System Usage Rate	20%	35%
System Efficiency	Network Throughput	Around 70	Around 250
	Network Load Rate	50M	200M
	System Response Time	3s	2s

System Reliability	Fault Detection	N/A	Fault Detection Daemon
	Fault Recovery	N/A	Fault Tolerance
	Fault Prevention	N/A	Robustness Testing
	Data Backup	N/A	Backup, Total Increment Alternation

Technical Index Comparison of BDMI Phase 1 and Phase 2

2.2 Secure Environment (SE)

2.2.1 Purpose

The ultimate goal of Secure Environment (SE) is to protect user’s private key, data, and engines by high security level. However, the current mainstream Trusted Execution Environment (TEE) and other solutions are still immature. For example, TEE is expensive and difficult for mass-production, and lacks effective security protection mechanism. Thus, the SE realized by TEE will become unreliable in man-device separation scenario. Therefore, we need to delve into the SE research.

2.2.2 Methods

First, EA5 level IDV could solve the man-device separation problem effectively. EA5 level IDV embraces 6 elements below:

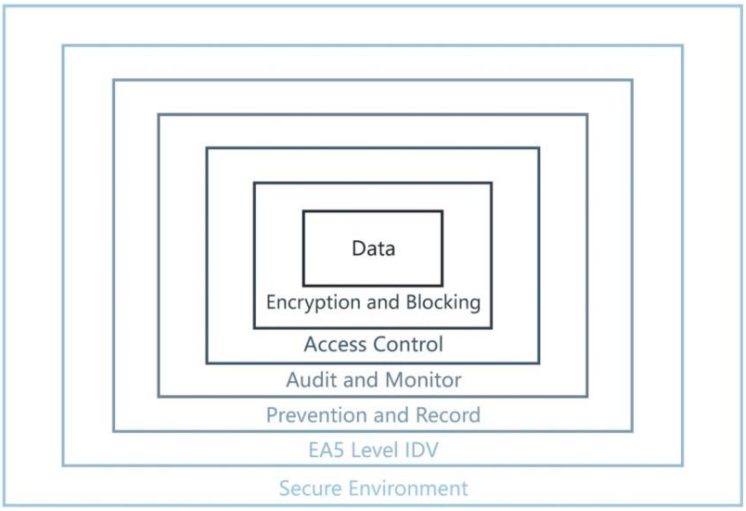
- Unique biometric data serves as the base of BDMI.
- The key data of BDMI used for IDV, including biometric data, are all validated in advance by the relevant government authorities.
- The data of BDMI used for IDV are comprehensive enough so that it can meet the different requirements of various clients.
- To ensure the reliability of BDMI, cross-checking is always carried out during IDV, between the government validated ID data and behavior data and scene data of the same user.
- To ensure solidity of BDMI, BDMI always uses updated data when an IDV is executed, to capture the latest changes, if any.
- Once an IDV is completed, the result will be properly documented for audit so that personal credit of the user can be evaluated and calculated.

Second, Secure Firewall is adopted to prevent suspected accesses and record the access details in Secure Environment, for instance who did what at what time. Secure Firewall solution consists of monitor model setting, white list setting, blacklist setting, strategy setting and so on.

Third, real-time scanning is conducted to the system environment to detect potential hazard. The complete safety strategy is developed to scan the system, alarm to the hazard, and provide optimal solution.

Forth, the access control capability is strengthened by reducing internal threaten and improving compliance. The strategy includes privileged user control, data access safety strategy, no need to adjust the application program, built-in audit and report.

Fifth, storage and backup security is achieved through transparent data encryption. Specific strategies include tablespace and column-level encryption, backup encryption and data pump encryption, unstructured data encryption and so on. In addition, the transmission process is secured through the combination of SSL/TLS and other network encryption schemes.



2.2.3 Conclusions

Through the research of the schemes and strategies as abovementioned, we have initially constructed the Secure Environment (SE) based on software. That is, an SE in which the user’s private key, data, and program engine can be stored and cannot be accessed at will by others. The “unalterable” business loop is achieved where the data are accessible only after EA5 level IDV is conducted, and all operations are completely recorded when content in SE is accessed. This scheme is embedded in our system to create a real secure environment and to ensure the rights and interests of THEKEY users.

2.2.4 Prospects of Trusted Products

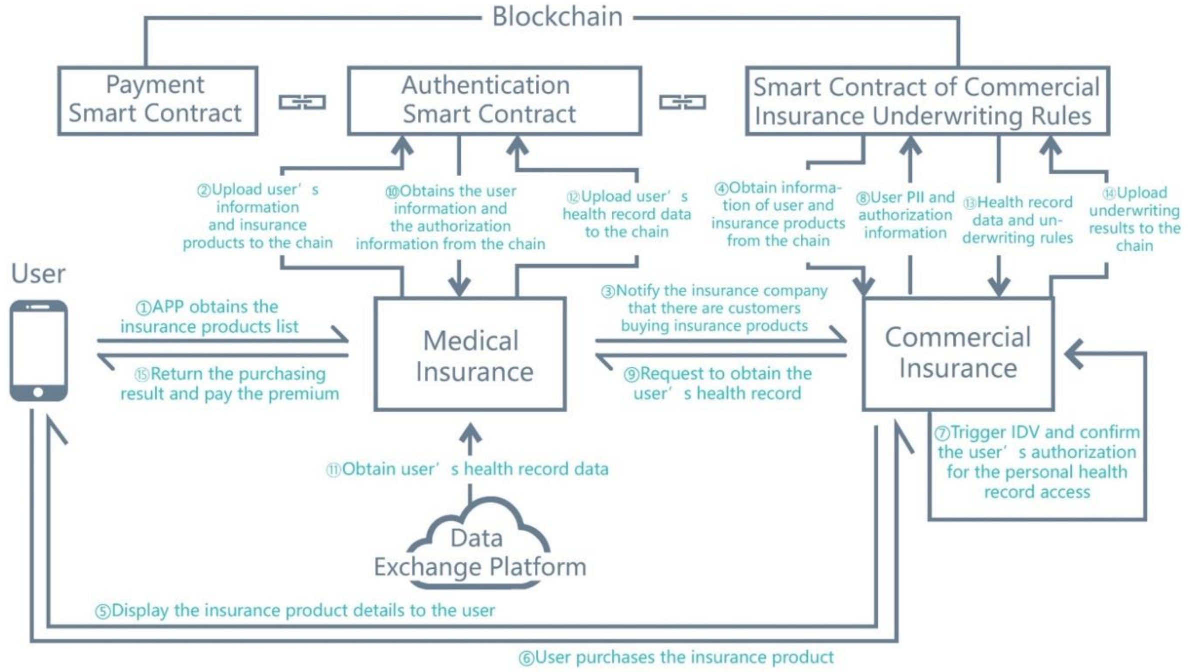
For the future development of Trusted Products, we believe that Trusted Execution Environment (TEE) and Secure Environment (SE) shall be closely integrated. Based on this research, we will further study SE, and relevant TEE according to the software requirements in SE, in order to ensure the products reliability from both the hardware and software perspectives, providing the users of THEKEY a safer and more convenient experience.

2.3 Multi-scenario Applications

2.3.1 Underwriting in Commercial Insurance

In the underwriting of commercial insurance, the medical records of the insured will be invoked to complete the process. Therefore, IDV will be conducted to the insured in the process. BDMI technology provides an optimized solution for IDV in the underwriting of commercial insurance.

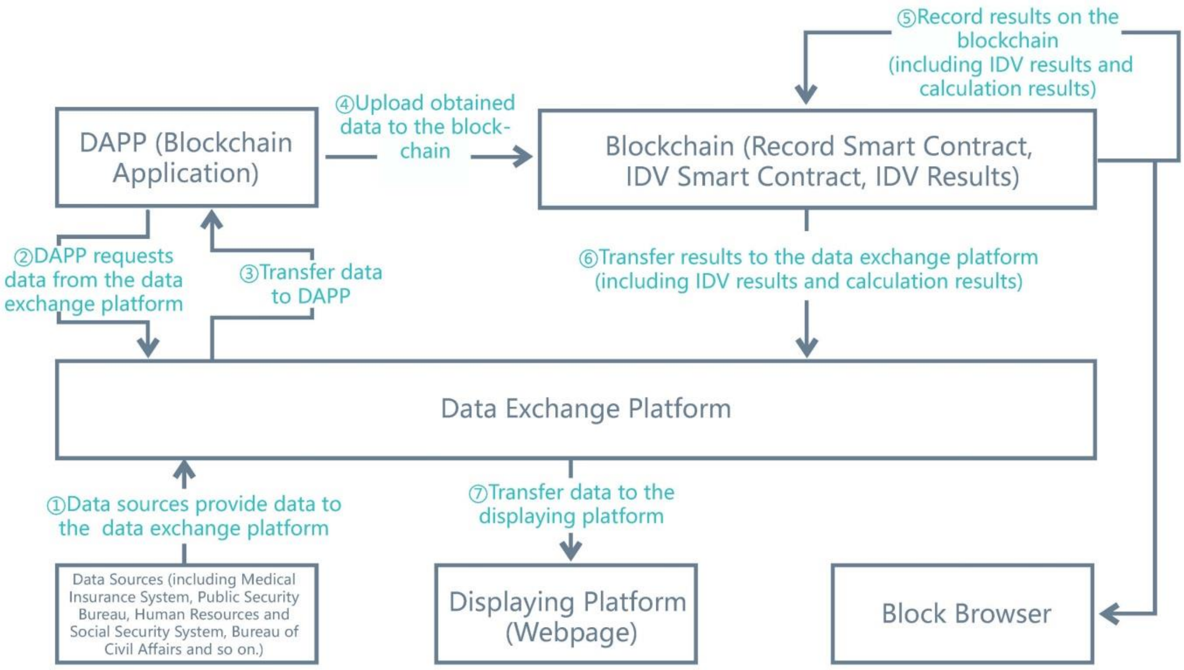
The process is as follows: first, the user browses the insurance product list through the APP to select ; the insurance company DAPP obtains the information of the user and the insurance product, and provides a detailed introduction of the product to the user; the user then confirms to buy the product; the insurance company conduct IDV by BDMI technology to the user; after successful IDV, the user authorizes the insurance company to retrieve the personal health record data; the Medical Insurance DAPP obtains the user information and the authorization from the chain and obtains the personal health information from the Data Exchange Platform and uploads to the chain; the insurance company DAPP obtains personal health information; Smart Contract conducts verification according to the underwriting rules; after the verification succeeds, the user can purchase the product and pay the premium through the APP.


Blockchain
Payment Smart Contract
Authentication Smart Contract
Smart Contract of Commercial Insurance Underwriting Rules
②Upload user's information and insurance products to the chain
⑩Obtains the user information and the authorization information from the chain
⑫Upload user's health record data to the chain
④Obtain information of user and insurance products from the chain
⑧User PII and authorization information
⑬Health record data and underwriting rules
⑭Upload underwriting results to the chain
User
①APP obtains the insurance products list
⑮Return the purchasing result and pay the premium
Medical Insurance
③Notify the insurance company that there are customers buying insurance products
⑨Request to obtain the user's health record
Commercial Insurance
⑦Trigger IDV and confirm the user's authorization for the personal health record access
⑪Obtain user's health record data
Data Exchange Platform
⑤Display the insurance product details to the user
⑥User purchases the insurance product

2.3.2 Multi-dimensional Elderly Survival Authentication

In the pension distribution scenario, pension can only be distributed after the IDV is conducted to the pensioners. Therefore, IDV is a critical step in the process. The IDV is achieved by utilizing BDMI technology, therefore to ensure the safety of the national Social Security fund and at the same time, enhance the administration and transaction efficiency and improve user experience.

The pension department triggers an IDV request of the pensioners and stores the request on the blockchain; the request invokes the IDV Engine through the Smart Contract, conducts IDV by BDMI technology and stores the IDV results on the blockchain; meanwhile the administration staff determines the pension disbursement by the IDV results.


⑤Record results on the blockchain (including IDV results and calculation results)
④Upload obtained data to the block-chain
DAPP (Blockchain Application)
Blockchain (Record Smart Contract, IDV Smart Contract, IDV Results)
②DAPP requests data from the data exchange platform
③Transfer data to DAPP
⑥Transfer results to the data exchange platform (including IDV results and calculation results)
Data Exchange Platform
①Data sources provide data to the data exchange platform
⑦Transfer data to the displaying platform
Data Sources (including Medical Insurance System, Public Security Bureau, Human Resources and Social Security System, Bureau of Civil Affairs and so on.)
Displaying Platform (Webpage)
Block Browser

3. OVERVIEW OF THEKEY ECOSYSTEM

After the two phases MVP, we have built up a complete Ecosystem, which includes:

3.1 Basic Capability

- IDV Technology
- CPA Technology
- IPFS Decentralized Storage
- NEO Smart Contract to support NEO smart economy

3.2 Application Scenario

- Underwriting in Commercial Insurance
- Multi-dimensional Elderly Survival Authentication

3.3 BDMI System Improvement on Performance, Efficiency and Reliability

- Real Identity Wallet
- Secure Environment In-depth Research
- BDMI Performance Improvement by Authentication Token
- BDMI Efficiency Improvement by Load balancing Strategy
- BDMI Reliability Improvement by Daemon, Data Backup and Robustness Test

4. CONCLUSION

After the two phases MVP, we came to the following conclusions:

First, the accomplishment of the EA5 level IDV, RIW, SE research, BDMI capability improvement and the multi-scenario application of IDV (including commercial insurance underwriting and Elderly Survival Authentication) signifies the completion of the work mentioned in the White Paper “A Decentralized Ecosystem of An Identity Verification Tool Using National Big-data and Blockchain”. The application scenarios have been deployed on the NEO public chain to support NEO smart economy.

Second, EA5 level IDV comprises two levels of IDV, namely, EA5- and EA5+ according to the two phases. In the Elderly Survival Authentication scenario, IDV without biometric authentication can satisfy the demand for accurate pension disbursement. It is a typical application of EA5- level IDV. EA5+ level IDV can be achieved by the combination of multi biometric authentication and other technologies, and meet the security demands of various application scenarios.

Third, after the two phases MVP development, BDMI Mainnet has reached the deployment standard. But there are still six aspects to be improved in the Elderly Survival Authentication deployment as following:

- Multi-scenario application requires a multi-consensus mechanism, and the current single-consensus mechanism is not sufficient to meet this requirement.
- There is a strong correlation between performance and the consensus mechanism.
- Security of whichever platform we would choose would be beyond our scope of control, leading to safety and/or security risks to data, funds and patients.
- Current platforms have not been designed to handle the sheer amount of data, such as patients’ medical image/footage, etc..
- The business logic can only be realized via Smart Contracts and DAPP development, severely limiting or negating the possibility for extreme platform capacity.
- Governance logic of virtual world does not suit the real world.

In regard to the abovementioned problems, we have worked out the solution and are endeavoring on the real world deployment. I thank you all for the support you have given to THEKEY and me. Please expect our next report.

Appendix 1: List of Codes

https://github.com/thekeygithub/MVP

Mainnet Smart Contract:

0xEA39A3BBD678714DC7E3342AF8CB02444346A95B318B5D50F17FAB1D408116D9

a) Mobile-APP: Source code of Android APP in the Android smartphone, MVP Testnet

b) Hospital-DAPP: Hospital Server Code

c) Hospital-terminal-APP: Hospital Server All-in-one Machine Program Code

d) IPFS-api: source code of IPFS private network data access API service

e) THEKEY-DAPP: THEKEY Server Code

f) NEO: Smart Contract, including Authentication Contract, Payment Contract and Data Storage Contract

g) NEO-cli-THEKEY: modified source code of neo-cli for the wallet transfer interface

h) Mobile-APP: Source code of Android APP in the Android smartphone, Underwriting of Commercial Insurance in MVP Mainnet

i) Backend-DAPP: Commercial/Medical Insurance server source code

j) Blockchain-Explore: Blockchain-Explore source code

k) Cookie Token: Authentication Token source code

l) KeepAlive: Daemon source code

m) BIgdataPlatform: Data Exchange Platform obtains source code of medical records

n) Shangbaodapp: Commercial Insurance server source code

Appendix 2: Product Procedure in Technical Report

a) The hospital DAPP collects user information and triggers IDV

b) THEKEY DAPP obtains user information for IDV and returns results

c) The hospital DAPP obtains the IDV result and the prescription ledger information, the user pays the bill, and then generates the claim settlement on the chain.

d) Real Identity Wallet

e) Authentication Token

f) Load Balancing Indication

g) Underwriting in Commercial Insurance

h) Multi-dimensional Elderly Survival Authentication

i) Smart Contract Application