ReapChain

BusinessPaper

ver 0.9

REAPCHAIN.Inc

Contents

Background

Blockchain is a distributed computing technology that provides reliability, stability, security, and efficiency of data. It is attracting attention as a foundation technology that drives the Fourth Industrial Revolution along with IoT. In particular, with the recent rapid development of hardware and network-related IoT technologies, various discussions on the convergence of IoT and blockchain are being made, and blockchain technologies in multiple fields such as production process tracking and manufacturing management processes through IoT technologies are expected to be used efficiently in the future. However, in the IoT industry, security and authentication are operated by a centralized method, but it has several side effects regarding security, cost, and trust.

ReapChain provides a new hybrid blockchain that can improve the existing IoT system and solve the problems of the blockchains through a new consensus algorithm by authenticating individual devices and by preventing data forgery based on PID of things technology. With the new hybrid blockchain, ReapChain aims to realize the distributed processing of large amounts of data generated from the IoT industry.

ReapChain proposes the following methodology to build a blockchain-based IoT-specific platform with enhanced transparency and security through ReapChainBaaS for a developer friendly-blockchain development environment.

· **Methodology**

- To establish a blockchain by blockchainifying the end-to-end section through the IoT specialized ReapChainBaaS.
- To implement PID (Private ID), a new device authentication system through a private key encryption technology of the ReapSDK.

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

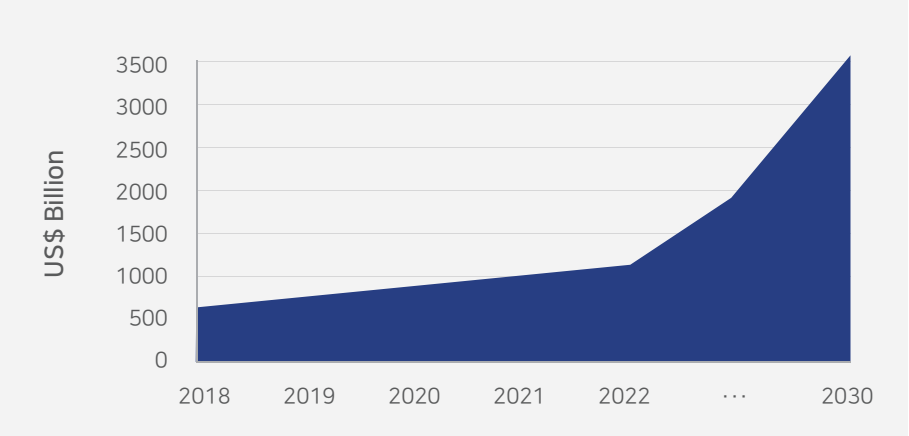
1. IoT Market Overview and Status

1.1 Global IoT Market Status

The growth of the IoT market is accelerating due to the development of communication technologies such as IoT networks, and 5G and the expansion of the infrastructure. Also, as cyber-attacks targeting IoT systems are becoming a reality, and the damages from the attack are increasing, the IoT security market is rapidly growing as well.

The total global IoT market will grow by 12.8% annually from 2016 to 2022 to reach $1.2 trillion in 2022, and by 2030, it will be a $3.1 trillion of vast market. The IoT embedded system market will reach $83.9 billion by 2023, and the global market size of IoT devices and service platforms will be $1.1 billion. Total IoT security spending amounted to $1.5 billion in 2018, with a high annual growth rate of 27.9%.

< Figure 1. Global IoT Market Forecast >



[Source : Forest and Sullivan (2018)]

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

1.2

The Need for Blockchain in the IoT Industry

With the rapid development of hardware and network-related IoT technologies in recent years, the importance of data integrity, system security, and device control in the IoT industry are increasing.

Blockchain technology is emerging as a solution in the IoT field because blockchain technology has advantages such as distributed data structure, cryptography theory and security technology, and consensus technology that is hard to manipulate and change data.

< Table 1. Expected Effects of Blockchain Technology Adoption in the IoT Industry >

Category	Benefit
Improve data reliability	In the blockchain, data is stored in encrypted form and is shared with all participants, not in a centralized way. Because participants continuously verify the shared ledger, it is almost impossible to forge and alter the recorded data, and it ensures reliability by breaking away from the centralized control method.
Improved security (device authentication)	The distributed structure of the blockchain does not affect the overall performance even if one part of the operation stops working, and it is relatively safe from attacks such as DDoS or hacking threats because it can prevent access by unauthorized users.
Vigorous Data transaction	Transactions are possible in a P2P method without a central system or an intermediary. Also, It is possible to purchase the IoT device license or industry-related data with blockchain tokens.

Blockchain can be applied systematically to the IoT industry, where connection and data sharing of various devices is emphasized, as it can effectively utilize the strengths of distributed data storage. Also, since the centralized system and infrastructure are not needed, facility investment and operating costs can be lowered, helping the expansion of the IoT industry.

In particular, the blockchain applied IoT system will present an opportunity to expand the application areas of the IoT industry. Centered on fields that emphasize the convenience of P2P-based data sharing and the safe data storing and utilizing, the needs for introducing blockchain-based IoT systems are expected to increase.

2. Limitations of IoT System Implementation

2.1 Processing Large Amounts of Data in the IoT Industry

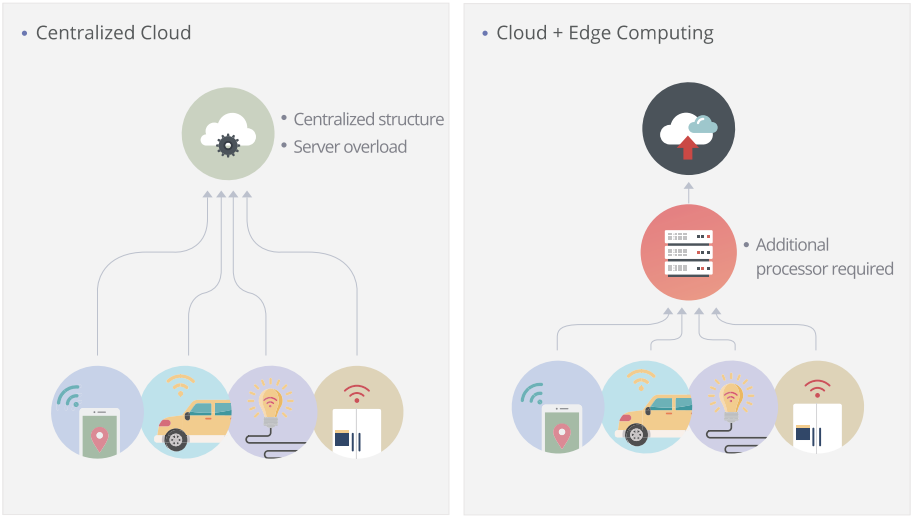
The problem of processing large amounts of data in a centralized architecture

As IoT services become invigorated, the number of devices connected to the network is increasing rapidly, and it leads to a rise in data traffic. In particular, as the wearable and connected car services begin, data traffic is expected to increase in the area of infotainment (Information+Entertainment).

Most IoT companies manage IoT devices after renting computing resources from cloud service providers. However, since the existing cloud system is inefficient to handle exploding data because the centralized server processes all the data, it causes the degrading of the overall speed and quality of IoT services.

Recently, "edge computing" technology has been introduced to process real-time data based on distributed small servers to reduce the data traffic burden and lower the probability of service delay. However, since edge computing requires additional processors to handle increasing computing tasks, cost problems in facility maintenance and difficulties in system management may occur.

< Figure 2. Changes in Storing Methods of Data in the IoT Industry >



2.2

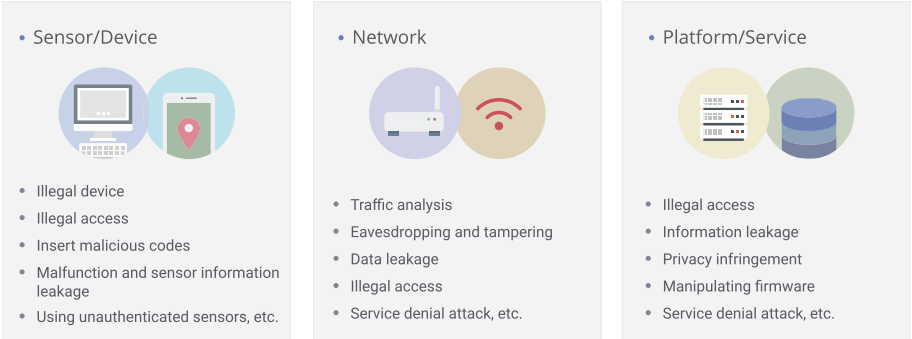
Security in the IoT Industry

Security issues regarding hacking of the IoT devices and accessing by unauthorized devices

Devices connected to the IoT must be connected to the network with individual IDs that can identify themselves. In the IoT industry, various devices are information providers, but there is no reliable ID authentication system for individual devices and a verification system for data transmitted between devices.

In the IoT environment, as shown in <Figure 3.>, since various devices are interconnected, it is difficult to use the encryption algorithm used in the existing system, making it vulnerable to external attacks such as Malware and DDoS. Various attacks against the IoT devices occur frequently and the hacked devices are highly likely to be used as a means to spread malicious codes and spam by leaking essential data such as user account information and passwords. Since the forged data of hacked devices cannot be verified and secured, malfunction of the entire system due to incorrect data transmission and other various side effects can occur. If authentication of IoT devices or data security systems does not exist, there can be threats across the entire IT services.

< Figure 3. Security Threats in the IoT Environment >



2.3

Convergence of Blockchain and IoT System

Difficulties in developing blockchain-based software

Many companies are trying to expand their business areas using IoT technology. But their infrastructures are implemented with various technologies and processes, making the system structure very complicated. Therefore, companies do not have the flexibility and competence related to system development in integrating the existing system with new technology such as blockchain, which utilizes new programming frameworks and development languages.

For this reason, most companies tend to rely on third parties for the implementation of blockchain-based business processes and the system establishment for the business processes through outsourcing contract, which requires a lot of cost and time. Therefore, companies need specialized development tools and environment which support various development languages such as java, c#, c++, and PHP accustomed to their programmers and enable the development of DApps with ease.

Integration problem of blockchain and IoT system

Existing blockchains seek various methods to complement the shortcomings and secure high processing speed and scalability for convergence with the IoT industry. However, it has not yet solved the issues related to the security of devices and decentralization with satisfaction.

For a public blockchain, it is hard to implement a practical IoT system because of the low processing speed caused by the limited computational power of a node when data transactions occur. Private blockchain-based IoT systems partially guarantee higher processing speed and scalability than public blockchains by restricting the authority to participate in the blockchain network. However, data transparency cannot be guaranteed because decentralization is not achieved. To solve the dilemma of private blockchain and public blockchain, the blockchain industry-related workers and developers need a new technology that integrates the existing blockchain technology with various devices in the IoT industry.

3. ReapChain's Solution – ReapChainBaaS

- ReapChain offers ReapChainBaaS as a solution for the perfect convergence of IoT technology and blockchain.

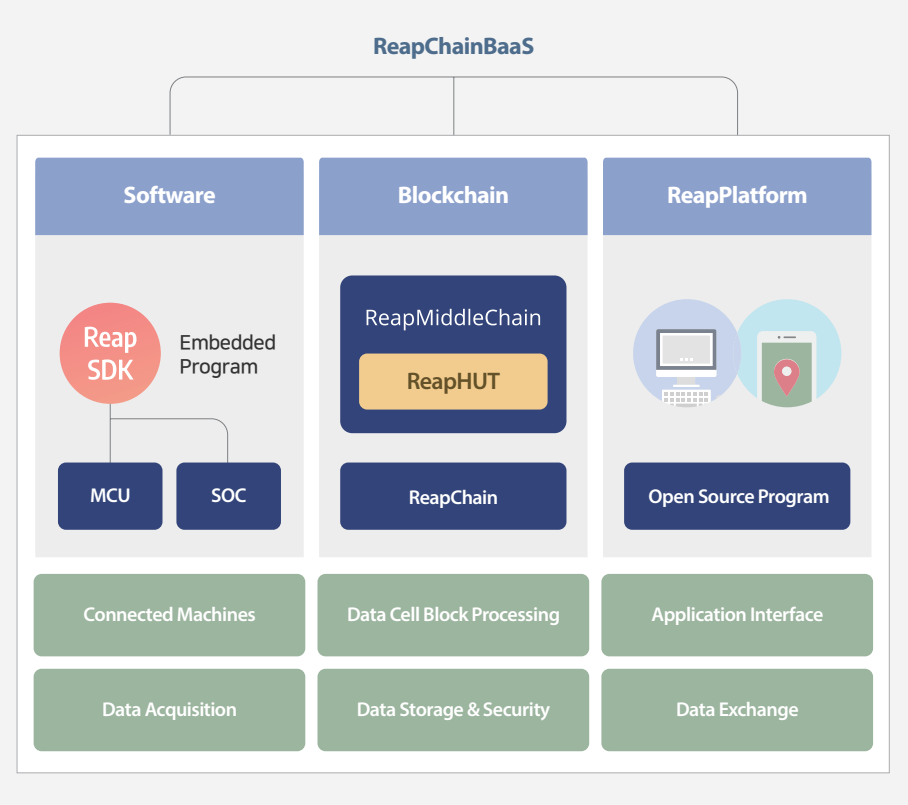
3.1 Overview of ReapChainBaaS

BaaS (Blockchain as a Service) is a cloud computing platform that provides a development environment for blockchain-based software.

ReapChain offers services in the form of BaaS and provides a business customized API to build a blockchain infrastructure without blockchain expertise. Therefore, by utilizing ReapChainBaaS, anyone can quickly and conveniently integrate the blockchain with the IoT related services and shorten the service development time.

The primary services of ReapChainBaaS include ReapSDK, which can implement PID (Private ID) of IoT devices, Reap HUT, a storage service, and ReapPlatform, which acts as an operating platform and a data storage.

< Figure 4. ReapChainBaaS Configuration >



3.2

The Primary Services of ReapChainBaaS

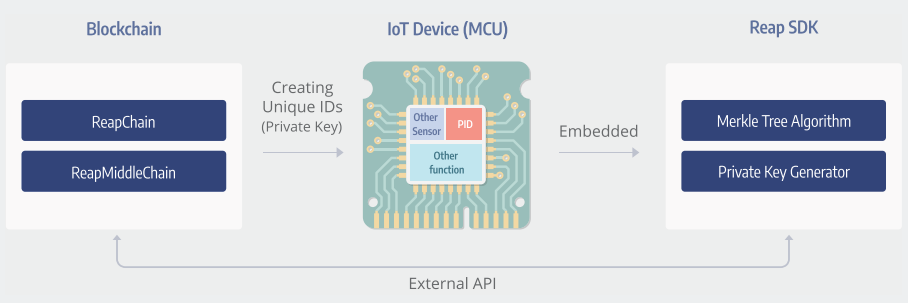
ReapSDK: Implementing PID (Private ID) of IoT device

DID is a technology that has been used only for personal identity authentication. DID technology is extended its application to devices through the encryption technology of ReapSDK to implement a unique device authentication system, PID, to ensure data security.

① Implementation of PID through ReapSDK

ReapSDK generates a 32-byte of PID on each IoT device and stores it in internal non-volatile memory. When a data transaction occurs, by receiving and storing the final hash information generated from ReapMiddleChain, each IoT device can verify device reliability by becoming a node of ReapChain.

< Figure 5. Implementation of PID >



- Device Private Key: Private keys are issued for each MCU to create and assign independent and unique IDs to devices.
  - A user's private key is encrypted with a password and stored.
  - The encryption algorithm is an improved version of AES-128 used in the Ethereum. The algorithm is encrypted about 10,000 to 200,000 times and stored in the form of a Keystore file to prepare Brute Force attacks.
  - Keystore files encrypted with an 8-digit password that combines alphabets and numbers are almost impossible to decrypt.
- Merkle-Tree Data: IoT devices are allowed to store 5 to 50 hash values depending on the specification and performance of MCU and can perform partial functions of a blockchain node. The last value of Merkle-Tree (Hash-Tree) is stored to prevent forgery.
- ReapChain External API: ReapChain External API supports protocol functions for ReapMiddleChain and IoT devices to communicate with each other.

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

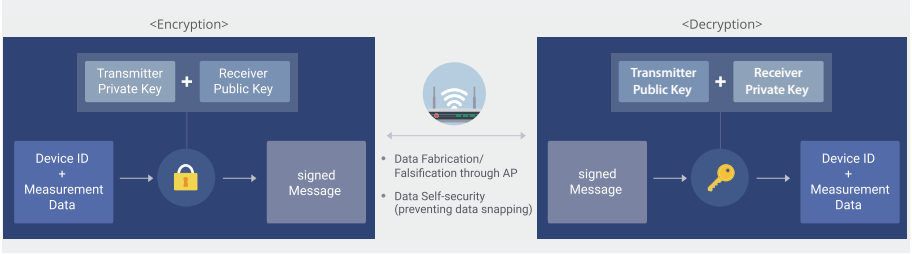
3.2

The Primary Services of ReapChainBaaS

② Data forgery prevention through private key encryption technology

The data generated from MCU is processed to create a signed message through unique encryption technology utilizing the unique private key of each device and the public key of the reception device, and it is transmitted to ReapChain via ReapMiddleChain. Since the delivered signed message requires a private key of the receiving device and the public key of the transmitting device for decryption, data forgery can be detected even if hackings have occurred on communication devices such as routers and AP. Also, even if data snapping (interception of data) occurs through a communication device, without a private key, the decryption of data is impossible.

< Figure 6. Signed Message through Encrypted Private Key >



- Device ID information and measurement data are generated in the devices.
- Generated data is encrypted to create a signed message through a unique private key of a device and a public key of a data receiving device.
- Since encrypted-signed messages transmitted through AP requires a unique private key of the receiving device to decrypt, unauthorized devices cannot restore the original data.
- The receiving device of an encrypted signed message can decrypt the data using its private key and a public key of transmitting device of the data.
- If forged data by hacking is transferred, the forgery can be detected because it cannot be decrypted by the private key of the receiving device and public key of the transmitting device.

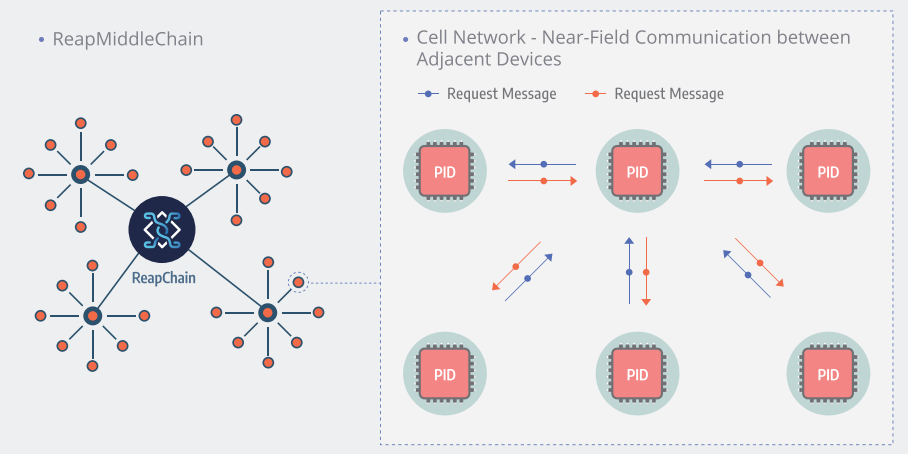
3.2

The Primary Services of ReapChainBaaS

③ Mutual verification between adjacent devices using Merkle Tree algorithm

The Network is divided into multiple layers, and in many cases, downsized IoT devices are not equipped with an interface that supports direct communication with the main net. In the IoT systems, to secure the accuracy of the data provided by the final sensor node, a reliability verification is inevitable not only for relay nodes but also for independent short-range wireless networks connecting each node. As shown in <Figure 7. >, in the cell network to which Reap SDK is applied, secondary security is possible by checking for the forgery of transmitted data, comparing the adjacent edge node with the Merkle tree value of the end node.

< Figure 7. Structure of Near-Field Communication between adjacent devices >



- Encrypt end-to-end communication data based on the encrypted public key.
- Verify the integrity of the block by connecting IoT devices to the cell network.
- Proceed verification by the connected nodes on synchronized blocks by storing the most recent N block hash values in each IoT device.

3.2

The Primary Services of ReapChainBaaS

ReapHut: Storage for additional strong security and efficient data management

ReapHut is a private temporary storage space for data transfer and irreversible storage with WORM (Write-Once Read-Many) storage technology is applied that cannot be changed once data is written. Data stored in ReapHut can be deleted after a certain period of time, and it has a function to classify and determine essential data to be finally transmitted to ReapChain.

The Data management technology of ReapHut has SHA-256-based digital security, real-time data encryption, and time modulation prevention. It is fundamentally impossible to forge or delete data because access to data is not allowed without access rights.

ReapPlatform: A platform for convenient and efficient service management

As a data store, ReapPlatform is a space where data transactions take place and a platform for trading necessary data between data processing companies and service providers & users.

Also, ReapPlatform is a platform that interconnects IoT devices & servers and applications. It is implemented based on oneM2M, an international standard of IoT, and an operating platform that manages device information and provides services such as access control, authentication, and user management.

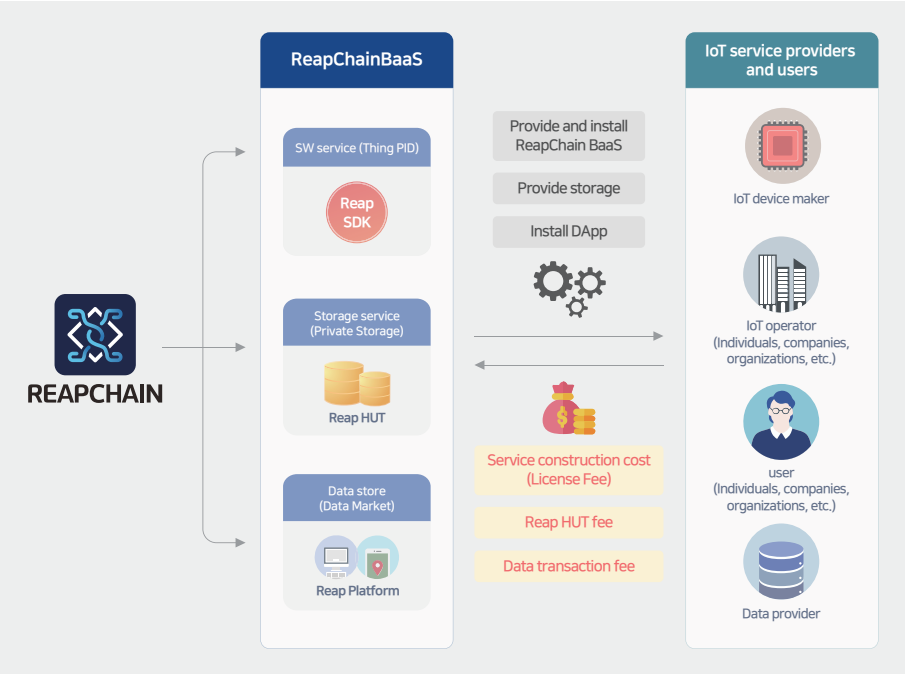
4. Business Model

4.1 Business Model

ReapChainBaaS based Business Model

ReapChain aims to combine various business areas by invigorating the IoT industry specialized platform, to establish a reasonable fee and incentive system, and to build a competitive business model through a prosperous token economy by providing ReapChainBaaS.

< Figure 8. ReapchainBaaS Based Business Model >



By utilizing ReapPlatfom as a data hub, the IoT service providers and users can register and trade data quickly and easily. It makes participants in the IoT industry generate synergy by linking with other industries and realize a blockchain-based data economy ecosystem.

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

4.1 Business Model

ReapChainBaaS revenue structure

① ReapChainBaaS service fee (license fee)

Service users pay a fee according to a plan as a license fee in introducing ReapChainBaaS.

- ReapChainBaaS service fee includes the total cost of installing the ReapChain Protocol and managing security solutions and complex backend solutions.

② ReapHut usage fee

Reap HUT is private temporary storage. Service users can choose monthly usage amounts and pay a fee according to the amount of usage.

- When using the ReapHut service, users can specify and select monthly usage amounts, and the cost is set differently according to the chosen usage.

③ Data trading fee

Users who need customer data for analysis & utilization and PR & marketing purchase the data from the data producer within ReapPlatform and pay a certain amount of fee for data trading to ReapChain.

< Table 2. Examples of ReapChainBaaS rates >

Plan : Rating system applied (General/Intermediate/Advanced)

Price : Flat rate method (Monthly billing)

ReapSDK	ReapHut (Capacity)	ReapChain (Number of TX)
Charge Once at the time of initial installation	Offer different capacity according to the rating system	Offer different number of TX according to the rating system

· Monthly billing system: When using the service, the fee varies according to the set capacity.

· Detailed standards are subject to change depending on the situation when the service opens.

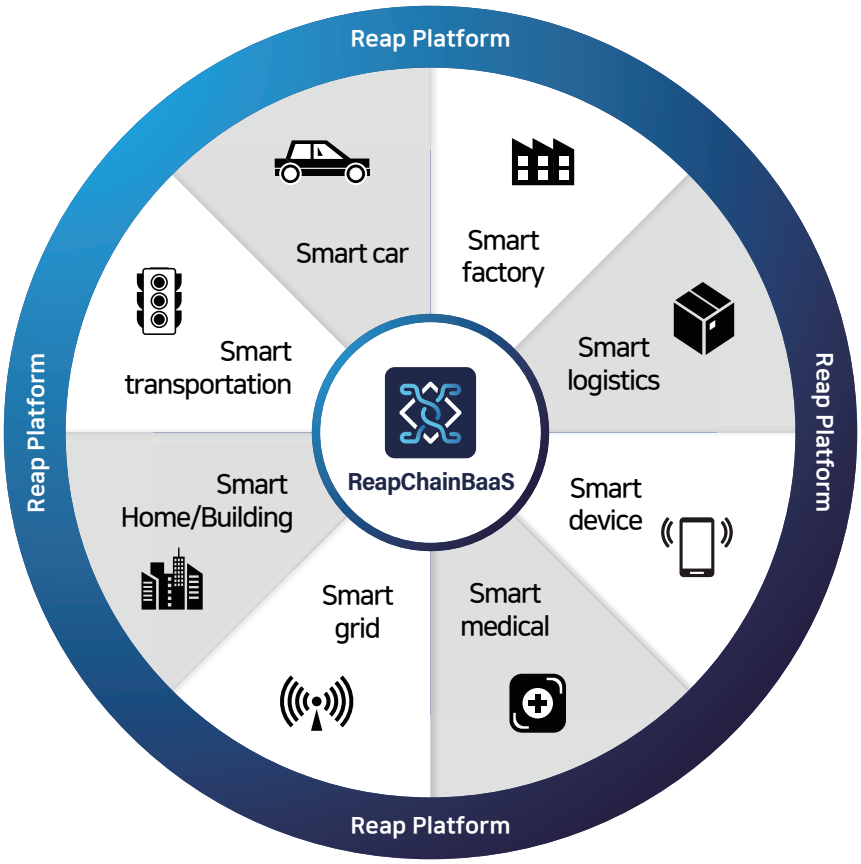
REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

4.2

Applicable Fields

ReapChain aims to provide a platform suitable for various IoT industry fields through ReapChainBaaS and build an integrated platform that can share and utilize data through interconnection and expansion among IoT industry ecosystem participants.

< Figure 9. ReapChainBaaS applicable fields >



REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

4.2

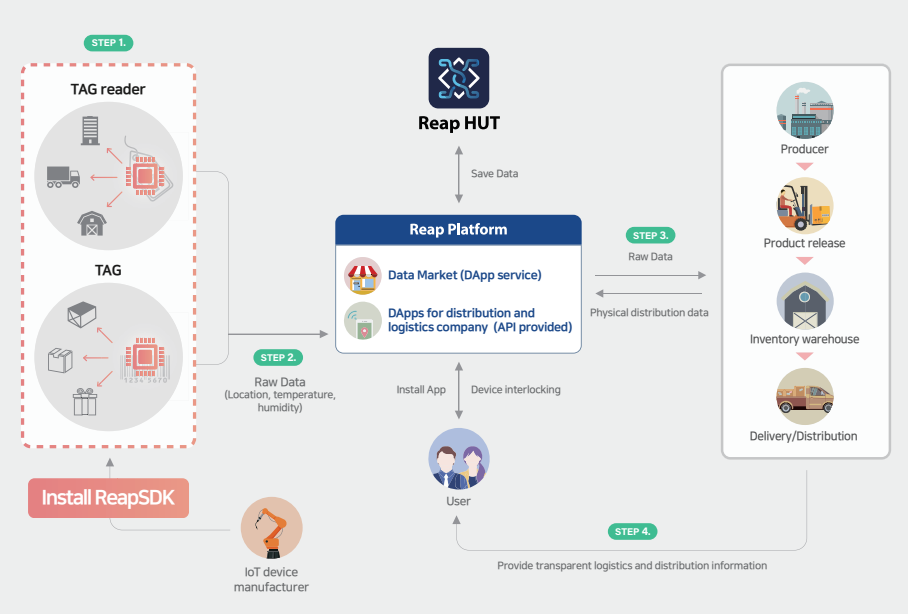
Applicable Fields

Smart logistics service through product history and tracking

Distribution/logistics companies utilizing ReapChainBaaS can optimize the stability, efficiency, and processing speed of the logistics system by collecting, analyzing, and sharing data from a series of processes such as shipping, gathering, transporting of goods, and accurate delivering to customers. Users are provided with transparent logistics and distribution information.

Manufacturers and distributors can grasp the information in the distribution/logistics process in real-time to provide final delivery information to the consumers and reduce unnecessary production through transaction information.

< Figure 10. ReapChainBaaS-based distribution system flow chart >



Step1. Product production and data input based on the TAG system with ReapSDK applied.

Step2. Continuous transmission and verification of product status data through the TAG system.

Step3. Transmission and verification of additional data such as location information in the entire distribution process and warehousing & forwarding records by ReapPlatform.

Step4. Reception and verification of reliable data on products purchased by users.

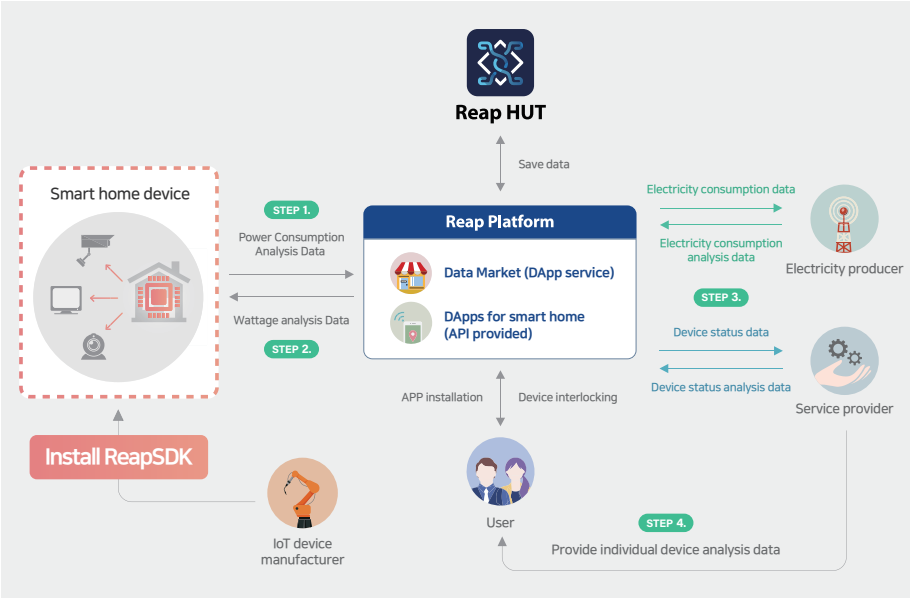
4.2

Applicable Fields

Smart home energy management service

Power companies utilizing ReapChainBaaS can operate efficiently through the production of an appropriate amount of power by analyzing the power consumption amounts of individual industries and each household. By providing the required amount of power to each household at the right time, the service providers can prevent unnecessary energy consumption. Users can receive transparent and reliable services through individual device status-related data and power consumption analysis data. Manufacturers can get Real-time data regarding power consumption amount and device status.

< Figure 11. ReapChainBaaS-based power system flow chart >



Step1. Transmission and verification of the various data and power consumption amounts generated from ReapSDK applied smart home devices.

Step2. Continuous transmission and verification of device status and power consumption data through smart home devices.

Step3. Checking the amount of power each household needs by a power company, and analysis of the device status data to improve service quality by service providers through ReapPlatform.

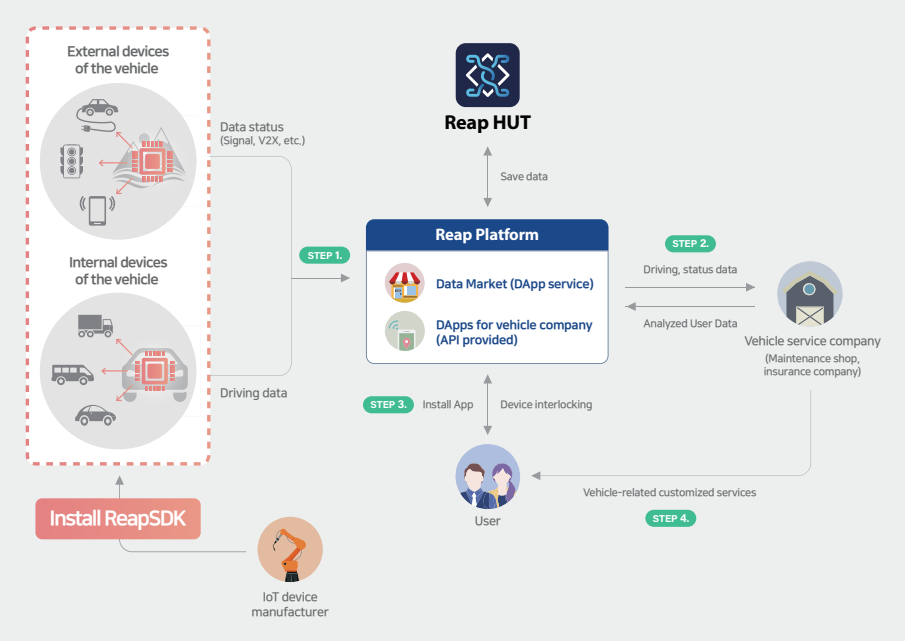
Step4. Reception of reliable data and verification of information for smart home individual devices at each household.

4.2 Applicable Fields

Smart vehicle service using driving data

Service providers utilizing ReapChainBaaS provide information on surroundings of drivers by checking in detail based on V2X (Vehicle to Everything) data to car manufacturers, car users, and service providers. Car users receive convenient vehicle-related services, and car manufacturers can increase sales by producing equipment that service companies need. As service providers, insurance companies can provide customized services, such as differentiated products based on the driving habits of car users.

< Figure 12. ReapChainBaaS-based vehicle service flow chart >



· V2X (Vehicle to Everything): With the vehicle centered, this technology exchanges or provides information with other devices delivering wired and wireless networks.

Step1. Continuous transmission and verification of data from a vehicle's internal / external devices that ReapSDK is applied.

Step2. Reception of vehicle driving and status data and transmission of analysis data by vehicle service companies through ReapPlatform.

Step3. Reception and verification of reliable vehicle data through interlinking the devices by car users.

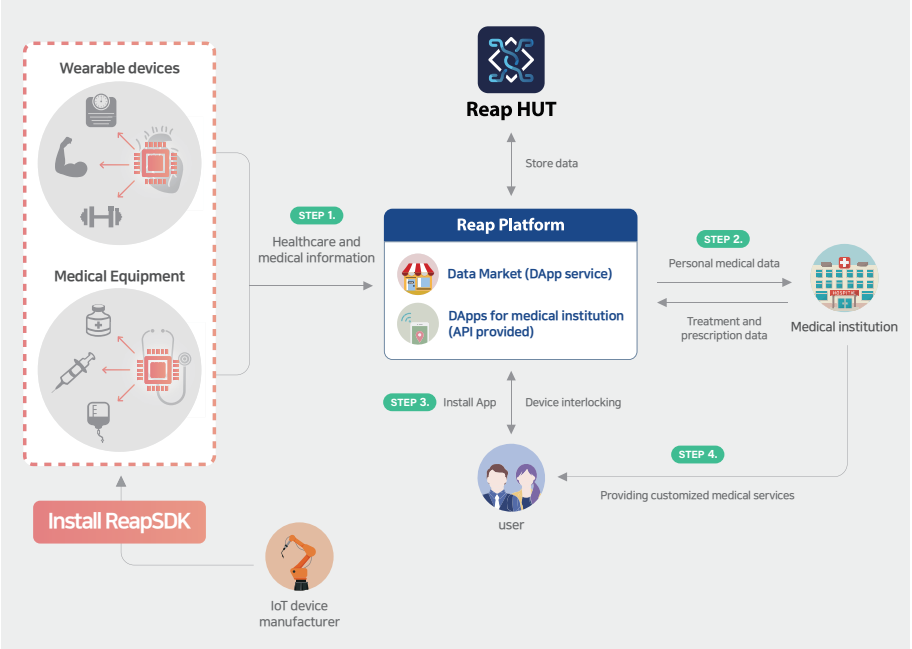
Step4. Providing customized vehicle-related services based on analyzed data through ReapPlatform.

4.2 Applicable Fields

Smart medical service based on the personal medical information

Medical institutions can provide customized medical services based on personal medical data such as medical information and treatment records collected through ReapPlatform provided by ReapChainBaaS and can reduce medical malpractice that may occur because of the patient information not shared. Users can avoid incorrect prescriptions and unconscientious medical institutions, and manufacturers provide optimized devices through medical institution data.

< Figure 13. ReapChainBaaS-based medical service flow chart >



Step1. Continuous transmission and verification of personal medical data generated from medical devices that ReapSDK is applied.

Step2. Reception of personal medical data and verification of usage records by medical institutions through ReapPlatform.

Step3. Reception and verification of reliable data information regarding medical services provided by users.

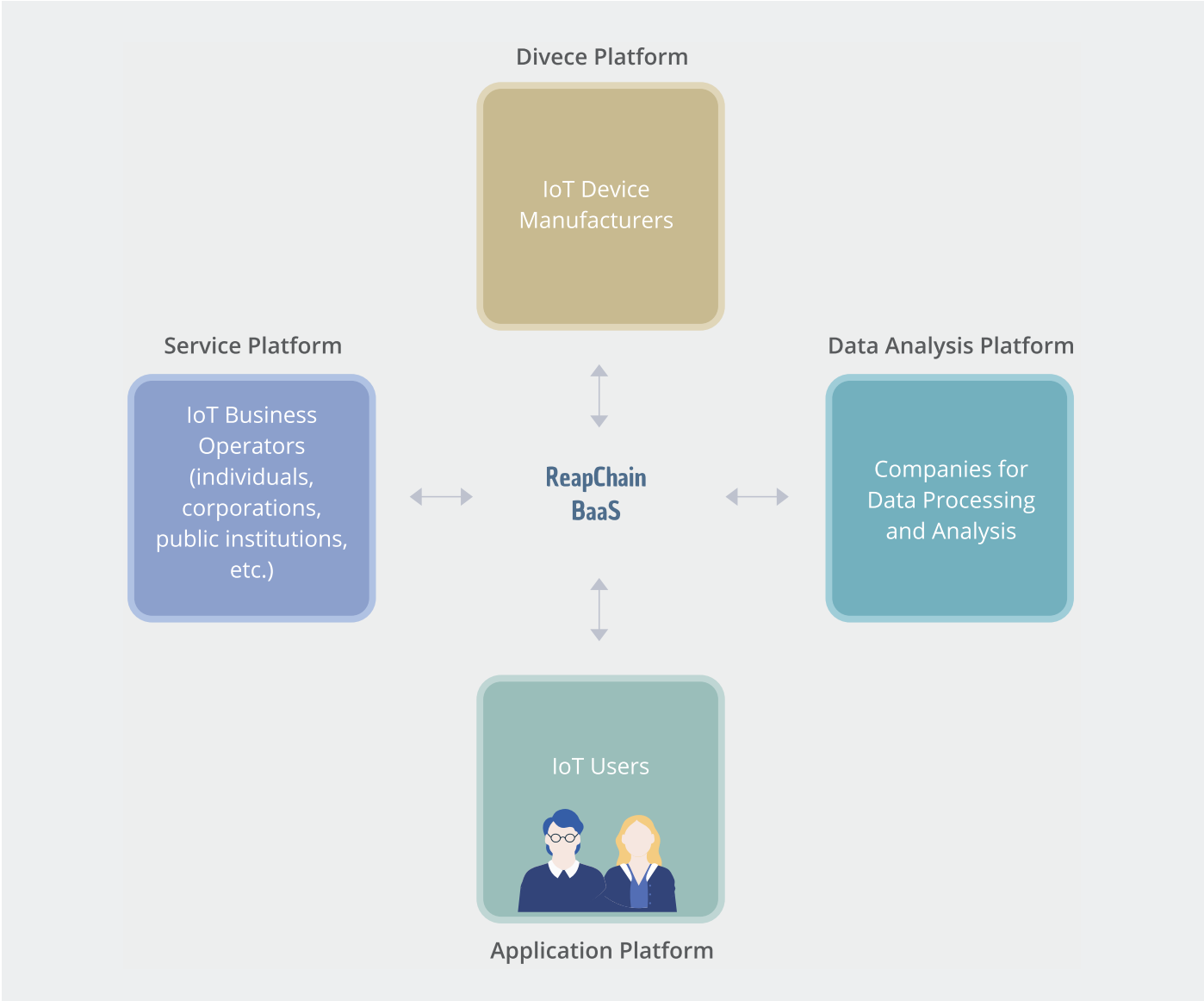
Step4. Providing customized medical services based on reliable medical treatment data.

5. Ecosystem

Business Ecosystem based on ReapChainBaaS

Participants in the ReapChain ecosystem consists of IoT service users, IoT device manufacturers, entrepreneurs such as individuals, companies, government, and public institutions who want to develop the IoT-based system and companies who utilize the IoT-based data to process and analyze.

< Figure 14. Business Ecosystem Configuration >



6. Roadmap

2022

4Q
REAPCHAIN Mainnet Performance Indicator Announced
Completion of advancement of middle chain for payment
Start NFT Marketplace Service

3Q
Mainnet officially opened
Started Reapchain-based NFT platform service

2Q
NFT Marketplace Construction
Advancement of middle chain for payment

1Q
REAPCHAIN-based NFT platform establishment
Started payment country service for small business payment system

2021

4Q
REAPCHAIN TestNet operation
REAPCHAIN-based simple payment "REAPPAY" official service
REAPCHAIN-based sales omission prevention system "Dream Tomorrow" official service

3Q
PID-based IOT logistics system open beta
REAPCHAIN-based simple payment "REAPPAY" open beta
REAPCHAIN-based sales omission prevention system "Dream Tomorrow" open beta
REAPCHAIN-based DID international standardization registration

2Q
Build service infrastructure scalability
REAPCHAIN-based simple payment "REAPPAY" closed beta test
REAPCHAIN-based sales omission prevention system "Dream Tomorrow" Closed Beta Test
Digital traditional market and delivery solution "JANGBODA" official service

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

2021

1Q

Establishment of commercial service environment and stabilization of operation

PID-based IOT logistics system closed beta test

REAPCHAIN Closed Beta Test

Closed beta test of digital traditional market and delivery solution

Establishment of commercial service environment and stabilization of operation

2020

4Q

Whitepaper Ver 1.0 released

Closed Beta Integration Testing

Build REAPCHAIN BaaS-based service infrastructure

Establishment of Microservice-based REAP Platform service infrastructure

Securing BM for spreading REAP Platform - Signed MOU with IoT device company

Securing BM for spreading REAP Platform - MOU with IoT platform service company

3Q

Whitepaper Ver 0.9 released

Alpha Integration Test

REAPCHAIN Beta (Ver 2.0) development and verification test

ReapMiddleChain Beta (Ver 2.0) development and verification test

Reap Platform & SDK Beta (Ver 2.0) launch and verification test

Reap Wallet (Ver 1.0) Open

Pre-Sale and exchange listing

Token Generation (TGE) and Distribution

MCU based object PID development

2Q

REAPCHAIN Alpha (Ver 1.0) development and verification test

ReapMiddleChain Alpha (Ver 1.0) development and verification test

Reap Platform & Reap SDK Alpha (Ver 1.0) launch and verification test

REAPCHAIN Token Sale - Private Sale 1st

REAPCHAIN Token Sale - Private Sale 2nd

1Q

REAPCHAIN MVP (Ver 0.8) Verification Test

ReapMiddleChain MVP (Ver 0.8) Verification Test

Whitepaper Ver 0.8 released

Seed Sale

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

2019

4Q

Reap Platform & Reap SDK (Ver 0.1) design and development

Smart Contract establishment and Reap Wallet (Ver 0.1) development

3Q

ReapMiddleChain (Ver 0.1) Design and Development

2Q

REAPCHAIN Mainnet (Ver 0.1) development

1Q

REAPCHAIN Mainnet planning and design

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

7. Team & Partners

Core Members

JAKE LEE

CEO

Graduated from Youngnam University in Mechanical Engineering

a member of the North Gyeongsang Youth Policy Committee.

a member of the Special Committee on Blockchain in North Gyeongsang Province.

Start-up, 13 years of Management in Fintech

SEUNGJONG LEE

COO

Department of Computational Statistics, College of Natural Sciences, Seoul National University

Adjunct Professor, Department of Computer Engineering, Korea Polytechnic University

Adjunct Professor, Department of Computer Engineering, Korea Polytechnic University Security IT-related and executive work at Samsung Electronics, Cellbig Co., Ltd., Mococo Co., Ltd., and Nemustech Co., Ltd. Line Plus Dev Rleation Lead

Outside Director, Korea Data Industry Promotion Agency

Member of Gyeonggi-do 4th Industrial Revolution Committee

Member of Gyeonggi-do Informatization Committee

Advisory member of Fair Trade Commission data portal establishment

KHAN KIM

CSO

New York University stern school of business

Columbia University MBA

Optima Consulting, LG Investment & Securities, LendLease, KPMG

SUHO KWON

CTO

Sogang University Computer Science, Operating System Lab.

Samsung Electronics, New Media Life, Samsung Techwin(Hanwha Techwin), SK Hynix, Pax Datatech

Present) Head of Education Center, KBIPA (Korea Blockchain Promotion Association)

Present) Head of ReapChain Research Center

More than 20 Years Experience in Embedded System Development and Software Quality Engineering

JAY YOO

CMO

University of Seoul, Ph.D. Candidate in Marketing Strategy

University of Minnesota (Twin Cities) MBA

Korea University B.A.

Present) ReapChain, General Manager

Present) SoongEui Women's College, Adjunct Professor

Former) 25 years of experience in marketing and strategy at Cheil Communications, Hyundai Corporation and Hyundai Motor Company

Advisors

HYEONSANG EOM

Ph.D. Computer Science, the University of Maryland at College Park (UMCP), Maryland (MD), USA, 2003

Distributed Processing and Computer/ Embedded System

Computer System/Network/Application/ Software Performance Engineering

Mobile Application/Middleware (Including Security)

15 years of experience at Seoul National University Professor Distributed Computing Systems LAB

TAEHONG KANG

Graduated from Soongsil University majoring in Electronic Calculation

Doctor of Computer Science at Soongsil Graduate School

Present) Professor of Soongsil University Graduate School of Information Science

Present) Vice President of ROBOPIA INVESTMENT INC., CTO

Former) Advisory Councilor, KOSCOM INC. Former) Vice President, DELIGHT CHAIN INC., CTO

Former) Director, Korea Information Processing Department

Former) Director of the Korea Information Science Society

Former) Director of the Global FinTech Industrial Development Center

CHULHO LEE

Present) Assistant Professor, Department of Business and Technology Management, KAIST

Ph.D. in Management Science, The University of Texas at Dallas, USA

M.A. in Business Administration, Pusan National University, KOREA

B.S. in Business Administration, Pusan National University, KOREA

Associate Professor, Department of Management Science and Engineering, Harbin Institute of Technology, China

Visiting Assistant Professor, Department of Management and MIS, Xavier University, USA

Economics of Information Security

Behavioral Economics of Privacy and Security

Empirical Study of Information Systems

SEUNGHUN HAN

University of Central Florida Finance Ph.D

University of South Carolina Statistics M.S

Present) Korea Advanced Institute of Science and Technology(KAIST) Faculty of Technology Management AACSB AOL (Assurance of Learning) Associate Professor

Present) Korea Information Sociology Society Director and Vice Chairman

Big Data, Economics, Science, and Technology Society, Council Member 2018 Excellent Lecture Award

Chairman of AACSB AOL Committee, Faculty of Technology Management

Steering Committee, Graduate School of Technology Management

AACSB Committee Member, College of Business Administration

Other Undergraduate Admissions Committee members, Additional TA Improvement Committee members, ICC Internationalization Committee member, Participated in the financial engineering minor program operation committee and Korea-Japan CAMPUS Asia project group

Research papers selected from 54 [Academic achievements of KAIST 2012]

HYUKJUN KWON

Soonchunhyang University, Department of Economics and Finance, Assistant Professor

Ph.D. in Information System, Yonsei University

Yonsei University Master of Business Administration

Present) KOMSCO Blockchain Advisory Professor

Present) Promoter and Steering Committee of the Korean Blockchain Society

Present) Vice President of the Korea Payment and Payment Association

Present) Director of the Korea Information Processing Society

Present) Director of the Korea Electronic Commerce Association

Present) Advisory Professor, Blockchain, Korea Insurance Development Institute

Present) Commissioner of the Korea Institute of Behavioral Sciences

Former) BK21 Senior Researcher (Yonsei University Graduate School of Information)

Former) Promoter of Korea Information Technology Convergence Society and Director of Industry-University Cooperation

Blockchain, Distributed Leger Technology Fintech,Token Economy VR and AI

CHEOLHWAN KIM

Graduated from Seoul National University in Electronic Engineering

Present) Professor at Hanyang University

Present) Advisor, International Genuine Management Association

Present) Advisor, AVI U Systems Co., Ltd.

Present) Consulting for Gdynet Korea

Present) Productivity Center Blockchain Lecture

Present) ICT Polytech Blockchain Lecture

Former) DACOM Distributed Transaction Processing Application Development

Former) Gigalink Founder (Network Equipment Development)

Former) Director, Intops (Russia, Israel New Technology Project)

Former) Israel MusicGenome / ExpoBee Korea Consultant

Former) K-ICT Mentoring Center, Korea Youth Entrepreneurship Foundation

Former) Korea Technology Venture Foundation Mentor

Advisors

HYUNWOO YI

Graduated from the Department of Law, Korea University

Seoul National University Graduate School of Law (Basic Law major)

Passed the 40th Judicial Exam

Completed the 30th Judicial Research & Training Institute

Aram Law Firm - ARAM

Law Firm - SOJONG

Law Firm - HUMAN

Law Firm - DONGIN

Law Firm (Limited) – DR & AJU

Present) Law Firm (Limited) - BARUN lawyer member

Present) Advisory Committee, Legal Advisory Group, International Investment Dispute, Ministry of Justice

Present) Member of the Legislative Analysis Review Committee

Present) Member of the Regulatory Review Committee of the Ministry of Employment and Labor

JONGWON KIM

Graduate from Department of Metal Engineering, Seoul National University

Present) Executive director of Korea Blockchain Industry Promotion Association

Former) CEO of Goverentech

Former) Outside Director, Seoul Metro

HOSUP KAN

Certificate at Fashion Institute of Technology. NewYork

Drexel University. Philadelphia. Dept. of Fashion Design M.S

Sungkyunkwan University. Seoul. Dept. of Fashion Design B.S/Ph.D

Designer & Illustrator for Kokin Inc, Nicole Paris, DKNY(Donna Karan New York)

Creative Director for Amore Pacific Co.,Ltd. Men's Cosmetic 'ODYSSEY SPORT'

Fashion Director for SK stoa Co.,Ltd.

Mentor for Project Runway Korea Season 1~4

25 years of Experience in Professor, College of Design, Dongduk Women's University & Professor, College of Fine Art, Hongik University

Visiting Researcher of Harvard University,Boston

President in Korea Fashion & Culture Association

President in The Korean Society of Fashion Business

SUNGJIN KIM

Graduated from Busan University with a master's degree in computer science

A mentor specializing in Samsung Multicampus Blockchain and big data

Korea Communications Commission & TTA DMB/IPTV Technical/Service Standards Committee

ISO/IEC MPEG-2/4 International Standard Committee

28 years of experience in Media service platform at Samsung Advanced Institute of Technology, Pan Media and IT development, including digital twin and Blockchain.

8. References

· SMTECH (Ministry of SMEs, 2019), "2020-2022 Strategic Technology Roadmap, IoT & Blockchain & Big Data."

· Berg Insight (2019), "The Global Wireless M2M/IoT Market Report Bundle 2019."

· Frost and Sullivan (2018), "Global Embedded Computing Ecosystem Market, Forecast to 2023."

· SPRI (Software Policy Research Institute, 2018), "Research on Software Usage Rate on Embedded/Intelligent System."

· Gartner (2019), "Scenarios for the IoT Marketplace 2019."

· IEC (International Electrotechnical Commission, 2017), "Wireless Sensor Network in IoT."

· Lee, Chan Hyeok, and Ki-Hyung Kim (IEEE, 2018) "Implementation of IoT system using blockchain with authentication and data protection."

· Van Alstyne, Marshall W., Geoffrey G. Parker, and Sangeet Paul Choudary (Harvard business review, 2016), "Pipelines, platforms, and the new rules of strategy."

· Dae-Hwa Lee, Jung Ji-Jung, and Hyung-Sik Kim (OSIA Standards & Technology Review, 2019) "A Study on Blockchain and Smart Contract Technology Suitable for IoT Environment."

· ETRI (Electronics and Telecommunications Research Institute, 2018) "Sensor Industry and Major Promising Sensor Market and Technology Trend Report," "Blockchain and Consensus Algorithm."

· NIPA (Information and Communication Industry Promotion Agency, 2018), "Key Technology Trends and Implications for the Data Technology Era."

· STEPI (Korea Institute for Science and Technology Policy, 2018) "Blockchain Technology Trend and Implications."

· Hana Financial Management Research Institute (2018), "Expansion and Implications of Platform Economy Leading the Fourth Industrial Revolution."

· LG Economic Research Institute (2018), "Manufacturing in the post-scale era, leap forward to platform business."

· KISDI (Information and Communication Policy Research Institute, 2018) "Blockchain Diversification: Blockchain Spread without Mining."

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

Disclaimer

Please read the information below carefully. The information below applies to anyone reading this white paper. The ReapChain white paper (hereinafter referred to as "white paper") is written and provided based on the time of writing (as is), so any content contained in the white paper may be changed or updated at any time at the discretion of ReapChain Inc. Any content in this white paper There is no guarantee that even if it does not change until a future point in time.

If you have any doubts about this white paper's contents, you should consult with an accountant, attorney, or other experts before purchasing.

1. This white paper aims to cover summary information and introduction to ReapChain, which is being prepared by ReapChain Inc. This white paper is not legally binding on ReapChain or ReapChain Inc., and any phrases in the white paper are not subject to the nature of subscriptions, purchases, investment proposals, or investment enforcement.

2. Please note that any information or analysis in this white paper cannot be the basis for investment decisions and is not an investment proposal or advice. Any content or data of a future-planning nature in this white paper may change for any reason, may not be accurate, and there is no guarantee or promise regarding the content.

3. ReapChain Inc., including directors, agents, employees, contractors, and sales partners, is not liable for any damages of any kind, either directly or indirectly, arising from the information contained in this document as follows: (1) Applicable The accuracy and completeness of the contract content according to the white paper; (2) Errors or omissions in the white paper; (3) Unable to read white papers due to unconfirmed causes; (4) Any other damages arising from the use or non-use of the white paper.
Also, ReapChain Inc. is not solely liable for any of the following issues that may arise from a decision-making action made using the information contained in this document, even if such damage is foreseeable: (1) Profits, profits, liabilities, and any other form of monetary damage; (2) Income, sales, capital reduction, debt and other losses incurred during business transactions, business activities, and operating profit-related activities; (3) data loss or corruption; (4) incidental or special damages; (5) wasted or lost administrative time; (6) Indirect or consequential damage.

4. The white paper's content may change depending on the ongoing ReapChain content, market changes, technological development, and changes in ICO or token regulations. However, ReapChain Inc. is not obligated to notify or report to readers about any event, platform, plans, changes in estimates, or changes within the margin of error specified in this white paper in the future.

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

5. Please be advised that information on the law, tax, regulation, finance, and accounting in this white paper is not advice. The purchase of REAP may result in material losses to buyers, including the material assets paid for REAP purchase. Before purchasing REAP, buyers are encouraged to consult with experts in tax, regulatory, finance, legal, etc. about the potential risks, revenues, and consequences of a REAP transaction.

6. It is entirely up to REAP buyers to determine whether it is legally possible to dispose of income tax or other issues that may arise in relation to the acquisition and disposition of REAP within their legal jurisdiction and whether it is legal for foreign currency exchange.

7. Publication and distribution of this white paper are prohibited in countries where the white paper's publication and distribution are not permitted. The information in this white paper has not been verified or authorized by any regulatory agency, and any actions contrary to the law do not affect ReapChain Inc. There is no guarantee that this white paper's publication and distribution comply with all regulations of the country in which it was issued.

8. The official data for ReapChain is this white paper and written in Korean. This white paper may be translated into other languages . It may be used for oral or written communication with prospective and existing buyers, and some information may be misinterpreted, misinterpreted, or lost in the process. Therefore, please be aware that we cannot guarantee the accuracy of these alternative communications. In the event of such inaccurate communication, the information in this official white paper written in Korean takes precedence.

9. All white paper contents are protected by copyright. Individual sections of the white paper may be downloaded or printed only for personal use or other proprietary notices. This white paper may not be reproduced in whole or in part, reproduced by electronic means or otherwise, or modified, linked, or used for public or commercial purposes without the prior written permission of ReapChain Inc.

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915

Investment risk

ReapChain Inc. is notifying buyers of several types of risks, including the risk of losing a significant amount of the REAP purchase price. The accuracy of any risk or uncertainty information presented below is not guaranteed.

Buyers are deemed to agree to REAP's purchase and sale, aware of and purchase as is, as is a risk, expressly without warranty of any form by REAP.

1. Blockchain Risk: Due to the blockchain system's congestion, transactions may be processed late, or transactions may be invalidated. In particular, the smart contract responsible for the issuance and distribution of REAP is based on a technology called the Ethereum blockchain. The Ethereum protocol may have weaknesses and vulnerabilities, and various bugs can occur, including those that result in loss of REAP. Also, due to this Ethereum blockchain problem, ReapChain Inc. And material damage to REAP buyers.

2. Personal Information Risk: User's personal information is required to distribute and control REAP in the REAP buyer's electronic wallet. Therefore, if personal data is leaked, REAP in the purchaser's electronic wallet may be revealed. Moreover, due to the buyer's information leakage, a third party may steal the REAP by reading its electronic wallet.

3. Security Risk: Like all cryptocurrencies, Ethereum is vulnerable to mining attacks such as'double payment attacks' or '51% attacks'. Hackers or other groups with malicious intent use the attack method described above to enter ReapChain Inc. Alternatively, it can attack REAP, and if such a blockchain attack is successful, it can seriously damage REAP transactions and REAP.

4. E-wallet compatibility risk: To purchase or store REAP, you must use an e-wallet that is technically compatible with REAP. If you use another wallet, you may not be able to access and view the purchased REAP.

5. Force Majeure Risk: ReapChain is still under development. ReapChain Inc. will endeavor to develop and maintain ReapChain, as written in the white paper. Still, the details may change due to various reasons such as laws, design, technology, administrative regulations, etc... ReapChain Inc. is subject to force majeure, such as changes in the regulatory frame or required permits and licensing. Taxation policies, the emergence of platforms, or open-source adversely affecting ReapChain Inc. or ReapChain, lack of market interest, and other similar events. In the event of a decrease in REAP value or loss or loss of liquidity due to factors, all liability for compensation is waived.

REAP CHAIN Inc. OÜ
Office Address: Estonia, Harju maakond, Tallinn, Mustam e linnaosa, Laki tn 30, 12915