

ReapChain

BusinessPaper

ver 0.9

Contents

	Background	03
01.	IoT 시장 개요 및 현황	04
	1.1 글로벌 IoT 시장 현황	04
	1.2 IoT 산업에서 블록체인의 필요성	05
02.	IoT 시스템 구현의 한계	06
	2.1 IoT 산업의 대용량 데이터 처리	06
	2.2 IoT 산업의 보안	07
	2.3 블록체인과 IoT 시스템의 융합	08
03.	ReapChainBaaS	09
	3.1 ReapChainBaaS의 개요	09
	3.2 ReapChainBaaS 기반 주요 서비스	10
04.	Business Model	14
	4.1 Business Model	14
	4.2 적용 가능 분야	16
05.	Ecosystem	20
06.	Roadmap	22
07.	Team & Partners	23
08.	참고문헌	25
	Disclaimer	26

Background

블록체인은 데이터의 신뢰성과 안정성, 보안성, 효율성을 제공하는 분산 컴퓨팅 기술로서 IoT와 함께 4차 산업혁명 신성장 산업을 견인하는 기반 기술로 주목받고 있습니다. 특히, 최근 하드웨어 및 네트워크 관련 IoT 기술이 급속도로 발전함에 따라 IoT와 블록체인의 융합에 대한 다양한 논의가 이루어지고 있고, 향후 IoT 기술을 통한 제품 생산 과정 추적이나 제조 관리 과정 등 다양한 분야에서 블록체인 기술이 유용하게 사용될 것으로 기대됩니다. 하지만 IoT 산업에서 보안 및 인증 등을 하나의 관리자에게 일임하는 방식으로 운영하여 왔으나, 이러한 중앙 집중형 방식은 보안과 비용, 그리고 신뢰 측면에서 여러 가지 부작용을 내포하고 있습니다.

ReapChain은 디바이스 PID 기술을 기반으로 개별기기 인증 및 데이터의 위변조를 방지하여, 기존 IoT 시스템을 개선하고 신규 합의 알고리즘을 통해 현존하는 블록체인의 문제점을 해결할 수 있는 새로운 하이브리드 블록체인을 제시하여, IoT 산업에서 발생하는 대용량 데이터의 분산 처리를 실현하고자 합니다.

ReapChain은 손쉬운 블록체인 개발 환경 구현을 위해 ReapChainBaaS를 통해 투명성과 보안성이 강화된 블록체인 기반 IoT 특화 플랫폼을 구축하고자 다음과 같은 방법론을 제시합니다.

· 방법론

- IoT 산업에 특화된 ReapChainBaaS를 통하여 End-to-End 구간 전체를 블록체인으로 구현
- ReapSDK의 프라이빗키 암호화 기술을 통해 새로운 디바이스 인증체계인 PID를 구현

1. IoT 시장 개요 및 현황

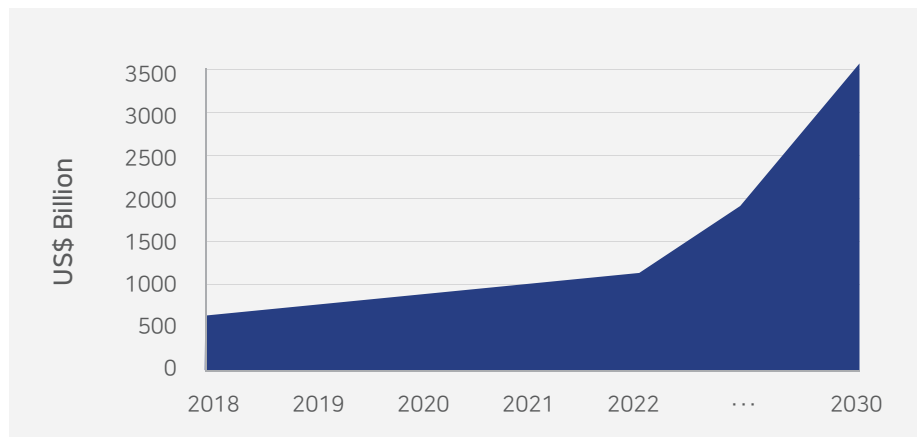
1.1

글로벌 IoT 시장 현황

IoT 전용망, 5G 등 통신 기술의 발달 및 인프라 저변 확대로 인해 IoT 시장의 성장이 더욱 가속화되고 있습니다. 또한 IoT 시스템을 타겟으로 한 사이버 공격이 현실화되고 있고 그 피해가 커져가면서 IoT 보안 시장도 빠른 속도로 성장하고 있습니다.

글로벌 IoT 전체 시장 규모는 2016~2022년까지 연평균 12.8% 성장하면서 2022년에는 1조 1,933억 달러 규모로 성장할 것이며, 2030년에는 3조 1,277억 달러에 이르는 거대한 시장을 형성할 것입니다. 그 중, IoT 임베디드 시스템 시장은 2023년에 838억 6천만 달러에 이를 것이며, IoT 디바이스 및 서비스 플랫폼의 세계 시장 규모는 약 11억 달러에 달하는 것으로 나타났습니다. IoT 총 보안 지출 규모는 2018년 15억 달러를 기록했으며, 연평균 27.9%의 높은 성장률을 보이고 있습니다.

<그림1. 글로벌 IoT 시장 규모 및 전망>



[출처: Forest and Sullivan (2018년)]

IoT는 시스템이라는 형태로 판매되어 컨설팅 및 설치 서비스까지 통합적으로 제공되며, 블록체인과 디바이스IoT 산업과의 연동은 서비스 플랫폼을 통해 이루어집니다. ReapChainBaaS는 플랫폼 및 소프트웨어 서비스 형태로 제공됨에 따라 IoT 디바이스 제조업자 및 IoT 사업자, 그리고 IoT 사용자 모두가 활용이 가능합니다.

1.2

IoT 산업에서
블록체인의 필요성

최근 하드웨어 및 네트워크 관련 IoT 기술이 급속도로 발전함에 따라 IoT 산업에서의 데이터 무결성, 시스템 보안, 디바이스 제어에 대한 중요성이 매우 높아지고 있습니다.

블록체인 기술은 기본적으로 분산 데이터 구조, 암호 이론과 보안성 기술, 데이터 조작 및 변경이 어려운 합의 기술 등의 장점을 가지고 있기 때문에 IoT 분야의 문제점을 해결하기 위해 블록체인이 해결책으로 떠오르고 있습니다.

< 표1. IoT 산업에서의 블록체인 기술 도입에 따른 기대효과 >

구 분	기대효과
데이터 신뢰성 향상	블록체인은 데이터가 암호화된 형태로 저장되고, 중앙 집중형 방식이 아닌 모든 참여자들에게 이를 공유하고 있습니다. 참여자들은 공유 원장을 지속적으로 검증하기 때문에, 기록 데이터의 위변조가 거의 불가능하고 중앙 통제 방식을 탈피하여 신뢰성을 보장합니다.
보안성 향상 (기기 인증)	블록체인의 분산형 구조는 한 부분의 작동이 중지되더라도 전반적인 성능에는 영향을 미치지 않으며, 비 인증된 사용자의 접근을 방지할 수 있기 때문에 DDoS 등의 공격이나 해킹 위협에도 상대적으로 안전합니다.
데이터 거래 활성화	중앙시스템이나 거래의 중개인 없이 P2P 방식으로 거래를 수행할 수 있으며, 블록체인 토큰으로 사물인터넷 기기의 사용 권한이나 데이터를 구매하는 것이 가능합니다.

블록체인은 분산 데이터 저장 방식의 강점을 효과적으로 활용할 수 있기 때문에 다양한 기기의 연결 및 데이터 공유가 강조되는 IoT 산업에 유기적으로 접목될 수 있습니다. 게다가 중앙 집중 시스템 및 이를 위한 인프라가 필요하지 않기 때문에 설비투자 및 운용 비용을 낮출 수 있어서 IoT 산업의 확산에 큰 도움이 될 것으로 보입니다.

특히 블록체인이 적용된 IoT 시스템은 IoT 산업의 응용 분야를 더욱 확대하는 계기가 될 것입니다. P2P 기반 데이터 공유의 편리성과 더불어 안전한 데이터의 저장 및 활용이 강조되는 분야를 중심으로 블록체인 기반 IoT 시스템을 도입하려는 분위기가 확산될 것으로 전망됩니다.

2. IoT 시스템 구현의 한계

2.1

IoT 산업의 대용량 데이터 처리

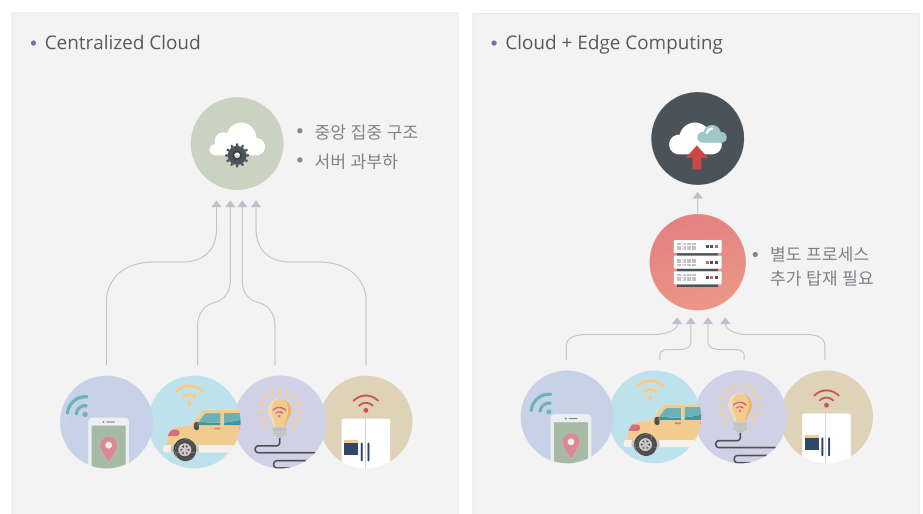
중앙 집중형 아키텍처의 대용량 데이터 처리 문제

IoT 서비스가 활성화 되면서 네트워크에 연결된 디바이스가 급격히 늘어나는 추세이며, 이러한 디바이스의 증가는 데이터 트래픽의 증가로 이어질 수밖에 없습니다. 특히, 웨어러블이나 커넥티드카 서비스가 시작되면서 인포테인먼트(Information+Entertainment) 측면에서 데이터 트래픽의 폭증이 예상되고 있습니다.

대부분의 IoT 기업들은 클라우드 서비스 사업자에게 컴퓨팅 자원을 임대 받은 후 IoT 디바이스를 관리하고 있습니다. 그러나 기존 클라우드 시스템은 중앙 집중 서버가 모든 데이터를 처리하기 때문에 폭증하는 데이터를 처리하기에는 비효율적이며, IoT 서비스 전체의 속도 및 품질 저하를 가져오고 있습니다.

최근에는 데이터 트래픽 부담을 줄이고 서비스 지연 확률을 낮추기 위해서, 분산된 소형 서버를 기반으로 실시간 데이터를 처리하는 '엣지 컴퓨팅' 기술이 도입되었습니다. 하지만 엣지 컴퓨팅은 연산처리를 담당할 별도의 프로세스가 추가로 탑재되어야 하기 때문에 설비 유지에 대한 비용 문제나 시스템 관리의 어려움이 존재합니다.

< 그림2. IoT 산업 - 데이터 저장 방식의 변화 >



2.2

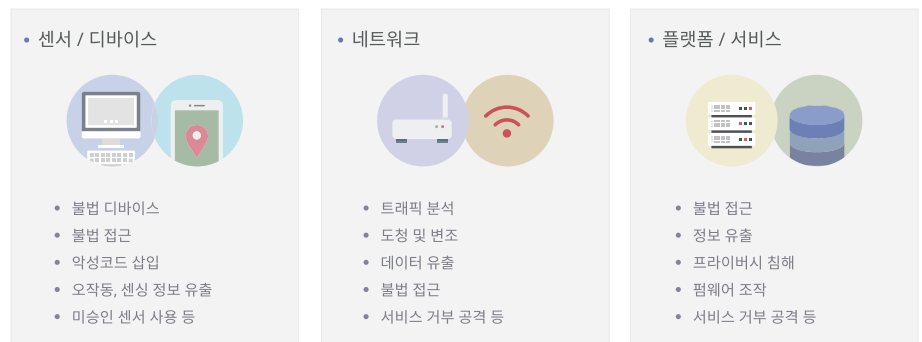
IoT 산업의 보안

IoT 디바이스의 해킹 및 비인가된 디바이스의 접근으로 인한 보안 문제

IoT에 연결되는 디바이스들은 자신을 구별할 수 있는 개별 ID를 가지고 네트워크로 연결되어야 합니다. 현재 IoT산업에서는 다양한 디바이스들이 정보제공 주체로 등장하고 있지만, 개별 디바이스들에 대한 신뢰성 있는 ID인증 및 디바이스들 간 상호 전송되는 데이터들의 검증 체계가 없는 상황입니다.

IoT 환경에서는 <그림 3>에서와 같이 다양한 디바이스들이 상호 연결되어 있는 구조적 특성을 가지기 때문에 기존 시스템에서 사용되던 암호화 알고리즘을 사용하기 어려워 Malware, DDos 등 외부의 공격에 취약합니다. 실제로 다양한 IoT 디바이스에 대한 공격 사례가 빈번하게 등장하고 있으며, 해킹된 디바이스는 사용자 계정 정보, 각종 패스워드 등 중요 데이터가 유출되어 악성코드와 스팸을 퍼뜨리는 유포지로 활용될 가능성이 높습니다. 또한 해킹된 디바이스의 위변조된 데이터는 검증 및 보안이 불가능하기 때문에 잘못된 데이터 전송에 따른 전체 시스템의 오작동 등 다양한 부작용이 발생하게 됩니다. 따라서, IoT 디바이스에 대한 인증이나 데이터 보안 체계 미확립 시 전체 IoT 서비스에 위협이 발생할 수 있습니다.

< 그림 3. IoT 환경에서의 보안 위협 >



2.3

블록체인과 IoT 시스템의 융합

블록체인 기반 소프트웨어 개발의 어려움

많은 기업들이 IoT 기술을 활용해 사업 영역을 확장하고자 노력하고 있으나, 이러한 기업들의 인프라는 다양한 기술 및 프로세스로 구현되어 있기 때문에 시스템 구조가 매우 복잡합니다. 따라서 새로운 프로그래밍 프레임 워크와 개발 언어를 사용하는 블록체인과 같은 신규 기술을 접목하는데 있어서 기업들은 시스템 개발 관련 유연성 및 역량을 갖추지 못한 실정입니다.

그렇기 때문에 대부분의 기업들은 블록체인 기반 비즈니스 프로세스의 구현과 이에 따른 시스템 구축 업무를 주로 아웃소싱 계약을 통해 제3자에게 의존하는 경향이 많으며, 이는 많은 비용과 시간을 요구하게 됩니다. 따라서 기업들은 자사의 개발자들이 익숙한 기존 개발언어인 java, c#, c++, php 등 다양한 언어를 지원하고 쉽게 DApp을 개발할 수 있는 전문적인 툴과 환경을 제공받기를 원하고 있습니다.

블록체인과 IoT 시스템의 통합 문제

기존 블록체인들은 IoT 산업과의 융합을 위해 블록체인의 단점을 보완하고 높은 처리 속도와 확장성을 확보하기 위한 다양한 방법을 모색하고 있지만, 아직까지 만족할 만한 수준으로 디바이스 보안이나 탈중앙화와 관련된 문제를 해결하지는 못하고 있습니다.

퍼블릭 블록체인의 경우 데이터 트랜잭션 발생 시, 노드(Node)의 제한된 연산능력으로 인한 낮은 처리 속도로 인해 실용적인 IoT 시스템 구현에 어려움이 있습니다. 프라이빗 블록체인 기반의 IoT 시스템은 블록체인 네트워크에 참여할 수 있는 권한 제한을 통해 퍼블릭 블록체인 대비 높은 처리 속도와 확장성을 일부 보장하지만, 탈중앙화가 이루어지지 않아 데이터의 투명성을 담보할 수 없습니다. 이에 블록체인 산업 관련 종사자들과 개발자들은 기존 블록체인 기술과 IoT 산업의 다양한 디바이스를 하나로 융합하여 주는 새로운 기술의 필요성을 제기하고 있습니다.

3. ReapChain의 Solution – ReapChainBaaS

- ReapChain은 IoT 기술과 블록체인의 완벽한 융합을 위한 솔루션으로 ReapChainBaaS를 제공합니다.

3.1

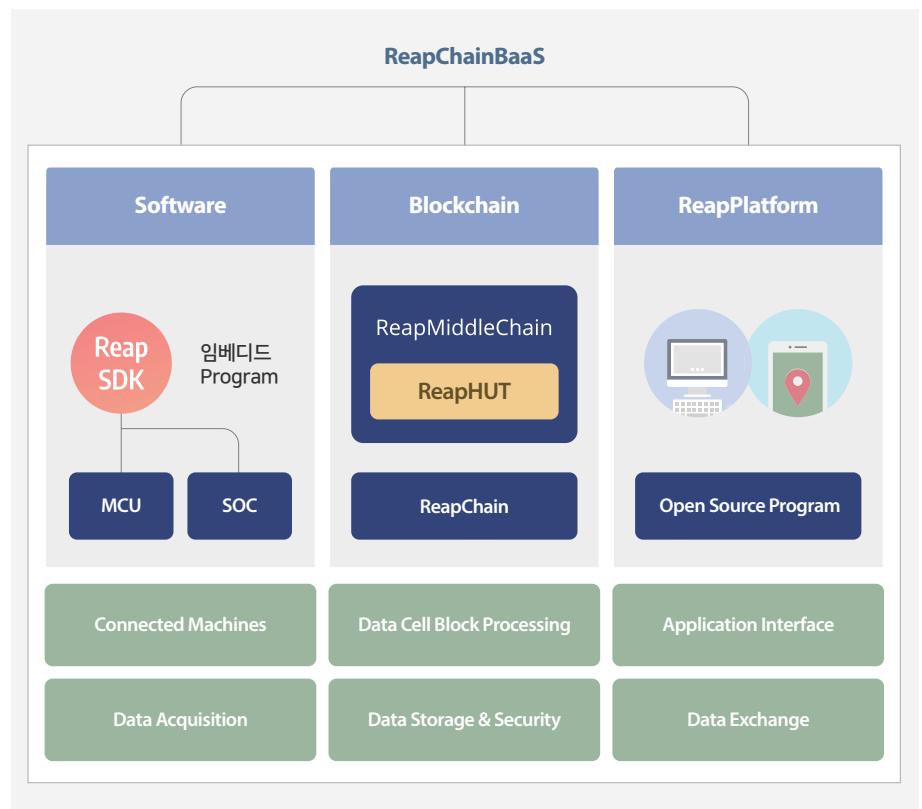
ReapChainBaaS 의 개요

BaaS (Blockchain as a Service)는 블록체인 기반 소프트웨어의 개발 환경을 제공하는 클라우드 컴퓨팅 플랫폼이며, 서비스형 블록체인을 의미합니다.

ReapChain의 서비스는 BaaS 형태로 제공되며, 별도의 전문지식 없이도 블록체인 인프라를 구축할 수 있는 간단한 모델과 비즈니스 맞춤형 API를 제공합니다. 따라서 ReapChainBaaS를 활용하면 누구나 쉽고 편리하게 블록체인과 IoT 산업을 융합할 수 있으며 서비스 개발 시간을 단축하고, 개발을 용이하게 하는 등의 이점이 있습니다.

ReapchainBaaS 기반 주요 서비스는 IoT 디바이스의 PID(Private ID)를 구현할 수 있는 ReapSDK와 스토리지 서비스인 ReapHUT, 운영 플랫폼이자 데이터 스토어 역할을 하는 ReapPlatform이 있습니다.

< 그림 4. ReapChainBaaS 구성도 >



3.2

ReapChainBaaS 기반 주요 서비스

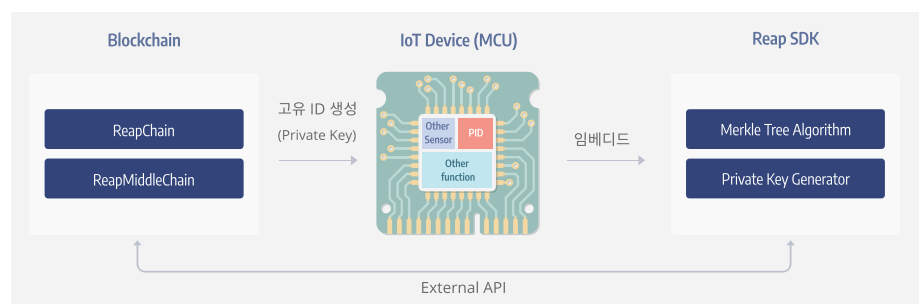
ReapSDK : IoT 디바이스 PID(Private ID) 구현

개인의 신원 인증에만 한정되어 적용되던 DID 기술을 ReapSDK의 독자적인 암호화 기술을 통해 각각의 디바이스에 적용하여, 새로운 디바이스 인증체계인 PID를 구현하고 데이터의 보안성을 확보하고자 합니다.

① ReapSDK를 통한 Private ID 구현

ReapSDK는 개별 IoT 디바이스에 32 Byte의 PID를 생성하여 내부의 비휘발성 메모리에 저장합니다. 그리고 데이터 전송(Transaction) 시, ReapMiddleChain에서 생성되는 최종 해시정보를 전달받고 저장함으로써 개별 IoT 디바이스가 ReapChain에서 하나의 노드가 되어 디바이스의 신뢰성을 검증할 수 있습니다.

< 그림 5. 디바이스 PID의 구현 >



- 디바이스 프라이빗 키: 각 MCU마다 고유의 프라이빗 키를 발급해 기기간 독립적이고 고유한 ID 값을 생성하고 부여한다.
- 사용자의 프라이빗 키는 패스워드로 암호화하여 저장한다.
- 암호화 알고리즘은 기존 이더리움에서 사용하는 AES-128을 개량한 형태이며, 브루트 포스(Brute Force) 공격에 대비하여 10,000~200,000번 정도 암호화하여 키스토어 파일 형태로 보관된다.
- 알파벳과 숫자가 조합된 8자리의 패스워드로 암호화된 키스토어 파일은, 암호화를 풀기가 거의 불가능한 형태이다.
- 머클 트리 (Merkle Tree) 데이터: IoT 디바이스는 MCU의 사양 및 성능에 따라 5개 ~ 50개의 해시 값을 저장할 수 있으며, 블록체인 노드의 일부 기능을 가진다. 머클 트리(해시 트리)의 마지막 값을 저장해 위변조를 방지할 수 있다.
- ReapChain 외부(External) API: ReapMiddleChain과 IoT Device가 통신하기 위한 프로토콜 기능을 지원한다.

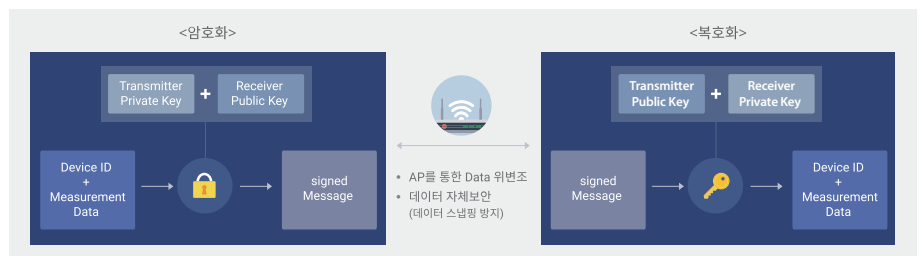
3.2

ReapChainBaaS 기반 주요 서비스

② 프라이빗 키의 암호화 기술을 통한 데이터 위변조 방지

MCU에서 생성된 데이터는 각 기기가 보유한 고유의 프라이빗 키와 독자적인 암호화 기법을 통해 Signed Message로 생성된 후 ReapMiddleChain을 거쳐 ReapChain으로 전달됩니다. 전달된 Signed Message는 복호화를 위해서 동일한 Private Key가 필요하기 때문에, 라우터 및 AP와 같은 통신 장치의 해킹이 발생해도 데이터의 위/변조 여부 확인이 가능합니다. 또한 통신장치를 통해 데이터 스냅핑(Data Snapping, 데이터를 가로채는 행위)이 발생해도 프라이빗 키 없이는 데이터의 복호화가 불가능하게 됩니다.

< 그림 6. 암호화된 프라이빗 키를 통한 Signed Message >



- 기기에서는 데이터를 전달하기 위해 Device ID 정보와 Measurement Data를 생성한다.
- 생성된 데이터를 기기가 가진 고유의 프라이빗 키와 데이터를 수신할 장치의 공개된 퍼블릭 키를 통한 암호화 과정을 거쳐 Signed Message를 생성한다.
- AP를 통해 전달되는 암호화된 Signed Message를 복호화하기 위해서는 전송받는 기기의 고유의 프라이빗 키가 필요하기때문에 승인되지 않은 기기는 원본 데이터를 복원할 수 없다.
- 암호화된 Signed Message를 전달받은 수신 장치는 보유한 프라이빗 키와 데이터를 전송한 장치의 퍼블릭 키를 이용해 데이터를 정상적으로 복호화 가능하다.
- 전송 과정에서 해킹을 통한 변조된 데이터가 전송이 되는 경우 수신 장치의 프라이빗 키와 전송한 장치의 퍼블릭 키를 통해 복호화 되지 않기에 위/변조 여부를 확인 가능하다.

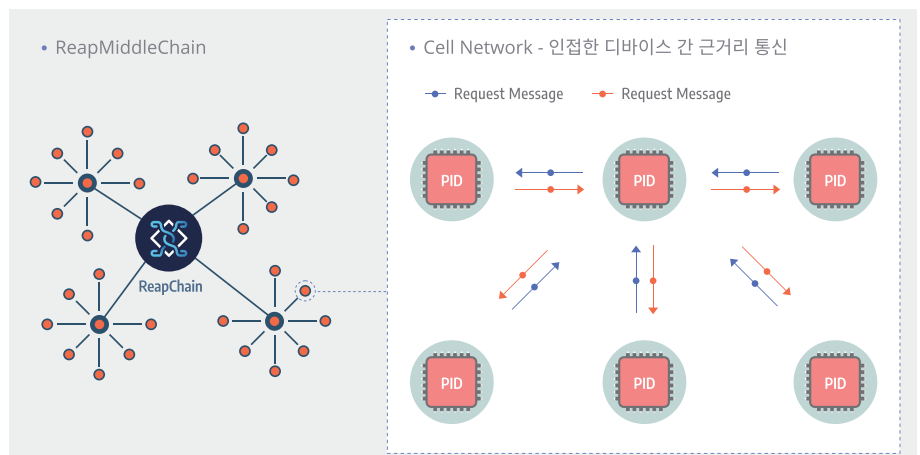
3.2

ReapChainBaaS 기반 주요 서비스

③ 머클 트리 (Merkle Tree) 알고리즘을 활용한 인접한 디바이스 간 상호 검증

네트워크는 여러 계층으로 분리되어 있고, 소형화된 IoT 디바이스에서는 메인 넷과 직접적인 통신을 지원하는 인터페이스가 존재하지 않는 경우가 많습니다. IoT 시스템의 최종 센서 노드에서 제공되는 데이터의 정확성을 위해서는 데이터를 중계해주는 릴레이 노드 뿐만 아니라 각 노드간 연결된 독자적인 단거리 무선 네트워크에서의 신뢰성 검증은 필수입니다. <그림 7>에서 보듯이 ReapSDK를 적용한 Cell 네트워크에서는 인접한 엣지 노드와 종단 노드의 머클 트리 값을 비교해 전송되는 데이터의 위/변조 유무를 확인하여 2차적인 보안이 가능합니다.

< 그림 7. 인접 디바이스 간 근거리 통신 구조 >



- 암호화된 퍼블릭 키를 기반으로 종단간 통신 데이터를 암호화한다.
- 노드와 연결된 IoT 기기들이 Cell Network로 연결되어 블록의 무결성을 검증한다.
- 각 IoT 기기들은 최근 N개의 블록 해시값을 저장하여, 연결된 노드가 Synchronized된 블록에 대해 검증을 함께 진행한다.

3.2

ReapChainBaaS 기반 부가 서비스

ReapHut : 강력한 추가 보안 및 효율적인 데이터 관리를 위한 스토리지

ReapHut은 프라이빗 임시 스토리지로써, 데이터 전송 및 저장 공간입니다. ReapHut에 저장된 데이터는 일정기간이 지난 후 삭제가 가능하며, ReapChain에 최종 전송될 필수 데이터를 분류하고 결정하는 기능을 가지고 있습니다.

ReapHut은 WORM(Write-Once Read-Many) 스토리지 기술을 적용하여, 데이터를 한번 기록하면 훼손할 수 없는 특성을 가진 비가역성 스토리지입니다. ReapHut의 데이터 관리 기술은 SHA-256 기반 디지털 보안과 데이터 실시간 암호화, 시간 변조 방지 기능 등을 가지고 있으며, 접근 권한 없이는 데이터에 대한 접근 자체가 불가능하기 때문에 위변조 및 삭제가 원천적으로 불가능합니다.

ReapPlatform : 편리하고 효율적인 서비스 관리를 위한 플랫폼

ReapPlatform은 데이터 스토어로서 데이터 거래가 발생하는 공간이며, 데이터 가공 업체, 서비스 제공자와 이용자, 그리고 데이터가 필요한 업체들간에 필요한 데이터를 매매할 수 있는 플랫폼입니다.

또한 ReapPlatform은 IoT 기기와 서버, 어플리케이션을 상호 연결하는 플랫폼으로써 IoT 국제표준인 oneM2M 기반으로 구현되었으며, 기기 정보를 관리하고 접근 제어, 인증, 사용자 관리 등의 서비스를 제공하는 운영 플랫폼입니다.

4. Business Model

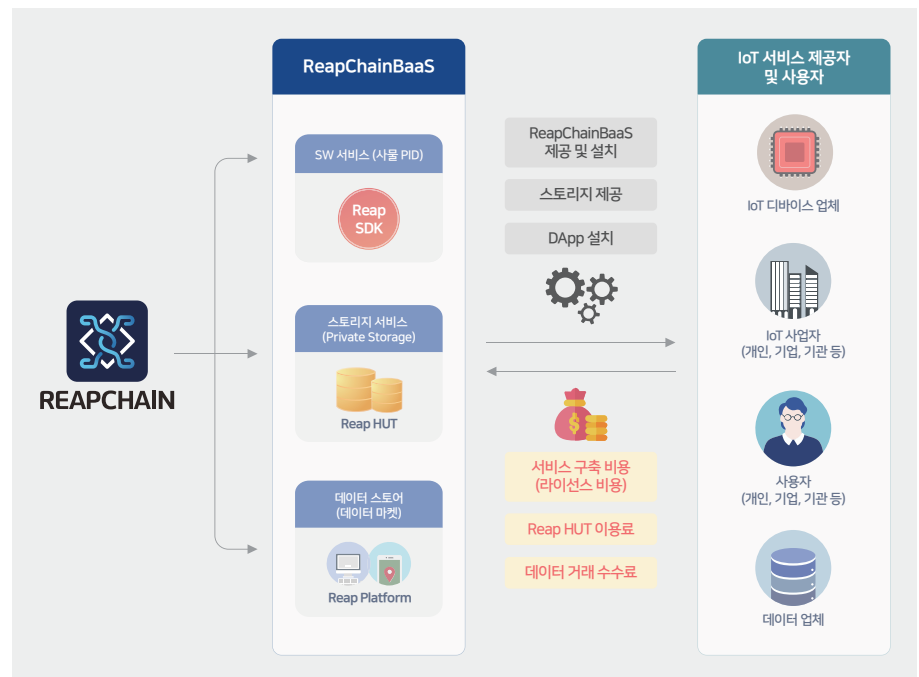
4.1

Business Model

ReapChainBaaS 기반 Business Model

ReapChain은 ReapChainBaaS 서비스를 통하여 IoT 산업에 특화된 플랫폼을 활성화 함으로써 다양한 비즈니스 영역들을 결합하고 합리적인 수수료와 인센티브 체계를 구축하며, 수익성 높은 토큰 이코노미를 통해 경쟁력 있는 비즈니스 모델을 확립하고자 합니다.

< 그림 8. ReapChain 비즈니스 모델 >



IoT 서비스 제공자 및 사용자들은 ReapChain이 제공하는 ReapPlatform을 하나의 데이터 허브로 활용하여 데이터를 쉽고 빠르게 등록하고 거래할 수 있습니다. 이를 통해 IoT 산업의 참여자들은 타 산업과의 연계 및 시너지 효과를 창출하고 블록체인 기반 데이터 경제 생태계를 실현할 수 있습니다.

4.1

Business Model

ReapChainBaaS 수익 구조

① ReapChainBaaS 서비스 이용료 (라이선스 비용)

서비스 사용자들은 ReapChainBaaS를 도입하기 위한 라이선스 명목으로 일정 금액을 요금제 방식으로 지급합니다.

- ReapChain Protocol을 설치해주고, 보안 솔루션부터 복잡한 백엔드(Backend)까지 관리해주는 총 비용을 포함합니다.

② ReapHut 이용료

서비스 사용자들은 필요에 따라 ReapHut 용량을 추가 구매할 수 있으며, 스토리지의 사용량에 비례하여 사용료를 지급합니다.

- ReapHut 서비스 사용시 월 사용량을 지정하여 선택할 수 있으며, 선택한 사용량에 따라 비용이 다르게 책정됩니다.

③ 데이터 거래 수수료

분석 및 활용 그리고 홍보 및 마케팅 목적으로 별도의 고객 데이터가 필요한 사용자들은 ReapPlatform 내에서 비용을 데이터 생산자에게 지불하고 데이터를 구매할 수 있으며, 데이터 거래에 따른 일정 수수료를 ReapChain에게 지불합니다.

< 표 2. ReapChainBaaS 요금 기준 예시 >

구분 : 등급제 적용 (일반/중급/고급)

금액 : 정액제 방식 (월 과금)

ReapSDK	ReapHut (용량)	ReapChain (제공 TX)
최초 설치 시 1번 과금	등급제에 따라 차등 용량 제공	등급제에 따라 차등 Tx 횟수 제공

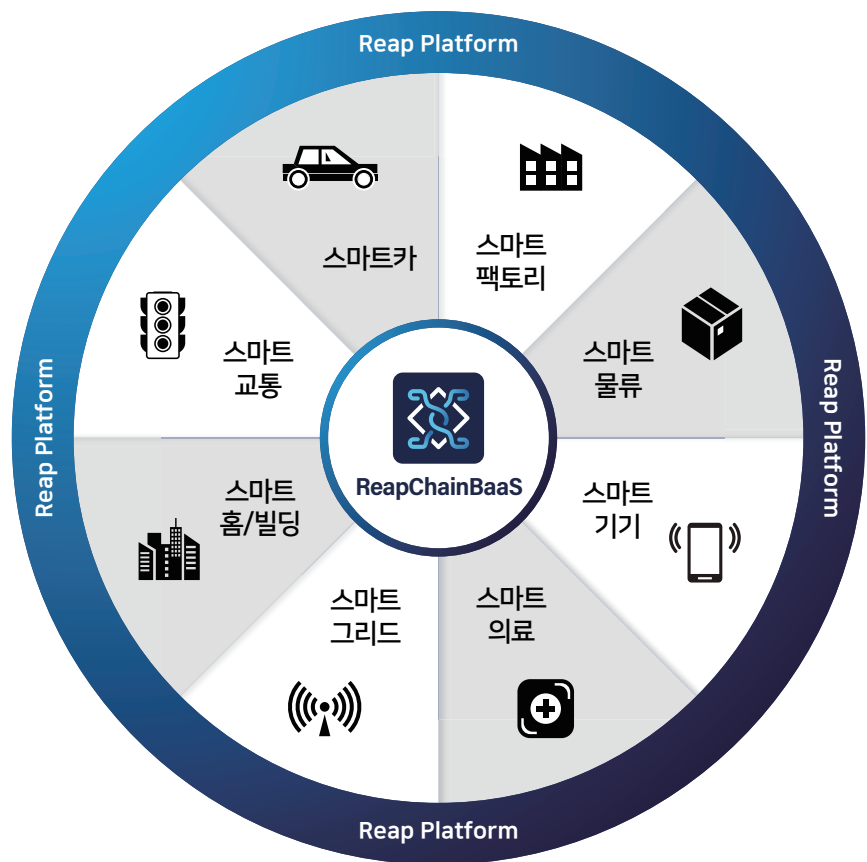
- 월 과금제 방식: 서비스 이용 시, 설정 용량에 따라 요금이 변동됩니다.
- 세부적인 기준은 서비스 오픈 시, 상황에 따라 변경될 수 있습니다.

4.2

적용 가능 분야

ReapChain은 ReapChainBaaS를 통하여 다양한 IoT 산업분야에 적합한 플랫폼을 제공하고 IoT 산업 생태계 참여자들간의 상호 연계 및 확장을 통해 데이터를 공유하고 활용할 수 있는 통합 플랫폼을 구축하고자 합니다.

< 그림 9. ReapChainBaaS 적용가능 분야 >



4.2

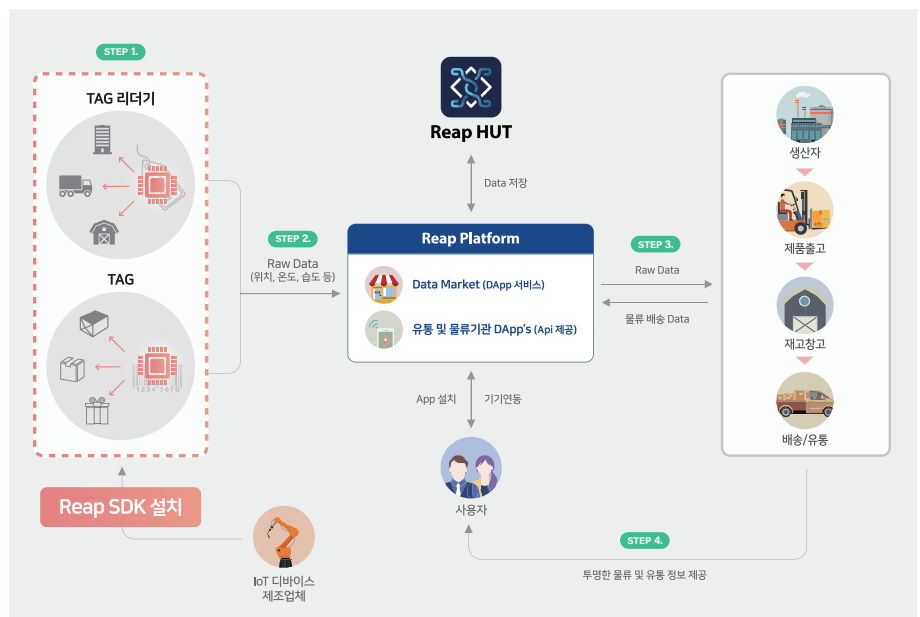
적용 가능 분야

제품 이력 및 추적을 통한 스마트 물류 서비스

ReapChainBaaS를 사용하는 유통/물류 업체들은 제품 선적, 집하, 운송에서부터 소비자까지 정확히 전달되는 일련의 과정에서 모든 정보를 수집, 분석하고 공유하여 물류 시스템의 안정성, 효율성, 처리 속도를 최적화할 수 있으며, 사용자들은 투명한 물류 및 유통 정보를 제공받을 수 있습니다.

제조 및 판매 업체들은 유통/물류 배송과정에서의 정보를 실시간으로 파악하여 최종 소비자에게로의 최종 배송 정보 등을 제공하고 거래 정보를 통해 불필요한 생산을 줄일 수 있습니다.

< 그림 10. ReapChainBaaS 기반 유통 시스템 Flow Chart >



Step1. ReapSDK가 적용된 TAG system을 기반으로 제품 생산 및 데이터 입력

Step2. TAG system를 통해 제품 상태 데이터를 지속적으로 전송 및 검증

Step3. ReapPlatform을 통해 유통 전 과정에서의 위치 정보, 입출고 기록 등 추가 데이터 전송 및 검증

Step4. 소비자가 구매한 제품에 대한 신뢰할 수 있는 데이터 수신 및 확인

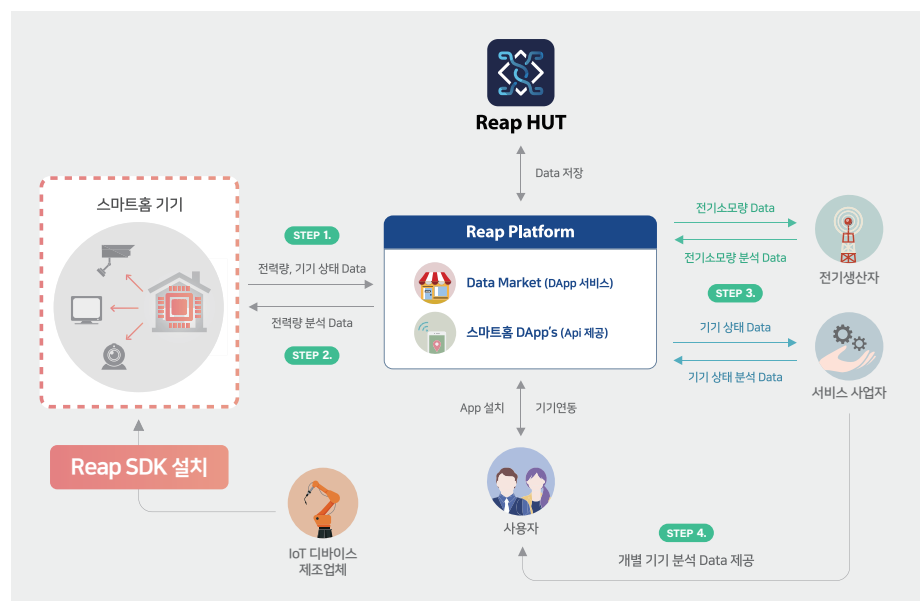
4.2

적용 가능 분야

스마트 홈 에너지 관리 서비스

ReapChainBaaS를 사용하는 전력회사는 각 산업 및 가정에서 소비되는 전기 소모량을 분석하여 적정량의 전기생산을 통한 효율적인 운영이 가능하며, 서비스 사업자는 스마트 홈 개별기기의 상태 데이터를 기반으로 각 가정으로 필요한 시기에 필요한 양만큼 전력을 제공하여 불필요한 에너지 소비를 방지할 수 있습니다. 사용자는 개별 기기 상태 관련 데이터 및 전력량 분석 데이터를 통해 투명하고 신뢰할 수 있는 서비스를 제공받을 수 있으며, 제조업체는 제공된 기기의 전기 소모량에 대한 데이터 및 기기 상태에 대한 실시간 정보를 제공받을 수 있습니다.

< 그림 11. ReapChainBaaS 기반 전력 시스템 Flow Chart >



- Step1. ReapSDK가 적용된 스마트 홈 기기에서 발생된 각종 데이터 및 전력량을 전송 및 확인
- Step2. 스마트 홈 디바이스 기기를 통해 기기 상태 및 전력량 데이터를 지속적으로 전송 및 검증
- Step3. ReapPlatform을 통해 전기생산자는 각 가정에서 필요한 전기량을, 서비스 사업자는 서비스 질 향상을 위한 기기 상태 데이터를 확인
- Step4. 가정에서는 스마트 홈의 개별 기기에 대한 신뢰할 수 있는 데이터 수신 및 정보 확인

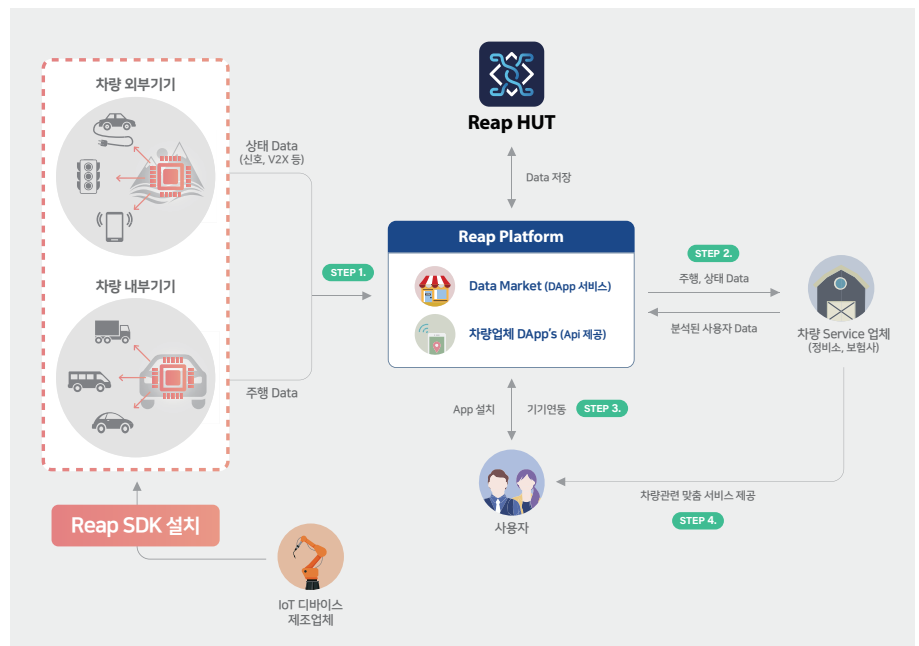
4.2

적용 가능 분야

주행 데이터를 활용한 스마트 차량 서비스

ReapChainBaaS를 사용하는 서비스 제공업체들은 V2X(Vehicle to Everything Communication, 차량사물통신) 데이터를 바탕으로 자동차 사용자의 주변 정보를 구체적으로 확인하여 자동차 제조업체, 자동차 사용자 및 서비스 제공자에게 제공합니다. 자동차 사용자는 편리한 차량 관련 서비스를 제공받을 수 있고, 자동차 제조업체는 서비스업체가 필요로 하는 기기 생산을 통해 매출을 증가시킬 수 있습니다. 서비스 제공자인 보험사는 자동차 사용자의 운전습관을 기반으로 차별화된 상품을 제공하는 등 사용자 맞춤형 서비스 제공이 가능합니다.

< 그림 12. ReapChainBaaS 기반 차량서비스 Flow Chart >



- V2X (Vehicle to Everything): 차량을 중심으로 유무선망을 통해 다른 사물과 정보를 교환하거나 제공하는 기술입니다.

Step1. ReapSDK가 적용된 차량 내/외부 기기에서 지속적인 데이터 전송 및 검증
 Step2. 차량 서비스업체는 ReapPlatform을 통해 차량주행 및 상태 데이터 수신 및 분석 데이터 전송
 Step3. 사용자는 기기 연동을 통해 신뢰할 수 있는 차량 데이터 정보 수신 및 확인
 Step4. ReapPlatform을 통해 제공받은 분석 데이터를 기반으로 차량관련 맞춤 서비스 제공

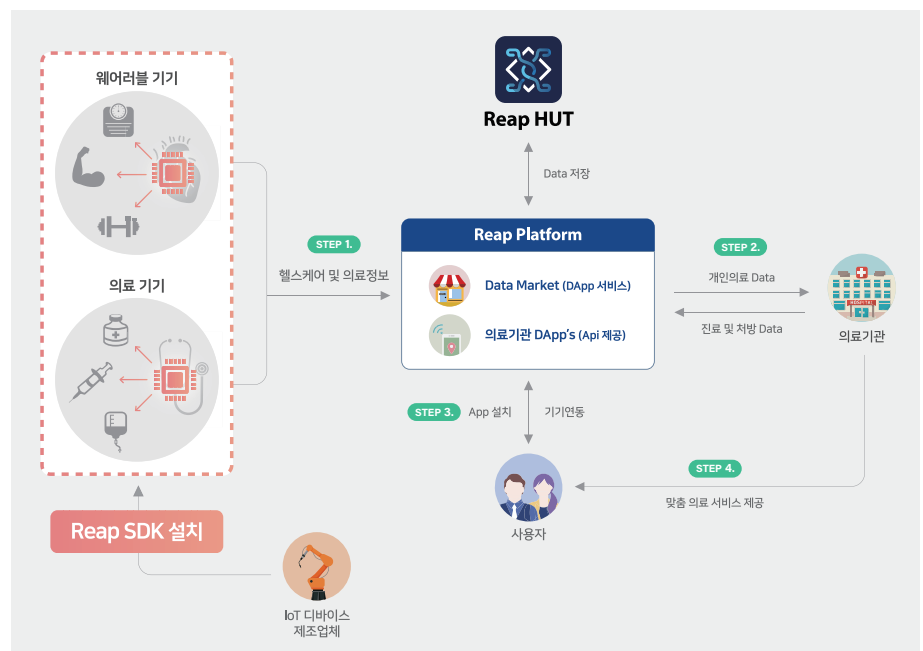
4.2

적용 가능 분야

개인의료 정보 기반 스마트 의료 서비스

의료기관은 ReapChainBaaS에서 제공하는 ReapPlatform을 통해 수집된 진료정보, 치료기록 등 개인의료 데이터를 기반으로 맞춤형 의료서비스를 제공할 수 있으며, 환자정보가 공유되지 않음으로 발생할 수 있는 의료사고를 줄일 수 있습니다. 사용자는 잘못된 처방, 비양심적인 의료기관을 피할 수 있고, 제조업체는 의료기관 데이터를 통해 최적화된 기기를 제공합니다.

< 그림 13. ReapChainBaaS 기반 의료 서비스 Flow Chart >



Step1. ReapSDK가 설치된 의료 기기에서 발생하는 개인의료 데이터 지속적인 전송 및 검증

Step2. 의료기관에서 ReapPlatform을 통해 개인의료 데이터 수신 및 사용기록 검증

Step3. 사용자는 제공받는 의료 서비스에 대한 신뢰할 수 있는 데이터 정보 수신 및 확인

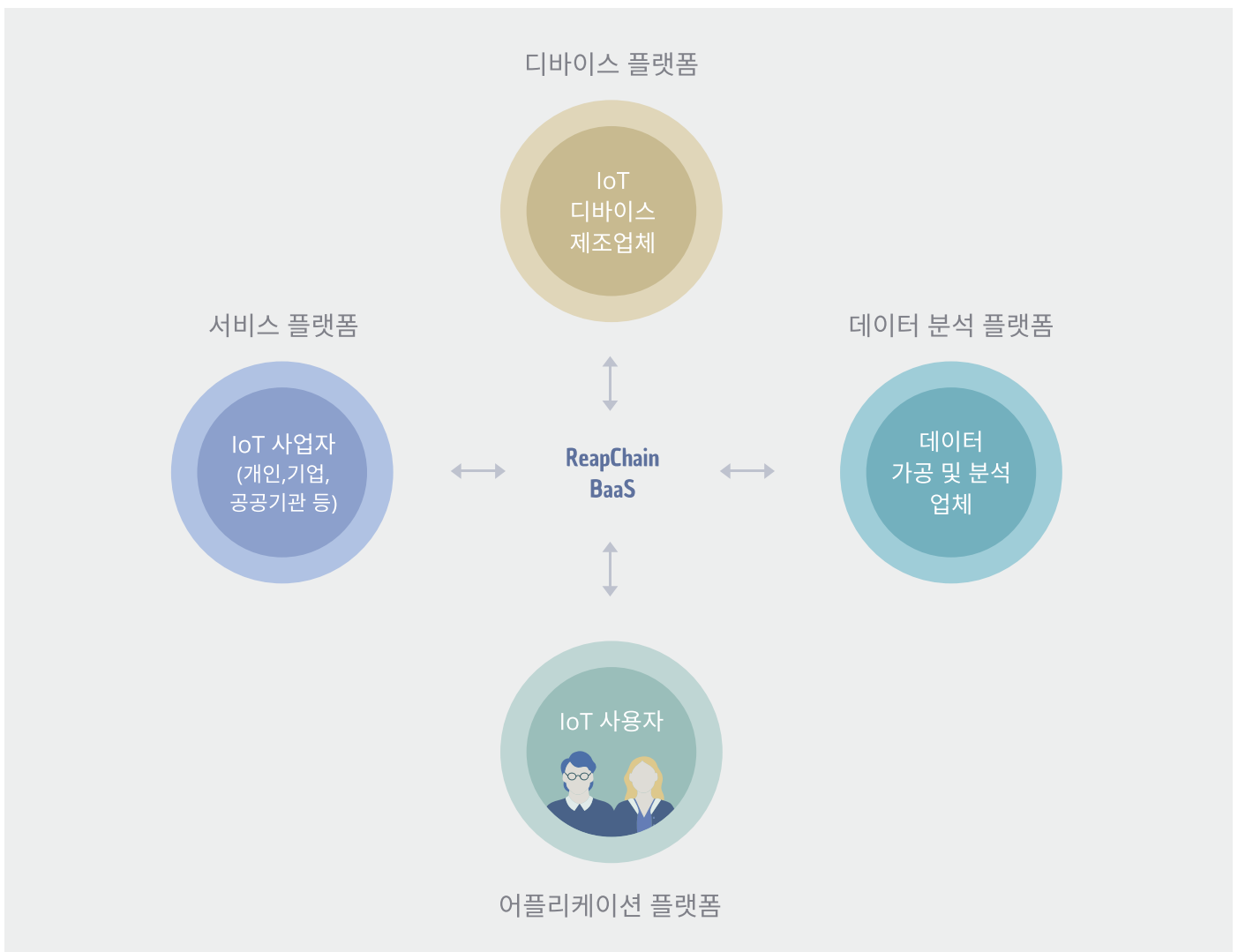
Step4. 신뢰할 수 있는 진료 데이터를 바탕으로 맞춤형 의료 서비스 제공

5. Ecosystem

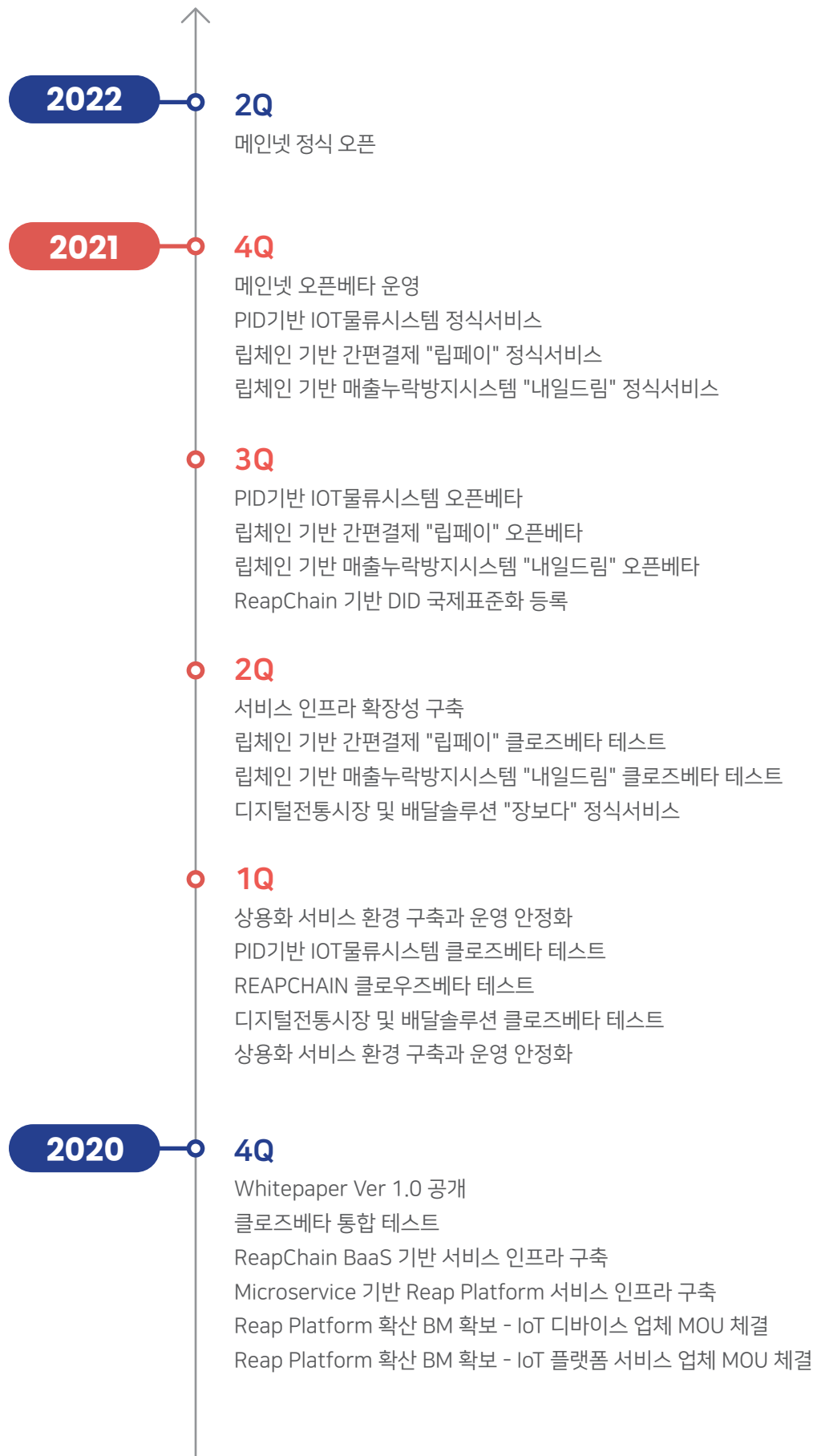
ReapChainBaaS 기반 Business Ecosystem

ReapChainBaaS 생태계의 구성원은 IoT서비스를 이용하는 사용자, IoT 디바이스 제조업체, IoT 기반 시스템을 구축하고자 하는 개인, 기업, 정부 및 공공기관 등 사업자, 그리고 IoT 산업 기반 데이터를 가공 및 분석하여 활용하고자 하는 업체로 구성됩니다.

< 그림 14. Business Ecosystem 구성도 >



6. Roadmap



2020

3Q

Whitepaper Ver 0.9 공개
Alpha 통합 테스트
ReapChain Beta (Ver 2.0) 개발 및 검증 테스트
ReapMiddleChain Beta (Ver 2.0) 개발 및 검증 테스트
Reap Platform & SDK Beta (Ver 2.0) 런칭 및 검증 테스트
Reap Wallet (Ver 1.0) 오픈
Pre-Sale 및 거래소 상장
토큰 생성 (TGE) 및 분배
MCU 기반 사물 PID 개발

2Q

ReapChain Alpha (Ver 1.0) 개발 및 검증 테스트
ReapMiddleChain Alpha (Ver 1.0) 개발 및 검증 테스트
Reap Platform & Reap SDK Alpha (Ver 1.0) 런칭 및 검증 테스트
ReapChain 토큰 세일 - Private Sale 1차
ReapChain 토큰 세일 - Private Sale 2차

1Q

ReapChain MVP (Ver 0.8) 검증 테스트
ReapMiddleChain MVP (Ver 0.8) 검증 테스트
Whitepaper Ver 0.8 공개
Seed Sale

2019

4Q

Reap Platform & Reap SDK (Ver 0.1) 설계 및 개발
Smart Contract 구축 및 Reap Wallet (Ver 0.1) 개발

3Q

ReapMiddleChain (Ver 0.1) 설계 및 개발

2Q

ReapChain 메인넷 (Ver 0.1) 개발

1Q

ReapChain 메인넷 기획 및 설계

7. Team & Partner

Core Members



JAKE LEE
co-CEO

영남대 기계공학
경북 청년정책 위원회 위원
경북 블록체인 특별위원회 위원
스타트업, 핀테크분야에서 경영 13년
(주)엘엔벤처그룹 대표이사
(주)코인베스트 대표이사



SEUNGJONG LEE
COO

서울대학교 자연과학대학 계산통계학과
한국산업 기술대학교 컴퓨터공학과 겸임교수
삼성전자,셀빅(주),(주)모코코,네무스텍(주)에
서 보안IT관련 및 경영자 근무
라인플러스 Dev Rleation 리드
한국데이터산업진흥원 사외이사
경기도 4차산업혁명위원회 위원
경기도 정보화위원회 위원
공정거래위원회 데이터포털 구축 자문위원



KHAN KIM
CSO

뉴욕대 경영학과
콜롬비아 대학원 MBA
옵티마 컨설팅, LG투자증권, 렌드리스, KPMG



SUHO KWON
CTO

서강대학교 컴퓨터과학, 운영체제 연구실.
삼성전자, 뉴미디어라이프, 삼성테크윈(한화
테크윈), SK하이닉스, 팍스데이타텍 근무
현) KBIPA(한국블록체인진흥협회) 교육센터장
현) ReapChain 연구소장
임베디드 시스템 개발 및 소프트웨어 품질 엔
지니어링 분야에서 20년 이상의 경력



JAY YOO
CMO

서울시립대학사수로 (마케팅전략)
University of Minnesota (Twin Cities) MBA
고려대학교 사학과
현) 립체인 전략기획부
현) 송의여자대학교 스토아메니지먼트과 겸
임교수
전) 현대종합상사, 제일기획, 현대자동차

Advisors



HYEONSANG EOM

박사학위 / 컴퓨터 과학, University of Maryland at College Park (UMCP), Maryland (MD), 미국, 2003
 분산 처리 및 컴퓨터 / 임베디드 시스템
 컴퓨터 시스템 / 네트워크 / 애플리케이션 / 소프트웨어 성능 공학
 모바일 애플리케이션 / 미들웨어 (보안 포함)
 서울 대학교 분산 컴퓨팅 시스템 LAB 교수
 15 년 경력



TAEHONG KANG

송실대 전자계산학과 졸업
 송실대학원 컴퓨터학과 박사
 현) 송실대 정보과학대학원 겸임교수
 현) (주)로보피아투자전문 부사장, CTO
 전) (주)코스콤 자문위원
 전) (주)딜라이트체인 부사장, CTO
 전) 한국정보처리학회 이사
 전) 한국정보과학회 이사
 전) 글로벌핀테크산업진흥센터 센터장



CHULHO LEE

부산대학교 경영학과 석사
 부산대학교 경영학과, 학사
 중국 하얼빈 공과대학 경영공학과 부교수
 미국 Xavier대학교 경영학과 객원교수
 정보 보안 경제, 개인정보보호 및 보안 행동경제, 정보 시스템에 대한 실증 등 다수의 연구 활동



SEUNGHUN HAN

University of Central Florida Finance Ph.D
 University of South Carolina Statistics M.S
 현) 한국과학기술원(KAIST) 기술경영학부 AACSB AOL(Assurance of Learning) 부교수
 현) 한국정보사회학회 이사 및 부회장
 Big Data, Economics, Science, and Technology Society, Council Member
 2018년 우수 강의상 수상
 기술경영학부 AACSB AOL 위원회 위원장
 기술경영전문대학원 운영위원
 경영대학 AACSB 위원회 위원
 기타 학부 입학전형 위원, 추가 TA개선 위원회 위원, ICC국제화위원회 위원, 금융공학 부 전공 프로그램 운영 위원 및 한중일 CAMPUS Asia 사업단 위원으로 참여
 KAIST 2012년을 빛낸 연구성과" 54개 중에 연구논문이 선택



HYUKJUN KWON

순천향대학교 경제금융학과 조교수
 연세대학교 경영학석사
 B.S. in Information Systems of School of Business, Virginia Commonwealth University, USA
 현) 한국조폐공사 분산원장(Blockchain)자문 교수
 현) 한국블록체인학회 발기인 및 운영위원
 현) 한국지급결제학회 부회장
 현) 한국정보처리학회 이사
 현) 한국전자거래학회 이사
 현) 보험개발원 블록체인 자문교수
 현) 한국행동과학연구소 위촉위원
 전) BK21 책임연구원 (연세대학교 정보대학원)
 전) 한국정보기술융합학회 발기인 및 산학협동 이사
 Blockchain, Distributed Ledger Technology
 Fintech, Token Economy VR and AI



CHEOLHWAN KIM

서울대 전자공학과 졸업
 현) 한양대 겸임교수
 현) 국제제품관리협회 자문이사
 현) ㈜아비유시스템즈 고문
 현) 지디넷코리아 자문
 현) 생산성본부 블록체인 강의
 현) ICT 폴리텍 블록체인 강의
 전) 데이콤 분산트랜잭션처리 응용개발
 전) 기가링크 창업자(네트워크 장비 개발)
 전) 인텔스 연구소장(러시아, 이스라엘 신기술 프로젝트)
 전) 이스라엘 MusicGenome/ExpoBee 한국 컨설턴트
 전) 한국청년기업가정신재단 K-ICT 멘토링센터 멘토
 전) 한국기술벤처재단 멘토

Advisors



HYUNWOO YI

고려대학교 법학과 졸업
서울대학교 대학원 법학과 수료(기초법 전공)
제 40회 사법시험 합격
제 30기 사법연수원 수료
법무법인 아람
서정 법무법인
법무법인 휴먼
법무법인 동인
법무법인(유한) 대륙아주
현 법무법인(유한) 바른 구성원 변호사
현 법무부 국제투자분쟁 법률자문단 자문위원
현 법제처 법령해석심사위원회 위원
현 고용노동부 규제심사위원회 위원



DAVID LEE

현) 디센트레 대표
Hdac Operation Director
Advisor of FORESTING
Advisor of B21
Advisor of FLETA
한양대학교 경영대학원 MBA 석사
SW융합협의회 블록체인 자문위원
KOSA SW모니터링단 위원
Blockchain Raider Contributor
2019 SW모니터링단 과학기술정보통신부 장관상 수상



JONGWON KIM

서울대 금속공학과
현) 사단법인 한국블록체인산업진흥협회 상
임이사
전) 거변테크 대표
전) 서울메트로 사외이사



HOSUP KAN

미국 뉴욕 Fashion Institute of Technology 수료
미국 드렉슬대학교 패션디자인 석사
성균관대학교 대학원 의상학박사
Kokin Inc., Nicole Paris, DKNY 디자이너 역임
(주)아모레퍼시픽 '오트세이 스포츠' 크리에
이티브 디렉터
(주)SK 스토아 패션디렉터
프로젝트 런웨이 코리아 시즌1~4 멘토
동덕여자대학교 디자인대학 교수
홍익대학교 미술대학 교수
미국 하버드대학교 초청 연구교수
사단법인 한국패션문화협회 회장
사단법인 한국패션비즈니스학회 회장



SUNGJIN KIM

부산대 전산학 석사
삼성멀티캠퍼스 블록체인 빅데이터 전문멘토
방송위 & TTA DMB/IPTV 기술/서비스 표준 전임
ISO/IEC MPEG-2/4 국제표준 전임
삼성종합기술원, 판미디어 등에서 미디어서비
스플랫폼, 디지털트윈, 블록체인 등 IT 개발 경력
28년

Partners



Advisory group



8. 참고문헌

- SMTECH (중소벤처기업부, 2019), "2020-2022 전략기술로드맵, IoT & 블록체인 & 빅데이터"
- 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 (소프트웨어정책연구소, 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 block chain 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"
- 이대화, 지우중 and 김형식 (OSIA Standards & Technology Review, 2019) "IoT 환경에 적합한 블록체인 및 스마트 컨트랙트 기술 연구"
- ETRI (한국전자통신연구원, 2018) "센서산업과 주요 유망센서 시장 및 기술동향 보고서", "블록체인과 합의 알고리즘"
- NIPA (정보통신산업진흥원, 2018), "데이터 기술 시대를 대비한 주요기술 동향 및 시사점"
- STEPI (과학기술정책연구원, 2018) "블록체인(Blockchain) 기술동향과 시사점"
- 하나금융경영연구소 (2018), "4차 산업혁명을 주도하는 플랫폼 경제의 확산과 시사점"
- LG경제연구원 (2018), "탈규모 시대의 제조업, 플랫폼 비즈니스로 도약"
- KISDI (정보통신정책연구원, 2018) "블록체인의 다변화: 채굴 없는 블록체인의 확산"

Disclaimer

면책조항

아래 내용들을 주의 깊게 읽으시기 바랍니다. 아래 내용은 본 백서를 읽는 모든 사람에게 적용됩니다. ReapChain 백서(이하 “백서”)는 작성 당시를 기준(as is)으로 하여 작성 및 제공되므로 백서에 포함된 어떠한 내용이라도 ReapChain Inc.의 재량에 따라 언제든지 변경되거나 업데이트 될 수 있으며, 본 백서의 어떠한 내용이라도 장래 시점까지 변경되지 않는다는 점을 담보하지 않습니다.

만일 본 백서의 내용에 대해 어떠한 의심의 여지가 있는 경우 구매 전 회계사, 변호사 또는 기타 전문가와 상의해야 합니다.

1. 본 백서의 목적은 ReapChain Inc.가 준비 중인 ReapChain에 대한 요약된 정보와 소개를 다루는 것에 있습니다. 본 백서는 ReapChain 또는 ReapChain Inc.에 대해서 법적으로 구속력이 없으며 백서 상 어떠한 문구들도 구독, 구매, 투자 제안 그리고 투자 강요의 성격을 띠고 있지 않습니다.

2. 본 백서 상 모든 정보나 분석 내용은 투자결정의 근거가 될 수 없으며, 어떠한 투자 제안이나 조언도 아님을 알려드립니다. 본 백서 상의 미래 계획적인 성격을 띄는 어떠한 내용이나 데이터는 어떠한 이유에서든 바뀔 수 있으며 정확하지 않을 수 있고 그 내용에 관한 어떠한 보장이나 약속도 없음을 알려드립니다.

3. 이사, 에이전트, 직원, 계약자, 판매 파트너를 포함한 ReapChain Inc.는 다음과 같이 본 문서에 포함된 정보에 따라 발생할 수 있는 직접적 또는 간접적으로 발생하는 모든 종류의 손해를 책임지지 않습니다: (1) 해당 백서에 따른 계약 내용의 정확성 및 완전성; (2) 백서의 오류 또는 누락; (3) 확인되지 않은 원인으로 인한 백서 열람 불가능; (4) 백서 사용 또는 미사용으로 인해 발생하는 기타 모든 손해.

또한, ReapChain Inc.는 본 문서에 포함된 정보를 이용하여 한 의사 결정 행위에 따라 발생할 수 있는 다음 사항들에 대하여 사전 경고가 주어졌거나 해당 손해가 예측 가능할 경우에도 전적으로 책임을 지지 않습니다: (1) 이익, 수익, 부채 및 기타 모든 형태의 금전적 손해; (2) 사업 거래, 사업 활동, 영업 이익 관련 활동 중에 발생한 수입, 매출, 자본 감소, 채무 기타 손실; (3) 데이터 손실 또는 손상; (4) 부수적 또는 특수 손해; (5) 낭비되거나 손실된 관리 시간; (6) 간접적이거나 필연적인 손해

4. 진행중인 ReapChain의 내용이나 시장의 변화, 기술 발전 그리고 ICO나 토큰 규제의 변화에 따라서 백서의 내용은 달라질 수 있습니다. 그러나 ReapChain Inc.는 차후에 본 백서에 명시된 사건, 플랫폼, 향후 계획, 추정치의 변화나 오차범위 안의 변경 사항 등에 대해 독자들에게 통보하거나 보고 할 의무가 없음을 알려 드립니다.

5. 본 백서 상 법, 세무, 규제, 금융, 회계와 같은 분야에 대한 정보들은 조언이 아님을 알려드립니다. REAP의 구입은 구매자들에게 REAP의 구매를 위해 지불한 물질적 자산을 포함해 물질적인 손실을 가져올 수 있습니다. REAP 구입에 앞서, 구매 자들은 세무, 규제, 금융, 법률 등의 전문가들에게 잠재적 위험부담, 수익 및 REAP 거래가 초래할 수 있는 결과들에 대해서 상담할 것을 권합니다.

6. 자신의 법적 관할권 내에서 REAP의 인수와 처분 등에 관하여 발생할 수 있는 소득세 등 기타 과제 처분 및 해외 환전에 대한 법적 가능 여부를 판단하는 것은 전적으로 REAP 구매자의 몫입니다.

7. 백서의 출판·배포가 금지된 나라에서 본 백서의 출판·배포를 금합니다. 본 백서에 있는 정보들은 어떠한 규제 기관의 검증이나 인가도 받지 않았으며, 법에 저촉되는 어떠한 행위도 ReapChain Inc.에 효력이 없습니다. 본 백서의 출판·배포가 그 발행된 나라의 규제 사항을 모두 준수하였다는 것을 보장하지 않습니다.

8. ReapChain에 대한 공식 자료는 본 백서이며 한국어로 작성되었습니다. 본 백서는 다른 언어로 번역될 수 있으며 예비 구매자 및 기존 구매자 등과 구두 혹은 서면 의사 소통을 하는데 사용될 수 있으며 이 과정에서 일부 정보가 곡해되거나 잘못 해석되거나 손실될 수 있습니다. 따라서 이러한 대체적인 의사소통의 정확도를 보장할 수 없음을 숙지하시기 바랍니다. 그러한 부정확한 의사소통 발생 시 한국어로 작성된 본 공식 백서의 정보가 우선합니다.

9. 모든 백서 내용은 저작권의 보호를 받습니다. 개인적 용도 또는 기타 소유권 고지 사항이 있는 경우에만 백서의 개별 섹션을 다운로드하거나 인쇄할 수 있습니다. ReapChain Inc.의 사전 서면 허가 없이는 본 백서를 전체적으로 또는 부분적으로 복제하거나 전자적 수단 또는 기타 방식으로 복제하거나, 공공 또는 상업적 목적으로 수정, 링크, 사용할 수 없습니다.

투자위험

ReapChain Inc.은 구매자들에게 REAP 구매대금 상당의 손실을 볼 수 있다는 위험을 포함하여 여러가지 종류의 위험을 고지하고 있습니다. 아래에 쓰여진 위험 부담이나 비확실성에 관한 정보의 정확성은 담보되지 않습니다.

구매자들은 REAP의 매매 및 보유로서 명백하게 REAP의 어떠한 형태의 보증도 없는 현재 상태 그대로의 위험 부담을 인지하고 구매한다는 것에 동의한 것으로 간주됩니다.

1. 블록체인 리스크: 블록체인 시스템 혼잡으로 거래가 늦게 처리되거나 거래가 무효화될 수 있습니다. 특히 REAP의 발행과 분배를 담당하는 스마트 계약은 이더리움 블록체인이라는 기술에 기초하고 있습니다. 이더리움 프로토콜은 약점과 취약성을 가지고 있을 수 있으며 REAP이 손실되는 버그를 포함해 각종 버그가 발생할 수 있습니다. 또 이러한 이더리움 블록체인의 문제로 ReapChain Inc. 및 REAP 구매자에게 물질적 피해가 발생할 수 있습니다.

2. 개인정보 리스크: 사용자의 개인정보는 REAP 구매자의 전자 지갑에 있는 REAP의 분배와 통제를 위하여 필요합니다. 따라서, 개인정보가 유출될 경우 구매자의 전자 지갑에 있는 REAP이 유출될 수 있습니다. 더욱이, 구매자의 개인정보 유출로 인해 제3자가 구매자의 전자 지갑을 열람하여 REAP을 훔쳐갈 수도 있습니다.

3. 보안 리스크: 다른 모든 암호 화폐와 마찬가지로 이더리움은 '이중 지불 공격' 혹은 '51% 공격'과 같은 마이닝 공격에 취약합니다. 해커들 혹은 다른 악의적인 의도가 있는 집단들이 위와 같은 공격 방법으로 ReapChain Inc. 또는 REAP을 공격할 수 있으며, 이러한 블록체인 공격이 성공할 경우 REAP 거래와 REAP에 큰 타격을 줄 수 있습니다.

4. 전자지갑 호환성 리스크: REAP을 구입하거나 저장하기 위해서 REAP과 기술적 호환이 되는 전자 지갑을 사용해야 합니다. 만약 다른 지갑을 사용하신다면 구입하신 REAP을 접속하여 보시지 못하실 수 있습니다.

5. 불가항력 리스크: ReapChain은 아직 개발 중에 있으며 ReapChain Inc.는 ReapChain을 백서에 쓰인 내용 그대로 개발 및 유지하도록 노력할 것이나 그 세부사항에서 법률, 디자인, 기술, 행정상 규제 등 여러가지의 이유에서 변화가 생길 수 있습니다. ReapChain Inc.은 규제 프레임이나 요구되는 허가 및 라이선스 및 과세 정책의 변화, ReapChain Inc.이나 ReapChain에 불리한 영향을 끼치는 플랫폼 또는 오픈소스의 등장, 시장의 관심 부족 및 기타 이와 유사한 사태가 발생하는 등 불가항력적인 요인으로 인하여 REAP의 가치 하락이나 손실 및 유동성에 손해가 발생할 경우, 그로 인한 배상책임이 모두 면제됩니다.