



# REAPCHAIN

White Paper

Ver 0.8

# 목차

---

01	초록	1
02	요약	2
03	IoT 시장 개요 및 시장 규모	
3-1.	IoT 개요	4
3-2.	글로벌 시장 규모	4
3-3.	분야별 시장 규모	5
04	Pain Point	
4-1.	IoT 시장의 Pain Point	7
4-2.	기존 블록체인의 한계	9
4-3.	블록체인과 IoT시스템의 융합 문제	10
05	ReapChain Protocol	
5-1.	Overview	11
5-2.	ReapChain Technology	12
5-3.	ReapChain의 구현 체계	20
06	Business Model	
6-1.	ReapChain IoT 적용 가능분야	22
6-2.	ReapChain IoT 적용 예시	24
6-3.	비즈니스 모델	27
07	Ecosystem	
7-1.	ReapChain Ecosystem	29
7-2.	향후 계획	30
08	Roadmap	31
09	Token Economy	
9-1.	Token Economy	32
9-2.	Token Allocation	34
10	Team	36
11	Partner	37
12	참고문헌	38
13	Disclaimer	39

# Glossary

---

- **ReapChain BaaS:** BaaS (Blockchain as a Service)는 블록체인 기반 소프트웨어의 개발 환경을 제공하는 클라우드 컴퓨팅 플랫폼이며, 서비스형 블록체인을 의미합니다. ReapChain BaaS는 기기들을 연결하고 인증하는 Reap SDK와 데이터 처리 및 저장을 담당하는 ReapMiddleChain 및 ReapChain, 전체 서비스를 운영 및 관리하기 위한 Reap Platform으로 구성되어 있습니다.
- **탈중앙화 신원증명 (DID, Decentralized Identity):** 기존 신원확인 방식과 달리 중앙 시스템에 의해 통제되지 않으며 블록체인 기술을 기반으로 개개인이 자신의 정보에 완전한 통제권을 갖도록 하는 기술입니다.
- **사물 PID (Private ID):** ReapChain은 개인 (사람)에 한정되어 적용되던 DID (Decentralized ID)기술을 ReapChain만의 독자적인 암호화 기술을 Reap SDK를 통해 개개의 사물 (디바이스)에 적용하여, 새로운 사물 인증 체계인 PID (Private ID)를 구현합니다. 사물 PID는 고유 ID (프라이빗 키) 발급을 통해 비인증된 사용자가 개별 기기의 ID를 볼 수 없도록 하는 '인비저블 ID (Invisible ID)' 기술과 ReapChain에 의해 이중 검증을 받은 송신자만이 IoT 단말과 통신 가능하도록 하는 '상호 검증' 기술을 통해 이루어집니다.
- **Shell-Core Structure:** 퍼블릭 블록체인과 프라이빗 블록체인이 완벽히 융합된 새로운 형태의 이중 블록체인 구조입니다. Shell-Core Structure는 두 겹의 체인을 가지며, 외곽에서는 ReapMiddleChain에 의해 Cell 블록을 형성하고 내부에서는 합의 알고리즘에 의해 ReapChain을 형성하는 이중 구조로 설계됩니다.
- **Reap SDK:** SDK는 Software Development kit란 의미이며, Reap SDK는 IoT 산업의 다양한 개별 기기들의 (칩, 모듈, 태그 등) 전용 소프트웨어 개발 도구입니다. Reap SDK는 ReapChain Enabled SDK란 의미를 포함하고 있습니다.
- **ReapMiddleChain:** Shell-Core Structure에서 프라이빗 블록체인의 역할을 하는 외곽을 형성하며, 기존 블록체인에서 처리하기 힘든 밀리초(1/100초) 단위의 짧은 간격으로 발생하는 시계열 데이터를 분산 처리할 수 있습니다.
- **Reap Platform:** 다양한 응용 및 보안 서비스의 용이한 생성과 실행을 지원하는 플랫폼으로, IoT 서비스 배포를 지원하는 애플리케이션을 의미합니다. 서비스를 운영 및 관리할 수 있는 플랫폼이자, 데이터 스토어로서 거래가 이루어지는 공간을 나타냅니다.
- **양원제 합의 알고리즘 (PoDC, Proof of Double Committee):** 기존 합의 알고리즘인 DPoS (Delegated PoS) 방식과 PBFT (Practical Byzantine Fault Tolerance) 방식을 개선한 ReapChain만의 신규 합의 알고리즘이며, 상시 운영되는 14개의 상임위 노드와 쿼텀난수를 통해 선정된 15개의 운영위 노드, 총 29개의 노드가 블록 생성을 위한 합의 과정에 참여합니다.
- **QSN (Quantum Safety Net):** ReapChain Main Net 내부에 쿼텀난수 생성기가 포함된 신뢰성 높은 내부 네트워크를 의미합니다.
- **쿼텀난수 생성기 (QRNG; Quantum Random Number Generators):** ReapChain은 방사성 동위원소에서 방출하는 알파입자 기반의 양자물리 법칙을 적용된 난수 발생기로 인간이 예측 불가능한 난수를 생성 가능합니다.

- **Signed Message:** IoT 기기에 개별적으로 생성되는 고유 ID(프라이빗키)와 Reap SDK에서 구현된 독자적인 암호화 기법을 통해 생성되는 보안성 높은 암호화 메시지입니다.
- **WORM (Write Once Read Many) 스토리지:** WORM 스토리지는 Read-only 저장 매체인 광-디스크처럼 한번 기록하면 데이터를 훼손할 수 없는 특성을 가지며, 데이터에 대한 접근 및 위변조가 불가능한 비가역성 스토리지를 의미합니다.
- **Reap HUT:** ReapChain BaaS로 전달되는 Raw 데이터 중에서 필수 데이터를 분류하고, 이를 Cell 블록화하여 ReapChain으로 전송하기 위한 엣지 컴퓨팅의 분산 처리 및 저장 기능을 담당하는 프라이빗한 임시 데이터 베이스를 의미합니다.
- **AES-128:** 고급 암호화 표준(Advanced Encryption Standard, AES)는 암호화와 복호화 과정에서 동일한 키를 사용하는 대칭 키 알고리즘으로 AES-128은 암호화 키에 대한 길이가 128 bit 인 암호화 구조를 의미합니다.
- **SHA-256:** SHA(Secure Hash Algorithm)는 해시 알고리즘의 한 종류로 어떤 길이의 값을 입력하더라도 256 bit 길이로 구성된 64자리의 값을 출력하며, 입력되는 값이 조금만 변동되어도 출력되는 값이 완전히 달라지기 때문에 출력 결과로 입력되는 값을 추적하는 것이 불가능한 알고리즘입니다.
- **웨어러블:** 정보통신 기술이 접목된 기기를 사용자의 손목, 팔, 다리, 머리 등 몸에 지니고 다닐 수 있는 기기로 만드는 기술로 플렉서블 디스플레이, 소형 스마트 센서, 저전력 무선 통신, 모바일 기기 등의 기술이 몸에 착용 가능한 시계, 안경, 의류, 모자 등에 접목되어 어디서나 사용 가능한 장치입니다.
- **커넥티드 카:** 다른 차량이나 교통 및 통신 인프라, 보행자 단말과 실시간으로 통신하는 것으로 정보통신 기술과 자동차를 연결시켜 양방향 소통이 가능하게 하며, 운전자의 편의와 교통 안전에 기여되며 인터넷의 다양한 서비스를 제공하는 것입니다.
- **머클 트리 (Merkle Tree):** 데이터의 간편하고 확실한 인증을 위해 SHA-256 기반의 암호화 기술을 통해 복호화되지 않는 단방향 암호화 방법입니다.
- **인포테인먼트:** 정보를 의미하는 인포메이션 (Information)과 오락거리와 인간친화적인 기능을 의미하는 엔터테인먼트 (Entertainment)의 통합 시스템입니다.

# 01. 초록

---

## 1-1. 초록

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 블록체인의 암호화 기술이 유용하게 사용될 것으로 기대 됩니다

- 미션

ReapChain은 IoT 산업의 End-to-End 구간 전체를 블록체인화 하여 보다 안전하고 투명한 블록체인 기반 IoT 생태계를 구현합니다.

- 목표

ReapChain Protocol을 활용한 IoT 융합 플랫폼 구축

- ReapChain만의 새로운 하이브리드 블록체인 구현
- ReapMiddleChain을 통한 데이터의 대용량 처리 구현
- 사물 PID를 통한 IoT 디바이스 인증 및 데이터 보안성 확보

IoT 산업에서 보안, 인증, 안전 등의 이슈는 중재자에게 의존하는 방식으로 해결해 왔으나, 이러한 중앙 집중형 방식은 비용과 보안 및 신뢰 측면에서 여러 가지 부작용을 내포하고 있습니다.

ReapChain은 신규 합의 알고리즘을 통해 현존하는 블록체인의 문제점을 해결할 수 있는 새로운 하이브리드 블록체인을 제시하고, ReapMiddleChain을 통해 IoT 산업에서 발생하는 대용량 데이터의 분산 처리를 실현합니다.

그리고 사물 PID를 기반으로 개별기기 인증 및 데이터의 위변조를 방지하여, 기존 IoT 시스템을 개선하고자 합니다.

ReapChain의 기술력은 ReapChain BaaS 형태로 제공되며, ReapChain의 기술력을 통해 투명성과 보안성이 강화된 IoT 특화 플랫폼을 구축하여 안전하고 투명한 블록체인 생태계를 조성하고자 합니다.

## 02. 요약

### 2-1. 요약

ReapChain은 Shell-Core Structure의 하이브리드 블록체인으로 기존 블록체인이 가진 트릴레마(Trilemma) 문제를 해결하고, 사물 PID와 ReapMiddleChain의 분산화된 스토리지 서비스를 기반으로 기존 IoT 시장의 문제점을 해결하여 블록체인과 IoT 산업의 융합을 구현하고자 합니다.

#### 하이브리드 블록체인 (Shell-Core Structure)

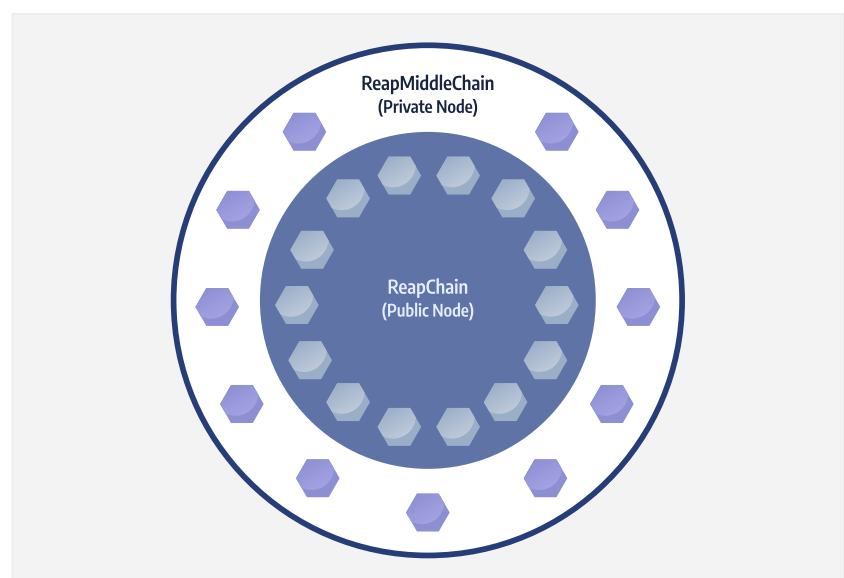
최근 프라이빗 블록체인과 퍼블릭 블록체인 기술을 융합한 하이브리드 블록체인이 다양하게 개발되고 있습니다. 하지만 기존 블록체인이 가진 트릴레마 문제를 해결하고 실생활에서 온전하게 사용할 수 있는 하이브리드 블록체인은 아직까지 등장하지 못했습니다.

ReapChain은 현존하는 블록체인의 문제점에 대한 해결방법으로 Shell-Core Structure의 하이브리드 블록체인을 제시합니다.

Shell-Core Structure는 신규 합의 알고리즘인 양원제 합의 알고리즘을 기반으로 구현되며, 퍼블릭 블록체인과 프라이빗 블록체인이 완벽히 융합된 새로운 형태의 이중 블록체인 구조입니다.

Shell-Core Structure는 속도가 빠른 프라이빗 블록체인을 외곽에 배치하여 시간상으로 먼저 처리하고 보안성과 탈중앙화에 강한 퍼블릭 블록체인은 안쪽에 배치하여 후 처리하는 방식인 립체인만의 독특한 트랜잭션 처리 구조입니다.

<그림 1> Shell-Core Structure 구성도

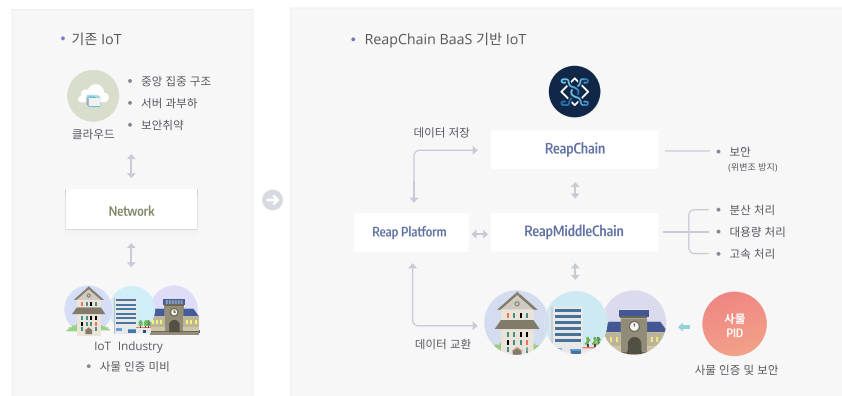


## 2-1. 요약

### ReapChain BaaS (Blockchain as a Service)

ReapChain은 IoT 시장의 문제점을 해결하기 위해, 블록체인 기반 사물 기기의 PID를 구현하여 개별 기기를 인증하고 데이터 위변조를 방지하고자 합니다. 또한 ReapMiddleChain의 분산화된 데이터 처리 기술을 통해 효과적인 데이터 저장 및 관리 서비스를 제공합니다. 또한 ReapChain의 기술을 BaaS 형태로 제공하여, 블록체인과 IoT 산업을 융합하고, 기존 IoT 시스템을 개선합니다.

<그림 2> 기존 IoT와 ReapChain BaaS기반 IoT 비교



- ReapMiddleChain을 통한 대용량 데이터의 분산 처리 및 저장
- 사물 PID 를 통한 기기 인증 및 데이터 위변조 방지

ReapChain BaaS는 기기들을 연결하고 인증하는 Reap SDK, 데이터 처리 및 저장을 담당하는 ReapMiddleChain과 ReapChain, 전체 서비스를 운영 및 관리하기 위한 Reap Platform으로 구성되어 있습니다

# 03. IoT 시장

## 3-1. IoT 개요

IoT(Internet of Things) : 사물인터넷

IoT 기술은 센서와 통신 기능을 내장한 사물에 인터넷을 연결하고, 발생한 데이터를 획득, 처리하여 사용자에게 제공하는 기술입니다.

IoT는 이동통신망을 이용하여 사람과 사물, 사물과 사물간 지능통신을 할 수 있는 M2M(Machine to Machine)의 개념을 인터넷으로 확장한 것으로 사물은 물론, 현실과 가상세계의 모든 정보와 상호작용하는 방향으로 발전하고 있습니다.

IoT 산업의 3대 핵심 요소는 센서와, 네트워크, 플랫폼 기술입니다.

<표 1> IoT 3대 핵심요소

센서	네트워크	플랫폼
<ul style="list-style-type: none"><li>• 각종 스마트 센서</li><li>• IoT 디바이스</li><li>• 예) 온도, 습도, 이미지, 가스, 헬스케어센서, 분광센서 등</li></ul> <p>다양한 센서를 이용하여 원격감지, 위치 및 모션 추적 등을 통해 사물과 주위 환경으로부터 정보를 획득하는 기능</p>	<ul style="list-style-type: none"><li>• 무선 네트워크</li><li>• 사물 인터넷 프로토콜</li><li>• 예) Beacon, RFID, NFC, Bluetooth, ZigBee 등</li></ul> <p>사람·사물·서비스를 연결할 수 있는 유·무선 네트워크를 의미</p>	<ul style="list-style-type: none"><li>• 하드웨어 플랫폼</li><li>• 네트워크 게이트웨이 플랫폼</li><li>• 예) 아두이노, 라즈베리파이</li></ul> <p>정보의 센싱, 가공, 추출, 처리, 저장, 판단 기능을 의미하는 검출 정보 기반 기술과 위치 정보 기반기술, 보안 기술,데이터 마이닝 기술, 웹 서비스 기술 등으로 구성</p>

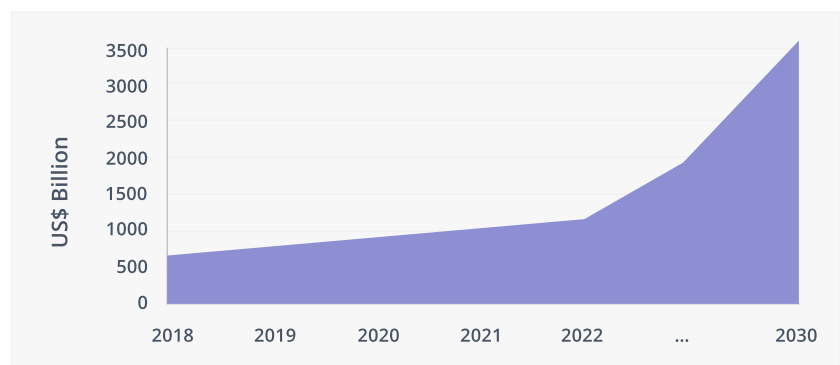
## 3-2. 세계시장규모

2030년 글로벌 IoT 시장 규모:  
3조 1,277억 달러

IoT 전용망, 5G 등 통신 기술의 발달 및 인프라 저변 확대로 인해 IoT 시장의 성장이 더욱 가속화되고 있습니다.

글로벌 IoT 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.

<그림 3> 글로벌 IoT 전체 시장 규모





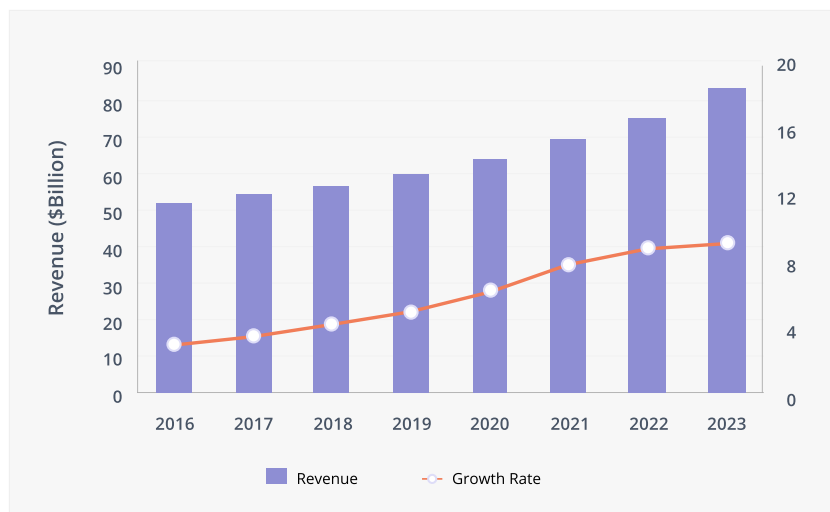
### 3-3. 분야별 시장규모

2030년 IoT 임베디드 시장 규모:  
1,326억 달러

#### IoT 임베디드 시스템 시장

IoT는 시스템이라는 범주로 판매되고 있으며, 컨설팅 및 설치 서비스까지 통합적으로 제공됩니다. 글로벌 IoT 시스템 구축 및 프로젝트를 주도하고 있는 IoT 임베디드 시스템 시장은 수십억 달러 규모로 전 세계적으로 확대되고 있습니다.

<그림 4> IoT 임베디드 시스템 시장



<출처: Forest and Sullivan (2018년)>

IoT 임베디드 시스템은 2023년까지 전 세계적으로 300억 개 이상의 연결된 장치가 활용될 것으로 예측되며, 그 규모는 2023년에는 838억 6천만 달러에 이를 것입니다. IoT 임베디드 시스템 시장은 연평균 7.1%의 꾸준한 성장세를 보이며 2030년에는 1,326억 달러 규모로 성장할 것입니다.

2030년 IoT 플랫폼 시장 규모:  
616억 달러

#### IoT 플랫폼 시장

IoT 서비스는 모두 플랫폼을 기반으로 연동되어 작동하고 있습니다.

IoT 플랫폼은 디바이스 플랫폼, 네트워크 플랫폼, 서비스 플랫폼, 데이터 분석 플랫폼으로 구분할 수 있으며, 전 세계는 이미 IoT 플랫폼 장악을 위한 경쟁이 본격화되고 있습니다.

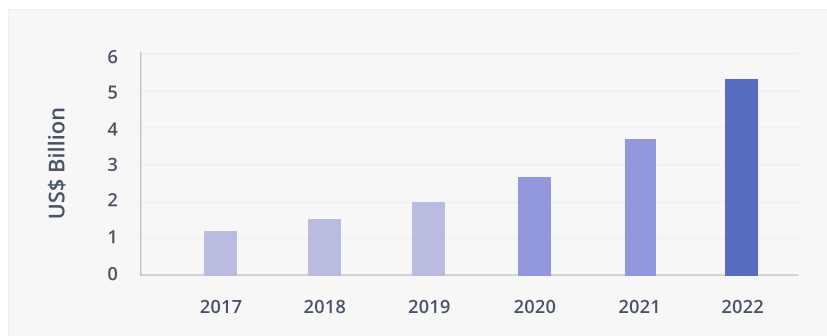
### 3-3. 분야별 시장규모

**디바이스 플랫폼:** 디바이스가 제공하는 하드웨어 자원과 이러한 하드웨어 자원을 이용하는 플랫폼으로, 운영체제(OS), 센서와 소프트웨어 등을 포함한 오픈소스 하드웨어, 하드웨어와 연동되는 센서 및 구동기 등을 포함

**서비스 플랫폼:** 다양한 응용 서비스의 용이한 생성 및 실행을 지원하는 플랫폼으로, IoT 서비스 배포를 지원하는 애플리케이션 구현 및 유통 플랫폼

2030년 IoT 보안 시장 규모:  
**279억 달러**

<그림 5> 글로벌 IoT 플랫폼 시장 중 디바이스 및 서비스 플랫폼 시장 규모



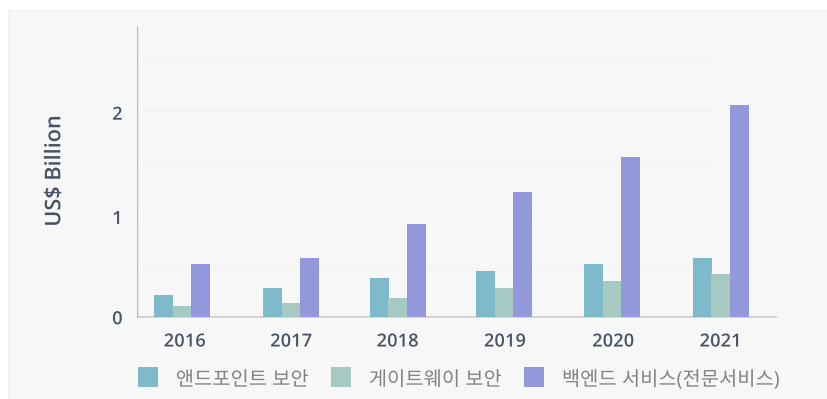
< 출처: Berg Insight (2018) >

유럽의 IoT 전문 분석 기관인 베르그 인사이트(Berg Insight)가 지난 2018년 발표한 자료에 의하면, 세계 IoT 플랫폼 시장 중에서도, 2017년 IoT 디바이스 및 서비스 플랫폼의 세계 시장 규모는 약 11억 달러에 달하는 것으로 나타났으며, 연평균 36.2%의 고속 성장을 거듭해 2030년에는 약 616억 달러에 달하는 거대한 시장이 될 것입니다.

#### IoT 보안 시장

IoT 시스템을 타겟으로 한 사이버 공격이 현실화되고 있고 그 피해가 커져가면서 IoT 분야가 발전할수록 IoT 보안 시장도 동시에 성장하고 있습니다.

<그림 6> 글로벌 IoT 보안지출



< 출처: 가트너(2018년 3월) >

시장조사 기관인 가트너의 조사에 의하면, 세계 약 20%의 기업이 지난 3년 이내 최소 한 차례 이상의 IoT 기반 공격을 경험했다고 나타났습니다.

2018년 기업 IoT 총 보안 지출 규모는 15억 달러를 기록했으며, 연평균 27.9%의 높은 성장률을 보이면서 2021년에는 31억 달러, 2030년에는 279억 달러 규모에 이를 것입니다.

# 04. Pain Point

## 4-1. 기존 IoT 시장의 Pain Point

“데이터 트래픽 폭증에 따른 대용량 데이터 처리 문제”

사물 자체 메모리에서 사물의 다양한 정보를 모두 저장하고 관리하기에는 어렵기 때문에, 별도의 서버 기반 저장 시스템을 통해 관리되고 연결된 모든 사물은 중앙 서버에 의해 제어되는 구조입니다.

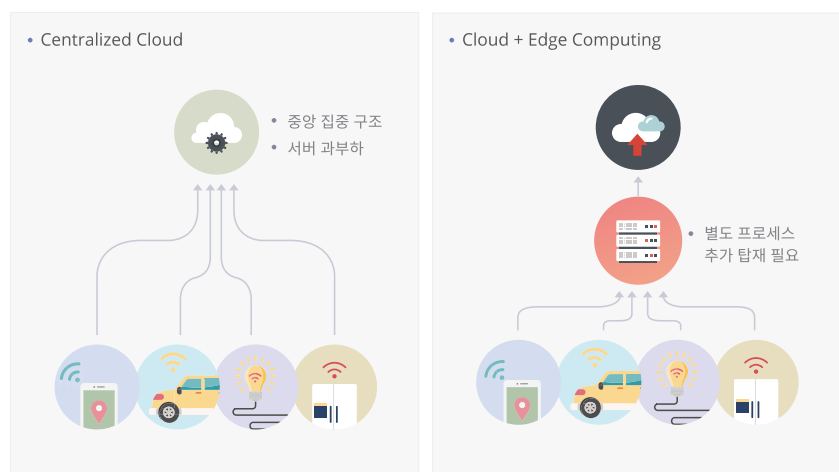
### 중앙 집중형 아키텍처의 대용량 데이터 처리 문제

IoT 서비스가 시작되면서 네트워크에 연결된 사물은 급격히 늘어나는 추세이며, 사물 수의 증가는 데이터 트래픽의 증가로 이어질 수밖에 없습니다. 특히, 웨어러블이나 커넥티드카 개념이 등장하면서 향후에는 인포테인먼트(Information+Entertainment) 측면에서 데이터 트래픽 폭증이 예상되고 있습니다.

대부분의 기업들은 클라우드 서비스 사업자에게 컴퓨팅 자원을 임대 받은 후 사물인터넷 기기를 관리하고 있습니다. 그러나 기존 클라우드 시스템은 중앙 집중 서버가 모든 데이터를 처리함에 따라 IoT 환경에서 폭증하는 데이터를 처리하기에는 비효율적이며, IoT 서비스 전체의 속도 및 품질 저하를 발생시키게 됩니다.

최근 트래픽 부담을 줄이고 서비스 지연을 줄이기 위해, 분산된 소형 서버를 기반으로 실시간 데이터를 처리하기 위한 ‘엣지 컴퓨팅’ 기술도 사용하고 있습니다. 하지만 엣지 컴퓨팅은 연산처리를 담당할 별도의 프로세스가 추가로 탑재되어야 하기 때문에 설비 유지나 시스템 구성에 있어 어려움이 존재합니다.

<그림 7> IoT 산업 - 데이터 저장 방식의 변화



## 4-1. 기존 IoT 시장의 Pain Point

### “IoT 산업의 취약한 보안 문제”

IoT 산업에서는 네트워크 카메라, 방송·통신 단말기, 인터넷 전화기 등 다양한 사물이 정보 제공 주체로 등장함에 따라 해당 기기에 대한 식별이 필요합니다.

### IoT 사물의 해킹 및 비인가된 기기 접근으로 인한 문제

IoT에 연결되는 사물들은 자신을 구별할 수 있는 개별 ID를 가지고 네트워크로 연결되어야 합니다.

현재 IoT 산업에서는 다양한 사물이 정보제공 주체로 등장하고 있지만, 개별 사물에 대한 신뢰성 있는 ID 인증 및 데이터 검증 체계가 없는 상황입니다.

IoT 환경에서는 <그림 8>과 같이 다양한 장치들이 연결되어 있는 구조적 특성을 가지기 때문에 기존 시스템에서 사용되던 암호화 알고리즘을 사용하기 어려워 Malware, DDoS 등의 공격에 취약합니다.

다양한 IoT 사물 공격 사례가 빈번하게 등장하고 있으며, 해킹된 사물은 사용자 계정 정보, 각종 패스워드 등 중요 데이터가 유출되어 악성코드와 스팸을 퍼뜨리는 유포지로 활용될 가능성이 높습니다. 해킹된 기기의 위변조된 데이터는 검증 및 보안이 불가능하기 때문에 잘못된 데이터 전송에 따른 전체 시스템의 오작동 등 다양한 부작용이 발생하게 됩니다.

따라서, IoT 사물에 대한 인증이나 데이터 보안 체계 미 확립 시 IT 서비스 전반의 위협이 발생할 수 있습니다.

<그림 8> IoT 환경에서의 보안 위협



## 4-2. 기존 블록체인의 한계

"블록체인의 트릴레마 문제와 기존 합의 알고리즘의 단점"

트릴레마 (Trilemma) 문제:

현재 블록체인 기술은 탈중앙화(Decentralization), 확장성(Scalability), 보안성(Security)의 문제를 동시에 해결하는 것이 어렵습니다.

### 트릴레마 (Trilemma) 문제

프라이빗 블록체인은 보안성이 강하고 속도가 상대적으로 빠른 장점을 가지고 있지만, 관리주체가 중앙화가 되는 단점을 가지고 있습니다.

반면에 퍼블릭 블록체인은 탈중앙화의 장점을 가지고 있지만 느린 처리속도와 확장성이 단점으로 지적이 되고 있어 실사용 부분에서 많은 문제점을 가지고 있습니다.

### 기존 합의알고리즘의 한계

기존 합의 알고리즘인 PoW(Proof of Work)와 PoS(Proof of Stake), DPoS(Delegated Proof of Stake)와 BFT(Byzantine Fault Tolerance)는 에너지 소모적인 하드웨어 연산 구조나 한정된 위임자에 의한 중앙화, 51% 외부 공격에 취약한 구조 등 한계를 가지고 있습니다.

<표 2> 기존 합의 알고리즘 비교

합의 알고리즘	단점
PoW (Proof of Work)	에너지 소모적인 하드웨어 연산에 의존하고, 연산결과를 구성하여 중앙화 됨
PoS (Proof of Stake)	특정 우월 지분의 독점과 보상을 위해 포크가 일어나더라도 모든 블록에 지분을 증명하는 Nothing at stake 문제 개선 필요
DPoS (Delegated Pos)	일부 최상위 지분 보유 노드에 대한 외부 공격에 취약하고, 한정된 위임자에 의한 중앙화
PBFT (Practical BFT)	모든 노드의 합의 참여로 인하여 참여 노드 수의 제곱에 비례하는 메시지 통신량으로 인해 합의 속도 지연
Tendermint (DPoS + PBFT)	리더가 정해져 있어 외부 공격에 취약

### 4-3. 블록체인과 IoT시스템 의 융합 문제

퍼블릭 블록체인의 경우 데이터 트랜잭션 발생 시, 제한된 스토리지와 낮은 처리 속도로 인해 실용적인 IoT 시스템 적용에 어려움이 있습니다.

프라이빗 블록체인 기반의 IoT 시스템은 블록체인 네트워크에 참여할 수 있는 권한 제한을 통해 개방형 블록체인 대비 높은 처리 속도와 확장성을 일부 보장 가능하지만, 탈중앙화가 이루어지지 않아 데이터의 무결성을 보장할 수 없습니다.

기존 블록체인들은 IoT 산업과의 융합을 위해 기존 블록체인의 단점을 보완하고 높은 처리속도와 확장성을 확보하기 위한 다양한 방법을 모색하고 있지만, 기기 보안이나 탈중앙화와 관련된 문제를 해결하지는 못했습니다.

IoT 기반 데이터의 교환 및 검증을 위해서는 IoT 디바이스가 블록체인의 노드로 참여하거나 IoT 디바이스에 내장되어 있는 MCU에 블록체인 데이터를 포함하는 방법이 있으나, 현실적으로 기술 개발 수준이 미비한 상황입니다.

# 05. ReapChain Protocol

---

## 5-1. Overview

ReapChain은 앞서 제시한 블록체인의 한계를 극복하고, IoT 기반의 대용량 데이터의 처리 문제와 비 인가된 사물로 인한 보안상의 취약점을 해결하기 위해 다음과 같은 솔루션을 제시하고자 합니다.

ReapChain은 새로운 하이브리드 블록체인을 구현함으로써, 기존 블록체인의 한계인 트릴레마 문제를 해결하고, ReapChain BaaS를 활용하여 IoT 시스템과의 효과적인 융합을 가능하게 합니다.

ReapChain BaaS를 통해 구축된 IoT 시스템은 비 인가된 사물로부터의 예측 불가능한 트랜잭션을 차단할 수 있고, 대용량 트랜잭션도 유연하고 효율적으로 처리할 수 있습니다.

### Shell-Core Structure

ReapChain은 퍼블릭과 프라이빗 블록체인을 융합한 Shell-Core Structure를 통해 외부에는 3자 합의 알고리즘(Proof of triple Confirmation)의 프라이빗 블록체인(ReapMiddleChain)이 구성되고 내부에는 양원제 합의 알고리즘(PoDC, Proof of Double Committee)의 퍼블릭 블록체인(ReapChain)을 구성하여 기존 블록체인의 한계인 '확장성, 보안성, 탈중앙화'의 3가지 문제를 동시에 해결하고 IoT 시스템과의 효과적인 융합을 가능하게 합니다.

### 사물 PID (Private ID)

개별 IoT 디바이스는 Reap SDK를 통해 각 기기마다 고유의 ID인 프라이빗 키를 획득하여 불법적인 해킹이나 접근을 방지합니다.

Reap SDK가 적용된 IoT 디바이스에서는 트랜잭션 발생 시, 권한이 허가된 인원 또는 기기로부터만 접근이 가능하며 데이터의 위/변조 여부에 대한 확인이 가능하게 됩니다. 이를 통해 잘못된 데이터 전송에 따른 관리 시스템의 오작동이나 부작용을 방지할 수 있습니다.

## 5-2. ReapChain Technology

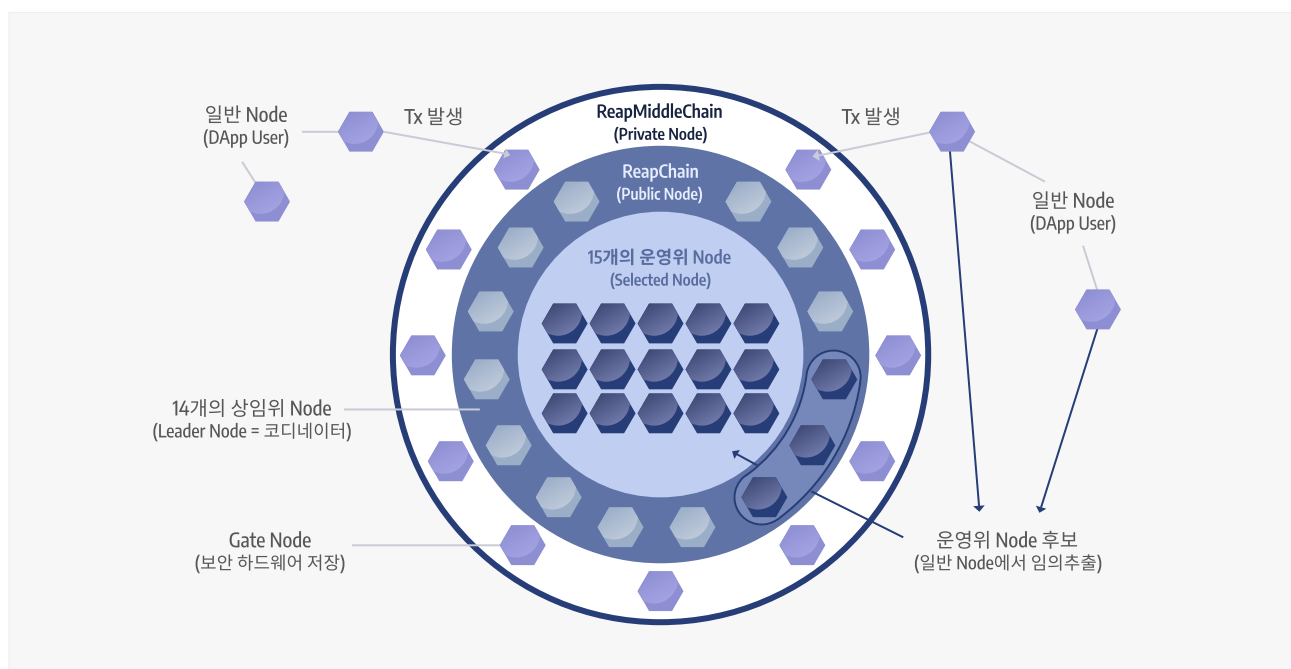
### Shell-Core Structure

퍼블릭과 프라이빗 블록체인이 완벽히 융합된 Shell-Core Structure와 PoDC합의 알고리즘을 통해 새로운 하이브리드 블록체인을 구현하여 기존 블록체인의 트릴레마 문제를 해결합니다.

Shell-Core Structure는 두 겹의 체인을 가지며, 외곽에서는 ReapMiddleChain에 의해 가원장 개념의 Cell 블록을 형성하고, 내부에서는 진원장 개념의 확정블록을 형성하는 이중 구조로 설계됩니다.

Shell-Core Structure는 <그림 9>과 같이 속도가 빠른 프라이빗 블록체인을 외곽에 배치하여 가원장 개념으로 트랜잭션을 먼저 처리하고, 보안성과 탈중앙화가 강한 퍼블릭 블록체인은 안쪽에 배치하여 진원장 개념으로 후 처리하는 블록체인의 새로운 구조입니다.

<그림 9> Shell-Core Structure = 퍼블릭 + 프라이빗 블록체인



#### ① PoDC (Proof of Double Committee) 합의 알고리즘

진원장인 ReapChain은 신규 합의 알고리즘인 양원제 합의알고리즘(PoDC)를 기반으로 구현됩니다.

#### 양원제 구성을 통한 탈중앙화 구현

ReapChain은 상시 운영되는 14개의 상임위 노드와 15개의 운영위 노드(운영위후보 노드 중에서 보안에 강한 키템 난수를 활용한 방식으로 선택된 15개의 노드)로 구성되며, 총 29개의 노드가 블록 생성을 위한 합의 과정에 참여합니다.



ReapChain에서는 노드의 수가 늘어나더라도 합의 과정에는 매번 키템 난수로 선정된 29개의 노드(상임위 : 14개, 운영위 : 15개)만 참여하며, 합의에 참여하는 노드 중에서 운영위 노드가 참여하는 비율은 항상 51% 이상 유지되어 탈중앙화를 구현합니다. 상시 운영되는 상임위 노드 또한 투표를 통해 변경 가능하기 때문에 전체 노드가 투명하게 운용되어 집니다.

<표 3> ReapChain Node의 종류 및 권한

권한	Q-Manager	거버넌스 노드	상임위원회 노드	운영위원회 노드	일반 노드
노드 관리	X	○	X	X	X
블록생성 권한	X	X	○	X	X
합의 참여	X	X	○	○	X
트랜잭션 처리	X	X	○	○	○
블록 검사	X	X	○	○	○

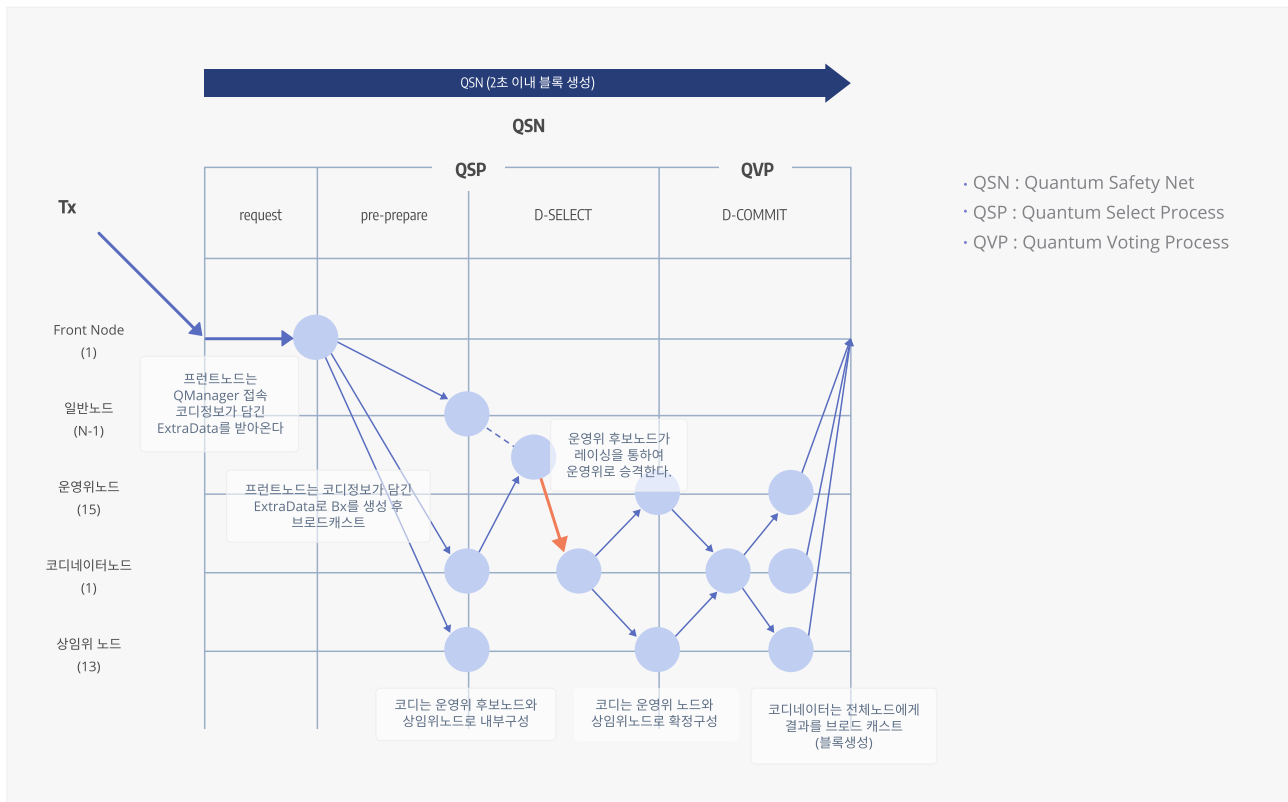
- **Q-Manager:** 키템 난수를 생성 및 관리하고, 거버넌스에서 제공받은 노드 정보를 활용하여 키템 난수로 코디네이터 및 운영위원회 후보군 선정 과정을 지원함.
- **거버넌스 노드:** 수수료, 배당 정책과 랜덤 일반 노드 선발 정책 그리고 모든 종류의 노드 관리 정책 기능 등이 포함된 특수한 노드임.
- **상임위원회 노드:** ReapChain에서 상시 운영되는 노드로서, 합의 과정에 참여하여 블록 생성 권한을 가지고 있음.  
(상임위원회 조건 : 총발행량 2% [ 9800만 REAP ] staking)
- **운영위원회 노드:** 운영위원회 후보 노드 중 키템 난수를 이용한 랜덤 선정 방식으로 선정된 노드로서, 합의 과정에 참여하여 트랜잭션 검증을 진행함.  
(운영위원회후보조건 : 10만 REAP staking)
- **일반 노드:** 누구나 설치할 수 있는 노드로서, 운영위원회 후보 노드에 선택적으로 참여할 수 있음.

### 확장성이 강화된 합의 프로세스 구조

ReapChain은 상시 운영되는 상임위원회 노드 중에서 코디네이터를 선정합니다. 선정된 코디네이터를 중심으로 나머지 28개의 노드 간 직접 통신을 통해 최소의 네트워크 트래픽으로 합의에 도달함에 따라 블록 생성 주기는 2초에 불과합니다.

ReapChain의 내부 네트워크인 QSN (Quantum Safety Net)에서는 하기 그림과 같이 코디네이터를 통해 메시지가 한 번만 발생합니다. 코디네이터는 오직 하나의 블록 생성자(Block Producer)가 되어 블록을 생성하며, 2초 이내에 블록이 생성되지 못한 경우에는 해당 주기의 블록생성은 건너뛰게 됩니다. 코디네이터는 복수개의 추가 코디네이터 후보를 선정함으로써 순간적인 장애가 발생한 경우에도 합의를 빠르게 진행할 수 있습니다.

&lt;그림 10&gt; ReapChain 합의 및 블록생성 프로세스



ReapChain은 <그림 10>의 과정을 통해 일반적인 P2P 네트워크에서 broadcast 및 확인 메시지를 모으는 과정에서 발생하는 시간 지연과 네트워크 부하를 줄일 수 있습니다.

### 퀀텀 난수를 활용한 보안성 강화 (51% 공격 방어)

ReapChain은 상임위원회의 코디네이터 선정 및 운영위원회 후보중에 운영위원회 선출을 공정하게 결정하는데 있어 퀀텀 난수를 이용합니다.

ReapChain은 방사성 동위원소에서 방출하는 알파입자 기반의 양자물리 법칙을 적용한 퀀텀난수 생성기 (QRNG; Quantum Random Number Generators)를 통해 예측할 수 없는 방식으로 난수가 생성되기 때문에 선정된 15개의 운영위 노드는 51% 외부 공격에 안전합니다.

Q-manager는 퀀텀 난수를 이용하여 운영위원회 후보 결정을 위한 후보군을 제공하지만 실제 후보가 되는 것이 어떤 노드인지 퀀텀 난수를 발생시킨 Q-manager에서는 알 수 없습니다. 실제 운영위원회 결정은 블록체인 네트워크 상에서 후보군의 레이싱을 통하여 결정되므로 무결성을 보장하고 있습니다.

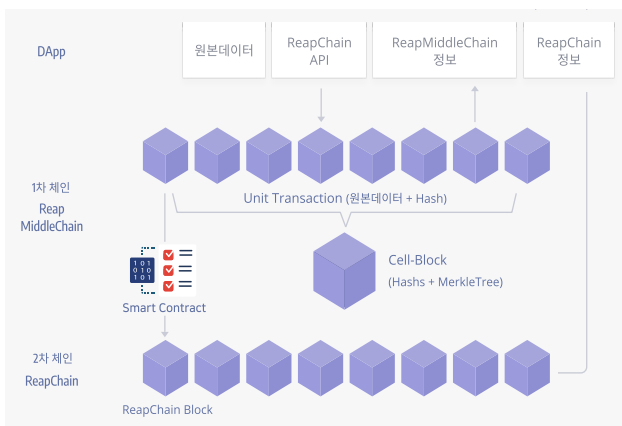
## ② ReapMiddleChain

ReapMiddleChain에서는 IoT 사물에서 발생하는 연속적인 트랜잭션을 시계열 순서대로 블록화하는 분산 처리(Cell 블록) 프로세싱과 WORM 스토리지를 이용하여 대용량 데이터를 효과적으로 처리할 수 있습니다.

또한 가원장 개념으로 트랜잭션이 발생하면 3자 합의를 통해 프리컨펌을 제공함으로써 IoT 사물에 빠른 응답을 제공하며 사전 트래픽을 조정하여 2초마다 생성되는 진원장인 ReapChain의 메인넷 블록처리의 부하를 조정할 수 있습니다.

### ReapMiddleChain의 Cell 블록 프로세싱

<그림 11> Cell 블록 Processing



ReapMiddleChain은 기존 블록체인에서 처리하기 힘든 밀리초(1/100초) 단위의 짧은 간격으로 발생하는 시계열 데이터를 Cell 블록이라는 미니 블록 형태로 분산 처리하여 속도를 극대화합니다. 이후 압축된 블록들을 ReapChain으로 전송하여 최종 블록화를 완성합니다.

기본적으로 트랜잭션은 국제표준 XML 구조를 활용하기 때문에 XML parsing 과정을 통해 프로토콜의 내용 검증과 숫자의 정합성을 확인합니다.

### 3자 검증(Triple Confirmation)을 통한 데이터 처리속도 향상

<그림 12> 데이터 검증 및 초고속 합의 프로세스



<그림 12>과 같이 ReapMiddleChain에서는 데이터 수신자 및 발신자 쌍방에 대한 디바이스를 상호 확인하는 이중 검증(Double Confirmation) 과정을 통해 디바이스 자체의 신뢰성을 확보하며, 목격자(Witness)를 증인으로 하는 공증 과정을 포함한 3자 합의 과정을 동시에 완료함으로써 빠른 데이터 처리가 가능합니다.

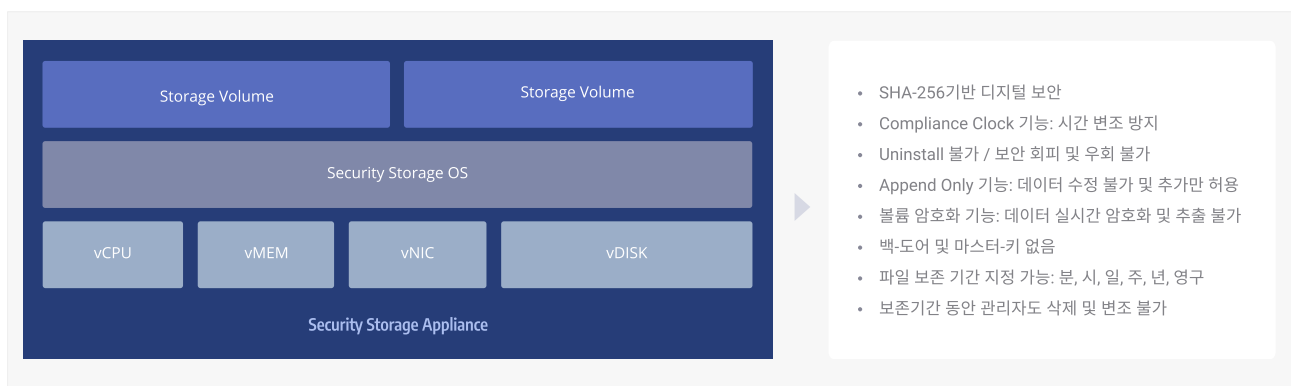
### WORM (Write Once Read Many) 스토리지를 활용한 보안 향상

ReapMiddleChain은 원천데이터, 트랜잭션 Cell 블록을 관리하고 ReapChain을 통해 최종 블록화를 진행합니다. 이 과정에서 발생하는 모든 데이터는 비가역성인 WORM 스토리지에 기록되어 데이터에 대한 접근 및 위변조가 불가능합니다.

기존에 사용되고 있는 일반적인 스토리지의 문제점은 작성자, 관리자 등 권한을 가진 사용자가 데이터를 삭제하거나 변조하는 것을 근본적으로 막을 수 없다는 점입니다.

WORM (Write-Once Read-Many) 스토리지는 Read-only 저장 매체인 광-디스크처럼 한번 기록하면 데이터를 훼손할 수 없는 특성을 가진 비가역성 스토리지를 말합니다.

<그림 13> WORM 스토리지 구조 및 주요 기능



ReapMiddleChain은 <그림13>와 같이 ReapChain만의 WORM 스토리지 기술을 적용하여, 블록체인에 특화된 비가역성 스토리지에 데이터를 저장합니다.

ReapMiddleChain의 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.

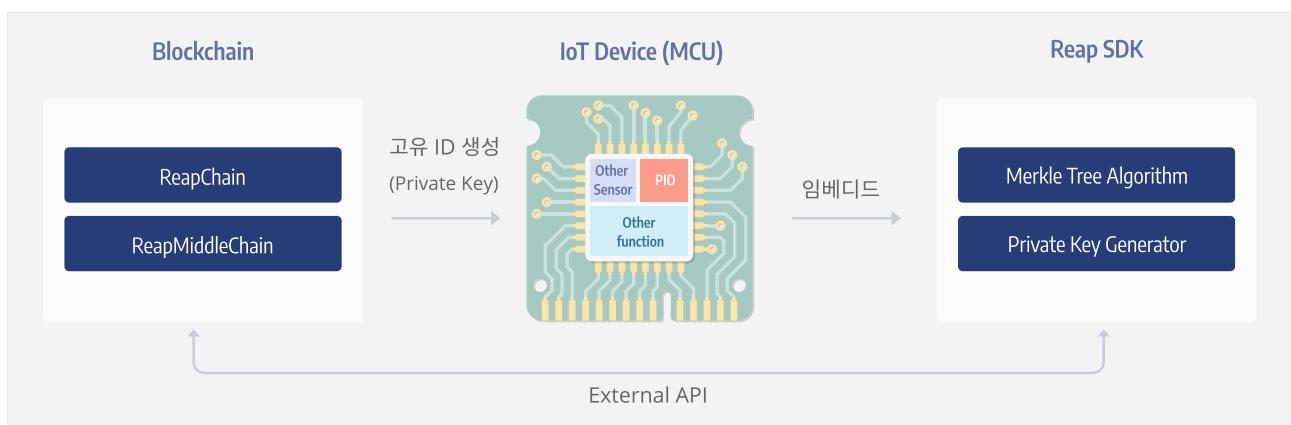
## 사물 PID

개인 (사람)의 신원 인증에만 한정되어 적용되던 DID 기술을 Reap SDK의 독자적인 암호화 기술을 통해 개개의 사물 (디바이스)에 적용하여, 새로운 사물 인증체계인 PID를 구현하고 데이터의 보안성을 확보하고자 합니다.

사물 PID는 기기 간 고유 ID (프라이빗 키) 발급을 통해 비인증된 사용자가 개별 디바이스의 ID를 볼 수 없도록 하는 '인비저블 ID (Invisible ID)' 기술과 ReapChain에 의해 이중 검증을 받은 송신자만이 IoT 기기와 통신 가능하도록 하는 '상호 검증' 기술을 통해 구현됩니다.

## Reap SDK를 통한 인비저블 ID 구현

<그림 14> 사물 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.

Reap SDK는 기존 MCU (Micro Controller Unit)을 기반으로 개발되는 프로젝트 모듈 또는 설정에 대한 지원이 가능합니다. Reap SDK를 사용하면 기존의 네이티브 SDK 코드를 재사용할 수 있도록 구성해 코드간 상호 운용성을 가지며 유지보수 및 관리 비용의 최소화가 가능합니다.

Reap SDK는 개별 IoT 디바이스에 32 Byte의 고유 ID (프라이빗 키)를 생성하여 내부의 비휘발성 메모리에 저장됩니다. 그리고 데이터 전송(Transaction) 발생 시, ReapMiddleChain에서 생성되는 최종 해시 정보를 전달받고 저장함으로써 개별 IoT 디바이스가 ReapChain의 작은 노드가 되어 디바이스의 신뢰성을 검증할 수 있습니다.

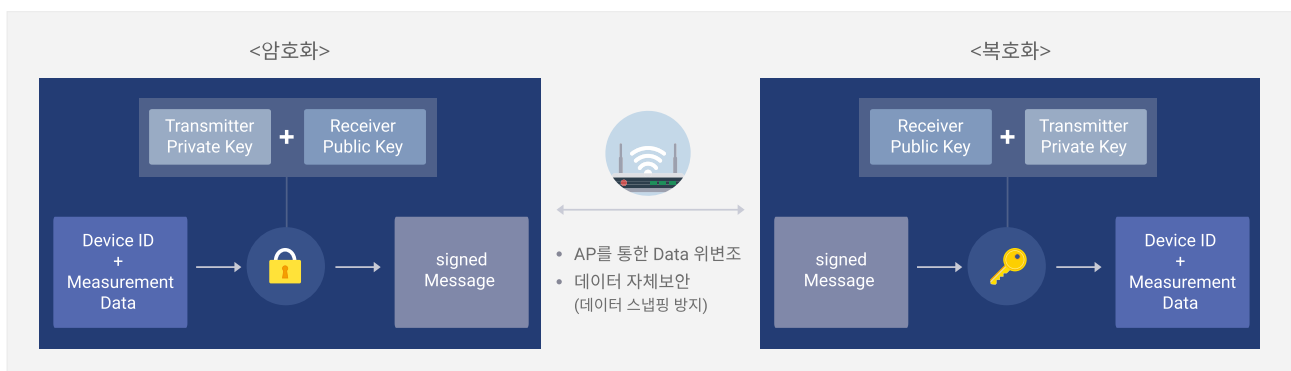
## 암호화된 Signed Message를 통한 데이터 위변조 방지

MCU에서 생성된 데이터는 각 기기가 보유한 고유의 프라이빗 키와 외부에 공개된 수신 장치의 퍼블릭 키를 이용하여 독자적인 암호화 기법을 통해 Signed Message로 생성되어 ReapMiddleChain을 거쳐 ReapChain으로 전달됩니다.

전달된 Signed Message는 복호화를 위해 수신 장치의 프라이빗 키와 전송 장치의 퍼블릭 키를 필요로 하기 때문에, 라우터 및 AP와 같은 통신 장치의 해킹이 발생해도 데이터의 위/변조 여부를 확인 가능합니다.

또한 통신장치를 통해 데이터 스넵핑 (Snapping, 데이터를 가로채는 행위)이 발생해도 프라이빗 키 없이는 데이터 복호화가 불가능하게 됩니다.

<그림 15> 암호화된 Signed Message 생성 및 전송



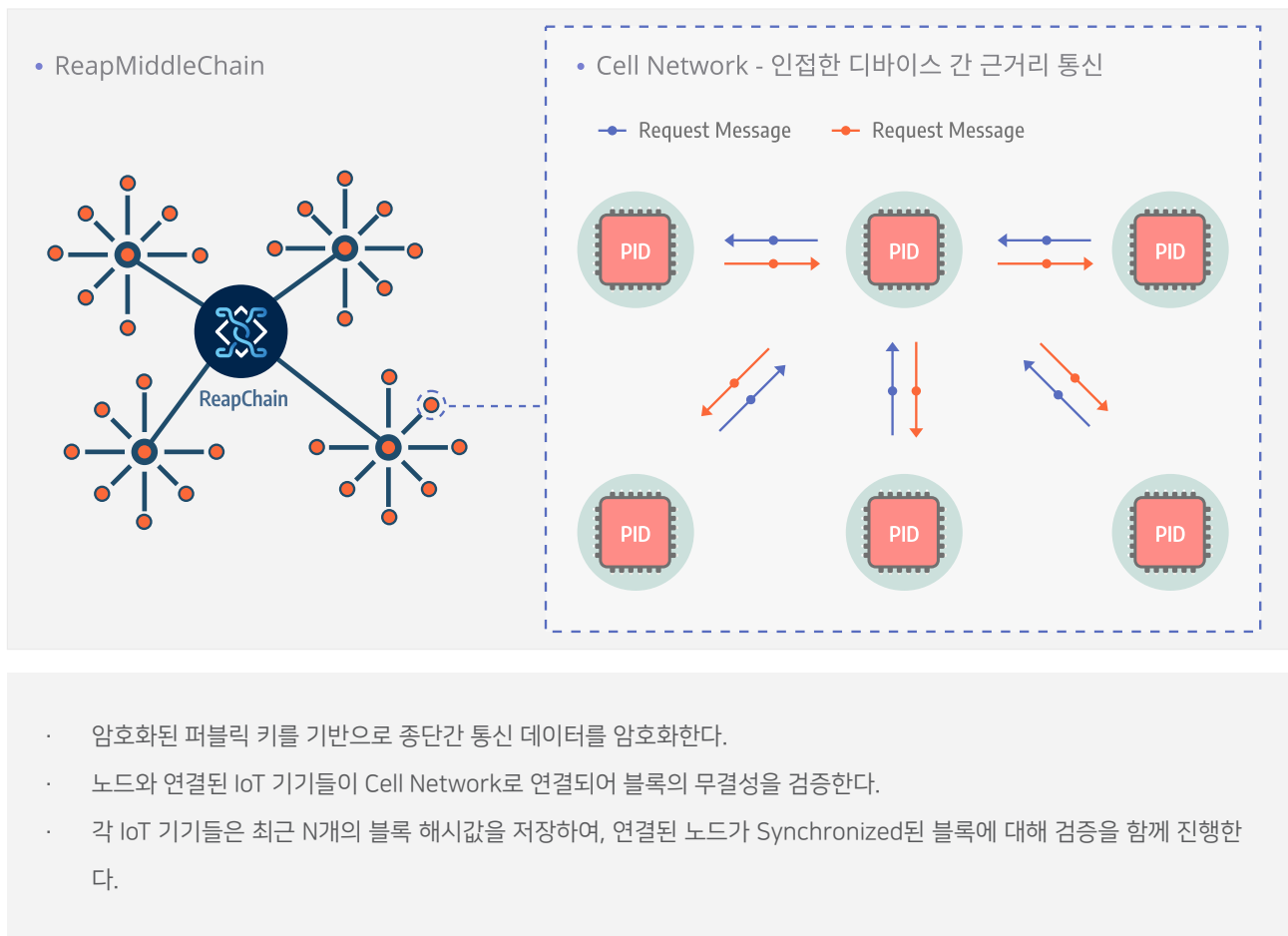
- 기기에서는 데이터를 전달하기 위해 Device ID 정보와 Measurement Data를 생성한다.
- 생성된 데이터를 기기가 가진 고유의 프라이빗 키와 데이터를 수신할 장치의 공개된 퍼블릭 키를 통한 암호화 과정을 거쳐 Signed Message를 생성한다.
- AP를 통해 전달되는 암호화된 Signed Message는 복호화하기 위해 전송받는 기기의 고유의 프라이빗 키가 필요하기에 다른 사용자는 원본 데이터를 복원할 수 없다.
- 암호화된 Signed Message를 전달받은 수신 장치는 보유한 프라이빗 키와 데이터를 전송한 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.

## 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 시스템에서 최종 센서 노드가 제공하는 데이터의 정확성을 위해서는 데이터를 중계해주는 릴레이 노드 뿐만 아니라 각 노드간 연결된 독자적인 단거리 무선 네트워크에서의 신뢰성 검증은 필수입니다.

<그림 16> 인접 디바이스 간 근거리 통신 구조



<그림 16>와 같이 Reap SDK를 적용한 Cell Network에서는 인접한 엣지 노드와 종단 노드의 머클 트리 값을 비교해 전송되는 데이터의 위변조 유무를 확인하여 2차적인 보안이 가능합니다.

## 5-3. ReapChain 구현체계

### 계층적인 아키텍처 (System Architecture) 구축

Shell-Core Structure 상에서 ReapChain 및 ReapMiddleChain, DApp과의 효과적인 연동을 위하여 계층적인 아키텍처 구조를 제공합니다. 계층적인 아키텍처의 시스템 전체를 수정하지 않고도 특정한 계층의 기능이나 성능을 개선할 수 있는 것이 가장 큰 장점입니다.

<그림 17> 아키텍처 구성도 및 구성 요소 정의



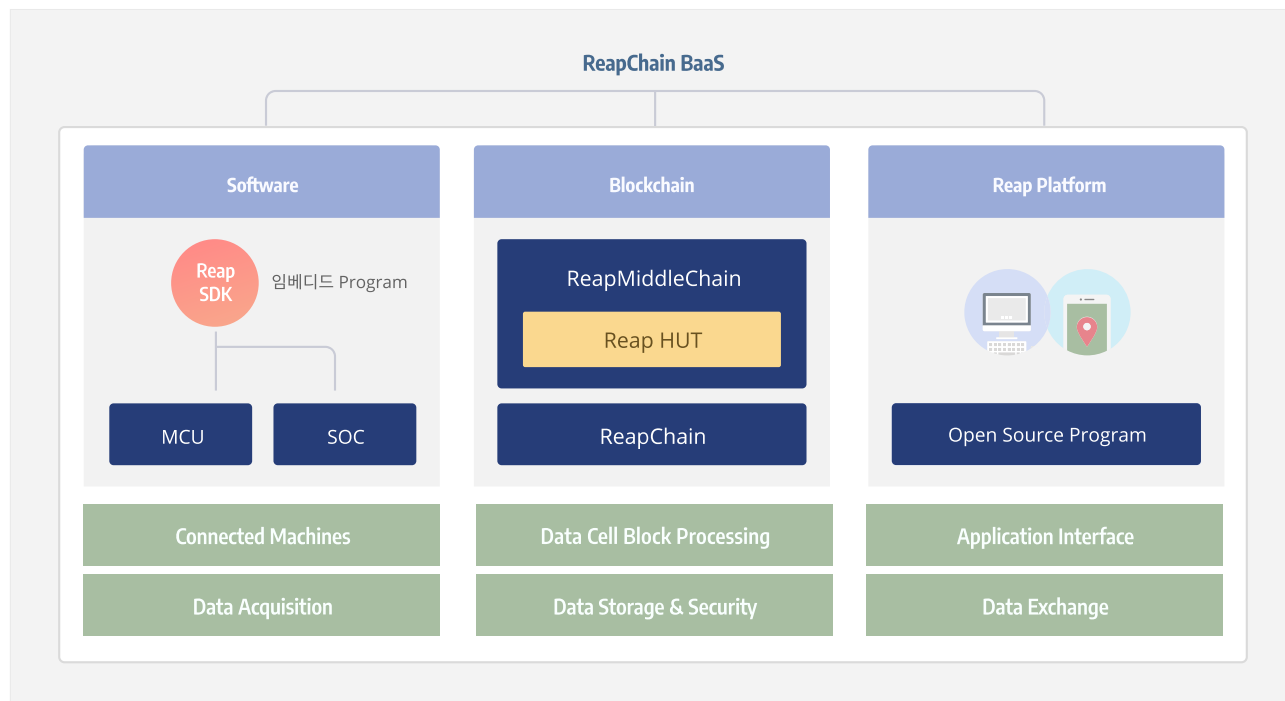
- DApp Layer (Reap Platform): 다양한 형태의 비즈니스 어플리케이션이 제공되는 계층
- ReapMiddleChain Layer: 트랜잭션을 Cell Block으로 초고속 처리하는 계층
  - BAI (Blockchain Aggregator Interface): 애플리케이션이 ReapChain과 일관되고(seamless) 손쉽게(easy) 연동할 수있는 환경 제공
  - Blockchain API Adaptor: ReapChain 코어 기능과 연동 제공
- ReapChain Main Net Layer
  - Core: ReapChain 노드의 주요 역할인 분산 합의, 블록 생성, 원장 저장 및 노드를 제어하기 위한 노드 Agent와 Node 제어 모듈 등으로 구성
  - Governance: ReapChain이 유지되기 위해 필요한 관리 기능을 제공하는 특수한 계층



## ReapChain BaaS 구축

ReapChain의 서비스는 BaaS 형태로 제공되기 때문에, 블록체인 인프라를 구축하기 위한 새로운 하드웨어나 아키텍처 구성 없이, 누구나 쉽고 편리하게 블록체인과 IoT 산업의 융합이 가능 합니다.

<그림 18> ReapChain BaaS 구성도



# 06. Business Model

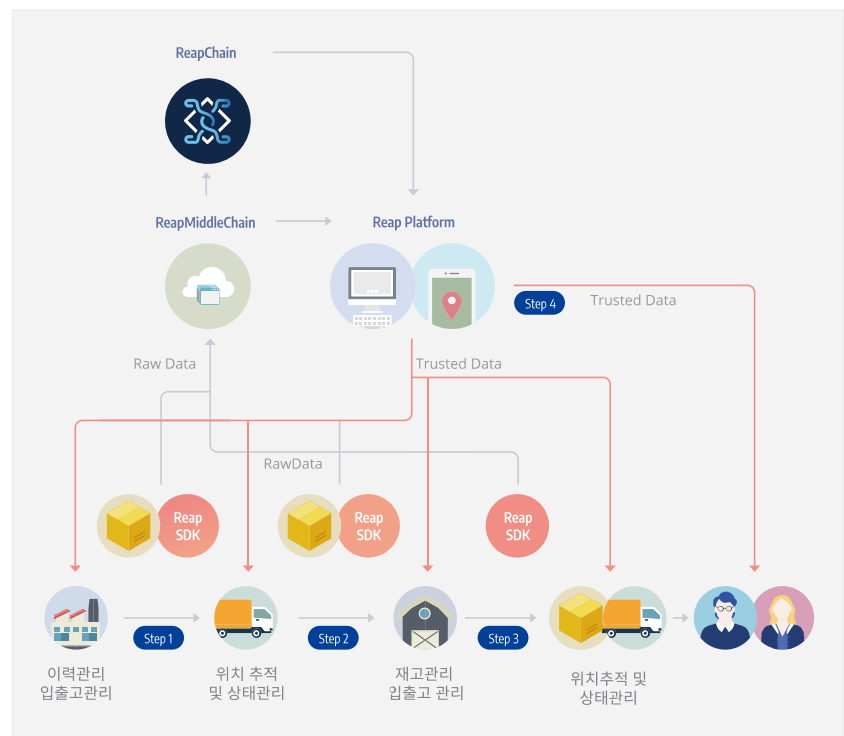
## 6-1. ReapChain 적용 가능 분야

### 유통 및 물류

공급망의 가시성과 효율성을 높이고 원활한 배송에 차질이 생기는 것을 방지하기 위해 물류 운영에 IoT를 적용할 수 있습니다.

ReapChain은 화물 선적, 집하, 운송에서 소비자에게 정확히 전달되기까지 일련의 과정에서 정보를 수집, 분석, 공유하여 안정성, 효율성, 그리고 처리 속도를 최적화 하여 유통 및 물류 산업의 혁신을 달성할 수 있게됩니다.

<그림 19> ReapChain BaaS 기반 유통 시스템 Flow Chart



Step 1. Reap SDK 적용된 IoT 센서를 기반으로 제품 생산 및 데이터 (기본정보) 입력

Step 2. 센서를 통해 제품 상태 데이터를 지속적으로 전송 및 검증

Step 3. 유통 전 과정에서의 위치 정보, 입출고 기록 등 추가 데이터 전송 및 검증

Step 4. 최종 소비자가 구매한 제품에 대한 신뢰할 수 있는 데이터 수신 및 확인

## 6-1. ReapChain 적용 가능 분야

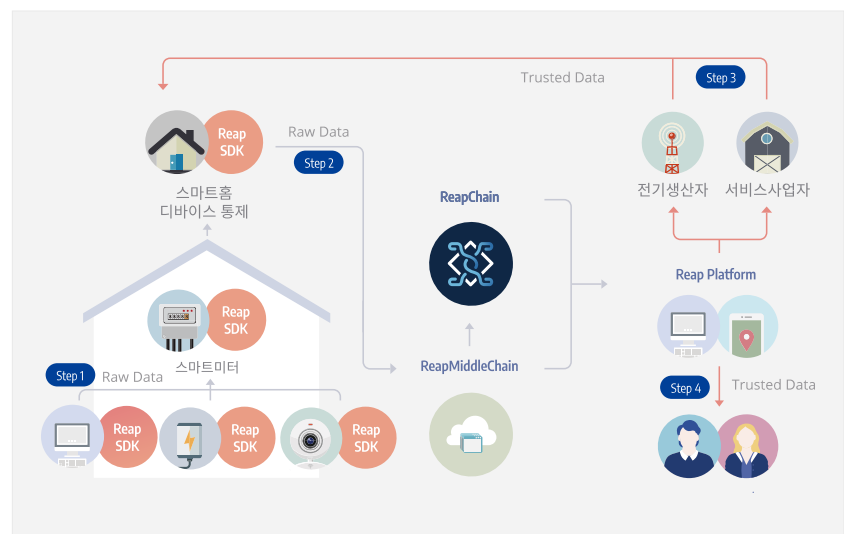
### 에너지

에너지 분야는 IoT 같은 첨단정보통신기술(ICT)을 접목함으로써 가사 자동화, 에너지 관리 효율화 등을 추구하고 있습니다.

특히나 홈 네트워크 환경은 지난 몇 년 사이에 급격히 변화되고 있으며 컴퓨터 및 각종 센서들과 같은 디바이스 수가 폭발적으로 늘어남에 따라 보안, 실시간 데이터 처리, 기기인증 부분에 대한 문제가 증가하고 있습니다.

ReapChain BaaS를 활용한 에너지 관리시스템은 상기 발생하는 문제점을 개선하고 효율적인 시스템을 구축할 수 있게 됩니다.

<그림 20> ReapChain BaaS 기반 전력 시스템 Flow Chart



Step 1. Reap SDK가 적용된 스마트 홈 기기에서 발생된 각종 데이터 및 전력량을 스마트 미터를 통해 집계

Step 2. 스마트 홈 디바이스 통제기기를 통해 기기 상태 및 전력량 데이터를 지속적으로 전송 및 검증

Step 3. Reap Platform을 통해 전기생산자는 각 가정에서 필요한 전기량을, 서비스 사업자는 서비스 질 향상을 위한 기기 상태 데이터를 확인

Step 4. 가정에서는 스마트 홈의 개별 기기에 대한 신뢰할 수 있는 데이터 수신 및 정보 확인

## 6-2. ReapChain IoT 적용 예시

\* 물류 IoT 적용 예시

### 물류 창고 시스템

대형 농산물 물류창고 중간 관리자로 근무하고 있는 월슨은 IoT 시스템을 활용하여 재고 및 창고 관리를 하고 있습니다.

기존의 IoT 시스템에서는 비인증된 사용자의 접근이나 해킹으로 인해 기기가 오작동하거나 잘못된 재고 정보를 전달하여 난감한 경우가 많았습니다. 또한, 유통과정을 거치면서 원산지와 제조일자 등이 중간에 변경되어 최종 소비자에게 잘못된 물품 정보가 전달되는 경우도 발생하였습니다.

하지만, ReapChain의 BaaS를 적용하여 이러한 문제를 해결할 수 있었습니다. 쌀을 생산하는 농부는 쌀포장지에 Reap SDK가 적용된 태그를 부착하여 재배 환경이나 생산자 정보 등을 ReapChain에 1차적으로 기록하고, 이후 월슨은 물류 창고로 입고되는 단계에서 원산지, 생산자 정보 등을 상호 검증합니다.

물품을 실은 팔레트가 지정 장소에 도착하면 Reap SDK 기반 센서를 통해 상품의 무게 및 크기, 부피 등에 관한 정보가 자동적으로 전달되고, 팔레트에 부착된 센서에서 창고관리 시스템으로 신호를 보내 실시간으로 모니터링 됩니다.

재고 및 입출고 관리 시, ReapChain BaaS가 적용된 시스템은 Reap SDK를 통해 디바이스와 리더기 간 상호 검증 과정을 거침으로써, 비 인증된 사용자의 접근을 막을 수 있습니다. 해당 정보나 데이터의 변경 및 삭제가 시도되면 ReapChain에서 최초의 데이터 정보와 비교 검증하여 잘못된 정보 (생산자, 제조일자 등)로 인해 발생할 수 있는 문제를 방지할 수 있습니다.

월슨은 ReapChain BaaS가 적용된 IoT 시스템을 통해 물류 시스템의 효율성을 높이고, 유통 전과정에서 입력된 모든 데이터에 대한 정보와 이력을 투명하게 관리하여 소비자에게 정확한 상품 정보를 전달할 수 있습니다.

## 6-2. ReapChain IoT 적용 예시

\* 에너지 IoT 적용예시

### 스마트 홈

전업 주부인 제니는 최근 스마트 홈 서비스에 가입하여, IoT 어플리케이션에 표시되는 데이터를 바탕으로 집에서 발생하는 전체 전력 사용량에 대한 정보를 받습니다. 제니는 스마트 홈을 통해 전기 요금이 저렴한 시간대에 전기 소비를 하고 있는 스마트한 주부입니다.

가정에서 사용하는 스마트 홈 디바이스는 생활가전, 주방기기, 냉난방기, 충전기, 조명, 안전기기 등 매우 다양하기 때문에 전력량을 집계해주는 스마트 미터 장치의 역할은 아주 중요합니다. 스마트 홈 디바이스는 개인 정보를 포함하고 있을 수 있어 반드시 보호해야 될 정보들입니다.

제니가 사용하고 있는 기존의 스마트 홈 시스템에서는 각 사물 고유 ID에 대한 해킹이나 해킹된 사물의 위변조된 데이터에 대한 검증이 미비하여, 잘못된 데이터 전송에 따른 관리 시스템의 오작동이나 부작용이 발생하게 됩니다. 제니는 전력량을 집계해주는 스마트 미터 장치가 해킹되어 평소보다 2배나 많은 전기 요금을 낸 경험도 있습니다.

하지만, ReapChain BaaS를 통해 기존 스마트 홈 시스템을 업데이트 하면서, 이러한 문제를 해결할 수 있었습니다.

Reap SDK를 적용시킨 센서에서 수집된 정보들은 실시간으로 ReapChain에 기록되고, 스마트 미터에서는 각 개별 디바이스의 고유 ID값을 확인하여 디바이스의 복제나 고유 ID의 변경에 따른 오작동을 사전에 방지할 수 있습니다. 제니는 이제 안심하고 스마트 홈 시스템을 사용하고 있습니다.

## 6-2. ReapChain IoT 적용 예시

\* 에너지 IoT 적용예시

### 스마트 그리드

전력 공급 업체인 A사는 IoT 플랫폼을 통해 얻은 데이터를 바탕으로 각 가정에 필요한 만큼의 전기량을 확인하고 이에 기반하여 월 총 전력 공급량을 계획하여 생산하고 있습니다.

기존의 가정에서 사용하는 스마트 미터에서 전송되는 데이터는 탈취, 누락 등으로 인해 위변조가 되어 잘못된 데이터가 표시되고 전기 생산자에게 잘못된 정보가 전달되어 월 전기 생산량을 계획하는데 차질이 생기는 경우가 발생하였습니다.

A사는 ReapChain BaaS를 도입하여 이러한 문제를 해결하였습니다. Reap SDK가 적용된 스마트 홈디바이스는 각 기기마다 고유 ID인 프라이빗 키를 획득하고 A사에서는 인증된 사용자인지 확인을 합니다. A사는 위변조 되지 않은 전력량 데이터를 토대로 정확한 월별 전기 생산량을 계획하고 생산할 수 있습니다.

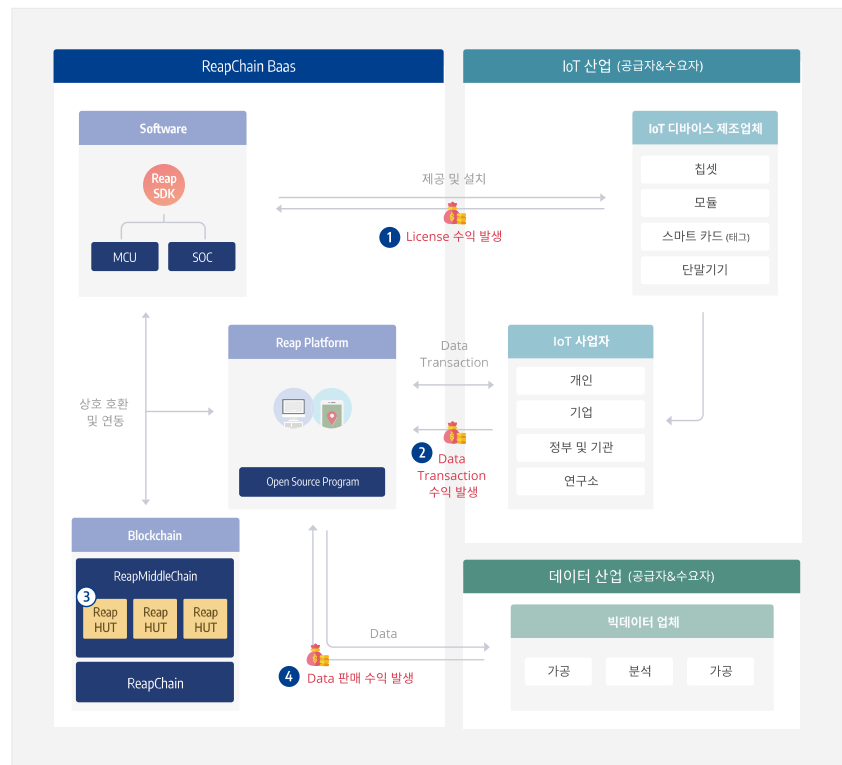
스마트 홈 시스템을 사용하는 가구 수가 증가함에 따라 전기 사용량이 많은 특정 시간대에서 대용량 데이터가 발생할 수 있습니다. 기존의 A사에서 사용하는 IoT 전력망 구조에서는 이를 신속하게 처리하기 위해서 엣지 컴퓨팅 등 새로운 기술이나 별도의 장치를 설치하고 유지 및 관리해야 하는 문제가 발생하였습니다.

하지만, ReapChain BaaS가 적용된 전력망에서는 ReapMiddleChain을 통해 별도의 엣지 컴퓨팅 기술을 도입하지 않고도 대용량 데이터를 실시간으로 전송 가능하며 고속으로 처리할 수 있기 때문에, A사는 별도의 장치를 설치하지 않고도 엣지 컴퓨팅과 같은 효과를 누릴 수 있게 되었습니다.

### 6-3. 비즈니스 모델

ReapChain의 비즈니스는 IoT 기반 다양한 사업분야로 구성되는 플랫폼 및 DApp 비즈니스이며, i) 플랫폼 활성화를 통한 각 비즈니스 영역의 결합, ii) 합리적인 수수료와 인센티브 체계 구축, iii) 경쟁력과 수익성을 갖춘 토큰 이코노미를 통해 경쟁력 있는 인프라를 구축하여, 비즈니스 모델을 확립하고자 합니다.

<그림 21> ReapChain 비즈니스 모델 구성도



- ① Reap SDK는 소프트웨어 서비스(SaaS, Software as a Service)로 제공되어 라이선스 비용이 발생
- ② Reap Platform은 서비스 운영 플랫폼이자 데이터 스토어 플랫폼으로써 데이터 거래가 발생하는 공간
- ③ Reap HUT은 임시 스토리지로서 데이터 전송 및 저장에 따른 비용이 발생
- ④ 데이터 가공업체는 Reap Platform을 통해 필요한 데이터를 획득

## 6-3. 비즈니스 모델

### ReapChain의 수익구조

ReapChain BaaS(Blockchain as a Service)를 통해 비즈니스 모델구축이 가능하며, 수익 창출이 가능합니다.

- **서비스 이용료 (라이선스 비용):** 서비스 사용자들은 ReapChain BaaS를 도입하기 위한 라이선스 명목으로 일정 금액을 요금제 방식으로 지급합니다.
  - ReapChain 기술 기반 BaaS를 설치해주고, 보안 솔루션부터 복잡한 백엔드(Backend)까지 관리해주는 총 비용을 포함합니다.
- **데이터 트랜잭션 수수료:** 서비스 사용자들은 ReapChain 상에서 발생하는 모든 데이터 트랜잭션에 대한 일정 수수료를 지급합니다.
- **Reap HUT 이용료:** 서비스 사용자들은 필요사항에 따라 Reap HUT을 이용할 수 있으며, 프라이빗한 임시 스토리지의 사용량에 대해 유동적으로 수수료를 지급합니다.
  - Reap HUT은 프라이빗한 임시 스토리지로써, 서비스 사용시 월 사용량을 지정하여 선택할 수 있으며, 정해진 사용량에 따라 비용이 다르게 책정 됩니다.
  - 또한, Reap HUT에 저장된 데이터는 일정기간이 지난 후 삭제가 가능하며, ReapChain에 최종 전송될 필수 데이터를 분류하고 결정하는 기능을 가지고 있습니다.
- **데이터 등 정보 구매:** 분석 및 활용, 홍보 및 마케팅 목적으로 별도의 고객 데이터가 필요한 사용자들은 일정한 비용을 지급하고 이를 구매할 수 있습니다.



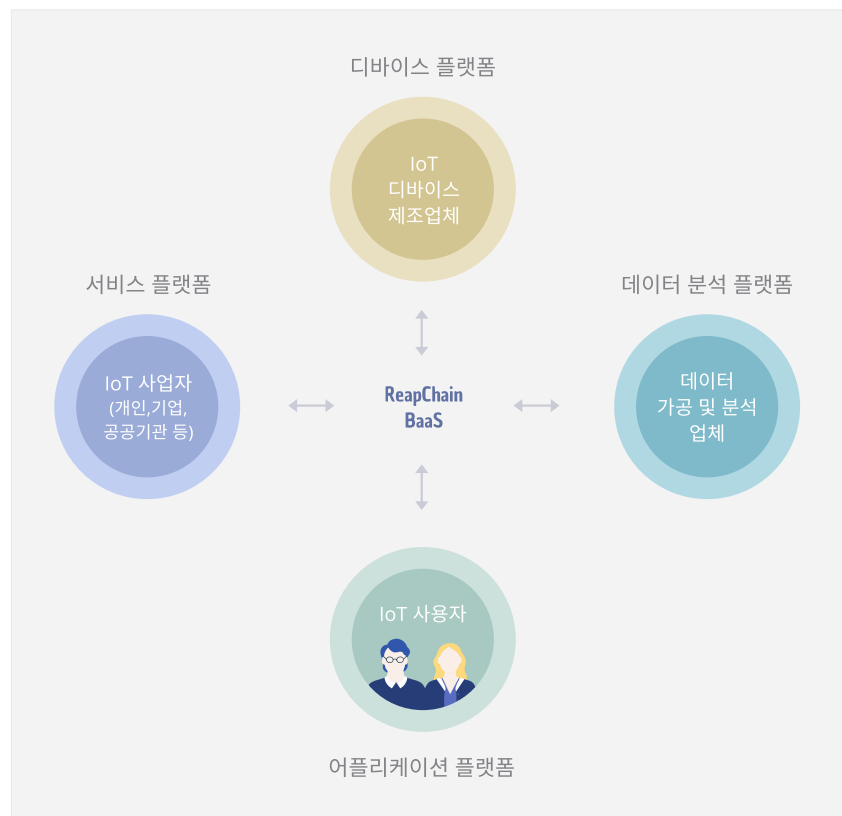
# 07. Ecosystem

## 7-1. ReapChain Ecosystem

ReapChain 생태계 상의 참여자들은 IoT 기반 4차 산업 생태계의 구성원으로써, 경제적 이익을 얻는 것과 동시에 IoT 산업의 발전에 기여하게 될 것입니다.

ReapChain 생태계 구성원은 ① IoT서비스를 이용하는 사용자와 ② ReapChain BaaS를 활용하고 도입할 수 있는 IoT 디바이스 제조업체 ③ IoT 기반 시스템을 구축하기 위한 개인, 기업, 정부 및 공공기관 등 사업자, ④ 그리고 IoT 기반 데이터를 구매하여 가공 및 분석, 활용하기 위한 업체로 구성됩니다.

<그림 22> 생태계 구성도 및 구성원 개요



- **디바이스 제조업체:** 센서 및 구동기 등 IoT 디바이스가 제공하는 하드웨어 자원과 이러한 하드웨어 자원을 연결하는 운영체제(OS) 및 소프트웨어 등을 포함한 서비스를 제공하는 업체
- **IoT 사업자:** 다양한 응용 서비스의 용이한 생성 및 실행을 지원하는 서비스로, IoT 기반 응용 소프트웨어의 배포를 지원하는 애플리케이션 구현 및 네트워크 서비스 업체
- **데이터 분석 업체:** 다양한 디바이스로부터 획득되는 데이터를 가공 및 분석하고 활용하는 업체
- **IoT 사용자:** 어플리케이션을 통해 IoT 서비스를 이용하는 개인이나 주체

## 7-2. 향후 계획

### 전 산업의 데이터 공유 플랫폼 생태계 구축

향후에는 데이터가 모든 산업의 발전과 새로운 가치 창출의 촉매 역할을 하는 새로운 '데이터 경제 (Data Economy)' 시대가 도래할 것이며, 데이터 기반의 새로운 서비스들은 기존 경제의 가치사슬들을 더욱 복잡하고 거대한 생태계로 바꿔 놓을 것으로 예상됩니다.

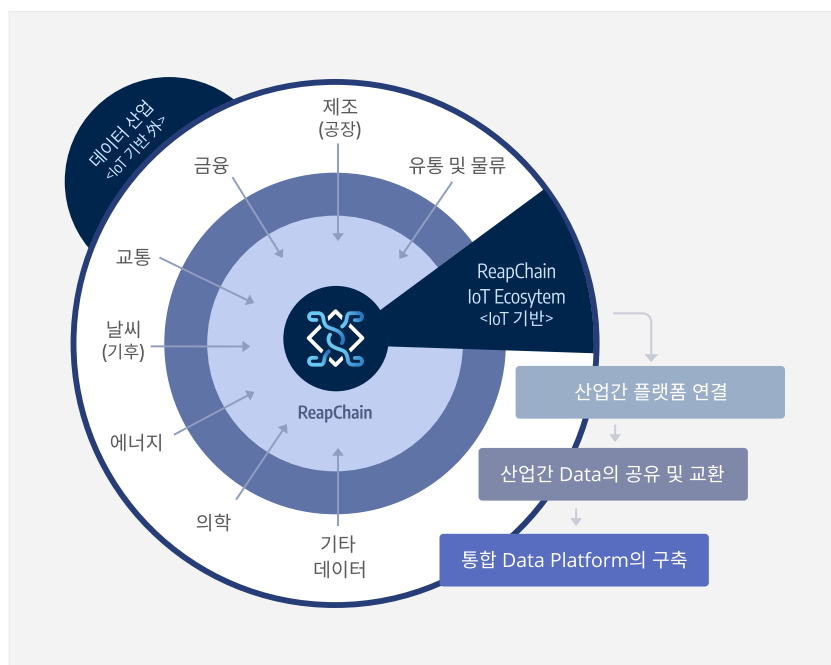
각종 IoT 센서 등에서 발생하는 대량의 데이터는 산업과 경제 활성화를 견인하는 원동력으로 작용할 전망입니다.

### 데이터 산업으로의 플랫폼 생태계 (Ecosystem) 확장

기업, 개인, 공공분야 등 각 분야 다양한 주체들은 실시간으로 수많은 데이터를 발생시키면서, 동시에 데이터를 활용하게 될 것입니다.

ReapChain은 ReapChain 인프라를 활용하여, IoT를 통해서 수집되고 저장되는 수많은 데이터를 기반으로 의학, 금융 등 타 산업 플랫폼과의 연계 및 확장을 통해 데이터를 상호 공유하고 활용할 수 있는 통합 플랫폼을 구축할 수 있게 됩니다.

<그림 23> ReapChain의 향후 계획



ReapChain의 미래는 개방형 데이터 공유 플랫폼을 기반으로 전 산업간 양질의 데이터 유통을 촉진합니다.

또한, ReapChain은 전 산업에 걸쳐 누구나 데이터를 쉽고 빠르게 등록하여, 하나의 플랫폼에서 공유할 수 있는 플랫폼 생태계의 허브 역할을 함으로써, 블록체인 기반 공유경제 생태계를 실현 할 것 입니다.

# 08. Roadmap

---



# 09. Token Economy

## 9-1. Token Economy

ReapChain은 블록체인 참여자들이 자발적으로 ReapChain을 활성화하도록 경제적 인센티브를 제공함으로써 누구나 쉽게 사용할 수 있는 플랫폼 공유경제 비즈니스 모델을 지향합니다.

일반적으로 PoW(Proof-of-Work)방식은 블록을 채굴한 노드가 트랜잭션 수수료를 수취하며, PoS(Proof-of Stake)방식은 암호화폐를 예치해야만 보상을 받는 구조에 비해 ReapChain은 REAP을 보유하거나 생태계에 참여하기만 해도 트랜잭션 수수료가 배분됩니다.

ReapChain 내에서는 상호 유기적으로 생태계에 참여하고 이에 따라 보상을 받는 구조를 만들어 IoT 기반 인프라가 풍성해지고 IoT 산업이 활성화되는 선순환 구조를 이루고자 합니다.

① ReapChain 생태계의 연료 역할을 하는 REAP은 일정 지분을 보유하고 있거나 거래 검증 및 블록생성을 통해 ReapChain 네트워크를 유지하는 사용자에게 트랜잭션 수수료를 리워드 및 인센티브로 지급됩니다.

② 리워드는 총 수수료 수입이며, 수수료 적립액 100만 REAP이 충족되는 경우 지급합니다. 또한 배분 시점에 적립금이 상한액을 초과하는 경우 모두 합산하여 지급합니다.

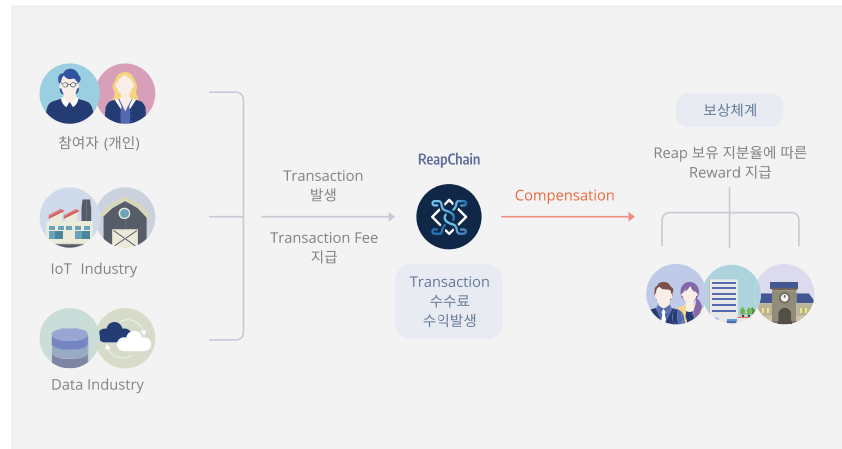
③ ReapChain은 생태계 활성화를 위해 REAP 보유자와 상임위원회, 운영위원회 및 후보군에 대해서도 리워드를 지급합니다.

④ 총 적립금의 배분 비율은 전체 REAP 보유자에 대해 70%, 운영위원회 및 후보군 20%, 상임위원회 10%로 하며, 중복지급을 허용합니다.

## 9-1. Token Economy

### 기본 수수료 및 리워드(Reward) 체계

<그림 24> ReapChain 토큰 이코노미 및 보상체계



- **지불 수단:** ReapChain은 기본적인 지불 결제 수단이며, 단위는 REAP입니다.
- **기본 수수료 (트랜잭션 수수료):** ReapChain 생태계 참여자 및 서비스 사용자들은 ReapChain에서 발생하는 모든 트랜잭션에 대한 기본 수수료 및 오퍼레이션 코드 연산에 따른 추가 수수료를 REAP으로 지급하게 됩니다.
- **리워드 방식:** ReapChain 생태계 참여자들에게는 REAP 보유 지분 및 기여도에 따라 리워드로 REAP을 제공합니다

### ReapChain 활성화를 위한 추가 인센티브(Incentive) 10%

총 수수료 수입에 대한 리워드와는 별도로 REAP 총 발행량 중 10%는 생태계 참여에 대한 리워드로 10년에 걸쳐 매년 1%씩 지급하며, 120만번째 블록 생성 시 전체 REAP 보유자들에게 개별 REAP 보유량에 비례하여 지급합니다.

## 9-2. Token Allocation

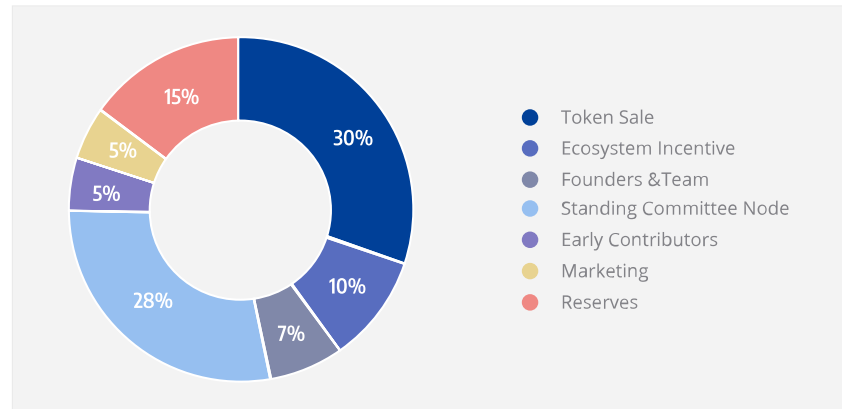
### Token Value

총 발행량: 49,000,000,000 (49억개)

개당 토큰의 가격: 0.03 USD

### 토큰 할당 비율 (Token Allocation)

REAP 토큰은 <그림 25>과 같은 비율로 분배됩니다.



#### ① 토큰 세일 (Token Sale)

REAP 토큰의 30%는 락업 (Lock-up) 기간을 적용하여 판매될 예정입니다.

#### ② 생태계 참여 인센티브 (Ecosystem Incentive)

총수익에 대한 분배와 별도로 REAP 총 발행량 중 10%는 생태계 참여에 대한 보상으로 10년에 걸쳐 매년 1%씩 지급하며, 120만번째 블록 생성 시 전체 REAP 보유자들에게 개별 REAP 보유량에 비례하여 지급합니다.

#### ③ 설립자 & 팀 (Founders & Team)

우리 프로젝트 성공을 위해 헌신을 하고, 각자의 재능과 노력하는 설립자와 팀원들에게 7%를 배정합니다. 토큰의 배분은 기여도에 따라 지급하며, 배분일 이후 각자 수령일로부터 12개월후 50%, 24개월후 50% Lockup 해제합니다.

#### ④ 상임위원회 (Standing Committee Node)

상임위 노드로 선정되기 위해서는 2%의 토큰을 보유하여야 하며, 총 14개의 구성된 상임위 노드에 총 28%가 배정이 됩니다.

#### ⑤ 초기 기여자 (Early Contributors)

우리 프로젝트를 지지하는 Early Contributors에게 5%를 배정합니다. 토큰의 배분은 기여도에 따라 지급하며, 각자 수령일로부터 12개월후 50%, 24개월후 50% Lock-up 해제합니다.

#### ⑥ 마케팅 (Marketing)

ReapChain 프로젝트 홍보를 위해 다양한 글로벌 마케팅 캠페인을 진행하기 위해 5%를 배정합니다. Lockup 기간은 마케팅 캠페인마다 별도로 정할 예정입니다.

#### ⑦ 회사 보유분 (Reserves)

15%는 회사 보유분입니다. 회사는 최소 5% ~ 최대 15% 보유를 유지하도록 관리할 예정입니다.

## 9-2. Token Allocation

### 토큰 배분 (Token Distribution)

토큰의 배분일은 2020년 2Q~3Q 예정이며(추후 공지), 모든 토큰의 지급은 배분일 이후 전송합니다. (TGE는 상장 예정일 2주전 정도로 예상하고 있습니다.)

### 기금의 사용 (Use of Proceeds)

기금 모금이 끝나면 다음과 같은 방법으로 자금을 배분하여 운영합니다. 만약 우리가 우리의 완전한 자금 목표를 달성하지 못한다면, 이러한 배분은 우리가 프로젝트 개발을 위해 가장 중요하고 우선적인 것으로 결정한 것을 반영하기 위해 조정할 수 있습니다.

- 시장 안정화 40.0% (바이백)
- R&D 36.3%
- Operations 11.0%
- Marketing 10.0%
- Capital Reserves 2.7%

### 수익금의 사용 (Use of Platform Revenue)

ReapChain에서 생성된 수익은 기술 지원, 프로모션 및 회사, 관계사 운영 및 재무 관리 목적으로 사용되며 REAP의 가치를 안정화하기 위해 때때로 바이백 됩니다.

# 10. Team

---

## Team



JUSTIN KIM  
CEO



JAKE LEE  
co-CEO



KHAN KIM  
CSO



MASON SON  
CRDO



SUNGJIN KIM  
CTO

---

## Advisors



SEUNGHUN HAN



CHULHO LEE



TAEHONG KANG



HYUKJUN KWON



CHEOLHWAN KIM



HYUNWOO YI



DAVID LEE



JONGWON KIM



# 11. Partners

---



---

## Advisory group



# 12. 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"
- 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"
- Yoshiharu Akahane, Aikei Minabu (블록체인 구조와 이론, 2017), "ブロックチェーン仕組みと理論"
- 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"
- A. Asayag, G. Cohen, I. Grayevsky, M. Leshkowitz, O. Rottenstreich, R. Tamari & D. Yakira, "Helix Consensus Algorithm (Orbs Research, 2018), "Helix Consensus Algorithm"
- AMO Whitepaper v5.1 (2018), "<https://www.amo.foundation/>"
- IoTeX Whitepaper v1.5 (2018), "<https://docs.iotex.io/>"
- Waltonchain Whitepaper v2.0 (2018), "<https://www.waltonchain.org/>"
- G. Konstantopoulos (2017), "Understanding Blockchain Fundamentals, Part 1: Byzantine Fault Tolerance"
- Juan Carlos Garcia (Reviews of Modern Physics, 2017), "Quantum Random Number Generators"
- Miguel Castro, Barbara Liskov (ACM-Transactions on Computer Systems), "Practical Byzantine Fault Tolerance and Proactive Recovery"
- Mingxiao, Du, et al. (International Conference on Systems, Man, and Cybernetics, 2017), "A review on consensus algorithm of blockchain"
- Bach, L. M., Branko Mihaljevic, and Mario Zagar. (International Convention on Information and Communication Technology, Electronics and Microelectronics, 2018) "Comparative analysis of blockchain consensus algorithms."
- Gramoli, Vincent (Future Generation Computer Systems, 2017) "From blockchain consensus back to byzantine consensus"
- Baliga, Arati (Persistent, 2017), "Understanding blockchain consensus models"
- Van Alstyne, Marshall W., Geoffrey G. Parker, and Sangeet Paul Choudary (Harvard business review, 2016), "Pipelines, platforms, and the new rules of strategy"
- Lo, Sin Kuang, et al. (IEEE Access, 2019), "Analysis of Blockchain Solutions for IoT: A Systematic Literature Review"
- Gero Dittmann, Jens Jelitto (IBM Research, 2019), "A Blockchain Proxy for Lightweight IoT Devices"
- Androulaki, Elli, et al. (IBM Research, 2018), "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains"
- Niya, Sina Rafati, et al. (IEEE International Conference on Blockchain and Cryptocurrency, 2019), "Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams"
- Pe a, Miguel Angel Lopez, and Isabel Muñoz Fernandez (IEEE 5th World Forum-IoT, 2019), "SAT-IoT: An Architectural Model for a HighPerformance Fog/Edge/Cloud IoT Platform"

# 13. Disclaimer

---

## 면책 조항

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 규제에 따라서는 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, 구매자들은 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 규제기관의 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.

## 투자 위험

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.