[Transaction Innovation - IoT Contract & M2M Transaction Platform based on Blockchain]

저자에게 질의 사항 및 제안 사항 연락처: support@hdac.io

2017. 11.

개요

IoT 산업이 기하급수적인 성장을 하고 있다. Hdac 플랫폼은 성장하는 IoT 환경에서 필요한 나머지 부분들을 채울 수 있다. 특히 Hdac 플랫폼은 아래와 같은 분야에 응용될 수 있다.

1. 인증 - 복수의 사용자 또는 디바이스가 서로를 정확하게 확인할 수 있다.

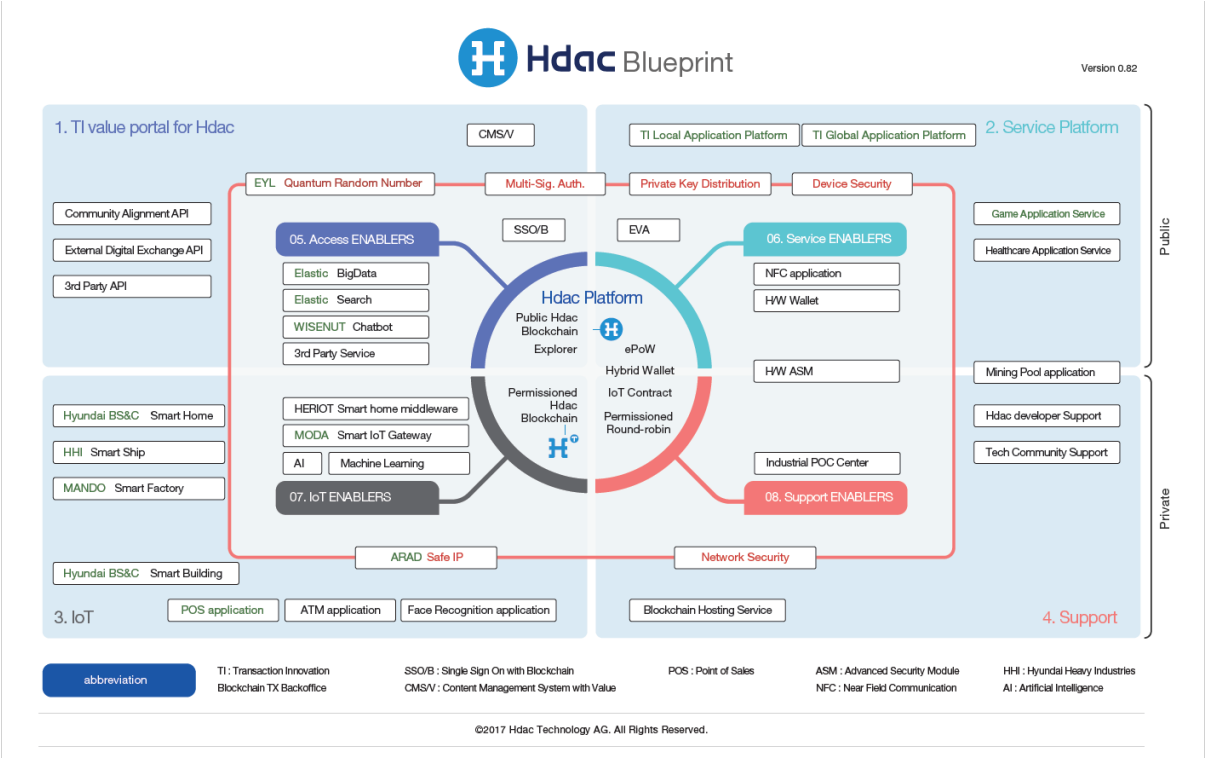
2. 매핑 – 사용자 또는 디바이스가 인증이 된 후 이상 없이 서로 연결된다.

3. M2M 거래 - 복수의 디바이스에서 청구 및 지불이 가능하다.

Hdac은 상기 세 가지 이슈를 블록체인과 IoT를 결합하여 해결한다. 블록체인에서 인증, 매핑 및 증명이 된 IoT 디바이스 사이에서 자동화, M2M 및 초 저비용의 거래가 가능해진다.

구조학적으로 Hdac의 시스템은 퍼블릭 및 프라이빗 블록체인을 이용하여 이전의 퍼블릭 블록체인과는 차원이 다른 거래 스피드를 가능케 한다. 해당 기술은 양자 난수 생성을 사용하여 안전한 거래를 구현할 수도 있다.

Hdac 시스템은 궁극적으로 급속히 성장하는 IoT 산업의 효율성 및 보안을 보장할 것이다.



소개

미래는 초연결 사회로 발전할 것이며 경제 체계는 디지털 혁신을 거듭할 것이다. 이를 위해 암호화폐로써 가치가 검증된 블록체인과 IoT(Internet of Things; 사물인터넷)의 적절한 결합을 통한 기술적 진보는 매우 중요한 역할을 하게 될 것이다. 시장과 사용자는 보다 신뢰성 높고 합리적인 소비를 원할 것이며 이러한 수요는 블록체인으로 구현할 수 있는 M2M의 발전을 견인할 것으로 기대한다.

우리가 바라보는 미래 디지털 세상은 "신뢰도 높은 블록체인 네트워크 상에서 Hdac 블록체인은 하나의 플랫폼으로써 작동하고 세상의 무수한 IoT 디바이스의 편리한 서비스를 간편하게 이용하는 세상"이 될 것이다. 경제는 신뢰라고 한다. 새로운 기술들도 결국 신뢰를 기반으로 구축되었을 때 그 가치가 빛을 발할 것이다. Hdac 블록체인은 우리가 맞이할 4차 산업혁명의 신뢰 기반을 만들 수 있는 블록체인과 IoT가 융합되면서 보다 합리적이고 효율적인 트랜잭션 체계를 실현하는 핵심 도구가 될 것이다.

Hdac 블록체인을 통하여 실현하고자 하는 기술 철학은 일상 생활에서의 트랜잭션 환경을 획기적으로 개선하는 것에 있다. 모든 경제 활동은 원활하고 쉬운 트랜잭션이 뒷받침 되어야 한다. Hdac 플랫폼 통하여 합리적인 소비와 모든 커뮤니케이션이 정확하고 스마트한 관리가 가능하게 될 것이다.

근시일 내에 블록체인과 암호화폐는 IoT환경에 적합한 트랜잭션 수단으로써 역할을 하게 될 것으로 기대된다. 아파트 관리비, 이동통신 요금 등 현재의 중앙화된 청구/입금/정산 시스템으로부터 야기되는 고비용 저효율 구조를 개선하기 위해 P2P(Peer-to-Peer) 트랜잭션과 함께 M2M(Machine to Machine) 처리를 위한 머신커런시(Machine Currency)가 구현되고 있다.

하지만 모든 것이 연결된 환경에서 적절한 권한을 가진 사용자인지 확인(인증)하고 적합한 디바이스에 연결하여, 요구된 작업을 처리하는 데 필요한 인증 기능도 필요하게 된다. 이러한 변화는 생활에 필요한 소비재 구매와 공공서비스 이용 등 모든 경제 활동에 있어서 합리적인 소비와 투명한 정산이 가능한 소액 지불(Micro Payment) 문화를 실현되게 해 줄 것이다. 예를 들어 전기, 수도, 케이블TV, 인터넷 등 공공재 이외에도 소비재에 대해 사용자가 실제 필요한 만큼 사용하고, 실제 사용한 만큼 즉시 거래가 이루어진다.

Hdac 프라이빗 블록체인 기반의 스마트 트랜잭션 수단인 Hdac*T(Hdac Token)는 IoT 환경에서 다양한 조건에 따라 주어진 처리를 할 수 있도록 설계되어 있다. Hdac 프라이빗 블록체인은 이러

한 M2M 트랜잭션 기능과 간단한 트랜잭션 서비스 환경을 지원하며, Hdac이 추구하는 합리성과 효율성으로 IoT 디바이스를 사용하고 제어할 수 있는 플랫폼이 될 것이다.

또한 Hdac은 IoT 디바이스 간의 통신과 트랜잭션에 대한 사용자 보안 강화 및 트랜잭션 편의성 증대를 위한 하드웨어 지갑을 제공하는 등, 하이브리드 블록체인 플랫폼으로 진화해 갈 것이다.

블록체인과 IoT

IoT에서의 블록체인 활용

스마트 홈이나 스마트 팩토리와 같은 환경에서는 센서가 장착된 다양한 IoT 디바이스가 존재하고 이것들은 긴밀하게 상호 연결이 되어 있어 상호 간의 조건에 맞추어 보다 안전하고 신뢰성 있게 작동하도록 프라이빗 블록체인을 구축할 수 있다. 프라이빗 블록체인은 사용자의 인증뿐만 아니라, 디바이스 간의 상호 인증, 작동 내역의 기록, 그리고 시나리오 기반의 IoT Contract가 수행되도록 구성되어야 한다. 또한 프라이빗 블록체인은 기 운영중인 퍼블릭 블록체인과 상호 작용을 해야만 실질적인 편리성이 높아질 것이다. 그런 측면에서 사용자가 퍼블릭 블록체인에서 사용될 HDAC(Hdac*C)을 프라이빗 블록체인에서 효과적으로 활용할 수 있도록 구성해야 한다. 우리는 프라이빗 블록체인과 퍼블릭 블록체인이 상호 연결되도록 구성하여 통상적인 사용자 측면과 특정한 용도로 구성된 프라이빗 블록체인과 효과적으로 사용할 수 있는 신뢰 기반 생태계를 조성하고자 한다. 즉, 퍼블릭 블록체인의 P2P 정산 이상의 트랜잭션이 가능하며, 프라이빗 블록체인에서 작동하는 IoT 디바이스 간의 상호 계약 및 트랜잭션을 위한 Hdac*T를 구현하여 보다 합리적인 소비와 트랜잭션이 가능한 플랫폼을 제공한다.

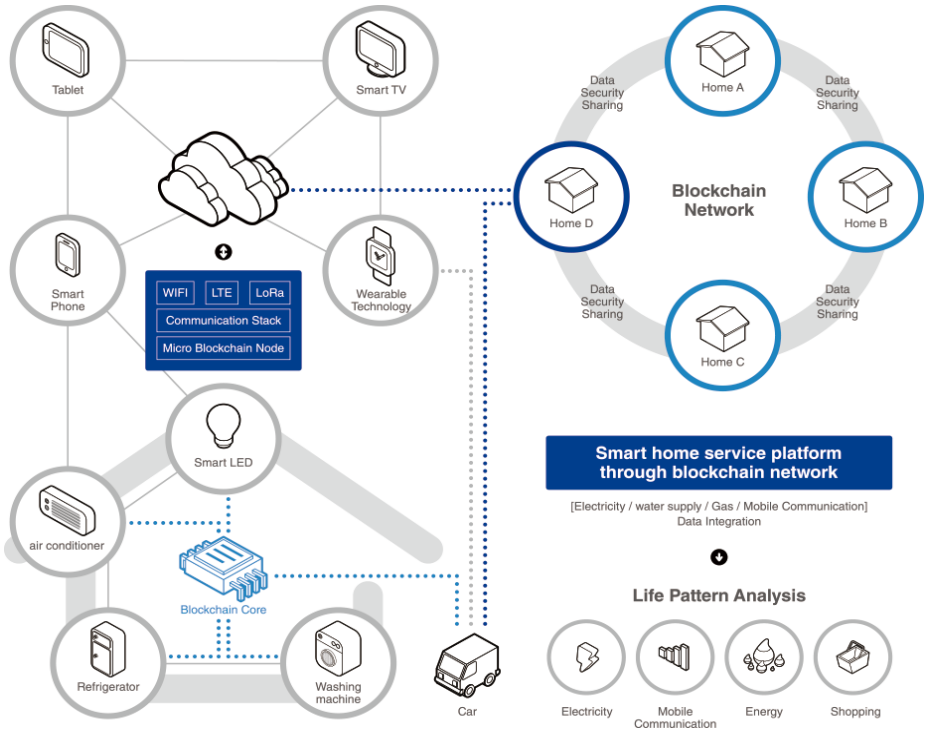


그림 1. IoT에서 활용 가능한 프라이빗 블록체인 활용의 예시

예를 들면, 사용자가 지정된 용량 또는 일정 예산 내에서 디바이스를 작동시키고 싶다고 가정하자. 사용자는 스마트폰, 컴퓨터, 스마트 TV, 리모컨 등에 탑재된 컨트롤 디바이스에서 지정된 값(용량 또는 금액)을 설정하여 해당 디바이스에 데이터를 전달한다. 그러면 해당 디바이스의 측정 데이터 처리부에서는 사용자가 전송한 값을 계량을 담당하는 디바이스에게 전송하고 작동을 시작하게 된다. 이때 작동되는 디바이스는 계량을 담당하는 디바이스에서 지정된 값에 도달했다는 신호를 전송할 때까지 작동하게 된다. 그리고 작동 디바이스는 지정된 값 도달시 또는 사용자 컨트롤 디바이스에서 현재 작동 상태 확인을 요청할 경우 데이터를 전달하여 사용자가 확인할 수 있도록 한다. 이때 사용자 컨트롤 디바이스, 작동 디바이스, 계량 디바이스 간에 이루어지는 커뮤니케이션 과정 사이에는 인증 과정이 필요하게 된다. 인증된 디바이스가 아닐 경우에는 명령을 보내거나 모니터링 할 수 없도록 하는 상호 인증 체계를 도입할 수 있다. 아울러 인증되어 체결된 IoT Contract에서는 M2M 트랜잭션을 만드는데 사용될 수 있으며, 프라이빗 블록체인의 경우 사용자가 정의한 Hdac*T가 IoT 디바이스를 활성화하기 위한 트랜잭션으로 이용될 수 있다.

사용자 정의 Hdac*T는 IoT Contract에서 특정한 용도로만 한정하여 트랜잭션을 시행하도록 속성을 부여할 수 있으며, 사용자가 원하지 않는 디바이스 또는 용도로 전용하는 것을 방지할 수 있다. 이는 앞서 설명한 보안성을 유지하면서 비용 사용의 투명성을 제공하는데 큰 역할을 한다. 가령 예를 들면 지진이나 화재 발생시 주거자가 안전하게 대피할 수 있도록 가스 및 전기를 차단할 수 있다.

블록체인 네트워크 간의 연동

퍼블릭 블록체인 간의 연동

초기 블록체인 기술이 탈 중앙화, 투명성, 사용성, 신뢰성 측면에서 점차 각광을 받으면서, 활용 분야는 암호화폐와 존재 증명, 예측 시장, 국제 금융 등 산업 전반으로 확대되고 있다. 이에 따라 트랜잭션과 데이터의 양도 증가하여, 퍼블릭 블록체인에서 트랜잭션을 감당할 수 없는 경우도 고려해 보아야 한다.

퍼블릭 블록체인과 퍼블릭 블록체인 사이의 연결은 암호화폐 거래소를 통해서 데이터를 교환하는 방식으로 이미 구현되고 있다. 즉, 암호화폐 거래소에 등록된 블록체인의 경우, 거래소가 중계를 해 주는 방식으로 상호 암호화폐 간의 교환이 이루어질 수 있다. 이 방식은 물리적으로 원화-달러 사이의 교환과 같은 방식으로 이루어지기 때문에, 사람들이 쉽게 확인하고 서비스를 이용할 수 있다는 장점이 있다.

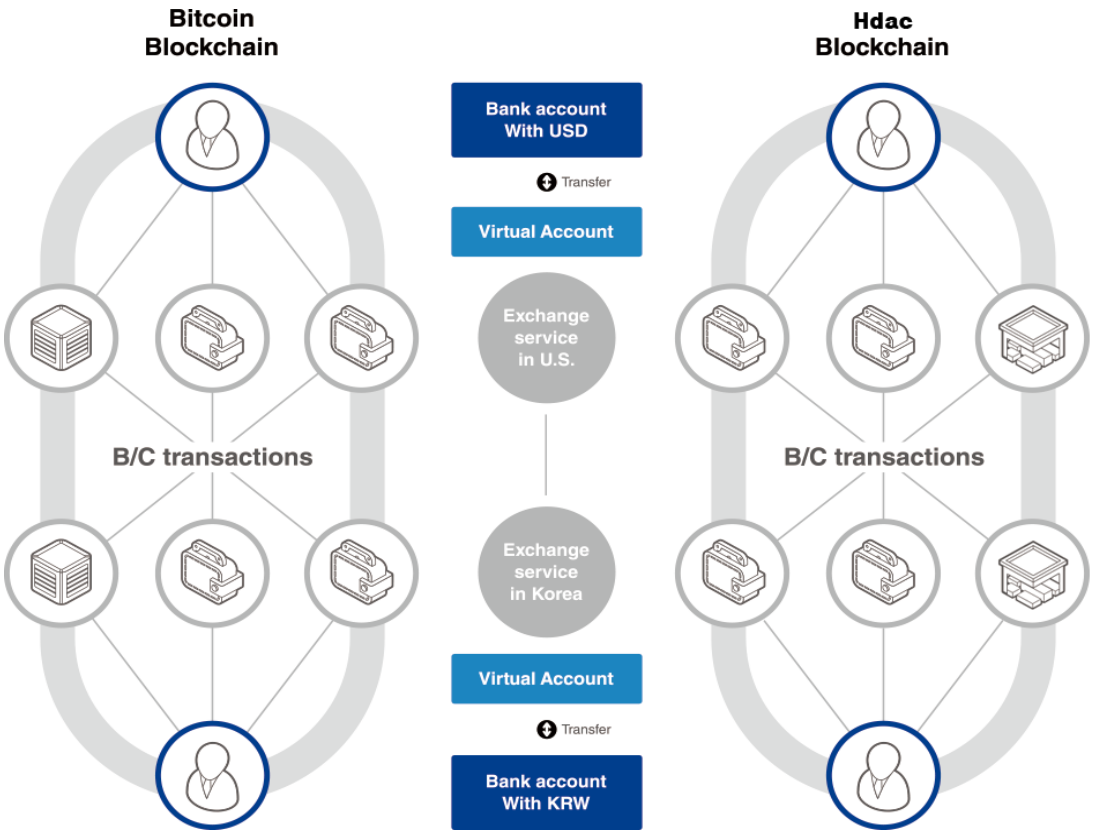


그림 2. 퍼블릭 블록체인 간의 연결 예시

계층적인 방식으로 퍼블릭 블록체인이 연결될 수도 있다. 예를 들어 구 단위 또는 군 단위의 투표가 이루어질 수 있는 하위 블록체인이 있고, 여기에서 나온 결과들은 중간 단계의 블록체인으로 연동이 되어 통합된다. 이때 중간 블록체인은 시 단위 또는 도 단위의 규모이며, 다수의 하위 블록체인을 가지는 구조가 될 수 있다. 즉, 하위 블록체인에서 수집된 트랜잭션의 요약본이 중간 블록체인으로 전달되는 방식이다. 상위 블록체인은 국가 규모의 블록체인으로 모든 하위 블록체인 정보들이 통합되는 구조로 볼 수도 있다.

이 예는 하나의 단적인 예이지만, 트리 형태의 블록체인 네트워크 상에서 다양한 형태로 적용이 가능할 수 있다. 이 경우 퍼블릭 블록체인 사이의 연동은 거래소 역할을 하는 별도의 중계자를 통해서 연동이 될 수 있다. 이 방식은 블록체인의 체인화라고 할 수도 있다.

퍼블릭 블록체인과 프라이빗 블록체인 간의 연동

프라이빗 블록체인 네트워크는 퍼블릭과 달리 접근 권한이 강화된 블록체인이며, 설정에 따라 퍼블릭처럼 자유롭게 각 노드에 접근이 불가능할 수도 있다. 따라서 퍼블릭 블록체인에서 프라이빗 블록체인에 접근하기 위해서는 중계를 해 주는 브리지 노드(Bridge Node) 또는 중계자가 필요하다. 브리지 노드는 프라이빗 블록체인 노드와 동일하게 작동하면서, 퍼블릭 및 프라이빗 양쪽 블록체인의 wallet을 가지고 있으며 양쪽에 모두 접근 가능해야 한다.

프라이빗 블록체인의 특성상 특정한 노드나 디바이스에 접근하기 위해서는 사전에 인증되고 등록된 퍼블릭 블록체인의 노드이어야 한다. 즉, 프라이빗 블록체인의 관리자가 접근 권한을 부여한 경우에만 프라이빗 블록체인에 접근할 수 있다. 또는 특정한 트랜잭션인 경우는 관리자에 의해서 별도의 권한이 부여되어 노드나 디바이스로 보낼 수 있다. 근본적으로 프라이빗 블록체인을 사용하기 위해서는 프라이빗 블록체인과 동일하게 인증 후 사용자 등록이 되어야 한다.

금융 트랜잭션 측면에서 보면, Hdac 퍼블릭 블록체인과 Hdac 프라이빗 블록체인의 가치 변화가 없는 토큰 사이의 트랜잭션을 생각해 볼 수 있다. Hdac*T 트랜잭션은 특정한 기업 또는 특정 목적을 위해 사용될 수 있다. 이 경우 둘 사이의 교환 비율을 정하고 거래소를 통해서 교환이 이루어질 수도 있다. 현재 단일 블록체인 내에서 HDAC과 Hdac*T 사이의 교환이 이루어질 수 있도록 설계되어 있다. 향후 블록체인 사이의 교환은 브리지 노드 또는 거래소를 통해서 이루어지게 된다.

우리는 대규모 IoT 디바이스가 발생시키는 트랜잭션을 효과적으로 처리하기 위한 방안을 검토

했다. IOTA의 트랜잭션 처리 구조나 속도 및 이더리움의 차세대 네트워크에 대해서 조사를 했다. 수만~수십만 tx/sec 이상의 대규모 트랜잭션을 처리하기 위해서는 단순히 물리적인 네트워크 성능이나 컴퓨팅 성능만으로는 한계가 있다. 단일 블록체인 상에서는 제한된 수준의 트랜잭션만 처리가 가능함을 테스트 네트워크로 확인했다. 따라서 높은 수준의 트랜잭션 처리는 다수의 분리된 프라이빗 블록체인으로 각각 처리하고, 별도의 상위 블록체인을 통해서 정보를 통합하는 방식이 적절하다고 판단했다.

특히 글로벌 환경에서 작동하는 퍼블릭 블록체인은 처리 속도가 매우 제한적인데, 이유는 네트워크 전송 지연 문제와 수많은 노드에 대한 트랜잭션 및 블록 동기화 문제 때문이다.

Hdac 퍼블릭 블록체인 또한 글로벌 인터넷 환경에서 최적의 속도를 낼 수 없는데, 원인이 시간에 따른 네트워크 처리 속도의 변화와 블록 동기화에 따른 지연 문제임을 확인했다. 따라서 향후 대규모 트랜잭션 처리 블록체인은 용도별 다수의 프라이빗 블록체인으로 구성된 계층적인 또는 분산된 구조의 블록체인들의 네트워크라고 할 수 있다. 우리는 이런 유형의 블록체인을 구현하기 위해서 계속 연구하고 노력하겠으며, 결과가 나오는 대로 온라인에 공유해서 전체 블록체인 생태계의 발전을 위해 노력할 것이다.

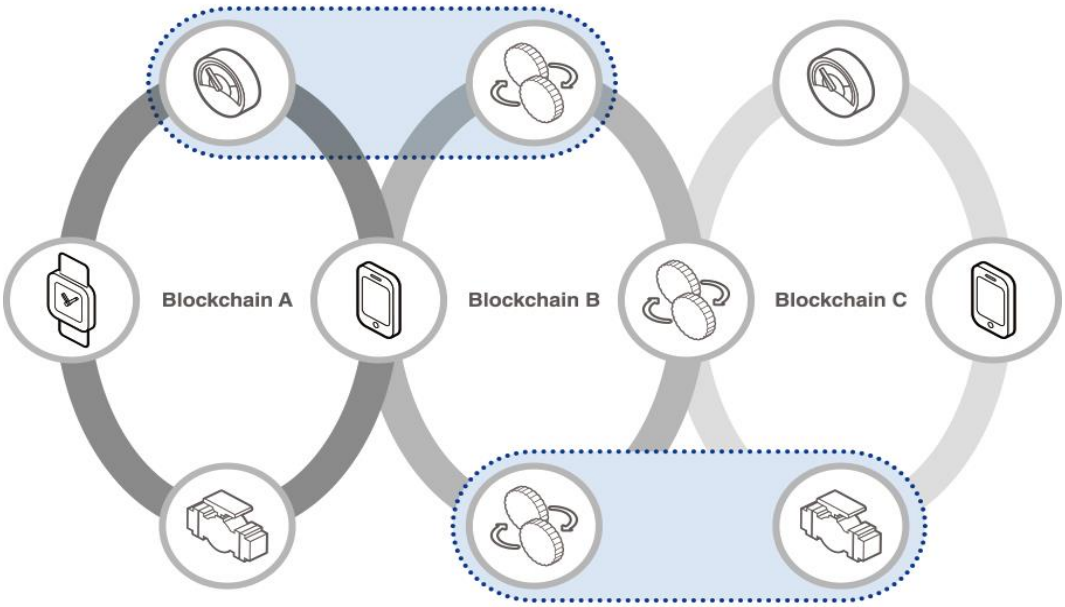


그림 3. 계층적 구조로 연결된 블록체인

IoT와 보안

세계 산업시장에서 ICBM (IoT, Cloud, Big Data, Mobile) 등이 신 산업혁명의 핵심 기술로 주목받고 있는 가운데 IoT는 다양한 경제적 가치와 더불어 사용자의 효율성과 편의성을 한층 높여줄 것으로 기대된다. 그러나 이러한 긍정적인 성과를 달성하기 위해서는 사물 간의 연결성이 보장되고 신뢰도가 확보되어야 한다. 즉, 인터넷 연결의 편리함이 내포하고 있는 불신과 보안 위협 요인을 제거하는 것이 우선적으로 해결되어야 할 과제이다.

IoT의 핵심 키워드는 '스마트'와 '연결'이다. 기존에 인터넷 접속과 전혀 관련이 없었던 사물이나 장치들이 인터넷에 연결되어 다양한 서비스로 재탄생 되기 때문에 기존 인터넷 환경에서 발생할 수 있는 모든 위협과 취약점을 그대로 상속받을 수 있다. 한편, 외부 침입에 의한 보안 취약성과는 별개로 IoT 기반의 서비스에서 실시간 수집되는 데이터들은 사생활 침해 문제를 유발시킬 수 있어 보안성이 전제되지 않은 연결은 프라이버시 침해뿐만 아니라 사회적 문제가 될 수 있다. IoT를 기반으로 형성될 초연결 사회의 근간에는 신뢰 기반의 P2P 네트워크 체계와 신뢰를 전제로 할 수 있는 IoT 디바이스 간 계약 및 운영이 필수적이며 이것을 전제로 고도화된 트랜잭션 시스템 체계로 진화할 수 있을 것이다.

트랜잭션 혁신과 M2M 트랜잭션

신 산업혁명에서 빼놓을 수 없는 핵심 단어 중의 하나는 IoT이며, 인터넷을 기반으로 모든 사물을 연결하고 사람과 사물, 사물과 사물 사이의 정보를 상호 소통하는 지능형 기술 및 서비스를 통칭한다. 그러나 IoT는 사물과 사물이 연결되는 네트워킹 기술과 각종 서비스에 적합하도록 가공하는 기술, 통신하는 인터페이스 기술, 대량의 데이터를 저장하고, 처리하는 분산 처리하는 기술들이 필수적이며, 해킹이나 정보 유출을 대비한 보안 기술들을 필요로 한다.

이와 같은 IoT 기술을 기반으로 한 다양한 서비스들이 등장하고 있는 가운데, 블록체인 상의 많은 사물들이 IoT Contract에 의해 지능적으로 작동되고, 다양한 산업에서 서비스가 가능해질 것으로 기대된다. 특히, IoT Contract는 디바이스를 제어하고, 접근을 통제하며, 사물 간의 소통에 도움을 줄뿐만 아니라, 익명성을 보장하고, 여기에서 발생하는 모든 트랜잭션은 원장은 기록이 된다. 기록된 원장은 IoT 빅데이터로서 머신 러닝의 학습 데이터로 사용되어 최종적으로는 인공지능(AI)를 통한 비용절감 효과를 얻을 수 있을 것으로 기대된다.

블록체인에서 IoT 디바이스 간의 신뢰 확보

IoT의 연결 구조와 블록체인의 네트워크 구조는 아래 그림과 같이 매우 유사하다.

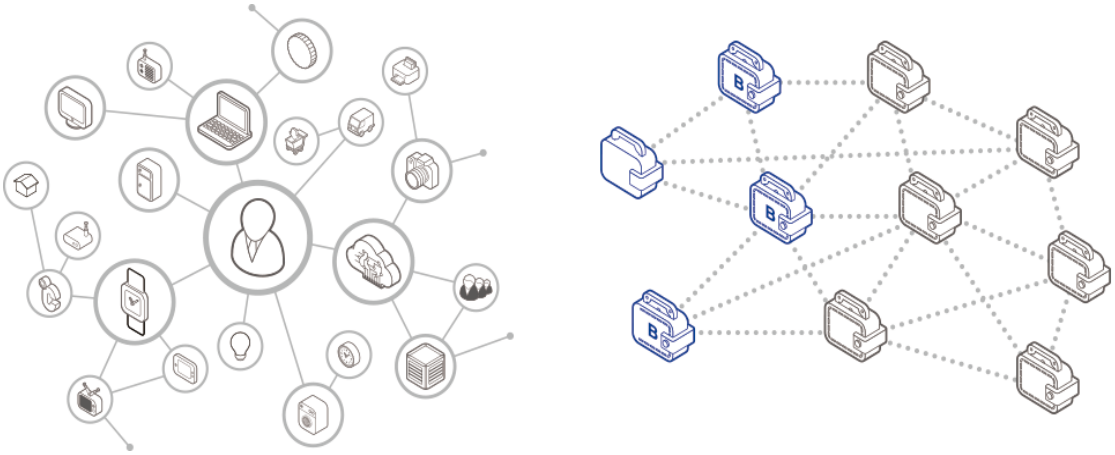


그림 4. IoT 연결 구조와 블록체인 네트워크 구조 비교

블록체인을 IoT와 융합하면 사물들 사이의 신뢰성 있는 연결과 안전한 처리를 보장하기 위한 조건인 기밀성(Confidentiality)과 무결성(Integrity)을 쉽게 구현할 수 있다. 이것은 연결된 사물들이 위조(Fabrication)와 변조(Modification) 공격에 대응하고, 통신하는 상호 간의 신뢰성을 높여주게 된다. 특히 블록체인은 블록 내에 담겨있는 거래 원장에 대해 복잡한 수학적 암호화 및 분산 정보 복제를 통해 외부 공격에 뛰어난 대응 능력을 포함하고 있다. 또한 블록체인은 중앙 집중 방식이 아닌 탈 중앙 방식을 사용하고 있어, 해커들에게 공격 대상을 파악하기 어렵게 하는 장점을 갖고 있다.

이와 같은 특징들은 IoT 디바이스에 대한 개별 공격이 전체 디바이스에 미치는 영향을 최소화하게 된다. IoT 디바이스들 사이에서 제공되는 신뢰 기반의 서비스들을 다음과 같이 요약해 볼 수 있다.

- P2P와 분산 구조를 통해 공격 대상이 분산되어 있어 공격자에게 공격 대상을 정하기 어렵게 한다. → 프라이빗 블록체인의 경우, 분산 컴퓨팅의 전개가 한정되는 경우 Safe IP와 같은 네트워크 보안을 통하여 트랜잭션을 보호하여 보안 이슈를 해결할 수 있다.
- 신뢰 기반 네트워크를 통한 투명성 유지할 수 있으며, 참여자의 거래 내역을 공유하고 내역을 신뢰성 있게 보관한다.

- 거래 내역의 무결성을 보장하여 위조 및 변조 공격에 대응할 수 있으며, 모든 참여자가 거래 내역을 증명한다.
- 거래의 주체가 되는 IoT 디바이스에 대한 인증 및 권한 부여 절차가 필요하다.
- 퍼블릭 블록체인의 경우 분산에 따른 구축 및 유지의 효율성을 증대시킬 수 있으며, 탈중앙화로 인해 구축 비용의 절감과 자원의 효율적인 분배로 효율성을 증대한다.

결론적으로 블록체인 네트워크는 상호 송수신할 다양한 데이터들뿐만 아니라, 분산 IoT 환경에서 서비스 제공자와 사용자 모두에게 신뢰할 수 있는 환경을 제공해 줄 것이다.

Hdac의 특징

Hdac 플랫폼의 주요 기능

Hdac 블록체인의 주요한 기능은 다음과 같다.

Hdac 프라이빗 블록체인에서는 사용자 정의 디지털 토큰인 Hdac*T를 제한 없이 다양한 용도로 만들고 사용할 수 있으며, 토큰의 명칭을 정의하거나 하부의 허가된 관리자가 자유롭게 토큰을 만들어서 배포할 수도 있다. 이 토큰은 HDAC와 유사한 용도로 사용할 수도 있다. 또 특정한 기업이나 특정한 목적으로 발행된 Hdac*T를 필요에 따라 적절한 비율로 HDAC와 교환할 수 있는 방안도 제시할 수 있다.

Hdac 프라이빗 블록체인에는 다양한 권한 관리 기능이 있으며, 최초의 블록체인 노드를 구축한 관리자가 다른 노드에게 권한을 부여할 수 있다. 권한의 유형으로는 접근 권한, 송수신 권한, 채굴 권한, 토큰 발행 권한 등을 지정할 수 있으며, 운영 중에도 효과적으로 변경할 수 있다.

Hdac 블록체인은 편리한 설치와 설정 기능을 제공하며, 간편하게 사용자가 정의하는 블록체인을 구성할 수 있다. 또한 새로운 노드 구성도 간단해서, 한 줄의 명령만으로 기존의 블록체인에 풀노드로 참여할 수 있고 모든 구성은 자동으로 복제되어 공유된다. 프라이빗 블록체인의 경우에는 ePoW와 Round Robin 방식의 블록 생성을 모두 지원한다.

개선된 다중 사용자 서명을 지원하여 안전한 에스크로 거래와 같은 서비스를 지원할 수 있다. 또한 Hdac 프라이빗 블록체인에는 특정한 두 사용자 사이의 암호화된 채널을 만들어서 통신할 수 있는 기능도 제공한다.

이와 함께 IoT 제어 및 다양한 응용 분야에 특화된 프라이빗 블록체인을 위한 기능과, 블록체인과 블록체인의 연결을 위한 기반 기술을 지속적으로 개발하고 제공할 예정이다. IoT와 관련된 상세한 내용은 Hdac 블록체인 기술 로드맵에서 명시한다.

HDAC은 Hdac 퍼블릭 블록체인을 기반으로 하고 있으며, 일반적인 블록체인의 특징을 모두 수용하고 있다. 기존의 블록체인이 가지고 있는 한계들은 시간이 흐름에 따라 진화 과정에서 하나 둘씩 나타나고 있으며 Hdac 블록체인은 블록체인을 기반으로 하는 타 플랫폼과의 차별성을 강조하면서 효율성이나 보안 측면, 기능성과 신속한 운영 측면에서 다른 플랫폼과 구별될 수 있도록 몇 가지 기능을 수정하거나 보완하였다. 합의 알고리즘 부분에 있어서 기존의 PoW 방식을 발전시켜 효율적인 에너지 사용을 유도하고 공평한 분배가 되도록 하는 ePoW 합의 알고리즘을 제시

한다. 또한 Lyra2Rev2 ASIC-resistent 알고리즘을 적용하여 채굴 독점을 제한한다.

먼저 블록체인의 문제점으로 대두되고 있는 데이터 적재 부분에 있어서 기존 블록체인의 블록과 트랜잭션에 추가되는 데이터의 제한적인 용량을 유동적으로 사용할 수 있도록 수정하였으며, 이를 통해서 블록체인을 이용한 다양한 응용이 가능하게 되었다.

그리고 Hdac 프라이빗 블록체인의 경우, 보안성이 강화되어야 하므로 하드웨어 형태의 양자 난수 발생기를 통해 난수를 생성함으로써, 난수 패턴 분석을 통한 해킹 가능성을 배제하고 보안성을 높일 수 있다.

또한 관리 권한을 부여할 수 있는 Permission 개념이 추가되어 프라이빗 블록체인에서 특정 사용자만이 블록체인의 풀노드(Full Node)로 참여할 수 있다. 또한 Hdac 프라이빗 블록체인은 사용자가 정의한 토큰(Hdac*T)을 생성하고 유통에 활용할 수 있는 서비스 모델을 제시하며, 용도에 따라 개별적인 프라이빗 블록체인을 구축할 수도 있다.

우리는 실시간 처리용 IoT 환경을 구현하는데 적합한 다수의 블록체인을 검토했다. 비트코인을 비롯한 대부분의 퍼블릭 블록체인은 실시간 처리에 적합한 모델을 적용하기 어렵다고 판단했다. 이더리움은 IoT 환경에 적합한 모델을 가지고 있지만, 대부분의 IoT 디바이스가 C/C++언어로 주로 개발되며 CPU와 메모리 성능이 제한되는 환경이어서 IoT 디바이스에 이더리움의 Smart Contract를 탑재하기에 용이하지 않다고 판단했다. 하지만 향후 이더리움과 호환성을 가지도록 개발될 수는 있을 것이다. IOTA는 대량의 트랜잭션을 소화할 수 있는 가능성이 있지만, 우리가 지향하는 표준 블록체인 기술이 아니며 기술적인 세심한 검토가 필요하다는 판단에서 제외했다. 그 외 다수의 제품을 검토한 후 가장 보편적으로 사용되는 비트코인에 기반을 두면서 프라이빗 블록체인을 효과적으로 구현할 수 있는 멀티체인(Multichain)을 선정하게 되었다.

Hdac 블록체인은 멀티체인에서 개선되었으며, 멀티체인은 비트코인에서 개선된 블록체인이다. 우리는 특히 IoT를 효과적으로 지원하고, 다양한 서비스를 신속하고 효과적으로 프라이빗 블록체인에서 제공하기 위한 블록체인을 탐색했으며, 이에 적합한 블록체인을 선정하고 개선을 수행했다. 따라서 Hdac 블록체인은 비트코인의 특성과 프라이빗 블록체인에 최적화된 특성을 가지고 있다. Hdac 블록체인은 IoT를 위한 플랫폼으로 작동하기 위한 기반을 제공한다. 빠른 트랜잭션 처리 속도와 트랜잭션 확장성을 바탕으로 산업, IoT, 유통, 물류, 공공 자료 관리, 전자 투표 등의 다양한 서비스 분야에 활용될 수 있을 것으로 전망한다.

비트코인은 약 10 분마다 블록을 하나씩 생성하며, 이더리움은 약 12 초마다 하나의 블록이 생성된다. 네트워크에 공유되는 시간을 고려할 때 전송된 트랜잭션 결과를 확인하려면 1~2 분 이상

의 시간이 소요된다. 이를 고려해 볼 때 비트코인은 약 7 tps이며, 이더리움은 약 25 tps이다. 특히 비트코인은 현재 블록 사이즈가 최대 1MB 로 제한되어, SegWit2x 등을 통해서 블록 사이즈를 늘리는 대안이 제시되고 있다.

Features	Bitcoin	Hdac	Ethereum
Main Features	Financial Transactions (Bitcoin script)	IoT friendly blockchains, Public/private blockchains	Smart Contracts (Solidity, Serpent etc.)
Consensus Algorithm	PoW	ePoW, Trust-based	Current : PoW Future : CASPER(PoS)
Transaction Speed	7 tx/sec	~160 tx/sec (public)* ~500 tx/sec (private) 1000 tx/sec (target)	25 tx/sec
Block Time	10 minutes	3 minutes	12 seconds
Block Size	1MB	Dynamic (Max. 8 MB)	Dynamic
Extra Data	80 Byte (OP_RETURN)	Dynamic (Max. 4 KB)	Dynamic (5 gas / byte)
Topology	Public blockchain	Public/private blockchains, Permissioned blockchains	Public blockchain, Permissionless blockchain

* 서버 성능 및 네트워크 환경에 따라 위 내용은 변동될 수 있다.

표 1. 암호화폐 속성 비교

Hdac 블록체인은 이러한 단점들을 보완하고 제3 세계의 낙후된 트래픽 속도를 고려해서 블록 생성 주기는 3분으로 정했다. 최대 블록 사이즈(Block Size)는 8MB이며 트랜잭션 양에 따라 가변적으로 대응하도록 하였다.

이렇게 수치를 결정한 이유는 제3 세계의 일반적인 평균 인터넷 트래픽 속도가 1~2Mbps 정도에 불과하다. 따라서 Hdac 블록체인은 이러한 속도의 수분의 1 정도만 수용할 수 있다면, 풀노드를 운영할 수 있는 환경을 조성하는 방안을 제시하기 위해서이다. 일반적인 지갑을 통한 트랜잭션 처리는 더 낮은 트래픽 환경에서도 이용이 가능하다. Hdac 프라이빗 블록체인으로 제한된 내

부 환경에서 테스트한 결과 비트코인에 비해 이론적인 수치에 근접하는 약 20배 이상의 대규모 트랜잭션에서 안정적인 처리가 가능함을 확인했다.

Hdac 블록체인은 향후 IoT 지향 블록체인으로서 트랜잭션에 대용량의 부가적인 데이터를 처리할 수 있는 방안을 제시한다. 또한 향후 Hdac 블록체인이 지향하는 IoT 보안과 응용 서비스 확장을 위해 필요할 경우, 트랜잭션 크기는 동적으로 적응이 가능하다.

합의 알고리즘

블록체인은 새로운 블록을 연결하기 위해 유효한 블록임을 검증하는 단계에서 블록체인 네트워크에 참여하는 모든 노드가 합의하는 데 필요한 기본 조건들이 있다. 모든 참여 노드(풀노드)는 동일한 과정으로 동일한 결과 값을 확인할 수 있어야 하며, 모든 검증 과정은 같은 값을 결정해야 한다. 그리고 결정된 값은 특정 노드에 의해 제안된 것이어야 한다.

Hdac 블록체인은 작업 증명(PoW) 방식을 기본으로 하며, 신뢰 기반의 프라이빗 블록체인을 위한 합의 알고리즘에 대한 채굴 방식도 지원하고 있다.

여기서 블록을 생성하기 위한 작업을 '마이닝(Mining)' 또는 '채굴'이라고 하며, 마이닝에 참여한 노드를 '마이너' 또는 '채굴자'라 한다. Hdac 퍼블릭 블록체인은 거래가 시작되면, 마이너들에게 브로드캐스트하여, 거래를 알리고 참여를 독려하며, 마이너들은 생성된 블록을 검증하기 위해 연산을 수행한다. 블록체인의 합의 알고리즘에는 PoW(Proof of Work), PoS(Proof of Stake), DPoS(Delegate Proof of Stake) 등이 있으며, 이와 같은 합의 알고리즘은 다수의 참여자가 일정 시간이 소요되는 연산 과정을 수행함으로써 누가 블록을 생성할지를 결정한다.

이러한 합의 알고리즘은 경쟁적 채굴 과정에서 하나의 블록 보상을 획득하기 위해 해싱 파워를 소모적으로 사용함으로써 에너지 낭비적인 요소가 강하다. 또한 PoW 이든 PoS 방식이든 더 큰 해싱 파워를 가졌거나 더 많은 지분(Stake)를 가질수록 보상 혹은 부의 축적이 한 쪽으로 집중 될 수 있는 문제를 내포하고 있으며, 실제로 특정 지역의 마이닝 풀(mining pool)에서 채굴이 집중되는 현상이 발생하고 있다.

Hdac 블록체인은 새로운 블록을 생성하고 블록체인에 연결하기 위한 합의 알고리즘으로 ePoW를 사용한다. ePoW (PoW based on equitable chance and energy-saving)는 평등한 기회와 에너지 절약에 기반한 PoW를 의미한다. Hdac 블록체인의 합의 알고리즘은 이 두 가지를 기본 철학으로 삼고 있다. 그리고 특정한 채굴자에게 블록 보상이 집중되는 것을 막기 위해 Lyra2Rev2 ASIC-resistent 알고리즘을 추가했다.

ePoW 합의 알고리즘은 작업 증명에 참여하는 노드의 개체 수 감소를 방지하고, 다수의 마이닝 노드가 참여할 수 있는 동기를 부여할 수 있고, 결과적으로 채굴 경쟁을 위한 과도한 컴퓨팅 파워 투입에 따른 에너지 낭비 방지와 채굴 기회의 공정한 기회 분배를 도모하고자 하는 의도에서 출발하였다.

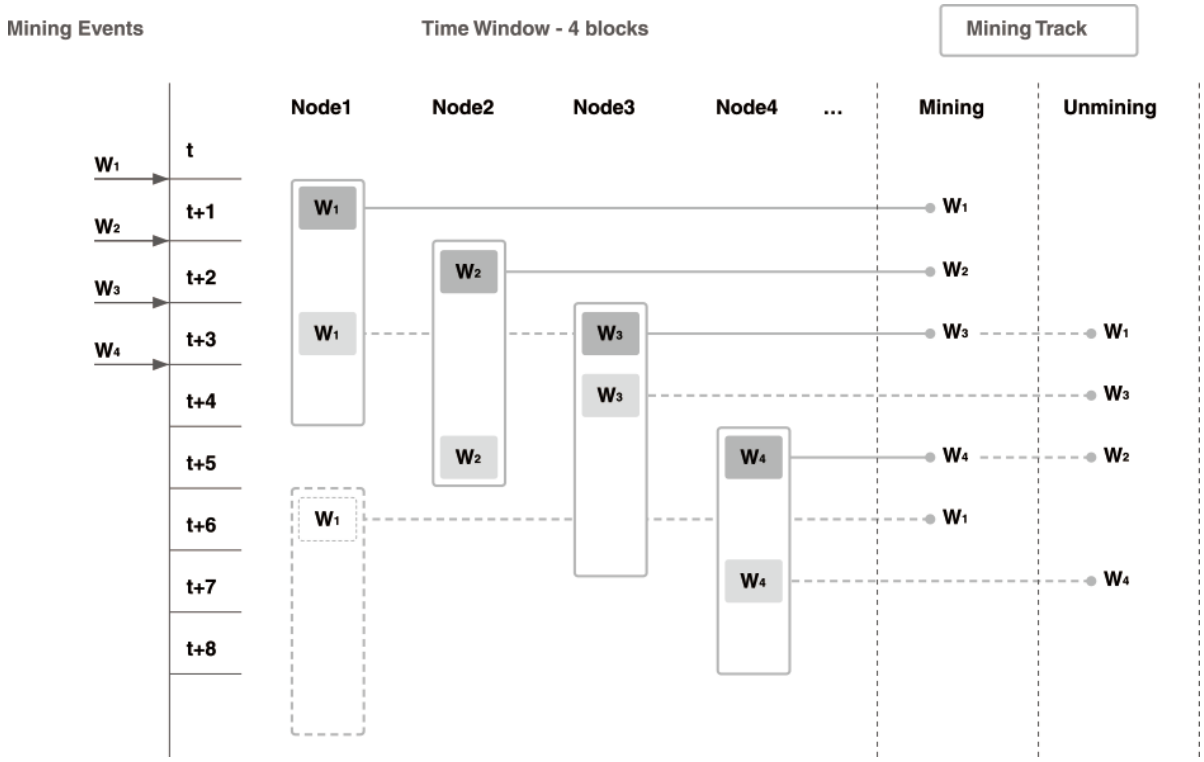


그림 5. ePoW 합의 알고리즘

Hdac 블록체인의 ePoW는 블록 윈도우(block window) 개념을 적용하여 채굴 독점/과점을 줄이도록 하는 합의 알고리즘이다. 또한 채굴 성공 후 블록 윈도우 적용 기간 동안은 자발적으로 채굴 시도를 하지 않도록 하여 해시 계산에 소모되는 낭비적 에너지를 줄이도록 하는 알고리즘이다. 어떤 노드가 채굴에 성공할 경우 블록 윈도우 적용 기간 동안은 새로운 블록을 채굴할 수 없다. 설사 욕심 많은 노드가 이러한 메커니즘을 무시하고 새로운 블록 채굴에 성공해도 Hdac 블록체인 전체 네트워크에서 유효한 블록으로 인정받지 못하고 때문에 채굴에 에너지를 사용할 필요성이 없어지기 때문이다.

블록 해시는 난이도에 따라 데이터의 규격을 만족해야 하며 또한 주어진 블록 윈도우 내에 있지 않아야 한다. 이 블록 윈도우 사이즈는 시간 함수, Ws = f(t) 형태로 표현될 수 있다. f(t)는 시

간에 비례하여 증가하는 함수이며, 따라서 윈도우 사이즈는 시간이 흐름에 따라 점진적으로 증가하게 된다. 이는 곧 초기 참여자에게는 큰 기회가 있으며, 시간이 지남에 따라 특정 채굴 노드가 채굴을 독점하기가 점점 더 어려워지고, 더 공평한 분배가 이루어질 수 있다는 의미이다.

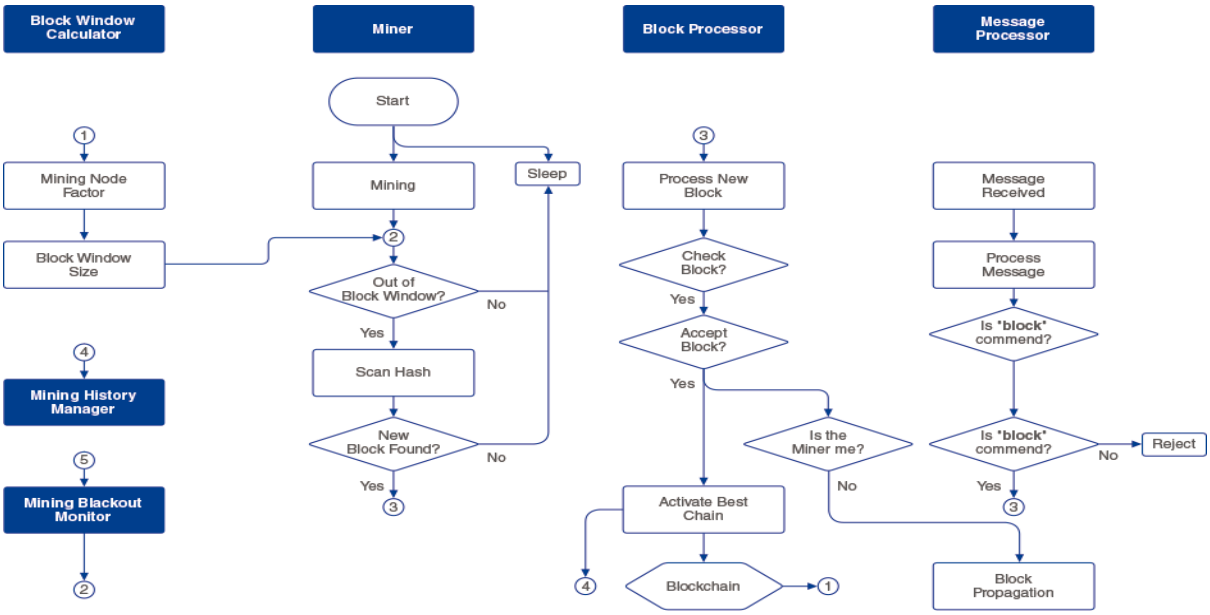


Figure 6. ePoW flow chart

그림 6. ePoW Flow Chart

ePoW 블록 윈도우는 작업 증명 주기 안에 채굴을 달성한 마이닝 노드에 대해 연속된 채굴 시도에 제약을 부여하기 위해 적용된다. 블록 윈도우 사이즈(Ws)는, f(t) = [(N*0.7)x(현재까지의 누적 블록 수(t))]/(10년간 누적 블록 수(tm))로 정의 되며, 노드 인자(N)는 최근 채굴 성공 노드 목록에서 산정된다. 여기서 최대 블록 윈도우 사이즈(Wm) 도달 시점이 10년인 것은 총 발행량의 80% 이상에 도달하는 시점으로 정하였기 때문이다.

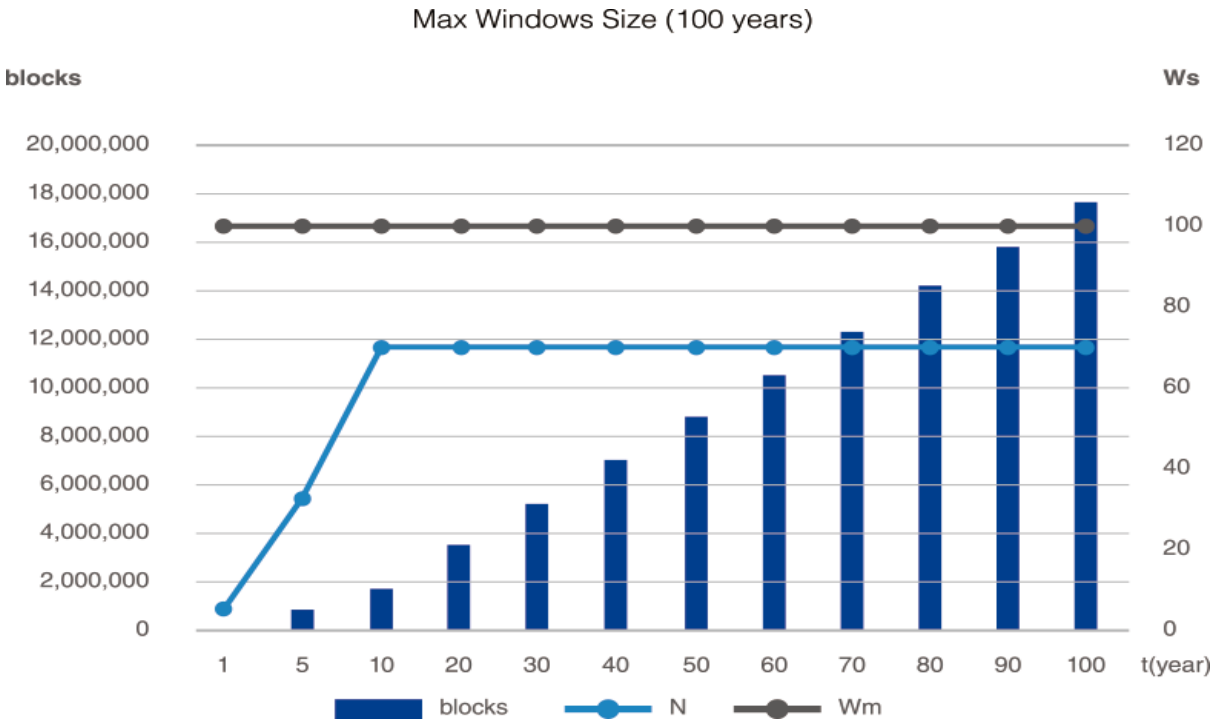


그림 7. 블록 윈도우 시뮬레이션(100 년)

채굴 노드 인자를 100으로 하여 100년 간의 블록윈도우 사이즈를 시뮬레이션 할 경우 위의 그림과 같다. 제네시스 블록이 시작된 시점부터 블록 윈도우는 서서히 증가하고, 최대 블록윈도우 사이즈에 도달한 시점(tm) 이후에는 노드 인자에 의해 크기가 증가하거나 감소하게 된다.

우리는 ePoW에 대한 개발을 완료하였으며 Lyra2Rev2 ASIC-resistant 알고리즘 적용도 완료했다. ePoW 합의 알고리즘은 건전한 채굴 환경 조성을 위해 다양한 기술적인 방법을 지원할 것이며, 채굴 노드의 보안성을 강화하기 위해 별도의 ASM(Advanced Security Module)을 개발 중이며 이것을 보안강화 옵션으로 선택할 수 있도록 할 것이다.

양자 난수를 활용한 보안 강화

블록체인 기반의 플랫폼은 높은 보안성으로 이미 검증되었다. 블록체인에서 사용되는 프라이빗 키, 퍼블릭 키, 지갑 주소 등은 유사 난수(Pseudo Random Number)를 이용해서 만들어진다. 최근에 발생한 사례를 살펴보면, 유사 난수의 패턴을 분석하여 특정 목적에 사용되는 값을 만들어 냄으로써 유사 난수의 보안 취약점이 발견되었다. 이러한 취약점을 보완하기 위한 다양한 시도가 있었으며, 그 중 이론적으로 패턴 분석이 불가능하다는 양자 난수(Quantum Random Number)를 이용한 방법이 등장했다. Hdac 프라이빗 블록체인의 경우 난수 생성기를 양자 난수

로 대체할 수 있는 방안을 제시한다.

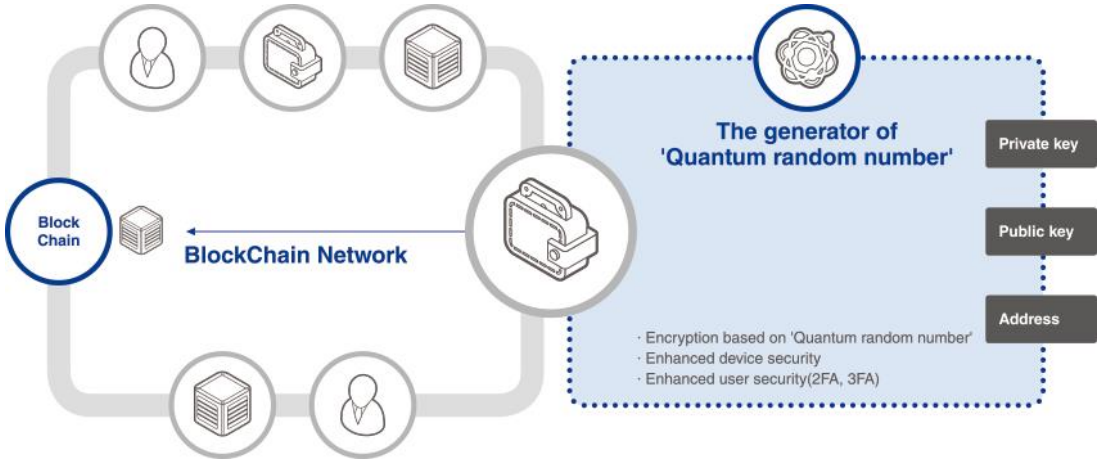


그림 8. 양자 난수를 활용하여 향상된 디바이스 보안

블록체인은 유사 난수를 이용하여 프라이빗 키, 퍼블릭 키, 지갑 주소를 만들어내고 있다. 이러한 프로세스에 의해 만들어진 지갑 주소는 SHA256 해싱을 통하여 해시 값으로 표현된다. 또한 표기법에 따라서 주소의 시작 글자는 다음과 같이 구성되며, Hdac 블록체인 'H'를 사용한다. 이렇게 주소 마다 첫 문자를 다르게 하는 것은 특정 코인 사용자가 다른 코인으로 화폐를 전송하지 못하도록 하는 일종의 보호 체계라고 볼 수 있다. 특정 코인이 같은 이니셜을 사용할 경우, 주소의 첫 문자가 중복되는 상황이 발생하게 되기 때문에 타 코인으로 인한 전송 오류를 범할 수 있다. 따라서 Hdac 블록체인은 이를 대비하기 위하여 checksum 부분에 "Hdac" 문자열을 추가했다.

HDAC 발행, 채굴 및 보상

비트코인과 비교하여 Hdac 블록체인의 HDAC 발행 정책은 다음과 같다.

Hdac 블록체인의 총 HDAC 발행량은 12,000,000,000HDAC이다. Hdac 블록체인의 최초 블록 보상(First Block Reward)은 5,000HDAC으로 시작한다. 블록 생성 주기는 3분이고, 1,032,000 블록마다 보상은 절반으로 줄어드는 반감기가 설정되어 있다. 즉, 최초 블록(Genesis Block) 생성 이후 약 71개월마다 블록 보상은 절반으로 줄어든다. 총 HDAC 발행량의 7%는 Hdac 블록체인의 기술 구현과 거래 활성화를 위한 인프라 및 생태계 조성 및 유동성 관리에 사용될 예정이며 7%는 Presale와 TGE에서 Hdac 재단에 기부한 참여자에게 분배될 예정이다.

이러한 메커니즘은 발행량이 무한대로 늘어나 가치가 낮아지는 인플레이션 보다는 총 발행량이 고정되어 있어 HDAC의 본질적인 가치를 유지할 목적을 지닌 정책이다. 구매자와 판매자의 비축 본능이 만나는 지점의 균형 가격(Equilibrium Price)이 유지될 수 있을지는 더 지켜봐야 한다.

Hdac 블록체인 네트워크에 참여하여 채굴을 원하는 채굴자는 블록 보상과 함께 거래 수수료를 보상으로 받게 된다. 약 6년마다 반감되는 블록 보상은 한 블록에 담기게 되는 트랜잭션 수가 점차적으로 늘어남으로써 반감기에 따른 채굴 보상액을 채워준다.

Hdac 블록체인 기술 로드맵

프라이빗 블록체인 네트워크의 구성

프라이빗 블록체인 네트워크는 인증을 거친 후에 등록이 되고 블록체인 네트워크에서 작동이 가능하다. 따라서 누구나 네트워크에 접근하는 퍼블릭 블록체인과는 성격이 다르다고 할 수 있다. 프라이빗 블록체인 네트워크의 구성 요소는 아래와 같다.

- **블록체인 노드**: 풀노드로 모든 트랜잭션 블록을 기록. 관리자가 수행한 사용자-디바이스, 디바이스-디바이스 사이의 제어, 트랜잭션, 관리와 관련된 설정 정보를 저장함
- **관리자**: 블록체인에 사용자, 게이트웨이, 디바이스를 등록하고 이들 사이의 접근 권한을 부여하는 사람. 설정 내용은 풀노드에 안전하게 저장되며, 네트워크를 통해서 아래의 사용자, 게이트웨이, 디바이스로 전달되며 각 사용자와 디바이스는 자신과 관련된 최신 설정을 유지함. 기존의 IoT 운영 환경과 유기적으로 통합할 수도 있음.
- **사용자**: 블록을 저장하지 않는 단순 노드로 작동되는 프로그램을 가진 사람 또는 디바이스.
- **게이트웨이**: 다수의 더미 디바이스나 센서를 제어하기 위한 장비로 IoT Contract 내용을 해석한 다음 더미 디바이스나 센서에 전달할 수도 있다. 각 디바이스나 센서는 개별 주소와 연결될 수도 있다.
- **디바이스**: 블록을 저장하지 않는 단순 노드 또는 게이트웨이에 연결되는 장치로 개별 주소와 대응하며 IoT Contract 내용을 해석하고 실행할 수도 있다.

사용자는 프로그램이 첨부된 IoT Contract를 게이트웨이나 디바이스로 전송한다. 디바이스는 전송된 IoT Contract를 수신 후 해석하고 실행을 한다. 사용자는 명시적으로 권한이 부여된 게이트웨이나 디바이스에 대해 접근하거나 제어하는 트랜잭션들을 전송할 수 있다.

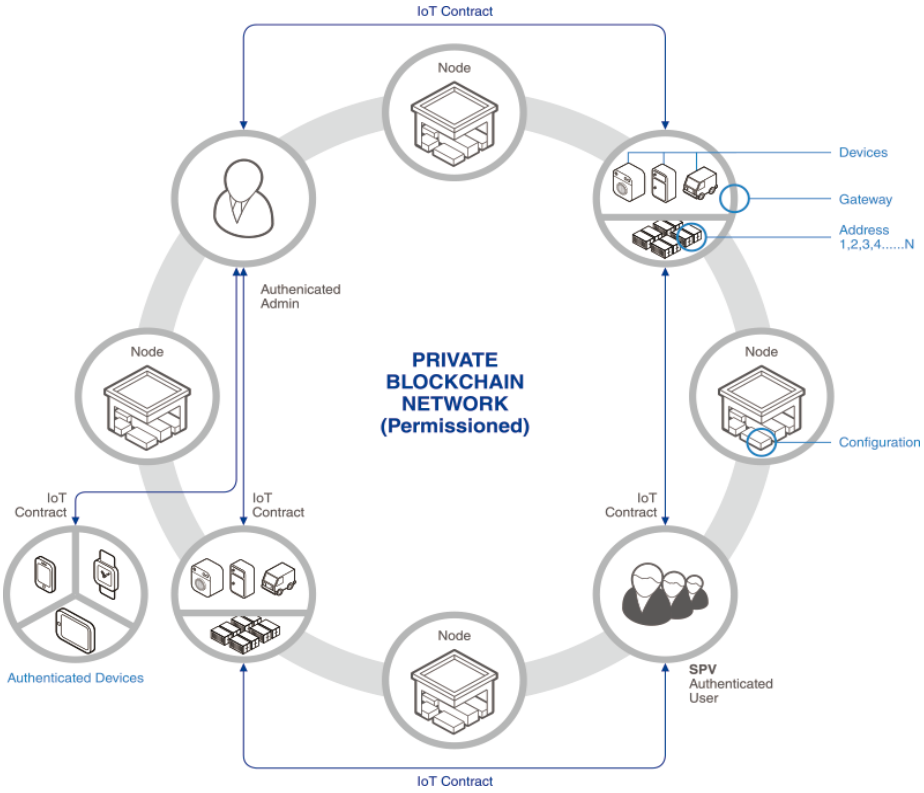


그림 9. 프라이빗 블록체인 네트워크 구조

프라이빗 블록체인상의 사용자-디바이스 매핑

프라이빗 블록체인 상의 사용자는 디바이스를 제어하기 위한 명확한 접근 권한 규칙에 따라 디바이스에 접근할 수 있어야 한다. 그리고 사용자는 설정에 따라 특정한 장비를 제어하거나 장비의 상태를 읽기만 할 수 있어야 하고, 특정한 장비에는 일반 사용자의 접근이 불가능하게 할 수도 있어야 한다. 여기에 따라 관리자는 사용자와 디바이스 또는 게이트웨이의 주소별 접근 권한을 설정할 수 있다. 이 접근 권한 설정은 블록체인 네트워크의 모든 풀노드에 저장되며, 또한 모든 노드와 게이트웨이, 디바이스에 전파되어 설정이 공유된다. 사용자와 디바이스에 대한 접근 및 제어, 트랜잭션 권한은 블록체인 내에 기록이 안전하게 보존되며, 트랜잭션이 발생할 때 이 기록과 대조하여 권한이 확인된 후에, IoT Contract가 수행될 수 있다.

일반적인 IoT 운영 환경에서는 이미 이러한 권한 부여가 되어 있는 경우가 많다. 따라서 프라이빗 블록체인에서는 이미 운영 중인 IT 환경과 결합하여 활용하는 방식도 유용할 것으로 본다.

권한 매핑의 유형은 아래와 같다.

- 사용자-디바이스/게이트웨이 매핑

- 사용자-사용자 매핑
- 디바이스/게이트웨이-디바이스 매핑

또한 매핑 권한은 다음과 같다.

- 접근 권한: 장비에 접근할 수 있는 권한을 나타낸다. 최소 접근 등급을 지정할 수 있을 것이다. 사용자나 디바이스는 등급을 가지며, 특정한 등급 이상만 접근이 가능하다. 접근이 불가능한 경우 아래의 모든 권한은 사용할 수 없다.
- 상태 조회 권한: 현재 상태를 읽을 수 있는 권한이며, 세부 권한은 별도의 문자열로 명시할 수 있고, 해당 디바이스에서 해석하여 적용 여부를 판단할 수 있을 것이다.
- 상태 제어 권한: 디바이스를 제어하거나 상태를 바꿀 수 있는 권한이며, 세부 권한은 별도로 명시할 수 있고, 해당 디바이스에서 해석하여 적용 여부를 판단할 수 있을 것이다.
- 트랜잭션 권한: 트랜잭션을 해석해서 자동으로 기기를 제어할 수 있는 권한이다. 트랜잭션의 수행 시간은 주어진 토큰에 따라서 제한될 수가 있다.
- 기타 권한 (디바이스별 상세 권한 지정): 기타 세부 권한은 별도의 코드나 문자열로 명시할 수 있고, 해당 디바이스에서 해석하여 적용 여부를 판단할 수 있다. 이 내용은 디바이스에 의존하는 방식이므로 모든 디바이스에 대한 구체적인 제어 방안은 여기에 명시하지 않는다.

프라이빗 블록체인 네트워크를 이용하는 모든 트랜잭션은 이 접근 권한에 따라서 전송 여부가 결정이 된다. 즉, A라는 사용자가 B라는 디바이스에 접근할 권한이 없는데도 불구하고 A에서 B로 가는 트랜잭션이 발생한 경우, B 디바이스 및 모든 블록체인 노드에서 이 트랜잭션을 거부하게 된다. 이 경우, 오류는 블록체인 내의 침해 탐지 노드에 통보될 수 있으며, 관리자는 즉시 내용을 확인할 수 있게 된다.

관리자가 최초의 사용자-디바이스 또는 디바이스-디바이스 간의 권한을 설정한 후, 블록체인 네트워크에 변경 내용이 생기는 경우 각 사용자 및 디바이스의 권한이 조정될 수 있다. 또한 디바이스의 추가, 삭제가 일어나는 경우 이에 따른 매핑을 수행해야 한다. 설정에 따라서 새로운 디바

이스가 추가되는 경우 기본적인 권한을 지정할 수도 있을 것이다.

디바이스 별 접근 권한 매핑 과정은 경우에 따라 매우 복잡할 수도 있다. 따라서 이러한 권한 매핑을 효과적으로 처리하기 위해서, 사용자 또는 게이트웨이, 디바이스를 특정한 그룹으로 묶어서 처리하는 방안이 시도될 수 있다. 또는 복잡한 매핑을 제어하기 위한 스크립트 형태의 사용자 API 또는 명령을 제공할 수도 있으며, 경우에 따라서 사용자-디바이스의 매핑은 시간과 공간의 위치 및 상태 등과 관련해서 더욱 복잡한 형태로 표현될 수 있을 것으로 본다. Hdac 프라이빗 블록체인에서는 RPC를 통해 스크립트 형태로 주소를 가진 디바이스별 접근 권한을 제어할 수 있다.

이러한 사용자-디바이스 매핑 방안은 이미 IoT 산업계에서 사용되고 있으며, 블록체인과 적절한 업무 연계를 통해서 기존의 관리 체계를 최소한의 수정하면서 최대한의 효과를 내도록 운영할 수도 있을 것이다.

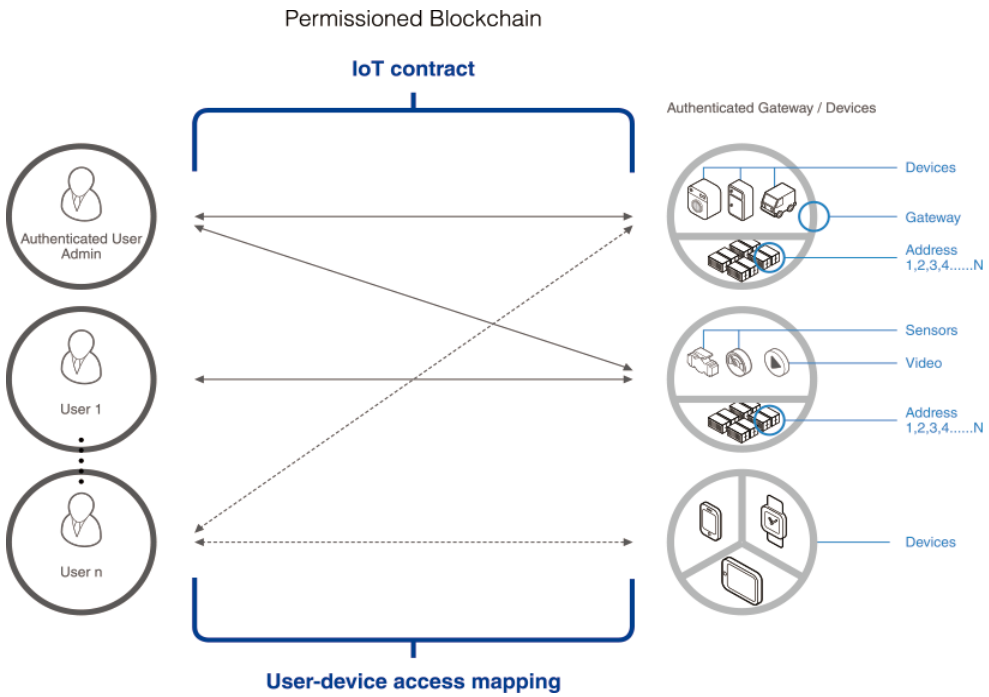


그림 10. 프라이빗 블록체인상의 사용자와 디바이스 간 매핑 예시

IoT Contract

IoT Contract는 M2M을 위한 기반으로 작동할 수 있다. IoT Contract는 스마트 계약(Smart Contract)의 대상을 IoT 디바이스로 확장한 개념으로써, 프로그래머는 IoT 디바이스의 동작을 제어하는 프로그램 즉, IoT용 스마트 계약을 생성하고, 특정한 디바이스로 IoT Contract를 보내어 기

계 수준에서 자동화된 작업을 수행할 수 있다. IoT Contract는 사용자-디바이스 또는 디바이스-디바이스 사이에서 제어 명령을 전달하는 트랜잭션에 포함되며, 이 트랜잭션을 사용하기 위해서는 뒤에 설명할 사용자-디바이스 또는 디바이스-디바이스 인증이 선행되어야 한다.

이 트랜잭션을 사용하기 전에 사용자와 디바이스는 우선 블록체인 네트워크에서 인증 절차를 거쳐서 등록이 되어 있어야 한다. 사용자의 경우는 2-팩터 인증을 거쳐서 인가된 사용자만 블록체인 네트워크에 접근이 가능해야 한다. 사용자 인증 방식으로는 ID, 패스워드, OTP, 생체 인증(지문, 홍채, 얼굴 인식 등) 등을 추가할 수 있고, 이를 통해서 인증을 하게 된다.

디바이스는 스스로 등록이 어려우므로, 최초에 블록체인 관리자가 관련된 디바이스를 확인하고 등록을 해야 한다. 디바이스의 고유한 ID를 결정하기 위해서 몇 가지 방안이 고려되고 있다. 우선 디바이스 자체에 고유한 ID를 가지는 경우(보안칩 등)는 문제가 없지만, 그렇지 않은 경우는 디바이스의 고유한 응답 정보, MAC Address, CPU ID, Disk ID 및 OS이미지, 전자 지갑 주소 등에 대한 해시(hash)값을 등록해서 위변조 시 디바이스를 자동으로 블록체인 네트워크에서 분리하고 관리자에게 통보할 수 있다.

디바이스에서 가동되는 프로그램은 IoT Contract에 따라, 상태가 변하는 경우 디바이스를 조작하거나 디바이스 간의 자동 트랜잭션을 수행할 수도 있고 정해진 곳으로 상태 정보나 데이터를 전송할 수도 있다. 이 때 디바이스 사이의 자동 트랜잭션은 M2M이라고 할 수 있으며 사전에 사용자-디바이스 및 디바이스-디바이스 매핑에서 송수신이 허용된 주소로만 트랜잭션 송수신이 가능하다. 명령을 받는 A디바이스는 프로그램 내용에 따라 다른 B디바이스로 상태 정보나 제어 정보를 전송하고 B디바이스를 제어할 수도 있다.

프라이빗 블록체인 네트워크에 설정이 등록되어 있고 제어권이 있는 경우에만 제어가 가능하다. 이와 같이 Hdac 프라이빗 블록체인을 통해 'IoT Contract' 서비스를 제공함으로써, 사용자와 디바이스, 디바이스와 디바이스 사이의 상태 제어, 거래 및 관리가 가능하며 이를 통해서 M2M 트랜잭션 서비스를 제공할 수 있다.

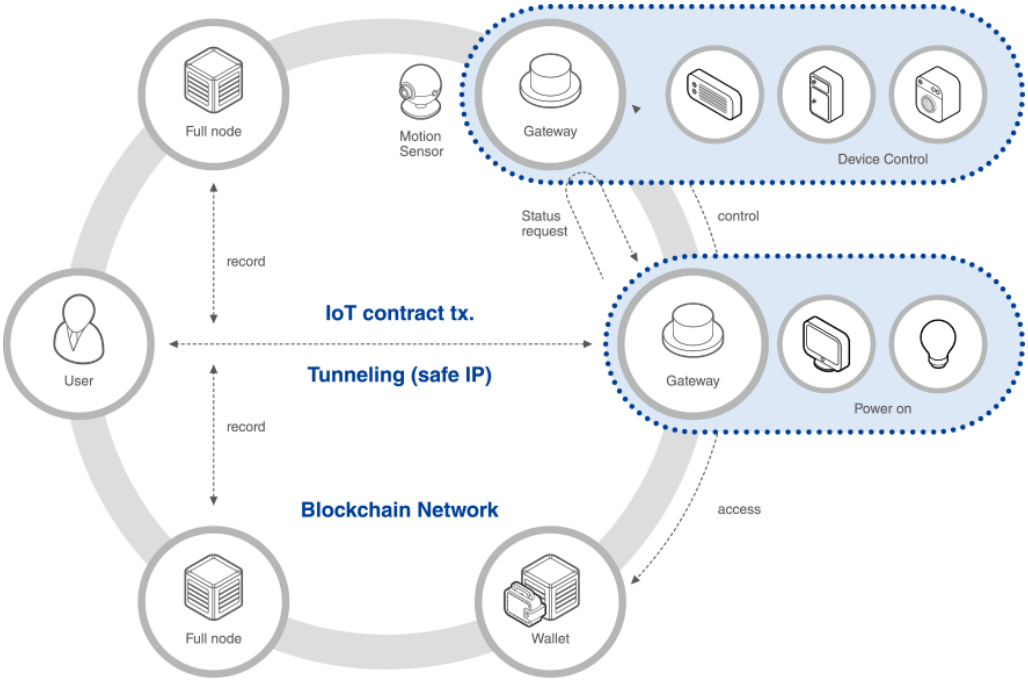


그림 11. IoT Contract 서비스 구조

IoT Contract에는 사용자가 디바이스를 제어하거나, 사용자가 디바이스의 상태를 통보받거나, 자동으로 어떤 조건이 되었을 경우에 자동적으로 트랜잭션이 이루어져 디바이스가 작동하도록 자동화 프로그램을 추가할 수 있다. 이 프로그램은 디바이스의 조건에 따라서 단순한 JSON 형식의 데이터를 전달할 수도 있으며, 좀 더 복잡한 정보를 처리할 수 있는 프로그래밍 가능한 API 형태도 제공될 수도 있다.

성능이 높은 디바이스에서는 좀 더 복잡하고 정교한 프로그래밍이 IoT Contract에 추가되어 디바이스로 전달되고, 디바이스 내에서 작동하는 인터프리터 또는 버추얼머신(Virtual Machine)을 통해서 해석되고 처리될 수도 있다.

속도나 보안 측면에서 IoT 디바이스를 제어하기 위한 가장 효과적이고 편리한 방식은 API를 이용해서 디바이스에 맞는 프로그래밍을 개발하는 방식이고, 유연성 측면에서는 인터프리터나 버추얼머신을 이용하는 방식이 효과적이 될 수 있다. 인터프리터나 버추얼머신의 경우는 단지 사용자 측면의 제어 프로그램만 변경하면 디바이스를 변경하지 않아도 되기 때문에 간편하고 유연하게 다양한 응용 분야에 적용될 수 있다. 하지만 인터프리터나 버추얼머신을 사용하는 경우 비교적 높은 수준의 컴퓨팅 파워와 메모리를 요구하기 때문에 낮은 성능의 디바이스에는 직접 적재할 수 없다.

예를 들어 A타입의 디바이스가 100개 있고, 이 디바이스를 관리하는 정책이 변경되는 경우,

100개 디바이스에 대한 수정이나 업데이트 작업을 수행하기 보다는 제어권을 가진 사용자 측면의 IoT Contract를 변경하는 방식이 훨씬 효율적이며 안전할 수 있다.

IoT에서 트랜잭션은 실시간으로 이루어져야 하기 때문에 블록체인에 적정한 수의 디바이스가 등록되어 있고, 적절한 처리 성능을 보장하는 네트워크를 가지는 경우, 500tx/sec 정도의 트랜잭션을 처리할 수도 있다. 처리할 수 있는 트랜잭션 량이나 응답 시간은 네트워크와 디바이스의 성능에 따라 달라질 수 있다.

특히 트랜잭션이 높은 보안성을 요구하는 곳에서는 VPN과 같이 일반 네트워크와 완전히 분리된 보안 채널을 통해서 디바이스까지 전송될 수 있다. 즉, 중간에 일반 네트워크를 통해서는 접근이 불가능하게 만들 수도 있다. 프라이빗 블록체인에서는 디바이스와 풀노드가 N:1로 배치될 수 있는 보안 장비를 사용하여 네트워크 구간의 보안을 강화할 수도 있다. 또 필요에 따라서 사용자 프로그램과 데이터 블록은 디바이스 보안 문제상 암호화되어 전송될 수도 있다.

IoT Contract의 상세 스펙은 아래와 같이 구성된다.

- 기본 블록체인 트랜잭션
- 사용자 정의 JSON 헤더
  - 사용자 정보, 사용자 유형, 허가된 내용, 처리 명령과 데이터, 응답 방식 등으로 구성
- 사용자 프로그램
  - 추가적인 JSON 데이터 또는 high level 프로그래밍 언어 또는 실행할 오브젝트 정보
  - API, 인터프리터 또는 버추얼머신(Virtual Machine)에서 처리할 수도 있음
- 상기 사용자 프로그램에서 사용할 데이터 또는 스트림

<table>
<tr><td rowspan="3">IoT Contract</td><td colspan="2">Default Blockchain Transaction</td></tr>
<tr><td colspan="2">User Defined JSON Header
(UserInfo., UserType, Permission, OpCode, OpData, ReplyType, etc.)</td></tr>
<tr><td>User Program (Script)</td><td>User Data (Binary)</td></tr>
</table>

표 2. IoT Contract 의 구조

사용자 프로그램은 high level 언어이며, IoT 개발자들에게 익숙한 C언어와 유사한 문법을 가지는 인터프리터 또는 버추얼머신을 통해서 프로그램이 해석될 것이다. 여기에서 우리는 특정한 프로그램 해석기인 인터프리터나 버추얼머신을 사용하여 사용자 프로그램을 해석하는 방식을 구현

하겠지만, 간편하게 새로운 유형의 해석기인 버추얼머신을 사용자가 추가할 수 있도록 소스 코드와 인터페이스를 최대한 간결하게 유지할 것이다.

프라이빗 블록체인에 대한 보안

IoT에서 가장 중요한 관심은 단연 IoT 디바이스 및 블록체인에 대한 보안 문제이다. 이들 보안 문제의 상당 부분은 프라이빗 블록체인을 사용함으로써 해결할 수 있다. 그러나 여러 가지 유형의 네트워크 및 서버에 대한 공격은 프라이빗 블록체인으로 완전히 해결이 안되기 때문에 다른 보안 기술과의 연계가 고려되어야 한다.

프라이빗 블록체인의 경우 노드와 디바이스 간에 또는 블록체인 노드와 사용자 간의 네트워크를 일반 네트워크와 분리하는 별도의 보안 채널을 이용함으로써 보안성을 향상시킬 수도 있다. 이 방식은 물리적인 하드웨어 또는 디바이스에 탑재되는 Agent 형태를 통해서 실현될 수 있으며, 기존의 블록체인 노드나 디바이스 구성을 변경하지 않아도 되는 장점이 있다. 블록체인용 코드를 이식할 수 없는 일반 디바이스는 별도의 디바이스 어댑터 노드를 통해서 제어가 이루어질 수 있으며, 이 경우 이 노드에서 트랜잭션은 디바이스를 직접 제어하기 위한 신호로 변경되어 제어가 가능하다.

또한 필요에 따라 서버 내부에도 다양한 보안 위협에 대응할 수 있는 방안도 함께 마련되어야 한다. 최근의 스마트 디바이스는 TLS 또는 SSL 등의 프로토콜이 내장되어 있으며, 제어 신호에 대한 다양한 보안 장치를 갖추고 있다. 사용자-디바이스 간의 암호화된 트랜잭션인 IoT Contract는 TLS/SSL 및 다양한 프로토콜을 사용하는 디바이스에 대응할 수 있으며, 복잡한 암호화를 수행하기 어려운 낮은 성능의 디바이스에는 선택적으로 IDEA(International Data Encryption Algorithm) 또는 ARIA(경량 환경 및 하드웨어 구현을 위해 최적화된, Involutional SPN 구조를 갖는 범용 23 블록 암호 알고리즘) 또는 디바이스에 따라 AES128~AES256 표준 대칭키 암호 알고리즘으로 암호화할 수도 있다.

이 방식은 디바이스 내부의 프로그램을 변경해야 하는 문제가 있기 때문에, 기존에 이미 만들어져 있는 디바이스에는 적용하기 어려운 문제가 있다. 따라서 아주 낮은 성능의 디바이스는 더미 디바이스로 분류될 수가 있고, 이런 유형의 디바이스는 별도의 보안 채널을 통해서 작동하는 게이트웨이로 관리할 수도 있다.

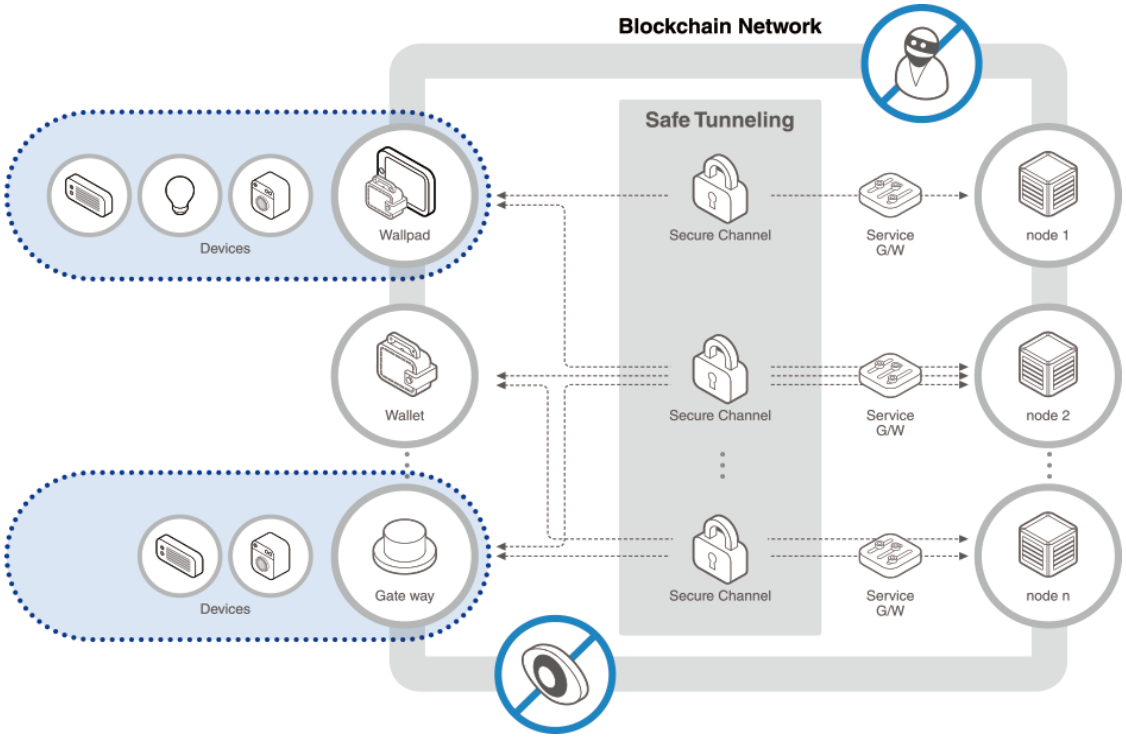


그림 12. 블록체인의 향상된 네트워크 보안

프라이빗 블록체인이 기존의 보안 프로세스와 잘 융합되어 구축되었다고 해도, 여전히 예기치 않은 보안 취약점들이 존재할 수 있다. 따라서 프라이빗 블록체인 상에서 이루어지는 사용자-디바이스 간의 사용자 설정 변경이나 디바이스 추가 변경, 설정 변경, 매핑 변경 등에 대해서 상시 감시해야 할뿐만 아니라 내용 변경 시 이전 설정과 비교도 가능해야 한다. 이러한 빅데이터는 효과적인 도구를 사용해서 검색하거나, 머신 러닝이 탑재된 도구를 이용해서 분석할 수 있다.

그리고 주요한 내용이 변경될 경우, 관리자에게 2차 인증을 시도하게 하는 과정들이 필요하며, 네트워크 상에서 이루어지는 DoS나 DDoS를 비롯한 다양한 네트워크 공격에 대한 대응이 가능해야 한다. 따라서 하나 이상의 노드를 Watchdog(감시자)로 작동하도록 설정하여 비정상 트랜잭션을 감지하고 이벤트를 생성하는 역할을 수행한다. 각 노드 내에는 해당 서버의 상태를 모니터링하는 기능을 넣어서 블록체인이 작동하기 어려운 상황이 되기 전에 관리자에게 통보하고 조치를 취하도록 하는 기능을 수행할 수도 있다.

Watchdog 노드에서 감지하는 이벤트는 아래와 같다.

- 비 정상 트랜잭션: 도착 주소가 존재하지 않는 트랜잭션, 비정상 트래픽을 유발하는 과다

트랜잭션 등에 대한 추적 관리. 비인가 된 트랜잭션과 IoT Contract.

- 각 노드의 상태 감지: 풀노드인 경우 디스크 용량 및 서버 상태 및 네트워크 상태를 감시하고, 일정 수준 이상이 되면 Watchdog에게 통보
- 사용자-디바이스, 디바이스-디바이스 매핑 변경 감시: 내용이 변경된 경우 감지. 변경이 금지된 매핑 변경 시 추적 관리.

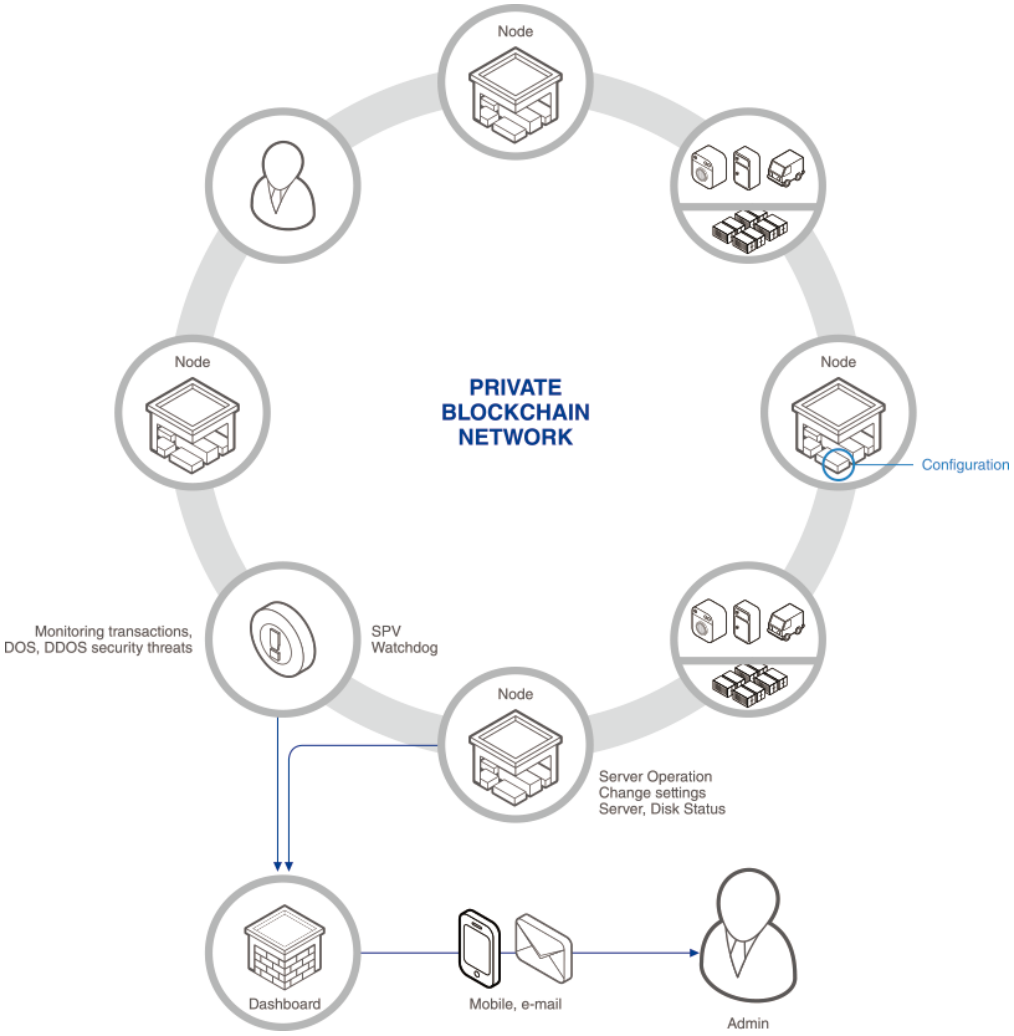


그림 13. 프라이빗 블록체인에서의 위협 감지

Hdac 생태계

Hdac 생태계 발전 전략

Hdac 블록체인 기반의 차세대 산업 플랫폼 개발 및 생태계 조성을 위해 아래 그림과 같이 단계별 전략을 통해 Hdac 블록체인 생태계를 조성하고자 한다.

그림 14. Hdac 생태계 개발 전략

Eco-Player와 파트너

Hdac 블록체인의 원천기술 개발, 응용 프로그램 개발뿐만 아니라 활성화를 위해 현대 BS&C(Hyundai BS&C), 더블체인(Doublechain), 현대페이(Hyundai Pay), BLOKO는 DTC(Digital Transformation Community)를 구성하여 커뮤니티 활동을 하고 있다.

또한 대용량 DB설계 및 튜닝 전문기업인 '위즈베이스(WisBase)', 정보보호 솔루션 업체인 '피앤피시큐어(PnP Secure)', 양자난수칩 개발사 '이와이엘(EYL)', 웹방화벽과 VPN 전문기업 '인투정보(INTO Information)', 논리적 폐쇄망 솔루션 공급사 '아라드네트웍스(ARAD)', IoT디바이스 기술파트너 '모다(MODA)', '㈜밀(ripple)' 등 다양한 산업 적용을 위한 원천 기술 개발 및 서비스 개발을 위해 다양한 파트너사와 협조 체제를 구축 중에 있다. 그 외 인텔과 IoT 및 안면인식 출입보안 솔루션 개발에 협업하고 있다.

현대BS&C와 더블체인은 2016년 12월 블록체인 기반 핀테크 사업 착수를 위해 MOU를 체결하

였고 블록체인 기반의 플랫폼 개발 및 운영 효율성을 극대화하는 동시에 IoT, 블록체인 융합 솔루션의 공동개발 등 다양한 시너지를 내고자 공동 사업을 추진 중에 있다.

2017년 6월 블록체인 기술 고도화와 서비스의 조기 론칭을 위해 블록체인 전문 기업 현대페이(Hyundai Pay)를 본격 출범하여 진행 중에 있으며, 2017년 7월 20일 현대페이(Hyundai Pay)와 더블체인(Doublechain)은 빅데이터·머신러닝 전문기업인 엘라스틱서치(Elasticsearch) 한국지사와 전략적 제휴를 통해 Hdac 기반 핀테크 사업 및 블록체인 연관 사업을 공동 전개할 계획이다.

에코시스템	파트너사	협약 내용 / 역할
DTC	현대페이	Hdac 블록체인 코어 개발 지원, HDAC 가치 제고 및 활성화
	더블체인	블록체인 플랫폼 개발, 가상계좌 개발
	현대 BS&C (Hyundai BS&C)	스마트 IoT(HERIOT 등), 스마트 IoT 홈 기술 연구 협업
	BLOKO	블록체인 연구 및 기술 커뮤니티 운영
응용기술	이와이엘 (EYL)	양자난수 기술, 플랫폼 지원.
	인투정보 (INTO Information)	웹 방화벽. 보안 컴플라이언스 지원.
	모다 (MODA)	IoT Gateway device 개발, 제조.
	위즈베이스 (WisBase)	대용량 DB, 튜닝
	아라드네트웍스 (ARAD Networks)	Safe IP 기술 지원
	엘라스틱서치 (Elasticsearch)	검색엔진, 빅데이터 전처리, 머신러닝 기술 지원
	㈜밀 (Mill Corp)	IoT 제품 제조, 산업용 PC 제조

표 3. Eco-Player

Hdac 생태계 조성 로드맵

연도	진행 계획
2017	- Hdac Generation Event - Release Hdac consensus algorithm - Completion of Hdac operating environment Field test (ASM mining pool, Wallet1.0, Explorer, etc.) - Release H/W Wallet (KASSE 1.0) release, ASM (Advanced Security Module) Ver 0.9 - Release Hdac apps API (ASM mining, Wallet, Explorer)
2018	- Release Hdac operating environment (ASM 1.0 mining pool, wallet2.0, etc.)

	release - Hdac IoT Contract PoC - IoT authentication and device control (Smart Home PoC) - Private Blockchain PoC (Game Application, POS Hdac*T site) - Smart IoT diffusion PoC (apartment, factory, etc.)
2019	- Release Practical application of Hdac IoT Contract & Smart Home (HerIoT) - Release Practical application of Hdac IoT Contract & Smart Factory (Mando case) - Hdac Public-Private Hybrid Blockchain Use-case development
2020	- IoT High Speed Transaction Distributed Processing Blockchain Development - Release Private Blockchain Security Enhancements, Advanced Security Module Ver 2.0 release - Hybrid (Public-Private) Blockchain Network Live Operation (M2M transaction)

표 4. Hdac 생태계 조성 로드맵

부록A – 예시

IoT Contract 예시

JSON Header는 아래와 같이 단순한 제어 명령을 담고 있을 수도 있다. 사용자 처리 함수로 JSON 데이터를 전달하고, 사용자는 JSON 데이터 내용을 해석해서 디바이스를 제어할 수 있다.

```
// 전등을 on (전등의 주소로 IoT Contract 가 온 경우)
{ "operation" : "on", "rerurn" : "yes" } // 제어 명령 수행 후 응답을 돌려주는 경우
{ "operation" : "off" }
```

```
// 에어컨을 켜고, 온도를 섭씨 22 도로 맞추고, 바람은 자연풍으로 설정. 온도를 돌려 줌
{ "operation" : "on", "temperature" : "22c", "wind" : "natural", "return" : "temperature" }
// 에어컨을 켜고, 온도를 화씨 70 도로 맞추고, 60 분 후 자동 off
{ "operation" : "on", "temperature" : "70f", "timer" : "60 minute" }
```

아래의 예는 단순한 IoT Contract 프로그램으로, 사용자가 집에 있으면 에어컨을 가동하고, 없으면 에어컨과 TV를 자동으로 끄고 사용량만큼 처리하는 예이다.

```
#include "hdac.h"

Node AC = "75578a276a3b2d50a1b4ddae16724185ae2d6d25"; // Air conditioner
Node TV = "1BZDfv3gjrFi2YpZ4FnPWhgRovbyM5coFmAAEA"; // TV
Node IS = "Infrared Sensor"; // Infrared Sensor
Node MO = "Management Office";

hdac_t *hdac = NULL;
time_t PowerOnTime = 0;

main()
{
   hdac = HdacInit();

   IS.AddEvent(hdac, ProcessISEvent);
   ExecuteContract(hdac); // IoT Contract 종료 신호 올 때까지 대기
   HdacExit(hdac);
}
```

```
// 이벤트 처리
void ProcessISEvent(hdac_t *hdac, Node node, NodeEvent ev)
{
  if (hdac == NULL || hdac->disabled == true)
    return;

  if (ev.GetStatus("motion") == 0 && PowerOnTime > 0)
  {
    AC.SetStatus("power", "off"); // 에어컨 OFF
    TV.SetStatus("power", "off"); // TV OFF

    int elapsed = time() - PowerOnTime;
    if (node.balance > 1) // 잔액이 충분하면 처리
      MO.Pay(0.0001 * elapsed / 60); // Pay exact amount
    else
      node.Alert("Low Balance"); // 사용자에게 통보
    PowerOnTime = 0;
  }
  else if (ev.GetStatus("motion") == 1 && PowerOnTime <= 0)
  {
    AC.SetStatus("power", "on"); // 에어컨 가동
    TV.SetStatus("power", "on"); // TV 가동
    PowerOnTime = time();
  }
}
```

부록B – 면책 사항

본 문서의 정보는 통보없이 변경 또는 업데이트 될 수 있으며, HdacTech.AG의 의도로 해석되어서는 안된다. 본 문서는 정보를 제공하는 목적만의 용도이며, Hdac.io 또는 연관된 기업의 주식 또는 증권을 판매할 제안이나 권유의 뜻을 담고 있지 않다. 그러한 제안이나 권유는 기밀의 발행 약정의 수단을 통해서만 이루어질 것이며, 모든 적용되는 증권 및 기타 법을 따라 진행될 것이다.

부록C – 인용

Antonopoulos, Andreas, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media Inc. (California: 2017).

Arad Networks, "Why SPN Solutions?" http://www.aradnetworks.com/spn_why, (March 2017).

Banafa, Ahmed, "Internet of Things (IoT): Security, Privacy and Safety," Datafloq, https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948.

Beecham Research Limited, "IoT Security Threat Map," http://www.beechamresearch.com/download.aspx?id=43, (2015).

Belson, David [Ed.], "The State of the Internet / Q3 2015," Akami, https://www.akamai.com/us/en/multimedia/documents/report/q3-2015-soti-connectivity-fi nal.pdf, (December 2015).

Boldt, Bill, "Without Security, is the Internet of Things Just a Toy?" Pubnub, https://www.pubnub.com/blog/2015-01-30-without-security-internet-things-just-toy/, (January 2015).

Buterin, Vitalik, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," https://github.com/ethereum/wiki/wiki/White-Paper, (2014).

Elasticsearch, "Heart of Elastic Stack," https://www.elastic.co/kr/products/elasticsearch, (2017).

EYL Partners, “Product Overview” http://www.eylpartners.com/index.php/product-overview/, (2017).

Greenspan, Dr. Gideon, "MultiChain Private Blockchain ? White Paper,” Coin Sciences, http://www.multichain.com/download/MultiChain-White-Paper.pdf, (2014).

Intel Software, “Intel Realsense Camera SR300,” https://software.intel.com/en-us/realsense/sr300, (June 2016).

La Marca, Daniela, “Gartner: hype in 2015 around the internet of things (iot) and wearables,” Mediabuzz, http://www.mediabuzz.com.sg/asian-emarketing-latest-issue/210-asian-e-marketing/digi tal-marketing-trends-a-predictions-week-1/2504-gartner-hype-in-2015-around-the-intern et-of-things-iot-and-wearables, (Jan. 2015).

Modacom, “Smart IoT Gateway (Hub),” http://web.modacom.co.kr/ko/product/product_view.php?cate=IoT%20Products, (Feb. 2017).

Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System,” https://bitcoin.org/bitcoin.pdf, (2008).

P&P Secure, “Domestic DB Security # 1 'P & S Secure,'” http://www.pnpsecure.com/NEWS--NOTICE/page-4, (Sept. 2017).

Postscapes, “Internet-of-Things Software Guide: Find and compare the best IoT Software development tools, OS, language platforms, and frameworks,” https://www.postscapes.com/internet-of-things-software-guide/, (2017).

Sandoval, Kristopher, “Blockchain: Beyond Cryptocurrency,” NordicAPIs, https://nordicapis.com/the-uses-of-blockchain-beyond-cryptocurrency/, (May 2016).

Waterman, Shaun, “Report: IoT security products face huge challenges,” Cyberscoop, https://www.cyberscoop.com/forrester-iot-security-report-q1-2017/, (Jan. 2017).