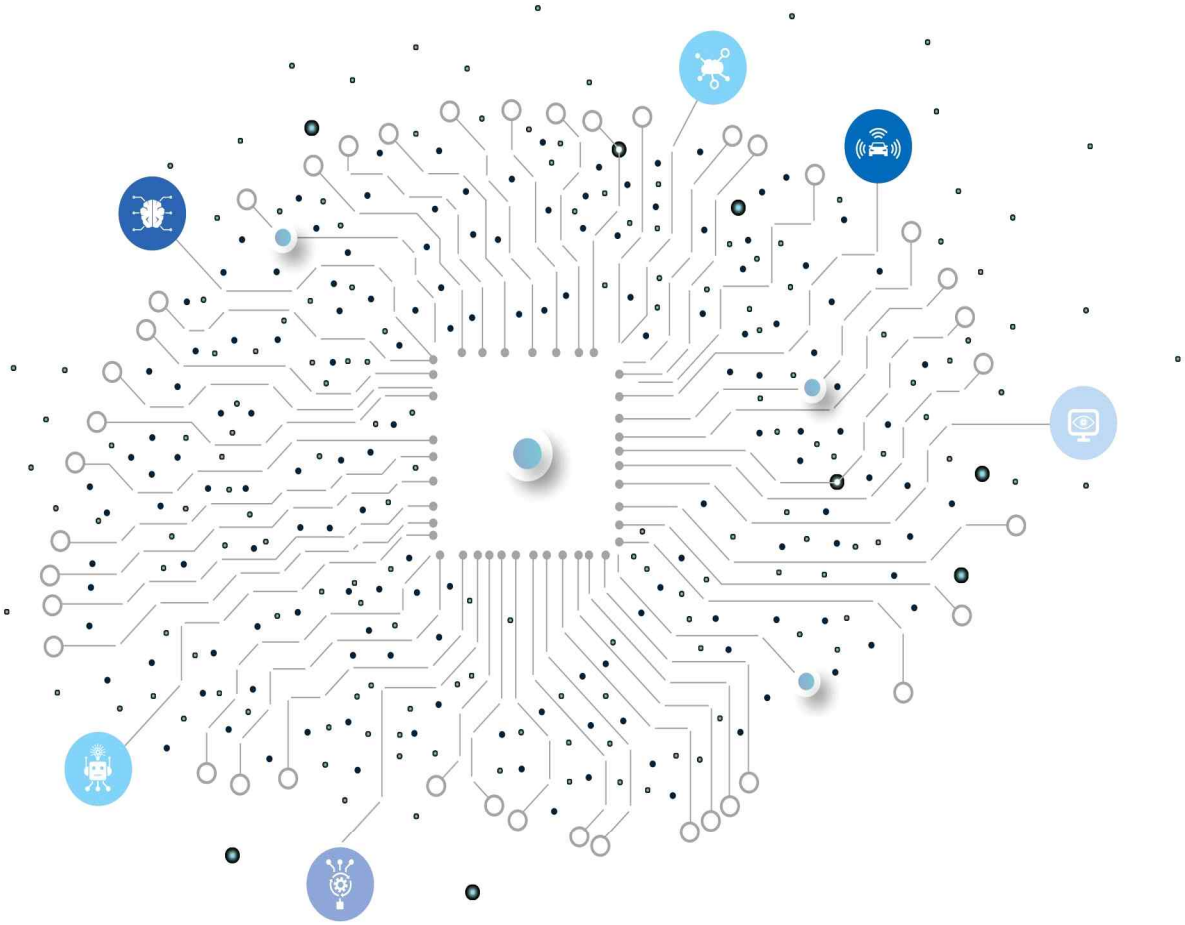
AI Network Lab
INSIGHT
Vol.13
(2022.12)



전자 거래의 응용 전력 거래의 Private 블록체인과 보안

| 작 성 | ㈜루멘소프트 김병진 이사 (sirmd@outlook.com)

NIA 한국지능정보사회진흥원
NATIONAL INFORMATION SOCIETY AGENCY

o 『AI Network Lab 인사이트』는 인공지능, 클라우드, 5G 등 4차 산업혁명의 핵심인 지능정보기술과 네트워크 신기술에 대한 동향을 간략하고 심도 있게 분석한 보고서입니다.

o 본 연구보고서는 과학기술정보통신부의 방송통신발전기금조성사업, 한국지능정보사회진흥원의 초연결지능형연구개발망 구축·운영사업의 연구과제 결과이며, 한국지능정보사회진흥원/한국능률협회와 공동 기획하였습니다.

o 본 보고서의 내용은 한국지능정보사회진흥원의 공식 견해와 다를 수 있습니다.

발 행 처 한국지능정보사회진흥원

발 행 인 황종성

기 획 한국지능정보사회진흥원 지능형인프라본부 공공인프라팀

보 고 서 온라인 서비스 www.nia.or.kr

Contents

개요

○ 블록체인(Blockchain)은 분산 컴퓨팅 기술 기반으로 관리 대상 데이터를 “블록”이라고 하는 소규모 데이터들이 P2P(Peer to Peer Network :작은 소수의 서버에 집중하는 것이 아니라 네트워크 참여자의 디바이스들이 계산과 대역폭 성능에 의존하여 구성되는 네트워크 또는 통신망) 방식 기반으로 생성된 체인 형태의 연결고리 기반으로 데이터를 저장하여 누구라도 임의적으로 수정할 수 없고 누구라도 변경의 결과를 확인할 수 있는 분산 컴퓨터 기술을 이용 원장(거래 전부를 기록하는 장부) 관리 기술이다.

○ 블록체인에서 원장(영어 : Ledger)을 소규모 서버에 저장 또는 중앙에서 저장하는 것이 아닌 네트워크 구성원들의 컴퓨터에 저장하는데 이 구성의 컴퓨터를 노드라고 하며, 이곳에서 모든 거래기록을 저장함으로 해당 노드의 운영하는 조직 또는 운영자가 임의로 조작 불가능하도록 고안 되었다. 블록체인 기술은 비트코인이라는 암호화폐 거래에 사용되는 것인데 사람들이 비트코인과 이더리움을 블록체인으로 알고 있다. 블록체인 기술암호화폐가 아닌 거래 기술을 의미하며 분산 환경 기술을 통해 데이터인 블록이 거래되는 것을 기록하여 위변조를 쉽게 할 수 없도록 하는 기술을 뜻한다.

○ Public 블록체인과 Private 블록체인으로 구분하며 금융권이나 국가기관처럼 신뢰할 수 있는 기관에서 블록체인 기술을 통해 거래에 대한 위변조 및 거래의 신뢰를 보장할 수 있는 기술이 필요하며 이를 사용하는 경우 Private 블록체인 기술을 사용한다. Private 블록체인 기술을 이용하여 우리나라 전력공급를 담당하는 공기업 한국전력공사와 전력 거래를 담당하는 전력거래소에서 Private 블록체인을 이용하여 전력 거래 시 위변조 및 신뢰성을 보장할 수 있다.

보 고 서 요 약

블록체인이란 무엇인가?

- 블록체인의 기술을 이해하기 위해서는 분산 컴퓨팅(Distrubute Computing)에 대한 개념과 기술을 이해하는 것으로 시작하면 좋다. 네트워크 또는 인터넷에 연결된 여러 컴퓨터들의 성능을 이용하여 메시지를 한 대의 컴퓨터에서 다른 한 대의 컴퓨터로 메시지를 보낼 때 이 메시지의 내용을 암호화하고 내용을 보기 위해서 복호화등 메시지를 보낼 때 필요한 여러 처리 및 계산 문제를 하나의 컴퓨터가 아닌 연결된 컴퓨터로 처리 및 계산하여 해결하는 모델이다. 이 분산 컴퓨팅 환경을 컴퓨터 엔지니어나 과학자들은 별렬 컴퓨팅, 병행 컴퓨팅과 많은 부분이 겹치기도 한다. 블록체인은 분산 컴퓨팅 기술에서 메시지의 데이터를 저장할 때 하나의 데이터 저장소가 아닌 여러 데이터 저장소에 저장하는 기술로 다양한 분야에 활용이 가능한 기술이다. 블록체인은 이 메시지를 보내거나 받을 때를 기록하는 것에서부터 시작하면 이해하기 조금 더 쉽다. 데이터를 주고 받는 것을 우리 일상생활의 돈을 주고 받는 것 또는 빌리기 갚는 것을 기록하는 것으로 생각하면 이를 기록하는 장부가 있을 것이며 블록체인에서는 이 장부를 한곳에 저장하는 것이 아니라 분산 컴퓨팅 기술을 이용하여 여러 곳의 데이터 저장소에 저장하고, 이를 임의적으로 위변조 못하도록 하여 거래의 신뢰성을 높이는 기술이다. 일반적으로 알고 있는 비트코인과 이더리움은 이 기술을 이용하여 가상의 자산인 암호화폐를 만들고 이를 거래할 때 블록체인 기술을 검증한 결과물이라 할 수 있다.

블록체인과 Web 3.0

- 블록체인과 함께 Web 3.0은 연관이 매우 높다. 블록체인의 인프라를 구성할 때 필요한 기술이다. 블록체인은 시스템에 연관하여 서비스를 구성하면 비즈니스 로직과 사용자 UX를 담당하며 같이 사용되고 있다. 두 기술에서 핵심 단어 하나 있으며 ”탈중앙화“의 용어가 있다. 중앙에 데이터를 저장하는 데이터베이스 시스템

에 저장하는 것이 아니라 다른 컴퓨터나 데이터 저장소에 저장하며, 기존 데이터베이스 시스템이 아닌 분산 데이터베이스 시스템에 저장 한다. 탈중앙화는 데이터를 한곳에서 저장하는 것이 아니라 여러 곳에서 분산하여 저장하는 것이 핵심이며 마케팅 용어로 알고 있는 Web 3.0을 이용하여 사용자 UX와 함께 블록체인과 같이 사용된다. 탈중앙화에서 블록체인은 시스템의 인프라의 서버를 구성하고 이를 비즈니스와 UX는 Web 3.0 담당하며 서로 유기적으로 시스템이 구성된다고 할 수 있다.

블록체인의 종류와 특징

- 블록체인의 특징은 거래가 일어날 때 이를 분산에서 저장하고, 저장할 때 암호화를 진행하는 것이 핵심이다. 암호화의 경우 해시함수를 활용하는 것이 일반적이며 거래가 이루어 질 때 머클 트리의 특징을 가진다. 블록체인을 구성할 때 크게 3가지로 구분이 된다. Public, Consortium, Private 블록체인으로 구분할 수 있다. Public의 경우 우리가 이미 알고 있는 비트코인, 이더리움등이 있으며 Consortium은 R3 CEV로 시티그룹, 뱅크오브아메리카, JP모건체이스, 골드만삭스, 모건스탠리, UBS등 43개의 금융회사들이 참여하는 블록체인컨소시엄이 있으며, Private 블록체인의 경우 나스닥 비상장 주식 거래소 플랫폼 링크(Linq)가 있다. Public이나 Consortium의 경우 거래 증명이 거래 증명자가 누구인지 알수 없거나, 거래 증명자가 인증을 거쳐 알려진 상태인 반면 Private 블록체인 중앙 기간에 의하여 거래 증명이 이루어진다. Public 블록체인은 개방형 블록체인으로 누구나 네트워크에 참여하여 트랜잭션(하나의 거래가 이루어지는 단위 : Database에서는 하나의 명령어가 실행되는 단위) 생성할 수 있어 공공의 장부로 구분하며, 통상 블록체인이라 하면 Public 블록체인을 뜻한다. Public 블록체인의 경우 누구나 참여할 수 있고, 모든 참여자의 상호 검증을 거쳐 신뢰도가 높다. 트랜잭션 내역이 모두에게 공개되어 네트워크 참여한 컴퓨터 또는 노드가 이를 검증하고 거래를 승인하기 때문이다. 모든 참여자가 거래 기록을 남기고 이를 공유하기 때문에 참여자가 많으면 이를 공유하기 위하여 처리 속도가 느리게 된다. Private 블록체인의 경우 폐쇄형으로 Publc의 상대적 개념이다. 법적 책임이 있는 신뢰할 수 있는 서비스 제공자(기업 또는 공공기관)의 승인을 받은 사용자만 참여할 수 있는 블록체인이다. 주로 기업에서 활용하여 엔터프라이즈 블록체인(Enterprise Blockchain)이라 하

며, 여러 기업이 참여하는 컴소시엄 블록체인도 넓은 의미로 볼 경우 Private 블록체인으로 볼 수 있다.

블록체인을 이용한 공기업의 전자 거래의 활용

- 블록체인은 거래 기술을 저장하는 장부이기 때문에 거래가 일어나는 환경에서 얼마든지 활용할 수 있다. 우리 주변에서 신뢰할 수 있는 공기업 중에 일상 생활에서도 이미 사용하고 있다. 코로나-19의 백신 접종을 위한 앱(App)인 쿠브(COOV)도 블록체인을 활용한 증명서를 발행하는데 여기서 사용되는 기술도 블록체인 기술을 사용한다. 이 앱에서는 질병관리청이라는 신뢰할 수 있는 국가기관과 외교부와 연결하여 외국에서 필요한 백신 증명서를 영어로 발급받을 수 있다. 이 모든 의 핵심기술이 바로 블록체인이다. 공공기관처럼 신뢰할 수 있는 공기업에서도 활용할 수 있는데 바로 한국전력에서도 사용할 수 있다. 전력을 생상하고 이를 공급, 사용하는 경우 전력생산을 개인이 발전사업 허가를 받고 1,000kW 이하의 신재생 발전설비를 갖추고 생산된 전력을 판매할 수 있다. 개인이 전력을 생산하고 판매할 경우 전력시장에 참여하거나 한국전력공사와 전력수급계약(PPA)를 체결하여 거래할 수 있다. 거래를 위해 신재생에너지 공급인증서(REC:Renewable Energy Certificate) 발급을 받고, 전력거래소에서 전력 거래를 승인받고, 한국전력공사에서 금액을 정산할 때 한계가격(SMP:System Marginal Price)을 그 시간대의 시장가격으로 결정하여 정산을 한다. 이에 대해 에너지경제연구원의 경우 “수시 연구보고서 15-10”의 “우리나라 P2P 전력거래 가능성 연구” 보고서도 있다. 공기업인 한국전력공사가 신뢰할 수 있는 기관으로 Private 블록체인을 구성하여 전력거래소와 전력발전사 또는 개인이 생산하는 전력의 거래를 블록체인으로 원장에 기록하면 전력거래의 신뢰성을 확보할 수 있다. 또한 전기차 시대에서 전기차 충전설비를 통해 전기차가 전기를 충전하고 금액 지불을 할때 그 전기를 신재생에네지를 사용할 경우, 앞에서 이야기하는 전력수급계약을 통해 한국전력공사의 블록체인으로 기록하여 전기차 충선설비를 운영하는 업체와 투명하게 거래를 할 수 있다. 블록체인의 특징인 거래라는 것을 이용하여 공기업인 한국전력공사에서 이를 위한 검증과 실제 KEPCO 체인구축을 하고 있다.

※ 시사점

4차 산업혁명이라는 말이 계속 주변에서 나온다. 4차 산업혁명은 디지털 혁명 위에 구축되고 있다. 로봇, 인공지능, 나노기술, 양자 컴퓨터과 프로그래밍, 생명공학, IoT 등 여러기술들이 디지털 기술 기반으로 이루어 지고 있다. 디지털 세계에서 생성되는 데이터는 한곳에서 소유하고 관리하는 것이 일반적인 환경으로 보통 개인의 정보와 금융 거래 등의 데이터는 기업이나 국가기관에서 관리하였다.

탈중앙화를 내세운 Web 3.0의 기술이 있으며, 탈중앙화의 핵심은 개인 또는 디지털 환경에서 생성된 데이터(블로그등 개인 소셜 네트워크에 있는 데이터) 데이터가 중앙에서 저장하고 관리하는 것이라 이를 분산된 환경에서 저장하고 관리하는 것이다. 데이터를 생성되고 이를 분산해서 저장할 때 이를 기록하는 것을 장부(원장)라고 할 경우 저장할 때 블록체인의 기술을 활용할 수 있으며 4차 산업혁명에 필수적인 기술이다. 현재 여러 가지 사회적 이슈인 가상자산의 경우 자산을 디지털화하고 이를 중앙의 신뢰할 수 기관이 아닌 특정 개인이나 기업에서 가상의 자산을 만들고 이를 거래할 때 블록체인 기술을 이용하여 가상 자신의 소유권과 거래가 위변조가 되지 않았다는 것을 증명하고 거래하는 것이다. 이는 기존의 신뢰할 수 있는 기관에서 주식 거래를 관리하거나, 화폐를 국가의 중앙은행에서 관리하는 개념과 다른 개념으로 새로운 혁신이라 할 수 있다.

눈으로 보이지 않는 가상의 자산을 신뢰할 수 있는 기관인 국가가 운영하는 은행 또는 공기업에서 가상의 자산을 발행하고 이를 기록하면, 탈중앙화라 할 수 없다. 그렇지만 지금처럼 사회적 이슈가 발생하는 암화화폐의 경우 적절한 안전장치와 국가기관이나 공기업을 중신으로 신뢰할 수 있는 블록체인 기술이 필요하다.

투명한 공급망을 구축하고 신뢰성을 확보하기 위한 기술로 블록체인 기술이 매우 중요하다. 일상생활에서 기업과 공기업, 공공기관에서 블록체인 기술을 이용하여 신원증명을 위해 모바일 운전면허증과 신분증이 있으며, 이를 활용 수 있는 기술이 매우 많다. 특히 유통 분야의 경우 블록체인을 통해 거래의 투명성과 신뢰를 받을 수 있다. 대표적으로 우리나라의 경우 중고차 시장의 신뢰성과 투명성이 매우 낮은 측에 속한다. 이미 기업들이 빠르게 이를 활용하려고 하고 있지만, 중고차의 경우 자동차 거래 특성상 공공기관과 연결된 부분이 있다. 전력 거래의 경우 신뢰할 수 있는 공기업인 한국전력공사가 있으며 거래를 진행할 때 전력수급계약을 맺고 개인과 한국전력공사, 기업과 한국전력공사 전력 거래를 할 때 블록체인을 활용할 경우 전력 거래의 신뢰성과 투명성을 확보할 수 있다.

주 요 내 용

(1) 블록체인이란 무엇인가?

가. 개요

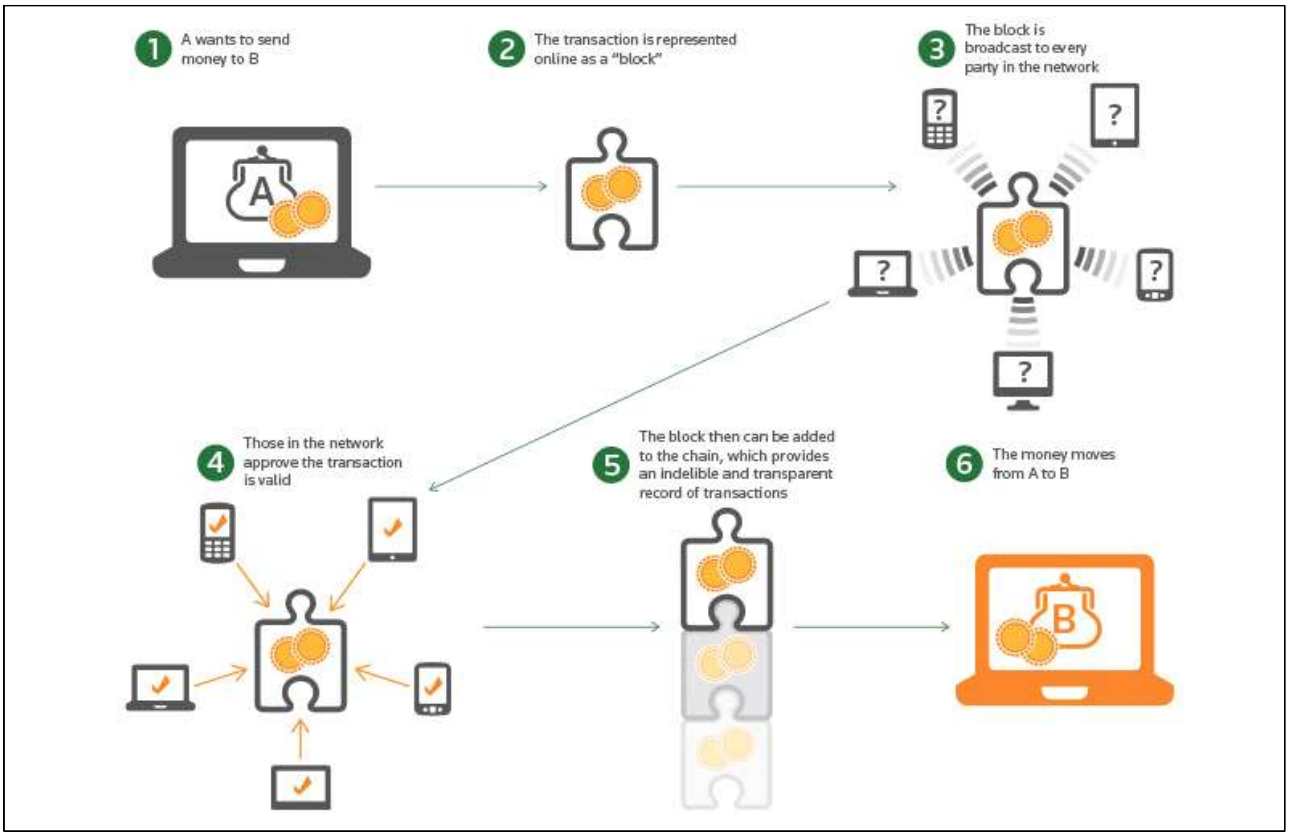
블록체인이란 P2P 네트워크 기반으로 거래 데이터를 분산하여 저장하는 기술로 요약할 수 있다. 단순 데이터를 저장하는 것은 특정한 저장소나 데이터베이스 저장한다. 블록체인은 “데이터를 몇월 몇일 누가 누구에서 데이터를 전달했어요”라는 데이터를 블록이라는 단위의 소규모 데이터를 생성한다. 이를 중앙집중식 방식인 한곳에 블록을 저장하는 것이 아닌 여러곳에 저장하는 것이다. 여러 곳에서 저장할 때 블록을 암호화하여 높은 보안성을 확보하면서 거래 과정에서 작은 소규모 데이터를 통해 신속성과 투명성을 가질 수 있다. 보안성이 강화되면 보안 위협으로부터 안전할 수 있으며, 누군가 거래에 대한 보장(보증)을 하는 증명서비스의 항목들을 블록체인 시스템에서 수렴할 수 있다.

블록체인 시스템을 구축하고 사용할 경우 보안성이 높고 위변조가 어렵다는 특성이 있기 때문에 거래라는 것이 일어나는 환경만이 아니라 데이터를 저장하고 이를 증명하는 시스템에서도 활용할 수 있기 때문에 다양한 분야에서 사용 가능하다. 블록체인 시스템의 또 하나의 활용은 계약을 할 경우 중간 신뢰 담당자(Trusted Third Party:보증 시스템 또는 쉽게 보증인)없이 거래할 수 있도록 스마트계약(Smart Contract)을 할 수 있다.

현재 블록체인 암화화폐 기반의 가상자산과 코로나-19 백신 증명서, 신분증 확인 서비스등에서 활용되고 있으며, 신재생에네지를 생산하는 개인이나 기업에서 전력 거래를 할 경우에도 활용될 수 있다.

나. 블록체인의 원리

블록체인 기술은 거래 정보를 기록한 장부를 원장(Ledger)라는 용어로 표시한다. 이 원장을 P2P(개인과 개인의 거래)거래를 한곳에서 저장하는 중앙 집중식 저장방식이 아닌 탈중앙화 방식의 분산된 저장소에 저장하는 것이 핵심이다. 블록체인은 거래 정보를 블록이라는 단위로 저장한 데이터를 연결된 컴퓨터가 있고 이를 참여자라고 지칭하며 모든 참여자 컴퓨터 공유한다.



[그림1. Thomson Reuter(2016.1.16.), "lock-chain technology: Is 2016 the year of the block-chain"]

블록체인의 통한 거래는 앞의 그림을 기준으로 설명할 수 있다. 1) A가 B에 송금을 하면, 2) 해당 거래 정보가 담긴 블록이 생성되며, 3) 블록이 네트워크상의 모든 참여자에서 전송된다. 4) 참여자들은 거래 정보의 유효성을 상호 검증하고, 5)참여자 과반이 데이터와 일치하는 경우 거래 내역을 정상으로 판단하고 이를 검증 완료 블록으로 이전에 생성된 블록이 있을 경우 이를 연결하고 새로운 블록은 최초로 기록

한다. 6) A가 B에 송금하여 거래가 완료된다. 이렇게 거래가 생성될 때마다 블록이 생성되고 참여자가 서로 검증하여 블록을 서로 연결한다. 연결이란 참여자 컴퓨터에 거래 정보를 저장한다는 것과 같다. 이를 위변조 할 경우 참여자의 과반의 컴퓨터에서 거래 기록을 위변조해야 하기 때문에 보안위협이나 해킹이 어렵거나 불가능하다고 이야기한다.

기존 거래는 중앙에 신뢰하는 시스템이나 보증을 하는 시스템 환경이였다면, 중안이 아닌 참여자 모두의 시스템에 저장하여 제 3자의 보증 없이 당사자간에 안전하게 거래가 이루어진다.

다. 블록체인의 기술 발전과 변화

블록체인은 초기 P2P를 기반의 데이터 교환에서부터 시작한다. 이 데이터 교환의 증명을 할 수 있는 기술이 나오고, 이를 기록하는 과정에서 기록이 핵심기술이다. 이 기술에서 암호화 분산 환경에 대한 발전과 연관도 있다.

이 블록체인은 1세대에서 3세대로 구분을 하며, 현재는 2세대라 할 수 있다.

[그림2. 블록체인의 세대별 기술 발전의 진행 상황]

이 블록체인의 기술 발전으로 인하여 여러 변화가 생길 수 있다.

[그림3. 블록체인 기술에 따른 주요 부분의 변화]

1) 금융 부분과 의료 부분의 변화

금융에서는 가상 자산과 함께 보험 서비스를 들수 있다. 보험금의 청구에서 사람이 직접 서류를 구비하여 청구하는 것이 아니라, 병원에서 진료를 받고 이를 보험사와 연동하여 보험에 필요한 서류를 서로 연결하고, 이를 블록체인으로 처리하면 보험금 청구가 쉽고 블록체인으로 되어 있기 때문에 위변조가 불가하다는 장점이 있다. 또한 의료에서는 개인의 데이터를 이용한 데이터 서비스를 하는 기업이 있다.

개인 데이터를 이용하여 헬스 서비스와 연동하거나 개인의 의료정보를 암호화 하고 이를 병원이나 특정 의료 서비스와 연결하여 사용할 때 데이터를 안전하게 보호하고 거래할 수 있는 블록체인을 사용하는 것이다.

2) 디지털 자산(콘텐츠)

디지털 자산의 경우 비트코인이나 가상화폐를 생각 할 수 있지만, 우리는 저작권에서도 블록체인 기술을 사용할 수 있다. 특히 음원시장이나 한정판 상품의 경우 NFT(대체 불가 토큰:Non-Fungible Token)에 기술의 경우 저작권과 이를 이용한 가상 자산으로 활용되고 있다.

3) 공공 부분

공공 구분은 바로 코로나 19를 위한 백신 접종 증명 앱을 보면 알 수 있다. 백신 접종에 대한 기록, 여권 정보와 연결하여 증명서 발급까지 가능한 것이 바로 쿠브(COOV) 앱을 들 수 있다.

4) 물류 및 유통 부분

블록체인의 기술중에 적용 및 활용에 적합한 분야로 바로 물건을 수입 및 제조 후 이를 유통하여 추적할 때 위변조를 막을 수 있다. 특히 중고차의 경우 신차를 생산하고 차의 고유번호를 이용하여 물류 및 유통를 투명하게 진행하고, 중고차에서는

문제가 있는 차를 확인할 때 위변조가 불가능하고, 공공 부분과 연결 사고차 및 보험조회와 침수차등을 확인할 수 있도록 하는 시스템을 블록체인으로 구축하면, 중고차 거래 및 유통에 신뢰성을 확보할 수 있다.

5) 에너지 부분

전력을 생산하는 시설이 이제는 태양광등을 이용하여 개인이 생산할 수 있는 방법이 있다. 우리나라의 경우 이를 한국전력공사에서 구매를 진행하게 되는데 이 거래가 조금 절차가 있다.

[그림4. 전력에너지 클라우드 플랫폼에서 참조한 전력거래 절차]

여기서 거래할 때에는 한국전력공사가 한국전력거래소에서 전력금액등의 여러 가지를 확인 후 거래가 이루어 진다. 거래가 이루어지는 상황이라면 당연히 블록체인 기술을 사용할 수 있다. 언론을 통해 확인해 보면 2021년 7월의 인렉트리파워의 뉴스에서 삼성 SDS와 한국전력공사 전력연구원에서 블록체인을 이용해서 전력구매계약(PPA) 제도에서 이를 적용하려고 한다.

(2) 블록체인과 Web 3.0

가. 탈중앙화와 블록체인

데이터를 중앙에 데이터를 저장하여 이 데이터의 소유와 사용을 수집한 사람 또는 기업이 활용하는 것이 전통적인 컴퓨터 시스템 환경이였다. 개인이 생성한 데이터의 경우도 중앙에 저장되거나 수집되면 이를 수집한 기업이나 개인이 활용하는데 아무런 제약이 없었지만, 이제 이런 데이터의 소유권에 대한 것이 이슈로 이야기 되고 있다. 바로 디지털 자산의 소유권이다. 사용자가 직접 생산한 데이터를 자산으로 보거나 개인의 데이터를 자산으로 볼 경우 이를 사용하는 곳과 어디에 있는지 확인하는 것이 중요하다. 또한 내 개인 데이터가 어떻게 다른 기업이나 공공기관에서 사용되지 알고 있는 것이 매우 중요하다고 할 수 있다. 여기서 블록체인이 기술을 이용하여 내 개인 데이터 안전하게 보호되고 어디에 사용되고 있으며, 거래가 되었는지 확인하기 위해서도 블록체인 기술을 사용하는 것이 좋다.

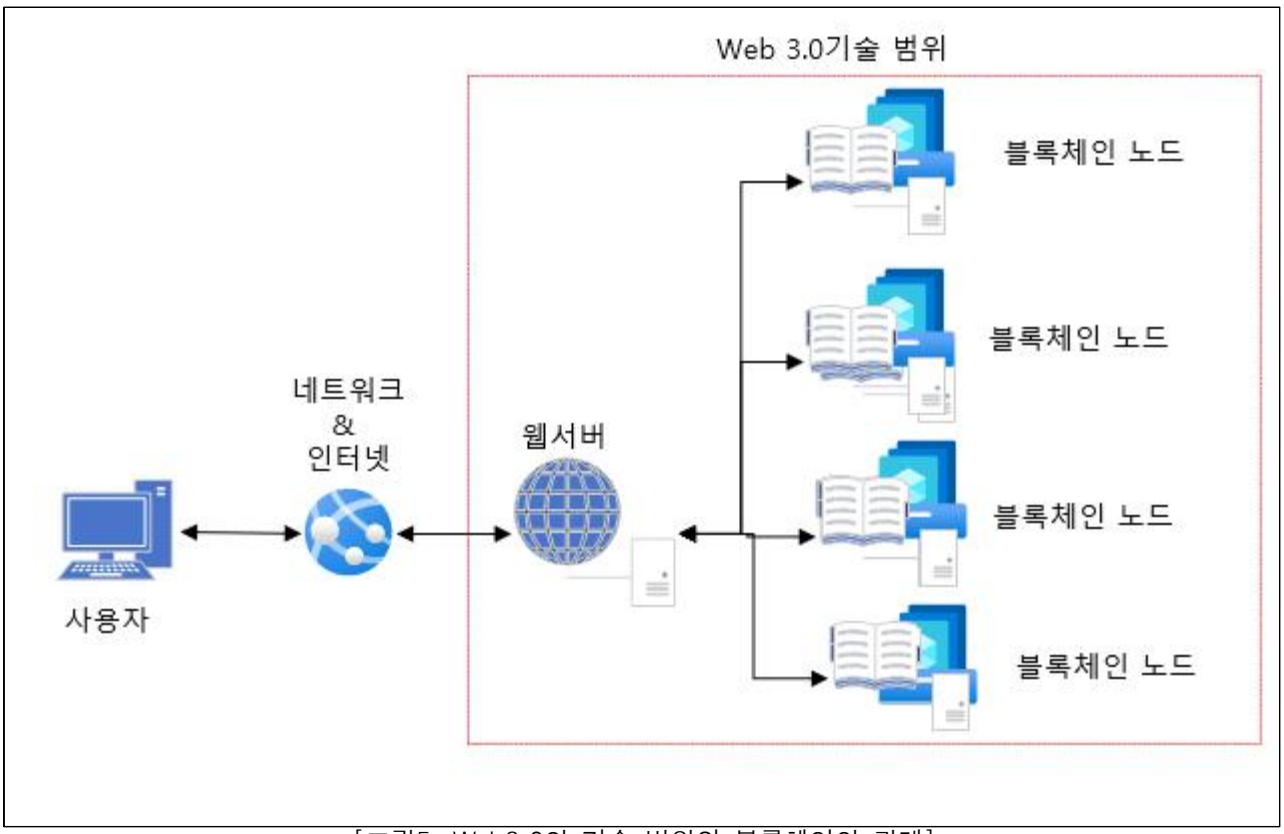
나. 분산 식별자

개인의 어떤 서비스를 이용하기 위해서는 회원가입이나 인증을 받아 계정을 생성해야 한다. 계정 생성시 개인정보를 요구하는 경우에는 내 개인정보가 보안 문제를 이야기하고 해킹사고 발생할 수 있다. 요즘에는 계정 생성시 네이버나 카카오, 구글등의 소셜로그인 기능을 이용하는 경우 대부분 이지만 네이버와 카카오의 내 데이터가 해킹을 통해 유출될 가능성은 당연히 존재한다. 또한 얼마전 데이터센터의 자연재해로 로그인이 불가능할 경우와 같은 특정 기업에 종속되어 서비스가 원활하지 못한 경우도 존재한다. 이런 문제를 해결하기 위해서 Web 3.0에서 자기주건식별자 개념을 제시하고 있으며, 분산식 식별자가 W3C에 표준화되었다.

다. 블록체인과 Web3.0

Web 3.0은 블록체인과 같이 이야기하는 경우가 많다. Web 3.0은 탈중앙화의 특징으로 블록체인도 탈중앙화라는 공통적인 특징이 있으며, 블록체인은 인프라에서 서버 부

분의 시스템과 데이터를 저장하는 기술을 담당하면, 이를 사용자가 이용하기 편리하고 앞에서 이야기한 스마트 계약을 할 수 있는 서버와 사용자 앱(App)과의 연결을 담당하는 것이 Web 3.0 기술이다. 특히 이더리움의 경우 EVM(Ethereum VIrtual Machine)에 설치된 서버 시스템과 앱과 통신에서 Web 3.0은 필수요소에 들어간다.



[그림5. Web3.0의 기술 범위와 블록체인의 관계]

Web 3.0의 기술은 Public 블록체인의 이더리움과 Private 블록체인에서 Hyperledger Fabric에서도 앱과 서버의 연결에서도 사용된다. 스마트 계약을 지원하는 블록체인에서는 비즈니스 로직과 사용자가 웹으로 접근할 때 처리하는 부분을 담당하고 이를 블록체인 시스템과 상호 소통한다고 이해하면 된다.

(3) 블록체인의 종류와 특징

가. 블록체인의 유형

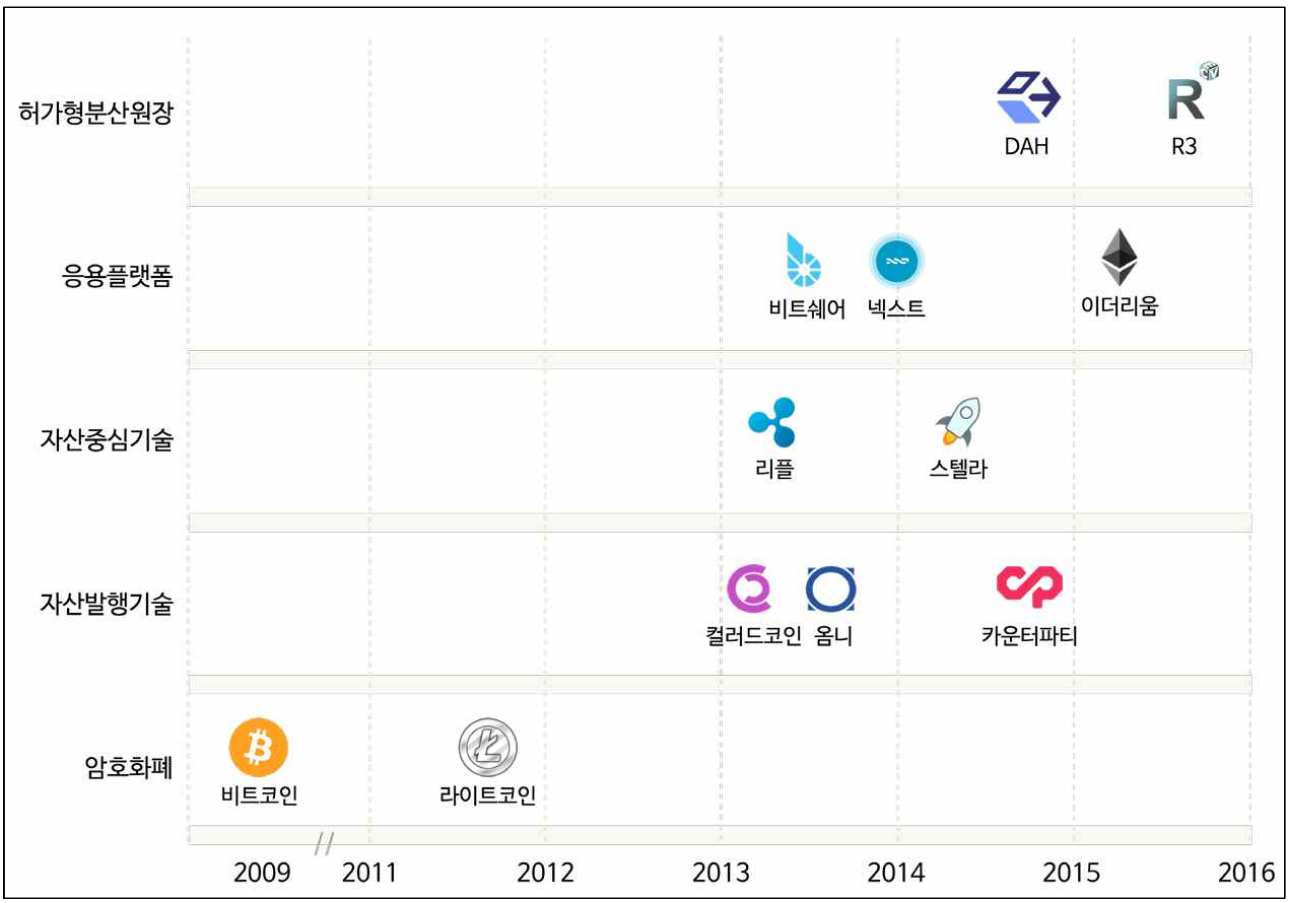
보통 블록체인은 크게 2개로 구분하거나 3개로 구분하는 경우가 있다. 이는 활용되는 목적에 따라 분류가 되며 각각의 특징이 있다.

1) Public 블록체인

블록체인은 비트코인이라는 것으로 출발하는 것이 일반적인데 이유는 블록체인 기술을 이용하여 나온 대표적인 바로 가상자산과 이를 활용한 비트코인이기 때문이다. Public 블록체인을 이야기 할 때에는 2009년부터 2016년까지의 자료를 참고하여 보면 가상 자산거래에 대한 것을 시작으로 응용 플랫폼으로 이더리움까지가 많이 알려진 상태이다.

Public 블록체인의 경우 다수의 참여자가 참여하기 때문에 한번 법칙이 정해거나 규약이 정해지면 이를 변경하기가 매우 어려움이 따른다. 대표적인이 얼마전 이더리움에서 이중 지불 방지를 위해 작업증명에서 지분증명으로 변경할 때 많은 시간이 필요로 하게 된다. 익명성이 보장되고 누구가 접근 가능하다는 장점이 있으며, 이를 악용하는 사례도 있기는 하지만 가상 자산거래가 블록체인 기술을 알리고 사용하는데 기여한 것은 부정할 수 없다. Public 블록체인의 단점은 바로 참여자 많아지므로 이를 증명하기 위한 시간이 많이 필요하다는 것인데 바로 거래 속도가 느리거나 네트워크 확장이 어렵다는 단점도 있다.

[자료 출처: EBA "Cryptotechnologies, a major IT innovation and Catalyst for Change]



2) Private 블록체인

블록체인의 종류 중에 Linux Foundation의 Hyperledger Fabric으로 Open Source 만을 사용하여 만든 기술이다. Hyperledger Foundation 웹 사이트를 방문하면 Open Source 로 자유롭게 이 기술을 사용할 수 있다. 엔터프라이즈 환경(일반적인 대규모 환경)에서 블록체인 플랫폼을 위한 모듈형 블록체인 프레임워크인 동시에 거의 표준처럼 사용하고 있다. 개발형의 모듈형 아키텍처는 필요시 바로 연결 및 사용할 수 있는 형태의 구성요소를 사용하여 다양한 형태로 활용 가능한다.

Hyperledger Fabric는 개방형의 검증된 엔터프라이즈 분산 원장 플랫폼이라고 불리며 "인가된(알려진)" 네트워크 참여자들에게만 자신이 공유하고자 하는 데이터만 공유 가능한다. 또한 스마트계약(Smart Contract)을 지원하며, Open Source로 얼마든지 내부

코드를 활용하여 기업에 맞게 수정할 수 있다.(GitHub에 이미 소스 코드가 있다.) 이미 검증된 것이라 말할 수 있는 것은 IBM과 삼성 SDS등의 기업에서 기술 개발에 참여하고 있으며 여러 모듈 형태를 Open Source로 제공하고 있다.

블록체인에서도 세대를 구분지어서 표시한다. 보통 1세대의 경우 비트코인으로 중앙집중식에서 탈중앙식으로 변경된 시점을 이야기하면, 2세대는 2015년의 이더리움부터 2세대로 구분하는 경우가 있다. 이는 이더리움의 스마트계약을 지원하면서 블록체인의 기술에 확장할 수 있는 계기가 되었으며, Hyperledger Fabric의 경우 2세대 블록체인에 있는 스마트계약을 지원한다. Public 블록체인의 경우 누구나 블록체인에 참여하여 누구나 데이터를 확인할 수 있는 구조인데 이는 기업에서 사용할 경우 무리가 있고, 기업에사 사용할 수 있는 블록체인인 Private 블록체인이 필요하게 되었다. 이를 충족하는 Private 블록체인이 바로 Hyperledger Fabric 으로 모듈형태로 컨테이너 기술을 지원하고, 필요시 직접 서버에 구성하는 것도 가능하다. 경험 상 서버에 직접 구성하는 것도 컨테이너 기술을 사용하는 것을 권장한다.

기업에서 사용가능한 Hyperledger Fabric은 크게 신원관리, 개인정보 보호 및 기밀유지와 같은 특징이 있다. 또한 Open Source로서 소스 코드가 누구나 접근할 수 있고, 스마트계약을 지원하여 다양한 응용프로그램에 활용될 수 있다. 대포적인 것이 카카오페이의 경우 인증 서비스에서 사용되는 기술이 바로 Hyperledger Fabric를 사용하고 있다.

기술의 발전으로 이제 블록체인도 하이브리드(Hybrid) 블록체인 기술로 발전하고 있다. Public + Private 블록체인을 합친 것으로 2개의 블록체인의 특징을 모두 갖춘 블록체인이다. Hyperledger Fabric의 장점인 모듈형이기 때문에 Public 블록체인 기능 추가도 가능하기 때문이다.

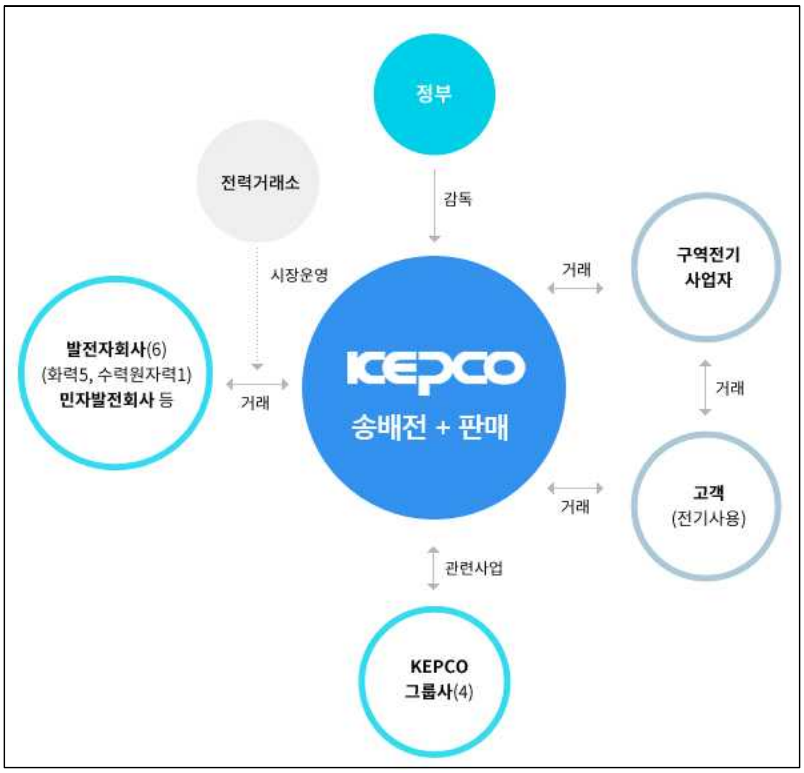
[표] 블록체인의 종류와 특징(Public과 Private)

구분	Public 블록체인	Private 블록체인
관리자	거래에 참여하는 모든 사람	중앙에서 권한을 준 사람
정책	한번 정해진 정책은 변경하기 어려움	중앙 기관에서 쉽게 변경 가능
거래 속도	네트워크 확장에 따라 속도록 느림	네트워크 확장이 용이하고 속도가 빠름
데이터	모든 참여자에게 공개	허가 받은 사람만 공개
식별성	식별 불가능	식별가능
거래 증명	PoW,PoS	중앙에서 거래 증명
예시	비트코인, 이더리움	Hyperledger Fabric

(4) 블록체인을 이용한 공기업의 전자 거래의 활용

4차 산업혁명에서 중요한 것 중에 한가지로 블록체인으로 활용하는 분야에서 에너지 분야 있다. 우리나라의 경우 에너지 공기업이라 할 수 있는 한국전력공사가 있으며 에네지를 생산하는 자회사와 에너지 거래를 하는 전력거래소가 있다. 한국전력공사는 에너지를 개인이 생산하는 경우에도 이를 구매하고, 필요한 곳에 공급하는 역할을 한다. 구매를 할 때에 조금 복잡하게 이루어지며, 개인과의 거래를 할때에는 전력구매계약(PPA) 제도가 있고 이를 통해 개인이 생상하는 에너지를 구매하게 된다.

국내 전력 산업의 구조는 다음과 같다.



[그림6. 한국전력공사 웹 사이트 참조]

개인과 한국전력공사와 거래를 할대 전력 거래소의 금액을 확인해야 하는 것이 있으며 그 금액에 맞추어서 개인이 생산하는 에너지를 구매 후 금액을 지불하게 된다. 여기서 블록체인을 통해 거래 내역과 금액을 블록체인 시스템으로 연동하는 것이다.

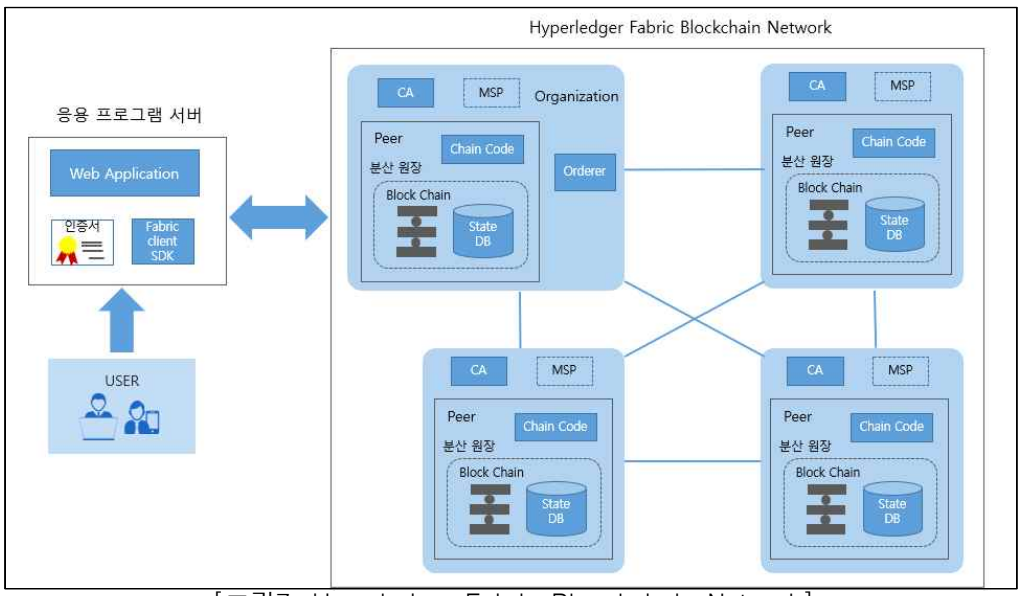
국내 에너지를 담당하는 한국전력공사는 공기업이기 때문에 네트워크가 인터넷과 연

구분	비트코인	이더리움	하이퍼레져
권한 제약	비허가형	비허가형	허가형
데이터 접근제한	Public	Public / Private	Private
합의 방식	PoW	PoS	PBFT
확장성	노드 확장성 높으나 성능 확장성 낮음	노드 확장성 높으나 성능 확장성 낮음	노드 확장성과 성능 확장성 모두 높음
권력집중도	낮음	보통	낮음
익명성	익명성 제공 거래데이터 암호화 없음	익명성 제공 거래데이터 암호화 없음	익명성 제공 거래데이터 암호화
자체통화	비트코인	이더	없음
스크립팅	스택 기반 스크립팅 제 한적 제공	가능성 높음 고급언어 지원(솔리디티)	가능성 높음, 체인코드 고급언어 지원(Go)

결이 제한적이다. 따라서 Public 블록체인보다는 Private 블록체인이 유리하기도 하다.

하지만 때에 따라서는 인터넷과 연결해야 하는 경우도 있어서 블록체인의 대표적인 이더리움과 연동을 해야 할 수도 있다.

우선은 Private 블록체인으로 구성하는 것을 먼저 고려하면 다음과 같다.

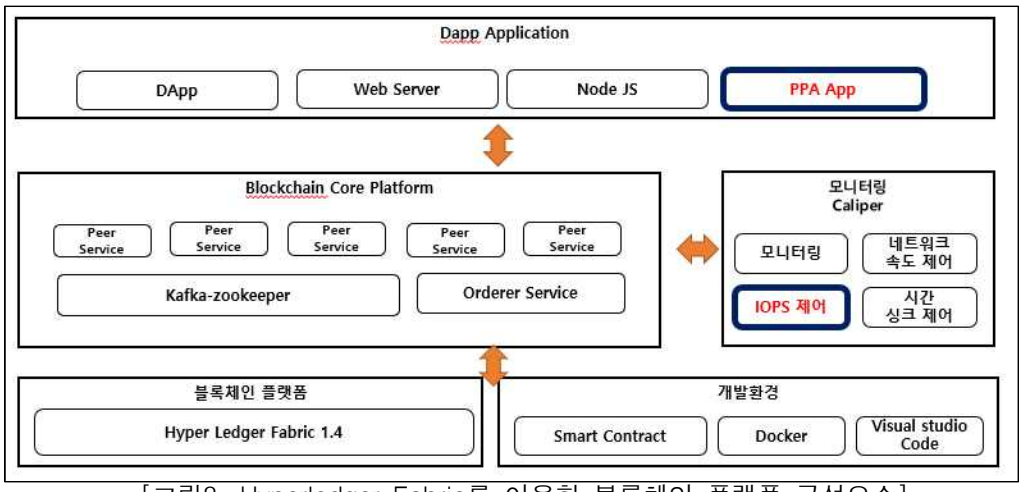


[그림7. Hyperledger Fabric Blocakchain Network]

앞의 그림을 정리하면 다음과 같다.

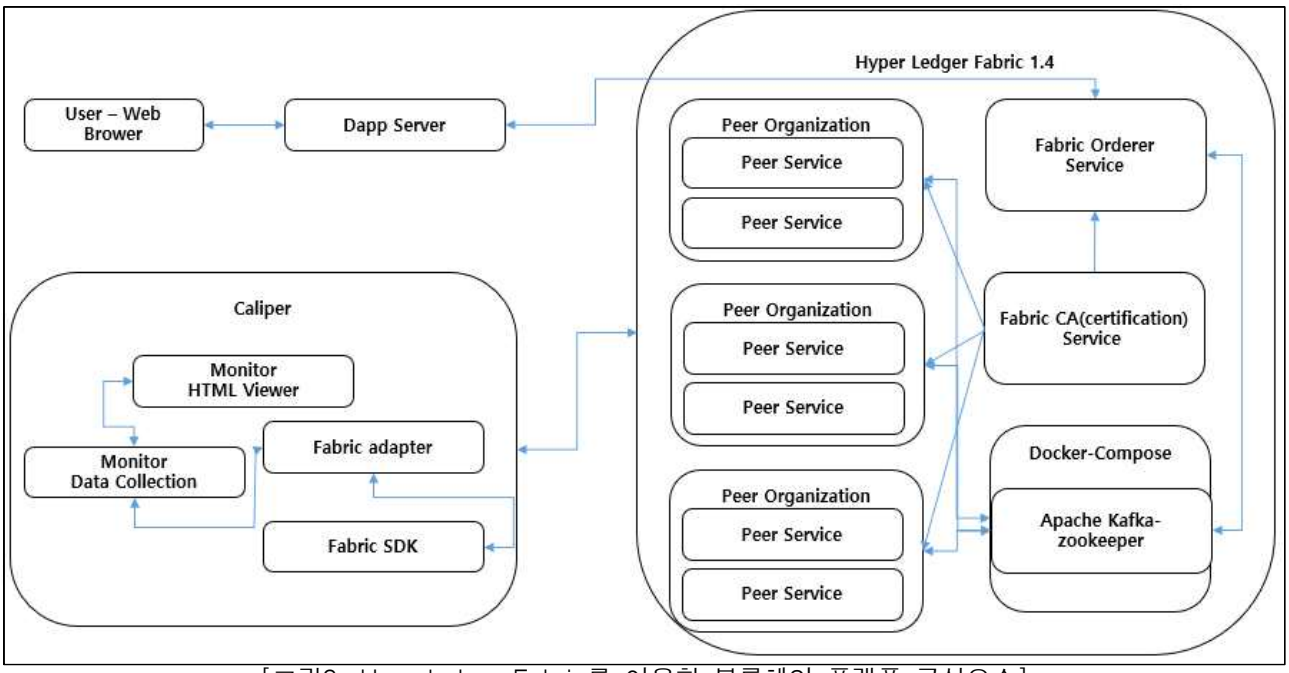
- Organization (조직) : HLF 네트워크 참여, Peer 혹은 Orderer
- Peer(피어) : 조직내 노드, 블록체인, state DB, 체인코드보유
- Endorser 역할 : 응용프로그램(클라이언트) 요청에 따라 트랜잭션에 대해 endorsement(보증)한다.
- Committer 역할 : 트랜잭션과 실행결과의 타당성을 확인해 블록체인과 상태 DB를 갱신한다.
- Orderer(오더러) : 보증된 트랜잭션의 결과를 블록체인과 상태 DB에 기록하는 순서 제어
  네트워크 내 모든 트랜젝션 제어, 이중화 구성
  분산메세징 기술 'Apache Kafka'
  '비잔틴결함 허용' 합의 알고리즘
- 체인코드 : 스마트 계약을 구현하기 위한 프로그램. Go 버전
  트랜잭션 요청에 따라 실행되며 상태 DB를 읽고 쓰거나 과거 상태DB에 기록된 내역 (블록내 포함)을 조회 가능하며 용도에 따라 여러 개의 체인코드 구현 가능.
  이때, 다른 State DB내용 못 읽음
- MSP(Membership Service Provider) : HLF에서 제공하는 CA 또는 외부 CA와 연계하여 사용자 등록, Ecert발생 및 NetworkMSP, Channel MSP(channel policy, 채널 관리, 조직 추가, 체인코드설치/초기화 등) Peer MSP(모든 피어의 파일시스템 내 설치), Orderer MSPChannel (논리적분리 네트워크) : 멀티채널 가능, 각 채널은 동일한 분산원장 (블록체인, 상태DB) 보유.

이를 이용하여 플랫폼 구성요소는 다음과 같이 구성 가능하다.



[그림8. Hyperledger Fabric를 이용한 블록체인 플랫폼 구성요소]

이를 이용해서 다음과 같은 연결 구성도를 그릴 수 있다.



[그림9. Hyperledger Fabric를 이용한 블록체인 플랫폼 구성요소]

신재생 에너지의 블록체인에서는 여러 알고리즘에서는 Hyperledger의 알고리즘을 기반으로 진행하고, 이를 모니터링까지 해야 한다.

Hyperledger의 모니터링은 Cailper를 이용하여 별도의 모니터링 시스템을 구성하는 것이 가능하다. 모니터링은 속도 체크와 데이터가 정상적으로 블록에 저장되었는지에 대한 모니터링으로 구축하고, 여기서 Peer 노드와 Orderer 노드의 시스템 모니터링까지 추가로 해야 시스템 구성이 완료될 수 있다.

단순히 거래 시스템만 구축하는 것이 아니라 블록체인을 구성하고 이를 모니터링까지 하는 시스템을 구축하는 것이다.

(5) 결론 및 시사점

블록체인의 단점과 양자 컴퓨팅의 기술

- 블록체인의 핵심기술은 거래를 분산해서 저장하고 이를 암호화하는 것이 핵심이다. Pulbic 블록체인의 거래가 위변조가 되지 않는다는 핵심은 여러 곳에 분산되어 저장된 기록을 위조할 때 한곳이 아닌 여러 분산된 모든 곳의 기록을 위조해야 하기 때문에 기록이 저장된 노드가 많으면 많을수록 위조가 어렵다. Private 블록체인의 경우 기록하는 노드가 적은 경우 외부 침입이나 해커에 취약할 수 있다는 단점도 있다. 블록체인의 거래를 할 때 암호화를 하게 된다. 컴퓨터 기술이 발전하면서 분산 컴퓨팅 환경을 이용한 병렬컴퓨터 또는 슈퍼컴퓨터가 있고, 이들 컴퓨터는 연산에 특화되어 있다. 블록체인은 해시함수를 주로 활용하는데 해시함수는 단방향 변화이기 때문에 해시값을 이용해서 원본 데이터를 복원할 수 없다는 특징이 있다. 양자 컴퓨팅의 기술이 주목받으면서 실제 양자 컴퓨팅으로 블록체인의 암호화를 복원이나 해킹을 해서 암호화폐에 대한 보안 위협이 있을 수 있다. 양자컴퓨터는 기존과 비교 불가능한 수준으로 연산을 처리하기 때문이다. 1996년 양자컴퓨터 기반의 검색 알고리즘을 발명하고, 그 알고리즘은 AES(Advanced Encryption Standard)와 같은 대칭키 암호나 SHA-2(Secure Hash Algorithm 2), SHA-3(Secure Hash Algorithm 3)와 같은 해시함수에 적용될 수 있다. Public 블록체인의 기술을 활용한 비트코인의 경우 SHA-256을 사용한다. 현재는 양자컴퓨터와 그 기술이 몇몇 기업(Google, IBM등)과 미국 정부에서 주로 사용되지만 기술의 발전으로 암호화 기술 역시 변화한다. “안전한 보안이란 영원히 존재하지 않는다”라는 것이 핵심이다. 암호화폐와 블록체인도 마찬가지 보안위협에 영원히 안전하지 않기 때문에 새로운 기술을 꾸준히 연구하고 미리 대비하는 것이 필요하다.

참 고 문 헌

[1] 한국전력공사 - 국내전력산업의 소개

https://home.kepco.co.kr/kepco/KO/C/htmlView/KOCCHP001.do?menuCd=FN05030301

[2] 전력거래소 - 주요사업 내용

https://new.kpx.or.kr/menu.es?mid=a10401010000

https://new.kpx.or.kr/menu.es?mid=a10401020000

https://new.kpx.or.kr/menu.es?mid=a10401030000

https://new.kpx.or.kr/menu.es?mid=a10401040000

https://new.kpx.or.kr/menu.es?mid=a10401050000

[3] KIRI- 보험연구원 : 블록체인의 소개

[4] 전력통계정보 시스템

[5] 재생에너지 클라우드 플랫폼

[6] 2018년 과학기술정보통신부 - 신뢰할수 있는 4차 산업혁명을 구현하는 블록체인 기술 발전 전략

[7] 한국전력공사 전력연구원 - 최인지 차장 연구 논문

[8] (주)루멘소프트 - PPA PoC 프로젝트 참조