컨소시엄 블록체인을 활용한 새로운 계약서비스에 대한 연구

권혁준*, 한명욱**, 박진일***, 한상완****

<요약>

4차 산업에서 주목받고 있는 기술 중 하나는 블록체인이다. 이 연구의 핵심은 컨소시엄 블록체인을 통해 '스마트계약' 이라는 새로운 기술을 활용하여 기존의 방식보다 효율적이고 보안성이 높은 계약서비스를 제공하는 것을 지향한다. 기존의 계약 서비스는 계약자간 직접 만나서 계약서를 검토해야하는 수작업이 많으므로 시간과 중개수수료 등 비용적인 측면에서 효율적이지 않은 부분이 있었다. 하지만 컨소시엄 블록체인을 통한 스마트계약을 활용할 경우 중개수수료가 사라지고 거래에 필요한 시간 또한 계약서상의 조건만 만족하면 자동으로 계약이 이루어지기에 기존의 계약에 비해 적은 시간이 소요된다. 비트코인의 기술인 블록체인, 이더리움의 스마트 계약은 현재 많은 분야의 산업에서 활용되어 지고 있고 개발되어 지고 있다. 따라서 이 연구에서는 계약 산업에서 컨소시엄 블록체인을 통한 스마트계약을 어떻게 활용 할 수 있을까에 대한 연구를 한다. 여기에 더하여 스마트계약의 발전가능성과 문제점에 대해서도 알아본다.

핵심주제어 : 비트코인, 이더리움, 블록체인, 스마트계약, 컨소시엄 블록체인

* (제1저자) 순천향대학교 IT금융경영학과 교수, gloryever@sch.ac.kr
** (공동저자) 순천향대학교 IT금융경영학과, skrlsla1@gmail.com
*** (공동저자) 순천향대학교 IT금융경영학과, wlsdlf322@gmail.com
**** (공동저자) 순천향대학교 IT금융경영학과, tkddhks6@gmail.com

Ⅰ. 서론

1. 블록체인 정의

현재 우리는 4차 산업혁명(The Fourth Industrial Revolution)이 일어나는 시대에 살고 있다. 여기서 4차 산업혁명[1]이란 인공 지능(Artificial Intelligence), 사물 인터넷(IOT : Internet of Things), 빅데이터(Big Data), 모바일(Mobile), 블록체인(Block Chain) 등 첨단 정보통신기술이 경제, 사회 전반에 융합되어 혁신적인 변화가 나타나는 차세대 산업혁명이다. 4차 산업혁명의 여러 기술 중 블록체인은 비트코인(BitCoin)과 함께 많은 이슈를 불러 일으켰다.

비트코인은 2009년 1월, 나카모토 사토시라는 가명의 컴퓨터 프로그래머가 만든 디지털 통화로, 지폐나 동전과 달리 물리적인 형태가 없는 온라인 가상화폐이다. 나카모토 사토시는 비트코인을 중앙 집권인 오프라인 금융권이 아닌 탈중앙화 된 온라인상에서 거래하기 위해 블록체인이라는 기술을 개발하였다. 하지만 비트코인보다는 블록체인 기술이 더 주목받았고, 다양한 분야에 적용하기 위해 개발되기 시작하였다.

여기서 블록체인이란 P2P 네트워크[2]를 통해서 관리되는 분산 데이터베이스의 한 형태로, 거래 정보를 담은 장부를 중앙 서버 한 곳에 저장하는 것이 아니라 블록체인 네트워크에 연결된 여러 컴퓨터에 저장 및 보관하는 기술이다. 따라서 모든 거래 정보가 담긴 블록체인이 네트워크를 통해 연결되어 있기 때문에 중앙 서버 운영에 따른 해킹의 위험성이 없으며, 모든 네트워크 참여자들이 블록체인에 담겨 있는 정보 및 가치를 검증, 저장, 실행함으로써 관리자가 임의로 거래 정보를 위·변조하는 것이 원칙적으로 불가능하게 설계되었다.

---

1) 네이버, IT용어사전,
(http://terms.naver.com/entry.nhn?docId=3548884&cid=42346&categoryId=42346), 2017. 11. 08

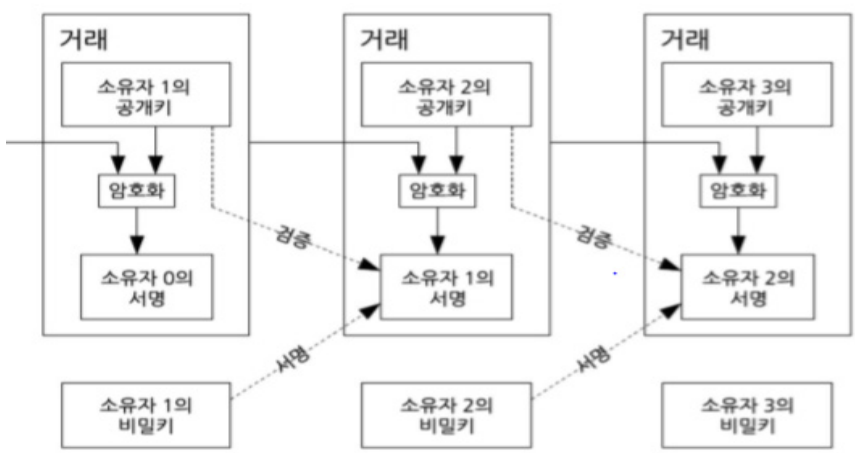
2) Peer-To-Peer Network로 컴퓨터와 컴퓨터를 직접 연결해 서버 없이도 인터넷을 통해 네트워크 내의 컴퓨터를 공유하게 할 수 있는 기술

2. 블록체인 원리

블록체인은 일정시간 동안[3] 발생한 모든 거래 정보가 기록된 '블록'을 생성, 블록체인에 연결된 모든 컴퓨터로 전송하고, 전송된 블록의 유효성이 확인될 경우 기존 블록체인에 연결하는 방식이다.

네트워크에 참여하는 각 참여자를 노드로 삼아 데이터의 보관, 공유, 관리 부담을 나누는 기술로, 중앙 서버 없이 참여자 간의 검증 및 서명을 통해 보안성과 무결성을 보장한다.

<그림 1> 블록체인 참여자 간 검증 및 서명



출처 - S. Nakamoto, 'Bitcoin : A Peer-to-Peer Electronic Cash System', 2009

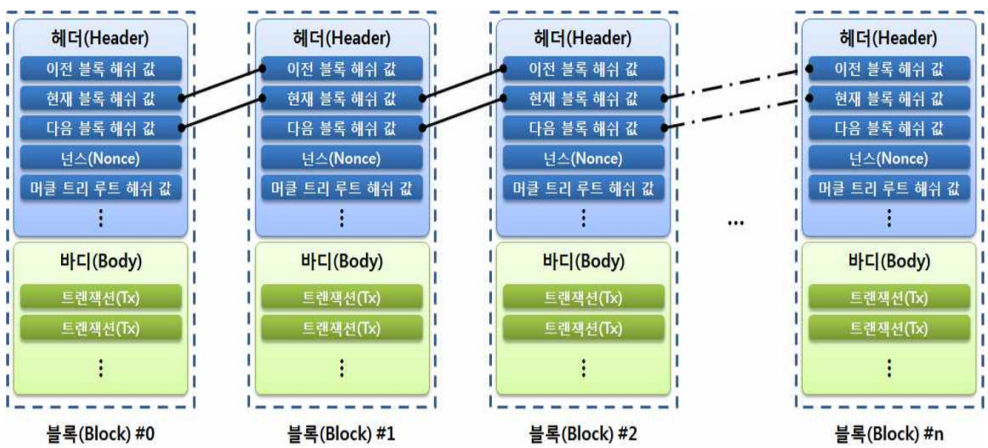
이러한 블록체인의 검증 및 서명은 공개키 기반(PKI)[4]의 암호구조로 설계되어 해킹 및 임의 조작에 대한 위험으로부터 안전하다.

3. 블록체인 구조

3) 가상 화폐의 종류마다 시간이 다름. 비트코인의 경우 약 10분을 의미함.
4) Public Key Infrastructure, 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하기 위한 복합적인 보안 시스템

블록체인은 P2P 네트워크에서 새로운 거래내역이 생성될 시 새로운 블록을 형성하고, 기존 블록에 계속 연결되는 구조를 가진다. 각 블록은 헤더(Header)와 바디(Body)로 구성된 구조로, 헤더는 이전과 현재 블록의 해시값, 난수(Nonce)를 포함한다.[5)]

<그림 2> 블록체인 연결 구조



출처 - 금융보안원, 보안연구부, '블록체인 및 비트코인 보안 기술', 2015

새로 형성된 블록의 거래내역정보는 이전 블록의 해시 값을 포함하고 있으며, 이전 블록은 다시 그 이전 블록의 해시 값을 포함하고 있다. 만약 특정 블록의 데이터를 위조 또는 해킹하려면 블록을 생성한 모든 참여자 또는 51%이상의 컴퓨터를 해킹하여 블록을 수정해야하며, 이어진 모든 블록을 수정해야 가능하기 때문에 데이터의 위·변조 및 해킹이 거의 불가능하다.

4. 블록체인 종류

블록체인은 블록체인 네트워크 참여자의 특성과 크기에 따라 여러 가지 형태로 존재하고 사용용도에 맞게 응용이 가능하다. 네트워크 참여자

5) "블록체인 및 비트코인 보안 기술", 보안연구부, 금융보안원, 2015

의 특성에 따라 구분하면, 퍼블릭 블록체인(Public Blockchain), 프라이빗 블록체인(Private Blockchain) 및 컨소시엄 블록체인(Consortium Blockchain)으로 나뉜다.[6]

1) 퍼블릭 블록체인(Public Blockchain)

퍼블릭 블록체인은 누구나 네트워크 블록에 참여 할 수 있는 블록체인을 뜻하며, 최초의 블록체인 활용사례이다. 기본적으로는 누구나 블록 후보를 만들어 제출하고 분산 합의를 통해 하나의 블록을 선정하여 신뢰할 수 있는 블록으로 인정받는 구조이다. 누구나 블록에 참여할 수 있기 때문에 인터넷을 통해 모두에게 공개되며, 운용 가능한 거래 장부가 존재한다.

하지만 참여자가 많을수록 참여자의 모든 노드를 검증해야하기 때문에 많은 시간과 컴퓨팅 파워가 요구된다. 또한 많은 노드의 검증으로 인한 거래 속도 지연의 문제점도 존재한다.

대표적인 예로는 가상화폐, 스마트 계약 플랫폼인 비트코인과 이더리움이 있다.

2) 프라이빗 블록체인(Private Blockchain)

프라이빗 블록체인은 퍼블릭 블록체인의 문제점인 거래 속도 지연과 불필요한 시간낭비를 보완하기 위해 개발된 개인형 블록체인이다. 즉, 하나의 기관에서 독자적으로 사용하는 블록체인을 말한다. 퍼블릭 블록체인과는 다르게 참여자가 제한되어 있으며, 1개의 주체가 내부 전산망을 블록체인으로 관리 및 권한을 행사한다. 그렇기 때문에 퍼블릭 블록체인보다 상대적으로 거래 처리 속도가 빠르다.

대표적인 예로는 나스닥[7]이 있다.

3) 컨소시엄 블록체인(Consortium Blockchain)

컨소시엄 블록체인은 프라이빗 블록체인과 퍼블릭 블록체인의 중간으로 협회나 조합에 참여한 기관만 블록체인 네트워크에 참여가 가능한 반중앙형 블록체인이다. 미리 선정된 N개의 주체들만 블록체인에 참여 가

6) "국내외 금융 분야 블록체인 활용 동향", 보안연구부, 금융보안원, 2015
7) 'A Bitcoin Technology Gets Nasdaq Test', The Wall Street Journal, 2015. 05

능하며, N개의 주체들 간의 합의된 규율을 통해 공중 참여가 가능하다. 네트워크 확장이 용이하고 거래 속도가 빠르다.

대표적인 예로는 R3의 Corda와 IBM의 Hyperledger Fabric가 있다.

지금까지 블록체인의 원리, 구조, 종류 등 블록체인 기술에 대해서 전반적으로 살펴보았다. 이처럼 블록체인은 중앙 서버 없이 블록체인에 참여하여 네트워크에 연결된 컴퓨터가 모든 거래 내역을 공유, 검증 및 서명함으로써 무결성을 보장하고, 해킹에 대한 위험성을 방지하는 기술로 다양한 분야에서 활용되고 있다.

이러한 강점으로 블록체인은 앞서 간략하게 얘기했던 스마트계약(Smart Contract)을 활용할 수 있는 플랫폼(Platform)이 될 수 있다. 블록체인을 통한 스마트계약은 활용하여 기존의 계약 절차에 대한 비효율성을 줄일 수 있다.

최근에 국토교통부에서는 기존에 있던 서류기반의 계약 시스템을 버리고 온라인을 통해 쉽고 빠르게 부동산 거래를 하게 만드는 시스템인 전자계약 서비스를 실행했다. 전자계약 서비스는 전자서명과 공인인증서를 통해 보안적인 측면을 강화하였다. 그러나 블록체인을 활용한 스마트계약을 도입한다면 전자계약 서비스를 이용하는 고객들에게 보다 더 많은 편리성과 높은 보안성을 가져다 줄 수 있다.

Ⅱ. 본문

1. 스마트계약(Smart Contract)

1) 정의

스마트계약(smart contract)[8]이란 개념은 1994년 Nick Szabo가 최초로 제안했다. Nick Szabo는 기존 계약서가 서면으로 되어있기 때문에 계약 조건을 이행하기 위해서는 실제 사람이 계약서대로 수행을 해야 하지만 이를 디지털 명령어화 한다면 조건에 따라 계약 내용을 자동으로 실행할

8) 'Formalizing and Securing Relationships on Public Networks', Nick Szabo, 1997

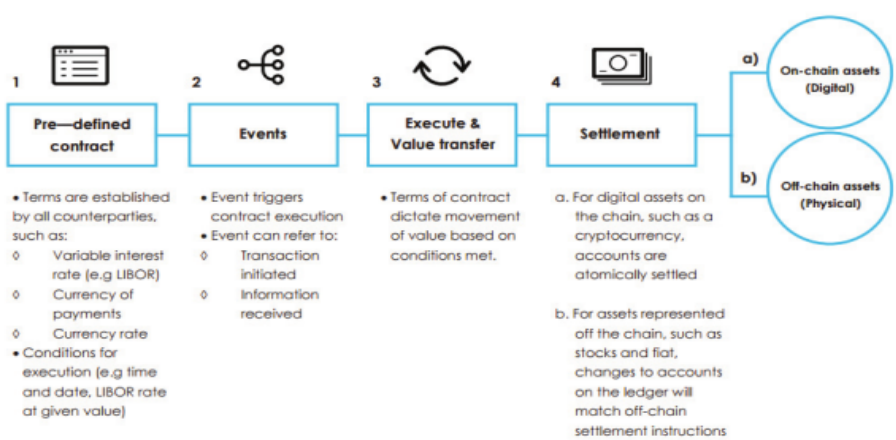
수 있다고 주장했다. 디지털로 된 계약서는 결과가 명확하고, 복잡한 프로세스를 축소시킬 수 있다는 장점이 있었지만 1994년 Nick Szabo가 제안했을 때는 디지털로 된 자료들이 쉽게 복사되어 조작이 용이하다는 단점으로 인해 개념상으로만 존재하고 구체적으로 활용되어지지 못했다.

블록체인이 존재하기 전에는 이러한 스마트계약이 실현되어지지 못했는데, 그 이유는 계약 당사자들이 각자의 데이터베이스를 소유하고 있었기 때문이다. 하지만 블록체인이라는 기술이 나옴으로써 개개인의 데이터베이스가 필요 없어지게 되었고, 네트워크 상 공유된 데이터베이스로 인해 제 3자의 개입이 필요하지 않게 되었다.

2) 이행 과정

스마트계약이 이루어지는 과정 <그림 5>와 같다. 계약을 생성하기 전 계약 조건을 블록체인 상에 프로그래밍하여 블록을 생성한다. 계약조건에는 유효기간, 거래 내용, 거래당사자 등 코드 별로 분류된 계약요소들을 채워 넣을 수 있으며, 해당 계약 조건이 만족될 때까지 계약은 실행되지 않는다. 계약조건이 블록체인 참여자에 의해 만족이 된다면, 거래는 자동적으로 실행이 된다.

<그림 3> 스마트계약 이행 과정



출처 – 한국은행 금융결제국 '분산원장 기술의 현황 및 주요 이슈'

3) 이더리움의 탄생

처음으로 블록체인을 활용한 스마트계약은 비트코인 스크립트이다. 비트코인 트랜잭션에 원시 언어인 OPCODE로 스크립트를 작성해서 보내면 조건에 따라 자동으로 거래를 실행한다. 스크립트가 올바르게 작성되면 거래를 정상적으로 이루어졌다고 간주하는 일종의 계약 개념이 있으므로 이를 계약 코드(Contract Code)로 일컫는다. 하지만 비트코인 스크립트의 한계는 반복문을 사용할 수 없다는 것과 비트코인 잔고 외의 다른 정보를 관리할 수 없다는 점이다. 이러한 한계점에도 불구하고 비트코인 스크립트에서 반복문을 허가할 경우 블록체인의 스크립트 구조로 인해 무한 루프가 발생한다. 이럴 경우 네트워크 전체가 마비되며 해커들은 쉽게 DoS(Denial of Service) 공격이 가능하다.

따라서 비트코인 스크립팅 시스템의 한계점을 극복하고자 나온 스마트계약 특화 블록체인 플랫폼이 이더리움(Ethereum)이다. 이더리움은 완벽한 어플리케이션 개발 플랫폼을 위하여 그들의 분산원장 플랫폼에 “튜링완전성”[9]을 제공하는 강력한 프로그래밍 틀을 장착했다.[10]

이는 무한대의 확정성을 가지고 있으며, 분산원장 기술에 있어 새로운 혁신이 되고 있다. 이러한 이더리움의 탄생으로 인해 본격적으로 스마트계약이라는 용어를 사용하기 시작하였다. 따라서 프로그래밍 언어를 이용하여 스마트계약을 완벽하게 설계한다면 이전에는 존재하지 않았던 프로그램에 의해 운영되는 계약형태의 사업 개념과 영역이 탄생한다.

4) 스마트계약 플랫폼 종류

현재 스마트계약을 중심으로 개발되고 있는 분산원장 플랫폼은 이더리움 외에도 다양하게 존재한다. 그 종류로는 시네레오(Synereo)와 타우체인(Tau-Chain), 그리고 큐텀(Qtume)이 있다. 시네레오의 특징이라 함은 이더리움과는 다른 튜링완전성을 보장하며, 소셜 네트워크상에서 구현중 인 것이다. 시네레오는 이더리움보다 더 나은 검증을 할 수 있는데,

9) 어떤 프로그래밍 언어나 추상 기계가 튜링 기계와 동일한 계산 능력을 가진다는 의미로 계산적인 문제를 프로그래밍 언어나 추상 기계로 풀 수 있다는 의미를 가지고 있다.
10) ‘분산원장 기술의 현황 및 주요 이슈’, 한국은행, 2016

이는 수학적으로 정확한 시맨틱에 근거하기 때문이다.

그리고 타우체인은 튜링완전성을 포기하고 결정성만을 선택했다. THeTAO[11] 사례를 통해 튜링완전성이 강력한 프로그래밍 가능성을 가지고 있다는 것을 보여주었지만 이와 동시에 매우 치명적일 수 있다는 것을 보여준다. 다시 말해 타우체인의 경우는 강력함을 포기하고 안정성을 택했다고 볼 수 있다.

마지막으로 큐텀은 EVM(Ethereum Virtual Machine)의 호환되지 않는 버전과 수정 된 비트코인 코어 인프라를 결합한 코인이다. 모듈성, 상호 운용성 및 안정성에 집중하여 설계한 큐텀은 신뢰할 수 있는 분산 응용 프로그램을 구축하기 위한 중요한 툴이다. 스마트계약의 라이플 사이클 관리와 기능 제공, 산업 표준 설정과 가장 중요한 스마트폰과 태블릿에서 블록체인을 생성할 수 있는 플랫폼을 제공한다.

블록체인의 스마트계약은 보안 측면에서 무결하다. 즉 암호화된 키값과 암호화된 데이터만으로 트랜잭션을 구성한다. 기존 시스템은 특정한 공인기관의 시스템 오류 발생 시 모든 네트워크가 마비될 수 있으며, 거래 기록과 같은 정보가 하나의 기관에 집중되어 있기 때문에 해킹과 같은 악의적인 공격에 표적이 되기 쉽다. 하지만 블록체인을 사용할 경우에는 거래 정보를 증권거래소나 은행 등의 중앙 서버에서 보관하는 방식과는 다르게 블록체인에 존재하는 모든 블록 참여자들이 거래 내역을 공유하는 시스템이다. 따라서 중앙 서버에 집중화 된 시스템이 필요 없기 때문에 비용의 감소뿐 만 아니라 거래 정보가 분산화 되기 때문에 해킹의 위험성도 감소한다.

전체 시스템의 처리 속도나 범위가 제 3자의 역량에 의해 결정되었던 기존 시스템과 다르게 블록체인은 네트워크 내의 모든 참여자가 공동으로 거래 정보를 기록/검증/보관함으로 제 3자의 개입이 없어도 거래 기록의 신뢰성을 확보하는 동시에, 빠른 속도 및 거래의 효율성을 기대 할 수 있다. 또한, 앞에서 말했듯이 실시간으로 블록체인의 여러 노드에 대한 모니터링을 가능하므로 가시성을 극대화 시킬 수 있다. 이러한 가시성은 자기부인 방지와 투명성의 기능을 얻을 수 있다.

---

11) THeTAO : 탈중앙자율조직의 첫 번째 케이스로, 투자자가 직접 운영하는 클라우드펀딩을 통해 벤처케피탈 펀드를 지향한 조직이었지만, 해킹으로 인해 운영이 종료되었다.

5) 활용 및 활용 분야

‘에스크로 서비스’란 신뢰할 수 있는 제3자가 중계하는 서비스다. 에스크로는 거래 계약을 중계하고 계약 이행을 강제하는 신뢰할 만 한 제 3자가 있기 때문에 가능한 서비스다. 스마트 계약은 신뢰할만한 제 3자의 역할을 프로그램이 대신한다. 특히 블록체인은 중앙 집권화 된 기관이 없이도 블록체인 참여자를 통해 계약의 신뢰성을 확보하고 거래를 진행한다. 이더리움 거래 자체도 스마트 계약의 사례라고 할 수 있다.

금융거래, 투표, 개인 인증 등 계약의 형태로 진행되는 모든 행위는 블록체인을 통해 스마트 계약의 형태로 구현할 수 있다. 물론 스마트 계약을 위한 프로그램 코드의 작성과 검증 등 부가적인 노력이 필요하다. 하지만 기존의 시스템보다 보안 측면의 리스크를 감소시킬 수 있기 때문에 다양한 분야에 응용되어 활용되고 금융과 비금융 분야로 분류할 수 있다.

(1) 금융 분야

현재에는 금융권의 니즈를 충족시키기 위해 블록체인 기반의 거래 플랫폼을 제공할 뿐만 아니라, 스마트계약 기능을 이용하여 중개기관의 필요성을 높이고, 거래 시간 감소 및 효율성을 높이기 위한 시스템을 개발 중이다. 상품거래 시 두 당사자의 채무를 확정하는 프로그램화 된 스마트계약을 이용함으로써 거래를 체결하는 데 활용되기도 한다.

벤처캐피탈, 엔젤투자, 클라우드 펀딩, 개인 등의 투자자와 기업을 연결시켜 투자금을 확보하기 위한 플랫폼을 제공할 때에도 계약을 사용할 수 있다. 클라우드 플랫폼을 통해 창업자에 대한 정보와 아이템에 대한 정보를 제공하고, 투자자는 투자자를 플랫폼 안에서 직접 투자할 수 있다. 이러한 방법은 무역거래에서 계약서나 신용장과 같은 문서의 위, 변조 방지와 처리절차를 간소화할 수 있다.

하지만 앞서 설명했듯이 현재 한국을 비롯해 여러 나라의 ICO를 전면 폐지하면서 스마트계약뿐만 아니라 스타트업 계열의 블록체인 기술에 대한 개발이 지체되고 있다.

(2) 비금융 분야

공증, 소유권 등과 관련된 분쟁 문서의 위조, 변조가 발생되지 않도록 하는 기술의 개발, 전자투표의 신뢰성 및 투표 메커니즘을 제공하여 선거 시스템의 투명성 제공, 상품 및 재고 관리 등의 전산화로 중개기관을 대체하는 거래 플랫폼 개발 등이 있다. 에너지 부분에서도 활용되어지고 있는데, 전력회사가 전기 자동차의 사용자의 사용자 인증을 통해 전력을 충전 받으면서 에너지 전달의 효율성과 이동성을 가질 수 있다.

최근에는 사물인터넷이 블록체인과 결합해 발전하면서 스마트계약하고 사물인터넷과 연계되어 사용되고 있다. 사물인터넷이 스스로 집 안에 있는 소모성 품목을 인식하고 용량을 확인하여 다 사용하였을 때 스마트계약을 이용하여 자동으로 주문하는 기술이 있다.

6) 발전가능성

스마트계약을 통해 만들어지고 있는 DAO(Distributed Autonomous Organization)[12] 혹은 DAPP(Distributed Autonomous Applications)[13]는 가까운 미래의 사회를 변화시킬 것은 분명하다.

스마트계약은 기존의 계약에 비해 신속하고 효율적인 사업을 가능하게 한다. 과거에 수일 혹은 수주 이상 걸리던 전통적 방식의 계약은 스마트계약에 의해 빨라지고, 계약의 자동적인 성립에 의해 신속하고 정확한 업무진행이 가능하다. 또한 기존 계약에 있었던 제 3자의 개입을 배제한다.

그 이유는 스마트계약이 기존 금융 서비스들이 가지고 있던 별도의 시스템 없이 디지털 화폐 환경 내부에 프로그램으로써 탑재될 수 있기 때문이다. 블록 참가자 간에 동기화 및 공유되는 블록체인 기술을 활용하면 서로 다른 원장들을 조화시킬 필요가 없으며, 작업의 흐름을 개선할 뿐만 아니라 스마트계약을 통해 기존 계약의 특징인 수작업에 대한 불편함을 제거할 수 도 있다.

현재 사용되어지고 있는 블록체인 기반 플랫폼에서 스마트계약의 기능은 거래 기록에 대한 위조 및 수정이 불가능하기 때문에 일반적으로 소

12) DAO(Distributed Autonomous Organization) : 탈 중앙 자율조직
13) DAPP (Distributed Autonomous Applications) : 탈중앙화 어플리케이션

유권 이전, 증여 등의 계약에서 활용되어 왔다. 하지만 미래에는 금융뿐만 아니라 법률 거래나 저작권, 공공서비스분야 까지 다양한 분야에서 적용될 가능성이 높다.

스마트계약은 시간이 지날수록 발전하면서 많은 종류의 어플리케이션을 개발할 것이다. 다음과 같은 단계를 거치면서 진화 및 발전을 할 것이라 예측된다. 현재 활발하게 이루어지고 있는 가상화폐자산의 교환부터 시작해서, 가상화폐자산을 거래할 때 의무와 권리를 존재함을 명시하고 그러한 의무와 권리를 거래 참여자가 등록함에 따라 간단한 형태의 스마트계약을 할 수 있을 것이다. 또한, 1:1의 계약이 아닌 부동산 거래와 같이 다수의 계약자가 참가하는 단계에서, 작은 규모의 중소기업, 대기업의 규모, 정부의 기능과 사회의 기능을 부분적으로 스마트계약이 활용되는 단계까지 기대할 수 있다.

THeTAO는 현재 실패한 기업으로 기록되어지고 있지만 스마트계약이 업체규모의 기능까지 실행되어진 것으로 봐선 앞으로의 발전 가능성은 무궁무진하다.

7) 한계점

이러한 높은 활용도와 발전 가능성이 있어도 현재 블록체인과 같은 문제점이 존재하고 있다.

(1) 수정불가능

블록체인에서는 이미 정해진 몇 가지 기초적인 검증 조건을 통과하면 모든 것이 기록될 수 있다. 따라서 만약에 해킹이 일어난다면 해킹된 금액의 이체를 막을 수 없으며, 실제로 다른 계약을 성사시키더라도 되돌릴 수 없다. 기본적으로 인간의 실수와 해킹 등의 사고를 인정하지 않는 시스템이기 때문에, 한번 문제가 일어나게 되면 수정이 불가능하고 체인 속에 남아있게 된다.[14)]

14) '분산원장 기술의 현황 및 주요 이슈', 한국은행, 2016

(2) 투명성

블록체인의 경우에는 기본적으로 모든 데이터가 모두에게 공개된다. 계약 내용이나 거래 내용이 모두 공개가 되는 것은 계약 당사자들에게 큰 피해를 입힐 가능성이 높다. 예를 들어 계약 당사자에 대한 모든 정보가 모두에게 공개되기 때문에 범죄가 일어날 가능성이 생긴다.

(3) 처리비용의 낭비

스마트계약은 모든 참여자들이 자료를 공유하는 방식으로, 즉 모든 노드가 동일한 작업을 한다는 뜻이다. 이는 얼마나 많은 노드가 계약에 참여하든 상관없이, 처리 효율성은 하나의 노드보다 높을 수 없다. 따라서 스마트계약이 제3자의 개입을 배제하여 중개비용이나 중앙관리로 인한 운영비용의 발생을 감소시킬 수는 있지만, 처리비용의 낭비로 인해 비효율적인 가능성이 높고, 의사결정을 하는 시간도 더 오래 걸릴 수밖에 없다.

(4) SW동일성 및 가치변동성

스마트계약을 체결하기 위해서는 모든 당사자들 간의 블록체인 소프트웨어의 버전이 동일해야 한다. 즉, 해당 소프트웨어를 계속해서 꾸준히 서로 업데이트하고 관리가 필요하다. 그리고 현재 이더리움 플랫폼에서 스마트계약을 실행할 시 이더 토큰이 필요하다. 이러한 토큰이 스마트계약을 함에 있어 필요한 경우 현재 토큰 가치의 변동은 큰 위험이 될 수 있다. 가치변동에 따라 스마트계약이 기존의 계약보다 효율적으로 될 수 있고 비효율적으로 될 수 도 있다.

2. 컨소시엄 블록체인의 필요성

1) 인프라 구축

정부와 민간이 함께 블록체인 생태계를 만들어 나가는 것이 블록체인의 잠재력을 극대화하기 위한 하나의 방법이다. 특히 계약을 이행함에 있어 참여자 간 소통이 필요한 은행 전산망 특성상 계약에 대한 시스템

구성을 위한 협의가 필수적이다.

따라서 정부와 계약에 참여하는 기업은 스마트계약에 대한 인프라를 구축하는 것은 필수적이다. 현재 대부분의 국가들이 블록체인에 대한 산업 활성화 및 기술 개발에 몰두하였고 표준화 추진 및 기술 개발, 인력 양성 등을 포함한 다양한 지원계획까지 선보였다.

그러나 가상화폐를 투자 명목으로 사용하여 수백억 원을 가로챈 범죄가 적발되고, 많은 사람들이 투기적으로 이용하는 등 피해자들이 발생하였다. 그리하여 금융업에서 가장 고 위험 범죄로 속하는 자금세탁에 대한 위험성을 야기하였다. 따라서 중국에 이어 한국 정부에서는 ICO에 대한 규제를 강화하는 방안을 발표하였다.

ICO는 코인을 통해 행하였던 클라우드 펀딩에 대한 규제를 강화한 것으로, 코인이 많은 블록체인 산업들의 기반을 형성하는 시점에서 여러 국가들의 규제는 매우 부정적일 수밖에 없다. 하지만 시간이 지날수록 블록체인에 대한 사람들의 관심은 증가하고 있고 블록체인에 대한 많은 기술이 발전하고 있는 시점에서 ICO규제는 시간이 지나면 점차 풀릴 것이라고 예상하고 있다. 그에 따라 향후 블록체인을 적용할 수 있는 조직은 활용하기 위한 인프라의 구축을 준비해야 한다.

2) 필요성

현재 블록체인 기반으로 스마트계약을 사용하기에는 토큰의 가치변동성과 처리비용의 낭비, 투명성이 주요 한계점으로 드러나고 있다. 이를 극복하기 위해서는 퍼블릭 블록체인보단 컨소시엄 블록체인을 통하여 스마트계약 서비스를 실행하여야 한다.

앞서 설명했듯이 퍼블릭 블록체인은 누구나 참여할 수 있기 때문에 블록에 기록한 모든 정보가 인터넷을 통해 열람이 가능하다. 즉, 퍼블릭 블록체인을 통해 스마트계약을 제공할 시 계약에 대한 모든 데이터가 인터넷을 통해 공개되기 때문에 계약 기밀 유출의 가능성이 있다.

누구나 참여가 가능하다는 것은 블록체인에 참여한 모든 노드가 트랜잭션을 검증한다는 뜻이다. 따라서 모든 노드의 검증에 따른 블록체인

거래 속도와 성능 하락은 빠른 속도로 이루어지는 영업 분야에선 스마트 계약을 적용하기에는 어려움이 있다.

퍼블릭 블록체인을 통해서 노드를 생성하기 위해서는 코인을 필요로 하는데, 현재 코인에 대한 가치변동성이 매우 심하기 때문에 처리비용의 낭비에 대한 한계점은 더욱 심화될 것이다.

하지만 컨소시엄 블록체인을 사용하여 스마트계약을 진행할 시 앞서 얘기한 한계점을 해결할 수 있다. 컨소시엄 블록체인은 운영주체가 명확하고, 새로운 금융거래를 하는 것이 아닌 기존에 있던 금융거래를 통해서 이행하기 때문에 모든 금융 관련법과 규제사항을 준수한다. 스마트계약에 대한 규제사항은 법적으로 보장된다.

퍼블릭 블록체인에서 사용하는 알고리즘은 블록 생성 후 나중에 블록이 확정되기 때문에 확정되는 시간 안에 네트워크 분기가 생길 수 있다. 따라서 정확하고 확실한 데이터를 보장해야 하는 계약의 특징에 분기 발생 위험은 적합하지 않다. 하지만 컨소시엄 블록체인은 비잔티움 장애 허용 계열의 분산합의 알고리즘을 사용하여 네트워크의 분기를 허용하지 않기 때문에 더욱 스마트계약과 어울린다.

또한, 노드 간 권한을 다르게 설정하여 허가 받은 대상들만 노드로 참여할 수 있기 때문에 퍼블릭 블록체인보다 상대적으로 투명성으로 인한 위험성에서 안전하고, 노드 상에는 컨소시엄 블록체인에 참여하여 권한을 부여받은 기업만 존재하기 때문에 계약체결 속도가 퍼블릭 블록체인에 비해 상당히 빠르다. 가치 변동성에 대해서도 컨소시엄 참여자들만의 코인을 생성하여 노드를 형성하기 때문에 가치변동성에 대한 한계도 해결할 수 있다.

현재 컨소시엄 블록체인을 활용하여 금융권에 도입하고 있는 대표적인 업체로는 R3의 Corda가 있다. 블록체인 도입 초반에는 블록체인의 특징인 탈중앙화에 대한 금융권의 저항이 심하였고, 그에 따른 많은 요구사항이 생겨났다.

대표적인 요구사항은 서로 권한이 다른 노드들, 스마트 계약, 커스터마이징, 빠른 속도이다. R3는 금융권들의 니즈를 만족시키기 위해 컨소

시엄 블록체인을 형성하였고 Corda라는 플랫폼을 개발했다.

R3의 Corda는 앞서 말한 금융권들의 니즈를 받아들이고자 모든 블록체인 참여자들이 데이터를 공유하는 방식을 포기하고 서로 권한을 가진 사람들만 노드에 참여하여 데이터를 공유하는 방식으로 생겨났다. 스마트계약의 한계점인 투명성을 극복할 수 있고, 이러한 특징은 스마트계약을 실행하면 권한을 가진 참여자들이 역할에 따라 스마트계약을 검증, 데이터 공유하는 일을 수행하는 플랫폼이다. 현재 전 세계적으로 많은 은행들이 블록체인에 대한 미래성을 보고 참여하고 있는 컨소시엄 블록체인이다.

따라서 HUG는 R3처럼 계약 업무와 관련된 기업들과의 컨소시엄 블록체인을 형성하거나, 기존에 만들어진 컨소시엄 블록체인에 가입하여 스마트계약에 필요한 요소를 확충할 필요가 있다.

Ⅲ. 결론

계속해서 진행 중인 4차 산업혁명 시대에는 다양한 신기술이 계속해서 적용 및 개발될 것이며, 다양한 분야에 적용될 것이다. 블록체인 또한 많은 강점으로 인해 계속해서 개발될 것이며, 보안성과 기밀성이 요구되는 금융 분야에는 특히 강조될 것이다.

HUG에서 주로 서비스하는 보증계약의 경우 계약자간의 정확한 계약이행과 확실한 신뢰관계 및 철저한 보안성을 필요로 한다. 스마트 계약을 활용한다면 기존 계약의 복잡한 프로세스를 스마트계약을 통해 간소화 시킬 수 있으며 보안성 또한 강화 시킬 수 있다.

이처럼 보안성과 기밀성이 요구되는 분야에 강조되는 만큼 계약 부분 업무가 많이 차지하는 HUG에 스마트계약 플랫폼을 적용하는 것은 필수적일 것이다.

본고에서는 블록체인이 현재 어떠한 작용을 하고 있으며, HUG에 컨소시엄 블록체인을 통해 스마트계약 플랫폼을 도입할 시 어떠한 이득을 얻는 가에 대해 제시하였다.

현재 많은 사람들이 수기로 작성하는 기존의 계약 방식에 불편함을 느끼고 있으며, 제 3자로 인한 데이터 유출 및 위·변조의 가능성에 대해 위험을 느끼고 있다.

블록체인을 활용한 스마트계약 플랫폼은 데이터 해킹, 데이터 위·변조 가능성에 대한 위험을 감소시켜주며, 디지털로 이루어지는 편리함, 수수료 감소, 빠른 체결 속도는 많은 사람들에게 HUG를 긍정적으로 인식시키는 계기가 될 것이다.

논문접수일	2017.11.03.
논문심사일	2017.11.16.
게재확정일	2017.12.07.

참고문헌

- 김정규·이주연, 2017, “디지털혁신과 금융서비스의 미래 : 도전과 과제”, 지급결제조사자료 2017 - 1호, 금융결제국
- 보안연구부 보안기술팀, 2015(a), “블록체인 및 비트코인 보안 기술”, 보안연구부-2015-029호, 금융보안원
- 보안연구부 보안기술팀, 2015(b), “국내외 금융 분야 블록체인 활용 동향”, 보안연구부-2015-028호, 금융보안원
- 최복용·함영욱, 2016, “블록체인을 활용한 디지털 증거의 무결성 강화 방안 연구”, 치안정책연구 제30-3호 09, 치안정책연구소
- 한국은행, 2016, “분산원장 기술의 현황 및 주요 이슈”
- Antonopoulos, A. M., 2015, “비트코인, 블록체인과 금융의 혁신(Mastering Bitcoin)”, 고려대학교 출판문화원
- Nakamoto, S., 2008, “Bitcoin : A Peer-to-Peer Electronic Cash System”
- Szabo, N., 1997, “Formalizing and Securing Relationships on Public Networks”
- Hope, B., Casey, M. J., 2015. 05. 10, “A Bitcoin Technology Gets Nasdaq Test”, The Wall Street Journal
- 네이버 IT용어사전, 2017. 11. 08, 4차 산업혁명 “http://terms.naver.com/entry.nhn?docId=3548884&cid=42346&categoryId=42346”

A Study on the New Contract Service Using Consortium Block Chain

Kwon Hyuk Jun*, Myeong Uk Han**, Jin-il Park***,
Sang Wan Han****

<Abstract>

One of the key technologies in the fourth industry is the block chain. The focus of the study is to utilize the consortium block chain to leverage new technologies called 'smart contract' to deliver more efficient and secure contract services than conventional approaches. Traditional contract services have met contracts to review and write manually. so there are less effective aspects, such as time and brokerage fees, in terms of time and brokerage. However, using a Smart contract through a consortium block chain, the brokerage fees disappear and the time required to deal with the transaction is automatically shortened compared to conventional contracts, if the contract is satisfactory. Bitcoin's technology chain, Block Chain, and ethereum's smart contract are currently being utilized and developed in many fields of industry. Therefore, the study examines how the contract can be used by the consortium block chain. In addition, we will explore the possibilities and problems of smart contract.

Key Word : Bit coin, Ethereum, Block Chain, Smart Contract. Consortium Block Chain

* (First Author) Soon Chun Hyang Univ. IT Finance Management Professor. Email : gloryever@sch.ac.kr
** (Co-Author) Soon Chun Hyang Univ. IT Finance Management, Email : skrlsla1@gmail.com
*** (Co-Author) Soon Chun Hyang Univ. IT Finance Management, Email : wlsdlf322@gmail.com
**** (Co-Author) Soon Chun Hyang Univ. IT Finance Management, Email : tkddhks6@gmail.com