제2부. 기술적 이슈

Ⅰ. 블록체인 기술 개발 및 연구 현황

본 장은 주요 사례들을 중심으로 각 분야에서 현재 추진중인 블록체인 기술의 연구 및 개발 방향과 대표적인 활용 분야에 대해 서술한다.

1. 블록체인 컨소시엄

블록체인 컨소시엄은 블록체인에 대한 활용 방안을 찾고자 하는 기업 및 기관들이 블록체인을 연구하고 최종적으로는 여러 기업 및 기관들이 함께 사용할 수 있는 공동의 블록체인망을 개발하는 모임을 의미한다. 주로 블록체인 기술을 기반으로 하는 스타트업이 중심이 되고, 블록체인 시스템을 연구 또는 활용하고자 하는 기업들이 모이면서 구성된다. 최근에는 금융기관뿐 아니라 블록체인 활용 방안을 찾고자 하는 비금융기관들도 컨소시엄에 참여하는 추세이다. 블록체인은 기본적으로 분산형 네트워크이고 중앙의 통제자 대신 여러 서버가 노드를 담당하고 네트워크를 분할해서 운영하는 시스템이다. 따라서 특정 기업이 단독으로 개발해서 상용화하는 경우 오히려 블록체인 네트워크를 활성화하고 효율적으로 활용하는데 제약이 될 수 있으며, 많은 기업들이 블록체인 네트워크를 함께 구성해서 사용하는 것이 규모의 경제를 구축하고 블록체인의 효율성을 높이는데 더 적합하다. 이러한 이유로 많은 기업이 컨소시엄을 구성해 공동으로 활용할 수 있는 블록체인 플랫폼을 만들기 위해 연구하고 있다.

가. R3 CEV

블록체인 컨소시엄의 대표적인 사례 중 하나는 R3 CEV이다. R3 CEV 컨소시엄은 블록체인 기술 기업인 R3가 중심이 되어 은행 등 금융기관이 활용할 수 있는 블록체인을 연구 및 개발하는 것을 목표로 하는 컨소시엄으로 현재 60개 이상의 금융기관이 참여하여 연구를 진행하고 있다. 국내 은행 중에는 하나은행이 최초로 R3 CEV에 가입했으며[100], 신한은행, KB국민은행, 우리은행, IBK기업은행이 가입을 마무리했거나 진행중인 등 다른 국내 금융기관들도 참여에 관심을 보이고 있다.[101] R3 CEV의 가장 두드러진 성과는 지난 3월 금융 기관에 특화된 블록체인 서비스인 코다(Corda)를 개발하여 발표한

100) http://www.hanafn.com/pr/news/newsDetail.do?seq=3317&page=0
101) http://www.ddaily.co.kr/news/article.html?no=147909

것이다. 비트코인, 이더리움 등과 달리 유통되는 내부화폐가 없는 코다는 금융기관의 계약을 관리하고 기록하기 위해 만든 블록체인 플랫폼으로 블록체인의 특징인 분산화된 메커니즘을 유지하는 동시에 금융기관에서 활용하기 더 편리하도록 설계한 서비스이다. R3 CEV는 코다에 거래 당사자와 조정기관만이 거래 내역을 확인할 수 있는 정보 공개 권한 범위 설정, 합의 메커니즘의 다양화 및 스마트 계약(smart contract) 기능 등 기존 블록체인 대비 여러 기능을 추가 및 조정했다고 발표했다.[102] 이후 금융 기업 바클레이스와 함께 코다를 기반으로 한 스마트계약 탬플릿 시연회를 개최하기도 하는 등 금융기관용 블록체인 컨소시엄 가운데 가장 많은 협력 기업을 가지고 있고 대외적으로 많이 알려져 있다.[103]

<그림 1-1> 바클레이스와 시연한 코다 소개 영상

자료: Barclays

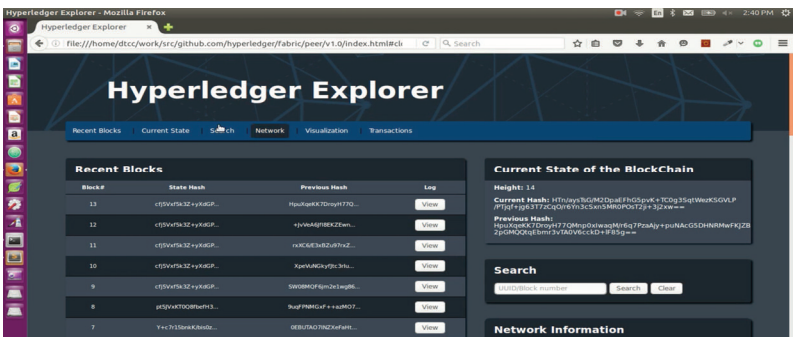
올해 10월 R3 CEV는 코다의 코드를 오픈소스화하여 11월 30일에 범산업 블록체인 컨소시엄인 하이퍼레저(Hyperledger)에게 제공한다고 발표했다. R3 측은 각 기관이 다른 블록체인 플랫폼을 만들어 각자가 섬처럼 소통할 수 없는 결과를 초래하지 않도록 표준화하는 방법으로 코다의 코드를 하이퍼레저에 제공하기로 결정했으며 코다가 금융산업 블록체인의 표준이 되기를 바란다고 밝혔다.[104]

102) http://www.coindesk.com/r3cev-blockchain-regulated-businesses/
103) https://www.youtube.com/watch?v=1UhrmsTZNvc
104) http://www.reuters.com/article/us-banks-blockchain-r3-exclusive-idUSKCN12K17E?feedType=RSS&feedName=technologyNews

나. 하이퍼레저 프로젝트 (Hyperledger Project)

R3 CEV가 금융기관이 활용할 수 있는 블록체인 구성을 목표로 결성된 컨소시엄이라면, 하이퍼레저 프로젝트(Hyperledger Project)는 비금융기관까지 참여해 공동으로 사용하는 범산업용 블록체인 플랫폼 구성을 목표로 하는 컨소시엄이다. 리눅스 재단(Linux Foundation)이 주도하는 오픈소스 블록체인 컨소시엄인 하이퍼레저 프로젝트에는 현재까지 100여개의 기업이 가입하였으며 인텔, IBM 등 대형 IT 기업, R3, 코인플러그 등 블록체인 기술 기업, JP모건 등 금융 기업 및 제조사, 컨설팅 업체 등 다양한 분야의 기업들이 참여하고 있다. 한국에서는 한국예탁결제원과 삼성SDS가 하이퍼레저 프로젝트에 가입하였다.[105][106] 다양한 기업군들이 모인 컨소시엄인만큼 컨소시엄 내에서 협업 및 개발을 통해 다양한 블록체인 활용 방안을 연구하고 있고 이와 관련한 신규 플랫폼들도 발표하고 있다. JP모건에서 발표한 스마트 계약 기반 블록체인 플랫폼 Juno[107], 컨설팅 기업인 엑센츄어(Accenture)에서 제안한 블록체인 기반 약품 정품 인증 플랫폼[108] 등 하이퍼레저 프로젝트 내에서 다양한 블록체인 활용 방안이 연구되고 있다. 또한 IBM, 인텔, DTCC 등이 공동으로 하이퍼레저 참여 기업들이 자유롭게 블록체인을 활용할 수 있는 내부 오픈소스 서비스인 하이퍼레저 익스플로러(Hyperledger Explorer)를 개발하는 등 참여 기업간 자유로운 협업을 통해 블록체인 활용 방안을 연구하고 있다.[109]

<그림 1-2> 하이퍼레저 익스플로러 시연 자료



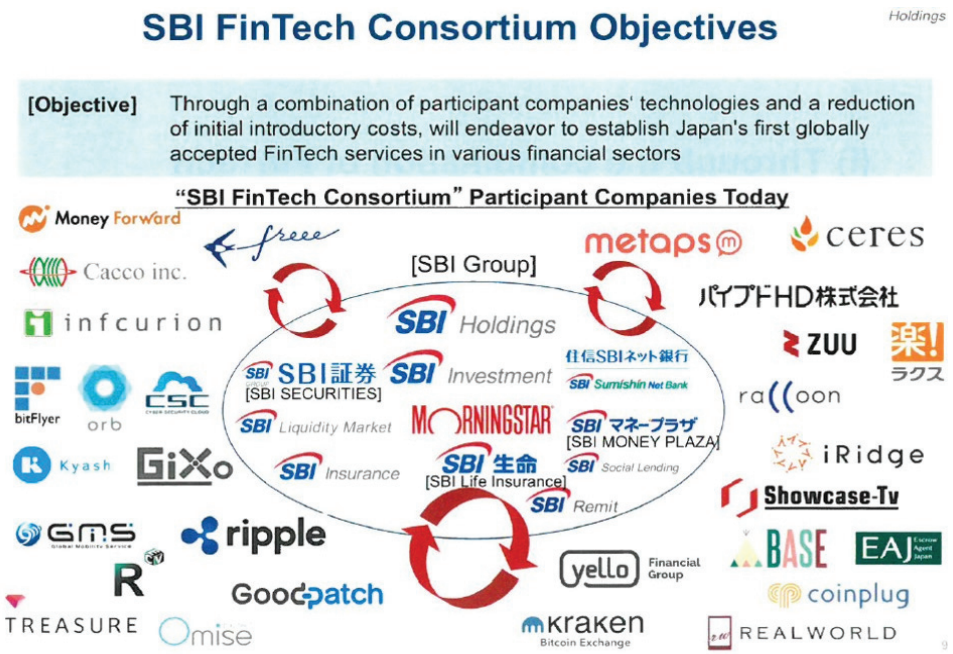
자료: Coindesk

105) https://www.hyperledger.org/announcements/2016/08/30/hyperledger-project-grows-170-percent-in-six-months
106) https://www.hyperledger.org/announcements/2016/07/27/hyperledger-project-has-welcomed-more-than-60-members-since-february
107) https://bitcoinmagazine.com/articles/jpmorgan-unveils-juno-prototype-at-hyperledger-meeting-1457629074
108) http://www.coindesk.com/hyperledger-counterfeit-drugs-blockchain/
109) http://www.coindesk.com/hyperledger-first-blockchain-explorer/

다. 아시아 지역의 블록체인 컨소시엄

아시아 시장에서도 시장 특성을 고려한 블록체인 개발을 목표로 하는 컨소시엄이 다수 구성되고 있는데, 일본의 SBI 핀테크 컨소시엄과 중국의 차이나레저(Chinaledger)가 대표적인 사례이다. SBI 핀테크 컨소시엄은 일본의 SBI 금융그룹이 주축이 되어 만든 컨소시엄으로, 블록체인을 기반으로 사물인터넷 등 금융권과 핀테크 분야의 활용법을 모색하고 있다. 빅데이터, 사물인터넷, 인공지능 등 신기술을 금융 분야에 적용할 수 있는 핀테크 생태계 구축을 목표로 만들어진 컨소시엄으로, 이같은 신기술을 적용할 수 있는 근간 시스템을 블록체인으로 보고 이에 대한 연구 및 개발을 추진중이다. SBI 금융그룹의 계열사 이외에도 금융기관용 블록체인 프로토콜인 리플, 코인플러그 등이 동 컨소시엄에 합류하였으며, 아시아에서 활용할 수 있는 블록체인 플랫폼 및 이를 활용한 핀테크 상품을 만드는 것을 목표로 한다.[110]

<그림 1-3> SBI 핀테크 컨소시엄 가입 회원들



일본에 SBI 컨소시엄이 있다면, 중국의 대표적인 블록체인 컨소시엄으로는 차이나레저(Chinaledger)를 들 수 있다. 차이나레저는 올해 5월 중국의 완샹

110) https://www.sbigroup.co.jp/english/investors/disclosure/presentation/pdf/160519presentations.pdf

(Wanxiang) 블록체인 랩을 주축으로 중국의 대형 금융기관들이 참여한 블록체인 연구 컨소시엄이다. 구체적인 기업의 리스트와 프로젝트 내용이 공개되지 않았지만, 중국내 약 11개의 대형 금융기관이 프로젝트에 참여했다고 발표했으며, R3 CEV와 이더리움 재단이 자문위원으로 참여했다. 차이나레져는 중국 내 금융기관 간 통용할 수 있는 오픈소스 블록체인 플랫폼 개발을 목표로 연구 및 개발을 진행할 예정이다.[111] 특히 완샹 그룹은 블록체인에 대해 공격적 투자를 하고 있어 컨소시엄 성장에 긍정적인 영향을 줄 것으로 예상된다.

2. 블록체인 프로토콜

블록체인 컨소시엄을 통해 여러 기업 및 기관들이 협업하여 공동으로 사용할 수 있는 블록체인 네트워크를 만들기 위한 시도와 함께, 블록체인의 활용 방안을 확장하고 새로운 대안 블록체인을 개발하고자 하는 프로토콜 개발도 진행되고 있다. 이더리움(Ethereum), 리플(Ripple) 등이 대표적인 사례인데, 이들 프로토콜은 블록체인을 기반으로 비트코인 이외의 다른 서비스에 블록체인을 활용할 수 있는 플랫폼으로서 블록체인의 기존 장점을 유지하면서도 비트코인 블록체인 등이 가지는 한계들을 극복하기 위한 대안이다.

가. 이더리움(Ethereum)

이더리움은 2013년 해커인 비탈릭 부테린(Vitalik Buterin)이 차세대 분산 어플리케이션 플랫폼이라는 이름으로 백서(Whitepaper)를 발표하면서 알려지기 시작한 블록체인 프로토콜이다. 개발자인 비탈릭 부테린은 이더리움 프로토콜로 2014년 World Technology Award에서 페이스북 창업자인 마크 주커버크를 제치고 IT Software 부문을 수상자가 되었다.[112]

이더리움 블록체인 프로토콜이 가진 가장 큰 특징은 블록체인의 응용 범위를 넓게 확장시켰다는 것이다. 우선 기능이 제한적이던 기존의 블록체인과 달리 이더리움은 프로그래밍 언어 단위를 잘게 분할하여 응용하는 사실상의 튜링 완전 언어(Turing Complete Language)를 구현한 블록체인 프로토콜이다. 언어단위를 잘게 쪼갠 블록체인 프로토콜이기 때문에 이더리움 위에서는

111) https://bitcoinmagazine.com/articles/china-joins-the-blockchain-race-with-chinaledger-alliance-1462204569
112) http://www.wtn.net/summit-2014/2014-world-technology-awards-winners

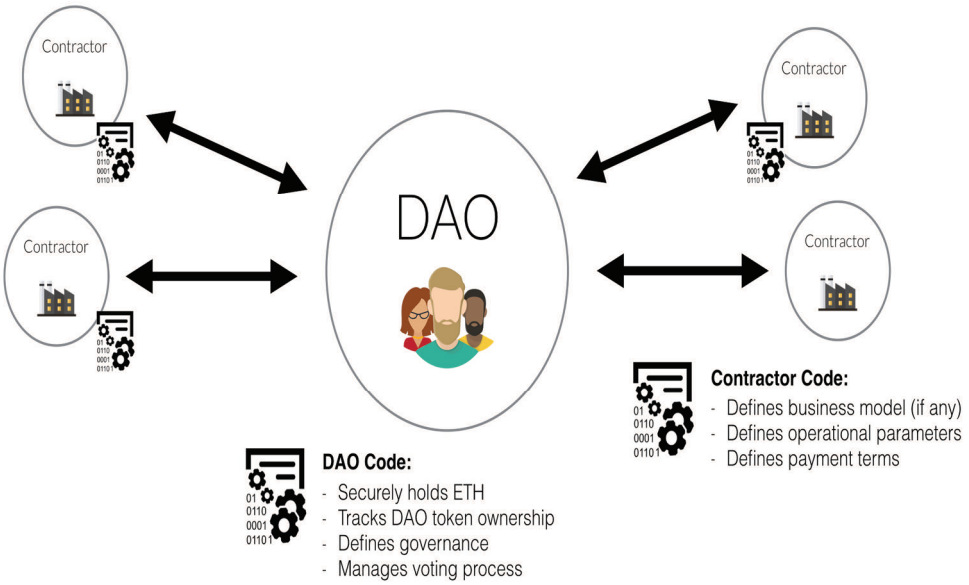
다양한 경우의 수를 가진 프로그램을 개발할 수 있다는 장점이 있다. 하지만 그만큼 구현할 수 있는 프로그램의 경우의 수도 늘어나기 때문에 다양한 보안상의 공격에 대비해야 한다는 과제 또한 존재한다.

또한 이더리움이 가장 각광을 받는 블록체인 프로토콜로 꼽히는 이유는 스마트 계약(Smart Contract) 시스템에 특화하여 개발된 블록체인 프로토콜이기 때문이다. 스마트 계약은 법적 거래 혹은 계약을 컴퓨터 코드로 짜놓은 프로그램으로 거래 내용, 유효 기간, 거래 당사자 등 코드별로 분류된 계약 요소들을 채우고 이 조건이 충족되면 자동으로 계약이 실행 및 종료되는 시스템이다. 기존에 법적 중재자나 집행인이 필요했던 방식과 달리 서로의 합의 하에 내용을 채우면 자동으로 만들어지는 자기 강제적 언어 기반의 플랫폼이기 때문에 계약 내용의 구성이 잘 되고 신뢰할 만한 기반을 가진다면 익명의 사람들이 서로에 대한 신뢰나 중개기관이 없이도 시간과 비용을 절감하며 계약을 체결할 수 있는 시스템을 구축할 수 있다. 현재 비트코인 방식 블록체인의 경우 분산원장 데이터베이스로서 비용, 보안, 속도 등의 측면에서 기존 시스템을 개선할 수 있는 기술로 주목받고 있지만, 비트코인 이후 기술을 활용할 만한 두드러진 대표 컨텐츠가 나오지 않은 상황이다. 스마트 계약은 데이터베이스를 저장하는 플랫폼으로서의 블록체인의 기능을 상당 부분 확장할 수 있고 활용도를 높일 수 있기 때문에 만약 블록체인 위에 스마트 계약을 구동할 수 있는 시스템이 갖춰진다면 금융 거래, 무역, 계약, 인증 등 수많은 분야에서 블록체인의 활용도를 획기적으로 높일 수 있다. 아직은 초기 단계로 완전하게 구현된 것은 아니지만 이미 기초적인 스마트 계약 시스템이 개발되었고, 향후 스마트 계약을 구현하는 프로토콜로 발전될 것으로 전망된다. 또한 비트코인 블록체인에서 거래를 처리하는데 소요되는 약 10분이라는 시간 제약을 극복하고 12초 내외에 거래가 처리되도록 시스템을 구성하는 등 비트코인 블록체인의 거래의 확장성 문제도 일정 부분 극복했다.

이더리움은 현존하는 블록체인 프로토콜들 중 활용 가능 범위가 넓기 때문에 마이크로소프트 등 많은 기업들이 이의 활용에 관심을 보이고 있고, 다수의 블록체인 스타트업들도 이더리움의 화폐 단위인 이더(Ether) 거래소부터 스마트 계약까지 이더리움을 활용하는 프로그램 및 서비스 개발을 진행중이다. 최근 화제가 된 분산형 자치 조직 DAO(Decentralized Autonomous Organization)는 이더리움이 적용된 대표적인 사례다. DAO는 이더리움을 활

용하여 중앙 운영주체가 없이도 분산과 자율을 바탕으로 운영되는 크라우드 펀딩 플랫폼으로서 최고경영자, 대표, 이사회 등이 없이 다수가 자유롭게 이더리움 프로토콜을 통해 익명으로 펀딩에 참여할 수 있다. 이 플랫폼에는 이더리움의 내부 화폐인 이더(Ether)를 보유하고 있으면 누구라도 참여해 투자를 할 수 있는데, 이더를 소유한 사람은 DAO에 참여하기 위해 보유한 이더를 DAO의 주소로 전송하고 동일한 가치의 DAO코인을 받게 된다. 아이디어를 가지고 있는 사람은 누구든지 DAO에 자신의 아이디어를 게시할 수 있고, DAO 토큰을 가진 사람은 원하는 아이템에 자유롭게 투자할 수 있으며, 투자한 토큰의 수만큼 투표권이 주어지고 수익 또한 투자한 토큰 지분만큼 할당받게 된다. 투자를 받고자 하는 사람은 이더리움의 스마트 계약 코드에 따라 투자 유치 신청서를 제출하고 투자자들은 그 코드를 확인하고 투자하며, 코드에 따라 계약이 자동적으로 실행된다. 약 한 달간의 투자자 및 투자금 모집에서 DAO는 크라우드 펀딩 역사상 가장 많은 금액인 약 1억 6천만 달러의 투자를 유치하면서 가장 성공적인 블록체인 적용 사례로 평가받고 있다.

<그림 1-4> 이더리움 기반 크라우드펀딩 플랫폼 The DAO



자료: The DAO

그러나 DAO는 최근 해킹 공격을 받아 안정성에 대한 의심을 받기도 했다. DAO에는 투자를 위해 전환한 DAO 토큰을 다시 이더로 바꾸는 스플릿

(Split) 기능이 있는데, 해커는 이 스플릿 기능의 취약점을 공격하여 같은 토큰을 여러 번 인출하도록 함으로써 약 5,500만 달러의 금액을 추가로 인출하였다. 이 사태를 해결하기 위해 이더리움 재단과 커뮤니티는 논의와 투표 끝에 DAO와 연관된 이더 자금에 대해 또 다른 블록체인 프로토콜을 만들어 새 블록체인에 가치가 유지되도록 하는 이른바 하드 포크(Hard Folk)를 시행하기로 결정했다. 하드 포크는 성공적으로 실행되어 해커가 해킹을 통해 획득한 이더는 가치가 없게 되었다. 하지만 이같은 결정에 반발한 소수의 사용자 및 개발자들이 기존 이더리움 프로토콜에 잔류를 선언했고, 그 결과 이더리움 시스템은 하드 포크로 새롭게 생성된 이더리움과 기존의 이더리움 프로토콜에 잔류해 있는 이더리움 클래식(Ethereum Classic)으로 이원화되어 존재하고 있다. DAO 해킹 사건의 사례는 이더리움 플랫폼 자체의 결함보다는 이를 적용한 DAO라는 어플리케이션의 맹점을 공격한 사례이기 때문에 이더리움은 여전히 차세대 블록체인으로서 주목을 받고 있지만, 이더리움 개발을 담당하는 이더리움 재단 측에서는 이번 사태를 통해 발견된 문제점들을 바탕으로 이더리움의 확장성과 보안성 향상을 목표로 지속적으로 이더리움 개발을 진행중이다.

최근 많은 기업들은 이더리움의 높은 활용도에 주목해 단순한 이더리움 기반 서비스 개발을 넘어서 이더리움 기반 폐쇄형 블록체인(Private Ethereum) 플랫폼을 개발하고 있다. 올해 10월 세계 최대 금융기관 중 하나이자 하이퍼레저의 참가 기관인 JP모건은 Quorum이라는 이름의 이더리움 기반 자체 폐쇄형 블록체인 네트워크를 개발했다고 발표했다.[113][114] 또한 미디어기업이자 최근 하이퍼레저에 가입한 톰슨 로이터도 이더리움을 기반으로 하는 블록체인 플랫폼인 BlockOne을 발표하는 등 이더리움을 블록체인 플랫폼으로 활용하여 개발하는 사례가 증가하고 있다.[115][116]

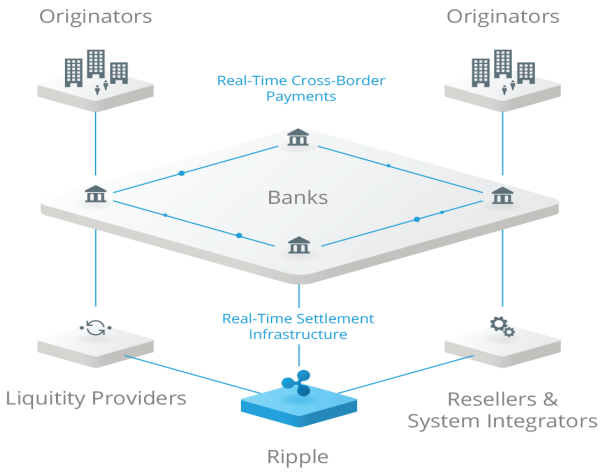
나. 리플(Ripple)

리플(Ripple)은 블록체인 프로토콜 중 국가 간 혹은 금융기관 간 송금 및 결제에 초점을 맞추어 개발한 블록체인 프로토콜이다. 블록체인 기술은 송금 분야에서 기존 시스템의 비효율적인 요소를 해결할 수 있는 기술로 평가받

113) http://www.coindesk.com/jpmorgan-ethereum-blockchain-quorum/
114) https://www.cryptocoinsnews.com/jp-morgan-joins-ethereum-developing-private-blockchain-quorum/
115) https://blockone.thomsonreuters.com/
116) http://www.coindesk.com/thomson-reuters-blockchain-ethereum-devcon2/

는다. 특히 해외송금 시스템의 경우 송금을 위해 여러 중개은행들이 개입하고 SWIFT 등 국제송금 전용 전신망을 사용하는 등 다수의 제3기관의 개입으로 많은 수수료 비용이 발생하고, 결제 요청 통신, 완료 통신 등 각 과정마다 결과가 따로 생성되는 등 복잡한 절차가 필요할 뿐 아니라 결제 완료 시점까지 결제 리스크에 노출되기도 한다. 또한 다른 금융기관들이 각자의 시스템을 통해 결제 및 청산을 하기 때문에 해외송금이 완료되기까지 1주일 이상이 걸리기도 할 정도로 비효율적인 시스템을 가지고 있다. 리플은 현재의 복잡한 송금 시스템을 극복할 대안으로 블록체인의 분산된 네트워크를 이용해 중개기관을 최대한 배제하는 신속한 송금과 실시간 결제 및 청산 시스템 구축을 시도하고 있다. 기존에 여러 단계를 통해 이루어졌던 복잡한 송금 및 결제를 분산원장이라는 하나의 플랫폼을 만들어 빠르고 간단한 결제 시스템을 구축하는 것이 리플의 목표이다.

<그림 1-5> 리플의 시스템 구조



자료: Ripple

리플 프로토콜에서는 XRP라는 이름의 화폐단위를 사용한다. XRP는 총 1천억개 정도가 이미 발행되어 있으며 한 번 거래가 이뤄질 때마다 0.00001XRP가 수수료로 지불된다. 리플 네트워크에 참여하는 금융기관이 일반적인 이체나 환전을 할 때는 XRP를 활용할 필요없이 리플의 블록체인 시스템을 활용하여 송금 및 결제를 할 수 있지만, XRP를 매개로 활용하면 마일리지, 카드 포인트 등 다른 종류의 화폐나 유가물도 교환할 수 있게 된다. 지난 7월 리플에서 발간한 보고서에서는 현재 은행 시스템은 매우 거대하기 때문에 당장 모든 은행이 전 분야에서 블록체인을 송금 플랫폼으로 적용할 수는 없겠

지만, 현재의 고비용의 비효율적인 송금시스템을 개선할 수 있는 방안으로서 블록체인 기반 송금 시스템의 적용 분야를 조금씩 넓혀간다면 금융기관들은 획기적인 비용절감과 효율성 증가의 효과를 기대할 수 있을 것이라고 밝혔다.[117]

리플은 송금 및 결제에 초점을 맞춘 블록체인 프로토콜인 만큼 금융기관과의 협업에 적극적인 행보를 보이고 있다. 장기적으로는 SWIFT를 대체하는 송금 및 결제 플랫폼을 만들기 위해, 다수의 금융기관이 참여하는 블록체인 기반 지불결제 네트워크 구성을 목표로 하고 있다. 지난 5월에는 산탄데르(Santander) 은행 영국 지부와 일본의 미즈호 은행이 리플의 블록체인을 기반으로 하는 Payment 시스템 개발 계획을 발표했고 이를 금년중 출시하는 것을 목표로 테스트 중이라고 밝혔다.[118] 지난 7월에는 다국적 기업용 소프트웨어 기업인 SAP가 두 은행과 합작하여 블록체인 기술을 활용한 국가 간 송금 및 결제 시스템의 기술검증을 진행할 계획이라고 발표했다.[119]

올해 9월에는 리플과 여섯 개 은행이 함께 분산원장 기술을 기반으로 은행 간 해외 송금 및 결제 시스템을 개발하는 Global Payments Steering Group (이하 GPSG)을 결성했다. GPSG은 금융기관과 협업을 통해 기존 플랫폼보다 더 신속하게 송금할 수 있는 분산원장 시스템을 개발하고 이와 동시에 분산원장 기반 송금 및 결제에 대한 표준과 운영 방식에 대한 합의안을 만들어 은행들이 활용할 수 있는 블록체인 플랫폼을 만들 계획이다.[120] 이외에도 리플은 다양한 금융기관과 마이크로소프트, MIT 등과의 공동 연구를 진행하는 등 다양한 기업들과의 협업을 통해 자사의 프로토콜을 활용하여 결제시장에서 블록체인을 활용할 수 있는 방안을 모색중이다.

다. 디지털 에셋 홀딩스(Digital Asset Holdings)

디지털 에셋 홀딩스는 JP모건 임원 출신인 Blythe Masters가 설립한 블록체인 기업으로 자본시장을 위한 분산원장을 개발중이다. 자본시장에서 활용할 수 있는 디지털 자산 모델링 언어(Digital Asset Modeling Language, 이하

117) The journey to Real-time cross border commercial payments using distributed ledger technology, Ripple and Accenture, 2016
118) http://www.coindesk.com/santander-uk-payments-app-ripple/
119) https://bitcoinmagazine.com/articles/sap-and-ripple-collaborate-on-cross-border-payments-trial-using-blockchain-technology-1468862163
120) https://ripple.com/insights/announcing-ripples-global-payments-steering-group/

DAML)라는 이름의 분산원장용 스마트 계약 언어를 개발하고 있다.

디지털 에셋 홀딩스는 이더리움과 달리 DAML을 튜링 불완전 언어로 설계했다. 튜링 불완전 언어는 기능적으로 제한되어 있어 활용도가 떨어질 수 있지만, 튜링 완전 언어로 프로그램을 설계했을 때에 비해 고려해야 할 오류와 변수를 최소화할 수 있는 장점이 있다. 디지털 에셋 홀딩스는 기능을 어느 정도 희생하더라도 자본시장에 더 최적화된 안정적이고 높은 보안성을 가진 분산원장 플랫폼을 제공하는 것을 목표로 한다.

디지털 에셋 홀딩스는 자본시장 블록체인 플랫폼 도입을 목표로 설립된 기업인만큼 주로 자본시장 관련 기업 및 기관과 협업을 통해 분산원장 기술을 적용하는 방안을 개발하고 있다. 올해 3월에는 미국 예탁결제원(Depository Trust & Clearing Corporation)과 블록체인 기반의 Repo 결제 및 청산 시스템 개발에 합의했으며,[121] 호주 증권거래소(Australian Stock Exchange)에서는 디지털 에셋 홀딩스에 추가 투자를 하는 등[122] 자본시장에서 블록체인 도입을 목표로 협력이 진행중이다.

3. 금융기관 및 기업의 블록체인 활용 현황

이더리움, 리플 등 프로토콜이 전반적인 금융 시스템이나 서비스를 다루는 하나의 플랫폼으로 블록체인을 개발한다면, 금융기관 등의 기업들은 각 기관이 내부적으로 가지고 있는 시스템의 비효율적인 요소들을 제거하고 새로운 서비스를 개발하기 위한 시스템으로서 블록체인에 접근하고 있다.

우선 다수의 금융 기관들이 블록체인 시스템을 기반으로 하여 자체적으로 유통하는 디지털 화폐를 개발하는 방안에 대해 연구하고 있다. 금융기관들이 블록체인의 분산형 네트워크를 통해 디지털 화폐를 유통할 수 있게 되면 고객들의 거래 내역을 쉽게 확인하는 등 고객관리와 자산 관리가 용이해지고 기존 화폐 관리비용을 절감할 수 있을 뿐만 아니라, 해외 지점과 연동하여 다른 화폐로 환전이 쉬워지는 등 많은 장점들을 바탕으로 시스템을 효율적으로 운영하고 추가적인 서비스도 개발할 수 있기 때문이다. 이전까지는 디지털 화폐를 유통하고 관리할 수 있는 안전한 시스템이 없었기 때문에 이를

121) https://digitalasset.com/press/dtcc-digital-asset-repo-poc.html
122) https://digitalasset.com/static/documents/30_22Jun_ASX%20Increases%20Investment%20in%20Digital%20Asset%20Holdings.pdf

구현하기가 쉽지 않았지만, 비트코인이라는 가상 화폐를 성공적으로 유통하고 있는 분산형 네트워크인 블록체인 기술이 디지털 화폐 생태계를 만들 수 있는 기술이라 판단됨에 따라 많은 금융기관들이 블록체인 기반 화폐를 발행하는 방안을 연구 및 개발 중이다.

또한 금융기관들은 비트코인으로 증명된 바와 같이 중개기관 없이 실시간으로 송금이 가능하다는 블록체인의 장점을 바탕으로 블록체인 기반의 해외송금 플랫폼 개발도 진행중이다. 현재 SWIFT망 등의 전신료와 중개은행에 지불하는 수수료 등으로 은행들의 송금 서비스 관련 시간적, 비용적 부담이 높은 상황에서 중개기관 없이 바로 송금을 처리할 수 있는 블록체인 플랫폼은 낮은 비용으로 빠른 시간에 송금을 할 수 있는 대안으로서 각 금융사가 큰 관심을 갖고 있다. 이외에도 금융기관들은 결제청산 시스템, 스마트 계약 기능을 활용한 거래 플랫폼 등을 개발하고 있다.

대표적인 사례는 일본의 MUFG코인이다. 일본 최대 금융기관중 하나인 미쓰비시 UFG 금융그룹(이하 MUFG)는 블록체인 활용방안을 활발히 연구중인 아시아의 대표적인 대형 금융기관으로, R3 CEV의 회원이기도 하다. MUFG는 내부적으로 송금, 가상화폐, 결제시스템 등 다양한 블록체인 기술 기반 플랫폼을 실험 중인데 이중 가장 주목받는 연구 분야가 자체 코인 발행이다. MUFG는 블록체인을 활용한 자체 가상화폐인 MUFG 코인을 개발하고 있는데, 은행 계좌 잔액을 MUFG 코인으로 전환하여 모바일 앱 등을 통해 은행 서비스에 간편하게 사용할 수 있고, 향후 ATM을 통해 MUFG를 엔화로 전환하여 출금하는 서비스도 구상중이다. 아직까지 구체적인 실행 여부는 정해지지 않았지만 MUFG 코인의 발행이 확정된다면 2017년 말 출시를 목표로 하고 있다. 또한 MUFG는 블록체인 스타트업과의 협업을 통해 블록체인 기반 약속어음 교환 플랫폼의 기술검증을 진행 중이다.[123] 일본의 또 다른 대형 금융기관인 미즈호 금융그룹 또한 여러 블록체인 기업들과의 협력을 통해 블록체인 활용 방안을 찾고 있다. 올해 2월에는 컨설팅기업과 협력을 맺고 미즈호 금융그룹 전체에 블록체인을 기반으로 한 기록관리 시스템을 연구할 것이라고 발표했고, IBM과 협력을 통해 블록체인 기반 송금 및 결제 시스템에 대한 테스트도 진행 중이라고 밝혔다.[124][125]

---

123) http://www.coindesk.com/chain-mufg-blockchain-promissory-notes/
124) https://www.cryptocoinsnews.com/mizuho-cognizant-develop-blockchain-solutions-record-keeping/
125) https://www.cryptocoinsnews.com/mizuho-ibm-digital-currency-test/

은행 간 자체 컨소시엄을 구성해 결제를 위한 디지털 코인 개발에 착수한 사례도 등장하고 있다. UBS, 도이체방크, 산탄데르, 뉴욕 멜론 은행 (BNY Mellon) 등 4개 대형 은행은 송금 및 결제 시스템에 적용되는 블록체인 기반 가상화폐인 Utility Settlement Coin을 개발 중이며, 이를 2018년 초에 출시할 계획이라고 발표했다.[126] 4개 은행 중 UBS 주도로 이루어지는 이 시스템은 금융기관들이 주식, 채권 등 금융상품을 거래할 때 은행 간 상이한 시스템을 통합하여 블록체인을 기반으로 거래 즉시 결제가 완료되는 자체 디지털 화폐 플랫폼으로서 거래시점과 결제시점 사이의 상대방 리스크 노출 위험을 극복할 수 있다. 현재는 2018년 출시를 앞두고 각국 규제 당국의 승인과 중앙은행의 협조를 얻기 위해 노력중이다.[127]

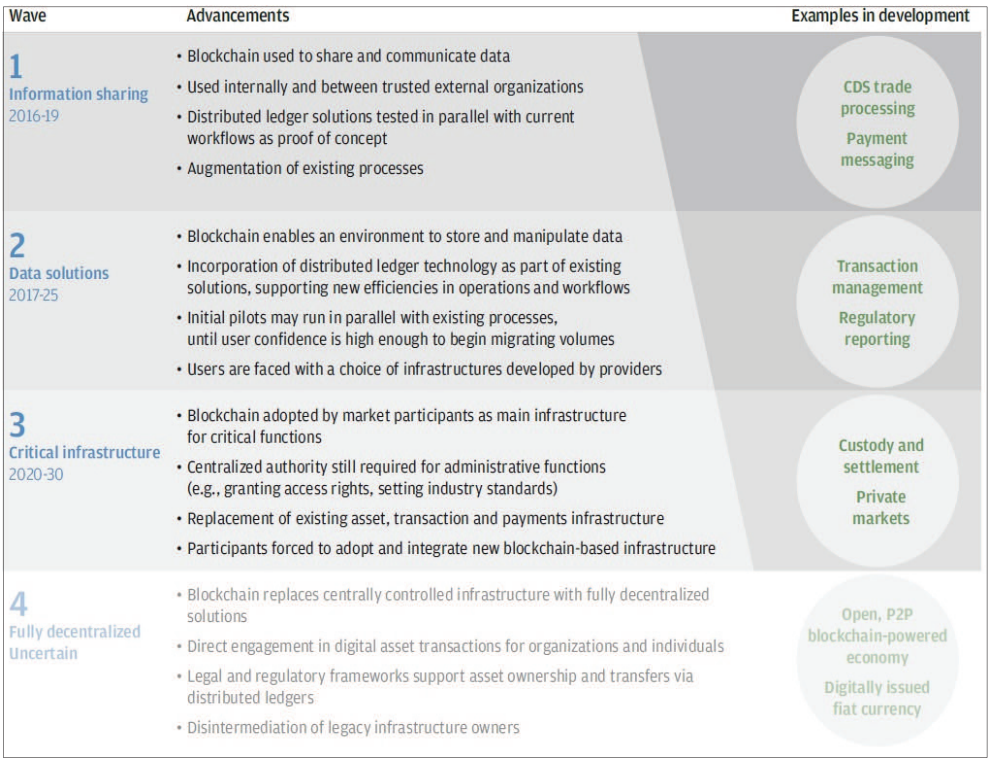
금융 회사인 VISA도 블록체인에 대해 활발히 연구 및 투자를 하고 도입 방안을 모색하고 있다. 올해 10월에는 블록체인 스타트업과 협업을 통해 비자 네트워크를 이용한 블록체인 기반의 실시간 결제 플랫폼을 2017년 출시를 목표로 개발할 것이라고 발표했다.[128] 또한 VISA 유럽지부에서 새로운 시스템과 혁신적인 서비스에 대한 연구를 담당하고 있는 VISA Europe Collab에서는 현재 블록체인을 새로운 송금 플랫폼을 개발할 수 있는 기반기술 중 하나로 보고 이에 대한 연구를 진행중이다. 지난 9월에는 블록체인 관련 스타트업과 협력하여 블록체인 기반 송금 플랫폼에 대한 기술 검증을 약 100일간 진행할 것이라고 발표했다. VISA 측은 블록체인 기반의 새로운 송금시스템은 기존 SWIFT망을 기반으로 하는 송금 시스템보다 최대 80% 가까이 비용을 절감할 수 있을 것으로 추산하며 VISA의 네트워크와 블록체인 기술을 결합하여 기존 송금 시스템의 비용을 절감하고, 송금 및 결제 시스템 기반이 취약한 개발도상국에서 VISA의 네트워크와 시장을 확장할 수 있는 발판이 될 것으로 기대하고 있다.[129]

미국의 대표적인 금융기업인 JP모건도 지난 2월 약 2,200여명의 고객을 대상으로 블록체인 기반 시스템을 통해 런던에서 도쿄로 달러를 송금하는 테스트에 성공했다고 밝혔다. JP모건은 지난 7월 자산관리 산업에서의 블록체인 활용법에 대한 보고서를 발표했는데, 향후 5~10년간은 블록체인 기술을 내부자료 공유 등 간단한 어플리케이션을 통해 주로 활용해 보고, 새로운 기

126) https://bitcoinmagazine.com/articles/major-banks-developing-utility-settlement-coin-an-industry-standard-for-digital-central-bank-cash-1472140867
127) https://www.ft.com/content/1a962c16-6952-11e6-ae5b-a7cc5dd5a28c
128) http://www.coindesk.com/visa-blockchain-payments-service/
129) https://www.cryptocoinsnews.com/visa-test-blockchain-payments-among-banks-swift-rival

술의 리스크를 고려해 기존의 시스템과 연동 혹은 병행하면서 다양한 실험을 진행할 것이라고 밝혔다.[130)]

<그림 1-6> JP모건의 예상 블록체인 도입 4단계



자료: Unlocking Economic Advantage with Blockchain

많은 글로벌 기업과 금융기관들이 블록체인 도입을 검토하고 연구를 진행하는 가운데 국내에서도 블록체인에 대한 관심과 도입 시도가 이루어지고 있다. 삼성전자는 지난해부터 IBM과 함께 사물인터넷 등을 통해 블록체인을 활용할 수 있는 방안을 연구 중이다. 각 금융기관들도 R3 CEV나 하이퍼레저 등 블록체인 컨소시엄에 가입하고 있으며, 일부 금융기관들은 스타트업과 협력하여 인증, 송금, 전자 자산 등의 분야에서 블록체인 기반 플랫폼을 테스트하는 등 도입을 준비하고 있다.

130) Unlocking Economic Advantage with Blockchain, JP Morgan & Oliver Wyman, 2016

<표 1-1> 국내 블록체인 도입 동향 (가나다 순)

기업명	블록체인 도입 현황
삼성전자	• IBM과 함께 블록체인 활용 방안 검토 중 [131]
삼성SDS	• 블록체인 업체 블로코에 투자 [132] • 블록체인 컨소시엄 Hyperledger 가입
신한은행	• 블록체인 컨소시엄 R3CEV 가입 • 블록체인 기반 골드바 구매 교환증 및 보증서 서비스 출시[133]
우리은행	• 코인플러그와 블록체인 관련 업무협약 체결 [134]
전북은행	• 블록체인 기반 간편 로그인 서비스 개발 [135]
하나은행	• 블록체인 컨소시엄 R3CEV 가입
한국예탁결제원	• 블록체인 컨소시엄 Hyperledger 가입
한국조폐공사	• 코인플러그와 블록체인 기반 사업협력 MOU 체결 [136]
BNK금융	• 코인플러그와 블록체인 기반 서비스 업무협약 체결 [137]
IBK기업은행	• 코빗과 블록체인 기반 서비스 업무협약 체결 [138]
KB국민카드	• 코인플러그와 블록체인 기반 개인인증 서비스 구축 [139]
KB국민은행	• 블록체인 컨소시엄 R3CEV 가입 • 코인플러그와 블록체인 기반 해외송금 플랫폼 개발 [140] • 코인플러그와 블록체인 기반 비대면 실명인증 플랫폼 개발[141]
NH농협은행	• 블록체인 업체 코빗과 제휴 [142]

4. 정부 및 공공기관의 블록체인 활용 현황

블록체인은 공공 분야에서도 활용 가능성이 높은 기술이다. 거래내역이 투명하게 공개되고 거래내역이 추적가능하며 중앙집중이 아닌 분산형 네트워크로 구성되는 블록체인은 세금, 토지, 여권, 신분증, 보조금 등 정부가 관리하고 분배하는 모든 자산을 쉽게 등록하고 내역을 추적하는 서비스를 만드

131) http://www.hankyung.com/news/app/newsview.php?aid=2016082351841
132) http://www.yonhapnews.co.kr/bulletin/2016/07/14/0200000000AKR20160714026300017.HTML?input=1195m
133) http://www.yonhapnews.co.kr/bulletin/2016/08/17/0200000000AKR20160817102400002.HTML?input=1195m
134) http://www.fntimes.com/paper/view.aspx?num=162024
135) http://www.ddaily.co.kr/news/article.html?no=142206
136) http://www.ebn.co.kr/news/view/849764
137) http://www.yonhapnews.co.kr/bulletin/2016/01/15/0200000000AKR20160115145100051.HTML?input=1195m
138) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20160310163334&type=det&re=
139) http://www.ddaily.co.kr/news/article.html?no=140988
140) http://www.etnews.com/20151201000427
141) http://www.g-enews.com/ko-kr/news/article/news_all/20160429131201210615 1_1/article.html
142) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20150826155406&type=det&re=

는 데 활용될 수 있다. 또한 블록체인 기술은 같은 내용의 원장을 여러 네트워크 참가자가 나눠서 가지고 있기 때문에, 기존 중앙집중 방식으로 운영되는 경우 외부의 공격에 취약하고 이에 따라 보안 시스템에 많은 비용을 지불해야 했던 문제점을 극복할 수 있을 것이라고 보고 있다.

정부 혹은 공공기관의 서비스는 시민들의 정보를 안전하게 보관하고 편리하게 제공하는 것을 목표로 한다. 일반 기업도 고객에 대한 정보 관리를 중요시하지만 공공기관은 상대적으로 보유하는 정보의 양이 많고 대상이 거주하는 시민 전체에 해당하기 때문에 이같은 개인정보들을 철저히 보관해야할 책임이 있다. 이에 더하여 정부 및 공공기관의 정보 관리는 시민들에게 편리한 공공 서비스를 제공하는 것을 목표로 지향해야 한다. 블록체인 개발도 이러한 방향성을 갖고 진행되고 있으며, 특히 가상화폐, 소유권 등록 등의 분야에서 활발하게 연구되고 있다.

우선 주요국 중앙은행들은 블록체인을 기반으로 디지털 화폐를 발행하여 유통하는 방안에 대해 다양하게 연구하고 있다. 위에서 언급한 사례와 같이 일반 금융기관도 블록체인 기반의 가상화폐 개발을 진행하고 있지만, 민간 금융기관은 화폐의 역할을 대신하는 블록체인 기반 코인을 만드는 데 관심이 있는데 비해, 중앙은행은 법정화폐를 발행하고 유통하는 주체로서 디지털 화폐를 블록체인을 통해 직접 발행하고 유통하는 방안을 연구하고 있다는 점에서 차이가 있다. 현재 중앙은행이 실물 화폐를 발행하고 유통하는 데는 많은 비용이 든다. 특히 동전의 경우 액면 가치가 실제 금속으로서의 소재 가치와 큰 차이가 없고 분실이 잦기 때문에 유통과 관리에 드는 비용에 비해 효율성이 떨어진다는 평가를 받고 있다. 또한 현재 화폐 시스템은 탈세를 추적하기가 용이하지 않다는 문제점이 있다. 블록체인 기반 디지털화폐 시스템은 거래내역을 실시간으로 확인할 수 있고 빠른 결제 및 청산이 가능하며 분실에 대한 우려가 없다는 장점을 갖는다. 세계경제포럼에 따르면 800명의 조세 전문가 중 약 73%가 2025년 이전에 블록체인을 기반으로 조세를 걷는 사례가 나타날 것이라고 예상했다.[143] 중앙은행은 블록체인이 향후 디지털 화폐를 유통하고 관리할 수 있는 플랫폼이라 보고 개발을 진행하고 있다. 관련 분야에서 가장 활발한 연구를 진행하고 있는 곳은 영란은행이다. 지난 3월 영란은행은 University College London의 교수진과 함께 영란은행에서 발행하는 디지털 화폐인 RSCoin을 보고서를 통해 발표했고, 이후 7월에는

143) http://www.coindesk.com/world-economic-forum-governments-blockchain/

디지털 화폐 발행이 거시경제학적으로 미칠 영향에 대한 보고서를 발표했다. 영란은행은 디지털화폐가 가져다 줄 긍정적 영향력이 크고 장기적으로는 필요성도 있지만 단시일 내에 디지털화폐를 발행하기로 결정한 것은 아니며 우선 디지털화폐의 잠재적인 편익과 부작용 등을 고려하여 향후 구체적인 방안을 정해야 한다는 입장이다.

네덜란드 중앙은행도 지난 2월 중앙은행이 통제하는 블록체인 기반 디지털 화폐인 DNB 코인에 대한 아이디어를 발표했고, 이후 오픈소스인 비트코인 소프트웨어를 기반으로 실험을 진행하였다고 밝혔다. 동 실험에서는 비트코인과 같은 가상화폐를 발행할 때와 가상화폐가 더 이상 발행되지 않는 두 가지 상황을 가정하여 시스템 안정성과 보안을 중심으로 시스템에 대한 테스트를 진행하였다. 네덜란드 중앙은행은 아직까지 디지털화폐에는 많은 한계가 있고 다수 금융기관의 공감대가 형성되는 데도 시간이 걸리겠지만, 블록체인이 지속적으로 발생하고 있는 금융사고 등을 예방할 수 있는 플랫폼으로서 하나의 대안이 될 수 있다고 판단하고 있으며 중앙은행 발행 디지털 화폐에 대한 연구를 계속 진행할 것임을 밝혔다.[144] 캐나다 중앙은행도 블록체인을 기반으로 중앙은행이 직접 발행하는 가상화폐인 CAD Coin에 대한 아이디어를 연구 중이라고 발표했다. 역시 실제 도입을 전제로 한 연구라기보다는 기술에 대한 이해와 활용 가능성을 점검하기 위한 개념적인 테스트 단계이지만, 블록체인 기술을 통해 은행 간 지급 및 결제에서 디지털화폐를 활용할 수 있을 것이라고 보고 이를 위한 연구를 진행 중이다.[145] 정부 발행 디지털 화폐에 대한 보다 자세한 내용은 4장에서 기술한다.

또한 블록체인 기술은 모든 거래내역이 공개되고 추적될 수 있는 투명성을 바탕으로 공공기금의 운영과 소유권 증명 및 이전 분야에서도 활용 방안을 연구 중이다. 정부가 관리하는 기록 및 자료가 이미 대체로 디지털 정보로 보관되고 있어 각국 정부는 정보를 효율적이고 안전하게 관리할 수 있는 시스템을 찾고 있다. 중앙의 통제기관 없이 자유롭게 거래가 가능한 비트코인과 그 근간이 되는 블록체인 기술은 정부에서 적절한 활용 방안만 찾는다면 소수의 서버에 집중된 데이터 처리의 비효율성과 보안에 대한 불안함을 극복할 수 있는 좋은 대안으로 평가받고 있다.

---

144) http://www.coindesk.com/dutch-central-bank-preparing-boldest-blockchain-experiment-yet/
145) http://www.coindesk.com/bank-of-canada-pursues-hands-on-distributed-ledger-research/

영국 정부의 경우, 공공분야에서 블록체인을 활용할 수 있는 방안에 대해 많은 관심을 가지고 적극적인 연구를 진행중이다. 지난 1월 영국 과학부에서 발표한 보고서에서는 블록체인이 보안, 프라이버시, 신뢰 등의 문제를 극복한다면 공공 분야에서 다양하게 활용 가능할 것이라고 밝히며, 다양한 측면에서 블록체인 개발 연구를 진행할 것이라고 발표했다.[146] 또한 지난 7월 영국 노동연금부(Department for Work and Pensions)에서는 바클레이스 은행 및 다수의 핀테크 스타트업과 연계해 블록체인 네트워크를 통한 연금 수령 및 사용 내역 기록에 관한 연구를 진행한다고 발표했다.[147]

에스토니아 정부는 블록체인을 전면적으로 도입하고자 하는 정부 중 하나이다. 에스토니아 정부는 에스토니아 주민의 기록을 디지털화하여 관리하는 e-residency 시스템을 준비 중인데 이의 기반이 되는 플랫폼으로서 블록체인 도입을 준비하고 있음을 밝혔다.[148] 에스토니아 정부는 나스닥과 함께 동 인프라를 바탕으로 전자투표 플랫폼을 개발하는 등 e-residency 플랫폼을 통해 주민들이 빠르고 편리하게 공공 서비스를 이용할 수 있는 통합 플랫폼 구축에 적극적인 자세를 보이고 있다.

싱가포르 정부의 경우 기업과의 협업을 통한 블록체인 활용방안을 연구 중이다. 지난 7월 싱가포르 정부와 IBM이 협력 관계를 맺고, 블록체인 혁신 센터를 조성하고 IBM 연구진과 싱가포르의 개발자들이 협업하여 국가 내 여러 지역과 산업 분야에서 활용할 수 있는 블록체인 기술을 개발할 것이라고 발표했다. 싱가포르의 경제개발청(Economic Development Board)과 통화청(Monetary Authority of Singapore)은 IBM의 블록체인 기술을 바탕으로 다자간 거래 플랫폼을, 항만청(Port Authority of Singapore)은 공급사슬 개선 방안을 도출해 3년 이내에 금융과 무역 산업에서 활용할 수 있는 블록체인 기반 파일럿 프로그램들을 발표할 예정이라고 밝혔다.[149]

분산 네트워크를 가진 블록체인은 공공 문서를 등록하고 보관하는 플랫폼으로서도 공공기관의 적극적인 연구 대상이 되고 있다. 많은 정부에서 문서 보관 비용을 절감하고 증명서를 간편하게 발급할 수 있으며 다른 서비스로의 확장 또한 용이한 블록체인 기반 문서 서비스를 도입하고자 하는 움직임

146) Distributed Ledger Technology: beyond block chain, UK Government office of Science, 2016
147) https://www.cryptocoinsnews.com/uk-trials-blockchain-based-social-welfare-payments/
148) http://www.bbc.com/news/technology-36276673
149) http://www.coinspeaker.com/2016/07/12/ibm-opens-blockchain-innovation-centre-in-singapore/

이 시작되고 있다. 러시아 정부의 경우 비트코인 자체에 대해서는 회의적인 태도를 취하고 있지만, 블록체인에 대해서는 개방적인 태도를 보이며 이를 적극적으로 도입하기 위한 노력이 진행중이다. 러시아 연방 반독점청(Federal Anti-monopoly Service, 이하 FAS)은 하이퍼레저에 가입한 러시아 최대 금융기관 Sberbank와 함께 블록체인 기반 문서관리 시스템을 테스트하고 있다고 발표했다.[150]

스웨덴에서는 블록체인을 활용하여 토지의 소유권과 이전 내역을 기록하는 스마트 계약 플랫폼을 만드는 방안을 연구 중에 있다. 스웨덴 국립 토지연구소(Swedish National Land Survey)는 블록체인 스타트업, 컨설팅 기업, 통신회사와 협약을 맺고 블록체인 시스템을 활용하여 기존에 수작업으로 이루어지던 토지 조사를 보다 효율적이고 안전하게 바꾸기 위한 방안을 연구 중이며, 블록체인을 활용한 스마트 계약 플랫폼을 통해 활용한 토지 등록 시스템을 개발할 계획이라고 밝혔다.[151]

중동 또한 블록체인 도입에 매우 적극적으로 움직이는 지역이다. 아랍에미리트는 현재까지 과도하게 이어지고 있는 석유 자원에 대한 경제적 의존 구조를 탈피하기 위해 신사업에 대한 투자를 확대하는 전략의 일환으로 블록체인을 새로운 산업을 육성할 수 있는 기술로 평가하고 이에 대한 개발을 적극적으로 진행하고 있다. 금년 10월 두바이 정부는 2020년까지 전면적 도입 목표 하에 정부의 모든 문서 시스템에 블록체인을 도입하는 프로젝트를 진행한다고 발표했다. 두바이 도시 정부는 이 프로젝트를 통해 정부의 업무 효율성을 높이고 블록체인 기반 신사업을 육성한다는 입장이다.[152]

5. IT기업들의 블록체인 활용 현황

블록체인 기반 서비스를 제공하는 가장 대표적인 IT기업은 마이크로소프트와 IBM이다. 해당 IT 기업들은 다른 기업들이 활용할 수 있는 오픈소스 블록체인 플랫폼을 개발하여 다른 기업들이 블록체인 기반 서비스를 테스트하고 활용할 수 있는 서비스를 제공하고 있으며, 이를 통해 소프트웨어 기업으로서 시장의 주도권을 찾고 고객을 확보하고자 하고 있다.

150) http://www.coindesk.com/the-russian-government-is-testing-blockchain-for-document-storage/
151) http://www.coindesk.com/sweden-blockchain-smart-contracts-land-registry/
152) http://www.coindesk.com/dubai-government-documents-blockchain-strategy-2020/

가. IBM

IBM은 리눅스 재단(Linux Foundation)의 하이퍼레저 프로젝트를 주도하는 IT기업으로서 블록체인을 차세대 산업기술로 판단하고 다른 산업군과 기업들이 활용할 수 있는 블록체인 플랫폼을 소프트웨어 서비스로 제공하는 것을 목표로 개발을 추진중이다. 지난 7월 IBM은 높은 보안성을 갖는 리눅스원(LinuxONE)을 기반으로 고객들이 자유롭게 블록체인 시스템 안에서 프로그램을 테스트하고 운영할 수 있는 플랫폼을 개발했다고 발표했다. 기존의 블록체인 플랫폼을 통해 고가의 제품 데이터를 다루어 온 에버레저(Everledger) 등 블록체인 스타트업들이 새로운 플랫폼을 테스트해 보겠다는 의사를 밝혔으며, IBM은 보다 안전하고 신뢰성이 높은 새로운 블록체인 플랫폼을 보다 많은 기업들이 실험장으로 활용할 것을 기대하고 있다.[153] IBM은 최근 구글, 아마존 등의 기업의 부상으로 인해 상대적으로 좁아진 소프트웨어 기업으로서의 입지를 되찾고 새로운 먹거리를 확보하기 위한 방안으로 블록체인 플랫폼의 개발을 통해 다른 기업들과의 연계를 강화하고 고객을 확보하겠다는 구상을 가지고 있으며, 세계 각지의 컨퍼런스에서 적극적으로 IBM의 아이디어를 발표하는 등 대외적으로도 활발하게 블록체인에 대한 전략을 홍보하고 있다.

나. 마이크로소프트

마이크로소프트 또한 블록체인 기반 오픈소스 플랫폼을 개발하여 다른 기업들이 사용할 수 있는 서비스를 제공하고 있으며 다른 블록체인 기업들과의 협업을 통해 블록체인으로 응용할 수 있는 여러 플랫폼들을 구상 및 발표하고 있다.

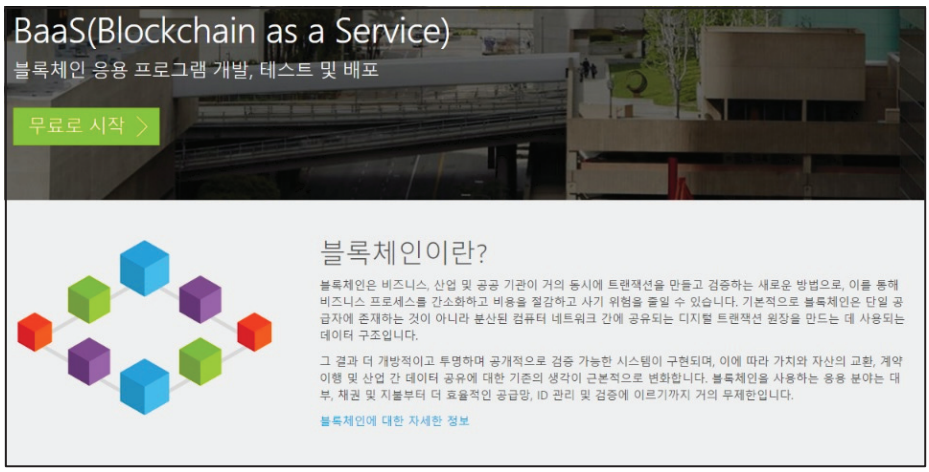
또한 블록체인 스타트업과 협업을 통해 블록체인 기반 신분인증 시스템을 구축하겠다고 밝혔다. UN은 2030년까지 세계 모든 사람들이 법적 신분을 가지는 것을 목표로 한다고 밝혔고, 마이크로소프트는 위변조가 불가능하고 내역이 명확하게 공개되며 높은 확장성을 가진 블록체인 네트워크를 통해 개인 신분인증 플랫폼을 구축할 계획이라고 밝혔다.[154]

또한 마이크로소프트는 이더리움 블록체인 벤처기업 Consensys와 함께 동사의 클라우드 서비스 플랫폼인 애져(Azure) 위에 이더리움을 기반으로 한

153) https://www-03.ibm.com/press/us/en/pressrelease/50169.wss
154) https://bitcoinmagazine.com/articles/microsoft-building-open-blockchain-based-identity-system-with-blockstack-consensys-1464968713

BaaS(Blockchain as a Service)를 구축했다.[155] 마이크로소프트는 이더리움 기반 서비스를 제공함으로써 블록체인을 활용하고 싶었지만 접근성이 떨어져 활용이 어려웠던 고객들에게 블록체인 기반 어플리케이션, 프로그램 등을 테스트 할 수 있는 플랫폼을 제공하고 이를 통해 고객들을 확보하겠다는 계획이다.

<그림 1-7> 마이크로소프트의 블록체인 서비스 BaaS



6. 기타 블록체인 활용 현황

가. 정품 인증 및 소유권 이전

최근 기업 및 산업계에서는 분산화된 네트워크를 통해 위변조가 불가능하고 거래내역이 공개되는 투명성을 가진 블록체인 기술을 활용하여 안정적인 정품인증 서비스와 상품의 소유권 이전 시스템을 도입하고자 하는 데 관심을 보이고 있다. 특히 모조품 피해 발생 사례가 많고 소비자들이 이전 소유자나 제작자, 원산지 등을 알기를 바라는 고가의 제품군에서 블록체인 적용 방안을 적극적으로 모색하고 있다.

영국 기반 블록체인 스타트업인 에버렛져(Everledger)는 다이아몬드의 정보를 등록하고 소유권 내역을 확인하는 서비스를 제공하고 있다. 에버렛져는 약 98만개의 다이아몬드 정보를 블록체인에 등록하고 레이저코드를 입력해

155) https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/

해당 다이아몬드의 거래내역과 진품 여부를 확인할 수 있는 서비스를 제공 중이다. 올해 초부터는 인증 대상 범위를 미술 작품으로 확대하여 전시 작품 및 전시회 데이터베이스를 블록체인에 구축하여 위변조 여부를 확인할 수 있는 시스템을 개발 중이다.[156] 금년 7월에는 러시아의 시계 브랜드인 Raketa가 블록체인 기업과의 협업을 통해 블록체인 네트워크에 상품 정보를 등록하고 정품 인증을 제공하는 서비스를 개발 중이라고 발표했다.[157]

나. 자본시장 거래 플랫폼

비트코인 블록체인은 분산된 네트워크를 통해 거래되는 비트코인이라는 가상화폐를 실시간으로 추적할 수 있다는 장점을 가지고 있다. 이러한 기술적 장점을 바탕으로 블록체인은 단순히 돈 뿐만 아니라 주식, 채권 등 가치를 지닌 증권을 거래할 수 있는 플랫폼으로서 주목받고 있으며, 특히 자본시장에서 증권을 거래할 수 있는 플랫폼으로 개발되고 있다. 우선 블록체인을 활용하여 장외 주식 거래를 효율적으로 처리할 수 있는 시스템을 개발하는 데 많은 관심이 집중되고 있다. 장외 주식 거래는 일반적으로 거래를 담당하는 거래소 등의 중개를 거치지 않고 개인 간의 합의로 이루어지는 비상장주식의 거래를 의미한다. 일반적인 주식 거래와는 달리 공식적인 플랫폼이 없고, 플랫폼이 있더라도 직접 거래를 중개하기보다는 거래 정보를 게시할 수 있는 게시판 정도의 수준이기 때문에, 거래 대상을 찾고 이를 완결시키기까지의 과정이 매우 복잡하다. 또한 공식적인 플랫폼이 존재하지 않기 때문에 여전히 전화, 이메일 등으로 거래 주문 및 확인이 이루어지는 등 효율성이 떨어지고 거래처리 시간도 오래 소요되며 거래과정에서 사기 위험에도 종종 노출되는 문제점이 있다. 국내에는 한국금융투자협회가 개설한 K-OTC라는 장외주식 거래 시장이 있지만, 비상장회사 중 공개회사만 등록이 가능해 다른 회사들은 개인적인 연락을 통해 계약을 맺거나 사설업체에 의존하고 있는 상황이다. 이와 같이 장외주식 거래 플랫폼의 부재와 복잡한 절차로 인해 많은 사건·사고들이 일어나는 등 불편함이 지속되고 있어 장외 주식 거래 활성화에 큰 어려움이 있다.

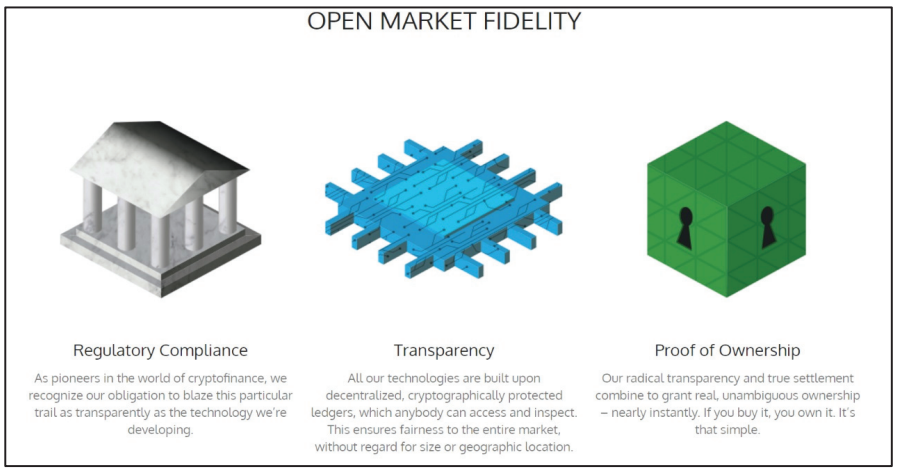
몇몇 자본시장 관련 기관들은 비활성화된 장외 주식 거래에 블록체인 기술이 대안이 될 것이라고 판단하고 블록체인 기반 장외 주식 플랫폼의 개발

156) http://www.coindesk.com/everledger-announces-partnership-vastari-combat-art-fraud/
157) https://bitcoinmagazine.com/articles/raketa-watches-trials-blockchain-technology-to-fight-counterfeiting-1467905237

및 상용화를 준비하고 있다. 거래내역이 투명하게 공개되는 블록체인은 장외 주식 거래에 신뢰를 확보할 수 있는 기반이 될 수 있고, 이미 중개인 없이 직접 거래되는 장외 주식 거래 시스템은 중개자 없이 운영되는 블록체인 플랫폼에 특히 잘 적용될 수 있을 것으로 보이기 때문이다. 현재까지 개발된 블록체인 기반 장외 주식 거래 플랫폼 중 가장 널리 알려진 것은 NASDAQ에서 10월 공개한 linq라는 플랫폼이다. 지금까지 외부에서 거래되던 장외 주식을 NASDAQ의 linq 플랫폼을 통해 거래하는 경우 거래의 투명성이 높아지고 신속한 서비스를 제공할 수 있을 것으로 기대된다.[158] 한편 NASDAQ은 linq에 적용된 블록체인 기술을 바탕으로 에스토니아 소재 거래소에 등록된 주주들을 대상으로 블록체인 기반 전자투표 시스템도 개발하여 상용화할 계획이다.[159]

한편 온라인 상거래 업체 Overstock은 블록체인 기반 주식 및 채권 거래 플랫폼인 t0를 개발했다. 여기서 t0는 기존의 거래가 청산 및 결제되는 데 통상 T+3일이 걸렸던 것과 달리 거래 즉시 청산과 결제가 이루어진다는 것을 의미한다. 동 t0플랫폼에서는 주주들이 자유롭고 신속하게 주식 거래를 할 수 있으며 이미 Overstock의 주식이 등록되었다고 발표하였다.[160]

<그림 1-8> Overstock의 주식 거래 플랫폼 t0



자료: t0.com

158) http://www.forbes.com/sites/laurashin/2015/10/27/nasdaq-unveils-blockchain-enabled-platform-linq-announces-6-inaugural-clients/#13707bbb30a3
159) http://www.coindesk.com/nasdaq-shareholder-voting-estonia-blockchain/
160) https://bitcoinmagazine.com/articles/sec-approves-overstock-com-s-filing-to-issue-shares-using-bitcoin-blockchain-1449539558

다. 전자 투표

블록체인은 분산된 네트워크를 통한 보안성을 확보할 수 있다는 장점과 거래 내역이 투명하게 공개되며 즉시 처리가 가능하다는 장점을 가지고 있어 이를 전자 투표 플랫폼으로 활용하기 위한 방안도 활발하게 연구되고 있다. 올해 8월 발표된 세계경제포럼의 블록체인 보고서에서는 일반적인 투표와 주주총회 등에서 이루어지는 위임 투표(proxy voting)를 블록체인의 대표적인 활용 분야 가운데 하나로 소개했다.[161] 특히 위임 투표의 경우 제3자의 개입이 많고 절차가 복잡해 투표율도 저조하고 오류가 생기는 경우도 많은데, 블록체인의 분산화된 네트워크를 통해 이를 극복할 수 있을 것으로 예상된다.

나스닥의 경우 에스토니아 주식시장을 담당하는 Nasdaq OMX Tallinn Stock Exchange 대상으로 블록체인 기반 전자 투표를 연구 중이라고 발표했다.[162] 나스닥은 현재 에스토니아의 주주 투표율이 낮은 상황이고 이미 에스토니아에 블록체인 기반 개인정보 플랫폼이 구축되어 있어 주식 투표 플랫폼 도입시 편익이 클 것으로 기대하고 있다.[163]

러시아의 경우 예탁결제원(National Settlement Depository)에서 블록체인 기반 전자 위임 투표(e-proxy voting) 플랫폼을 개발해 테스트에 성공했다고 발표했으며,[164] 러시아 정부도 블록체인 기술을 현재 개발 중인 전자정부 프로그램에 도입하여 지방정부의 의사결정에 시민들의 의견을 반영할 수 있는 투표 플랫폼을 개발 중이라고 밝혔다.[165] 하지만 블록체인 기반 투표 플랫폼의 경우 아직까지 확장성 문제와 투표에서 필요한 익명성의 문제를 어떻게 기술적으로 구현할 수 있을 것인가가 관건으로 남아있다.

라. 헬스케어 기록 관리 플랫폼

블록체인 활용 분야로서 최근 큰 주목을 받기 시작한 분야가 헬스케어 시장이다. 헬스케어 분야에서 개선사항이 필요하다고 평가받는 것은 환자의 건강기록 데이터를 각 병원, 업체마다 따로 보관하고 있다는 점이다. 환자의

161) The future of financial infrastructure, WEF, 102pg, 2016
162) http://ir.nasdaq.com/releasedetail.cfm?releaseid=954654
163) http://www.coindesk.com/nasdaq-shareholder-voting-estonia-blockchain/
164) https://www.cryptocoinsnews.com/russias-nds-uses-blockchain-for-e-proxy-voting/
165) http://www.coindesk.com/moscow-russia-government-blockchain-voting/

기록이 병원이나 업체들 간에 공유되지 않기 때문에 환자의 건강 상태를 모든 병원이 확인하는 데 많은 비용이 소요될 뿐만 아니라 환자 입장에서도 연속성 있는 치료를 받을 수 없다는 문제가 있다. 그렇다고 하나의 일원화된 통합 관리 시스템을 만들어서 모든 진료 기록을 등록 및 보관하기에는 관리하는 주체를 선정하기 어렵고 데이터가 안전하게 보관될 것이라는 보장을 하기 어려운 문제가 있었다. 헬스케어 시장에서는 데이터가 분산된 네트워크를 통해 등록 및 관리되고 지속적으로 동기화되는 블록체인을 활용하는 경우 환자의 기록을 관리 및 추적하기가 용이해짐으로써 효과적인 치료법을 제시하는 데 기여할 수 있을 것으로 기대하고 있다.

우선 지난 5월 미국 보건복지부(US Department of Health and Human Services)는 헬스케어 데이터의 상호 운용을 중심으로 블록체인을 헬스케어 분야에서 활용할 수 있는 방안에 대한 논문 경연대회를 개최했다.[166] 경연대회를 통해 70여개 이상의 아이디어가 제안되었고, 이 경연대회에 제출된 제안들을 바탕으로 하이퍼레저의 참가자인 IBM, 엑센추어 및 일부 스타트업이 헬스케어 분야에서 블록체인을 활용하기 위한 방안을 연구하는 조직을 만들어서 연구를 진행중이다.[167]

국가적으로 블록체인 기반 건강기록 시스템을 도입하고자 하는 사례도 있다. 블록체인을 기반으로 하는 디지털 신원 시스템을 보유 중인 에스토니아 정부의 경우 블록체인 기반 시스템을 국가의 헬스케어 시스템에도 도입하기 위해 준비 중이다. 현재 에스토니아 전자정부 시스템에 포함되어 있는 개인 건강기록부를 블록체인을 활용하여 실시간으로 업데이트해서 확인할 수 있으며, 이를 통해 건강 정보를 외부의 공격과 기록 위변조로부터 안전하게 지킬 수 있을 것으로 기대하고 있다.[168]

166) http://www.coindesk.com/health-human-service-department-seeks-blockchain-papers/
167) http://www.coindesk.com/hyperledger-launches-blockchain-working-group-for-healthcare/
168) http://www.coindesk.com/blockchain-startup-aims-to-secure-1-million-estonian-health-records/

Ⅱ. 개방형 / 폐쇄형 블록체인

본 장에서는 블록체인의 두 가지 유형인 개방형 블록체인과 폐쇄형 블록체인의 특징을 설명하고 각 블록체인이 가진 장점과 과제 그리고 활용 방안에 대해 서술한다.

1. 개방형 블록체인

가. 개방형 블록체인의 특징 및 장점

블록체인은 운영 방식에 따라 개방형 블록체인(Public Blockchain)과 폐쇄형 블록체인(Private Blockchain)으로 나눌 수 있다. 개방형 블록체인과 폐쇄형 블록체인은 분산된 네트워크를 통해 정보를 관리한다는 기본적인 개념은 동일하지만, 참여 기관의 제한 여부, 운영 체제의 차이를 갖는다. 아래는 개방형 블록체인과 폐쇄형 블록체인의 특징을 구분해 놓은 표이다.

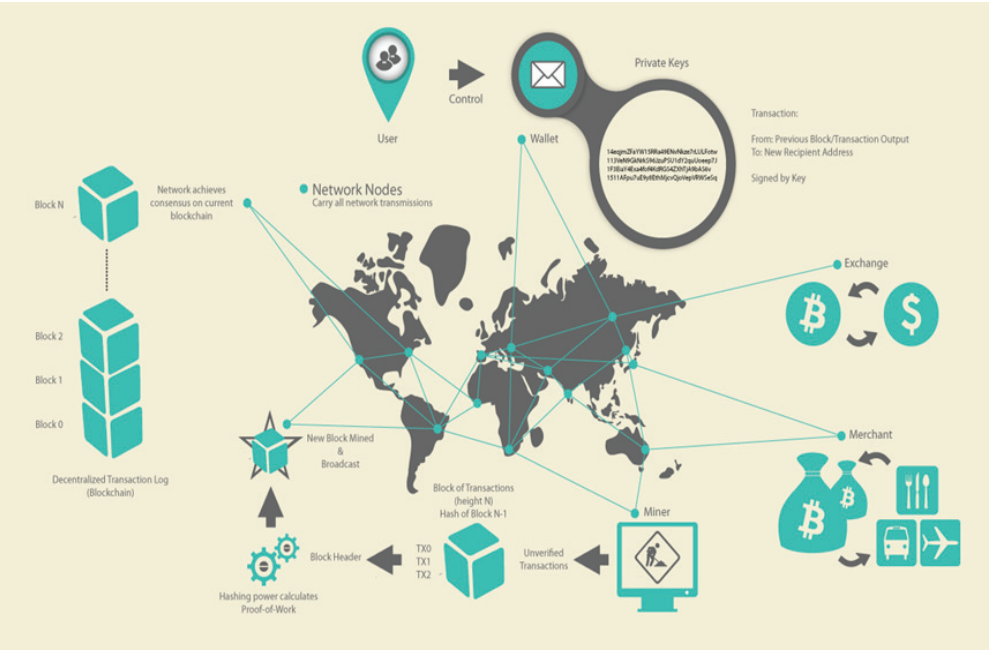
<표 2-1> 개방형, 폐쇄형 블록체인 비교

	개방형 블록체인	폐쇄형 블록체인
거래 기록의 열람	누구나 익명으로 잔고와 거래내역 열람 가능	통제기관과 거래당사자만 거래 기록 열람 가능
거래 참여	큰 인증 과정 없이 누구나 쉽게 계좌를 개설하고 거래에 참여	승인된 기관만이 거래에 참여 가능
거래의 검증/승인	누구나 에너지를 투입하여 검증/승인 과정 참여 가능	승인된 기관과 통제기관만이 거래의 검증/승인 과정 참여
거래의 보관	누구나 거래 내역을 보관할 수 있음	승인된 기관(e.g. 거래당사자)나 통제기관이 거래를 보관
합의의 도출	작업 증명 (Proof-of-Work), 지분 증명 (Proof-of-Stake) 등의 알고리즘으로 합의 도출	BFT(Byzantine Fault Tolerance) 계열 알고리즘을 통해 합의 도출
자체 암호화폐 필요 여부	필요함	꼭 필요하지는 않음
결제의 완결성 보장	네트워크 분기 (Fork) 등의 문제로 결제가 왜곡될 가능성이 존재	시스템적으로 결제의 완결성 보장
충분한 확장 가능성	제한적 확장	활용 방안에 따라 적합한 확장 가능
예시	비트코인, 이더리움	R3 CEV, DAH, Fidoledger

자료: 피넥터

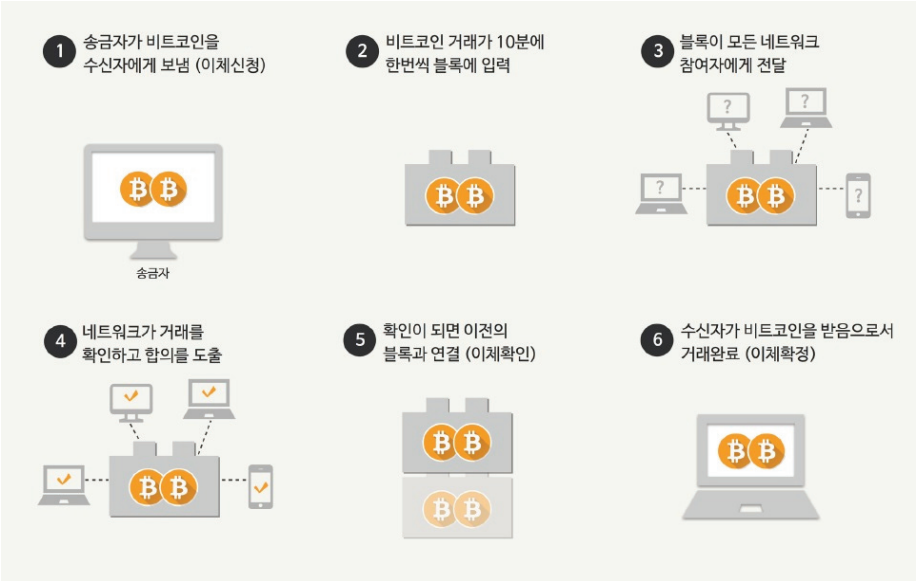
개방형 블록체인(Public Blockchain)은 참여 인원 혹은 기관의 제한이 없이 누구나 참여할 수 있는 블록체인 시스템을 의미한다. 개방형 블록체인은 대부분의 사람들이 생각하는 일반적인 블록체인의 개념으로, 누구나 제약 없이 블록체인에 참여할 수 있으며 특정한 기능을 구현하는 하나의 고정된 형태로 존재하는 플랫폼이다. 잘 알려져 있는 비트코인의 시스템이 개방형 블록체인의 대표적인 예시라고 할 수 있다. 이후 개방형 블록체인에 대한 내용은 비트코인 블록체인을 중심으로 서술한다.

<그림 2-1> 개방형 블록체인



비트코인 블록체인은 비트코인이라는 가상화폐를 거래하는 개방형 블록체인 플랫폼으로써 비트코인을 구매하고 소유한 사람은 물론 비트코인이 없지만 비트코인 주소를 가지고 있는 사람도 비트코인 프로토콜에 참여할 수 있고, 누구나 블록체인의 거래 내역들을 조회할 수 있다. 비트코인 블록체인의 운영 시스템은 다음과 같다.

<그림 2-2> 비트코인의 거래 절차



자료: 피넥터

한 사람이 다른 사람에게 비트코인을 전송하겠다는 거래 내역을 전송하면, 그 거래 내역은 거래 당사자의 주변 네트워크 참여자(이하 노드)에게 전파된다. 거래 내역을 받은 노드들은 거래가 문제없이 유효하다고 판단하면 다른 주변 노드들에게 전파를 하고 이 과정을 거쳐 모든 노드들은 거래 내역을 보유하게 된다. 이 거래의 전파는 몇 십초 정도의 매우 짧은 시간 안에 진행되며 결국 모두가 거래 장부를 확인하고 보유하게 하는 프로세스이다. 즉, 두 사람 간의 거래가 진행되는 동시에 비트코인 블록체인에 참여하는 다른 노드들에게 거래 내역이 전파된다.

한편, 노드들에게 전파된 거래는 검증과 승인을 위해 추가적인 절차가 필요하다. 그리고 전파된 거래가 검증되고 승인이 되기 위해서는 비트코인 블록체인 내의 핵심적인 시스템 유지 방식인 작업 증명(Proof-of-Work)과 채굴(mining)이 이뤄진다. 비트코인 블록체인에서는 일정한 연산을 계속해야 풀 수 있는 문제가 10분마다 만들어진다. 채굴자(miner)들은 이 문제를 풀기 위해 본인들의 컴퓨팅 파워를 투입한다. 암호화 해시 알고리즘을 기반으로 하는 이 연산에 대한 풀이를 작업 증명이라 부르고, 이 소모적으로 보이는 컴퓨팅 파워의 투입은 비트코인을 발행하고 내·외부의 공격으로부터 블록체인을 보호하는 보안의 기반이 된다. 작업 증명을 위해서는 각 문제에 설정된

솔루션이 나올 때까지 각 채굴자들은 SHA-256^2이라는 암호화 알고리즘을 통해 전체 비트코인 네트워크에 걸쳐 반복적으로 초당 수천 건의 암호화 작업을 진행해야 한다. SHA-256^2는 데이터를 암호화하는 기법 중 하나로 주어진 데이터를 특정 암호 알고리즘을 통해 데이터의 크기에 상관없이 32바이트, 즉 64자리의 결과값으로 치환하는 암호기법이다. 해당 암호기법은 언제나 같은 데이터를 동일한 해시값으로 전환하고, 데이터의 작은 변화에도 완전히 다른 해시값이 만들어지기 때문에 해당 거래의 암호값을 통해 위·변조의 여부와 진위여부를 파악할 수 있는 틀이 되며, 특정 자료의 진본 여부를 인증하는 서비스로 확장될 수 있다.

<그림 2-3> SHA-256 암호기법

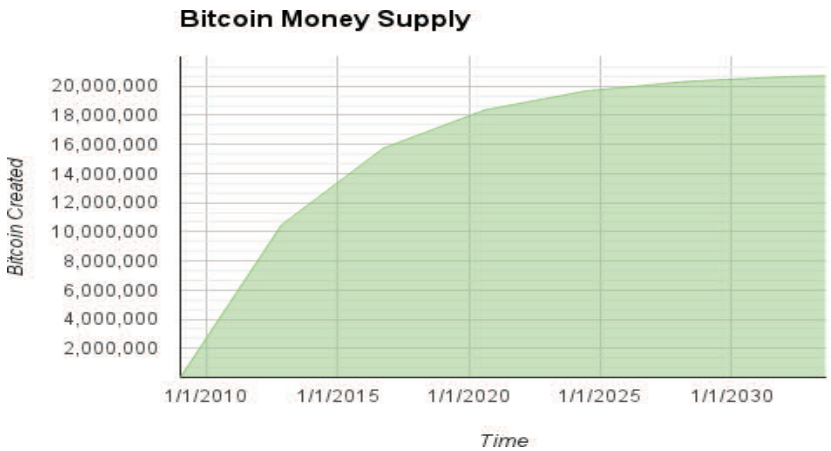
자료: 피넥터

채굴자의 컴퓨터를 일명 풀 노드(Full Node)라고 부른다. 풀 노드는 비트코인 블록체인 안에서 비트코인의 거래 정보를 저장하고 거래를 승인하는 등 비트코인 블록체인의 모든 과정에 참여하는 노드들을 의미하며 채굴 또한 이 과정에 포함된다. 현재는 전 세계적으로 약 7,000개의 풀 노드가 있으며 이들 각각이 저장하는 블록체인의 크기는 약 80GB이다. 노드에 대한 설명은 4장에서 더 상세히 서술한다.

문제의 난이도는 채굴자들이 함께 문제를 풀었을 때 10분 안에 풀 수 있는 수준으로 자동으로 조정된다. 정확히는 매 2,016개의 블록이 만들어질 때마다 난이도가 조정되는데, 새 블록이 약 10분마다 형성된다고 했을 때 약 2주간의 시간을 의미한다. 2,016개의 블록이 만들어지는 평균시간이 블록당 10분보다 짧으면 2,016개의 블록이 생성된 이후 난이도를 상향 조정해 블록 생성시간을 늘리고, 반대로 평균시간이 10분보다 길게 형성되면 이후에는 난이도를 하향 조정하여 블록 생성 시간을 줄이는 시스템이다.

이렇듯 컴퓨팅 파워를 투입하여 지난 10여분간의 거래 내역이 기록된 블록을 최초로 형성한 채굴자(혹은 집단)에게 승인한 거래 내역의 모음인 블록을 기존 블록체인(장부)에 등록할 수 있는 권한을 주고, 블록 생성을 통해 새롭게 발행된 비트코인을 보상으로 지급한다. 투입하는 에너지가 많을수록 채굴 경쟁에서 이겨 신규 발행 비트코인을 받을 확률이 높아지기 때문에 채굴만을 위해 엄청난 양의 컴퓨팅 파워를 투입하여 전문적으로 채굴을 하는 사례 또한 증가하고 있다. 최근까지 한 번의 채굴로 발행된 비트코인은 한 블록당 25BTC였으나 올해 7월 반감(halving)이 발생하여 채굴 비트코인 양이 이전의 절반인 12.5BTC로 줄어들었다. 한편 블록 형성에 성공한 채굴자는 신규 발행 비트코인과 함께 거래 과정에서 지급된 소액의 수수료 또한 추가 보상으로 받게 된다. 비트코인 프로토콜은 일정 기간(약 4년)마다 반감이 발생하여 최종적으로 2140년에 약 2,100만개의 비트코인이 발행된 이후에는 추가적인 채굴 없이 거래 수수료만으로 운영되게끔 설계되어 있다. 구조적으로 한정된 양의 금액을 발행하고 그 발행량도 시간이 지나면서 지수적으로 줄어들기 때문에 화폐 발행량 증가로 인한 인플레이션이 발생하지 않는 구조를 가지고 있다.

<그림 2-4> 비트코인 통화 공급량

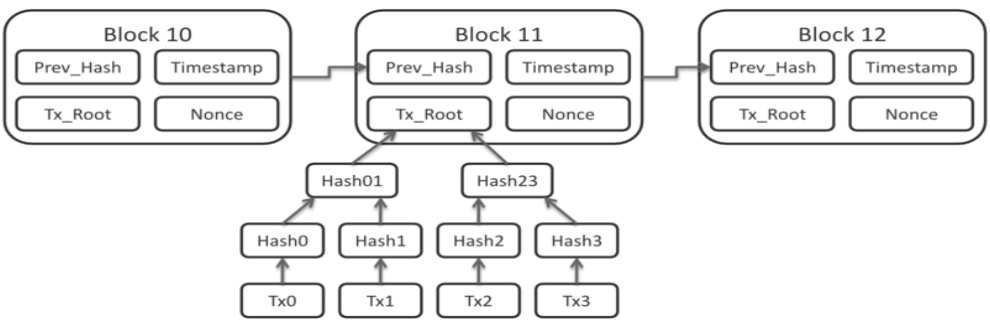


자료: Mastering Bitcoin

이러한 과정으로 만들어진 비트코인의 블록에는 거래 내역 및 정보가 저장되어 있다. 블록 내 핵심적인 주요 데이터를 담고 있는 앞부분을 블록 헤더(Header)라 부르고 이 블록 헤더에는 거래의 주요 정보들이 담겨 있다. 우선 블록 헤더에는 해당 블록의 직전 블록인 부모 블록의 암호(Hash) 값이 있다.

각 블록의 앞부분에 이전 블록의 정보가 연결되어 있는 구조이기 때문에 마치 블록이 연결되어 있는 것 같다는 의미의 블록체인이라는 이름이 지어졌다. 이러한 구조에서 과거에 생성된 특정 블록을 위변조하기 위해서는 다음 블록체인이 연결될 약 10분의 시간동안 그 블록 이후에 연결되어 있는 모든 블록을 새롭게 생성해 내야 하기 때문에 이런 구조적 특성이 블록체인의 위·변조를 사실상 불가능하게 만들며 블록체인을 비가역적 데이터라고 부르는 요인이 된다. 그 외에도 블록 헤더 부분에는 해당 블록 채굴 당시의 난이도, 블록 생성 시간을 보여주는 타임스탬프, 논스(Nonce)값이 표시되며, 모든 거래 내역의 요약본이라고 할 수 있는 머클 트리 루트가 표시된다. 머클 트리는 블록에 들어가는 수많은 거래 데이터를 요약하고 검증할 수 있도록 만드는 데이터 구조를 의미하며, 각 거래 내역을 암호화한 노드가 쌍으로 구성되어 하나의 노드로 합쳐져 다시 암호화되는 과정이 반복된다. 머클 트리의 과정을 거쳐 모든 암호화된 거래 내역이 요약되어 있는, 가장 상위에 있는 하나의 값을 머클 트리 루트라고 부른다. 아무리 많은 건수의 거래 내역이 요약되어 있다 하더라도 머클 트리 루트의 크기는 32바이트로 동일하다. 머클 트리 구조는 수많은 거래값을 요약해 헤더에 보관한다는 장점뿐 아니라, 요약된 거래 내용이 루트에서 출발하여 아래로 연결되어 갈라지는 모습을 하고 있기 때문에 루트와 거래를 연결하는 인증 경로를 통해 해당 거래의 유효성을 입증할 수 있고 잘못된 거래 내역이 발생할 시 짧은 시간에 신속하게 파악이 가능하다는 장점이 있다. 머클 트리에 대한 추가적인 내용은 3장에서 서술한다.

<그림 2-5> 블록 헤더의 구성도



자료: Matthaus Wander

비트코인 블록체인으로 대표되는 개방형 블록체인은 일반적으로 하나의 단일한 목적을 가지고 운영되며 익명의 사람들이 참여할 수 있고 악의를 가진

참여자들의 공격을 막기 위해 채굴 등의 내부 시스템을 통해 구조적으로 신뢰를 구축한다. 우선, 개방형 블록체인의 장점은 중앙기관이 없어도 거래 플랫폼을 유지할 수 있다는 안정성에 있다. 이전에도 분산된 서버를 통한 P2P 네트워크를 활용한 사례는 있었지만 분산원장을 통한 가상화폐 플랫폼을 개발한 경우는 비트코인 블록체인이 처음이다. 가장 견고한 보안 체계가 필요한 화폐 시스템을 블록체인 네트워크로 구현하여 지금까지 중앙 기관 없이 운영되고 있는 비트코인은 개방형 블록체인이 가지고 있는 견고함과 안전성을 보여준다. 비록 마운트곡스나 홍콩 비트코인 거래소 해킹 등 거래소에서 비트코인이 유실된 사건들이 있었지만, 은행에 강도가 들었다고 해서 화폐 시스템에 대한 문제로 볼 수 없듯이 이는 비트코인을 담당하는 거래소에 국한된 사례로 볼 수 있다. 비트코인 블록체인 자체는 악의적 공격을 미연에 방지하고 대응할 수 있는 보안성을 가지고 있고 이는 개방형 블록체인 위에서 움직이는 비트코인이 여전히 화폐적 가치를 지니고 있는 기반이 된다.

또한 개방형 블록체인은 높은 개방성과 투명성의 장점을 가지고 있다. 일반적으로 금융거래를 하기 위해서는 개인정보 등록이나 계좌 생성 등 긴 절차를 가지고 있다. 금융에 있어서 정보와 보안은 가장 중요한 이슈이기 때문이다. 하지만 운영 주체가 없이 시스템만으로 운영되는 개방형 블록체인은 높은 진입장벽을 가지고 있는 기존 서비스들과 달리 시간의 제약없이 쉽게 주소를 만들어서 네트워크에 참여할 수 있고 일정한 컴퓨팅 파워만 있으면 원하는 역할을 모두 수행할 수 있다. 필요에 따라서는 채굴에만 참여할 수도 있고 전자화폐를 이용만 할 수도 있으며 블록체인 네트워크에 필요한 모든 역할을 수행할 수도 있다. 역할의 선택과 변화에 제약이 없다. 개방형 블록체인인 이더리움의 경우에도 누구나 모든 거래 내역을 확인할 수 있다. 비트코인에 등록된 모든 거래 내역, 수/발신 주소, 잔액 등의 기록을 다 확인할 수 있으며 이는 개방형 블록체인 내의 거래 시스템이 위·변조를 막고 위·변조 시도가 있을 시 실시간으로 검증할 수 있게끔 투명하게 운영되게 하는 기능을 한다.

나. 개방형 블록체인의 과제 및 대안

개방형 블록체인은 이름 그대로 모두에게 개방되어 있고 불특정한 익명의 참가자들이 참여할 수 있다. 그렇기 때문에 시스템 상으로 서로간의 신뢰를 가지고 거래를 하고 악의적인 내·외부의 공격을 방지하기 위해 높은 안정성

을 가진 시스템 구축이 필요하며 실제로 많은 장치들을 개방형 블록체인 내에서 구축하고 있다. 일반적인 화폐 시스템에서는 중앙은행 등 특정 기관이 유통 및 관리를 책임지고 그 기관에 대한 신뢰를 바탕으로 화폐 시스템에 대한 신뢰가 형성된다. 하지만 이와 달리 비트코인 블록체인의 경우 거래와 시스템을 전적으로 통제할 중앙기관이 아예 없기 때문에 익명의 참여자들 간의 신뢰를 형성하고 안전을 확보할 수 있는 많은 장치들이 개방형 블록체인을 안정적으로 운영할 수 있는 기반이 된다.

하지만 개방형 블록체인이 외부의 공격으로부터 완벽하게 자유로운 시스템이라고 부르는 데에는 한계가 있으며, 위에서 언급한 장점들이 오히려 단점이 되어 개방형 블록체인을 다른 분야로 응용하는 데 한계로 작용하기도 한다.

우선 비트코인 블록체인의 경우 분산원장 시스템을 기반으로 모든 거래 내역이 공개되는 투명성이 금융기관이 개방형 블록체인을 활용하는 데 제약이 된다. 개방형 블록체인에서는 모든 참여자가 모든 거래 내역을 조회할 수 있으며 각 계좌에 대한 정보도 찾아볼 수 있다. 개방형 블록체인의 투명성은 비트코인 시스템에 신뢰를 부여하고 높은 안정성을 가지는 데 결정적인 역할을 하지만 이 투명성은 블록체인을 다른 분야로 응용하는 데 제약이 되며 특히 금융기관에서 응용하기에 어려운 점으로 작용한다. 금융기관 간의 거래는 기본적으로 개인정보의 보안을 유지할 필요성이 크기 때문에 개인정보의 무제한적인 개방은 부적절하며, 금융기관 내에서도 공개하면 안 되는 기밀자료들이 존재한다. 이렇듯 금융기관을 이용하는 고객과 금융기관들은 거래내역이 자신의 거래와 관계없는 기관 및 단체에게도 공개된다는 사실을 받아들이기 쉽지 않을 것이다.

그리고 개방형 블록체인의 익명성 또한 활용성을 제약하는 요인으로 작용한다. 비트코인 같은 개방형 블록체인은 기본적으로 어떠한 참여의 제한이 없이 익명으로 거래가 이루어지는 플랫폼이다. 하지만 정반대로 금융기관이나 일반 기업에서는 고객의 정보를 아는 것이 매우 중요한 과제이다. 전 세계적으로 자금세탁 방지(Anti Money Laundring), 고객 알기 제도(Know Your Customer) 등과 같이 탈세, 마약 밀매, 테러자금 조달 등을 방지하기 위한 규제가 주요 이슈이며, 우리나라에서도 원칙적으로 본인 명의가 아닌 다른 사람의 이름으로 계좌를 만들거나 거래하는 것이 금지되어 있다. 따라

서 금융기관이 광범위하게 블록체인을 사용하기 위해서는 고객들이 실명으로 거래하는 시스템이 필요하며, 익명을 유지하며 사용할 수 있는 금융서비스는 매우 협소하거나 사실상 없다고 볼 수 있다. 이는 개방형 블록체인의 기본 전제인 익명성과는 사실상 정반대의 상황이기 때문에 금융기관과 일반 기업들이 개방형 블록체인을 그대로 사용하는 것은 매우 까다로운 일이다.

또한 개방형 블록체인은 효율성에 있어서도 한계점이 명확한데, 개방형 블록체인을 유지하는 데 필요한 과도한 시간, 비용 그리고 작은 용량 등이 지적된다. 우선 개방형 블록체인을 유지하는 데 많은 비용이 든다. 비트코인 화폐 시스템에서 화폐를 발행하기 위한 방법인 채굴은 비트코인 네트워크에서 신뢰성을 확보하기 위한 가장 중요한 장치이다. 위에서 언급했듯이 채굴이란 비트코인 네트워크의 참여자가 본인의 컴퓨팅 파워를 이용해 직접 거래를 승인하고 블록체인에 거래 내역을 등록한 후, 발행된 비트코인이 거래의 승인과 등록에 기여한 컴퓨터 중 하나에 보상으로 주어지는 과정을 말한다. 채굴은 익명의 참여자가 비트코인 블록체인을 공격할 수 없게끔 신뢰를 형성하고 비트코인 화폐 시스템을 운영하게 만드는 핵심적인 방안이지만 많은 시간과 많은 전력 소모량을 필요로 한다는 단점이 있다. 작업 증명과 채굴의 과정을 통해 시스템을 보호하는 컴퓨팅 파워를 가지게 되지만 거래 자체만을 놓고 봤을 때는 굳이 그렇게 많은 에너지를 소모할 필요가 없다.

또한 개방형 블록체인의 긴 승인 시간은 특히 금융기관에서 활용하기에는 시간적 비효율성이 있다. 일반적으로 비트코인 거래의 최종 승인은 6 Confirmation이라고 부르는데, 거래를 완료한 이후 6개의 블록이 만들어지면 거래 위·변조의 가능성이 사실상 없기 때문이다. 평균적으로 1개의 블록이 만들어지는 데 10분이 걸리기 때문에 통상 1시간 정도가 지나야 해당 거래가 완전히 안전하다고 판단할 수 있다. 일반적인 거래에서 승인까지 1시간이 걸린다면 그 화폐는 실질적인 활용도를 가진다고 보기 어려울 것이다. 가게에서 물품을 사고 결제를 하는데 최종 승인이 날 때까지 1시간이 걸린다면 이용에 큰 불편함이 초래되기 때문이다.

비트코인의 작은 거래 용량과 블록의 크기도 활용을 어렵게 만든다. 비트코인은 현재 1초에 약 7건의 거래를 처리하는데 이는 세계적 지급카드 네트워크인 비자(Visa)의 처리량인 초당 약 2,000건보다 한참 못 미치는 수준이다. 이는 거래가 기록되는 블록의 용량이 최대 1MB에 불과하고 거기에서도 활

용할 수 있는 공간은 제한적이기 때문인데, 따라서 일반적인 금융기관들이 요구하는 다양하고 많은 용량의 정보들을 처리하는 데는 큰 한계를 보일 수 밖에 없다.

또한 개방형 블록체인이 가진 비가역성은 금융기관이 활용하는 데 어려움으로 작용한다. 비트코인 블록체인의 경우 화폐를 발행하고 거래를 중개하는 중앙기관이 없는 혁신적인 모델이지만 화폐 시스템을 책임지는 중앙기관이 없기 때문에 거래시 사고 등이 발생하는 경우 모든 책임이 거래 당사자에게 귀속된다는 문제가 있다. 비트코인 주소나 거래금액을 잘못 기입해서 전송하는 경우에도 이에 대해 정정을 요청할 수 있는 중앙기관이 없으며, 비트코인 주소를 제외하면 송금을 받는 상대방에 대한 정보를 알 수 없기 때문에 서로 아는 사이가 아닌 한 잘못된 송금을 받은 사람을 찾는 것은 매우 어렵다. 또한 따로 비트코인 계정을 보관해서 관리하는 주체도 없기 때문에 비트코인 주소를 분실한 경우 다시 돈을 돌려받거나 계정을 찾을 수 있는 방법은 사실상 없다. 중개기관을 없앤 가상화폐 플랫폼이라는 비트코인 블록체인의 시스템은 금융기관의 관심을 가지게 할 만한 흥미로운 모델이지만 중앙기관이 관리하는 정보가 없는 분산화된 네트워크의 속성은 오히려 소비자 정보를 관리하고 중개함으로써 신뢰를 얻는 금융기관이 활용하기에 어려움으로 작용한다.

이렇듯 일반적인 개방형 블록체인은 익명의 다수가 참여할 수 있도록 견고한 시스템을 갖추고 있으나, 다른 분야로의 활용에 있어서는 여러 한계점을 가지고 있다. 하지만 이미 다수가 참여하고 목적과 기능이 제한되어 있는 기존 개방형 블록체인을 일방적으로 변형하거나 수정할 수 없기 때문에 개방형 블록체인의 장점을 유지하면서 새로운 기능들을 더하여 특정 기능을 강화하거나 활용도를 높인 개방형 블록체인들이 새롭게 개발되어 등장하고 있다.

우선 비트코인의 대체 암호 화폐(Alternative Cryptocurrency)인 알트코인이 있다. 알트코인은 비트코인 블록체인의 화폐적 기능의 개선을 위해 만들어진 대체 암호화폐들을 통칭하며 비트코인이 화폐로서 가지고 있는 확장성, 거래속도 등의 문제점들을 극복하고 더 활용도가 높은 암호화폐를 만들기 위한 시도들이다. 현재 거래되고 알트코인의 종류는 약 700개로 추산된다.[169] 대부

169) www.coinmarketcap.com

분의 알트코인은 비트코인과 유사한 시스템과 기능을 가지고 있기 때문에 비트코인과 기본적인 시스템은 동일하며, 많은 디지털화폐 거래소에서 다양한 알트코인들이 실제로 거래되고 있다. 하지만 비트코인이 암호 화폐 시장에서 차지하는 점유율이 약 90%에 달할 정도로 압도적이고 비트코인 블록체인에 투입된 자원과 인력이 많기 때문에 알트코인이 실질적으로 비트코인이 가진 화폐의 역할을 대신하기는 어려울 것이다. 하지만, 통화 발행의 속도와 발행량 조절, 합의 알고리즘을 변경하거나 새로운 기능을 추가하는 등의 변형을 통해 암호화폐의 기능적 확장과 활용에 있어서의 새로운 가능성을 모색하려는 시도가 이어지고 있다.

대표적인 예시로는 라이트코인(Litecoin)을 들 수 있다. 라이트코인은 가장 먼저 만들어진 알트코인 중 하나로 현재 비트코인, 이더리움, 리플에 이어 암호화폐 시가총액 기준 4위의 암호화폐이다. 주요 특징은 블록의 생성 시간을 10분에서 2분 30초로 단축하고 기존 비트코인에서 사용하던 SHA-256 암호화 방식 대신 Scrypt 방식을 사용하며, 총 화폐 발행량도 비트코인의 약 2,100만 코인보다 4배가 많은 8,400만 코인으로 늘어나는 등 기존 비트코인 시스템보다 빠르고 유연하고 확장성 있는 시스템으로 운영되고 있다.

이외에도 비트코인보다 더 강력한 익명성을 구현하기 위해 만들어진 모네로(Monero), 작업증명 채굴 방식 대신 순수한 지분 증명(Proof-of-Stake) 방식으로 구현하고 블록생성 시간을 1분으로 줄인 넥스트(NXT), 라이트코인으로부터 분기되어 나와서 2015년까지 1,000억 코인을 발행할 정도로 발행 규모를 높인 도기코인(Dogecoin) 등 기존 비트코인 블록체인의 시스템을 개선하여 더 확장성이 있고 활용이 쉬운 알트코인 개발이 이어지고 있다.

<그림 2-6> 암호 화폐의 자본 규모 순위 (10월 기준)

All Currencies

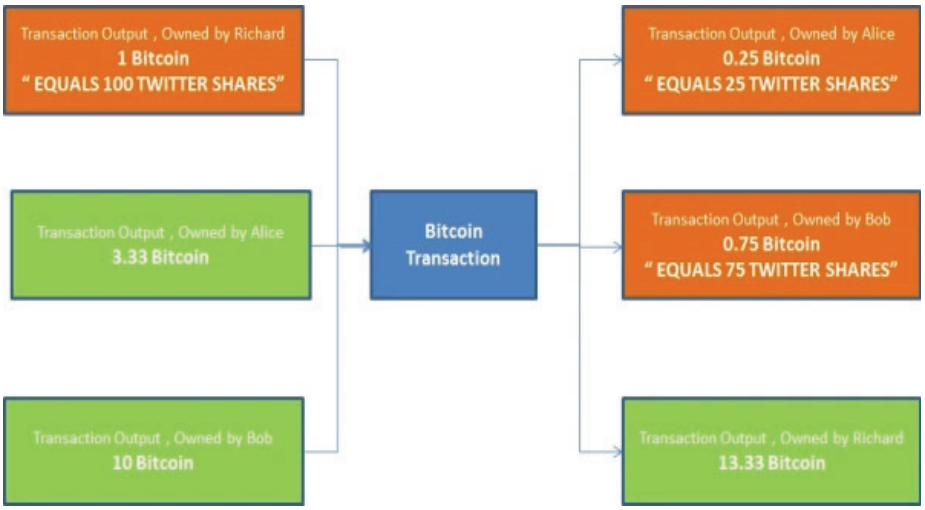
All ▾ Currencies ▾ Assets ▾ USD ▾ ← Back to Top 100

#	Name	Symbol	Market Cap	Price	Available Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$9,490,080,851	$597.49	15,883,140	$60,872,600	0.03%	0.04%	-1.80%
2	Ethereum	ETH	$1,121,526,200	$13.31	84,248,631	$23,603,100	0.66%	1.24%	11.37%
3	Ripple	XRP	$243,871,892	$0.006878	35,458,607,580 *	$1,506,640	0.04%	-0.38%	-11.96%
4	Litecoin	LTC	$179,891,543	$3.77	47,681,429	$1,071,260	0.20%	-2.06%	-1.00%
5	Monero	XMR	$133,190,360	$10.28	12,959,791	$3,189,580	-0.93%	-0.12%	6.23%
6	Ethereum Cla...	ETC	$107,031,359	$1.27	84,203,066	$5,405,380	-0.16%	8.17%	-0.80%
7	Dash	DASH	$78,331,006	$11.59	6,757,566	$414,224	0.17%	1.34%	-4.57%
8	Steem	STEEM	$71,868,313	$0.472179	152,205,654	$514,707	1.22%	13.28%	-5.31%
9	NEM	XEM	$46,750,500	$0.005195	8,999,999,999 *	$49,733	-0.17%	-4.46%	-6.90%
10	MaidSafeCoin	MAID	$38,454,238	$0.084972	452,552,412 *	$103,734	1.20%	-0.13%	-12.73%
11	DigixDAO	DGD	$30,063,000	$15.03	2,000,000 *	$112,260	6.50%	-5.70%	0.18%
12	Factom	FCT	$26,304,736	$3.01	8,753,219 *	$1,426,300	3.09%	-1.52%	-12.12%
13	Lisk	LSK	$24,408,300	$0.244083	100,000,000 *	$328,924	-0.20%	-1.39%	-4.29%
14	Dogecoin	DOGE	$24,079,742	$0.000227	106,153,917,124	$96,647	0.46%	-1.59%	-3.80%
15	Waves	WAVES	$18,922,000	$0.189220	100,000,000 *	$41,369	-1.25%	-1.34%	14.89%
16	Nxt	NXT	$15,640,044	$0.015656	998,999,994 *	$162,471	-0.20%	0.04%	-21.11%
17	Emercoin	EMC	$14,888,289	$0.385861	38,584,592	$38,105	-0.48%	-0.57%	-4.03%
18	Counterparty	XCP	$14,106,966	$5.38	2,623,195 *	$236,096	0.61%	8.77%	25.72%

자료: coinmarketcap

개방형 블록체인의 활용도를 높이기 위한 또 다른 방법으로는 컬러드 코인(Colored Coin)이 있다. 여기서 컬러드(Colored)라는 단어는 비트코인에 특정한 가치를 입힌다는 뜻으로 해석할 수 있다. 따라서 새롭게 블록체인을 만든 알트코인과는 달리 컬러드 코인은 기존의 비트코인 블록체인을 이용하는 방법으로, 비트코인 블록체인의 기록에 다른 자산 기록들의 정보를 '입히는' 방식으로 이용한다. 컬러드 코인을 사용하고자 하는 기관은 비트코인의 정보가 저장되는 공간에 유통하고자 하는 디지털 자산의 정보를 입히고 자산의 정보가 입혀진 코인은 해당 기관에 의해 관리된다. 컬러드 코인을 기반으로 자체적인 플랫폼을 만들어 해당 기관의 고객들이 하나의 가치를 가진 자산으로써 활용하되, 해당 기관이 컬러드 코인의 개인키를 가지고 있기 때문에 고객이 비트코인의 용도로 사용을 제한하고 컬러드 코인으로써만 사용하게 하는 환경을 조성할 수 있다. 연관성을 제거하여 컬러드 코인의 컬러를 뺄 수도 있고 그냥 비트코인으로 거래를 하여도 문제는 없다. 다만, 현재 성공적으로 발행 및 유통되고 있는 비트코인에 또 다른 가치를 입혀서 비트코인을 다른 방향으로 활용할 수 있는 방법 중에 하나로 볼 수 있다.

<그림 2-7> 컬러드 코인의 전개



자료: Richard Gendal Brown

컬러드 코인 기술은 법적으로 공식적인 효력을 갖지 않을 수도 있지만 이미 많은 참여자들과 컴퓨팅 파워가 투입되어 사실상 조작하는 것이 불가능할 정도로 견고한 비트코인 블록체인 구조를 바탕으로 특정 시점에서 자신의 소유권과 상태를 확인할 수 있는 수학적 근거로 제시될 수 있다. 다만, 컬러드 코인에 비트코인보다 훨씬 높은 가치의 자산이 입혀졌을 경우 비트코인 블록체인 시스템에 대한 공격의 유인이 될 수 있기 때문에 각 금융기관이나 단체가 당장 도입을 하기에는 한계가 있다. 현재 비트코인 블록체인에 투입되는 전력의 양은 연간 약 5천억원 규모로 추산하는데 이 금액을 넘어서는 자산이 컬러드 코인으로 거래가 된다면 외부에서 그 비용을 감수하고 비트코인 블록체인을 공격하는 유인이 생기게 되며 이는 블록체인 시스템 자체에도 큰 위협이 된다. 또한 서로 다른 기관이 만든 컬러드 코인끼리 거래할 수 있는 방식이 비트코인 거래로 제한된다는 점도 컬러드 코인의 활용을 어렵게 만든다. 결제의 동시성이 중시되는 금융거래에서 약 1시간 동안 승인을 기다려야 하는 개방형 블록체인 거래 메커니즘은 활용의 범위를 제약한다. 활용 확장성에 있어서의 한계점으로 인해 금융기관에서 컬러드 코인의 활용도는 떨어지지만, 최근에는 컬러드 코인의 메커니즘을 차용한 폐쇄형 블록체인 플랫폼들이 등장하고 있다. 대표적인 사례는 Colu라는 미국의 스타트업이다. Colu는 상품권, 티켓 등의 정보를 블록체인의 코인 형태로 등록하거나 새로운 코인을 만들어서 자유롭게 거래할 수 있도록 만든 블록체인 플랫폼으로 폐쇄형 블록체인을 활용했지만 블록체인의 코인에 특정 자산의 가

치를 입혀 거래를 용이하게 하는 컬러드 코인의 플랫폼을 차용한 사업 모델이다.

알트코인과는 다르게 화폐 플랫폼으로써 블록체인이 아닌 다른 기능에 주목하여 새롭게 만든 블록체인 프로토콜 또한 개방형 블록체인의 한계점을 극복하기 위한 방안으로 제시되고 있다. 앞에서 설명했던 이더리움과 리플 등이 그 예시가 될 수 있다. 최근 DAO를 통해 각광을 받은 이더리움의 경우는 기존 블록체인보다 스마트 계약(Smart Contract)의 기능을 강화하고 처리 속도를 높인 개방형 블록체인이며, 송금 및 결제 기능을 강화한 리플이나 스텔라(Stellar) 등의 개방형 블록체인 등도 등장하여 활용 방안을 찾고 있다. 하지만 아직까지 이러한 대안적 개방형 블록체인들도 한계점을 가지고 있다. 이더리움의 경우 최대 처리 속도를 12초로 대폭 단축하며 활용 가능성을 높였지만, 여전히 개발 초기 단계에 있고 프로토콜의 용량이나 보안의 문제에 있어서는 여전히 개선이 필요하다는 의견이 있다. 최근 발생한 DAO 해킹 사건의 경우에도 이더리움 블록체인 자체의 문제에서 비롯된 사고는 아니었지만 블록체인의 활용법에 있어서 문제점이 나타나는 경우 블록체인의 안전성에 상관없이 많은 사람들이 피해에 노출될 수 있음을 시사한다.

또 다른 개방형 블록체인에 대한 대안은 폐쇄형 블록체인(Private Blockchain)이다. 폐쇄형 블록체인은 블록체인에 참여하는 기관의 수를 제한함으로써 정보 공개 범위를 제한할 수 있으며 참여 기관이 공개하기를 원치 않는 회사 혹은 고객의 정보를 밖으로 드러내지 않을 수 있다는 장점을 가지고 있다. 폐쇄형 블록체인에 대한 상세한 설명은 다음 장에서 서술한다.

다. 개방형 블록체인의 활용 방식

개방형 블록체인의 경우 모두가 참여할 수 있는 플랫폼이지만 특정한 목적을 가지고 만들어진 블록체인 플랫폼인 만큼 활용에 제약이 많고 플랫폼 자체를 변형하거나 조작하는 것이 불가능에 가까워 이를 응용하여 다른 분야로 활용하기가 매우 까다로운 편이다. 하지만 개방형 블록체인의 경우 누구나 자유롭게 참여해 활용할 수 있는 공유지와 같은 플랫폼인 만큼 뒤에 언급할 폐쇄형 블록체인보다 일반적인 접근성이 뛰어나기 때문에 활용성의 제약에도 불구하고 쉽게 이용할 수 있다는 특징이 있다. 특히 과도한 중개자의 개입 필요성으로 인해 비효율성이 초래되는 분야에서 개방형 블록체인의 응

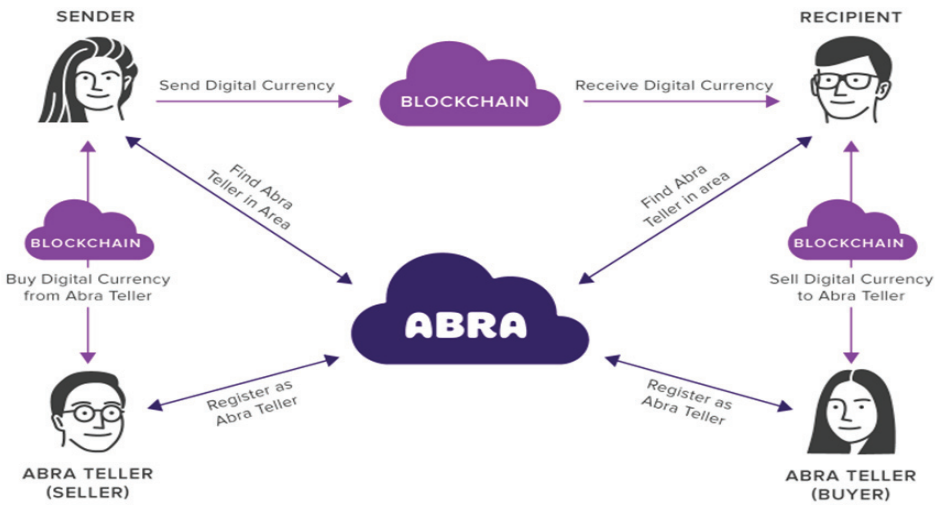
용이 적절히 활용될 수 있다.

(1) 해외 송금

가장 대표적인 분야는 송금, 그 중에서도 해외송금이다. 현재 해외송금의 경우 SWIFT 등의 전산망과 중개은행을 거치면서 많은 수수료가 부과되고 이는 특히 해외로 소액 송금을 하는 사용자에게 높은 수수료 부담으로 전가된다. 하지만 누구나 사용할 수 있으면서도 위·변조의 위험이 적고 화폐와 국경의 경계에 구애 받지 않는 비트코인 블록체인은 낮은 수수료로 돈을 전송할 수 있는 플랫폼으로 활용될 수 있으며 실제로 많은 스타트업이 이를 해외송금 플랫폼으로 활용하고 있다. 대부분의 경우 송금하게 될 금액을 해당 국가 화폐로 환전하기 전에 먼저 비트코인으로 전환하고, 전환된 비트코인을 해당 수신 국가의 화폐로 다시 전환하는 시스템을 적용한다.

대표적인 사례는 필리핀 기반 해외 송금 업체인 Abra다. Abra를 통해 필리핀에 거주하는 사람이 미국에 사는 사람에게 송금하려고 할 때, 송금 송신자는 우선 본인과 가장 가까이 있는 Abra 텔러를 찾아 송금할 돈을 건네준다. 금액을 받은 Abra 텔러는 해당 금액을 비트코인 블록체인 시스템에 전환하여 넣는다. 이후 송금 수신자는 본인과 가장 가까운 Abra 텔러를 찾아 송금한 금액을 요청하고, 수신자와 가까이 있는 텔러는 블록체인 내의 금액을 인출하여 수신자에게 지급하는 시스템이다. Abra는 비트코인 블록체인이 가진 개방성을 송금 서비스에 적용하여 성공한 사례이다. 리플의 경우 Abra 등 송금 업체가 활용하는 비트코인 블록체인과는 다르게 송금 및 결제에 특화된 자체 개방형 블록체인 프로토콜을 개발하고 여기에 금융기관들이 참여하고 있는 케이스다. 리플은 분산화된 네트워크를 통해 은행 간 혹은 국가 간 송금을 복잡한 절차 없이 빠르게 진행할 수 있다. 이와 같이 누구나 쉽게 활용할 수 있고 중개자와 국경의 경계 없이 활용할 수 있다는 비트코인 블록체인의 장점을 기반으로 송금 플랫폼을 만들어 수수료를 대폭 절감하고 송금 시간을 단축을 도모하는 사례들이 다수 생겨나고 있다.

<그림 2-8> 아브라의 개방형 블록체인 활용 구조도



자료: Abra

(2) 크라우드 펀딩

불특정 다수가 참여하여 금액을 모으고 투자하는 크라우드 펀딩도 개방형 블록체인을 적용할 수 있는 또 다른 분야이다. 특히 비트코인보다는 이더리움 등 타 개방형 블록체인을 통해 지속적으로 연구되고 있다. 계속 언급되는 DAO의 경우 이더리움이라는 개방형 블록체인 프로토콜 위에 얹어진 일종의 어플리케이션으로 누구나 참여할 수 있다는 개방형 블록체인의 장점을 이용해 이더리움 블록체인을 크라우드 펀딩에 적용한 사례라고 할 수 있다. 비록 이후 해킹 사고와 이후 처리 과정에서 논란이 발생하기도 했지만, 역대 모금액 1위의 이더리움 기반 크라우드 펀딩 플랫폼이었던 분산형 자치 조직 DAO가 개방형 블록체인을 활용한 크라우드 펀딩의 성공적인 예시라고 할 수 있다.

(3) 앵커링(Anchoring)

또한 개방형 블록체인은 기능적으로 폐쇄형 블록체인(Private Blockchain)을 보조하는 역할을 할 수도 있다. 뒤에서 언급할 폐쇄형 블록체인은 참여 기관의 수를 제한하는 블록체인 네트워크로서 참여기관의 현황 파악이 쉬우며 거래 내역을 추적하기에 용이하다. 하지만 참여기관이 소수이기 때문에 개방

형 블록체인에 비해 내부자에 의한 데이터 공격에 취약점을 노출할 수 있으며, 외부 기관이 폐쇄형 블록체인의 데이터가 위·변조 및 조작되지 않았고, 100% 신뢰할 만한 블록체인 시스템이라는 수학적 근거를 제시하기가 어려울 수도 있다. 개방형 블록체인은 앵커링(Anchoring)이라는 방식으로 이러한 폐쇄형 블록체인의 취약성과 신뢰의 문제를 해소하는 데 도움을 줄 수 있다. 앵커링은 폐쇄형 블록체인의 데이터를 암호화하여 개방형 블록체인의 블록 안에 저장하는 기술을 말한다.

비트코인 블록체인의 경우 전 세계적으로 네트워크가 구축되고 이미 많은 블록이 형성되고 컴퓨팅 파워가 투입된 블록체인 네트워크이기 때문에 위·변조에 대한 문제가 사실상 없다고 할 수 있다. 비트코인 블록체인에 폐쇄형 블록체인 데이터의 해시값을 등록함으로써 기존 데이터에 대한 신뢰도를 확보하고 거래 위·변조 여부에 대한 증거로 응용될 수 있다.

<그림 2-9> 앵커링 구조도

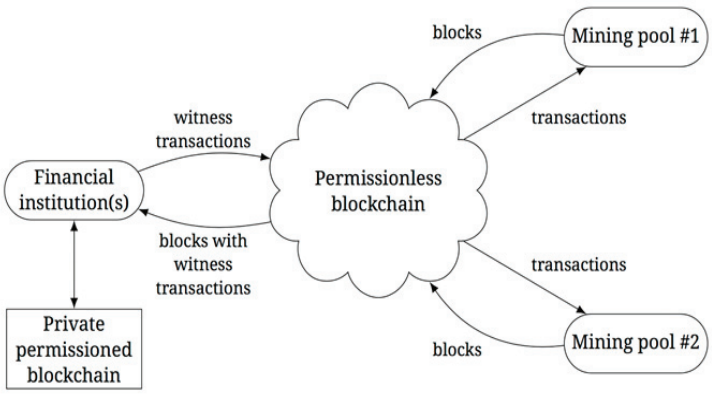


Figure 5: Anchoring a private permissioned blockchain with the supporting public blockchain (e.g., Bitcoin). Unlike merged mining, anchoring requires no or limited cooperation with mining pools

자료: Bitfury WhitePaper 2015

2. 폐쇄형 블록체인

가. 폐쇄형 블록체인의 특징 및 장점

위에서 언급한 바와 같이, 개방형 블록체인이 가진 여러 한계점들을 보완하

고 활용도를 높이기 위해 등장한 것이 폐쇄형 블록체인(Private Blockchain)이다. 금융기관과 기업들은 비트코인과 같은 개방형 블록체인을 통해 블록체인이 기존의 중앙화된 금융 및 산업 시스템의 비효율성과 문제점을 해결해 줄 분산화된 네트워크로써 대안이 될 수 있음을 알게 되었다. 하지만 위에서 언급한 한계점들로 인해 활용상에 많은 제약들이 있었고 이를 극복하기 위한 방안으로 개방형 블록체인의 기본적인 틀을 유지하면서 확장성을 높이는 폐쇄형 블록체인이 등장하게 되었다.

폐쇄형 블록체인의 기본적인 운영 원리는 개방형 블록체인과 크게 다르지 않다. 폐쇄형 블록체인 시스템도 기본적으로 특정 중앙서버가 없이 여러 노드들이 분산형 네트워크를 구성하고, 구성된 노드들의 승인 과정을 통해 데이터 모음이 완성되는 방식으로 이루어져 있으며, 이는 개방형과 폐쇄형 두 블록체인 시스템이 동일하다. 하지만 현재 개방형 블록체인이 가지는 확장성, 익명성, 활용성 측면에서의 한계가 명확하기 때문에 블록체인이 가지고 있는 비용, 보안, 속도 등의 강점만을 활용하기 위한 블록체인으로 개발된 것이 폐쇄형 블록체인이다. 위에서 언급한 R3 CEV, 하이퍼레저 등의 컨소시엄과 기업들의 블록체인 연구 사례들이 폐쇄형 블록체인을 만들고자 하는 대표적인 시도들이다.

즉, 폐쇄형 블록체인은 개방형 블록체인과 활용상 제약을 극복하고 각 분야에 맞게 개량해서 만들어진 블록체인을 통칭한다. 그렇기 때문에 따로 표준화된 기준이나 모델은 없지만 하나로 묶이는 가장 큰 폐쇄형 블록체인의 특징은 블록체인을 사용하는 기업 혹은 기관의 용도와 목적에 맞게 참여자의 수를 제한하고 블록체인의 기능을 변형하였다는 점이다.

우선, 폐쇄형 블록체인은 목적과 상황에 맞게 승인된 기관만이 거래에 참여할 수 있고 거래 기관의 종류와 수도 제한할 수 있다는 특징이 있다. 하나의 블록체인을 만든 후 참여 기관을 제한하여 받아들이는 방법도 있고, 아예 다수의 기관들이 같이 모여서 컨소시엄 형태로 서로 합의 하에 새로운 폐쇄형 블록체인을 함께 구성할 수도 있다. 기관들의 참여에 제한을 두기 때문에 개방형 블록체인과 달리 참여 기관이 어디인지 알 수 있는 기명 블록체인 네트워크를 구성할 수 있고, 그렇기 때문에 참여 기관의 신뢰성 확보가 쉽다는 장점을 가진다. 기관의 수와 종류에 제한을 둘 수 있을 뿐만 아니라 권한도 차등적으로 설정할 수 있다. 개방형 블록체인에서도 역할의 구분은 존재하지

만 각 참여자가 임의로 역할을 설정하거나 변경할 수 있으며, 구조적으로 개별 참여자를 통제할 수 있는 방법은 없다. 하지만 폐쇄형 블록체인은 참여하는 블록체인의 합의, 거래, 검증 등의 역할을 미리 정하여 구성할 수 있기 때문에 블록체인의 기능을 더 효율적으로 수행할 수 있다.

또한 폐쇄형 블록체인은 참여 기관의 수가 제한적이고 기관의 현황 또한 알기 쉽기 때문에 어떤 기관이 언제 거래를 했는지에 대한 내역도 보다 구체적으로 파악할 수 있다. 개방형 블록체인의 경우 거래 내역이 모두에게 투명하게 공개가 되지만 거래에 참여하는 사람들은 익명의 다수이기 때문에 거래에 문제가 생겼더라도 누가 문제를 일으켰는지 알아내기가 어렵다. 하지만 폐쇄형 블록체인에서는 해당 네트워크의 허가를 받은 제한된 참여자들만으로 구성되기 때문에 거래 당사자가 누구이며 거래 내역은 어떤지 파악하기가 용이하다. 이는 기존 개방형 블록체인이 익명의 다수에 대한 보안을 위해 조성한 작업 증명 등의 에너지 소모적인 방법 대신 더 낮은 비용으로 효율적인 보안 시스템을 구성할 수 있다는 장점으로도 이어진다.

그리고 특정 사안에 있어서 논의를 하고 합의를 이끌어내는 데 있어 개방형 블록체인보다 구성원의 의견을 모으는 데 용이하다. 이에 더하여 참여자의 현황과 거래 내역을 쉽게 파악할 수 있다는 특성은 개방형 블록체인에서 다수의 익명의 참여자들 간의 신뢰를 구축하기 위한 시스템을 운영하기 위해 만들었던 채굴 등의 장치들을 다른 효율적인 방법으로 대체할 수 있다는 장점이 있다.

그리고 폐쇄형 블록체인은 참여 기관들이 모든 정보를 공유할 필요가 없다는 장점도 있다. 개방형 블록체인은 기본적으로 블록체인 네트워크에 참여하는 노드들이 거래를 검증하고 전파하여 모든 노드들이 장부를 보유하는 시스템이기 때문에 모든 참여자들이 다른 참여자들의 거래 내역을 확인하고 공유할 수 있으며, 이는 장부 조작을 막을 수 있는 수단 중 하나가 되었다. 하지만 이러한 구조는 정보에 대한 보호가 필수적인 금융기관들이 활용하기에는 많은 리스크를 가지고 있다는 문제가 있었다. 하지만 폐쇄형 블록체인은 각 참여자들이 어떤 자료를 공개하고 하지 않을 것인지, 공개한다면 어떤 범위까지 공개를 할 것인지 범위를 설정할 수 있다. 이는 블록체인의 투명성, 효율성 등 기존에 가지고 있던 장점을 유지하며 활용도를 높일 수 있는 근간이 된다.

또한 폐쇄형 블록체인을 통해 기존의 개방형 블록체인보다 비용 절감에서도 이점이 있다. 분산형 네트워크인 블록체인은 중앙 서버를 관리하고 유지하는 비용을 절감할 수 있다는 장점이 있었지만, 개방형 블록체인의 경우는 외부의 공격과 블록에 대한 조작 등 보안상의 문제를 해결하기 위해 작업증명과 채굴이라는 과정을 통해 실제 거래에 필요한 양보다 훨씬 많은 에너지와 전기를 사용하여 시스템을 보호하도록 설계되었다. 하지만 참여 기관을 제한하도록 설계된 폐쇄형 블록체인은 이같은 소모적 보안 시스템 없이도 네트워크를 구성할 수 있게 되었으며, 데이터베이스의 분산을 통해 비용을 절감할 수 있는 효과를 누릴 수 있다. 그리고 익명의 다수의 안전한 거래를 위해 필요한 10분간의 거래 검증 시간도 다른 보안의 방법으로 대체할 수 있게 되기 때문에 거래 검증의 시간을 대폭 단축하고 초당 거래 건수도 확장할 수 있는 등 활용상의 유연성을 확보할 수 있게 된다.

나. 폐쇄형 블록체인의 과제 및 대안

모든 폐쇄형 블록체인에는 자료와 거래 내역의 공개 범위 제한을 기술적으로 어떻게 구현할 것인가의 과제가 있다. 가령 중앙은행이 주관하고 금융 기관들이 참여하는 블록체인을 구성했을 때, 각 금융기관들은 중앙은행에는 공개할 수 있지만 타 금융기관에는 공개하고 싶지 않은 정보들이 있다. A은행이 B은행에 송금을 한다고 가정했을 때, A은행과 B은행은 이 거래 내역은 거래를 한 당사자와 중앙은행에는 공개하겠지만 타 은행에는 공개하기를 원치 않을 것이며 공개할 필요도 없을 것이다. 하지만 개방형 블록체인의 작업증명 방식을 그대로 폐쇄형 블록체인에 적용한다면 민감한 정보를 노출하기 원하지 않는 금융기관들은 해당 블록체인 네트워크에 참여를 꺼리게 될 것이다. 따라서 폐쇄형 블록체인을 구성할 때 각 금융기관의 정보를 어디에게 어느 정도까지 공유할 것이며, 그 공유 범위를 기술적으로 어떻게 설정할 것인가가 폐쇄형 블록체인 활용에서 가장 중요한 요소 중 하나라고 할 수 있다. 이에 대한 기술적으로 블록체인 내의 공개키(Public key)와 개인키(Private Key)의 Control을 통해서 구현할 수 있다. 접근 권한에 대한 기술적 통제 방안은 제 3장의 블록체인 기반 지급결제시스템에서 상세히 서술한다.

또한 폐쇄형 블록체인에서 중요한 점은 어떻게 하나의 합의된 시스템을 구축할 것인가에 있다. 비트코인 블록체인 등의 개방형 블록체인의 경우, 모두가 접근하여 블록체인을 사용할 수 있는 구조이다. 한편으로 모두가 접근할

수 있다는 의미는 비트코인을 사용하고 비트코인 블록체인의 일원이 된다는 것이고 이는 비트코인 블록체인이 가지고 있는 시스템에 합의를 한다는 뜻이자 비트코인이 가진 채굴 등의 시스템과 블록체인에 담기는 정보, 거래 절차 등에 규칙을 따르겠다는 의미를 내포하고 있다. 반면, 폐쇄형 블록체인은 특정 기관들만이 참여하는 블록체인이기 때문에 접근성에 있어 제한을 둘 수 있지만, 기관들이 활용하기 위해 만들어지는 블록체인이기 때문에 블록체인을 개발하는 모든 부분에 있어서 합의를 도출해야 한다.

시스템에 대한 합의 내용은 기술적 측면도 있지만 각 참여 기관의 내역을 통합해야 한다는 정책적 측면도 존재한다. 예를 들어 금융기관들이 스마트 계약을 바탕으로 하나의 통합 폐쇄형 블록체인을 구축한다고 가정했을 때, 그 스마트 계약에는 어떤 내용들이 들어가야 할지, 금융 거래 유형을 어떻게 구분할지, 형식은 어떻게 갖춰야 할지, 정보의 접근 권한은 어떻게 설정해야 할지 등을 모두 고려해야 한다. 사실상 하나부터 열까지 다 합의를 통해 완전히 새로운 통합 시스템을 만드는 것이다. 각 금융기관은 기존에 유지하고 있는 시스템이 있고 그 시스템에 담긴 세부 내용 및 절차는 각자 달랐다. 이전 중앙화된 구조에서는 중개 혹은 결제를 담당하는 제3기관의 형식에 맞춰서 거래를 진행했지만, 폐쇄형 블록체인을 구성하게 되면 블록체인에 기록할 모든 사항에 대한 합의가 필요하기 때문에 많은 시간이 소요될 수밖에 없다. 지금까지는 합의와 조율을 담당하는 제3기관(예를 들면 외환 거래의 SWIFT 망)이 그 역할을 수행했고, 제3기관으로 인해 초래되는 시간적, 비용적 비효율성을 블록체인이 해결해 줄 것으로 기대하고 있지만, 그 이전에 각 폐쇄형 블록체인이 합의안을 어떻게 구성할 것인가의 문제를 해결해야 할 것이다. 게다가 하이퍼레저처럼 업무상의 공통분모가 적은 금융기관과 비금융기관이 함께 사용하는 폐쇄형 블록체인을 만드는 복합적인 컨소시엄의 경우라면 특정한 합의점을 찾아내는 것이 더 어려운 일이다. 합의된 시스템을 구성하는 문제는 기술적인 영역도 존재하지만 블록체인 플랫폼에 채워질 내용의 문제로서 각 블록체인 컨소시엄 혹은 업체들이 블록체인의 활용에 있어서 시스템과 구성 요소에 대한 충분한 논의와 합의가 필요한 사항이다. 이를 해결하기 위한 1차적인 방안으로는 한 기업이 우선 주도적으로 블록체인 플랫폼을 개발하여 참여자들을 모으거나(R3 CEV가 이와 유사하다) 기업들이 모여 여러 플랫폼들을 개발하고 테스트하고 피드백을 받으면서 개선을 하는 방안이 있다(하이퍼레저가 이와 유사하다).

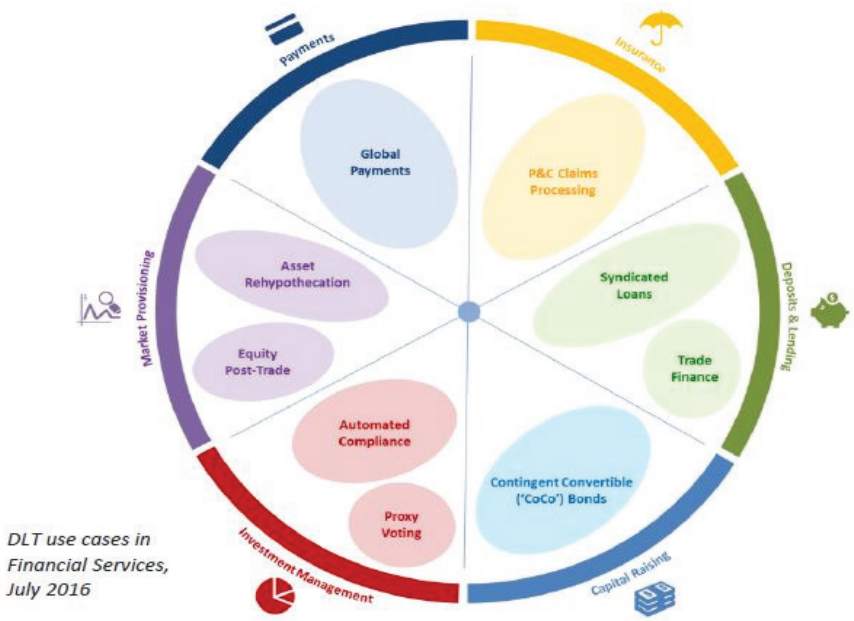
또한 폐쇄형 블록체인의 과제중 하나는 개방형 블록체인이 가지고 있던 보안 장치들을 대체하는 방법을 찾는 것이다. 개방형 블록체인이 높은 보안성을 가질 수 있는 이유 중 하나는 컴퓨팅 파워 측면에서 웬만한 수준으로는 공격할 수가 없는 시스템을 가지고 있기 때문이다. 비트코인 블록체인의 경우 수많은 컴퓨터가 자발적으로 블록체인 네트워크에 참여하고, 작업 증명과 채굴의 과정을 위해 수많은 전기 에너지가 비트코인 블록체인에 투입이 된다. 비트코인의 거래 내역을 조작 혹은 위·변조 하기 위해서는 해당 컴퓨팅 파워의 절반 이상을 보유해야 하는데, 이는 전세계 슈퍼컴퓨터 중 성능을 기준으로 상위 1위에서 500위까지의 용량을 합친 것보다 크다. 결국 구조적으로 공격하기가 거의 불가능에 가까울 뿐만 아니라, 공격이 가능할 정도의 에너지를 가지고 공격에 성공하더라도 비트코인 블록체인에 대한 경제적 이익을 볼 수 없고 오히려 손해를 보게 된다. 하지만 폐쇄형 블록체인은 참여기관의 수가 제한되어 있기 때문에 아무리 큰 기업들이 블록체인 네트워크에 참여하더라도 최대 용량에는 한계가 있으며 개방형 블록체인에 비해 쉽게 공격에 노출될 수도 있다. 또한 소수의 기관이 참여하는 만큼 내부 참여 기관의 악의적 공격에 대해서는 더 취약하기 때문에 내부 공격에 대비할 수 있는 합의 알고리즘 시스템과 관련 규정, 사용자 관리 방안 등에 대한 철저한 구성이 필요하다. 금융기관의 경우 블록체인의 활용은 돈과 이에 관련된 정보에 직결되는 문제이고 중앙은행의 경우 한 번의 보안상의 문제도 국가 경제에 큰 손실을 일으킬 수 있는 만큼 어떻게 폐쇄형 블록체인이 내·외부적 문제에 대해 안심할 수 있을 정도의 보안 체계를 구축하는가는 폐쇄형 블록체인의 운영에 있어서 중요한 문제이다.

내부적 보안 문제를 보완할 수 있는 대안 중 하나로 개방형 블록체인의 활용 사례로 언급한 앵커링을 들 수 있다. 앵커링은 내부 자료가 위·변조가 되지 않았다는 수학적, 구조적 신뢰도를 얻기 위한 방법으로 폐쇄형 블록체인의 정보를 암호화하여 비트코인 블록체인의 블록 내에 연결하여 해당 거래가 위변조가 되지 않았다는 신뢰를 확보할 수 있는 방안이다. 하지만 이는 보안에 대한 근본적인 대책이라기 보다는 파일들이 위·변조되지 않았음을 증명하는 방법에 그친다는 한계가 존재한다.

다. 폐쇄형 블록체인의 활용 가능 분야

폐쇄형 블록체인은 개방형 블록체인이 갖는 활용상의 한계를 극복하기 위해 참여 기관을 제한하는 모든 블록체인을 통칭하는 표현이고, 활용하고 싶은 블록체인의 특징들을 선택하여 만드는 블록체인이다. 블록체인으로 구현하고자 했던 모든 분야에서 활용할 수 있기 때문에 활용 방안은 다양하다. 앞선 사례들에서 언급한 기업, 정부, 금융 기관 등이 활용하고자 하는 블록체인은 대부분 기업이 자체적으로 개발하거나 블록체인 기업과 협업하여 만드는 폐쇄형 블록체인이며 이를 가상화폐, 개인 문서 및 정품 인증, 유통, 결제 및 청산 시스템 등 다양한 분야에서 활용하여 시스템의 효율성을 제고하고자 하고 있다. 실제로 올해 8월에 세계경제포럼(WEF)에서 발표한 분산원장 보고서에 따르면 블록체인은 금융 시장의 결제, 협조 융자, 보험, 무역금융 등 약 9개의 분야에서 활용할 수 있을 것이라고 발표했는데,[170] 이는 기존의 개방형 블록체인의 확장성의 한계를 넘어서 기술적으로 발전한 폐쇄형 블록체인이 등장하기 시작했기 때문에 가능한 결과이다.

<그림 2-10> 금융 기관의 분산 원장 활용 케이스



자료: WEF

170) The future of financial infrastructure, World Economic Forum, 2016

(1) 결제 시스템

폐쇄형 블록체인은 개방형 블록체인이 가진 분산형 네트워크를 유지하기 때문에 데이터의 분산화와 실시간 검증이 가능하다는 장점을 가진다. 거기에 더하여 폐쇄형 블록체인은 기존의 개방형 블록체인이 가진 처리속도상 한계를 극복(비트코인의 경우 1초당 평균 7건의 거래를 처리하기 때문에 초당 수천 건의 거래를 처리하는 금융 기관의 거래량을 감당하기 어려움)하고 더 많은 거래량과 신속한 합의 체계를 구현할 수 있어 금융기관의 결제 시스템에서 많이 활용될 수 있다.

기존 분산형 네트워크의 장점을 유지하여 정보를 실시간으로 처리하며 검증할 수 있는 블록체인은 해외 송금이나 문서, 자산을 전송하는 업무에 용이하게 적용될 수 있다. 중개기관이나 검증 절차 필요 없이 실시간으로 정보를 동기화하여 공유할 수 있기 때문에 결제 리스크를 줄일 수 있다. 다만, 불특정 다수가 참여하는 개방형 블록체인의 경우 정보의 보안을 중시하는 금융기관에서는 활용이 어렵기 때문에 자체적인 폐쇄형 블록체인 개발을 통해 결제 시스템을 구현하고자 하는 사례들이 있다. 앞에서 언급한 디지털 에셋 홀딩스가 대표적인 사례가 될 수 있다.

(2) 자체 운영 디지털 화폐

중앙은행과 은행이 주로 연구하는 금융기관 운영 가상화폐에 있어서도 폐쇄형 블록체인이 중심이 되고 있다. 비트코인으로 대표되는 개방형 블록체인은 통제하는 중앙기관 없이 통화를 발행, 유통 및 관리할 수 있는 혁신적인 사례이다. 비트코인 블록체인의 시스템은 금융기관에게는 디지털 화폐를 운영할 수 있는 기술적 가능성을 보여줬지만, 개방형 블록체인을 그대로 활용하기에는 확장성, 익명성, 높은 투명성 등이 문제가 되었다. 그로 인해 블록체인의 장점을 유지하면서도 금융기관에 맞는 디지털 화폐에 대한 필요성이 제기되었고 이 틀에 맞는 금융권들의 폐쇄형 블록체인 개발이 진행 중이다. 민간 금융기관 중에서는 1장에서 언급한 MUFG 코인이나 Utility Settlement Coin 등을 대표적인 사례로 들 수 있으며, 영란은행의 RSCoin도 이 경우에 해당한다.

(3) 인증

블록체인이 가진 무결성과 보안성을 바탕으로 인증 서비스에 활용하는 방안이 활발히 개발되고 있다. 블록체인 자체에 문서를 올린다기보다는 문서가 가지고 있는 고유의 암호값을 만들어 이를 블록체인에 등록하고 블록체인에 등록된 암호값을 통해 디지털 정보가 진본인지 아닌지를 확인할 수 있는 플랫폼으로 활용하고 있다. 많은 고객의 기밀 정보를 보관하는 금융기관이나 다양한 국민들의 정보를 관리해야 하는 공공 기관에서 블록체인을 활용한 인증 서비스를 구축하고 있다. 개방형 블록체인의 경우 확장성의 문제와 활용의 제약 등으로 넓은 범위의 활용이 쉽지 않기 때문에 폐쇄형 블록체인으로 개발하여 문서의 처리량과 속도를 높이고 안전성을 담보하고자 하는 시도들이 진행중이다. 국내에서는 KB국민카드가 블록체인 기업인 코인플러그와 함께 블록체인 기반 개인인증 서비스를 개발하여 11월 국내 최초 서비스 상용화를 준비하고 있으며,[171] IBM과 마이크로소프트도 인증 플랫폼을 개발 중이다.[172][173]

(4) 무역 금융(Trade Finance)

현재 무역금융 시스템은 국제송금 시스템과 유사하게 복잡한 절차에 따른 시간적, 비용적 비효율성을 가지고 있다. 다수의 중개기관을 통해 문서와 금액이 보내지기 때문에 중개기관을 통해 이동하는 시간 동안 결제 리스크에 노출되며 중개기관에 지불해야 하는 비용도 높다. 또한 많은 문서들을 확인하고 전송하는 작업이 상당 부분 여전히 수작업으로 진행되기 때문에 이 과정에서도 시간의 지연과 실수가 발생하고 결제 리스크가 발생한다.

세계 주요 금융기업들은 무역금융 블록체인 플랫폼을 연구하거나 출시했다. UBS는 IBM과 함께 하이퍼레저를 기반으로 무역의 전 과정을 관리할 수 있는 블록체인 플랫폼을 개발 중이라고 발표했고[174] JP Morgan, 바클레이스나 뱅크 오브 아메리카 등의 금융기관들도 일제히 스마트 계약 등을 통해 무역금융의 프로세스를 자동화, 일원화 할 수 있는 무역금융 플랫폼을 개발하고 있다.

---

171) http://news.mk.co.kr/newsRead.php?no=739530&year=2016
172) http://www.coindesk.com/microsoft-identity-platform-multiple-blockchains/
173) http://www.coindesk.com/ibm-completes-blockchain-trial-french-bank-credit-mutuel/
174) http://www.coindesk.com/ubs-blockchain-prototype-trade/

(5) 스마트 계약(Smart Contract) 관련 플랫폼

스마트 계약은 자기 강제적 언어(self-enforcing language)로 특정 조건을 프로그램화하여 조건이 충족되면 자동으로 실행이 되는 컴퓨터 코드이다. 예를 들어 채권을 스마트 계약에 등록을 한다고 가정했을 때, 만기, 이자율, 지급 지시 등의 내용을 코드로 블록체인에 입력하면 이에 따라서 자동으로 시행되는 방식이다.

사실 스마트 계약 자체는 폐쇄형 블록체인에만 해당하는 내용은 아니다. 비트코인의 경우에도 작업증명 및 채굴의 과정이 일종의 스마트 계약을 기반으로 하는 프로그램이라 볼 수 있으며, 이더리움의 경우에는 스마트 계약에 특화되어 여러 프로그램들을 실행할 수 있는 프로토콜로 발전하고 있다. 블록체인을 도입하는 금융기관 혹은 단체가 폐쇄형 블록체인을 기반으로 하는 자체적인 블록체인 플랫폼을 구축하고자 하는 경우 이더리움을 기반으로 자체적인 블록체인을 만드는 프라이빗 이더리움(Private Ethereum) 플랫폼을 활용하거나 자체적으로 스마트 계약을 입힌 폐쇄형 블록체인을 도입할 수 있다.

전자투표, P2P 펀딩 등 현재 복잡한 절차를 가지고 있거나 많은 부분 수작업으로 이뤄지고 있어서 보안 및 결제 리스크에 노출되는 금융 서비스들을 위주로 스마트 계약을 이용한 서비스 플랫폼 개발이 활발하다. 아직까지 스마트 계약 프로그램은 많은 측면에서 추가적인 개발이 필요한 부분이 있지만 많은 폐쇄형 블록체인 기업들이 이를 블록체인의 활용도를 높일 수 있는 핵심적인 기술로 인식하고 연구개발을 적극 추진중이다.

결국 현재 폐쇄형 블록체인은 중앙화된 시스템이나 과도한 중개기관의 개입 혹은 수동으로 진행되는 절차 등으로 효율성이 떨어진다고 판단되는 분야를 중심으로 논의 또는 적용되고 있다. 이 경우 블록체인을 통한 비용의 절감, 절차의 간소화, 거래 시간의 단축 등 많은 부분에서 개선을 이끌어낼 수 있기 때문이다.

Ⅲ. 중앙은행의 블록체인 활용 방안

본 장은 신한은금융망에 대한 설명과 블록체인기술을 신한은금융망에 적용하는 방안에 대해 기술한다. 해당 장에서 설명하고 블록체인 기술을 적용하는 신한은금융망은 한국은행과 금융기관 간의 거래를 담당하는 거액결제시스템, 그 중에서도 혼합결제시스템으로 범위를 좁혀서 기술한다.

1. 한국은행의 지급결제시스템의 구성

가. 신한은금융망의 혼합형 결제 시스템

한국은행은 기존의 한은금융망을 개선한 신한은금융망(BOK-Wire+)를 개발하여 2009년부터 운영하고 있다. 신한은금융망을 운영하기 이전 기존 한은금융망은 금융기관들이 유동성 리스크에 잘 대처할 수 있도록 특정 시간에 모든 거래 내역을 확인하여 상계 처리하는 실시간 총액결제 방식으로 운영하고 있었다. 하지만 거래 유형이 다양해지고 거래량 또한 증가하면서 이에 걸맞는 새로운 금융망 시스템이 필요하게 됨에 따라 한국은행은 한은금융망에서 동시처리를 더 쉽게 하기 위해 혼합형결제시스템을 추가한 신한은금융망 시스템을 개발하여 운영하고 있다. 신한은금융망은 기존의 전용 단말기에 거래 내역을 입력하는 단일 방식에서 벗어나, 한국은행의 금융망과 금융기관의 서버를 연결하는 서버 간 직접접속 방식을 병행하여 사용함으로써 업무처리의 편의성과 신속성을 강화했으며, 양자간 거래 및 다자간 거래를 위한 실시간 거래 동시처리가 용이한 혼합결제시스템을 추가로 운영하여 신용리스크와 시스템리스크를 감소시킬 수 있게 되었다.

주요 지급결제 업무는 주로 혼합결제시스템에서 처리되는데, 혼합결제시스템에서 관리하는 업무는 크게 세 가지로 나뉜다. 수취인 지정 자금 이체를 포함하는 금융기관 간 일반 자금이체 업무와 콜거래 자금결제 업무, 그리고 증권대금 동시결제(DvP)가 혼합결제시스템의 업무이다.

현재 신한은금융망에 참여하고 있는 금융기관들은 약 130여개이다. 각 금융기관들은 한은금융망에 연결되어 있는 전용 단말기를 통해 한은금융망에서 거래를 진행한다. 이후 신한은금융망이 등장하면서 국내 대형 은행과 일부

증권사, 콜거래 기관은 서버 직접 접속 방식을 통해 바로 신한은금융망을 사용하거나 단말기와 서버 접속 방식을 병행하여 사용할 수 있고, 나머지 기관들은 전용 단말기를 통해 신한은금융망을 이용하고 있다.

나. 일반자금 이체 업무

혼합형 결제 시스템에서의 일반자금 이체 업무는 금융기관 간의 동시 처리 필요성이 높은 이체 업무를 처리한다. 우선 일반자금 이체 업무는 결제 처리의 신속성에 따라 신속지급지시와 보통지급지시로 나뉜다. 신속지급지시는 빠른 시간에 지급지시를 이행하기 위한 시스템으로 A가 B에게 지급지시를 보낼 경우, A의 계좌에 잔고가 있고 한도가 충분하다면, 금액을 지급받게 되는 B의 상황에 상관없이 바로 금액이 보내지는 지급지시이다. A의 계좌에 잔고가 충분하지 않거나 한도를 초과한 경우에는 결제되지 않고 대기파일로 이동한다.

보통지급지시는 계좌에 잔액과 한도가 충분하더라도 바로 결제되지 않고 대기하는 지급지시 시스템으로 A가 B에게 보통지급지시를 신청한 경우, B의 대기 파일에 A에게 보내야 할 지급지시가 있을 때 묶어서 양자간 상계처리를 하는 지급지시 시스템이다. 신속지급지시가 잔액 부족이나 지급 한도 초과일 경우에는 대기파일로 이동하게 되고, 보통지급지시는 상계 처리할 상대의 지급지시가 없으면 바로 대기 파일로 이동하는 구조이다. 신한은금융망의 시스템 마감 시간이 임박한 17시 이후에는 신속지급지시만 입력되며 대기파일에 남아있던 지급지시들도 모두 신속지급지시로 전환된다. 기본적으로 신속지급지시는 보통지급지시에 비해 우선적으로 처리되지만 잔액과 지급한도, 유동성 등의 상황에 따라 유연하게 조정할 수 있다.

일반자금 이체 업무의 처리 방식에 따라서는 양자간 동시처리와 다자간 동시처리로 나눌 수 있다. 양자간 처리는 일반적으로 보통지급지시를 이행하는 방식으로 지급지시 입력 기관(A)이 신규 보통지급지시를 입력하면 거래 상대 기관(B)의 대기 파일을 검색하고 A기관에게 보낼 지급지시 파일이 있다면 동시처리를 시도하는 방식이다. 일반적으로 신속지급지시가 보통지급지시보다 먼저 처리되지만 동시처리 결과 유동성이 유입되는 기관의 경우는 보통지급지시를 우선적으로 처리할 수 있다.

다자간 동시처리는 30분마다 한 번씩 수행되는데 각 금융기관별로 대기중인 지급지시를 확인하여 기관별 예상 유출입액을 계산한 후 잔액과 한도 안에서 결제가 가능한 경우 해당 기관들의 지급지시를 동시에 수행하는 시스템이다. 한 번의 결제에 참여할 수 있는 기관의 수에는 제한이 없고 모든 금융망에 참여하는 금융기관의 거래 내역을 최대한 한 번에 처리하기 때문에 거래 내용이 복잡해질 수 있다.

다. 콜거래 업무

콜거래 업무는 혼합결제시스템에 참여하는 금융기관들을 통해 이루어지는 기업 간의 콜거래를 결제하는 업무를 뜻한다. 콜 중개를 담당하는 회사도 혼합결제시스템에 참여하고 있지만 금융기관 간의 직접 거래도 가능하다. 신한은금융망은 콜자금의 공급과 상환에 관련한 자금들을 결제하는 플랫폼을 제공하고 있으며 하루 이상의 상환 기한이 있는 기일물과 하루 내에 공급 및 상환이 이뤄지는 반일물거래 모두 이용이 가능하다. 콜거래 시스템은 다른 혼합결제와 달리 거래 시간이 정해져 있고 거래 금액 상환도 특정 시간에 일괄적으로 내역을 처리한다. 오전 반일물 거래는 신한은금융망 업무 개시 시점부터 10시50분까지 공급한 후 오후 2시5분에서 일괄적으로 상환되며, 오후 반일물 거래는 11시10분부터 13시50분까지 공급하여 오후 5시5분 상환, 하루를 넘어가는 1일물 이상의 콜거래는 거래 시간에 공급되고 매일 오전 11시5분에 금액을 상환하는 시스템을 가지고 있다. 콜자금이 콜거래 시스템을 거치지 않고 일반 원화자금 이체 시스템으로 전달이 된 경우 콜자금 상환 영수증을 어음교환에 회부하거나 아예 일반 원화자금 이체를 통해 자금을 이체할 수 있다. 신한은금융망에서는 콜거래의 유형, 기관, 금리, 금액 등을 파악할 수 있기 때문에 단기금융시장의 자금흐름을 쉽게 파악할 수 있으며, 여기서 파악한 자료들을 통해 단기적으로 금리를 조정하거나 금융기관에 필요한 정보를 제공할 수 있다.

라. 증권대금 동시결제(Delivery Versus Payment: DvP)

증권대금 동시결제 업무의 경우, 기존의 증권을 구매할 때 대금을 결제하는 시기와 증권을 수취하는 시기 사이의 결제리스크를 극복하기 위한 방안으로 만들어진 시스템으로 한국은행, 한국예탁결제원, 금융기관이 연결된 3자간 거래 시스템이다. 기관 간에 증권매매거래가 체결되면 한국예탁결제원에서는

매도자의 계좌에서 매수자의 계좌로 증권을 이체하는 동시에 대금결제의 내역을 금액, 종류별로 구분하여 한국은행으로 전송한다. 이후 거래를 체결한 금융기관이 신한은금융망을 통해 거래 내역을 확인하고 매수자가 결제를 신청하면 결제전용예금계좌를 통해 매수자의 계좌에서 매도자의 계좌로 거래금액을 송금하는 방식이다. 증권대금 동시결제는 유형상 신속지급지시로 구분이 되어, 양자간 및 다자간 동시처리 없이 건별로 바로 결제되는 방식으로만 처리된다.

마. 혼합결제시스템 지급지시 유형 요약

신한은금융망의 혼합결제시스템은 역할에 따라 크게 일반자금 이체, 콜거래, 증권대금동시결제로 나뉜다. 일반자금 이체는 보통 금융기관이 지급지시를 통해 자금을 보내는 방법이며 콜거래는 단기간에 자금을 빌리고 받는 초단기 대출을 의미한다. 증권대금동시결제는 한국예탁결제원과 연동한 시스템으로 예탁결제원에서 증권의 거래가 체결되면 신한은금융망의 계좌와 연동하여 거래에 참여한 금융기관의 자금을 송금하는 시스템을 의미한다.

각 유형의 거래 방식은 세부적인 절차에서 차이가 있지만 크게는 신속지급지시와 보통지급지시로 나눌 수 있다. 신속지급지시는 상대방의 상태에 상관없이 지급지시 신청 기관의 잔액과 한도를 초과하지 않으면 바로 지급지시를 이행할 수 있는 지급지시 유형이며, 보통지급지시는 상대방이 지급지시 신청 기관에 보내야 할 금액이 있으면 그 둘을 상계 처리하는 방식을 말한다. 일반자금 이체와 콜거래는 신속지급지시와 보통지급지시 중 하나를 선택하여 이행할 수 있으며 증권대금동시결제는 신속지급지시로만 진행할 수 있다.

해당 두 지급지시를 뒷받침하는 시스템은 대기파일이다. 신속지급지시의 경우 잔액이나 한도 부족 등의 이유로 전송할 수 없는 경우, 보통지급지시의 경우 상계처리할 수 있는 상대방의 지급지시내역이 없는 경우에 대기파일로 이동하게 된다. 두 파일은 이후 상대방의 지급지시에 따라서 상계 처리가 되며 일반적으로는 신속지급지시가 보통지급지시보다 우선적으로 처리되지만 지급지시의 유형이나 순서 등의 변경을 통해 각 지급지시의 우선순위를 조정할 수 있다.

대기파일에 있는 지급지시는 양자간 혹은 다자간 동시처리를 통해 해소된다. 양자간 처리는 일반적인 보통지급지시 시스템을 의미하는 것으로 상대방이 보내야 할 지급지시가 있으면 그 둘을 상계하여 처리하는 방식이다. 다자간 동시처리는 30분마다 한번씩 모든 금융기관의 대기파일의 거래 내역을 상계처리하여 대기파일에 있는 지급지시를 최대한 한번에 처리하는 방법으로 두 방식 모두 금융기관의 유동성을 확보하기 위한 시스템이다.

신속지급지시의 경우는 양자간 혹은 다자간 동시처리를 통해 해소가 가능할 뿐만 아니라 계좌의 잔액 혹은 한도의 증가나 대기 순서 조정과 같은 변동사항이 있을 경우 바로 총액결제로 처리될 수 있다.

2. 지급결제시스템에서 블록체인의 활용 방안

가. 분산원장의 핵심 기술

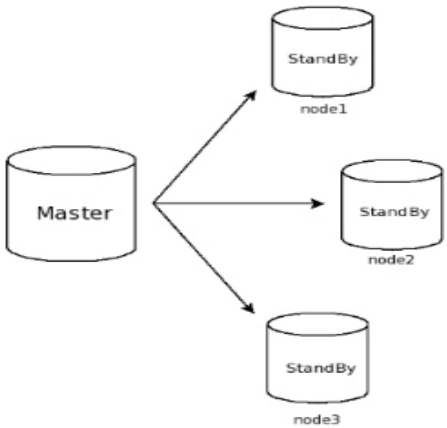
혼합결제시스템에서의 블록체인의 활용 방안을 설명하기에 앞서 지급결제시스템에 적용할 수 있는 블록체인, 즉 분산원장 기술(Distributed Ledger Technology:DLT)의 핵심 기술에 대한 정리가 필요하다고 판단하여 주요 기능을 중심으로 기술에 대한 설명을 덧붙이고자 한다. 분산원장 기술은 분산 데이터베이스, 암호화 해시함수, 공개키 암호화 기술, P2P 네트워크 프로토콜, 합의 알고리즘 등 다음의 5가지 주요 핵심 기능을 가지고 있다. 따라서 분산원장 기술을 적용한 시스템을 설계하기 위해서는 위에서 언급한 5가지 기능을 우선적으로 고려하여야 한다.

(1) 분산 데이터베이스

우선 블록체인의 기본적 구조인 분산 데이터베이스(distributed database)를 설명한다. 분산 데이터베이스란 네트워크상에서 다수의 저장 공간에 데이터를 분산 저장하는 데이터베이스를 의미한다. 이에 바탕이 되는 시스템은 통합 분산 데이터베이스 관리 시스템(distributed database management system, 이하 DDBMS)인데, DDBMS는 사용자로 하여금 모든 데이터가 한곳에 저장된 것처럼 보일 수 있도록 데이터를 관리한다. 즉, DDBMS는 특정 데이터베이스에서 데이터가 저장, 변경, 삭제될 때, 자동으로 혹은 주기적으로 모든 데이터베이스의 데이터를 동기화하는 시스템을 의미한다.

아래의 그림은 분산데이터베이스의 예를 보여준다. 분산데이터베이스의 목적은 데이터 처리의 지역화, 데이터 운영 및 관리의 지역화, 데이터 처리부하의 분산 및 병렬 데이터 처리 및 데이터의 가용도와 신뢰성 향상이다. 분산 데이터베이스 기술은 네트워크의 성능 향상에 따라 빅데이터 처리에 주로 사용되고 Master/Standby 형태를 가진다.

<그림 3-1> 분산데이터베이스의 예시 (Master/Standby 형태)



하지만 본 연구에서 제안하는 한국은행 지급결제시스템에서 사용되는 분산데이터베이스는 통합관리시스템이 존재하지 않는다. 즉, 분산 데이터베이스를 가지고 있는 사용자가 데이터에 대한 저장 요청을 받게 되면 정해진 규칙에 따라 데이터의 정합성을 스스로 판단하고 기록하는 역할을 수행한다. 또한, 분산원장의 분산 데이터베이스는 저장은 가능하지만 변경, 삭제가 원천적으로 불가능한 비가역성(irreversibility)을 주요 특징으로 한다. 아래의 그림과 같이 모든 데이터베이스는 모두 Read/Write를 지원하는 동등한 레벨로 유지된다.

<그림 3-2> 동등한 레벨의 데이터베이스 유형

(2) 암호화 해시 함수

암호화 해시 함수(cryptographic hash function)는 해시 함수의 일종으로, 만들어진 해시 값으로부터 원래의 입력 값과의 관계를 찾기 어려운 성질을 가지는 경우를 의미한다. 암호화 해시 함수가 가져야 하는 성질은 다음과 같다.

첫 번째는 역상 저항성(preimage resistance)이다. 역상 저항성은 만들어진 해시값을 가지고 그 해시값을 생성하는 입력값을 찾는 것이 계산상 불가능함을 의미한다. 입력값을 통해 해시값을 생성하지만 해시값을 통해서는 입력값을 찾는 것이 불가능한 일방향함수의 특성을 가지고 있다.

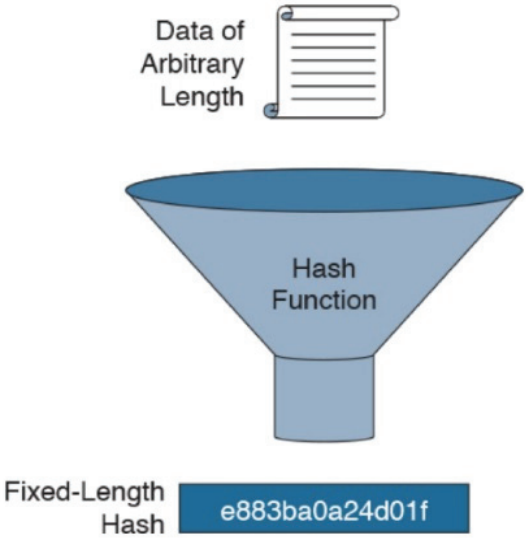
두 번째는 제2역상 저항성(second preimage resistance)이다. 제2역상 저항성은 해시값을 생성하는 입력값에 대해서, 그 입력의 해시값을 바꾸지 않은 상태로 입력값을 변경하는 것이 계산상 불가능함을 의미한다.

세 번째는 충돌 저항성(collision resistance)이다. 충돌 저항성은 같은 해시값을 생성하는 다른 두 개의 입력값을 찾기가 계산상 불가능함을 의미한다.

즉, 암호화 해시 함수는 수학적으로 해시값을 변경하지 않은 상태로 입력값을 수정하는 공격이 불가능하기 때문에 안전하며, 결국 이러한 성질을 가지는 해시값은 원래 입력값이 의도적으로 손상되지 않았는지에 대한 검증 장치로 사용할 수 있다. 해시함수는 가상화폐 시스템에서 폭넓게 사용되고 있

다. 검증노드(validator)는 거래내역과 해시함수에 의해 생성된 축약값(digest)을 비교하여 자신이 저장하고 있는 데이터와 다른 저장소에 있는 값들이 정확하게 일치하는지를 빠른 속도로 확인할 수 있다. 아래 그림은 해시 함수의 동작 예를 나타낸 것으로 임의의 크기의 데이터가 입력으로 사용되고, 출력으로는 선택한 해시 함수의 종류에 따라 동일한 크기의 값이 나오게 된다.

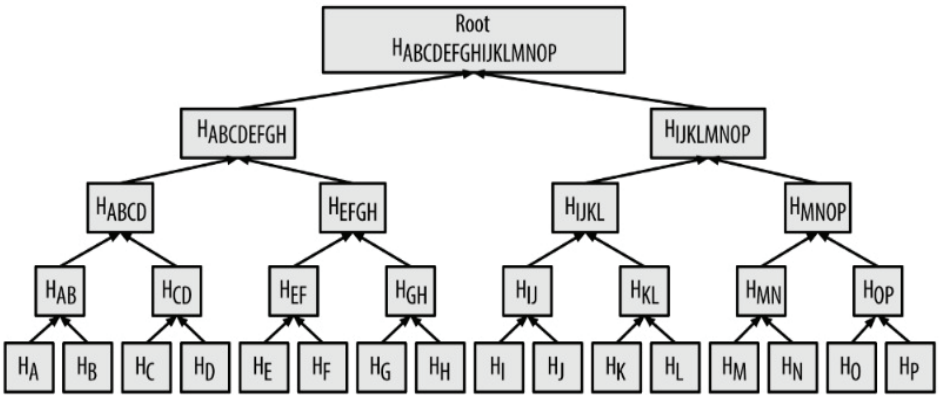
<그림 3-3> 해시함수 동작 원리도



제안하는 지급결제시스템에서는 원래의 데이터를 하나하나 비교하지 않고도 데이터의 무결성을 빠른 시간에 확인할 수 있도록 머클 트리(Merkle Tree) 방식을 사용한다. 2장에서도 간략하게 설명한 머클 트리는 이진 해시 트리(binary hash tree)라고도 하는데, 규모가 큰 데이터 집합의 완전성을 효율적으로 요약하고 검증하는 데 사용되는 데이터 구조로서, 암호 해시를 담고 있는 이진 트리다. 머클 트리는 블록 내에 있는 모든 거래를 요약하기 위해 사용되며, 거래의 집합 전체에 대한 디지털 지문을 만들어내고, 특정 거래가 블록 내부에 포함되는지 여부를 검증하는 데 매우 효율적인 프로세스를 제공한다. 루트 혹은 머클 루트(Merkle Root)라고 부르는 해시 하나가 남을 때까지 노드 쌍을 반복적으로 암호화해서 머클 트리를 만든다. 이렇게 생성된 머클 트리는 비트코인이나 이더리움 같은 개방형 블록체인에 기록되며, 허가된 요청에 따라 거래 내역의 묶음이 해당하는 시간에 해당 금액만큼 거래가 이루어졌다는 사실을 확인할 수 있으며, 지급결제시스템에 저장된 데이터의 무결성을 검증하는데 사용된다.

아래의 그림은 머클 트리의 16개의 입력 값으로부터 머클 루트를 생성하는 과정을 나타낸다. 그림에서 H는 해시 함수를 뜻하고, A~P는 해시 함수의 입력으로 사용된 값을 나타낸다.

<그림 3-4> 머클 트리의 구조도



자료: Mastering Bitcoin

(3) 공개키 암호화 방식

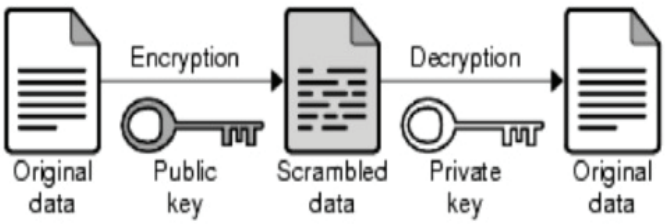
공개키 암호 방식은 암호 방식의 한 종류로, 사전에 비밀키를 나눠가지지 않은 사용자들이 안전하게 통신할 수 있도록 하는 기술이다. 공개키 암호 방식에서는 공개키(Public Key)와 비밀키(Private Key)가 존재하며, 공개키는 누구나 알 수 있지만 그에 대응하는 비밀키는 해당 키의 소유자만이 알 수 있어야 한다. 공개키는 은행의 계좌번호에, 비밀키는 비밀 PIN번호에 대입해서 생각하면 유사한 개념이다. 공개키 암호를 구성하는 알고리즘은 비대칭 암호라고 부르기도 한다. 공개키 암호 기술은 크게 두 가지 종류로 나눌 수 있다.

첫 번째는 공개키 암호이다. 공개키 암호는 특정한 비밀키를 가지고 있는 사용자만 암호화된 내용을 복호화하고 원래 메시지를 읽어볼 수 있음을 의미한다.

두 번째는 공개키 서명이다. 공개키 서명은 해당 데이터가 특정한 비밀키로 만들었다는 것을 해당 공개키를 이용하면 누구나 확인할 수 있음을 의미한다.

아래의 그림은 공개키 암호화의 과정을 설명하는 도식이다. 최초의 데이터에 PKI의 공개키를 적용하여 암호화(encryption)하고 이렇게 생성된 암호화된 데이터(scrambled or encrypted data)는 해당 공개키에 상응하는 개인키로 복호화(decryption)하면 원본 데이터를 얻을 수 있게 된다.

<그림 3-5> 공개키 암호화의 과정



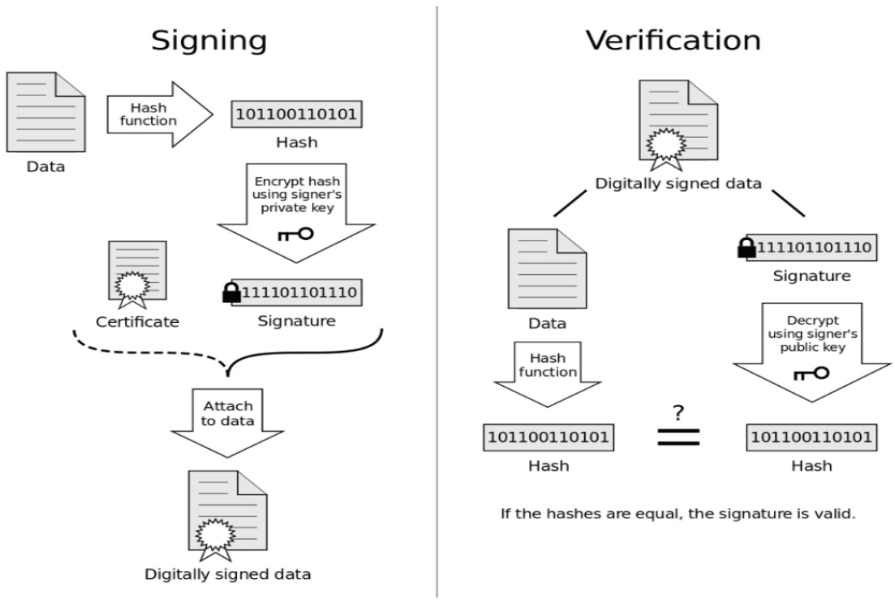
일반적으로 공개키 암호 방식은 비밀키 암호(혹은 대칭 암호)보다 계산이 복잡한 단점이 있기 때문에, 효율을 위해 비밀키 암호와 함께 사용된다. 메시지를 임의로 만들어진 비밀키를 이용해 암호화한 다음 이 비밀키를 다시 수신자의 공개키로 암호화하여 메시지와 함께 전송하는 것이다. 이렇게 하면 공개키 암호 기술로는 짧은 비밀키만을 암호화하고 보다 효율적인 비밀키 암호 기술로 전체 메시지를 암호화하므로 양쪽의 장점을 취할 수 있다.

제안하게 될 분산원장 기술 기반 지급결제시스템에서는 효율적인 공개키 암호 기술과 공개키 서명 기술을 모두 사용한다. 우선, 공개키 암호기술은 사용자의 거래를 기록할 때, 거래내역을 암호화하여 저장함으로써 거래에 참여한 사용자와 관리자만이 해당 내역을 읽어볼 수 있도록 한다. 공개키 서명 기술의 경우, 거래를 생성한 주체가 본인이 생성한 데이터가 변경되지 않았음을 증명하는데 사용되며 해당 거래를 생성할 권리(즉, 개인키의 보유여부)가 있음을 나타낸다. 아래의 그림은 전자서명의 과정을 나타내고 있다.

왼쪽의 서명(Signing) 과정을 살펴보면 다음과 같다. 우선 원본 데이터로부터 암호화 해시함수를 통하여 해시 값을 생성한다. 이후에 해시함수를 통해 생성된 해시 값을 서명인의 개인키를 이용하여 암호화(encryption)한다. 이렇게 암호화를 통해 만들어진 서명 값, 서명인의 공개키를 가지고 있는 인증서, 그리고 원본 데이터를 모두 포함하는 서명된 데이터(Digitally signed data)를 생성한다.

오른쪽은 서명된 데이터(Digitally signed data)를 통신채널로 전달받아 검증(Verification)하는 과정을 나타내고 있으며, 과정은 다음과 같다. 우선 서명된 데이터(Digitally signed data)로부터 서명 값, 인증서 및 원본데이터를 분리한다. 분리된 데이터들 중 원본 데이터로부터 해시 값을 생성하고, 인증서는 유효성을 확인한 이후 서명인의 공개키를 추출한다. 이후에 추출된 공개키를 이용하여 서명 값을 복호화(Decryption)하고, 복호화된 서명 값과 원본데이터의 해시 값을 비교하고, 두 값이 일치하면 검증이 완료된다.

<그림 3-6> 공개키 기술 전자서명의 과정



(4) P2P 네트워크 프로토콜

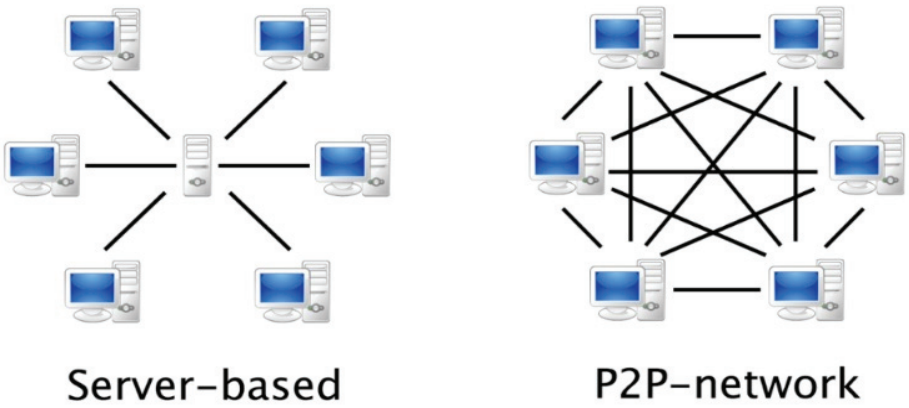
거의 모든 개방형 블록체인은 인터넷상에서 피어 투 피어(peer-to-peer) 네트워크 아키텍처 구조를 이루고 있다. 피어 투 피어, 즉 P2P라는 용어는 네트워크에 참여하는 개인은 서로에게 동료이며 모두 동등한 지위를 가지고 있고 '특별한' 노드는 존재하지 않으며 모든 노드가 네트워크 서비스를 공급하는 역할을 분담하는 것을 의미한다. 네트워크상의 여러 노드는 서로 '동등한' 토폴로지를 가지면서 그물망 네트워크에서 서로 연결되어 있으며, 네트워크 내에는 어떠한 서버나 중앙화된 서비스, 위계질서도 존재하지 않는다. P2P 네트워크의 노드는 서비스를 제공하고 동시에 서비스를 이용하는 공급

자이자 동시에 소비자의 역할을 한다. P2P 네트워크는 본질적으로 회복력이 있고 분산화되어 있으며 개방 체제다. P2P 네트워크 아키텍처의 좋은 예는 IP 네트워크상의 노드들이 모두 동등했던 초기 인터넷에서 찾아볼 수 있다. 오늘날의 인터넷 아키텍처는 초기보다는 계층적이지만 인터넷 프로토콜은 여전히 동등한 토폴로지를 유지한다. 비트코인을 제외하고 P2P 기술을 가장 광범위하게 성공시킨 사례는 파일 공유의 선구자이자 비트토렌트(BitTorrent)의 전신인 냅스터(Napster)다.

아래의 그림은 클라이언트-서버 구조의 네트워크와 P2P 네트워크를 비교한 그림이다. 웹 시스템도 확장된 '클라이언트 서버 시스템'으로 분류되나, 일반적으로는 클라이언트-서버 시스템이라고 하면, 사용자 PC에는 클라이언트가 설치되어 화면을 처리하고 서버에서는 자료를 처리하는 시스템을 일컫는다. 서버(Server)란 서비스를 제공하는 컴퓨터이며, 다수의 클라이언트를 위해 존재하기 때문에 일반적으로 매우 큰 용량과 성능을 가지고 있었다. 가장 대표적인 예로 월드와이드웹(www)를 들 수 있다.

반면에 P2P 네트워크는 망 구성에 참여하는 기계들의 계산과 대역폭(bandwidth) 성능에 의존하여 구성되는 통신망을 뜻한다. P2P 네트워크는 오디오나 비디오, 데이터 등 임의의 디지털 형식 파일의 공유에 사용되는 것이 매우 보편적이다. 또한, 인터넷 전화(VoIP)같은 실시간 데이터 등도 P2P 기술을 통해 서로 전달될 수 있다.

<그림 3-7> 클라이언트-서버 구조와 P2P 구조의 비교



한편, 블록체인의 P2P 네트워크 아키텍처는 토폴로지의 선택 그 이상을 의미한다. 블록체인 설계의 주요 원리는 분산화된 통제이며, 이는 동등하고 분산화된 P2P 합의 네트워크 상에서만 시행 및 유지될 수 있다. '블록체인 네트워크'라는 용어는 P2P 프로토콜을 실행하는 노드의 집합을 말한다.

본 연구에서 제안하는 지급결제시스템에서는 다수의 거래장부가 존재하며 이를 관리하는 관리자 모듈이 존재한다. 이 관리자 모듈은 거래장부와의 모든 상호작용을 관리 총괄하며 다른 관리자 모듈과의 P2P 통신을 지원하는 역할을 수행한다.

(5) 합의 알고리즘

분산 데이터베이스에 동일한 내용을 기록하기 위해서는 합의 알고리즘이 사용되어야 한다. 합의 알고리즘과 접근 제어는 분산원장의 목적에 따라 다양한 방법들이 사용될 수 있다. 개방형 블록체인 네트워크의 접근제어가 불가능하기 때문에 악의적인 참여자를 배제할 수 없다. 그러므로 데이터 조작에 대한 안전하고 강력한 방어책이 필요하며 작업증명(Proof-of-Work)이나 유사한 방법들을 합의 알고리즘으로 사용하는 방법이 합리적이다. 폐쇄형 블록체인의 경우에는 장부의 접근 권한을 오직 신뢰할 수 있는 사용자에게만 부여하기 때문에, 다량의 정보를 PBFT(Practical Byzantine Fault Tolerance) 같은 효율적인 합의 알고리즘을 이용하여 안전하게 저장 관리하는 것이 가능하다.

PBFT에서 사용되는 노드는 다음의 세 가지다. 첫 번째는 리더노드이다. 리더노드는 비트코인 블록체인의 채굴자와 같은 역할을 하는 노드로 새로운 블록을 만들고 네트워크에 전파하는 기능을 수행한다. 리더노드의 선정은 round robin이나 contention-based의 다양한 방식을 사용할 수 있다.

두 번째는 검증노드이다. 검증노드는 개방형 블록체인의 풀노드(Full Node)에 해당하며 모든 블록체인에 저장된 데이터를 로컬에서 검증하는 것이 가능하며 리더노드로부터 전달받은 블록의 유효성을 판단하여 리더노드에게 응답하는 기능을 수행한다.

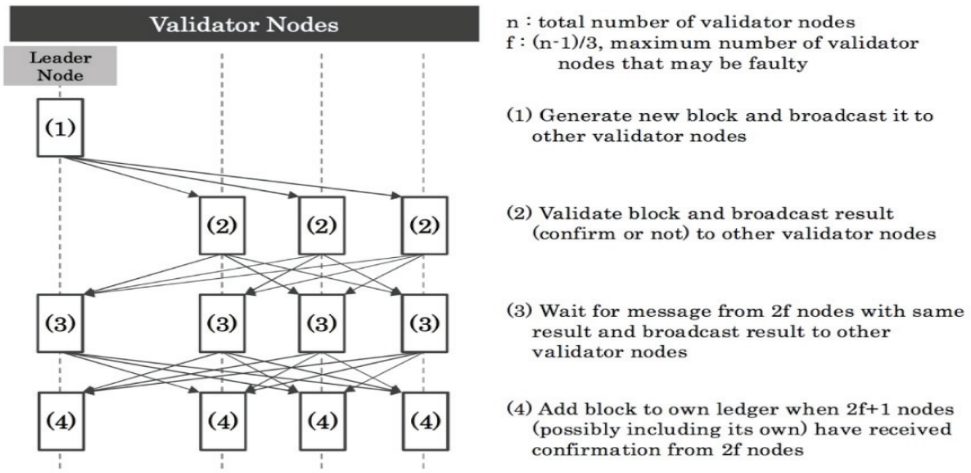
세 번째는 비검증노드이다. 비검증노드는 개방형 블록체인의 SPV(Simple Payment Verification) 노드에 해당하며, 전체 블록체인을 저장하고 있지는 않지만 하나의 거래를 생성하는 것이 가능하며 검증노드의 도움을 받으면 각각의 거래를 검증하는 것도 가능하다.

PBFT 기반 알고리즘은 약 참여노드의 2/3이상이 거래 내역들을 검증하게 되면 합의에 이르게 된다. 이는 안전하며 안정된 즉각적인 합의를 가능하게 하기 때문에, 블록체인의 분기를 막는 것이 가능하다. PBFT기반 알고리즘에서 검증노드는 장부에 거래 내역을 기록하고 합의과정에 참여하는 기능을 하고 있다. 반면에 검증 기능이 없는 노드는 거래를 만드는 데는 참여하지만 합의과정에는 참여할 권한을 가지지 못한다.

아래의 그림은 PBFT의 합의과정을 나타내고 있다. 비잔티움 장애 허용(Byzantine Fault Tolerance)은 두 장군 문제(Two Generals Problem)를 일반화한 문제인 비잔티움 장군 문제(Byzantine Generals Problem, 이하 BGP)로부터 파생된 장애 허용 분야 연구의 한 갈래다. BGP는 레슬리 램포트와 쇼스탁, 피스가 공저한 1982년 논문에서 처음 언급됐다. 이 논문에서 저자들은 적군의 도시를 공격하려는 비잔티움 제국군의 여러 부대가 지리적으로 떨어진 상태에서 각 부대의 지휘관들이 전령을 통해 교신하면서 공격 계획을 함께 세우는 상황을 가정하고 있다. 이 부대의 지휘관 중 일부에는 배신자가 섞여있을 가능성이 있고, 배신자는 규칙을 충실히 따르는 충직한 지휘관들과 달리 규칙에 얽매이지 않고 마음대로 행동할 수 있다. 이 때 배신자의 존재에도 불구하고 충직한 지휘관들이 동일한 공격 계획을 세우기 위해서는 충직한 지휘관들의 수가 얼마나 있어야 하며, 이 지휘관들이 어떤 규칙을 따라

교신해야 하는지에 대한 문제가 BGP이다.

<그림 3-8> PBFT 기반 합의 알고리즘

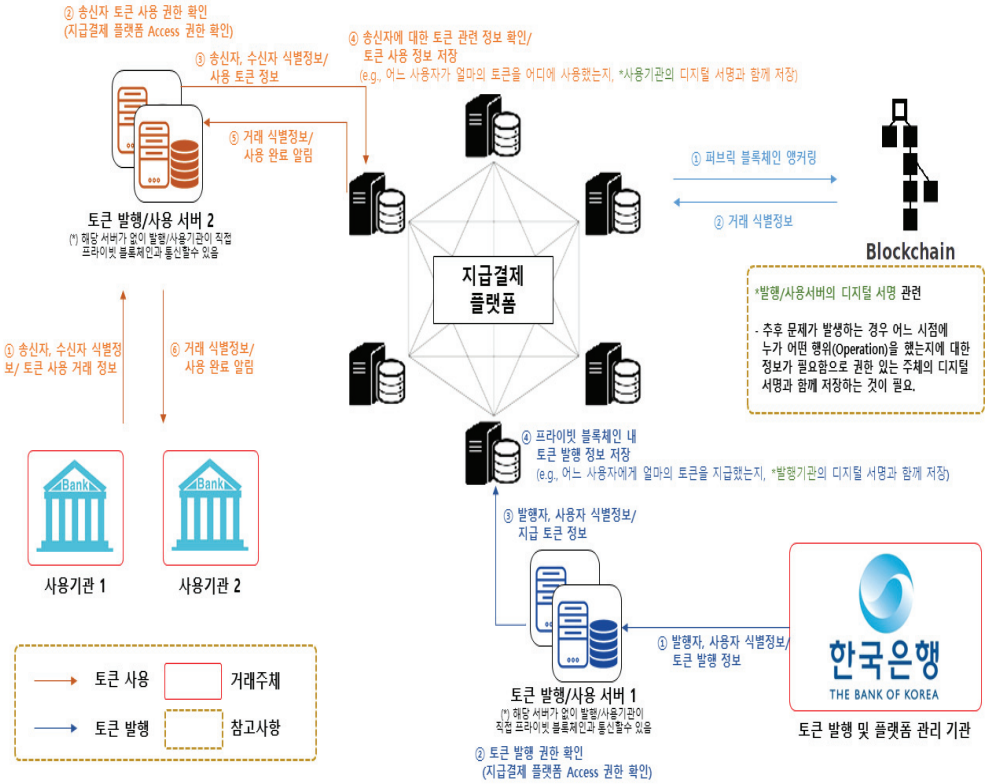


자료: JPX working paper

제안하는 지급결제시스템에서는 모든 금융기관이 검증노드가 될 필요는 없으며, 한국은행을 제외한 대부분의 금융기관은 검증기능을 보유하지 않는 노드이다. 검증노드의 숫자는 합의 알고리즘을 위한 메시지 트래픽 때문에 네트워크 대역폭에 영향을 준다. 그러므로 특정 금융기관만이 검증노드의 역할을 수행하게 된다. 합의과정에는 블록을 생성하는 리더노드가 존재해야하며, 리더노드가 메시지를 전파하면 이를 전송받은 검증노드는 정해진 규칙에 따라 메시지를 검증하고 유효하면 각각의 원장을 독립적으로 업데이트 하게 된다.

나. 블록체인의 적용 방법

<그림 3-9> 토큰 기반 블록체인 지급결제시스템 흐름도



자료: 코인플러그

위 그림은 혼합결제시스템을 블록체인 플랫폼을 이용하여 구성한 시스템의 기본적인 흐름도이다. 기본적으로 블록체인을 기반으로 하여 지급결제시스템 내에서 유통될 Digital 토큰(이하 토큰)을 발행하고 유통하는 형태로 지급결제시스템이 구성된다. 기본적인 흐름은 다음과 같다. 지급결제 플랫폼 내에서 사용하는 토큰을 권한 있는 발행자가 생성(토큰 생성 시에는 토큰 발행자의 전자서명을 포함)하고 인가받은 참여자들이 토큰의 거래(거래 시에는 참여자의 전자서명을 포함)를 폐쇄형 블록체인에 기록하고 거래 내역을 영구히 보존하는 방식이다.

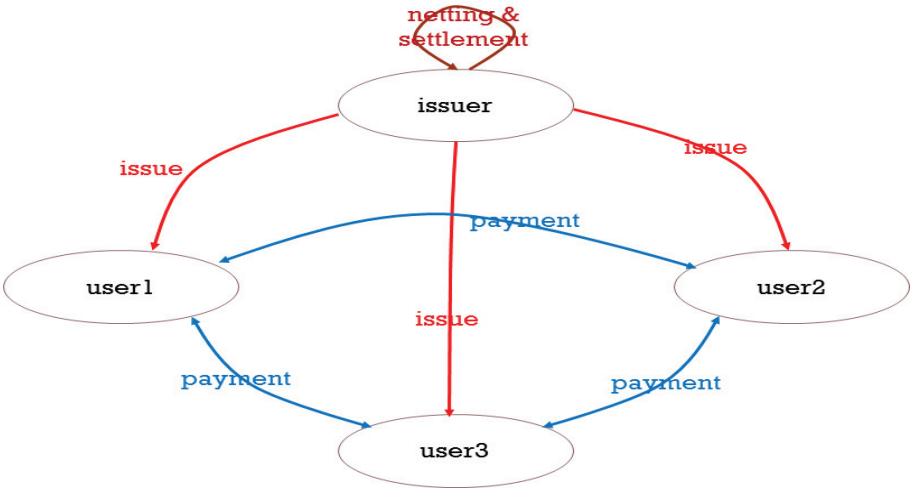
(1) 사용의 전제 조건

본 시스템을 사용하기 위한 전제조건은 다음과 같다. 첫째로는 토큰의 사용자들(금융기관)은 본인이 사용할 공개키(public key)를 사전에 지급결제시스템 블록체인 관리자(대부분의 경우 토큰 발행기관이 관리자의 역할을 함께 수행)에 등록하여야 한다. 이는 토큰 발행을 담당하게 될 발행기관, 즉 한국은행이 금융망에 참여하는 금융기관들의 모든 공개키를 관리하는 역할을 함께 수행하고 모든 거래 내역을 승인, 관리, 점검하는 역할을 수행하게 된다는 것을 의미한다.

둘째, 한국은행의 지급결제 플랫폼에 참여하는 모든 사용자들은 암호학적으로 유효한 공개키를 사용하여야 한다. 대표적인 방법으로는 RSA와 ECC 등의 기법이 있다

세 번째로는 지급결제시스템 플랫폼에서 생성되는 모든 거래는 유효한 서명(Signature)을 적어도 하나이상 포함하고 있어야 한다. 여러 참여자의 공개키들로부터 가공된 값을 사용하면 다중서명 방식을 적용할 수도 있다. 다중서명 방식은 n개의 공개키가 보관이 되어 있고, 하나의 거래를 만들기 위해서는 적어도 m개 이상의 개인키가 서명을 제공해야 한다는 조건을 설정하는 것이다. m-of-n 제도라고도 알려져 있는데, 예를 들어 2-of-3 다중서명이면 공개키 3개가 잠정적 서명자로 등록이 되어 있고 유효한 거래를 만들기 위해서는 적어도 2개의 개인키를 사용해야 하는 경우라고 설명할 수 있다. 다자간 거래 등에서 다중서명 방식이 적합하다고 판단될 경우 해당 기술의 적용 방안을 모색해 사용할 수 있을 것이다.

<그림 3-10> 토큰의 발행자와 사용자간의 블록체인의 구성도



자료: 코인플러그

위 그림은 지급결제시스템에 참여하는 토큰의 발행자와 사용자간에 발생할 수 있는 모든 이동을 간략하게 나타낸 구성도이다. 이는 토큰의 생성, 거래, 정산 등의 모든 과정을 포함한다. 지급결제시스템은 다음과 같은 특성을 가진다.

첫 번째로 모든 거래는 암호화되어 분산원장에 기록되어야 하며, 관리자의 역할을 하는 한국은행과 거래에 참여한 기관만 거래 내역을 읽어볼 수 있도록 구성한다.

두 번째로 결제의 유형은 현재 혼합결제시스템과 마찬가지로 신속결제와 보통결제로 구분된다. 신속결제는 사용자가 충분한 양과 한도의 토큰이 있을 경우 실시간으로 처리하며, 보통거래의 경우는 사용가능한 잔액에 상관없이 거래 요청을 각 금융기관의 대기 파일의 역할을 하는 임시 데이터베이스에 저장하고 상계처리가 가능할 때 혹은 정해진 시간에 처리한다.

세 번째로 모든 거래는 관리자 혹은 사용자의 유효한 전자서명을 포함하고 있기 때문에, 권한이 있는 제3의 감사자가 감사에 사용할 수 있는 근거 자료가 될 수 있다.

네 번째로는 사용자의 잔고는 결제가 완료된 후 항상 positive 값을 유지하

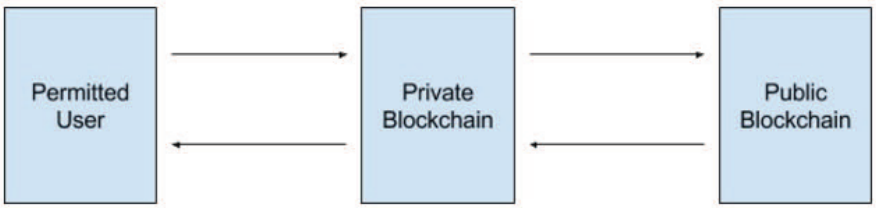
여야 한다. 거래가 완료된 이후에는 잔고가 마이너스로 표시될 수 없으며 각 사용자의 토큰 잔고는 항상 0 이상으로 유지되어야 한다.

(2) 금액의 예치

우선 블록체인 기반 혼합결제시스템의 사용자, 즉 참여 금융기관이 블록체인 기반의 지급결제시스템을 이용하기 위해서는 결제시스템에서 사용할 만큼의 금액을 예치해야 한다. 사용자가 시스템의 관리자, 즉 한국은행에 사용할 만큼의 금액을 예치하면 관리자는 예치한 금액에 따라 사용할 수 있는 토큰을 발행한다. 토큰의 발행은 오로지 시스템의 관리자인 한국은행만이 할 수 있으며, 토큰의 발행량은 예치 금액과 1:1 비율 혹은 다른 방법으로 시스템의 운영 방식과 활용 방안에 맞게끔 조정할 수 있다.

(3) 사용자 인가 및 등록 절차

<그림 3-11> 사용자 인가 및 등록 절차



모든 지급결제시스템 참여자(한국은행 금융망 참여 금융기관)는 블록체인 기반 지급결제시스템을 사용하기에 앞서, 본인을 인증하고 해당 시스템에서 사용할 공개키를 선 등록하여야 한다. 절차는 다음과 같다.

(가) 처음 참여하는 시스템 참여자 A(이하 User A)는 사용할 공개키 A와 개인키 A를 안전하게 로컬에서 생성한다.

(나) 공개키 A를 지급결제 블록체인 관리자(이하 Private BCM)에게 전송한다. 지급결제시스템에서는 한국은행이 Private BCM을 담당한다.

(다) 한국은행(Private BCM)은 User A가 유효하다고 판단되면 임의의 번호(Random Number, 이하 RN)를 생성하여 User A에게 전달한다. 이 때,

해당 User A의 유효성을 판단하는 방법은 여러 방법이 있는데 공인 인증서나 블록체인 인증서 등 PKI 기반 인증서를 사용할 수 있으며, 기타 참여자가 유효함을 증명하는 온오프라인의 어떠한 방법을 사용해도 무방하다.

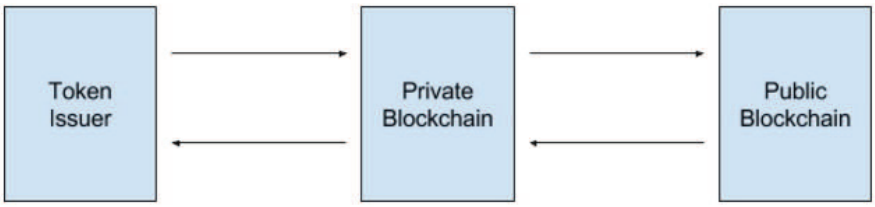
(라) User A는 발급받은 임의의 번호(RN)를 개인키 A로 전자서명을 하고 전자서명을 한 개인키의 결과값인 전자서명 A를 블록체인 관리자인 한국은행에 전달한다.

(마) 한국은행은 서명이 정상적으로 되었는지를 검증하고, 검증이 완료되면 해당 전자 서명값, RN, 공개키 A를 지급결제 블록체인 데이터베이스에 저장한다. 이후 한국은행은 해당 값들을 검색할 수 있는 거래 ID(이하 Txid A)를 User A에게 전달한다.

(바) 위의 절차가 완료되면 User A는 지급결제시스템의 사용자로의 등록이 완료된다.

(4) 토큰 발행 절차

<그림 3-12> 토큰 발행 절차



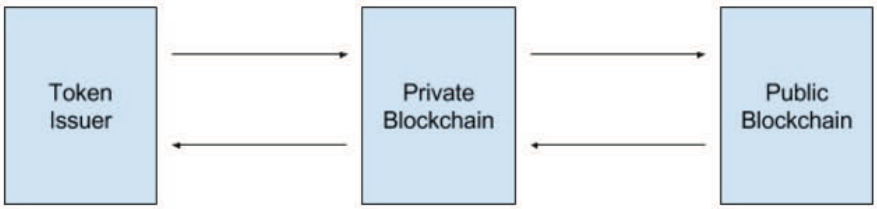
사용자의 등록이 정상적으로 완료되면, 해당 사용자는 지급 및 입금 채널을 통하여 예치금을 입금하고 이에 해당하는 토큰을 발급받게 된다. 토큰의 발급은 발급기관이 담당하게 되는데 지급결제시스템의 관리자(한국은행)가 전적으로 이를 담당한다. 우선 아래의 절차를 통하여 토큰이 발행된다.

(가) 토큰 발행기관인 한국은행은 토큰을 발행하기 위하여 토큰 발행 거래(Issuance Transaction)를 생성하고 지급결제 블록체인 관리자에 전송한다.

(나) 한국은행 내 블록체인 관리자(Private BCM)는 토큰 발행기관의 공개키를 이용하여 발행거래의 유효성을 검증한다. 발행거래가 유효하면 지급결제 블록체인 데이터베이스에 등록하고 블록체인 거래 ID를 토큰 발행기관과 사용자에게 전달한다. 만약 발행거래가 유효하지 않으면(e.g., 전자서명 검증 실패), Error message를 발행기관에 전달한다.

(5) 토큰 사용 절차

<그림 3-13> 토큰 사용 절차



정상적으로 토큰을 발급받은 사용자인 금융기관들은 서로의 전자서명을 사용하여 거래를 생성하고 토큰을 상호간에 전달할 수 있다.

(가) 우선 토큰 사용자들은 구매한 토큰을 사용하기 위하여, 지급 지시를 생성하고 지급결제 블록체인 관리자에게 전송한다.

(나) 지급결제 블록체인 관리자는 가지고 있는 사용자의 공개키를 통해 지급지시의 유효성(전자서명)을 검증한다.

(다) 지급지시가 유효하고 지급지시의 유형이 '신속'이고 토큰 잔액이나 한도가 충분하면, 블록체인 데이터베이스에 거래내역을 등록하고 PrivTxid를 거래에 참여한 모든 사용자에게 전달한다.

(라) 지급지시가 유효하고 지급지시 유형이 '보통'이거나 혹은 '신속'인데 잔액이나 한도가 충분하지 않다면 해당 거래를 대기 폴더의 역할을 하는 Netting DataBase(이하 NDB)에 등록하고 이후 상응하는 거래가 들어왔을 때 상계 처리 및 결제를 시도한다. 결제가 성공하면 관련 거래 내역들을 PrivBCDB에 등록하고 블록체인 거래 ID들을 거래에 참여한 사용자들에게 전달하고, NDB에 있던 거래항목들은 삭제한다.

(마) 지급지시가 서명 등의 문제로 유효하지 않으면, Error message를 거래를 생성한 사용자에게 전달한다.

3. 블록체인 도입의 조건 및 고려사항

가. 프라이버시 문제

가장 널리 사용되고 있는 개방형 블록체인인 비트코인의 경우, 익명성을 가진 ID들로 이루어진 모든 거래내역이 저장되어 있고 누구나 원하면 내용을 접근하여 읽어보는 것이 가능하다. 따라서 특정 ID에 얼마나 많은 비트코인이 할당되어 있는지 알아내는 것이 가능하다. 이렇듯 높은 투명성과 변조가 불가능한 장부의 기능은 개인의 소유권을 증명할 수 있는 비트코인의 분산 특성의 기본이 되고 있다. 하지만, 금융데이터를 직접 저장해야하는 지급결제시스템에서 거래금액과 참여금융기관들의 ID를 암호화하지 않고 저장하게 될 경우, 참여금융기관의 모든 거래내역이 블록체인에 접근할 수 있는 모든 노드에게 유출될 수 있다. 일반적인 금융거래에서 거래내역(거래 규모, 가격 등)은 관계된 금융기관이 아닌 상대에게 공개되지 않기 때문에, 개방형 블록체인 형태를 그대로 사용하는 것은 부적절하다.

하지만 모든 거래내역을 암호화할 경우, 관리자 노드(즉, 특수권한이 주어져 거래를 승인하는 등의 역할을 하는 노드, 지급결제시스템 블록체인에서는 한국은행이 그 역할을 한다) 또한 암호화된 데이터를 읽어볼 수 없게 된다는 문제점이 있다. 결국 상황과 필요에 따라 선택적인 거래 내역의 공개가 필요하다. 이에 대한 해결방안들이 몇 가지가 존재하는데 대표적인 방법은 다음의 두 가지 경우들이다.

(1) PKI based Key Exchange(e.g., Diffie-Hellman)

Diffie‐Hellman key exchange는 암호키를 교환하는 하나의 방법으로, 두 사람이 암호화되지 않은 통신망을 통해 공통의 비밀키를 공유할 수 있도록 한다. 휫필드 디피와 마틴 헬만이 1976년에 발표하였다. Diffie‐Hellman key exchange 방법은 암호키를 교환하는 하나의 방법으로, 두 사람이 암호화되지 않은 통신망을 통해 공통의 비밀키를 공유할 수 있도록 하는 기술이다. 이 방법을 사용하게 되면 거래에 관여하는 두 기관이 서로의 공개키만을 이용

하여 비밀키를 생성하는 것이 가능하다. 이후 두 거래자는 모든 거래 내역을 비밀키를 이용하여 암호화한 후에 전송하게 된다. 현재 제안하는 지급결제시스템에서는 토큰 발행자(한국은행)라는 Super Node가 존재하므로 두 거래자는 거래를 생성하기 전에 토큰 발행자의 공개키를 이용하여 두 당사자 간의 거래에 사용할 비밀키를 암호화하여 전송하면 토큰 발행자는 모든 거래당사자들의 비밀키를 획득하게 되고 이를 이용하여 거래내역을 살펴볼 수 있다.

송신자와 수신자가 공개된 통신망에서 Diffie - Hellman Key Exchange를 하기 위해서는 다음과 같은 절차를 거친다.

(가) n,g : 크기가 큰 정수들로서 메시지의 송수신에 참여하는 모든 사람들에게 공개되어 있다. 그리고 특히 g값은 n보다는 작고 1보다는 크다.

(나) 송신자는 비교적 크기가 큰 난수 x를 발생시키고 이 값을 보관한다.

(다) 수신자 역시 비교적 크기가 큰 난수 y를 발생시키고 이 값을 보관한다.

(라) 송신자는 다음의 계산을 하여 그 결과를 수신자에게 보낸다.

$$X = gx \bmod n$$

(마) 수신자는 다음의 계산을 하여 그 결과를 송신자에게 보낸다.

$$Y = gy \bmod n$$

(바) 송신자는 Y를 받아서 다음의 계산을 한 후 비밀키 Ks를 얻는다.

$$Ks = (Y)x \bmod n = gyx \bmod n$$

(사) 수신자는 X를 받아서 다음의 계산을 한 후 비밀키 Kr을 얻는다.

$$Kr = (X)y \bmod n = gxy \bmod n$$

위의 (바)와 (사)에서 계산된 결과인 Ks와 Kr이 같은 값을 갖는다는 것을 알 수 있다. 따라서 송신자와 수신자는 이 값을 비밀키로 하여 메시지를 암호화/복호화할 수 있게 된다.

(2) Confidential Transactions(e.g., hyperledger)

Confidential Transaction(이하 CT)은 Blockstream의 Sidechain에서 최초 적용한 방식으로 현재는 하이퍼레저의 기본 거래방식이다. CT를 사용하게 되면 거래 당사자들만이 거래량을 확인할 수 있으며, 개방형 블록체인의 UTXO(Unspent Transaction Output)과 같이 이중지불을 막을 수 있는 것이 가능하다. CT에서는 비밀 주소의 개념을 사용할 수도 있어서 거래당사자의 신원도 보호하는 것이 가능하다.

나. 권한 분리와 접근 제어

개방형 블록체인 네트워크는 모두에게 읽고 쓰기의 접근권한을 부여하고 있다. 하지만, 본 연구에서 제안하는 블록체인 기반 혼합결제시스템의 폐쇄형 블록체인은 인가된 사용자에게만 제한적으로 네트워크의 접근권한을 부여하게 된다. 본 보고서에서는 지급결제시스템의 사용 노드 권한을 다음의 두 가지로 구분한다.

(1) 토큰 발행자 (토큰 Issuer)

제안하는 블록체인 시스템에서 사용되는 모든 토큰 및 참여기관의 등록/파기를 관리하는 슈퍼 노드(Super Node)로서 사용자들에게 읽고 쓰는 권한을 부여할 수 있으며, 등록된 토큰 사용자에게 새로운 토큰을 발행할 수 있다(한국은행 담당). 토큰 발행자는 모든 거래내역을 읽을 수 있는 권한을 가지고 있으나, 블록체인의 특성상 거래가 승인되어 블록체인에 기록된 거래내역을 변경하는 것은 원천적으로 불가능하다. 또한, 제안하는 블록체인의 주요 서비스 중 하나로 장부에 기록되어 있는 거래내역이 생성 후에 변경되지 않았음을 확인 가능하게 해주는 감사기능이 제공되는데 이를 통해 필요한 감사정보를 인가된 제3자에게 제공할 수 있다.

(2) 토큰 사용자(토큰 User)

토큰 사용자(토큰 User)는 토큰 발행자로부터 발급받은 토큰을 타 사용자에게 이동하기 위해서, 발행자에게 사전에 등록한 공개키와 연동되어 있는 개인키로 전자서명을 하여 거래를 생성할 수 있는 권한이 있으며, 거래장부에

서 본인의 거래와 관련된 내역은 항시 읽어볼 수 있는 권한이 있다. 한국은행을 제외한 혼합결제시스템에 참여하는 대부분의 금융기관은 토큰 사용자 노드들이라고 할 수 있다.

다. 개방형 블록체인과의 연결(앵커링)

앞에서 언급했듯이 폐쇄형 블록체인에는 채굴이라는 개념이 존재하지 않는다. 이는 빠르게 합의에 이를 수 있는 좋은 방안이기도 하지만 악의적인 블록체인 관리자가 존재한다면 분산장부의 무결성을 증명하는 것이 불가능하다. 이러한 이유로 보고서에서 제안하는 지급결제시스템은 개방형 블록체인과의 연결을 주기적으로 실시하는 구조를 선택적으로 가질 수 있다. 즉, 한국은행 블록체인의 분산장부에 기록되는 내용을 가공하여(즉, 프라이빗 분산원장의 내용을 전혀 노출시키지 않는 방법으로) 머클트리를 블록별로 생성하고 머클트리의 최종값인 머클루트를 개방형 블록체인에 기록한다. 이를 통해 개방형 블록체인을 최소한으로 이용하면서도 개방형 블록체인의 채굴파워를 이용하여 한국은행의 폐쇄형 블록체인의 무결성을 유지할 수 있게 된다. 개방형 블록체인을 이용하여 폐쇄형 블록체인의 데이터를 가공하여 기록하는 방법인 앵커링을 통해 폐쇄형 블록체인의 무결성을 증명하고 신뢰를 제고할 수 있다.

라. 기술 관련 리스크

(1) 블록체인의 확장성

우선 블록체인의 처리 가능한 거래량이 현재 신한은금융망 등에서 금융기관의 실제 거래 규모를 처리할 수 있을 만큼 충분한지 고려해야 한다. 현재 코인플러그가 출시한 폐쇄형 블록체인인 FIDO Ledger를 예를 들어 보면, FIDO Ledger는 3000TPS(Transactions per second)의 데이터 처리량을 가지고 있기 때문에, 현재 신한은금융망의 거래 규모를 고려했을 때 FIDO Ledger를 포함한 다른 폐쇄형 블록체인을 적용하는 것 자체에는 큰 문제는 없을 것으로 보인다. 하지만 현재까지 지급결제시스템에 블록체인 기술을 상용화한 사례가 많지 않고, 시간별 거래 건수의 편차나 참여하는 기관이 다양해지고 결제의 종류도 다양해지는 등 추가적인 변수가 다수 존재한다는 점을 고려할 필요가 있다. 그렇기 때문에 폐쇄형 블록체인의 확장성에 대한 지

속적인 연구와 개발이 필요할 것으로 보이며, 중앙은행과 금융기관들도 계속적인 테스트를 통해서 어느 정도의 폐쇄형 블록체인의 개발이 필요한지 확인할 필요가 있을 것이다.

(2) 데이터의 감시 및 통제 방법

한국은행 블록체인에 참여하는 모든 토큰 사용자 노드들(토큰 User)은 토큰 발행자 노드(토큰 Issuer, 한국은행)로부터 읽고 쓰는 권한에 대해서 엄격하게 접근통제를 받게 되어 있다(Ⅲ-3-나. 권한 분리와 접근 제어 참조). 또한 토큰 Issuer는 개방형 블록체인과의 연결을 통하여 데이터의 감사요청이 발생할 때, 데이터가 생성시점부터 변조되지 않았음을 증명할 수 있다.

(3) 보안상의 리스크

폐쇄형 블록체인에 사용하는 PBFT 합의 알고리즘은 2/3이상이 합의할 경우에만 데이터의 기록이 가능하다. 그러므로 악의적인 검증노드가 1/3이상이 존재한다면 유효한 데이터를 기록하는 것이 불가능하다. 이는 개방형 블록체인의 51% 공격과 유사하지만, 폐쇄형 블록체인은 허가받지 않은 노드들의 참여가 원천적으로 불가능하기 때문에 1/3이상의 검증노드가 악의적으로 동작할 가능성은 매우 낮다. 하지만 이같은 한계를 고려하여 접근제어의 명확한 룰과 적용이 필수적이며, 토큰 발행자의 책임 하에 운영되어야 한다.

한편, 폐쇄형 블록체인에는 채굴이라는 방식이 존재하지 않기 때문에 장부의 데이터를 변경시키는 공격에 대비하여 다량의 연산자원을 투입하지 않아도 블록체인을 운영할 수 있다. 하지만 이에 따라 폐쇄형 블록체인은 보안상의 공격에 대하여 근본적인 한계를 가지며 이를 극복하기 위해서는 개방형 블록체인과의 앵커링을 주기적으로 실시하고 제3자가 항시 감사에 참여하는 방안을 이용할 수 있다.

마. 민간 분산원장 시스템과의 권한 구분

현재 블록체인의 개발 진행은 구체적인 활용법을 찾기 위한 초기 단계로서, 대부분의 경우 블록체인 기술을 가지고 있는 다양한 민간 기관들이 블록체인을 연구하며 활용 방안을 찾고 기업들 간의 협업을 통해 블록체인 활용에

대한 테스트를 진행하고 있다. 앞에서 언급했던 블록체인 기반 컨소시엄인 R3CEV나 하이퍼레저 프로젝트 등은 기업들 간의 공동 연구를 통해 개발 및 운영되고 있는 민간 분산원장 컨소시엄이며 리플 등의 블록체인 프로토콜도 금융기관에서 송금 및 결제 플랫폼으로 관심을 보이며 여러 협업들을 진행하고 있다. 또한 IBM과 마이크로소프트 등의 IT 기업들도 각자의 블록체인을 개발하며 활용 방안에 대한 연구를 진행하고 있다. 국내에서는 블록체인 기업인 코인플러그(Coinplug)가 기업용 폐쇄형 블록체인인 FIDO Ledger를 개발하여 금융기관들의 관심을 받고 있다.

현재 단계에서 중앙은행 혹은 공공 기관이 자체적으로 블록체인 기술을 개발하는 데는 많은 어려움이 있다. 자본의 투입과 기술적 노하우가 필요한 블록체인 개발에는 많은 시간과 비용의 투입이 불가피하고, 더욱이 아직까지 어느 중앙은행 혹은 공공 기관이 블록체인 상용화를 한 사례는 많지 않다. 그렇기 때문에 우선 블록체인 기술을 연구 및 도입하고자 하는 공공 기관은 어떤 식으로든 민간 기관의 도움이 불가피하며 블록체인 기술을 보유하고 있는 민간 기관과의 협업을 통해 블록체인의 활용 가능 분야 및 구체적 활용 방안에 대해 연구를 하고, 그와 동시에 이후 블록체인 개발 및 활용을 어떻게 할지, 민간기관의 도움을 받거나 민간 기관이 운영하는 블록체인을 활용한다면 권한 설정을 어떻게 할 것인가 등의 논의도 이루어져야 할 것이다. 영란은행의 디지털 화폐 연구도 대학 교수들과 함께 진행하고 있으며 싱가포르의 공공기관의 경우 IBM과 함께 여러 분야에서 함께 블록체인의 활용 방안을 연구 중이다.

이렇듯 현재 블록체인 도입 과정에서 자체적인 블록체인 개발이 어려운 상황임을 고려할 때 민간 혹은 타 기관의 분산원장 시스템 도입이 불가피하며, 그렇기 때문에 분산원장을 도입할 때 블록체인 기관과 중앙은행의 역할 분담을 어떻게 할지, 어떻게 단계를 설정해서 분산원장을 도입할지 등을 검토할 필요가 있다. 단기적으로는 시스템에 대한 운영은 한국은행이 맡아서 하되, 시스템에 대한 관리나 개발은 블록체인을 개발하는 기관이 담당하고 장기적으로는 한국은행이 모든 시스템을 전담해서 관리할지, 계속해서 민간 기관이 개입할지, 개입을 한다면 어느 분야까지 개입을 할지에 대한 논의가 필요할 것으로 보인다.

4. 블록체인 도입의 기대효과

현재까지 지급결제 분야에서 블록체인 도입에 대한 구체적 사례가 많지 않기 때문에 비용 등의 측면에 있어서 직접적인 비교는 어려운 점이 있다. 하지만, 현재까지 블록체인이 가지고 있는 보안성, 실시간 결제, 확장성 있는 플랫폼 등의 장점은 여러 연구를 통해 이미 검증이 되었으며 현재의 지급결제시스템을 개선할 수 있는 가능성이 있는 데이터베이스 플랫폼이라는 것은 분명한 사실이다. 많은 금융기관과 중앙은행이 블록체인 기반의 지급결제시스템의 연구에 착수하고 있고 높은 활용도를 가지고 있다는 것이 분명하다면 중앙은행 시스템에 대한 테스트 환경을 마련하여 선제적으로 실험을 해보고 활용방안을 찾을 필요가 있을 것으로 보인다.

가. 보안적으로 갖추어진 데이터베이스 플랫폼

블록체인은 중앙화된 시스템의 보안 이슈를 보완할 수 있는 데이터베이스 플랫폼으로 기능할 수 있다. 우선 블록체인은 단일 공격점이 없기 때문에 외부의 공격으로부터 더 안전하다는 장점을 가지고 있다. 외부의 공격을 통해 하나의 노드가 손상을 입더라도 블록체인의 동기화 과정을 통해 다른 노드들이 쉽게 문제를 파악할 수 있고, 다른 노드들에는 원 데이터가 남아있기 때문에 빠르고 쉽게 자료를 복구할 수 있다. 이는 내부의 공격에 있어서도 적용된다. 내부에서 거래 내역의 위변조를 시도하게 되면 블록체인의 분산화된 네트워크를 통해 데이터를 실시간으로 검증할 수 있다. 또한 모든 거래 내역은 블록의 형태로 연결이 되어 있고 블록은 해시값을 부여받게 되는데 해당 해시값은 이전 블록과 현재 블록을 근거로 만들어진다. 결국 하나의 거래 내역을 조작하기 위해서는 이와 연결되어 있는 모든 거래 내역들을 위변조 해야 하기 때문에 위변조를 성공하기 어려우며 공격 시도도 바로 확인하여 검증할 수 있는 구조를 가지고 있다.

또한 블록체인은 거래 과정에서도 암호화 서명을 통해 위변조의 위험을 방지한다. 블록체인 내에서는 거래의 당사자의 서명이 있어야만 거래가 공식적으로 승인되는 구조를 가지고 있다. 혼합결제시스템에 적용될 블록체인의 경우 거래를 하는 두 당사자의 서명과 한국은행의 사인이 거래에 포함되어야 정식적으로 거래를 인정받고 블록에 등록될 수 있기 때문에, 거래와 상관없는 주체가 거래를 방해하는 경우를 방지할 수 있다.

나. 타 시스템으로의 확장성 있는 플랫폼

블록체인 플랫폼이 새로운 시스템으로 각광을 받고 있는 데에는 거래 내역의 투명성, 거래의 안전성, 분산 네트워크를 통한 신속성 등 기능적으로 가지고 있는 여러 장점들이 있지만 특히 블록체인이라는 하나의 플랫폼을 통해 여러 서비스를 만들어 낼 수 있다는 서비스 상의 확장성이 주된 장점으로 알려져 있다. 1장에서 나온 여러 연구 사례들에서 알 수 있듯이, 많은 분야에서 블록체인이 갓 도입을 시작했거나 실험과 연구, 테스트 위주의 초기 단계임에 불과하지만, 인증, 기록, 결제 및 청산, 송금, 스마트 계약, 투표, 가상화폐 등 다양한 분야에서 이를 응용하기 위한 연구가 진행중이다. 블록체인으로 무엇이든 할 수 있다고 말할 수는 없겠지만, 기존에 전체적인 사업의 프로세스가 여러 절차 혹은 여러 기업 등으로 쪼개져 있고 이로 인해 시간적, 비용적 비효율성이 심각한 사업 분야의 경우, 분산화된 네트워크를 통해 프로세스를 간소화하고 시간적, 비용적 절감을 구현할 수 있다. 이를 바탕으로 여러 서비스를 붙여 해당 분야의 서비스를 통합해서 제공할 수 있는 플랫폼으로 활용될 가능성도 있다.

또 하나의 장점은 단순히 여러 분야에서 사용할 수 있고 여러 서비스를 만들 수 있는 것 뿐 아니라, 만들어진 서비스들을 하나의 블록체인 기술을 기반으로 서로 연동할 수 있다는 점이다. 블록체인은 기본적으로 분산형 네트워크로 구성되어 있고 각 금융망들이 하나의 큰 노드 역할을 수행하여 서로 다른 분야의 시스템이 연동할 수 있는 블록체인 네트워크를 만들 수 있다. 현재 한국은행에는 이번에 보고서에서 적용한 혼합결제시스템뿐만 아니라 총액결제, 소액결제, 증권결제 등 다른 지급결제시스템이 운영되고 있고 외환전산망, 국고전산망 등 한국은행 내에서 다른 기능을 담당하는 전산망들도 존재한다. 현재에도 각 금융망들이 서로 연동될 수는 있으나 근본적으로 각각의 목적으로 만들어진 분리된 망이기 때문에 시스템 연동에 있어서 개선이 필요하며 보안, 관리 등에도 각각의 비용이 소요된다. 반면, 블록체인 플랫폼은 하나의 플랫폼으로 실시간으로 다수의 서비스를 동기화할 수 있어 서비스의 이용과 보안상의 비용 절감을 할 수 있다는 장점을 가진다.

다. 결론

블록체인을 기반으로 하는 지급결제시스템은 실시간 데이터의 동기화를 통해 실시간 결제 및 청산이 가능하며 분산 네트워크와 암호 알고리즘을 통해 보안적으로 안전한 네트워크를 구성할 수 있다. 또한 하나의 플랫폼으로 여러 서비스를 연동하여 사용할 수 있다는 플랫폼 확장성을 가지고 있기 때문에 세계 각국의 금융기관과 은행에서 블록체인 기반 결제 시스템 플랫폼을 개발하며 도입을 준비 중에 있다. 하지만, 현재까지는 시스템의 전환 비용이나 신기술에 대한 적용 방안 문제 등 활용시 고려해야 할 사항들이 존재하기 때문에 중앙은행의 지급결제시스템 및 금융망의 블록체인 적용 방안에 대한 지속적이고 적극적인 연구 및 개발과 함께 적용을 위한 단계적인 접근이 필요할 것으로 보인다.

Ⅳ. 블록체인 기반 디지털 통화의 가능성

1. 블록체인 기반 디지털 통화 개발 현황

가. 현금 없는 사회의 도입

현재 세계적으로 '현금 없는 사회'에 대한 논의가 증가하고 있다. 2030년까지 현금 없는 사회를 목표로 했으나 오히려 속도를 늦춰야 할 필요성을 느낀다는 스웨덴의 경우나 상점에서 현금을 합법적으로 거부할 수 있는 덴마크 등의 북유럽의 예시는 이미 많이 알려진 사례이다. 대한민국 또한 '현금 없는 사회'에 대한 논의를 진행하고 있는데, 점진적인 연착륙을 위해 우선적으로 2020년을 목표로 '동전 없는 사회'를 준비하고 있다. 대한민국을 포함한 많은 국가들이 현금 없는 사회에 대한 논의를 본격적으로 시작하고 있는 첫 번째 이유는 현행 현금 유통 시스템의 문제점을 개선하기 위함이고 두 번째 이유는 그 문제점을 개선할 수 있을 정도의 기술적 발전이 이루어지고 있기 때문이다.

현금 없는 사회를 도입하고자 하는 첫 번째 이유는 현행 현금 시스템이 가지고 있는 발행, 관리, 유지상의 비효율성 때문이다. 현금의 경우 절도와 분실 및 손실 등 실물 화폐로서 가질 수 있는 위험으로부터 자유롭지 못하다. 노르웨이 중앙은행의 연구에 따르면, 현금 거래에 소요되는 건당 비용은 카드를 이용했을 때 보다 약 73%가 높으며, 미국의 경우 ATM 사용료, 도난, 인쇄 비용 등 현금 발행, 사용 및 관리를 위해 민간과 정부가 부담하는 비용이 미국 GDP의 1.2%에 육박할 것으로 보인다.[175]

특히 가장 큰 문제를 유발하는 것은 현금 중에서도 동전과 고액권인데, 동전은 발행과 유통의 어려움, 고액권은 지하경제로 인한 유통의 어려움이 주요 이유이다. 우선적으로 동전은 액면 대비 제조 원가가 비싸 발행 자체에도 비용 부담이 크다. 지난해 100원짜리 동전 2억5,000만개를 포함하여 동전 6억개를 제조하는 데 든 비용은 539억원에 달하지만 동전의 환수율은 10%에 불과할 정도로 제조와 발행 비용에 비해 유통이 잘 되지 않는 구조를 가지고 있다.[176] 고액권은 높은 가치의 화폐를 지폐로 유통하기 때문에 비용상

175) 현금 없는 경제: 의미와 가능성, KERI, 2016
176) http://biz.chosun.com/site/data/html_dir/2016/05/05/2016050500724.html

문제는 없지만 가치가 너무 높기 때문에 유통이 되지 않는다는 문제점이 있다. 2015년 기준 5만원권 환수율은 40.1%로 1만원권의 95.3%의 절반에도 못 미친다.[177] 이는 고액권이 유통되기보다는 가치를 보관하는 목적에 머물러 있으며 이에 따라 현금의 유통과 관리에 있어 비효율성이 발생된다.

두 번째는 이미 국내에서 현금 없는 사회를 논의하기 충분할 정도로 전자 거래의 비중이 높고 활성화가 되어 있기 때문이다. 기존의 거래 방식들의 불편함과 비효율성에도 불구하고 현재까지도 현금과 동전이 상당 부분 이용되고 있으나, 전자 거래 기술의 발달로 더 효율적인 전자 거래를 할 수 있는 기반이 구성되었고 이를 바탕으로 기존의 지폐 시스템이 가지고 있는 불편함을 개선할 수 있다는 것이다.

특히 한국의 경우 정보통신 인프라가 잘 갖춰져 있고 신용카드 결제 등 전자결제 인프라가 잘 구축되어 있는 등 전자 거래가 활성화되어 있는 국가이다. 한국은 국제정보통신연맹(ITU)에서 매년 발표하는 정보통신기술발전지수(IDI)에서 2015년 1위를 차지할 정도로 기술적인 발전이 빠른 상황이다.[178] 거래건수에서도 지급수단별 이용비중이 신용카드(39.7%)가 현금(36.0%)을 추월하면서 비현금거래가 현금거래보다 비중이 높아지는 추세이다. 이미 많은 부분에서 금융 거래의 전자화가 이뤄지고 있고, 국민들이 전자 거래에 익숙해지는 상황에서, 중앙은행 또한 디지털 화폐를 직접 발행하기 위한 기술적, 제도적 논의도 본격적으로 이뤄지고 있으며 이를 구현할 수 있는 기술로서 블록체인이 큰 가능성을 갖고 있다고 판단하여 관련 연구가 활발히 진행되고 있다.

나. 블록체인 기반 디지털 통화의 장점

이미 많은 분야에서 전자화된 금융 거래가 활성화되고 기존 전자 거래의 시스템에 대한 기술적 발전도가 높은 상황이다. 하지만 디지털 통화 발행에 있어 많은 금융기관과 중앙은행은 비교적 새로운 기술로 평가받고 있는 블록체인 기술을 중심으로 연구를 추진하고 있다.

비교적 새로운 기술이라 할 수 있는 블록체인을 기반으로 하는 디지털 화

177) http://www.newsis.com/ar_detail/view.html?ar_id=NISX20160319_0013968457&cID=10401&pID=10400
178) http://www.m-economynews.com/news/article.html?no=17662

폐에 대한 가능성이 언급이 되는 것은 특정 기업이나 고객에 국한된 전자 화폐가 아닌 중앙은행이 국민들을 대상으로 발행하는 전자 화폐이기 때문이다. 중앙은행이 전자화된 화폐를 발행한다는 것은 기존에 오프라인으로 유통되던 화폐를 온라인으로 유통을 한다는 의미이며, 이는 발행, 유통, 환수 등 화폐가 만들어내는 모든 과정을 디지털화하고 이를 전적으로 중앙은행이 관리한다는 의미이다. 이를 위해서는 현금을 대체할 수 있을 정도의 보안성과 확장성이 필요하고 현 화폐 시스템의 문제를 해결할 수 있는 투명성 확보가 가능한 화폐 시스템이 필요하다는 것을 의미한다. 현재 전자거래 시스템이 화폐를 대체해 나가고 있지만 중앙은행이 이같은 시스템을 기반으로 디지털 화폐를 발행하는 경우 보안의 문제나 거래 규모의 문제를 감당할 수 있을지에 대한 의문이 있고 시스템을 관리하기 위한 비용문제 또한 존재한다.

블록체인은 비트코인의 기반기술로서 이미 시스템적으로 화폐를 발행하고 유통할 수 있다는 가능성이 확인되었다. 비록 비트코인 등의 개방형 블록체인은 그 활용에 있어서의 한계로 인해 타 기관이 직접적으로 사용할 수는 없지만, 비트코인의 기반 기술인 블록체인이 가지고 있는 가능성은 많은 곳에서 확인되었고 이를 통해 폐쇄형 블록체인의 연구개발과 컨소시엄 구성 등이 활발해졌다. 이 연구는 다시 특정 기관이 발행하는 가상화폐에 대한 연구로 이어졌고 정부가 직접 디지털 화폐를 발행하는 방안에 대한 관심으로까지 이어지게 되었다.

우선 전자화폐 플랫폼으로서 블록체인 도입을 고려하는 이유 중 하나는 블록체인을 통해 거래의 투명성을 담보할 수 있기 때문이다. 기존 화폐 시스템의 단점 중 하나는 화폐가 어떻게 사용되고 있는지 내역을 파악하기가 어렵다는 점이고, 이 어려움으로 인해 낮은 환수율과 저조한 사용도의 문제를 극복하기 어렵게 만든다. 반면, 블록체인이 가지고 있는 가장 큰 장점 중 하나는 투명성이다. 분산형 네트워크를 통해 장부를 공유하기 때문에 거래 내역을 확인하고 개별 거래들을 추적할 수 있다. 개방형 블록체인의 대표적인 사례인 비트코인은 누구나 거래 내역을 조회할 수 있고, 폐쇄형 블록체인도 구성하기에 따라서 블록체인 관리 기관이 모든 거래 정보를 확인할 수 있다는 장점이 있다. 이는 현재의 화폐 시스템의 단점인 고액, 저액 화폐의 낮은 환수율과 고액권이 지하 경제로 스며드는 문제를 극복할 수 있으며, 화폐 사용 내역들을 통해 화폐의 흐름을 분석하고 거시적인 화폐 정책을 구상하는 데도 도움이 될 수 있다는 장점을 가지고 있다.

두 번째로는 블록체인을 통해 거래내역을 추적할 수 있으면서도 익명성을 구현할 수 있는 플랫폼을 구성할 수 있기 때문이다. 다른 여러 보안적 장치와 함께 블록체인 내의 거래의 투명성은 거래의 위변조를 방지하고 실시간으로 거래를 파악할 수 있는 기반이 되었다. 하지만 다른 한편으로 일체의 거래내역이 공개되는 투명성으로 인해 거래내역과 기밀 정보의 보안을 강조하는 금융기관들이 개방형 블록체인을 직접 활용하는 데 어려움이 컸고, 이를 극복하기 위해 각 금융기관과 스타트업들은 기록들의 열람과 조회의 권한을 설정할 수 있는 폐쇄형 블록체인을 개발하기 시작했다. 기본적으로 거래 내역을 투명하게 공개하는 블록체인이지만 폐쇄형 블록체인의 경우는 접근 권한 설정에 따라 거래 당사자만이 거래를 확인할 수 있는 시스템을 구성할 수 있고 이는 개방형과 거래의 익명성을 동시에 유지할 수 있는 플랫폼으로 활용될 수 있다.

세 번째는 활용도, 특히 동전으로 대표되는 소액 현금 결제의 활용도를 높일 수 있다. 현재 동전은 환수율이 10%에 불과할 정도로 유통이 저조한데, 이는 물가상승으로 인해 동전으로 거래할 만한 물품이 많지 않은 데다 무게와 부피 때문에 많은 금액을 동전으로 들고 다니기도 힘들기 때문이다. 또한 분실도 잦아서 제대로 사용되지 못하는 경우도 많다. 디지털 통화는 지폐와 동전을 전자화함으로써 소지의 불편함 문제를 줄일 수 있고, 쉽게 사용할 수 있는 환경을 만들어준다. 또한 실물 화폐처럼 분실할 염려가 없기 때문에 활용도와 환수율을 높이고 숨어있던 화폐의 유통을 활발하게 만들 수 있는 시스템으로 활용될 수 있다.

네 번째로는 블록체인 기술이 보안상 문제를 극복할 수 있는 방안이 될 수 있다. 블록체인 기술은 중앙기관 없이 화폐를 발행 및 유통한 대표적인 케이스인 비트코인의 근간이 되는 시스템이다. 비트코인 블록체인이 기능적인 한계점들을 가지고 있지만, 보안상으로는 비트코인 블록체인에 대한 내외부 공격으로 인한 피해 없이 정상적으로 운영이 되고 있다. 블록체인 기술은 시스템에 대한 내외부 보안에 큰 비용을 지출할 필요 없이 분산화된 네트워크를 통해 시스템적으로 보안의 문제를 해결한 플랫폼이다. 전자화된 화폐를 발행할 때 이용자들이 사용하는 전자화폐가 안전하게 보관되고 분실이나 위변조를 방지할 수 있는 안정성 있는 플랫폼을 제공할 수 있어야 하며, 이를 뒷받침할 수 있는 기술로 블록체인이 활용될 수 있을 것이라고 보고 있다.

다. 블록체인 기반 디지털 통화 연구 현황

현재 블록체인 기반의 디지털 통화에 대한 연구는 초기 단계에 있다고 볼 수 있다. 디지털 화폐가 현금의 문제점과 비효율성을 극복할 수 있는 대안으로 평가받고 있지만 아직까지 현금에 대한 수요가 상당 수준을 유지하고 있고, 현금을 전자화하는 데 따른 기술적 문제, 국민들이 전자화폐를 받아들이는 데 있어 정서적 문제 등이 남아있기 때문이다. 현재는 화폐 발행 및 유통 플랫폼으로서 블록체인의 기술적 가능성과 활용 방안에 대한 검토에 착수하고 있는 단계이며 향후 본격적인 활용에 앞서 심도 있는 연구가 우선 추진되고 기술적 성숙도가 높아질 필요가 있는 것으로 판단된다.

블록체인 기반 디지털 화폐에 대해 구체적인 보고서를 작성한 중앙은행은 사실상 영란은행이 유일하다. 영란은행은 올해 4월 블록체인 기반 중앙은행 발행 디지털 화폐인 RSCoin 보고서를 발표했고, 현재까지 계속해서 관련 연구를 진행중인 것으로 알려져 있다. 네덜란드 중앙은행(DNB Coin), 캐나다 중앙은행(CAD Coin) 등도 블록체인 기반의 디지털 화폐에 대한 연구를 진행 중이라고 밝혔지만, 디지털 화폐를 연구한다는 언론 발표 이후에 보고서 등의 구체적인 결과물은 아직 공개되지 않은 상태다. 중국 정부도 올해 2월 전자화폐 발행을 위한 기술로 클라우드 컴퓨터, 전자 칩 기술 등과 함께 블록체인을 고려하며 연구를 진행 중이라고 밝혔지만,[179] 이후에 블록체인에 대한 구체적인 추가 언급은 없는 상태이다.

2. 중앙은행의 디지털 통화 발행 방안

중앙은행이 발행하는 블록체인 기반 디지털 화폐는 화폐의 발행 권한을 전적으로 담당하는 중앙은행의 시스템과 발행 권한이 완전히 분산화된 비트코인 블록체인의 기술적 장점을 조합하려는 독특한 시도이다. 하지만 기존의 지폐와 동전으로 대표되는 화폐 시스템의 비효율성을 극복하기 위한 방안을 찾는 중에 분산화된 네트워크에서 화폐를 발행·유통하는 비트코인은 디지털 화폐발행을 가능하게 해주는 기술적 근거를 제공해 주었고, 비트코인으로 대표되는 개방형 블록체인의 한계를 극복할 수 있는 방안으로 폐쇄형 블록체인이 대두되고 기술적 개발이 이어지면서 각 중앙은행을 중심으로 블록체인을 기반으로 하는 디지털 화폐의 발행 논의가 올해 들어 본격적으로 시작되고 있다.

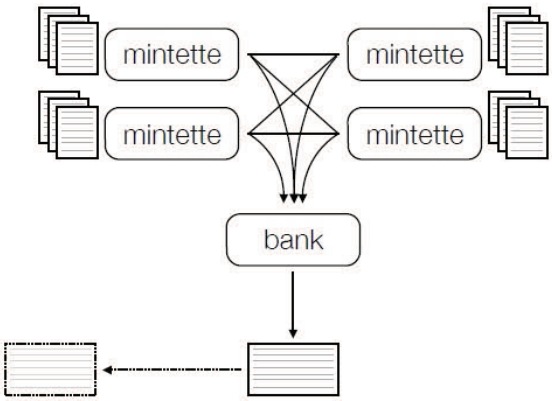
179) http://www.coindesk.com/chinas-central-bank-weighing-blockchain-as-one-option-for-digital-currency/

본 보고서에서는 영란은행이 발표한 RSCoin에서 제안된 모델을 중심으로 중앙은행 발행 디지털 화폐의 구조와 한국은행에 시사하는 점을 서술하고자 한다.

가. RSCoin의 블록체인 기반 화폐 유통

RS코인은 올해 4월 영란은행에서 발표한 중앙화된 은행 기반 암호화폐(Centrally Banked Cryptocurrencies)라는 이름의 보고서에서 처음 등장했다. 비트코인처럼 블록체인의 분산화된 네트워크를 도입하되 중앙은행이 전적으로 발행과 통제를 담당하는 구조를 가지고 있다.

<그림 4-1> RS코인의 개괄적인 구조도



자료: RSCoin Report

RS코인 모델의 가장 큰 특징은 분산원장 기술을 활용하지만 중앙은행이 모든 것을 통제하는 블록체인이라는 것이다. 블록체인의 형식을 빌려서 여러 노드들이 거래를 확인하고 승인하는 과정을 거치지만 화폐의 발행과 거래에 대한 최종 승인 등 주요 절차는 모두 중앙은행이 담당을 하고 다른 절차들은 중앙은행이 승인한 타 기관들에 위임하는 식으로 블록체인을 운영한다. 결국 블록체인이라는 형식을 따온 중앙집권화된 발행 시스템을 구현하고자 한다.

두 번째 특징은 블록체인 구조를 이원화하여 운영한다는 것이다. RS코인 구조도를 살펴보면 거래의 수집과 초기 블록들을 생성하는 하위 단계 블록

(lower-level block)과 최종 블록의 생성 및 화폐의 발행을 담당하는 상위 단계 블록(higher-level block)으로 나뉜다. 여기에서 중앙은행은 기능적으로 상위 단계 블록을 담당하고, 하위 단계 블록의 역할을 담당하지는 않지만 이를 통제하는 권한을 가진다. 이는 결국 실질적인 업무는 최소화하되 통제의 권한은 최대화한 구조로 하위 단계 블록에서 1차적으로 거래를 확인하고 블록을 생성하면 상위 단계 블록에 전송을 하고, 상위 단계 블록을 담당하는 중앙은행에게 가장 중요한 승인과 블록 등록의 역할을 맡기지만, 다른 역할들은 최소화하면서 시스템을 유지하게 한다.

단계별 블록에 대해 보다 상세히 살펴보면, 하위 단계 블록은 거래 내역을 종합하는 Mintette가 모여서 구성이 되는데 Mintette는 거래 내역을 모아서 블록을 만드는 역할을 한다. 개방형 블록체인에서의 채굴자 역할과 유사하며, 블록을 만드는 절차도 비트코인 등의 개방형 블록체인과 비슷하다. 개방형 블록체인에서의 채굴자와 차이점은 Mintette의 경우 작업 증명 등의 채굴 과정을 통해 블록을 만드는 대신 PKI 방식 등을 통해 중앙은행의 승인을 받아 블록을 생성한다. 중앙은행의 승인을 받은 Mintette들은 거래의 모음인 블록을 생성하며 다른 노드들과의 공유를 통해 1차적인 블록을 완성한다. Mintette는 중앙은행이 담당할 수도 있고 중앙은행이 신뢰할 만한 대형 상업 은행 등의 금융망 참여기관들이 담당할 수도 있는 등 다양한 방식을 선택할 수 있다.

<그림 4-2> 하위 단계 블록의 거래 승인 절차

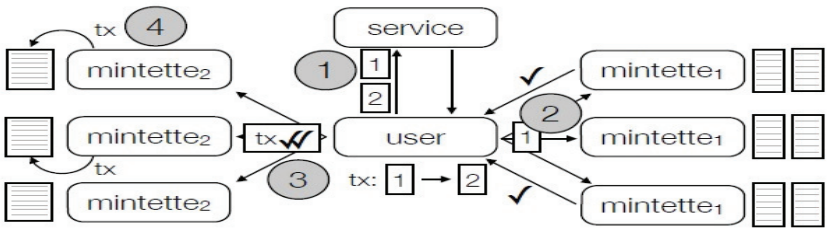


Fig. 2: The proposed protocol for validating transactions; each mintette m_i is an owner of address i. In (1), a user learns the owners of each of the addresses in its transaction. In (2), the user collects approval from a majority of the owners of the input addresses. In (3), the user sends the transaction and these approvals to the owners of the transaction identifier. In (4), some subset of these mintettes add the transaction to their blocks.

자료: RSCoin Report

상위 단계 블록에서는 하위 단계 블록에서 만든 블록들을 공식적인 블록체인에 등록하는 역할을 한다. 상위 단계 블록은 하위 단계에서 만들어진 블록의 무결성을 검증하고 확인이 되면 이를 상위 레벨의 블록체인에 등록한다. 즉, 1차적으로 정리가 된 블록을 마지막에 검증하여 2차적으로 공식적인 블록체인에 등록하는 것을 의미한다. RS코인의 사용자는 상위 단계 블록만을 확인해도 충분히 거래 내역을 체크할 수 있는 구조가 되며, 하위 단계 블록에 대한 확인을 하고 싶은 경우에도 거래 내역을 확인할 수 있도록 설계하는 것도 가능하다.

RS코인은 결국 블록체인의 형식을 빌려 분산화 네트워크를 활용하되 발행 등 주요 권한은 중앙은행이 보유하는 네트워크를 가진다. RS코인을 통해 기존의 비트코인보다 더 확장성이 있으면서도 중앙은행이 활용을 높일 수 있는 방법을 찾겠다는 것이 보고서의 주요 내용이다. 더욱이 보고서에는 하위 단계 블록의 역할을 중앙은행이 신뢰할 만한 금융기관들이 담당할 수도 있다고 설명하고 있으며, 중앙은행은 Mintette에 대해 전적인 권한을 가지고 있고 하위 단계 블록을 담당하는 Mintette에게 일정량의 수수료를 지급하는 내용도 포함되어 있다. 이는 하위 단계 블록에서 기존 개방형 블록체인의 모델을 최대한 유지하면서 화폐 유통을 담당하게끔 만들고, 중앙은행은 화폐 발행기관으로서 화폐를 발행하고, 유통된 거래에 대해 최종적으로 승인을 하고, 화폐 유통을 관리하는 하부 기관을 관리하고 보상하는 역할만을 맡겠다는 의미를 가진다.

나. 디지털 화폐 발행 방법

RS코인의 보고서 자체는 이원화된 블록체인 구조를 바탕으로 거래를 검증하고 합의를 도출하는 등 시스템을 운영하는 방법을 간략히 설명한 자료이며, 디지털 화폐에 대한 구체적인 발행의 절차, 거래 내역을 전달받는 방식 등 실제 운영을 위한 구체적인 요건 등에 대한 설명은 담겨 있지 않다. 중앙은행이 어떤 블록체인 구조를 가지고 검증을 하며 블록체인을 구성할지도 중요한 요소이지만 블록체인을 통해 발행된 화폐를 어떻게 발행하며 사람들이 사용하도록 할 수 있을지도 고려해야 할 요소일 것이다.

장기적으로 블록체인 기반의 디지털 화폐를 만들기 위해서는, 우선적으로 역할에 대한 구분이 필요하다. 이를 위해서는 비트코인 블록체인의 구조를

참조할 수 있다. 현재까지의 개방형 블록체인 중 가장 많은 사용자를 보유하고 있는 비트코인 블록체인은 익명의 다수를 대상으로 하는 개방형 블록체인 네트워크로서 각 노드들은 서로 동등한 위치에 있지만 각자 다른 역할을 가지며 유지될 수 있다. 비트코인 블록체인의 노드들은 크게 네 가지 기능을 가질 수 있으며 이 기능을 어떻게 나누어 가지고 있느냐에 따라 비트코인 네트워크에서의 역할이 달라진다.

기능적으로 봤을 때 비트코인 네트워크의 노드들은 모든 블록체인 정보의 데이터베이스가 담겨있는 풀 블록체인 데이터베이스(full blockchain database), 비트코인 채굴을 담당하는 채굴자(Miner), 거래와 블록을 전파하는 네트워크 라우팅(Network Routing), 비트코인 거래를 할 수 있는 지갑(wallet)이 있다. 이 네 가지 기능이 어떻게 조합되는지에 따라 노드의 역할이 바뀌며 참여자가 자유롭게 변경할 수 있다.

우선 모든 노드들은 네트워크 내에 라우팅 기능을 가지고 있으며, 여기에서 다른 기능들이 더해진다. 라우팅 기능을 통해 모든 노드들은 거래와 블록을 검증하고 전파하면서 노드들을 연결하고 블록체인 네트워크를 유지하는 역할을 수행한다.

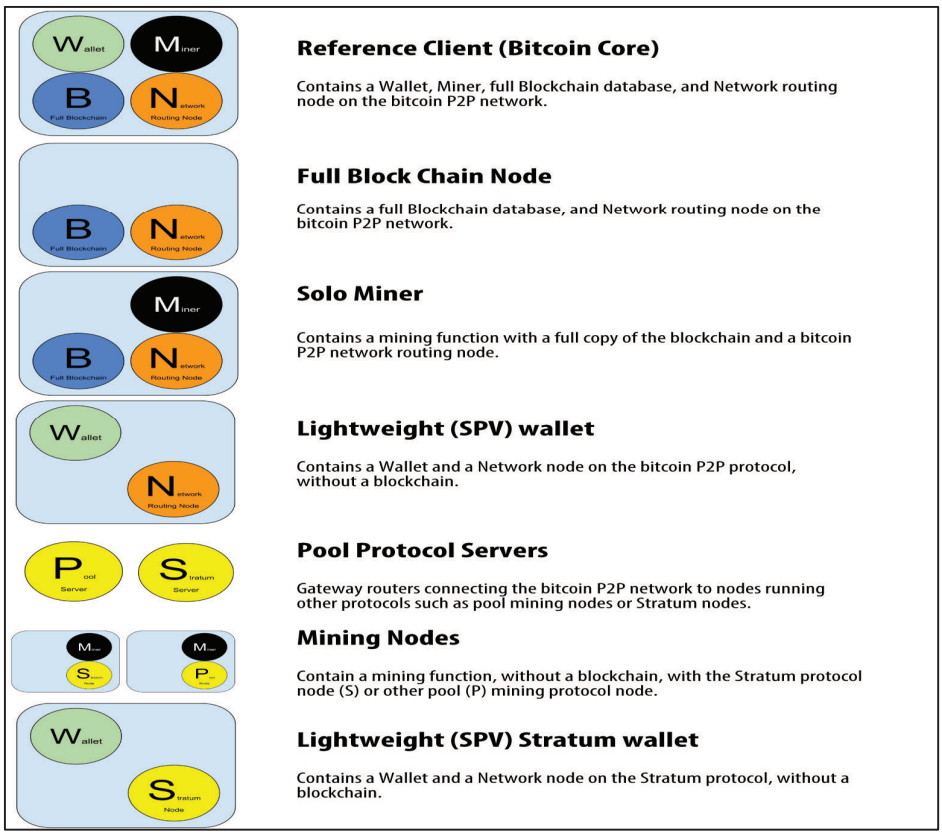
풀 노드(full node)라고 불리는 노드들은 모든 데이터베이스를 가장 최신의 상태로 가지고 있는 노드들이다. 비트코인 거래의 모든 정보를 저장하고 독자적으로 신뢰할 수 있는 방법을 통해 거래를 검증하는 사용자로서 비트코인 생태계를 유지하는 모든 기능을 직접 수행하는 사용자다.

두 번째로는 채굴 노드(Miner)가 있다. 채굴 노드는 작업증명을 푸는 전용 하드웨어를 가지고 평균 약 10분마다 나타나는 문제를 풀기 위해 경쟁하는 노드들로서 채굴을 통한 신규 화폐 발행이 그들의 동기부여가 된다. 채굴 노드는 풀 노드로서 블록체인 거래 내역 전부를 들고 있을 수도 있지만, 풀 노드 없이 서버에 의존하여 기능할 수도 있다.

다른 하나는 라이트웨이트 노드(lightweight node)가 있다. 라이트웨이트 노드는 SVP(Simple Payment Verification) 노드라고도 불리는데, 풀 노드처럼 전체 블록체인 기록을 가지고 있지는 않지만 단순지불검증이라는 방법을 이용하여 거래를 검증하고 비트코인 거래에 참여하는 노드들을 의미한다. 비트

코인 거래를 원하지만 다른 부담을 지고 싶지 않아하는 경우로 일반적인 비트코인 플랫폼 사용자들은 대부분 라이트웨이트 노드들이다. 라이트웨이트 노드는 블록 헤더만 다운로드하고 각 블록에 있는 거래들은 가지고 있지 않기 때문에 풀 노드보다 약 1,000배 가량 작은 크기를 가지고 있으며, 거래를 검증할 때는 이웃 노드들에게 의존하는 방법을 이용하여 거래를 검증한다. 풀 노드와 라이트웨이트 노드를 비교하여 검증 과정을 설명하자면, 풀 노드는 해당 지역 전체를 볼 수 있는 지도를 가지고 여행을 다니는 사람이라면, 라이트웨이트 노드들은 지도 없이 주변 사람들에게 길을 물어보며 여행을 다니는 사람에 해당한다고 볼 수 있다.

<그림 4-3> 비트코인 네트워크에서 노드들의 역할



자료: Mastering Bitcoin

비트코인 노드들의 기능과 비교해 보자면, 중앙은행은 풀 노드로서 모든 거래 내역을 보유하고 화폐를 발행하는 역할을 하게 되고 이를 이용하는 국민들은 라이트웨이트 클라이언트로서 전자화폐의 사용만을 할 수 있는 역할을 하게 될 것이다. 채굴 노드의 경우도 화폐를 발행하는 중앙은행이 이 기능을 맡게 되지만, 구체적으로는 블록체인의 구조에 따라 다른 방법으로 대체될 수 있다. 이는 개방형 블록체인에서 채굴을 위해 만들어진 작업 증명 등의 방식 대신 다른 방법으로 화폐 발행을 대체할 수 있기 때문이다. 3장에서 소개된 혼합결제시스템의 방식처럼 발행을 담당하는 중앙은행이 발행 거래를 생성하여 배포하는 방식 등을 활용할 수 있다.

3. 디지털 통화 도입의 조건 및 고려 사항

가. 보안성

정부가 발행하는 디지털 화폐는 지폐, 동전과 마찬가지로 모든 국민들이 사용하게 될 화폐이다. 그렇기 때문에 견고한 보안 시스템은 필수적이며 국민들에게 기술적으로 문제가 없다는 신뢰를 보장해야 한다.

정부가 블록체인을 기반으로 하여 화폐를 발행하게 된다면 사용자 관리와 화폐 발행은 중앙은행이 담당하게 되겠지만, 사용 대상이 대한민국에 사는 모든 사람들 혹은 한국의 화폐를 사용하고자 하는 모든 사람들이 된다면, 사실상 불특정 다수가 사용하는 개방형 블록체인의 형태에 가까울 것이다. 개방형 블록체인의 가장 대표적인 사례인 비트코인 블록체인의 경우는 거래에 참여하는 노드들이 직접 채굴 노드와 풀 노드들의 역할을 맡았고 노드들이 작업 증명 등을 통해 투입한 컴퓨팅 파워가 외부의 공격을 어렵게 하는 보안상의 근거가 되었고, 노드들은 그 대가로 비트코인을 발행받도록 설계되어 있다. 즉, 개방형 블록체인은 사용자가 발행자가 되어 보안 시스템을 자발적으로 구성하는 메커니즘으로 운영이 된다. 하지만 중앙은행이 발행하는 디지털 화폐의 경우 다수의 인원이 자유롭게 참여한다는 점에서는 개방형 블록체인의 성격을 가지고 있지만 역할과 권한의 구분이 명확하고 특정 발행기관이 정해져 있다는 점에서 기본적으로 폐쇄형 블록체인이라고 할 수 있다. 그리고 발행과 거래 내역의 기록 등의 권한은 중앙은행 고유의 권한으로서 이 역할을 다른 기관 또는 개인에게 양도할 수는 없다.

결국 개방형 블록체인처럼 운영되는 폐쇄형 블록체인인 정부 발행 디지털 화폐에서는 기존 개방형 블록체인에서 참여자가 자발적으로 수행하는 기능을 중앙은행이 어떻게 처리할 것인가의 문제가 남는다. RS코인의 방식에서와 같이 하위 단계의 블록들이 참가자들의 거래 내역을 모아 하나의 블록을 생성하고 상위 블록인 중앙은행은 거래의 유효성을 재검사하고 승인하여 공식 블록체인에 등록하는 등 많은 사용자와 거래 건수를 안전하게 처리하고 내역을 등록할 수 있는 시스템에 대한 연구가 필요하다.

나. 확장성 (처리 용량 및 속도)

블록체인 기술이 디지털 화폐를 구현할 수 있는 기술로 각광을 받고 많은 중앙은행과 금융기관이 이를 기반으로 하는 디지털 화폐에 관한 연구를 진행하고 있지만 현재까지 개발된 블록체인 기술이 한 국가의 화폐를 유통할 만큼의 처리 용량과 속도를 가지고 있는지도 고려해야 할 것이다. 3장에서 설명한 지급결제시스템의 경우에는 혼합결제시스템에 참여하는 금융 기관만이 블록체인 기반 지급결제시스템에 참여하고 거래 유형 또한 금융 기관 간의 거액 결제에 국한된다. 이렇듯 기관의 수와 거래의 유형이 제한적이기 때문에 거래의 건수 또한 상대적으로 많지 않다. 일반적으로 블록체인 내에서 거래의 규모는 거래 금액의 크기보다는 건수가 더 중요한 문제이기 때문에 거액결제시스템에서는 확장성의 문제는 큰 이슈가 아닐 것으로 보인다. 하지만 일반 개인간 거래에서 현금이 유통되는 건수도 비교할 수 없을 정도로 많고 거래에 참여하는 대상자가 전 국민이다. 현재의 블록체인의 기술적 수준이 이를 감당할 수 있을 만큼 높아지기에는 개발과 기술의 추가적인 진보가 필요할 것으로 보인다.

우선 중앙은행은 지속적으로 블록체인 활용 방안을 연구하면서 동전을 대체하는 전자지갑이나 소액 결제 등에서만 활용하는 등 규모와 역할의 제한을 두는 블록체인 기반 화폐 유통을 우선 시작하고 이후 점진적으로 블록체인 기반 디지털 화폐 도입을 확대해 나가는 것과 같은 접근법이 필요할 것으로 보인다.

또한 현금 유통의 경우 일일 거래 건수를 정확하게 파악하기가 불가능하기 때문에 다양한 테스트를 통해서 어느 정도 규모의 현금 거래를 블록체인에 적용할 수 있을지, 전면적인 도입을 가정할 때는 어느 정도의 기술적 개선이

필요한지 등에 대해 지속적으로 연구할 필요가 있다.

다. 시장, 국민의 디지털 화폐에 대한 적응

기술 자체에 대한 문제는 아니지만 화폐를 실제 사용하는 시장, 국민들의 기술에 대한 적응 문제도 중요한 이슈이다. 거래 수단이 다변화되고 전자 거래의 비중이 높아지고 있지만 여전히 많은 부분에서 현금거래가 이루어지고 있다. 한국은행의 조사에 따르면 지난해 소비자들의 지급결제 수단 중 신용/체크/직불카드의 비중이 전체의 53.8%를 차지했지만, 반면 현금결제 비중은 38.9%에서 36.0%로 줄어들었으며, 금액 기준으로 보면 29%에 불과하다. 따라서 약 60%의 거래가 신용카드 등의 전자적인 방법으로 이루어지고 있으나, 반대로 생각하면 36%에 달하는 상당수 거래가 현금으로 이루어지고 있음을 의미한다. 특히 장노년층과 재래 시장 등의 특정 부분에서는 아직 전자거래가 익숙하지 않기 때문에 이와 같은 측면에서 충격을 최소화하면서 점진적으로 도입하기 위한 방안 등에 고민도 함께 따라야 할 것이다.

또한 국민들의 디지털 화폐 사용에 대한 정서적인 문제도 고려해야 한다. 디지털 화폐를 발행하는 우선적인 목표는 화폐 발행 및 보관을 위한 비용을 절감하고 지폐 사용에 따른 번거로움을 줄임으로써 국민들의 화폐 활용 편의성을 증대하는 것과 함께 지하경제의 양성화를 통한 세율 인상 없는 넓은 세수 확보이다. 하지만 디지털 화폐가 정부에 유리하고 국민에 불리한 정책을 도입하기 위한 교두보라는 인식이 확산될 수 있는 데다, 국가가 개인의 모든 거래 내역을 상시 감시하고 자유로운 화폐의 사용을 제한할 수도 있다는 점에서 국민적 반감이 형성될 수도 있다.

또한 최근 화두로 등장한 현금 없는 사회의 추진 목적이 저금리 기조 하에서 마이너스 금리 정책을 실시하기 위한 것이 아닌가 하는 논의도 진행되고 있다. 현재 중앙은행에서 마이너스 금리를 도입하더라도 개인들이 금융자산을 현금으로 보유하는 경우에는 경기 부양 정책으로서 실질적으로 효과가 크게 줄어든다. 하지만 모든 현금을 전자화하여 정부가 직접 발행 및 관리한다면 마이너스 금리 정책을 보다 용이하게 실시할 수 있고, 결국 국민들은 피해를 보게 될 수 있다는 우려도 형성되고 있다.

결국 디지털 화폐를 이용하는 주체는 국민이기 때문에 정서적 반감의 진위

여부를 떠나서 중장기적으로 공감대를 형성하고 제도 도입을 충실하게 준비하기 위한 시간이 필요하다. 화폐 사용의 감시 문제와 관련하여 정부의 목적이 사적인 거래의 감시가 아니며 편리하고 투명한 거래를 보장하기 위함임을 적극 홍보하여 불안을 해소하는 한편, 기술적으로도 개인의 거래 내역 노출이 최소화될 수 있도록 보호장치에 대한 연구가 동반되어야 할 것이다.

라. 디지털 화폐 구축을 위한 기술적 인프라 문제

비록 현재 국내에서 전자거래의 비중이 크고 현금결제가 빠르게 전자 거래로 대체되고 있지만, 중앙은행이 발행하는 디지털 화폐를 전면적으로 도입했을 때, 전자 결제에 익숙하지 않는 기관들에게 어떻게 기술적 인프라를 공급할 수 있을 것인가의 문제 또한 고려할 필요가 있다.

현재 현금 시스템이 가지고 있는 가장 큰 장점은 어디서나 즉시 거래가 가능하다는 편의성이다. 현금을 보유하고 있으면 돈을 주는 주체나 받는 주체 모두 추가적인 장치나 절차 없이 바로 거래가 성사되는 편의성과 즉시성이 현금 거래의 가장 큰 장점이다. 현재 신용카드, 각종 페이 등으로 대표되는 전자거래는 돈 그 자체가 아니라 돈의 역할을 대신하는 지급결제 수단을 수용하는 것이기 때문에 신용카드나 다른 지급결제 서비스의 수용 여부는 개인의 선택이며 이를 강제할 수 없다. 하지만 중앙은행이 발행하는 전자화폐는 100% 화폐의 역할을 해야 하기 때문에 모든 사람들이 현금으로 거래를 하는 데에 전혀 문제가 없듯이, 지금의 현금 거래처럼 혹은 현금 거래에 준하는 편의성을 제공해야 전자화폐에 대한 활용도가 높아질 수 있을 것이다.

마. 결론

현재 블록체인 시스템은 디지털 통화 시스템을 구현할 수 있는 안정성, 투명성, 익명성 등의 장점을 가지고 있지만 거래 규모, 확장성 등의 블록체인 자체의 문제와 디지털 화폐의 도입 방안 및 인프라와 같은 외부적인 문제가 존재한다. 그러나, 블록체인은 디지털 화폐 인프라를 구현할 수 있는 가능성 있는 기술로 인정받고 있으며, 현재도 혁신성 있는 기술로서 계속 연구가 진행되고 있고 빠른 속도로 발전해나가고 있다. 디지털 화폐의 플랫폼으로서 블록체인에 대한 지속적인 연구와 함께 '동전 없는 사회'의 전자 지갑 도입 및 이를 위한 플랫폼 연구 등을 점진적으로 추진해 나감으로써 블록체인을

통해 현금 없는 사회를 정착하기 위해 노력해야 할 것이다.

제2부 참고문헌

한국은행 금융결제국, 신한은금융망(BOK-Wire+) 구조 해설, 2009

한국은행, 2015년도 지급결제보고서, 2016

Antonopoulous, M, Andreas, “비트코인, 블록체인과 금융의 혁신“ (Mastering Bitcoin), 고려대학교 출판문화원, 2015

Citibank, Digital Disruption: How fintech is forcing banking to a tipping point, 2016

Coindesk, Banks and the blockchain report, 2015

Danezis, George and Meiklejohn, Sarah, Centrally Banked Cryptocurrencies, 2016

Deloitte, Blockchain: Enigma, Paradox, Opportunity, 2016

Finector, 블록체인 발전 과정과 이해, 2016

Finector, 금융기관을 위한 블록체인의 이해, 2016

IMF, Virtual Currencies and Beyond: Initial Considerations, 2016

Japan Exchange Group, Applicability of Distributed Ledger Technology to Capital Market Infrastructure, 2016

Moodys, Robust, Cost-effective Applications Key to Unlocking Blockchain’s Potential Credit Benefits, 2016

Nomura Research Institute, Survey on Blockchain Technologies and Related Services, 2015

UK Government Chief Scientific Adviser, Distributed ledger technology: beyond block chain, 2016

World Economic Forum, The future of financial infrastructure, 2016