블록체인패러다임과 핀테크 보안

박성준
동국대학교

요 약

현재 금융권에서는 핀테크 활성화를 위한 다양한 정책 추진과 다양한 비즈니스 모델이 창출되고 있는 실정이다. 그러나 핀테크의 본질에 대한 오해가 있는 듯하다. 핀테크의 본질은 중앙집중형 금융서비스를 P2P 분산형 서비스로 혁신하는 것을 의미한다. 이 특성이 기존의 전자금융 또는 e 금융과 핀테크의 차별성을 나타내는 중요한 개념인 것이다.

이런 측면에서 블록체인 기술이 핀테크 활성화의 기본 인프라 역할을 담당하게 될 것이다. 블록체인이란 P2P 네트워크에서 상호 신뢰 할 수 없는 사람들 간의 신뢰를 확보해주는 P2P 신뢰네트워크이기 때문이다. 특히, 블록체인 기술과 암호기술을 융합한 암호블록체인을 설명하고 암호블록체인이 제2의 인터넷으로 핀테크 산업 및 보안을 근본적으로 바꾸는 블록체인패러다임을 역설한다.

한편으로는 블록체인의 탄생 배경으로 인해 블록체인에 대한 다양한 오해가 있는 듯하다. 본고에서는 블록체인 기술에 대한 정확한 이해를 바탕으로 향후 핀테크 보안에 있어서 중요한 역할을 담당할 수밖에 없는 이유와 발전 방향에 대해 논하고자 한다.

Ⅰ. 서 론

블록체인 기술은 2008년 사카시 나까모도의 P2P 기반 암호화폐인 비트코인에 대한 역사적인 논문에서 비트코인의 이중지불방지를 위한 개념으로 도입되었다[1]. 사카시 나까모도는 암호학, 컴퓨터공학, 게임이론 및 경제학 등 다양한 개념 및 기술을 융합하여 비트코인을 완성하였다. 그러나 비트코인의 탄생 배경에 따른 목적은 단지 P2P 기반 암호화폐이다. 비록 블록체인을 기반기술로 사용하였으나 제한적이었다.

비트코인에서 사용된 블록체인 기술의 일반화는 부탈린의 이더리움에 의해 완성되었다[2]. 이더리움은 비트코인의 한계성을 극복하여 모든 응용서비스가 가능한 일반적인 블록체인 개념을 도입하였다. 이후 블록체인 기술은 전 세계적으로 재조명받기 시작하였으며, 현재는 비트코인 자체보다는 블록체인 기술에 대한 연구가 활발히 진행되고 있는 상황이다. 이더리움 블록체인의 비전 및 목표는 P2P 네트워크 기반 하나의 글로벌 신뢰컴퓨터를 만드는 것이다.

비트코인과 이더리움의 가장 큰 차별성 중 하나는 튜링 완전성(Turing-completeness)이다. 비트코인은 튜링 불완전성 특성을 가지며, 이더리움은 튜링 완전성(Turing-completeness) 특성을 가진다. 비트코인이 튜링 불완전성 특성을 가지고 있는 이유는 보안 문제 때문인 것은 주지의 사실이다. 한편 이더리움은 튜링 완전성을 확보하는 대신 보안성 문제를 금전적인 문제(가스(gas) 개념 도입)와 결부 시켰다. 즉, 이더리움을 사용하기 위해서는 미리 약속된 가스를 지급하여야 한다.

이더리움의 튜링 완전성 특성으로 인해 이더리움은 모든 응용서비스 개발을 가능하게 만드는 블록체인플랫폼으로 탄생하게 된다. 현재는 각 비즈니스 영역의 특성(속도, 정보보호 특성 등)에 따라 다양한 블록체인 플랫폼이 개발되고 있는 실정이며, 각 블록체인은 자체의 비전과 목표를 가지고 있다.

현재 블록체인 관련하여 장부(ledger), 공유장부(shared ledger), 분산장부(Distributed ledger), 블록체인 및 암호화폐 등 다양한 용어들이 사용되고 있으며, 〈그림 1〉에서 개념적인 도식을 나타내었다.

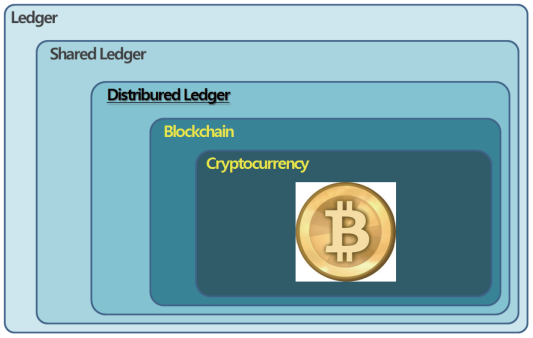

그림 1. 블록체인 관련 용어 개념

〈그림 1〉에서 알 수 있듯이 블록체인은 분산장부(Distributed Ledger) 중 신뢰성을 확보하는 한 가지 방법임을 알 수 있다. 그러나 일반적으로 블록체인과 분산장부를 동일 시 해도 무방하다.(물론 분산장부의 신뢰성을 확보하기 위해 반드시 블록체인 기술만이 존재하는 것은 아니며, 현재 금융권에서 활용되고 있는 R3가 블록체인 개념을 사용하지 않는 대표적인 분산장부이다. 사실 R3에서도 필요한 경우 블록체인 개념을 사용할 수 있다고 필자는 생각한다)

국내에서는 한국은행이 블록체인과 관련하여 분산원장 기술에 대해 다음과 같이 정의하였다. 분산원장(Distributed Ledger) 기술은 거래정보를 기록한 원장을 특정기관의 중앙 서버가 아닌 P2P(Peer-to-Peer) 네트워크에 분산하여 참가자가 공동으로 기록하고 관리하는 기술이다[2].

본고에서는 블록체인과 분산장부를 동일한 개념으로 생각하고자 한다.

블록체인은 상호 신뢰하지 않는 참여자들 간의 분산된 장부들의 무결성을 확보하는 기술이다.

즉, 기존의 중앙집중식 모델에서는 제3의 신뢰기관(TTP : Trusted Third Party)이 신뢰성을 확보해주는 역할을 담당하였다. 그러나 분산장부 모델에서는 신뢰성을 확보해주는 TTP을 제거하였기 때문에 누군가는 신뢰성을 확보해주어야 하며, 이를 P2P 네트워크 참여자들이 공동으로 해결해야 한다는 것이다.

P2P 네트워크의 신뢰성을 확보해주는 방법에 따라 블록체인은 크게 public 블록체인과 private 블록체인으로 구분된다.

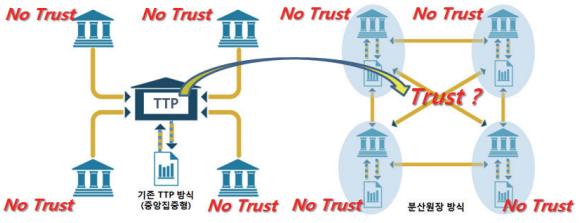

그림 2. 분산장부 모델

먼저 블록체인은 P2P 신뢰네트워크로서 네트워크 참여자들의 제한성에 따라 permissionless와 permissioned로 구분된다. permissionless 블록체인은 네트워크 참여에 제한이 없는 블록체인을 의미하며, permissioned 블록체인은 네트워크 참여에 제한을 두는 블록체인이다. 한편으로는 P2P 네트워크의 신뢰성을 확보하는 방법에 따라 public과 private로 구분된다. 네트워크의 신뢰성을 확보하는 네트워크 참여자들의 자격에 제한을 두지 않는 경우가 public 블록체인이며, 제한을 두는 경우를 private 블록체인(또는 consortium)이라고 한다. 따라서 크게 봐서는 4가지 블록체인이 존재하게 된다. 그러나 일반적으로 public 블록체인은 public, permissionless 블록체인을 통칭하며, private 블록체인은 private, permissioned 블록체인을 통칭한다.

대표적인 public 블록체인으로는 비트코인, 이더리움, 카르다노[4] 등이 있으며, private 블록체인에는 하이퍼레져(hyperledger)[5], 리플(ripple)[6], R3[7] 등이 있다.

블록체인의 원천기술은 바로 네트워크 참여자 간의 합의 메커니즘으로 볼 수 있다.〈그림 3〉

물론 합의 메커니즘은 public 블록체인과 private 블록체인에 따라 그 특성이 분리된다. Public 블록체인의 합의 메커니즘으로는 컴퓨팅 파워에 의존하는 작업증명(PoW : Proof of Work), 암호화폐 보유량에 의존하는 지분증명(PoS : Proof of Stake), 평판 및 투표에 의해 일종의 국회를 구성하는 방식인 위임지분방식(DPoS : Delegated Proof of Stake) 등이 있으며, private 블록체인 합의 방식으로 대표적인 것이 비잔틴장군 문제를 해결하는 솔루션인 PBFT(Practical Byzantine Fault Tolerance) 방식이다[8].

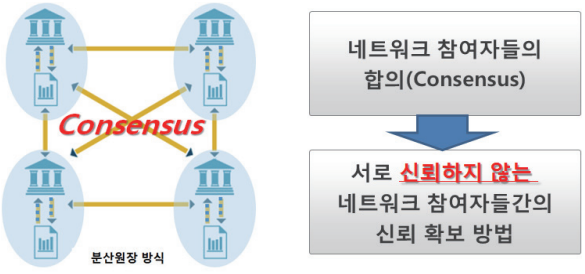

그림 3. 합의 메커니즘 도입 필요

그리고 일반적으로 public 블록체인은 필요에 따라 private 블록체인으로 쉽게 변환되지만, private 블록체인은 public 블록체인으로 변환 할 수 없다.

블록체인의 목적은 본질적으로 TTP를 제거한 P2P 네트워크의 신뢰성 확보 기술이다. 그러나 여기서 신뢰성이란 상호 신뢰하지 않는 네트워크 참여자 간의 장부의 무결성(immutability)을 의미한다. 즉, 데이터 무결성을 보장한다는 것이다. 특히, 블록체인 기술의 특성상 공개성과 투명성으로 인해 정보보호서비스와는 배치되는 것으로 오해할 수 가 있으며, 더구나 블록체인이 보안기술이라는 것은 어떻게 보면 역설적이기도 하다.

일반적인 정보보호 4대 서비스로는 비밀성, 인증, 무결성, 부인봉쇄서비스이다. 블록체인 기술은 일반적으로 정보보호 4대 서비스 중에서 무결성과 부인봉쇄 서비스 중 일부의 기능을 내

포하고 있다.

핀테크 활성화를 위해서는 다양한 핀테크 서비스에 대한 정보보호서비스도 같이 개발되어야 한다. 특히, 기본적으로 P2P 네트워크상의 금융서비스인 핀테크의 특성 상 핀테크 보안은 반드시 P2P 신뢰네트워크인 블록체인과 융합되어야 한다. 즉, 핀테크 보안은 기반인프라인 블록체인과 융합되는 것이 핀테크 활성화를 위한 전제조건이라는 것이다.

Ⅱ. 본론

블록체인 기술의 장점을 극대화하고, 정보보호서비스 기능을 블록체인에 내재하기 위해 암호기술과 융합된다.

일반적으로 암호기술은 크게 비밀성 기능을 갖는 암호화기술(Encryption), 인증기능을 갖는 전자서명기술(Digital Signature), 랜덤성을 확보하는 의사난수기술(Pseudorandomness), 프로토콜 상의 정보(또는 지식)를 주지 않기 위한 영지식대화형증명기술(ZKIP : Zero Knowledge Interactive Proof system), 그리고 암호화된 상태로 계산을 하기 위한 비밀계산기술(SC : Secure Computation) 등이 있다.

비트코인에서는 계정 및 거래 생성을 위해 전자서명기술을 사용하였으며, 각 계정의 공개키 및 개인키 생성을 위해서는 의사난수기술을 사용하였다.

블록체인에 정보보호서비스를 내재하기 위해서는 비트코인에서 사용한 2가지 기술 외에 나머지 모든 기술이 사용된다. 특히, 영지식대화형증명기술(ZKIP : Zero Knowledge Interactive Proof system) 및 비밀계산기술(SC : Secure Computation)이 중요한 역할을 담당하게 된다.

필자는 블록체인 기술과 블록체인에서의 정보보호 문제를 해결하기 위해 암호기술을 융합한 블록체인을 암호블록체인이라 명명하였다.〈그림 4〉

그림 4. 암호블록체인

비트코인과 이더리움을 제외한 hyperledger, R3 등 대부분의 블록체인 플랫폼은 기본적으로 암호블록체인으로 볼 수 있다.

블록체인의 기능은 크게 분산 DB, 암호화폐, 스마트계약 등이 있다.

분산 DB 기능은 저장하고자 하는 대상을 중앙집중화된 DB가 아닌 P2P 네트워크에 분산화 저장한다는 것을 의미한다. 암호화폐 기능은 P2P 네트워크상에서 화폐시스템을 설계할 수 잇다는 것이며, 이는 가치 전송으로 확대된다. 스마트계약 기능은 제3의 신뢰기관 또는 중재자 없이 P2P 네트워크 참여자 간의 신뢰할 수 있는 계약을 구성할 수 있다는 것이다.

스마트계약은 기본적으로 분산화, 자율성, 자급자족 기능을 갖는 튜링 완전성을 가진 소프트웨어로 간략히 정의할 수 있다. 한편으로는 블록체인은 스마트계약을 위한 플랫폼이라고 정의할 수 있다.

블록체인 기술은 암호기술과 융합하여 블록체인의 기본적인 기능 외에도 정보보호 4대 서비스인 비밀성, 인증, 무결성, 부인봉쇄 기능 뿐 아니라 가장 중요한 개인정보보호 기능 또한 내재한다.〈그림 5〉

구분	인터넷	블록체인인터넷	암호블록체인인터넷
비밀성	X	X	O
인증	X	X	O
무결성	X	O	O
부인봉쇄	X	△	O
개인정보보호	-	-	O

그림 5. 암호블록체인과 정보보호

본고에서는 지금부터 블록체인과 암호블록체인을 동일 시 하는 것으로 한다.

이러한 관점을 바탕으로 필자는 블록체인패러다임을 역설하고 있다.

20여 년 전 필자는 사이버패러다임을 역설하면서 사이버세상(인터넷 세상)의 도래에 대비하기 위해 사이버보안 필요성을 강조하였다. 사이버보안이란 기존의 종이문서의 기반을 둔 사회의 보안 개념을 인터넷 및 전자문서에 기반을 둔 보안개념으로 바꾸는 것이다.

사이버패러다임이 기존의 종이기반 비즈니스 모델을 인터넷에 기반을 둔 전자문서 활용 비즈니스 모델로의 전환을 의미했다면, 블록체인 패러다임은 인터넷 기반의 모든 비즈니스 모델을 블록체인 기반으로 전환하는 것을 의미한다.

특히, 사이버패러다임과 블록체인패러다임은 본질적인 측면

에서 큰 차이를 나타낸다. 사이버패러다임은 기존 비즈니스 모델(TTP 모델)은 유지하면서 업무 프로세스를 혁신하는 것이다.〈그림 6〉 한때 이러한 업무 혁신 과정을 리엔지니어링 또는 리스트락쳐링이라 명명하였다. 그리고 사이버패러다임이 현실화되기까지 대략 10년에서 15년 정도 소요되었다.

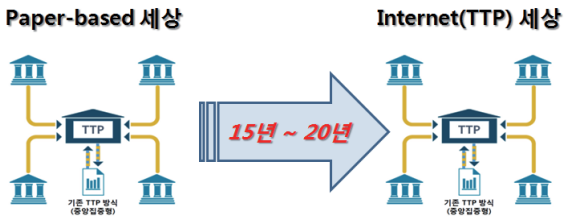

그림 6. 사이버패러다임

그러나 블록체인패러다임은 TTP를 제거하는 특성으로 인해 업무 프로세스 혁신 뿐 아니라 비즈니스 모델 자체의 혁신이기도 하다.〈그림 7〉 같은 맥락으로 향후에는 블록체인 리엔지니어링 또는 블록체인 리스트락쳐링이 필요하다. 그리고 무엇보다도 사이버패러다이미 현실화되는 기간보다 블록체인패러다임이 현실화 되는 기간은 매우 빠를 것으로 10년 이내가 될 것으로 예상된다.

그림 7. 블록체인패러다임

이러한 연유로 블록체인 기술은 파괴적인 혁신 기술이라고도 한다.

그리고 사이버보안이 필요하듯이 이제는 블록체인패러다임에 따른 블록체인 보안이 필요하게 된다. 즉, 사이버패러다임에 의해 사이버보안이 탄생하고 발전했다면, 블록체인패러다임에 의해 블록체인 보안이 탄생하고 발전된다는 것이다.

물론 블록체인 기술은 현재 상용화하기 위해서 해결해야 하는 문제들이 존재한다. 가장 핵심적인 문제는 속도이다.

일반인들이 오해하는 것 중 하나가 블록체인의 거래 속도가 초당 7건으로 거래 속도가 매우 큰 많은 응용서비스에서는 적합하지 않다는 것이다. 그러나 이는 비트코인의 거래 속도이며, 다양한 블록체인의 경우 응용서비스에 적합하도록 속도를 향상시킨 노력을 경주하고 있다. 인터넷이 처음 나왔을 때를 상기해 보자. 다들 기억하겠지만 초기 인터넷 속도는 2,400bps 정도였다. 그러나 인터넷 통신 속도는 매우 빠르게 발전되어 왔으며 현재는 속도 때문에 생기는 문제는 거의 없다. 마찬가지로 블록체인의 거래 속도 또한 빠르게 발전하리라 사료된다.

2016년에 일본의 금융회사들이 블록체인 스터디 그룹을 조직하여 블록체인 기반의 은행 간 지급결제 시스템에 대한 실험 및 검증을 한 결과 초당 1,500건의 충분한 거래 속도를 확보하였다(일본의 은행 간 속도 조건 : 1,388건)[9].

핀테크 산업은 블록체인패러다임이 금융 산업에 적용된 한 사례로 볼 수 있다. 즉, 핀테크 산업은 기존의 인터넷 기반의 금융 산업을 블록체인 기반으로 전환한 것이다.

핀테크 보안의 경우도 먼저 기존 인터넷 기반 금융 산업 보안에 대한 인식의 전환을 요구한다. 즉, 핀테크 보안은 인터넷 기반의 보안이 아닌 암호블록체인 기반의 보안을 고려하여야 한다.

기존 인터넷의 경우 TTP(서버) 기반의 정보보호 관점에 집중적으로 치중되어 있다. 그러나 암호블록체인 기반의 핀테크 산업은 TTP가 존재하지 않는다. 따라서 기존의 정보보호 관점에서 다루기에는 한계가 존재한다.

또한 앞서 이야기 했듯이 기존 인터넷은 단순한 정보통신망 역할이었으나, 암호블록체인의 경우 무결성을 보장하는 분산 DB, 암호화폐, 그리고 스마트계약 등 기본적인 데이터 및 거래에 대한 무결성 보장 기능 외에, 비밀성, 인증, 부인봉쇄 등 기본적인 4대 정보보호 기능과 개인정보보호 기능까지도 내포하고 있다. 이는 암호블록체인 기반의 핀테크 보안에서 상당 부분은 암호블록체인 기능으로 보장할 수 가 있다는 것을 의미한다.

따라서 핀테크 보안이란 기존의 인터넷 기반의 금융보안과는 달리, 암호블록체인이 보장하는 정보보호서비스를 제외한 핀테크 서비스 특성에 따른 보안에 집중하여야 한다. 대표적인 부분이 스마트폰 보안 분야로 생각할 수 있다. 즉, 서버보안이 아닌 클라이언트 보안 부문이다.

이는 정보보호 분야 역시 블록체인패러다임 관점에서 제조명해야 함을 의미한다.

공격 대상인 서버가 없는 블록체인의 경우 해커는 서버가 아닌 네트워크와 경쟁해야 한다. 비트코인 또는 이더리움을 해킹한다는 것은 무엇을 의미하는 건가? 비트코인 및 이더리움에 대한 다양한 해킹 소식이 전해질 때마다, 안타까운 것은 해킹의 의미에 대한 오해다. 예를 들어, 비트코인을 해킹했다는 것은 비트코인 자체가 아닌 클라이언트 지갑을 해킹한 사례이다. 이는 내 지갑에 있는 돈을 도난당했다는 것이며, 돈 자체 시스템에 대한 문제는 아닌 것이다.

암호블록체인패러다임에 근거하여 정보보호 분야도 새롭게

정립되어야 한다.

현재 다양한 관점에서 제기되고 있는 핀테크 보안은 암호블록체인으로 상당부분 해결할 수 있다고 생각한다.

Ⅲ. 결 론

본고에서는 암호블록체인패러다임을 역설하였다. 핀테크 산업이란 인터넷 기반의 금융 산업을 암호블록체인패러다임에 의한 암호블록체인 기반의 금융 산업을 의미한다.〈그림 8〉

이러한 관점에서 블록체인은 제2의 인터넷 또는 차세대 인터넷으로 간주할 수 있으며, 단순 정보통신망인 기존의 인터넷과는 달리 〈그림 8〉에서 알 수 있듯이 암호블록체인은 블록체인으로서의 분산 저장기술, 암호화폐 및 스마트계약 등을 가지고 있으며, 또한 기본적인 정보보호 4대 서비스와 개인정보보호서비스를 내포하고 있는 보안적으로 매우 우수한 차세대 인프라이다.

사이버패러다임에 의해 사이버보안을 고려했다면, 이제 블록체인패러다임에 의한 블록체인 보안을 연구 해야 한다. 이는 블록체인패러다임에 의한 정보보호 관점도 재조명되어야 함을 의미한다.

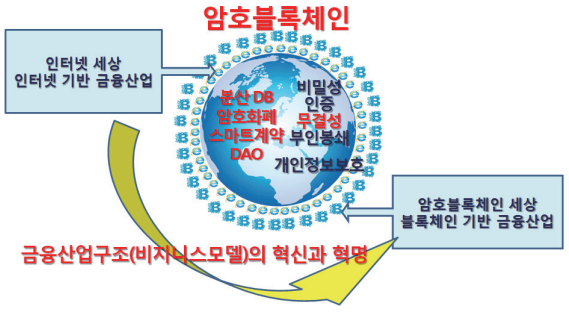

그림 8. 암호블록체인패러다임과 핀테크

암호블록체인상의 핀테크 보안은 블록체인이 가지고 있는 근본적인 정보보호 기능 외에 핀테크 산업의 다양한 서비스에 필요한 정보보호 조건들을 다시 분석하고 블록체인 인프라와 병행하여 정립해야 한다는 것이다.

참 고 문 헌

[1] ""Bitcoin: A Peer-to-Peer Electronic Cash System"" at https://bitcoin.org/bitcoin.pdf

[2] ""Corporate website of Ethereum Foundation"" at https://www.ethereum.org/

[3] 한국은행, "분산원장 기술과 디지털통화의현황 및 시사점", 2016년 1월

[4] Aggelos Kiayias, Alexander Russell, Bernardo David, Roman Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol", 2016년 12월

[5] ""Hyperledger Whitepaper"" at http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf

[6] ""The Ripple Protocol Consensus Algorithm"" at https://ripple.com/files/ripple_consensus_whitepaper.pdf

[7] ""About R3"" at http://r3cev.com/about/

[8] KPMG, "CONSENSUS", 2016년 8월

[9] 「Blockchain Study Group, Report on Practical Experiment of Blockchain Technology in Japanese Domestic Interbank Payment Operation, Nob. 30, 2016.」

약 력

박 성 준

1983년 한양대학교 이학사
1985년 한양대학교 이학석사
1996년 성균관대학교 공학박사
1983년~1994년 한국전자통신연구원 선임연구원
1996년~2000년 한국정보보호센터 기반기술팀장
2000년~2009년 ㈜비씨큐어 대표이사
2002년~현재 동국대학교 국제정보보호대학원 겸임교수
2016년~현재 동국대학교 국제정보보호대학원 블록체인연구센터 센터장
관심분야: 암호학, 블록체인