블록체인을 통한 핀테크 보안과 시사점

Security and Implications of FinTech based Block chain

이 지 용(한국과학기술원 산업경영연구소)

차 례

■ keyword : | 블록체인 | 핀테크 산업 | 보안기술 |

1. 서론

최근 해외 대형 투자회사들이 블록체인 도입을 적극 추진 중인 가운데 국내외 핀테크 산업에서도 블록체인 기술을 활용한 신서비스 개발에 큰 관심을 보이고 있다. 모든 금융사가 고객의 거래내역을 비밀스럽게 보관하기 위해서 비싼 보안 프로그램과 장비를 구축해야만 하는 상황을 고려할 때, 오히려 거래내역을 모든 사용자가 공유하도록 함으로써 위·변조의 가능성을 방지한다는 블록체인의 발상은 핀테크 산업에 대단히 큰 매력을 어필한다.

현재 금융권에서는 핀테크 활성화를 위한 다양한 정책 추진과 다양한 비즈니스 모델이 창출되고 있다[1]. 핀테크와 블록체인의 결합을 통해 금융거래의 비용·속도·보안성 등에 대한 다양한 논의가 이루어지고 있는데, 특히 보안성에 대한 이슈는 매우 큰 비중을 차지하고 있다. 블록체인을 통한 금융거래의 보안성 강화는 특히 심도있게 다루어지고 있는 이슈이다. 따라서 본고에서는 블록체인이 핀테크 기술과 결합하여 금융산업의 보안성 문제를 해결할 수 있는 키워드임을 확인하고, 구체적인 방안에 대해 논의해 보고자 한다.

2. 국내외 블록체인 기술 동향

2.1 블록체인 정의

블록체인은 2008년 사토시 나카모토(Satoshi Nakamoto)의 논문 'Bitcoin: A Peer-to-Peer Electronic Cash System[2]'을 통해 처음 소개되었다. 그의 논문에서 블록체인은 P2P기술 기반의 '분산형 장부'로 정의되며, 다음과 같은 설계 원리를 갖는다. 모든 네트워크 사용자는 거래장부 사본을 나누어 보관 하고, 가장 최근 10분 동안의 거래 내역을 갖고 있던 거래장부의 끝에 더한다. 기존의 장부가 손상될 경우 다른 사용자의 장부를 복제해 빈 곳을 메우는데, 임의의 조작을 방지하기 위해 참가자의 과반수가 인정한 거래 내역만 장부에 기록한다. 10분 간격으로 최신 상태로 업데이트된 거래장부 묶음이 '블록'이며, 블록들이 모인 거래장부 전체를 '블록체인이라 정의한다. 블록체인은 네트워크의 모든 참여자가 공동으로 거래 정보를 검증·기록·보관함으로써 제3의 공인기관 없이 거래 기록의 무결성 및 신뢰성을 확보한다[3].

2.2 블록체인 기술

초기의 블록체인 기술은 분산화 된 인증·검증 기술로 가상화폐의 발행·유통·거래에 제한되는 반면, 최근 등장한 차세대 블록체인 플랫폼들은 다양한 영역으로의 확장을 목표로 진화·발전하고 있다. 대표적인 예로 이더리움(Ethereum)을 들 수 있는데, 이는 가상화폐의 기능과 더불어 비트코인의 거래스크립트를 다양한 형태로 프로그램 가능하게 만든 스마트계약(Smart Contract)을 구현함에 따라 다양한 분산 어플리케이션(부동산 계약·온라인 투표 등)을 개발하고 구동할 수 있는 플랫폼으로 확장되고 있다[3].

블록체인 기반기술은 크게 네 가지(P2P네트워크·암호화·분산 장부·분산 합의)로 구성된다(표 1). 이 기술

들은 블록체인의 가치라 할 수 있는 탈중앙화, 데이터 무결성 유지 등을 위해 상호 보완적인 관계를 취하고 있으며 블록체인 동작 매커니즘의 근간을 이룬다.

3. 핀테크 산업과 블록체인

핀테크(Fintech)란 금융(Finance)과 기술(Technology)의 합성어로 IT기술에 기반 새로운 형태의 금융서비스를 지칭한다. 모바일 인터넷 환경의 발달과 인공지능·소셜 네트워크 서비스·빅데이터·블록체인 등 첨단 ICT가 금융산업과 융합하면서 새로운 금융기술인 '핀테크'의 열풍으로 발현되고 있다. 핀테크 산업을 통해 제공되는 새로운 서비스는 지급결제·대출(P2P)·전자화폐·증권 및 금융정보·인터넷 전문은행 등이 있다. 특히 지급결제 분야에서 집중적인 투자가 이루어지고 있는데, 이는 모든 금융 서비스 및 거래가 지급과 결제를 통해 국내 지급결제 시장의 규모가 급격히 증가하면서(전년도 대비 2015년에 58.4%로 증가) 지급결제 과정에서의 보안문제가 핵심 이슈로 떠올랐고[9][10], 핀테크 산업을 위한 새로운 보안기술로 블록체인이 주목받고 있다.

표 1. 블록체인 기반기술

기술	설명
P2P 네트워크	·(개념) 블록체인 참여자들 간의 연결 및 통신 기반으로 동등한 계층의 참여자들로 구성 ·(종류) 구조적 P2P(Structured P2P)와 비구조적 P2P(Unstructured P2P)*로 분류 - *중앙집중형 방식(서버중심의 망 구성)과 분산형 방식(데이터의 flooding 알고리즘 기반)으로 구분 ·통신시 UDP(User Datagram Protocol) 사용 vs (블록체인) TCP/IP 사용 - 블록체인의 참여자들은 자신과 물리적으로 가장 인접한 참여자들의 IP를 사용하여 메시지 및 데이터를 교환 (ex. 비트코인의 경우 IP 3개 유지)
암호화	·(기술1) 머클 트리(Merkle Tree): 데이터의 무결성 검증 - 해시트리의 일종으로 모든 비-리프(non-leaf)노드의 이름이 자식 노드들의 해시로 구성된 트리[4] ①(리프노드) 파일이나 특정 값 등의 데이터 ②(상위노드) 각각의 자식 노드들의 해시 값 ③(로트노드) 트리를 구성하는 모든 리프 토드들의 데이터의 해시 값 - 루트 노드의 해시 검증을 통해 데이터들의 위·변조를 검증 - 블록체인에서는 리프 노드에 참여자들 간의 거래, 정보 들을 삽입, 주로 SHA-256 함수를 사용 ·(기술2) 공개키 기반 디지털 서명: 거래 부인 방지 - 사전에 비밀 키를 나누어 가지지 않은 참여자간의 안전한 통신을 이루어지게 하는 암호화 기술(ex. 본인 인증) - 두 개의 키가 존재 ①(공개키) 모든 참여자들이 공유 → (블록체인) 거래의 유효성 검증 ②(비밀키) 해당 소유자만 보유 - 사용자가 해당거래에 서명(비밀키) →블록체인 네트워크에 거래정보 전송(공개키) →거래 정보 수신자(모든 참여자들)는 해당거래의 유효성 검증(송신자의 공개키) →해당 정보를 블록체인 참여자가 보냈음을 확인
분산 장부	·(개념) 네트워크에 속한 모두와 공유된 암호화되고 변경할 수 없는 거래 기록의 리스트[3] - 분산 장부의 기록에 대한 참여자들의 합의를 전제로 P2P 네트워크상에 적용(블록체인에서도 동일) ·(블록체인) 모든 거래·정보에 대해 참여자들의 검증 후 기록, 모든 참여자가 동일한 정보유지 ·(특징) 블록체인이 제공하는 데이터 무결성 보장의 바탕 - 모든 블록체인 참여자들은 동일한 분산 장부의 데이터를 유지 →데이터 위·변조 및 이중거래 시도시 높은 비용과 컴퓨팅 리소스가 필요 ·(한계) 높은 저장용량 요구/용량 지속적 증가→블록체인의 확장성과 사용성을 제한
분산 합의	·(개념) 분산 컴퓨팅과 멀티 에이전트 시스템등의 분야에서 결함이 있는 프로세스가 있는 경우, 전반적인 시스템의 신뢰성을 달성하기 위하여 프로세스나 에이전트 간의 특정 데이터 값에 대한 동의를 이끌어내는 프로토콜[5] ①유효성(Validity): 모든 올바른 프로세스들이 동일한 데이터를 제안할 경우, 모든 프로세스들이 제안된 데이터에 유효·무효를 결정 ②무결성(Integrity): 모든 올바른 프로세스들이 하나의 데이터를 채택할 경우, 그 데이터는 다른 프로세스에 의해 제안된 데이터를 의미 ③동의(Agreement): 모든 올바른 프로세스들은 반드시 어떤 데이터에 대해 동의를 해야 함 ④종료(Termination): 모든 올바른 프로세스들은 어떤 데이터들에 대해 결정을 내려야 함 ·(비트코인) 작업 증명(Proof-of-work)[1]프로토콜을 사용 - 참여자들이 블록으로 저장되기 위한 거래 및 데이터들과 SHA-256 해시 함수를 사용하여 시행착오 방식으로 특정해시 값을 찾아내는 '작업'을 함으로써 참여자간의 블록정보에 대한 합의도출 - 많은 양의 소요시간(평균 약 10분)·전력 및 컴퓨터 리소싱 낭비 문제 발생 → 사용 지양 추세 ·(최근 블록체인) 지분증명(Proof-of-stake)[6] 알고리즘을 사용 - 투표기반 합의 알고리즘 - 보안성은 작업 증명 합의보다 낮아졌지만 합의 속도, 전력낭비 문제를 해결 - 이를 기반으로 위임지분증명(DelegatedProof-of-Stake)[7], PBFT(Practical Byzantine FaultTolerance)기반의 Tendermint[8] 등의 합의 알고리즘이 개발되어 활용

4. 국내 핀테크 산업의 발전방향 및 시사점

공인인증서와 같은 복잡한 인증절차를 거쳐야했던 기존의 결제시스템에서, '모바일 페이'라는 비교적 간편한 플랫폼을 활용한 서비스의 확장으로 젊은 층 뿐만 아니라 기존의 결제수단을 사용하는 이용자 역시 새로운 핀테크의 패러다임에 자연스럽게 빠져들고 있다. 보안성이 높고 저렴한 관리비용, 그리고 빠른 데이터 처리속도를 가진 블록체인 기술은, 이러한 패러다임에 맞는 글로벌 금융시스템의 새로운 기회로 부상하고 있다. 블록체인기술이 갖는 혁신성은, 핀테크의 발전을 더욱 가속화시킬 수 있는 기술이다. 새로운 보안체계를 구축할 뿐만 아니라, 거래비용의 절감 차원에서도 비즈니스모델로서 큰 가능성을 보여주고 있다. 블록체인 기술은 금융분야 뿐만 아니라, 물류・유통에서 정부의 공공·행정서비스까지 적용될 수 있는 4차 산업 혁명의 핵심 기술이지만[11], 법적 규제의 한계성을 넘어서야 한다. 블록체인 도입 시 개인정보보호법 제2조(정의), 제3조(개인정보 보호 원칙)에서 아직까지 그 한계를 찾아 볼 수 있다.

또한, 한국블록체인협회와 더불어 한국인터넷진흥원(KISA)는 블록체인 산업 활성화와 관련한 대응에 더욱 속도를 대고 있는데, 2016년에 발족한 블록체인 TF(Task Force)의 운영과, 블록체인 기술 활용 가능성을 검증하기 위한 실증 시범사업도 추진하고 있다. 하지만, 세계적으로도 블록체인기반 기술 개발이 초기단계 이기 때문에, 국내 금융업계 다수의 기관들과 협업하여 공동연구를 추진하거나, 이해관계에 있는 다른 단체와 적극적인 논의를 할 수 있는 구조의 개선이 필요하다. 법적·제도적 측면에서의 협의와 시스템의 요구에 맞춘 표준에 대한 논의가 선행된다면, 많은 신규 블록체인 스타트업과 국내 금융기관과의 제휴 뿐 만 아니라, 비금융 분야에서도 기존의 시스템을 대체할 수 있는 서비스를 도입·개발 할 수 있는 환경이 구축될 것이다.

참 고 문 헌

[1] 박성준 (2017), "블록체인패러다임과 핀테크 보안", 정보통신학회지, Vol. 34(3), pp. 23-28

[2] Satoshi Nakamoto (2008), "Bitcoin: A peer-to-peer electronic cash system"

[3] 정보통신산업진흥원 (2008), 블록체인 기술의 이해와 개발 현황 및 시사점, 이슈리포트 2018-제13호

[4] https://ko.wikipedia.org/wiki/%ED%95%B4%EC%8B%9C_%ED%8A%B8%EB%A6%AC

[5] Coulouris, George, Jean Dollimore, Tim Kindberg (2001), Distributed Systems: Concepts and Design (3rd Edition), Addison-Wesley, p. 452, ISBN 0201-61918-0

[6] VASIN, Pavel. Blackcoin's proof-of-stake protocol v2. 2014

[7] LARIMER, Daniel. Delegated Proof-of-Stake (DPOS)Bitshare whitepaper, 2014

[8] KWON, Jae (2014), "Tendermint: Consensus without mining" (URL http://tendermint. com/docs/tendermint {_} v04.pdf)

[9] 이수정, 변해민, 박유리, 전정훈, "핀테크 산업에서 블록체인 도입의 한계점", 정보처리학회지, Vol. 24(3), pp. 22-29

[10] 박병주, 최슬기, 김득훈, 곽진 (2017), "국내・외 핀테크 서비스 및 정책 동향 분석", 한국통신학회지(정보와 통신), Vol. 34(3), pp. 4

[11] 미래창조과학부 (2017), 「미래부, 정보보호 분야 블록체인 기술 적용 시범사업 추진」 보도자료

저 자 소 개

● 이 지 용(Ji Yong Lee)

- 2007년 2월 : 한국과학기술원 산업 및 시스템공학과 (공학사)
- 2009년 2월 : 한국과학기술원 산업 및 시스템공학과 (공학석사)
- 2017년 8월 : 한국과학기술원 산업 및 시스템공학 (공학박사)
- 2018년 1월 ~ 한국과학기술원 산업경영연구소 선임연구원

<관심분야> : 경영정보시스템, 전자상거래, 빅데이터, 정보보안