블록체인(Blockchain) 개요 및 활용사례

(보안연구부 보안기술팀 / 2015.6.24)

□ 개요

○ 블록체인(Blockchain)이란 블록(Block)을 잇따라 연결(Chain)한 모음[1]으로 블록에 일정 시간 동안 확정된 거래내역을 담는 일종의 금융장부임

○ 블록체인 기술은 P2P(Peer-to-Peer) 네트워크에서 발생하는 모든 거래(Transaction)정보를 담고 있는 원장(블록체인)을 모든 노드(Peer)가 저장 및 업데이트 하고 무결성을 유지하도록 하는 기술임

○ 비트코인(Bitcoin)[2]에서부터 시작된 블록체인 기술은 최근 핀테크 기술과 융합되어 기존 중개자 역할을 대체하고 있음

□ 블록체인

○ **(구조 및 동작)** 블록체인은 이전 블록의 정보(해쉬 값), 현재의 거래정보 및 해쉬 값 등을 포함하여 블록을 생성하므로 블록의 내용을 조작 할 수 없으며, 거래 정보가 공개되어 있기 때문에 투명하게 관리가 가능함

< 블록체인의 기본 구조 >

자료 : BITCOINIST.NET, Thoughts on Bitcoin Block Size Economics 그림 재구성

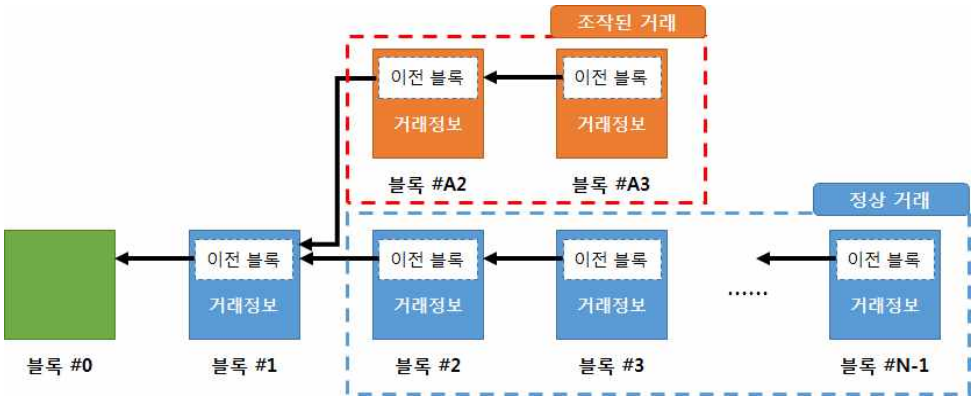
1) 과반수 이상의 사용자가 동의한 거래내역만 보관할 블록으로 묶고, 새로 만든 블록은 이전 블록체인 뒤에 덧붙이는 과정을 반복함

2) 비트코인(Bitcoin)은 2009년 나카모토 사토시(Nakamoto Satoshi)가 만든 디지털 통화로, 통화를 발행하고 관리하는 중앙 장치가 존재하지 않는 구조를 가지고 있다. 비트코인의 거래는 P2P 기반 분산 데이터베이스에 의해 이루어지며, 공개 키 암호 방식 기반으로 거래를 수행함
자료 : 위키피디아 비트코인, 블록체인 내용 재구성

○ **(안전성)** 각 블록체인은 구성 요소[3]가 이전 블록체인과 연관되어 있으며, 비트코인의 경우, 해시함수(SHA-256)의 암호학적 특성[4]을 이용하므로 무결성을 보장함

- 해쉬값을 악용하여 조작된 거래의 블록체인을 생성할 수 있지만, 블록체인의 길이는 신뢰성을 의미하므로 조작된 블록체인은 자연히 제거됨

< 조작된 거래가 포함된 블록체인 구조 >



자료 : 위키백과, bitcoin의 블록체인 설명 재구성

○ **(특징)** 블록체인은 거래장부를 P2P 네트워크상에 공유·관리하고, 이용자가 직접 블록체인을 생성·검증 할 수 있음

구분	내 용
제3자 없는 신뢰성 보장	블록체인 시스템 자체가 그 안에 담긴 기록의 무결성을 증명·보증하므로, 은행·신용카드사 등에서 신뢰성을 담보할 중앙 집중적 조직이나 제3자가 필요 없음
경제성	블록체인의 신뢰성을 담보할 중앙집중적 조직이나 구조가 필요 없어, 시스템 구축 및 유지보수 비용이 적어 금융거래 비용절감효과 가짐
안전성	모든 사용자(노드)가 거래장부를 갖고 있기 때문에 네트워크 일부에 문제가 생겨도 전체 블록체인에 영향이 없으며, 인터넷처럼 분산된 구조로 중앙 집중적인 기존 금융 시스템보다 안전함
거래내역의 투명성	기존 금융거래는 금융회사와 거래 당사자 사이 비밀이나, 블록체인은 모든 거래내역을 기록, 공유하여 기존 금융시스템보다 투명하고 추적이 용이함
개인정보보호	휴대폰만 있어도 블록체인을 통해 금융서비스를 이용할 수 있어, 금융회사는 개인정보를 수집·보관·유출의 부담이 줄어듦

3) 비트코인 블록의 경우, 약 10분간의 비트코인 거래내역과 바로 이전 블록의 해시(hash), 논스(nonces, 거래 데이터를 해시하기 전에 더해지는 난수 값) 등을 포함하며, 한번 쓰여진 블록은 조작이 불가능하며 누구나 볼 수 있는 공공장부의 성격을 가짐 비트허브, [Weekly심층기획] 삼성전자와 IBM이 반한 비트코인 블록체인 기술, 2015.4.23

4) A라는 원본에서 해시를 만드는 것은 쉽지만 역으로 해시해서 원본을 만드는 것은 암호학적으로 불가능에 가까우며, 해시함수는 블록체인이 조작되었는지 확인하는 용도로 사용됨

□ 블록체인 활용 사례

○ 비트코인, P2P 대출, 주식 거래(거래 인증), 공인인증서 등 기존 중개자 역할을 대체하는 곳에서 활용범위를 넓혀나가고 있음

구분	내 용
비트코인	디지털 통화로 발행하고 관리하는 중앙 장치가 존재하지 않는 구조를 가지고, 거래는 P2P 기반 분산 데이터베이스를 이용한 공개키 암호 방식 기반으로 거래를 수행. 거래내역이 가입자간 모두 공개되며, 익명성을 보장할 뿐만 아니라 수수료가 거의 없음
P2P 대출	개인 투자자들이 금전을 맡기면, 대출을 원하는 이용자들의 평판 정보를 분석하여 금전을 빌려줌으로써 발생되는 수익을 개인 투자자들에게 분배해주는 서비스. 투자자 및 대출자의 금전은 블록체인을 이용하여 투명성 및 신뢰성을 보장함
주식 거래 (거래 인증)	나스닥의 프라이빗 마켓은 변호사에게 거래를 승인받도록 하여 거래 속도가 느렸으나, 이 과정을 블록체인으로 대체하여 모든 거래를 자동으로 검증하는데 이용할 계획임
공인인증서	기존 인증기관의 역할을 피어(peer)들간의 트랜잭션을 보안해주고, 무결성 또는 투명성을 갖춤에 따라 공인인증서의 역할을 대신함

자료 : BREAKING NEWS, [블록체인 속 핀테크]②P2P 금융혁신 내용 재구성

□ 시사점

○ **(새로운 금융 비즈니스 모델 제공)** 비트코인의 경우처럼 해당 기술을 시스템에 적용 및 확장하여 다양한 비즈니스 모델이나 도메인에 적용하기 쉬우며, 복잡한 네트워크 솔루션이나 중앙화된 생태계 구축이 필요 없음

○ **(거래기록 증명 방식의 변화)** 블록체인 구조상에서 자동으로 장부가 기록되기 때문에 블록체인은 거래를 기록하고 증명하는 방법(거래의 투명성 제공)에 거대한 변화를 가져올 것임

○ **(제3자 없는 신뢰성 및 보안성 제공)** 기존의 PKI기술을 활용한 제3의 신뢰기관이 필요한 전자서명에 적용되는 기술보다 분산구조로 신뢰성, 프라이버시 보호 등의 보안성을 높일 수 있음

○ **(경제효과의 극대화)** 중앙 집중적 조직이나 구조가 필요 없어 금융거래 비용절감효과 가짐

- 영국의 중앙은행인 영란은행도 블록체인 기술이 금융시장에 적용되면 거래의 투명성이 보장되고 거래 수수료도 크게 저렴해질 것으로 예상[5]함

5) 비트허브, [Weekly 심층기획] 비트코인 블록체인 기술을 삼성전자와 미국 IBM, 도입계획, 2015.4.10