Ⅱ. 블록체인의 이해

1. 블록체인의 의미

블록체인이란 P2P(Peer to Peer) 네트워크를 통해서 관리되는 분산 데이터베이스의 한 형태로, 거래 정보를 담은 장부를 중앙 서버 한 곳에 저장하는 것이 아니라 블록체인 네트워크에 연결된 여러 컴퓨터에 저장 및 보관하는 기술로 다양한 분야에 활용이 가능한 기술이다. 블록체인은 분산원장 기술(DLT: Distributed Ledger Technology)이라고도 불리며, 이는 거래 정보를 기록한 원장 데이터를 중앙 서버가 아닌 참가자들이 공동으로 기록 및 관리하는 것을 의미한다.

블록체인은 분산처리와 암호화 기술을 동시에 적용하여 높은 보안성을 확보하는 한편 거래과정의 신속성과 투명성을 특징으로 한다. 보안성의 강화로 해커의 공격과 데이터의 왜곡 그리고 기존 중앙집중 서버 방식(Central Server)에서 가장 큰 문제인 디도스 공격을 원천적으로 방어할 수 있다. 그리고 블록체인 플랫폼을 이용하면 제3자의 거래에 의존하던 여러 과정들을 생략할 수 있어, 그에 따른 비용을 획기적으로 절약할 수 있다. 제 3자가 거래 중심의 보장 및 증명서비스의 항목들을 블록체인 시스템에 수렴할 수 있다.

보안성이 높고 위·변조가 어렵다는 특성 때문에 데이터 원본의 무결성 증명이 요구되는 다양한 공공·민간 영역에 적용되고 있으며, 새로운 신뢰사회 구현의 기반 기술로 주목받고 있는 중이다. 또한, 블록체인 기술은 거래 장부인 데이터뿐 아니라 거래 계약도 중간 신뢰 담당자(Trusted Third Party) 없이 거래를 할 수 있는데 이것이 바로 앞서 언급한 스마트계약(Smart Contract)이다.

현재, 블록체인은 해외 송금서비스, 장외주식, 채권, 마일리지 등 거래, 디지털 통화

발행 및 이체서비스 등 다방면에 걸쳐 다양한 형태로 적용되기 시작하였으며, 금융 분야뿐만 아니라 지역화폐(Local Currency) 및 물류·유통, 에너지산업 등 다양한 분야에서 활용될 것으로 평가된다.

〈표 Ⅱ-1〉 금융업의 블록체인 적용 분야

분야	기능 및 효과
인증	• 별도의 공인인증기관 없이 간편하고 안전한 대체 인증수단 제공
결제 및 송금	• 소액 결제 및 해외 송금서비스의 보안성 제고 및 수수료 비용절감
증권거래	• 통화, 장외주식, 파생상품 등의 거래에 소요되는 거래시간의 획기적 단축
스마트계약	• 조건에 의해 거래가 자동적으로 성립됨에 따라 중간관리자에 의한 사기, 위조 방지
대출·투자·무역거래	• 중개자를 배제한 비대면 P2P 대출서비스 • 크라우드 펀딩을 통해 소액자금 조달 및 투자 • 송장 정보 공유를 통한 송장 사기방지

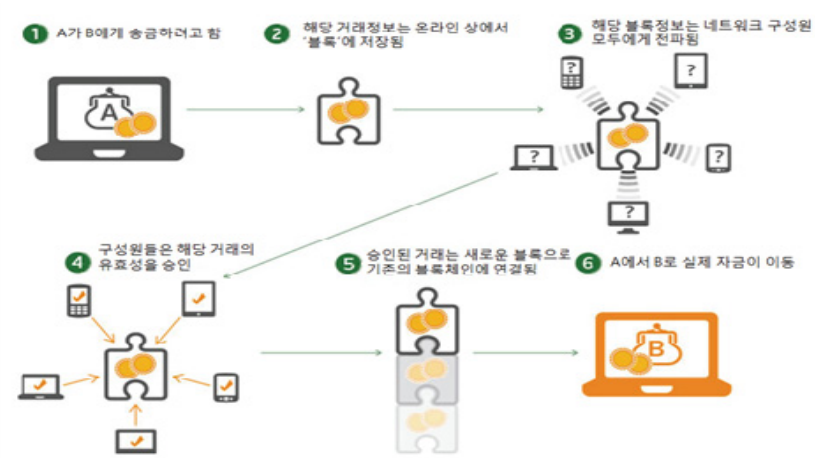
자료: 서정호·이대기·최공필(2017)

2. 블록체인의 원리

블록체인 기술은 거래정보를 기록한 원장 데이터를 중앙 서버가 아닌 네트워크에 참가하는 모든 공동체가 거래를 기록하고 관리하는 P2P[12](Peer to Peer, 개인 대 개인) 거래를 지향하는 탈중앙화를 핵심 개념으로 하는 기술이다. 기존 금융 시스템에서는 금융회사들이 중앙 서버에 거래 기록을 보관해 온 반면, P2P 방식을 기반으로 하는 블록체인에서는 거래 정보를 블록에 담아 차례대로 연결하고 이를 모든 참여자가 공유한다.

12) P2P란 서버나 클라이언트 없이 개인 컴퓨터 사이를 연결하는 통신망을 말하며, 연결된 각각의 컴퓨터가 서버이자 클라이언트 역할을 하며 정보를 공유하는 방식임

〈그림 Ⅱ-1〉 블록체인을 통한 거래 방법



자료: Thomson Reuters(2016. 1. 16), "lock-chain technology: Is 2016 the year of the block-chain"

거래 과정은 다음과 같이 이루어진다. ① A가 B에게 송금 희망 등의 거래 요청을 한다. ② 해당 거래 정보가 담긴 블록이 생성된다. ③ 블록이 네트워크상의 모든 참여자에게 전송되면, ④ 참여자들은 거래 정보의 유효성을 상호 검증한다. ⑤ 참여자 과반수의 데이터와 일치하는 거래내역은 정상 장부로 확인하는 방식으로 검증이 완료된 블록은 이전 블록에 연결되고, 그 사본이 만들어져 각 사용자의 컴퓨터에 분산 저장된다. ⑥ A가 B에게 송금하여 거래가 완료된다.

이렇게 거래할 때마다 거래 정보가 담긴 블록이 생성되어 계속 연결되면서 모든 참여자의 컴퓨터에 분산 저장되는데, 이를 해킹하여 임의로 수정하거나 위조 또는 변조하려면 전체 참여자의 과반수 이상의 거래 정보를 동시에 수정하여야 하기 때문에 사실상 불가능하다. 따라서 접근을 차단함으로써 거래 정보를 보호·관리하는 기존의 금융 시스템과는 전혀 달리, 블록체인에서는 모든 거래 정보를 누구나 열람할 수 있도록 공개한 상태에서 은행 같은 공신력 있는 제3자의 보증 없이 당사자 간에 안전하게 거래가 이루어진다.[13]

13) 보험사나 보험 산업은 프라이빗(폐쇄형) 블록체인을 도입하게 될 가능성이 높은데 이 경우 참여하는 노드 수(분산되어 데이터를 저장되는 주체의 수)가 매우 적은 경우 해커나 외부 침입에 다소 취약할 수도 있음

3. 블록체인 적용 시 기대효과

블록체인 기반인 분산원장 기술(Distributed Ledger Technology, DLT)의 일반적인 장점은 보안성의 강화, 처리과정의 신뢰성 증진과 감시 가능성의 확대, 비용절감 등이다. 그러나 현재까지 소개되고 있는 분산원장 기술의 활용 사례들은 일반적인 장점들을 모두 수용하기보다는 각각 독특한 편익과 결점을 지니고 있다.[14] 이는 아직까지 분산원장 기술이 발전 초기단계에 있고, 대규모의 성공적인 실험에는 한계가 있음을 보여주고 있다. 비록 방대한 이론적 해법과 소규모의 개념 증명(Proof of Concept)이 가능성을 보이고 있지만 시스템의 호환성, 법과 규제의 강제 가능성 등에서 문제를 보이고 있는 것도 사실이다.

현재 분산원장은 기술적으로 이중지불이 방지되는 인증된 거래, 데이터의 추적과 투명한 거래, 해킹이 불가능한 생태계에 기반을 두어 활용되고 있다. 이러한 서비스의 공통적인 특징은 제3자의 중개에 의존하지 않는 비즈니스 모델로 상당한 비용절감 효과를 발휘할 수도 있다는 것이다.

블록체인을 기업에 전사적으로 도입하기 위해서는 상당한 시간 및 비용이 소요되겠지만 성공적으로 도입하는 경우 비용절감 효과도 클 것이다. 비용절감 효과는 크게 IT 시스템과 기업경영 측면으로 구분하여 볼 수 있다. IT시스템 측면에서는 응용기술 개발비용, 인프라 장비 조달비용, 중간구조 개발비용 등의 절감을 거둘 수 있고, 기업경영 측면에서는 회계감사 비용, 종이서류 관리비용, 노동비용 등의 절감을 가져올 수 있다.

14) 권혁준 외(2016)

〈표 Ⅱ-2〉 블록체인 기술의 잠재적 편익과 장애요인

잠재적 편익	장애요인
거래 속도의 증가	• 분산원장 기술별로 환경이 달라 공개와 비공개, 가장 적절한 합의 방법과 그에 따른 에너지 소모 등의 차이 존재
정확성의 증가와 인적오류 감소	• 분산원장의 규모성과 현존 솔루션 간의 경합 능력이 불확실함 • 특히 대규모의 빠른 응용에서는 아직까지 분산원장의 승인 과정이 느림
사기의 기회 감소	• 분산원장 기술별이나 현존 비분산원장 기술과의 호환성이 검증되지 않아 현존 시스템의 혁신위험과 내부부서 간 승인 및 책임 문제 존재
효율성 증진과 인프라비용 감소	• 기업 비밀정보의 공유는 원치 않기에 산업 표준의 제정에 아직 회의적임
거래의 투명성과 감시 가능성 증가	• 기술개발 이전에 규제기관의 지원이 필요한 산업이 있으나 규제기관 간의 부조화로 개혁을 제한할 수 있음 • 분산원장에 탑재되는 자산의 다양성은 다수의 규제기관의 개입 개연성을 높이며, 분산원장 기술의 실패를 대비한 응급 대책을 요구
악성공격에 대한 회복력 증가	• 디지털화된 자산에 대해 데이터의 소유자, 보유자, 보유처, 국가 간 규제, 스마트계약의 코팅에러 등 대비 필요
보안성 강화	• 해커의 공격 가능성과 프라이버시의 인정 범위
응용가능성 확대	• 분산원장 기술의 비용 효율성은 요구되는 투자와 실행 위험에 대비되어야 함

자료: Mody's Investor service(2016. 7)

권혁준(2016)은 분산원장 기술을 적용 시 자본시장 기준으로 16%의 비용과 청산 및 결제의 시간(T+2)을 절약할 수 있다는 추정치를 제시하였다.[15] 해외의 다수 보고서도 블록체인의 적용의 초기 효과로서 후선비용(Back office cost)의 감소를 보고하고 있다.

15) 권혁준 외(2016)

4. 블록체인의 유형

가. 블록체인의 종류와 특징

블록체인은 활용되는 목적에 따라 3가지 종류로 나뉘며 각 블록체인마다 특징이 있다.

퍼블릭 블록체인(Public Blockchain)은 개방형 블록체인으로 누구나 트랜잭션을 생성할 수 있어 앞에서 설명한 공공거래장부에 해당하며, 통상 블록체인이라 하면 퍼블릭 블록체인을 지칭한다. 퍼블릭 블록체인은 누구나 참여할 수 있고 모든 참여자의 상호 검증을 거쳐 신뢰도가 높다. 트랜잭션 내역이 모두에게 공개되어 네트워크에 참여한 모든 노드(Node)가 이를 검증하고 거래를 승인하기 때문이다. 하지만 모든 참여자의 거래 기록을 남기고 이를 공유하느라 처리 속도가 느리다는 단점이 있다.

프라이빗 블록체인(Private Blockchain)은 폐쇄형 블록체인으로 퍼블릭 블록체인의 상대적 개념이다. 프라이빗 블록체인은 서비스 제공자(기업 또는 기관)의 승인을 받아야만 참여할 수 있으며 주로 기업에서 활용하여 엔터프라이즈 블록체인(Enterprise Blockchain)이라고도 한다. 여러 기업(또는 기관)이 공동으로 참여하는 컨소시엄 블록체인(Consortium Blockchain)도 넓은 의미에서 프라이빗 블록체인의 범주에 속한다.

〈표 Ⅱ-3〉 블록체인의 종류와 특징

구분	Public Blockchain	Consortium Blockchain	Private Blockchain
관리자	모든 거래 참여자	컨소시엄에 소속된 참여자	한 중앙 기관이 모든 권한 보유
거버넌스	한번 정해진 법칙을 바꾸기 매우 어려움	컨소시엄 참여자들의 합의에 따라 법칙을 바꿀 수 있음	중앙 기관의 의사결정에 따라 용이하게 법칙을 바꿀 수 있음
거래속도	네트워크 확장이 어렵고 거래 속도가 느림	네트워크 확장이 쉽고 거래 속도가 빠름	네트워크 확장이 매우 쉽고 거래 속도가 빠름
데이터 접근	누구나 접근 가능	허가 받은 사용자만 접근 가능	허가 받은 사용자만 접근 가능
식별성	익명성	식별 가능	식별 가능

〈표 Ⅱ-3〉 계속

구분	Public Blockchain	Consortium Blockchain	Private Blockchain
거래증명	PoW, PoS 등 알고리즘에 따라 거래 증명자가 결정됨. 거래 증명자가 누구인지 사전에 알 수 없음	거래 증명자가 인증을 거쳐 알려진 상태 사전에 합의된 규칙에 따라 거래 검증 및 블록 생성이 이루어짐	중앙 기관에 의하여 거래 증명이 이루어짐
활용사례	비트코인	R3 CEV	나스닥 비상장 주식 거래소 플랫폼인 '링크(Linq)'

자료: 김신정·김하은·염용진(2017. 6)

프라이빗 블록체인은 법적 책임을 지는 기관만 트랜잭션을 생성할 수 있다. 또한 프라이빗 블록체인에서는 승인된 기관만 트랜잭션을 검증하고 거래를 승인한다. 프라이빗 블록체인은 승인받은 노드만 참여하고, 다른 노드의 검증을 구할 필요가 없기 때문에 처리 속도가 훨씬 빠르다. 하지만 프라이빗 블록체인의 사용자는 서비스 제공자에게 전적으로 의존해야 하기 때문에 퍼블릭 블록체인에 비하여 신뢰성에 한계가 있다. 하지만 프라이빗 블록체인에서 발생하는 시간상의 트랜잭션을 해쉬 함수를 만들어 퍼블릭 블록체인에 저장하는 방식, 앵커링(Anchoring)[16]으로 신뢰성을 극복하며, 이러한 기술적 발달이 프라이빗 블록체인의 여러 문제를 해결하고 있다.[17] 이러한 앵커링 적용은 앞으로 프라이빗 블록체인의 진본성과 악의적 왜곡의 합의를 방지할 수 있는 가장 획기적인 신기술로 적용되어지고 있으며, KB국민카드 프라이빗 블록체인 또한 앵커링 시스템을 통해 시행되고 있다.

한국조폐공사가 추진 중인 블록체인 공공 플랫폼의 경우도 앵커링 시스템을 포함시키는 플랫폼으로 설계되어 진본성을 퍼블릭 블록체인 노드의 참여로 보증하고 있다.

16) (주)코인플러그 특허(2015)

17) 각 당사자의 중앙이 따로 있는 상태에서 서로 다른 프라이빗 블록체인 플랫폼을 연동할 경우 표준화 문제가 대두될 것임. 또한 블록체인은 역가역성 문제를 가지고 있어 한번 생성된 블록은 지울 수도 수정할 수도 없어 사용자와 블록 허용자(블록의 생성자)는 이에 대한 방안과 수정에 따른 초과 블록을 염두에 둬야 함. 프라이빗 블록체인은 블록의 사이즈와 트랜잭션을 참여하고 있는 합의 알고리즘의 합의에 의한 임의의 프로토콜 수정이 가능하므로 각 보험사들은 프라이빗 블록체인의 사이즈와 트랜잭션의 정책도 사전에 수립해야 할 것임

프라이빗 블록체인의 설치는 네트워크 참여 컴퓨터(Node)의 개수 조정으로 설치비용의 감소를 기존 Server 중심의 비용을 줄일 수 있다. 블록체인 플랫폼은 기존의 서비스 단위의 개별 서비스마다 만들어내는 단일 프로그램이 아니라 여러 가지 응용 프로그램을 한 플랫폼에 서비스 할 수 있다(증명, 서류, 보험금 지급, 토큰의 생성 등).

컨소시엄 불록체인은 프라이빗 블록체인의 확장으로써 서로 다른 프라이빗 블록체인의 결합으로 각기 다른 블록체인에서 생성한 이질적인 블록을 오더링이라는 프로세스로 연결하여 신뢰성의 확보 및 확장성을 가진 블록체인이다.

5. 블록체인의 기술적 개념

가. 해시함수

블록체인, 암호화폐 기술에 대한 내용에 매번 등장하는 것 중 하나가 해시함수(Hash Function)이다. 해시함수의 해시(Hash)는 '어떤 데이터를 고정된 길이의 데이터로 변환'하는 것을 의미한다.[18] 해시함수를 거치면 원본 데이터를 알아볼 수 없도록 특수한 문자열로 변환이 되는데, 해시함수는 압축이 아니라 단방향 변환이기 때문에 해시값을 이용해서 원본 데이터를 복원할 수 없다는 특징을 가지고 있다.

1) 해시함수의 유용성

해시함수는 다음과 같은 성격이 있기 때문에 보안에서 유용하게 쓰인다. 원본 데이터에 아주 작은 변화만 있어도 완전히 다른 해시값이 만들어지게 된다. 예를 들어 '안녕하세요. snowdeer 입니다.' 문장에 마침표 하나만 더 찍어도 해시값은 'n4k3049fjdId843jKiro23jf50l3sL23'와 같이 완전히 다른 값이 나오게 되는 것이다. 즉 해시함수를 이용하게 되면, 원본 데이터의 사소한 변화도 쉽게 확인할 수 있게 된다. 또한 해시

18) 스팀잇 홈페이지, [블록체인]-해시함수 이해 4(https://steemit.com/kr/@endiyou/1)

함수는 눈사태 효과 덕분에 전자 서명, 증명서 등에서 해시값을 많이 활용하고 있다.[19] 본문에 약간의 수정만 가해져도 해시값이 완전히 달라져 위·변조 판별이 용이하기 때문이다. 블록체인의 해시함수가 양방향 변환이 가능했더라면 암호화에 쓰일 수가 없었을 것이다. 하지만 해시함수는 단방향 변환이며, 복원이 불가능하기 때문에 블록체인 기술 및 전자 서명 등 암호화에 사용될 수 있다.

각종 서버에서 사용자 정보들, 특히 비밀번호 등을 해시값으로 변환해서 저장하는 이유도 이러한 해시함수의 단방향 변환 성질 때문으로 볼 수 있다. 만약 서버가 해킹을 당해 사용자 정보가 유출이 되더라도 해시값으로 암호화된 값이 유출이 되면 원본 값을 복원할 수 없기 때문에 그나마 피해를 줄일 수 있다.

블록체인에서는 이 해시값을 이용해 해당 블록에 서명하고 이전 블록의 해시값을 다음 블록에 기록함으로써 체인 형태의 연결 리스트(Linked List)를 형성하게 된다. 따라서 특정 블록을 해킹하려면 그 블록에 연결된 다른 블록들도 수정을 해야 하기 때문에 데이터의 위·변조가 아주 어려운 구조를 가지고 있다.

2) 해시함수의 특성[20]

해시함수는 아래와 같은 기본적 특성을 가지고 있다.

① 어떤 길이의 데이터도 입력으로 사용될 수 있다.

② 결과는 정해진 길이로 나온다.[21]

③ 계산 시간이 합리적으로 추정 가능해야 한다.[22]

하지만 그중에서도 특별히 블록체인에 유용하고 실제로 사용되는 특성은 다음과 같다.

④ 결과 값이 중복될 가능성이 거의 없다.

⑤ 입력 값을 알 수 없다.

⑥ 결과 값을 알려주고 입력 값을 찾을 수 있는 특별한 공식이 없다.

---

19) snowdeer 홈페이지, 블록체인 소개-(2) 블록과 해시함수 (https://homoefficio.github.io/2017/11/19/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%ED%95%9C-%EB%B2%88%EC%97%90-%EC%9D%B4%ED%95%B4%ED%95%98%EA%B8%B0/)

20) 스팀잇 홈페이지, 해시함수의 이해1-해시함수란?(https://steemit.com/kr/@endiyou/1)

21) SHA256은 입력되는 데이터의 길이와 상관없이 항상 256bit가 결과로 나옴

22) 입력 길이에 제한이 없기 때문에 최소한 입력 길이에 선형적으로 비례하는 특성은 있어야 함

〈그림 Ⅱ-2〉 블록체인 기술에서의 해시함수 적용 예시[23)]

3) 해시함수에 관한 추가 설명

블록체인을 활용한 암호화폐에서 사용되는 암호기술은 해시(Hash)함수, 전자서명(Digital Signature), 공개키 암호화(Cryptography) 알고리즘이라 말할 수 있다. 여기서 해시함수는 임의 데이터를 특정 길이의 문자, 숫자로 조합된 해시값으로 변환하는 암호 알고리즘의 일종이다. 해시함수에서 산출되는 해시값(Hash Value)은 지문(Fingerprint)이라고도 하는데, 암호화폐에서 해시값 비교(Hash check)를 통하여 원본의 위·변조 여부를 판단하는 무결성 검증에 사용될 수 있다.

블록체인에서는 해시함수를 사용하는 3가지 목적을 살펴보면 첫째, 공개키의 해시값을 지갑주소로 활용하여 익명화된 거래를 수행하고, 가상 화폐의 전자지갑 주소는 공개키 기반 암호화 알고리즘에서 생성된 공개키의 해시값을 사용한다. 개인정보(정확히는 송신자의 계좌정보) 없이 익명화된 거래를 통해 송금자의 신원을 감추고, 송금 할 수 있다. 둘째, 해시함수를 사용하여 2가지의 무결성 검증에 사용하게 된다. 체인으로 연결된 블록헤더의 해시값을 활용하여, 해시값 체인으로 연결된 블록의 무결성 검증에 사용된다. 또 다른 무결성 검증은 각 블록의 전체 거래를 하나의 해시값(머클 루트)으로 저장하고, 필요할 경우에는 언제든, 해당 블록의 머클 루트 값으로, 블록 내에 포함

23) homoefficio 홈페이지, 블록체인 한번에 이해하기(http://snowdeer.github.io/blockchain/2018/01/06/blockchain-seminar-about-blockchain/)

된 개별 거래의 위·변조 여부를 검증할 수 있다. 모든 거래 데이터의 해시값을 머클 트리(Merkle Tree)를 이용하여 만들어지는 머클 루트(Merkle Root)에 저장하고, 향후 거래내역의 위·변조 여부를 검증할 때, 원본 해시값과 비교를 통하여, 각 거래의 무결성을 검증할 수 있다.

또한 머클 루트는 1MB로 크기가 제한되어 있는 비트코인의 각 블록의 크기를 효율적으로 사용할 수 있게 한다. 전체 거래내역을 다 저장할 필요 없이, 머클 루트라는 한 개의 해시값만 저장하면, 해당블록 내의 모든 거래내역의 진위를 필요할 때 비교할 수 있기 때문이다. 마지막으로 합의 알고리즘에서 PoW(Proof of Work) 방식을 사용할 경우, 해시값을 활용한 채굴문제에 활용한다. 해시값을 활용한 채굴문제를 먼저 맞추는 채굴자에게 채굴권한과 보상을 제공한다. 해시캐시(Hashcash) 문제풀이를 통한 작업증명(PoW)은 채굴(Mining)이라고도 하는데, 채굴자에 대한 보상을 통해, 채굴을 경쟁하고, 채굴자가 자율적으로 새로운 블록을 생성하도록 유도할 수 있는 원리를 가지고 있다.

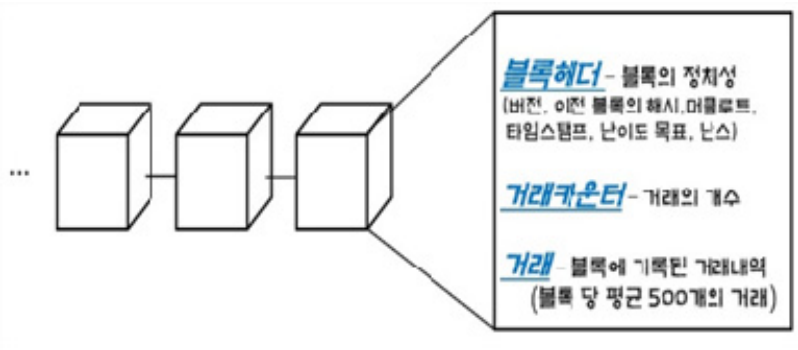
나. 머클 트리(Merkle Trees)

1) 블록체인(Blockchain)하에 머클 트리 특징

거래내역을 확인하기 위해 전체 600 Giga(2018. 8 현재)를 차지하는 자료들을 일일이 비교하며 특정 트랜잭션(거래)이 위·변조 되었는지 확인하는 건 너무 비효율적이며, 특정 트랜잭션의 위·변조 여부를 빠르고 효율적으로 조회할 수 있어야 하는데 이에 따라 등장한 방식이 머클 트리 방식이다.[24]

24) medium 홈페이지, 비트코인 코어 소스코드로 살펴보는 머클 트리(https://medium.com/@dlgusdn616/bitcoin01-01)

〈그림 Ⅱ-3〉 블록체인 기술에서의 블록 구조 및 알고리즘



블록은 블록의 정체성을 띠는 데이터를 가진 블록헤더, 해당 블록에 거래의 개수를 알려주는 거래 카운터, 그리고 가장 많은 공간을 차지하는 거래목록들이 있다.

그중에서도 블록헤더는 아래 3가지로 구성되어 있다고 볼 수 있다.

① 현재 블록이 이전(Previous) 블록과 연결되어 있음을 나타내는 이전 블록의 해시 값을 포함한다는 부분

② 난이도, 타임스탬프, 난스 등 채굴 경쟁과 직접적 연관이 되는 부분

③ 머클 루트(Merkle Root)

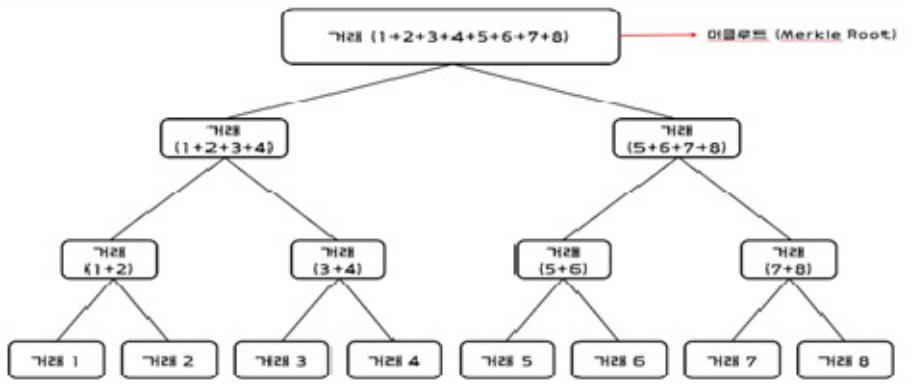
①은 블록이 이전 블록과 연결되어 있다는 것을 나타내며 해당 블록을 식별하는 것이고, ②는 채굴자들이 연산을 통해 블록을 채굴하는 데 연관된 것들이다. 마지막으로 ③의 머클 루트(Merkle Root)란 머클 트리(Merkle Trees)에서 뿌리 부분에 해당하는 것으로, 해당 블록에 있는 모든 거래내역(수백에서 수천 가지의 거래량)을 요약하여 작은 사이즈의 용량으로 블록헤더에 존재하는 데이터이다.

그런데 머클 트리(Merkle Trees)에 대해 찾아보면 다들 이진 트리(Binary Trees)라는 표현을 써서 설명하고 있는데, 여기서 '이진 트리'란 거래를 두 개씩 묶는다는 의미이다.

아래 그림은 가장 단순하게 8개의 거래로 묶어 예를 든 것인데, 8개뿐만 아니라 몇

개의 거래 데이터가 있든 하나의 뿌리(루트)로 만들 수 있다. 이 과정은 그림처럼 두 개씩 거래를 묶은 다음 SHA256 알고리즘을 통해 해시값으로 나타내고 또 그렇게 묶은 값들을 다시 두 개씩 묶어서 해싱하여 수백 개의 거래 값들을 그림 가장 꼭대기에 위치한 하나의 데이터로 만들어주는 것이다.[25]

〈그림 Ⅱ-4〉 머클 트리(Merkle Trees) 방식 중 이진 트리(Binary Trees)[26]



이렇게 두 개씩 묶어서 올라가면 좋은 점은 거래량이 기하급수적으로 늘어나도 특정 거래를 찾는 경로는 단순하다는 것이다. 거래의 건수인 N이 증가할 때마다 특정 거래의 경로를 찾는 경우의 수는 log2(N)으로 늘어나기 때문이다.[27]

머클 트리 방식을 사용하게 되면, 거래내역을 위조하려는 시도가 있어도 머클 트리의 경로를 따라가 해시값이 다른 블록을 찾게 되어 빠르게 거래의 위·변조도 알 수 있게 되고 이를 방지할 수 있다.

블록체인의 용량은 시간이 지날수록 지속적으로 늘어가기 때문에 이제는 성능이 좋은 컴퓨터만 모든 블록체인을 다운받는 '풀노드(Full Node)'가 될 수 있는데, 이 머클 트리의 이진 트리 방식은 우리가 가지고 다니는 모바일로도 블록데이터의 일부만 다운받는 '라이트 노드(Light Node)'로서 쉽고 빠르게 특정 거래를 찾도록 해준다.

---

25) 거래가 몇백, 몇천 개든지 뭉쳐서 요약된 머클 루트의 용량은 32바이트로 항상 같음
26) 스팀잇 홈페이지, 쉽게 설명하는 블록체인(https://steemit.com/kr/@jsralph/merkle-trees)
27) 여기서 log 스케일이 2인 것은 거래를 두 개씩 묶어서 올라가기 때문임

2) 머클 트리 방식에 대표적으로 사용되는 기술

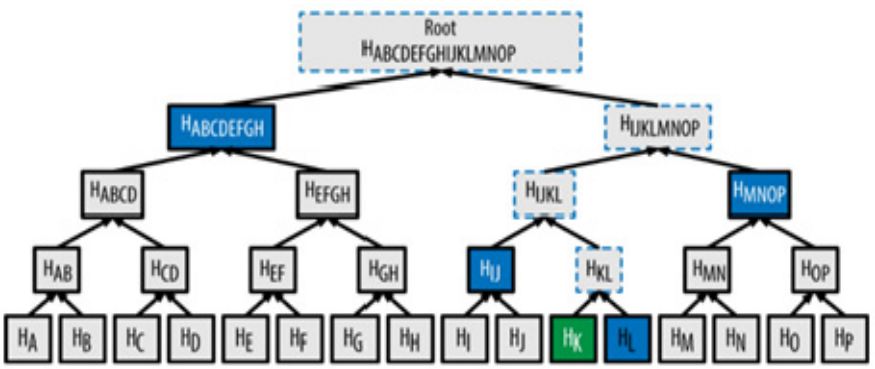
1. SHA256(Secure Hash Algorithm): 어떠한 입력값이 들어와도 항상 고정된 크기(256bit)의 데이터를 반환하는 해시함수이다.
2. Binary Tree(이진 트리): 트랜잭션의 해시(거래내역)를 두 개씩 묶어 또 다른 해시를 만들어내는 알고리즘이 사용된다.

3) 예시를 통한 머클 트리 작동 방식

가정: 비트코인 블록체인의 특정 블록(100번 블록) 안에는 트랜잭션(A~P)이 존재하고 있다.

실제 구현: 각 트랜잭션들은 CTransaction 클래스의 1차원 vector로 CBlock 내에 저장되어 있다.

〈그림 Ⅱ-5〉 머클 트리 작동방식 체계에 대한 예[28)]



28) medium 홈페이지, 비트코인 코어 소스코드로 살펴보는 머클 트리(https://medium.com/@dlgusdn616/bitcoin01)

가지고 있는 트랜잭션 중 트랜잭션 K(위 그림에서 녹색으로 표시)의 위·변조가 의심되어 위·변조 여부를 조사하려 한다. 이때 필요한 정보는 파란색으로 칠해진 4개의 해시값(H_L, H_IJ, H_ABCDEFGH), 그리고 머클 루트다.

각 트랜잭션들의 해시(uint 256: SHA256의 결과값은 unsigned 256bit)를 저장하기 위해 vector〈uint256〉 vMerkleTree가 존재한다.

6. 블록체인 컨소시엄

블록체인 기술은 거래가 가능한 대부분의 자산에 적용이 가능하므로 다방면에 걸쳐 다양한 형태로 검토 중이며, 블록체인의 개발은 주로 컨소시엄 형태로 플랫폼 개발이 이루어지고 있어 다수의 이해관계 금융회사 및 기업들이 공동으로 금융서비스에 적용시키려고 하고 있다. R3CEV 컨소시엄은 블록체인 기술기업인 R3가 중심이 되어 은행 등 금융기관이 활용할 수 있는 블록체인 표준 플랫폼(Corda)을 개발하였다.

Hyperledger 컨소시엄은 리눅스 재단이 주도하는 오픈소스 블록체인 컨소시엄으로 IT기업, 블록체인 기술기업, 금융기업, 제조사, 컨설팅기업 등 다양한 기업들이 협업 및 개발을 통해 다양한 블록체인 활용방안 및 여러 프로젝트를 진행하여 IBM의 Fabric이 두각을 나타내고 있다. 이 외에도 아시아 컨소시엄인 일본의 SBI 핀테크 컨소시엄과 중국의 Chinaledger가 있다.

상기 나열한 여러 블록체인 컨소시엄은 여러 특징과 목적에 맞게 달리 설계되었다. R3CEV가 개발한 "코다(Corda)"는 국가 간 대형 은행 또는 중앙은행 간의 송금 및 대금액 이체를 목적으로 블록에 이체 정보를 저장하는 형태이다. 가능한 사용처로는 중앙은행이나 수출입은행 등이다.

〈표 Ⅱ-4〉 주요 분산원장 기술 컨소시엄 및 여러 분산원장 모듈

컨소시엄	참가기관	주요 특징
R3 컨소시엄	• 60여 개 대형 해외 메이저 금융회사 • 국내 5개 은행(국민, 신한, KEB하나, 기업, 우리)	• 금융회사 계약 기록관리 시스템(Corda) 개발 • 대량금액 및 국가 간 거대 자본 이체
Hyperledger	• 금융회사 및 비금융 IT 기업 등 100여 개 기업 • 국내 기업(한국예탁결제원, 코인플러그, 삼성SDS)	• 오픈소스 • 범산업용 블록체인 플랫폼의 연구개발, LG 모나 체인 • IBM 주도의 “Fabric”이 가장 유명함
SBI 컨소시엄	• 리플, 코인플러그 등 참여	• 아시아에서 활용 가능한 블록체인 플랫폼 개발
Fido Ledger	• 국내 벤처 기업인 코인 플러그가 만든 Ledger	• 스마트 컨트랙트를 자유롭게 쓸 수 있음 • 블록체인 인증분야에 특화되어 있음

하이퍼레져(Hyperledger)는 가장 많이 응용되고 있는 블록체인 레져(Ledger)로서 여러 이타적인 또는 동종 업종의 프라이빗 블록체인을 오더링(Ordering) 이라는 재배열을 함으로써 진본성을 확인하는 대표적 컨소시엄 Ledger의 한 형태이다. 가능한 사용처로는 여러 기관을 포함한 국세청, 관세청 등이다.

국내 블록체인 벤처회사인 (주)코인플러그가 만는 파이도 레져는(Fido Ledger) 스마트 컨트랙트와 코인플러그가 가지고 있는 세계 특허인 블록체인 인증 특허를 이용한 블록체인의 형태이다. 가능한 사용처로는 인증이 필요한 금융, 보험 및 자산 분야이다. 여러 다른 레져(Ledger)들이 각 특성에 맞게 개발 출현되고 있는 중이다.

퍼블릭 블록체인은 누구나 참여할 수 있는 블록체인이며 트랙잭션과 컨퍼메이션 정보를 누구나 볼 수 있다. 하지만 누구나 참여 가능한 퍼블릭 블록체인은 기업이나 기관에 적용하기에는 제약이 있다. 블록 생성자 또한 어느 누구나(Anyone) 가능하며 블록의 생성 시간의 제약과 컴퓨터의 참여 간의 알고리즘 및 합의 등이 기업 비즈니스 모델에 확장하기 어려운 특성을 가지고 있기 때문이다. 이러한 이유 때문에 대부분의 기업은 프라이빗 블록체인으로 블록체인 플랫폼을 구성하고 있다.