블록체인의 발전 전망과 금융기관의 대응 현황

2016. 10.

BNK 금융경영연구소

담당 : 수석연구위원 김진완
(051-620-3184)

■ 목 차 ■

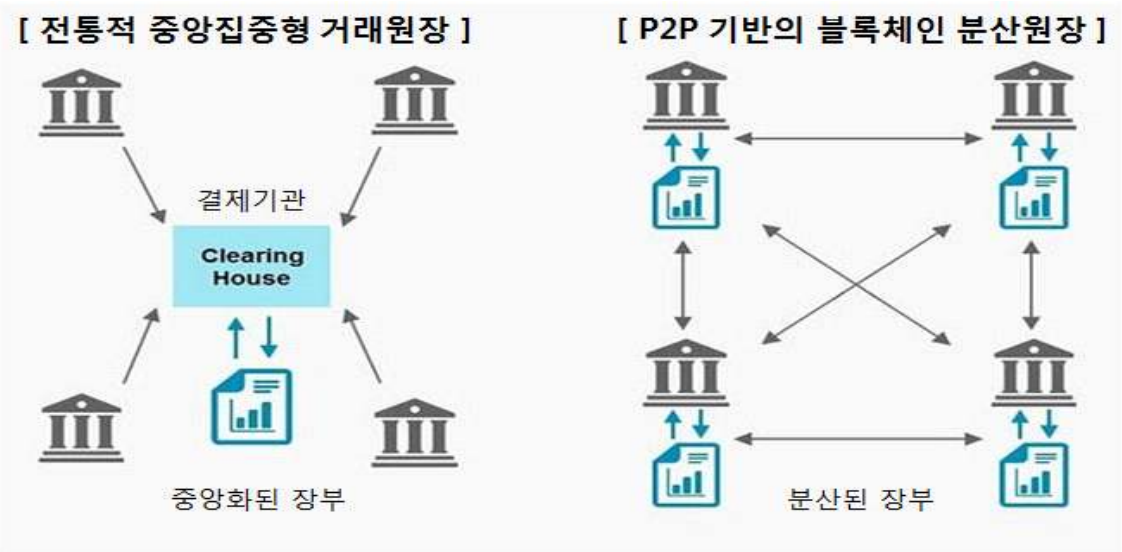
1 블록체인의 이해

1. 블록체인의 개념

□ 블록체인(Blockchain)은 당사자간 거래정보를 네트워크에 참여하는 모든 구성원이 공동으로 보관하는 분산 장부(Distributed ledger) 기술임

- 거래정보의 검증을 위해 10분 동안 발생한 거래를 모아 묶은 형태를 블록이라고 하며, 개념적으로 블록들이 순차적으로 연결된다는 의미에서 블록체인이라고 함
- 네트워크의 전체 구성원이 공동으로 거래정보를 기록·검증·보관함으로써 중앙은행이나 행정기관 등과 같은 "공인된 제3자"(Trusted 3rd party)의 공증 없이도 거래기록의 신뢰성 확보 가능
- 새로운 거래가 발생할 때 마다 각 구성원이 보관 중인 장부를 똑같이 업데이트하므로 해킹시 모든 장부를 변조해야 한다는 점에서 보안성이 매우 높음

〈 공인된 제3자 방식 vs. 분산 원장 방식 〉



자료 : 'The Fintech 2.0 Paper, Santander, 2015.

< 참고 > 공인된 제3자 방식의 문제점 및 블록체인 기술의 단점

공인된 제3자 방식의 문제점

○ 공인된 제3자를 선정해 거래기록 및 관리, 거래기록의 정확성을 검증하도록 위탁하는 대가로 일정의 수수료를 지불해야 함

○ 중앙 집중형 서버에 거래정보를 보관하고 있기 때문에 해커에게 위치가 쉽게 노출되어 적대적 공격의 표적이 되기 쉬움

○ 공인된 제3자의 역량에 따라 전체 시스템의 성능이 결정되며, 오류가 발생했을 때 전체 시스템에 심각한 영향을 미침

〈 블록체인의 단점 〉

단점	설명
1. 스케일 제약(Lack of Scale)	현재 사용 중인 시스템을 대체하기 위한 한계비용이 높음
2. 최첨단 기술(Bleeding Edge)	금융권에 적용하기에는 아직 기술적 성숙도가 낮음
3. 내재 비용 (Inherently More Costly)	중앙집중화 시스템에 비해 높은 컴퓨팅 파워가 요구됨
4. 컨센서스(Consensus)	거래승인에 필요한 참가자들의 합의 과정이 거래 속도에 영향을 미침

자료 : Digital Disruption, Citi Gps, 2016.

2. 블록체인의 핵심원리

□ 공인된 제3자의 공증 없이 거래를 할 경우에는 이중거래가 발생할 수 있는데 블록체인은 타임스탬프 서버라는 개념을 이용해서 블록의 작업증명이라는 방법으로 해결책 제시

타임스탬프 서버(Timestamp Server)

□ 우체국에서 편지나 소포 위에 스탬프를 찍어주는 것처럼 모든 거래를 모아 순서적으로 나열한 후 확정된 거래라고 스탬프를 찍어 모두에게 알리면 거래가 인증되어 이중거래를 막을 수 있다는 개념

- 다만 거래를 하나씩 나열할 경우 너무 많아지기 때문에 10분마다 거래를 모아 하나의 블록으로 만든 후 거기에 스탬프를 찍어주게 됨
- 타임스탬프 서버는 네트워크 이론에서 말하는 하나의 "노드(node)"이며 전체 네트워크 참여자 중에서 타임스탬프 역할을 원하는 노드는 모두 참여 가능

□ 컴퓨터 상에서 스탬프를 찍는다는 것은 10분간의 거래를 모은 블록 전체 내용을 해시함수의 입력값으로 사용하여 해시값을 만드는 행위

❖ 임의 길이의 입력값을 고정된 길이의 출력값으로 바꾸는 수학공식인 해시함수를 통해 영문과 숫자의 배열로 변환된 출력값을 해시값이라고 함

- 최초 블록을 제외한 모든 블록에는 바로 직전 블록의 해시값과 블록 내용을 모두 입력값으로 투입하여 해시값을 산출

〈 블록의 연결 - 블록체인 〉

자료 : Bitcoin: A Peer-to-peer Electronic Cash System, Satoshi Nakamoto, 일부 수정

해시함수(Hash Function)

○ 컴퓨터 암호화 기술의 일종으로 임의 길이의 입력값을 고정된 길이의 출력값(해시값)으로 바꾸는 수학공식

○ 비트코인에 사용되는 해시함수는 SHA-256으로 어떤 길이의 입력값을 넣더라도 결과로 나오는 해시값은 256bit 길이로 출력되기 때문에 거래내역을 간략화 시킬 수 있음
(아무리 긴 거래내역이라도 256자리 비트로 표현)

○ 특정 입력값이 해시함수를 통해 영문, 숫자의 배열로 변환된 결과값을 해시값이라고 함
ex> 1DCBF036EF010C301F24BD54CB03ECB15346EDEFDC0EB3F765AA348422FE5F3B

○ 해시함수는 어떤 방식으로도 입력값을 추론하거나 계산할 수 없는 특징을 가지고 있음

- 역상 저항성 : 해시값과 함수를 안다고 해도 그 입력값을 찾을 수 없음

- 충돌 저항성 : 같은 해시값을 찾는 두 개의 다른 입력값을 찾는 것은 거의 불가능함

블록체인 작업증명(Proof of Work)

□ **블록의 해시값은 누구라도 쉽게 구할 수 있어 악용될 소지가 있기 때문에 이를 방지하기 위해 블록체인 작업증명이라는 방법을 통해 거래를 검증(verification) 하게 됨**

□ **타임스탬프 서버(노드)에서 새 블록의 해시값을 구할 때 특정수의 패턴이 나타나는 해시값을 만들기 위해 필요한 추가적인 입력숫자(Nonce, 난스)를 찾게 되는데 이를 작업증명이라고 표현**

- 예를 들면, 첫 16자리에 0이 연속으로 나오는 패턴을 가진 해시값을 만들려면 어떤 숫자를 입력값으로 추가해야 하는지를 찾아내라는 것임

- 네트워크 참여자들 가운데 일부가 타임스탬프 서버(노드)로 활동하며 이들 중 가장 먼저 추가 입력값(nonce)을 찾는 노드가 블록의 해시값을 만들게 되는데 이것이 최종 스탬프를 찍는 행위가 됨

□ 스탬프가 찍힌 블록은 전체 네트워크 참여자들에게 전달되고 각 참여자들은 전송 받은 블록에 포함된 거래의 유효성을 검증한 후 이전 블록과 체인으로 연결하여 블록체인 원장이 완성

- 거래 유효성 검증은 블록에 포함된 모든 거래가 이전에 쓰이지 않은 경우에만 승인
- 전체 네트워크의 50% 이상이 블록을 승인하면 이전 블록과 체인으로 연결

블록체인 메커니즘 요약

① 새로운 거래 내역이 발생하면 모든 노드에 알려짐

② 각 노드들은 새로운 거래 내역을 10분마다 블록에 취합

③ 타임스탬프 서버(노드)들은 그 블록에 대한 작업증명 과정을 통해 거래를 검증

④ 작업증명에 성공한 노드는 전체 노드에게 해당 블록을 전송

⑤ 각 노드들은 해당 블록에 포함된 모든 거래가 이전에 쓰이지 않은 경우에만 승인

⑥ 50% 이상의 노드가 동의(승인)한 경우 이전 블록과 체인으로 연결

□ 블록체인 시스템에서 작업증명 과정은 3가지 중요성을 가짐

① 수많은 노드들이 서로 경쟁하고 감시함으로써 거래의 유효성을 철저히 검증할 수 있음

② 누구도 신규 블록을 독점적으로 만들지 못하게 함으로써 임의의 조작이나 개입을 원천적으로 차단할 수 있음

③ 어려운 채굴과정을 통해 신규 블록의 형성 속도를 10분으로 맞춰 거래의 수집과 배포, 거래의 유효성 확인 등이 무리 없이 진행될 수 있음

※ 자세한 블록체인의 작동원리는 “부록 : 블록체인 메커니즘” 참조

3. 블록체인의 유형

□ 블록체인은 네트워크 참가자의 성격, 범위 등에 따라 여러 가지 형태로 응용되고 있으며 금융기관은 프라이빗이나 컨소시엄 블록체인에 관심을 가짐

- **퍼블릭 블록체인(Public blockchains)** : 거래에 참여하는 누구라도 송금 및 열람이 가능한 공개된 형태로 특정 기관의 허가를 받지 않고 작업증명과정을 통해 거래 정당성을 인증하는 완전 분산형 구조
- **프라이빗 블록체인(Private blockchains)** : 한 기관이 모든 권한을 가지는 개인화된 형태로 거래에 참여하는 모든 사람은 기관의 허가를 받아야만 하는 분산장부의 장점을 이용한 중앙집권형 구조
- **컨소시엄 블록체인(Consortium blockchains)** : 미리 선정된 노드들에 의해 통제되는 형태로 n개의 금융기관이 노드를 한 개씩 운영하고 각 기관의 동의에 의해 거래가 생성되는 부분적 분산형태 구조

〈 블록체인의 유형 〉

유형	개념	활용사례
퍼브릭 블록체인	• 최초의 블록체인 활용 사례 • 인터넷을 통해 모두에게 공개 및 운용 가능한 장부 • 컴퓨팅 파워의 네트워크 제공을 통해 누구든 공증 작업에 참여 가능 • 네트워크 확장이 어렵고 거래 속도가 느림	Bitcoin, Ripple, Ethereum, DASH 등
프라이빗 블록체인	• 개인형 블록체인 • 하나의 주체가 내부 전산망을 블록체인으로 구현 • 블록체인 플랫폼 서비스 등장	NASDAQ, Overstock 등
컨소시엄 블록체인	• 반중앙형 블록체인 • 컨소시엄에 포함된 소수의 주체들만 참여 가능 • 주체들간 합의된 규칙을 통해 공증에 참여 • 네트워크 확장이 용이하고 거래속도가 빠름	R3CEVC, HSBC, Citi, Barclays, 등

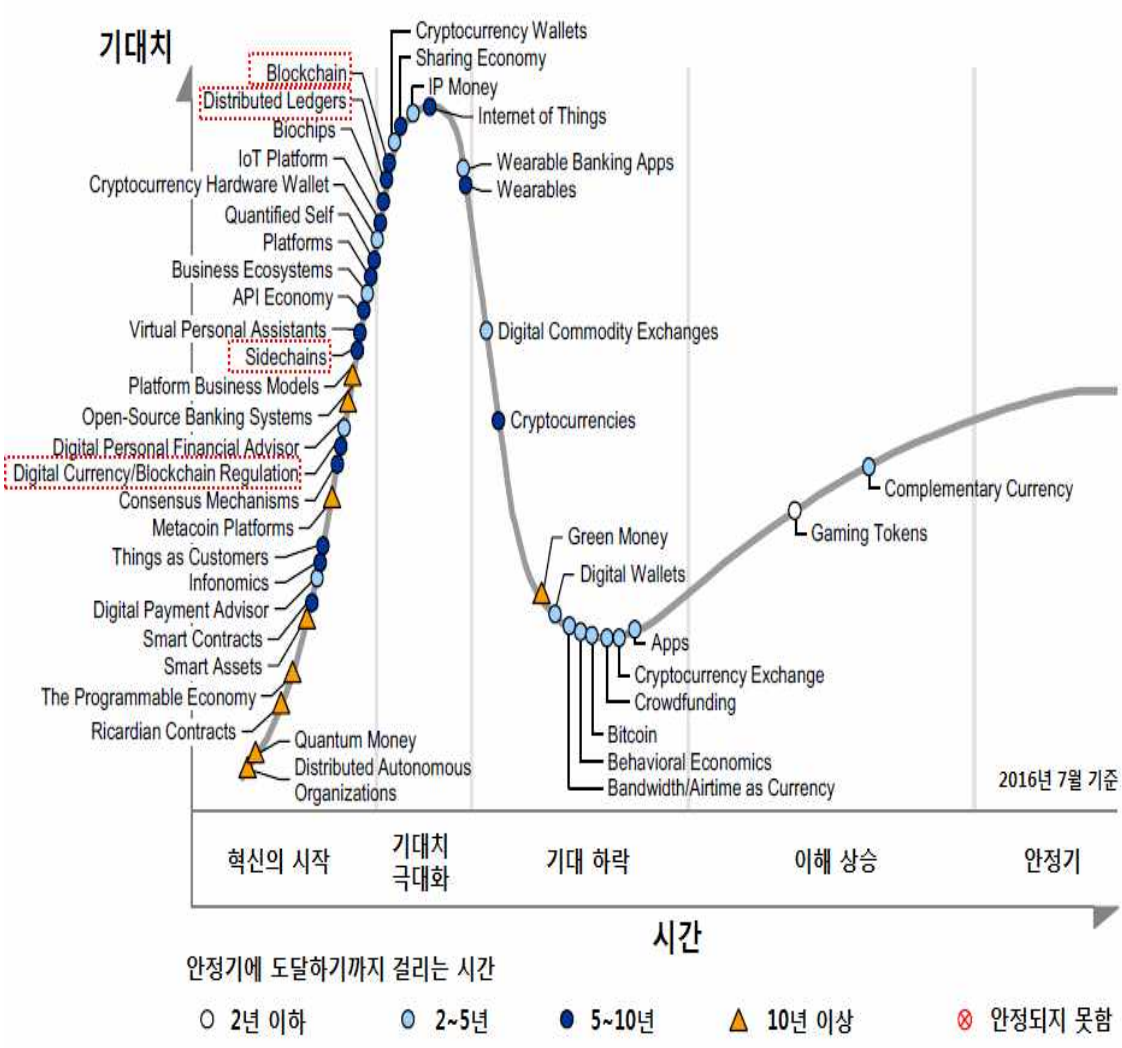
자료 : 금융보안원 재인용

2 블록체인의 발전 전망

□ 가트너는 기술 성숙도를 표현하는 하이프사이클에서 블록체인 관련 기술이 안정기에 도래하기 위해 5~10년이 소요될 것으로 예측

- 블록체인(Blockchain), 분산원장(Distributed Ledgers) 기술은 혁신의 시작 단계를 벗어나 기대치 극대화 단계로 진입
- 기대치 극대화는 비현실적이고 과장된 예측들이 나오는 시기로 기술 리더 중 일부는 성공하지만 기술적 한계로 실패로 이어지는 경우가 더 많음

〈 블록체인 기술의 하이프사이클 〉



단계	정의
혁신의 시작	기술의 출현, 대중 앞에서의 시연, 제품 출시 또는 이벤트로 관심을 끌고 여러 보도자료가 쏟아지는 단계
기대치 극대화	비현실적이고 과장된 예측들이 나오는 시기로 기술 리더 중 일부는 성공하지만 기술적 한계에 부딪혀 실패로 이어지는 경우가 더 많은 단계
기대하락	과도한 기대만으로 기술이 발전할 수 없기 때문에 급속하게 관심 밖으로 멀어지는 단계
이해상승	점점 다양한 조직에서 실험을 반복하고 노력을 기울이면서 산업 전반에 기술의 적용성, 위험요인, 유용성에 대한 이해가 높아지는 단계
안정기	시장에서 기술의 실용성이 인정받고 받아들여지기 시작하며 관련 도구 및 방법론이 안정화되는 단계

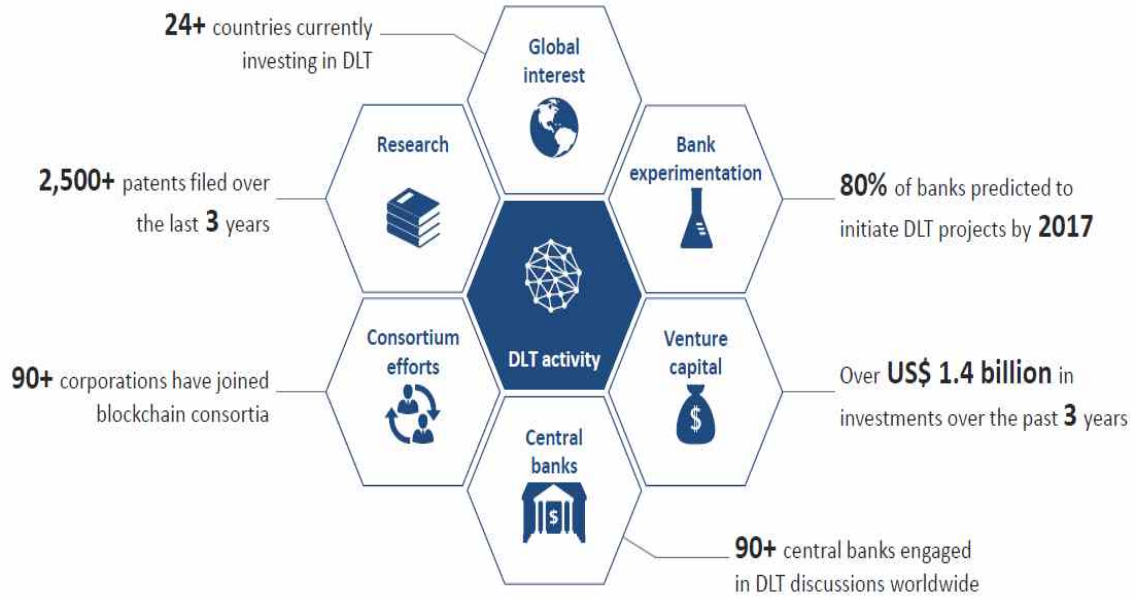
자료 : Hype Cycle for Blockchain Technologies and Programmable Economy, 2016, Gartner.

□ **세계경제포럼(World Economic Forum; WEF)은 블록체인 기술이 향후 10년 내에 급속히 확산되지는 않겠지만 다양한 영역에서 동시 다발적인 적용사례들이 나타날 경우 기술적용 속도는 예상보다 훨씬 빨라질 것으로 전망**

- 2017년까지 전 세계 은행의 80%가 블록체인 테스트를 시작할 것으로 예측
- 지난 3년간 14억달러가 블록체인에 투자
- 90개 이상의 중앙은행이 분산원장기술에 대한 글로벌 논의에 참여
- 24개국 이상에서 분산원장기술에 대한 투자 진행 중
- 지난 3년간 2,500개 이상의 블록체인 관련 특허 발생
- 90개 이상의 기업이 블록체인 컨소시엄에 합류

* WEF는 차세대 금융서비스 혁신을 이끌 기술로 생체인증(Biometrics), 클라우드 컴퓨팅(Cloud computing), 인지컴퓨팅(Cognitive computing), **블록체인(Blockchain)**, 기계학습(Machine learning)/예측적 분석(Predictive analytics), 양자컴퓨팅(Quantum computing), 로보틱스(Robotics)의 7가지를 제시

〈블록체인의 글로벌 동향〉



자료 : The future of financial infrastructure, WEF, 2016. 8.

□ IBM은 새로운 기술의 혜택을 완전하게 이해하기까지는 오랜 시간이 소요된다는 점에서 금융산업의 블록체인 발전을 단기, 중기, 장기적으로 구분하여 전망

(~ 2016) 지속적인 실험과 개념에 대한 증명, 표준화를 포함한 필수적인 구성요소에 대한 개발 작업 진행

(2016~2020) 뱅킹과 자본시장의 특정 영역에서 중요한 어플리케이션 등장

(~ 2025) 본격적으로 블록체인을 수용하고 기술적 대세로 자리 잡음

□ 유엔미래보고서 2050에서는 미래를 바꿀 새로운 기술 10선에 블록체인을 포함

- 안전한 거래를 중시하는 금융분야뿐만 아니라 정부가 기록하고 관리해야 하는 각종 공공 서비스 영역에서 큰 변화 예고
- 특히, 정부가 독점적으로 보관해온 모든 자료나 정보를 여러 곳으로 분산함으로써 해킹 우려없이 누구나 분석 및 활용이 가능해지고 출생·사망·혼인신고 및 토지·기업 등기 등의 행정기능 일부를 대체할 수 있다는 점에 주목

□ **엑센츄어에 따르면 2017년은 얼리 어답터에 속하는 금융기관들이 블록체인 기술을 본격적으로 수용하는 한 해가 될 것으로 예상**

- 2017년 얼리 어답터 금융기관이 지속적으로 블록체인 기술을 이끌어 나갈 것이며 2025년까지 관련 어플리케이션의 완성도가 높아질 것으로 기대

□ **다양한 기관에서 블록체인이 미래에 많은 경제적 가치를 창출하게 될 것으로 전망**

- 세계경제포럼(WEF)은 2027년까지 글로벌 GDP의 최소 10%가 블록체인 플랫폼에서 발생할 것으로 예측
- 산탄데르(Santander InnoVentures)는 블록체인이 국경간 결제, 증권 거래, 규제 대응을 위한 은행의 관련 인프라 비용을 2022년까지 연간 150~200억달러 절감할 수 있을 것으로 추정
- 파이낸셜타임즈(FT)에 따르면 블록체인 기술을 적용하면 은행들이 고객 데이터베이스 유지 보수 및 보안에 따른 비용을 연간 200억달러 줄일 수 있을 것으로 추정
- 금융조사업체에 따르면 투자은행들이 블록체인 기술을 적용할 경우 거래비용의 약 30%를 절감할 수 있다고 예상

3 금융기관의 대응 현황

□ Credit Suisse, Goldman Sachs, Barclays, RBS, BBVA, UBS 등 9개 대형 글로벌 은행들이 블록체인 기술을 표준화하기 위해 핀테크 스타트업인 R3와 제휴하여 블록체인 기술 검증 국제 컨소시엄 R3CEV 구성

- 이후 Bank of America, Citi group, HSBC, JPMorgan, Deutsche Bank 등의 대형 은행들이 추가로 가입하면서 회원사가 50개를 넘어섰음
- 국내의 경우 하나은행, 신한은행, 국민은행이 참여하고 있으며 우리은행, 기업은행도 합류 예정
- 회원사는 연간 25만달러의 회비를 납부하고 다양한 아이디어로 비즈니스 모델을 제시하고 R3CEV가 이에 대한 기술 검증을 하면 각 금융회사 전문가들이 실제 도입가능한지에 대한 교차 검증을 진행

〈 R3CEV의 프로젝트 사례 〉

프로젝트명	내용
Project Zero	11개 은행이 이더리움(Ethereum) 블록체인 플랫폼을 기반으로 이더리움의 비트코인이라고 할 수 있는 이더(Ether)라는 암호화된 화폐를 교환하는 실시간 정산업무 테스트 완료
Project One	42개의 은행에서 이러디움 블록체인 플랫폼 기반의 스마트 계약[주1)] 실행 테스트 완료
Project Genesis	40개 은행이 이더리움(Ethereum), 체인(Chain), 에리스(Eris), 인텔(Intel), IBM[주2)]의 5개 업체 블록체인 기술을 이용하여 스마트 계약 형태로 된 기업어음의 발행, 거래, 해지의 3가지 과정 테스트 완료

주1) : 스마트 계약이란 일정 조건을 만족시키면 거래가 자동 실행 및 집행되도록 프로그램화시켜 블록체인으로 검증하는 것을 의미

주2) : 이더리움(Ethereum), 체인(Chain), 에리스(Eris), 인텔(Intel), IBM 등은 비트코인 블록체인의 한계를 극복하고 보다 범용적인 플랫폼으로 확장시키기 위해 블록체인 시스템을 개발하고 있음

자료 : R3CEV 홈페이지(r3cev.com)

□ 자국의 규제와 제도, 환경에 맞는 블록체인 기술을 개발할 필요성을 인식함에 따라 자국내 블록체인 연합체를 구성

- 국내에서는 금융위원회가 주관하는 블록체인 연구회를 운영하고 있으나 아직 실질적인 성과는 없으며 연내에 은행·증권·카드업 등을 모두 아우르는 금융권 공동 블록체인 컨소시엄을 출범시킬 계획

❖ 연구회 참여기관은 금융위원회, 금융 유관기관(한국은행, 금융감독원, 금융보안원, 금융결제원, 한국거래소), 은행(하나금융지주, 신한은행, 국민은행, 우리은행, 기업은행), 학계(금융연구원, 인하대, 성신여대), 핀테크업체(코빗, 블로코, 코인플러그)로 구성

- 중국은 증권거래소, 원자재 거래소 등 11개의 금융기관이 중국블록체인연합(China Ledger Alliance)을 구성하여 중국의 법규 안에서 적용 가능한 분산원장 솔루션에 대한 연구 및 개발 진행
- 네덜란드 중앙은행은 자국 은행들이 블록체인 기술의 응용에 관한 정보의 공유 및 개발을 위해 블록체인 개발 캠퍼스 설립
- 프랑스 금융당국 및 금융사들은 컨소시엄을 구성하여 중소기업의 자금조달 환경 개선을 위한 블록체인 적용 연구 중

□ 은행들은 글로벌 컨소시엄 참여뿐만 아니라 자체적인 블록체인 서비스 개발에도 적극적으로 나서고 있음

- 국내 은행들은 블록체인 활용을 위해 핀테크 기업과의 파트너십을 체결하여 해외송금, 비대면 실명확인 시스템 등을 개발 중
- 최근 국민카드는 공인인증서 대신 블록체인 기술을 활용한 간편인증서비스를 상용화 하였다고 발표
- 외국의 은행들은 해외송금뿐만 아니라 주식매매, 신디케이트론, 자산등기 등 다양한 분야에서 블록체인의 실제 사용을 위한 연구를 활발히 진행 중

〈 국내 은행의 블록체인 관련 활동 〉

은행명	내용
국민은행	▪ 비대면 실명 확인 증빙자료의 위·변조 확인 시스템 구축 ▪ '코인플러그'와 해외송금 서비스 개발 중 ▪ 캄보디아 모바일뱅크에 기술 적용
신한은행	▪ 골드바 구매 교환증 및 보증서 발급서비스에 적용 ▪ 국내 핀테크 기업 '스트리미', 영국 핀테크 기업 및 연구소와 5자간 MOU를 체결하여 해외송금 서비스 개발 중
하나은행	▪ '센트비'와 블록체인 기술을 활용한 소액 외화이체 업무 협력 논의
기업은행	▪ '코빗', '비트페사'와 해외송금 서비스 개발 추진

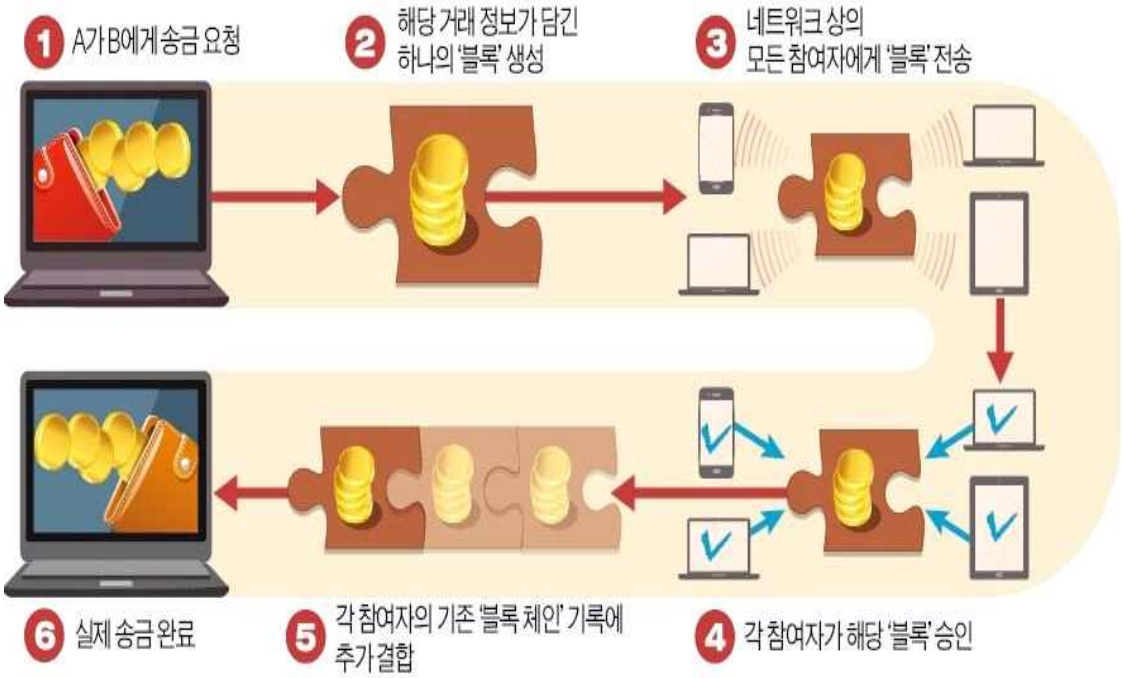
〈 해외 은행의 블록체인 관련 활동 〉

은행명	내용
Deutsche	▪ 신용화폐 지급결제, 자산등기, 장외파생상품 거래, 규제보고, 자금세탁 방지시스템, 주식매매시스템 등에 다양한 블록체인 적용 사례 연구 ▪ 런던, 베를린, 실리콘밸리의 연구소에서 실험
Santander	▪ 블록체인에 대한 20~25건의 사용 사례 보유 ▪ 블록체인 연구를 위한 "Cryto 2.0" 팀 구성
Societe Generale	▪ 비트코인, 블록체인, 암호화폐 관련 전문 직원 채용
UBS	▪ 런던에 암호화폐 실험실을 가지고 있으며 거래 및 결제, 스마트 채권 분야 등에서 블록체인 실험 진행
Westpac	▪ 크로스 보더(국가간 결제) 플롯폼을 개발하기 위해 리플과 제휴
Mizuho	▪ 국경간 증권 거래 시스템 테스트 완료 ▪ 문서 기록 및 관리시스템과 신디케이트론 업무에 블록체인 적용 예정
Bank of Ireland	▪ 딜로이트와 블록체인 공동 작업증명(proof-of-concept) 테스트를 완료함으로써 기존 금융시스템과 분산장부 기술이 결합될 수 있다는 것을 입증

부록 : 블록체인 메커니즘

□ 블록체인 기술을 적용한 대표적 응용시스템인 비트코인 전송 프로세스를 통해 각 단계별 작동원리를 살펴보고자 함

〈 블록체인 기반의 비트코인 전송 프로세스 〉



1. 비트코인 송금

□ 비트코인 사용을 위해서는 컴퓨터에 비트코인 프로그램을 설치한 후 생성된 전자지갑에 계정을 만들면 거래 가능

- 계정을 만들면 한 쌍의 비대칭 암호키인 공개키와 비밀키가 생성
- 공개키(Public Key)는 돈이 송금될 주소이며, 비밀키(Private Key)는 지갑에 저장되어 송금할 때 서명용으로 사용

□ 비트코인과 블록체인 원리를 파악하기 위해서는 아래 용어들에 대한 이해가 필요

비대칭 암호화 기법(Asymmetric Encryption)

○ 암호화는 데이터에 특정규칙을 적용하여 정해진 사람 이외에는 알아볼 수 없도록 함으로써 불법적인 방법에 의해 데이터가 손실되거나 변경되는 것을 방지하기 위한 기법

○ 예를 들어, A와 B가 0을 1로 그리고 1을 0으로 해석하기로 약속한 후 A가 '101'을 '010'으로 바꾸어(암호화) 전달하면 B는 이를 다시 '101'로 변환(복호화)시켜 메시지를 확인하게 되는데 여기서 '0과 1을 바꾸는 기법'을 암호화키라고 이해하면 됨

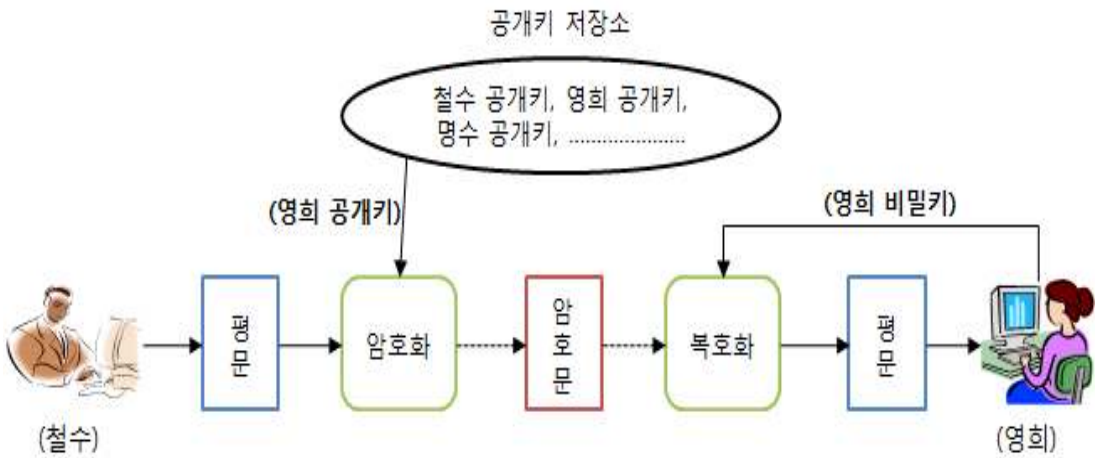
○ 사례처럼 암호화와 복호화에 동일한 암호화키를 사용하는 방식을 대칭키 암호화라고 하는데 거래를 하는 모든 상대방의 암호화키를 보관해야 하는 복잡성과 분실시 제3자에게 메시지가 노출된다는 문제점으로 비대칭 암호화 기법 등장

○ 비대칭이란 암호화와 복호화에 사용되는 키가 서로 다르다는 의미로 하나의 키를 이용해서 데이터를 변형하면 이를 복원할 때는 나머지 하나의 키를 이용하는 방식

○ 하나는 공개 되어도 좋은 키(공개키, Public key)이고, 나머지 하나는 내가 비밀스럽게 보관해야 할 키(비밀키, Private key)로 구성

○ 비대칭 암호화 함수의 특징은 두 개의 키 중 하나의 키를 적용하여 메시지를 변형하면 다시 복원할 때는 변형할 때 사용한 키가 아닌 반드시 다른 하나의 키를 이용해야만 복원시킬 수 있도록 만듬

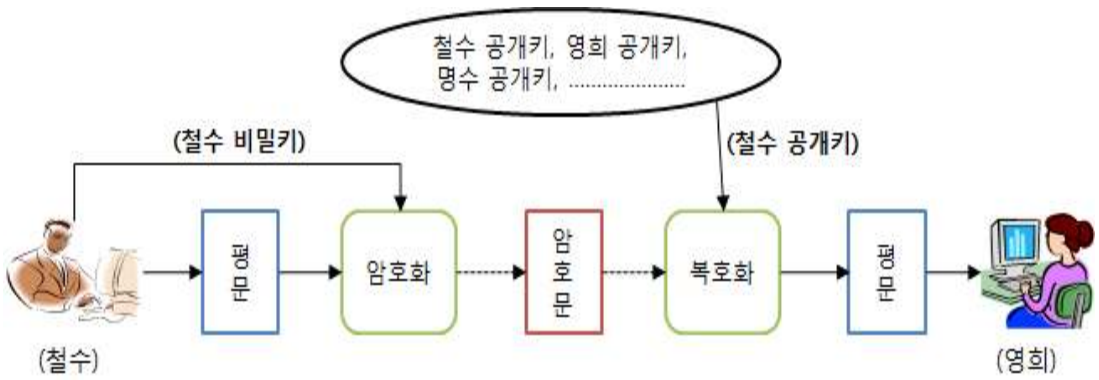
○ 아래 그림에서 철수는 공개되어 있는 영희의 공개키를 가져와 메시지를 암호화 시킨 후 영희에게 보내면 영희는 자신이 보관하고 있는 비밀키로 복호화시켜 메시지 내용을 확인하게 됨



전자서명(Digital Signature)

○ 비대칭 암호화 방식을 이용한 전자서명은 메시지를 작성자가 직접 작성했다는 사실과 메시지 내용이 전송과정에서 위·변조되지 않았다는 사실을 증명하고, 작성자가 향후에 작성사실을 부인하지 못하게 방지하는데 사용

○ 일반적인 암호화 과정과는 반대로 철수는 자신이 보관 중인 비밀키로 메시지를 암호화 시킨 후 영희에게 보내면 영희는 공개되어 있는 철수의 공개키를 이용해 메시지를 복원시켜 철수가 보낸 메시지가 맞다는 것을 확인할 수 있음



해시함수(Hash Function)

○ 컴퓨터 암호화 기술의 일종으로 임의 길이의 입력값을 고정된 길이의 출력값(해시값)으로 바꾸는 수학공식

○ 비트코인에 사용되는 해시함수는 SHA-256으로 어떤 길이의 입력값을 넣더라도 결과로 나오는 해시값은 256bit 길이로 출력되기 때문에 거래내역을 간략화 시킬 수 있음
(아무리 긴 거래내역이라도 256자리 비트로 표현)

○ 특정 입력값이 해시함수를 통해 영문, 숫자의 배열로 변환된 결과값을 해시값이라고 함
ex> 1DCBF036EF010C301F24BD54CB03ECB15346EDEFDC0EB3F765AA348422FE5F3B

○ 해시함수는 어떤 방식으로도 입력값을 추론하거나 계산할 수 없는 특징을 가지고 있음

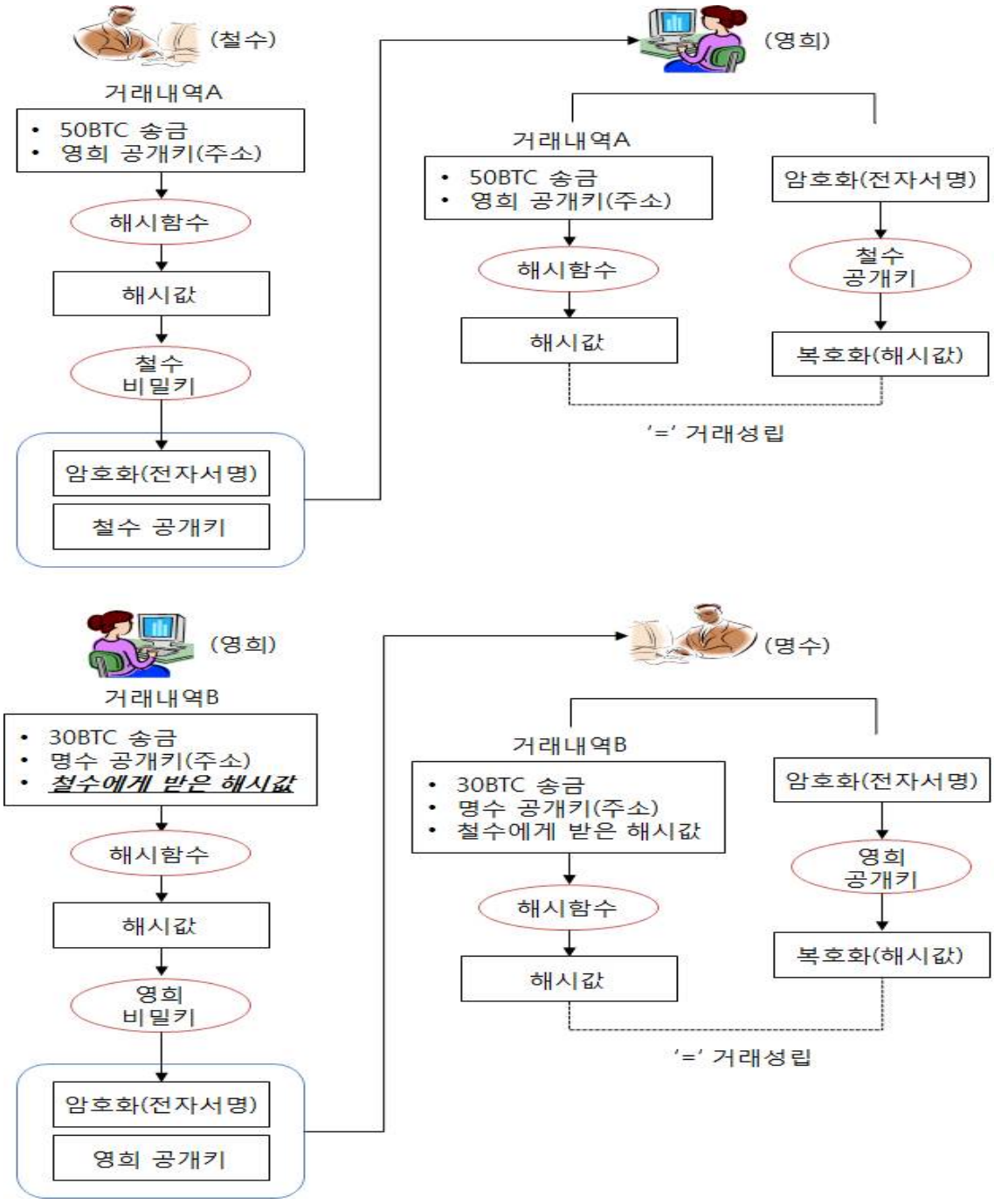
- 역상 저항성 : 해시값과 함수를 안다고 해도 그 입력값을 찾을 수 없음

- 충돌 저항성 : 같은 해시값을 찾는 두 개의 다른 입력값을 찾는 것은 거의 불가능함

□ 비트코인은 해시함수와 비대칭 암호화 기법을 이용해 거래를 암호화

❖ 사례 설명을 위해 철수 50BTC, 영희 30BTC, 명수 20BTC를 보유하고 있다고 가정

〈 비트코인 거래 암호화 〉



(철수 → 영희 비트코인 송금)

- 철수는 50BTC을 영희 주소로 보낸다는 거래내역A를 입력값으로 해시함수를 이용하여 해시값을 구한 후 이를 자신의 비밀키로 변형(전자서명)시켜 전체 네트워크에 거래내역A, 공개키와 함께 전파
- 영희는 전자서명된 해시값을 철수의 공개키로 복호화시켜 구하고, 거래내역A를 입력값으로 해시함수를 이용해 직접 해시값을 구한 뒤 두 값이 일치하는지를 확인
- 두 값이 일치한다는 것은 메시지가 철수가 보냈다는 것을 확신할 수 있으며 영희가 50BTC을 받았다는 의미

(영희 → 명수 비트코인 송금)

- 영희가 명수에게 비트코인을 송금하는 방법은 앞선 절차와 동일하나 한 가지 차이점은 영희가 철수로부터 비트코인을 받았다는 사실을 알리기 위해 거래내역B에는 철수에게 받았던 해시값이 추가로 포함
- 비트코인의 최초 거래(철수→영희)를 제외한 모든 거래는 영희가 명수에게 행하는 방법으로 이전 거래의 해시값을 포함하여 진행

*** 즉 거래를 할 때 해시함수에 이전 거래의 해시값이 들어가기 때문에 임의의 제3자가 받지도 않은 비트코인을 다른 누군가에게 보낼 수 없도록 설계**

Q1. 위 거래에서 공인된 제3자의 검증이 없기 때문에 전자화폐의 이중거래(Double Payment) 가능성이 존재하지 않는가?

- 예를 들어, 영희가 명수에게 보낸 방식과 동일하게 제3자에게 비트코인을 전송하면 명수가 받은 30BTC에 대한 권리가 변동될 수 있음

2. 블록체인 생성

□ 공인된 제3자의 공증 없이 거래를 할 경우에는 이중거래가 발생할 수 있는데 블록체인은 타임스탬프 서버라는 개념을 이용해서 블록의 작업증명이라는 방법으로 해결책 제시

(1) 타임스탬프 서버(Timestamp Server)*

□ 우체국에서 편지나 소포 위에 스탬프를 찍어주는 것처럼 모든 거래를 모아 순서적으로 나열한 후 확정된 거래라고 스탬프를 찍어 모두에게 알리면 거래가 인증되어 이중거래를 막을 수 있다는 개념

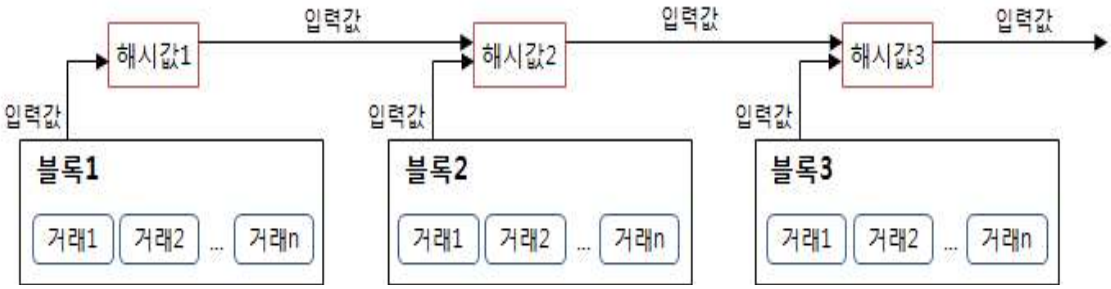
- 다만 거래를 하나씩 나열할 경우 너무 많아지기 때문에 10분마다 거래를 모아 하나의 블록으로 만든 후 거기에 스탬프를 찍어주게 됨

  * 네트워크 이론에서 말하는 하나의 "노드(node)"라고 생각하면 됨

□ 컴퓨터 상에서 스탬프를 찍는다는 것은 10분간의 거래를 모은 블록 전체 내용을 해시함수의 입력값으로 사용하여 해시값을 만드는 행위

- 최초 블록을 제외한 모든 블록에는 바로 직전 블록의 해시값과 블록 내용을 입력값으로 투입하여 해시값을 산출
- 블록의 해시값에 직전 블록의 해시값이 포함되어 있기 때문에 개념적으로 이전 블록과 연결된다는 의미에서 이를 블록체인이라고 함

〈 블록의 연결 - 블록체인 〉



자료 : Bitcoin: A Peer-to-peer Electronic Cash System, Satoshi Nakamoto, 일부 수정

Q2. 블록의 해시값은 누구라도 쉽게 구할 수 있는데 단순히 블록의 해시값만 구했다고 선착순으로 거래를 인증 할 경우 악용될 가능성은 없는가?

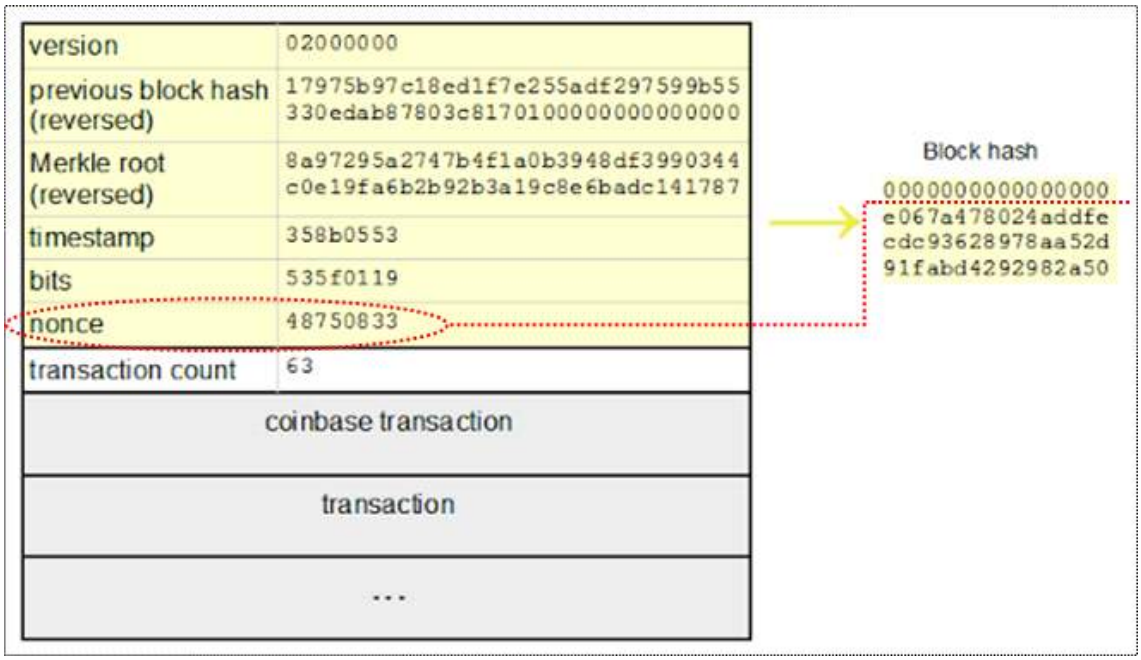
- 네트워크 공격자들도 타임스탬프 서버로 위장하여 재빨리 스탬프를 찍어 이중거래를 시도할 수 있음
- 과거에 스탬프가 찍혔던 블록의 해시값을 순간적으로 바꾸어 새로운 체인으로 대체할 가능성 존재
- 이러한 문제를 해결하기 위해 블록체인 작업증명이라는 방법을 통해 거래를 검증(verification)하게 됨

(2) 블록체인 작업증명(Proof of Work)

□ **타임스탬프 서버(노드)에서 새 블록의 해시값을 구할 때 특정수의 패턴이 나타나는 해시값을 만들기 위해 필요한 추가적인 입력숫자(Nonce, 난스)를 찾게 되는데 이를 작업증명이라고 표현**

- 예를 들면, 첫 16자리에 0이 연속으로 나오는 패턴을 가진 해시값을 만들려면 어떤 숫자를 입력값으로 추가해야 하는지를 찾아내라는 것임
- 해시값과 함수를 안다고 해도 그 입력값을 직접 계산하는 것은 불가능하기 때문에 일일이 추가 입력값(nonce)을 투입하고 해시값을 확인하는 시행착오(Trial and Error) 방법으로 시도해야 됨
- 추가 입력값(nonce)은 컴퓨터를 통해 시행착오 방법으로 찾기 때문에 타임스탬프 역할을 하는 노드들이 가지고 있는 컴퓨터의 CPU 처리속도에 비례하여 해답 발견 확률이 증가
- 블록체인 작업증명에 참여하는 노드가 변할 수 있고 하드웨어 기술이 발전하기 때문에 추가 입력값(nonce)을 찾는 문제의 난이도는 시간당 평균 발생 블록수가 일정하게 유지될 수 있도록 시스템적으로 조정됨
- 전체 네트워크 참여자 중에서 작업증명 역할을 원하는 노드는 누구라도 작업증명 과정에 참여할 수 있음

〈 블록 구조 〉



□ 결국 네트워크 참여자들 가운데 일부가 타임스탬프 서버(노드)로 활동하며 이들 중 가장 먼저 추가 입력값(nonce)을 찾는 노드가 블록의 해시값을 만들게 되는데 이것이 최종 스탬프를 찍는 행위가 됨

- 가장 먼저 스탬프를 찍은 노드는 보상으로 비트코인을 받게 됨

채굴에 따른 비트코인 보상

○ 비트코인 시스템에서 각 노드가 해시값을 찾아 새로운 블록을 만드는 행위를 채굴(Mining)이라 하고, 이런 노드를 운영하는 사람을 채굴자(Miner)라고 함

○ 채굴에 성공하면 새로운 블록 1개당 50BTC을 보상으로 받게 되는데 이 금액은 4년마다 절반으로 줄어들어 2009년 1월 발행 이후 현재는 12.5BTC을 받을 수 있음

○ 비트코인의 총 발행량은 2100만 BTC로 제한되어 있기 때문에 2140년이면 채굴에 따른 보상을 지급할 수 없게 되며 그 후부터는 비트코인 사용자에게 거래세(Transaction Fee)를 부과하여 대체하게 됨

○ 채굴자들이 치열하게 블록 만들기 경쟁을 하는 이유는 보상으로 주어지는 비트코인 때문인데 현재 주어지는 12.5BTC은 약 660만원(2016. 10. 5 비트코인 환율기준)의 경제적 이득을 볼 수 있음

□ 새로운 블록의 해시를 발견하는 노드들에게 비트코인을 보상으로 주기 때문에 네트워크 공격자 보다는 훨씬 많은 다수의 정직한 노드가 네트워크에 참여할 것으로 예상

- 전체 네트워크에서 정직한 노드의 CPU 파워가 50%를 넘게 되면 채굴경쟁에서 공격자를 항상 앞서는 결과를 유지할 수 있다고 봄
- 악의적 스탬핑을 하는데 들어가는 컴퓨터 전력 사용량이 거래조작을 통해 얻을 수 있는 경제적 이익보다 높기 때문에 현실적으로 불가능

□ 스탬프가 찍힌 블록은 전체 네트워크 참여자들에게 전달되고 각 참여자들은 전송 받은 블록에 포함된 거래의 유효성을 검증하는데 이때 50% 이상의 참여자들이 동의하면 이전 블록과 체인으로 연결되어 블록체인 원장이 완성

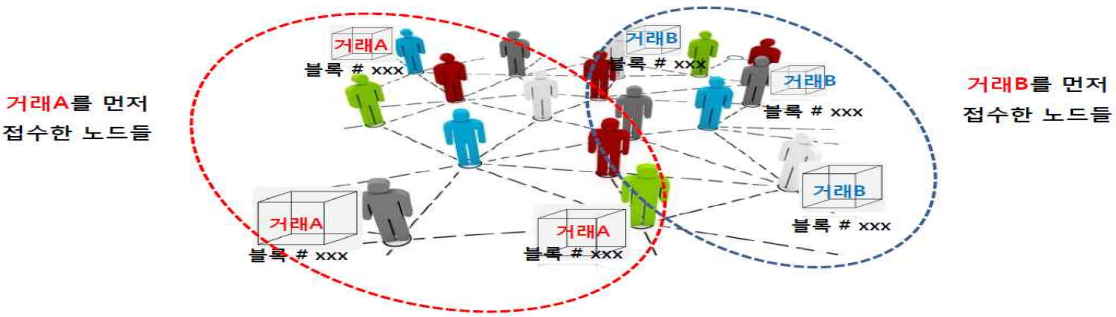
Q3. 만약 부정사용자가 이중거래를 시도했다면 블록체인 시스템에서 어떻게 문제를 해결하는가?

(3) 블록체인 유지 규칙

□ 부정사용자가 거래A와 거래B를 중복 사용한 경우 전체 네트워크의 일부 노드는 거래A를 가지고 나머지는 거래B로 채굴작업 진행

- 비트코인의 거래내역은 네트워크의 모든 노드에게 전달
- 각 노드는 동일한 내역을 가진 두 거래 중 하나만을 접수

〈 중복 거래내역의 접수 〉

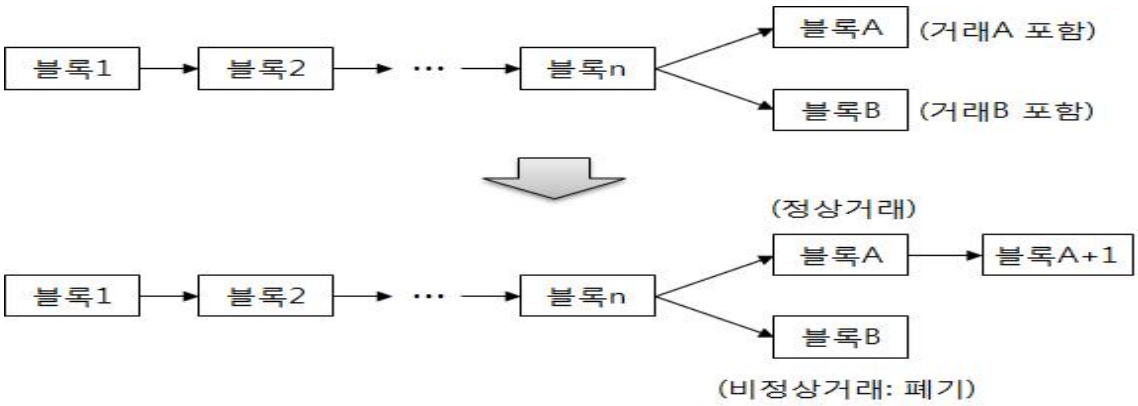


□ 이중거래의 경우 두 거래 중 가장 긴 블록체인을 만들어 내는 쪽에 접수된 거래만 '정상'으로 처리하고, 긴 블록체인 만들기에 실패한 블록에 포함된 거래는 '비정상'으로 간주하여 자동 폐기

- 이중거래가 발생하면 거래A와 거래B는 특정 노드들에 의해 각각 다른 블록으로 형성되어 동시에 블록체인으로 연결
- 10분 후 새로운 블록(A+1)이 만들어져 블록A에 연결되는지 블록B에 연결되는지를 보고 긴 체인을 형성한 블록A에 포함된 거래는 정상으로 판단하여 유지하지만 블록B는 비정상거래로 인식하여 폐기

*** 비트코인 시스템은 항상 가장 긴 체인만 유지되도록 설계되었는데 이를 'The longest chain wins'라고 표현하며 이를 통해 이중거래 문제 해결**

〈 블록체인 유지 규칙 〉



블록체인 메커니즘 요약

① 새로운 거래 내역이 발생하면 모든 노드에 알려짐

② 각 노드들은 새로운 거래 내역을 10분마다 블록에 취합

③ 타임스탬프 서버(노드)들은 그 블록에 대한 작업증명 과정을 통해 거래를 검증

④ 작업증명에 성공한 노드는 전체 노드에게 해당 블록을 전송

⑤ 각 노드들은 해당 블록의 모든 거래가 이전에 쓰이지 않은 경우에만 승인

⑥ 50% 이상의 노드가 동의한 경우 이전 블록과 체인으로 연결