[IT Essential] BlockChain 2

> 금융업 비즈니스와 Blockchain 비교 및 종류

- 진행: 박종철 컨설턴트
- 날짜: 2020.09.16
- 목차
    1. 지난 강의 REMIND
    2. 금융 비즈니스 프로세스
    3. 블록체인의 종류
    4. 블록체인의 역사
    5. 요약
    6. 추가 자료

- 목표
    1. 금융 비즈니스의 프로세스를 알 수 있다.
        - 신뢰 구축과 이중 지불 문제
    2. BlockChain 의 종류를 알 수 있다.
    3. BlockChain 의 탄생 배경과 철학을 알 수 있다.

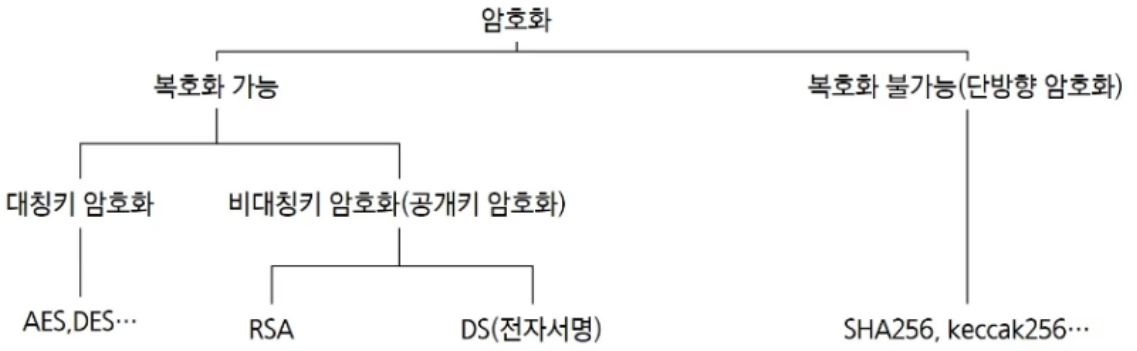
1. 지난 강의 REMIND

1. BlockChain

- 정의: 블록에 데이터를 저정, 해시함수로 묶어 이전 블록을 가리켜 놓은 것
- 특징: 보안성, 투명성, 무결성, 탈중앙화

2. 암호화

- 복호화 가능한 암호화와 불가능한 단방향 암호화로 나뉜다



3. 활용

- 결제, 암호화폐(거래 내역), 지역 화폐
- 스마트 계약, 물류 관리, 문서 관리, 의료정보 관리, 저작권 관리, 한정판 디지털 상품(Non Fungible Tokens), 게임 아이템 관리, 소셜미디어 관리, 전자투표, 신원확인
- World Computing

2. 금융 비즈니스 프로세스

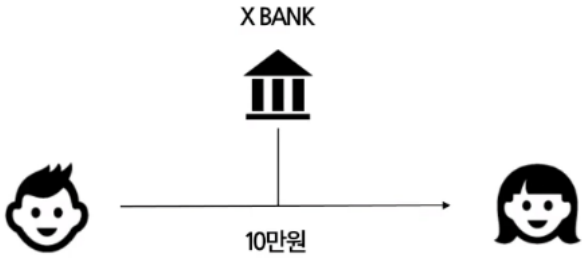
1. 은행에서 송금하기

> A 가 B 에게 10만원을 보내는 경우를 생각해보자.

1. 당행 송금

1. 은행 어플을 켠다
2. 본인인증, 계좌번호, 금액을 적는다
3. 비밀번호를 입력한다
4. 송금 버튼을 누른다

   👉 여기서 송금이 의미하는 바가 무엇일까?



   - 각각의 계좌를 확인하면 0.1초 내로 A는 10만원이 빠진 것을, B 는 10만원이 입금 된 것을 알 수 있다.
   - 하지만 X 은행이 B 에게 달려가 10만원을 쥐어준 것이 아니라 `통장`에 그 입출금 변동 내역이 `기록` 된 것이다. 돈은 실제로 은행에 있지 않다. (대출 받아 간 사람들한테 있다.)

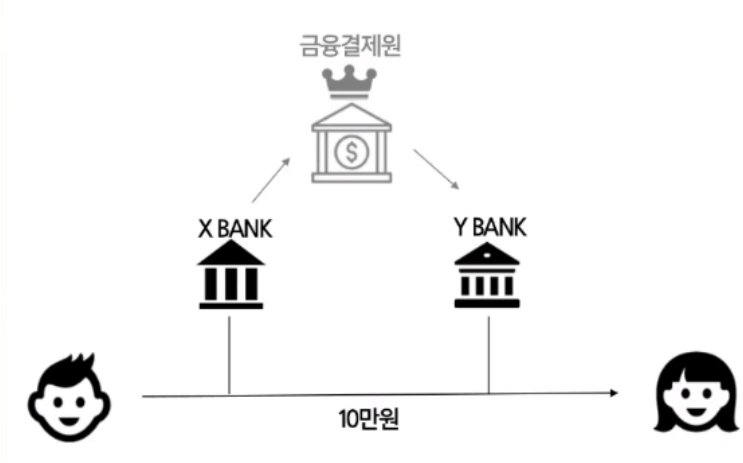
5. 수수료: 없음

6. 소요시간: 수 초 내

2. 타행 송금

1. 에서 4 번의 과정은 동일하다.

   👉 여기서 송금이 의미하는 바가 무엇일까?

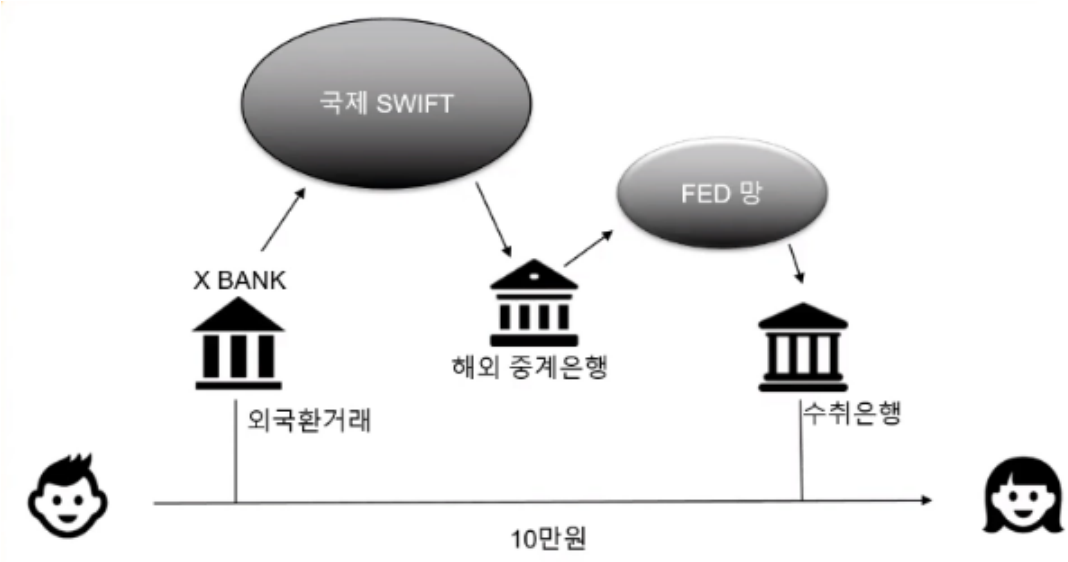


   - 누가 X 은행과 Y 은행을 보증할까?
   - X 은행과 Y 은행을 중재하고, 각각을 보증하는 사람이 필요할 것이다. ==> 금융결제원
   - 각 은행들은 상위 금융결제원에 종속 되어 신뢰 관계를 유지할 수 있다.
2. 수수료: 경우에 따라 500~1000원
3. 소요시간: 수 초 내

3. 해외 송금

1. 에서 4 번의 과정은 동일하다.

   👉 여기서 송금이 의미하는 바가 무엇일까?



   - 외국환 거래를 통해 국제 SWIFT 망을 통한다.
   - 해외 중개은행은 valid check 를 한다.
   - 처리 후 FED 망을 통해 수취 은행으로 보낸다.
   - 이를 매입하여 받는 사람에 대해 Valid check 및 환율 등등을 체크한다.
   - 관리가 쉽지 않다.
   - (디카프리오는 교수님의 친구이다.)

2. 수수료: 10~20% + a
3. 소요시간: 5~7 영업일

2. 은행이 왜 필요한걸까?

- ✨신뢰✨ 때문에. 보증과 신뢰 문제!
    - 하지만 이로인해 **이중 지불 문제** (수수료)가 발생한다. 은행과 같은 중개인에게 수수료를 내야 하는 것.
    - 신뢰 문제를 해결한다면 중개인 없이 거래를 할 수 있지 않을까?

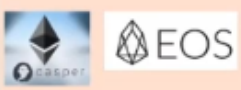
3. 디지털 자산의 이동

> A 가 B 에게 mp3 파일을 보내는 경우를 생각해보자.

1. 블록체인의 특징

- 블록체인은 하나의 블록이 이전 해시값(과거의 모든 거래내역)을 포함하고 있다.
- 이 블록은 네트워크에 참여한 다른 노드들이 검증하는 단계를 거친다.
    - 노드들은 `합의 알고리즘`을 통해 검증
- 즉, 위변조가 불가능한 데이터를 저장하고 공유 및 검증하기 때문에 이중지불이 불가능하다.

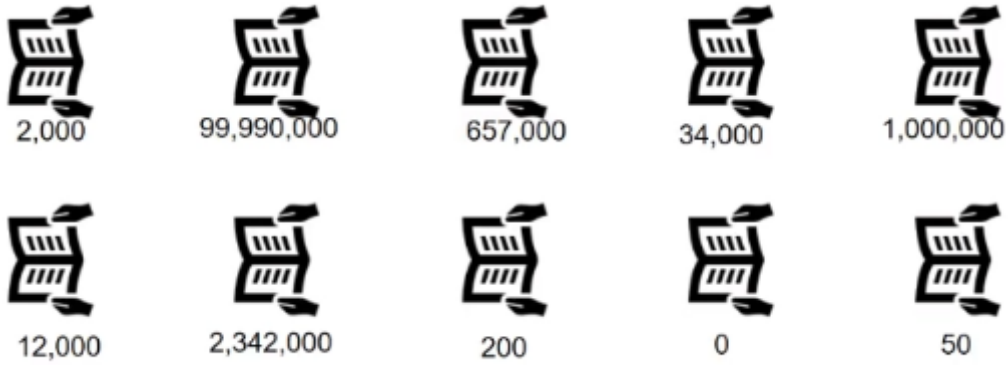
2. 합의 알고리즘

	작업증명 Proof of Work (PoW)	지분증명 Proof of Stake (PoS)	Byzantine Fault Tolerance (BFT)
제안자격 취득 방법	목표값 이하의 해시를 찾는 작업	플랫폼 토큰을 보유한 양 &기간에 따라 결정	정해진 순번 또는 정해진 확률에 의해
네트워크 참여 제한	없음	없거나 낮음	높음
합의에 필요한 연산량 및 비용	높음	낮음	낮음
위협	51% 공격	51% 공격	담합
대표적인 블록체인			

작업증명 (PoW)

1. 자격 취득: 목표값 이하의 해시를 찾는 작업을 무수히 반복함으로써 자신이 작업에 참여했음을 증명하는 알고리즘
2. 비용: 해싱값을 찾기 위해 매우 많은 연산을 한다. 합의에 필요한 연산량 및 비용이 높은 이유
3. 위협: 한 참여자가 전체 연산의 51% 를 연산한다면, 해당 블록을 참여자가 마음대로 쓸 수 있다. 해당 대한 합의에 참여자가 늘 이길 것이기 때문!

3. 신원확인 방법



- 블록체인은 익명성과 투명성을 특징으로 가진다. 그렇다면 계좌가 자신의 것임은 어떻게 증명할 수 있을까?
- 얼마가 들어있는지 공개 되어있는 이름없는 계좌
    - 공개키 암호화를 통해 주장할 수 있다.
    - 계좌의 공개키 주소를 가지고 있는 개인키로 복호화를 하였을 때, 복호화가 된다면 증명할 수 있다.
    - 이를 통해 출금 및 이체를 할 수 있다.

3. 블록체인의 종류

	PUBLIC	Private
참여형	ethereum	
제한형	Klaytn	ripple STELLAR corda HYPERLEDGER

1. 블록체인의 종류

1. 누구나 접속할 수 있고, 누구나 작업증명을 통해 블록을 재현할 수 있다 -> 비트코인, 이더리움
2. 모든 참가자가 허가 및 확인을 받아 합의해야 한다 -> Hyperledger, corda

2. 주요 암호화폐 비교

개발자	나카모토 사토시 (익명)	비탈릭 부테린
언어	C++	C++, GO, Solidity(Smart Contract)
합의 알고리즘	PoW	PoW -> PoS 변환예정
구현방법	UTXO 구조 (Unspent Transaction Output)	어카운트 기반 (EOA Externally Owned Account)와 Smart Contract로 구분

Block 125552

Hash: 00000000000000001e8d6829a8a21adc5d38d0a473b144b6765798e61f98bd1d
Previous block: 00000000000000e3a41b85b8b29ad444def299fee21793cd8b9e567eab02cd81
Time: 2011-05-21 17:26:31
Difficulty: 244 112.487774
Transactions: 4
Total BTC: 84.52
Size: 1.496 kilobytes
Merkle root: 2b12fcf1b09288fcaff797d71e950e71ac42b91e8bdb2304758dfcffc2b620e3
Nonce: 2504433986

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
51d37bdd87...	0	0.135	Generation: 50 + 0.01 total fees	15uNvBTUdMaiZ6d3GWCeXFu2MagXL3XM1q: 50.01
60c25dda8d...	0	0.259	1HuppjXc7dPrr2a67LqacDW5T4VunFrpqC: 29.5	1B8xLT5fi8KUPVJvyQftbc8WjruJyEarQ: 0.5 1RQbvzgRSLEsmv1JNe8MG76wdUgMwbsuvw: 29
01f314cdd8...	0.01	0.617	1NdzSE6qHubscXJtv7gJp2pddfL9L3ui6E: 0.03 1Jp9m5VvRUfc7VokfCvgE8KU5qkqcfnbsm: 0.02 1HcYJPpTm8DEpMmTb3YfKckX7ZcWPtmv: 4.82	175PNxeLc1YzTwwG6TcqywesHYdVqchbwC: 0.01 1MneNMRJmcqVQeqE7v4dqpgpNhhyxqq8R6: 4.85
b519286ad0...	0	0.404	12fDCoCVvDCkQShZ5RTh9ysgCkmkRMNQbT: 0.14 13CbwauXJPwkzY4XnaxqfkfnyNBwtHG9fe: 0.01	1Mox7p8fqJKBcYNRGHTdT5hBRxdMP6YHPy: 0.15

```
signedTransaction = {
    nonce: web3.toHex(0),
    gasPrice: web3.toHex(20000000000),
    gasLimit: web3.toHex(100000),
    to: '0x687422eEA2cB73B5d3e242bA5456b782919AFc85',
    value: web3.toHex(1000),
    data: '0xc0de',
    v: '0x1c',
    r: '0x668ed6500efd75df7cb9c9b9d8152292a75453ec2d11030b0eec42f6a7ace602',
    s: '0x3efcbbf4d53e0dfa4fde5c6d9a73221418652abc66dff7fddd78b81cc28b9fbf'
};
```

To가 일반 EOA계좌면 Value Transfer
To가 SmartContract계좌면 SmartContract 실행
To가 없으면 SmartContract 배포

4. 블록체인의 역사

> 블록체인 기반 암호화폐는 왜 탄생하게 되었을까?
>
> 왜 은행이라는 중개기관을 사용하지 않게 되었을까?

- 블록체인은 사이퍼 펑크라는 운동을 뿌리로 두고 있다.
  - 중앙집권화 된 국가와 거대 기업에 대항하여, 암호 기술을 이용함으로써 개인의 프라이버시, 익명성을 보장하는 탈중앙시스템을 만들고자 하는 사회운동
  - 중앙 집권화 된 국가 또는 거대 기업에 의존하지 않고자 하는 것이 철학
- 비트코인도 중앙 정부 정책 및 은행에 의해 화폐가치가 정해지는 것이 불안하다는 생각으로부터 시작 됨

- 내일 당장 은행이 망해버리면 누가 책임을 질 것인가?

5. 요약

- 은행은 송금시에 중계 역할로 한 쪽에서 차감 다른 쪽에서 입금해 줌으로써 신뢰와 `이중 지불 문제`를 해결한다.
- 블록체인의 자격 증명은 `합의 알고리즘`을 통해서 이중 지불 문제를 해결한다.
- 블록체인 암호화폐의 종류로 퍼블릭 타입의 참여 제한이 없는 암호화폐는 `비트코인과 이더리움`이 있다.
- 블록체인은 보안성, 투명성, 무결성, 탈중앙화의 특징을 가지고 있다.

6. 추가 자료

1. 이중지불

- 이중지불
- 이중지불에 관한 개념 정리

- **이중지불**(double spending)이란 원본 파일에 저장된 가치를 지불한 뒤, 해당 파일을 복사하여 다른 사람에게 또 지불하는 것을 말한다. 예를 들어, A가 B에게 1,000원이라고 기록된 파일을 전송한 후 다시 해당 파일을 복사하여 C에게 또 1,000원을 전송하는 것을 말한다. 영어로 **더블스펜딩**(double spending)이라고 한다.
- 컴퓨터와 인터넷에서 모든 파일은 복사가 가능하기 때문에 이중지불 문제를 피할 수 없다. 기존의 인터넷 시스템에서는 이중지불 문제를 피하기 위해 신뢰할 수 있는 중개기관을 두고, 중개기관이 보관하고 있는 기존 데이터에서 해당 금액만큼 차감하는 방식으로 가치를 전달했다. 결국 기존 인터넷 시스템에서 가치를 전송하려면 반드시 은행이라는 중개기관에 의존해야 했다.
- 블록체인은 과거의 모든 거래내역이 담긴 장부를 해시함수로 변환하여 하나의 파일로 만들어 전송하고, 그 결과를 블록체인 네트워크에 참여한 다른 노드들이 검증하게 함으로써 이중지불 문제를 해결할 수 있게 되었다.

2. 합의 알고리즘

- 작업증명 알고리즘이란?
- PoW 와 PoS 의 정의

- 비잔틴 장애 허용 알고리즘
    - **비잔틴 장애 허용**(BFT; Byzantine Fault Tolerance)이란 장애가 있더라도 전체의 3분의 1을 넘지 않는다면, 시스템이 정상 작동하도록 허용하는 합의 알고리즘이다. **비잔티움 장애 허용**이라고도 쓴다.
    - 비잔틴 장군의 문제

비잔틴 장군의 문제는 광활한 영토 지역마다 장군들이 통치하는 것을 가정한다. 이웃 나라 공격이 성공하려면 같은 날, 같은 시각에 모든 장군이 이끄는 병력을 집중시켜야 하는데, 이러한 목적을 달성하기 위한 메시지가 올바르게 전달되지 못하면 병력이 분산되어 공격은 실패하게 된다. 또한 장군들 가운데 배신자가 있다면 이러한 가능성은 더욱 커지게 된다. 여기서 비잔틴 장군 문제의 핵심은 동일한 내용의 메시지를 장군들끼리 공유할 수 있는 방법을 찾는 것이다