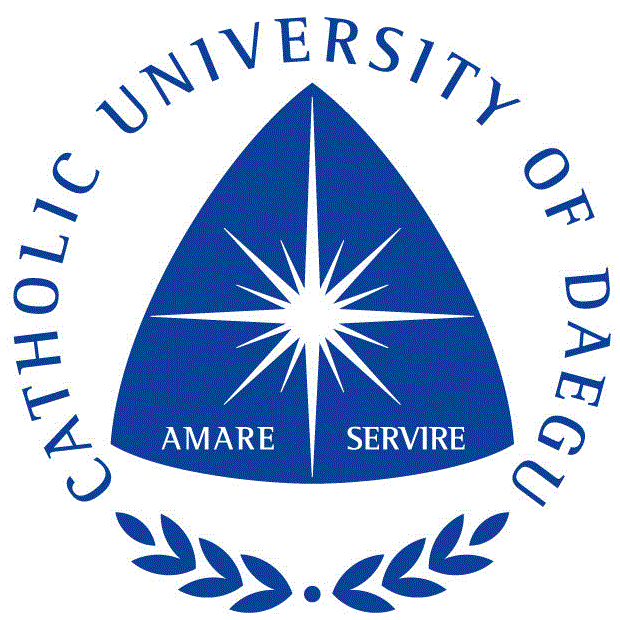
SUMMARY

대구가톨릭대학교 18학번 김성학



|  |  |
| --- | --- |
| **학과** | 컴퓨터공학전공 |
| **학번** | 18113699 |
| **이름** | 김성학 |
| **담당 교수** | 김기성 교수님 |

블록체인의 본질이 무엇인지, 실제로 가치가 있는지에 대한 가치 판달을 할 수 있게 하는 목적으로 작성하였음.

※ 본 내용은 개인적으로 공부하며 정리하는 내용이라 틀릴 수 있습니다.

**블록체인 개념 정리 v0.1**

**대구가톨릭대학교 18학번 김성학**

\*\* 1-1. 시사교양 느낌쓰(금융 시스템) \*\*

**배경** : 현재 인터넷 기반 상거래는 전자 결제를 처리할 신뢰받는 제 3자 역할(금융기관)을 전적으로 의존해 왔다. 이 시스템은 대다수 거래에 잘 동작하지만, 여전히 신뢰 기반 모델의 태생적 약점을 극복하지 못한다. [폐쇄적이고 복잡한 현재의 전자 금융 시스템]

이걸 P2P로 쉽게 쉽게 거래하면 되는데 왜 못하는가?

디지털 데이터를 자산화하기 어렵기 때문

그 이유: 디지털 데이터는 위조(복제)와 변조가 쉽다.

**\* 디지털데이터 특징**

1. 복사 하기 쉽다. Ctrl+c, Ctrl+v

2. 파일 전송하기 쉽다. @이메일, 카카오톡

이러한 특징은 돈이 가지지 말아야 될 특징과 정확하게 일치한다. = 돈은 위조**X**, 변조**X**

즉, 돈을 디지털화하기 매우 까다롭고 어렵다.

그래서 어떻게 하냐? 신뢰할 수 있는 금융기관이 돈을 데이터화시켜서 보관을 한다.

그러면서 금융감독기관이 이 금융기관들을 감시한다. 변조하지 않았지, 복제하지 않았는지.

그리고 인증기관이 돈을 데이터화시켜서 혼자서 다루기 때문에 매우 폐쇄적이다.

**\* 송금 시스템**

그 상황에서 사용자들이 이 디지털화된 돈을 다루려면 내 돈이다라는 것을 증명해야된다. 즉, 신원인증 해야됨 (디지털 서명: 공인인증서)

인증서 만료되면 갱신. 다른컴퓨터에 있으면 또 옮기고.. 매우 불편하다.

\* 복잡한 **결제 프로세스 (흐름이 클수록 수수료 多多)**

송금보다 더 복잡하다. 그리고 시중에는 금융기관이 하나가 아니다. Ex) 농협, 국민은행, 우리은행, 신한은행 등등, 또 카드사도 여러 군데 있다. Ex) 카카오뱅크카드, 토스카드 등등

그 많을 것들을 통합해 줄 서비스가 또 필요. 그것이 바로 (오프라인) VEN사, (온라인) PG사

만약에 이 복잡한 시스템에 블록체인이 들어온다고 하면 사용자가 상품주문을 한 후 그 해당 블록체인에 트랜잭션을 전송하면 되고, 가맹점은 몇 분 후에 그 트랜잭션이 블록에 담겼는지 확인을 하고 상품 배송 (결제 프로세스가 매우 단순해짐)

- 즉, 블록체인 **짱!!!**

블록체인이란?

개방형 금융 플랫폼

금융의 간소화

● 결제 프로세스를 단순화시켜 효율성을 높일 수 있다.

● 결제 프로세스의 단순화에 따른 수수료 절감 효과가 발생한다.

금융의 개방화

● 허가가 필요 없기 때문에(비허가성) 시스템에 참여하거나 떠나는 것이 자유롭다.

● 따라서 누구나 금융 서비스에 자유롭게 참여하거나 떠날 수 있다.

금융의 대중화

● 금융 기관이 아니더라도 누구나 금융 서비스를 설계하고 구축할 수 있다.

● 누구나 사람의 개입이 필요한 금융 시스템을 자동화 할 수 있다.

\*\* 1-2. 시사교양 느낌쓰 (비트코인의 탄생 배경)\*\*

[리먼 브라더스, 양적 완화 정책]

[문제발생 - 문제원인 - 해결방법 - 결과 - 현재상황]

■ **이전 금융시스템의 문제점 :** 1938년 경제 대공황부터 싹이 자라나기 시작. 2008년 09월에 리만 브라더스가 파산신청 등과 같은 시대적 배경으로 금융위기가 많았다. (제 3자, 원초적인 약점)

-> 구제금융은 정부가 기업을 **세금**으로 보조해주는 것인데, 신용등급도 자세히 측정하지 않고 채권을 계속해서 유동화시켰고 방만하게 사람들에게 돈을 빌려줌.

그렇게 은행들이 수익을 엄청나게 올리다가 몇몇은 구제, 나머지는 결국 파산

결국, 그 파산으로 인한 피해는 국민들이 본다. (경제 위기 -> 실업자)

그런데 기업을 세금으로 보조해준다? (시민 입장: 불합리)

또한 양적 완화라는 정책을 실시.

주로 부실 채권들을 정부가 사줌으로써 돈을 시장에 품.

-> 1. 물가 상승

-> 2. 자산 가격도 상승

일반시민 입장) 자신은 실업자가 되는데 물가는 오르고 주식 가격도 오름.

**주식O**, 부자는 더 부자 **/** **주식X**, 가난한 사람들은 더 가난해짐 -> 빈부격차 커짐

이 문제의 주범은 정부가 돈을 찍어낼수 있는 발권력이 있기 때문에 이러한 일들이 발생!!

이러한 구제금융에 대해 사토시 나카모도가 비판.

그러므로, 사토시 나카모토가 국가로부터 일반 시민에게로 발권력을 빼앗아하고 싶어함.

-> 국가가 임의로 통화를 발행하지 못하게 저런 일이 발생하더라도 시장 원리에 따라서 잘못한 사람은 망하고 일반 사람들은 피해보지 않도록 어떤 규칙에 의해서 발행이 되도록 만드는 새로운 화폐를 개발함.

★ [영화] 빅쇼트(2016), [다큐멘터리] 비트코인: 암호화폐에 베팅하라(2016) 추천

=====================================================================================

현재? : 돈을 가지고 있으면 자산 가격이 계속 하락 (화폐 가치↓) => 돈이 아닌 무언가 가지기 시작 (원래는 금을 사거나, 부동산을 삼. 하지만 너무 비싸서 요즘은 주식, 코인)

그리고 원래 비트코인은 국가로부터 발권력을 빼앗아와서 국가가 이런 짓을 못하도록 하는게 목적이지만, 그런데 10년이 지난 지금의 상황을 보면 비트코인이 그런 목적을 완전히

달성**X** -> 아직 국가가 강력한 발권력을 가지고 있고, 돈을 여전히 찍어내서 경제를 살릴려함.

하지만 비트코인이 한 가지 바꿔놓은 것: 돈을 찍어내는 것에 대한 어떤 헷지 포지션(가격 고정 또는 스테이블 코인처럼 파생상품으로 가격 고정)을 사람들이 잡을 수 있게 만들어줬다. (총 발행량이 한정되어 있고, 발행되는 것도 블록당 몇개로 한정되어 있음)

그래서 사람들이 비트코인을 이용해서 자신들의 자산을 형성하고 지키고 싶어함.

그리고 요즘은 비트코인을 이용해서 디파이 서비스로 다른 상품들을 파생시켜나가고 있음.

-> 즉, 비트코인을 담보로 다른 자산을 빌려가지고 파생시키는 금융 서비스들을 만들어내는 시도를 많이 하고 있음. (비트코인 유동화) -> 결국 비트코인은 계속해서 중요한 지위를 가지고 있을 것이고 이걸 담보로 다른 상품들을 만들어내기 때문에 비트코인에 대한 수요↑↑

=====================================================================================

논문 : 2008년 10월 31일, 비트코인 아이디어 최초 공개 - 사토시 나카모토(가명)

**“Bitcoin: A Peer-to-Peer Electronic Cash System” 논문 발표 [P2P 금융 시스템인 비트코인을 제안]**

■ 은행과 같은 중앙기관 없이 시스템에 의해 화폐가 발행되고, 네트워크 참여자들의 자발적인 참여에 의해 자산을 거래할 수 있는 시스템을 설계하고 구현하였다.

=====================================================================================

/\* 이러한 문제점을 해결하기 위해 나온 해결책이 바로 **블록체인**이다.

요약: 블록체인은 장부를 작성하는 거에 대한 일종의 알고리즘이다. \*/

\*\* 2. 집중적으로 파헤치는 느낌쓰 (비트코인 동작의 원리)\*\*

자산이 디지털화가 되기 힘든 이유 :

데이터는 복제가 쉽고, 조작이 쉽다는 특징을 가지고 있음.

이러한 특징은 화폐 및 증권이 가지지 말아야 할 특징임.

-> 전자금융 시스템을 만들기 위해서는 신뢰할 수 있는 기관이 들어와서 자산을 디지털화 해주고 사람들은 그 신뢰 기관을 통해서 디지털화가 된 자산을 거래할 수 있다.

하지만, 비트코인은 신뢰할 수 있는 기관이 없이도 P2P로 그러한 금융 시스템을 만들었다.

어떻게 만들었을까??

1. 신원 인증을 없앰. (디지털서명을 통해서) [트랜잭션을 보낼 때 전자서명을 하는 기술]

금융 거래를 할 때, 내 자산이 서버에 데이터화가 되어있는데, 그 자산에 대한 변경권, 송금을 하거나 결제를 하거나 할때, 그게 내 자산이라는 걸 증명해야됨. -> 공인인증서, 카드인증을 통해 본인을 확인하는 절차를 먼저 가짐. -> 결국, 신원 인증기관에 정보를 맡기고, 등록해야지만 전자상거래에 참여할 수가 있다. -> 신원 인증 때문에 거래를 자유롭게 할 수 없음.

그래서, 사토시 나카모토는 전자서명을 통해서 신원 인증 과정을 없앰.

누구나 지갑 프로그램을 깔면 그 프로그램을 통해서 주소를 만들어서 거래를 할 수가 있는 시스템을 만들었음.

2. 이중지불 문제가 발생했을 때 이것을 해결하기 위한 합의 알고리즘 만듬.

즉, 어떤 자산을 거래를 할 때, 그 자산의 소유주만 거래를 할 수 있게 만들어줬다고 해도 그 소유주가 같은 자산을 송금하는 트랜잭션을 2번 이상 발생시킬 수가 있다. 그랬을 경우에 둘 중 뭘 인정할 거냐는 문제.

(자신의 자산을 가지고 이 시스템을 공격할 수 있음, Double Spending Problem)

=====================================================================================

이때, 트랜잭션이란? 금융 거래를 의미.

데이터베이스에서는 데이터의 어떤 상태를 바꾸는 단위가 트랜잭션

비트코인에서는 거래의 의미로써, 누가 누구에게 돈을 보내는 데이터가 담긴 상태의 변경 단위를 **트랜잭션**이라 부름.

트랜잭션

■ 트랜잭션에 디지털 자산의 거래에 대한 데이터(송금 및 결제)를 담을 수 있다.

■ 디지털 자산을 거래할 때는 그 자산에 대한 소유권을 가진 참여자만 해당 트랜잭션을 발생시킬 수 있어야 한다.

■ 이 때 필요한 것이 전자서명 기술이고, 공개 키(Public key) 암호화 방식이 주로 사용된다.

■ 공개 키 암호화 알고리즘에 비밀 키(secret Key)를 시드(seed)로 하여 공개 키(public Key)를 얻을 수 있다.

■ 비밀 키를 사용하여 원본 데이터의 전자서명을 얻을 수 있고, 그 전자서명의 유효성을 원본 데이터와 공개 키로 검증할 수 있다.

공개키 암호 방식 : 타원 곡선을 이용하여 만듦. \*어려워서 생략 [' - ']

[ 더 알고 싶으면 '지미송'이 쓴 비트코인 서적 볼 것 ]

이 공개 키 암호화 방식을 통해서 어떻게 트랜잭션을 검증하는지를 알아보자!!

이 전에 먼저 알아야될 용어:

해시 함수(Cryptographic Hash Function (CHF))

■ 임의의 데이터를 일정한 길이의 문자열로 바꿔주는 \*단방향 함수

\*단방향 함수 : 어떤 입력값을 통해서 출력값을 도출해내기 쉽지만, 반대로 출력값을 가지 고 입력값을 찾기는 매우 어려운 함수를 의미

안녕하세요 -> c465 a465 ab4d 56f4 56c4 b65f 4f65 a4f9

안녕하세여 -> 56ac 6164 6846 5ac4 65f4 5d45 465f 48ff

■ 조금만 달라도 확 달라진다!!

■ 같은 입력값은 항상 같은 출력값을 출력하기 때문에 결정적(deterministeic)이며, 검증(verification)이 쉽다.

=====================================================================================

공개 키 방식을 이용한 트랜잭션의 서명 및 확인 과정

[트랜잭션 -> (해시) -> 해시값 -> (비밀 키) -> 전자서명]

[사용자 -> 트랜잭션 및 전자서명 -> 블록체인 네트워크]

|| 같은 해시함수를 써서 트랜잭션을 해시값으로 도출

|| 공개키를 가지고 전자 서명을 검증 -> 도출된 해시값 == 검증된 해시값[T]

=====================================================================================

즉, 이 비밀 키를 가지고 각 유저는 자신의 자산에 대한 소유권을 증명할 수 있다!!

하지만, 전자서명으로 못 막는 것이 있다. 그것이 바로 이중 지불 문제

예) 1,000원을 가지고 있는 사람이 두 사람에게 동시에 각 1,000월을 송금하는 트랜잭션을 발생시키는 경우

비트코인은 P2P시스템이기 때문에 모든 피어들이 같은 선택을 해야됨.

이러한 경우에 어떤 트랜잭션을 맞는 것으로 합의할 것인가에 대한 문제가 발생한다.

분산 네트워크] 이러한 문제를 해결하는 알고리즘 : 합의 알고리즘(consensus algorithm)

이중 지불 문제를 **비잔틴 장군 문제로 치환**

[상황] **비잔틴 장군 문제 (BFT)**

1. 적군의 도시를 공격하려는 비잔티움 제국군 여러 부대로 나눠져 있는데, 한꺼번에 성을 공격해야지만 성공(Victory), 이때 각 부대는 전령을 통해서 소통을 함.

2. 각 부대를 이끄는 장군들 중에서 배신자가 있을 수 있음. 그 배신자가 공격 즉, 합의를 방해한다면 이 비잔틴 제국군의 공격은 실패할 수 있음.

3. 이러한 상황에서 배신자가 아닌 나머지 장군들이 힘을 합쳐서 성을 공격하기 위해선 어떻게 해야될까?

\*가정\*

■ 배신자의 수가 전체 장군의 수(n)의 ⅓미만 일때,

■ 모든 메시지는 올바르게 전달이 되고 믿을만한 채널을 사용

■ 모든 메시지가 동기적으로 전달된다는 것이 중요!!

(동기적: 전령들이 시간차를 두고 움직이지 않고 한꺼번에 움직여서 메시지를 한꺼번에 받음)

■ 1. 사령관이 장군1, 장군2, 장군3(배신자)에게 “공격”하라는 메시지를 보냄

2. 장군1은 장군2와 장군3(배신자)에게 “공격”하라는 메시지를 보냄

3. 장군2는 장군1과 장군3(배신자)에게 “공격”하라는 메시지를 보냄

4. 장군3(배신자)은 장군1과 장군2에게 “퇴각”하라는 메시지를 보냄

**다수결**로 정함.

이때, 장군1은 “공격”메시지 2개와 “퇴각”메시지 1개를 가지고 있음 (공격)

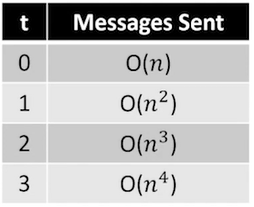
나머지도 마찬가지.

즉, 메시지를 다 받은 다음에 다수결에 따르면 어떻게 행동해야 될지를 알게 된다.

그래서 전체 노드들 중에서 배신자의 비율이 3분의 1보다 적다면 비잔틴 제국군은 적군의 성을 함락시킬 수 있다.

단점: 계속 메시지를 주고받아야되기 때문에 합의에 필요한 메시지의 수가 기하급수적으로 증가한다. (t : 시스템이 돌아가고 나서 정해지는 값, n: 미리 정할 수 있는 값)

Ex) 배신자의 수(t), 전체 노드의 수(n)일 때,



t= 0일 때, n에 비례

t=1일 때, n²에 비례

t=2일 때, n³에 비례

t=3일 때, n⁴에 비례

n이 늘어나면 t가 늘어날 때, 메시지의 수가 기하급수적으로 증가

※ 이러한 시스템은 n을 마구 늘리지 못함. -> (시스템에 부하가 많이 걸리기 때문)

이런 전통적인 합의 알고리즘을 BFT(Byzantine Fault Tolerance)라고 부름.

그것을 잘 쓸 수 있도록 변형시킨게 PBFT(Pratical Byzantine Fault Tolerance)이라고 함.

우선 이러한 시스템 BFT는 노드의 수가 일정 이상 커질 수가 없고, 이 시스템에서 컴퓨터가 꺼지거나 네트워크가 단절되거나 하는 상황이 발생해서 과반 이상의 노드가 이탈하게 되면 합의를 이룰 수 없음. 노드의 수↑ => 부하↑ // 새로운 노드가 자유롭게 들어올 수 없음.

**단점 :** 메시지 패싱 방식으로 합의를 하기 때문에 노드 수가 많아지거나 적어지면 합의가 어려움. (도중 나갔다가 들어올 수 있는 구조가 아님!! 이미 정해진 노드 수)

결국, 폐쇄적인 시스템 // PBFT는 적합한 합의 알고리즘 X,, 비트코인이 원하는 합의 알고리즘이 아님!! (PBFT 방식은 돌아가면서 블록을 만듦)

그 후에 나온 것이 PoW, PoS 합의 알고리즘!!

\*\***비트코인을 단위로 알아보자!**

비트코인 : 일렉트로닉 캐시 시스템,

돈을 다루는 시스템, 즉 이 시스템에서 돈을 전송하는 단위를 트랜잭션이고, 그 트랜잭션을 묶어서 하나의 블록으로 패키징하고 그 블록으로 합의를 하는 것

비트코인에서 합의의 단위: 블록 (그 후에 나온 모든 블록체인들도 블록 단위)

■ 블록 : 합의(consensus) 및 P2P네트워크의 상태를 동기화(state synchronization)시키는 단위

■ 블록에는 서로 모순되지 않는 트랜잭션들을 모아서 처리한 뒤 이 후의 상태가 유효한 것들만 담긴 블록 상태(block state)를 만든다. (이때, 비트코인은 UTXO구조를 가진 트랜잭션을 블록에 담음) UTXO에 대해 공부 해보자

■ 이렇게 처리 후 다음 블록을 생성한다. 이때, 새로 생성된 블록은 그 이전 블록의 데이터의 요약본, 블록의 해시 값을 포함을 시켜서 새로 만듦.

그렇게 해서 선형적으로 블록이 증가하도록 함.

요약 : 각 블록은 트랜잭션들의 집합이고, 트랜잭션들의 집합은 그 트랜잭션들을 처리하고 난 후 상태(state)이다. 그 상태는 각 어카운트들의 금융 상태를 의미한다. (누가 얼마나 가지고 있음 등등)

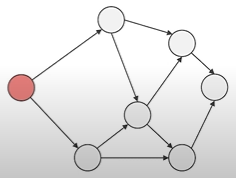
그 금융 상태를 기반으로 그다음 블록에서 트랜잭션들을 수행을 하게 되면 그 다음 상태가 생성될 것. 또 그 상태라는 정보를 가지고 블록을 만들고, 이처럼, 블록이 진행될수록 금융 상태가 블록 단위로 분절되어서 업데이트 된다는 것을 알 수 있음.

**\*\*그 블록이 어떻게 네트워크에 전파(propagation)되는지에 대해 알아보자!!**

가십 프로토콜(gossip(소문) protocol) or 에피데믹(epidemic)[전염병처럼 퍼짐]이라고도 불림

모든 노드들에게 한 번에 전파 = 대역폭의 낭비(Bandwidth), **비효율**

트리 형식으로 연결하여 전파 = 도중에 노드가 나가면 그 후 자식트리 전송 **실패**



메시지를 전파하는 노드가 자기의 이웃들에게만 메시지를 전파 = 받는 메시지가 중복되지만 허용, 그 이유 도중에 노드가 나가도 연결됨, **안정적**

전염병처럼 처음에 전송속도는 느리지만 후에는 빠름 = **비효율X**

즉, 가십 프로토콜로 인해 모든 노드들이 금융 상태를 가질 수 있음.

모든 노드들이 유효한 금융 상태를 가지고 있으면 그다음 블록을 만들어서 네트워크에 전파

누가 이 블록을 만들 것이냐?

■ 비트코인은 참가와 떠나는게 자유로운 개방형 네트워크이기 때문에 누구나 블록을 생성할 수 있어야한다.

■ 하지만 누구나 블록을 생성할 수 있으면서 블록 생성 속도가 네트워크 전파 속도보다 빠르면 쉽게 경쟁 상태(race condition)에 빠지게 되어 단일한 전역 상태를 만들 수 없다.

■ 따라서 누구나 블록을 생성할 수 있으면서도 단일 최신 상태에 도달할 수 있는 새로운 합의 알고리즘이 필요한다.

이중 지불 문제를 **비트코인의 합의 알고리즘으로 치환**

그 해결법이 바로 랜덤 타이머를 두는 것!!

ㅇ