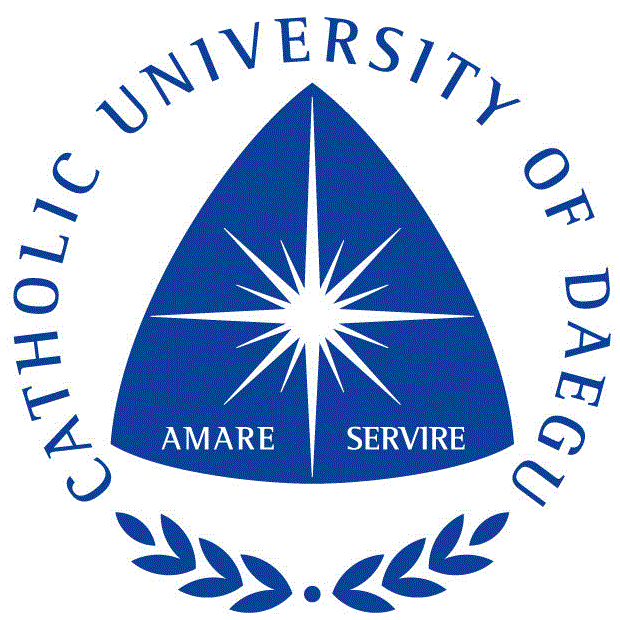
SUMMARY

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)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) [트랜잭션과 전자서명 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 문제(double spending problem)와 합의 알고리즘

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.