NewWave
Week2
BitCoin

ESTD 2020
NewWave
- STUDY-

Agenda

01 What is Bitcoin(₿)?

02 About Currency

03 History of BTC

04 About BTC

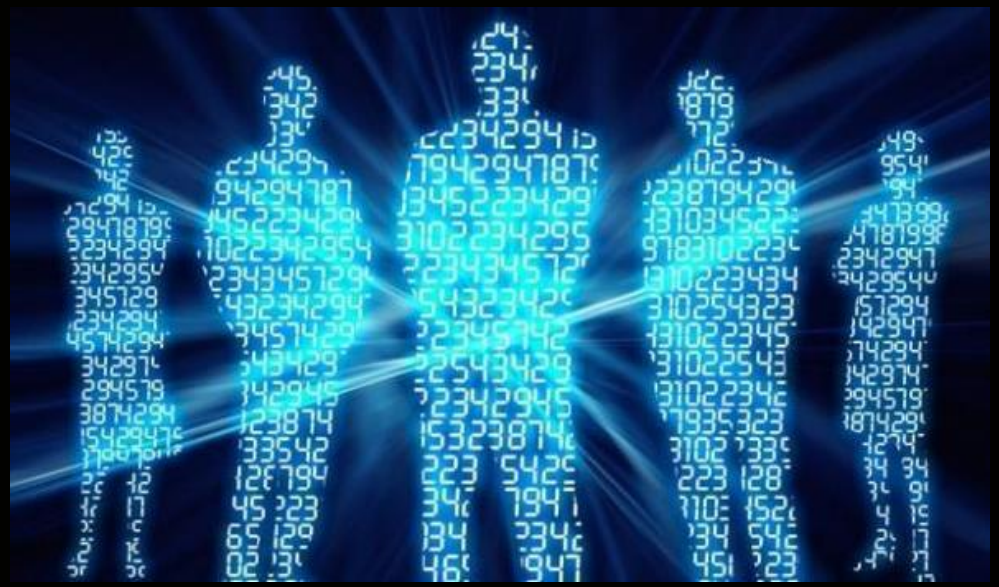
What is Bitcoin?

BitCoin(=BTC)

블록체인 기술을 기반으로 만들어진

세계 최초의 분산 디지털 암호화폐

사토시 나카모토



세계 최초 암호화폐인 비트코인(bitcoin)을 만든 사람이며 블록체인 기술의 창시자이다.

이름은 일본인이지만, 국적, 성별, 나이, 단일 인물 유무, 사망 유무도 알려지지 않아서

그가 정확히 누구인지는 아무도 모른다.

About Currency

Yap Island

Rai Stone

화폐는 그 자체로서 가치가 있는 것이 아닌,

내가 속한 공동체가 그것이 가치가 있다고

‘신뢰’하고 ‘보증’해주기 때문에 가치가 있다.

화폐의 진화

01 **식품 및 물품화폐**

고대시대 보리, 밀 같은 식품화폐부터
조개껍데기와 같음 물품화폐 사용

02 **금속화폐와 지폐**

현재까지도 사용되는 금속화폐(동전)과 지폐
대부분 사람들이 화폐를 하면 떠올리는 개념

03 **전자화폐**

현대화폐의 가장 최신버전으로,
현재 사용되는 화폐의 87%가 신용카드 및 계좌잔고
등 물리적 실체가 없는 단순한 숫자로 존재

04 **암호화폐**

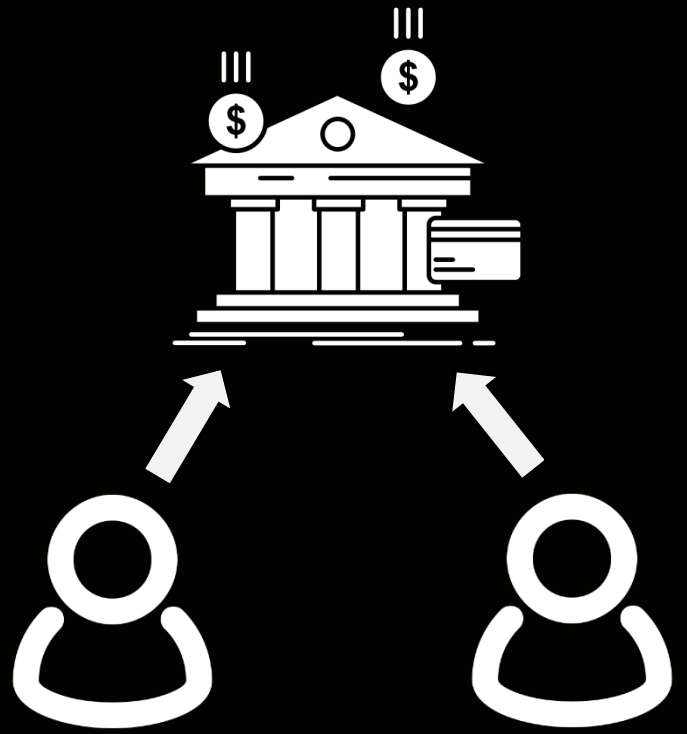
블록체인(blockchain) 기술로 암호화되어,
분산발행되고 일정한 네트워크에서
화폐로 사용할 수 있는 전자정보

전자화폐의 문제점

이중지불 문제

디지털 데이터의 특성상 쉽게 복사가 가능하며,
원본과 복사본의 차이가 없다.
즉 신뢰를 잃을 수 있다는 의미이다.

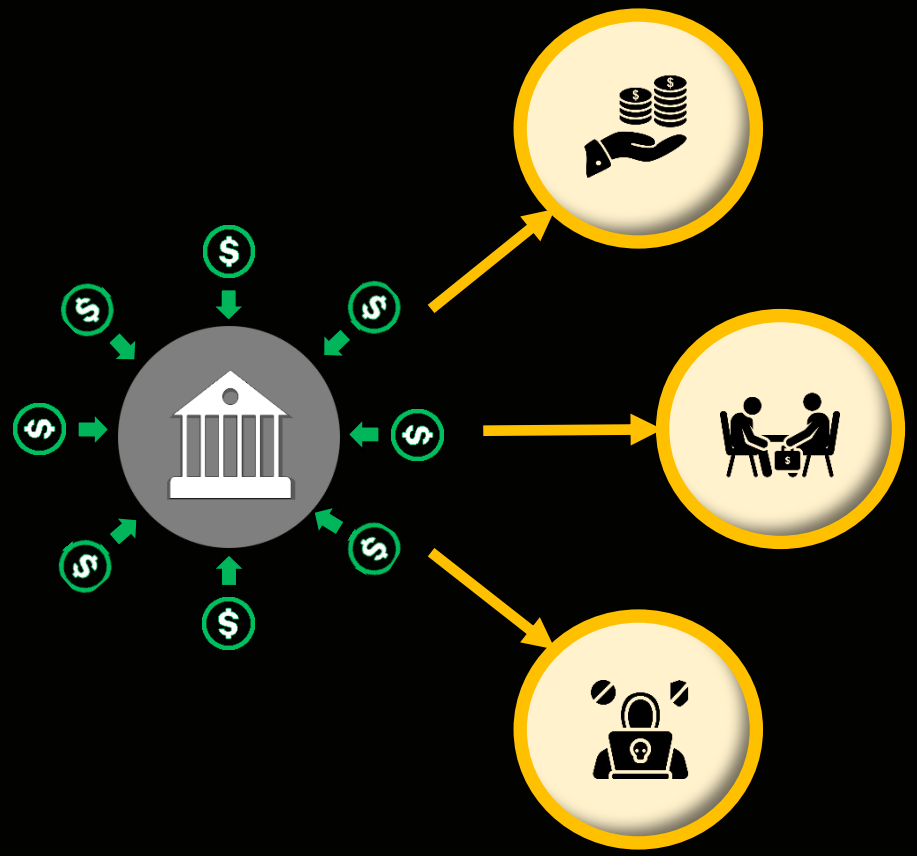
해결



제 3자(국가, 은행) 관리

모든 사람들은 제 3자가 관리를 잘 할 것이라 믿고,
문제가 생기면 제 3자가 책임을 진다고 생각하여
통장에 있는 찍혀있는 숫자가 화폐로 사용되는 것이다.

중앙집중화의 문제



#중개비용 발생

장부의 신뢰성을 보증하기 위해
복잡한 프로세스를 거치게 되어 중개비용이 발생한다.

#중앙기관의 무능이나 부패

제 3자가 믿을 만한지도 문제가 된다.
대부분의 나라에서는 국가기관이 화폐에 대한 통제권을 가지고 있어,
국가정책에 개인들은 어쩔 수 없이 따라야한다.

#해킹의 타겟

장부가 한 곳에 집중 되어 있으므로
해커들이 노리기 쉬워진다.

History of BTC

CyperPunks
(Ciper + Punk)

1980년대부터 컴퓨터와 인터넷의 발달로 정부와 거대 기업이

개인의 사생활과 관련된 모든 정보를 수집할 수 있게 되자,

정부나 거대 기업들이 개인정보를 알 수 없도록 **암호기술을**

사용함으로써 프라이버시를 보호하고자 한 사회운동가들

그 중 한 분야가 '**암호화폐**'분야였다.

그 이유는 오프라인 거래는 흔적을 남기지 않지만,

온라인 거래의 경우 모든 정보들이 기록 및 공개되기 때문이다.

BTC 이전 암호화폐 역사

E

E-Cash

데이비드 차움(David Chaum)

1980년대 후반 온라인 트랜잭션의
개인 정보 보호에 초점을 맞춘
것으로 최초의 상업적 암호화폐

★

CyperPunk 선언

1993년 중앙집권화된 국가와 거대 기업들로부터
개인의 프라이버시를 보호하기 위해
암호화된 익명 거래 시스템을 개발할 것을 제안

H

HashCash

아담 백(Adam Back)

1997년 익명성을 보장하고
이중지불을 방지할 수 있는
암호화폐 생성

B

B-Money

웨이 다이(Wei Dai)

1998년 익명성과 분산 방식의
암호화폐인 비머니(B-Money)를 고안

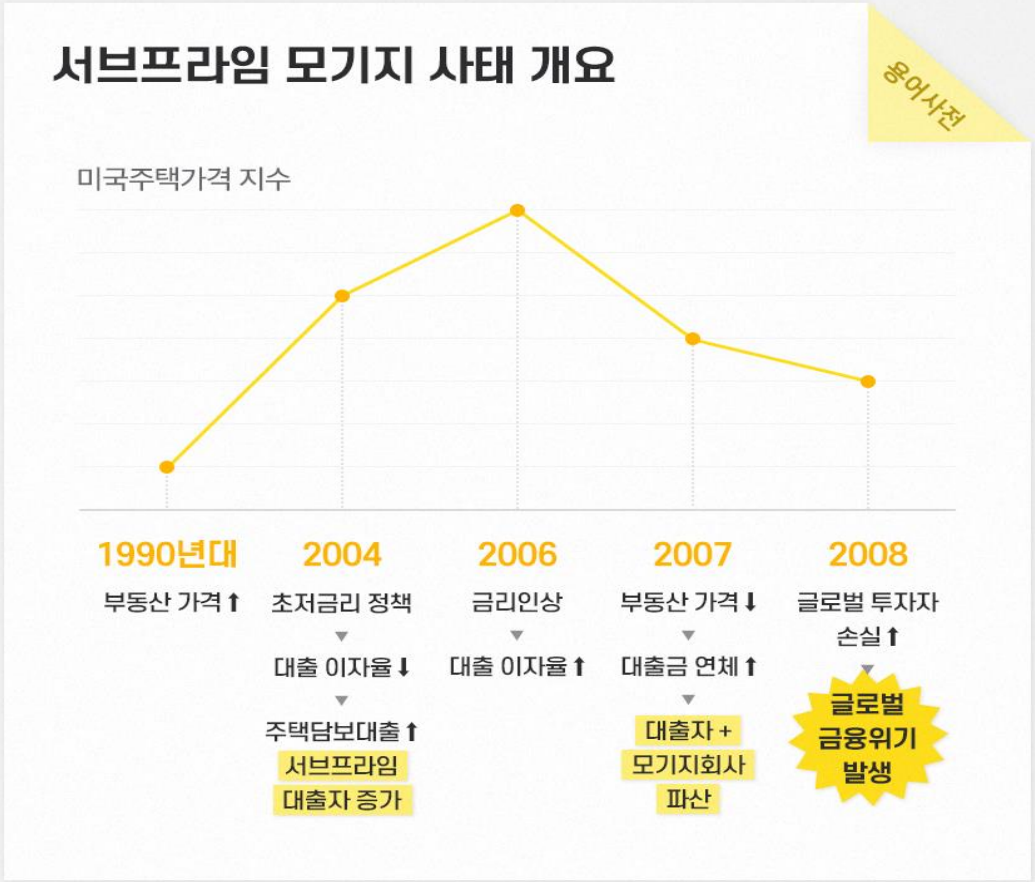
BITGOLD INTERNATIONAL

Bit-Gold

닉 재보(Nick Szabo)

1998년 스마트 계약 기반의
암호화폐인 비트골드(bit gold)를 고안
→ 2004년 HashCash기반
'재사용 PoW'활용하여 비트골드 제안

미국發 세계경제위기



1 미국의 초저금리정책(~ 2004)

2000년대 초반의 IT거품붕괴, 2001년 911사태, 2003년 아프간 전쟁 등으로 미국의 경기는 침체를 겪음

→ 자국의 경기를 부양하기 위해 **초저금리 정책** 실시

2 서브프라임 모기지 사태(2004 ~ 2007 ~)

정책으로 인해, 낮은 신용등급의 사람들에게 쉽게 대출 해주는 주택담보대출 상품 '**모기지론**' 등장 → 너도나도 대출

2004년 초 저금리 정책이 끝나자 상환이 불가능한 상황 발생

3 리먼 브라더스 사태 (2008 ~)

그 결과 작은 업체부터 연쇄적으로 파산하며,

마지막으로는 거대 투자은행 '리먼 브라더스' 까지 파산함

→ 미국은 **자국우선정책**을 펼치며 세계경제위기를 만들어 냄.

비트코인의 시작

미국發 경제위기는 세계 경제 위기를 만들어 내게 된다.

전 세계적으로 부동산의 가격과 주식의 가격은 폭락하게 되고,

***문제의 원인은 무능한 정부가 금리 조정과 화폐를 찍어내는 것이라 생각하는 사람들이 생기기 시작한다.**

이런 시대적 배경 속에서 **사토시 나카모토(Satoshi Nakamoto)**라는 익명의 사람은

은행과 같은 중앙기구가 없더라도

네트워크 참여자들에 의해 P2P 방식으로 스스로 작동하는 새로운 화폐 시스템을 구상하였다.

2008년 11월 1일 〈Bitcoin: A Peer-to-Peer Electronic Cash System〉이라는 9쪽짜리 논문을 작성하고,

https://bitcoin.org/bitcoin.pdf 사이트에 올렸다.

Genesis Block 발행

2009년 1월 3일 오후 6시 15분 05초

비트코인의 최초 블록인 제네시스 블록 탄생하였다.

이로 인해 50개 비트코인이 처음으로 채굴되었다.

비트코인 최초의 거래내역 메세지의 문구는 다음과 같은 말이 적혀 있었다.

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

사토시 나카모토는

블록체인 기술을 이용함으로써 **익명성이 보장**되는

탈중앙화된 세계 최초의 암호화폐인 비트코인 개발에 성공했다.

이로써 사이퍼펑크 운동가들이 오랫동안 꿈꾸던

"익명성을 보장하는 암호화폐 시스템"이 마침내 실현되었다.

About BTC

중앙기관X 데이터 신뢰 보증방법

How??

bitcoin

어떻게 화폐로서 기능하는가?

#BTC시스템

비트코인은 모든 거래 기록이 담긴 장부를
참가자들에게 나눠줌으로서 신뢰를 보증한다.

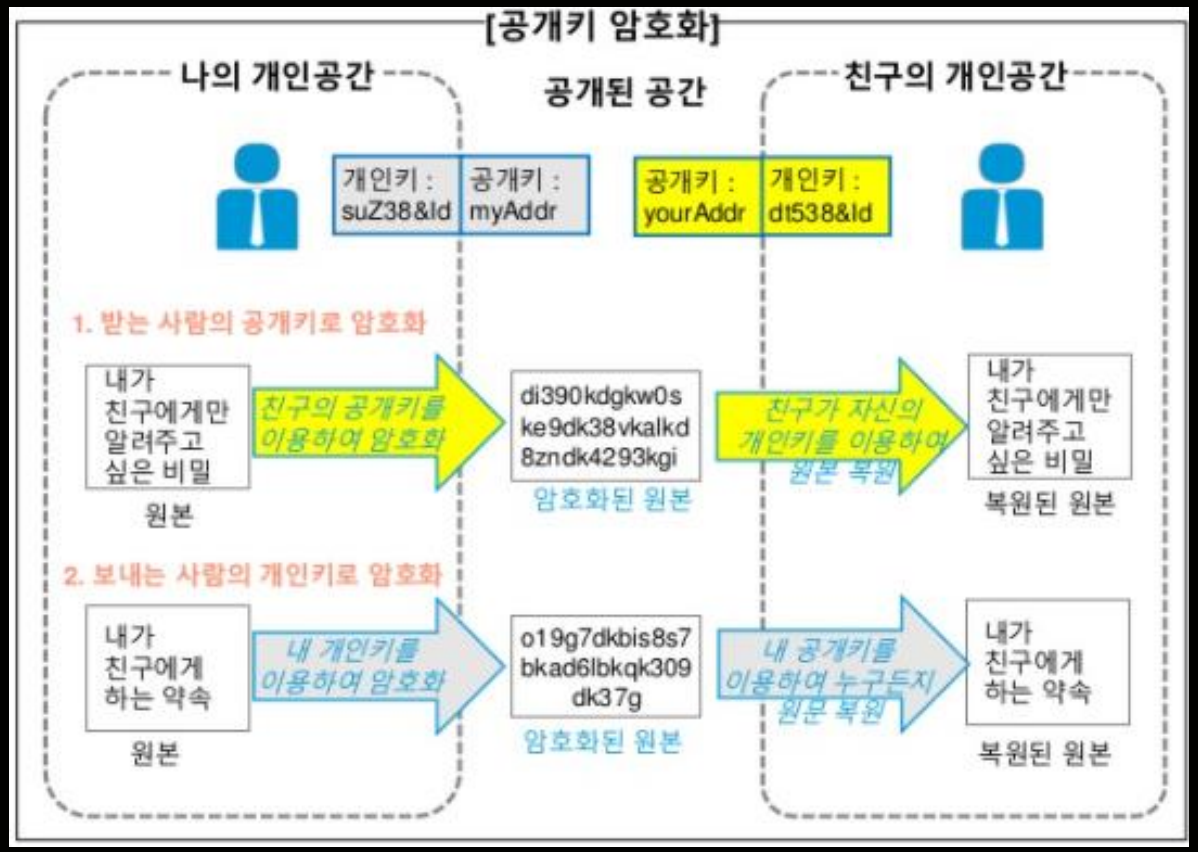
참가자의 장부를 50%넘게 해킹하지 않는 이상,
실제 거래로 인정되지 않는다.

서로서로의 감시자 역할을 하기에 신뢰가 생겨,
장부에 적힌 숫자가 '화폐'로 기능한다.

비트코인 관련 기술


비트코인의 거래 절차와 관련 기술
P2P 네트워크
지갑 만들기
거래
배포
거래 검증
블록 생성
확인
거래 종료
보상금 지급
디지털 서명(비밀키/공개키 암호화, 해시함수1*)
채굴(Mining), 합의 알고리즘)
블록, 블록체인
블록 암호화(해시함수2*)

공개키 암호화



- **개인 키(Private Key)**

비밀로 유지되는 '키'로서 양쪽에 공유되지 않고 한쪽 만 보유

(접속 및 송금시 비밀번호)

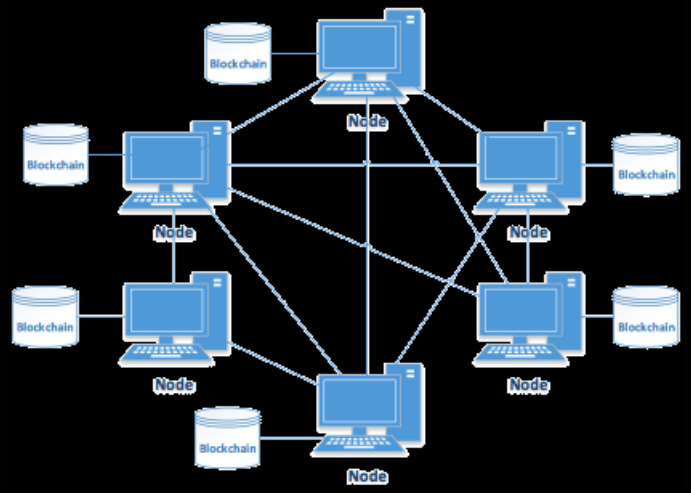
- **공개 키(Private Key)**

비밀이 아니며 널리 공유한 '키'

(송금 될 주소 or 돈 받을 주소)

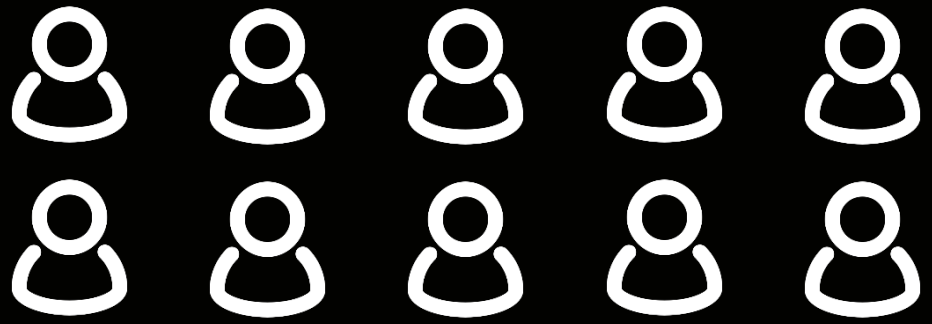
P2P Network

비트코인은 모든 사람들이 참여를 하고 싶으면 참여 할 수 있는 시스템으로
각자 자신의 컴퓨터의 성능을 제공하여 시스템의 일원이 된다.
이때 각각의 컴퓨터는 **노드(Node)**라고 말할 수 있으며,
각각의 노드들은 다른 노드와 연결이 되어 있고, **클라이언트와 서버역할** 수행
서로 간에 통신으로 **데이터 동기화와 감시 역할을 수행한다.**



BTC참여과정_1단계

#10명의 참가자(=Node)



#준비물

빈 종이 펜 파일 특수기계 (해쉬함수)

① 장부 기록

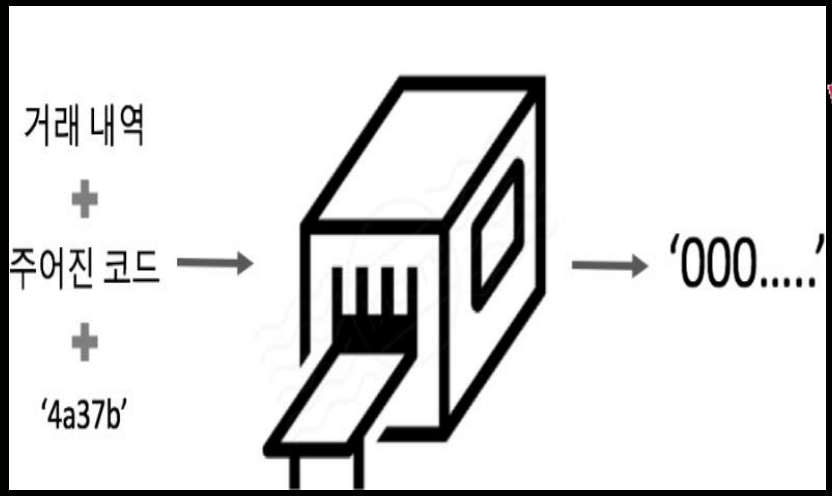
10명의 참가자들은 서로 돈을 주고받을 때 마다,
그 내용을 다른 참가자들에게 알린다.

BTC참여과정 _2단계(해쉬함수)

② 거래기록 봉인

내용을 기록한 종이가 **진본**이며,
위변조가 되지 않았음을 확인하기 위해
특수기계(해쉬함수)를 활용한다.

- **입력 값과 출력 값 사이에는 아무런 연관성이나 규칙이 없다.**
- **입력 값을 몇 번 넣어도 같은 출력 값이 나온다.**
  (입력 값으로 출력 값을 쉽게 확인 가능)
- **출력 값을 가지고는 입력 값을 알 수 없다. (비가역성)**



<문제> A+B+C를 더해서 기계에 넣을 때 출력값 '000' 나오는 C는?
(A=거래기록, B=주어진 코드, C=봉인번호)

C를 알아내기 위해 10명의 사람들은 기계에 모든 숫자를 넣어본다.
→ 노가다 결과 '4a37b'라는 봉인번호 발견 → 공유 및 검증
→ 찾아낸 사람과 모두의 거래기록과 동일하다면 같은 출력 값이 나옴.
50%이상 봉인번호가 맞다고 동의하면,
번호를 찾아낸 사람이 받아쓴 종이는 **'진본'**으로 인정된다.

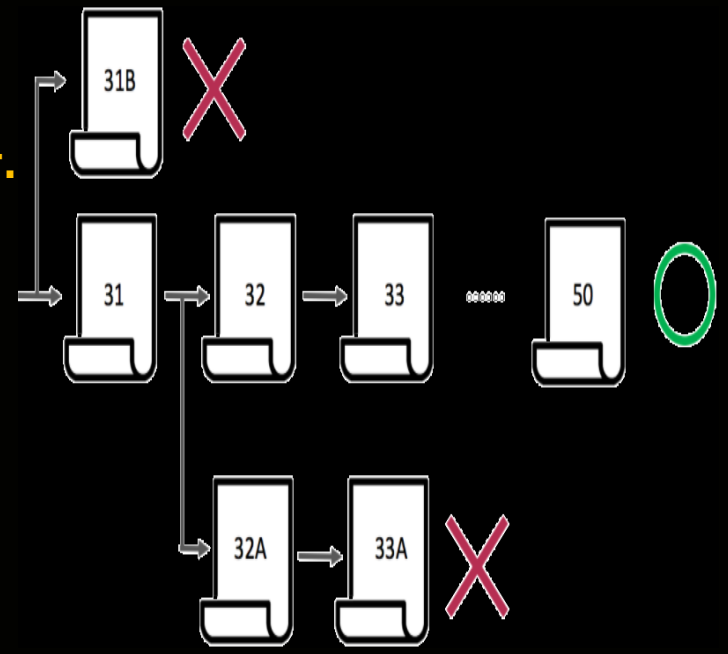
BTC참여과정 _3단계

③ 종이를 파일에 보관

이제 모든 사람은 봉인번호가 적힌 **'진본'종이를 복사하여 각자 파일에 보관한다.**

10명의 사람들은 다시 1번부터 작업을 **반복**한다.

반복결과 모든 사람이 같은 내용의 내용을 보관하게 되고, 진본임을 신뢰할 수 있다.



① 장부에 한 번 쓰여진 내용은 수정되거나 지워지지 않으며 영구적으로 저장된다.

② 어떤 사람이나 기관도 이 장부에 대한 권한을 가지고 있지 않다.

③ 모든 사람은 이 장부의 사본을 가지고 있으며 언제든 꺼내 볼 수 있다.

→ 거래내역이 담긴 종이 한 장을 '**블록**'이라고 하고,

→ 블록들이 엮여서 하나의 파일을 구성하기 때문에, 파일을 '**블록체인**'이라고 부른다.

BTC 참여보상(합의 알고리즘)

무임승차자 문제

그렇다면 왜 사람들은 그 시간과 돈을 써서 봉인하는 과정에 참여할까?

누군가 봉인해주기를 기다렸다가, 봉인된 종이만 전달받아 보관하면 되는 것이 아닐까?

⬇

참가자들이 종이를 봉인해야 할 유인이 없을 경우, 아무도 하지 않을 것이고, 신뢰도가 깨진다.

비트코인은 경제적 인센티브를 통해 무임승차자 문제를 해결한다.

① 일정량의 코인 지급

가장 먼저 봉인코드를 찾아낸

1명의 참가자는

일정량의 **코인**을 지급받는다.

② 거래 수수료 지급

모든 거래들에서

수수료를 조금씩 떼어 준다.

노력을 들여 작업(Work)을 한 사람에게 코인을 주는 시스템을 PoW(작업증명)라고 한다.

BTC 해결하고자 하는 문제와 해결책

문제	해결책
중앙집중화된 화폐	장부를 분산시키고 다수결로 검증
데이터 복사 및 위변조시 알 수가 없음 (이중지불문제)	해쉬함수를 사용하여, 블록을 봉인
무임승차자 문제	참가자에게 비트코인 및 수수료 보상
사후 위조의 문제	1, 블록은 앞의 블록과 연결되어 위조불가 2. 가장 긴 체인만 진본으로 인식
51% 공격	독립된 개인이 충분히 많으면 담합이 어려움

BTC특징 : 탈중앙화

★가장 중요한 특징

- 정부가 발행하는 화폐와 다르게 하나의 기관이 비트코인 네트워크를 지배하고 있지 않다.
- 전 세계 모든 개인, 기업, 그리고 채굴과 거래 확인에 개입하는 기계까지 포함한 모든 것들이 거대한 네트워크의 일부로 작동하도록 설계되었다.
- **네트워크의 일부가 작동이 안되는 경우에도 화폐는 계속해서 작동이 될 수 있도록 설계**되었다.
- 분산된 오픈 네트워크를 통해 '**이중결제문제**'가 해결된다.

기존 화폐와 달리 정부나 중앙은행, 금융기관의 개입없이 개인간(P2P)의 거래가 가능하다.

BTC특징 : 익명성

2단계

실제로 비트코인 사용자들은 지갑의 주소를 가지고 있고,
인터넷으로 거래를 하기 때문에 IP기록이 남아
사용자의 거래내역은 모두 공개된다.
따라서 **완전한 익명성을 보장하지 않는다.**

3단계

비트코인을 공식화폐로 환전하기 위해서는
각국의 암호화폐 거래소를 통해야 하며,
대부분의 암호화폐 거래소는 본인인증을 거치도록 되어 있다.
공식화폐로 환전할 때 그 주체가 누구인지 알 수 있다.
따라서 익명성은 사라진다.

1

2

3

1단계

블록체인 상의 거래는 제3자를 통한 신분인증이 필요 없는 P2P 거래다.
또한 거래 당사자의 신분 인증 대신 문자열로 이루어진 거래 주소를
통해 거래가 진행되기 때문에 **거래 당사자의 익명성이 증가한다.**

BTC특징 : 한정된 수량

정부가 원하면 더 찍어낼 수 있는 기존 화폐와는 달리 최대 발행량이 2,100만개로 한정되어 있다.

- **한정된 수량_비트코인 21,000,000개인 이유?**

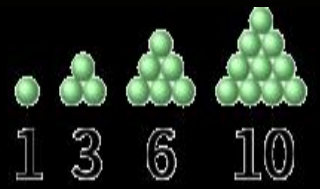
'21'은 삼각수로 계산하기가 간단하고 효율적으로 진행하기 좋은 값

→ **비트코인 4년을 주기로한 반감기 프로토콜** 결정

① 4년마다 생성되는 블록수 계산

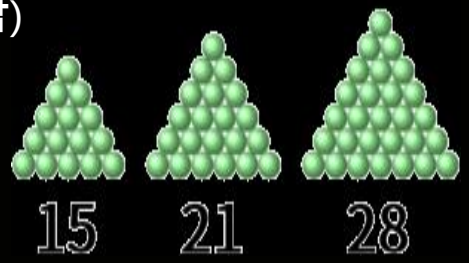
시간당 블록 생성수×하루 시간×연간 일수×년

= 6×24×365×4 = 210,240 ≒ 210,000



② 각각의 블록 당 보상합계(4년마다 반감)

50+25+12.5+6.25+3.125+1.5625+… ≒ 100



③ 대략적 발행 상한개수 (=①×②)

210,000×100 = **21,000,000개**

- **반감기_최근 채굴량(2020.12.19 기준)**

약 1850만개로 앞으로 250만개가 조금씩 채굴되어

2040년 쯤 99%, 2140년에는 100% 채굴되어 더 이상 공급이 없다.

BTC는 4년마다 반감기를 거쳐 채굴량이 줄어가는 구조

BTC특징 : 한정된 수량

한정된 수량과 반감기가 가지는 의미

① 화폐 인플레이션 위험 배제

결국 법정 화폐라는 것은
무한정으로 발급가능하기에
시간이 지나면 지날수록
그 값어치가 점차 줄어들고
인플레이션으로 인해서
하락할 수밖에 없다.

② BTC 공급감소로 수요증가 전망

수요와 공급의 원칙에 따라서
공급량이 너무 많아지면
비트코인의 가치를 낮출 수 있기에
수량을 한정하고,
4년마다 반감기를 통해
비트코인 채굴속도를 어렵고 느리게 만든다.

BTC특징 : 불변성 & 가분성

불변성

BTC는 우리가 쓰는 화폐와 다르게 거래를 되돌릴 수 없다.
거래가 네트워크에 기록되고 약간의 시간만 지나도
그 거래를 수정하는 것은 불가능하다.

비트코인의 모든 거래는 누구에게도 간섭될 수 없다.

가분성

비트코인 단위				
MBTC	KBTC	hBTC	deBTC	**BTC**
1,000,000	1,000	100	10	**1**
dBTC	cBTC	mBTC	uBTC	**satoshi(사토시)**
0.1	0.01	0.001	0.00000	**0.00000001**

2,100만개의 비트코인은 전 세계 통화로 사용되기는
턱없이 부족한 숫자지만, 1BTC가 소수점 아래 8자리,
즉 **BTC=0.00000001BTC까지 분할이 가능하다.**

앞으로 발행될 모든 비트코인의 총량이 2,100만개로 결과적으로는
21,000,000 * 100,000,000 = 2,100,000,000,000,000(2100조) 사토시가 유통될 수 있다.
(* 비트코인 3,000만원 → 사토시 3원)


Thank you