블록체인과 암호화폐 비트코인

NOTE 15

한국기술교육대학교 컴퓨터공학부 김상진

sangjin@koreatech.ac.kr
www.facebook.com/sangjin.kim.koreatech

교육목표

- 비트코인 이전 암호화폐
- 비트코인
  - 한기코인
  - 블록체인의 불가역성
  - 채굴
  - 하드포크 vs. 소프트포크
  - 비트코인 개선
  - 비트코인의 안전성
  - 비트코인의 문제점

- http://goo.gl/DFQFqT
- http://goo.gl/wEcFyq

암호화폐

- 명목 화폐와 동일한 특징을 가지는 암호화폐를 만들 수 있을까?
  - 명목 화폐의 중요 특징
    - 위조의 어려움
    - 휴대가능
    - 익명성 보장
    - 양도가능
    - 분할가능
    - 오프라인 지불방식
    - 범용 지불
  - 명목 화폐: 실질적 가치와 관계 없이 표시된 액면가로 통용되는 화폐

  - 오프라인 지불: 제3의 중재자의 참여 없이 지불할 수 있음
  - 온라인 지불: 지불에 제3의 중재자의 참여가 항상 필요함 (예: 신용카드)
- 암호화폐가 유통되기 위해서는 정부의 허가가 필요한 것은 아닌가?
  - 암호화폐도 중앙은행 또는 중앙은행이 허가한 기관만 발행할 수 있어야 ...
- 암호화폐는 디지털 값?
  - 지불: Alice가 가진 이 값을 상점에게???
  - 화폐는 유통되어야 의미가 있음
  - 가상화폐(제도권에서 인정되지 않은 화폐)가 목표가 아님

  - 원장에 교환 내역만 정확하게 기록되면 충분

Narayana R. Kocherlakota, Money is Memory, 1996

기존 암호화폐의 유통 시나리오

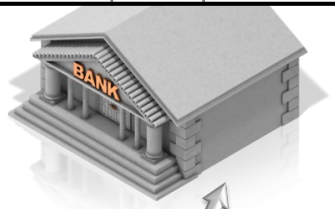
트랜잭션 번호	종류	일련번호	대상
111	인출	323	Alice
124	입금	323	한기마트

원장 유지

인출: 은행 ⟹ 고객

명목화폐 ⟹ 암호화폐

323



323

지불: 고객 → 상점

323

입금: 상점 ⟹ 고객

암호화폐 ⟹ 명목화폐

David Chaum, “Blind Signatures for Untraceable Payments,” Advances in Cryptology, CRYPTO ’82, pp. 199–203, 1983.

- 온라인 지불 방식

기존 암호화폐의 특성 및 문제점

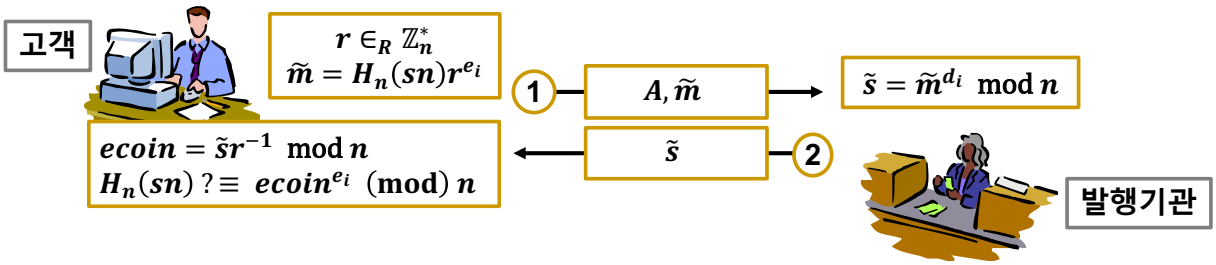
- 온라인 vs. 오프라인
  - 온라인: 지불 과정에 제3의 기관의 참여가 필요함
- 위조 문제: 전자서명 기술을 사용함. 발행기관 외에는 발급할 수 없음
- 이중 사용(double spending) 문제
  - 디지털화 때문에 생긴 문제
  - 온라인: 승인하기 전에 발행기관이 이중 사용 여부 확인 (일련번호 확인)
  - 오프라인
    - 오직 발급받은 사용자만 사용 가능
    - 차후 입금과정에서 이중 사용이 발견되면 발급자에게 책임
- 보통 거스름의 제공(발행기관만 전자화폐 발급 가능), 양도, 분할 등이 가능하지 않음 (명목화폐의 중요 특성을 만족 못함)
  - 고객과 상점을 명확하게 구분
- 비트코인 이전 암호화폐는 주로 연구 논문으로 발표되었고, 현실 세계에서 유통되지는 못하였음 (why?)

은닉서명을 이용한 온라인 전자화폐 (1/2)

- 은행: 액면가마다 서로 다른 RSA 공개키 쌍을 사용

공개키	3	5	7
액면가	50원	100원	500원

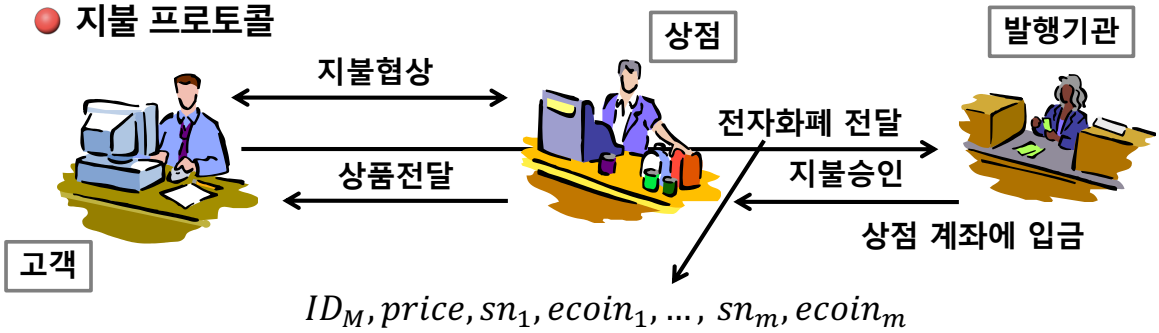
- 인출 프로토콜



- 거스름이 제공되지 않으므로 정확한 금액을 맞추어 지불해야 함
- 충분한 금액이 있어도 지불하지 못할 수 있음

은닉서명을 이용한 온라인 전자화폐 (2/2)

- 지불 프로토콜



$ID_M, price, sn_1, ecoin_1, \ldots, sn_m, ecoin_m$

- 은닉서명을 통해 위조불가능성 제공
- 은닉서명을 통해 고객의 무조건적 익명성 보장 가능
  - 전자상거래 측면에 지불 과정만 익명성이 보장된다고 익명성이 보장되는 것은 아님
  - 상점의 익명성은 보장하지 않음
- 암호화폐는 안전한 채널을 통해 전달되어야 함
  - 도청을 통해 다른 사용자가 사용할 수 없도록 하기 위함
- 은행은 일련번호를 확인하여 이중사용을 방지해야 함

비트코인

- 자체 강화 방식 (탈중앙 방식)
  - 전자화폐를 발행하는 중앙집중 신뢰 기관을 사용하지 않음
- 오프라인 방식?
  - 지불 과정에서 특정 서버의 도움을 받지 않음
  - 하지만 지불 내용을 전체 비트코인 네트워크에 전달하여야 하며, 확정되기까지 일정 시간이 필요함

- 항상 지불이 가능
- 하지만 이해 당사자만 참여하는 방식이 아님

- 양도 가능
  - 고객과 상점 간 뿐만 아니라 고객 간에도 화폐를 양도할 수 있음

- 고객, 상점을 구분하지 않음

- 분할 및 통합 가능
  - 하나의 화폐를 여러 화폐로 나눌 수 있으며, 여러 화폐를 하나로 통합할 수 있음 (이 자체도 또 다른 거래, 문제는?)
- 익명 지불 가능
- 첨삭만 가능한 분산 원장(append-only transaction-based distributed ledger) 사용: 공개 분산 원장 (블록체인)

한기코인

- 비트코인을 이해하기 위한 가상의 암호화폐
- 한기코인의 규칙
  - 규칙 1. 총장(S)만 코인을 만들 수 있음
  - 규칙 2. 코인의 소유자는 다른 사람에게 코인을 양도할 수 있음
  - 규칙 3. 모든 거래는 전체 공개됨 (첨삭만 가능한 원장에 공개한다고 가정)
- 모든 참여자는 공개키 쌍을 가지고 있음
  - 거래를 진행하기 위해서는 상대방의 공개키를 확보해야 함
  - 익명성 때문에 인증서를 사용하지 않음 (프라이버시 보장???)
  - 총장은 인증서를 사용한다고 가정함
- 화폐를 나타내는 별도 디지털 정보가 있는 것은 아님
  - 거래를 원장에 기록하며, 이 기록이 화폐 역할을 함
- 한기코인에서 거래는 헤더, 입력, 출력, 서명으로 구성됨
  - 입력과 출력 모두 여러 개일 수 있음
  - 입력의 소유자는 모두 같은 사람이라고 가정함 (꼭 필요한 것은 아님)

제3자에게 그리고
지불자의 프라이버시만

한기코인

- 한기코인 거래의 확인
  - 입력 금액의 합이 출력 금액의 합과 같아야 함
    - 생성 거래는 입력이 0임 (이 조건을 충족하지 않음)
  - 입력은 이전에 사용하지 않은 다른 거래의 출력이어야 함
  - 입력 소유자(출력 수취인)의 유효한 서명이 있어야 함

- UTXO(Unspent Transaction Output) 기반

T1	H(header||in||out)
header	type: 생성, #in: 1, #out: 1, size: , …
in	이전 거래: null
out	금액: 100원, 수취인: $H(+K_S)$
서명	$Sig.-K_S(T1)$

여기서 S는 총장

- 코인 생성 거래는 총장의 서명이 필요함
- 이 때문에 총장만 코인을 발행할 수 있음
- 발행의 수취인이 꼭 총장일 필요는 없음

한기코인

T2	H(header||in||out)
header	type: 지불, #in: 1, #out: 1, size: , …
in	이전 거래: T1:0
out	금액: 100원, 수취인: $H(+K_A)$
서명	Sig.-K_S(T2)

T3	H(header||in||out)
header	type: 지불, #in: 1, #out: 1, size: , …
in	이전 거래: T2:0
out	금액: 100원, 수취인: $H(+K_B)$
서명	Sig.-K_A(T3)

T4	H(header||in||out)
header	type: 지불, #in: 1, #out: 1, size: , …
in	이전 거래: T2:0
out	금액: 100원, 수취인: $H(+K_C)$
서명	Sig.-K_A(T4)

- 100원의 소유가 A로 이전
- 수정 불가?
  - 공개
- T2:0 ⟹ 거래2, 0번째 out
- 어디까지 되돌아가면서 확인해야 할까?
  - 이전 거래 T2만?
- 이중사용 방지?
  - 공개
  - 검색 필요
    거래 중 in이 T2인 트랜잭션만

한기코인

트랜잭션 번호	IN			OUT			
	NO.	NO.	지불자	금액	수취인	금액	수취인
T1				400	S		
T2				500	S		
T3	T1:0		S	300	A	100	S
T4	T2:0		S	200	B	300	S
T5	T4:0		B	150	A	50	B
T6	T3:0	T5:0	A	400	C	50	A
T7	T3:1	T4:1	S	400	S		
T8	T6:1		A	100	B		invalid
T9	T4:0		B	200	A		double

- 총 생성한 금액은?
- S의 재산은?
- A의 재산은?
- B의 재산은?
- C의 재산은?

- 이 거래 원장은 수정할 수 없어야 함
- 유효하지 않은 거래는 원장에 포함될 수 없어야 함

한기코인

- 발행 문제
  - 총장만 가능, 서명하여 발행하기 때문에 다른 참여자는 발행할 수 없음
- 거래 내용 변경 문제, 이중 사용 문제
  - 원장에 공개된 내용을 변경(수정, 삭제)할 수 없어야 함
  - 유효하지 않은 코인은 원장에 기록할 수 없어야 함
  - 어떻게 보장?
    - 중앙집중식: 총장이 유효성 검증 후 서명하여 공개?
    - 비트코인은 이것을 탈중앙 방식으로 제공함

비트코인

- Satoshi Nakamoto라는 익명으로 2008년에 처음 소개됨
- 1 BTC 거래가격

2017. 5. 31	2018. 5. 21	2019. 5. 7	2020. 5. 11	2021. 5. 14
$2,451	$8,505	$5,732	$8,760	$50,438
₩3,129,000	₩9,384,000	₩6,654,000	₩10,678,000	₩61,906,000

2022. 5. 6	2023. 5. 19			
$36,398	$26,841			
₩47,101,000	₩36,240,000			

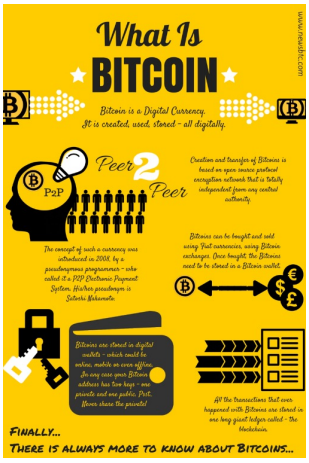
  - http://www.coindesk.com/price/, bitthumb
- 지금까지 발행된 비트코인 수: http://www.blockchain.com/

2017. 5. 31	2018. 5. 21	2019. 5. 7	2020. 5. 11	2021. 5. 14
16,364,938	17,043,350	17,685.450	18,373,525	18,709,887.5

2022. 5. 6	2023. 5. 19			
19,031,962.5	19,377,375			

비트코인의 일반 참여자

- 일반 참여자는 비트코인 지갑을 만들어야 하며, 이 지갑을 만들기 위해서는 공개키 쌍이 필요함
  - 인증서 기반은 아님. (왜? 익명성을 위해)
  - 공개키는 지갑의 주소 역할을 함
    - 누군지 모르더라도 이 주소가 소유주로 되어 있는 코인은 대응되는 개인키 없이는 지불에 사용할 수 없음
  - 한 참여자는 여러 개 쌍(지갑)을 사용할 수 있음
  - 문제점. 개인키를 분실하게 되면 가지고 있던 해당 키와 연결된 모든 코인을 사용할 수 없음
    - 더 이상 코인 역할을 할 수 없음
- 비트코인 지갑은 비트코인 소프트웨어와 달리 다양한 업체가 다양한 형태로 제공하고 있음
  - 안전성???



- 개인키의 안전한 유지가 가장 중요한 요소
- hot (internet 연결) vs. cold

비트코인 네트워크와 참여 노드 종류

- 비트코인 네트워크: P2P 네트워크 (모든 노드가 동등 역할을 해야 함)
- 종류
  - 완전 노드(full node)
    - 최초 블록부터 지금까지 모든 블록에 포함된 정보를 유지해야 함
    - 채굴자는 완전 노드를 운영해야 함
    - bitcoin.org, bitcoincore.org에서 코어 클라이언트 소프트웨어 설치 (최신 버전: 23.1, 발표 날짜: 2022. 12. 21)
      - 약 10일 이상 소요 (모든 데이터(481GB)를 다운받는 데 걸리는 시간)
    - 완전 노드 운영 동기: 비트코인 건전성에 기여, 투표권 획득 등
  - 부분 노드(lightweight node, partial node)
    - 본인의 거래를 위해 필요한 최소한의 정보만 유지함
    - 블록 헤더들만 유지

비트코인에서 통신 방식

- 각 사용자는 자신이 생성한 트랜잭션을 전체 네트워크에 전달해야 함
- P2P 네트워크에서 한 메시지를 전체 네트워크에 전달하는 방법
  - 애드혹 네트워크에서는 이와 같은 통신 방법을 flooding이라 함
    - 한 노드가 메시지를 전송하면 그것을 수신한 모든 노드는 다시 전송함
      - 이미 전송한 메시지는 다시 중계하지 않음 (중복 검사)
  - Gossip 프로토콜
    - 단계 1. 한 노드는 주기적으로 일정한 횟수만큼 랜덤한 수(>=2)의 수신자를 선택하여 메시지를 전송함
    - 단계 2. 메시지를 수신한 사용자도 단계 1의 과정을 수행함
    - 단계 1에서 수신자를 1명만 선택하여도 $O(\log n)$ 주기가 지나면 n명에게 도달할 수 있음

비트코인 트랜잭션

- push (명목화폐) vs. pull (신용카드)
- 코인 소유자만 지불 가능
- 직접 지불자에서 수취인으로 가치가 이동함

- 입력
  - 입력의 합은 출력 합보다 같거나 커야 함
  - 각 입력마다 전자서명 필요
    - 같은 지갑의 UTXO를 사용하더라도 별도 서명 필요
- 출력
  - 출력의 대상이 지불자와 같게 하여 거스름을 구현함
  - 입력과 출력의 차액은 수수료가 됨
    - 수수료는 지불자가 결정. 수수료가 높을수록 거래가 확정되는 속도가 빠를 수 있음
    - 채굴자의 몫이므로 수수료가 높은 트랜잭션을 블록에 포함하는 것이 채굴자에게 유리함
- 다중 입력, 다중 출력 가능
  - 보통 출력은 수수료를 포함하기 때문에 기본적으로 다중

탈중앙 암호화폐, Really??? (1/2)

- Satoshi Nakomoto는 천재
- 디지털 세상에서 Alice가 만원을 가지고 있고, 이 중 오천원을 Bob에게 지불하고 싶다. 어떻게?
  - 오천원의 가치를 나타내는 비트 데이터를 Alice의 장치에서 Bob의 장치로 옮긴다. 이것이 기존 전자화폐의 생각 (ㅋㅋㅋ)
  - 실제 디지털 세상에서는 물질적인 무엇인가가 옮겨질 필요가 없음
- 유효한 거래 기록을 유지하고, 이 기록을 변경(수정 및 삭제)할 수 없어야 하며, 누구나 확인할 수 있도록 공개하면 안전한 거래가 가능
  - 비트코인은 자신이 가지고 있는 일정 금액을 누구에게 지급하고 싶다는 의사를 나타내는 전자서명된 트랜잭션을 생성하여 공개함
  - 공개를 위해 비트코인에 있는 모든 노드에 트랜잭션을 전달함
  - 각 노드는 수신된 거래의 기본적 유효성(예: 서명 값)을 확인해야 하며, 유효하지 않은 것은 중계하지 않음
  - 이를 통해 각 노드는 발생한 모든 거래 정보를 축적함
    - 완전 노드만 이 역할을 함

탈중앙 암호화폐, Really??? (2/2)

- 전자서명된 트랜잭션을 공개하는 방식에서 다음 문제를 해결하면 탈중앙 암호화폐가 가능함
  - 화폐 발행 문제.
    - 탈중앙 기법으로 화폐를 발행할 수 있어야 하며, 규칙에 어긋나게 임의로 발행할 수 없어야 함
  - 거래 위조 문제. (cf. 화폐 위조)
    - 자신이 가지고 있는 금액만큼만 지불할 수 있어야 함
    - Alice가 소유한 암호화폐는 Alice만 사용할 수 있어야 함
      - 전자서명 기술을 이용하여 해결함
    - 유효한 거래만 기록되어야 함
  - 이중 사용 문제. 한번 기록된 거래는 변경할 수 없어야 함
    - 이전 기록에 대한 수정, 삭제 등이 가능하지 않아야 함
      - 원장의 불가역성(immutability)이 보장되어야 함. 동시에 누구나 열람하고 확인할 수 있어야 함
- 블록체인이라는 기술(+전자서명 기술)을 이용하여 이 문제들을 모두 해결함???

용어 정리

- 분산 원장(DL, Distributed Ledger)
  - 불가역성 제공
  - 모든 탈중앙 노드가 같은 데이터를 중복 유지함
    - 노드 간의 신뢰를 가정하지 않음
- 분산 원장의 종류
  - 블록체인
    - 블록 단위로 데이터 기록
  - DAG(Directed Acyclic Graph)
    - 개별 트랜잭션 단위로 기록
    - 예) Nano, IOTA
- 분산 합의 기술
  - 기록된 데이터의 불가역성, 일관성을 제공하기 위해 사용하는 기술
  - 규칙, 규칙 준수를 위한 보상 체계(incentive), 규칙을 준수하지 않을 경우 불이익 체계(disincentive)를 포함

불가역성의 보장 (1/7)

B

T1	Sig.A(T1)
T2	Sig.B(T2)
T3	Sig.D(T3)
T4	Sig.A(T4)
T5	Sig.C(T5)

- 트랜잭션은 전자서명되어 전체 네트워크로 전파됨
- 이 트랜잭션들을 모아 블록을 구성하고 블록을 확정함
  - 블록에 포함된 트랜잭션은 수정 및 삭제할 수 없어야 함
  - 기본적으로 수정은 전자서명 때문에 지불자만 가능함
  - 따라서 다음 2가지가 보장되어야 함
    - 블록에 포함된 트랜잭션을 삭제할 수 없어야 함
    - 유효 트랜잭션들은 블록에 시기적절하게 포함되어야 함
- 중앙집중 방식이 아니라 탈중앙 방식으로 불가역성을 제공하고 싶음
- 하지만 우선 무결성 보장 기법부터 검토해 보자
  - 해시함수, MAC, 전자서명 →

H(B)
MAC.K(B)
Sig.S(B)

  - 누구든지 무결성을 안전하게 확인하기 위해서는 위 3가지 기술 중 전자서명이 유일한 대안
  - 탈중앙 방식으로 전자서명을 활용하여 무결성을 제공할 수 있나?

불가역성의 보장 (2/7)

- 해시함수
  - 문제점. 누구나 M을 M'으로 바꾸고 $H(M')$을 계산할 수 있음
- MAC
  - MAC은 키가 있는 사람만 생성할 수 있음
  - 이 사람은 일반 해시함수와 마찬가지로 수정할 수 있음
  - 이 키가 없으면 확인할 수 없음
- 전자서명
  - 해시함수와 달리 서명키를 가지고 있는 사용자만 해당 사용자의 서명을 생성할 수 있음
  - 누구나 확인키를 가지고 있으면 서명의 유효성을 확인할 수 있음
  - 문제점
    - 해시함수보다 계산 비용이 상대적으로 높음
    - 서명자의 권한이 막강함
      - 서명자는 데이터 삭제할 수 있고, 데이터 포함을 거부할 수 있음

- 탈중앙이 목적이므로 특정 사용자만 서명하는 방식은 가능하지 않음

불가역성의 보장 (3/7)

- 비트코인에서는 어떻게?
  - 각 거래는 전자서명하여 기록
    - 타인의 거래 기록은 지불자의 서명키를 확보하지 않는 이상 수정할 수 없음
  - 일정 기간에 발생한 모든 기록을 블록이라는 문서로 통합하고, 이 블록에 대한 해시값을 계산함
    - 블록의 크기는 1MB로 제한. Why? 전파의 용이성
      - 문제점. 트랜잭션의 크기는 가변적이지만 대략 0.3KB이기 때문에 최대 약 3,000개 정도만 한 블록에 기록 가능
        - 거래 처리 용량이 제한적임
- 그러면 여전히 수정 가능한 것은 아닌가?

불가역성의 보장 (4/7)

- 그러면 여전히 수정 가능한 것은 아닌가?
  - 단순히 블록 B에 대한 해시값 $H(B)$를 계산하는 것이 아님
  - 특정한 형태의 해시값을 계산하여야 유효한 해시값으로 인정
    - 이 때문에 암호퍼즐이라 함
    - $H(B||N_1), \ldots, H(B||N_k)$처럼 블록 값 외에 랜덤값 N_i을 바꾸어 가면서 원하는 형태의 해시값이 나올 때까지 반복
    - 이 반복에 필요한 시간을 조절할 수 있음
      - 현재 비트코인에서는 10분이 되도록 난이도를 조정함
      - 왜 10분? 우연한 포크 발생 확률을 줄이기 위함
    - 난이도 조정. 2,016개 블록마다 (약 2주마다)

00000000000000000000571070473e2d29e7512e7733156707d0c8a06c27e79ff

- 19개
- 실제 77개

- Height: 776,998 *2023-02-17
- https://blockchain.info/ko

Python 예)

Python3, pycryptodome

```
from Crypto.Hash import SHA256
block = 'Sangjin is Handsome'
for x in range(0, 2**16-1):
    data = (block+str(x)).encode('utf-8')
    hval = SHA256.new(data).hexdigest()
    print(str(x)+': '+hval)
    if hval.startswith('0000'):
        print('====FOUND====')
        break
```

block = 'Satoshi Nakamoto is a genius'

앞 4개만 0, 실제 18개, 2^{72}개 해시 계산 필요

```
131065:3b533df42019d051d938f4d7551b263bb07c563bd445421ad9cdda56d3bab19f
131066:9edd464a3586bfaf1b33a39d89970516d9de40eb3be210f8efa56ffe742a3d1a
131067:e3516433b4841a2f62d36c98141997d063a659ae65e2a88575741d5290cda567
131068:de0fbe90ba20211bce2e7bf80d8cd3fe299455ef760c6a45fe5ae3ea7298b464
131069:1f961174e2ff07a0c4bf471fcd8a8381118870abd3b1b572e12108b714227320
131070:b2e79e2be72494b64ead2ec0c866fdd19f72f8b2dfd61664a12038cc57decdf2
```

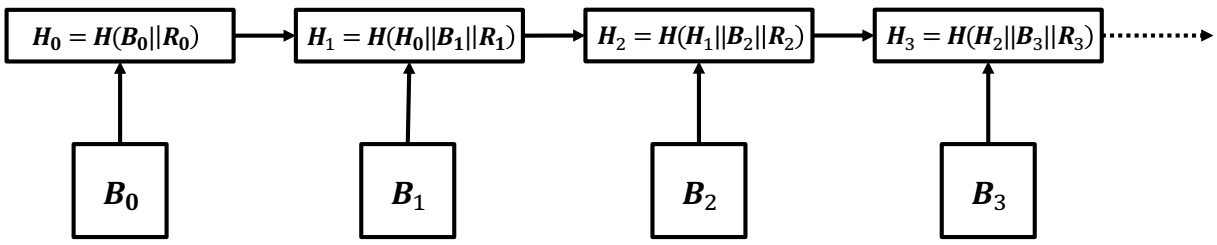
```
125379:38d13fe90300ba2271858f52dc8b4c1ac622917984ccad2780418fdde1dc7195
125380:03873f5cd41aca0fba1b579302ba90fc932f0534d1bcdcd5e094b86207778ebe
125381:7c34596886a1142d226708d37f62462d39c19e9d13e55a0db9eeb621a67ed904
125382:7312fbb7ada08e6f0cf11b764938697946795f59d6e83a5093b761541b30e56e
125383:c738b51d9b6d16ac695bf3f6a61c95f0ef5ddce434039d1940c02474b595ef25
125384:7ebe45cd010decead7c3004a8d5781850f442c59194d883820554900cb3006f4
125385:505930581667eb8b9d7be3effe84e111ec675a9d839d09683c962e882ddf9085
125386:00001e62f42c974a26a57e689ee92b95c76a6a47b12727761f82c74136cb5e49
```

불가역성의 보장 (5/7)

- 암호 퍼즐을 해결하면 비트코인을 얻을 수 있음.
  이 때문에 이를 채굴(mining)이라 함
  - 블록에 코인베이스(coin-base) 트랜잭션을 포함
    - 입력 없이 정해진 금액을 채굴자(본인)에게 지급하는 형태의 트랜잭션
- 10분 정도의 노력을 하면 계산할 수 있다!!!
  - 이 때문에 이를 작업 증명(proof-of-work)이라 함
  - 누구나 10분 정도에 퍼즐을 해결할 수 있는 수준의 비트코인 채굴기를 사면 본인의 기록을 수정하고, 타인의 기록을 삭제하는 등 블록을 수정할 수 있음
    - 그러면 불가역성은 어떻게?

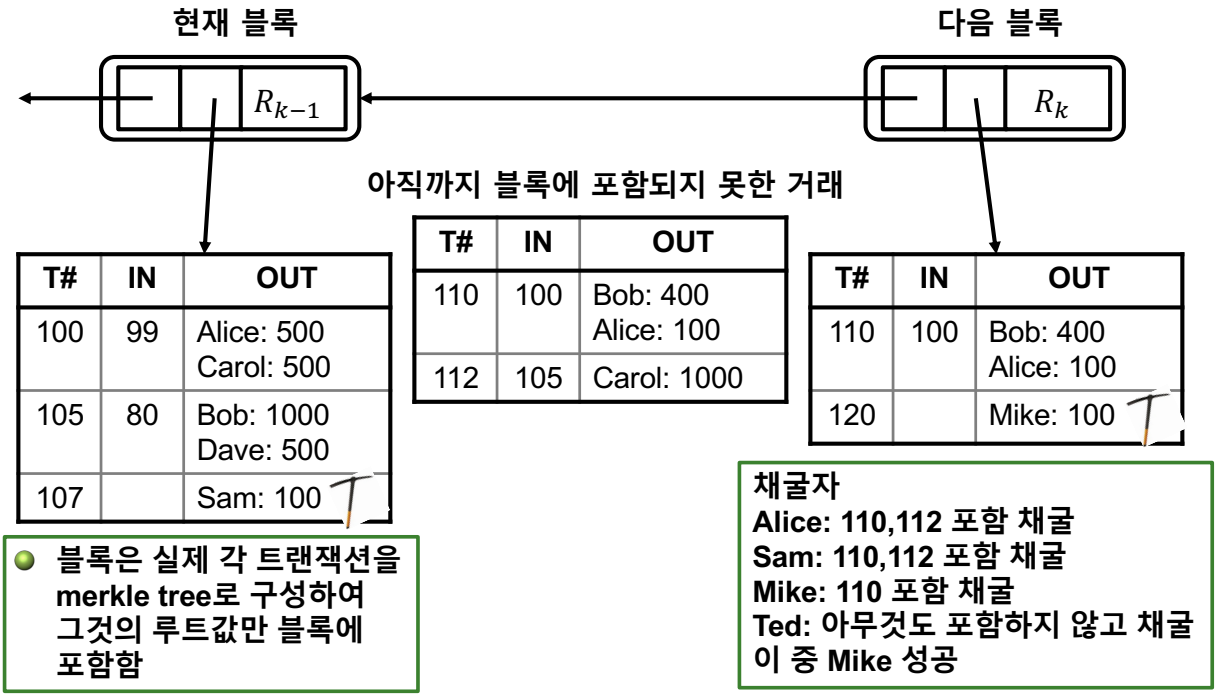
불가역성의 보장 (6/7)

- 불가역성을 제공하기 위해 블록들을 연결함
  - 블록에 대한 해시값을 계산할 때 이전 블록의 해시값을 포함
    - $H_0 = H(B_0||R_0), H_1 = H(H_0||B_1||R_1), \ldots, H_k = H(H_{k-1}||B_k||R_k), \ldots$
    - 이 체인은 중단없이 계속 생성되는 성질을 가지고 있음
    - 중간 체인 값이 바뀌면 그 이후 모든 값이 무효가 됨
    - 한 블록만 바꾼다고 수정이 가능한 것이 아님



- 블록을 연결하는 해시 퍼즐만 사용하면 모든 문제가 해결???
  - 포크 문제 ⟹ 즉시 확정이 가능하지 않음
  - 끊임없이 생성되어야 함 ⟹ 보상 체계

블록체인과 채굴 예시



T#	IN	OUT
100	99	Alice: 500 Carol: 500
105	80	Bob: 1000 Dave: 500
107		Sam: 100

T#	IN	OUT
110	100	Bob: 400 Alice: 100
112	105	Carol: 1000

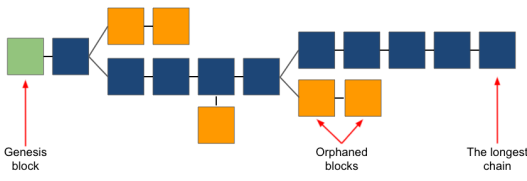
T#	IN	OUT
110	100	Bob: 400 Alice: 100
120		Mike: 100

- 블록은 실제 각 트랜잭션을 merkle tree로 구성하여 그것의 루트값만 블록에 포함함

채굴자
Alice: 110,112 포함 채굴
Sam: 110,112 포함 채굴
Mike: 110 포함 채굴
Ted: 아무것도 포함하지 않고 채굴
이 중 Mike 성공

불가역성의 보장 (7/7)

- 비트코인 암호 퍼즐의 해결은 장비 싸움이지만 확률적인 프로세스이기 때문에 우연히 두 사람이 동시에 해결할 수 있음 (일시적 포크 발생)
  - 이 문제를 해결하기 위해 비트코인에서 가장 긴 체인을 우선하는 원칙이 있음
    - 이처럼 암호화폐는 규칙을 통해 문제를 해결하는 경우가 많음
    - 유효 체인에 자신이 생성된 블록이 들어가야 보상을 받을 수 있음
  - 일정 깊이가 되어야 확정됨
  - 여기서 잠깐.
    - 블록 높이: 최초 블록이 0, 그 이후부터 차례로 할당
    - 블록 깊이: 가장 최근 블록이 1이고 최근순으로 할당
      - 블록 깊이가 6보다 커지면 취소될 확률은 거의 없어짐
- 장비 싸움이기 때문에 한 주체가 전세계의 채굴에 사용되는 해시 파워의 51%을 차지하면 이 주체는 마음대로(???) 블록체인을 조작할 수 있게됨
  - 하지만 아직까지 이와 같은 문제는 발생하지 않음
  - 이 때문에 현 생태계가 건전하다고 함



블록 높이0비트코인 블록체인 내 깊이 값 0에서의 블록들

요약	
높이	0 (Main chain)
해시	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
이전 차단	0000000000000000000000000000000000000000000000000000000000000000
다음 블록	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
시각	2009-01-03 18:15:05
난이도	1
Bits	486604799
거래 수	1
출력 합계	50 BTC
예상된 거래량	0 BTC
크기	0.285 KB
번역	1
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
해시 난수	2083236893
블록 보상	50 BTC
거래 수수료	0 BTC

- 10개
- 제네시스 블록(genesis block): 사토시 생성

해시시	00000000000000000000ccd659f64e60dd470712d666e892197e22a2a2f696537
확인	8
타임 스탬프	2020-02-06 08:52
신장	616160
갱부	BTC.com
거래 횟수	3,617
어려움	15,466,098,935,554.65
머클 루트	927493767c0c24ab61e30b6fdb306dfbbf67e2d525f3d84ce828b500c88a8839
번역	0×20000000
비트	387,068,671
무게	3,993,441 WU
크기	1,408,110 bytes
목하	1,530,310,505
거래량	2308.96697109 BTC
블록 보상	12.50000000 BTC
수수료 보상	0.08664401 BTC

- 19개
- 목표값 bits = 387,068,671
- 16진법으로 변환 = 171232FF
- 17 | 1232FF
- 1232FF * 2^(0x08 * (0x17-0x03)) =1.74314E+54
- hex
- 0000 0000 0000 0000
- 0012 32ff 0000 0000
- 0000 0000 0000 0000
- 0000 0000 0000 0000

트랜잭션 비트코인 거래에 대한 세부정보 보기

338700ac76836461a636e5743b616bd369828f64aa03364fa4e8de0a745ed562

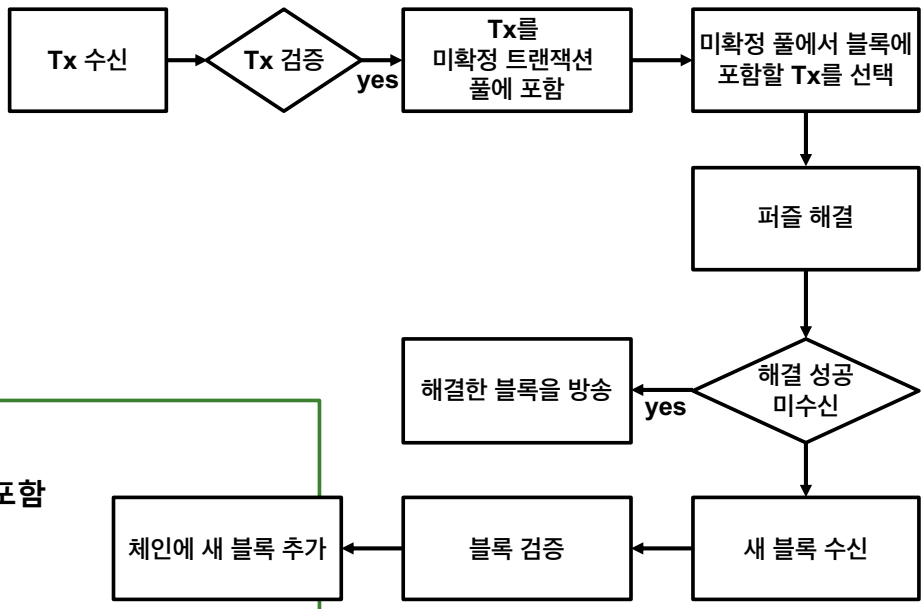
17A16QmavnUfCW11DAApiJxp7ARnxN5pGX	→	1bds64Ra2sXrLTG7iEgRptHGhcvTqTdmy 0.07788673 BTC 1G7ntfikkX8o4oMhk8sSUbFJUMjYwSg9bg 0.50185238 BTC 17A16QmavnUfCW11DAApiJxp7ARnxN5pGX 45.22520869 BTC

2 승인 | 45.8049478 BTC

요약	
크기	291 (bytes)
무게	1164
수신 시간	2018-12-19 02:03:39
블록에 포함됨	554420 (2018-12-19 02:04:06 + 0 의사록)
승인	2
시각화	트리 차트 보기

입력 및 출력	
총 거래량	45.8059478 BTC
총 출력	45.8049478 BTC
거래 수수료	0.001 BTC
1 바이트 당 수수료	343.643 sat/B
무게 단위당 요금	85.911 sat/WU
예상 BTC거래량	0.07788673 BTC
스크립트	스크립트 보기 & coinbase

채굴자의 역할과 프로세스



- 트랜잭션 수신
  - 트랜잭션 확인
  - 유효하면 풀에 포함
- 블록 수신
  - 블록 확인
  - 새 블록 시작
- 블록 생성 경쟁
  - 풀에서 블록에 포함될 트랜잭션 선택
  - 암호 퍼즐 해결
  - 블록 수신 전 해결하면 블록 전파

- 블록 확인의 중요성: 유효한 트랜잭션들로 구성되어 있는 블록만 인정함

채굴(mining)

- 누가 해시값을 계산하나?
  - 비트코인: 아무나, Why? 보상이 있음
    - 성공적으로 계산한 사람은 새 비트코인과 블록에 포함된 각 트랜잭션의 수수료를 얻게 됨
      - 비트코인의 발급 방법
    - 이들을 그래서 채굴자라 함
  - 누구도 전 세계 채굴자들의 능력 총합의 50% 이상을 독차지할 수 없어야 함
    - 생태계의 건전성이 중요함
    - 참고. 채굴 비용: 하드웨어 구축 비용 + 전기세 + 시간 + 시설운영비 + 인건비 + 기타
      - 성공확률은 투자 비용에 좌우됨
      - 냉각비용이 중요
  - Satoshi가 만든 생태계가 아니라 스스로 만들어진 생태계임
    - 처음부터 이렇게 될 것이라 확신했을까?

채굴 보상(incentive, reward) (1/2)

- 채굴 보상은 보상으로 신규 발행되는 비트코인과 해당 블록에 포함된 트랜잭션 수수료임
- 현재 비트코인에서 채굴에 성공하면 6.25 BTC를 보상으로 받음
  - 2023년 5월 시세(약 3,500만원)와 보상 액 6.25 BTC를 고려하면 블록마다 약 이억천팔백칠십오만원 정도의 채굴 수입이 발생함
- 채굴자는 자신이 구성한 블록의 첫 번째 트랜잭션으로 보상과 수수료 합을 자신에게 지불하는 트랜잭션을 포함함(coinbase transaction)
- 블록마다 신규 발행되는 비트코인은 일정 주기(약 4년)마다 절반으로 감소함
  - 가장 최근에 감소한 시점은 2020년 5월 12일임 (다음은 2024년 4월 27일)
- 총 발행될 비트코인 수는 21,000,000개이며, 이 중 92.3% 이상 이미 발행됨
  - 2032년이 되면 99%가 발행될 예정이며, 2140년이면 발행이 중단될 것으로 예측됨
  - 2032년 이후에는 블록마다 발생하는 것이 1 BTC 이하임

https://www.bitcoinblockhalf.com/

채굴 보상 (2/2)

- 트랜잭션 수수료는 트랜잭션 크기에 비례하며, 적정 금액은 시세에 따라 계속 변하고 있음
  - 현재는 1 바이트에 102 satoshi 정도임
    - 블록 크기가 1MB이므로 이 계산에 의하면 최대 1.02 BTC)
  - 자신의 트랜잭션이 빨리 포함되도록 수수료를 많이 지급할 수 있음
  - 평균이 0.51 BTC라 하면 현재 시세를 고려하면 2,500만원 정도
    - 채굴을 통한 신규 코인에 의한 보상과 비교하면 상대적으로 적은 금액

2021.5.14	2022. 2. 17
per transaction 26,000 satoshi	per transaction 22,848 satoshi

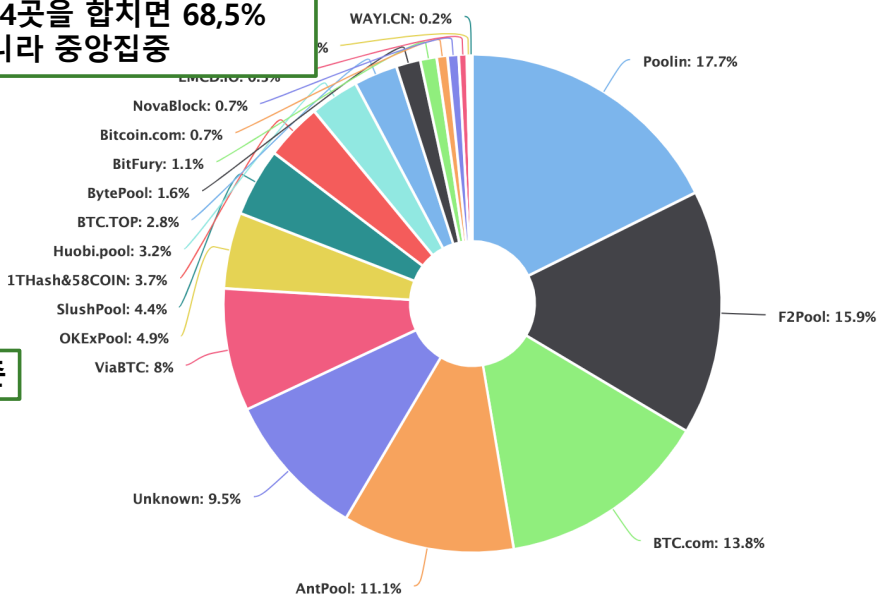
- 1satoshi = 0.00000001 BTC = 0.3원
- 22,848 satoshi = 약 7,000원

https://bitcoinfees.earn.com/

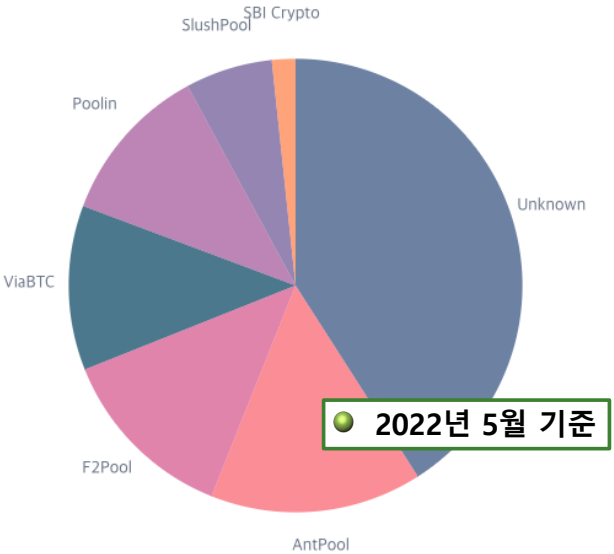
51% 공격

- 한 주체(개인 또는 집단)가 전세계의 채굴에 사용되는 해시 파워의 51%을 차지하여 해당 블록 체인 생태계를 교란하는 공격
- 실제 할 수 있는 일
  - 이중 사용
    - 예) 이전 트랜잭션을 블록에서 제거하고 해당 트랜잭션의 사용된 코인으로 새 트랜잭션을 구성하여 체인에 새롭게 추가
    - 참고. 자신의 비트코인만 이중 사용 가능. 물론 공모는 언제든지
  - 서비스 교란
    - 기존 유효한 트랜잭션을 무효화하는 것이 가능
    - 트랜잭션 거부
      - 시스템 가치 하락 ⟹ 공격한 주체에게 이득이 없음
        ⟹ 오히려 지금은 채굴을 통해 보상을 얻는 것이 훨씬 유리함
- 현재 해시율 분포: 애초 목표와 달리 중앙 집중화??
  - https://www.blockchain.com/ko/pools

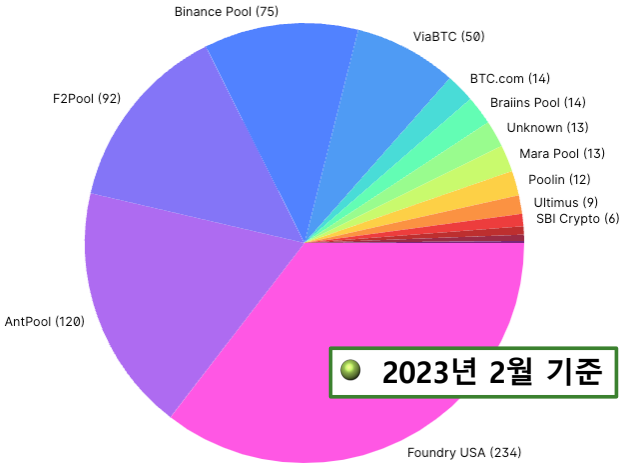
- 이미 채굴 보상이 투자 대비 작다고 할 수 있음.
  하지만 중단하면 오히려 더 손해 (가치하락 때문)
  - 이미 큰손들은 떠날 준비(보유한 코인 환매)를 하고 있다고 보는 시각도 많음
- 상위 3곳을 합치면 57.4%, 4곳을 합치면 68,5%
  - 이미 채굴은 분산이 아니라 중앙집중



- 2020년 5월 기준



- 2022년 5월 기준



- 2023년 2월 기준

51% 공격 사례

- Bitcoin Gold Hit by Double Spend Attack, Exchanges Lose Millions, https://www.ccn.com/bitcoin-gold-hit-by-double-spend-attack-exchanges-lose-millions/
  - 51% 능력을 갖춘 채굴자가 특정 코인을 지불에 사용한 후 체인의 내용을 무효화하여 해당 코인을 지불에 다시 사용함
- Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack, https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack/
  - 채굴자가 암호 퍼즐을 해결하였지만 공개하지 않고 계속 채굴한 다음 이것을 일시에 공개하여 기존 블록들을 무효화시키는 공격 (BWA, Block Withstanding Attack)
  - 이기적인 채굴(selfish mining)
- 위 두 사례에서 알 수 있듯이 암호화폐가 PoW 방식을 사용하고 있지만, 전체 채굴자의 해시 파워가 크지 않으면 51% 이상을 확보하여 공격에 성공하는 것이 가능하다는 것을 보여주고 있음

작업 증명(PoW, Proof-of-Work)

- 비트코인에서 사용하는 분산 합의 기술
  - 채굴자가 수행
- 작업 증명의 문제
  - 전기 소비로 인한 환경 파괴
    - 다른 효과적인 방법이 필요
  - 일반 응용에서는 이와 같은 자발적 생태계를 구축하기 힘들 수 있음
- 지분 증명(PoS, Proof-of-share)과 같은 새 방법이 제안됨

CPU ⟹ GPU ⟹ FPGA ⟹ ASIC ⟹ Cloud Mining/Mining pool

Mining Farm

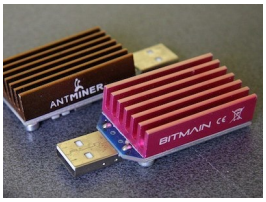



Mining Device

$479.95

$1,987.95

$499.95



$49.66

- ASIC에 의한 채굴 집중화
- ASIC 기업(Bitmain)에 의한 채굴 왜곡
- 극복방안. 해시함수의 변경 (이더리움)
- ASIC 기업은 계속 채굴을 위한 전용 하드웨어 개발을 시도하고 있음

https://www.bitcoinmining.com/bitcoin-mining-hardware/

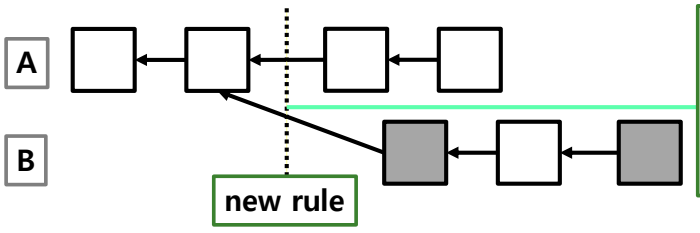
하드포크 vs. 소프트포크 (1/3)

- 비트코인은 P2P 시스템이기 때문에 모든 노드가 동일 소프트웨어를 사용하도록 강제화하기 쉽지 않음
  - 의미. 노드마다 사용하는 SW 버전이 다를 수 있음
- 소프트웨어 버전의 변경은 소프트웨어 결함을 해소하기 위한 이유도 있지만, 규칙 변경을 위해 변경되는 경우도 있음
  - 트랜잭션 검증 규칙, 블록 구성 규칙 등은 일관성(노드마다 같은 규칙을 사용해야 함)이 반드시 유지되어야 함
- 규칙 변경
  - 경우 1. 과거와 호환되지 않는 규칙의 도입
  - 경우 2. 과거와 호환되는 규칙의 도입

- 경우 1를 하드포크, 경우 2를 소프트포크라 함
- 둘 다 포크되었지만 긴 체인 우선에 의해 한 쪽 체인이 모두 무효화되지 않고, 각 체인을 계속 유지할 수 있음
- 규칙 변경에 영향을 주는 집단: 채굴자뿐만 아니라 모든 완전 노드

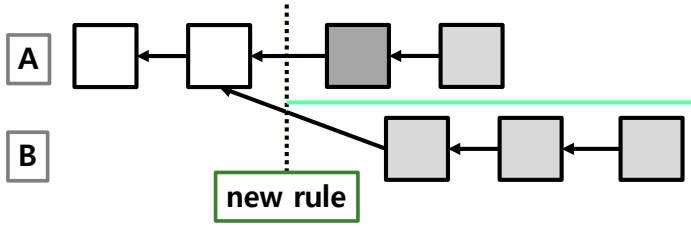
하드포크 vs. 소프트포크 (2/3)

- 하드포크: 규칙 변경이 과거와 호환되지 않음 (새 규칙의 추가 포함)
  - 집단 A: 이전 규칙 사용, 집단 B: 새 규칙 사용 (예: 블록 크기 증가)



- A는 파랑은 인정하지 못함
- A가 규칙에 합의하지 않은 이상 두 체인이 계속 유지될 수밖에 없음
- A 집단이 합의하는 것도 쉽지 않음. 기존 이득을 모두 포기해야 함

- 소프트포크: 규칙 변경이 과거와 호환 (기존 규칙의 삭제 포함)
  - 집단 A: 이전 규칙 사용, 집단 B: 새 규칙 사용 (예: 블록 크기 감소)



- A는 모두 인정, B는 녹색을 인정하지 못함
- 하드포크와 달리 A는 B 쪽 체인으로 넘어가는 것에 문제가 없음. → 긴 체인 우선 원칙에 따라 쉽게 하나로 통일 가능 → 통일되기 위해 B 집단이 다수가 되어야 함

하드포크 vs. 소프트포크 (3/3)

- 하드포크의 종류
  - 계획된 하드 포크(planned hard fork)
  - 논쟁 하드 포크(contentious hard fork)
- 누가 주도하느냐에 따라 구분될 수도 있음
  - 채굴자 주도(MAHF) vs. 사용자 주도(UAHF): A(Activated)
  - 채굴자 주도가 가장 확실
    - 완전 노드들도 동의해야 포크가 더 매끄럽게 이루어질 수 있음
- 포크가 주는 또 다른 의미는 기술과 상관없이 언제든 불가역성이 보장되지 않을 수 있다는 것을 의미함

- 암호화폐가 사용하는 소프트웨어 보통 오픈 소스 형태임
- 이 소스를 일부 수정하여 새 암호화폐를 만들 수 있고, 이 경우에도 포크하였다고 함
  예) LiteCoin은 비트코인에서 포크한 암호화폐임

비트코인의 개선 - 세그윗

- 세그윗(segwit)
  - 비트코인 블록의 크기는 1MB로 제한됨
    - 이 블록은 트랜잭션의 내용으로 구성됨
    - 트랜잭션의 내용 중 가장 많은 부피를 차지하는 것은 전자서명 값임
  - 세그윗은 “segregation of witness”의 약어로 트랙잭션 내부 내용 중 전자서명 부분을 분리함
  - 블록 크기 1MB에서 분리함으로써 더 많은 트랜잭션을 블록에 포함할 수 있음
  - 소프트 포크로 도입함 (2017)
  - 전체 트랜잭션을 그대로 유지하면서 트랜잭션의 ID를 바꿀 수 있는 보안 허점도 세그윗을 통해 극복함
    - 더 이상 트랜잭션 ID를 서명에 포함하지 않음
  - 서명도 별도 해시 트리로 구성하여 coinbase 트랜잭션에 포함함
  - SegWit2x의 하드 포크 도입에 대한 시도도 있었음 (2017)

2계층 블록 체인 기술

- 블록 체인의 확장성 문제와 높은 수수료 문제를 극복하기 위해 블록 체인에 외적인 방법을 사용하는 기술을 2계층(layer 2) 블록체인 기술이라 함
  - 확장성을 위한 오프체인 해결책
- 지불 채널(payment channel)
  - 기본 생각. A와 B가 여러 차례 거래를 해야 할 경우 모든 거래 내용을 블록 체인에 기록하지 않고 최종 결과만 기록함
    - 수수료 절약
    - 트랜잭션 처리 속도 향상
  - 소액 지불에 적합

지불 채널 이해를 위해 필요한 사전 지식

- 다중 서명 지갑
  - 보통 비트 코인 지갑은 하나의 공개키 쌍과 연결되어 있음
  - 다중 서명 지갑은 여러 개의 공개키를 하나의 지갑과 임계 기반 형태로 연결할 수 있음
  - 예) 2-3 multisig 지갑: 지불자, 판매자, 중재자 (3개 중 2개의 서명 필요)
  - 예) 2-3 multisig 지갑: 2개의 키와 백업 키
  - 여러 개의 공개키를 이용하여 지갑 주소를 만듦
- 시간 잠금: 일정 시간이 지나야 트랜잭션 또는 트랜잭션의 출력을 사용할 수 있도록 하는 기술
  - 시간: 실제 시간 또는 블록 높이
    - 절대 시간, 상대적 시간 개념 모두 가능

- CLTV(CheckLockTimeVerify)
- CSV(CheckSequenceVerify)

	절대	상대
트랜잭션 수준	nLockTime	nSequence
UTXO 수준	CLTV	CSV

- 트랜잭션 수준: 트랜잭션의 블록 등록을 지연
- UTXO 수준: UTXO의 사용을 지연

지불 채널 이해를 위해 필요한 사전 지식

- 예) TX_2는 TX_1의 UTXO를 사용하는 트랜잭션
  - TX_2 입력의 nSequence = 10 blocks
    - TX_2는 TX_1이 등록된 이후 10개 블록이 지나야 블록 체인에 등록할 수 있음
- CLTV/CSV 잠금은 잠금이 해제되기 전에 유효한 트랜잭션이 등록되면 이중 사용으로 사용할 수 없게 됨
- 해시 시간 잠금 (HTLC, Hash Time Locked Contracts)
  - 지불을 처리하기 위한 조건을 트랜잭션에 포함
  - 트랜잭션에 $H(x)$를 포함하면 x가 없으면 이 트랜잭션은 유효한 트랜잭션이 되지 못함
  - 만료 시간이 함께 연결되어, 만료 시간 전에 x가 공개되어 트랜잭션이 처리되지 않으면 트랜잭션은 무조건 무효화됨

지불 채널 (1/3)

- 양방향 지불 채널
  - 채널 개설. A와 B는 일정한 금액을 2-2 다중 서명 지갑에 예치함. 이 트랜잭션은 블록 체인에 기록함
    - 개설 이후 한 사용자가 부당하게 채널을 닫을 수 있기 때문에 예치한 금액을 회수할 수 있는 트랜잭션(패널티 트랜잭션)을 교환한 후에 개설을 완료함
    - 이 트랜잭션은 적절한 잠금 장치(CLTV)를 설정하여 정상적인 경우에는 사용할 수 없도록 함
  - 채널 종료. A와 B는 언제든지 닫을 수 있음. 채널을 닫으면 최종 트랜잭션이 블록 체인에 기록됨

- 패널티 트랜잭션을 생성할 때 nLockTime, CLTV 둘 중 하나를 사용할 수 있음
  - 트랜잭션: nLockTime:24hours, 입력: 다중지갑 100, 출력: A 100
  - 트랜잭션: nLockTime:0, 입력: 다중지갑 100, 출력: A 100(CLTV: 24hours)
- nLockTime는 트랜잭션 가단성(malleability) 공격에 취약하기 때문에 주로 CLTV를 사용함
- 트랜잭션 가단성 공격이란 유효한 동일 트랜잭션을 여러 개 만들 수 있기 때문에 발생할 수 있는 공격. (트랜잭션 내용은 동일하고 유효하지만 위치나 값을 약간 바꾼 경우 해시값이 달라지며, 결과 서명 값도 달라짐)

지불 채널 (2/3)

- 예) B는 스트림 서비스 제공, A는 이 서비스를 사용하고 싶음
  - 시청 시간에 따라 서비스 금액을 지급해야 함
  - 지불 채널 개설 (2-2 multisig 지갑 개설)
  - A는 이 지갑에 100satoshi 예치
    - B는 100satoshi를 A에게 지급하는 패널티 트랜잭션을 생성하여 전달함
      - CLTV 설정
  - A는 시청할 때마다 1satoshi를 B에게 지급하는 트랜잭션을 생성
  - Tx1: 1satoshi ⟹ B, 99satoshi ⟹ A (A가 서명하여 생성한 Tx)
  - Tx2: 2satoshi ⟹ B, 98satoshi ⟹ A
    - B는 수신한 트랜잭션에 서명하여 언제든지 채널을 닫을 수 있음
      - 닫으면 패널티 트랜잭션은 사용을 할 수 없게 됨
  - B가 일정 시간이 지나도 닫지 않으면 A는 자신이 되돌려 받아야 하는 금액을 받지 못함
    - A는 패널티 트랜잭션을 서명하여 최초 예치한 금액을 회수할 수 있음

- 미미는 티빙을 시청하고자 함
- 티빙은 드라마 1편에 100원에 해당하는 비트코인을 받음

- 2-2지갑 (미미, 티빙) 생성: 시청지갑
- 이 지갑은 미미와 티빙이 모두 서명해야 사용 가능

- 미미는 1,000원에 해당하는 돈을 시청지갑에 지불함

- 미미는 드라마를 보기 전에 100원 티빙에게 지급하는 트랜잭션을 생성함
- 출력: 100원 티빙, 850원 미미 (미미 서명)

- 미미가 마지막 생성한 트랜잭션은
- 출력: 500원 티빙, 450원 미미 (미미 서명)

- 티빙은 마지막 트랜잭션을 닫아야 이득임. 이전 트랜잭션을 닫으면 오히려 손해

- 티빙이 어떤 거래도 닫지 않으면 미미는 손해임
- 최초에 티빙은 패널티 트랜잭션을 만들어 미미에게 주어야 함
- 출력: 1000원 미미

- 미미가 패널티 트랜잭션을 먼저 블록에 등록하면 티빙은 손해임
- 패널티 트랜잭션에 잠금 장치를 하여 일정 시간이 지나야 블록에 등록할 수 있도록 함

지불 채널 (3/3)

- 사용자 A가 여러 사용자와 소액 거래를 하고 싶으면 각 사용자와 지불 채널을 개설해야 함 ⟹ 번거로움
  - 개선 방안. 지불 채널 네트워크(PCN, Payment Channel Network)
    - 예) Lightening network
  - A ⟹ B, B ⟹ C, C ⟹ D 채널이 개설되어 있으면 A는 B와 C를 통해 D에게 지불할 수 있음
    - 네트워크 자체에서 필요한 경로 설정을 해줌
  - HLTC의 사용이 필요함
    - A가 B를 통해 C에게 1BTC을 지급하고 싶음. B는 중계를 하지 않을 수 있음
    - A가 C로부터 $H(x)$를 받아 B에게 1BTC를 주는 트랜잭션의 HLTC로 설정함
    - B는 HLTC $H(x)$를 포함한 C에게 1BTC를 주는 트랜잭션을 생성함
    - C는 x를 제시하여 트랜잭션을 유효하게 만듦. B도 x를 사용함

비트코인 블록체인의 특성

- 10분마다 계속 생성됨. 누군가 계속 생성해 주어야 함
- 첨삭만 가능
  - 특정 블록을 수정하기 위해 암호 퍼즐을 계산하여도 해당 블록 이후 모든 블록의 암호 퍼즐을 새롭게 계산하여야 하며, 계속 생성되고 있는 기존 체인보다 더 긴 체인을 만들어야 함
  - 단점이 될 수 있음. 기록을 영구히 삭제할 수 없음
    - 블록체인은 aging 기능이 없음
- 분산 저장되어 있음
  - 분산 저장된 모든 데이터를 다 바꾸기 힘듦
  - 이 때문에 다른 말로 분산 원장(distributed ledger)이라 함
- 공개형 블록체인. 누구나 접근 가능함
- 블록에 기록을 포함하는 권한은 블록을 생성하는 주체의 마음
- 체인 순서에 의해 각 블록이 생성된 시점에 대한 상대적 시간을 알 수 있음
- 오픈 소스로 운영됨 (신뢰성이 높음)

건전해야 가치가 유지 또는 상승

비트코인의 안전성

- 가정. 비트코인 SW는 안전함
- 비트코인의 발행
  - 채굴을 통해서만 새 코인을 만들 수 있음
  - 채굴 방식 때문에 특정 참여자나 기관이 손쉽게 많은 양의 비트코인을 만들 수 없음
- 기존 거래 내역의 수정
  - 해당 거래 내역을 수정하고, 그 내역이 포함된 블록을 새롭게 채굴해야 함
  - 해당 블록 뿐만 아니라 그 이후 모든 블록을 다시 채굴해야 함
  - 블록은 10분마다 계속 채굴되며, 긴 체인이 우선되기 때문에 거래 내역의 수정은 가능하지 않음
  - 매우 강력한 채굴자(전 세계의 해시 파워의 50% 이상을 차지)가 등장하면 문제가 발생할 수 있으나 현재의 생태계를 고려하였을 때 현실성이 없음
- 코인 가로채기: 해당 코인을 사용하기 위해서는 개인키가 필요함

비트코인의 문제점

- 화폐 기능
  - 가격의 불예측성
  - 거래 확정 속도
  - 불법 거래 사용
- 코인 거래소 등장
  - 기존 시스템과의 차이
  - 중재자의 등장
- 채굴의 중앙 집중화: 채굴자와 일반 사용자가 명백하게 구분됨
  - 현재는 일반 사용자도 없고 투자자만
- 채굴방법 때문에 일어나는 환경 파괴
  - PoW ⟹ PoS
- 확장성 문제
  - 세그윗, 지불 채널, sharding 등 다양한 확장 방안이 도입되거나 검토되고 있음

비트코인의 문제점

- 블록크기의 제한과 블록 생성 속도
  - 블록 크기의 제한은 전파 속도 때문에
  - 생성 속도는 안전성 때문에
    - 용도를 고려하여 크기와 난이도를 잘 조절하여야 함
  - 하지만 이 문제 때문에 결국 비트코인이 비트코인캐시로 갈라짐 (2017년 8월)
    - 2017년 10월에는 비트코인 골드로 또 갈라짐
      - ASIC 사용한 채굴을 못하기 위해 PoW 방식 변경
    - 비트코인캐시는 다시 Bitcoin SV로 갈라짐 (2018. 11)

Bitcoin Bitcoin Cash