비트코인의 기반 기술

블록체인의 원리

김 석 원
skimaza@spri.kr

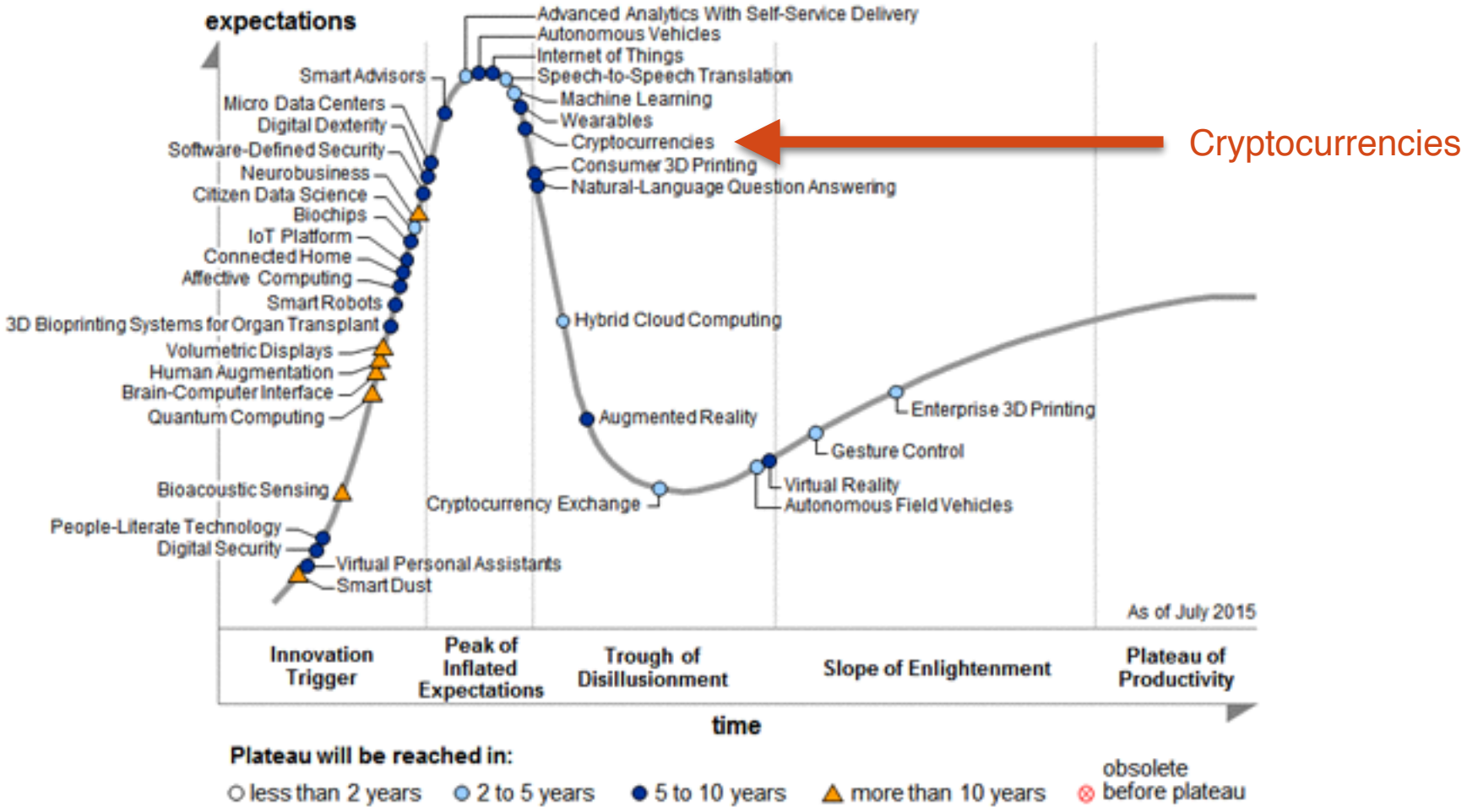
2016.01.20

소프트웨어 중심사회의 Think Tank SPRi Software Policy & Research Institute

왜 또 블록체인인가?

- 비트코인의 기술 기반인 블록체인에 대한 원리를 다룬 자료의 부족
  - 블록체인의 가능성에 대한 판단이 어려움
- IBM, Goldman Sachs, JP Morgan 등 해외에서는 블록체인의 혁신성을 인식하고 활용하려는 움직임이 있음
  - 국내에도 스타트업 중심으로 활동이 있으나 소규모
- 비트코인은 거품이 있었으나 고비를 넘기고 여전히 확산 중
  - 비트코인은 죽을지 모르나 블록체인은 살아남을 것

가트너 Hype cycle 2015



Cryptocurrencies

http://www.gartner.com/newsroom/id/3114217

비트코인 통계

시가총액

2014/01 2016/01

가격

2014/01 2016/01

하루 거래건수

2014/01 2016/01

https://blockchain.info/charts http://www.coindesk.com/price/

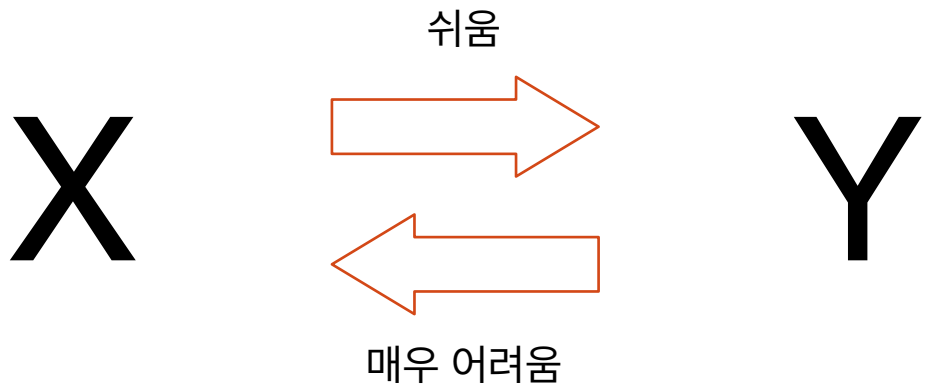
주요 개념의 관계

블록체인은 **분산**되고, **독립**적이며, **개방**된 공통 장부(원장, ledger) 관리 기술
비트코인은 이 공통 장부를 거래기록 용도로 활용한 애플리케이션

P2P와 비대칭키 부분은 본 발표에서 깊이 다루지 않음

Hash 함수

한 방향 계산은 쉬우나 역방향 계산은 매우 어려운 수식



간단한 예) 특정 소수로 나눈 값의 나머지 함수 (modular)

가령 7로 나눈 나머지 함수 MOD7

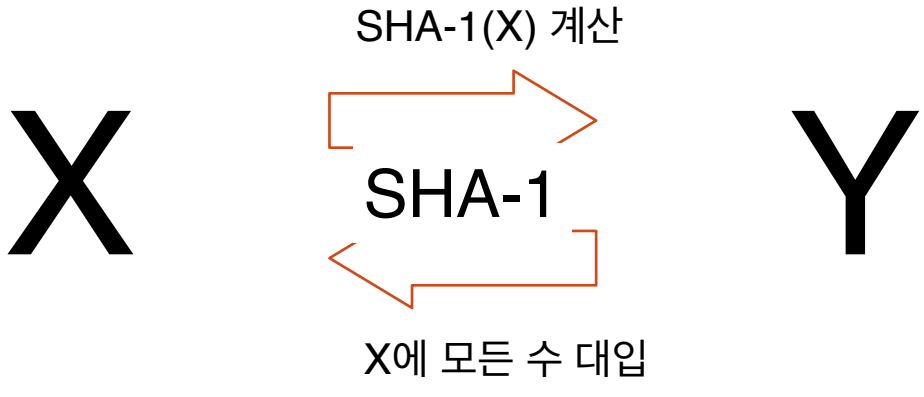
X=19일 때, Y=MOD7(19) = 5 간단히 계산

Inverse-MOD7(5) = 5, 12, 19, … 등 무수히 많음

(단순 나머지함수는 X를 정확히 찾아내는 것이 불가능하지만 개념 이해를 위해 제시)

얼마나 어려운가?

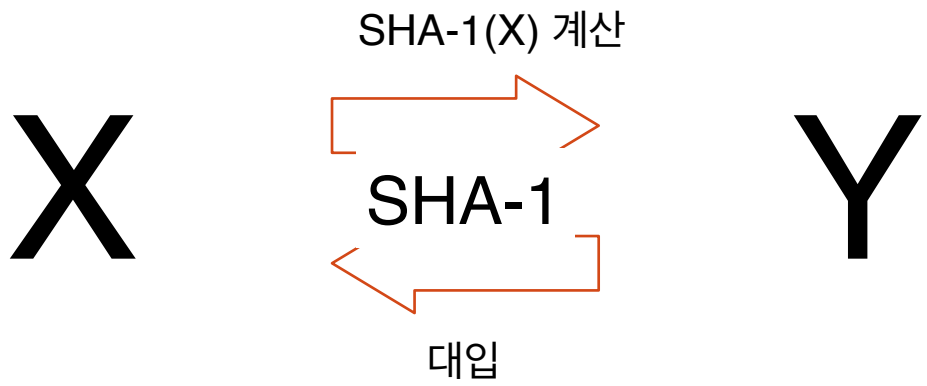
해쉬값(Y)에서 원래 입력값(X)을 알아내는 방법
(SHA-1이라는 해쉬함수를 쓰는 경우)



정확한 Y가 나오는 X를 찾으려면
Y가 160비트일 때 최대 2^{160}번 시도

SHA: Secure Hash Algorithm
공개 표준 해쉬 함수로 결과값은
160비트로 고정

Hash 함수



- 입력에서 출력으로 한 방향 계산은 쉬우나 역으로 출력값에서 입력값을 계산하는 것은 불가능하거나 매우 어려운 함수. 역함수 계산은 대입법 뿐
- 출력값은 미리 정해진 길이(비트수)의 데이터로 규정. 모든 출력값은 같은 길이
- Y는 X의 요약. 주로 X의 무결성을 검증하는 용도로 사용

- Hashcash는 160비트 SHA-1, 비트코인은 256비트 SHA-2를 사용

Hashcash

SHA-1(X) = Y인 X 찾기에서
SHA-1(X) ≤ K 인 X 찾기로 완화

- 해쉬를 거꾸로 생각해 보자
  - 한쪽 방향 계산은 아주 많은 계산을 해야 하나, 반대 방향은 금방 계산할 수 있다
- 역방향 계산에 대한 제약을 조금 풀면?
  - 원래의 해쉬는 정확한 Y값을 계산하는 X를 찾아야 하기 때문에 어려움
  - Y가 주어지고 대응하는 X를 찾기 위해 모든 X값을 대입하는 과정을 완화
- 어떤 수(K) 보다 작은 Y가 나오는 X값을 찾기
  - K = 000…00111111…111 라면?

해쉬 제약 완화

Y에서 X를 구하려면
X=0부터 차례로 대입해 봐야 함

Y가 160비트일 때

매우 어려움

X → SHA(X) → Y = 1001……..010

160비트
특정 숫자

제약 완화

난이도 조절 가능

X → SHA(X) → 00…0 | 10……..1

20비트
모두 0

140비트
아무 숫자

2^{160} 중 하나에서 2^{20} 중 하나로!

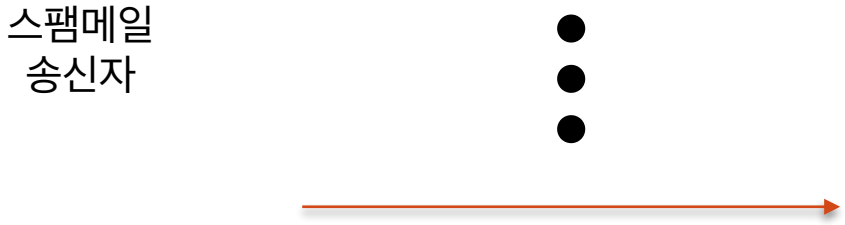
완화된 해쉬 조건

- 한쪽 방향 계산은 쉽고 역방향 계산은 적절한 난이도

- 역방향 계산하는 쪽은 어느정도 노력 소모
  - X값 찾기
- 정방향 계산하는 쪽은 단번에 계산하여 정답인지 확인이 가능
  - X값을 해쉬하여 제약을 만족하는지 확인

- 스팸메일 필터로서의 용도!
  - 메일을 보내기 위해 노력(계산)을 들여야 함 (역방향)
  - 메일 받은 사람이 보낸 사람의 노력을 들였는지 확인하는 것은 단번에 함 (정방향)

Hashcash 스팸메일 필터링



스팸메일은 천만번 중 하나 정도의 효과
(2008 미국 조사)

보낼 때 1인당 시간이 많이 걸린다면? 즉 비용이 많이 든다면?
→ 스팸메일을 보내는 노력에 비해 효과가 현저히 떨어짐

한 명당 1초씩 걸리면?
→ 백일에 1명 정도의 효과 → 가치 상실

수신자가 송신자의 노력을 '검증'할 수 있다면?

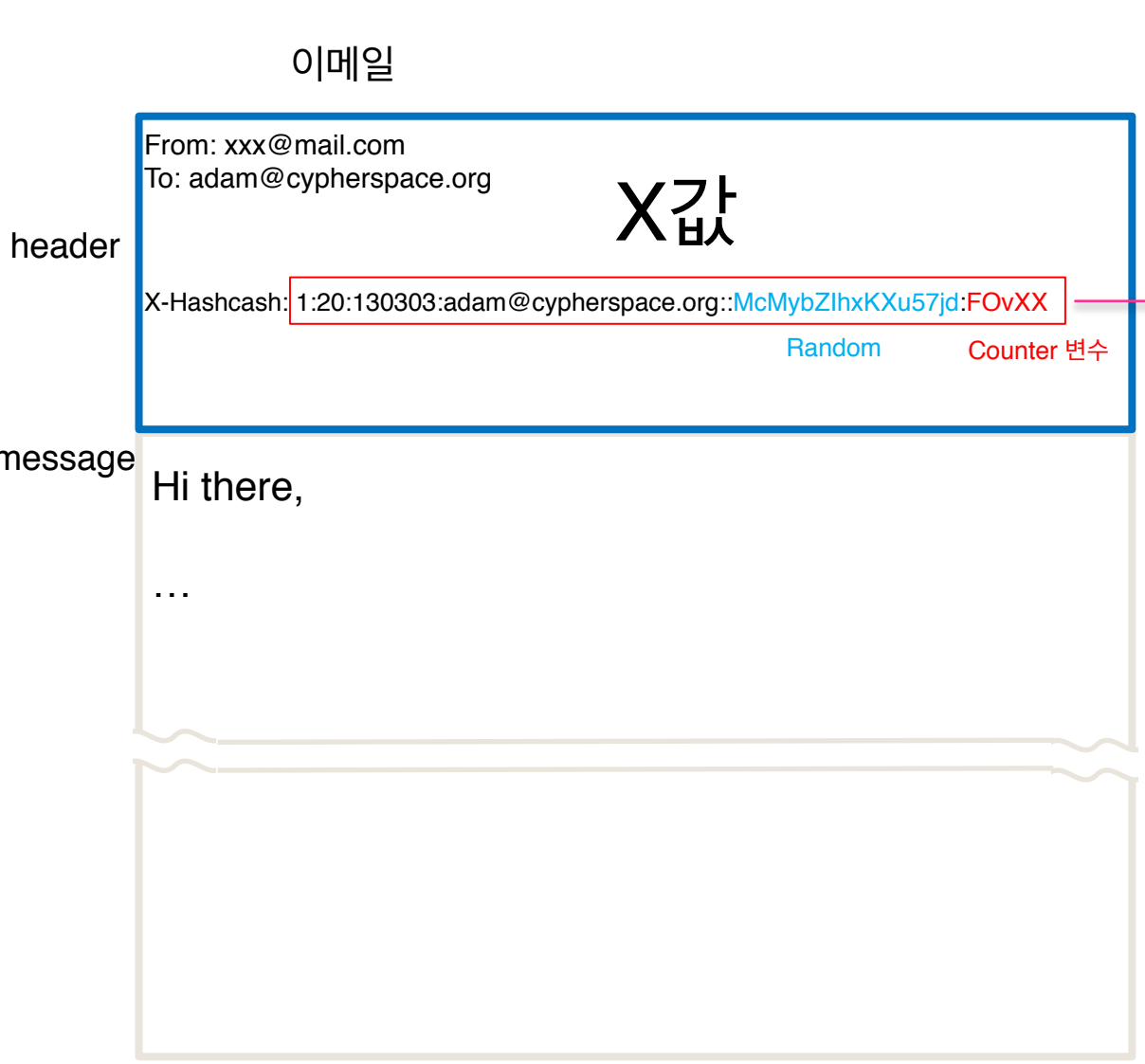
정상 사용자는 문제없다 → 보내기를 누르고 1초 후에 전송

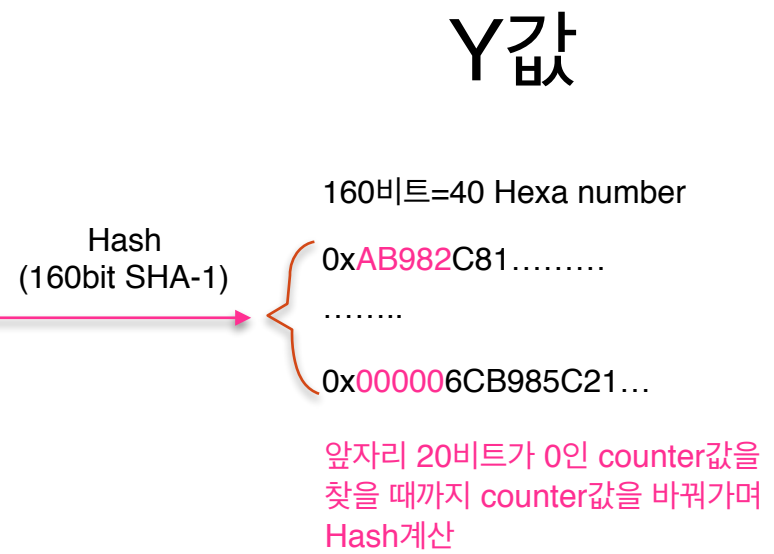
메일 보낼 때 노력을 했다는 증거를 함께 보내자

Proof of Work

http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf

Hashcash 구성





Counter값을 찾으면 그 값(FOvXX)이 포함된 헤더와 함께 메일 전송

해쉬함수의 특성상 수신자는 한번 계산으로 이 값의 앞자리 20비트가 0이라는 조건을 만족하는지 검증 가능

https://en.wikipedia.org/wiki/Hashcash

X-Hashcash 상세

X값

1:20:130303:adam@cypherspace.org::McMybZlhxKXu57jd:FOvXX

ver bits date 수신자 주소 Random Counter

- **Counter**
  - **“일일이 대입 " 을 구현하기 위해 counter값이 있음**
  - **입력값(X)의 제일 뒤에 counter값 필드를 두고 그 값을 차례로 증가하여 (즉 입력값을 바꿔가며) 조건에 맞는 Y가 나올 때까지 Hash 계산을 반복**
- **Random**
  - **같은 해쉬값의 반복적 이용을 막기위해 수신인은 한번 받은 해쉬값을 보관**
  - **메일을 받으면 이미 받은 해쉬인지 확인**

Hashcash 개념 요약

- 해쉬를 역으로 활용하여 메일보내는 노력(Proof-of-work)을 증명
  - 노력이 신뢰를 높인다
- 검증은 간편
- 제3자 개입 없이 개인 대 개인간의 검증

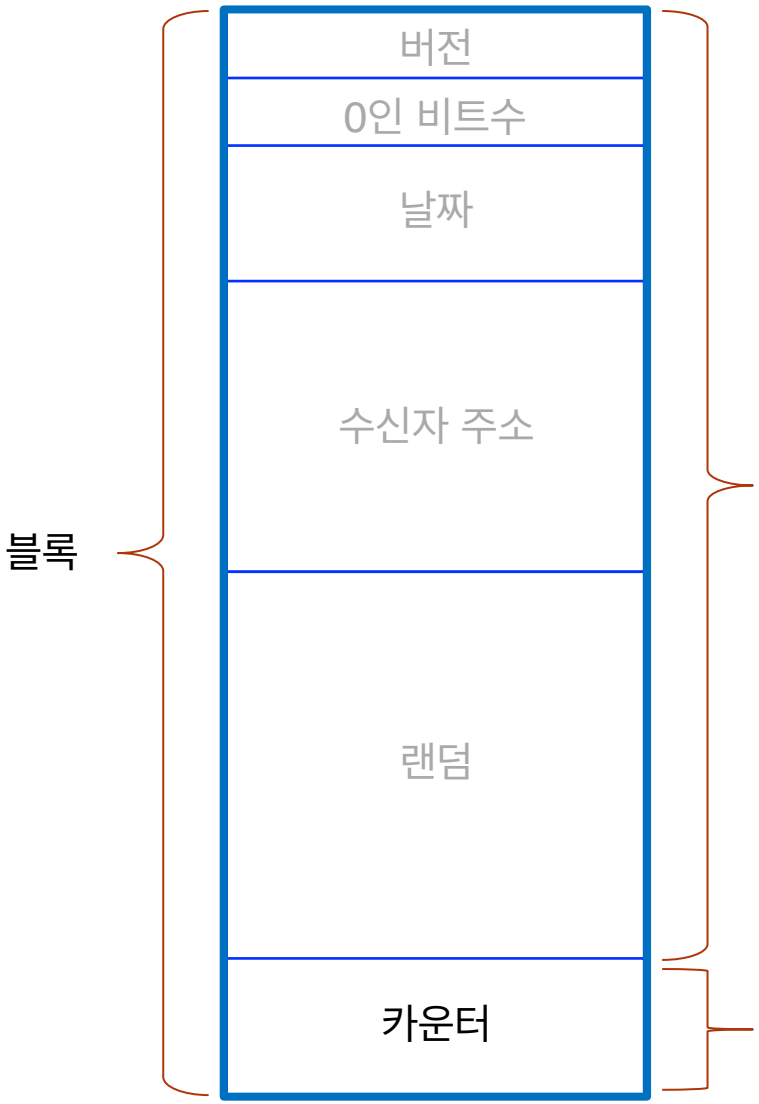
Hashcash 아이디어를 공통 장부 관리에 응용

분산

독립

개방

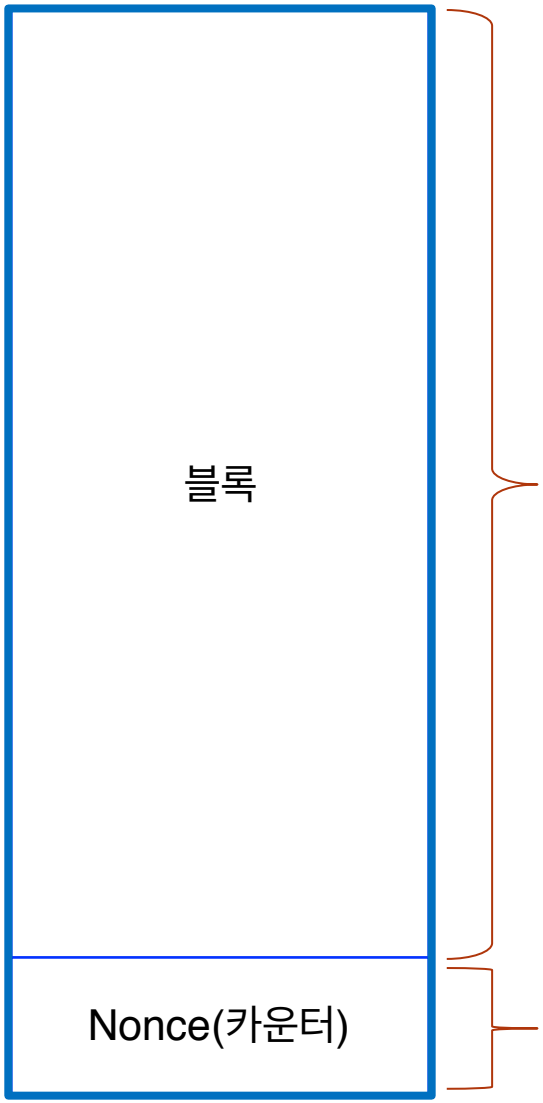
Hashcash 메일헤더를 블록형태로 표현하면



SHA(블록) ≤ K 인 카운터 값 찾기

메일이 아닌
다른 형식의 블록에도
Proof-of-Work를
적용할 수 있다

블록에 Hashcash 아이디어 적용



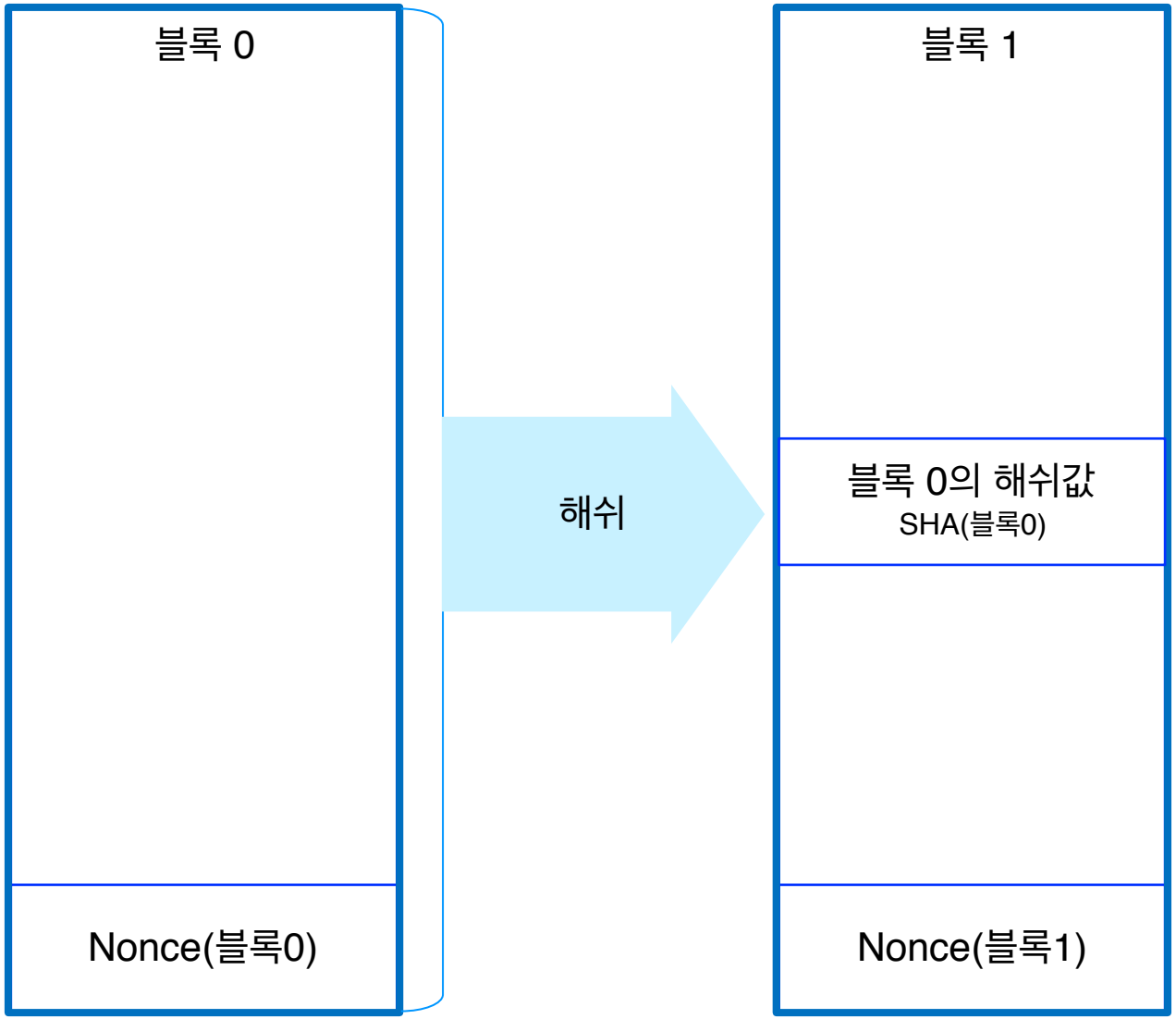
SHA(블록) ≤ K 인 nonce 값 찾기

블록 내용을 보증하기 위한
노력의 증거

불특정 다수가 블록 내용을
검증하고 그 노력에 대한
보상을 해주는 체계

내용이 늘어나면?

내용의 추가 - 블록 연결



블록의 연결은 현재 블록에 이전 블록의 해쉬값을 포함

→

블록0를 알 때

새 블록1을 만들기는 어렵다.

블록0를 알 때

새 블록1을 받은 후 검증하기는 쉽다

블록1은 블록0의 신뢰도를 강화

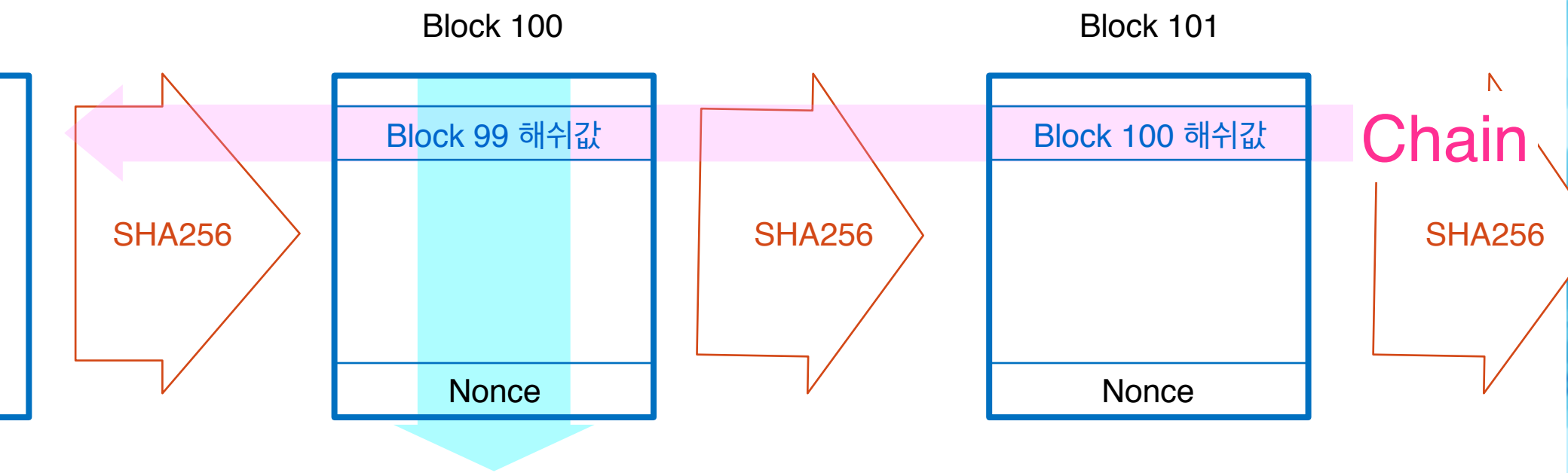
→ 노력이 신뢰를 높인다!

기술발전 속도로 봐서 적절한 난이도의 해쉬함수와 해쉬값 제약은?

블록체인에서 난이도 강화

- 스팸메일 필터보다 중요한 응용을 위해 난이도 강화
- 해쉬함수는 공개 표준 해쉬함수 중 256-bit SHA-2 (SHA-256) 사용
- K값 강화
  - 해쉬결과 범위 조정
  - 256비트 중 선행0비트 수는 40개 → 앞의 40자리는 0, 나머지 216자리는 튜닝 가능

블록의 연결 - Chain of Hash values



표준 해쉬 함수
SHA256 사용

Block 100에 대해 SHA256 해쉬값의 앞자리 40비트가 0이 되는 Nonce 값을 찾기

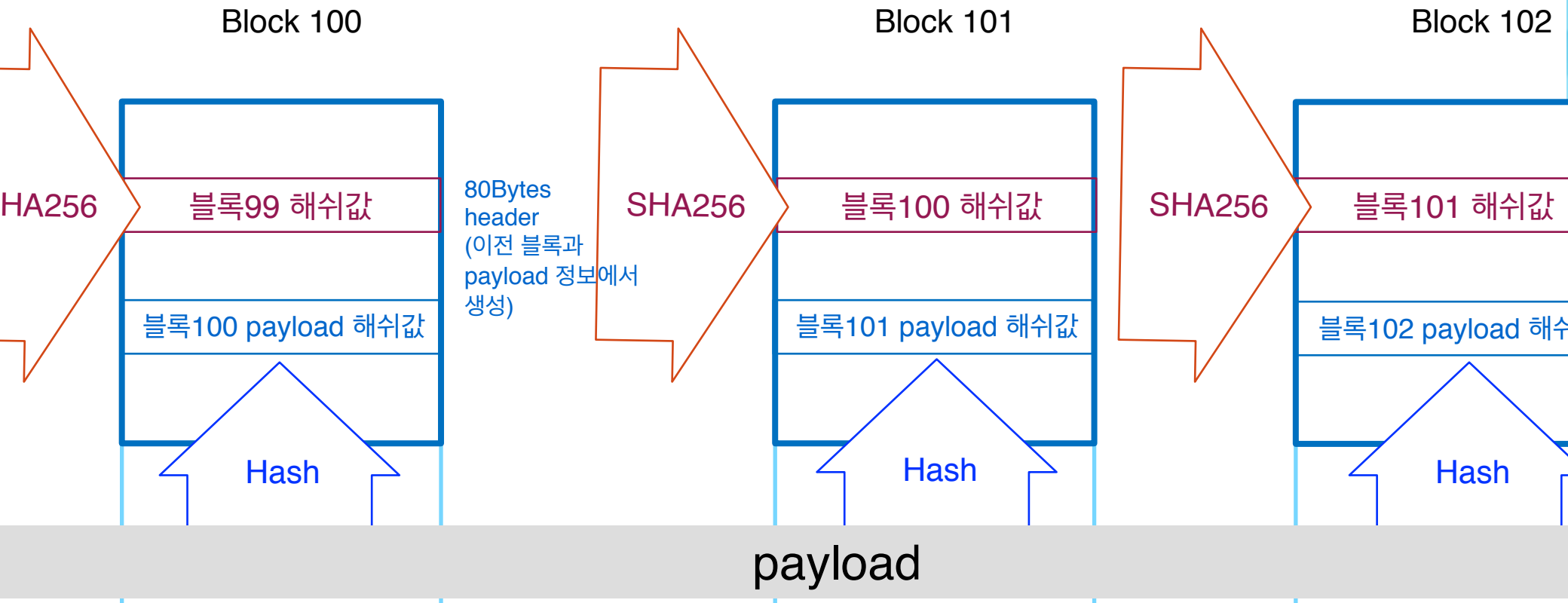
256비트

0x0000000000 6CB9……80AE

40비트

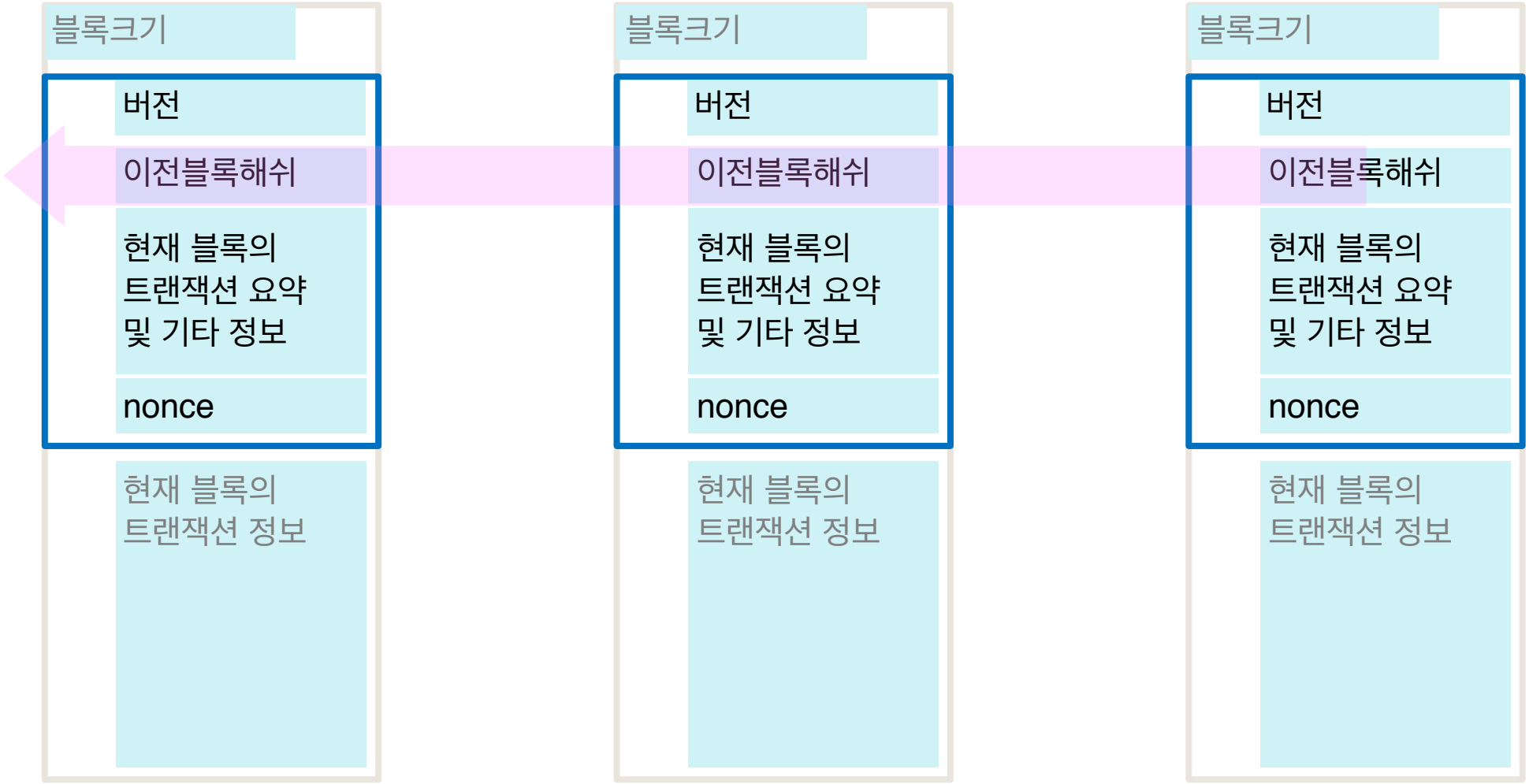
전체 블록을 해쉬할 필요가 있을까?

블록헤더만 해쉬한다 - 효율성



- 블록의 내용인 payload를 해쉬하여 블록헤더에 포함
- 해쉬는 내용의 요약
  - payload의 해쉬가 헤더에 포함
  - 헤더만 해쉬해서 연결해도 본문(payload)을 요약한 효과

블록체인의 구조

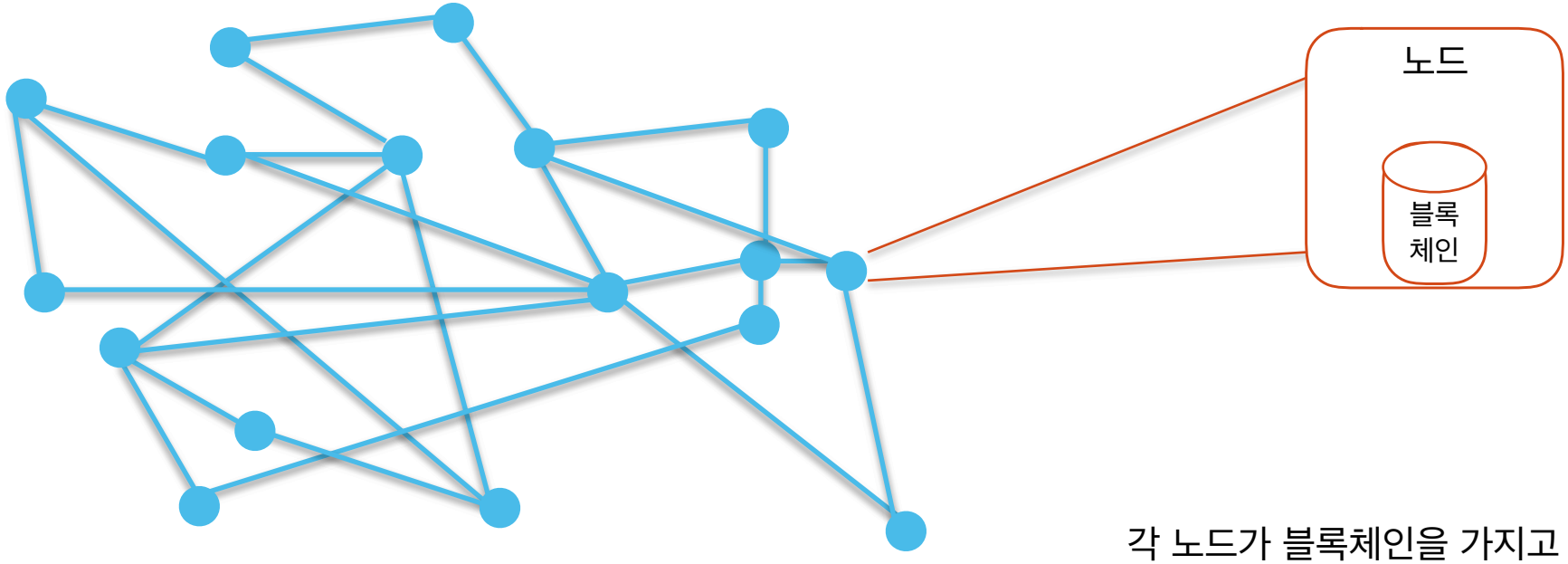

블록크기
버전
이전블록해쉬
현재 블록의
트랜잭션 요약
및 기타 정보
nonce
현재 블록의
트랜잭션 정보
블록크기
버전
이전블록해쉬
현재 블록의
트랜잭션 요약
및 기타 정보
nonce
현재 블록의
트랜잭션 정보
블록크기
버전
이전블록해쉬
현재 블록의
트랜잭션 요약
및 기타 정보
nonce
현재 블록의
트랜잭션 정보

블록체인 구조 요약

- 블록은 이전블록의 해쉬값을 포함
  - 새 블록을 만들기 위해 이전 블록을 가지고 충분한 노력을 들인 증거 - Proof-of-work
  - 다른 곳에서 만든 블록이 정당한지 검증이 용이
- 체인이 길어질 수록 블록의 신뢰도 증가
- 블록의 내용은 따로 해쉬하여 헤더에 저장
  - 블록의 검증을 헤더만 가지고 할 수 있음
  - 실제 비트코인은 단순해쉬가 아니고 좀 더 복잡한 방법(이진 해쉬 트리)을 이용하나 여기서는 생략

- 새 블록은 누가 만드나?

블록체인 네트워크



각 노드가 블록체인을 가지고
모두 독자적으로 작업하는
P2P 네트워크

P2P 네트워크 구성

- 각 노드, 즉 컴퓨터는 독자적으로 블록체인의 내용을 검증할 수 있다
  - 아무도 믿지 않아도 됨
- 각 노드는 독자적으로 블록체인에 블록을 추가할 수 있다
  - 그러나 1등만 전파됨 → 다른 노드가 인정해 줌
- 모든 노드는 정해진 규칙하에서 동작
  - 자신의 이익을 극대화하는 방향으로 규칙이 설계

- 참여를 유인하는 인센티브가 있어야 한다
  - 비트코인은 1등에게 신규 발행 비트코인과 블록내 거래의 수수료 지급
  - 이 과정이 채굴(mining)임
  - 다른 응용에서도 적절한 인센티브를 설계해야 함

블록체인 요약

- 블록을 만드는데 노력을 들였다는 것을 객관적으로 증명하는 방법
  - 누구나 블록을 만들 자격이 있다
  - 누구나 블록이 정당한지 검증할 수 있다
- Distributed Ledger Management
  - 블록을 연결하여 하나의 공통 문서(기록 혹은 장부, ledger)를 축적해 가는 방법
  - 블록이 연결될 수록 이전 블록의 신뢰는 점점 커짐
    - 위에 쌓이는 새 블록은 아래에 놓인 이전 블록이 옳다는 것을 검증하고 쌓인 것이기 때문
  - 체인의 구조에 의해 직전 블록의 해쉬값만 검증해도 모든 블록이 옳다는 것을 검증한 것임
    - (주의) 여기서 검증했다는 것은 많은 노력을 들여 블록체인을 만들었다는 의미이며 완전무결하다는 의미는 아님
- 중앙집중적인 관리 주체 없이 블록체인의 동작과 검증이 가능
- 완전 분산화된 Peer-to-peer 네트워크에서 운영이 가능한 아키텍처
  - 피어가 많을 수록 더 안전해 짐

비트코인 기본 개념

- 블록체인을 통화에 적용한 응용 사례
  - 블록의 payload에 거래 내역 보관

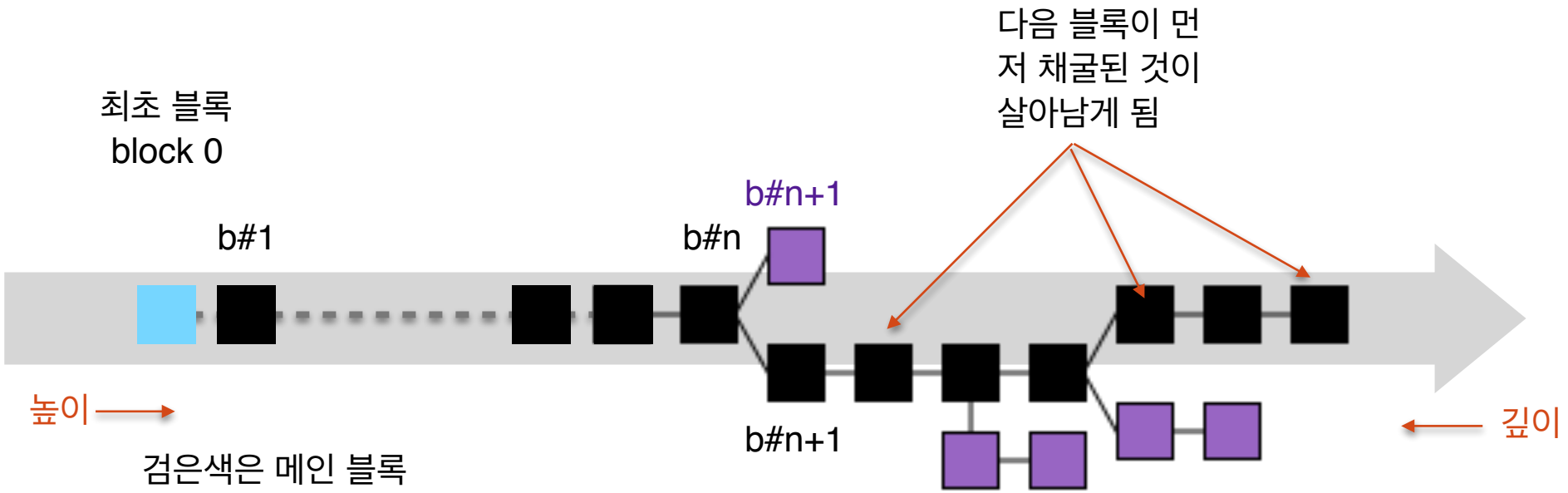
- Hashcash의 proof-of-work는 정체가 뭔가?
  - 이메일을 보내기 위해 노력한 증거, 즉 신뢰
- 통화의 정체는 뭔가?
  - 같은 가치의 다른 것으로 교환할 수 있다는 신뢰
  - 신뢰는 제3자에 의해 보증됨 – 발행 국가
  - 이 신뢰는 절대 100%가 아님
  - 신뢰가 가치임

- 일정한 노력을 들여 획득했다는 신뢰를 줄 수 있으면 통화로 쓸 수 있다는 아이디어

비트코인 채굴

- 채굴, Mining은 새 블록을 만드는 작업
  - 이전 블록의 해쉬값을 찾아낸 것이 Proof-of-work
  - 채굴은 조금씩 코인을 쌓아가는 과정이 아니라 10분에 한번씩 벌어지는 달리기 경주나 로또와 유사
  - 전세계에서 채굴에 참여한 모든 컴퓨터가 평균 10분에 한번씩 전세계의 거래(트랜잭션)를 모아 조건을 만족하는 Hash값을 구하여 새 블록 생성
- 새 Block이 만들어지면 즉시 다른 노드에 전송
  - 계산 중에 다른 노드가 만든 블록이 입수되면 즉시 계산 중단하고 그 다음 블록을 만드는 계산에 착수
  - 새 블록이 블럭체인에 추가된 노드만 채굴 보상금 수령 (신규발행 + 거래 수수료 : 코인베이스 거래)
  - 평균 10분에 한 노드만 비트코인을 받도록 지속적으로 튜닝
- 동시에 여러 노드가 채굴에 성공하면?
  - 긴 블록 선호 정책
  - 채굴보상금은 즉시 사용할 수 없음 (수령후 100 블록 추가된 이후)

블록체인 분기



긴 블록 선호 정책으로 해소

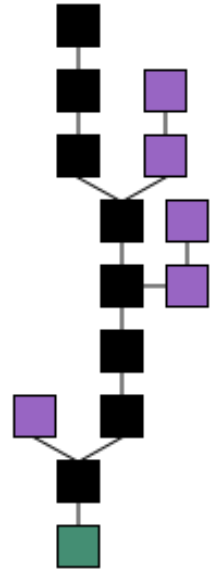
각 노드의 이익을 극대화하는 정책

짧은 블록에 노력을 투자하면 손해

그림 https://en.bitcoin.it/wiki/File:Blockchain.png

블록체인 분기 (계속)

- 각 블록체인은 모두 정당한 기록임
  - 다른 채굴자가 만들어서 서로 다른 거래가 들어 있고, 해쉬값도 다른 형태
- 분기의 수렴
  - 노드가 같은 높이인데 서로 다른 블록체인을 받으면 길이가 긴 것을 택함
  - 시간이 지나면서 짧은 블록체인은 점차 사라지게 됨
  - 실제로 깊이가 1인 분기는 1주에 1번꼴로 발생하나 2인 경우는 거의 없음
    - 버그(2013년 3월)를 제외하면 최장 분기는 4 블록 (2번 발생)



- 정산
  - 거래에는 영향이 없음 - 거래를 블록으로 묶을 때 서로 다르게 묶은 것일 뿐
  - 짧은 블록체인에 포함되었던 거래는 채굴자가 다시 검증
  - 코인베이스 거래는 영향을 받음 - 분기된 블록을 만든 채굴자 중 하나에게만 보상금 제공
    - 100 block maturation time
    - 비트코인에서는 100단계까지 늘어난 후에 실제 발급된 비트코인을 사용하도록 하라는 제안(규정?)을 하고 있음 - 10분에 하나씩 추가되면 100단계가 되는데 1000분 = 16시간 40분이 걸림. 즉 하루정도 후에 사용할 수 있게 됨.

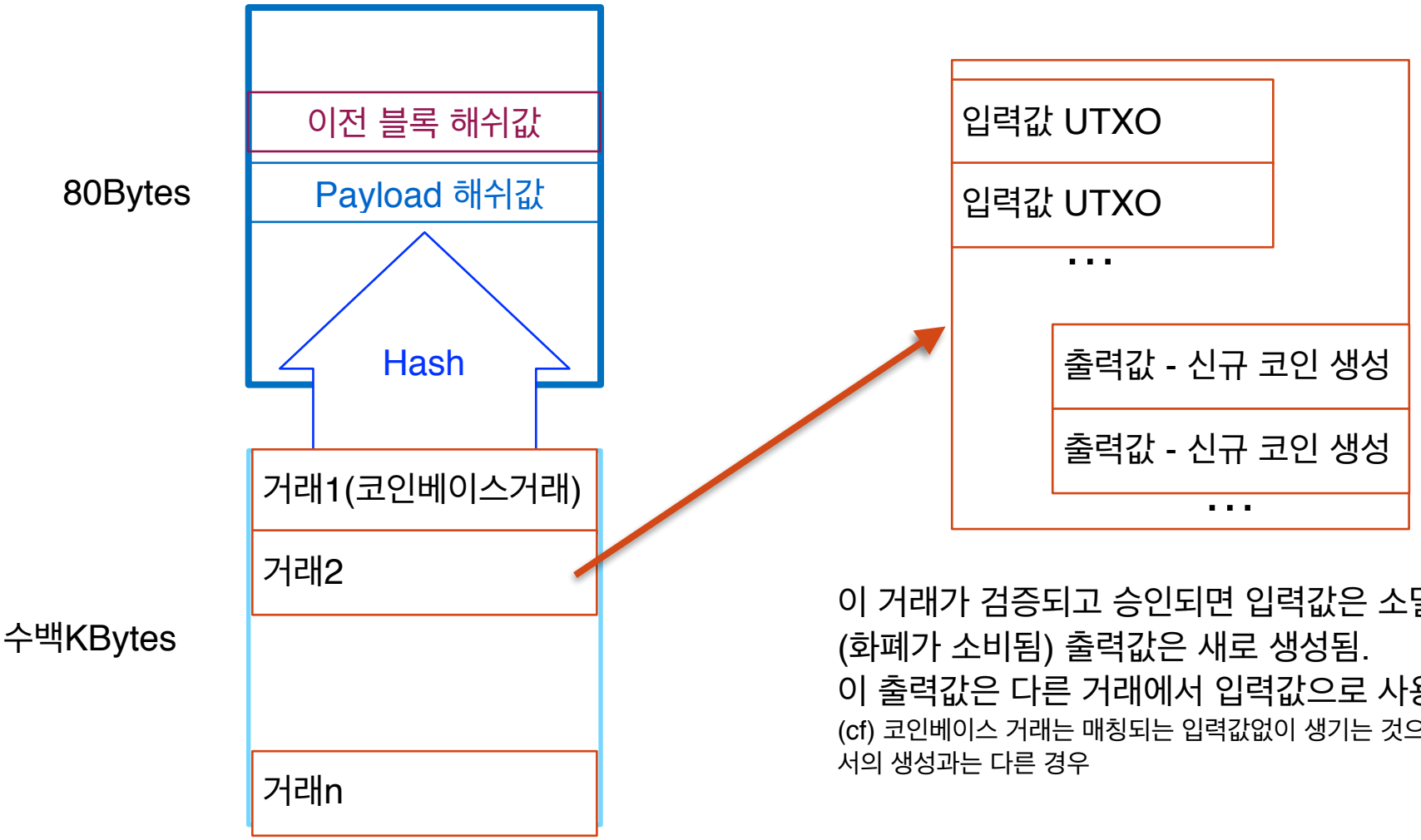
거래

- 블록체인의 payload에 거래 기록 보관
  - 전 세계에 오직 하나의 거래 장부(ledger)만 존재 (궁극적으로는)

- 각 비트코인은 거래내역이 아니라 실세계의 화폐(코인)와 유사
  - 화폐인데 액면가가 미리 정해진 것이 아니라 거래의 결과에 의해 결정됨
  - 예) 100원 내고 30원을 쓰고 70원을 거슬러 받으면
    - 내 100원이 사라지고
    - 새로 내 70원이 생기고
    - 상대방의 30원도 새로 생긴다

- 디지털 서명과 지급할 주소 표현은 비대칭키 이용

거래

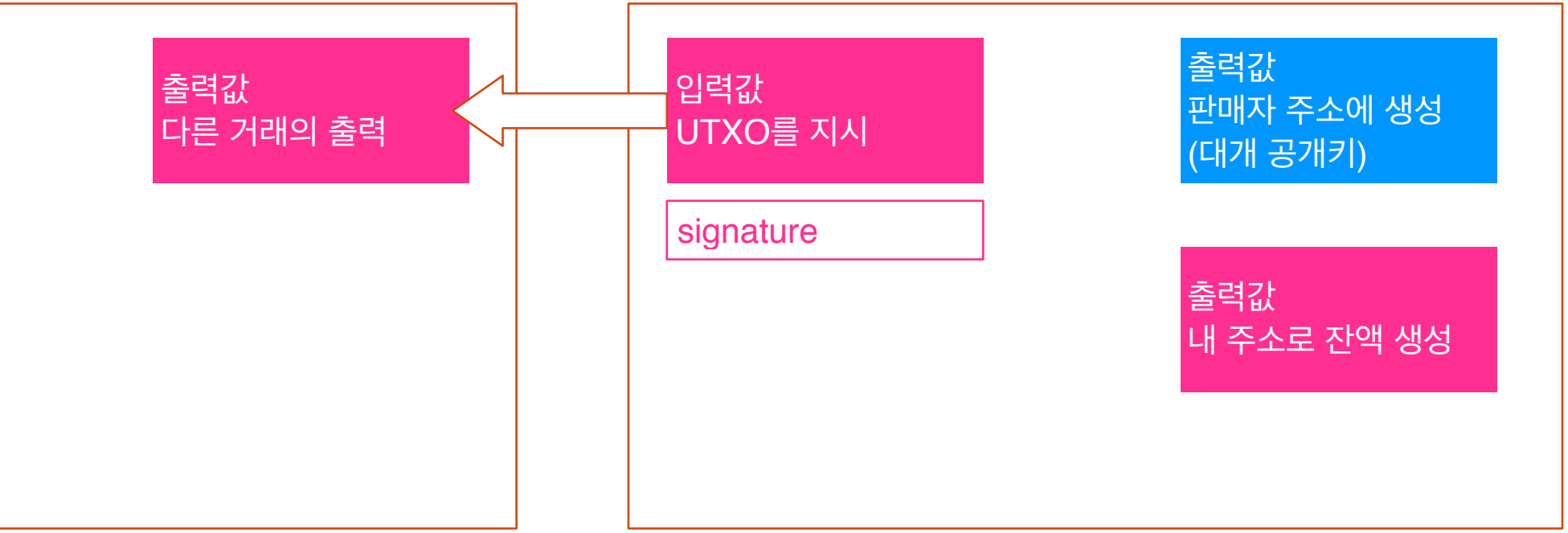


이 거래가 검증되고 승인되면 입력값은 소멸되고 (화폐가 소비됨) 출력값은 새로 생성됨.
이 출력값은 다른 거래에서 입력값으로 사용됨

(cf) 코인베이스 거래는 매칭되는 입력값없이 생기는 것으로 여기서의 생성과는 다른 경우

UTXO: Unspent Transaction Output
아직 소비되지 않고 내 지갑에 남아있는 비트코인 화폐

거래 세부 구성



출력값은 한번 쓰면 사라짐 → 검증 단순

수수료 = 총 입력값 - 총 출력값 (자동 지정)

수수료가 높으면 채굴에서 우선 순위가 높아짐

비대칭 키

두가지 키의 쌍으로 생성 (PrivateKey, PublicKey) 혹은 (개인키, 공유키)
개인키로 암호화한 것은 공유키로, 공유키로 암호화한 것은 개인키로 풀 수 있음
개인키는 자신이 보관하고 공유키는 공개함

내 공유키로 풀리면 내 개인키로 암호화한 것임

내 공유키로 암호화한 것은 내 개인키로만 풀 수 있음

거래 비교

	구매자	결과			비고
		판매자	구매자	수수료	
화폐	10,000	7,000	3,000	0	수수료 없음
비트코인	10,000	7,000	2,750	250	채굴 수수료(가변)
신용카드	10,000	7,000-a	3000-b	a+b	수수료

- 각 비트코인은 화폐와 유사
  - 사용자는 지갑이 있고 여기에 여러 주소(공개키) 보관
  - 한 주소에 여러 비트코인을 보관
  - 사용하면 폐기되고 대신 그 가치와 같은 여러 개의 비트코인이 새로 생김
- 거래는 신용카드와 유사
  - 각 거래에는 수수료를 정할 수 있음
  - 수수료는 이 거래를 검증해 준 제3자(채굴자)가 가져감
  - 높을 수록 빨리 채굴

비트코인의 거래 요약

- 거래 기록
  - 신뢰는 불특정 다수의 채굴(Proof of Work) 과정에서 온다
  - 검증은 각 채굴자의 개별적 검증
- 화폐와 대응
  - 화폐는 물리적 이동
  - 비트코인에서는 이동한 기록
- 거래 행위
  - 지불할 때 내가 가진 화폐를 주고 잔액을 받는다
  - 비트코인에서는 내가 가진 코인을 없애고 수신인의 새 코인을 만들고, 잔액만큼의 내 코인도 새로 만든다

이것이 성립하려면?

- 구매자가 사용하려는 비트코인에 대한 보증
- 거래에 대한 검증
- 이중거래 방지

- 위험과 효율의 균형을 제3자가 아닌 이용자가 선택

비트코인을 사용하는 거래 시나리오

이벤트

구매자(A): 비트코인 지불

↓ 수 초

판매자(B): 거래 전파 확인

↓ 수십 분

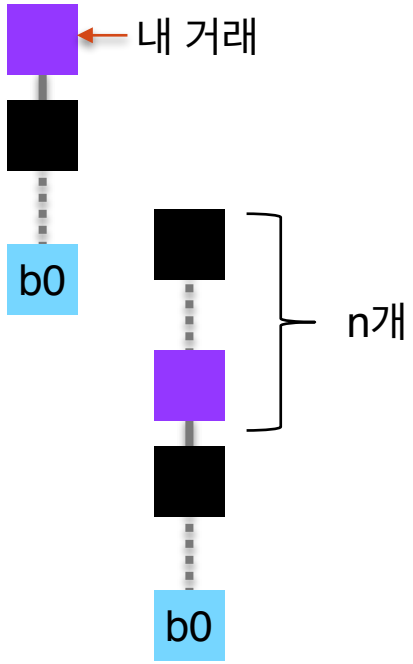
거래가 블록체인에 포함됨(채굴됨)

↓ 수 시간

충분한 깊이에 도달(다른 블록이 쌓임)

블록체인 상태

여러 노드에서
거래 유효성 검증



상품 제공 시점

B가 결정

소액 거래

↓

거액, 인터넷

수집된 거래의 노드별 독립 검증

- 모든 노드는 전달된 거래의 형식과 내용을 검증
  - 검증된 거래만 다른 노드에 전파
- 검증 내용
  - 형식
    - 구문, 합법적 필드값, 값의 범위
  - 거래 유효성
    - 거래의 입력이 Unspent TX Output (UTXO) 인가
    - 즉 사용하려는 코인이 유효한가
    - 입력값 ≥ 출력값 확인
  - 코인베이스 거래 확인
    - 코인베이스 출력을 사용하려면 최소 100블록 싸이클 후에 사용 가능 - 블록 분기 문제 대처

거래의 상태별 신뢰도

- 거래 전파 직후
  - 구매자가 거래를 전송하면 수초 이내에 전세계 대부분 노드에 전파
  - 이 거래는 아직 블록체인에 포함되지 않았음 - 승인 전 단계
  - 전파된 거래를 받은 노드는 각자 독립적으로 거래를 검증
    - 형식과 내용에 대한 약 20여 가지 체크리스트
  - 거래가 전파된다는 것은 다른 거래에서 같은 UTXO를 이용할 수 없게 되었다는 뜻
- 블록체인에 포함되었을 때 - 평균 10분 후(우선순위가 높은 경우)
- 내가 지정한 깊이에 도달했을 때
- 100 block maturation time rule
  - 코인베이스 거래

안전한 거래 규모

단순화한 모델로 확률을 계산한 예 (공격비용, 성공확률 등을 고려. 채굴비 =25BTC 경우)

불변의 절대적 수치는 아님

1 BTC=$431 01/16/2016 일 때

$10,000(≈23BTC) 규모의 거래도 큰 위험은 없음

전체의 40% 계산 능력을 지배해야 함

블록깊이

해쉬파워

q	1	2	3	4	5	6	7	8	9	10
2%	2400	42K	644K	9370K	≈∞	≈∞	≈∞	≈∞	≈∞	≈∞
4%	1150	10K	82K	615K	4437K	≈∞	≈∞	≈∞	≈∞	≈∞
6%	733	4722	25K	127K	626K	3018K	14M	≈∞	≈∞	≈∞
8%	525	2650	10K	42K	159K	588K	2144K	7749K	≈∞	≈∞
10%	400	1685	5741	18K	56K	168K	503K	1486K	4361K	12M
12%	316	1158	3391	9212	24K	62K	157K	396K	990K	2460K
14%	257	837	2172	5200	11K	27K	60K	132K	290K	632K
16%	212	628	1474	3178	6580	13K	26K	52K	102K	200K
18%	177	484	1043	2061	3901	7202	13K	23K	42K	74K
20%	150	380	763	1399	2453	4190	7039	11K	19K	31K
22%	127	303	571	983	1615	2582	4053	6288	9671	14K
24%	108	244	436	710	1103	1665	2467	3608	5229	7525
26%	92	198	337	523	775	1113	1570	2182	3005	4106
28%	78	161	263	392	556	766	1035	1377	1815	2372
30%	66	131	206	296	406	539	701	899	1141	1435
32%	56	106	162	225	299	385	485	602	740	901
34%	47	86	127	172	221	277	340	411	491	582
36%	38	69	99	130	164	200	240	283	331	383
38%	31	54	76	98	121	144	169	196	224	254
40%	25	42	57	72	87	102	118	134	151	168
42%	19	31	41	51	61	70	80	90	99	109
44%	13	21	28	34	40	46	51	57	62	68
46%	8	13	17	21	24	27	30	32	35	38
48%	4	6	8	9	10	12	13	14	15	16
50%	0	0	0	0	0	0	0	0	0	0

Table 2: The maximal safe transaction value, in BTC, as a function of the attacker's hashrate q and the number of confirmations n.

BTC: 비트코인 단위
작은 단위로 satoshi도 있음
1BTC = 100,000,000 satoshi

Analysis of hashrate-based double-spending http://arxiv.org/pdf/1402.2009.pdf

블록의 확산 요인

- 각 노드가 자신의 이익을 극대화하려는 활동에 의해 전파되어 전체 블록체인이 동기화
  - 분산, 독립, 효율
- 노드 작업의 우선 순위
  - 외부에서 전달된 새 블록 검증과 전파
  - 다음 블록 채굴
  - 이것이 자신의 이익을 위해 가장 유리한 선택임
    - 새 블록 검증하지 않으면 -> 다른 노드에 의해 검증되므로 의미없는 노력의 낭비
    - 전파하지 않고 계속 채굴하면 -> 어차피 전파되고 있음. 최악의 경우 나만 최신 블록에 대한 정보에 뒤져서 손해 볼 수 있음. (예. 이미 채굴되고 검증된 과거 블록에 대한 채굴)
- 절차
  - 채굴이 성공하면 즉시 모든 이웃 노드에게 해당 블록 전송
  - 각 노드는 새 블록을 전송받아 검증한 후 전파
  - 각 노드는 새 블록을 자신의 블록체인 복사본에 추가
  - 각 노드는 다음번 블록에 대한 채굴 시작
- 대략 수 초 내에 전세계로 퍼짐

이중 거래

- 소액 거래는 편의상 거래가 블록체인에 포함되기 전에 완료
  - 판매자의 재량이나 커피살 때 10분 이상 기다린 후에 서비스받으려고 하지 않을 것임
  - 보통 거래가 전파되고 있는 것만 확인하고 정상 거래로 취급
    - 거래가 전파된다는 것은 거래 내역에 대한 검증은 마쳤다는 의미
    - 블록체인에 포함되고 그 뒤에 다른 블록이 쌓인다는 것은 점점 더 그 거래가 무효화되기 어려워진다는 의미
- 규모가 큰 거래는 일정한 깊이 이상 블록체인이 쌓였을 때 승인
  - 깊이의 결정은 미리 정해진 것이 아니라 거래 당사자가 정함
  - 유연성, 거래별로 따로 계산하는 자동화 가능
  - 충분한 깊이에 이르면 채굴된 블록의 proof-of-work가 축적되어 신뢰 확보
- 전세계 채굴 계산 능력의 51%를 확보하면 조작 가능

비트코인의 진화

노드의 전문화

- Full blockchain node는 수십 GB 블록을 저장
- 모든 블록을 저장하지 않는 노드
  - 거래만 하는 Lightweight Wallet
  - 채굴만 하는 채굴노드
- 이런 노드를 블록저장 노드에 연결시키는 게이트웨이 노드
  - Pool server
  - Stratum server

- 채굴 집단의 탄생
  - https://blockchain.info/blocks

위협 - 비트코인

- 양자컴퓨터
- Full 노드 수
- 거래 건수 제약
- 중국의 채굴 능력 확대
  - 집중화에 의한 집단 행동 위험
- 채굴풀 - 집단 채굴
  - 국가 혹은 집단의 공격
  - 바이러스를 통한 분산채굴
- 지갑 분실, 도난, 해킹

BTCC Deploys 100 Full Bitcoin Nodes Across Five Continents

Source: BTCC

PRESS RELEASE

CN, December 26, 2015 at 12:14 GMT

Leading Bitcoin Platform Becomes First Exchange and Mining Pool To Donate Nodes

BTCC today deployed 100 full bitcoin nodes across five continents to support the bitcoin network. Full bitcoin nodes enforce the rules of the bitcoin network by serving a full copy of the bitcoin blockchain and validating blocks and transactions.

BTCC is the first bitcoin exchange and first mining pool to donate and deploy full bitcoin nodes for the maintenance of the bitcoin network.

Press Contact

Name
Tendai Musakwa

Email address
press@btcc.com

Phone number
+86 (21) 5489-4951

Bitcoin has 'failed,' says one of its most prominent developers

Rob Price
Jan. 15, 2016, 6:14 AM · 21,349 · 22

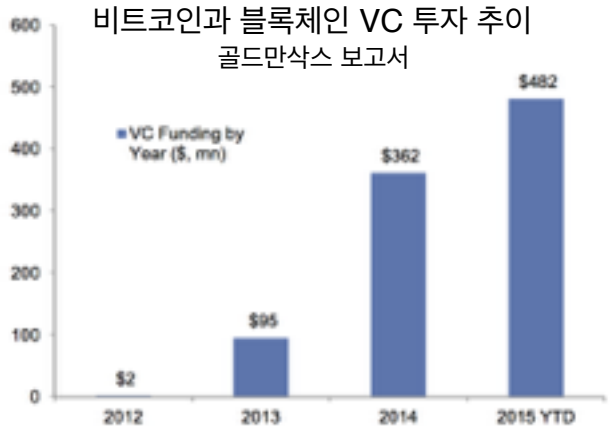
FACEBOOK · LINKEDIN · TWITTER · EMAIL · PRINT

A disillusioned high-profile developer has quit bitcoin — claiming in an explosive blog post that the "experiment ... has failed."

Mike Hearn has been a prominent part of the controversial digital

기회 - 블록체인

- **R3CEV**
  - JP Morgan Chase, Goldman Sachs, Barclays
  - 제3자가 관여하는 분산 기록 관리
- **Open Ledger Project**
  - IBM, Intel, JP Morgan, Linux Foundation, etc.
  - Redefining supply chains, contracts, etc.
- **Ethereum**
  - Non-profit
  - Smart contracts
- **ADEPT**
  - IBM, Samsung
  - IoT 장치 기록



주요 참고 자료

- 비트코인, 블록체인과 금융의 혁신, 최은실 외 옮김, 2015. (원본은 Mastering Bitcoin: Unlocking Digital Cryptocurrencies, A. M. Antonopoulos, 2015. chimera.labs.oreilly.com/books/1234000001802/index.html)
- Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, bitcoin.org/bitcoin.pdf, 2008.
- Analysis of hashrate-based double-spending, M. Rosenfeld, arxiv.org/pdf/1402.2009.pdf, 2012.
- Hashcash - A Denial of Service Counter-Measure, www.hashcash.org/papers/hashcash.pdf, 2002.
- Have a Snack, Pay with Bitcoins, T. Bamert et al., 2013. www.tik.ee.ethz.ch/file/848064fa2e80f88a57aef43d7d5956c6/P2P2013_093.pdf
- Themes, Dreams and Flying Machines, Goldman Sachs, 2015. www.goldmansachs.com/our-thinking/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf
- www.wikipedia.org
- Blockchain info, blockchain.info
- Bitcoin Wiki, en.bitcoin.it/wiki/Main_Page
- CoinDesk, www.coindesk.com
- HashCash, www.hashcash.org.