블록체인

- 작업 증명 방식의 블록체인에 대하여-

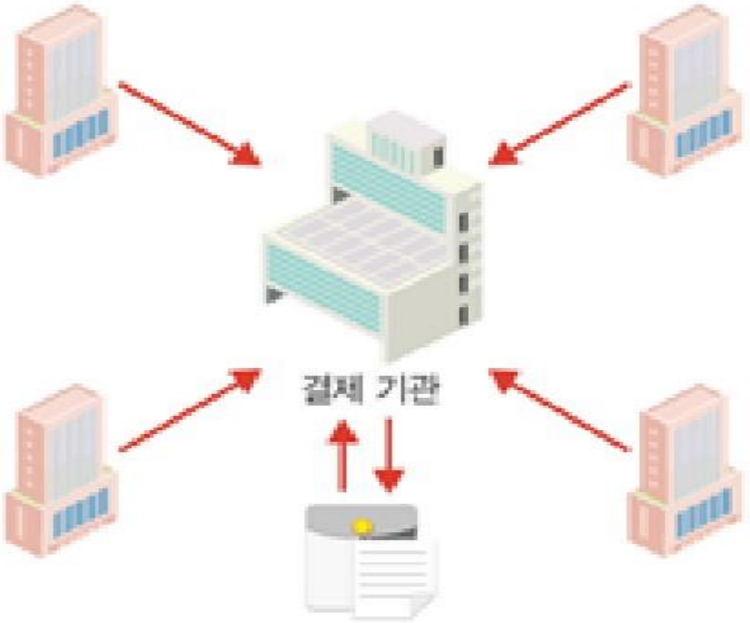
안태진(taejin@codecure.smuc.ac.kr)

상명대학교 보안동아리 CodeCure

목 차

블록체인의 탄생

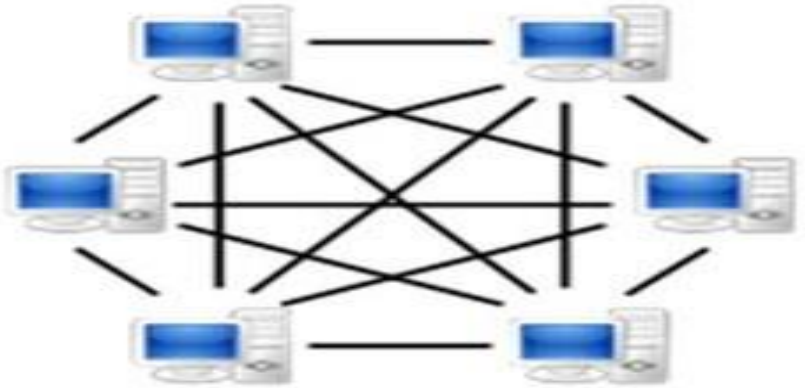
- 블록체인 이전 화폐시스템 -> 중앙화 시스템
  - 중앙화 시스템의 문제점 존재
    - e.g., 중앙화 시스템, 중앙기관 신뢰 문제, 유지 관리비
      - 중앙기관 신뢰 문제: 중앙기관 해킹, 중앙기관이 기록 조작



중앙화된 장부

블록체인의 탄생

- P2P 시스템으로 탈 중앙화 된 화폐 시스템(<- 가상화폐) 구축
  - P2P : Peer-to-Peer의 약자, 컴퓨터들이 중앙 요소와 통신 하지 않고 데이터를 주고 받는 시스템
    - e.g., 토렌트
  - 장점: 수수료, 유지 관리비, 해킹 위험 감소



블록체인의 탄생

- P2P 기반 화폐시스템의 취약성 존재
  - 합의 불가 문제
    - 다른 사용자들을 믿을 수 없음
  - 이중 지불
    - 거래 내역 A가 퍼지기 전에 거래 내역 B생성

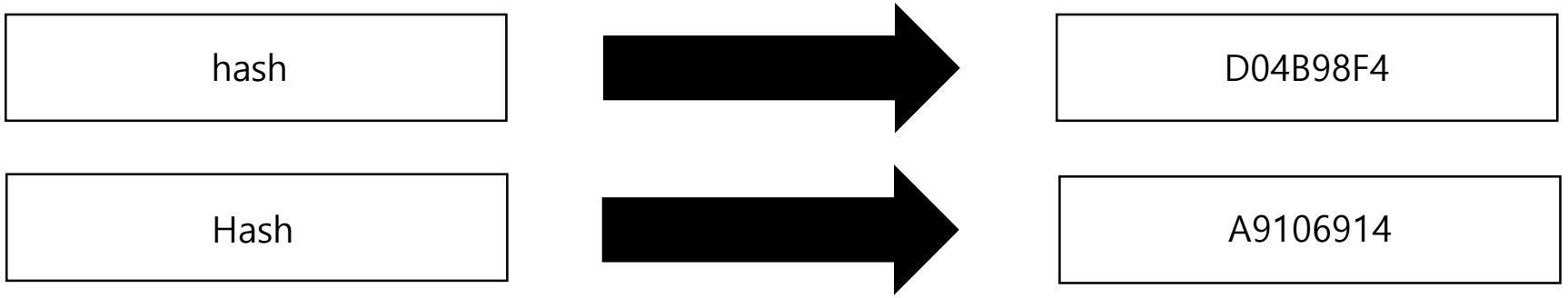
블록체인의 탄생

- P2P 시스템의 취약성 보완 위해 블록체인 탄생
- 합의 불가 문제 -> ‘작업 증명’, ‘지분 증명’ 등으로 보완
- 이중 지불 문제 -> ‘분산 원장 시스템’으로 보완
  - 원장: 거래를 계정별로 기록, 계산 하는 장부

목 차

블록체인에 대하여 - 주요 용어

- 해시 함수 (Hash Function)
  - 임의의 길이 데이터를 정해진 크기의 데이터로 변환
- 특징
  - 같은 값이 입력되면 항상 같은 값 출력
  - 한 글자만 바뀌어도 다른 값 출력
    - 해시 값만 보고 원본 유추 불가능에 가까움



블록체인에 대하여 - 주요 용어

- 난스 (Nonce)
  - Nonce(네이버 사전): ‘특정 상황에서만 쓰기 위해 만든’
  - 즉, 채굴에 쓰이기 위해 만들어진 임의의 변수
    - 채굴: 블록체인에서 블록을 생성하는 일
      - 블록: 데이터들의 모음집

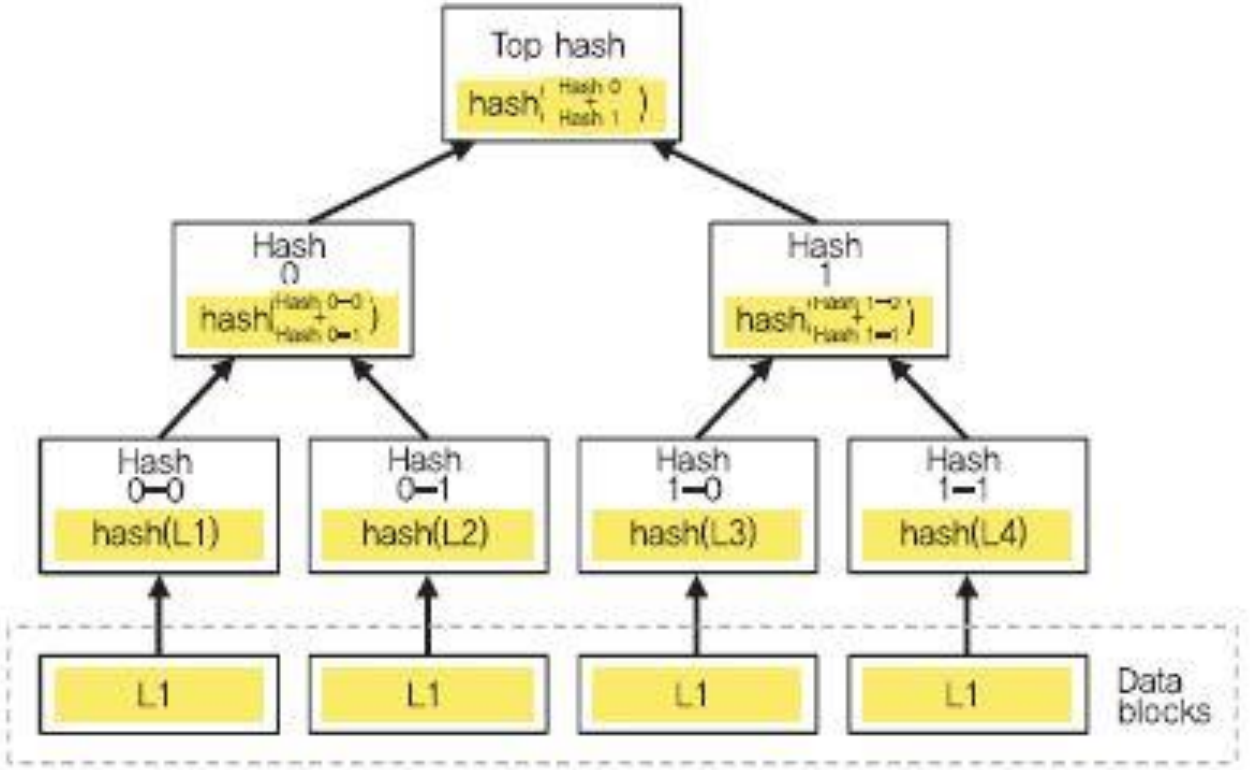
블록체인에 대하여 - 주요 용어

- 해시 퍼즐 (Hash Puzzle)
  - 해시 함수의 특징을 이용한 퍼즐
  - 단순 계산이 아니라 일일이 대입하여 해결
  - (조건: 해시 값 앞자리 3자리가 0이 되게하라)

난스	데이터 + 난스	해시 값
0	Hello World! 0	4EE4B774
1	Hello World! 1	3345B9A3
.	.	.
.	.	.
.	.	.
613	Hello World! 613	E861901E
614	Hello World! 614	00068A3C

블록체인에 대하여 - 주요 용어

- 머클 트리 (Merkle Tree)
  - 거래 내역들을 요약하는 방법
  - 마지막 남은 해시 값이 '머클 트리 루트'



목 차

블록체인에 대하여 - 간단 정의

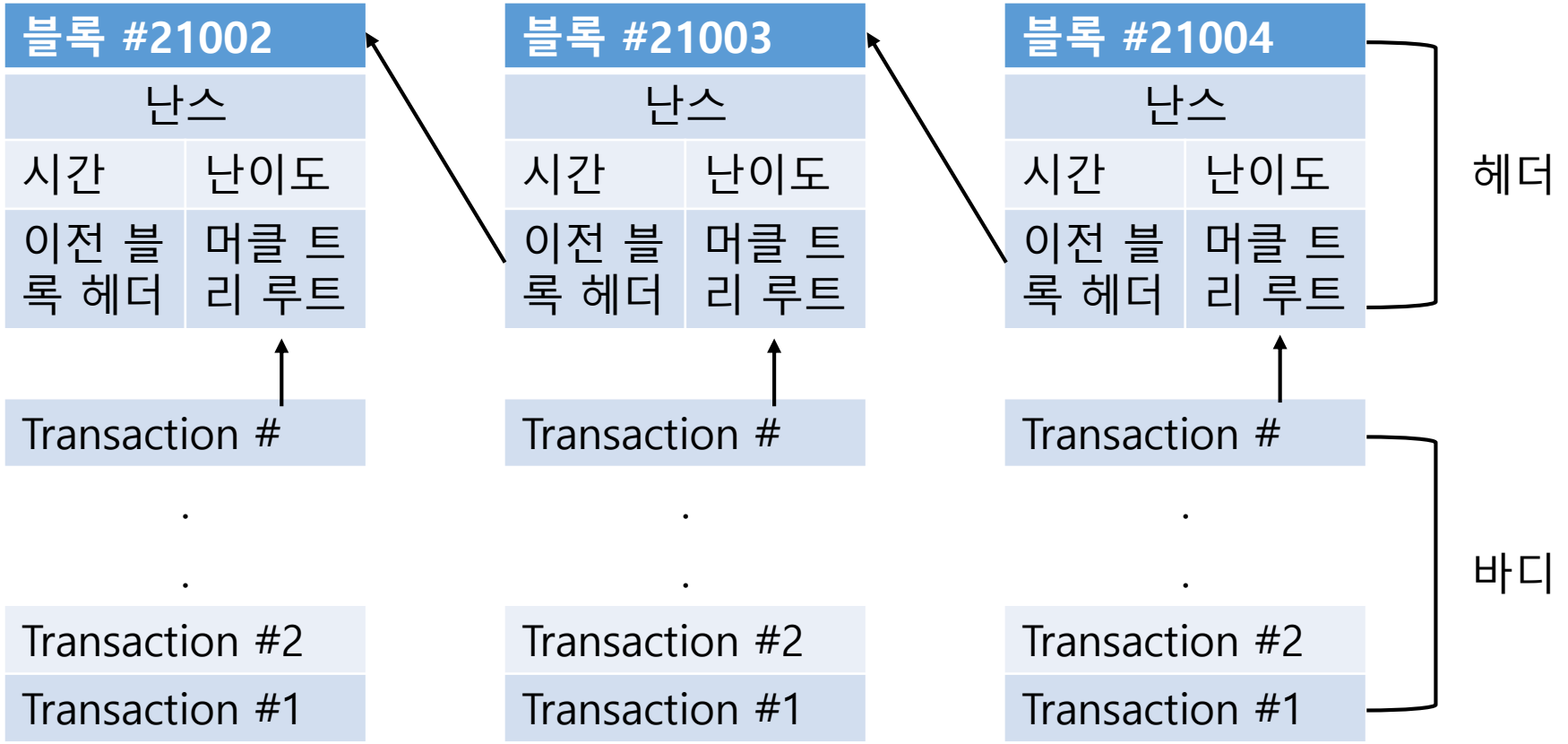
- 블록체인: 네트워크에서 일어나는 거래들이 암호화 되어 구성원간 공유되는 시스템
- P2P 시스템으로 구성원간 일어나는 거래 정보들이 모든 사용자에게 공유
  - 거래 정보: 트랜잭션(Transaction)
- 각 블록들은 앞 블록의 정보를 가지고 있음으로서 체인화

목 차

- 블록체인의 탄생
- 블록체인에 대하여
  - 주요 용어
  - 간단 정의
  - 작동 원리
- 블록체인의 활용

블록체인에 대하여 - 작동 원리

- 1. 각 컴퓨터들은 블록을 생성 (채굴)
  - 채굴은 블록의 헤더를 해싱하는 일
  - 난스 값 변경해가며 난이도에 맞는 해시 값 계산



블록체인에 대하여 - 작동 원리

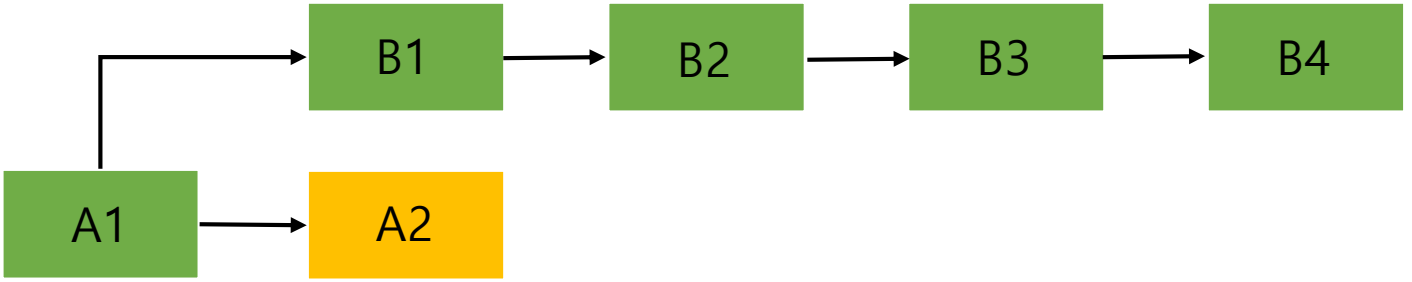
- 2. 사용자들은 블록이 올바르게 생성됐는지 확인
  - 블록의 검증
    - 블록이 생성 되면 컴퓨터들은 올바르게 생성됐는지 확인

- 3. 올바르게 생성된 블록은 기존의 블록체인의 연결, 그렇지 않은 블록 파기
  - 파기된 블록의 거래내역들은 다른 블록에 포함, 다시 블록화

블록체인에 대하여 - 작동 원리

- 블록의 분기
  - 블록의 분기시 가장 길게 이어진 블록 따라 만듬
    - 블록의 분기: 블록이 동시에 생성된 경우, fork라고도 함

- 고아 블록: 분기시 선택되지 못한 블록
  - 고아 블록에 포함된 거래 내역들은 다른 블록에 포함, 다시 블록화 됨



블록체인에 대하여 - 작동 원리

- 합의 불가 -> 작업증명, 지분증명 등으로 해결
  - 작업 증명(PoW)
    - 모든 참여자들이 채굴을 하여 블록들 생성 가장 빨리 블록을 만든 참여자에게 보상 제공
  - 지분 증명(PoS)
    - 가장 지분을 많이 가지고 있는 참여자에게 블록 생성 기회 주어짐

블록체인에 대하여 - 작동 원리

- 이중 지불 -> 분산 원장 시스템으로 보완

- 각각의 컴퓨터들이 원장 보유, 이중 지불 있을시에 발견
  - 의심되는 거래내역 컴퓨터들과 원장 비교, 다수의 원장을 따름

목 차

- 블록체인의 탄생
- 블록체인에 대하여
  - 주요 용어
  - 간단 정의
  - 작동 원리
- 블록체인의 활용

블록체인의 활용

- 1. 블록체인 + 금융
  - 수수료 감소, 금융 데이터 저장 용이, 가상화폐 사용
    - e.g., 골드만삭스, 비트코인, 은행의 대출
- 2. 블록체인 + 정부
  - 정부의 할 일의 디지털 화, 정부 비밀 문서 해킹 위험 감소
    - e.g., 에스토니아, 온두라스, 영국
- 3. 블록체인 + 판권
  - 판권을 블록체인에 도입 -> 저작권 귀속 쉽게 확인, 저작권 위변조 x, 판매자와 사용자 직접 거래 수익 증가
    - e.g., Blockai, 이모젠 힙, Copytrack

감사합니다!