블록체인 특강

빅픽처랩(주)
안 휘

서울특별시 SEOUL METROPOLITAN GOVERNMENT

kaibc 한국에이아이블록체인융합원 Korea AI Blockchain Convergence

강사 소개

- **블록체인기반 소프트웨어 시스템 설계 및 개발 전문가**
- **경력**
  - 빅픽처랩(주), CTO, 2018.5 ~ 현재
  - 주식회사 네브마인, CEO, 2016 ~ 2018
- **학력**
  - KAIST, 전산학부, 박사 수료, 2013
  - CMU, MSIT-SE, 석사, 2012
  - KAIST, 전산학과, 학사, 2010
- **대표 프로젝트**
  - **잇닷 & trust-chain**: 익명기반 오피니언보드 솔루션
  - **it-chain**: 오픈소스 블록체인 엔진

안 휘
E. hwi.ahn@bigpicturelabs.io
M. 010-2695-0232

목 차

1

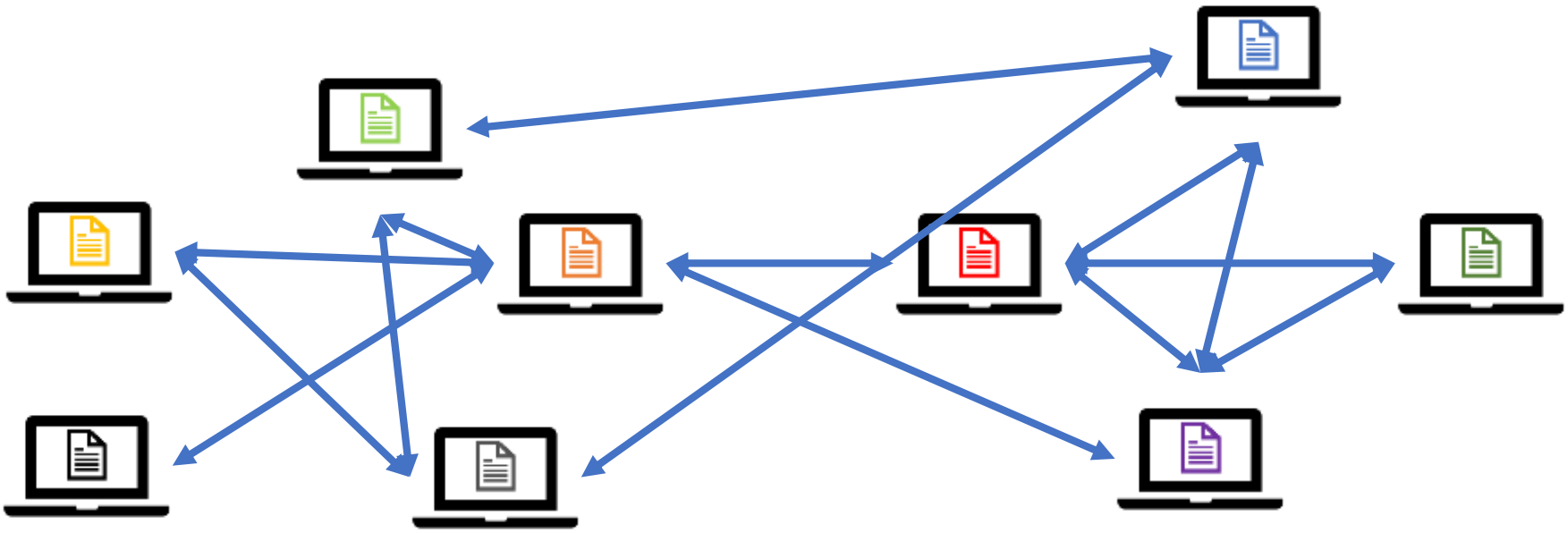
인터넷과 4차 산업혁명

인터넷이란 무엇인가
4차 산업혁명이란 무엇인가
왜 블록체인이 4차 산업혁명의 기반 기술 중 하나인가

목차

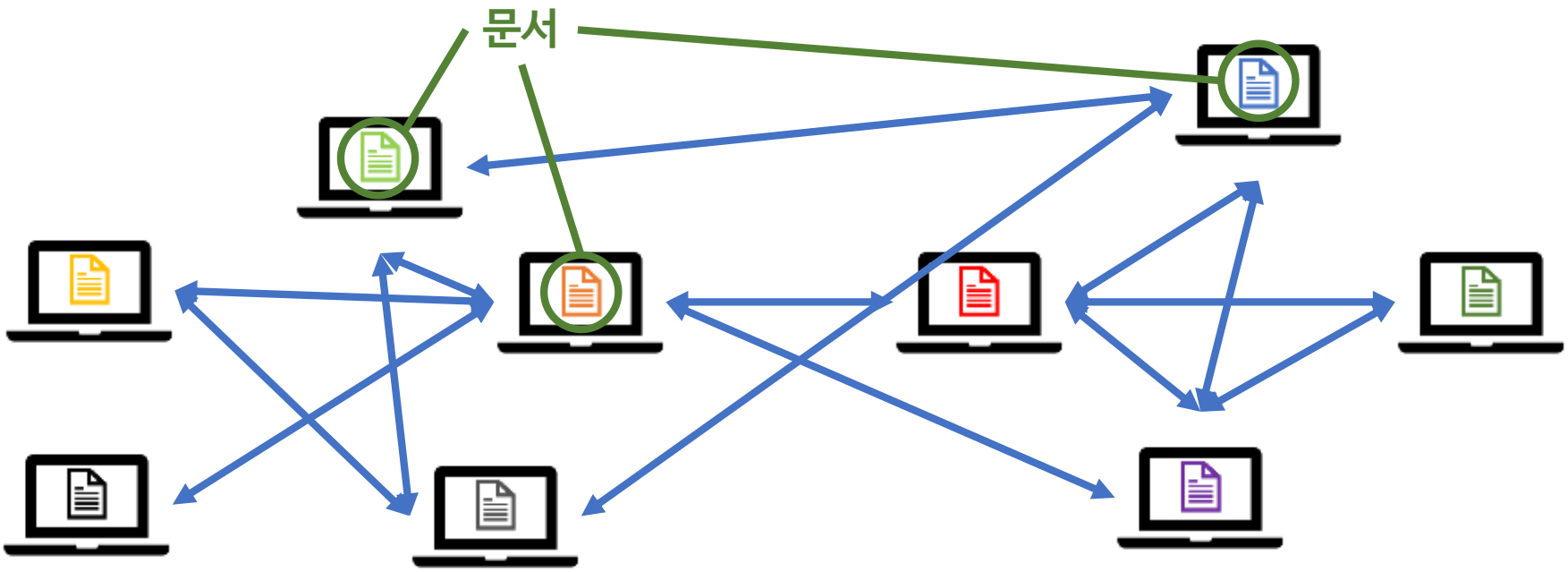
1. 인터넷과 웹 서비스

- **네트워크**
  - 컴퓨터들이 연결되어 있는 것
  - 왜? 서로의 **정보를 공유**하기 위해
- **인터넷: 네트워크의 네트워크**
  - 컴퓨터들 사이의 모든 네트워크를 연결한 거대한 네트워크



1. 인터넷과 월드 와이드 웹

- **월드 와이드 웹(World Wide Web, WWW)**
  - 줄여서 “웹”
  - 가장 대중적인 인터넷 기반 정보 공유 공간
  - 정보는 HTML로 작성된 문서로 공유됨

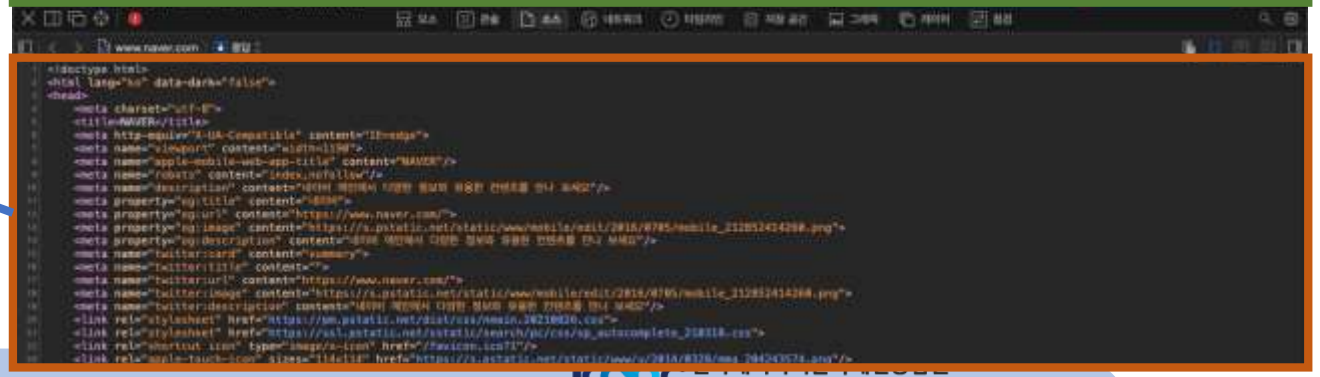


1. 인터넷과 월드 와이드 웹

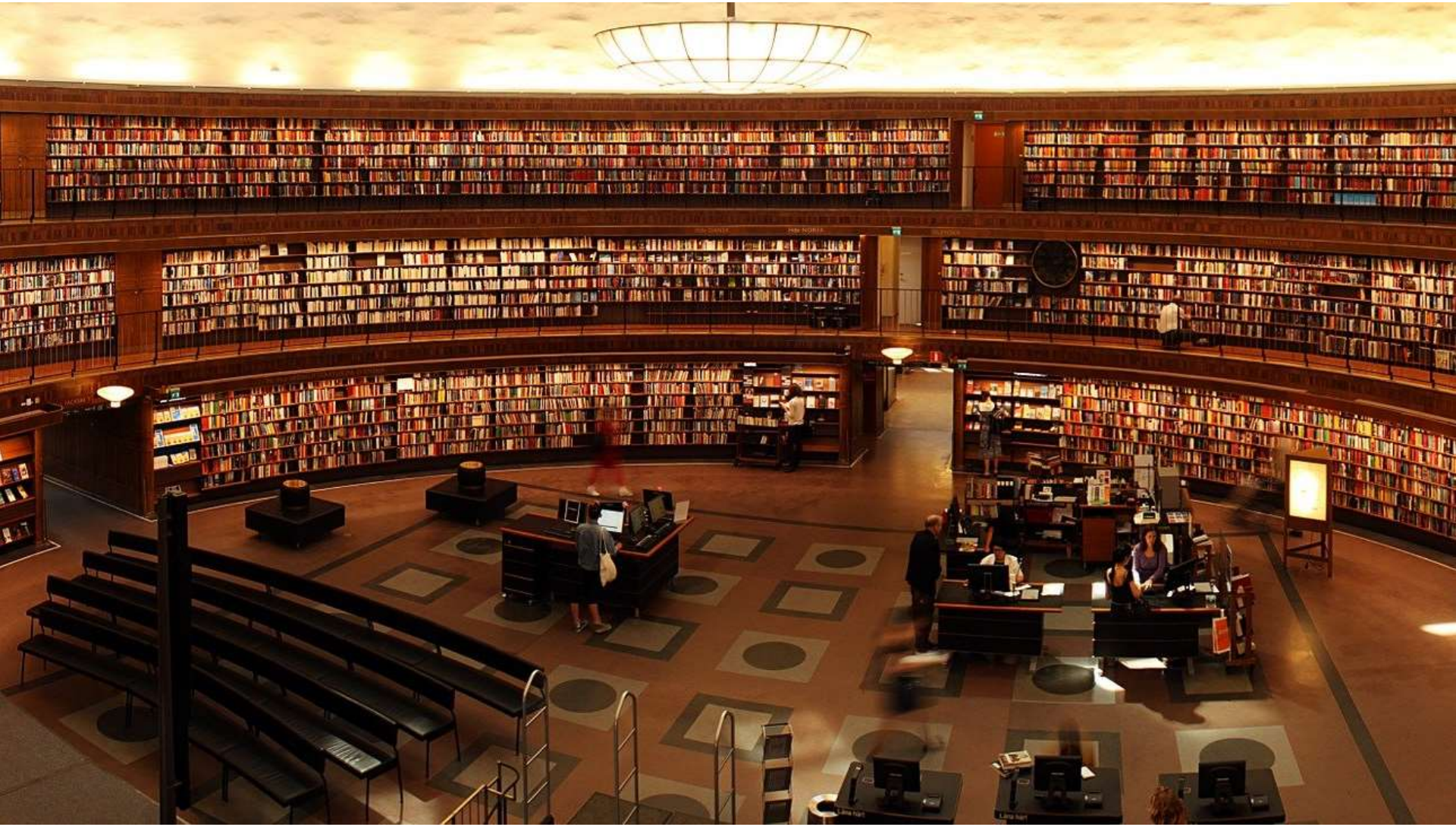
- **월드 와이드 웹(World Wide Web, WWW)**
  - 줄여서 “웹”
  - 가장 대중적인 인터넷 기반 정보 공유 공간
  - 정보는 HTML로 작성된 문서로 공유되고 “웹 브라우저”를 통해 봄

웹 브라우저로 본 문서의 모습

HTML로 작성된 문서



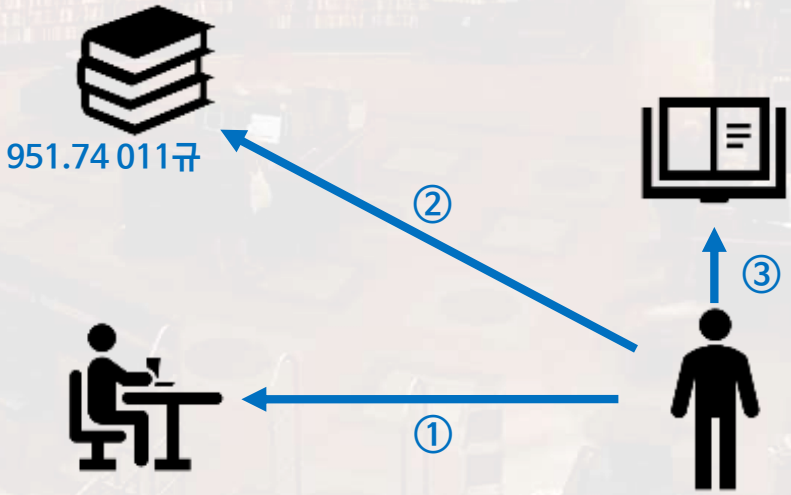
2. 월드 와이드 웹: 거대한 도서관



2. 월드 와이드 웹: 거대한 도서관

- **여러분은 책을 보러 왔습니다. 아는 건 책 제목 뿐입니다.**

1. 사서에게 찾아가 책 분류번호(“951.74 011규”)를 물어봅니다.
2. 책 분류 번호를 가지고 실제 책이 있는 위치로 가서 책을 얻습니다.
3. 책을 처음 펼치면, 목차 또는 색인을 통해, 원하는 페이지를 찾아 읽습니다.
   - 만족할 때까지 3번 행위를 반복합니다.
4. 읽을 만치 읽었으면, 이제 집에 갑니다.



2. 월드 와이드 웹: 거대한 도서관

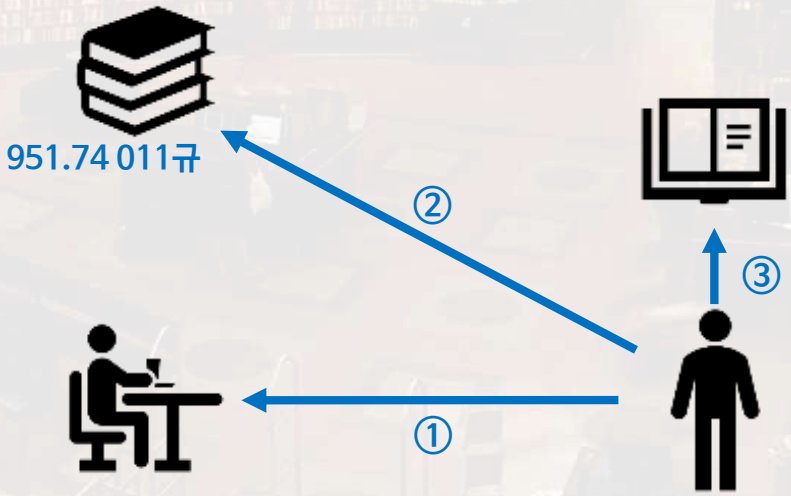
- **인터넷으로 바꿔봅시다**
  - 여러분: 웹 브라우저 (~~익스플로러~~, 크롬, 파이어폭스, 사파리 등)
  - 사서: DNS 서버

  - 책: 웹 사이트
    - 실제로 웹 사이트는 책과 마찬가지로 수백, 수천 개의 “문서”의 모음입니다
  - 목차 또는 색인: index.html
  - 페이지: 웹사이트를 구성하는 “문서”
    - 여러분들이 브라우저를 통해 보는 것이 바로 이 “문서”입니다

2. 월드 와이드 웹: 거대한 도서관

- **여러분은 웹사이트를 보러 왔습니다. 아는 건 인터넷 주소 뿐입니다.**

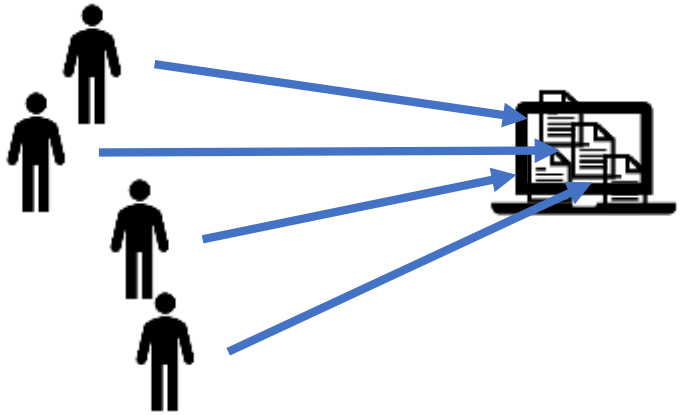
1. DNS 서버에게 찾아가 실제 인터넷주소(“143.248.xxx.xxx”)를 물어봅니다.
2. 실제 인터넷 주소를 가지고 실제 웹사이트가 있는 위치로 가서 웹사이트을 얻습니다.
3. 웹사이트가 처음 열리면, index.html을 통해, 원하는 페이지를 찾아 읽습니다.
   - 만족할 때까지 3번 행위를 반복합니다.
4. 읽을 만치 읽었으면, 이제 끕니다.



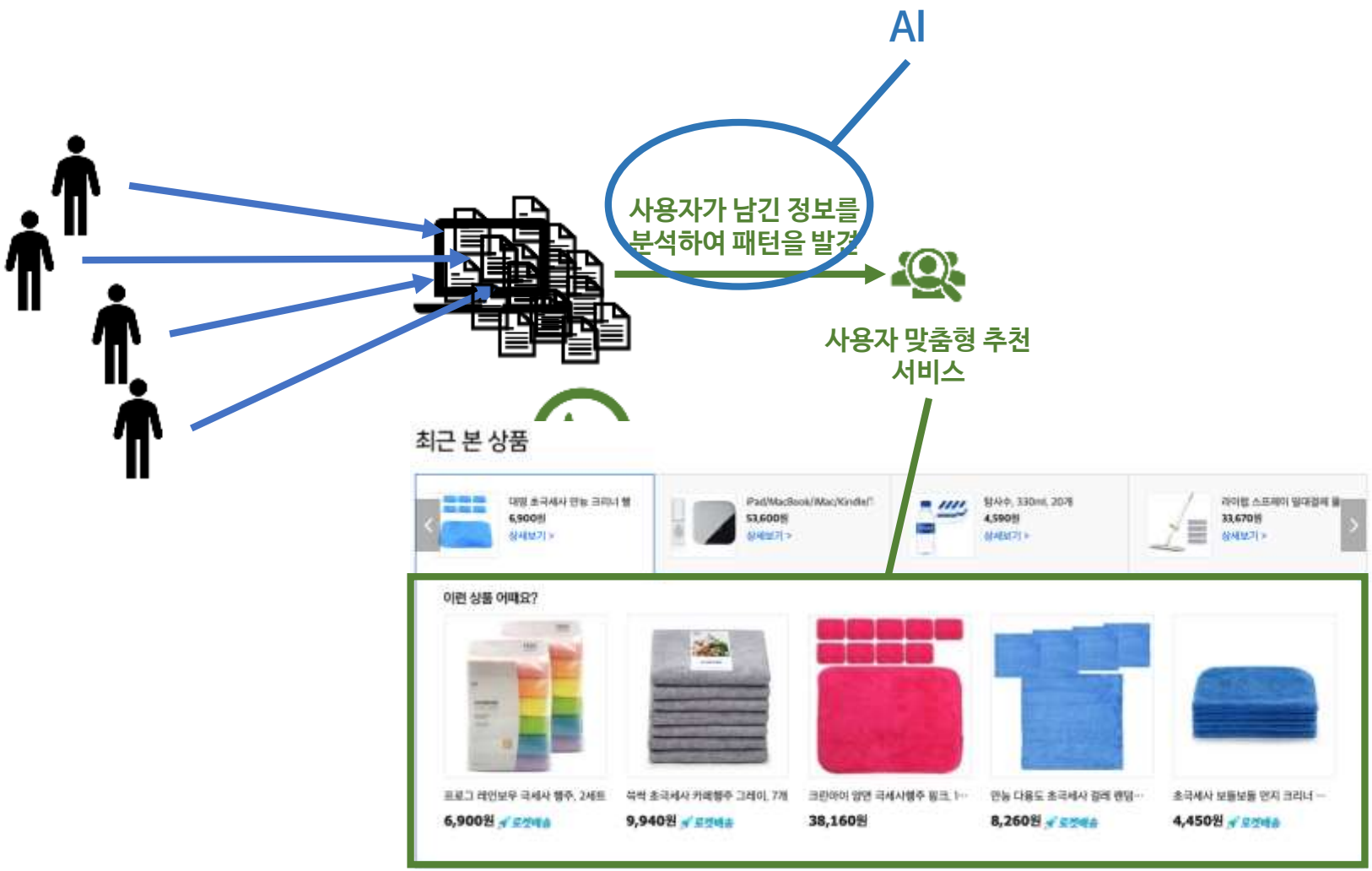
2. 월드 와이드 웹: 거대한 도서관

- **웹 1.0**
  - 1994년 ~ 2004년
  - 텍스트 중심 (진짜 책 같았음)
  - 단방향 (사용자는 단순히 읽기만 함)

- **웹 2.0**
  - 사용자가 정보를 생산
  - 블로그, 댓글, 게시판, …
  - 독자가 책을 써주는 셈
  - 웹 사이트에서 웹 “애플리케이션”으로 진화



3. 4차 산업혁명


AI
사용자가 남긴 정보를
분석하여 패턴을 발견
사용자 맞춤형 추천
서비스
최근 본 상품
이런 상품 어때요?
6,900원
9,940원
38,160원
8,260원
4,450원

3. 4차 산업혁명

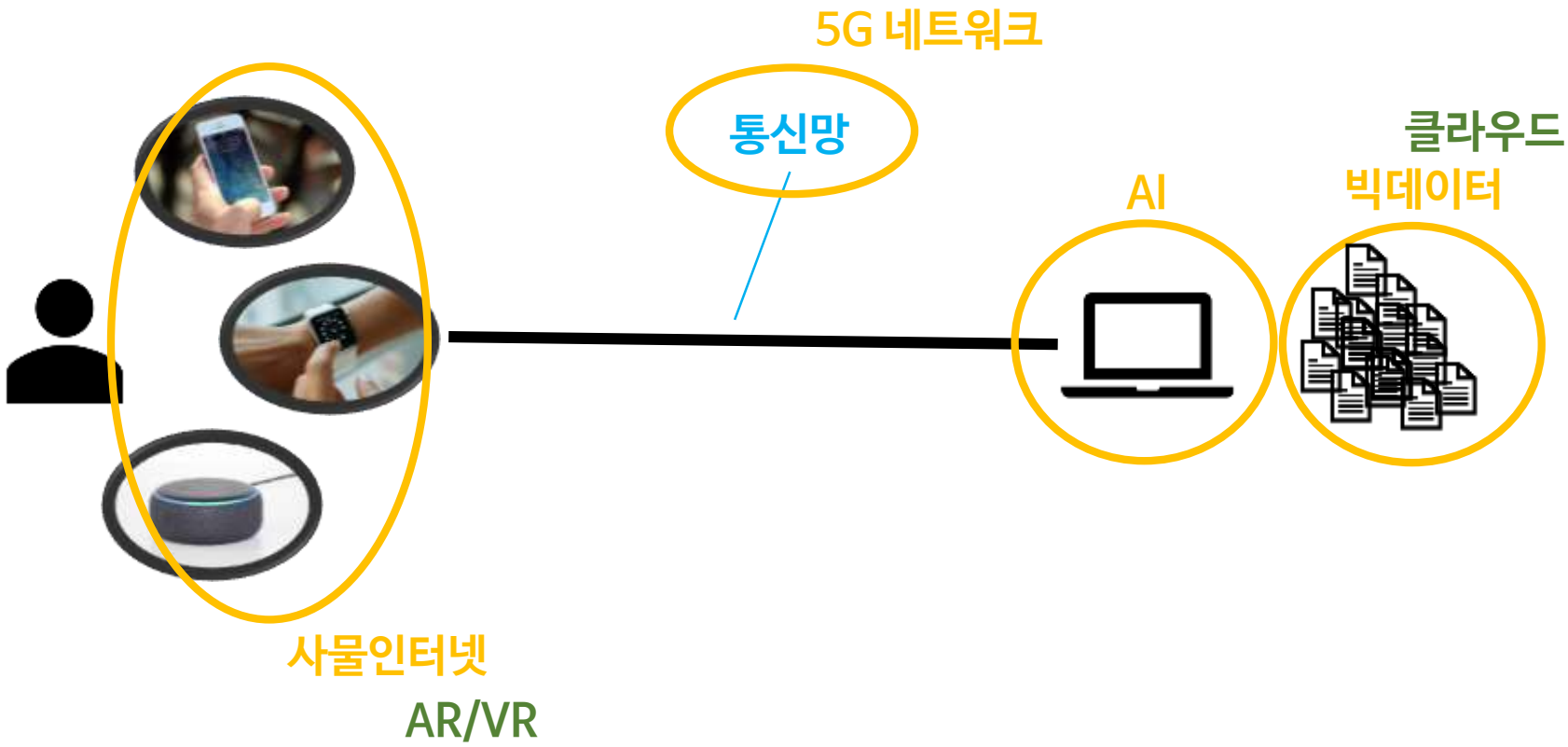
- **인공지능**
  - 수많은 정보로부터 특정 패턴을 찾아 주는 것
    - 수많은 셀카들로부터 사람 얼굴을 식별하는 패턴을 발견함
      - (그 동안 구글 포토가 공짜였던 이유)
    - 수많은 “좋아요” 기록을 통해, 사용자가 구입할만한 상품을 식별하는 패턴을 발견함
      - (인스타그램, 페이스북의 타겟 광고가 정확한 이유)

3. 4차 산업혁명

- **인공지능**
  - 무엇을 가능하게 해주는데? – 걸을 수 있습니다

3. 4차 산업혁명

- 4차 산업혁명 시대의 주요 기술

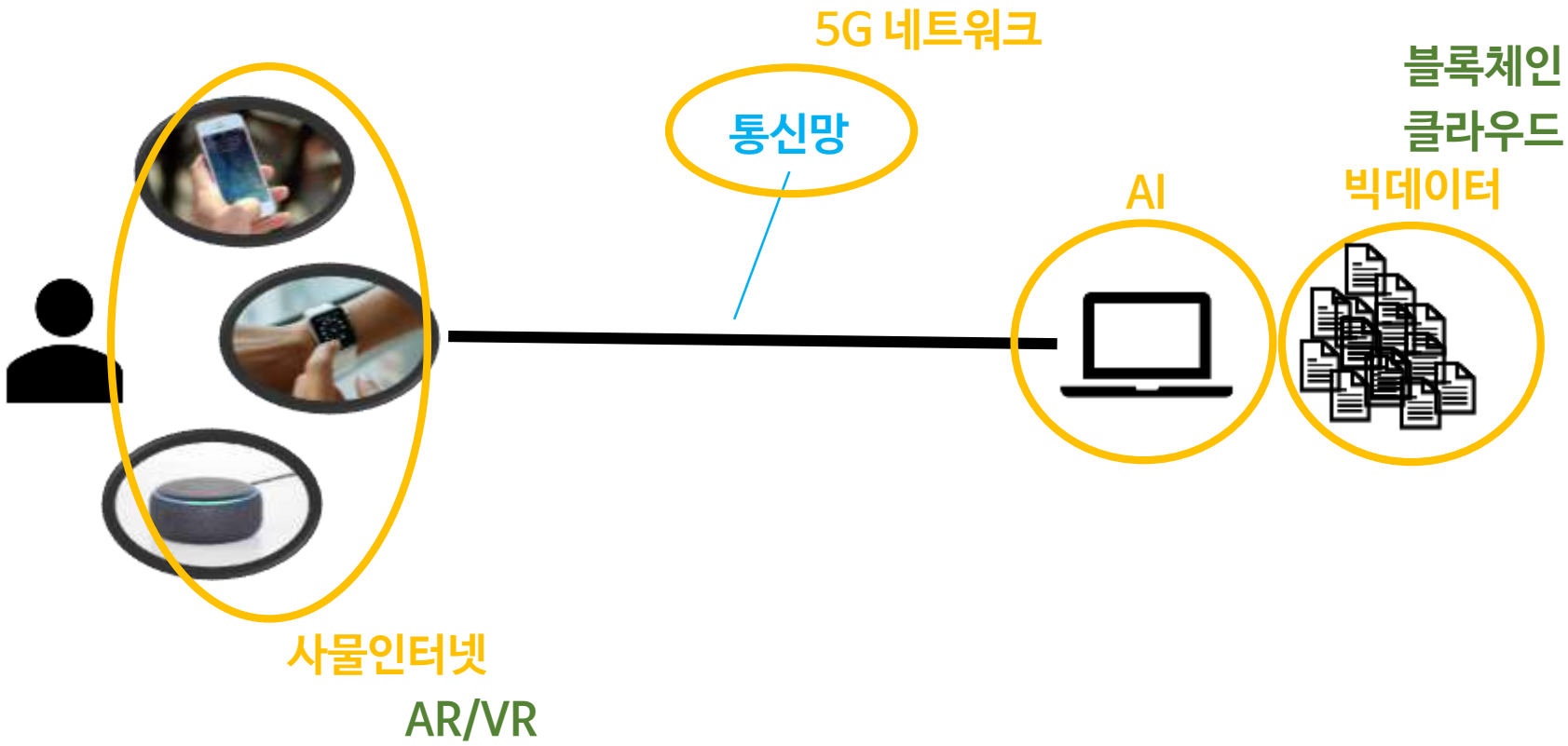


3. 4차 산업혁명

- 4차 산업혁명 시대의 핵심 기술

4. 4차 산업혁명 속 블록체인

- 4차 산업혁명 시대의 주요 기술



4. 4차 산업혁명 속 블록체인

- **4차 산업혁명**
  - 모든 정보를 너도나도 닥치는 대로 많이 모아야 이기는 게임

카카오

네이버

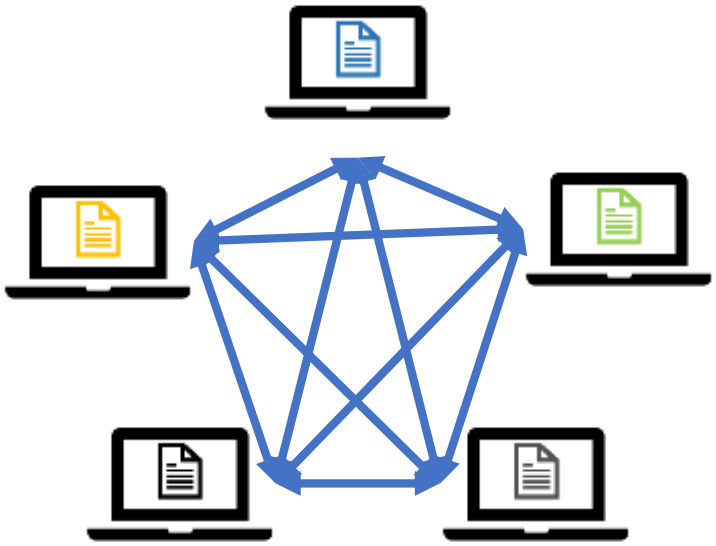
삼성전자

  - 그런데 저렇게 모이고 공유된 정보들이… 신뢰할 수 있긴 한 건가?

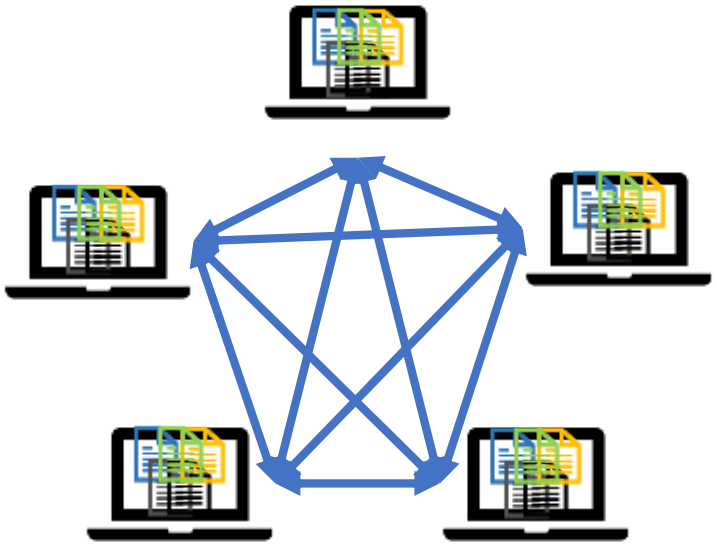
  - **계약서, 개인 자산, 지적 자산**같이 중요한 정보를 저렇게 공유해서는 안되겠는데… 이 데이터들을 사용하는 서비스들은 아무래도 4차 산업혁명의 물결에 올라타기 어렵겠네 -〉 **블록체인 기술로 보완**

4. 4차 산업혁명 속 블록체인

- **블록체인**
  - 정보가 마구잡이로 공유되고 사용되는 4차 산업혁명 시대에
    “관계자 간에 **신뢰할 수 있는 방법**으로 **정보를 공유**하는 기술”



기존 인터넷



블록체인

2

블록체인 발전과 전망

블록체인의 시작과 발전, 그리고 미래 전망

목차

1. 블록체인의 시작: 비트코인
2. 블록체인의 발전: 이더리움과 프라이빗 블록체인
3. 블록체인의 현재
4. 블록체인의 발전 방향 및 전망

1. 블록체인의 시작: 비트코인

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

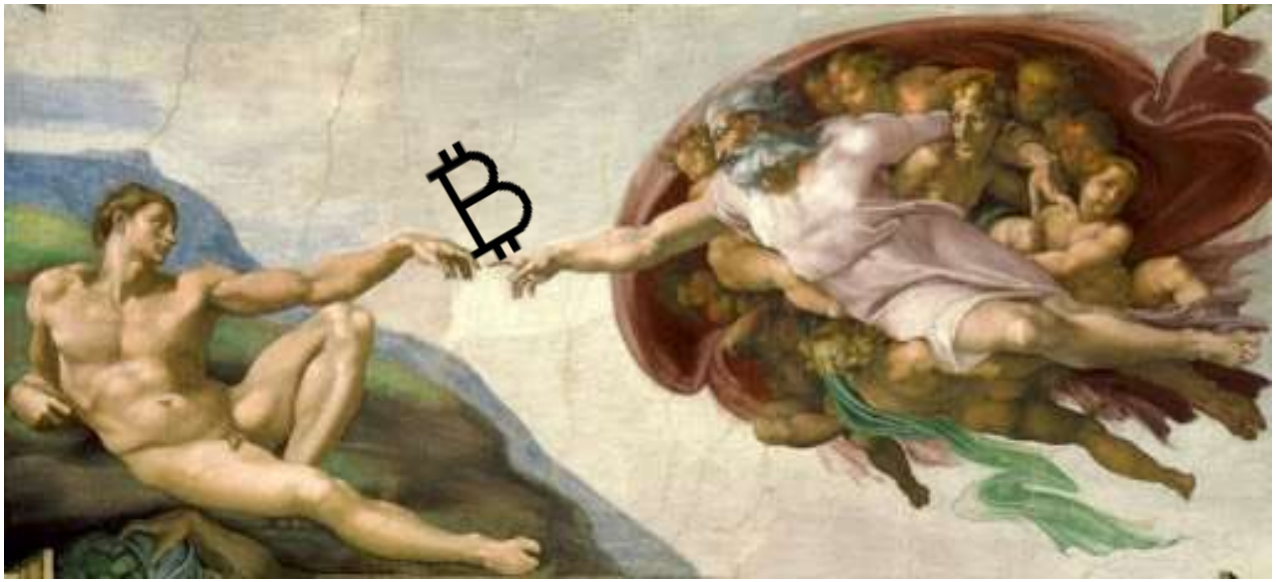
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the

1. 블록체인의 시작: 비트코인

- 2008년 10월, 논문이 보안 학회 쪽 메일링 리스트에 링크됨
- 2009년 1월, 오픈소스로 첫 비트코인 프로그램이 개발되어 공개됨
- 2009년 1월, 비트코인의 첫 블록이 사토시 나카모토에 의해 생성됨

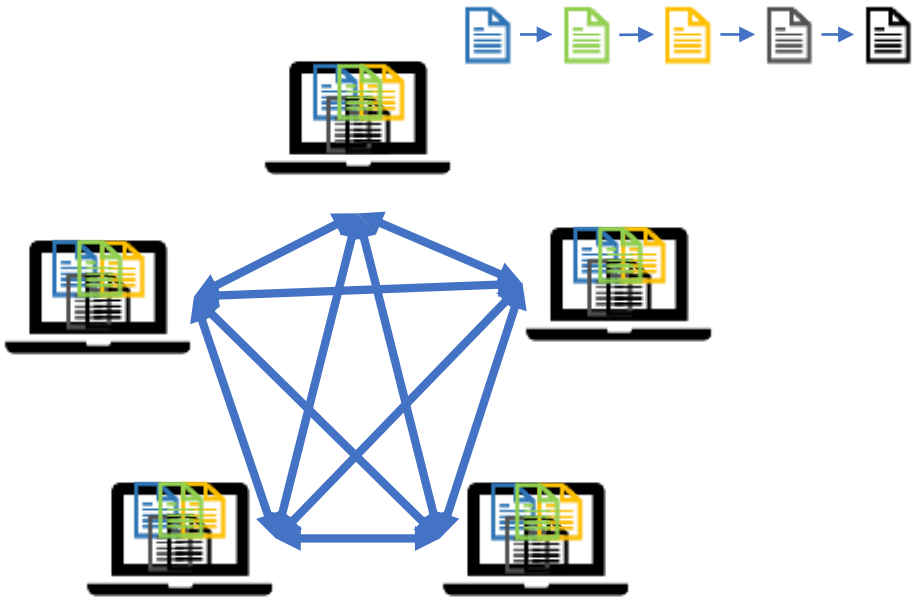


1. 블록체인의 시작: 비트코인

- **“신뢰할 수 있는 방법으로 정보를 공유하기 위한” 사토시 나카모토의 제안**
  - 저 사람이 그 사람이 맞는지 어떻게 알죠?
    -〉 비밀키 서명을 이용하면 알 수 있을 것이다.
  - 저 사람을 믿을 수 없는데 어떻게 믿나요?
    -〉 모두가 똑같은 정보를 복사해서 나누어 가질 것이다.
  - 저 사람이 몰래 고치면 어쩌죠?
    -〉 정보들은 모두 체인으로 엮어서 앞에 정보를 위조하면 뒤 따라오는 수천 수만개의 정보를 모두 위조해야 하게끔 만들 것이다.
  - 정보를 저장하는 당사자가 수천 개의 컴퓨터들인데, 어떻게 모두 같은 정보를 복사하죠?
    -〉 채굴이라는 방식으로 돌려서 1등 먹는 사람이 책임지고 이상 없는지 검증하고, 걔가 검증한게 정답이다. 1등하면 노력의 대가로 돈 준다.

1. 블록체인의 시작: 비트코인

- **“신뢰할 수 있는 방법으로 정보를 공유하기 위한” 사토시 나카모토의 제안**
  - 정보 저장 원칙 -〉 모두가 동일한 카피를 갖는다
  - 정보 저장 형태 -〉 체인 형태로 위변조를 막는다
  - 정보 공유 형태 -〉 채굴이라는 합의 과정을 통해 공유한다



1. 블록체인의 시작: 비트코인

- **그래서… 그런 기발한 방법으로 공유할 정보는 무엇이죠?**
  -〉 역시 가장 신뢰가 필요한 중요한 정보는…

나의 은행 잔고!

- 은행 잔고는 나의 입출금 내역의 합산
- 비트코인이 저장 & 공유하는 정보는 **“비트코인의 입출금 내역”**

1. 블록체인의 시작: 비트코인

- 돈의 변천

2. 블록체인의 발전: 이더리움과 프라이빗 블록체인

- **이더리움**
  - 비트코인: 블록체인에 “입출금 기록”만 저장 가능
  - “무엇을 저장할지, 개발자들이 결정하도록 하자”
  - 블록체인 세상의 “**앱 스토어**”가 되겠다
    - 앱 = **스마트 컨트랙트**

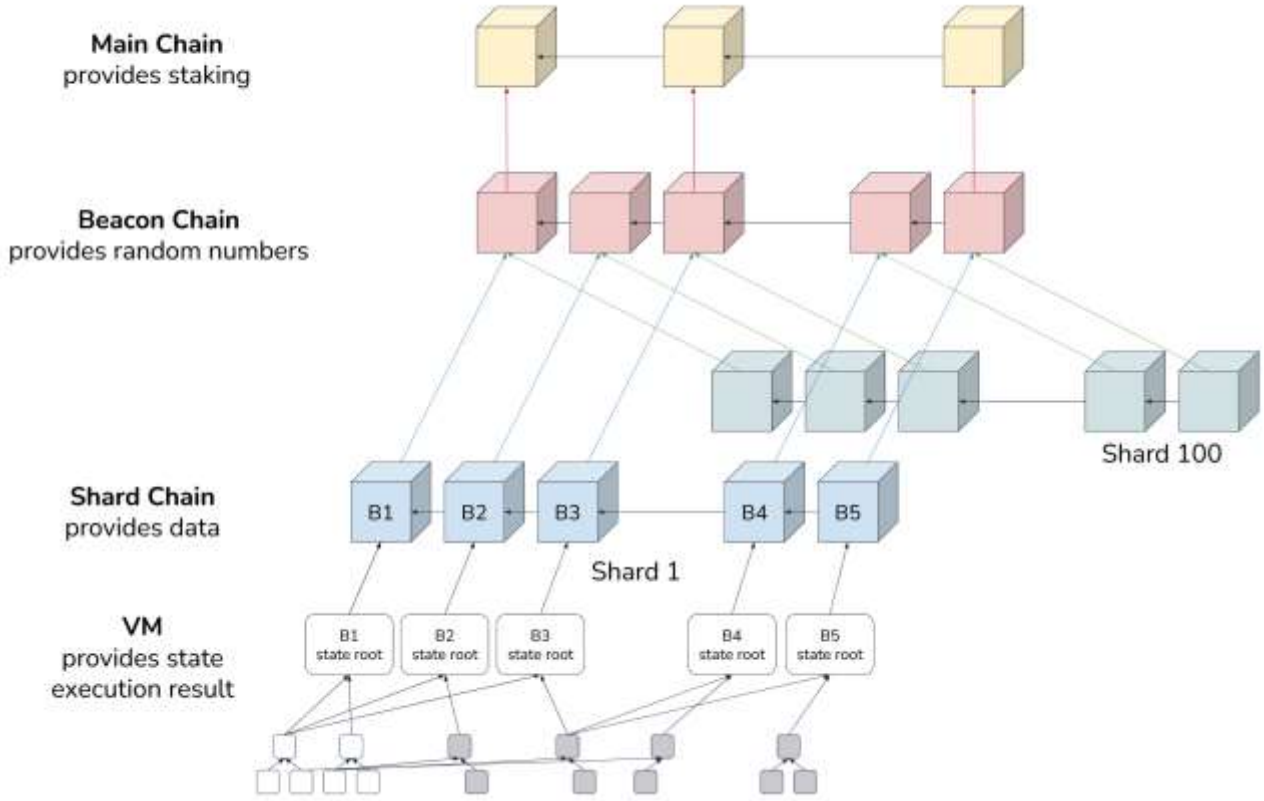
- 2013년 비탈릭 부테린이 백서를 작성하여 개발을 제안
- 2014년 이더리움 재단 설립 및 개발 자금 펀딩
- 2015년 7월 30일 비탈릭 부테린에 의해 개발됨
- 2020 ~ 2023년: 이더리움 2.0 진화 예정

2. 블록체인의 발전: 이더리움과 프라이빗 블록체인

- **이더리움**
  - 저장 원칙, 형식, 공유 방식은 비트코인과 동일
  - 기반에 비트코인과 동일하게 이더 라는 암호화폐가 법정 화폐처럼 존재

  - 가장 개발자 친화적인 블록체인
  - 가장 다양한 시도가 이루어지고 있음
    - 대부분의 알트 코인들은 이더리움의 스마트 컨트랙트
    - DeFi, NFT 등도 모두 이더리움의 스마트 컨트랙트
    - 앞으로도 수많은 시도가 이루어질 것임

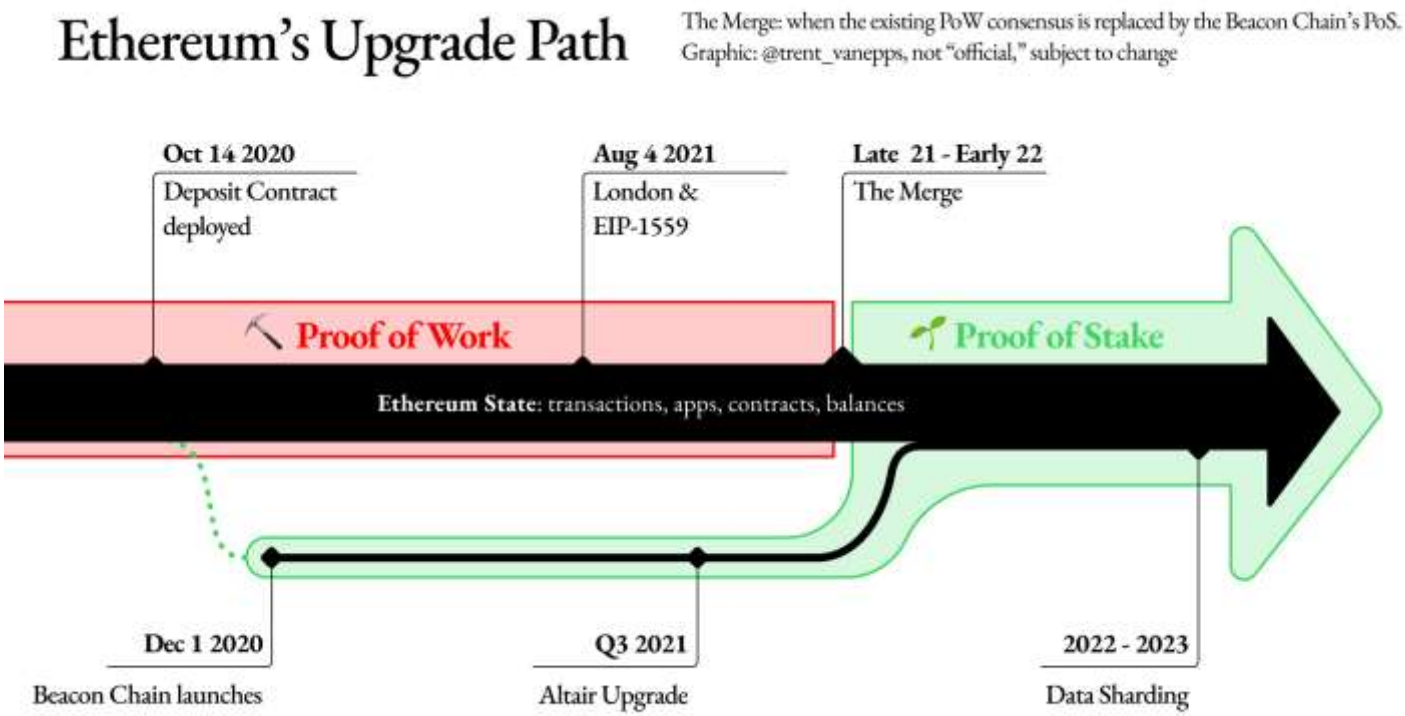
- **이더리움**
  - 이더리움 2.0



https://docs.google.com/presentation/d/1G5UZdEL71XAkU5B2v-TC3lmGaRIu2P6QSeF8m3wg6MU/edit#slide=id.g3c326bb661_0_298

2. 블록체인의 발전: 이더리움과 프라이빗 블록체인

- **이더리움**
  - 이더리움 2.0

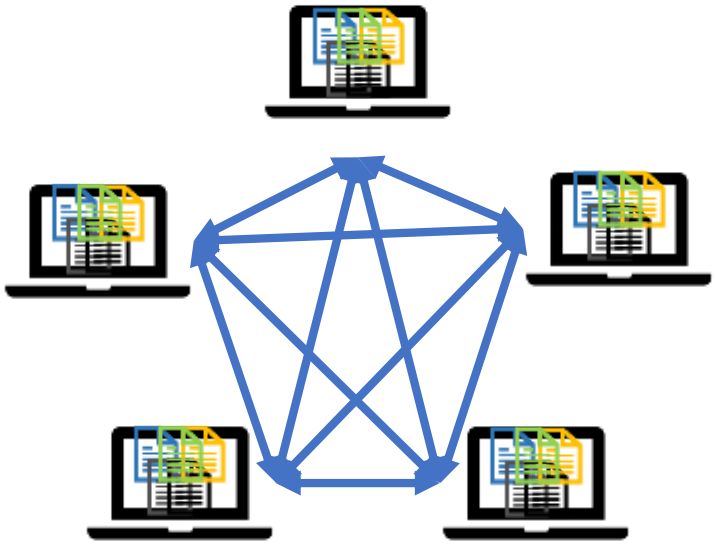


https://twitter.com/trent_vanepps/status/1415741658067517441/photo/1

2. 블록체인의 발전: 이더리움과 프라이빗 블록체인

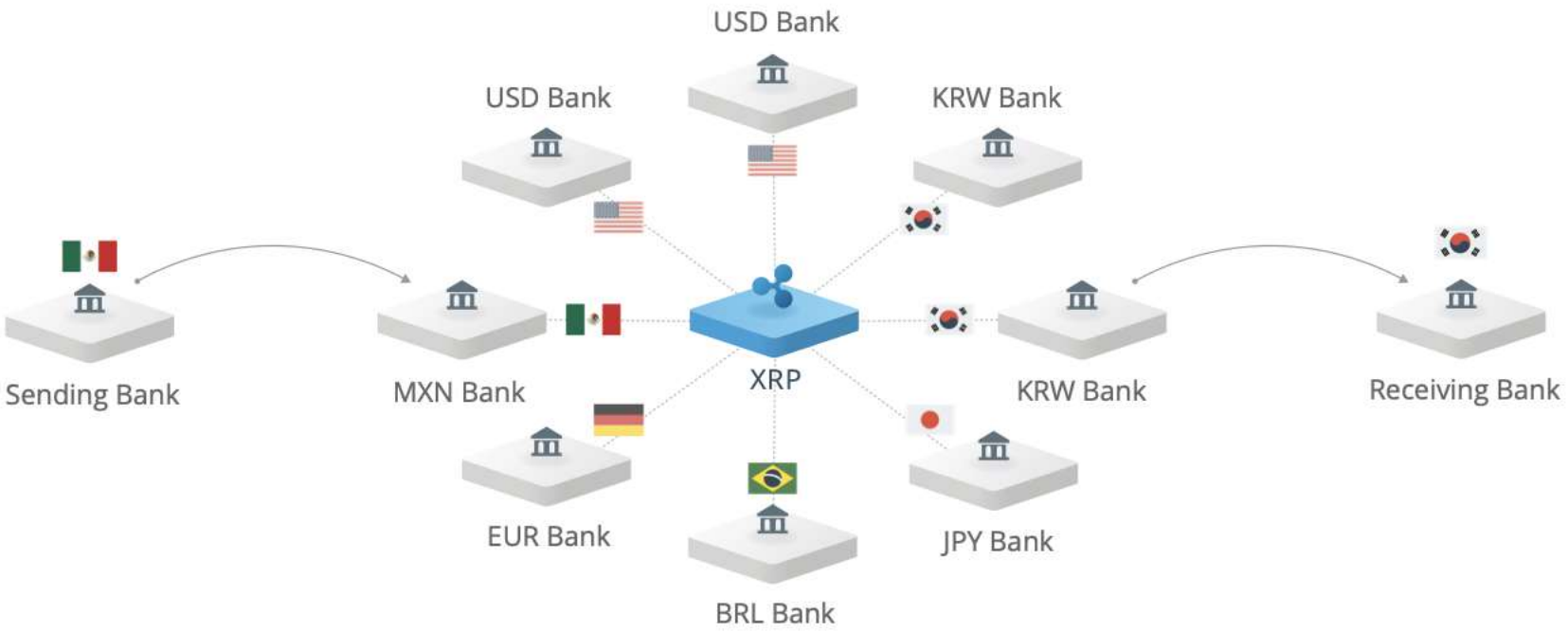
- **프라이빗 블록체인**
  - 비트코인, 이더리움:
    언제든, 누구든, 원하면 블록체인에 저장된 정보를 공유받고 자신의 컴퓨터에 저장할 수 있음
    -〉 퍼블릭 블록체인

  - 프라이빗 블록체인은 “정해진 컴퓨터들끼리만” 정보를 공유하고 저장함



2. 블록체인의 발전: 이더리움과 프라이빗 블록체인

- **프라이빗 블록체인**
  - 리플
    - 국제 송금 네트워크



3. 블록체인의 현재

- 암호화폐
- NFT
- DeFi

3. 블록체인의 현재

- **암호화폐**
  - 이더리움의 스마트 컨트랙트로 내가 만든 코인의 “입출금 내역”을 저장하게 하면, 그게 바로 암호화폐
    - 만드는건 전혀 어렵지 않음
  - 거래소
    - 주식으로 치면, “코스피 거래소 + 증권사” 가 결합된 형태
    - 거래 가능한 암호화폐 리스트를 관리하고 거래를 중계 -〉 코스피 거래소
    - 사용자 개인의 계좌(지갑)를 관리 -〉 증권사
  - 암호화폐가 잘되고 못되고는 그 어떤 기술 기반과 관계없이, 온전히 수요와 공급에 따라 움직이는 금융의 영역 -〉 제발 개발자에게 무슨 코인 사냐고 물어보지 말자

3. 블록체인의 현재

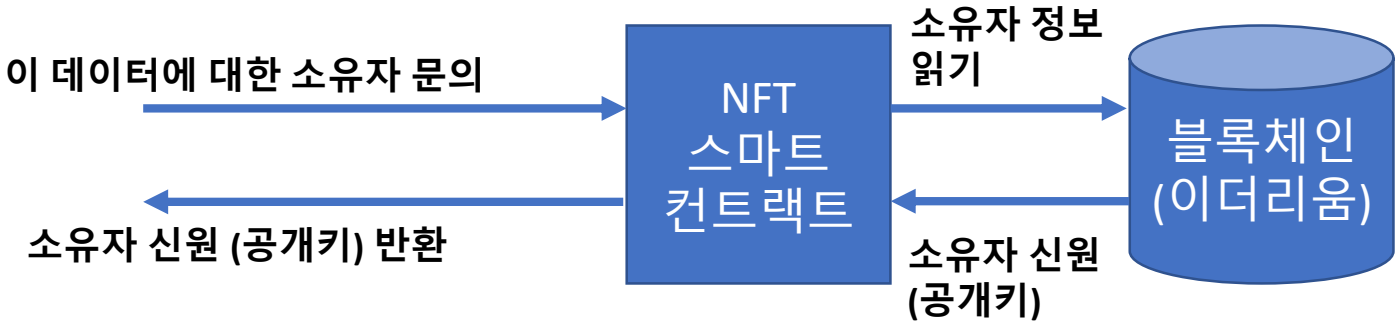
- NFT (Non-Fungible Token)
  - 대체 불가능 vs 대체 가능
    - 대체 가능 토큰
      - 내가 가진 1비트코인 = 너가 가진 1비트코인
      - 내가 가진 1비트코인은 다른 사람이 가진 1비트코인과 같고, 대체 가능
    - 대체 불가능 토큰
      - 내가 가진 1개의 “대체 불가능 토큰”은 다른 그 어떤 토큰으로도 대체 불가능
      - 예: 특정 그림의 소유권

3. 블록체인의 현재

바둑기사 이세돌 9단(왼쪽 사진)이 NFT(Non fungible token·대체불가능토큰)로 발행한 알파고와의 경기 중 '신의 한 수'가 표시된 5번기 제4국 기보(오른쪽 사진). 기보를 포함한 이 대국 동영상의 NFT는 18일 마감된 경매 결과 약 2억5000만 원에 낙찰됐다. 뉴스1·뉴시스

- "당시 바둑판 위에 돌이 차례로 놓이는 모습, '신의 한 수' (백 78수)가 표시된 기보와 함께 촬영한 이 9단의 사진, 서명 등이 담긴 동영상 파일이 NFT로 발행됐다." (동아일보 기사)
  - 블록체인은 기본적으로 "저장" 기술. 위의 데이터를 이더리움에 저장한 후, 이더리움 스마트 컨트랙트를 통해 소유자임을 검증할 수 있다.
  - 아무리 데이터가 복제되어 디지털 상에 뿌려지더라도, '그 데이터의 소유자는 나야' 라고 이더리움을 통해 언제든 증명이 가능

3. 블록체인의 현재



- 무한히 복사가 가능한 디지털 상에서도 “원본” 이라는 것이 존재할 수 있다는 것을 보여줌
- 사람들의 소유욕을 자극함
  - 무한히 복제 가능한 게임 아이템에도 수많은 돈을 지불
  - 비록 디지털 코드에 불과한 데이터도 ‘원본’에 대해 사람들은 돈을 지불할 수 있음
- 우리의 사회가 실물 사회에서 디지털 사회로 옮겨가고 있음을 보여주는 소프트웨어 서비스 중 하나

3. 블록체인의 현재

- DeFi (Decentralized Financial)
  - 블록체인 네트워크 위에서 동작하는 금융 어플리케이션
  - 탈중앙화 거래소 (DEX, Decentralized Exchange)
    - 예금/대출과 같은 은행 업무를 수행
    - 이미 정해진 규칙에 따라 이율 등이 결정됨
    - 이더리움으로 대부분 개발됨
  - 현재 (2021년 3월) 한화 48조원 규모의 자금이 예치되어 있음

4. 블록체인의 발전 방향 및 전망

- **곧 다가올 적용 분야**
  - 중앙은행 디지털화폐(CBDC, Central Bank Digital Currency)
    - 중앙은행이 직접 발행하는 암호화폐
    - 프라이빗 블록체인 (중앙은행과 주요 은행들 참여)
  - 정부 공문서 관리, 투표, 지역화폐, 지역주민인증, 물류, 자동차 부품 추적 등에 시범 사업 중
- **아직은 초기 기술로 지속적인 투자 연구가 필요**
  - 기술 컨샙과 가능성은 매우 훌륭함
  - 아직 시장을 장악한 주도적인 소프트웨어 시스템의 부재로 가능성이 매우 넓게 열려 있음

3

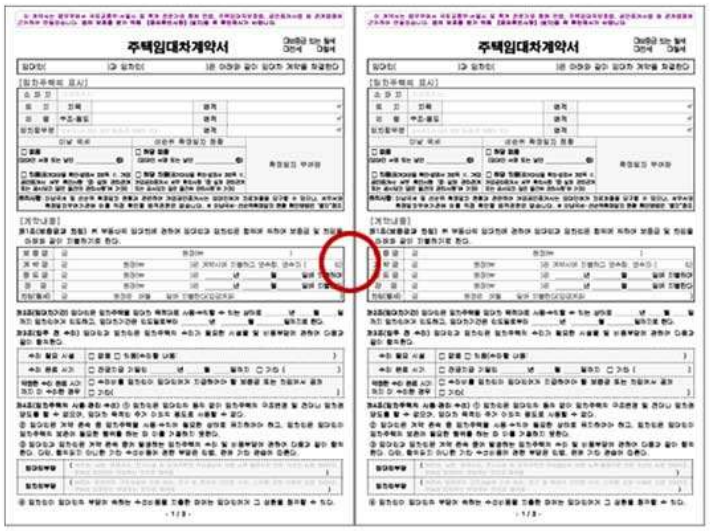
블록체인 기술의 구성요소

블록체인 기술이란 무엇인가? 그것의 장점과 한계는 무엇인가?

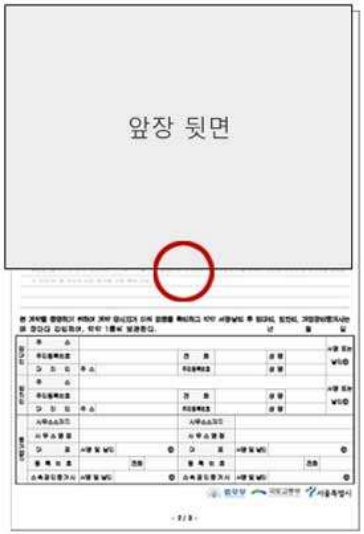
목 차

1. 블록체인 기술의 닮은꼴

- **부동산 계약서 구성요소**
  - **인감도장**: 내가 바로 내가 맞는 것을 증명
  - **참여자 숫자만큼 복사한 계약서**: 실제 데이터
  - **할인**: 참여자들 각각이 갖고 있는 데이터가 모두 동일함을 확인
  - **간인**: 데이터의 순서가 중간에 위변조되지 않음을 확인



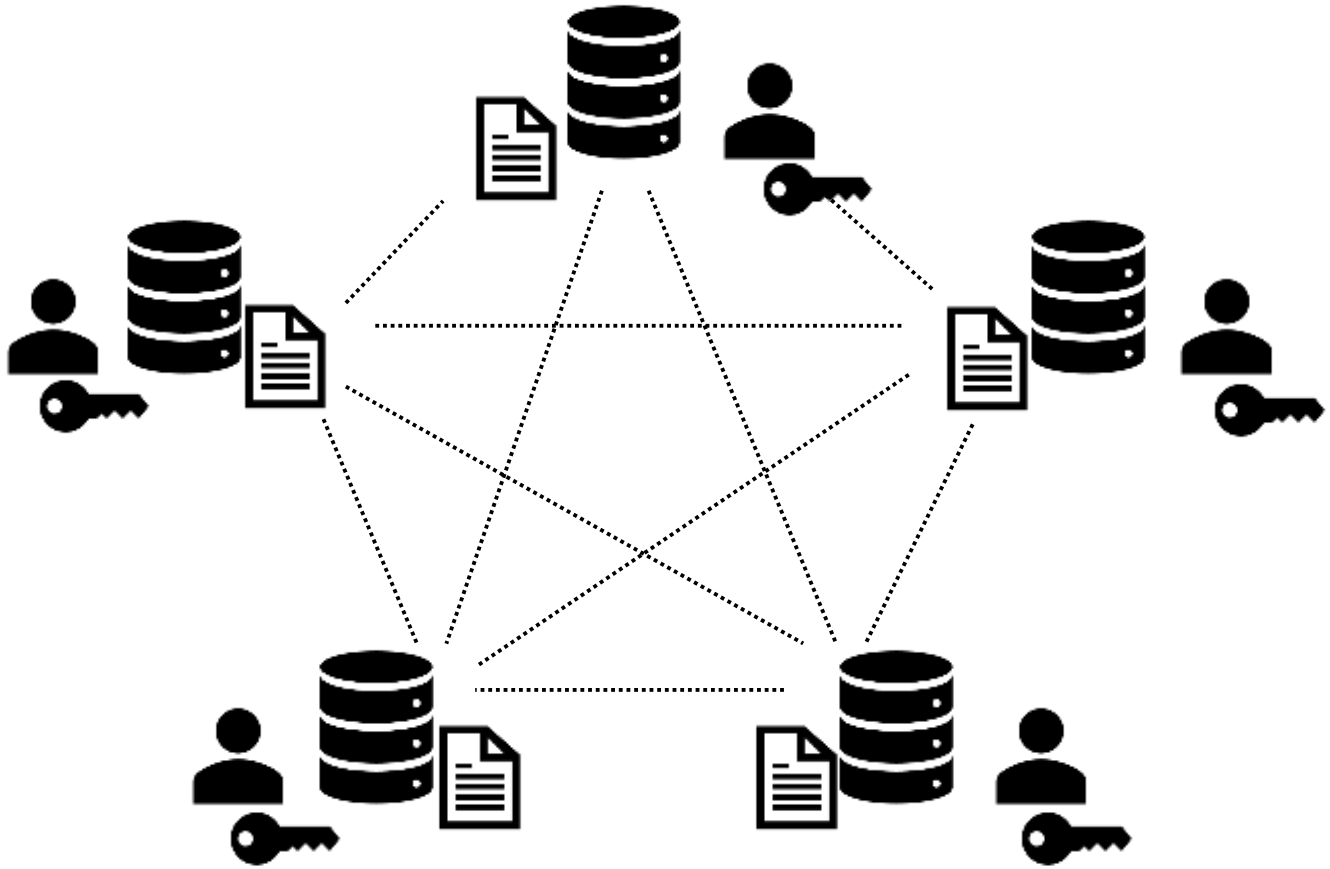
할인(割印)



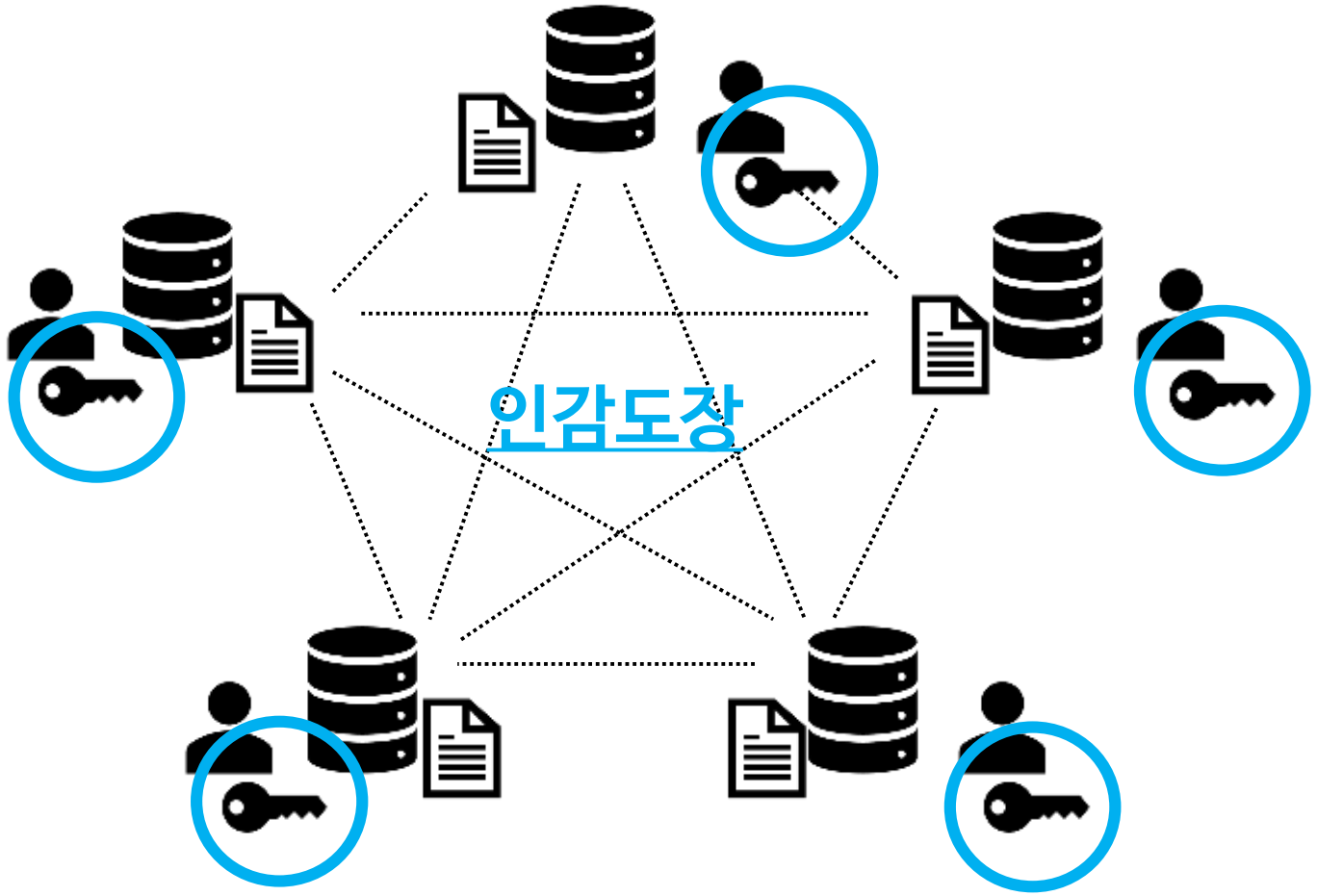
간인(間印)

1. 블록체인 기술의 닮은꼴

- 인간적 신뢰가 구축되지 않은 관계자들 5명이 존재

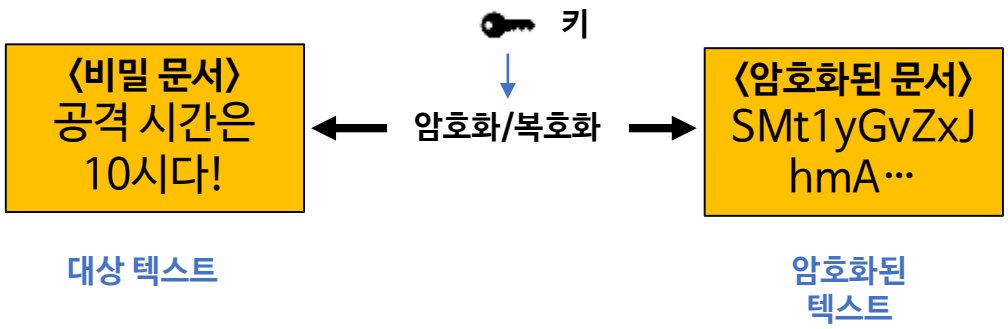


2. 공개키 암호화 기술



2. 공개키 암호화 기술

- **디지털 인감도장: 공개키 암호화 기술 (PKI)**
  - 키: 암호화 또는 복호화를 하기 위해 사용되는 텍스트

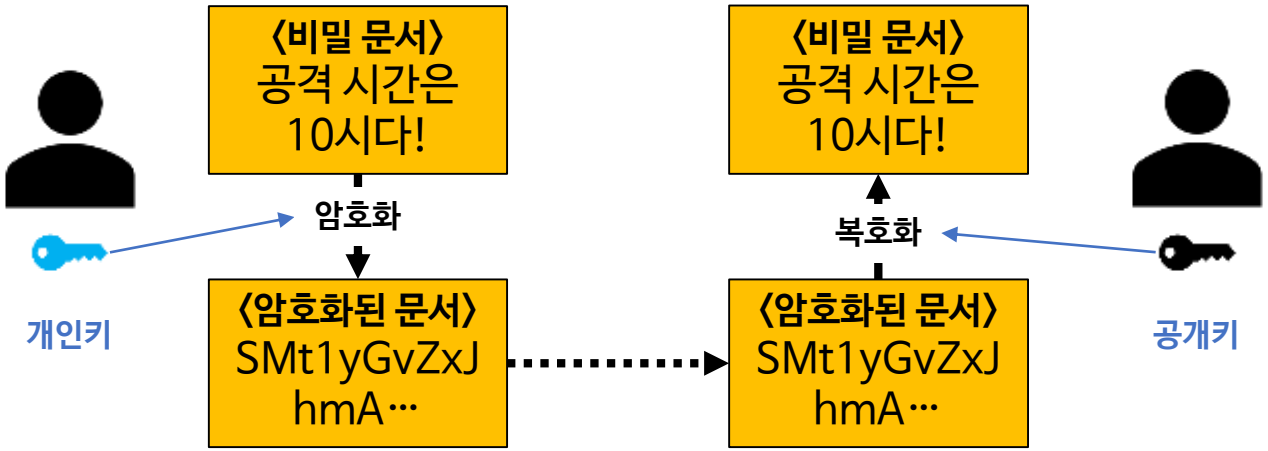


2. 공개키 암호화 기술

- **디지털 인감도장: 공개키 암호화 기술 (PKI)**
  - 암호화 기술
    - 단방향 암호화 기술
      - 복호화가 불가능
    - 비밀키 암호화 기술
      - 하나의 키로 암호화/복호화 모두 수행
      - 해당 키가 절대 유출되면 안되기 때문에 “비밀키” 암호화 기술
    - 공개키 암호화 기술
      - 고유한 2개의 키(암호화용 키, 복호화용 키)가 쌍으로 존재
      - 하나의 키로 암호화한 내용은 다른 키로만 복호화 가능

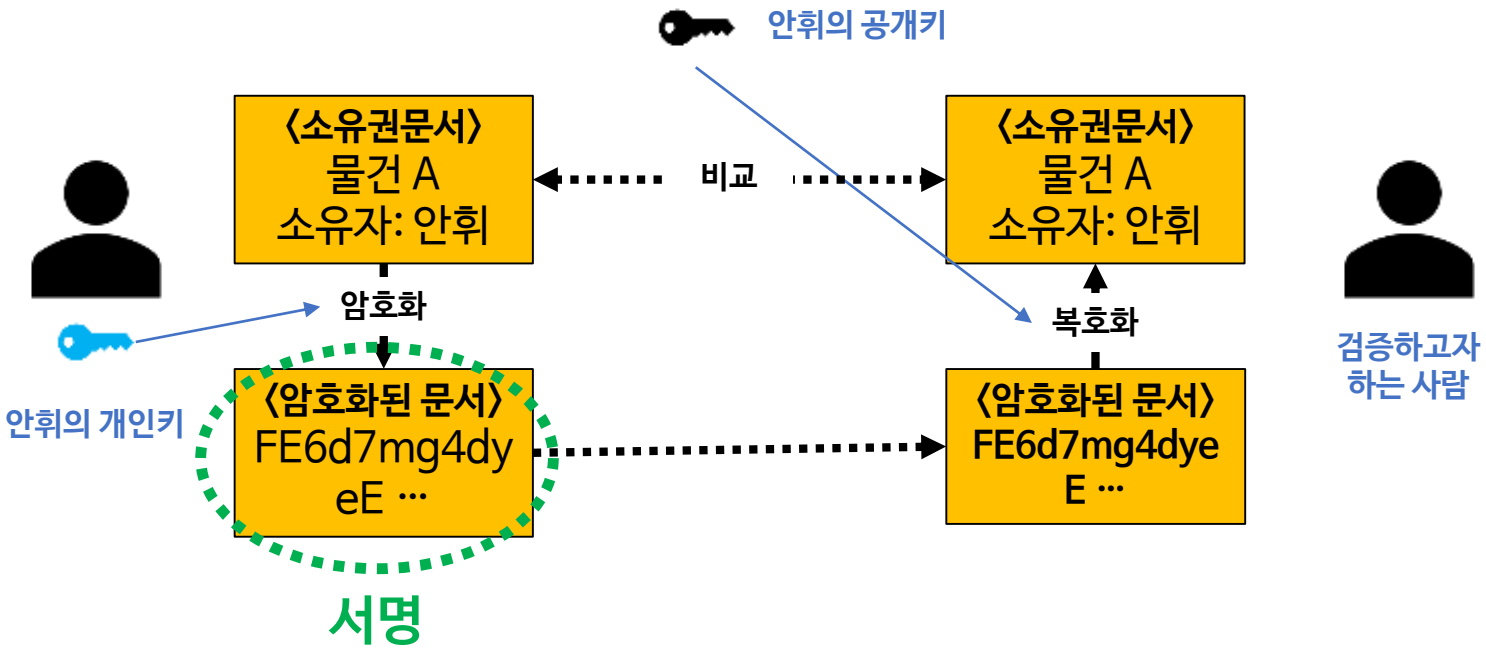
2. 공개키 암호화 기술

- **디지털 인감도장: 공개키 암호화 기술 (PKI)**
  - PKI는 암호화와 복호화를 하기 위한 키를 2개 준비
    - 고유한 한 쌍의 키: 암호화용 키 1개, 복호화용 키 1개
    - 개인키로 암호화하면, 복호화는 같은 쌍의 공개키로만 가능



2. 공개키 암호화 기술

- **디지털 인감도장: 공개키 암호화 기술 (PKI)**
  - PKI를 이용한 내용 검증

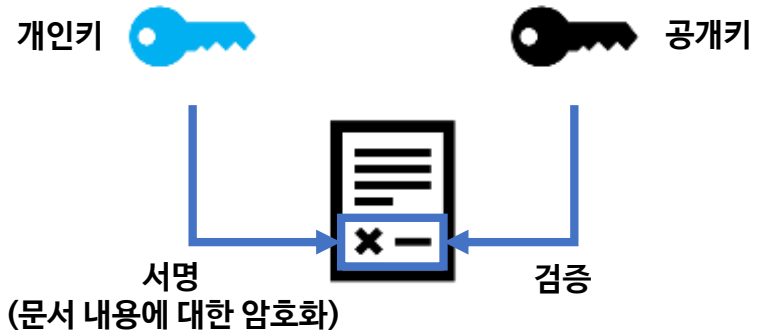


2. 공개키 암호화 기술

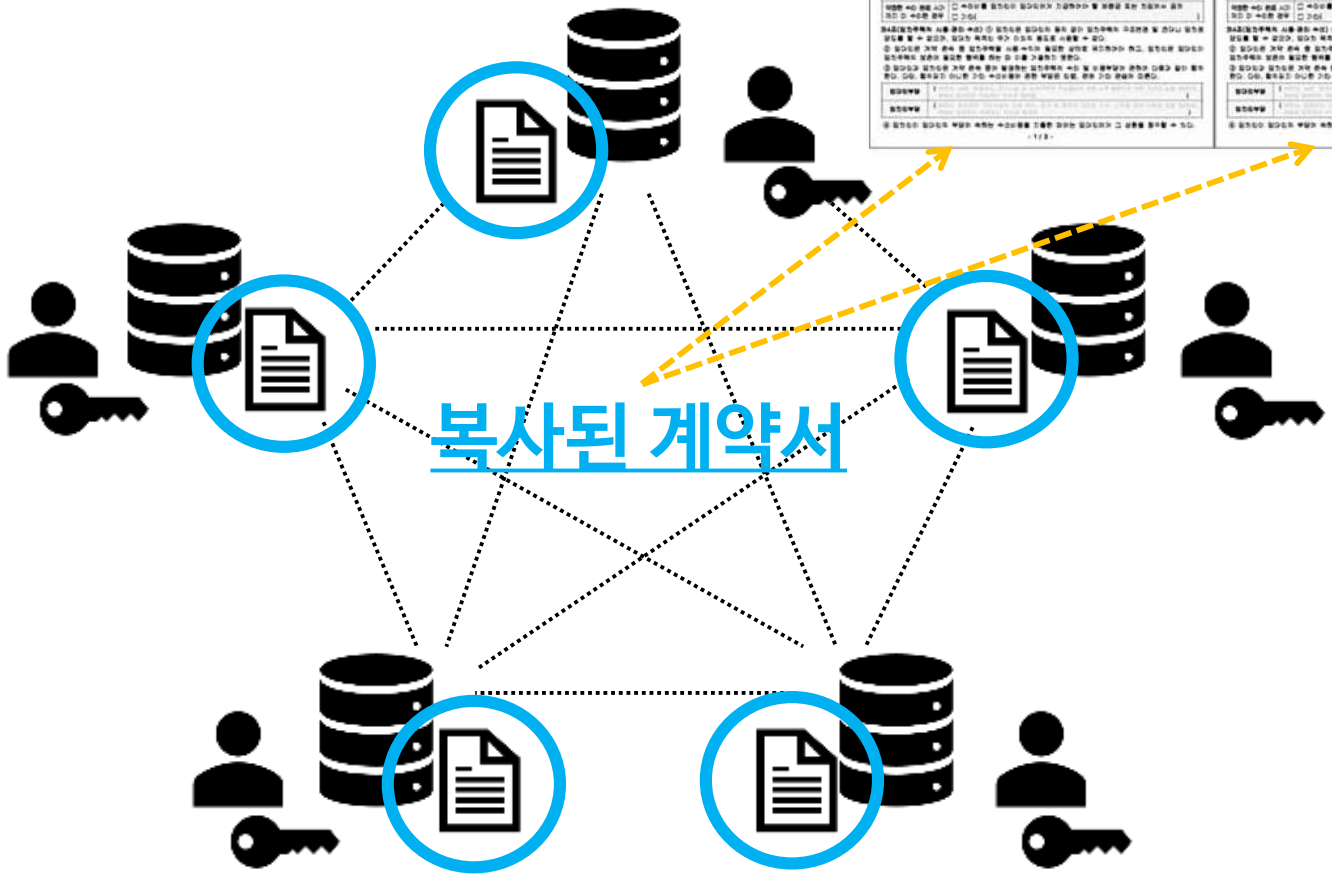
- **디지털 인감도장: 공개키 암호화 기술 (PKI)**

- 부동산 계약서의 **인감도장**
  - 나 = 인감도장
  - 증명 = 인감증명서 (정부가 보장)

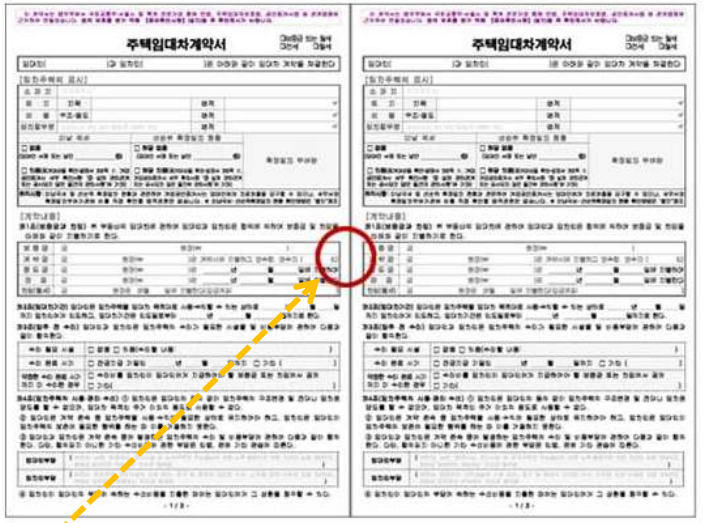
- 블록체인
  - 나 = 개인키
  - 증명 = 공개키를 통해 보장

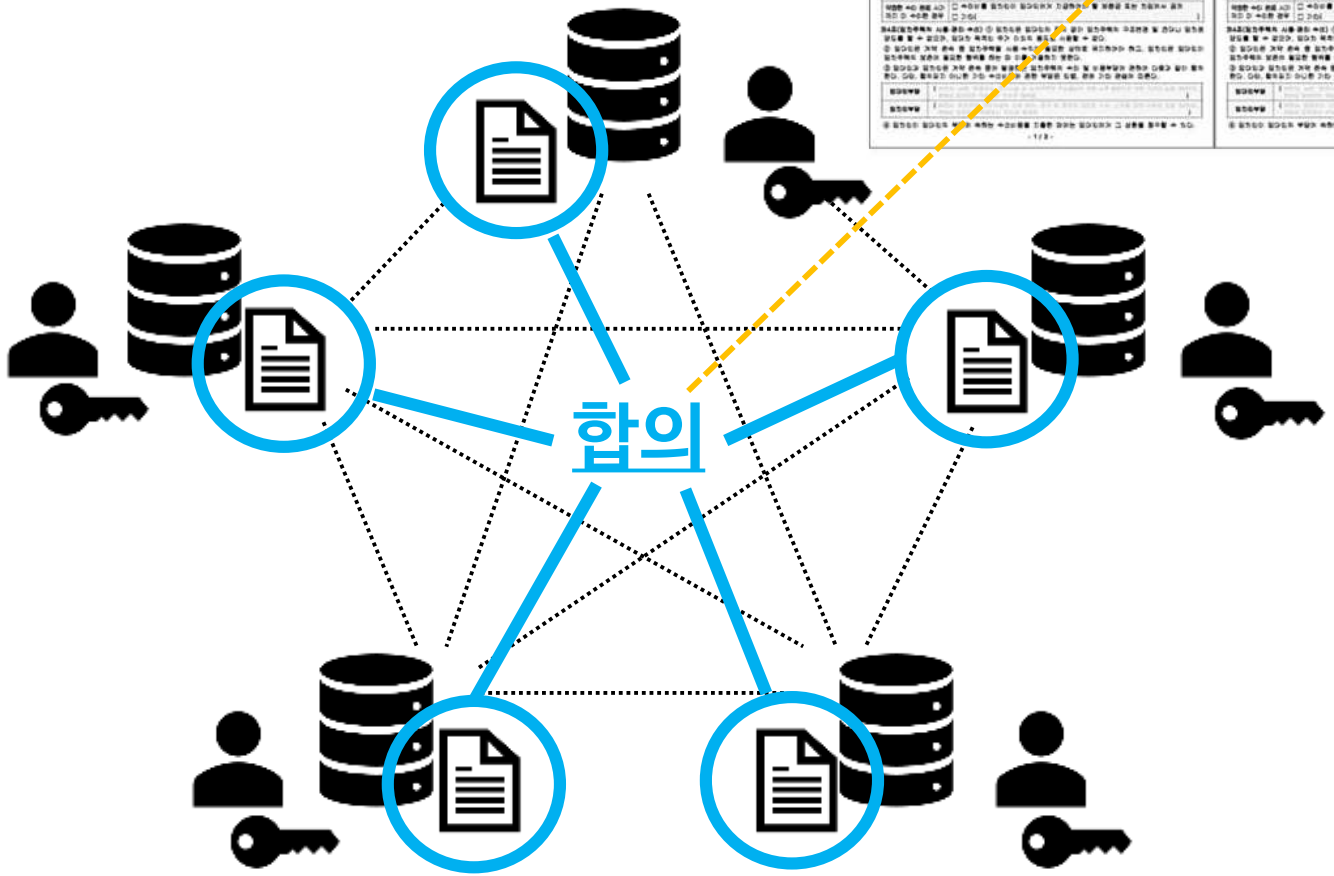


3. 합의 기술



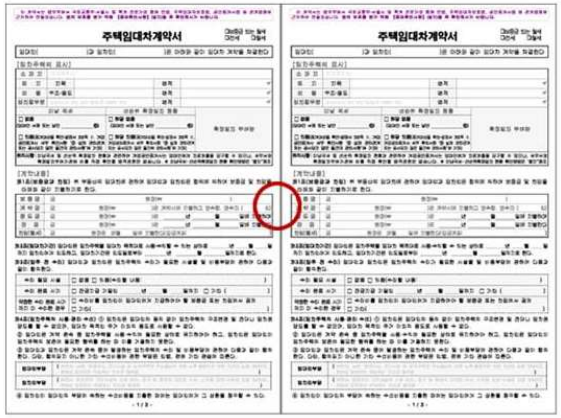
3. 합의 기술





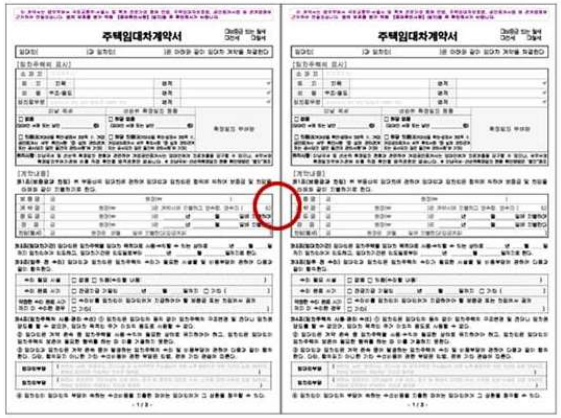
3. 합의 기술

- **복사한 계약서 및 할인: 합의 기술 (Consensus)**
  - " 참여자 모두가 동일한 계약서를 가지고 있음 " 을 증명하는 기술
  - 그럼... 참여자가 몇명?
    - 비트코인 노드 10,005 개 (2019년 기준)
    - 이더리움 노드 7,598 개
  - 만명 도장찍기 =〉 소프트웨어 서비스는 사람의 공간적 한계를 뛰어넘음



3. 합의 기술

- **복사한 계약서 및 할인: 합의 기술 (Consensus)**
  - Proof of Work: 노력에 의한 합의
  - Proof of Stake: 지분에 의한 합의
  - Fault Tolerance Algorithms: 리더에 의한 합의



3. 합의 기술

- **Proof of Work: 노력에 의한 합의**
  - 특정 조건에 맞는 숫자(Nonce, Number used once)를 찾는 작업
    - 빠르게 찾을 수 있는 방법 없음
    - 해당 조건에 맞는 숫자를 찾을 때까지 오로지 하나하나 해보는 방법 밖에 없음

    - 먼저 정답을 찾는 사람이 갖고 있는 계약서가 진품 (블록 생성 권한을 갖음)
      → 나머지 참여자들은 해당 내용을 복사해서 가지고 있음

3. 합의 기술

- Proof of Work: 노력에 의한 합의

  - …근데 왜 이 짓(?)을 할까?
    - “블록생성권한”을 갖고, 블록을 만들면 정해진 양 만큼 보상이 주어짐
      → 보상을 “채굴”한다라고 표현
    - 네트워크가 유지되기 위해서는 누군가 문서를 검증하고, 확인하는 작업을 해주어야 함
    - 보상은 네트워크 유지에 대한 보상임
  - 비트코인, 이더리움 등 대부분 이 방식을 따르고 있음

3. 합의 기술

- **Proof of Stake: 지분에 의한 합의**
  - 토큰 보유량에 따라 블록생성권한을 조정함
  - 구현에 따라 여러 모습이 존재
    - 토큰 보유량에 따라 블록생성 및 검증을 수행할 대표자를 선정
    - 토큰 예치 등을 통해 권한 부여
    - …
  - Proof of Work 의 과도한 에너지 사용 문제를 해결
  - 이더리움이 향후 이 방향으로 진화할 예정

3. 합의 기술

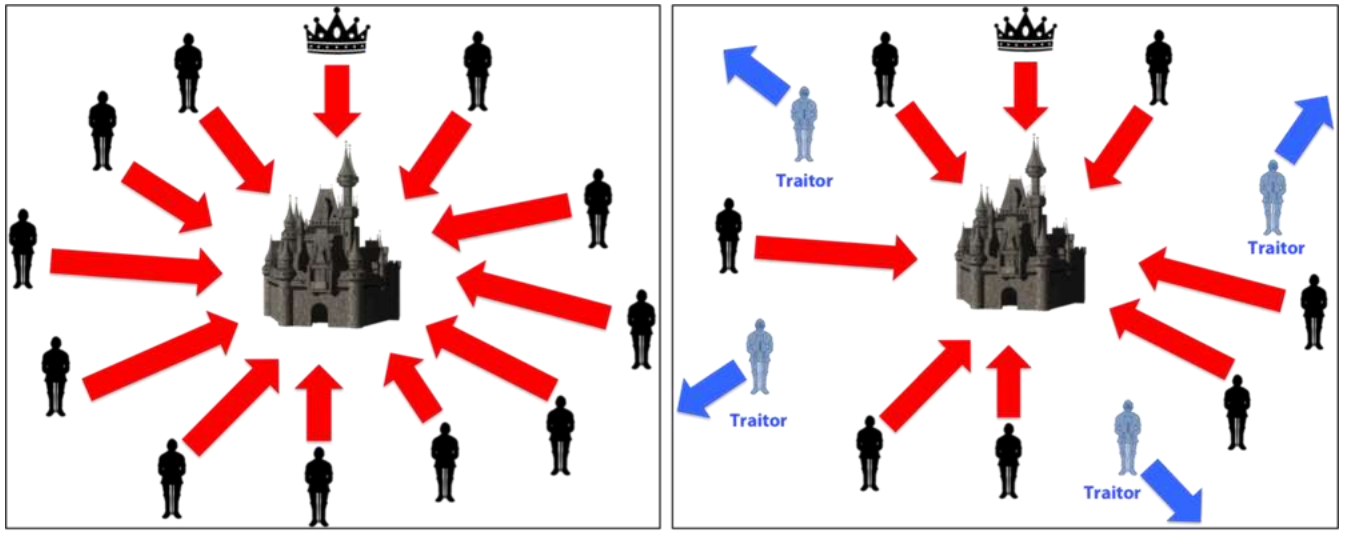
- **Proof of Stake: 지분에 의한 합의**
  - 이더리움 2.0의 PoS
    - **Validator**: 블록을 검증
      - 검증을 위해 충분한 하드웨어를 준비해야 함
      - 최소 32 Eth를 "보증금"으로 걸어야 함
        - 검증 요청에 불응하거나, 검증에 실패(혼자만 다른 값을 출력)하면, 보증금에서 벌금이 깍임
        - 검증에 성공하면, 보증금이 늘어남 =〉 보상
    - 블록 확정
      - 블록 검증은 정해진 시간 마다 랜덤하게 구성된 Validator들에 의해 진행됨
      - 전체 보증금의 2/3 만큼의 지지를 확보해야 블록은 확정됨
      - 현재 전체 보증금 규모는 약 100억달러(12조원)정도임

3. 합의 기술

- **Fault Tolerance Algorithms: 리더에 의한 합의**
  - Fault Tolerance Algorithms
    - 참여자 중 일부가 불능 상태(fault)가 되더라도, 네트워크를 유지시키는 알고리즘
    - 예:
      - 3대의 컴퓨터가 동일한 내용을 검증하여 저장 중
      - 1대의 컴퓨터가 갑자기 불능이 됨
      - 그래도 내용이 올바르게 검증되었다는 것을 보장함
    - Crash fault vs Byzantine fault
      - Crash fault: 참여자 중 일부가 불능 상태에 빠짐
      - Byzantine fault: 참여자 중 일부가 “배신자”가 됨

3. 합의 기술

- Fault Tolerance Algorithms: 리더에 의한 합의
  - Byzantine Fault

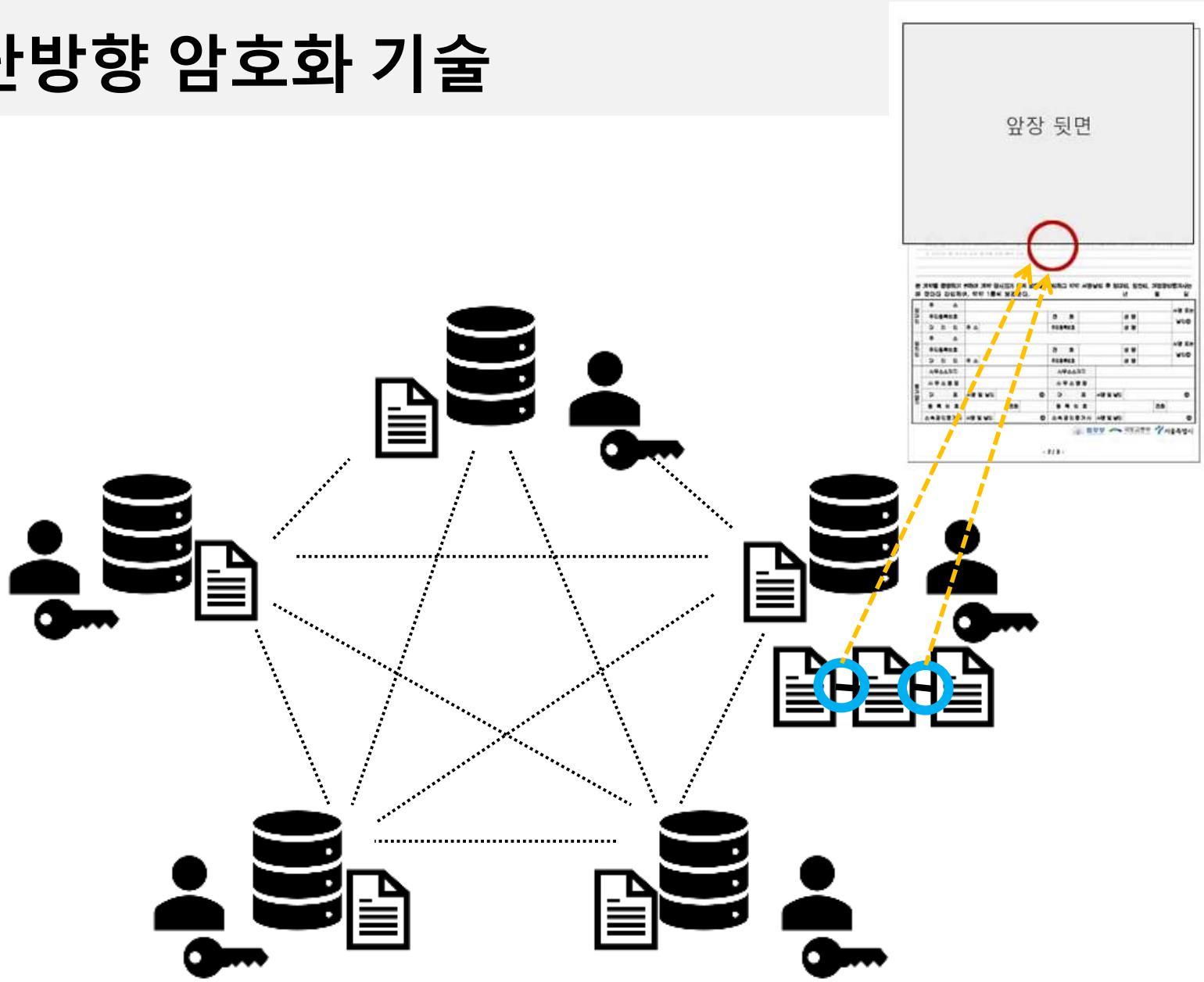


Coordinated Attack Leading to Victory　　Uncoordinated Attack Leading to Defeat

3. 합의 기술

- **Fault Tolerance Algorithms: 리더에 의한 합의**
  - Fault Tolerance Algorithms
    - 일반적으로 절반(Crash fault), 또는 1/3(Byzantine fault)의 참여자가 불능상태에 빠져도 합의가 올바르게 진행되는 것을 보장함
    - 소수의 참여자들이 빠르게 합의하기 때문에 다른 합의 대비 매우 빠르고, 에너지 소모가 거의 없음
    - 보통 참여자 숫자가 20~30 정도면 한계에 도달
    - 프라이빗 블록체인에서 주로 사용
    - 현재 기술은 Crash Fault 수준

4. 단방향 암호화 기술



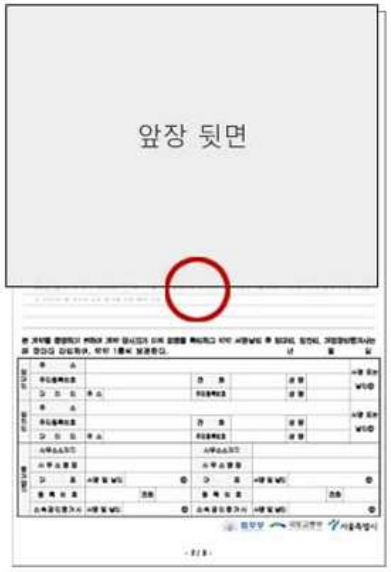
4. 단방향 암호화 기술

- **간인: 해시 기술 (Hash)**
  - 해시
    - **단방향 암호화** 기술
    - 특정 문서를 복구 불가능한 문자열로 암호화해줌

Hello, World! → (해시!) → DFFD6021BB2BD5B0AF676290809EC3A53191DD81C7F70A4B28688A362182986F

Hello, World? → (해시!) → F16C3BB0532537ACD5B2E418F2B1235B29181E35CFFEE7CC29D84DE4A1D62E4D

- 원래는 비밀번호 저장, 문서 위변조 방지에 사용됨



4. 단방향 암호화 기술

- 간인: 해시 기술 (Hash)
  - 이전 데이터의 해시값을 함께 저장함

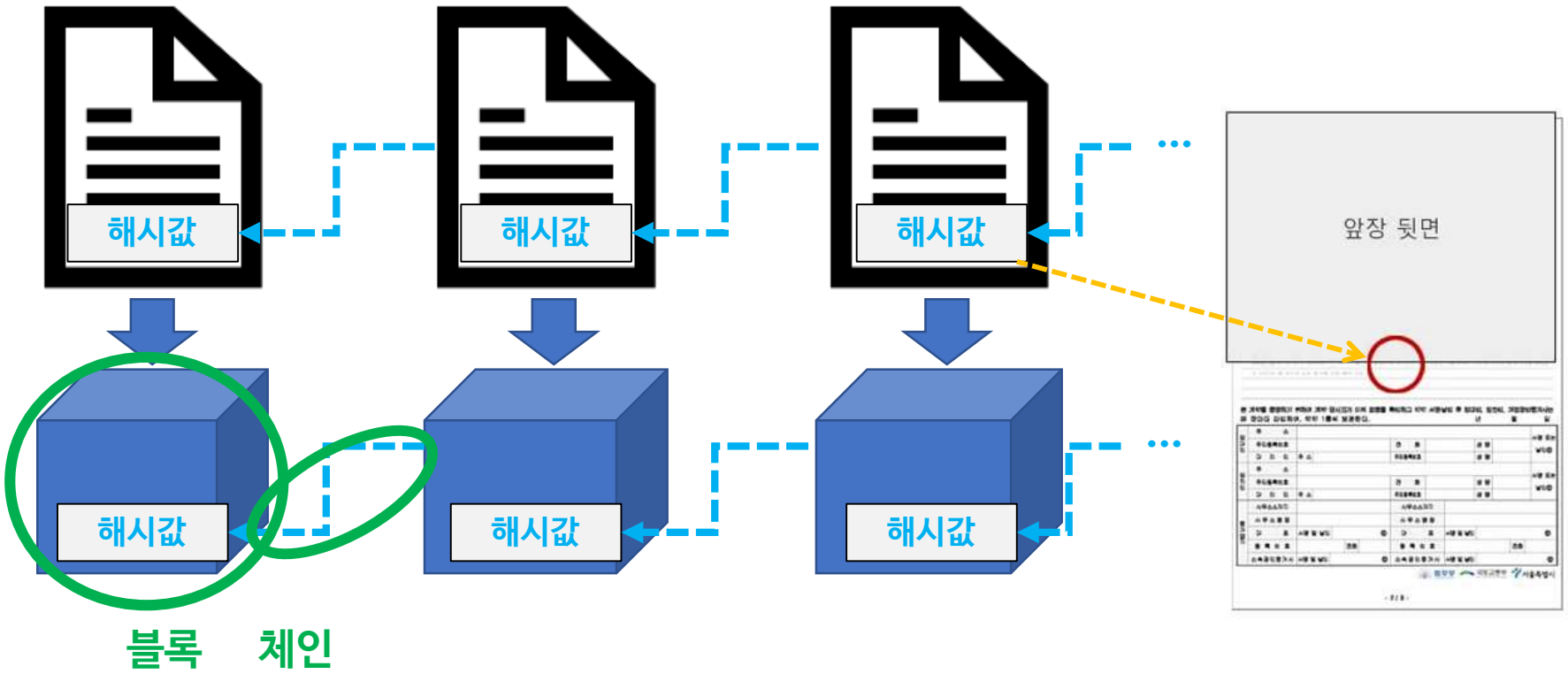
4. 단방향 암호화 기술

- 간인: 해시 기술 (Hash)

- 저장된 데이터를 위조하려면, 그 뒤에 저장한 모든 데이터를 위조해야 함
  -〉 위변조가 현실적으로 불가능

4. 단방향 암호화 기술

- 간인: 해시 기술 (Hash)



5. 스마트 컨트랙트

- **블록체인 = 데이터 저장소**
- **스마트 컨트랙트 = 블록체인 입출력 프로그램**
  - 블록체인에 데이터를 쓰고, 읽는 프로그램
  - 비트코인
    - 블록체인에 비트코인 전송 이력을 쓰고, 읽는 스마트 컨트랙트 1개만 존재
  - 이더리움
    - 개발자가 자유롭게 블록체인에 저장할 데이터를 결정하고, 이를 읽고 쓰는 프로그램을 만들 수 있음 = **스마트 컨트랙트 플랫폼**

6. 블록체인 기술이란

- **장점**
  - 위변조 불가
    - 저장된 데이터는 위변조에 매우 강함
    - 사람이 갖는 공간적, 시간적 한계를 뛰어넘기 때문에, 체인 형태로 구성된 데이터를 모두 위조하는건 “현실적”으로 불가능
    - 공공 목적으로 활용될 때 가장 고려할만한 장점
  - 투명성
    - 모든 참여자들이 데이터를 나누어가짐
    - 지금도 전세계 비트코인 거래 내역은 투명하게 모두가 볼 수 있음
    - 암호화폐 거래를 통해 자신을 숨길 수 있다는 것은 허상
      (자신의 공개키를 아는 순간 전세계 모든 사람이 거래내역을 파악할 수 있음)
    - 프라이버시와 다름을 명확히 이해할 것

6. 블록체인 기술이란

- **한계**
  - 프라이버시
    - 사실 블록체인과 관계없음.
    - 프라이버시는 서비스 설계에서 논할 일이지, 블록체인을 쓴다고 해결되는 문제가 아님!
    - 그래서 투명성이 장점인 블록체인에 개인정보를 올리는건 “매우 섬세한” 서비스 설계가 필요한 일
  - 성능
    - 블록체인은 성능 관점에서 제약이 심한 시스템: 느리고, 자원을 많이 차지함.
    - 민간 기업 도입이 무산되는 가장 큰 이유
    - 투명성, 위변조 불가를 통해 공공의 목적을 달성할 경우, 성능 제약에도 도입 가능 =〉 블록체인이 공공 영역에서 더 논의되어야 하는 이유!

4

이더리움 개발환경 맛보기

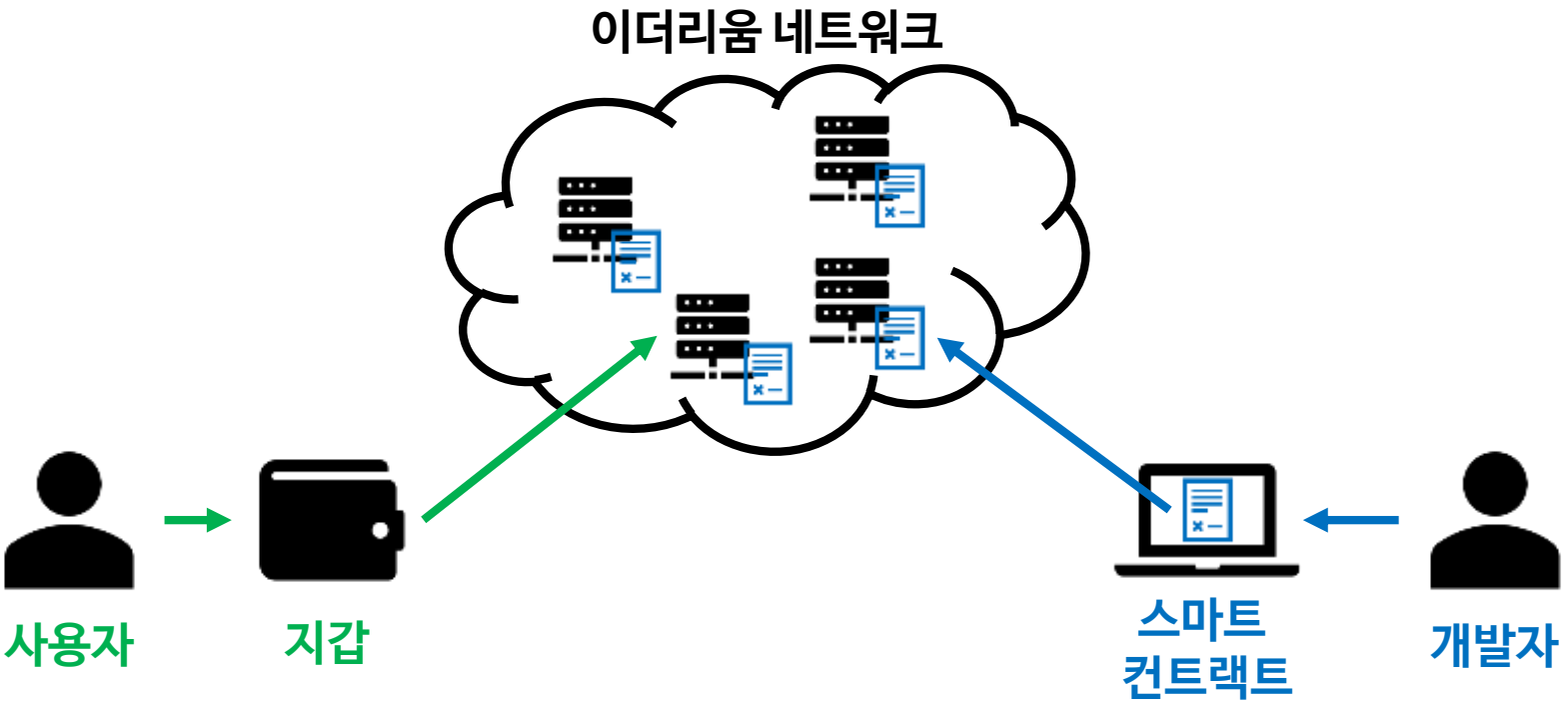
이더리움 개발 도구들 소개

서울특별시 SEOUL METROPOLITAN GOVERNMENT

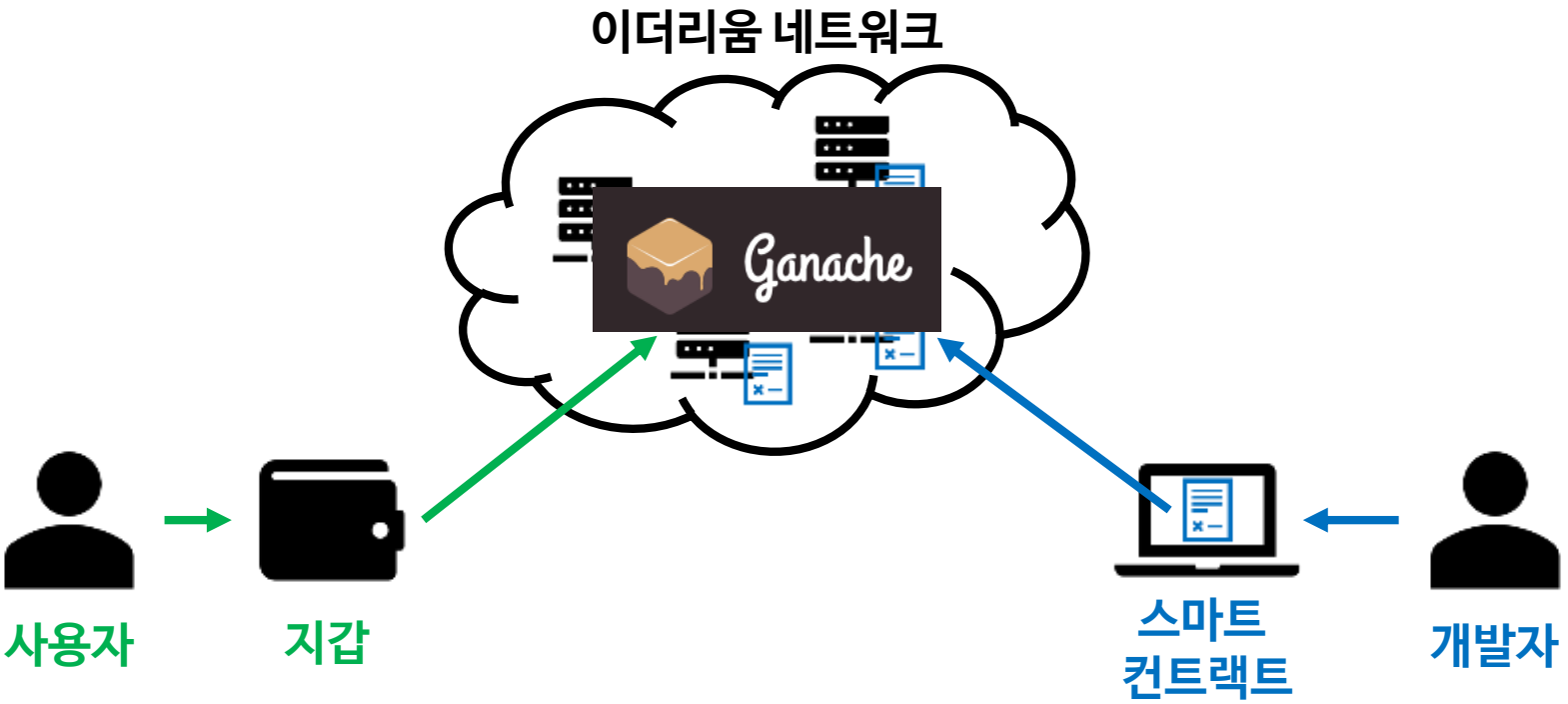
kcbc 한국에이아이블록체인융합원 Korea AI Blockchain Convergence

목 차

1. 이더리움 개발환경 구성

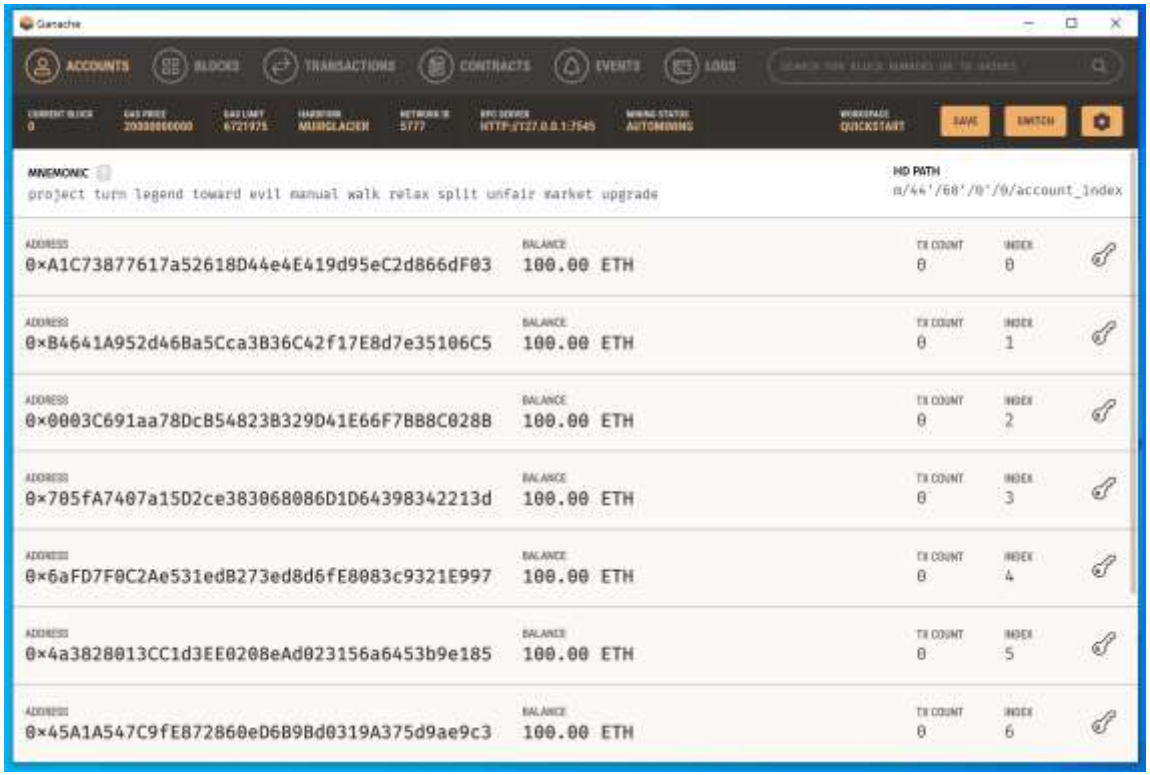


1. 이더리움 개발환경 구성



1. 이더리움 개발환경 구성

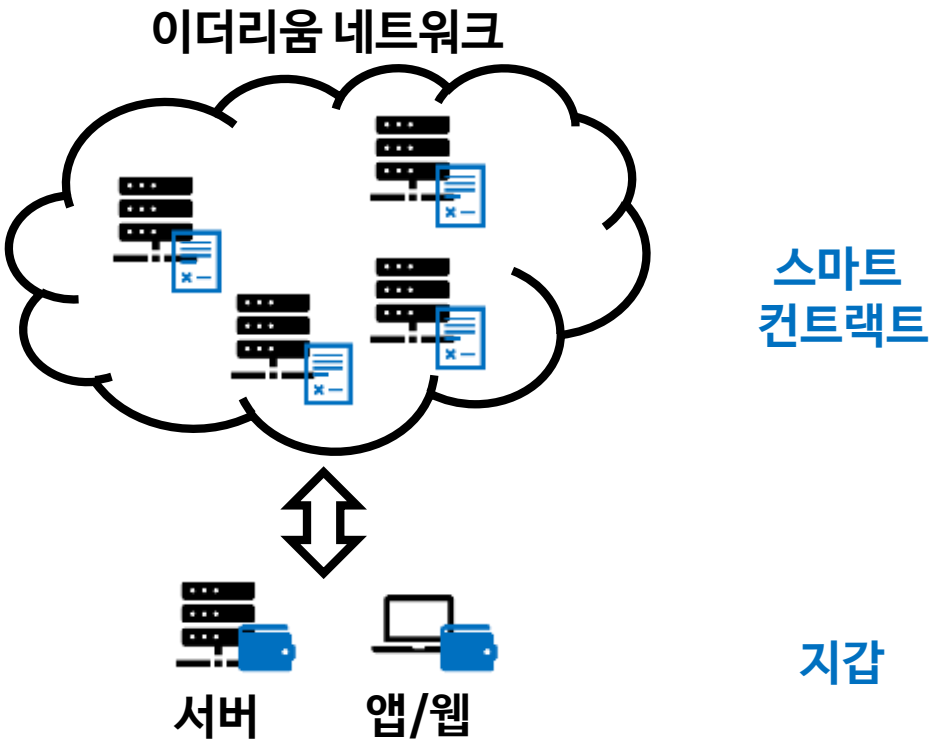
- Ganeche
  - 이더리움 네트워크를 가상으로 띄워주는 역할
  - Geth 같은 걸로 직접 마이닝 하면서 개발하기에는 너무 느림
  - Ganeche는 이더리움 관련 API들을 순식간에 실행시켜줌



1. 이더리움 개발환경 구성

- **Truffle**
  - Node.js 기반 이더리움 스마트 컨트랙트 개발 및 배포 도구
  - 스마트 컨트랙트 테스트
  - 스마트 컨트랙트 빌드 및 배포

2. 개발 도구



2. 개발 도구

- **스마트 컨트랙트 개발: Solidit**
  - Truffle로 개발환경 구성
  - Solidity 언어
    - 진입 장벽이 좀 있음
    - 너무 혼자 튀는 문법이 많아서, 첫
      - 클래스 문법처럼 사용하는 C
      - Contract 내 맴버 변수가 바
      - EVM에 특화된 코딩 기법
      - …
    - 코드 execution 자체가 곧 비용이
      숙련자와 초보자의 격차가 클 것으

```
for (uint256 i=0; i < array.length; i++) {
   doStuff(array[i]);
}
```

[PASS] test_loop() (gas: 106969)

```
uint256 length = array.length;
for (uint256 i=0; i < length; i++) {
   doStuff(array[i]);
}
```

[PASS] test_loop() (gas: 106682)

```
uint256 length = array.length;
for (uint256 i=0; i < length; ++i) {
   doStuff(array[i]);
}
```

[PASS] test_loop() (gas: 106182)

```
uint256 length = array.length;
for (uint256 i=0; i < length;) {
   doStuff(array[i]);
   unchecked { i++; }
}
```

[PASS] test_loop() (gas: 94382)

```
uint256 length = array.length;
for (uint256 i=0; i < length;) {
   doStuff(array[i]);
   unchecked { ++i; }
}
```

[PASS] test_loop() (gas: 93882)

2. 개발 도구

- **스마트 컨트랙트 개발: Solidity**
  - Solidity 개발
    - Remix IDE
      - 다 갖춰진 환경
      - Truffle, VSCode와 매우 유사
      - VSCode 플러그인도 제공
    - Visual Studio Code + solidity plugin + truffle

2. 개발 도구

- **지갑 개발**
  - 이더리움 키 관리 및 이더리움 네트워크와의 통신을 위한 라이브러리를 이용하는 개발
  - Go 언어: geth (Go Ethereum 라이브러리)
    - 이더리움 클라이언트를 개발하는 코어 라이브러리
    - 많은 것이 가능하지만, 개발 편의를 위한 함수들이 다소 부족
  - JavaScript: web3.js, ethers.js
    - web3.js
      - 가장 오래됨. 안정적임. 폭넓은 커뮤니티를 갖고 있음
      - 다소 올드한 라이브러리 구성을 갖음
    - ethers.js
      - web3.js와 맞먹는 안정성을 갖음. 좋은 커뮤니티를 갖고 있지만, 국내 자료가 다소 부족
      - web3.js에 비해 좀 더 모던한 JavaScript 라이브러리 형태를 갖음