Basic Block chain / Web3

i-Keeper CERT 오나희

목차

1. Blockchain?

Block + chain

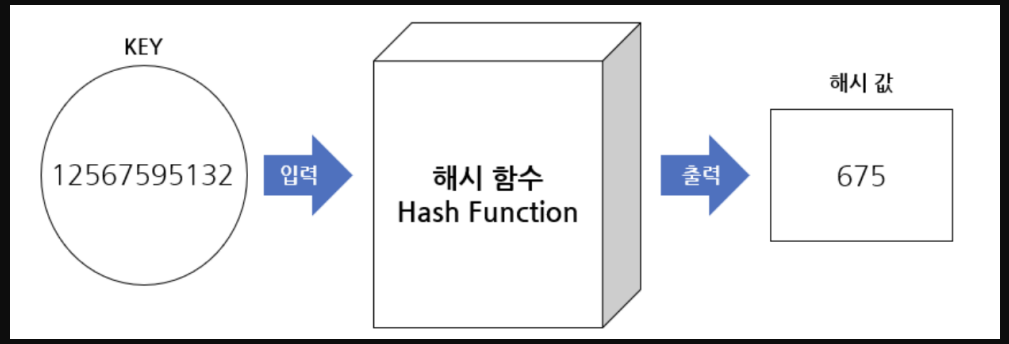
1. Blockchain?

Block

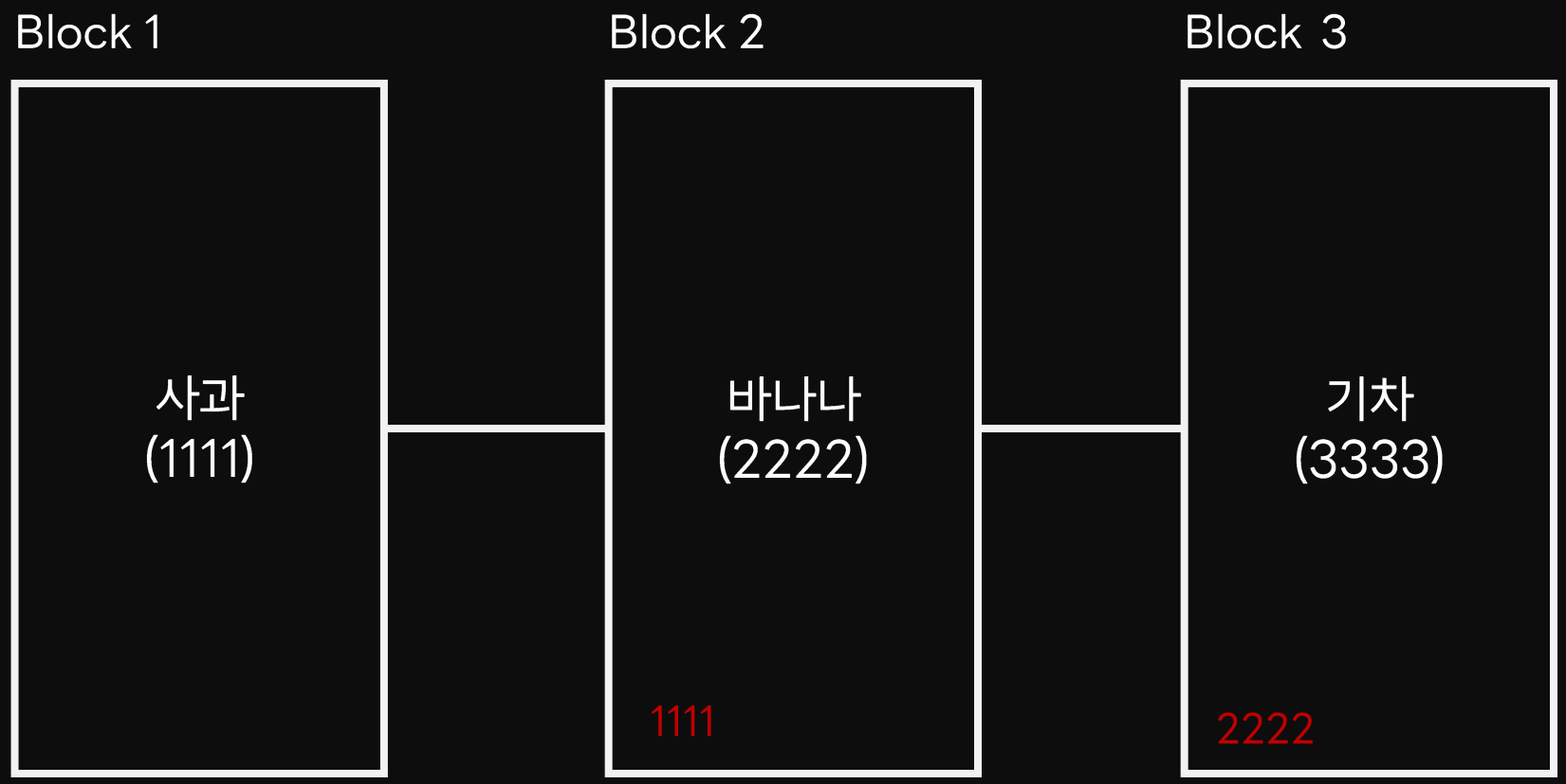
1. 데이터를 저장하는 단위

2. 각 블록은 고유한 *해시값(임의의 길이를 가진 데이터를 고정된 길이의 데이터로 변환한 결과) 존재

3. 각 해시값은 글자 하나라도 달라지면 해시값 또한 달라짐 = 무결성 검증에 주로 쓰임

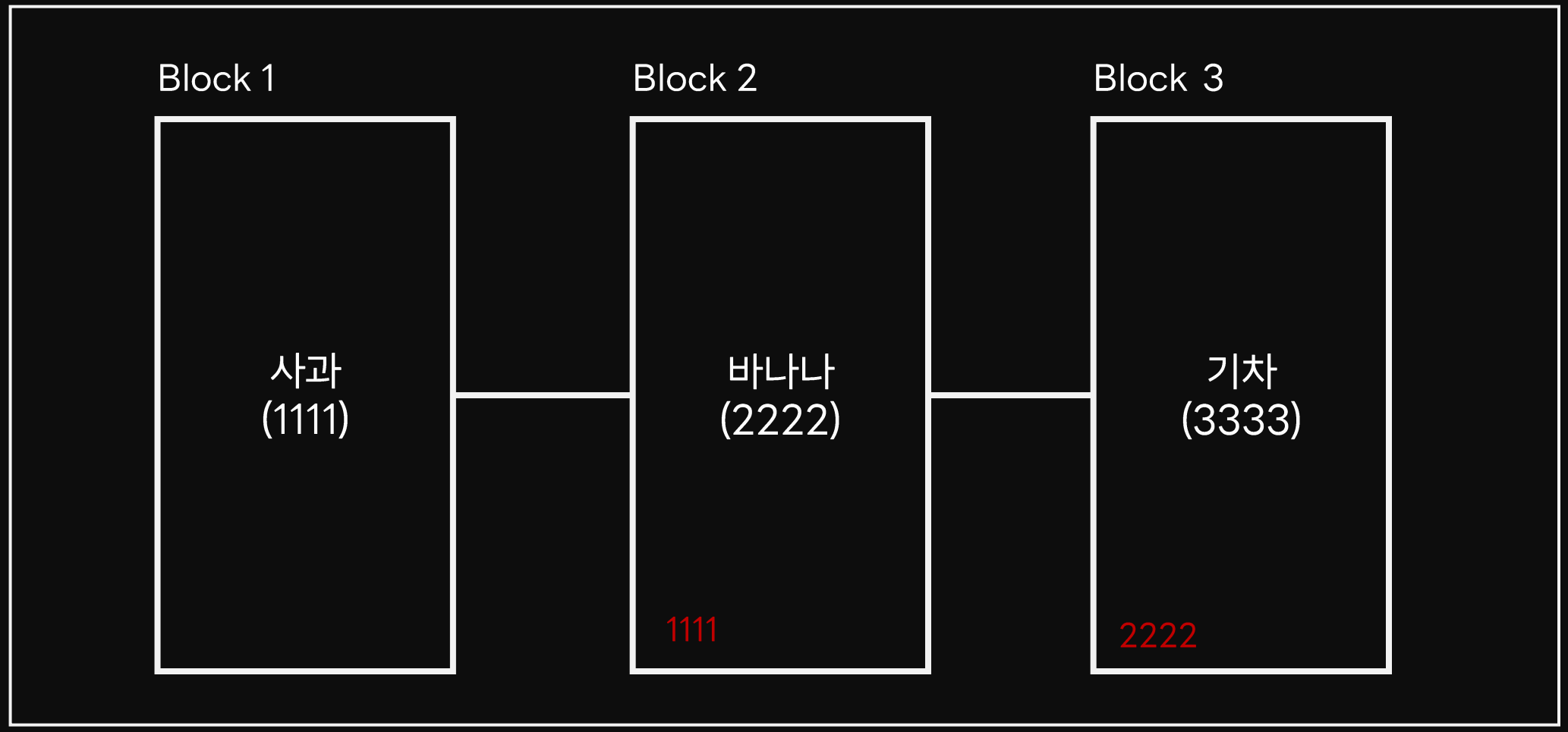


1. Blockchain?



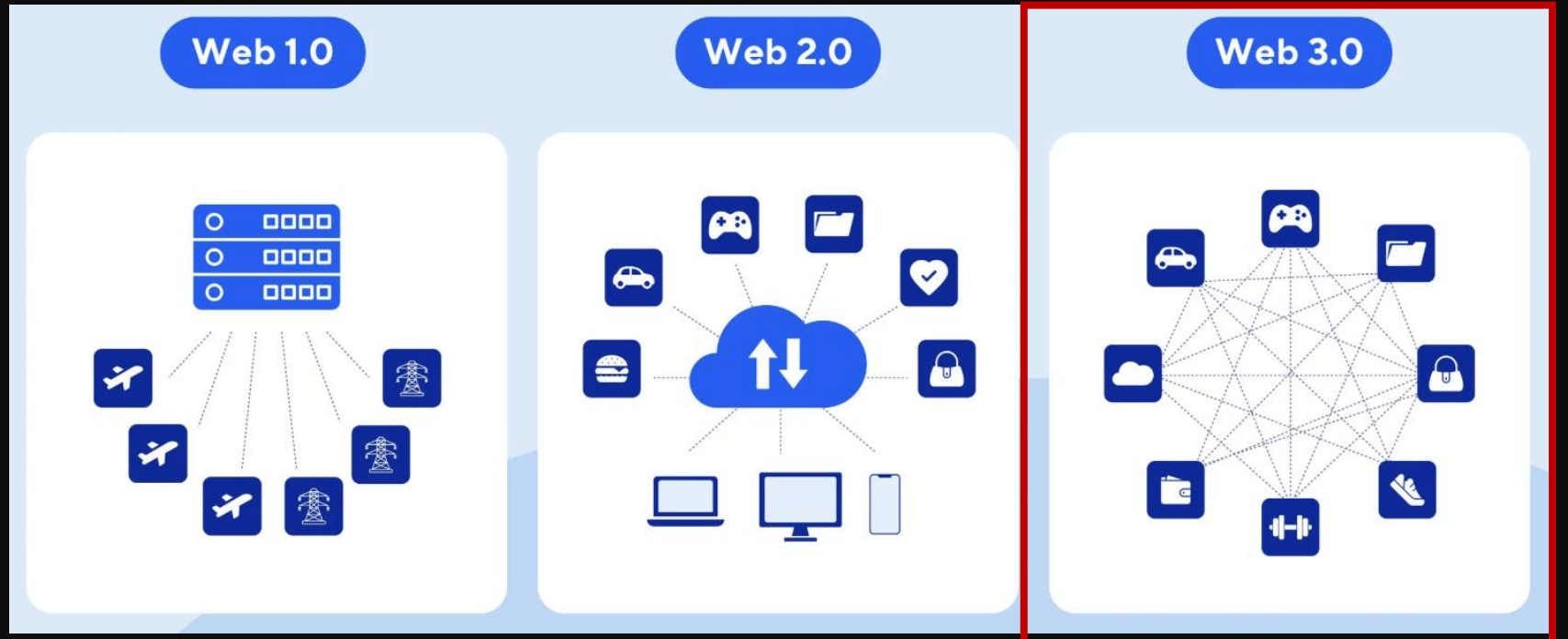
각 블록은 이전 블록의 해시값을 가지고 체인처럼 연결되어 있고 블록의 값이 달라지면 체인이 깨지게 된다

1. Blockchain?



이 전체 구조는 블록체인 네트워크에 연결되어 블록체인을 저장, 검증, 전파하는 모든 컴퓨터들에 저장되게 된다

2. Web3?



중앙 서버에서 정보를
일반적으로 제공
사용자(클라이언트)와의
상호작용 거의 없음

Ex) 단순 정보 제공 사이트

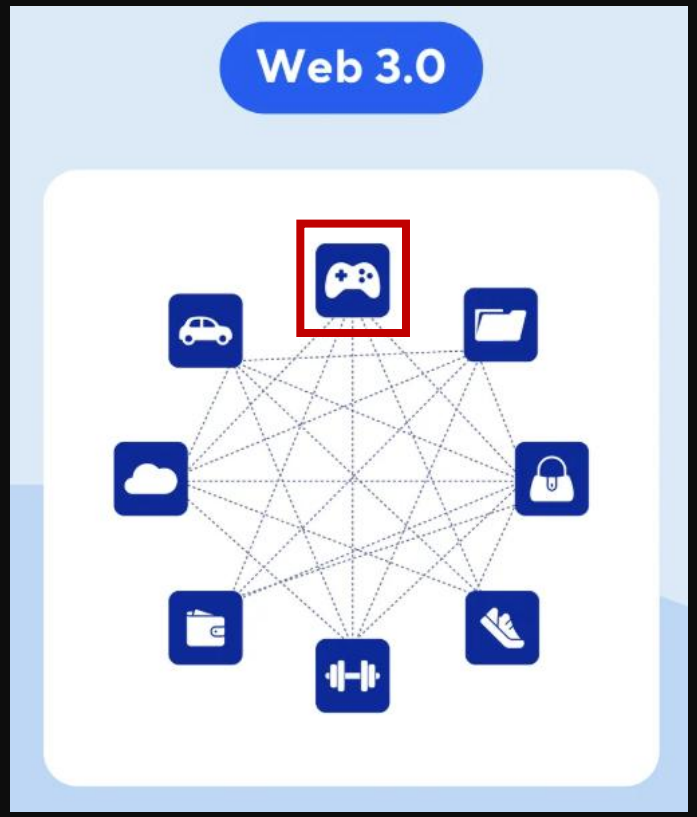
중앙 플랫폼에 데이터를
업로드, 다운로드

Ex) 유튜브, 페이스북 등

중앙 플랫폼에 데이터를
업로드, 다운로드

Ex) 블록체인 기반
Dapp
(Decentralized Application,
탈중앙화 애플리케이션)

3. Web3과 block chain



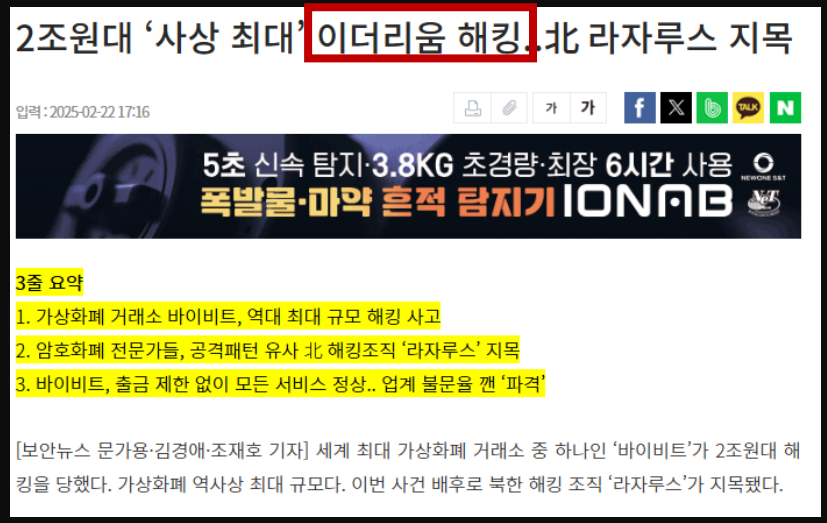
Web 3.0의 핵심 인프라가 블록체인!

이 체인이 네트워크 내 모든 노드(컴퓨터)에
복사·저장되어, 한 곳을 해킹해도 전체를 바꾸기 어려움

3. Web3과 block chain

블록체인 안전하다면서 왜 해킹 당하나?

→ 기술은 완전할 수 있어도
그걸 쓰는 사람의 실수가 있기 때문에



2조원대 '사상 최대' 이더리움 해킹..北 라자루스 지목

입력 : 2025-02-22 17:16

3줄 요약

1. 가상화폐 거래소 바이비트, 역대 최대 규모 해킹 사고
2. 암호화폐 전문가들, 공격패턴 유사 北 해킹조직 '라자루스' 지목
3. 바이비트, 출금 제한 없이 모든 서비스 정상.. 업계 불문율 깬 '파격'

[보안뉴스 문가용·김경애·조재호 기자] 세계 최대 가상화폐 거래소 중 하나인 '바이비트'가 2조원대 해킹을 당했다. 가상화폐 역사상 최대 규모다. 이번 사건 배후로 북한 해킹 조직 '라자루스'가 지목됐다.

전국이 멈췄던 '먹통사태' 1년…카카오, 안정성 확보로 신뢰회복 '박차'

최문정 기자

입력: 2023.10.15 00:00 / 수정: 2023.10.15 00:00

지난해 10월15일 SK C&C 판교 데이터센터 화재로 서비스 먹통
자체 IDC 구축 막바지·개발자 도구 이중화 등 재발방지책 마련

Web2 가 중앙 집중형이라 화재로 인해 불타자 먹통이 되었다

년도	피해액 (원)	누적 피해액
2021	1.7조	1.7조
2022	5조	6.7조
2023	2.4조	9.1조
2024	3.2조	12.4조

출처 : Certik

최근 4년 간 누적 피해액 약 12.4조(원)
추가로 2025년 1분기만의 피해액 무려 2.3조(원)

4. Ethereum

송금내역을 블록체인에 기록함으로써

사람들은 더이상 중개인인 은행을 거치지 않고

자유롭고 안전하게 거래할 수 있다

블록체인에 송금 내역이 아닌

프로그램 그 자체를 올릴 수는 없을까?

→ 이더리움 시작

4. Ethereum

smart contract (스마트 컨트렉트)

블록체인 기술을 기반으로 계약조건을 코드화 하여
계약 당사자 간의 합의 된 조건이 충족되면
별도의 중개자 없이 계약내용이
자동으로 실행되도록 하는 디지털 계약

이더리움 : 스마트 컨트렉트를 구현하기 위한 탈 중앙화 된 web3 기반 플랫폼

4. Ethereum

회사가 비행기가 2시간 이상 지연되면 보험금을 지급한다 란 계약조건이 있을 때

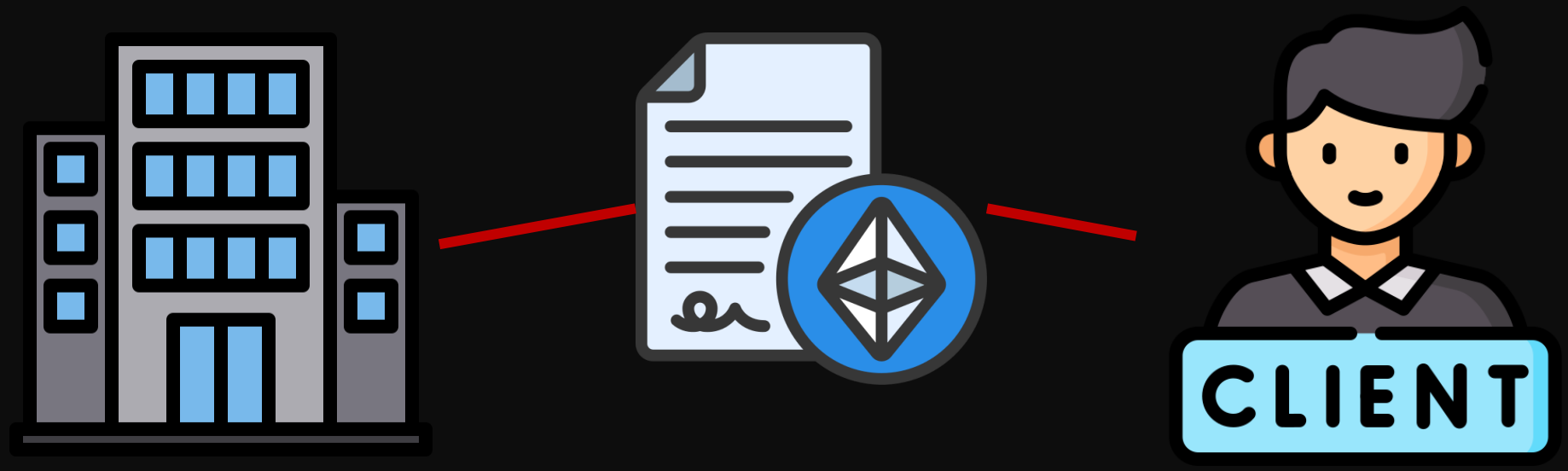
4. Ethereum

클라이언트(승객)은 직접 지연사실을 증빙해야 할 서류가 필요함

보험사가 서류 검토 후 지연 여부를 확인하고 내부 승인 절차를 거쳐야 함

항공사, 보험사, 결제기관 등 여러 중간 단계를 거쳐 결국 클라이언트(승객) 에게 돈이 늦게 지급되게 됨

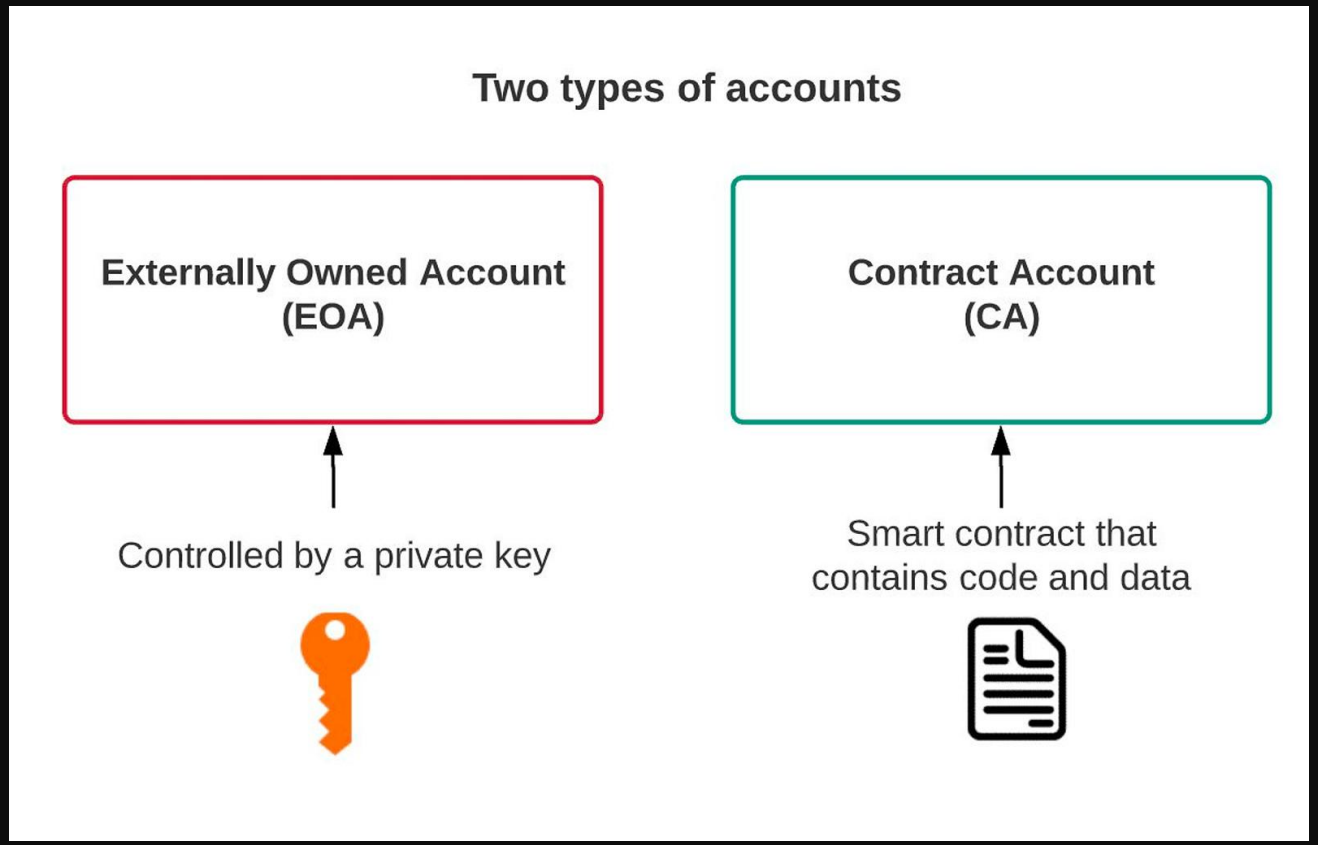
4. Ethereum



따라서 스마트 컨트렉트를 사용하면 과정이 간단해진다

다만 보험금을 저장, 송금 할 계좌가 필요하게 된다

4. Ethereum



EOA : 사람이 직접 만든 계좌 / CA : 스마트 컨트렉트의 계좌

4. Ethereum

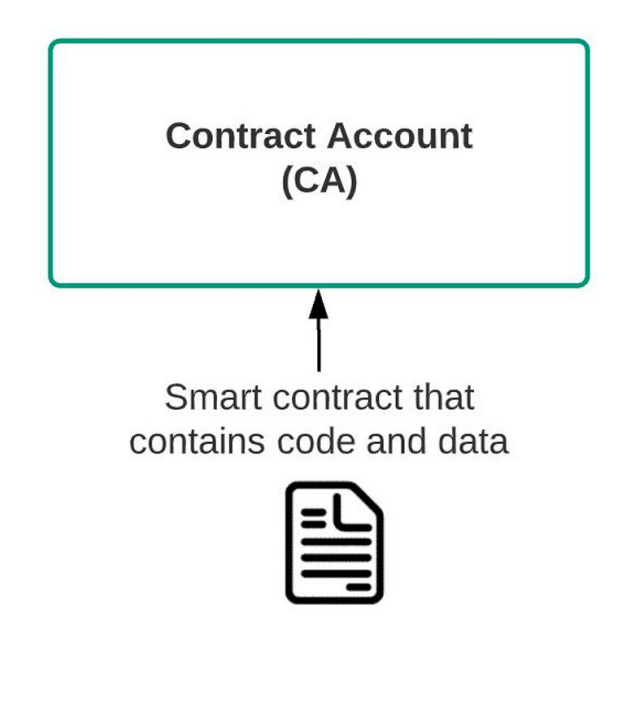
EOA (Externally Owned Account, 외부 소유 계정)

사람이 쓰는 지갑

내가 가진 비밀 열쇠(개인 키)로 여는 지갑이라서

내가 원할 때만 돈을 보낼 수 있다

4. Ethereum



CA (Contract Account, 컨트랙트 계정)

프로그램이 갖고 있는 지갑

지갑 안에는 돈도 있고 자동으로 실행되는 약속(코드)도 들어 있다

스스로는 움직이지 않고, EOA 같은 외부에서 명령을 주면

코드에 따라 자동으로 돈을 보내거나 일을 처리한다

4. Ethereum

트렌젝션 = 블록체인에 어떤 행동을 요청하는 메시지

악성 사용자가 앞으로 생길 모든 블록에 쓸데없는 트렌젝션을 계속 날리게 되면
정말 필요한 사람의 트렌젝션 처리가 느려지고 네트워크 마비가 발생한다

이를 막을 수 있는 것 = 가스 (GAS)

4. Ethereum

가스 (GAS)

이더리움 이더로 지급 가능하며

트렌젝션을 처리하거나 프로그램을 실행시키기 위한 연료(비용)

4. Ethereum

이더 (Ether) : ETH로 표기

ETH = 이더리움 네트워크에서 거래·연산·보안의 중심 통화

1. 거래수단 : 사용자가 이더를 지갑에 보관하고, 다른 지갑으로 송금이 가능
2. 가스지불 : 트렌젝션이나 스마트 계약을 실행할 때 필요한 수수료 지급

4. Ethereum

ETH = 돈

Gas = 일을 시킬 때 드는 수수료 계산 방법

Account = 돈을 보관하고 거래하는 주체 (사람 계정, 프로그램 계정)

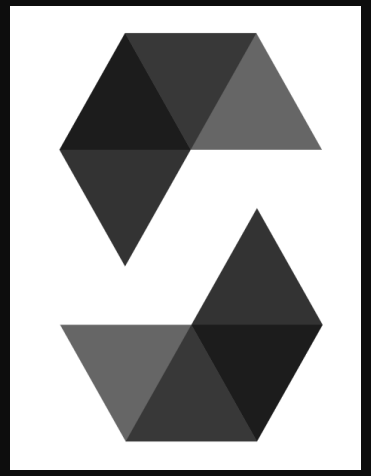
4. Ethereum

블록체인 : 거래 기록을 여러 컴퓨터가 공동으로 보관하는 분산 시스템

비트코인 : 세계 최초의 블록체인 기반 암호화폐

이더리움 : 블록체인 기술을 확장한 2세대 암호화폐이자, 분산 애플리케이션 플랫폼

5. Solidity



이더리움(Ethereum) 개발을 위한 프로그래밍 언어

→ 자바와 유사

5. Solidity

돼지 저금통에 이더를 저장하고 인출하는 스마트 컨트렉트 구현