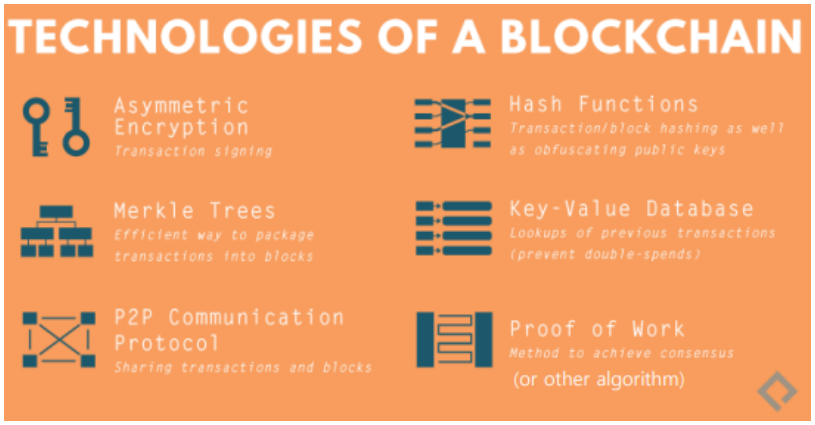
W1. Intro

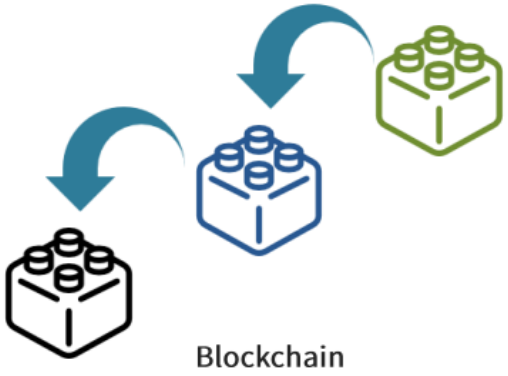
▼ 1-2 블록체인의 핵심 기술

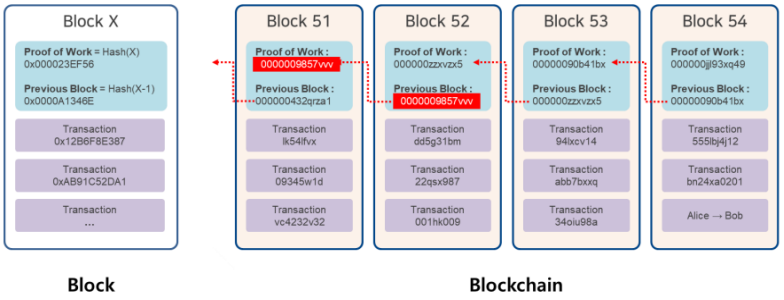
- 블록체인 핵심 기술



  - 비대칭 암호화 기술 : 트랜잭션 서명을 위해 사용
  - 해시 함수 : 트랜잭션과 블록 해싱을 위해 사용
  - Merkle Tree : 트랜잭션을 블록으로 효율적으로 패키징하는 기법
  - Key-Value Dadabase : 이전 트랜잭션을 조회함
  - P2P 통신 프로토콜 : 거래 및 블록 데이터 공유
  - 합의 달성을 위한 업무 증명(Proof of Work)

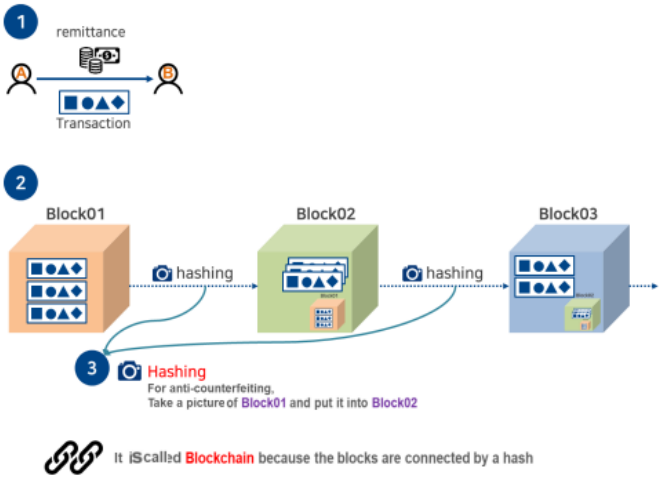
- **블록체인(Blockchain)**





- 하나씩 차례로 연결된 블록 그룹을 의미함
- 새 블록은 이전에 구축된 블록체인의 뒷면에 추가되며 이 과정은 정기적으로 반복됨
  - 비트코인의 경우, 매 10분마다 새로운 블록이 생성됨
- 새 블록이 만들어지면 이전 블록에 연결하기 위해 링크가 만들어짐 → 연결된 블록이 있는 블록체인이 형성됨
- 연결된 블록은 영구적으로 저장되며, 그 안에 있는 *트랜잭션 레코드(거래 장부)는 편집할 수 없음
  - 누가 얼마나 많은 코인을 누구에게 보냈는지에 대한 데이터
  - 당사는 이러한 거래 기록들을 수집하여 저장용 상자에 보관하는데 이 상자를 블록이라고 함

- **블록체인 Hashing 기술**

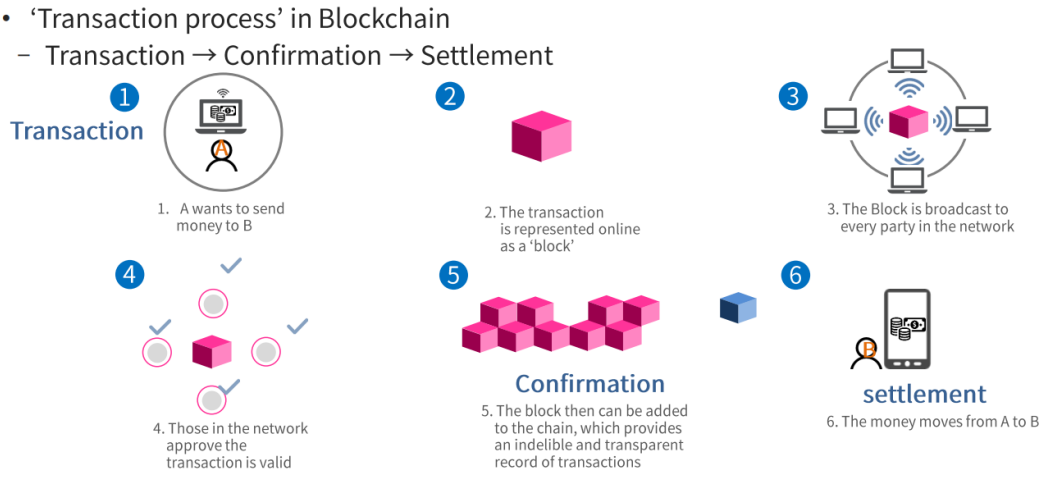


- 블록01이 가득차면 해시값이 작성됨 Hashing은 블록의 데이터를 특수 번호로 변환하는 과정을 말하고, 변환된 값을 해시 값이라고 함 이는 상자의 사진을 그대로 찍고 다음 블록에 그 그림을 넣는 것과 같음
- 내용이 약간이라도 변경되면 해시 값이 바뀌기 때문에 위조 여부 확인에 용이함
- 블록1, 블록2의 해시 및 트랜잭션 데이터가 기록된 후 블록3은 그림 02를 다시 기록함

  >> 결국 블록을 해킹하기 위해서는 01상자를 해킹하고 그런 다음 모든 상자의 그림을 변경해야 함

  >>> 여러 상자가 연결되어 있으므로 위조하기가 매우 어려움!

- **블록체인에서의 전자 결제 전송 과정**
  - 거래 이전 → 송금 확인 → 송금 정산



A가 B한테 비트코인을 전송하기 위해 필요한 트랜잭션을 생성함. 이 트랜잭션에는 전송할 금액과 B의 공개키(주소)가 포함됨
A는 자신의 개인 키로 이 트랜잭션에 서명을 등록함 이 서명은 A가 이 트랜잭션의 소유자임을 증명하는 역할을 함
서명이 포함된 트랜잭션은 네트워크로 전파됨
마이너(채굴자)는 새로운 블록을 채굴하여 네트워크에 전파함
마지막으로 비트코인을 받은 B가 자신의 지갑에서 트랜잭션 세부 사항을 승인하고 전송 완료됨

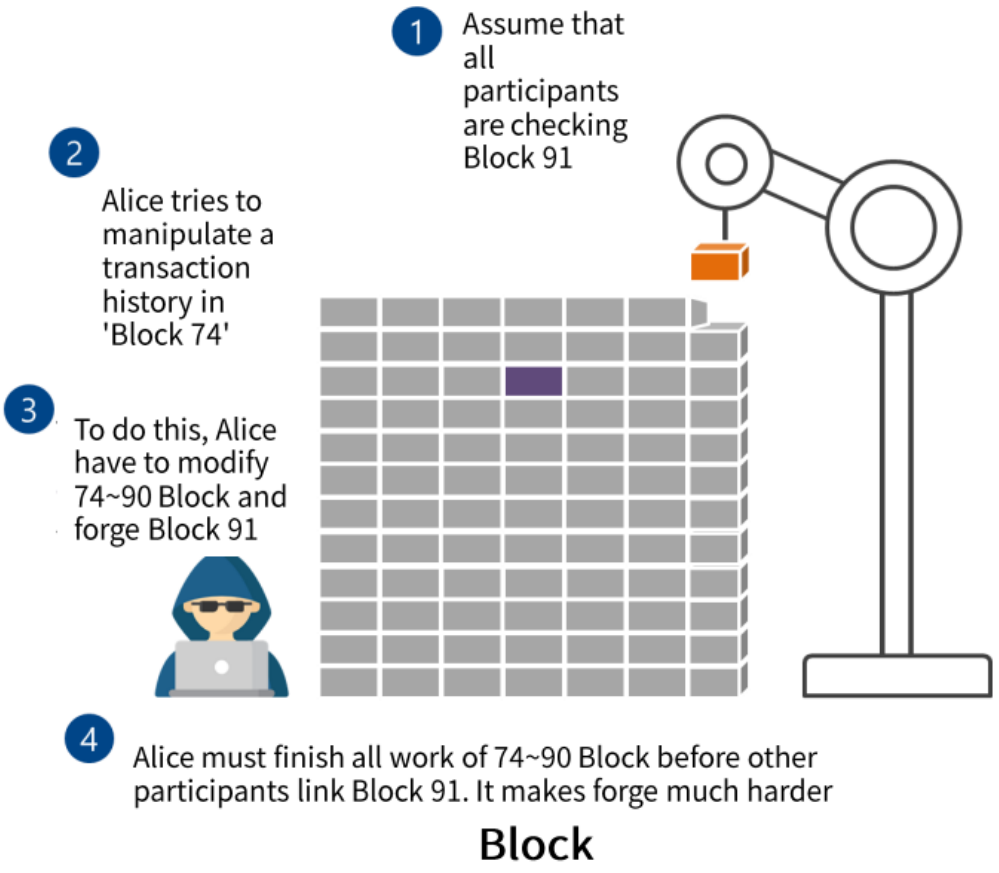
1. A가 개인 키를 사용해 트랜잭션을 신청함
2. A의 전송 트랜잭션 세부 사항은 다른 트랜잭션 세부 사항과 함께 새로운 블록에 포함되며, 이 블록의 해시 값을 계산함
3. 마이너는 새로운 블록을 성공적으로 채굴하기 위해 필요한 타깃 해시를 계산하고, A의 전송 트랜잭션을 포함한 이 블록을 네트워크에 전파함
4. 네트워크 참여자들은 수신된 블록의 유효성을 검사하고 합의에 도달할 수 있음
5. 이 새로운 블록에 포함된 전송 트랜잭션은 이전 블록과 연결되어 블록체인 상에 저장되며, 전송이 한 번 확인됨
6. 전송 트랜잭션 A의 수신자, B가 전송 확인을 확인하면 트랜잭션이 완료되고 전송이 확인됨

1 ~ 5 단계는 블록체인의 길이를 연장하면서 계속 반복됨

- 비트코인 시스템은 각 전송에 총 6(60분) 번의 전송 확인을 받아야 함

  거래 내역이 포함된 블록 다음에 5개의 블록이 추가로 연결되며, 수취인이 이체를 확인하면 트랜잭션이 완료됨

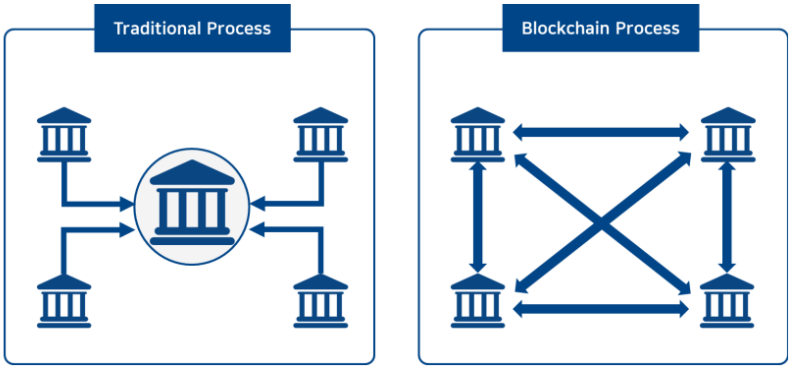
- 블록체인 위조가 어려운 이유



90개의 블록이 생성되어 연결되었을 때, 어떤 참가자가 block 74에서 트랜잭션 기록을 수정하고 싶다고 하자.
그럼 그는 17개 블록의 모든 컴퓨팅 비용을 지불하고 위조해야 한다.
또한, 이 작업은 다른 참여자가 block 91을 완료하기 전에 수행되어야 한다.
따라서 트랜잭션 기록을 조작하는 것은 거의 불가능하다.

- 블록체인의 핵심 특징
  - 분산 분권화 (decentralized management)
  - 데이터의 공유 → 거래 투명성
  - 트랜잭션 데이터의 불변성

    데이터가 블록체인에 기록되면 해당 데이터를 제거하거나 수정할 수 없음



▼ 1-3 블록체인의 한계와 활용 범위

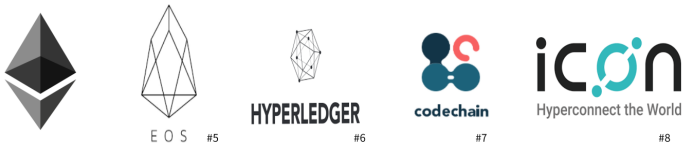
- 비트코인의 한계
  1. 작동하는데 엄청난 비용이 듦
     - 전기량 多
     - 마이닝이라고 불리는 프로세스를 거치며 마이닝 비용이 들고, 마이너가 새로운 블록을 성공적으로 찾으면 네트워크에서 보상으로 비트코인을 지불해야 함
     - 통화를 사용하려면 거래 수수료가 발생함
  2. 거래확인에 오랜 시간이 걸림 → 실시간 결제 수단으로 사용 어려움
     - 한 블록을 생성하는데 약 10분이 소요되는데, 거래에 최소 6개의 블록이 필요하므로 최소 60분이 필요함
  3. 초 단위로 생성할 수 있는 트랜잭션 수가 너무 작음
  4. 한 블록에 포함될 수 있는 트랜잭션 수가 한정되어 있음
  5. 암호화폐 거래 정보만(트래랜잭션 정보만) 블록에 저장 가능함

     계약에 관련된 정보는 저장 불가
  6. 스마트 계약 부적합

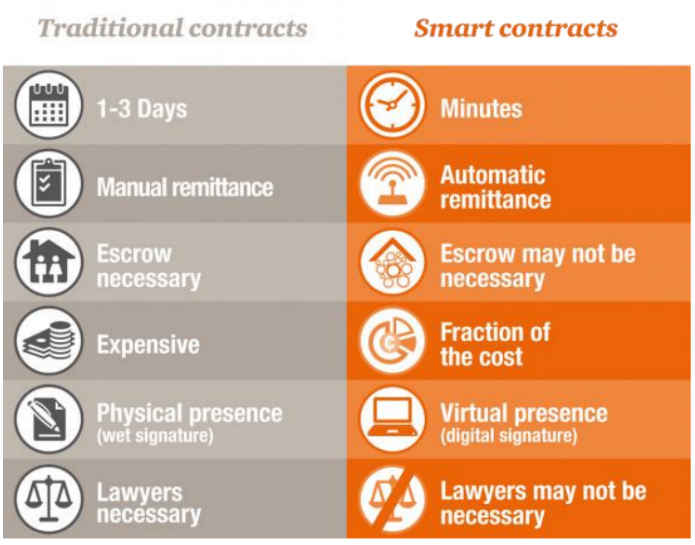
     비트코인의 스크립트 언어가 제한적이라 복잡한 계약 조건을 표현하기 힘듦 따라서 복잡한 스마트 계약을 실행하거나 저장하기 부적합함

- 블록체인 종류
  - 블록체인의 또 다른 응용 → 스마트 계약

- 비트코인의 한계를 극복하기 위해 다양한 블록체인들이 등장함



- **스마트 계약**



#9

  - 스마트 계약은 자가 실행 계약으로, 컴퓨터 코드로 작동하고 자체 시스템으로 실행되어 개시된 후에는 사람이 직접 입력하지 않아도 수행됨
  - 준비와 실행이 빠름
    - 자동 송금을 설정할 수 있고, 에스크로가 필요하지 않을 수 있음
  - 비용이 저렴함
    - 변호사와 같은 관련 당사자가 필요하지 않음

- AI 혹은 블록체인 기술을 적용할 때 고려할 점
  1. 지금까지 해결하지 못한 난제를 해결할 수 있는가
  2. 기업은 자본 지출 또는 운영 비용을 줄일 수 있는가
  3. 고객에게 더 나은 서비스를 제공할 수 있는가

4. 새로운 수익 창출을 위해 새로운 서비스를 만들 수 있는가

- 블록체인 유형
  - 공개(public) 블록체인
  - 비공개(private) 블록체인

- **공개 블록체인**
  - *노드(특히 마이닝 노드)가 누구의 허가 없이 블록 마이닝에 참여할 수 있음

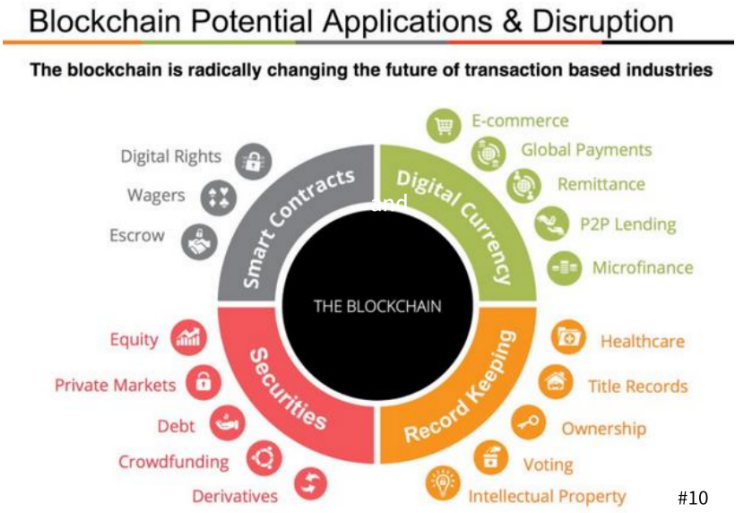
    즉, Non-permissioned

    - 노드(Node): 네트워크 상에서 활성화된 참여자를 의미함 각 노드는 분산된 컴퓨터나 장치로서 전체 네트워크에 연결되어 있는 중요한 역할을 함
  - ex) Bitcoin, Ethereum

- **비공개 블록체인**
  - 개인 또는 허가된 블록체인에서 합의를 위해 마이닝에 참여할 수 있는 권한이 필요함
  - 대부분의 엔터프라이즈 응용 프로그램이 사용함

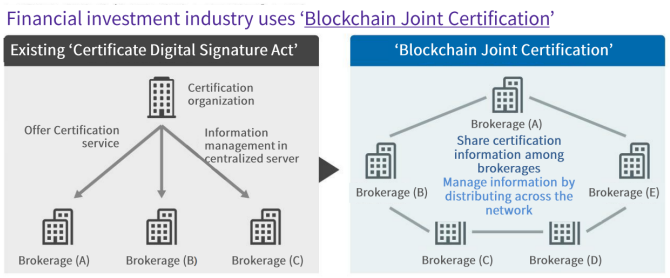
    ex) Hyperleader, Microsoft Blockchain as Service(MS BasS)

- 블록체인 활용 분야



- 블록체인 상용 서비스

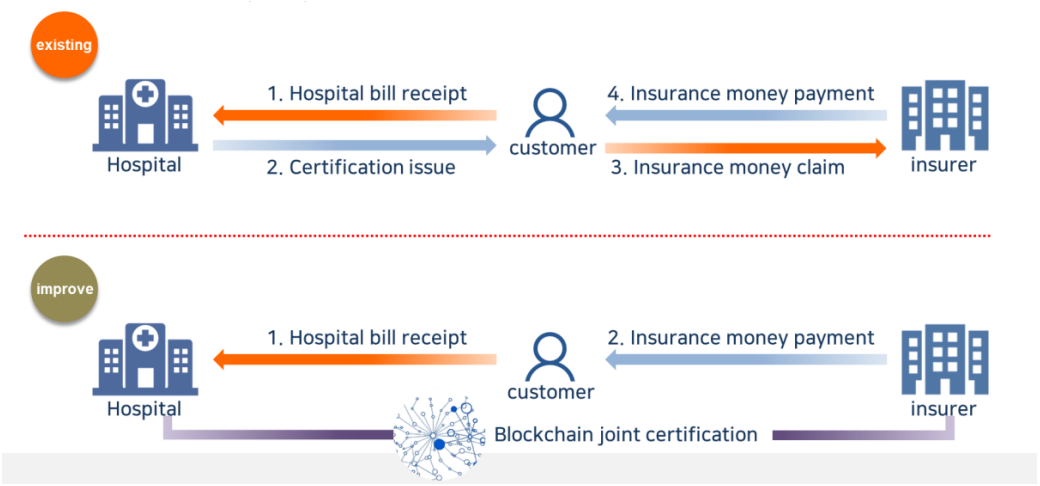
1. 금융 서비스_CHAIN ID



  - 정부에서 발행하는 기존의 공인인증서를 대신하여 인증 서비스를 제공하는 블록체인 기반의 금융 투자 지역 공동 인증 서비스

기존의 공인인증서	Chain ID
중앙 서버에 의해 관리됨	탈중앙화
금융 소비자는 새로운 금융 기관과 거래를 시작할 때마다 인증서를 다시 발급받아야 함	3년마다 인증서 갱신할 수 있음 보안 회사에서 새 계정을 개설할 때마다 발급받을 필요 없음

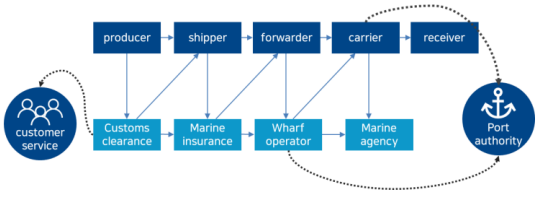
2. 보험금 자동 지급 서비스



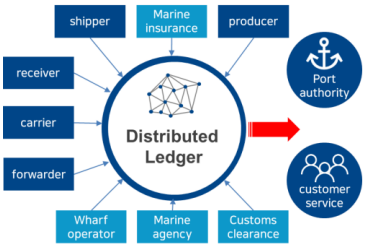
- 보험 가입자가 병원에서 진료를 받고 간단한 절차(휴대폰 터치)로 보험금을 청구하는 시스템
- 블록체인 기술을 통해 분산 원장에 등재된 보험계약을 활용하는 서비스로, 보험금 지급 조건 충족 시 의무기록 사본과 보험금 청구서가 자동으로 생성돼 보험사에 전달됨

기존의 시스템	블록체인 기반 시스템
가입자가 의료 보험 혜택을 받기 위해서는 병원 치료 후 받은 영수증 및 문서들을 보험사에 제출해야 함	병원 기록 및 보험 회사의 분석, 인증 및 지불 계약을 자동으로 추출함
프로세스가 복잡하고 불편하며 처리하는 데 오랜 시간이 걸림	전체 프로세스가 보험 계약자 및 병원의 블록체인에서 투명하게 기록 및 처리됨

3. 해상 운송 및 무역



Current EDI structure



Blockchain based structure

- 기존의 EDI 시스템의 문제

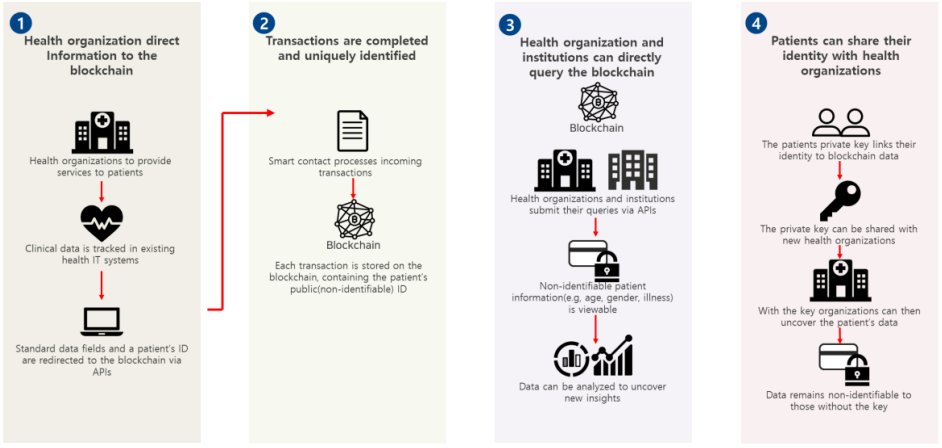
- 물류 운송을 위해 여러 단계와 기관을 거쳐야 함
  - 글로벌 공급망이 복잡해지고 범위가 확장됨에 따라 물류 요원이 처리해야 하는 업무 증가함
- 수입/수출 업자의 경우 과잉재고가 발생하고 화물량이 늘어남에 따라 행정 처리가 중복되고 있음 항구의 가시성 확보가 힘듦
- 문서 처리 시간이 실제 문서 이송 시간보다 김

- 블록체인 기반 EDI 시스템 장점

1. 컨테이너 운송, 항구 및 물류 전반에 대한 가시성을 확보할 수 있음
   - 블록체인 기술은 제품 생산자, 운송업자, 부두 운영자 및 수취인뿐만 아니라, 세관 및 항만 당국을 포함한 모든 컨테이너 국제 운송 참가자가 공유하는 원장을 사용해 가시성을 획기적으로 향상시킴

2. 운송 거래가 종이 없이 이루어지므로 용지 관리 비용과 시간을 절약할 수 있음
   - 블록체인 기반 솔루션은 위조를 방지하고 사기 거래 소스를 차단함으로써 데이터 교환을 크게 줄임 → 비용 절감

4. 의료 데이터 관리



- 기존의 의료 시스템
  - 환자 데이터가 의료 기관, 실험실, 보험사 등에 분산되어 있어 제한된 기준으로 정보를 공유함

>> 의료기관이 환자의 과거 데이터를 입수하여 환자를 정확하게 진단하고 추가 검사 및 촬영을 실시하기 어려움

>> 실험실은 데이터 부족으로 연구에 어려움을 겪음

>> 보험 회사는 의료 서비스 제공자와 문서를 교환해야 하는 처리 과정 때문에 보험료를 지불하는 데 오랜 시간이 걸림

- 블록체인 방식의 의료 시스템
  - 의료 데이터 공유 기능 사용

    >> 다양한 의료 기관에서 다른 기관의 환자 기록을 보고, 불필요한 검사 또는 사진을 삭제하여 정확한 평가를 수행할 수 있음

    >> 실험실은 많은 환자의 의료 데이터를 사용해 적극적으로 연구 수행할 수 있음

    >> 보험사는 즉시 의료 정보를 확인하여 처리 시간을 단축할 수 있음

    >> 환자는 자신의 데이터를 제공하여 필요할 때 의료 기록을 확인할 수 있으며, 돈이 도입되면 혜택을 볼 수 있음