1. 블록체인의 개념

블록체인은 블록에 데이터를 담아 체인 형태로 연결한 뒤, 수많은 컴퓨터에 이를 동시에 복제•저장하는 분산형 데이터 저장 기술이다. 기존에는 거래 내역, 진료내역 등과 같은 데이터를 단일 조직(정부 기관, 은행 등)이 기록하고 관리하였지만, 블록체인은 데이터를 분산시켜 투명하게 공개하기 때문에 조작이 불가능하다. 따라서 신뢰성 높은 중앙 기관의 개입 없이 P2P 거래가 안전하게 가능하다.

1.1 특성

- **분산화**: 중앙집중식 시스템과는 달리 제 3의 신뢰기관을 요구하지 않음.

- **불변성**: 체인상의 트랜잭션은 신속하게 검증될 수 있으며 유효하지 않은 트랜잭션은 블록체인의 노드들에 의해 받아들여지지 않음. 일단 트랜잭션이 블록체인에 기록되면 해당 내용을 삭제하거나 수정하는 것이 거의 불가능.

- **익명성**: 각 사용자는 자신이 유사 익명 주소로 블록체인과 상호 동작. 이 주소는 사용자 실체 신원 식별 정보가 포함되지 않아 익명성이 보존될 수 있음. 하지만 트랜잭션 내용을 모두 공개하므로 트랜잭션 익명성은 보장될 수 없음.

- **추적성**: 모든 트랜잭션은 블록상 노드들에 할당된 이전 미사용 트랜잭션에 참조됨. 따라서 모든 트랜잭션은 쉽게 확인하고 추적할 수 있음.

1.2 종류

블록체인은 접근/권한에 따라 크게 퍼블릭 블록체인과 프라이빗 블록체인 두가지로 나눌 수 있다.

퍼블릭 블록체인은 제한없이 불특정 다수 누구나 운영하고 참여할 수 있기 때문에 투명성이 보장된다. 하지만 그만큼 데이터가 많은 컴퓨터에 복제되어야 하므로 거래속도가 느리고, 네트워크 확장이나 수정 등의 업그레이드가 느리다. *Ex) 비트코인, 이더리움*

프라이빗 블록체인은 검증된 사람만 참여할 수 있어, 투명성이 낮지만 처리 속도가 빠르고 모안 측면에서는 상대적으로 우위에 있다. 또한, 네트워크의 규칙 또는 거래 내용 수정이 가능해 업그레이드 및 잘못된 계약에 대한 정정도 상대적으로 쉬움. *Ex) 리플, 아이콘*

→ 소수의 기관(기업, 플랫폼 등)에 의한 데이터 독점 방지. 공익 실현 가능. 해킹 거의 불가능. 공정계약 가능.

2. 활용 (출처: https://luniverse.io/2021/01/25/ten-blockchain-usecases/?lang=ko)

2.1 금융

2.1.1 암호화폐

암호화폐는 가장 많이 활용되는 분야이다. 블록체인 기반 네트워크의 참여자로서 진정성을 보여주기 위해 특정한 형태의 작업 증명을 제시하고, 이에 따라 새로운 코인을 생성해 보상받으며 상호 거래내역을 검증하는 화폐이다.

이론적으로는 해킹이 불가능하여 보안 및 안정성에 대한 장점을 가진다. 하지만 익명성으로 인해 불법 자금 세탁 등 범죄에 악용되는 사례가 있으며, 불안정한 가격 변동성, 투명성으로 100% 보장되지 않는 익명성, 에너지 소모 등의 문제점이 존재한다.

~~2.1.2 NFT -> 다음 PT 준비~~

2.2 장외주식거래 주주명부관리

국내에 비통일주권을 거래할 수 있는 별도의 플랫폼은 거의 없었다. 거래를 위해선 거래 게시판을 이용해 직접 매도자와 매수자를 찾아야 하는데, 거래 방법이 번거롭고 거래를 보증해주는 주체가 없기 때문에 신뢰하기 어렵다는 단점이 있다. 개인간의 거래는 위변조 가능성이 높을 뿐 더러, 즉각적으로 주주명부에 반영되기 어렵고 먹튀와 같은 각종 리스크가 존재한다. 이에 블록체인을 적용하여 주권 발급 및 주주명부 등 문서작업을 간소화하고 데이터 안정성을 보장한다.

2.3 식품 원산지 추적

최근 블록체인 기술을 활용해 식품의 원산지와 유통 정보 등을 확인할 수 있는 식품 안전망 시스템이 진화하고 있다. 기존의 불투명한 원산지 기록으로 인해, 시금치를 먹고 대장균 환자와 사망자가 속출했던 사건이 있었다.

이러한 피해를 줄이기 위해 유통시장이 블록체인 기술을 도입해 소비자의 신뢰 확보에 나서고 있다. 농장부터 시작해 보관창고, 그리고 운송 경로 등에 IoT 태그를 부착하여 원산지, 보관 온도, 유통기한 등 모든 유통과정을 블록체인에 실시간으로 업데이트함으로써 소비자들에게 투명하게 공개하였다.

2.4 이 외 분야

이 외에도 **보험금 청구**(병원 서류가 블록체인에 기록되어 간편하게 보험금 청구 가능), **의약품 관리 및 추**

적(유통 중 발생할 수 있는 다양한 문제점 해결 가능), **청산결제**(증권시장에서 2영업일이 걸리지 않고 당일 청산 가능), **온라인 중고 거래 플랫폼**(모든 거래 내용이 블록체인에 기록되어 범죄 입증과 예방 가능), **무역**(운송 과정에 필요한 수많은 서류와 승인정보를 관리 및 처리함으로써 시간과 비용 절감), **건강여권**(코로나 검사결과를 저장 가능), **전자 계약서 관리**(나라마다 상이한 전자계약 관련 법과 제도를 반영해 신뢰도 높은 계약관리 체계 확보 가능), **포인트 통합 시스템**(모든 기업의 포인트 시스템을 통합시켜 한 곳에서 관리 가능) 등에 활용 가능하다.

→ 위/변조가 불가능하고 투명성을 가졌다는 점을 이용한다는 것이 핵심.

3. 문제점

- **효율성 문제**: 데이터가 업데이트될 때마다 계속해서 복제해야 하므로 서버 전체의 효율이 떨어질 수 있음.

- **데이터 관련 취약점**: 참여자들이 잘 분산되어 있는 것이 이상적이지만, 특정 그룹이 50% 이상의 노드를 소유하면 변조 가능하다는 취약점 존재.

- **프라이버시 이슈**: 기록된 데이터 수정은 거의 불가능하므로, 지우고 싶은 데이터가 있어도 불가능.

- **악용 가능성**: 불법 거래대금 결제, 비자금 조성, 탈세를 가능하게 함.

그 외에도 **책임소재 모호, 완벽한 익명성 보장 불가능, 개인키의 해킹과 분실 해결 불가능, 실시간 및 대용량 처리 어려움**의 문제가 있음.

3.1 해결방안 (출처: 금융보안원)

기능		문제점	해결방안
알고리즘 기능강화	협의 가로채기	• 참여자 과반수를 장악하여 블록체인 합의과정조작	• 비정상 참여자 모니터링 • 거래검증 • 거래처리량 제한
	비정상 거래	• 메인체인에서 유효하지 않은 거래 발생	• 합의통합 • 유효성 체크
	SW 취약점	• 블록체인 SW의 보안취약점으로 인해 키 도난, 합의조작 등에 악용	• Secure Coding • 합의 알고리즘 보완 및 개선
	가용성 저하	• 블록체인 처리속도 한계와 거래량 증가로 인해 가용성 저하	• 유효성 검증 참여자 제한 • 선택적 거래정보 저장
공격대응 능력강화	비정상 거래	• 사기거래, 자금세탁, 이중지불 등의 거래 발생가능	• 거래 허용 참여자 관리
거래소 보안강화	키 관리강화	• 암호화폐거래소나 핫월렛 사용으로 인한 키 탈취	• 콜드월렛 • Multi-factor 인증
	거래소 인프라 강화	• 국내 대형 암호화폐거래소의 지속적인 해킹사고	• 기본 보안수칙 강화 • 보안인증강화(ISMS-P, ISO27001등) • 자산의 70%이상 콜드월렛에 보관