



# Blockchain & Cryptocurrency

## 개요

블록체인 개요

가상화폐

중앙은행의 디지털 화폐 시장 동향

## Episode of First Bitcoin Transaction

- 플로리다의 Laszlo Hancyecz는 다음과 같은 제안을 게시  
"2010년 5월 22일에 10,000BTC로 피자 두개를 살 것이다."  
여기서 피자의 현재 가치는 \$187M이다.  
BTC 당  $\$ 18,777 * 10,000 = \$ 187,000,000$ (2020年12月)  
10년 동안 \$30의 620만 번  
※ 수취인 제레미는 주당 10,000 BTC를 각 \$400, \$,000,000에 매각함

## 블록체인 개요 Blockchain Overview

- 블록체인은 암호화로 서명 된 거래의 분산 디지털 원장
- 각 블록은 유효성 검사 후 이전 블록에 암호화 방식으로 연결
- 새로운 블록 추가 시 이전 블록을 수정하기 더 어려움 (**변조방지 생성**)
- 새로운 블록은 네트워크 내 원장 사본과 충돌에 복제되며, 이중 지불 문제를 포함하여 설정된 규칙을 사용하여 자동으로 해결

## Four Characteristics to Build Trust

- 안전한 암호화 : 블록체인은 암호화 보안
- 원장만 추가 : 전체 거래 내역 제공
- 공유 원장 : 원장이 여러 참여자 사이에 공유
- 분산 원장 : 블록체인 분산 가능

## Key Components of Blockchain

원장 : 거래 내역을 추적하기 위한 거래 모음

**암호화 해쉬 함수**: 블록체인을 수학적으로 안전하게 생성

- 입력 데이터를 가져와 데이터를 해시하고 동일한 결과를 생성하여 데이터에 변경사항이 없음을 증명
- $\text{hash}(x) = \text{동일한 } Y, \text{ digest}$  (요약, 소화하다 → 쉽게는 블록체인 결과값)
- 계산적으로 거의 불가능한 세가지 특성

**Preimage resistant**: 다이제스트가 되는  $x$  찾기

**Second preimage resistant**:  $x$ 가 주어지면 두번째 입력을 찾고  $\text{hash}(x) = \text{hash}(y)$ 가 되는  $y$ 를 찾음

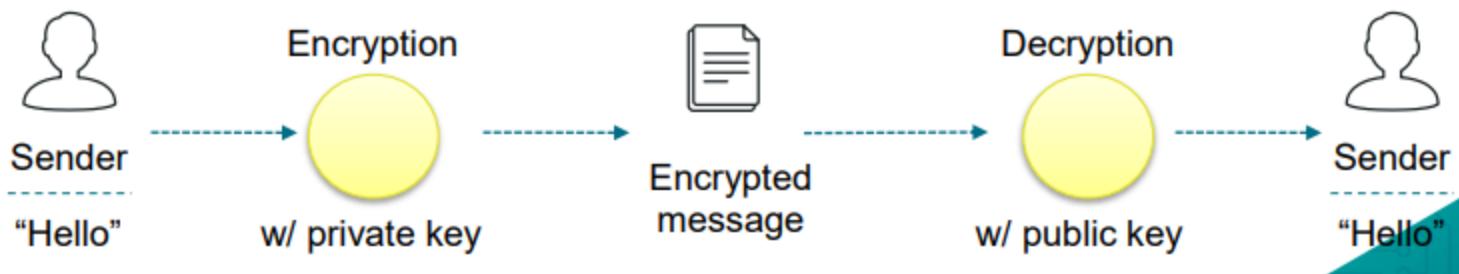
**Collision resistant**: 동일한 출력에 대한 두개의 입력을 찾고  $\text{hash}(x) = \text{hash}(y)$ 인  $x, y$ 를 찾음

- **비대칭 키 암호화(공개 및 개인키)** **Asymmetric-key cryptography (Public & Private Key)**

메커니즘을 제공함으로써, 서로를 신뢰하지 않는 사용자들 사이의 신뢰관계가 무결성과 신뢰성을 검증 할 수 있음

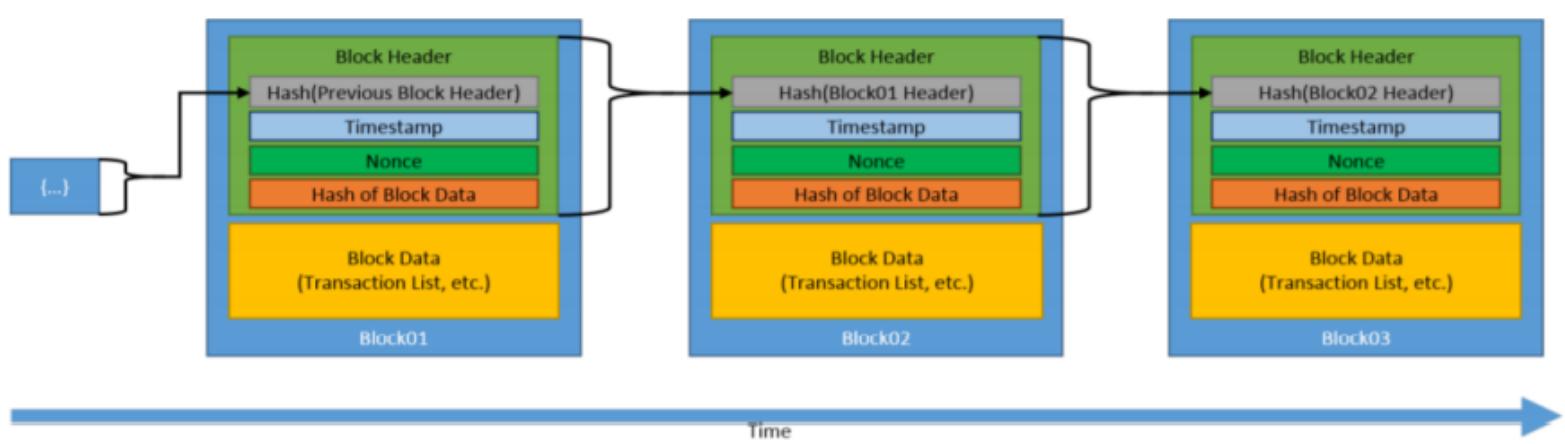
- 키 사용법

개인키는 디지털 서명에 이용, 공개키는 주소를 파생하고 개인키로 생성된 서명을 확인하는 데 이용



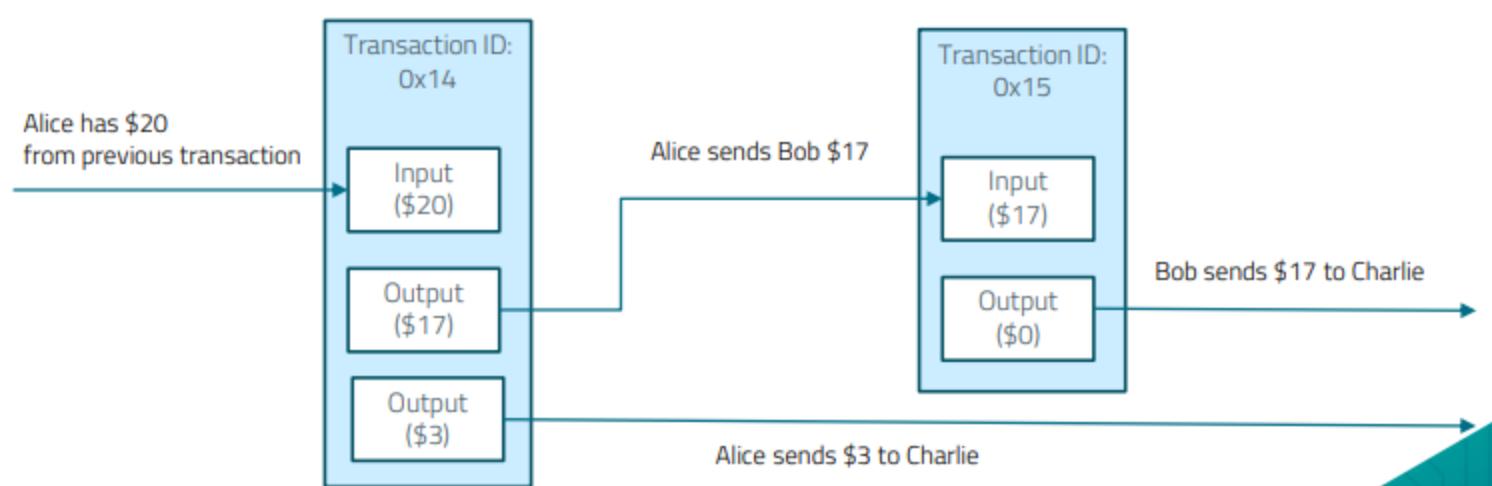
## Block

- 블록 헤더와 블록 데이터를 포함
  - 블록 헤더에는 이 블록에 대한 메타 데이터가 포함
  - 블록 데이터에는 검증되고 인증 된 거래 목록이 포함



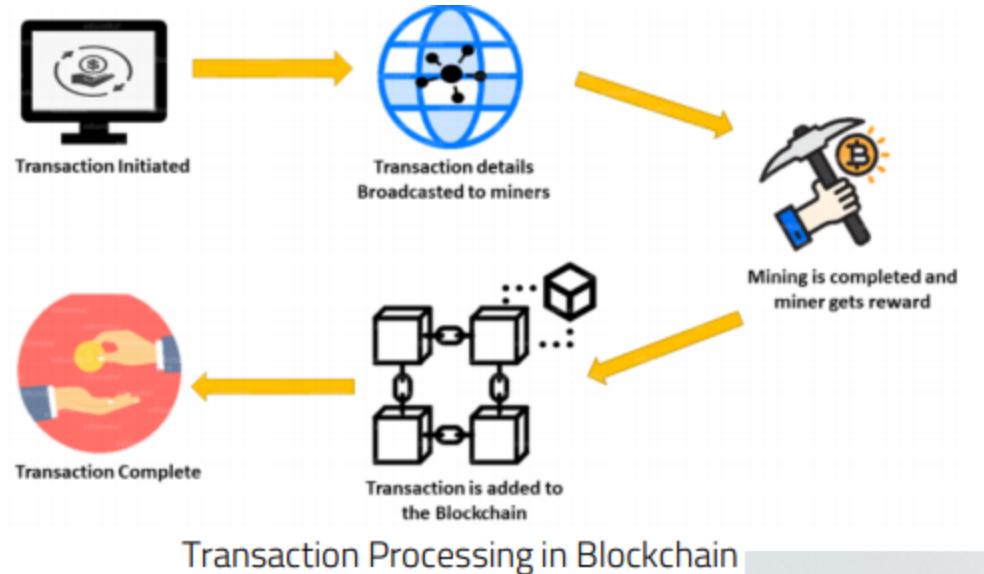
## Transaction

- 당사자 간의 상호 작용



## 채굴 Mining

- 새 거래를 검증하고 공개 원장에 추가하는데 사용되는 프로세스
- 합의 모델 : 다음 블록을 게시하는 노드 결정 (작업 증명을 통한 BTC)



## 한계 그리고 오해 Limitations & Misconceptions

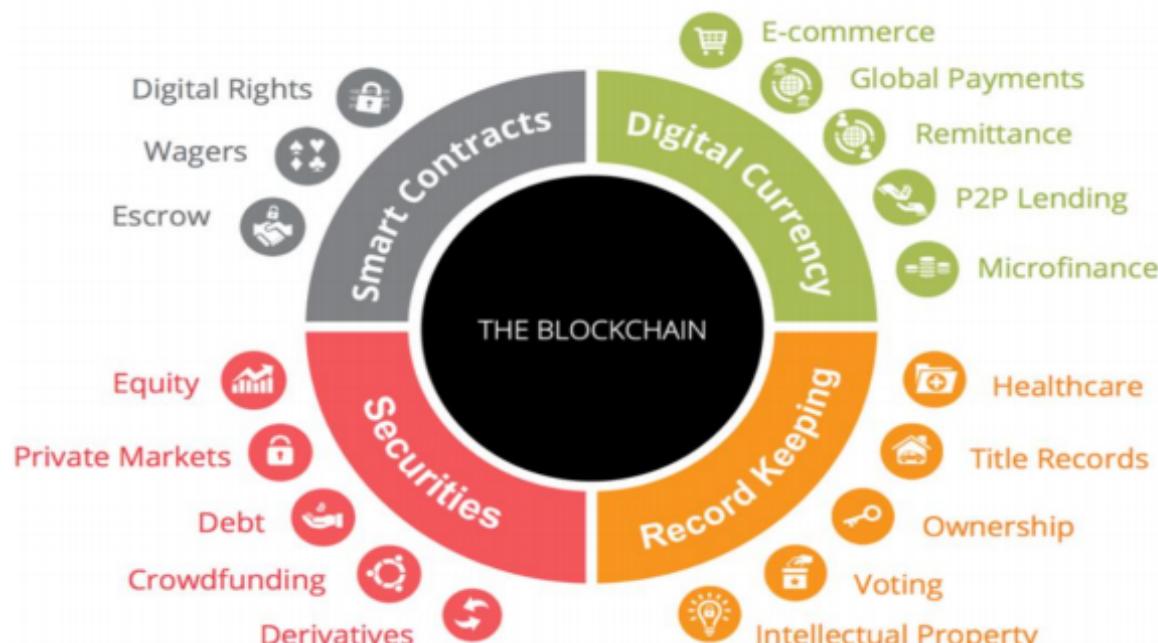
- 불변성 : 블록체인 자체는 완전한 불변으로 간주 될 수 없음(꼬리블록의 취약성 존재)
- 부적절한 블록 게시 보상 : 문제 해결을 위한 계산 능력에 비해 블록을 발행하는데 있어 부적절한 보상의 위험 존재
- 오라클 문제 : 블록체인과 외부를 연결하는 별도의 인프라 문제
- 블록 체인 거버넌스에 관련된 사용자 : 소프트웨어 개발자, 게시 노드 및 블록 체인 네트워크 사용자는 모두 블록 체인 네트워크 거버넌스에 참여



거버넌스(governance)는 일반적으로 '과거의 일방적인 정부 주도적 경향에서 벗어나 정부, 기업, 비정부기구 등 다양한 행위자가 공동의 관심사에 대한 네트워크를 구축하여 문제를 해결하는 새로운 국정운영의 방식'

## 잠재적 응용 프로그램 Potential Applications

거래 기반 산업의 미래를 바꾸는 블록 체인 촉매제



## 블록체인의 과제 Challenges of Blockchain

- 인식 및 이해
- 상호 운용성
- 검증 비용
- 성능 및 효율성
- 거버넌스 및 규정
- 개인 정보 보호 및 보안

## Cryptocurrency

### 암호화폐

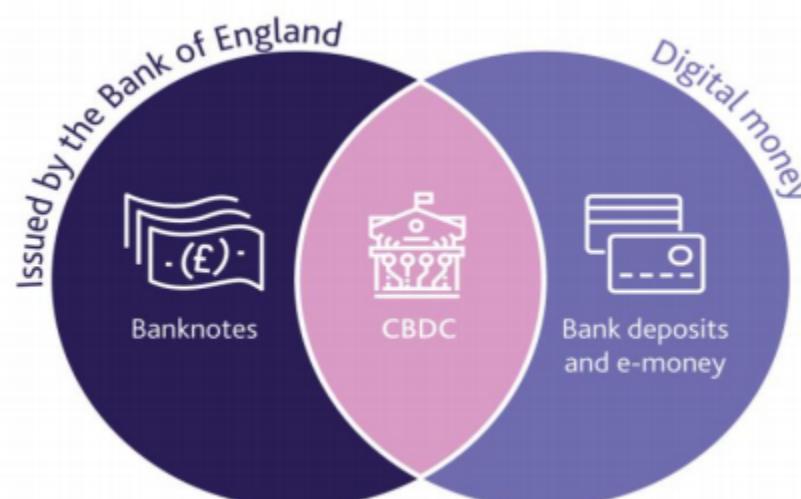
디지털 자산이며 암호화로 보호되므로 위조 또는 이중 지출이 거의 불가

### Facebook Diem (formerly Libra)

- 프로젝트 Libra (2020년 12월 이후 Diem)는 2019년 6월에 공식적으로 발표
- 현지 통화로 지원되는 글로벌 디지털 통화 및 결제 솔루션 Libra(Diem)
- 허가 된 블록 체인 기반 결제 시스템을 사용
- 암호 화폐로 구현된 개인통화 포함
- Libra 협회를 스위스 비영리로 설정하여 Libra 및 네트워크를 관리
- 서비스 및 보관 토큰을 제공하는 자회사 Calibra 설정
- 미국 정부 승인을 받는데 어려움이 있지만 중앙은행 디지털 화폐 프로젝트의 진척을 촉진

## CBDC (Central Bank Digital Currency)

가게와 기업이 결제하는 데 사용할 수 있는 전자 형태의 중앙은행 돈



### CBDC Project Status

