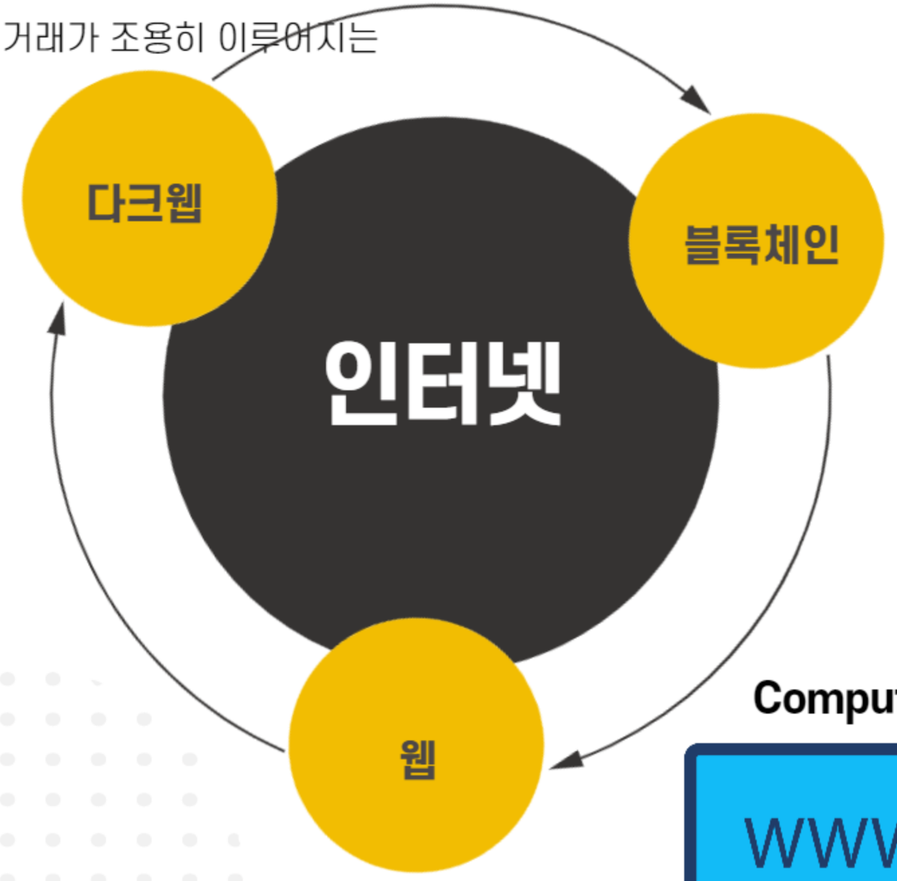
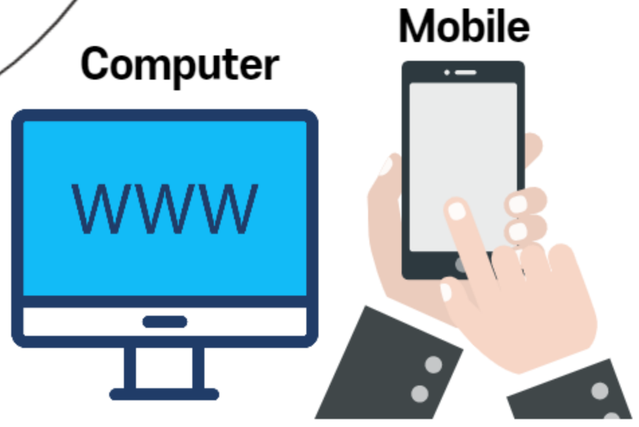
Block Chain

김수진

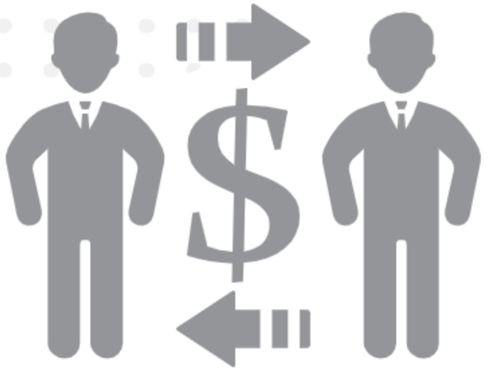
인터넷 사용 수단

뒷 거래가 조용히 이루어지는



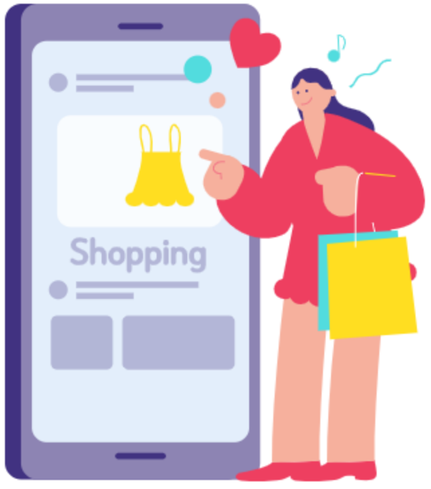


실생활 서비스



송금

공유 경제
(UBER, Air BnB)



인터넷 상거래

이중지불

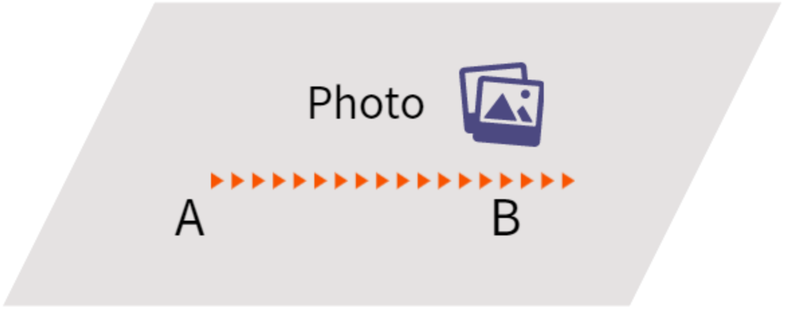
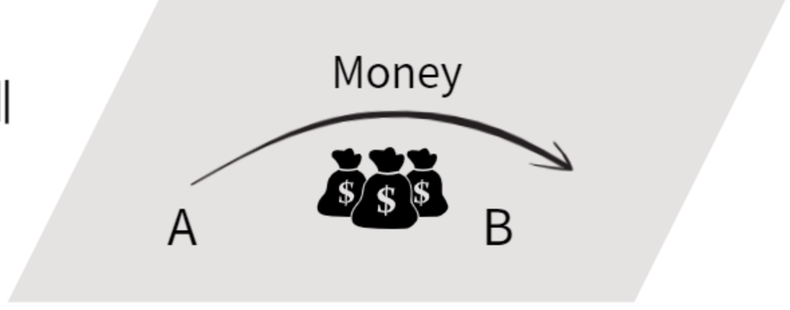


Photo
A
B

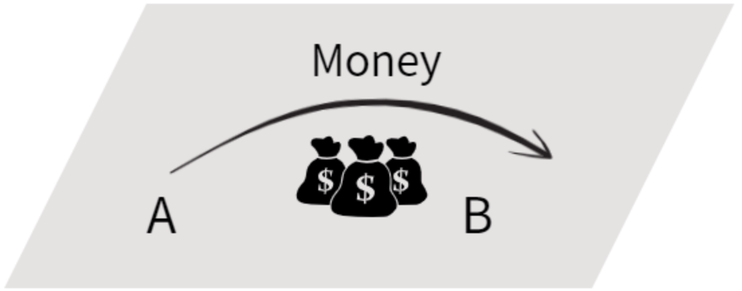

A
B
copy
share
+ photo
+ photo

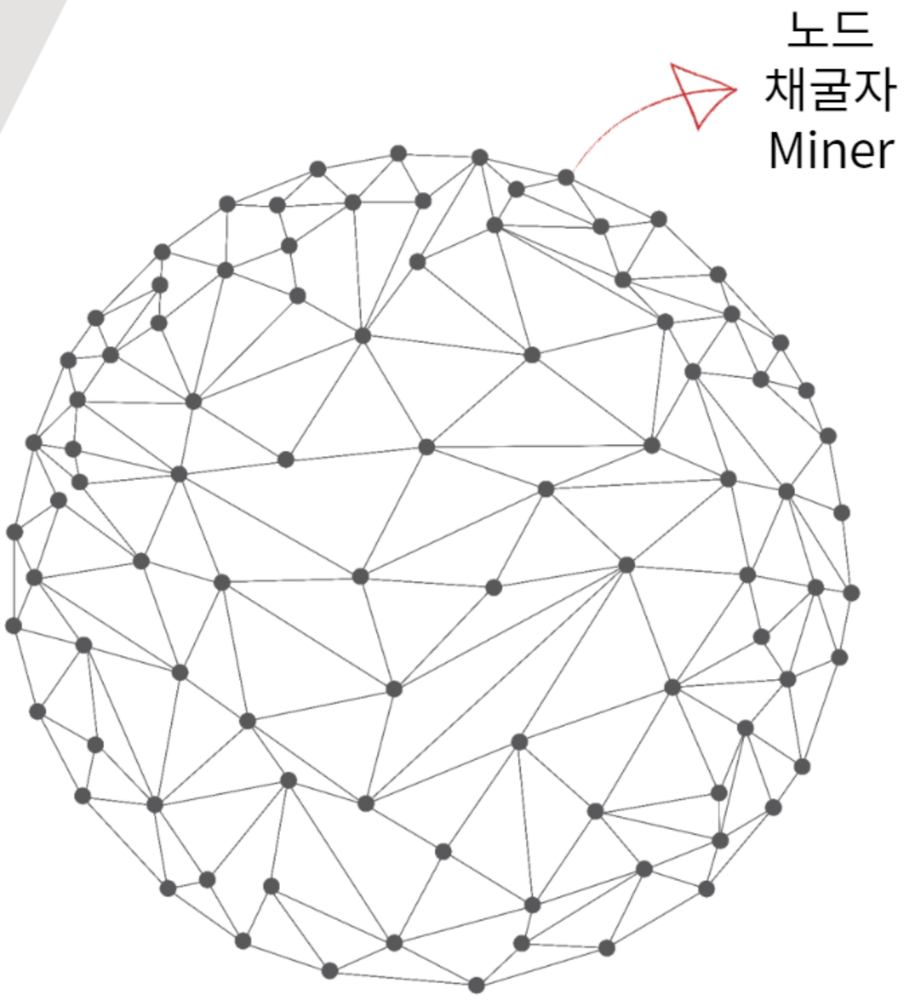
현존문제


Money
A
B


A
B
10000
+ 10000
중개
(-10000)
(+10000)
기록!!!

비트코인 송금 방법





Step 1

거래 요청

Step 2

10분간의 거래 요청들을
블록체인 system으로 전송

Step 3

모든 채굴자들이
10분간의 거래 정보들을 비교하고
참, 거짓 가려내는 작업

전체 노드(채굴자) 51% 이상이
참이라고 동의

Step 4

모든 채굴자들
참인 정보만 공통 장부에 기록!!

10분간의 참인
거래 정보들

비밀번호
찾는 방법

비밀번호가 만들어진
해시함수 역추적

f(임의의 값) = 0000·····

앞에 '0'이 4개 되는
해시값이 도출되는
임의의 값을 찾아내야 한다 !

채굴자들,
비밀번호 찾기 경쟁!!

보상: 비트코인

POW 작업증명

해시값 찾아내는 방법

채굴

비밀번호 직접 찾아내는 작업
= 해시값 찾아내는 작업

채굴자들이 돈을 버는 방법

수수료 : 거래가 참인지 증명·보증함
채굴 보상 : 블록의 비밀번호(해시값) 찾아냄

① 각각의 노드(채굴자)
블록의 암초를 풀기위해
경쟁

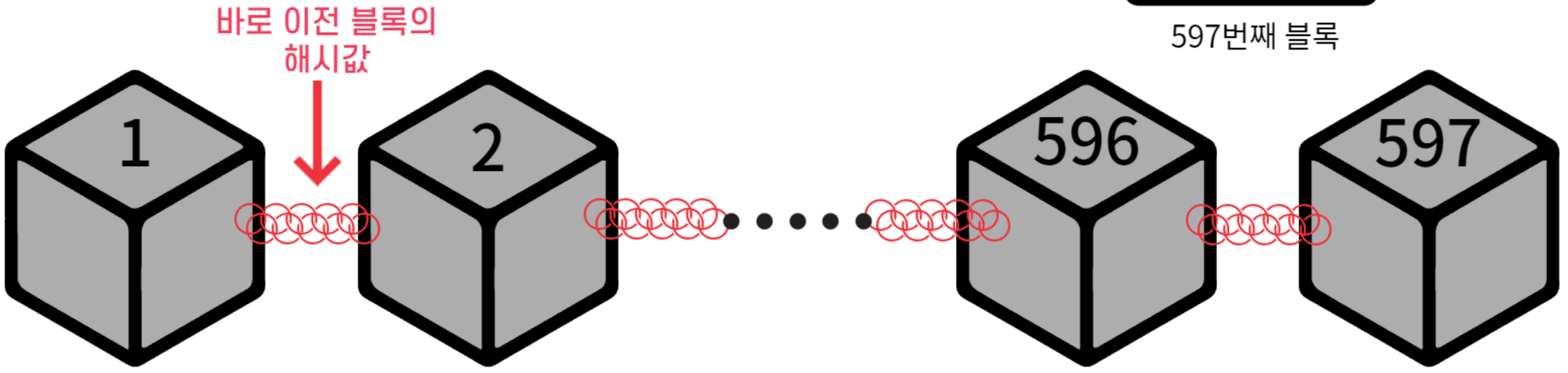
② 제일 먼저 '암호'를 푼 채굴자,
다른 채굴자들에게 **전파**

③ 다른 채굴자들 **승인·합의** 해줌

④ 비밀번호를 찾은 채굴자가
블록생성

Block Chain

597번째 블록



10분간의
참인
거래내역

10분간의
참인
거래내역
+
1번 블록의
해시값

10분간의
참인
거래내역

10분간의
참인
거래내역

Block Chain

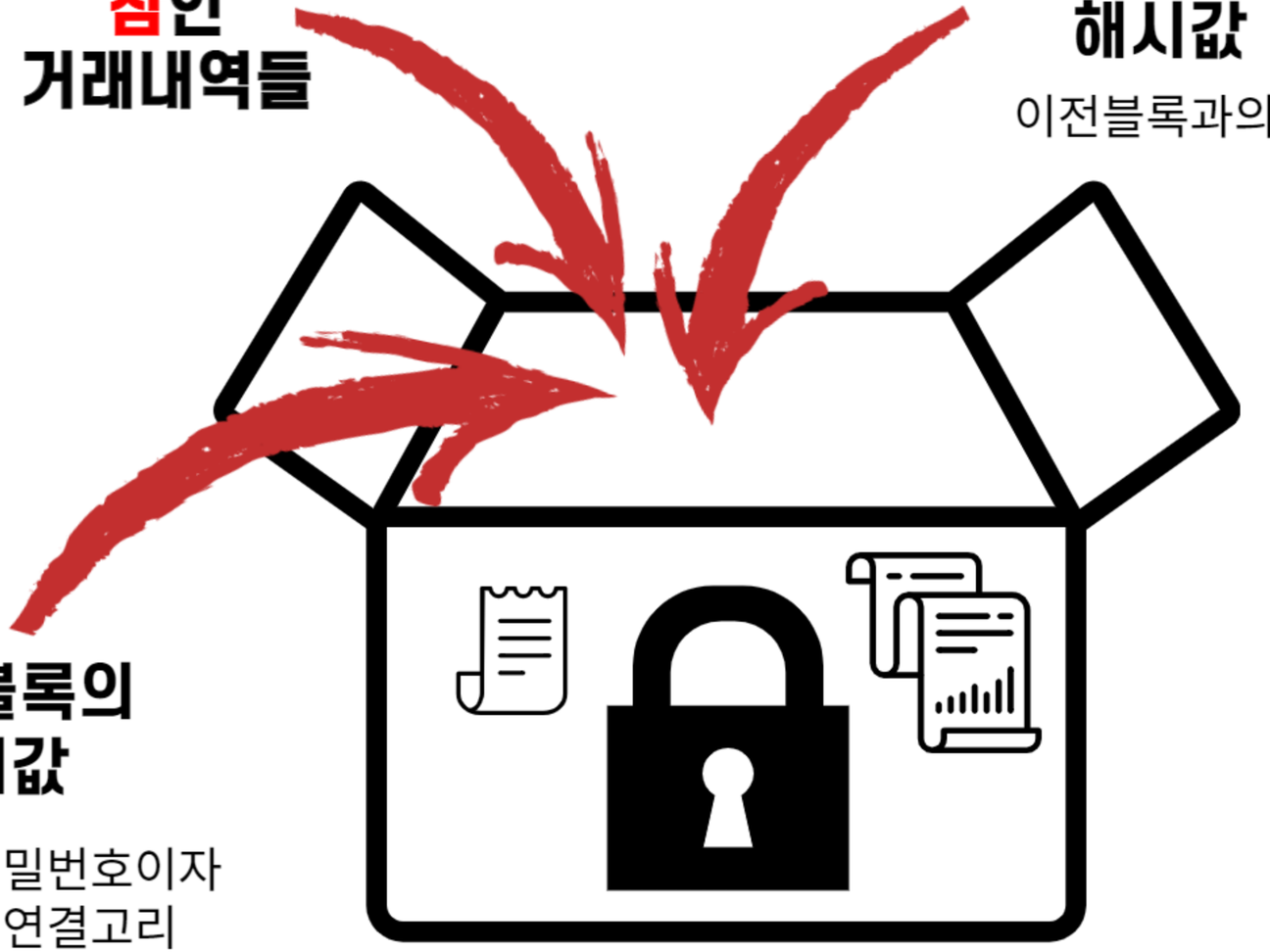
기존의 은행이나 거대 플랫폼 기업과 같이
사람과 사람의 계약이나 거래 상호작용을 중개해 주는
제 3의 기관을 대신해주는 컴퓨팅시스템

채굴자들이 '진짜'라
인정하는 거래 내역 모음

10분간의 참인 거래내역들

이전 블록의 해시값

이전블록과의 연결고리

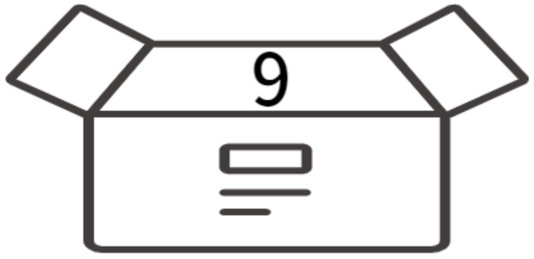


현재 블록의 해시값

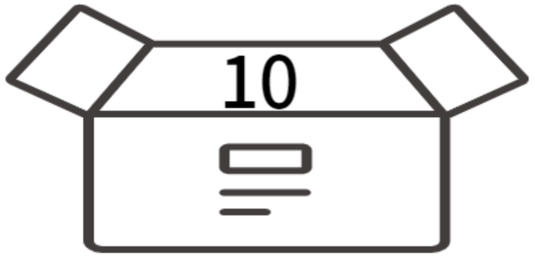
현재 블록의 비밀번호이자
다음 블록의 연결고리

Block Chain의 특징

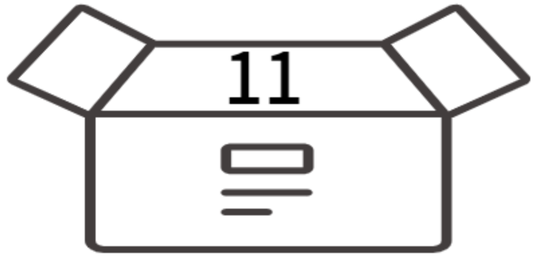
보안성



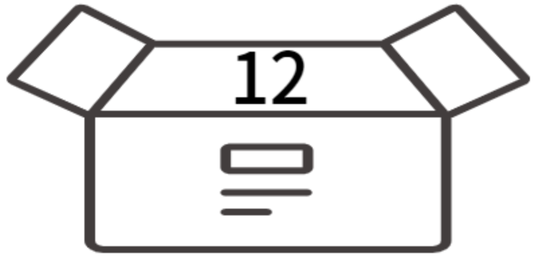
10분간의 거래 정보



10분간의 거래 정보



10분간의 거래 정보



10분간의 거래 정보

9블록 해시값

9블록 해시값

10블록 해시값

10블록 해시값

11블록 해시값

11블록 해시값

12블록 해시값

차곡차곡 쌓여가는 구조

채굴자의 51%이상의
승인을 받아야
참인 거래내역으로 인정

탈중앙화된
합의 프로토콜

숫자화되고
암호화된 정보들

익명성

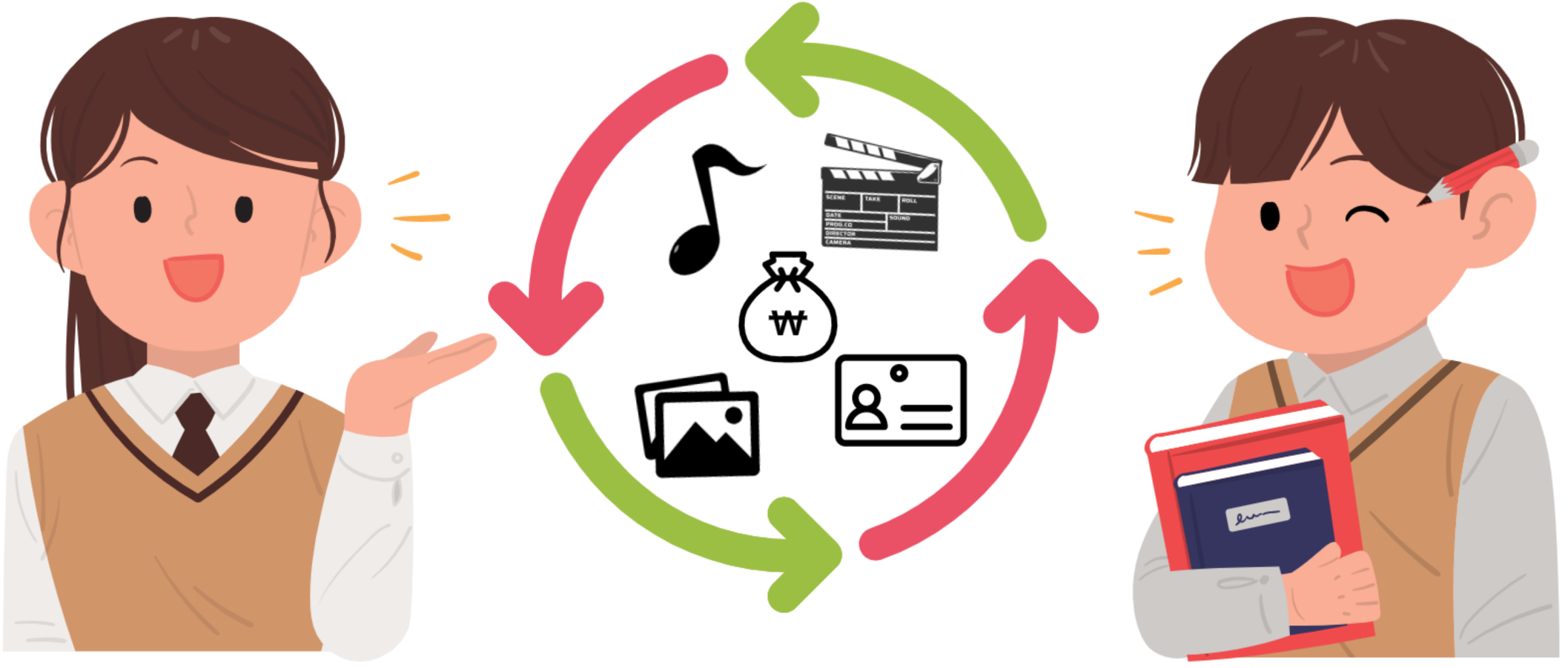
투명성

P2P

개인과 개인이 직접 연결 되어 정보나 파일을 공유하는 것

Peer

Peer



채굴할 수 있는 컴퓨터 사양만 된다면
누구나 할 수 있음
(오픈소스를 통해 누구나 비트코인을 만들수 있음)

“스마트 계약”

계약 조건이 충족되면
보증인, 보증회사 없이
블록체인이

자동으로 금액을 전송!

블록체인 활용 분야

기업

"인적자산" 비용
감소

"물적자산" 비용
감소

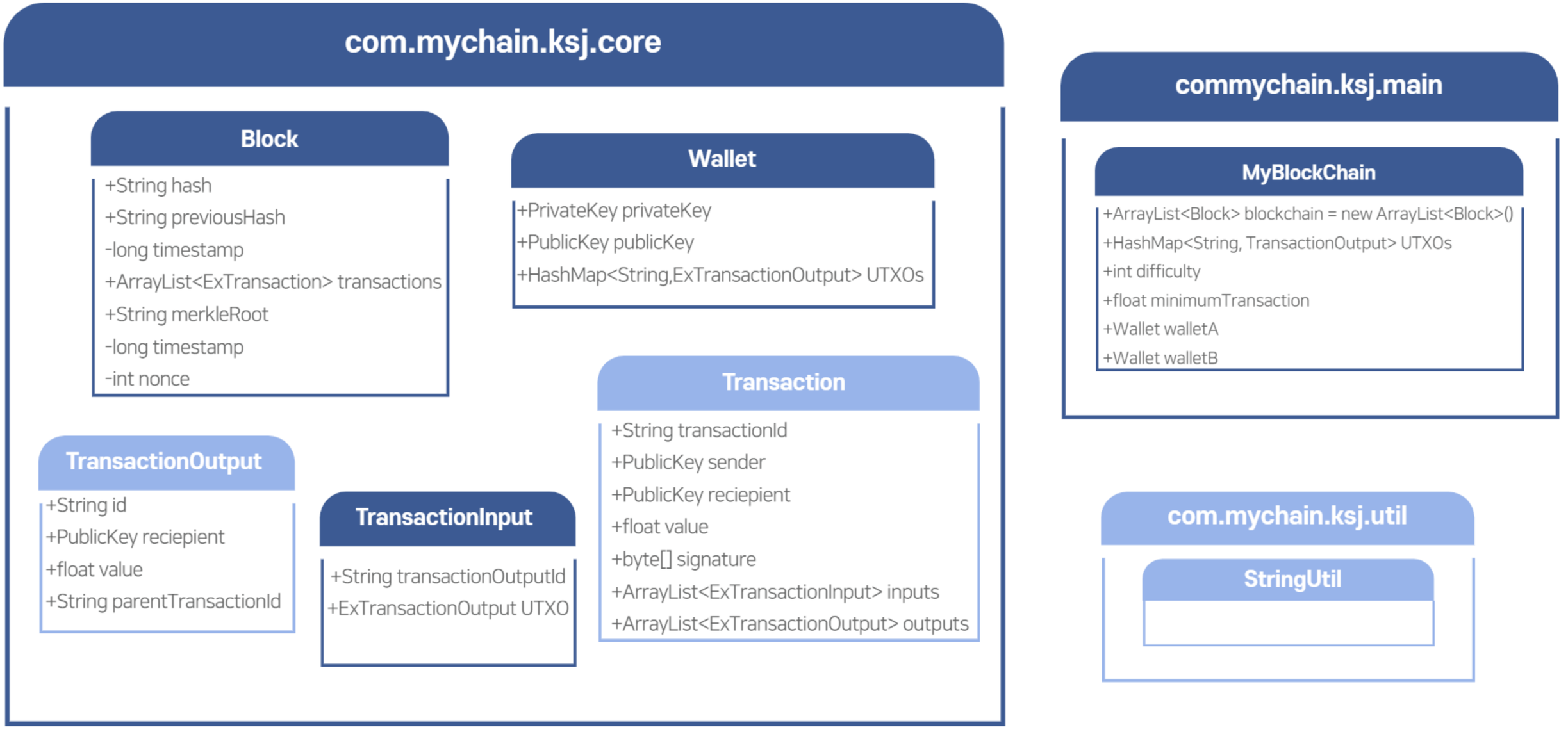
"유통거래" 비용
감소

소비자

"제품 & 서비스가격 & 수수료" 비용
감소


개인신원확인
에너지
TAX
정부 행정
시스템
금융
블록체인
의료

클래스 다이어그램


com.mychain.ksj.core
Block
+String hash
+String previousHash
-long timestamp
+ArrayList<ExTransaction> transactions
+String merkleRoot
-long timestamp
-int nonce
Wallet
+PrivateKey privateKey
+PublicKey publicKey
+HashMap<String,ExTransactionOutput> UTXOs
Transaction
+String transactionId
+PublicKey sender
+PublicKey reciepient
+float value
+byte[] signature
+ArrayList<ExTransactionInput> inputs
+ArrayList<ExTransactionOutput> outputs
TransactionOutput
+String id
+PublicKey reciepient
+float value
+String parentTransactionId
TransactionInput
+String transactionOutputId
+ExTransactionOutput UTXO
commychain.ksj.main
MyBlockChain
+ArrayList<Block> blockchain = new ArrayList<Block>()
+HashMap<String, TransactionOutput> UTXOs
+int difficulty
+float minimumTransaction
+Wallet walletA
+Wallet walletB
com.mychain.ksj.util
StringUtil