

한 번에 끝내는 블록체인 개발 A to Z

Chapter 1

Blockchain 1.0 - Bitcoin

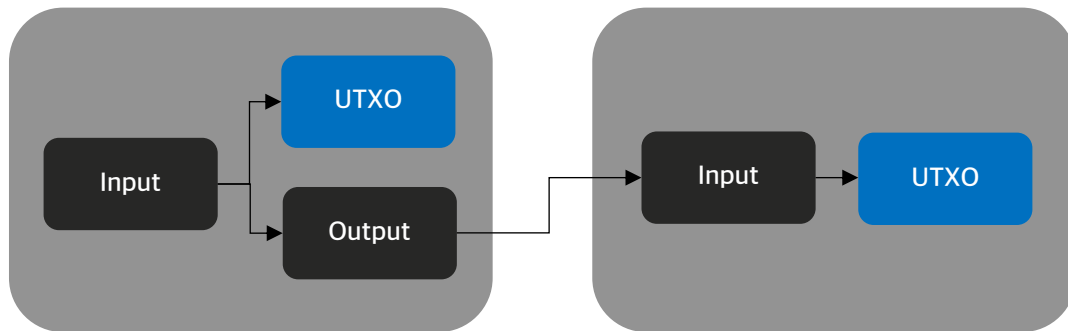
Chapter 1

Blockchain 1.0 - Bitcoin

Transaction Structure

UTXO

- UTXO(Unspent Transaction Output)
이란 아직 사용되지 않은 Output을
지칭한다.
- Bitcoin은 UTXO 방식으로 운영되며,
UTXO 사용 여부를 통해서 자산의 안전성을
확인한다.



Transaction 구조

Size	Field	설명
4 bytes	Version	현재 값1
2 byte array	Flag	Witness Tx 여부에 따라 달라짐
1-9 bytes	Number of Inputs	Input의 개수
Variable	Inputs	Input 정보
1-9 bytes	Number of Outputs	Output의 개수
Variable	Outputs	Output 정보
Variable	Witnesses	Witness 서명 데이터
4 bytes	Locktime	Transaction 시간 제한

Input의 구조

Size	Field	설명
32 bytes	Transaction Hash	현재 Input이 포함된 Tx Id
4 bytes	Output Index	Tx 안에서 Seq
1-9 bytes	Unlocking-Script Size	Unlocking Script 크기
Variable	Unlocking-Script	Output을 Input으로 바꾸는 서명정보
4 bytes	Sequence Number	기본 값 0xffffffff

Output의 구조

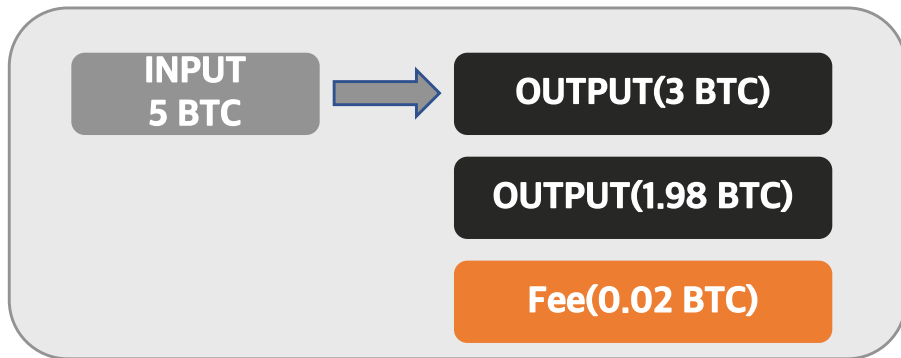
size	Field	설명
8 bytes	Amount	송금할 금액(Satoshi 단위)
1-9 bytes	Locking-Script Size	Locking-Script Size
Variable	Locking-Script	송금자의 정보가 담긴 데이터

Transaction Fee

Bitcoin 수수료는 전체 INPUT의 총합에서 전체 OUTPUT의 총합을 뺀 값이다.

블록에서 설명하였듯이, 채굴자들이 거래를 더 빠르게 하기 위해서는 수수료를 높여야한다.

(채굴자들이 선호하는 거래는 용량이 작고 수수료가 높은 거래이기 때문에 Fee per byte가 높아야 한다.)



Size	222 bytes
Weight	888
Included in Block	Mempool
Confirmations	0
Total Input	0.22074426 BTC
Total Output	0.22070810 BTC
Fees	0.00003616 BTC
Fee per byte	16.288 sat/B

(출처 : Blockchain.info)

Coinbase


PoW 에서 채굴에 성공하게 되면, 채굴에 성공한 채굴자(Miner)에게 기본 보상 수수료와 거래 수수료를 보상으로 제공한다. 이러한 보상금액은 Block의 가장 첫 번째 거래로 Block에 포함된다.

Inputs ⓘ

[HEX](#)[ASM](#)

Index	0	Details	Output
Address		Value	N/A
Pkscript	N/A		
Sigscript	ffff001d OP_4 5468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73		
Witness			

Outputs ⓘ

Index	0	Details	Unspent
Address	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa 	Value	50.00000000 BTC
Pkscript	04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG		

(출처 : blockchain.com)

Bitcoin 거래 방식 - P2PK

Prev Output

ScriptPubKey

Public Key

04ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7df5f14
2c21c1b7303b8a0626f1bade5c72a704f7e6cd84c

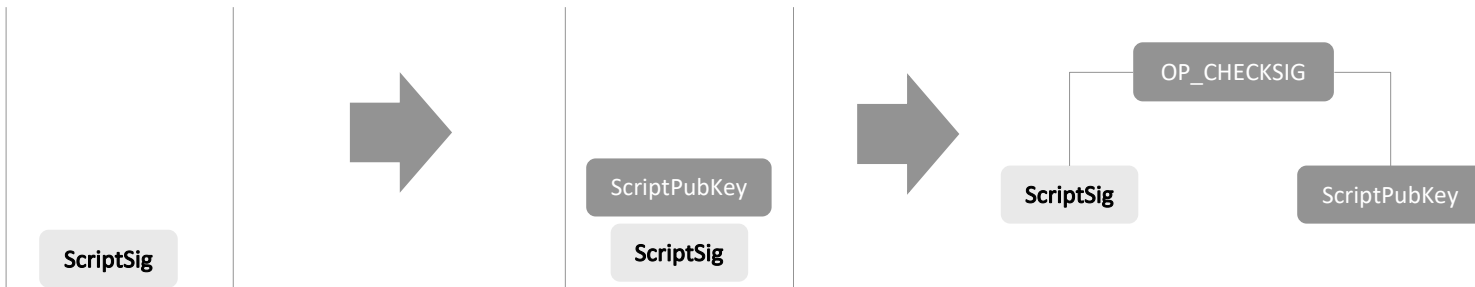
OP_CHECKSIG

Input

ScriptSig

Signature

30440220576497b7e6f9b553c0aba0d8929432550e092db9c130aae37b84b545e7f4a36c022066cb982ed
80608372c139d7bb9af335423d5280350fe3e06bd510e695480914f01



Bitcoin 거래 방식 - P2PKH

Prev Output

ScriptPubKey

OP_DUP

OP_HASH160

Public Key Hash

12ab8dc588ca9d5787dde7eb29569da63c3a238c

OP_EQUALVERIFY

OP_CHECKSIG

Input

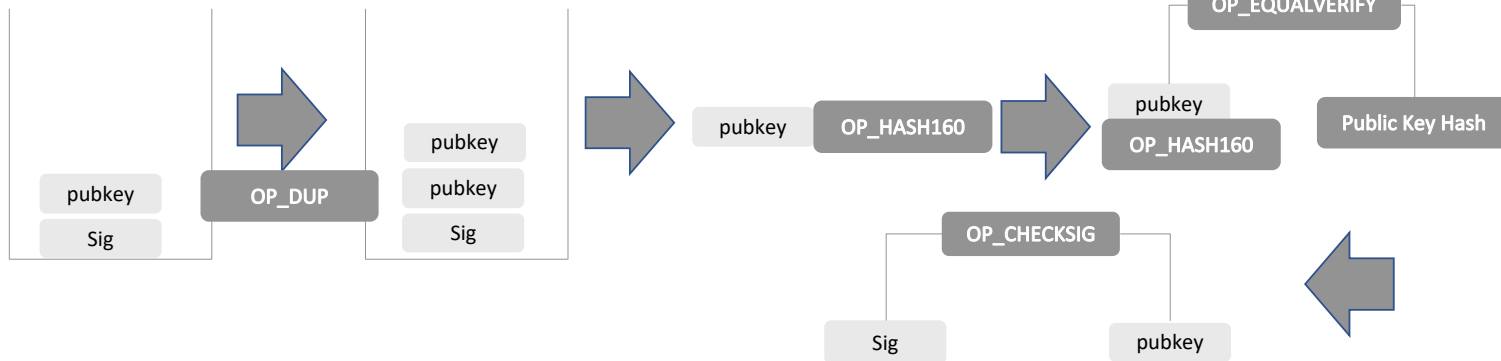
ScriptSig

Signature

30440220576497b7e6f9b553c0aba0d8929432550e092db9c130aae37b84b545e7f4a36c022066cb982ed
80608372c139d7bb9af335423d5280350fe3e06bd510e695480914f01

044d05240cfbd8a2786eda9dadd520c1609b8593ff8641018d57703d02ba687cf2f187f0cee2221c3afb1b5
ff7888caced2423916b61444666ca1216f26181398c

Public Key



Bitcoin 거래 방식 - NULL_DATA

- 블록체인 상에 데이터를 저장하는 방식
- Input의 ScriptSig가 들어가지 않는 거래
- OP_RETURN 을 사용

ScriptPubKey

OP_RETURN

68656c6c6f20776f7226c64

블록체인상에 저장할 데이터

Bitcoin 거래 방식 - SEGWIT

2017년 Bitcoin 업그레이드로 인해 지원하는 새로운 거래 형식

Prev Output

ScriptPubKey

0

Public Key Hash

12ab8dc588ca9d5787dde7eb29569da63c3a238c

Input

ScriptSig

Signature

30440220576497b7e6f9b553c0aba0d8929432550e092db9c130aae37b84b545e7f4a36c022066cb982ed
80608372c139d7bb9af335423d5280350fe3e06bd510e695480914f01

Witness
Data

044d05240cfbd8a2786eda9dadd520c1609b8593ff8641018d57703d02ba687cf2f187f0cee2221c3afb1b5
ff7888caced2423916b61444666ca1216f26181398c

Public Key

Bitcoin 거래 방식 - TapRoot

- 2021년 Bitcoin 업그레이드로 인해 지원하는 새로운 거래 형식
- 슈노르 서명 방식 지원
 - 공동 공개 키를 생성하여 하나의 서명으로 공동 서명
- MAST(Merkelized Abstract Syntax Trees) 지원
 - Bitcoin Script 실행 사실을 숨길 수 있음
 - Bitcoin의 프라이버시를 향상 시키고 트랜잭션의 수수료를 감소

Lightning Network

- Lightning Network란 Bitcoin Layer 2 기술로 블록체인 상에서 일정 금액을 생성하고 이를 네트워크 상에 배포(블록에 미포함)시키지 않고 잠금된 금액을 기반으로 실시간 거래가 가능하도록 하는 기술이다.
- 엘살바도르 국민들은 현재 이 기술로 Bitcoin을 법정화폐로 사용하고 있다.

