블록체인 자산추적

91714167 유재경

목차

01

개요

개요

1. 계기 | 2. 목표

읍살라젠 ♡ 관심기업

외국계IT보안-블록체인 지갑주소 추적/분석 신입(계약직/정규직 전환)채용

블록체인 CIRC 보안 조사관 (○명)

담당업무

• 읍살라시큐리티의 CIRC (Crypto Incident Reponse Center)의 담당 보안 리서처
가상자산 서비스 기업 및 개인의 해킹, 투자사기, 불법거래 등의 피해 사례를 의뢰 받고, 자사의 가상자산 추적 솔루션을 활용, 조사 분석하여 암호화폐 추적 레포트 작성
(개인 및 기업고객 상담, 가상자산 추적 작업, 레포트 작성 및 기타 관련 제반 업무)

• 피해자 상담

• 오픈소스 데이터 분석

• 개요

1. 계기 | 2. 목표

읍살라젠 ♡ 관심기업

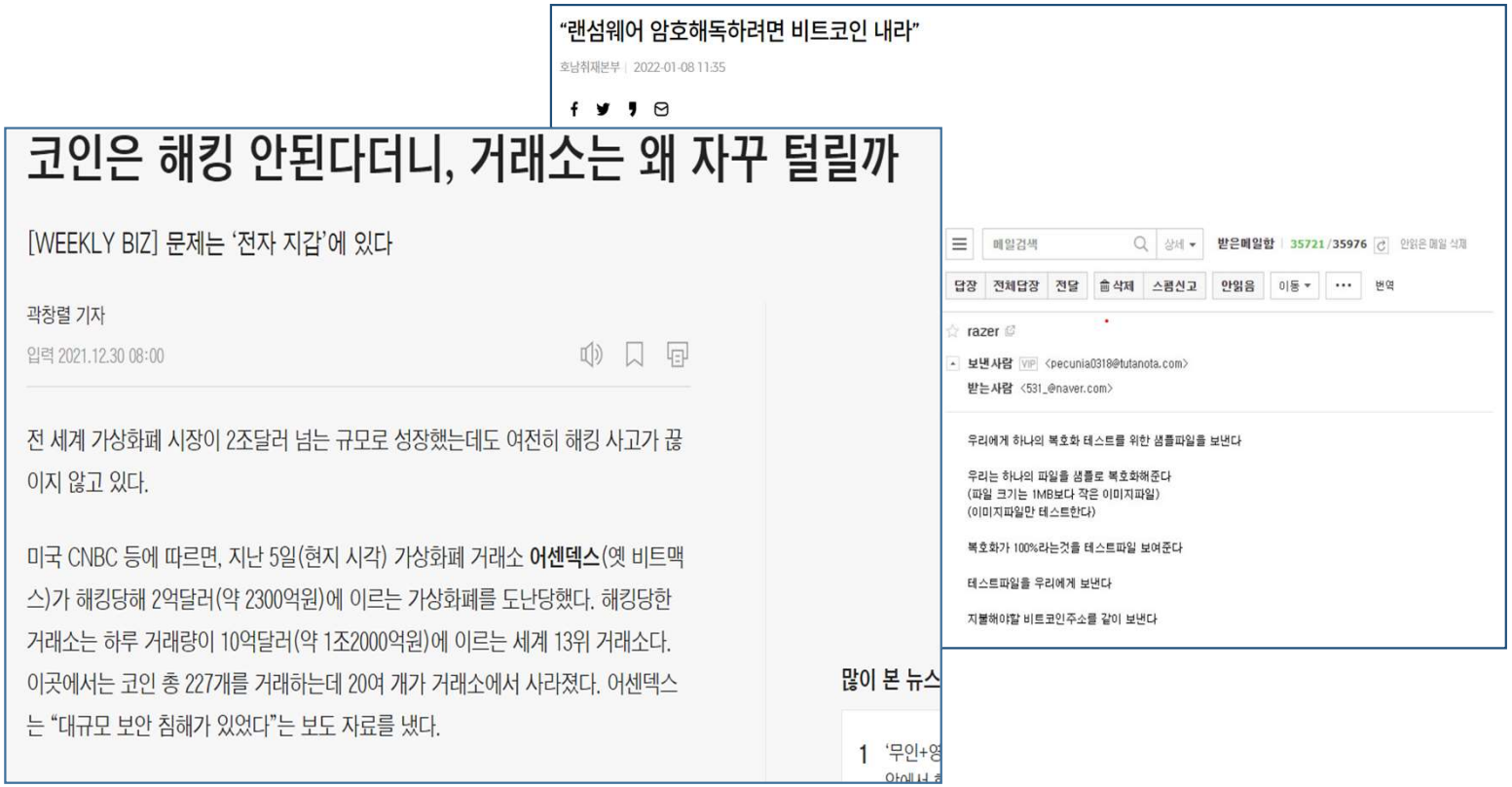
외국계IT보안-블록체인 지갑주소 추적/분석 신입(계약직/정규직 전환)채용

블록체인 CIRC 보안 조사관 (○명)	담당업무 • 읍살라시큐리티의 CIRC (Crypto Incident Reponse Center)의 담당 보안 리서처 가상자산 서비스 기업 및 개인의 해킹, 투자사기, 불법거래 등의 피해 사례를 의뢰 받고, 자사의 가상자산 추적 솔루션을 활용, 조사 분석하여 암호화폐 추적 레포트 작성 (개인 및 기업고객 상담, 가상자산 추적 작업, 레포트 작성 및 기타 관련 제반 업무) • 피해자 상담 • 오픈소스 데이터 분석

• 개요

1. 계기

2. 목표



"랜섬웨어 암호해독하려면 비트코인 내라"

호남취재본부 | 2022-01-08 11:35

코인은 해킹 안된다더니, 거래소는 왜 자꾸 털릴까

[WEEKLY BIZ] 문제는 '전자 지갑'에 있다

곽창렬 기자

입력 2021.12.30 08:00

전 세계 가상화폐 시장이 2조달러 넘는 규모로 성장했는데도 여전히 해킹 사고가 끊이지 않고 있다.

미국 CNBC 등에 따르면, 지난 5일(현지 시각) 가상화폐 거래소 **어센덱스**(옛 비트맥스)가 해킹당해 2억달러(약 2300억원)에 이르는 가상화폐를 도난당했다. 해킹당한 거래소는 하루 거래량이 10억달러(약 1조2000억원)에 이르는 세계 13위 거래소다. 이곳에서는 코인 총 227개를 거래하는데 20여 개가 거래소에서 사라졌다. 어센덱스는 "대규모 보안 침해가 있었다"는 보도 자료를 냈다.

많이 본 뉴스

1 '무인+

메일검색 | 상세 | 받은메일함 | 35721/35976 | 안읽은 메일 삭제

답장 | 전체답장 | 전달 | 삭제 | 스팸신고 | 안읽음 | 이동 | ... | 번역

razer

보낸사람 VIP <pecunia0318@tutanota.com>

받는사람 <531_@naver.com>

우리에게 하나의 복호화 테스트를 위한 샘플파일을 보낸다

우리는 하나의 파일을 샘플로 복호화해준다
(파일 크기는 1MB보다 작은 이미지파일)
(이미지파일만 테스트한다)

복호화가 100%라는것을 테스트파일 보여준다

테스트파일을 우리에게 보낸다

지불해야할 비트코인주소를 같이 보낸다

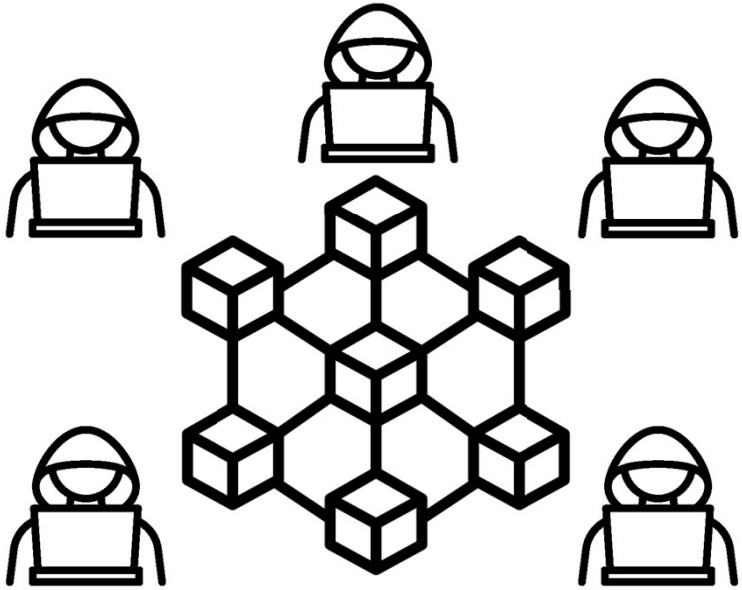
• 개요

1. 계기 | 2. 목표

02

자산추적을 하는 이유

• 자산추적을 하는 이유



블록체인 네트워크

익명성을 띄고 있는 블록체인

단순히 체인 네트워크를 통해서는
지갑의 주인이 누구인지,
거래대상이 누구인지 알아내는 것은
불가능하다고 볼 수 있다.

• 자산추적을 하는 이유

암호화폐의 최종목적지

결국 공격자는 최종적으로
암호화페를 현금으로 교환하는 것을
원할 것이다.

• 자산추적을 하는 이유

"거래소 사용하고 싶으면 신원확인 필요"

암호화폐의 최종목적지

우리나라 등 37개국이 가입한 국제자금세탁방지기구(FATF)에서 지정한 자금세탁방지 규칙에 의해 신원을 확인하도록 되어있음

• 자산추적을 하는 이유

BTC 송금

UPbit

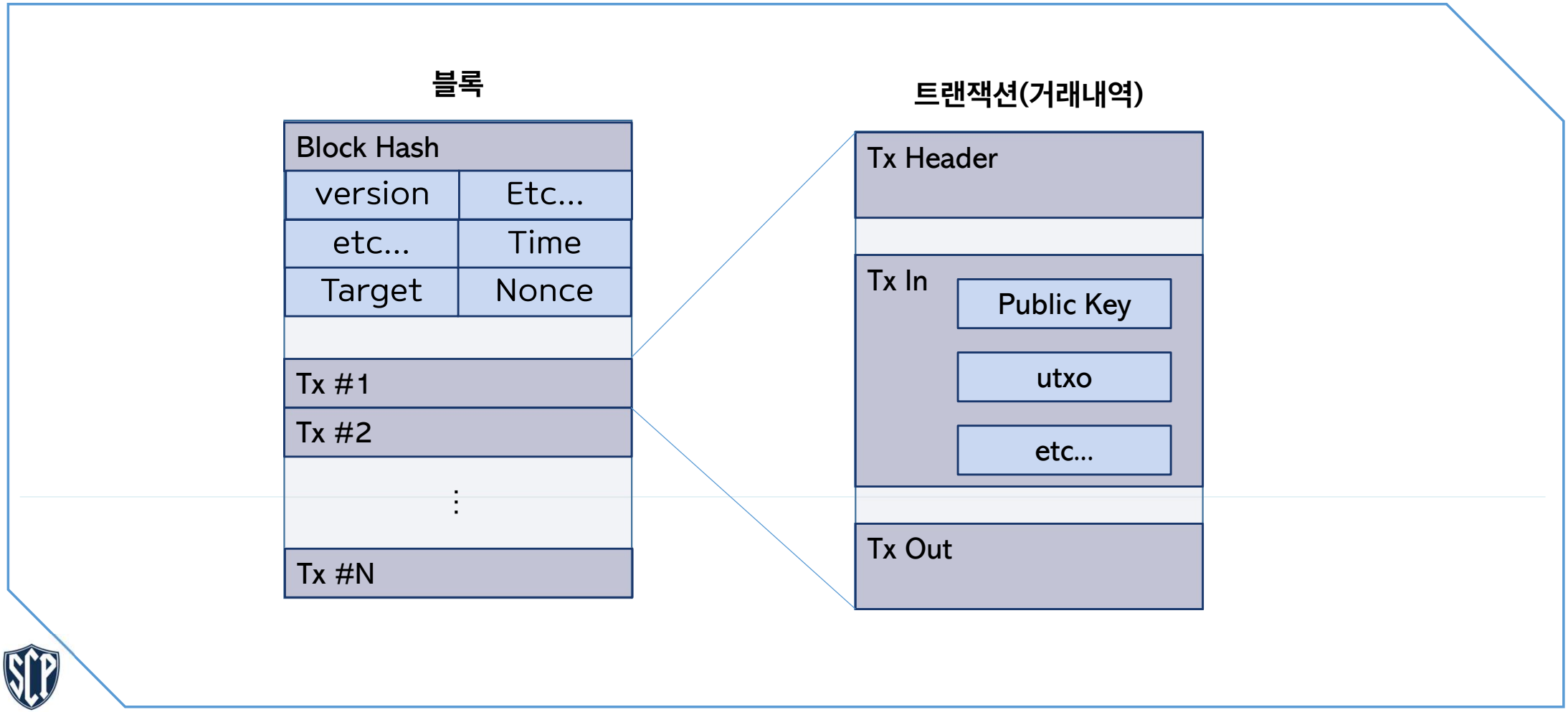
암호화폐의 최종목적지

최종적으로 현금으로 환전하기 위해 거래소로 송금할 때를 추적하는 것이 자산추적의 최종목표이다.

03

자산추적 원리

• 자산추적 원리


블록
Block Hash
version
Etc...
etc...
Time
Target
Nonce
Tx #1
Tx #2
Tx #N
트랜잭션(거래내역)
Tx Header
Tx In
Public Key
utxo
etc...
Tx Out

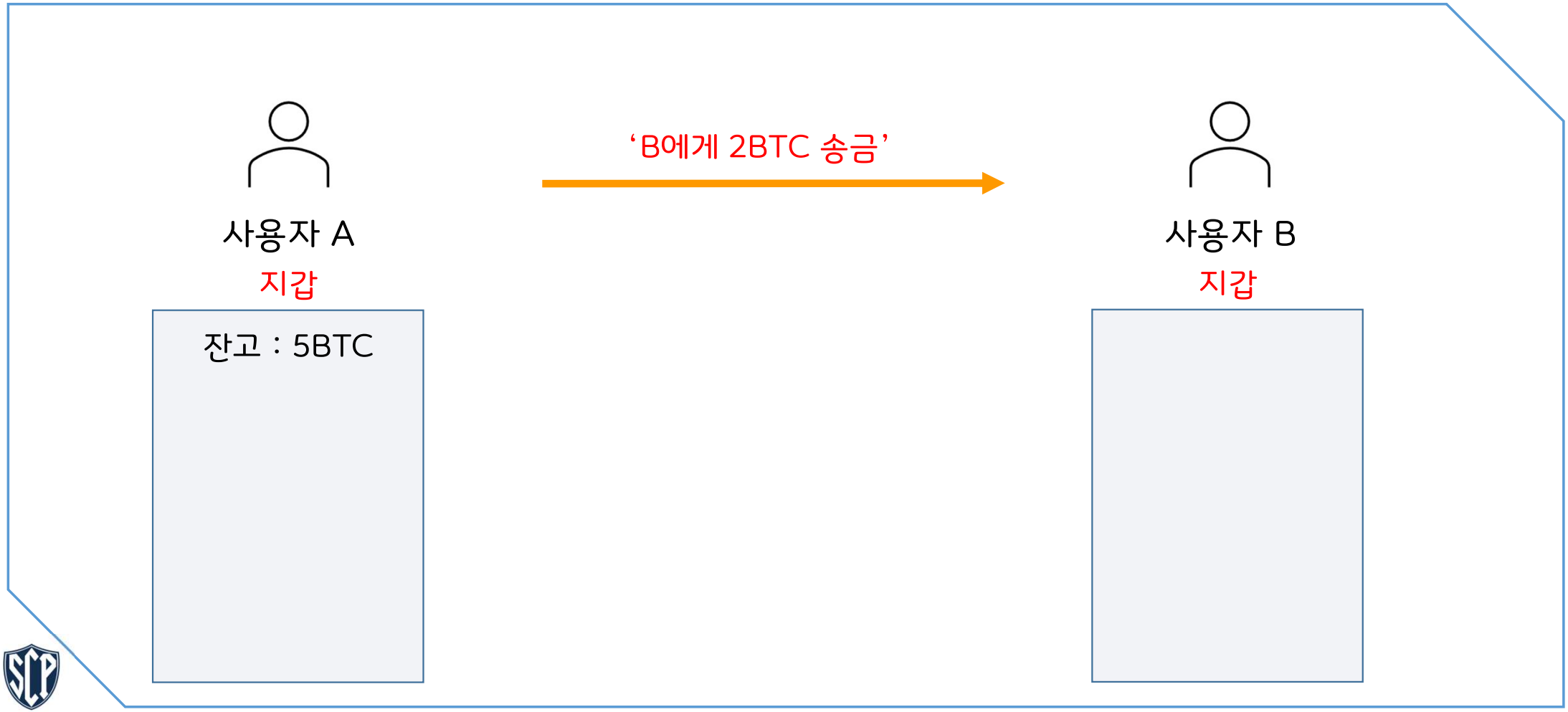
• 자산추적 원리

UTXO	
vin	vout

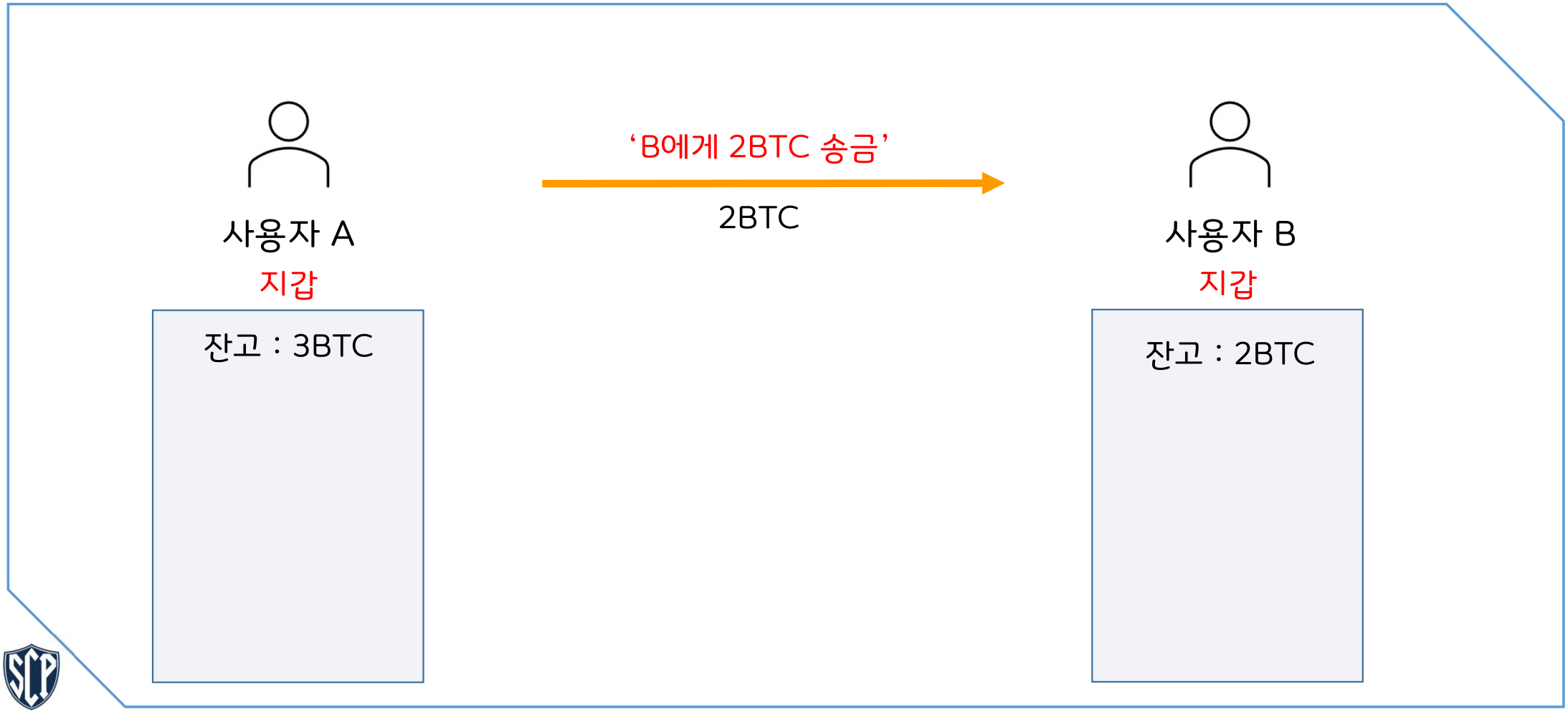
UTXO란?

Unspent Transaction Outputs 의 약자로, 미사용 트랜잭션 출력값을 말한다.

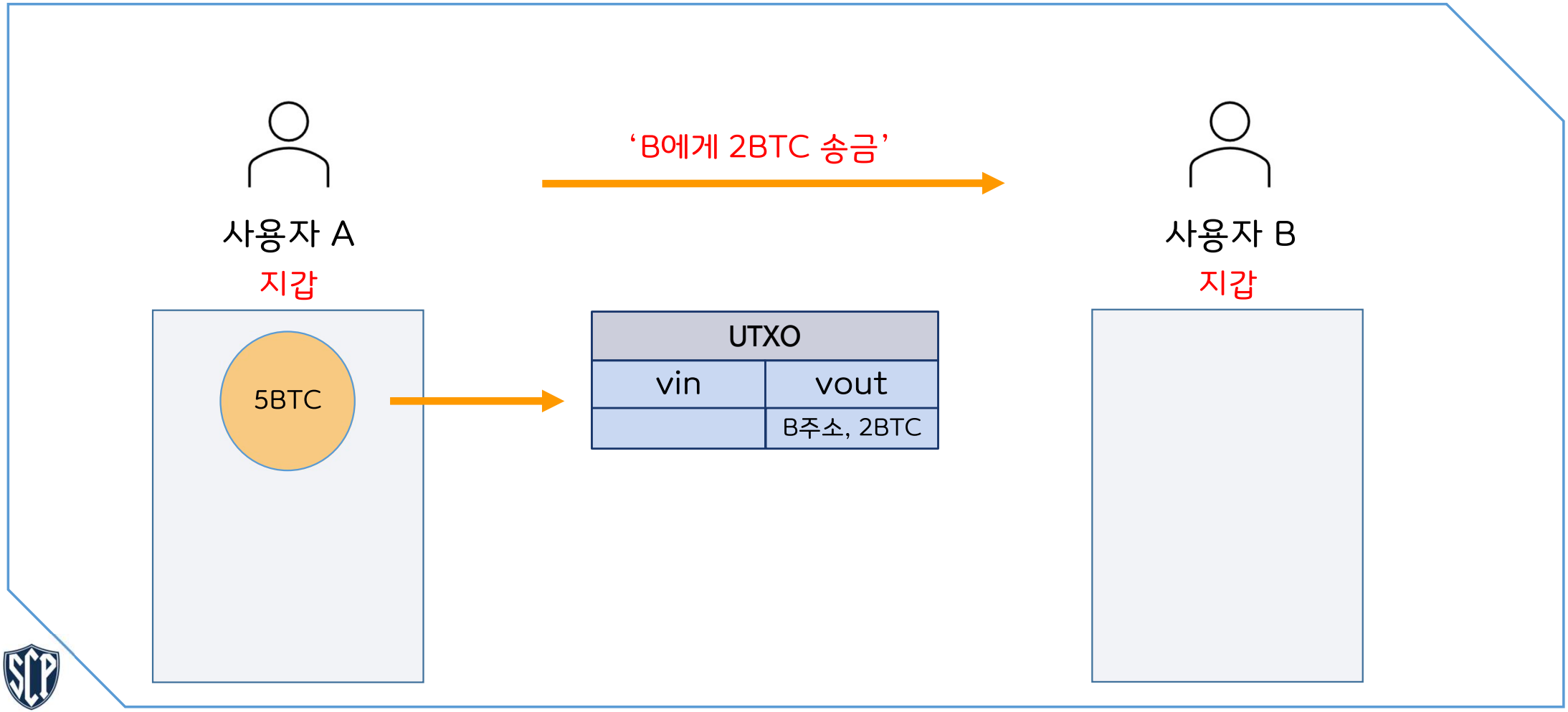
• 자산추적 원리



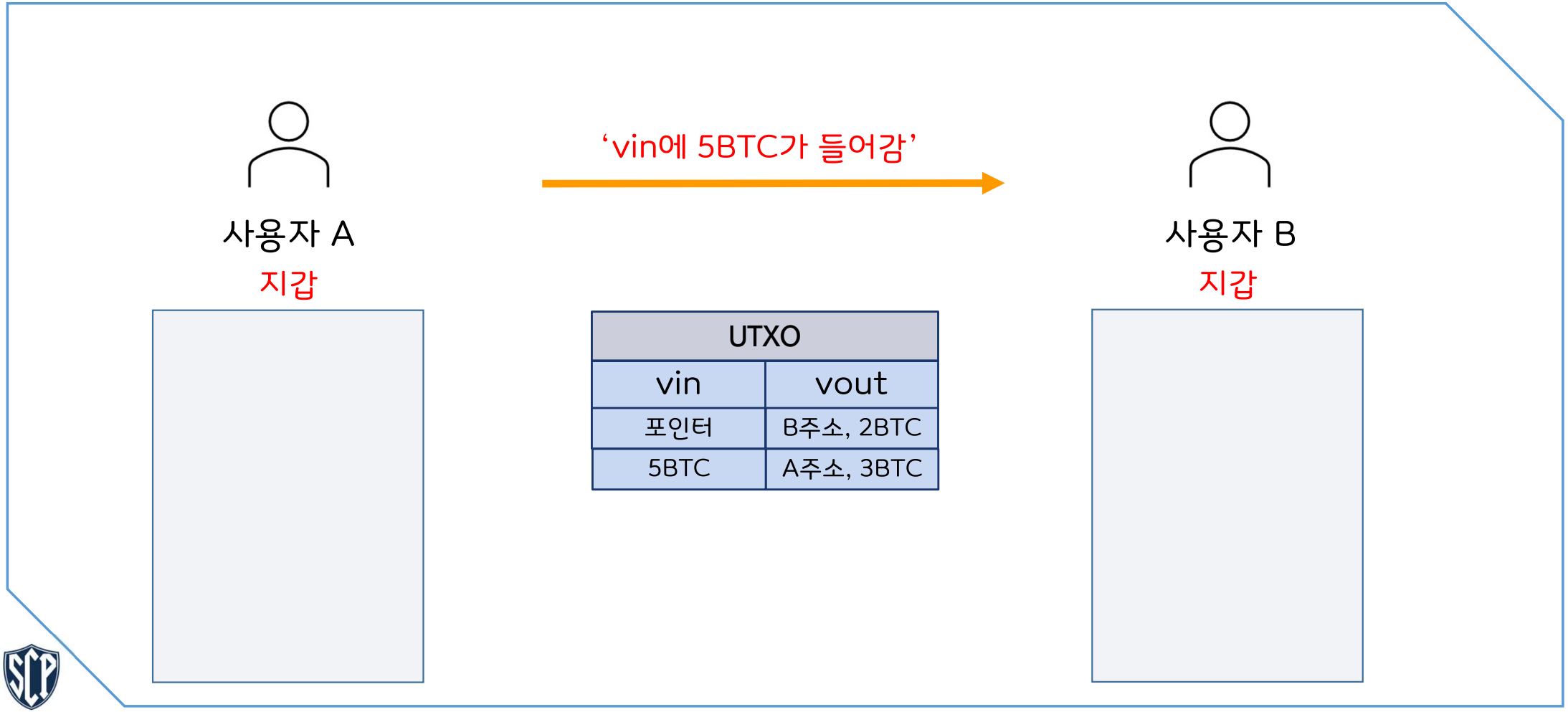
• 자산추적 원리



• 자산추적 원리

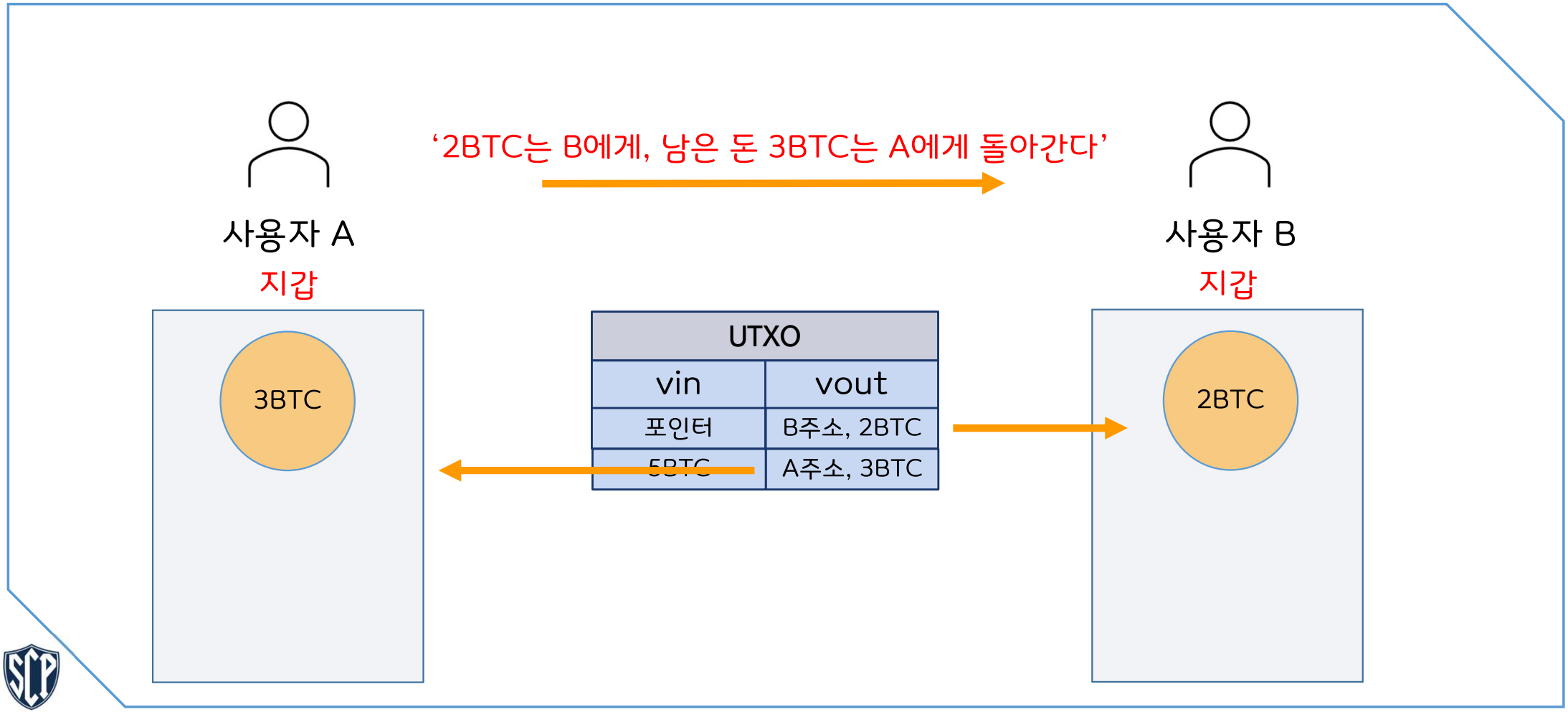


• 자산추적 원리

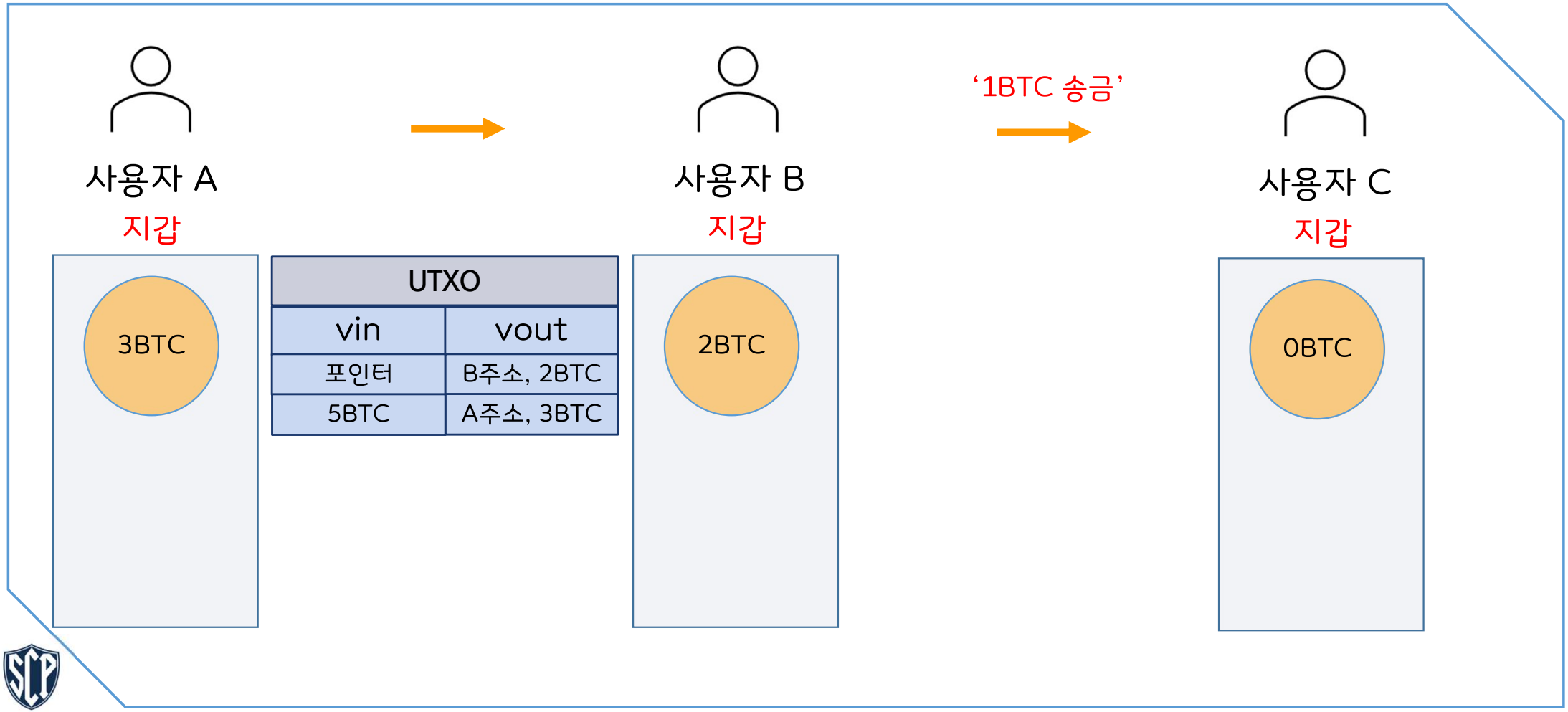


UTXO	
vin	vout
포인터	B주소, 2BTC
5BTC	A주소, 3BTC

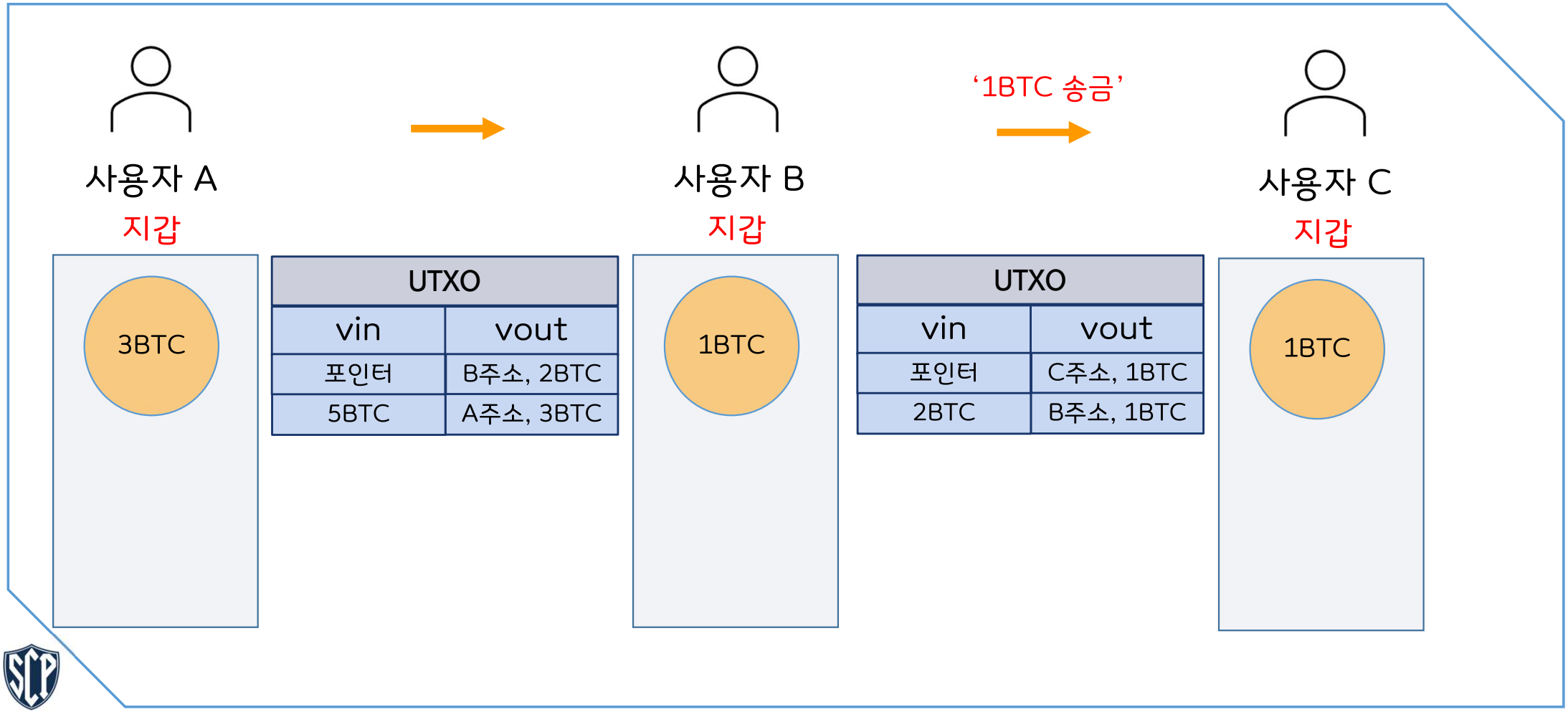
• 자산추적 원리


'2BTC는 B에게, 남은 돈 3BTC는 A에게 돌아간다'
사용자 A
지갑
사용자 B
지갑
3BTC
UTXO
vin
vout
포인터
B주소, 2BTC
5BTC
A주소, 3BTC
2BTC

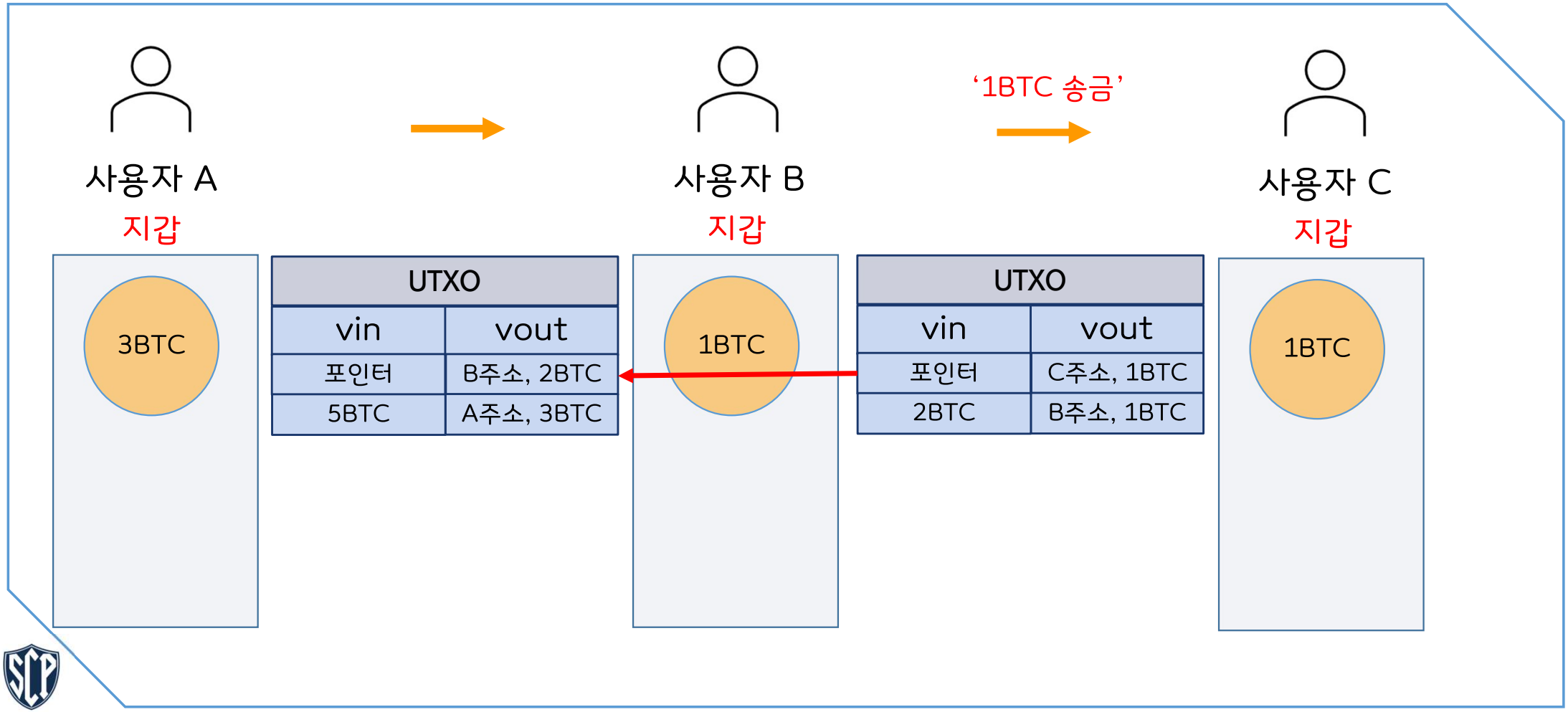
• 자산추적 원리


사용자 A
지갑
3BTC
UTXO
vin
vout
포인터
B주소, 2BTC
5BTC
A주소, 3BTC
사용자 B
지갑
2BTC
'1BTC 송금'
사용자 C
지갑
0BTC

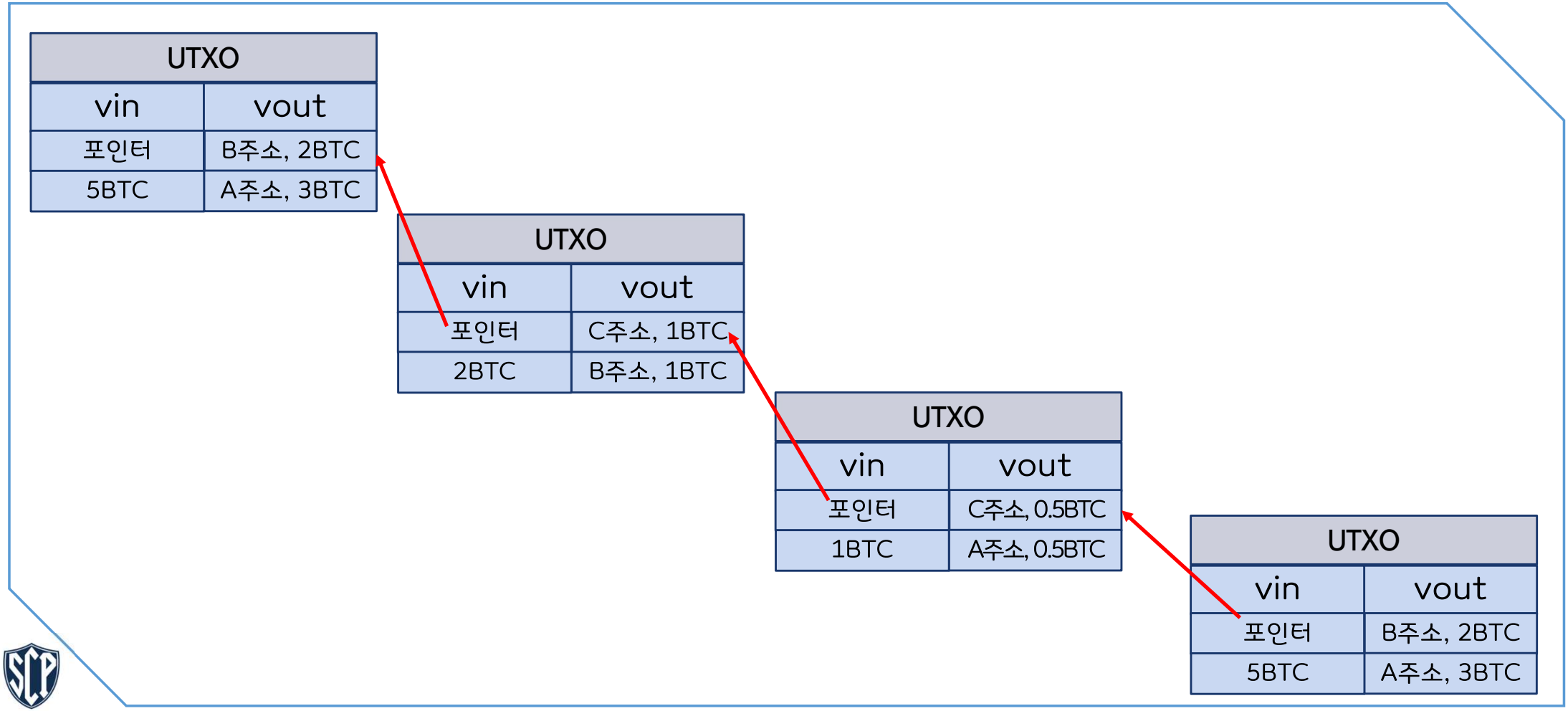
• 자산추적 원리


사용자 A
지갑
3BTC
UTXO
vin
vout
포인터
B주소, 2BTC
5BTC
A주소, 3BTC
사용자 B
지갑
1BTC
'1BTC 송금'
UTXO
vin
vout
포인터
C주소, 1BTC
2BTC
B주소, 1BTC
사용자 C
지갑
1BTC

• 자산추적 원리


사용자 A
지갑
3BTC
사용자 B
지갑
1BTC
UTXO
vin
vout
포인터
B주소, 2BTC
5BTC
A주소, 3BTC
'1BTC 송금'
사용자 C
지갑
1BTC
UTXO
vin
vout
포인터
C주소, 1BTC
2BTC
B주소, 1BTC

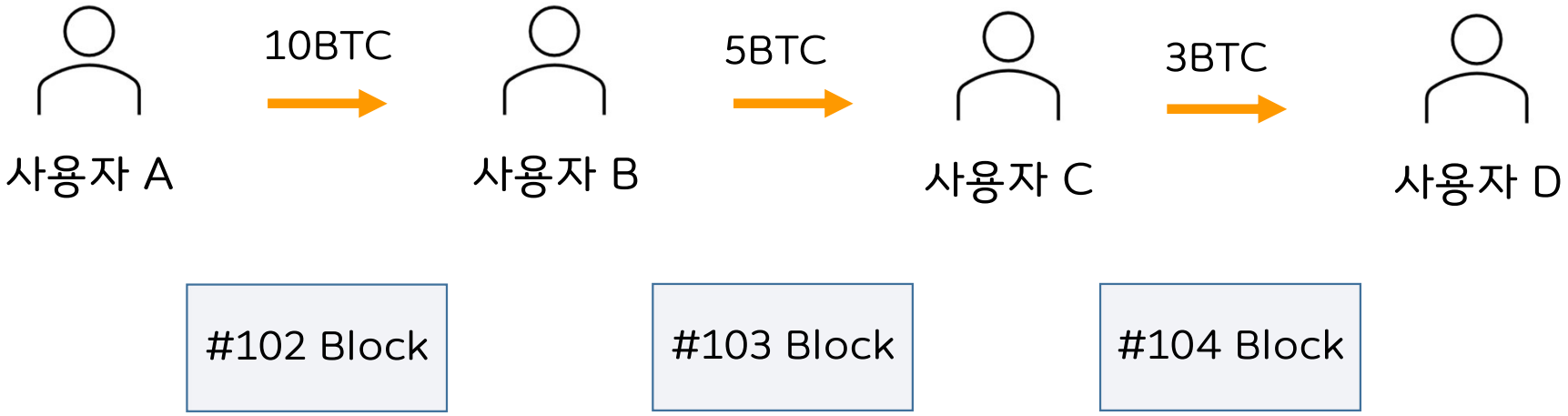
• 자산추적 원리


UTXO
vin
vout
포인터
B주소, 2BTC
5BTC
A주소, 3BTC
UTXO
vin
vout
포인터
C주소, 1BTC
2BTC
B주소, 1BTC
UTXO
vin
vout
포인터
C주소, 0.5BTC
1BTC
A주소, 0.5BTC
UTXO
vin
vout
포인터
B주소, 2BTC
5BTC
A주소, 3BTC

04

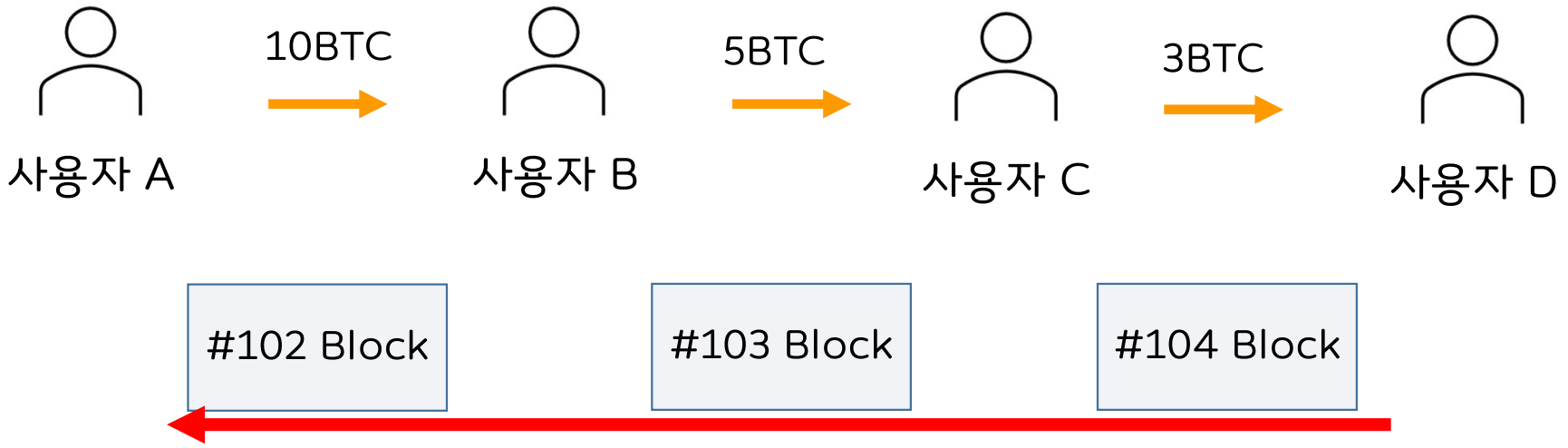
실습 및 목표

• 실습 및 목표



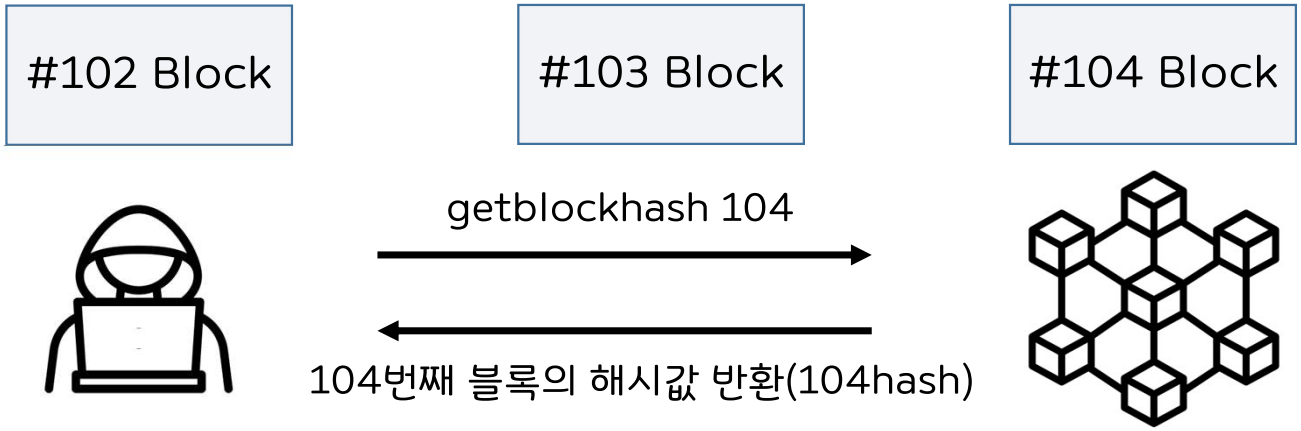
테스트를 위한 환경구성

• 실습 및 목표



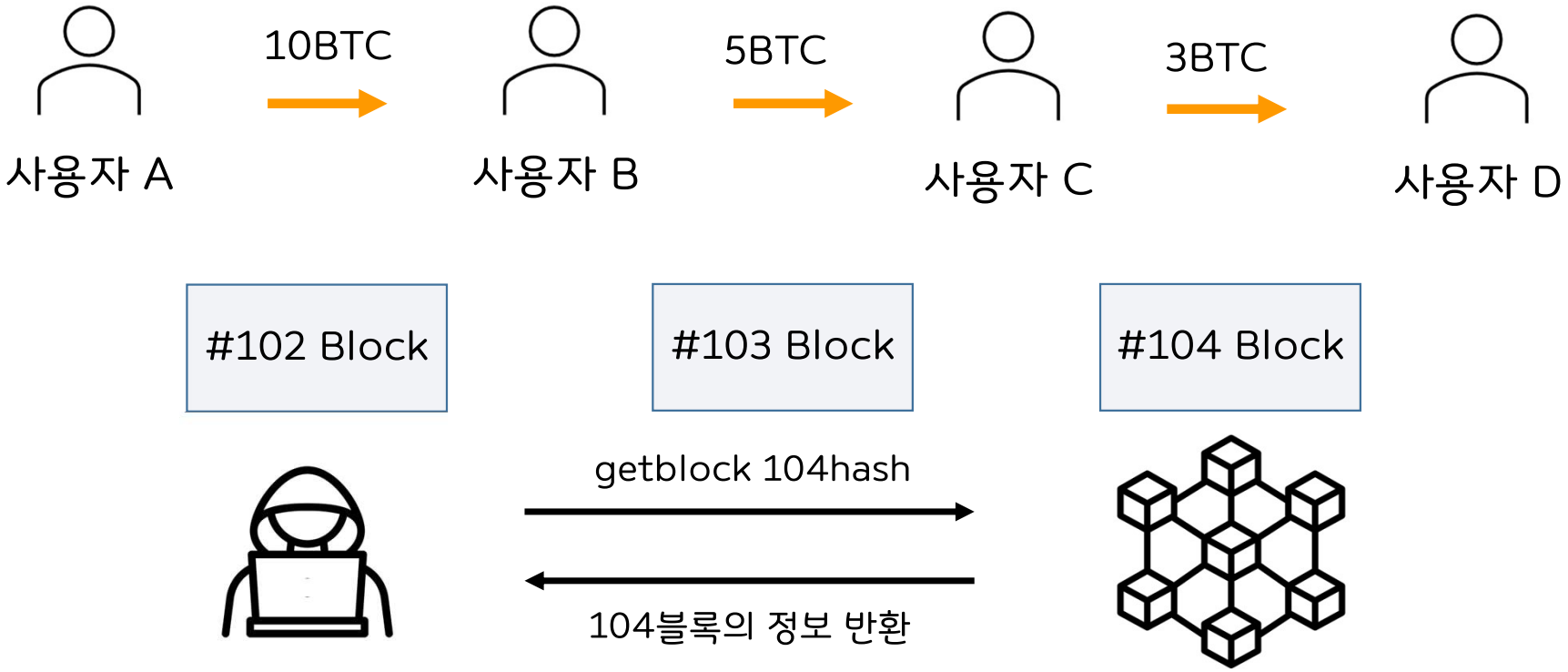
104번째에 있는 거래내역으로부터
거슬러 올라가보자

• 실습 및 목표

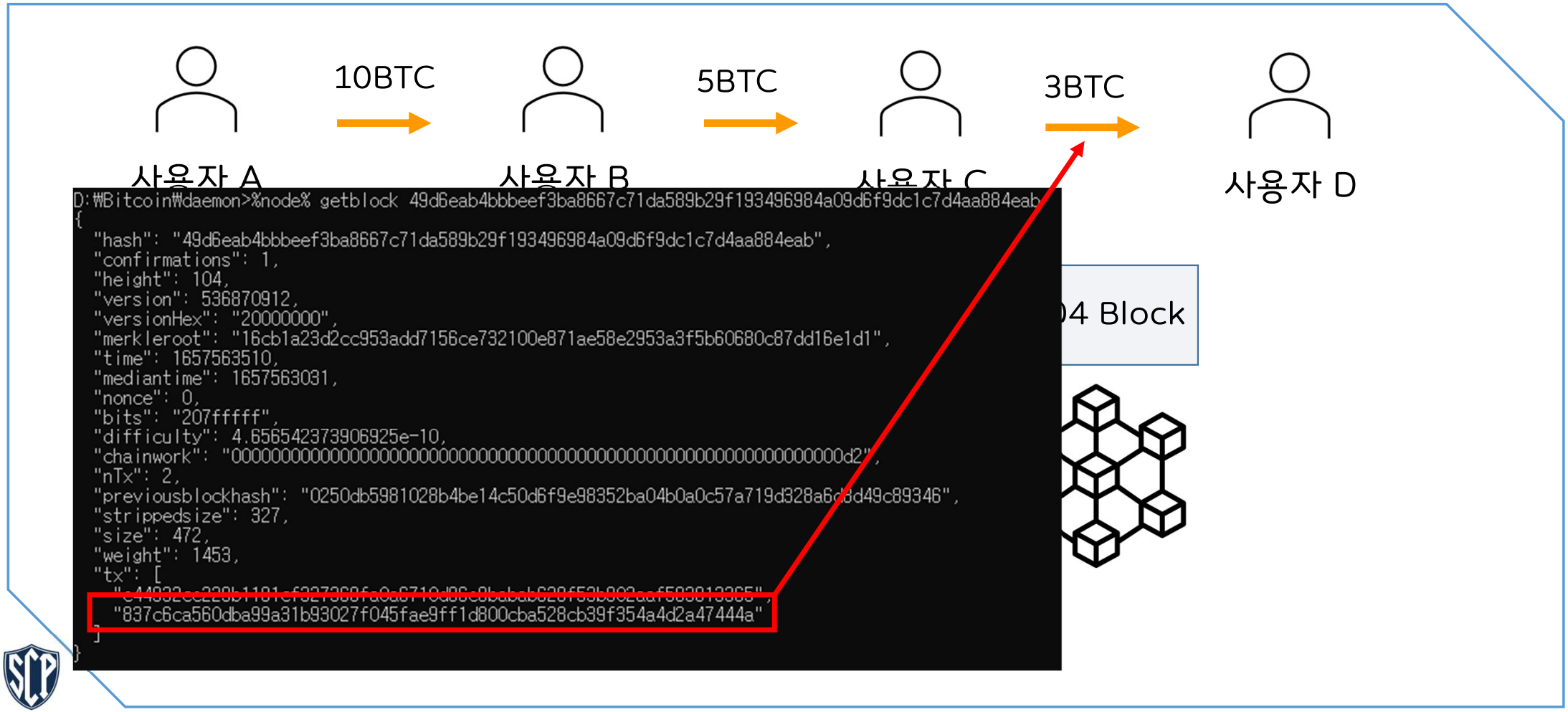



```
D:₩Bitcoin₩daemon>%node% getblockhash 104
49d6eab4bbbeef3ba8667c71da589b29f193496984a09d6f9dc1c7d4aa884eab
```

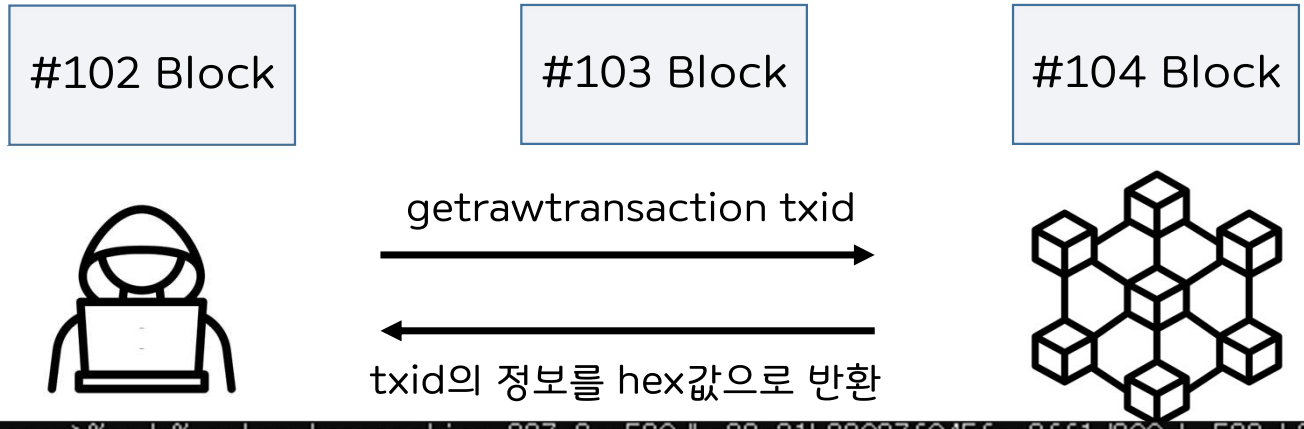
• 실습 및 목표


10BTC
5BTC
3BTC
사용자 A
사용자 B
사용자 C
사용자 D
#102 Block
#103 Block
#104 Block
getblock 104hash
104블록의 정보 반환

• 실습 및 목표

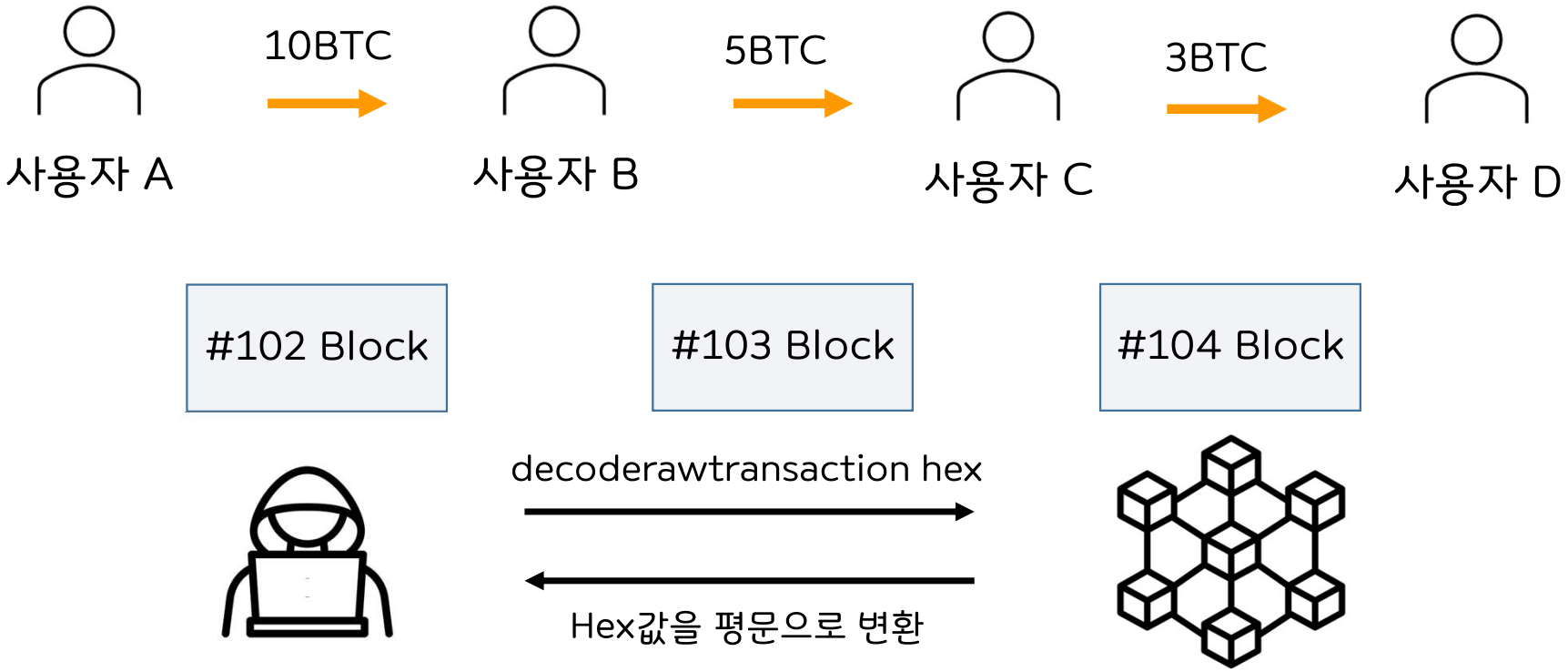

10BTC
5BTC
3BTC
사용자 A
사용자 B
사용자 C
사용자 D
D:₩Bitcoin₩daemon>%node% getblock 49d6eab4bbbeef3ba8667c71da589b29f193496984a09d6f9dc1c7d4aa884eab
{
"hash": "49d6eab4bbbeef3ba8667c71da589b29f193496984a09d6f9dc1c7d4aa884eab",
"confirmations": 1,
"height": 104,
"version": 536870912,
"versionHex": "20000000",
"merkleroot": "16cb1a23d2cc953add7156ce732100e871ae58e2953a3f5b60680c87dd16e1d1",
"time": 1657563510,
"mediantime": 1657563031,
"nonce": 0,
"bits": "207fffff",
"difficulty": 4.656542373906925e-10,
"chainwork": "00000000000000000000000000000000000000000000000000000000000000d2",
"nTx": 2,
"previousblockhash": "0250db5981028b4be14c50d6f9e98352ba04b0a0c57a719d328a6d8d49c89346",
"strippedsize": 327,
"size": 472,
"weight": 1453,
"tx": [
"837c6ca560dba99a31b93027f045fae9ff1d800cba528cb39f354a4d2a47444a"
]
}
04 Block

• 실습 및 목표




```
D:₩Bitcoin₩daemon>%node% getrawtransaction 837c6ca560dba99a31b93027f045fae9ff1d800cba528cb39f354a4d2a47444a
02000000000101bd1097a089aac6dcd4aad818a0f158ebcc50b0f17b3da63b62d08dad2b1a38c50000000000fdffffff023bb4eb0b000000001600
143e324f34efdacbbe7a3d18d6e7d74389124ce1c900a3e11100000000160014ffaaf9a037379b6256c4d481811a14d40e16acb5024730440220
48981785675804ba54e3547c0480cf3c993c6d045770e0aefad4b6818964604c02200ab1c75e9240eada4be58118de11f26690e7234bf5daddc3e
abf94e5cbdbe5f40121030329e1f66f4aee226b7d82aa4362ef6d6eff513b3297a99bcdad89e3b02b922b42000000
```

• 실습 및 목표


10BTC
5BTC
3BTC
사용자 A
사용자 B
사용자 C
사용자 D
#102 Block
#103 Block
#104 Block
decoderawtransaction hex
Hex값을 평문으로 변환

```
{
  "txid": "837c6ca560dba99a31b93027f045fae9ff1d800cba528cb39f354a4d2a47444a",
  "hash": "4b690af8489381fb93d5be56d712e29129c00ca4210e8fe99cd0eed4e8ee7753",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 66,
  "vin": [
    {
      "txid": "c5381a2bad8dd0623ba63d7bf1b050cceb58f1a018d8aad4dcc6aa89a09710bd",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "3044022048981785675804ba54e3547c0480cf3c993c6d045770e0aefad4b6818964604c0
90e7234bf5daddc3eabf94e5cbdbe5f401",
        "030329e1f66f4aee226b7d82aa4362ef6d6eff513b3297a99bcdad89e3b02b922b"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 1.99996475,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 3e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "desc": "addr(bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw)#qakcyyrq",
        "hex": "00143e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "address": "bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 3.00000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "desc": "addr(bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr)#dygnqqpl",
        "hex": "0014ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "address": "bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr",
        "type": "witness_v0_keyhash"
      }
    }
  ]
}
```


#104 Block

사용자 C

지갑

5BTC -3BTC = 2BTC

사용자 D

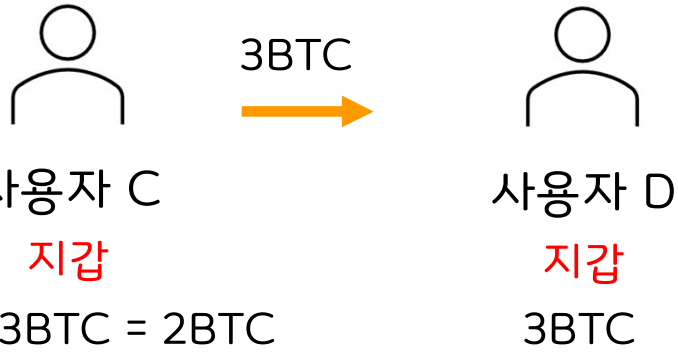
지갑

3BTC

C가 D에게 보냈던 3BTC에 대한
거래내역을 볼 수 있다.

```
{
  "txid": "837c6ca560dba99a31b93027f045fae9ff1d800cba528cb39f354a4d2a47444a",
  "hash": "4b690af8489381fb93d5be56d712e29129c00ca4210e8fe99cd0eed4e8ee7753",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 66,
  "vin": [
    {
      "txid": "c5381a2bad8dd0623ba63d7bf1b050cceb58f1a018d8aad4dcc6aa89a09710bd",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402204898178567580 4ba54e3547c0480cf3c993c6d045770e0aefad4b6818964604c
0e7234bf5daddc3eabf94e5cbdbe5f401",
        "030329e1f66f4aee226b7d82aa4362ef6d6eff513b3297a99bcdad89e3b02b922b"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 1.99996475,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 3e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "desc": "addr(bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw)#qakcyyrq",
        "hex": "00143e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "address": "bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 3.00000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "desc": "addr(bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr)#dygnqqpl",
        "hex": "0014ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "address": "bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr",
        "type": "witness_v0_keyhash"
      }
    }
  ]
```

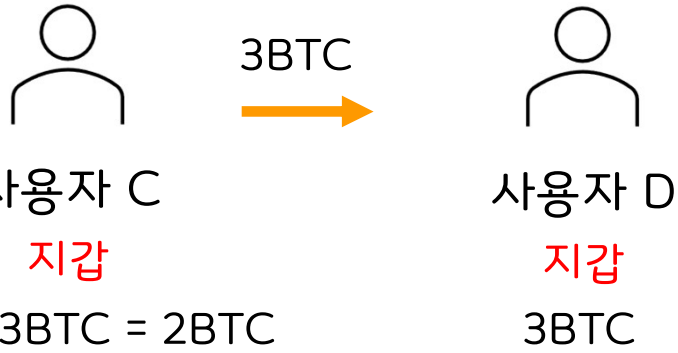

#104 Block



해당영역이 UTXO부분

```
{
  "txid": "837c6ca560dba99a31b93027f045fae9ff1d800cba528cb39f354a4d2a47444a",
  "hash": "4b690af8489381fb93d5be56d712e29129c00ca4210e8fe99cd0eed4e8ee7753",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 66,
  "vin": [
    {
      "txid": "c5381a2bad8dd0623ba63d7bf1b050cceb58f1a018d8aad4dcc6aa89a09710bd",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402204898178567580 4ba54e3547c0480cf3c993c6d045770e0aefad4b6818964604
0e7234bf5daddc3eabf94e5cbdbe5f401",
        "030329e1f66f4aee226b7d82aa4362ef6d6eff513b3297a99bcdad89e3b02b922b"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 1.99996475,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 3e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "desc": "addr(bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw)#qakcyyrq",
        "hex": "00143e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "address": "bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 3.00000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "desc": "addr(bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr)#dygnqqpl",
        "hex": "0014ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "address": "bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr",
        "type": "witness_v0_keyhash"
      }
    }
  ]
}
```


#104 Block



해당영역이 vin부분

```
{
  "txid": "837c6ca560dba99a31b93027f045fae9ff1d800cba528cb39f354a4d2a47444a",
  "hash": "4b690af8489381fb93d5be56d712e29129c00ca4210e8fe99cd0eed4e8ee7753",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 66,
  "vin": [
    {
      "txid": "c5381a2bad8dd0623ba63d7bf1b050cceb58f1a018d8aad4dcc6aa89a09710bd",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "3044022048981785675804ba54e3547c0480cf3c993c6d045770e0aefad4b6818964604c
0e7234bf5daddc3eabf94e5cbdbe5f401",
        "030329e1f66f4aee226b7d82aa4362ef6d6eff513b3297a99bcdad89e3b02b922b"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 1.99996475,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 3e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "desc": "addr(bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw)#qakcyyrq",
        "hex": "00143e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "address": "bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 3.00000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "desc": "addr(bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr)#dygnqqpl",
        "hex": "0014ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "address": "bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr",
        "type": "witness_v0_keyhash"
      }
    }
  ]
}
```


#104 Block

지갑

5BTC -3BTC = 2BTC

사용자 D

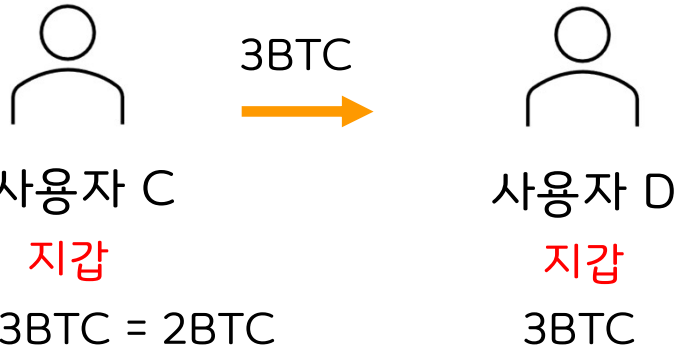
지갑

3BTC

해당 영역이 vout부분

```
{
  "txid": "837c6ca560dba99a31b93027f045fae9ff1d800cba528cb39f354a4d2a47444a",
  "hash": "4b690af8489381fb93d5be56d712e29129c00ca4210e8fe99cd0eed4e8ee7753",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 66,
  "vin": [
    {
      "txid": "c5381a2bad8dd0623ba63d7bf1b050cceb58f1a018d8aad4dcc6aa89a09710bd",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402204898178567580 4ba54e3547c0480cf3c993c6d045770e0aefad4b6818964604c
30e7234bf5daddc3eabf94e5cbdbe5f401",
        "030329e1f66f4aee226b7d82aa4362ef6d6eff513b3297a99bcdad89e3b02b922b"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 1.99996475,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 3e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "desc": "addr(bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw)#qakcyyrq",
        "hex": "00143e324f34efdacbbe7a3d18d6e7d74389124ce1c9",
        "address": "bcrt1q8cey7d80mt9mu73arrtw046r3yfyecwfk29ucw",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 3.00000000,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "desc": "addr(bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr)#dygnqqpl",
        "hex": "0014ffaaf9a037379b6256c4d481811a14d40e16acb5",
        "address": "bcrt1ql740ngphx7dky4ky6jqczxs56s8pdt949qvuvr",
        "type": "witness_v0_keyhash"
      }
    }
  ]
```


#104 Block



해당부분이 이전 UTXO에 대한 포인터
해당 포인터는
사용자 B와 사용자 C간의 거래를
가리킨다.

```
{
  "txid": "c5381a2bad8dd0623ba63d7bf1b050cceb58f1a018d8aad4dcc6aa89a09710bd",
  "hash": "6ad6f424d60a6343d46e19ddc4793b8b079dbcb661bc1ae6429d89d8b9523579",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 102,
  "vin": [
    {
      "txid": "4f91c18dfcdb50e68b48ff3ee89ebf42f3c7fd0d4a2b14e331691829a7f22313",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402206d8d6ade01adaaec1248e8bb2a1de1b91f1f74e2bf4bac07c2ec184655d87789
5cd736228866a9bc243dc0bdabbad7c001",
        "02b44e72997265a07b05958d5527db5dcdab84677c40b0c985afb74fee79246881"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 5.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 60e0dc8aba7a6809a2ca5a5bca58e68bd409181a",
        "desc": "addr(bcrt1qvrsdez460f5qngk2tfdu5k8x302qjxq6d56zrm)#3suze9fh",
        "hex": "001460e0dc8aba7a6809a2ca5a5bca58e68bd409181a",
        "address": "bcrt1qvrsdez460f5qngk2tfdu5k8x302qjxq6d56zrm",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 4.99996475,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 4aa6402a3ad889c5c5827eb4642da593a7524b34",
        "desc": "addr(bcrt1qf2nyq236mzyut3vz066xgtd9jwn4yje55r9kmq)#hsv0d6hp",
        "hex": "00144aa6402a3ad889c5c5827eb4642da593a7524b34",
        "address": "bcrt1qf2nyq236mzyut3vz066xgtd9jwn4yje55r9kmq",
        "type": "witness_v0_keyhash"
      }
    }
  ]
}
```


#103 Block

사용자 B

지갑

10BTC − 5BTC = 5BTC

사용자 C

지갑

5BTC

해당부분이 이전 UTXO에 대한 포인터

```
{
  "txid": "4f91c18dfcdb50e68b48ff3ee89ebf42f3c7fd0d4a2b14e331691829a7f22313",
  "hash": "d69bf54572aa2e95eef4f9badb4814ba85ba670397523b2804cda2d4005833f9",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 101,
  "vin": [
    {
      "txid": "18b7147f5fafdbf8290c593b904fb5d65b26606ca825c5411a3a73a630bb99a4",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402204104e4608eb04a665afa1ce1252c9f34649a3ba973a0b3e354a0088a5e9247b9
62ece2f3b71eed813d6c95858b2ca4e801",
        "02a3d0cdc287fadcfa24cce9034f2f8c0ba5d9b563f40a78cb9124cd3ff88610ba"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 10.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 1d56482ba29a8febfeeace2677d5736c0f3f5e2a",
        "desc": "addr(bcrt1qr4tys2azn287hlh2ecn804tnds8n7h32wjsxfg)#hlec6sgc",
        "hex": "00141d56482ba29a8febfeeace2677d5736c0f3f5e2a",
        "address": "bcrt1qr4tys2azn287hlh2ecn804tnds8n7h32wjsxfg",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 39.99996475,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 3ed7f6efaa5dacf10662e14d9a0af56ef5fcdbbd",
        "desc": "addr(bcrt1q8mtldma2tkk0zpnzu9xe5zh4dm6lekaauzf2mw)#9tpws2rm",
        "hex": "00143ed7f6efaa5dacf10662e14d9a0af56ef5fcdbbd",
        "address": "bcrt1q8mtldma2tkk0zpnzu9xe5zh4dm6lekaauzf2mw",
        "type": "witness_v0_keyhash"
      }
    }
  ]
}
```


#102 Block

사용자 A

지갑

50BTC − 10BTC = 40BTC

사용자 B

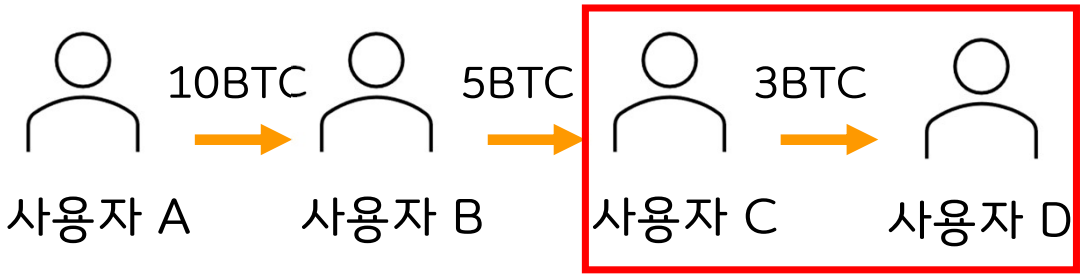
지갑

10BTC

이런식으로 거슬러올라갈 수 있다.

```
{
  "txid": "4f91c18dfcdb50e68b48ff3ee89ebf42f3c7fd0d4a2b14e331691829a7f22313",
  "hash": "d69bf54572aa2e95eef4f9badb4814ba85ba670397523b2804cda2d4005833f9",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 101,
  "vin": [
    {
      "txid": "18b7147f5fafdbf8290c593b904fb5d65b26606ca825c5411a3a73a630bb99a4",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402204104e4608eb04a665afa1ce1252c9f34649a3ba973a0b3e354a0088a5e9247b9
62ece2f3b71eed813d6c95858b2ca4e801",
        "02a3d0cdc287fadcfa24cce9034f2f8c0ba5d9b563f40a78cb9124cd3ff88610ba"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 10.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 1d56482ba29a8febfeeace2677d5736c0f3f5e2a",
        "desc": "addr(bcrt1qr4tys2azn287hlh2ecn804tnds8n7h32wjsxfg)#hlec6sgc",
        "hex": "00141d56482ba29a8febfeeace2677d5736c0f3f5e2a",
        "address": "bcrt1qr4tys2azn287hlh2ecn804tnds8n7h32wjsxfg",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 39.99996475,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 3ed7f6efaa5dacf10662e14d9a0af56ef5fcdbbd",
        "desc": "addr(bcrt1q8mtldma2tkk0zpnzu9xe5zh4dm6lekaauzf2mw)#9tpws2rm",
        "hex": "00143ed7f6efaa5dacf10662e14d9a0af56ef5fcdbbd",
        "address": "bcrt1q8mtldma2tkk0zpnzu9xe5zh4dm6lekaauzf2mw",
        "type": "witness_v0_keyhash"
      }
    }
  ]
}
```

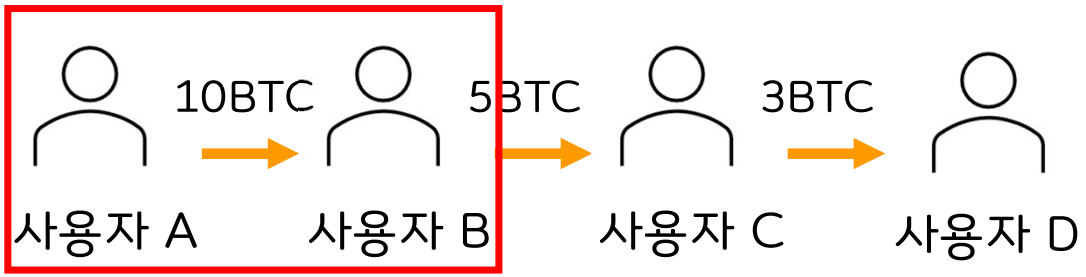

#102 Block



제일 마지막 거래부터 시작

```
{
  "txid": "4f91c18dfcdb50e68b48ff3ee89ebf42f3c7fd0d4a2b14e331691829a7f22313",
  "hash": "d69bf54572aa2e95eef4f9badb4814ba85ba670397523b2804cda2d4005833f9",
  "version": 2,
  "size": 222,
  "vsize": 141,
  "weight": 561,
  "locktime": 101,
  "vin": [
    {
      "txid": "18b7147f5fafdbf8290c593b904fb5d65b26606ca825c5411a3a73a630bb99a4",
      "vout": 0,
      "scriptSig": {
        "asm": "",
        "hex": ""
      },
      "txinwitness": [
        "304402204104e4608eb04a665afa1ce1252c9f34649a3ba973a0b3e354a0088a5e9247b9
62ece2f3b71eed813d6c95858b2ca4e801",
        "02a3d0cdc287fadcfa24cce9034f2f8c0ba5d9b563f40a78cb9124cd3ff88610ba"
      ],
      "sequence": 4294967293
    }
  ],
  "vout": [
    {
      "value": 10.00000000,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 1d56482ba29a8febfeeace2677d5736c0f3f5e2a",
        "desc": "addr(bcrt1qr4tys2azn287hlh2ecn804tnds8n7h32wjsxfg)#hlec6sgc",
        "hex": "00141d56482ba29a8febfeeace2677d5736c0f3f5e2a",
        "address": "bcrt1qr4tys2azn287hlh2ecn804tnds8n7h32wjsxfg",
        "type": "witness_v0_keyhash"
      }
    },
    {
      "value": 39.99996475,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 3ed7f6efaa5dacf10662e14d9a0af56ef5fcdbbd",
        "desc": "addr(bcrt1q8mtldma2tkk0zpnzu9xe5zh4dm6lekaauzf2mw)#9tpws2rm",
        "hex": "00143ed7f6efaa5dacf10662e14d9a0af56ef5fcdbbd",
        "address": "bcrt1q8mtldma2tkk0zpnzu9xe5zh4dm6lekaauzf2mw",
        "type": "witness_v0_keyhash"
      }
    }
  ]
}
```


#102 Block



가장 첫번째 부분까지 거슬러 올라감

• 실습 및 목표

"비트코인 트랜잭션 데이터 분석을 통한 거래 추적 및 분석 연구"

"비트코인 트랜잭션 데이터를 이용한 불법 거래 추적 연구"

"사이버 범죄에 악용되는 암호화폐 불법거래 추적"

• 실습 및 목표

"사이버 범죄에 악용되는 암호화폐 불법거래 추적"

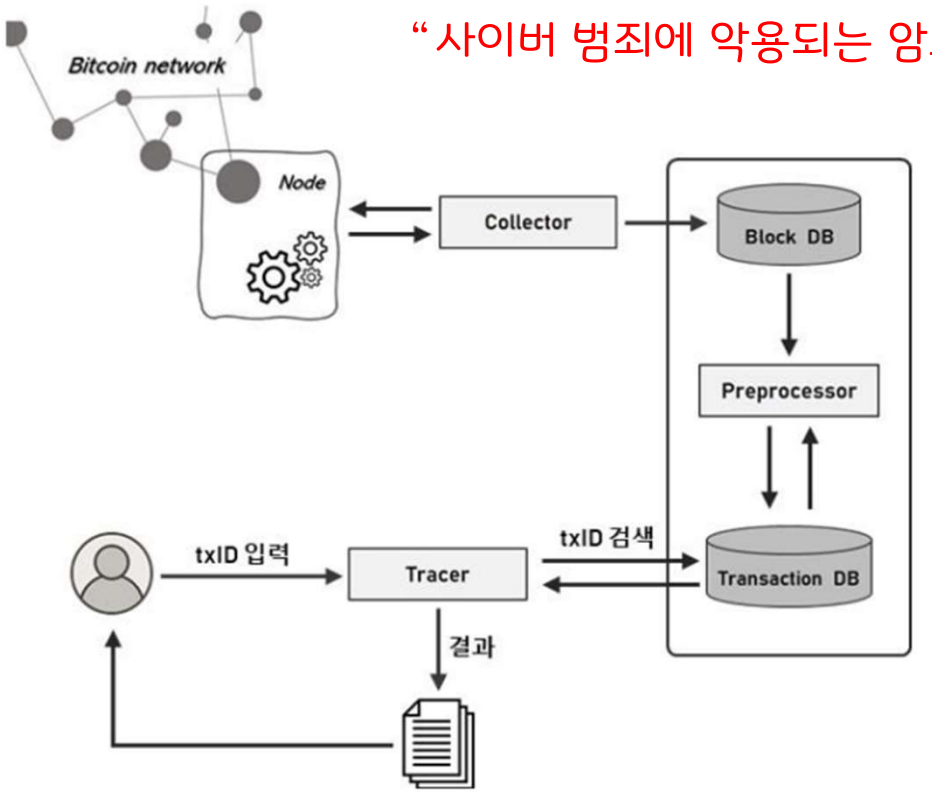


그림 4-3. UTXO 추적 방법

• 실습 및 목표

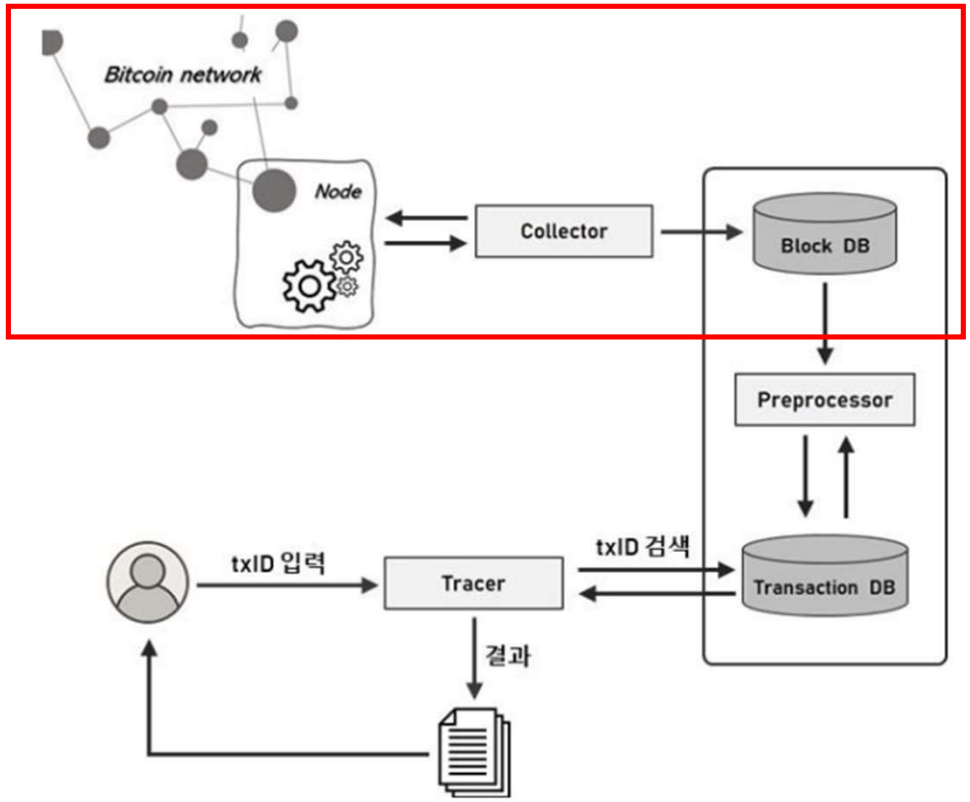


그림 4-3. UTXO 추적 방법

1. 비트코인 네트워크의 모든 블록을 Block DB에 저장

• 실습 및 목표

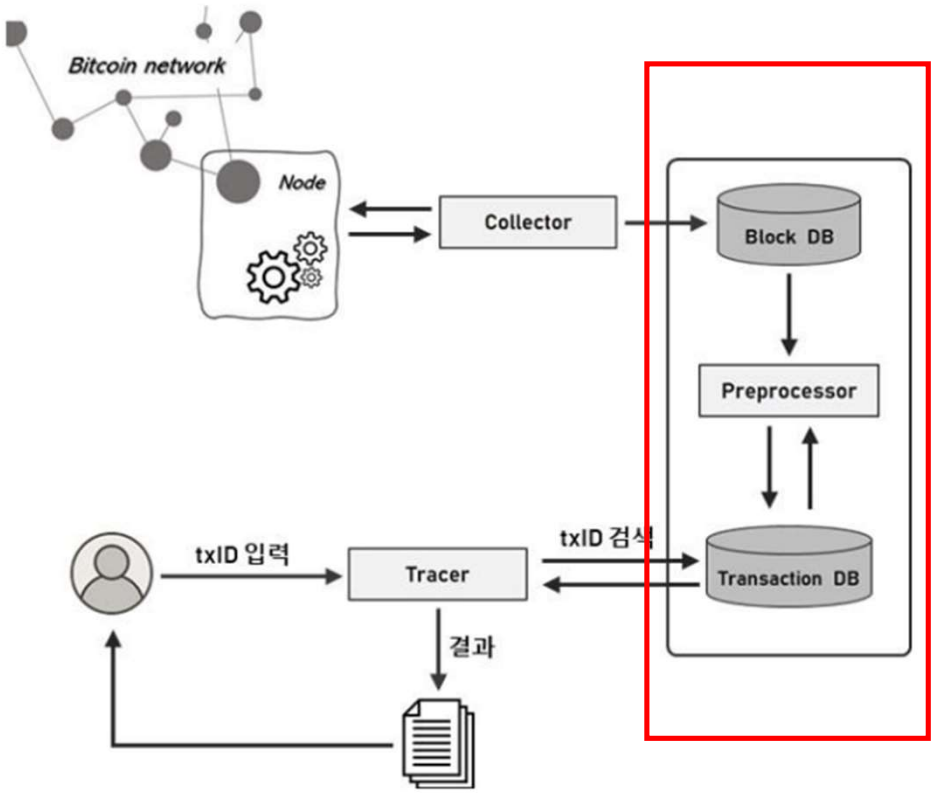


그림 4-3. UTXO 추적 방법

1. 비트코인 네트워크의 모든 블록을 Block DB에 저장

2. Block DB에서 거래내역만 Transaction DB에 저장

• 실습 및 목표

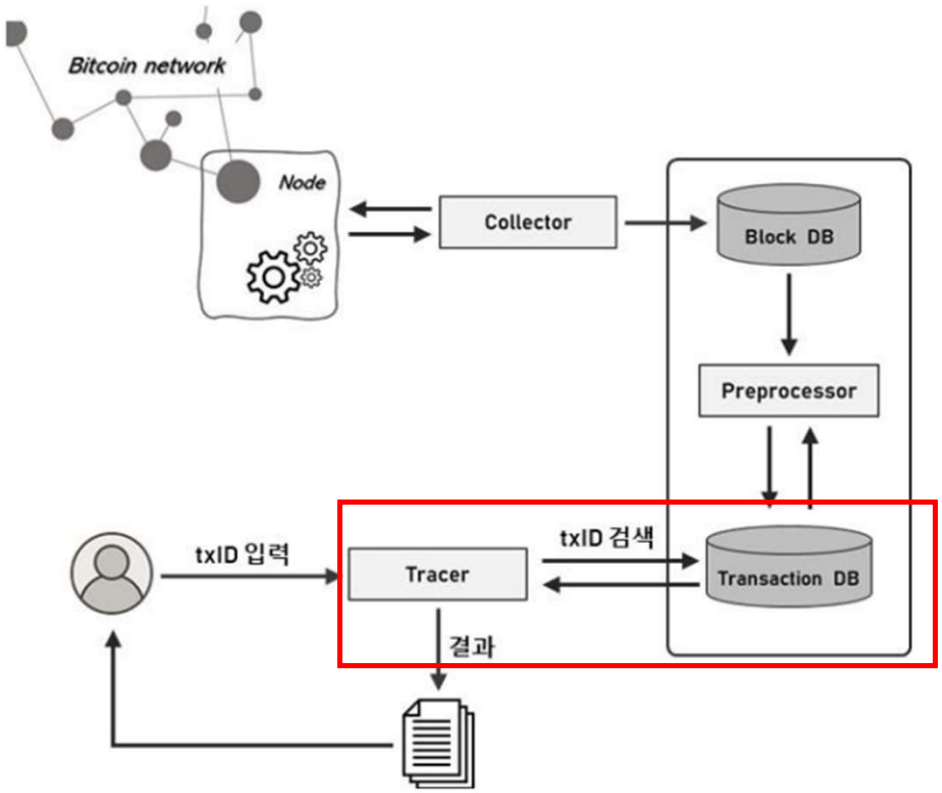


그림 4-3. UTXO 추적 방법

1. 비트코인 네트워크의 모든 블록을 Block DB에 저장

2. Block DB에서 거래내역만 Transaction DB에 저장

3. Transaction DB에 모인 거래내역을 Tracer를 통하면 해당 txID의 최종거래소 도착지 추적

• 실습 및 목표

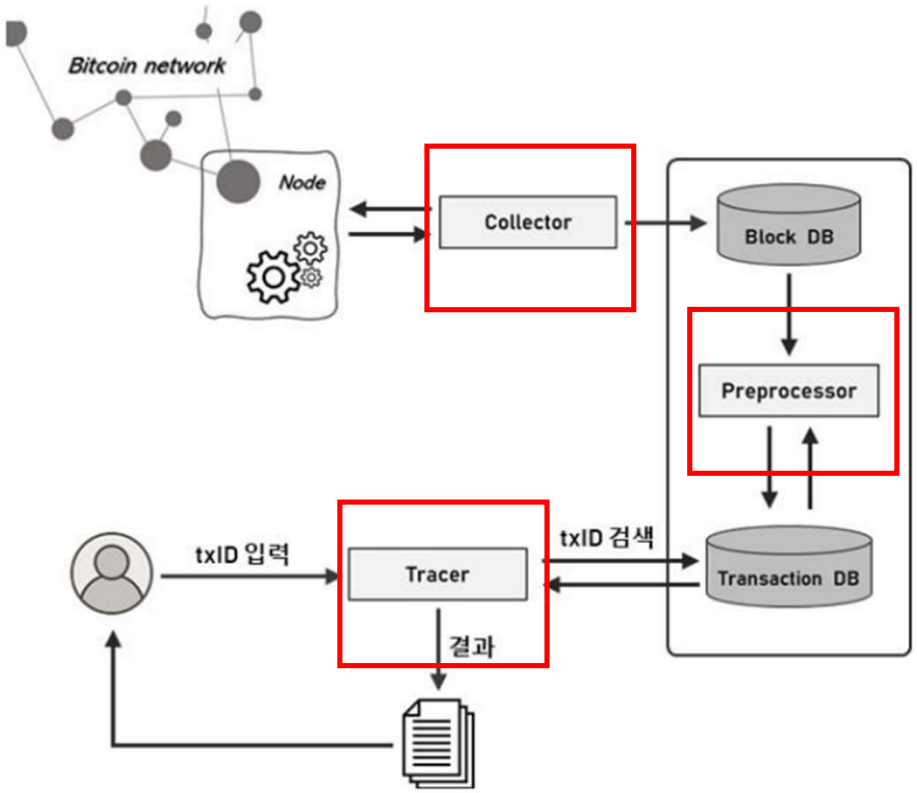


그림 4-3. UTXO 추적 방법

1. 비트코인 네트워크의 모든 블록을 Block DB에 저장

2. Block DB에서 거래내역만 Transaction DB에 저장

3. Transaction DB에 모인 거래내역을 Tracer를 통하면 해당 txID의 최종거래소 도착지 추적

4. 프로젝트 중, 만들어야 하는 프로그램은 Collector, Preprocessor, Tracer 총 3개이지만...

• 실습 및 목표

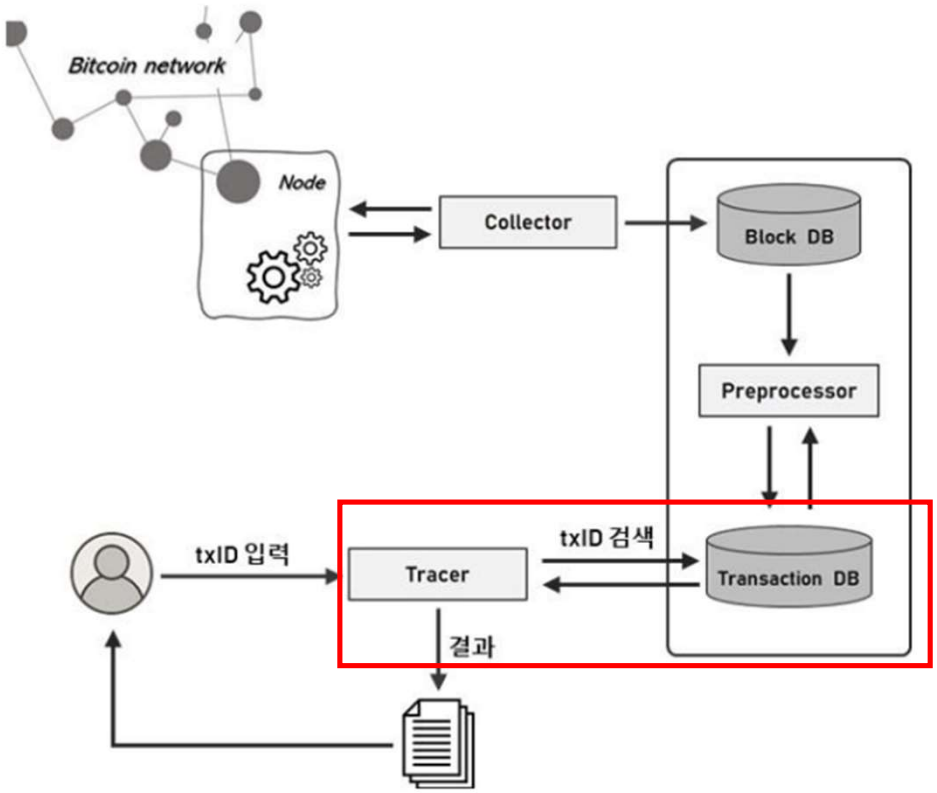


그림 4-3. UTXO 추적 방법

사실 이게 핵심이고 나머지는 필요가 없음

• 실습 및 목표

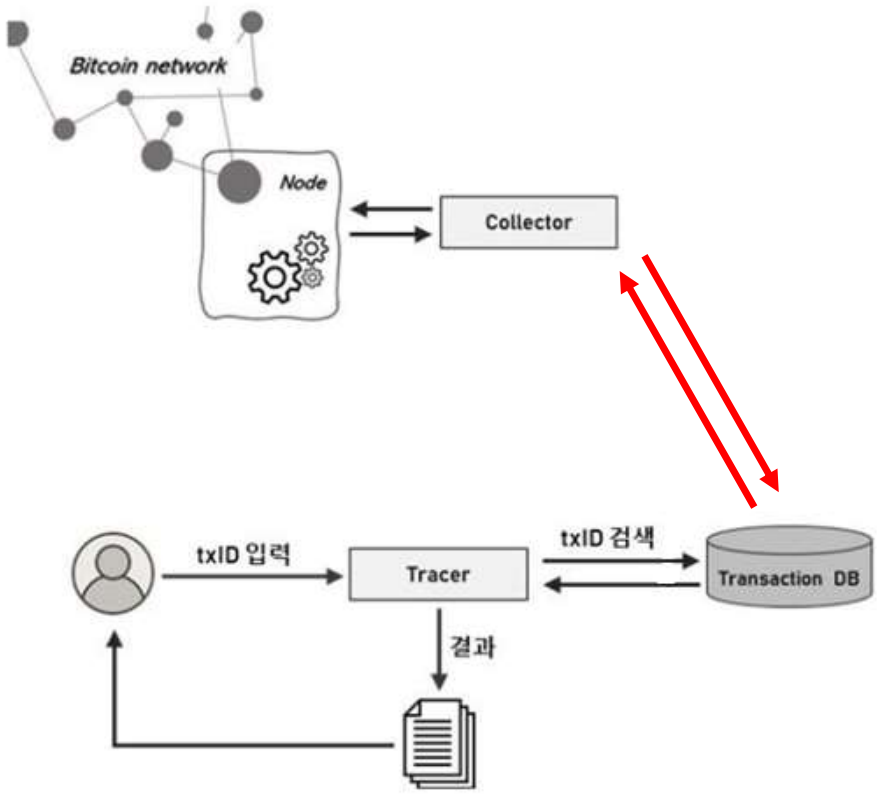


그림 4-3. UTXO 추적 방법

이렇게 만들면 또 가치가 있지 않을까?

Q & A

감사합니다:)