

비트코인 주소 생성 및 익명화

최승주

<https://youtu.be/wbpOUuXrS6M>

Contents

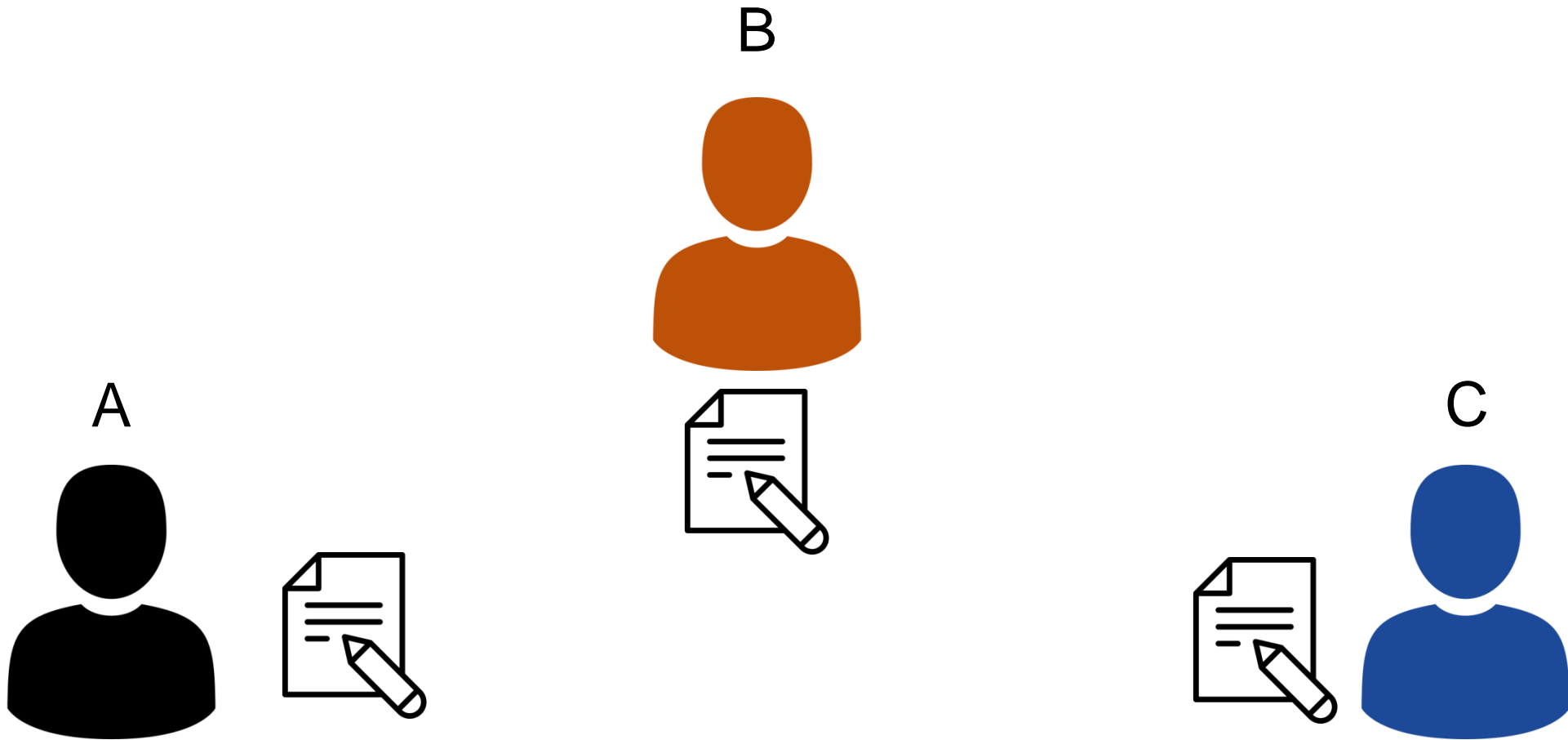
비트 코인 주소 생성 및 트랜잭션

블록체인 익명성 분석

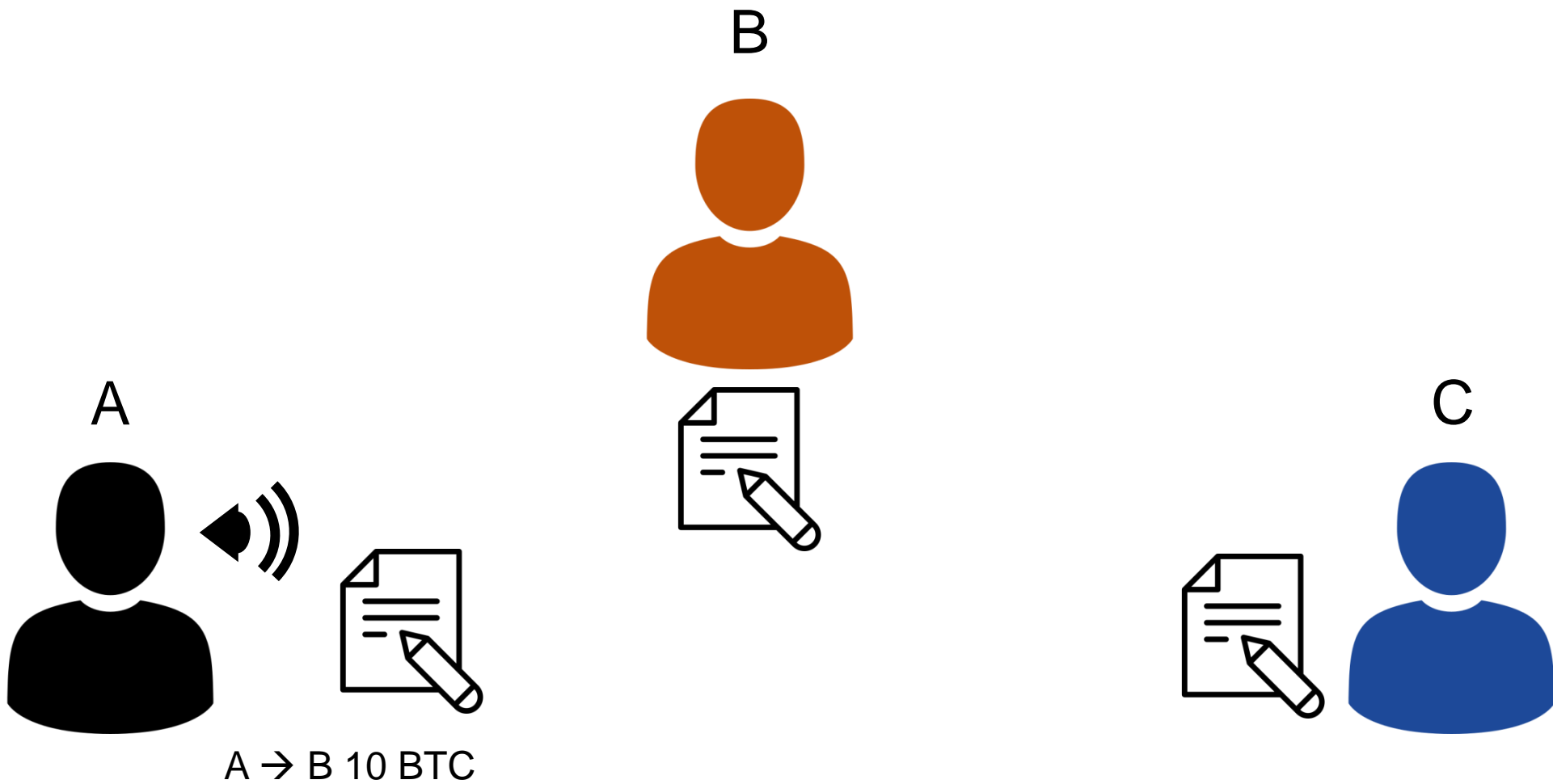


CryptoCraft LAB

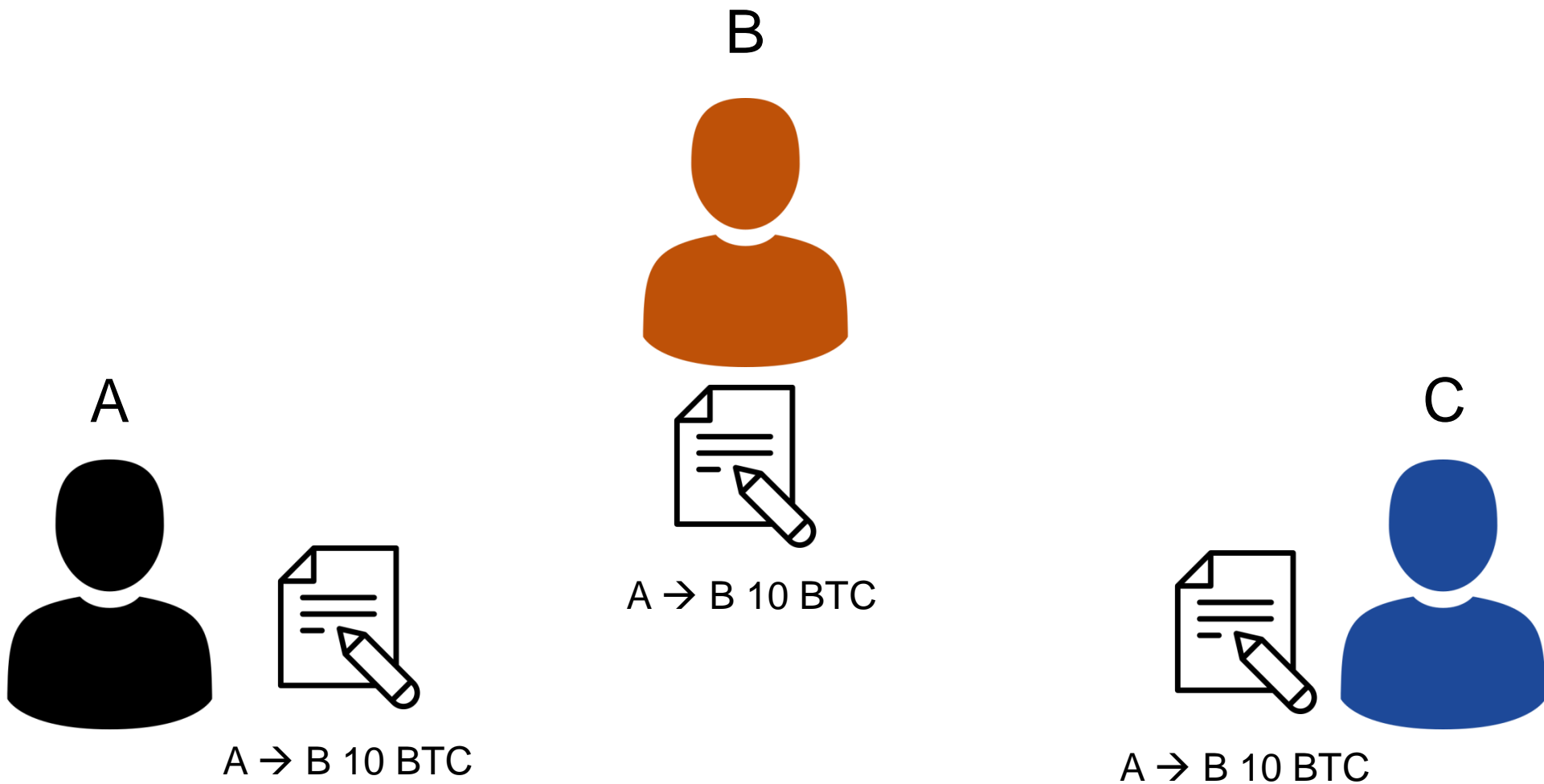
블록 체인



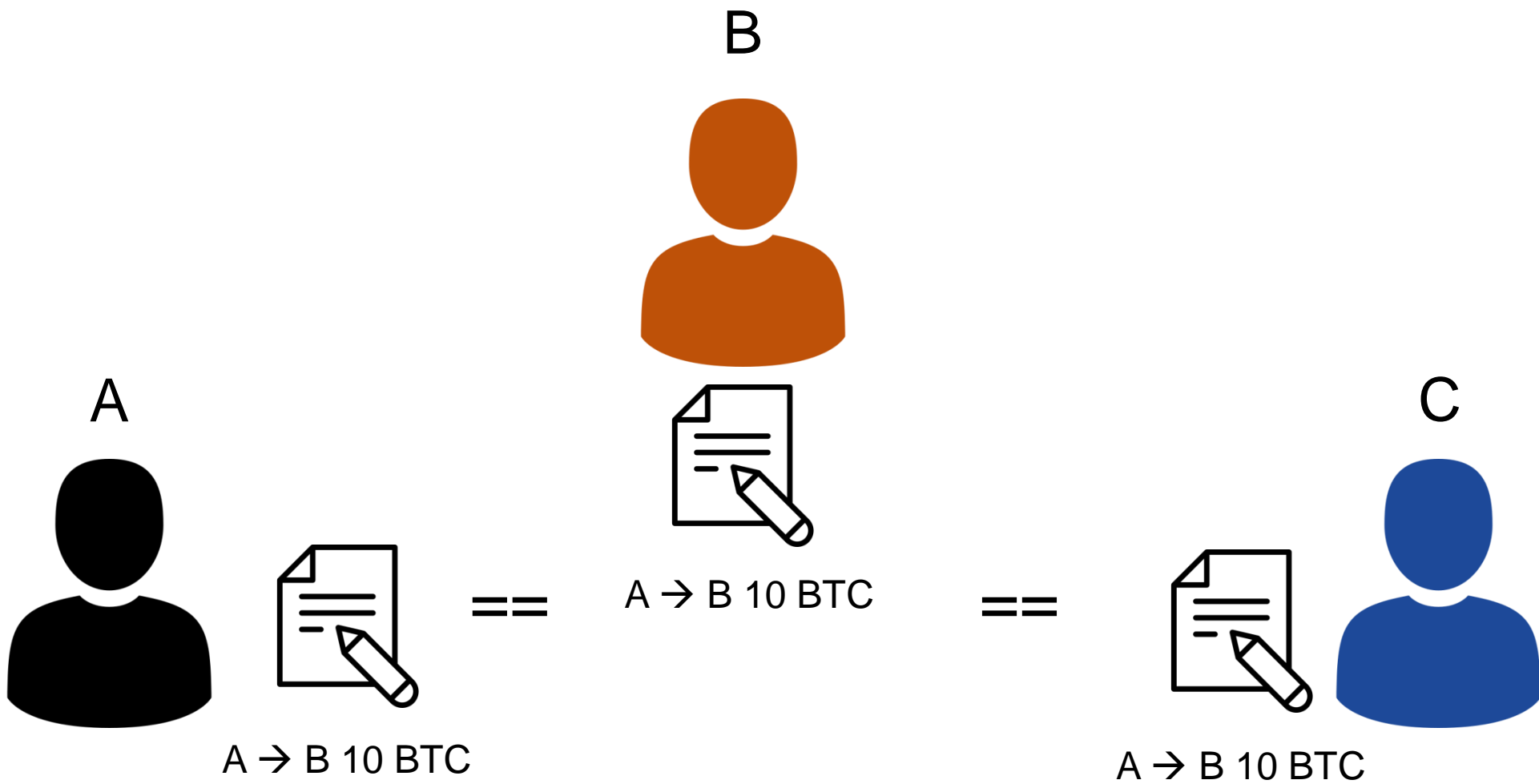
블록 체인



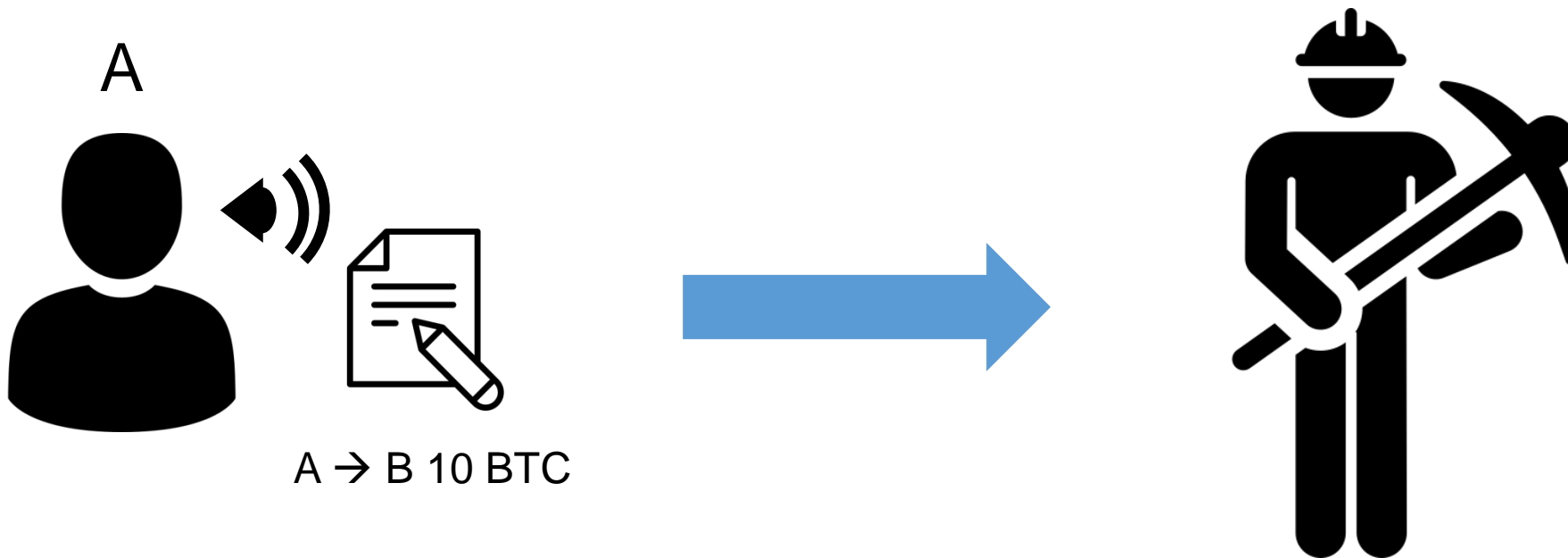
블록 체인



블록 체인



블록 체인



블록 체인

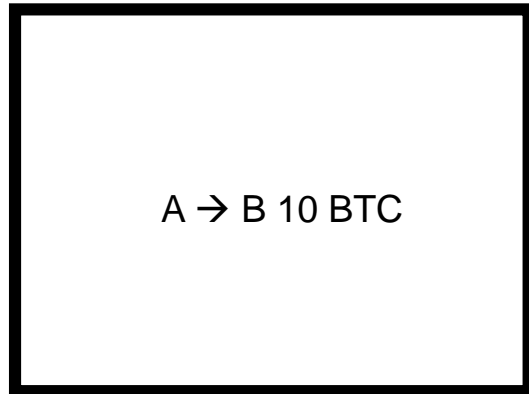


0xrq65q21128g

A → B 10 BTC

블록 체인

0xrq65q21128g



+



Value 1

Value 2

Value 3

...

= 0x15351...

= 0x9732...

= 0x48612...

Target:

Find less than
0x13948...

블록 체인

0xrq65q21128g

A → B 10 BTC

+



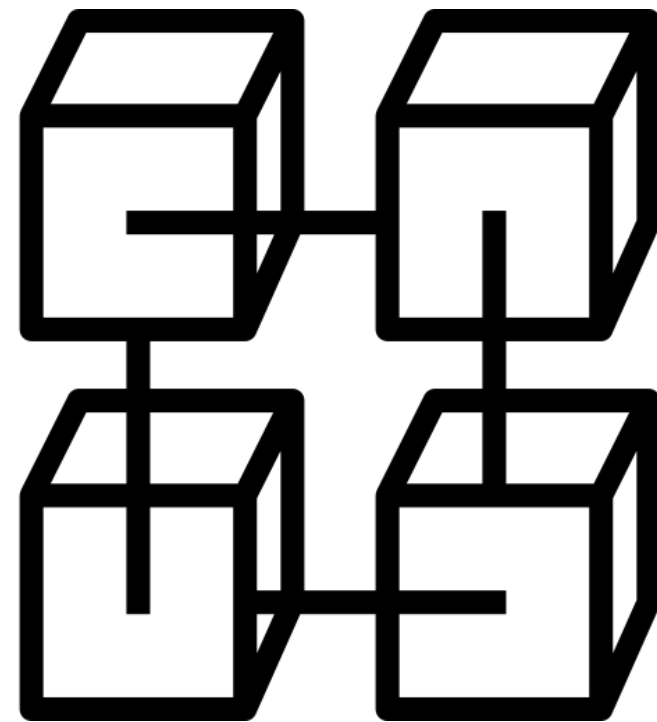
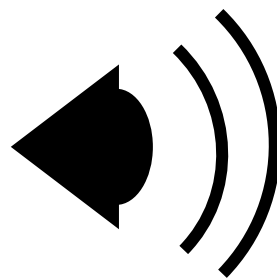
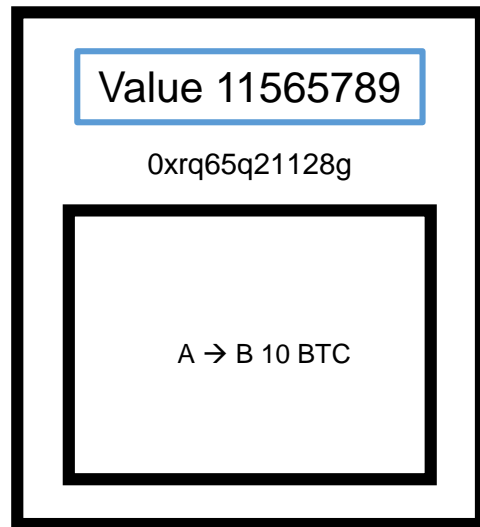
Value

11565789 = 0x128263...

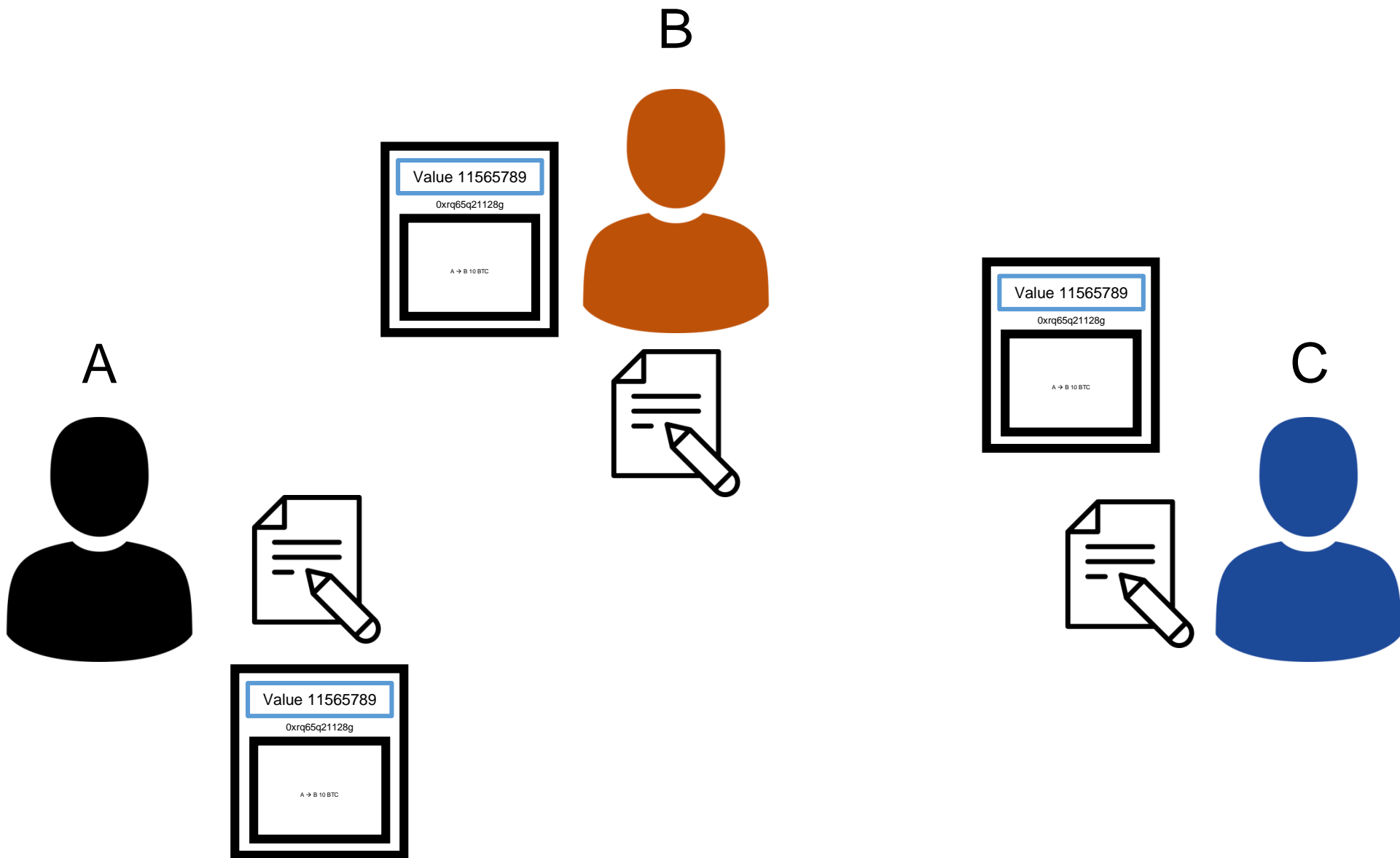
Target:

Find less than
0x13948...

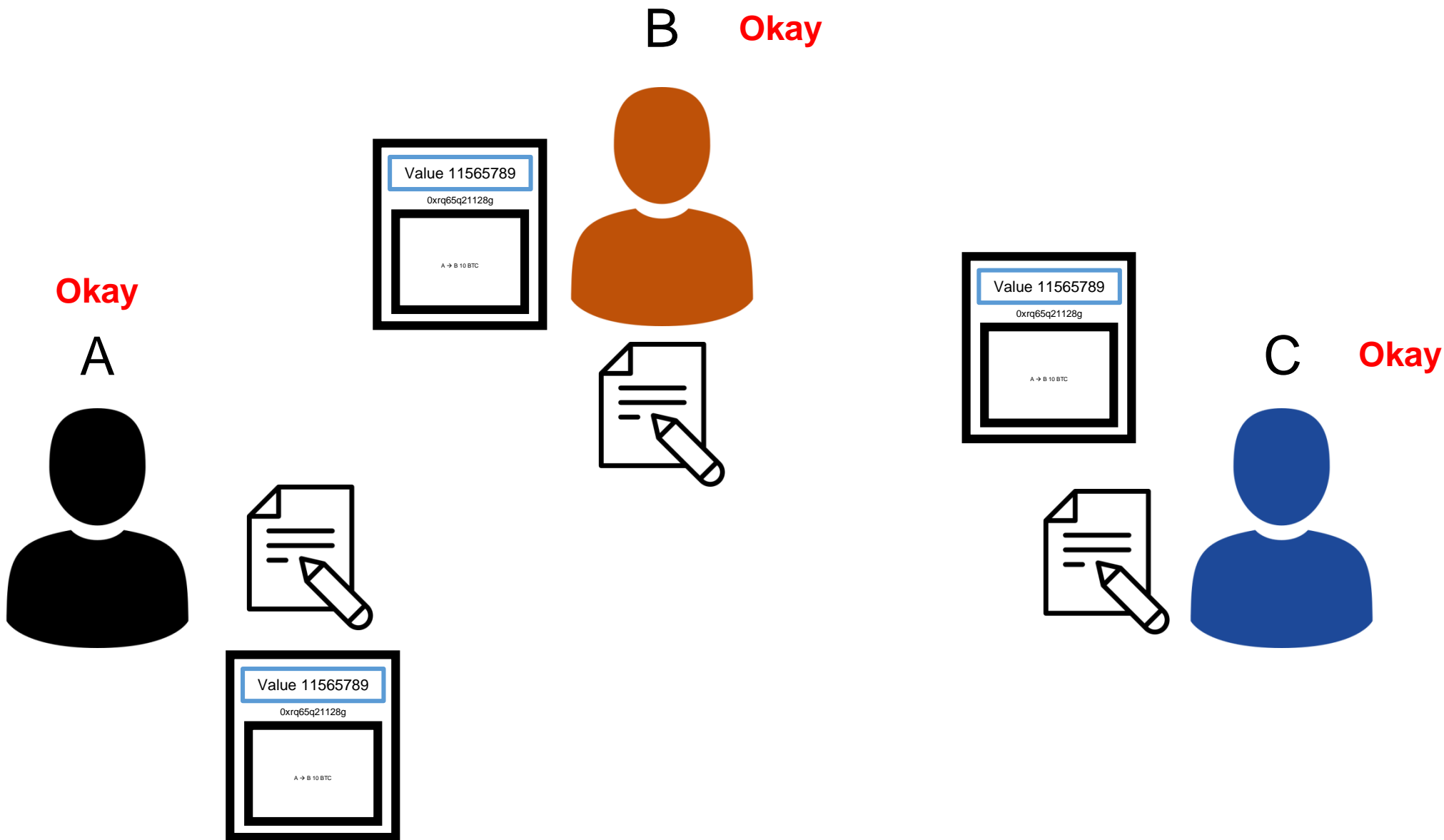
블록 체인



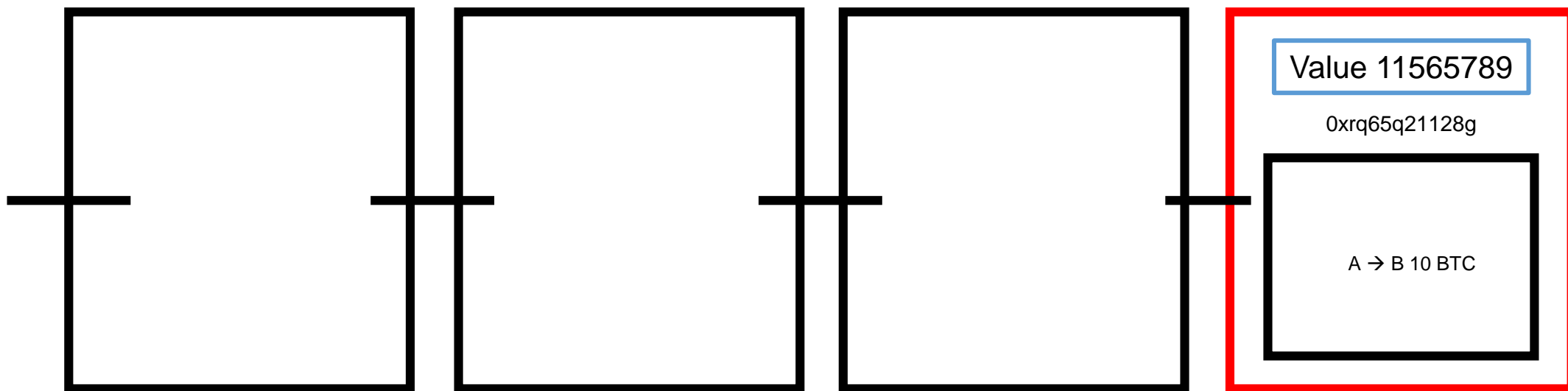
블록 체인



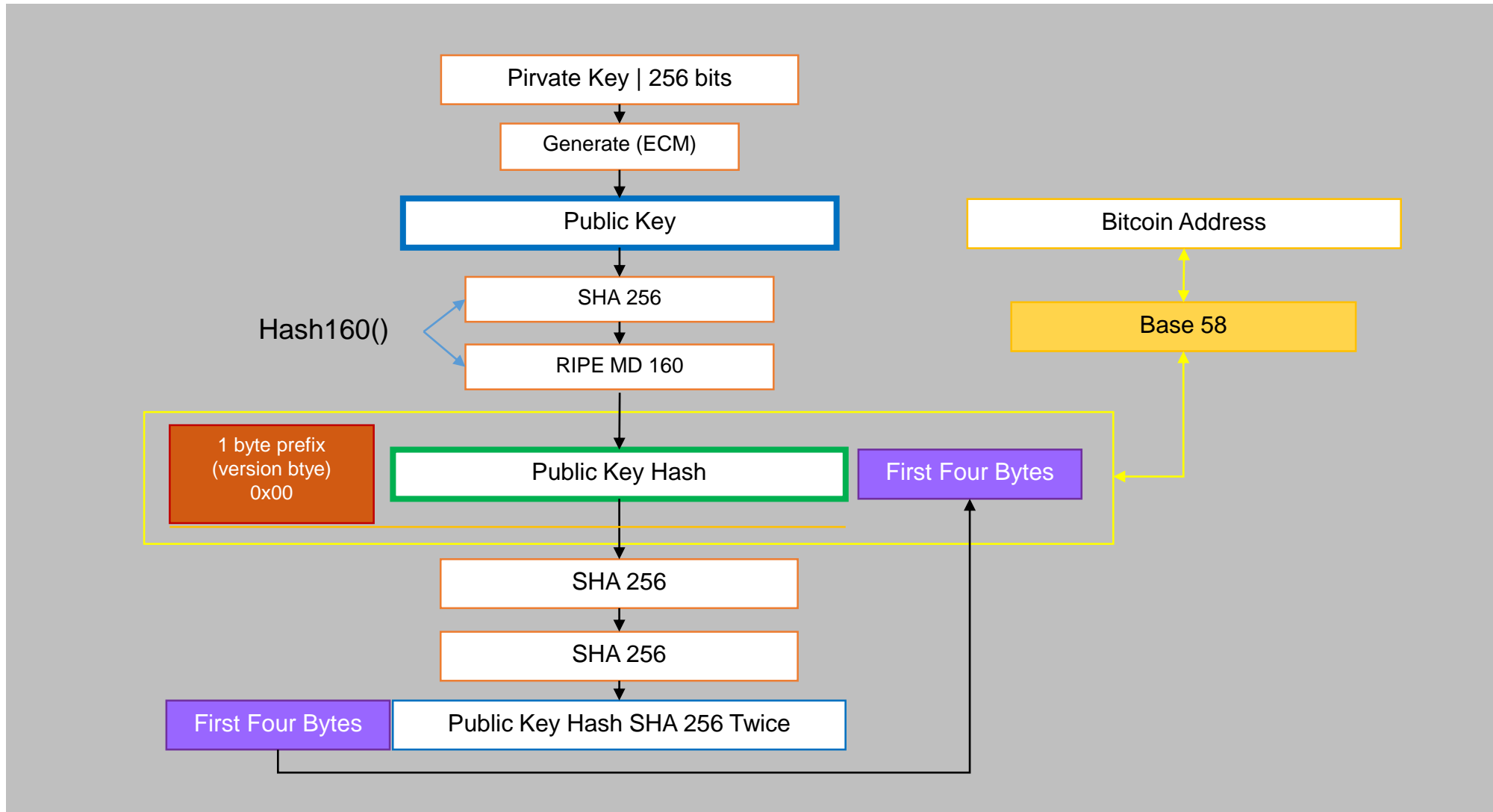
블록 체인



블록 체인



주소 생성



주소 생성 – ui.cpp

```
{
// Ask name
CGetTextFromUserDialog dialog(this, "New Bitcoin Address", "Label", "");
if (!dialog.ShowDialog())
return;
string strName = dialog.GetValue();

// Generate new key
string strAddress = PubKeyToAddress(GenerateNewKey());
SetAddressBookName(strAddress, strName);

// Add to list and select it
int nIndex = InsertLine(m_listCtrl, strName, strAddress);
SetSelection(m_listCtrl, nIndex);
m_listCtrl->SetFocus();
}
```


주소 생성 – main.cpp

```
vector<unsigned char> GenerateNewKey()
{
    CKey key;
    key.MakeNewKey();
    if (!AddKey(key))
        throw runtime_error("GenerateNewKey() : AddKey failed\n");
    return key.GetPubKey();
}

bool AddKey(const CKey& key)
{
    CRITICAL_BLOCK(cs_mapKeys)
    {
        mapKeys[key.GetPubKey()] = key.GetPrivKey();
        mapPubKeys[Hash160(key.GetPubKey())] = key.GetPubKey();
    }
    return CWalletDB().WriteKey(key.GetPubKey(), key.GetPrivKey());
}
```

Base 58

Cat

		ASCII	
2	C	67	$67 * 2^{(2 * 8)}$
1	a	97	$97 * 2^{(1 * 8)}$
0	t	116	$116 * 2^{(0 * 8)}$

Base 58

Cat

C	$67 * 2^{(2 * 8)}$	4390912
a	$97 * 2^{(1 * 8)}$	24832
t	$116 * 2^{(0 * 8)}$	116
		4415860

Base 58

Cat

계산	몫	나머지
$4415860 / 58$	76135	30
$76135 / 58$	1312	39
$1312 / 58$	22	36
$22 / 58$	0	22

Base 58

Cat

	나머지	Base 58
3	30	X
2	39	g
1	36	d
0	22	P

Result: PdgX



Base 58

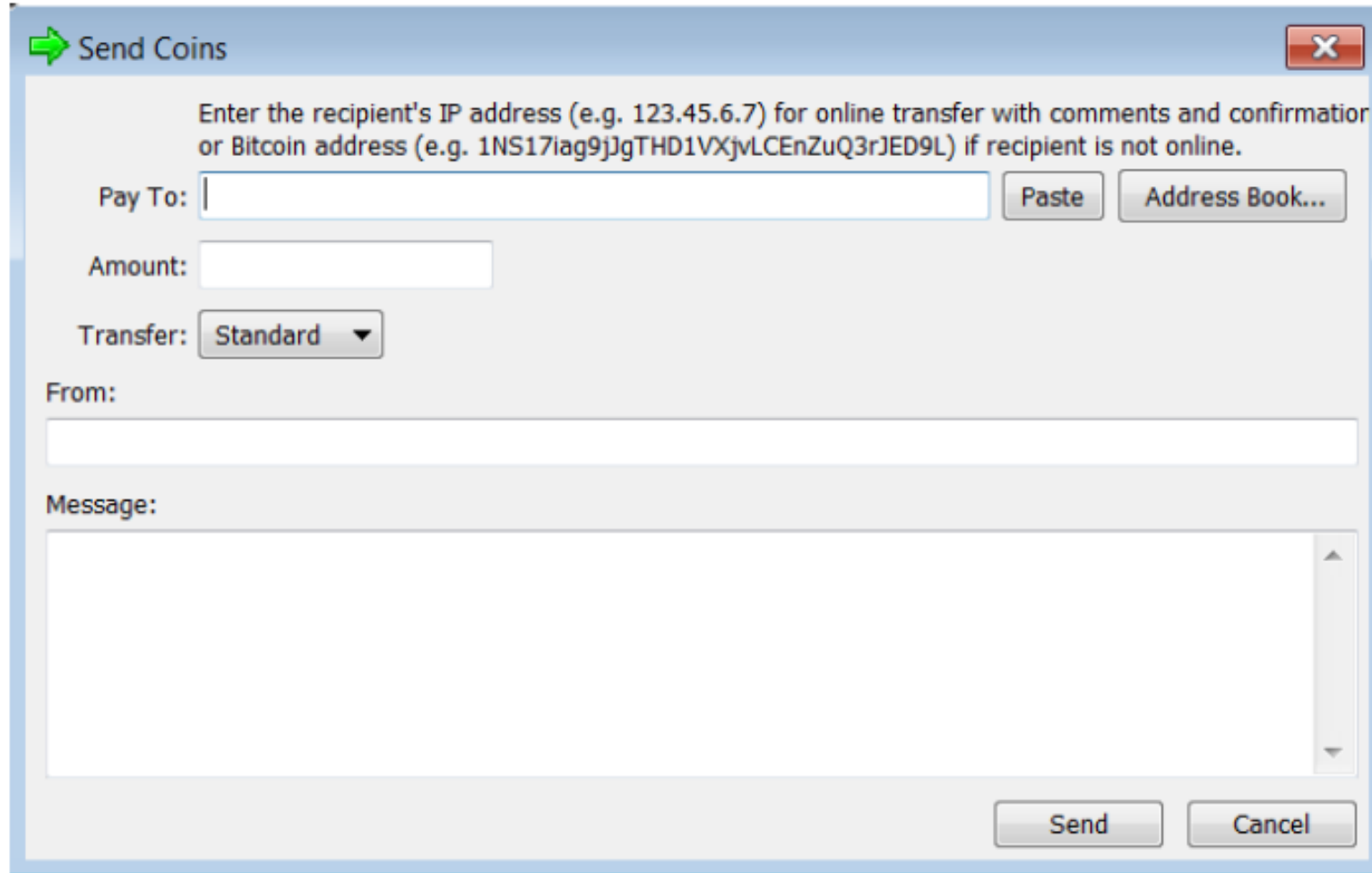
Base 64

- 0~9, A~Z, a~z, =, +, / ..etc
- 가독성 떨어짐
- 전체 선택 시 특수 문자에서 걸림

Base 58

- 0~9, A~Z, a~z
- o, 0, l, I, 특수 문자 제외

비트 코인 트랜잭션



Send Coins

Enter the recipient's IP address (e.g. 123.45.6.7) for online transfer with comments and confirmation or Bitcoin address (e.g. 1NS17iag9jJgTHD1VXjvLCEnZuQ3rJED9L) if recipient is not online.

Pay To:

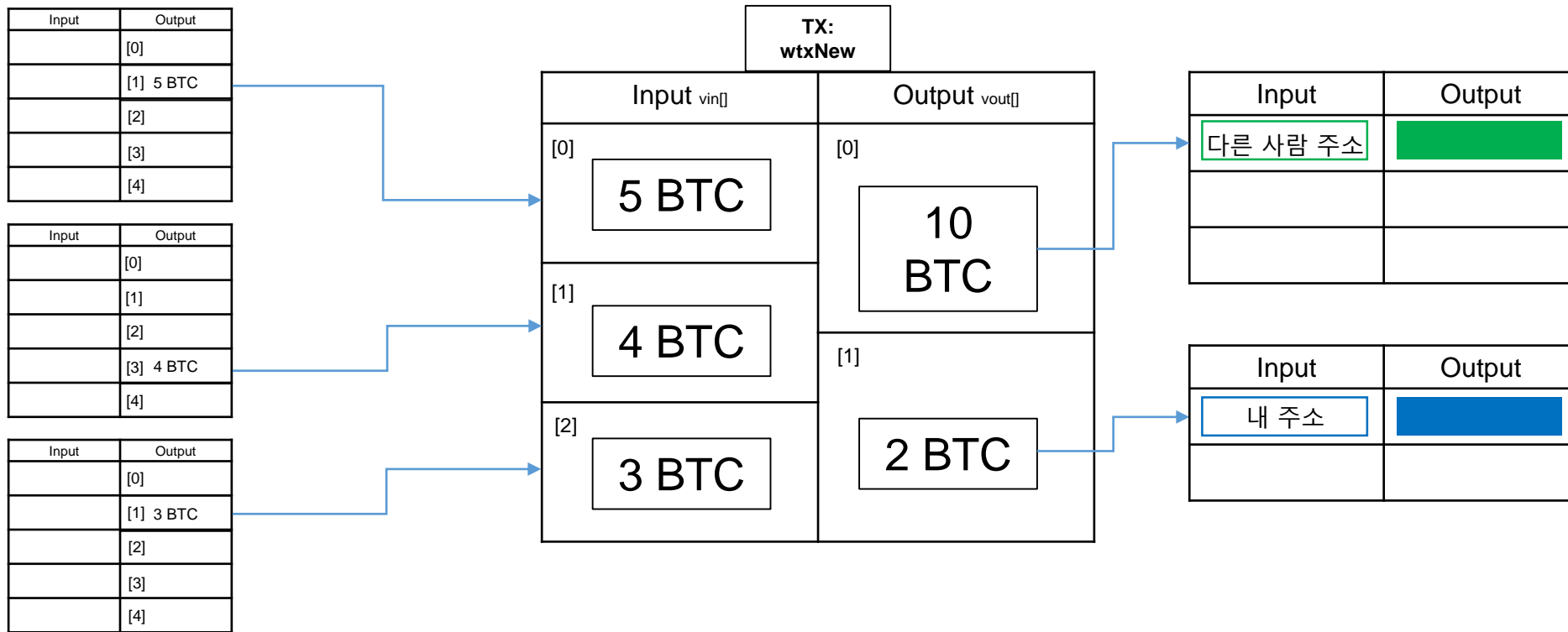
Amount:

Transfer:

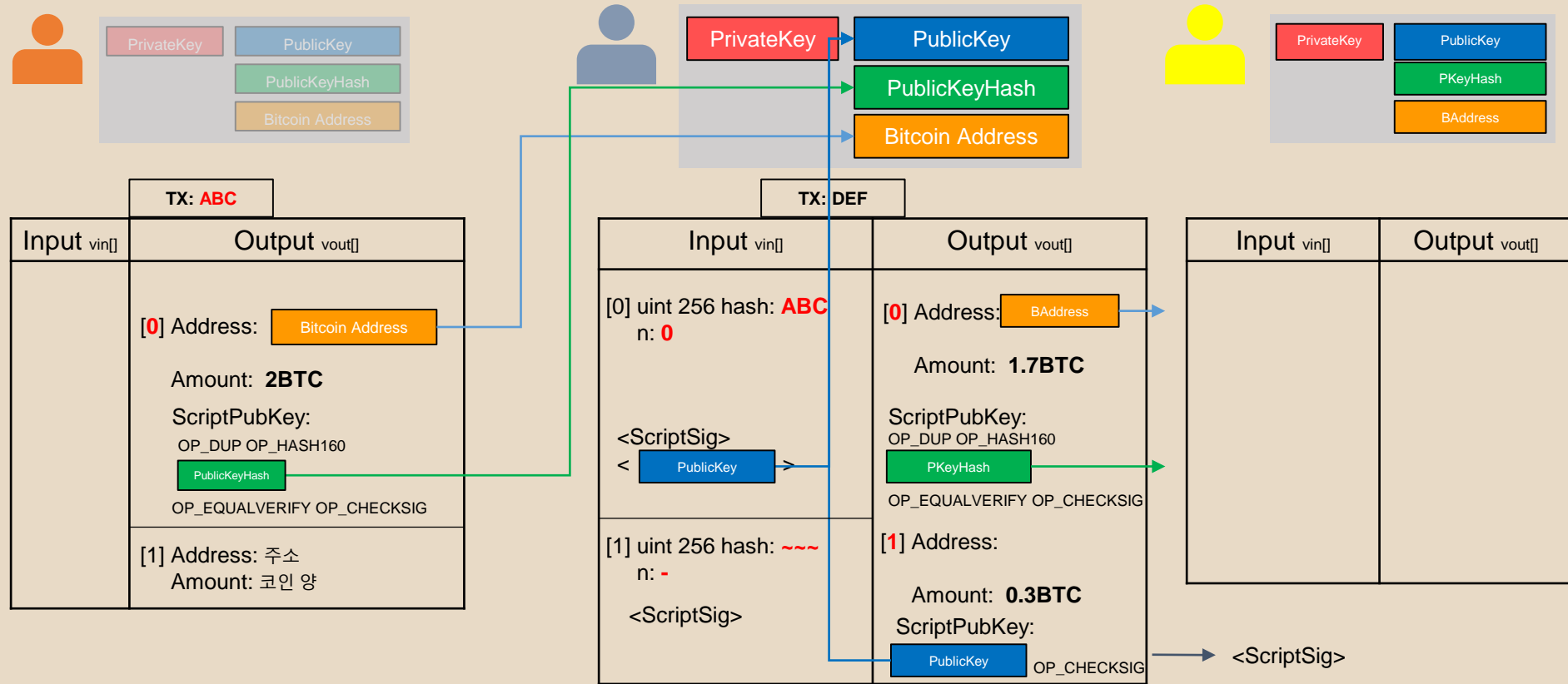
From:

Message:

비트 코인 트랜잭션



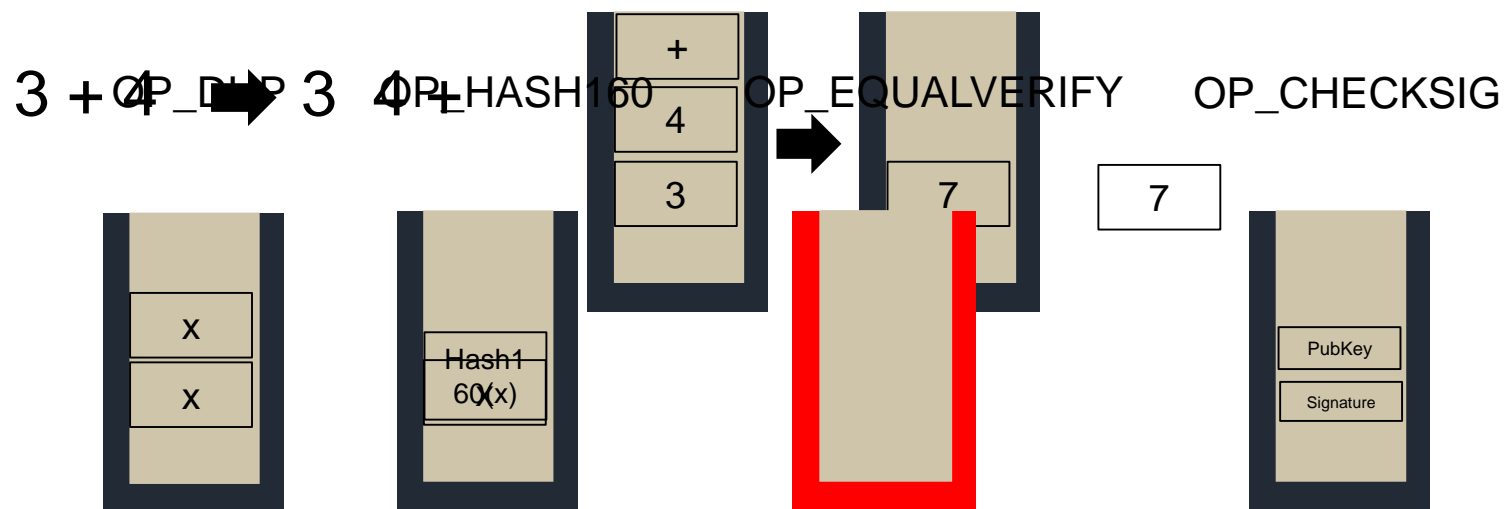
비트 코인 트랜잭션



비트 코인 트랜잭션

- Script 언어

- 비트 코인에서 node를 돌리는 언어
- 소규모 가벼운 프로그램 언어
- None 튜링 언어
- Stack Based 언어



비트 코인 트랜잭션

- Script 언어

Quiz's Answer

A **<Signature>** **<PublicKey>**

B **<Signature>**

Output Quiz

OP_DUP OP_HASH160 **<PublicKey160>** OP_EQUALVERIFY OP_CHECKSIG

<PublicKey> OP_CHECKSIG

<Signature> **<PublicKey>** OP_CHECKSIG

블록체인 익명성

- 암호 화폐를 이용한 많은 악용 사례
 - 가상화폐를 활용한 범죄 피해액에 2조 7000억 원에 달함
 - 랜덤웨어의 비용을 가상화폐를 통해 요구
 - 암시장에서 활용

블록체인 익명성

- 주소 형태

0x10A259146C4AC177A74D17591bf83739587a219D

0xA60b375aA200949a56c26E99fCFF0a0DAE6E9a51

0xF40893049EBfa855d6ad5b64613811805881bFE2

<https://ropsten.etherscan.io/address/0x10a259146c4ac177a74d17591bf83739587a219d>

블록체인 익명성

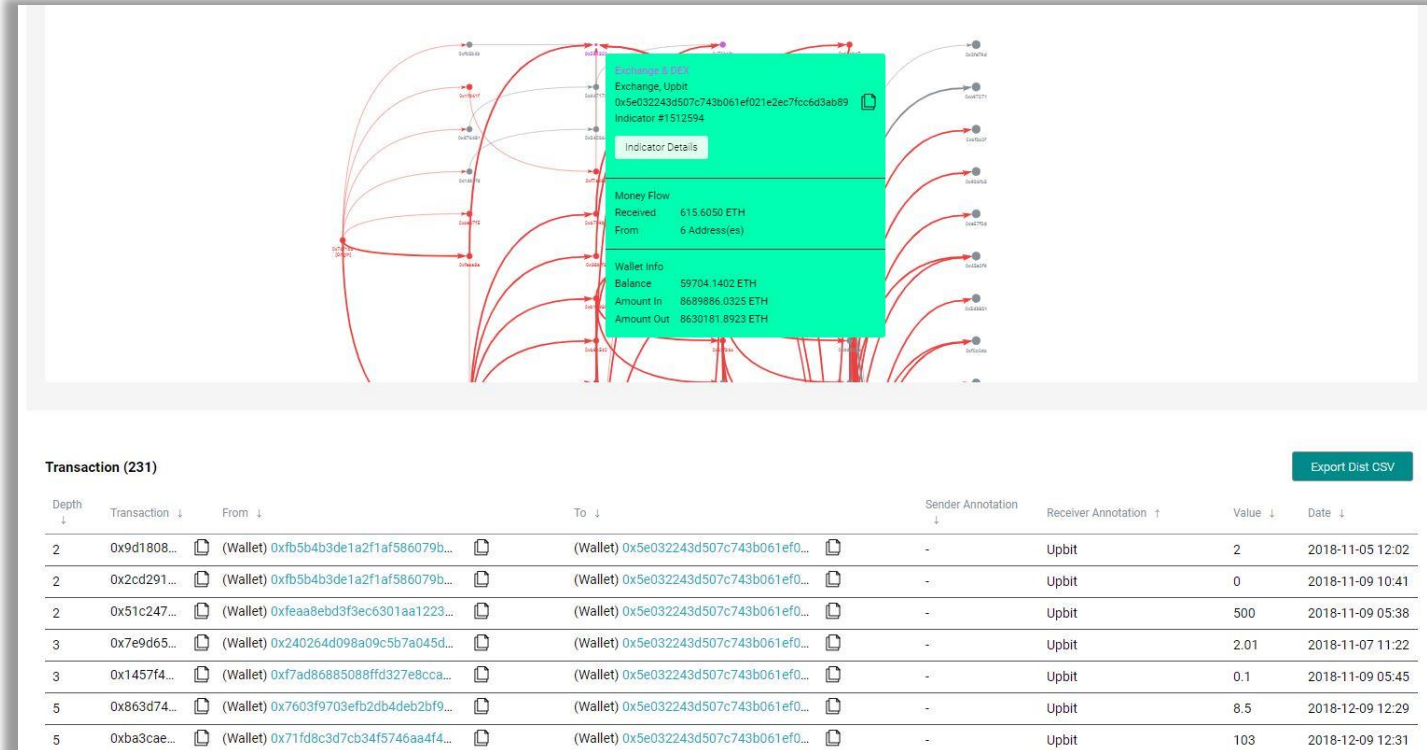
- 주소 형태
 - 사람에게 의미가 없는 듯한 형태
 - 해당 주소만으로 신분을 알아낼 수 없음
 - 한 명이 여러 개의 주소 사용 가능성 있음
- 익명성 분석
 - 공개된 장부이기에 추적은 가능
 - 머신 러닝으로도 분석 가능

블록체인 익명성

- 추적을 통한 분석
 - 센티넬 프로토콜
 - 암호화폐 추적 솔루션 사용: CATV(Crypto Analysis Transaction Visualization)
 - 추적을 막기 위한 믹싱 앤 텀블러(Mixing and Tumbler) 또한 분석 가능
 - 보안 위협 정보 수집
 - 위험한 주소면 트랜잭션 차단
 - 약 131만6762건의 위험 정보

블록체인 익명성

- 추적을 통한 분석
 - 관련되어 있는 모든 트랜잭션을 시각적으로 보여줌



블록체인 익명성

- 머신 러닝을 통한 분석
 - 체인 분석(Chainalysis) 회사에서 2억 개가 넘는 트랜잭션 데이터를 분류함
 - 지도 학습(Supervised Machine Learning)을 통해 학습
 - 분류: 거래소, 개인 지갑, 도박, 랜섬웨어 등 10개 항목
- 결과
 - 약 77%의 정확도로 식별되지 않은 트랜잭션 분류가 가능
 - 여러 개의 주소를 사용해 트랜잭션을 발생시키는 경우에도 분류 가능

블록체인 익명성

- 현실 세계의 신원과 블록체인 상의 주소의 연결점을 찾을 수 있는 곳
 - 거래소
 - 암호화폐를 실제 현금으로 환전하기 위한 장소
 - 개인적인 권한으로는 정보에 대한 협조를 하지 않음
 - 정부 차원의 개입이 필요
 - 블록체인 정책적 문제

감사합니다

