Bitcoin Transactions

Sameh El-Ansary, PhD

Transactions

- In Bitcoin **no balance is recorded** only transactions!!
- All design aspects are created to make sure transactions are:
  - Created
  - Propagated
  - Validated
  - Agreed Upon (added to the blockchain)

Types of Transactions

- Coinbase
  - Transactions that create new Bitcoins
- Standard
  - Transferring that transfer Bitcoin from one/many "senders" to/many "receivers"
  - We will start with this one ☺

SAMPLE TRANSACTION

Sample Transaction

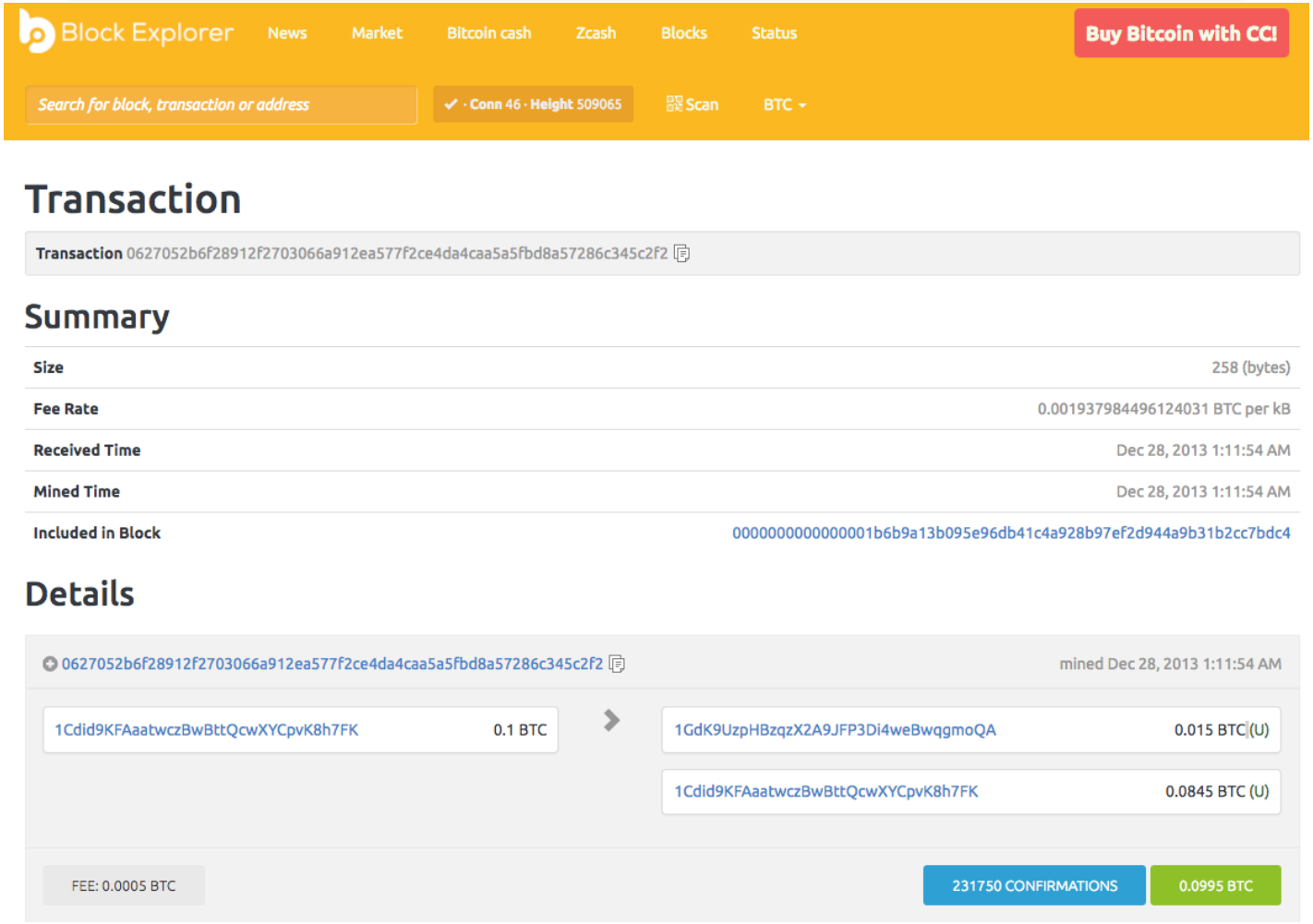
- Alice has **0.1 BTC** (she got that from Joe)
- She wants to buy a cup of coffee from Bob for **0.015 BTC**

Sample Transaction

- Alice will take the **0.1 BTC** she has and will send:
  - 0.0150 to Bob
  - 0.0845 to herself (the change)
  - 0.0005 as a transaction fee
- Total Transaction Input: 0.1 BTC
- Total Transaction Output: 0.1 BTC
- Let us look at this transaction in more detail:

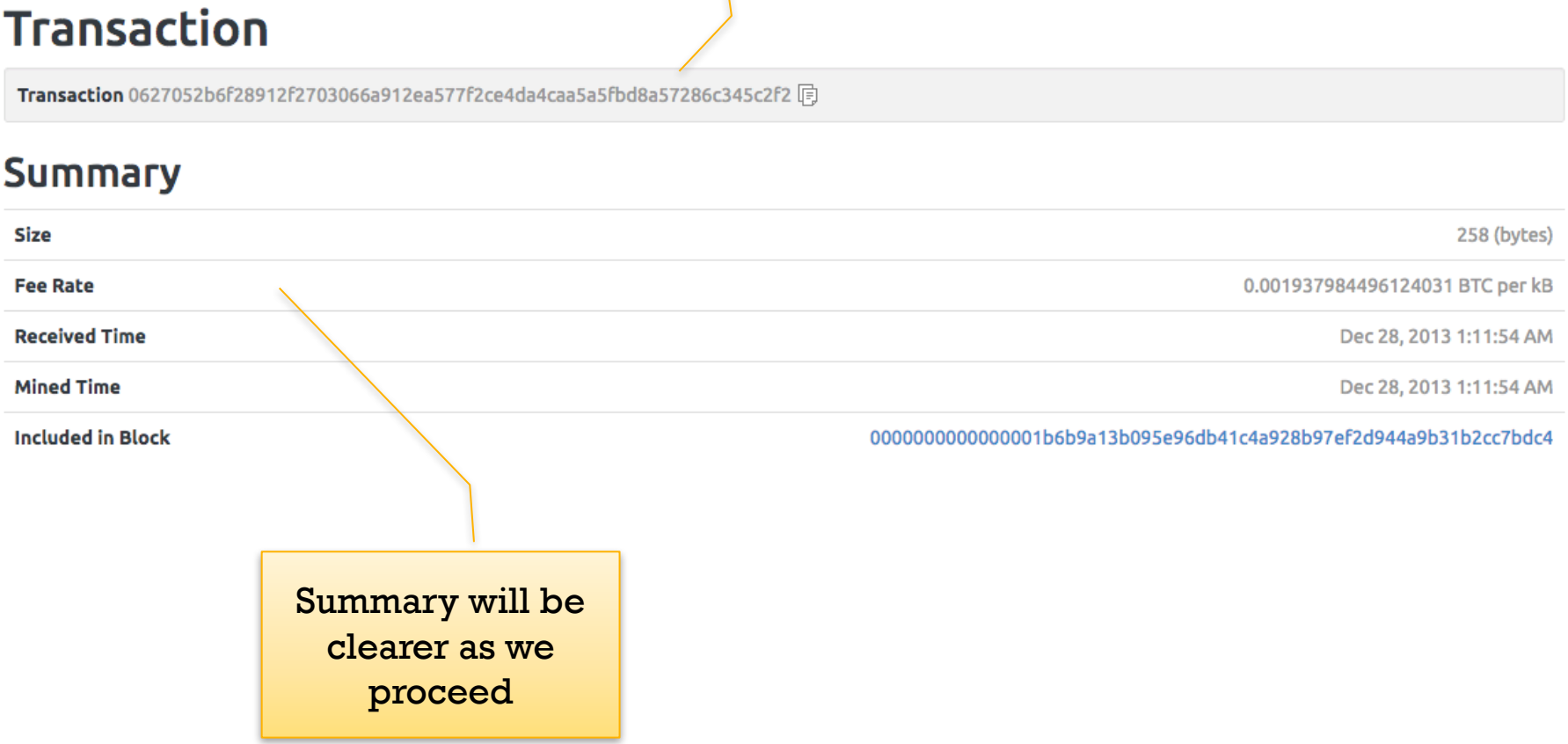
Alice's Transaction On Blockexplorer.com

https://blockexplorer.com/tx/06270…



Alice's Transaction On Blockexplorer.com

Transaction Hash
(unique identifier)

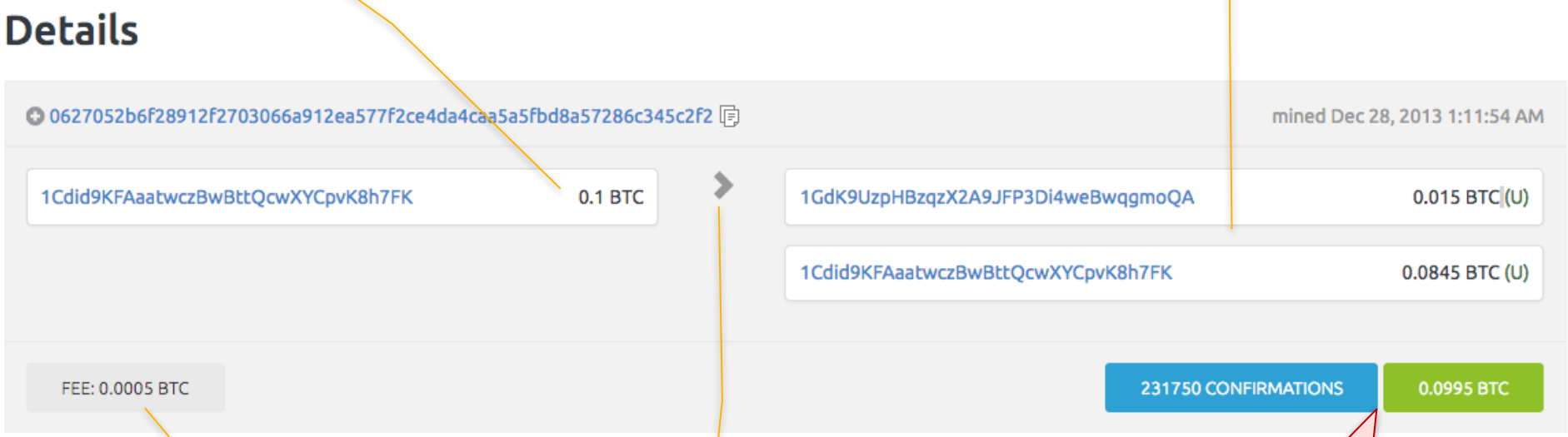


Summary will be clearer as we proceed

Alice's Transaction On Blockexplorer.com

Transaction Input
Referring to a Past Transaction that had 0,1 BTC as output

Transaction Outputs
Referring to a Past Transaction that had 0,1 BTC as output



Transaction Fees

Input(s) == output(s)+fees

Not the real transaction!!! A prettified one!!!

Transactions - Behind the Scenes


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f03
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECK
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECK
    }
  ]
}
```


This is the actual Transaction !!

No sender, No Receiver, No Fees!!!

Only Inputs and outputs, lets' take them one by one.

Transactions—Behind the Scenes


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f03
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECK
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECK
    }
  ]
}
```


1 Transaction Input (**VIN**)

2 Transaction Outputs (**VOUT**)

Transactions—Behind the Scenes


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f03
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECK
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECK
    }
  ]
}
```


1 Transaction Input
vin

2 Transaction Outputs
vout

Transaction Input

"txid" refers to the transaction where Alice got her 0.1 BTC.
i.e. TX 7957.. : Joe → Alice 0.1 BTC

We call that a **UTXO (Unspent Transaction Output)**

We have to download this transaction to see if something was actually sent to Alice

```
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb64
    "sequence": 4294967295
  }
]
```

Transaction Input

The referenced UTXO might have many outputs. **"vout"** specifies the index of the output in the referenced transaction

```
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb64
    "sequence": 4294967295
  }
]
```

Transaction Input

"scriptSig": is a signature that proves that we can spend this UTXO we are referring to.

We say that we are:
"*unlocking the UTXO to spend it*"

```
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb64
    "sequence": 4294967295
  }
]
```

Transaction Input


```
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb64
    "sequence": 4294967295
  }
]
```


"sequence": we will cover it later

Transaction Outputs

- Consists of two parts:
  1. **Amount of bitcoin**
     - The unit is the Satoshi
     - 100 000 000 Satoshi = 1 BTC
  2. **A cryptographic puzzle**
     - Determines the requirements to spend the coin
     - AKA locking script, witness script, scriptPubKey

Transaction Output

The price of the cup of coffee sent to Bob

```
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY
    OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG
  }
]
```

Change sent back to Alice

Transaction Output

- **"scriptPubKey"**: is an "unlocking" script written in a special language
- It describes how to verify that a spender of this output has the right to spend it. , i.e. tells you how to verify the signature supplied by the spender in his "unlocking" script


```
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY
    OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG
  }
]
```


Different receiver, .. So different scriptPubKey

i.e. Transactions do not have receivers!!

They specify a puzzle that only the intended receiver can solve.

Transaction Output


```
"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY
    OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG
  }
]
```


This vout is transferred to **Bob**. Therefore, when he wants to spend it, he will have to refer to this **UTXO, index 0**. His **ScriptSig** will be used as input to this **scriptPupKey**, if successful, he can spend it.

This vout is transferred to **Alice**. Therefore, when she wants to spend it, she will have to refer to this **UTXO, index 1**. Her **ScriptSig** will be used as input to this **scriptPupKey**, if successful, she can spend it.

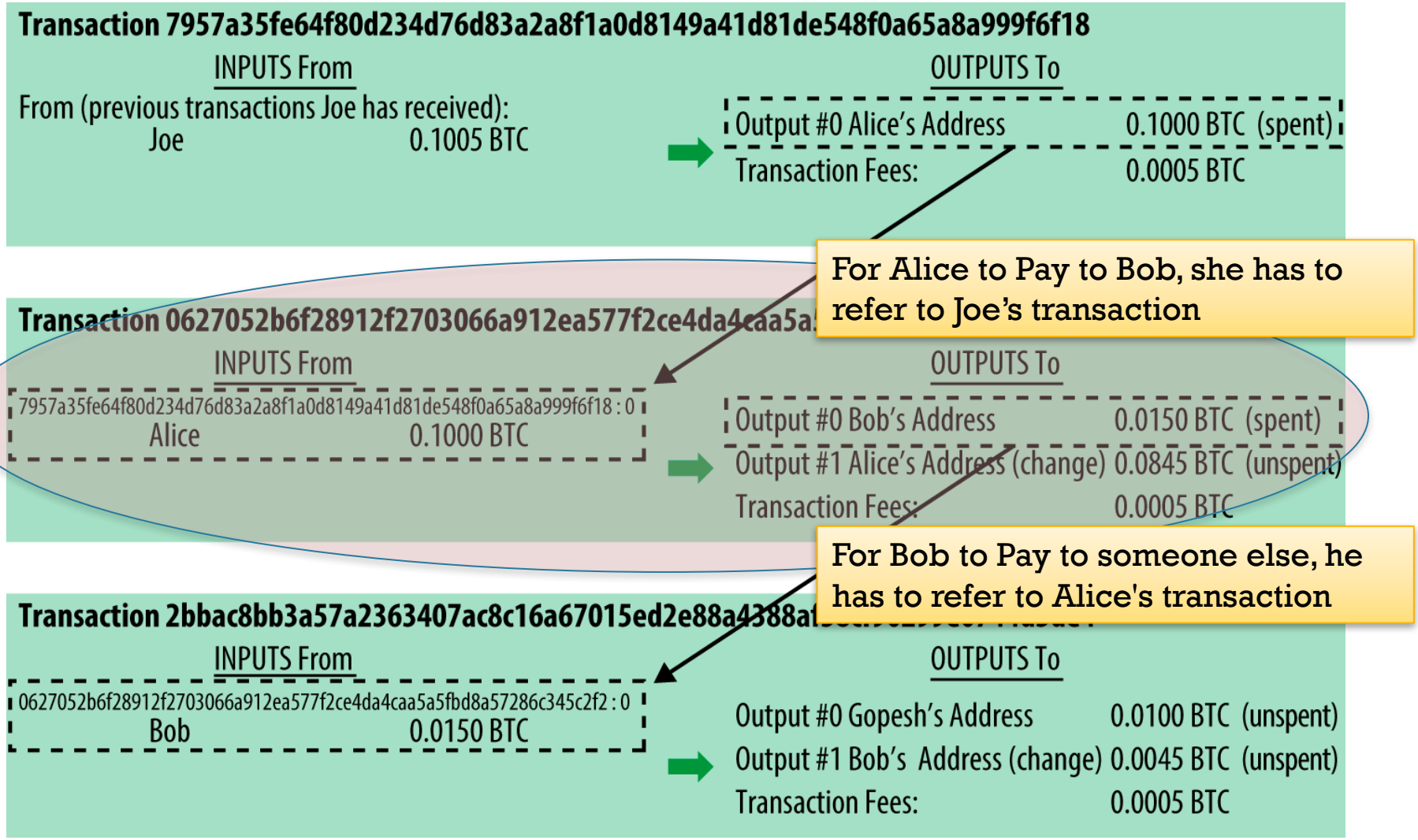
No Senders, No Receivers


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f03
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECK
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECK
    }
  ]
}
```


Alice's address is not here as a sender but she provided a solution to a puzzle (lock script) of Joe's UTXO.

We did not specify a receiver but be created a puzzle that only the intended receiver can answer

Sample Transaction Review



Transaction Fees

- ~~No Senders~~ (Well, the solution of a puzzle)
- ~~No Receivers~~ (well the hash of the address)

Hey where are the fees recorded ???

Transaction Fees

- Who collects them?
  - Miners.. Who?
  - Nodes running full Bitcoin nodes
  - They have an incentive to stay in the network to "mine" blocks (sets of transactions) and collect the fees
- Where is the fee amount recorded?
  - It is not recorded anywhere
  - It is the **left-overs** from the vin after sending out all the vouts

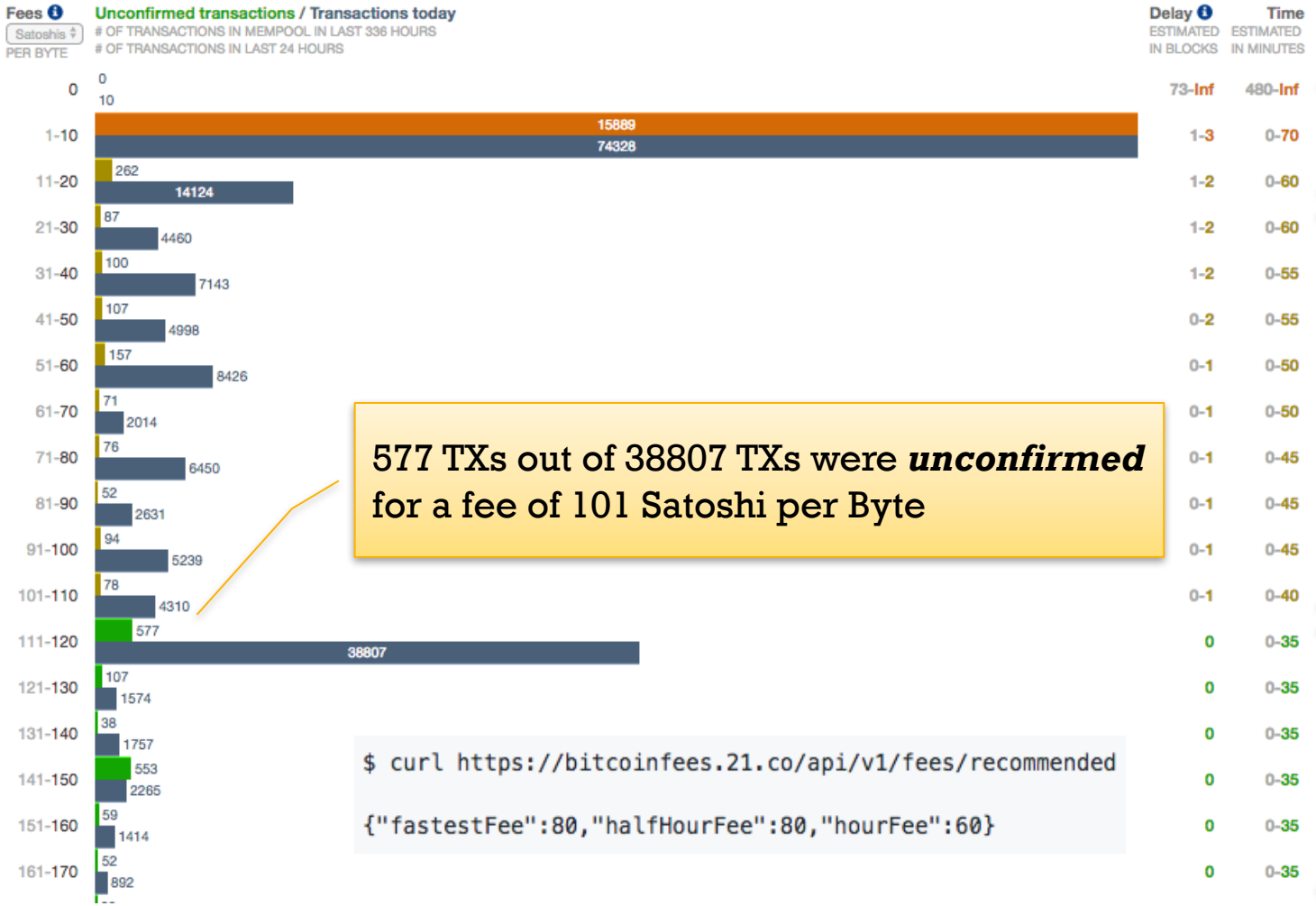
Transaction Fees

- Who decides the fee?
  - Supply and demand
  - The issuer of the TX proposes a fee
  - The miners (more in ch10) *might* be interested to mine it (record it in the blockchain)
  - The TX size in bytes is also a factor, for the same fee a larger TX might be dumped
- What happens to dumped transactions?
  - They can take longer to process
  - They might stall forever if the fee is too low.

Transaction Fees

- How do we know what is a reasonable fee?
  - Usually your wallet application contacts a 3rd party fee estimation service like: https://bitcoinfees.21.co
  - The services tells you what **fee** can you propose to get your TX of a certain **size** mined in **T** minutes.

Transaction Fee Estimation



577 TXs out of 38807 TXs were ***unconfirmed*** for a fee of 101 Satoshi per Byte

```
$ curl https://bitcoinfees.21.co/api/v1/fees/recommended

{"fastestFee":80,"halfHourFee":80,"hourFee":60}
```

>60min
Very Bad

> 30 min
Slow

< 30 min
OK

~10 min at best

Discussion

- What is the effect on micropayments?
- What is the effect on fundraisers?
- What is the effect on newbies?

TRANSACTION SERIALIZATION

TX Output Serialization

Size	Field	Description
8 bytes (little-endian)	Amount	Bitcoin value in satoshis (10^{-8} bitcoin)
1–9 bytes (VarInt)	Locking-Script Size	Locking-Script length in bytes, to follow
Variable	Locking-Script	A script defining the conditions needed to spend the output

TX Input Serialization

Size	Field	Description
32 bytes	Transaction Hash	Pointer to the transaction containing the UTXO to be spent
4 bytes	Output Index	The index number of the UTXO to be spent; first one is 0
1–9 bytes (VarInt)	Unlocking-Script Size	Unlocking-Script length in bytes, to follow
Variable	Unlocking-Script	A script that fulfills the conditions of the UTXO locking script
4 bytes	Sequence Number	Used for locktime or disabled (0xFFFFFFFF)

Alice's TX Serialized

Example 1. Alice's transaction, serialized and presented in hexadecimal notation

0100000001186f9f998a5aa6f048e51dd8419a14d8a0f1a8a2836dd734d2804fe65fa35779 00000000 8b 48 3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e381301410484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adffffffff0260e31600000000001976a914ab68025513c3dbd2f7b92a94e0581f5d50f654e788acd0ef8000000000001976a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac00000000

- Vin:
  - TX ID: 7957….81 TX hash in reverse order
  - 00000000 ouput index
  - Length of scriptSig is 139 bytes → 8b in hex
  - FFFFFFFF sequence number
- Vout:
  - 0.015 BTC = 1,500,000 Satoshis → 0x 16e360
    The scriptPubKey length is 25 bytes → 0x 19

Knowledge Checklist

- ✓ Transactions (Standard & Coinbase)
- ✓ No balances only TX
- ✓ UTXO
- ✓ VIN
- ✓ VOUT
- ✓ SCRIPTSIG (unlocking script)
- ✓ SCRIPTPUBKEY (locking script)
- ✓ P2PKH
- ✓ P2SH
- ✓ FEES & ESTIMATION
- ✓ **SCRIPT LANGUAGE**
- ✓ TX SERIALIZATION