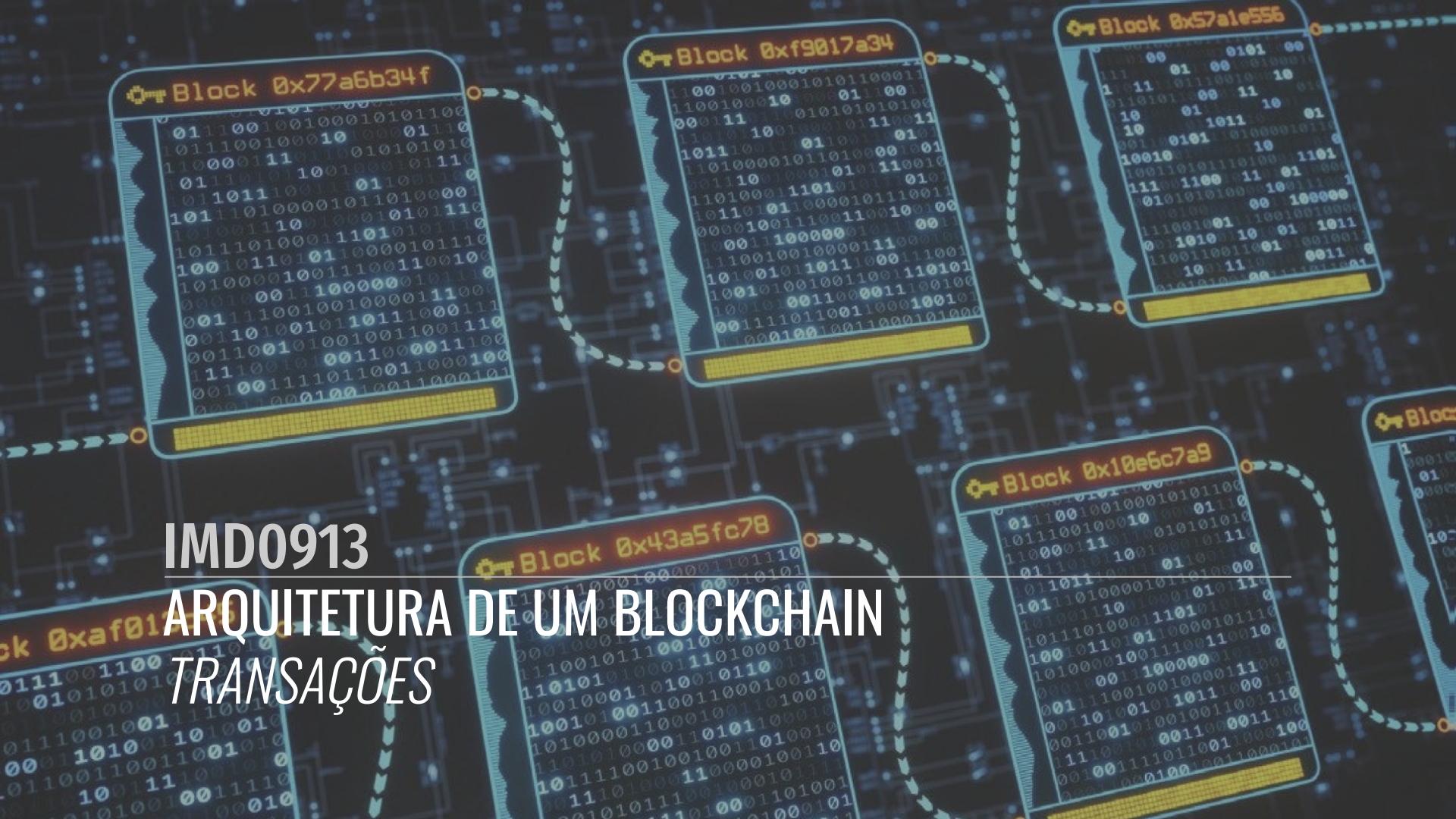
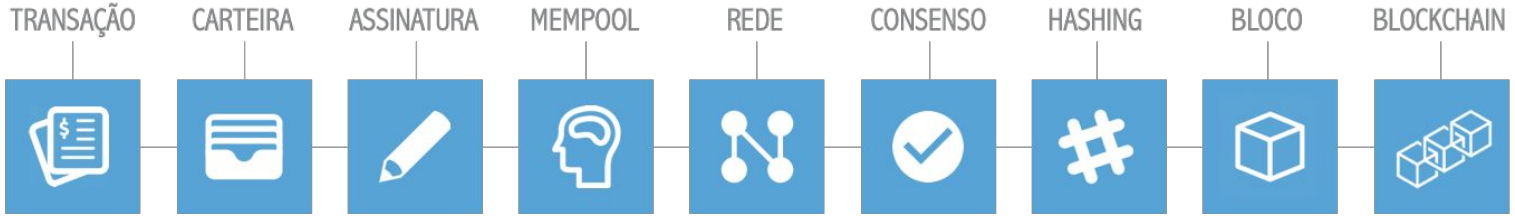


IMD0913

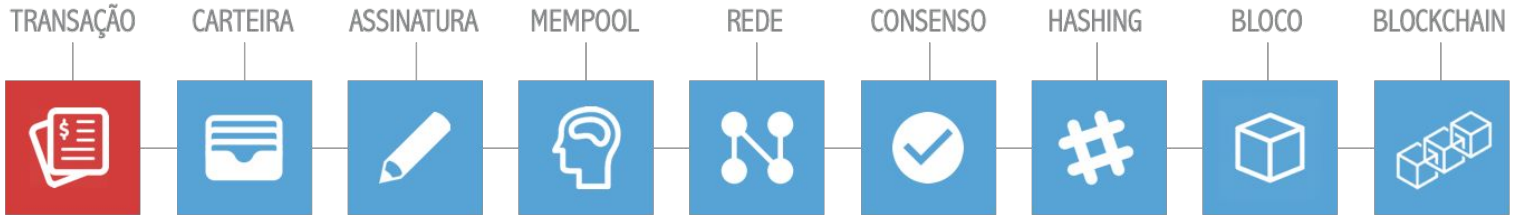
ARQUITETURA DE UM BLOCKCHAIN

TRANSAÇÕES

ARQUITETURA DE UM **BLOCKCHAIN**



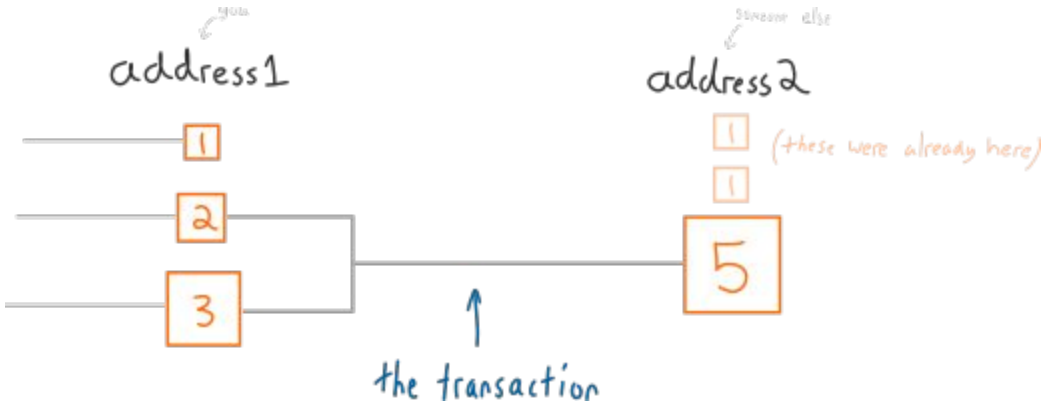
ARQUITETURA DE UM **BLOCKCHAIN**



Transação

Estrutura de dados que codifica uma transferência de valor de uma fonte de fundos chamada de entrada (*input*) para um destino chamado saída (*output*).

Transação


address1
address2
1
2
3
5
1
1
(these were already here)
the transaction

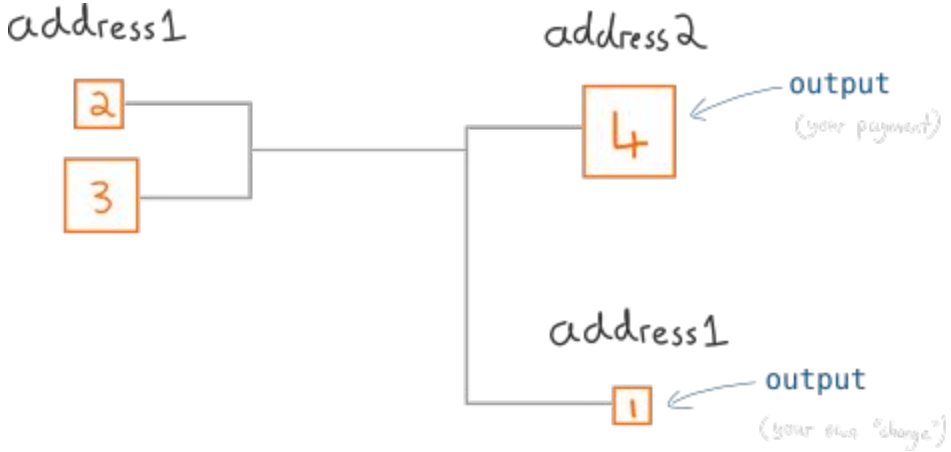
Transação

Transação

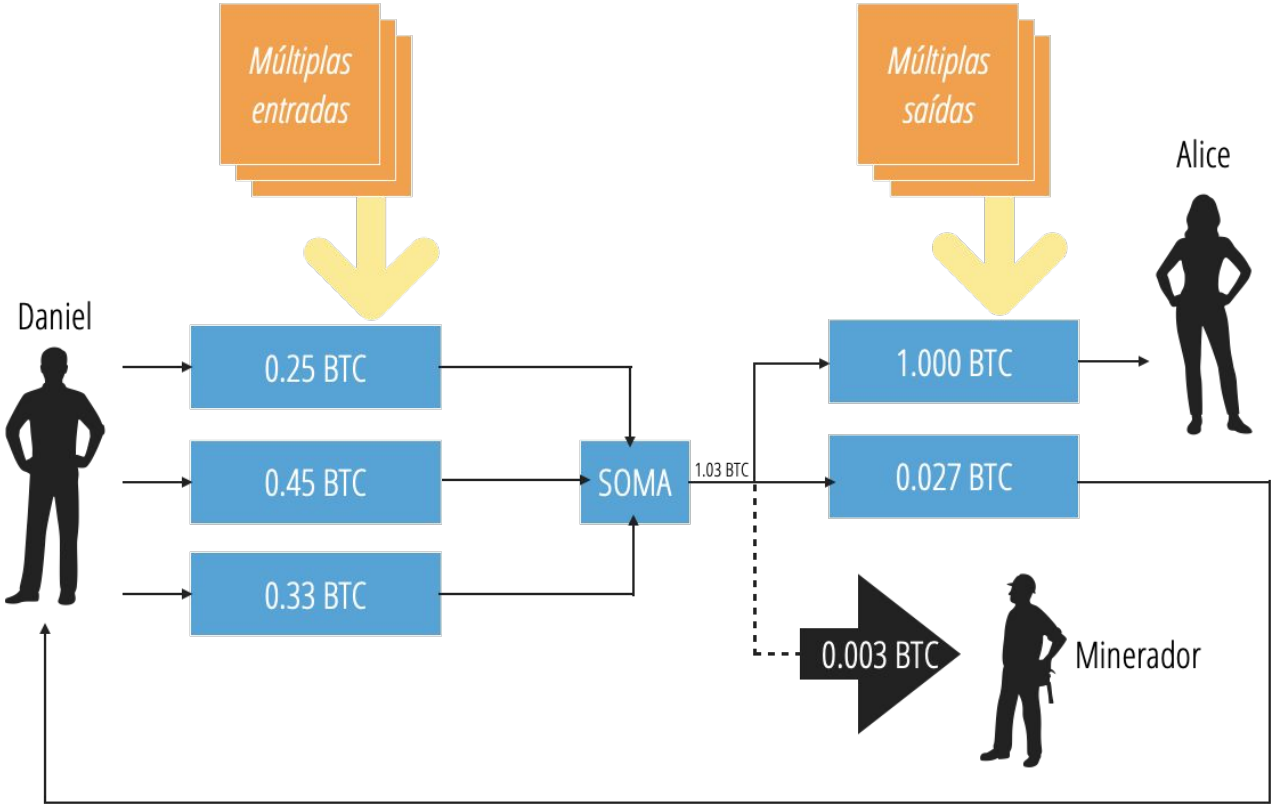
Daniel quer enviar para Alice 1 BTC + 0.003 BTC de taxa de transação (*fee*), totalizando 1.003 BTC

Como receber o troco de 0.27 BTC de volta?

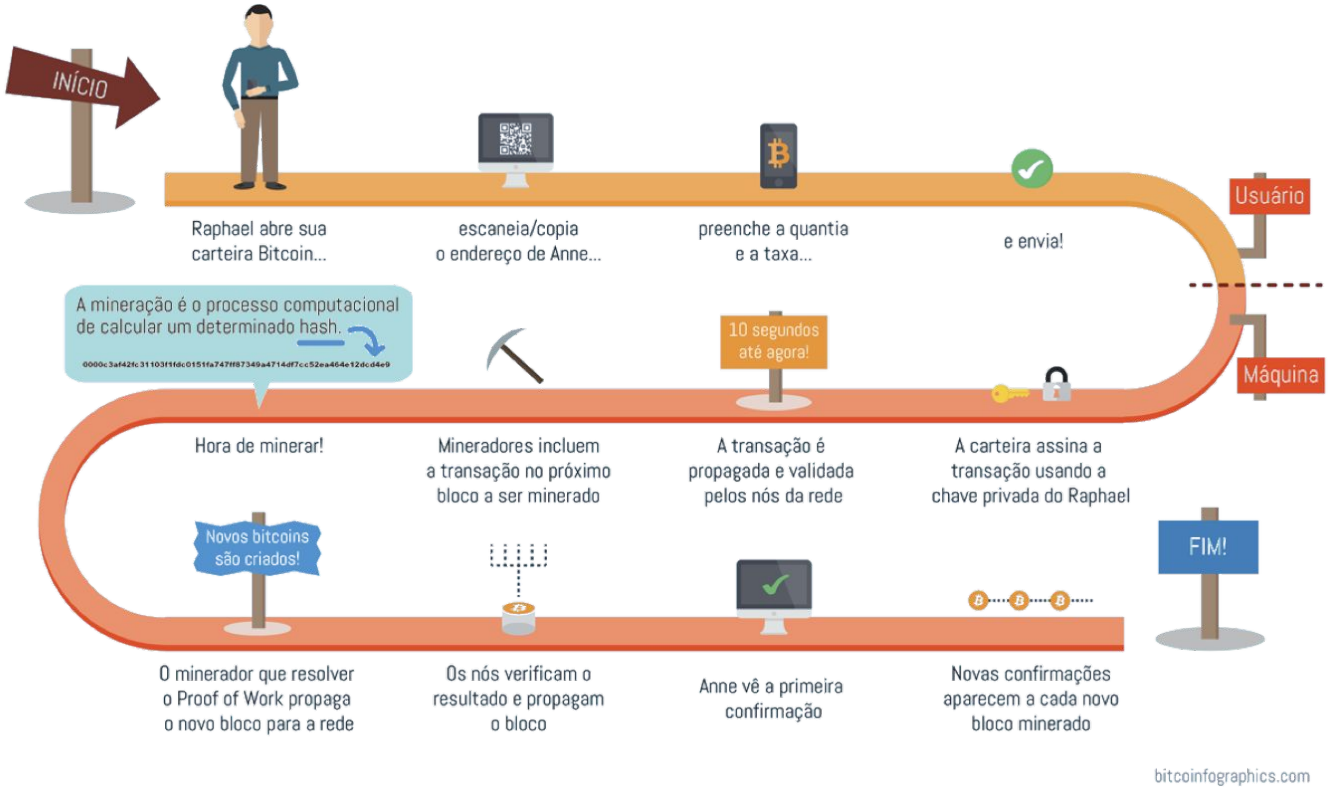
Transação


address 1
2
3
address 2
4
output
(your payment)
address 1
1
output
(your own "change")

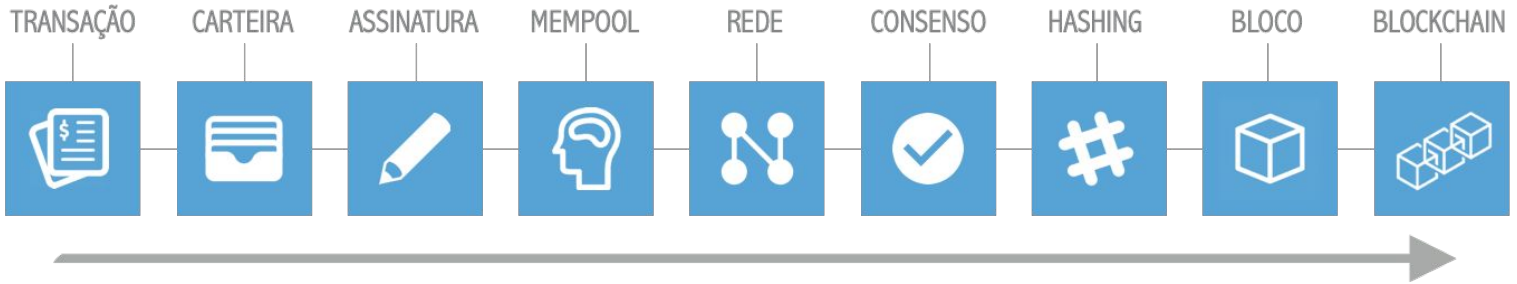
Transação


Múltiplas entradas
Múltiplas saídas
Alice
Daniel
0.25 BTC
0.45 BTC
0.33 BTC
SOMA
1.03 BTC
1.000 BTC
0.027 BTC
0.003 BTC
Minerador

Ciclo de vida de uma transação Bitcoin



Ciclo de Vida de uma Transação

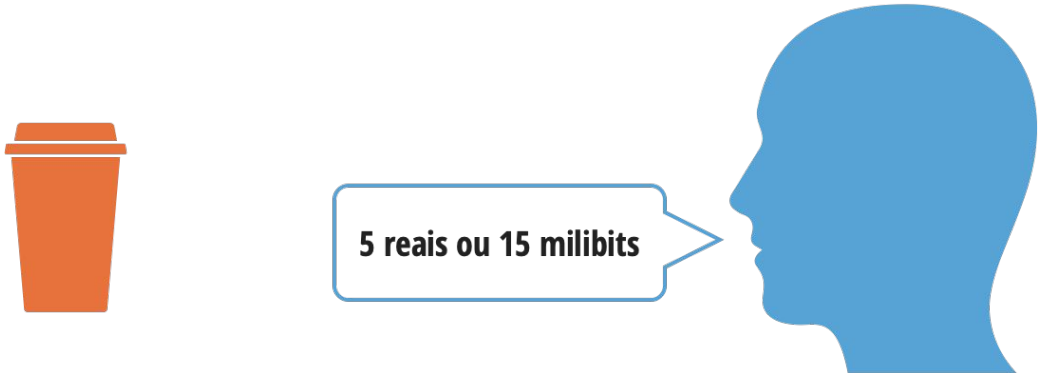


Comprando um café...

Alice acabou de entrar no mundo do Bitcoin. Seu amigo João vendeu BTCs para ela por dinheiro, realizando uma transação de **0.10 BTC** para Alice

Agora Alice irá realizar sua primeira transação de varejo: comprar um café em um estabelecimento que aceita Bitcoins (*Bob's Cafe*)

R$ 5,00 ou 0.015 BTC



Comprando um café...

Podemos consultar um nó para requisitar os UTXOs do endereço de Alice usando uma API:

```
[danilo@imd ~]$ curl https://blockchain.info/unspent?active=1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
```


```
{
	"unspent_outputs":[
		{
			"tx_hash":"186f9f998a5...2836dd734d2804fe65fa35779",
			"tx_index":104810202,
			"tx_output_n": 0,
			"script":"76a9147f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a888ac",
			"value": 10000000,
			"value_hex": "00989680",
			"confirmations":0
		}
	]
}
```

Comprando um café...

O sistema de Bob consegue criar um QR Code contendo uma solicitação de pagamento (*payment request*)

Facilmente o endereço Bitcoin de Bob pode ser escaneado

Comprando um café...

O sistema de Bob consegue criar um QR Code contendo uma solicitação de pagamento (*payment request*)

Facilmente o endereço Bitcoin de Bob pode ser escaneado

Comprando um café...

O sistema de Bob consegue criar um QR Code contendo uma solicitação de pagamento (*payment request*)

Facilmente o endereço Bitcoin de Bob pode ser escaneado

Comprando um café...

Alice escaneia com o QR Code com seu celular, e autoriza o pagamento de 0.015 BTC para o endereço indicado

Em segundos Bob vê a transação em seu sistema *

http://btc.com/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

Transação

Home / Block - 277316 / Transaction 0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

Summary

Height	277316	Input	0.10000000 BTC
Confirmations	395817	Output	0.09950000 BTC
Timestamp	2013-12-27 20:11:54	Sigops	8
Size (rawtx)	258 Bytes	Fees	0.00050000 BTC
Virtual Size	258 Bytes	Fees Rate (BTC / kVB)	0.00193798 BTC
Weight	1,032	Other Explorers	BLOCKCHAIR

Input (1)	0.10000000 BTC	Output (2)	0.09950000 BTC
1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	0.10000000	1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA	0.01500000
		1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK	0.08450000

395,817 Confirmations

Comprando um café...

Note que a transação é recebida por Bob em segundos, mas isso não quer dizer que ela já está incluída em um bloco

Mas Bob pode verificar que a transação de fato tem *outputs* resgatáveis por Bob

Também pode verificar que a transação foi bem formada, usando UTXOs, além de incluir taxas de transação (*fees*) suficientes para ser incluída em um próximo bloco

Nesse ponto, Bob pode assumir, com poucos riscos, que a transação será em breve incluída em um bloco e confirmada

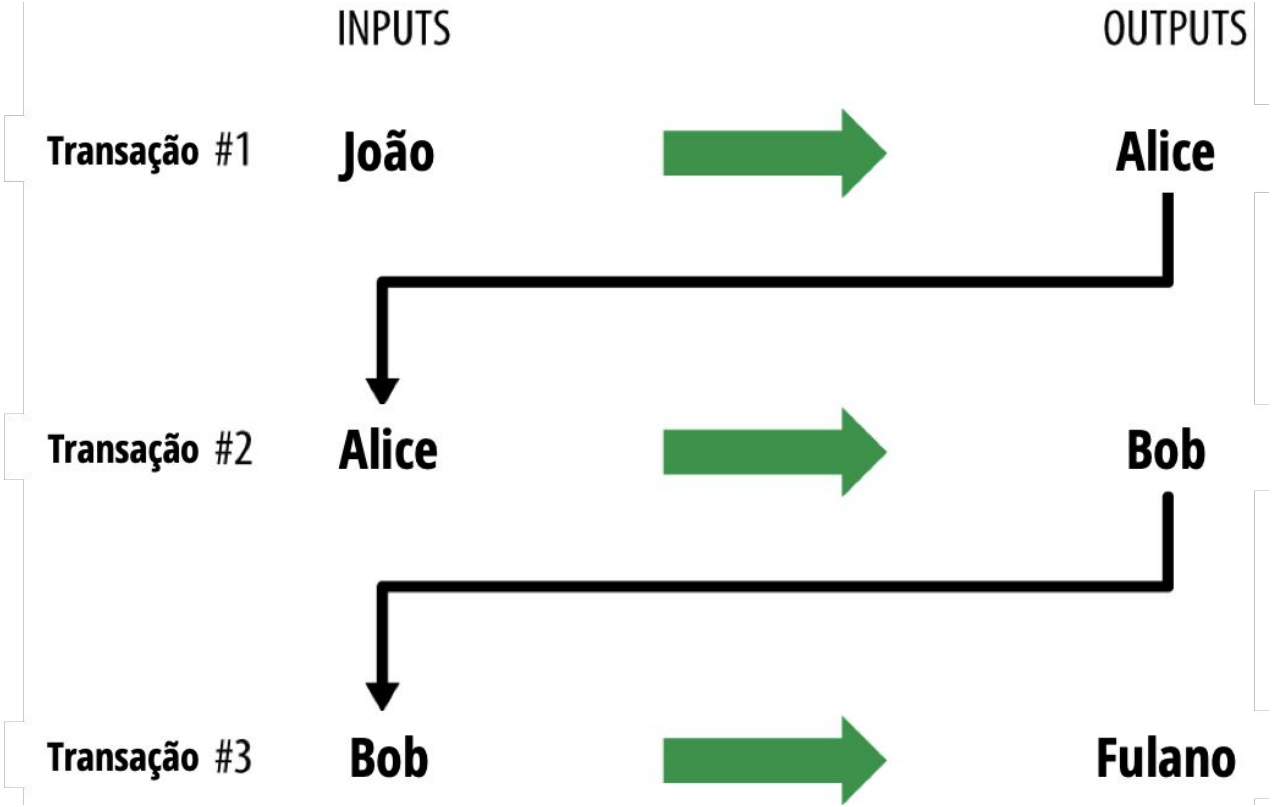
Comprando um café...

Um engano comum sobre transações bitcoin é que elas precisam ser confirmadas esperando 10min por um novo bloco, **ou até 60min para 6 confirmações completas.**

Apesar de confirmações indicar que a transação foi aceita por toda a rede, esse *delay* é desnecessário para itens de pequeno valor como um café.

O comerciante pode aceitar transações de pequeno valor sem confirmações, com riscos similares a alguém comprando algo com cartão de crédito clonado.

Transação


INPUTS
OUTPUTS
Transação #1
João
Alice
Transação #2
Alice
Bob
Transação #3
Bob
Fulano

Transação: *behind the scenes*


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "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",
    }
  ]
}
```

Transação: modelo de dados

```
0100000001186f9f998a5aa6f048e51d
d8419a14d8a0f1a8a2836dd734d2804f
e65fa35779000000008b483045022100
884d142d86652a3f47ba4746ec719bbf
bd040a570b1deccbb6498c75c4ae24cb
02204b9f039ff08df09cbe9f6addac96
0298cad530a863ea8f53982c09db8f6e
381301410484ecc0d46f1918b30928fa
0e4ed99f16a0fb4fde0735e7ade8416a
b9fe423cc5412336376789d172787ec3
457eee41c04f4938de5cc17b4a10fa33
6a8d752adfffffffff0260e316000000
00001976a914ab68025513c3dbd2f7b9
2a94e0581f5d50f654e788acd0ef8000
000000001976a9147f9b1a7fb68d60c5
36c2fd8aeaa53a8f3cc025a888ac0000
0000
```

= 258 *bytes*

https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

Transação: modelo de dados

Versão

Contador de entradas

Entrada(s)

Contador de saídas

Saída(s)

Locktime

```
0100000001f3f6a909f8521adb57d898
d2985834e632374e770fd9e2b98656f1
bf1fdfd427010000006b48304502203a
776322ebf8eb8b58cc6ced4f2574f4c7
3aa664edce0b0022690f2f6f47c52102
2100b82353305988cb0ebd443089a173
ceec93fe4dbfe98d74419ecc84a6a698
e31d012103c5c1bc61f60ce3d6223a63
cedbece03b12ef9f0068f2f3c4a7e7f0
6c523c3664ffffffff0260e316000000
00001976a914977ae6e32349b99b7219
6cb62b5ef37329ed81b488ac063d1000
000000001976a914f76bc4190f3d8e23
15e5c11c59cfc8be9df747e388ac0000
0000
```

Transação: modelo de dados

Versão

Toda Tx indica a versão do Bitcoin, para que saibamos quais regras essa Tx segue

```
01000000
01f3f6a909f8521adb57d898
d2985834e632374e770fd9e2b98656f1
bf1fdfd427010000006b48304502203a
776322ebf8eb8b58cc6ced4f2574f4c7
3aa664edce0b0022690f2f6f47c52102
2100b82353305988cb0ebd443089a173
ceec93fe4dbfe98d74419ecc84a6a698
e31d012103c5c1bc61f60ce3d6223a63
cedbece03b12ef9f0068f2f3c4a7e7f0
6c523c3664ffffffff0260e316000000
00001976a914977ae6e32349b99b7219
6cb62b5ef37329ed81b488ac063d1000
000000001976a914f76bc4190f3d8e23
15e5c11c59cfc8be9df747e388ac0000
0000
```

Transação: modelo de dados

Contador de entradas

Indica quantas entradas foram utilizadas para esta Tx

```
0100000001f3f6a909f8521adb57d898
d2985834e632374e770fd9e2b98656f1
bf1fdfd427010000006b48304502203a
776322ebf8eb8b58cc6ced4f2574f4c7
3aa664edce0b0022690f2f6f47c52102
2100b82353305988cb0ebd443089a173
ceec93fe4dbfe98d74419ecc84a6a698
e31d012103c5c1bc61f60ce3d6223a63
cedbece03b12ef9f0068f2f3c4a7e7f0
6c523c3664ffffffff0260e316000000
00001976a914977ae6e32349b99b7219
6cb62b5ef37329ed81b488ac063d1000
000000001976a914f76bc4190f3d8e23
15e5c11c59cfc8be9df747e388ac0000
0000
```

Transação: modelo de dados

Entrada(s)

Informações relacionadas as entradas da Tx

```
0100000001f3f6a909f8521adb57d898
d2985834e632374e770fd9e2b98656f1
bf1fdfd427010000006b48304502203a
776322ebf8eb8b58cc6ced4f2574f4c7
3aa664edce0b0022690f2f6f47c52102
2100b82353305988cb0ebd443089a173
ceec93fe4dbfe98d74419ecc84a6a698
e31d012103c5c1bc61f60ce3d6223a63
cedbece03b12ef9f0068f2f3c4a7e7f0
6c523c3664ffffffff0260e316000000
00001976a914977ae6e32349b99b7219
6cb62b5ef37329ed81b488ac063d1000
000000001976a914f76bc4190f3d8e23
15e5c11c59cfc8be9df747e388ac0000
0000
```

Transação: modelo de dados

Contador de saídas

Indica quantas saídas foram foram geradas por essa Tx

```
0100000001f3f6a909f8521adb57d898
d2985834e632374e770fd9e2b98656f1
bf1fdfd427010000006b48304502203a
776322ebf8eb8b58cc6ced4f2574f4c7
3aa664edce0b0022690f2f6f47c52102
2100b82353305988cb0ebd443089a173
ceec93fe4dbfe98d74419ecc84a6a698
e31d012103c5c1bc61f60ce3d6223a63
cedbece03b12ef9f0068f2f3c4a7e7f0
6c523c3664ffffffff0260e316000000
00001976a914977ae6e32349b99b7219
6cb62b5ef37329ed81b488ac063d1000
000000001976a914f76bc4190f3d8e23
15e5c11c59cfc8be9df747e388ac0000
0000
```

Transação: modelo de dados

Saída(s)

Informações relacionadas as saídas da Tx

```
0100000001f3f6a909f8521adb57d898
d2985834e632374e770fd9e2b98656f1
bf1fdfd427010000006b48304502203a
776322ebf8eb8b58cc6ced4f2574f4c7
3aa664edce0b0022690f2f6f47c52102
2100b82353305988cb0ebd443089a173
ceec93fe4dbfe98d74419ecc84a6a698
e31d012103c5c1bc61f60ce3d6223a63
cedbece03b12ef9f0068f2f3c4a7e7f0
6c523c3664ffffffff0260e316000000
00001976a914977ae6e32349b99b7219
6cb62b5ef37329ed81b488ac063d1000
000000001976a914f76bc4190f3d8e23
15e5c11c59cfc8be9df747e388ac0000
0000
```

Transação: modelo de dados

Locktime

Menor tempo ou bloco que a Tx pode ser incluída ao blockchain:

- **< 500M altura de bloco**
- **> 500M Unix timestamp**

```
0100000001f3f6a909f8521adb57d898
d2985834e632374e770fd9e2b98656f1
bf1fdfd427010000006b48304502203a
776322ebf8eb8b58cc6ced4f2574f4c7
3aa664edce0b0022690f2f6f47c52102
2100b82353305988cb0ebd443089a173
ceec93fe4dbfe98d74419ecc84a6a698
e31d012103c5c1bc61f60ce3d6223a63
cedbece03b12ef9f0068f2f3c4a7e7f0
6c523c3664ffffffff0260e316000000
00001976a914977ae6e32349b99b7219
6cb62b5ef37329ed81b488ac063d1000
000000001976a914f76bc4190f3d8e23
15e5c11c59cfc8be9df747e388ac0000
0000
```

Transação: modelo de dados

```
0100000001f3f6a909f8521adb57d898d2985834e632374e770fd9e2b98656f1bf
1fdfd427010000006b48304502203a776322ebf8eb8b58cc6ced4f2574f4c73aa6
64edce0b0022690f2f6f47c521022100b82353305988cb0ebd443089a173ceec93
fe4dbfe98d74419ecc84a6a698e31d012103c5c1bc61f60ce3d6223a63cedbece0
3b12ef9f0068f2f3c4a7e7f06c523c3664ffffffff0260e31600000000001976a9
14977ae6e32349b99b72196cb62b5ef37329ed81b488ac063d1000000000001976
a914f76bc4190f3d8e2315e5c11c59cfc8be9df747e388ac00000000
```


```
b138360800cdc72248c3ca8dfd06de85913d1aac7f41b4fa54eb1f5a4a379081
```

ID da transação

Transação: *behind the scenes*


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "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",
    }
  ]
}
```


https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

Transação: *behind the scenes*


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "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",
    }
  ]
}
```


CADÊ O ENDEREÇO DE ALICE?

CADÊ O ENDEREÇO DE BOB?

CADÊ O INPUT DE 0,1 BTC DE ALICE?

Transação: *behind the scenes*

Alice: 1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK
Bob: 1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "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",
    }
  ]
}
```


https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

Transação: entradas e saídas

Full nodes registram todos os UTXOs disponíveis (conjunto UTXO)

Toda transação representa uma mudança no conjunto de UTXO

Quando dizemos que a carteira de um usuário recebeu bitcoin:

- A carteira dele detectou um UTXO que pode ser “gasto" com uma das chaves controlada por ela
- Ou seja, o saldo do usuário é a **soma de todos os UTXOs que a carteira do usuário pode gastar,** e que pode estar espalhada em centenas de transações e centenas de blocos
- O conceito de saldo é criado pela aplicação da carteira

Transação: entradas e saídas

A saída de uma transação pode conter um valor (inteiro) indicando um múltiplo de *satoshis*

Valores de saída são **discretos e indivisíveis** (satoshis)

Uma saída não gasta só pode ser consumida de maneira integral por uma transação

Se um UTXO é maior que o valor desejado na transação, ainda assim deve ser consumida integralmente

E o **troco** deve ser gerado na transação!

A única transação que não consome UTXO é a **coinbase**. Lembra dela?

Transação: saídas (*outputs*)

Consistem em duas partes:

Uma quantidade de bitcoin, em *satoshis*;

Um enigma criptográfico que determina as condições exigidas para gastar aquele *output*

Transação: saídas (*outputs*)

Consistem em duas partes:

Uma quantidade de bitcoin, em *satoshis*;

Um enigma criptográfico que determina as condições exigidas para gastar aquele *output*

também conhecido como *locking script* ou scriptPubKey

Transação: saídas (*outputs*)


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "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",
    }
  ]
}
```


https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

Transação: entradas (*inputs*)

São as saídas não resgatadas de outra transação

Todas as entradas referenciam de volta uma saída (qual a exceção?)

Identifica (por referência) qual UTXO será consumida e provê a prova de propriedade (***proof-of-ownership***) através de um ***unlocking script***

Um ou mais UTXOs podem ser necessários

Transação: entradas (*inputs*)

Consistem em quatro partes:

- Referência para o ID da transação que contém o UTXO a ser gasto
- Índice que indica qual UTXO dentro da transação referenciado será utilizado
- O necessário para satisfazer as condições estabelecidas pela UTXO daquela transação
- Número de sequência

também conhecido como *unlocking script* ou ScriptSig

Transação: entradas (*inputs*)


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "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",
    }
  ]
}
```


https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

Transação: entradas (*inputs*)


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
"3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813
0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value":
      "scriptPu
    },
    {
      "value":
      "scriptPu
    }
  ]
}
```

```
"vout": [
   {
     "value": 0.10000000,
     "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG"
   }
 ]
```


https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2