BitcoinのTransactionとは

@DG Lab Nakagawa

Agenda

- Transactionとは
  - インプットとは
  - アウトプットとは
  - インプットとアウトプットの関係
  - 手数料（fee）とは
  - UTXO（Unspent Transaction Output）とは

Transactionとは

Transactionとは

satoshi(BTC)を

取引する時に使い

ブロックの中に残るデータ

Transactionとは

簡単な構造

名称	概要
version	Transactionのバージョン（基本「1」）
tx_in count	**インプットの数**
tx_in[0] … tx_in[n]	**インプット**
tx_out count	**アウトプットの数**
tx_out[0] … tx_out[n]	**アウトプット**
lock_time	Unixタイムスタンプ、またはブロック高（基本0）

Transactionとは

※Transactionは、
少なくとも1つのインプットとアウトプットを持つ

簡単な構造

名称	概要
version	Transactionのバージョン（基本「1」）
tx_in count	**インプットの数**
tx_in[0] … tx_in[n]	**インプット**
tx_out count	**アウトプットの数**
tx_out[0] … tx_out[n]	**アウトプット**
lock_time	Unixタイムスタンプ、またはブロック高（基本0）

インプットとは

インプットとは

簡単な構造

名称		概要
previous_output	hash	未使用のTransactionID(TXID)
	index	上記IDのインデックス
script length		スクリプトのデータサイズ
signature script		署名スクリプト（unlocking Script）
sequence		シーケンス

インプットとは

簡単な構造

※Transactionのインプットとは
未使用Transaction（UTXO）のエンドポイント

名称		概要
previous_output	hash	未使用のTransactionID(TXID)
	index	上記IDのインデックス
script length		スクリプトのデータサイズ
signature script		署名スクリプト（unlocking Script）
sequence		シーケンス

後で説明！

アウトプットとは

簡単な構造

名称	概要
value	**送信額**
pk_script length	スクリプトのデータサイズ
pk_script	**送信先？（locking script）**

アウトプットとは

簡単な構造

※Transactionのアウトプットとは
送信額と送信先？(locking script)

名称	概要
value	**送信額**
pk_script length	スクリプトのデータサイズ
pk_script	**送信先？（locking script）**

後で説明！

インプットとアウトプットの関係

インプットとアウトプットの関係

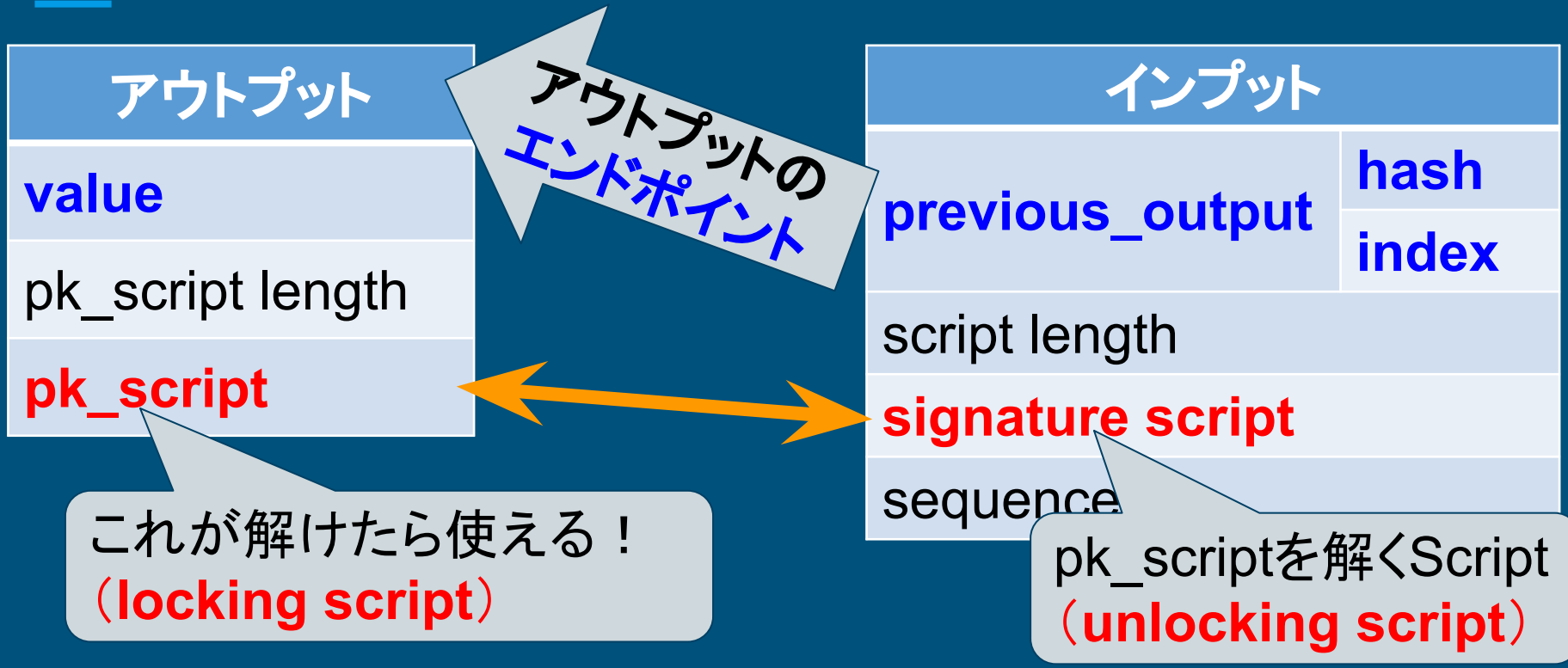
アウトプットは次のトランザクションのインプットとなる

どうやったら使える？誰でも使える？

トランザクション1（Tx1）
インプット0（tx_in[0]）
インプット1（tx_in[1]）
アウトプット0（tx_out[0]）
アウトプット1（tx_out[1]）

トランザクション2（Tx2）
インプット0（tx_in[0]）
アウトプット0（tx_out[0]）
アウトプット1（tx_out[1]）

インプットとアウトプットの関係



Transactionの例

- 手数料（fee）
- UTXO

Transactionの例

取引：AAAさんがCCCさんに500,000satoshi支払う

Tx1
tx_ins
  tx_in[0]
tx_outs
  tx_out[0] 1,000,000 AAA
  tx_out[1] 998,000 BBB

Tx2
tx_ins
  tx_in[0] Tx1 0
tx_outs
  tx_out[0] 500,000 CCC
  tx_out[1] 498,000 AAA

Transactionの例

※Transacationの
アウトプットは使い切り

取引：AAAさんがCCCさんに500,000satoshi支払う

Tx1
tx_ins
  tx_in[0]
tx_outs
  tx_out[0] 1,000,000 AAA
  tx_out[1] 998,000 BBB

Tx2
tx_ins
  tx_in[0] Tx1 0
tx_outs
  tx_out[0] 500,000 CCC
  tx_out[1] 498,000 AAA

手数料（fee）とは

Tx1
tx_outs
tx_out[0]　1,000,000 AAA

Tx2
tx_outs
tx_out[0]　500,000　CCC
tx_out[1]　498,000　AAA

1,000,000 - (500,000 + 498,000) = 2,000
手数料（fee）は、2,000satoshi

※：bitcoinでは手数料を1,000satoshi以上にしないと
ブロードキャストしない可能性があります

手数料（fee）とは

手数料（fee）＝「インプットの総額」ー「アウトプットの総額」

- **手数料（fee）はどうやって決まる？**
  トランザクションのデータサイズ／1byteあたりのSatoshi
  1,000satoshi以上が望ましい

- **手数料（fee）が少ないとどうなる？**
  ブロックに入るのに時間がかかる

手数料（fee）とは

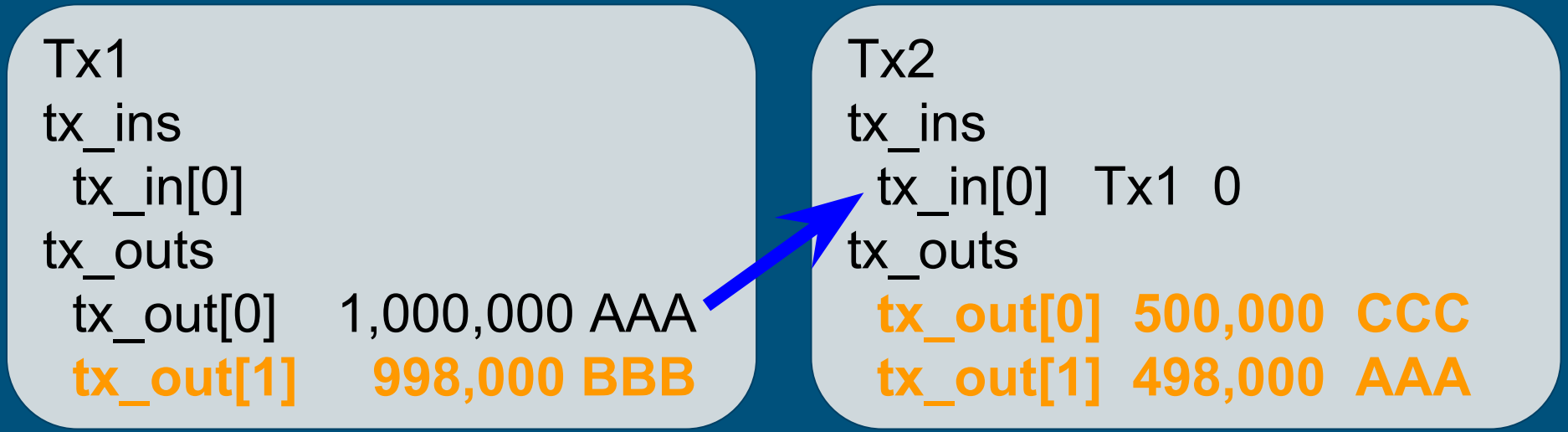
現在のMainnetのFeeは？

https://estimatefee.appspot.com/

※：1Kbyteあたりの手数料（fee）

UTXO（Unspent Transaction Output）とは

※：UTXOは未使用Transaction
(TransactionIDとアウトプットのインデックス)



演習

演習

次の4つの取引が行われた場合、AAA、BBB、CCCが所持しているsatoshiの総額とUTXOはどれか？

Tx1
tx_ins
tx_in[0]
tx_outs
tx_out[0] 1,000,000 AAA
tx_out[1] 998,000 BBB
tx_out[2] 1,000,000 CCC

Tx2
tx_ins
tx_in[0] Tx1 2

tx_outs
tx_out[0] 500,000 BBB
tx_out[1] 498,000 AAA

Tx3
tx_ins
tx_in[0] Tx2 0

tx_outs
tx_out[0] 498,000 CCC

Tx4
tx_ins
tx_in[0] Tx3 0
tx_in[1] Tx1 0
tx_outs
tx_out[0] 1,496,000 BBB

Tx1
tx_ins
tx_in[0]
tx_outs
tx_out[0] 1,000,000 AAA
tx_out[1] 998,000 BBB
tx_out[2] 1,000,000 CCC

Tx2
tx_ins
tx_in[0] Tx1 2

tx_outs
tx_out[0] 500,000 BBB
tx_out[1] 498,000 AAA

Tx3
tx_ins
tx_in[0] Tx2 0

tx_outs
tx_out[0] 498,000 CCC

Tx4
tx_ins
tx_in[0] Tx3 0
tx_in[1] Tx1 0
tx_outs
tx_out[0] 1,496,000 BBB

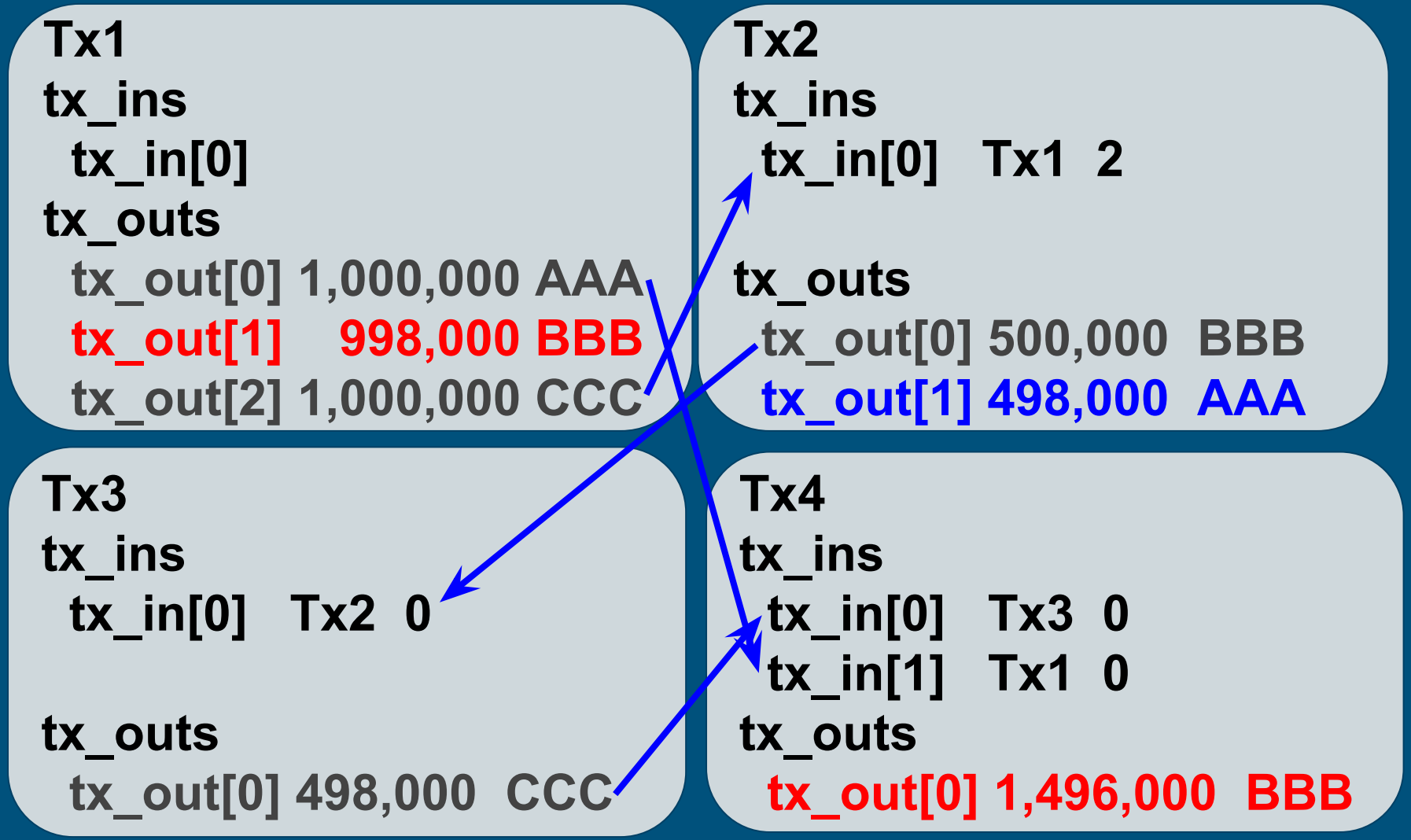
回答

UTXO
Tx1 1
Tx2 1
Tx4 0

AAA
Tx2 1 498,000
Total：498,000 satoshi

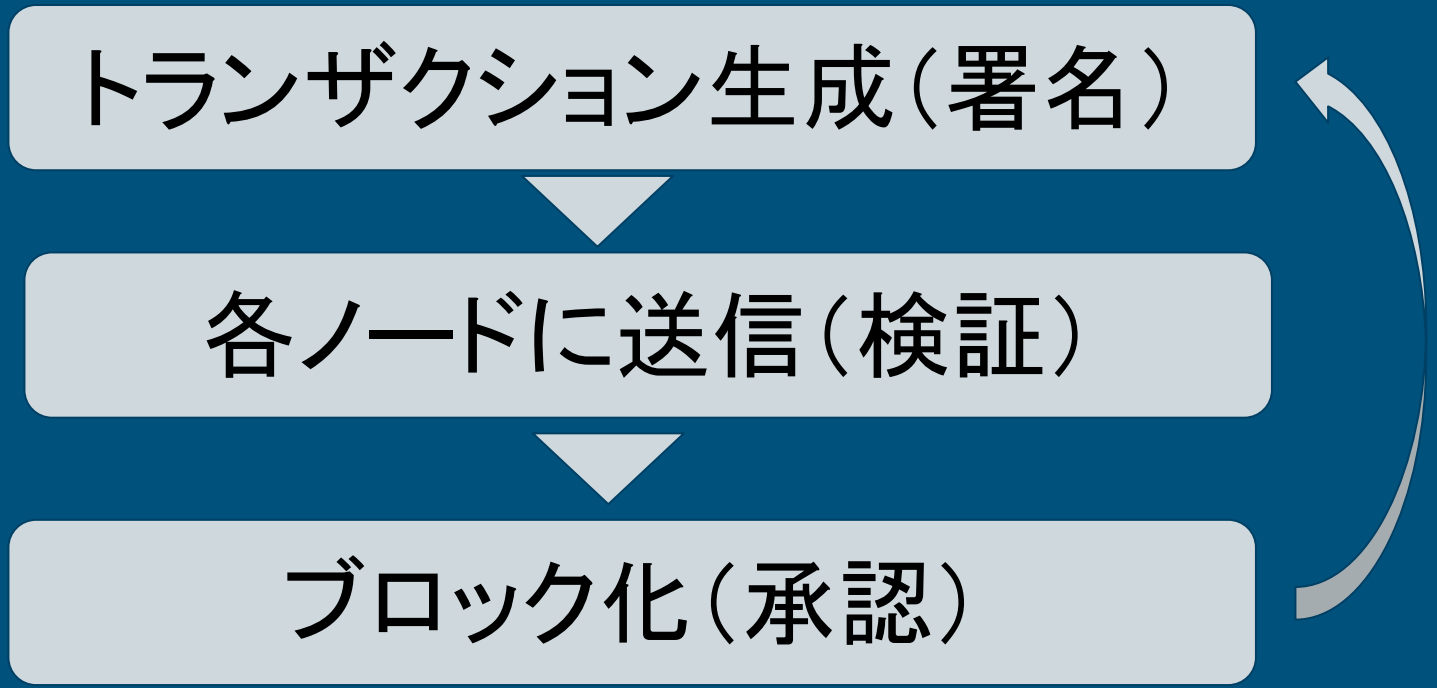
BBB
Tx1 1 998,000
Tx4 0 1,496,000
Total：2,494,000 satoshi

CCC
Total：0 satoshi


Tx1
tx_ins
tx_in[0]
tx_outs
tx_out[0] 1,000,000 AAA
tx_out[1] 998,000 BBB
tx_out[2] 1,000,000 CCC
Tx2
tx_ins
tx_in[0] Tx1 2
tx_outs
tx_out[0] 500,000 BBB
tx_out[1] 498,000 AAA
Tx3
tx_ins
tx_in[0] Tx2 0
tx_outs
tx_out[0] 498,000 CCC
Tx4
tx_ins
tx_in[0] Tx3 0
tx_in[1] Tx1 0
tx_outs
tx_out[0] 1,496,000 BBB

まとめ

Transactionのライフサイクル



まとめ

- Transactionは、少なくとも1つのインプットとアウトプットを持つ
- インプットとは未使用Transaction（UTXO）のエンドポイント
- アウトプットとは送信額と送信先？（locking script）
- アウトプットは使い切り
- 手数料（fee）＝「インプットの総額」ー「アウトプットの総額」
- 手数料（fee）はトランザクションのサイズによって決まる
- UTXOは使用していないTransaction
  (TransactionIDとアウトプットのインデックス)

参考資料

- ビットコインとブロックチェーン:暗号通貨を支える技術
  ISBN-13: 978-4757103672
- Bitcoin: A Peer-to-Peer Electronic Cash System
  https://bitcoin.org/bitcoin.pdf
- Protocol documentation
  https://en.bitcoin.it/wiki/Protocol_documentation
- Transactions
  https://bitcoin.org/en/developer-guide#transactions

takatoshi@dglab.com