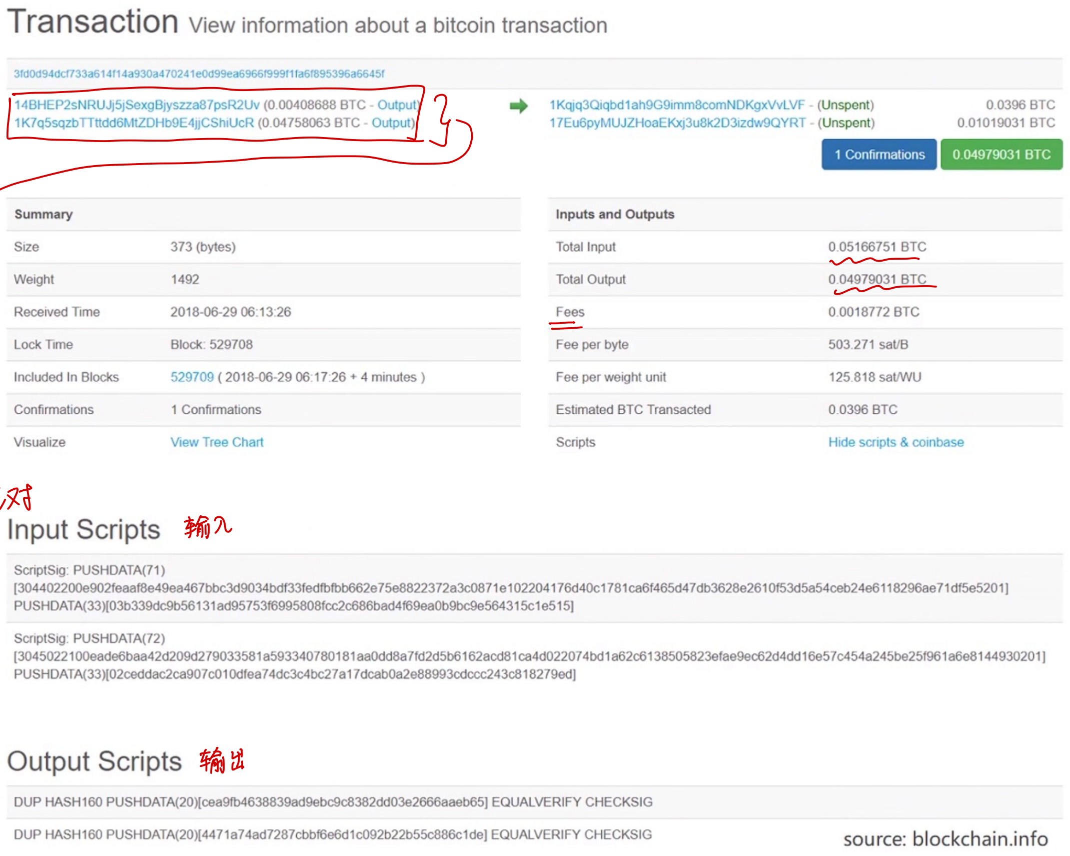


Transaction View information about a bitcoin transaction

3fd0d94dcf733a614f14a930a470241e0d99ea6966f999f1fa6f895396a6645f

14BHEP2sNRUJj5jSexgBjyszza87psR2Uv (0.00408688 BTC - Output)
1K7q5sqzbTTttdd6MtZDHb9E4jjCShiUcR (0.04758063 BTC - Output)

1Kqjq3Qiqbd1ah9G9imm8comNDKgxVvLVF - (Unspent) 0.0396 BTC
17Eu6pyMUJZHoaEKxj3u8k2D3izdw9QYRT - (Unspent) 0.01019031 BTC

1 Confirmations | 0.04979031 BTC

Summary	
Size	373 (bytes)
Weight	1492
Received Time	2018-06-29 06:13:26
Lock Time	Block: 529708
Included In Blocks	529709 (2018-06-29 06:17:26 + 4 minutes)
Confirmations	1 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.05166751 BTC
Total Output	0.04979031 BTC
Fees	0.0018772 BTC
Fee per byte	503.271 sat/B
Fee per weight unit	125.818 sat/WU
Estimated BTC Transacted	0.0396 BTC
Scripts	Hide scripts & coinbase

配对

Input Scripts 输入

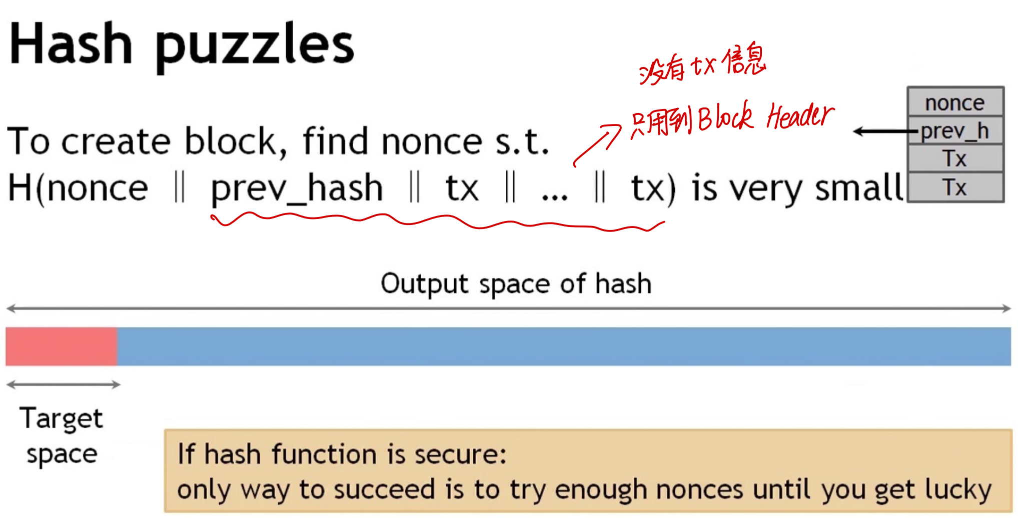
```
ScriptSig: PUSHDATA(71)
[304402200e902feaaf8e49ea467bbc3d9034bdf33fedfbfbb662e75e8822372a3c0871e102204176d40c1781ca6f465d47db3628e2610f53d5a54ceb24e6118296ae71df5e5201]
PUSHDATA(33)[03b339dc9b56131ad95753f6995808fcc2c686bad4f69ea0b9bc9e564315c1e515]

ScriptSig: PUSHDATA(72)
[3045022100eade6baa42d209d279033581a593340780181aa0dd8a7fd2d5b6162acd81ca4d022074bd1a62c6138505823efae9ec62d4dd16e57c454a245be25f961a6e8144930201]
PUSHDATA(33)[02ceddac2ca907c010dfea74dc3c4bc27a17dcab0a2e88993cdccc243c818279ed]
```

Output Scripts 输出

```
DUP HASH160 PUSHDATA(20)[cea9fb4638839ad9ebc9c8382dd03e2666aaeb65] EQUALVERIFY CHECKSIG
DUP HASH160 PUSHDATA(20)[4471a74ad7287cbbf6e6d1c092b22b55c886c1de] EQUALVERIFY CHECKSIG
```

source: blockchain.info



Hash puzzles

To create block, find nonce s.t.
H(nonce ‖ prev_hash ‖ tx ‖ … ‖ tx) is very small

没有tx信息
只用到Block Header

If hash function is secure:
only way to succeed is to try enough nonces until you get lucky

这是比特币教材配套的一页PPT。大家看看有问题吗？