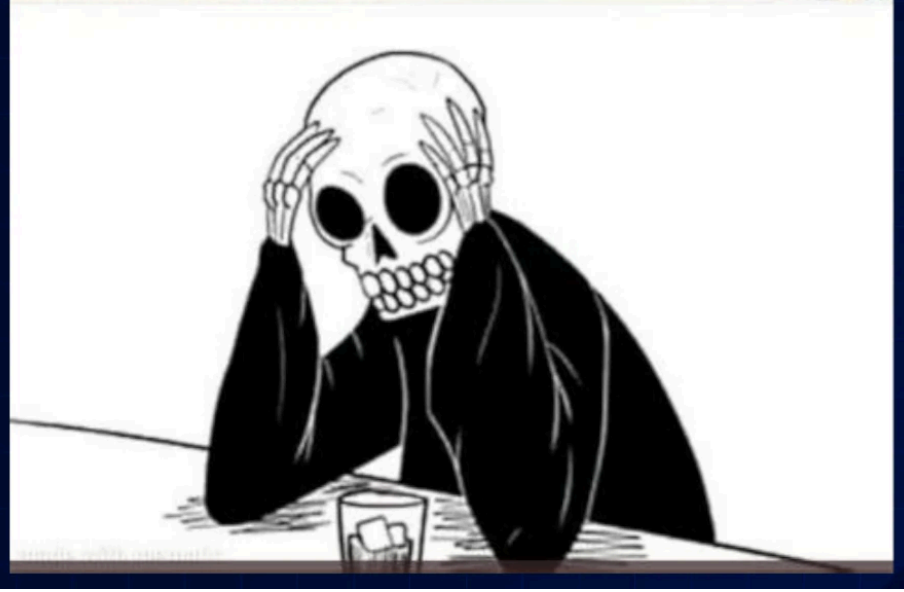
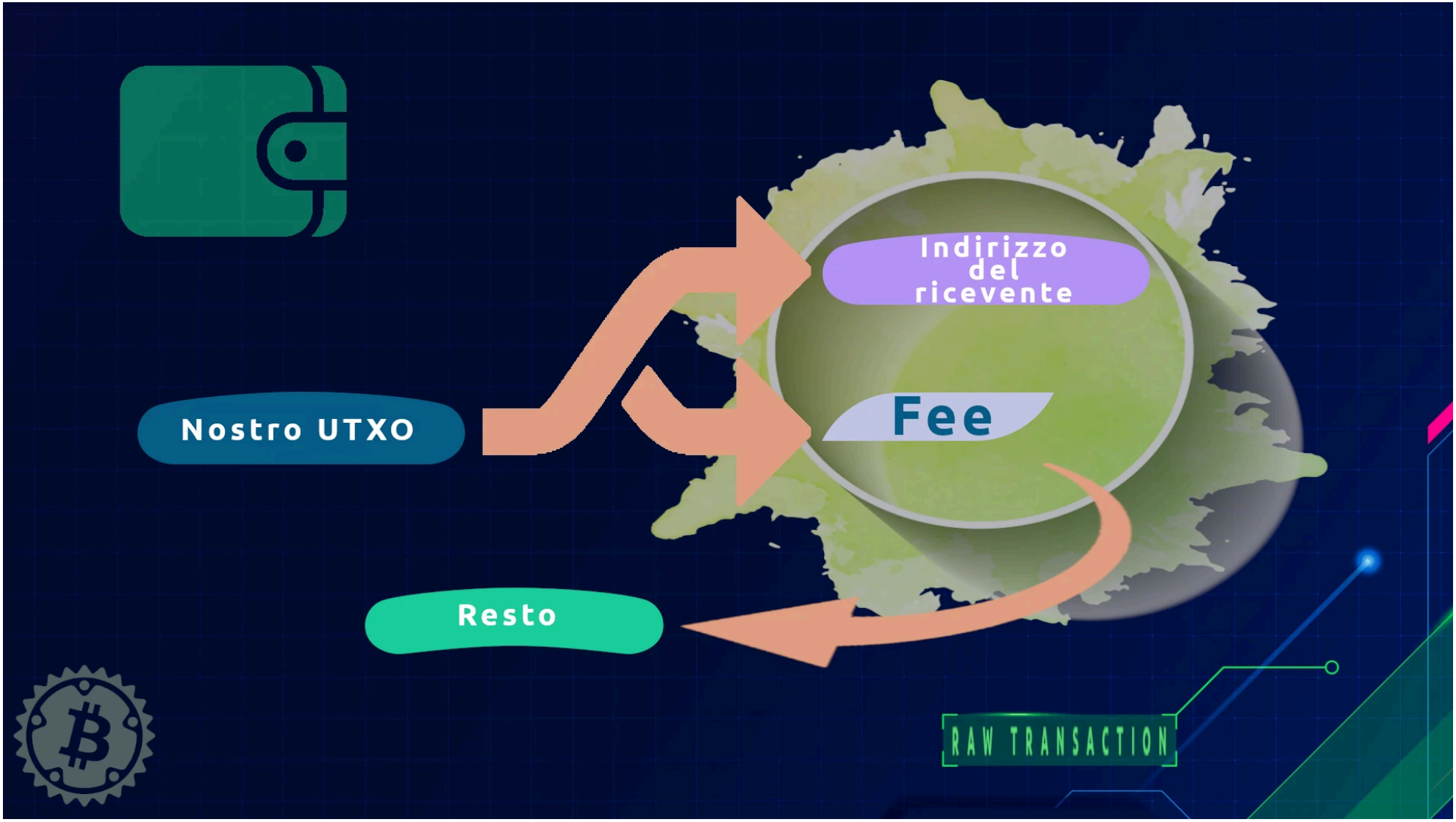
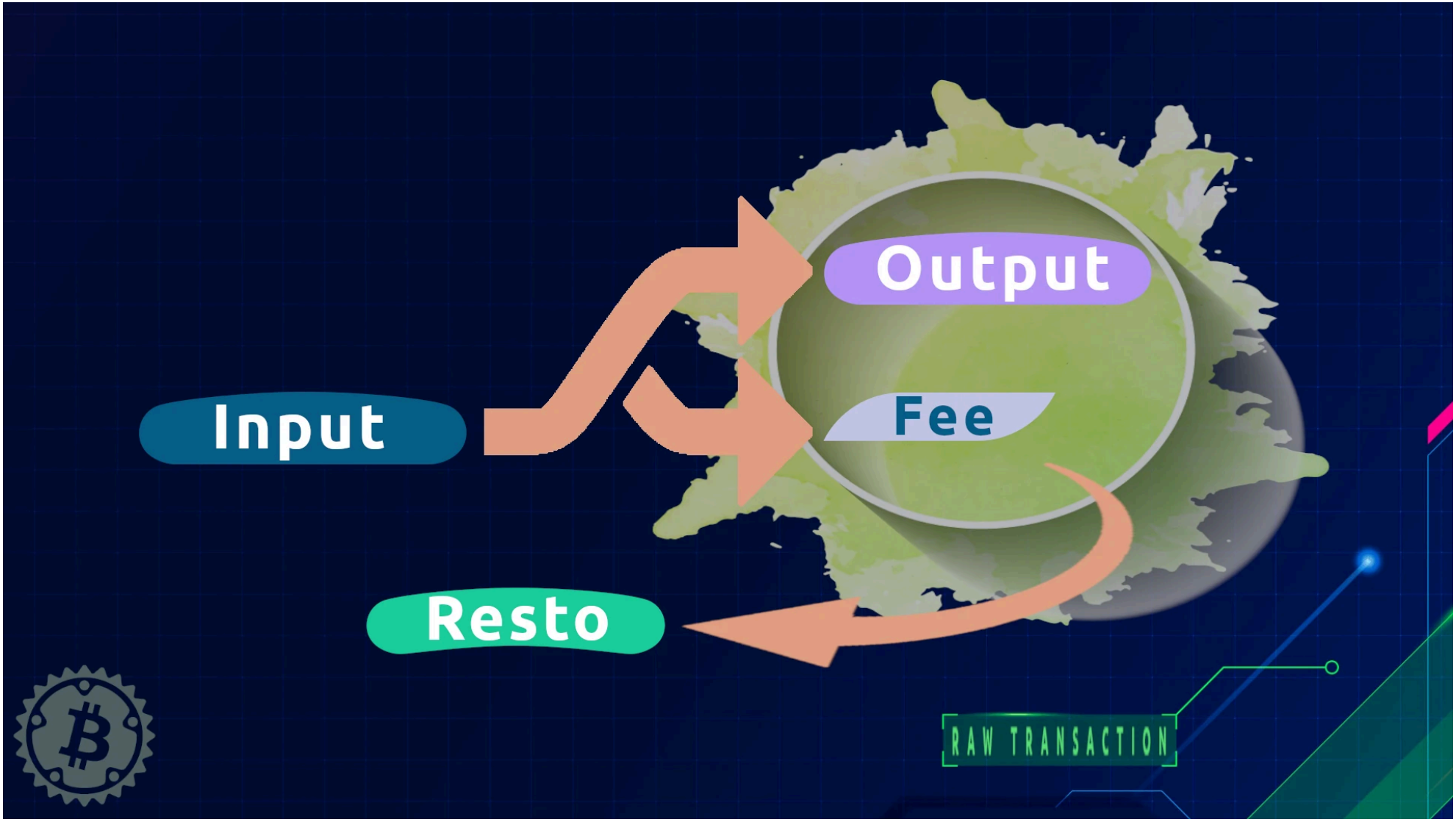

{
"version": "02000000",
"marker": "00",
"flag": "01",
"inputcount": "01",
"inputs": [
{
"txid":
"eeb3727abb795157c1dcaa6cfb70b4df23390a7b9ba8e1c2456e6b05ac28c3a6",
"vout": "00000000",
"scriptsigsize": "00",
"scriptsig": "",
"sequence": "fdffffff"
}
],
"outputcount": "01",
"outputs": [
{
"amount": "de9000000000000",
"scriptpubkeysize": "16",
"scriptpubkey": "0014f197f02d16ff3ad6cfb59ee0d2d0fb666d6942ed"
}
],
"witness": [
{
"stackitems": "02",
"0": {
"size": "47",
"item": "304402201339e0c38b8f44e08cc596cc6ab8bd8caffc6b3648802afa7ba769f
3adfed66302205230fe2e94affd87439a48edfe09e1fed460ffc34bebaeb7d862b7d904c
b2b4a01"
},
"1": {
"size": "21",
"item":
"026237abe420d2887c61daccd9f45b637eca5e75ed88e203999e2fabc80ce8ed37"
}
}
],
"locktime": "14160e00"
}
LA STRUTTURA DELLA
TRANSAZIONE
BITCOIN
[Introduzione]
RAW TRANSACTION

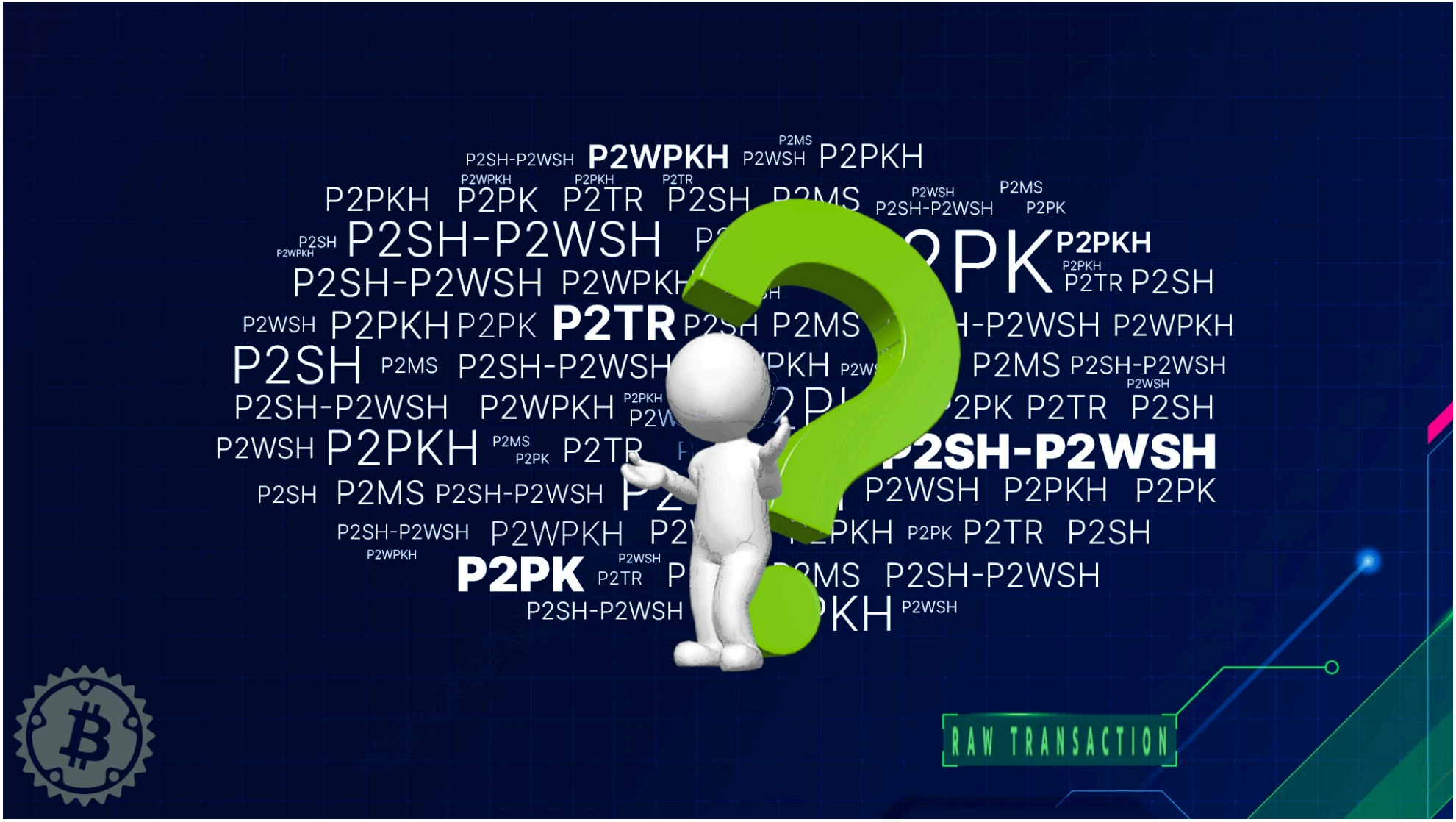


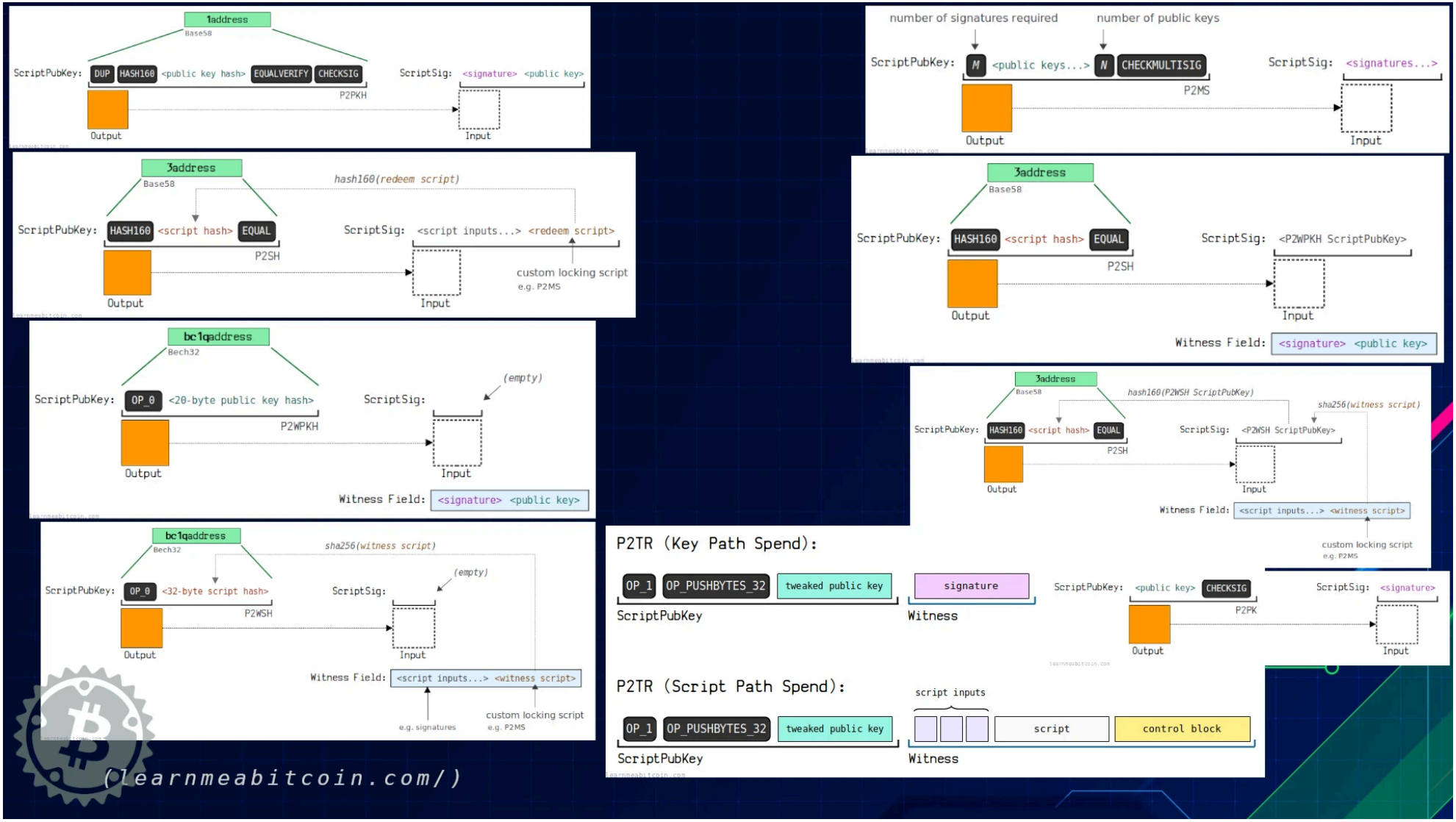
meme

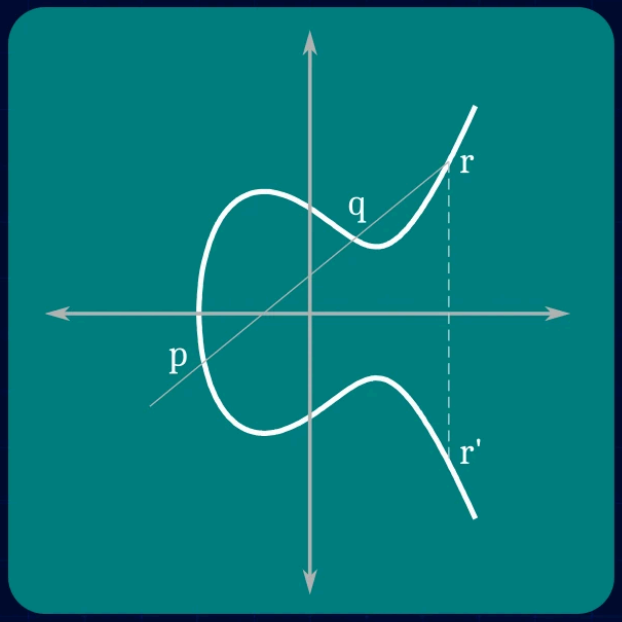

Indirizzo del ricevente
Nostro UTXO
Fee
Resto
RAW TRANSACTION


Output
Input
Fee
Resto
RAW TRANSACTION


Per iniziare a costruire la transazione, dobbiamo chiedere un indirizzo alla controparte.
RAW TRANSACTION


P2SH-P2WSH
P2WPKH
P2MS
P2WSH
P2PKH
P2PK
P2TR
P2SH
RAW TRANSACTION


1address
Base58
ScriptPubKey:
DUP
HASH160
<public key hash>
EQUALVERIFY
CHECKSIG
P2PKH
ScriptSig:
<signature>
<public key>
Output
Input
number of signatures required
number of public keys
ScriptPubKey:
M
<public keys...>
N
CHECKMULTISIG
P2MS
ScriptSig:
<signatures...>
Output
Input
3address
Base58
hash160(redeem script)
ScriptPubKey:
HASH160
<script hash>
EQUAL
P2SH
ScriptSig:
<script inputs...>
<redeem script>
custom locking script
e.g. P2MS
Output
Input
3address
Base58
ScriptPubKey:
HASH160
<script hash>
EQUAL
P2SH
ScriptSig:
<P2WPKH ScriptPubKey>
Output
Input
Witness Field:
<signature>
<public key>
bc1qaddress
Bech32
ScriptPubKey:
OP_0
<20-byte public key hash>
P2WPKH
ScriptSig:
(empty)
Output
Input
Witness Field:
<signature>
<public key>
3address
Base58
hash160(P2WSH ScriptPubKey)
sha256(witness script)
ScriptPubKey:
HASH160
<script hash>
EQUAL
P2SH
ScriptSig:
<P2WSH ScriptPubKey>
Output
Input
Witness Field:
<script inputs...>
<witness script>
custom locking script
e.g. P2MS
bc1qaddress
Bech32
sha256(witness script)
ScriptPubKey:
OP_0
<32-byte script hash>
P2WSH
ScriptSig:
(empty)
Output
Input
Witness Field:
<script inputs...>
<witness script>
e.g. signatures
custom locking script
e.g. P2MS
P2TR (Key Path Spend):
OP_1
OP_PUSHBYTES_32
tweaked public key
ScriptPubKey
signature
Witness
ScriptPubKey:
<public key>
CHECKSIG
P2PK
Output
ScriptSig:
<signature>
Input
P2TR (Script Path Spend):
script inputs
OP_1
OP_PUSHBYTES_32
tweaked public key
ScriptPubKey
script
control block
Witness
(learnmeabitcoin.com/)



Operazioni matematiche sulla curva ellittica

- generazione chiavi master
- derivazione chiavi (priv/pub) figlie

RAW TRANSACTION

COSA CREDIAMO CI SIA NELLA TX

- Chiavi pubbliche, o meglio: indirizzi

- importo

- Firma digitale

RAW TRANSACTION

COSA C'È VERAMENTE NELLA TX

- Chiavi pubbliche
  O meglio: ScriptPubKey

- Smart Contract.
  Condizioni di spesa
  (locking / unlocking)

- Firma digitale

- importo

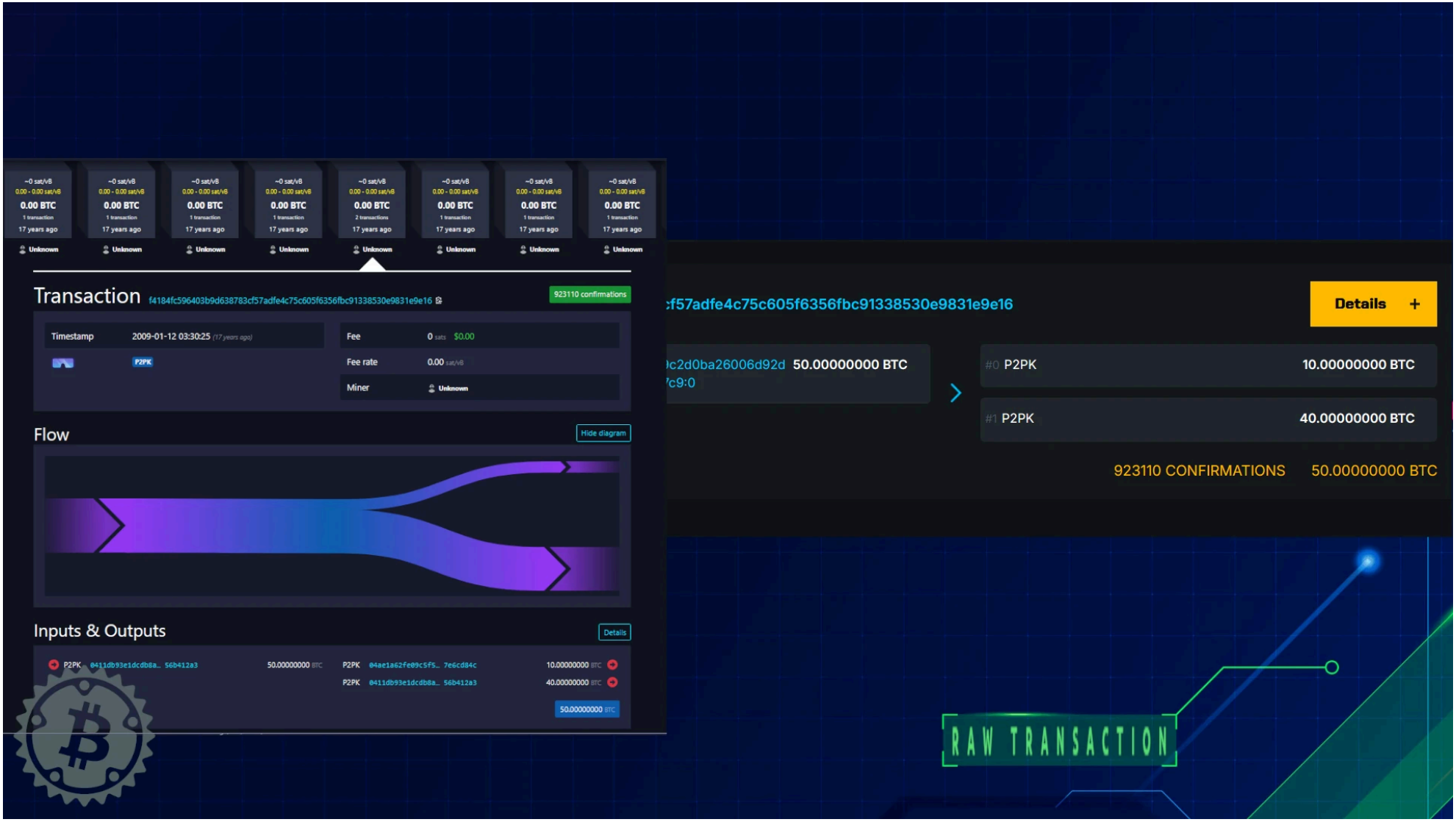
- Versione

- Marker

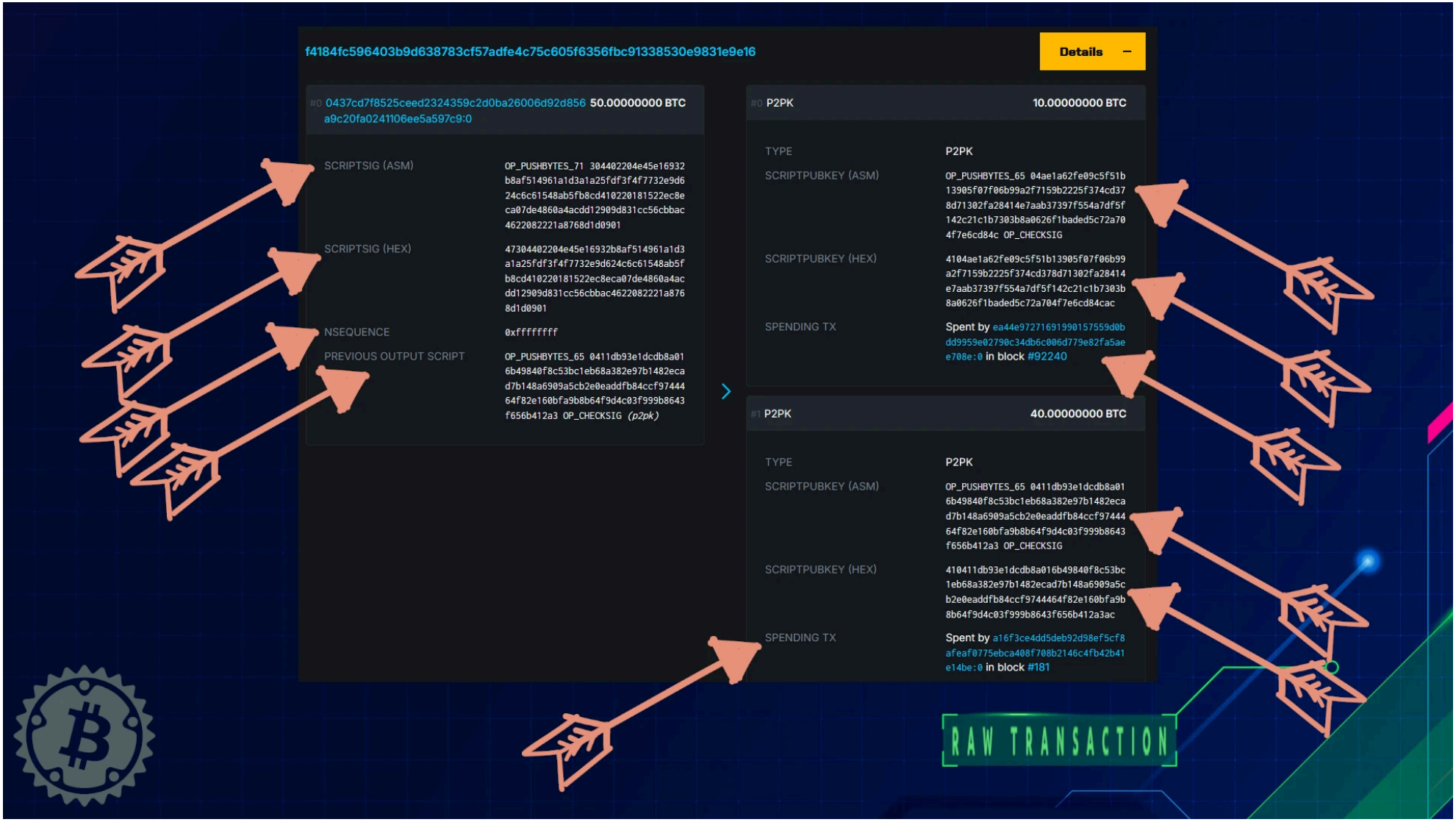
- Flag

- Locktime

RAW TRANSACTION


Transaction
f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16
923110 confirmations
Timestamp
2009-01-12 03:30:25
Fee
0 sats $0.00
Fee rate
0.00
Miner
Unknown
Flow
Hide diagram
Inputs & Outputs
Details
50.00000000 BTC
10.00000000 BTC
40.00000000 BTC
Details
#0 P2PK
10.00000000 BTC
#1 P2PK
40.00000000 BTC
923110 CONFIRMATIONS
50.00000000 BTC
RAW TRANSACTION

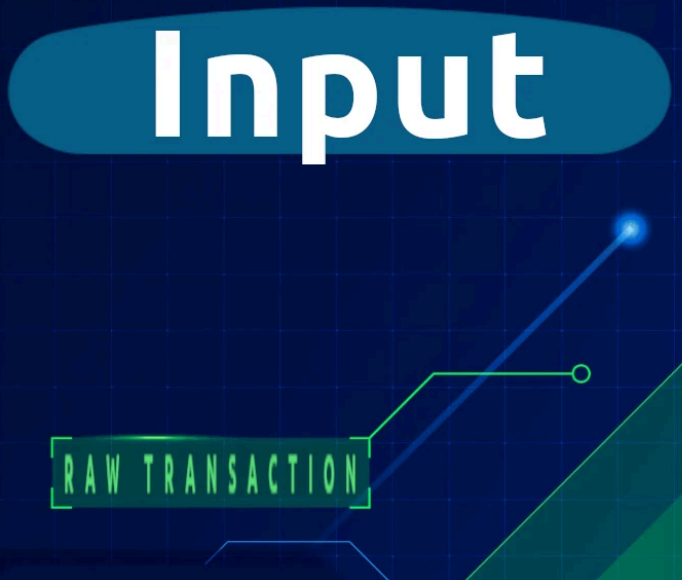

Transaction
f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16
923110 confirmations
Timestamp
2009-01-12 03:30:25
Fee
Fee rate
Miner
Unknown
Flow
Hide diagram
Inputs & Outputs
Details
50.00000000 BTC
10.00000000 BTC
40.00000000 BTC
Details +
10.00000000 BTC
40.00000000 BTC
923110 CONFIRMATIONS
50.00000000 BTC
RAW TRANSACTION


f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16
Details
#0 0437cd7f8525ceed2324359c2d0ba26006d92d856a9c20fa0241106ee5a597c9:0
50.00000000 BTC
SCRIPTSIG (ASM)
OP_PUSHBYTES_71 304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d0901
SCRIPTSIG (HEX)
47304402204e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624c6c61548ab5fb8cd410220181522ec8eca07de4860a4acdd12909d831cc56cbbac4622082221a8768d1d0901
NSEQUENCE
0xffffffff
PREVIOUS OUTPUT SCRIPT
OP_PUSHBYTES_65 0411db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3 OP_CHECKSIG (p2pk)
#0 P2PK
10.00000000 BTC
TYPE
P2PK
SCRIPTPUBKEY (ASM)
OP_PUSHBYTES_65 04ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7df5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84c OP_CHECKSIG
SCRIPTPUBKEY (HEX)
4104ae1a62fe09c5f51b13905f07f06b99a2f7159b2225f374cd378d71302fa28414e7aab37397f554a7df5f142c21c1b7303b8a0626f1baded5c72a704f7e6cd84cac
SPENDING TX
Spent by ea44e97271691990157559d0bdd9959e02790c34db6c006d779e82fa5aee708e:0 in block #92240
#1 P2PK
40.00000000 BTC
TYPE
P2PK
SCRIPTPUBKEY (ASM)
OP_PUSHBYTES_65 0411db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3 OP_CHECKSIG
SCRIPTPUBKEY (HEX)
410411db93e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8b64f9d4c03f999b8643f656b412a3ac
SPENDING TX
Spent by a16f3ce4dd5deb92d98ef5cf8afeaf0775ebca408f708b2146c4fb42b41e14be:0 in block #181
RAW TRANSACTION


STRUTTURA DELLA TX
Versione
Input
Output
Locktime
RAW TRANSACTION

INPUT

- Hash della transazione *parent*
- Index TX della transazione *parent*
- *ScriptSig* (script di sblocco / unlocking)
- *Sequence*



OUTPUT

- Importo (espresso in satoshi)

- *SriptPubKey* - script di blocco

FEE

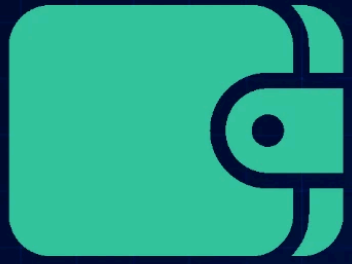
- Non sono esplicite, ma calcolate

- *La somma degli input, meno la* somma degli output, identifica le fee

CHANGE/RESTO

- Deve essere esplicitato 😂 altrimenti finisce nelle fee per il miner

Resto



RAW TRANSACTION

TRANSAZIONE

- trasferimento di valore, da uno smart contract ad un altro che viene trasmesso alla rete e raccolto in blocchi
- fa riferimento agli output delle transazioni precedenti come nuovi input della TX e consuma tutti gli input verso nuovi output

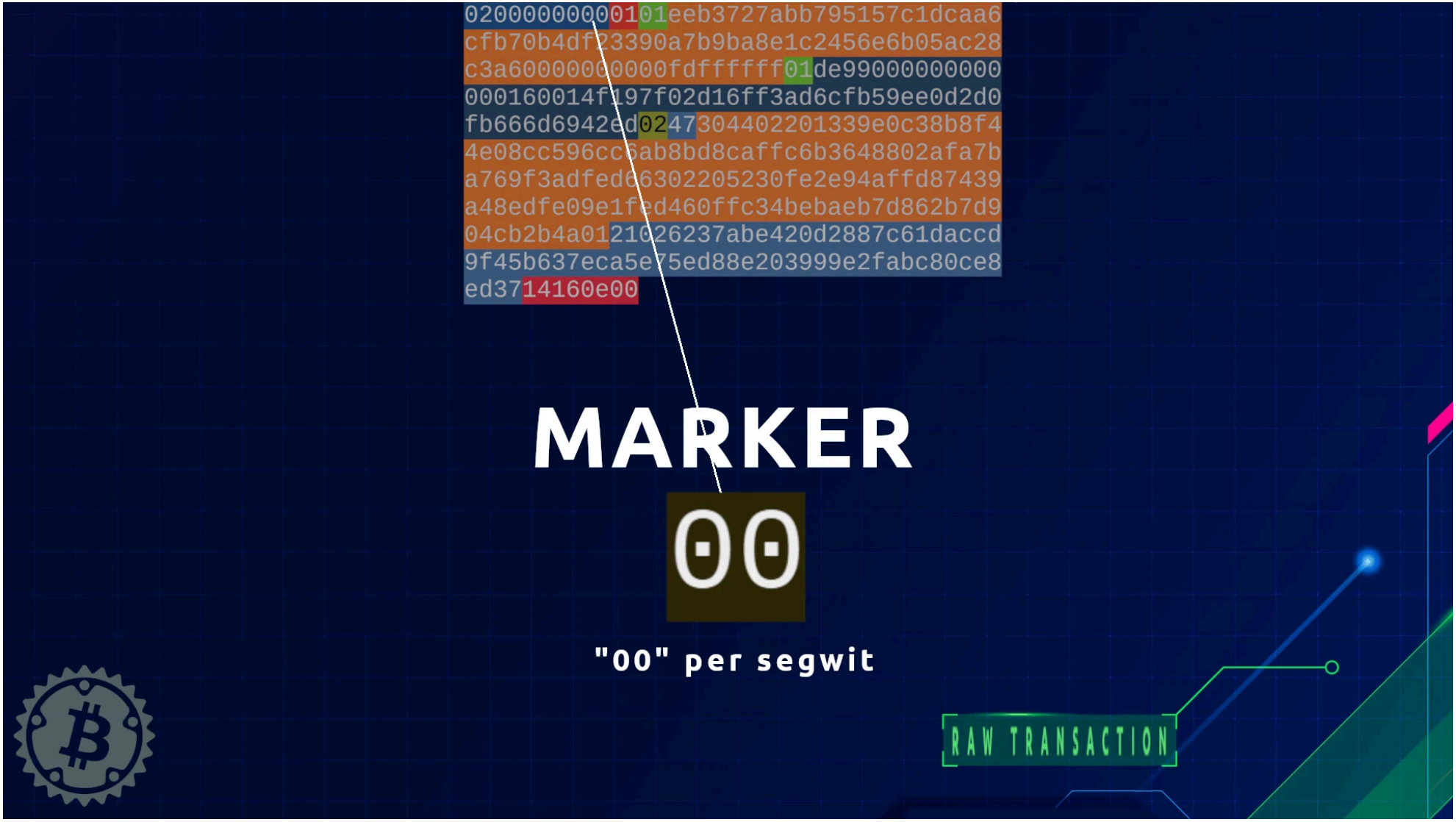
/en.bitcoin.it/

RAW TRANSACTION

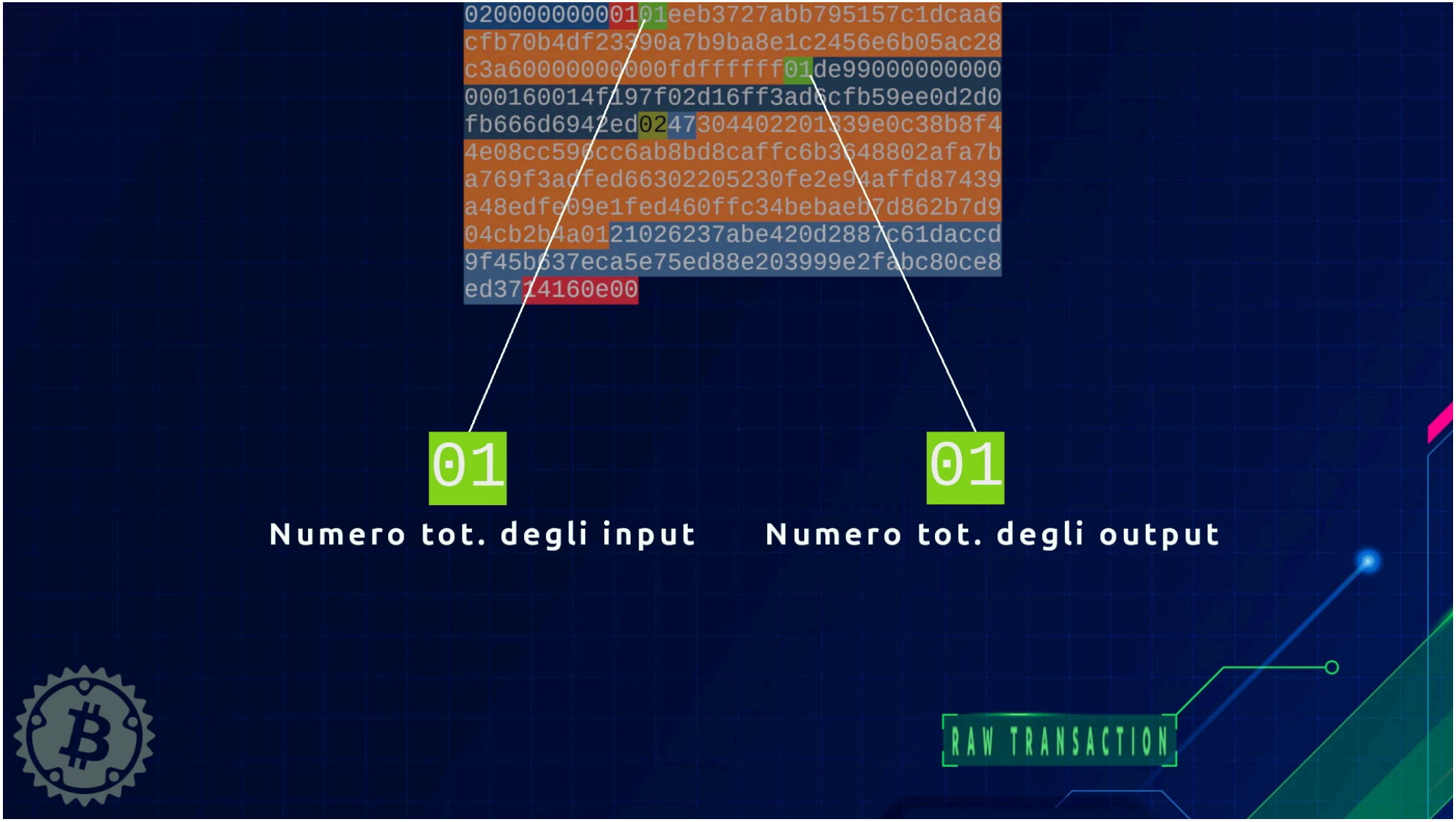
TRANSAZIONE

TRANSAZIONE


02000000000101eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a6000000000fdffffff01de99000000000
00160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed0247304402201339e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
VERSION
02000000
RAW TRANSACTION

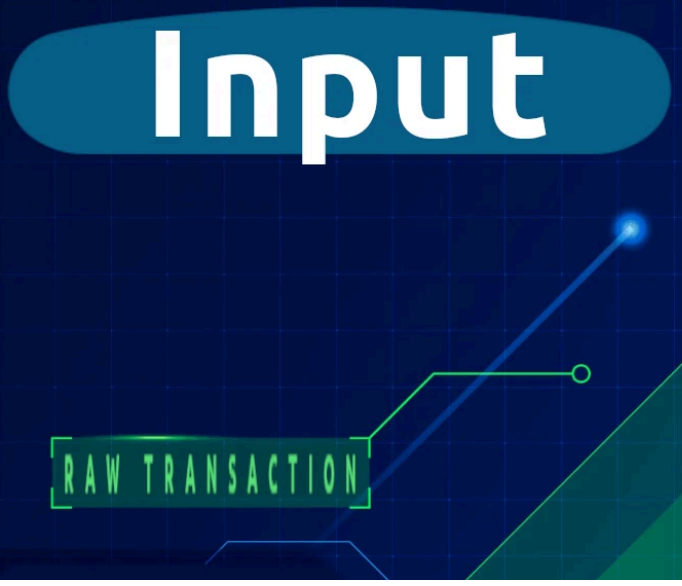

02000000000101eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a6000000000fdffffff01de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022013 39e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
MARKER
00
"00" per segwit
RAW TRANSACTION

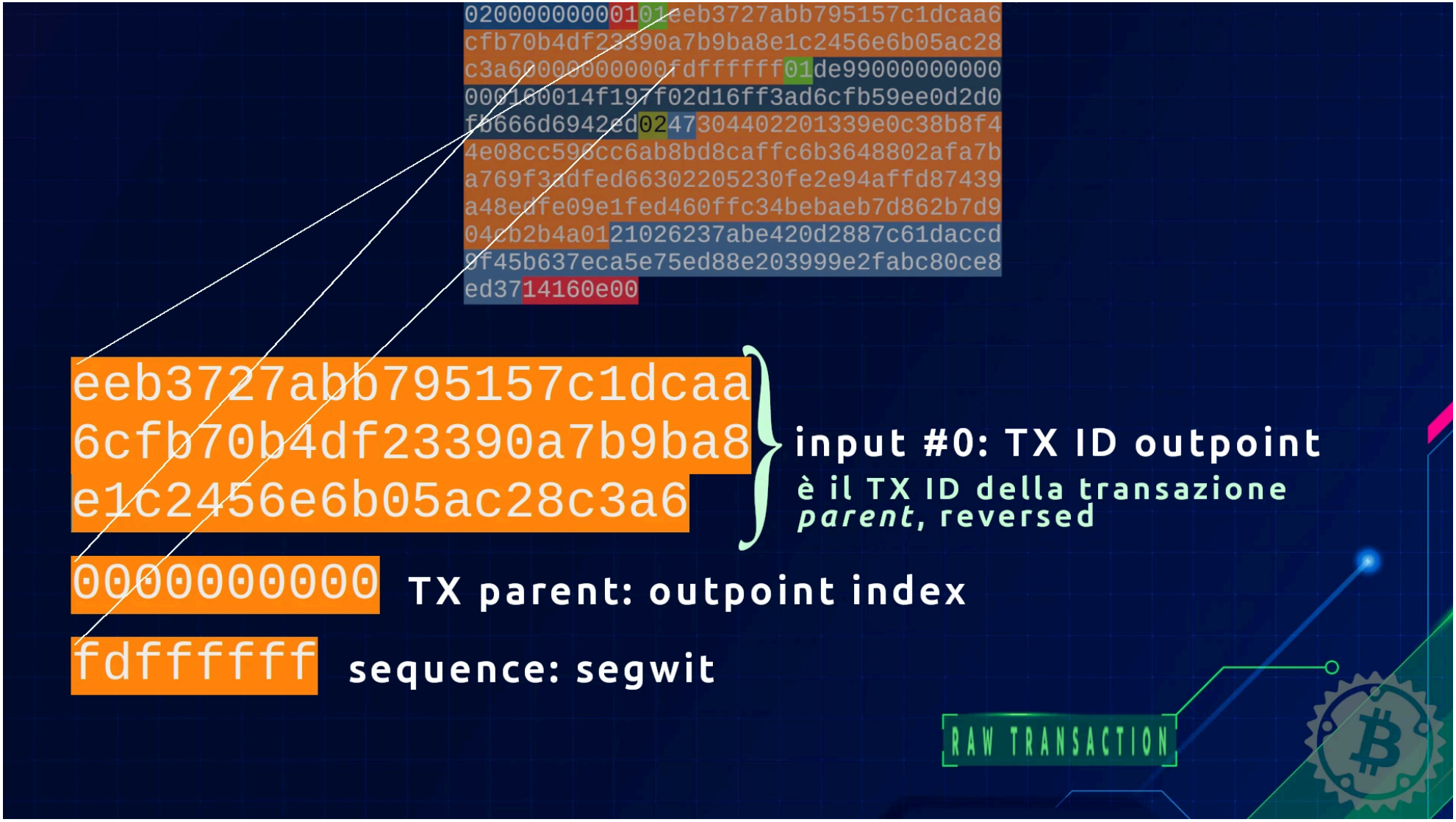

01000000001c997a5e56e104102fa209c6a852dd90660a20
b2d9c352423edce25857fcd3704000000004847304402204
4e45e16932b8af514961a1d3a1a25fdf3f4f7732e9d624
c6c61548ab5fb8cd410220181522ec8eca07de4860a4ac-
dd12909d831cc56cbbac4622082221a8768d1d0901ffff-
ffff0200ca9a3b00000000434104ae1a62fe09c5f51b139
05f07f06b99a2f7159b2225f374cd378d71302fa28414e7
aab37397f554a7df5f142c21c1b7303b8a0626f1baded5
c72a704f7e6cd84cac00286bee0000000043410411db93
e1dcdb8a016b49840f8c53bc1eb68a382e97b1482ecad7
b148a6909a5cb2e0eaddfb84ccf9744464f82e160bfa9b8
b64f9d4c03f999b8643f656b412a3ac00000000
RAW TRANSACTION

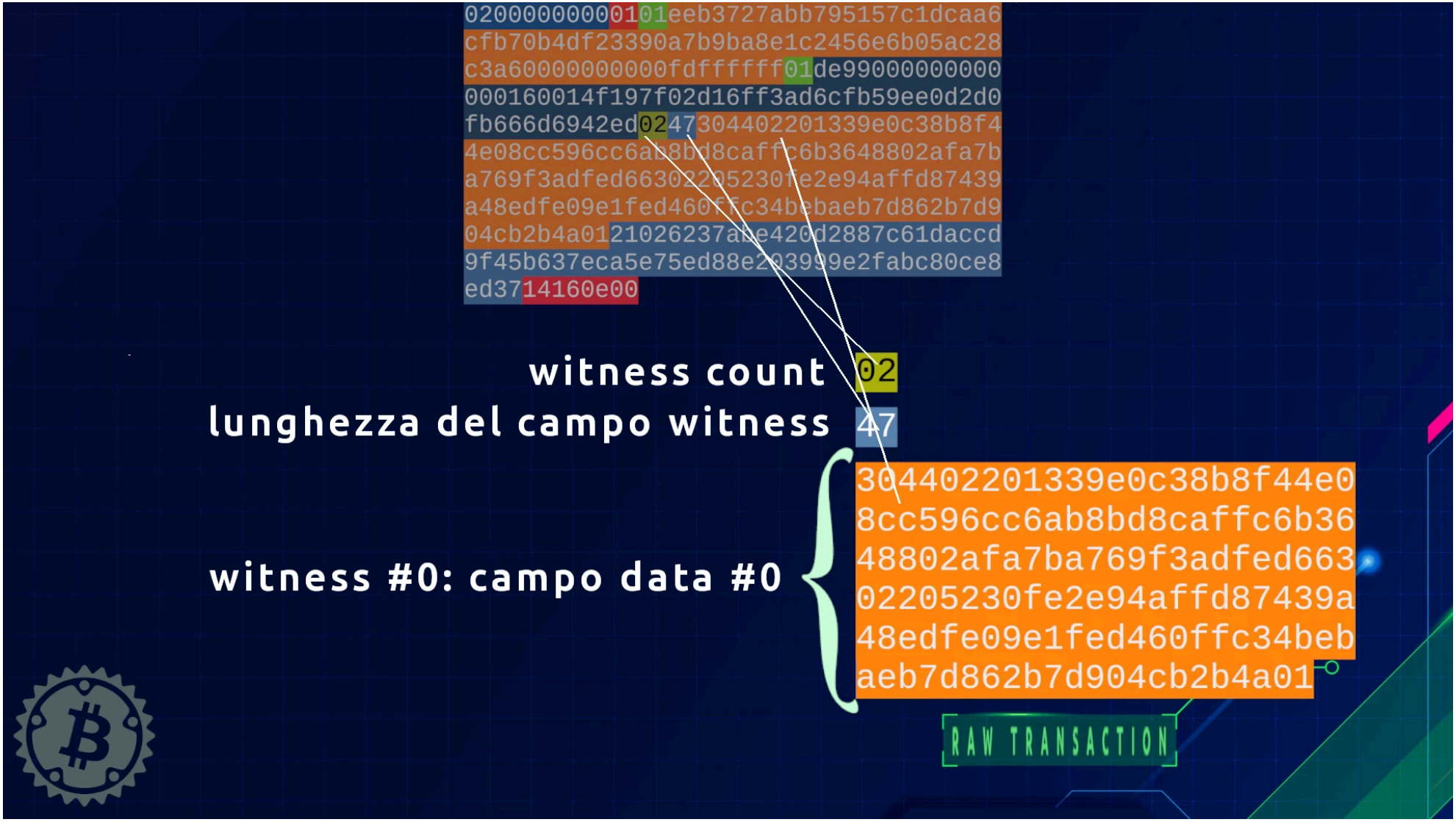

0200000000 01 01 eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a60000000000fdffffff 01 de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022013 39e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
01
Numero tot. degli input
01
Numero tot. degli output
RAW TRANSACTION

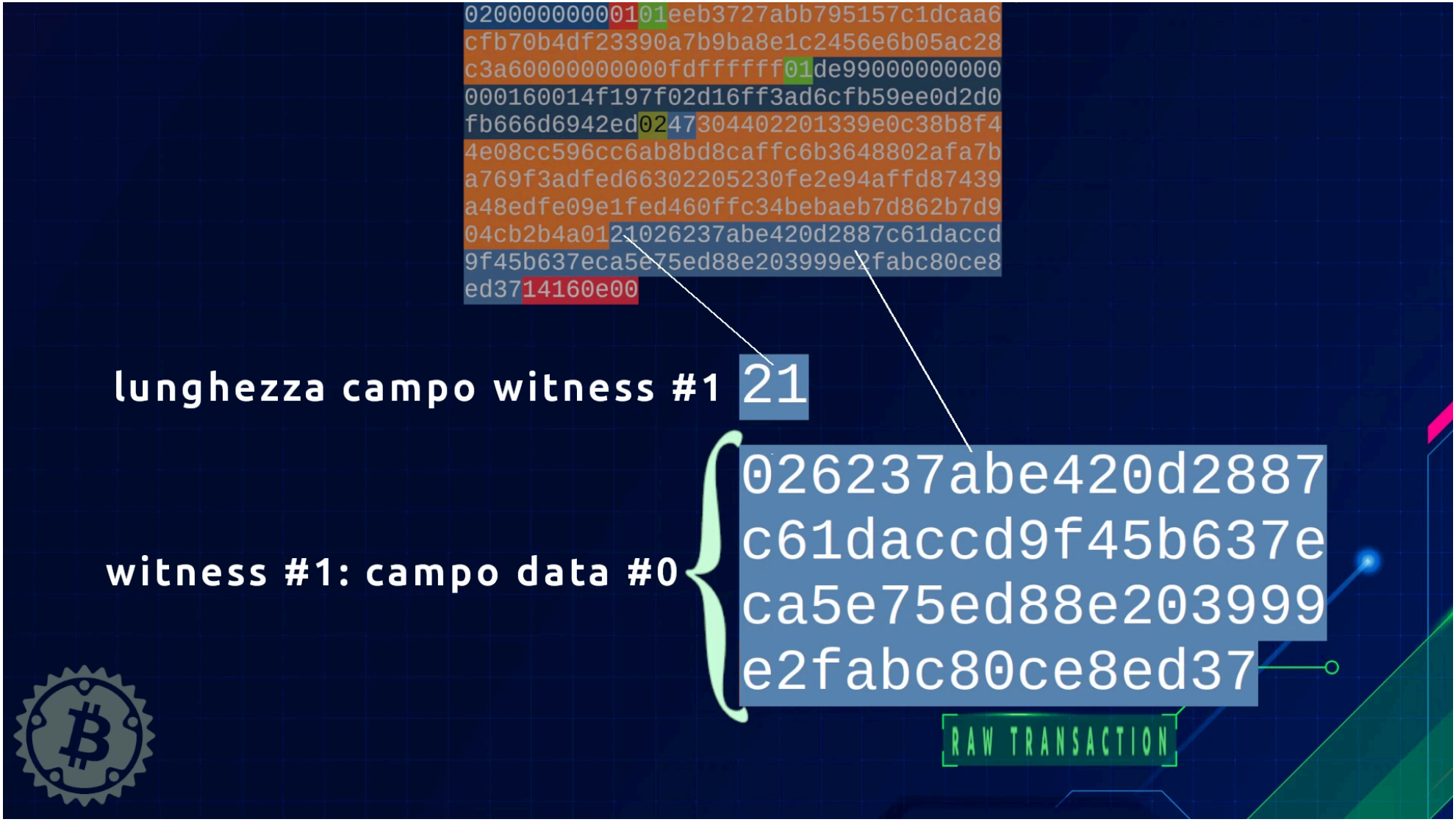
INPUT

- Hash della transazione *parent*
- Index TX della transazione *parent*
- *ScriptSig* (script di sblocco / unlocking)
- *Sequence*




02000000000101eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a6000000000000fdffffff01de99000000000
0001600014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022013 39e0c38b8f4
4e08cc590cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
0f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
eeb3727abb795157c1dcaa
6cfb70b4df23390a7b9ba8
e1c2456e6b05ac28c3a6
input #0: TX ID outpoint
è il TX ID della transazione
parent, reversed
00000000000
TX parent: outpoint index
fdffffff
sequence: segwit
RAW TRANSACTION


02000000000101eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a60000000000fdffffff01de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022013 39e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed6630220523 0fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
witness count
02
lunghezza del campo witness
47
witness #0: campo data #0
304402201339e0c38b8f44e0
8cc596cc6ab8bd8caffc6b36
48802afa7ba769f3adfed663
02205230fe2e94affd87439a
48edfe09e1fed460ffc34beb
aeb7d862b7d904cb2b4a01
RAW TRANSACTION


0200000000010 1eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a60000000000fdffffff01de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022013 39e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
lunghezza campo witness #1 21
witness #1: campo data #0
026237abe420d2887
c61daccd9f45b637e
ca5e75ed88e203999
e2fabc80ce8ed37
RAW TRANSACTION


0200000000010 1eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a60000000000fdffffff01de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022013 39e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
LOCKTIME
14160e00
RAW TRANSACTION


0200000000010 1eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a60000000000fdffffff01de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022 01339e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
Importo: espresso in sats
de9900000000000
Dimensione della nuova ScriptPubKey
16
ScriptPubKey
0014{publickeyhash}
0014f197f02d16ff3ad6cf
b59ee0d2d0fb666d6942ed
RAW TRANSACTION

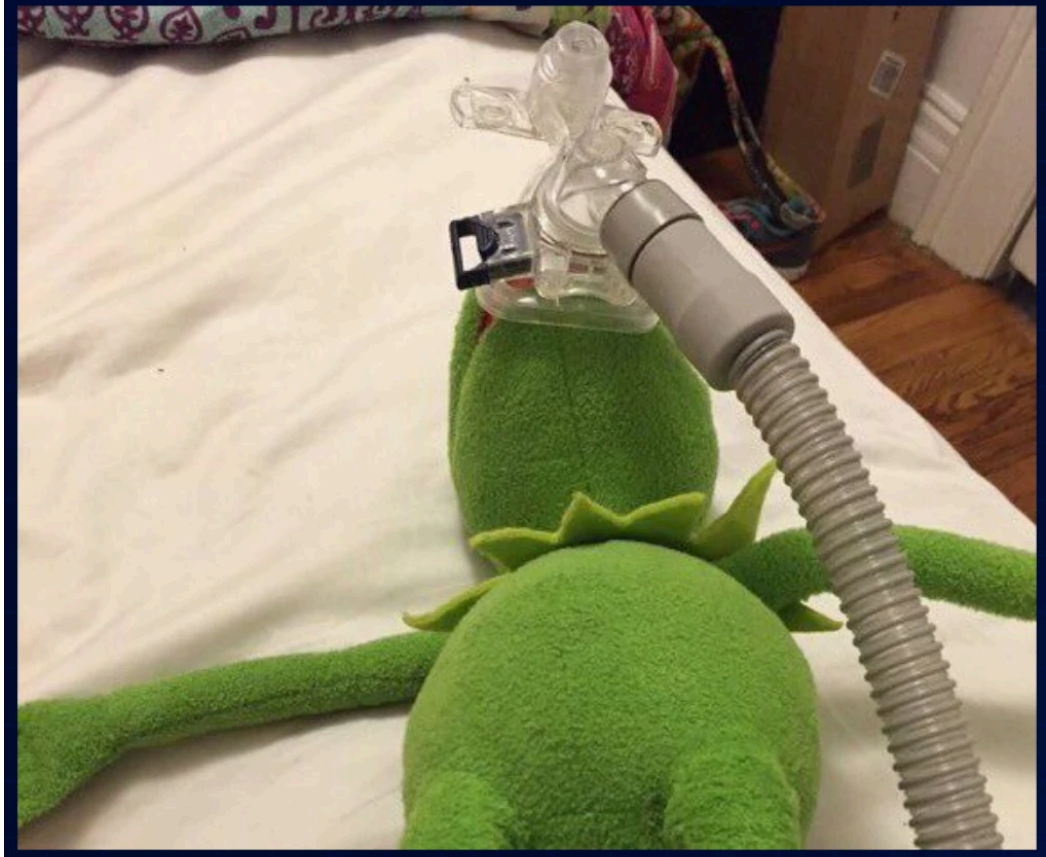

02000000000101eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a60000000000fdffffff01de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed0247304402201339e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
IMPORTO
Campo di 16 byte, che può valere al massimo 0xFFFFFFFFFFFFFFFF
Cioè 18446744073709551615 sats in un solo output.
Equivale a 184.467.440.737,09551615 BTC, che è
ben di più dei 21milioni previsti dal protocollo
RAW TRANSACTION

76a914{publickeyhash}88ac	P2PKH (legacy) - Blocca l'output ad un hash di una chiave pubblica. Per sbloccarlo si deve fornire la chiave pubblica originale e una firma valida
a914{scripthash}87	P2SH (legacy) - Blocca l'output ad un hash di uno script. TPer sbloccarlo si deve fornire lo script originale insieme allo script che soddisfa l'output.
0014{publickeyhash}	P2WPKH - Blocca l'output tall'hash di una pubkey e funziona come P2PKH. Lo script di sblocco, però finisce nel campo witness, anziché nel campo scriptsig.
0020{scripthash}	P2WSH - Blocca l'output all'hash di uno script e funziona come P2SH. Lo script di sblocco, però finisce nel campo witness, anziché nel campo scriptsig.

RAW TRANSACTION


{
"version": "02000000",
"marker": "00",
"flag": "01",
"inputcount": "01",
"inputs": [
{
"txid": "eeb3727abb795157c1dcaa6cfb70b4df23390a7b9ba8e1c2456e6b05ac28c3a6",
"vout": "00000000",
"scriptsigsize": "00",
"scriptsig": "",
"sequence": "fdffffff"
}
],
"outputcount": "01",
"outputs": [
{
"amount": "de99000000000000",
"scriptpubkeysize": "16",
"scriptpubkey": "0014f197f02d16ff3ad6cfb59ee0d2d0fb666d6942ed"
}
],
"witness": [
{
"stackitems": "02",
"0": {
"size": "47",
"item": "304402201339e0c38b8f44e08cc596cc6ab8bd8caffc6b3648802afa7ba769f3adfed66302205
230fe2e94affd87439a48edfe09e1fed460ffc34bebaeb7d862b7d904cb2b4a01"
},
"1": {
"size": "21",
"item": "026237abe420d2887c61daccd9f45b637eca5e75ed88e203999e2fabc80ce8ed37"
}
}
],
"locktime": "14160e00"
}
02000000000101eeb3727abb795157c1dcaa6
cfb70b4df23390a7b9ba8e1c2456e6b05ac28
c3a60000000000fdffffff01de99000000000
000160014f197f02d16ff3ad6cfb59ee0d2d0
fb666d6942ed02473044022013 39e0c38b8f4
4e08cc596cc6ab8bd8caffc6b3648802afa7b
a769f3adfed66302205230fe2e94affd87439
a48edfe09e1fed460ffc34bebaeb7d862b7d9
04cb2b4a0121026237abe420d2887c61daccd
9f45b637eca5e75ed88e203999e2fabc80ce8
ed3714160e00
RAW TRANSACTION

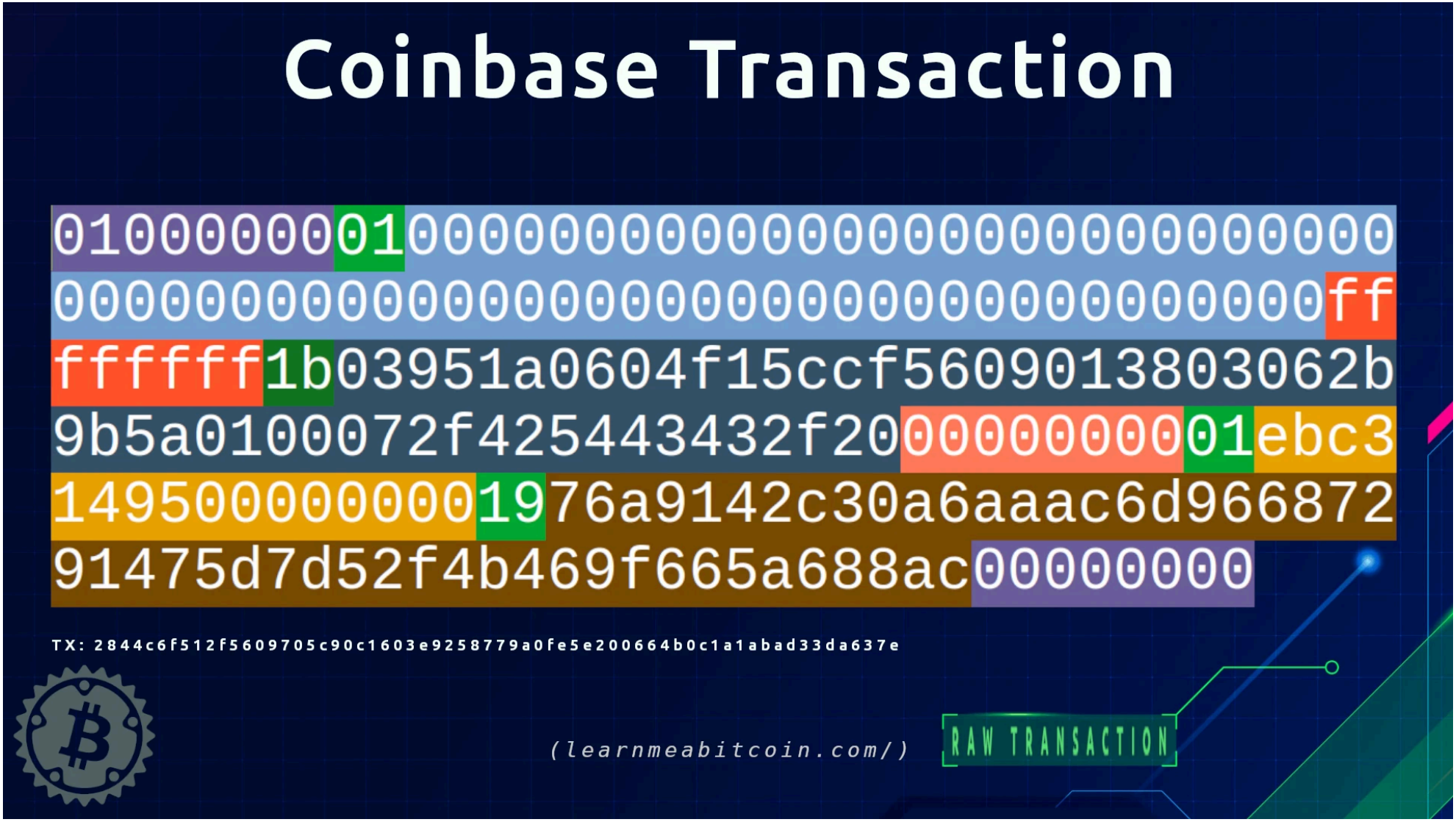
Lo 5t14m0 p3rd3nd0?

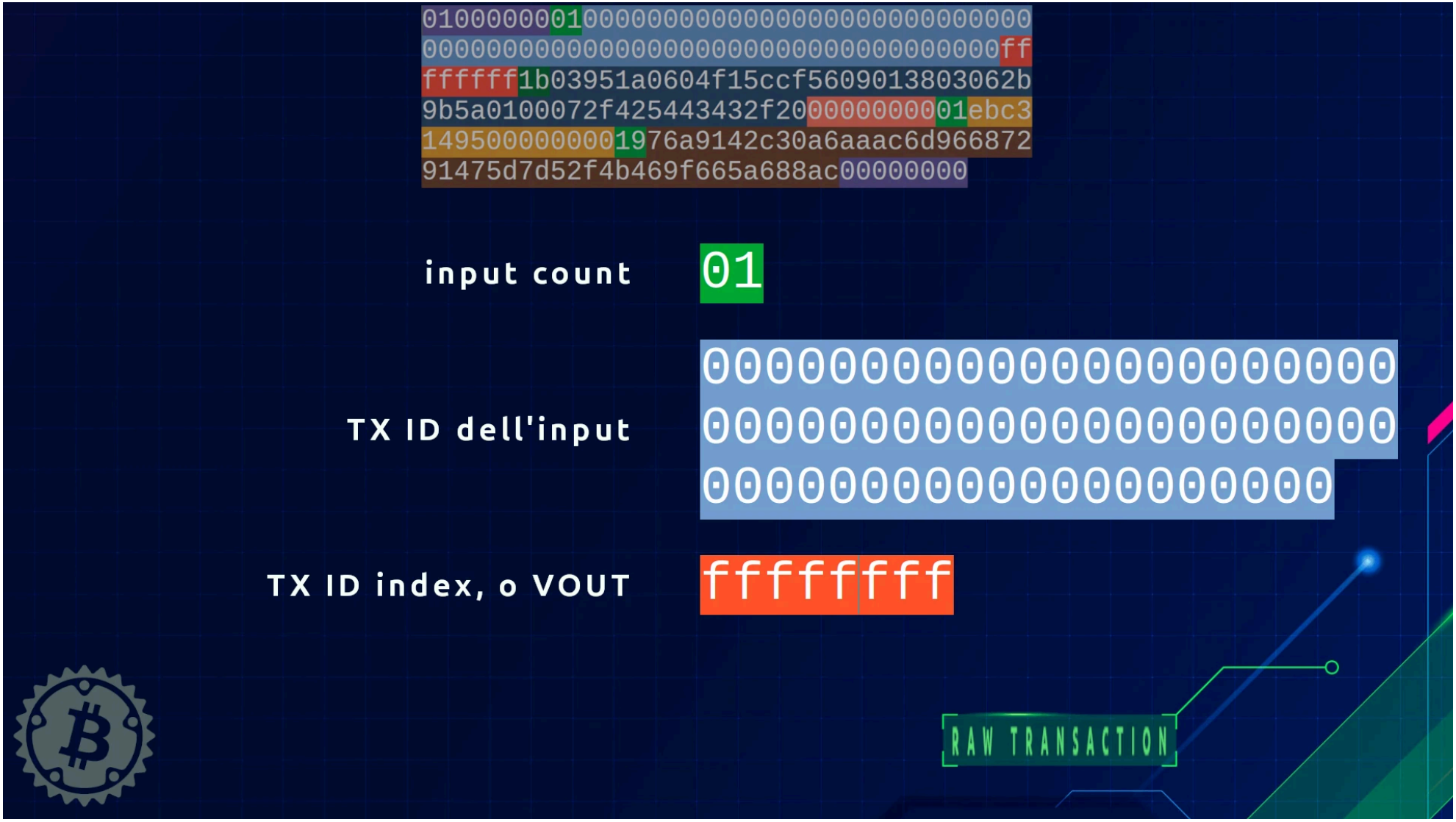


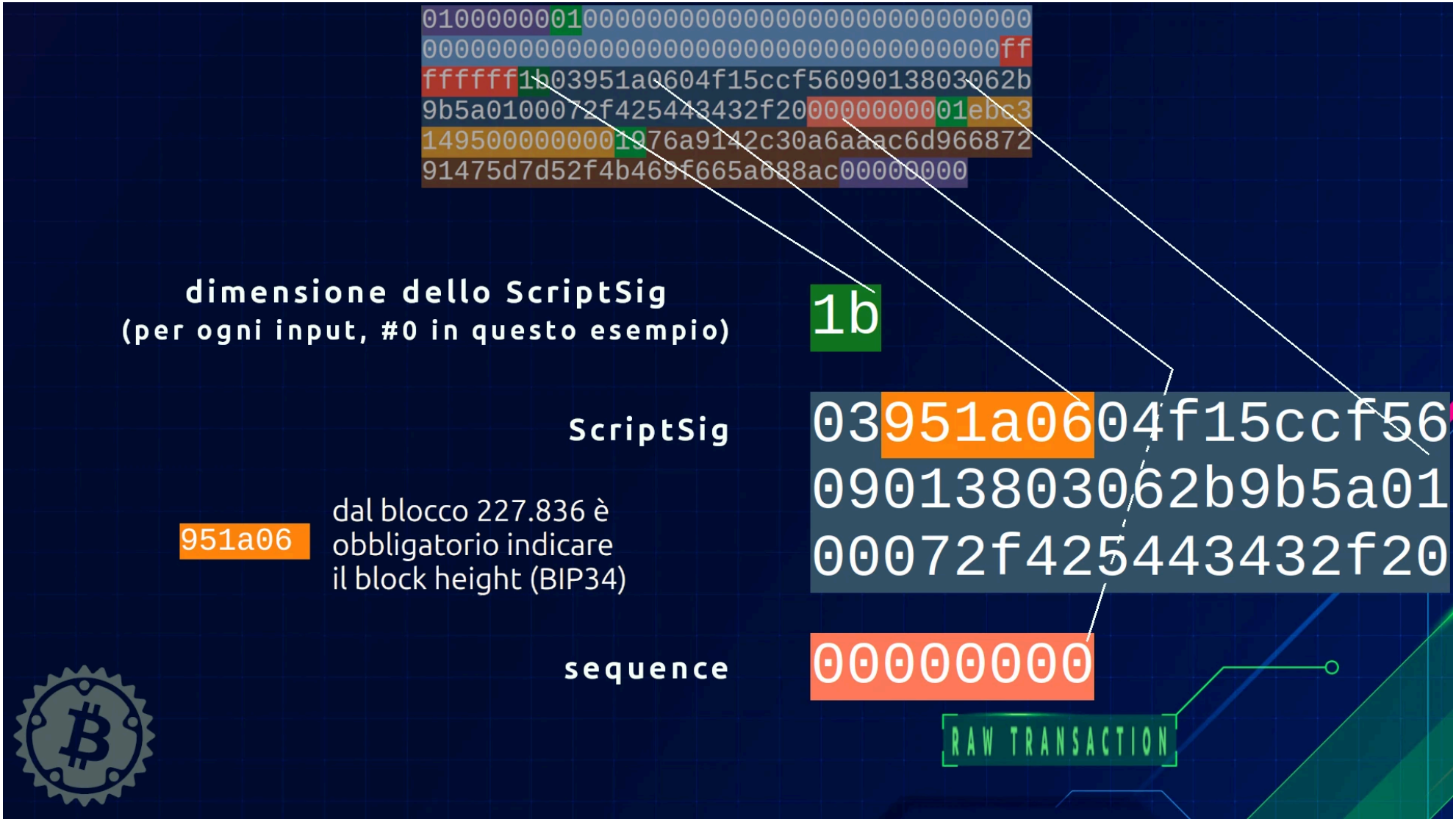
4nc0r4 un 4ltr0 p410 di B45T4RD4T3 c1 st4nn0?

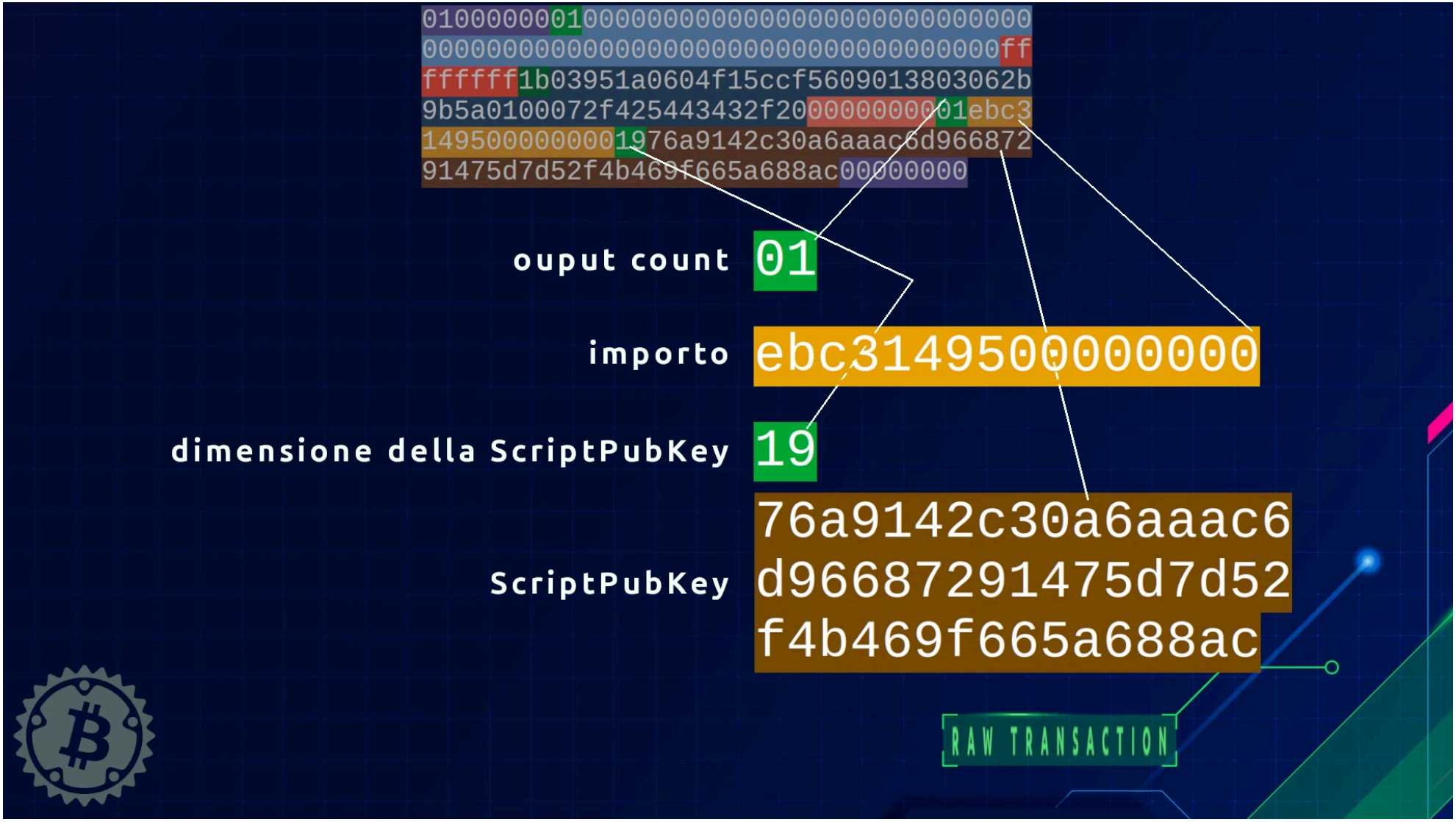
meme

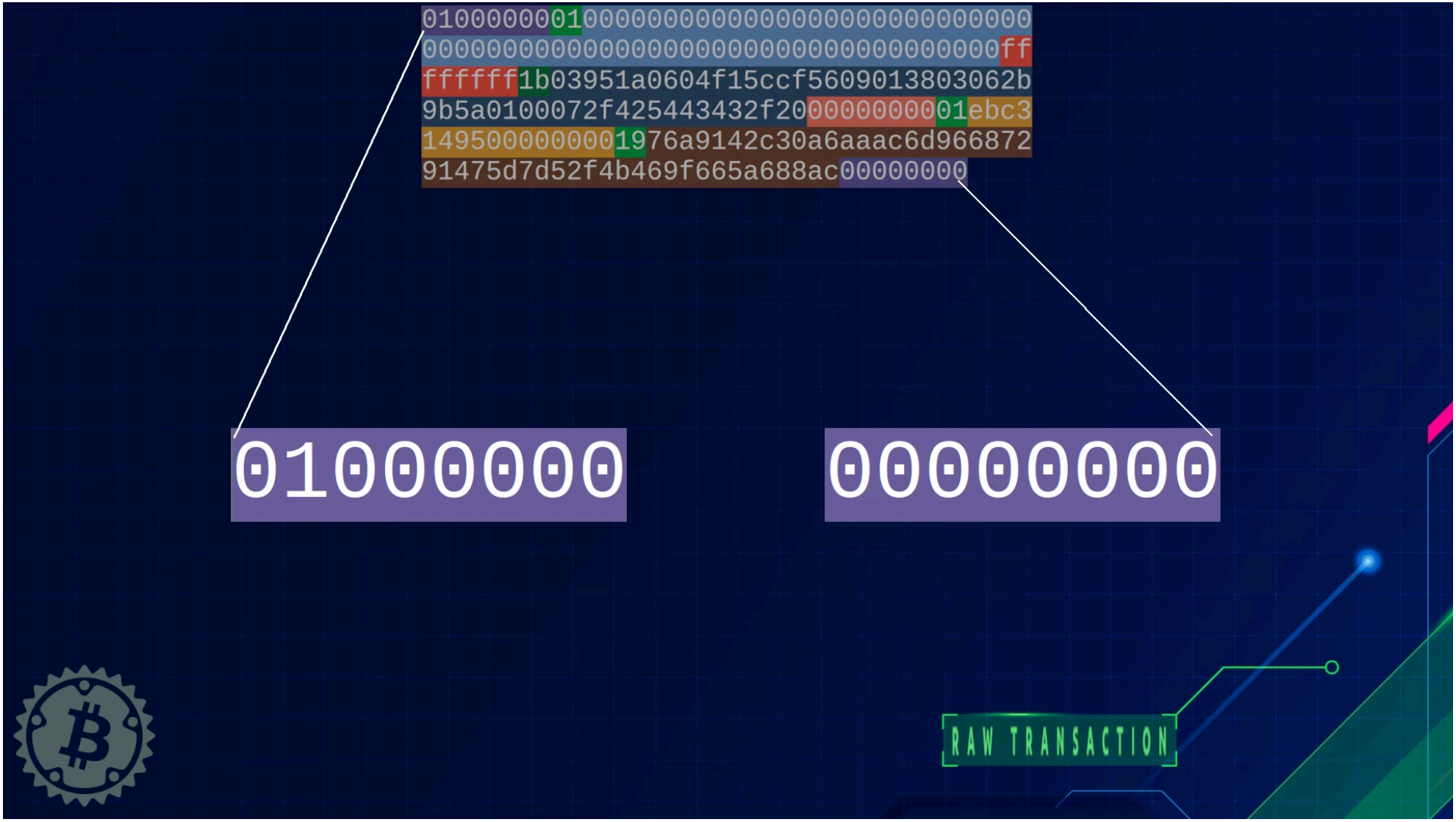
Coinbase Transaction

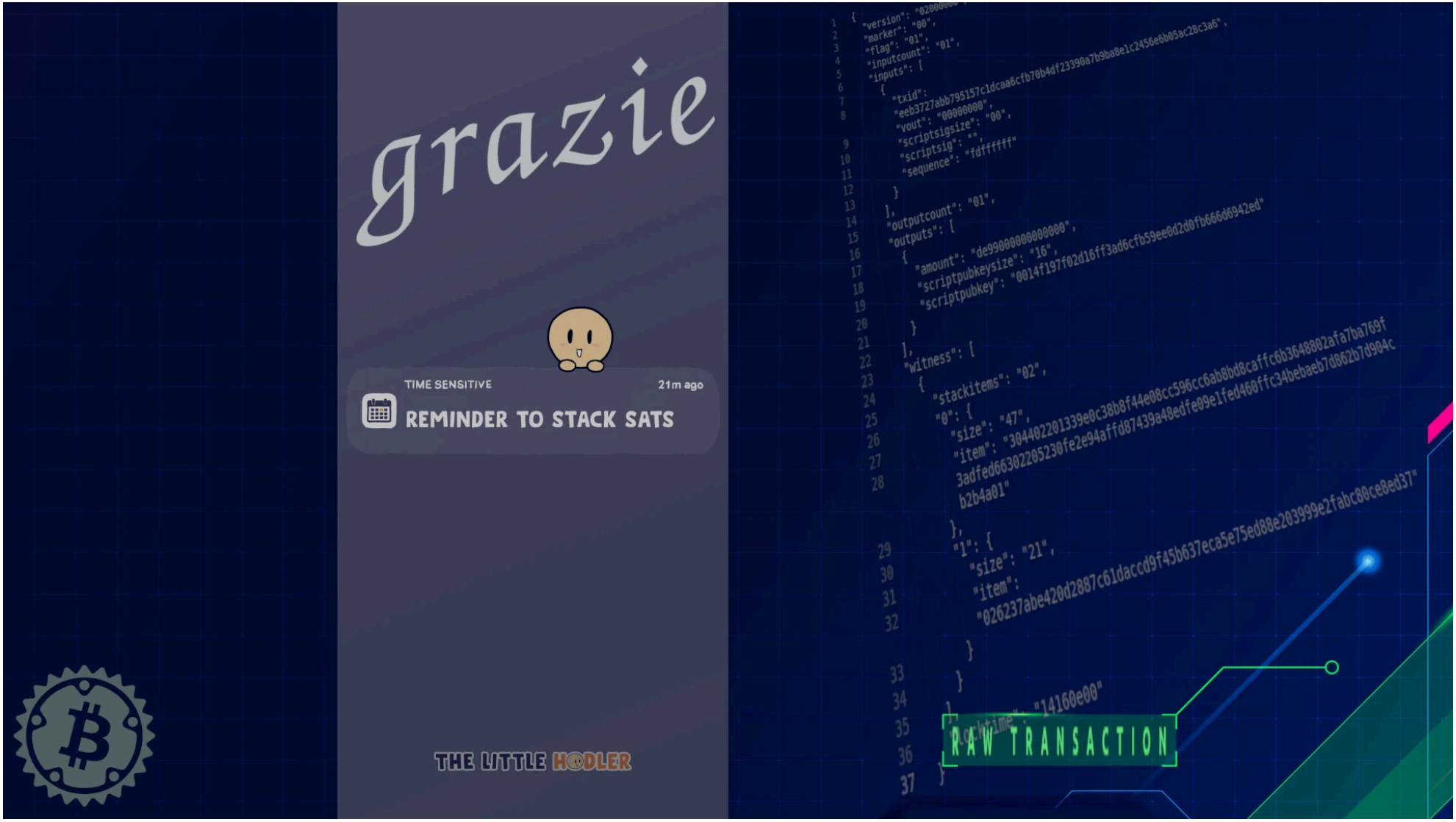



01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff1b03951a0604f15ccf5609013803062b9b5a0100072f425443432f2000000000001ebc3149500000000019 76a9142c30a6aaac6d966872 91475d7d52f4b469f665a688ac00000000
input count
01
TX ID dell'input
0000000000000000000000000000000000000000000000000000000000000000
TX ID index, o VOUT
ffffffff
RAW TRANSACTION


0100000001000000000000000000000000000000
0000000000000000000000000000000000000000ff
ffffff1b03951a0604f15ccf5609013803062b
9b5a0100072f425443432f2000000000 01ebc3
1495000000001976a9142c30a6aaac6d966872
91475d7d52f4b469f665a688ac00000000
dimensione dello ScriptSig
(per ogni input, #0 in questo esempio)
1b
ScriptSig
03951a0604f15ccf56
0901380306 2b9b5a01
00072f425443432f20
951a06
dal blocco 227.836 è
obbligatorio indicare
il block height (BIP34)
sequence
00000000
RAW TRANSACTION


01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff1b03951a0604f15ccf5609013803062b9b5a0100072f425443432f2000000000 01ebc3149500000000 1976a9142c30a6aaac6d96687291475d7d52f4b469f665a688ac00000000
ouput count
01
importo
ebc3149500000000
dimensione della ScriptPubKey
19
ScriptPubKey
76a9142c30a6aaac6d96687291475d7d52f4b469f665a688ac
RAW TRANSACTION


01000000010000000000000000000000000000000000000000000000000000000000000000ffffffff1b03951a0604f15ccf5609013803062b9b5a0100072f425443432f2000000000001ebc3149500000000019 76a9142c30a6aaac6d966872 91475d7d52f4b469f665a688ac00000000
01000000
00000000
RAW TRANSACTION


grazie
TIME SENSITIVE
21m ago
REMINDER TO STACK SATS
THE LITTLE HODLER
{
"version": "02000000",
"marker": "00",
"flag": "01",
"inputcount": "01",
"inputs": [
{
"txid":
"eeb3727abb795157c1dcaa6cfb70b4df23390a7b9ba8e1c2456e6b05ac28c3a6",
"vout": "00000000",
"scriptsigsize": "00",
"scriptsig": "",
"sequence": "fdffffff"
}
],
"outputcount": "01",
"outputs": [
{
"amount": "de99000000000000",
"scriptpubkeysize": "16",
"scriptpubkey": "0014f197f02d16ff3ad6cfb59ee0d2d0fb666d6942ed"
}
],
"witness": [
{
"stackitems": "02",
"0": {
"size": "47",
"item": "304402201339e0c38b8f44e08cc596cc6ab8bd8caffc6b3648802afa7ba769f
3adfed66302205230fe2e94affd87439a48edfe09e1fed460ffc34bebaeb7d862b7d904c
b2b4a01"
},
"1": {
"size": "21",
"item":
"026237abe420d2887c61daccd9f45b637eca5e75ed88e203999e2fabc80ce8ed37"
}
}
"locktime": "14160e00"
}
RAW TRANSACTION