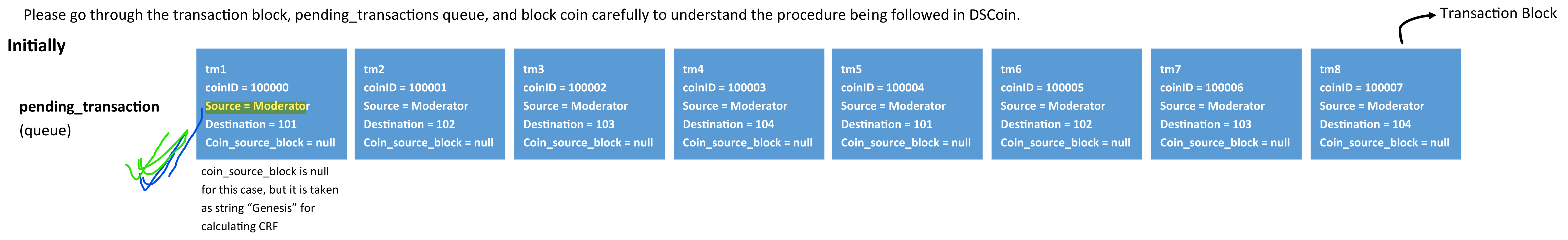
DSCoin_Honest Example:

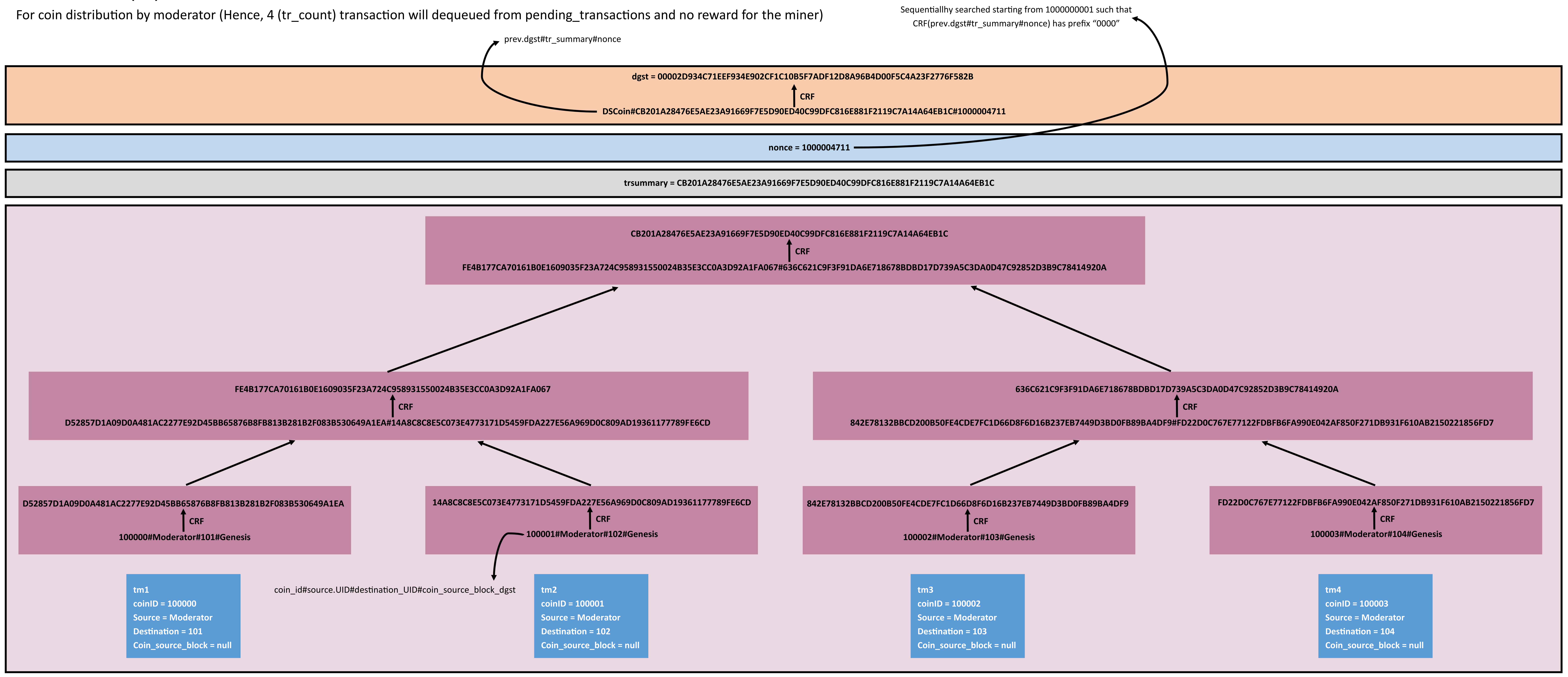
- Let us assume that, there are 4 members in our DSCoin example with UID's 101. 102, 103, and 104 respectively.
- Let the tr_count is set to be 4 in this example.
- Initially, the moderator distributes 2 coins to each member. And hence, a total of 2 Transaction Blocks are created in order to distribute the coins to the user. These 2 transaction blocks are created by the moderator and hence, no rewards are allotted for mining these transaction blocks namely, tb1 and tb2.
- Say, tm1, tm2, …. tm8 are the transactions for distributing the initial coins to the members.
- Please go through the transaction block, pending_transactions queue, and block coin carefully to understand the procedure being followed in DSCoin.



Transaction Block
Initially
pending_transaction (queue)
tm1 coinID = 100000 Source = Moderator Destination = 101 Coin_source_block = null
tm2 coinID = 100001 Source = Moderator Destination = 102 Coin_source_block = null
tm3 coinID = 100002 Source = Moderator Destination = 103 Coin_source_block = null
tm4 coinID = 100003 Source = Moderator Destination = 104 Coin_source_block = null
tm5 coinID = 100004 Source = Moderator Destination = 101 Coin_source_block = null
tm6 coinID = 100005 Source = Moderator Destination = 102 Coin_source_block = null
tm7 coinID = 100006 Source = Moderator Destination = 103 Coin_source_block = null
tm8 coinID = 100007 Source = Moderator Destination = 104 Coin_source_block = null
coin_source_block is null for this case, but it is taken as string "Genesis" for calculating CRF

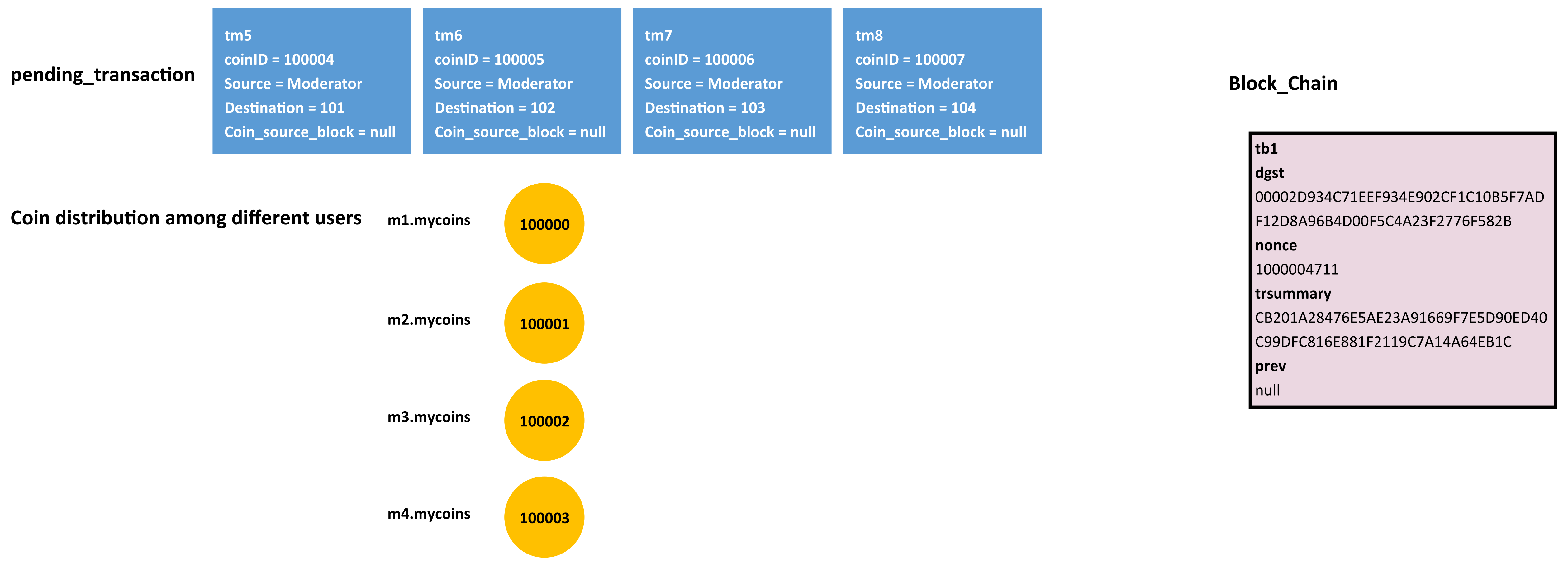
TransactionBlock 1 (tb1):

For coin distribution by moderator (Hence, 4 (tr_count) transaction will dequeued from pending_transactions and no reward for the miner)



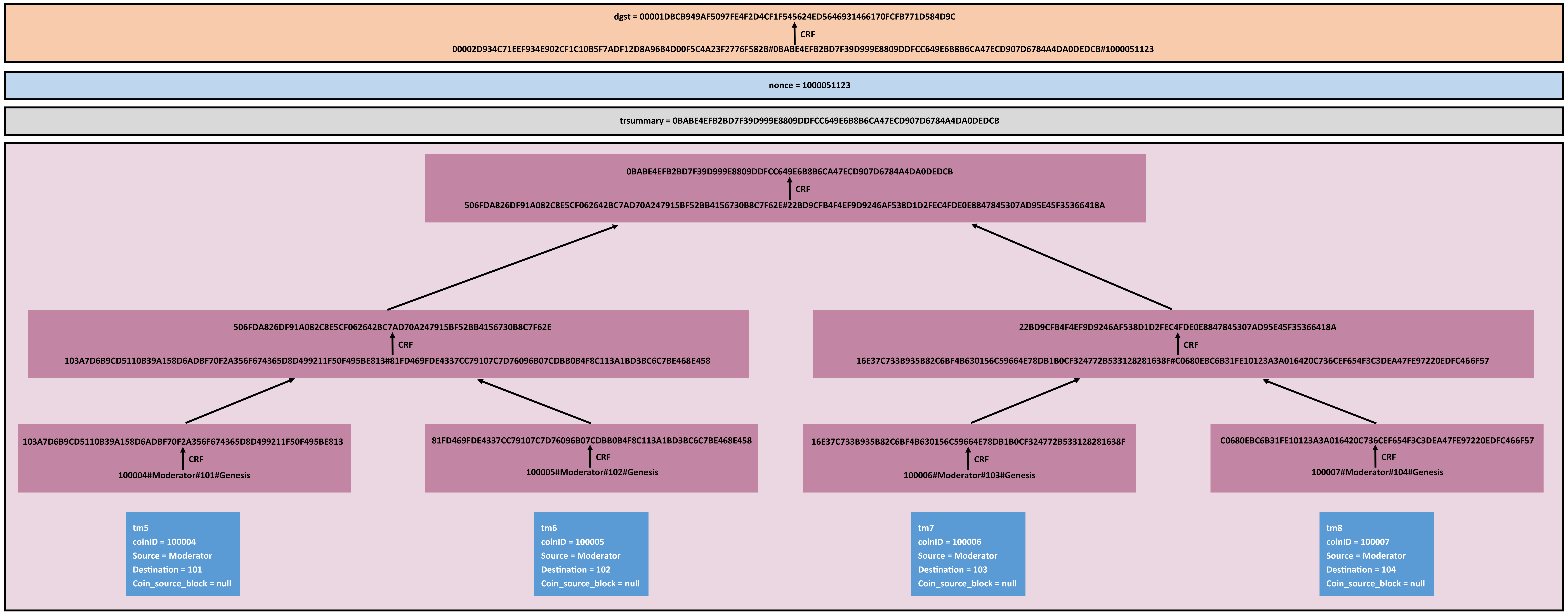
Sequentiallhy searched starting from 1000000001 such that CRF(prev.dgst#tr_summary#nonce) has prefix "0000"
prev.dgst#tr_summary#nonce
dgst = 00002D934C71EEF934E902CF1C10B5F7ADF12D8A96B4D00F5C4A23F2776F582B
CRF
DSCoin#CB201A28476E5AE23A91669F7E5D90ED40C99DFC816E881F2119C7A14A64EB1C#1000004711
nonce = 1000004711
trsummary = CB201A28476E5AE23A91669F7E5D90ED40C99DFC816E881F2119C7A14A64EB1C
CB201A28476E5AE23A91669F7E5D90ED40C99DFC816E881F2119C7A14A64EB1C
CRF
FE4B177CA70161B0E1609035F23A724C958931550024B35E3CC0A3D92A1FA067#636C621C9F3F91DA6E718678BDBD17D739A5C3DA0D47C92852D3B9C78414920A
FE4B177CA70161B0E1609035F23A724C958931550024B35E3CC0A3D92A1FA067
CRF
D52857D1A09D0A481AC2277E92D45BB65876B8FB813B281B2F083B530649A1EA#14A8C8C8E5C073E4773171D5459FDA227E56A969D0C809AD19361177789FE6CD
636C621C9F3F91DA6E718678BDBD17D739A5C3DA0D47C92852D3B9C78414920A
CRF
842E78132BBCD200B50FE4CDE7FC1D66D8F6D16B237EB7449D3BD0FB89BA4DF9#FD22D0C767E77122FDBFB6FA990E042AF850F271DB931F610AB2150221856FD7
D52857D1A09D0A481AC2277E92D45BB65876B8FB813B281B2F083B530649A1EA
CRF
100000#Moderator#101#Genesis
14A8C8C8E5C073E4773171D5459FDA227E56A969D0C809AD19361177789FE6CD
CRF
100001#Moderator#102#Genesis
842E78132BBCD200B50FE4CDE7FC1D66D8F6D16B237EB7449D3BD0FB89BA4DF9
CRF
100002#Moderator#103#Genesis
FD22D0C767E77122FDBFB6FA990E042AF850F271DB931F610AB2150221856FD7
CRF
100003#Moderator#104#Genesis
coin_id#source.UID#destination_UID#coin_source_block_dgst
tm1 coinID = 100000 Source = Moderator Destination = 101 Coin_source_block = null
tm2 coinID = 100001 Source = Moderator Destination = 102 Coin_source_block = null
tm3 coinID = 100002 Source = Moderator Destination = 103 Coin_source_block = null
tm4 coinID = 100003 Source = Moderator Destination = 104 Coin_source_block = null

After creation and insertion of tb1 in block_chain

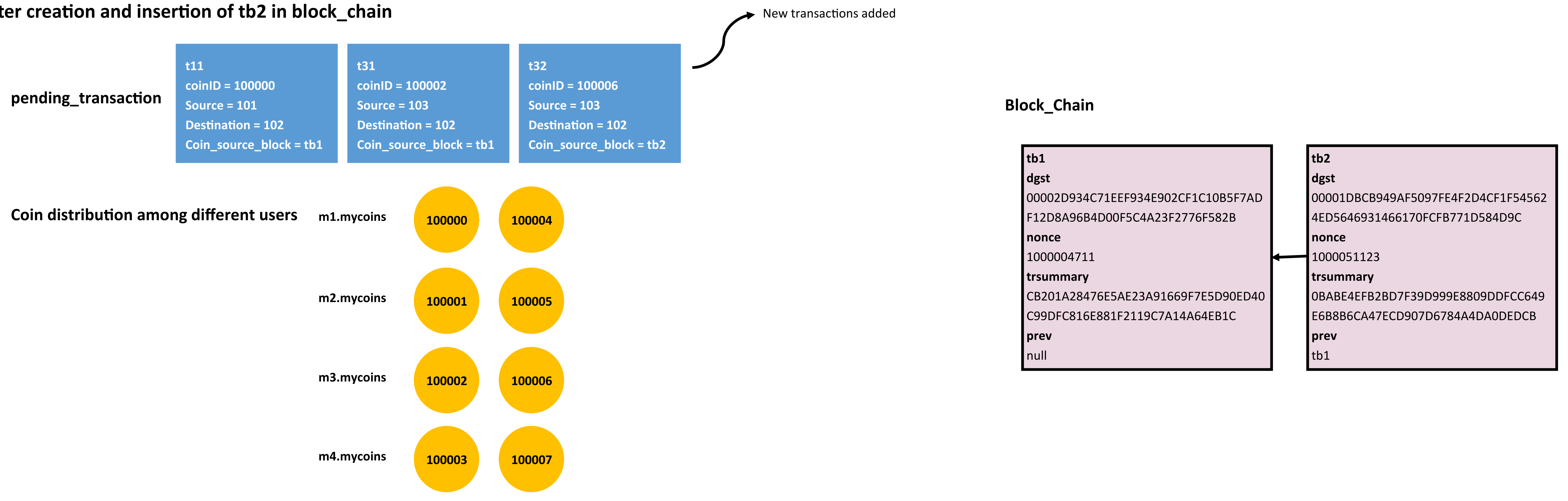


TransactionBlock 2 (tb2):

For coin distribution by moderator (Hence, 4 (tr_count) transaction will dequeued from pending_transactions and no reward for the miner)

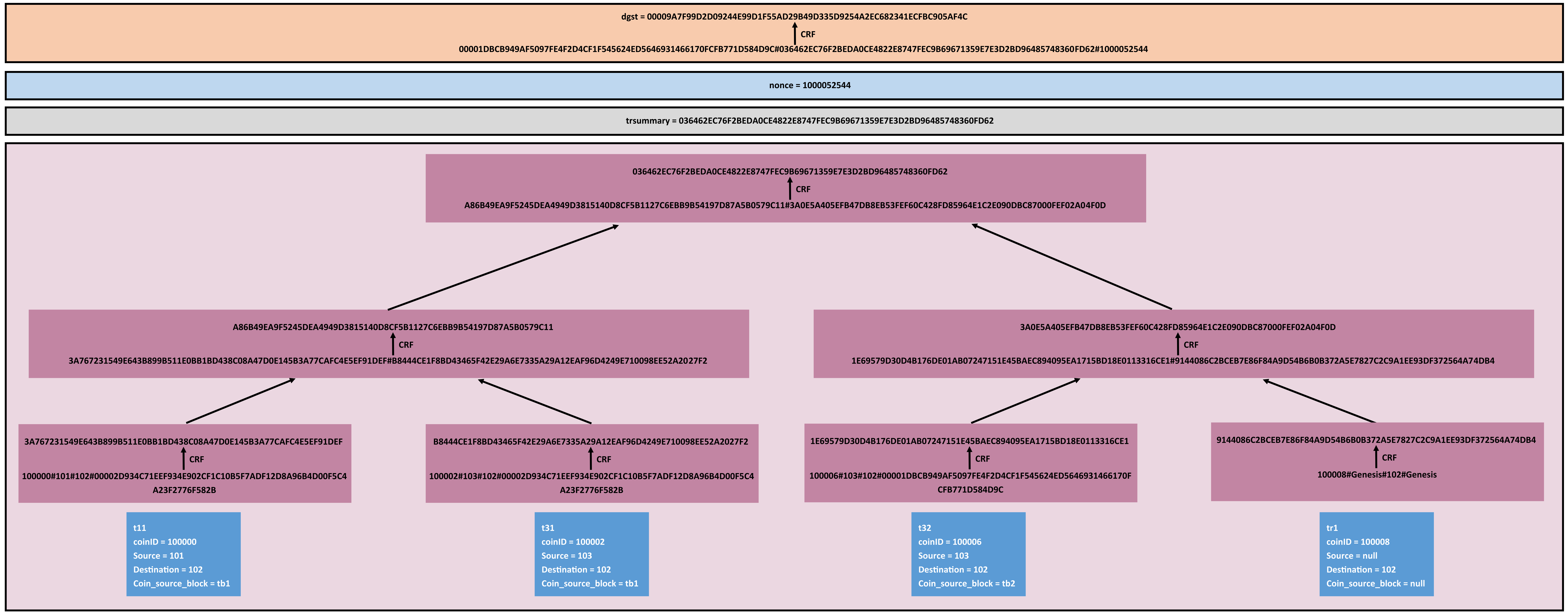

dgst = 00001DBCB949AF5097FE4F2D4CF1F545624ED5646931466170FCFB771D584D9C
CRF
00002D934C71EEF934E902CF1C10B5F7ADF12D8A96B4D00F5C4A23F2776F582B#0BABE4EFB2BD7F39D999E8809DDFCC649E6B8B6CA47ECD907D6784A4DA0DEDCB#1000051123
nonce = 1000051123
trsummary = 0BABE4EFB2BD7F39D999E8809DDFCC649E6B8B6CA47ECD907D6784A4DA0DEDCB
0BABE4EFB2BD7F39D999E8809DDFCC649E6B8B6CA47ECD907D6784A4DA0DEDCB
CRF
506FDA826DF91A082C8E5CF062642BC7AD70A247915BF52BB4156730B8C7F62E#22BD9CFB4F4EF9D9246AF538D1D2FEC4FDE0E8847845307AD95E45F35366418A
506FDA826DF91A082C8E5CF062642BC7AD70A247915BF52BB4156730B8C7F62E
CRF
103A7D6B9CD5110B39A158D6ADBF70F2A356F674365D8D499211F50F495BE813#81FD469FDE4337CC79107C7D76096B07CDBB0B4F8C113A1BD3BC6C7BE468E458
22BD9CFB4F4EF9D9246AF538D1D2FEC4FDE0E8847845307AD95E45F35366418A
CRF
16E37C733B935B82C6BF4B630156C59664E78DB1B0CF324772B533128281638F#C0680EBC6B31FE10123A3A016420C736CEF654F3C3DEA47FE97220EDFC466F57
103A7D6B9CD5110B39A158D6ADBF70F2A356F674365D8D499211F50F495BE813
CRF
100004#Moderator#101#Genesis
81FD469FDE4337CC79107C7D76096B07CDBB0B4F8C113A1BD3BC6C7BE468E458
CRF
100005#Moderator#102#Genesis
16E37C733B935B82C6BF4B630156C59664E78DB1B0CF324772B533128281638F
CRF
100006#Moderator#103#Genesis
C0680EBC6B31FE10123A3A016420C736CEF654F3C3DEA47FE97220EDFC466F57
CRF
100007#Moderator#104#Genesis
tm5
coinID = 100004
Source = Moderator
Destination = 101
Coin_source_block = null
tm6
coinID = 100005
Source = Moderator
Destination = 102
Coin_source_block = null
tm7
coinID = 100006
Source = Moderator
Destination = 103
Coin_source_block = null
tm8
coinID = 100007
Source = Moderator
Destination = 104
Coin_source_block = null

After creation and insertion of tb2 in block_chain

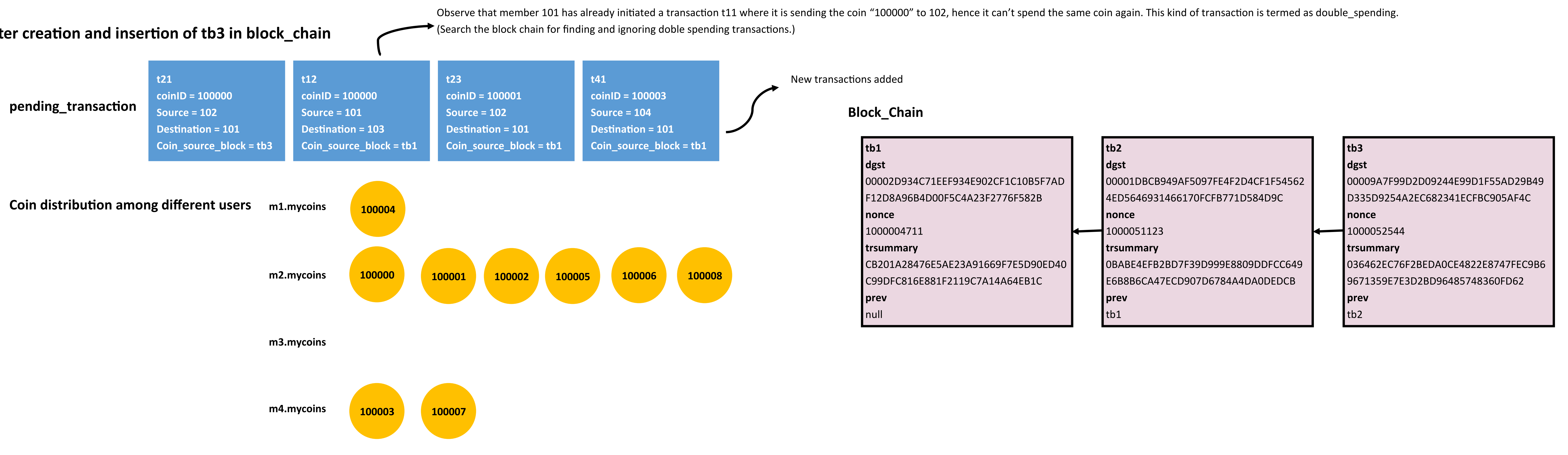


TransactionBlock 3 (tb3): (Mined by m2 (UID: 102))

Mined by a member, hence 3 (tr_count – 1) number of transactions are dequeued from the pending_tranasctions and a transaction for reward for miner is added to the block


dgst = 00009A7F99D2D09244E99D1F55AD29B49D335D9254A2EC682341ECFBC905AF4C
CRF
00001DBCB949AF5097FE4F2D4CF1F545624ED5646931466170FCFB771D584D9C#036462EC76F2BEDA0CE4822E8747FEC9B69671359E7E3D2BD96485748360FD62#1000052544
nonce = 1000052544
trsummary = 036462EC76F2BEDA0CE4822E8747FEC9B69671359E7E3D2BD96485748360FD62
036462EC76F2BEDA0CE4822E8747FEC9B69671359E7E3D2BD96485748360FD62
CRF
A86B49EA9F5245DEA4949D3815140D8CF5B1127C6EBB9B54197D87A5B0579C11#3A0E5A405EFB47DB8EB53FEF60C428FD85964E1C2E090DBC87000FEF02A04F0D
A86B49EA9F5245DEA4949D3815140D8CF5B1127C6EBB9B54197D87A5B0579C11
CRF
3A767231549E643B899B511E0BB1BD438C08A47D0E145B3A77CAFC4E5EF91DEF#B8444CE1F8BD43465F42E29A6E7335A29A12EAF96D4249E710098EE52A2027F2
3A0E5A405EFB47DB8EB53FEF60C428FD85964E1C2E090DBC87000FEF02A04F0D
CRF
1E69579D30D4B176DE01AB07247151E45BAEC894095EA1715BD18E0113316CE1#9144086C2BCEB7E86F84A9D54B6B0B372A5E7827C2C9A1EE93DF372564A74DB4
3A767231549E643B899B511E0BB1BD438C08A47D0E145B3A77CAFC4E5EF91DEF
CRF
100000#101#102#00002D934C71EEF934E902CF1C10B5F7ADF12D8A96B4D00F5C4
A23F2776F582B
B8444CE1F8BD43465F42E29A6E7335A29A12EAF96D4249E710098EE52A2027F2
CRF
100002#103#102#00002D934C71EEF934E902CF1C10B5F7ADF12D8A96B4D00F5C4
A23F2776F582B
1E69579D30D4B176DE01AB07247151E45BAEC894095EA1715BD18E0113316CE1
CRF
100006#103#102#00001DBCB949AF5097FE4F2D4CF1F545624ED5646931466170F
CFB771D584D9C
9144086C2BCEB7E86F84A9D54B6B0B372A5E7827C2C9A1EE93DF372564A74DB4
CRF
100008#Genesis#102#Genesis
t11
coinID = 100000
Source = 101
Destination = 102
Coin_source_block = tb1
t31
coinID = 100002
Source = 103
Destination = 102
Coin_source_block = tb1
t32
coinID = 100006
Source = 103
Destination = 102
Coin_source_block = tb2
tr1
coinID = 100008
Source = null
Destination = 102
Coin_source_block = null

After creation and insertion of tb3 in block_chain



Observe that member 101 has already initiated a transaction t11 where it is sending the coin “100000” to 102, hence it can’t spend the same coin again. This kind of transaction is termed as double_spending.
(Search the block chain for finding and ignoring doble spending transactions.)

pending_transaction

t21	t12	t23	t41
coinID = 100000	coinID = 100000	coinID = 100001	coinID = 100003
Source = 102	Source = 101	Source = 102	Source = 104
Destination = 101	Destination = 103	Destination = 101	Destination = 101
Coin_source_block = tb3	Coin_source_block = tb1	Coin_source_block = tb1	Coin_source_block = tb1

New transactions added

Coin distribution among different users

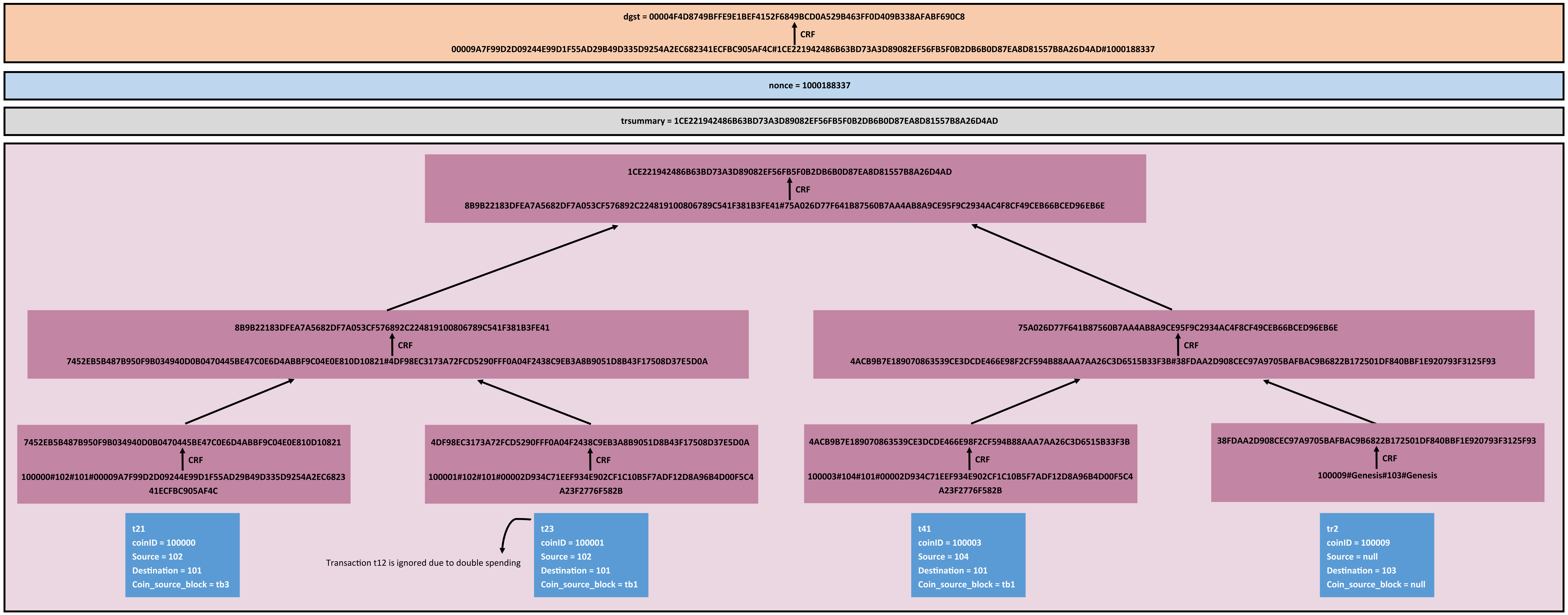
m1.mycoins	100004					
m2.mycoins	100000	100001	100002	100005	100006	100008
m3.mycoins						
m4.mycoins	100003	100007				

Block_Chain

tb1	tb2	tb3
dgst	**dgst**	**dgst**
00002D934C71EEF934E902CF1C10B5F7AD	00001DBCB949AF5097FE4F2D4CF1F54562	00009A7F99D2D09244E99D1F55AD29B49
F12D8A96B4D00F5C4A23F2776F582B	4ED5646931466170FCFB771D584D9C	D335D9254A2EC682341ECFBC905AF4C
nonce	**nonce**	**nonce**
1000004711	1000051123	1000052544
trsummary	**trsummary**	**trsummary**
CB201A28476E5AE23A91669F7E5D90ED40	0BABE4EFB2BD7F39D999E8809DDFCC649	036462EC76F2BEDA0CE4822E8747FEC9B6
C99DFC816E881F2119C7A14A64EB1C	E6B8B6CA47ECD907D6784A4DA0DEDCB	9671359E7E3D2BD96485748360FD62
prev	**prev**	**prev**
null	tb1	tb2

TransactionBlock 4 (tb4): (Mined by m3 (UID: 103))

Mined by a member, hence 3 (tr_count – 1) number of transactions are dequeued from the pending_tranasctions and a transaction for reward for miner is added to the block



dgst = 00004F4D8749BFFE9E1BEF4152F6849BCD0A529B463FF0D409B338AFABF690C8

CRF

00009A7F99D2D09244E99D1F55AD29B49D335D9254A2EC682341ECFBC905AF4C#1CE221942486B63BD73A3D89082EF56FB5F0B2DB6B0D87EA8D81557B8A26D4AD#1000188337

nonce = 1000188337

trsummary = 1CE221942486B63BD73A3D89082EF56FB5F0B2DB6B0D87EA8D81557B8A26D4AD

1CE221942486B63BD73A3D89082EF56FB5F0B2DB6B0D87EA8D81557B8A26D4AD

CRF

8B9B22183DFEA7A5682DF7A053CF576892C224819100806789C541F381B3FE41#75A026D77F641B87560B7AA4AB8A9CE95F9C2934AC4F8CF49CEB66BCED96EB6E

8B9B22183DFEA7A5682DF7A053CF576892C224819100806789C541F381B3FE41

CRF

7452EB5B487B950F9B034940D0B0470445BE47C0E6D4ABBF9C04E0E810D10821#4DF98EC3173A72FCD5290FFF0A04F2438C9EB3A8B9051D8B43F17508D37E5D0A

75A026D77F641B87560B7AA4AB8A9CE95F9C2934AC4F8CF49CEB66BCED96EB6E

CRF

4ACB9B7E189070863539CE3DCDE466E98F2CF594B88AAA7AA26C3D6515B33F3B#38FDAA2D908CEC97A9705BAFBAC9B6822B172501DF840BBF1E920793F3125F93

7452EB5B487B950F9B034940D0B0470445BE47C0E6D4ABBF9C04E0E810D10821

CRF

100000#102#101#00009A7F99D2D09244E99D1F55AD29B49D335D9254A2EC6823
41ECFBC905AF4C

4DF98EC3173A72FCD5290FFF0A04F2438C9EB3A8B9051D8B43F17508D37E5D0A

CRF

100001#102#101#00002D934C71EEF934E902CF1C10B5F7ADF12D8A96B4D00F5C4
A23F2776F582B

4ACB9B7E189070863539CE3DCDE466E98F2CF594B88AAA7AA26C3D6515B33F3B

CRF

100003#104#101#00002D934C71EEF934E902CF1C10B5F7ADF12D8A96B4D00F5C4
A23F2776F582B

38FDAA2D908CEC97A9705BAFBAC9B6822B172501DF840BBF1E920793F3125F93

CRF

100009#Genesis#103#Genesis

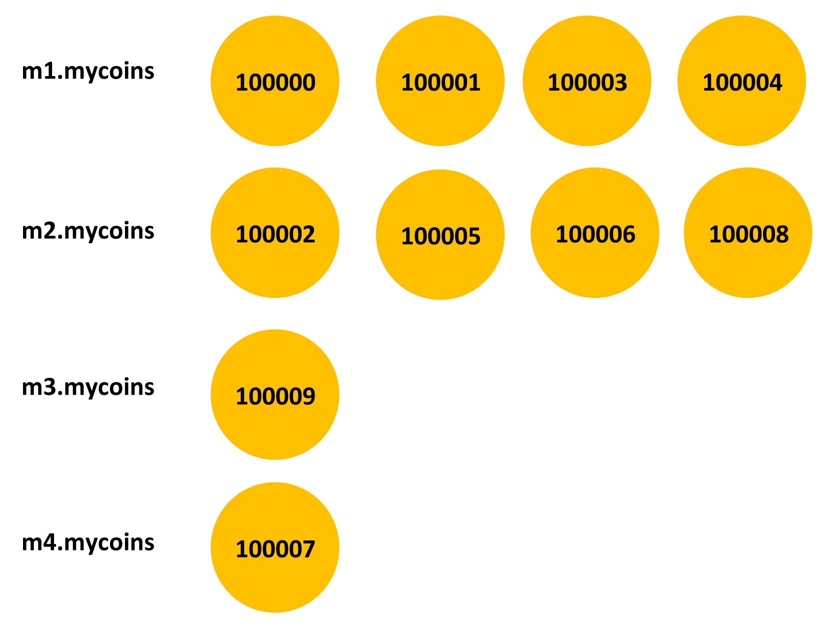
t21	t23	t41	tr2
coinID = 100000	coinID = 100001	coinID = 100003	coinID = 100009
Source = 102	Source = 102	Source = 104	Source = null
Destination = 101	Destination = 101	Destination = 101	Destination = 103
Coin_source_block = tb3	Coin_source_block = tb1	Coin_source_block = tb1	Coin_source_block = null

Transaction t12 is ignored due to double spending

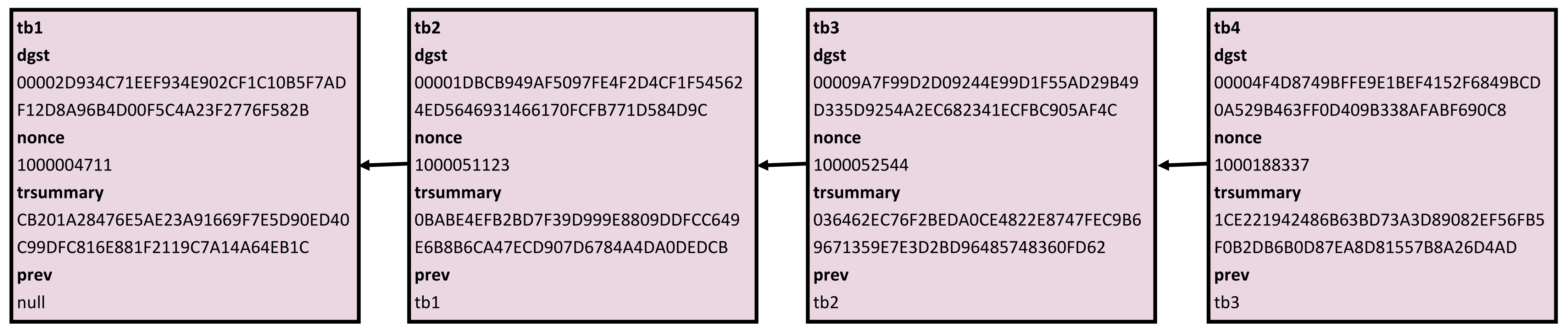
After creation and insertion of tb4 in block_chain

pending_transaction (empty queue)

Coin distribution among different users



Block_Chain



tb1
dgst
00002D934C71EEF934E902CF1C10B5F7AD
F12D8A96B4D00F5C4A23F2776F582B
nonce
1000004711
trsummary
CB201A28476E5AE23A91669F7E5D90ED40
C99DFC816E881F2119C7A14A64EB1C
prev
null

tb2
dgst
00001DBCB949AF5097FE4F2D4CF1F54562
4ED5646931466170FCFB771D584D9C
nonce
1000051123
trsummary
0BABE4EFB2BD7F39D999E8809DDFCC649
E6B8B6CA47ECD907D6784A4DA0DEDCB
prev
tb1

tb3
dgst
00009A7F99D2D09244E99D1F55AD29B49
D335D9254A2EC682341ECFBC905AF4C
nonce
1000052544
trsummary
036462EC76F2BEDA0CE4822E8747FEC9B6
9671359E7E3D2BD96485748360FD62
prev
tb2

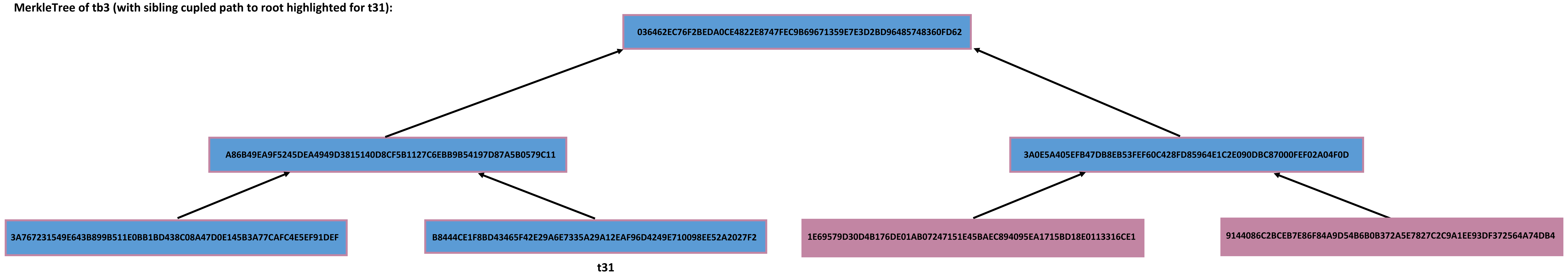
tb4
dgst
00004F4D8749BFFE9E1BEF4152F6849BCD
0A529B463FF0D409B338AFABF690C8
nonce
1000188337
trsummary
1CE221942486B63BD73A3D89082EF56FB5
F0B2DB6B0D87EA8D81557B8A26D4AD
prev
tb3

finalizeCoinsend Example

finalizeCoinSend(t31, DSobj)

- We first need to find the TransactionBlock containing t31,
  we first sequentially search tb4.tr_array (as tb4 is the last_block of the block chain), since t31 is not present in tb4, using prev pointer we goto tb3, and sequentially search for t31, and since it is present in tb3, we will now take tb3 and do the following.
- We have to compute the sibling coupled path to the root for t31 in tb3 Merkle tree to prove membership of transaction (i.e. proof that transaction t31 is a member of TransactionBlock tb3)

MerkleTree of tb3 (with sibling cupled path to root highlighted for t31):



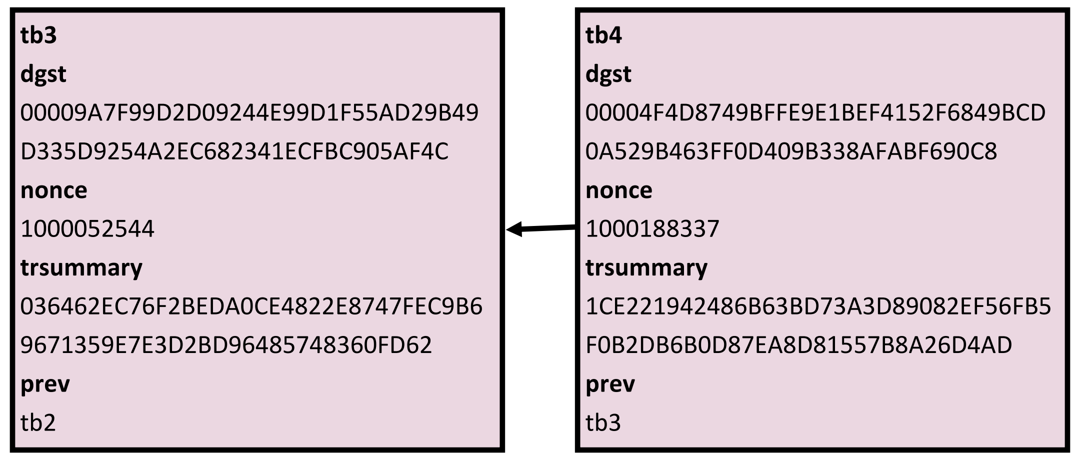
036462EC76F2BEDA0CE4822E8747FEC9B69671359E7E3D2BD96485748360FD62
A86B49EA9F5245DEA4949D3815140D8CF5B1127C6EBB9B54197D87A5B0579C11
3A0E5A405EFB47DB8EB53FEF60C428FD85964E1C2E090DBC87000FEF02A04F0D
3A767231549E643B899B511E0BB1BD438C08A47D0E145B3A77CAFC4E5EF91DEF
B8444CE1F8BD43465F42E29A6E7335A29A12EAF96D4249E710098EE52A2027F2
t31
1E69579D30D4B176DE01AB07247151E45BAEC894095EA1715BD18E0113316CE1
9144086C2BCEB7E86F84A9D54B6B0B372A5E7827C2C9A1EE93DF372564A74DB4

Sibling coupled path to root for t31: (to be outputted)

3A767231549E643B899B511E0BB1BD438C08A47D0E145B3A77CAFC4E5EF91DEF	A86B49EA9F5245DEA4949D3815140D8CF5B1127C6EBB9B54197D87A5B0579C11	036462EC76F2BEDA0CE4822E8747FEC9B69671359E7E3D2BD96485748360FD62
B8444CE1F8BD43465F42E29A6E7335A29A12EAF96D4249E710098EE52A2027F2	3A0E5A405EFB47DB8EB53FEF60C428FD85964E1C2E090DBC87000FEF02A04F0D	null

- Now, we have to compute a list of pair of strings of k+2 pairs, where k is the number of transaction blocks after the transaction block tB is present in. i.e. in our case after tb3, there is 1 block, therefore a list of 3 pair of strings is to be computed where each pair of string looks like: (t_i.dgst, t_i.previous.dgst + “#” + t_i.trsummary + “#” + t_i.nonce) and first block looks like (tB.previous.dgst, null).

Block Chain with and after tb3:



tb3	**tb4**
dgst	**dgst**
00009A7F99D2D09244E99D1F55AD29B49	00004F4D8749BFFE9E1BEF4152F6849BCD
D335D9254A2EC682341ECFBC905AF4C	0A529B463FF0D409B338AFABF690C8
nonce	**nonce**
1000052544	1000188337
trsummary	**trsummary**
036462EC76F2BEDA0CE4822E8747FEC9B6	1CE221942486B63BD73A3D89082EF56FB5
9671359E7E3D2BD96485748360FD62	F0B2DB6B0D87EA8D81557B8A26D4AD
prev	**prev**
tb2	tb3

Therefore, the List of Pair of Strings will look like:
(to be outputted)

00001DBCB949AF5097FE4F2D4CF1F545624ED5646931466170FCFB771D584D9C (tb2.dgst)	00009A7F99D2D09244E99D1F55AD29B49D335D9254A2EC682341ECFBC905AF4C (tb3.dgst)	00004F4D8749BFFE9E1BEF4152F6849BCD0A529B463FF0D409B338AFABF690C8 (tb4.dgst)
null	00001DBCB949AF5097FE4F2D4CF1F545624ED5646931466170FCFB771D584D9C# 036462EC76F2BEDA0CE4822E8747FEC9B69671359E7E3D2BD96485748360FD62# 1000052544 (tb2.dgst#tb3.trsummary#tb3.nonce)	00009A7F99D2D09244E99D1F55AD29B49D335D9254A2EC682341ECFBC905AF4C# 1CE221942486B63BD73A3D89082EF56FB5F0B2DB6B0D87EA8D81557B8A26D4AD #1000188337 (tb3.dgst#tb4.trsummary#tb4.nonce)