Figure 1

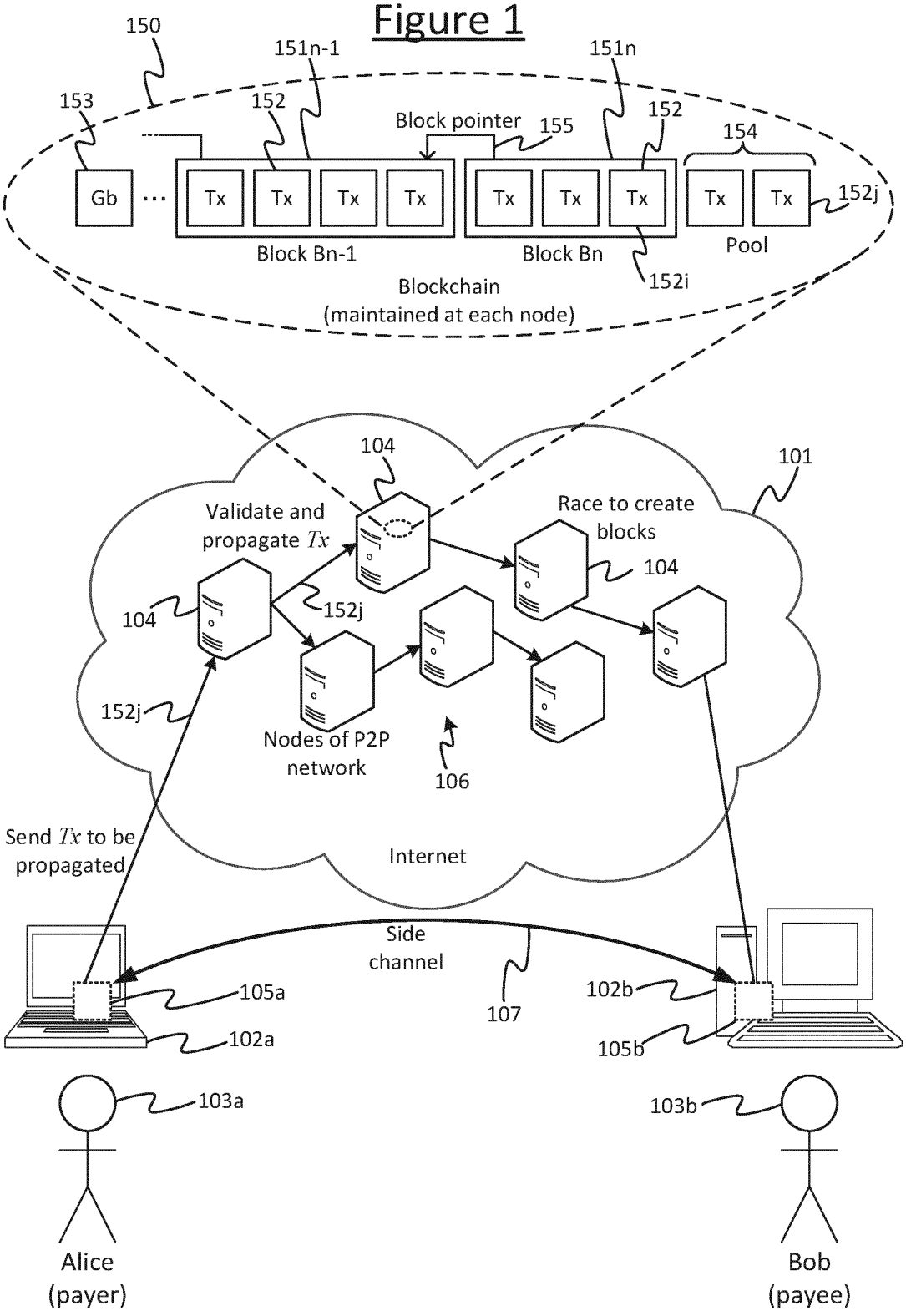
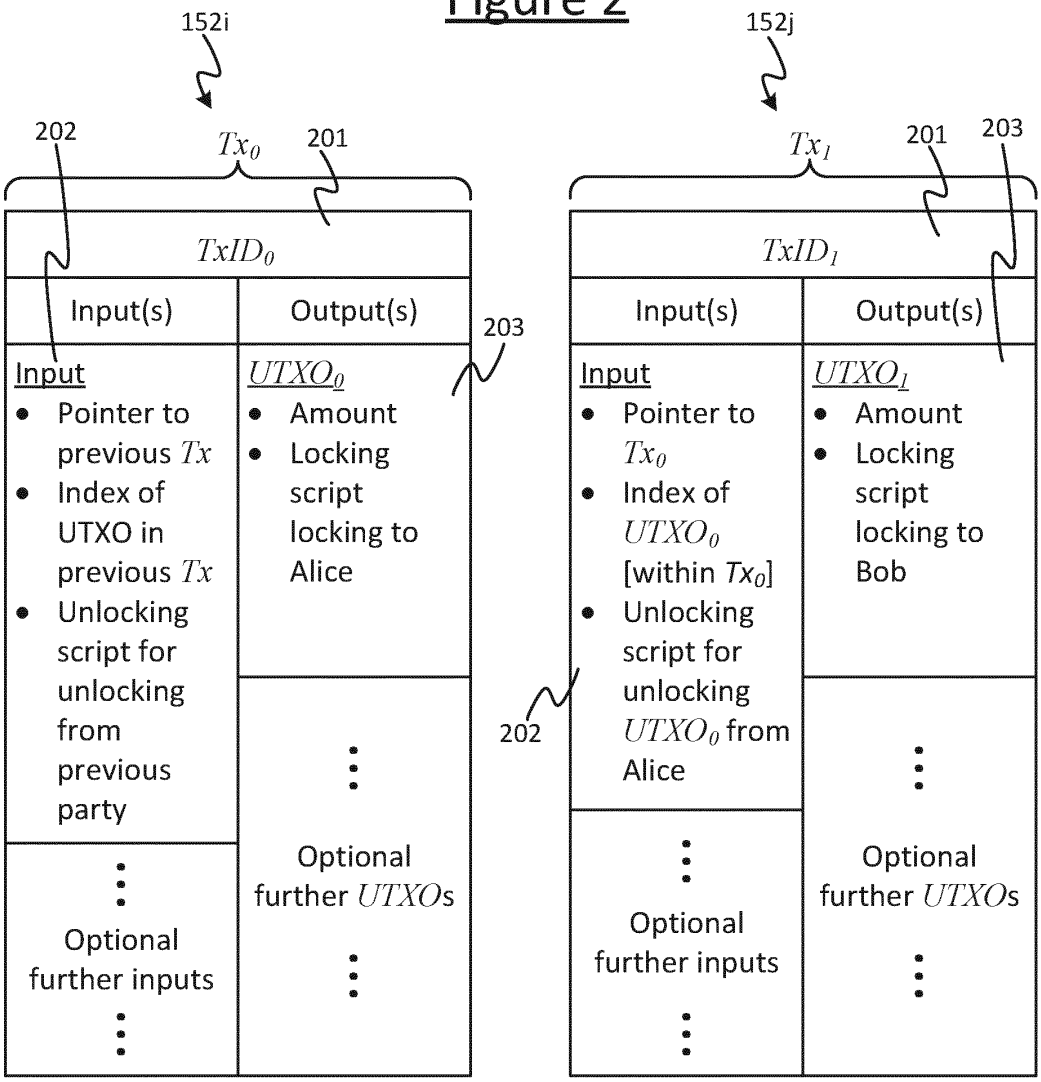

150
151n-1
151n
153
152
Block pointer
155
152
154
Gb
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
152j
Block Bn-1
Block Bn
Pool
152i
Blockchain
(maintained at each node)
104
101
Validate and
propagate Tx
Race to create
blocks
104
104
152j
152j
Nodes of P2P
network
106
Send Tx to be
propagated
Internet
Side
channel
107
105a
102a
102b
105b
103a
103b
Alice
(payer)
Bob
(payee)

Figure 2



Transaction from Alice to Bob

Validated by running: Locking script from output 203 of Tx_0, together with Alice's unlocking script from input 202 of Tx_1. This checks that Alice's unlocking script in Tx_1 meets the condition(s) defined in the locking script of previous transaction Tx_0.

Figure 3A

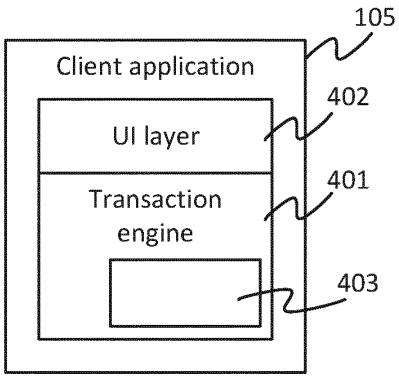


Figure 3B

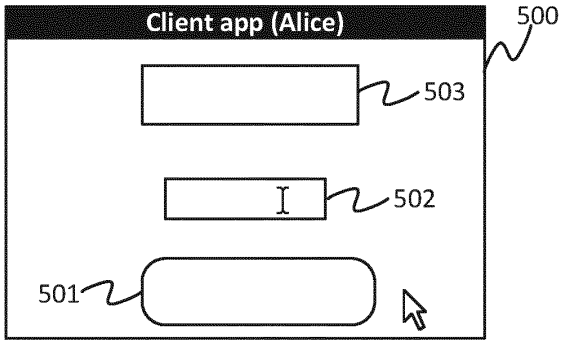


Figure 4

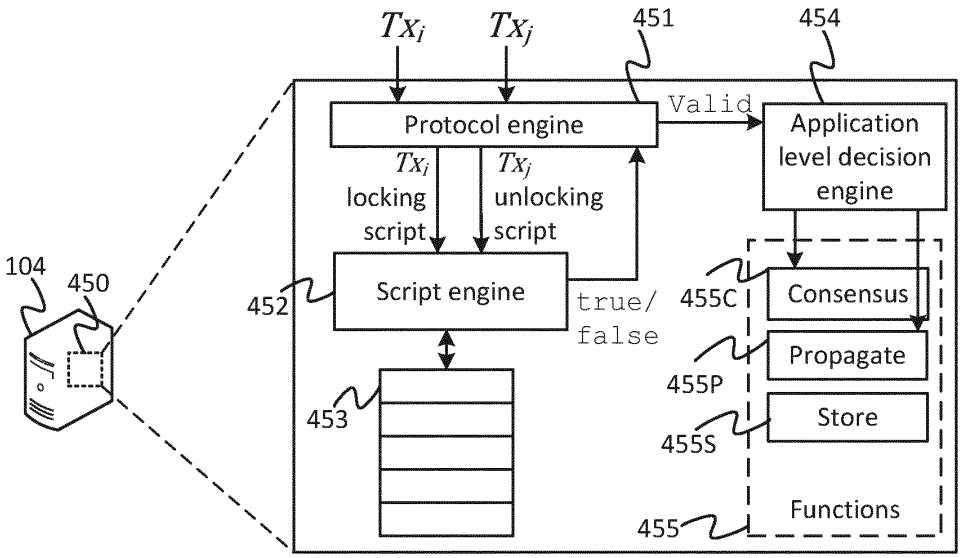

Tx_i
Tx_j
451
454
Protocol engine
Valid
Application level decision engine
Tx_i locking script
Tx_j unlocking script
104
450
452
Script engine
true/ false
455C
Consensus
Propagate
455P
Store
455S
453
Functions
455

Figure 5

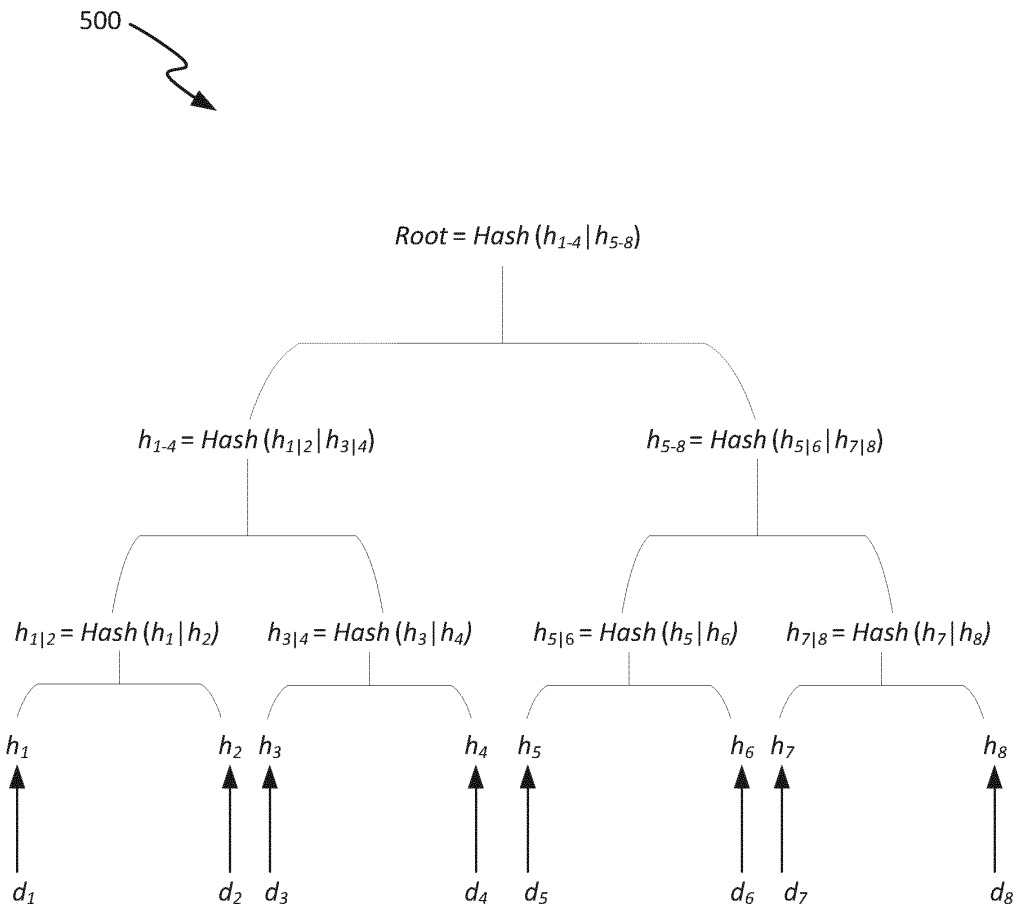

500
Root = Hash (h1-4 | h5-8)
h1-4 = Hash (h1|2 | h3|4)
h5-8 = Hash (h5|6 | h7|8)
h1|2 = Hash (h1 | h2)
h3|4 = Hash (h3 | h4)
h5|6 = Hash (h5 | h6)
h7|8 = Hash (h7 | h8)
h1
h2
h3
h4
h5
h6
h7
h8
d1
d2
d3
d4
d5
d6
d7
d8

Figure 6

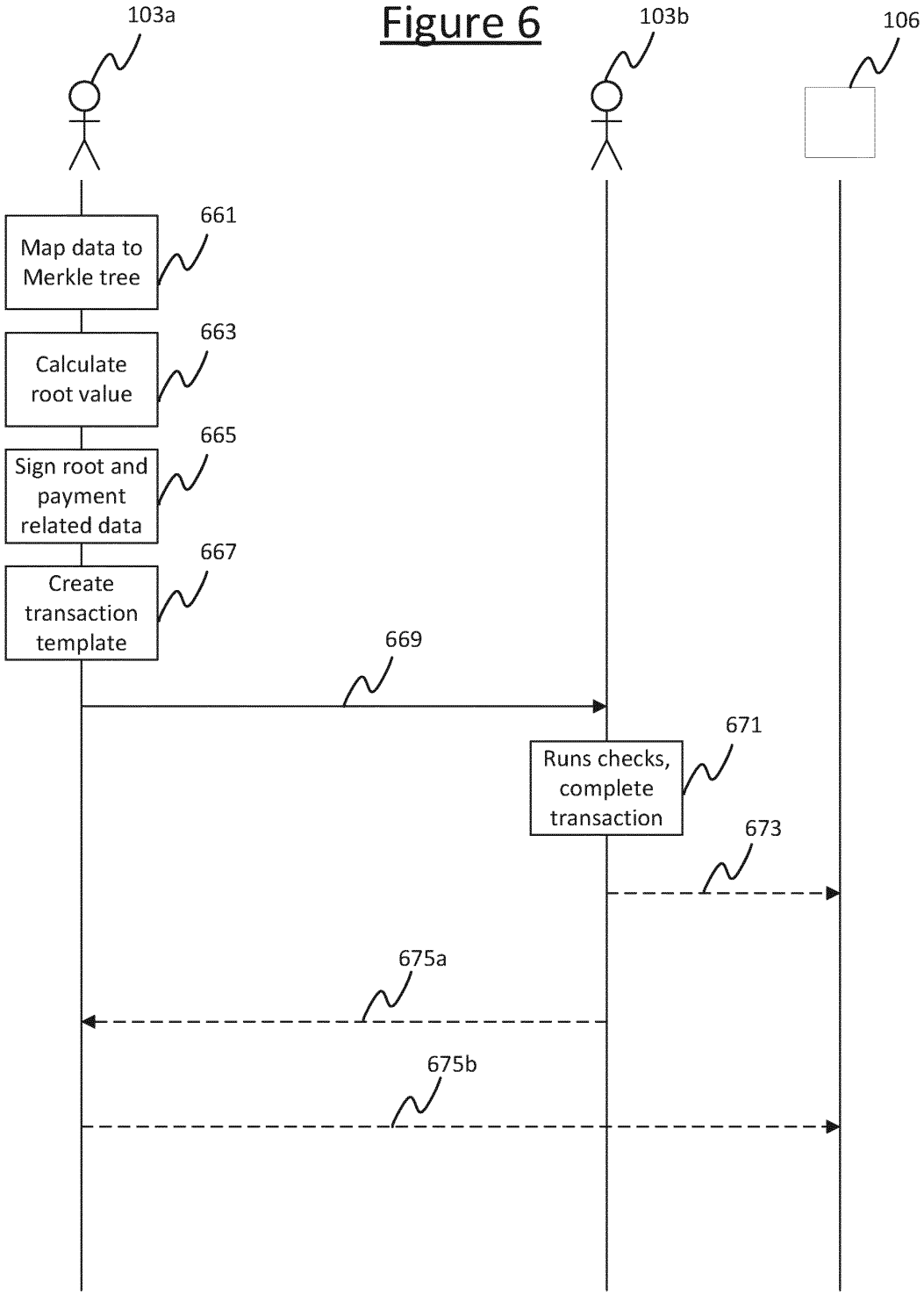
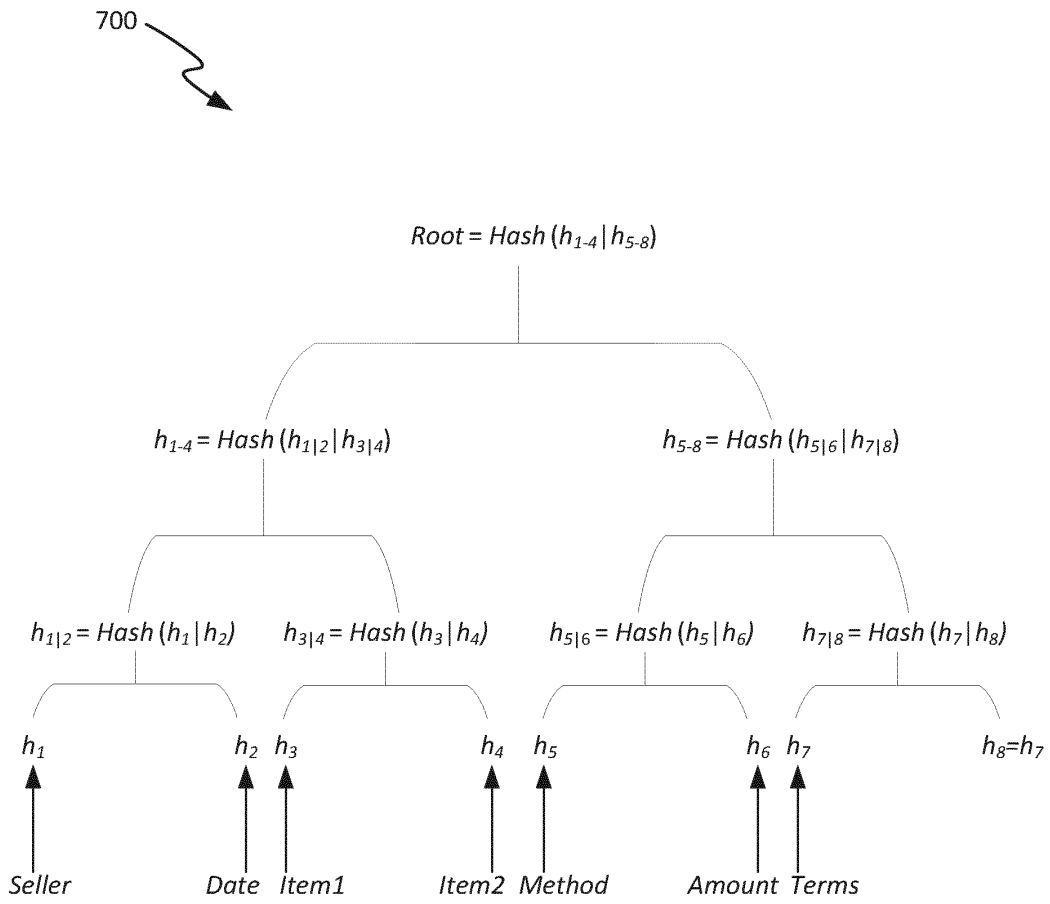

103a
103b
106
Map data to Merkle tree
661
Calculate root value
663
Sign root and payment related data
665
Create transaction template
667
669
Runs checks, complete transaction
671
673
675a
675b

Figure 7


700
Root = Hash (h1-4 | h5-8)
h1-4 = Hash (h1|2 | h3|4)
h5-8 = Hash (h5|6 | h7|8)
h1|2 = Hash (h1 | h2)
h3|4 = Hash (h3 | h4)
h5|6 = Hash (h5 | h6)
h7|8 = Hash (h7 | h8)
h1
h2
h3
h4
h5
h6
h7
h8=h7
Seller
Date
Item1
Item2
Method
Amount
Terms