Figure 1

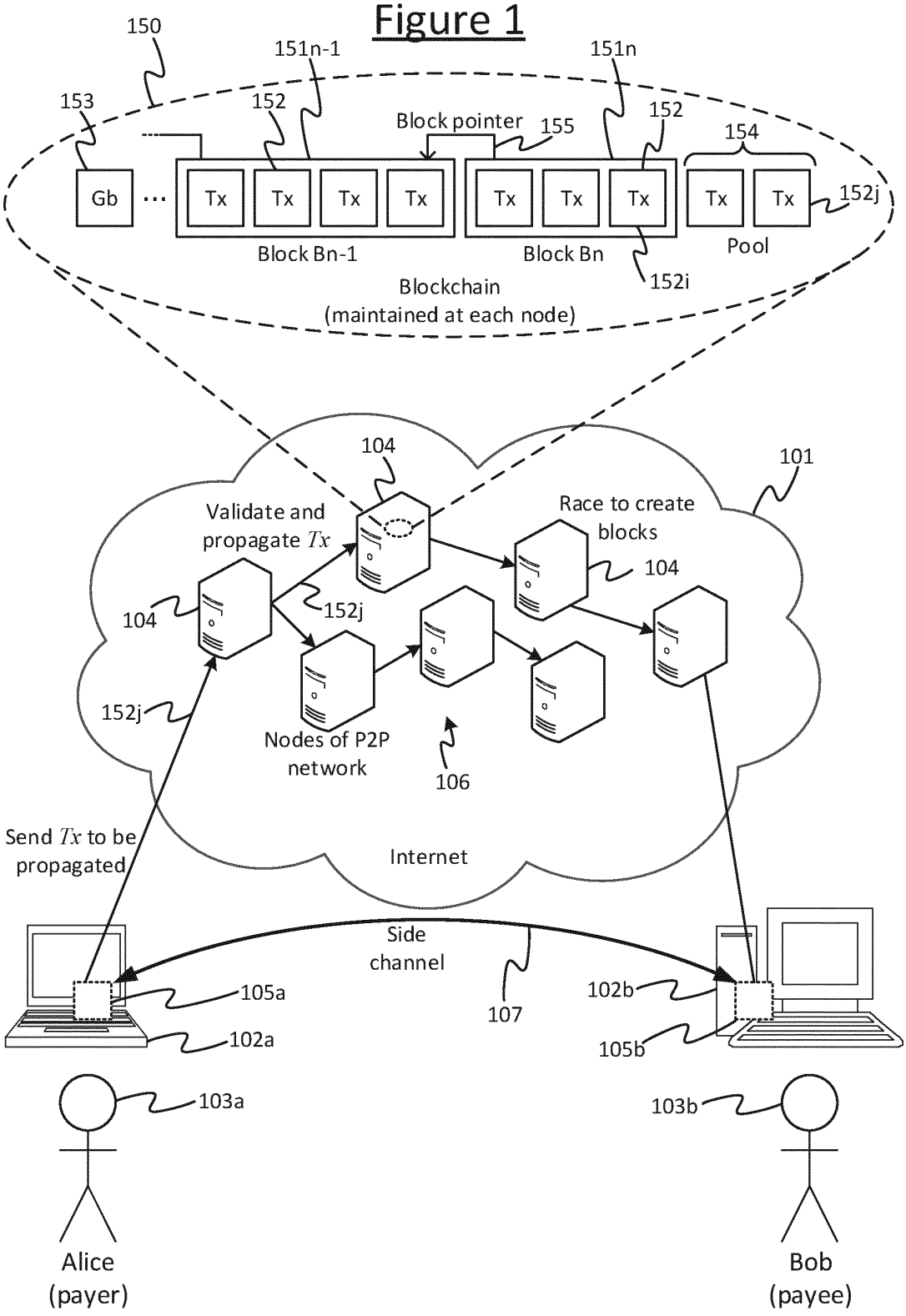
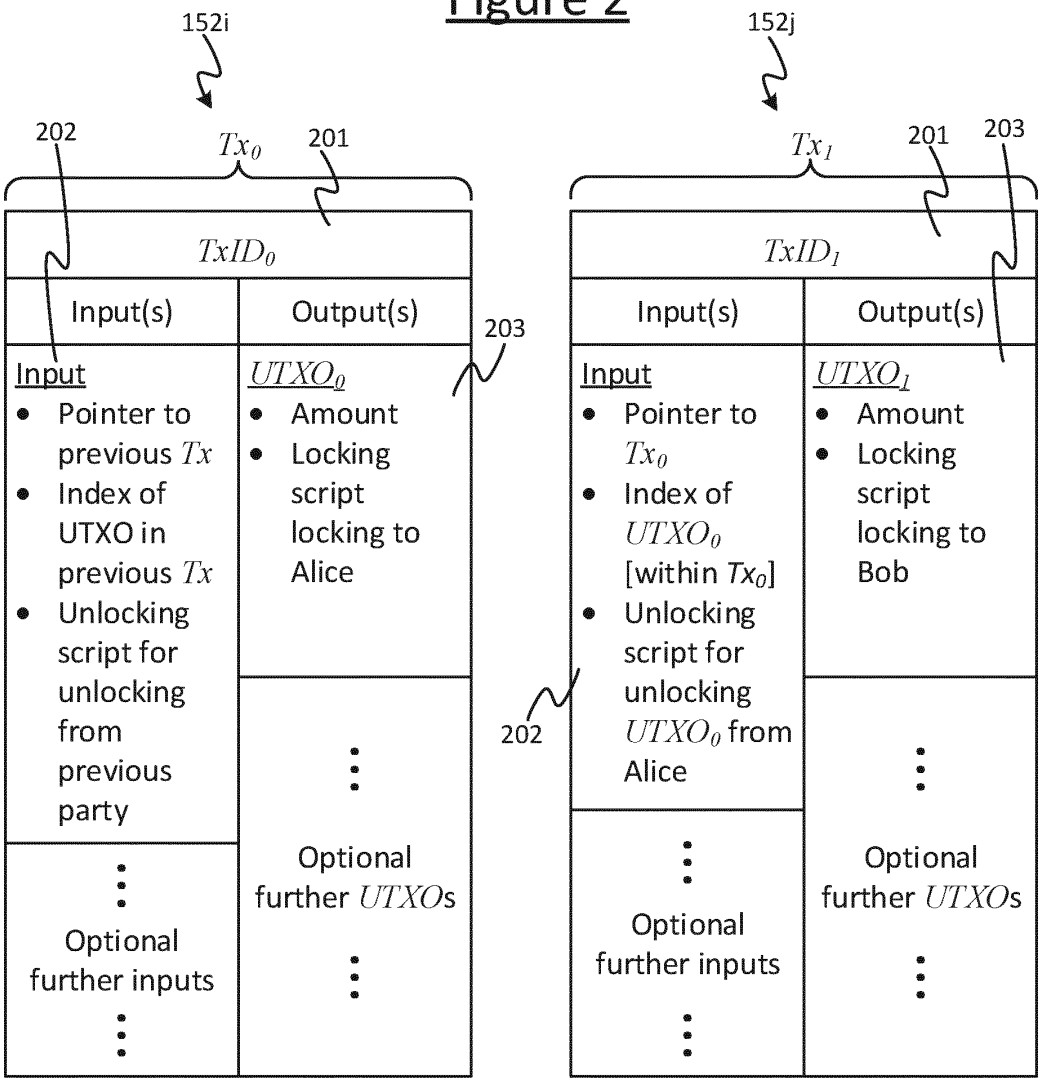

150
151n-1
151n
153
152
Block pointer
155
152
154
Gb
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
Tx
152j
Block Bn-1
Block Bn
Pool
152i
Blockchain
(maintained at each node)
104
101
Validate and
propagate Tx
Race to create
blocks
104
104
152j
152j
Nodes of P2P
network
106
Send Tx to be
propagated
Internet
Side
channel
107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

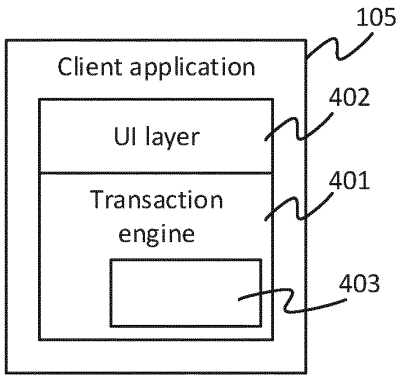


Figure 3B

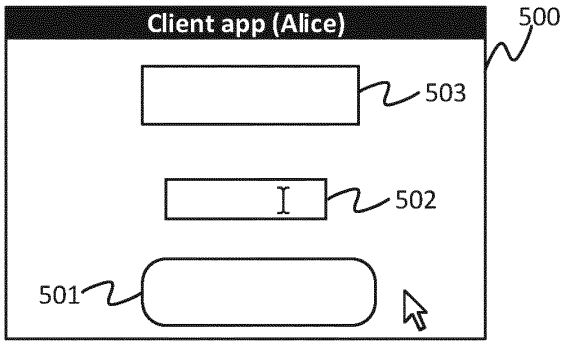


Figure 4

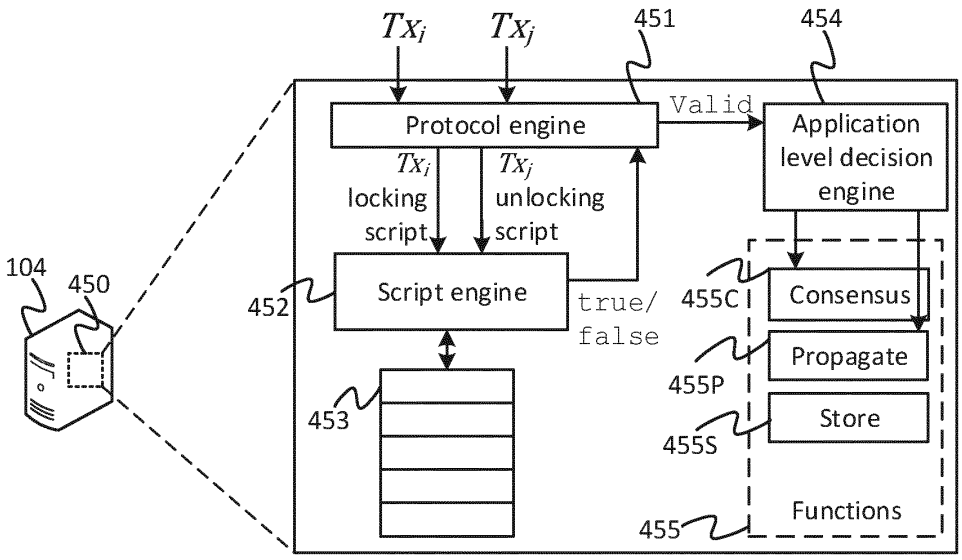

Tx_i
Tx_j
451
454
Protocol engine
Valid
Application level decision engine
Tx_i locking script
Tx_j unlocking script
104
450
452
Script engine
true/ false
455C
Consensus
Propagate
455P
Store
455S
453
Functions
455

Figure 5

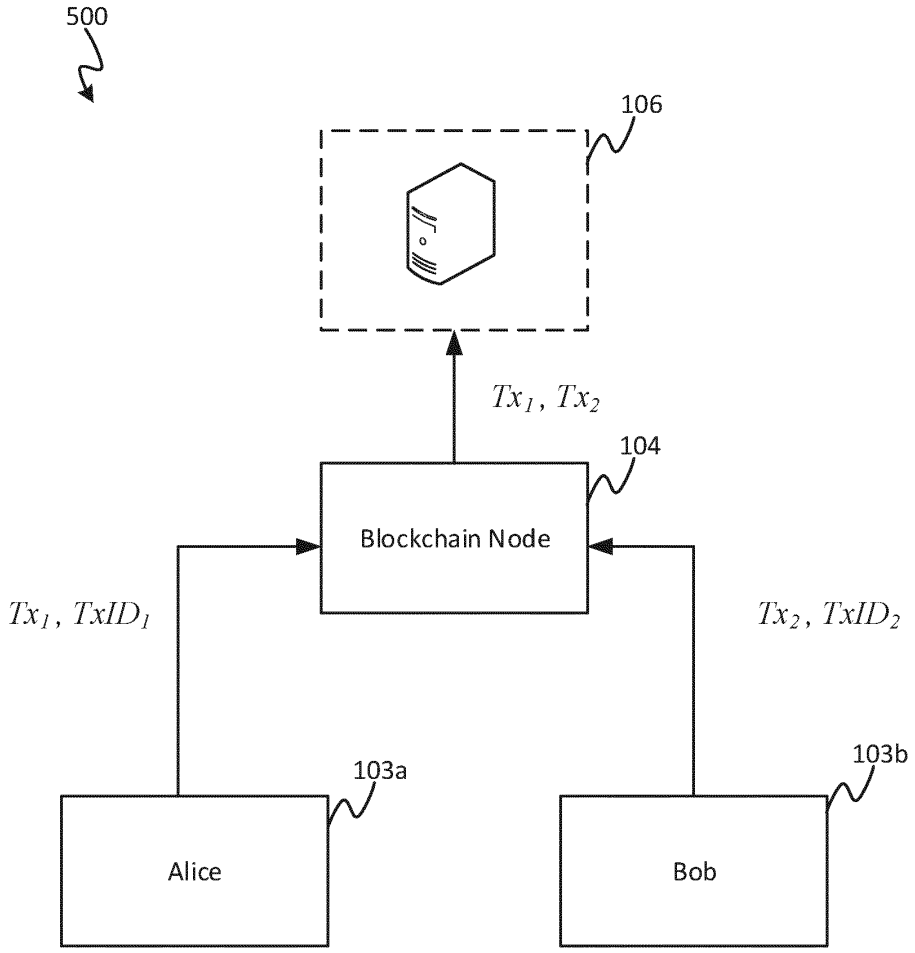

500
106
Tx_1, Tx_2
104
Blockchain Node
Tx_1, $TxID_1$
Tx_2, $TxID_2$
103a
103b
Alice
Bob

Figure 6

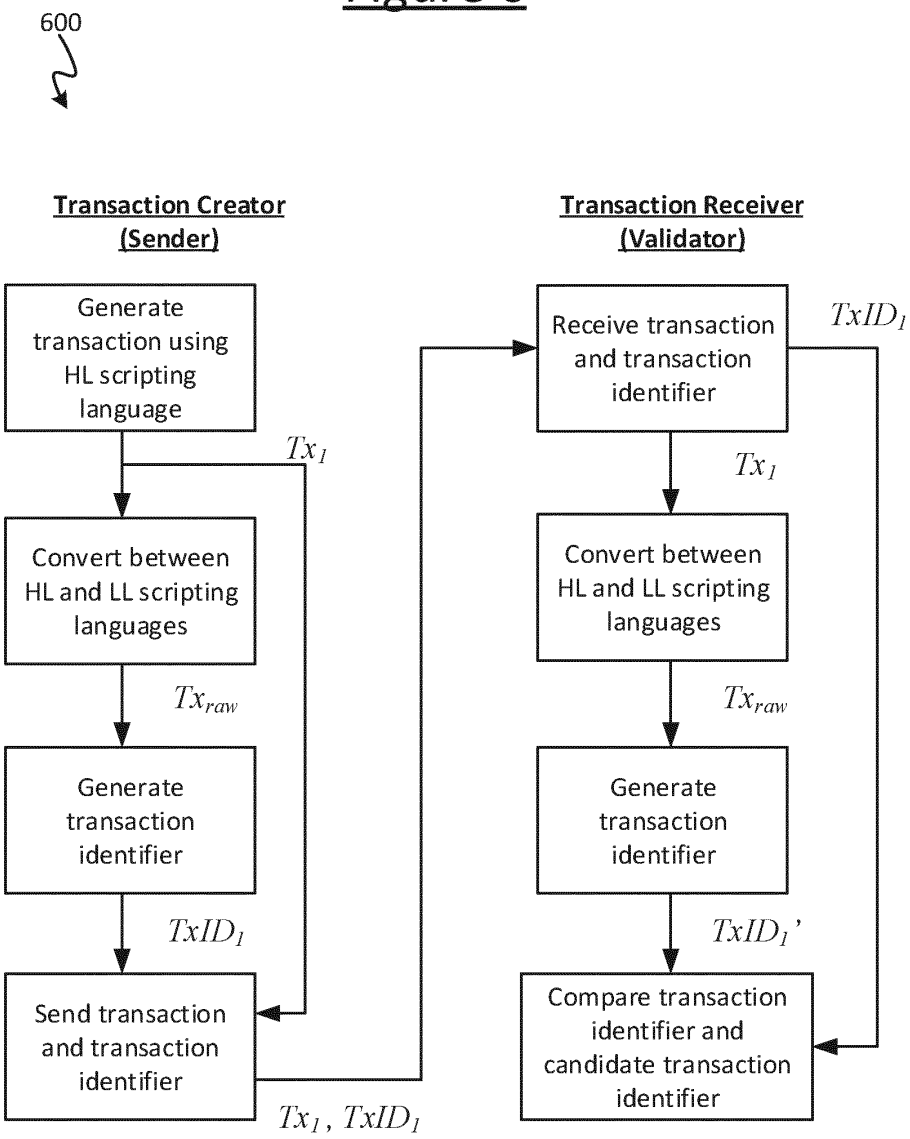

600
Transaction Creator (Sender)
Transaction Receiver (Validator)
Generate transaction using HL scripting language
Convert between HL and LL scripting languages
Generate transaction identifier
Send transaction and transaction identifier
Receive transaction and transaction identifier
Convert between HL and LL scripting languages
Generate transaction identifier
Compare transaction identifier and candidate transaction identifier
Tx_1
Tx_{raw}
$TxID_1$
Tx_1, $TxID_1$
$TxID_1$
Tx_1
Tx_{raw}
$TxID_1$'

Figure 7

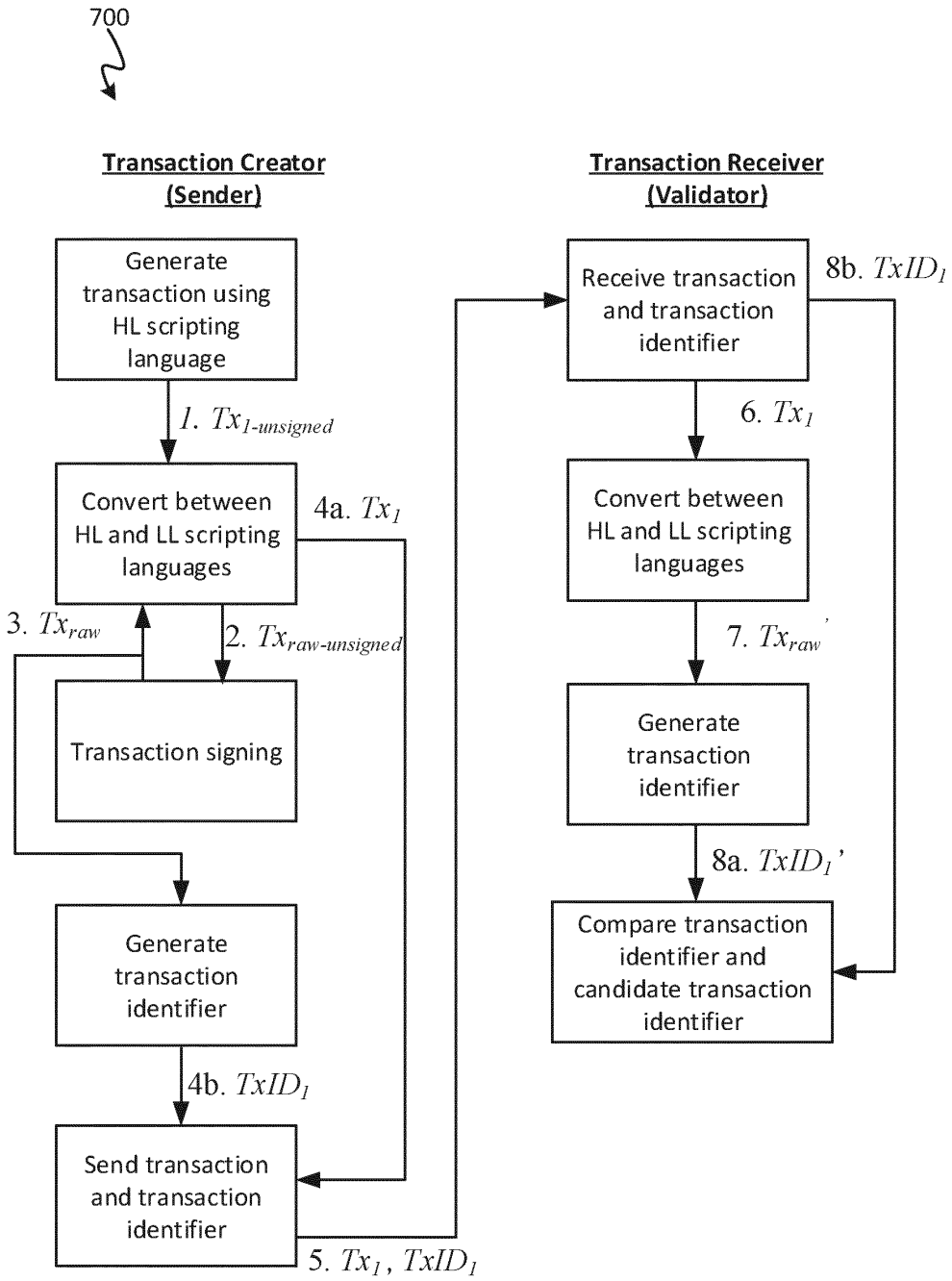

700
Transaction Creator (Sender)
Transaction Receiver (Validator)
Generate transaction using HL scripting language
1. $Tx_{1\text{-}unsigned}$
Convert between HL and LL scripting languages
4a. Tx_1
3. Tx_{raw}
2. $Tx_{raw\text{-}unsigned}$
Transaction signing
Generate transaction identifier
4b. $TxID_1$
Send transaction and transaction identifier
5. Tx_1, $TxID_1$
Receive transaction and transaction identifier
8b. $TxID_1$
6. Tx_1
Convert between HL and LL scripting languages
7. Tx_{raw}'
Generate transaction identifier
8a. $TxID_1$'
Compare transaction identifier and candidate transaction identifier

Figure 8

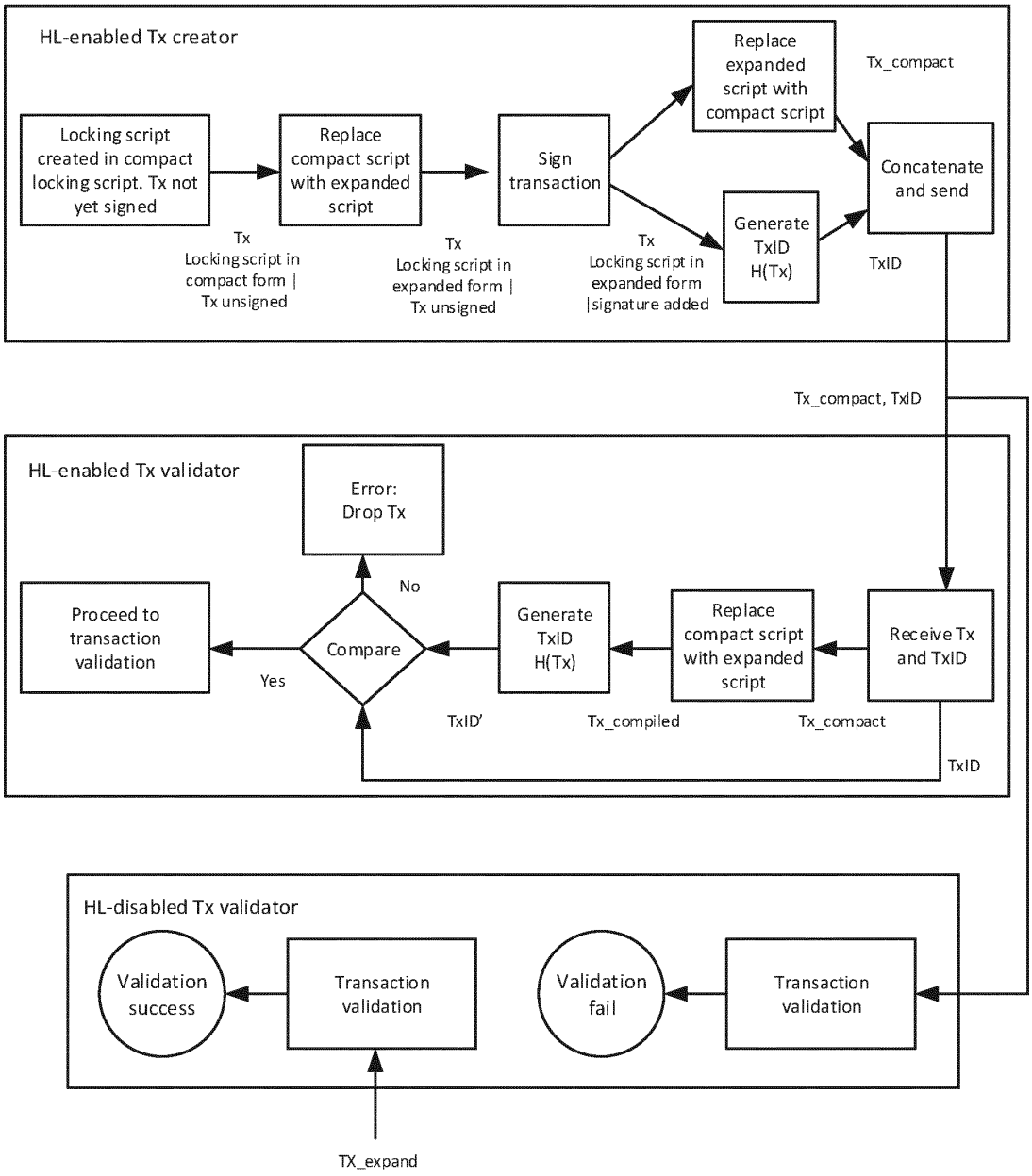
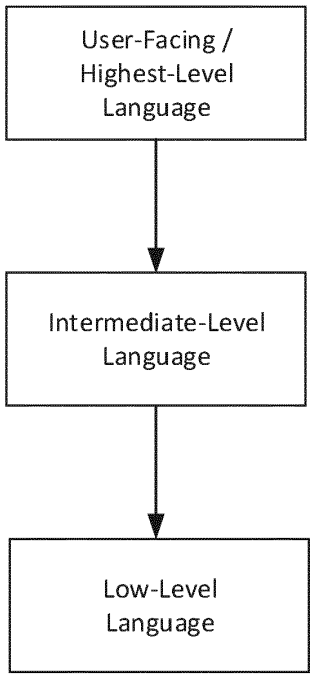

HL-enabled Tx creator
Locking script created in compact locking script. Tx not yet signed
Tx
Locking script in compact form | Tx unsigned
Replace compact script with expanded script
Tx
Locking script in expanded form | Tx unsigned
Sign transaction
Replace expanded script with compact script
Tx_compact
Generate TxID H(Tx)
Tx
Locking script in expanded form |signature added
Concatenate and send
TxID
Tx_compact, TxID
HL-enabled Tx validator
Error: Drop Tx
No
Proceed to transaction validation
Compare
Yes
Generate TxID H(Tx)
TxID'
Replace compact script with expanded script
Tx_compiled
Receive Tx and TxID
Tx_compact
TxID
HL-disabled Tx validator
Validation success
Transaction validation
Validation fail
Transaction validation
TX_expand

Figure 9


User-Facing / Highest-Level Language
Intermediate-Level Language
Low-Level Language