

1/7

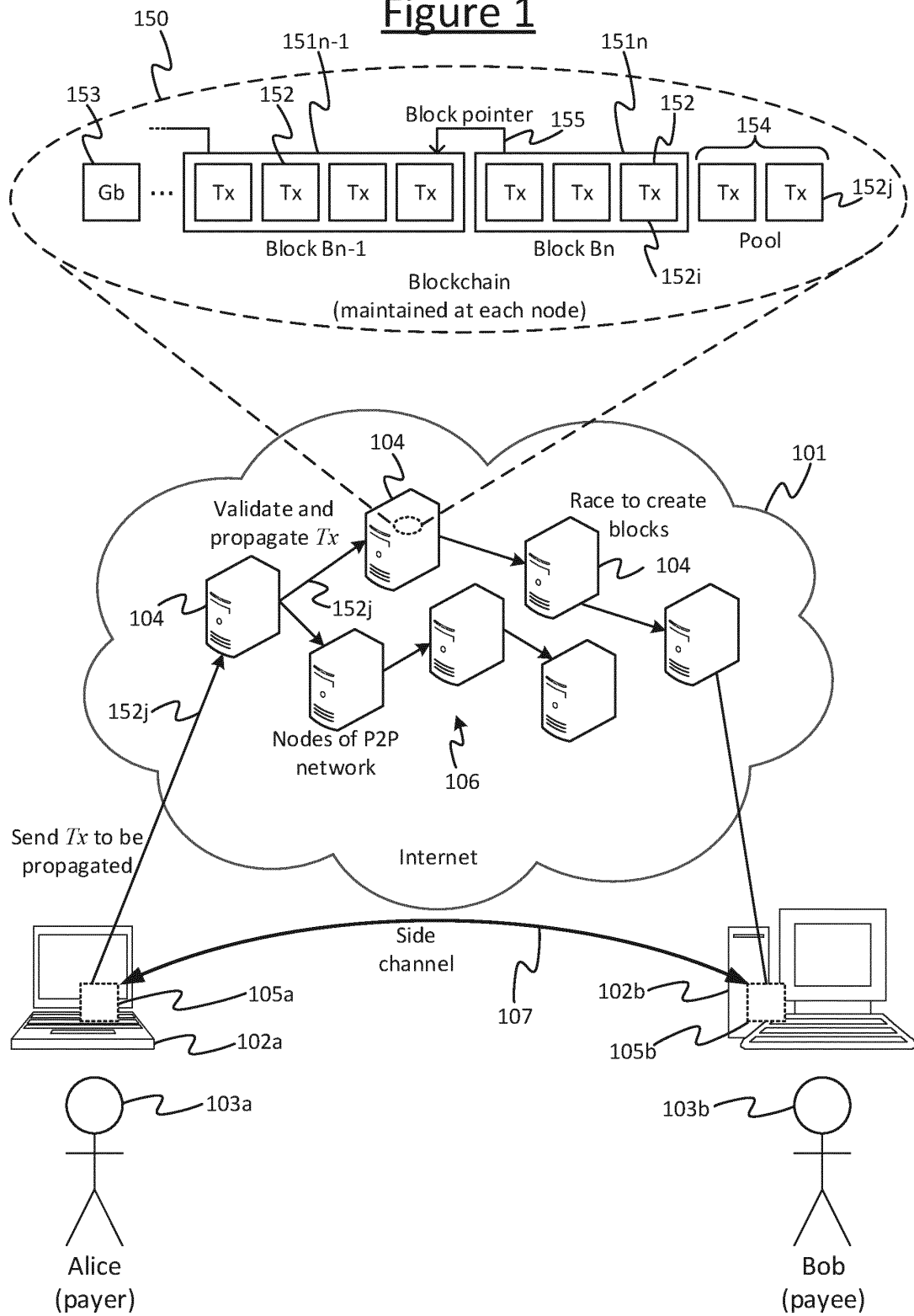
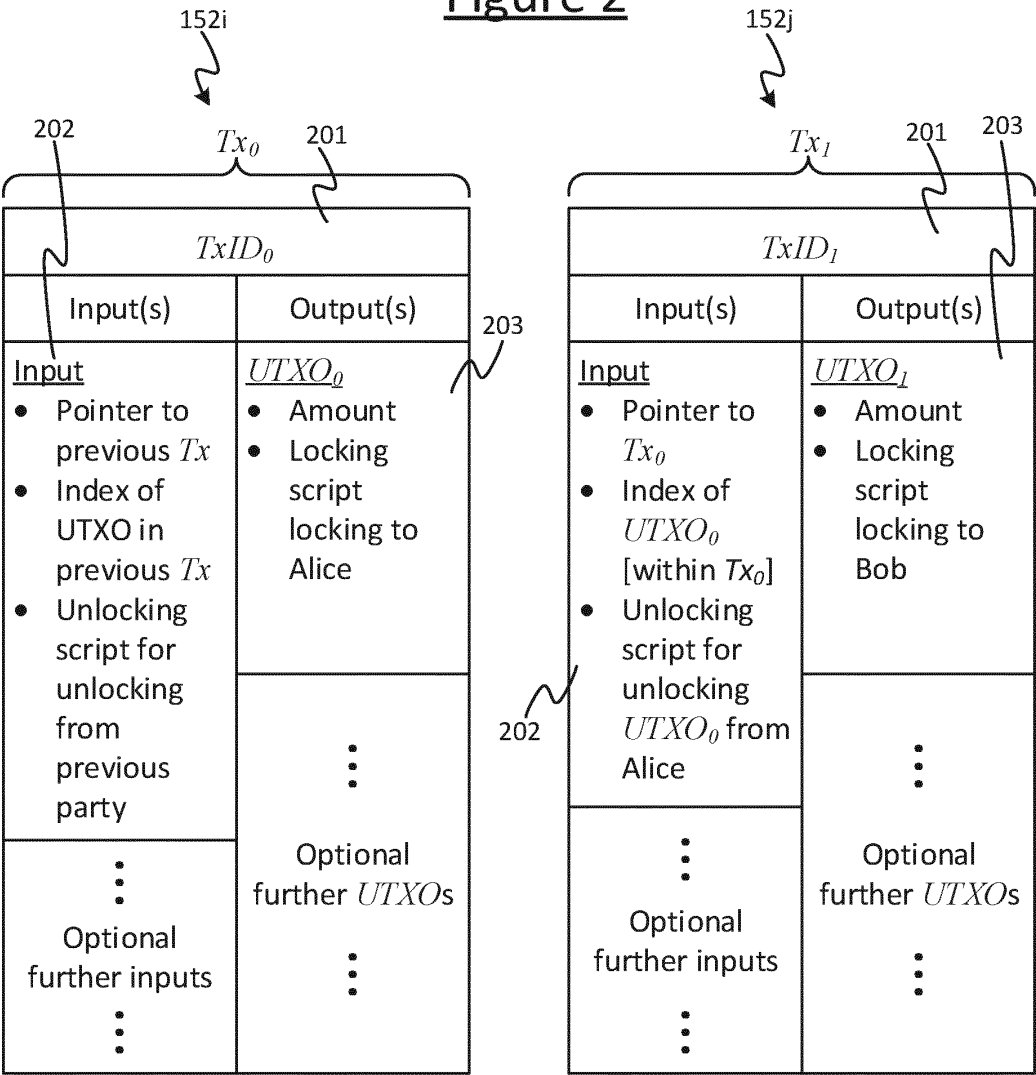
Figure 1

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

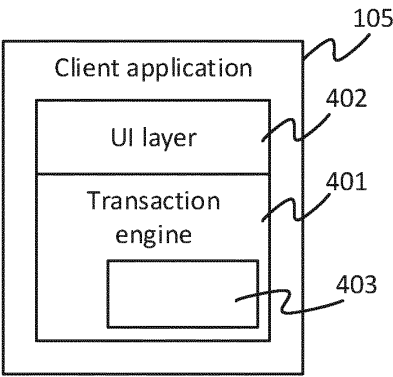


Figure 3B

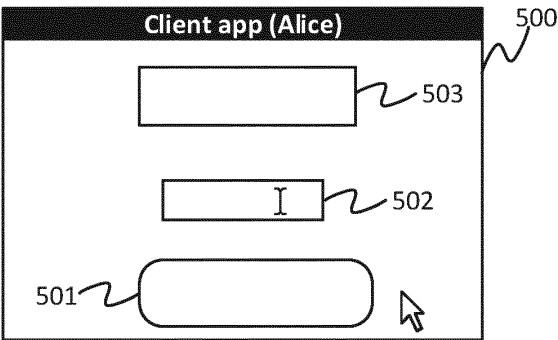
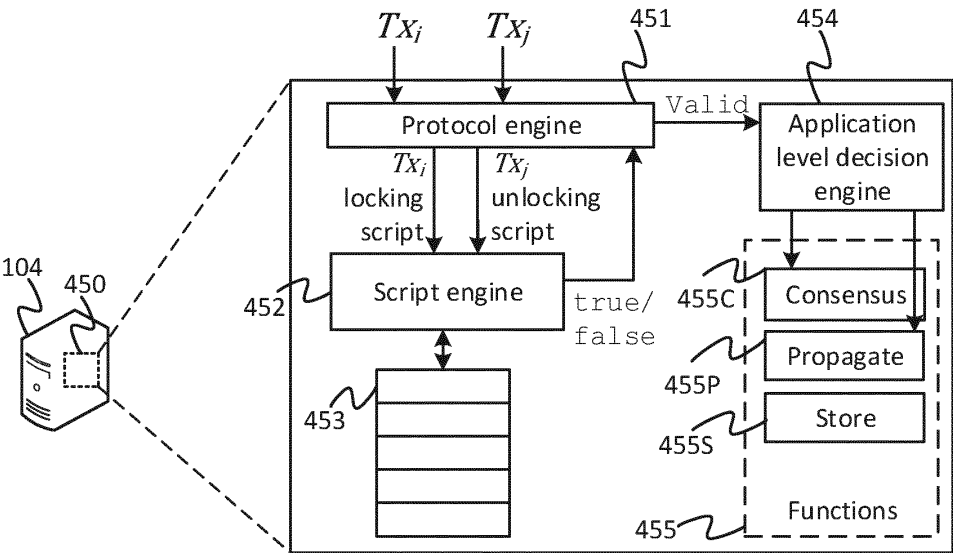


Figure 4



5/7

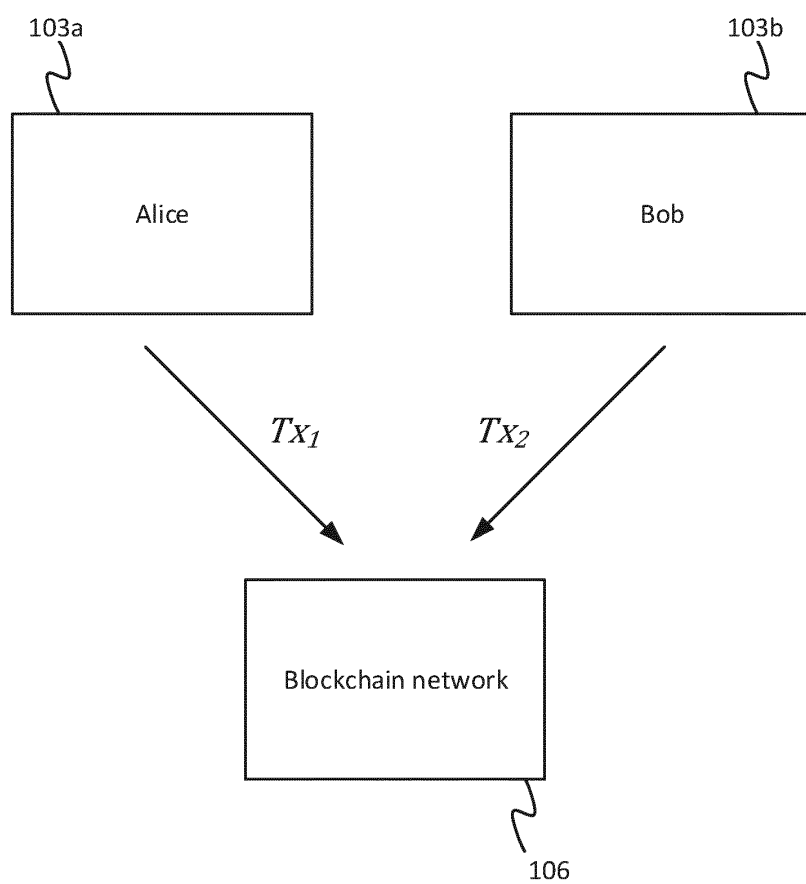
Figure 5

Figure 6

TxID ₀				
Version	1	Locktime	0	
In-count	1	Out-count	1	
Input list			Output list	
Outpoint	Unlocking script	nSeq	Value	Locking script
Outpoint _A	< Sig _A > < PK _A >	FFFFFF FF	1000	[outputsRequest][sign] OP_CHECKSIGVERIFY OP_SWAP <0x68> OP_SPLIT OP_NIP OP_8 OP_SPLIT OP_SWAP OP_CAT OP_EQUALVERIFY OP_DUP OP_HASH160 <H(PK_B)> OP_EQUALVERIFY OP_CHECKSIG

Figure 7

TxID ₁				
Version	1	Locktime	0	
In-count	1	Out-count	1	
Input list			Output list	
Outpoint	Unlocking script	nSeq	Value	Locking script
TxID ₀ 0	< Sig _B > < PK _B > < Data ₁ > < Data ₂ >	FFFFF FFF	1000	[outputsRequest][sign] OP_CHECKSIGVERIFY OP_SWAP <0x68> OP_SPLIT OP_NIP OP_8 OP_SPLIT OP_SWAP OP_CAT OP_EQUALVERIFY OP_DUP OP_HASH160 <H(PK_B)> OP_EQUALVERIFY OP_CHECKSIG

Figure 8

TxID ₁				
Version	1	Locktime	0	
In-count	1	Out-count	1	
Input list			Output list	
Outpoint	Unlocking script	nSeq	Value	Locking script
TxID ₀ 0	< Sig_B > < PK_B > < Data₁ > < Data₂ > < Data₃ >	FFFFFF FF	1000	[outputsRequest][sign] OP_CHECKSIGVERIFY OP_SWAP <0x68> OP_SPLIT OP_NIP OP_8 OP_SPLIT OP_SWAP OP_CAT OP_EQUALVERIFY OP_DUP OP_HASH160 <H(PK_B)> OP_EQUALVERIFY OP_CHECKSIG