

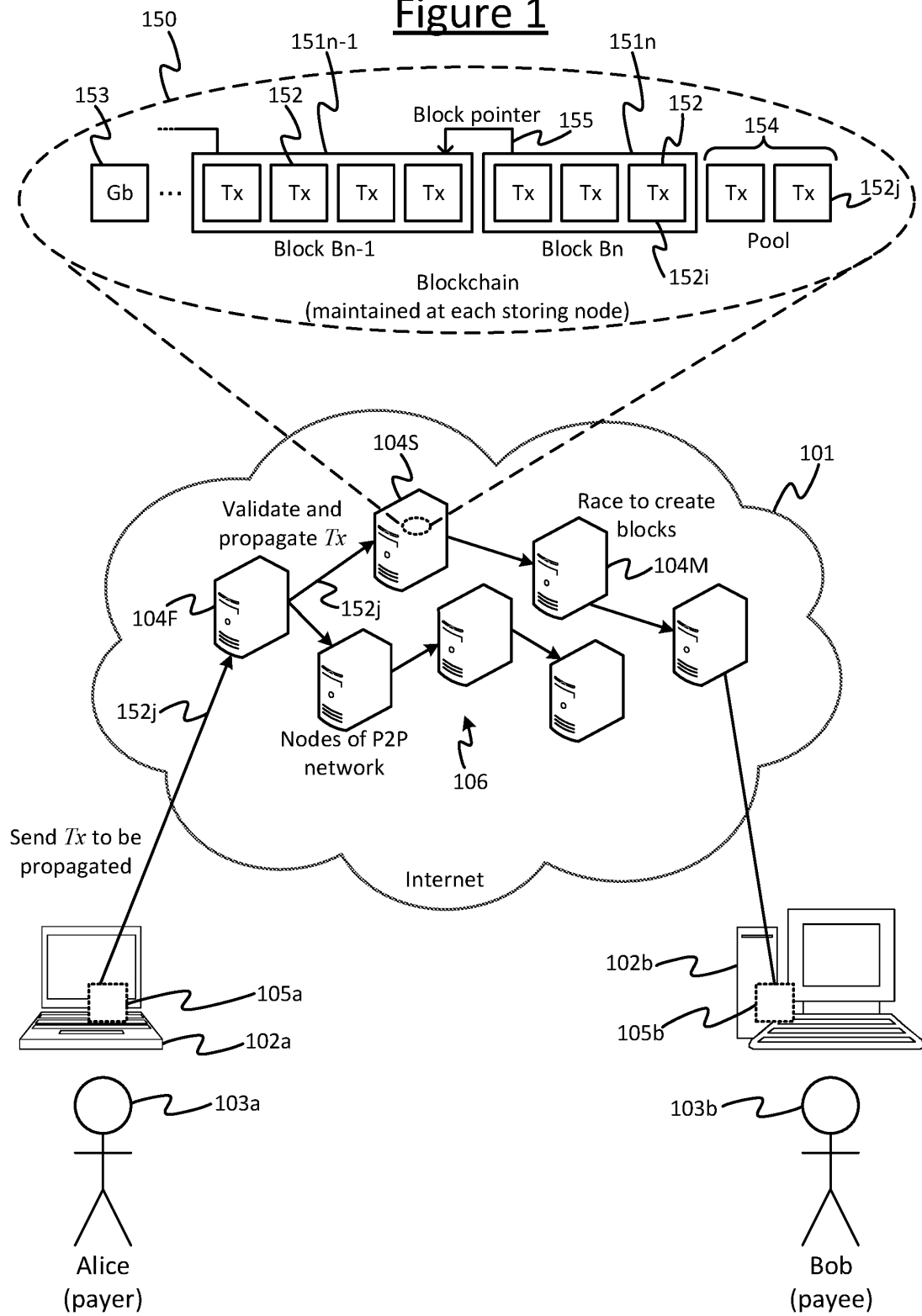
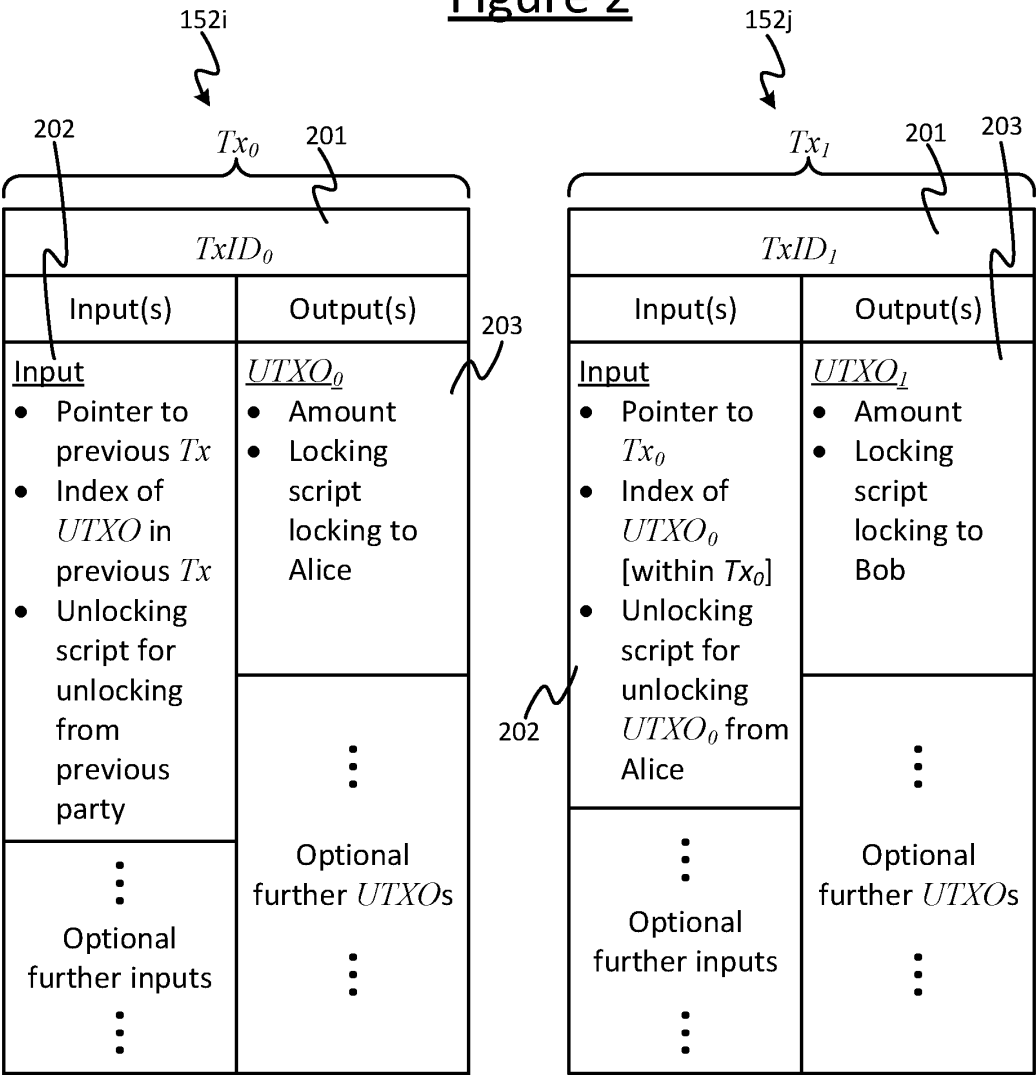
Figure 1

Figure 2



Transaction
from Alice to Bob

↓

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

Figure 3

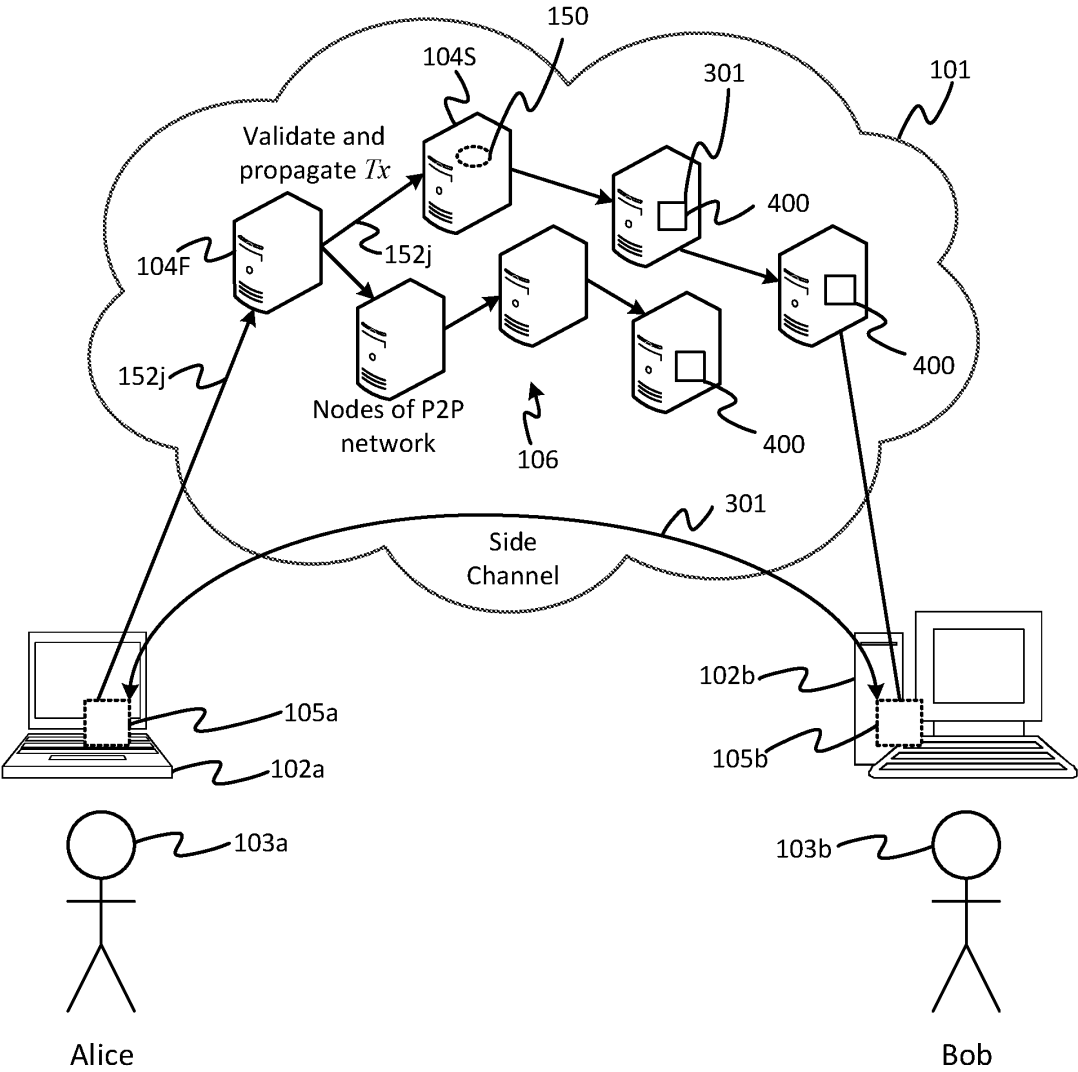


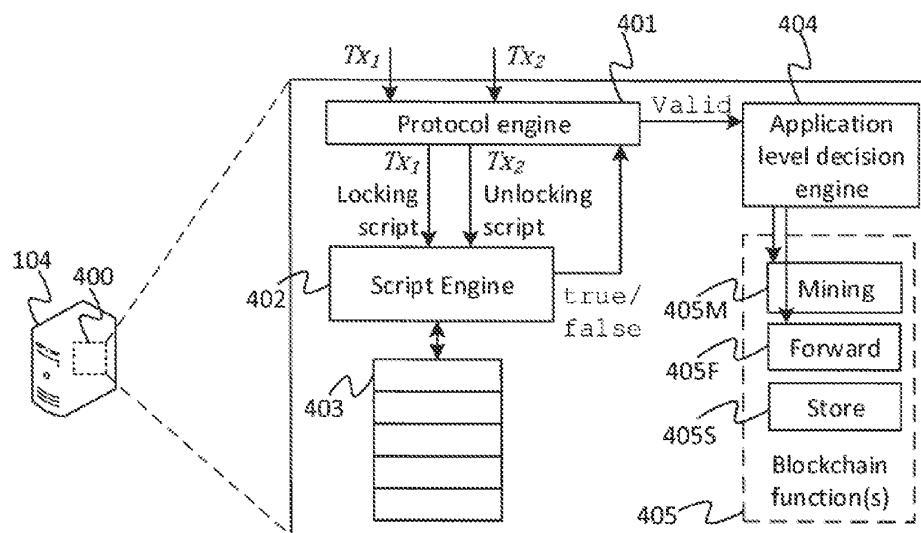
Figure 4

Figure 5

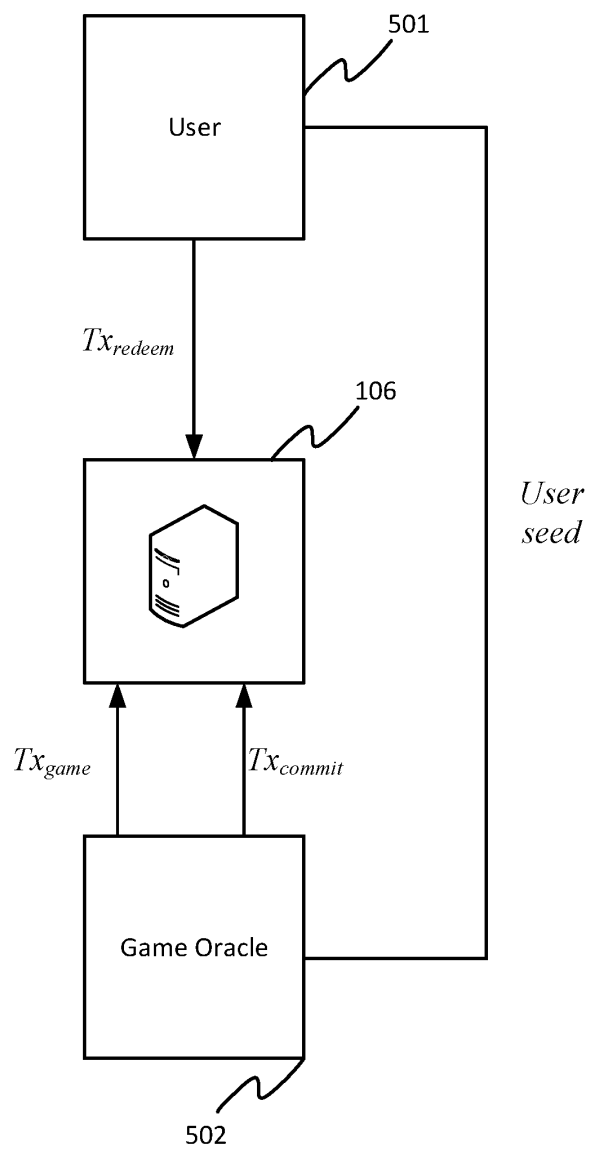


Figure 6

Table 1: Script to generate random number $\langle R_N \rangle$		
Stack	Script	Description
empty	$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_N \rangle$ OP_ADD OP_ADD ... OP_ADD OP_HASH256 $\langle N \rangle$ OP_MOD	
$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_N \rangle$	OP_ADD OP_ADD ... OP_ADD OP_HASH256 $\langle N \rangle$ OP_MOD	Constants are added to the stack
$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_{N-1} + s'_N \rangle$	OP_ADD ... OP_ADD OP_HASH256 $\langle N \rangle$ OP_MOD	Top two values on stack added
$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_{N-2} + s'_{N-1} + s'_N \rangle$	... OP_ADD OP_HASH256 $\langle N \rangle$ OP_MOD	Top two values on stack added
$\langle \sum_i s'_i \rangle$	OP_HASH256 $\langle N \rangle$ OP_MOD	Repeated addition of top two values
$\langle H(\sum_i s'_i) \rangle$	$\langle N \rangle$ OP_MOD	Top value hashed twice with SHA-256
$\langle H(\sum_i s'_i) \rangle \langle N \rangle$	OP_MOD	Constants are added to the stack
$\langle R_N \rangle$	empty	Remainder of 2^{nd} value divided by 1^{st} value computed; a random number

Figure 7

Table 2: Script to spend funds encumbered by the Oracle transaction			
AltStack	Stack	Script	Description
empty	empty	$\langle Sig P_w \rangle$ OP_TOALTSTACK $\langle P_1 \rangle$ $\langle P_2 \rangle$... $\langle P_N \rangle$ $\langle R_N \rangle$ OP_ROLL OP_TOALTSTACK OP_DROP ... OP_DROP OP_FROMALTSTACK OP_FROMALTSTACK OP_SWAP OP_CHECKSIG	
	$\langle Sig P_w \rangle$	OP_TOALTSTACK $\langle P_1 \rangle$ $\langle P_2 \rangle$... $\langle P_N \rangle$ $\langle R_N \rangle$ OP_ROLL OP_TOALTSTACK OP_DROP ... OP_DROP OP_FROMALTSTACK OP_FROMALTSTACK OP_SWAP OP_CHECKSIG	Constants are added to the stack
$\langle Sig P_w \rangle$	$\langle P_1 \rangle$ $\langle P_2 \rangle$... $\langle P_N \rangle$ $\langle R_N \rangle$	OP_ROLL OP_TOALTSTACK OP_DROP ... OP_DROP OP_FROMALTSTACK OP_FROMALTSTACK OP_SWAP OP_CHECKSIG	Winning signature {WSG} moved to altstack
$\langle Sig P_w \rangle$	$\langle P_1 \rangle$... $\langle P_N \rangle$ $\langle P_w \rangle$	OP_TOALTSTACK OP_DROP ... OP_DROP OP_FROMALTSTACK OP_FROMALTSTACK OP_SWAP OP_CHECKSIG	Winning public key {WPK} moved to top of stack
$\langle Sig P_w \rangle$ $\langle P_w \rangle$	$\langle P_1 \rangle$... $\langle P_N \rangle$	OP_DROP ... OP_DROP OP_FROMALTSTACK OP_FROMALTSTACK OP_SWAP OP_CHECKSIG	WPK moved to altstack
$\langle Sig P_w \rangle$ $\langle P_w \rangle$	empty	OP_FROMALTSTACK OP_FROMALTSTACK OP_SWAP OP_CHECKSIG	Remaining $N-1$ public keys dropped from stack
$\langle Sig P_w \rangle$	$\langle P_w \rangle$	OP_FROMALTSTACK OP_SWAP OP_CHECKSIG	WPK moved back to stack
empty	$\langle P_w \rangle$ $\langle Sig P_w \rangle$	OP_SWAP	WSG moved back to stack
	$\langle Sig P_w \rangle$ $\langle P_w \rangle$	OP_CHECKSIG	Winning signature checked
	TRUE	empty	