

Figure 1

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 2

Initiation transaction		
Number of inputs		N
Input 1 (unlocking)	Value	x
	Signature script [P2PKH]	$\langle \text{Sig } P_1 \rangle \langle P_1 \rangle \langle r'_1 \rangle$ OP_DROP
Input 2 (unlocking)	Value	x
	Signature script [P2PKH]	$\langle \text{Sig } P_2 \rangle \langle P_2 \rangle \langle r'_2 \rangle$ OP_DROP
...		
Input N (unlocking)	Value	x
	Signature script [P2PKH]	$\langle \text{Sig } P_N \rangle \langle P_N \rangle \langle r'_N \rangle$ OP_DROP
Number of outputs		1
Output (locking)	Value	$N \times x$
	Public key script [P2PKH]	OP_DUP OP_HASH160 $\langle \text{Hash160}(P_0) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Oracle transaction		
Number of inputs		1
Input (unlocking)	Value	$N \times x$
	Signature script [P2PKH]	$\langle \text{Sig } P_0 \rangle \langle P_0 \rangle$
Number of outputs		1
Output (locking)	Value	$N \times x$
	Public key script [P2PKH]	$\langle P_1 \rangle \langle P_2 \rangle \dots \langle P_N \rangle \langle R_N \rangle$ OP_ROLL OP_TOALTSTACK OP_DROP ... OP_DROP OP_FROMALTSTACK OP_CHECKSIG

Figure 3

Oracle transaction (with house)		
Number of inputs		1
Input (unlocking)	Value	$(N \times x) + r$
	Signature script [P2PKH]	$\langle \text{Sig } P_0 \rangle \langle P_0 \rangle$
Number of outputs		1
Output (locking)	Value	$(N \times x) + r$
	Public key script [P2PKH]	$\langle P_1 \rangle \langle P_2 \rangle \dots \langle P_N \rangle \langle R_N \rangle$ OP_ROLL OP_TOALTSTACK OP_DROP ... OP_DROP OP_FROMALTSTACK OP_CHECKSIG OP_IF OP_1 OP_ELSE $\langle \Delta T_k \rangle$ OP_CHECKSEQUENCEVERIFY OP_DROP $\langle P_H \rangle$ OP_CHECKSIG OP_ENDIF

Figure 4

Winnings-redemption transaction		
Number of inputs		1
Input (unlocking)	Value	$N \times x$
	Signature script [P2PKH]	$\langle \text{Sig } P_W \rangle$
Number of outputs		1
Output (locking)	Value	$N \times x$
	Public key script [P2PKH]	OP_DUP OP_HASH160 $\langle \text{Hash160}(P_W) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Figure 5

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

Figure 6

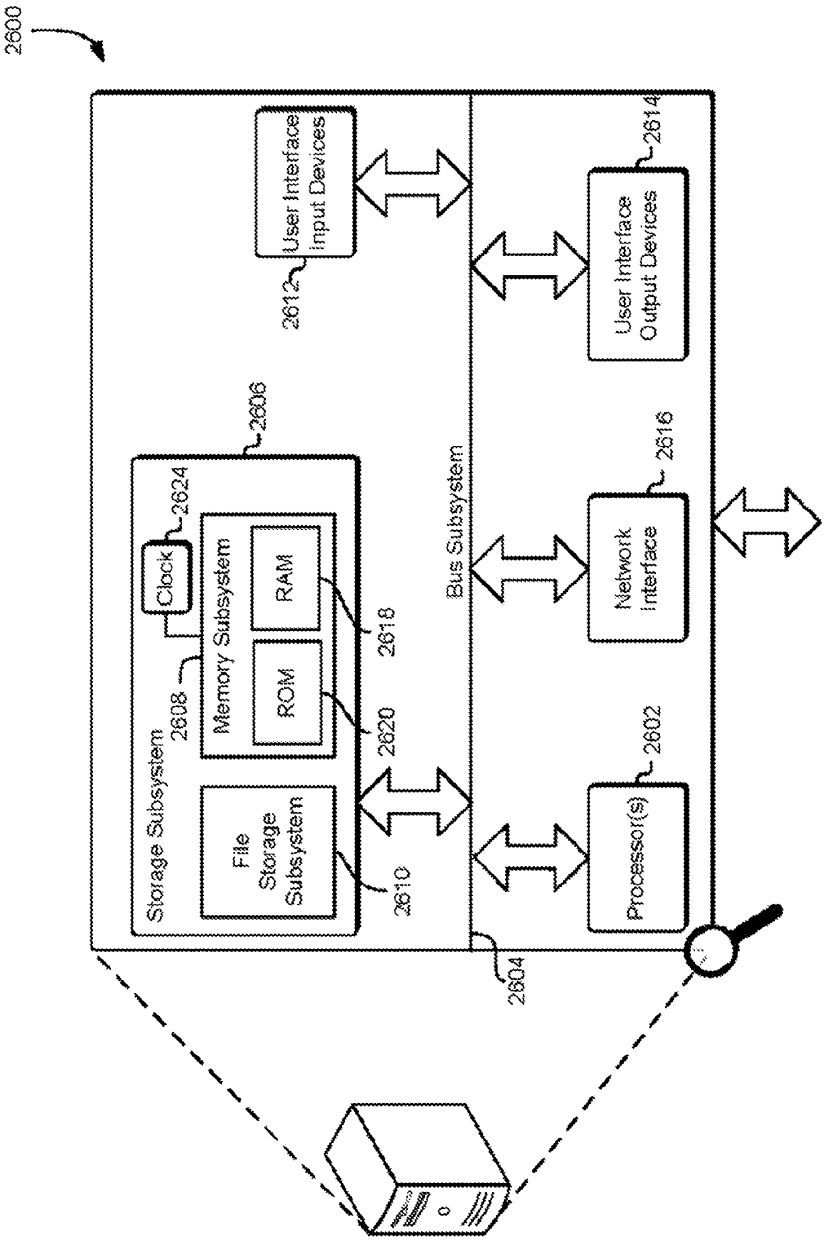


Figure 7