

FIGURE 1

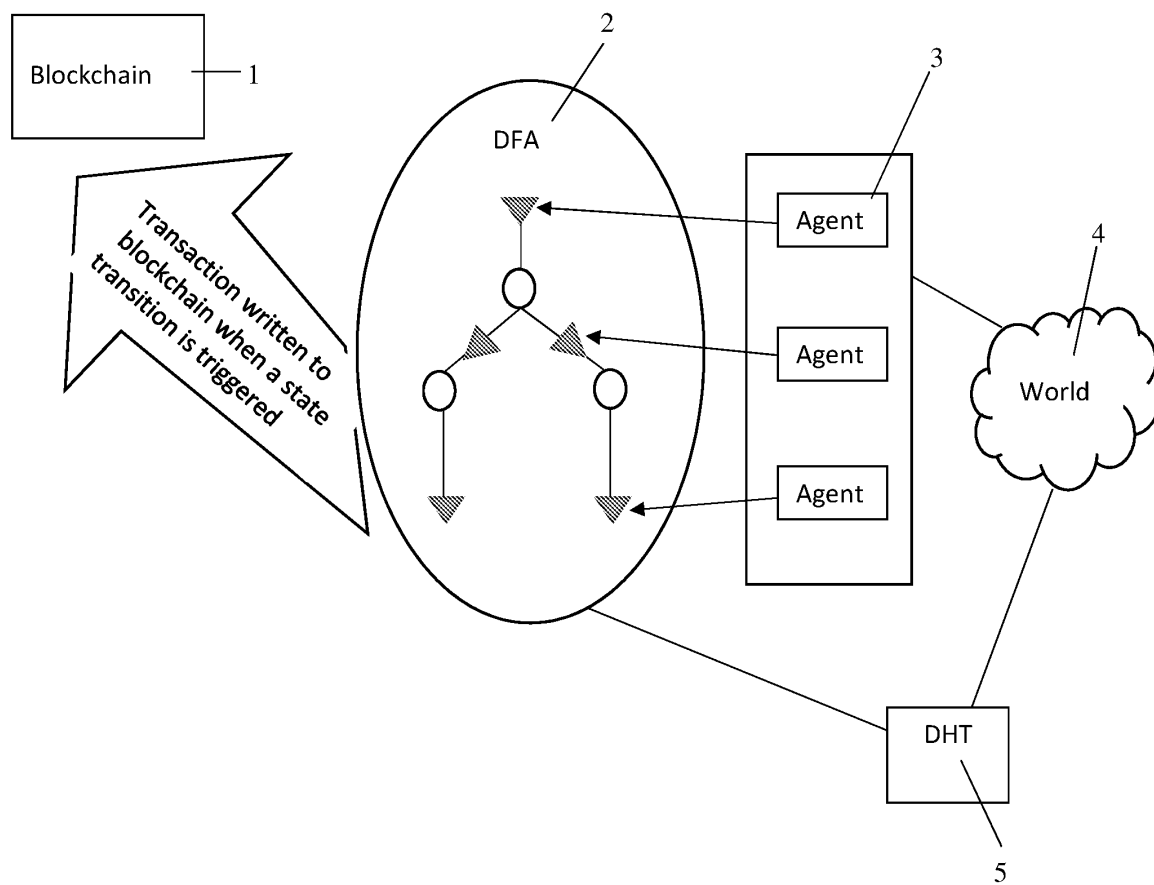


FIGURE 2

Figure 2 provides an illustrative embodiment of the invention wherein a smart contract is executed as a DFA implemented on a blockchain using P2PKH Transactions to represent the states that are triggered and entered.

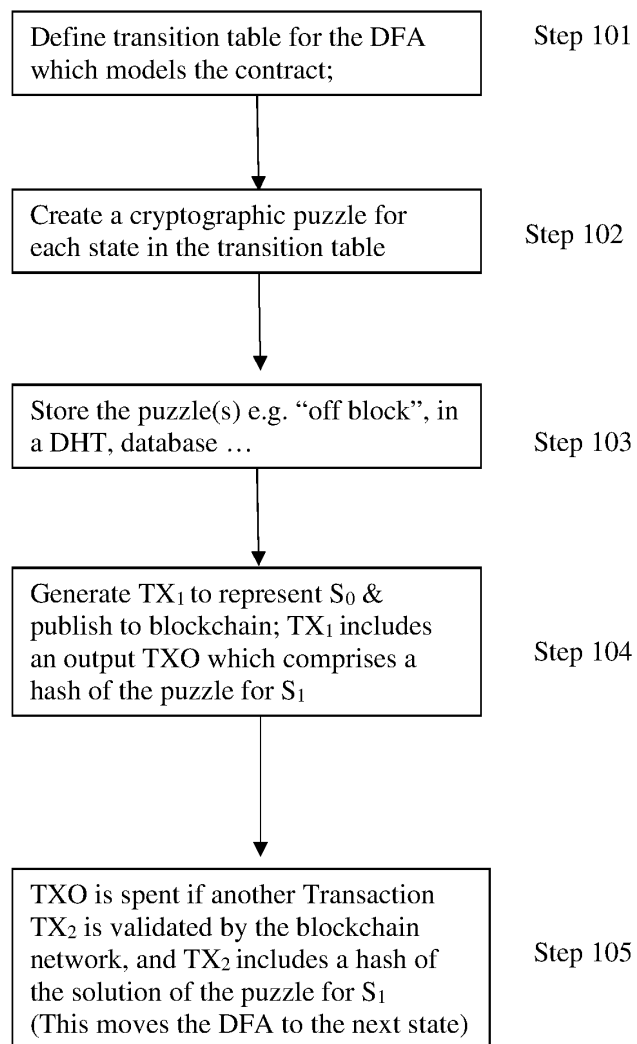


FIGURE 3

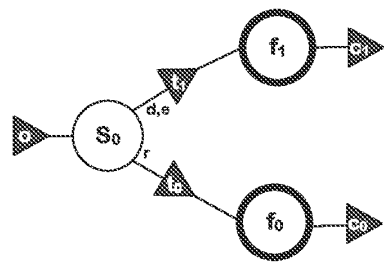


Diagram describing a blockchain-based DFA for a zero-coupon bond contract.

FIGURE 4

Transaction identifier			origination <i>o</i>
Version number			<version number>
Number of inputs			1
Input	Previous transaction	Hash	<10 mBTC from originator>
		Output index	00
	Length of signature script		<unlocking script length>
	Signature script		<originator signature> <originator public key>
	Sequence number		<sequence number>
Number of outputs			2
Output 0	Value		600000
	Length of public key script		<locking script length>
	Public key script		OP_HASH256 <state <i>s</i> ₀ puzzle> OP_EQUAL
Output 1	Value		300000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <Botnet agent public key hash> OP_EQUALVERIFY OP_CHECKSIG
Locktime			0

FIGURE 5

Transaction identifier			transition t_f
Version number			<version number>
Number of inputs			1
Input	Previous transaction	Hash	<6 mBTC from origination o >
		Output index	00
	Length of signature script		<unlocking script length>
	Signature script		<state s_e puzzle solution>
	Sequence number		<sequence number>
Number of outputs			2
Output 0	Value		400000
	Length of public key script		<locking script length>
	Public key script		OP_HASH256 <state f_f puzzle> OP_EQUAL
Output 1	Value		100000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <Botnet agent public key hash> OP_EQUALVERIFY OP_CHECKSIG
Locktime			0

FIGURE 6

Transaction identifier			completion c_f
Version number			<version number>
Number of inputs			1
Input	Previous transaction	Hash	<4 mBTC from transition t_f >
		Output index	00
	Length of signature script		<unlocking script length>
	Signature script		<state f_f puzzle solution>
	Sequence number		<sequence number>
Number of outputs			2
Output 0	Value		100000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <originator public key hash> OP_EQUALVERIFY OP_CHECKSIG
Output 1	Value		200000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <Botnet agent public key hash> OP_EQUALVERIFY OP_CHECKSIG
Locktime			0

FIGURE 7

Transaction identifier			origination o
Version number			<version number>
Number of inputs			1
Input	Previous transaction	Hash	<10 mBTC from originator>
		Output index	00
	Length of signature script		<unlocking script length>
	Signature script		<originator signature> <originator public key>
	Sequence number		<sequence number>
Number of outputs			2
Output 0	Value		600000
	Length of public key script		<locking script length>
	Public key script		OP_HASH160 <state s_0 redeem script hash> OP_EQUAL
Output 1	Value		300000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <Botnet agent public key hash> OP_EQUALVERIFY OP_CHECKSIG
Locktime			0

FIGURE 8

Transaction identifier			transition t_f
Version number			<version number>
Number of inputs			1
Input	Previous transaction	Hash	<6 mBTC from origination o >
		Output index	00
	Length of signature script		<unlocking script length>
	Signature script		OP_0 <Botnet agent signature> <state s_0 redeem script>
	Sequence number		<sequence number>
Number of outputs			2
Output 0	Value		400000
	Length of public key script		<locking script length>
	Public key script		OP_HASH160 <state f_f redeem script hash> OP_EQUAL
Output 1	Value		100000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <Botnet agent public key hash> OP_EQUALVERIFY OP_CHECKSIG
Locktime			0

FIGURE 9

Transaction identifier			completion c_f
Version number			<version number>
Number of inputs			1
Input	Previous transaction	Hash	<4 mBTC from transition t_f >
		Output index	00
	Length of signature script		<unlocking script length>
	Signature script		OP_0 <Botnet agent signature> <state f_f redeem script>
	Sequence number		<sequence number>
Number of outputs			2
Output 0	Value		100000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <originator public key hash> OP_EQUALVERIFY OP_CHECKSIG
Output 1	Value		200000
	Length of public key script		<locking script length>
	Public key script		OP_DUP OP_HASH160 <Botnet agent public key hash> OP_EQUALVERIFY OP_CHECKSIG
Locktime			0

FIGURE 10

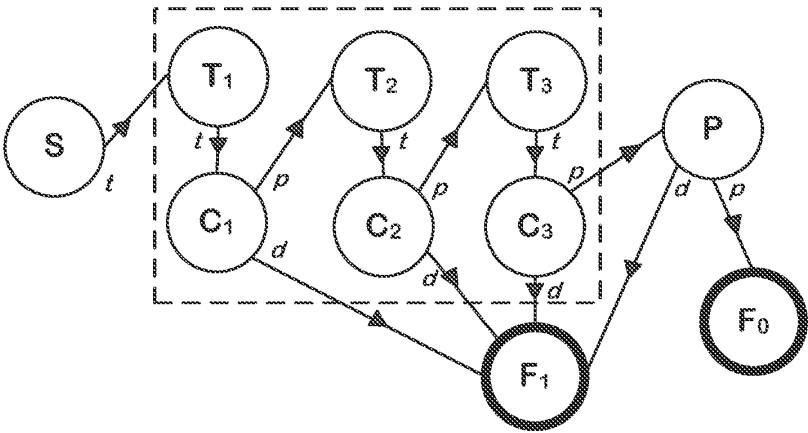


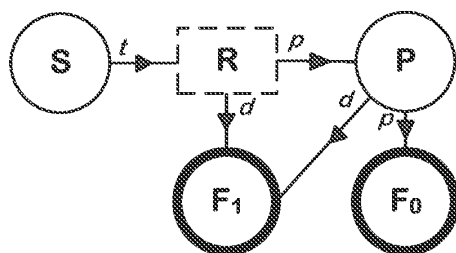
FIGURE 11

Figure 11: State diagram of the coupon bond with a recurrent state.

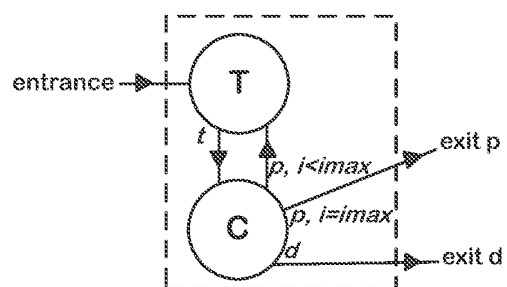
FIGURE 12

Figure 13

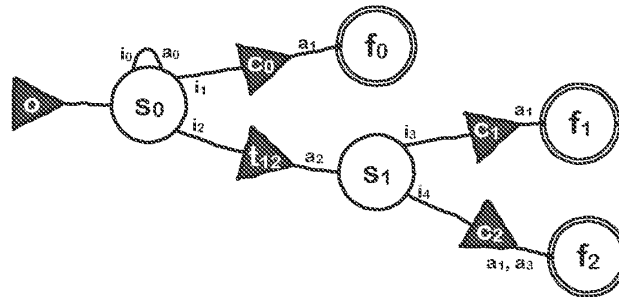


Figure 13: State diagram for a European call option example of the “compilation and execution” section of the application, showing the states (blobs) and the blockchain transactions (triangles) to be submitted: origination (o), transitions (t) and completions (c).