

Figure 1

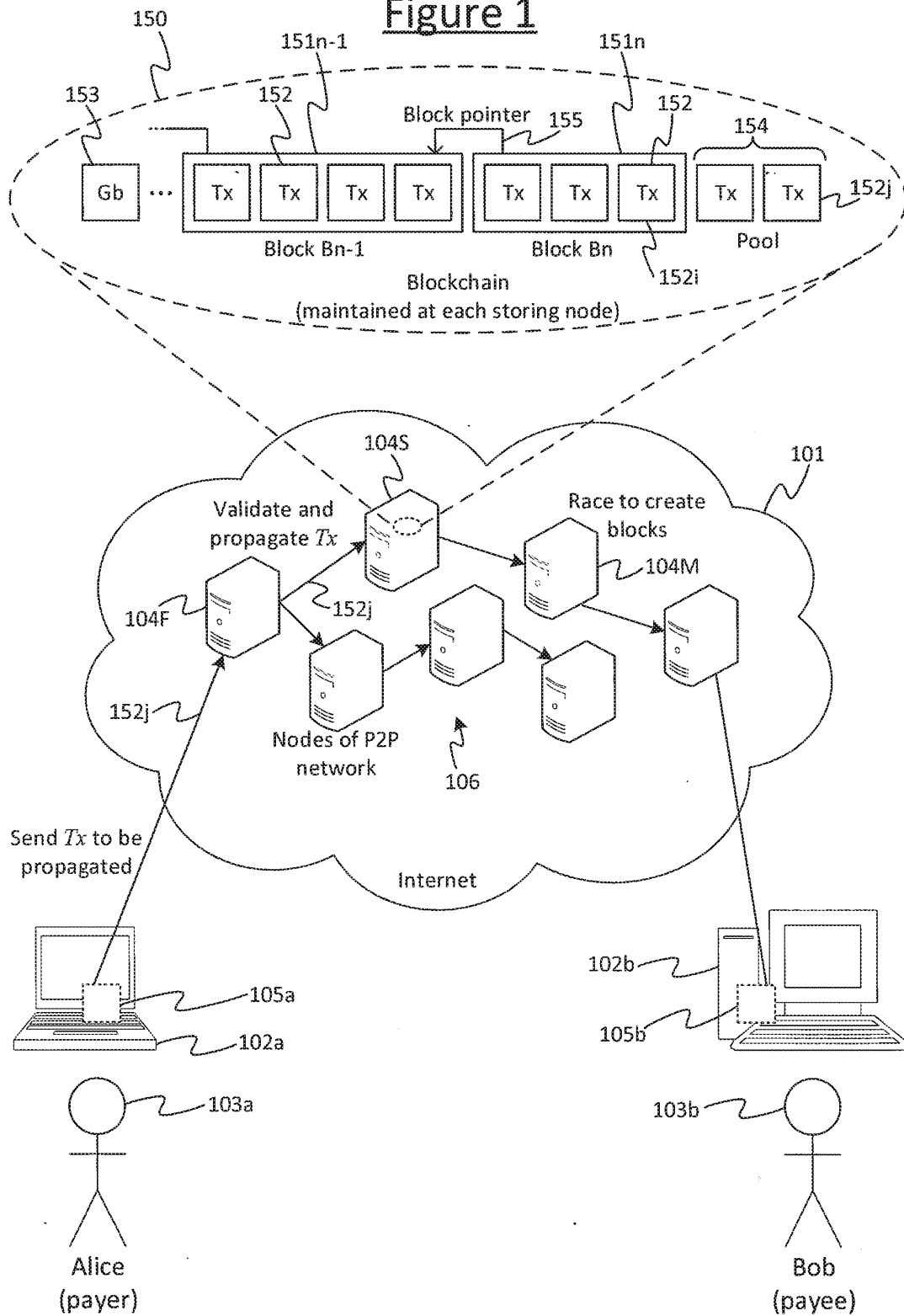
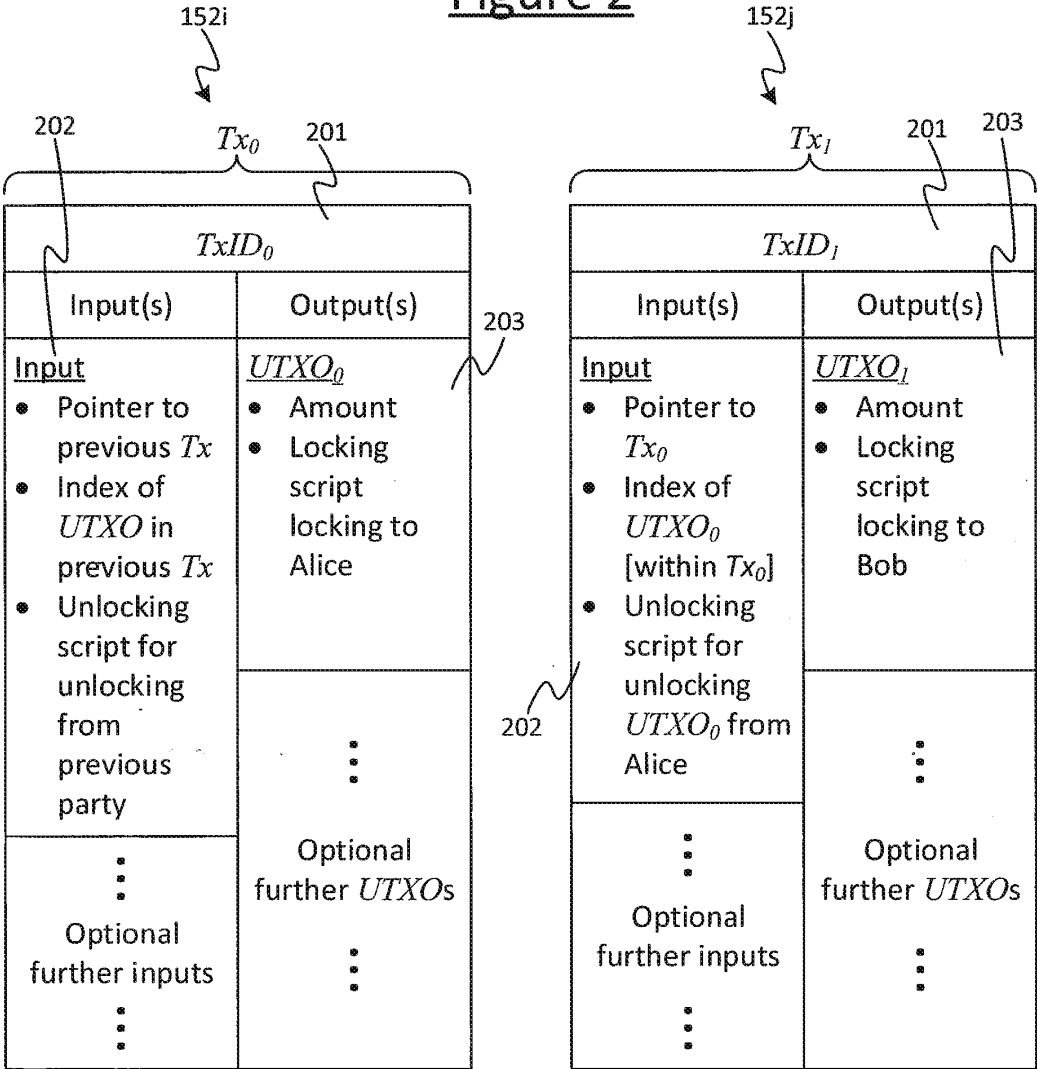


Figure 2



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.

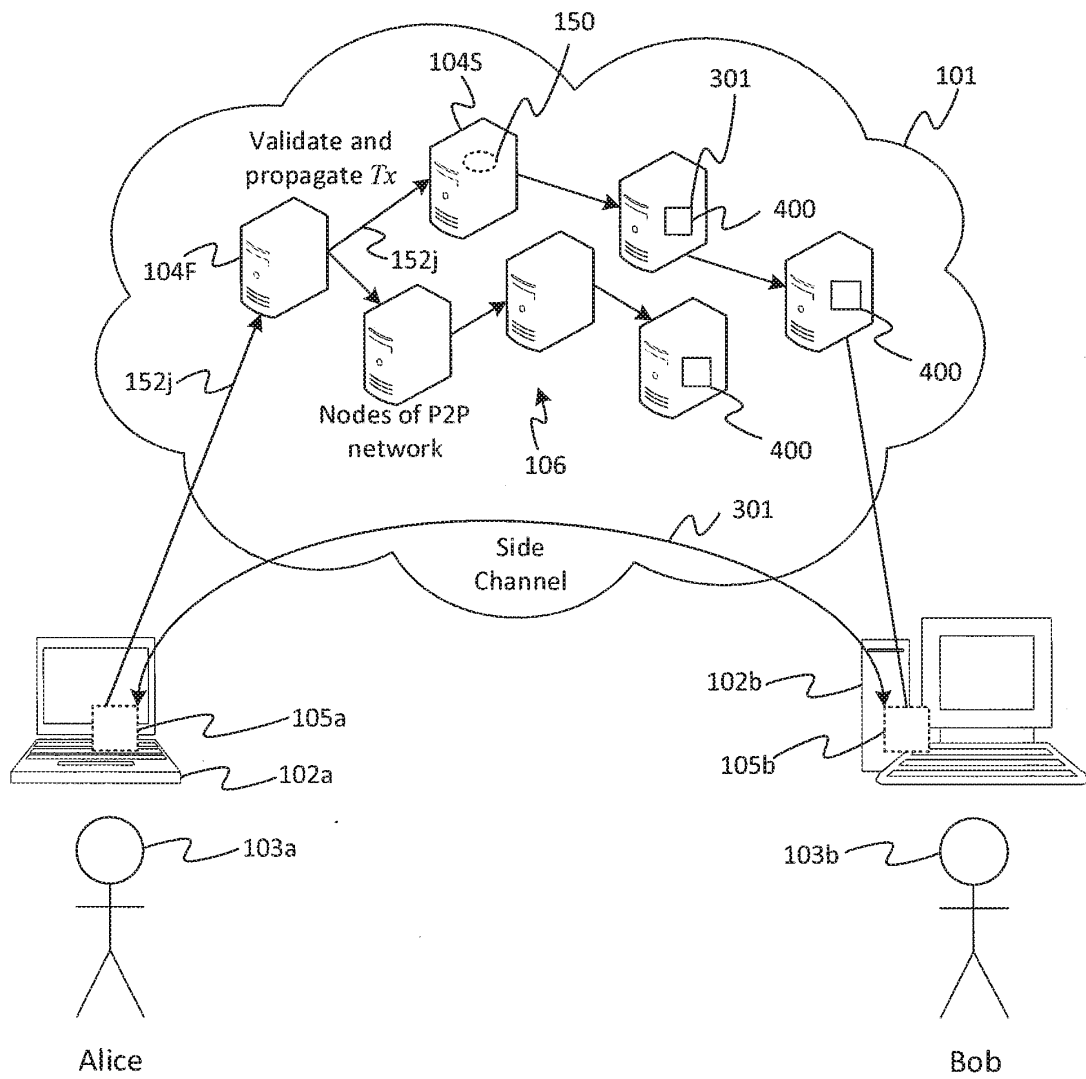
Figure 3

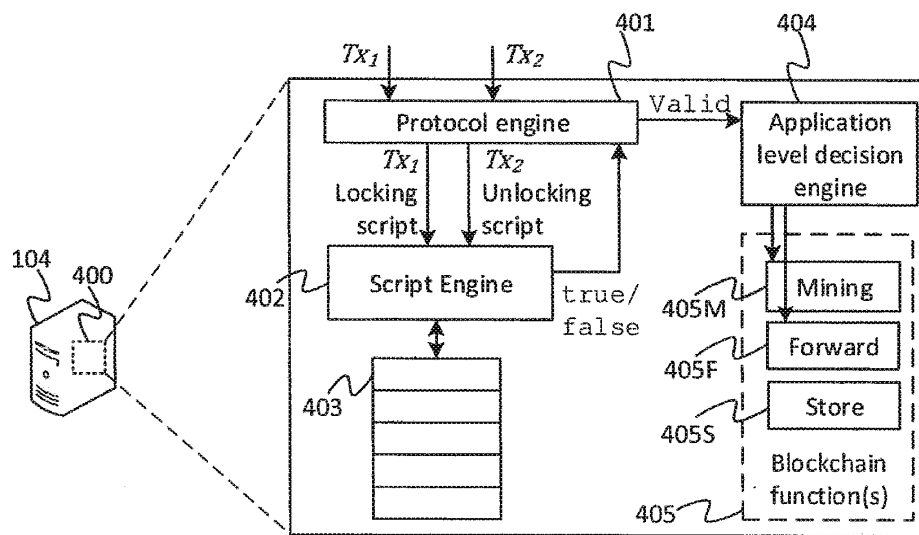
Figure 4

Figure 5

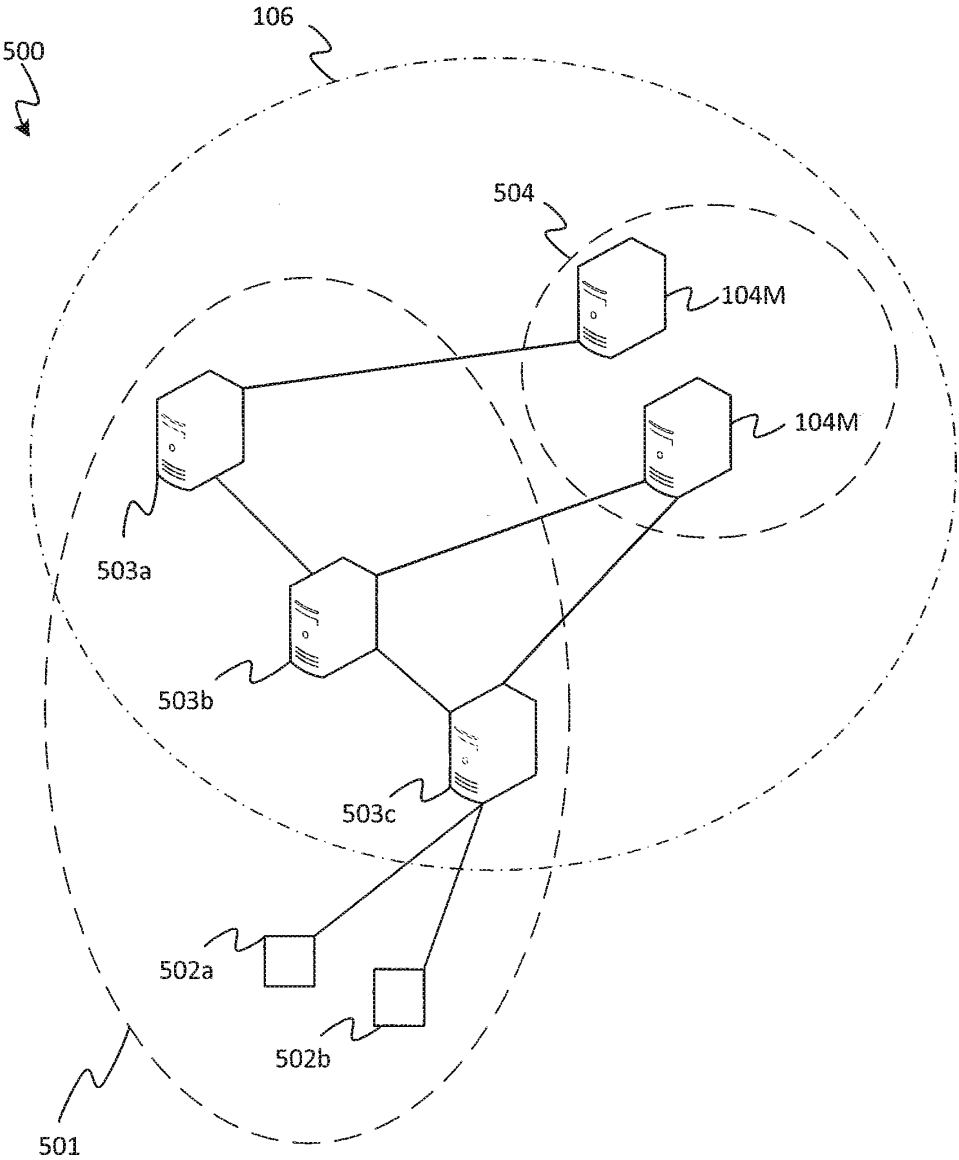


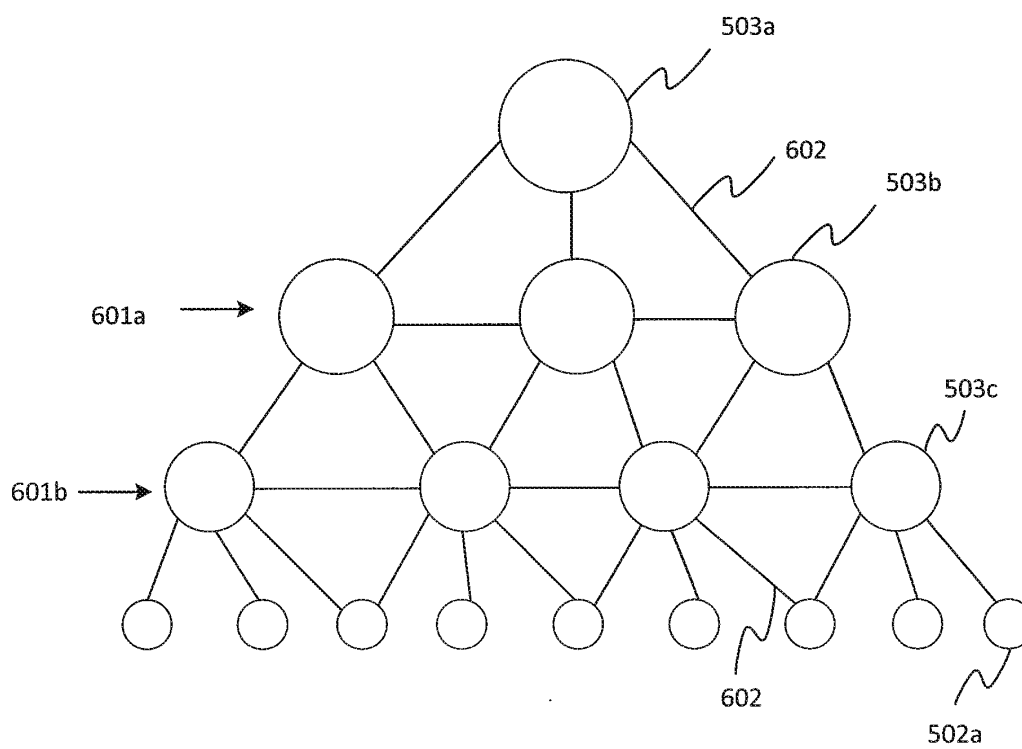
Figure 6

Figure 7a

Tx ₁ (partial)			
Inputs		Outputs	
Value		Value	
x	< Sig _{PK0} > < PK ₀ >	0	OP_FALSE OP_RETURN 0x4d494f54 < Command data >

701a

702a

Figure 7b

Tx ₁ (complete)			
Inputs		Outputs	
Value		Value	
x	< Sig _{PK0} > < PK ₀ >	0	OP_FALSE OP_RETURN 0x4d494f54 < Command data >
> 0	< Sig _{PK1} > < PK ₁ >	x	OP_DUP OP_HASH160 < H ₁₆₀ (PK ₁) > OP_EQUALVERIFY OP_CHECKSIG

701b

702b

Figure 8a

Tx_I (partial)			
Inputs		Outputs	
Value		Value	
x	$\langle Sig_{PK0} \rangle \langle PK_0 \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 $\langle Command\ data \rangle$
		$x + \delta$	OP_DUP OP_HASH160 $\langle H_{160}(PK_1) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

801a

802b

802a

Figure 8b

Tx_I (complete)			
Inputs		Outputs	
Value		Value	
x	$\langle Sig_{PK0} \rangle \langle PK_0 \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 $\langle Command\ data \rangle$
$> \delta$	$\langle Sig_{PK1} \rangle \langle PK_1 \rangle$	x	OP_DUP OP_HASH160 $\langle H_{160}(PK_1) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

801b

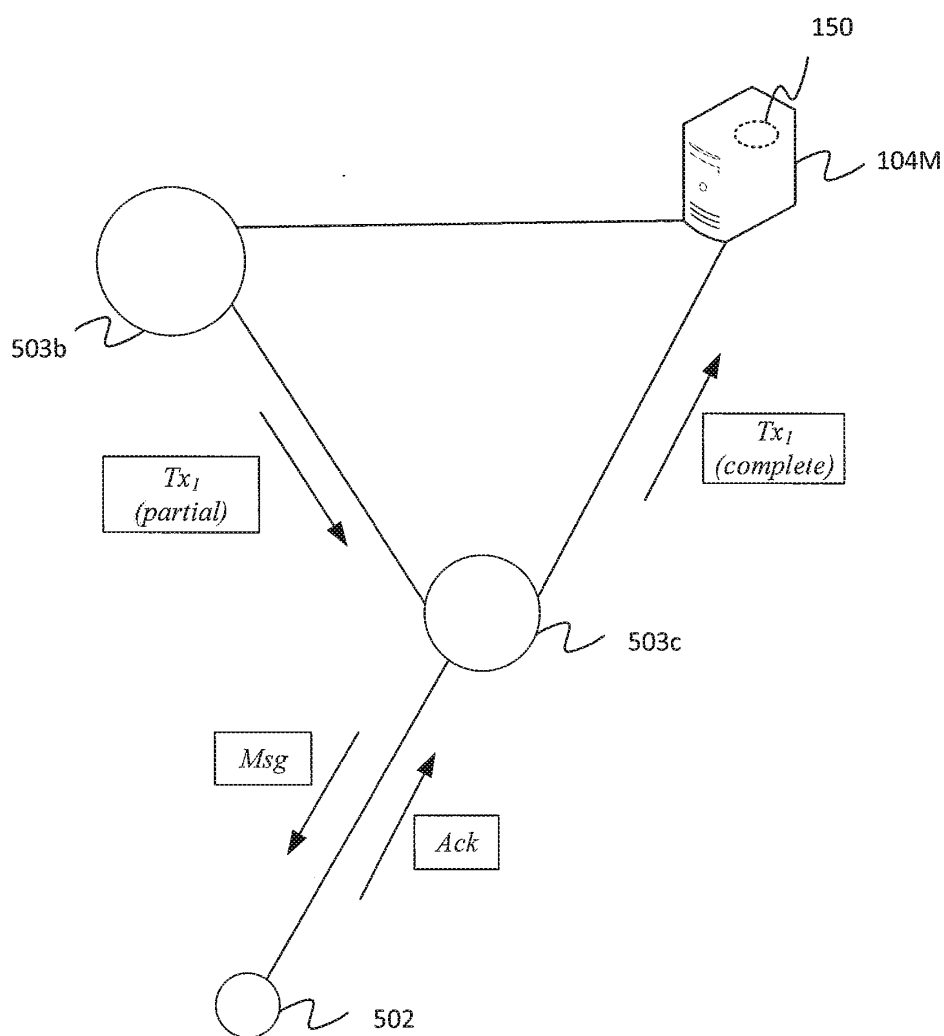
Figure 9

Figure 10a

Tx_I (partial)			
Inputs		Outputs	
Value		Value	
x	$\langle Sig_{PK_{serv}} \rangle \langle PK_{serv} \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 $\langle Command\ data \rangle$
		$x + \delta$	OP_DUP OP_HASH160 $\langle H_{160}(PK_{slave}) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Figure 10b

Tx_I (complete)			
Inputs		Outputs	
Value		Value	
x	$\langle Sig_{PK_{serv}} \rangle \langle PK_{serv} \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 $\langle Command\ data \rangle$
$> \delta$	$\langle Sig_{PK_{slave}} \rangle \langle PK_{slave} \rangle$	x	OP_DUP OP_HASH160 $\langle H_{160}(PK_{slave}) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Figure 11a

Tx ₁ (request)			
Inputs		Outputs	
Value		Value	
x ₁	< Sig _{PK0} > < PK ₀ >	0	OP_FALSE OP_RETURN 0x4d494f54 < Command data >
		y ₁	OP_2 OP < PK ₁ > < PK ₂ > OP_CHECKMULTISIG

1101a

Figure 11b

1102b

1102a

Tx ₂ (approval)			
Inputs		Outputs	
Value		Value	
x ₂	< Sig _{PK1} > < PK ₁ > < Sig _{PK2} > < PK ₂ >	0	OP_FALSE OP_RETURN 0x4d494f54 < Command data >
		y ₂	OP_DUP OP_HASH160 < H ₁₆₀ (PK ₃) > OP_EQUALVERIFY OP_CHECKSIG

1101b

1102c

Figure 12a

Tx_I (partial)			
Inputs		Outputs	
Value		Value	
x	$\langle Sig_{PK_{serv_0}} \rangle \langle PK_{serv_0} \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 OP_PUSHDATA1 [Payload length] $\langle BIE1 \text{ Encrypted command data} \rangle$ OP_PUSHDATA1 [Payload length] $\langle BIE1 \text{ Encrypted Encryption key} \rangle$
		$x + \delta$	OP_DUP OP_HASH160 $\langle H_{160}(PK_{slave_0}) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Figure 12b

Tx_I (complete)			
Inputs		Outputs	
Value		Value	
x	$\langle Sig_{PK_{serv_0}} \rangle \langle PK_{serv_0} \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 OP_PUSHDATA1 [Payload length] $\langle BIE1 \text{ Encrypted command data} \rangle$ OP_PUSHDATA1 [Payload length] $\langle BIE1 \text{ Encrypted Encryption key} \rangle$
$> \delta$	$\langle Sig_{PK_{slave_1}} \rangle \langle PK_{slave_1} \rangle$	$x + \delta$	OP_DUP OP_HASH160 $\langle H_{160}(PK_{slave_0}) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Figure 13

Outputs	
Value	
0	OP_FALSE OP_RETURN OP_PUSHDATA1 0x4d494f54 – <i>IoT protocol identifier</i> 0x01 – <i>Payload type</i> 0x00000001 – <i>IoT software version number</i> 0x3dd5dfac...32 – <i>Device ID</i> 0x234a3789...22 – <i>Device Pubkey</i> 0x4d348912...87 – <i>Device certificate location data</i> 0x3ad21fac – <i>Command</i> 0x5665b456 – <i>Status</i> 0x5665b456 – <i>Previous status</i>

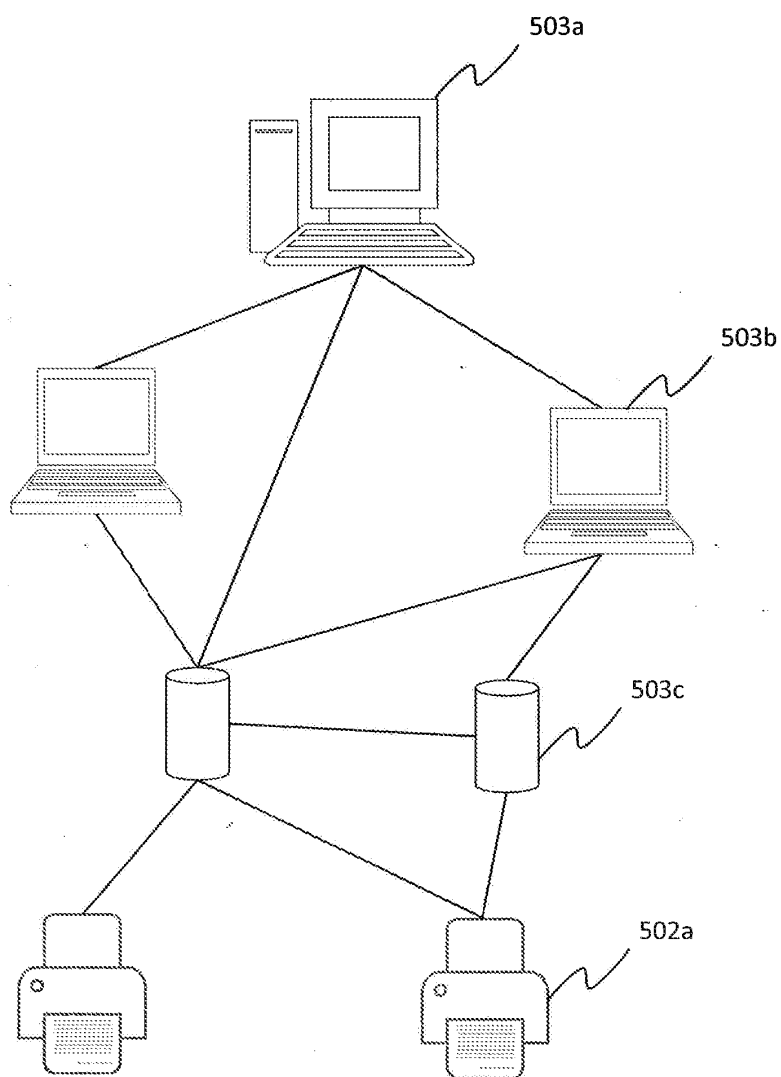
Figure 14

Figure 15a

Tx_1 (certificate)			
Inputs		Outputs	
Value		Value	
x_1	$\langle Sig_{PK_{admin}} \rangle \langle PK_{admin} \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 $\langle Certificate\ data \rangle$
		y_1	OP_DUP OP_HASH160 $\langle H_{160}(PK_{admin}) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Figure 15b

Tx_1 (partial)			
Inputs		Outputs	
Value		Value	
x_2	$\langle Sig_{PK_{laptop_0}} \rangle \langle PK_{laptop_0} \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 $\langle Encrypted\ Command\ data \rangle$
		y_2	OP_DUP OP_HASH160 $\langle H_{160}(PK_{controller_0}) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

Figure 15c

Tx ₁ (controller)			
Inputs		Outputs	
Value		Value	
x ₂	< Sig _{PK_{laptop},0} > < PK _{laptop} ,0 >	0	OP_FALSE OP_RETURN 0x4d494f54 < Encrypted Command data >
x ₃	< Sig _{PK_{controller},0} > < PK _{controller} ,0 >	y ₂	OP_DUP OP_HASH160 < H ₁₆₀ (PK _{controller} ,0) > OP_EQUALVERIFY OP_CHECKSIG

Figure 16a

Tx_I (certificate)			
Inputs		Outputs	
Value		Value	
x_I	$\langle Sig_{PK_{reg}} \rangle \langle PK_{reg} \rangle$	0	OP_FALSE OP_RETURN 0x4d494f54 $\langle Certificate\ data \rangle$
		y_I	OP_DUP OP_HASH160 $\langle H_{160}(PK_{reg}) \rangle$ OP_EQUALVERIFY OP_CHECKSIG

1501a

1502b

1502a

Figure 16b

Outputs	
Value	
0	OP_FALSE OP_RETURN OP_PUSHDATAI $\langle payload\ length \rangle$ 0x4d494f54 – IoT protocol identifier 0x02 – Payload type 0x00000001 – IoT software version number 0x3dd5dfac...32 – New device ID 0x234a3789...22 – New device Compressed Pubkey 0x3ad21fac – Device type 0x00000004 – Device IoT node type 0x0000...06f – IPv6 address and port number 0x5664b456 – UNIX time creation date 0x5665b456 – UNIX time certificate expiry date 0x76d5335c.....45 – Additional information