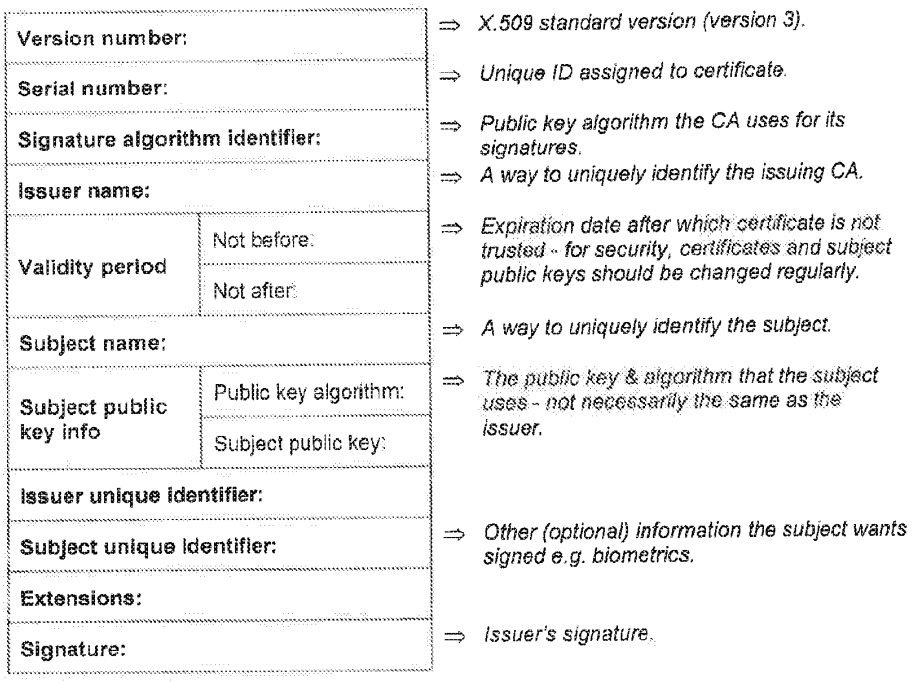

Version number:
⇒ X.509 standard version (version 3).
Serial number:
⇒ Unique ID assigned to certificate.
Signature algorithm identifier:
⇒ Public key algorithm the CA uses for its signatures.
Issuer name:
⇒ A way to uniquely identify the issuing CA.
Validity period
Not before:
Not after:
⇒ Expiration date after which certificate is not trusted - for security, certificates and subject public keys should be changed regularly.
Subject name:
⇒ A way to uniquely identify the subject.
Subject public key info
Public key algorithm:
Subject public key:
⇒ The public key & algorithm that the subject uses - not necessarily the same as the issuer.
Issuer unique identifier:
Subject unique identifier:
⇒ Other (optional) information the subject wants signed e.g. biometrics.
Extensions:
Signature:
⇒ Issuer's signature.

FIGURE 1

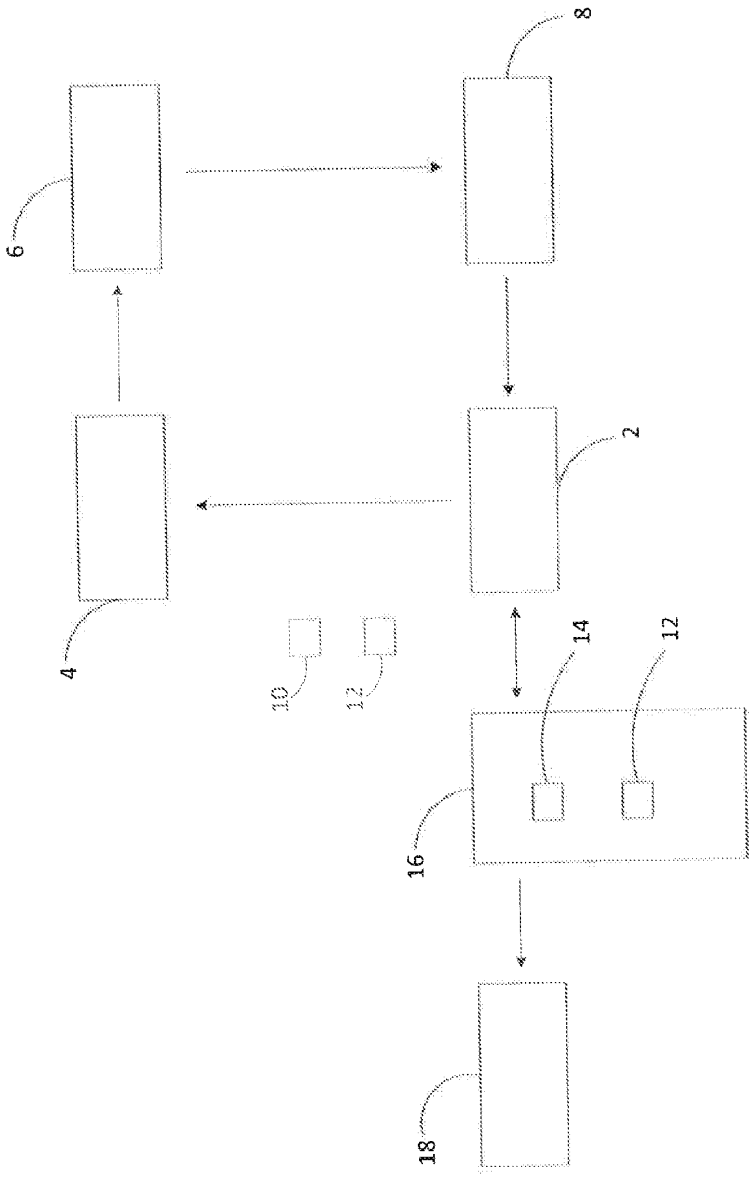


FIGURE 2

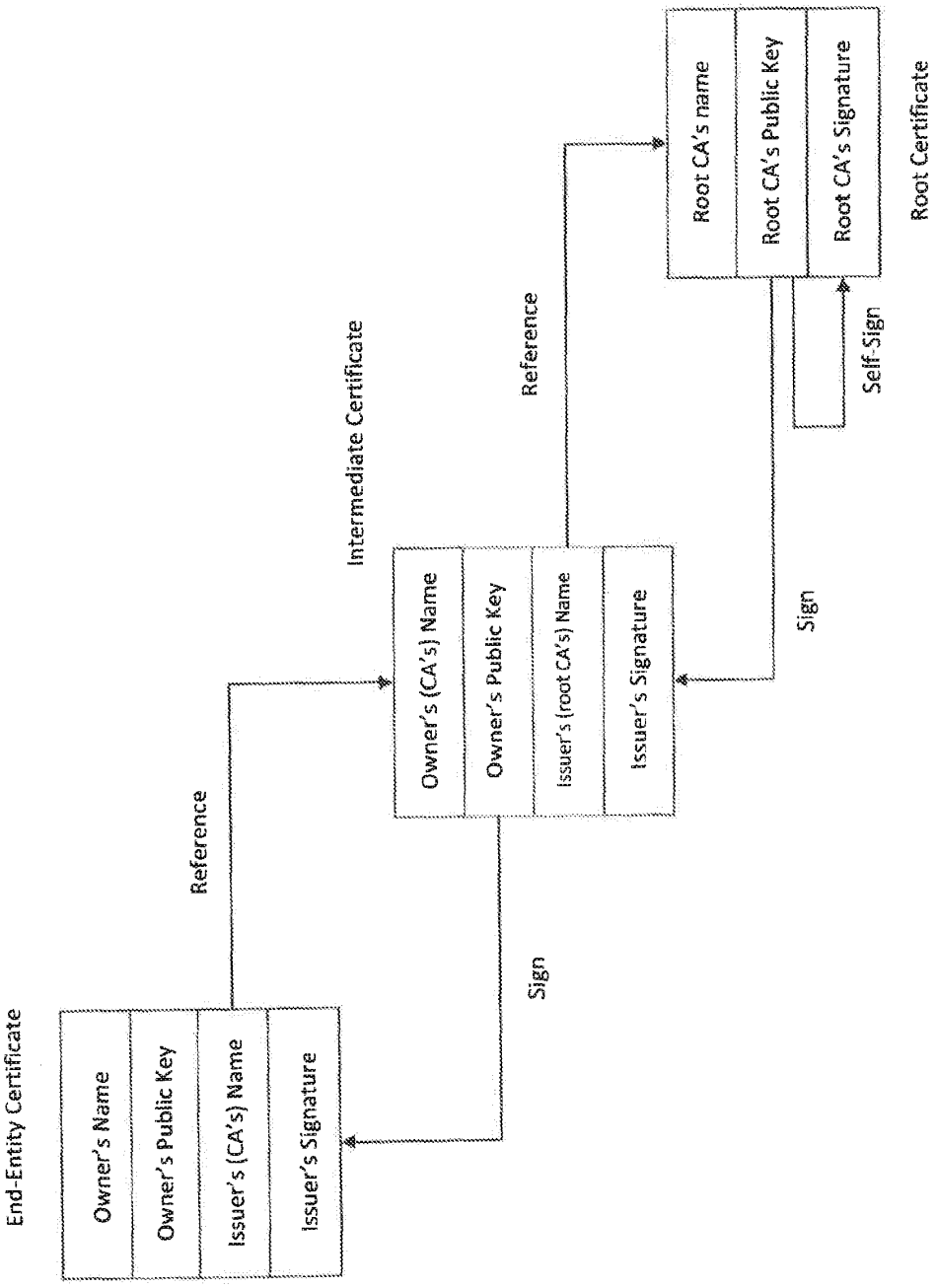

End-Entity Certificate
Owner's Name
Owner's Public Key
Issuer's (CA's) Name
Issuer's Signature
Reference
Sign
Intermediate Certificate
Owner's (CA's) Name
Owner's Public Key
Issuer's (root CA's) Name
Issuer's Signature
Reference
Sign
Root CA's name
Root CA's Public Key
Root CA's Signature
Self-Sign
Root Certificate

FIGURE 3

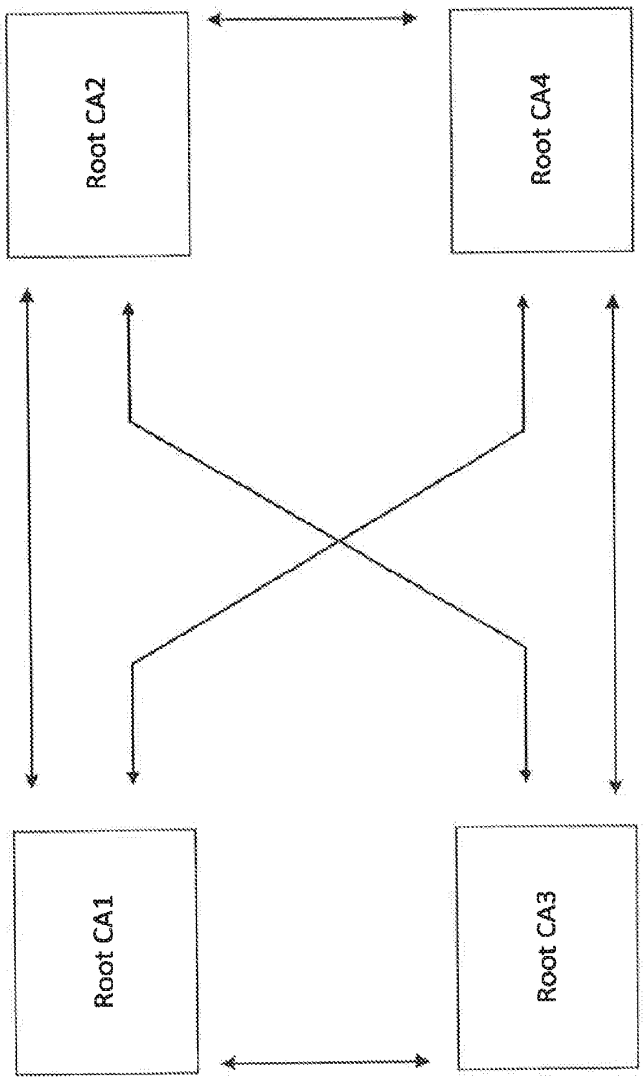


FIGURE 4

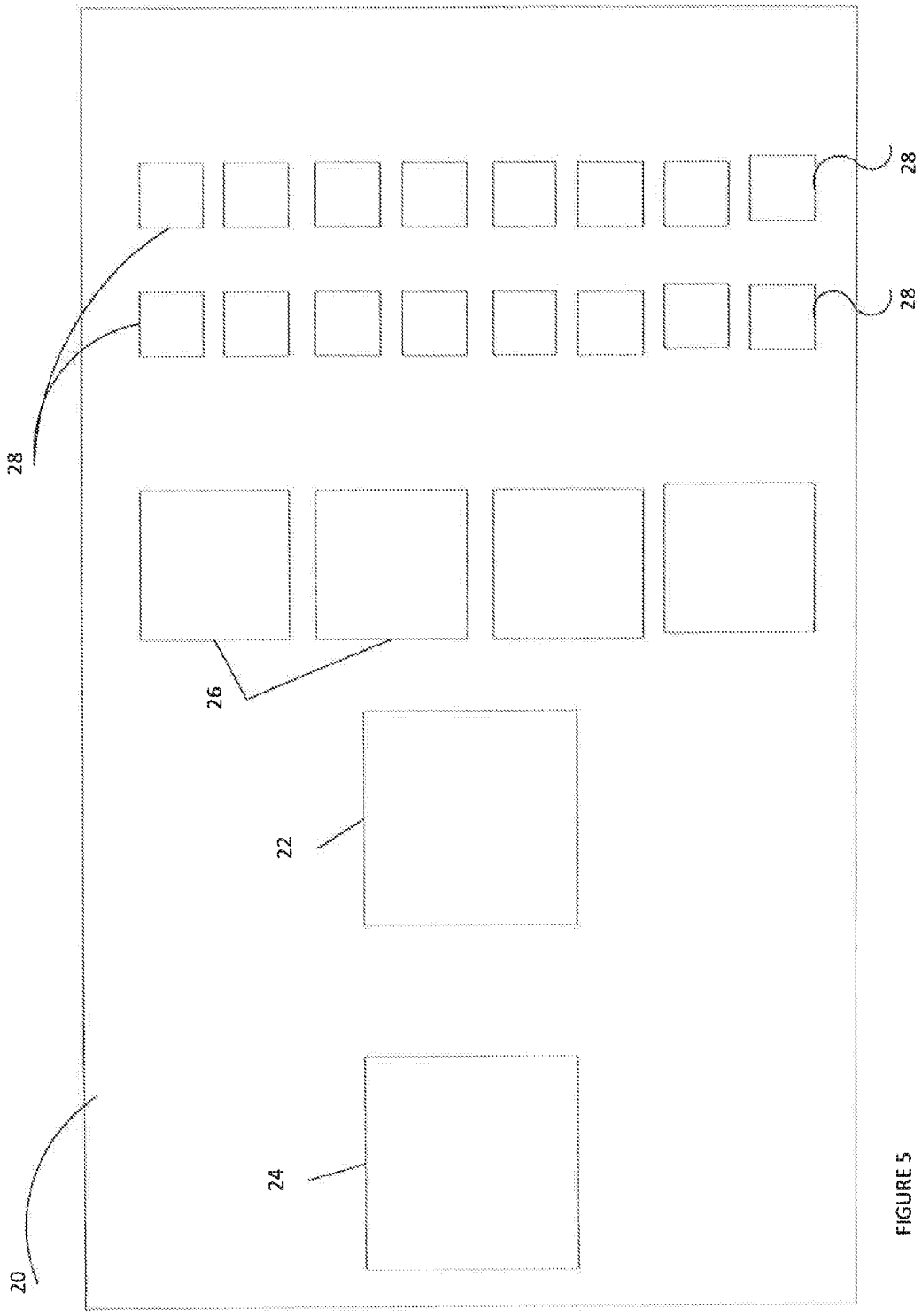


FIGURE 5

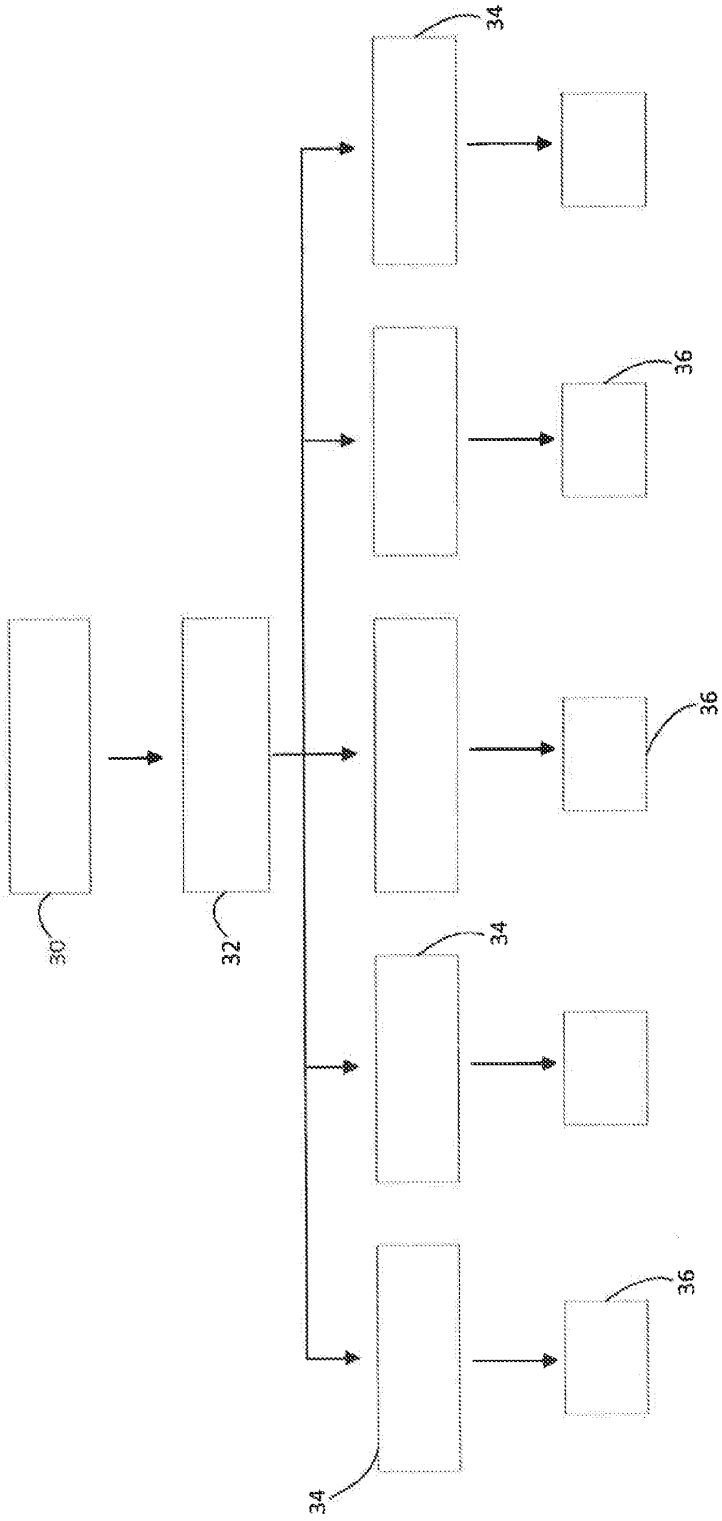


FIGURE 6

Prefix:		⇒ *Prefix (4 bytes) identifying the digital certificate.*
Serial number:		⇒ *Unique ID (32 bytes) assigned to certificate.*
Issuer name:		⇒ *CA's name (32 bytes).*
Issuer certificate location:	TxID:	⇒ *Location of the issuer's certificate containing the issuer's CA public key. The data comprises a transaction ID (32 bytes) and output number (4 bytes).*
	Vout:	
Intermediate certificate location:	TxID:	⇒ *Location of the intermediate certificate comprising a transaction ID (32 bytes) and output number (4 bytes).*
	Vout:	
Root certificate location:	TxID:	⇒ *Location of the Root certificate comprising a transaction ID (32 bytes) and output number (4 bytes).*
	Vout:	
Validity period	Not before:	⇒ *Expiration date (8 bytes each) after which certificate is not trusted - for security, certificates and subject public keys should be changed regularly.*
	Not after:	
Subject name:		⇒ *Name of person, group, company or other entity being certified (128 bytes). Encoded using ASCII.*
Subject public key:		⇒ *Public key of the subject (32 bytes).*
Subject device identifier:		⇒ *4-byte identifier (optional) for the device that holds the certified private/public key*
Subject unique identifier:		⇒ *32-byte identifier (optional) used by the issuing CA to represent the subject's identity.*
Extensions:		⇒ *Other (optional) information the subject wants signed e.g. biometrics, company logos, arbitrary messages (0-1024 bytes).*

FIGURE 7

Inputs		Outputs	
Value	Script	Value	Script
x BSV	$< PK_{CA}^{issue} > < SIG_{CA}^{issue} >$	y BSV	1. *UTXO Registration:* OP_DUP HASH160 $< PK_{CA}^{issue} >$ OP_EQUALVERIFY OP_CHECKSIG
		0 BSV	2. *X.509 Digital Certificate:* OP_RETURN$< CA \ll PK_A \gg >$

FIGURE 8

Inputs		Outputs	
Value	Script	Value	Script
x BSV	$< Output\ 1\ from\ TxID_{CTX-PK_A} >$	y BSV	1. *UTXO Registration:* OP_DUP HASH160 $< PK_{CA}^{Issue} >$ OP_EQUALVERIFY OP_CHECKSIG
		0 BSV	2. *X.509 Digital Certificate:* OP_RETURN$< CA \ll PK_{A-new} \gg >$

FIGURE 9

Inputs		Outputs	
Value	Script	Value	Script
x BSV	$< Output\ 1\ from\ TxID_{CTX-PK_A} >$	y BSV	1. *UTXO Registration:* <expiry time> OP_CHECKLOCKTIMEVERIFY OP_DROP OP_DUP HASH160 $< PK_{CA}^{Issue} >$ OP_EQUALVERIFY OP_CHECKSIG
		0 BSV	2. *X.509 Digital Certificate:* OP_RETURN $< CA \ll PK_{A-new} \gg >$

FIGURE 10

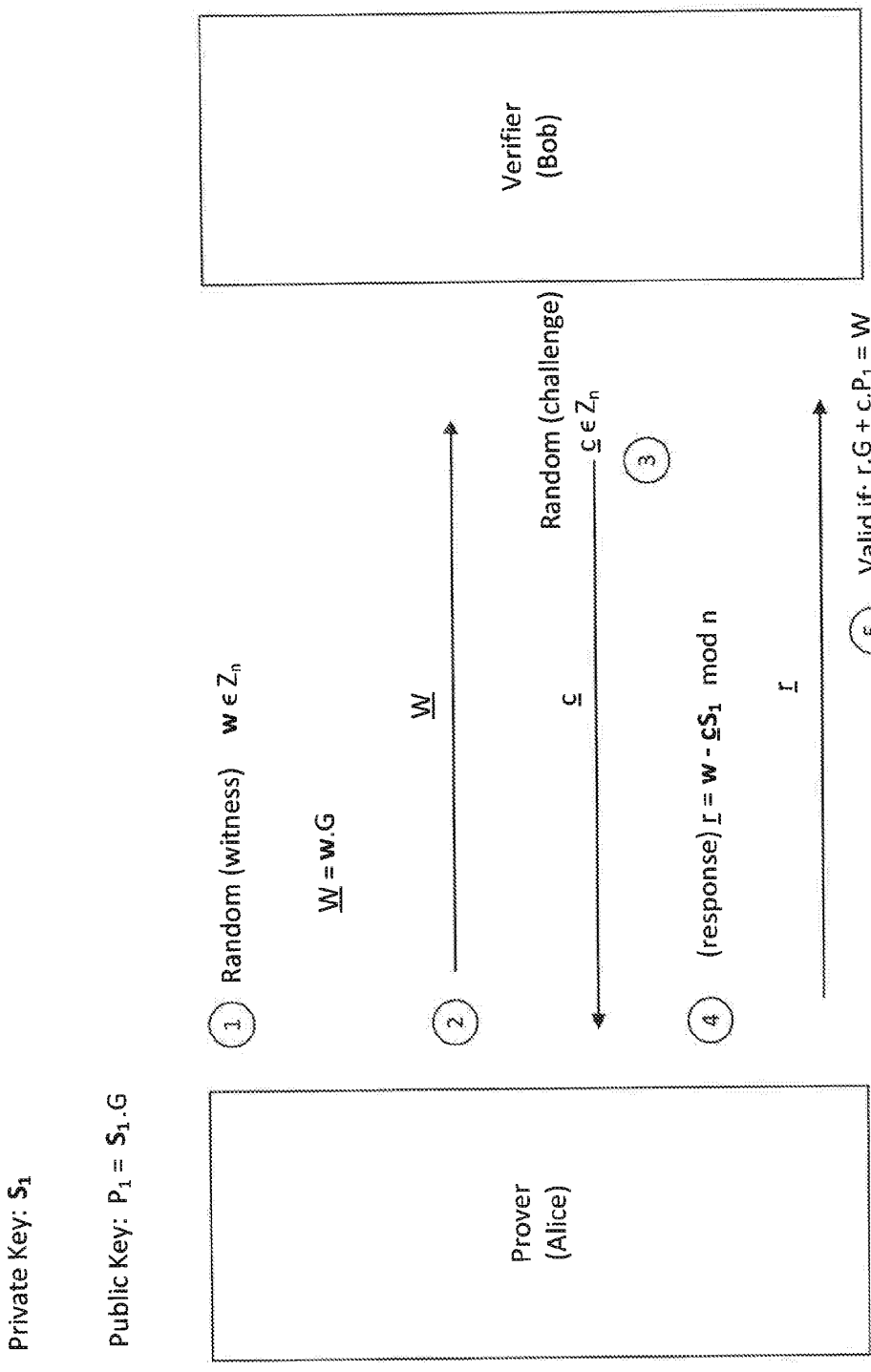

Private Key: s_1
Public Key: $P_1 = s_1.G$
Prover (Alice)
Verifier (Bob)
1 Random (witness) $w \in Z_n$
$W = w.G$
2 W
3 Random (challenge) $c \in Z_n$
c
4 (response) $r = w - cs_1 \mod n$
r
5 Valid iff: $r.G + c.P_1 = W$

FIGURE 11

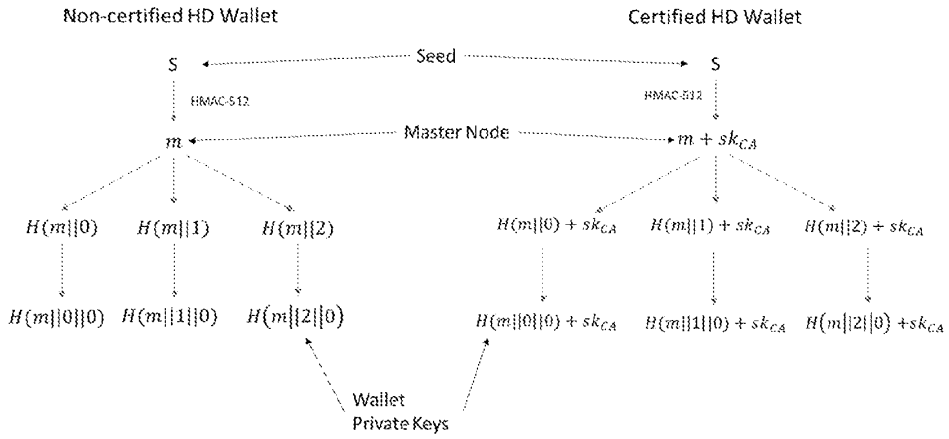

Non-certified HD Wallet
Certified HD Wallet
S
Seed
S
HMAC-512
HMAC-512
m
Master Node
m + sk_CA
H(m||0)
H(m||1)
H(m||2)
H(m||0) + sk_CA
H(m||1) + sk_CA
H(m||2) + sk_CA
H(m||0||0)
H(m||1||0)
H(m||2||0)
H(m||0||0) + sk_CA
H(m||1||0) + sk_CA
H(m||2||0) + sk_CA
Wallet
Private Keys

FIGURE 12

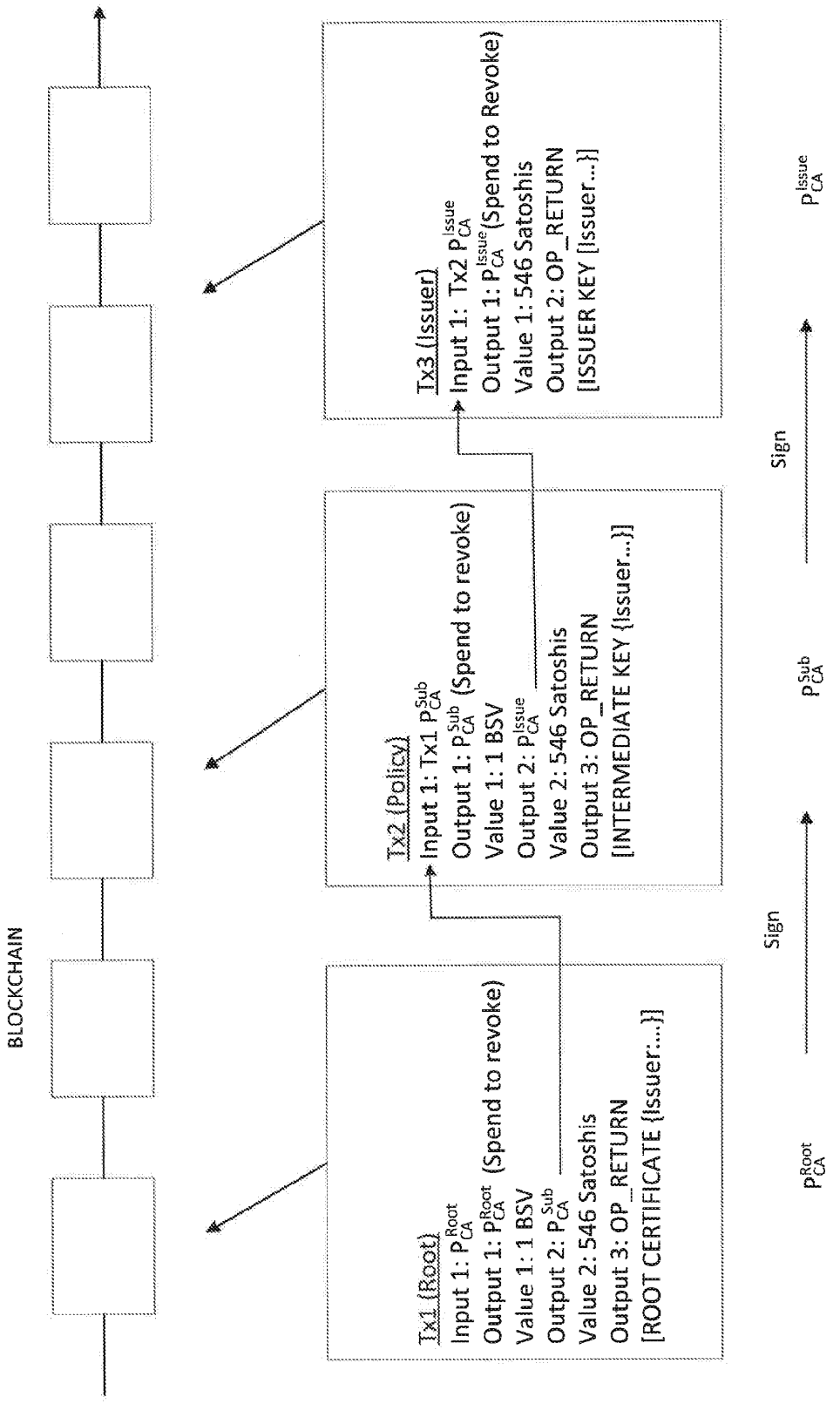

BLOCKCHAIN
Tx1 (Root)
Input 1: P_{CA}^{Root}
Output 1: P_{CA}^{Root} (Spend to revoke)
Value 1: 1 BSV
Output 2: P_{CA}^{Sub}
Value 2: 546 Satoshis
Output 3: OP_RETURN
[ROOT CERTIFICATE {Issuer:...}]
Tx2 (Policy)
Input 1: Tx1 P_{CA}^{Sub}
Output 1: P_{CA}^{Sub} (Spend to revoke)
Value 1: 1 BSV
Output 2: P_{CA}^{Issue}
Value 2: 546 Satoshis
Output 3: OP_RETURN
[INTERMEDIATE KEY {Issuer...}]
Tx3 (Issuer)
Input 1: Tx2 P_{CA}^{Issue}
Output 1: P_{CA}^{Issue} (Spend to Revoke)
Value 1: 546 Satoshis
Output 2: OP_RETURN
[ISSUER KEY [Issuer...]]
Sign
Sign
P_{CA}^{Root}
P_{CA}^{Sub}
P_{CA}^{Issue}

FIGURE 13

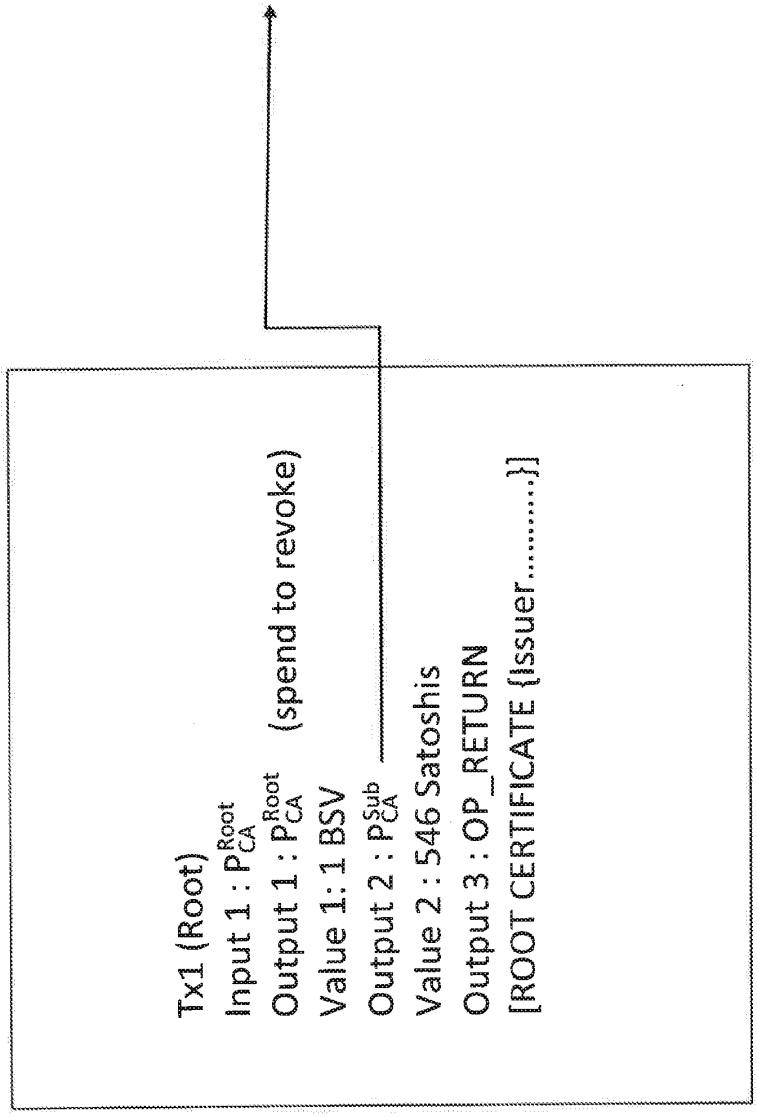

Tx1 (Root)
Input 1 : P_{CA}^{Root}
Output 1 : P_{CA}^{Root} (spend to revoke)
Value 1: 1 BSV
Output 2 : P_{CA}^{Sub}
Value 2 : 546 Satoshis
Output 3 : OP_RETURN
[ROOT CERTIFICATE {Issuer.....}]

FIGURE 14

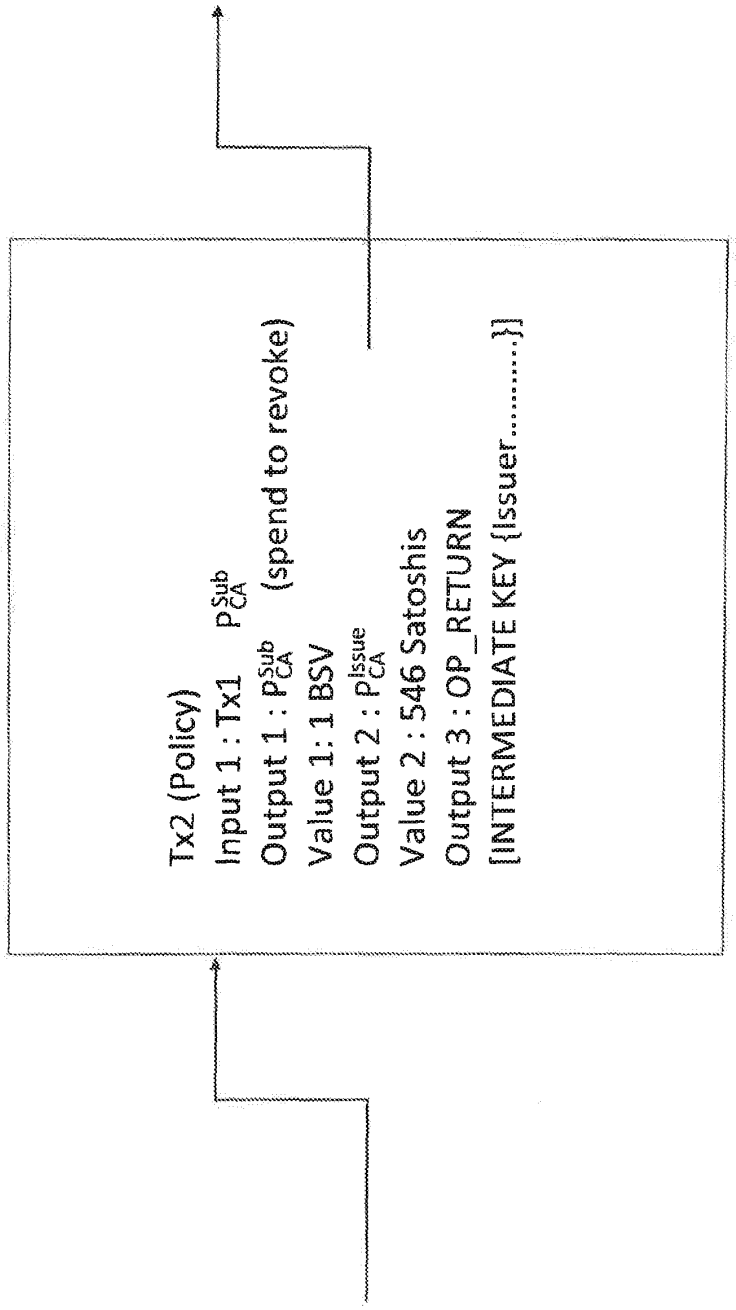

Tx2 (Policy)
Input 1 : Tx1 P_{CA}^{Sub}
Output 1 : P_{CA}^{Sub} (spend to revoke)
Value 1: 1 BSV
Output 2 : P_{CA}^{Issue}
Value 2 : 546 Satoshis
Output 3 : OP_RETURN
[INTERMEDIATE KEY {Issuer.....}]

FIGURE 15

PKI	Bitcoin blockchain PKI
Root certificate	OP_RETURN of TX1
Root CA's name	OP_RETURN of TX1
Signature for root certificate	Signature in input 1 of TX1
Signature for subordinate key	Signature in input 1 of TX1
Intermediate certificate	OP_RETURN of TX2
Reference to Root CA	Input 1 of TX2 spends output 2 of TX1
Signature for issuing key	Signature in input 1 of TX2
Issuer certificate	OP_RETURN of TX3
Reference to intermediate certificate	Input 1 of TX3 spends output 2 of TX2
Sub-fields within each certificate	Included in OP_RETURN payload data

FIGURE 16

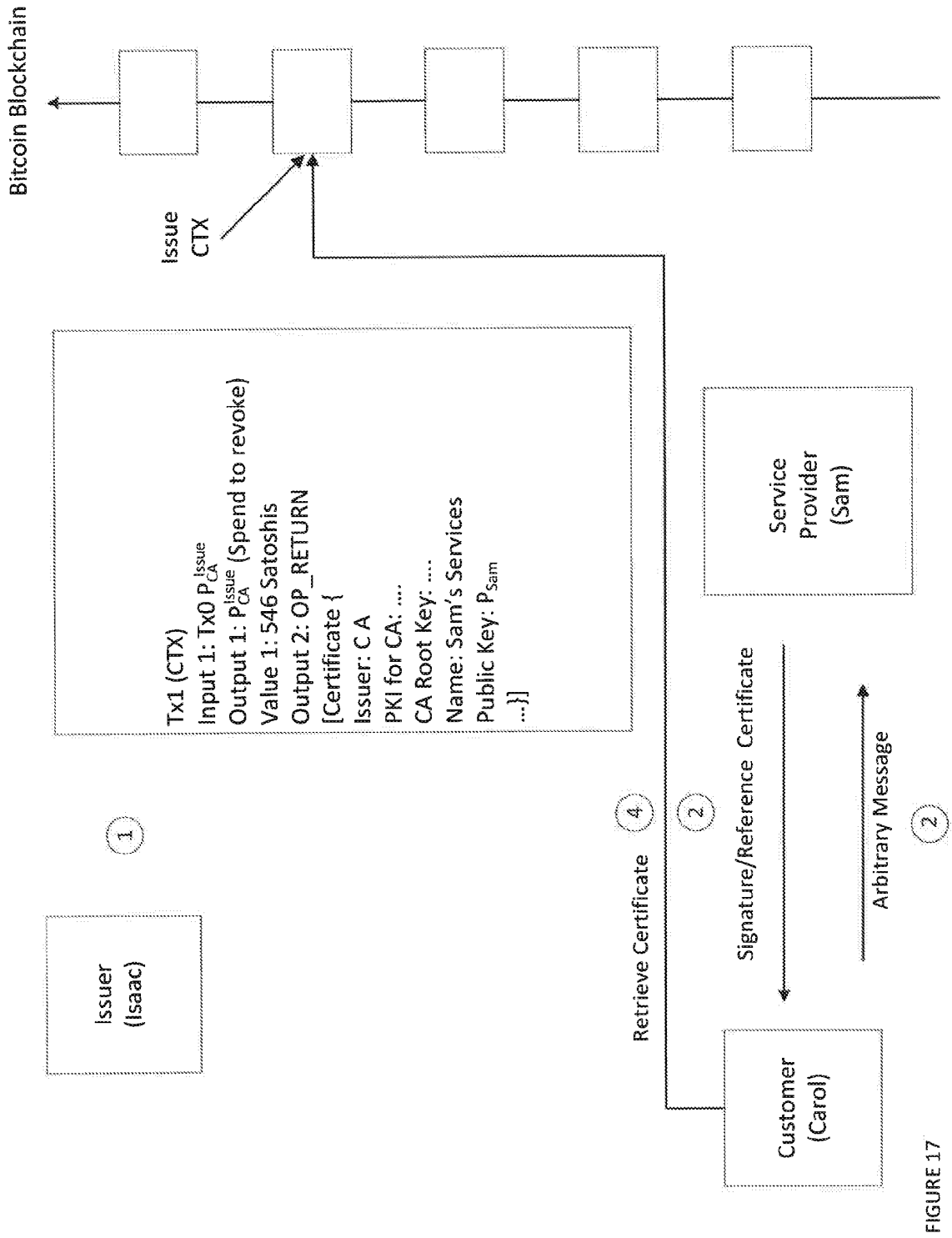

Bitcoin Blockchain
Issue CTX
Tx1 (CTX)
Input 1: Tx0 P_{CA}^{Issue}
Output 1: P_{CA}^{Issue} (Spend to revoke)
Value 1: 546 Satoshis
Output 2: OP_RETURN
[Certificate {
Issuer: CA
PKI for CA: ....
CA Root Key: ....
Name: Sam's Services
Public Key: P_{Sam}
...}]
1
Issuer (Isaac)
Service Provider (Sam)
4
Retrieve Certificate
2
Signature/Reference Certificate
Arbitrary Message
2
Customer (Carol)

FIGURE 17

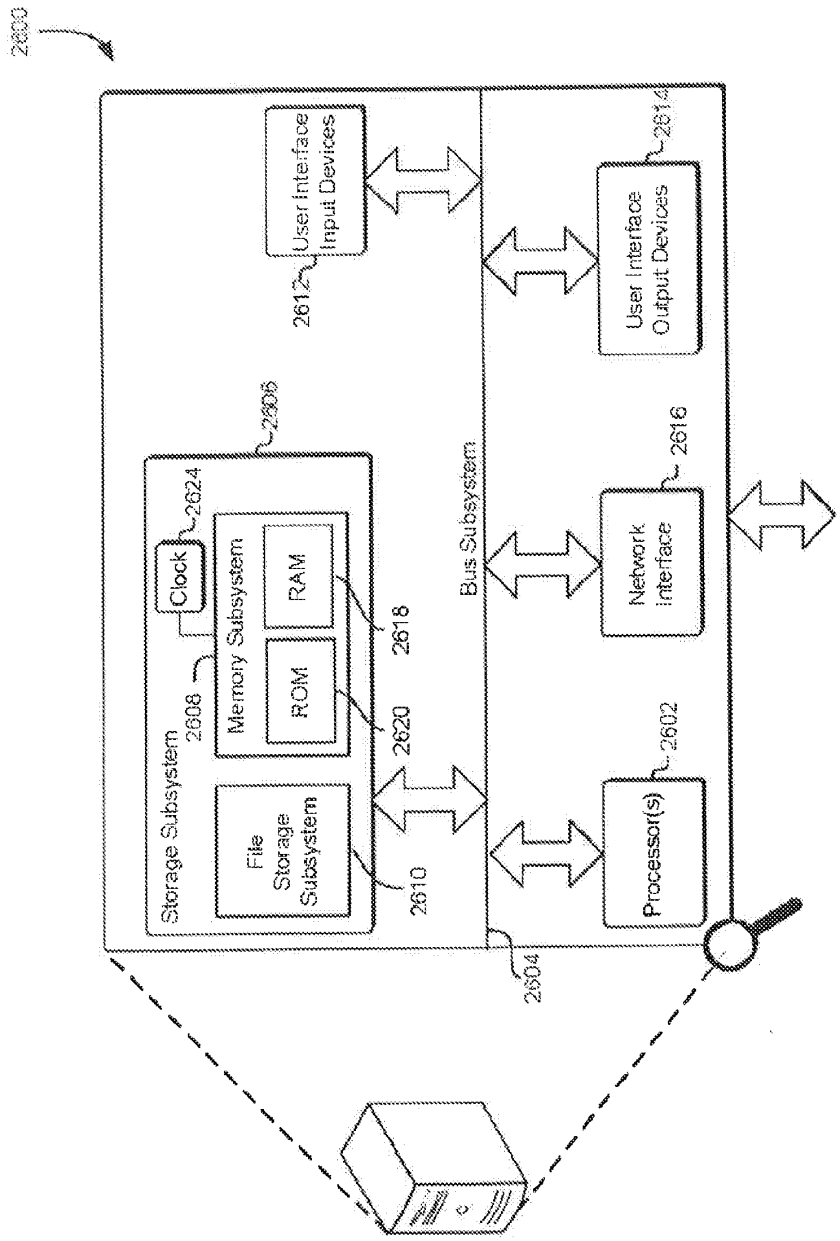

2600
User Interface Input Devices
2612
2614
User Interface Output Devices
2606
2624
Clock
Memory Subsystem
2608
RAM
ROM
2618
2620
Storage Subsystem
File Storage Subsystem
2610
Bus Subsystem
2616
Network Interface
2602
Processor(s)
2604

FIGURE 18