

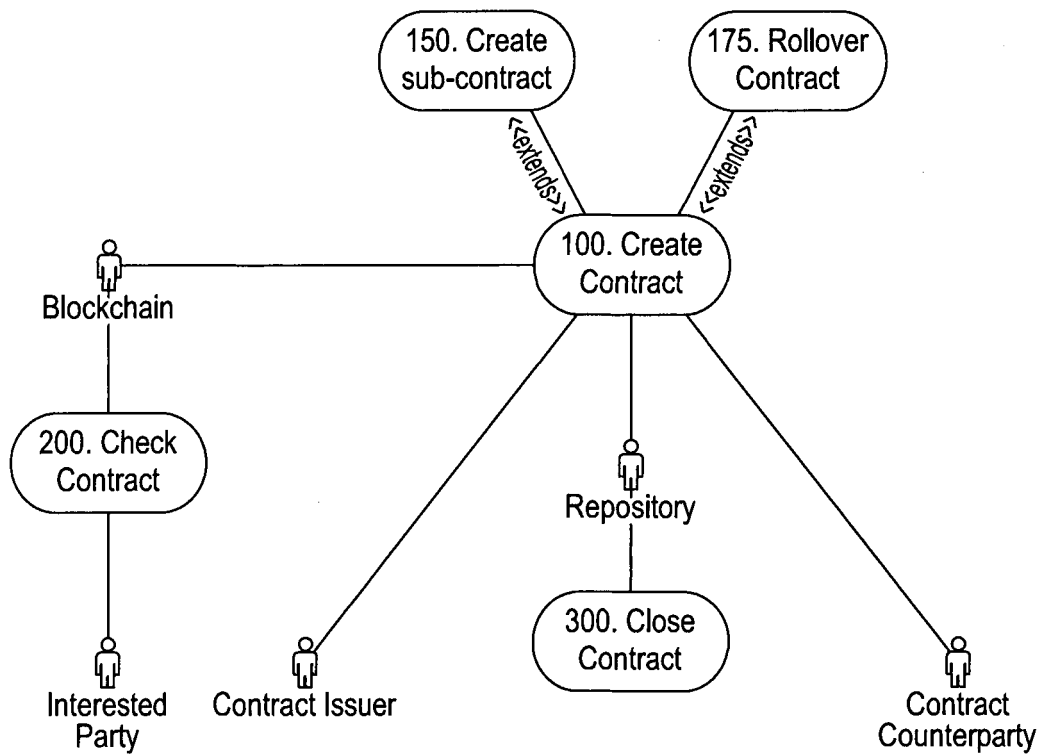


Fig. 1

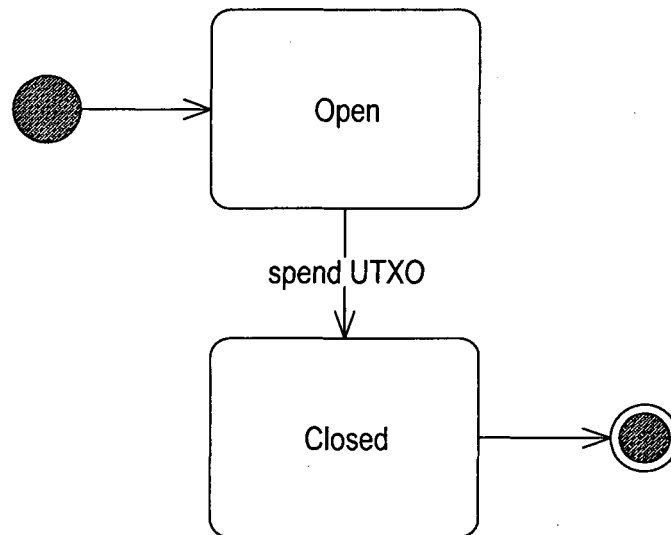


Fig. 2a

Scenario Definition

Bob: Wish to register my house onto the Blockchain

House Base Metadata

Field	Sub-field	Bytes	Value	Comments
Asset Metadata A	ContractType	4	0x0000FF04	Indicates unit
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxx	Address of the <i>Asset Definitor</i> file
	Padding	12		Spare
Asset Metadata B	ContractHash	20	#####...	Hash of the <i>Asset Definitor</i> file (not the tokenisation!)
	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options	2	0x0000	No options specified
	Padding	8		Spare

Fig. 2b

This is the transaction to publish the ownership of the asset onto the Blockchain; this is a fairly straight-forward transaction		
Bob's Publication		
BOB-S1-T1	Transaction-ID	
Version number	Version number	
1	Number of inputs	
<Bob's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output	
IDX-00	Prev Trans Output Index	
Script length	Script length	
Sig-Bob PubK-Bob	ScriptSig	
Sequence number	Sequence number	
1	Number of outputs	
2,000	Output value	
Output script length	Output script length	
OP_HASH160 <redeem script hash> OP_EQUAL	Output script	Redeem Script: allowing Bob to cancel the contract at any time
498,000	Output value	<<<< OP_1AssetMetadataA AssetMetadataB PubK-Bob OP_3 OP_CHECKMULTISIG
Output script length	Output script length	
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script	
LockTime	LockTime	

Fig. 2c

When Bob gets rid of the asset, or no longer wants it public (or semi-public) knowledge, then he simply spends the transaction output	
Bob's Contract Cancellation	
BOB-S1-T2	Transaction-ID
Version number	Version number
1	Number of inputs
BOB-S1-T1	Prev Trans Output
IDX-00	Prev Trans Output Index
Script length	Script length
Sig-Bob OP_1AssetMetadataA AssetMetadataB PubK-Bob OP_3 OP_CHECKMULTISIG	ScriptSig
Sequence number	Sequence number
1	Number of outputs
1,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160<PubK-Bob Hash>OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 2d

Scenario Definition

Bob: Wish to create an asset with hidden ownership and publish it to the Blockchain

House Base Metadata

Field	Sub-field	Bytes	Value	Comments
Asset Metadata A	ContractType	4	0x0000FF04	Indicates unit
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxx	Address of the <i>Asset Definiton</i> file
	Padding	12		Spare
Asset Metadata B	ContractHash	20	#####...	Hash of the <i>Asset Definiton</i> file (not the tokenisation!)
	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options Padding	2 8	0x0000	No options specified Spare

Fig. 3a

Bob's Funding of the Asset	
BOB-S2-T1	
1	
<Bob's previous unspent BTC output - assume 500,000 satoshi>	
IDX-00	
Sig-Bob PubK-Bob	
2	
4,000	Output value
OP_DUP OP_HASH160<PubK-Asset Hash>OP_EQUALVERIFY OP_CHECKSIG	
496,000	
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	

Fig. 3b

		Asset's Publication	
	ASSET-S2-T1		
	Version number		Version number
	1		
	BOB-S2-T1		
	IDX-00		
	Sig-Asset PubK-Asset		
	2		
	1,000		
Redeem Script; requires both Bob and the Asset to cancel it			
OP_2AssetMetadataA AssetMetadataB PubK-Asset PubK-Bob OP_4 OP_CHECKMULTISIG >>>>	OP_HASH160<Redeem script hash>OP_EQUAL		
	2,000		
	OP_DUPOP_HASH160 <PubK-AssetHash> OP_EQUALVERIFY OP_CHECKSIG		

Fig. 3c

Contract Closure	
ASSET-S2-T2	Transaction-ID
Version number	Version number
1	Number of inputs
ASSET-S2-T1	Prev Trans Output
IDX-00	Prev Trans Output Index
Script length	Script length
Sig-Asset Sig-Bob OP_2 AssetMetadataA AssetMetadataB PubK-Asset PubK-Bob OP_4 OP_CHECKMULTISIG	ScriptSig
Sequence number	Sequence number
1	Number of outputs
1,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160<PubK-Bob Hash>OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 3d

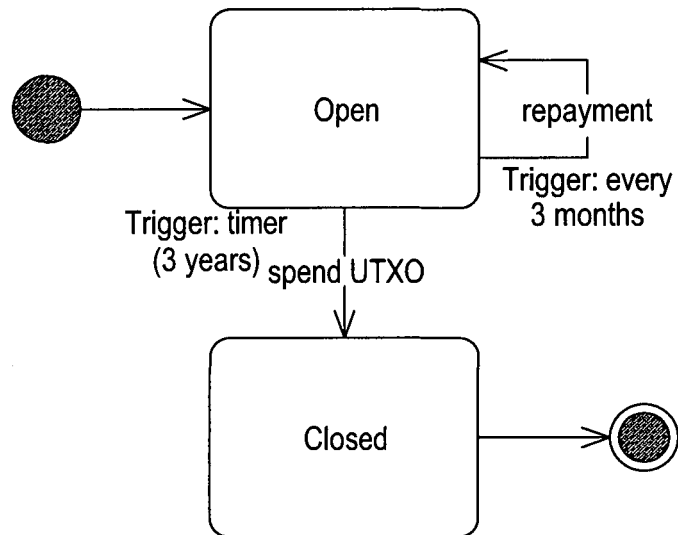


Fig. 4a

Scenario Definition

Bob: I am leasing a car from Eve for a period of three years

Lease Base Metadata

Field	Sub-field	Bytes	Value	Comments
Asset Metadata A	ContractType	4	0x0000FF04	Indicates unit
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxx	Address of the <i>Asset Definition</i> file
	Padding	12		Spare
Asset Metadata B	ContractHash	20	#####...	Hash of the <i>Asset Definition</i> file (not the tokenisation!)
	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options Padding	2 8	0x0000	No options specified Spare

Fig. 4b

	Eve's Creation of the Lease Contract		Transaction-ID
	EVE-S3-T1		Version number
	1		Number of inputs
	<Eve's previous unspent BTC output - assume 500,000 satoshi>		Prev Trans Output
	IDX-00		Prev Trans Output Index
	Script length		Script length
	Sig-Eve PubK-Eve		ScriptSig
	Sequence number		Sequence number
	2		Number of outputs
	2,000		Output value
	Output script length		Output script length
Redeem Script; requires simply Eve to close it (note that a solution requiring both Bob & Eve would also be possible)			Output script
	>>>>		Output value
	OP_1AssetMetadataA AssetMetadataB PubK-Eve OP_3 OP_CHECKMULTISIG		Output script length
	498,000		Output script
	Output script length		Lock Time
	OP_DUP OP_HASH160 <PubK-Eve Hash> OP_EQUALVERIFY OP_CHECKSIG		
	Lock Time		
Eve's Timelocked Termination of the Contract			Transaction-ID
	EVE-3-T2		Version number
	1		Number of inputs
	EVE-3-T1		Prev Trans Output
	IDX-00		Prev Trans Output Index
	Script length		Script length
	Sig-Eve OP_1AssetMetadataA AssetMetadataB PubK-Eve OP_3 OP_CHECKMULTISIG		ScriptSig
	Sequence number		Sequence number
	1		Number of outputs
	2,000		Output value
	Output script length		Output script length
	OP_DUP OP_HASH160 <PubK-Eve Hash> OP_EQUALVERIFY OP_CHECKSIG		Output script
	Date when EVE-S3-T1 was transmitted plus 3 years		Lock Time
NOTE: Transaction is submitted ahead of time rather than at the end of the three-year period			
	>>>>		

Fig. 4c

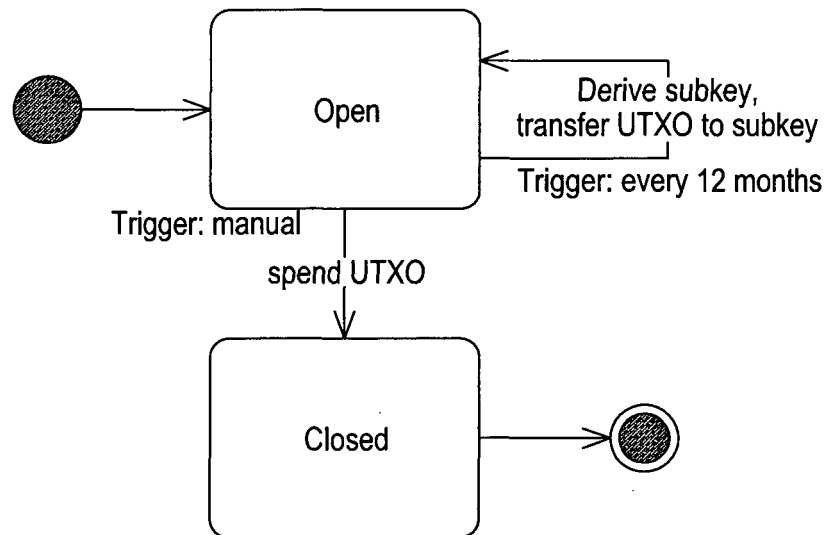


Fig. 5a

Scenario Definition

Bob: I am leasing a house from Eve on an annual basis, but can cancel within 2 months of the anniversary

Lease Base Metadata

Field	Sub-field	Bytes	Value	Comments
Asset Metadata A	ContractType	4	0x0000FF04	Indicates unit
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxx	Address of the <i>Asset Definition</i> file
	Padding	12		Spare
Asset Metadata B	ContractHash	20	#####...	Hash of the <i>Asset Definition</i> file (not the tokenisation!)
	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options Padding	2 8	0x0000	No options specified Spare

Fig. 5b

Redeem Script: requires 2 out of Bob, Eve and the independent computing agent to unlock OP_2AssetMetadataA AssetMetadataB PubK-Bob PubK-Eve PubK-Oracle OP_5 OP_CHECKMULTISIG	Eve's Creation of the Lease Contract			
	EVE-S4-T1	Transaction-ID	Version number	Number of inputs
	1	<Eve's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output	Prev Trans Output Index
	IDX-00	Script length	Script length	ScriptSig
	Sig-Eve PubK-Eve	Sequence number	Sequence number	Number of outputs
	2	Output value	Output value	Output script length
	1,000	Output script length	Output script length	Output script
	OP_HASH160<Redeem script hash>OP_EQUAL	Output value	Output script length	Output script
	499,000	Output script length	Output script length	Lock Time
	OP_DUP OP_HASH160 <PubK-Eve Hash> OP_EQUALVERIFY OP_CHECKSIG	Transaction-ID	Version number	Number of inputs
	Lock Time	Eve's Timelocked Roll-on of the Contract	Prev Trans Output	Prev Trans Output Index
	EVE-S4-T2	Script length	Script length	ScriptSig
	Version number	Sig-Eve Sig-Bob OP_2AssetMetadataA AssetMetadataB PubK-Bob PubK-Eve	Sequence number	Sequence number
	2	OP_5 OP_CHECKMULTISIG	Number of outputs	Output value
	<Eve's mining fee of 1000 satoshi (note that no change can be given from this transaction) because of the effect of the timelock) which means that she'll probably generate a previous transaction to get an input of the exact value>	Output script length	Output script length	Output script
Redeem Script: requires 2 out of Bob, Eve's contract roll-on subkey and the independent Agent (oracle) to OP_2AssetMetadataA AssetMetadataB PubK-Bob PubK-Eve SK1 PubK-Oracle OP_5 OP_CHECKMULTISIG NOTE: Transaction is submitted ahead of time	IDX-00	OP_HASH160 <redeem script hash> OP_EQUAL	Output script length	Output script
	Script length	Date when EVE-S4-T1 was transmitted plus 1 year	Output script length	Lock Time
	Sig-Eve Sig-Bob OP_2AssetMetadataA AssetMetadataB PubK-Bob PubK-Eve		Output script	Lock Time
	OP_5 OP_CHECKMULTISIG		Output script	Lock Time
	Sequence number		Output script	Lock Time
	1		Output script	Lock Time
	1,000		Output script	Lock Time
	Output script length		Output script	Lock Time
	OP_HASH160 <redeem script hash> OP_EQUAL		Output script	Lock Time
	>>>>		Output script	Lock Time

Fig. 5c

After the first year, Bob continue's with the lease and doesn't terminate. Immediately after EVE-S3-T2 is published then it is picked up by the Agent (oracle) and rolled-on for another year (note that it is also possible that this could be done by EVE using internal logic of her own)		Eve's Timelocked Roll-on of the Contract	
		EVE-S4-T3	Transaction-ID
		Version number	Version number
		2	Number of inputs
		<Eve's mining fee of 1000 satoshi (note that no change can be given from this transaction) because of the effect of the timelock) which means that she'll probably generate a previous transaction to get an input of the exact value>	Prev Trans Output
		IDX-00	Prev Trans Output Index
		Script length	Script length
		Sig-Eve PubK-Eve	ScriptSig
		EVE-S4-T2	Sequence number
		IDX-00	Prev Trans Output Index
Redeem Script; requires 2 out of Bob, Eve's second contract roll-on subkey and the independent Agent to unlock OP_2AssetMetadataA AssetMetadataB PubK-Bob PubK-EveSK2 PubK-Oracle OP_5 OP_CHECKMULTISIG NOTE: Transaction is submitted ahead of time		Script length	Script length
		Sig-EveSK1 Sig-Oracle OP_2AssetMetadataA AssetMetadataB PubK-Bob PubK-EveSK1 PubK-Eve OP_5 OP_CHECKMULTISIG	ScriptSig
		Sequence number	Sequence number
		1	Number of outputs
		1,000	Output value
		Output script length	Output script length
		OP_HASH160 <redeem script hash> OP_EQUAL	Output script
		Date when EVE-S4-T2 was transmitted plus 1 year	LockTime
		>>>>	

Fig. 5c (continued)

Bob's Contract Termination	
BOB-S4-T1	Transaction-ID
Version number	Version number
2	Number of inputs
<Bob's mining fee of 1000 satoshi (note that no change can be given from this transaction) because of the effect of the timelock) which means that she'll probably generate a previous transaction to get an input of the exact value>	Prev Trans Output
IDX-00	Prev Trans Output Index
Script length	Script length
Sig-Bob PubK-Bob	ScriptSig
EVE-S4-T2	Sequence number
IDX-00	Prev Trans Output Index
Script length	Script length
Sig-Bob Sig-Oracle OP_2AssetMetaDataA AssetMetadataB PubK-Bob PubK-EveSK1 PubK-Eve OP_3 OP_CHECKMULTISIG	ScriptSig
Sequence number	Sequence number
1	Number of outputs
1,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160<PubK-Eve Hash>OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 5d

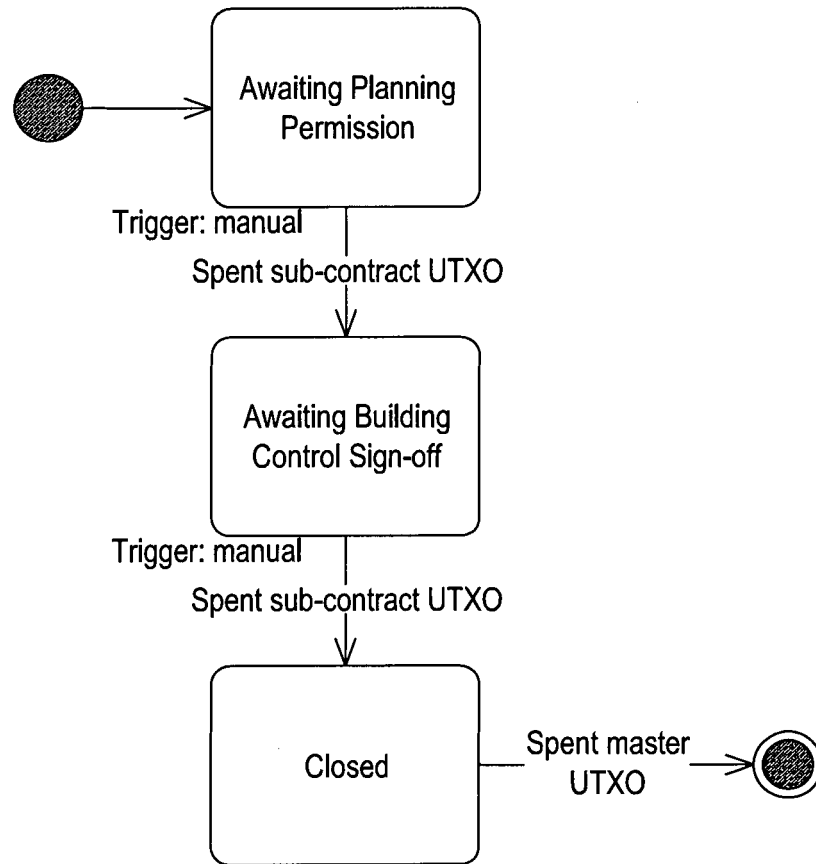


Fig. 6a

Scenario Definition

Bob: I am building a property, and I need two independent assessments at different times in the process
(planning permission and building accreditation) before the contract is fulfilled

House Base Metadata

Field	Sub-field	Bytes	Value	Comments
Asset Metadata A	ContractType	4	0x0000FF04	Indicates unit
	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxx	Address of the <i>Asset Definiton</i> file
	Padding	12		Spare
Asset Metadata B	ContractHash	20	#####...	Hash of the <i>Asset Definiton</i> file (not the tokenisation!)
	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options Padding	2 8	0x0000	No options specified Spare

Fig. 6b

Bob's Creation of the Property Build Contract		
BOB-S5-T1	Transaction-ID	
Version number	Version number	
1	Number of inputs	
<Bob's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output	
IDX-00	Prev Trans Output Index	
Script length	Script length	
Sig-Bob PubK Bob	ScriptSig	
Sequence number	Sequence number	
2	Number of outputs	
2,000	Output value	
Output script length	Output script length	
		Redeem Script: requires 2 out of Bob, Oracle to conclude
OP_HASH160 <redeem script hash> OP_EQUAL	Output script	>>>> OP_1AssetMetaDataA AssetMetaDataB PubK-Bob PubK-Oracle OP_4 OP_CHECKMULTISIG
497,000	Output value	
Output script length	Output script length	
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script	
LockTime	LockTime	

Fig. 6c

Bob's Creation of the sub-contract using his derived key to confirm planning approval		
BOB-S5-T2	Transaction-ID	
Version number	Version number	
1	Number of inputs	
BOB-S5-T1	Prev Trans Output	
IDX-01	Prev Trans Output Index	
Script length	Script length	
Sig-Bob PubK Bob	ScriptSig	
Sequence number	Sequence number	
2	Number of outputs	
2,000	Output value	
Output script length	Output script length	
OP_HASH160 <redeem script hash> OP_EQUAL	Output script	Redeem Script: requires Planning Authority to approve & Oracle to approve, but Bob and stand-in for either
494,000	Output value	>>>> OP_2AssetMetadataA AssetMetadataB PubK-BobSK1 PubK-PlanningAuthority PubK-Oracle OP_5
Output script length	Output script length	
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script	
Lock Time	Lock Time	

Fig. 6c (continued)

Bob's Creation of the sub-contract using his derived key to confirm building standard approval		
BOB-S5-T3	Transaction-ID	
Version number	Version number	
1	Number of inputs	
BOB-S5-T2	Prev Trans Output	
IDX-01	Prev Trans Output Index	
Script length	Script length	
Sig-Bob PubK Bob	ScriptSig	
Sequence number	Sequence number	
2	Number of outputs	
2,000	Output value	
Output script length	Output script length	
OP_HASH160 <redeem script hash> OP_EQUAL	Output script	Redeem Script; requires Building Standard to approve & Oracle to approve but Bob can stand-in for either
491,000	Output value	>>>> OP_2AssetMetaDataA AssetMetadataB PubK-BobSK2 PubK-BuildingStandard PubK-Oracle OP_5
Output script length	Output script length	
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script	
LockTime	LockTime	

Fig. 6c (continued)

Planning Authority Sign-off			
BOB-S5-T4		Transaction-ID	
Version number		Version number	
1		Number of inputs	
BOB-S5-T2		Prev Trans Output	
IDX-00		Prev Trans Output Index	
Script length		Script length	
Sig-PlanningAuthority Sig-Grade OP_2AssetMetaDataA AssetMetadataB PubK-BobSK1		ScriptSig	
PubK-PlanningAuthority PubK-Grade OP_5 OP_CHECKMULTISIG			
Sequence number		Sequence number	
1		Number of outputs	
1,000		Output value	
Output script length		Output script length	Note
OP_DUP OP_HASH160<PubK-PlanningAuthority Hash>OP_EQUALVERIFY OP_CHECKSIG		Output script	The satoshi pays the planning authority fee(note that there maybe a two output <<<< model for both the orade and planning authority)
LockTime		LockTime	

Fig. 6d

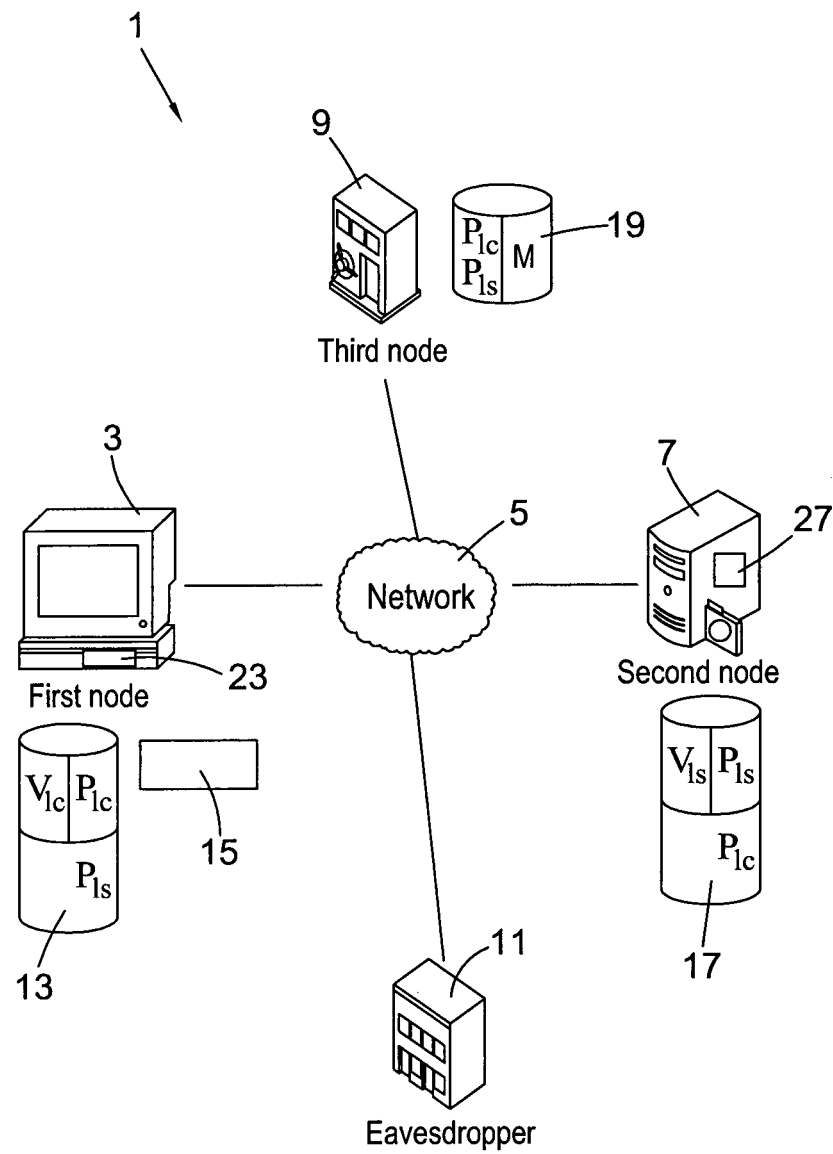


Fig. 7

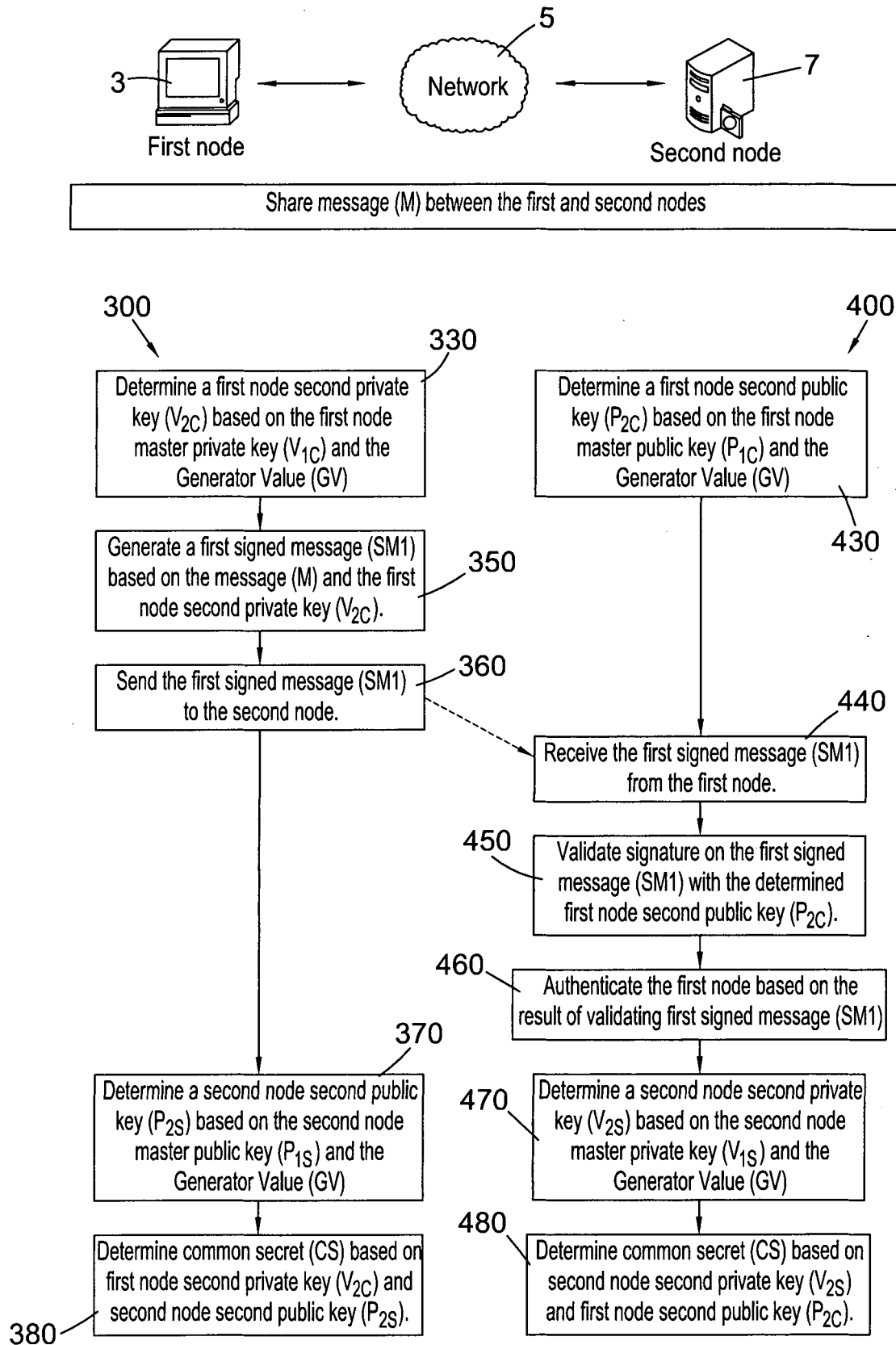


Fig. 8

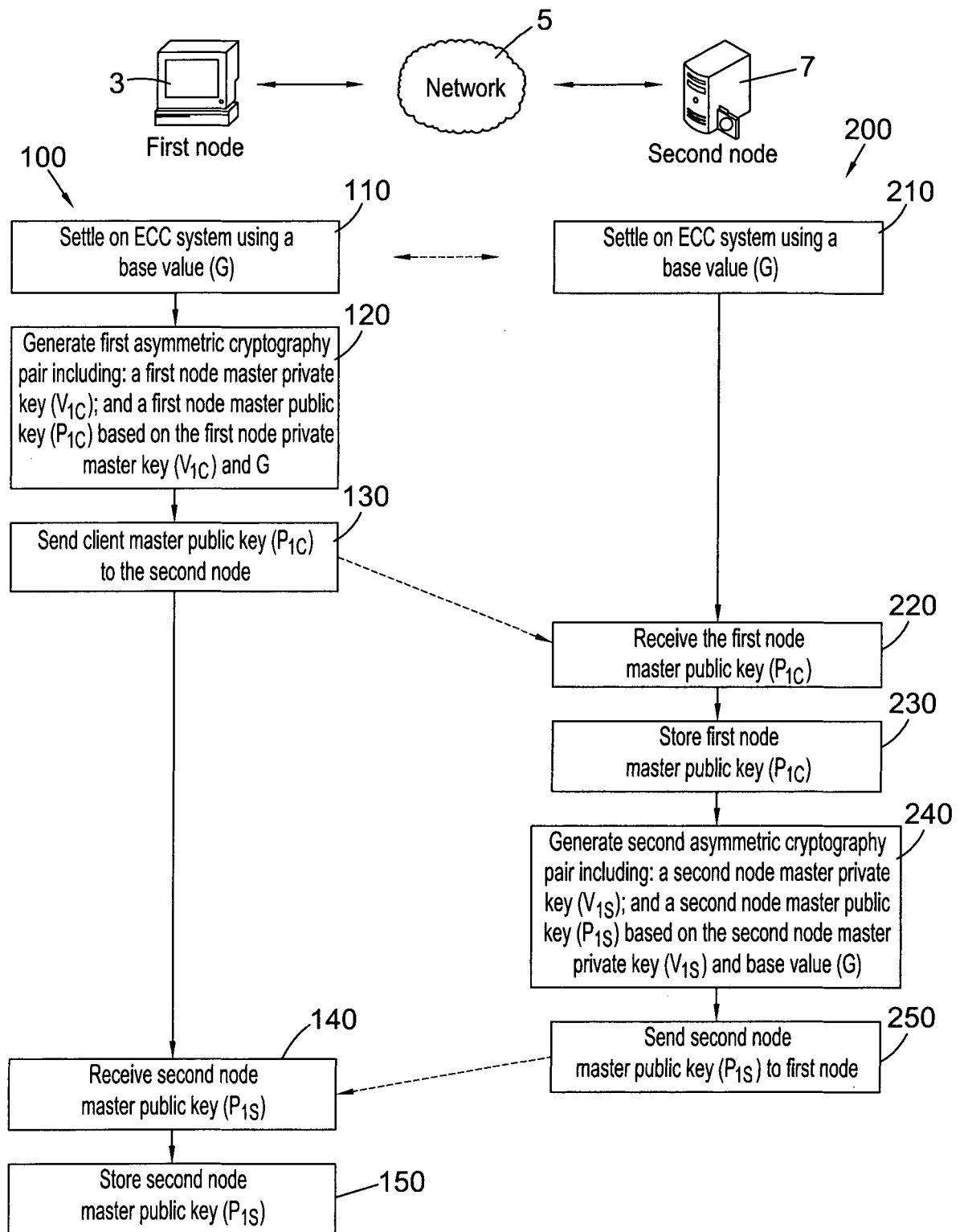


Fig. 9

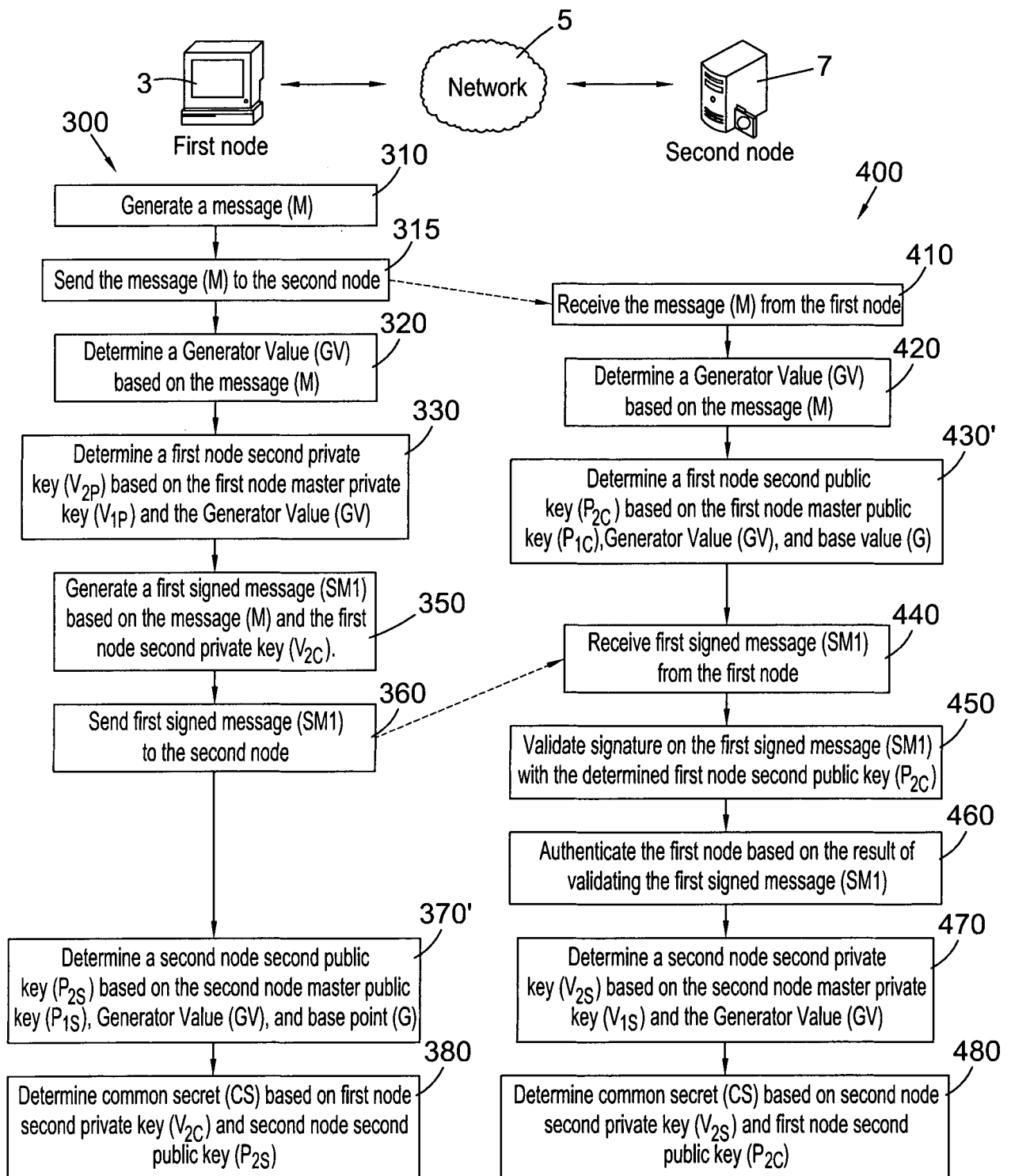


Fig. 10

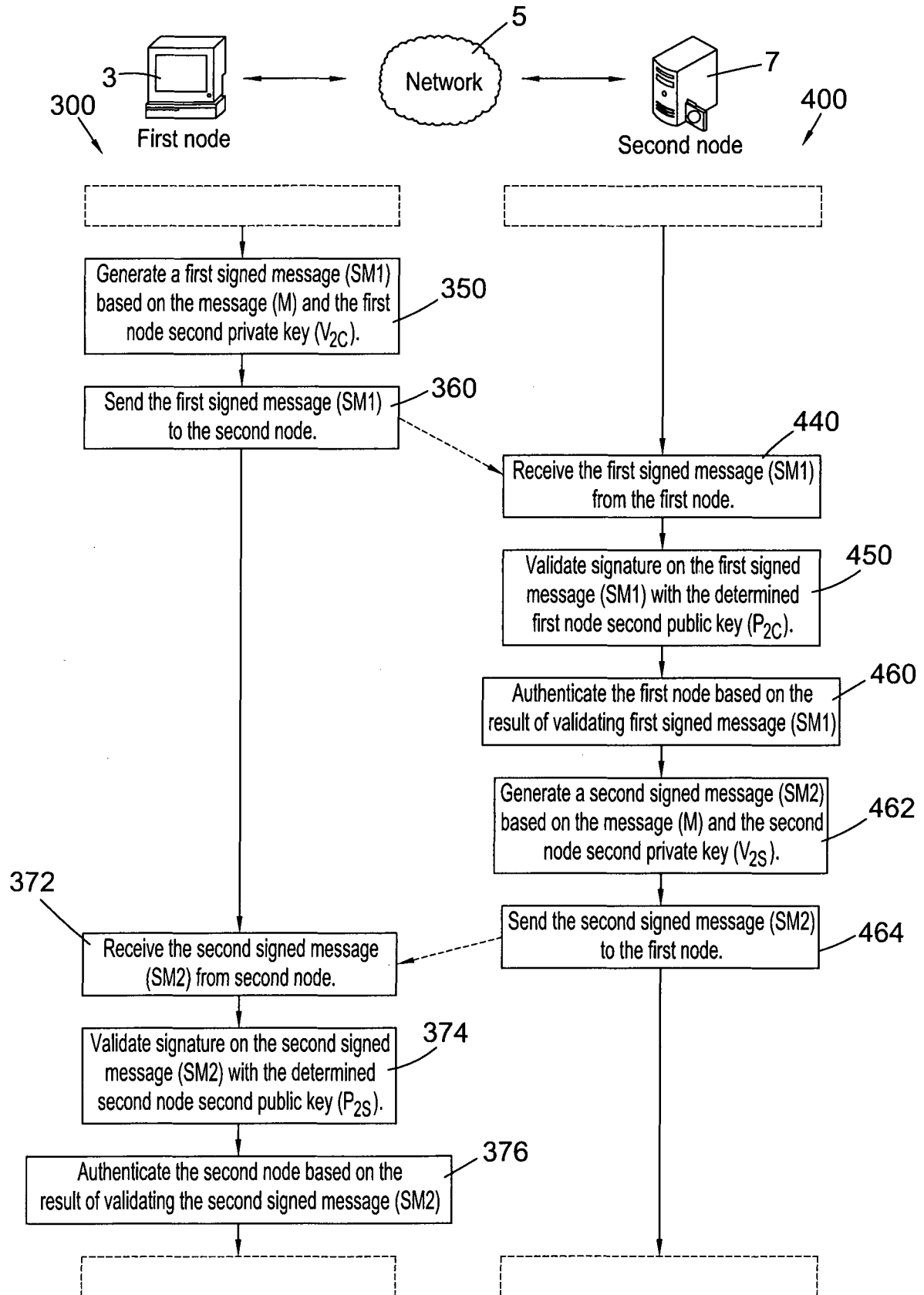


Fig. 11

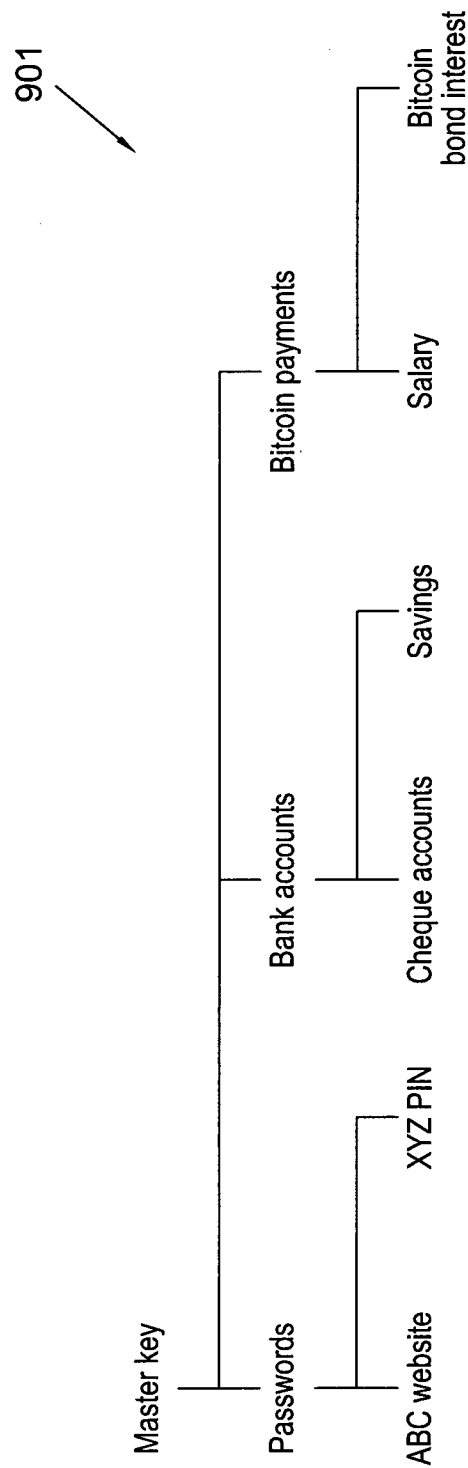


Fig. 12

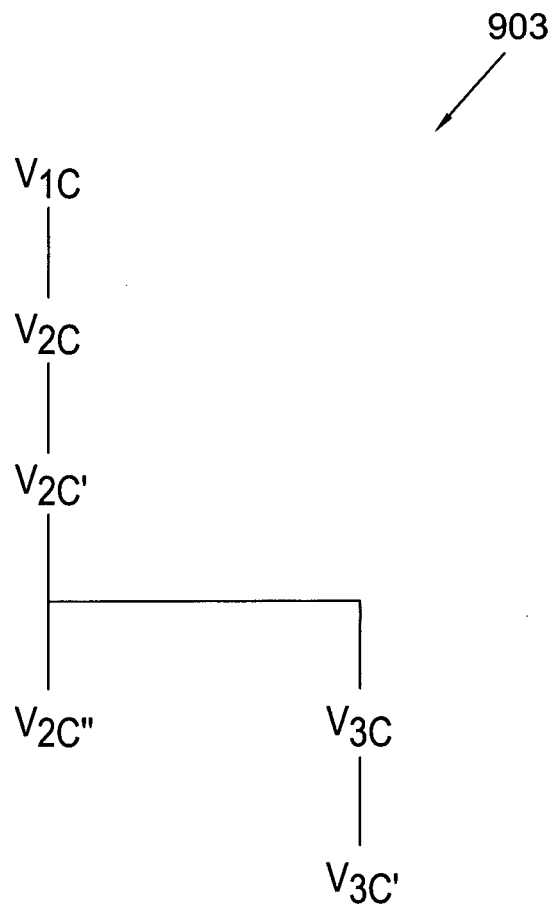


Fig. 13