

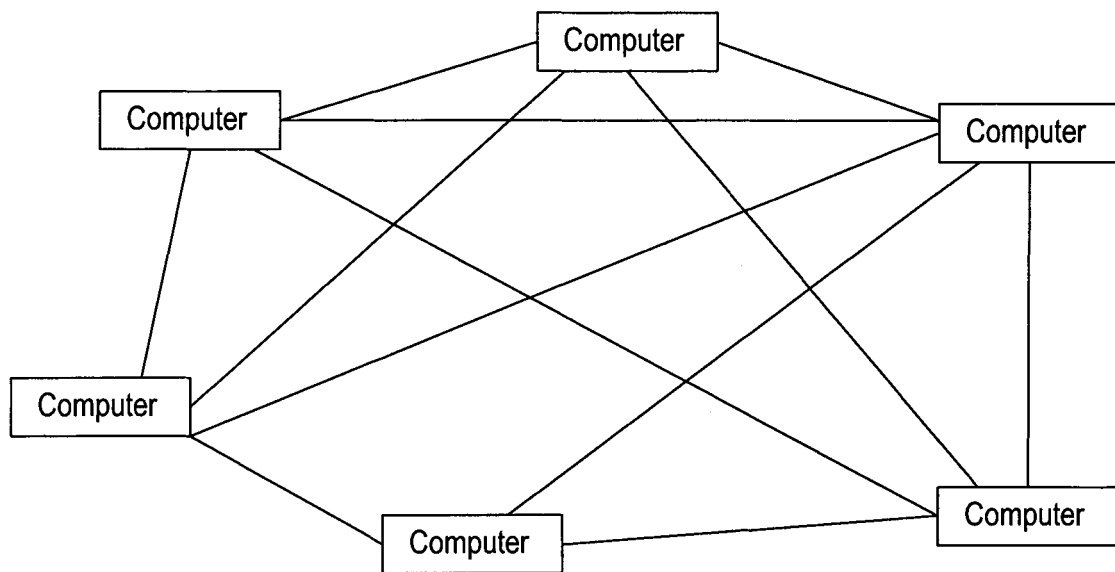


Fig. 1

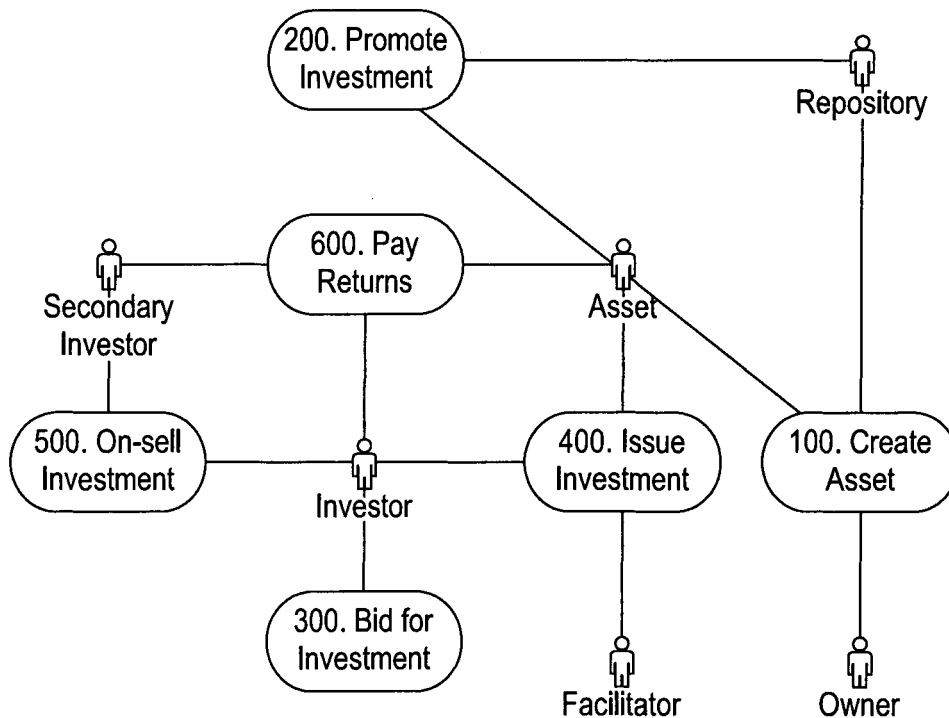


Fig. 2a

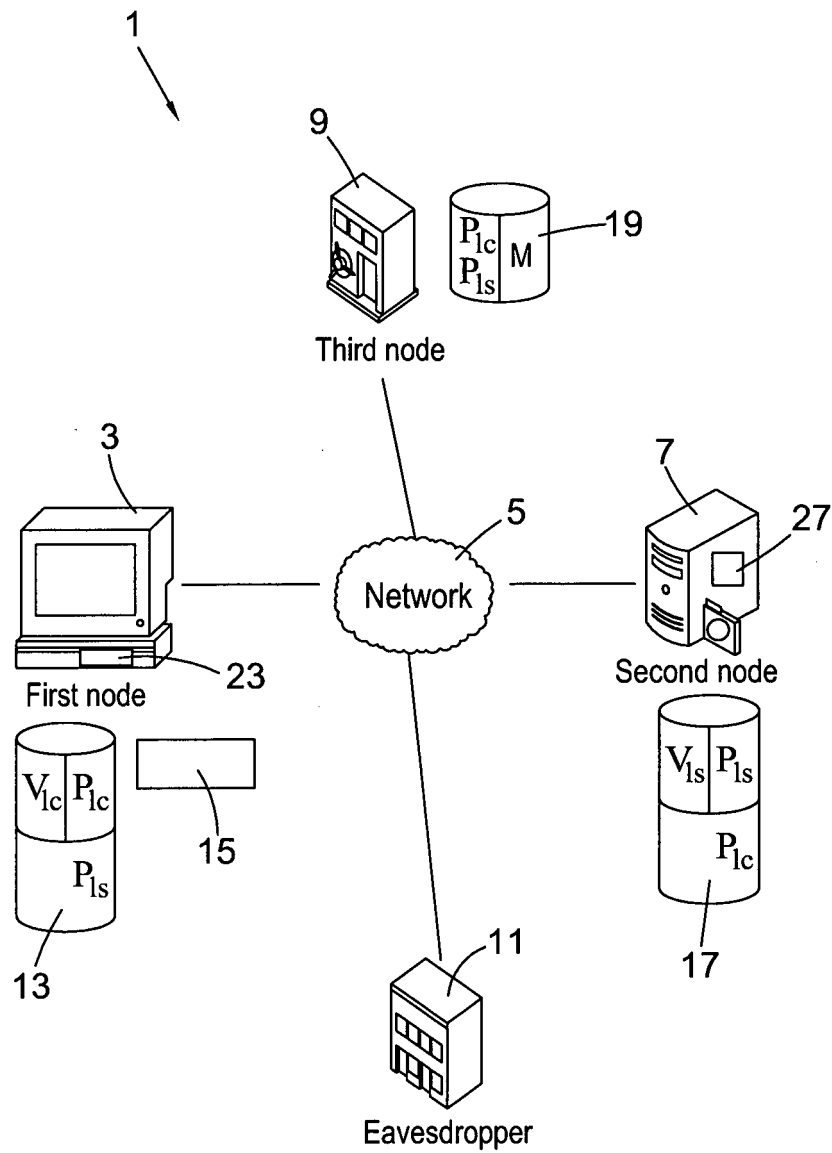


Fig. 2b

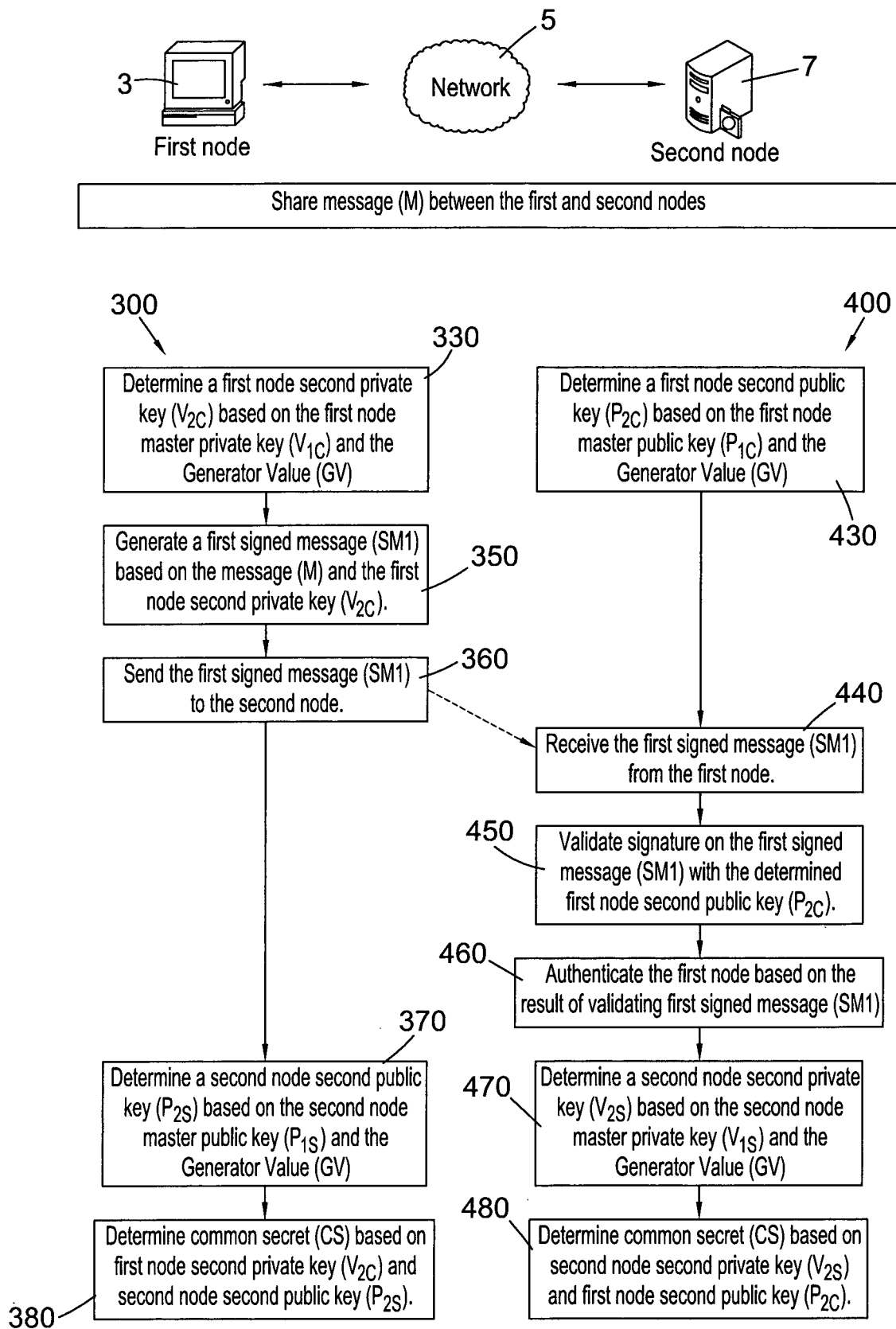


Fig. 2c

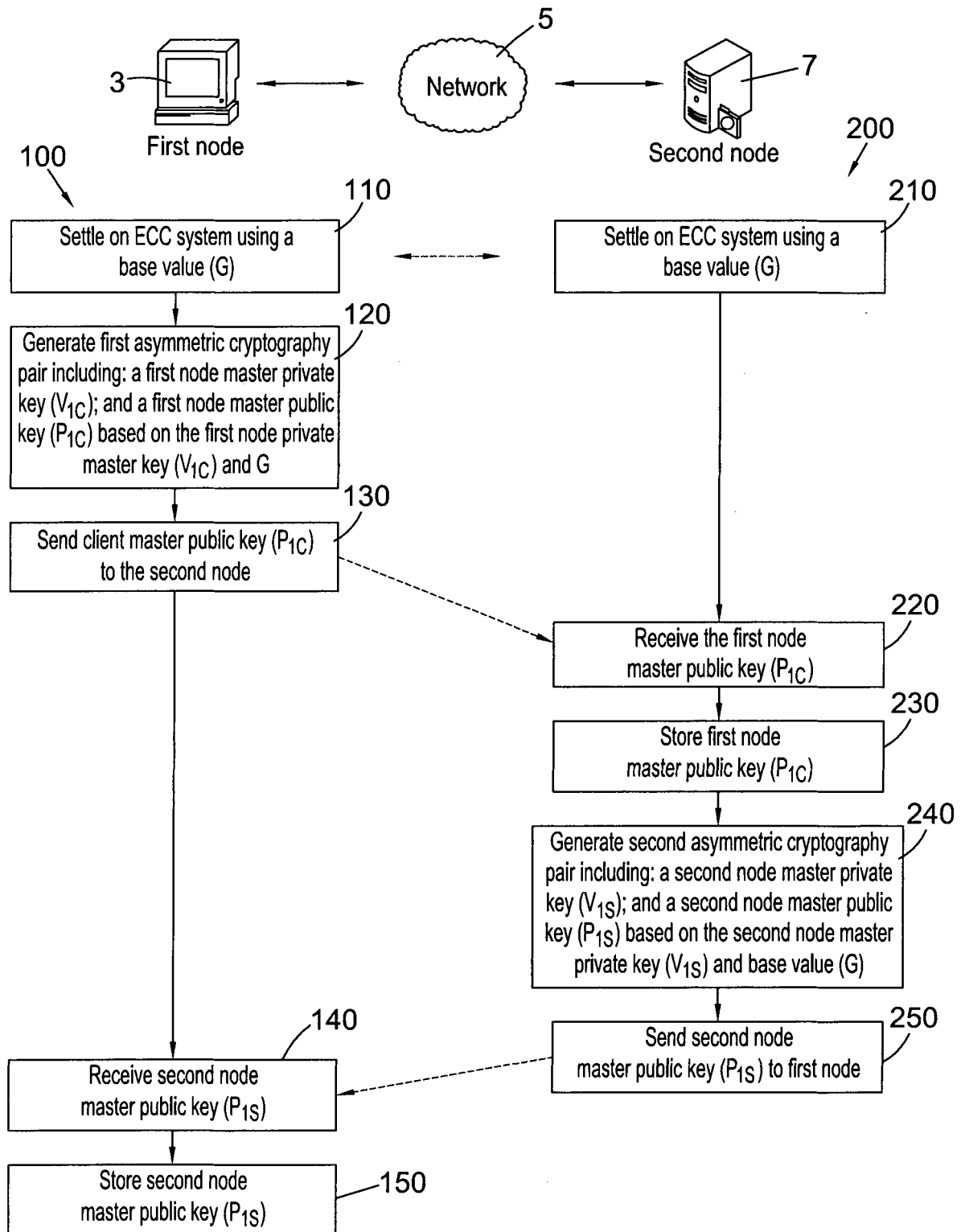


Fig. 2d

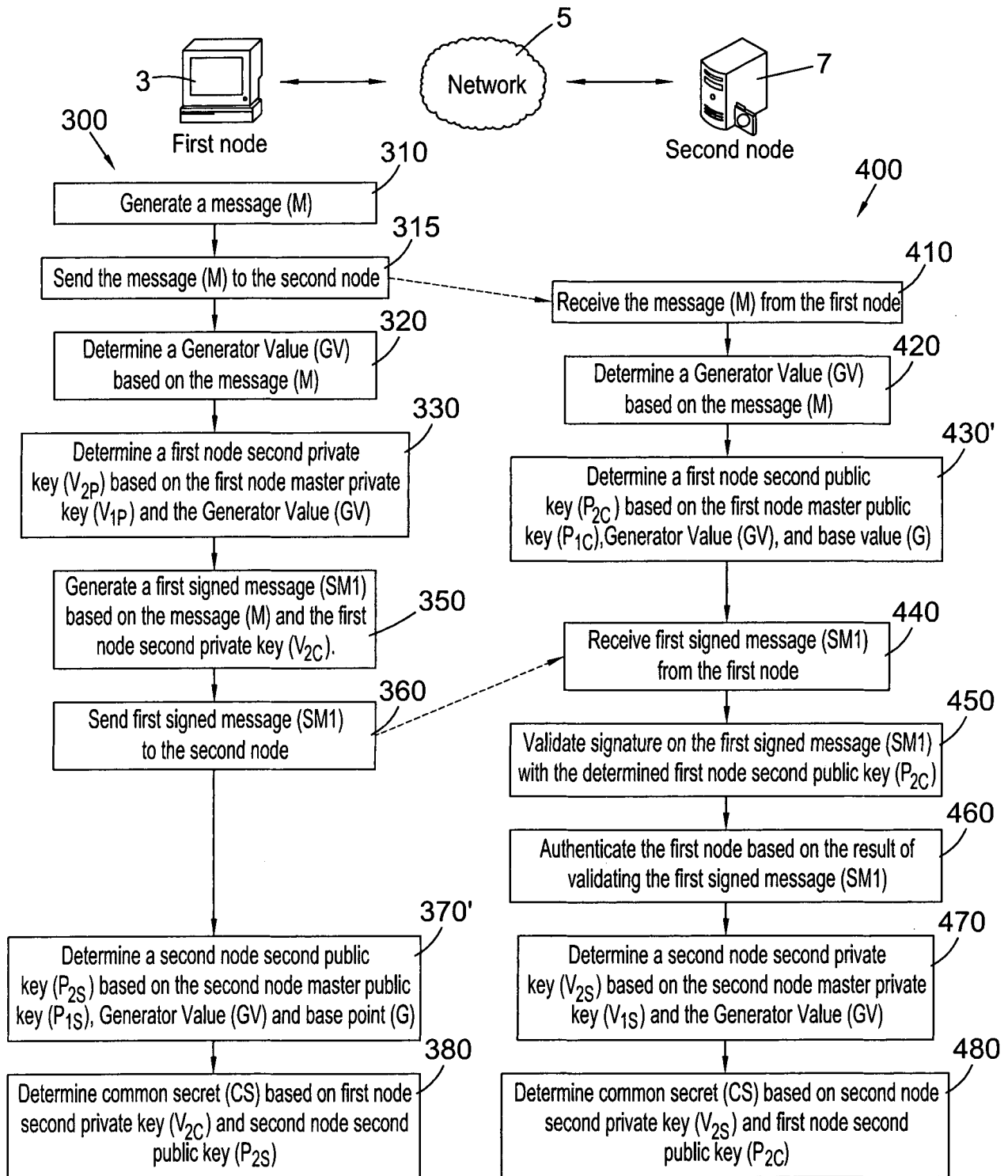


Fig. 2e

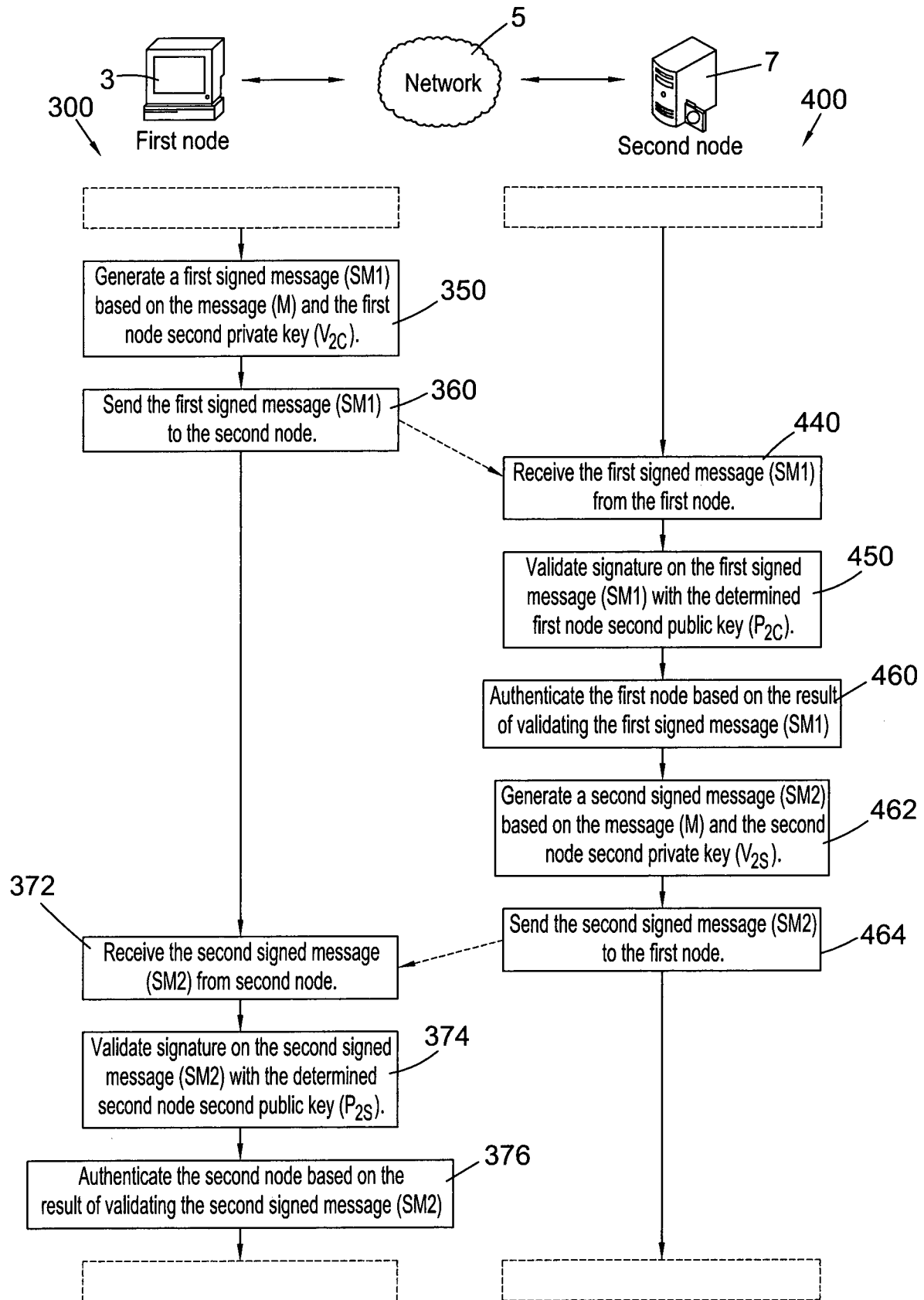


Fig. 2f

Colin's Setup	
COLIN-S1-T1	Transaction-ID
Version number	Version number
1	Number of inputs
<Colin's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Colin PubK-Colin	ScriptSig
Sequence number	Sequence number
1	Number of outputs
105,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Asset Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
394,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Colin Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 3

Asset's Offer	
ASSET-S1-T1	Transaction-ID
Version number	Version number
1	Number of inputs
COLIN-S1-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Asset PubK-Asset	ScriptSig
Sequence number	Sequence number
1	Number of outputs
104,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
<set to the deadline specified (midnight 31-Dec-2016), expressed as UnixTime>	LockTime
ASSET-S1-T2	Transaction-ID
Version number	Version number
1	Number of inputs
ASSET-S1-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Asset <OP_1 AssetMetadataA AssetMetadataB InvestmentMetadataA InvestmentMetadataB PubK-Asset OP_5 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
1	Number of outputs
103,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Asset Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
<set to the deadline specified (midnight 31-Dec-2016), expressed as UnixTime>	LockTime

Fig. 4

Colin's Bid	
COLIN-S1-T2	Transaction-ID
Version number	Version number
1	Number of inputs
<Colin's previous unspent BTC output - assume 1000 BTC satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Colin PubK-Colin	ScriptSig
Sequence number	Sequence number
2	Number of outputs
51,000,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
48,999,999,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Colin> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 5

10/28

Bob's Bid	
BOB-S1-T1	Transaction-ID
Version number	Version number
1	Number of inputs
<Bob's previous unspent BTC output - assume 1000 BTC 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
23,000,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
76,999,999,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 6

11/28

Mary's Bid	
MARY-S1-T1	Transaction-ID
Version number	Version number
1	Number of inputs
<Mary's previous unspent BTC output - assume 1000 BTC satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Mary PubK-Mary	ScriptSig
Sequence number	Sequence number
2	Number of outputs
9,000,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
90,999,999,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Mary> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 7

12/28

Frank's Bid	
FRANK-S1-T1	Transaction-ID
Version number	Version number
1	Number of inputs
<Frank's previous unspent BTC output - assume 1000 BTC satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Frank PubK-Frank	ScriptSig
Sequence number	Sequence number
2	Number of outputs
17,000,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
82,999,999,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Mary> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 8

Asset Issue Investment	
ASSET-S1-T3	Transaction-ID
Version number	Version number
5	Number of inputs
ASSET-S1-T2	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Colin PubK-Colin	ScriptSig
COLIN-S1-T2	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Asset Sig-Facilitator <OP_2 AssetMetadataA AssetMetadataB InvestmentMetadataA InvestmentMetadataB PubK-Asset PubK-Facilitator OP_5 OP_CHECKMULTSIG>	ScriptSig
BOB-S1-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Asset Sig-Facilitator <OP_2 AssetMetadataA AssetMetadataB InvestmentMetadataA InvestmentMetadataB PubK-Asset PubK-Facilitator OP_5 OP_CHECKMULTSIG>	ScriptSig
MARY-S1-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Asset Sig-Facilitator <OP_2 AssetMetadataA AssetMetadataB InvestmentMetadataA InvestmentMetadataB PubK-Asset PubK-Facilitator OP_5 OP_CHECKMULTSIG>	ScriptSig
FRANK-S1-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length

Fig. 9

Sig-Asset Sig-Facilitator <OP_2 AssetMetadataA AssetMetadataB InvestmentMetadataA InvestmentMetadataB PubK-Asset PubK-Facilitator OP_5 OP_CHECKMULTSIG>	ScriptSig
Sequence number	Sequence number
6	Number of outputs
51,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
23,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
9,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
17,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
10,000,000,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Colin> OP_EQUALVERIFY OP_CHECKSIG	Output script
2,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Asset Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 9
(continued)

Colin's Investment Return Funding	
COLIN-S1-T3	Transaction-ID
Version number	Version number
1	Number of inputs
<Colin's previous unspent BTC output - assume 100 BTC satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Colin PubK-Colin	ScriptSig
Sequence number	Sequence number
2	Number of outputs
1,000,001,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Asset> OP_EQUALVERIFY OP_CHECKSIG	Output script
8,999,998,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Colin> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 10

Asset's Investment Return	
ASSET-S1-T4	Transaction-ID
Version number	Version number
1	Number of inputs
COLIN-S1-T3	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Asset PubK-Asset	ScriptSig
Sequence number	Sequence number
4	Number of outputs
510,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
230,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
90,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
170,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
LockTime	LockTime

Fig. 11

Field	Sub-field	Bytes	Value	Comments
Asset	ContractType	4	0x0000FF04	Indicates unit
Metadata A	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	Address of the <i>Asset Definition</i> file
	Padding	12		Spare
Asset	ContractHash	20	#####...	Hash of the <i>Asset Definition</i> file (not the tokenisation!)
Metadata B	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options	2	0x0000	No options specified
	Padding	8		Spare
Invest	ContractType	4	0x0000FF03	Indicates unit
Metadata A	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	IPv6 address of the <i>Investment</i> file (not the tokenisation!)
	OfferRequestCode	1	'	
	NumberShares	8		Hex value defining the number of shares
	Conditions	1	00000000 ₂	No conditions
	PeggingRate	1		Coded value represents the BTC/share pegging rate
	AssetLinkage	1	0x02	Shared ownership of
	Padding	1		
Invest	ContractHash	20	#####...	Hash of the <i>Investment</i> file (not the tokenisation!)
Metadata B	Jurisdiction	2	EN	Specifies that the contract is governed under English law
	Options	1		
	ReturnUnit	1		
	ReturnPeriod	4		
	ReturnGap	1		
	Padding	3		
	Padding	3		

Fig. 12

Jane's Purchase from Bob	
JANE-S2-T1	Transaction-ID
Version number	Version number
1	Number of inputs
<Jane's previous BTC account, assume 200 BTC>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Jane PubK-Jane	ScriptSig
Sequence number	Sequence number
2	Number of outputs
12,000,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
7,999,999,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Jane> OP_EQUALVERIFY OP_CHECKSIG	Output script

Fig. 13

Bob's transfer of asset to Jane	
BOB-S2-T1	Transaction-ID
Version number	Version number
2	Number of inputs
ASSET-S1-T3	Prev Trans Output
IDX-01	Prev Trans Output index
Script length	Script length
Sig-Bob Sig-Asset <OP_2 AssetMetaDataA AssetMetadataB InvestmentMetadataA InvestmentMetadataB PubK-Bob PubK-Asset OP_6 OP_CHECKMULTISIG>	ScriptSig
<Bob's regular BTC account (to pay mining fee) - assume 10000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Bob PubK-Bob	ScriptSig
Sequence number	Sequence number
3	Number of outputs
10,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
13,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
9,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob> OP_EQUALVERIFY OP_CHECKSIG	Output script

Fig. 14

Asset's Investment Return	
ASSET-S2-T1	Transaction-ID
Version number	Version number
1	Number of inputs
COLIN-S2-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Asset PubK-Asset	ScriptSig
Sequence number	Sequence number
5	Number of outputs
510,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
130,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
90,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
170,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
100,000,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
LockTime	LockTime

Fig. 15

Field	Sub-field	Bytes	Value	Comments
Asset	ContractType	4	0x0000FF04	Indicates unit
Metadata A	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	Address of the <i>Asset Definition</i> file
	Padding	12		Spare
Asset	ContractHash	20	#####...	Hash of the <i>Asset Definition</i> file (not the tokenisation!)
Metadata B	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options	2	0x0000	No options specified
	Padding	8		Spare
Invest	ContractType	4	0x0000FF03	Indicates unit
Metadata A	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	IPv6 address of the <i>Investment</i> file (not the tokenisation!)
	OfferRequestCode	1		
	NumberShares	8		Hex value defining the number of shares
	Conditions	1	00000000 ₂	No conditions
	PeggingRate	1		Coded value represents the BTC/share pegging rate
	AssetLinkage	1	0x01	Investment secured against
	Padding	7		
Invest	ContractHash	20	#####...	Hash of the <i>Investment</i> file (not the tokenisation!)
Metadata B	Jurisdiction	2	EN	Specifies that the contract is governed under English law
	Options	1		
	ReturnUnit	1		
	ReturnPeriod	4		
	ReturnGap	1		
	Spare	3		

Fig. 16

Field	Sub-field	Bytes	Value	Comments
House	ContractType	4	0x0000FF04	Indicates unit
Metadata A	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	Address of the <i>Asset Definition</i> file
	Padding	12		Spare
House	ContractHash	20	#####...	Hash of the <i>Asset Definition</i> file (not the tokenisation!)
Metadata B	Jurisdiction	2	EN	Specifies that the asset is covered by English law
	Options	2	0x0000	No options specified
	Padding	8		Spare
Invest	ContractType	4	0x0000FF03	Indicates unit
Metadata A	ContractPointer	16	xxxx.xxxx.xxxx.xxxx (...) .xxxx	IPv6 address of the <i>Investment</i> file (not the tokenisation!)
	OfferRequestCode	1		
	NumberShares	8		Hex value defining the number of shares
	Conditions	1	00000000 ₂	No conditions
	PeggingRate	1		Coded value represents the BTC/share pegging rate
	AssetLinkage	1	0x02	Shared ownership of
	Padding	7		Spare
Invest	ContractHash	20	#####...	Hash of the <i>Investment</i> file (not the tokenisation!)
Metadata B	Jurisdiction	2	EN	Specifies that the contract is governed under English law
	Options	1		
	ReturnUnit	1	0x01	Calendar month
	ReturnPeriod	4	0x00	Uncapped period (e.g. the investment has no end date)
	ReturnGap	1	0x06	Returns every 6 months
	Padding	3		Spare
	Padding	3		Spare

Fig. 17

Property Creation	
BLAR-S4-T1	Transaction-ID
Version number	Version number
1	Number of inputs
<BLAH's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-BLAR PubK-BLAR	ScriptSig
Sequence number	Sequence number
5	Number of outputs
1,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
1,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
1,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
1,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
495,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-BLAR Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 18

House 1 Sale to Alice	
NTDL-S4-T1	Transaction-ID
Version number	Version number
2	Number of inputs
BLAR-S4-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-NTDL Sig-BLAR OP_2 House1MetadataA House1MetadataB PubK-NTDL PubK-BLAR OP_4 OP_CHECKMULTISIG	ScriptSig
<BLAH's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-BLAR PubK-BLAR	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
499,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-BLAR Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 19

Rental Investment Product Creation	
SP-S4-T1	Transaction-ID
Version number	Version number
1	Number of inputs
<SP's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-SP PubK-SP	ScriptSig
Sequence number	Sequence number
2	Number of outputs
100,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
399,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-SP Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 20

Rental Investment Product Creation	
SP-S4-T2	Transaction-ID
Version number	Version number
1	Number of inputs
<SP's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-SP PubK-SP	ScriptSig
Sequence number	Sequence number
2	Number of outputs
200,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Alice Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
299,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-SP Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 21

Alice Onsell her Investment	
ALICE-S4-T1	Transaction-ID
Version number	Version number
2	Number of inputs
SP-S4-T1	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Alice Sig-SP OP_2 House1MetadataA House1MetadataB InvestMetadata1 InvestMetadata2 PubK-Alice PubK-SP OP_6 OP_CHECKMULTISIG	ScriptSig
<Alice's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-Alice PubK-Alice	ScriptSig
Sequence number	Sequence number
4	Number of outputs
51,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
29,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
200,000	Output value
Output script length	Output script length
OP_HASH160 <redeem script hash> OP_EQUAL	Output script
299,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Alice Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 22

Rental Investment Product Creation	
SP-S4-T3	Transaction-ID
Version number	Version number
1	Number of inputs
<SP's previous unspent BTC output - assume 500,000 satoshi>	Prev Trans Output
IDX-00	Prev Trans Output index
Script length	Script length
Sig-SP PubK-SP	ScriptSig
Sequence number	Sequence number
4	Number of outputs
102,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Alice Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
58,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Bob Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
40,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-Eve Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
299,000	Output value
Output script length	Output script length
OP_DUP OP_HASH160 <PubK-SP Hash> OP_EQUALVERIFY OP_CHECKSIG	Output script
LockTime	LockTime

Fig. 23