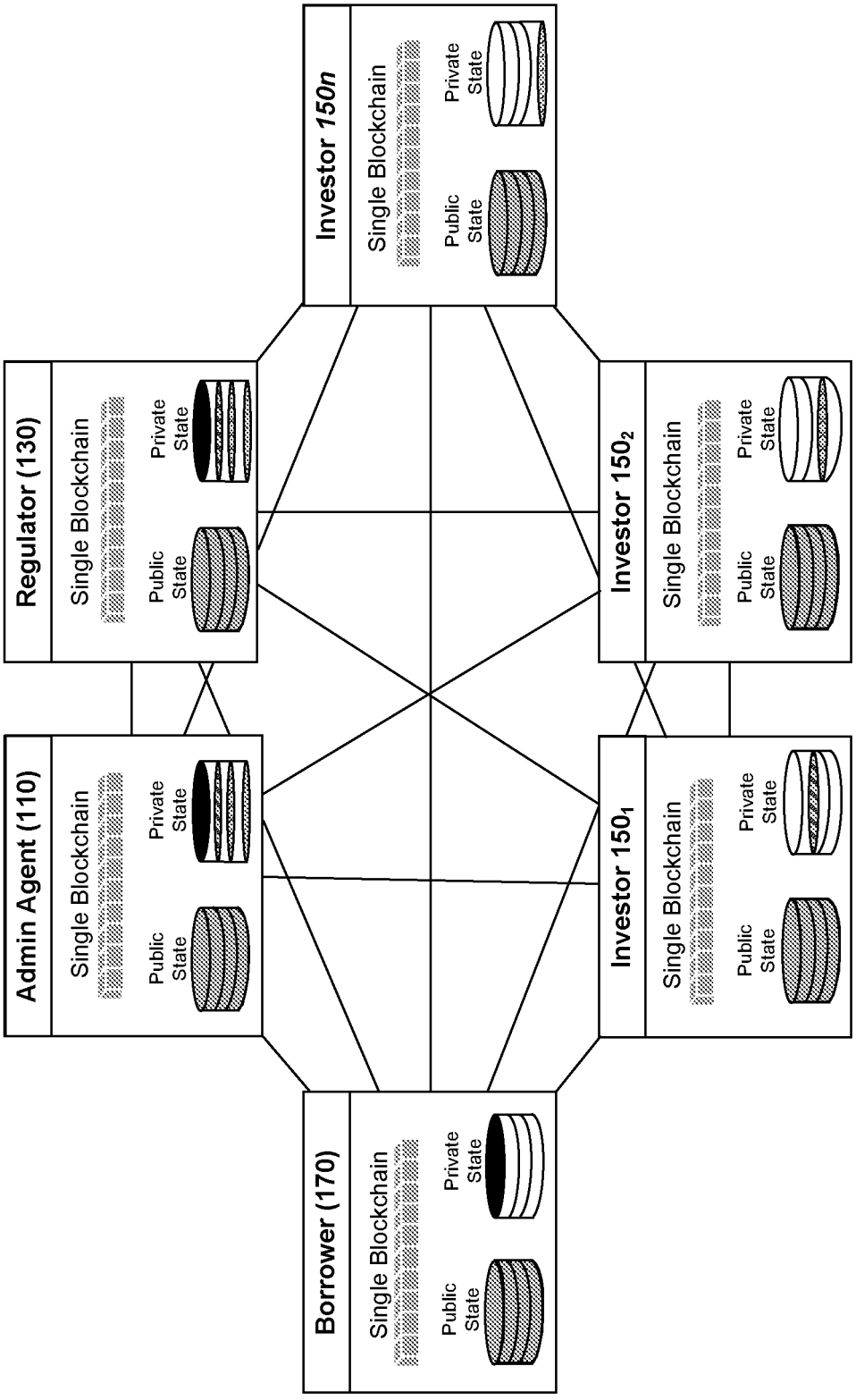
Admin Agent (110)
Single Blockchain
Public State
Private State
Regulator (130)
Single Blockchain
Public State
Private State
Borrower (170)
Single Blockchain
Public State
Private State
Investor 150n
Single Blockchain
Public State
Private State
Investor 150₁
Single Blockchain
Public State
Private State
Investor 150₂
Single Blockchain
Public State
Private State

Figure 1

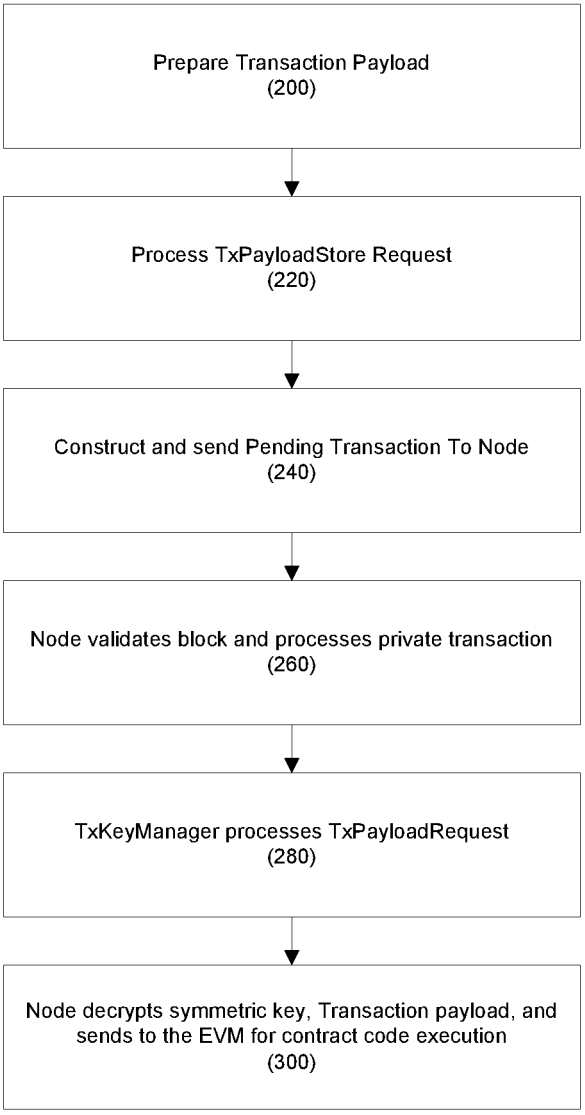
Prepare Transaction Payload
(200)
Process TxPayloadStore Request
(220)
Construct and send Pending Transaction To Node
(240)
Node validates block and processes private transaction
(260)
TxKeyManager processes TxPayloadRequest
(280)
Node decrypts symmetric key, Transaction payload, and sends to the EVM for contract code execution
(300)

Figure 2A

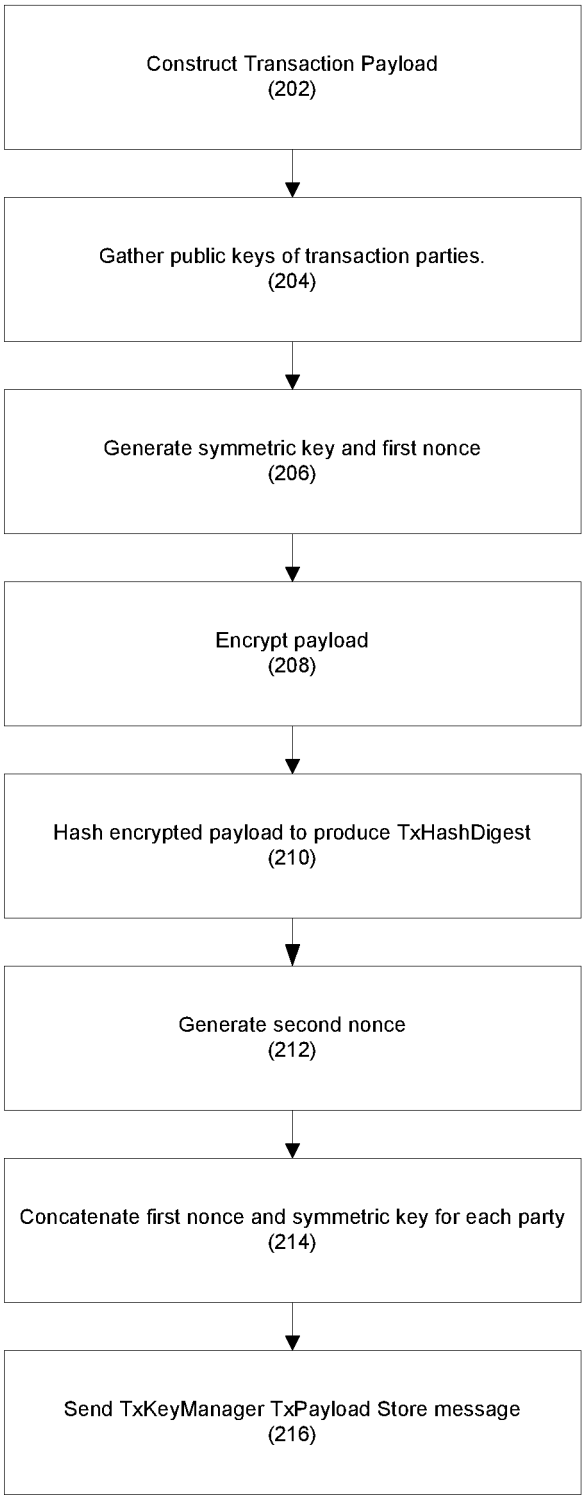
Construct Transaction Payload
(202)
Gather public keys of transaction parties.
(204)
Generate symmetric key and first nonce
(206)
Encrypt payload
(208)
Hash encrypted payload to produce TxHashDigest
(210)
Generate second nonce
(212)
Concatenate first nonce and symmetric key for each party
(214)
Send TxKeyManager TxPayload Store message
(216)

Figure 2B

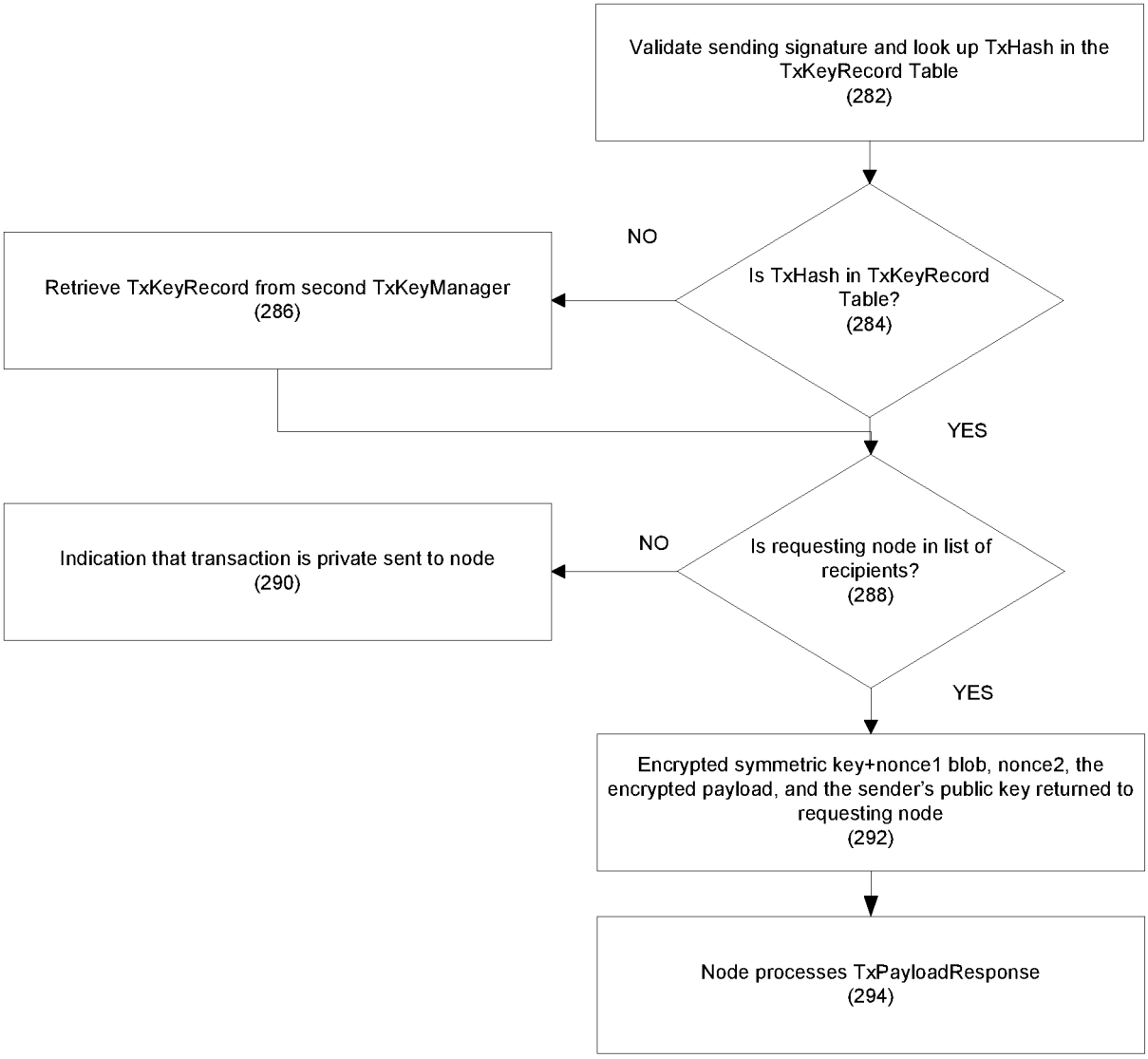
Validate sending signature and look up TxHash in the TxKeyRecord Table
(282)
Is TxHash in TxKeyRecord Table?
(284)
NO
Retrieve TxKeyRecord from second TxKeyManager
(286)
YES
Is requesting node in list of recipients?
(288)
NO
Indication that transaction is private sent to node
(290)
YES
Encrypted symmetric key+nonce1 blob, nonce2, the encrypted payload, and the sender's public key returned to requesting node
(292)
Node processes TxPayloadResponse
(294)

Figure 2C

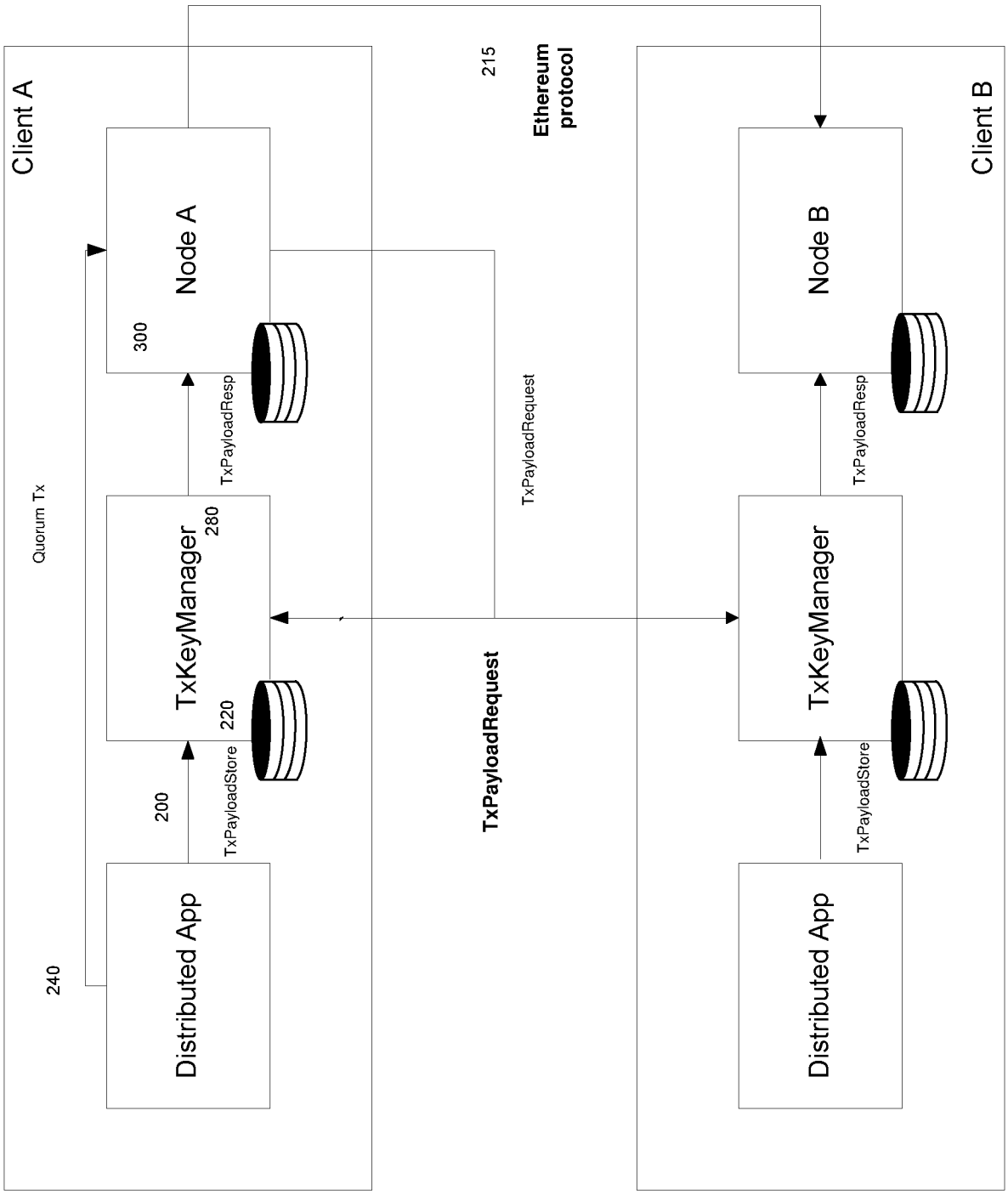
Client A
Client B
Ethereum protocol
215
Node A
300
Node B
TxKeyManager
280
TxKeyManager
220
Distributed App
200
Distributed App
240
TxPayloadResp
TxPayloadResp
TxPayloadStore
TxPayloadStore
TxPayloadRequest
TxPayloadRequest
Quorum Tx

Figure 3

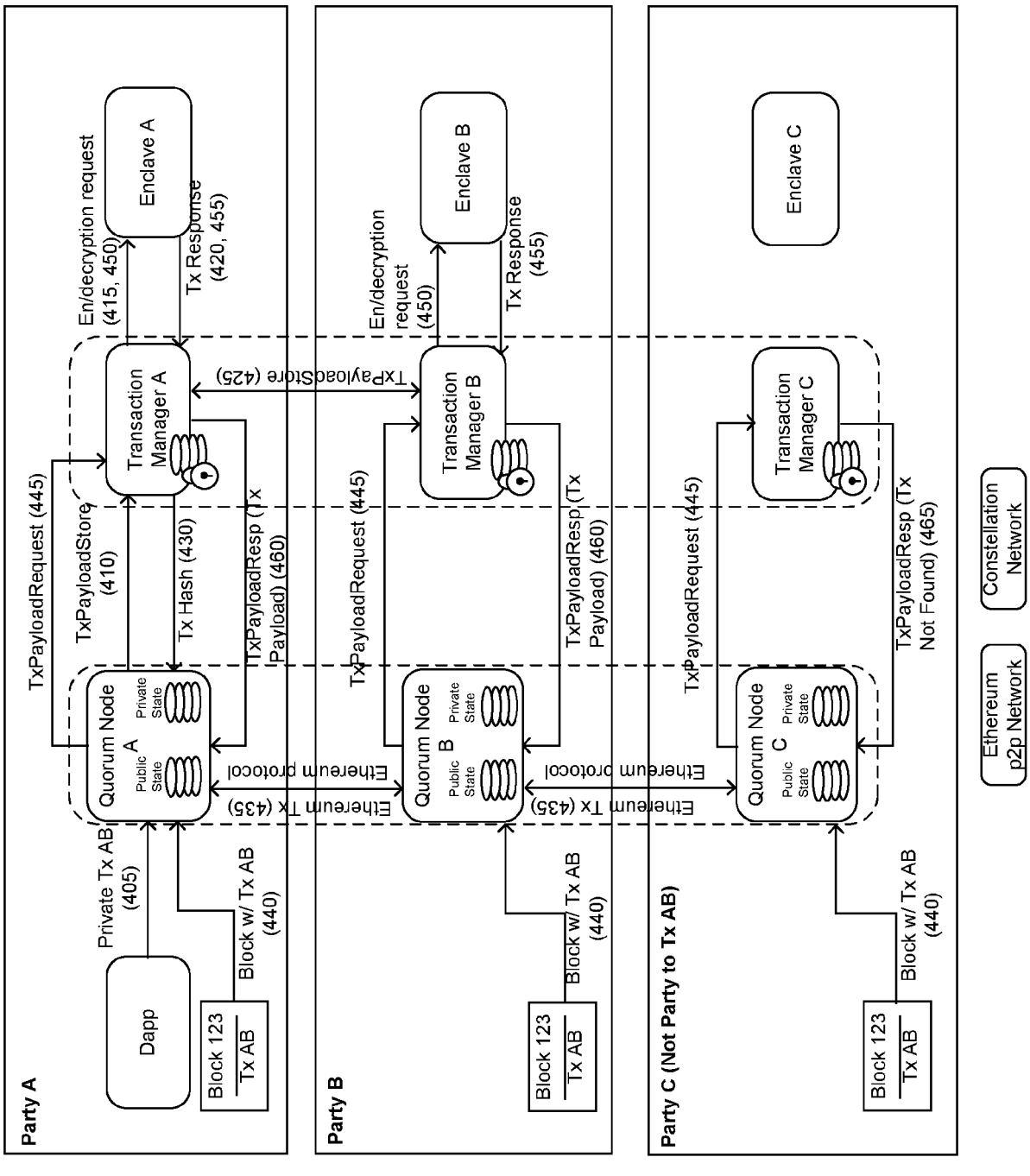
Party A
Party B
Party C (Not Party to Tx AB)
Dapp
Private Tx AB (405)
Block 123
Tx AB
Block w/ Tx AB (440)
Quorum Node A
Public State
Private State
Transaction Manager A
Enclave A
TxPayloadRequest (445)
TxPayloadStore (410)
Tx Hash (430)
En/decryption request (415, 450)
Tx Response (420, 455)
TxPayloadResp (Tx Payload) (460)
Ethereum protocol
Ethereum Tx (435)
TxPayloadStore (425)
Quorum Node B
Transaction Manager B
Enclave B
En/decryption request (450)
Tx Response (455)
Quorum Node C
Transaction Manager C
Enclave C
TxPayloadResp (Tx Not Found) (465)
Ethereum p2p Network
Constellation Network

Figure 4

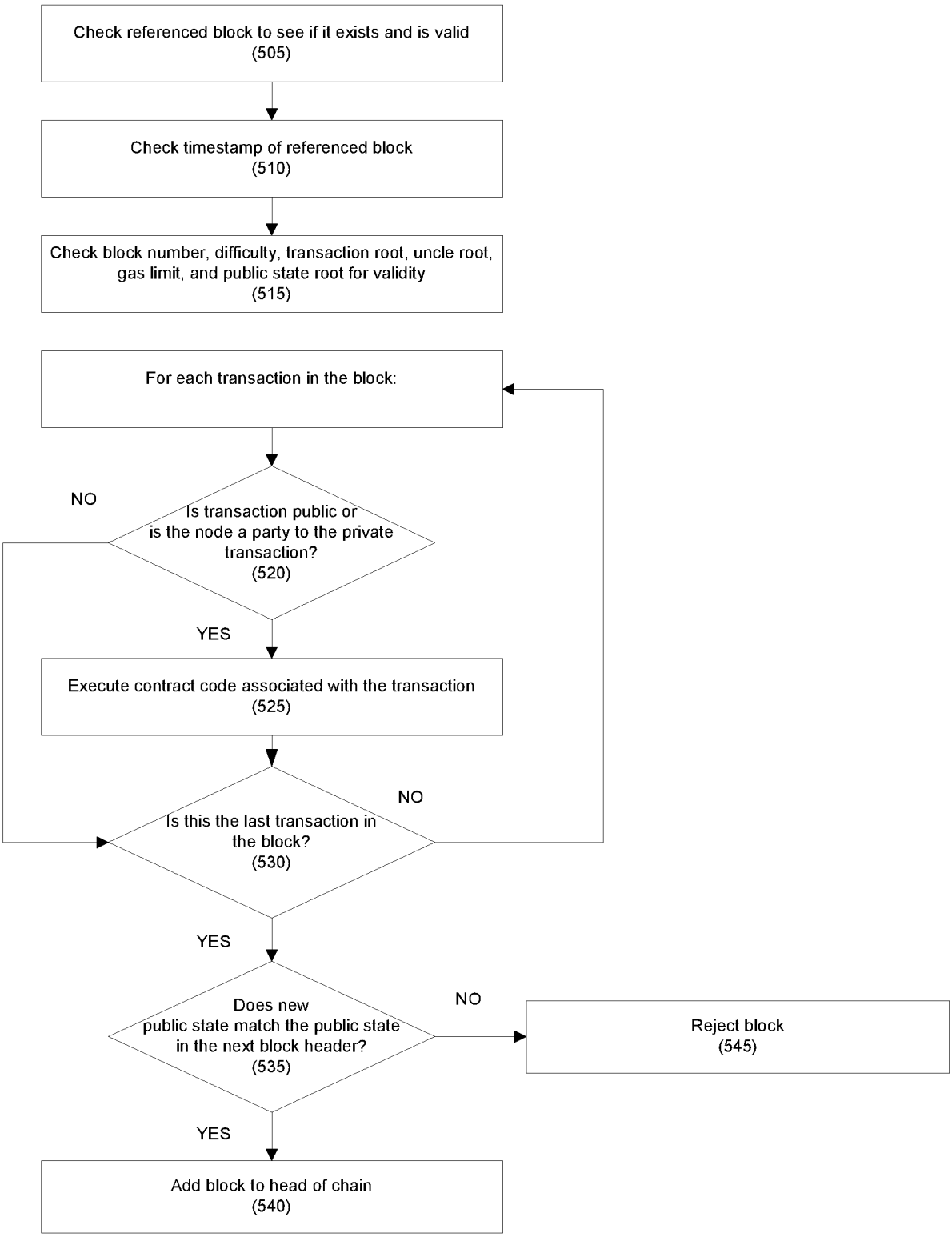
Check referenced block to see if it exists and is valid
(505)
Check timestamp of referenced block
(510)
Check block number, difficulty, transaction root, uncle root, gas limit, and public state root for validity
(515)
For each transaction in the block:
Is transaction public or is the node a party to the private transaction?
(520)
NO
YES
Execute contract code associated with the transaction
(525)
Is this the last transaction in the block?
(530)
NO
YES
Does new public state match the public state in the next block header?
(535)
NO
Reject block
(545)
YES
Add block to head of chain
(540)

Figure 5

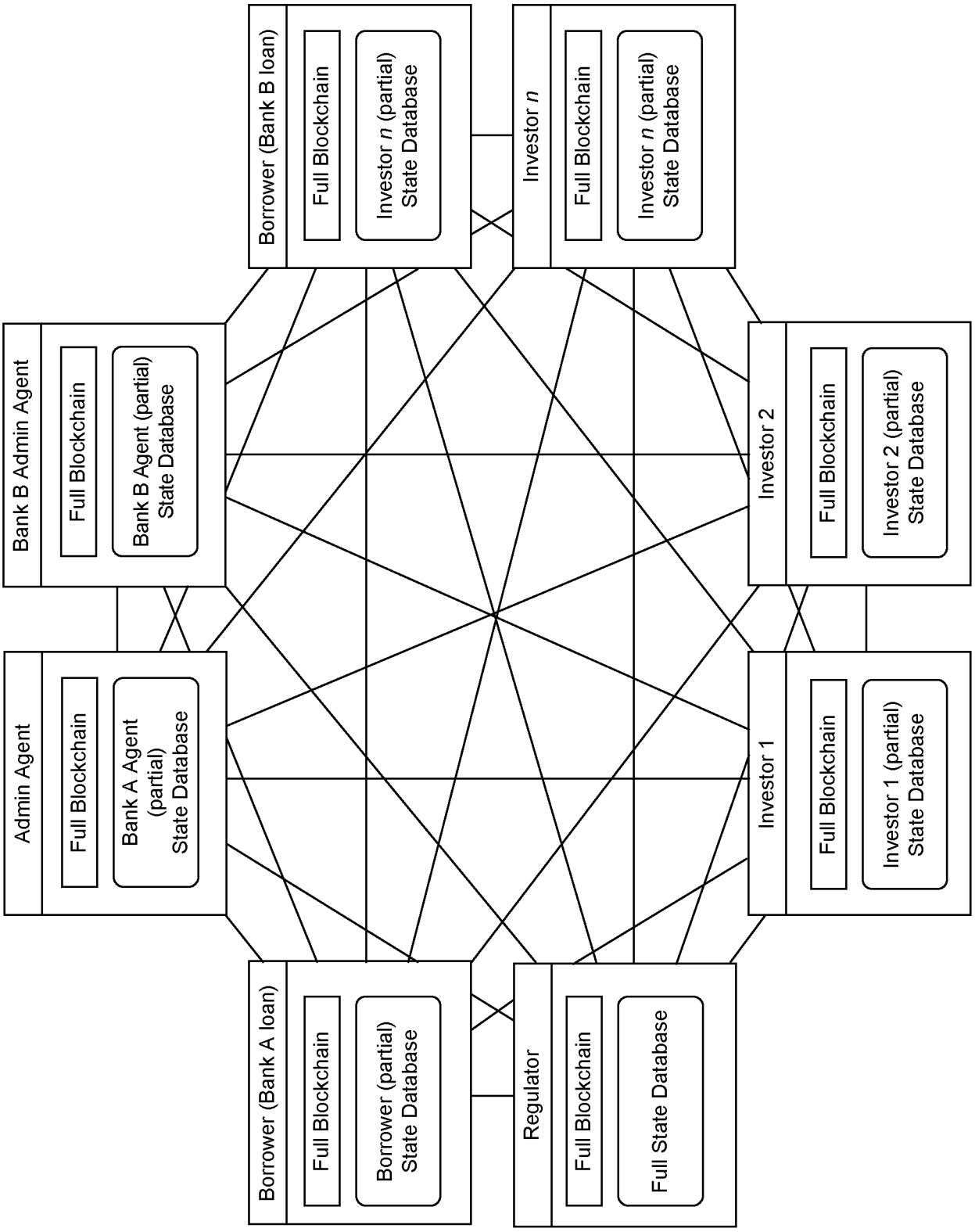
Admin Agent
Full Blockchain
Bank A Agent (partial) State Database
Bank B Admin Agent
Full Blockchain
Bank B Agent (partial) State Database
Borrower (Bank A loan)
Full Blockchain
Borrower (partial) State Database
Borrower (Bank B loan)
Full Blockchain
Investor n (partial) State Database
Regulator
Full Blockchain
Full State Database
Investor n
Full Blockchain
Investor n (partial) State Database
Investor 1
Full Blockchain
Investor 1 (partial) State Database
Investor 2
Full Blockchain
Investor 2 (partial) State Database

Figure 6

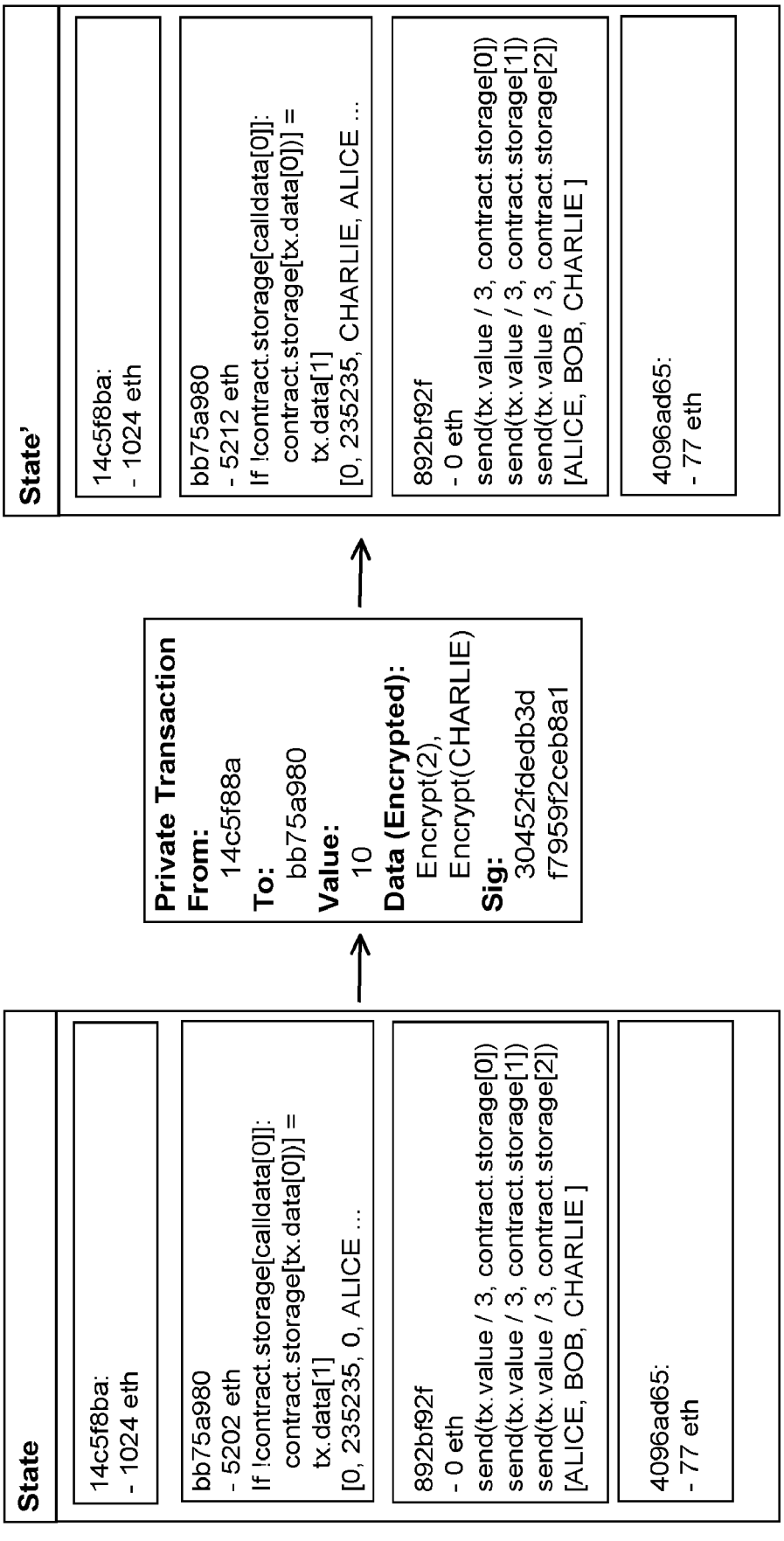
State
14c5f8ba:
- 1024 eth
bb75a980
- 5202 eth
If !contract.storage[calldata[0]]:
contract.storage[tx.data[0]] =
tx.data[1]
[0, 235235, 0, ALICE ...
892bf92f
- 0 eth
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
[ALICE, BOB, CHARLIE]
4096ad65:
- 77 eth
Private Transaction
From:
14c5f88a
To:
bb75a980
Value:
10
Data (Encrypted):
Encrypt(2),
Encrypt(CHARLIE)
Sig:
30452fdedb3d
f7959f2ceb8a1
State'
14c5f8ba:
- 1024 eth
bb75a980
- 5212 eth
If !contract.storage[calldata[0]]:
contract.storage[tx.data[0]] =
tx.data[1]
[0, 235235, CHARLIE, ALICE ...
892bf92f
- 0 eth
send(tx.value / 3, contract.storage[0])
send(tx.value / 3, contract.storage[1])
send(tx.value / 3, contract.storage[2])
[ALICE, BOB, CHARLIE]
4096ad65:
- 77 eth

Figure 7

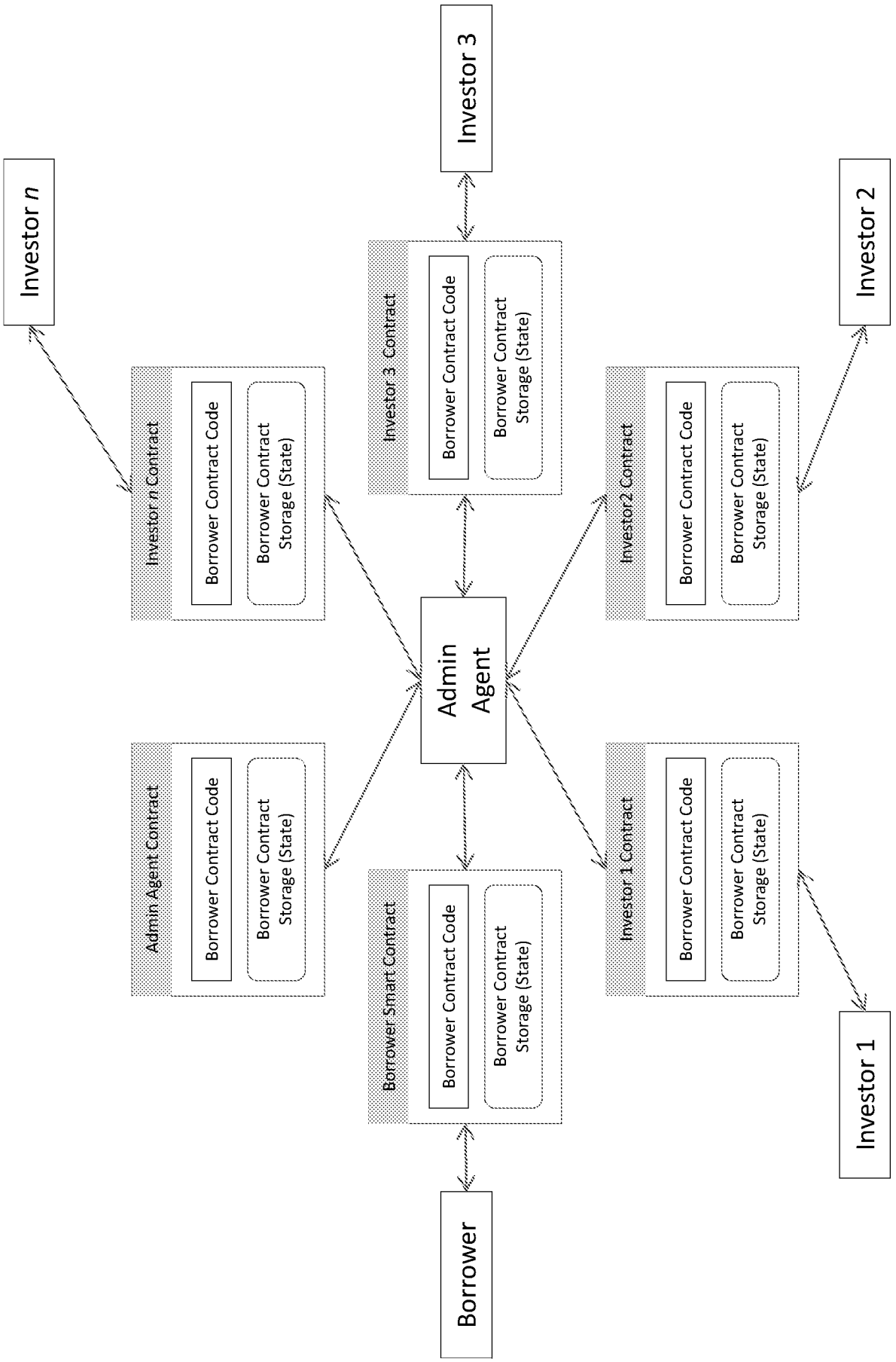
Investor n
Investor 3
Investor 2
Investor n Contract
Borrower Contract Code
Borrower Contract Storage (State)
Investor 3 Contract
Borrower Contract Code
Borrower Contract Storage (State)
Investor2 Contract
Borrower Contract Code
Borrower Contract Storage (State)
Admin Agent
Admin Agent Contract
Borrower Contract Code
Borrower Contract Storage (State)
Borrower Smart Contract
Borrower Contract Code
Borrower Contract Storage (State)
Investor 1 Contract
Borrower Contract Code
Borrower Contract Storage (State)
Borrower
Investor 1

Figure 8