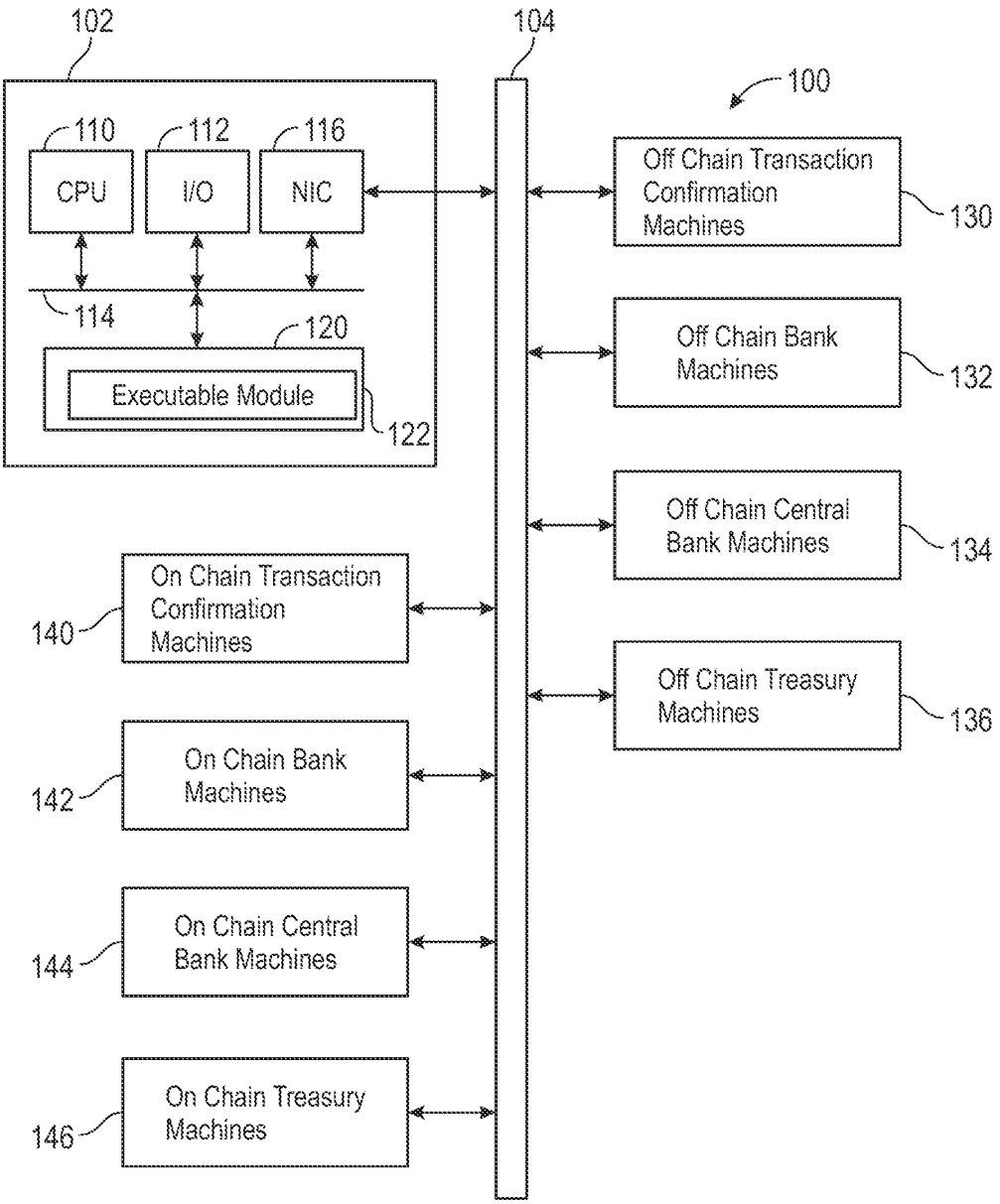

102
104
100
110
112
116
CPU
I/O
NIC
114
120
Executable Module
122
Off Chain Transaction Confirmation Machines
130
Off Chain Bank Machines
132
Off Chain Central Bank Machines
134
Off Chain Treasury Machines
136
On Chain Transaction Confirmation Machines
140
On Chain Bank Machines
142
On Chain Central Bank Machines
144
On Chain Treasury Machines
146

FIG. 1

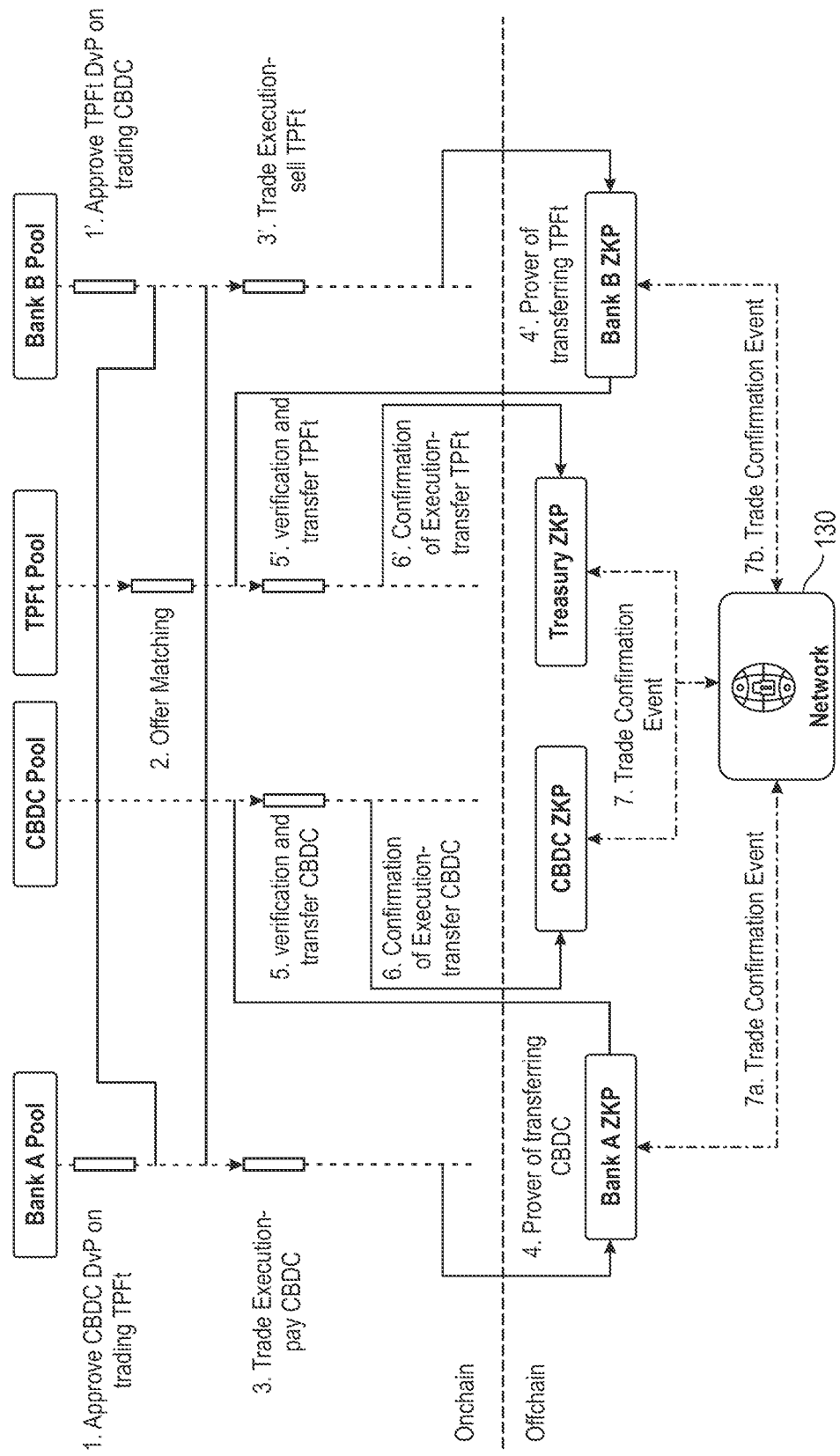

Bank A Pool
CBDC Pool
TPFt Pool
Bank B Pool
1. Approve CBDC DvP on trading TPFt
2. Offer Matching
3. Trade Execution-pay CBDC
4. Prover of transferring CBDC
5. verification and transfer CBDC
6. Confirmation of Execution-transfer CBDC
1'. Approve TPFt DvP on trading CBDC
3'. Trade Execution-sell TPFt
4'. Prover of transferring TPFt
5'. verification and transfer TPFt
6'. Confirmation of Execution-transfer TPFt
Bank A ZKP
CBDC ZKP
Treasury ZKP
Bank B ZKP
7. Trade Confirmation Event
7a. Trade Confirmation Event
7b. Trade Confirmation Event
Network
130
Onchain
Offchain

FIG. 2

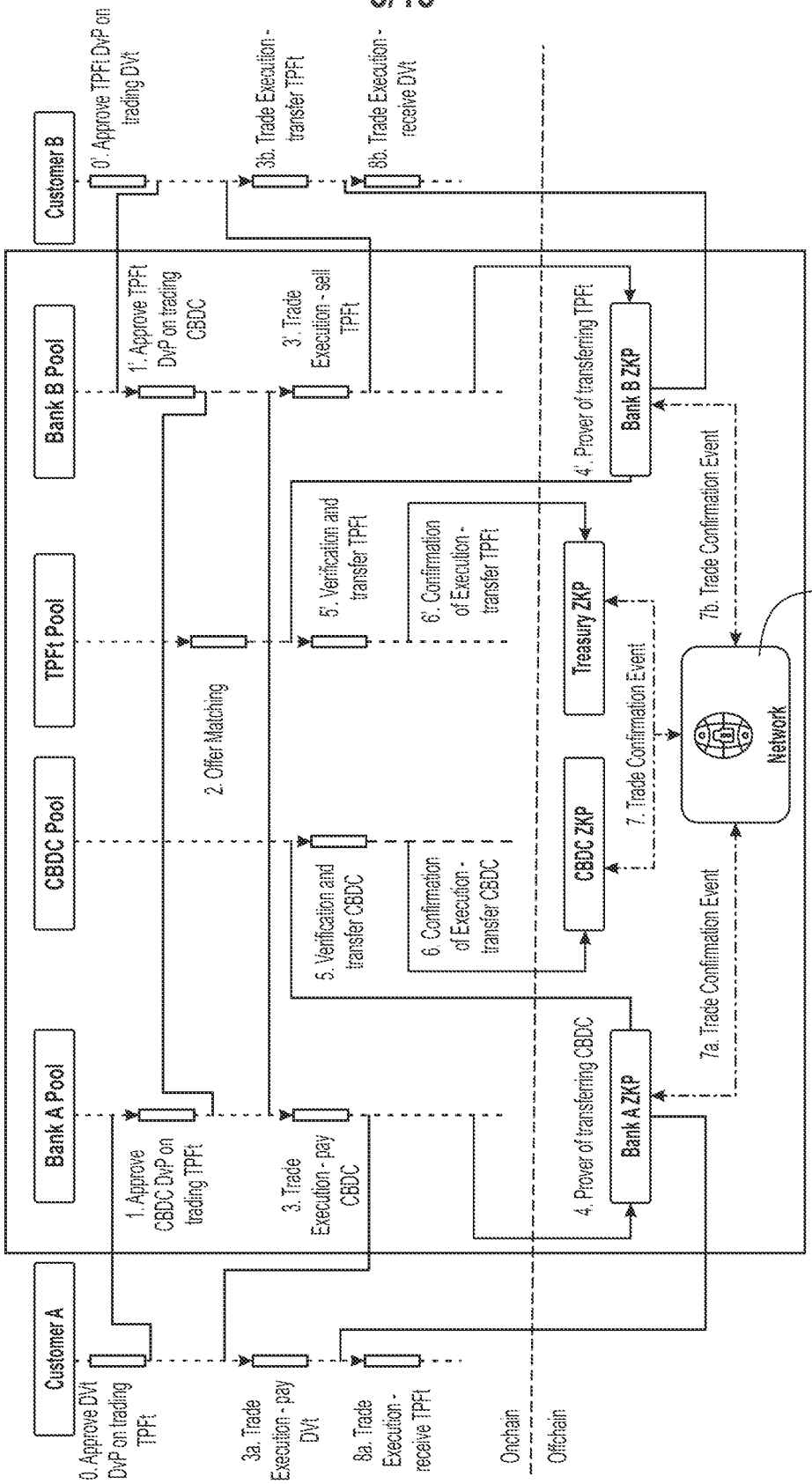

Customer A
Customer B
Bank A Pool
Bank B Pool
CBDC Pool
TPFt Pool
Bank A ZKP
Bank B ZKP
CBDC ZKP
Treasury ZKP
Network
130
0. Approve DVt DvP on trading TPFt
0'. Approve TPFt DvP on trading DVt
1. Approve CBDC DvP on trading TPFt
1'. Approve TPFt DvP on trading CBDC
2. Offer Matching
3. Trade Execution - pay CBDC
3'. Trade Execution - sell TPFt
3a. Trade Execution - pay DVt
3b. Trade Execution - transfer TPFt
4. Prover of transferring CBDC
4'. Prover of transferring TPFt
5. Verification and transfer CBDC
5'. Verification and transfer TPFt
6. Confirmation of Execution - transfer CBDC
6'. Confirmation of Execution - transfer TPFt
7. Trade Confirmation Event
7a. Trade Confirmation Event
7b. Trade Confirmation Event
8a. Trade Execution - receive TPFt
8b. Trade Execution - receive DVt
Onchain
Offchain

FIG. 3

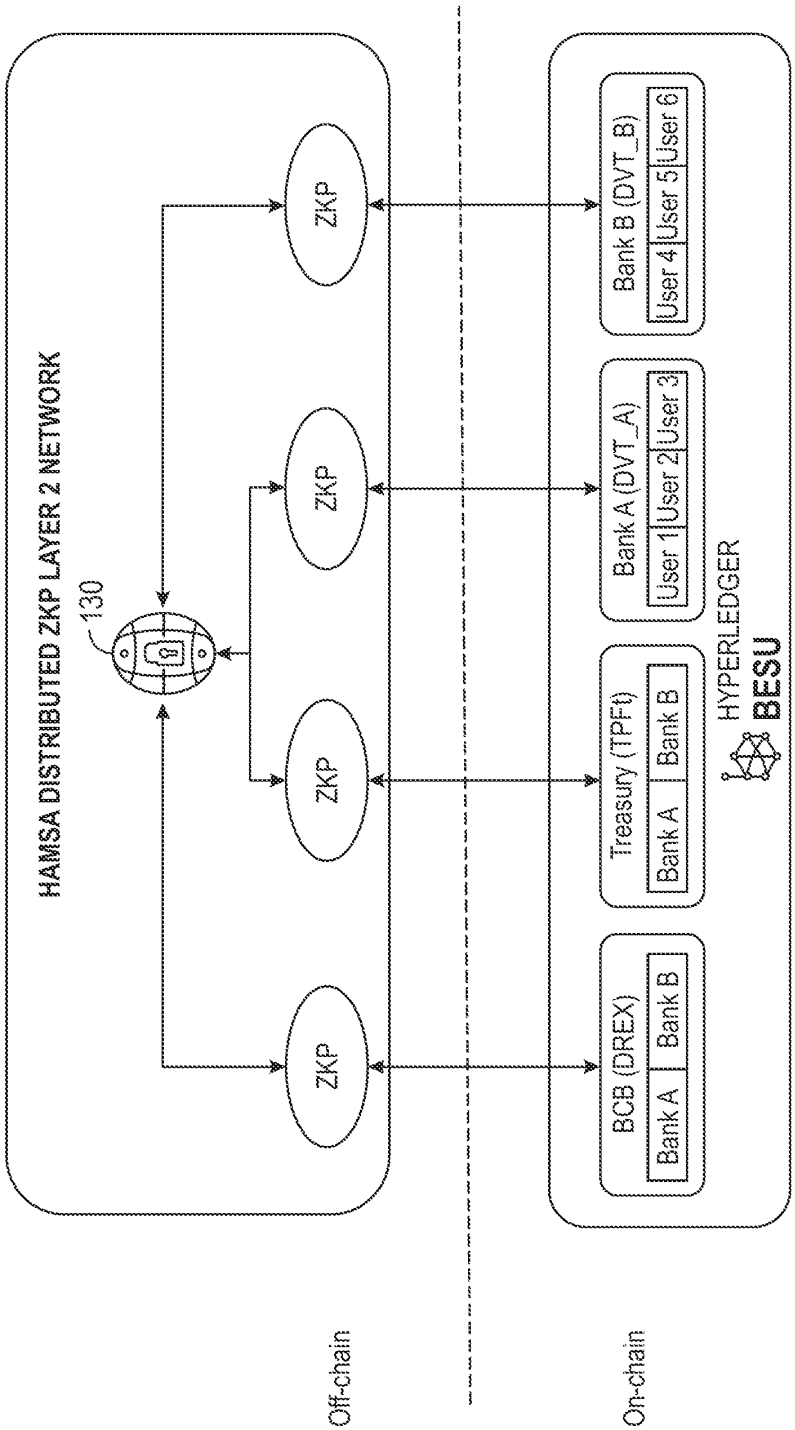

HAMSA DISTRIBUTED ZKP LAYER 2 NETWORK
130
ZKP
ZKP
ZKP
ZKP
Off-chain
On-chain
BCB (DREX)
Bank A
Bank B
Treasury (TPFt)
Bank A
Bank B
Bank A (DVT_A)
User 1
User 2
User 3
Bank B (DVT_B)
User 4
User 5
User 6
HYPERLEDGER
BESU

FIG. 4

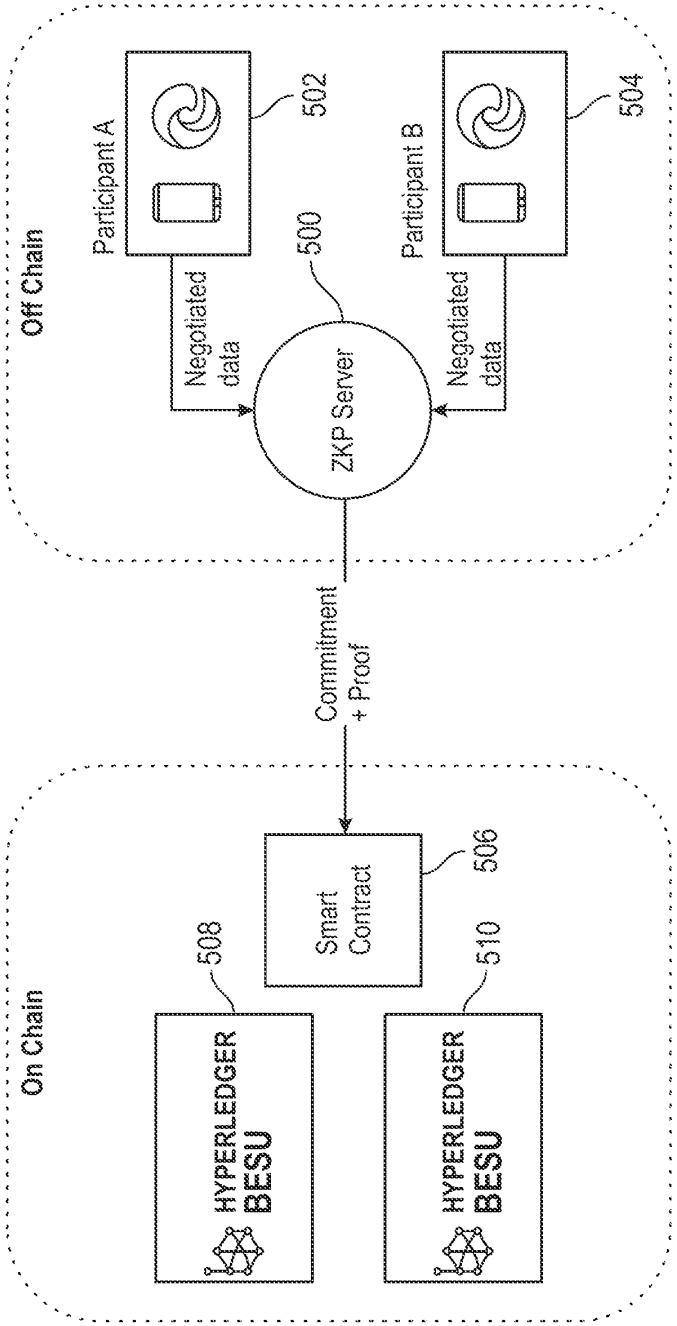

Off Chain
Participant A
502
Participant B
504
500
Negotiated data
ZKP Server
Negotiated data
Commitment + Proof
On Chain
508
Smart Contract
506
510
HYPERLEDGER BESU
HYPERLEDGER BESU

FIG. 5

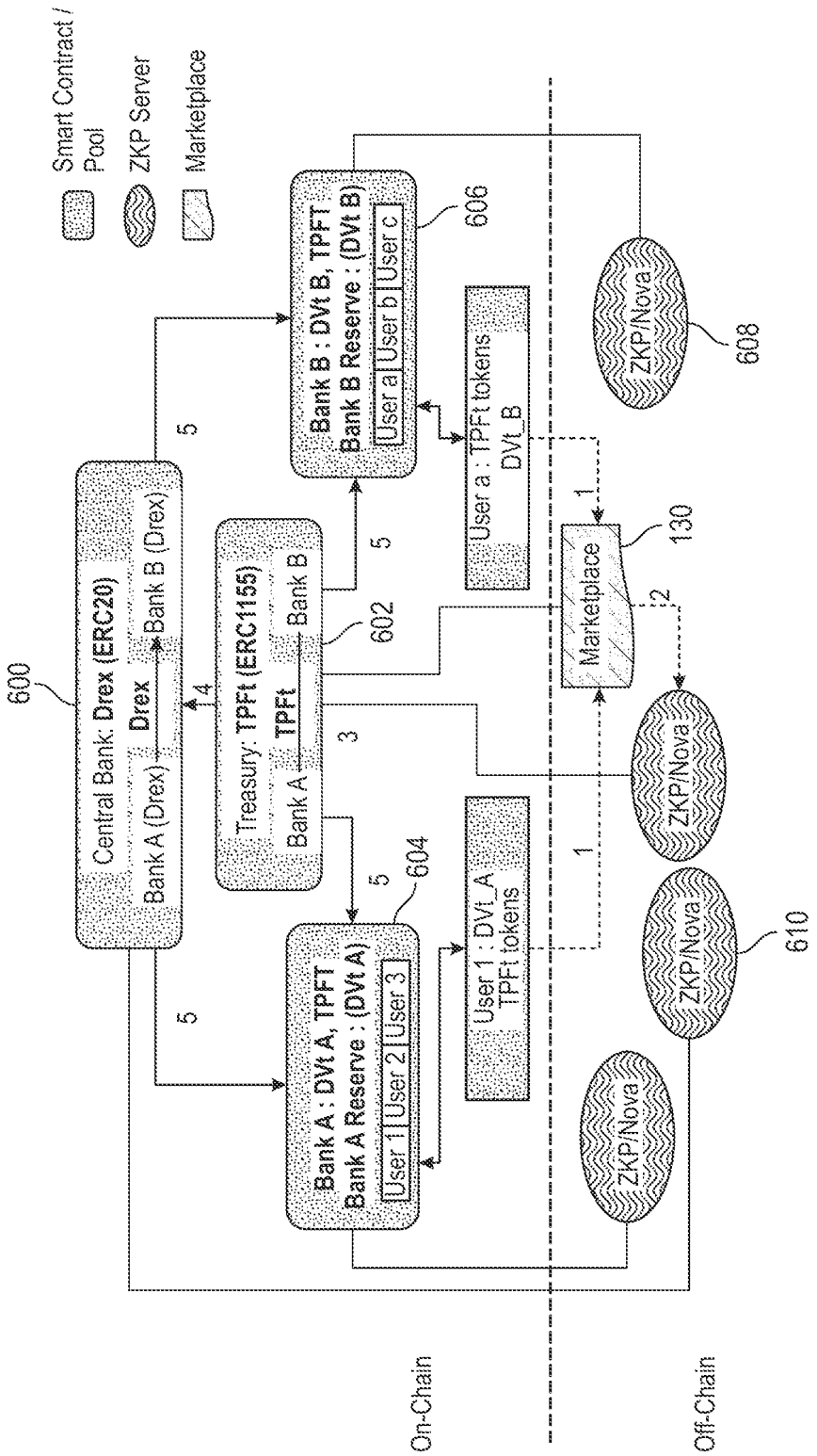

Smart Contract / Pool
ZKP Server
Marketplace
600
Central Bank: Drex (ERC20)
Drex
Bank A (Drex)
Bank B (Drex)
Treasury: TPFt (ERC1155)
TPFt
Bank A
Bank B
602
Bank A : DVt A, TPFT
Bank A Reserve : (DVt A)
User 1 | User 2 | User 3
604
Bank B : DVt B, TPFT
Bank B Reserve : (DVt B)
User a | User b | User c
606
User 1 : DVt_A TPFt tokens
User a : TPFt tokens DVt_B
Marketplace
130
ZKP/Nova
608
610
On-Chain
Off-Chain
1
2
3
4
5

FIG. 6

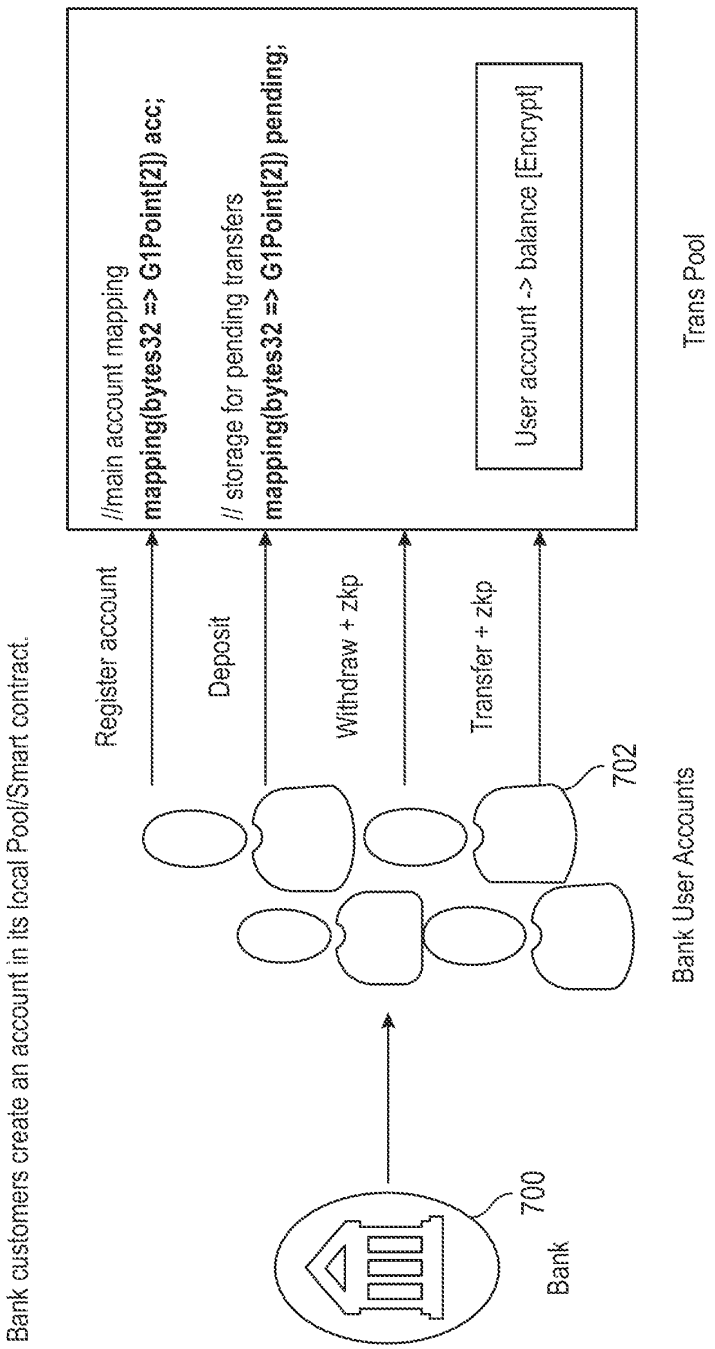

Bank customers create an account in its local Pool/Smart contract.
Register account
Deposit
Withdraw + zkp
Transfer + zkp
//main account mapping
mapping(bytes32 => G1Point[2]) acc;
// storage for pending transfers
mapping(bytes32 => G1Point[2]) pending;
User account -> balance [Encrypt]
Trans Pool
700
Bank
702
Bank User Accounts

FIG. 7

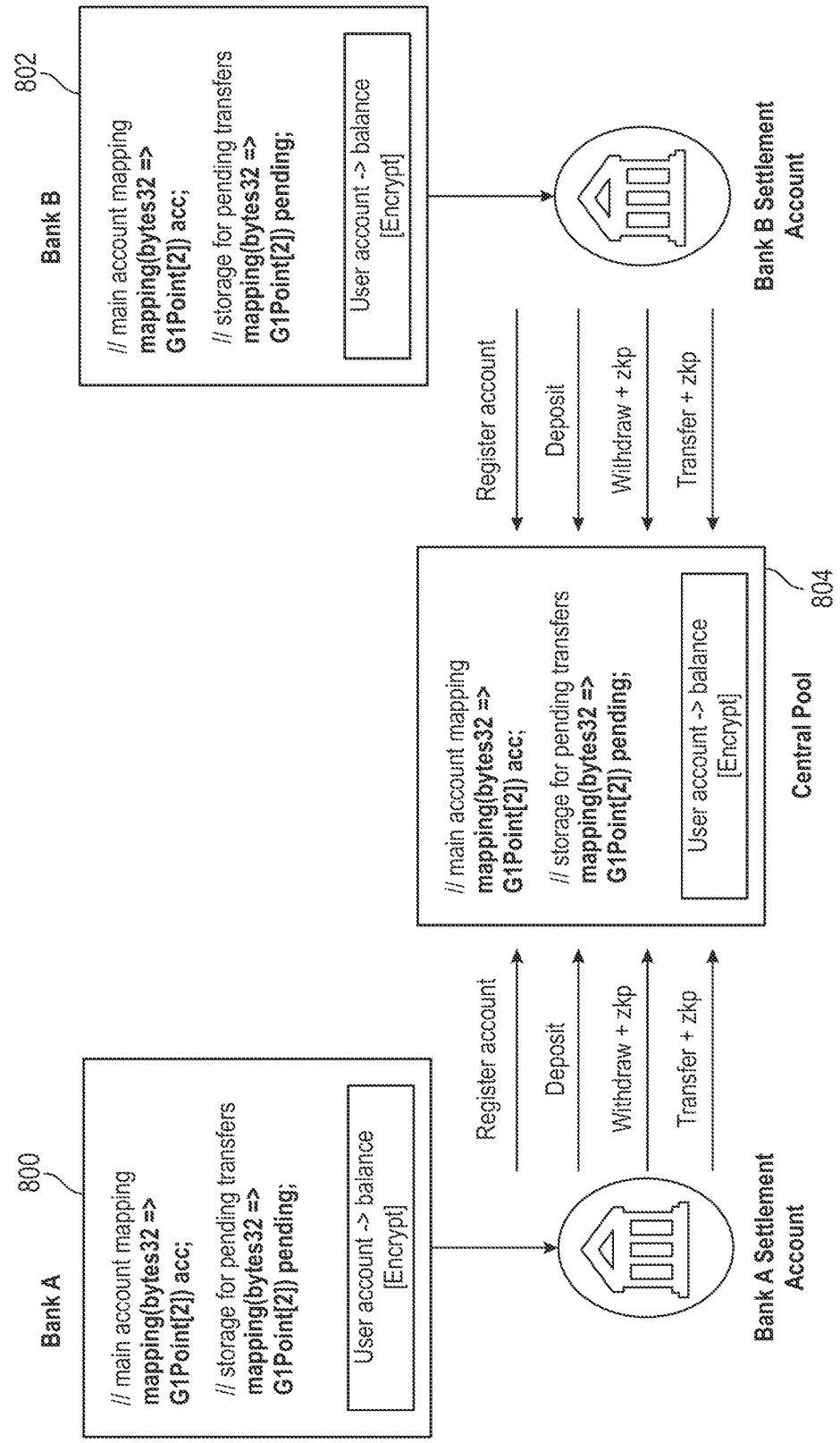

800
Bank A
// main account mapping
mapping(bytes32 =>
G1Point[2]) acc;
// storage for pending transfers
mapping(bytes32 =>
G1Point[2]) pending;
User account -> balance
[Encrypt]
Bank A Settlement
Account
802
Bank B
// main account mapping
mapping(bytes32 =>
G1Point[2]) acc;
// storage for pending transfers
mapping(bytes32 =>
G1Point[2]) pending;
User account -> balance
[Encrypt]
Bank B Settlement
Account
804
Central Pool
// main account mapping
mapping(bytes32 =>
G1Point[2]) acc;
// storage for pending transfers
mapping(bytes32 =>
G1Point[2]) pending;
User account -> balance
[Encrypt]
Register account
Deposit
Withdraw + zkp
Transfer + zkp
Register account
Deposit
Withdraw + zkp
Transfer + zkp

FIG. 8

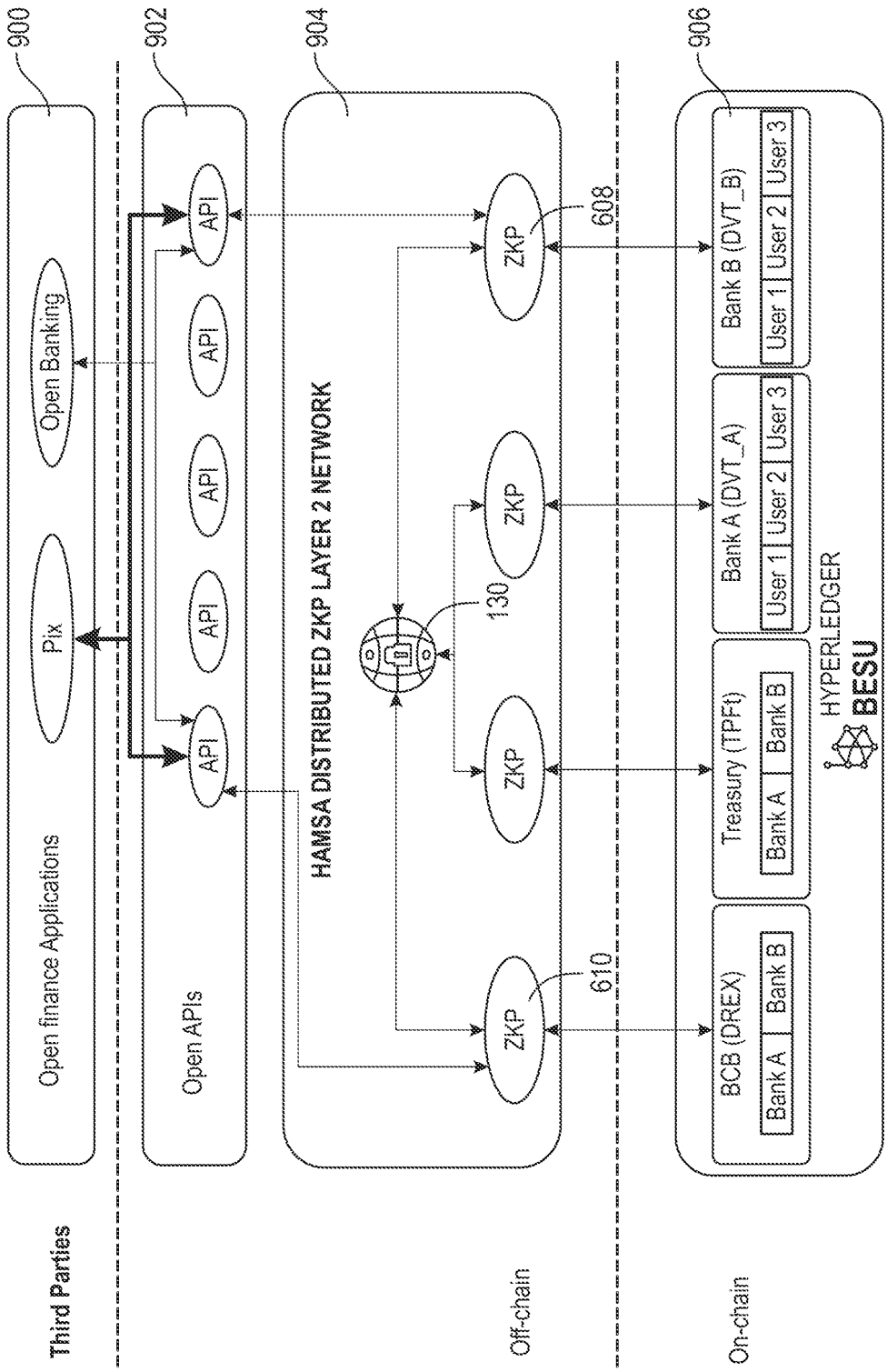

900
902
904
906
Open finance Applications
Open Banking
Pix
Open APIs
API
API
API
API
API
HAMSA DISTRIBUTED ZKP LAYER 2 NETWORK
ZKP
ZKP
ZKP
ZKP
608
610
130
BCB (DREX)
Bank A
Bank B
Treasury (TPFt)
Bank A
Bank B
Bank A (DVT_A)
User 1
User 2
User 3
Bank B (DVT_B)
User 1
User 2
User 3
HYPERLEDGER
BESU
Third Parties
Off-chain
On-chain

FIG. 9

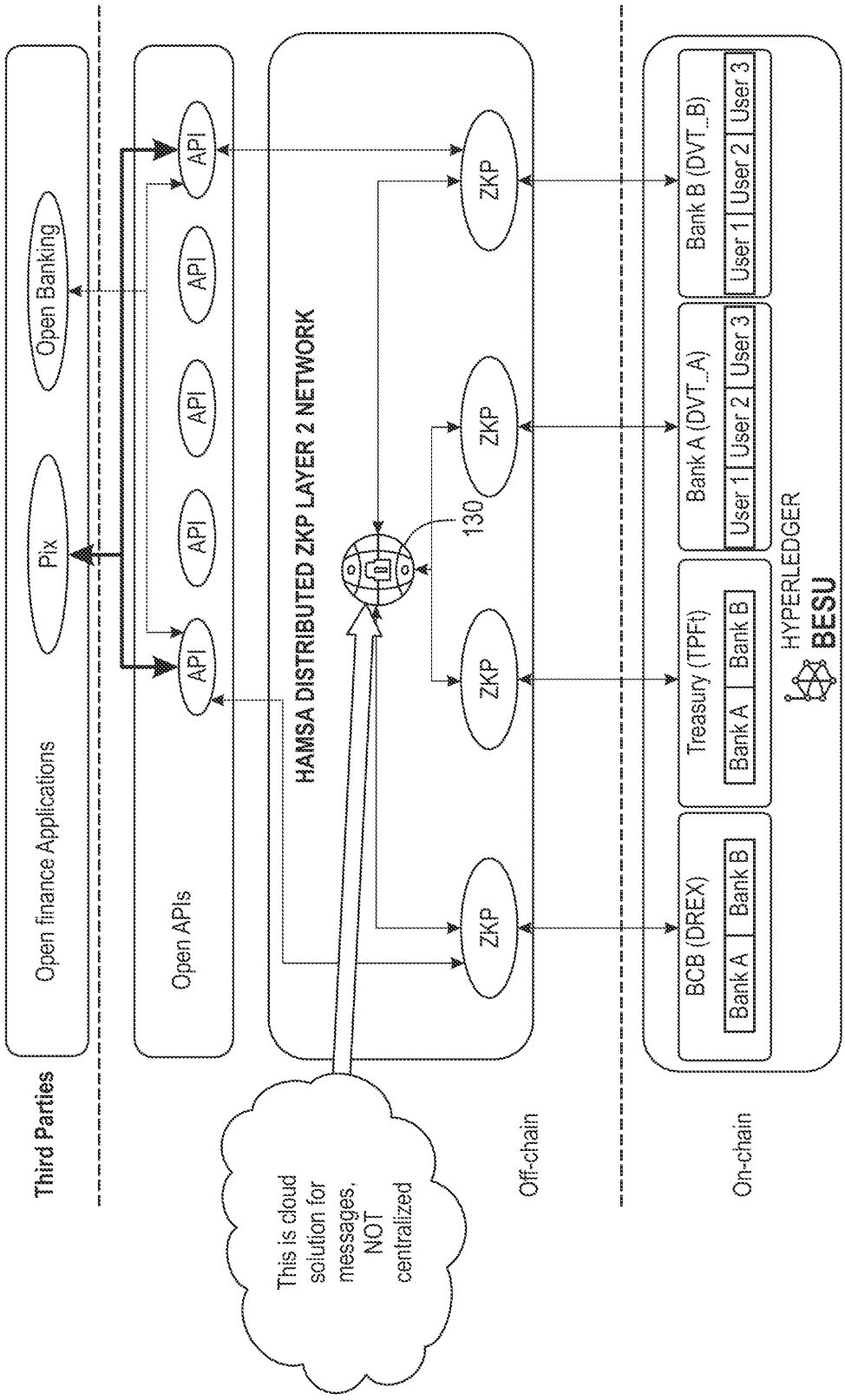

Third Parties
Open finance Applications
Pix
Open Banking
Open APIs
API
API
API
API
API
HAMSA DISTRIBUTED ZKP LAYER 2 NETWORK
130
ZKP
ZKP
ZKP
ZKP
Off-chain
On-chain
BCB (DREX)
Bank A
Bank B
Treasury (TPFt)
Bank A
Bank B
Bank A (DVT_A)
User 1
User 2
User 3
Bank B (DVT_B)
User 1
User 2
User 3
HYPERLEDGER
BESU
This is cloud solution for messages, NOT centralized

FIG. 10

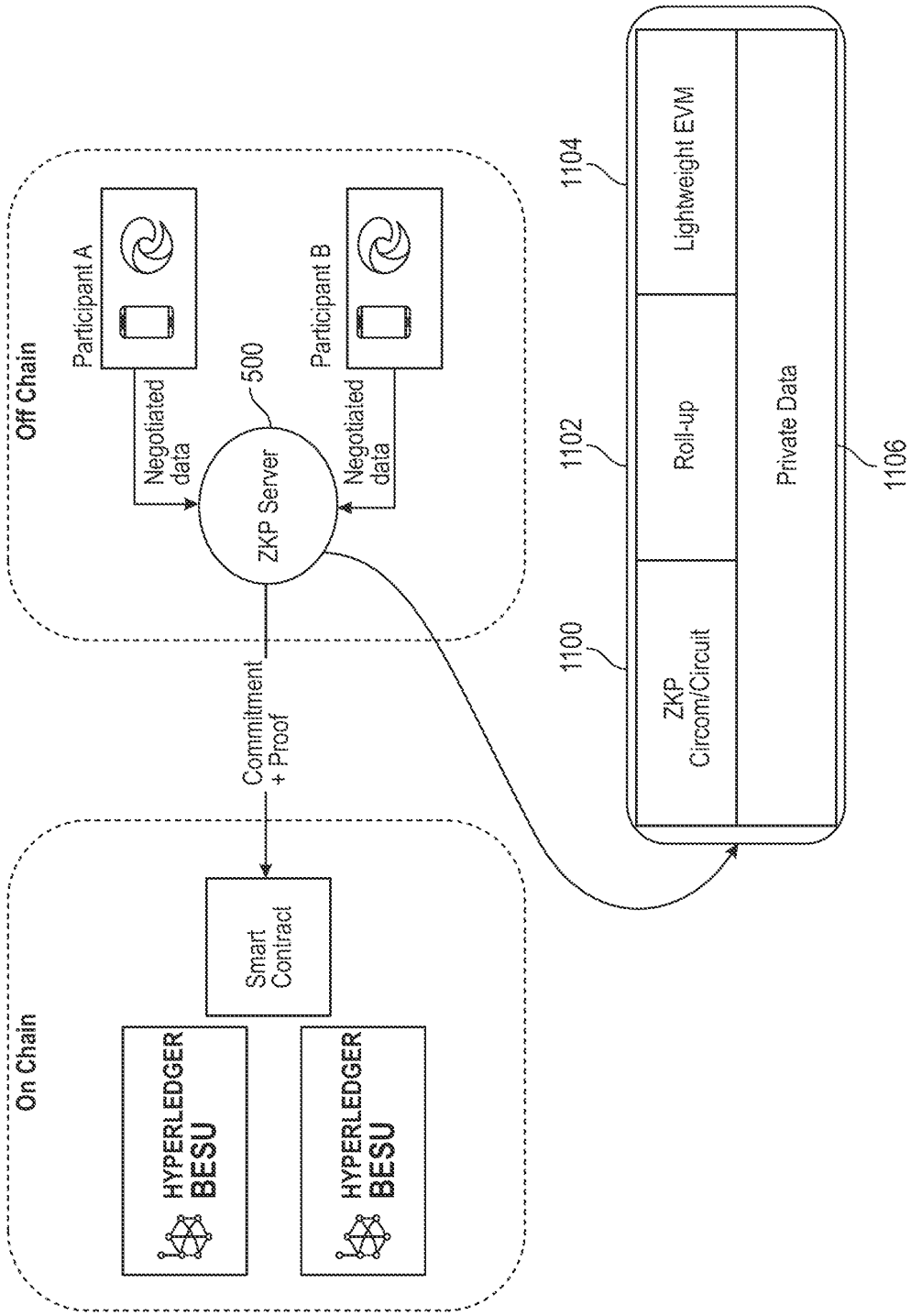

Off Chain
Participant A
Participant B
Negotiated data
Negotiated data
500
ZKP Server
Commitment + Proof
On Chain
Smart Contract
HYPERLEDGER BESU
HYPERLEDGER BESU
1100
ZKP Circom/Circuit
1102
Roll-up
1104
Lightweight EVM
Private Data
1106

FIG. 11

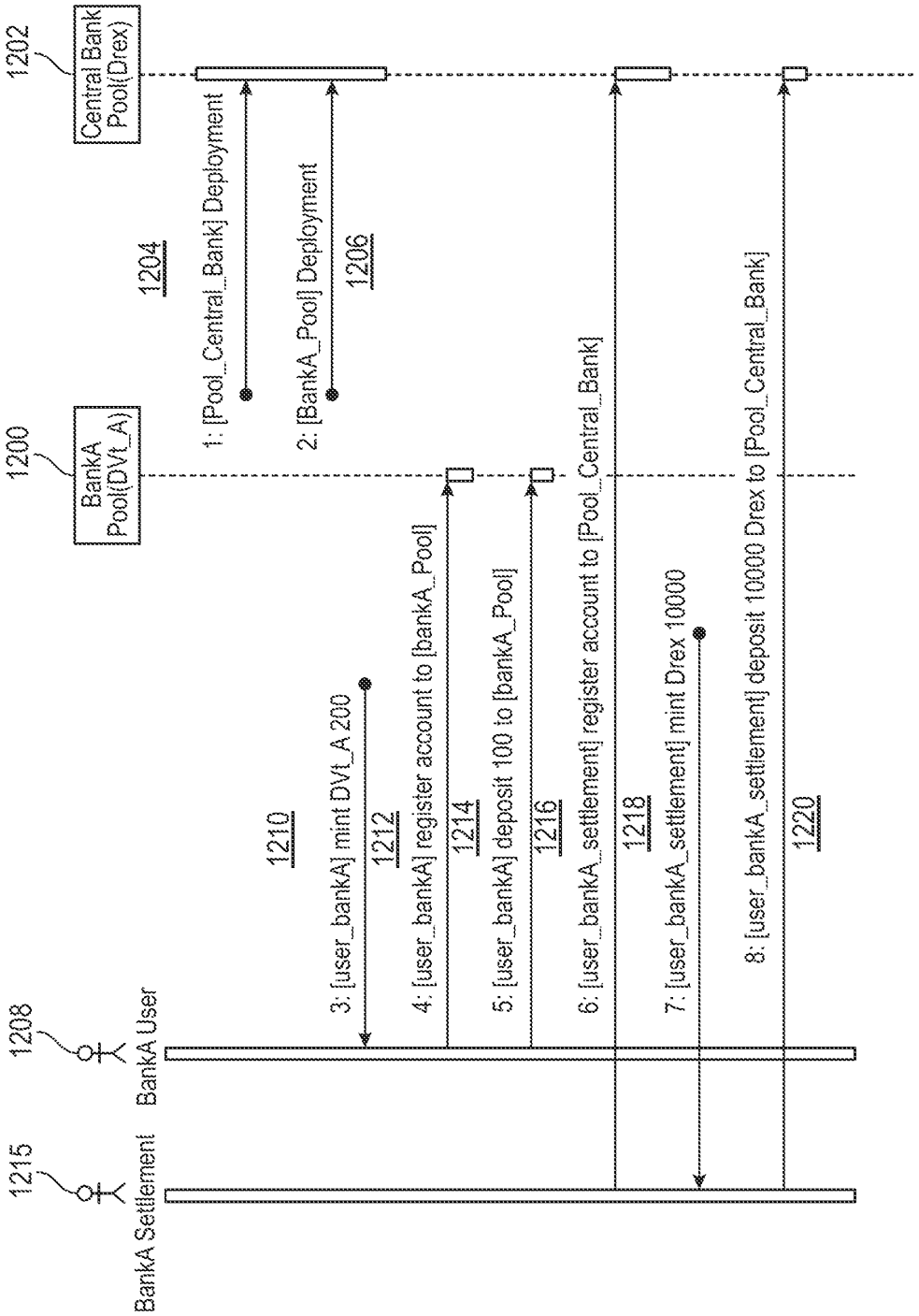

1202
Central Bank Pool(Drex)
1200
BankA Pool(DVt_A)
1204
1: [Pool_Central_Bank] Deployment
2: [BankA_Pool] Deployment
1206
1208
BankA User
1215
BankA Settlement
1210
3: [user_bankA] mint DVt_A 200
1212
4: [user_bankA] register account to [bankA_Pool]
1214
5: [user_bankA] deposit 100 to [bankA_Pool]
1216
6: [user_bankA_settlement] register account to [Pool_Central_Bank]
1218
7: [user_bankA_settlement] mint Drex 10000
8: [user_bankA_settlement] deposit 10000 Drex to [Pool_Central_Bank]
1220

FIG. 12

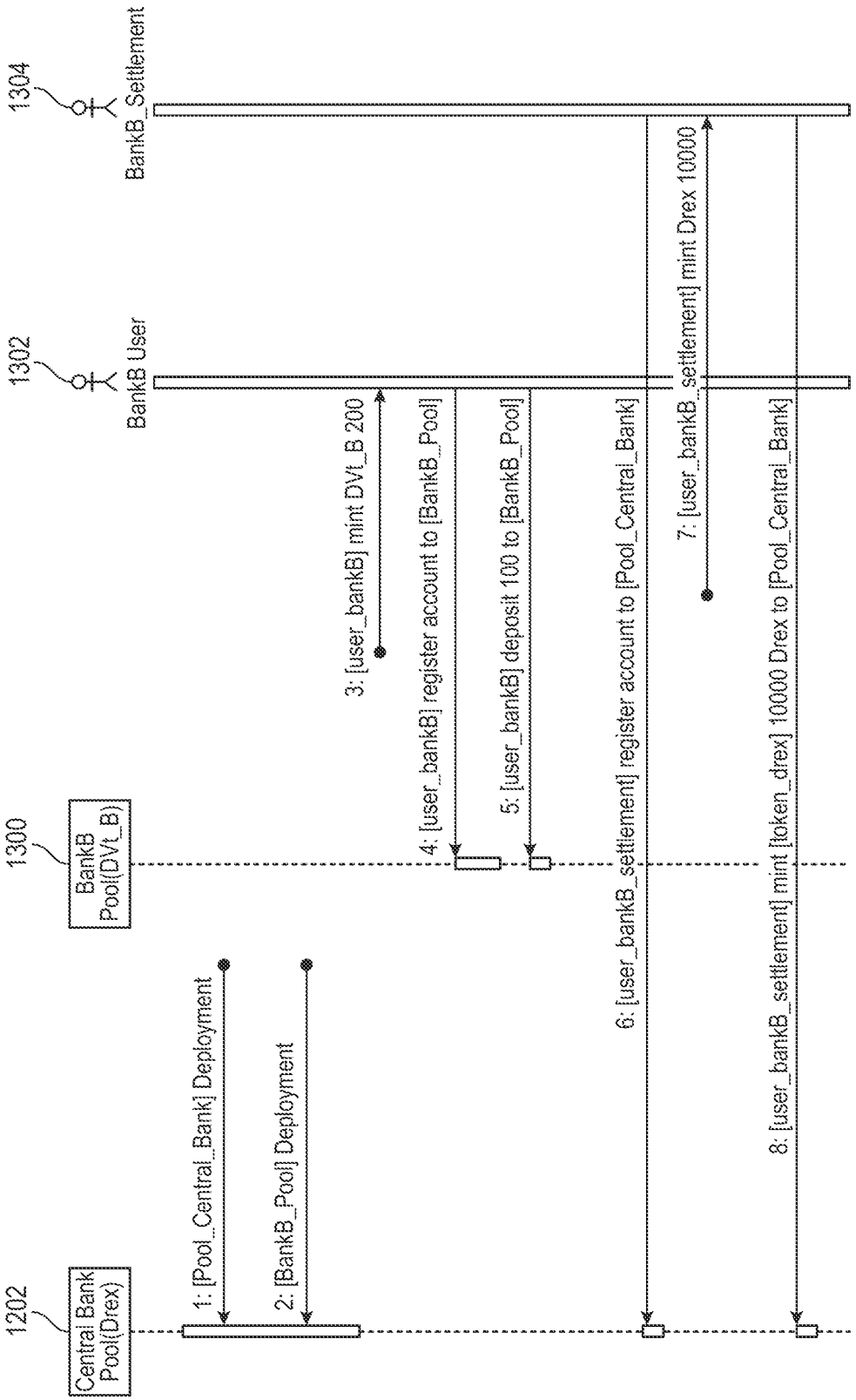

1202
Central Bank Pool(Drex)
1300
BankB Pool(DVt_B)
1302
BankB User
1304
BankB_Settlement
1: [Pool_Central_Bank] Deployment
2: [BankB_Pool] Deployment
3: [user_bankB] mint DVt_B 200
4: [user_bankB] register account to [BankB_Pool]
5: [user_bankB] deposit 100 to [BankB_Pool]
6: [user_bankB_settlement] register account to [Pool_Central_Bank]
7: [user_bankB_settlement] mint Drex 10000
8: [user_bankB_settlement] mint [token_drex] 10000 Drex to [Pool_Central_Bank]

FIG. 13

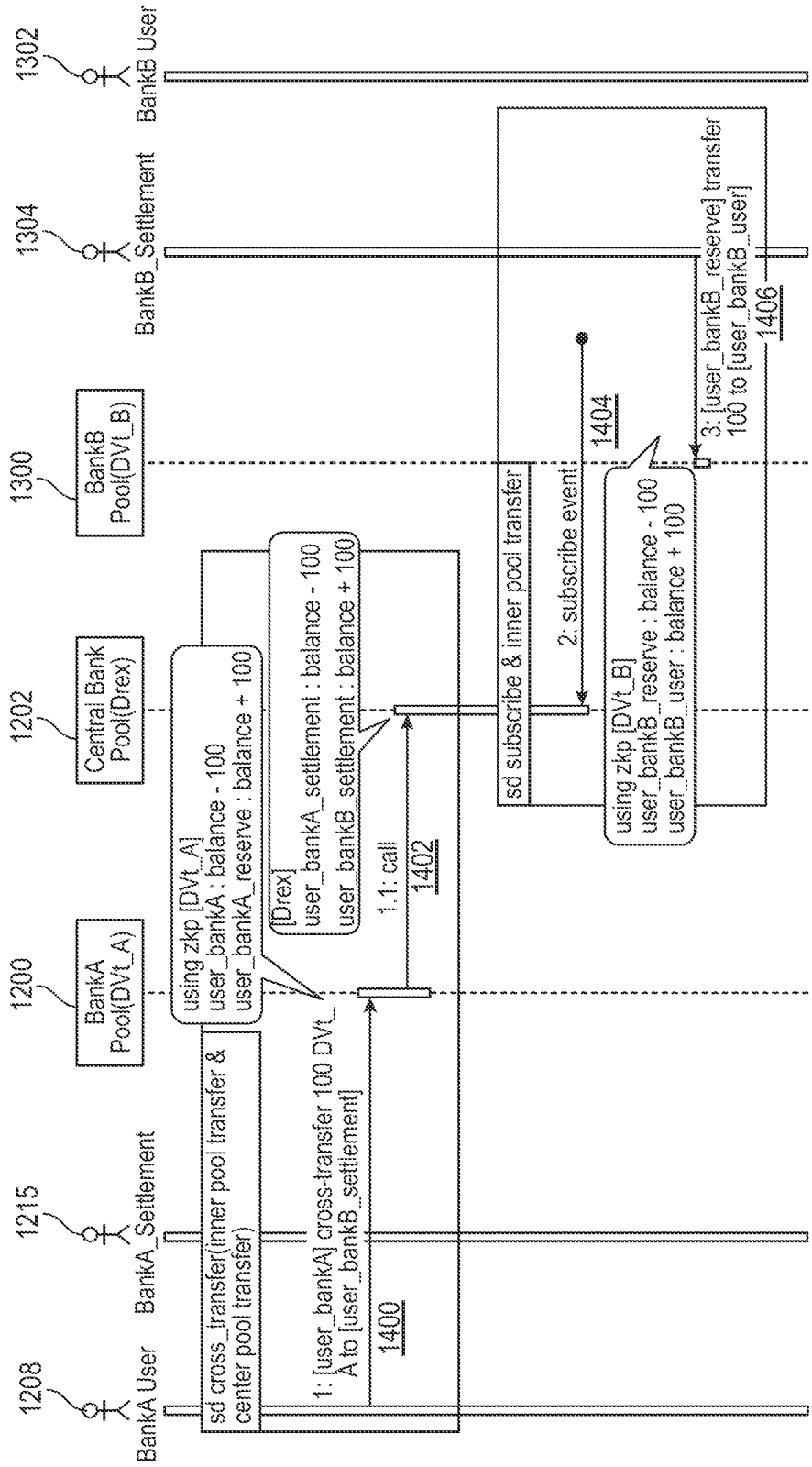

1208
BankA User
1215
BankA_Settlement
1200
BankA Pool(DVt_A)
1202
Central Bank Pool(Drex)
1300
BankB Pool(DVt_B)
1304
BankB_Settlement
1302
BankB User
sd cross_transfer(inner pool transfer & center pool transfer)
1: [user_bankA] cross-transfer 100 DVt_A to [user_bankB_settlement]
1400
using zkp [DVt_A]
user_bankA : balance - 100
user_bankA_reserve : balance + 100
[Drex]
user_bankA_settlement : balance - 100
user_bankB_settlement : balance + 100
1.1: call
1402
sd subscribe & inner pool transfer
2: subscribe event
1404
using zkp [DVt_B]
user_bankB_reserve : balance - 100
user_bankB_user : balance + 100
3: [user_bankB_reserve] transfer 100 to [user_bankB_user]
1406

FIG. 14

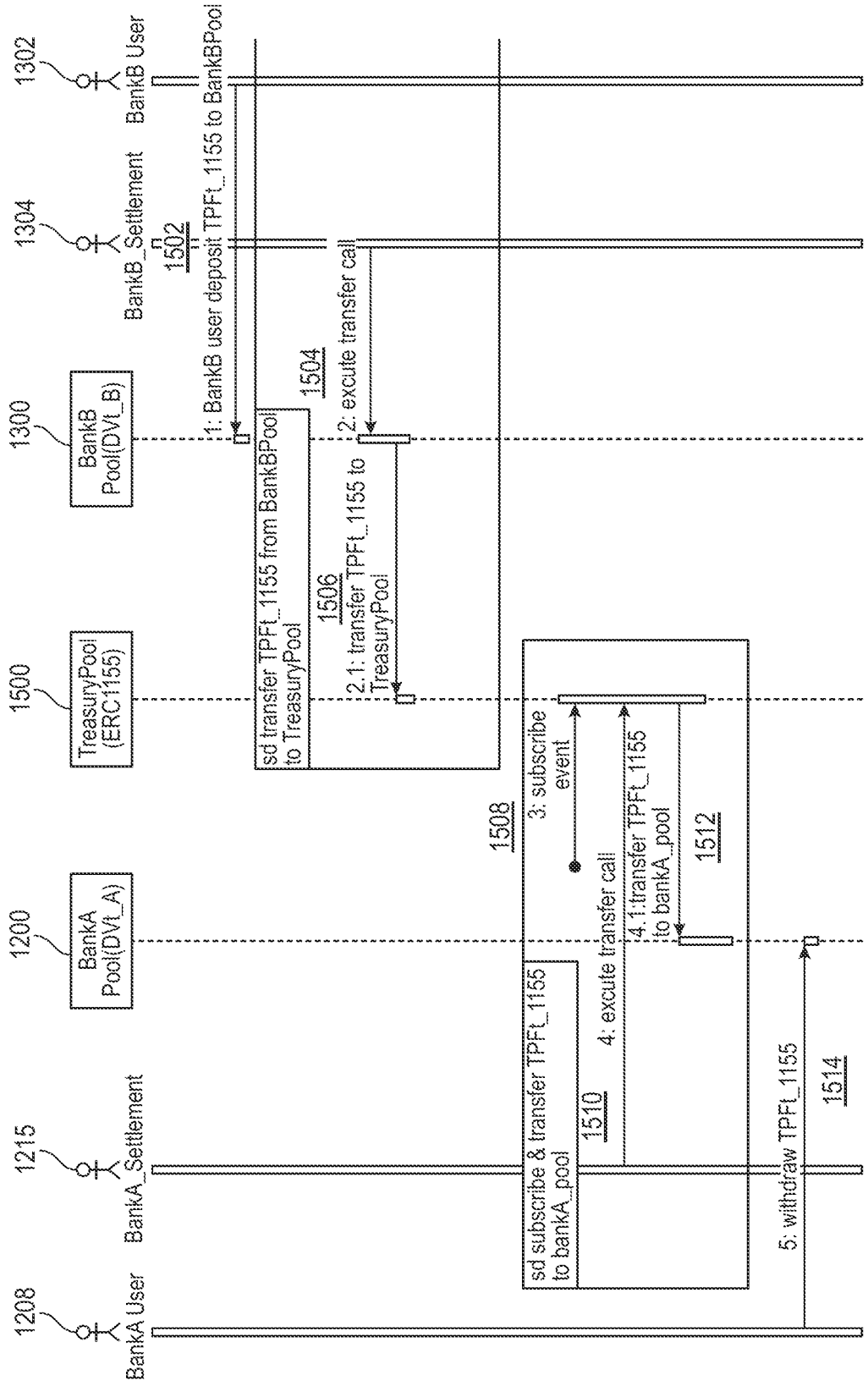

1302
BankB User
1304
BankB_Settlement
1502
1: BankB user deposit TPFt_1155 to BankBPool
1300
BankB Pool(DVt_B)
1504
2: excute transfer call
sd transfer TPFt_1155 from BankBPool to TreasuryPool
1506
2.1: transfer TPFt_1155 to TreasuryPool
1500
TreasuryPool (ERC1155)
1508
3: subscribe event
1200
BankA Pool(DVt_A)
4: excute transfer call
4.1:transfer TPFt_1155 to bankA_pool
1512
sd subscribe & transfer TPFt_1155 to bankA_pool
1510
1215
BankA_Settlement
5: withdraw TPFt_1155
1514
1208
BankA User

FIG. 15