Figure 1

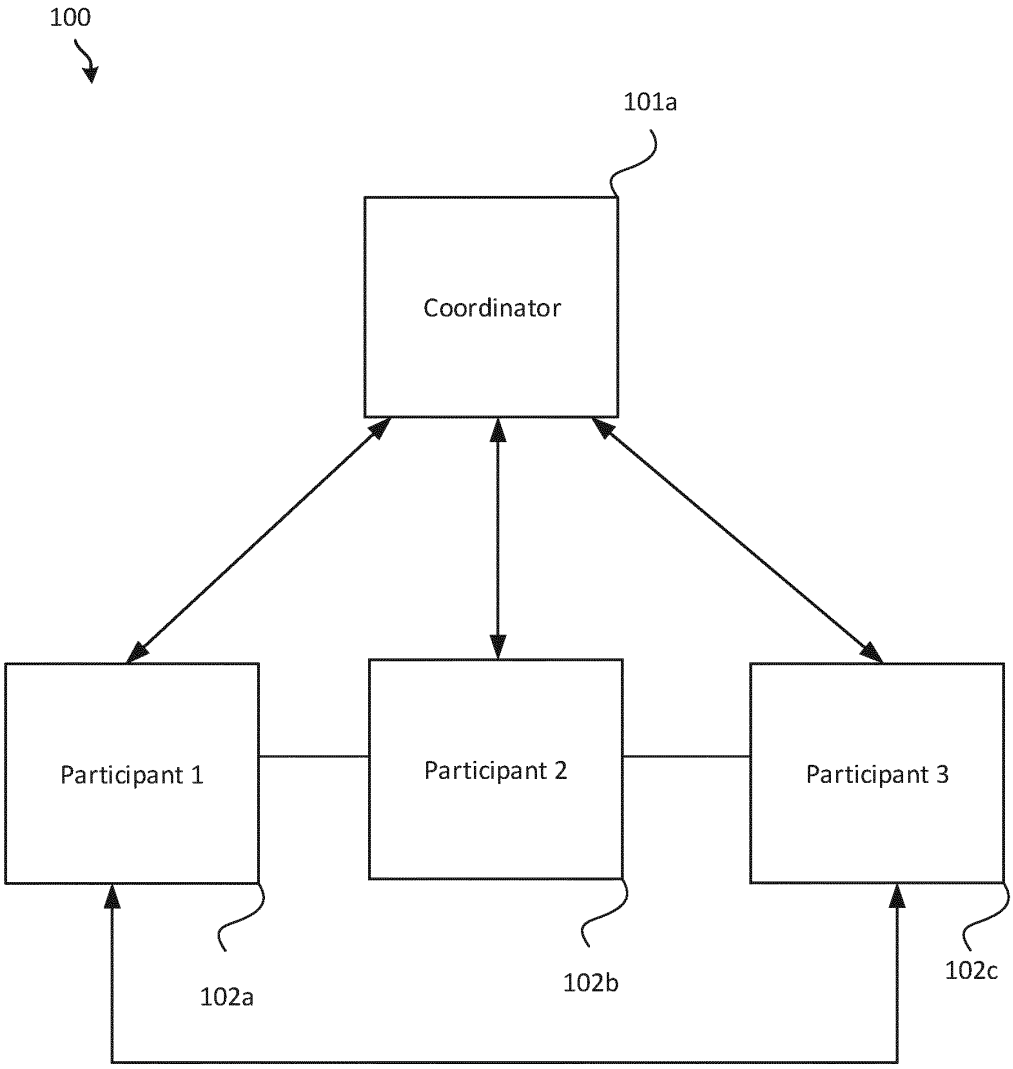

100
101a
Coordinator
Participant 1
Participant 2
Participant 3
102a
102b
102c

Figure 2

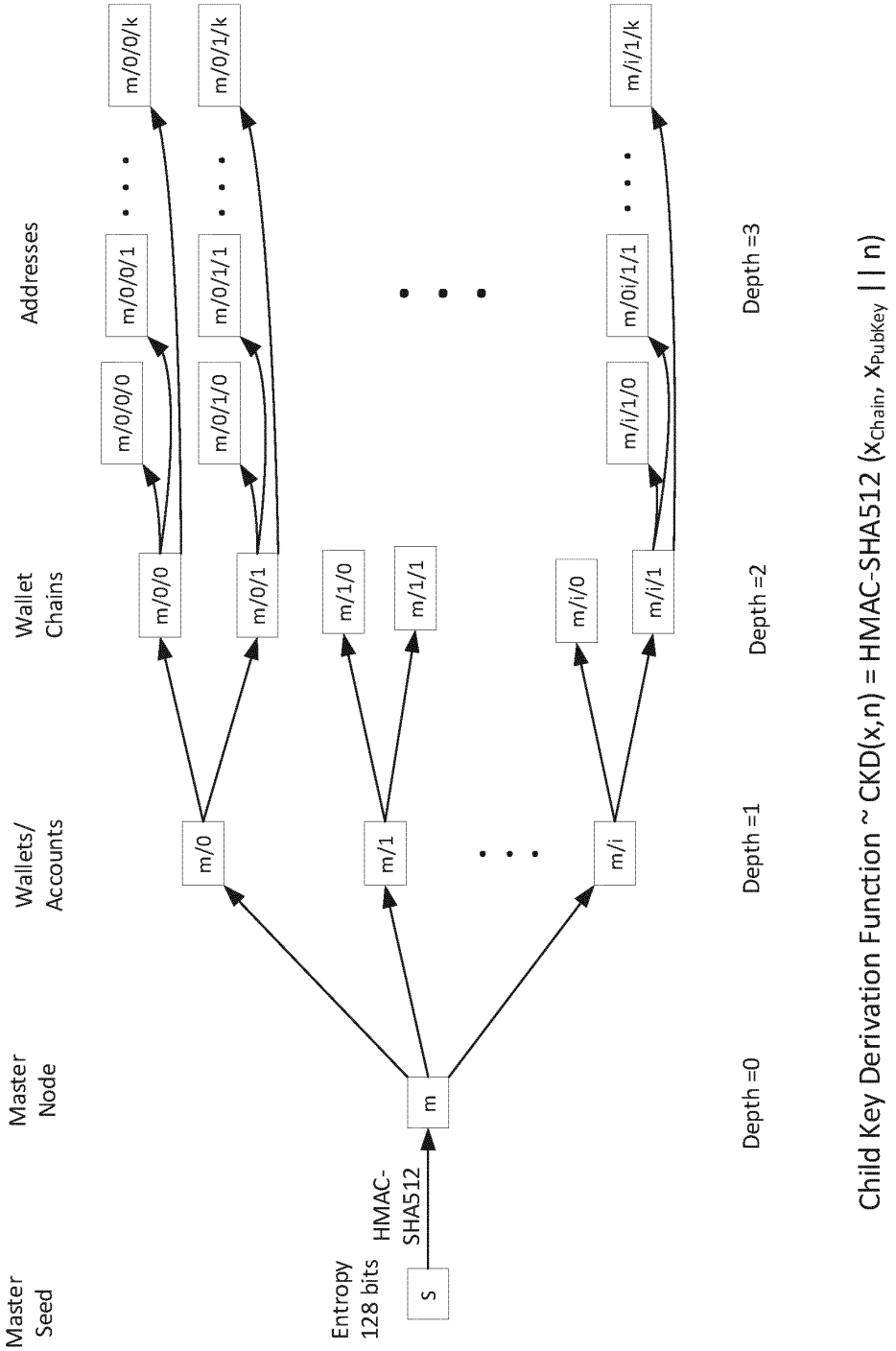

Master Seed
Entropy 128 bits
HMAC-SHA512
Master Node
Wallets/ Accounts
Wallet Chains
Addresses
Depth =0
Depth =1
Depth =2
Depth =3
s
m
m/0
m/1
m/i
m/0/0
m/0/1
m/1/0
m/1/1
m/i/0
m/i/1
m/0/0/0
m/0/0/1
m/0/1/0
m/0/1/1
m/i/1/0
m/0i/1/1
m/0/0/k
m/0/1/k
m/i/1/k
Child Key Derivation Function ~ CKD(x,n) = HMAC-SHA512 (xChain, xPubKey || n)

Figure 3

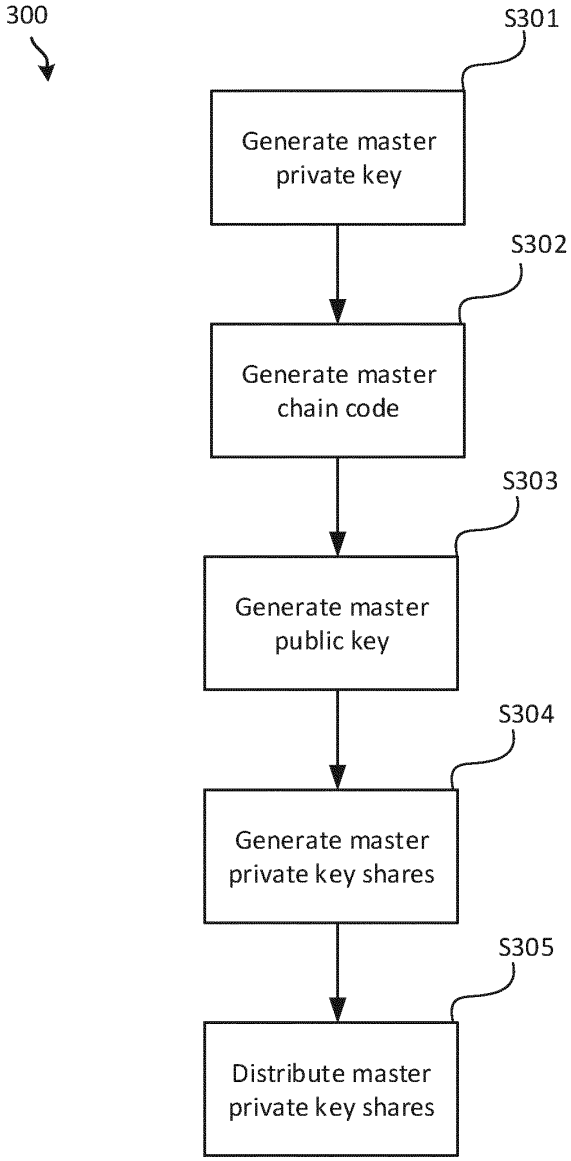

300
S301
Generate master private key
S302
Generate master chain code
S303
Generate master public key
S304
Generate master private key shares
S305
Distribute master private key shares

Figure 4

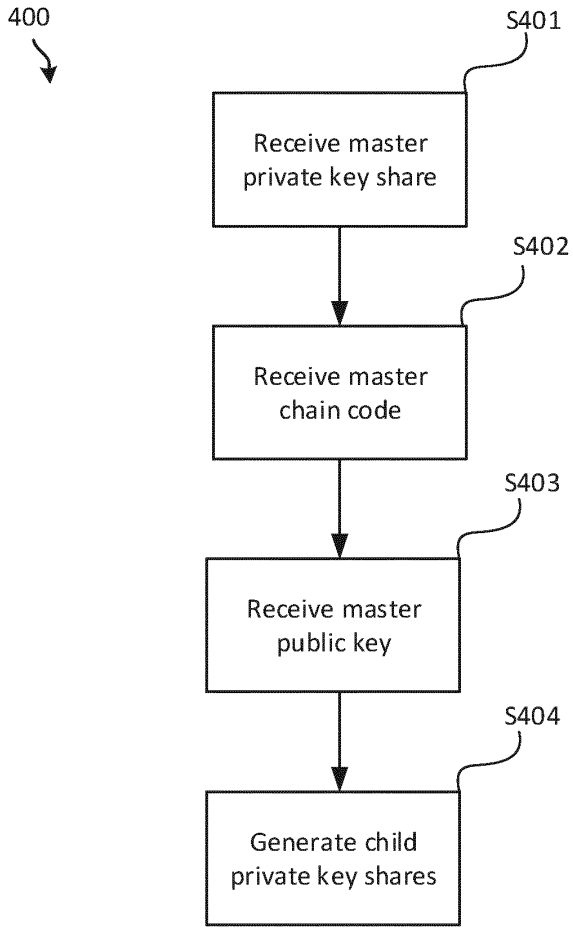
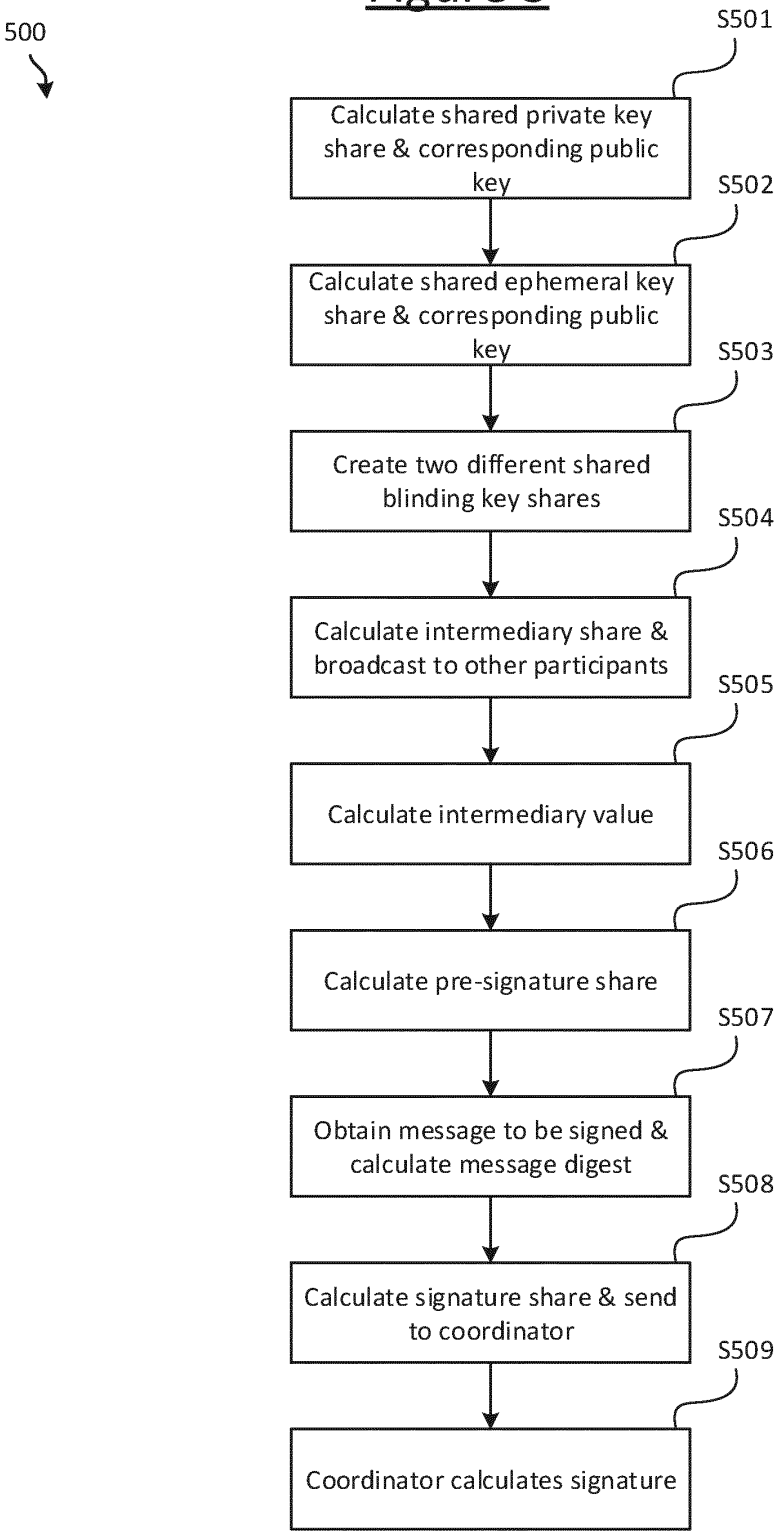

400
S401
Receive master private key share
S402
Receive master chain code
S403
Receive master public key
S404
Generate child private key shares

Figure 5


500
S501
Calculate shared private key share & corresponding public key
S502
Calculate shared ephemeral key share & corresponding public key
S503
Create two different shared blinding key shares
S504
Calculate intermediary share & broadcast to other participants
S505
Calculate intermediary value
S506
Calculate pre-signature share
S507
Obtain message to be signed & calculate message digest
S508
Calculate signature share & send to coordinator
S509
Coordinator calculates signature