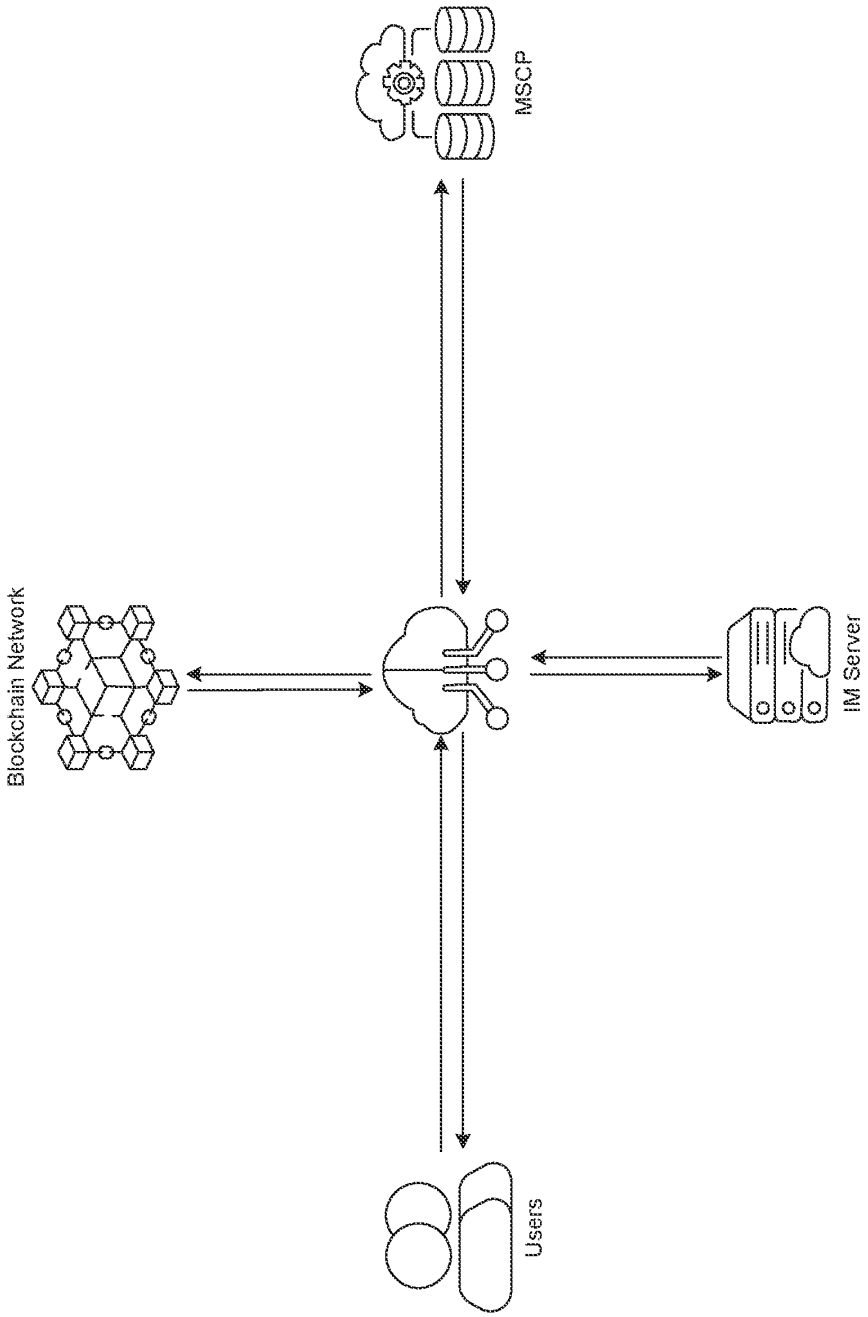

FIG. 1

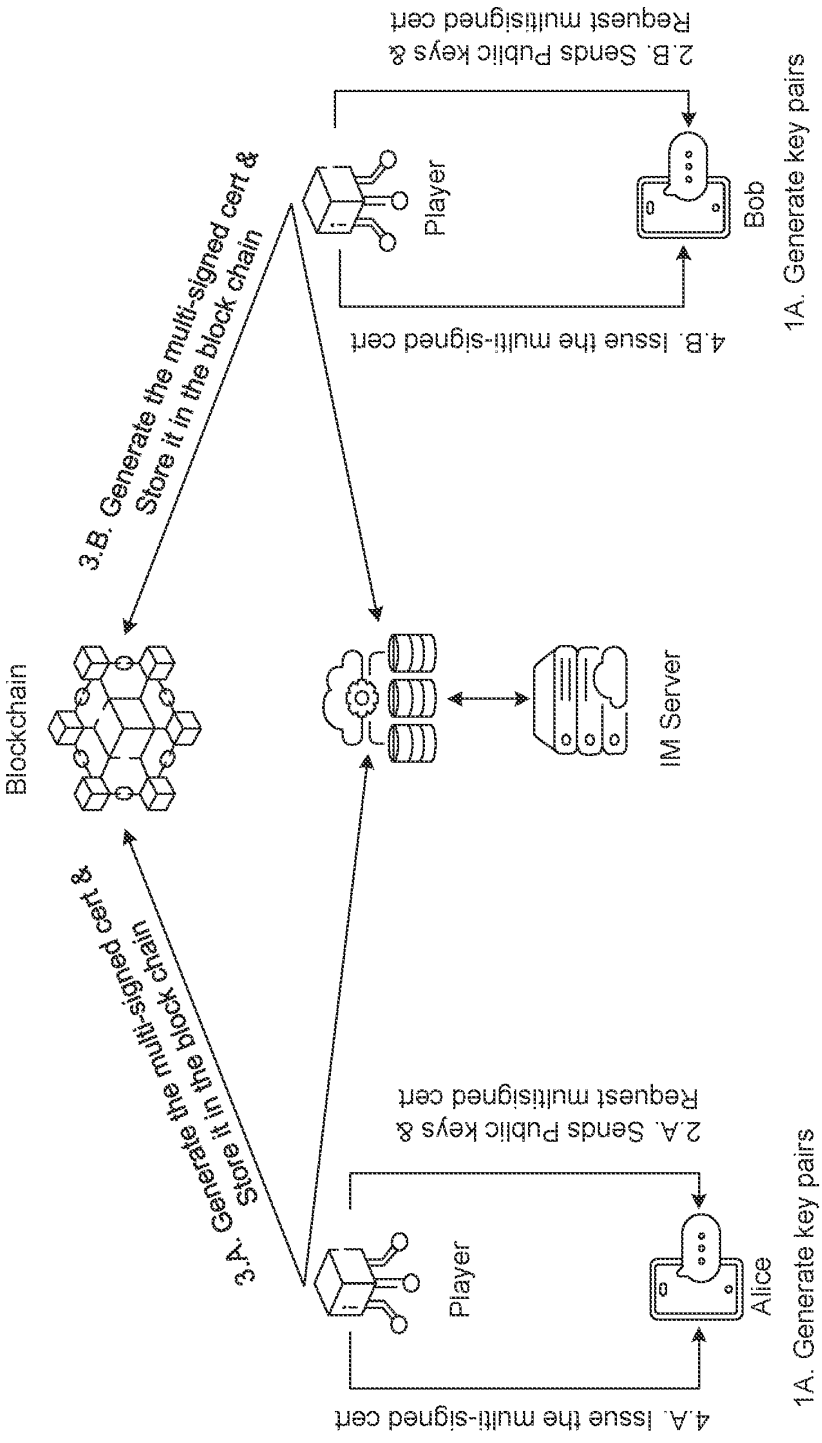
1A. Generate key pairs
Alice
Player
2.A. Sends Public keys & Request multisigned cert
4.A. Issue the multi-signed cert
1A. Generate key pairs
Bob
Player
2.B. Sends Public keys & Request multisigned cert
4.B. Issue the multi-signed cert
IM Server
Blockchain
3.A. Generate the multi-signed cert & Store it in the block chain
3.B. Generate the multi-signed cert & Store it in the block chain

FIG. 2

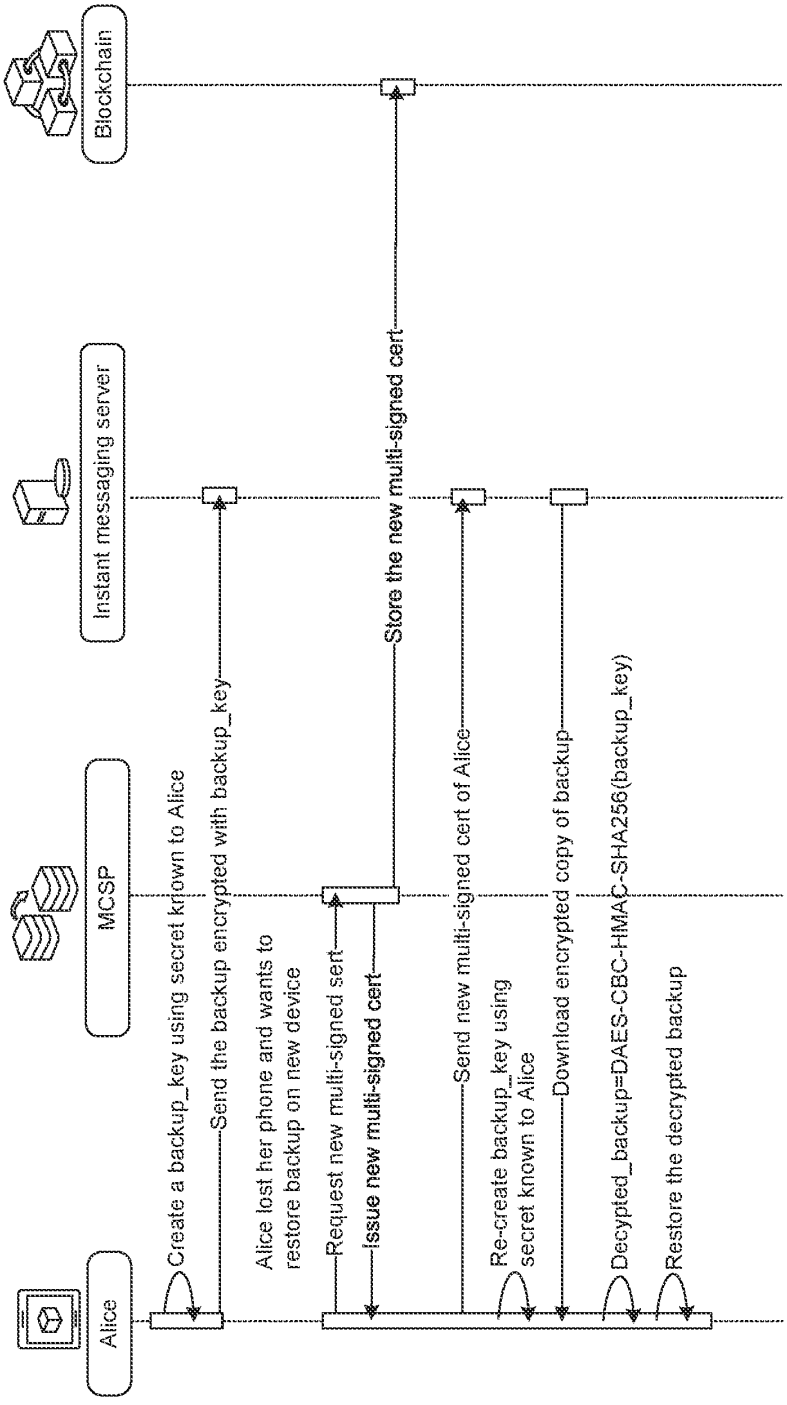
Alice
MCSP
Instant messaging server
Blockchain
Create a backup_key using secret known to Alice
Send the backup encrypted with backup_key
Alice lost her phone and wants to restore backup on new device
Request new multi-signed sert
Issue new multi-signed cert
Store the new multi-signed cert
Send new multi-signed cert of Alice
Re-create backup_key using secret known to Alice
Download encrypted copy of backup
Decypted_backup=DAES-CBC-HMAC-SHA256(backup_key)
Restore the decrypted backup

FIG. 3

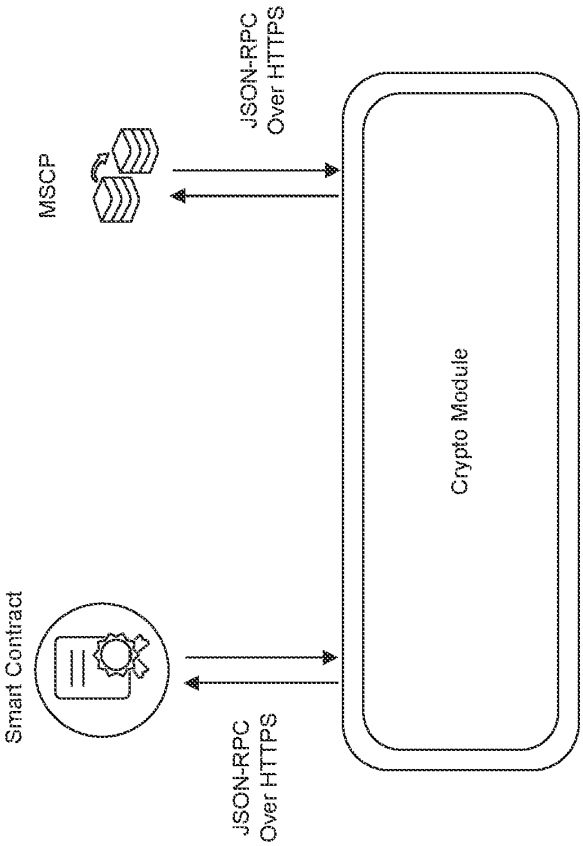
MSCP
JSON-RPC
Over HTTPS
Crypto Module
Smart Contract
JSON-RPC
Over HTTPS

FIG. 4

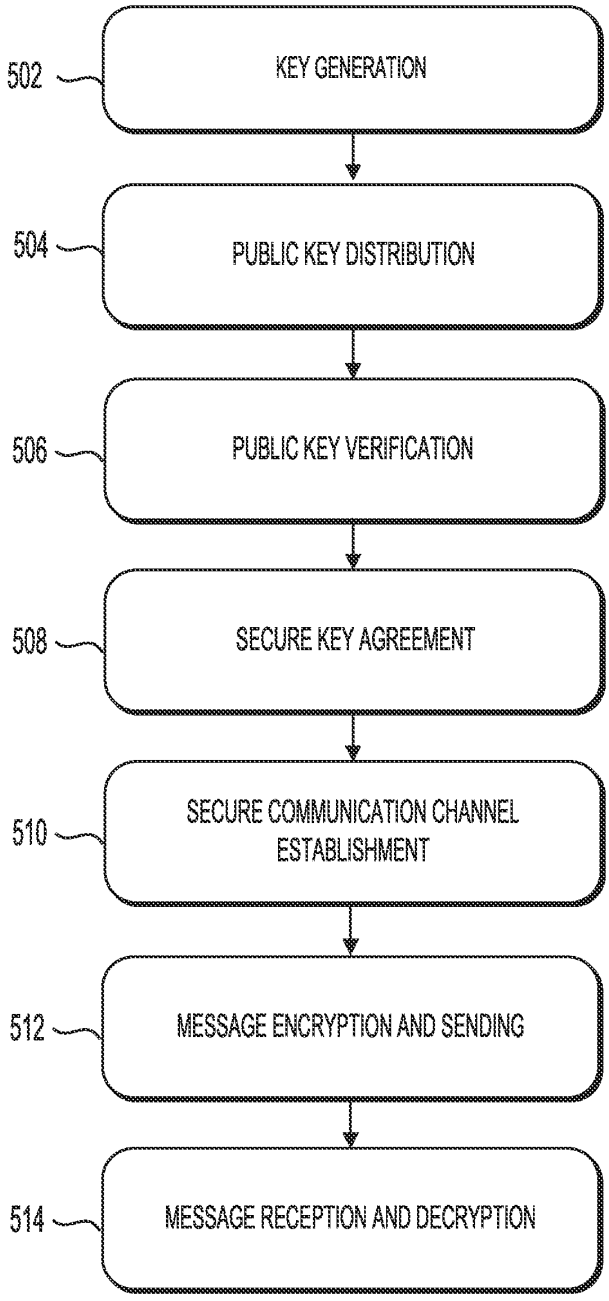
502
KEY GENERATION
504
PUBLIC KEY DISTRIBUTION
506
PUBLIC KEY VERIFICATION
508
SECURE KEY AGREEMENT
510
SECURE COMMUNICATION CHANNEL ESTABLISHMENT
512
MESSAGE ENCRYPTION AND SENDING
514
MESSAGE RECEPTION AND DECRYPTION

FIG. 5