IMPLEMENTATION

\_ **Authority**: The authority generates the public parameter *PK* and the master private key *MSK* of the system. The authority keeps the *MSK* secret and publishes *PK* available for the subscribers. The authority also generates a secret key generated based on the CP-ABE method and that key is issued to each financial institution (FI).

\_ **Clients** are the customers of financial institutes who join the blockchain-based KYC. Each customer has her own key pair used to encrypt and decrypt her credential data. To allow the credentials to be stored in any FI's database or in the cloud system, the FI must get the consent digitally signed by the client.

\_ **IPFS** is a cloud database that stores encrypted documents of KYC bound to each user account. It serves for user's credentials to generate transaction for cryptocurrency. It houses distributed hash table (DHT) keeping the address of the hash value of the clients' credential files which are encrypted in the IPFS storage.

\_ **Blockchain** is used to store the transactions of all KYCrelated activities. All sensitive transactions of the clients are encrypted. The data on the blockchain is tamperproof based on hash value and cryptography mechanism, which also prevents some illegal activities.

\_ **Smart contracts** are used to control and automate all KYC processes. In our system, there are three smart contracts including (1) Register contract is responsible for authenticating users, enrolling new users, and uploading the encrypted credentials to the IPFS, (2) Master contract is responsible for controlling client profiles, keeping hash value of the citizen ID of all clients for interacting with IPFS, and e-consent generation, and (3) Verify contract is responsible for KYC verification.