

## README

Different classes and activities are created for the different functionalities of the application

### ValidationActivity.java

- Has all the API implementation related to Validation screen activities like
- Validation of block-Checking whether the block received is valid(both normal block and the ZKP block)
- Checking whether a particular block is present in blockchain
- Sending the Validation block to the validator(both normal block and the ZKP block)
- On screen activities for the user like selecting attribute, generating QR code, generating alert messages etc.

Note:

ZKP block = Blocks that stores the proof from the authority in the transaction field of the full block.

normal block = Blocks that store hash of the actual value in transaction field of the full block.

### AuthenticationActivity.java

- Has the API implementations for the Authentication screen activities, such as reading the user data, generation of the QR code etc.

### Communication.java

This class though named Communication.java has implementations related not only to communication but also related to block creations, authentication etc. Due to the earlier trustchain design it was difficult to decouple other features with communication.

It has the following broad functionalities:

- Sending and Receiving a block
- Creating TrustChain FullBlock, HalfBlock, NewBlock
- Checking the authentication of the normal and ZKP blocks
- Utility communication API's to send and receive data between Peers.

### Server.java

This class is used to receive communications on the TCP socket.

### ClientTask.java

This class is used instead to send message to a TCP socket.

### MainActivity.java

- Has the implementation of the homescreen, which just consists of the launcher for different activities.

TrustChainDBHelper.java

- Implementation of the standard DB API's for storing and retrieving blocks and utility data.

ZKPHashChain.java

- Implementation of the Zero Knowledge Proof as described in this paper

- <https://www.cs.utexas.edu/~sebs/papers/vex-sigcomm13.pdf>

- Has the API's to authenticate, verify, generating verification proof

Message.proto:

Has the structure of the messages communicated between any two devices.