Abbiamo deciso di suddividere il sistema in 3 app che gestiscono il sito secondo quanto segue:

Abbiamo deciso di non utilizzare il modello di default fornito da Django ma crearne uno ereditato dalla classe base AbstractUser. Questo ci ha permesso di aggiungere campi personalizzati per il controllo del tipo di utente, caricamento dell’immagine del profilo e impostazione dell’indirizzo email invece del campo “username” come identificativo univoco per l’utente, che effettuerà il login tramite e-mail e password.

Per l’autenticazione abbiamo deciso di usare la tecnologia JWT (Javascript Web Token). Questo è un tipo di autenticazione token-based. A differenza del token di Django un token JWT non viene salvato sul server, ma solo lato client. Il token viene generato dal server al momento del login da parte dell’utente con l’indirizzo e-mail e password corretta. Le informazioni dell’utente vengono cifrate tramite una chiave univoca (contenuta nelle impostazioni del progetto, nel file settings.py) e spedite al client dentro il token. Il token è composto da tre parti:

* Header: contiene il metodo di cifratura e informazioni sul sottotipo di token
* Payload: contiene le informazioni dell’utente (nome, e-mail, ecc..) insieme alla data e orario di emissione e di scadenza del token. Questa parte del token è personalizzabile da parte dello sviluppatore
* Signature: firma di verifica del token (HMAC)