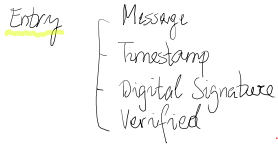
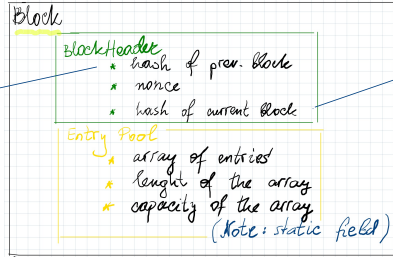
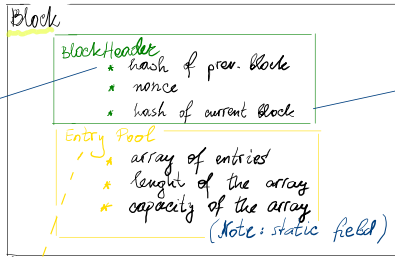


Blockchain Structure



Cryptography

Two operations:

- Sign(Entry)
- Verify(Entry)

Digital Signature

Basic Algorithm:

- ① From param set (p, q, g) generate a key pair
- ② Use modular exponentiation to calculate temp. values.
- ③ From temp. values generate a (r, s') pair which is the actual signature.

Hash Manager

We are currently using the Secure Hash Algorithm.