# Object Design Trade-offs

## Blockchain as a distribution system

There are several type of distribution systems which are mostly running in a centralised manner but in CrypDist we chose to move with Blockchain. Blockchain is mainly a database system which is used for secure money transactions throughout the years under the name of Bitcoin currency. It is a slow but free technique. Since it does not depend on any third party people during the transactions of data, it can be accepted as one of the most secure data transaction methods. Because of its direct structure it is not subject to any governmental control too. After the thorough consideration of above factors and thinking that our aim is to provide free data access, we decided to implement Blockchain even if it is comparably slower and more complex to implement than traditional centralised distribution systems.

## SHA256 Hashing Function

SHA256 hashing algorithm is from the SHA2 crypto algorithm family which is mainly designed by the National Security Agency (NSA). It is widely used in processes requiring high security standards because of its high collision resistant nature. But these advantages come with some computation related disadvantages. For example, SHA256 is a comparable slow algorithm than the algorithms in SHA1 family and there is lack of support for SHA-2 on systems running Windows XP SP2 or older.[[1]](#footnote-1) Additionally, when we compare the feasibility complexities of different algorithms including SHA256, we can conclude that it is relatively more complex than many other algorithms. But in any case, SHA256 is one of the most secure algorithms and the data that we give service of is very sensitive. Thus, when we consider that the security is one of the top priority in our application, SHA256 is the best fit.

1. <https://en.wikipedia.org/wiki/SHA-2> [↑](#footnote-ref-1)