Modern systems are required to be developed very rapidly and have full functionality within a year or less. One major objective of identity management systems (IMSs) is to establish trust among entities that initially start with distrust. The existing solutions have however been rather centralized whereas the identity provider ends up performing too many roles. On one hand, centrally storing sensitive information, authentication, and authorization increases the risk of becoming central data silos, which in turn reduces the user's control over their own personal information. On the other hand, an identity management cannot be weakly decentralized where the user does not have full control, privacy and legal compliance.

As identity management systems have evolved over the years, they come with certain flaws and security concerns. While IMSs have problems with legal compliance, security and anonymity, the blockchain technology comes with these points as its main strengths. Blockchain can help adhere to compliance (GDPR); organizations can use it in order to generate trust amongst entities more efficiently and securely, and banks can also use blockchain in order to cut costs in Know-Your-Customer (KYC) processes, which in turn helps combat money-laundering.

This thesis studies several existing solutions of blockchain-based identity management systems. More concretely, I will investigate how they hold up in order to become a fully functional solution that can be used by everyone and where users feels like they have control over their information. The thesis reviews the evolvement, authentication methods and limitations of conventional identity management systems, and looks into several schemes of the emerging blockchain-based identity management systems. Finally I propose some realworld use cases based on two selected schemes and discuss the advantage and potential of the solutions.