zk-SNARK is a cryptographic protocol, which enables transformation of an arbitrary computation into short effectively verifiable argument of correctness of this computation. Further more, it enables a prover to decide exactly, which inputs of the computation will be public and which inputs will stay private. The goal of this work is to present features, construction and applications of modern zk-SNARKs. In a construction part of this work we describe construction based on linear PCP and Paillier cryptosystem. In an application part we explain principles of anonymous cryptocurrency Zcash and we describe a completely new application of zk-SNARKs in networks of trust.