zk-SNARK je kryptografický protokol, který umožňuje libovolný výpočet přeměnit na krátký efektivně ověřitelný argument jeho správnosti. Navíc tento protokol umožnuje dokazovateli přesně rozhodnout, která část vstupů výpočtu bude veřejná a která zůstane skrytá. Cílem této práce je seznámit čtenáře s vlastnostmi, konstrukcí a aplikacemi zk-SNARKů. V konstrukční části popisujeme konstrukci založenou na lineárním PCP a Paillierově kryptosystému. V aplikační části vysvětlujeme princip anonymní kryptoměny Zcash a přicházíme s zcela novým uplatněním zk-SNARKs v reputačních systémech.