Summary of zero cash Alexander Wandrup

The acronym zk-SNARK stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge,”. It is a way to prove possession of something without revealing information about what you got. Im Bitcoin you can't do a transaction without revealing information like your public key etc. Zk-SNARK allows you to prove that without providing such information, and allows you to do a transaction with no interaction between the prover and the verifier. In order to do this some of the consensus rules need to be encoded. The first step is to break down the logical steps of transaction validation into a mathematical representation. This is done by making an arithmetic circuit. That is a circuit similar to a logical circuit just with the logical gates switched out with arithmetic operations. Then a system called 1 Constraint System, short for R1CS is used to check that values are traveling correctly through the circuit. In order to prevent provers from trying to attempt to predict what points the verifier will check, zk-Snark uses mathematical techniques like homomorphic encryption and pairings of elliptic curves to evaluate polynomials blindly without knowing what point is being evaluated. In order to maintain zero-knowledge random shifts of the polynomials are used.