Central bank digital currency (CBDC) is money that a country's central bank can issue. It is also referred to as e-cash. One of the major problems with e-cash is double-spending or double-use. As compared to users connected to an online trusted-third-party, offline users cannot verify if e-cash is already spent or not. More specifically, in a buyer-merchant setting, it is difficult to detect double-spending of a payment if a bank/broker service is not available.

[1] combats this using cooperative P2P Systems where merchant(s) can be a witness to verify a payment. It assumes the hardness of discrete-log problem and uses blind signatures to blind(hide) private information. Besides being insecure in a post-quantum setting, this design is susceptible to sybil attack **[2]** where an entity may create fake-multiple identities to act as witnesses.

A study by VISA **[3]** tackles double spending in offline transaction by leveraging digital signatures generated by TEE (Trusted Execution Environment). This component is present in most mobile devices in secure hardware, which are hard to replicate and compromise.

In my thesis, I will employ lattice-based blind signatures in the P2P cooperative system. This ensures security in the post-quantum setting. I will also investigate if TEE can be used to ensure authenticity of unique devices to protect the architecture from sybil attack.

[1] Combating Double-Spending Using Cooperative P2P Systems - https://people.cs.ksu.edu/~eyv/papers/ecash-icdcs07.pdf

[2] Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies - https://eprint.iacr.org/2015/464.pdf

[3] Towards a Two-Tier Hierarchical Infrastructure: An Online Payment System for Central Bank Digital Currencies - https://arxiv.org/pdf/2012.08003.pd