Pedersen Commitment

As the name implies, Pederson Commitments is a form of a commitment scheme. Pedersen commitment scheme's purpose is to allow a party to commit to a value without disclosing it, with the option to later expose and verify the committed value. Secure coin flipping, zero-knowledge proofs, and secure computation are just a few of the cryptographic protocols that use commitment schemes, but this article will only talk about Pedersen commitment and its application in zero-knowledge proof.

How Pedersen Commitment Works:

Pedersen commitment is an unconditionally concealing homomorphic commitment scheme based on the discrete logarithm issue. The scheme's framework is as follows:

1. Pick a group G that has a large prime order p. Let g, f ∈ G be generators of G
2. Committer picks a random valuer r ∈ Zp and computes C = g^m f^r mod p Send and C to the verifier
3. Committer sends (m, r) to the verifier. The verifier checks whether C equals g^m f^r mod p and accepts if it holds.

g^m f^r mod p is known as Pedersen commitment to M. Represented as C(m,r).

Homomorphism is mandatory for Pederson commitment to work. By using homomorphism, Pedersen guarantees to maintain the structure between two random structures. e.g:

f (a+b) = f(a) + f(b)

To understand the application of Pedersen commitment, let's have a quick explanation of Zero-Knowledge proof.

Zero Knowledge Proof:

Is it possible to demonstrate that something is true without providing the evidence? This is what 'Zero-Knowledge Proof' technology proposes, a strategy that uses cryptographic algorithms to allow several parties to verify the authenticity of a piece of information without having to share the material that makes it up.

For the simplest example, let's suppose your friend is color blind and you have two pens, one is red and the other is blue. You have to prove to your color blind friend that both pens have different colors but you are not going to tell him which pen is red and which pen is blue. You ask your color blind friend to swap both pens behind his back and you will tell him whether he have swapped the pens or not. So, every time when he swaps the pen or not, you will tell him the correct answer because you can see two different colors. When you will provide the correct answer every time, your friend must have to believe that the pens are different in color because otherwise, you could not be able to answer correctly. This is how zero-knowledge proof works; you are proving that both pens have different colors but you are not revealing which pen has which color.

The employment of Pedersen commitment to zero-knowledge proofs is one particularly inspiring example. Commitments are employed in zero-knowledge proofs (ZKP) for two major reasons: first, they allow the prover to engage in "cut and pick" proofs, in which the verifier selects what to learn, and the prover only reveals what matches the verifier's selection. Commitment schemes allow the prover to specify all the information ahead of time and only divulge what is necessary later in the proof. Second, the verifier will typically express their choices ahead of time in a commitment, which is employed in zero-knowledge proofs. This allows the prover to create zero-knowledge proofs in parallel without revealing any new information.

Applications of Pedersen commitment in ZKP:

1. **Anonymous Voting**

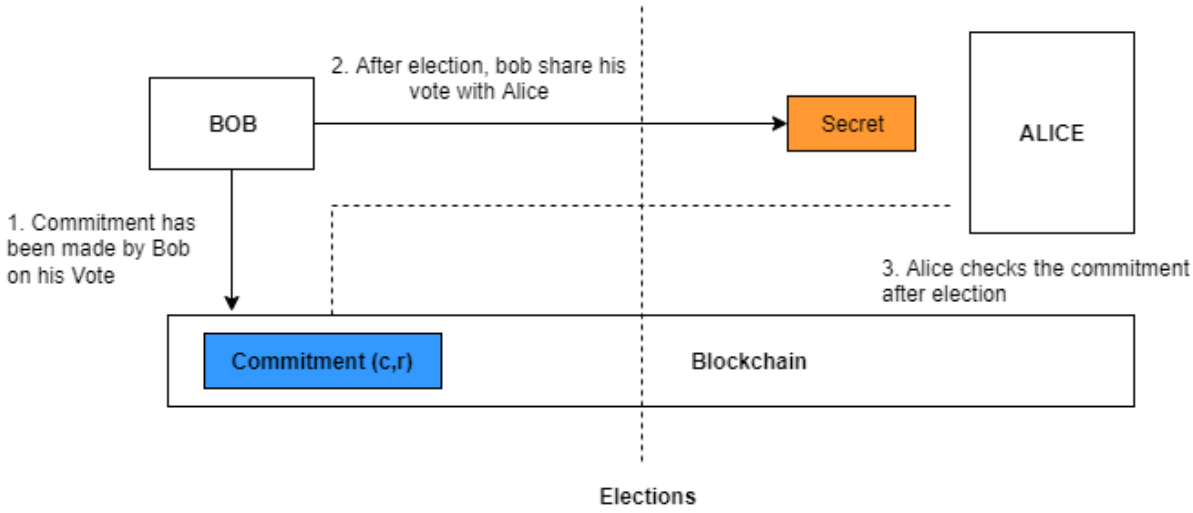

Figure 1: Pedersen commitment in Voting

Commitment schemes and ZKP together are being used to handle anonymous and verified voting. There is no longer a requirement for a trusted third party to validate the outcomes because they are recorded on a public blockchain. Furthermore, any chance of censorship is eliminated. In the figure 1 above, Bob will make a commitment and place it on blockchain. Bob also shares the secret with Alice after the election. Alice will verify the secret by checking the commitment after the election.

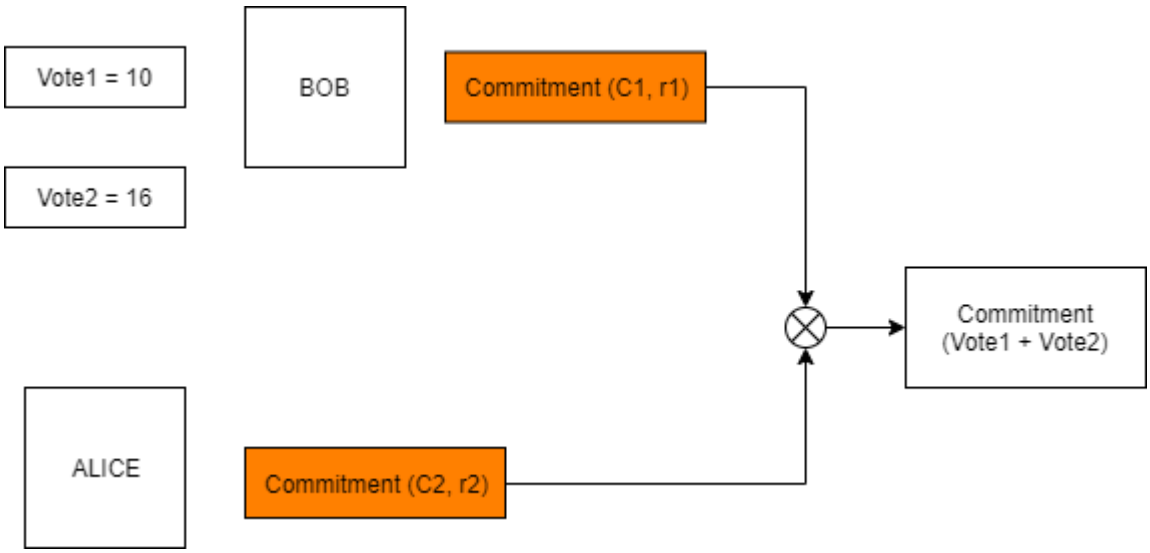

Figure 2: Counting Votes using Pedersen Commitment

Using Pedersen commitment, we can take multiple commitments and multiply them together as values which will be equivalent to adding two votes together. As shown in figure 2, we can add all the votes together and all the commitments together and the final result must be equal in order to correctly count and verify the voting.

Eligible voters can use ZKPs to establish their eligibility to vote without revealing their identity, effectively making the voting system anonymous. ZKP also give voters the option of requesting verifiable proof that their vote was counted in the final tally by the institution reporting the results.
Even if the votes themselves are not available on a public blockchain, the electoral authority can audit the vote outcomes.

2. Exchanges and Digital Assets

It's critical to include a privacy layer to ensure that the amount being transacted and the participants in each transaction stay private. This problem is solved by commitment schemes and ZKP. Problems like order front-running are readily avoided when all relevant transaction information is hidden. Monero cryptocurrency is the best example of this application. Furthermore, if auditing of specific orders is ever required, this functionality can be implemented as well.
In the case of asset settlement, for example, the best execution of an order can be certified without revealing the entire order book. As the verification process is automated, this provides for a more efficient audit method. This will also reduce the likelihood of disagreements between counterparties. It also permits the exchange operator to keep sensitive data private if necessary.

Pedersen commitment is a reliable cryptographic commitment scheme that preserves privacy and confidentiality in various modern technological applications i.e., cryptocurrency, voting, blockchain, etc. with its simple property and implementation, Pedersen commitment is becoming popular among the cryptographic researchers for protecting the privacy of applications.