SRF Name: **Pavan R Kashyap**
Application no: **ENGS6382**
Guide name**: Dr. N Raghu Kishore**
Institution: **Mahindra Ecole Centrale**

PROJECT TITLE: Devising quantum-resistant protocols for a Blockchain network

Quantum Computers are computers that use the concepts of quantum mechanics to substantially increase the computational power of conventional computers. As of today, we do not have full fledged quantum computers deployed for use, but they will become a commonplace in the near future. Whilst quantum computers can make our computation exceptionally fast, they pose potential threats to the field of security.

Majority of today's systems/devices use public key cryptography algorithms like RSA and ECDSA to ensure that the confidentiality of the messages is kept intact. Public key cryptography, the bracket that encompasses these algorithms, involves the usage of two keys, the public key and the private key. The public key is the key that is globally visible to everyone. The private key is the key that is known only to the owner of the key. These keys originate in pairs and they are passed along with the plain text/cipher text into encryption/decryption algorithms.
Traditional cryptography such as this, relies on current computational difficulties to prevent the private key from being disclosed by the public key.

The day quantum Computers become a reality, traditional cryptographic algorithms (like RSA and ECDSA) will get easily broken (NP hard problems). So, how do we protect ourselves from potential threats the day quantum computers take over? Whilst a quantum computer is able to solve the discreet logarithm problem (ECDSA) and the factorization problem (RSA), it is observed that there are certain algorithms that cannot be broken even by a quantum computer. Such algorithms classify as Post Quantum Cryptographic algorithms i.e cryptographic algorithms of the future that will resist attacks by a powerful quantum computer.

Lattice cryptography is one such post quantum cryptographic technique that has the most potential so far. It involves generating an N-dimensional lattice, all points being integers (and generating basis vectors that allow us to express every point in the lattice as a linear combination of those basis vectors). Two problems in lattice cryptography that hold great promise are the Shortest Vector Problem (SVP) and the Learning with Errors (LWE) problem.

The SVP problem aims at the finding the shortest vector (to a fixed or relative origin) by finding a certain linear combination of the basis vectors. Ideally, if these basis vectors are orthogonal, the shortest vector is the smallest integer in every basis dimension. However, when the basis vectors are not orthogonal, several possible linear combinations are possible. The computer must not only now compute the shortest solution, but it must also iterate through all the solutions generated to verify if that is indeed the shortest solution. Unlike the previous algorithms where there was a definite solution to the problem, here we have to first find a solution and then verify if that is the optimal solution. So, this increases the time complexity of solving the problem.

Similarly, LWE is another problem that aims to make it harder for an attacker to guess the secret key stored. It involves generating linear equations of N-dimensions. Conventionally, it is easy to solve an N dimensional linear equation if we are given with N equations i.e. that we can obtain a unique solution from those equations. If we were to use these N-dimensional equations as is, a classical computer can also very easily obtain the private key (the solution) in no time. To combat this, we decide to introduce a large number of equations (all N-dimensional and linear but their count > N). To make it even difficult for the attacker, we introduce an arbitrary noise/error into the RHS side of every equation. This noise/error is known only to the initiator of the equations, not to anyone else. The introduction of the errors and the increased equation count now makes it harder for an attacker to actually a) decipher the private key and b) identify all the errors in each equation and c) verify if the private key (solution) actually satisfies all the equations after stripping them off the noise/error. Again, these changes increase the complexity of this algorithm.

The aim of this internship was to identify if we could generate/introduce protocols that use quantum-resistant algorithms in Blockchain so that we can protect the decentralised network from quantum attacks.

The internship started by exploring the traditional layout of a Blockchain environment. This involved understanding the traditional algorithms and techniques in place. This was done to identify the protocol and architecture and identify potential sites for use of Quantum resistant algorithms.

The potential sites where quantum computers can affect the blockchain system are

1. ECDSA digital signature scheme
2. The encryption mechanism in place
3. The SHA-256 algorithm used and the Merkel tree generated
4. The Proof-of-Work solving

Over the course of this internship, I will be working on devising two protocols.

The first protocol uses the Learning with Errors problem (LWE) to replace the traditional ECDSA scheme. LWE is strictly used for encryption as of now. The underlying concept of LWE has been used to design this protocol. The protocol aims at generating a new Digital Signature scheme that is analogous to traditional schemes, but is quantum-resistant. A detailed elaboration of the same will be provided in the final report.

The second protocol uses the Shortest Vector Problem (SVP) to replace the traditional Proof-of-Work and Merkel tree construction schemes. It introduces a new approach of N-dimensionalizing a Merkel tree i.e mapping the transactions onto an N-dimensional q-ary lattice, and using the SVP to generate the tree. It introduces novel reward schemes aimed at levelling the disparity currently prevalent in the Blockchain network. It also aims at introducing a new concept – computation power as an investment. More on this protocol's working will be shared in the final report.

Whilst it is true that these protocols may not directly affect us today, innovation for the future must always start early. We must not get into a huddle the day Quantum computers become a reality; we must be prepared to tackle the threats posed by it early on.