B.E. PROJECT Report on

Juxtaposition of Blockchain Technology with emerging Quantum Computing
A case study on E-Voting & Referendum

Submitted in partial fulfillment of the requirements
of the degree of

BACHELOR OF ENGINEERING

in

INFORMATION TECHNOLOGY

by

Group No: 13

Roll No.	Name
105	Vinayak Mhatre
106	Sarvesh Pande
107	Jay Shah

Supervisor:

Dr. G. T. Thampi
(Professor, Department of Information Technology, TSEC)

Information Technology Department
Thadomal Shahani Engineering College
University of Mumbai

2020-2021

CERTIFICATE

This is to certify that the B.E. PROJECT entitled **"Juxtaposition of Blockchain Technology with emerging Quantum Computing, A case study on E-Voting &Referendum"** is a bonafide work
Of

Roll No.	Name
105	Vinayak Mhatre
106	Sarvesh Pande
107	Jay Shah

Submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the degree of **"BACHELOR of ENGINEERING"** in **"INFORMATION TECHNOLOGY"**.

Dr. G. T. Thampi
Project Guide

Dr. Madhuri Rao
Head of Department

Dr. G. T. Thampi
Principal

B.E. Project Report Approval for B.E sem VI

B.E. Project report entitled **Juxtaposition of Blockchain Technology with emerging Quantum Computing, A case study on E-Voting & Referendum**
by

Roll No.	Name
105	Vinayak Mhatre
106	Sarvesh Pande
107	Jay Shah

is approved for the degree of ***"BACHELOR of ENGINEERING" in "INFORMATION TECHNOLOGY"***.

Examiners

1.....

2.....

Date:

Place:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have notmisrepresented or fabricated or falsified any idea/data/fact/source in mysubmission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has notbeen taken when needed.

1) _____
Vinayak Mhatre (105)

2) _____
Sarvesh Pande (106)

3) _____
Jay Shah (107)

Date:

Acknowledgement

It is our pleasure to present this project on **Juxtaposition of Blockchain Technology with emerging Quantum Computing, A case study on E-Voting & Referendum**

.

First of all, let us thank Prof. Dr. G. T. Thampi, the principal of Thadonal Shahani Engineering College, Bandra. We express deep gratitude and sincere thanks to Head of the Department and our project guide, Dr. G. T. Thampi for their encouragement and support throughout the project, also the honest feedback and constructive criticism provided helped a lot to improve and eliminate flaws.

We would like to give out sincere thanks to information technology department staff, who leads to excellently and timely complete the project with great technical support and lab support.

We hope our work would be taken as a step towards improving the current stock prediction systems.

Thank You.

Vinayak Mhatre (105)

Sarvesh Pande (106)

Jay Shah (107)

Table of Content

Chapter 1

Introduction

1.1 Blockchain Technology

A blockchain, originally block chain, is a growing list of records, called blocks that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed, and oftentimes public, digital ledger consisting of records called blocks that is used to record transactions across many computers so that any involved block cannot be altered retroactively, without the alteration of all subsequent blocks. This allows the participants to verify and audit transactions independently and relatively inexpensively. A blockchain database is managed autonomously using a peer-to-peer network and a distributed timestamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a value-exchange protocol.

1.2 Quantum Computing

Quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. Computers that perform quantum computations are known as quantum computers. All computing systems rely on a fundamental ability to store and manipulate information. Current computers manipulate individual bits, which store information as binary 0 and 1 states. A classical computer gives 2 bits of information as: 00,01,10,11. But quantum computer allows these 2 bit of information to be in a superposition. They can be #00, #01, #10, #11. (Where # represents any co-efficient)

Quantum computers leverage quantum mechanical phenomena to manipulate information. To do this, they rely on quantum bits, or qubits. One of the most promising applications of quantum computers is for simulating the behavior of matter down to the molecular level. The machines are also great for optimization problems because they can crunch through vast numbers of potential solutions extremely fast.

1.3 E-Voting

Electronic voting (also known as e-voting) is voting that uses electronic means to either aid or take care of casting and counting votes.

Depending on the particular implementation, e-voting may use standalone electronic voting machines (also called EVM) or computers connected to the Internet. It may encompass a range of Internet services, from basic transmission of tabulated results to full-function online voting through common connectable household devices. The degree of automation may be limited to marking a paper ballot, or may be a comprehensive system of vote input, vote recording, data encryption and transmission to servers, and consolidation and tabulation of election results.

Electronic voting technology can include punched cards, optical scan voting systems and specialized voting kiosks (including self-contained direct-recording electronic voting systems, or DRE). It can also involve transmission of ballots and votes via telephones, private computer networks, or the Internet.

In general, two main types of e-voting can be identified:

- E-voting which is physically supervised by representatives of governmental or independent electoral authorities (e.g. electronic voting machines located at polling stations);
- Remote e-voting via the Internet (also called i-voting) where the voter submits their votes electronically to the election authorities, from any location.

1.4 Referendum

A referendum is a direct and universal vote in which an entire electorate is invited to vote on a particular proposal and can have nationwide or local forms. This may result in the adoption of a new policy or specific law. In some countries, it is synonymous with a plebiscite or a vote on a ballot question.

The REFERENDUM allows citizens, through the petition process, to refer acts of the Legislature to the ballot before they become law. The referendum also permits the Legislature itself to refer proposed legislation to the electorate for approval or rejection.

There are two types of referenda: the referendum bill and the referendum measure. The primary purpose of both is to give voters an opportunity to approve or reject laws either proposed or enacted by the Legislature. The two types of referenda are as follows:

- Referendum Measures are laws recently passed by the Legislature that are placed on the ballot because of petitions signed by voters.
- Referendum Bills are proposed laws referred to the electorate by the Legislature.

1.5 Juxtaposition of Blockchain and Quantum Computing

The following paper proposes how the two emerging technologies; Blockchain and Quantum Computing can co-exist and enhance the performance and security of current applications particularly in the case of E-voting and Referendum. In order to achieve it, we first understand the algorithms and the fundamentals on which these technologies work. On the basis of that, we discuss here the 2 approaches to achieve juxtaposition between them as follows:

1. Achieving post quantum or quantum resistant blockchain
2. Implementing blockchain in quantum computing

1.6. Aim & Objective

Above, we have mentioned the technicalities of each technology and the detailed explanation of the project title. Now, the reason for the selection of this topic was merely the vision of understanding these technologies and harvesting the most out of these so that in future, our research would give a blueprint of how they can co-exist together that was seeded into our minds by our project guide, Dr. G. T. Thampi. These are the technologies that comprise of the present and future. And even though, these technologies are still being implemented, their impact on us is exponential. Quantum Mechanics was merely a thought, an idea in 1925 and even if Quantum Mechanics' idea was first discovered and the first ever quantum computer consisting of 2 qubits was created in 1998. However, the execution of blockchain has come to fruition in 2008 where this technology was executed successfully. For all these years, no technology or algorithm posed a threat to Blockchain since it makes use of asymmetric-key cryptography and hash functions. But in 2016, IBM announced their first ever quantum processor of 53 qubits which was soon followed by Google's quantum computer, claiming that it could perform the calculations in 3 minutes that they reckoned, the most powerful classical supercomputers on the planet would take 10,000 years. Thus, the leverage that blockchain has, gets tossed up and basically, 2 of the most trending technologies that will be used in possibly all sectors like we have mentioned further here, perhaps, cannot co-exist since Quantum Computing poses as a threat to the functioning of Blockchain. This proved to be the driving force behind our research. We now highlight how these technologies have made their roots so strong in our lives and how will they facilitate these departments practically to give you a summary of the positive effect they are having on us and why was it all the more necessary for us to undertake this research paper.

Blockchain:

1. **Smart Contracts**

A smart contract is a digital form of contract which has programmable architecture. So, the details of the contracts are stored in the Blockchain block. As the technology matures, more organizations are expected to take advantage of it to reduce costs and enable fast and secure transactions. Smart contracts market is expected to reach 300 USD Million by 2023 with 32% CAGR since it is

2. **Banking**

According to one source, moving securities on a blockchain could save from $17 to $24 million each year in global trade processing costs.

3. Cryptocurrency

Uses in Bitcoin and other cryptocurrencies is a well-known application of Blockchain. The cryptocurrency market cap has been projected to reach as high as $1-2 trillion in 2018. The technology underlying cryptocurrencies has been said to have powerful applications in various sectors ranging from healthcare to media.

4. Healthcare

Blockchain technology can play an important role, such as improved clinical trial data management by reducing delays in regulatory approvals, and streamline the communication between diverse stakeholders of the supply chain, etc. Moreover, the spread of misinformation has intensely increased during the outbreak, and existing platforms lack the ability to validate the authenticity of data, leading to public panic and irrational behavior. Healthcare professionals can use Blockchain to store patient's records safely. It will enhance the safety of the information.

5. Voting

Using Blockchain in Voting will indulge in the safety of counting and misinterpretation. Voting is one of the most important ways of ensuring that fair and diplomatic decisions are being made. Without voting, people would not be able to have a say on certain decisions and proposed changes. However, there are certain flaws with the current voting system that blockchain can solve.

- **Transparency:** The first benefit that blockchain can bring about is transparency. By using blockchain, votes can be tallied and stored on an immutable public ledger.

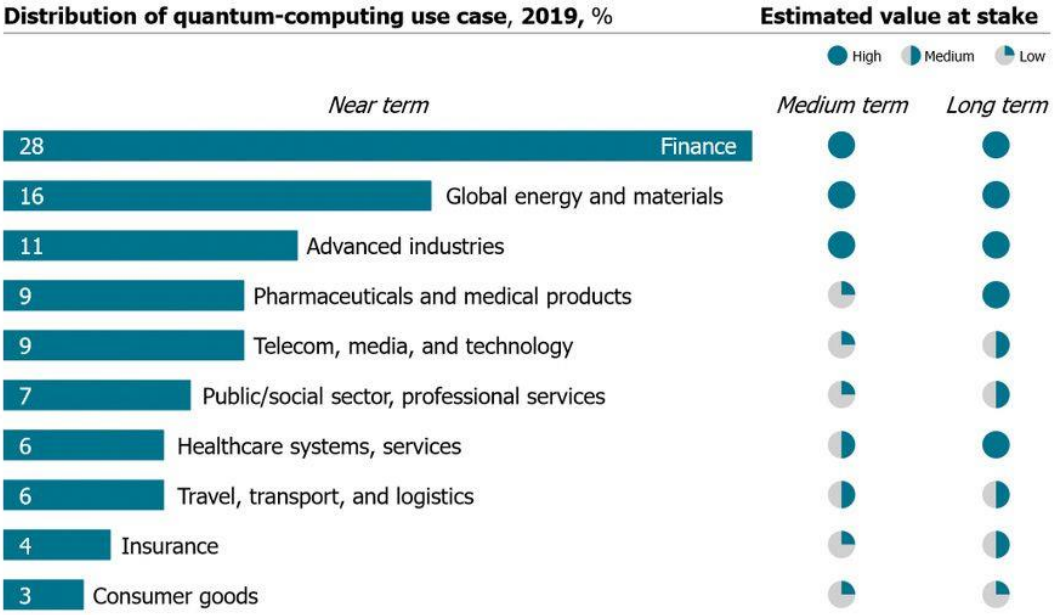
- **Security:** All votes could be verified as soon as voting is finished to ensure they are all counted correctly. Without blockchain, this would have to be done by a central body overseeing the process. This causes many questions to arise about the trust of these central bodies. But with blockchain and its decentralised ledger system, there is no need for a potentially fallible or corruptible central body.

- **Anonymity:** Blockchain allows for anonymity when voting. As with transactions on the blockchain, voters can use their private keys to keep themselves anonymous.

- **Processing Time:** Instead of having to wait for a large number of people to communicate manually, all organisers will be able to see the outcome instantly on the blockchain. Results can be gathered and processed quickly and straight after the voting has finished.

Quantum Computing:

According to a new report from McKinsey & Partners, in partnership with the Viva Technology show, the technology will have a global market value of $1 trillion by 2035. Illustrating the possibly transformative nature of the advance, one of the report's co-authors pointed to the current coronavirus pandemic.



After the primary briefing given to us by our principal, we did our basic research on the stance that these 2 technologies have in the current times. These technologies being implemented relatively in the recent times, keeps the researchers around the globe on the edge of their seats because of the advancement and new iterative features that have been brought into consideration and since both of these giants are quite recent in the world of science and technology, the topic of juxtaposition has not been taken up by many people. But the importance of the same remains at utmost priority due the impact it has had and will continue to have on our lives. Common example could be the huge investment being made across the globe in cryptocurrency.

It has become imperative for the world to find solutions and creating an environment where instead of posing as threats to each other, there is way where not just juxtaposition of these 2 emerging technologies take place but also, both, Blockchain & Quantum Computing can facilitate each other in to better operability & functioning.

Chapter 2

Review of Literature

2.1 Domain explanation:

"Juxtaposition of blockchain with emerging quantum computing, a case study [E-Voting and referendum]". The topic can be well understood when broken down into parts. The highlights of the topic are as follows:

- **Blockchain:**

1) The blockchain consists of a sequence of blocks that are stored on and copied between publicly accessible servers.
2) Each block consists of four fundamental elements:

a) The hash of the preceding block;

b) The data content of the block (i.e. the ledger entries);

c) The nonce that is used to give a particular form to the hash;

d) The hash of the block.

To summarize the concept of blockchain, we shall take a look at the three pillars that support blockchain; **Decentralization**, **Transparency** & **Immutability**.

- **Proof-of-Work** (POW) can be simply understood as a proof that you have done a certain amount of work. In a blockchain system, any node that wants to generate a new block and write it to the blockchain must resolve the POW puzzle in the blockchain network. POW puzzle is an NP-hard problem.
- **Smart contracts** are trackable and irreversible applications that execute in a decentralized environment (e.g., blockchain). Once the smart contract has been deployed nobody can edit the code or change its execution behaviour. Smart contract execution guarantees to bind parties together to an agreement as written.

2.2 Existing Solutions:

- **Blockchain-based Electronic Voting:** In every democracy, the security of an election is a matter of national security. Electronic voting machines have been viewed as flawed, by the security community, primarily based on physical security concerns. Anyone with physical access to such machine can sabotage the machine, thereby affecting all votes cast on the aforementioned machine.

  A blockchain is a distributed, immutable, incontrovertible, public ledger. This new technology works through four main features:

i. The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.

ii. There is distributed control over who can append new transactions to the ledger.

iii. Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

iv. A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

Chapter 3

Current Scenario

Threat to blockchain: In the context of quantum computing, we are confronted with two aspects of invalidating the promises of blockchain. First, the inversion of hashes is assumed to be computationally difficult. If this can be dramatically simplified by a quantum computer, the authenticity of the upstream blockchain can no longer be guaranteed and the authenticity of entries in the blockchain is compromised.

Quantum Computing poses a threat to Blockchain using the following algorithms:
The principal threat is **Grover's algorithm**, which can dramatically speed up function inversion. This allows the generation of a modified pre-image from a given hash (a hash collision) allowing a signed data block to be modified. This voids guarantees of authenticity of the ledger entries undermining the entire blockchain. The speed-up due to Grover's algorithm is a factor of the square root of the number of possible hashes, meaning that a hash subjected to quantum attack would only be as secure as one with half as many bits subjected to classical attack.

1) **Grover's algorithm** is specifically a solution to the problem of finding a pre-image of a value of a function that is difficult to invert. If we are given a signature that is the hash value of some data $s = H(d)$, and the function $H(d)$ can be implemented on a quantum computer, then Grover's algorithm allows us to find d for a given s in time of order $O(\sqrt{n})$where n is the size of the space of valid hashes. In other words, it allows us to generate hash collisions more efficiently than brute force search, which would be (n).

   For a hash of length k bits this means that we have a significant speedup by a factor of 2 $k/2$. This can be very large even for small values of k.

2) **Shor's Algorithm:** Shor's Algorithm provides a dramatic improvement in the efficiency of factoring large numbers. Thus, Shor's algorithm can be used to attack RSA encryptionand related problems. In practical terms, this makes RSA keys of 4096 bits in practice unbreakable with classical computation, but breakable with quantum computation. The consequence is that any aspect of a blockchain implementation that relies on RSA or similar algorithms would be vulnerable to quantum computational attack. This allows solution of problems such as the discrete logarithm problem, which in turn makes such cryptographic algorithms as ElGamal encryption, Diffie-Helman key exchange, the Digital Signature Algorithm, and elliptic curve cryptography insecure.

Thus we aim at:

- The arrival of powerful quantum computers will shatter currently deployed public key cryptography and weaken symmetric-key cryptography, thereby undermining the cybersecurity that protects our systems and infrastructure. The digital signature scheme used in blockchain technology to authenticate transactions is completely vulnerable.
- The problem of quantum-proofing the blockchain can be divided into two scenarios. The first scenario refers to quantum-proofing new blockchains, that is, designing quantum-resistant blockchains from scratch, whereas the second refers to quantum-proofing existing blockchains (such as the Bitcoin network).
- Perhaps the cost-effective way of making the blockchain resistant against quantum attacks is to replace the currently deployed digital signature schemes (based on RSA or EC-DSA) with post-quantum ones, which derive their security from the difficulty of certain mathematical problems; hence, they offer what is often called computational security.
- Post-quantum digital signature schemes offer security against a quantum adversary, at the expense of much larger public/ private key sizes or signature sizes, which may pose serious scalability challenges. Reducing both the signature sizes and the public/private key sizes is paramount to designing a robust and efficient quantum-resistant blockchain.

Chapter 4

Methodology

4.1 Ideal Characteristics of Blockchain Post-Quantum Schemes

In order to be efficient, a post-quantum cryptosystem would need to provide blockchains with the following main features:

- **Small key sizes:** The devices that interact with a blockchain need to ideally make use of small public and private keys in order to reduce the required storage space. In addition, small keys involve less complex computational operations when managing them. This is especially important for blockchains that require the interaction of Internet of Things (IoT) end-devices, which are usually constrained in terms of storage and computational power. It is worth indicating that IoT, like other emerging technologies (e.g., deep learning), has experienced a significant growth in the last years but IoT devices still face some important challenges, mainly regarding security which are limiting to some extent its jointly use with blockchain and its widespread adoption.
- **Small signature and hash length:** A blockchain essentially stores data transactions, including user signatures and data/block hashes. Therefore, if signature/hash length increases, blockchain size will also increase as well.
- **Fast execution:** Post-quantum schemes need to be as fast as possible in order to allow a blockchain to process a large amount of transactions per second. Moreover, a fast execution usually involves low computational complexity, which is necessary to not to exclude resource constrained devices from blockchain transactions.
- **Low computational complexity:** This feature is related to a fast execution, but it is important to note that a fast execution with certain hardware does not imply that the post-quantum cryptosystem is computationally simple. For instance, some schemes can be executed fast in Intel microprocessors that make use of the Advanced Vector Extensions 2 (AVX2) instruction set, but the same schemes may

be qualified as slow when executed on ARM-based microcontrollers. Therefore, it is necessary to look for a trade-off between computational complexity, execution time and supported hardware devices.

- **Low energy consumption:** Some blockchains like Bitcoin are considered to be power hungry mainly due to the energy required to execute its consensus protocol. There are other factors that impact power consumption, like the used hardware, the amount of performed communications transactions and, obviously, the implemented security schemes, which can draw a relevant amount of current due to the complexity of the performed operations.

4.2 Post-Quantum Cryptosystems for Blockchain

There are three main types of post-quantum cryptosystems and a fifth kind that actually mixes both pre-quantum and post-quantum cryptosystems. The following subsections analyze the potential application of such schemes for the implementation of encryption/decryption mechanisms and for signing blockchain transactions.

PUBLIC-KEY POST-QUANTUM CRYPTOSYSTEMS

1) LATTICE-BASED CRYPTOSYSTEMS

As Micciancio and Regev (2008) have explained in their paper, a lattice is a set of points in n-dimensional space with a periodic structure[11]. Given 'n' linearly independent vectors b1,b2,b3....bn, with each vector containing m entries, the lattice generated by them is defined as all possible weighted sums of these vectors when scaled by integers. To create a 2D vector we choose two points for e.g (4,2) & (2,4) and choosing another random number such as a=6,b=-3 and multiplying a with 1st point and b with 2nd which would compute to (24,12) & (-6,-12) and by unceasing this process would generate a lattice with the basis containing vectors (4,2) & (2,4). Depending on these a short vector, long vector, and closest vector problem. A short basis lattice problem can be explained as, given a long basis for some lattice "L", find the short basis for L. The advantage of the lattice is that no efficient algorithm, classical or quantum, can solve these problems in better than exponential time.

It includes the generation of cryptographic primitive that involves lattice in underpinning security or security proofing. Lattice-based cryptographic constructions are quite appealing for post-quantum cryptography, as they ensure robust security proofs, even for worst-case hardness, relatively impressive implementations while keeping things simple. Lattice-based cryptography is believed to be secure against quantum computers.

2) CODE-BASED CRYPTOSYSTEMS:

As Overbeck R., Sendrier N. (2009) have explained, codebased cryptography are the cryptosystems that use error correcting codes C in the algorithmic primitive. The algorithmic primitive is the underlying one-way function. This primitive may consist in adding an error to a word of C or in computing a syndrome relative to a parity check matrix of C[8]. The initail versions of the cryptosystems is a public key encryption scheme and it was proposed by Robert J. McEliece (1978). The public key is a random generator matrix. This matrix is the arbitrarily permuted variation of the Goppa code. The private key is an arbitrary binary Goppa code that is irreducible. Ciphertext is gained after the addition of errors to the codeword. These errors can be removed only by the owner of the Goppa code which is the private key. When some parameter adjustments were made three decades later, no attack was known to represent a serious threat on the system, even on a quantum computer[9]. After the first proposal of a code based cryptosystem by Robert J. McEliece, all other proposals suffered a common problem: they all had large memory requirements. A similar performance problem was observed in JeanBernard Fischer and Jacques Stern's[10] pseudo-random generator. Various proposals were made to modify McEliece's scheme in order to reduce the key size, however, most of them turned out to be insecure or inefficient. Code-based cryptography, however, is a potential candidate for post-quantum cryptography.

3) MULTIVARIATE-BASED CRYPTOSYSTEMS

According to Ding, Jintai & Yang, Bo-Yin (2009), the foundation of Multivariate Cryptography schemes is the challenge of computing non-linear equation structures over finite fields[12]. As Asif, Rameez. (2021) has explained in his paper titled Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms, seeking a solution for such structures is called an NP-complete/NP-hard problem. All Multivariate PublicKey Cryptosystems (MPKC) use the same basic architecture, since they all rely on the use of multivariate polynomials over a finite field. The degree of polynomial is two in most cases which results in multivariate quadratic polynomials. These are still credited with being solved as NP-hard[13]. The Shor's algorithm does not seem to crack the MQPKC more easily with a classical computer. This is because it does not rely on any of the complex problems that Shor's algorithm can solve when compared to various other versions of public-key cryptography. It is also a potential candidate group for, a quantum-resistant encryption scheme[14]. When compared to other encryption schemes, multivariate offers various advantages. Multivariate schemes outperform most of it’s competitors with regard to speed and can be implemented efficiently. What makes multivariate schemes attractive is the fact taht they are quick and demand only modest computational resources. [15]. Multivariate schemes employ simple arithmetic operations such as multiplication and addition and thus can be utilized on cheap devices like RFID chips. Also, signatures in Multivariate schemes are very short, upto a few hundred bits. However, the major disadvantage of multivariate schemes is that it has a large size of public keys. The public key size is typically about 10 to 100kB which are much larger than that of RSA like classical schemes.

Comparison of post-quantum cryptography algorithms				
Name of the algorithm	**Claimed Quantum Security**	**Claimed Classical Security**	**Public Key Size**	**Private Key Size**
Code-based Cryptography	64 bits, 96 bits,128 bits	128 bits, 192 bits, 256 bits	6,824 ~ 10,862,529 bits	320 ~ 159,376 bits
Lattice-based Cryptography	100 bits, 101 bits, 164 bits, 230 bits, 233 bits, 128 bits ~ 308 bits	128 bits, 192 bits, 256 bits, 153 bits ~ 368 bits	6400 bits ~ 172,160 bits	320 ~ 25,344 bits
Multivariate-based Cryptography	128, 192, 256 bits	46 bytes ~ 7106 Kbytes	93 Kbytes ~ 122701 KBytes	N.A

We have done a comparative study that distinguishes these algorithms based on various parameters.

4.3. QUANTUM-SECURED BLOCKCHAIN

In the research paper by Kiktenko, et al. a blockchain protocol has been proposed. A secure authentication based on a network in which each pair of nodes is connected via a quantum key distribution (QKD) link. Here, a blockchain protocol with a two-layer network with n nodes is considered. The first layer communicates private keys securely for each pair of nodes in the QKD network. The second layer is used to transmit messages with authentication tags securely that are created using the private keys obtained from the first layer. The chaining process proposed here is different than usual. In the proposed Quantum-secured blockchain, the unconfirmed transactions are aggregated together to avoid quantum computer attacks. This ensures protection from attacks of quantum computer in minimum two number of ways. First, the digital signatures would not rig the transactions. Second, a node equipped with quantum computing capabilities is able to generate new blocks colossally faster than another node without quantum computing capabilities. It is also emphasized that the protocol is relatively data intensive. It is not necessary to transmit data through quantum channels. Quantum channels are not for any purpose other than generating private keys[7]. The proposed protocol seems to be effective against attacks by quantum computers on the generation of new blocks and circulation of transactions. However, the database is still vulnerable while it is being stored. This protocol has been tested in Moscow experimentally.

4.4. Methodology to implement Quantum electronic voting:

Electronic voting protocols consist of election authorities, talliers, voters and bulletin board. In this work, we will be dealing with protocols involving only one election authority EA and/or one tallier T, as well as the voters V. EA sets the parameters of the protocol, V cast ballots and T gathers the votes, computes and announces the election outcome. Informally, a voting protocol Π has three distinct phases (setup, casting, and tally) and running time proportional to a security parameter δ0.

- **Setup phase:** A defines the voting choices of all voters. C and A generate the protocol parameters X according to Π.
- **Casting phase:** The protocol Π specifies the algorithm Cast Ballot for generatingand casting the ballots. C generates ballots according to the Cast Ballot algorithmon behalf of honest voters and A on behalf of the corrupted ones.
- **Tally phase:** The protocol Π specifies the tallying algorithm Tally. C computes the election result on behalf of the parties specified in Π by running the Tally algorithm. If none of these parties is honest, A computes the tally instead.

Ideally, an e-voting protocol will satisfy at least the following properties:

- **Correctness:** compute the correct outcome if the adversary doesn't interfere.
- **Double voting:** allow voters to vote at most once, Privacy: keep the vote of a voter private.
- **Verifiability:** allow for verification of the results by voters and external auditors.We focus on privacy and verifiability type properties.

Improvements in electronic voting and referendum post quantum computing and blockchain juxtaposition:

1) When quantum computers and blockchain are juxtapositioned, we can assume that electronic voting and referendum would witness a giant leap in terms of processing the votes and choices.
2) As the votes are stored as blocks currently, if any block experiences tampering, that block may have to be discarded or if need arises the complete blockchain may be rebuilt. It is quite obvious that these operations are very expensive and repetitive. Here's where the quantum computer can intervene and take over. As previously recorded the quantum computers as polynomially faster than current classical computers. Thus, in case of tampering the blockchain could be rebuilt in very less time.

Chapter 5 Conclusion

5.1 Challenges:

The major challenges that we faced while publishing this paper were:

1) Limited resources and redundant data that we came across since this topic is relatively new.
2) Also, the algorithms proposed and compared are merely based on the theoretical knowledge and results will be much more efficient once these algorithms are implemented and tested by a quantum computer.
3) The approaches we have taken majorly inclines towards protecting blockchain from quantum computing. Thus, giving rise to Post Quantum Cryptography. However, facilitating Quantum Computing with blockchain still remains a disintegrated project.
4) The Post Quantum Cryptography Algorithms have been studied and explained in this paper on a very trivial scale. Detailed description of the same was difficult due to the complexity of the topic and equations involved in these algorithms.
5) E-voting is already being implemented by the means of small scale projects, even the U.S.A. 2020 elections implemented a fair module of E-voting but it remains to see how proper execution of E-voting using Post Quantum Cryptography takes place.

5.2 Solutions:

1) Under the constant guidance of our project guide, Dr. G.T. Thampi, it was relatively easy to understand these topics and their significance.
2) Based on the theortical knowledge derived from various references, the comparative study that we have produced lays a strong foundation to implement these algorithms on a classical computer and Quantum computer. With the help of this comparative study, we were able to determine the pros, cons, specifications and feasibility of each algorithm and give our take on which algorithm in our opinion will be sustainable for developing a Post Quantum Cryptosystem.
3) We have been able to give a fair blueprint on how an E-voting system can be developed using Post Quantum Cryptography after fusing the current E-voting system with the proposed PQC.

5.3 Conclusion

Thus, this paper gives a brief idea about two of the most significant technologies that define the future of engineering science; Blockchain & Quantum Computing. This literature provides us with the current scenario of these 2 technologies and how Quantum Computing is posing a threat to Blockchain and it suggests two approaches to facilitate the same. A comparative study has been done on various Post Quantum Cryptography Algorithms and based on the analysis, we determine which algorithm suits the best for the new iterated E-voting which shall be conducted in the future.

Performance comparison of post-quantum cryptography algorithms			
Lattice-based cryptography	Fast	Resistant against quantum attacks	Key exchange: 1Kb
Code-based cryptography	Slower than Lattice-based cryptography	Resistant against quantum attacks	Key exchange: 1Mb
Multivariate-based cryptography	Slow	Limited resistance against quantum attacks	Key exchange: Not Applicable

Chapter 5

References

1) S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. [Online]. Available: https://bitcoin.org/bitcoin.pdf

2) M. Swan, “Blockchain: blueprint for a new economy”. First Edition, O’Reilly Media, Jan. 2015.

3) T. M. Fernández-Caramés, O. Blanco-Novoa, I. FroizMíguez and P. Fraga-Lamas, “Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applications in Big Data-Driven Supply Chain Management,” Sensors, vol. 19, no. 10, p. 2394, May 2019.

4) L. K. Grover, “A fast quantum mechanical algorithm for database search”. In Proc. 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, USA, May 1996.

5) Brandon Rodenburg, PhD Stephen P. Pappas, PhD, “Blockchain and Quantum Computing” MITRE Technical Report, June 2017.

6) P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,” SIAM Journal on Computing, vol. 26, no. 5, pp. 1484-1509, Oct. 1997.

7) Kiktenko, et al. “Quantum-secured Blockchain”, June 5, 2018.

8) Overbeck R., Sendrier N. (2009) Code-based cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540- 88702-7_4

9) McEliece, R.: A public key cryptosystem based on algebraic coding theory.DSN progress report, 42– 44:114–116 (1978).

10) Fischer JB., Stern J. (1996) An Efficient PseudoRandom Generator Provably as Secure as Syndrome Decoding. In: Maurer U. (eds) Advances in Cryptology — EUROCRYPT ’96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68339- 9_22

11) Micciancio D., Regev O. (2009) Lattice-based Cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540- 88702-7_5

12) Ding, Jintai & Yang, Bo-Yin. (2009). Multivariate Public Key Cryptography. 10.1007/978-3-540-88702-7_6.

13) Ding, Jintai & Petzoldt, Albrecht. (2017). Current State of Multivariate Cryptography. IEEE Security & Privacy. 15. 28-36. 10.1109/MSP.2017.3151328.

14) Asif, Rameez. (2021). Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms. IoT. 2. 71-91. 10.3390/iot2010005.

15) Ding J., Petzoldt A., Wang L. (2014) The Cubic Simple Matrix Encryption Scheme. In: Mosca M. (eds) PostQuantum Cryptography. PQCrypto 2014. Lecture Notes in Computer Science, vol 8772. Springer, Cham. https://doi.org/10.1007/978-3-319-11659-4_5

16) T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," in IEEE Access, vol. 8, pp. 21091- 21116, 2020, doi: 10.1109/ACCESS.2020.2968985.

17) F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

18) Vujičić, Dejan & Jagodic, Dijana & Ranđić, Siniša. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. 1-6. 10.1109/INFOTEH.2018.8345547.