Table of Contents

1. **Chapter 1 Introduction** 10
    - 1.1. **Brief history** 10
    - 1.2. **What is Blockchain** 11
    - 1.3. **Blockchain applications** 12
        - 1.3.1. **Bitcoin** 12
        - 1.3.2. **Ethereum** 12
    - 1.4. **Components of Blockchain** 13
        - 1.4.1. **Cryptography** 13
        - 1.4.2. **Peer 2 peer** 14
        - 1.4.3. **Game theory** 14
    - 1.5. **Blockchain Structure** 15
2. **Chapter 2 Bitcoin network** 17
    - 2.1. **Structure** 17
    - 2.2. **How Bitcoin works** 17
        - 2.2.1. **Creating an address** 17
        - 2.2.2. **Create transactions** 18
        - 2.2.3. **Propagation mechanism** 19
        - 2.2.4. **Proof of work** 20
    - 2.3. **Bitcoin Technical Challenges** 21
        - 2.3.1. **Scalability** 21
        - 2.3.2. **Usability** 21
        - 2.3.3. **Throughput** 21
        - 2.3.4. **Majority attacks** 22
        - 2.3.5. **Double spending attack** 22
        - 2.3.6. **Inconsistency** 23
        - 2.3.7. **Forking** 23
        - 2.3.8. **Eclipse attack** 24
    - 2.4. **Problem statement** 25
    - 2.5. **Contribution** 25
    - 2.6. **Organization** 25
3. **Chapter 3: Blockchain cryptography (ECC)** 26

3.1. **Introduction** 26

3.2. **Definition** 26

3.3. **Point addition** 27

3.4. **How point addition works in ECC** 28

3.5. **Doubling and addition** 29

3.6. **Finite field and subgroup** 30

3.7. **Digital signature ECDSA** 31

4. **Chapter 4 NTRU Cryptography** 33

4.1. **Introduction** 33

4.2. **Parameters and spaces** 33

4.3. **Example of encryption and decryption** 35

4.4. **NTRUSign** 36

4.4.1. **Parameters** 36

4.4.2. **Key Generation** 36

4.4.3. **Signing** 36

4.4.4. **Verification** 36

5. **Chapter 5 NTRU and ECC Comparison** 37

5.1. **Introduction** 37

5.2. **Key size:** 37

5.3. **Previous Research:** 37

5.4. **Conclusion** 42

6. **Chapter 6: Accelerating propagation delay by using NTRU verification process** 43

6.1. **Introduction** 43

6.2. **Proposed method** 43

6.3. **The model** 43

6.4. **Implementation** 46

6.5. **The results** 46

6.5.1. **First Scenario** 47

6.5.2. **Second Scenario** 48

6.5.3. **Third Scenario** 49

6.5.4. **Fourth Scenario** 50

6.5.5. **Fifth Scenario** 51

6.6. **Conclusion and future work** 53

7. **References**.. 54