# INTRODUCTION

Recently electronic financial transactions and contract are frequently used for business. Therefore, method for securing those transactions are necessary. One method for securing an electronic contract is proposed by Sony, et al. [1].

Sony, et al. proposed a method for securing a contract by introducing a method based on blockchain and ECDSA. However, Sony’s method [1] has a drawback, because it uses ECDSA which has high time complexity. Furthermore, cryptosystem based on discrete logarithm is not resistant against quantum attack [2].

Therefore, this research proposed a method that is resistant against quantum computing attacks and reduces the time complexity. To overcome the quantum attack and reduce the time complexity of the digital signing process, McElliece Cryptosystem and Niederreiter based signature are introduced to the blockchain-based contract. Since McElliece Cryptosystem and Niederreiter based signature uses scalar multiplication then the processing time is less than ECDSA.

Experiment result shows that the time complexity of signing the contract using the proposed method is less than the time complexity when using Sony’s method [1].