1. Introduction

Authentication is usually a combination of email and password enable access to the account. Web application are platforms that uses authentication system to check an account is really accessed by own user. Authentication has three factors: something that you know, something that you have, and something that you are. Authentication usually encounter in web applications is one-factor authentication or password-based authentication refers to the category something that you know [1, 2, 3, 4]. Password-based authentication has weaknesses, that are easy to brute force attacks, so the users data are vulnerable of being stolen [5, 6]. Users usually use the same password on many platforms to make it easier to remember [4, 7]. Such method is vulnerable to attacks. Hackers who succeed in getting the user passwords from one platform can also stole the user data on another platforms. Therefore, password-based authentication cannot accommodate the security and confidentiality of account data [8, 9, 10].

To resolve the weakness of password-based authentication in web applications by adding a layer of security and combining two authentication factors together called two factor authentications (2FA). 2FA is an authentication system that combines the first-factor authentication (something that you know) with the second factor (something that you have). Performance as same as with 2FA password-based authentication, but 2FA is requiring to enter additional information in the form of tokens or one-time passwords (OTP). The token is generated by a third-party then be sent to the user via SMS or mailing system.

According to paper [11], tokens generate are done by the users and stored into the blockchain. Tokens can be used every time will do 2FA. In this way, the token used for each authentication has the same value and token only used once. Refers to [2], Tokens generate system handled by a smart contract and sent to the user via OTP-SMS, but They are still use third-parties to send tokens and is not secure for the 2FA system because tokens can be stolen by attackers through MITM (Man-In-The-Middle) [2, 12].

We propose a 2FA framework that is different from the existing system and develop with dApp as a token generating system. DApp is a decentralized application that runs on peer-to-peer networks [3]. Another difference is that the general 2FA system will send the generated token via third-party to the user to be inputted on. However, the user does not need to manually input the token because checking will be done automatically by the system. Implementing Ethereum blockchain technology to avoidance using third-party and to develop this system because Ethereum can modify centralized systems into distributed systems with programming capabilities. This system can counter MITM and 2FA attacks systems from third-parties.