# ZK-ARAB: Zero Knowledge Account Recovery and Authentication through the Blockchain

*December, 2023*

***Muhammad-Jibril B.A. (Khalifa MBA)***

*Founder, Imam, Chief Architect*

**Slixon Technologies | Setheum Labs| Open Web3 Foundation**

## I. Abstract

With zkARAB, you can use one Zero Knowledge based Authentication system for all your apps, zk-ARAB is your one-stop authenticator. With our SDKs, developers can integrate zkARAB in their web3 apps and even their web2 apps - effectively making them web3 apps, they can enable features from Web3 Wallet account login to Email login, and allow their users to recover their accounts and optionally setup passwords without losing security or password confidentiality and confidence, equipped with 2FA, all based on Zero Knowledge Proofs. Users will find it quite simple and easy to use apps based on zkARAB.

## II. Table of Contents

## 1. Introduction

We have seen a multiple of times when people or organisations lose access to their crypto assets either by forgetting their hardware wallet passcodes or losing its whereabouts, and many different other examples that go from the simplest of mistakes to very complex problems that all lead to losing access to valuable assets. Setheum is trying to solve that with the introduction of `ZK-ARAB`.

Some people lose all their life's work to this class of problems, some lose all their savings, others lose all their investments or their hope and interest in this industry and seem to get confused worrying if this revolution has failed them or if they have failed it or both. A lot of us are guilty of this, many people went under and many people went extreme, but we are still here aren't we. This is why CEXs(centralised exchanges) have helped in onboarding most of the people coming into the industry and retaining most of them, CEXs can provide easy key management options and wallet recovery methods for their users. This is why CEXs also provide these custodial services not just to retail investors, family offices and newbies but also to institutional investors like banks, VCs and hedge funds.

Apart from the classical Social Recovery system, Setheum is building a Zero Knowledge based Account Recovery and Authentication System that we call zkARAB (Zero Knowledge Account Recovery and Authentication through the Blockchain). DeFi(Decentralised Finance) cannot reach mass adoption to the scale of centralised options without solving this class of problem, the wallet recovery problem.

# 2. Substrate Social Recovery Pallet

Thanks to the substrate framework and the talented team, contributors and ecosystem behind its development, for developing a `Social Recovery` system to recover lost accounts. Substrate has a `pallet-recovery` module that enables users to assign a list of contacts as a social circle of recovery to allow them to recover their wallet.

# 3. ZK-ARAB: Your One-Stop Authentication Shop

zkARAB (Zero Knowledge Account Recovery and Authentication through the Blockchain) is a Zero Knowledge based Account Recovery and Authentication System through the Blockchain and Web3 Applications built on zkSNARKs. zk-ARAB is not just for blockchain wallets and dApps can be used to integrate Zero Knowledge based Authentication and Recovery for both web3 and web2 apps.

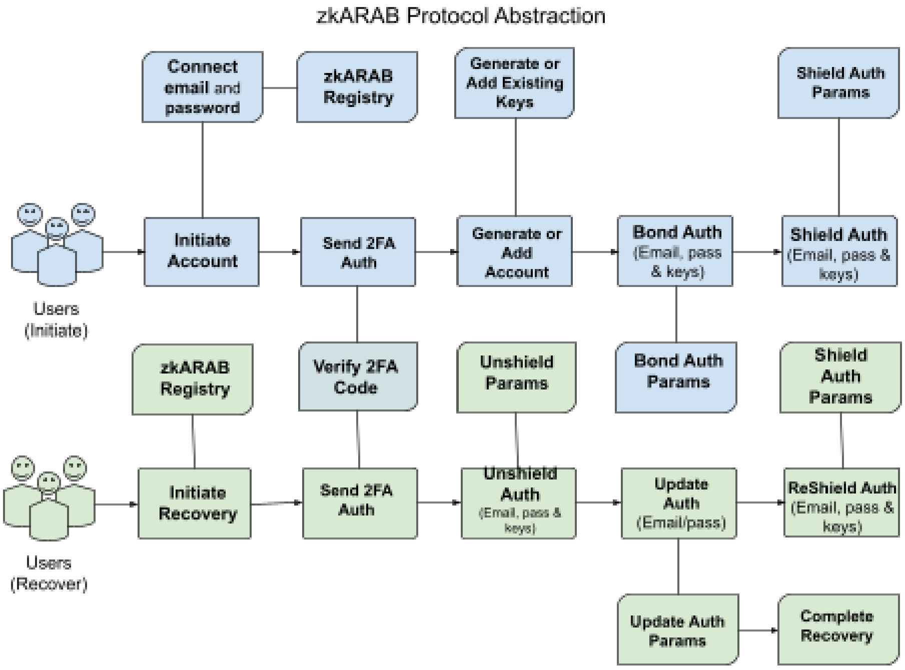

Figure-1: zkARAB Protocol Abstraction Overview

## 3.1. zkARAB Initiation Process

The Initiation process of the zkARAB setup looks like this under the hood;

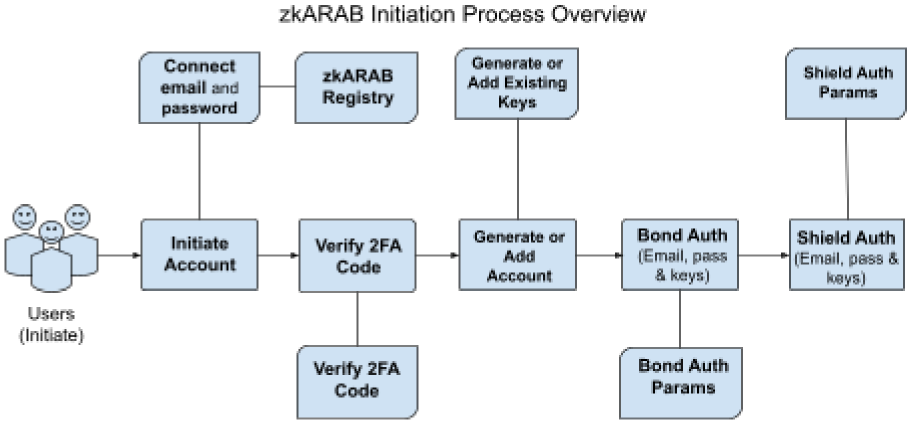
zkARAB Initiation Process Overview
Connect email and password
zkARAB Registry
Generate or Add Existing Keys
Shield Auth Params
Users (Initiate)
Initiate Account
Verify 2FA Code
Generate or Add Account
Bond Auth (Email, pass & keys)
Shield Auth (Email, pass & keys)
Verify 2FA Code
Bond Auth Params

Figure-2: zkARAB Initiation Process Overview

## 3.2. zkARAB Recovery Process

The recovery process of the zkARAB setup looks like this under the hood;

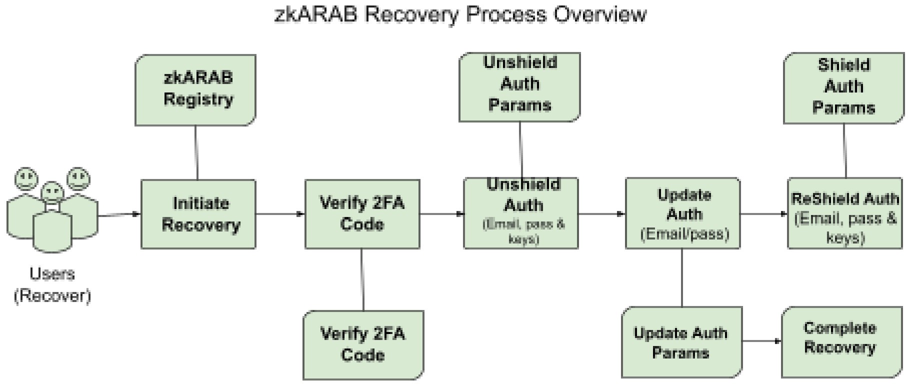

Figure-3: zkARAB Recovery Process Overview