

## Задача 2

# Протокол восстанавливаемых биометрических ключей

### Актуальность задачи

На данный момент одной из наиболее актуальных проблем является отсутствие инструментов по восстановлению приватного ключа. Сейчас пользователю приходится сохранять резервную копию за которую он несет персональную ответственность и которую можно потерять. Использование биометрии пользователя может решить эту проблему.

### Целевая аудитория сервиса

Пользователи DeFi-протоколов, владельцы криптокошельков

### Образ финального решения

Прототип системы, позволяющей безопасно восстанавливать доступ к криптокошельку с использованием биометрических данных пользователя.

### Предполагаемая функциональность

*Ниже описана предполагаемая функциональность, вы можете предложить свою реализацию поставленной задачи восстановления ключа.*

1. Генерация биометрического ключа: Разработка алгоритма для генерации уникального биометрического ключа на основе данных пользователя (например, отпечаток пальца, сканирование лица или голос). Использование методов глубокого обучения (DL) для создания устойчивого и воспроизводимого ключа.

2. Восстановление ключа с использованием биометрии: Разработка механизма восстановления приватного ключа на основе биометрических данных пользователя. Обеспечение уникальности и безопасности процесса восстановления.

3. Доказательство уникальности биометрических данных: Создание системы, которая подтверждает уникальность биометрических данных пользователя для восстановления ключа без необходимости хранения самого ключа.

Демонстрация работы системы: Создание интерактивного демо, показывающего процесс восстановления приватного ключа с использованием биометрии. Визуализация работы протокола и процесса генерации/восстановления ключа..

### Требования к разработке

Открыты к любым предложениям по реализации.

### Требования к сдаче решений на платформе

1. Ссылка на репозиторий с кодом
2. Презентация
3. Ссылка на прототип
4. Сопроводительная документация (.doc/.pdf)

Если тебе нужно найти команду –  
присоединяйся к сообществу разработчиков  
ComUnity по ссылке вот здесь.

Если у тебя есть вопрос по задаче,  
то ты можешь написать его на почту  
[blockchain@sberbank.ru](mailto:blockchain@sberbank.ru) либо в чат ComUnity  
по ссылке вот здесь