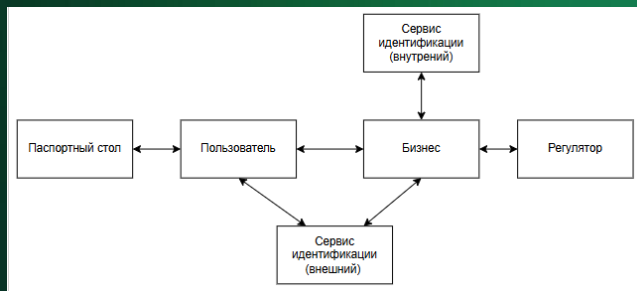


## Задача 4

# zkKYC

### Актуальность задачи

Задача актуальна в любом бизнес процессе, где бизнес должен проводить процедуру KYC - совершение финансовых транзакций, каршеринг, продажа алкоголя и т.п. В частности в экосистеме "блокчейн" пользователь, который хочет купить цифровой актив, должен проходить процедуру KYC, доверяя свои данные третьим лицам. Так же это актуально для экосистем DeFi с разрезе AML



Классическая схема взаимодействия пользователя в бизнес процессе, где необходим KYC. Основные проблемы такого взаимодействия в том, что пользователь не контролирует передачу данных от сервиса идентификации бизнесу, а иногда сам бизнес может попросить передать данные и сделать проверку, через свой собственный сервис идентификации.

### Целевая аудитория сервиса

Пользователи кастодиальных и/или некастодиальных кошельков, где есть интеграция с внешним сервисом, например биржей. Сервисы, которые хотят упростить пользовательский опыт и снизить риски утечки данных

### Образ финального решения

Веб-страница, где пользователь проходит авторизацию в стороннем сервисе и совершает транзакцию, предоставив необходимые доказательства.  
Пример подобного сервиса  
<https://www.youtube.com/watch?v=oGjJ-rTFtQc>

### Предполагаемая функциональность

1. Сервис идентификации должен быть представлен в виде SSI (self-sovereign identity), например Decentralized ID.
2. Пользователь НЕ ДОЛЖЕН предоставлять персональную информацию бизнесу (ФИО, адрес, дату рождения)
3. Пользователь ДОЛЖЕН предоставить доказательство бизнесу, что он соответствует необходимым критериям (совершеннолетний, гражданство, не является террористом и т.п.)
4. Бизнес, который подозревает пользователя в отмывании денег или другой противоправной деятельности, ДОЛЖЕН иметь возможность предоставить информацию об этом регулятору. Учитываем, что регулятор может обратиться напрямую в паспортный стол.
5. Бизнес МОЖЕТ предъявить обвинения пользователю через регулятор
6. Регулятор МОЖЕТ идентифицировать пользователя на основе предоставленной информации от бизнеса
7. Бизнес не хранит никакой персональной информации, кроме той, что предоставил ему регулятор

Желательно:

Решение должно ложиться на кастодиальные и некастодиальные кошельки, а так же DeFi

### Требования к разработке

Желательно:

для back-end использовать java/golang  
для frontend - js/typescript  
демонстрация в сети ethereum

### 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