

IDChain

17/02/2017

Удаленная идентификация на Blockchain

Проблема удаленной идентификации

Все более востребованной становится возможность проведения процедуры идентификации личности удаленным способом. Это в первую очередь связано с проблемами снижения доступности финансовых услуг и ухудшения условий конкуренции на рынке. Так же удаленная идентификация необходима при обслуживании лиц с ограниченными возможностями и проживающими в труднодоступных местностях.

Статья 3 Федерального закона от 07.08.2001 №115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма») дает следующее определение. «Идентификация» – это совокупность мероприятий по установлению определенных Законом № 115-ФЗ сведений о клиентах, их представителях, выгодоприобретателях, бенефициарных владельцах, а также по подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий

Согласно 115-ФЗ для осуществление удаленной идентификации необходимо выполнение следующие процессов:

1. получить идентификационные сведения о клиенте;
2. подтвердить достоверность полученных сведений;
3. удостоверить (верифицировать) личность клиента;

Как осуществить удаленную идентификацию?

В соответствии с Федеральным законом от 07.08.2001 N 115-ФЗ О ПРОТИВОДЕЙСТВИИ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА:

1.5. Кредитная организация вправе поручать на основании договора, в том числе многостороннего (включая правила платежной системы), другой кредитной организации, ..., проведение идентификации или упрощенной идентификации клиента...

На основании пункта 1.5 Федерального закона от 07.08.2001 №115-ФЗ кредитная организация может поручать проведение идентификации клиента. Поэтому применив принцип интероперабельности возможна организация консорциума организаций, которые смогут предоставлять или получать услугу удаленной идентификации собственных клиентов. При этом участниками консорциума могут быть не только банки или сотовые операторы, которые могут как предоставлять услугу удаленной идентификации, так и получать её, но и организации, которые хотят только получать услугу идентификации, такие как брокеры, МФО и , в принципе, любые организации, которым требуется услуга удаленной идентификации клиентов. В рамках консорциума отношения между участниками будут регулироваться договором присоединения, в котором будет прописана логика работы смарт контракта.

Интероперабельность(англ.interoperability— способность к взаимодействию) — это способность продукта или системы, интерфейсы которых полностью открыты, взаимодействовать и функционировать с другими продуктами или системами без каких-либо ограничений доступа и реализации.

Классический процесс удаленной идентификации по OAuth 2.0

Участники:

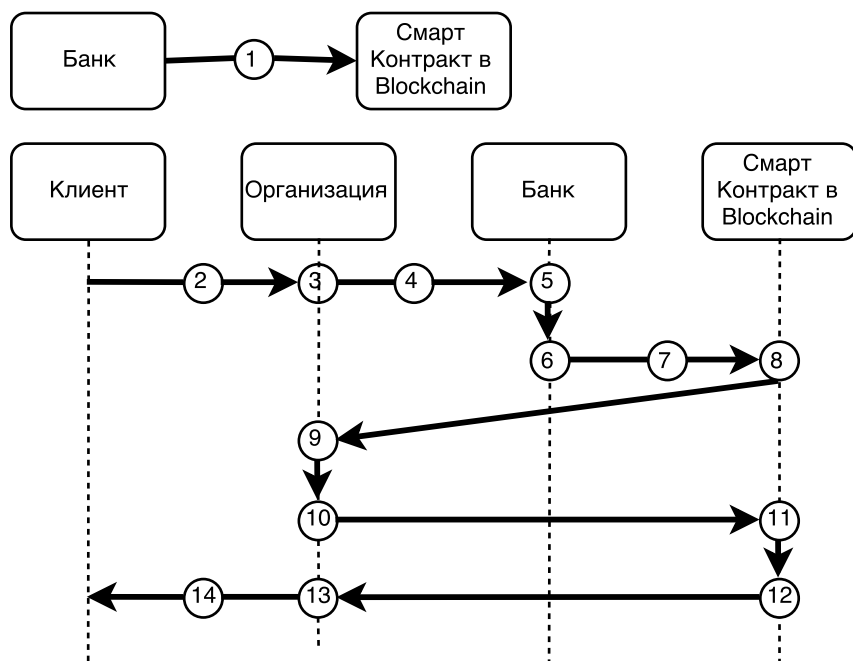
- **Клиент** - это физическое лицо, которое хочет получить услугу у **Организации**.
- **Банк** - это кредитная организация (участник консорциума), в которой **Клиент** проходил процедуру первичной идентификации с личным присутствием.
- **Организация** - это участник консорциума, которому необходима услуга удаленной идентификации **Клиента**.

Процесс:

1. При обращении **Клиента** в **Организацию** за услугой, **Клиент** собственноручно передает свои персональные данные **Организации**.
2. **Организация** перенаправляет **Клиента** в **Банк** для прохождения процедуры удаленной аутентификации(авторизации).
3. После успешной аутентификации **Банк** отправляет **Организации** персональные данные **Клиента**, хранимые в собственной АБС.
4. **Организация** сверяет персональные данные, полученные от **Клиента**, с персональными данными, полученными от **Банка**.
5. Если данные совпали, то идентификация является успешной.

Но при использовании данной схемы возникает проблема недоверия **Банков** к друг другу, т.к. факт передачи персональных данных и факт успешной сверки нигде не зафиксированы, и могут быть оспорены обеими сторонами. Также возникают сложности, связанные с передачей, обработкой и хранением персональных данных Клиента. Для решения данных проблем используется технология Blockchain.

Предлагаемый механизм удаленной идентификации на технологии Blockchain

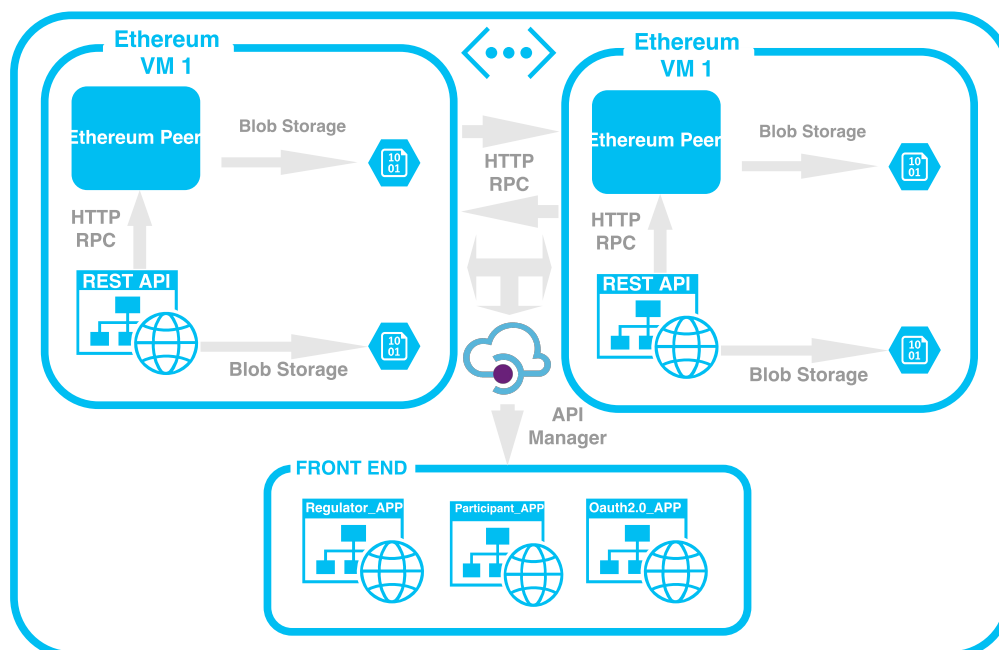


Хеш-функцией называется алгоритм, конвертирующий строку произвольной длины (сообщение) в битовую строку фиксированной длины, называемой *хеш-кодом*, проверочной суммой или цифровым отпечатком.

Токен - уникальный в рамках консорциума ключ Клиента.

1. Банк формирует пару значений для Клиента, которая состоит из хеша токена и хеша сложенных между собой персональных данных Клиента и токена. После чего Банк помещает эту пару значений в смарт контракт.
2. Клиент обращается за услугой в Организацию.
3. Организация предоставляет Клиенту интерфейс для ввода персональных данных и выбора организации, в которой Клиент хотел бы идентифицироваться(в нашем случае это Банк).
4. Переадресация Клиента на интерфейс ДБО Банка(предполагается Интернет-Банк) для прохождения аутентификации(авторизации).
5. Банк проводит аутентификацию по собственному механизму(например, двухфакторная, биометрия и т.д.).
6. При успешном прохождении Клиентом аутентификации Банк шифрует открытым ключом Организации токен Клиента.
7. Отправка в Организацию зашифрованного токена Клиента через смарт контракт для фиксации факта передачи токена.
8. Формирование сообщения с зашифрованным токеном и передача его Организации.
9. Получение и расшифровка токена с помощью закрытого ключа.
10. Формирование и отправка запроса с хешом токена и хешом сложенных между собой персональных данных, предоставленных Клиентом через интерфейс Организации, и токена.
11. Сверка данных, размещенных Банком в смарт контракте, и данных, переданных Организацией.
12. В случае успешной сверки смарт контракт фиксирует факт успешной сверки и отправляет ответ Организации.
13. Организация получает ответ об успешной идентификации Клиента.
14. Организация предоставляет услугу Клиенту.

Реализация механизма на платформе Ethereum



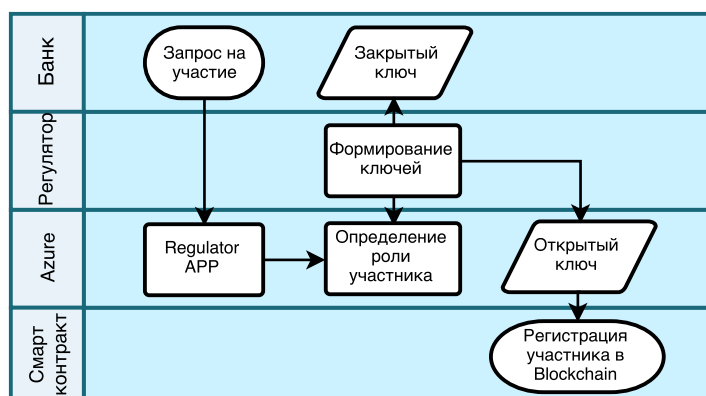
Механизм реализован на базе Microsoft Azure с использованием Blockchain платформы Ethereum. Консорциум состоит из развернутых в Microsoft Azure виртуальных машин, на которых установлена нода Ethereum и REST API сервер. Множество таких виртуальных машин образует закрытую Blockchain сеть. При этом одна из виртуальных машин является регулятором. Регулятор имеет право на работу с приложением Regulator_APP. Данное приложение позволяет регулировать процесс участия в консорциуме, а именно: регистрировать новых участников консорциума, удалять участников, выдавать соответствующие роли участникам.

После включения в консорциум участник может выбрать один из двух вариантов работы в Blockchain сети:

- настройка собственной виртуальной машины с последующим её включением в Blockchain сеть;
- работа через веб-приложение Participant_APP.

Использование приложения Participant_APP позволяет упростить вход участника в консорциум. Приложение Oauth2.0_APP необходима для осуществления процесса переадресации Клиента и последующего подтверждения аутентификации Клиента.

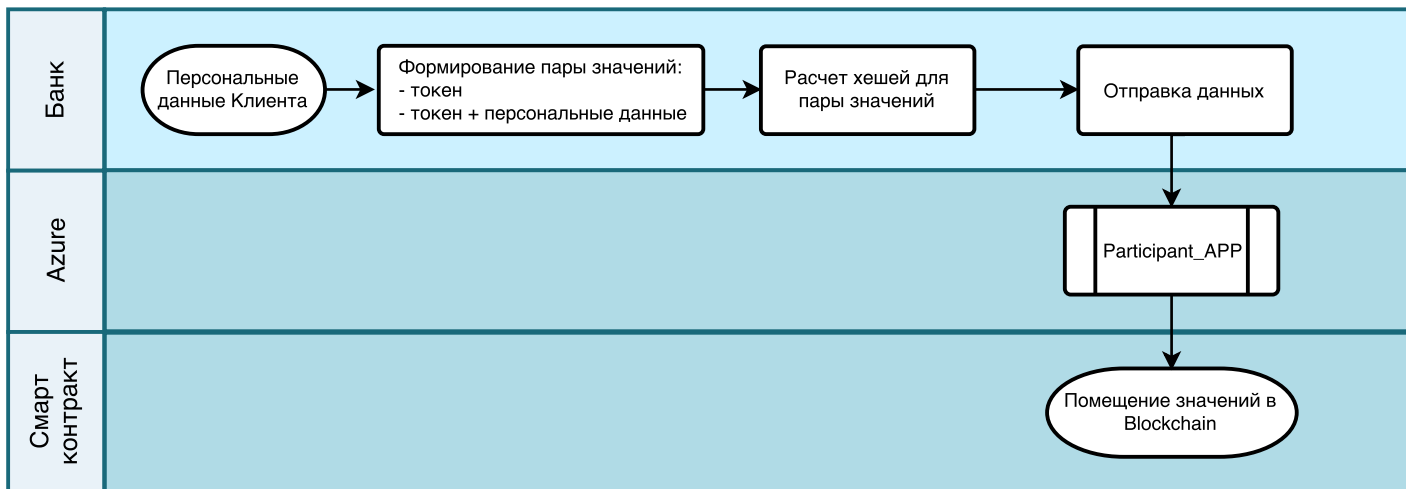
Процесс регистрации участника



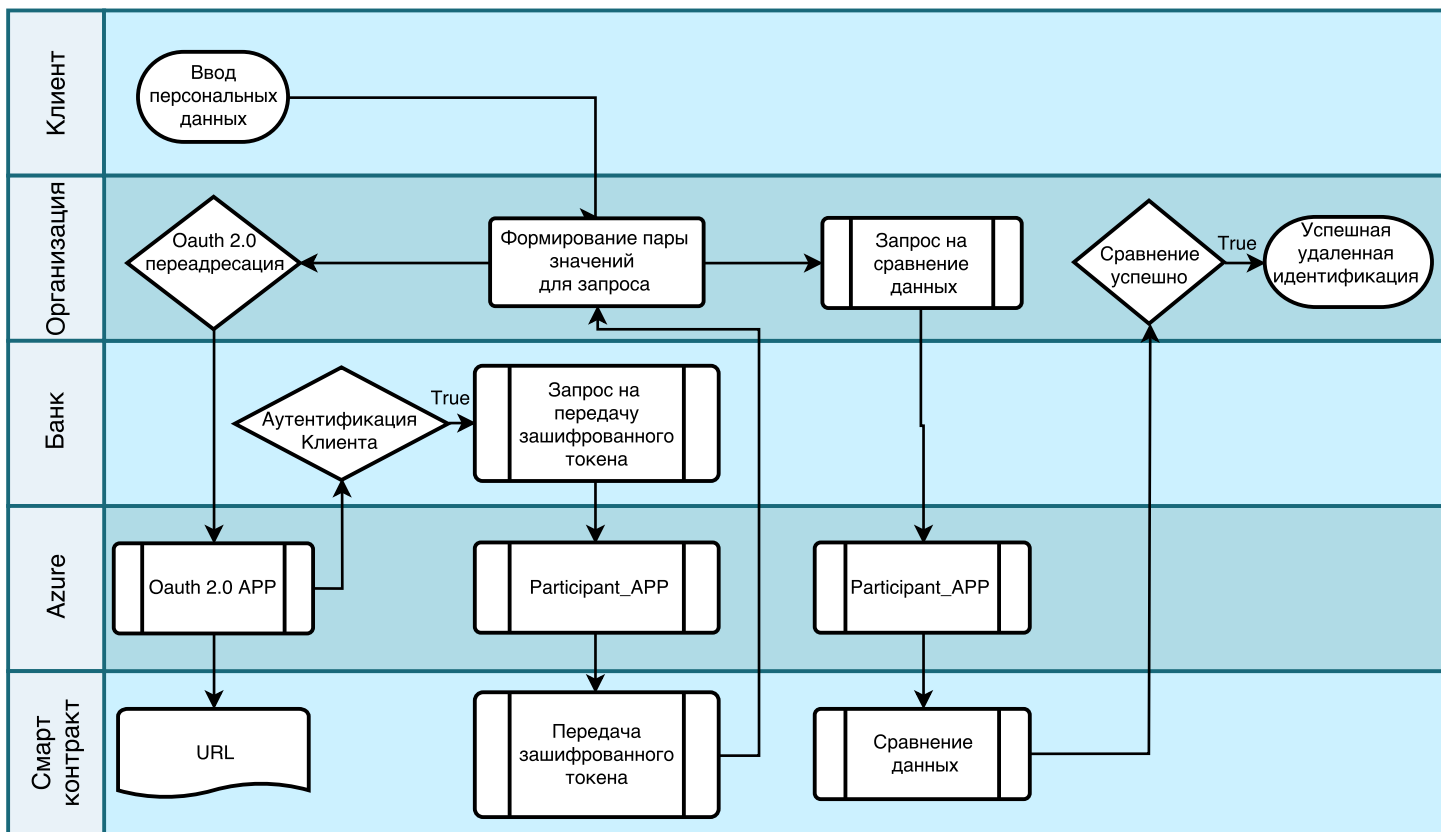
Реализация механизма на платформе Ethereum

Рассмотрим два основных процесса удаленной идентификации, реализованных на Ethereum и развернутых в Microsoft Azure.

Процесс загрузки данных Банком



Процесс удаленной идентификации



Почему именно IDChain?

- Консорциум, реализующий механизм удаленной идентификации на технологии Blockchain, позволяет обеспечить выполнение основных процессов, необходимых для проведения идентификации:
 - 1) "получение идентификационных сведений о клиенте" - получение персональных данных непосредственно от клиента;
 - 2) "подтвердить достоверность полученных сведений" - сравнение значений хеш-функций, хранящихся в Blockchain, с рассчитанными в моменте;
 - 3) "удостоверить (верифицировать) личность клиента" - аутентификация в банке, который проводил первичную идентификацию клиента.
- Использование технологии Blockchain обеспечивает хранение и неизменность информации о всех проведенных идентификаций.
- При этом банки получают ценную информацию о том, куда именно обратился их клиент и получают транзакционную прибыль от успешно предоставленной услуги идентификации.