АО «Лаборатория Касперского»
www.kaspersky.com, +7-495-797-8700

Описание функциональных характеристик Системы для организации электронного голосования Polys

1 Общая часть

1.1 Термины и определения

Алиас (Alias) – экземпляр смарт-контракта Alias, являющийся представлением пользователя системы в блокчейне. Алиас хранит guid – уникальный идентификатор пользователя в системе, и список блокчейн-аккаунтов, принадлежащих пользователю.

АС – автоматизированная система.

Голосование – способ принятия решения группой людей (собранием, электоратом), при котором общее мнение формулируется путём подсчета голосов членов группы.

Блокчейн (Blockchain) – аппаратно-программный комплекс, включающий в себя блокчейн-узлы, распределенный реестр и смарт-контракты.

Блокчейн-аккаунт – ключевая пара (публичный и приватный ключи) для подписания блокчейн-транзакций. Публичный ключ сохраняется в блокчейне, приватный ключ служит для подписания транзакций и хранится на устройстве пользователя.

Блокчейн-транзакция (транзакция) – вызов метода смарт-контракта, изменяющий состояние блокчейна. Транзакция выполняется на всех узлах сети. На всех узлах сети транзакция должна иметь одинаковый результат выполнения. Транзакция всегда создается внешней системой и подписывается блокчейн-аккаунтом.

Блокчейн-узлы (ноды) – синхронизированные между собой аппаратно-программные комплексы, обеспечивающие формирование и ведение распределенного реестра, а также выполнение смарт-контрактов.

Параметры системы шифрования (голосов) – набор значений для зашифрования и расшифрования голосов. У набора есть публичная часть – открытый ключ, модуль и генератор системы, которой достаточно для зашифрования голоса, и приватная – закрытый ключ, который необходим для расшифрования голоса.

Распределенный реестр – инкрементальная база данных, экземпляры которой размещены на блокчейн-узлах и синхронизируются согласно механизму консенсуса. В распределенном реестре хранится лог транзакций (организованных в блоки), код смарт-контрактов и лог изменения хранилища данных смарт-контрактов (транзакциями).

Смарт-контракт – программный код, представляющий из себя описание структуры хранения данных и набор функций (методов), записанный в распределенный реестр.

1.2 Назначение

Polys – основанная на технологии блокчейн автоматизированная система, предназначенная для проведения онлайн-голосований.

1.3 Описание ролей пользователей

Организатор голосования – субъект или организация, инициирующие проведение голосования и настраивающие параметры голосования.

Избиратель – субъект, имеющий право принять участие в голосовании.

Администратор АС – член команды разработчиков АС, выполняющий функции по конфигурированию АС под нужды организаторов голосования и управление лицензиями.

2 Реализация

2.1 Характеристики бизнес-требований

2.1.1 Общие характеристики

АС реализует:

- обеспечение возможности анонимного голосования;
- обеспечение возможности скрывать промежуточные результаты голосования;
- блокировку попыток повторного голосования избирателей, которые уже реализовали свое избирательное право;
- обеспечение автоматического подсчета голосов;
- обеспечение выдачи результатов голосования одновременно всем участникам;
- обеспечение прозрачности на всех этапах голосования;
- поддержку разных типов голосований;
- поддержку механизма лицензирования – ограничения для организаторов голосования на использование типов голосований, способов аутентификации избирателей и числа избирателей.

2.1.2 Типовой сценарий использования

Типовой сценарий использования АС предполагает следующую последовательность этапов:

1. Регистрация и аутентификация организатора голосования. На данном этапе в АС создается новый пользователь с ролью Организатор голосования, данные для аутентификации сохраняются в базу данных АС. Пользователю присваивается guid, а также создается алиас в блокчейне.
2. Выдача лицензии. На данном этапе администратор АС создает смарт-контракт лицензирования в соответствии с теми условиями и возможностями, которые указаны в приобретенной организатором голосования лицензии, и привязывает его к алиасу организатора голосования.
3. Создание и настройка голосования (в т.ч. создание списка избирателей). На данном этапе организатор голосования осуществляет конфигурирование параметров голосования, генерирует параметры системы шифрования и вносит в АС список избирателей, допущенных к голосованию.
4. Запуск голосования. На данном этапе создается смарт-контракт голосования со всеми указанными организатором голосования параметрами.
5. Аутентификация избирателя. На данном этапе в АС создается новый пользователь с ролью Избиратель, данные для аутентификации

сохраняются в базу данных АС. Пользователю присваивается guid, а также создается алиас в блокчейне.

6. Участие в голосовании. На данном этапе избиратель аутентифицируется в АС, после чего АС предоставляет возможность избирателю принять участие в тех голосованиях, к которым он был допущен на этапе создания и настройки голосования. Одновременно АС контролирует, чтобы каждый избиратель мог принять участие в голосовании только один раз. Голос избирателя (заполненный электронный бюллетень) зашифровывается с использованием параметров системы шифрования, созданных организатором голосования на третьем этапе. Далее создается транзакция отправки голоса, подписанная приватным ключом блокчейн-аккаунта избирателя, и транзакция отправляется в Блокчейн.
7. Завершение голосования и подсчет голосов. На данном этапе организатор голосования инициирует процедуру завершения голосования и публикует в Блокчейн полные параметры системы шифрования голосования. АС блокирует прием новых голосов, расшифровывает голоса избирателей с использованием полных параметров системы шифрования и автоматически подсчитывает результаты голосования.

2.2 Системные характеристики

АС включает в себя следующий набор компонент.

Блокчейн – сеть блокчейн-узлов с настроенной синхронизацией данных между ними.

Сервер идентификации и аутентификации (IdP) – аппаратно-программный комплекс, предназначенный для выполнения следующих функций:

- регистрация новых пользователей;
- ведение базы данных пользователей;
- идентификация и аутентификацию пользователей;
- восстановление доступа пользователей к АС;
- управление лицензиями.

Приложения пользователей:

- **Приложение организатора** – предоставляет организатору голосования возможность настраивать параметры голосований, настраивать доступ избирателей к голосованиям, отслеживать ход голосований, оформлять и распечатывать протоколы голосований.
- **Приложение избирателя** – предоставляет избирателю возможность принимать участия в голосованиях, доступ к которым настроен организатором голосования, а также контролировать корректность учета голоса после завершения голосования.

Структурная схема АС представлена на рисунке 1.

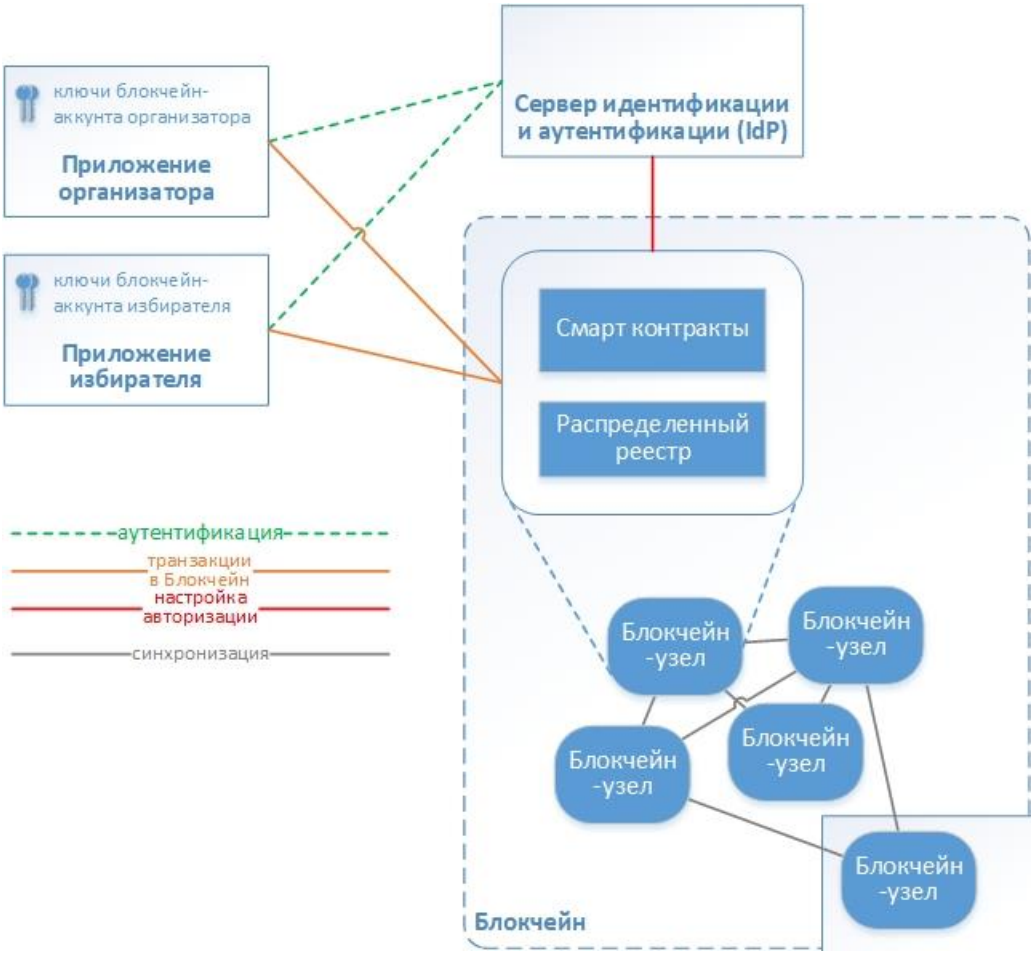

Рисунок 1. Структурная схема АС.

2.3 Характеристики компонент АС

2.3.1 Характеристики IdP

2.3.1.1 Функциональные:

IdP обеспечивает выполнение следующих функций:

- регистрацию и аутентификацию пользователей АС следующими способами:
  - посредством одноразовых паролей, отправляемых по SMS или на email;
  - посредством внешних провайдеров аутентификации (через протокол OAuth);
  - посредством уникального идентификатора, закодированного в машиночитаемом виде (в виде QR-кода);
- управление лицензиями для организаторов голосований:
  - активация лицензии, ограничивающей доступные варианты организации голосования и количество избирателей;
  - контроль срока истечения лицензии;
  - деактивация лицензии с истекшим сроком;
- создание смарт-контрактов с деанонимизированным списком избирателей для голосований по спискам, предоставленным организатором.

2.3.1.2 Характеристики пользовательского интерфейса

IdP-сервер предоставляет интерфейс в виде набора команд, вызываемых посредством протокола HTTP.

2.3.2 Характеристики смарт-контрактов

2.3.2.1 Функциональные характеристики

Смарт-контракты выполняют следующие функции:

- контроль лицензии организатора на создание голосований;
- авторизация избирателей для участия в голосованиях, в которых у них имеется активное избирательное право;
- прием и учет электронных бюллетеней, полученных от авторизованных избирателей;
- блокировка попытки сохранить электронные бюллетени, переданные неавторизованными избирателями;
- блокировка попыток избирателя повторно проголосовать после того как избиратель успешно реализовал свое избирательное право;
- контроль времени проведения голосования;
- автоматический подсчет голосов после завершения голосования;
- вывод результатов после окончания голосования для всех пользователей.

2.3.3 Характеристики Приложения организатора

2.3.3.1 Функциональные характеристики

Приложение организатора обеспечивает:

- интерфейс для аутентификации в АС;
- применение лицензии для получения расширенных возможностей;
- возможность связаться с разработчиками АС;
- генерирование параметров системы шифрования необходимых для зашифрования и расшифровывания заполненных избирателями электронных бюллетеней;
- настройку следующих параметров голосования посредством UI:
  - название голосования, основной вопрос голосования и комментарий к нему;
  - фоновое изображение;
  - варианты ответов, комментарии и изображения к ним;
  - метод голосования (за один вариант ответа, за несколько вариантов ответа, распределение баллов между вариантами);
  - даты начала и окончания голосования: возможность ручного запуска и остановки голосования, планирование отсроченного времени;
  - выбор способа аутентификации избирателей: по почте, уникальным кодам, по публичной ссылке;
  - загрузка структурированного файла с идентификаторами избирателей (email-адресами, номерами телефонов и пр.);
  - имя организатора голосования;
- возможность предварительного просмотра вида голосования на устройствах избирателей до запуска голосования (до создания смарт-контракта голосования в блокчейн);
- сохранение и удаление черновиков с настройками голосований;
- запуск голосования (создание смарт-контракта голосования в блокчейн);

- вывод информации о ходе голосования после запуска (явка);
- скачивание и распечатка закодированных в машиночитаемом виде (в виде QR-кодов) уникальных идентификаторов;
- остановка запущенного голосования, в параметрах которого было выставлено ручное завершение голосования;
- просмотр и печать результатов завершённого голосования.

2.3.3.2 Требования к поддерживаемым платформам

Приложение организатора является web-приложением и работает в среде браузера.

Поддерживаемые браузеры:

- MS Internet Explorer версии 11 и выше;
- Google Chrome версии 76 и выше;
- Mozilla Firefox версии 68 и выше;
- Apple Safari версии 6.0 и выше.

2.3.3.3 Требования к графическому интерфейсу

Поддерживаются разрешения экрана от 1024x768.

2.3.4 Характеристики приложения избирателя

2.3.4.1 Функциональные характеристики

Приложение избирателя обеспечивает:

- интерфейс для аутентификации в АС;
- просмотр информации обо всех голосованиях, к которым избиратель имеет доступ как голосующий;
- обозначение своего выбора среди вариантов ответа в соответствии с методом голосования, выбранным организатором голосования;
- зашифрование заполненного бюллетеня с использованием открытого ключа организатора голосования;
- отслеживание факта учета голоса в ходе голосования;
- проверку корректности учета голоса после завершения голосования;
- загрузку из Блокчейна и отображение результатов автоматического подсчета голосов после завершения голосования.

2.3.4.2 Требования к поддерживаемым платформам

Приложение избирателя является web-приложением и работает в среде браузера.

Поддерживаемые браузеры:

- MS Internet Explorer версии 11 и выше;
- Google Chrome версии 76 и выше;
- Mozilla Firefox версии 68 и выше;
- Apple Safari версии 6.0 и выше.

2.3.4.3 Требования к графическому интерфейсу

Интерфейс приложения:

- корректно отображается на экранах с диагональю 4,7” и выше;

- поддерживает автоматическое переключение между портерной и альбомной ориентациями экрана;
- предусматривает ввод чисел как с экранной клавиатуры, так и прокруткой/выбором;
- поддерживает настройку размера шрифта.

2.4 Нефункциональные характеристики АС в целом

2.4.1 Доступность

АС предусматривает возможность обеспечения показателя доступности 98%.

2.4.2 Надежность

АС обладает транзакционной целостностью – в случае аварии или некорректного завершения любой операции автоматизированная система остается в состоянии, предшествующим началу выполнения операции и предоставляет возможность повторить операцию с теми же данными.

2.4.3 Возможности и простота локализации (Localizability)

Пользовательские интерфейсы АС поддерживают возможность работы на русском и английском языках.