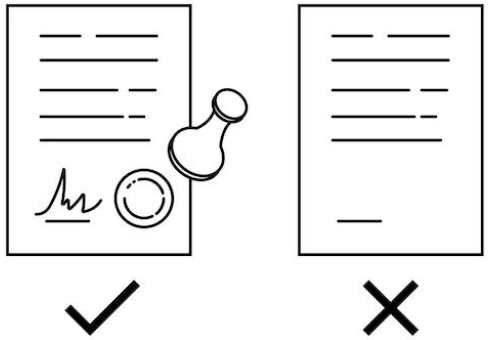
Метод создания уникальных сертификатов, подтверждающих окончание учебного заведения, на основе технологии невзаимозаменяемых токенов

Студент: Соколов Ефим Маркович
Научный руководитель: к.ф.-м.н., доцент Вишневская Т.И.

Москва
2022г.

Актуальность



Решаемые проблемы:

- предоставление оригинальных документов об образовании при устройстве на работу;
- надобность проверки подлинности документов об образовании;
- хранение бумажных документов.

Цель работы и постановка задачи

Цель работы

Разработка и программная реализация метода создания уникальных сертификатов, подтверждающих окончание учебного заведения, с помощью технологии невзаимозаменяемых токенов.

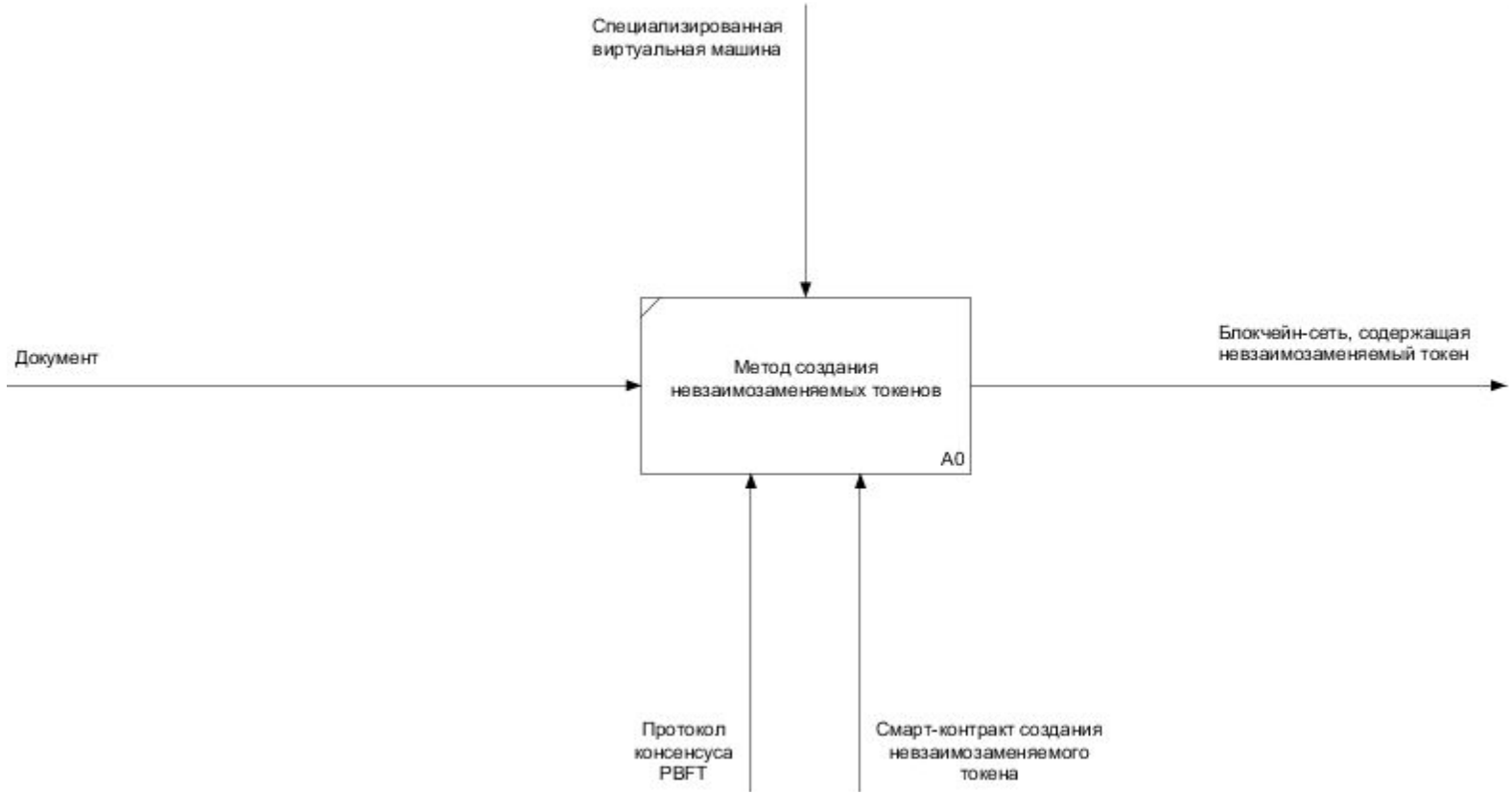
Задачи

- проанализировать существующие способы выдачи сертификатов об окончании учебного заведения;
- разработать блокчейн-сети, в которой реализован метод выдачи уникальных сертификатов;
- программно реализовать разработанный метод;
- исследовать зависимость времени финализации транзакции от количества участников сети, и произвести сравнение с аналогами.

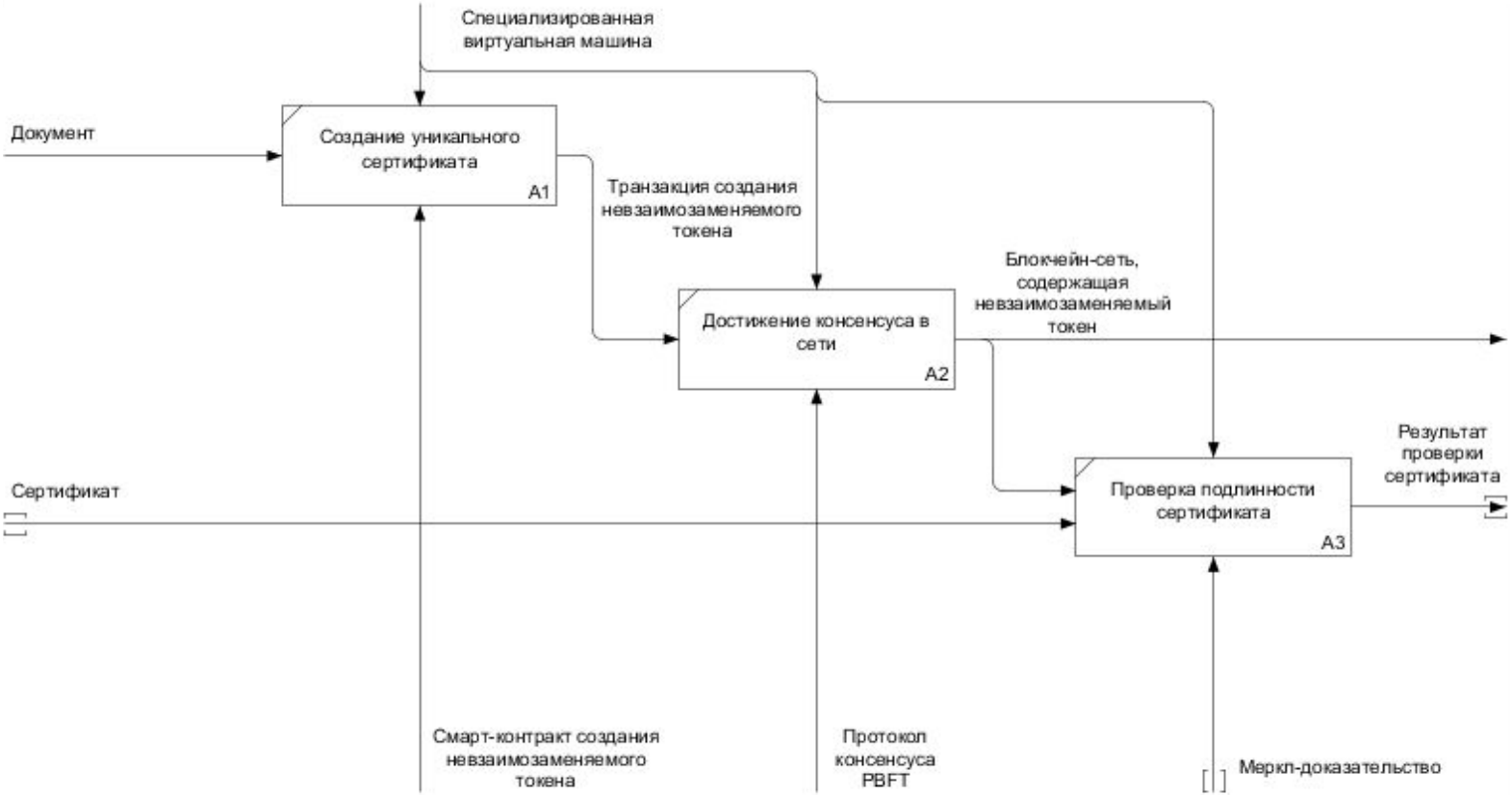
Существующие методы выдачи сертификатов об образовании

Критерий / Реализация	**Защита от утраты**	**Защита от износа**	**Защита от подделывания**	**Проверка подлинности**
Документы об окончании вуза РФ	-	-	+	-
Сертификаты Coursera	+	+	-	-

Постановка задачи



Предложенный метод



Виртуальные машины

Характеристика	Спец. ВМ	Стандарт. ВМ	Нативный код
Безопасность	+	+-	-
Неограниченность ресурсов	-	+-	+
Учет затраченных ресурсов	+	+	-

Способы обновления кода контрактов

Характеристика	Смарт-контракты	Нативный код
Безопасность	-	-
Неограниченность ресурсов	-	+
Гибкость	+	-

Протоколы консенсуса

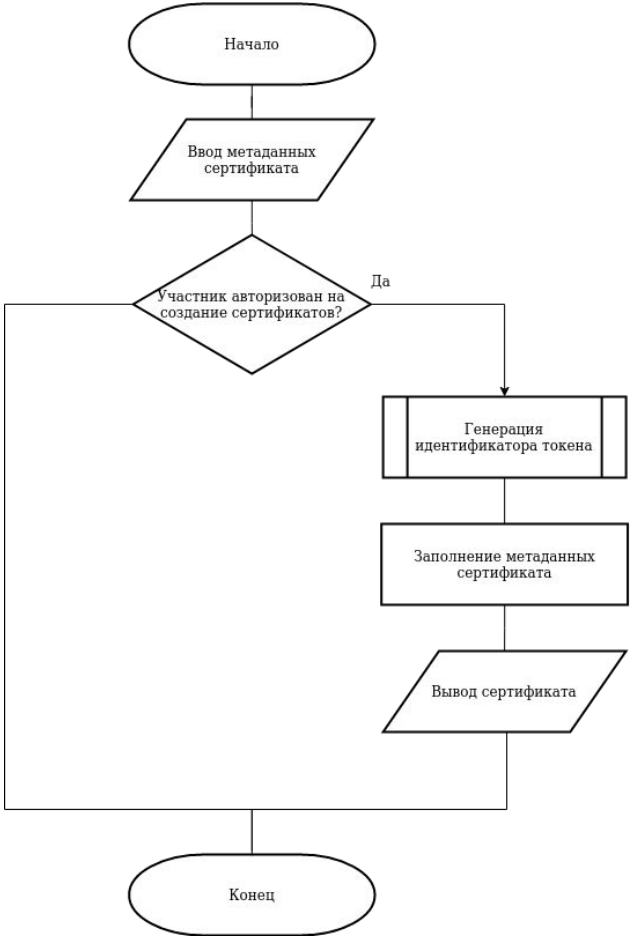
Характеристика	**Доказательство выполнения работы (PoW)**	**Доказательство доли владения (PoS)**	**Делегирование доказательств долей владения (DPoS)**	**Протокол “PBFT”**	**Протокол “Tendermint”**
Идентификация узла	нет	нет	нет	да	да (и удержания залога)
Энергоэффективность	нет	частичная	частичная	да	да
Допустимое число атакующих	<25% вычислительной мощности	<51% доли	<51% валидаторов	<33.33% валидаторов	<33.33% валидаторов

Алгоритм создания уникального сертификата

Пусть *ID* – идентификатор сертификата

$$ID_n = ID_{n-1} + 1$$

$$ID_0 = 1$$



Алгоритм проверки подлинности сертификата

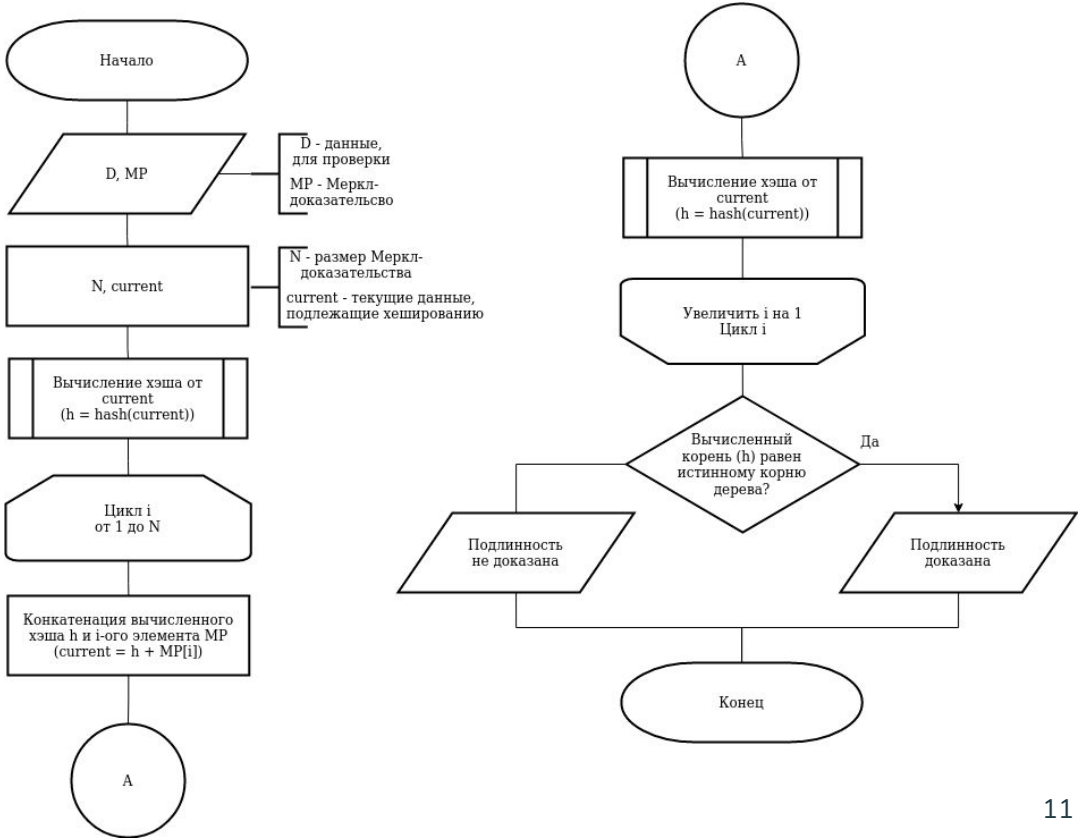
Пусть L – блок, который необходимо проверить

Тогда доказательство вхождения:

$root = hash_K$:

$$hash_k = \begin{cases} hash(L), \text{ если } k = 1 \\ hash(hash_{k-1} + auth_{k-1}), \text{ если } 2 \le k \le K \end{cases}$$, где

- K - глубина дерева Меркла;
- $root$ – корень дерева Меркла
- $auth = \{auth_1, \ldots, auth_{K-1}\}$ – Меркл-доказательство



Средства программной реализации

Языки программирования:

- Rust:
  - в Rust отсутствует «сборщик мусора»;
  - большое количество библиотек для разработки блокчейна.
- Solidity:
  - спроектирован и создан как язык для написания смарт-контрактов;
  - исполняется EVM, абстрагируясь от реализации узлов сети.

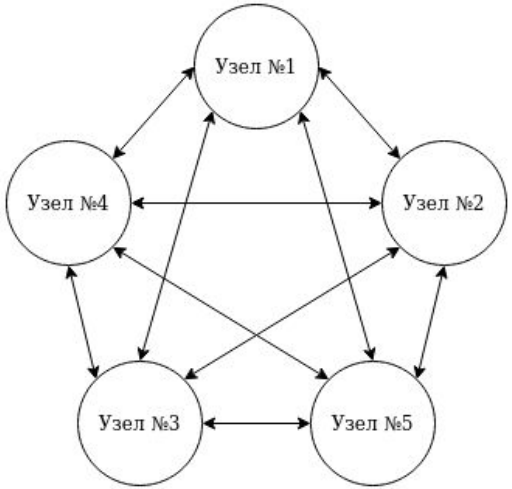
Среда разработки:

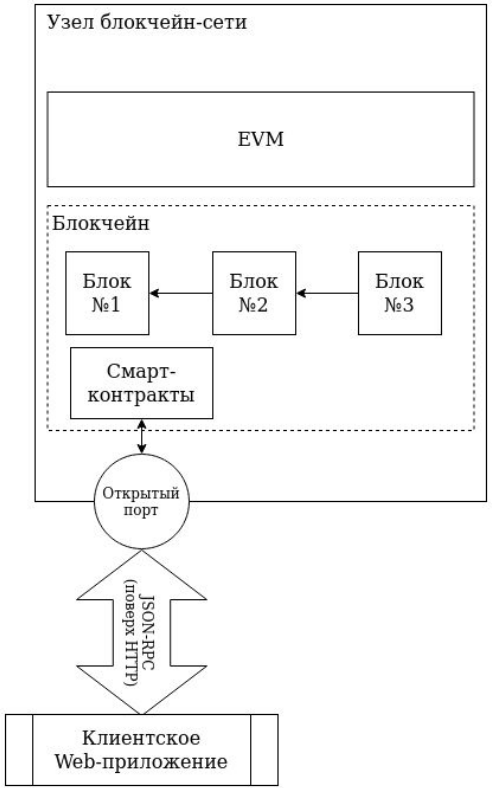
- VS Code:
  - свободно распространяется;
  - содержит плагины, облегчающие процесс написание кода.

Библиотеки:

- Substrate:
  - позволяет создавать гибкие и настраиваемые блокчейны;
  - поддерживается активным сообществом разработчиков.

Структура разработанного ПО

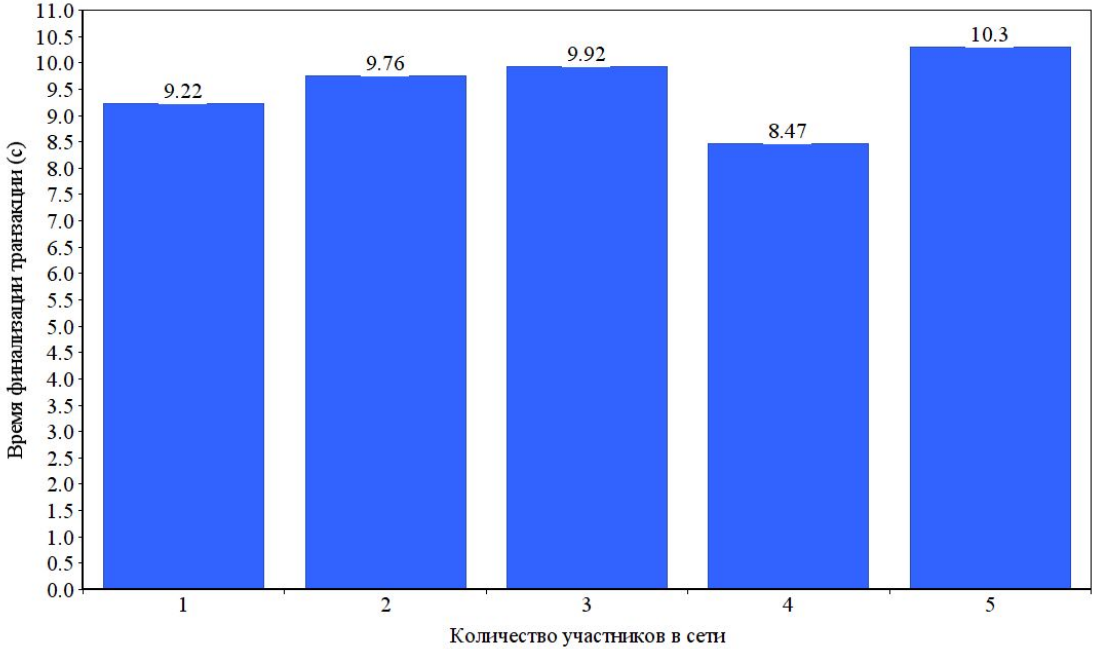




Исследование зависимости времени финализации транзакции от количества участников в сети

Транзакция: ***создание смарт-контракта учебного заведения***

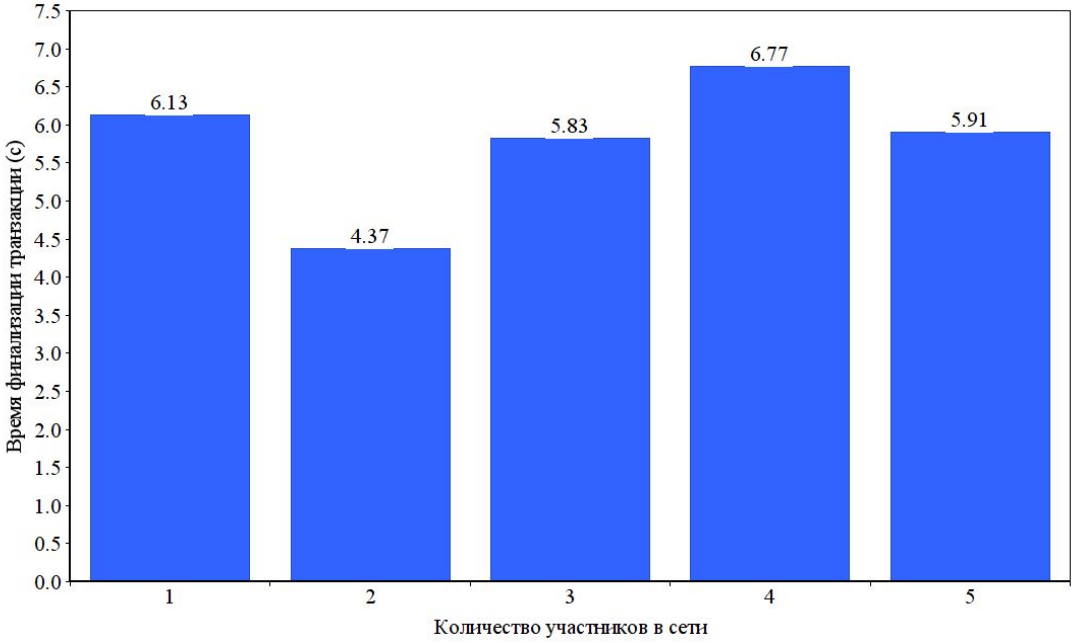
- Среднее время выполнения: 9.53 секунд;
- Колебания в пределах в 12%.



Исследование зависимости времени финализации транзакции от количества участников в сети

Транзакция: ***создание уникального сертификата***

- Среднее время выполнения: 5.80 секунд;
- Колебания в пределах в 25%.



Сравнение с существующими аналогами

Критерий / Реализация	**Защита от утраты**	**Защита от износа**	**Защита от подделывания**	**Проверка подлинности**
Документы об окончании вуза РФ	-	-	+	-
Сертификаты Coursera	+	+	-	-
Предложенный метод	+	+	+	+

Достоинства и недостатки

Достоинства:

- защита от износа и подделывания выданных документов об образовании;
- возможность предоставить электронное подтверждение подлинности документа, не оформляя бюрократических запросов;
- неограниченное количество участников сети.

Недостатки:

- в случае если документ, хранящийся по ссылке в сертификате, скомпрометирован, тогда соответствующий сертификат тоже будет ложный;
- большие вычислительные мощности, требуемые от машины.

Заключение

Была достигнута цель работы:

Был разработан и программно реализован метод создания уникальных сертификатов, подтверждающих окончание учебного заведения, на основе технологии невзаимозаменяемых токенов.

Были выполнены поставленные задачи:

- проанализированы существующие способы выдачи сертификатов об окончании учебного заведения;
- разработана блокчейн-сеть, в которой реализован метод выдачи уникальных сертификатов;
- программно реализован разработанный метод;
- исследована зависимость времени финализации транзакции от количества участников сети, а также произведено сравнение с аналогами.

Дальнейшее развитие проекта

1. Переписывание кода смарт-контрактов на Rust;
2. Произвести внешний аудит разработанных смарт-контрактов;
3. Развить блокчейн-сеть до парачейна Polkadot.