

# Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича

Кафедра сетей связи и передачи данных

## Разработка публичного децентрализованного реестра с использованием технологии blockchain

Выполнил:

Научный руководитель:

студент гр. ИКВТ-62 Гарифуллин В.Ф.

к.т.н., доцент Владимиров С.С.

Санкт-Петербург 2020

СПб ГУТ)))

# Цель работы

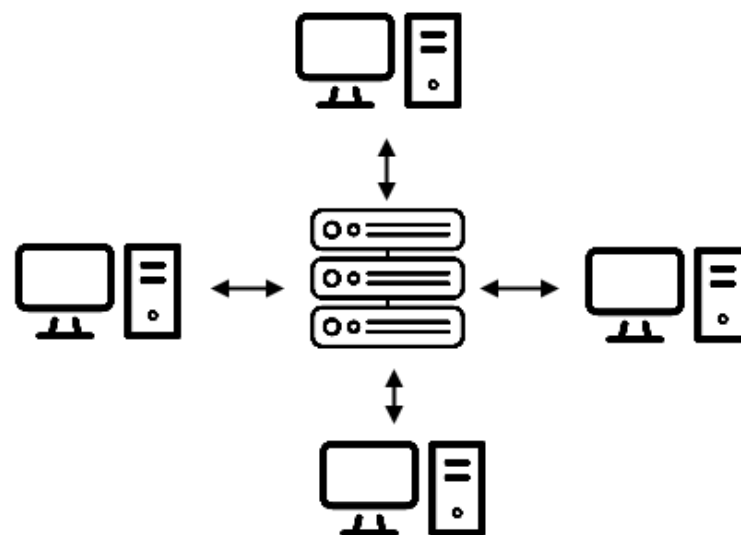
- Проектирование и разработка кроссплатформенного программного обеспечения для организации публичного децентрализованного реестра с использованием технологии blockchain.

# Задачи работы

1. Анализ преимуществ и недостатков существующих электронных реестров.
2. Анализ существующих решений для организации публичных децентрализованных реестров.
3. Рассмотрение принципов организации распределённых реестров на основе технологии blockchain.
4. Сравнительный анализ и выбор технологий для использования в реестре.
5. Разработка программного обеспечения для организации реестра и графического интерфейса для удобной работы с ним.

# Электронные реестры

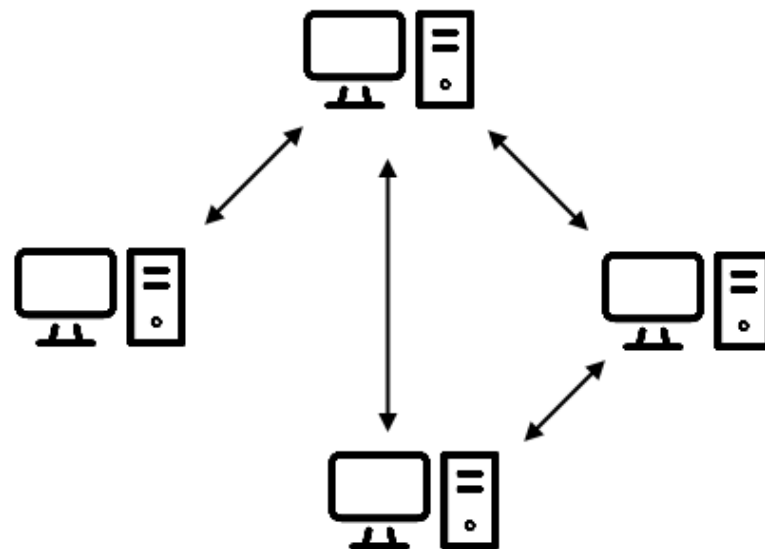
- Преимущества:
  - Экономия времени
  - Экономия средств
- Недостатки:
  - Ненадёжность
  - Непрозрачность



*Клиент-серверная архитектура*

# Распределённые системы

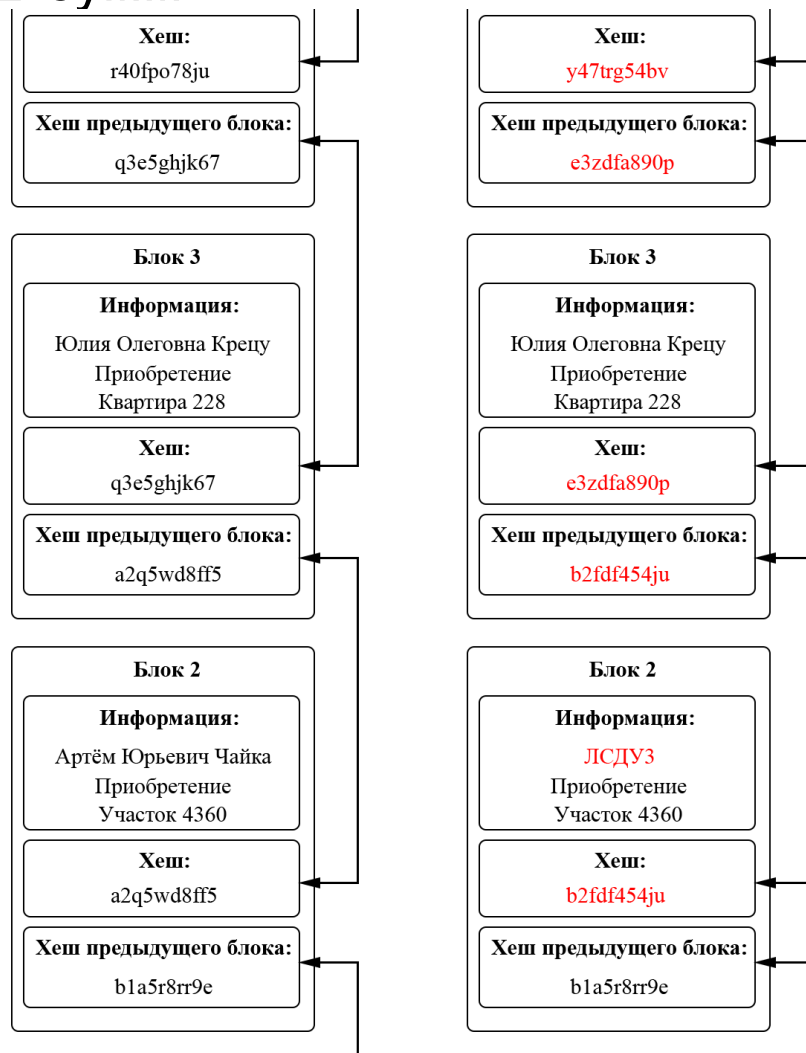
- Существующие решения для распределённого обмена данными:
  - Gnutella
  - BitTorrent
  - IPFS
- Отсутствующий функционал:
  - Ограничение на добавление информации только уполномоченными лицами
  - Обеспечение достоверной последовательности записей



*Децентрализованная сеть*

# Технология Blockchain

- Blockchain – цепочка блоков, которые связаны между собой с помощью хеш-сумм.



# Выбор хеш-функции

Параметр	SHA-256	SHA-384	SHA-512
Устойчивость к коллизиям	Да	Да	Да
Время хеширования миллиона строк одинаковой длины, с	9,88	36,14	35,98
Размер хеш-суммы, бит	64	96	128

# Цифровая подпись (1)

- Криптографические алгоритмы с открытым ключом:
  - RSA
  - DSA
  - Алгоритмы, основанные на эллиптических кривых

Длина открытого ключа в битах при сопоставимой криптостойкости

Эллиптическая криптография	RSA
163	1024
233	2240
283	3072
409	7680
571	15360

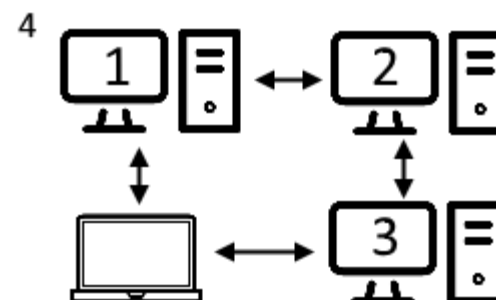
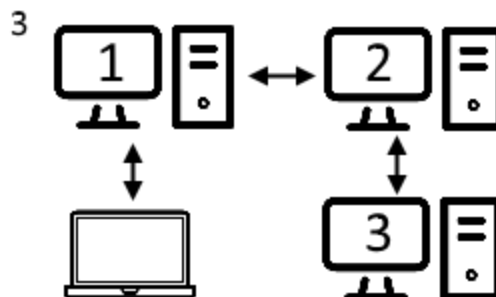
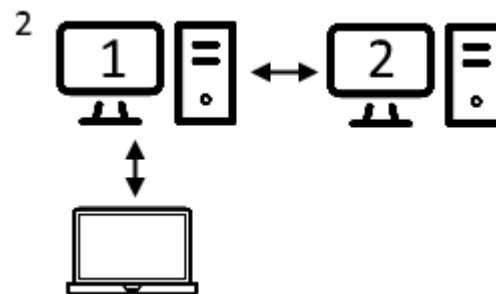
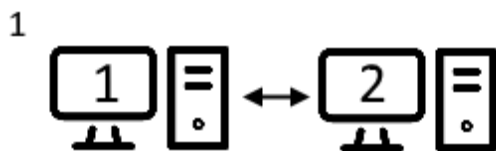


## Цифровая подпись (2)

- Ed25519 – схема подписи EdDSA, основанная на эллиптической кривой Curve25519 и использующая SHA-512.
- Преимущества:
  - Эллиптическая кривая Curve25519 считается полностью безопасной.
  - Не используются ветвления и потенциально опасные операции с памятью.
  - В процессе подписи не используется генератор случайных чисел.
  - Используемая длина открытого ключа в 256 бит обеспечивает криптостойкость, сопоставимую с RSA с длиной ключа в 3000 бит (разница в 12 раз).

# Структура сети

- Два типа узлов: обычные узлы хранения и мастер-узлы.
- Обычные узлы обращаются к мастер-узлам для получения новых блоков, а также для получения информации о новых мастер-узлах.
- Процесс добавления нового мастер-узла:



# Транзакции

- Транзакция – данные, добавляемые пользователем в сеть, и служебная информация.
- Транзакции нужны для предотвращения коллизий.
- Блоки состоят из транзакций.
- Ещё не занесённая в блок транзакция называется неподтверждённой.
- Данные, хранящиеся в транзакции:
  - Временная метка
  - Тип транзакции
  - Передаваемая информация
  - Публичный ключ отправителя
  - Хеш транзакции
  - Цифровая подпись отправителя

# Алгоритм консенсуса (1)

- Алгоритм консенсуса нужен для предотвращения коллизий.
- Алгоритм консенсуса позволяет удостовериться, что участник сети, подписавший новый блок, сделал это правомерно.
- Алгоритм доказательства полномочий (Proof of Authority). подразумевает наличие ограниченного числа валидаторов.
- Валидаторы – мастер-узлы, которые имеют право подписывать блоки.

## Алгоритм консенсуса (2)

- Используется следующий алгоритм выбора валидатора для подписи блоков:
  1. Фиксируем текущую временную метку
  2. Делим на время валидации одного валидатора
  3. Округляем до ближайшего целого
  4. Берём результат пункта 3 по модулю числа валидаторов
  5. Получившийся результат – номер валидатора, который может подписывать блоки в данный момент

Временная метка, мс	Время GMT+3	Валидатор
1590266468000	20:41:08	1
1590266469000	20:41:09	2
1590266470000	20:41:10	2
1590266471000	20:41:11	0
1590266472000	20:41:12	0
1590266473000	20:41:13	1

# Генезис-блок

- Генезис-блок – самый первый блок в цепочке.
- Данные, хранящиеся в генезис-блоке:
  - Время
  - Хеш генезис-блока
  - Генезис-транзакция:
    - Тип транзакции (genesis)
    - Открытые ключи валидаторов
    - Открытые ключи отправителей (людей, имеющих право добавлять записи в реестр)

# Структура блоков

- Блоки хранят следующие данные:
  - Время подписи блока
  - Транзакции (неограниченное количество)
  - Публичный ключ валидатора
  - Хеш предыдущего блока
  - Хеш данного блока
  - Цифровая подпись валидатора

# Добавление новой информации

1. Узел добавляет в транзакцию данные, подписывает её и отправляет мастер-узлам.
2. Мастер-узлы проверяют транзакцию и заносят в пул неподтверждённых транзакций.
3. Валидатор, который согласно алгоритму консенсуса в данный момент может подписывать блоки, проверяет транзакции, которые находятся в пуле неподтверждённых транзакций, формирует из них блок, подписывает его и заносит в цепочку.
4. Все остальные узлы во время синхронизации получают этот блок, проверяют его и занесут его в цепочку.



# Разрабатываемые приложения

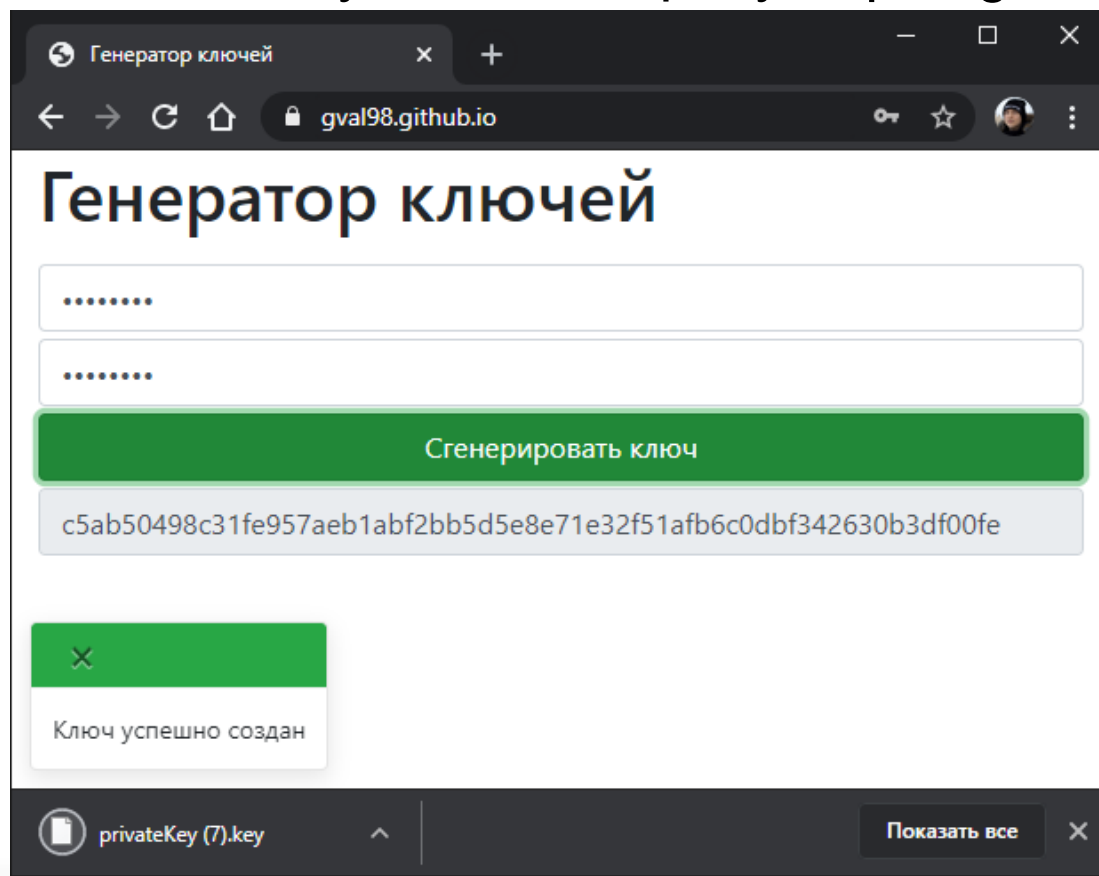
Интерфейс	Консольный	Графический	Веб
Поддерживаемые операционные системы	Windows, Linux	Windows, Linux	Все ОС с наличием браузера
Хранение всей цепочки блоков	Да	Да	Нет
Проверка блоков и транзакций	Да	Да	Нет
Взаимодействие с сетью	Со всеми мастер-узлами	Со всеми мастер-узлами	С одним мастер-узлом
Запуск обычного узла	Нет	Да	Нет
Запуск мастер-узла	Да	Да	Нет
Запуск узла валидации	Да	Нет	Нет
Запуск веб-интерфейса	Да	Нет	Нет
Отправка транзакций	Нет	Да	Да
Удобный просмотр транзакций	Нет	Да	Да

# Средства разработки

- Критерии выбора средств разработки:
  - Поддержка асинхронности
  - Кроссплатформенный графический интерфейс
- Для разработки было решено использовать следующие средства:
  - Язык программирования JavaScript
  - Среда исполнения Node.js
  - Фреймворк Electron для создания графического приложения
  - Фреймворк Bootstrap для создания интерфейса графического приложения и веб-версии

# Хранение и создание ключей

- Все закрытые ключи хранятся в зашифрованном с помощью алгоритма симметричного шифрования AES виде.
- Для создания ключей было разработано консольное и веб-приложение, доступное по адресу <https://gval98.github.io>



# Графическое приложение (1)

Blockchain Registry

Кадастровый номер

ИНН

ИНН продавца

ИНН покупателя

Минимальная сумма

Максимальная сумма

Начальная дата

Конечная дата

Q

Новые транзакции +

28.05.2020, 19:25:46

Кадастровый номер: 41:13:116024:805  
ИНН продавца: 7708648569  
ИНН покупателя: 7709225144  
Сумма: 3158586 Р

475727ef9e6ec139bd0e5b5022afa0eecacabbbcacd586aa0fe839b38b201027

28.05.2020, 19:25:50

Кадастровый номер: 45:10:109657:800  
ИНН продавца: 7709165892  
ИНН покупателя: 7708576782  
Сумма: 7677478 Р

475727ef9e6ec139bd0e5b5022afa0eecacabbbcacd586aa0fe839b38b201027

Последние транзакции >

28.05.2020, 19:25:45

Кадастровый номер: 42:13:107860:813  
ИНН продавца: 7709130918  
ИНН покупателя: 7707162901  
Сумма: 6432806 Р

475727ef9e6ec139bd0e5b5022afa0eecacabbbcacd586aa0fe839b38b201027

28.05.2020, 19:25:42

Кадастровый номер: 46:12:100790:803  
ИНН продавца: 7707355188  
ИНН покупателя: 7708083403  
Сумма: 7847882 Р

475727ef9e6ec139bd0e5b5022afa0eecacabbbcacd586aa0fe839b38b201027

28.05.2020, 19:25:42

Кадастровый номер: 42:12:116231:807  
ИНН продавца: 7707086649  
ИНН покупателя: 7709075123  
Сумма: 6971409 Р

475727ef9e6ec139bd0e5b5022afa0eecacabbbcacd586aa0fe839b38b201027

28.05.2020, 19:25:42

Кадастровый номер: 43:13:107288:806  
ИНН продавца: 7709254859  
ИНН покупателя: 7709212741  
Сумма: 4055620 Р

475727ef9e6ec139bd0e5b5022afa0eecacabbbcacd586aa0fe839b38b201027

Доступные узлы ⚙

Адрес	Высота
127.0.0.1:1111	213
127.0.0.1:3333	213

Windows taskbar with icons for Google, blockchain-handler, Blockchain Registry, and Word document.

19:25

28.05.2020

# Графическое приложение (2)

Blockchain Registry

Кадастровый номер | ИНН | ИНН продавца | ИНН покупателя | Минимальная сумма | Максимальная сумма | Начальная дата | Конечная дата

Новые транзакции + | Последние транзакции > | Доступные узлы ⚙️

30.05.2020, 16:13:30

Кадастровый номер: 40:101140101:841  
ИНН продавца: 7424559659  
ИНН покупателя: 7143584666  
Сумма: 4500000 Р

47572

Кадастровый номер: 42:13:145233:841  
ИНН продавца: 72586543218  
ИНН покупателя: 79453518564  
Сумма: 6500000 Р

1e6c708a24317ec06bf92cf4bc100e0532d78a6e6d100e6116fdc09404363b40

30.05.2020, 00:02:02

Кадастровый номер: 42:13:145233:841  
ИНН продавца: 72586543218  
ИНН покупателя: 79453518564  
Сумма: 6500000 Р

1e6c708a24317ec06bf92cf4bc100e0532d78a6e6d100e6116fdc09404363b40

Новая транзакция

Выберите ключ отправителя Browse

Введите пароль от ключа

Кадастровый номер

ИНН продавца

ИНН покупателя

Сумма в рублях

Отправить

Адрес	Высота
185.244.172.208:1111	18
blockchain-registry.ru:443	18
139.28.222.91:1111	18

Диплом | ВКР\_Гарифуллин\_... | udot\_present.pptx ... | Презентация\_bloc... | ВКР\_Гарифуллин\_... | Blockchain Registry

22:07  
06.06.2020

# Веб-приложение (1)

Blockchain Registry

blockchain-registry.ru/web

Кадастровый номер

ИНН

ИНН продавца

ИНН покупателя

Минимальная сумма

Максимальная сумма

Начальная дата

Конечная дата

🔍

Новые транзакции +

30.05.2020, 16:13:26

Кадастровый номер: 40:101140101:841

ИНН продавца: 7424559659

ИНН покупателя: 7143584666

Сумма: 4500000 P

475727ef9e6ec139bd0e5b5022afa0eecacabbcbacd586aa0fe839b38b201027

Последние транзакции >

30.05.2020, 16:12:52

Кадастровый номер: 40:10:140101:840

ИНН продавца: 7431259865

ИНН покупателя: 7135484584

Сумма: 3500000 P

475727ef9e6ec139bd0e5b5022afa0eecacabbcbacd586aa0fe839b38b201027

30.05.2020, 01:44:44

Кадастровый номер: 41:11:141131:844

ИНН продавца: 7546253102

ИНН покупателя: 7955456325

Сумма: 3900000 P

1e6c708a24317ec06bf92cf4bc100e0532d78a6e6d100e6116fdc09404363b40

30.05.2020, 00:02:02

Кадастровый номер: 42:13:145233:841

ИНН продавца: 72586543218

ИНН покупателя: 79453518564

Сумма: 6500000 P

1e6c708a24317ec06bf92cf4bc100e0532d78a6e6d100e6116fdc09404363b40

29.05.2020, 23:35:40

Кадастровый номер: 40:10:105101:840

ИНН продавца: 7415687953

ИНН покупателя: 7456858545

Сумма: 5500000 P

Транзакция успешно отправлена

Blockchain Registry...

Диплом.docx - Wo...

nodes.json - blockc...

16:13 30.05.2020

# Веб-приложение (2)

16:37 📶 🔋 95

🏠 [blockchain-registry.ru/web](https://blockchain-registry.ru/web) 1 ⋮

Кадастровый номер

ИНН

ИНН продавца

ИНН покупателя

Минимальная сумма

Максимальная сумма

Начальная дата

Конечная дата

🔍

⏪ Последние транзакции ⏩

30.05.2020, 16:13:30

**Кадастровый номер:** 40:101140101:841  
**ИНН продавца:** 7424559659  
**ИНН покупателя:** 7143584666  
**Сумма:** 4500000 ₽

475727ef9e6ec139bd0e5b5022afa0eecacabbbcacd586  
aa0fe839b38b201027

Веб-приложение для уже запущенной  
сети доступно по адресу:  
<https://blockchain-registry.ru/web>

# Заключение

- В ходе выполнения работы были решены следующие задачи:
  - Рассмотрены существующие решения для децентрализованного обмена данными, в том числе с использованием технологии blockchain.
  - Произведён сравнительный анализ технологий, используемых в blockchain проектах и децентрализованных сетях.
  - Разработано кроссплатформенное программное обеспечение для организации публичных децентрализованных реестров и графический интерфейс для удобной работы с ним.
- Разработанные приложения могут быть успешно применены для создания публичных реестров на базе технологии Blockchain с целью их децентрализации, увеличения надежности и прозрачности.



Кафедра сетей связи и передачи данных

**Спасибо за внимание!**

Разработка публичного децентрализованного реестра с использованием технологии blockchain

Выполнил:	студент гр. ИКВТ-62 Гарифуллин В.Ф.
Научный руководитель:	к.т.н., доцент Владимиров С.С.

Санкт-Петербург 2020