Санкт-Петербургский государственный университет
Программная инженерия

Реализация протокола электронного голосования на блокчейне Hyperledger Fabric

Автор: С. А. Скаредов, 16.Б11-мм
Научный руководитель: доцент кафедры СП, к.ф.-м.н. К. Ю. Романовский
Консультанты: старший преподаватель кафедры СП Я. А. Кириленко
ведущий разработчик «DSX Technologies Russia» Ф. П. Долголев
Рецензент: технический директор «DSX Technologies Russia», к.ф.-м.н. А. Н. Иванов

Санкт-Петербург, 2020

Электронное голосование

- Требования
  - Надёжность
  - Приватность
  - Проверяемость
- Виды
  - Традиционное
  - Акционерное
- Примеры
  - Голосование на блокчейне в России, Эстонии, Турции, Америке
  - Национальный расчётный депозитарий
    - Годовое общее собрание акционеров Московской биржи
    - Более 84% проголосовавших электронно (8-27.04.2020)

E-voting

- DSX Technologies и Accenture
- Система акционерного голосования
- Анонимизация волеизъявления участника
- Возможность проверки честного учёта голосов
- Патенты
  - US10,388,097: Blockchain-based cryptologic ballot verification
  - US10,445,965: Blockchain-based cryptologic ballot organization

Application-based подход

Chaincode-based подход

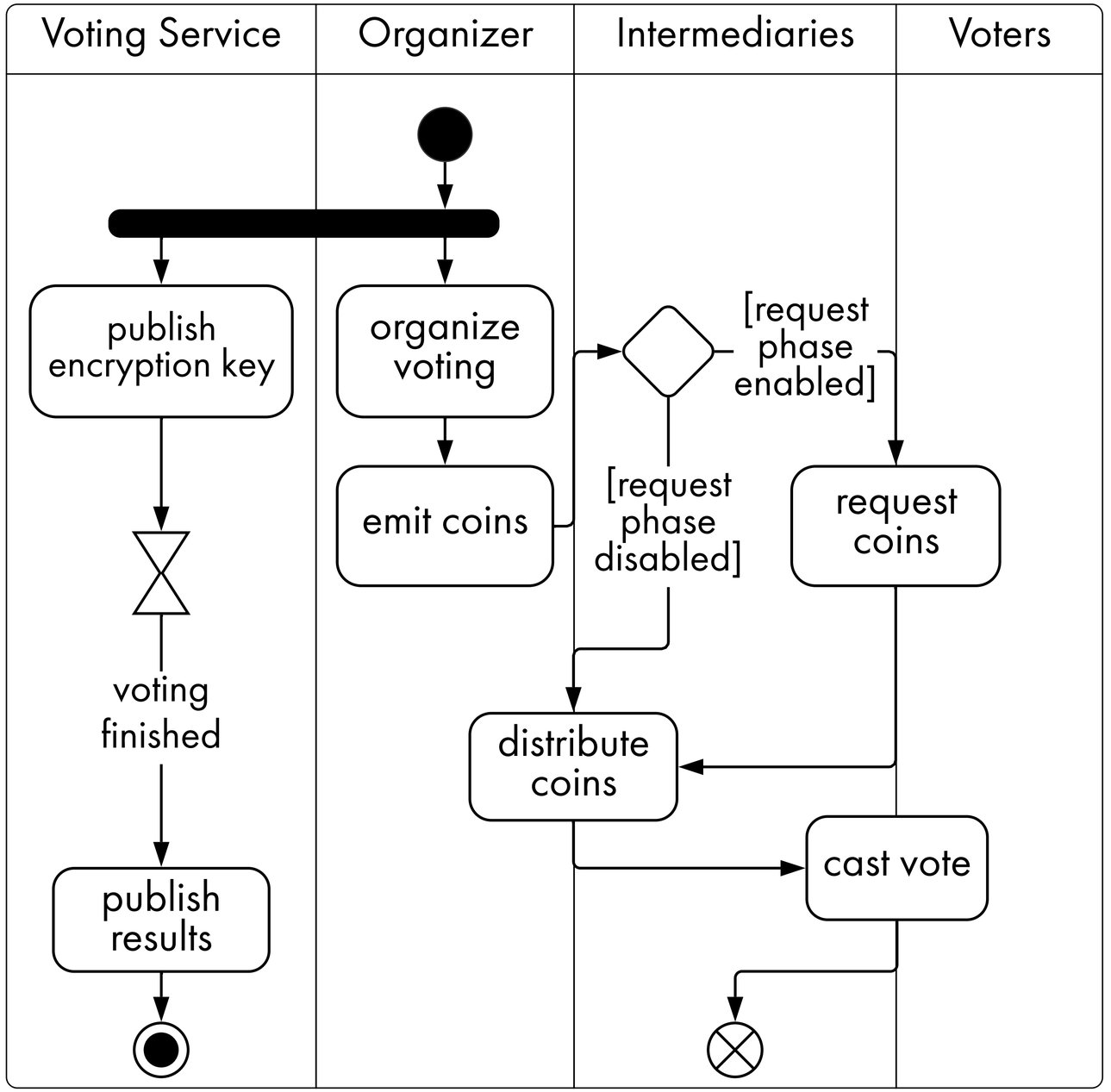
Цель: Реализация протокола тайного электронного акционерного голосования на блокчейне Hyperledger Fabric

Задачи:

- ❑ Обзор предметной области
  - ❑ Протокол E-voting
  - ❑ Hyperledger Fabric
- ❑ Проектирование архитектуры системы
  - ❑ Анализ существующего решения
  - ❑ Разработка нового подхода
  - ❑ Сравнение подходов
- ❑ Реализация нового подхода
  - ❑ Реализация системы смарт-контрактов
  - ❑ Рефакторинг off-chain приложения
- ❑ Тестирование системы

Протокол

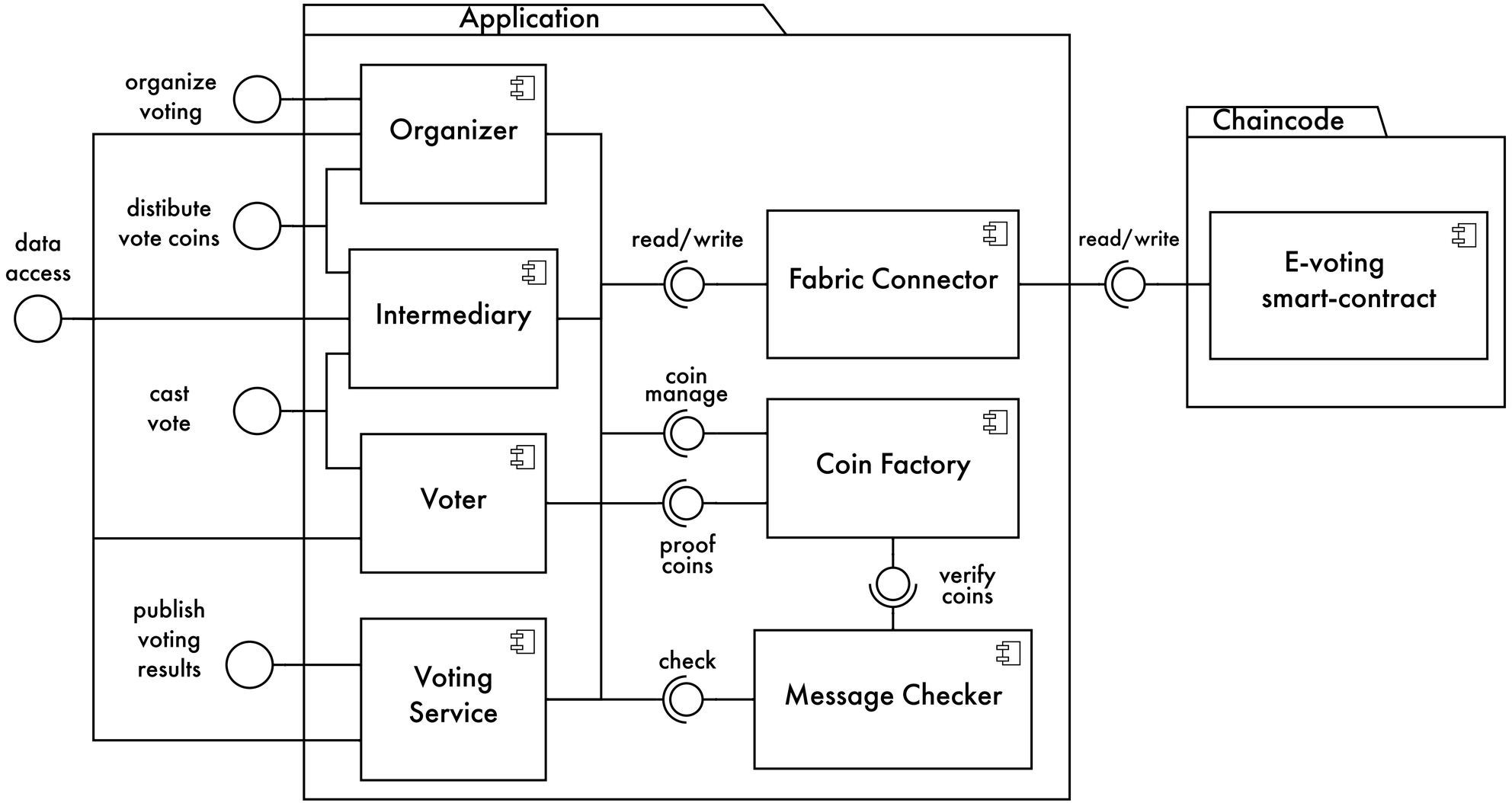
- Монеты
  - Аддитивно гомоморфное шифрование
    - $E(x + y) = E(x) + E(y)$
  - Криптографическое доказательство неотрицательности
    - $E(10) = E(15) + E(-5)$
- Процесс
  - Инициализация голосования
  - Распределение монет
  - Голосование
  - Подсчёт и публикация результатов



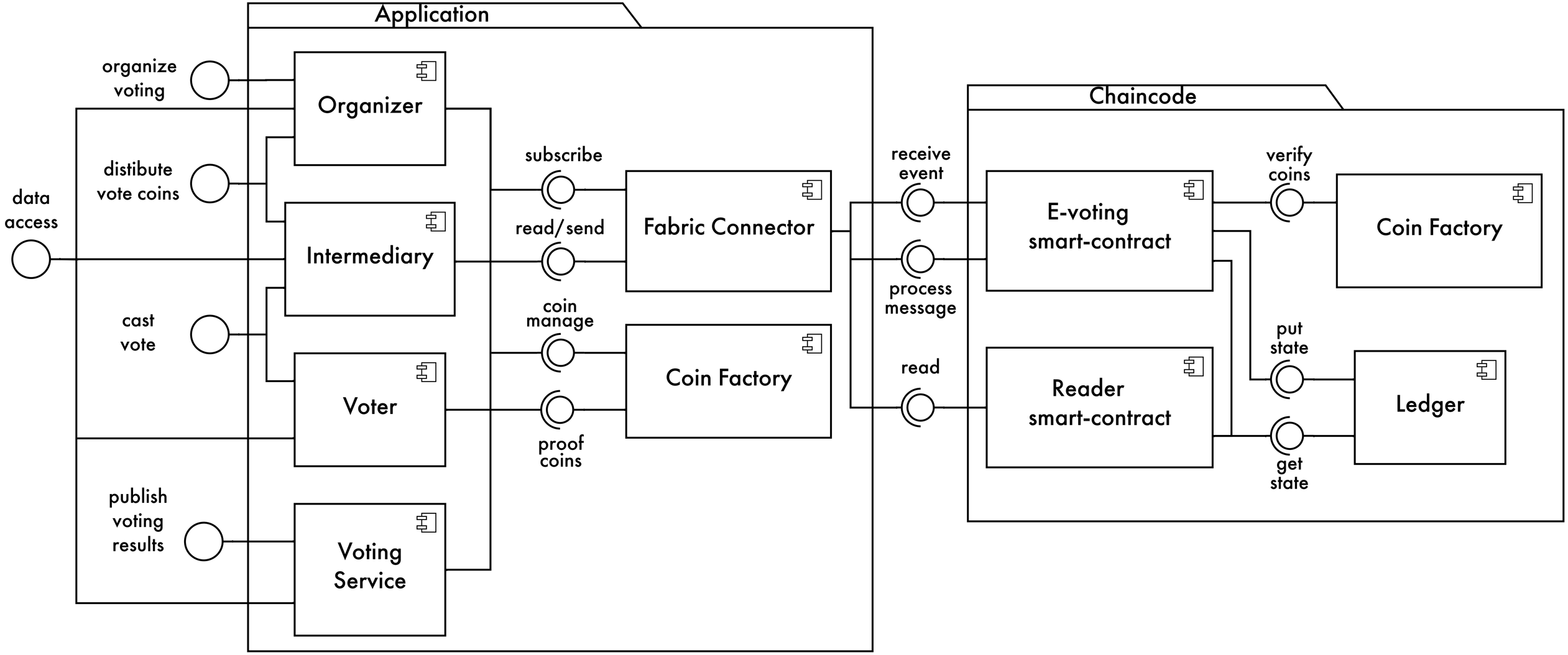
Hyperledger Fabric

- Open-source блокчейн-платформа
  - Linux Foundation
- Корпоративное применение
  - Идентификация и авторизация пользователей
  - Приватные распределённые реестры
- База данных «ключ-значение»
- Поддержка смарт-контрактов
  - Go, Java, JavaScript
- Инструменты для off-chain приложений
  - Go-, Java-, JavaScript-SDKs

Application-based



Chaincode-based



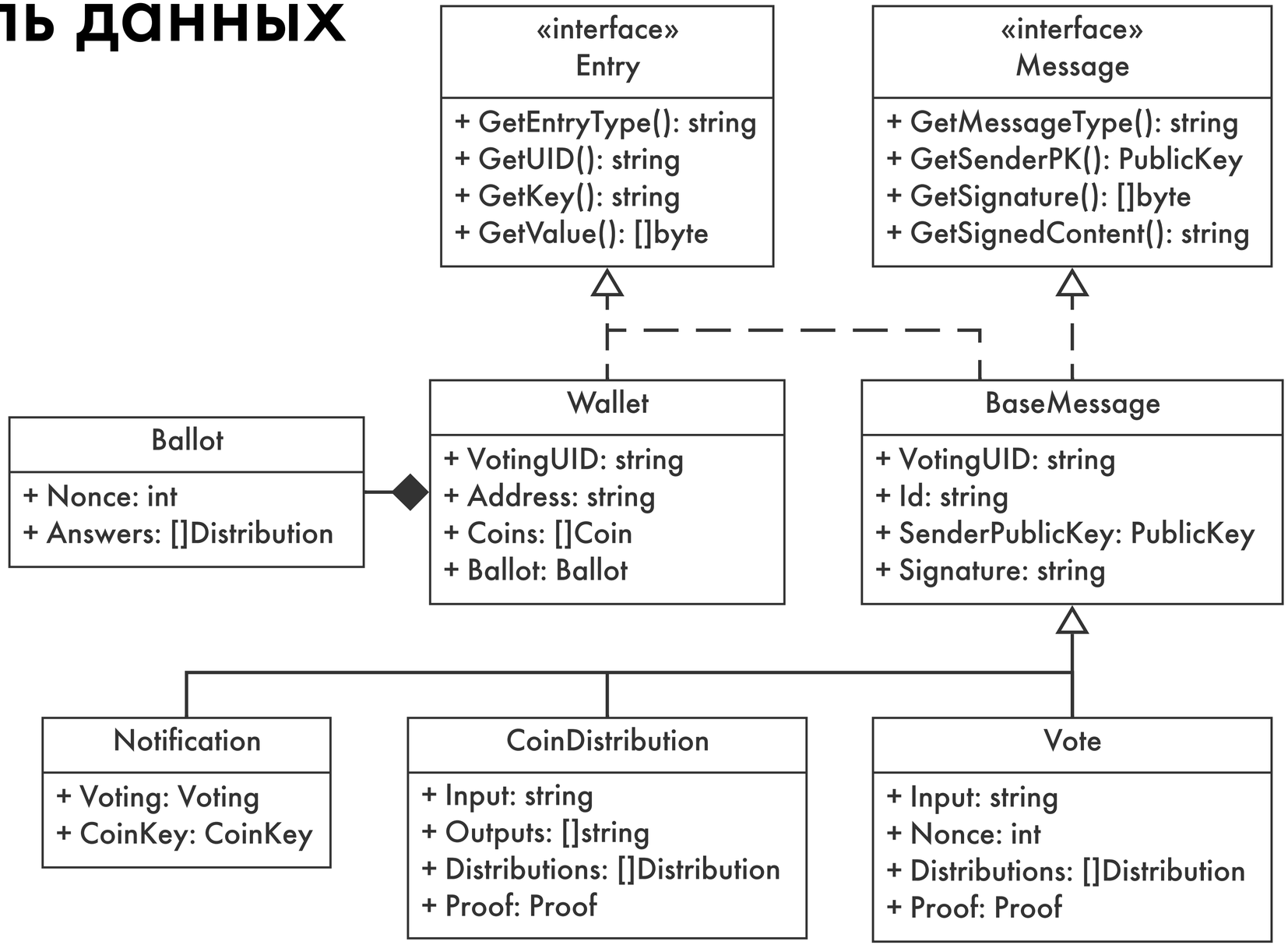
Сравнение подходов

Критерий \ Подход	Application-based	Chaincode-based
Модель данных	«Сырые» строки	Программные объекты
Состояние системы	Локальное	Общее
Хранимые данные	Все сообщения	Корректные сообщения
Синхронизация	Индивидуальная	Автоматическая
DLT-зависимость	Слабая	Сильная

Детали реализации

- ❑ Модель данных
- ❑ Способ хранения в базе данных «ключ-значение»
- ❑ Логика валидации
- ❑ Использование возможностей Hyperledger Fabric

Модель данных



Композитные ключи

Объект	Тип объекта	Подтип объекта	ID голосования	ID объекта
Уникальное сообщение	«message»	«emission»	+	–
Повторяющееся сообщение	«message»	«vote»	+	<message ID>
Кошелёк	«wallet»	–	+	<wallet address>

Обработчики и контекст

- Контекст
  - Контейнер для обрабатываемого сообщения
- BeforeTx
  - Десериализация сообщения
  - Проверка подписи
  - Запись сообщения в контекст
- AfterTx
  - Запись сообщения в реестр
  - Публикация события

Тестирование

- Проверка работоспособности
  - Голосование акционеров Московской биржи
  - 30 голосов по 3 ответа
  - 1500 участников
- Сравнение времени работы логики валидации подходов

Результаты нагрузочного тестирования

Метод	Application (ms/op)	Chaincode (ms/op)
organize	0.468 ± 0.010	0.477 ± 0.001
emit	0.150 ± 0.002	0.310 ± 0.001
distribute	150.167 ± 0.702	82.826 ± 0.353
vote	601.631 ± 2.746	268.063 ± 1.041
finalize	117.593 ± 2.402	148.902 ± 0.863

Конфигурация рабочей станции (18)

Результаты

- ✓ Проведён обзор предметной области
  - ✓ Протокол E-voting
  - ✓ Hyperledger Fabric
- ✓ Спроектирована архитектура системы
  - ✓ Проанализировано существующее решение
  - ✓ Разработан новый подход
  - ✓ Произведено сравнение подходов
- ✓ Реализован новый подход
  - ✓ Реализована система смарт-контрактов
  - ✓ Проведён рефакторинг off-chain приложения
- ✓ Проведено тестирование системы

Конфигурация рабочей станции

- **Операционная система:** macOS Mojave v10.14.6
- **ЦПУ:** Intel Core i7, 2.6 GHz, 6 Cores, 12 Logical processors
- **ОЗУ:** 32 GB 2400 MHz DDR4
- **Java:** AdoptOpenJDK 8 (v1.8.0_242, x86_64)
- **JMH:** org.openjdk.jmh:jmh-core:1.21
- **Go:** go1.14.2 (darwin/amd64)
- **Hyperledger Fabric:** v2.1.0 (commit: 1bdf97537)