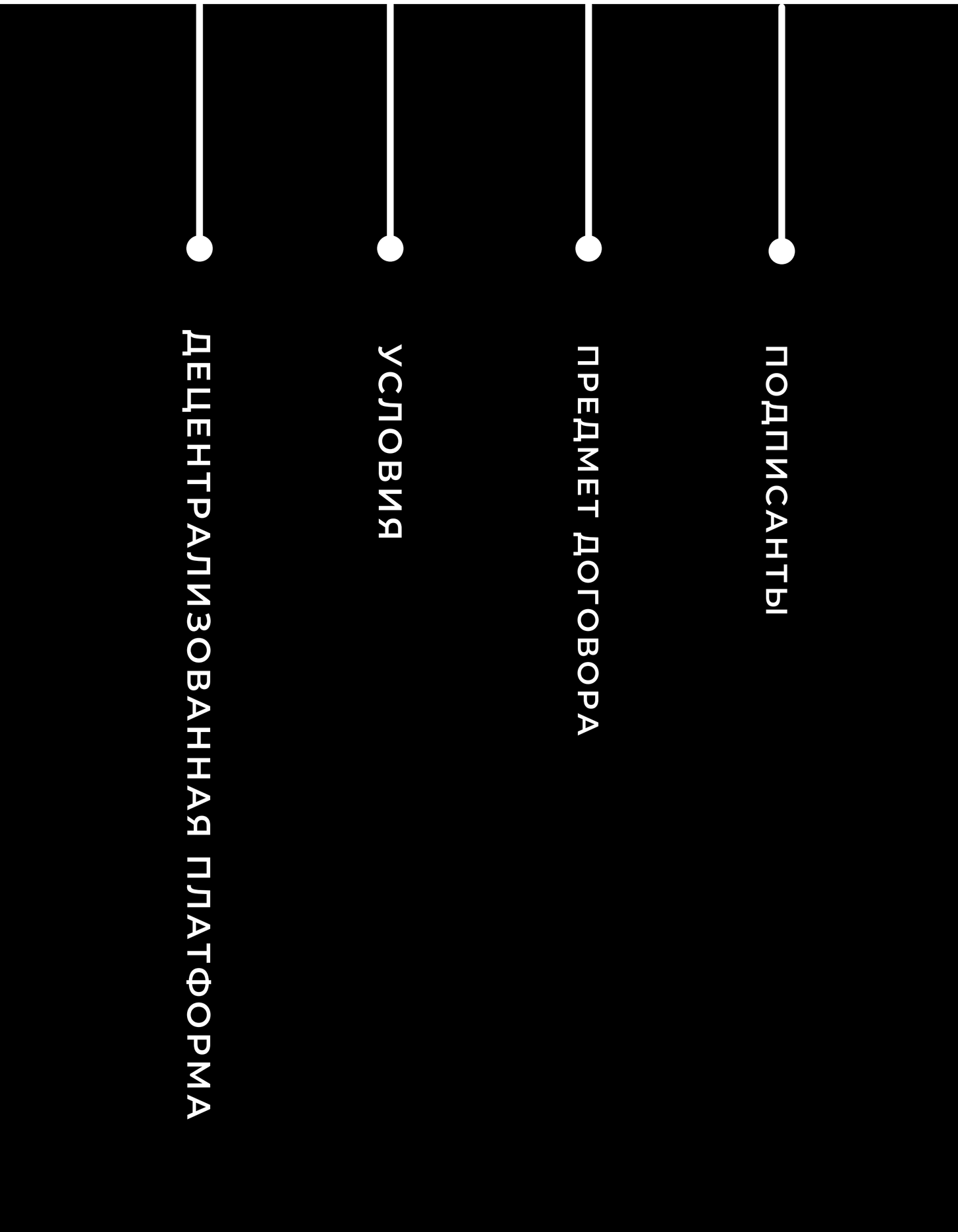
СМАРТ-КОНТРАКТЫ

ВЫПОЛНИЛ:
СТУДЕНТ ГРУППЫ
С8118-10.05.01
ММЗИ
СОЛОДИЛОВ
ЮРИЙ

Что такое смарт-контракт ?

СМАРТ-КОНТРАКТ – ЭТО ЦИФРОВЫЕ ПРОТОКОЛЫ ДЛЯ ПЕРЕДАЧИ ИНФОРМАЦИИ, КОТОРЫЕ ИСПОЛЬЗУЮТ МАТЕМАТИЧЕСКИЕ АЛГОРИТМЫ ДЛЯ АВТОМАТИЧЕСКОГО ВЫПОЛНЕНИЯ ТРАНЗАКЦИИ ПОСЛЕ СОБЛЮДЕНИЯ УСТАНОВЛЕННЫХ УСЛОВИЙ И ПОЛНОГО КОНТРОЛЯ ПРОЦЕССА.

Основные объекты «умного» контракта



Преимущества и недостатки смарт-контрактов

+ СКОРОСТЬ
+ НЕЗАВИСИМОСТЬ
+ БЕЗОШИБОЧНОСТЬ
+ НАДЕЖНОСТЬ

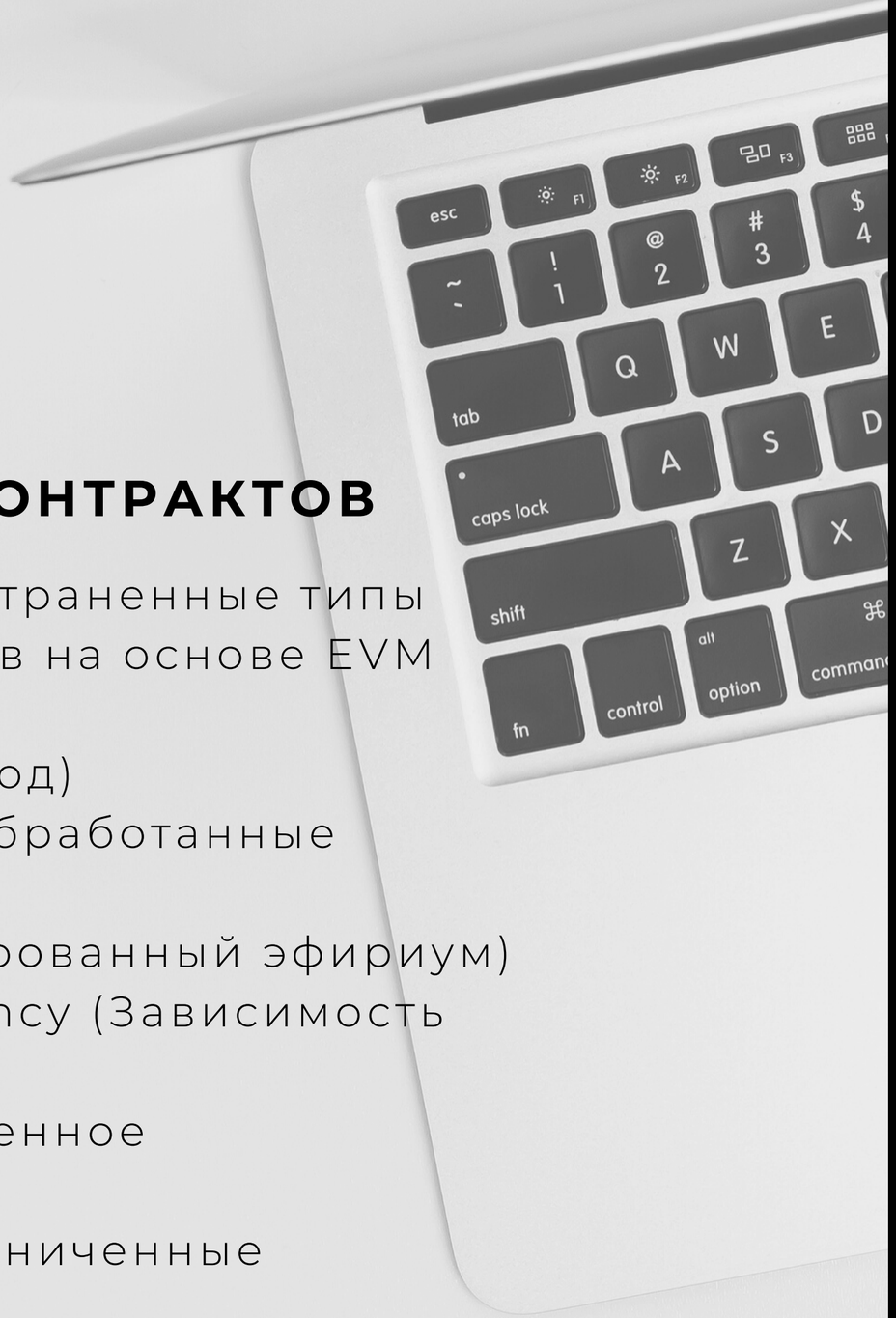
- ОТСУТСТВИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ
- СЛОЖНОСТЬ РЕАЛИЗАЦИИ
- НЕВОЗМОЖНОСТЬ ИЗМЕНЕНИЯ СМАРТ-КОНТРАКТА

СМАРТ-КОНТРАКТЫ ETHEREUM. НАИБОЛЕЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ

Блокчейн платформа Ethereum позволяет ее пользователям реализовывать на ней процессы разной сложности, поскольку она является программируемой платформой.

Код этих контрактов хранится в распределенном реестре и выполняется виртуальной машиной Ethereum (EVM), которая является основной этой блокчейн платформы.

Смарт-контракты Ethereum. Наиболее распространенные уязвимости



ОСОБЕННОСТИ:

- EVM
- Плата за выполнение кода
- Структура смарт-контракта

УЯЗВИМОСТИ СМАРТ-КОНТРАКТОВ

Некоторые наиболее распространенные типы уязвимостей смарт-контрактов на основе EVM (Ethereum Virtual Machine):

- Re-Entrancy (Повторный вход)
- Unhandled Exceptions (Необработанные исключения)
- Locked Ethereum (Заблокированный эфириум)
- Transaction Order Dependency (Зависимость порядка транзакции)
- Integer overflow (Целочисленное переполнение)
- Unrestricted Action (Неограниченные действия)

Известные атаки

THEDAO EXPLOIT

Эксплойт DAO - одна из самых печально известных ошибок в блокчейне Ethereum. DAO представляет собой полностью автоматический инвестиционный фонд. Желающие могут выставлять свои предложения на публику. DAO полностью построен на базе Ethereum, что дает полную поддержку смарт-контрактов этой технологии.

Злоумышленник использовал уязвимость в функции контракта splitDAO, которая предназначалась для создания дочерних версий проекта.

Вывод

СМАРТ-КОНТРАКТЫ ПОЗВОЛЯЮТ ПОЛНОСТЬЮ АВТОМАТИЗИРОВАТЬ ПРОЦЕСС СОВЕРШЕНИЯ СДЕЛОК, НО ОНИ ИМЕЮТ СВОИ ПРЕИМУЩЕСТВА И НЕДОСТАТКИ. НЕОБХОДИМО ПОЛНОСТЬЮ ПРОРАБОТАТЬ ЛОГИКУ РАБОТЫ УМНОГО КОНТРАКТА И ЗАРАНЕЕ ПРЕДУСМОТРЕТЬ ОШИБКИ В ПРОГРАММНОЙ РЕАЛИЗАЦИИ, ТАК КАК ИЗМЕНИТЬ ЕГО БУДЕТ УЖЕ НЕВОЗМОЖНО.