



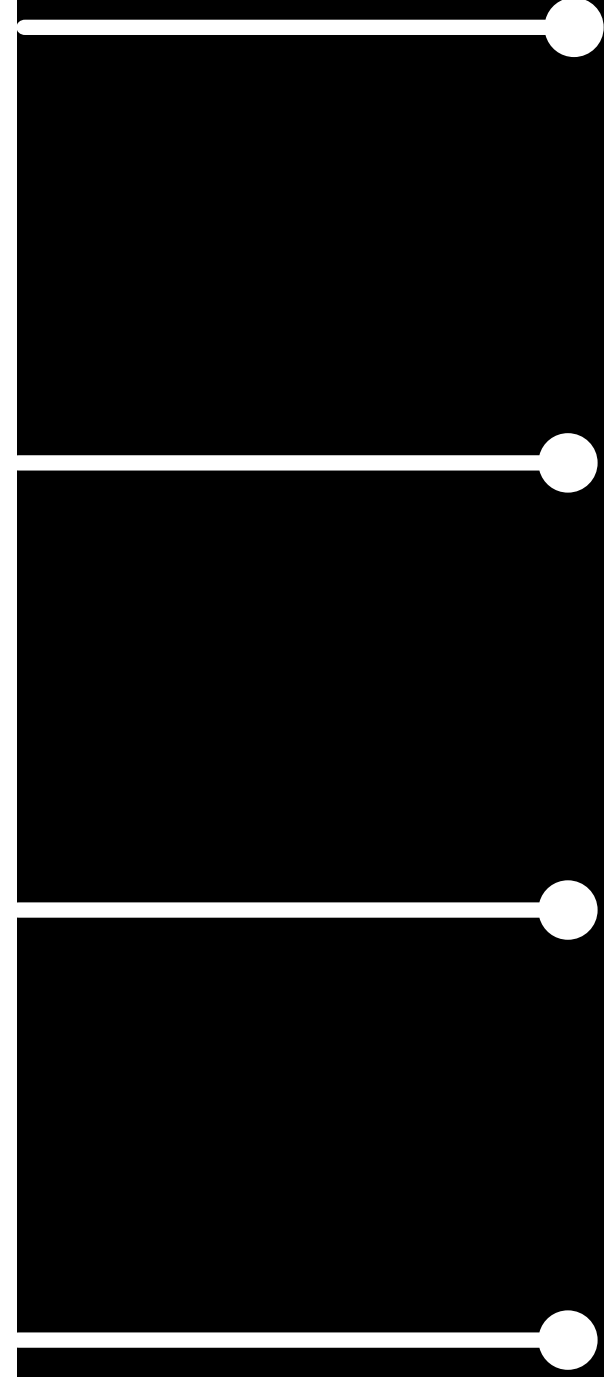
СМАРТ-КОНТРАКТЫ

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



- ПОДПИСАНТЫ
- ПРЕДМЕТ ДОГОВОРА
- УСЛОВИЯ
- ДЕЦЕНТРАЛИЗОВАННАЯ ПЛАТФОРМА

Преимущества и недостатки смарт-контрактов

-
- + СКОРОСТЬ
 - + НЕЗАВИСИМОСТЬ
 - + БЕЗОШИБОЧНОСТЬ
 - + НАДЕЖНОСТЬ

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

An illustration on a bright blue background. At the top, a white document with the title 'Smart Contract' in bold black font is shown. Below the title, there are several horizontal lines representing text. In the foreground, two hands are shaking in a firm grip. Each hand is holding a smartphone. The hand on the left is holding a light blue phone, and the hand on the right is holding a white phone. The background of the illustration features a pattern of yellow hexagons with black and grey stripes. The overall theme is digital agreement or smart contracts.

Smart Contract

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



THE DAO 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.

