ЦЕНТР
ЦИФРОВЫХ
ТРАНСФОРМАЦИЙ

ВЭБ
БАНК
РАЗВИТИЯ

ВЫЗОВЫ И ПОДХОДЫ К РЕШЕНИЮ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДРЫВНЫХ ТЕХНОЛОГИЙ.

ТРИФОНОВ МИХАИЛ

АНОНИМНОСТЬ КРИПТО-РАСЧЁТОВ

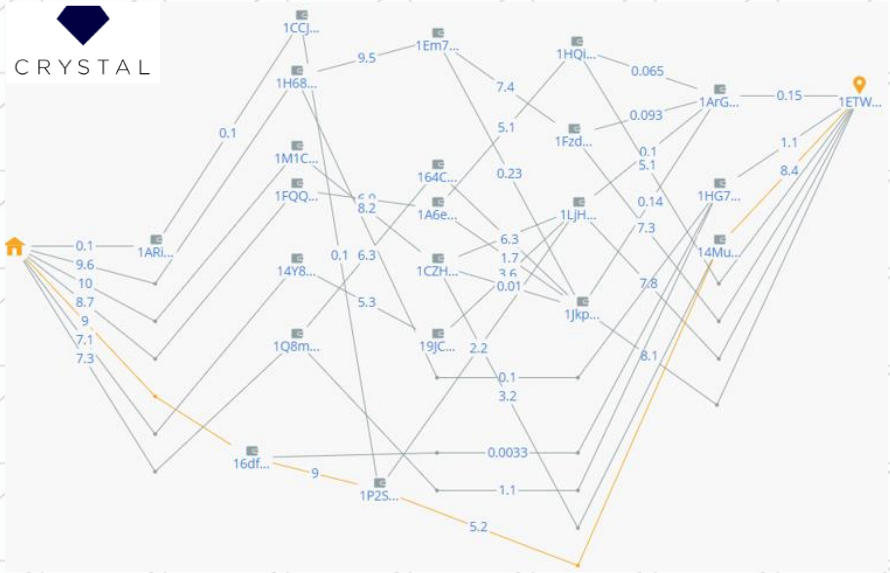
ЦЕНТР ЦИФРОВЫХ ТРАНСФОРМАЦИЙ

ВЫЗОВ :

БЛОКЧЕЙН И КРИПТО-ВАЛЮТЫ ДАЮТ ВОЗМОЖНОСТЬ АНОНИМНОЙ P2P-ПЕРЕДАЧИ АКТИВОВ.

ДЛЯ РЕГУЛЯТОРОВ РИСКИ АНОНИМНОСТИ ПРЕВЫШАЮТ ЛЮБЫЕ ВОЗМОЖНЫЕ ВЫГОДЫ ИННОВАЦИОННОО ИНСТРУМЕНТА.
ОТСУТСТВИЕ ВОЗМОЖНОСТИ УСТАНОВИТЬ, КТО СОВЕРШАЕТ ОПЕРАЦИИ С КРИПТО-СЧЕТАМИ, ЗАСТАВЛЯЕТ ОЦЕНИВАТЬ ЭТИ ОПЕРАЦИИ КАК МАКСИМАЛЬНО ОПАСТНЫЕ, ЧТО ЗНАЧИТЕЛЬНО УСЛОЖНЯЕТ ПРИНЯТИЕ И ПРИМЕНЕНИЕ ТЕХНОЛОГИИ.

ПО МЕРЕ РОСТА ПОПУЛЯРНОСТИ ТЕХНОЛОГИИ, СТАНОВИТСЯ АКТУАЛЬНОЙ ВОЗМОЖНОСТЬ ОТСЛЕЖИВАНИЯ ПОТОКОВ КРИПТОВАЛЮТ.



РЕШЕНИЕ:

ПРОГРАММНЫЕ АЛГОРИТМЫ ПОЗВОЛЯЮТ УСТАНОВИТЬ СВЯЗЬ МЕЖДУ ДЕЙСТВИЯМИ В БЛОКЧЕЙН СЕТЯХ И РЕАЛЬНЫМИ ОБЪЕКТАМИ, А ТАКЖЕ АНАЛИЗИРОВАТЬ ТРАНЗАКЦИОННУЮ АКТИВНОСТЬ КРИПТО-ВАЛЮТ (BITCOIN, BITCOIN CASH, ETHEREUM):

- КОЛИЧЕСТВО ПОЛУЧЕННЫХ КРИПТО-ВАЛЮТНЫХ СРЕДСТВ.
- ВСЕ КРИПТО-КОШЕЛЬКИ СВЯЗАННЫХ ОБЪЕКТОВ И ИХ СРЕДСТВА.
- ТЕКУЩЕЕ МЕСТОПОЛОЖЕНИЕ КОНКРЕТНЫХ «МОНЕТ», ВПЛОТЬ ДО ТОЧКИ ВЫВОДА СРЕДСТВ.
- ПОСТРОЕНИЕ ГРАФОВ ЗАВИСИМОСТИ ЛЮБОГО МАСШТАБА.

ВИРУС-ВЫМОГАТЕЛЬ WANNACRY
АЛГОРИТМ ОТСЛЕЖИВАНИЯ СФОРМИРОВАЛ ГРАФ СВЯЗЕЙ И ОПРЕДЕЛИЛ ТОЧКУ ВЫВОДА СРЕДСТВ ЗА НЕСКОЛЬКО ЧАСОВ

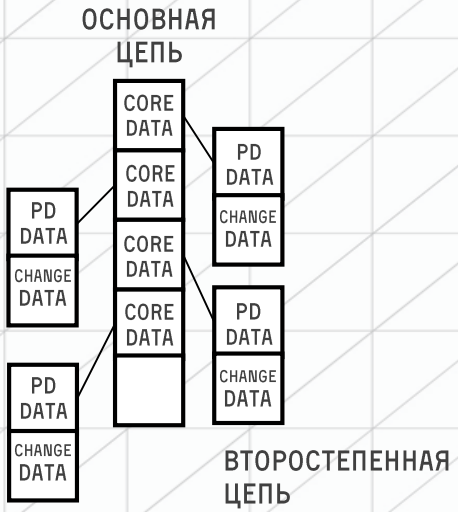
ЦЕНТР ЦИФРОВЫХ ТРАНСФОРМАЦИЙ

ПРОБЛЕМА ЮРИДИЧЕСКОГО ЗАБВЕНИЯ

ВЫЗОВ:

ОДНИМ ИЗ ВИДОВ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН ЯВЛЯЕТСЯ НЕИЗМЕННОЕ ХРАНЕНИЕ ДОКУМЕНТОВ. ПРИ РЕГИСТРАЦИИ ДАННЫХ ОНИ СТАНОВЯТСЯ УНИКАЛЬНЫМИ, НЕПОВТОРИМЫМИ И **НЕ УДАЛЯЕМЫМИ**. ЛОГИКА ВНЕСЕНИЯ И ХРАНЕНИЯ ИНФОРМАЦИИ ЯВЛЯЕТСЯ ОСНОВОЙ НАДЕЖНОСТИ ТЕХНОЛОГИИ.

«ПРАВО БЫТЬ ЗАБЫТЫМ» ИЗЛОЖЕНО В СТАТЬЕ №17 НОВОГО ОБЩЕГО РЕГЛАМЕНТА ЗАЩИТЫ ДАННЫХ (GDPR) ЕВРОПЕЙСКОГО СОЮЗА И ВСТУПИЛО В СИЛУ 28 МАЯ 2017 ГОДА. ПРАВО ПОЗВОЛЯЕТ ЛЮБОМУ ЧЕЛОВЕКУ ИСПРАВИТЬ ИЛИ УДАЛИТЬ СВОИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ИЛИ ЖЕ ПРЕКРАТИТЬ ИХ ИСПОЛЬЗОВАНИЕ, ЕСЛИ ДАННЫЕ БОЛЬШЕ НЕ НУЖНЫ ДЛЯ КОНКРЕТНЫХ ЦЕЛЕЙ, ИЛИ ЕСЛИ ЧЕЛОВЕК ОТОЗВАЛ СВОЕ СОГЛАСИЕ НА ИХ ИСПОЛЬЗОВАНИЕ.



ОСНОВНАЯ ЦЕПЬ:
- ХРАНЕНИЕ СВЯЗЕЙ ВТОРОСТЕПЕННЫХ ЦЕПЕЙ.
- КРИПТОГРАФИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО КОРРЕКТНОСТИ, ЦЕЛОСТНОСТИ И СОГЛАСОВАННОСТИ ИЗМЕНЕНИЙ.
- КОНТРОЛЬ УРОВНЕЙ ДОСТУПА К ВТОРОСТЕПЕННЫМ ЦЕПЯМ.

ВТОРОСТЕПЕННАЯ ЦЕПЬ:
- ХРАНЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.
- ИЗМЕНЕНИЕ / УДАЛЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ.

РЕШЕНИЕ:

ОТСУТСТВИЕ ВОЗМОЖНОСТИ УДАЛЕНИЯ РАЗМЕЩЕННЫХ ДАННЫХ, ПО РЕШЕНИЮ СУДА ИЛИ ДРУГИМ ПРИЧИНАМ, СТАЛО СЛОЖНОСТЬЮ ДЛЯ РЯДА ПИЛОТНЫХ ПРОЕКТОВ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ БЛОКЧЕЙН В ГОС. СЕКТОРЕ.

- КОНТРОЛЬ НАД ОБЩЕДОСТУПНЫМИ ДАННЫМИ В ОДНО-РАНГОВОЙ СЕТИ ДОВЕРЕННЫХ УЗЛОВ (ШИФРОВАНИЕ ЧУВСТВИТЕЛЬНЫХ ДАННЫХ), ЧТО СОПРЯЖЕНО С **РИСКОМ ИСТЕЧЕНИЯ СРОКА ВАЛИДНОСТИ** КЛЮЧЕЙ ШИФРОВАНИЯ.

- ПРИМЕНЕНИЕ ЛОГИКИ **ЗАВИСИМЫХ ЦЕПЕЙ**, ПРИ КОТОРОЙ ЧУВСТВИТЕЛЬНЫЕ ДАННЫЕ ХРАНЯТСЯ И ИЗМЕНЯЮТСЯ В ОТДЕЛЬНОЙ «ПРИКРЕПЛЕННОЙ» ЦЕПИ. ИЗМЕНЕНИЕ ИЛИ УДАЛЕНИЕ ДАННЫХ В «ПРИКРЕПЛЁННОЙ» ЦЕПИ **НЕ ТРЕБУЕТ** ПЕРЕРАСЧЕТА ОСНОВНОЙ ЦЕПИ.

БЕЗОПАСНОСТЬ IOT

**КИБЕРАТАКИ НА IOT СТАЛИ РЕАЛЬНОСТЬЮ.
В ПЕРИОД С 2015 ПО 2018 ГОДЫ С НИМИ СТОЛКНУЛИСЬ
ОКОЛО 20% ОРГАНИЗАЦИЙ, ОПРОШЕННЫХ GARTNER.**

ВЫЗОВ:

РАЗВИТИЕ КОНЦЕПЦИИ ИНТЕРНЕТА ВЕЩЕЙ И ЕЕ ВНЕДРЕНИЕ В РАЗЛИЧНЫЕ СФЕРЫ ЖИЗНИ, ПРЕДУСМАТРИВАЕТ НАЛИЧИЕ ОГРОМНОГО КОЛИЧЕСТВА АВТОНОМНЫХ УСТРОЙСТВ. ПО ДАННЫМ ПОРТАЛА STATISTA В 2017 ГОДУ УЖЕ РАБОТАЕТ БОЛЕЕ **20 МЛРД** УСТРОЙСТВ. К 2025 ГОДУ ПРОНГНОЗИРУЕТСЯ СУЩЕСТВОВАНИЕ НЕ МЕНЕЕ **75 МЛРД** УСТРОЙСТВ, ПОДКЛЮЧЕННЫХ К СЕТИ И ПЕРЕДАЮЩИХ СООТВЕТСТВУЮЩИЕ ИХ ФУНКЦИОНАЛУ ДАННЫЕ.

ДАННЫЕ И ФУНКЦИОНАЛ УСТРОЙСТВ ЯВЛЯЮТСЯ МИШЕНЬЮ ДЛЯ ЗЛОУМЫШЛЕННИКОВ.

БОТНЕТ **MIRAI** ПУТЕМ ПОДБОРА КОМБИНАЦИЙ ДЕФОЛТНЫХ ЛОГИНОВ И ПАРОЛЕЙ ВЗЛОМАЛ БОЛЬШОЕ КОЛИЧЕСТВО СЕТЕВЫХ КАМЕР И РОУТЕРОВ, КОТОРЫЕ В ДАЛЬНЕЙШЕМ БЫЛИ ИСПОЛЬЗОВАНЫ ДЛЯ DDOS-АТАКИ.

ПРОБЛЕМАТИКА:

- БОЛЬШИНСТВО РАБОТАЮЩИХ СЕГОДНЯ IOT-УСТРОЙСТВ ИМЕЮТ ДОСТУПНЫЕ ИНТЕРФЕЙСЫ УПРАВЛЕНИЯ И ДЕФОЛТНЫЕ ПАРОЛИ, СЛЕДОВАТЕЛЬНО ИМЕЮТ ВСЕ ПРИЗНАКИ ВЕБ-УЯЗВИМОСТИ.
- ПРОИЗВОДИТЕЛИ ЖЕРТВУЮТ УРОВНЕМ РАЗРАБОТКИ И ПОРОГОМ ЗАЩИЩЕННОСТИ УСТРОЙСТВ, В УГОДУ БЫСТРОМУ ВЫВОДУ ПРОДУКТА НА РЫНОК.
- ХАКЕРАМИ БЫЛА ПОЛУЧЕНА ВОЗМОЖНОСТЬ ДИСТАНЦИОННОГО УПРАВЛЕНИЯ ЭЛЕКТРОКАРДИОСТИМУЛЯТОРАМИ, ПОЗДНЕЕ ОНИ ПРОДЕМОНСТРИРОВАЛИ ПОЛУЧЕНИЕ ДОСТУПА К ИНСУЛИНОВЫМ ПОМПАМ И КАРДИО-ДЕФИБРИЛЛЯТОРАМ.

РЕШЕНИЕ:

- ФОКУСИРОВКА ПРОИЗВОДИТЕЛЕЙ НА БЕЗОПАСНОСТИ ВЫПУСКАЕМЫХ IOT УСТРОЙСТВ И ПРОДУКТОВ.
- СОЗДАНИЕ САНДАРТОВ РАЗРАБОТКИ И **СЕРТИФИКАЦИЯ.**
- СИМБИОЗ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ.

БЕЗОПАСТНОСТЬ IOT – БЛОКЧЕЙН

ВЫЗОВ:

СУЩЕСТВУЮЩАЯ АРХИТЕКТУРА:

- ЦЕНТРАЛИЗОВАННЫЕ ОБЛАЧНЫЕ ПЛАТФОРМЫ ОСТАЮТСЯ «УЗКИМ МЕСТОМ» КОМПЛЕКСНЫХ РЕШЕНИЙ IOT. ЛЮБАЯ НЕИСПРАВНОСТЬ ИЛИ ОШИБКА ПЛАТФОРМЫ ВЛИЯЕТ НА ВСЮ СЕТЬ IOT.
- ВОЗМОЖНОСТЬ АВТОРИЗАЦИИ НА УСТРОЙСТВЕ И ИЗМЕНЕНИЕ ЕГО НАСТРОЕК И ПАРАМЕТРОВ ВЗАИМДЕЙСТВИЯ В СЕТИ ИНТЕРНЕТ.

РЕШЕНИЕ:

ИЗМЕНЕНИЕ ЛОГИКИ ВЗАИМОДЕЙСТВИЯ:

- СУЩЕСТВУЮЩИЙ ПЕРЕХОД ОТ ЗАМКНУТЫХ ИЗОЛИРОВАННЫХ МОДЕЛЕЙ ВЗАИМОДЕЙСТВИЯ УСТРОЙСТВ, К ОБЛАЧНЫМ ЦЕНТРАЛИЗОВАННЫМ МОДЕЛЯМ, РАБОТАЮЩИМ ПО ПРИНЦИПУ АУТЕНТИФИКАЦИИ.
- РЕАЛИЗАЦИЯ ПОЛНОСТЬЮ РАСПРЕДЕЛЁННЫХ МОДЕЛЕЙ, РАБОТАЮЩИХ ПО ПРИНЦИПУ ПОЛНОГО ОТСУТСТВИЯ ДОВЕРИЯ, В КОТОРЫХ ЛЮБАЯ ТРАНЗАКЦИЯ ПОДТВЕРЖДАЕТСЯ СЕТЬЮ РАСПРЕДЕЛЁННЫХ УЗЛОВ.

ПОДХОД:

РЕАЛИЗАЦИЯ ЕДИНОЙ ПЛАТФОРМЫ (ЭКОСИСТЕМЫ) С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН:

- КОНТРОЛЬ СОСТОЯНИЯ ОБЪЕКТОВ IOT.
- ДЕЦЕНТРАЛИЗОВАННОЕ ХРАНЕНИЕ НАСТРОЕК И ПАРАМЕТРОВ.
- КОНТРОЛЬ ТРАНЗАКЦИОННОЙ АКТИВНОСТИ IOT.
- ВОЗМОЖНОСТЬ ВОССТАНОВЛЕНИЯ НЕ САНКЦИОНИРОВАННЫХ ИЗМЕНЕНИЙ.
- СМАРТ КОНТРАКТЫ ДЛЯ IOT.

ЦЕНТР
ЦИФРОВЫХ
ТРАНСФОРМАЦИЙ

ВЭБ
БАНК
РАЗВИТИЯ

ВЫЗОВЫ И ПОДХОДЫ К РЕШЕНИЮ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОДРЫВНЫХ ТЕХНОЛОГИЙ.

ТРИФОНОВ МИХАИЛ