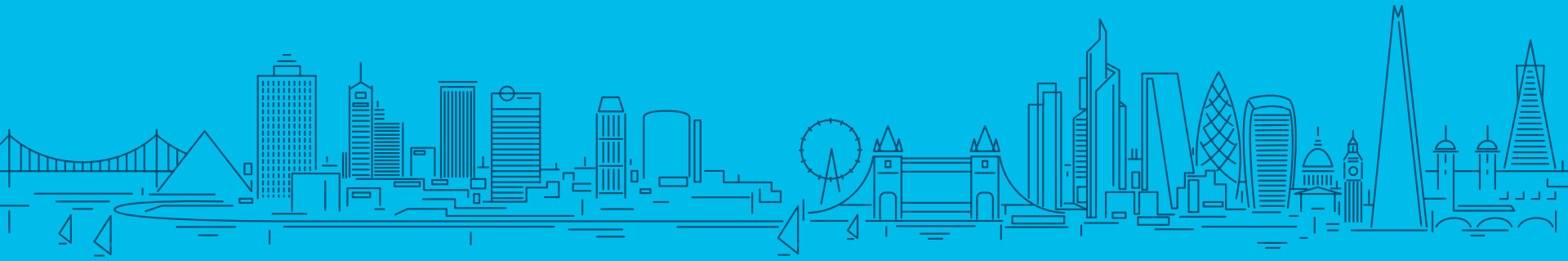


Блокчейн для кибербезопасности

Примеры реализованных проектов

Алексей Лукацкий
Бизнес-консультант по кибербезопасности
20 марта 2019

infosecurity EUROPE

EST. 2018 GEEK STREET

Félix Brezo, Ph. D.

Intelligence Analyst & Blockchain Consultant

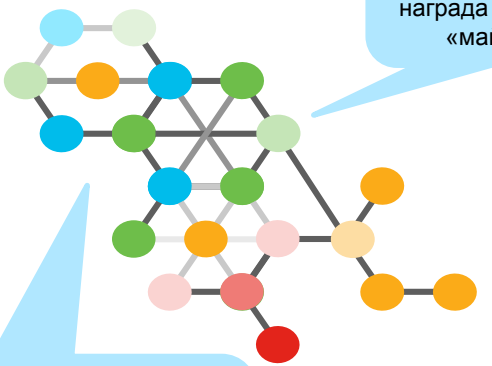
BLOC ASED C&C T QUES: TOWA ISTENT AN

Eleven Paths

Обратимся к терминам, но всего один раз

Открытый публичный

За поддержание открытого блокчейна подразумевается награда (мотивация) «майнерам»

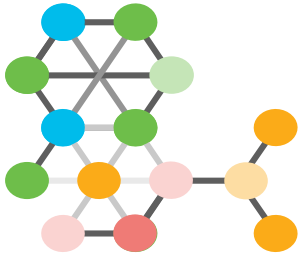


Любой (даже недоверенный участник) может отправить данные в блокчейн, которые никто не проверяет

ь доверия

Транзакции никем не контролируются и их формирование осуществляется в свободном порядке

Закрытый публичный (консорциум)



Контроль доверия

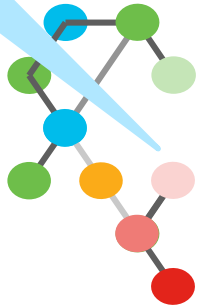
Алгоритмический

Традиционный

Согласование транзакций происходит среди избранных участников консорциума

Закрытый частный

Если формально это еще блокчейн, то фактически уже нет, так как нарушена основная идея



Контроль доверия

Алгоритмический

Традиционный

Все транзакции отслеживаются и контролируются центральным органом

Может и в ИБ можно применять блокчейн? Да, но не всегда!

КРИТЕРИЙ	ОПИСАНИЕ
Нет взаимодействующих сторон	• Если в сценарии не участвует несколько сторон, которые обмениваются какими-то ценностями или данными, то блокчейн в этом сценарии не нужен
Нет необходимости в общих данных	• Если для выполнения или проверки транзакции сторонам, осуществляющим операции, не требуется согласовывать базовые факты или данные, тот этот сценарий не подходит для блокчейна
Нужно хранить много данных	• Если основной идеей сценария является хранение больших объемов данных, блокчейн не подходит, так как он реплицирует данные между всеми участниками, увеличивая стоимость хранения
Требуется централизация	• Если сценарий требует централизации для выполнения транзакций или процессов, то блокчейн не подходит

Отсюда ряд первых и простых выводов

- ГосСОПКА и ФинЦЕРТ могли бы быть построены на блокчейне, с помощью которого можно было бы устроить обмен информацией об инцидентах ИБ (без PCAPов и иных больших артефактов), но в условиях требования централизации реализация на блокчейне теряет весь смысл
- Реализация базы инцидентов внутри организации на блокчейне также не имеет смысла, так как нет взаимодействующих сторон

Когда блокчейн мог бы помочь

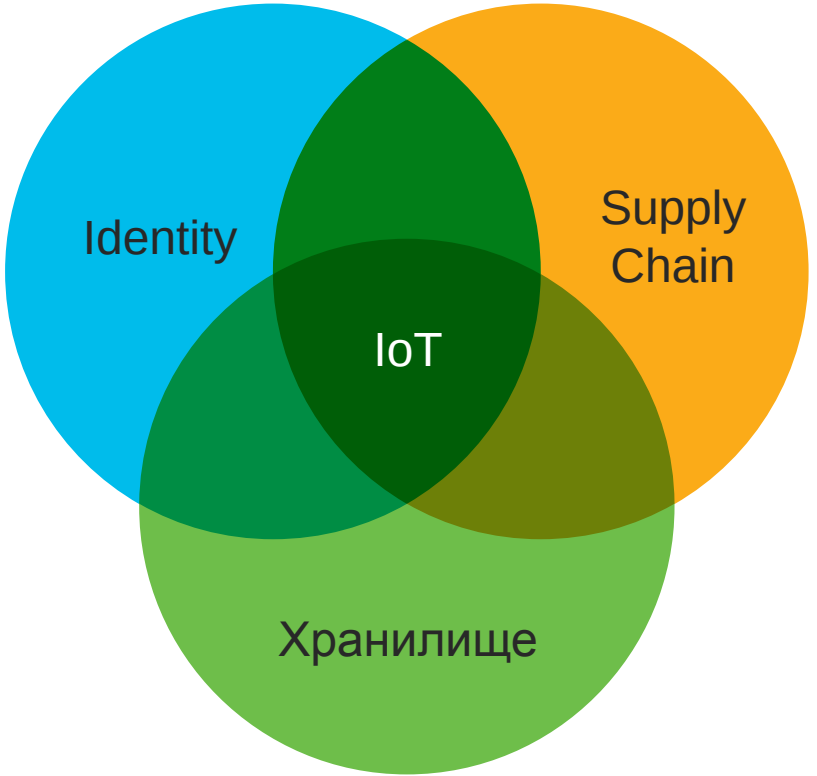
НАПРАВЛЕНИЕ	ОПИСАНИЕ
Передача и владение виртуальными активами	• Блокчейн разрешает безопасный обмен цифровых активов • Варианты использования: обмен такими активами как валюта, права собственности, сертификаты, программное обеспечение, купоны и т.п.
Неизменные, защищенные от доступа записи транзакций	• Блокчейн обеспечивает аудируемые и неизменные записи транзакций • Варианты использования: стороны имеют низкое доверие или участники могут иметь желание вмешаться в транзакции и подменить их данные
Быстро, безопасно и без посредников	• Блокчейн устраняет потребность в третьей стороне для проверки транзакций • Варианты использования: стороны полагаются на медленных и дорогостоящих посредников для осуществления транзакций
Беспристрастное выполнение условий контракта	• Блокчейн гарантирует guarantees беспристрастное автоматизированное исполнение закодированных условий контракта • Варианты использования: требуется автоматическое и беспристрастное исполнение условий контракта между участниками, такие как оплата, долговые обязательства, договора аренды и т.п.

И где тут безопасность ?

Возможные сценарии применение блокчейна в кибербезопасности

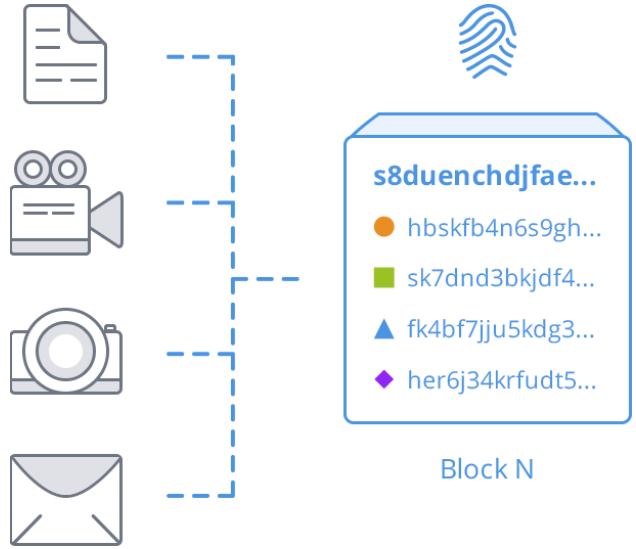
- Проверка обновлений / ПО
- Борьба с DDoS
- Защита периметровых устройств
- Отказ от паролей
- PKI
- Защита цепочки поставок
- Защищенный DNS
- База данных инцидентов
- Защищенные логи
- Достоверность данных
- Контроль целостности политик / конфигов
- Управление идентификационными данными
- Защищенное хранилище

Основные применения блокчейна в ИБ сейчас!



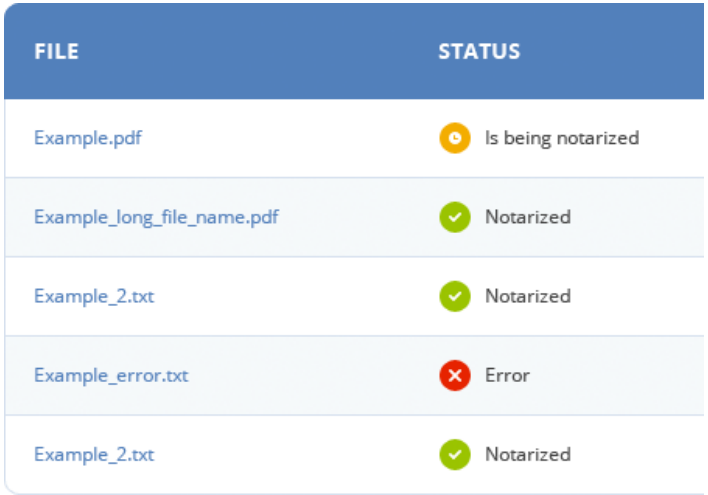
Защищенные файловые хранилища

- Acronis Notary, Gaia, Fluree, Enigma, Chronicled
- Децентрализованное шифрованное хранилище небольших порций информации (до нескольких мегабайт в блоке)
  - Часто меняется парадигма – нельзя обмениваться данными напрямую, можно пригласить к совместному использованию
- Централизованное хранилище с реестром записей о файлах



Acronis Notary на стыке хранения и identity

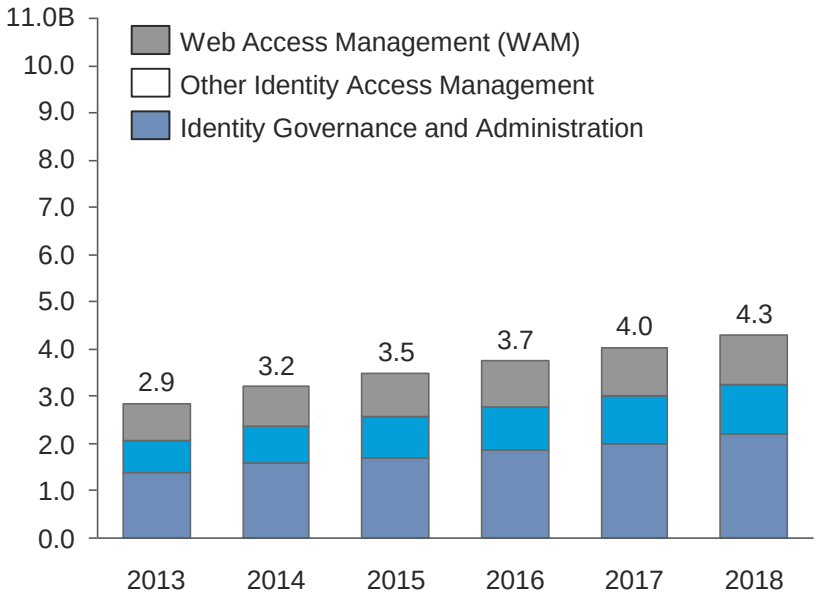
- Защищенное централизованное хранилище
- Для каждого загруженного файла снимается цифровой отпечаток (хэш), который помещается в блок Ethereum
- Проверка аутентичности каждого файла может проводиться вручную или автоматически



Digital Identity

- Digital identity входит в топ дискуссий на последних Blockchain Summit
  - Государственные регистрации и и нотариальные сервисы
  - Управление web-доступом
  - Реестры цифровых прав
- Предложение использовать блокчейн для улучшения биометрической системы идентификации в Индии

Размер рынка Digital Identity ($млрд)



Source: Gartner , CSTG research

Целостная цифровая идентичность

ПРОБЛЕМА

- **> 1 миллиарда людей не имеют никакого официально признаваемого идентификатора**
- **Без идентификации они части невидны, не могут голосовать, не получают медпомощи, образования, финансов и т.п.**
- **Без аккуратных данных о популяции, частные и госорганизации не могут предоставлять сервисы людям**

РЕШЕНИЕ БЛОКЧЕЙН

- **Взаимодействует между блокчейнами**, облаками и организациями, собирая воедино и оцифровывая идентификационные данные, которые часто находятся на разных континентах (GocID, медзаписи, пенсионные записи и т.д.)
- **Предоставляет людям** на платформе возможность **прямого согласия** на то, кто имеет доступ к их данным, а также когда и с кем стоит делиться этой информацией
- **Предоставляет возможность организациям** точно **обслуживать людей** на основе записей в блокчейне

СЕТЬ БЛОКЧЕЙН

- Государство
- Министерство здравоохранения
- Национальное бюро регистраций
- Избирательные комиссии
- Работа с беженцами
- ООН

УРОВНИ ЦЕННОСТИ

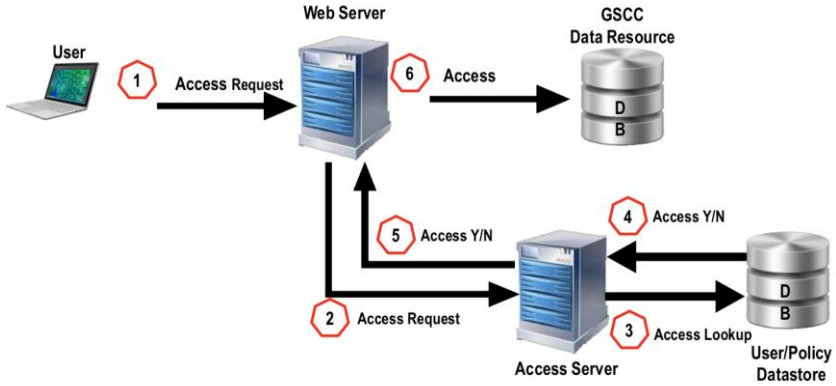
- Расширение возможности людей с идентификацией
- Экономические возможности
- Глобальное развитие

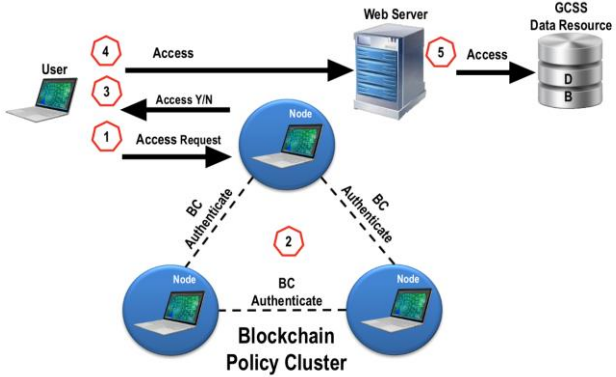
https://blogs.microsoft.com/blog/2018/01/22/partnering-for-a-path-to-digital-identity/

Реальные кейсы с блокчейном в Identity

- Эстонское правительство на базе решений Guardtime
- BlockVault – децентрализованный менеджер паролей
- Civic – отказ от паролей, имен, 3rd-аутентификаторов или физических токенов
- REMME – защита от атак за счет MFA пользователей и устройств. SSL-сертификаты на блокчейне
- CertCoin – PKI на блокчейне
- А также Sovrin, Evernym, Alastria, uPort…

Академия морской пехоты ВМФ США применяет блокчейн для доступа к системе управления поставками





На базе Oracle Access Management

67% всех запросов на доступ связаны с проверками прав доступа

Полученные преимущества

- Децентрализованная аутентификация пользователей
- Потенциальное снижение сетевой загрузки
- Не требуется ДМЗ
- Нет централизованного дорогостоящего web-сервера и хранилища
- Потенциальный рост доступности для удаленных пользователей
- Реализация политики на уровне алгоритма

Второй популярный кейс: управление цепочками поставок

Отслеживайте происхождение продукта в крупной распределенной цепочке поставок и уменьшайте потери доходов от контрафакта, фальсификата и **закладок**

Весь жизненный цикл продукта отслеживается блокчейном для обнаружения ошибок, сбоев и аномалий

Результат

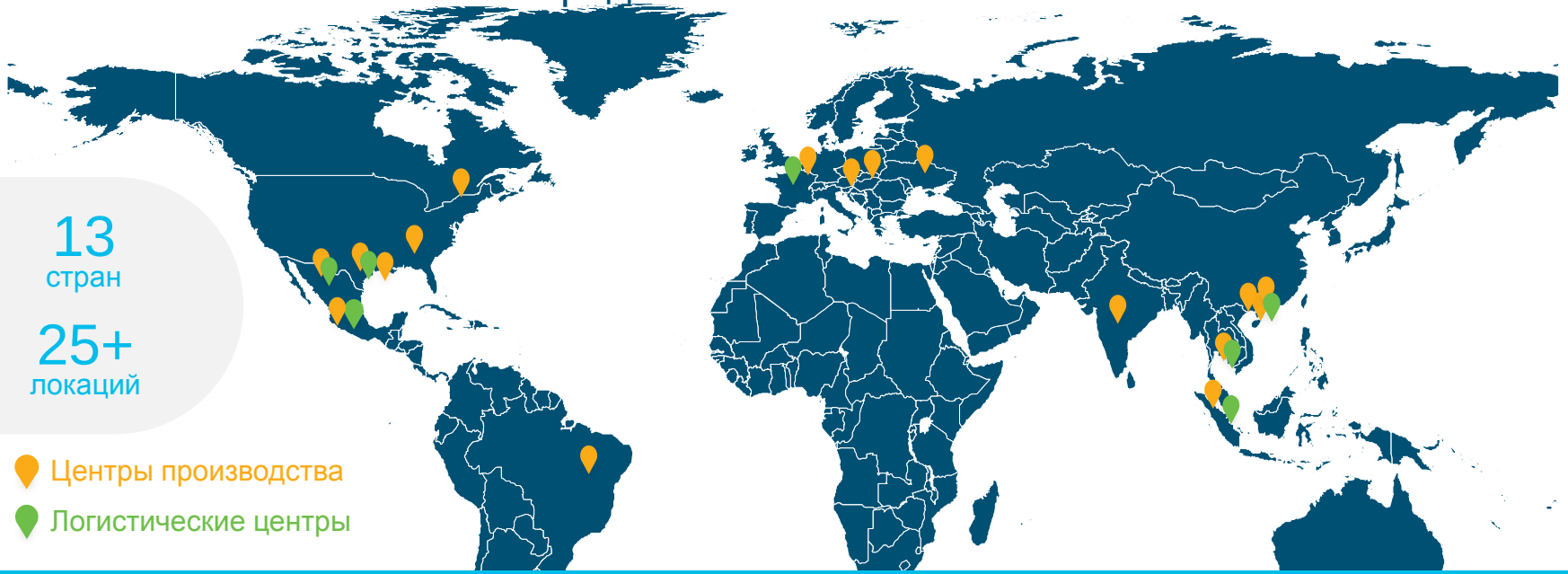
- Упрощение истории аудита и происхождения продукта
- Безопасное совместное использование исторических данных через цепочку поставок
- Отслеживание цепочки поставок и передач прав собственности
- Уникальная цифровая подпись для продукта

Управление цепочками поставок

- Проекты (в контексте кибербезопасности)
  - Cisco
  - Intel
- Производители
  - Chronicled
  - Blockverify
  - Cisco
  - Guardtime

Цепочки поставок Cisco

Глобально. Сложно. Распределенно.



13
стран

25+
локаций

Центры производства

Логистические центры

30,000+
позиций заказа

20,000+
виртуальных команд

1M+
заказов ежегодно

80M+
позиций доставляется ежегодно

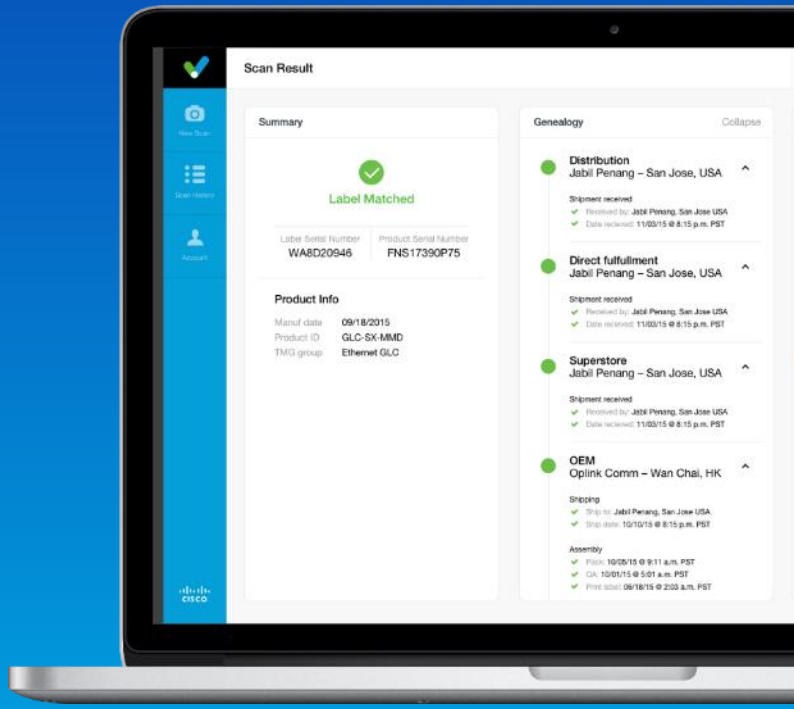
700+
активных поставщиков

62,000
компонент

XTRACE

Блокчейн-приложение, отслеживающее генеалогию продукта и обеспечивающее доверенное, аккуратное, распределение данных и видимость в реальном времени по всей цепочке поставок

- Простой API для подключения к участникам цепочки поставок и обеспечения обмена данными в реальном времени
- Смарт-контракты для отслеживания генеалогии продукта и родительских взаимоотношений между компонентами
- Миграция с реляционных БД, ERP-систем, B2B-сообщений и заводских MES-систем
- Базовый уровень с SDK для расширения возможностей отслеживания данных по всем компонентам и позициям

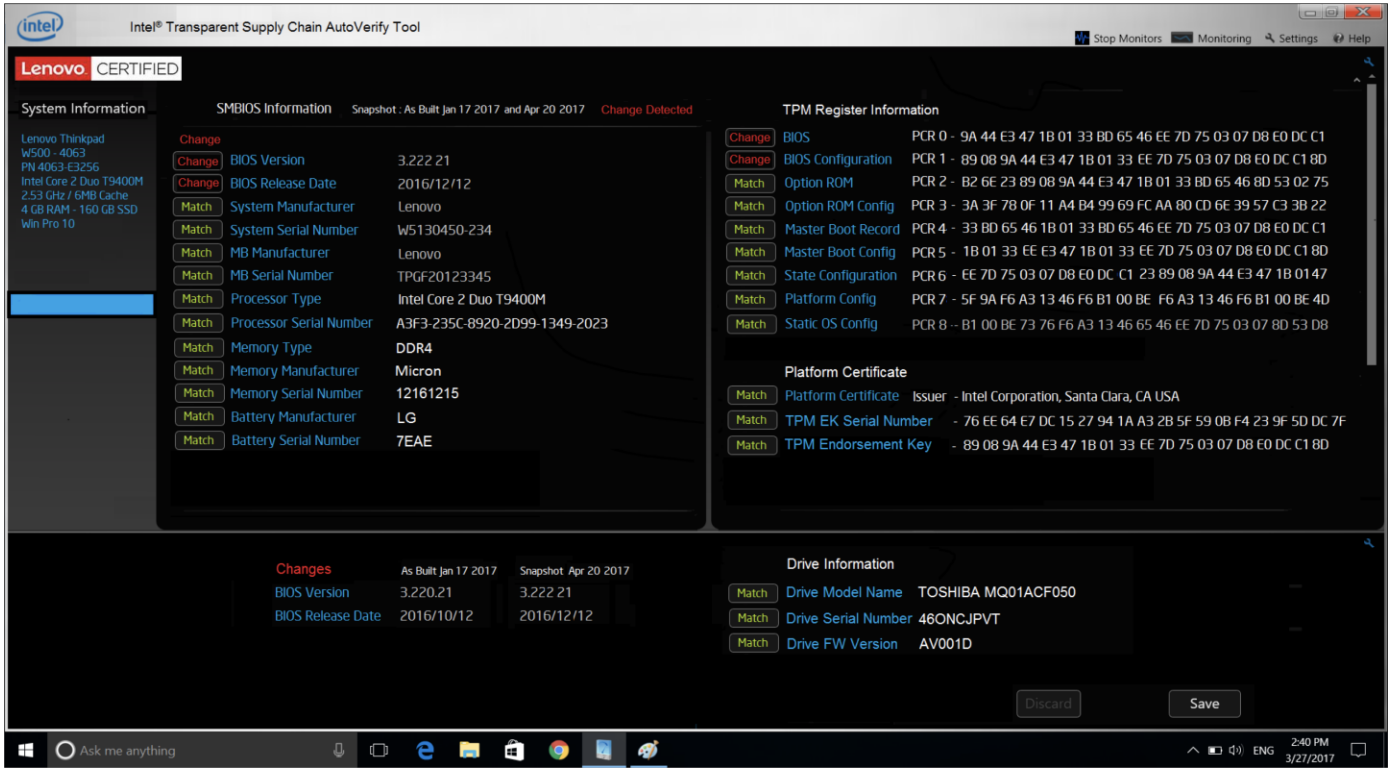


FootPrint

Блокчейн-приложение для обнаружения контрафакта, фальсификата и закладок

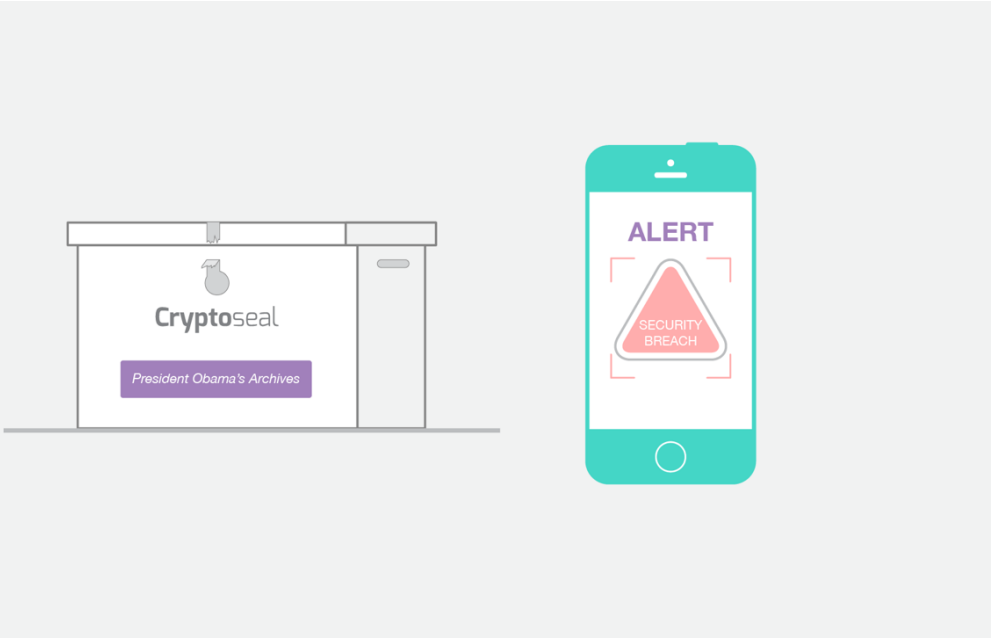
- Мобильное и веб-приложений, которое обеспечивает пользователям простой способ верифицировать аутентичность продукта
- Соединяется с XTrace для предоставления аудируемой истории генеалогии продукта
- Может использовать защищенные криптотокены для проверки владения и деактивации электронных контрафактных продуктов

Intel Transparent Supply Chain AutoVerify Tool



Chronicled может помочь WADA и архивам

- Аппаратные функции
  - Противовзломный клейкий стикер
  - Криптомикрочип
- Программные функции
  - Моделирование данных для гибких схем
  - Регистрация вещей в блокчейне
  - Проверка вещей в блокчейне



Trusted IoT Alliance

BNY MELLON

BOSCH

CISCO

FOXCONN

gemalto

bITSE

CHRONICLED

FILAMENT

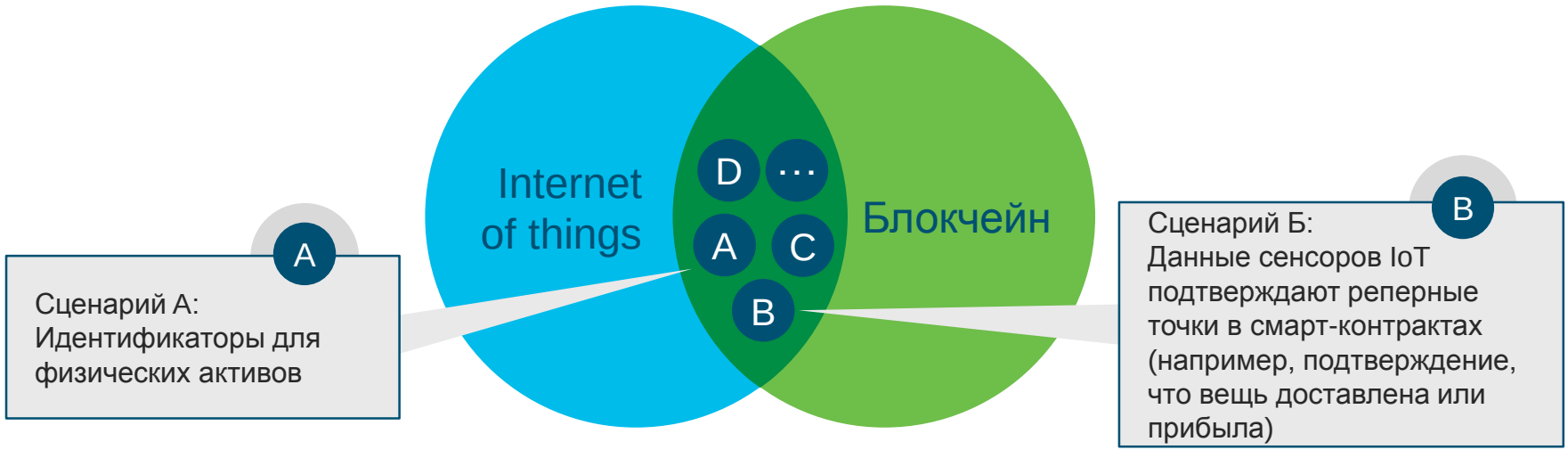
Ledger

slock.it

skuchain

CONSENSYS

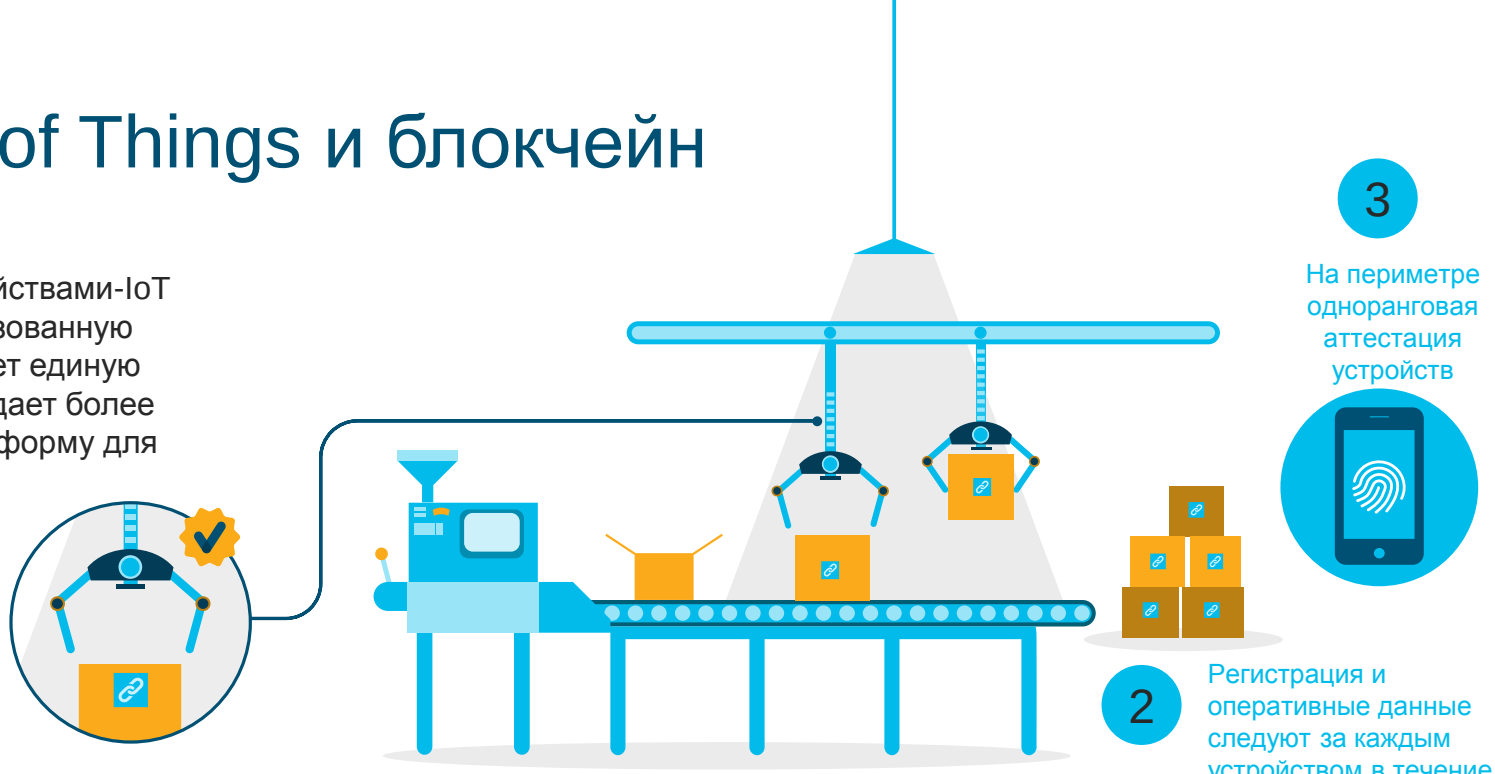
Как используется блокчейн в IoT?



20 миллиардов IoT-устройств в 2020-м году

Internet of Things и блокчейн

Управление устройствами-IoT через децентрализованную платформу снижает единую точку отказа и создает более защищенную платформу для работы устройств.



1

Производители регистрируют новое устройство и оперативные данные в блокчейне

2

Регистрация и оперативные данные следуют за каждым устройством в течение всего жизненного цикла

3

На периметре одноранговая аттестация устройств

Результат

Децентрализация и автономность

Исключает единую точку атаки

Защищенная и устойчивая платформа для устройств

Защита IoT устройств

ПРОБЛЕМА

- **Промышленная IoT инфраструктура высоко распределенна и уязвима к атаками и вредоносам**
- **Многие IoT-устройства поставляются с предсказуемыми паролями, заданными по умолчанию и взаимодействием с центральной системой, снижающей масштабируемость**

БЛОКЧЕЙН РЕШЕНИЕ

- Распределение данных безопасности и аутентификации через сеть устройств, создавая **невзламываемую, самоконтролируемую «фабрику» безопасности**
- Плотно **интегрирует безопасность** в **устройства и приложения** вместо централизованной системы безопасности
- Защищает сеть при подключении новых устройств и **изолирует зараженные устройства** через процесс **согласования** и достижения консенсуса между устройствами

СЕТЬ БЛОКЧЕЙН

- IoT-устройства
- Промышленные приложения и системы

УРОВНИ ЦЕННОСТИ

- Обеспечивает защищенное масштабируемое промышленное внедрение IoT
- Снижение рисков кибератак и утечек данных

- Используется в решениях ABB и Itron

https://techcrunch.com/2017/12/14/xage-emerges-from-stealth-with-a-blockchain-based-iot-security-solution

Распределен-ный доступ к умным устройствами

ПРОБЛЕМА

- **Большинство существующих домашних умных систем не обеспечивает гибкого контроля доступа для индивидуальных устройств**
- **Пользователи не могут выборочно предоставлять доступ разным группам (члены семьи или гости)**
- **Например, дети должны иметь возможность открыть дверь, но не мониторить камеры наблюдения**

COMCAST

РЕШЕНИЕ БЛОКЧЕЙН

- Предоставление простого способа предоставлять, отзывать и адаптировать доступ к любому IoT-устройству способом, который безопасен, приватен и высоко устойчив к взлому
- Создает **уникальную цифровую идентичность для каждого заказчика**, которые ассоциированы с распределенным реестром
- Заказчики могут ассоциировать **индивидуальные IOT-устройства** с их реестром и **затем установить или отозвать права доступа** как требуется

СЕТЬ БЛОКЧЕЙН

- Подключенные устройства
- Системы умного дома

УРОВНИ ЦЕННОСТИ

- Дать заказчикам контроль данных и доступа к их подключенным домашним устройствам
- Обеспечение приватности заказчиков

http://labs.comcast.com/blockchain-for-the-connected-home-combining-security-and-flexibility

Реальные кейсы с IoT на блокчейне

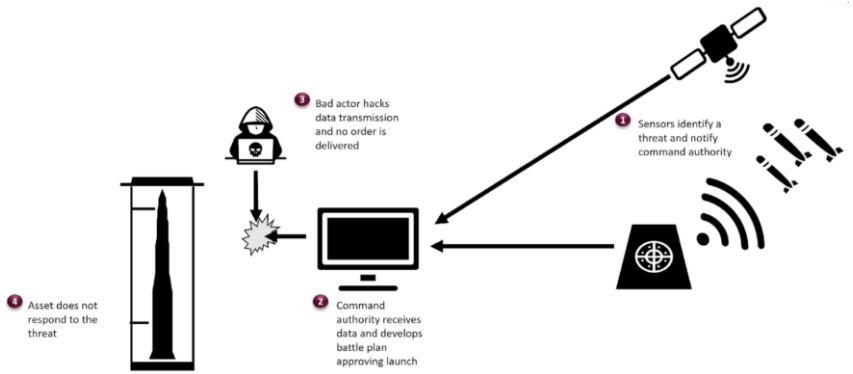
- Telstra защищает домашние IoT-устройства с помощью блокчейна, который хранит биометрию пользователей
- Elering (Эстония) вместе с Guardtime обеспечивает идентичность умных датчиков Smart Grid на блокчейне и неизменность всех событий с умных датчиков
- Аналогичный проект реализует и IOTA

Все это может быть связано со смарт-контрактами – оплата электроэнергии, инициирование расследования, замена устройства и т.п., но к ИБ это уже имеет опосредованное отношение

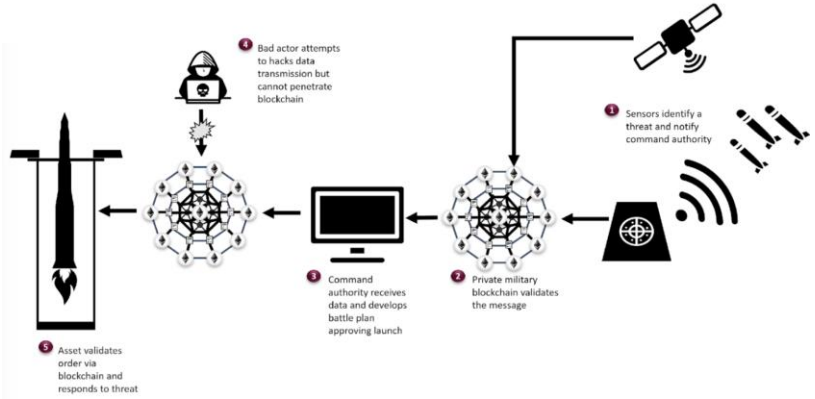
Хранение телеметрии в блокчейне

- По аналогичной схеме возможна реализация и проектов на блокчейне в кибербезопасности – SOC, SIEM, журналы регистрации и т.п.

Блокчейн для критической инфраструктуры или SOC под атакой



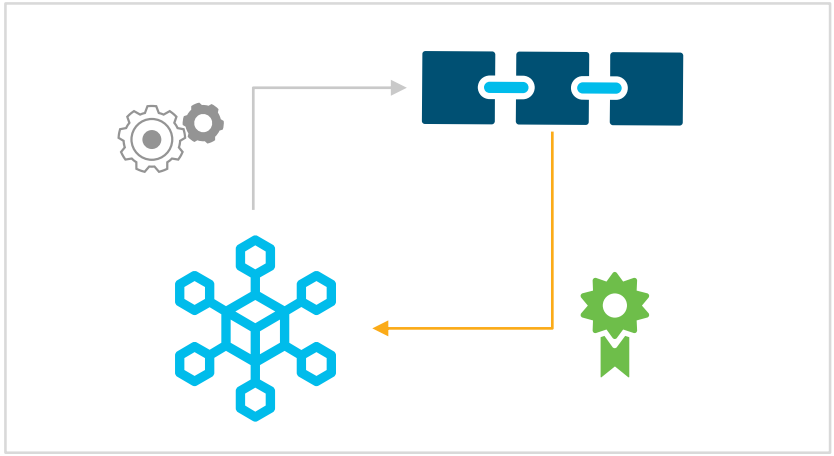
Централизованное управление огнем



Управление огнем на базе блокчейна

Проект ConsenSys ориентирован на военное применение, но схожая идеология может быть применена для защиты КИИ или SOC

Как обеспечить соответствие с блокчейном?



Участники блокчейн-сети

- Корпоративные ЦОДы
- Регуляторы
- Аудиторы

КАК БЛОКЧЕЙН МОЖЕТ ПОМОЧЬ

- Сетевые конфиги, политики и состояние ИБ сохраняются на блокчейне
- Любые изменения в сетевой конфигурации или политиках могут быть отслежены с помощью смарт-контракта и записаны в блокчейн
- Использование смарт-контрактов для мониторинга изменений, определения статуса соответствия и высвечивания любых областей, которые выходят за рамки соответствия
- Блокчейн будет поддерживать постоянные записи изменений и статус соответствия, которым могут доверять внешние стороны, включая регуляторов и аудиторов
- Организации могут делиться статусом соответствия в реальном времени с внешними сторонами и снижать последствия в случае аудита или расследования

Другие кейсы применения блокчейна в ИБ

Защита DNS

- BlockStack
- MaidSafe
- Nebulis

Защита от DDoS

- BlockArmour
- Gladius

Цифровые контейнеры для конфигов, VM, ACL

- Guardtime MIDA

Антивирусная платформа

- Levelnet

Антивирусный маркетплейс

- PolySwarm

Защищенный мессенджер

- Obsidian

А как же…

Threat Intelligence

Обмен инцидентами

Vulnerability Management

Patch Management

Маркетинговый хайп

Разные реализации имеют разную функциональность

Часто сложно отделить маркетинг от реальности

По-прежнему масштабируемость остается проблемой и направлением активных исследований

Блокчейн более сложен и ему не хватает прозрачности и аудируемости традиционных технологий

Отсутствие общих стандартов и правил

В ИБ блокчейн пока не столь распространен

В исследовании 2018-го года из 43 блокчейн-проектов какой-нибудь эффект показало только… **0 (ноль)** проектов!

Вопросы?

alukatsk@cisco.com