Kaspersky Blockchain Security

Комплексное решение для защиты технологий на базе блокчейна

Проекты на базе блокчейна становятся все популярнее. С их помощью можно решать широкий спектр задач, отнюдь не ограниченный криптовалютами. Технология блокчейн используется как фундамент бизнес-процессов во многих сферах, даже на производстве.

В том или ином виде блокчейн присутствует в IoT сетях, системах управления документооборотом, криптовалютах и многих других областях. Сегодня эта технология – основной компонент и один из новейших рабочих стандартов для различных сфер бизнеса.

Несмотря на то, что блокчейн по своей природе отличается повышенным уровнем безопасности, его применение все равно влечет за собой риски. Блокчейн содержит конфиденциальную информацию об активах и инфраструктуре пользователей и организаций, поэтому важно обеспечить этой технологии надежную защиту.

Комплексная безопасность для систем на основе блокчейна

Incident Response
Немедленная реакция на вторжение, кражу учетных данных и нарушения безопасности.

Education & Awareness
Узнайте, как реагировать, когда ваш блокчейн под угрозой, и как предотвращать инциденты безопасности.

Application Security Assessment
Проверка кода, обнаружение недостатков платформы и угроз для смарт-контрактов.

Protection Against Fraud & Phishing
Сократите риск фишинга и утечек данных, вызванных действиями злоумышленников.

Зачем нужен блокчейн?

Скорее всего, вы уже знаете об основных преимуществах технологии блокчейна – в первую очередь то, что она обеспечивает высокий уровень надежности и безопасности.

Децентрализация
Блокчейн, как правило, состоит из распределенной одноранговой (P2P) сети. Конечные точки – узлы – воспроизводят все данные, содержащиеся в системе. Такая архитектура предохраняет от системных отказов, поскольку ни одна конечная точка не является незаменимой и уникальной. Этот же подход защищает блокчейн от взлома, потому что потенциальному злоумышленнику придется преодолеть системы безопасности каждого узла для доступа к системе и всем данным.

Криптография
Данные доступны только при использовании набора приватных и публичных ключей. Достоверность транзакции проверяется сложным алгоритмом шифрования, что довольно надежно предохраняет систему от вмешательства извне.

Протокол консенсуса
Изменения в системе допускаются только с согласия всех держателей крупных долей – по мощности или по объему активов. Это называется протоколом консенсуса. Новые транзакции добавляются в блокчейн только по решению всех долевых участников, что предотвращает нарушения.

Система кажется вполне безопасной, но так ли это?

Есть множество рисков, которые не бросаются в глаза и на которые не так просто корректно отреагировать.

Уязвимости в смарт-контрактах
Смарт-контракты и коды блокчейнов могут содержать ошибки или даже серьезные бэкдоры, которыми могут воспользоваться киберпреступники. Кроме того, представляют опасность угрозы, связанные с инъекцией кода, небезопасным хранением или передачей данных. Приложения могут подвергаться рискам, связанным с несовершенством коммуникации между клиентом и сервером.

Уязвимости веб-сайта/угроза DDoS
Порталы ICO и сайты криптобирж подвергаются риску DDoS-атак и взломов.

Фишинг

Уязвимости в децентрализованных приложениях
Социальная инженерия, мошенничество и фишинг представляют серьезную угрозу даже для систем с высоким уровнем защиты, к которым относятся и блокчейн-системы, – мошенники могут выманить у пользователей их учетные данные.

Низкий уровень операционной безопасности и кибергигиены
В некоторых случаях злоумышленники, захватив контроль над более чем 50% блокчейна, могут подтверждать мошеннические транзакции.

Необходима защита, которая обеспечит комплексное решение по защите блокчейна – от корпоративного реестра до криптобирж и проектов по продаже токенов.

Преимущества децентрализации

Централизованные системы безопасности можно взломать, атаковав центральный узел. В последние несколько лет кибератаки привели к компрометации сотен миллионов пользовательских учетных данных.

- Facebook (2018) – 87 миллионов профилей (источник: The Guardian)
- LinkedIn (2016) – 167 миллионов наборов данных из учетных записей (источник: Telegraph)
- eBay (2014) – 145 миллионов профилей (источник: Reuters)
- JPMorgan Chase (2014) – 83 миллиона учетных записей (источник: The Guardian)

В 2017 году вирус-шифровальщик WannaCry зашифровал 300 000 компьютеров по всему миру. По оценкам экспертов, ущерб составил около 1 млрд долл. США. (Источник: Telegraph)

Децентрализованные сети тоже уязвимы

- В июне 2016 года злоумышленникам удалось использовать в своих интересах механизм возврата средств DAO (децентрализованной автономной организации). Двухступенчатый смарт-контракт смог вернуть инвестору Ethereum, но затем токены были переведены из его кошелька. При этом первый шаг не был добавлен в блокчейн, поэтому хакер повторял его много раз, пока не получил таким образом 79,6 млн долл. США. Чтобы вернуть деньги, разработчики решили переписать историю, однако такое решение вызвало немало вопросов. (Источник: Business Insider)
- В декабре 2017 года крупный майнинг-маркет Bitcoin под названием NiceHash потерял 60 млн долл. США в результате взлома. (Источник: bitcoin.com)

- Ключи необходимо предоставлять только доверенным пользователям, прошедшим внутренние проверки.
- Доступ к блокчейну должен быть надежно зашифрован и защищен от посторонних.
- Сетевые участники должны задействовать как можно больше уровней безопасности: логин, пароль, публичные и приватные ключи, сертификаты.
- Блокчейны и смарт-контракты не должны содержать вредоносный код.
- Клиент-серверная или одноранговая коммуникация должна быть защищена от кражи данных во время их передачи.
- Необходимо донести план действий на случай атаки до сведения каждого пользователя.
- Каждый пользователь должен знать, какие профилактические меры принять для предотвращения утечек данных.
- Доступ к различным компонентам блокчейна должен предоставляться строго в соответствии с рангом пользователя.

Теперь вы знаете, насколько уязвимым может быть проект на основе блокчейна и как важно обеспечить его всестороннюю безопасность.

«Лаборатория Касперского» представляет решения по защите проектов на базе блокчейна

Технология блокчейн применяется во многих областях, включая Интернет вещей, банковское дело и электронные госуслуги. Импульс к развитию технологии дали криптоактивы, и именно в этой сфере блокчейн востребован по-прежнему больше всего.

Технология обеспечивает комплексную безопасность для ICO, STO и криптобирж – сфер, где концентрируются финансовые активы и, соответственно, высоки риски.

Предложения токенов, в том числе ICO или STO (предложение безопасных токенов), – это процедура по привлечению инвестиций за счет продажи токенов компании. Криптобиржа – это место, где пользователи покупают и продают криптовалюты. Однако и ICO/STO, и криптобиржи находятся в киберпространстве, а потому уязвимы для киберугроз.

Решения для защиты блокчейна

Blockchain App Security

Сети на основе блокчейна используются в самых разных сферах и отраслях. И хотя по своей природе технология блокчейн безопаснее многих других, она все равно требует комплексной защиты. Вероятность ошибок кода, целевых атак или неавторизованного доступа можно сократить благодаря следующим мерам:

- Немедленное реагирование на инциденты
- Проверка кода
- Защита от мошенничества и фишинга
- Обучение пользователей

Token Offering Security

Для организации ICO/STO применяются смешанные технологии, которые нуждаются как в защите самого кода, так и в защите от веб-угроз:

- Проверка смарт-контрактов и отчетность по ним
- Защита от мошенничества и фишинга
- Расследование инцидентов
- Мониторинг безопасности веб-сайтов
- Тренинги по безопасной работе в интернете
- Тестирование на проникновение
- Проверка кода проекта
- Защита от DDoS-атак

Crypto Exchange Security

Криптобиржи требуют постоянной защиты и мониторинга:

- Защита от мошенничества и фишинга
- Расследование инцидентов
- Мониторинг безопасности веб-сайтов
- Обучение в области безопасной работы в интернете
- Тестирование на проникновение
- Предотвращение целевых атак
- Защита от DDoS-атак
- Квартальные отчеты безопасности
- Регулярная проверка кода

Вспомогательные решения для Blockchain Security

Kaspersky Smart Contract Review
Позволяет убедиться, что смарт-контракт написан безопасно, соответствует рекомендованным методикам и использует бизнес-логику в соответствии с аналитическими документами проекта. Проводит тщательный анализ кода смарт-контракта на предмет логических ошибок, уязвимостей, незадекларированного функционала.

Kaspersky Incident Response
Основная цель реагирования на инциденты – снизить воздействие нарушения безопасности или атаки на вашу IT-среду. Сервис охватывает весь цикл расследования инцидентов.

Kaspersky Educational Services
Сегодня предприятия вынуждены иметь дело с непрерывно растущим объемом постоянно эволюционирующих киберугроз. В этих условиях сложно переоценить важность тренингов в области IT-безопасности.

Kaspersky Penetration Testing
Тестирование на проникновение – это практическая демонстрация возможных сценариев атаки, которые могут использовать злоумышленники, чтобы обойти средства безопасности в вашей корпоративной сети и получить высокий уровень доступа к важным системам.

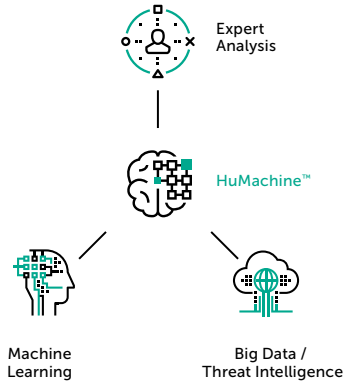
Kaspersky Application Security Assessment
Позволяет отыскать уязвимости в любых приложениях – от встроенных решений и крупных решений на базе облака до мобильных продуктов.

Kaspersky DDoS Protection
Комплексное решение по защите от DDoS-атак и устранению их последствий, способное защитить компанию на любой стадии возможной угрозы.

Kaspersky Anti Targeted Attack
Платформа объединяет передовые технологии и глобальные аналитические данные, благодаря чему она быстро выявляет целевые атаки и реагирует на них на любом этапе их жизненного цикла в системе.

Kaspersky Anti-Phishing Feeds
Сервис предоставляет подробные, точные и актуальные потоки данных о фишинговой и мошеннической активности, а также в реальном времени отслеживает появление фишинговых сайтов, имитирующих ваш бренд, и сообщает о них.

Kaspersky Fraud Prevention
Решение основано на широком спектре передовых технологий, в том числе машинном обучении, и применяется для своевременного обнаружения изощренных мошеннических схем в мобильных и веб-каналах.



www.kaspersky.ru