ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Факультет компьютерных наук
Департамент программной инженерии

УДК 004.9

УТВЕРЖДАЮ
Академический руководитель
образовательной программы
«Программная инженерия»,
профессор департамента программной
инженерии, канд. техн. наук

_____ В.В. Шилов
«___» _____ 2018 г.

Выпускная квалификационная работа

на тему Разработка и исследование скоринговых моделей финансовых рисков ICO
по направлению подготовки 09.03.04 «Программная инженерия»

Научный руководитель
профессор департамента
программной инженерии, к.т.н.,

С.М. Авдошин

_____
Подпись, Дата

Выполнил
студент группы БПИ 141
4 курса бакалавриата
образовательной программы
«Программная инженерия»

А.В. Лазаренко

_____
Подпись, Дата

Москва 2018

Реферат

Отчет: 61 с., 18 рис., 2 табл., 92 источника.
Ключевые слова: *Bitcoin, blockchain, ethereum, ICO, кибератаки, криптовалюты, скоринг*.

Представлены результаты выпускной квалификационной работы «Разработка и исследование скоринговых моделей финансовых рынков ICO», выполненной в соответствии с Приказом Национального исследовательского университета «Высшая школа экономики» № 2.3-02/0805-04 от 08.05.18

Краткое описание

В настоящей работе приведена обзор и анализ различных моделей скоринга финансовых рисков ICO. Предложена новая скоринговая модель, учитывающая участие тех или иных лиц в команде проекта и риски, связанные с информационной безопасностью. Приведено подробное изучение проектов, столкнувшихся в своей деятельности с рисками информационной безопасности.

Научная новизна работы заключается в том, что была разработана скоринговая модель финансовых рисков ICO и изучены риски, связанные с информационной безопасностью ICO проектов.

Практическая значимость заключается в том, что разработанная модель может быть применена различными организациями и физическими лицами для инвестирования в ICO проекты, а результаты изучения финансовых рисков ICO компаний могут быть использованы ими же при разработке стратегии защиты от кибератак.

Предмет исследования – финансовые риски ICO проектов.

Объект исследования - скоринговые модели финансовых рисков ICO проектов, связанные с информационной безопасностью.

Методами исследования являются следующие: метод восхождения от абстрактного к конкретному, метод идеализации, методы моделирования и абстрагирования.

Целью исследования разработка новой скоринговой модели финансовых рисков ICO проектов и комплексное изучение существующих моделей:

Задачи исследования:

- Изучить существующие скоринговые модели финансовых рисков ICO
- Изучить риски, связанные с информационной безопасностью ICO проектов
- Предложить новую скоринговую модель финансовых рисков
- Внедрить результаты работы в процессы компании Group-IB
- Изучить успешные кибератаки на блокчейн проекты.

Результаты работы

- Были изучены существующие скоринговые модели финансовых рисков ICO
- Были изучены ключевые риски проведения ICO, связанные с информационной безопасностью проекта
- Разработанная скоринговая модель была внедрена в деятельности компании Group-IB
- По теме ВКР было написано 3 публикации и сделаны выступления на 8 конференциях.

Публикации

- Лазаренко А.В. Хакер №228. Как крадут ICO [Электронный ресурс] // Журнал Хакер [Официальный вебсайт]. URL: https://xakep.ru/issues/xa/228/ (дата обращения: 24.04.2018).
- S.M. Avdoshin, A.V. Lazarenko. Bitcoin Users Deanonimization Methods [Электронный ресурс] // ИСП РАН [Официальный вебсайт]. URL: http://www.ispras.ru/en/proceedings/isp_30_2018_1/isp_30_2018_1_89/ (дата обращения: 25.04.2018).
- A.V. Lazarenko, S.M. Avdoshin. Financial Risks of the Blockchain Industry: A Survey of Cyberattacks. Springer series "Advances in Intelligent Systems and Computing" (принято к публикации)

Конференции

- Skolkovo Cyberday. Россия, Москва, технопарк Сколково, 25.10.2017. https://sk.ru/foundation/events/october2017/cyberday/. Тема доклада: Защита ICO.
- Bitcoin & Blockchain Conference. Россия, Москва. 15.11.2017. http://ict-online.ru/news/n150365/. Тема доклада: Защита $30 миллионного ICO от кибератак.
- Moontec 17. Эстония, Таллин, 4-5 декабря 2017. http://moontec.io/speakers/. Тема доклада: How ICO Hackers Steal Money.
- Russian Internet Week 2017. Россия, Москва. -03.11.2017. http://riw.moscow/en/forum/program/3/634 . Тема доклада: Как крадут деньги при ICO.
- Круглый стол CryptoInvestForum. Россия, Москва. 15.12.2017. http://cryptoinvestforum.ru/?rmcb=1524645846
- ICO Protection Days. Россия, Москва. 22.11.2017. https://idcfoundation.timepad.ru/event/610282/. Тема доклада: Защита проектов ICO.
- RSA 2018 Asia Pacific & Japan. Singapore, 27.07.2018. Тема доклада: Hacking the Blockchain Industry Projects.
- FTC 2018. Vancouver, Canada. 10.11.2018-11.11.2018. Тема доклада: Financial Risks of the Blockchain Industry: A Survey of Cyberattacks.

Ключевые слова: *Bitcoin, blockchain, ethereum, ICO, кибератаки, криптовалюты, скоринг.*

Abstract

In the last few years blockchain companies gained a lot of popularity. ICO (initial coin offering) is the one of the most widespread way of raising money. Tokens issued with ICO are almost immediately available on the cryptocurrency exchanges. Despite all the transparency and availability of public blockchain data it is still very hard to identify a really good and profitable project with reliable team and sufficient level of security. Due to this fact we decided to conduct a research on the scoring models of the financial risks of ICO projects.

The goal of the current paper is research and development of Scoring models for financial risks assessment. We provided the first academic research on financial risks related to information security and investment transaction tracing. The classification of scoring models is shown in the paper as well as the results of research.

Keywords: *bitcoin, blockchain, cryptocurrency, cyberattacks, ethereum, ICO, scoring.*

Оглавление

Определения и обозначения

• **AML -** от англ. (anti-money laundering) противодействие отмыванию денежных средств – комплекс мероприятий, направленных на противодействие легализации доходов, полученных преступным путем, и пресечение финансовых поток, предназначенных для террористической деятельности;
• **Blockchain** – выстроенная по определенным правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.
• **BTC –** от англ. (bitcoin) – цифровая валюта, функционирующая на основе технологии блокчейн.
• **Compliance checking** – контроль рисков несоответствия.
• **DAPP** – от англ. (Decentralized Application) – децентрализованное приложение, имеющее сходство со смарт-контрактами. Позиционируется как очередной этап развития блокчейн-технологий.
• **DDoS –** от англ. (Distributed Denial of Service) – распределенная атака отказа в обслуживании, целью которой является прекращение функционирования какого-либо интернет ресурса.
• **ERC20** – стандарт платформы Ethereum, определяющий набор правил, которые должны быть соблюдены для того, чтобы токен был принят и имел возможность взаимодействовать с другими токенами в сети.
• **ETH -** от англ. (Ethereum) – тикер цифровой валюты, функционирующей на основе блокчейна Ethereum.
• **Hype –** навязчивая реклама, шумиха, ажиотаж. Обычно используется для характеризации крупного ажиотажа и интереса вокруг какого-либо проекта или события.
• **ICO –** от англ. (Initial Coin Offering) – форма привлечения инвестиций в виде продажи инвесторам фиксированного количества единиц криптовалют, полученных разовой или ускоренной эмиссией.
• **KYC –** от англ. (know your customer) – термин банковского и биржевого регулирования для финансовых институтов и букмекерских контор, а также других компаний, работающих с деньгами частных лиц, означающий, что они должны идентифицировать и установить оичность контрагента прежде чем проводить финансовую операцию.
• **MVP** – от англ. (minimum viable product) – это минимально жизнеспособный продукт, который позволяет получить осмысленную обратную связь от пользователей, понять что им нужно и не создавать то, что им неинтересно и за что они не готовы платить.
• **NEP-5 –** технический стандарт токенов, используемый для смарт-контрактов на блокчейне NEO.
• **White paper –** документ, который помогает принять решение потенциальному клиенту в пользу определенной компании или конкретного продукта. Обычно содержит в себе описание технологии, бизнес-модель, сведения о команде и детали проведения ICO.
Дефейс
• **Лендинг –** основная страница на сайте, основной задачей которой является сбор контактных данных целевой аудитории или же привлечение первоначального внимания к проекту.
• **Фишинг –** вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным банковских карт, приватным ключам от криптовалютных кошельков.

1 Введение

Научная новизна работы заключается в том, что была разработана скоринговая модель финансовых рисков ICO и изучены риски, связанные с информационной безопасностью ICO проектов.

Практическая значимость заключается в том, что разработанная модель может быть применена различными организациями и физическими лицами для инвестирования в ICO проекты.

Предмет исследования – финансовые риски ICO проектов.

Объект исследования - скоринговые модели финансовых рисков ICO проектов, связанные с информационной безопасностью.

Методами исследования являются следующие: метод восхождения от абстрактного к конкретному, метод идеализации, методы моделирования и абстрагирования.

Целью исследования разработка новой скоринговой модели финансовых рисков ICO проектов и комплексное изучение существующих моделей:

Задачи исследования:

- Изучить существующие скоринговые модели финансовых рисков ICO
- Изучить риски, связанные с информационной безопасностью ICO проектов
- Предложить новую скоринговую модель финансовых рисков
- Разработать программу из компонент с открытым исходным кодом, реализующую автоматизируемые части скоринговой модели
- Экспериментально доказать, что скоринговая модель может использоваться для оценки финансовых рисков ICO проектов.

В последние годы использование ICO в качестве инструмента для привлечения инвестиций достигло пика своей популярности. По данным различных агрегаторов, было реализовано более чем 900 разных кампаний по сбору средств в криптовалюте. За все это время, стартапам удалось собрать 5.6 миллиардов долларов [1]. При этом, 46% проектов, успешно привлекших средства, уже провалились. Этот факт создает потребность в скоринговых моделях финансовых рисков.

Естественно, средства инвесторов находятся в зоне огромного риска. Из-за неаккуратного инвестирования в криптовалютные проекты можно потерять 100% вложенного капитала. К сожалению, крайне редко понятно заранее, насколько тот или иной проект сможет реализовать все ожидания и обещания, данные инвесторам. Без инструментов, позволяющих адекватно оценивать риски потери всех средств, инвестирование в криптовалютные проекты можно легко сравнить с игрой в казино, поскольку для рядового, непрофессионального инвестора крайне сложно сделать выводы о стабильности команды и потенциальной полезности того или иного проекта, выходящего на ICO.

Поскольку все процессы в ICO производятся в автоматическом режиме, вся ответственность за средства инвесторов переходит на плечи программного обеспечения, используемого для привлечения средств (например, для этого используются смарт-контракты). Из-за этого, риски, связанные с информационной безопасностью, представляют собой огромную опасность для команды проекта и конечных инвесторов. Так, в 2017 году киберпреступникам удалось украсть 10% всех средств, инвестированных в ICO через Ethereum. Общий ущерб составил почти 225 миллионов долларов, 30 тысяч инвесторов лишились в среднем по 7500 долларов.

2 Обзор и анализ источников, аналогов, выбор методов исследования

2.1 Обзор источников, аналогов

На момент проведения исследования существуют только модели, позволяющие оценить общую инвестиционную привлекательность каждого конкретного проекта, не учитывая факторы, связанные с чистотой привлекаемого капитала и информационной безопасностью проекта. Обзор каждого из методов приведен ниже.

2.1.1 Методика Icorating

2.1.1.1 Риск-оценка

Оценка риска нацелена на оценку потенциально мошеннических действий. Чем выше оценка риска, тем меньше информации о деталях ICO, разработке продукта, команде и документации, что ставит под сомнение возможность успеха запуска и продажи выпущенных токенов или криптовалюты на биржи [2].

Проекты оцениваются по таким характеристикам, как:

- Команда (ее состав, опыт участников и т.д.);
- Разработчики (опыт блокчейн разработки, реализованные коммерческие проекты);
- White paper;
- MVP;
- Риски, связанные с правовым регулированием;
- Смарт контракты (для ICO);
- Партнеры;
- Советники;

Риск-оценка предназначена для того, чтобы дать инвестору первоначальное представление о проекте и его команде, обнаружить любые возможные мошеннические намерения команды проекта, подчеркнуть уровень готовности проекта и наличие или отсутствие продукта.

Оценка этого параметра делится на пять уровней: очень низкий, низкий, средний, высокий и очень высокий. Чем ниже оценка параметра, тем ниже риск мошенничества со стороны команды проекта и тем выше качество его проработки.

Вторичная цель этого параметра - продемонстрировать шансы успешного проведения ICO и оценить перспективы дальнейшего роста проекта.

2.1.1.2 Нуре-оценка

Нуре-оценка показывает уровень интереса инвесторов к проекту. Чем выше оценка, тем больше людей рассматривают вопрос инвестирования в проект.

Нуре-оценка выставляется на основе следующих факторов:

- Количество пользователей на основных страницах социальных сетей проекта;
- Количество упоминаний в прессе;
- Упоминания в основных технологических и финансовых изданиях;
- Количество результатов в выдаче поисковой системы;
- Количество посетителей на главном веб-сайте;
- Анализ социальных сетей включает следующие платформы:
    - Bitcointalk
    - Telegram
    - Twitter

- Medium
- YouTube

Среди известных финансовых и технологических изданий, методика компании учитывает следующие: Techcrunch, VentureBeat, Forbes, WSJ, Reuters и т.д. Проект обязательно должен упоминаться в изданиях, отличных от узкоспециализированных криптовалютных журналах, поскольку попасть в них значительно сложнее и репутация изданий существенно выше. Более того, упоминания в крупных технологических и финансовых СМИ снижают риск мошенничества.

Hype-оценка делится на пять уровней: очень низкая, низкая, средняя, высокая и очень высокая. Чем выше оценка, тем выше интерес к проекту со стороны сообщества. Большое внимание аудитории при запуске может служить хорошим показателем инвестиционной привлекательности проекта. Зачастую приравнивается к уровню потенциального спроса на токены проекта после их выхода на криптовалютные биржи.

2.1.1.3 Инвестиционная оценка

Инвестиционная оценка отвечает на следующие вопросы:

- Является ли информация о текущем состоянии проекта, команде, рынке и степени развития технологической составляющей продукта достоверной и верифицированной;
- Каковы шансы команды на успешную реализацию продукта или услуги с заявленным (официально подтвержденным) набором разработок, командных компетенций, бизнес-моделью, текущим развитием рынка и конкурентной средой.

Методика составленная компанией ICORating направлена на то, чтобы учитывать все традиционные подходы к оценке инвестиционной привлекательности стартапов с учетом особенностей построения проектов на основе технологии блокчейна.

2.1.2 Методика Icomarketdata

Каждый ICO подлежит оценке на основе четырех групп критериев [3]:

- Оценка команды;
- Оценка продукта;
- Экономики токенов;
- Оценка бизнеса.

Каждая группа критериев содержит несколько подкритериев с переменной степенью важности в общей разбалловке.

Рейтинг составляется по каждому подкритерию с базовой оценкой от 1 до 5. Оценка 1 - наихудший рейтинг, оценка 5 - исключительный рейтинг. Среднее значение рассчитывается с учетом всех критериев и подкритериев.

Все критерии имеют переменную степень важности в общих баллах и рассчитываются следующим образом:

$$R = \{4 * Founders_{score} + 3 * Advisors_{score} + 2 * PoC_{score} + 2 * MVP_{score} + 3 * TechnologyLayer_{score} + 3 * TokenUtility_{score} + 3 * NetworkEffect_{score} + Valuation_{score} + MarketPotential_{score} + Competition_{score} + Supply_{score} + Vesting_{score} + Hype_{score}\} * 1/26$$

Оценки, связанные с командой:

- $\boldsymbol{Founders_{score}}$: Известны ли основатели? Имеют ли они соответствующий опыт и связи?
  - Неизвестные люди. Нет серьезной справочной информации;
  - Имеется неполная информация, нет соответствующего опыта;
  - Имеется справочная информация, никакого соответствующего опыта;

- Имеется широкий и релевантный опыт;
- Опытные, известные в широком кругу специалисты.

- $\boldsymbol{Advisors_{score}}$: Какой уровень приверженности, опыта и связей вызывают советники?
  - Нет авторитетных советников с соответствующим опытом.
  - Немногочисленные советники, у которых практически нет соответствующего опыта.
  - Советники с соответствующим опытом.
  - Уважаемые советники, имеющие соответствующий опыт и связи.
  - Высокопрофессиональные опытные, хорошо связанные и известные консультанты.

Оценки, связанные с проектом:

- $\boldsymbol{PoC_{score}}$**:** Решает ли Proof of Concept поставленную перед проектом задачу?
  - Нет, некогерентная концепция или нет необходимости в ней;
  - PoC трудно понять, необходимости или задачи не существует;
  - Четкая концепция, которая решает настоящую проблему;
  - Ясная, продуманная концепция, которая затрагивает реальную проблему, представляющую большой интерес;
  - Исключительное доказательство решения критической проблемы.
- $\boldsymbol{MVP_{score}}$**:** Есть ли MVP? Насколько детально проработан?
  - Непротестированная концепция;
  - Первоначальные тесты, отсутствует MVP;
  - MVP готов, запуск альфа-версии;
  - MVP готов, запуск бета-версии;
  - Полностью работающий исходный продукт.
- $\boldsymbol{TechnologyLayer_{score}}$: Является ли продукт инновационным? Способен ли он вносить вклад в экосистему blockchain?
  - Нет, продукт - это просто клон, не привносящий никакого вклада;
  - Продукт представляет собой DAPP с минимальным интересом к функционалу и небольшим вкладом в экосистему blockchain;
  - Продукт представляет собой DAPP, обмен или протокол, предназначенный для решения реальной проблемы;
  - Инновационный продукт, предлагающий решение проблемы с высокой вероятностью успеха;
  - Инновационный протокол, решающий важнейшие проблемы, представляющие наибольший интерес.

Оценки, связанные с экономикой токенов:

- $\boldsymbol{TokenUtility_{score}}$: имеет ли токен какую-либо утилитарную ценность?
  - Нет, токен не имеет никакой полезности;
  - У токена есть ограниченная, неясная утилитарная ценность;
  - У токена есть некоторая добавленная, но не неотъемлемая ценность;
  - Токен внедрен в сеть и имеет присущую ему ценность;
  - Токен имеет как неотъемлемую, так и добавленную стоимость и встроен в ядро сети.
- $\boldsymbol{NetworkEffect_{score}}$**:** Являются ли сильные сетевые эффекты встроенными в систему? Стимулируют ли стимулы стимулировать рост сети?
  - Сетевые эффекты не встроены;
  - Минимальные сетевые эффекты, нечеткие стимулы;
  - Появляются сетевые эффекты и стимулы;
  - Сплошные сетевые эффекты с явными стимулами из-за неотъемлемой полезности;
  - Сильные сетевые эффекты, согласованные стимулы и высокая полезность.

Оценка бизнеса:

- $\boldsymbol{Valuation_{score}}$: разумна ли оценка привлекаемого капитала для проекта? Достаточно, но не слишком много для проекта?
  - Нет, оценка смехотворна, проект может сделать с 1/10 суммы;

- Оценка выше, чем потребуется проекту. Скорее всего, хватит денег;
- Оценка целесообразна для объема проекта;
- Оценка является скромной для объема проекта;
- Оценка впечатляюще скромна по сравнению с высоким качеством проекта.

- $\boldsymbol{MarketPotential_{score}}$: каков потенциал рынка? Может ли проект проникнуть на рынок и покорить мир?
  - Четкий рыночный потенциал не прослеживается;
  - Ограниченный рыночный потенциал;
  - Видимый рынок и потенциал роста;
  - Твердый рынок и потенциал роста;
  - Исключительный потенциал роста рынка;
- $\boldsymbol{Competition_{score}}$: имеет ли проект конкурентов? Насколько привлекательнее он выглядит относительно конкурентов?
  - Ужасная позиция, проект соревнуется с множеством сильных игроков;
  - Слабая позиция, проект сталкивается с сильной конкуренцией;
  - Средняя позиция, проект сталкивается с сильной конкуренцией;
  - Твердая позиция, проект сталкивается с слабой конкуренцией;
  - Исключительное положение, у проекта почти нет конкуренции.
- $\boldsymbol{Supply_{score}}$: распределяет ли группа разумное количество токенов, чтобы стимулировать создание сильных стимулов и сетевых эффектов?
  - Незначительное распределение, жадная команда;
  - Малое распределение, низкие стимулы для участников сети;
  - Скромное предложение, слабые стимулы;
  - Разумное предложение, ответственная команда;
  - Большое предложение, солидная, изобретательная команда.
- $\boldsymbol{Vesting_{score}}$: имеет ли команда достаточную долю, чтобы оставаться стимулированной?
  - Большая доля, без лок апп периода;
  - Малые ставки, без лок апп периода;
  - Скромные ставки, отсутствие лок апп периода;
  - Разумные ставки, короткий лок апп период;
  - Солидный пакет, большой лок апп период.
- $\boldsymbol{Hype_{score}}$: представлен ли проект в социальных сетях и чатах? Есть ли к проекту интерес?
  - Отсутствие присутствия, негативное освещение;
  - Скромное присутствие и отсутствие интереса;
  - Разумное присутствие и скромный интерес;
  - Твердое присутствие и высокий интерес к проекту;
  - Исключительное присутствие, высокий интерес и значительная шумиха вокруг проекта.

2.1.3 Методика Foundico

Компания предложила алгоритм [4], который учитывает более 25 критериев, обеспечивает предварительный скоринг, который впоследствии одобряется или корректируется экспертами-модераторами до публикации проекта.

Алгоритм оценки включает пять групп показателей:

- Основная информация;
- Финансы;
- Продукт;
- Маркетинг;
- Команда.

Каждая группа содержит соответствующие подгруппы, а качество представленной здесь информации влияет на общий результат.

Каждая группа сначала проходит автоматическую проверку, а затем корректируется вручную, основываясь на ручном анализе предоставленной информации и ее полноте.

Общая информация включает:

- Название проекта;
- Тикер валюты;
- Логотип;
- Ссылка на сайт;
- Описание проекта;
- Дата и время начала ICO;
- Дата и время завершения ICO.

Когда все основные моменты для ICO указаны, это показывает ответственный подход менеджеров к разработке продукта. Это первое, что проверяют инвесторы при рассмотрении потенциальных объектов для инвестиций.

Финансовые показатели включают:

- Капитализацию (soft && hard cap);
- Распределение средств;
- Разрешенные валюты;
- Информация о токенах: объем и цена;
- Наличие условного депонирования;

Наличие четкой финансовой политики помогает инвесторам оценить уровень риска при инвестировании. Подробное раскрытие информации о движении денежных средств во время и после ICO помогает инвесторам понять, способна ли команда впоследствии стимулировать разработку своего токена.

Продуктовые показатели включают:

- Доступность и полнота «Дорожной карты»;
- Доступность и качество White paper;
- Наличие работоспособного прототипа;

Когда команда проекта предоставляет достаточно подробное описание продукта, это помогает инвесторам понять, насколько сложно реализовать их идею. Чем меньше информации предоставлено о продукте на этапе ICO, тем меньше уровень уверенности инвесторов в будущей жизнеспособности компании.

Маркетинговые показатели включают:

- Количество каналов продвижения и качество их использования;
- Доступность презентации и видео проекта;

Связь между командой проекта с одной стороны и инвесторами и сторонниками с другой стороны является ключом к успеху любой инвестиционной кампании. Используя широкий спектр каналов продвижения, команда может охватить большее количество людей, увеличивая количество потенциальных инвесторов.

Командные показатели включают:

- Количество членов команды и их личности;
- Наличие биографии, фотографий и ссылок на аккаунты в социальных сетях;

Крупные инвесторы всегда внимательно изучают всех членов команды. Наличие хорошо зарекомендовавшей себя команды, включающей доверенных членов, является ключевым показателем того, насколько успешным может быть ICO. Чем больше информации доступно для отдельных членов команды (фотографии, ссылки на социальные сети, биография), тем выше общий балл, который проставляется для команды.

2.1.4 Методика Tokenmetrics

Методика скоринга, используемая компанией Tokenmetrics [5] учитывает следующий набор групп оценочных параметров:

- Экономика ICO
- Качественные метрики
- Hype – метрики

2.1.4.1 Экономика ICO

Максимальное количество привлекаемых средств (Token-sale hardcap)

$$R = 4 * (1 - \frac{hardcap}{market_{cap}}) * MS_{ROI} * TKN_{avg}$$

где

- $hardcap$ *– максимальное количество привлекаемых средств;*
- $market_{cap}$*- рыночная капитализация по всем криптовалютам;*
- MS_{ROI} *– отношение среднего максимального количества привлекаемых средств от успешного ICO к итоговой рыночной криптоиндустрии в момент тех ICO;*
- TKN_{avg} *- средний процент токенов успешных проектов, выделенный для публичной продажи;*

На сегодняшний день средний процент от общего объема рынка ICO до общей капитализации криптовалютного рынка составляет 0,038%, а 63% - это средний процент токенов, который выделяется успешными проектами для публичного краудсейла. Эти цифры изменяются с течением времени, поскольку каждый месяц появляются новые проекты.

Итоговая капитализация ICO

Максимально - 2 балла. Формула выглядит следующим образом: 2 * (1 - ограничение капитализации на крышке / текущем криптовом рынке * средний процент закрытия рынка ICO на полностью разводненной основе до общей капитализации криптового рынка в течение наиболее успешной ICO (от ROI).

$$R = 2 * \left(1 - \frac{hardcap}{market_{cap}}\right) * MS_{ROI}$$

Этот показатель помогает правильно оценить количество токенов, выделенных для частной продажи, и оценить общую стоимость стартапа, привлекающего средства.

Максимальная скидка

Максимально - 2 балла. ICO, предоставившие инвесторам максимальную скидку 0% - 15%, получают 2 балла, 16% - 24% - 1,5 балла, 25% - 49% - 0,5 балла, все ICO проекты с более чем 50% скидкой получают 0 баллов. Чем выше максимальная скидка, тем выше риск сбрасывания токенов после ICO. Соответственно, тем меньше и оценка.

Процент распределяемых токенов

Максимально - 2 балла. ICO, которые выделяют более 80% или менее 30% для публичной продажи, получают 0 баллов, другие проекты получают баллы, основанные на их позиции относительно среднего числа наиболее успешных ICO, что составляет 63 %.

Слишком малая доля в распределении токенов ICO может привести к демпированию цен после ICO, поскольку многие токены будут у очень небольшого количества людей,

которые могут манипулировать ценой для своей собственной выгоды. Слишком высокий процент выделения токенов для ICO может показать, что намерения команды не совпадают с намерениями участников ICO, поскольку команда удерживает слишком малое количество токенов.

Инфляция токенов

Максимально - 1 балл. Если происходит инфляция токенов в момент ICO, проект получает 0 баллов, если нет инфляции - 1. Инфляция цены на токен плоха для держателей токенов, чем больше токеново проект собирается создавать, тем больше будет разбавлена цена для конечного потребителя.

Программа выкупа

Максимально - 1 балл. Если проект планирует осуществлять программу обратного выкупа токенов – получает 1 балл, если нет – 0 баллов.

Сожжение лишних токенов

Максимально - 1 балл. Проект получает один балл, если все непроданные в момент краудсейла токены будут уничтожены и ноль, если нет.

Цена токена на ICO

Максимально - 2 балла. При оценке стоимости токена ICO применяется тот же принцип, что и при оценке % токенов, выделенных во время ICO, однако формула отличается. Средняя цена успешных ICO составляет 0,11 доллара США, и чем ближе цена на токен ICO, тем выше мы оцениваем его более высокую оценку. ICO с маркером стоимости менее 0,01 доллара США, но более 0,001 получает 0,5 балла. Если стоимость токена составляет менее 0,001, проект получает 0.

Страны с запретом на участие в ICO

Максимально - 1 балл. ICO, запрещающие покупку токенов для граждан более, чем 5 стран (по юридическим причинам), получают 1 очко. Если запрет распространяется на граждан от 3 до 4 стран то, ICO получает 0,75 балла, если 1-2 - 0,5 балла, в противном случае 0. Компания считает, что чем больше стран исключено, тем больше вероятность того, что после ICO будет неудовлетворенный спрос.

KYC / AML

Максимально - 1 балл; ICO, требующие, чтобы все участники прошли тщательный KYC, получают 1 балл, если нет - 0. KYC во время ICO увеличивает шансы на то, что токен будет указан в листингах на основных криптовалютных биржах.

Совместимость токена с стандартами ERC20 или NEP-5

Максимально - 1 балл; ICO с токеном, соответствующим стандарту ERC20 получает 1 балл, совместимый с NEP-5 0,5 балла, несовместимый - 0 очков. Авторы считают, что совместимость с основными криптовалютными стандартами с соответствующей инфраструктурой, такими как легкие кошельки, должна значительно увеличить число потенциальных инвесторов, желающих купить, и, что важно, хранить токены в приватном (а не в обменном) кошельке.

2.1.4.2 Качественные показатели

Команда

Максимально - 6 баллов. Связанные профили ключевых членов команды (качество заполнения профиля, есть ли в списке проект ICO, есть ли другие компании, в которых члены команды являются текущими сотрудниками), количество сотрудников, прошлый

опыт членов команды (насколько это актуально, в каких компаниях они работали в прошлом, какие позиции они занимали и на какой срок), насколько члены команды дополняют друг друга, насколько способна команда реализовывать вовремя этапы дорожной карты, была ли команда успешной в достижении предыдущих основных этапов проекта (если таковые были). Как долго члены основной команды работают друг с другом.

Советники (Advisers)

Максимально - 2 балла. Каков был прошлый опыт соответствующих советников, есть ли какие-либо высокопоставленные имена в списке (например, Крис Скиннер или Дон Таскпотт), которые могут вызвать шумиху вокруг проекта. Есть ли свидетельства того, что перечисленные советники действительно «советуют» «Проект (связанные профили, статьи в СМИ, блоги и т. Д.).

Значимость и идея

Максимально - 4 балла. Целевой объем рынка, есть ли необходимость в технологии блокчейн, есть ли место для сетевого эффекта, есть ли необходимость в токенах, готовы ли потенциальные клиенты платить за криптовалюту, есть ли инновационная идея, есть ли у проекта устойчивые конкурентные преимущества, какое влияние на криптовалютную индустрию будет иметь проект;

Экономика токенов

Максимально - 1 балл. Нужно смотреть, есть ли юз кейсы для токенов или нет. Как много драйверов для повышения стоимости токенов есть в природе.

Дорожная карта

Максимально - 1 балл. Насколько детально разработана дорожная карта, насколько близки к ключевым вехам находится дата ICO, как долго не будет новостей после ICO, насколько амбициозны и в то же время достижимы этапы «дорожной карты».

Продуктовая стадия

Максимально - 4 балла. Имеет ли проект рабочий продукт, MVP, код на Github или, по крайней мере, закрытый прототип будущего продукта. При отсутствии публичного прототипа, ищутся доказательства существования разработки продукта, в соответствии с дорожной картой проекта. Наличие прототипа не только повышает легитимность проекта, но и значительно повышает шансы на то, что токен будет указан в листингах на крупных криптовалютных биржах после ICO.

ICO с рабочим продуктом получают 4 балла, при наличии MVP - 3 очка, проекты с кодом на Github (или любой другой системе контроля версий) получают 2 балла, с закрытым прототипом 1 балл. Если проект является исключительно бумажным или имеет только макет, он получает 0 баллов.

Конкурентная среда

Максимально - 1 балл. Есть ли конкуренты в криптопространстве (если нет конкурентов вне криптопространства), какова их оценка (стоимостная) и как она выглядит в сравнении с оценкой проекта после ICO. Чем выше оценка проекта, тем выше рейтинг. Например, максимальный рейтинг проставляется проекту, который по меньшей мере в 6 раз менее ценен на этапе ICO, чем ближайший конкурент;

Партнерские отношения

Бонусно - 1 балл. Имеет ли проект партнерские отношения с хорошо зарекомендовавшими себя организациями перед ICO. Есть ли какие-либо доказательства того, что партнерство действительно обеспечено. Неаккумулируемые логотипы разных компаний, заявленных как партнеры на веб-сайте ICO, не учитываются.

Юридическое лицо

Бонусно - 1 балл. Проверяется, есть ли действующий бизнес за ICO с рабочими продуктами и известными партнерами, или же компания была создана в последнее время.

Например, SelfKey создается и поддерживается основателями KYC Chain, которые могут использовать существующие партнерские отношения в интересах SelfKey и которые доказали свою легитимность и навыки ведения бизнеса.

Листинг на криптобиржах

Бонусно - 1 балл. Если проект заключил сделку с любыми биржами из ТОП-100 (с точки зрения ежедневного объема торгов) и раскрыл сделку перед ICO. Это редкость в большинстве случаев, однако некоторые проекты могут обеспечить сделку с некоторыми биржами перед ICO. Обменники и биржи, которые не входят в ТОП-100, не рассматриваются, поскольку предполагается, что существует высокая вероятность того, что биржи и обменники могут оказаться мошенническими.

План распределения средств ICO

Максимально - 1 балл. Есть ли четкий план? Какова детализация плана? Отражает ли это поведение компании? Какой % из бюджета выделяется на маркетинг (выделение более 35% на маркетинг это очень плохо, поскольку сбор средств для дальнейшего увеличения шумихи вокруг проекта - это не то, чего ищут).

2.1.4.3 Hype – метрики

Сообщество в Telegram

Максимально - 2 балла и бонусно – 1 балл. Формула для расчета этого показателя так же проста: (количество подписчиков в телеграме группы ICO) / 10 921. 10 921 - это среднее число пользователей телеграма, которые успешно реализовали проекты во время этапа ICO. Это число будет постоянно меняться, по мере добавления новых проектов в список.

Отзывы

Максимально - 2 балла и бонусно – 1 балл. Производится обзор нескольких веб-сайтов и блогов, которые привлекают большую часть внимания криптовального сообщества и имеют собственную методологию оценки проектов. Во-первых, вычисляется количество обзоров, делается оценка, а затем корректировка этой оценки, в соответствии с общим выражением отзывов, которые мы рассматриваем в процессе ранжирования.

Если общее настроение положительное, то мы умножаем рейтинг на 1,5; если отрицательное, то умножаем на 0.5, а если общее настроение нейтрально, мы судим исключительно по количеству отзывов.

Список блогов и сайтов, на которые мы смотрим: crushcrypto, ICOdrops, Ian Balina, TheGobone, OhHeyMatty, ICObench, Hacked, Coinbloq. Если ICO был рассмотрен 7 или более блогерами, проставляется оценка в 2 балла, если 5 или 6 – проставляется оцкенка в 1.75 балла, если 3 или 4 – проставляется оценка в 1.35 балла, если 1 или 2 - 0.75 балла, в противном случае – 0.

Качество коммьюнити

Максимально - 1 балл. Для оценки качества связи просматриваются основные каналы коммуникаций. Прежде всего, рассматривается количество различных социальных сетей и совместных платформ, на которых представлен ICO. Затем осуществляется оценка того, как команда реагирует на вопросы сообщества, оценивается качество ответов, скорость и этику ответов, предоставляемых командой.

Оценивается, способна ли команда поддерживать общественную заинтересованность в своем проекте путем создания и публикации новостей в социальных сетях о разработке

своего проекта. Оценивается интервью с учредителями и другими информационными агентами. Способность команды поддерживать общественный интерес имеет решающее значение для успеха проекта после ICO.

Если вышеперечисленные пункты соблюдаются командой, проект получает 1 балл, если нет – 0.

Наличие FUD

Максимально - 0 баллов, минимально -2 балла. FUD означает страх, неопределенность и сомнения инвесторов. Это оценка впечатления инвесторов, резко снижающая стоимость токенов и финансовые результаты ICO.

FUD появляется, когда возникают некоторые существенные неопределенности в отношении проекта. Например, DADI был пойман за политический плагиат, что значительно подорвало доверие к этому проекту в криптопространстве. Это пример случая, когда проект получает оценку -2. У ArcBlock также был FUD, поскольку было раскрыто только 4 основных члена команды. Все остальные инженеры и программисты остались скрыты.

Баунти / реферальная программа

Максимально - 1 балл. Если ICO запускает баунти или реферальную программу, оно получает 0, если нет - 1 балл.

2.1.5 Методика Icomarks

Компания Icomarks учитывает следующие параметры при скоринге ICO проектов [6]

Профиль ICO

Эта отметка определяется объемом информации о ICO. Самая подробная информация положительно влияет на рейтинг, например:

- Общая информация (описание, видео, white paper и т.д.);
- Финансовая информация (платформа, тип токена, цена, hard && soft cap и т.д.);
- Основные этапы проведения ICO;
- Ссылки и деятельность в социальных сетях;
- Публичная информация о команде и советниках.

Социальная активность

Постоянное обновление новостей проекта и большое количество подписчиков в социальных сетях (Twitter, Facebook и Telegram) положительно влияют на оценку присутствия в социальных сетях.

Оценка домена

Эта отметка показывает авторитет веб-сайта и рассчитывается на основе многих факторов, таких как: Alexa Rank, количество обратных ссылок, возраст домена и другие.

KYC команды

Эта оценка становится выше, если члены команды и советники имеют ссылки в социальных сетях (например, LinkedIn, Twitter, Facebook и другие) и активно обновляют свой контент.

Продукт

Эта оценка определяется вручную экспертами ICOmarks. Прежде всего, они оценивают рыночный потенциал продукта, потому что для проекта недостаточно просто выпускать свои токены. В будущем токены проекта должны быть востребованы. Это один из самых важных факторов.

Эта оценка также зависит от стадии реализации проекта: просто концепция, мок-ап, альфа / бета-версия или готовый продукт. Анализ конкурентной среды и актуальность проблемы, которую продукт должен решить.

Бизнес

Эта отметка вручную определяется экспертами ICOmarks. Они проверяют, имеет ли компания высококачественный и разработанный технический документ, включающий подробное описание технических аспектов продукта. Долгосрочный план развития компании (дорожная карта) с конкретными целями, разбитыми по периодам. Продуманный план эмиссии и распространения токенов.

2.1.6 Методика ICOBazaar

Система рейтинга состоит из взвешенной формулы с пятью факторами [7], каждый из которых оценивает какой-то отдельный аспект проекта или ICO - вес каждого фактора определялся опытными специалистами ICObazaar в области блокчейна и финансов и отражал воспринимаемую относительную важность каждого из них , Шестой фактор состоит из рейтинговой оценки (по шкале 0-5), сделанной отраслевым экспертом-консультантом / инвестором отдельно от команды ICObazaar. Каждый из пяти факторов, оцененных ICObazaar, подробно описан ниже в нашей методологии.

Методология рейтинга

Система оценки ICObazaar предназначена для оценки общего качества и жизнеспособности продукта, команды и технической реализации позади любого данного ICO. Чтобы сформулировать оценку для любого проекта и ICO, мы оцениваем каждый из них, оценивая следующие пять факторов:

- Идея проекта + техническая документация
- Команда
- Медиа и коммьюнити
- Техническая реализация
- Веб-сайт

Каждый из этих пяти факторов оценивается по шкале 0-5, и каждому из них присваивается определенный вес. Как указано выше, шестым фактором является рейтинг (ы) оценки (также по шкале 0-5), предоставленный одним или несколькими отраслевыми экспертами в соответствии с их индивидуальными критериями, независимо от критериев и методологии ICObazaar. Экспертный фактор также имеет определенный вес и предел, описанный ниже.

Weight-Adjusted Formula

ICObazaar использует формулу, скорректированную по весу, для оценки ICOs. Каждый из этих шести факторов имеет свой собственный удельный вес (в десятичной форме), сумма которого равна 1. Формула суммирует каждый из этих шести факторов для получения одного класса для каждого проекта, работающего на ICO.

Формула оценивания следующая:

$$Grade = \sum_{k=1}^{n} W * R$$

где:

- W – вес
- R - рейтинг

Ниже представлено описание разбалловки по рейтингу.

(R1) Идея проекта + Техническая документация

- Финансовый план
- Дорожная карта
- Состав
- Техническое объяснение
- Использование токена
- Релевантность продукта
- Продукт (есть MVP)
- Качество презентации продукта / идеи (маркетинг)

(R2) Команда

- Уровень опыта
- Публичность / прозрачность членов команды
- Офлайн-присутствие
- Качество консультантов / партнеров

(R3) Media + Community

- Наличие СМИ
- Размер онлайн-сообщества
- Качество Web / Социальное присутствие

(R4) Техническая реализация

- Динамика рынка
- Условное депонирование
- Доступность смарт-контракта
- Тип блочной цепи

(R5) Веб-сайт

- Количество локализаций (охват рынка)
- Наличие юридических условий и политик
- Общее качество

(R6) Экспертный рейтинг

Этот рейтинг создается отдельными экспертами в области блокчейна и финансов, критерии и методология оценки которых являются проприетарными и действуют независимо от ICObazaar.

Расширенная формула выглядит следующим образом:

$$Grade = (R_1 * w_1 + R_2 * w_2 + R_3 * w_3 + R_4 * w_4 + R_5 * w_5) * W_1 + R_6 * W_2$$

Где:

- W_1- вес рейтинга экспертов ICObazaar
- w- вес каждого фактора, определенного командой ICObazaar

w – вес каждого фактора, определенный специалистами ICObazaar.

$$\sum_{1}^{5} w_n = 1$$

Распределение рейтинга и оценок (по версии ICObazaar)

Оценка	Рейтинг	Описание рейтинга	
5	AAA	Наивысшее	Инвестиционная оценка
4.5	AA	Выше среднего	
4	A		
3.5	BBB	Нижняя средняя	
3	BB	Спекулятивная	Спекулятивная оценка
2.5	B	Высоко спекулятивная	
2	CCC	Огромный риск	Высокий риск
1.5	CC	Экстремальный риск	
1	C	Минимальный шанс на успех	По умолчанию
0.5	DD	По умолчанию	
0	D		

Таблица 1. Распределение рейтинга и оценок (по версии ICOBazaar)

Описание основных рейтинговых категорий:

Инвестиционная оценка. Проекты в этой категории имеют чрезвычайно высокий потенциал для краткосрочного и долгосрочного роста. Инвестиции в эти проекты имеют высокий потенциал возврата инвестиции и роста прибыли.

Спекулятивная оценка - развитие и позитивный рост проектов в этой категории неопределены. Инвестиции в эти проекты считаются рискованными, однако есть вероятность, что указанные инвестиции можно будет вернуть.

Высокий риск. Проекты в этой категории должны рассматриваться как очень рискованные инвестиции. Некоторым элементам реализации проекта, команды и / или ICO не хватает качества. Шансы проектов в этой категории, позитивно развивающихся в краткосрочной или долгосрочной перспективе, очень низки.

По умолчанию - проекты в этой категории являются крупными инвестиционными красными флагами. У них есть критические проблемы с бизнес-моделью и / или техническими возможностями. Существует минимальная вероятность того, что проекты в этой категории окажутся объектом для прибыльных инвестиций.

2.1.7 Методика Icoscoring

Методология анализа основана на подходах [8], используемых при оценке проектов, привлекающих венчурные инвестиции. Она основана на работах признанных авторитетов венчурной экосистемы - Джоша Лернера и Стивена Каплана, а также на персональном опыте основателей компании. В венчурную методологию внесены корректировки учитывающие особенности ICO.

Система оценки, разработанная командой проекта, основана на анализе важнейших параметров любого проекта: продукт, рынок, команда, бизнес-модель и финансы. Окончательный рейтинг каждого проекта производится путем оценки 35 критериев проекта.

Компания выносит следующие категории для вынесения вердикта:

Команда

- Полнота команды: области ответственности разделены; ключевые компетенции закрыты;
- Члены команды имеют большой опыт работы в данной отрасли, с использованием конкретных технологий;
- Мотивация участников согласована: у руководства есть доля, учредители готовы вкладывать собственные средства в развитие проекта.

Продукт

- Текущая стадия разработки продукта: альфа-версия, прототип, рабочий образец и т.д. Видно ли на GitHub или любой другой системе контроля версий динамику развития продукта (исходный код)?
- Отзывы клиентов: мнение о проекте в Интернете (комментарии, социальная активность, регулярные обновления для коммьюнити);
- Уровень приспособляемости: высокотехнологичные / качественные НИОКР;

Рынок

- Размер и масштаб рынка: региональный или глобальный, объем в деньгах;
- Высокие темпы роста целевого рынка;
- Соответствие компании тенденциям рынка;
- Состояние конкурентной среды в этом сегменте рынка;

Финансы

- Предоставляет ли компания адекватные текущие и достижимые, основанные на показателях, прогнозные финансовые показатели?
- Сравнение оценок: проект, который привлекает средства и его аналог, который успешно привлек венчурное финансирование;
- Оценка объема привлеченных инвестиций - проверка соответствия запрашиваемого финансирования целям и статьям затрат по сравнению с случаями с открытого рынка;

Бизнес модель

- Как технология Blockchain может изменить бизнес и его операционные и финансовые аспекты;
- Анализ типа и роли токена;
- Гарантии для инвесторов (условное депонирование, гарантии от незаконного присвоения средств и изменения команды в случае неэффективного управления);
- Соответствует ли модель компании действующей правовой структуре.

2.1.8 Методика Coingecko

CoinGecko представляет Gecko ICO Score [9], который объединяет рейтинги различных влиятельных лиц и веб-сайтов обзора ICO. В настоящий момент мы используем 20 источников для объединения показателя ICO Gecko.

Поскольку различные рецензенты и веб-сайты используют разные методы подсчета очков, мы нормализуем баллы до общего знаменателя перед вычислением среднего балла, основанного на упоминаниях о нашем счете ICO Gecko. Наш счетчик Gecko ICO использует 5-звездную рейтинговую систему, причемs 5 звезд являются лучшими, а 1 звезда - наихудшей.

Это источники, которые используют для расчета нашего показателя ICO Gecko:

- CrushCrypto
- Cryptobot
- CryptoBred
- CryptoBriefing
- CryptoRated
- DiddyCarter
- Ian Balina
- ICOCrunch
- ICO Drops
- ICO HotSheet
- Рыночные данные ICO
- Рейтинг ICO
- Midgard Ventures
- Lendex
- Liu
- Mandy
- OhHeyMatty
- Picolo
- Sergio
- TheGobOne

Ниже приведена формула, которую мы используем для нормализации оценок среди разных рецензентов:

Ian Balina и OhHeyMatty:

Эти рецензенты больше не делят свою электронную таблицу ICO и только упоминают в своих видеороликах YouTube, заинтересованы ли они или не заинтересованы в конкретном ICO. Мы награждаем 5 звезд, если они заинтересованы, и 1 звезда, если они не заинтересованы.

- Интересует - 5 звезд
- Не интересует - 1 звезда

Sergio, ICO HotSheet, CryptoBot, Lendex и Liu

Эти рецензенты используют систему оценки 1-100. Мы награждаем следующие звезды, основываясь на их оценках:

- 80-100 - 5 звезд
- 60-79 - 4 звезды
- 40-59 - 3 звезды
- 20-39 - 2 звезды
- 1-19 - 1 звезда

CryptoBriefing и Midgard Ventures

Эти рецензенты используют систему подсчета очков 0-10. Мы награждаем следующие звезды, основываясь на их оценках:

- 7,5-10,0 - 5 звезд
- 5,5-7,4 - 4 звезды
- 3,5-5,4 - 3 звезды
- 1,5-3,4 - 2 звезды
- 0,1-1,4 - 1 звезда

CryptoRated, ICOCrunch, ICO Market Data и Picolo

Эти рецензенты используют систему подсчета очков 0-5. Мы награждаем следующие звезды, основываясь на их оценках:

- 4,5-5,0 - 5 звезд
- 3,5-4,4 - 4 звезды
- 2,5-3,4 - 3 звезды
- 1,5-2,4 - 2 звезды
- 0,1-1,4 - 1 звезда

CryptoBred

CryptoBred использует систему счисления 1,2 и 3 звезды. Мы награждаем следующие звезды, основываясь на их оценках:

- 3 звезды - 5 звезд
- 2 звезды - 3 звезды
- 1 звезда - 1 звезда

TheGobOne

TheGobOne использует систему оценки S, A, B, C, D. Мы награждаем следующие звезды, основываясь на их оценках:

- S - 5 звезд
- A - 4 звезды
- B - 3 звезды
- C - 2 звезды
- D - 1 звезда

DiddyCarter

DiddyCarter использует систему Бычьего, Хорошего и Нейтрального очков. Мы награждаем следующие звезды, основываясь на их оценках:

- Бычий - 5 звезд
- Хорошее - 4 звезды
- Нейтральный - 3 звезды

Mandy

Мэнди использует систему Go, Get on Exchange и Neutral scoring. Мы награждаем следующие звезды, основываясь на их оценках:

- Go - 5 звезд
- Получить на бирже - 4 звезды
- Нейтральный - 3 звезды

CrushCrypto

CrushCrypto оценивает ICO на своем плюшевом и долгосрочном потенциале холдинга. Он оценивает вероятность перевертывания и долгосрочного удерживания, используя следующие оценки: Хороший, Нейтральный, Отрицательный. Мы награждаем следующие звезды, основываясь на их плюшевом / долгосрочном потенциале холдинга:

- Хорошее / Хорошее - 5 звезд
- Хорошее / Нейтральное - 4 звезды
- Нейтральный / Хороший - 4 Звезды
- Нейтральный / Нейтральный - 3 звезды
- Нейтральный / Отрицательный - 2 звезды
- Отрицательный / Нейтральный - 2 звезды
- Отрицательный / Отрицательный - 1 звезда

ICODrops

ICODrops использует систему с высоким, средним, нейтральным, низким и без рейтинговой оценки. Мы награждаем следующие звезды, основываясь на их оценках:

- Высокий - 5 звезд
- Средний - 4 звезды
- Нейтральный - 3 звезды
- Низкий - 2 звезды
- Не оценено - 1 звезда

Рейтинг ICO

Рейтинг ICO использует положительную, стабильную, рискованную, отрицательную систему подсчета очков. Мы награждаем следующие звезды, основываясь на их оценках:

- Положительно - 5 звезд
- Стабильный + - 4 звезды
- Стабильный - 3 звезды
- Рискованный - 2 звезды
- Рискованный + - 1 звезда
- Отрицательный - 1 звезда

Пример расчета оценки ICO в Gecko

(Нормализованный показатель Яна Балины + Нормализованный показатель CrushCrypto + Нормализованный рейтинг рейтинга ICO + Нормализованный показатель TheGobOne + Нормализованный показатель DiddyCarter) / 5 Mentions

Примерно в таком духе и рассчитывается рейтинг на основе этой методологии.

2.1.9 Методика Icoplum

2.1.9.1 Алгоритм оценки

В нашем алгоритме оценки мы делим оценку на 4 разные группы [10]. ICO можно оценивать несколько раз в день, а рейтинг не может быть изменен вручную. Все ICO оцениваются в одном и том же состоянии по одному и тому же алгоритму оценки. Следовательно, мы рассматриваем эту часть рейтинга как цель.

Это зависит от команд ICO, их деятельности, их самопожертвования и их реакции на запросы нашего редактора, если их профиль обновлен и имеет потенциал для оценки.

Каждый посетитель, пользователь или член команды ICO может проверить результаты профиля ICO с помощью нашего инструмента анализатора ICO, который доступен. Инструмент был выпущен, чтобы помочь командам ICO стать лучше, более прозрачными и активными в своих кампаниях ICO.

Команда

Наличие хорошей команды - один из ключей к успеху. Инвесторы, как правило, исследуют каждого члена команды, а более опытные члены ICO - это дополнительная ценность.

Мы проверяем количество членов команды, фотографии, полные имена и ссылки в социальных сетях. Существует дополнительный плюс для членов с успехом в ICO в команде. Это члены команды, которые участвуют или участвуют в двух или более ICO (либо в качестве советника, либо в команде), и из-за этого считается более надежным.

Информация ICO

Предоставление всей необходимой информации очень важно для потенциальных инвесторов. Не показывать всю информацию или ее отсутствие можно воспринимать как неуверенность или неопределенность. Есть несколько данных ICO, которые мы принимаем во внимание в этой группе - все, начиная с даты начала и окончания ICO и заканчивая тикером.

Представление продукта

Потенциальные инвесторы хотят понять продукт и узнать о планах и целях после ICO на будущее. Никаких планов не равно интересам.

В презентации продукта мы рассмотрим технический документ, основные этапы и видеопрезентацию. Мы не оцениваем контент и его оригинальность, а скорее доступность информации.

Маркетинг и социальные сети

Привлечение потенциальных инвесторов и поддержание открытого общения с ними является одним из важнейших ключей кампании ICO.

Мы следим за деятельностью в разных социальных сетях, что дает нам лучший обзор того, как взаимодействовать с командой ICO со своими потенциальными инвесторами. Даже если индустрия ICO не будет тесно связана с аудиторией в конкретной социальной сети, важно присутствовать везде, чтобы все инвесторы могли говорить о проекте.

2.1.9.2 Эксперты

Мы рекомендуем нашим специалистам следовать следующей методологии оценки. Каждый эксперт может оценить любой ICO, которого он или она хочет, а затем может также изменить эту ставку. Эксперты оценивают себя независимо, и мы обычно не ставим под сомнение их решения и мнения. Единственный случай, когда мы будем вмешиваться в вопросы, - это случаи, когда эксперт будет оценивать ICO, частью которого он является. Мы также не позволяем экспертам давать плохие ставки своим конкурентам только потому, что они выше в таблице лидеров. Уровень каждого эксперта взвешен в отношении его или ее опыта, многолетнего опыта работы на местах и возможных доступных публикаций. Мы рассматриваем эту часть рейтинга как субъективную.

Рейтинг от 1 до 5 присваивается ICO для команды, видения и продукта. Эксперты должны подумать о следующих рекомендациях при оценке ICO.

Команда

Команды с сильными и заслуживающими доверия членами, которые могут продемонстрировать приверженность времени и прошлые проекты.
Codebase на разных платформах и коммитах.
Сообщество и согласованный поток информации, обновляемый с прогрессом проекта.

Продукт

Уровень зрелости продукта. Рабочие продукты легче судить, чем концепции. Технологии. Эксперты рассматривают, есть ли какая-либо технология (blockchain, non-blockchain). Проблема. Как и в традиционной экономике, команды ICO должны решать конкретные проблемы с их продуктом / сервисом. Карта продуктов, которая показывает краткосрочные и долгосрочные стратегии и рост. Конкурентный анализ, отражающий приверженность проекта пониманию рыночной конъюнктуры.

Бизнес стратегия

Рыночный потенциал и количество существующих пользователей.
Краткосрочная и долгосрочная бизнес-стратегия.
Текущие инвестиции.
Оценка и распределение токенов, показывающие ограничение рынка и процесс эмиссии и ценообразование на токенах.

Отказоустойчивость

Правовое понимание и готовность адаптироваться к изменяющимся нормам.
Безопасность, условное депонирование и список советников.

2.1.9.3 Краткие юридические обзоры

Некоторые из ИСО были также оценены нашими партнерами - юридическими экспертами, которые предоставили короткий юридический обзор. Эти эксперты по правовым вопросам предоставляют свои обзоры самостоятельно, и полные правовые обзоры рассматриваются как оплачиваемая услуга, предоставляемая экспертом-юристом.

2.1.10 Методика Coindelite

Используется методика [11] сильно схожая со всеми остальными, вышеописанными. Эксперты вручную проставляют определенные баллы за бизнес модель, оценку технологической инновационности и так далее. В целом, очень схоже со всем тем, что было описано выше.

2.2 Анализ источников

Все существующие методологии скоринга финансовых рисков ICO проектов, как минимум, частично повторяют друг друга. Практически все методологии в своей оценке учитывают следующие категории для проставления баллов:

- Продукт
- Рынок
- Команда
- Бизнес-модель
- Финансы
- Юридическое лицо
- Технология
- White-paper

Каждая из описанных методологий предлагает свои собственные модели оценивания, так или иначе использующие вышеперечисленные категории. Разница заключается лишь в том, что каждая из методик использует свою собственную, уникальную формулу для оценивания ICO.

Кроме того, некоторые методологии учитывают индивидуальные мнения отдельно взятых экспертов из криптосообщества либо же используют усредненную и агрегированную оценку других вендоров по оцениванию ICO проектов.

2.3 Выбор методов исследования

2.3.1 Методы экспериментально-теоретического уровня

Для осуществления исследования будут использованы следующие методы:

- Эксперимент: предложенные модели скоринга финансовых рисков ICO проектов будут проверены экспериментально.
- Анализ: детальный анализ существующих аналогов и решений, с целью глубокого погружения в предметную область и понимания недостающих решений и точек для генерации нового научного знания.
- Индукция: с помощью индукции будет выведена общая модель скоринга финансовых рисков ICO проектов, с целью понимания того, что нужно учитывать при оценивании проектов.
- Гипотетический: в процессе исследования выдвигаются гипотезы относительно некоторых эмпирических особенностей оценки.

2.3.2 Методы теоретического уровня

Для осуществления исследования будут использованы следующие методы:

- Обобщение: следует из анализа существующих решений и аналогов.
- Идеализация: в процессе исследования будет выведена модель «идеального» ICO проекта, который будет использоваться в качестве эталонного значения.
- Формализация: оценка финансовых рисков будет формализована с помощью математических знаков и обозначений.
- Анализ и синтез: из большого количества критериев и параметров будут изучены все существующие. Впоследствии, будет собрана итоговая модель скоринга финансовых рисков.

3 Риски ICO и блокчейн проектов

Финансовые риски ICO проектов можно классифицировать по конечному держателю риска. Конечными держателями риска могут быть следующие категории:

- Команда проекта;
- Инвесторы проекта;
- Компании, продающие товары и услуги ICO проектам и блокчейн компаниям.

Для команды проекта рисками являются потеря средств после привлечения капитала, провал кампании по привлечению средств, падение стоимости токена в будущем, привлечение средств, полученных незаконным путем и будущие затраты на правовое и техническое урегулирование вопроса.

Для инвесторов проекта это риски, связанные с потерей вложенных средств из-за их хищения создателями проекта или третьими лицами, а так же, риск падения стоимости токенов в будущем, что означает потерю потенциальной прибыли от инвестиций в проект.

Для третьей группы рисками являются потеря репутации, отсутствие прибыли при оказании услуг, банкротство клиента при модели работы за выручку от привлеченных средств.

Таким образом, при рассмотрении всей картины в целом, можно выделить следующие факторы риска (их обоснованность следует из дальнейшего исследования, описанного ниже):

- ***Команда проекта***. Является большим фактором риска сразу по нескольким причинам: благонадежность команды и состоятельность команды. Благонадежность команды отражает действительное желание использовать привлекаемые средства для реализации предложенного проекта, а не желание привлечь и похитить средства. Состоятельность команды отражает способность команды реализовать предложенный проект.
- ***«Чистота» привлекаемого капитала.*** В связи с появлением регулирования криптовалютной индустрии, важность «чистоты» привлекаемого капитала набирает свои обороты. Поскольку ICO проекты попадают под правовое регулирование, актуальное для рынка ценных бумаг, привлечение средств незаконным путем обрекает проект на непредвиденные расходы и судебные тяжбы.
- ***Бизнес модель проекта***. Влияет на общую инвестиционную привлекательность. Без правильной бизнес модели проект не будет прибыльным и не соберет достаточное количество капитала. Кроме того, бизнес модель влияет на будущую цену токена на криптовалютных биржах, что невероятно важно для инвесторов, использующих ICO в качестве спекулятивного инструмента.
- ***Информационная безопасность***. Личная информационная безопасность команды проекта и безопасность программного обеспечения и технической инфраструктуры является невероятно важным аспектом, поскольку уровень защищенности напрямую влияет на вероятность хищения всех привлеченных средств.

Фактор риска «Информационная безопасность» не является очевидным. Не является очевидным и факт того, что риски информационной безопасности являются финансовыми рисками. Поскольку для хищения всех средств достаточно похитить приватный ключ проекта, любую кибератаку стоит расценивать как непосредственный финансовый риск. С целью выявления конкретных типов рисков, связанных с информационной безопасностью, было проведено два исследования: первое изучило реальные атаки на ICO проекты, находящиеся под защитой команды Group-IB и публично доступные кейсы, а второе было проведено мной с целью изучения всех успешных кибератак на блокчейн проекты. Причиной, из-за которой изучались не только ICO проекты, но и блокчейн проекты по типу криптовалютных кошельков, бирж и т.д., является зависимость безопасности одного от другого. Так, например, при взломе криптовалютного кошелька, проект может потерять все

свои средства по независящем от самого проекта причинам. Следовательно, любое место, кто может произойти потеря средств, является риском для ICO проекта.

Риски, связанные с бизнес-моделью проекта не будут описываться в этом разделе, поскольку проанализированные источники литературы обеспечивают практически полный охват всего того, что можно про них написать. Еще одно описание тех же самых рисков не добавляет научной новизны работе.

3.1 Риски информационной безопасности

3.1.1 Атаки на ICO проекты

3.1.1.1 Кража White Paper

Одна из особенностей проектов блокчейн-индустрии — это полная открытость и прозрачность. Большая часть разработок и исходных кодов публикуется в открытом доступе. Очевидно, что в первую очередь команда публикует WP.

Совсем недавно был зарегистрирован интересный случай, когда злоумышленники смогли заработать на копировании чужого проекта. Схема выглядит очень просто: берется легитимный, хорошо проработанный White Paper на русском языке, делается его полная копия через Google Translate, создается лендинг с описанием проекта, новой командой (фейковой, естественно) и новым брендом [12]. Проект грамотно раскручивается в Сети: появляется контекстная реклама, огромные треды на [13] и так далее.

Например, специалисты из компании [14] обнаружили, что владельцы проекта Wi-Fi Global [15] скопировали и перевели WP команды worldwifi.io. Если присмотреться внимательно, Wi-Fi Global — это всего лишь немного переработанный вариант World Wi-Fi. При этом сообщество в «Телеграме» у Wi-Fi Global насчитывает две с лишним тысячи человек и, по словам участников проекта, им удалось привлечь 500 тысяч долларов на pre-ICO.

3.1.1.2 Компрометация аккаунтов

Поскольку на сайте проекта обычно имеется детальная информация обо всех членах команды, разведка для злоумышленников существенно упрощается. Ни для кого не секрет, что в Сети содержится огромное количество дампов утекших паролей. Если скомпрометированный пароль используется где-то еще, то это может привести к крайне нежелательным последствиям — не только для владельца аккаунта, но и для проекта и инвесторов.

Именно такая неприятная история приключилась с авторами проекта Enigma [16]. Хакеры успели заработать полмиллиона долларов еще до того, как была анонсирована дата проведения ICO. Атакующие смогли скомпрометировать веб-сайт Enigma и несколько аккаунтов в социальных сетях.

Основатели проекта — выходцы из Массачусетского технологического института. Исполнительный директор постоянно использовал простые и повторяющиеся пароли для своих аккаунтов. Благодаря этому хакеры получили доступ к адресу его электронной почты (на которой не было двухфакторной аутентификации). Естественно, завладеть доступом к другим сервисам и аккаунтам, привязанным к адресу, не составило труда. Следом были скомпрометированы учетные данные других членов команды. Злоумышленники получили доступ к странице enigma.co (сайт, на котором производилась продажа токенов, не был скомпрометирован) и мессенджеру Slack [17].

Получив доступ к enigma.co, хакеры разместили там анонс продажи токенов, написали об этом в Slack в чате для сообщества и сделали почтовую рассылку по украденному списку. Все это — чтобы распространить свой адрес, на который предлагалось перевести токены. Всего им удалось собрать 1492 ETH — порядка полутора миллионов долларов.

3.1.1.3 Дефейсы

Все самое плохое, как правило, происходит именно в день ICO. Шквал DDoS атак одновременно с наплывом пользователей, лавина сообщений в канал проекта в Telegram и Slack, спам по списку рассылок.

Самое обидное, что может произойти, — дефейс сайта во время ICO. Цель хакеров очень простая: поставить на официальный портал проекта свой кошелек и собирать средства на него.

Жертвой такой атаки стал проект CoinDash [18]. Во время ICO сайт CoinDash был взломан, хакеры выставили на главной странице проекта нелегитимный кошелек. Понятное дело, что все инвесторы ринулись закидывать криптовалюту не на кошельки CoinDash, а на хакерские. Жертвами атаки стали больше двух тысяч инвесторов, потеряв в совокупности около 37 000 ETH.

Команда проекта оказалась порядочной и возместила ущерб инвесторам, попавшимся в руки хакеров.

Фишинг встречается почти всегда, когда на ICO выходит более-менее известный проект. Рассылка мошеннических писем, как правило, сопровождается мощной DDoS-атакой на сайт проекта. Смысл всего этого очень прост: хакеры копируют содержимое сайта, делают похожий домен и выкладывают в интернет. Ничего необычного здесь нет, все как и всегда. В случае с ICO создаются фиши двух типов: первый тип заточен под кражу приватного ключа пользователя, второй просто просит перекинуть криптовалюту на адрес кошелька или смарт-контракта.

Как кто-то может оставить на сайте мошенников приватный ключ? Не кажется ли это подозрительным? Увы, когда в деле замешано желание быстро обогатиться, случается еще и не такое. Судя по Etherscan [19], люди иногда делают и повторные переводы, ничего при этом не получая взамен.

По статистике компании Chainalysis [20], около 56% всех средств, украденных с ICO, были похищены с помощью фишинговых атак. Примерная оценка ущерба от фишинга — 115 миллионов долларов. По данным Group-IB [21], крупная фишинговая группировка зарабатывает от 3 тысяч до 1 миллиона долларов в месяц. Сейчас фишинг — самый популярный способ хищения средств у инвесторов. В разгар «криптовалютной лихорадки» все стремятся как можно быстрее купить токены (зачастую они продаются с большой скидкой) и не обращают внимания на такие мелочи, как кривые домены.

Типичная схема — злоумышленники покупают контекстную рекламу в поисковых движках, организовывают лавину сообщений в мессенджерах и любыми способами стараются нагнать трафик на фишинговый сайт. В общем, при желании можно даже ввести показатель инвестиционной привлекательности проекта, подсчитав количество фишинговых сайтов, сделанных на его основе.

Есть очень хороший проект [22] где агрегируют фишинг по ICO. В его базе насчитывается 2533 вхождения. Существенно для столь молодой индустрии. Для одного только MyEtherWallet [23] зарегистрировано 2206 фишинговых доменов.

3.1.1.4 Хищение средств после ICO

Самый плохой вариант для любой ICO-команды — потерять средства после успешного сбора. Это случается из-за неаккуратного обращения с криптовалютой, уязвимостей в смарт-контрактах и зиродеев в популярных кошельках. И даже если отбросить уязвимости в собственном ПО, риск потери средств в остальных случаях нивелировать достаточно сложно.

Хороший пример — проект The DAO [24], у которого атакующие смогли украсть [25] как минимум 53 миллиона долларов. Другой пример — проект aeternity, у которого было похищено [26] 30 миллионов долларов через зиродей-уязвимость в кошельке Parity.

Уязвимости смарт-контрактов активно изучаются сообществом. Например, в работе ученых из Университета Кальяри [27] описаны разные техники эксплуатации.

Существуют и попытки повысить безопасность — к примеру, утилита Oyente [28] проверяет смарт-контракты на уязвимости в автоматическом режиме.

Скорее всего, «криминальные» смарт-контракты еще найдут свое применение в мире высоких технологий. Например, в научной работе «Кольцо Гига: исследование будущего криминальных смарт-контрактов» [29] исследователь Ари Юэльс и его коллеги рассматривают варианты того, как можно использовать смарт-контракты во вред.

3.1.1.5 Нивелирование рисков

Самая уязвимая часть любого проекта — это его команда. Плохая защита персональных аккаунтов, отсутствие элементарной культуры компьютерной гигиены зачастую приводит к тому, что аккаунты мессенджеров и соцсетей компрометируются и атакующие получают возможность рассылать ссылки на фишинговые сайты налево и направо, дискредитировать команду, менять данные на сайтах и так далее. Хуже этого может быть только компрометация приватных ключей от криптовалютных кошельков.

Итак, вот что нужно сделать, чтобы проведение ICO не было омрачено криминалом.

1. Защита от DDoS-атаки. Практически каждый раскрученный проект сталкивается с атаками этого типа. Лучше заранее озаботиться качественной защитой от DDoS. Недоступность сайта зачастую отталкивает потенциальных инвесторов от вложений.
2. Защита команды проекта. Все члены команды должны защитить свои персональные аккаунты в социальных сетях, поставить двухфакторную аутентификацию, внедрить парольные политики.
3. Информационная безопасность приложений. Естественно, нужно проверить все на наличие уязвимостей и сделать качественные настройки доступа к критичным службам на серверах.
4. Проверка смарт-контрактов на наличие известных уязвимостей. Нужно как минимум просканировать их автоматическими средствами.
5. Обучите комьюнити распознавать фишинг. Это относительно простая и дешевая мера, которая позволит существенно обезопасить потенциалных инвесторов от потери средств.

3.1.1.6 Выводы

Проанализировав более полутора сотен атак на блокчейн-проекты (биржи, обменники, кошельки, фонды), мы пришли к выводу, что основная масса проблем кроется в уязвимости самих криптосервисов, использующих технологию блокчейна. В случае с Ethereum криптосервисы сталкиваются как с уязвимостями в собственных смарт-контрактах, так и с хорошо изученными проблемами вроде дефейсов, компрометации аккаунтов и фишинга. Зачастую хакерам даже не нужно знать особенности работы смарт-контрактов и тонкости работы блокчейна. Традиционные и хорошо отработанные методы отлично работают при хищении криптовалюты у пользователей.

Риски информационной безопасности являются одними из самых критических с точки зрения сохранности инвесторских денег, поскольку первый взлом может стать последним. Если проект не заботится об информационной безопасности, то средства инвесторов находятся в огромной опасности.

3.1.2 Атаки на блокчейн проекты

3.1.2.1 Введение

С 2011 года хакеры стали обращать пристольное внимание биткоин-биржи. Как мы покажем далее, хакеры успешно применили все традиционные методы кибератак на блокчейн проектах. Вообще говоря, хакерам не нужно ничего знать о технологии блокчейн, кроме того, для чего нужен приватный ключ от кошелька. Успешные атаки невероятно выгодны для злоумышленников, поскольку они могут заработать миллионы долларов при осуществлении одной успешной атаки с относительно низкой вероятностью быть

пойманными. Более того, псевдоанонимные свойства криптовалют позволяют злоумышленникам относительно безопасно и просто заниматься обналичиванием и отмыванием похищенных средств.

В связи с крупным ажиотажом вокруг ICO проектов и криптовалютами, хакеры начали перефокусироваться с традиционных кибератак на банки на атаки на Blockchain проекты. Криптовалютный рынок - очень динамичный рынок, на котором правовое регулирование практически отсутствуют, а скорость внедрения и разработки новых технологий невероятно высокая. Темпы развития рынка очень высоки, и именно скорость развития является одной из причин отсутствия должного внимания к кибербезопасности. Без должного внимания к кибербезопасности, команды блокчейн проектов теряют деньги из-за простых ошибок. Например, известно много случаев, когда хакеры успешно применяли брутфорс атаки, используя старые пароли или примитивные методы социальной инженерии для кражи приватных ключей от криптовалютных кошельков. Сами же свойства безопасности, присущие технологии блокчейн, не спасают пользователей от самих себя.

В большинстве случаев, главной целью злоумышленника является кража приватного ключа. Лицо, управляющее приватным ключом, является владельцем криптовалюты в кошельке. Безопасное хранение приватных ключей от криптовалютных кошельков является наиболее важным аспектом использования криптовалют. Без приватных ключей невозможно подписать транзакцию и использовать криптовалюту в качестве средства оплаты. Как правило, наиболее прибыльными целями для хакеров являются криптовалютные кошельки, обменники, биржи и другие платформы, у которых в обращении имеется большое количество криптовалюты.

В 2017 году большое количество команд привлекло деньги через ICO. Сумма привлеченных средств превысила то, что было поднято на ранних этапах финансирования с использованием венчурного капитала. Различные блокчейн стартапы собрали более 1,25 миллиарда долларов [30]. Естественно, частные инвесторы начали использовать криптовалюты в качестве инвестиционного или спекулятивного инструмента. Даже пенсионеры начали отслеживать биржевые котировки и извлекать прибыль от торговли. Блокчейн проекты достигли пика своей популярности.

2017 год стал очень прибыльным годом для хакеров. Основными целями для атак были проекты ICO. Почти каждый крупный ICO проект столкнулся с значительным количеством DDoS-атак и фишинговых атак на своих инвесторов. Хакеры смогли украсть 225 миллионов долларов из привеченного через ICO капитала (в эфире) [31]. Интересно, что почти 50% украденных средств были похищены с помощью фишинга.

Существует множество различных атак на саму систему блокчейна: от использования значительных объемов вычислительной мощности сети (атака 51%) до довольно сложных методов [32]. Однако такие методы не так широко распространены на практике. Традиционная эксплуатация уязвимостей или повторное использование учетных данных доминируют в инструментарии атакующего. Мы видели несколько случаев, когда использовались атаки, нацеленные на саму технологию блокчейн.

Мы проанализировали различные ресурсы, доступные в открытом доступе и собрали данные об успешных инцидентах. В анализ вошли только те случаи, в которых были похищены значительные суммы денег. В этом исследовании не содержится информации о теоретических векторах атак на блокчейн системы. Мы не учитываем многочисленные случаи фишинга в проектах ICO или случаи хищения криптовалюты отдельных лиц при общем подсчете статистики. Случаи мошенничества и случаи плагиата с white paper мы относим к социальной инженерии и тоже не включаем в общую статистику.

Блокчейн проекты, попавшие в исследование, можно классифицировать следующим образом (если кража была совершена во время проведения ICO - мы используем категорию «ICO»):

- Криптовалюта
- Криптовалютная биржа

- ICO
- Оборудование для майнинга
- Майнинг пул
- Платформа
- Частное лицо
- Криптовалютный кошелек

При проведении исследования мы выявили следующие типы атак:

- *Блокчейн атаки* при осуществлении которых использовались конкретные аспекты технологии Blockchain. Например, это может быть так называемая атака 51% [33] или атака подмены транзакций [34].
- *Повторное использование учетных данных* - примеры использования скомпрометированных паролей, доступных в публичных утечках. Например, когда злоумышленник находит пароль от учетной записи электронной почты в Интернете, а этот пароль совпадает с паролем из учетной записи пользователя facebook, злоумышленник, теоретически, может туда зайти. Другим случаем повторного использования учетных данных является атаки перебора по словарю, когда злоумышленник пытается войти в систему, используя огромное количество пар (логин, пароль) для входа, чтобы получить доступ к системе. Атаки по словарю - широко распространенный метод, используемый в настоящее время, и, соответственно, он очень популярен среди хакеров, которые пытаются совершить кражу с небольших криптовалютных бирж, где политики безопасности существенно более низкие.
- *Domain hijacking* [35] - случаи изменения сведений о регистрации домена. Например, хакеры изменяют А-записи и перенаправляют трафик веб-сайта на вредоносный сервер для сбора данных (логин, пароли) или повторных запросов на пересылку средств.
- *Инсайдерские атаки* - случаи, при которых один или несколько основных членов команды используют свой доступ к информационным системам для кражи приватных ключей или другой чувствительной информации.
- *Вродоносное ПО* - примеры использования специально разработанного вредоносного программного обеспечения для кражи конфиденциальной информации. Мы обнаружили вредоносное ПО для персональных компьютеров и устройств на базе операционной системы Android. Программное обеспечение может быть похитителем паролей, бэкдором или любым другим вредоносным файлом, способным помочь злоумышленнику получить конфиденциальную информацию или удаленный доступ к системе.
- *Фишинг* - случаи, использования нелегитимной копии веб-сайта с очень походим доменом или поддельных версиях веб-сайтов элкетронной почты для кражи конфиденциальной информации или загрузки вредоносного ПО на компьютер жертвы. Другой атакой, которую мы также классифицируем как фишинг, является атака восстановления SIM-карты. В этом типе атаки злоумышленник делает функциональную копию SIM-карты жертвы для получения SMS-сообщений от поставщика услуг двух факторной атуентификации или использует уязвимости SS7 для перехвата SMS-кодов.
- *Уязвимости в исходном коде* - использование логических ошибок или каки-либо уязвимых местах в программном обеспечении, используемом компанией.

Целевые атаки широко распространены на практике, поэтому читатель должен понимать, что почти каждая успешная атака на криптовалютный обменник является целевой атакой. Мы не будем выделять целевые атаки в отдельную категорию в исследовании, потому что мы хотим показать рабочие тактику, методы и процедуры

злоумышленников, а так же, мы хотим использовать подробную классификацию типов атак (см. Таблицу 1).

Зачастую, никаких технических подробностей об инцидентах взлома попросту нет, поэтому мы используем наиболее разумную причину успешной атаки, если нет точной информации об инциденте.

3.1.2.2 Успешные атаки на блокчейн проекты

Во время кибератаки хакер обычно пытается украсть криптовалюту из кошельков. В некоторых проектах криптовалюта хранится в горячих и холодных кошельках (горячие кошельки - это кошельки, которые подключены к Интернету, холодные кошельки не подключены к Интернету. Обычно холодные кошельки расположены на отдельном устройстве без подключения к Интернету), некоторые из них их нет. Как мы покажем позже в исследовании, иногда есть способы украсть криптовалюту даже из холодных кошельков. Украдена может быть не только криптовалюта, но и любая другая конфиденциальная информация, такая, например, как база данных с учетными данными пользователей. Такие угрозы, как переиспользование парольной информации и кража баз данных несут за собой, как правило, не только финансовый ущерб, но и репутационный.

Данный раздел делится на подтемы. Каждая подтема представляет собой отдельный тип атаки и состоит из описания инцидента безопасности с нанесенным ущербом.

3.1.2.2.1 Блокчейн атаки

Krypton && Shift [36] (Криптовалюта). 29.08.2016. Похищено: 21 465 KR ~ $ 3000

Этот случай представляет атаку 51% [33] в проекте, основанном на блокчейне Ethrereum. Поскольку использовался форк блокчейна Ethereum, злоумышленники смогли использовать большую часть вычислительной мощности в сети, чтобы украсть токены. Команда проекта подозревает, что атака, возможно, была просто пробой осуществления подобных атак на блокчейн Ethereum.

Mt. Gox [37] (Криптовалютная биржа). 25.02.2014. Похищено: 740 000 BTC (всего), 386 BTC через блокчейн атаку.

Самая большая кража биткоинов, известная до сих пор. В июне 2011 года [38] Mt.Gox была взломана в первый раз из-за взломанного компьютера аудитора компании. Атакующий использовал украденные учетные данные для перевода 2000 BTC со счетов клиентов на бирже. Затем было похищено 740 000 биткоинов. Mt. Gox утверждают, что была применена атака с подменой транзакций, но исследователи в работе [39] продемонстрировали, что только 386 биткоинов были связаны с транзакциями для атак с подменой транзакций. Точные сведения о краже биткоинов до сих пор неизвестен.

The DAO [40] (ICO). 17.06.2017. Потеря: 3 600 000 ETH

Атакующий использовал уязвимость в смарт-контракте и вывел весь эфир с основного кошелька, на котором он хранился. The DAO был самым большим ICO в истории (на момент выхода). Команда The DAO собрала более 100 миллионов долларов. Уязвимость была обнаружена, и злоумышленник вывел более 3,6m ETH. Эксплуатация уязвимостей в смарт контрактах - очень мощный и многообещающий способ хищений криптовалюты. В сообществе исследователей обсуждаются варианты потенциального применения смарт контрактов в криминальных целях [87].

3.1.2.2.2 Повторное использование учетных данных

Bitcoinica (криптовалютная биржа) [41]. похищено: 40 000 BTC.

Bitcoinica была скомпрометирована дважды. В первый раз была успешно осуществлена атака, при которой все пароли были скомпрометированы. Второй взлом произошел из-за мастер-пароля программы LastPass, который был копией пароля скомпрометированного во время предыдущего взлома. Разработчик Bitcoinica использовал API ключ биржи Mt.Gox в

качестве пароля для веб-сайта в программе «LastPass». Поэтому хакеры смогли украсть биткоины из аккаунта на Mt.Gox, принадлежащего Bitcoinica.

Bter [42] (Exchange). Похищено: 7170 BTC.

Холодный кошелек проекта был скомпрометирован. Никаких технических подробностей об инциденте нет.

CoinDash [43] (ICO). Похищено: 43 438 ETH.

Хакеры смогли изменить публичный адрес кошелька для сбора средств на легитимном веб-сайте ICO. В результате весь эфир был отправлен в кошелек хакеров. Такая атака - так называемый дефейс. Однако, наиболее вероятной причиной успешности атаки является повторное использование парольной информации. Задача изменения контента веб-сайта становится достаточно тривиальной, если известен пароль от аккаунта в хостинг провайдере.

Enigma [44] (ICO). Похищено: 1492 ETH.

Enigma столкнулась с большим количеством проблем со скомпрометированными учетными записями: ее сайт был взломан вместе с аккаунтами в социальных сетях всех членов команды. С помощью отправки спама, хакеры собрали почти 500000 долларов за короткий промежуток времени. Злоумышленник опубликовал сообщения в мессенджере Slack, изменил веб-сайт и подделал электронные письма, которые отправлялись по списку адресов электронной почты участников сообщества. Пользователи обнаружили [45], что доступ к электронной почте генерального директора Enigma был доступен хакерам. Пароль от электронной почты был доступен в Интернете. Однако, тот же пароль использовался для разных рабочих учетных записей без двухфакторной аутентификации.

Cointerra [46] (Оборудование для майнинга). Сумма хищения неизвестна.

Различные адреса электронной почты членов команды были скомпрометированы специально для внесения изменений в запросы на поставки устройств для майнинга. Вероятно, некоторое количество устройств было отправлено не в те руки.

Steemit [47] (Платформа). Похищено: ~ 80000 долларов Steem

Учетные записи пользователей были скомпрометированы, а небольшое количество долларов Steem было украдено.

Inputs.io [48] (Cryptocurrency кошелек). Похищено: 4100 BTC

Хакер скомпрометировал учетную запись хостинга, используя старые учетные данные из очень старых учетных записей электронной почты. Атакующий обошел 2FA из-за некачественного внедрения на стороне сервера. Были похищены не только биткоины, но и база данных с учетными записями пользователей.

3.1.2.2.3 Атаки инсайдеров

Bitfinex [49] (Криптовалютная биржа). Похищено: 120000 BTC.

Биткоины были украдены из обособленных кошельков пользователей. Наиболее вероятный ход событий - это инсайдерская атака.

Mintpal [50] (Криптовалютная биржа). Похищено: 3700 BTC.

Инцидент произошел в июле 2014 года, когда компания сообщила, что она была «взломана». Один из владельцев Mintpal похищенные биткоины через биржу LocalBitcoins, что сделало проведение расследования инцидента достаточно простым.

796 [51] (Криптовалютная биржа). Похищено: 1000 BTC.

Хакеры поменяли адрес для вывода средств. Подробный анализ журнальных файлов показал, что система была обновлена за несколько дней до возникновения инцидента. Вероятная инсайдерская атака.

CryptoRush [52] (Криптовалютная биржа). Похищено: 950 BTC.

Главной версией коммьюнити биржи является кража биткоинов самими владельцами.

PicoStocks [53] (Криптовалютная биржа). Похищено: 6000 BTC.

Злоумышленник использовал старые ключи PicoStocks, чтобы украсть криптовалюту как с горячих, так и с холодных кошельков. Главным объяснением причины возникновения инцидента является инсайдерская работа.

Bit LC [54] (Криптовалютная биржа). Похищено: 2 000 BTC.

Уникальный случай: средства в горячих кошельках были в безопасности, но криптовалюта в холодных кошельках была похищена. Вероятно, один из владельцев похитит средства, поскольку, он исчез сразу после кражи.

3.1.2.2.4 Вредоносное ПО

ShapeShift [55] (Криптовалютная биржа). Похищено: 469 BTC, 5800 ETH.

Хакеры воровали криптовалюту с горячих кошельков биржи три раза в течение двух недель. Системный администратор установил бэкдор на другую машину разработчика. После этого он использовал свои собственные ключт, чтобы опустощить горячий биткоин-кошелек и уничтожил ключи разработчика, чтобы покрыть следы. Команда ShapeShift перенесла свое программное обеспечение на облачный хостинг и удалило учетные записи системных администраторов для повышения безопасности. Второй злоумышленник купил доступ к бэкдору и похител средства с горячих кошельков, когда биржа ShapeShift еще не была в общем доступе. ShapeShift снова перешел на другой хостинг. Атакующий снова использовал доступ к бэкдору и опустошил горячие кошельки с биткоинами и эфиром.

Exco.in [56] (Криптовалютная биржа). Похищено: 2000 BTC.

Первоначальное исследование показало, что во время DDoS-атаки две отдельные сделки вышли из-под контроля из-за ошибки или эксплойта и передали очень большое количество биткоинов в другую учетную запись. Один из пользователей биржи смог получить доступ ко всем биткоинам на бирже Exco.in.

Cryptsy [57] (Криптовалютная биржа). Похищено: 13000 BTC.

Хакер внедрил троян в исходный код Cryptsy. Загруженное вредоносное ПО позволило хакеру переводить биткоины и лайткоины из хранилища Cryptsys. Злоумышленник известен созданием и развитием проекта Lucky7Coin [58].

Yapizon [59] (Криптовалютная биржа). Похищено: 3816 BTC.

Хакер скомпрометировал четыре горячих кошелька криптовалютной биржи. Пока еще неясно, как произошел инцидент, но слухи говорят, что использовалось вредоносное ПО.

Allinvain [60] (Частное лицо). Похищено: 20000 BTC.

Личный компьютер Allinvain был скомпрометирован. Файл wallet.dat был попросту украден и все биткоины со счетов были похищены.

3.1.2.2.5 Фишинг

Bithumb [61] (Криптовалютная биржа). Похищено: 340 BTC.

Хакеры похитили личную информацию о 31800 пользователях сайта Bithumb, включая их имена, номера мобильных телефонов и адреса электронной почты (3% клиентов). Большая часть средств была украдена с использованием «голосового фишинга», где мошенники вызванивают жертв по одному и представляются, как представители Bithumb, запрашивая идентификационные номера на основе информации из Bithumb. Количество, о котором идет речь, было одноразовым паролем «жертвы», который предоставил злоумышленнику прямой доступ к средствам.

Bitstamp [62] (Криптовалютная биржа). Похищено: 18866 BTC.

Злоумышленники атаковали шесть сотрудников Bitstamp во время недельной фишинговой кампании. Атакующие использовали методы социальной инженерии для доставки файлов вредоносных программ с использованием персонализированных сообщений и интересов людей. Фишинг был полностью адаптирован и хорошо подготовлен. Системный администратор Bitstamp долго пытался получить членство в профессиональной организации. Хакеры использовали этот факт и сделали фальшивый файл, который, как считал системный администратор, был легитимным. Он загрузил файл и его машина была

скомпрометирована. После этого хакеры смогли получить доступ к двум серверам, содержащим файл wallet.dat для горячего кошелька Bitstamp и кодовой фразе для этого файла.

Различные ICO, блокчейн проекты и MyEtherWallet [63]. Похищено: ~150 миллионов долларов.

Фишинг на ICO широко распространен. Почти каждый крупный ICO проект сталкивается с этой проблемой. Фишинг на ICO проекты можно разделить на две отдельные категории: попытки кражи секретного ключа и запрос на перевод средств. Существует хороший ресурс, который собирает информацию о фишинговых версиях сайтов различных блокчейн проектов. Самым популярным ресурсом для создания фишинга является эфириуем-кошелек. Мы видели огромное количество фишинговых веб-сайтов и доменов на практике. Некоторые группы злоумышленников смогли заработать от 3000 до 1 000 000 долларов в месяц. Согласно данным Chainanalysis, более 50% всех доходов от киберпреступности на Ethereum, сгенерированных в 2017 году, было связано с фишингом.

На сегодняшний день лучшим фишинговым агрегатором является etherscamdb. С момента запуска (18.01.2018) от etherscamdb обнаружено 2581 фишинговых сайтов. Самый популярный проект для фишинга - MyEtherWallet с 2214 уникальными фишинговыми сайтами. Топ-10 блокчейн проектов по производству фишинга представлен на рисунке 1.

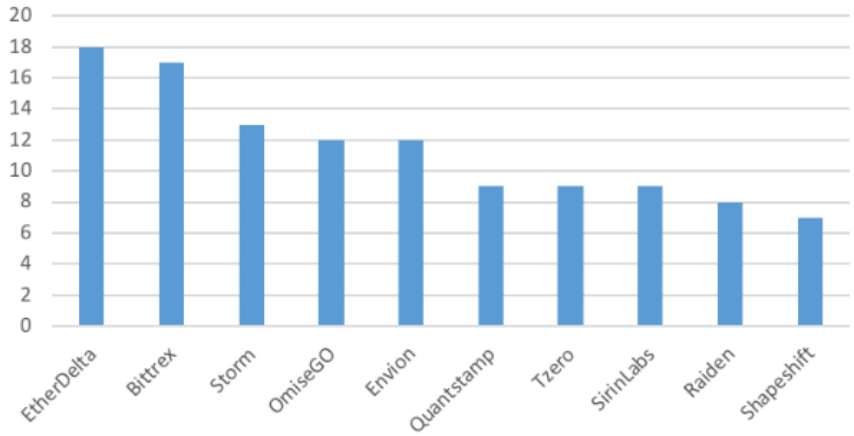

Рис. 1. Топ 10 блокчейн проектов по количеству фишинговых веб-сайтов

В среднем, на каждый проект приходится три фишинговых веб-сайта. Фишинг на ICO можно разделить на две категории: кражи личных ключей и запросы на перевод средств.

3.1.2.2.6 Уязвимости в исходном коде

FlexCoin [64] (Криптовалютная биржа). Похищено: 896 BTC.

Все монеты из горячих кошельков были похищены. Команда проекта Flexcoin держала основную массу биткоинов в холодных хранилищах, поэтому они были в безопасности. Атакующий вошел в интерфейс биржи под абсолютно новой учетной записью и успешно использовал уязвимость в клиентском исходном коде, которая позволяла перемещать средства между разными аккаунтами пользователей биржи. Отправляя тысячи одновременных запросов, злоумышленник переводил криптовалюту из одной учетной записи пользователя в другую до тех пор, пока отправляющая учетная запись не была перегружена до такой степени, что все балансы были обновлены.

BTC-E [65] (Криптовалютная биржа).

База данных BTC-E была скомпрометирована. Дамп базы данных доступен в открытом доступе. Средства на счетах пользователей не пострадали. Наиболее вероятной причиной взлома является SQL-инъекция, обнаруженная злоумышленником.

Cavirtex [66] (Криптовалютная биржа).

База данных с учетными записями пользователей была взломана. Средства украдены не были. Cavirtex вышел из бизнеса после взлома из-за сомнений в их репутации и отсутствии

необходимых мер безопасности. Нет никаких подробностей о взломе, но наиболее вероятной причиной является скомпрометированное программное обеспечение биржи.

GateCoin [67] (Криптовалютная биржа). Похищено: 185000 ETH + 250 BTC

Атака была проведена на горячие кошельки и в результате средства были потеряны. Все средства были сохранены в поддельных холодных кошельках. Атакующие модифицировали системы GateCoin, таким образом, что запросы проходили в обходи мультиподписей холодных кошельков и переходили напрямую на горячие кошельки.

BitFloor [68] (Криптовалютная биржа). Похищено: 24000 BTC

Атакующий скомпрометировал несколько серверов BitFloor и получил доступ к незашифрованной резервной копии ключей кошельков. Во время обновления один из сотрудников выполнил ручное обновление и переместил данные в незашифрованный раздел на своем диске.

Kipcoin [69] (Криптовалютная биржа). Похищено: 3000 BTC

Нападавший, очевидно, получил доступ к серверу Kipcoin и загрузил файл wallet.dat в это время. Затем хакер подождал и перевел деньги на собственные счета.

Poloniex [70] (Криптовалютная биржа). Похищено: 97 BTC.

В результате хакерской атаки Poloniex потеряла 12,3% совокупного количества биткоинов. Биржа был скомпрометирована ранее, с помощью неизвестной уязвимости в исходном коде. Официальным объяснением является следующее: «Хакер обнаружил, что если вы разместите несколько заявок на изъятие средств практически в одно и то же время, они будут обработаны в течение более или менее того же времени. Это приводит к отрицательному балансу, но валидных вставках в базы данных, данные из которой, затем, успешно используются для вывода средств».

Bitcurex [71] (Криптовалютная биржа). Похищено: 2300 BTC.

Пока неясно, как была совершена атака. Единственное, что мы знаем, это заявление, опубликованное администрацией Bitcurex: «В результате работы служб сторонних систем Bitcurex был поврежден внешним вмешательством через программный интерфейс при автоматическом сборе и обработке данных. Следствием этих действий является потеря части активов, находящихся под управлением bitcure.com ». Вероятно, злоумышленник смог найти секретные ключи в каталогах на сервере.

Bitcoin7 [72] (Криптовалютная биржа). Похищено: 11000 BTC.

Хакер смог получить доступ в сеть и проник в основное хранилище с биткоинами сайта и двум из 3 резервных кошельков. Кроме того, злоумышленник получил доступ к базе данных пользователей.

Coinapult [73] (Криптовалютная биржа). Похищено: 150 BTC.

Кошелек компании был скомпрометирован. Пока неясно даже с сообщением о том, использовал ли злоумышленник эксплойт или уязвимость в исходном коде. Эксплуатация уязвимостей, скорее всего, основана на доступной информации.

BIPS [74] (Криптовалютная биржа). Похищено: 1295 BTC

Хакеры скомпрометировали серверы с процессингом биткоинов и вытащили криптовалюту из кошельков клиентов. По данным источников, более 22 000 потребительских кошельков были скомпрометированы. Перед атакой хакеры начали атаку DDoS на BIPS в качестве маневра для отвлечения внимания.

Bitmain [75] (Оборудование для майнинга). Потеря: неизвестно

Хакеры скомпрометировали один из старых серверов Bitmain, и смогли похитить учетные записи клиентов компании. Точные причины инцидента недоступны в публичных источниках.

BTCGuild [76] (Майнинг пул). Похищено: 1254 BTC

После обновления произошла ошибка в программном обеспечении, с помощью которого выплачивались средства. 16 злоумышленников смогли воспользоваться ситуацией и похитили средства с горячих кошельков.

Ozcoin [77] (Майнинг пул). Похищено: 922 BTC

Злоумышленнику удалось взломать сервер Ozcoin, уничтожить веб-сайт и базу данных. Нападающему удалось изменить сценарий выплаты Ozcoin, поэтому все деньги были выплачены по его адресу.

Tether [78] (платформа). Похищено: $ 31 000 000 USDT

Хакер смог украсть 31 млн. Долл. США из-за уязвимости в программном обеспечении.

Linode [79] (облачный хостинг). Потери: 46653 BTC (всего для всех затронутых проектов).

Linode - это сервис, который позволяет клиентам настраивать и запускать виртуальные машины и использовать их в качестве хостинг-провайдера. Многие пользователи использовали Linode для работы с экосистемой биткоин. На хостинге находилось программное обеспечение, управляющие майнинг-пулами, биткоин биржами и т.д. Нападавшие смогли получить привилегии уровня технической поддержки клиентов, которые позволили ему узнать, какие клиенты держали биткоин кошельки на серверах этого хостинга. Затем, вору удалось войти в учетные записи из-за уязвимостей в программном менеджере Linode, который клиенты используют для настройки своей виртуальной машины, - перезагрузить компьютеры и изменить корневые пароли.

Parity [80] (Криптовалютный кошелек). Похищено: 153 037 ETH

Кошелек Parity был взломан дважды. Оба взлома были вызваны уязвимостями программного обеспечения.

Aeternity [81] (ICO). Похищено: 30 000 000 долларов США

Aeternity потерял деньги из-за эксплуатации 0day уязвимости в кошельке Parity, который использовался для хранения средств.

Moonco.in [82] (Криптовалютный кошелек). Потери: 4000 BTC.

Веб-сайт проекта был взломан. Нет технических подробностей, доступных в Интернете.

3.1.2.3 Анализ

Мы проанализировали 48 различных инцидентов безопасности (мы считаем фишинговые сайты различных проектов Blockchain единым инцидентом) и отнесли их к одной из категорий, упомянутых в качестве типа атаки. Мы собрали информацию о возвращенных средствах и о том, смог ли проект продолжить успешное функционирование после успешного осуществления взлома. Мы собрали всю информацию о потерях и инцидентах с криптовалютами.

Количество кибератак ежегодно увеличивается из-за восходящего тренда во внедрении технологии Blockchain (см. Рис.2). Существует тенденция к переходу на хищение криптовалюты вместо традиционных хакерских целей, поэтому мы прогнозируем, что в будущем будет еще больше кибератак на блокчейн проекты.

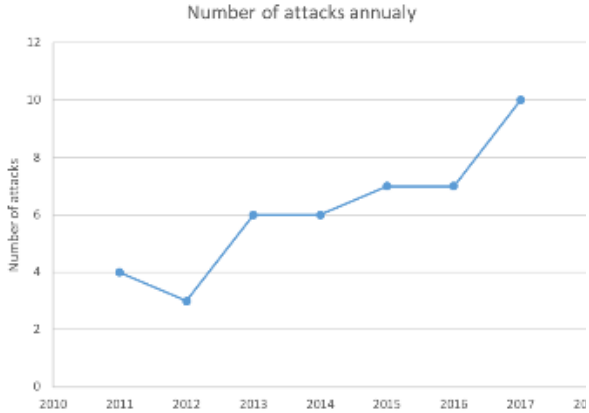

Рис. 2. Количество атак за год

Рис. 3. BTC украденные за год

Большинство украденных биткоинов были похищены в 2014 году (см. Рисунок 3). Это связано с инцидентом на японской бирже Mt.Gox. До сих пор нет достоверной информации о технических деталях взлома. Некоторые люди полагают, что BTC-e несет ответственность за кибератаку.

Как мы можем видеть на рис. 4, первая кибератака, в результате осуществления которой была похищена криптовалюта Ethereum была проведена в 2016 году. Первым проектом, у которого хакеры украли Ethereum, была криптовалютная биржа ShapeShift. Количество кибератак, нацеленных на хищение Ethereum, было намного большим, чем количество инцидентов с прицелом на биткоин в прошлом году, основной причиной которых являлся рост цен ETH и появление ICO с большой рыночной капитализацией. Ethereum - это новая технология даже по сравнению с Bitcoin, поэтому хакерам значительно увеличить прибыль от фишинга и различных проектов мошенничества.

Рис. 4. ETH украдено за год

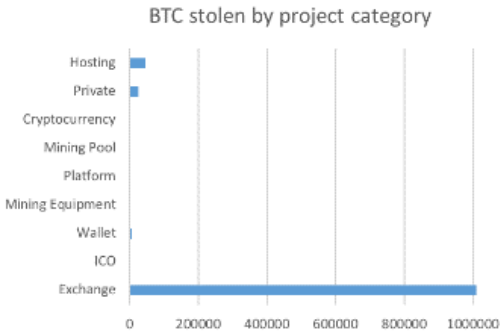

Рис. 5. BTC украдено по категориям проектов

Очевидно, что большинство украденных биткоинов, были получены из криптовалютных бирж (см. Рис.5). Криптоавлютные биржи по-прежнему является первичными целями для хакеров, которые перешли к атакам на блокчейн проектам из банковских кибератак.

С другой стороны, порог входа в кибератаки на Ethereum проекты значительно ниже (см. Рисунок 4), благодаря высокой эффективности фишинга.

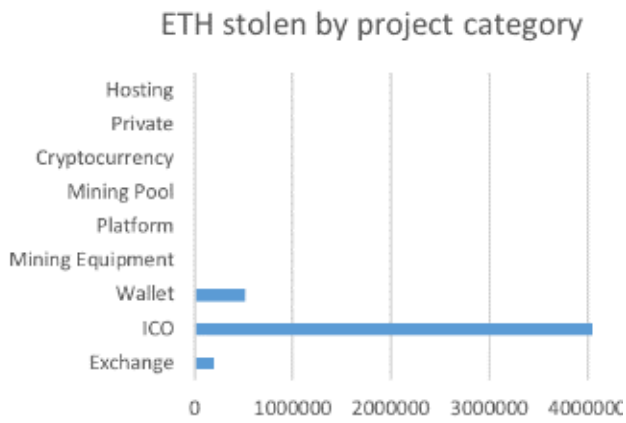

Рис. 6. ETH украдено по категории проекта

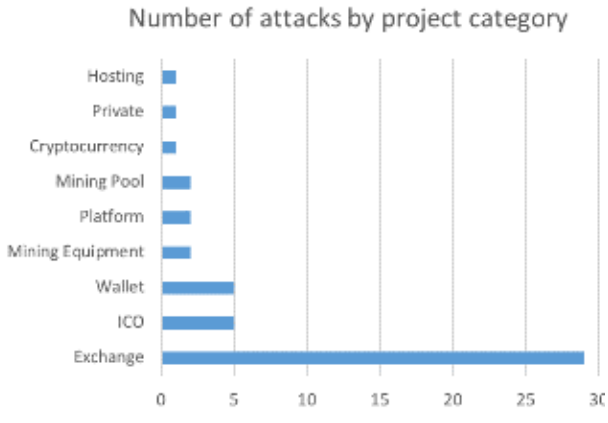

Рис. 7. Количество атак по категории проекта

Диаграмма показывает, что количество кибератак на криптовалютные биржи превосходит количество атак на все другие проекты. Вероятно, количество атак на проекты Ethereum, использующие специальные атаки, нацеленные на саму технологию блокчейн, будет увеличиваться из-за повсеместного внедрения смарт-контрактов и технологии блокчейн в глобальную экономику и управление цепями поставок (см. Рис. 6, 7, 8, 9).

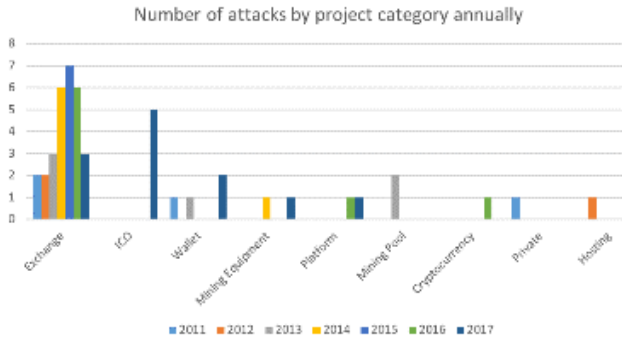

Рис. 8. Количество атак по категории проекта за год

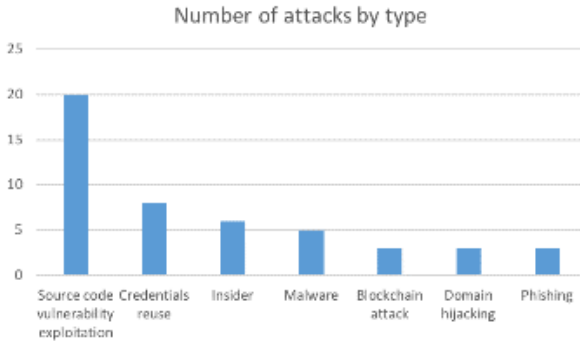

Рис. 9. Количество атак по типу

Использование уязвимостей исходного кода является распространенным типом атаки на блокчейн проекты. Любая часть уязвимого программного обеспечения может использоваться для кражи приватных ключей или любых других данных. Даже безопасность, обеспечиваемая самой технологией блокчейн, не защищает пользователей от повторного использования учетных данных, инсайдеров и вредоносных программ. Эти типы атак довольно популярны и достаточно мощны для кражи средств (см. Рис. 10, 11).

Большинство биткоинов были украдены с использованием уязвимостей в исходном коде, но большинство эфира было украдено с помощью специфических атак Blockchain: через уязвимость в смарт-контракте. Мы прогнозируем, что уязвимости смарт-контрактов привлекут больше внимания со стороны хакеров. Это совершенно новая область, а в мире мало компаний, которые могут успешно найти уязвимости в интеллектуальных контрактах.

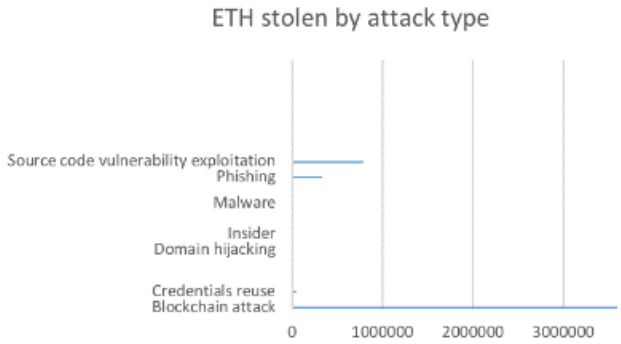

Рис. 10. ETH Украдено по типу атаки

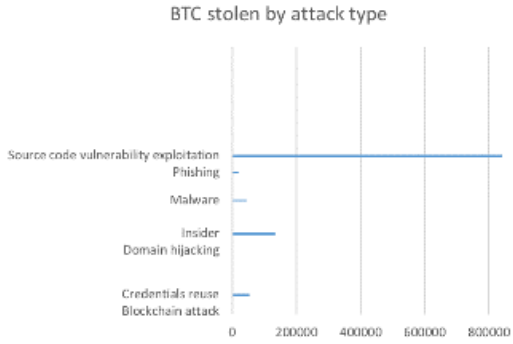

Рис. 11. BTC украдено по типу атаки

Статистика выживаемости проектов показывает, что большинство проектов погибло после кибератаки (59%), 46% проектов вернули деньги первоначальным инвесторам (см. Рис. 12, 13).

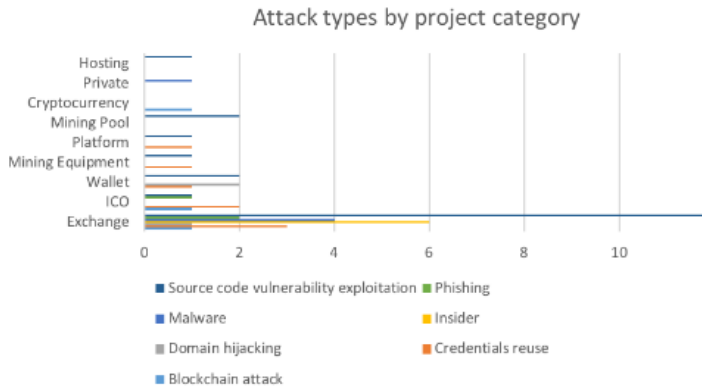

Рис. 12. Типы атак по категориям

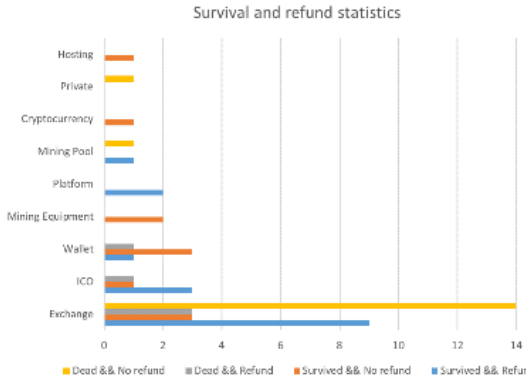

Рис. 13. Статистика по выжившим и умершим проектам

Project	Category	Attack type	Year
Krypton && Shift	Cryptocurrency	Blockchain attack	2016
Mt.Gox	Exchange		2014
The Dao	ICO		2017
Bitcoinica	Exchange	Credentials reuse	2012
Bter	Exchange		2015
CoinDash	ICO		2017
Enigma	ICO		2017
Cointerra	Mining Equipment		2014
Steemit	Platform		2016
MT.Gox	Exchange		2011
inputs.io	Wallet		2013
blockchain.info	Exchange	Domain hijacking	2016
BlackWallet	Wallet		2018
Classic Ether Wallet	Wallet		2017
Bitfinex	Exchange	Insider	2016
Mintpal	Exchange		2014
796	Exchange		2015
CryptoRush	Exchange		2014
PicoStocks	Exchange		2013
Bit LC	Exchange		2013
ShapeShift	Exchange	Malware	2016
Exco.in	Exchange		2015
Cryptsy	Exchange		2016
Yapizon	Exchange		2017
Allinvain	Private		2011
Bithumb	Exchange	Phishing	2017
Bitstamp	Exchange		2015
Various ICOs	ICO		2017
Flexcoin	Exchange	Source code vulnerability exploitation	2014
BTC-E	Exchange		2014
Cavirtex	Exchange		2015
GateCoin	Exchange		2016
BitFloor	Exchange		2012
Kipcoin	Exchange		2015
Poloniex	Exchange		2017
Bitcurex	Exchange		2016
Bitcoin7	Exchange		2011
Coinapult	Exchange		2015
BIPS	Exchange		2013
Bitmain	Mining Equipment		2017
BTCGuild	Mining Pool		2013
Ozcoin	Mining Pool		2013
Tether	Platform		2017
Linode	Hosting		2012
Aeternity	ICO		2017
Mt.Gox	Exchange		2014
Parity	Wallet		2017
Moonco.in	Wallet		2011

Таблица 2. Классификация кибератак на блокчейн проекты.

3.1.2.4 Дискуссия

Огромная сумма денег, украденная у инвесторов в ICO с помощью фишинг атаки, показывает нам, что даже с помощью надежных и прозрачных технологий, таких как блокчейн, люди не защищены от собственной глупости. Широкое применение фишинговых атак для проектов ICO представляет собой сложную и серьезную угрозу для всех пользователей криптовалют. Потенциальные инвесторы не защищены от этой угрозы, поэтому сообщество должно быть более внимательным к фишинговым атакам.

Повторное использование учетных данных - это еще одна проблема, которая очень важна для блокчейн проектов. Без надежной парольной политики не будет эффективной защиты от вторжений. Если команда разработчиков использует одни и те же пароли для всех криптовалютных кошельков и социальных сетей, возникновение кражи - это только вопрос времени.

Использование вредоносных программ и использование уязвимостей в исходных кодах - это старые и хорошо известные методы взлома, которые работают даже с новыми технологиями, такими как блокчейн, потому что всегда будут компьютеры, люди и машины с установленным программным обеспечением.

До сих пор мы видим, что не так много связанных с блокчейнами кибератак. Мы считаем, что при широком внедрении технологии блокчейн количество связанных кибератак значительно увеличится. Вероятно, основными целями для хакеров будут смарт-контракты и блокчейн платформы. Если злоумышленник сможет взломать блокчейн

платформу (например, Ethereum), последствия этого будут ужасными. При сильном экономическом фоне и способности ждать некоторое время нападающие получат большую прибыль от одной кибератаки.

3.1.2.5 Выводы

Значительное количество криптовалюты было украдено с начала 2011 года. В настоящее время специфические векторы атаки на блокчейн широко не распространены. Использование уязвимостей в исходном коде, повторное использование учетных данных и слабые политики хранения приватных ключей являются основными критериями успешных краж. В преступности, связанной с хищением биткоинов, криптовалютные обмены являются лучшими целями нападения, в таких организациях, как «Эфириум», гораздо больше шансов привлечь хакеров, поскольку на стадии производства не так много проектов Ethereum.

К сожалению, в основном нет никакой технической информации о деталях инцидента. При всей прозрачности блокчейна мы все еще не можем найти точные причины и детали проведенных краж. Индустрия должна повысить уровень внимания к проблеме кибербезопасности в блокчейн проектах. По нашему мнению, прозрачные отчеты об инцидентах могут помочь отрасли повысить уровень защищенности инвесторов и проектов.

3.2 Риски, связанные с командой проекта

3.3 Риски, связанные с «чистотой» привлекаемого капитала

Большим риском для команды ICO проекта и его инвесторов является риск привлечения средств, добытых незаконным способом. Например, могут быть привлечены средства, полученный с помощью отмывания фиатных денег, либо же своровванных у какого-либо юридического или физического лица. В некоторых юрисдикциях, например, в США, Сингапуре и Японии, привлечение средств, полученных незаконным путем, может лишить команду проекта легитимного статуса проекта и закрыть им выход на крупные рынки. Более того, если ICO проводится с юрисдикции, где обеспечивается строгое регулирование криптовалютного рынка, можно получить реальные тюремные сроки за привлечение такого капитала, поэтому необходимо проводить тщательную проверку инвесторских средств на их чистоту. Для этого активно используются методики, помогающие существенно улучшить процессы KYC.

Почему возникает такая сложность с проведением KYC процедур? Если при проведении IPO или традиционных краудфандинговых кампаний у компании эмитента есть возможность запрашивать паспортные данные, руководствуясь текущим законодательством, то в криптовалютном мире достаточно зарегистрировать личный кабинет, используя любой почтовый ящик (зачастую это не требуется) и перевести криптовалюту на указанный адрес. В связи с этим, достаточно трудно быстро определить источник заработка капитала.

В целом и общем, любая криптовалюта является псевдоанонимной (если в нее не было заложено специальных средств анонимизации транзакций, как, например, в Monero или ZCash) – т.е., все транзакции обозримы для абсолютно всех людей в мире, но атрибуция каждого конкретного кошелька к физическому или юридическому лицу неизвестна, поскольку не требуется прохождение процедуры идентификации личности при создании нового криптовалютного кошелька.

Для того, чтобы оценить легитимность происхождения криптовалюты, необходимо использовать специальные методы деанонимизации кошельков и транзакций. По сути, проверка на чистоту является скорингом кошелька. Чистота определяется разными методами, в том числе, отдалением от майнеров и проверенных криптовалютных бирж.

3.3.1 Методы деанонимизации криптовалютных транзакций

3.3.1.1 Модель угроз

Основная цель деанонимизатора – собрать большой массив данных, который позволит связать реальных людей или используемые ими IP-адреса с транзакциями и биткоин кошельками. Вместо реального имени пойдойдет, так же, электронная почта, номер телефона, имя пользователя или любой другой цифровой идентификатор транзакции.

Деанонимизатор может получить доступ ко всей публичной информации в Интернете: частные и общественные форумы, веб-сайты и социальные сети. Таким образом, деанонимизатор может выявить реальное имя конкретного человека, проанализировав всю доступную информацию. Другой подход заключается в «подслушивании» неточной информации о транзакциях у пользователей [83]. Например, деанонимизатор может подслушать «Элис, его Боб. Завтра утром я пошлю вам 45 $ биткоинов ».

Помимо общедоступной информации деанонимизатор может вводить вредоносные узлы биткоин-серверов в сеть, чтобы перехватывать IP-адреса и пытаться связать определенные транзакции с IP-адресами клиента. Если атакующий будет использовать оба вектора атаки вместе, он сможет повысить точность деанонимизации. Почти каждый метод деанонимизации состоит из двух фаз: фазы сбора данных и фазы анализа данных. Сбор данных может быть активным: используются вредоносные узлы (биткоин серверы) для подслушивания трафика и распространения адреса. Сбор данных может быть пассивным: анализ данных, собиранных из публичных блокчейнов без какого-либо взаимодействия с сетью.

3.3.1.2 Деанонимизация

Процесс деанонимизации представляет собой процесс связывания публичного адреса биткоина с цифровым идентификатором пользователя или его IP-адресом. Сам процесс делится на два уровня: сетевой уровень P2P и уровень транзакций.

Очень важно определить владельца публичного адреса биткоина. Мы определяем владельца публичного адреса биткоин кошелька как владельца соответствующего приватного ключа. Например, если биржа или веб-сайт используется для передачи биткоинов, а у пользователя нет доступа к приватному ключу, биржа или веб-сайт является владельцем биткоин кошелька.

Вопрос владения приватным ключом от криптовалютного кошелька это сложная задача. Например, если биржа хранит приватный ключ конкретного человека, то человек не может напрямую контролировать свои биткоины без биржи. Вместо этого пользователь использует внешнюю службу, которая управляет соответствующим приватным ключом.

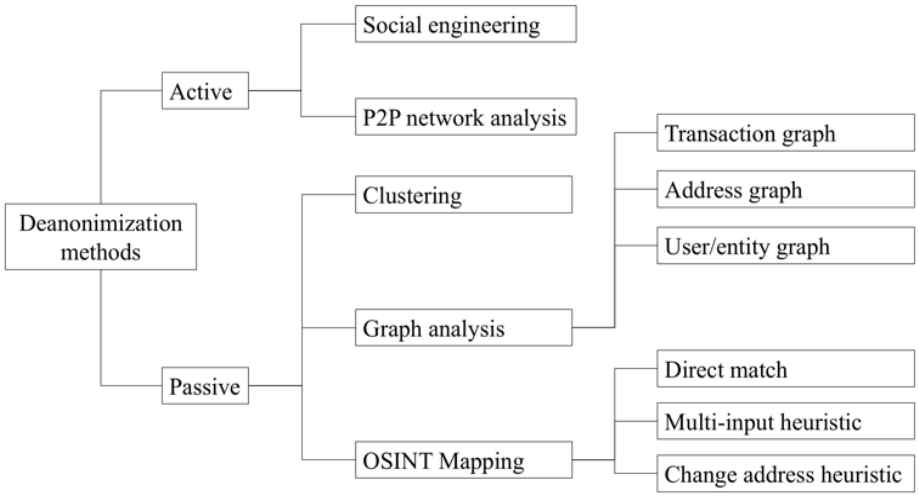

Рис. 14. Классификация методов деанонимизации

Методы деанонимизации (см. Рис.14) можно разделить на две категории: пассивные и активные.

Пассивные методы не взаимодействуют напрямую с одноранговой сетью bitcoin. Пассивные методы используют только данные, которые анализируются из блокчейна или любого другого публичного источника информации. Пассивные методы часто опираются на комплексные методы анализа графов и различные эвристики, связанные с протоколом биткоин.

Активные методы используют вредоносные узлы биткоина и методы социальной инженерии. Вредоносные узлы - это узлы с модифицированным программным обеспечением под контролем злоумышленника. Такие узлы используются для перехвата трафика или прямой связи с другими одноранговыми узлами в сети. Атаки социальной инженерии подходят для деанонимизации частично неизвестных пользователей в цепочке транзакций.

Open source intelligence on Bitcoin wallets.

Без внешней информации, собранной из разных источников, нет способа найти владельца биткоин кошелька.

Этап сбора информации может быть разделен на две разные категории: пассивный сбор и активный сбор. При активном сборе деанонимизатор пытается найти публичный адрес человека путем прямой связи с ним. Прямая связь - попытка установить контакт с целью и выяснить адрес во время разговора или запрос на платеж [84]. Этот метод является самым надежным, поскольку продавец не будет лгать о своем публичном обращении после сделки. Другой активный подход использует вредоносные узлы биткоинов для подслушивания трафика. Этот сценарий поможет злоумышленнику собрать IP-адреса. При пассивном сборе злоумышленник пытается собрать данные из разных источников, находящихся в открытом доступе. Существуют различные категории источников данных, в которых злоумышленник может находить цифровые имена пользователей биткоин-пользователей: веб-сайты, форумы, социальные сети, шахтные пулы, кошельки, банковские обмены, небанковские обмены, вендоры, азартные игры, биткоин миксерычы. Существуют различные сборщики информации, связанные с адресами кошельков, доступные в сети [85, 86].

Основная цель этапа сбора информации - собрать как можно больше тегов для публичных адресов биткоин кошельков, потому что почти каждый метод деанонимизации будет намного более эффективен на практике, если за ним будет стоять солидное количество данных.

Пассивные методы

1) *Прямое совпадение*

Это самый простой метод деанонизации. Злоумышленник пытается найти владельца адреса биткоина, с помощью поиска публичного ключа в общедоступных источниках. В случае успеха деанонимизатор найдет соответствующий цифровой идентификатор.

2) *Эвристика с несколькими входами*

Авторы статьи [87] предложили эвристику транзакций с несколькими входами. Операция с несколькими входами происходит, когда пользователь хочет выполнить платеж, а сумма платежа превышает значение каждого из доступных балансов биткоина в кошельке пользователя. Существующие клиенты Bitcoin выбирают набор BTC из кошелька пользователя и выполняют оплату посредством транзакций с несколькими входами. Прямой вывод из этого следует, что если эти BTC принадлежат различным адресам, то входные адреса принадлежат одному и тому же пользователю.

3) *Изменить эвристику адреса*

Изменяющиеся адреса: биткоин-сеть генерирует новый адрес, так называемый «теневой» адрес, с помощью которого отправитель платежа может получить сдачу. Используя эту эвристику, мы можем легко найти кошелек пользователя, с помощью

которого был отправлен перевод. Теневые адреса - это механизм, используемый для возврата денег плательщику, участвующему в транзакции, поскольку биткоины могут быть разделены только путем расходования средств.

Все методы, основанные на эвристиках, сильно зависят от метода прямого совпадения. Без правильно собранных данных все эвристики бесполезны.

4) *Кластеризация*

Авторы статьи [87] предложили методы кластеризации, основанные на двух предыдущих эвристиках. Использование первых эвристических исследователей позволило разделить сеть на 5 579 176 кластеров пользователей (они начались с 12 056 684 открытых ключей). Авторы использовали графы транзакций и графы адресов.

Авторы статьи [87] усилили вторую эвристику, предложенную в [88]. Если злоумышленник может идентифицировать теневые адреса, она может поэтому кластерировать не только входные адреса для транзакции (в соответствии с эвристикой 1), но также адрес изменения и самого пользователя. Кроме того, при пользовательском использовании протокола биткотнов можно указать адрес изменения для данной транзакции. До сих пор одно общее использование этой настройки, которую наблюдали авторы [87], заключалось в том, чтобы указать адрес изменения, который фактически совпадает с адресом ввода.

В целом, авторы предложили новую эвристику кластеризации на основе теневых адресов, позволяющую нам группировать адреса, принадлежащие одному и тому же пользователю. Используя предложенную технику, исследователи смогли идентифицировать основные учреждения (например, биржи и сайты азартных игр) и взаимодействие между ними, используя лишь небольшое количество идентифицированных транзакций.

5) *Фингерпринтинг*

В работе [89] авторы показывают, что сторонний веб-трекер может деанонимизировать пользователей криптовалюты. Например, когда кто-то платит на веб-сайте для покупок, в будущем, сервис обладает достаточным количеством информации для деанонимизации человека. Поскольку онлайн-отслеживание является очень всеобъемлющим и эффективным инструментом в современном Интернете, утечка данных о биткоин-платежах является серьезной угрозой для сегодняшних пользователей.

В процессе снятия отпечатков есть два варианта:

• **Единая транзакционная связь**. Цель атаки - связать веб-пользователя с в блокчейне. Если трекер имеет доступ к получающему адресу, он тривиально строит связь. Другое дело, когда трекер знает приблизительную цену и время транзакции. Атакующий просто выполняет поиск журналов транзакций.

• **Пересечение кластеров**. Дополнительная атака, когда противник стремится идентифицировать кластер адресов в биткоин кошельках. Цель атаки - связать две покупки одних и тех же пользователей с блоеснцном. Дальнейшая обработка просто использует известные методы атаки пересечения графа.

6) *Деанонимизация с анализом графов*

Приватность владения биткоин кошельком – очень хрупкая вещь. Как только приватность ломается, обратно вернуть ее становится очень тяжело. Публичный адрес анонимен до тех пор, пока о нем никто не знает. Именно поэтому настоятельно рекомендуется использовать новый биткоин-адрес для каждого нового платежа.

В сочетании с описанными пассивными методами, анализ графа может помочь деанонимизатору выявить реальную личность - владельца биткоин - кошелька. Например, если мы знаем посредников в цепочке, мы можем использовать эту информацию, чтобы вручную найти настоящее имя, используя социальные сети или методы социальной инженерии.

Другим примером анализа графа являются алгоритмы обнаружения сообщества и метрики центральности. Мы можем обнаружить сообщество друзей или соседей, найти людей в середине цепи, которые вовлечены в незаконную деятельность.

Авторы статьи [89] использовали Page Rank на графе Directed Address. Основная цель этого - определить наиболее интересные узлы. Эта техника способна определять крупные игровые сайты и торговые площадки с биткоинами.

Мы уверены, что сложные методы деанонизации, предназначенные для социальных сетей, также будут работать на графике транзакций биткоинов. Это может значительно увеличить процент деанонимизированных пользователей.

Графы, которые описаны ниже, являются основным инструментом для процесса деаноминирования пассивных биткоинов.

7) *Граф транзакций*

Весь блокчейн можно рассматривать как ациклический граф транзакции (см. Рис.15) G = {T, E}, где T представляет собой набор транзакций, хранящихся в блокчейне, E - набор однонаправленных ребер между этими транзакциями. G представляет собой поток монет между транзакциями в блокчейне с течением времени.

Набор входных и выходных монет в транзакции можно рассматривать как весовые коэффициенты на границах G. В частности, каждый вход в транзакции несет отметку времени и количество монет, которые формируют вход для этих транзакций.

Граф транзакций является основным графом при атаках деанонимизации. Граф адресов и граф пользователя / объекта построены с использованием графика транзакций.

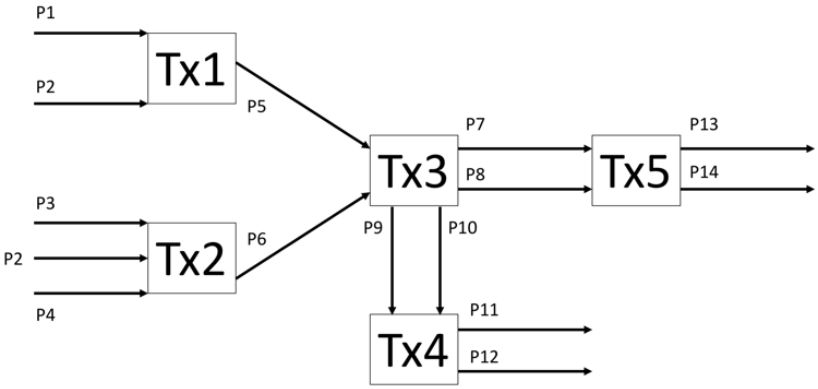

Рисунок 15. Граф транзакций

8) Граф адресов

При обходе графа транзакций мы можем легко определить взаимосвязь между различными входными и выходными адресами (открытые ключи и эти отношения могут использоваться для генерации адресного графа (см. Рис. 16), G = {P, E}, где P является набор адресов биткоинов и E - это грани, соединяющие эти адреса.

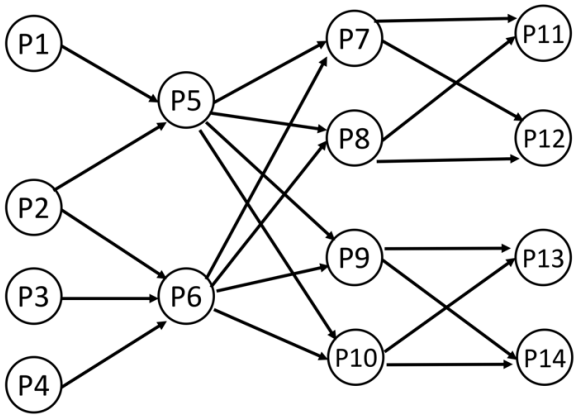

Рисунок 16. График адресов

9) Граф пользователя / объекта

Используя граф адресов вместе с несколькими эвристиками, которые получены из протокола биткоин, следующим шагом является создание графа сущности путем группировки адресов, которые, по-видимому, принадлежат одному и тому же пользователю.

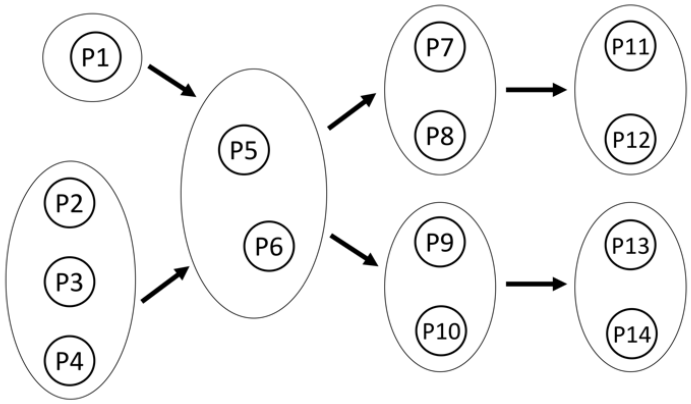

Рисунок 17. График пользователя / объекта

Активные методы

1) Социальная инженерия

Этот метод довольно экзотичен в случае деаномизации пользователей биткоинов. Однако он отлично работает в случае расследований. Например, если вы знаете только одноразовый псевдоним и связанный с ним биткоин-адрес, вы можете выполнять атаки социальной инженерии.

2) Сетевой анализ P2P

Сеть Bitcoin P2P содержит два класса узлов: серверы и клиенты. Клиенты - это узлы, которые не принимают входящие TCP-соединения (например, узлы за NAT), тогда как серверы принимают входящие соединения. Клиенты и серверы имеют разные сетевые протоколы и проблемы с анонимностью. Например, клиенты не ретранслируют транзакции. Основное внимание в методах деанонимии уделяется серверам. Все атаки на сеть P2P основаны на механизме транслирования транзакций. Злоумышленник должен захватить IP-адрес, инициировавший транслирование транзакций. Если у злоумышленника есть ресурсы, похожие на ISP, вектор деанонимии на основе IP может быть мощным инструментом.

Различные исследователи использовали протоколы распространения на основе сплетен [90], чтобы показать, что можно деанонимизировать пользователей, используя связь IP-адреса пользователей с его псевдонимом в сети Bitcoin.

В 2015 году сообщество биткоин ответило на предлагаемую атаку, изменив механизм распространения адресов в сети на другой механизм, известный как диффузия. Атаки использовали «суперноды», который подключен к активным узлам биткоинов и прослушивает транзакционный трафик, передаваемый узлами. Используя этот метод, точность связи составляла до 30% [90].

В новой версии протокола используются независимые экспоненциальные задержки. Однако исследователи из [90, 91] утверждают, что неясно, действительно ли такое изменение защищает от предложенных атак [90]. При распространении диффузии каждый источник или узел ретрансляции передает сообщение каждому из своих неинфицированных соседей с независимой экспоненциальной задержкой скорости λ.

Атаки в [90] используют супернастройку, которая подключена к большинству серверов в сети Bitcoin. Суперноды могут выполнять несколько подключений к каждому честному серверу, причем каждое соединение происходит от другого (IP-адрес, порт). Следовательно, честный сервер не понимает, что соединения супернода - все из одного и того же объекта. Супернод может скомпрометировать произвольно многие неиспользуемые соединения сервера, вплоть до жесткого предела из 125 полных соединений. Супернод в [90] также

отмечает временные метки, при которых сообщения передаются с каждого честного сервера. Поскольку противник поддерживает несколько активных подключений к каждому серверу, он получает сообщение несколько раз с каждого сервера. Суперноды используются для сопоставления транзакций и IP-адресов путем угадывания правильного набора узлов ввода конкретного пользователя. Супернейд пытается перехватить распространение IP-адресов клиентов и сопоставить его с объявленной транзакцией. Эта атака применяется для механизма распространения IP-адресов в биткоине. Такая атака достигает 86% вероятности IP-соответствия на тестовой сети (34% в среднем по основной сетке в 2013 году). В документе [92] показано, что новый протокол не эффективен в отношении атак с одноранговым трафиком.

4 Скоринговые модели финансовых рисков ICO проектов

Ключевыми факторами при оценке финансовых рисков ICO являются следующие:

- Команда
- Проект
- Бизнес-модель
- Технология
- Безопасность
- Советники
- Рыночный потенциал
- Наличие конкурентов
- Интерес к проекту со стороны рядовых инвесторов
- Параметры ICO
- Юридическое обеспечение
- Экспертные оценки

Для оценки, связанной с бизнес-моделью проекта никакого смысла разрабатывать новую скоринговую модель нет. Имеет смысл использовать любую из моделей, описанных выше.

Предлагаемая скоринговая модель должна состоять из четырех компонентов:

1) Оценка бизнес-модели
2) Оценка чистоты транзакций
3) Оценка команды проекта
4) Оценка информационной безопасности

4.1 Оценка бизнес-модели

Для того, чтобы оценивать бизнес-модель для каждого из проектов, предлагается использовать методологию, предложенную порталом ICOBazaar. Ее можно без всяких проблем забирать напрямую с сайта проекта. Никаких дополнительных данных здесь не требуется.

Для расчета будет браться рейтинг, предоставленный командой ICOBazaar.

4.2 Оценка чистоты транзакций

Оценка чистоты транзакций проводится на основе предложенных методологий из предыдущего пункта и описанный в статьях. Для использования в скоринговой модели предлагается брать процент чистых транзакций во всех транзакциях привлеченного капитала.

Если нет возможности использовать собственноручно написанное программное обеспечение, то можно использовать существующие решения, например, QLUE от blockchain intelligence group или решение, разработанное командой проекта Chainalysis. Обе эти разработки позволят получить относительно свежий срез по чистоте транзакций и использовать его на практике.

4.3 Оценка команды проекта

С большей вероятностью, сети из Эдвайзеров и команд, занимающихся скам-проектами будут связаны друг с другом. Для этого мы предлагаем использовать систему, использующую алгоритмы анализа социальных сетей, с целью поиска сомнительных связей советников или членов команды с лицами, использующими сомнительные стратегии заработка.

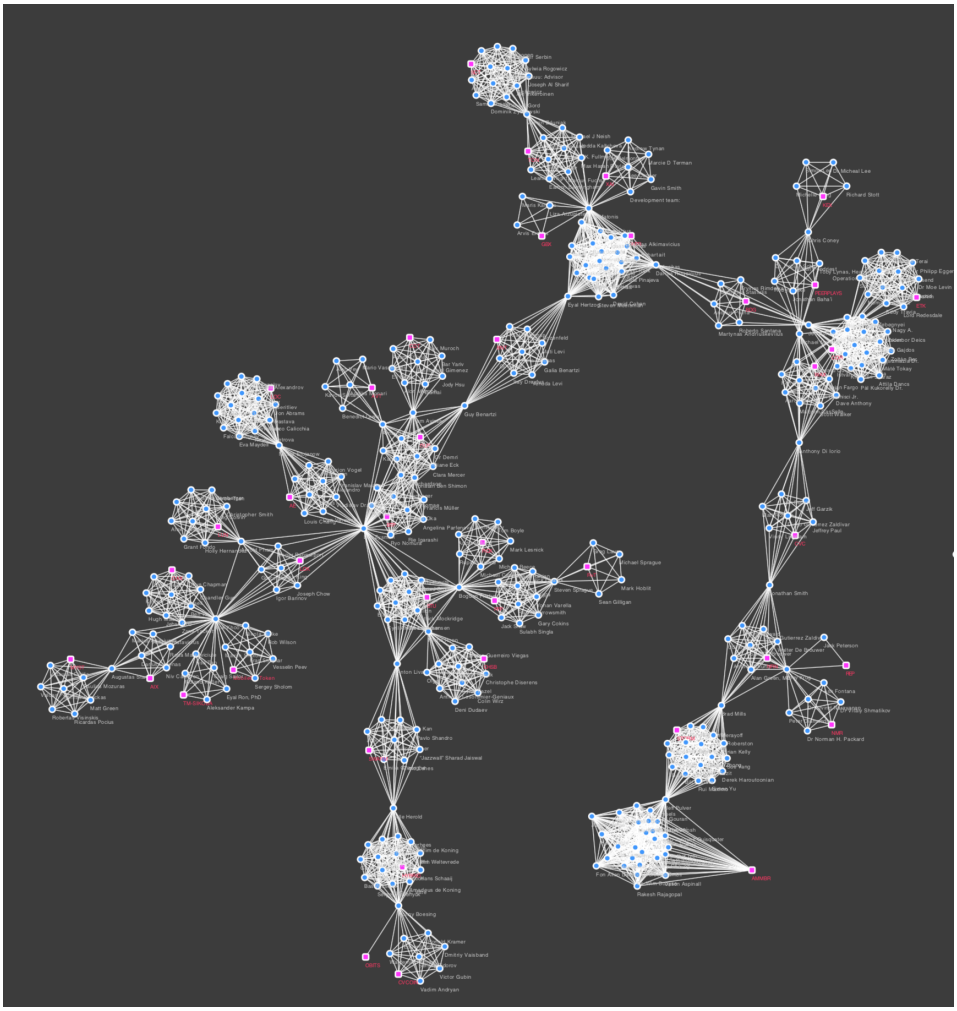

Рисунок 18. Граф команд ICO проектов

Если человек через одно рукопожатие замешан в организации скам проекта или мошеннического ICO, то коэффициент благонадежности команды получается становится более маленьким. Чем больше наблагонадежных участников в команде – тем хуже.

4.4 Оценка рисков информационной безопасности

4.4.1 Безопасность персональных аккаунтов

Для оценки безопасности персональных аккаунтов необходимо использовать публичные данные по утечкам, с целью поиска уязвимых email адресов. Если у команды проекта много утекших паролей, сложность которых является крайне низкой, тогда они получают меньше баллов, чем все остальные.

Разбалловка здесь должна быть следующая:

- *5 баллов*: скомпрометированной парольной информации нет в публичных источниках
- *4 балла*: имеется скомпрометированная парольная информация, сложность паролей высокая
- *3 балла*: имеется скомпрометированная парольная информация, сложность паролей средняя
- *2 балла*: имеется скомпрометированная парольная информация, сложность паролей низкая
- *1 балла*: каждый член команды имеет скомпрометированный почтовый ящик, пароль от которого входит в топ 100 самых распространенных паролей в мире.

4.4.2 Безопасность смарт-контрактов

Степень безопасности смарт контракта, с помощью которого осуществляется привлечение средств ICO проекта является невероятно важным аспектом оценки ICO. Уже известны случаи хищения средств у ICO проектов с помощью уязвимостей в смарт-контрактах.

До 2018 года практически не существовало хороших решений для оценки безопасности смарт-контрактов. Однако, в последнее время, появилось относительно небольшое количество автоматизированных решений, позволяющих выносить вердикты и получать результирующий отчет по найденным уязвимостям.

Методика оценивания предельно простая – чем больше уязвимостей найдено в контракте – тем выше риск баллы за безопасность смарт-контракта. Всего известно 12 типов уязвимостей в смарт контрактах на основе Ethereum. Пока что не до конца понятно, какие из этих уязвимостей являются наиболее критичными, поскольку вектор их эксплуатации не до конца изучен.

Поскольку предполагается быстрое вынесение вердикта с помощью скоринговой модели, мы будем использовать только автоматизированные методы исследования смарт-контрактов, в числе которых находятся следующие:

1. Oyente (https://github.com/melonproject/oyente)
2. Remix (http://remix.readthedocs.io/en/latest/)
3. F* Framework (https://arxiv.org/abs/1802.08660)
4. Gasper (https://ieeexplore.ieee.org/document/7884650/)
5. Securify (https://securify.ch)
6. SmartCheck (http://smartcontracts.smartdec.net)
7. Imandra Contracts (https://www.imandra.ai)
8. Mythril (https://github.com/ConsenSys/mythril)

Инструменты, указанные выше, осуществляют анализ байткода и статический анализ языка программирования Solidity.

Поскольку все вышеперечисленные инструменты для проверки наличия уязвимостей в смарт контрактах можно запускать в автоматическом режиме, проще и надежнее использовать все из них. При составлении скорингового балла мы будем суммировать количество найденных уязвимостей в смарт-контрактах из всех сервисов. Чем больше сумма – тем менее безопасным считается смарт-контракт. Если не было найдено никаких увязвимостей – ставится один балл.

4.4.3 Безопасность используемого программного обеспечения

Этот пункт возможен только лишь при использовании команды аудиторов ИБ. После ручного аудита, разбалловка может быть следующей:

- 5 баллов: не обнаружено критических уязвимостей и логических ошибок в ПО
- 4 балла: не обнаружено критических уязвимостей, логические ошибки не критичные
- 3 балла: обнаружена 1 критическая уязвимость
- 2 балла: обнаружено 2 критических уязвимостей
- 1 балл: обнаружено более 2 критических уязвимостей

4.5 Скоринговые модели

В целом и общем, для скоринга доступно 4 компонента:

- Благонадежность команды проекта (а)
- Бизнес-модель (б)
- Чистота транзакций (в)
- Информационная безопасность (г)

Существует три вида скоринговых моделей (классификация по принципу доступности информации для человека, проводящего классификацию):

- White-box - лицу, проводящему скоринг, доступна следующая информация:
  - Все исходные коды всего программного обеспечения
  - White-paper
  - Информация о транзакциях, поступающих на счет
- Grey-box – лицу, проводящему скоринг, доступна следующая информация:
  - Исходный код смарт-контракта
  - Доступ к веб-приложению
  - White-paper
- Black-box – лицу, проводящему скоринг, доступна следующая информация:
  - White-paper
  - Исходный код смарт-контракта

Обозначения в формулах:

- tc – коэффициент команды, рассчитывается, как 100% - 100%/(количество неблагонадеэных членов;
- P_{acc} – оценка безопасности персональных аккаунтов;
- P_{soft} – оценка безопасности программного обеспечения;
- P_{smart} – сумма уязвимостей в смарт-контракте;
- tx – оценка чистоты транзакций;
- BM – баллы за бизнес модель из методики ICOBazaar;

Все рейтинговые баллы могут быть использованы для сравнения нескольких проектов между собой.

4.5.1 Скоринговая модель White-box

$$R = tc * [0.3 * \frac{P_{acc} + P_{soft}}{P_{smart}} + 0.1 * tx + 0.6 * BM]$$

4.5.2 Скоринговая модель Grey-box

$$R = tc * [0.4 * \frac{P_{acc} + P_{soft}}{P_{smart}} + 0.6 * BM]$$

4.5.3 Скоринговая модель Black-box

$$R = tc * [0.7 * BM + 0.3 * \left(\max \sum P_{smart} - P_{smart}\right)]$$

5 Выбор средств реализации программы для проведения исследований, планирование и обработка результатов эксперимента

Основными программными средствами для проведения исследования являются следующие:

- Языки программирования Python, bash
- Программа для визуализации графов Cytoscape

Все эксперименты были проведены на базе компании Group-IB при оценке проектов, приходящих за аудитом информационной безопасности. Все соответствующие справки о внедрении приведены в приложении.

6 Выводы

Были изучены все виды финансовых рисков, возникающие у ICO проектов. Было проведено масштабное исследование рисков информационной безопасности и предложена новая скоринговая модель

Научная новизна модели заключается в том, что она учитывает такие критерии, как «чистота» криптовалютных транзакций и риски информационной безопасности.

Результаты работы были внедрены в деятельности компании Group-IB, представлены на 8 конференциях и опубликованы в 3 статьях.

7 Список источников

1. Williams-Grut O. Only 48% of ICOs were successful last year – but startups still managed to raise $5.6 billion [Электронный ресурс] // Business Insider [Официальный вебсайт]. URL: https://www.businessinsider.nl/how-much-raised-icos-2017-tokendata-2017-2018-1/?international=true&r=UK (дата обращения: 24.04.2018).
2. Project Evaluation [Электронный ресурс] // ICORATING [Официальный вебсайт]. URL: https://icorating.com/methodology/ (дата обращения: 24.04.2018).
3. ICO Rating Methodology [Электронный ресурс] // ICOMarketData [Официальный вебсайт]. URL: https://www.icomarketdata.com/icorating (дата обращения: 24.04.2018).
4. ICO Score calculation methodology [Электронный ресурс] // Foundico [Официальный вебсайт]. URL: https://foundico.com/methodology/ (дата обращения: 24.04.2018).
5. Token Metrics ICO rating methodology [Электронный ресурс] // Medium [Официальный вебсайт]. URL: https://medium.com/@tokenmetrics/token-metrics-ico-rating-methodology-1e28926e1602 (дата обращения: 24.04.2018).
6. Rating methodology [Электронный ресурс] // ICOMarks [Официальный вебсайт]. URL: https://icomarks.com/rating (дата обращения: 24.04.2018).
7. ICOBAZAAR Rating System [Электронный ресурс] // ICObazaar [Официальный вебсайт]. URL: https://icobazaar.com/icobazaar-rating-system (дата обращения: 24.04.2018).
8. Our methodology [Электронный ресурс] // ICO Scoring [Официальный вебсайт]. URL: https://icoscoring.com/en/methodology/ (дата обращения: 24.04.2018).
9. ICO Score Methodology [Электронный ресурс] // CoinGecko [Официальный вебсайт]. URL: https://www.coingecko.com/en/ico_methodology (дата обращения: 24.04.2018).
10. Rating Methodology [Электронный ресурс] // ICOPlum [Официальный вебсайт]. URL: https://icoplum.com/ratings (дата обращения: 24.04.2018).
11. Rating Methodology [Электронный ресурс] // Coin Delite [Официальный вебсайт]. URL: https://coindelite.com/ratings (дата обращения: 24.04.2018).
12. Лазаренко А.В. Хакер №228. Как крадут ICO [Электронный ресурс] // Журнал Хакер [Официальный вебсайт]. URL: https://xakep.ru/issues/xa/228/ (дата обращения: 24.04.2018).
13. Bitcoin Forum [Электронный ресурс] // BitcoinTalk [Официальный вебсайт]. URL: https://bitcointalk.org (дата обращения: 24.04.2018).
14. Crypto Detectives [Электронный ресурс] // CryptoDetectives [Официальный вебсайт]. URL: https://cryptodetectives.ru/en/home/ (дата обращения: 24.04.2018).
15. Wi-Fi Global [Электронный ресурс] // Coinspeaker [Официальный вебсайт]. URL: https://www.coinspeaker.com/ico/project/wi-fi-global/ (дата обращения: 24.04.2018).
16. Enigma [Электронный ресурс] // Enigma [Официальный вебсайт]. URL: https://enigma.co (дата обращения: 24.04.2018)
17. Slack: where work happens [Электронный ресурс] // Slack [Официальный вебсайт]. URL: https://slack.com (дата обращения: 24.04.2018).
18. CoinDash [Электронный ресурс] // CoinDash [Официальный вебсайт]. URL: https://coindash.io (дата обращения: 24.04.2018).
19. Etherscan: The Ethereum Block Explorer [Электронный ресурс] // Etherscan [Официальный вебсайт]. URL: https://etherscan.io (дата обращения: 24.04.2018).
20. Chainalysis – Blockchain analysis [Электронный ресурс] // Chainalysis [Официальный вебсайт]. URL: https://www.chainalysis.com (дата обращения: 24.04.2018).
21. Cybersecurity products and services provider company - Group-IB [Электронный ресурс] // Group-IB [Официальный вебсайт]. URL: https://www.group-ib.com (дата обращения: 24.04.2018).
22. Ethereum Scam Database [Электронный ресурс] // Etherscamdb [Официальный вебсайт]. URL: https://etherscamdb.info (дата обращения: 24.04.2018).

23. Myetherwallet [Электронный ресурс] // MyEtherWallet [Официальный вебсайт]. URL: https://www.myetherwallet.com (дата обращения: 24.04.2018).
24. The DAO (organization) [Электронный ресурс] // Wikipedia [Официальный вебсайт]. URL: https://en.wikipedia.org/wiki/The_DAO_(organization) (дата обращения: 24.04.2018).
25. О. Парамонов. DAO теряет миллионы долларов в час из-за ошибки в своем коде и тянет Ethereum за собой [Электронный ресурс] // Xakep [Официальный вебсайт]. URL: https://xakep.ru/2016/06/17/splitdao-attack/ (дата обращения: 24.04.2018).
26. М. Нефёдова. Уязвимость в Ethereum-кошельке Parity привела к краже $30 млн [Электронный ресурс] // Xakep [Официальный вебсайт]. URL: https://xakep.ru/2017/07/20/parity-bug/ (дата обращения: 24.04.2018).
27. N.Atzei, M. Bartoletti, T. Cimoli. A Survey of Attacks on Ethereum Smart Contracts [Электронный ресурс] // IACR [Официальный вебсайт]. URL: https://eprint.iacr.org/2016/1007.pdf (дата обращения: 24.04.2018).
28. An Analysis Tool for Smart Contracts – Oyente [Электронный ресурс] // Github [Официальный вебсайт]. URL: https://github.com/melonproject/oyente (дата обращения: 24.04.2018).
29. A. Juels, A. Kosba, E. Shi. The Rings of Gyges: Investigating the Future of Criminal Smart Contracts [Электронный ресурс] // IC3 [Официальный вебсайт]. URL: http://www.initc3.org/files/Gyges.pdf (дата обращения: 24.04.2018).
30. Kharpal A (2017) Initial coin offerings have raised $1.2 billion and now surpass early stage VC funding [Электронный ресурс] // CNBC [Официальный вебсайт]. URL: https://www.cnbc.com/2017/08/09/initial-coin-offerings-surpass-early-stage-venture-capital-funding.html (дата обращения: 24.04.2018)
31. The Rise of Cybercrime on Ethereum. [Электронный ресурс] // [Официальный вебсайт] URL: https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/ (дата обращения: 14.03.2018)
32. Li. X. A survey on the security of Blockchain systems. [Электронный ресурс] // Science Direct [Официальный вебсайт]. URL: https://www.sciencedirect.com/science/article/pii/S0167739X17318332 (дата обращения: 14.03.2018)
33. 51% attack. [Электронный ресурс] // Investopedia [Официальный вебсайт]. URL: https://www.investopedia.com/terms/1/51-attack.asp (дата обращения: 14.03.2018)
34. Transaction malleability. [Электронный ресурс] // Bitcoin.it [Официальный вебсайт]. URL: https://en.bitcoin.it/wiki/Transaction_malleability (дата обращения: 14.03.2018)
35. Domain Hijacking. [Электронный ресурс] // Wikipedia.org [Официальный вебсайт]. URL: https://en.wikipedia.org/wiki/Domain_hijacking (дата обращения: 14.03.2018).
36. Leung A. Test Attack in Krypton, Ethereum Classic Might be Next. [Электронный ресурс] // Cointelegraph [Официальный вебсайт] https://cointelegraph.com/news/test-attack-on-krypton-ethereum-classic-might-be-next (дата обращения: 14.03.2018)
37. Mt. Gox shutdown a major blow for bitcoin. [Электронный ресурс] // CBC [Официальный вебсайт]. URL: http://www.cbc.ca/news/technology/mt-gox-shutdown-a-major-blow-for-bitcoin-1.2550256 (дата обращения: 14.03.2018)
38. Norry A. The History of the Mt Gox Hack: Bitcoin’s Biggest Heist. [Электронный ресурс] // Blockconomi [Официальный вебсайт]. URL: https://blockonomi.com/mt-gox-hack/ (дата обращения: 14.03.2018)
39. Decker C. Bitcoin Transaction Malleability and MtGox. [Электронный ресурс] // Arxiv [Официальный вебсайт]. URL: https://arxiv.org/pdf/1403.6676.pdf (дата обращения: 14.03.2018)
40. Siegel D. Understanding The DAO Hack for Journalists. [Электронный ресурс] // Medium [Официальный вебсайт]. URL: https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993 (дата обращения: 14.03.2018)

41. Bitcoinica people hacked again, for ~350K US$ this time. [Электронный ресурс] // Reddit [Официальный вебсайт]. URL: https://www.reddit.com/r/netsec/comments/wi1xf/bitcoinica_people_hacked_again_for_350k_us_this/ (дата обращения: 14.03.2018).
42. Bter Freezes Accounts After 7170 Bitcoin Theft, Offering ~10% Bounty. [Электронный ресурс] // CCN [Официальный вебсайт]. URL: https://www.ccn.com/breaking-bter-freezes-accounts-7170-bitcoin-theft-offering-10-bounty/ (дата обращения: 14.03.2018)
43. Zhao W. $7 Million Lost in CoinDash ICO Hack. [Электронный ресурс] // CoinDesk [Официальный вебсайт] https://www.coindesk.com/7-million-ico-hack-results-coindash-refund-offer/ (дата обращения: 14.03.2018)
44. Russel J. Hackers nab $500000 as Enigma is compromised weeks before its ICO [Электронный ресурс] // Techcrunch [Официальный вебсайт] https://techcrunch.com/2017/08/21/hack-enigma-500000-ico/ (дата обращения: 14.03.2018)
45. Warning, Enigma website and slack probably hacked [Электронный ресурс] // Reddit [Официальный вебсайт] https://www.reddit.com/r/ethtrader/comments/6v0vei/warning_enigma_website_and_slack_probably_hacked/ (дата обращения: 14.03.2018)
46. Finchman N. CoinTerra Hacked [Электронный ресурс] // Mineforeman [Официальный вебсайт] https://mineforeman.com/2014/02/03/cointerra-hacked/ (дата обращения: 14.03.2018)
47. Important Security Announcement: Steemit CEO Ned Scott [Электронный ресурс] // Steemit [Официальный вебсайт]. URL: https://steemit.com/steemit/@steemitblog/important-security-announcement-steemit-ceo-ned-scott (дата обращения: 14.03.2018).
48. Inputs.io [Электронный ресурс] // Bitcointalk [Официальный вебсайт]. URL: https://bitcointalk.org/index.php?topic=248803.640 (дата обращения: 14.03.2018).
49. Bitcoins worth $94M stolen in hack on Bitfinex exchange [Электронный ресурс] // CBC [Официальный вебсайт]. URL: http://www.cbc.ca/news/technology/bitcoin-bitfinex-hack-1.3705353 (accessed: 14.03.2018).
50. Riley D. Mintpal scammer Ryan Kennedy arrested in U.K. over theft of 3700 Bitcoins [Электронный ресурс] // Siliconangle [Официальный вебсайт]. URLL: https://siliconangle.com/blog/2015/02/23/mintpal-scammer-ryan-kennedy-arrested-in-u-k-over-theft-of-3700-bitcoins/ (дата обращения: 14.03.2018).
51. 796 lost 1000 bitcoin [Электронный ресурс] // Bitcointalk [Официальный вебсайт] https://bitcointalk.org/index.php?topic=938765.0 (дата обращения: 14.03.2018)
52. Sankin A. Everybody gets hacked: A cryptocurrency exchange's public meltdown [Электронный ресурс] // Dailydot [Официальный вебсайт]. URL: https://www.dailydot.com/business/cryptorush-exchange-blackcoin/ (дата обращения: 14.03.2018)
53. Picostock hacked, even cold wallet emptied [Электронный ресурс] // Reddit [Официальный вебсайт]. URL: https://www.reddit.com/r/Bitcoin/comments/1rrnua/picostocks_hacked_even_cold_wallet_emptied/ (дата обращения: 14.03.2018).
54. Bitlc.net [Электронный ресурс] // Archive [Официальный вебсайт]. URL: http://web.archive.org/web/20130302231015/https://www.bitlc.net/ (дата обращения: 14.03.2018).
55. The ShapeShift Hack: Simply Incredible [Электронный ресурс] // HackingDistributed [Официальный вебсайт]. URL: http://hackingdistributed.com/2016/04/25/shapeshift-hack-simply-incredible/ (дата обращения: 14.03.2018).
56. DeMartino I. Notorious 'Hacker Group' Allegedly Involved In Exco.In Theft, Owner Accuses CCEDK of Withholding Info [Электронный ресурс] // Cointelegraph [Официальный вебсайт]. URL: https://cointelegraph.com/news/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info (дата обращения: 14.03.2018)

57. Raza A. Cryptsy Hacked: Bitcoin Worth $6 Million Stolen [Электронный ресурс] // Hackread [Официальный вебсайт]. URL: https://www.hackread.com/cryptsy-hacked-bitcoin-worth-usd-6-million-stolen/ (дата обращения: 14 Mar 2018).
58. Lucky7Coin – PoW/PoS, BonusBlock based on your lucky 7s [Электронный ресурс] // Bitcointalk [Официальный вебсайт]. URL: https://bitcointalk.org/index.php?topic=295157.0 (дата обращения: 14.03.2018)
59. South Korean Bitcoin Exchange Yapizon Hacked; $5 Million Stolen [Электронный ресурс] // Hackread [Официальный вебсайт]. URL: https://www.hackread.com/south-korean-bitcoin-exchange-yapizon-hacked/ (дата обращения: 14.03.2018).
60. I just got hacked – any help is welcome! (25, 000 BTC stolen) [Электронный ресурс] // Bitcointalk [Официальный вебсайт]. URL: https://bitcointalk.org/index.php?topic=16457.msg214423#msg214423 (дата обращения: 14.03.2018)
61. Parker L. Fourth Largest Bitcoin exchange. Bithumb, hacked for billions of Won [Электронный ресурс] // Bravenewcoin [Официальный вебсайт]. URL: https://bravenewcoin.com/news/fourth-largest-bitcoin-exchange-bithumb-hacked-for-billions-of-won (дата обращения: 14.03.2018).
62. Higgins S. Details of $5 Million Bitstamp Hack Revealed [Электронный ресурс] // Coindesk [Официальный вебсайт]. URL: https://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/ (дата обращения: 14.03.2018).
63. Myetherwallet
64. Bitcoin bank Flexcoin closes after hack attack [Электронный ресурс] // TheGuardian [Официальный вебсайт]. URL: https://www.theguardian.com/technology/2014/mar/04/bitcoin-bank-flexcoin-closes-after-hack-attack (дата обращения: 14.03.2018).
65. BTC-e [Электронный ресурс] // Wikipedia [Официальный вебсайт]. URL: https://en.wikipedia.org/wiki/BTC-e (дата обращения: 14.03.2018).
66. Bitcoin Exchange Cavirtex Shut's Down After Database Hack Leaves User Data Exposed [Электронный ресурс] // Bitcoinist [Официальный вебсайт]. URL: http://bitcoinist.com/bitcoin-exchange-cavirtex-shuts-database-hack-leaves-user-data-exposed/ (дата обращения: 14.03.2018).
67. Higgins S. Gatecoin Claims $2 Million in Bitcoins and Ethers Lost in Security Breach [Электронный ресурс] // Coindesk [Официальный вебсайт]. URL: https://www.coindesk.com/gatecoin-2-million-bitcoin-ether-security-breach/ (дата обращения: 14.03.2018).
68. Buterin V. Bitfloor Hacked, $250000 Missing [Электронный ресурс] // BitcoinMagazine [Официальный вебсайт]. URL: https://bitcoinmagazine.com/articles/bitfloor-hacked-250000-missing-1346821046/ (дата обращения: 14.03.2018).
69. Kipcoin [Электронный ресурс] // Coinjournal [Официальный вебсайт]. URL: https://coinjournal.net/chinese-exchange-kipcoin-hacked/ (дата обращения: 14.03.2018).
70. Poloniex Loses 12.3% of its Bitcoins in Latest Bitcoin Exchange Hack. Bitcoins [Электронный ресурс] // Coindesk [Официальный вебсайт]. URL: https://www.coindesk.com/poloniex-loses-12-3-bitcoins-latest-bitcoin-exchange-hack/ (дата обращения: 14.03.2018)
71. Shares D. Bitcurex Forced to Shut Down After $1.5 million Theft [Электронный ресурс] // Bitcoin.com [Официальный вебсайт]. URL: https://news.bitcoin.com/bitcurex-forced-million-theft/ (дата обращения: 14.03.2018).
72. Bitcoin7.com 'hacked'. Database and wallets 'stolen' [Электронный ресурс] // Bitcointalk [Официальный вебсайт]. URL: https://bitcointalk.org/index.php?topic=46982.0 (дата обращения: 14.03.2018)

73. Perez Y.B. Bitcoin Firm Coinapult Restores Services Following Hack [Электронный ресурс] // CoinDesk [Официальный вебсайт]. URL: https://www.coindesk.com/bitcoin-firm-coinapult-restores-services-following-hack/ (дата обращения: 14.03.2018).
74. Khandelwal S. Danish Bitcoin Exchange BIPS hacked and 1,295 Bitcoins worth $1 Million Stolen [Электронный ресурс] // TheHackerNews [Официальный вебсайт]. URL: https://thehackernews.com/2013/11/danish-bitcoin-exchange-bips-hacked-and_25.html (дата обращения: 14.03.2018).
75. Bitmain hacked [Электронный ресурс] // Reddit [Официальный вебсайт]. URL: https://www.reddit.com/r/Bitcoin/comments/6uw8rw/bitmain_hacked/ (дата обращения: 14.03.2018).
76. BTCGuild Hacked? [Электронный ресурс] // Reddit [Официальный вебсайт]. URL: https://www.reddit.com/r/Bitcoin/comments/ntntj/btcguild_hacked/ (дата обращения: 14.03.2018).
77. Buterin V. OzCoin Hacked, Stolen Funds Seized and Returned by StrongCoin [Электронный ресурс] // Bitcoinmagazine [Официальный вебсайт]. URL: https://bitcoinmagazine.com/articles/ozcoin-hacked-stolen-funds-seized-and-returned-by-strongcoin-1366822516/ (дата обращения: 14.03.2018)
78. Tether hits back after $31M Cryptocurrency hack [Электронный ресурс] // Nakedsecurity [Официальный вебсайт]. URL: https://nakedsecurity.sophos.com/2017/11/23/tether-hits-back-after-31m-cryptocurrency-hack/ (дата обращения: 14.03.2018).
79. Peck M.E. Thousands of Bitcoins stolen in a hack on Linode [Электронный ресурс] // IEEE Spectrum [Официальный вебсайт]. URL: https://spectrum.ieee.org/tech-talk/computing/networks/thousands-of-bitcoins-stolen-in-a-hack-on-linode (дата обращения: 14.03.2018).
80. Petrov S. Another Parity Wallet hack explained [Электронный ресурс] // Medium [Официальный вебсайт]. URL: https://medium.com/@Pr0Ger/another-parity-wallet-hack-explained-847ca46a2e1c (дата обращения: 14.03.2018).
81. Parity Multisig Wallet Hack [Электронный ресурс] // Aeternity [Официальный вебсайт]. URL: https://blog.aeternity.com/parity-multisig-wallet-hack-47cc507d964d (дата обращения, 14.03.2018).
82. Mooncoin was hacked, the database has been hacked [Электронный ресурс] // Reddit [Официальный вебсайт]. URL: https://www.reddit.com/r/Bitcoin/comments/khv6v/mooncoin_was_hacked_the_database_has_been_leaked/ (дата обращения: 14.03.2018).
83. M.Fleder, M.S.Kester, S.Pillai. Bitcoin Transaction Graph Analysis [Электронный ресурс] // Cornell University Library [Официальный вебсайт]. URL: https://arxiv.org/pdf/1502.01657.pdf (дата обращения: 22.10.2017)
84. S.Meiklejohn, M.Pomarole, G.Jordan. A Fistful of Bitcoins: Characterizing Payments Among Men with no Names [Электронный ресурс] // UC San Diego [Официальный вебсайт]. URL: https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf (дата обращения: 22.10.2017).
85. Bitcoin Address Tags [Электронный ресурс] // Blockchaininfo [Официальный вебсайт]. URL: https://blockchain.info/ru/tags (дата обращения: 22.10.2017)
86. Bitcoin Address Checker [Электронный ресурс] // BitcoinWhosWho [Официальный вебсайт]. URL: http://bitcoinwhoswho.com (дата обращения: 22.10.2017)
87. E. Androukli, G.O. Karame Evaluating User Privacy in Bitcoin [Электронный ресурс] // Cryptology ePrint Archive [Официальный вебсайт]. URL: https://eprint.iacr.org/2012/596.pdf (дата обращения: 22.10.2017)
88. S.Goldfeder. When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies [Электронный ресурс] // Cornell University Library [Официальный вебсайт]. URL: https://arxiv.org/pdf/1708.04748.pdf (дата обращения: 22.10.2017)

89. M.Fleder, M.S. Kester, S. Pillai. Bitcoin Transaction Graph Analysis [Электронный ресурс] // Cornell University Library [Официальный вебсайт]. URL: https://arxiv.org/abs/1502.01657 (дата обращения: 22.10.2017)
90. A. Biryukov, D. Khovratovich. Deanonymisation of clients in Bitcoin P2P network [Электронный ресурс] // ACM DL [Официальный вебсайт]. URL: https://dl.acm.org/citation.cfm?id=2660379 (дата обращения: 22.10.2017)
91. G. Fanti, P.Viswanath. Anonymity Properties of the Bitcoin P2P Network [Электронный ресурс] // Cornell University Library [Официальный вебсайт]. URL: https://arxiv.org/abs/1703.08761 (дата обращения: 22.10.2017)
92. M. Spagnuolo, F. Maggi. BitIodine: Extracting Intelligence from the Bitcoin Network [Электронный ресурс] // FC & DS 2014 [Официальный вебсайт]. URL: http://fc14.ifca.ai/papers/fc14_submission_11.pdf (дата обращения: 22. 10. 2017)