МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н. Г. ЧЕРНЫШЕВСКОГО»**
Кафедра математической кибернетики и компьютерных наук

УСТОЙЧИВОСТЬ К ВЗЛОМУ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 4 курса 411 группы
направления 02.03.02 — Фундаментальная информатика и информационные технологии
факультета КНиИТ
Борщева Даниила Юрьевича

Научный руководитель
доцент _____ М. С. Семенов

Заведующий кафедрой
к. ф.-м. н. _____ С. В. Миронов

Саратов 2019

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Устойчивость вычислительных сетей на основе технологии блокчейн определяет их безопасность, а как результат, вызывает или подрывает доверие людей, пользующихся подобными продуктами.

Актуальность данной темы определяется активным внедрением технологии блокчейн во все сферы нашей жизни. Технологии, в основе которых лежит блокчейн, уже не ограничиваются только криптовалютами и финансовой сферой: блокчейн начинают использовать и для заключения юридически значимых контрактов в самых разных сферах деятельности — от строительства до политики.

Предмет исследования. В ходе написания балакаврской работы были проанализированы потенциальные атаки на криптовалюту Биткоин, а так же рассмотрены стратегии защиты от них. Была разработана блокчейн-платформа с основными протоколами консенсуса. Распространенная по одноранговой сети платформа была подвержена атаке 51% группой вредоносных пользователей с целью выявить уязвимые компоненты сети для предотвращения подобного рода атак.

Цель бакалаврской работы — разработать вычислительную сеть на основе технологии блокчейн и проверить ее устойчивости к взлому. Поставленная цель определила **следующие задачи**:

1. Изучить принципы построения блокчейн сетей.
2. Написать ПО для организации тестовой блокчейн сети.
3. Изучить основные уязвимости блокчейна и атаки, которые могут проводиться для несанкционированного изменения данных в блокчейне.
4. Развернуть собственную блокчейн сеть и произвести на нее атаку 51% с целью исследования устойчивости к взлому.
5. Проанализировать результаты атаки 51% и сформулировать рекомендации для последующего улучшения защищенности блокчейн сети.

Методологические основы блокчейн технологии представлены в книге Майкла Кросби [1], анализ потенциальных атак в статье Мени Розенфельда [2] и построение серверной части приложения с помощью Spring в статье [3].

Структура и объем работы. Бакалаврская работа состоит из введения, 2 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы — 48 страниц, из них 33 страницы — основное содержа-

ние, включая 5 рисунков и 1 таблицу, цифровой носитель в качестве приложения, список использованных источников информации – 20 наименований.

1 Безопасность технологии блокчейн

Блокчейн — децентрализованная и распределенная по одноранговой сети база данных. Копия базы распространяется каждому участнику сети с равными правами. Так как у этой сети нет центрального сервера, она является децентрализованной.

В структуре блокчейна лежит цепочка блоков (block chain) [1], где каждый блок хранит в себе набор данных (транзакций). Блоки связанны между с собой хеш-суммами. При создании блока, он хешируется некой хеш-функцией, например, SHA-256 [4]. Полученный хеш записывается в следующий блок. Если изменить данные в текущем блоке, пересчитается хеш, который не будет совпадать с хешем, записанным в следующем блоке. Таким образом, данные в блоках нельзя изменить. Эту неизменность гарантирует криптография, поэтому электронные валюты вроде Биткоина, использующие в своей основе блокчейн, называются «криптовалютами».

Применение технологии блокчейн не ограничивается криптовалютами, однако их процент в развитии этой технологии очень большой. Основными алгоритмами механизмов консенсуса в криптовалютах являются доказательство работы (proof of work) и подтверждение доли (proof of stake [5]). Эти алгоритмы управляют процессом добавления блоков в цепочки. В PoS наибольшую вероятность добавить новый блок в цепочку имеет пользователь с наибольшей долей валюты в сети. Таким образом, с ростом цепочки более старые пользователи набирают преимущество перед новыми. В PoW необходимо проделать сложную вычислительную работу, чтобы добавить блок в цепочку. Как правило, нужно подобрать такой заголовок, чтобы хеш блока удовлетворял определенному условию. Таким образом, этот процесс требует мощного оборудования и затрат на электричество. В PoS пользователей, формирующих новые блоки называют минтерами (чеканщиками), а в PoW — майнерами (добытчиками).

В Биткоине доказательство работы реализовано алгоритмом Hashcash [6]. Обычные узлы формируют пул транзакций, который в последствии будет помещен в блокчейн майнером, первым нашедшим нужный блок. Задача майнера — найти такой nonce (уникальное число), который в сумме с остальными данными блока будет обработан хеш-функцией, а ее результат в двоичном представлении будет меньше или равен определенную значению, устанавлива-

емому системой. Единственный способ найти нужный nonce — перебор всевозможных значений. Это доказывает тот факт, что майнинг — честный процесс. Однако бывают случаи, когда пользователи одновременно находят подходящий блок, и тогда происходит разветвление блокчейна. В этом случае сеть с грамотно прописанными протоколами консенсуса должна четко определить правильную ветвь и распространить по всем участникам именно ее, а сами участники должны быть заинтересованы в расширении именно этой ветви.

Большинство атак на криптовалюты требуют дорогостоящего оборудования, если речь идет об атаке на PoW-сети, либо большой доли, если о PoS. Самыми распространенными атаками на PoS платформы являются:

— проблема «ничего на кону»;
— проблема начального распределения;
— атака издалека.

В проблеме «ничего на кону» большой шанс успешной атаки, если средства равномерно распределены между пользователями. Это объясняется тем, что при разветвлении блокчейна рационально минтить блока на всевозможных ветвях, поэтому пользователи с большой долей валюты в сети рискуют потерять свои средства.

Самыми распространенными атаками на PoW платформы являются:

— атака Сибиллы;
— атака двойной траты;
— DoS-атака.

Атака Сибиллы подразумевает окружение жертвы подконтрольными злоумышленнику узлами с целью подчинить его работу себе. На практике эта атака тяжело осуществима, так как подобраться к этой жертве со всех сторон тяжело, ибо система связывает узлы случайным образом. Атака двойной траты наиболее известна, так как влечет большую выгоду для атакующего. Под ней подразумевается формирование собственной цепочки, в результате которой атакующий перепишет транзакции и сможет себе вернуть потраченную валюту за совершенную раннее покупку. DoS-атака популярна среди централизованных платформ, так как предполагает выведение из строя сервера путем отправки ему большого количества запросов. Однако она так же осуществима и на децентрализованные сети, так как можно отправлять запросы множеству узлов, выводя их из строя. Более опасной версией этой атаки является

DDoS-атака. В этом случае отправка запросов осуществляется не от одного злоумышленника, а от целой группы.

2 Разработка платформы блокчейн и проверка ее устойчивости

Для разработки собственной блокчейн-сети был выбрал язык программирования Java. Каждый узел в сети является как клиентом, так и сервером, поэтому разработка платформы свелась к реализации этих компонентов, а так же логики и доступа к данным.

В логике реализованы модели данных, блока и цепочки. В класс блока входят следующие атрибуты: метка времени создания, данные, хеш предыдущего блока, текущий хеш и алгоритм хеширования. В качестве алгоритма был взят SHA-256, который используется во всех компонентах сети. В классе цепочки реализованы всевозможные инициализации блокчейна, базовые протоколы консенсуса и клиентские запросы.

Данные хранятся в реляционной базе данных PostgreSQL. Доступ к ним реализован с помощью библиотек JPA и Hibernate, которая реализует ORM подход. Таким образом, когда приложение обращается к базе данных для получения блоков, оно конвертирует их реляционное представление в объектное, с которым будут работать последующие слои приложения.

Серверная часть реализована с помощью фреймоврка Spring [3]. На вход по определенному порту поступают HTTP запросы, который сервер принимает и отдает на дальнейшую обработку логике, получает от нее данные и на их основе формирует ответ клиенту.

Вредоносное программное обеспечение (майнер) был написан на языке программирования C#. Он получает текущий хешрейт сети, по нему ищет подходящий nonce, локально проверяет валидность блока и в случае успеха отправляет этот блок сети. По сути эта программа не является вредоносной в руках честного майнера, но в предстоящем исследовании под атакующим программным обеспечением выступает точно такая же копия майнера с небольшой надстройкой.

Для проверки устойчивости разработанной платформы была проведена атака 51% [7]. Суть атаки заключается в завладении мощности большей, чем у половины сети. Это может быть осуществлено либо одним злоумышленником, либо целой группой. Это позволит сформировать свою цепочку блоков, которая будет длиннее, чем основная, в результате чего она будет принята системой как действительная. Именно атака 51% является родоначальницей атаки двойной траты. Если майнер или пул майнеров обладает большей мощностью, то он

сможет сформировать новую цепочку и вернуть в ней потраченные средства. Первоначально сеть была распределена по 3 узлам с примерно одинаковыми CPU (количество ядер и частота). Так как майнинг в ходе этого исследования осуществлялся с помощью центрального процессора, только он входил в характеристику мощности майнера. Из 3 узлов 2 являются атакующими, таким образом они обладали примерно 66% мощности всей сети, что удовлетворяет условию для проведения атаки 51%. Первым шагом два узла запустили копию блокчейна на другом порту параллельно основному. В этой копии злоумышленники обменивались блоками между собой, а в основном блокчейне продолжали принимать блоки от «честного» майнера. Когда цепочка в копии превысила цепочку в основном блокчейне, злоумышленники поменяли конфигурацию основного блокчейна, предоставив ему базу данных с копии. При подключении нового узла сеть предоставит ему цепочку злоумышленников, в то время как цепочка «честного» майнера будет признаваться недействительной. Результаты исследования показали, что при основной цепочке размером в 10 блоков, которую продолжал строить первый майнер, вредоносным майнерам потребовалось примерно 13 минут, чтобы с нуля построить цепочку длиннее основной. Для предотвращения подобного рода атак необходимо расширять сеть и усовершенствовать механизм консенсуса, однако второе лишь уменьшит шансы злоумышленников на успешную атаку или сделает ее максимально затратной.

ЗАКЛЮЧЕНИЕ

Целью данной работы являлась разработка собственной вычислительной сети на основе технологии блокчейн и проверка ее устойчивости к взлому. Были выполнены следующие задачи: описан принцип работы блокчейна, проанализированы алгоритмы криптовалют, были выявлены слабые и сильные стороны блокчейн-технологий, составлен список потенциальных атак, произведен их обзор. Для проведения собственной атаки был разработан блокчейн на языке программирования Java. В ходе разработки были затронуты различные технологии и использованы необходимые фреймворки и библиотеки. Для совершения атаки был разработан майнер на языке программирования C#. Была проведена атака 51%, результаты которой подтвердили теорию. Результаты исследования показали, что для предотвращения подобного рода атаки необходимо расширять сеть и преобразовывать механизм консенсуса с целью сделать атаки максимально невыгодными.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 *Crosby, M.* BlockChain Technology / M. Crosby, Nachiappan, P. Pattanayak, S. Verma, V. Kalyanaraman. — Sutardja Center for Entrepreneurship and Technology, 2015.

2 *Rosenfeld, M.* Analysis of hashrate-based double-spending [Электронный ресурс] / M. Rosenfeld. — URL: https://bitcoil.co.il/Doublespend.pdf (Дата обращения 15.05.2019). Загл. с экр. Яз. англ.

3 Building rest services with spring [Электронный ресурс]. — URL: https://spring.io/guides/tutorials/bookmarks/ (Дата обращения 20.05.2019). Загл. с экр. Яз. англ.

4 Sha-256 [Электронный ресурс]. — URL: https://en.bitcoinwiki.org/wiki/SHA-256 (Дата обращения 05.05.2019). Загл. с экр. Яз. англ.

5 *Buterin, V.* Proof of stake: How i learned to love weak subjectivity [Электронный ресурс] / V. Buterin. — URL: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/ (Дата обращения 08.05.2019). Загл. с экр. Яз. англ.

6 Hashcash адама бэка: От борьбы со спамом до цифровой наличности [Электронный ресурс]. — URL: https://coinspot.io/interesting/hashcash-adama-beka-ot-borby-so-spamom-do-cifrovoj-nalichnosti/ (Дата обращения 18.05.2019). Загл. с экр. Яз. рус.

7 51% attack blockchain [Электронный ресурс]. — URL: https://en.bitcoinwiki.org/wiki/51%25_attack (Дата обращения 17.05.2019). Загл. с экр. Яз. англ.