УДК 004.75

Разработка децентрализованного DNS-сервера на основе технологии блокчейн

М. А. Акимов[1*]

[1] Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: mike-98@yandex.ru

Аннотация. В статье рассмотрены сценарии использования классических DNS-серверов и освещены связанные с ними текущие недостатки. Рассмотрена альтернатива в виде распределенного DNS-сервера, основанного на технологии блокчейн, произведено ее сравнение с классическими DNS-серверами с точки зрения информационной безопасности, выделены достоинства и недостатки. Освещены проблемы, связанные с разработкой распределенного DNS-сервера и предложены варианты их решения.

Ключевые слова: информационная безопасность, DNS, распределенный реестр, блокчейн, Etherium

Development of a distributed DNS-server based on blockchain technology

M. A. Akimov[1*]

[1] National Research Nuclear University Mephi, Moscow, Russian Federation
* e-mail: mike-98@yandex.ru

Abstract. The article discusses the scenarios for using classic DNS servers and highlights the current disadvantages associated with them. An alternative in the form of a distributed DNS server based on blockchain technology is considered, it is compared with classical DNS servers in terms of information security, advantages and disadvantages are highlighted. The problems associated with the development of a distributed DNS server are discussed and options for their solution are proposed.

Keywords: Cybersecurity, DNS, distributed ledger, blockchain, Etherium

Введение

Существует множество сценариев, в которых возникает необходимость во владении собственным DNS-сервером. Например, это могут быть задачи корпоративной сети и ее интранета, задачи по ограничению множества обрабатываемых DNS-имен в организации, либо желание иметь свой, независимый DNS-сервер. Однако, при создании собственного DNS-сервера, возникают сразу несколько проблем.

1. Обеспечение отказоустойчивости DNS-сервера.

Если на единственный DNS-сервер будет произведена атака типа «отказ в обслуживании» (DOS), то вся инфраструктура, завязанная на данный сервер, не сможет продолжать свою работу, если для ее выполнения использовались доменные имена, обрабатываемые данным сервером.

2. Зависимость рекурсивных DNS-серверов от корневых DNS-серверов.

Если DNS-сервер не является корневым, то в случае отсутствия у него записи, он обращается к вышестоящему DNS-серверу. Таким образом, отказ в обслуживании какого-либо пула DNS-серверов корневыми серверами через некоторое время, после того как устареет кэш, выведет из строя и дочерние DNS-сервера. Информацию о действующих корневых DNS-серверах можно найти на сайте операторов корневых DNS-серверов https://root-servers.org. Следует отметить, что на территории РФ

3. Зависимость DNS-серверов от внешнего регулятора.

Например, на сегодняшний день множество компаний, предлагающих VPN, также предлагают использовать свой DNS-сервер, аргументируя это тем, что, анализируя запросы на DNS-сервер, можно получить примерную информацию о круге интересов пользователя.

Это действительно так, однако под давлением внешнего регулятора или управляющей организации тот или иной DNS-сервер может не только анализировать, но и подделать или умышленно не обрабатывать те или иные запросы. Если от подделки можно защититься с помощью сертификатов, то в случае отказа обработки доменного имени мы можем потерять доступ к той или иной информации.

4. Возможные атаки на DNS-сервера.

Известны атаки, направленные на отравление кэша DNS, когда до получения официального ответа от вышестоящего DNS-сервера, серверу отправляют заведомо ложный ответ. Такая атака возможна как для локального / офисного DNS-сервера, так и для вышестоящих серверов, не являющихся корневыми.

Кроме того, не стоит забывать о вероятности взлома одного из вышестоящих серверов.

Методы и материалы

Все перечисленные на предыдущих этапах проблемы предлагается решить с помощью распределенного DNS-сервера на основе технологии Блокчейн.

Предлагается следующая архитектура (рис. 1).

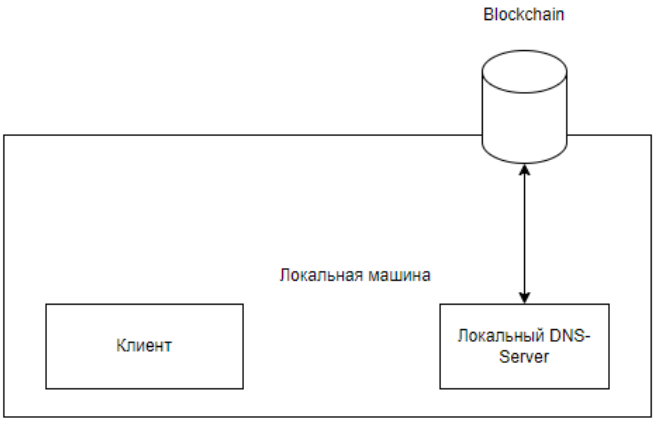

Рис. 1. Предлагаемая архитектура распределенного DNS-сервера

DNS-сервер (Name-сервер, nameserver, NS) – сервер, преобразующий доменные имена, с которыми работают пользователи, в понятные компьютерам IP-адреса или в обратном направлении. Обычно не делают разницы между понятиями NS и DNS-серверов [1].

На представленной схеме Клиенту предлагается взаимодействовать не с внешним DNS-сервером, а с локальным, запрашивающим данные о записях напрямую из распределенной сети.

Описанные выше проблемы решаются следующим образом:

1. Обеспечение отказоустойчивости DNS-сервера.

Распределенные сети в значительной мере более отказоустойчивы чем отдельные сервера. Вывести из строя один сервер проще чем множество.

2. Зависимость рекурсивных DNS-серверов от корневых DNS-серверов.

В данном случае источником для локального DNS-сервера выступает распределенная сеть, которая не может единолично принять решение ограничить к ней доступ какому-либо клиенту.

3. Зависимость DNS-серверов от внешнего регулятора.

Если рассматривать децентрализованную распределенную сеть, например, такую, которую предлагает платформа Ethereum, то в ней не будет единого регулятора, а значит и соответствующих рисков.

4. Возможные атаки на DNS-сервера.

Так как локальное серверное приложение находится на той же машине, что и клиент, то большинство атак на него либо невозможны, либо приведут к необходимости компрометировать машину клиента. В последнем случае любая защита DNS-сервера не имеет смысла, так как злоумышленник будет иметь полный контроль над системой клиента.

Технология Блокчейн (англ. Blockchain, дословно – цепочка блоков) – это технология распределенного реестра, поддерживающая постоянно расширяющийся список нередактируемых блоков/записей с временными метками, связанными друг с другом, образующая цепочку блоков, и устанавливающая правила для транзакций, привязанных к этим блокам [2].

Блокчейн не требует наличия администратора базы данных и централизованного пространства для хранения данных, а добавление новых записей в этот реестр возможно лишь при достижении консенсуса.

Таким образом, использование технологии блокчейн подходит под поставленную задачу создания децентрализованного DNS-сервера и позволит обеспечить отказоустойчивость и целостность реестра, хранящего DNS-записи, одновременно избавляя от рисков, связанных с наличием внешнего или внутреннего регуляторов.

Однако, технология блокчейн обладает рядом особенностей, которые необходимо будет учесть в реализации DNS-сервера, а именно:

а) длительная обработка транзакций. При внесении нового i-того блока в реестр не только большинство узлов должно достигнуть консенсуса, но и должно появиться также несколько блоков после внесенного i-того блока. Время до принятия сетью i+n блоков может достигать 30-ти минут;

б) отклик сети на чтение из реестра тоже не мгновенный, это может повлиять на работу DNS-сервера.

Результаты

В результате работы было разработан DNS-сервер в соответствии с описанной ранее архитектурой.

Для проверки работы DNS-сервера был выбран домен test-server.yo. Ранее нами была добавлена A-запись для имени test-server.yo, ссылающуюся на адрес 127.0.0.1 (localhost). На данный момент на 80-м порту локально поднят сервер и в результате работы dns мы увидим то, что представлено на рис. 2.

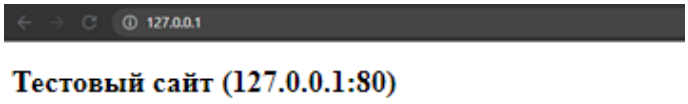

Рис. 2. Ответ сервера, находящегося по адресу 127.0.0.1 на 80-м порту

На текущем этапе система не может сопоставить ip данному DNS-имени (рис. 3).

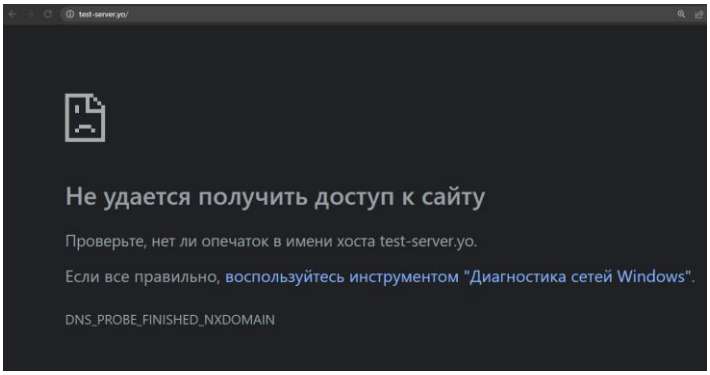

Рис. 3. DNS-сервер отключен, имя test-server.yo не определено

Запускаем наш сервер, обновляем страницу и смотрим вывод (рис. 4).

Рис. 4. Вывод в консоль DNS-server обращается к распределенной сети

DNS-сервер обратился к распределенной сети и прочитал внесенное нами ранее значение 127.0.0.1, соответствующее localhost или локальной машине.

Проверим, получится ли сопоставить ip DNS-имени test-server.yo после запуска сервера (рис. 5).

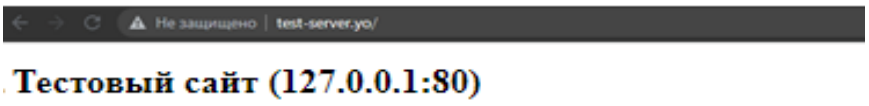

Рис. 5. DNS-сервер отработал успешно

Обсуждение

В рамках экспериментального исследования предложенного подхода в сравнительном анализе с существующими решениями, мы пришли к выводу, что распределенный DNS-сервер уступает обычным по некоторым параметрам, а именно:

По скорости добавления записей. Каждая транзакция в сети должна быть одобрена и закреплена несколькими блоками. Время добавления новой записи в блокчейн может достигать 30 минут.

По скорости ответов. Ответы из распределенной сети приходят достаточно быстро, но этого недостаточно для корректной работы DNS-сервера. Приходится на первый запрос отвечать еще до того, как пришел ответ из распределенной сети, что приводит к необходимости определять DNS по несколько раз.

Вероятно, при старте сервера можно запрашивать все зарегистрированные зоны, однако из-за того, что все операции в реальной сети платные – не известно, будет ли это выгодней.

Для такого сервера необходимо ограничить количество обрабатываемых доменов первого уровня. Например, оставить только «.yo» домены, чтобы не перегружать распределенную сеть запросами всех существующих доменов т.к. ресурсы сети ограничены.

Заключение

В рамках выполненной работы были получены следующие результаты:

Оценены достоинства и недостатки концепции децентрализованного DNS-сервера.

Продемонстрирована жизнеспособность путем успешной реализации распределенного DNS-сервера на платформе блокчейн Ethereum и проверена его работоспособность.

Несмотря на перечисленные недостатки, реализованный в ходе работы сервер обладает важными для обеспечения безопасности взаимодействия с DNS-сервером характеристиками целостности и доступности.

Обеспечивает отказоустойчивость (доступность).

Распределенные сети в значительной мере более отказоустойчивы чем отдельные сервера. Вывести из строя один сервер проще чем множество.

Используемая в реализации распределенная сеть на платформе Ethereum за годы своего существования уже доказала свою надежность при условии грамотного написания смарт-контрактов.

Не зависит от корневых DNS-серверов (доступность).

В данном случае источником для локального DNS-сервера выступает распределенная сеть, которая не может единолично принять решение ограничить к ней доступ какому-либо клиенту.

С точки зрения самого сервера выходит, что каждый локальный DNS-сервер будет являться корневым для каждой машины, на которую он будет установлен.

Не зависит от внешнего регулятора (целостность и доступность).

Платформа Ethereum, используемая в данной реализации, не предполагает наличия единого регулятора, а значит и соответствующих рисков.

Не подвержен типичным атакам на DNS-сервера (целостность).

Так как локальное серверное приложение находится на той же машине что и клиент, то большинство атак на него либо невозможны, либо приведут к необходимости компрометировать машину клиента. В последнем случае любая защита DNS-сервера не имеет смысла, так как злоумышленник будет иметь полный контроль над системой клиента.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Nic.ru. – Режим доступа: https://www.nic.rau.

2. Natalia Miloslavskaya, Alexander Tolstoy, Vladimir Budzko, Maniklal Das, «Blockchain Application for Cybersecurity Management» / Natalia Miloslavskaya, Alexander Tolstoy, Vladimir Budzko, Maniklal Das // «Essentials of Blockchain Technology» - 2019. - 141-168 с. – Режим доступа: https://www.researchgate.net/publication/339720704.