Таким образом, полученная система сочетает в себе такие положительные стороны блокчейна, как неизменяемость и децентрализация, простоту доступа к данным и проверку их подлинности. Помимо этого, организациям, уже имеющим сервер авторизации или свою базу активов, будет не сложно интегрироваться в систему, связывая did пользователя со своей базой пользователей. При этом отсутствует зависимость от публичных блокчейн-сетей и для всех данных и идентификаторов используются публичные стандарты, разрабатываемые консорциумом W3C.

Литература

1. Andries Van Humbeeck, The Blockchain-GDPR Paradox / Andries Van Humbeeck // Медиаплощадка Medium [Электронный ресурс]. – Режим доступа: https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047
2. Gautam Dhameja, GDPR and CRAB—What's the deal? / Gautam Dhameja // Медиаплощадка Medium [Электронный ресурс]. – Режим доступа: https://blog.bigchaindb.com/gdpr-and-crab-whats-the-deal-5c2f6b55d90
3. Chaincode for Developers // Официальная документация Hyperledger Fabric [Электронный ресурс]. – Режим доступа: https://hyperledger-fabric.readthedocs.io/en/latest/chaincode4ade.html
4. Verifiable Credentials Data Model // Официальная документация World Wide Web Consortium (W3C) [Электронный ресурс]. – Режим доступа: https://www.w3.org/TR/verifiable-claims-data-model/
5. Decentralized Identifiers (DIDs) // Официальная документация World Wide Web Consortium (W3C) [Электронный ресурс]. – Режим доступа: https://w3c-ccg.github.io/did-spec/

УДК 004.77

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ «BLOCKCHAIN» ДЛЯ ОРГАНИЗАЦИИ НОТАРИАЛЬНОЙ ДЕЯТЕЛЬНОСТИ

студент Лобач В.О.,
Научный руководитель - к. ф.-м. н. Козадаев К.В.
Белорусский государственный университет
Минск, Беларусь

Нотариальная деятельность считается одной из областей, которую внедрение технологий на базе распределённых децентрализованных сетей способно в корне изменить и улучшить. Хотя в краткосрочной перспективе в силу ограничений на уровне законодательства такие изменения маловероятны, в данной работе рассматривается реализация, способная на это в будущем.

В общем смысле, нотариус является независимым, беспристрастным свидетелем, который документирует наличие или отсутствие определенного факта. На практике нотариус:

- подтверждает подлинность копий / переводов документов;
- проверяет подлинность подписей;
- определяет факты из реального мира.

И если эти функции на данном этапе развития технологий заменить сложно, то улучшить процесс хранения и передачи данных, используемый при документообороте в государственном и частном секторе вполне реально.

Существующие решения в области электронного нотариата и документооборота, как правило, построены на базе централизованных сетей и реляционных СУБД. Подобные решения подходят для небольших масштабов, но в силу своей архитектуры

плохо подходят для систем, при проектировании которых важны горизонтальное масштабирование, производительность при обработке большого объёма данных и безопасность.

Разработанное решение, основанное на технологиях блокчейн и IPFS, обеспечивает высокий уровень защищённости и распределённости, что позволяет внедрить и использовать его в любой сфере, связанной с документами и персональными данными, будь то финансовый, юридический, частный или военный сектор.

Концепция технологии блокчейн предложена Сатоши Накамото в 2008 году, а впервые применена на практике при появлении биткоина в 2009-м.

Система работает следующим образом:

- Создается первичный блок, в нем отсутствует запись о предыдущем блоке.
- Каждый последующий блок содержит информацию о «родителе», в виде транзакции в собственном заголовке, используемом при генерации очередного блока.
- Пользователи системы видят все количество блоков, но обладают доступом лишь к своим.
- Любые изменения без подтверждения криптографическими ключами отклоняются.
- Передача закрытого ключа предоставляет полный доступ к блоку (деньгам и иным активам). Благодаря этому легко регистрировать сделки, проводимые через онлайн-ресурсы.

Ключевая особенность технологии заключается в децентрализации системы. Если базу данных, расположенную на едином сервере, взломать теоретически можно при условии применения любых существующих средств защиты, то с блокчейном ни один из этих методов не сработает. Простыми словами – там нечего взламывать [1, 2].

Однако, в силу особенностей архитектуры и высокой вычислительной сложности при добавлении новых блоков, блокчейн совершенно не подходит для хранения больших объёмов данных.

Для этой проблемы существует целый ряд решений. Одно из них – IPFS [3]. Это одноранговый P2P протокол, в котором каждый узел хранит коллекцию хешированных файлов (рисунок 1). У IPFS есть ряд недостатков, например, неизменяемость данных и необходимость для узлов быть определённое время в сети. Но в контексте применения в области нотариата эти недостатки нивелируются.

У IPFS есть ещё один недостаток. Если у злоумышленника есть хэш-сумма документа, он может получить к нему доступ. Поэтому важные файлы не подходят для IPFS в их исходном состоянии. Следовательно, разумно использовать дополнительные инструменты шифрования для защиты файлов перед их загрузкой в IPFS.

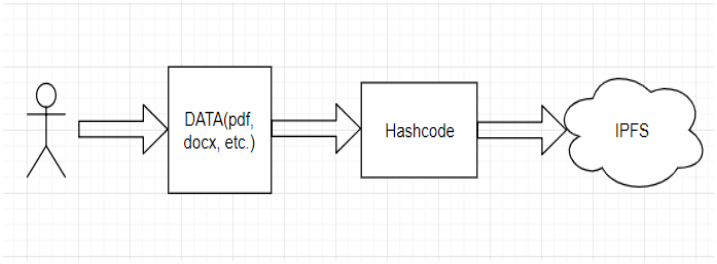

Рис. 1. Принцип работы IPFS

В разработанной системе используется сочетание технологий блокчейн и IPFS. Вместо хранения самих файлов в блокчейне хранится их хэш-сумма. Это даёт возможность реализовать механизм децентрализованного хранения важных документов с возможностью доступа к ним всем участникам сети и механизмы proof of existence и proof of ownership (рисунок 2).

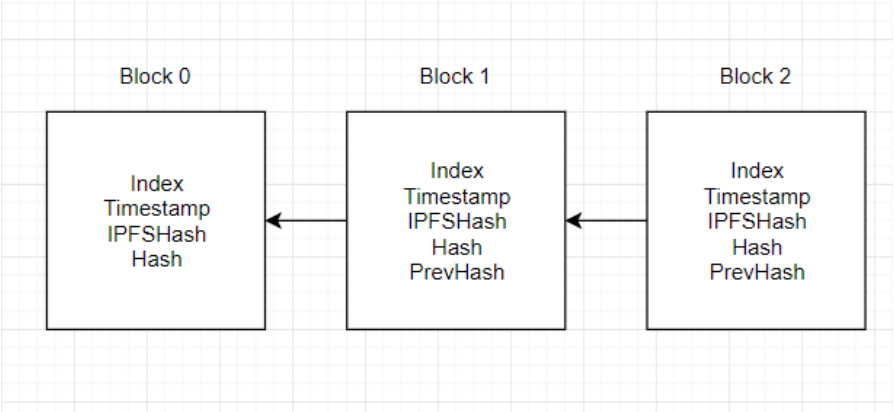

Рис. 2. Применение blockchain для хранения хэш-сумм файлов

Разработанное приложение состоит из 2 модулей. Первый – реализация цепочки транзакций в виде блокчейн при помощи языка Go. Включает в себя описание структуры блока записи, алгоритмы хэширования и генерации новых блоков, валидации для разрешения коллизий внутри цепочки транзакций, а также серверную логику для возможности работать в фоновом режиме и коммуницировать с другими сервисами по REST API. Коллизии в блокчейне разрешаются по алгоритму Proof-of-Storage. Этот модуль используется для хранения хэш-сумм файлов в IPFS.

Второй – реализация интерфейса для взаимодействия с IPFS, а также логика для шифрования/дешифрования файлов алгоритмом SHA256 и REST API для доступа к системе по протоколу HTTP и взаимодействия с блокчейн. Разработан модуль при помощи языка Java и асинхронного фреймворка Vert.x. Помимо этого, в рамках IPFS реализовано кластерное решение, создающее приватную подсеть в рамках глобальной. Это гарантирует, что доступ к конфиденциальным данным получат только те узлы, которые имеют на это право.

При добавлении файла в систему он проходит через блок Java application, сам файл шифруется и помещается в IPFS, а его хэш помещается в новый блок цепи транзакций блокчейн (рисунок 3). При попытке доступа к файлу по хэш-коду из блокчейна происходит проверка, находится ли узел, с которого выполняется запрос, в рамках приватной подсети. Если узел проходит проверку, то по хэш-коду обрабатывается запрос к IPFS на получение файла, после чего файл дешифруется. Неизменяемость файлов гарантирует целостность внутри сети. Есть возможность хранить целые группы файлов, получать к ним доступ через браузер или сохранять локально.

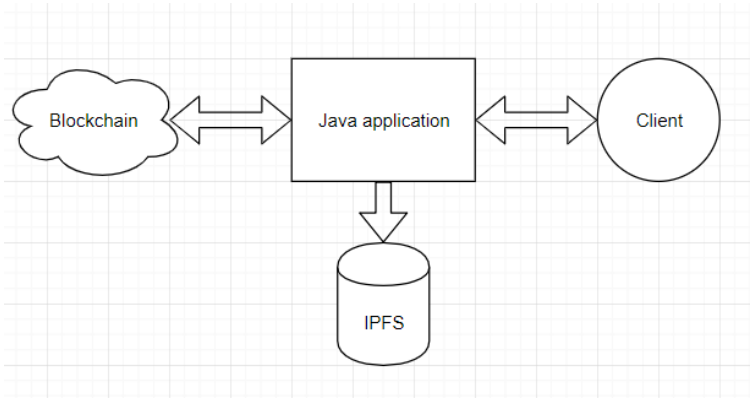

Рис.3. Блок-схема работы приложения

Таким образом, разработанная система позволяет хранить любые документы в IPFS и получать к ним доступ из любого узла, у которого есть на это право. При этом все требования по безопасности личных данных обеспечиваются на уровне самой

технологии, используемой в реализации. Подобное приложение способно существенно облегчить работу в сфере нотариата и документооборота, позволяя получить нужный документ из любого места в рамках сети без необходимости проверять его подлинность и целостность. При этом внедрение этой системы не лишит работы юристов, финансистов и банковских служащих, т.к. содержимое документов, хранимых в сети – всё ещё зона ответственности человека.

Литература

1. Swan, M. Blockchain: Blueprint for a New Economy. — O'Reilly Media, Inc., 2015. — 152 p.
2. Лелу, Л. Блокчейн от А до Я. Все о технологии десятилетия. — Москва: Эксмо, 2018. — 256 с.
3. Inter Planetary File System Project Documentation [Electronic resource. – Mode of access: https://docs.ipfs.io. Date of access: 20.11.2018.

УДК 004.93’1

Q-ПРЕОБРАЗОВАНИЕ ДЛЯ ОБРАБОТКИ ПОЛИФОНИЧЕСКОЙ МУЗЫКИ

магистрант Огородникова Е В.,
Научный руководитель - к. ф.-м. н., доцент Козлова Е.И.
Белорусский государственный университет
Минск, Беларусь

Первым шагом в алгоритме распознавания нот часто является представление звукозаписи в виде спектрограммы. Из-за природы звука, задача определения начала сыгранной ноты и ее длительности является нетривиальной. На сегодняшний день нет единого подхода, решающего данную проблему. Известными методами получения спектра являются дискретное оконное преобразование Фурье, Q-преобразование и гребенчатые фильтры. На практике себя хорошо зарекомендовало применение постоянного Q-преобразования [1].

Каждый звук является совокупностью гармонических колебаний, в которой выделяется основной тон и дополнительные – обертоны. Человек воспринимает звуки в диапазоне от 16 до 20 000 Гц. Звуки с частотами f_0 и $2f_0$ воспринимаются как очень похожие. Частоты кратные f_0 объединяются в тональный класс. В классической европейской музыке, например, преобладает использование равномерно темперированного строя. В типичном случае каждая октава представляет собой музыкальный интервал, в котором соотношение частот между звуками составляет один к двум. Этот интервал делится на *двенадцать* полутонов (нот). Ноты, принадлежащие одному тональному классу, имеют одинаковые названия [2].

Таким образом, в равномерно темперированном строе можно выделить 12 тональных классов. Частоту n-ой ноты можно вычислить по формуле (1):

$$f_n = 2^{\frac{n}{N_0}} f_0, \tag{1}$$

где N_0 – количество компонент в одной октаве, f_0 – частота настройки. Обычно выбирают f_0 = 440 Гц, что соответствует ноте ля 1-й октавы. Благодаря равномерной темперации появляется возможность транспонирования музыкального произведения на произвольный интервал.

Первым шагом в алгоритме распознавания нот является представление звука в виде спектрограммы – распределения звуковой энергии по частотам со временем. Спектрограммы звука обычно состоят только из двух основных форм: гармоник, которые являются узкополосными, охватывают короткий частотный диапазон и имеют