визуально неразличимые по сравнению с большим количеством фильтров результаты при большей скорости обучения.

В качестве функции потерь использовалась кросс-энтропия, а в качестве оптимизатора – алгоритм стохастического градиентного спуска с адаптивной оценкой моментов (adam). В роли меры качества восстановленного изображения (рисунок 1) использовался критерий соотношения сигнал/шум (PSNR) [2].

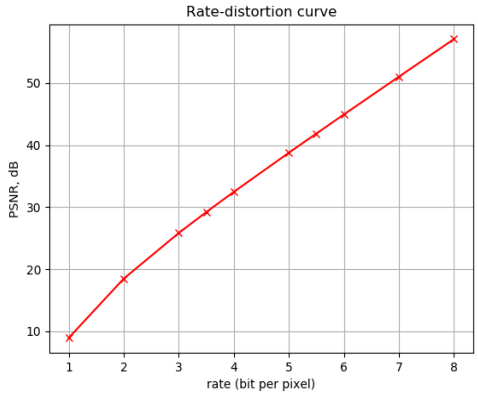

Рис. 1. Зависимость степени сжатия (бит/пиксель) от оценки сигнал/шум (PSNR)

В работе удалось достичь главной цели исследования – сжать данные. Несмотря на неполную репрезентативность используемых в обучении изображений, полученные результаты показывают возможность использования этого алгоритма для сжатия. В перспективе нейронную сеть планируется обучить для работы с реальными полноразмерными изображениями.

Литература

1. Goodfellow I. Deep learning / I. Goodfellow, Y. Benjio, A. Courville. — Cambridge : MIT press, 2016. — 800 p.

2. Toderici G. Full Resolution Image Compression with Recurrent Neural Networks / G. Toderici, D. Vincent, N. Johnston //CVPR. – 2017. – P. 5435-5443.

УДК 004.75

ДЕЦЕНТРАЛИЗОВАННЫЙ РЕЕСТР РЕЗЮМЕ НА БАЗЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

магистрант Баслак О.В.,
Научный руководитель – академик НАН Беларуси Чернявский А.Ф.
Белорусский государственный университет
Минск, Беларусь

В современном мире стоит вопрос о подделке данных, содержащихся в резюме, таких как аттестат или диплом об образовании, сертификаты о прохождении курсов, опыт работы и обязанности. Зачастую появляется необходимость доказать наличие образования, полученного десятки лет назад, но диплом потерян, и необходимо его восстановление, бумага в архиве университета выцвела, или сам архив уничтожен, либо само учебное заведение было расформировано.

Реестр резюме, построенный с использованием технологии блокчейн, дает следующие преимущества:

- простое подтверждение подлинности данных,

- контроль владельцем личных данных доступа к ним,
- наличие истории выдачи активов (сертификатов) и доступа к этим данным [1].

Среди существующих решений можно рассмотреть, например, IPDB (Interplanetary database) на базе BigchainDb, а также все решения, использующие блокчейн как полноценную базу данных. Они дают пользователю права на создание и передачу активов другим пользователям, вся история при этом сохраняется в блокчейн, однако они не позволяют удалить данные об активах.

Такое решение не соотносится с законами об обработке и хранении персональных данных, как, например, «Общий регламент по защите данных (GDPR)», хотя и вводится такое понятие как «burn-операция» (сжигание) вместо удаления в стандартном наборе операций из создания, чтения, изменения и удаления [2].

Другая категория приложений хранит в блокчейне только верификационную информацию, а сами данные при этом хранятся в обыкновенной базе данных. Например, Acclaim или Accredible, использующий открытый протокол Chainpoint для сохранения хеша данных о сертификате или бейдже в блокчейн Bitcoin. Сам по себе протокол Chainpoint подразумевает использование открытого блокчейна для сохранения данных вместе с транзакцией. Минусом данного подхода является использование стороннего блокчейна. В случае, если его использование прекратится, и все узлы пропадут из сети, все данные для валидации (хеши) пропадут вместе с ним.

В разработку Hyperledger Fabric было внесено предложение по работе с приватными данными и в данный момент эта возможность находится в активной разработке, однако для этого необходимо создание конфигурационного файла *collections_config.json*, который распространяется по всем узлам в сети. В нем содержится информация о том, кто кому на какие данные дал доступ, что очень неудобно с точки зрения бизнеса [3].

В данной работе предлагается следующее решение. На каждом узле сети, которые являются членами консорциума, разворачивается блокчейн на базе Hyperledger Fabric. Узлами сети могут быть организации, заинтересованные в подтверждении данных через блокчейн. Это могут быть правительственные структуры, центры занятости, учреждения образования, центры сертификации, проводящие различные экзамены на получение сертификата и т.д.

Все данные для резюме создаются в виде Verifiable Credential (рисунок 1) [4].

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://example.com/examples/v1"
  ],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science in Mechanical Engineering"
    }
  },
  "proof": { ... }
}
```

Рис 1. Пример структуры записи с использованием распределённого идентификатора организации

Все узлы сети используют блокчейн для хранения хешей выданных бейджей, логирования кто и когда получал доступ к тем или иным данным (рисунок 2).

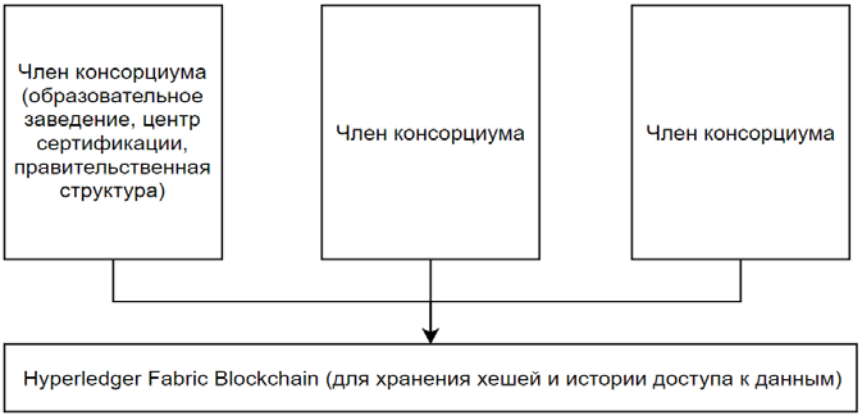

Рис 2. Архитектура системы

Каждый член консорциума, желающий вносить свои данные в блокчейн, создает децентрализованный идентификатор (Decentralized ID, или DID [5]), который будет содержаться в данных, добавляемых в блокчейн. Данные о DID вместе с публичным ключами также сохраняются в блокчейн, т.к. по задумке создателей, идентификаторы не изменяемы. При этом сами идентификаторы могут быть опубликованы в достоверных источниках.

Каждый узел консорциума хранит заверенные им данные у себя, но всегда остается возможность владельцу данных загрузить, например, свой сертификат в формате json и запросить удаление своих данных из базы организации-узла. Имея только json-файл сертификата, можно проверять его подлинность по хешу в блокчейне.

Для доступа к данным используется общее для всех клиентское приложение (или веб-сервис), использующее общий API, которое соединяется с серверами узлов сети. Приложение выполняет роль хранилища идентификаторов, как кошельки в криптовалютных блокчейнах (рисунок 3). Для владельцев активов (те, кому выдаются сертификаты, дипломы и т.д.) также создается децентрализованный id. В базе узла, выдающего актив, сохраняется запись, соотносящая пользователя с его DID.

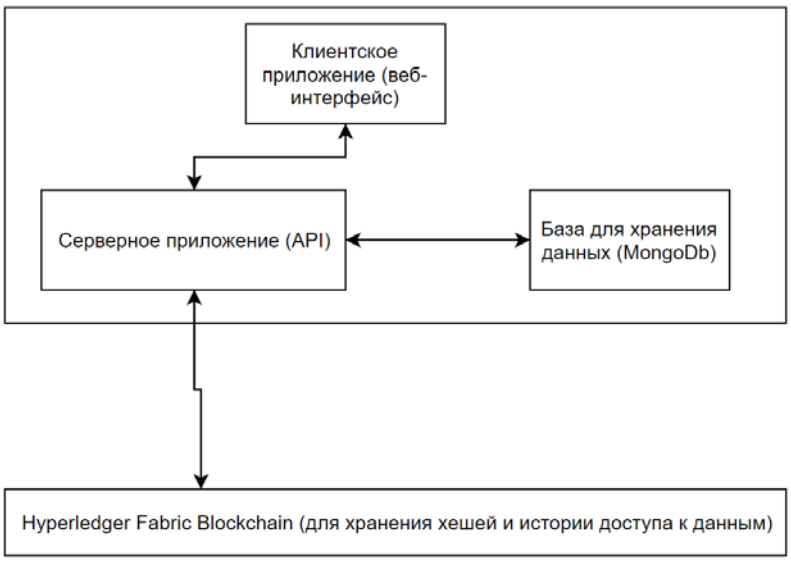

Рис 3. Архитектура узлов системы

В качестве точек расширения остается возможность для регулирования доступа к данным по запросу с возможностью его отклонения, записи таких запросов, а также их результатов.

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