УДК 004.056.5

АНАЛИЗ ПРОБЛЕМ ВНЕДРЕНИЯ ДЕЦЕНТРАЛИЗОВАННОЙ ИДЕНТИФИКАЦИЯ ЛИЧНОСТИ НА ОСНОВЕ ТЕХНОЛОГИИ БЛОКЧЕЙНА

П. О. Ковалев

Белорусский государственный университет, Беларусь, Минск,
kovalevpo2001@gmail.com

Рассмотрена проблема идентификации на основе технологии блокчейн, обусловленная необходимостью повышения безопасности данных, обеспечения конфиденциальности и устранения зависимости от централизованных провайдеров. Проанализированы методы построения систем самосуверенной идентичности. Представлены механизмы защиты персональных данных с применением криптографических доказательств.

Ключевые слова: блокчейн; децентрализованная идентификация; самосуверенная идентичность; цифровой идентификатор; верифицируемые учетные данные; защита персональных данных.

ANALYSIS OF THE CHALLENGES OF IMPLEMENTING DECENTRALISED PERSONAL IDENTIFICATION BASED ON BLOCKCHAIN TECHNOLOGY

P. O. Kovalev

Belarussian state university, Belarus, Minsk, kovalevpo2001@gmail.com

The problem of identification based on blockchain technology is considered, caused by the need to improve data security, ensure confidentiality and eliminate dependence on centralized providers. Methods for constructing self-sovereign identity systems are analyzed. Mechanisms for protecting personal data using cryptographic evidence are presented.

Keywords: blockchain; decentralised identification; self-sovereign identity; digital identifier; verifiable credentials; personal data protection.

Введение

Проблема идентификации личности в цифровом пространстве становится все более актуальной в связи с ростом числа онлайн-сервисов, требующих подтверждения личности пользователей. Традиционные централизованные системы идентификации имеют ряд недостатков, включая риски утечки данных, зависимость от доверенных посредников и отсутствие контроля пользователей над своими персональными данными. Де-

централизованная идентификация на основе технологии блокчейн предлагает альтернативный подход, позволяющий пользователям самостоятельно управлять своими цифровыми идентификаторами без необходимости полагаться на центральный орган [1].

Для создания систем децентрализованной идентификации, блокчейн используется в качестве надежной инфраструктуры для хранения и верификации цифровых идентификаторов и связанных с ними метаданных. Важно отметить, что сами персональные данные обычно не хранятся в блокчейне из соображений конфиденциальности и соответствия нормативным требованиям. Вместо этого в блокчейне размещаются децентрализованные идентификаторы, которые служат указателями на верифицируемые учетные данные, хранящиеся в защищенных децентрализованных хранилищах или на устройствах пользователей [2].

Возможности внедрения децентрализованной идентификации и сферы применения

Ключевой концепцией децентрализованной идентификации является самосуверенная идентичность (Self-Sovereign Identity, SSI), которая предоставляет пользователям полный контроль над своими персональными данными. В модели SSI пользователь создает собственные децентрализованные идентификаторы, получает верифицируемые учетные данные от доверенных эмитентов и самостоятельно решает, какие данные раскрывать проверяющим сторонам [3].

Процесс работы системы SSI. Система самосуверенной идентичности включает следующие этапы:

1. Создание идентификатора: пользователь генерирует пару криптографических ключей и регистрирует DID в блокчейне.
2. Получение учетных данных: авторитетные организации (государственные органы, учебные заведения, работодатели) выдают пользователю верифицируемые учетные данные, подписанные их цифровыми подписями.
3. Хранение данных: пользователь хранит полученные учетные данные в своем цифровом кошельке.
4. Предъявление данных: при необходимости пользователь может предоставить верифицируемые учетные данные третьим сторонам, создавая криптографические доказательства без раскрытия всей информации.
5. Верификация: проверяющая сторона может удостовериться в подлинности предоставленных данных, проверив цифровую подпись эмитента через блокчейн, без необходимости связываться с ним напрямую.

Сферы применения. Децентрализованная идентификация на основе блокчейна может быть эффективно внедрена в следующих областях:

- Государственные услуги: создание единой цифровой идентичности гражданина для доступа к государственным услугам с сохранением конфиденциальности и минимизацией административных издержек.
- Финансовый сектор: упрощение процедур KYC (Know Your Customer) и AML (Anti-Money Laundering), снижение рисков мошенничества и обеспечение трансграничной идентификации.
- Здравоохранение: управление медицинскими данными пациентов с возможностью избирательного раскрытия информации медицинским учреждениям при сохранении конфиденциальности.
- Образование: верификация академических достижений и квалификаций без необходимости обращения в учебные заведения.
- Трудоустройство: проверка квалификации соискателей и подтверждение трудового опыта.
- Онлайн-сервисы: упрощение процессов аутентификации и авторизации без необходимости создания множества учетных записей и паролей.

Преимущества использования:

- Повышение контроля пользователей над персональными данными: владельцы данных самостоятельно решают, какую информацию, кому и когда предоставлять.
- Минимизация раскрытия информации: возможность предоставления только необходимых данных с использованием избирательного раскрытия и нулевого разглашения знаний.
- Устранение зависимости от централизованных провайдеров идентификации: снижение рисков компрометации данных при взломе или отказе центральных серверов.
- Повышение надежности идентификации: криптографическая верификация данных и невозможность их подделки.
- Переносимость идентификационных данных: возможность использовать один набор верифицируемых учетных данных в различных системах и сервисах.
- Снижение административных издержек: устранение необходимости повторной верификации данных разными организациями.
- Устойчивость к цензуре: невозможность блокирования доступа к идентификационным данным третьими сторонами.

Недостатки использования:

- Технологические барьеры: сложность внедрения и интеграции с существующими системами идентификации.
- Проблемы масштабируемости: ограничения производительности и пропускной способности публичных блокчейнов.
- Правовые и регуляторные вызовы.
- Управление ключами: риски потери приватных ключей.

• Социальное принятие: необходимость повышения технической грамотности пользователей.

• Отсутствие стандартизации: несовместимость различных систем децентрализованной идентификации из-за отсутствия единых стандартов.

Результаты и возможные решение проблем внедрения

В ходе исследования были проанализированы ключевые проблемы, препятствующие широкому внедрению систем децентрализованной идентификации, и разработаны потенциальные решения этих проблем. Результаты исследования показывают, что современные технологические разработки и методологические подходы способны преодолеть большинство существующих барьеров при условии системного подхода к их внедрению.

Проблема масштабируемости и производительности

• Использование слоев второго уровня (Layer 2): внедрение решений, позволяющих обрабатывать большую часть транзакций за пределами основного блокчейна.

• Применение консорциумных блокчейнов: создание специализированных блокчейн-сетей для идентификации с ограниченным числом доверенных валидаторов.

• Оптимизация данных: хранение в блокчейне только минимально необходимой информации (хеши и метаданные), а не полных верифицируемых учетных данных.

Вопросы конфиденциальности и защиты данных

• Внедрение технологий с нулевым разглашением знаний для криптографического доказательства владения информацией без её раскрытия.

• Разработка гибридных архитектур: комбинация блокчейна с децентрализованными хранилищами данных для обеспечения контроля доступа к конфиденциальной информации.

Проблема управления ключами

• Внедрение социального восстановления: разделение секретов между доверенными лицами для восстановления доступа при потере ключей.

• Многофакторная аутентификация: использование комбинации биометрии, аппаратных токенов и паролей для снижения рисков компрометации.

• Системы доверенного хранения: разработка безопасных облачных решений для резервного копирования ключей со строгим контролем доступа.

Отсутствие стандартов и нормативно-правовой базы

- Участие в разработке стандартов: поддержка инициатив W3C по стандартизации децентрализованных идентификаторов (DID) и верифицируемых учетных данных (VC).
- Сотрудничество с регуляторами: взаимодействие с государственными органами для разработки нормативной базы, соответствующей технологическим возможностям блокчейна.
- Создание отраслевых консорциумов: объединение компаний и организаций для разработки общих подходов к внедрению децентрализованной идентификации.

Библиографические ссылки

1. World Economic Forum. Digital Identity [Электронный ресурс]. Режим доступа: https://widgets.weforum.org/blockchain-toolkit/digital-identity/index.html (дата доступа 15.03.2025)

2. *Alex Preukschat.* Self-Sovereign Identity: Decentralized digital identity and verifiable credentials // Manning Publications, 2021. 504c.

3. *Allen, C.* The Path to Self-Sovereign Identity. [Электронный ресурс]. Режим доступа: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity (дата доступа 15.03.2025)