**Применение доказательства с нулевым разглашением в децентрализованных идентификаторах**

***Чжан Ифу***

*Студент (магистр)*

*Московский государственный университет имени М.В.Ломоносова,*

*Институт русского языка и культуры, Москва, Россия*

*E-mail:* [*vsszhang@outlook.com*](mailto:vsszhang@outlook.com)

С ростом потребности в цифровой идентификации системы децентрализованных идентификаторов (DID) и верифицируемых удостоверений (VC), рекомендованные консорциумом W3C, постепенно становятся основой нового поколения решений управления цифровой идентичностью. Однако традиционные централизованные и федеративные модели по-прежнему недостаточно эффективны в вопросах защиты приватности и предоставления пользователям контроля над личными данными. Использование технологии самосуверенной идентичности (SSI), основанной на блокчейне, позволяет решить указанные проблемы: пользователи получают возможность самостоятельно контролировать способ и степень раскрытия личной информации, что способствует переходу к новой парадигме управления цифровой идентичностью.

Тем не менее, VC по-прежнему содержат чувствительные данные, что особенно актуально в таких сферах, как здравоохранение и финансы. Для решения данной проблемы в настоящей работе предлагается интеграция доказательств с нулевым разглашением (ZKP) в систему VC на основе виртуальной машины miden-vm с использованием протокола STARK и криптографического алгоритма Rescue Prime. В результате пользователь может подтвердить наличие требуемых атрибутов без раскрытия самих данных, существенно повышая безопасность и приватность системы.

Разработанная в рамках исследования инфраструктура совместима с моделями данных DID и VC, предложенными W3C, а её практическая эффективность и надёжность были подтверждены экспериментально. Результаты продемонстрировали способность предложенного подхода защищать конфиденциальные данные и обеспечивать надёжность идентификации, указывая на высокую перспективность интеграции DID и ZKP в области цифровой идентичности.

**Литература**

1. Decentralized Identifiers (DIDs) v1.0 [Электронный ресурс]. – W3C, 2022. – URL: https://www.w3.org/TR/did-1.0/ (дата обращения: 07.03.2025).
2. Preukschat A., Reed D. Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials. – Shelter Island: Manning Publications, 2021. – С. 57–59.
3. Мукшашфиду Скувутешфды Вфеф Ьщвуд м2ю0 хЭлектронный ресурсъю – Ц3Сб 2022ю – ГКДЖ реезыЖ..цццюц3ющкп.ЕК.мс-вфеф-ьщвуд. (дата обращенияЖ 07ю03ю2025)ю