ARTICLE HISTORY: Received: April 13, 2022 Accepted: June 6, 2022 Published: June 13, 2022

УДК: 004.67

ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ ПРИНЦИПОВ ДЕЦЕНТРАЛИЗОВАННОЙ ИДЕНТИЧНОСТИ В ЕВРОПЕЙСКОМ СОЮЗЕ

Ермолаев К. А.
Ermolaev K. A.
Кандидат экономических наук, доцент кафедры инноваций и инвестиций
PhD in Economics, Associate Professor of the Department of Innovations and Investments
Казанский (Приволжский) Федеральный Университет
Kazan (Volga region) Federal University
Казань, Россия
Kazan, Russia
Ёрматов Ш. Э.
Yormatov S.E.
Магистрант
Master student
Национальный исследовательский университет «Высшая школа экономики»
National Research University «Higher School of Economics»
Санкт-Петербург, Россия
Saint-Petersburg, Russia

TECHNOLOGICAL ASPECTS OF IMPLEMENTING THE PRINCIPLES OF DECENTRALIZED IDENTITY IN THE EUROPEAN UNION

Аннотация: В статье рассмотрены ключевые предпосылки и нормативно-правовые условия перехода к новой модели управления персональными данными и обеспечения кибербезопасности в Европейском союзе. Разобраны демонстрационные примеры реализации принципов децентрализованной идентичности с позиции организационно-ролевой и функциональной моделей, которые предопределяют требования к технической и информационной архитектуре для их реализации. По результатам проведенного анализа были с одной стороны, сформулированы ключевые драйверы развития и наиболее перспективные сферы применения технологий децентрализованной идентичности, а с другой стороны, технические сложности, препятствующие их масштабному применению в настоящее время.

Abstract: The article discusses the key prerequisites and regulatory conditions for the transition to a new model for managing personal data and ensuring cybersecurity in the European Union. Demonstration examples of the implementation of the principles of decentralized identity are analyzed from the standpoint of organizational-role and functional models that predetermine the requirements for the technical and information architecture for their implementation. Based on the results of the analysis, on the one hand, the key drivers of development and the most promising areas of application of decentralized identity technologies were formulated, and on the other hand, technical difficulties that prevent their large-scale application at present.

Ключевые слова: Децентрализованная идентичность, блокчейн, цифровизация, инновации, кибербезопасность

Key words: Decentralized identity, blockchain, digitalization, innovations, cyber security

Глобальная цифровизация мировой экономики обуславливает необходимость формирования нового подхода к организации сбора, хранения и передачи пользовательских данных в рамках процессов цифровой идентификации пользователей. Рост утечки персональных данных и зависимость пользователей от транснациональных компаний, аккумулирующих персональные данные, входят в число драйверов разработки новых систем информационной безопасности в цифровом пространстве [1, с. 3].

Децентрализованная или суверенная идентичность, которая в зарубежной литературе обозначается терминами “decentralized identity” или “self-sovereign identity”, набирает популярность как наиболее безопасная современная модель сбора, хранения, передачи и использования личных данных пользователей [2, с. 4]. Владелец идентификационной информации, в качестве которого выступает физическое лицо или компания, в рамках этой модели имеет более широкий контроль над своими данными и принимает решение об условиях и путях передачи данных третьим лицам. Реализация децентрализованной идентичности предполагает

использование технологий распределенного реестра, цифровых кошельков и криптографической защиты информации.

Кроме того, внедрение новой технологической базы идентификации пользователей требует принятия соответствующих законов и нормативных актов. С этой целью 23 июля 2014 года был подписан Регламент Европейского Союза № 910/2014 “Об электронной идентификации и доверительных услугах для электронных транзакций на внутреннем рынке” (Регламент eIDAS). Регламент eIDAS обеспечивает нормативно-правовую среду для безопасного и бесперебойного электронного взаимодействия между государственными структурами, гражданами и коммерческими организациями. В том числе, принятый стандарт гарантирует использование национальных схем электронной идентификации (eID) для доступа к государственным услугам в других странах Европейского Союза, обеспечивает стандартизацию и географическую унификацию идентификационных данных, то есть принятие единых стандартов цифровой идентичности в пределах Европейского Союза. Важно отметить, что этот шаг адаптирует пространство Европейского Союза для цифрового взаимодействия на различных уровнях, гарантируя трансграничное функционирование и признание наряду с традиционными бумажными процессами. Таким образом, регламентированное внедрение принципов децентрализованной идентичности в пределах конкретного региона формирует пространство доверия, которое обозначается в зарубежных источниках термином “trust framework”, частью которого становятся государственные структуры, компании и физические лица.

Пример реализации подхода децентрализованной идентичности представлен на графике (рис. 1) и может быть описан с использованием следующих основных терминов:

1) *Эмитент* – организация, ответственная за выпуск идентификационных данных о пользователе. Эмитент имеет возможность выпускать идентификационные данные, добавлять их в блокчейн хранилище, формировать и выдавать приватные ключи доступа к хранилищам, присваивать цифровые подписи. В лице эмитента, в рамках децентрализованной идентичности, может выступать как государственный орган, так и частная компания, наделенная полномочиями по выпуску идентификационных данных в форме криптографически защищенных децентрализованных идентификаторов.

2) *Пользователь* – это субъект децентрализованной идентичности и собственник идентификационных данных. Пользователем может быть как физическое так и юридическое лицо.

3) *Верификатор* – сторона, которой пользователь предоставляет требуемый объем минимально установленных данных в виде кода децентрализованных идентификаторов в процессе получения услуги или покупки продукта.

4) *Идентификационные данные (ИД)* – криптографически зашифрованные личные данные пользователя, сформированные эмитентом или ответственным органом и в последующем хранимые в децентрализованных базах данных для автоматизированного подтверждения или опровержения информации о пользователе по требованиям верификатора в любой момент времени, в том числе при принятии решения об оказании услуг или продаже товара.

5) *Децентрализованные идентификаторы* – идентификационный алгоритм в составе документа децентрализованной идентификации (DID Document), обеспечивающий автономное признание в цифровом пространстве. Иными словами, децентрализованные идентификаторы позволяют определить, подтвердить или опровергнуть информацию об организации, отдельном лице или любом другом объекте, которая хранится в децентрализованных хранилищах данных (блокчейн).

6) *Ключи децентрализованных идентификаторов* – составная часть алгоритмов децентрализованной идентичности на основе криптографического шифрования, являющиеся уникальными и позволяющие получить автоматизированный доступ к продукту или услуге.

7) *Цифровые кошельки* – личное хранилище децентрализованных идентификаторов и ключей доступа пользователя с возможностью выборочного предоставления минимально необходимой информации при использовании продукта или услуги.

8) *Блокчейн хранилище* – распределенная цепочка блоков хранения криптографически зашифрованных данных, обладающие высоким уровнем безопасности.

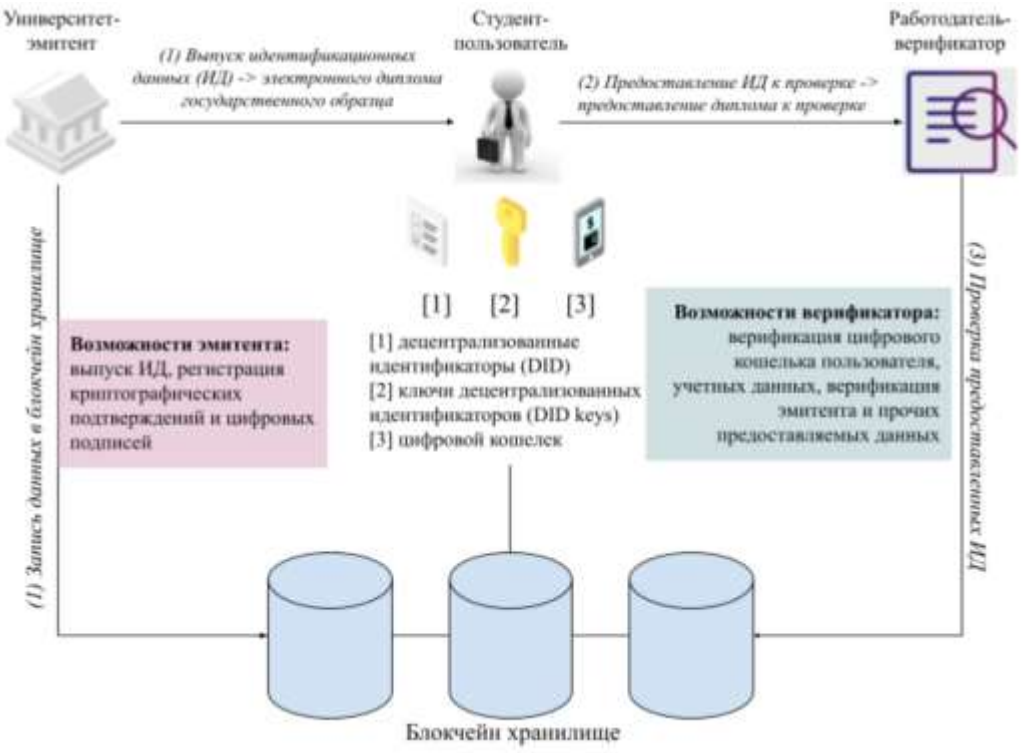

Рисунок 1. Пример реализации подхода децентрализованной идентичности (источник: на основе данных [1])

В рамках этого примера рассматривается трудоустройство студента и подтверждение электронного диплома работодателем. Рассмотрим каждый шаг подробнее:

1) После окончания учебных курсов и сдачи студентом соответствующих экзаменов университет - *эмитент* - формирует электронный диплом в виде кода и делится им со студентом в рамках криптографически зашифрованной операции. Параллельно электронный диплом записывается и отправляется в *блокчейн хранилище*.

Полученный *студентом-пользователем* код, содержащий установленный объем классической для диплома информации, с этого момента является частью массива *идентификационных данных* студента и называется *децентрализованным идентификатором* пользователя. Совокупность идентификационных данных *пользователя*, включая полученный диплом, формируют его цифровую идентичность.

Студент хранит полученный код в *цифровом кошельке*, доступ к которому он имеет, например, через биометрические данные. Наряду с этим студент имеет *ключи децентрализованных идентификаторов* или, иначе говоря, приватный ключ к блокчейн хранилищу, для проверки собственных децентрализованных идентификаторов.

2) На втором шаге *студент-пользователь* делится дипломом в виде криптографически зашифрованного кода с работодателем через *цифровой кошелек*.

3) *Работодатель-верификатор* отправляет запрос на подтверждение информации о подлинности предоставленных студентом данных. *Блокчейн хранилище* автоматически обрабатывает запрос и отправляет соответствующую обратную связь работодателю.

В случае подтверждения предоставленных данных работодатель может принять решение о соответствии кандидата требованиям позиции. При этом “глубина” подтверждения настраивается пользователем и варьируется от информационного сообщения о наличии такого диплома, до предоставления полных данных по диплому.

Преимущества такого подхода для описанного примера заключаются в следующем: для работодателя - выявить недостоверные данные со стороны недобросовестных кандидатов, обеспечить проверку идентификационной информации пользователя в режиме реального времени; для пользователя - ускорить трудоустройство и передавать работодателю только необходимую информацию, исключить использование идентификационной информации третьими лицами; для университета - автоматизировать процессы выдачи дипломов, хранения архивной информации, выдачи справок об обучении, восстановления потерянных дипломов, обеспечить информационную безопасность хранимых данных.

Возможности применения децентрализованной идентичности в пределах нескольких стран, входящих в пространство доверия, можно продемонстрировать внедрением и признанием электронного паспорта [3, с. 1]. Например, путешественник из страны А потерял паспорт в стране В, что не является уникальной ситуацией. Проверка личности туриста и восстановление документа займет определенное количество времени, моральных и финансовых издержек. С внедрением децентрализованной идентичности и принципов единого пространства доверия, такой турист имел бы возможность использовать электронный паспорт, который хранится в его цифровом кошельке в виде криптографически защищенного кода. Процессы активизации электронного паспорта автоматизированы и оперативны за счет скорости блокчейн сети, в которую входят обе страны единого пространства доверия.

Еще один пример удобства использования децентрализованной идентичности в пределах нескольких стран можно привести в сфере медицинского обслуживания при перевозке личных медицинских записей и данных медицинской карты [3, с. 1]. Например, пользователь из страны А, имеющий желание пройти лечение за рубежом в стране В, получает возможность поделиться данными об истории болезней, лечения и профилактических процедур через свой цифровой кошелек. Данные медицинской карты хранятся в двух местах: во-первых, в блокчейн хранилище благодаря эмитенту - учреждению здравоохранения в стране А, который проводил медицинское обследование и лечение пациента; во-вторых, в цифровом кошельке пациента. В учреждении здравоохранения страны В пациент напрямую делится данными своей медицинской карты без опасений их утечки и незаконного использования, так как обе страны внедрили принципы децентрализованной идентичности и находятся в едином пространстве доверия.

Несмотря на очевидные достоинства децентрализованной идентичности на данный момент решения на ее основе находятся на стадии разработки и пилотной апробации. Во многом это связано с необходимостью решения целого списка технических проблем, начиная от разработки технологических основ унифицированного криптографического кода для пользователей всех уровней и тестирования криптографических методов защиты информации, организации системы распределенного хранения информации и создания цепочки блокчейн хранилищ в пространствах доверия и др. На данный момент над решением этих проблем работают целый ряд компаний, включая IBM, tykh, Evernym, Cisco, Royal Credit Union, T-Mobile и многие другие, которые запустили коммерческие и социально-значимые пилотные проекты по реализации принципов децентрализованной идентичности и подтверждения ее преимуществ [4,5].

Уже в среднесрочной перспективе децентрализованная идентичность наряду с созданием пространств доверия сможет повысить удобство трансграничного перемещения и социальную мобильность населения, увеличить информационную эластичность в процессах горизонтального и вертикального взаимодействия, ускорить процессы глобализации за счет удобной и безопасной технологической базы. Так, эксперты аналитической компании Гартнер прогнозируют выход на плато продуктивности и повсеместное распространение технологий децентрализованной идентичности в течение следующих 2-5 лет [6]. Формирующийся в Европейском союзе и развитых странах мира тренд перехода к децентрализованной идентичности необходимо учитывать не только на уровне коммерческих компаний, но также и на уровне органов государственной власти. В том числе при достижении целей Национальной программы «Цифровая экономика Российской Федерации», которая предусматривает защиту прав, свобод и законных интересов личности и бизнеса в условиях цифровой экономики, а также создание эффективных механизмов государственного регулирования и поддержки в области информационной безопасности при интеграции национальной цифровой экономики в международную экономику.

Список литературы

1) Soltani R., Nguyen U. T., An A. A survey of self-sovereign identity ecosystem //Security and Communication Networks. – 2021. – Т. 2021

2) Shashank M. G., Sangeetha V., Shilpa H. An Exploratory Study on Self-Sovereign Identity Powered by the Blockchain Technology. – EasyChair, 2021. – №. 5484.

3) How to Convince Dad* of the Importance of Self-Sovereign Identity [Электронный ресурс]: GitHub – 2018. – Режим доступа: https://github.com/WebOfTrustInfo/rwot7-toronto/blob/master/final-documents/convincing-dad.md (дата обращения 10.01.2022)

Challenges to self-sovereign identity [Электронный ресурс]: Sofware Engineering – 2021. – Режим доступа: https://damienbod.com/2021/10/11/challenges-to-self-sovereign-identity/ (дата обращения 12.01.2022)

4) Sovrin project official website [Электронный ресурс]: Sovrin – 2015. – Режим доступа: https://sovrin.org/stewards/ (дата обращения 12.01.2022)

Gartner Identifies Key Emerging Technologies Spurring Innovation Through Trust, Growth and Change [Электронный ресурс]: аналитическая компания Gartner – 2021. – Режим доступа: https://www.gartner.com/en/newsroom /press-releases/2021-08-23

5) Gilani K. et al. A survey on blockchain-based identity management and decentralized privacy for personal data //2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). – IEEE, 2020. – С. 97-101.

6) Kurbatov O. et al. Global Digital Identity and Public Key Infrastructure //ISCI'2019: Information security in critical infrastructures. – 2019. – С. 237.

7) Olsson O. Challenges with the GDPR: A Software Developing Organization's Guide to GDPR Compliance. – 2019.

8) EIDAS supported self-sovereign identity [Электронный ресурс]: EIDAS – 2015. – Режим доступа: https://ec.europa.eu/futurium/en/system/files/ged/ eidas_supported_ssi_may_2019_0.pdf (дата обращения 15.01.2022)