УДК 342.736

19. ЦИФРОВАЯ ИДЕНТИФИКАЦИЯ И ПРАВОВЫЕ АСПЕКТЫ БЛОКЧЕЙН-ТЕХНОЛОГИЙ ДЛЯ УДОСТОВЕРЕНИЯ ЛИЧНОСТИ

Винник В. С., студент группы 334701, Калацей В.Е., студент группы 334701

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ермакова Е.В. – канд. экон. наук

Аннотация. В статье рассматриваются блокчейн-технологии как основа децентрализованной цифровой идентификации личности. Анализируется переход от централизованных моделей к концепции Self-Sovereign Identity, обеспечивающей пользователю контроль над персональными данными. Исследуются возможности применения таких решений в процедурах KYC и электронном правительстве. Особое внимание уделяется правовым аспектам использования блокчейна, включая защиту персональных данных, электронную подпись, автоматизацию волеизъявления и признание цифровых идентификаторов. Оцениваются международные подходы, в том числе eIDAS 2.0, а также перспективы совершенствования законодательства Республики Беларусь в сфере цифровой идентификации.

Ключевые слова. цифровая идентификация, блокчейн, Self-Sovereign Identity, SSI, персональные данные, электронная подпись, KYC, электронное правительство, eIDAS 2.0, децентрализованные идентификаторы.

В данной работе исследуется концепция децентрализованной цифровой идентификации на базе технологии распределенных реестров (блокчейн). Рассматривается переход от централизованных моделей управления данными к парадигме Self-Sovereign Identity (SSI), обеспечивающей пользователю полный контроль над своими атрибутами личности. Проанализированы правовые вызовы, связанные с применением блокчейна в процедурах KYC и электронного правительства, включая конфликты с законодательством о персональных данных и требованиями к электронной подписи [1]. Особое внимание уделено международному опыту (регламент eIDAS 2.0, инициативы в странах Азии и Ближнего Востока) и перспективам адаптации правового поля Республики Беларусь к новым формам цифрового волеизъявления.

Современная цифровая экономика требует принципиально нового уровня доверия при дистанционном взаимодействии субъектов [2], [3]. Традиционные методы идентификации, опирающиеся на централизованные базы данных государственных реестров или коммерческих провайдеров, всё чаще сталкиваются с проблемами безопасности, фрагментации и отсутствия реального контроля со стороны субъекта данных. Масштабные утечки персональных данных из крупных государственных и корпоративных систем в последние годы демонстрируют уязвимость архитектуры с единой точкой отказа. В условиях стремительной цифровизации общественных отношений актуализируется потребность в создании неизменяемой, защищенной и децентрализованной системы удостоверения личности. Блокчейн-технологии предлагают архитектурное решение, способное трансформировать цифровую идентичность из набора записей в чужих базах данных в автономный актив пользователя [4]. Более того, переход к децентрализованным моделям позволяет перераспределить экономические издержки на верификацию, исключив необходимость многократного прохождения процедур идентификации у каждого нового поставщика услуг.

Под цифровой идентификацией в широком смысле понимается совокупность электронных атрибутов, позволяющих однозначно определить физическое или юридическое лицо в информационном пространстве [5]. Традиционно эта процедура требует участия доверенной третьей стороны, которая верифицирует данные. Однако внедрение технологии распределенных реестров позволяет реализовать принципы децентрализации и неизменности без посредников. В такой системе идентификатор базируется на криптографических методах, где закрытый ключ служит инструментом волеизъявления, а открытый ключ — уникальным адресом в реестре [6]. Это исключает наличие единой точки отказа и делает процесс проверки подлинности прозрачным и защищенным от несанкционированных изменений.

С технической точки зрения инфраструктура децентрализованной идентификации строится на трех взаимосвязанных уровнях. Первый уровень — это реестр (блокчейн или иная распределенная система), выполняющий функцию механизма обнаружения и верификации. Второй уровень — это децентрализованные идентификаторы (DID), которые представляют собой глобально уникальные строки, не требующие централизованного регистратора. DID связываются с DID-документами, содержащими криптографические ключи и конечные точки для аутентификации. Третий уровень — это верифицируемые учетные данные (VC), которые представляют собой криптографически защищенные утверждения эмитента (государства, банка, образовательного учреждения) о субъекте. Такая архитектура позволяет реализовать модель SSI, где человек является единственным владельцем своих данных и самостоятельно решает, какой объем информации раскрывать конкретному контрагенту.

В рамках SSI реализуются принципы автономности (независимость от эмитента после получения данных) и минимизации данных. Важнейшим инструментом здесь выступают доказательства с нулевым

разглашением (Zero-Knowledge Proofs — ZKP), которые позволяют подтвердить определенный факт, например, достижение совершеннолетия или наличие активного банковского счета, не раскрывая при этом саму дату рождения, номер счета или иные избыточные персональные сведения. Это создает принципиально новый уровень конфиденциальности, недостижимый в рамках традиционной модели «запрос-ответ», где верификатор получает избыточную информацию.

Практическое применение блокчейн-идентификации охватывает критически важные секторы экономики. В банковской сфере использование распределенных реестров для процедур «Знай своего клиента» (KYC) позволяет радикально снизить операционные издержки. По оценкам аналитических агентств, совокупные затраты финансовых институтов на соблюдение KYC-требований ежегодно исчисляются миллиардами долларов. Единожды пройдя верификацию у одного доверенного эмитента (например, уполномоченного банка-агрегатора), пользователь получает цифровой токен (VC), который признается другими участниками сети. Это не только сокращает временные издержки для клиента, но и повышает точность данных за счет исключения человеческого фактора при многократном вводе информации.

В сфере электронного правительства блокчейн обеспечивает надежное хранение и мгновенную проверку дипломов, лицензий и актов гражданского состояния. Важно отметить, что технология позволяет перейти от модели «выгрузки данных» к модели «предъявления данных». Государственные органы, выступая в роли эмитентов, могут выпускать верифицируемые учетные данные в цифровой кошелек гражданина. Впоследствии гражданин предъявляет эти данные любой организации (банку, работодателю, нотариусу), которая может проверить их подлинность напрямую через распределенный реестр, не обращаясь к государственному органу. Это создает фундамент для трансграничного взаимодействия, где цифровой кошелек гражданина становится универсальным инструментом доступа к государственным и коммерческим услугам в любой юрисдикции, поддерживающей соответствующие стандарты [7].

Промышленный интернет вещей (IIoT) и логистика также выступают драйверами внедрения децентрализованной идентификации. В цепочках поставок цифровая идентичность позволяет отслеживать не только движение товаров, но и статус допуска персонала к работе с опасными объектами, автоматизируя процессы пропускного режима и соблюдения нормативных требований без участия централизованного оператора.

Развитие технологий опережает формирование нормативной базы, однако на международном уровне уже наметились четкие тренды. Регламент eIDAS 2.0 в Европейском союзе устанавливает стандарты для европейских цифровых кошельков (EU Digital Identity Wallet), закрепляя их юридическую силу наравне с физическими документами [8], [9]. Ключевым отличием eIDAS 2.0 от предыдущих версий является признание концепции «самостоятельного предъявления» атрибутов и обязательство государств-членов предоставить гражданам возможность использования таких кошельков для взаимодействия как с государственным, так и с частным сектором. ЕС легитимизирует использование доказательств с нулевым разглашением и устанавливает требования к взаимной совместимости (interoperability) национальных решений.

За пределами Европы показателен опыт стран Ближнего Востока и Азии. Объединенные Арабские Эмираты реализуют стратегию блокчейн-идентификации на уровне государственных сервисов, используя распределенные реестры для визового контроля и идентификации резидентов. В Сингапуре проект National Digital Identity (NDI) сочетает централизованную регистрацию биометрических данных с децентрализованным управлением ключами для коммерческих транзакций. В странах Латинской Америки (Аргентина, Бразилия) наблюдаются пилотные проекты по созданию суверенных идентификаторов для малообеспеченных слоев населения, не имеющих доступа к традиционным банковским услугам, что демонстрирует социальную функцию технологии.

Основной правовой вызов, единый для всех юрисдикций, заключается в обеспечении соответствия блокчейн-систем требованиям законодательства о защите персональных данных, таких как GDPR. Существует определенный парадокс между свойством неизменяемости блокчейна и «правом на забвение» [10]. Для решения этой коллизии современные архитектуры используют хранение данных «вне сети» (off-chain), фиксируя в самом реестре лишь криптографические доказательства (хэши) или ссылки на зашифрованные хранилища, что позволяет соблюдать правовые нормы без ущерба для целостности системы. Технические стандарты, разрабатываемые W3C (World Wide Web Consortium) для VC и DID, также ориентированы на обеспечение «композитности» данных, позволяя удалять персональные данные из off-chain хранилищ без нарушения структуры распределенного реестра.

В Республике Беларусь правовой фундамент цифровой идентификации составляют Закон «Об электронном документе и электронной цифровой подписи», Закон «О защите персональных данных», а также нормы Гражданского кодекса, регулирующие форму сделок. Текущая модель управления открытыми ключами (ГосСУОК) носит строго централизованный характер, основанный на иерархической инфраструктуре открытых ключей (PKI). Это создает определенные барьеры для интеграции децентрализованных систем [10].

Как отмечается в современных исследованиях, серьезным вызовом остается проблема автоматизации волеизъявления. Существующее законодательство в большинстве случаев требует явного, однозначного подтверждения намерений субъекта (принцип «собственноручности» в широком

смысле). В то время как блокчейн-агенты и смарт-контракты предполагают автономное совершение юридически значимых действий на основе заложенного алгоритма. Возникает вопрос о том, можно ли считать действие, инициированное закрытым ключом, хранящимся в цифровом кошельке, действием самого лица, учитывая отсутствие института «цифрового агента» в гражданском законодательстве.

Кроме того, сохраняются вопросы ответственности за действия программных представителей (смарт-контрактов) и необходимость адаптации норм о локализации данных к условиям глобальных распределенных систем. Законодательство о персональных данных устанавливает жесткие требования к хранению и обработке данных на серверах, находящихся на территории Республики Беларусь. Однако в публичных блокчейн-сетях валидаторы (узлы) могут находиться в разных юрисдикциях, что потенциально вступает в противоречие с принципом территориальности обработки данных. Решением здесь может выступать использование национальных (permissioned) блокчейн-сетей, контролируемых уполномоченными государственными органами, либо гибридных моделей, где в распределенном реестре циркулируют только нечувствительные данные (хэши).

Проведенный анализ позволяет утверждать, что цифровая идентификация на базе блокчейна является неизбежным этапом развития ИКТ-сферы. Критическая оценка текущего регулирования показывает, что жесткая привязка к централизованным удостоверяющим центрам ограничивает масштабируемость цифровых сервисов, особенно в сфере трансграничной торговли и международного сотрудничества. По нашему убеждению, будущее принадлежит гибридным моделям, где государство выступает гарантом первоначальной валидации личности (процесс онбординга), а блокчейн обеспечивает повседневный оборот этих данных в децентрализованной среде.

Правовое регулирование должно сместиться от контроля над хранением информации к установлению четких правил управления доступом и признания цифровых доказательств в судебной практике. Это потребует внесения изменений в гражданское и процессуальное законодательство в части: признания статуса децентрализованных идентификаторов (DID) как законного средства идентификации, равнозначного паспортным данным в рамках определенных правоотношений, легализации доказательств с нулевым разглашением (ZKP) как допустимого вида доказательств по гражданским и административным делам, введения понятия «цифровой кошелек» в правовое поле, определив режим хранения криптографических ключей и ответственность операторов кошельков за их сохранность, адаптации норм о смарт-контрактах, уточнив, что выполнение алгоритмического кода, активированного действиями сторон, порождает правовые последствия, аналогичные традиционному договору.

Особого внимания требует институт «цифрового наследования». В условиях SSI, где закрытый ключ является единственным инструментом доступа к цифровым активам и идентификационным данным, отсутствие механизмов передачи ключей наследникам может привести к утрате юридически значимой информации. Необходимо разработать правовые механизмы, позволяющие депонировать ключи у доверенных третьих лиц или устанавливать «цифровых наследников» в рамках нотариальных действий.

Внедрение блокчейн-технологий для удостоверения личности способно создать безопасную и эффективную среду для цифровой экономики. Такая среда базируется на криптографической защите, отсутствии единой точки отказа и возможности мгновенной верификации данных без участия посредников. Переход к модели суверенной идентичности (SSI) позволит минимизировать риски утечек персональных данных, которые в настоящее время происходят преимущественно из централизованных хранилищ, содержащих миллионы записей. В децентрализованной модели субъект данных хранит свои атрибуты локально в цифровом кошельке, а в распределенном реестре фиксируются лишь криптографические доказательства, что существенно снижает привлекательность таких систем для злоумышленников. Кроме того, SSI способствует снижению транзакционных издержек на верификацию: вместо многократного прохождения процедур KYC или предоставления нотариально заверенных копий документов участники оборота получают возможность однократной верификации у доверенного эмитента с последующим многократным использованием верифицируемых учетных данных. Наконец, данная модель возвращает пользователям реальный контроль над их цифровым следом, позволяя самостоятельно определять, какие именно атрибуты, в каком объеме и на какой срок предоставлять конкретным контрагентам, а также отзывать доступ к данным без необходимости обращаться к администратору базы данных.

Своевременная адаптация законодательства, учитывающая как неизменность распределенного реестра, так и необходимость соблюдения прав субъектов данных (включая право на забвение), позволит Республике Беларусь не только интегрироваться в глобальное цифровое пространство, но и занять лидирующие позиции в области безопасного управления идентификацией в рамках ЕАЭС и Союзного государства. Унификация подходов к децентрализованной идентификации на пространстве Евразийского экономического союза создаст основу для взаимного признания цифровых удостоверений, упростит трансграничную торговлю, миграционные процессы и доступ граждан к медицинским и образовательным услугам на территории стран-участниц. В рамках Союзного государства Беларуси и России гармонизация регулирования в этой сфере позволит сформировать общее цифровое пространство, где децентрализованные идентификаторы будут выполнять функцию единого удостоверения личности, признаваемого всеми государственными органами и хозяйствующими субъектами обеих стран. Реализация таких перспектив требует начала системной работы по приведению национального законодательства в соответствие с технологическими реалиями, включая создание экспериментальных

правовых режимов (регуляторных песочниц) для апробации SSI-решений, а также разработку национальной стратегии перехода к децентрализованной идентификации с четкими этапами, сроками и распределением ответственности между государственными органами.

Список использованных источников:

1. Об электронном документе и электронной цифровой подписи : Закон Респ. Беларусь, 28 дек. 2009 г., № 113-З : в ред. Закона Респ. Беларусь от 17.07.2023 г. [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871. – Дата доступа: 05.03.2026.

2. World Economic Forum. Reimagining Digital Identity: A Strategic Imperative [Electronic resource]. – Mode of access: https://www.weforum.org/reports/reimagining-digital-identity-a-strategic-imperative. – Дата доступа: 05.03.2026.

3. Ермакова, Е.В. Государственное управление инновационной деятельностью // Право. Экономика. Социальное партнерство [Электронный ресурс] : сб. науч. тр. Междунар. ун-т «МИТСО» ; редкол.: В. Ф. Ермолович [и др.]. – Минск : Междунар. ун-т «МИТСО», 2023. – С. 529–532. – Дата доступа: 09.03.2026.

4. Giannopoulou, A. Self-sovereign identity / A. Giannopoulou, F. Wang // Internet Policy Review. – 2021. – Vol. 10, № 2. [Electronic resource]. – Режим доступа: https://policyreview.info/articles/analysis/self-sovereign-identity. – Дата доступа: 08.03.2026.

5. Фещенко, С.Л. Норма идентификации в контексте цифровизации межгосударственных цепей поставок // Наука и инновации. – 2023. – № 3. – С. 59–64. – Дата доступа: 10.03.2026.

6. Mühle, A. A Survey on Self-Sovereign Identity in Communication Networks / A. Mühle, A. Grüner, T. Gayor, C. Meinel // IEEE Communications Surveys & Tutorials. – 2018. – Vol. 20, № 3. – P. 1876-1909 – Дата доступа: 05.03.2026.

7. European Digital Identity Regulation (eIDAS 2.0) [Electronic resource]. – Режим доступа: https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en. – Дата доступа: 05.03.2026.

8. Deloitte. eIDAS 2.0: The digital identity revolution [Electronic resource]. – Режим доступа: https://www2.deloitte.com/lu/en/pages/financial-services/articles/eidas-2-0-digital-identity-revolution.html. – Дата доступа: 05.03.2026.

9. Фещенко, С.Л. Цифровизация межгосударственных цепей поставок: понятие идентификации в нормативных правовых актах государств – членов ЕАЭС (Беларуси, России и Казахстана) / С. Л. Фещенко // Научные труды Белорусского государственного экономического университета. – Минск : Колорград, 2023. – Вып. 16. – С. 469–476. – Дата доступа: 05.03.2026.

10. О персональных данных : Закон Респ. Беларусь, 7 мая 2021 г., № 99-З [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=12551. – Дата доступа: 07.03.2026.

UDC 342.736

DIGITAL IDENTIFICATION AND LEGAL ASPECTS OF BLOCKCHAIN TECHNOLOGIES FOR IDENTITY VERIFICATION

Vinnik V.S., Kalatsei V.E.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Ermakova E.V. – Associate Professor of the Department of Management

Annotation. The article examines blockchain technologies as a foundation for decentralized digital identity. It analyzes the transition from centralized models to the Self-Sovereign Identity concept, which enables users to control their personal data. The paper explores the potential application of such solutions in KYC procedures and e-government. Particular attention is paid to the legal aspects of blockchain use, including personal data protection, electronic signature, automation of expression of will, and recognition of digital identifiers. International approaches, including eIDAS 2.0, as well as the prospects for improving the legislation of the Republic of Belarus in the field of digital identification, are also assessed.

Keywords. digital identification, blockchain, Self-Sovereign Identity, SSI, personal data, electronic signature, KYC, e-government, eIDAS 2.0, decentralized identifiers.