DOI 10.37882/2223–2966.2023.04.40

ЭВОЛЮЦИЯ РАЗВИТИЯ ДЕЦЕНТРАЛИЗОВАННЫХ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Ярыгин Павел Константинович
Аспирант, Национальный исследовательский ядерный университет «МИФИ», г. Москва
yarygin_pavel@mail.ru

Аннотация. Главной целью данной статьи является исследование развития электронных платежных систем, а именно децентрализованных электронных платежных систем. В статье приводится описание принципов работы и схемы расчетов с помощью электронных платежных систем (ЭПС) — централизованной и децентрализованной. Механизмы работы децентрализованных ЭПС рассмотрены на примере самых популярных на данный момент криптовалют — Bitcoin и Ethereum. Также приводится классификация цифровых денег, их разновидности. В конце статьи описаны новые области применения технологий распределенного реестра — использование их в национальных цифровых валютах. Таким образом, можно сказать, что децентрализованные электронные платежные системы — важная технология, которая уже сейчас серьезно изменяет существующий мировой экономический порядок.

Ключевые слова: электронная платежная система, технология распределенного реестра, децентрализованная электронная платежная система, цифровые деньги, национальная цифровая валюта.

EVOLUTION OF THE DEVELOPMENT OF DECENTRALIZED ELECTRONIC PAYMENT SYSTEMS

P. Yarygin

Summary. The main purpose of this article is to study the development of electronic payment systems, namely decentralized electronic payment systems. The article describes the principles of operation and payment schemes using electronic payment systems (EPS) — centralized and decentralized. The mechanisms of operation of decentralized EPS are considered on the example of the most popular cryptocurrencies at the moment — Bitcoin and Ethereum. The classification of digital money and its varieties is also given. At the end of the article, new areas of application of distributed registry technologies are described — their use in national digital currencies. Thus, we can say that decentralized electronic payment systems are an important technology that is already seriously changing the existing world economic order.

Keywords: electronic payment system, distributed registry technology, decentralized electronic payment system, digital money, national digital currency.

Введение

Электронная платежная система (ЭПС) — это система, которая позволяет проводить транзакции и оплачивать товары и услуги через электронный носитель, такой как банковская карта, мобильное приложение или интернет-банкинг, без необходимости использовать бумажные деньги или чеки. За последние годы ЭПС стали очень популярными из-за распространения интернет-банкинга и онлайн-покупок. Развитие технологий привело к улучшению и расширению систем обработки платежей, и по мере роста их надежности количество проверок и операций с наличными деньгами и дальше будет снижаться. С распространением сети Интернет электронная коммерция обрела глобальные масштабы и сейчас уже вся современная экономика неразрывно связана с электронной коммерцией.

Предмет исследования

Схема централизованной ЭПС

Большинство электронных платежных систем являются централизованными. Это значит, что в ней есть центральный расчётный агент — посредник, который

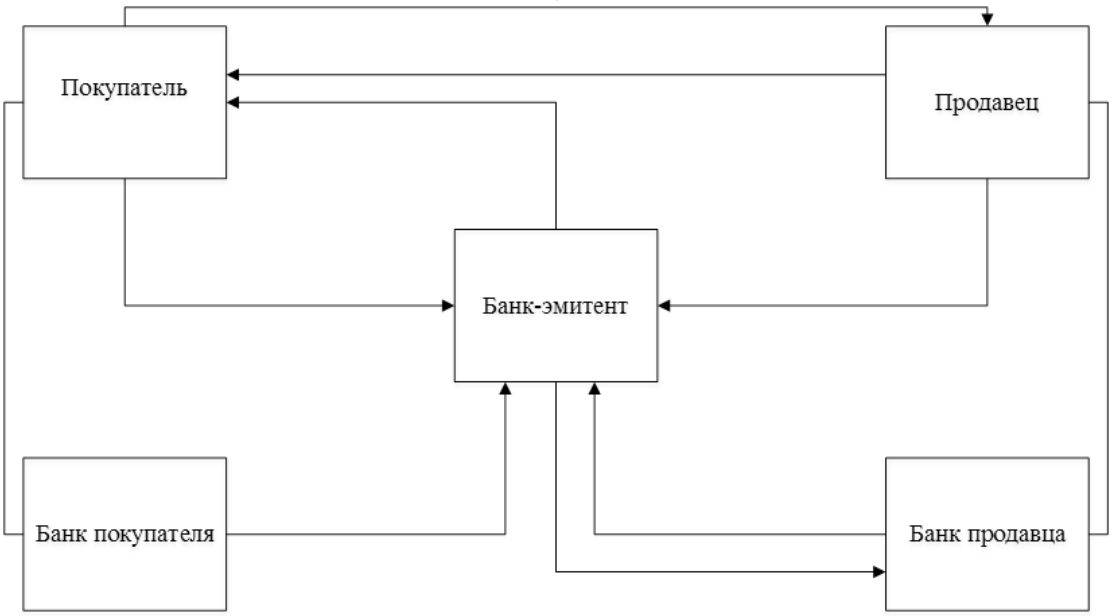

Рис. 1. Схема расчёта цифровыми деньгами

оказывает услуги по проведению расчётов. Примерная схема расчета цифровыми деньгами в централизованной электронной платежной системе представлена на рисунке 1.

Цифровая купюра состоит из номинала, серийного номера и электронной цифровой подписи банка-эмитента [1].

Покупатель (клиент А) формирует заготовку цифровой купюры, где стоит его собственная ЭЦП, и отправляет её в банк-эмитент. Банк, зная открытый ключ клиента А, идентифицирует его, удаляет подпись, ставит свою ЭЦП, вычитает со счёта клиента А нужную сумму и отправляет цифровую купюру. Получив обратно цифровую купюру, покупатель может заплатить за товар продавцу (клиенту В), переслав её, предварительно подписав своей ЭЦП. Клиент В проверяет подпись клиента А, удаляет ее и отправляет в банк-эмитент. Банк-эмитент проверяет, не была ли использована эта купюра, и заносит её в список использованных купюр.

В рассмотренной схеме не обеспечивается анонимность платежей, так как банк знает номера купюр. Поэтому Д. Чаум предложил протокол слепой подписи [1]. В этом случае клиент А скрывает от банка номер купюры при отправлении заготовки. Если в будущем данная купюра будет предъявлена в банк, то банк обязан ее принять, потому что на купюре находится подпись банка. Как и прежде, банк вносит номер этой купюры в список купюр, предъявленных для оплаты, но он не способен определить, кто передал эту купюру. Во время подписания купюры банк не видел ее номер, поэтому не может привязать купюру к конкретному клиенту.

Технология распределенного реестра

Технология распределенного реестра (Distributed Ledger Technology, DLT) представляет собой новый подход к созданию баз данных, главной особенностью которого является отсутствие единого центра управления — запись и хранение данных о транзакциях происходят не на одном централизованном сервере, а на нескольких узлах сети независимо друг от друга. Каждый узел в сети имеет копию главного реестра, а новые транзакции проверяются и записываются консенсусом узлов [2]. Это создает безопасную и прозрачную запись всех транзакций в сети.

Блокчейн — является одной из разновидностей DLT, которая использует серию блоков для хранения данных безопасным и децентрализованным способом. Блоки соединены друг с другом в цепочку, и данные, хранящиеся в каждом блоке, помечены временем и проверены сетью компьютеров, составляющих блокчейн. Другие похожие DLT-решения используют не блочную структуру, а, например, ациклические графы или хешграфы.

Блокчейн — это технология децентрализованного хранения и распределенного внесения записей о транзакциях без необходимости в каком-то центральном органе (посреднике). Блокчейн основан на криптографических методах защиты информации — каждый блок цепочки содержит криптографический хэш, ко-

торый связывает его с предыдущим блоком в цепочке, создавая неизменяемую запись всех транзакций. Данные хранятся в компьютерной сети, и ни одна организация не имеет над ними контроля, что делает их устойчивыми к подделке и обеспечивает целостность каждой из цепочек блоков, содержащих данные о транзакциях.

Сеть работает с помощью механизмов консенсуса, которые гарантируют, что все участники согласны с действительностью транзакций, и могут включать подтверждение работы, подтверждение доли и другие механизмы [3].

Одной из ключевых особенностей блокчейна является его неизменяемость — как только блок был добавлен в цепочку, он не может быть изменен или удален. Это делает его высокозащищенной и прозрачной системой для хранения и проверки данных.

Технология блокчейн была впервые разработана в 2008 году как технология, лежащая в основе цифровой криптовалюты Биткоин (об этом далее будет подробно описано), однако с тех пор технология была адаптирована для использования в широком спектре приложений, выходящих далеко за рамки только криптовалют, включая управление цепочками поставок, системы голосования, ведение реестров жилищного имущества и так далее.

Вообще термин «Crypto Currensy», в переводе с английского означающий «криптовалюта», появился в журнале «Форбс» в 2011 году, и с тех пор название прочно вошло в обиход [4]. Единицей измерения в этой системе считаются «коины» (буквально — «монеты»). Криптовалюта не имеет никакого реального выражения в виде номинальных металлических монет или бумажных банкнот. Эти финансовые активы существуют исключительно в цифровом виде, поэтому рассматривать их лишь в качестве общепринятого средства оплаты некорректно. В первую очередь они — продукт развития информационной цифровой среды, регулирование оборота которого невозможно.

Децентрализованные ЭПС

Почти все электронные платежи в интернете осуществляются через финансовые организации, которые являются надежным третьим лицом в процессе транзакций. В большинстве случаев система работает хорошо, но тем не менее она основана на доверии, что является существенным недостатком. В связи с использованием посредников в финансовых транзакциях возникают проблемы с возвратом средств, а также увеличиваются расходы на транзакции. Это делает невозможным проведение полностью невозвратных платежей и нецелесообразным проведение малых повседневных платежей. Кроме того, сервисам, которые предоставляют невозвратные услуги, необходимо использовать доверенных посредников, что увеличивает стоимость транзакций. Продавцы вынуждены быть предельно осторожными в отношении своих покупателей и запрашивать дополнительную информацию, что увеличивает затраты и вызывает сомнения. Эти затраты и проблемы можно избежать, используя обычные деньги, но в интернете отсутствует механизм безопасных платежей без доверенного посредника.

Bitcoin

Децентрализованные электронные платежные системы появились совсем недавно. Наибольшую популярность они обрели после выхода в свет статьи с описанием протокола Bitcoin, опубликованной в 2008 году Сатоши Накамото [5]. Сатоши Накамото объединил идеи нескольких предыдущих изобретений и создал систему электронных денег, которая полностью децентрализована. Одним из ключевых новшеств является алгоритм консенсуса Proof-of-Work, который позволяет добавлять новые блоки в блокчейн, подтверждать транзакции и верифицировать единую версию реестра во всех копиях, которые хранятся на отдельных узлах (нодах). Это стало возможно благодаря соединению нескольких технологий и идей.

Сеть Bitcoin была запущена в январе 2009 года на основе реализации, опубликованной Накамото, и с тех пор была улучшена сообществом. Сатоши Накамото покинул сообщество в апреле 2011 года, оставив ответственность за разработку кода на группу добровольцев. «Сатоши Накамото» — это псевдоним, а личность изобретателя или группы изобретателей Bitcoin до сих пор остается неизвестной. Но несмотря на это система Bitcoin полностью децентрализована и никому не подконтрольна. Это изобретение представляет собой новаторский подход и уже привело к развитию новой науки в области распределенных вычислений, экономики и эконометрики.

Главной целью создания Bitcoin было достижение свободы от контроля посредниками. Одними из главных проблем в стандартной централизованной модели являются отсутствие анонимности, полная зависимость от доверенного сервера и монополизация рынка. Bitcoin же является децентрализованной системой.

Количество биткоинов ограничено 21 миллионом, их не может быть больше (рис. 2) [6]. Никакое государство не может напечатать или обесценить биткоины, так как в соответствии с концепцией, биткоины принадлежат только пользователю, должны быть защищены

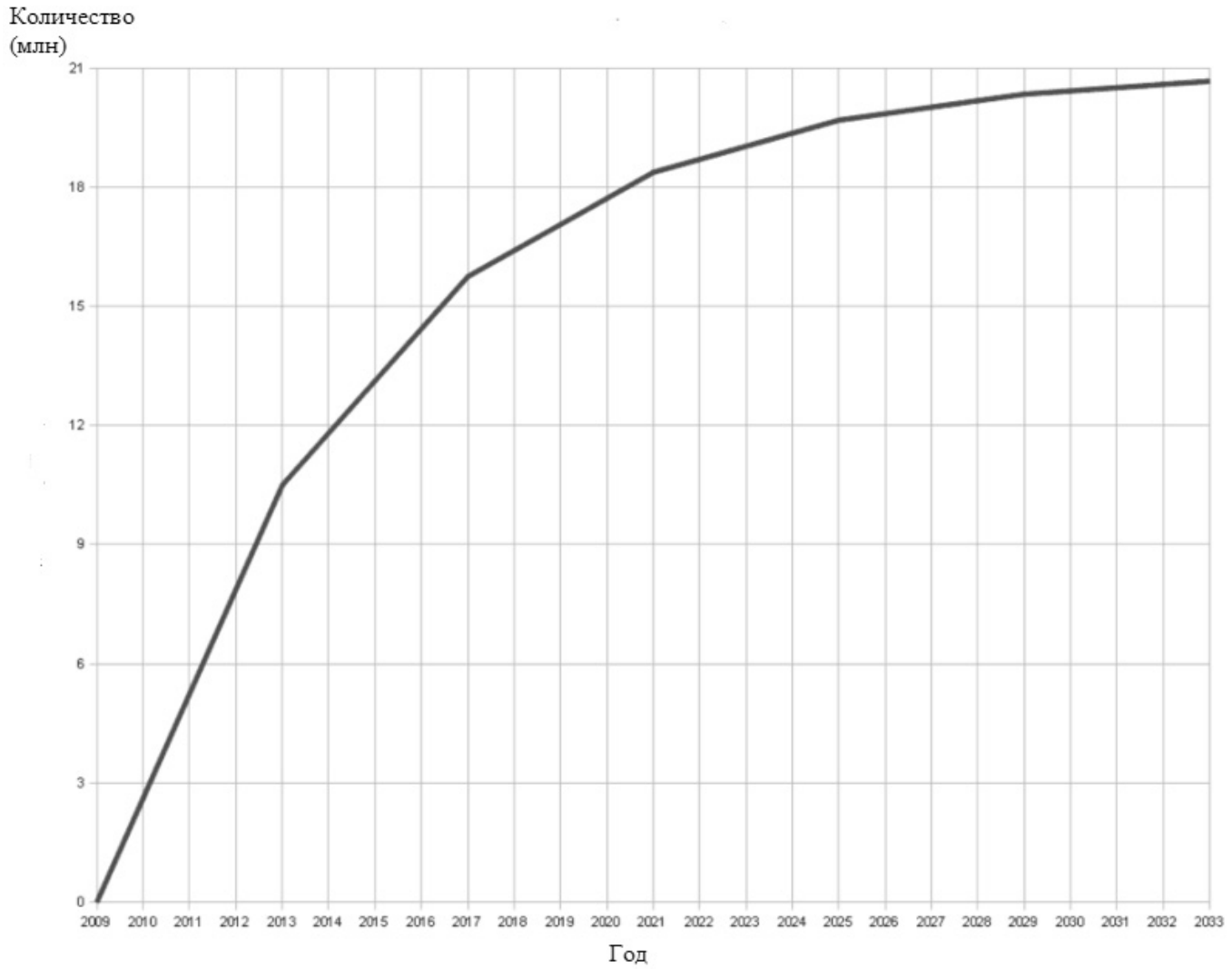

Рис. 2. График зависимости количества биткоинов от года

от подделки и могут использоваться для мгновенных платежей с любым человеком в любом месте, где есть доступ к сети. Ограниченность выпуска защищает валюту от инфляции.

Одно из главных свойств Bitcoin — это полная прозрачность, что означает, что все пользователи сети могут видеть всю цепочку блоков. Bitcoin — это виртуальная валюта, которую невозможно напечатать, она эмитируется путем процесса создания новых блоков, известного как майнинг, который выполняется с помощью специального программного обеспечения, основанного на инновационной технологии блокчейн. Блокчейн является основой этого уникального финансового феномена, который обеспечивает финансовую мощь криптовалюты. Глобальная сеть Bitcoin имеет уникальную структуру и механизм работы, и любой желающий может стать ее пользователем. За годы существования Bitcoin образовалось сообщество, и криптовалютой можно зарабатывать, покупать товары и услуги, обменивать ее на другие валюты и торговать на криптовалютных биржах. Принцип добычи новых средств заключается в решении математических задач, и успешный майнер получает вознаграждение в Bitcoin. Однако с течением времени задачи становятся сложнее, требуется больше энергии и вычислительных мощностей, а размер вознаграждения уменьшается каждые 4 года. Поэтому люди объединяются в майнинг-пулы для увеличения дохода путем совместной работы. Полученное вознаграждение в Bitcoin делится между участниками в соответствии с их вкладами и затратами.

Ethereum

Ethereum — другая криптовалюта, построенная на блокчейне. По состоянию на апрель 2022 года явля-

ется второй по объему капитализации. Ethereum создана в 2015 году В. Бутериным и Г. Вудом [7]. Ethereum отличается от других криптовалют тем, что его создатели не ограничивают его функцию только как средство платежей. Вместо этого они предлагают его использовать как платформу для создания децентрализованных онлайн-сервисов. Например, его можно использовать для обмена ресурсами или регистрации сделок с активами при помощи смарт-контрактов.

Разработчики Ethereum следовали следующим принципам:

- простота: протокол Ethereum должен быть как можно более простым, даже ценой некоторого хранения данных или неэффективности по времени. Любая оптимизация, которая добавляет сложности, не должна включаться, если эта оптимизация не дает существенной выгоды;
- универсальность: фундаментальная часть философии дизайна Ethereum заключается в том, что Ethereum имеет внутренний язык сценариев, который программист может использовать для построения любого смарт-контракта или типа транзакции, которые могут быть математически определены;
- модульность: части протокола Ethereum должны быть сконструированы таким образом, чтобы они были максимально модульными и разделяемыми;
- гибкость: детали протокола Ethereum четко не установлены и могут меняться при надобности.

Анализ новых областей применения

Цифровые деньги

Цифровыми деньгами принято называть валюты, которые существует полностью в цифровой форме, без физического аналога, такого как наличные деньги. Операции с этими валютами обычно осуществляются онлайн или в электронном виде. Обычно в них применяются криптографические методы для обеспечения безопасности и проверки транзакций. Криптовалюты, такие как Bitcoin, Ethereum и Litecoin, представляют собой тип цифровой валюты, которая работает независимо от центрального банка и может использоваться для совершения покупок и отправки этих денег без необходимости в традиционном посреднике. Это децентрализованные криптовалюты.

В дополнение к криптовалютам существуют также централизованные цифровые валюты, такие как цифровой юань или цифровой евро, которые выпускаются и поддерживаются национальными правительствами. Эти валюты предназначены для использования их в качестве альтернативы наличным деньгам и традиционным банковским счетам, и они могут подвергаться большему регулированию и надзору, чем децентрализованные криптовалюты.

Говоря про цифровые деньги, стоит перейти к рассмотрению понятия «цифровые финансовые активы» (ЦФА). Под ними следует понимать электронное финансовое средство, которым закрепляется совокупность имущественных и неимущественных прав, подлежащих, по аналогии с ценными бумагами, удостоверению, уступке и безусловному осуществлению: цифровые субъективные права (в т.ч. денежные требования); права на доход по эмиссионным ценным бумагам; права участия в капитале непубличного акционерного общества; право требовать предоставления эмиссионных ценных бумаг, предусмотренных решением о выпуске цифровых финансовых активов [8].

Ряд ученых полагает, что ЦФА являются любые активы, представленные в цифровой форме, которые обладают номиналом, эквивалентным конкретному стоимостному выражению, независимо от способа их выражения и наличия у держателя права собственности [9]. В контексте рассматриваемой интерпретации цифровые финансовые активы включают:

1. информационные активы:
   - структурированные цифровые данные (например, базы данных, отчетность юридического лица);
   - цифровой продукт, фактор стоимости которого обусловлен использованием специальных знаний (например, анализ сведений о финансовой отчетности);
2. инкапсулированные в цифровом формате инфраструктуры, расположенные в сетевом хранилище, наличием которых пользователю (субъекту цифрового права) предоставляется право получать некий информационный продукт (например, ведение учета, составление отчетности, анализ и т.д.) удаленно;
3. цифровые финансовые активы (в т.ч. криптовалюта, токены), которыми устанавливаются имущественные права собственников на виртуальные (информационные, цифровые) или реальные ценности (электронные деньги: фиатные и нефиатные);
4. цифровые нефинансовые активы (в т.ч. виртуальное цифровое имущество, права доступа к электронным платформам, сервисам и пр.).

Криптовалюта, как и наличные деньги, является объектом для совершения платежей, и ее подлинность

может быть проверена без необходимости передачи дополнительной информации. В отличие от этого, электронные платежные системы, такие как Alipay и WeChat Pay, работают путем передачи прав на активы, хранящиеся где-то еще. Хотя это делает процесс платежа более удобным, но также требует развитой инфраструктуры.

В зависимости от эмитента деньги можно разбить на банковские (b-money), электронные (e-money), инвестиционные (i-money), деньги центрального банка (наличные и цифровые — Central Bank Digital Currency, CBDC) и криптовалюту.

Все виды денег могут быть технологически централизованными (где все транзакции обрабатываются на едином сервере) или же децентрализованными, где технология распределенного реестра (Distributed Ledger Technology, DLT) используется для обработки транзакций через несколько серверов. Эти серверы могут быть ограничены приватными сетями (permissioned network) или же доступны публично (permissionless network), как, например, в Bitcoin.

Платежи могут осуществляться через посредников и гарантироваться государством в случае банковских инструментов, либо через частные структуры в большинстве других случаев.

Еще один критерием классификации является стоимость, которая может быть фиксированной или изменяемой. Если стоимость фиксированная, то это означает, что цена транзакции задана заранее и не изменится. Например, если требуется внести в банк вклад на 10 евро, то можно обменять его на банкноту в 10 евро. Такой подход хорошо подходит для электронных средств платежа и стейблкоинов, обеспеченных фиатными деньгами, таких как Paxos (PAX), USD Coin (USDC) и TrueUSD (TUSD), которые гарантируют эквивалентность своей валюты с долларами в пропорции 1 к 1 [10]. Другие цифровые деньги имеют изменяемую стоимость. Например, стейблкоины, которые обеспечены золотом, нефтью или другими сырьевыми активами, переоцениваются вместе с соответствующими рынками, поэтому они не могут быть отнесены к электронным деньгам, а относятся к инвестиционным деньгам.

Национальные цифровые валюты

Национальные цифровые валюты — это цифровые версии фиатной валюты страны, которые выпускаются и поддерживаются центральным банком или денежно-кредитным управлением. Они предназначены для использования в повседневных транзакциях, точно так же, как физические наличные или цифровые платежи. Цифровая валюта не заменяет существующих наличных или безналичных денег, а появляется в дополнение к ним. Они могут храниться в цифровых кошельках, как и традиционные валюты, и могут быть доступны через мобильные или настольные устройства. Транзакции записываются в защищенный реестр, который поддерживает центральным банком, и могут быть совершены мгновенно, без необходимости в посредниках, таких как коммерческие банки.

Главными целями национальных цифровых валют является расширение доступа к финансовым услугам, повышение эффективности и скорости транзакций, а также снижение затрат, связанных с использованием наличных денег и традиционных платежных систем. Одним из ключевых различий между цифровыми и традиционными валютами является уровень контроля и конфиденциальности, который предполагается при их внедрении.

Несмотря на то, что в основе национальных цифровых валют используется технология блокчейн, это не означает, что они являются криптовалютами: криптовалюты, как правило, децентрализованы, они работают в распределенной сети без центрального органа власти, в то время как национальные цифровые валюты создаются и выпускаются центральным банком или правительством, которые контролируют предложение цифровой валюты и могут регулировать его по своему усмотрению. Национальные цифровые валюты поддерживаются фиатной валютой правительства, в то время как криптовалюты могут быть обеспечены другими активами или вообще не иметь поддержки. Кроме того, национальные цифровые валюты могут подвергаться более строгому регулированию и надзору со стороны правительства или центрального банка. Внедрение цифровых национальных валют — относительно новое явление, но многие страны уже предприняли шаги в развитии этого направления. Среди таких стран Китай, Швеция, Багамские острова, Тунис, Эквадор, Камбоджа, Иран и т.д. Россия также заинтересована в создании цифрового рубля, который в настоящее время разрабатывается в нашей стране.

Заключение

Национальные цифровые валюты рассматриваются как способ модернизации и совершенствования существующей финансовой системы, делая ее более доступной, эффективной и безопасной. Внедрение национальных цифровых валют — сложный процесс, который требует тщательного рассмотрения потенциальных выгод и проблем, а также участия множества заинтересованных сторон, включая центральные банки, регулирующие органы и частный сектор.

ЛИТЕРАТУРА

1. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / Под ред. М.А. Иванова. — М.: НИЯУ МИФИ, 2012. — 400 с.
2. Что такое технология распределенного реестра [Электронный ресурс] // Портал BeInCrypto. URL: https://ru.beincrypto.com/learn/chto-takoe-tehnologiya-raspredelennogo-reestra/. — (Дата обращения: 02.02.2023);
3. Аннагурбанова С., Абдурасулов А., Ахмедова М. Консенсус механизма блокчейн — Вестник науки. 2023. — № 2 (59).
4. Старков Р.Ф., Шехтер К.В. Криптовалюта — Молодежный вестник ИРГТУ. 2018. № 3. — С. 131–134.
5. Bitcoin: A Peer-to-Peer Electronic Cash System [Электронный ресурс]. URL: https://bitcoin.org/bitcoin.pdf — (Дата обращения: 05.02.2023).
6. Почему количество биткоинов ограничено 21 миллионом [Электронный ресурс] — Портал Crypto.ru. URL: https://crypto.ru/pochemu-kolichestvo-bitcoin-ogranicheno/. — (Дата обращения: 05.02.2023).
7. Ethereum: a secure decentralised generalised transaction ledger Eip-150 revision [Электронный ресурс]. URL: http://gavwood.com/Paper.pdf. — (Дата обращения: 06.02.2023).
8. Токолов А.В. Правовое регулирование информационных отношений в сфере оборота цифровых финансовых активов: дис. … канд. юр. наук 12.00.13 — Москва. 2022. — 215 с.
9. Остроушко А.В., Тимофеева И.Н. О необходимости совершенствования системы правового регулирования цифровых активов в Российской Федерации — Юридические исследования. 2021. № 4. — С. 59–76.
10. Цифровые деньги и какими они бывают [Электронный ресурс]. URL: https://econs.online/articles/techno/tsifrovye-dengi-i-kakimi-oni-byvayut/. — (Дата обращения: 11.02.2023).

Журнал «Современная наука: актуальные проблемы теории и практики»

МИФИ