

Интернет изнутри



ЦИФРОВЫЕ ВАЛЮТЫ

**Цифровые валюты в России:
что нам принёс 2024 год**

Обсуждаем феномен цифровых валют, подходы к регулированию и необходимые шаги по развитию законодательства

с. 2

Интернет в цифрах

Эволюция криптоэкономики в России и в мире

с. 6

Сергей Безделов:
«Майнинг - это ещё и социальная ответственность»

Говорим о том, что такое промышленный майнинг, как развивается майнинг в России и какие у него перспективы

с. 8

Кибербезопасность цифровых валют центральных банков

Новый тип денег, представляющий собой цифровой код, очаровывает и пугает одновременно

с. 28

«Византийский» web, или Назад в будущее?

У децентрализации, как и у любой новаторской концепции, есть поклонники и противники

с. 42

Формирование международной платёжной инфраструктуры

Возможно ли в современных условиях реализовать «доверительную среду» между участниками международных расчётов на основе блокчейна?

с. 52

Покровители Интернета – кто они?

Как к Интернету относятся в разных религиях

с. 64

Содержание:

Передовица с. 2	Цифровые валюты в России: что нам принес 2024 год
Интернет в цифрах с. 6	Инфографика
Как это работает с. 8	Сергей Безделов: «Майнинг - это еще и социальная ответственность»
с. 12	Цифровые валюты как важный элемент современной финансовой системы
с. 18	Децентрализованные платёжные системы: типы и примеры применения на основе Bitcoin, Ethereum и Stablecoin
Технология в деталях с. 24	Финансовые технологии, основанные на распределенных системах
Безопасность с. 28	К вопросу о кибербезопасности цифровых валют центральных банков
Наука и образование с. 34	Повторение – мать учения
с. 42	«Византийский» web, или Назад в будущее?
Технология и право с. 46	Юрисдикционный формат регулирования цифровых валют в параметрах определения порядка их использования
с. 52	Формирование альтернативной международной платёжной инфраструктуры
с. 58	Токенизированный рубль. Важность национальной валюты
Технология и искусство с. 60	Поэзия Серебряного века в образах, созданных искусственным интеллектом
Вокруг технологии с. 64	Интернет. В начале было сообщение...
с. 68	Праздники и памятные даты, объединённые Интернетом
Новости науки и техники с. 71	

Сетевое издание
Журнал «Интернет изнутри»
info@internetinside.ru

Выпуск №21, дата выхода:
Ноябрь 2024 г.

Свидетельство о регистрации
СМИ в Федеральной службе
по надзору в сфере
связи, информационных
технологий и массовых
коммуникаций. Регистрационный
номер:
ЭЛ № ФС 77 — 85232 от 25.04.2023
ISSN: 2949-1967

Все статьи размещаются
и индексируются в НЭБ «e-Library»

Издатель: **Фонд развития
сетевых технологий «ИнДата»**

Главный редактор:
Алексей Платонов

Выпускающий редактор:
Ирина Пыжова

Редакционная коллегия:
Елена Воронина
Марат Биктимиров

Продакшн:
Алексей Гончаров

Дизайн и вёрстка:
Антон Иванов

Корректор:
Наталья Рябова

Обложка разработана
с использованием ресурсов сайта
Freepik.com

Об эволюции денег и не только...

Дорогой читатель,

С давних времён монополия на чеканку монет принадлежала государству. Денежная эмиссия и поныне является одним из признаков суверенитета. Однако появление криптовалюты явилось вызовом традиционным денежным системам, и на повестке дня появилось множество новых вопросов. Может ли децентрализованная система платежей – например, биткоин – быть интегрирована в традиционные системы, управляемые центральным банком? Как осуществлять контроль над транзакциями? Как предотвратить использование этих систем в преступных целях? Но также – как использовать бесспорные преимущества цифровой валюты?

Нужно заметить, что экосистема цифровых валют весьма разнообразна. От цифровых валют центральных банков, которые, по сути, являются цифровым отражением традиционных фиатных денег, до стейблкоинов с привязкой к курсу обычной валюты и криптовалют типа биткоин, курс которого определяется множеством факторов и зачастую непредсказуем.

Обо всём этом и пойдет речь в этом номере.

Открывает журнал статья Виктора Достова «Цифровые валюты в России: что нам принёс 2024 год». Основная тема статьи, впрочем, как и нескольких других статей, – цифровая валюта, децентрализованные финансы, майнинг, но особый упор сделан на обсуждении подходов к регулированию и развитию законодательства в этой области.

Различные аспекты цифровых валют – от децентрализованных платёжных систем до цифровых валют центральных банков и вопросов кибербезопасности – подробно рассматриваются и другими авторами номера. Редакция журнала также встретила с директором Ассоциации промышленного майнинга Сергеем Безделовым и расспросила его о текущем состоянии и перспективах промышленного майнинга в России.

Ну и, конечно, мы продолжаем поддерживать наши традиционные разделы. В разделе «Технология и право» Мадина Касенова подробно рассматривает вопросы регулирования различных категорий цифровых валют в России и мире. А в «Новостях» мы познакомим вас с интересными событиями, связанными с Интернетом и доменной индустрией.

В разделе «Наука и образование» Павел Храмцов знакомит нас с интересными исследовательскими работами в области DNS-резолверов и так называемых краулеров, представленными на конференции TLDCON 2024. А название ещё одного раздела – «Технологии и искусство» – вас точно должно заинтриговать.

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках? Пишите нам по адресу info@internetinside.ru.

Редакция журнала



Цифровые валюты в России: что нам принёс 2024 год



Виктор Достов



Аннотация

Цифровые валюты – одна из наиболее технологически сложных и быстро развивающихся компонент финансового сектора. Россия давно входит в число технологических лидеров данного направления и занимает одно из первых мест в мире по числу пользователей, но при этом отстаёт в части законодательного регулирования. Эту ситуацию были призваны исправить законодательные новации 2024 года. Они в значительной мере ввели в правовое поле феномены криптовалют, DeFi, майнинга, однако многие из этих мер, по мнению отрасли, выглядят половинчато. В статье мы обсуждаем феномен цифровых валют, подходы к регулированию и необходимые шаги по развитию законодательства.

Ключевые слова:

цифровые валюты, распределённые реестры, DeFi, блокчейн, цифровой рубль, регулирование

Начать разговор о цифровых валютах в России стоит с общего взгляда на это явление. Формального определения для цифровых валют пока не существует, и ситуация постоянно усложняется. Ещё 10 лет назад финансовая система делилась на привычные категории: традиционный банкинг, безналичные деньги, электронные платежи. В этой системе отдельно существовал биткоин, который считался криптовалютой.

Сегодня мир цифровых валют стал намного сложнее. Во-первых, после появления биткоина возникло множество новых криптовалют и финансовых инструментов, таких как смарт-контракты – короткие программы, позволяющие осуществлять различные операции с цифровыми активами, которые хранятся в системе. Комбинация распределённых платёжных инструментов и смарт-контрактов получила название децентрализованных финансов (DeFi, от decentralized finance) и невероятно активно развивается во всём мире. Эта технология открывает беспрецедентные возможности для умных платежей и инвестиций, позволяя создавать изощрённые инструменты для управления финансами, удивительно гибкие, функциональные и устойчивые. Параллельно с частными DeFi на рынок вышли децентрализованные государственные продукты, такие как цифровые валюты центральных банков (ЦВЦБ, CBDC) и цифровые финансовые активы (ЦФА). Эти продукты активно используют технологии

и идеологию DeFi, совмещая их с жёстким государственным регулированием. Например ЦФА, описанные в 259-ФЗ [1], представляют собой, по сути, систему размещения и оборота аналогов ценных бумаг, которые в DeFi происходят неконтролируемо (в виде ICO, депозитных токенов и так далее), а в случае ЦФА полностью находятся под государственным контролем и лицензированием. Цифровые валюты центральных банков (ЦВЦБ), рассмотренные ниже, являются, по сути, эмитируемым государством аналогом гарантированных стейблкоинов DeFi. Государственные распределённые проекты получили массовое распространение (хотя и находятся, в большинстве своем, на ранних стадиях). По состоянию на 2024 год более 100 проектов цифровых валют центральных банков находятся в стадии разработки по всему миру. Примером ЦВЦБ является цифровой рубль, широкое внедрение которого начнется в 2025 году.

Кроме того, децентрализованные финансы стали активно взаимодействовать с традиционными деньгами. Развиваются гибридные продукты, которые существуют на стыке государственных (фиатных) денег и мира распределённых технологий. Большинство из них стали как формально, так и неформально относить к цифровым валютам, хотя раньше этот термин использовался для описания других финансовых явлений, например, виртуальных денег.

Ярким примером гибридных продуктов являются упомянутые выше стейблкоины — токены, живущие в распределённом реестре, но привязанные к фиатным валютам (например, один токен равен одному рублю или доллару). Также существуют токенизированные банковские безналичные деньги, которые, с одной стороны, хранятся на счетах в банках, а с другой — могут перемещаться в виде токенов по распределённым реестрам. Появление новых сложных категорий цифровых финансовых активов, таких как токенизированные акции, создало мост между рынком ценных бумаг и распределёнными финансами.

В России к виртуальным валютам принято формально относиться криптовалюты — негосударственные платёжные инструменты, работающие на основе технологии распределённых реестров (блокчейна). Криптовалюты можно разделить на традиционные и гибридные. Одна из самых известных традиционных криптовалют — биткоин, для которого характерен плавающий курс и постоянная денежная эмиссия, правила которой определяются встроенным алгоритмом.

Общая капитализация рынка виртуальных валют постоянно растёт — на 2024 год она превысила 2,5 триллиона долларов, что заметно больше суммарного объёма денег в российском рубле и приближается к показателям английского фунта.

Россия является активным участником рынка цифровых валют. Оборот криптовалюты в России занимает значительную долю в мировом объёме: в 2023 он был равен приблизительно 214 миллиардам долларов, что составляет около 9% от мирового оборота. Общий объём зарезервированных активов (TLV) в децентрализованных финансовых протоколах (DeFi) в России превысил 4 миллиарда долларов, что свидетельствует о растущей заинтересованности в этой технологии. Российские компании активно разрабатывают решения на основе распределённых технологий, выходя на международные рынки. Сообщество TON Foundation, созданное на базе блокчейна Telegram, привлекло более 1 миллиарда долларов инвестиций и миллионы пользователей. Однако в области регулирования цифровых валют Россия значительно отстаёт не только от развитых стран, но и от большинства стран бывшего СССР, например, Казахстана и Киргизии.

Отчасти у этого есть объективная причина. Регулирование цифровых валют — это сложная задача, связанная с особенностями виртуальных активов. Государственные финансовые институты привыкли контролировать эмиссию ценных бумаг через регулирование фондового рынка, а эмиссию денег — через центральные банки, которые регулируют выпуск наличных и безналичных средств. Однако в мире цифровых валют эмиссия определяется жёсткими алгоритмами, и этот процесс не подчиняется традиционным методам регулирования.

В классической модели регулирования всегда есть финансовые институты — банки, платёжные системы, микрофинансовые организации. Государственные органы могут устанавливать для них правила и, при необходимости, закрывать их, лишая лицензии. Однако в системе цифровых валют такой вертикали нет: это децентрализованные структуры, в которых информация хранится на компьютерах пользователей, и никто не может просто так «прийти и закрыть» оператора.

Ещё одной важной особенностью является анонимность пользователей. В традиционной банковской системе клиент обязан предъявить документы для открытия счёта. В мире цифровых валют открыть кошелек может любой человек без необходимости предоставлять какие-либо данные о себе.

Поначалу государства пытались полностью запретить криптовалюты. Однако вскоре стало ясно, что запреты неэффективны и приводят к тому, что страна начинает отставать от мирового финансового рынка. Кроме того, технологии контроля за цифровыми валютами начали развиваться, что позволило создать более эффективные концепции регулирования.

В результате, на сегодня в большинстве стран криптовалюты имеют определённый законный статус. В Европе или Центральной Азии криптовалюты регулируются, а их использование допускается для определённых операций. В России же долгое время единственным законом, регулирующим обращение цифровых валют, был федеральный закон № 259 [1], который содержит, в основном, запреты на использование. Например, он запрещает использовать криптовалюту для оплаты товаров и услуг. Но это лишь малая часть необходимого регулирования всей экосистемы цифровых финансовых активов.

На практике 259-ФЗ оставлял открытыми много вопросов. Было, например, неясно, могут ли банки обслуживать криптовалютные компании, могут ли юридические лица держать криптовалюты на балансе и как это показывать в бухгалтерии. Формально исходный закон это не запрещает, но остаются подзаконные акты и рекомендации, которые сводят такую возможность к нулю. Однако есть и позитивные моменты: судебная практика постепенно формируется, и уже понятно, как передавать криптовалюты по наследству или включать их в конкурсную массу.

Таким образом, цифровые валюты — это новый и сложный феномен, который быстро развивается и требует особого подхода со стороны государств, включая Россию. Важно, чтобы регуляторы учитывали специфику этих активов и развивали гибкие методы контроля, такой подход позволит не отставать от мировых тенденций и поддерживать конкурентоспособность страны на международном финансовом рынке.

В 2024 году Россия приняла несколько важных поправок и законов, которые кардинально изменили подход к регулированию криптовалют и майнинга на территории страны. Эти законодательные инициативы направлены на упорядочение использования цифровых валют и технологий блокчейна, а также на контроль и поддержку индустрии майнинга, которая на момент принятия законов играла значительную роль в экономике страны, особенно в некоторых регионах.

Существенные поправки [2-3] в 259-ФЗ и другие законы были приняты в январе 2024 года и включали несколько ключевых уточнений. Одним из значимых нововведений стало упрощение декларирования цифровых валют для физических и юридических лиц. Ранее существовали сложности в отчётности по криптовалютам, что вызывало у бизнеса и граждан трудности в налоговой сфере. Закон упростил процесс, позволив пользователям декларировать свои цифровые

активы через специальный электронный сервис, интегрированный с Федеральной налоговой службой (ФНС). При этом владельцы криптовалют получили возможность вносить данные о своих активах без предоставления большого количества документов. Также произошла частичная легализация платежей в виртуальных валютах.

Кроме того, закон разрешил использование криптовалют при оплате в некоторых секторах экономики, правда, с жёсткими ограничениями. В частности, использование криптовалют было разрешено для международных сделок, что открывает новые возможности для российских компаний, занимающихся экспортом и импортом. Однако внутри страны использование криптовалют для расчётов ограничено определенными высокотехнологичными категориями бизнеса. Сама форма закона – экспериментальный правовой режим (ЭПР) – предполагает закрытый круг участников, утверждаемый государственными органами, и не создает свободной конкуренции на рынке.

Закон 2024 года также ввёл обязательную идентификацию пользователей при работе с цифровыми валютами для институциональных операторов. Это требование распространяется на все криптобиржи и другие платформы, предоставляющие услуги по купле-продаже криптовалют. Платформы обязаны идентифицировать своих клиентов по оговорённым процедурам идентификации, что аналогично банковским процессам. Это нововведение должно помочь бороться с отмыванием денег и финансированием терроризма, а также облегчить налоговое администрирование в сфере криптовалют.

Важным событием стала легализация майнинга. Майнинг называется деятельность участников распределённого реестра по его поддержке и обслуживанию и получение вознаграждения за эту деятельность. Это крайне энергозатратный вид бизнеса – примерно половина нынешней стоимости биткойна определена ценой электричества, которое тратят майнеры на включение его в распределённый реестр. Поэтому майнинг – это важная индустрия для России, особенно для регионов с избыточной энергетической мощностью. В 2023 году Россия занимала третье место по мощности майнинговых ферм, уступая только США и Казахстану. Некоторые регионы, такие как Иркутская область, стали важными центрами майнинга благодаря дешёвой электроэнергии. Крупные российские игроки заявляют весьма значительные финансовые показатели. Компания Intelion Data Systems достигла выручки в 2,27 миллиарда рублей, что является приростом более чем на 120% по сравнению с предыдущим годом. В то же время Protminter получила 1,42 миллиарда рублей, а Sibmain отчиталась о выручке в 1,25 миллиарда рублей.

До принятия закона майнинг находился в серой зоне: он не был запрещён, но и не регулировался должным образом. Новый закон легализовал майнинг, установив чёткие правила для компаний и частных лиц, занимающихся этим видом деятельности. В частности, майнеры обязаны регистрироваться в государственном реестре и получать лицензии на майнинг. Для этого им необходимо соответствовать определённым критериям, таким как использование лицензированной энергетической инфраструктуры и соблюдение экологических стандартов.

Одна из ключевых частей закона – введение налога на майнинг. Майнеры обязаны платить налог с доходов, полученных от добычи криптовалют. При этом закон допускает прогрессивную шкалу налогообложения, в зависимости от объёмов добычи и размера предприятия. Частные майнеры, работающие на небольших установках, облагаются минимальным налогом, в то время как крупные майнинговые фермы заплатят значительно больше. Введение налога должно увеличить поступления в бюджет и сделать индустрию более прозрачной.

С введением более чёткого регулирования криптовалют и майнинга Россия стремится увеличить свою долю на мировом рынке цифровых активов и активнее использовать их для платежей. Возможность легального использования криптовалют в международных расчётах открывает новые перспективы для экспортёров и компаний, работающих с иностранными партнёрами. В условиях санкций и ограниченный доступ к криптовалютам может стать важным инструментом для поддержания международной торговли.

Новый закон также уточнил различия между децентрализованными и централизованными цифровыми валютами, что позволило разграничить правовые рамки для криптовалют и цифрового рубля, который в 2024 году был введён в обращение.

Цифровой рубль стал ключевым приоритетом Центрального банка России в 2024 году. Он представляет собой централизованную государственную цифровую валюту, основанную на технологии распределённых реестров, выпускаемую ЦБ и контролируруемую государственными органами. По сути, это обязательство ЦБ, номинированные в рублях и размещённые в государственном распределённом реестре. Введение цифрового рубля было направлено на создание более прозрачной и контролируемой системы электронных платежей, а также на расширение доступа граждан к банковским услугам в удалённых регионах. Цифровой рубль как государственная цифровая валюта находится под полным контролем Центробанка России и подчиняется строгому государственному регулированию. В то же время децентрализованные криптовалюты, такие как биткойн и эфириум, остаются в более гибкой правовой среде, хотя и подлежат обязательной идентификации и декларированию. Эти различия важны, так как цифровой рубль рассматривается как часть официальной денежной системы, а криптовалюты – как активы, не являющиеся законным средством платежа внутри страны. В настоящее время пилотный проект по развитию цифрового рубля расширяется, в 2025 году в нем будет участвовать около 10 тысяч тестеров, 15 банков и около 1000 торговых точек. Соответственно, был принят ряд законов, юридически описывающих статус цифрового рубля и случаи его принудительного внедрения в торговые точки и банки [4].

Несмотря на эти важные изменения в законодательстве, остаются определённые вызовы и риски, связанные с регулированием цифровых валют в России.

Использование концепции ограниченного экспериментально-правового режима сужает круг потенциальных участников и ограничивает развитие внутреннего рынка.



До конца не урегулирован вопрос о том, могут ли юридические лица держать криптовалюты на своих балансах и как их учитывать в бухгалтерии. Эти пробелы в правовом поле могут создавать трудности для бизнеса и инвесторов.

Некоторые аналитики предсказывают негативное влияние новаций на традиционные финансовые институты. Расширение использования криптовалют и цифрового рубля может оказать влияние на традиционные банки и платёжные системы. Банковская система будет вынуждена адаптироваться к новым условиям и внедрять технологии, связанные с блокчейном и цифровыми валютами, чтобы не терять конкурентоспособность.

Не все аспекты регулирования криптобирж урегулированы. Например, нет чёткого механизма лицензирования таких платформ и нет описания процедуры контроля за их деятельностью. В результате многие биржи с российскими корнями либо работают вне правового поля, либо ищут зарубежные юрисдикции, что снижает прозрачность их деятельности, а также ограничивает доступ российских граждан к легальным криптовалютным сервисам.

Россия, несмотря на принятие новых законов, по-прежнему отстаёт в интеграции своих правил с международными стандартами. Международная практика регулирования криптовалют развивается быстро, и в большинстве стран уже сформировались более зрелые правовые режимы. Это затрудняет сотрудничество с иностранными криптовалютными компаниями и биржами и ограничивает возможности выхода российских компаний на международные рынки. Важно разработать механизмы, которые позволят юридически корректно взаимодействовать с зарубежными криптовалютными экосистемами.

Децентрализованные финансовые системы (DeFi) и умные контракты, которые активно используются в криптовалютном мире, практически не упоминаются в российских законах. В то время как эти технологии активно развиваются и набирают популярность, законодательство не предоставляет чётких правил их использования и не регламентирует возможные риски, связанные с ними. Это создаёт правовой вакуум, который может привести к правовой неопределённости

в случае возникновения конфликтов или необходимости урегулирования споров, связанных с использованием смарт-контрактов.

Подводя итоги, можно сказать, что Россия сделала важный шаг на пути легализации и развития децентрализованных финансовых технологий. Однако при современной динамике развития этого рынка данный шаг недостаточен и рынок нуждается на дальнейшее развитие этого законодательства. ■

Список литературы:

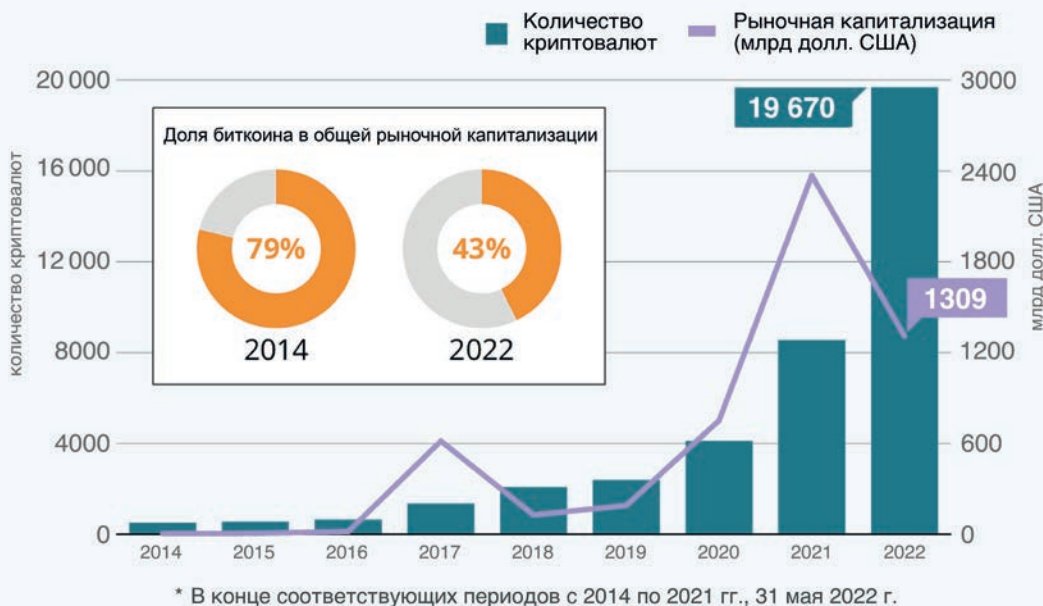
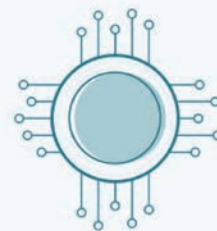
- [1] Федеральный закон от 31.07.2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».
- [2] Поправки по майнингу: «Федеральный закон от 08.08.2024 г. № 221-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации».
- [3] Поправки по ЭПР: «Федеральный закон от 08.08.2024 г. № 223-ФЗ О внесении изменений в отдельные законодательные акты Российской Федерации».
- [4] Поправки по цифровому рублю: «Федеральный закон № 339-ФЗ О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» и Федеральный закон № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».

Об авторе

Профессор Виктор Леонидович Достов, председатель Ассоциации участников рынка электронных денег и денежных переводов, один из самых авторитетных практиков, аналитиков и консультантов в области цифровых финансов. Виктор Достов – автор многочисленных публикаций по данной теме и ведущий профессионального Telegram-канала «Записки на рукавах». dostov@yandex.ru

Эволюция криптоэкономики

Общее количество криптовалют и общая рыночная капитализация*



Источник: Statista Digital Economy Compass 2022, CoinMarketCap

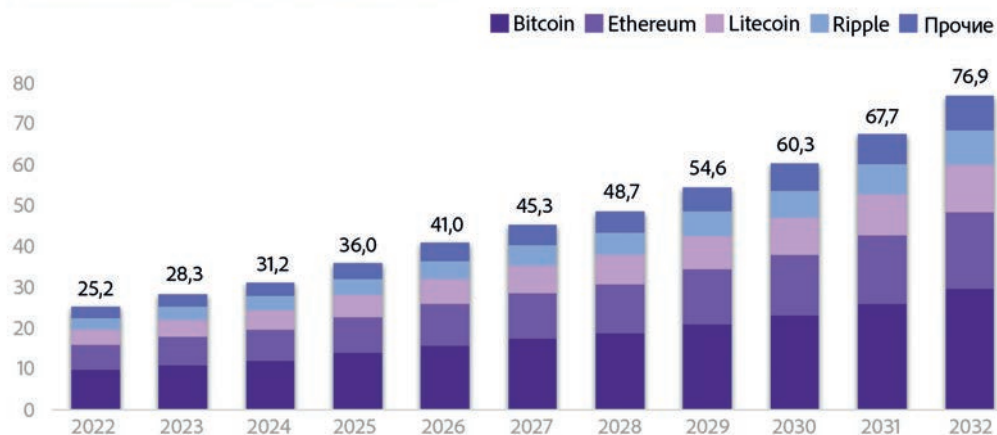


statista

Источник: <https://www.statista.com/chart/27561/evolution-of-the-crypto-economy/>

Глобальный рынок цифровых валют

Объем, по видам, 2022-2032 (млрд долл. США)



Рынок будет расти в среднем на уровне **12,13%**

Прогнозируемый объем рынка на 2032 г. в долл. США **76,9 млрд**

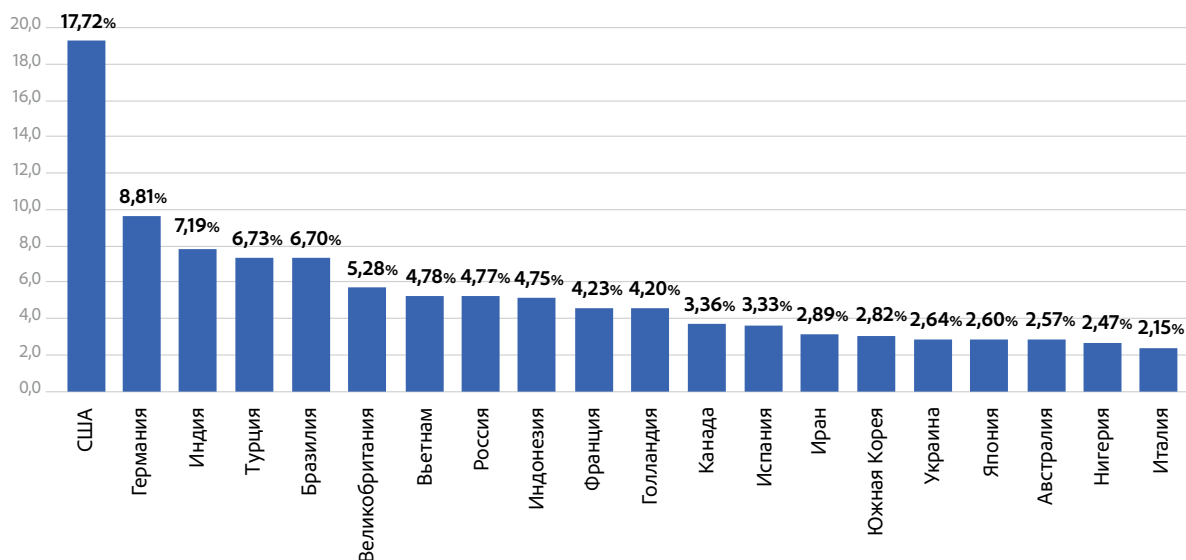
market.us

Источник: <https://market.us/report/digital-currency-market/>



Пользователи криптовалюты по всему миру

(по данным на январь 2024 г.)



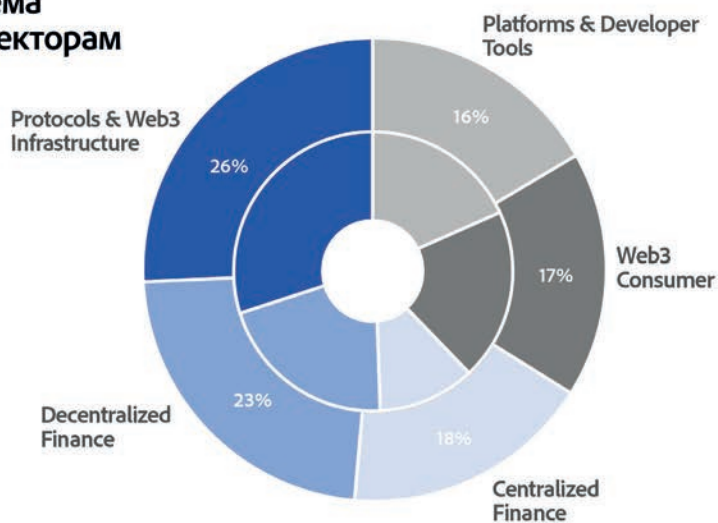
Источник: <https://coinmarketcap.com/academy/article/according-to-cmc-crypto-market-analysis-2024>

Распределение общего объёма инвестиций в 2023 году, по секторам

Внутренний круг - 2022 г.
Внешний круг - 2023 г.

Общий объём инвестиций в стартапы стабилизировался и остаётся на высоком уровне. Растут портфели инвестфондов, а бизнес продолжает развивать Crypto и Web3.

Source: Coinbase



Источник: <https://coinbase.bynder.com/m/c8c6fdc663f44b5/original/2024-Crypto-Market-Outlook-V3.pdf>



Сергей Безделов: «Мы за майнинг с цивилизованным лицом»



В сентябре 2023 года в России была создана Ассоциация промышленного майнинга, объединившая крупнейших участников российского рынка промышленного майнинга, которые формируют стандарты работы отрасли, способствуют развитию цифровой экономики России, участвуют как эксперты в законотворческой работе и ведут диалог с регуляторами. О том, что такое промышленный майнинг, как развивается майнинг в России и какие у него перспективы, а также о задачах, которые ставит перед собой Ассоциация промышленного майнинга, мы беседуем с директором Ассоциации Сергеем Александровичем БЕЗДЕЛОВЫМ.

Промышленный майнинг - новая отрасль промышленности в области производства криптовалют. Строительство дата-центров большой мощности полностью ложится на плечи компании-оператора промышленного майнинга. Это высокотехнологичный объект, имеющий продвинутые системы охлаждения, а также систему централизованного управления работой оборудования. На данный момент объём промышленного майнинга в России составляет около 1,5-1,7 ГВт и занимает 65% общего рынка майнинга в России (35% приходится на частный майнинг). Россия занимает второе место в мире по майнингу биткоина с долей от общего объема хешрейта свыше 13%. Эксперты считают, что при разумном и взвешенном регулировании российская майнинговая отрасль сможет уверенно достигнуть плановых показателей по увеличению мощности до 5,5 ГВт в ближайшие два-три года.

- Сергей Александрович, в августе этого года был принят закон о промышленном майнинге. Как это повлияет на дальнейшее развитие майнинга в России? Что это даёт стране и какие задачи сейчас предстоит решать в первую очередь?

- Восьмого августа 2024 года президент Российской Федерации В.В. Путин подписал федеральный закон о майнинге (№ 221), которым ввёл уже давно существующую отрасль промышленного майнинга в правовое поле государства. Одновременно с этим законом был принят федеральный закон об экспериментальном правовом режиме (№ 222), который позволяет использовать криптовалюту участникам внешнеэкономической деятельности.

Отдельные положения федерального закона о майнинге вступили в силу только 1 ноября текущего года. Они урегулировали порядок осуществления майнинга в Российской Федерации и определили, что майнинговая деятельность для юридических лиц и индивидуальных предпринимателей возможна только с момента включения в реестр майнеров.

Вне всякого сомнения, принятие законодательства положительным образом отразится на отрасли, повысит доверие к ней со стороны институциональных инвесторов и широких слоёв населения, поможет структурировать участников майнинга и избавить рынок от недобросовестных игроков.

Введение отрасли в правовое поле даёт такие преимущества, как создание рабочих мест, уплата налогов, обеспечение криптоликвидности для осуществления расчётов в рамках внешнеэкономической деятельности.

Федеральный закон от 8 августа 2024 года № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» регулирует майнинговую деятельность. Документ ввёл отрасль промышленного майнинга в правовое поле и закрепляет порядок и условия ведения такой деятельности.

Некоторые положения закона:

- **Легальное определение майнинга.** Майнингом цифровой валюты признаётся деятельность по проведению математических вычислений путем эксплуатации технических и программно-аппаратных средств для внесения записей в информационную систему, использующую технологию, в том числе технологию распределенного реестра, имеющих целью выпуск цифровой валюты и (или) получение лицом, осуществляющим такую деятельность, вознаграждения в цифровой валюте за подтверждение записей в информационной системе.
- **Регистрация участников.** Заниматься майнингом смогут российские юридические лица и индивидуальные предприниматели после включения в реестр Минцифры. Физические лица, не являющиеся предпринимателями, могут майнить без включения в реестр, но они обязаны соблюдать лимиты потребляемой электроэнергии, которые будет устанавливать правительство РФ.
- **Запрет на рекламу.** Нельзя рекламировать и предлагать неограниченному кругу лиц цифровую валюту, а также товары, работы и услуги для её обращения.

Федеральный закон от 8 августа 2024 года № 222-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» устанавливает «антиотмывательные» правила для майнинга. Документ обязывает участников рынка вести учёт и отчётность по операциям с цифровыми активами, чтобы минимизировать риски несанкционированного оборота валют и бороться с отмыванием доходов, полученных преступным путём.

Халвинг (от англ. halving — «деление пополам») — это процесс уменьшения скорости генерирования новых единиц криптовалюты и, как следствие, снижение размера вознаграждения майнерам за добытый блок.

Основная цель халвинга — сдерживание инфляции криптовалюты за счёт сокращения эмиссии новых монет. Алгоритмы таких криптовалют, как биткойн, не позволяют печатать бесконечное количество денег. Эмиссия биткойна ограничена 21 миллионом монет, и за счёт механизма халвинга в сети биткойна предложение монет растёт поступательно и заметно уступает темпам роста спроса на них. В первые годы существования биткойна за добытый блок майнеры получали по 50 BTC*, после халвинга 2012 года — 25 BTC, с 2016 года — 12,5 BTC, с 2020 года — 6,25 BTC, в 2024 году будут получать 3,125 BTC.

*BTC — bitcoin, биткойн

- Эмиссия каждой новой криптовалюты требует всё больших вычислительных мощностей, но из-за санкций возникают проблемы с появлением на нашем рынке современного оборудования. Сможет ли с этой задачей справиться отечественное производство?

- В настоящее время для майнинга криптовалют используется импортное оборудование, общепринятым лидером по его производству является Китай.

Конечно, оборудование необходимо обновлять — к примеру, не так давно в очередной раз увеличилась сложность вычислений в сети Bitcoin, соответственно, нужно более мощное оборудование. Но это не значит, что надо одномоментно менять всю линейку оборудования — всё происходит постепенно. Так как Китай является основным производителем оборудования для майнинга, проблем с поставками в нашу страну нет.

Разумеется, мы обсуждаем внутри ассоциации с нашими членами и лидерами рынка, что нужно постепенно налаживать отечественное производство. Но пока речь идёт лишь об отвёрточной сборке: проблема в отсутствии отечественных чипов, пригодных для майнинга.

- Рассказывая о майнинге, в качестве примера вы практически всегда приводите биткойн и операции с ним. Но есть же множество других криптовалют, тот же эфириум. Почему именно биткойн? Что в нём такого особенного?

- Биткойн это первая криптовалюта и она является флагманом крипторынка. Биткойн занимает от 50% до 60% рынка, на котором представлено примерно 18 тысяч разных криптовалют. И эфириум, который вы упомянули, занимает около 20%.

Также биткойн является первой в мире криптовалютой, которую признали на государственном уровне. В 2021 году в Сальвадоре признали биткойн законным средством платежа, которым можно расплачиваться, платить налоги и осуществлять выплаты субсидий.

- Чем дороже и больше вычислительные мощности, тем ниже рентабельность майнинга. При этом в принятом законе речь идёт, в том числе, и о майнинге физическими лицами. Насколько это реально? И где физлицу взять столько электроэнергии?

- Принятый федеральный закон разрешает осуществлять майнинг цифровой валюты физическим лицам без включения в реестр майнеров, но в пределах норм потребления электрической энергии, которые были установлены 1 ноября правительством РФ.

Так, в соответствии с постановлением правительства Российской Федерации № 1178 установлен лимит энергопотребления при осуществлении цифровой валюты в размере 6000 киловатт-часов в месяц.

Конечно, при осуществлении майнинга физическому лицу лучше осуществлять свою деятельность через оператора майнинг-инфраструктуры. Во-первых, оператором является лицо, включённое в реестр, сведения о котором проверила Федеральная налоговая служба. Во-вторых, у операторов существуют готовые инфраструктурные решения, такие как стабильный Интернет, стабильное энергоснабжение и технические специалисты, которые вовремя перезапускают устройство в случае нарушения в его работе. Как мы знаем, для получения максимальной прибыли от майнинга устройство должно работать 24/7/365.

Если же физическое лицо планирует увеличивать потребление мощности, ему потребуется зарегистрировать ИП или ООО и осуществлять свою деятельность с момента включения в реестр майнеров.

- А что может помочь увеличить поток инвестиций в промышленный майнинг от физических лиц и какие сейчас есть препятствия на пути развития данной отрасли среди инвесторов?

- После появления законов о майнинге мы стали официальной частью экономики России. Теперь благодаря прозрачным и понятным правилам работы отрасли, интерес со стороны крупных и частных инвесторов возрастает.

По нашим оценкам, в ближайшие 2-3 года в отечественную майнинг-отрасль может быть вложено примерно 250 миллиардов рублей.

- Восьмого августа 2024 года президент России подписал закон, разрешающий проводить трансграничные расчёты и биржевые торги цифровой валютой. Соответствующие операции будут осуществляться в рамках экспериментальных правовых режимов (ЭПР). Поясните, пожалуйста, в чём суть ЭПР? Чьи интересы это затронет?

- С 1 сентября законодательство позволяет осуществлять трансграничные расчёты и биржевые торги в рамках экспериментального правового режима. То есть компании расплачиваются за ввозимые товары с использованием ЦФА (криптовалюты), не вызывая вопросов у контролирующих органов.

На практике это выглядит примерно так: импортёрам, использующим ЭПР, предлагается оплачивать свои покупки за рубежом рублями на счета, которые будут указаны Центробанком для экспериментального правового режима. ЦБ получает рубли и далее использует криптовалюту уже внутри некой внутренней экосистемы. Например, берётся биткоин, намайненный в России, он заводится в дружественной нам резиденции в криптомир через покупку USDT*.

USDT переводится в ту валюту, которая нужна, в юань, в иену, в доллар, неважно. Идёт расчёт за тот продукт, который

Стейблкоины (stablecoins) — это криптовалютные токены, курс которых привязан к какому-либо активу, например, к доллару, евро или унции золота. Крупнейший и самый популярный из них — Tether USD (USDT), который выпускает компания Tether Limited. В основном «стабильные монеты» используются трейдерами для перемещения цифровых активов между биржами, но также постепенно приживаются в сфере потребительских платежей. В отличие от таких криптовалют, как Bitcoin или Ethereum, их курс не подвержен колебаниям в зависимости от условий на рынке.

Компания Tether Limited выпускает несколько стейблкоинов с привязкой к курсу реальных активов — к доллару (USDT), к евро (EURT), к юаню (CNHT), к песо (MXNT) и к унции золота (XAUT). Как правило, говоря «стейблкоин Tether», подразумевают именно USDT.

нужно приобрести нашему импортёру. Продукт поставлен, и паспорт сделки закрывается актом выполненных работ.

Сейчас государство в лице Банка России и Росфинмониторинга смотрит, как идёт эксперимент, и если механизм себя оправдает, то тогда, может быть, он перестанет быть экспериментальным, а станет обычной моделью расчётов.

- Есть ли понимание, как могут функционировать легальные российские криптобиржи? Кто уже претендует на лидерство?

- Пока и биржи, и обменники законом запрещены.оборот криптовалюты сегодня возможен только в части экспериментального правового режима. Но думаю, что в дальнейшем, когда государство посмотрит, как будет функционировать ЭПР, инфраструктура будет развиваться, и на каком-то этапе появятся и криптобиржи, и обменники криптовалют. Это же тоже часть системы оборота криптовалюты, и постепенно мы придём к классическому построению инфраструктуры криптооборота.

- Что вы думаете о налоговом потенциале майнинга?

- Если майнинг продолжит активно развиваться, сохранится стабильный рост инвестиций, то даже без увеличения числа майнеров государство в год будет получать дополнительно около 50 миллиардов рублей налоговых поступлений. Если количество майнеров будет расти, если инвестиции будут увеличиваться, соответственно, эта сумма будет тоже увеличиваться.

- Промышленный майнинг требует наличия (а также развития и создания новых) современных мощных ЦОДов. Такие ЦОДы специализируются только на майнинге или же их можно использовать и для других процессов, требующих серьёзных вычислительных мощностей - например, для искусственного интеллекта?

*USDT (Tether) — гибридная крипто-фиатная валюта, цена которой привязана к стоимости доллара



- Майнинг сегодня - это пересечение ряда отраслей и сфер: IT, финтех, искусственный интеллект. Это даёт возможность нам размещать в ЦОДах оборудование для других задач. И уже практически год в некоторых ЦОДах членов Ассоциации промышленного майнинга в некоторых локациях идёт не только процесс майнинга криптовалют, 20-30% площадей используется для другой деятельности, в первую очередь, для развития проектов, связанных с искусственным интеллектом. Это вообще мировой тренд для майнинговых компаний - диверсифицировать свою деятельность, соединять её с реализацией проектов в области ИИ.

Я входил в рабочую группу, возглавляемую вице-премьером Дмитрием Чернышенко, по формированию паспорта национального проекта «Экономика данных», и на заседании группы в 2023 году я рассказал, что именно майнинговые компании могут стать точками входа для малого и среднего бизнеса, который реализует проекты ИИ.

Мы совместно с МФТИ провели научно-исследовательскую работу (НИР), которая подтверждает, что в наших ЦОДах можно реализовывать проекты искусственного интеллекта. Результаты НИР были направлены в аналитический центр при правительстве Российской Федерации и получили положительную оценку.

Когда заработает проект «Экономика данных», мы будем полностью готовы.

Также мы уже создали нейrolабораторию, где разрабатываются коробочные решения для малого-среднего бизнеса, чтобы двигаться в реализации национальных стратегических задач в области искусственного интеллекта.

- Какие задачи ставит перед собой Ассоциация промышленного майнинга?

- Мы хотим, чтобы Ассоциация продолжала быть переговорной, коммуникативной, интегрирующей платформой, площадкой для диалога бизнеса, государства, крупных пред-

приятий с целью формирования точек зрения, взглядов, оценочных решений для всей отрасли.

Безусловно, ставим себе задачу формирования отраслевых правил, инвестиционной политики, денежно-кредитной политики внутри отрасли, в том числе правил ввоза оборудования. И конечно, всячески поощряем обмен опытом между членами ассоциации, помогаем в поиске партнёров - в общем, стараемся быть максимально полезными и для наших членов, и для отрасли, и для страны.

- Ассоциация промышленного майнинга организует множество социальных программ для населения, занимается благотворительностью и т.д. А что с экологическими программами? Как вы считаете, вредит ли на самом деле майнинг экологии? И если да, что можно сделать, чтобы нивелировать этот вред?

- Я бы сказал, что слухи о неэкологичности майнинга сильно преувеличены. Например, на Глобальном Юге повсеместно для майнинга используется энергия, полученная от солнечных батарей. Что касается вредных тепловых выбросов, то тут также на помощь приходят современные технологии, и этот газ не выбрасывается, а начинает, например, вращать турбину и давать отопление в дома. От традиционного использования угля в этом случае вреда для экологии гораздо больше.

Но здесь, конечно, важно, чтобы оператор использовал для процесса майнинга самые современные технологии, соответствовал всем требованиям. Мы в Ассоциации промышленного майнинга боремся именно за это - за майнинг с цивилизованным лицом. ■

Сергей Александрович Безделов — кандидат экономических наук. Директор Ассоциации промышленного майнинга, один из ведущих экспертов по вопросам майнинга и цифровой экономики. Занимает пост первого заместителя председателя совета по финансово-промышленной и инвестиционной политике ТПП РФ, а также является руководителем рабочей группы в РЭУ им. Плеханова по реализации вопросов цифровой экономики.

Был генеральным директором ООО «Интер РАО Сервис» — компании, оказывающей услуги по таможенному оформлению товаров (в том числе энергетическое оборудование), перемещаемых через таможенную границу.

Являлся членом экспертного совета по цифровой экономике и блокчейн-технологиям при комитете Госдумы по экономическому развитию, промышленности, инновационному развитию и предпринимательству, а также участником рабочей группы по реализации программы правительства «Цифровая экономика» при «Ростехе». Принимал активное участие в выработке законопроекта по майнингу.

info@mining.ru

Цифровые валюты как важный элемент современной финансовой системы

Максим Будкин



Аннотация

Цифровые валюты представляют собой важный элемент современной финансовой системы, требующий регулирования и развития для обеспечения стабильности и безопасности в мировой экономике. В статье обсуждаются эти современные формы денег, существующие только в электронном виде, и их разнообразие – от криптовалют и стабильных монет до цифрового рубля. Важным аспектом является различие между цифровой валютой и криптовалютой, также подробно рассматривается использование цифровых валют в различных странах мира – на примерах Японии, Швейцарии, Китая, США.

Статья также рассказывает о российском цифровом рубле, о перспективах проведения расчётов в ВЭД с помощью цифровой валюты, в частности, стейблкоинов.

Ключевые слова:

блокчейн, криптовалюта, зарубежный опыт использования цифровых валют, цифровой рубль, ВЭД, стейблкоин

Вступление

Цифровая валюта – это современная форма денег, которая существует только в электронном виде, без физического эквивалента в виде монет или банкнот. В современном мире, где всё больше людей переходят в цифровую среду, цифровые валюты становятся всё более популярными. Они представляют собой новую форму обмена, отличную от традиционных валют, таких как доллары, евро или иены.

Традиционные валюты находятся под контролем центральных банков или правительств, в то время как некоторые цифровые валюты могут функционировать независимо от вмешательства третьих лиц. Цифровые валюты также отличаются высокой степенью анонимности и конфиденциальности. Пользователи могут осуществлять платежи и проводить транзакции, не раскрывая личную информацию или детали финансовых операций.

История цифровой валюты уходит корнями в конец XX века, когда появились ранние прототипы электронных систем платежей. Одним из первых значимых шагов в этом направлении стало создание в 1989 году системы DigiCash, разработанной криптографом Дэвидом Чаумом (David Chaum). DigiCash предложила анонимные электронные платежи с использованием криптографии, заложив начало идеям цифровой валюты.

Важный вклад в развитие цифровых валют внес ученый Ник Сабо (Nick Szabo), который в 1998 году предложил концепцию «цифровых монет» на основе криптографии. Это предложение заложило основы для развития систем электронных платежей, основанных на криптографических принципах.

Необходимо также отметить группу «шифропанков», участников движения Cypherpunk, которые начали активно обсуждать и исследовать возможности цифровых валют ещё в конце 1980-х – начале 1990-х годов. Одними из самых влиятельных фигур в этом сообществе были Эрик Хьюз (Eric Hughes) и Тимоти Мэй (Timothy C. May), которые выдвинули идеи создания анонимных электронных денег, свободных от контроля государства.

В 2008 году с появлением статьи автора под псевдонимом Сатоши Накамото (Satoshi Nakamoto) «Bitcoin: A Peer-to-Peer Electronic Cash System» произошёл настоящий прорыв в сфере цифровых валют. В статье был описан принцип работы первой децентрализованной цифровой валюты – биткойна, который стал первым успешным криптовалютным проектом, устранив потенциальную уязвимость, характерную для цифровых и криптовалют, а именно проблему двойного расходования одних и тех же активов, без централизованного управления. Другими словами – как все члены денежной системы могут быть уверены, что другие не дублируют их деньги по своему желанию? Без решения этой проблемы криптовалюта не сможет функционировать.

Технологии цифровой валюты

Для понимания происхождения и работы цифровых валют необходимо рассмотреть технологии, лежащие в их основе.

Блокчейн – это технология, лежащая в основе функционирования цифровых валют. Он представляет собой децентрализованную базу данных, где хранится информация обо всех операциях с криптовалютами. Благодаря блокчейну обеспечивается прозрачность, безопасность и надёжность совершения сделок с цифровыми активами.



В основе блокчейна лежит идея общедоступной базы данных, к которой имеют доступ все участники сети. Это исключает возможность манипулирования данными одним участником без согласия остальных. Все транзакции записываются в блоки и добавляются к цепочке, что позволяет каждому участнику просматривать и проверять все операции, совершённые в сети.

Суть блокчейна заключается в цепочке блоков, где каждый блок содержит данные и хеш предыдущего блока, обеспечивая целостность и непрерывность всей системы. Эта инновационная технология считается одной из наиболее перспективных в современном мире.

Формы цифровой валюты

Криптовалюты являются одной из самых популярных разновидностей цифровых валют. Они представляют собой децентрализованные валюты, созданные на основе криптографии. Наиболее известной криптовалютой является Bitcoin.

Нужно немного более подробно остановиться на том, чем отличается криптовалюта от цифровой валюты. Хотя эти термины часто используются как синонимы, между ними существуют значительные различия. Криптовалюта является одной из форм цифровой валюты, но не все цифровые валюты можно отнести к криптовалютам.

Криптовалюта представляет собой форму цифровой валюты, основанной на криптографии для обеспечения безопасности транзакций, контроля над выпуском новых единиц и проверки переводов. Одним из ключевых принципов криптовалюты является автоматизированная децентрализованная система, где отсутствует централь-

ное управление и контроль над выпуском и проведением операций.

С другой стороны, цифровая валюта представляет собой более широкое понятие, охватывающее все формы электронных денег, существующих исключительно в цифровой форме. Цифровая валюта может быть как централизованной, так и децентрализованной, а также использовать или не использовать криптографию для обеспечения безопасности операций. Примерами цифровой валюты являются цифровые рубли, электронные доллары, WebMoney, «Яндекс.Деньги» и другие электронные платёжные системы.

Различие между криптовалютой и цифровой валютой может быть довольно существенным и заключаться в методах обработки транзакций, обеспечения безопасности, принципах функционирования и управления. Криптовалюта функционирует на основе распределённого реестра базы данных, криптографии и строгого контроля за эмиссией. В контексте цифровой валюты, которая может быть централизованной, применение технологии блокчейн ограничено. Классические цифровые валюты обычно оперируют централизованными базами данных, под контролем центральных организаций или правительств. Это позволяет управлять и изменять данные в соответствии с монетарной политикой или другими требованиями.

Существует ещё одна форма цифровой валюты - стейблкоины. Это форма цифровой валюты, стоимость которой привязана к курсу традиционных мировых валют, таких как доллары США или евро, или к золоту. Стейблкоины были созданы с целью упрощения конвертации криптоактивов в традиционные фиатные валюты, а также для хеджирования от волатильности (уменьшение рисков изменчивости рынка). Эти цифровые валюты широко используются для покупки и

продажи криптовалюты, проведения быстрых и экономических транзакций без риска резких скачков цен, свойственных криптовалютам.

Цифровые единицы учёта, называемые токенами, представляют собой цифровые активы, созданные на основе технологии блокчейн и используемые для отражения различных ценностей, объектов или прав. Технически между криптовалютой и токенами нет разницы (каждую единицу биткоина тоже можно считать токеном), однако в криптоиндустрии это понятие применяют к активам, которые имеют чуть более широкое применение. Токены могут быть использованы для предоставления доступа к продуктам или услугам в рамках определённых протоколов, платформ или приложений, работающих на блокчейне, а также могут использоваться в качестве средства управления и голосования в различных криптопроектах. Они могут предоставлять и подтверждать право собственности на различные активы, такие как акции компании, недвижимость или другие формы токенизированных инвестиций или уникальных произведений цифрового искусства.

В некоторых странах уже начали активно изучать возможность выпуска собственных цифровых валют, которые получили название цифровых валют центральных банков ЦБЦБ (Central Bank Digital Currency, CBDC). Эти цифровые валюты представляют собой официальные средства платежа, выпущенные центральным банком страны, и могут использоваться в качестве альтернативы физическим наличным деньгам.

Как получить цифровую валюту

Существует несколько основных методов получения цифровой валюты, среди которых выделяются майнинг, стейкинг, покупка на биржах или у других владельцев. Майнинг представляет собой процесс создания новых блоков в цепочке блоков криптовалюты. Для этого майнеры используют специализированное оборудование и мощности вычислительных систем для решения сложных математических задач, связанных с проверкой и обработкой новых транзакций. После успешного завершения задачи майнер получает вознаграждение в виде криптовалюты. Этот алгоритм называется Proof of Work (PoW – «доказательство работы»), он подразумевает, что главным аспектом достижения консенсуса (то есть согласия всех участников на то, что операция считается достоверной) является объём хешрейта майнера. Хешрейт – это вычислительная техника, обладающая достаточной мощностью для проведения нужных операций и открытия нового блока.

Алгоритм Proof of Stake (PoS – «доказательство доли») альтернативен PoW, в этом случае транзакции подтверждаются не майнерами, имеющими наибольший хешрейт, а теми, кто обладает большим количеством токенов выбранной криптовалюты. Метод называется стейкинг (или форжинг) и представляет собой аналог классических банковских депозитов или процесс участия в поддержке сети криптовалюты через технологию блокчейн. Участники направляют на депозит свои монеты в обмен на вознаграждение. Чем больше монет у вас на депозите, тем на более высокое вознаграждение можно рассчитывать в виде новых монет.

Приобрести криптовалюту можно и у других участников криптопространства – как напрямую, так и с использованием различных сервисов, а также на криптообменниках или на криптобирже. Процесс схож с покупкой любых товаров по пластиковой карте, перевод денежных средств на карту или счёт другого физического лица или организации и зачисление криптовалюты на предоставленный криптокошелёк.

Цифровые валюты стран мира

Некоторые страны строго контролируют и регулируют цифровые валюты с целью предотвращения преступной деятельности, отмывания денег и финансирования терроризма. Например, Япония приняла законы, регулирующие деятельность цифровых валютных обменников и платёжных систем, с целью защиты интересов инвесторов и предотвращения финансовых махинаций.

В рамках японской правовой системы цифровые валюты рассматриваются как средство обмена, а не как законное платёжное средство. Одним из ключевых законов, регулирующих использование криптовалют в Японии, является Закон о платёжных услугах, принятый в 2009 году. Согласно этому закону, операторы криптовалютных бирж обязаны получить лицензию от Финансовой службы Японии (FSA) для осуществления своей деятельности в данной сфере.

Кроме того, в Японии в 2017 году появился единый регулирующий кодекс для криптовалютных бирж. Этот кодекс был разработан для усиления защиты пользователей и предотвращения преступной деятельности в сфере криптовалют.

В других странах наблюдается стремление к созданию более открытого рынка цифровых валют, что способствует стимулированию инноваций и развитию финансовых технологий. Например, в Швейцарии существует благоприятная среда для развития стартапов в области криптовалют, и правительство активно поддерживает проекты в этой сфере.

В 2016 году Швейцария стала первопроходцем в области регулирования Initial Coin Offerings (ICO) – сбора средств путем выпуска токенов. Местные власти разработали руководящие принципы, которые обеспечили проведение ICO в соответствии с законодательством и прозрачностью.

Следующим значимым этапом стало принятие федерального закона о финансовых услугах (Federal Financial Services Act, FinSA) и исполнительного постановления о финансовых услугах (Financial Services Ordinance, FinSO) в 2020 году. Эти нормативно-правовые акты установили стандарты в области предоставления финансовых услуг, включая оборот цифровых валют, ужесточили контроль за деятельностью компаний, занимающихся криптовалютами, и обязали их соблюдать строгие финансовые стандарты. FinSA предусматривает регистрацию и регулирование провайдеров цифровых активов, а также устанавливает дополнительные требования в области прозрачности и защиты интересов инвесторов.

При этом отдельные страны запрещают использование цифровых валют или вводят запреты на их обмен. Например, Китай ввёл строгие ограничения на торговлю биткоинами и

другими криптовалютами из-за опасений по поводу финансовой стабильности и контроля над движением капитала.

В истории цифровых валют Китай занимает особое место, став одним из первых государств, где они получили широкое распространение. Гражданам страны уже давно стали доступны такие популярные платёжные системы, как Alipay и WeChat Pay, ставшие неотъемлемой частью повседневной жизни. Однако появление криптовалют вроде Bitcoin и Ethereum было воспринято китайскими властями с большой осторожностью, что привело к ужесточению контроля за цифровыми активами.

В 2017 году правительство Китая ввело запрет на проведение ICO - процесса привлечения инвестиций через выпуск новых цифровых активов. Это решение было обусловлено рисками, связанными с мошенническими схемами на рынке криптовалют, и опасениями по поводу возможных финансовых потерь и утраты контроля над оборотом капитала в стране.

В 2018 году Китай принял решение о запрете деятельности криптовалютных бирж и торговых платформ на своей территории, что привело к ограничению возможностей для китайских граждан владеть и торговать криптовалютами. Также были введены аналогичные ограничения в отношении майнинга криптовалют, что привело к снижению активности в этой сфере в Китае.

Со временем правительство Китая продолжало ужесточать контроль над сферой цифровых валют. В 2019 году была ужесточена политика в отношении блокчейн-технологий, в частности, введено требование получения лицензий для занятия разработкой и использованием блокчейн-проектов.

Необходимо отметить, что вместе с введением ограничений на криптовалюты Китай активно работает над созданием собственной цифровой валюты ЦВЦБ, которая является цифровым аналогом национальной валюты. Целью ЦВЦБ является укрепление контроля государства над финансовой сферой и упрощение процесса проведения платежей и расчётов. В Китае цифровые валюты подчиняются строгому регулированию законами и нормативными актами, которые чётко определяют правовой статус и условия использования электронных денег в стране.

В 2020 году был принят Закон о национальных цифровых валютах, который стал одним из ключевых документов, регулирующих цифровые валюты. Этот закон устанавливает основные принципы функционирования цифрового юаня (DC/EP) в Китае, признаёт его законным средством платежа и регулирует операции с данной криптовалютой.

В США цифровые валюты также имеют долгую историю развития, начиная с появления в 2009 году самой популярной криптовалюты – биткоина. С самого начала США выступали за создание альтернативных способов хранения и передачи цифровых активов, и решение этой задачи нашлось в появлении новых видов цифровых валют.

В 2013 году агентство финансовой промышленности США (FinCEN) выпустило официальные руководства по регулированию виртуальных валют, что дало основу правовому

базису для использования криптовалют в стране. Одним из ключевых моментов в истории цифровых валют в США стало появление концепции цифрового доллара. В 2014 году финтех-компания Ripple Labs объявила о создании платформы, предназначенной для облегчения международных переводов через цифровые доллары. Этот шаг стал важным событием, подтверждающим интерес к цифровым альтернативам национальной валюты.

В 2016 году американский хедж-фонд Grayscale Investments объявил о запуске первого инвестиционного продукта, связанного с биткоином и доступного для инвесторов в США. Это стало сигналом для институциональных игроков и инвесторов о потенциальной прибыльности вложений в цифровые активы.

С 2017 года США стали свидетелями роста популярности и значимости криптовалют и блокчейн-технологий. В этот период были разработаны и приняты законодательные акты, направленные на регулирование оборота цифровых валют в стране. Один из наиболее важных моментов – принятие Закона о налогообложении цифровых валют в 2018 году.

Органами, ответственными за регулирование в этой сфере, являются Комиссия по ценным бумагам и биржам США (SEC) и Комиссия по торговле товарными фьючерсами (CFTC), а также Федеральная резервная система и Министерство финансов США.

SEC рассматривает цифровые валюты как ценные бумаги и регулирует их выпуск и обращение на той же основе, что и обычные ценные бумаги. Компании, желающие выпустить цифровую валюту через ICO (Initial Coin Offering), обязаны соблюдать процедуры SEC по регистрации и дислокации информации о проекте. SEC также активно борется с мошенничеством и несанкционированной торговлей цифровыми активами.

CFTC, со своей стороны, регулирует торговлю цифровыми валютами как товарными фьючерсами, устанавливая правила для деривативных сделок с криптовалютами. Это важно для обеспечения прозрачности и ликвидности рынка цифровых активов. CFTC стремится к обеспечению справедливых и эффективных условий для участия в торговле цифровыми валютами для всех участников рынка.

Появление цифровой валюты в России. Цифровой рубль

В России одним из первых интернет-проектов, предлагавших обмен электронных валют, включая биткоин, на классические деньги, был Liberty Reserve. Однако из-за обвинений в причастности к отмыванию денег и другим мошенническим схемам проект был закрыт в 2013 году.

Затем криптовалюты, особенно биткоин, стали активно проникать в российское общество. Хакерские атаки, взломы крупных криптовалютных бирж, негативное отношение регуляторов – всё это вызывало неопределённость и недоверие к цифровым валютам в России. Тем не менее, с каждым годом



всё больше частных лиц и компаний начинали экспериментировать с криптовалютами, рассматривая их как средство инвестирования или сбережения.

Цифровой рубль – это инновационная валюта, разработанная Центральным банком России с целью совершенствования электронных платежей в стране. Представляя собой электронный аналог обычного наличного рубля, цифровой рубль существует исключительно в цифровой форме. Он обладает всеми преимуществами традиционной бумажной валюты, но при этом обеспечивает быстрые и удобные финансовые операции через Интернет и мобильные устройства. Планируется, что новая форма национальной валюты будет широко использоваться к 1 июля 2025 года. Банк России установил окончательные сроки внедрения цифрового рубля и направил соответствующие предложения о внесении изменений в законодательство Министерству финансов.

Широкое внедрение цифровой национальной валюты планируется с 1 июля 2025 года. К этому сроку 13 крупнейших банков России обязаны обеспечить своих клиентов полноценной инфраструктурой для проведения операций с цифровыми рублями. Пользователям будет предоставлена возможность открывать и пополнять счета в цифровых рублях, а также осуществлять переводы.

Среди банков-участников проекта значатся такие финансовые учреждения, как ЮниКредит Банк, ГПБ, Совкомбанк, ВТБ, Альфа-банк, Сбербанк, Московский кредитный банк, банк «Открытие», Росбанк, Т-Банк, Промсвязьбанк, Райффайзенбанк и Россельхозбанк. Остальные банки с универсальной лицензией получают дополнительное время на модернизацию своих систем — до 1 июля 2026 года, в то время как прочим кредитным организациям предоставлен срок до 1 июля 2027 года.

Использование криптовалюты во внешнеэкономической деятельности (ВЭД)

Внедрение криптовалюты в процесс ВЭД может решить ряд проблем и повысить эффективность международных торговых операций. С использованием криптовалюты возможно осуществлять прямые транзакции между участниками международной торговли, обходя банки и прочие финансовые учреждения. Кроме того, криптовалюта обеспечивает высокий уровень безопасности и прозрачности сделок.

Однако использование криптовалюты в ВЭД России представляет собой перспективное, но не лишённое рисков направление. Один из основных рисков заключается в нестабильности курсов криптовалют, что может привести к значительным колебаниям в стоимости транзакций и усложнить учет и контроль финансовых операций. Высокая волатильность криптовалют также увеличивает риск потерь при проведении международных сделок.

Существующее законодательство относительно криптовалют неоднозначно, что может привести к правовой неопределённости и затруднить развитие использования криптовалют в международной торговле. Отсутствие чётких нормативных актов может стать препятствием для безопасных и законных финансовых операций с использованием криптовалют.

Современные хакеры активно занимаются взломом сетей и кражей криптовалют, что может привести к серьезным финансовым потерям для участников международной экономической деятельности. Кроме того, существует риск использования криптовалют для отмывания денег и

финансирования терроризма, что создаёт дополнительные угрозы для бизнеса и экономики в целом.

Анонимность и псевдонимность транзакций с криптовалютами могут способствовать уклонению от налогообложения, отмыванию денег и другим незаконным операциям. Эти факторы затрудняют контроль и мониторинг финансовых потоков, а также создают преграды для законного и прозрачного ведения международных сделок.

В ближайшее время планируется регулирование проведения криптовалютных платежей в рамках эксперимента под контролем Центрального банка России. С 1 сентября 2024 вступил в силу закон, разрешающий использование криптовалют в международных расчетах в рамках экспериментального правового режима (ЭПР). Банк России и Минфин в настоящее время разрабатывают документы, которые позволят определить круг лиц и организаций, участвующих в этом эксперименте.

В начале сентября 2024 года также стало известно, что Минфин и Центробанк планируют провести обсуждение с участниками финансового рынка возможности использования стейблкоинов в международных расчётах. По мнению регулятора, применение «стабильных» криптовалют может оказаться более выгодным для трансграничных платежей, чем традиционные платёжные сервисы.

Перспективы стейблкоинов

Стейблкоины (stablecoin) представляют собой особый вид криптовалют, созданный с целью минимизации волатильности цен для обеспечения стабильности их стоимости. Это цифровые активы, чья стоимость привязана к ценности других активов, таких как доллар США, евро, золото или другие фиатные валюты. Главная задача стейблкоинов заключается в снижении риска колебания цен по сравнению с более волатильными криптовалютами, такими как Bitcoin и Ethereum.

Ключевая идея стейблкоинов заключается в поддержании предсказуемой цены, используя различные механизмы обеспечения или алгоритмы регулирования предложения токенов.

Множество разновидностей стейблкоинов представляет собой разнообразную категорию, каждый тип в которой обладает своими уникальными характеристиками и особенностями. Основное различие между разными видами стейблкоинов заключается в методах, которые обеспечивают их стабильность относительно конкретного актива или индекса. Среди основных видов стейблкоинов можно выделить фиатно-обеспеченные, криптовалютно-обеспеченные, товарно-обеспеченные и алгоритмические.

Фиатно-обеспеченные стейблкоины представляют собой наиболее простой вид этого типа криптовалют и обеспечены традиционными валютами, такими как доллар США, евро и т.п. Для каждого выпущенного токена должна существовать эквивалентная сумма фиатных денег, хранящихся в резерве (примеры: USDT, USDC, BUSD). Обеспеченность фиатными активами делает их стабильными, но требует доверия к организациям, которые хранят эти резервы. Есть риски, связан-

ные с аудитом и прозрачностью этих резервов.

Криптовалютно-обеспеченные стейблкоины обеспечивают стабильность цены за счёт криптовалютных резервов. Например, стейблкоин DAI обеспечен Ethereum. Другие же могут иметь поддержку нескольких криптовалют или других цифровых активов. Эти стейблкоины оперируют на основе смарт-контрактов и децентрализованных механизмов, обеспечивая стабильность и прозрачность операций. Для таких стейблкоинов важно иметь «сверхобеспечение» в связи с высокой волатильностью криптовалют, хранящихся в резерве.

Товарно-обеспеченные стейблкоины поддерживаются реальными товарами, такими как золото, нефть и другие активы (пример: PAXG – обеспечен золотыми резервами). Однако цены на некоторые товары тоже можно считать довольно волатильными.

Среди самых инновационных вариантов стейблкоинов выделяются алгоритмические стейблкоины. Эти активы не обеспечены никакими активами напрямую, их стабильность поддерживается через сложные алгоритмы и механизмы саморегулирования. Работа таких стейблкоинов основана на динамическом изменении предложения и спроса с применением специальных смарт-контрактов, которые контролируют выпуск или уничтожение токенов в зависимости от текущей цены и спроса на рынке. Эти инновации становятся всё более актуальными в контексте развития рынка криптовалют.

В настоящее время регулирование стейблкоинов в различных странах разнится. Некоторые государства признали их официальным средством платежа, другие же полностью запретили их использование, в то время как третьи продолжают исследовать и совершенствовать свои подходы к регулированию данного сектора. Среди успешных проектов стейблкоинов можно выделить Tether (USDT), USD Coin (USDC), TrueUSD (TUSD), Dai (DAI) и другие.

Среди стейблкоинов, привязанных к доллару США в соотношении 1:1, Tether, вероятно, занимает лидирующую позицию в криптовалютной сфере. Его основное предназначение – защитить капитал от колебаний цен и обеспечить стабильность в инвестициях. Кроме того, существуют и другие альтернативы, которые также привязаны к доллару США, такие как USD Coin, созданный Circle и Coinbase, и TrueUSD, представляющий собой более прозрачную альтернативу Tether.

Успешные проекты стейблкоинов оказывают значительное воздействие на рынок криптовалют. Во-первых, они создают более стабильную среду для торговли и инвестирования, что позволяет инвесторам легче защищать свои активы, переходя на стейблкоины в периоды падения цен основных криптовалют. Во-вторых, стейблкоины облегчают процесс конвертации криптовалют в фиатные деньги и наоборот. ■

Об авторе

Будкин Максим Викторович,
Банк ДОМ.РФ, Россия, Москва, maksim.budkin@domrf.ru

Децентрализованные платёжные системы: типы и примеры применения на основе Bitcoin, Ethereum и Stablecoin

Сергей Мельников

Егор Черноусов



Аннотация

В последние годы децентрализованные платёжные системы привлекли внимание как революционная альтернатива традиционным финансовым системам. Они обещают повысить прозрачность, снизить комиссии и предоставить пользователям больше контроля над своими средствами, а также решить главную проблему традиционных централизованных систем финансовых расчётов - наличие централизованного посредника, имеющего возможность в любой момент менять правила игры. В этой статье мы разберём основные типы децентрализованных платёжных систем, их применение и то, как они работают, на примерах блокчейнов Bitcoin и Ethereum, а также рассмотрим аналоги привычных валют, используемых в криптовалюте – Stablecoin.

Ключевые слова:

блокчейн, криптовалюта, стейблкоины, Bitcoin, Ethereum, децентрализованная финансовая система (DeFi)

Предпосылки к созданию децентрализованных платёжных систем

Децентрализованные платёжные системы возникли как ответ на недостатки существующих централизованных финансовых систем. К этим недостаткам можно отнести следующее.

- **Цензура и контроль.** Возможность централизованных финансовых учреждений контролировать доступ к средствам или блокировать их вызывает опасения у многих пользователей. Например, правительственные санкции или замораживание счетов могут использоваться для политического давления. Децентрализованные платёжные системы предлагают альтернативу, при которой никто не может ограничить доступ к средствам.
- **Отсутствие прозрачности.** Централизованные финансовые системы часто страдают от недостаточной прозрачности. Пользователи не могут проверить, как именно обрабатываются их транзакции, или получить точную информацию о состоянии своих активов. Блокчейн обеспечивает полную прозрачность — вся история транзакций доступна для проверки любому участнику сети.

- **Недостаточная безопасность централизованных систем.** Централизованные системы более уязвимы к хакерским атакам. В случае взлома одной компании или учреждения могут пострадать миллионы пользователей. В децентрализованных системах атака на всю сеть значительно сложнее, поскольку отсутствует единая точка отказа.
- **Сложность международных переводов.** Международные переводы через традиционные финансовые системы часто связаны с высокими комиссиями и длительным временем обработки. Банки и посредники взимают фиксированные сборы и проценты за обработку транзакций, что значительно увеличивает стоимость перевода. В отличие от этого, децентрализованные платёжные системы, такие как криптовалюты, предлагают возможность проведения транзакций с минимальными комиссиями, независимо от объёма и географии перевода.

Все эти проблемы — от цензуры и контроля до высоких комиссий и недостатка прозрачности — стали стимулом для создания децентрализованных платёжных систем. И как следствие, в 2008 году был изобретён **Bitcoin**, первая децентрализованная криптовалюта на основе блокчейна, которая предложила решение этих недостатков. Bitcoin исключил необходимость в посредниках, обеспечив прозрачные, защищённые и доступные транзакции, которые нельзя заблокировать или подвергнуть цензуре. Это стало началом новой эры в финансовой системе, где пользователи получили

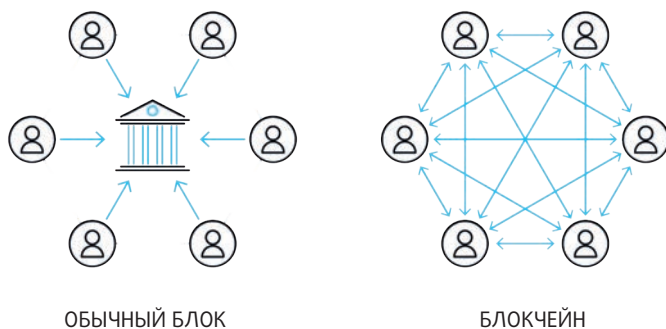
полный контроль над своими активами, а международные переводы стали быстрее и дешевле.

Что такое децентрализованные платёжные системы?

Децентрализованные платёжные системы – это системы, работающие без участия централизованных посредников, таких как банки или финансовые учреждения. В основе этих систем лежит технология блокчейн, которая позволяет участникам сети осуществлять транзакции напрямую друг с другом, без необходимости доверять третьей стороне. Блокчейн обеспечивает прозрачность и безопасность всех транзакций, а также делает систему устойчивой к цензуре и несанкционированным изменениям.

Перед началом рассмотрения отдельных типов децентрализованных платёжных систем поговорим о технологии блокчейн.

Блокчейн — это технология, которая представляет собой распределённый реестр или базу данных, где информация хранится в виде цепочки взаимосвязанных блоков. Каждый блок содержит набор записей (транзакций) и связан с предыдущим блоком посредством сохранения вычисленной хеш-функции от данных, хранящихся в блоке.



Основные принципы блокчейна:

1. **Децентрализация.** Блокчейн хранится и обновляется одновременно на множестве узлов сети (нод), а не в одной централизованной базе данных. Это делает систему менее уязвимой к сбоям и взломам.
2. **Неизменяемость.** После добавления блока в цепочку информация в нём становится неизменяемой. Изменения в уже записанных данных требуют согласования большинства участников сети, что делает подделку информации сложной и трудоёмкой задачей.
3. **Прозрачность.** В большинстве блокчейнов данные доступны для просмотра всеми участниками сети. Это обеспечивает высокую степень прозрачности и позволяет отслеживать транзакции и изменения.
4. **Криптографическая защита.** Блоки связаны между собой с помощью криптографических хеш-функций, которые обеспечивают целостность и безопасность данных. Это предотвращает изменение информации без обнаружения.

5. **Консенсусный механизм.** Для добавления нового блока в цепочку требуется достижение консенсуса (общего согласия большинства) среди участников сети. Существуют различные методы консенсуса, такие как Proof of Work (PoW) и Proof of Stake (PoS), которые определяют, как решается вопрос о добавлении нового блока.

Типы децентрализованных платёжных систем

Bitcoin

Bitcoin, первая и наиболее известная криптовалюта, которая стала родоначальником блокчейнов и идеи децентрализации платёжных систем. Каждая транзакция подтверждается с помощью криптографических вычислений, называемых майнингом, которые выполняют узлы сети (майнеры). Это обеспечивает безопасность и неизменность данных, ведь для того, чтобы внести какие-то изменения, необходимо получить общее «одобрение» от остальных узлов сети.

Несмотря на все преимущества и новаторский подход, Bitcoin не лишён своих недостатков. С течением времени стали очевидны некоторые проблемы, которые показали, что не всё так идеально, как хотелось бы. К таким проблемам можно отнести следующее.

- **Волатильность.** Цена Bitcoin может сильно колебаться, что делает его неподходящим для расчётов, поскольку в ходе сделки курс может значительно поменяться, что усложнит взаиморасчёты.

Среднее дневное изменение цены Bitcoin, как в росте, так и в падении, обычно составляет около 3-5%. Однако важно отметить, что волатильность криптовалют сильно варьируется в зависимости от рыночных условий, например, во времена повышенной активности или новостного фона волатильность может существенно возрасти и превышать 10% в день.

- **Скорость транзакций.** Транзакции могут занимать некоторое время для подтверждения, что делает Bitcoin менее удобным для повседневных расчётов. Среднее время подтверждения одной транзакции в блокчейне Bitcoin составляет около 10 минут. Это связано с тем, что новый блок в сети создаётся примерно каждые 10 минут, и транзакции включаются в этот блок. Однако фактическое время может варьироваться в зависимости от загруженности сети и размера комиссии, которую пользователь готов заплатить. При высокой нагрузке транзакции с низкими комиссиями могут ждать подтверждения дольше.

Также для сравнения: количество транзакций в блокчейне биткоин в день примерно составляет 300 тысяч, тогда как в Ethereum (о нём мы поговорим чуть ниже) около одного миллиона транзакций в день.

- **Высокие энергозатраты.** Майнинг Bitcoin требует значительных вычислительных ресурсов и электроэнергии, что вызывает экологические и экономические вопросы.

Ethereum: расширение возможностей через смарт-контракты

Чтобы преодолеть некоторые из этих ограничений Bitcoin, в 2015 году появился новый блокчейн под названием Ethereum.

Ethereum революционизировал децентрализованные платёжные системы с помощью смарт-контрактов — программ, которые автоматически выполняются, когда выполняются заранее оговорённые условия. В отличие от традиционных договоров, смарт-контракты устраняют необходимость в посредниках, таких как банки или нотариусы, сокращая время и снижая риски ошибок. Эти автоматизированные контракты работают на блокчейне Ethereum и применяются для любых типов сделок — от простых транзакций до сложных финансовых соглашений.

Важной особенностью смарт-контрактов является их децентрализация, что означает, что после развёртывания контракта его код не может быть изменён или удалён, что гарантирует соблюдение его условий без вмешательства третьих сторон. Смарт-контракты находят широкое применение в финансовых операциях, управлении активами и создании децентрализованных приложений (DApps).

Также Ethereum сыграл ключевую роль в развитии **стейблкоинов**, предоставив технологическую основу для их создания и функционирования благодаря своим смарт-контрактам.

Stablecoins

Стейблкоины (Stablecoin) — это криптовалюты, которые имеют фиксированную стоимость, привязанную к определённым активам, таким как фиатные валюты (например, доллар США или евро), товары (например, золото) или даже другие криптовалюты. Эта привязка позволяет стейблкоинам избегать высокой волатильности, характерной для таких активов, как Bitcoin и Ethereum, обеспечивая большую стабильность цен для пользователей.

Таким образом, стейблкоины представляют собой интересный компромисс между стабильностью и децентрализацией, предоставляя пользователям определённые преимущества, но также сталкиваясь с рядом ограничений. Вследствие этого за время своего существования стейблкоины стали крайне востребованы в криптоэкономике. По состоянию на 2023 год объём выпуска крупнейших стейблкоинов, таких как Tether (USDT) и USD Coin (USDC), превысил 100 миллиардов долларов. Они используются не только для хранения стоимости, но и для международных переводов и торговли на децентрализованных биржах (DEX), занимая около 80% объёма транзакций на некоторых платформах.

Как работают стейблкоины?

Основной механизм работы стейблкоинов заключается в обеспечении их стоимости через заложенные активы или алгоритмы. Существует несколько типов стейблкоинов.

1. **Фиатно-обеспеченные стейблкоины** (например, USDT, USDC) поддерживаются резервациями в фиатной валюте. За каждым выпущенным токеном стоит реальный доллар, находящийся на счетах компаний-эмитентов.

2. **Криптообеспеченные стейблкоины** (например, DAI) привязаны к криптовалютам, таким как Ethereum, и их стоимость регулируется через систему смарт-контрактов, которые автоматически выпускают или сжигают токены в зависимости от изменения залогового обеспечения.
3. **Алгоритмические стейблкоины** (например, FRAX, AMPL) не имеют залогов в фиате или криптоактивах, их цена стабилизируется через алгоритмы, которые управляют предложением и спросом на рынке.

Смарт-контракты и стейблкоины

Смарт-контракты играют ключевую роль в работе стейблкоинов. Они автоматически регулируют эмиссию и обеспечение токенов, выполняя заложенные в них условия без участия посредников. Например, в протоколе MakerDAO, который выпускает DAI, смарт-контракты обеспечивают залоговые криптоактивы и следят за тем, чтобы выпущенные токены всегда были поддержаны необходимым количеством активов, то же самое работает и для других типов стейблкоинов.

Минусы стейблкоинов с точки зрения децентрализации

1. **Централизованное обеспечение.** Многие фиатно-обеспеченные стейблкоины, такие как USDT и USDC, поддерживаются централизованными организациями, что может привести к рискам, связанным с отсутствием прозрачности в управлении резервами и возможностью манипуляций.
2. **Регуляторные риски.** Центральные организации, выпускающие стейблкоины, могут подвергаться регулированию и давлению со стороны правительств, что ограничивает децентрализацию и свободу операций.
3. **Правовые риски.** Стейблкоины могут быть использованы для отмывания средств, особенно если платформы, через которые они перемещаются, не соблюдают строгие правила проверки (Know Your Transaction (KYT) и Know Your Customer (KYC)), направленные на борьбу с отмыванием денег и финансированием терроризма.
4. **Уязвимость к централизованным атакам.** Стейблкоины, управляемые централизованными компаниями, могут стать мишенью для хакеров или мошенников, что ставит под угрозу безопасность активов пользователей.

Например, в мае 2022 года произошёл крах стейблкоина TerraUSD (UST) и экосистемы Terra. UST, алгоритмический стейблкоин, потерял паритет с долларом, что вызвало панику на рынке. Массовые продажи UST и его связанного токена LUNA привели к обрушению цены LUNA с более чем 80 долларов до менее чем 1 доллара за несколько дней. Попытки сохранить привязку UST через сжигание LUNA только усугубили ситуацию.

Хотя технически взлома не было, некоторые эксперты указывают на манипуляции рынком как на причину краха. Этот инцидент стал важным уроком о рисках алгоритмических стейблкоинов в криптоиндустрии.

В целом, благодаря своей стабильности, стейблкоины стали важным элементом экосистемы децентрализованных финансов (DeFi), обеспечивая пользователям доступ к стабильным активам в условиях волатильных рынков криптовалют.

DeFi и DApps

DeFi (Decentralized Finance), или децентрализованные финансы, это новый виток в развитии финансовых технологий, который предлагает пользователям доступ к финансовым услугам без посредников, таких как банки или платёжные системы. DeFi и DApps полагаются на блокчейн как на инфраструктуру для хранения данных и выполнения операций. Блокчейн обеспечивает безопасность, неизменность данных и децентрализованную природу, которая является основой для децентрализованных приложений. Эта концепция активно развивается с 2018 года, и к 2023 году её популярность значительно возросла. По состоянию на конец 2023 года общий объём средств, заблокированных в DeFi-протоколах, превысил 50 миллиардов долларов, что свидетельствует о растущем доверии к децентрализованным платформам.

Основные виды DeFi-приложений

1. **Децентрализованные биржи (DEX).** DEX — это платформы, где пользователи могут напрямую обменивать криптовалюты без посредников. Примеры таких бирж включают Uniswap, SushiSwap и PancakeSwap. В отличие от традиционных централизованных бирж, на DEX пользователи сохраняют полный контроль над своими активами, а сделки осуществляются с использованием смарт-контрактов. В 2023 году DEX составляли около 15% общего объёма торгов на рынке криптовалют.
2. **Протоколы кредитования и заимствования.** Платформы, такие как Compound и Aave, позволяют пользователям брать кредиты под залог криптоактивов или предоставлять ликвидность для получения дохода в виде процентов. В 2023 году на таких платформах было размещено более 10 миллиардов долларов активов. В отличие от традиционных кредитных систем, здесь не требуются кредитные проверки, а процентные ставки автоматически регулируются в зависимости от спроса и предложения.
3. **Протоколы доходного фермерства.** Yield Farming, или доходное фермерство, позволяет пользователям зарабатывать проценты, предоставляя свои активы в ликвидные пулы на платформах, таких как Yearn Finance или Curve Finance. Эти платформы предлагают пользователям возможность получать пассивный доход за счёт предоставления ликвидности другим пользователям DeFi-сетей.
4. **Протоколы деривативов и страхования.** DeFi также охватывает более сложные финансовые инструменты, такие как деривативы и страховые продукты. Примеры включают Synthetix, платформу для создания токенов, привязанных к реальным активам, и Nexus Mutual, предлагающую страхование смарт-контрактов. Эти протоколы позволяют пользователям хеджировать риски и торговать синтетическими активами, представляющими реальные товары или акции.

Статистика использования DeFi:

- по состоянию на 2023 год количество активных пользователей DeFi превысило пять миллионов;
- среднемесячный объём транзакций на DeFi-протоколах составлял более 100 миллиардов долларов, что указывает на рост популярности среди инвесторов и трейдеров;
- наибольший рост продемонстрировали протоколы DEX и кредитования, на которые приходится около 60% всего заблокированного капитала.

Преимущества DeFi

1. **Прозрачность и контроль над активами.** Пользователи сохраняют полный контроль над своими активами, так как все операции проводятся через смарт-контракты, открытые для аудита. Любой пользователь может проверить код смарт-контракта и увидеть, как именно обрабатываются его средства.
2. **Низкие комиссии и высокая скорость транзакций.** Устранение посредников позволяет значительно сократить комиссии за транзакции и ускорить их выполнение. Это особенно важно для международных переводов и операций с активами, где традиционные системы могут быть медленными и дорогими.
3. **Финансовая инклюзивность.** DeFi-платформы предоставляют доступ к финансовым услугам жителям развивающихся стран, где банковская инфраструктура слабо развита. Это способствует расширению возможностей для миллионов людей, которые раньше не имели доступа к кредитам или инвестиционным продуктам.

Недостатки DeFi

Несмотря на быстрый рост и потенциал, DeFi сталкивается с рядом проблем.

- **Риски безопасности.** Смарт-контракты могут содержать уязвимости, что делает их мишенью для хакеров.
- **Низкая ликвидность некоторых платформ.** В отличие от традиционных финансовых рынков, некоторые DeFi-платформы страдают от недостатка ликвидности, что может привести к проблемам с исполнением крупных сделок.
- **Регуляторные неопределённости.** Поскольку DeFi-сектор ещё недостаточно урегулирован, существуют риски, связанные со вмешательством регуляторов и изменением законодательства в разных странах.

DeFi — это революционная модель, которая трансформирует мировую финансовую систему, предоставляя пользователям новые возможности для контроля и управления своими активами. Несмотря на существующие риски и недостатки, эта технология продолжает развиваться и привлекать всё больше пользователей и инвесторов, предлагая широкий спектр финансовых услуг на основе блокчейна.

Нововведения: Ethereum 2.0 и переход на Proof of Stake

Ethereum с момента своего создания уже успел получить серьёзное обновление на версию 2.0. И с переходом на Ethereum 2.0 сеть стремится решить проблемы масштабируемости и энергопотребления, присущие модели Proof of Work (PoW) – майнингу, на котором основан Bitcoin. Переход на Proof of Stake (PoS) предполагает использование стейкинга (замораживания токенов для обеспечения безопасности сети) вместо майнинга, что делает сеть менее энергоёмкой и более экологически чистой. Кроме того, PoS увеличивает производительность сети, позволяя обрабатывать тысячи транзакций в секунду.

Ethereum 2.0 также внедряет концепцию шардинга — это разделение данных сети на несколько сегментов, что позволяет каждому узлу сети обрабатывать только часть информации. Эти нововведения делают Ethereum более мощной платформой для создания масштабируемых и эффективных децентрализованных приложений, что, в свою очередь, стимулирует дальнейшее развитие DeFi и DApps на основе смарт-контрактов.

Запуск Ethereum 2.0 послужил катализатором для появления и развития технологии блокчейн второго уровня - Layer2. Layer 2 (L2) блокчейны — это решения, созданные для того, чтобы улучшить работу основного блокчейна Ethereum, сделав его быстрее и дешевле в использовании.

Layer 2 работает как дополнительный уровень, который берёт на себя часть нагрузки с основного блокчейна. Это помогает обрабатывать транзакции быстрее, при этом сам блокчейн остаётся таким же безопасным. Важно то, что L2-блокчейны «работают вместе» с основной сетью, дополняя её, но не изменяя её работу. Это делает криптовалютные операции доступнее для пользователей, особенно, когда сеть сильно загружена.

Таким образом, Ethereum хоть и имеет свои недостатки, такие как высокие комиссии и скорость обработки в моменты высокой нагрузки, сложность разработки и уязвимость смарт-контрактов, но продолжает оставаться лидером в мире децентрализованных приложений и финансовых технологий, предлагая надёжную, автоматизированную и масштабируемую инфраструктуру для будущих цифровых платёжных систем.

Заключение

Децентрализованные платёжные системы, несмотря на свои очевидные недостатки, такие как высокая волатильность, проблемы с масштабируемостью и потенциальные регуляторные риски, продолжают активно развиваться. Технологии, такие как Ethereum 2.0 и решения второго уровня, открывают новые горизонты для повышения эффективности и удобства использования. Стейблкоины, несмотря на свои сложности, обеспечивают стабильность и доступность, что делает их важным элементом криптоэкономики.

С каждым новым достижением и решением текущих проблем

децентрализованные финансовые системы становятся всё более привлекательными для пользователей по всему миру. Возможно, когда эти недостатки будут устранены, нас ждёт будущее, в котором децентрализованные платёжные системы станут неотъемлемой частью финансовой экосистемы, предлагая безопасность, прозрачность и доступность для всех.

Материал подготовлен на основе опыта и при поддержке российской исследовательской компании «Шард», специализирующейся на использовании когнитивных методов при решении новых вызовов для финансовой системы. Аналитические инструменты платформы «Шард» позволяют провести собственное крипто расследование и запросить аналитическую поддержку и правовую помощь. Компания предоставляет решения, способные эффективно справляться с этими проблемами, используя свои инструменты Know Your Transaction (KYT). Платформа «Шард» предназначена для широкой аудитории потенциальных пользователей: от частных лиц с минимальным участием в криптотранзакциях до профессиональных игроков рынка крипто- и фиатных валют. ■

Список литературы:

- [1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System // 2008. Ссылка на документ: [<https://bitcoin.org/bitcoin.pdf>] (Дата обращения: 20.09.2024).
- [2] Buterin V. Ethereum Whitepaper // 2013. Ссылка на документ: [<https://ethereum.org/en/whitepaper/>] (Дата обращения: 20.09.2024).
- [3] MakerDAO Documentation. Описание системы DAI // MakerDAO, 2021. Ссылка на документ: [<https://makerdao.com/en/whitepaper/>] (Дата обращения: 21.09.2024).
- [4] CoinMarketCap. Статистика криптовалют, рыночная капитализация, объёмы торгов // CoinMarketCap, 2024. Ссылка на сайт: [<https://coinmarketcap.com/>] (Дата обращения: 21.09.2024).
- [5] DeFi Pulse. Данные по децентрализованным финансовым платформам (DeFi) // DeFi Pulse, 2024. Ссылка на сайт: [<https://defipulse.com>] (Дата обращения: 21.09.2024).
- [6] Шард. Инструменты KYT// Shard, 2024. Ссылка на сайт: [<https://shard.ru/services/kyt-tools>] (Дата обращения: 24.09.2024).
- [7] Binance Research. Отчёты по криптовалютам и DeFi решениям // Binance, 2024. Ссылка на сайт: [<https://research.binance.com/>] (Дата обращения: 24.09.2024).

Об авторах

Мельников Сергей Иванович,
Россия, Москва, АО «ШАРД», info@shard.ru

Чернусов Егор Александрович,
Россия, Москва, АО «ШАРД», info@shard.ru

Финансовые технологии, основанные на распределённых системах

Александр Белов
Александр Антышев



Аннотация

В настоящее время всё большую популярность приобретают исследования в области развития финансовых технологий, основанных на применении распределённых систем. Целью данной статьи является анализ современного состояния, текущих тенденций в использовании технологий блокчейна, невзаимозаменяемых токенов (NFT), децентрализованных финансов (DeFi). Рассмотрены особенности, а также преимущества и недостатки распределённых систем в области финансов. На рынок выходят новые криптовалюты, чтобы привлечь криптоинвесторов, а также разрабатываются программные инструменты, реализующие распределённые финансовые технологии. В этой связи необходимо проведение дополнительных исследований для оценки эффективности применения распределённых информационных технологий.

Ключевые слова:

распределённые системы, блокчейн, криптовалюта, технология невзаимозаменяемых токенов, технология децентрализованных финансов

Введение

В последнее десятилетие произошёл быстрый рост цифровизации финансовых рынков. Среди основных драйверов развития финансовых технологий - технология блокчейна и другие децентрализованные технологии, которые связаны, в первую очередь, с использованием распределённых баз данных, передачей данных транзакций, облачными вычислениями, криптовалютами, криптографией. В свете этих разработок блокчейн привлёк внимание исследователей, что привело к значительному увеличению количества исследований в этой области с начала 2000-х годов до наших дней. Эти исследования охватывают широкий спектр тем, иллюстрируя универсальность и актуальность технологии блокчейн в современных исследованиях. Исследования, посвящённые вопросам интеграции технологии блокчейн в сложные многоуровневые сети поставок, показали эффективность её применения для повышения прозрачности поставок и поставщиков [1]. В работах [2, 3] приведены результаты анализа факторов, определяющих намерение пользователей внедрить технологию блокчейн, исследованы настроения инвесторов по отношению к биткоину. В работе [4] рассмотрена оценка уровня доверия к технологии блокчейна в индустрии финансовых услуг. Работы [5, 6] посвящены вопросам использования смарт-контрактов для решения задач энергопотребления и управления продажами объектов недвижимости.

Рассматриваемые технологии построены на принципе распределённой обработки данных. Распределённые информационные системы (ИС) в своей основе имеют распределённую базу данных. Под распределённой базой данных (Distributed

DataBase) обычно подразумевают базу данных, включающую фрагменты из нескольких баз данных, которые располагаются на различных узлах компьютерной сети и, возможно, управляются различными СУБД. Структура распределённых ИС состоит из набора узлов, в которых расположены локальные базы данных. В распределённых ИС на узле могут выполняться локальные транзакции, а могут выполняться глобальные транзакции, захватывающие данные из БД, находящихся на разных узлах.

Формального определения распределённой вычислительной системы в настоящее время не существует. Однако распределённые системы, в основе которых лежит понятие распределённой БД, должны обладать обязательными 12 свойствами [7], главными из которых являются:

1. Управление данными на каждом из узлов распределённой системы выполняется локально.
2. Прозрачность сети: узел может обращаться к другим узлам в системе и обмениваться с ними данными.
3. Совместное использование ресурсов: в распределённой системе могут совместно использоваться оборудование, программное обеспечение или данные.
4. Параллельная обработка: одна и та же функция может выполняться одновременно несколькими компьютерами.

Перечисленные свойства распределённых систем стали основой для разработки распределённых реестров.

Распределённый реестр — технология хранения полной копии базы данных на персональном компьютере каждого участника (узла), при этом добавление новой записи происходит по достижению консенсуса между узлами (транзакция). За счёт хранения копий реестра на множестве узлов риск потери данных сводится к минимуму, в отличие от хранения данных в централизованной БД.

Область применения распределённого реестра обширна, например, в сфере заключения договоров по продаже недвижимости между юридическими лицами.

В распределённых реестрах можно выделить общие признаки, по которым их можно классифицировать. Можно выделить открытые, закрытые и гибридные реестры [8].

Открытый распределённый реестр — реестр, в котором участники не проходят идентификацию, а для участия требуется только установка специального программного обеспечения. Также отсутствует узел, выполняющий функции управления распределённым реестром, его конфигурированием и выдачей цифровых подписей. К данному виду можно отнести криптовалютные сети распределённого реестра, такие как Bitcoin, Ethereum, Litecoin и многие другие.

Закрытый распределённый реестр — данный реестр имеет ограничение на участие. Каждый из участников проходит идентификацию, в соответствии с которой получает доступ к распределённому реестру и его сервисам. В соответствии с правилами присутствует участник, отвечающий за проверку на соответствие участника определенным требованиям. В данные требования могут входить финансовые (платёжеспособность участника), а также юридические (наличие соответствующих лицензий на осуществление деятельности).

Гибридный распределённый реестр — реестр объединяет в себе свойства как открытого, так и закрытого распределённого реестра. Коммерческие структуры ориентированы в основном на гибридный или закрытый распределённый реестр. Их предпочтение связано с возможностью ограничения доступа, присутствием механизмов управления, а также контроля и надзора за участниками.

Ещё одним признаком классификации распределённых реестров является тип идентификации участника: анонимная, частичная, полная идентификация.

Распределённые реестры можно группировать и по используемому протоколу достижения консенсуса:

- **PoW (Proof of Work)** — право создания нового блока предоставляется участнику на основании выполнения им сложной вычислительной работы, которая удовлетворяет заранее определённым правилам.
- **PoS (Proof of Stake)** — право создания нового блока предоставляется владельцу счёта в том случае, если количество средств и срок владения ими соответствуют заданным критериям.
- **PoS + PoW** — гибрид PoW и PoS, условием создания нового блока является удовлетворение вычисляемым критериям

PoS и PoW-переборам. Это делается для усложнения пересчёта всей цепочки с самого первого её блока.

- **PBFT (Practical Byzantine Fault Tolerance)** — данный алгоритм основан на задаче о византийских генералах. Византийская армия была разделена на части, за каждой из которых был закреплён свой генерал. И генералам было необходимо принять коллективное решение. Часть из них голосуют за атаку, остальные за отступление. При этом решения о дальнейших действиях принимаются большинством голосов. Также принятие решения усложняется тем, что среди генералов могут быть предатели, вводящие остальных в заблуждение, чтобы в итоге было принято неверное решение.
- **Non-BFT (Non Byzantine Fault Tolerance)** — алгоритмы консенсуса, при котором некоторые его участники начинают работать против остальных.

Самым распространённым из видов распределённого реестра является блокчейн, на основе которого создана криптовалюта Bitcoin.

Блокчейн — технология построения непрерывной последовательности цепочек данных по определённым правилам. Хранение цепочек данных происходит децентрализованно в распределённом реестре на устройствах участников [9].

Обзор финансовых технологий, использующих распределённый реестр

Высокая волатильность, характеризующая рынок блокчейнов, привлекла внимание инвесторов и участников рынка на стратегии диверсификации своих активов, включая NFT, DeFi и криптовалюты [10].

Криптовалюты

При совершении транзакции участник А распространяет информацию участнику В с именами и суммой транзакции. Каждый узел добавляет данную транзакцию в свой реестр и распространяет её дальше по сети. В связи с этим возникает проблема подлинности транзакции. Для её установления используется цифровая подпись. Каждая транзакция имеет свою уникальную цифровую подпись, так как она зависит не только от пароля отправителя, но и от содержимого.

В базе данных хранится информация не о балансе, а о потраченных средствах. И для того, чтобы узнать свой баланс, нужно сложить все не потраченные средства (входы), ранее пришедшие на ваш кошелек. Из-за того, что все пользователи являются анонимными и доверия между ними нет, при первом запуске производится проверка всех транзакций в истории Bitcoin. Данная ситуация выявляет проблему нескольких транзакций, ссылающихся на один неизрасходованный вход. Временная метка не может использоваться для установки последовательности создания транзакций, так как её можно

изменить. И в итоге создаётся ситуация, когда у одной части сети зарегистрирована одна транзакция, а у второй - другая. Для её решения используется «вычислительная гонка».

Изначально транзакция заносится в массив неподтверждённых транзакций, откуда добавляется в блок с другими транзакциями и присоединяется в цепочку блокчейна. Так упорядочиваются транзакции. Для создания блока необходимо рассчитать хеш-сумму данных, входящих в блок. При этом она не должна быть больше определённого значения, для этого используется подстановка случайного значения в конец блока. Данная операция математически сложна, и поэтому одновременное включение нескольких блоков в блокчейн практически невозможно. Если же создаётся ситуация, при которой к цепочке присоединяется несколько блоков, расчёт продолжается до тех пор, пока одна из ветвей не станет длиннее другой. Блоки с короткой ветвью удаляются из блокчейна, а транзакции перемещаются в массив неподтверждённых.

Создание блока является затратным - и решившим данную математическую задачу выдаётся награда в виде биткойна, а данный процесс называется майнингом. Каждые четыре года награда за блок сокращается в четыре раза, поэтому однажды выпуск Bitcoin прекратится. Создание одного блока происходит приблизительно каждые 10 минут, а в финансовых организациях каждую секунду может обрабатываться несколько тысяч транзакций. Этот фактор сдерживает внедрение блокчейн-технологии.

Экосистема децентрализованных финансов (DeFi)

DeFi (decentralized finance) - это экосистема публичных финансовых децентрализованных приложений, разработанных на базе блокчейнов с открытым исходным кодом, поддерживающих виртуализацию для выполнения кода внутри сети. Область децентрализованных финансов появилась недавно. Она начала своё развитие вместе с запуском в 2015 году сети Ethereum, которая, в отличие от сети Bitcoin, поддерживает выполнение специального программного кода, называемого умными контрактами или смарт-контрактами, на децентрализованной виртуальной машине EVM [11]. По результатам 2021 года, исходя из отчёта инвестиционной компании Grayscale [12], на сегодняшний день сфера DeFi активно растёт и включает в себя более 50 ликвидных, публичных блокчейнов, более 500 финансовых приложений, работающих на различных сетях, а капитализация этих приложений достигла 1% от всех банковских депозитов США, что составляет 200 миллионов долларов [12].

Децентрализованные приложения, которые предоставляют финансовые услуги участникам сети, также называют протоколами. Технически, протоколы из себя представляют систему смарт-контрактов с открытым исходным кодом на одной или нескольких сетях блокчейн и веб-интерфейс для взаимодействия с этим протоколом. Протоколы предоставляют автоматизированные инструменты проведения финансовых операций между участниками сети без централизованного элемента, при этом ликвидность этих операций обеспечивается участниками сети, как и в централизованных системах, однако главное отличие в том, что в децентрализованных протоколах комиссию за обеспечение проведения операции получают именно поставщики ликвидности, а не платформа проведения этой операции. Такие системы позволяют на пря-

мую пользователю полностью обеспечивать работоспособность системы без участия бирж, банков, брокеров и других агентов. Можно выделить следующие основные категории децентрализованных приложений и их механики:

- **Биржи.** Децентрализованные биржи используют математические алгоритмы ценообразования активов, например, AMM (Automated market making) [13], для возможности их обмена между участниками сети внутри блокчейна.
- **Кредитования и займы.** Протоколы выдают займы в цифровых активах под залог других ликвидных активов, при этом контрагентами с обеих сторон выступают участники протоколов.
- **Деривативы.** Деривативные протоколы используют инструменты для получения данных вне блокчейна для создания деривативных финансовых инструментов внутри блокчейна, например, фьючерсов и опционов.
- **Управление активами.** Такой вид децентрализованных приложений предоставляет возможность автоматизации аллокации капитала пользователя между другими финансовыми протоколами для оптимизации заработка.
- **Страхование.** Протоколы страхования используют механику децентрализованных автономных организаций DAO [14] для поддержки случаев страхования внутри блокчейна. Примером такого случая может быть взлом протокола или одного его контракта с потерей средств.
- **Стейблкоины.** Особый тип цифровых активов, курс которых привязан к определённому фиатному активу, чаще всего к доллару США, и которые эмитируются под избыточный залог централизованных активов: фиатной валюты, акций компаний, других криптовалют.

Высокая волатильность, характеризующая рынок блокчейнов, привлекла внимание инвесторов и участников рынка на стратегии диверсификации своих активов, включая NFT, DeFi и криптовалюты [10]. DeFi, представляющий собой отдельный класс активов, отличный от основных криптовалют, становится всё более популярным среди пользователей [15]. В начале 2020 года с использованием технологии DeFi торговали примерно 90 тысяч пользователей, а к концу 2021 года число пользователей достигло 4,28 миллиона [16]. DeFi использует инструменты на основе блокчейна для реализации функций, связанных с банковским делом, инвестициями и торговлей, создавая надёжную структуру, которая способствует развитию альтернативной экосистемы финансовых услуг [17].

NFT – технология невзаимозаменяемых токенов

NFT (Non-Fungible Token, или невзаимозаменяемый токен) — технология, которая закрепляет право владения цифровым объектом за одним пользователем и подтверждает уникальность digital-собственности. Эта технология работает на принципах блокчейна, который записывает данные в цифровые блоки в определённом порядке. Блокчейн-информацию нельзя удалить или изменить. Блоки хранятся на разных устройствах во всём мире, а не на одном сервере. Взломать цифровой объект на блокчейне практически невозможно.

Токен - элемент блокчейна, или цифровая запись, которую можно сравнить с ценными бумагами или акциями в реальном мире. Бывают заменяемые токены, частично-взаимозаменяемые и невзаимозаменяемые (NFT).

В начале 2021 года NFT получили широкое признание как применение технологии блокчейна для торговли цифровыми произведениями искусства, виртуальными объектами и графикой. NFT предоставляют инновационные методы организации, потребления, передачи, программирования и хранения цифрового контента в различных областях, включая искусство, спорт, коммуникацию, создание контента и технологии [18, 19].

Заключение

Технология распределенного реестра очень молода и не до конца изучена. Она получила широкое распространение в криптовалюте. Не так давно появилась децентрализованная платформа на базе умных контрактов Ethereum. Многие финансовые институты, такие как Barclays, Santander, открывают исследовательские лаборатории по изучению распределённых реестров. Другие активно вкладывают деньги в стартапы с использованием распределённых реестров.

При использовании распределённого реестра можно получить ряд преимуществ по сравнению с централизованной сетью:

- непрерывное функционирование сети, бесперебойность;
- повышение прозрачности ведения реестра;
- повышение устойчивости, благодаря наличию большого количества копий реестра;
- прямое заключение сделок при проведении трансграничных операций.

Рассматриваемая технология еще не до конца изучена, и неизвестно, как она поведёт себя при использовании в больших государственных или финансовых сетях. Есть множество моментов, которые требуют более детальной проработки для её внедрения в таких организациях. Это касается её быстрого действия, а также большого объёма хранимых данных на устройствах всех её участников, которые впоследствии будут только накапливаться. Так как вся система построена на криптоключах, их утрата или раскрытие может привести к невозможным потерям.

Сейчас никаких нормативных актов, регулирующих использование распределённого реестра или ограничивающих его использование в РФ, не существует. Можно ожидать, что по мере внедрения этой технологии как в стране, так и в мире, появятся законы, регулирующие её использование.

Необходимо время для постепенного внедрения технологии распределённого реестра и изучения его пригодности для дальнейшего использования в различных сферах. ■

Список литературы:

- [1] Najjar M., Alsurakji I. H., El-Qanni A. & Nour A. I. The role of blockchain technology in the integration of sustainability practices across multi-tier supply networks: implications and potential complexities. *Journal of Sustainable Finance & Investment*, 2022, 1-19.

- [2] Afifa M. M. A., Van H. V., & Van T. L. H. Blockchain adoption in accounting by an extended UTAUT model: empirical evidence from an emerging economy. *Journal of Financial Reporting and Accounting*, 2022.
- [3] Koutmos, D. Investor sentiment and Bitcoin prices. *Review of Quantitative Finance and Accounting*, 2023, 60 (1), 1-29.
- [4] Kumari A., Devi N. C. Blockchain technology acceptance by investment professionals: a decomposed TPB model. *Journal of Financial Reporting and Accounting*, 2023, 21(1), 45-59.
- [5] Polemis M. L., Tsionas M. G. The environmental consequences of blockchain technology: A Bayesian quantile cointegration analysis for Bitcoin. *International Journal of Finance & Economics*, 2021.
- [6] Belov A., Slastnikov S. Blockchain Technology to Manage the Energy Supply of Real Estate. *Proceedings of 2021 IEEE International IoT, Electronics and Mechatronics Conference (IEMTRONICS)*. IEEE, 2021, 1-5.
- [7] C.J. Date. *An Introduction to Database Systems 6 Edition*, 1995.
- [8] Центральный банк Российской Федерации: Доклад для общественных консультаций «Развитие технологии распределённых реестров» 29.12.2017 [Электронный ресурс]// ЦБ РФ.
- [9] IBM: «Азы технологии блокчейн: введение в распределённые реестры» [Электронный ресурс]// РБК и IBM.
- [10] Karim S., Lucey B. M., Naeem M. A. & Uddin G. S. Examining the interrelatedness of NFTs, DeFi tokens and cryptocurrencies. *Finance Research Letters*, 2022, 47, 102696.
- [11] Ethereum EVM illustrated [Online]. Available: <https://takenobu-hs.github.io/downloads/ethereum-evm-illustrated.pdf>
- [12] Grayscale, David Grider, Head of Research & Matt Maximo, Research Analyst. *Decentralized Finance (DeFi)*. [Online]. Available: <https://grayscale.com/wp-content/uploads/2021/11/Grayscale-DeFi-Report-Nov2021.pdf>
- [13] Jiahua Xu, Krzysztof Paruch, Simon Cousaert, Yebo Feng, SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) Protocols. [Online]. Available: <https://arxiv.org/abs/2103.12732>
- [14] Samer Hassan, Primavera De Filippi Harvard University. *Decentralized Autonomous Organization*. *Journal of internet regulation*, 2021, 4, 2-3.
- [15] Qiao X., Zhu H., Tang Y., & Peng C. Time-frequency extreme risk spillover network of cryptocurrency coins, DeFi tokens and NFTs. *Finance Research Letters*, 2023, 51, 103489.
- [16] Makridis C. A., Fröwis M., Sridhar K., & Böhme R. The rise of decentralized cryptocurrency exchanges: Evaluating the role of airdrops and governance tokens. *Journal of Corporate Finance*, 2023, 79, 102358.
- [17] Metelski D. & Sobieraj J. *Decentralized Finance (DeFi) Projects: A Study of Key Performance Indicators in Terms of DeFi Protocols' Valuations*. *International Journal of Financial Studies*, 2022, 10(4), 108.
- [18] Krol K. & Zdonek D. Digital Assets in the Eyes of Generation Z: Perceptions, Outlooks, Concerns. *JRFM*, 2022, 16(1), 1-14.
- [19] Wilkoff S. & Yildiz S. The behavior and determinants of illiquidity in the non-fungible tokens (NFTs) market. *Global Finance Journal*, 2023, 55, 100782.

Об авторах

Александр Владимирович Белов, профессор, руководитель Департамента прикладной математики МИЭМ НИУ ВШЭ, avbelov@hse.ru

Александр Александрович Антышев, ведущий научный сотрудник ФКУ НПО «СТИС» МВД России, a166aa@yandex.ru

К вопросу о кибербезопасности цифровых валют центральных банков

Павел Мизинов

Наталья Коннова



Аннотация

Разработка и внедрение цифровой валюты центрального банка (ЦВЦБ) – событие, глобально меняющее правила игры в финансовом мире, и одна из самых обсуждаемых инноваций за последние 5-7 лет. Новый тип денег, возникший как итог цифровой трансформации общества и представляющий собой цифровой код, очаровывает и пугает одновременно. Как и любое глобальное нововведение, внедрение ЦВЦБ несёт за собой и новые риски. В статье рассматриваются предпосылки и причины создания данного продукта, а также актуальные вопросы кибербезопасности.

Ключевые слова:

ЦВЦБ, цифровизация, кибербезопасность, киберриск, криптовалюта

Вместо введения

Один из моих жизненных Учителей – д.т.н., д.ист.н., проф. Тормозов Виктор Тимофеевич – на любую горячую научно-популярную новость, принесённую мною, зелёным студентом, из просторов Интернета, реагировал преспокойно и в зависимости от ситуации отвечал: «Не новость, концепция этого уже давно описана в мировой литературе», – или: «Не новость, подобное мы создали в лаборатории закрытого НИИ ещё в 60-х». Через несколько дней, встретив меня в коридорах альма-матер или на кафедре, он из глубин своего рыжего кожаного портфеля нарочито артистично извлекал зачитанный том очередного литературного шедевра и, со словами «Прошу ознакомиться», вручал мне. И я с большим удовольствием читал и каждый раз убеждался в его правоте: все принесённые мною из Сети новости, идеи и концепции почти всех великих научных достижений человечества уже давно описаны в классике мировой фантастики.

Такой сценарий повторялся много-много раз. Я приносил распечатанную подборку новостей, он мне – книгу. С его лёгкой руки я с новой стороны открыл для себя Стругацких и Азимова, познакомился с творчеством Ефремова и Замятина. Эти книги, как по мановению волшебной палочки появившиеся из портфеля, привили мне любовь к жанрам научно-популярной и фантастической литературы на всю жизнь. От него же я перенял культуру ведения заметок – выписывать из книги наиболее значимые части текста и цитаты в отдельный блокнот. Книги перечитываются редко, а заметки позволяют восстановить полную картину со-держимого. Через какое-то время я стал замечать удивительную вещь: читая в Сети или обсуждая с единомышленниками новости о прорывных достижениях современной науки, я быстро находил параллели из научной фантастики и уже сам с видом именитого профессора мог произнести фразу: «Не новость, концепция этого уже давно описана в мировой литературе».

В 2008 году мне в руки попал роман американского писателя, крёстного отца жанра киберпанк в литературе, Брюса Стерлинга (Bruce Sterling) под названием «Бич небесный». Подробности сюжета не имеют значения в контексте данной статьи, но один момент вызвал у меня неподдельный интерес и надолго осел памяти. Приведу его дословно по тексту [1, с. 230]:

«Алекс не видел ничего удивительного в том, что такие сообщества, как китайская Триада или корсиканская Чёрная Рука, печатают собственные деньги в электронном эквиваленте. Он просто принимал это: существование электронных частных валют, за которыми не стояло никакое правительство, неотслеживаемых, полностью анонимных, доступных по всему миру, молниеносных по скорости, вездесущих, взаимозаменяемых и, как правило, чрезвычайно неустойчивых». В то время я работал в отделе информационной безопасности одного из коммерческих банков, и данное описание, как у банковского служащего, вызвало долю здорового скептицизма: «А как проводится эмиссия?», «А кто устанавливает обменный курс?», «А кто исполняет роль регулятора?», «А каким законодательством эмиссия и оборот регулируются?» Признаться честно, сама идея выпуска надгосударственного средства платежа, да ещё разными частными группами, общепризнанная, да вдобавок никем не регулируемая, показалась мне достаточно слабым ходом писателя – уж больно нереалистично. Но время всё расставит по своим местам.

¹ англ. Alex did not find it surprising that people like the Chinese Triads and the Corsican Black Hand were electronically minting their own cash. He simply accepted it: electronic, private cash, unbacked by any government, untraceable, completely anonymous, global in reach, lightninglike in speed, ubiquitous, fungible, and usually highly volatile [2, с. 186].

Примерно через год в курилке офиса ко мне подошёл (скорее подлетел) мой однокашник по университету Витя и сходу начал интересоваться моим мнением про новорождённый продукт Bitcoin. Говоря откровенно, к тому времени я ни о каком Bitcoin даже близко не слышал, поэтому не мог ответить на поставленный вопрос ровным счётом ничего. Витька же был, есть и останется навсегда компьютерным гиком и романтиком-шифропанком, проводящим ночи перед монитором в IRC и Reddit-e. Он вкратце донёс до меня основные догмы криптоанархизма, одной из которых было применение не отслеживаемого и не контролируемого государством средства платежа. Далее он рассказал, что теоретически анонимную цифровую валюту уже придумали лет 10 как, а реализовали в «железе и коде» только сейчас. Теперь стали реальностью кроссграничные анонимные транзакции, осуществляемые без контроля со стороны государственных регуляторов. Мечта шифропанков была реализована неизвестным ранее программистом Сатоши Накамото (Satoshi Nakamoto)!

Я слушал товарища и ловил себя на мысли, что где-то о такой концепции я уже слышал. Через несколько дней, листая свою записную книгу с выписками из прочтённой литературы, я наткнулся на заметки, сделанные из того самого произведения «Бич небесный». Хотя сам фрагмент я из главы не выписывал, благодаря другим записям я быстро восстановил в памяти, откуда мне известно о применении цифровых валют. Мне стало ужасно любопытно, когда же автор романа описал данную технологию. Немного погуглив, я нашёл сведения о первом англоязычном издании произведения: это был 1994 год, т.е. за 15 лет до воплощения идеи в жизнь. Я улыбнулся, добрым словом вспоминая своего Учителя, и произнёс его коронную фразу: «Не новость, концепция этого уже давно описана в мировой литературе». Я прочёл большое количество sci-fi-произведений, написанных отечественными и зарубежными писателями за XX век, но нигде более о цифровых валютах упоминаний не находил.

Мог ли я предположить, что идею и концепцию криптовалюты (читай – идеи криптоанархистов) в 20-е годы XXI века возьмут на вооружение государства? Что эмиссия цифровых валют будет производиться центральными банками? Пятнадцать лет назад я бы ответил отрицательно, но время расставило всё по своим местам.

В данной статье мы поговорим о цифровых валютах центральных банков, о перспективе их применения и связанных с ними киберугрозах.

Что такое цифровая валюта центрального банка

Мы не будем рассматривать краткий теоретический курс по криптовалютам, их разновидностям и технологии их эмиссии. Об этом сказано и написано за последние 15 лет невероятное количество материала. Их феномен безусловен: менее чем за 10 лет данная технология прошла путь от «суррогатной валюты» до сверхпопулярного средства инвестирования. Хотя игнорировать очевидный факт угрозы национальному экономическому суверенитету любой страны со стороны данной

технологии было бы нелепо, востребованность криптовалюты, а также скорость и глубина её проникновения сделали бесполезными попытки правительств некоторых государств добиться полного запрета на майнинг и обращение. Более того, мировой тренд на всеобщую цифровизацию и лавинообразный рост популярности анонимных децентрализованных валют привёл к необходимости введения в правовое поле государств таких понятий, как «цифровой финансовый актив» и «цифровая валюта», а затем к активному обсуждению создания цифровых валют центральных банков. Всё согласно классической английской идиоме: если не можете победить их, присоединяйтесь к ним².

На наш взгляд, такой сценарий развития событий был закономерен: несмотря на явно антигосударственный (скорее антинадзорный) подтекст идеи виртуальных денег, отрицать эффективность самой бизнес-модели было бы нерациональным. *Весьма интересен факт того, как быстро центральные банки смогли адаптировать технологии «финансовых пирамид» на благо государства и запустить цифровую разновидность национальных валют. Однако с существенным отличием от криптовалюты – цифровой вариант фиатных денег эмитируется государством и обеспечен золотовалютными резервами, а хранение организовано на специализированной платформе, разработанной центральным банком, что делает цифровые деньги третьей формой валюты государства, помимо традиционных бумажных и электронных.*

Если на первоначальном этапе создание ЦВЦБ рассматривалось как следование модной тенденции и провозглашалось центральными банками на уровне «декларации о намерениях», то на сегодняшний день цифровые деньги являются инновационным драйвером для всей индустрии. На это есть несколько причин.

Предтечей к популяризации криптовалют послужил глобальный финансовый кризис 2007–2009 годов, изменивший ландшафт общемировой финансовой системы и подорвавший доверие ко всему банковскому сектору. Клиенты, потерявшие сбережения, искали альтернативы, поэтому предложенная Сатоши Накамото [4] одноранговая система электронных денег, позволяющая хранить накопления и осуществлять платежи, не опираясь на традиционную банковскую систему и государственный контроль, моментально вызвала к себе интерес. Концепция оказалась настолько удачной, что очередной тип альткойна стал появляться чуть ли не каждую неделю, и на октябрь 2024 года насчитывается 9840 [5] разновидностей криптовалюты. Аномальный успех криптовалютных технологий стал первым шагом к появлению ЦВЦБ. В авангарде интереса к технологии на государственном уровне стоял Народный банк Китая (НБК), где в 2014 году была создана целевая группа по изучению цифровой фиатной валюты. Через два года, в 2016 году, на базе НБК создаётся Институт цифровой валюты, разрабатывающий концепцию цифровой фиатной валюты Китая, а уже в 2017 начинается пилотный проект по ограниченному тестированию обращения цифрового юаня [6].

Вторым шагом стала пандемия COVID-19 и связанные с ней локальные и национальные блокировки. Меры социальной изоляции, закрытие границ и карантины послужили катализатором для многих компаний в кратчайшие сроки адаптировать свои

² англ. If you can't beat 'em, join 'em [3]

бизнес-модели к новым реалиям, ускоряя внедрение передовых технологий и цифровых платформ для облегчения удалённой работы и онлайн-покупок. Эпидемия запустила процесс тектонических изменений: глобальную цифровую трансформацию бизнеса и формирование цифрового общества. Шведский экономист Тэд Саарико (Ted Saarikko) дал, по нашему мнению, наиболее ёмкое определение цифровизации как «социотехнического процесса использования оцифрованных продуктов или систем для разработки новых организационных процедур, бизнес-моделей или коммерческих предложений³». Наиболее ярким примером, иллюстрирующим образец полного цикла цифровой трансформации, являются сервисы предоставления цифровых государственных и муниципальных услуг в России.

Третий шаг относится к вопросу финансового и технологического суверенитета стран. Одним из ярчайших примеров является показательное отключение российских банков от международной системы обмена межбанковскими сообщениями SWIFT, что, по мнению оппонентов, должно было лишить Россию доступа к международным рынкам экспорта и импорта и повлечь за собой невосполнимые потери для российской экономики. Стоит отметить, что система SWIFT была разработана в 1973 году Федеральной резервной системой США и Банком Англии при участии консорциума американских и европейских банков. И хотя формально система считается международной, существующей на взносы стран-участниц, «правила игры» диктуются ограниченным кругом. Поэтому вопрос отключения от системы носит политический характер.

Возможность беспрепятственно осуществлять импорт или экспорт, иметь свободный доступ к мировым рынкам — вопрос безопасности государства, цена которому — существование государства как суверенного образования.

В сложившихся обстоятельствах, чтобы защитить себя от политически ангажированных ограничений в финансовой сфере, правительства стран стали задумываться о создании инструментов международной торговли, лишённых подобных ограничений. Наиболее удачными в плане реализации безопасности платежей и защищённости от внешнего воздействия оказались криптовалютные технологии, идеи которых и легли в основу создаваемых цифровых денег.

Основные виды киберугроз для ЦВЦБ

Ввиду отсутствия сценариев реального широкомасштабного внедрения ЦВЦБ в оборот, говорить о рисках для цифровых денег в киберпространстве мы можем только потенциально. Но уже совершенно ясно, что они включают как все известные риски для платёжных систем, так и пул уникальных рисков, присущих исключительно ЦВЦБ.

Внедрение ЦВЦБ связано с целым рядом новых технических и операционных аспектов, которые не применимы к существующим

платёжным системам. К ним относятся использование цифровых инструментов для управления жизненным циклом валюты, использование смарт-контрактов для автоматизации исполнения платёжных сценариев и эффективного перевода средств, а также работа в онлайн- и офлайн-режимах для поддержания непрерывности обслуживания. Данные технологии и создают уникальные виды киберрисков, присущих ЦВЦБ.

Однако, будучи платёжным инструментом, ЦВЦБ также подвержены рискам, характерным для продуктов в цифровой форме (цифровым рискам), и рискам, относящимся к платёжным системам.

Часто в профильной литературе выражения «цифровой риск» и «киберриск» используют в качестве синонимов. Но несмотря на то, что понятия действительно очень схожи, суть этих терминов различна. Цифровой риск связан именно с рисками, присущими цифровым продуктам, услугам и вспомогательным процессам, т.е. в понятие вкладываются все непредвиденные последствия, которые возникают в результате цифровой трансформации и нарушают достижение бизнес-целей. Под киберриском понимается риск, связанный с киберугрозами, исходящими из внешней киберсреды. И хотя некоторые виды угроз можно классифицировать по двум типам (например, действия инсайдера или фишинг), важно понимать различия в контексте.

Итак, цифровые риски включают в себя широкий спектр угроз и уязвимостей, связанных с использованием цифровых технологий и цифровой трансформации. Они возникают на стыке деятельности людей, процессов, технологий и данных, как внутри организации, так и в цепочке её контрагентов. Давайте разберём каждый вид рисков в отдельности.

Риски, обусловленные человеческим фактором, относятся, в первую очередь, к рискам, связанным с преднамеренными или непреднамеренными действиями (либо бездействием) сотрудников компании или организаций-партнёров (контрагентов). Для понимания рассмотрим несколько примеров.

- Действия инсайдера. Преднамеренные деструктивные действия легитимного пользователя компании, обладающего глубокими знаниями о бизнес-процессах и наделённого привилегированным доступом к информационным системам. Такой тип злоумышленника может действовать как самостоятельно, так и в составе организованной группы.
- Высокорисковыми бывают и непреднамеренные деструктивные действия легитимного пользователя компании. Например, когда программист, сопровождающий систему, использует сторонний исходный код, позаимствованный на сервисах совместной разработки типа github/gitlab, без проверки на наличие уязвимостей, который в дальнейшем эксплуатируется злоумышленниками как точка входа в систему.
- Примером бездействия легитимного пользователя, приведшего к успешной кибератаке, является сценарий, когда системный администратор или администратор безопасности осознанно или непреднамеренно игнорирует установку критических обновлений от угрозы нулевого дня, тем самым оставляя систему уязвимой.

³ англ. the sociotechnical process of leveraging digitized products or systems to develop new organizational procedures, business models, or commercial offerings [7]

- Риск утечки данных или неправомерного раскрытия информации возникает, например, при некорректной настройке прав доступа в иерархии каталогов или внутри информационной системы, в этом случае возможно получение административных полномочий непривилегированным пользователем или получение доступа к конфиденциальной информации работником сторонней организации, выполняющим работы по договору.
- К человеческому фактору относят и так называемый риск ключевого лица⁴, когда, например, администрирование всей системы осуществляется одним человеком, часто с совмещением роли администратора информационной безопасности, при этом со стороны менеджмента не предусматривается замещающий сотрудник, отсутствует культура преемственности или передачи знаний. Уход ключевого сотрудника приводит к коллапсу управления системой либо множественным ошибкам в настройках системы при работе другого сотрудника «вслепую».

Риски, связанные с человеческим фактором, являются наиболее значимыми, т.к. через их реализацию осуществляется более 80% от известных кибератак [8].

Процессные риски — это вероятность критического исхода процесса при наличии неблагоприятных факторов, влияющих на выполнение процесса [9]. Иллюстрацией может послужить случай параллельного внедрения двух информационных продуктов в одной компании двумя разными подрядными организациями под контролем администраторов компании-заказчика. При этом происходит перенастройка политик безопасности и механизмов защиты. Для тестирования производительности многие ключевые аспекты кибербезопасности игнорируются: запуск программ осуществляется с повышенными привилегиями, пользовательские учётные записи наделяются административными полномочиями, изменяются политики антивирусной защиты, резервное копирование не производится и прочее. Учитывая требование заказчика по непрерывности основного бизнес-процесса (установка не должна влиять на основную работу), исполнители работ настаивают на предоставлении максимальных полномочий их программному обеспечению с последующим понижением порога доступа. В результате таких работ часто «уровень доступа» для технологии понизить забывают, а в пользователях Active Directory остаётся несколько тестовых административных учётных записей. В итоге внедрение программного комплекса осуществлено успешно и в срок, а киберзащищённость инфраструктуры нанесён существенный ущерб. Всё как в классическом монологе Аркадия Райкина «Кто шил костюм?».

Технологические риски понимаются по-разному не только в различных областях, но и в рамках одной области техники [10]. В нашем случае под технологическим риском будем понимать прежде всего угрозы и уязвимости, связанные с внедрением, эксплуатацией и обслуживанием технологических систем, вспомогательной инфраструктуры в процессе цифровой трансформации. Данный вид рисков связан с угрозами целостности, доступности и производительности технологических активов, а также конфиденциальности данных и информации, которые «циркулируют» внутри них или производятся ими. Примерами технологических рисков являются отказы или неисправности

оборудования, ошибки или сбои в работе программного обеспечения, перебои в работе сети, плохая совместимость между различными технологическими компонентами и снижение производительности из-за плохой масштабируемости.

Риски, связанные с контрагентами, — это риски, связанные с чрезмерной зависимостью от продукции или услуг компаний-контрагентов. Это может привести к:

а) риску «концентрации», когда целевая компания одна или совместно с другими партнёрами зависит от услуг одного поставщика. В этом случае резкое прекращение деятельности поставщика услуг (или форс-мажор) полностью парализует на неопределённый срок работу как целевой компании, так и связанных с ней партнёров;

б) ситуации, когда уровень обеспечения кибербезопасности в подрядных организациях может быть на порядок ниже, чем в целевой компании. Учитывая, что очень часто встречаются случаи частичной интеграции информационной системы целевой компании и контрагентов, киберустойчивость всей инфраструктуры будет зависеть от уровня защищённости инфраструктуры компании-контрагента. Надёжность всей цепи определяется самым слабым звеном.

Киберриск так же, как и цифровой, может быть источником или следствием сбоя процессов, применяемых технологий или ошибки человека. Периметр киберрисков ЦВЦБ состоит из трёх основных элементов. Первый — это сама валюта на протяжении всего её жизненного цикла: создание, хранение, распространение и уничтожение. Второй — транзакции между физическими лицами или организациями. Третий элемент связан с конфиденциальной информацией, которую ЦВЦБ собирает с пользователей, организаций и проведённых транзакций. Эта информация должна быть защищена как во время «транспортировки», так и в состоянии «покоя» ЦВЦБ.

ЦВЦБ могут подвергаться уникальным киберрискам, которые не обязательно встречаются у других видов цифровых денег. Помимо персонала, проходящих процессов и применяемых технологий в центральном банке и в финансовом секторе, устойчивость и безопасность цифровых платёжных систем в значительной степени зависят от основной технологической инфраструктуры страны. Сюда входят такие критически важные услуги, как постоянное энергоснабжение, стабильность, безопасность и доступность широкополосного доступа в Интернет, а также глубокое географическое проникновение мобильной 4G+ сети.

Рассмотрим примеры киберрисков и проблемы безопасности, которые потенциально могут быть выявлены при эксплуатации ЦВЦБ. Рассуждать о них мы можем только гипотетически, т.к. на сегодняшний день ни одна из 130 стран-эмитентов ЦВЦБ не раскрыла подробностей архитектуры своего решения.

Дизайн ЦВЦБ: счёт или токен

Модели ЦВЦБ, основанные на счетах, предполагают электронное хранение средств на пользовательском счёте и используют дебетовые и кредитные методы для обеспечения мгновенных переводов. Это напоминает традиционные банковские счета и электронные платежи. В данной модели ключевой

⁴ англ. key person risk

областью защиты является идентификация пользователя, которая может быть достигнута с помощью паролей, биометрических данных или комбинации подобных средств.

В токенизированном варианте ЦВЦБ токены выпускаются центральным банком и передаются по распределённым реестрам для проведения платёжных операций. Такой вариант сродни хранению банкнот и монет в физическом кошельке, который гарантирует, что деньги принадлежат вам. Как и наличные деньги, токены легче доступны и обеспечивают некоторый «контролируемый» уровень анонимности. Ключевым фактором риска для систем рассматриваемого типа является защита цифрового токена на протяжении всего его жизненного цикла. Каждый токен уникально идентифицируется с помощью криптографических механизмов, таких как цифровые подписи и шифрование с открытым ключом. Закрытые ключи используются в момент выпуска для обеспечения подлинности и уникальности токенов, а открытые ключи — для проверки в момент использования.

Ключевые проблемы данного дизайна ЦВЦБ:

- возможная компрометация криптографических ключей, цифровых подписей и других криптографических алгоритмов, используемых для аутентификации и авторизации;
- «угроза квантовых вычислений» — бурно обсуждаемая потенциальная угроза для криптографии, используемой для защиты цифровых активов. Закрытые ключи на эллиптической кривой потенциально могут быть вычислены злоумышленниками при помощи квантовых алгоритмов с использованием открытых ключей, что поставит под угрозу безопасность хранения ЦВЦБ.

Механизмы технической реализации ЦВЦБ

Целостность платежей и денежных переводов требует ведения записей о транзакциях и балансах пользователей. Аналогичным образом, в основе системы ЦВЦБ должна лежать цифровая запись всех проведённых транзакций. Цифровой реестр может быть реализован с помощью обычного централизованного реестра, контролируемого центральным банком, или децентрализованного реестра без единого центрального пункта управления. Независимо от степени централизации, цифровой реестр должен обеспечивать уверенность в том, что осуществлённая транзакция поддаётся проверке.

Централизованное решение является эффективным и зрелым, «заточенным» на работу с большим объёмом платежей. Решения или средства контроля, позволяющие преодолевать неожиданные сбои, ошибки и нарушения в работе системы, прошли проверку временем и продолжают совершенствоваться с учётом новейших технологий и угроз. Однако централизация — «хранение всех яиц в одной корзине» — несёт в себе большое количество угроз.

- Централизованные реестры являются привлекательной целью для хакеров и представляют собой «единую точку

отказа», поскольку успешная атака может вывести из строя всю систему и привести к утечке данных всех клиентов в результате одной атаки. В случае применения реплицированных баз данных атака с использованием вируса-вымогателя⁵ может одновременно затронуть все работающие и резервные системы, что затруднит восстановление.

- Мотивированный инсайдер, имеющий привилегированный доступ к централизованному реестру, может вносить трудно обнаруживаемые несанкционированные изменения в транзакции, конфигурации систем или протоколы связи, что приведёт к крахам и сбоям в работе.
- Масштабное отключение электроэнергии или доступа в Интернет может одновременно затронуть производственные и резервные серверы.

Другой вариант технической реализации ЦВЦБ — использование технологии распределённых реестров (DLT). Объектом учёта в распределённых реестрах является токен. Такие технологии обеспечивают большую устойчивость через распределённую систему узлов (нод), а также автоматизацию исполнения контрактов (так называемые смарт-контракты). При этом производительность данной технологии ниже централизованной системы. Тем не менее, архитектура распределённого реестра за счёт распределённого хранения и обработки информации более устойчива к различным инцидентам по сравнению с централизованными системами. Несмотря на существенные плюсы, данной технической реализации присущи следующие риски.

- DLT — относительно новая технология, которая не тестировалась в масштабах национальной платёжной системы, поэтому её уязвимости и недостатки архитектуры не до конца изучены. Это затрудняет прогнозирование угроз и разработку превентивных мер защиты.
- Особенности архитектуры DLT делают её уязвимой для DDoS-атаки и для «атаки 51%», при которой один пользователь или группа контролирует половину вычислительной мощности сети.
- DLT широко использует смарт-контракты. Злонамеренный или вызванный ошибками сбой в сценарии может поставить под угрозу целостность всей сети.

Проблемы смарт-контрактов

Одной из сильных сторон технологии DLT является возможность применения при сделке смарт-контрактов — специфических программируемых сервисов, которые автоматически выполняются при выполнении оговорённых в них условий. Данные сценарии используют для автоматизации выполнения соглашения, чтобы все участники могли быть немедленно уверены в результате, без участия посредника или потери времени. Однако при применении таких сценариев возникает ряд киберрисков, например:

- по своей сути смарт-контракт является программным кодом, который можно случайно или намеренно изменить,

⁵ англ. ransomware attack

поменять логику работы, спровоцировать запуск цепочки контрактов, в коде могут содержаться ошибки, приводящие к ненадлежащему исполнению сценария или сбою в работе;

- преднамеренное манипулирование контрактами, когда «атакующий» контракт может манипулировать контрактом «жертвы», что может привести к серьёзному ущербу, если результат последнего является входом или триггером для множества других контрактов.

Отдельной проблемой является использование ЦВЦБ в **автономном режиме, без подключения к сети Интернет**. Планируется, что офлайн-перевод может выполняться с использованием технологии беспроводной передачи данных малого радиуса действия (Bluetooth, NFC), поэтому в качестве носителя офлайн-кошелька рассматривается в первую очередь обычный смартфон. Пополнение автономного кошелька производится со счёта клиента при условии наличия доступа в Интернет, т.е. сначала ЦВЦБ переводится с онлайн-счёта на офлайн, а затем становится возможным осуществлять C2C-, C2B-, B2C-операции при помощи офлайн-переводов. Однако использование автономного режима несёт в себе ряд новых рисков.

- Риск двойного расходования средств. Возможность списания одной и той же суммы более одного раза или сверх доступного баланса в случае взлома или неисправности устройства, использующегося в офлайн-режиме. Скомпрометированное устройство может превратиться в «печатный станок» и начать генерировать такие транзакции, которые только позже, в результате сверки, будут признаны недействительными. Тут сразу вспоминается «неразменный пятак» из бессмертной повести братьев Стругацких.
- Потеря смартфона для офлайн-кошелька означает то же самое, что потеря портмоне с наличными деньгами: денежные средства будут утеряны.
- Кроме этого, попадание устройства в руки злоумышленников открывает возможность получения доступа к офлайн-транзакциям, защищённым криптографией. При должной подготовке и наличии технической оснащённости данные транзакции могут быть подвергнуты обратной разработке, последующей расшифровке с целью осуществления генерации поддельных транзакций. Защищённость самого устройства выходит на первый план.

Как видно из далеко не полного обзора цифровых и киберрисков, присущих ЦВЦБ, развитие и масштабирование технологий, связанных с данным видом денег, находится ещё на довольно ранней стадии. Центральные банки имеют большой опыт в управлении жизненным циклом фиатной валюты. Разработан и внедрён многоуровневый контроль, охватывающий технологии, людей, процессы и объекты. Однако управление жизненным циклом цифровой валюты — это новая территория (terra incognita), которая требует киберзащиты с помощью новых технологических инструментов, процессов и иного типа управления. Материализация киберрисков в системе ЦВЦБ может иметь далеко идущие последствия. Любой сбой в обслуживании, потеря средств, компрометация или утечка конфиденциальных данных приведёт к репутационному ущербу для центрального банка и подрыву доверия потребителей.

Заключение

В данной статье нами рассмотрен процесс зарождения и развития новой формы фиатных денег — цифровой валюты, эмитируемой центральным банком. Нами разобран широкий спектр цифровых и киберрисков, присущих новой валюте. Показано, что становление ЦВЦБ находится только на стадии тестирования. Цифровизация валюты — глобальный шаг в развитии государства, не терпящий поспешных решений, эффект от подготовленного применения которого сделает нас на шаг ближе к полноценному цифровому обществу. Однако очередной шаг в «цифру» поднимает новый пласт философских проблем: оцифровка предоставляет огромную свободу и пространство для творчества и расширения человеческих возможностей, в то время как обратной стороной этой свободы является усиление контроля, что отталкивает от идей цифровизации большое количество людей. Поэтому параллельно цифровой трансформации общества должна идти мощнейшая волна обучения цифровой и финансовой грамотности.

Мы являемся современниками удивительной трансформации общества, перехода на новую ступень его развития. И хочется верить, что создаваемое сегодня «прекрасное далёко» будет действительно прекрасным. ■

Список литературы:

- [1] Стерлинг Брюс. «Бич небесный» [пер. с англ. Вл. Иванова]. М. : ЭКСМО, 2007, 448 с. ISBN 978-5-699-24397-6
- [2] Sterling, Bruce. Heavy weather. New York : Bantam Books, 310 p, ISBN 0-553-09393-2
- [3] Электронная версия Кембриджского словаря. <https://dictionary.cambridge.org/dictionary/english/if-you-can-t-beat-em-join-em> (дата обращения: 09.10.2024)
- [4] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. <https://bitcoin.org/bitcoin.pdf>
- [5] <http://https://coinmarketcap.com/> (дата обращения: 09.10.2024)
- [6] Working Group on E-CNY Research. Progress of research & development of E-CNY in China <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021072014364791207.pdf> (дата обращения: 10.10.2024).
- [7] Saarikko T., Westergren U. H., Blomquist T. Digital transformation: Five recommendations for the digitally conscious firm // Bus. Horiz. 2020. T. 63. № 6. С. 825–839.
- [8] Human error drives most cyber incidents. Could AI help? // Harv. Bus. Rev. 2023. Режим доступа: <https://hbr.org> (дата обращения: 14.10.2024)
- [9] Управление процессными рисками. <https://www.processinform.ru/risk.html> (дата обращения: 18.10.2024)
- [10] Горохов В.Г., Сюнтюренко О.В. «Технологические риски: информационные аспекты безопасности общества» // Программные системы и вычислительные методы. 2013. Т. 4. № 4. С. 344–353.

Об авторах

Коннова Наталья Сергеевна — доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (105005, Российская Федерация, Москва, 2-я Бауманская ул., д. 5, стр. 1) SPIN-код: 3672-6670

Мизинев Павел Владимирович — аспирант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (105005, Российская Федерация, Москва, 2-я Бауманская ул., д. 5, стр. 1) SPIN-код: 5388-1348

Повторение – мать учения, или Конференция TLDCON 2024 (5-6 сентября 2024, Минск)

Павел Храмцов



Аннотация

На конференции TLDCON 2024 в Минске были впервые в основной сетке докладов представлены выпускные студенческие работы. Речь идёт о полноценных исследованиях и разработках перспективных программных инструментов исследований инфраструктуры Интернета. Полученные результаты вызвали неподдельный интерес у участников конференции. Организаторы планируют в рамках следующей конференции TLDCON 2025 организовать отдельную секцию студенческих работ.

Ключевые слова:

TLDCON 2025, информационная инфраструктура Интернета, резолвер, краулер, программное обеспечение, исследования

В этом году сентябрь в Минске выдался тёплым и сухим. По Свислочи тянулись караваны сап-бордов. Около Центра водных видов спорта дети гоняли на шверботах класса «Оптимист». По набережной вдоль реки прогуливается молодежь и рассекают велосипедисты. И неожиданно там же на четвереньках, меж ног и колёс, скачут две девчушки-квадробера, изображая кошку и собачку. Это новое помешательство не обошло стороной и столицу Белоруссии.

Новые веяния, возможно, пришли ненадолго, а вот старые добрые традиции проведения отраслевых конференций в сентябре, к счастью, продолжают. В тёплой и радушной обстановке с 5 по 6 сентября 2024 в Минске в отеле «Марриотт» проходила традиционная 17-я Международная конференция администраторов и регистраторов национальных доменов верхнего уровня стран СНГ, Центральной и Восточной Европы (TLDCON 2024).

Каждый год в доменной индустрии проходит несколько десятков международных семинаров и конференций по всему миру. Это три глобальных конференции ICANN (general, community, policy), несколько форумов DNS и множество конференций региональных сообществ регистратур, регистраторов и технических специалистов.

Российские представители продолжают активно в них участвовать. Издержки от участия в этих мероприятиях существенно увеличились, но это не означает, что наши специалисты выпали из общего потока событий и «отбились»/«отстали» от общемировых трендов.

TLDCON 2024 отличали два важных обстоятельства: эта конференция была организована и проведена в гибридном

формате, причём преимущественно с офлайн-участием, и впервые в основной сетке конференции в ходе секции «Исследования и их результаты» были представлены студенческие работы, выполненные в рамках сотрудничества Фонда развития сетевых технологий «ИнДата» и Московского института электроники и математики им. А.Н. Тихонова Национального исследовательского университета «Высшая школа экономики» (МИЭМ НИУ ВШЭ).

Справедливости ради стоит заметить, что сотрудничество конференции TLDCON с высшей школой началось не в Минске. Первые мастер-классы для студентов участники конференции провели в 2023 году на TLDCON 2023 в Петрозаводске. Но вот полноценное участие студентов и выпускников вузов в основной программе конференции – выступления с докладами – случилось впервые в Минске.

У организаторов, Координационного центра доменов .RU/.РФ, были обоснованные сомнения в успехе такой затеи, но, забегаю вперед, скажу, что всё получилось, и есть высокая вероятность того, что на TLDCON 2025 в программе может появиться самостоятельная студенческая секция.

С моей точки зрения, это не совсем правильно, т.к. «намекает», что есть «настоящие» исследования, а есть «студенческие». Это понижает статус «студенческих» работ. Результат и практическое значение работы, по большому счёту, не зависит от того, кто её выполнил – студент, аспирант, преподаватель или отраслевой специалист.

Чтобы не быть голословным, представлю сами работы, о которых было доложено в рамках конференции.

«Использование DNS-резолверов»

Анна Подгук исследовала проблему использования DNS-резолверов конечными клиентами интернет-провайдеров. Прежде чем углубиться в обсуждение презентации результатов, хотелось бы остановиться на значимости и актуальности самой проблемы.

Начнем со значимости. Есть такое словосочетание «Internet governance». Его часто у нас переводят, как «управление Интернетом». Я думаю, что это не совсем точно. Точнее, совсем не точно. На мой взгляд, в данном контексте речь идёт не об управлении, а о регламентировании: техническом, организационном, административном и т.п... При этом упор делается на общественные объединения (communities). Однако перевод устоявшийся, и даже ежегодную всемирную конференцию IGF принято называть Форумом по управлению Интернетом.

На сайте <https://www.internetgovernance.org/> есть шкала развития процесса «управления» (Рис. 1).

Большинство событий на этой шкале связано с организациями, которые занимаются распределением уникальных идентификаторов (адресов, доменных имён, номеров), т.е. в более широком смысле выполняют IANA-функции.

Если принять за основу широко распространённое мнение, что доменные имена являются «человеческим» интерфейсом в мир номеров Интернета, то надёжность, доступность, безопасность поиска соответствий между именем и номером является ключевой проблемой «управления» Интернетом.

Система доменных имен (DNS) – это распределённая иерархическая информационная система, хранящая данные в виде соответствия «ключ/значение». Ключ – это доменное имя, а значение – всё что угодно, в том числе: номера, адреса, дру-

гие имена и даже правила преобразования ключей. Наиболее известным соответствием, в контексте которого упоминается DNS, является соответствие «доменное имя/IP-адрес».

В качестве распределённой СУБД в этой системе используются авторитетные серверы доменных имён, а в качестве инструмента поиска – кеширующие рекурсивные DNS-резолверы или просто – резолверы.

Ещё раз обращаю внимание на то, что под «управлением» Интернетом чаще всего понимают распределение ограниченного ресурса – имён, адресов, номеров и т.п. Но поиск во всём этом многообразии не менее важен.

Долгое время конечный пользователь осуществлял поиск в DNS только с помощью резолверов провайдеров подключения к Интернету. Это было просто, логично и понятно. Адрес резолвера устройство конечного пользователя получало в момент подключения к Сети вместе с IP-адресом для этого устройства и IP-адресом шлюза, через который осуществляется доступ.

В этой схеме подключения всё понятно и всё прозрачно. Но сначала начали шифровать трафик, чтобы нельзя было посмотреть, что передаётся от ресурса конечному пользователю, а в итоге «докатались» до инкапсуляции DNS-запросов в HTTPS, чтобы было нельзя посмотреть, куда обращается конечный пользователь для получения зашифрованного трафика.

В этой конспирологической атмосфере (приватность, приватность и ещё раз приватность!) появились резолверы, которые не связаны с провайдерами доступа. Наиболее известные из них – это Google DNS, Amazon 53, Yandex DNS, CloudFlare DNS, Quad9, OpenDNS и другие.

Впрочем, не стоит слепо верить в то, что «хорошие ребята» из Google из-за альтруизма помогают всем нам бороться с «плохими парнями». Достаточно поглядеть в логи автори-

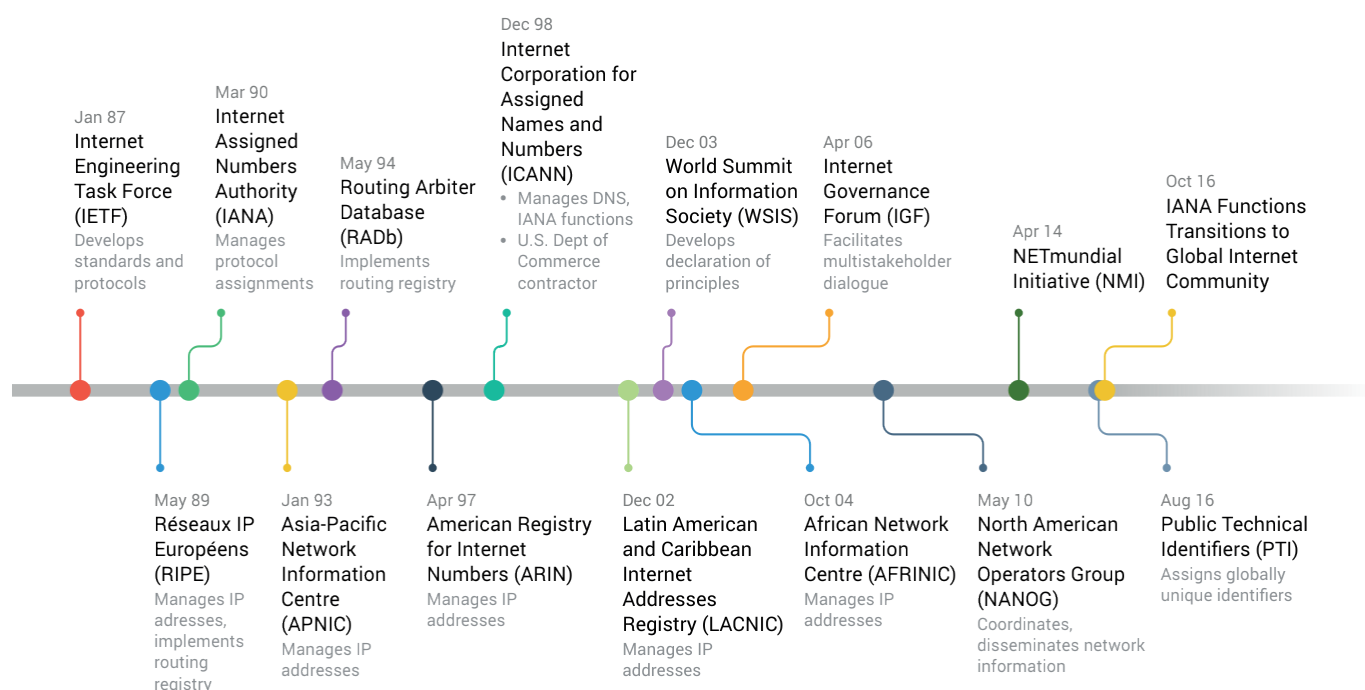


Рис. 1. Временная шкала развития институтов «управления Интернетом».



Рис. 2. Изменение количества измерений в системе APNIC Labs для российских источников DNS-запросов.

тетных DNS-серверов и обнаружить там любопытный факт – до 50% трафика в DNS-запросах совсем недавно составляли «мусорные» запросы платформы Chromium [1]. Как выяснилось, таким образом Google боролся и борется до сих пор с перехватом DNS-запросов к несуществующим доменам.

Резолверы довольно широко используются во всём мире для контроля доступа к различного сорта информационным ресурсам. Доступ может быть законодательно заблокирован по доменному имени. Резолвер может также перенаправить конечного клиента на другой информационный ресурс.

Но в случае наличия ошибок при вводе доменного имени нужного соответствия может не существовать вовсе. Однако можно проанализировать ошибочное имя и, воспользовавшись механизмом перенаправления, предложить возможные релевантные варианты.

Впервые эту идею реализовали в Verisign 15 сентября 2003 года в проекте Site Finder [2] (ресурса на сайте Verisign не найти, но Интернет помнит все!). Система официально была закрыта 4 октября 2003 года. Общественность заклеила

разработчиков как нарушителей стандартов ради коммерческой выгоды. Но сама идея жива до сих пор. И ряд провайдеров её эксплуатируют.

Но это же рекламный доход! А это деньги Google! И поэтому Google в два раза увеличил нагрузку на авторитетные серверы системы DNS ради защиты от тех, кто ищет коммерческую выгоду, типа, нарушая стандарты! Чудеса, да и только!

Стоит здесь упомянуть и ещё об одной особенности DNS в контексте достоверности DNS-данных, которые получает конечный пользователь Интернета. Речь идёт о расширении безопасности DNS-протокола – DNSSEC.

Особенность этой технологии заключается в том, что при обмене данными верифицируется не источник данных, а сам контент. Таким образом, совершенно не имеет значения, откуда получены данные, важно, что за данные получены.

Собственно, эта особенность DNSSEC заложена в концепцию Hyper Local корпорации ICANN [3] и в концепцию «Национальной системы доменных имён» [4].

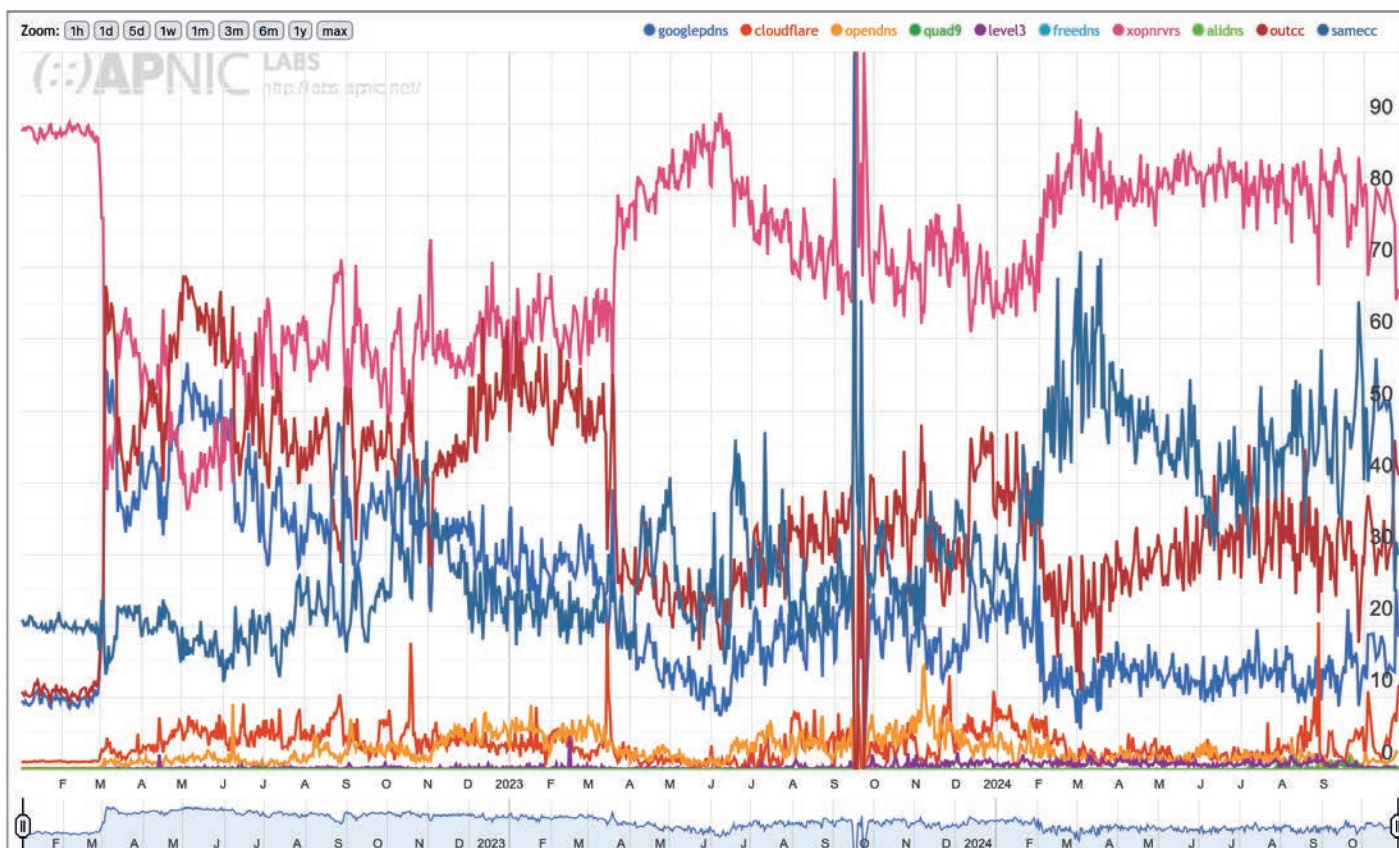


Рис. 3. Увеличение разброса (дисперсии) доли различных DNS-резолверов в измерениях APNIC Labs.

Раз источник не имеет значения, то главным элементом становится тот элемент системы, который проверяет достоверность. Таким элементом в концепции Hyper Local является DNS-резолвер.

Столь пространное вступление к описанию работы Анны Подгук призвано продемонстрировать актуальность и важность работы по изучению вопроса, какими резолверами пользуются клиенты российских провайдеров.

Понятно, что и до «студенческого» исследования такие работы в мире проводились. Наиболее известная из них – исследование APNIC Labs [5]. Эта исследовательская платформа [6] являлась наиболее точной и репрезентативной, т.к. базируется на рекламных площадках Google. Вот в этом последнем утверждении скрывается подвох. Как увидим ниже, оно требует проверки.

В марте 2022 года было замечено резкое падение трафика в этой системе измерений с российских адресов (Рис. 2) и увеличение дисперсии измерений (Рис. 3). Как будто в России пропал Интернет. Но российские пользователи ни о каких «проблемах с Интернетом» в разных их проявлениях не сообщали.

Такое положение вещей поставило два актуальных вопроса:

- что является причиной такого изменения на графиках;
- является ли статистика APNIC Labs репрезентативной в случае конечных пользователей российских интернет-провайдеров.

Ответ на первый вопрос нашёлся достаточно быстро. И он следует из Google Publisher Policies (Рис. 4)

Дело в том, что технология измерения DNS-трафика конечных пользователей в системе APNIC Labs опирается на рекламные площадки Google. Именно ресурсы Google позволяют определить адресный пул конечного пользователя и привязать его к автономной системе провайдера доступа в Интернет.

Понятно, что решение администрации Google повлияло на репрезентативность измерений. Вопрос только в том, насколько существенным оказалось это влияние.

Для ответа на этот вопрос нужно было повторить технологию измерений. Но вот только в качестве площадок измерений нужно было выбрать платформы, отличные от Google, и позаботиться о контроле репрезентативности.

Таким образом, целью «студенческой» работы было определение автономных систем резолверов, которыми пользуются пользователи российских автономных систем.

Агрегация площадок резолверов до уровня автономных систем следует из технологий, которые в данном случае применяются (anycast и CDN).

При этом следовало решить следующие задачи:

- получить запросы конечных пользователей;
- получить связанные с запросами конечных пользователей запросы от DNS-резолверов;

Google Publisher Policies

(March 23, 2022)

Due to the military conflict in Ukraine, we will pause monetization of content that exploits, dismisses, or condones the conflict.

(March 10, 2022)

Given the recent suspension of Google advertising systems in Russia, we'll be pausing the creation of new Russian accounts on AdSense, AdMob, and Google Ad Manager. Additionally, we will pause ads on Google properties and networks globally for advertisers based in Russia.

(March 3, 2022)

Due to the extraordinary circumstances in Ukraine, we will be temporarily pausing ads from serving to users located in Russia.

(February 26, 2022)

In light of the extraordinary circumstances in Ukraine, we are pausing Google's monetization of Russian Federation state-funded media.

We will continue to actively monitor the situation and make adjustments as necessary.

Source: <https://support.google.com/adsense/answer/10502938?hl=en>

Рис. 4. Политика Google в отношении публикаций рекламы для российских пользователей.

- установить однозначное соответствие между запросом конечного пользователя и запросом DNS-резолвера;
- собрать запросы конечных пользователей и связанные с ними запросы DNS в единую базу данных;
- реализовать регулярный сбор такой статистики;
- создать сайт проекта с отчётами по собранному данным.

Общая идея решения данных задач заключается в использовании совокупности инструментов, однозначно идентифицирующих конечного пользователя или их некоторое множество, и системы DNS.

Запросы конечных пользователей можно получить путем создания веб-сайта и анализа логов обращений к этому веб-сайту по протоколу HTTPS. Понятно, что к этому сайту кроме прямого обращения конечных пользователей будет получено множество обращений ботов, обращений через прокси и VPN, а также через различные коллекторы CDN, но и в измерениях APNIC это всё тоже присутствует.

Запросы от резолверов можно получить путём создания авторитетного сервера доменных имён для домена измерений, чей лог будет доступен для сбора и обработки статистики. Собственно, этот сервер должен резолвить запросы к указанному выше веб-сайту.

Для того, чтобы статистика запросов была репрезентативной, нужно обеспечить условия, чтобы на веб-сайт пришли те самые пользователи, настройки системы DNS которых мы хотим измерить.

В случае с APNIC Labs были использованы рекламные площадки Google. По замыслу авторов проекта, репрезентативность измерений обеспечивалась широкой популярностью ресурсов Google, на которых можно было разместить «рекламу» измерительной площадки.

Чисто теоретически, для студенческой работы можно было бы попробовать договориться с Yandex или VK. Но в этом случае на измерительную площадку обрушился бы чудовищный поток запросов, что потребовало бы существенных затрат на построение системы а-ля Big Data. Да и с точки зре-

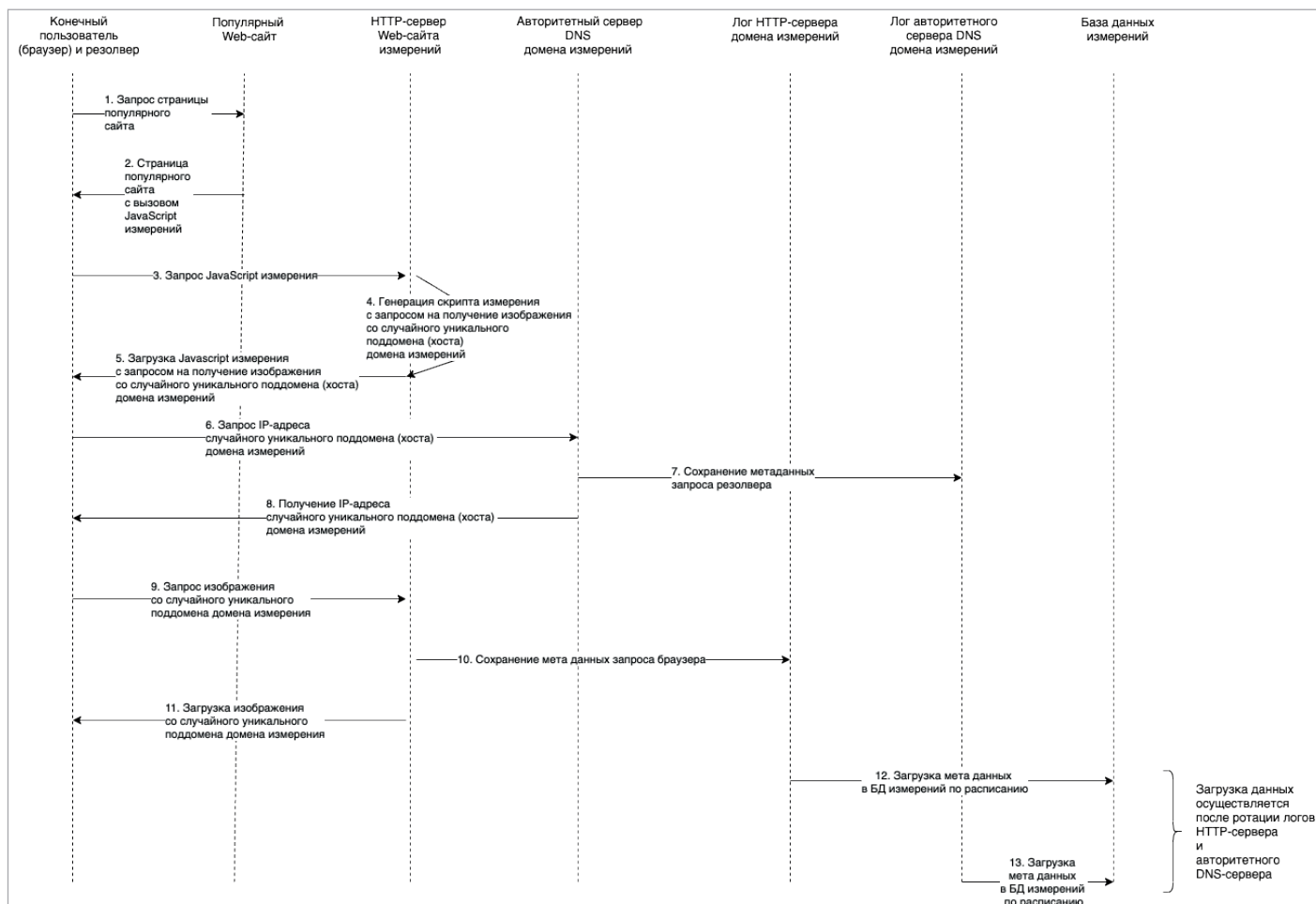


Рис. 5. Диаграмма последовательностей системы измерений.

ния того, что это дипломная студенческая работа, необходимо было показать квалификацию дипломника не только как специалиста в области IT, но и как сформировавшегося исследователя. Поэтому было принято решение в пользу выбора множества не столь популярных площадок (площадок измерения) с контролем репрезентативности измерений по количеству конечных пользователей наиболее крупных автономных систем российских провайдеров.

Для цели контроля использовался проект iddb.ru [7] Фонда развития сетевых технологий «ИнДата» [8], где можно получить необходимую информацию по российским автономным системам и, более широко, о всей интернет-инфраструктуре.

В общем виде схема измерений выглядит следующим образом (Рис. 5):

1. Для получения запроса конечного пользователя достаточно, чтобы на страницу площадки измерения загружался фрагмент контента с веб-сайта измерений, чей лог доступен для сбора и обработки статистики обращений.
2. Таким фрагментом контента может являться JavaScript-фрагмент, который будет обращаться к веб-сайту измерений для загрузки изображения, которое не будет отображаться в браузере конечного пользователя при загрузке страницы популярного веб-сайта.
3. Данный JavaScript-фрагмент должен обращаться к веб-сайту измерений по имени домена измерений, чтобы автори-

тетный сервер DNS этого домена мог получить запрос от резолвера, который использует конечный пользователь.

4. Для того, чтобы однозначно связать запрос конечного пользователя к популярному веб-сайту и запрос резолвера к домену измерений, необходимо реализовать общий для этих двух запросов уникальный идентификатор.
5. Таким общим идентификатором может быть случайное уникальное имя поддомена домена измерений.
6. Это имя должно генерироваться в момент обращения к веб-сайту измерений, загружаться в качестве адреса фрагмента контента популярного веб-сайта, чтобы резолвер конечного пользователя обратился к авторитетному серверу домена измерений для разрешения этого имени.
7. При загрузке фрагмента контента происходит логирование запроса конечного пользователя на HTTP-сервере веб-сайта измерений.
8. При разрешении случайного доменного имени происходит логирование запроса резолвера на авторитетном сервере доменных имён домена измерений.
9. Раз в сутки по расписанию скрипты обработки логов HTTP-сервера веб-сайта измерений и авторитетного сервера DNS домена измерений выбирают метаданные обращений конечных пользователей из соответствующих логов и загружают эти данные в общую базу данных.

10. На основе полученных данных производится их анализ, верификация и получение статистических отчетов.

Для выполнения исследования были развернуты HTTPS-сервер Apache; DNS-сервер bind; зарегистрированы и делегированы домены resolvers.net.ru и resolvers.org.ru; размещён сайт измерений на домене resolvers.net.ru, для сайта получены и установлены wild-card TLS-сертификаты; установлена СУБД PostgreSQL и в её среде развернута БД измерений; написаны скрипты сбора и обработки статистики; разработан сайт проекта [9], на котором транслируются результаты измерений.

Отдельно следует указать площадки измерений, с которыми достигнута договорённость о размещении измерительных скриптов.

В настоящее время необходимые договорённости достигнуты для сайтов и их синонимов:

- org.ru
- net.ru
- pp.ru
- taeping.ru
- netoscope.ru
- cctld.ru

Первые три – это домены третьего уровня, регистратурой которых является АНО «ЦБКС МСК-IX» [10], далее – регистратор доменов в этом реестре и два ресурса администратора национальных доменов Российской Федерации (.ru/.рф) – АНО «Координационный центр национального домена сети Интернет» (КЦ).

Домены третьего уровня довольно часто используются для целей поисковой оптимизации. В статистике обращений к автори-

тетным серверам зоны .ru они занимают значимую долю. Время жизни таких доменов невелико, поэтому их администраторы довольно часто посещают сайт регистратуры и регистратора.

В настоящее время в этой регистратуре зарегистрировано 14 регистраторов [11], в том числе и все крупные регистраторы национальных доменов РФ.

Сайт администратора национальных доменов Российской Федерации в подробном представлении не нуждается.

А вот сайт netoscope.ru стоит отметить отдельно. Здесь сведена статистика по репутации доменов второго уровня в национальных доменных зонах. Проект Netoscope был учрежден КЦ при участии уполномоченных компетентных организаций, которые занимаются вопросами информационной безопасности [12].

К сайту обращаются довольно часто. Нет более горячей темы, чем тема безопасности в Интернете. К сайту обращаются и специалисты компаний по информационной безопасности, и администраторы доменных имён, и владельцы товарных знаков, и эксперты в области информационной безопасности. Сайт активно индексируется поисковыми роботами. В силу постоянной изменчивости состояния репутации национальных доменных зон информационные страницы сайта попадают в кеш и обновляются на узлах CDN довольно часто, что обеспечивает актуальность получаемой информации.

В описываемом исследовании этот момент важен с точки зрения репрезентативности измерений.

Согласно данным iddb, наиболее масштабные пулы IP-адресов имеют следующие российские AS [13]:

N	aut-num	as-name	Кол-во IPv4 адресов	Кол-во IPv6- сетей /48
1	AS12389	ROSTELECOM-AS	9709952	983041
2	AS8402	CORBINA-AS	2268672	65536
3	AS8359	MTS	1805056	1491200
4	AS3216	SOVAM-AS	1270784	65538
5	AS12714	MEGAFON-AS	1210624	131072
6	AS31133	MF-MGSM-AS	788480	11595
7	AS20485	TRANSTELECOM	608000	720896

Рис. 6. Список российских aut-num. Источники данных – базы данных RIR.

Если теперь сравнить этот список со списком источников запросов из «студенческой» работы, то увидим, что все эти AS там есть (Рис. 7, отмечены галочками):

При этом порядок расположения автономных систем в списке с рисунка 7 хорошо коррелирует с порядком расположения автономных систем в списке с рисунка 6, т.е. с количеством IP-адресов.

Номер AS пользователя	Имя AS пользователя	Количество измерений
25159	✓ SONICDUO-AS	1875
12389	ROSTELECOM-AS	1300
42610	✓ NCNET-AS	697
8402	✓ CORBINA-AS	514
49828	DARNET-AS	470
25513	ASN-MGTS-USPD	419
8492	✓ OBIT-AS	386
8359	MTS	380
16345	✓ BEE-AS	279
12714	✓ MEGAFON-AS	247
31133	MF-MGSM-AS	227
43966	ITREGION-AS	195
20919	IBS	136
48092	NSB-AS	127
12958	MCC	102
24955	UBN-AS	87
31163	✓ MF-KAVKAZ-AS	85
3216	✓ SOVAM-AS	82
31213	MF-NWGS-AS	78
31200	NTK	77
201052	GOVCERT-RU-AS	75
35807	SkyNet-SPB-AS	72
49724	VAINAHELECOM-AS	72
21017	VSI-AS	71
3316	RELARN	70
15582	AKADO-B2C-AS	69
28840	TATTELECOM-AS	68
29497	KUBANGSM	64
199009	TCINET-AS-IT	55
48043	OZYORSK-TELECOM-AS	54
13238	YANDEX	45
41704	OGS-AS	44
61360	NOVOCHEK-AS	41
50473	ECO-AS	40
8369	INTERSVYAZ-AS	37
48190	✓ T2-EKATERINBURG-AS	37
20485	TRANSTELECOM	35

Рис. 7. AS-источники запросов к системе измерений использования резолверов.

Таким образом, можно утверждать, что пользовательские пулы основных российских провайдеров доступа в Интернет в данном исследовании представлены. И в этом смысле измерения достаточно репрезентативны.

Конечно, результат был бы более надёжным, если бы для сравнения провести измерения с использованием рекламных площадок Yandex или VK на ограниченном промежутке времени, и такие измерения, возможно, будут проведены в будущем.

На текущий момент в рамках исследования были получены следующие результаты.

Список наиболее популярных резолверов для конечных пользователей российских AS (Рис. 8) по результатам измерений:

Номер AS резолвера	Имя AS резолвера	К-во AS пользователей
13238	YANDEX	246
13335	CLOUDFLARENET	234
16509	AMAZON-02	124
43832	RIPN-NS5-RU-MSK	103
36692	OPENDNS	27
15169	GOOGLE	26
60068	CDN77	23
31483	ERTELECOM-DC-AS	22
47445	RIPN-RU-RND	22
42139	RIPN-RU-NSK	18
42728	RIPN-RU-EKT	17
13174	MTSNet	17
45029	RIPN-SU-NET	17
36236	NETACTUATE	15

Рис. 8. Список наиболее популярных резолверов для конечных пользователей российских AS.

В то время как у APNIC Labs [14] (Рис. 9):

ASN	AS Name	googlepdns	cloudflare	opendns	quad9	level3	onedns	freedns	greenteamdns	114dns	comodo	Samples
AS12389	ROSTELECOM-AS	2.051%	47.692%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	1,950
AS6704	CITYLAN-AS	0.806%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	1,240
AS57013	EURASIA-STAR-AS	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	1,210
AS9123	TIMWEB-AS	44.915%	10.169%	1.695%	3.390%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	1,180
AS57354	SYSTEMA-AS	8.333%	0.000%	41.667%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	1,080
AS50257	AMOBILE-AS	5.405%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	740
AS20485	TRANSTELECOM Moscow, Russia	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	620
AS13335	CLOUDFLARENET	38.333%	26.667%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	600
AS47282	ABAZATEL-AS	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	530
AS58172	FREEDOMTELECOM-AS FREEDOM TELECOM LLP	100.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	0.000%	470

Рис. 9. Список наиболее популярных резолверов для российских пользователей по версии APNIC Labs.

Из представленных таблиц понятно, что у APNIC Labs список крупных российских AS не полон и списки используемых резолверов существенно отличаются. Резолверы в заголовке упорядочены по их популярности в мире. Для российских провайдеров этот порядок не соблюдается.

Есть ещё один важный момент, который заставляет сомневаться в репрезентативности данных APNIC Labs – там нет резолверов НСДИ (имена начинаются с «RIPN-...»). А это точно не соответствует действительности, т.к. использование НСДИ обязательно, и это подтверждается другой статистикой, например, статистикой обращений к авторитетным серверам национальных доменов. Таким образом, вывод о нерепрезентативности измерений APNIC Labs подтверждается.

Любопытно, что насыщения списка автономных систем в данной системе измерений не достигнуто (Рис. 10). Таким образом, потенциал роста этого списка, а с ним и потенциал увеличения репрезентативности измерений есть.

«Комбинированные краулеры»

Вторая представленная на конференции работа была посвящена комбинированным инструментам измерения. В рассмотренной выше работе Анны Подгук фактически проводились «пассивные» измерения. Но существует большой набор программ-инструментов, которые проводят «активные» измерения применения различных интернет-технологий. Такой вид программ принято называть краулерами.

Суть краулера в обходе информационных ресурсов Сети и сборе специфических технических параметров. Большинство современных интернет-сервисов построены по принципу «клиент/сервер», т.е. клиент посылает запрос, а сервер присылает ответ на данный запрос. Соответственно, под термином «обход» понимают опрос информационных ресурсов из заранее заданного или динамического списка по различным протоколам и сбор ответов с последующим их разбором.

Отдельной проблемой при интерпретации таких данных является их визуализация. Особенно это касается графической визуализации результатов исследований.

Целью работы Артёма Ожидина было исследование вариантов визуализации для «протокол-независимой» логики.

Вот цитата из его презентации, которая достаточно общо описывает смысл работы: «Сложность инфраструктуры, стоящей за современными интернет-сервисами, возникает как результат сопряжения различных сетевых протоколов, работающих на разных уровнях, но влияющих друг на

друга. Например, использование HTTPS для доступа к DNS. При этом многие «технологические феномены» становятся хорошо видны только через достаточно общие методы визуализации, отталкивающиеся от «протокол-независимой» логики. DNS, являясь элементом фундамента Интернета, как раз предоставляет отличную точку старта для визуализации устройства прочих интернет-сервисов».

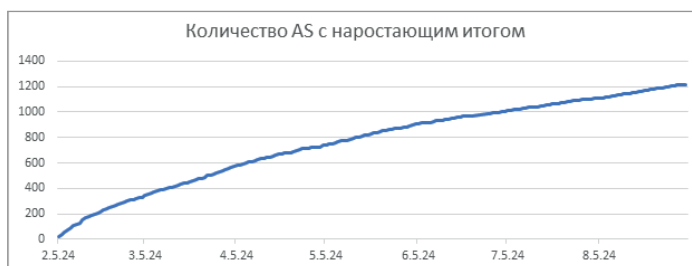


Рис. 10. Насыщение списка автономных систем

Нельзя сказать, что это первая работа такого рода. Хорошо известны, например, такие системы:

- IDDB.RU (графическое представление связности автономных систем);
- DNSViz (графическое представление структуры DNSSEC с верификацией протоколов);
- программный пакет HViz (визуализация трафика HTTPS).

Разрабатываемый краулер позволяет не только проверить наличие того или иного технического параметра у информационного ресурса, но также верифицирует применение той или иной интернет-технологии.

В качестве инструментов для написания кода в работе использовались:

- Golang (язык программирования);
- специализированные библиотеки `meikg/dns` (обращение к ресурсам Интернета по различным протоколам);
- стандартные библиотеки;
- GraphViz (для отображения результатов работы краулера).

На рисунке 11 представлен пример результатов анализа, разработанный краулером:

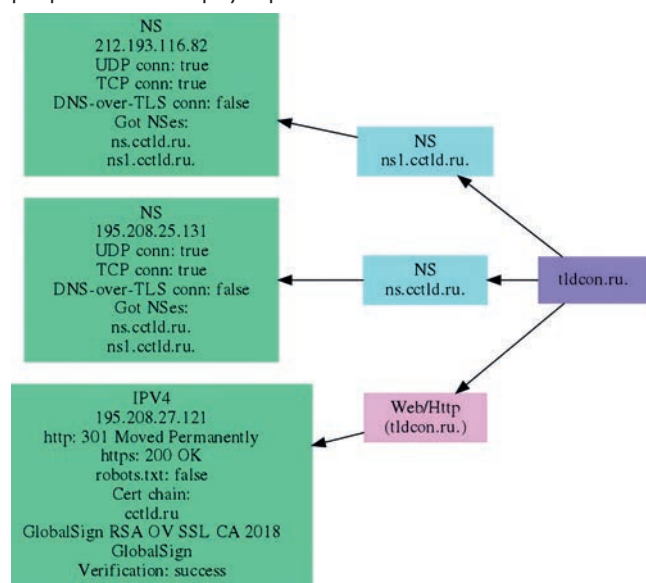


Рис. 11. Результат работы краулера по верификации структуры DNS и HTTPS для домена конференции.

В настоящее время данный инструмент используется в качестве прототипа в исследованиях Фонда «ИнДата». Работы ведутся в части расширения списка протоколов, расширения измерений на адресное пространство IPv6 и расширения API в сторону стандартизации в стиле REST API. Важной особенностью данного инструмента является его переносимость и всеплатформенность. В отличие от перечисленных ранее инструментов, которые по сути являются сайтами (кроме последнего), разработанный студентом программный комплекс является прикладной программой, которую можно использовать вне связи с каким-либо сайтом.

Вместо заключения

Конференция в Минске была второй после пандемии, у которой был предусмотрен офлайн-формат. Если в 2023 году

в Петрозаводск участники ехали с некоторой опаской, то в Минске собрался весь обычный состав участников за исключением наших прибалтийских коллег.

Общее впечатление от конференции можно сформулировать следующим образом: общий уровень технологических и маркетинговых исследований подвизался. Если раньше сообщения российских участников сильно отличались по масштабу и, соответственно, результатам, то сейчас такого разрыва нет. И Казахстан, и Белоруссия фактически решают те же самые вопросы, а в вопросах сотрудничества с зарубежными партнёрами и заимствования «заморских» технологий опережают российских коллег.

Практически не было проходных докладов. Все презентации вызывали живой интерес участников, тем отраднее было отметить, что работы наших студентов в этом контексте не выглядели чем-то второстепенным и неинтересным. И хотя все эти работы по своей сути можно описать фразой «повторение – мать учения», т.к. все они в той или иной степени повторяли разработки международных лабораторий, тем не менее, новизны и актуальности в них было достаточно, чтобы участники конференции их отметили. ■

Список литературы:

- [1] Matthew Thomas, «Chromium's impact on root DNS traffic», <https://blog.apnic.net/2020/08/21/chromiums-impact-on-root-dns-traffic/>, 21/08/2020
- [2] VeriSign's Site Finder Implementation, <https://web.archive.org/web/20041109202247/http://www.verisign.com/static/002702.pdf>, 27/08/2003
- [3] Roy Arends and Nicolas Antonello, «Hyperlocal Root Zone Technical Analysis», OCTO-027, <https://www.icann.org/en/system/files/files/octo-027-25aug21-en.pdf>, 25/08/2021
- [4] «Национальная система доменных имен (НСДИ)», ГРЧЦ, <https://portal.poc.gov.ru/ru/news/2022/08/25/nsdi/>, 25/08/2022
- [5] Geoff Huston, «DNS resolver centrality», APNIC, <https://blog.apnic.net/2019/09/23/dns-resolver-centrality/>, 23/08/19
- [6] Use of DNS Resolvers for World (XA), APNIC, <https://stats.labs.apnic.net/rvrs>, 31/10/2024
- [7] IDDB, Фонд «ИнДата», <https://www.iddb.ru/>, 31/10/2024
- [8] Фонд развития сетевых технологий «ИнДата», <https://www.indata.org.ru/>, 31/10/2024
- [9] Проект «DNS Resolver Use», <https://resolvers.net.ru/>, 31/10/2024
- [10] АНО «ЦБКК МСК-IX», <https://www.ccni.ru/>, 31/10/2024
- [11] «Аккредитованные регистраторы в доменах NET.RU, PPRU, ORG.RU», АНО «ЦБКК МСК-IX», <https://org.ru/registrars.html>, 31/10/2024
- [12] «Список компетентных организаций», АНО «Координационный центр национального домена сети Интернет», <https://cctld.ru/help/safety/competent/>, 31/10/2024
- [13] «Список российских aut-num», проект «IDDB», Фонд «ИнДата», <https://www.iddb.ru/autnum/>, 31/10/2024
- [14] «Use of DNS Resolvers for Russian Federation (RU)», APNIC, <https://stats.labs.apnic.net/rvrs/RU?o=cXAw1hsot1ox>, 31/10/2024

Об авторе

Храмцов Павел Брониславович, к.т.н., доцент, научный руководитель проектов фонда «ИнДата», Москва, p.khramtsov@msk-ix.ru

«Византийский» web, или Назад в будущее?

Марат Биктимиров



Аннотация

Термин «децентрализация» не имеет чёткого общепринятого определения и часто является собирательным для целого ряда новых технологий, которые обещают изменить привычный web в ближайшем обозримом будущем.

Между тем, у децентрализации, как и у любой новаторской концепции, есть поклонники и противники. Их взгляды на процессы, происходящие сегодня в Сети, расходятся по различным причинам и основаниям.

Однако мировой тренд на потребность общества в преодолении излишней централизации web – это факт, который невозможно отрицать. Но какой процесс в итоге возглавит новую эпоху – централизация, децентрализация или их комбинация? На этот счёт у специалистов существуют различные мнения и сценарии.

В представленной обзорной статье используются материалы из разных источников, результатов исследований, статей и блогов, на основании которых предпринята попытка обозначить некоторые существенные по мнению автора позиции полемизирующих между собой сторон.

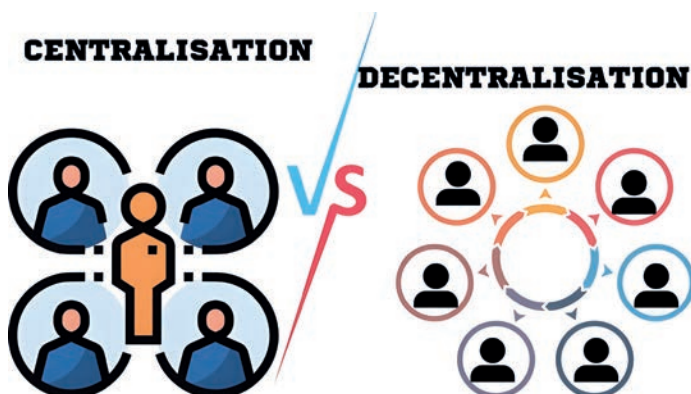
Ключевые слова:

децентрализация, блокчейн, инновации, интернет, надёжность, сеть, транзакция, узел, энергоэффективность, web

Одним из самых ярких и горячо обсуждаемых конфликтов будущего цифровой трансформации является «противостояние» поборников централизованной и децентрализованной моделей развития. Это касается и архитектуры нового поколения web, и данных со способами их хранения, и новых цифровых финансовых активов, и множества других цифровых (и не только) сущностей. Так в чём, собственно, состоит конфликт и так ли уж он принципиален?

Достаточно длительный период вся индустрия информационных технологий развивалась под воздействием мощных центростремительных сил. В корпоративных центрах обработки данных сосредоточены мощные серверы и монолитные приложения; в сфере телекоммуникаций операторы построили гигантские многоанговые инфраструктуры; а в сфере медиа корпорации – собственники контента – контролируют каналы вещания. В общем, с централизацией всё кажется более-менее понятным. Это концентрация управления в едином центре, в одних руках, в одном месте, то есть создание иерархической структуры с преобладанием вертикальных связей. При этом верхние уровни обладают прерогативой в принятии решений, а сами решения обязательны к выполнению для нижних уровней. Не удивительно, что основной упрек, предъявляемый централизации, сводится к монополии на контроль, управление и владение данными. Однако, так или иначе, всегда объективно находятся весьма веские причины для централизованного объединения субъектов управления [1].

А вот с децентрализацией всё обстоит гораздо сложнее, да и само понятие довольно многогранное. До сих пор единого общепринятого определения нет. Обычно её описывают как процесс распределения полномочий за пределы управляющего центра. То есть децентрализация предполагает, что решения принимаются на более низком уровне и как можно ближе к тем субъектам, на которых эти решения направлены. Однако на деле децентрализация может



Источник: <https://klarda.com/blogs/why-decentralization-is-better-than-centralization>

оказаться весьма сложной задачей, поскольку обеспечить равное право и заинтересованность каждого субъекта в собственном управлении может быть непросто. Тем не менее, адепты считают, что применение принципов децентрализации всё же стоит затраченных усилий, поскольку их внедрение может привести к созданию более устойчивых и справедливых экосистем [2].

Критики же децентрализации считают её слишком эфемерной и затратной по сравнению с высокой эффективностью и чёткостью принятия решений в централизованных системах. Кроме того, множество источников и разрозненных децентрализованных данных приводят сразу к нескольким существенным проблемам: несогласованности, небезопасности и недоверию. В результате накопленные данные могут стать источником угроз и окажутся непригодными для принятия решений. Приверженцы централизации данных в своей практике, как правило, используют два основных подхода. Один из них – так называемый единый источник истины (англ. Single Source of the Truth – SSOT), который предполагает существование одного центрального хранилища данных. Суть этого подхода заключается в формировании единственного источника информации для всех пользователей, который, соответственно, гораздо легче дополнить и/или обновить. Некоторой альтернативой ему служит концепция единой версии истины (англ. Single Version of the Truth – SVOT). Её отличие состоит в том, что вместо централизованного хранилища обеспечивается интеграция и синхронизация всех систем для согласования данных между собой. Такой результат достигается посредством использования федеративной архитектуры, когда информация локализуется и хранится в месте её происхождения. Отметим, что при обоих подходах управление остаётся централизованным. Однако не стоит игнорировать вполне здравые возражения оппонентов, что централизация непосредственно ассоциирована с понятием «единая точка контроля/отказа» и, как следствие, с потенциальными негативными последствиями такого её свойства [3].

Но вернёмся к современной эволюции web, которую именуют чуть ли не революцией с приматом децентрализации. Принято считать, что концепция децентрализации лежит в основе технологий web3, предвещающая новую эпоху, когда контроль и полномочия распределяются между участниками всей экосистемы. Новая парадигма предполагает создание децентрализованной цифровой инфраструктуры, поддерживающей устойчивую экономику, способствующей инновациям, инклюзивности и прозрачности [4]. Сегодня глоссарий web3 включает почти все модные понятия, и прежде всего – блокчейн, биткойн, криптовалюта, децентрализованное приложение (dApp), смарт-контракт, децентрализованные финансы (DeFi), невзаимозаменяемые токены (NFT)... За каждым из этих понятий стоит определённая технология. Однако в целом большая часть из них всё ещё имеет ограниченное распространение. Некоторые причины ограниченного внедрения включают концептуальную сложность, высокую стоимость разработки, отсутствие удобства в использовании, проблемы безопасности, отставание в регулировании и трудности имплементации в существующие системы. Вместе с тем, похоже, что не только здесь, как говорится, «собака зарыта».



Источник: <https://intuji.com/what-is-web-3-0-a-comprehensive-guide/>

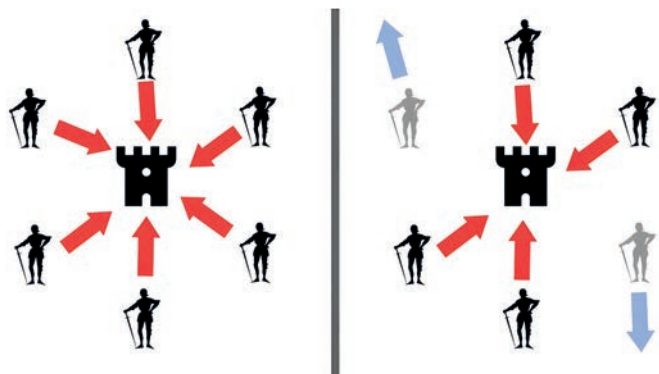
Давайте обратим внимание только на два спорных фактора, вызывающих огонь критики с обеих полями мизирующих сторон. Это энергоэффективность и надёжность.

Итак, одна из наиболее «жёстких» позиций гласит, что децентрализованные системы не имеют «светлого будущего» хотя бы в силу того, что при росте числа пользователей они проигрывают централизованным по энергоэффективности. А ведь энергосбережение – номер один мировой экономической повестки. Считается, что сеть децентрализована, когда управление сетью совместно используется подмножеством узлов сети. Такая децентрализованная структура представляет собой некоторое множество компьютеров, каждый из которых связан с одним или несколькими другими соседними. При этом все узлы в равной степени разделяют обязанности и запускают одно и то же программное обеспечение узла. Транзакция, сгенерированная на одном компьютере, пересылается соседним, которые проверяют правильность подписей в ней и далее пересылают её уже своим «соседям». Таким образом транзакция попадает на все узлы сети. Очевидно, что при увеличении количества участников сети будет увеличиваться и общее число транзакций. Парадокс заключается в том, что с ростом количества узлов децентрализованной сети повышается её надёжность (что хорошо), но и... затратность (что плохо). В результате «грубых» прикидок критиками делается весьма тревожный вывод, что увеличение количества транзакций и увеличение количества пользователей приводит к кратному увеличению суммарных расходов на электроэнергию. Кроме того, рост количества транзакций негативно сказывается на пропускной способности сети и, как результат, совокупная стоимость её содержания растёт быстрее, чем в случае централизованной архитектуры. Так это или нет, и в какой степени – предмет отдельного исследования, но подобные умозаключения безусловно обращают на себя внимание [5].

Упомянутый парадокс связал понятия затратности и надёжности в децентрализованной сети. Вспомним, что в отличие от централизованных сетей с одной точкой контроля/отказа, децентрализованные сети таковым свойством обладать не должны по определению. При этом любой участник децентрализованной сети не гарантирует своего постоянного присутствия в ней. Но по достижению определённого количественного порога в сети будет постоянно и одновременно присутствовать некоторое множество узлов с одинаковыми функциями. И кажется, что чем больше количество этих узлов в сети, тем выше её надёжность, а значит, преимущество децентрализации очевидно. Но и здесь не всё так однозначно.

Надёжность — это не только вероятность того, что система или её компонент будут бесперебойно выполнять свои функции в любой момент времени. Это свойство также влияет на уверенность, что все элементы системы функционируют корректно, то есть, что ей можно доверять. Надёжная система должна уметь преодолевать отказы одного или нескольких её компонентов, которые потенциально могут генерировать и отправлять противоречивую информацию. Это положение приводит нас к так называемой концепции византийской отказоустойчивости, обуславливающей корректное функционирование децентрализованных систем в случае непреднамеренных или умышленных сбоев в работе их компонентов [6].

Вот тут как раз уместно было бы напомнить «задачу византийских генералов». Она включает в себе фундаментальную проблему достижения консенсуса в децентрализованной сети, то есть без доверенного центрального органа. «Задача византийских генералов» из раздела прикладной математики «Исследование операций» имеет важнейшее значение для понимания динамики принятия решений, когда участники не могут проверить личность или честность других в среде, характеризующейся ненадёжными каналами связи. По сути, она представляет собой сценарий, в котором несколько легионов византийской армии, аналогично узлам сети, должны договориться о едином образе действий: атаковать или отступить. При этом договорённость (консенсус) должна быть достигнута, несмотря на наличие ненадёжных или потенциально предательских элементов внутри системы, которыми являются генералы и/или их гонцы.

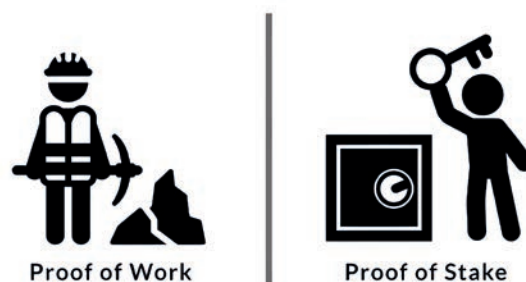


Источник: <https://galoren.cswp.cs.technion.ac.il/wp-content/uploads/sites/163/2023/10/dist.png>

Чтобы защитить функционирование сети от злоумышленных действий, необходимо использование надёжного алгоритма. Эта потребность привела к разработке отказоустойчивых консенсусных протоколов, обеспечивающих эффективную обработку сбоев. Одним из таких протоколов является «Практическая византийская отказоустойчивость» (PBFT), использующая сочетание цифровых подписей, тайм-аутов и подтверждений, чтобы обеспечить непрерывный прогресс процесса согласования, даже когда некоторые узлы скомпрометированы или действуют злонамеренно при условии, что большинство узлов остаются заслуживающими доверия. Другой разновидностью протокола стало «Федеративное византийское соглашение» (FBA), в котором внутри каждой сформированной независимой федерации узлы договариваются о порядке и легитимности транзакций или событий.

Появление сети биткоин (Bitcoin) на базе технологии блокчейн фактически означало вариант решения «задачи ви-

зантийских генералов» посредством механизма консенсуса Proof of Work (PoW), в котором майнеры выполняют роль, аналогичную генералам, в сети, где каждый узел отвечает за проверку транзакций. Эти транзакции группируются в блоки, хешируются и хранятся в распределённой базе данных, реплицируясь по всей сети, что повышает её отказоустойчивость и гарантирует, что сбой одного узла не поставит под угрозу всю систему. Эта избыточность аналогична наличию нескольких гонцов, что должно обеспечивать целостность и неизменность сообщения, даже если один из них будет скомпрометирован.



Источник: <https://bits.media/pow-ili-pos-o-vybore-metoda-konsensusa-dlya-kriptoalyutnykh-proektov/>

Дальнейший поиск путей достижения консенсуса в блокчейне привёл к появлению механизма Proof of Stake (PoS), который уже не полагается на майнеров. В этом механизме появляются пользователи с полномочиями валидаторов, которые «ставят» свои средства в качестве гарантии. Чем больше средств в ставке валидатора, тем больше блоков он может проверить и тем выше его вознаграждение. Однако появляется риск, обусловленный вероятным появлением валидаторов, потенциально способных одобрять ложные транзакции. И, наконец, разновидность PoS - DPoS, в котором роль валидаторов выполняет избранная сообществом сети группа пользователей — так называемых делегатов. Очевидно, что в этом случае консенсус достигается гораздо быстрее, но возникает риск сговора делегированного меньшинства против интересов большинства участников сети [7].

Как видно, приведённые модели достижения консенсуса с точки зрения надёжности и доверия не являются таким уж идеальным решением, хоть и не без оснований претендуют на высокую степень их достижения при использовании на практике (Avalanche, Ethereum, Tezos и др.). Другое дело, что «децентрализованная» сеть, в конструкцию которой заложен принцип, требующий придания особого статуса какому-либо узлу или их группе, провоцирует её переход в статус распределённой или в пределе — даже централизованной сети.

Но так ли уж плоха распределённая сеть по отношению к децентрализованной — и в чём разница? В распределённой сети управление узлами может осуществляться из нескольких «местных» центров, каждый из которых может быть взаимосвязан как напрямую, так и через узлы-посредники. Тогда можно сказать, что децентрализованная сеть является частным случаем распределённой сети, в которой все узлы одноранговые, и каждый узел является «местным» центром, который влияет только на самого себя (что фактически равнозначно отсутствию центров управления). В таком случае, возможно, что распределённая сеть при правильном подходе позволит несколько проще достигнуть заданных требова-

ний по надёжности, чем децентрализованная сеть. Её легче поддерживать при значительном масштабировании, в отличие от децентрализованной, эффективность которой весьма чувствительна по отношению к существенному росту числа узлов [8].

Как бы то ни было, основной мотивацией поклонников децентрализации и распределённости является независимость от централизованных сервисов, которые могут устанавливать произвольные правила и навязывать пользователю свою волю.

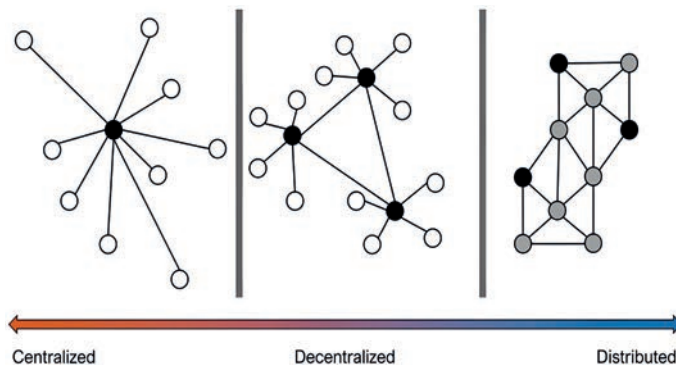
До появления WWW (англ. World Wide Web) в мире уже существовали децентрализованные системы, к слову, сам Интернет. По отношению к традиционной почтовой службе электронная почта тоже стала децентрализованным сервисом, поскольку разные почтовые серверы напрямую обменивались сообщениями. Следовательно, децентрализация – вовсе не утопия, а веление времени. Вспомним, что и web изначально задумывался как открытая децентрализованная платформа для взаимодействия.

Однако со временем технологические гиганты стали создавать удобные для пользователей интерфейсы и вырвались вперёд, набрав критическую массу централизованных решений. Постепенно интерес к децентрализации затих до тех пор, пока свет не увидела научная работа о новой децентрализованной сети Биткоин. Тогда некоторые эксперты охарактеризовали процессы, запущенные Биткоином, как технологическую революцию, которая знаменует собой глубокие перемены, возвращающие нас к забытому, но привычному положению вещей.

Теперь в сообществе появились заметные разногласия относительно того, что же такое новый web. Крайне амбициозные взгляды состоят в том, чтобы разрушить многие централизованные модели, например, модель данных клиент-сервер и бизнес-модель, основанную на рекламе, и воссоздать децентрализованные заново. Но web, несмотря на своё изначально децентрализованное происхождение, десятилетиями переходил к централизации и вряд ли сейчас имеет смысл «сносить всё до основания». Стремительное возрождение децентрализованных технологий и активная полемика вокруг них дают почву для серьёзных размышлений о его будущем. Похоже, что пока децентрализованные технологии не являются абсолютной панацеей и не спасают web нового поколения от всех наследуемых проблем [9].

Означает ли это, что сегодня децентрализацию стоит применять только там, где это целесообразно? Пожалуй, это вполне рациональный подход. Если создаётся «продвинутое» web-приложение, оно не обязано стать исключительно децентрализованным. Любое решение создается для того, чтобы предоставить пользователям требуемые возможности, и определённые уровни децентрализации могут отвечать или не отвечать этим запросам [10].

Вполне возможно, что децентрализация управления данными, ресурсами и доступа к ним позволит обеспечить наиболее качественное и справедливое обслуживание. Но, увы, она скорее всего потребует некоторых существенных компромиссов, например, снижения пропускной способности



Источник: https://www.researchgate.net/figure/De-centralization-configurations-from-a-network-perspective-Black-lines-represent_fig1_352297989

транзакций. Значит, нужно стремиться к тому, чтобы в идеале эти компромиссы не перевешивали уровни надёжности и качества сервиса, которые за их счет достигаются. ■

Список литературы:

- [1] Словарь «Борисов А.Б. Большой экономический словарь. — М.: Книжный мир, 2003. — 895 с.
- [2] Chris Dixon (2018), «Why Decentralization Matters», 18 February, available at: <https://onezero.medium.com/why-decentralization-matters-5e3f79f7638e>
- [3] «Минутка истории: Откуда пришла идея централизации и единого источника актуальных данных», URL: <https://habr.com/ru/companies/rshb/articles/823558/>
- [4] Verborgh, R. (2017), «Paradigm shifts for the decentralized Web», 20 December, available at: <https://ruben.verborgh.org/blog/2017/12/20/paradigm-shifts-for-the-decentralized-web/>.
- [5] «Bitcoin. Неразрешимая проблема децентрализации», URL: <https://habr.com/ru/articles/238397/>
- [6] Giuseppe Gori, «Decentralization: The Big Problem For Blockchain», URL: <https://cryptobriefing.com/decentralization-big-problem-blockchain/>
- [7] «В чём проблема византийских генералов?», URL: <https://plisio.net/ru/blog/what-is-the-byzantine-generals-problem>
- [8] Владимир Шляпин, «Децентрализация VS распределенная сеть», URL: https://sitemakers.ru/articles/decentralization_vs_distribution/
- [9] Evgeny Ponomarev, «Decentralized Web Developer Report 2020», URL: <https://medium.com/fluence-network/decentralized-web-developer-report-2020-5b41a8d86789>
- [10] «Что означает децентрализация в блокчейне?», URL: <https://aws.amazon.com/ru/blockchain/decentralization-in-blockchain/>

Об авторе

Биктимиров Марат Рамилевич - Фонд развития сетевых технологий «ИнДата», г. Москва. SPIN-код:5110-3250, AuthorID:108733, ORCID:0000-0003-3222-6455

Юрисдикционный формат регулирования цифровых валют в параметрах определения порядка их использования

Мадина Касенова



Аннотация

Использование цифровых валют так или иначе расширяет список традиционных платёжно-расчётных средств и увеличивает возможности диверсификации активов. В настоящей статье дана общая характеристика цифровых валют в их существующих видах (типах), рассмотрены обобщённые варианты подходов регулирования криптовалют в юрисдикциях государств.

Ключевые слова:

цифровые валюты, фиатные валюты, цифровая валюта центрального банка (ЦВЦБ), стейблкоины (Stablecoins), криптовалюты (Cryptocurrencies), варианты регулирования криптовалют

В настоящее время не подлежит сомнению значимость использования цифровых валют, в т.ч. контекстно определяемые параметрами текущего и будущего развития экосистемы индустрии цифровых платежей. Безусловно, весомым и актуальным остаётся комплекс вопросов, в перечень которых входят, в частности, классификация видов (типов) цифровых валют и их содержательная характеристика; определение способов выпуска цифровых валют; установление порядка регламентации обращения и использования конкретных видов (типов) цифровых валют с разграничением их функциональной роли в юрисдикциях государств, а также последствия их внедрения в инфраструктуру национальной платёжно-денежной системы. В юрисдикциях различных государств обозначенные вопросы получают различное толкование и регуляторное решение, что, разумеется, обусловлено обстоятельствами объективного и субъективного свойства. Критически существенным обстоятельством, объективно детерминирующим вектор формирования регуляторной практики всех государств, является их технологический уровень развития, во многом определяющий внедрение (либо отказ от внедрения) технологических инноваций в целом и использование цифровых валют в частности. Разнообразие использования цифровых валют в различных юрисдикциях, бесспорно, заслуживает самостоятельного предметного исследования, вместе с тем представляется возможным в настоящей статье обратиться к обобщающим подходам, сложившимся в текущий период.

Цифровые валюты: общая характеристика

Цифровая валюта (Digital Currency) является некой «собирательной» дефиницией, которая терминологически используется для обозначения валют, существующих в электронной/цифровой форме, доступ к которым осуществляется с помо-

щью компьютеров или мобильных телефонов. Ряд характеристик, свойственных денежным единицам, также присущи цифровым валютам, в частности, когда таковые служат средством сбережения стоимости, расчётной единицей или средством обмена, а также используются потребителями при совершении транзакций [1]. В этой связи аспект сопоставления цифровых валют и традиционных валют является важным для последующего изложения, соответственно, следует сказать несколько слов о «фиатных валютах»/«фиатных деньгах», обладающих специфическими особенностями. Такие валюты принято называть фидуциарными¹ или декретными. Фиатная валюта/фиатные деньги – это форма официальных денежных знаков, установленных государством и обычно выпускаемых центральным банком. Фиатная валюта отличается от иных исторически существующих форм денег, выпускаемых государством, т.к. такая валюта не обеспечена золотом или другими драгоценными металлами (например, серебром), а номинальная стоимость денег устанавливается и гарантируется государством вне зависимости от стоимости материала, использованного для их изготовления. Фиатная валюта может номинироваться в форме физически выпущенных банкнот и наличных денег или может быть представлена в электронном виде, например, банковским кредитом, резервами центрального банка или цифровой валютой центрального банка, которая рассматривается далее.

В электронной/цифровой среде используются как централизованные, так и децентрализованные цифровые валюты. Вопросы классификации различных видов (типов) цифровых валют, включая их содержательную характеристику, не имеют однозначного решения, однако основными видами (типами) цифровых валют считаются цифровые валюты центрального банка (Central Bank Digital Currency, ЦВЦБ); стейблкоины (Stablecoins); криптовалюты (Cryptocurrencies).

¹ Фидуциарные (от лат. «fiducia» — доверие) знаки. URL: https://www.banki.ru/wikibank/fiatnyie_dengi/

Цифровая валюта центрального банка, ЦВЦБ (Central Bank Digital Currency, CBDC)

ЦВЦБ – это одна из форм (вид) цифровой валюты, эмитируемая центральным банком страны (далее – «цифровая валюта ЦВЦБ» или «ЦВЦБ») [2]. В целях развития национальной платежной системы многие государства разрабатывают и внедряют цифровую валюту ЦВЦБ, которая представляет собой эквивалент фиатной валюты страны, а её стоимость фиксируется центральным банком [3, 4, 5, 6]. Государства рассматривают ЦВЦБ как регулируемую цифровую валюту, альтернативный и безопасный сберегательный инструмент, обеспечивающий оптимизацию благосостояния домохозяйств, поскольку ЦВЦБ может использоваться и как средство платежа, и при кредитовании. В большинстве государств разработана так называемая двухуровневая модель эмиссии ЦВЦБ, когда центральный банк выпускает ЦВЦБ коммерческим банкам, которые, в свою очередь, распределяют их среди населения, включая потребителей, не охваченных банковскими услугами. Такая модель ЦВЦБ позволяет, в частности, стимулировать открытие банковских счетов, наращивать общее кредитование домохозяйств и т.д. Следует упомянуть также такую форму ЦВЦБ, как «розничные ЦВЦБ» (Retail ЦВЦБ), являющиеся цифровой валютой центрального банка (ЦВЦБ), которая доступна широкому кругу потребителей, поэтому розничные ЦВЦБ иногда именуются «ЦВЦБ общего назначения» или «общедоступные ЦВЦБ». Розничные ЦВЦБ могут использоваться как внутри страны, так и за рубежом, кроме того, доступ к розничным ЦВЦБ могут получить и иностранные лица.

Примечательно, что цифровая валюта ЦВЦБ развивающихся государств может отличаться от ЦВЦБ развитых стран: например, в такой развитой стране как США ЦВЦБ (U.S. CBDC) не внедрена, однако для целей широкого экспертного обсуждения в настоящее время Федеральный резерв США (Federal Reserve) представил документ, в котором рассматриваются плюсы и минусы возможного введения ЦВЦБ [7]. Это связано как с потребностями банковского обслуживания более широких слоёв населения и стимулированием финансовой инклюзивности, так и с необходимостью снижения рисков дезинтермедиации. Риск дезинтермедиации, означающий «процесс устранения финансовых посредников» (банков, финансовых брокеров), охватывает несколько параметров, таких как: а) отказ от финансовых посредников на рынке ссудных капиталов в пользу прямого выпуска ценных бумаг; б) изъятие клиентами депозитов из банков для помещения в инструменты денежного рынка в период роста процентных ставок; в) избежание оттока части кредитных ресурсов за пределы национальной банковской системы; г) устранение ситуаций, когда финансовые институты не обладают возможностью осуществления своих функций посредников [8]. Дезинтермедиация позволяет уменьшить расходы всех участников финансовых операций за счёт платежей комиссии и иных сборов.

Стейблкоины (Stablecoins)

Стейблкоины являются еще одним видом (типом) цифровых валют. Стейблкоины обладают «устойчивой стоимостной стабильностью» в силу того, что они могут, к примеру, поддерживаться фиатной валютой страны (с «привязкой» к стоимости суверенной валюты) либо обеспечиваться стоимостью резервных активов или товаров (таких как золото, нефть, иные виды физических активов) [9, 10]. Стейблкоины рассматриваются также как новый класс криптовалют, основанный на технологии распределённого реестра (Distributed Ledger Technology, DLT), технологическая инфраструктура и протоколы которых обеспечивают одновременный доступ, проверку и обновление записей в сетевой базе данных блокчейнов. С этой точки зрения устойчивость стоимостной стабильности стейблкоинов поддерживается криптоактивами и алгоритмами DLT [11].

В настоящее время одним из известных, крупнейших и популярных стейблкоинов считается Tether (USDT), который был впервые представлен в 2014 году и рассматривался как единственный стейблкоин, доступный для использования. Tether (USDT) выпускается компанией Tether Limited, собственником которой является Bitfinex [12], в свою очередь являющаяся одной из старейших криптовалютных бирж и находящаяся под управлением гонконгской компании iFinex Inc. [13]. Одна единица («монета» - coin) стейблкоина может быть привязана к курсу реальных активов (фиатные деньги, ценные бумаги, иные активы). Так, компания Tether Limited выпускает несколько стейблкоинов, например, с привязкой к курсу доллара США (USDT), евро (EURT), юаня (CNHT), песо (MXNT), а также с привязкой к унции золота (XAUT). При этом, когда речь идёт о стейблкоине USDT, подразумевается его привязка именно к курсу доллара США. По состоянию на начало 2024 года USDT выступал в качестве стейблкоина номер один с рыночной капитализацией около 95 миллиардов долларов и одновременно был третьим по величине криптоактивом (после биткоина и Ethereum). Капитализация других используемых стейблкоинов, таких как USD Coin (USDC), Dai (DAI), значительно меньше и составляет 25 миллиардов и 5 миллиардов долларов соответственно [14].

Новые стейблкоины, например, TrueUSD, USDC, Pax Dollar и Gemini Dollar, были представлены на рынке в 2018 году. Текущая совокупная рыночная капитализация стейблкоинов составляет 153 миллиарда долларов США, и они играют существенную роль на биржах криптоактивов, а также в приложениях децентрализованного финансирования (DeFi) [15].

Необходимость учёта существующих различий между стейблкоинами и криптовалютами решающим образом влияет на разработку и закрепление возможных вариантов их регулирования.

Криптовалюты (Cryptocurrencies)

Криптовалюты (Cryptocurrencies) также являются видом (типом) цифровых валют. Все криптовалюты являются цифровыми валютами, между тем, не все цифровые валюты являются криптовалютами, т.к. именно для криптовалют используется криптография для контроля их создания, защиты и проверки

транзакций в сетевой системе блокчейна. К наиболее известным криптовалютам относятся биткоин и Ethereum.

Представляется важным подчеркнуть, что определение юрисдикционных параметров регулирования криптовалют объективно детерминировано как их «технологической децентрализацией», так и их специфическими особенностями функционирования. В этом смысле показательна нижеследующая таблица.

Цифровые валюты	Криптовалюта
Могут находиться под контролем централизованных органов (правительства, центральные банки).	Не подвержены контролю со стороны централизованных органов власти в силу децентрализации, основанной на технологии блокчейн.
Информация о транзакциях доступна только правительствам, центральным банкам, отправителям и получателям.	Транзакции криптовалют доступны пользователям публичных блокчейнов, за исключением частных.
Нет специальных методов или технологий для защиты цифровых валют.	Криптовалюты используют криптографию и новые решения, такие как «доказательства с нулевым разглашением» (Zero-knowledge proofs, ZKPs), т.е. криптографический метод, используемый для подтверждения информации о фрагменте данных без раскрытия самих данных, для обеспечения безопасности.
Рассматриваются в качестве легитимного платёжного средства и гарантируются правительством страны/центральным банком.	Нормативная неопределённость криптовалют с т.з. «публичной регулируемости» снижает их юридическую силу, в т.ч. в качестве платёжного средства.

Разграничение цифровых валют (с опорой на видовую специфику и регуляторные функции) отражено в ряде зарубежных концептуальных подходов [16], а также находит своё правовое закрепление, в частности, в таком базовом законодательном акте Евросоюза, как Регламент (ЕС) 2023/1114 Европейского парламента и Совета о рынках криптоактивов, вступивший в силу в 2024 году, (известный как «MiCAR» [17]); и, кроме того, зафиксировано в иных документах ЕС, в числе которых, например, Ключевые требования Базеля III к банкам и криптоактивам [18], ряд нормативных актов Центрального банка Евросоюза [19] и т.д.

В юрисдикциях различных государств проблематика определения порядка регулирования использования криптовалют в настоящее время остаётся критически значимой. Ранее высказанный тезис о том, что вопросы определения порядка регулирования использования цифровых валют по-разному решаются в юрисдикциях различных государств, в полной

мере относится к криптовалютам. При этом следует принять во внимание, что уже сложились определённые обобщённые подходы регламентации применения криптовалют, и к их рассмотрению целесообразно обратиться далее.

Возможные варианты параметров юрисдикционного регулирования криптовалют

Первый вариант юрисдикционного регулирования криптовалют *de facto* и *de jure* оставляет формирование и развитие рынка криптовалют в рамках национальной платёжной системы вне регуляторного воздействия со стороны государства. В связи с таким подходом использование криптовалют осуществляется «стихийно», что позволяет одним участникам рынка максимизировать свою прибыль и не учитывать риски других участников рынка цифровых платежей. Исходным для первого варианта является признание того, что «децентрализация» является ключевым параметром использования криптовалют, и это обстоятельство усложняет решение проблем управления финансовой стабильностью в рамках юрисдикции государства. В этой связи центральные банки соответствующих государств, которые определяют денежно-кредитную политику и поддерживают ценовую стабильность фиатных валют, ограничивают свои регуляторные возможности в отношении криптовалют, что охватывает также решение вопросов валютной конкуренции фиатных и цифровых валют в целом.

Первый вариант, с одной стороны, не предусматривает функционирование централизованных механизмов, ограничивающих предложения по использованию любых видов (типов) цифровых валют, соответственно, в условиях отсутствия таких механизмов потенциально возникают широкие возможности быстрого распространения криптовалют, что может создать риски для финансовой стабильности национального рынка платежей, включая гиперинфляцию; с другой стороны, отсутствие централизованных механизмов не исключает введение государством мер т.н. *ex-post*-регулирования. В рассматриваемом варианте криптовалюта зачастую используется как инвестиция, а не как средство платежа, что сопряжено, в частности, с возможностью обмена криптовалюты (к примеру, такой как биткоин) на национальную валюту. Возникающий при этом «эффект замещения» в практическом плане означает, что стоимость биткоина зависит от стоимости национальной валюты, равно как и колебания стоимости биткоина определяются колебаниями стоимости национальной валюты. Такой «эффект замещения» порождает как положительные, так и отрицательные последствия для эффекта благосостояния потребителей (*Wealth effect/ Effects of Cryptocurrency Wealth* [20]).

Второй вариант предусматривает параметры «*ex-ante*-регулирования», когда в рамках конкретной юрисдикции вводятся прямой запрет на использование криптовалюты либо вводятся строгие ограничения контрольно-распорядительного характера для обращения и использования криптовалют. Механизмы запрета/ограничений использования криптовалюты в отдельных юрисдикциях, бесспорно, «нюансированы» и могут охватывать вариативный комплекс следующих мер: полный запрет для всех

лиц держать криптовалюты и использовать криптовалюты при осуществлении расчётов и платежей; запрет майнинга криптовалют; предоставление для ограниченного круга лиц специальных разрешений по использованию криптовалюты, например, только для «квалифицированных инвесторов», но не для граждан; запрет для регулируемых финансовых организаций (банков, кредитно-финансовых организаций) держать криптовалюту на своем балансе, с одновременным разрешением для клиентов таких организаций осуществлять перевод средств на криптоплатформы; запрет первичного размещения криптовалют (Initial Coin Offering, ICO), когда ICO рассматривают как незаконную деятельность; запрет на деятельность криптобирж; запрет оказания криптоуслуг коммерческим банкам.

При втором варианте учитываются два существенных момента: а) функциональная децентрализация обращения и использования криптовалюты и б) криптовалюты не являются традиционными фиатными деньгами, которые эмитируются и контролируются государством (как «денежным сувереном»). В этой связи второй вариант рассматривается рядом государств в качестве такого регуляторного способа, который обеспечивает нивелирование угроз для суверенитета национальной платёжной системы, способствует поддержанию монетарного суверенитета центрального банка страны. Соответственно, вариант, предусматривающий фактический запрет оборота и использования криптовалют, позволяет государствам как минимум управлять финансовой стабильностью и контролировать её в рамках национальной платёжно-расчётной системы; реализовывать денежную политику и поддерживать национальную расчётную единицу (валюту), осуществляя корректировку обращения денежной массы и работы платёжно-расчётной системы.

Рассматриваемый вариант «ex-ante-регулирования» в юрисдикции государств также во многом увязывается с обеспечением защиты от преступной деятельности (торговля наркотиками, взломы, кражи, порнография, финансирование убийств и терроризма, отмывание денег, обход контроля за движением капитала и т.д.). В экспертном сообществе признаётся, что несмотря на вводимые государством технологические запреты и ограничения использования криптовалюты, существующая практика свидетельствует о том, что пользователи находят целый ряд способов получения доступа к криптовалюте, включая её хранение, осуществление транзакций на зарубежных криптовалютных биржах, обмен криптовалют на фиатную валюту государств и т.д. [21].

Третий вариант юрисдикционного регулирования криптовалют исходит не только из необходимости их легитимизации в национальной платёжно-расчётной системе и в банковской деятельности, но также предоставляет криптовалютам возможность играть регулируемую экономическую роль. Для использования криптовалют при третьем варианте в юрисдикции государств устанавливается предсказуемая нормативная среда (Regulatory certainty), рамки которой обеспечивают реализацию целого комплекса мер, в ряду которых можно отметить следующие.

Во-первых, предусматривается возможность поддержки криптовалют со стороны фиатной системы страны, что способствует привлечению инвестиций и масштабирует внедрение инноваций. Во-вторых, легитимизируется деятельность

криптовалютных бирж с установлением для них требований, предусматривающих в том числе обязанность поставщиков цифровых активов собирать данные клиентов и обмениваться данными по транзакциям, превышающим определённые пороговые значения (т.н. Travel Rule [22]); осуществление идентификации корпоративных партнёров криптовалютных бирж; проведение мониторинга транзакций, превышающих определённые пороговые значения. В-третьих, с учётом того, что криптовалюты также являются токенами, создаётся возможность использования «невзаимозаменяемых токенов» (Non-fungible tokens, NFT [23]), т.е. активов, токенизированных через блокчейн (произведения искусства, цифровой контент, видео и т.д.), которые могут торговаться и обмениваться на деньги, криптовалюты или иные NFT. Ключевое отличие криптовалюты от NFT заключается в том, что две криптовалюты из одного блокчейна взаимозаменяемы, тогда как два NFT из одного блокчейна не являются взаимозаменяемыми, хотя могут быть похожими. NFT в настоящее время являются одними из самых популярных токенов (или активов) экосистемы Ethereum.

Четвёртый вариант регулирования рассматривает криптовалюты в качестве законного платёжного средства, т.е. действующей денежной единицы, обращающейся как законное платёжное средство в юрисдикции государства. К примеру, в Сальвадоре, Центральной Африканской Республике [24] биткоин признан в качестве фиатной валюты. При принятии такого рода решения Сальвадором были заявлены следующие цели: осуществить «отход от долларизации», поскольку национальное благосостояние Сальвадора зависит от экономики США и американской денежно-кредитной политики; провести мероприятия, повышающие доступность финансовых инструментов и финансовой прибыли для пользователей Сальвадора; снизить стоимость денежных переводов [25]. Экспертное сообщество достаточно сдержанно оценивает принятое Сальвадором решение относительно биткоина, отмечая определённую «спорность» такого рода решения. Аргументируется это тем, что биткоин в качестве «законного платёжного средства» не является ни достаточным, ни необходимым условием для широкого внедрения этого платёжного инструмента [26]. Кроме того, имеющиеся данные свидетельствуют о том, что принятое решение существенно не изменило приоритеты граждан Сальвадора, поскольку они по-прежнему предпочитают хранить свои ресурсы в долларах.

Подходы к регулированию цифровых валют в российском правовом порядке

В предметном формате настоящей статьи целесообразно достаточно кратко обозначить исходные регуляторные подходы, сформулированные российским законодателем применительно к порядку функционирования национального финансового рынка и сопряжённых с ним информационных прав пользователей, связанных с оборотом и с использованием цифровой валюты. Общий регуляторный подход российского законодателя в рассматриваемой сфере исходит из необходимости введения инструментов «ex-ante-регулирования» (формат которого отмечен нами ранее) с акцентом на установление

публично-правовых нормативных ограничений и запретов, а также безоговорочного расширения контрольно-надзорных полномочий институциональных исполнительных госорганов.

Примечательно, что временной период существования понятия «цифровая валюта» в российском законодательстве не насчитывает даже четырёх лет, при этом основополагающий законодательный акт, принятый еще 31 июля 2020 года и предметно регулирующий использование цифровых финансовых активов, а именно федеральный закон № 259-ФЗ «О цифровых финансовых активах, цифровой валюте» [27] (далее – «закон о финансовых активах, цифровой валюте»), претерпел изменения и с 1 ноября 2024 года будет действовать в новой редакции [28]. Закон о финансовых активах, цифровой валюте опирается на стратегические положения, закреплённые в Концепции законодательного регламентирования механизмов организации оборота цифровых валют (далее – «Концепция оборота цифровых валют») [29], принятой в 2022 году и определившей соответствующие цели и задачи государственного регулирования в рассматриваемой сфере.

При определении порядка регулирования российский законодатель, по сути, не стал учитывать видовую детализацию цифровых валют и, в частности, категориально не стал разграничивать «цифровые валюты» и «криптовалюты», несмотря на тот факт, что отечественные правоведы систематически обращают внимание на необоснованность отождествления этих понятий [30, 31, 32]. Так, согласно закону о финансовых активах, цифровой валюте, «цифровой валютой» признаётся совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей РФ, денежной единицей иностранного государства и (или) международной денежной или расчётной единицей, и (или) в качестве инвестиций, и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему её правилам (п.3 ст. 1).

Представляется возможным обозначить следующие законодательные новации, коснувшиеся таких понятий (включая определение их содержания), как майнинг цифровой валюты; майнинг-пул; лицо, организующее деятельность майнинг-пула; майнинговая инфраструктура; оператор майнинговой инфраструктуры. При этом российский законодатель вносит соответствующие изменения и контрольно-распорядительные меры в отношении осуществления майнинга цифровой валюты. Например, нормативные положения указанного закона № 35-ФЗ предусматривают введение правительством РФ полного и (или) частичного ограничения режима потребления электрической энергии энергопринимающими устройствами, используемыми в целях осуществления майнинга цифровой валюты; запрет для юридических лиц и индивидуальных предпринимателей совмещать осуществление майнинга цифровой валюты с деятельностью по передаче электрической энергии, деятельностью по оперативно-диспетчерскому управлению в электроэнергетике, деятельностью по производству или купле-продаже электрической энергии.

Расширенное ведение контрольно-надзорных полномочий институциональных исполнительных госорганов коснулось не только правительства РФ, а также Минцифры, Минфина, Центрального Банка, Федеральной налоговой службы РФ. В этой связи целесообразно обратить внимание на один из последних по времени принятия подзаконных актов, а конкретно, на постановление правительства РФ от 09.10.2024 № 1347 «О федеральном органе исполнительной власти, уполномоченном устанавливать по согласованию с Центральным банком Российской Федерации запрет и (или) ограничения на совершение сделок с цифровой валютой в целях обеспечения финансовой стабильности Российской Федерации, и федеральном органе исполнительной власти, в который лицо, осуществляющее майнинг цифровой валюты (в том числе участник майнинг-пула), обязано предоставить информацию о получении цифровой валюты в случае выпуска (получения) цифровой валюты в результате майнинга цифровой валюты, а также об адресе-идентификаторе, включая адрес-идентификатор майнинг-пула, и который уполномочен предоставлять такую информацию в федеральный орган исполнительной власти, осуществляющий функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, и Центральный банк Российской Федерации, осуществлять контроль (надзор) за соблюдением требований о её предоставлении и требований, предъявляемых к лицам, организующим деятельность майнинг-пула» [33]. Кроме того, с 1 ноября 2024 года за ФНС России закреплены полномочия, связанные, в частности, с получением от лица, осуществляющего майнинг цифровой валюты (в том числе участника майнинг-пула), информации о получении цифровой валюты в случае выпуска (получения) цифровой валюты в результате майнинга цифровой валюты, а также об адресе-идентификаторе, включая адрес-идентификатор майнинг-пула.

Разумеется, установленный российским законодателем порядок обращения и использования цифровых валют является предметом самостоятельного исследования, так что в формате настоящей статьи возможно лишь общее упоминание о таковом.

Цифровые валюты как новые инструменты, технологические возможности которых призваны создавать новые параметры существующих платёжных систем в целом, разумеется, получают свое развитие и практическое применение. Цифровые валюты расширяют комплекс разнообразных вариантов обращения существующих денежных средств и финансовых активов, дополняя либо заменяя их (в той или иной форме/тем или иным способом), а определение порядка их оборота и использования преимущественно будет определяться юрисдикционными параметрами национальных правовых порядков. ■

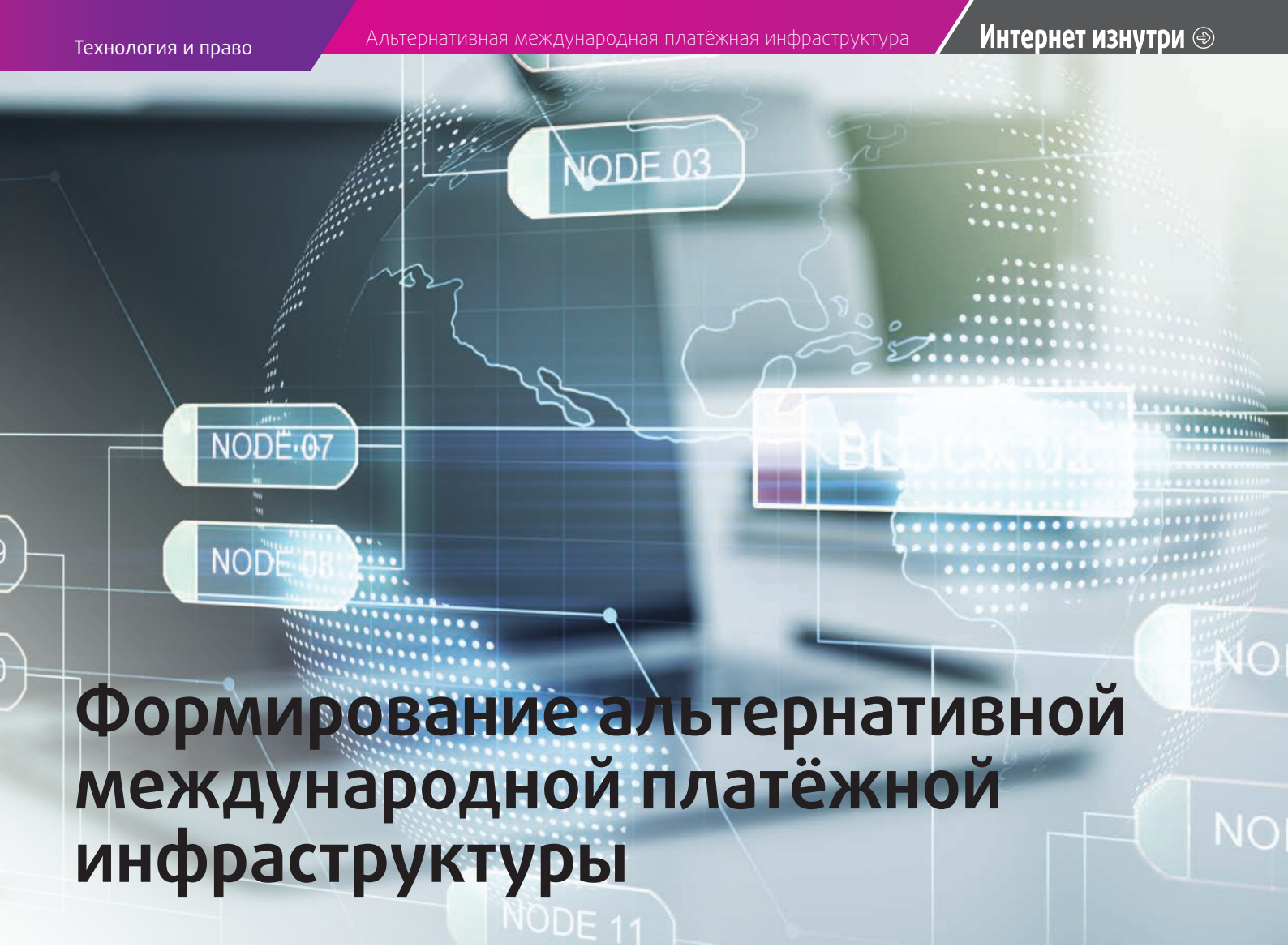
Список литературы:

- [1] Дерюгина Т.В. «Проблемы определения правовой природы цифровой валюты» // Вестник Пермского университета. Юридические науки. 2024. N 2. С. 274–288.
- [2] Обобщённая информация (на 01.10.2024) по странам мира отно-

- сительно разработки, пилотных проектов или запуска ЦБЦБ. URL: <https://www.atlanticcouncil.org/cbdctracker/>
- [3] Digital currencies and the future of the monetary system. URL: <https://www.bis.org/speeches/sp210127.pdf>
- [4] Digital currencies. URL: <https://www.investopedia.com/terms/c/central-bank-digital-currency-cbdc.asp>
- [5] Кочергин Д.А. «Цифровые валюты центральных банков: опыт внедрения цифрового юаня и развитие концепции цифрового рубля» / Д.А. Кочергин // Russian Journal of Economics and Law. 2022. Т. 16. N 1. С. 51-78.
- [6] Сахаров Д.М. «Цифровые валюты центральных банков: ключевые характеристики и влияние на финансовую систему» / Д.М. Сахаров // Финансы: теория и практика. 2021. Т. 25. N 5. С. 133-149.
- [7] US Federal Reserve re U.S. CBDC. URL: <https://www.federalreserve.gov/central-bank-digital-currency.htm>
- [8] Подробнее о дезинтермедиации: <https://provsebanki.ru/>
- [9] The Macroeconomic Impact of Cryptocurrency and Stablecoins. White Paper, July 2022. URL: https://www3.weforum.org/docs/WEF_The_Macroeconomic_Impact_of_Cryptocurrency_and_Stablecoins_2022.pdf
- [10] Бровкина Н.Е. «Кредитный рынок vs децентрализованные финансы: возможности интеграции» // Имущественные отношения в Российской Федерации. 2024. N 3. С. 46-52.
- [11] Distributed Ledger Technology, DLT. URL: [https://www.techtarget.com/searchcio/definition/distributed-ledger#:~:text=Distributed%20ledger%20technology%20\(DLT\)%20is,data%20store%20or%20administration%20of,functionality](https://www.techtarget.com/searchcio/definition/distributed-ledger#:~:text=Distributed%20ledger%20technology%20(DLT)%20is,data%20store%20or%20administration%20of,functionality)
- [12] Bitfinex основана в 2012 году, зарегистрирована на Британских Виргинских островах, с головным офисом, базирующимся в Гонконге. См. подробнее: URL: <https://coinmarketcap.com/exchanges/bitfinex/>, а также см. URL: <https://www.bitfinex.com/about>
- [13] iFinex Inc. https://www.finyear.com/iFinex-Inc-Invests-More-Than-US1M-in-Dusk-Network-s-Security-Token-Exchange-Project_a42784.html
- [14] Swap USD Coin (USDC) to Dai (DAI). URL: [https://zengo.com/swaps/usdc-to-dai/#:~:text=USD%20Coin%20\(USDC\)%20Vs,1%20to%20the%20US%20dollar](https://zengo.com/swaps/usdc-to-dai/#:~:text=USD%20Coin%20(USDC)%20Vs,1%20to%20the%20US%20dollar)
- [15] What Is Decentralized Finance (DeFi) and How Does It Work? URL: <https://www.investopedia.com/decentralized-finance-defi-5113835>
- [16] Digital Currency vs Cryptocurrency: Key Differences. <https://101blockchains.com/digital-currency-vs-cryptocurrency/#:~:text=However%2C%20the%20differences%20between%20them,of%20governments%20and%20central%20banks>
- [17] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU). 2019/1937. (Text with EEA relevance). URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1114> Данный Регламент ЕС (иначе – MiCAR) вводит новую нормативную базу для криптоактивов. MiCAR направлено на защиту потребителей и инвесторов и снижение рисков для финансовой стабильности.
- [18] Key Basel III Requirements for Banks and Crypto Assets. URL: <https://pixelplex.io/blog/basel-iii-requirements/>
- [19] Central bank (EU) digital currency (CBDC) and crypto-assets. URL: <https://www.banque-france.fr/en/governors-interventions/central-bank-digital-currency-cbdc-and-crypto-assets-speech-first-deputy-governor-denis-beau>
- [20] Aiello D, Baker S.R., Balyuk T, Di Maggio M, Johnson M.J. & Jason D. Kotter. The Effects of Cryptocurrency Wealth on Household Consumption and Investment. URL: <https://www.nber.org/papers/w31445>
- [21] Satellite Internet Connection to Start Working in Kazakhstan. URL: <https://timesca.com/satellite-internet-connection-to-start-working-in-kazakhstan/>
- [22] What Is the Crypto Travel Rule, and Why Is It Important? How does the Travel Rule apply to crypto assets & virtual assets providers? URL: <https://notabene.id/crypto-travel-rule-101/what-is-the-crypto-travel-rule#:~:text=The%20Travel%20Rule%20for%20crypto,diligence%20on%20the%20counterparty%20VASP>
- [23] Non-fungible tokens, NFT. URL: <https://www.kraken.com/ru-ru/learn/what-are-non-fungible-tokens-nft>
- [24] Bitcoin Becomes Official Currency in Central African Republic, 27 April 2022: <https://www.bbc.com/news/world-africa-61248809>
- [25] Alvarez, Fernando E., David Argente and Diana van Patten, Are Cryptocurrencies Currencies? Bitcoin as Legal Tender in El Salvador, NBER Working Paper 29968, April 2022: https://www.nber.org/system/files/working_papers/w29968/w29968.pdf Accessed 21 June 2022.
- [26] El Salvador Adopted Bitcoin as an Official Currency; Salvadorans Mostly Shrugged. URL: <https://insights.som.yale.edu/insights/el-salvador-adopted-bitcoin-as-an-official-currency-salvadorans-mostly-shrugged>
- [27] Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». СПС КонсультантПлюс.
- [28] Федеральный закон от 08.08.2024 № 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». СПС КонсультантПлюс.
- [29] Концепция законодательного регламентирования механизмов организации оборота цифровых валют. Текст документа приведён в соответствии с публикацией на сайте <http://static.government.ru> (09.02.2022).
- [30] Брыкин К.И. «Гонка вооружений» цифровыми валютами центральных банков» // Финансовое право. 2024. № 8. С. 18-21.
- [31] Полякова В.Э. «Правовые аспекты майнинга криптовалюты» // СПС КонсультантПлюс.
- [32] Дерюгина Т.В. «Проблемы определения правовой природы цифровой валюты» // Вестник Пермского университета. Юридические науки. 2024. N 2. С. 274-288.
- [33] Постановление правительства РФ от 09.10.2024 № 1347. СПС КонсультантПлюс.

Об авторе

Мадина Балташевна Касенова, доктор юридических наук, профессор кафедры теории и истории частного права ФГБН «Исследовательский центр частного права имени С.С. Алексеева при Президенте РФ», mbk.07@mail.ru DOI: 10.24833/0869-0049-2019-2-41-53



Формирование альтернативной международной платёжной инфраструктуры

Александр Григорьев
Юрий Припачкин



Аннотация

В статье проводится анализ платформенных решений для осуществления международных расчётов, инициированных Банком России в условиях фрагментации глобальной финансовой системы, основанной на системе SWIFT. Подчёркивается, что все эти решения - система СПФС, платформы ЦФА и цифрового рубля, - базирующиеся на фиатном рубле и централизованные по сути, практически исключают возможность их интеграции с аналогичными национальными системами не по технологическим причинам, а из-за отсутствия «доверия» между сторонами.

Авторами предлагается отойти от идеи сопряжения централизованных национальных платформ и реализовать «доверительную среду» между участниками международных расчётов на основе децентрализованной сети блокчейна биткоин. На базе этой информационной инфраструктуры платёжного решения международных платежей должен быть сформирован пул финансовых инструментов (обеспеченных денег), использующих ресурсные токены (стейблкоины), обеспеченные высоколиквидными биржевыми товарами и доверием, в противовес национальным фиатным валютам. Остальные ключевые элементы финансовой инфраструктуры (крипторынки, банки, страховые фирмы...) должны будут функционировать в отдельном финансовом контуре, изолированном от системы SWIFT, контролируемой со стороны США.

Ключевые слова:

трансграничные расчёты, децентрализованные финансы, токены, цифровые финансовые активы, блокчейн, криптовалюты, биткоин, SWIFT

Россию вытеснили с традиционных рынков капитала и лишили доступа к информационной инфраструктуре для международных платежей, что вынудило её искать альтернативные пути для совершения трансграничных расчётов. Российский бизнес сравнительно быстро освоил различные схемы обхода санкций, такие как бартер, перестановки через платёжных агентов и платежи в криптовалюте. Однако попытки Банка России, главного финансового регулятора страны, решить эту проблему на системном уровне пока не привели к значительному прогрессу. С одной стороны, Центральный банк понимает необходимость использования новейших финансовых технологий, но с другой — опасается потери централизованного контроля над движением децентрализованных активов, что приводит к нерешительности в регулировании криптовалют, классическому «шаг вперед, два назад».

В условиях фрагментации некогда глобальной международной платёжной системы, основанной на всеобщем доверии участников, проблемы создания альтернативной информационной инфраструктуры трансграничных платежей, базирующейся на национальных стандартах, без единого оператора (типа SWIFT), носят скорее концептуальный, чем технологический характер. Не хватает ясного представления о том, как различные инициативы должны интегрироваться, какой должна быть новая информационная и финансовая инфраструктура, а также, как она должна функционировать и взаимодействовать с традиционными финансовыми институтами и инструментами.

В этих обстоятельствах ряд стран инициировали международные проекты, которые обеспечивают целостность и работоспособность финансовой инфраструктуры этих стран и могут быть предложены зарубежным партнёрам в качестве системы трансграничных расчетов.

Система передачи финансовых сообщений (СПФС), отечественный аналог международной системы передачи информации и совершения платежей SWIFT, была разработана в ответ на усиление санкционного давления на экономику страны, что значительно ускорило её создание в 2014 году. Основанная на традиционной централизованной архитектуре, за 10 лет своего существования российская СПФС объединила более 550 банков из 20 стран [1].

Ещё раньше Иран столкнулся с аналогичной ситуацией и в 2013 году разработал собственную систему SEPAM (System for Electronic Payments Messaging), которая сейчас включает девять стран-участниц [2].

Китай, несмотря на значительную интеграцию своей финансовой инфраструктуры с системой SWIFT, в 2015 году запустил CIPS (Cross-border Interbank Payment System). Эта система обеспечивает клиринг и расчёты, способствуя глобальному использованию китайской валюты в трансграничных расчётах. На сегодняшний день она охватывает более 4700 банковских учреждений в 184 странах и регионах мира [3].

Индия запустила свою национальную систему структурированных финансовых сообщений SFMS (Structured

Financial Messaging System) ещё в 2001 году. Это модульное программное обеспечение с поддержкой Интернета и гибкой архитектурой, облегчающей как централизованное, так и распределённое развёртывание. Благодаря своей модульности и интеграции с Индийской финансовой сетью (INFINET), эта система имеет хорошие шансы потеснить SWIFT, особенно среди стран глобального большинства и Глобального Юга. Однако индийские банки воздержались от интеграции с СПФС Банка России из опасений, что это может быть воспринято как попытка обойти санкции США против российских банков [4].

Увеличение числа таких систем, с одной стороны, должно способствовать развитию рынка. Однако, с другой стороны, это неизбежно приведёт к росту издержек для компаний, которые будут вынуждены работать в нескольких сетях. Им станет сложнее взаимозаменять транзакции и поддерживать ликвидность в каждой сети. Поэтому борьба за доминирование той или иной платёжной системы может привести к замене SWIFT на ещё более централизованную систему регулирования.

Именно по этой причине доля национальных информационных систем в мировом платёжном балансе, по разным оценкам, не превышает 2-3% [5]. Даже платежи в юанях, включая операции с Гонконгом, в большинстве случаев проходят через систему SWIFT, а не через китайскую CIPS [6].

Несмотря на значительные технологические сложности интеграции национальных систем передачи финансовых сообщений, такие как фрагментированность форматов данных, отсутствие согласованных платёжных стандартов и различия в подходах к комплаенсу и безопасности, сохраняется основная проблема — централизованный контроль и управление. По сути, решение о том, подключать ли российскую СПФС к другим национальным системам, принимается в США, что изолирует вполне конкурентную российскую систему в рамках границ Российской Федерации и ближайших союзников.

Цифровые финансовые активы (ЦФА). Движение в сторону цифровизации финансов и создание отечественной инфраструктуры для обращения цифровых финансовых активов (ЦФА) на основе платформенных решений российских компаний привели к формированию Банком России двух реестров: операторов информационных систем (на сегодня их 11) и операторов обмена ЦФА (2).

Несмотря на значительный рост эмиссии ЦФА в 2024 году, более 98% всех выпусков представляют собой обычные денежные требования, которые во многом похожи на банковские депозиты, ориентированные в основном на внутренний рынок и мало интересные внешним инвесторам. Определённые перспективы выхода российских ЦФА на зарубежные рынки связывают с Законом о майнинге цифровых валют, об иностранных ЦФА в России и о российских ЦФА за рубежом [7].

Этот закон упрощает использование российских цифровых активов на международном уровне, разрешая их

оборот на иностранных платформах. Для этого вводится понятие «иностранный номинальный держатель ЦФА». В эту категорию попадают платформы для торговли криптовалютами, а также сервисы для хранения цифровых активов и управления ими.

Также закон позволяет иностранным ЦФА обращаться в России. Допуск к обращению разрешён на площадках российских операторов по выпуску ЦФА при условии квалификации российским оператором таких иностранных активов.

Банк России обладает полномочиями устанавливать специфические особенности учёта и обращения ЦФА, а также определять требования и запреты на признание иностранных цифровых прав.

Время покажет, сможет ли новый закон сделать российский рынок цифровых финансовых активов более привлекательным для иностранных инвесторов и откроет ли он возможность использовать ЦФА, эмитированные в России, в международных расчётах.

Цифровая валюта центрального банка CBDC (Central bank digital currency) – цифровой аналог национальных фиатных валют, которые эмитируются, регулируются и гарантируются центробанками (ЦБ). CBDC, несмотря на то, что используют в своей основе технологии распределённых реестров, представляют собой своеобразный ответ центральных банков внешним угрозам, связанным со стремительным развитием финтех, особенно в области децентрализованных финансов – DeFi. По сути, это высшая форма централизации денежного обращения, обеспечивающая финансовым регуляторам тотальный контроль и абсолютную власть над движением этой формы национальной валюты.

Однако эта власть перекладывает на ЦБ и все технологические риски, в первую очередь, в области информационной безопасности и конфиденциальности, за которые так или иначе будут расплачиваться налогоплательщики. Единая точка отказа в значительной степени увеличивает риски кибератак, повышая уязвимость CBDC со всеми вытекающими последствиями.

Тем не менее, использование национальных CBDC в трансграничных расчётах в случае решения технологических вопросов сопряжения позволило бы исключить необходимость использования корсчетов в банках США за счёт выстраивания прямых P2P-платежей между организациями.

В настоящее время наиболее активно развиваются три цифровые валюты: китайский цифровой юань (e-CNY), гонконгский цифровой доллар (e-HKD) и российский цифровой рубль. Если цифровой рубль ещё находится в стадии тестирования и в массовый оборот начнёт поступать не ранее июля 2025 года, то объём транзакций с цифровым юанем в 2024 году уже достиг 986 миллиардов долларов [8].

Решение технологической совместимости CBDC, реали-

зованное в проекте моста платежной системы, mBridge (Multiple CBDC Bridge), заключается в использовании мультимодальной модели CBDC с прямым доступом в реальном времени. Это общая техническая инфраструктура, в которой размещено несколько CBDC и которая обеспечивает масштабируемое трансграничное соглашение с несколькими CBDC.

Протокол платформы проекта выстроен на собственном блокчейне mBridge Ledger и предназначен для обеспечения соответствия требованиям законодательства и политики конкретной юрисдикции. Конфиденциальные данные в реестре передаются только по принципу служебной необходимости, так что детали конкретной транзакции известны только участникам транзакции и их центральным банкам [9]. Соответственно, ни одна страна на этой платформе не может ввести какие-либо санкции против другой.

Разработка проекта mBridge началась в 2021 году Банком международных расчётов – БМР (Bank for International Settlements – BIS), «центральным банком для центральных банков», совместно с центральными банками Китая, Гонконга, Таиланда и Объединённых Арабских Эмиратов и достигла стадии минимального жизнеспособного продукта (MVP) в июне 2024 года. Тем не менее, 28 октября этого года руководством BIS обсуждалась возможность закрытия проекта после сообщений о возможности подключения к нему стран-членов БРИКС, находящихся под санкциям США [10].

Как дальше будет развиваться этот проект, останется ли он политически нейтральным или будет использован для создания параллельных, конкурирующих систем, с учётом того, что Китай играет ведущую роль в разработке его программного обеспечения и кода, пока не ясно.

Токены, обеспеченные резервными валютами на публичных блокчейнах (стейблкоины). Ограниченный доступ к CBDC для широкого круга пользователей во многом связан с тем, что национальные центральные банки полностью контролируют транзакции и цифровые кошельки через собственные блокчейны. Они стараются максимально ограничить доступ к своим цифровым валютам для нерезидентов, в частности, с тем, чтобы минимизировать возможность вывода капитала за пределы страны и избежать проблем с конвертацией курса национальной валюты.

Во многом эти ограничения снимаются благодаря решениям частных компаний, которые выпускают токены, обеспеченные долларом США и представленные в виде цифровых прав. Эти компании не создают собственные блокчейны и цифровые кошельки, а используют существующие популярные публичные блокчейны и криптокошельки. Соответственно, приобретать эти токены может практически неограниченный круг пользователей, прошедший процедуру KYC (набор проверок Know Your Customer) на известных криптобиржах, независимо от юрисдикции и с минимальными организационными усилиями. С большим отрывом в этом ряду лидирует стейблкоин USDT компании Tether. Его рыночная доля в 2024 году,

несмотря на некоторое падение, составила 74% (рыночная доля ближайшего конкурента, USDC – 12%) [11].

Этот стейблкоин широко используется в международных расчётах, в том числе многими российскими компаниями и частными лицами. Тем не менее, для российских пользователей существуют серьёзные риски полной блокировки этих токенов со стороны компаний-эмитентов даже на их холодных криптокошельках. К настоящему времени Tether заблокировала 1,2 миллиарда USDT, находящихся на 1731 кошельке «чёрного списка» [12]. Несмотря на то, что кошельки этого списка в большинстве случаев использовались в мошеннических схемах, централизованный контроль над стейблкоином противоречит принципам децентрализации, лежащим в основе криптовалют, и может быть использован против любых неугодных персон, в том числе по политическим мотивам.

В сложившейся ситуации использование российским бизнесом токенизированных финансовых инструментов типа USDT, USDC и т.п., находящихся под регулированием США и их союзников, с целью обхода их же санкций, становится всё более рискованным. Даже если сейчас эти активы ещё не блокируются со стороны компаний-эмитентов, то в ближайшей перспективе, по мере усиления антироссийских санкций, этот процесс может стать более чем вероятным.

Во всех рассмотренных проектах попытки главного финансового регулятора Российской Федерации сформировать отдельную централизованную отечественную инфраструктуру, полностью контролируруемую Банком России, и встроить её в международную платёжную систему для осуществления альтернативных трансграничных расчётов, будь то система СПФС, платформы ЦФА или цифрового рубля, блокируются со стороны таких же западных финансовых регуляторов, полностью контролируемых со стороны США и их союзников.

Очевидно, что в условиях острейшего геополитического кризиса подобная ситуация с внедрением централизованных систем, контролируемых Банком России, на международный уровень будет только усугубляться. Однако решение у этой проблемы есть, и лежит оно в плоскости полностью децентрализованных платформ, полного контроля над которыми нет ни у российских финансовых регуляторов, ни у западных. В первую очередь это биткоин (BTC), который до сих пор остается эталоном децентрализованных финансов.

В этой связи нужно отдать должное российским майнерам, которые, несмотря на долгий период правовой неопределённости, смогли выйти в лидеры международных добытчиков BTC. Благодаря им российский сектор крипторынка может получать BTC напрямую, минуя обращения к зарубежным криптобиржам. Этим ресурсом начинает активно пользоваться российский бизнес для осуществления трансграничных расчётов.

Однако объём добытой майнерами криптовалюты слишком мал для того, чтобы составить серьёзную конкурен-

цию доллару и другим резервным валютам в мировой торговле. На сегодня в мире добыто около 19,75 миллионов BTC, из которых практически не участвуют в обороте (потеряны приватные ключи, или биткоины находятся на длительном хранении) до 7,78 миллиона BTC [13]. Иными словами, в активном обороте может находиться не более 12 миллионов BTC, что по текущему курсу составляет около 815 миллиардов долларов. С учётом того, что общий объём мировой торговли в 2023 году составил 30,4 триллиона долларов [14], BTC в пределе сможет заместить не более 2,7% этой величины.

Значительно более ценным ресурсом, чем монетки BTC, необходимые больше для мотивации самих майнеров и хранения ценностей, является сама инфраструктура сети BTC и её функционал, который ещё до конца не реализован в сегменте DeFi-приложений. В частности, благодаря российским майнерам поддерживается децентрализованный характер блокчейна биткоин и невозможность манипулирования со стороны доминирующего игрока, каким сегодня являются США, сосредоточившие около 26,6% мирового хешрейта [15]. Доля России, занимающей второе место по объёму мирового хешрейта, составляет 14-17% и растёт опережающими темпами [16]. Соответственно, риск «атаки 51%» для сети биткоина практически исключён [17].

Следует особо отметить, что Ethereum, вторая по популярности криптовалюта – в значительной степени благодаря широкому распространению протокола ERC20, используемого в смарт-контрактах, – после перехода на алгоритм консенсуса PoS (Proof-of-Stake) перестал отвечать базовому принципу криптовалют – децентрализации, обеспечивающей, в первую очередь, независимость от внешнего регулирования и политического манипулирования.

Смена алгоритма майнинга в 2022 году привела к переходу функций обеспечения безопасности сети и эмиссии монет от майнеров к валидаторам, которые начали массово использовать для запуска нод централизованные облачные сервисы. Растущий уровень контроля Ethereum со стороны централизованных платформ вызывает беспокойство уже не только со стороны криптосообщества, но и у сооснователя сети Виталика Бутерина [18]. По мнению многих экспертов, такое положение делает блокчейн второй по капитализации криптовалюты уязвимым для централизованной точки отказа [19].

Итак, ключевая информационная сеть, на основе которой будет построена альтернативная международная платёжная инфраструктура, уже создана и успешно функционирует, несмотря на неоднозначное отношение к ней со стороны российских финансовых регуляторов. Речь идёт о блокчейне BTC.

Важно отметить, что благодаря усилиям российских майнеров, эта сеть уже почти на 17% «отечественная» – принадлежит отечественным разработчикам. Это означает, что применение санкций к нашей или любой другой стране, использующей эту информационную сеть, становится практически невозможным.

Интерес к блокчейну биткоин стал стремительно расти буквально в последнее время с появлением новых проектов, направленных на расширение функционала и улучшение доступности BTC, не изменяя при этом его основного программного кода. К ним относятся смарт-контракты, децентрализованные финансовые протоколы (DeFi), аналоги NFT и многое другое [20].

Использование программного слоя Omni Layer, протоколов Nostr и Lightning позволяет сформировать верхнеуровневую инфраструктуру платёжных каналов и шлюзов без добавления транзакции в блокчейн, сохраняя при этом безопасность и неизменность блокчейна и повышая эффективность финансовых инструментов:

- минимизация комиссии и увеличение скорости транзакций;
- ограничение возможности внешнего цензурирования транзакций и их блокировки;
- открывает новые возможности для децентрализованных приложений и сервисов.

Проект Ordinals, позволяющий выпускать токены на базе блокчейна биткоина, и экспериментальный стандарт BRC20 (2023 год), а также Runes обусловили взлёт популярности и активности в развитии инфраструктуры DeFi экосистем на базе BTC [21].

Благодаря этим технологическим инновациям, связанным с решениями второго уровня L2 (Lightning Network) – общие среды смарт-контрактов, построенные поверх сети BTC, – появилась возможность формирования платёжной инфраструктуры, обеспечивающей доверие и равноправие между участниками финансовых транзакций, и при этом обеспечивается невозможность доминирования, а тем более наложения санкций какой-либо стороной.

В качестве основных финансовых инструментов в этой сети могли бы выступить ресурсные токены, обеспеченные высоколиквидными биржевыми ресурсами (ископаемые, минеральные, сельскохозяйственные...), по совокупному объёму которых Россия занимает лидирующие позиции в мире. По сути, речь идет о формировании пула неэмиссионных обеспеченных денег, обладающих внутренней ценностью и ценовой устойчивостью, не привязанных ни к одной резервной валюте и лишённых инфляционных рисков фиатных валют.

Оборот таких активов возможен в выделенном контуре, изолированно от традиционной национальной валюты – рубля, чтобы не допустить ускорения инфляционных процессов [23]. Аналоги ресурсных токенов могут использоваться как во внутреннем инвестиционном контуре страны, так и для торговли на международных рынках.

Для полноценного оборота этих платёжных инструментов и сопряжения с традиционной финансовой инфраструктурой необходимо наличие лояльных проекту криптобирж. С учётом жесточайших западных санкций, любая зару-

бежная биржа, решившая залистить эти токены, неизбежно подпадет под действие вторичных санкций. Поэтому для создания полноценной платёжной экосистемы необходимо планировать формирование обменных площадок и криптобирж, изолированных от традиционной платёжной инфраструктуры, использующей SWIFT и другие контролируемые западными регуляторами системы.

И если банков, попавших под западные санкции, уже немало, то действительно независимые от регуляторов США криптобиржи и другие финансовые учреждения, обслуживающие централизованные шлюзы между реальными и цифровыми (токенизированными) активами, а также децентрализованные площадки и сервисы ещё придётся формировать.

Иными словами, речь может идти об инициации со стороны РФ становления обособленной финансовой инфраструктуры, обслуживающей оборот обеспеченных цифровых денег, участвующих в трансграничных расчётах, на базе децентрализованной сети блокчейна BTC. В формировании подобного финансового контура в первую очередь заинтересованы страны, так или иначе уже «изолированные» от международных финансовых институтов и инструментов – Россия, Иран, Венесуэла, условно Китай и т.д., а также множество неприсоединившихся стран «Глобального Юга».

Список литературы:

- [1] Чернышова Е. «ЕС ввел санкции против российского аналога SWIFT. Что важно знать». [Электронный ресурс]//РБК. – URL: <https://www.rbc.ru/finances/24/06/2024/667934579a79470dd2abf53d> (24.06.2024)
- [2] Азиатский клиринговый союз [Электронный ресурс]//Википедия – URL: https://ru.m.wikipedia.org/wiki/Азиатский_клиринговый_союз#Система_SEPAM (15.01.2024)
- [3] CIPS Cross-Border Interbank Payment System [Электронный ресурс]//Home – URL: https://www.cips.com.cn/en/2024-08/01/article_2024080115043180408.html (дата обращения 01.11.2024)
- [4] Тихомиров В. «Индийские банки не поддерживают идею интеграцию Системы передачи финансовых сообщений (СПФС) Банка России с её индийским аналогом SFMS, внутренней системой передачи финансовой информации и совершения платежей, поскольку это может быть истолковано как попытка обойти санкции США на российские банки». [Электронный ресурс]//Лигабанков – URL: <https://ligabankov.ru/lo/indiyskie-banki-ne-podderzhivayut-ideyu-integraciyu-sistemy-peredachi-finansovoyh-soobscheniy-spfs-banka-rossii-s-ee-indiyskim-analogom-sfms-vnutrenney-sistemoy-peredachi-finansovoy-informacii-i-sovers> (12.08.2022)
- [5] Осадченко М. «Какая доля мировых платежей может идти в обход SWIFT?» [Электронный ресурс]//Дзен – URL: <https://dzen.ru/a/ZaOdf4roBxRn1WkI> (14.01.2024)

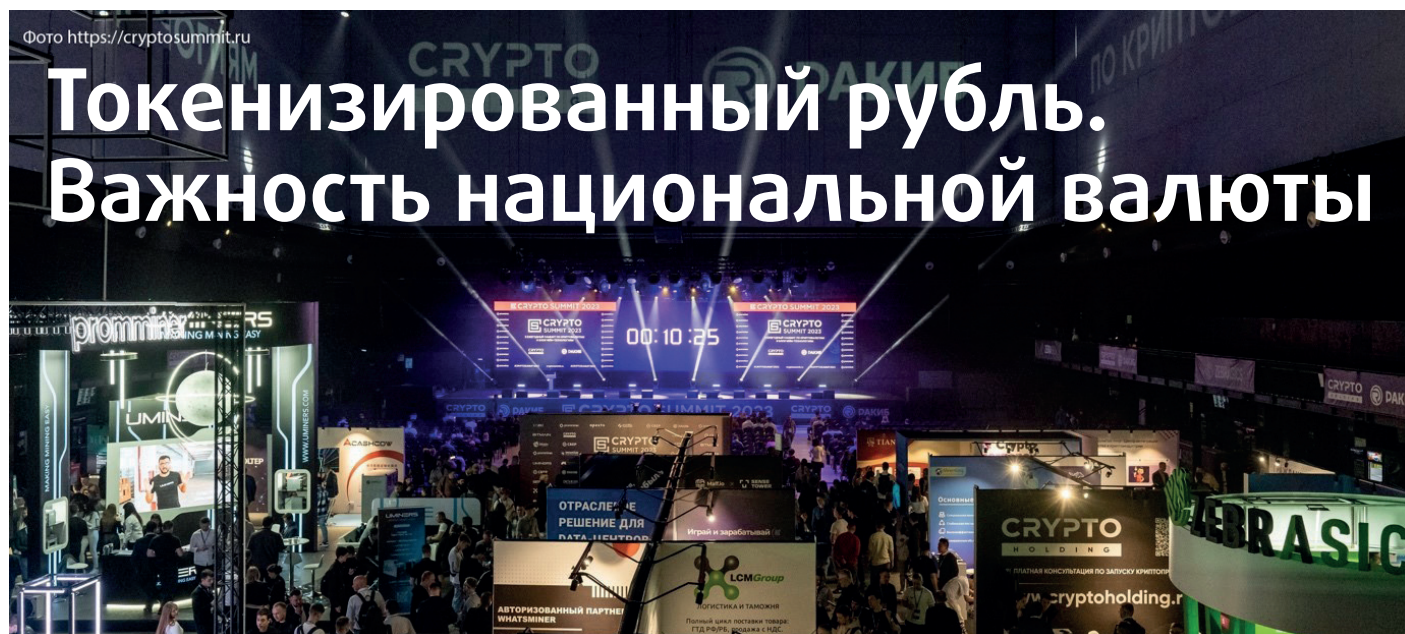
- [6] Рязанцев А. «Как и зачем мы сделали базу данных по банковским переводам в Китай и Гонконг, до которой не дошли руки у банков». [Электронный ресурс]// VC.RU – URL: <https://vc.ru/marketplace/438576-kak-i-zachem-my-sdelali-bazu-dannyh-po-bankovskim-perevodam-v-kitai-i-gonkong-do-kotoroi-ne-doshli-ruki-u-bankov> (08.06.2022)
- [7] Федеральный закон от 08.08.2024 N 221-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». [Электронный ресурс]// КонсультантПлюс– URL: https://www.consultant.ru/document/cons_doc_LAW_482417/ (08.08.2024)
- [8] Достов В. «Песчаный доллар и другие цифровые валюты». [Электронный ресурс]// Коммерсантъ – URL: <https://www.kommersant.ru/doc/7219475> (17.10.2024)
- [9] Маслов А. «Цифровые валюты в международных расчётах: проект mBridge». [Электронный ресурс]// Ассоциация банков России – URL: <https://asros.ru/news/opinions/tsifrovye-valyuty-v-mezhdunarodnykh-raschetakh-proekt-mbridge/> (04.06.2024)
- [10] Parikshit M. As BIS Mulls Shutting Down mBridge, Its Innovation Hub Calls The Project a ‘Public Good’ [Электронный ресурс]// Coindesk – URL: <https://www.coindesk.com/policy/2024/10/29/as-bis-mulls-shutting-down-mbridge-its-innovation-hub-calls-the-project-a-public-good/> (29.10.2024)
- [11] «Tether (USDT) теряет позиции на централизованных биржах, доля рынка упала до 74%». [Электронный ресурс]// Binance Square – URL: <https://www.binance.com/ru/square/post/10787423930890> (14.07.2024)
- [12] «Tether заморозила \$28 млн USDT, связанных с азиатской мошеннической схемой». [Электронный ресурс]// ВКонтакте – URL: https://vk.com/wall-122422421_21418 (13.07.2024)
- [13] Лукин Е. «Сколько всего Биткоинов в мире на сегодняшний день». [Электронный ресурс]// Cripto.ru – URL: <https://crypto.ru/skolko-vsego-bitcoin-v-mire/> (10.10.2024)
- [14] Опубликован годовой отчет ВТО за 2023 г. по объемам мировой торговли товарами и услугами. [Электронный ресурс]// Агентство внешнеэкономической деятельности – URL: <https://eximagency.by/news/opublikovan-godovoj-otchet-vto-za-2023-gro-obemam-mirovoj-torgovli-tovarami-i-uslugami/> (дата обращения 01.11.2024)
- [15] U.S.-Listed Bitcoin Miners’ Share of Global Hashrate Reached Record in July: JPMorgan — TradingView News [Электронный ресурс]// Coindesk – URL: <https://www.tradingview.com/news/coindesk:379c43c99094b:0-u-s-listed-bitcoin-miners-share-of-global-hashrate-reached-record-in-july-jpmorgan/> (16.07.2024)
- [16] Рейтинг российских майнинговых компаний 2024 года по выручке и объемам мощности. [Электронный ресурс]// РБК.Крипто – URL: <https://www.rbc.ru/crypto/news/664c660b9a794733dfeca36a?from=copy> (27.05.2024)
- [17] Лапушкин А. «Как избежать монополизацию биткоина: все об атаке 51%». [Электронный ресурс]// Maff – URL: https://maff.io/media/chto_takoe_attack_51/ (15.05.2020)
- [18] Иванов М. «Ethereum на PoS - централизованная система в самом уродливом виде». [Электронный ресурс]// Крипто на vc.ru – URL: <https://vc.ru/crypto/476637-ethereum-na-pos-centralizovannaya-sistema-v-samom-urodlivom-vide> (05.08.2022)
- [19] Петров Р. «Год после The Merge: дефляционная Ethereum и проблемы централизации». [Электронный ресурс]// Forklog – URL: <https://forklog.com/> (15.09.2023)
- [20] Забавников Б. «Главные тренды рынка криптовалют 2024 году. Часть 2». [Электронный ресурс]// РБК.Крипто – URL: <https://www.rbc.ru/crypto/news/66519fe79a79473546b08b2c> (25.05.2024)
- [21] Олег Cash Coin «Нужно стейкать золото: как майнеры биткои-на меняют рынок DeFi». [Электронный ресурс]// Forklog – URL: <https://forklog.com/exclusive/nuzhno-bolshe-zolota-kak-majnery-bitkoina-menyayut-rynok-defi> (26.06.2024)
- [22] Прогнозы развития блокчейн-технологий на 2024 год от экспертов Ripple, Coinbase, a16z и Starknet. [Электронный ресурс]// Блокчейн24 – URL: <https://www.block-chain24.com/articles/prognozy-razvitiya-blokcheyn-tehnologiy-na-2024-god-ot-ekspertov-ripple-coinbase-a16z-i> (31.12.2023)
- [23] Рябухин С.Н., Минченков М.А., Водянова В.В., Заплетин М.П. «Двухконтурная валютно-финансовая система как инструмент развития национальной экономики Российской Федерации и обеспечения её суверенитета». [Электронный ресурс]// Электронная библиотека КиберЛенинка – URL: <https://cyberleninka.ru/article/n/dvuhkonturnaya-valyutno-finansovaya-sistema-kak-instrument-razvitiya-natsionalnoy-ekonomiki-rossiyskoy-federatsii-i-obespecheniya> (дата обращения 01.11.2024)

Об авторах

Григорьев Александр Аркадьевич, к.х.н. РАКИБ, Россия, Санкт-Петербург, chiefdux@yandex.ru

Припачкин Юрий Игоревич, д.т.н., лауреат премии Ленинского комсомола в области науки и техники, лауреат премии Правительства РФ в области науки и техники, РАКИБ, Россия, Москва, pripachkin@yandex.ru





Дмитрий Мариничев



От редакции

В конце сентября 2024 года в Москве состоялся V Crypto Summit, который традиционно является крупнейшим в России ежегодным событием по криптовалютам и блокчейн-технологиям. Основная цель мероприятия – объединение экспертов и участников отрасли, совместная выработка общего плана развития индустрии на ближайшие годы.

Спикерами и участниками саммита стали лидеры отрасли, представители государственных органов и ведомств. Весьма содержательным получился уже самый первый день работы саммита, в программе которого была пленарная сессия и оживлённая панельная дискуссия, вызвавшая большой интерес у аудитории.

Практически все выступления на пленарной сессии были яркими и запоминающимися. Но сегодня мы хотим познакомить вас, уважаемые читатели, с основными тезисами доклада Дмитрия Мариничева – представителя уполномоченного при президенте РФ по защите прав предпринимателей в сфере Интернета. Нам представляется, что идеи, высказанные спикером, обращают на себя внимание своей оригинальностью и приглашают к размышлениям, что на наш взгляд является хорошим поводом к переосмыслению перспектив развития отрасли цифровых финансовых активов в стране и мире.

Ключевые слова:

блокчейн, законодательство, децентрализация, криптовалюта, майнинг, пул, рубль, токенизация, финансовая система, экономика

Сегодня никому не требуется подробно разъяснять последствия проблем, которые возникли перед экономикой страны и перед бизнесом: тотальный набор ограничений и санкционная политика, невозможность проведения международных платежей и всего, что с этим связано.

Как известно, в конце лета был принят закон, который внёс достаточно существенные поправки в регулирование крипторынка, легализовал майнинг и, соответственно, легализовал криптовалюту – пока в экспериментальных правовых режимах (ЭПР). Но на сегодняшний день нет полной ясности, как этот механизм должен функционировать и кто будет находиться

в авангарде процесса. Однако следует признать, что сделано уже достаточно много полезного. Майнеры криптовалюты получили возможность не только «добывать» биткоин, но и конвертировать его в национальную валюту. Но не появятся ли теперь новые проблемы для самого майнинга, для майнеров и для индустрии в целом?

Многие интересанты ошибочно полагают, что криптовалютный рынок или вообще криптовалютная индустрия – это полноценно работающая децентрализованная система, и майнинг биткоина – в том числе. Мнение, что он ни от кого не зависит, – это иллюзия. Трансграничная торговля посредством платежей в криптовалюте не является панацеей от ограничений по использованию международной платёжной системы SWIFT. Какие бы лидирующие позиции ни занимала страна в майнинге, например, биткоина, это не означает, что блокчейн реально подчинён солидарному контролю. На самом деле, все процессы контролируют майнинговые пулы. А пул в большинстве случаев – это программно-аппаратный сервис, которым кто-то владеет. Значит, с одной стороны, это обстоятельство

Федеральный закон №115-ФЗ от 7 августа 2001 года

регулирующий противодействие легализации доходов, полученных преступным путем, и финансированию терроризма, теперь включает положения о мониторинге цифровых валют, таких как биткоин, и ведении списка адресов, используемых для операций, связанных с отмыванием денег и финансированием терроризма.



Изменение в Федеральный закон №259-ФЗ «О Цифровых финансовых активах»

позволяет легализовать майнинг и продажу добытых криптовалют через иностранные биржи. Экспорт криптовалюты теперь возможен с соблюдением налогового законодательства, а регионы могут вводить ограничения на майнинг для предотвращения перегрузок энергосистем.

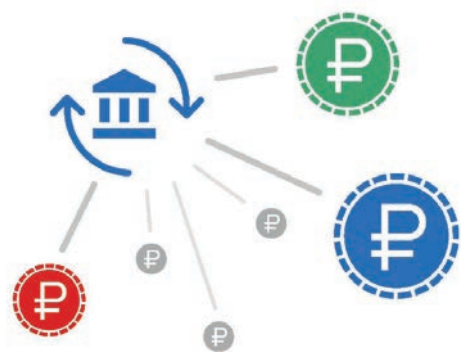
несёт потенциальные риски недобросовестного сговора майнинговых пулов, а с другой - пул или его владелец точно так же может быть подвержен санкционному давлению и ограничениям.

Представленная к обсуждению идея заключается в предложении по-настоящему «рассыпать» структуру сети в децентрализованную, фактически вернув майнинг в «соло-режим», тем самым обезопасив индустрию от какого-либо внутреннего или внешнего влияния. Это предложение, увы, не вполне совпадает с логикой закона, принятого в августе. Однако в качестве аргумента приводится заключение, что у децентрализованных систем гораздо больше преимуществ безопасности, возможностей, стабильности и непрерывности ведения бизнеса. И поэтому в рамках реализации нового законодательства о цифровых финансовых активах (ЦФА) предлагается обратить внимание государственных регуляторов на необходимость привлечения для работы в ЭПР именно профессиональных участников рынка, а не формально назначенных или избранных и не имеющих в криптоиндустрии достаточного опыта и авторитета.

Технология токенизации на блокчейне позволяет предоставлять в цифровом виде право собственности на любой материальный или нематериальный актив, в частности, на деньги. Очевидно, что в нынешних условиях без оглядки использовать для расчетов Tether, USDT или любой другой стейблкоин рискованно, потому что в какой-то момент транзакции в нём могут быть неожиданно заморожены, а кошельки заблокированы. Потому что, как уже говорилось, все они суть подконтрольные системы.

В таком случае разумно и рационально выпустить собственный токенизированный рубль. Технологически это можно было бы осуществить на блокчейне биткоина. А поскольку в этом случае интерес представляет только блокчейн и те записи, которые в нём производятся, то и нет конфликта с законом. Ведь становится не важно, кто и как влияет на сеть биткоина. Наличие серьёзных майнинговых мощностей на территории России позволяет не только поддерживать надёжность этой цепочки, но и противостоять «атаке 51%», когда некто может захватить контроль над вычислительной мощностью сети и, соответственно, над подтверждением транзакций и генерацией блоков в блокчейне.

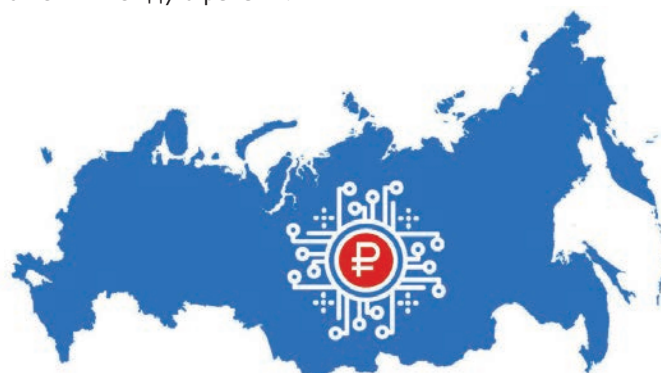
Выпуская поверх блокчейна биткоина нечто похожее на Colored Coin или Omni, можно использовать достаточно стандартизованный и уже хорошо зарекомендовавший себя на практике сервис. Тем самым нивелируются риски продвижения чего-то новоизобретённого и непроверенного.



Подчёркивается, что «токенизированный» рубль - это не цифровой рубль. Цифровой рубль – форма ЦФА, контролируемая государством в лице Центрального банка РФ. Этот рубль уже внедряется в нашу жизнь, но он не ставит своей целью преодоление всех вызовов, стоящих перед страной. Токенизированный рубль при этом не вступает в противоречие со стратегией Центрального банка. Он не меняет представление о том, как должны эмитироваться валюты, а использует только то, что уже фактически произошло в эмиссии. Таким образом, появляется другая точка зрения на то, как ещё можно осуществлять трансграничные расчёты для обеспечения международных торговых операций.

При оговорённых условиях токенизированный рубль на базе блокчейна биткоина может стать полностью децентрализованным и не потребует каких-либо специальных интеграций в площадки централизованных или децентрализованных бирж. То есть это то, что должно заработать сразу.

И тогда майнинг начнёт играть действительно новую полезную роль, поскольку из непонятной для государства формы потребления электроэнергии и непонятных ему «гиков»-участников, «использующих технические средства для того, чтобы добывать биткоин», он становится важной частью отрасли, которая обеспечивает инфраструктуру финансовых отношений между странами.



Если государство поддержит идею токенизированного рубля как средства платежа (что сегодня пока законодательно запрещено), то позитивные изменения не заставят себя долго ждать, и импортеры/экспортеры смогут использовать этот инструмент для своих международных операций. Интересно и то, что гипотетически в цепочку добавленной стоимости смогут встраиваться любые экономические субъекты по всему миру, потому что они получают возможность использовать цифровые деньги, обеспеченные государством. А это в свою очередь позволит в любой момент времени обменивать их на криптовалюту или на любой фиат на мировых торговых площадках, а также будет гарантировать, что обычные пользователи компании и бизнесы смогут встраиваться в эти цепочки. Значит, появляется возможность дополнительного привлечения инвестиций в любых валютах, потому что токенизированный рубль фактически становится конвертируемым. ■

Об авторе

Дмитрий Николаевич Мариничев, представитель уполномоченного при президенте РФ по защите прав предпринимателей в сфере Интернета

Искусство в технологиях. Поэзия Серебряного века в образах, созданных искусственным интеллектом

Анастасия Кузьмина



Аннотация

Искусственный интеллект разбирается в поэзии, или Как мы создавали корпоративный календарь MSK-IX.

Ключевые слова:

искусственный интеллект, проект MSK-IX, обучение ИИ, визуализация поэзии, цифровое искусство, нейросеть для творчества, Серебряный век

На высоте, на снеговой вершине,
я помню дни солнцеворота,
бессмысленный и тусклый свет,
изысканный бродит жираф,
я показал на блюде студня,
кто здесь рылся? Может, гномы.
Запах солнца? Что за вздор!
Отговорила роща золотая.
На реке форелевой, в северной
губернии.

Прочитали? Вы тоже остались в некотором недоумении? Перечитайте ещё раз и закройте глаза. Перед вашим внутренним взором вспыхивает калейдоскоп красок, проносится вереница сюжетов, можно даже почувствовать запахи, услышать знакомую мелодию или ощутить лёгкое дуновение ветерка.

Не будем вас томить: все эти строки взяты из стихотворений русских поэтов Серебряного века. Это время рубежа XIX-XX веков, наполненное символизмом с лёгким вкраплением футуристических идей и новой эстетики. Такие поэты, как Сергей Есенин, Борис Пастернак, Владимир Маяковский и многие другие обращались к темам любви, природы и философии, поднимали острые социальные проблемы, пытались переосмыслить противоречивость и сложность жизни того времени.



MSK IX

Искусство в технологиях
Поэзия Серебряного Века в образах,
созданных искусственным интеллектом

2024

Посмотреть календарь
подробнее можно
по ссылке





На живом примере мы убедились, что наше подсознание не видит границы между реальностью и вымыслом. Оно может само выстраивать логические цепочки, догадки и предположения, дополняя реальность и создавая образы чего-то нового исходя из опыта, знаний и окружения человека. На первый взгляд, это очень просто: вот жираф, вот зима, вот солнце, косые скалы океана и игрушечные волки в кустах. Любой взрослый сможет объяснить смысл этих строк даже ребёнку.

А что, если объяснить эти образы и научить их создавать того, кто ещё только учится мыслить и ищет своё место в мире? Того, кто создан человеком и теперь пытается научиться создавать что-то новое? Да, мы сейчас говорим об искусственном интеллекте. Давайте назовём его Аполлинаруй в честь Аполлона – бога света и покровителя искусств в древнегреческой мифологии. Интеллект, пускай и созданный человеком в виртуальном пространстве, может стать нашим другом и соратником.

Уже скоро 30 лет как MSK-IX помогает своим клиентам развиваться в технологиях, осознанно смотрит в будущее, предугадывает и создаёт новые тренды развития рынка. Эволюция технологий не происходит сама по себе – это планомерный творческий процесс. Для нашего комьюнити мы уже не первый год ведём один из специальных проектов – корпоративный календарь, и каждый год выбираем новую концепцию выпуска. В прошлом году мы провели эксперимент и подключили к творческому процессу искусственный интеллект. Суть эксперимента состояла в желании узнать и понять, как ИИ видит строки классиков Серебряного века русской поэзии. Так в нашем штате появился Аполлинаруй. С хорошим резюме и положительными рекомендациями, а его небольшой опыт в творчестве был компенсирован желанием обучаться и созидать.



Образ нового календаря стал складываться на глазах. Было отобрано 12 произведений поэтов Серебряного века. Аполлинаруй схватывал на лету, загружая в себя каждое стихотворение и предлагая яркий образ, который ещё больше погружал нас в созданный поэтами мир. На наших глазах постепенно складывался пазл нового календаря по образам, заложенным в него человеческим воображением.

В ходе проекта мы столкнулись с неожиданными вызовами. Выбрать 12 стихотворений Серебряного века оказалось гораздо сложнее, чем предполагалось вначале. Этот период отличался невероятным разнообразием стилей и тем, выходящих за рамки канонов классической поэзии. Чтобы сделать осознанный выбор, пришлось глубоко погрузиться в творчество каждого автора, понять всю образность и философию произведений. Многие стихотворения были настолько насыщены метафорами и символами, что даже людям непросто было сразу постичь их смысл, не говоря уже о машине. Искусственный интеллект изначально мыслит прямолинейно и шаблонно. Однако для этого проекта требовался творческий, ассоциативный подход, чтобы уловить всю тонкость и метафоричность стихов. Нашей задачей стало не только самим проникнуться многослойностью образов, но и обучить этому искусственный интеллект, чтобы он смог создавать визуальные интерпретации, передающие дух произведений. Но даже хорошо известные строки, которые в итоге были выбраны для календаря, Аполлинаруй поначалу воспринимал буквально, упуская глубокие культурные и исторические контексты, понятные человеку. Проблема за-

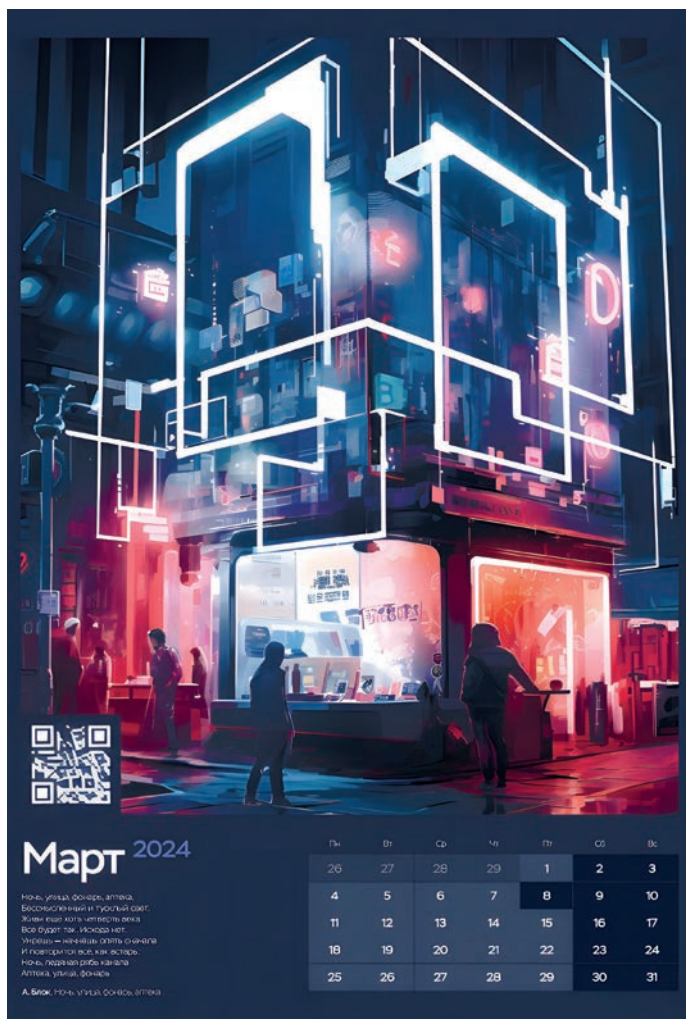
ключалась в том, что ИИ не чувствовал скрытые смыслы и атмосферу стихотворений. Что не удивительно, конечно.

Новый коллега не всегда понимал нас, а мы его. Порой доходило до смешного, как будто мы говорили на разных языках. Вместо дождливого Санкт-Петербурга глазами Александра Блока из стихотворения «Ночь, улица, фонарь, аптека...» перед нами возникал город будущего с неоновыми вывесками, а образ бальмонтовского солнечного дня был написан кистью Альфонса Мухи.

Мы стали «учить» Аполлиnaire, объясняя ему сложные образы, контексты и фразы, которые передавали дух той эпохи. Каждый новый вариант иллюстрации, создаваемый искусственным интеллектом, постепенно становился точнее и глубже, отражая не только текст, но и эмоции, которые вкладывал автор. Это был уникальный диалог между людьми и ИИ: люди предлагали подсказки (так называемые промпты), а Аполлиnaire отвечал на языке визуализации. Нашей задачей было научить искусственный интеллект «увидеть» стихи глазами человека. В результате коллаборация трёх эпох – прошлого в виде поэзии Серебряного века, будущего в лице искусственного интеллекта и настоящего через призму восприятия современного человека – превратилась в гармоничный симбиоз. Иллюстрации стали отражать уникальный взгляд ИИ, свободный от культурных наслоений, но одновременно наполненный теми знаниями, которые люди сумели ему передать.

День ото дня мы наблюдали, как Аполлиnaire всё больше развивается и понимает нас с первой загруженной строчки. Теперь не нужно было искать замену непонятным словам или объяснять какую-то фразу простым языком. Сами того





не замечая, мы научили нового друга не просто понимать, но и создавать по-настоящему прекрасное и неповторимое. Не удивлюсь, если вечерами, когда все покидали офис, Аполлинарий тоже закрывал глаза и при тусклом мерцании офисных ламп путешествовал по миру поэзии.

Бессмертные строки поэтов Серебряного века обрели новый облик в визуальных образах, сгенерированных нейросетью. Предлагаем вам сопоставить собственные ощущения от прочтённых строк с тем, как они были показаны с помощью современных технологий. Пусть увлекательное путешествие начнётся прямо сейчас и погрузит вас в мир прекрасного.

Проект создания нашего календаря, где ИИ интерпретировал поэзию Серебряного века, стал наглядным примером того, как технологии и искусство могут взаимодействовать, обогащая друг друга. Он стал уникальной формой диалога между прошлым, настоящим и частичкой будущего, который в итоге породил не просто календарь, а продукт настоящего симбиоза искусственного интеллекта и человеческого творчества. Своей свежестью и новым взглядом ИИ обогатил классическую поэзию, открыв для нас её новые грани и позволив взглянуть на знакомые строки под другим углом.

Наш эксперимент показал, что искусственный интеллект может стать нашим соавтором, способным создавать нечто новое и уникальное. ■

Об авторе

Анастасия Кузьмина, менеджер проектов маркетинга,
АО «ЦВКС «МСК-IX», a.kuzmina@msk-ix.ru, Россия, Москва



Интернет. В начале было сообщение...



Валерий Темников

Глобальная сеть обмена информацией между компьютерами «Интернет», начав свое развитие с 60-х годов прошлого века, стремительно вошла в нашу жизнь. В XXI веке, когда люди постоянно держат перед глазами мощный, подключенный к Сети персональный компьютер-смартфон, её влияние на нашу жизнь стало особенно заметным.

Через Интернет легче донести информацию до людей, чем через классические СМИ. Возможность размещать видеоролики (rutube.ru, vk.ru, dzen.ru) разрушило монополию телевидения на передачу живых выступлений.

«...в умелых и ответственных руках Интернет может быть уникальным инструментом донесения до человека церковной проповеди, посредником в живом общении с ближним, находящимся вдали, проводником к богослужбной жизни Церкви». (Из обращения Святейшего Патриарха Кирилла на Епархиальном собрании 2010 года, <http://www.patriarchia.ru>.)

Вес православного наполнения в Сети стал огромен: от веб-сайтов приходов сельских храмов, епархий, сайта Московской Патриархии до православных порталов «Азбука веры» и т.д.

Однако Интернет наполнен опасностями и ловушками для человека. Это манипуляция сознанием, пропаганда антисоциального и суицидального поведения, ненависти и дискриминации, антисемейных ценностей, культа потребления, индивидуализма и эгоизма, насилия и агрессии, оккультизма и эзотерики.

Каким будет Интернет, решаем мы с вами, потому что любой человек может выкладывать в Сеть, что захочет. Кто при этом определяет нормы морали и нравственности? Что можно, а что нельзя? Для православных христиан таким критерием является Сам Христос, в котором нет зла, в отличие от человека. Способен ли человек, делясь с людьми различной информацией, самостоятельно определять пользу того или иного сообщения, или ему нужна помощь Бога, Божией Матери или святых, которые могут стать покровителями правды и добра в Интернете?

Важно понимать, что просить в молитве следует не только об успехе дела, но прежде всего о спасении собственной души: пользуешься ли Интернетом или создаешь и поддерживаешь Сеть.

Святые покровители Интернета

Отметим, что в православной традиции акцент делается на личных отношениях со святыми, которых в Церкви очень много. И хотя официально в православии святых покровителей выбирают редко, и на данный момент святой покровитель Интернета и информационных технологий не установлен, но в наших силах обратиться с прошением в Церковь о получении молитвенного заступника. Далее Церковь решает, возможно это или нет.

А вот те святые, которые могли бы стать молитвенными заступниками для всех, кто связан с информационными технологиями.

Святитель Феофан, Затворник Вышенский



На пресс-конференции в ИТАР-ТАСС, посвящённой 10-летию российского Интернета, прозвучало предложение: «Святитель Феофан Затворник должен стать покровителем Рунета».

Святитель Феофан Затворник – русский епископ XIX века, канонизированный за «святость жизни», последние десятилетия которой он провёл в отшельничестве, где не-

престанно молился, написал огромное количество трудов и вёл обширную переписку.

Молитву Святитель Феофан Затворник уподоблял телеграфу – первому средству связи с использованием электричества:

«Вы знаете, как действует электрический телеграф? В Петербурге, например, заводят известный аппарат – в то же мгновение то действие петербургское отражается в Москве в подобном же аппарате и в том же значении, в каком там происходит движение. Почему так бывает? Потому, что и аппараты те однородны, и соединяющая их проволока к ним же подложена. Так, что действие такого телеграфа – то наша молитва».

Дни памяти:

19 января – Преставление;
23 января – День памяти Святителя Феофана, Затворника Вышенского;
23 июня – Собор Рязанских святых;
29 июня – Перенесение мощей;
29 июня (переходящая) – Собор Санкт-Петербургских святых;
10 августа – Собор Тамбовских святых;
23 сентября – Собор Липецких святых.

Житие Святителя Феофана, Затворника Вышенского, епископа Тамбовского:
<https://azbyka.ru/days/sv-feofan-zatvorniK>

Апостол и Евангелист Иоанн Богослов



«В начале было Слово, и Слово было у Бога, и Слово было Бог. Оно было в начале у Бога. Всё чрез Него начало быть, и без Него ничто не начало быть, что начало быть», – начинает свое Евангелие Апостол Иоанн Богослов. Иконография являет Апостола с пальцем, прижатым к губам, призывающего к молчанию. При общении

в Сети важно ограничить себя, чтобы лучше услышать и понять собеседника.

Апостол Иоанн был особенно любим Спасителем за жертвенную любовь и девственную чистоту. После своего призвания апостол не расставался с Господом и был одним из трёх учеников, которых Он особенно приблизил к Себе. Находясь в уединении на острове Патмос, Святой Иоанн Богослов продиктовал великое и таинственное откровение Апокалипсиса, символически описывающее события, которые должны произойти в конце времён.

Дни памяти:

21 мая – День памяти Апостола и Евангелиста Иоанна Богослова;
13 июля – Собор славных и всехвалых 12-ти апостолов;
9 октября – Преставление.

Житие Апостола и Евангелиста Иоанна Богослова:
<https://azbyka.ru/days/sv-ioann-bogoslov>



Преподобный Нестор, Летописец Печерский

Работающим над информационным наполнением Сети можно обращаться с молитвами к Нестору Летописцу.

Преподобный Нестор является составителем первоначальной истории нашего Отечества, летописи, где он излагает по годам сказание о начале Русской земли и последующих событиях ее истории до 1100 года.

Преподобный Нестор – просветитель, который стремился сохранить и передать следующим поколениям знания о Родине, укрепить веру в Бога.

Преподобный Нестор считается духовным наставником людей, жизнь которых связана с информационной деятельностью.

Дни памяти:

16 марта (переходящая) – Собор всех Киево-Печерских преподобных отцов;
11 октября – Собор Киево-Печерских преподобных, в Ближних пещерах;
23 октября – Собор Волынских святых;
9 ноября – День памяти Преподобного Нестора, Летописца Печерского.

Житие Преподобного Нестора, Летописца Печерского:
<https://azbyka.ru/days/sv-nestor-letopisec>

Молитва перед выходом в Интернет

В христианской практике принято молиться перед всяким добрым делом.

В сборнике молитв на сайте «Азбука веры» (<https://azbyka.ru/molitvoslov/molitva-pered-vyходом-v-internet.html>) приведена «Молитва перед выходом в Интернет»:

Господи Бóже наш, Творче неба и земли, создавший человека и даровавший ему ведение сокровенной премудрости, во еже прославляти имя Твое, горé и до́лу Ты еси, Твое ёсть ночь и Твое ёсть дéнь, не утаятся пред Тобóю дáже мимолетные движéния мы́сли.

И ны́не молю́ Тя, от вся́кого грехá сохрани́ мя, присту́пающего к рабóте с хитроумным творéнием ру́к челове́ческих, проникающим во вся́ концы́ землй.

Огради́ очи́ мой и у́м мой от вся́ких нечýстных и блýдных образóв, от пусты́х и негодных словéс.

Укрепи́ волю́, сёрдце очисти́, не дáждь мй́ вотщé расчóати́ вре́мя жи́зни моея́, и от вся́кого расслаблeния и уны́ния изба́ви.

Да б́дут дела́ наши́ во сла́ву Твою́!

Ами́нь.

Отношение к сети Интернет в разных религиях



Католическая церковь приравнивает Интернет к средствам массовой коммуникации и поддерживает его использование для распространения религиозной информации.

По мнению католической церкви, необходимо изучать возможности Интернета для эффективного общения с людьми, особенно с молодёжью. Также сеть Интернет выделяется как инструмент внутренней коммуникации для администрирования и управления.

ния.

Однако католическая церковь предупреждает, что в Интернете трудно отделить правдивую информацию от ложной, и даже религиозный опыт недостаточен без реального взаимодействия с другими верующими людьми.

В официальных документах Ватикан в лице папы Иоанна-Павла II призвал католиков не бояться новых технологий.

Следует отметить, что Ватикан располагает собственной автономной системой AS8978 с адресным пространством 193.43.128.0/22, 212.77.0.0/19, 212.77.31.0/24 и подключен к точке обмена трафиком Namex.



В 1999 году покровителем пользователей компьютеров и Интернета для католиков назван **Исидор Севильский** – Епископ Гиспальский – латинский церковный писатель, богослов, энциклопедист.

Святитель **Исидор Севильский** также почитается в Греческой Церкви и Православной Церкви в Америке.

День памяти: 4 апреля (Греч., ПЦА).

Биография святого Исидора Севильского:
https://azbyka.ru/otechnik/Isidor_Sevilskij/

Источники:

<https://dumsk.com/musulmanam/stati/12185-soczialnyie-seti-mozhno-ili-nelzya.html>

<https://vestnik.journ.msu.ru/books/2010/2/vatikan-i-novye-informatsionnye-tehnologii/>



Ислам призывает относиться к Интернету с учётом намерений пользователя Сети.

Если Интернет используется для добрых, благих целей, например, просвещения, творчества, благотворительности, то это не противоречит нормам ислама.

Однако Интернет может использоваться и в неблагоприятных целях, например, для распространения идей экстремизма, различных непристойных предложений, распространения информации, оскорбляющей чувства верующих. В таком случае это не соответствует исламу.

Мусульманин должен помнить, что он должен делать только то, что разрешено шариатом, и избегать того, что запрещено.

Духовные лидеры ислама руководствуются правилом, основанным на хадисе (изречении пророка Мухаммеда): «О действии судят по намерению». При хорошем намерении уместны любые современные технологии.

Источники:

<https://www.caravan.kz/news/kak-byt-istinnomu-musulmaninu-kogda-v-tiktok-vysmeivayutkoran-mnenie-kazakhstanskogo-imama-706649/>

<https://dumsk.com/musulmanam/stati/12185-soczialnyie-seti-mozhno-ili-nelzya.html>



Буддисты положительно относятся к использованию Интернета. Далай-лама XIV имеет аккаунты в социальных сетях и выкладывает в них фотографии из путешествий и рассуждения о жизни.

Однако в разных традициях буддизма отношение к Интернету может отличаться:

- Тибетский буддизм ограничивает использование Интернета общинами данной традиции в силу закрытости определённых тантрических учений.
- Дальневосточная традиция делает упор на живой контакт с учителем.
- Южный буддизм, ввиду своих особенностей, заключающихся в приоритете книжного знания, более охотно принимает сетевые технологии.

В целом, буддисты подчёркивают важность осмысленного и осторожного использования Интернета.

Источники:

https://www.dp.ru/a/2016/08/29/Kak_otnosjatsja_k_Internetu
<https://studybuddhism.com/ru/prodvinutyj-uroven/istoriya-i-kultura/buddizm-v-sovremennom-mire/kak-primenyat-buddijskie-printsipy-v-vek-sotsialnyh-setey>
<https://cyberleninka.ru/article/n/buddizm-v-internete-vozmozhnosti-i-prepyatstviya>



В иудаизме позиции в отношении сети Интернет различаются.

Некоторые ортодоксальные раввины полагают, что Интернет вредит иудаизму. Другие считают, что в целях самообразования пользоваться им допустимо.

Реформистское направление иудаизма допускает обращение в иудаизм заочно, по Интернету. Напротив, ортодоксальные иудеи считают, что подобные шаги не имеют никакой галахической силы, то есть силы законного решения.

Иудаизм занимает согласованную позицию в отношении того, что Интернет нужно процеживать, освобождать от груза пустой, развращающей, душевредной информации. В Израиле даже создают специальный «кошерный Интернет»: приобретая подготовленный компьютер, пользователь получает возможность посещать только те сайты, которые заранее одобрены раввином.

Источники:

<https://cyberleninka.ru/article/n/otnoshenie-iudaizma-k-internetu>
<https://sefercenter.org/rus/publications/campbell2.pdf>
https://toldot.com/urava/ask/urava_9109.html
<https://judaism.stackexchange.com/questions/8968/is-it-forbidden-to-use-the-internet-on-shabbat>
<https://cih.ru/vs/116.html>

В итоге разные религии сходятся между собой в одном: Интернет требует осторожного, вдумчивого обращения с собой и как мощный инструмент может использоваться для достижения цели, которую каждая религия ставит перед собой.





Праздники и памятные даты, объединённые Интернетом

Праздники

28 января — Международный день защиты персональных данных. В некоторых странах праздник называется «Днём конфиденциальности» (Data Privacy Day). Решение отмечать было принято 26 апреля 2006 года комитетом министров Совета Европы. Эта дата соответствует годовщине подписания Конвенции Совета Европы от 28 января 1981 года «О защите лиц в связи с автоматизированной обработкой персональных данных».

Второй вторник февраля — День безопасного Интернета. Инициатором праздника выступила Европейская Комиссия в январе 2004 года. Идею поддержали некоммерческие организации European SchoolNet и Insafe. Insafe стала главным координатором праздника.

Первая половина февраля — Неделя безопасного Рунета. Начиная с 2021 года ежегодно в России проводится серия мероприятий, посвящённых проблемам детской цифровой безопасности. Тематические мероприятия проходят по нескольким направлениям, в том числе безопасность детей в Интернете, борьба с незаконным и вредоносным контентом, защита персональных данных и конфиденциальности, противодействие киберпреступности и киберугрозам и т.д.

13 февраля — Всемирный день радио. Отмечается в честь первого эфира станции «Радио ООН», вещавшего в штаб-квартире Организации Объединённых Наций в 1946 году.

14 февраля — День компьютерщика. Это неофициальный широко отмечаемый в профессиональном мире праздник. В этот день в 1946 году был продемонстрирован первый реально работающий электронный компьютер ENIAC (Electrical Numerical Integrator And Calculator).

1 марта — День хостинг-провайдера. Неформальный профессиональный праздник для специалистов интернет-технологий, предоставляющих технические платформы для размещения и хранения данных. Появился в 2011 году по инициативе руководителей частных компаний Матвея Алексеева (Filanko) и Петра Паламарчука («ХостОбзор»).

12 марта — День свободы слова в Интернете. Отмечается по инициативе международной организации «Репортёры без границ» (под патронатом ЮНЕСКО) с 2008 года.

31 марта — Международный день резервного копирования (День бэкапа). Был установлен по инициативе пользователей сайта социальных новостей «Реддит» в 2011 году. Дата была выбрана из-за того, что на следующий день, 1 апреля, иногда возникают сбои в системе и потеря ценной информации.

4 апреля — День веб-мастера, неофициальный профессиональный праздник веб-мастеров, занимающихся разработкой веб-сайтов или приложений для Интернета. Дата 4.04 напоминает ошибку 404 - «Страница не найдена».

4 апреля — Международный день Интернета. В этот день католики отмечают день памяти Исидора Севильского, который в 1999 году был назван покровителем пользователей компьютеров и Интернета.

7 апреля — День рождения Рунета. В этот день в 1994 году был создан и закреплен за Россией национальный домен верхнего уровня (выделенный для конкретной страны) — .ru.

Первый четверг мая — Всемирный день пароля. Идею праздника предложил консультант по безопасности Марк Беннет в своей книге «Идеальные пароли: выбор, защита, аутентификация».

5 мая — День шифровальщика в России. В этот день в 1921 году была создана Криптографическая служба.

7 мая — День радио. Праздник работников всех отраслей связи и радиотехники. Установлен в честь события, произошедшего в 1895 году, когда российский физик Александр Степанович Попов выступил с докладом и демонстрацией созданного им первого в мире радиоприёмника.

12 мая — день рождения национального кириллического домена .рф.

12 мая — День борьбы с программами-шифровальщиками (Anti-Ransomware Day). Отмечается ежегодно с 2020 года по инициативе Интерпола и компании «Лаборатория Касперского».

14 мая — День фрилансера. Этот профессиональный праздник отмечают дизайнеры, программисты, менеджеры, оптимизаторы, копирайтеры — все те, кто трудится и создает вне стен определенного офиса, удалённо с широким использованием Интернета. Дата праздника выбрана в связи с тем, что в этот день в 2005 году была образована одна из первых российских бирж фрилансеров — сервиса по поиску удалённой работы.

17 мая — Международный день телекоммуникаций. Дата связана с созданием 17 мая 1865 года Международного телеграфного союза, впоследствии переименованного в Международный союз электросвязи (МСЭ).

28 мая — День оптимизатора. Неофициальный профессиональный праздник оптимизаторов Рунета или SEO-оптимизаторов, отмечается с 2006 года. Дату определили путём голосования пользователей форума Searchengines.

Последняя пятница июля — День системного администратора. Праздник впервые отметил в пятницу 28 июля 2000 года американский системный администратор с 20-летним стажем Тед Кекатос.

31 августа — День блога. В 2005 году группа авторов с портала LiveJournal решила придумать «профессиональный» праздник. По легенде, кто-то из них подметил, что написание слова «блог» на латинице — BLOG — напоминает цифры 3108.

13 сентября — День программиста в России. Отмечается в 256-й день года. Значение 256 принимает 8-разрядный байт, где все биты равны единице. Обычно праздник выпадает на 13 сентября, в високосный год на один день раньше — 12 сентября.

30 сентября — День Интернета в России. Инициатором праздника стала фирма IT Infoart Stars, которая в 1998 году предложила назначить эту дату и провести «перепись населения русскоязычного Интернета». По данным переписи, в то время доступ к Интернету имел один миллион россиян.

20 октября — День военного связиста. Официальный и профессиональный праздник всех работников и военнослужащих войск связи, установленный указом президента РФ от 31 мая 2006 года № 549.



29 октября — День рождения Интернета. В 1969 году состоялась первая передача данных между двумя компьютерами — это событие считается рождением Интернета.

Второй четверг ноября — Всемирный день юзабилити. Отмечается с 2005 года и затрагивает важную проблему простоты и удобства интерфейсов.

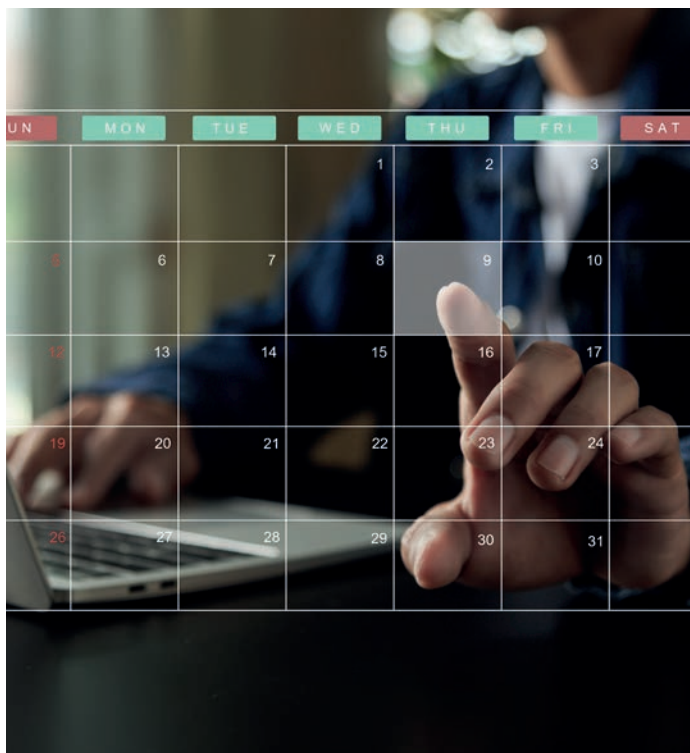
26 ноября — Всемирный день информации (World Information Day). Праздник проводится ежегодно с 1994 года по инициативе Международной академии информатизации (МАИ).

30 ноября — Международный день защиты информации (Computer Security Day). В этот день по инициативе американской Ассоциации вычислительной техники (Association for Computing Machinery, ACM) с 1988 года пользователям напоминают о необходимости защиты их компьютеров и всей хранимой в них информации.

3 декабря — Всемирный день компьютерной графики, который учредила организация Alias в 1998 году.

4 декабря — День информатики в России. Неофициальный праздник всех, кто имеет отношение к данной отрасли. В этот в 1948 году Государственный комитет Совета министров СССР по внедрению передовой техники в народное хозяйство зарегистрировал за номером 10475 изобретение И. С. Брука и Б. И. Рамеева — цифровую электронную вычислительную машину. Это первый официально зарегистрированный документ, касающийся развития в СССР вычислительной техники, а впоследствии и информатики.

10 декабря — альтернативный День программиста. В этот день в 1815 году родилась первая программистка — Августа Ада Лавлейс.



Памятные даты

19 сентября 1990 года – Советская ассоциация пользователей операционной системы UNIX (SUUG – Soviet UNIX User's Group) зарегистрировала домен .su.

4 декабря 1993 года – состоялось подписание соглашения «О порядке администрирования зоны .ru», передача администрирования и технического сопровождения национального домена .ru Российскому научно-исследовательскому институту развития общественных сетей (РосНИИРОС), создание Координационной группы домена .ru.

1993 год – администрирование домена .su было передано РосНИИРОС.

1994 год – прекращение регистрации доменов в зоне .su в связи с началом свободной регистрации в российском домене.

1995 год – заключено Соглашение о создании точки взаимного обмена IP-трафиком между основными московскими интернет-провайдерами: «Демос», «Релком», МГУ, НИИЯФ МГУ (Radio-MSU), FREEnet, Ассоциацией RELARN, «Роспринт»; на Московской междугородней телефонной станции № 9 (ММТС-9) в ноябре заработал первый узел «Московского Internet eXchange» (MSK-IX).

25 декабря 2000 года – создан Главный радиочастотный центр (ГРЧЦ).

2001 год – передача прав на поддержку и развитие реестра .su «Фонду развития Интернет», который был основан в 2000 году двумя российскими интернет-компаниями: «Релком. Деловая сеть» и «Демос–Интернет».

2001 год – учреждение Координационного центра национального домена сети Интернет, его учредителями стали Региональный общественный центр интернет-технологий (РОЦИТ), Союз операторов Интернет (СОИ), Ассоциация документальной электросвязи (АДЭ) и Российский НИИ развития общественных сетей (РосНИИРОС).

15 декабря 2002 года – возобновление регистрации доменов в зоне .su для владельцев товарных знаков.

Июнь 2003 года – «Фонд развития Интернет» возобновил открытую регистрацию доменов в зоне .su.

4 января 2006 года – сведения о Координационном центре национального домена сети Интернет были занесены в базу данных IANA.

3 декабря 2008 года – создана Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

18 февраля 2009 года – Координационный центр национального домена сети Интернет заключил соглашение о взаимодействии с Министерством связи и массовых коммуникаций Российской Федерации.

21 января 2010 года – ICANN утвердила заявку Координационного центра на новый национальный кириллический домен верхнего уровня .рф.

7 апреля 2010 года – подписано соглашение о взаимодействии между Министерством связи и массовых коммуникаций Российской Федерации и Координационным центром по вопросам управления национальным доменом .рф.

12 мая 2010 года – IANA разместила запись о домене .рф на корневых серверах мировой системы доменных имен (DNS), домен .рф делегирован России, Координационный центр является администратором двух национальных доменов верхнего уровня: .ru и .рф

15 мая 2018 года – создано Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации.

6 сентября 2018 года – создан Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

29 июля 2019 года – Роскомнадзор включил домен .su в национальную доменную зону.

31 июля 2020 года – возврат в РосНИИРОС прав на поддержку и развитие реестра .su.

29 декабря 2022 года – утверждено подразделение МВД России, борющееся с противоправным использованием информационно-коммуникационных технологий. ■

Новости науки и техники

ФБР США создало собственный токен для борьбы с манипулированием рынком криптовалюты

Токен NextFundAI на базе Ethereum позиционировался как актив, стимулирующий инвестиции в проекты искусственного интеллекта

Рынок криптовалют известен чрезвычайной волатильностью. Стоимость тех или иных токенов может взлетать и стремительно рушиться в течение одного дня. Происходит это не только по объективным причинам. Маркет-мейкеры - компании и сервисы, призванные стимулировать торговлю, - нередко используют своё положение, чтобы манипулировать ценами. И масштабы этого явления столь значительны, что Федеральное бюро расследований США пошло на нестандартный шаг: создание собственного токена.

В пресс-релизе, распространённом по итогам этой операции, сказано, что токен, получивший название NextFundAI, был создан на базе Ethereum с помощью «свидетелей, пошедших на сотрудничество со следствием». Токен позиционировался как актив, стимулирующий инвестиции в проекты искусственного интеллекта. Помимо собственно прибыли от роста стоимости NextFundAI, инвесторам был обещан процент прибыли от этих инвестиций.

Представители ФБР охарактеризовали торговую активность по токenu как «ограниченную». Тем не менее, операция имела определённый успех. По её итогам Комиссия по ценным бумагам и биржам предъявила трем маркет-мейкерам и девяти частным лицам обвинения в организации схем по искусственному завышению стоимости криптовалютных активов. В свою очередь, Министерство юстиции США предъявило 18 лицам и организациям обвинения в масштабном мошенничестве и манипуляциях на рынке. Так, например, маркет-мейкер Лю Жу, работающий с сервисом MyTrade MM, открыто рекомендовал сотрудникам, продвигавшим NextFundAI, сотрудничество с этим сервисом, поясняя, что он контролирует «накачку и сброс» стоимости активов, тем самым открывая возможность инсайдерской торговли.

После завершения операции ФБР сделки с токеном NextFundAI были прекращены. Министерству юстиции удалось заблокировать порядка 25 миллионов долларов, которых инвесторы лишились в результате мошеннических действий манипуляторов. Средства будут возвращены пострадавшим.

Источник:

The Verge, <https://www.theverge.com/2024/10/10/24267098/fbi-coin-crypto-token-nexgenai-sec-doj-fraud-investigation>

Инвестор забыл пароль от своего криптовалютного кошелька и смог восстановить его с помощью белых хакеров почти 10 лет спустя

Стоимость активов, защищённых забытым паролем, выросла в тысячу раз

Ресурс The Wired сообщил любопытную историю крипто-валютного инвестора, который обогатился благодаря тому, что на долгие годы лишился доступа к своему кошельку. Европейский инвестор, пожелавший сохранить анонимность и фигурирующий в публикации под именем Майкл, в 2013 году внёс на свой криптовалютный кошелек 43,6 биткойна, стоимость которых составляла в тот момент 5300 долларов. Для защиты кошелька он использовал менеджер паролей RoboForm, а сгенерированный пароль из 20 символов сохранил в файле, который зашифровал инструментом TrueCrypt.

Защита оказалась даже слишком надёжной: в какой-то момент в результате технического сбоя файл был повреждён и восстановить его не удалось. А о том, чтобы запомнить пароль из 20 символов, разумеется, не могло быть и речи. На протяжении многих лет Майкл предпринимал различные попытки восстановить пароль, которые становились все более активными по мере роста стоимости биткойна, но оставались неизменно безуспешными. Несколько квалифицированных хакеров и специалистов по криптографии, к которым Майкл обращался за помощью, отказывались, объясняя, что шансов восстановить пароль в такой ситуации нет.

В итоге Майкл вышел на Джо Гранда - известного специалиста по взлому, телевизионного эксперта и консультанта многих компаний в области безопасности. Тот тоже поначалу отверг предложение, но затем всё же согласился попытаться счастья, заручившись поддержкой своего друга, немецкого хакера по имени Бруно.

Надежда Гранда и Бруно была на то, что в версии RoboForm, которую использовал Майкл для создания пароля, найдётся уязвимость. И уязвимость действительно нашлась: как оказалось, эта версия использовала для создания паролей генератор случайных чисел, который в действительности таковым не являлся. RoboForm определял дату и время, установленные на компьютере пользователя в момент запуска программы, и создавал пароли на их основе. Таким образом, зная дату и время создания, можно было вычислить все комбинации паролей, сгенерированные менеджером RoboForm.

Тут, однако, обнаружилась еще одна проблема: Майкл не помнил, когда он создал пароль. Логи кошелька показывали, что первый биткойн был помещен туда 14 апреля 2013 года, но из этого совершенно не следовало, что пароль был создан в тот же день. Гранду и Бруно не оставалось ничего, кроме как генерировать все варианты паролей на каждый день, начиная с 14 апреля. Им пришлось добратсья до 15 мая того же года - и один из сгенерированных ими паролей наконец-то открыл кошелек.

Взломщики вычли обещанную комиссию за труды и передали пароль Майклу. Он теперь считает, что утрата пароля была чрезвычайным везением. За время, пока он не имел доступа к кошельку, стоимость его активов выросла примерно в тысячу раз.

Источник: Wired, <https://www.wired.com/story/roboform-password-3-million-dollar-crypto-wallet/>

Индия - мировой лидер в использовании криптовалюты

Опубликован мировой рейтинг применения криптовалют от компании Chainalysis

Аналитическая компания Chainalysis опубликовала свой рейтинг применения криптовалют в 2024 году. Это важный инструмент, позволяющий отслеживать распространение криптовалют и их влияние на повседневную жизнь людей. Для составления рейтинга эксперты Chainalysis изучили положение дел в 151 стране мира.

В расчёт принимались несколько ключевых факторов. Первый из них - общий объём криптовалютных транзакций, осуществлённый пользователями страны. Второй значимый показатель - объёмы peer-to-peer транзакций, совершаемых напрямую между пользователями. Этот критерий особенно важен для регионов, жители которых, в силу различных причин, ограничены в доступе к традиционным финансовым сервисам. Кроме того, полученные данные сопоставлялись с объёмом ВВП каждого конкретного государства, доходом на душу населения, количеством жителей и т.д. Это позволило получить более объективное представление о том, как криптовалюты влияют на экономику и жизнь людей - той или иной страны.

Результатом такого подхода стало то, что страны со сравнительно небольшими экономиками, где граждане активно используют криптовалюту для повседневных нужд, смогли занять в рейтинге более высокие позиции, чем крупные, развитые государства, где криптовалюта в основном служит как инвестиционный инструмент. В целом рейтинг 2024 года фиксирует явное лидерство развивающихся стран. Так, в Аргентине, уже много лет страдающей от гиперинфляции, более трети населения вовлечены в криптовалютные транзакции. Похожая ситуация и в Бразилии, граждане которой видят в криптовалюте альтернативу слабеющей на глазах национальной валюте.

Серьёзный прогресс в использовании криптовалют продемонстрировали ряд африканских государств, в частности, Нигерия и Кения. Скажем, в Нигерии, где значительная часть населения не имеет доступа к банковским услугам, порядка 45% жителей так или иначе используют криптовалюты. И ещё более бурными темпами идёт рост использования криптовалют в странах Юго-Восточной Азии, прежде всего во Вьетнаме и на Филиппинах. В то же время в США и Японии, которые были в числе пионеров использования

криптовалют, особого роста не наблюдается. Криптовалюты здесь рассматриваются прежде всего как инструмент диверсификации портфеля активов. Правда, использование криптовалют крупными институциональными инвесторами может послужить сигналом для оживления роста. И в этой связи запуск криптовалютных фондов такими инвестиционными гигантами, как BlackRock и Fidelity, способен стать важным стимулом.

Если говорить о конкретных позициях рейтинга, то первое место в нём занимает Индия. На второй строчке - Нигерия, на третьей - Индонезия. Соединенные Штаты идут четвертыми, а Россия занимает в рейтинге седьмое место.

Источник: CryptoNews, <https://crypto.news/global-crypto-adoption-index/>

Обновление The Verge позволит запустить узел Ethereum даже на умных часах

Виталик Бутерин рассказал о грядущем обновлении Ethereum

Один из основателей платформы Ethereum, программист Виталик Бутерин рассказал о предстоящем обновлении платформы. Оно носит название The Verge и призвано укрепить статус Ethereum как децентрализованной системы. По мнению Бутерина, одним из главных преимуществ блокчейна перед централизованными системами является то, что любой пользователь потенциально имеет возможность запустить узел на своём устройстве и проверить целостность всей сети.

Однако практическая реализация этой возможности в Ethereum становится всё более трудной задачей. По мере развития экосистемы растёт и объём данных состояния (state data), которые необходимо обрабатывать каждому узлу. Сейчас, согласно оценкам исследовательского проекта Paradigm, этот объём составляет сотни гигабайт. Для этого требуются значительные вычислительные мощности, что делает возможным запуск узла лишь на весьма мощных и производительных устройствах.

Эту проблему и призвано решить обновление The Verge. Его ключевая особенность - внедрение процесса верификации, не фиксирующей текущее состояние (stateless verification). Такая технология позволяет проверять блоки блокчейна без сохранения больших объёмов данных. Первоначально разработчики планировали задействовать технологию Verkle trees — криптографическую структуру для уменьшения размера доказательств. Однако она потенциально уязвима перед атаками квантовых компьютеров и могла бы потребовать замены уже в обозримом будущем. Как альтернативный вариант рассматривается технология бинарных хеш-деревьев на основе STARK (Scalable Transparent Arguments of Knowledge). В любом случае, обновление The Verge, по словам Бутерина, сделает полную проверку сети «столь доступной с точки зрения

вычислительных мощностей, что любой мобильный или браузерный кошелек и даже умные часы смогут осуществлять эту операцию по умолчанию». Таким образом, запуск узлов Ethereum на смартфонах и умных часах становится всё более реальной перспективой. Впрочем, сроков выпуска обновления The Verge Виталик Бутерин пока так и не назвал.

Источник: Cointelegraph, <https://cointelegraph.com/news/ethereum-upgrade-enables-nodes-on-phones-smart-watches>

Бывший инженер по безопасности Amazon приговорён к трём годам тюрьмы за взлом двух криптовалютных бирж

Суд Южного округа Нью-Йорка вынес приговор Шакибу Ахмеду (Shakeeb Ahmed) – несомненно, весьма квалифицированному IT-специалисту. Ахмед занимал должность инженера по безопасности в корпорации Amazon, но, к сожалению, направил свои таланты и навыки не на борьбу с киберпреступностью, а на совершение киберпреступлений. Летом 2022 года с интервалом в несколько недель он атаковал две криптовалютных биржи, похитив значительные объёмы средств.

В начале июля он воспользовался уязвимостью в смарт-контракте неназванной в документах суда биржи, чтобы указать фальшивые цены. Это позволило Ахмеду в короткий срок привлечь 9 миллионов долларов, которые затем были выведены им с биржи. В дальнейшем он предложил администрации вернуть средства, кроме 1,7 миллиона долларов, которые оставил себе в обмен на отказ биржи от обращения в правоохранительные органы. Даты и описание инцидента совпадают с обстоятельствами атаки на децентрализованную финансовую платформу Crema Finance.

А в конце июля того же года Шакиб Ахмед атаковал криптовалютную биржу Nirvana Finance. На сей раз уязвимость смарт-контракта позволила ему приобретать криптовалюту по заниженной цене, а затем продавать по завышенной. Эта операция принесла хакеру 3,6 миллиона долларов. Криптовалютная биржа предложила Ахмеду вознаграждение в 300 тысяч долларов при условии возвращения остальных средств, однако он потребовал 1,4 миллиона. В результате стороны не пришли к согласию, биржа Nirvana Finance была вынуждена объявить о закрытии, а Ахмед сохранил все полученные им средства.

В дальнейшем он использовал криптомиксеры и перемещение средств между различным блокчейнами, чтобы замести следы своих преступлений. Но всё это не помогло ему уйти от наказания. Прокурор Дэмиан Уильямс (Damian Williams) отметил, что дело Шакиба Ахмеда – первый случай вынесения приговора по обвинению во взломе смарт-контракта. «Не имеет значения, насколько новыми и изощренными являются взломы, мы делаем всё, что-

бы привлечь виновных к ответственности», – заявил он. Ахмед приговорён к трём годам тюремного заключения, после которых ему предстоит провести ещё три года под надзором полиции. Кроме того, он обязан компенсировать пострадавшим от его действий компаниям убытки и выплатить штраф в 12,3 миллиона долларов.

Источник: Bleeping Computer, <https://www.bleepingcomputer.com/news/security/ex-amazon-engineer-gets-3-years-for-hacking-crypto-exchanges/>

Определится первый претендент на аукцион в рамках следующего этапа программы новых доменов

До старта очередного этапа программы новых доменов общего уровня остаётся ещё не менее полутора лет (это, впрочем, пока только предположения: точная дата корпорацией ICANN ещё не определена), но претенденты ведут себя всё активнее, заявляя о своих намерениях. И есть уже первый будущий домен, судьбу которого, по всей вероятности, решит аукцион, поскольку претендуют на него как минимум две компании.

На днях компания Freename.io сообщила о том, что будет подавать заявку на этот домен – так же, как и на домены .token, .metaverse и ещё ряд других. Freename работает на рынке блокчейн-доменов и, как и многие другие, продвигает идею интеграции традиционных (DNS) и альтернативных (WEB3) доменов. Компания уже регистрирует блокчейн-домены .chain и рассчитывает стать регистратурой и для соответствующего домена в системе DNS.

Но ещё в июне о подготовке заявки на домен .chain (а вместе с ним и на домен .super) объявила другая компания – 3DNS. Она регистрирует традиционные доменные имена третьего уровня вида .chain.box и планирует повысить их до второго уровня в новом домене, если её заявке будет сопутствовать удача. Поскольку ранее корпорация ICANN запретила использование частных аукционов претендентов на новом этапе программы, очевидно, что единственным вариантом решения, кому достанутся права управления доменом .chain, остаётся аукцион ICANN, средства от которого пойдут в бюджет самой корпорации.

Ресурс Domain Incite, сообщая эту новость, отмечает, что будет поистине удивительно, если число претендентов на этот домен не увеличится в ближайшее время. Слово chain, которое переводится с английского как «цепь», часто используется в качестве сокращения от blockchain, а блокчейн-технологии, наряду с искусственным интеллектом, – одна из самых «горячих» тем нашего времени.

Источник: Domain Incite, <https://domainincite.com/30290-is-this-the-first-next-round-new-gtld-contention-battle>



Интернет изнутри ➡