https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

EDN: HAZXNR

ЭКОНОМИЧЕСКАЯ ОСНОВА ДОВЕРИЯ В СИСТЕМАХ БЛОКЧЕЙНА

© Клёнов В.Д., 2026

Клёнов Владислав Денисович, аспирант, Российский университет дружбы народов им. Патриса Лумумбы, Москва, Россия;
ORCID: 0009-0006-5613-8019; eLibrary SPIN: 6734-1097; xddd.jo@gmail.com

Статья поступила: 22.09.2025, **принята к печати:** 15.05.2026

Оригинальная статья

Аннотация. Уровень доверия в экономике остается одним из ключевых параметров, определяющих благосостояние общества. На традиционных этапах доверие формировалось преимущественно через межличностные отношения и институциональные механизмы. Развитие цифровых технологий сокращает возможности оппортунистического поведения посредников и снижает уязвимость доверителя. В этом контексте блокчейн выступает в роли катализатора трансформации доверия в экономике. В статье предложено структурированное определение понятия «доверие в блокчейне» и проанализированы условия его реализации в цифровых системах. Особое внимание уделено роли блокчейна как технической и институциональной инфраструктуры — выделены ключевые технические свойства блокчейна и показано, как они соотносятся с механизмами воспроизводства доверия и с экономической основой этих механизмов, включая модель безопасности сети. Рассмотрены два ведущих на текущий момент блокчейна — Bitcoin и Ethereum. Представлены исторические данные о «бюджете безопасности» с распределением по эмиссионным и комиссионным компонентам, а также данные об объеме заблокированных средств по классам активов. На основе этих данных выполнена оценка устойчивости экономической модели. Таким образом, доверие в блокчейне может рассматриваться как измеримый экономический конструкт. Модель безопасности блокчейна доказала свою жизнеспособность посредством притока реальных активов, однако ее относительная неэффективность ограничивает масштабирование. В этих условиях ключевой инновацией является перераспределение рисков внутри системы, что позволяет встроить доверие в ее архитектуру. Эмиссия нативной криптовалюты формирует экономический каркас модели, но в то же время наблюдается тенденция роста более устойчивых пользовательских (комиссионных) денежных потоков.

Ключевые слова: доверие, распределенное доверие, алгоритмизированное доверие, блокчейн, Bitcoin, Ethereum, децентрализация, безопасность блокчейна, DeFi.

Классификация JEL: O30, O31, E42, F39.

Для цитирования: Клёнов В.Д. (2026). Экономическая основа доверия в системах блокчейна // Экономическая наука современной России. Т. 29. № 2. С. 124–137. https://doi.org/10.33293/1609-1442-2026-29(2)-124-137. EDN: HAZXNR

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

EDN: HAZXNR

THE ECONOMIC BASIS OF TRUST IN BLOCKCHAIN

Vladislav D. Klyonov, Postgraduate Student, RUDN University, Moscow, Russia;
ORCID: 0009-0006-5613-8019; eLibrary SPIN: 6734-1097; xddd.jo@gmail.com

Received: 22/09/2025, **Accepted:** 15/05/2026

Original article

Abstract. The level of trust in the economy remains one of the parameters determining the well-being of society. Traditional elements were formed primarily through interpersonal relationships and institutional mechanisms. The development of digital technologies reduces the possibilities for opportunistic behavior of intermediaries and reduces the vulnerability of the trustor. In this context, blockchain acts as a catalyst for the transformation of trust in the economy. This article proposes a structured definition of the concept of «trust in blockchain» and analyzes the conditions for its implementation in the digital environment particular attention is paid to the role of blockchain as a technical and institutional infrastructure — the key technical properties of blockchain are highlighted. It is shown how they relate to the mechanisms of trust reproduction and the economic basis of these mechanisms, including the network security model. The second section examines two currently leading blockchains — Bitcoin and Ethereum: historical data on «security budget» is presented, broken down by emission and fee components, as well as data on the volume of locked funds by asset class. Based on this data, an assessment of the sustainability of the economic model is made. As a result, trust in blockchain can be viewed as a measurable economic construct. The blockchain security model proven its viability through the inflow of real assets, but its relative inefficiency limits scalability. Under these conditions, the key innovation is the redistribution of risks within the system, which allows trust to be built into its architecture. The emission of a native cryptocurrency forms the economic framework of the model, but at the same time, while a trend toward the growth of more sustainable user (fee) cash flows is observed.

Keywords: trust, decentralized trust, distributed trust, algorithmic trust, blockchain, Bitcoin, Ethereum, decentralization, blockchain security, DeFi.

Классификация JEL: O30, O31, E42, F39.

For reference: Klyonov V.D. The economic basis of trust in blockchain. *Economics of Contemporary Russia*, 2026;29(2):124–137. (In Russ.) https://doi.org/10.33293/1609-1442-2026-29(2)-124-137. EDN: HAZXNR

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

ВВЕДЕНИЕ

Доверие является фундаментальным элементом экономического взаимодействия, выполняя функцию снижения неопределенности и транзакционных издержек при кооперации между агентами. В условиях неполной, асимметричной информации и невозможности полностью предсказать действия контрагентов оно становится ключевым условием совершения успешной сделки. Однако сама необходимость доверять создает уязвимость к оппортунистическому поведению и формирует институциональные издержки (Mosch, 2004). Отечественные исследования также фиксируют, что высокий уровень доверия снижает операционные издержки в деловом обороте, в том числе при взаимодействии с новыми контрагентами (Жилина, 2008). При этом даже формальные контракты и гарантии не всегда способны устранить риск оппортунизма, что подчеркивает *значимость институтов, обеспечивающих доверие*. Уровень доверия различается между странами, сохраняет высокую инерционность, изменяясь в течение поколений или под влиянием масштабных событий, что подчеркивает важность постоянной работы над его развитием. При этом доверие коррелирует с экономическими показателями и проявляется многоканально: от финансовых рынков и инноваций до рынка труда и взаимодействия компаний в реальной экономике (Algan, Cahuc, 2014).

Сегодня технологический прогресс стремительно изменяет среду, в которой взаимодействуют экономические агенты, что, в свою очередь, затронуло и вопросы реализации доверия в такой среде. Технология блокчейн, функционирующая на основе подкрепленного криптографией и экономическими стимулами алгоритмического механизма распределенного консенсуса, смещает вектор приложения доверия от конкретного института к самой цифровой системе и ее архитектуре. Такой подход может модифицировать институциональную структуру транзакций, снижая зависимость от централизованных гарантов и меняя распределение структуры рисков и издержек между участниками. «Доверие — это вера доверителя в то, что субъект доверия будет вести себя в соответствии с его (доверителя) ожиданиями» (Трындина, Устюжанина, 2023). Блокчейн формирует инфраструктуру, в которой *поведение* субъекта предопределено условиями программируемых процессов, а *вера в их исполнение* обеспечивается интегральными свойствами самого распределенного реестра.

Цель статьи — дать определение *доверия в блокчейне*, проанализировать механизмы, условия и роль блокчейна в его реализации. Для этого необходимо раскрыть технические и экономические аспекты работы блокчейна, а также рассмотреть практические примеры ведущих публичных блокчейнов. Для рассмотренных блокчейнов проводится анализ степени защищенности пользователей и их активов в контексте реализуемого уровня доверия и, как итог, определена устойчивость их экономической модели и модели безопасности.

БЛОКЧЕЙН И ЕГО СВОЙСТВА

Блокчейн (распределенный реестр) можно описать как распределенную систему хранения данных, состоящую из совокупности узлов (образующих единую сеть), которые хранят копии единой цепочки блоков с записями о транзакциях. Каждый новый блок добавляется в цепочку после проверки его достоверности с помощью криптографических алгоритмов и механизма консенсуса между узлами (Yaga et al., 2019).

С экономической точки зрения блокчейн создает для потребителя ценность как инфраструктура, предлагая услуги регистрации и хранения записей, поддержание их консистентности[1]. В этом смысле блокчейн близок к облачным вычислениям, выступающим в качестве модели «инфраструктура как сервис» (infrastructure as a service, IaaS), на базе которой уже строятся различные прикладные сервисы и бизнес-модели. Эта институциональная функция инфраструктуры объясняет ее экономическую значимость и масштабное распространение.

Вместе с тем облачные решения сопряжены с потенциально значимыми рисками. Технический риск связан с тем, что безопасность систем опирается на текущую криптостойкость и развитие вычислительных возможностей (включая потенциальные квантовые угрозы), что делает устойчивость модели безопасности предметом постоянной оценки. Этот риск присущ любой системе, реализующий традиционную криптографию, включая блокчейн. Второй риск — необходимость доверия третьей стороне. Использование централизованной инфраструктуры влечет за собой зависимость от ее владельца и контрактных условий, из-за чего в кризисных ситуациях решения оператора могут повлиять на интересы пользователей. Обсуждение возможных технологических и/или институциональных альтернатив неизбежно подводит нас к блокчейну и его роли в такой трансформации подхода к доверию.

Концепция *распределенного доверия* существовала задолго до появления блокчейна, получив

[1] Консистентность записей в блокчейне означает, что все узлы сети имеют одинаковую и согласованную версию данных, гарантируя их подлинность и неизменность в будущем.

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

бурное развитие с появлением цифровых технологий. Она получила широкое распространение как концепция вне экономики — речь здесь идет об управлении доверием в распределенных мультиагентных системах (Pinyol, Sabater-Mir, 2013). Сегодня распределенное доверие рассматривается как важная часть шэринг-экономики[2] (Martini, Vespasiano, 2020).

Базисом распределенного доверия, как правило, являются инструменты репутации, основанные на повторных взаимодействиях (например, отзывы на платформе). В условиях цифровых платформ и потребности в их эффективности возникает и фактор алгоритмизированного доверия, часто вытесняющий распределенное доверие на второй план и возвращающий нас к вопросу о доверии центральному агенту (провайдеру платформы). В таких системах, связанных с реальным миром, как *шэринг-экономика*, возникает *trust frontier* — граница перехода между физической реальностью и ее цифровой репрезентацией, и на такой границе неизбежно возникает централизованный провайдер (Hawlitschek, Notheisen, Teubner, 2018). Необходимость такого компромисса при построении систем на основе распределенного доверия является вызовом, ответ на который дает блокчейн.

Технология блокчейн имеет ряд ключевых неотъемлемых (без которых технология не является блокчейном) свойств (Yaga et al., 2019):

1. *Криптографическая верификация.* Блокчейн использует хэш-функции, цифровые подписи и другие криптографические методы для проверки подлинности транзакций и защиты данных.

2. *Связанная цепочка блоков.* Транзакции группируются в блоки, каждый блок содержит *ссылку* (хэш[3]) на предыдущий. Изменение содержимого блока изменит его хэш и нарушит целостность последующей цепочки.

3. *Распределенность.* Реестр реплицируется на множестве узлов, что повышает отказоустойчивость и дает возможность независимой верификации действий без центрального доверенного оператора.

4. *Механизм консенсуса.* Алгоритмы консенсуса (Proof of Work, Proof of Stake и др.) обеспечивают согласование порядка транзакций, формирование новых блоков и разрешение конфликтов в цепочке.

5. *Прозрачность.* История транзакций доступна для проверки участниками сети, что облегчает аудит и обнаружение несоответствий.

6. *Необратимость транзакций.* После достижения консенсуса транзакции воспринимаются как окончательные, а изменение истории требует либо широкой реконфигурации сети, либо целевой атаки и, как правило, экономически и институционально затруднено.

В совокупности эти свойства гарантируют целостность и доступность информации в распределенном реестре. Конфиденциальность не является гарантированной по умолчанию и требует дополнительных проектных решений (таких как шифрование, приватные сети, протоколы на основе доказательства с нулевым разглашением и т.п.). Однако и без них участник сети *псевдонимен* (псевдонимность, pseudonymity) — адреса в сети не содержат персонифицирующей информации, но пользователя легко идентифицировать при взаимодействии адреса с централизованными контрагентами. Распределенная природа, безопасность информации и одновременная прозрачность позволяют делать вывод о потенциале блокчейна как инфраструктуры, доверие к которой становится интегральным (архитектурным), в отличие от закрытых систем, в которых алгоритмизированное доверие искажено под слоем вынужденного доверия к провайдеру.

Однако даже такая архитектура не делает блокчейн полностью неуязвимым со стороны внешних факторов.

1. *Контроль над большинством узлов*. Наличие репликации реестра не исключает ситуаций, когда один субъект приобретает или контролирует преобладающую долю валидаторов/узлов. Это подрывает честность механизма консенсуса и дает возможность целенаправленно изменять порядок или отбирать транзакции.

2. *Ограничение доступа на уровне интерфейсов*. Прозрачность реестра не гарантирует неограниченный доступ к информации и сервисам, поскольку доступ может быть ограничен извне, например на уровне интерфейса.

В этих обстоятельствах блокчейн по-прежнему сохраняет полезность, например, как средство внутреннего аудита в организации, где записи фиксируются и доступны уполномоченным лицам. Однако для того чтобы выполнять более значимую общественную роль, стать инфраструктурой распределенного доверия, одного базового набора свойств недостаточно. Для этого в анализе выделяются два варьируемых свойства технологии — *децентрализация* и *публичность*. Рассмотрим их подробнее.

[2] Шеринг-экономика (экономика совместного потребления) — модель, основанная на коллективном использовании товаров и услуг вместо их покупки. Классическим примером является каршеринг.

[3] Хэш — уникальный идентификатор фиксированной длины, который создается из входных данных произвольного размера с помощью одностороннего математического алгоритма (хэш-функции). Минимальное изменение входных данных приведет к кардинальному изменению результата функции (хэша).

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

Децентрализация означает, что функционирование сети обеспечивается множеством относительно независимых субъектов с разными экономическими интересами и без единой централизованной точки принятия решений. В таких условиях валидаторы не имеют возможностей систематически преследовать собственные интересы в ущерб сети. При низкой децентрализации (высокой централизации) неотъемлемые свойства блокчейна сохраняются, однако возникает ситуация, в которой участники вынуждены доверять контролирующим субъектам, что максимально приближено к традиционным централизованным решениям и зависит от воли контролирующих их институтов.

Публичность отражает степень открытости данных и возможности участия пользователя в процессах сети. В публичной среде любой субъект может читать реестр и инициировать транзакции без предварительной авторизации. В среде с низкой публичностью доступ и участие ограничены авторизованными участниками.

В отличие от неотъемлемых свойств блокчейна, наличие которых определяется бинарно (свойство либо присутствует, либо нет), варьируемые свойства децентрализации и публичности существуют в континууме.

1. Децентрализация измеряется не только фактом распределения субъектов, но и масштабом распределения. Так, сеть из 12 узлов, принадлежащих разным операторам, — это один уровень, а сеть из миллиона узлов с глобальным географическим и организационным разнообразием — принципиально иной.

2. Публичность определяется не просто формальным доступом к данным, а удобством и полнотой этого доступа. Например, если информация предоставляется в формате, требующем значительных ресурсов для обработки, или в виде агрегированных сводок, это фактически может служить средством ограничения открытости даже при заявленной доступности данных.

Поскольку децентрализация и публичность имеют градации, каждый отдельный блокчейн стоит рассматривать, исходя из широкого спектра состояний, а не в фиксированных категориях. Распределенное доверие к блокчейну строится на основе доверия к совокупности участников консенсуса. В этом контексте оно тем выше, чем выше степень децентрализации и публичности сети (см. рисунок).

ДОВЕРИЕ В БЛОКЧЕЙНЕ

В доцифровую эпоху доверие в экономике неизбежно реализовывалось напрямую между субъектом и его контрагентом. Это мог быть самостоятельный актор или представитель организации/института. Во втором случае контрагент ограничен набором правил и санкций за их нарушение, им же доверяет и субъект. Однако на практике ввиду человеческого фактора и иных причин у актора остается пространство для оппортунизма (причем в интересах как своих, так и его представительства). Стоит отметить, что *институциональное доверие* основывается на комбинации взвешенного расчета и эмоционального отношения, облегчая переход от первого ко второму (Леонова, 2015). В этом контексте система норм института не создает непреодолимые препятствия для оппортунизма актора, а лишь смещает баланс выгод и рисков.

С появлением цифровых технологий обезличивание и детерминированность взаимодействия позволили частично преодолеть эту проблему, однако прогресс замедляется ввиду распространения об-

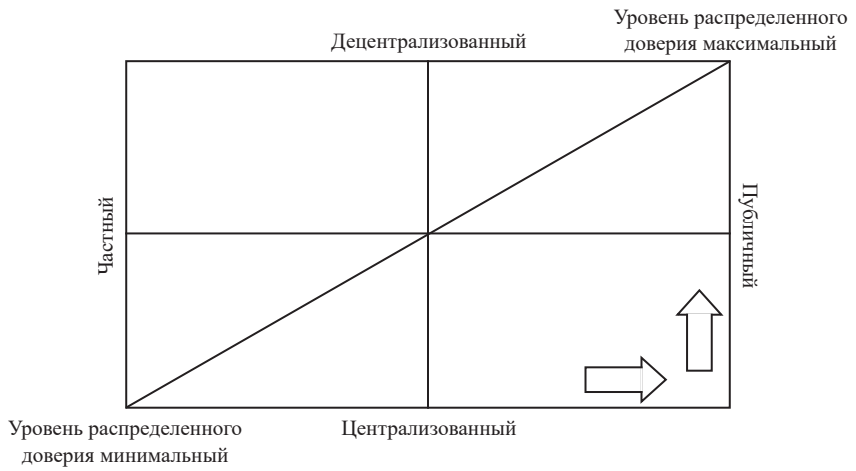

Рисунок. Зависимость распределенного доверия в блокчейне от степени его публичности и децентрализации

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

ширных механизмов идентификации. В блокчейне исполнение правил обеспечивается прозрачными алгоритмическими процедурами, а гарантия их соблюдения — сетью распределенных участников. Это формирует однородное ожидание участников относительно поведения системы и такое же отношение к ним, в том числе благодаря их псевдонимности.

Реализацию доверия в блокчейне удобно рассматривать на двух уровнях. Базовый слой, в котором независимые участники консенсуса верифицируют транзакции, а их добросовестное поведение подкреплено экономическими стимулами. Данный слой отвечает за реализацию распределенного доверия[4]. И слой приложений, который функционирует за счет смарт-контрактов — формализованных машино интерпретируемых соглашений, содержание которых определяется программным кодом, а корректность и необратимость исполнения обеспечиваются базовым слоем. Слой приложений реализует классическое алгоритмизированное доверие. Также он является частью именно программируемых блокчейнов, которые, хоть и имеют больший функционал, не являются стандартом (например, Bitcoin не является программируемым).

Сошлемся на определение доверия. Теперь доверитель вверяется не конкретному субъекту, а смарт-контракту. На первый взгляд это устраняет информационную асимметрию. Однако на практике доступность информации (условий смарт-контракта) не означает возможность ее считать — необходимы соответствующие компетенции. Происходит перераспределение источников потенциальных угроз: пользователь может быть полностью уверен в точности исполнения смарт-контракта, но при этом значительно возрастает его операционная ответственность (изучение содержания смарт-контракта, отсутствие права на ошибку при совершении операций, безопасное хранение ключей).

Безусловно, возникают и такие новые риски цифровой среды, как программные ошибки, взлом смарт-контракта, мошенничество. Накладываются и определенные ограничения, поскольку функционирование в такой среде возможно только в цифровой форме (иначе невозможно гарантировать выполнение условий смарт-контракта). Тем не менее эти риски и ограничения имеют преимущественно технический характер, то есть разрешимы по мере развития экосистемы и технологий. Например, для преодоления описанных ограничений существуют «*оракулы*» — поставщики данных из «реального мира», также функционирующие на основе консенсуса. Доверие становится вычислительным, реализуется принцип «код — это закон» (Atzori, 2017).

Стоит отметить, что в целом любая техническая система реализует данный принцип, поскольку ее функционал задан программно и подробно описан в спецификации, а сама техника не имеет возможности реализовывать оппортунистическое поведение. Например, нам не приходится сомневаться в корректности вычислений калькулятора или добросовестности стиральной машины. Блокчейн лишь совершенствует данную форму взаимодействия, предлагая: 1) видимые гарантии выполнения заданного функционала на основании распределенного доверия; 2) равный доступ к этим гарантиям для любого программного процесса. Это позволяет блокчейну служить инфраструктурой для широкого спектра экономических отношений, так как в нем сочетаются технологическая гибкость и финансово-экономические механизмы. Некоторые авторы подчеркивают, что блокчейн является институциональной технологией, снижая издержки для «институционального предпринимательства», то есть упрощает отдельным лицам процесс инициирования институциональных изменений (Allen et al., 2020).

После более детального ознакомления с концепцией реализации доверия в блокчейне рассмотрим два классических практических примера, где оно реализуется по-разному. Речь пойдет исключительно о публичных и децентрализованных блокчейнах, поскольку только по ним (благодаря их прозрачности) существует обширная информационная база.

Bitcoin (BTC) — первый публичный и децентрализованный блокчейн. Его функциональность ограничена базовым слоем, то есть исключительно передачей и хранением нативной криптовалюты. Эмиссия BTC строго ограничена алгоритмическим потолком в 21 млн *токенов*[5], что в сочетании с институциональным и рыночным консенсусом наделило BTC свойствами средства сохранения стоимости (store of value, SoV), сопоставимыми с золотом. Безопасность сети обеспечивается моделью доказательства выполнения работы (proof of work, PoW), согласно которой майнеры верифицируют блоки в обмен на вознаграждение в токенах BTC.

Ethereum представляет собой первый программируемый блокчейн с развитым уровнем приложений. Изначально построенный на PoW, в сентябре 2022 г. он перешел на *модель доказательства доли владения* (proof of stake, PoS), что привело к су-

[4] С поправкой на базовые алгоритмы для взаимодействия, доверие к которым является условием участия в блокчейне. Роль доверия к ним в контексте исследования менее значимая.

[5] URL: https://bitcoin.org/en/faq

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

щественному снижению энергопотребления и изменению экономической модели сети[6]. В PoS для участия в консенсусе и получения вознаграждения валидаторы обязаны блокировать его нативную криптовалюту ETH, одновременно рискуя частичной или полной потерей залоговых токенов при нарушении правил валидации — стейкинг. Изъятые у недобросовестных валидаторов Ethereum (ETH) выводятся из обращения («сжигаются»). В отличие от майнинга, стейкинг создает предпосылки для более традиционных форм доверия, поскольку стейки обладают «памятью», а поведение конкретного валидатора можно отслеживать во времени (Budish, 2022).

Наличие уровня приложений позволяет хранить в блокчейне не только нативную криптовалюту, но и токены, обеспеченные другими активами (например, WBTC[7], представляющий «обернутые» BTC для использования в экосистеме Ethereum). Кроме того, архитектура L2-решений предусматривает делегирование части функций безопасности базовому слою (L1). Это подчеркивает специфику модели обеспечения безопасности блокчейн-систем и ее относительную автономность, что дает возможность переносить гарантии безопасности базового уровня в различные сегменты экономической инфраструктуры. Возможность внедрения смарт-контрактов создало ключевой для блокчейн среды сегодня *рынок децентрализованных финансов* (DeFi). Характеристики DeFi достаточно исчерпывающе описывает Банк России в своем обзоре[8], выделяя следующие ключевые отличия от традиционных финансов:

1) *не связаны с хранением* — отсутствие посредника или отсутствие у него доступа к средствам;

2) *самоуправляемы* — сообщество может свободно предлагать изменения и голосовать за них;

3) *прозрачны* — сообщество имеет полный доступ к данным и коду блокчейна или протокола;

4) *универсальны* — кросс-секторальны и вариативны;

5) *компонуемы* — протоколы в DeFi могут быть свободно взаимно-интегрированы, что позволяет создавать инновационные продукты и структуры.

Это подчеркивает самостоятельность DeFi как уникальной сущности, зачастую рассматриваемой как альтернатива традиционным финансам. Тем не менее сегодня скорее реализуется сценарий их взаимной интеграции и DeFi как этап технологического развития традиционных финансов, каким, например, когда-то стал онлайн-банкинг.

В качестве показателя востребованности DeFi в работе используется метрика совокупного заблокированного объема (total value locked, TVL)[9], отражающая долларовый объем активов, размещенных в блокчейне. Для целей анализа целесообразно дифференцировать TVL по категориям, поскольку агрегированная величина смешивает экономически неоднородные активы. Предлагаемая классификация включает три следующие группы.

1. Crypto — TVL, формируемый криптовалютами и алгоритмическими стейблкоинами (токены с привязкой 1:1 к реальным активам, но обеспеченные криптовалютой или алгоритмическими процедурами), чья ценность определяется характеристиками средства сбережения (Store of Value, SoV), наличием денежных потоков или спекулятивными ожиданиями (наибольшая доля). Для доказательства работы доверия в блокчейне эта категория представляет ограниченную информативность.

2. Real — TVL, сформированный фиатными стейблкоинами[10] (токены с обеспечением 1:1 реальными, как правило, долларовыми активами) и токенизированными реальными активами[11] (real-world assets, RWA). Эта категория наиболее адекватно отражает перенос реальной ценности в блокчейн.

3. Total — суммарный показатель, объединяющий предыдущие категории и применяемый при оценке общей экономической активности в экосистеме.

TVL, связанный с нативной криптовалютой рассматриваемого L1, в рамках указанной классификации не выделяется отдельно ввиду его принципиальной взаимозависимости с работой базового блокчейна и отсутствия необходимости «доверять внешним механизмам» для существования в блокчейне. Динамика совокупного и реального TVL в сети Ethereum представлена в табл. 1. Данные по прочим блокчейнам в тексте не приводятся вследствие их относительной незначимости для поставленных задач.

---

[6] URL: https://ethereum.org/en/developers/docs/

[7] WBTC (Wrapped BTC) — токен в блокчейне Ethereum, который обеспечен токенами BTC в сети Bitcoin в соотношении 1:1. Его основная цель — дать держателям BTC доступ к функционалу сети Ethereum, недоступному в родной сети Bitcoin. Стоит отметить, что, поскольку нативного механизма такого трансфера не предусмотрено (настоящий BTC существует только в сети Bitcoin), возникает необходимость доверять провайдеру WBTC, который обеспечивает их выпуск и сохранность переданных ему в качестве залога BTC.

[8] URL: https://www.cbr.ru/Content/Document/File/141992/report_07112022.pdf (дата обращения: 31.03.2025).

[9] URL: https://defillama.com/chain/ethereum?currency=USD

[10] URL: https://defillama.com/stablecoins/Ethereum?backing=FIATSTABLES

[11] URL: https://defillama.com/protocols/rwa/ethereum

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

Следует также выделить TVL L2-решений, безопасность которых частично делегируется консенсусу Ethereum. По состоянию на 1 августа 2025 г. совокупный TVL пяти крупнейших L2 составлял 20 532 млн долл., из которых 11 785 млн приходилось на Real TVL. На основе данных табл. 1 видно, что в среднем более половины TVL в сети приходится на обеспеченные реальные активы (фиатные стейблкоины и RWA), причем их суммарный объем демонстрирует устойчивый прирост. В отличие от них Total TVL подвержен большей волатильности за счет изменений рыночной оценки криптовалют. К RWA на текущем этапе преимущественно относятся государственные облигации США и токенизированное золото. Токенизация финансовых активов выглядит менее проблематичной по сравнению с токенизацией товаров или недвижимости, где технические и институциональные барьеры значительно выше.

Данные показывают, что уже сегодня наблюдается значительный приток реальных или обеспеченных активов в блокчейн, что подтверждает рост доверия к инфраструктуре Ethereum.

ЭКОНОМИКА БЛОКЧЕЙНА

Доверие в контексте блокчейна является не абстрактной категорией, а полноценным экономическим конструктом, ключевым параметром которого выступает стоимость обеспечения безопасности (далее — бюджет безопасности). Бюджет безопасности представляет собой совокупные расходы протокола на вознаграждение участников консенсуса (майнеров или валидаторов). Компоненты вознаграждения традиционно включают прямые платежи пользователей (транзакционные комиссии, состоящие из базовой комиссии и надбавки за скорость исполнения транзакции) и эмиссию нативной криптовалюты. Причем наибольшую долю обычно занимает именно эмиссия.

В сети Bitcoin эмиссия жестко ограничена потолком в 21 млн BTC, а также предусмотрен механизм халвинга — снижения вознаграждения за блок на каждые 210 тыс. блоков (~4 года). Вследствие этого модель безопасности Bitcoin напрямую зависит от рыночной цены BTC, поскольку при снижении номинального вознаграждения в криптовалюте недостаточная компенсация за счет роста цены может ослабить экономические стимулы майнеров и привести к их выходу из сети.

Для Ethereum при PoW структура вознаграждений была схожа с Bitcoin, но без жесткого эмиссионного потолка, что позволяло осуществлять более гибкую эмиссионную политику. С целью частичной компенсации эмиссионного эффекта в августе 2021 г. был внедрен механизм сжигания базовой комиссии, тогда как надбавка за скорость исполнения транзакции продолжала выплачиваться майнерам. Это ограничивало влияние на темпы прироста предложения ETH. После перехода на PoS эмиссия для вознаграждений валидаторов существенно снизилась, что позволило приостановить рост предложения и на некотором отрезке времени обеспечить его сокращение (в пике –0,38%). Однако последующие изменения, направленные на снижение транзакционных издержек и масштабирование сети, привели к возобновлению роста предложения ETH, но уже в разы медленнее, чем при PoW.

Необходимо детализировать понятие безопасности блокчейна, поскольку именно оно формирует экономическую основу доверия. Безопасность можно считать обеспеченной, если чистая стоимость атаки превышает потенциальную выгоду атакующего. Для сети PoW чистая стоимость атаки определяется затратами на приобретение и эксплуатацию оборудования (включая электроэнергию), необходимого для получения и поддержания контроля более 50% вычислительной мощности сети. При добропорядочном поведении майнеров это эквивалентно затратам на содержание эквивалента всей текущей вычислительной инфраструктуры вплоть до момента атаки. Обладатель такого контроля получает возможность единолично формировать консенсус и, следовательно, определять «правильную» историю транзакций. Классическим вектором атаки при этом выступает двойной расход (double spending): атакующий переводит свои средства на внешний рынок (например, продает BTC за фиат), а затем формирует альтернативную цепочку блоков, в которой эти средства остаются у него, тем самым одновременно и сохраняя криптовалюту, и получая фиатные активы.

Отдельные исследователи подчеркивают дилемму «выбери свой яд» («pick your poison») применительно к безопасности Bitcoin. В сообществе доминирует точка зрения, что угроза двойного расхода, вероятно, не является проблемой («probably

Таблица 1. Динамика TVL в блокчейне Ethereum, данные на конец года

Показатель	2018	2019	2020	2021	2022	2023	2024	2025 (август)
Total TVL, млн долл.	423	3 862	34 584	188 279	107 760	96 172	177 525	215 720
Real TVL, млн долл.	419	3 184	18 451	77 961	80 003	64 368	105 682	123 059
Доля Real TVL, %	99	82	53	41	74	67	59	57

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

not a problem»)[12], поскольку успешная атака вызовет падение рыночной стоимости криптовалюты, что создаст потери и для атакующего (как на оборудовании ввиду его узкой специализации, так и на использованных для атаки BTC). Однако возникает следующая ситуация: если отклонение рыночной цены BTC незначительное, то атака становится выгодной, и необходимо увеличивать бюджет безопасности; если же отклонение значительное, то это приведет к коллапсу всей системы из-за подрыва доверия к сети, а также обвалу существующих прямых и производных активов на криптовалюты. Появление такого мотива, как саботаж, дополнительно осложняет оценку потенциальной выгоды атакующего и делает количественную оценку риска более сложной (Budish, 2022).

Расходы на обеспечение безопасности протокола имеют природу постоянного денежного потока (flow, далее — потоковый бюджет) в форме регулярных выплат участникам консенсуса — майнерам или валидаторам. Напротив, затраты, необходимые для проведения атаки, имеют характер единовременного капитального изъятия (stock, далее — капитальный бюджет). Поскольку атаку можно проводить в пределах небольшого числа блоков, бюджет безопасности должен поддерживаться непрерывно. Эквивалентность бюджета и TVL сети практически недостижима, а более уместна концепция некоторой величины резервов, расход на использование которых сделал бы атаку экономически неразумной. Согласно модели Гордона–Лоэба[13], максимальная доля оправданного бюджета для риск-нейтральной компании не должна превышать ~37% ожидаемого ущерба или ниже — в зависимости от класса (линейный/нелинейный эффект инвестиций) (Gordon, Loeb, 2002). Данное значение может послужить ориентиром для оценки экономики безопасности блокчейна в условиях теоретической неопределенности (примем ожидаемый ущерб, равный совокупному TVL сети).

Методика оценки потокового бюджета одинакова для сетей PoW и PoS, она опирается на текущие потоки вознаграждений, формируемые комиссиями и эмиссией. Оценка же капитального бюджета принципиально различается. Для сети PoW она осложнена межстрановыми различиями в стоимости оборудования и электроэнергии. При этом привязка затрат к физическому капиталу снижает прямую зависимость от краткосрочной рыночной волатильности. В сетях PoS капитальный бюджет оценивается напрямую — через стоимость заблокированных у валидаторов средств. Однако номинирование этого капитала в нативной криптовалюте ведет к высокой корреляции ее ценовых колебаний с безопасностью сети.

Программируемые блокчейны вводят дополнительную сложность. В сетях, где наряду с нативной криптовалютой обращаются привязанные к реальным активам инструменты, последствия атак становятся менее однозначными, поскольку наличие обеспечения повышает связь токенов с реальной стоимостью, однако их рыночная цена по-прежнему определяется спросом и предложением и подвержена отклонениям даже вне кризисных ситуаций. Двойной расход стейблкоинов потенциально вызовет ценовые смещения нативного токена и других активов в сети, однако эмитент стейблкоина при наличии обязательств по выкупу обязан обеспечить конвертацию в реальный актив. Дополнительно значимую роль играют централизованные посредники (например, биржи), оперирующие стейблкоинами вместо фиатных резервов, что может оказывать как стабилизирующее, так и дестабилизирующее влияние — в зависимости от институциональных условий.

В итоге это поднимает вопрос о возможности масштабирования блокчейна. Так, рост TVL сети требует пропорционального роста бюджета безопасности, при этом усиливая стимул проводить саботажную атаку на блокчейн. Безусловно, бюджет на каждого конкретного пользователя незначителен, что позволило блокчейнам успешно развиваться, а также сглаживать неэффективность масштабирования за счет роста активности сети (рост комиссий). Повышение экономической эффективности применительно к модели безопасности возможно в блокчейнах с меньшим уровнем доверия, что в сообществе иллюстрирует трилемма[14] — компромисс между безопасностью, масштабируемостью и децентрализацией[15].

Понимания, как строится экономика безопасности блокчейна, мы можем перейти к рассмотрению конкретных показателей. Сегодня майнеры потребляют 0,3–0,8% мирового электричества, что эквивалентно ~15 млрд долл. в год (на момент 2022 г.) (Budish, 2022). Эти величины вкупе со стоимостью специализированного оборудования отражают текущие расходы майнеров, но не дают прямой картины предоставляемых им экономических стимулов (потокового бюджета)

[12] URL: https://en.bitcoin.it/wiki/Weaknesses#Attacker_has_a_lot_of_computing_power

[13] Экономико-математическая модель, которая используется для определения оптимального уровня инвестиций в обеспечение информационной безопасности путем анализа затрат и потенциальных потерь.

[14] URL: https://www.theblock.co/learn/249536/what-is-the-blockchain-trilemma

[15] В контексте статьи — эквивалент распределенного доверия.

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

для поддержания безопасности сети. В табл. 2 представлены соответствующие данные для сети Bitcoin[16]. Фактически это денежные потоки, состоящие из комиссии за транзакции и эмиссии BTC (в BTC и долларах), рассчитанные как сумма 4-дневных отрезков (источник данных) за период 2009–2024 гг.

Поскольку Bitcoin рассматривается преимущественно как средство сохранения стоимости, а его функционал ограничен передачей и хранением BTC, то вклад комиссий в общий бюджет безопасности остается незначительным на всем рассматриваемом интервале. Максимальные доли комиссий в бюджете безопасности составили 4,7% в долларах (2017 г.) и 3,4% в BTC (2018 г.). Эта динамика выявляет угрозу для жизнеспособности модели безопасности при переходе рынка к более зрелому состоянию (отсутствие кратного роста цены) в сочетании с регулярными халвингами (*halving* — уполовинивание) вознаграждения.

Сеть Ethereum (ETH) демонстрирует иную структуру потоков. Напомним, что с августа 2021 г. сеть начала сжигать базовую комиссию, а после с сентября 2022 г. она перешла на PoS, в результате чего эмиссия значительно снизилась. Данные по сети[17] представлены в табл. 3. Объемы комиссий за транзакции (с августа 2021 г. — только объем надбавок), эмиссии и сжигания рассчитаны на ежедневной основе для периода 2015–2024 гг. Итоговый бюджет безопасности в анализе включает эмиссию и комиссионные выплаты. Объем сжигания в расчет бюджета не включен, поскольку он не представляет собой прямой выплаты валидаторам. Фактически же сжигание функционирует как дефляционный механизм, сопоставимый по экономическому эффекту с обратным выкупом акций, так как его влияние адресова-

[16] URL: https://www.blockchain.com/explorer/charts/total-bitcoins

[17] URL: https://etherscan.io/charts

Таблица 2. Бюджет безопасности блокчейна Bitcoin

Год	Комиссии		Эмиссия		Итого	
	BTC	тыс. долл.	BTC	тыс. долл.	BTC	тыс. долл.
2009	0,26	0	1 607 175	0	1 607 175	0
2010	6,83	0	3 430 300	210	3 430 307	210
2011	655	8	2 961 141	17 743	2 961 797	17 751
2012	1636	18	2 611 134	22 102	2 612 770	22 121
2013	4024	598	1 598 062	297 860	1 602 086	298 459
2014	1134	688	1 472 400	772 959	1 473 534	773 648
2015	1992	618	1 355 850	369 284	1 357 843	369 902
2016	6008	3633	1 041 069	585 612	1 047 078	589 245
2017	25 020	138 010	704 025	2 776 885	729 045	2 914 895
2018	6471	72 438	672 587	5 065 751	679 058	5 138 190
2019	4991	39 689	680 238	4 997 620	685 229	5 037 310
2020	6687	82 758	457 190	5 101 279	463 878	5 184 038
2021	5303	253 075	328 094	15 505 096	333 397	15 758 172
2022	1376	36 725	331 713	9 374 990	333 090	9 411 716
2023	6015	204 594	335 675	9 631 344	341 691	9 835 938
2024	4725	294 278	218 826	14 404 927	223 551	14 699 206

Таблица 3. Бюджет безопасности блокчейна Ethereum

Год	Комиссии		Эмиссия		Сжигание		Итого	
	ETH	тыс. долл.	ETH	тыс. долл.	ETH	тыс. долл.	ETH	тыс. долл.
2015	2 592	2	76 166 283	3657			76 168 875	3660
2016	14 974	148	11 327 570	112 881			11 342 544	113 029
2017	119 940	46 433	9 219 008	1 774 232			9 338 948	1 820 666
2018	268 195	160 161	7 429 909	3 598 863			7 698 104	3 759 024
2019	186 670	34 666	4 961 550	898 752			5 148 220	933 419
2020	1 524 139	596 026	4 988 606	1 536 898			6 512 745	2 132 925
2021	2 128 808	4 784 572	5 268 840	14 693 378	1 314 646	5 121 025	7 397 648	19 477 951
2022	283 124	641 746	3 961 412	8 863 229	1 482 911	3 656 670	4 244 536	9 504 976
2023	215 550	391 262	750 404	1 356 206	1 093 504	2 015 421	965 954	1 747 469
2024	158 529	483 178	926 449	2 824 508	633 999	1 985 157	1 084 978	3 307 687

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

но всем держателям ETH, а не только операторам консенсуса.

По результатам расчетов доля комиссий в бюджете безопасности Ethereum достигала максимума 27,9% в долларах (2020 г.) и 28,8% в ETH (2021 г.). По итогам 2024 г. доля комиссий составляла около 14,6%. При учете эффекта сжигания базовой комиссии доля пользовательских потоков в 2024 г. возрастает до 74,6%. Следует отметить, что валидаторы непосредственно получают лишь эмиссию и надбавки. Тем не менее высокая доля пользовательских потоков и модель дефляции указывают на более устойчивую экономическую модель безопасности по сравнению с Bitcoin, где основная часть бюджета формируется эмиссией.

Далее предлагается рассмотреть показатели капитального бюджета для сети Ethereum. Отметим, что заблокированные в стейкинге токены ETH — собственность валидаторов и одновременно ключевой элемент безопасности, то есть они не являются фактически бюджетом безопасности. Бюджет же нацелен на максимальное привлечение такого капитала в стейкинг и его удержание. Рассмотрим эти показатели и оценим их соотношение относительно TVL сети.

В табл. 4 представлено отношение бюджета безопасности (рассчитан аналогично табл. 2) и медианного значение стоимости заблокированных в стейкинге ETH[18] в долларах к среднегодовому значению TVL (по данным на начало/конец квартала) по категориям Total, Crypto и Real, а также отношение стоимости стейка к годовому бюджету безопасности. Безусловно, когда речь идет о криптовалютах, основной ставкой является рост цены ETH. Однако данное соотношение представлено для иллюстрации возможности альтернативного «дивидендного» подхода.

Покрытие TVL за счет текущих выплат из потокового бюджета безопасности остается незначительным — в разы ниже условного порога в ~37%, что может свидетельствовать о потенциальном пространстве для эффективного наращивания бюджета. Накопленный капитальный бюджет демонстрирует обратную динамику — его доля в покрытии увеличивается. Это объясняется как ростом объема заблокированных в стейкинге токенов, так и повышением рыночной стоимости ETH, поэтому утверждать о полном уходе от зависимости безопасности Ethereum от ценовой динамики нативной криптовалюты нельзя. Наблюдавшиеся в 2020–2022 гг. периоды низкого покрытия не породили публичных инцидентов успешных атак. Однако это не равнозначно утверждению о надежности состояния сети в такие периоды. Реальное прикладное значение блокчейна стало существенно возрастать лишь в конце 2024–2025 гг., что в полной мере еще не отражено в имеющихся данных. Интерес к сценариям саботажа мог возрасти, начиная с этого периода времени.

Особенно уязвима категория Real TVL, поскольку при падении стоимости ETH покрытие реальных активов стремительно снижается, тогда как агрегированная стоимость криптовалют может одновременно сокращаться, сглаживая отношение для Crypto TVL. Наглядным примером служит 2023 г., где разница в покрытии между Crypto TVL и Real TVL составляла почти 2,5 раза, что свидетельствует о реальной угрозе для обеспеченных реальных активов в условиях неблагоприятной ценовой динамики.

Важно отметить, что расчет потокового бюджета исходил из предпосылки, что валидатор реализует полученные вознаграждения в день их получения с целью нейтрализации валютного риска. Такой подход представляет максимально долларовоориентированную трактовку потоков. В реальной практике периодичность конверсии может варьироваться (месяц, квартал, год) и оказывать влияние на интерпретацию результатов. Тем не менее при сравнении показателей в натуральном выражении (в ETH) значимых отклонений по агрегированным метрикам не зафиксировано: Flow: ~2,4% — к Total TVL и ~4,2% — к Real TVL; Stock: ~42,3 и ~142,7% соответственно. Данные приведены на 2024 г., за прочие годы аналогичное незначительное отклонение сохраняется для Flow,

[18] URL: https://dune.com/hildobby/eth2-staking

Таблица 4. Соотношение потокового и капитального бюджетов безопасности к TVL сети

Год	Flow Ratio, %			Stock (median) Ratio, %			Stock / Flow
	Total	Crypto	Real	Total	Crypto	Real	
2018	2963,0	36221,1	3227,0				
2019	43,1	230,5	53,0				
2020	13,6	35,8	22,0	1,1	4,7	2,9	0,1
2021	16,7	29,4	38,7	14,0	24,6	32,3	0,8
2022	6,7	15,6	11,6	15,3	35,9	26,8	2,3
2023	1,8	5,8	2,6	43,8	143,1	63,1	24,5
2024	2,5	6,1	4,2	76,7	188,3	129,5	31,1

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

тогда как для Stock разрыв существенный, однако он объясняется динамикой стейкинга на раннем этапе его развития (то есть не является показательным). Наибольшее расхождение наблюдается в отношении Stock / Total TVL и объясняется замедленной динамикой цены ETH относительно прочих криптоактивов в соответствующий период.

Кроме прямых выплат из бюджета, валидаторы получают доступ к «экономической ренте» за счет манипуляции порядком включения транзакций (MEV). Для Ethereum доля MEV относительно бюджета безопасности составила примерно 1,6 в 2022 г., 28,2 — в 2023 г. и 17,8% — в 2024 г. Эти величины представляют значимые денежные потоки, которые не выплачиваются напрямую, но притягивают капитал валидаторов и тем самым повышают фактическое покрытие TVL и безопасность сети.

В заключение отметим, что для большинства блокчейнов основным источником бюджета безопасности остается эмиссия нативной криптовалюты, а не прямые комиссионные платежи. Современная финансиализация экономики является источником формирования спекулятивной оценки нативной криптовалюты, что обеспечивает жизнеспособность модели безопасности на раннем этапе. В дальнейшем предполагается переход к более фундаментальным источникам пополнения бюджета — рост прикладного использования и увеличение доли комиссионных выплат.

Цель данного раздела — продемонстрировать практическую экономическую основу доверия в блокчейне. Помимо прямых выплат участникам консенсуса, обеспечивающих текущие стимулы, держатели нативной криптовалюты фактически участвуют в финансировании безопасности через механизм эмиссии (непрямой налог), а пользователи сети оплачивают ее напрямую в виде транзакционных комиссий. Дополнительные экономические стимулы (такие как MEV) усиливают приток капитала участниками консенсуса и тем самым повышают фактическое покрытие TVL. Таким образом, доверие в системах блокчейн представляет собой экономически обоснованную модель обеспечения безопасности.

ЗАКЛЮЧЕНИЕ

В качестве заключения настоящей статьи автор формулирует ряд выводов относительно технологии блокчейн и концепции доверия в ней.

1. *Доверие в блокчейне — экономическая конструкция, а не теоретическая абстракция.* Концепция распределенного доверия существовала давно, однако блокчейн задал этим идеям понятный, технически выверенный экономический механизм реализации, сочетая его с принципами алгоритмизированного доверия без необходимости «компромисса провайдера».

2. *Модель безопасности блокчейна жизнеспособна.* Это подтверждается притоком реального капитала и отсутствием значимых инцидентов безопасности. Приток средств в DeFi и токенизация RWA показывают, что на блокчейн переносится не только спекулятивный капитал, но и реальные финансовые активы.

3. *Экономика безопасности дорогая, что является фундаментальным ограничением для масштабирования*. Рост объема активов в блокчейне требует сопоставимого роста расходов на безопасность. При этом блокчейны могут жертвовать уровнем доверия для достижения большей экономической эффективности.

4. *Ключевая инновация — ребалансировка рисков и расходов.* Блокчейн встраивает доверие в архитектуру системы, устраняя риски оппортунистического поведения за счет повышения операционной ответственности пользователя. Дороговизна и неэффективность модели безопасности равномерно распределяются между пользователями сети и держателями нативной криптовалюты, что обусловливает жизнеспособность модели.

5. *Нативный токен и эмиссия как каркас экономической модели.* Возможность поддерживать крупный и неэффективный бюджет безопасности возникла исключительно благодаря непрямому налогу на держателей нативного токена. И до сих пор бюджеты безопасности блокчейнов остаются сильно зависимыми от эмиссионных поступлений.

Доверие в блокчейне является результатом сочетания распределенного и алгоритмизированного доверия. Отдельные авторы отмечают наличие организационного доверия, то есть доверия к «социальному слою» (майнерам/валидаторам, биржам, разработчикам, активному сообществу), что создает технологический слой, и также подчеркивают невозможность вписать доверие в блокчейне в существующую категорию (Chawla, 2020). В цифровой среде, где любое взаимодействие определено работой тех или иных алгоритмов, понятие алгоритмизированного доверия становится базовым элементом, в связи с чем формы доверия к различным видам технологий будут определяться на основании иных характеристик, которые по умолчанию будут включать фактор доверия к алгоритмам. По этой причине автор формулирует собственное определение доверия в блокчейне, которое при соблюдении определенных условий может реализовываться в любой цифровой системе.

Доверие в блокчейне — интегральное (архитектурное) свойство цифровой системы, представля-

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

ющее собой однородное ожидание доверителями корректного и необратимого изменения состояния системы, реализованного алгоритмически и опирающегося на экономически обоснованный механизм распределенного консенсуса.

Блокчейн сегодня — инфраструктура, проверенная временем и постепенно обретающая все более широкое практическое применение. Заложенные в нем механизмы доверия создают потенциал для большего — становления блокчейна как института. «Институт — любая коллективно принятая система правил (процедур, практик), позволяющая нам создавать институциональные факты» (Searle, 2005). В некотором смысле публичные блокчейны начинали как попытка создавать институты — токен как право собственности и/или самостоятельные деньги, децентрализованные автономные организации (ДАО), принцип «код — это закон», который действительно реализуется на практике (без возможности «отмены принципа» в чрезвычайной ситуации), и т.д. Однако сегодня кажется, что эта попытка провалилась под давлением собственной тяжести построенного «Дикого Крипто-Запада» и все большей адаптации — как очередной инструмент традиционной финансовой системы.

СПИСОК ЛИТЕРАТУРЫ

Жилина И.Ю. (2008). Доверие в экономике // Экономические и социальные проблемы России. № 1. С. 37. URL: https://cyberleninka.ru/article/n/doverie-v-ekonomike

Леонова И.Ю. (2015). Доверие: понятие, виды и функции // Вестник Удмуртского университета. Серия Философия. Психология. Педагогика. № 2. С. 8. URL: https://cyberleninka.ru/article/n/doverie-ponyatie-vidy-i-funktsii

Трындина Н.С., Устюжанина Е.В. (2023). Доверие как экономическая категория: подходы к классификации и систематизации // Креативная экономика. Т. 17. № 1. С. 39–54. DOI: 10.18334/ce.17.1.116590

Algan Y., Cahuc P. (2014). Trust, Growth and Well-Being: New Evidence and Policy Implications. Handbook of Economic Growth, Elsevier, no. 2, pp. 49–120. DOI: 10.1016/B978-0-444-53538-2.00002-2

Allen D.W.E., Berg C., Markey-Towler B., Novak M., Potts J. (2020). Blockchain and the evolution of institutional technologies: Implications for innovation policy, Research Policy, vol. 49, no. 1, p. 8. DOI: 10.1016/j.respol.2019.103865

Atzori M. (2017). Blockchain Technology and Decentralized Governance: is the State Still Necessary? Journal of Governance and Regulation, vol. 6, no. 1, pp. 45–62. DOI: 10.22495/jgr_v6_i1_p5

Budish E.B. (2022). The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain. Chicago Booth Research Paper, no. 18-07, p. 71. DOI: 10.2139/ssrn.3197300

Chawla C. (2020). Trust in blockchains: Algorithmic and organizational. Journal of Business Venturing Insights, vol. 14, p. 8. DOI: 10.1016/j.jbvi.2020.e00203

Gordon L.A., Loeb M.P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security, vol. 5, no. 4, pp. 438–457. DOI: 10.1007/1-4020-8090-5_9

Hawlitschek F., Notheisen B., Teubner T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. Electronic Commerce Research and Applications, no. 29, pp. 50–63. DOI: 10.1016/j.elerap.2018.03.005

Martini E., Vespasiano F. (2020). Trust and Reciprocity: The Foundations of the Sharing Economy. Italian Sociological Review, vol. 10, no. 2, pp. 239–256. DOI: 10.13136/isr.v10i2.338

Mosch R.H.J. (2004). The Economic Effect of Trust: Theory and Empirical Evidence. PhD, Vrije Universiteit Amsterdam, Amsterdam. 210 p. URL: https://research.vu.nl/en/publications/the-economic-effects-of-trust-theory-and-empirical-evidence/

Pinyol I., Sabater-Mir J. (2013). Computational trust and reputation models for open multi-agent systems: a review. Artificial Intelligence Review, vol. 40, pp. 1–25. URL: DOI: 10.1007/s10462-011-9277-z

Searle J.R. (2005). What is an institution? Journal of Institutional Economics, vol. 1, no. 1, pp. 1–22. DOI: 10.1017/S1744137405000020

Yaga D., Mell P., Roby N., Scarfone K. (2019). Blockchain Technology Overview. National Institute of Standards and Technology Internal, p. 68. DOI: 10.6028/NIST.IR.8202

REFERENCES

Zhilina I.Yu. (2008). Trust in the economy, *Economic and Social Problems of Russia*, no. 1, p. 37. (In Russ.) URL: https://cyberleninka.ru/article/n/doverie-v-ekonomike

Leonova I.Yu. (2015). Trust: definition, types and functions. *Bulletin of Udmurt University. Series Philosophy. Psychology. Pedagogy*, no. 2, p. 8. (In Russ.) URL: https://cyberleninka.ru/article/n/doverie-ponyatie-vidy-i-funktsii

Tryndina N.S., Ustyuzhanina E.V. (2023). Trust as an economic category: approaches to classification and systematization. *Creative Economy*, vol. 17, no. 1, pp. 39–54. (In Russ.) URL: https://doi.org/10.18334/ce.17.1

Algan Y., Cahuc P. (2014). Trust, Growth and Well-Being: New Evidence and Policy Implications. *Handbook of Economic Growth*, *Elsevier*, no. 2, pp. 49–120. DOI: 10.1016/B978-0-444-53538-2.00002-2

https://doi.org/10.33293/1609-1442-2026-29(2)-124-137

Allen D.W.E., Berg C., Markey-Towler B., Novak M., Potts J. (2020). Blockchain and the evolution of institutional technologies: Implications for innovation policy, *Research Policy*, vol. 49, no. 1, p. 8. DOI: 10.1016/j.respol.2019.103865

Atzori M. (2017). Blockchain Technology and Decentralized Governance: is the State Still Necessary? *Journal of Governance and Regulation*, vol. 6, no. 1, pp. 45–62. DOI: 10.22495/jgr_v6_i1_p5

Budish E.B. (2022). The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain. *Chicago Booth Research Paper*, no. 18-07, p. 71. DOI: 10.2139/ssrn.3197300

Chawla C. (2020). Trust in blockchains: Algorithmic and organizational. *Journal of Business Venturing Insights*, vol. 14, p. 8. DOI: 10.1016/j.jbvi.2020.e00203

Gordon L.A., Loeb M.P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457. DOI: 10.1007/1-4020-8090-5_9

Hawlitschek F., Notheisen B., Teubner T. (2018). The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic Commerce Research and Applications*, no. 29, pp. 50–63. DOI: 10.1016/j.elerap.2018.03.005

Martini E., Vespasiano F. (2020). Trust and Reciprocity: The Foundations of the Sharing Economy. *Italian Sociological Review*, vol. 10, no. 2, pp. 239–256. DOI: 10.13136/isr.v10i2.338

Mosch R.H.J. (2004). *The Economic Effect of Trust: Theory and Empirical Evidence*. PhD, Vrije Universiteit Amsterdam, Amsterdam.p. 210. URL: https://research.vu.nl/en/publications/the-economic-effects-of-trust-theory-and-empirical-evidence/

Pinyol I., Sabater-Mir J. (2013). Computational trust and reputation models for open multi-agent systems: a review. *Artificial Intelligence Review*, vol. 40, pp. 1–25. DOI: 10.1007/s10462-011-9277-z

Searle J.R. (2005). What is an institution? *Journal of Institutional Economics*, vol. 1, no. 1, pp. 1–22. DOI: 10.1017/S1744137405000020

Yaga D., Mell P., Roby N., Scarfone K. (2019). Blockchain Technology Overview. *National Institute of Standards and Technology Internal*, p. 68. URL: DOI: 10.6028/NIST.IR.8202