Технологии информационного общества

ЦИФРОВЫЕ ВАЛЮТЫ И КРИПТОВАЛЮТЫ В ЭКОНОМИКЕ БУДУЩЕГО

Статья рекомендована к публикации членом редакционного совета А. В. Богдановым 2025.09.15

Ху Битай

Санкт-Петербургский государственный университет, факультет прикладной математики – процессов управления, аспирант
Санкт-Петербург, Российская Федерация
bitaihu@gmail.com

Хватов Валерий Владимирович

DGT Technologies AG, вице-президент по технологиям
Торонто, Канада
valery.khvatov@gmail.com

Щеголева Надежда Львовна

Доктор технических наук, доцент
Санкт-Петербургский государственный университет, факультет прикладной математики – процессов управления, профессор
Санкт-Петербург, Российская Федерация
n.shchegoleva@spbu.ru

Аннотация

Исследование анализирует эволюцию блокчейн-технологии, начиная с Bitcoin и Ethereum, раскрывая их роль в формировании децентрализованной экономики. В работе систематизированы ключевые алгоритмы консенсуса, их преимущества и ограничения, а также перспективы гибридных моделей. Особое внимание уделено цифровому юаню — первой цифровой валюте центрального банка, сочетающей централизованный контроль с инновациями (оффлайн-платежи, программируемость). Исследование подчёркивает необходимость баланса между инновациями, безопасностью и международной гармонизацией стандартов для устойчивого развития цифровой экономики.

Ключевые слова

блокчейн; биткоин; Эфириум; алгоритм консенсуса; смарт-контракт; цифровая валюта Центрального банка; цифровой юань; децентрализация; децентрализованные финансы; невзаимозаменяемый токен; Central Bank Digital Currency; CBDC; Digital Currency Electronic Payment; DCEP; Decentralized Finance; DeFi; Non-Fungible Token; NFT

Введение

Блокчейн и криптовалюты, появившиеся в эпоху цифровой трансформации, пересматривают основы доверия, прозрачности и управления данными, бросая вызов традиционным институтам. Технология, впервые реализованная в 2008 г. анонимным разработчиком Сатоши Накамото через Bitcoin, заменила посредников децентрализованным консенсусом [1], используя криптографические цепочки для неизменности записей. Ее значение выходит за рамки финансов: блокчейн формирует «интернет ценностей», передавая любые активы между участниками сети. Bitcoin, как «цифровое золото», оспорил фиатные системы и стал катализатором дискуссий о природе денег.

https://doi.org/10.52605/16059921_2026_01_122

Истинный прорыв пришел в 2015 г. с Ethereum, превратившим блокчейн в программируемую платформу [2]. Смарт-контракты Виталика Бутерина открыли эру Decentralized Applications (DApps), токенизации и Decentralized Autonomous Organization (DAO). Современные криптовалюты стали многофункциональными экосистемами: стейблкоины – реализуют доступ к реальным активам, Non-Fungible Token (NFT) – обеспечивают уникальность произведений искусства, Decentralized Finance (DeFi) – предназначены для реализации финансовых услуг без банков. Рост цифровых активов сопряжен с вызовами – от регуляторной неопределенности и экологических издержек майнинга до противоречий между анонимностью и нормами.

Исследование показывает, как технология, начавшаяся с Bitcoin, становится основой цифровой экономики XXI века. Следующие разделы анализируют архитектуру блокчейна, роль Bitcoin, инновации Ethereum и разнообразие криптовалют, демонстрируя их влияние на глобальную экономическую парадигму.

1 Блокчейн

Блокчейн как технология объединяет криптографию, распределенные вычисления и теорию игр [3], представляя собой децентрализованную базу данных с неизменяемой цепочкой блоков. Стоит отметить, что блокчейн относится к категории технологий распределенного реестра (Distributed Ledger Technologies – DLT), где данные хранятся в синхронизированной форме на множестве узлов. Однако в отличие от других DLT-решений (например, направленных ациклических графов), блокчейн характеризуется строгой последовательностью криптографически связанных блоков. Его ключевые принципы — отсутствие единого центра управления, прозрачность транзакций и защита от подделки через криптографические алгоритмы. В зависимости от уровня доступа блокчейн делится на три типа: публичные (Bitcoin, Ethereum), консорциумные (управляемые группами организаций) и частные (контролируемые одним субъектом). Эта архитектура исключает риски централизованных систем, обеспечивая устойчивость к атакам [4] и коллективное верифицирование данных.

Таким образом, блокчейн трансформировался из узкоспециализированной технологии в основу цифровой экономики, объединяя дисциплины от математики до экономики и формируя новые парадигмы управления данными и активами.

2 Биткоин

Bitcoin, созданный Сатоши Накамото в 2009 г., стал первой децентрализованной цифровой валютой, не зависящей от банков или государств. Его эмиссия ограничена 21 миллионом монет, а алгоритм халвинга (уменьшения награды майнеров вдвое каждые 4 года) обеспечивает дефицитность: после апрельского сокращения 2024 г. вознаграждение за блок снизилось до 3,125 Bitcoin (BTC) [4]. Выпуск монет завершится к 2140 г., что подчеркивает антиинфляционную природу системы.

Ключевая инновация Bitcoin — p2p-платежи без посредников через блокчейн. Это достигается тремя принципами:

- прямые транзакции между пользователями, исключающие финансовые институты;
- криптографическая защита: цифровые подписи (закрытый ключ для подписания, открытый — для верификации) гарантируют, что только владелец может распоряжаться средствами;
- неизменность реестра — каждая операция фиксируется в блокчейне, предотвращая подделку и двойное расходование (повторное использование одних и тех же средств).

Технология сочетает шифрование с открытым/закрытым ключом: данные транзакций шифруются открытым ключом, а расшифровка возможна только приватным ключом владельца, обеспечивая конфиденциальность и аутентичность. Таким образом, Bitcoin не просто платежный инструмент, а автономная система, переопределяющая понятия доверия и финансового суверенитета.

2.1 Хеш-функция

Хеш-функции, такие как SHA-256 в Bitcoin, обеспечивают криптографическую целостность данных (см. рис. 1).

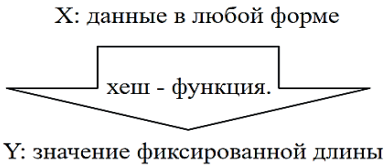

Рис. 1. Хеш-функция

Их ключевые свойства — односторонняя необратимость (невозможность восстановить исходные данные из хеша) и устойчивость к коллизиям (уникальность вывода для любого ввода). В отличие от симметричного шифрования, хеширование не требует ключей: например, хеш транзакции «Hello, world!» через SHA-1 преобразует текст в двоичный код, дополняет его до 512 бит и через серию раундов смешивает с константами (h0–h4), формируя уникальный 160-битный идентификатор. Этот процесс, даже для больших данных, выполняется за секунды, гарантируя неизменность записей в блокчейне.

Таблица 1. Криптографические хеш-функции и их характеристики

Хеш-функция	Основные характеристики	Длина вывода
MD5 (небезопасен)	128-битный хеш, ранее использовался для проверки целостности данных	128 бит
SHA-1 (уязвим)	160-битный хеш, основа ранних систем безопасности	160 бит
SHA-256	256-битный хеш, стандарт для блокчейн-технологий (Bitcoin)	256 бит
SHA-512	512-битный хеш, для систем с повышенными требованиями безопасности	512 бит

Генезис-блок Bitcoin (с хешем 000000000019d6...) служит неизменной точкой отсчета всей цепи. Каждый новый блок содержит хеш предыдущего, создавая криптографически связанную последовательность. Это исключает подмену данных: любая попытка изменить транзакцию изменит хеш блока и разорвет цепь, что будет мгновенно обнаружено узлами сети. Таким образом, SHA-256 и структура блокчейна обеспечивают безопасность и доверие в децентрализованной системе без централизованного контроля.

2.2 Стадии жизненного цикла блокчейна

Работа блокчейна состоит из пяти стадий, показанных на рис. 2. На первой стадии участники сети формируют новые транзакции, упаковывают транзакции в блоки, добавляя криптографические метки (хеши) для подтверждения подлинности, при этом каждый блок содержит набор проверенных операций и связывается с предыдущим блоком через хеш-указатель, формируя хронологическую цепочку. На второй стадии инициированные транзакции распространяются через децентрализованную P2P-сеть, достигая узлов-валидаторов.

На третьей стадии запускается механизм консенсуса: узлы независимо друг от друга проверяют валидность блока — корректность подписей, отсутствие двойных трат и соответствие правилам сети. Только после подтверждения большинством участников блок добавляется в реестр (четвертая стадия). Этот процесс гарантирует неизменность данных, так как изменение любого блока требует пересчета всей последующей цепи, что практически невозможно.

На завершающей пятой стадии синхронизированный реестр фиксируется на всех узлах, обеспечивая прозрачность и устойчивость к цензуре. Участники могут проверять историю транзакций, а приложения взаимодействуют с блокчейном через API, используя его как доверенную инфраструктуру для DApps, смарт-контрактов и цифровых активов.

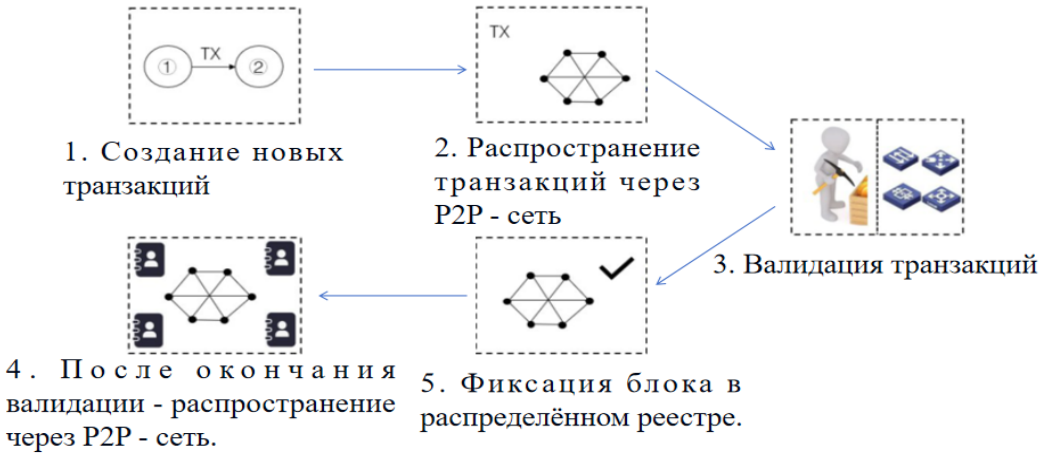

Рис. 2. Стадии жизненного цикла блокчейна

2.3 Формат хранения и ведения учета в биткоин

Хеш-значение в текущем заголовке блока включает хеш-значение предыдущего заголовка блока плюс хеш-значение транзакционных данных в текущем теле блока.

Если кто-то изменит A в первом блоке, то по значению ABC в последнем заголовке блока можно увидеть, что A было подделано (см. рис. 3).

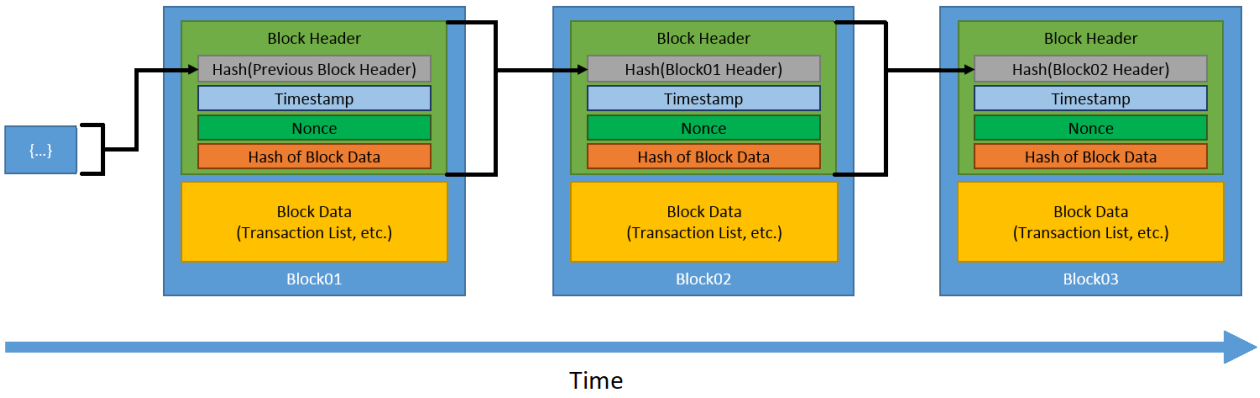

Рис. 3. MerkleRoot: Текущий хеш транзакционных данных в блоке

Для проверки транзакций (целостности данных) используется Корень Меркла [5], т. е. узел блокчейна должен проверить только отдельные блоки в дереве Меркла. Это называется доказательством Меркла. Например, в дереве Меркла, представленном ниже на рис. 4, узел блокчейна должен проверить только HAB, HC и HEFGH, чтобы убедиться, что хэш блока HD корректный и не изменялся.

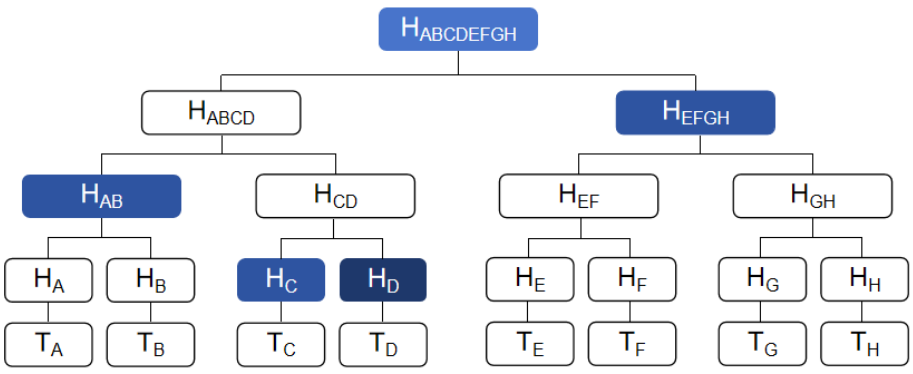

Рис. 4. Пример доказательства MerkleRoot

2.4 Форк, вызванный разными взглядами на биткоин в сообществе

Ограничение размера блока Bitcoin (1 МБ, ~ 8 транзакций/секунду) стало катализатором раскола в сообществе. Форк (разветвление) — это разделение блокчейна на две версии, возникающее при изменении правил сети. Хардфорк — тип форка с обратной несовместимостью: узлы, не обновившие ПО, перестают распознавать новые блоки. В отличие от софтфорка (обратно совместимые изменения), хардфорк создает параллельную цепь с независимой историей. Сторонники «Bitcoin как хранилища ценности» настаивали на сохранении текущих параметров, аргументируя это приоритетом безопасности сети и ненужностью частых платежей для актива с волатильным курсом. Их оппоненты, выступавшие за «Bitcoin как средство платежа», требовали увеличения блока Bitcoin для снижения комиссий и ускорения транзакций.

Этот идеологический конфликт привел к первому хардфорку Bitcoin 1 августа 2017 г., в результате которого появился Bitcoin Cash (BCH) [6] с увеличенным размером блока. BCH не только сохранил технические основы Bitcoin, но и стал самой капитализированной «ветвью» в истории криптовалют, символизируя борьбу между философией цифрового золота и прагматизмом платежного инструмента (см. рис. 5).

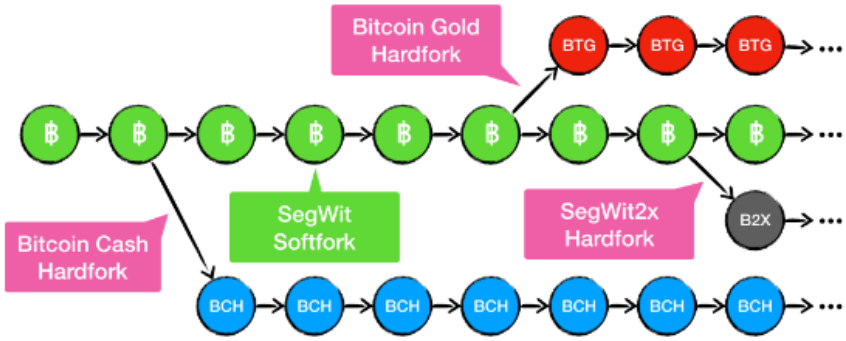

Рис. 5. Форк Bitcoin

2.5 Механизм консенсуса биткоин

Bitcoin использует механизм консенсуса Proof-of-Work (PoW), где майнеры решают криптографические задачи для создания блоков. Ключевое правило — признается только самая длинная цепь, что гарантирует безопасность сети. Каждый блок требует подбора такого Nonce (number that can only be used once) чтобы хеш его заголовка соответствовал целевой сложности (difficulty), автоматически корректируемой каждые 2016 блоков (~14 дней) для поддержания среднего времени генерации в 10 минут.

Целевая сложность (difficulty) в октябре 2024 г. составила 95,672,703,408,223.94 [7]

Два основных стимулирующих эффекта Bitcoin для майнеров:

- системная награда за создание блока (Block);
- комиссия за транзакции, полученная при создании блока (майнер может получить комиссию за все транзакции в его блоке).

К 2140 г., когда эмиссия Bitcoin прекратится, единственным доходом майнеров станут комиссии за транзакции. Их размер будет определять приоритет обработки: чем выше комиссия, тем быстрее транзакция попадет в блок. Это создаст рыночный механизм, где пользователи конкурируют за место в блокчейне, а майнеры оптимизируют прибыль, выбирая выгодные операции [8].

Безопасность сети обеспечивается вычислительной мощностью (хэш-рейтом), которая напрямую связана с уровнем сложности (difficulty). Например, при сложности 16,10 требуемый хэш-рейт рассчитывается как $\frac{16.1*10^{12}*2^{32}}{600}$, что демонстрирует масштаб ресурсов для генерации блока. Теоретически, контроль над 51% хэш-рейта позволит провести двойное расходование, но затраты на оборудование (ASIC-майнеры), электроэнергию и обслуживание делают такую атаку экономически бессмысленной.

Это подтверждает гипотезу Сатоши Накамото: рациональный участник с доминирующей вычислительной мощностью не станет атаковать сеть, так как его инвестиции обесценятся. Таким

образом, PoW-механизм Bitcoin балансирует между стимулами майнеров и устойчивостью к угрозам, сохраняя децентрализацию.

3. Эфириум

Ethereum, занимающий второе место после Bitcoin по влиянию в криптоиндустрии, переосмыслил роль блокчейна, превратив его в децентрализованный суперкомпьютер. Его ключевая инновация — возможность выполнения программных кодов (смарт-контрактов) без централизованного контроля. В отличие от традиционных систем с централизованным исполнением кода на серверах, Ethereum распределяет исполнение приложений по сети узлов, обеспечивая автономность и устойчивость к цензуре [9].

Белая книга проекта Ethereum провозгласила его миссией создание платформы для децентрализованных приложений (decentralized applications, DApps) — от токенизации активов до управления децентрализованными автономными организациями (decentralized autonomous organization, DAO). Смарт-контракты здесь не просто автоматизируют соглашения, но и устраняют посредников: условия выполняются алгоритмически, а данные записываются в неизменяемый блокчейн. Это открыло путь для децентрализованных финансов (DeFi), токенов с уникальными свойствами (NFT) и Web3-приложений, сделав Ethereum основой цифровой экономики нового поколения.

3.1 Смарт-контракт

Смарт-контракты Ethereum — это самоисполняющиеся алгоритмические соглашения, реализованные с помощью блокчейна [10]. В отличие от традиционных договоров, их выполнение автоматизировано и не требует посредников. Эта технология стала основой для децентрализованных приложений, работающих на платформе Ethereum. В отличие от централизованных аналогов (например, App Store), DApps управляются сетью узлов, обеспечивая прозрачность (все транзакции публично проверяются в блокчейне) и устойчивость к цензуре (отсутствие единой точки контроля для блокировки приложений).

Несмотря на то, что Ethereum и Bitcoin используют один механизм консенсуса PoW (с переходом Ethereum на PoS), цифровые подписи и P2P-архитектуру, их ключевое различие — функциональность. Ethereum выходит за рамки платежей, превращая блокчейн в среду для запуска приложений: от игр (CryptoKitties с уникальными NFT на стандарте ERC721) до децентрализованных финансов (DeFi). Например, в CryptoKitties каждая «кошка» — цифровой актив с неизменным ID, а транзакции управляются смарт-контрактами, исключая централизованный контроль.

Особенно активно использует Ethereum финансовый сектор: смарт-контракты позволяют создавать сложные инструменты — от кредитования до токенизированных активов. Это превращает блокчейн в инфраструктуру «цифровой экономики», где каждый адрес становится универсальным счетом для программируемых финансовых операций [11].

3.2 Цифровые активы в блокчейне

Цифровые активы в блокчейне, такие как стейблкоины (например, USD T [12], привязанный к доллару) или токены (представляющие право собственности, услуги или коллекционные объекты), расширили финансовые возможности технологии. Стейблкоины обеспечивают стабильность, а токены стандарта ERC-20[13]/ERC-721 [14] превратили блокчейн в инструмент для токенизации реальных активов — от искусства до акций. ICO (первичное предложение монет) стало новым механизмом привлечения инвестиций, где токены выступают как «цифровые акции» или утилитарные инструменты [15]. Однако переход от Proof-of-Work (PoW) к Proof-of-Stake (PoS) и его модификациям (DPoS) был вызван проблемами энергопотребления и централизации майнинга. DPoS, используемый в EOS, делегирует верификацию блоков избранным узлам, повышая скорость, но критикуется за компромисс с децентрализацией.

Регуляторные вызовы остаются ключевым барьером. Пример проекта Telegram (GRAM) показывает глобальную юрисдикционную сложность: SEC США заблокировала токен, аргументируя это нарушением законов о ценных бумагах, даже при отсутствии прямой регистрации в стране [16]. Китай, запретил ICO и криптобиржи, вступив в противоречие с либеральными юрисдикциями. Эти конфликты подчеркивают двойственность криптоактивов —

как инновационного финансового инструмента и объекта правовых рисков, требующего гармонизации международных стандартов.

4.Сравнение основных механизмов консенсуса и прогресс исследований по алгоритмам их улучшения

Блокчейн-консенсусные алгоритмы определяют, как децентрализованные сети достигают согласия о состоянии данных. Их эволюция отражает поиск баланса между тремя ключевыми параметрами: безопасностью, скоростью и децентрализацией. Ниже анализируются основные механизмы и их современные модификации.

4.1 Proof of Work (PoW)

Пионером консенсуса стал алгоритм PoW, реализованный в Bitcoin. Его суть заключается в решении криптографических задач методом перебора, где майнеры соревнуются за подбор значения Nonce для соответствия хеша блока заданной сложности. Хотя PoW обеспечивает высокую устойчивость к атакам (требуется контроль 51% вычислительной мощности), его критикуют за экстремальное энергопотребление и низкую пропускную способность (7–8 транзакций в секунду в сети Bitcoin) [1].

Современные исследования сосредоточены на смягчении экологического воздействия. Например, стратегия двухэтапного майнинга [17] разделяет процесс на предварительный отбор узлов и финальное хеширование, сокращая энергозатраты на 50%. Другой подход — интеграция «полезных вычислений»: алгоритм [18] использует мощности майнинга для обучения нейросетей, превращая бессмысленные вычисления в ресурс для искусственного интеллекта.

4.2 Proof of Stake (PoS)

Алгоритм PoS, впервые примененный в Nxt (2013), заменяет энергоемкий майнинг на систему, где вероятность создания блока зависит от доли токенов, которыми владеет узел [19]. Это снижает энергопотребление на порядки, но создает риск централизации: крупные держатели получают непропорциональное влияние. Для борьбы с этим вводятся механизмы «охлаждения стейка» — временной блокировки токенов после создания блока, а также динамическая корректировка сложности, учитывающая не только размер доли, но и длительность владения активами.

Инновации 2020-х включают аппаратную защиту через доверенные среды исполнения (TEE), предотвращающие атаки типа «Nothing-at-Stake», и гибридные модели, где часть вознаграждения распределяется между малыми узлами для стимулирования децентрализации. Например, алгоритм [20] ограничивает долю одного узла в создании блоков, предотвращая монополизацию сети.

4.3 Bitcoin-NG

Протокол Bitcoin-NG [21] разделяет блоки на ключевые (выбор лидера) и микроблоки (пакеты транзакций), позволяя лидеру обрабатывать транзакции непрерывно до смены валидатора. Это повышает пропускную способность до 60 раз по сравнению с классическим PoW, но создает риск временной централизации: пока действует полномочие лидера, он может цензурировать транзакции. Для минимизации рисков вводятся рандомизированные схемы выбора следующего лидера [22] и графовые структуры данных [23], обеспечивающие параллельную обработку цепочек микроблоков.

4.4 Delegated Proof of Stake (DPoS)

В DPoS [24] сообщество голосует за ограниченный набор «суперузлов», ответственных за создание блоков. Например, в EOS 21 суперузел генерирует блоки последовательно, достигая тысяч транзакций в секунду. Однако система критикуется за формирование олигополии: крупные игроки договариваются о распределении вознаграждений. Модернизации включают квадратичное голосование [25], где стоимость каждого дополнительного голоса растет экспоненциально, и модели на основе нечеткой логики [26], учитывающие неопределенность в выборе делегатов.

4.5 Raft

Алгоритм Raft, представленный в 2014 г. как упрощенная альтернатива Paxos, использует архитектуру «лидер-последователь» для координации данных через регулярные сигналы

активности [27]. Несмотря на сильную согласованность данных, зависимость от единого лидера ограничивает децентрализацию и масштабируемость, оставляя уязвимость к атакам и сложности параллельной обработки.

С 2022 г. внедряются модификации для оптимизации: кластеризация узлов на приоритетные группы [28] ускоряет обработку подзадач, а батчинг логов [29] снижает коммуникационные издержки. Оптимизация хранения через хеш-значения [30] экономит ресурсы, а автоматизация выбора лидера с генетическими алгоритмами [31] повышает эффективность. Эти улучшения адаптируют Raft для высоконагруженных систем, но не устраняют фундаментальную проблему централизованной архитектуры, ограничивающую применение в полностью децентрализованных средах.

4.6 PBFT и его производные

Алгоритм PBFT, предложенный Кастро и др. в 1999 г. [32], обеспечивает консенсус в системах с компрометированными до 1/3 византийских узлов через ротацию главного узла на основе модульного вычисления. Несмотря на высокую безопасность и децентрализацию, алгоритм страдает от низкой эффективности из-за многораундовой коммуникации, а также ограниченной масштабируемости из-за зависимости от группового взаимодействия узлов.

Современные модификации сосредоточены на оптимизации производительности и снижении нагрузки. Например, в [33] ввели систему двойных главных узлов для уменьшения централизации, а в [34] комбинировали пороговые и кольцевые подписи, сократив коммуникационные затраты на 30%. Другие подходы включают древовидную топологию [35] для разделения консенсуса на локальные уровни и двухэтапный процесс [36], снижающий сетевую нагрузку. Эти улучшения сохраняют баланс между безопасностью и эффективностью, но не решают фундаментальную проблему масштабируемости в крупных сетях.

4.7 HotStuff

Алгоритм HotStuff, предложенный в [37] в 2019 г., реализует консенсус через пороговые подписи и конвейерную обработку, снижая коммуникационные затраты до линейного уровня. Его ключевая инновация — разделение безопасности (математически гарантированной) и активности (гибко настраиваемой через модуль pacemaker), что использовано в LibraBFT для Facebook. Несмотря на высокую эффективность и масштабируемость, алгоритм сохраняет среднее энергопотребление из-за частого обмена сообщениями.

Современные модификации HotStuff (2020–2024) сосредоточены на оптимизации производительности при сохранении линейной коммуникационной сложности. В 2020 г. Фуладгар снизил задержки за счет переноса синхронных ожиданий за пределы критического пути. Дальнейшие улучшения включают внедрение виртуальных блоков [38] для предотвращения «зависаний» при смене лидера и многоконвейерной обработки с прогнозированием блоков [39], что повысило пропускную способность системы. Для устранения единой точки отказа в [40] предложили случайный выбор лидера.

4.8 Algorand

Алгоритм Algorand, предложенный в 2017 г. [41], использует верифицируемую случайную функцию (VRF) для распределения ролей между узлами: создание блоков, верификация или пассивное участие. Узлы, выбранные для формирования блоков, предоставляют криптографическое доказательство от VRF, обеспечивая прозрачность процесса. Алгоритм достигает низкой задержки и высокой пропускной способности благодаря случайному выбору комитета и упрощенному консенсусу, сохраняя высокую безопасность даже при 1/3 злоумышленных узлов, с полной децентрализацией и минимальным энергопотреблением.

Последующие модификации усилили алгоритм: в 2020 г. [42] внедрили ролевую систему вознаграждений для стимулирования кооперативного поведения узлов, а в 2022 г. [43] оптимизировали выбор транзакций через анализ комиссий, снизив частоту пустых блоков. В 2023 г. [44] ввели «узлы-детекторы» для идентификации некорректно ведущих себя участников с последующими санкциями, повысив общую безопасность. Ключевым улучшением 2024 г. [45] стала технология обфускации VRF, защищающая приватные ключи даже при компрометации хоста, что математически гарантирует устойчивость к обратному инжинирингу. Эти модификации

сохранили базовые преимущества Algorand, усилив его безопасность и эффективность в динамичных сетевых условиях.

4.9 PoET

Алгоритм PoET был предложен Боуманом и др. [46] в 2016 г. для снижения энергозатрат блокчейн-систем. Его ключевая идея — использование случайного временного ожидания (на основе вероятностного распределения) для выбора узла, формирующего блок, что устранило высокие вычислительные затраты PoW. Несмотря на повышение энергоэффективности и пропускной способности, алгоритм сохранил уязвимость: зависимость от доверенной среды исполнения (TEE) ограничила децентрализацию из-за требований к специализированному оборудованию. В 2021 г. [47] модифицировали алгоритм, добавив распределенную координацию узлов для снижения конфликтов при параллельном создании блоков. Однако их схема, требующая низких сетевых задержек, продемонстрировала ограниченную эффективность в гетерогенных сетях. Эти изменения сохранили базовые преимущества PoET — умеренное энергопотребление и высокую скорость обработки, но не решили проблему централизации.

4.10 PoA

Алгоритм PoA [48] объединяет принципы PoW и PoS: майнеры вычисляют хеш заголовка блока (без транзакций), после чего система случайным образом назначает N верификаторов на основе их доли владения токенами. Безопасность обеспечивается необходимостью одновременного контроля >50% вычислительной мощности сети и доли токенов в стейкинге. Для разрешения форков алгоритм использует модифицированный принцип самой длинной цепи: при возникновении конкурирующих ветвей валидность блоков дополнительно проверяется кворумом верификаторов, что минимизирует риск реорганизаций.

Алгоритм демонстрирует средние показатели: энергопотребление умеренное (снижено за счет гибридного подхода), безопасность средняя (риск сиблинг-атак), децентрализация ограничена зависимостью от узлов с высоким стейкингом. Низкая масштабируемость обусловлена комбинацией PoW/PoS и ресурсозатратностью.

Система последовательно модернизировалась: с 2019 г. PBFT-комитет на базе PoA [49] обеспечил финализацию блоков, затем механизм репутации [50] с батчинг-структурой оптимизировал валидацию. В 2021 г. динамическая ротация валидаторов через K-medoids и follow-the-satoshi [51] дополнилась в 2022 г. теоретико-игровой моделью [52] для противодействия централизации майнинг-пулов. Этот эволюционный путь сохранил гибридную архитектуру при значительном росте пропускной способности и устойчивости к атакам.

4.11 dBFT

В 2016 г. [53] предложили dBFT. Он основан на PBFT и использует идеи PoS. Узлы выбирают «участника–счётчика», а между ними достигается консенсус по PBFT.

dBFT с меньшим участием узлов в консенсусе снижает коммуникационные расходы, имеет высокую эффективность и низкое энергопотребление. Он поддерживает безопасность при менее трети узлов – злоумышленников, но его безопасность зависит от качества узлов, уровень – средний. Степень децентрализации – средняя, хотя выбор представителей происходит через голосование.

В 2020 г. [54] ввели механизм нескольких главных узлов, уменьшив зависимость от одного. Также добавили передачу избыточных сообщений, что усилило надежность, но увеличило коммуникационные расходы.

4.12 FBFT

F-BFT (Federated Byzantine Fault Tolerance) — это механизм консенсуса, используемый для решения проблемы согласованности узлов в распределенных системах. Он основан на классической теории отказоустойчивости на основе задачи о византийских генералов (BFT) и использовании концепции федерализации, предназначен для обеспечения надежности и согласованности данных всей системы в случае наличия злоумышленных узлов. F-BFT в основном применяется в сценариях эффективной и безопасной верификации транзакций, особенно подходит для финтеха и интернета вещей, и начал применяться на реальных блокчейн-платформах в 2019 г., с целью заменить традиционный BFT-механизм и повысить производительность и безопасность блокчейн–приложений [55].

F-BFT значительно сокращает время подтверждения транзакций, и его высокая эффективность подходит для тех приложений финтеха, которые требуют быстрого отклика. Используя характеристики отказоустойчивости на основе задачи о византийских генералов, он может эффективно противостоять атакам злоумышленных узлов, поддерживать согласованность и надежность системных данных, имеет высокую безопасность. F-BFT может динамически регулировать количество узлов, участвующих в консенсусе в зависимости отбизнес потребностей, что усиливает адаптивность и масштабируемость системы. По сравнению с PoW, F-BFT оптимизирует энергопотребление и подходит для реализации более устойчивого режима работы.

4.13 Сравнение различных алгоритмов консенсуса

Таблица 2. Сравнение различных алгоритмов консенсуса

Алгоритмы консенсуса	Эффек-тивность	Энерго-потреб-ление	Безопас-ность	Степень децен-трализа-ции	Масшта-бируе-мость	Сценарии применения	Платформа
PoW	низкая	высокое	высокая	средняя	низкая	публичные цепочки	Bitcoin
PoS	высокая	низкое	средняя	средняя	средняя	публичные цепочки	Ethereum
Bitcoin-NG	высокая	среднее	высокая	низкая	высокая	публичные цепочки	Waves
DPoS	высокая	низкое	средняя	низкая	высокая	публичные цепочки	EOS v1.0
Raft	средняя	среднее	средняя	низкая	низкая	гибридные цепочки	Fabric v1.4.4
PBFT	низкая	среднее	высокая	высокая	низкая	гибридные цепочки	Fabric v0.6.0
HotStuff	высокая	среднее	высокая	средняя	высокая	публичные цепочки	-
Algorand	высокая	низкое	высокая	высокая	высокая	гибридные цепочки	-
PoET	высокая	низкое	средняя	низкая	низкая	гибридные цепочки, приватные цепочки	Hyperledger Sawtooth
PoA	низкая	среднее	средняя	средняя	низкая	публичные цепочки	Decred
dBFT	высокая	низкое	средняя	средняя	высокая	гибридные цепочки	EOS v2.0, NEO
F-BFT	высокая	среднее	высокая	средняя	высокая	публичные, приватные, гибридные цепочки	DGT

4.14 Анализ преимуществ и недостатков различных алгоритмов консенсуса

Алгоритмы консенсуса (PoW, PoS, Bitcoin-NG и т. д.) нуждаются в безопасности и децентрализации, жертвуя эффективностью. Выбор узлов-счётчиков требует ресурсов.

Алгоритмы на основе (Dpos, Raft и т. д.) зависят от голосования, имеют меньшую децентрализацию, но высокую эффективность.

Алгоритмы (PBFT, Hotstuff и т. д.) зависят от выбора главных узлов, достигают высокой децентрализации, но упрощенный процесс выбора увеличивает вероятность выбора злоумышленного узла.

Механизмы (Algorand, PoET и т. д.) используют случайные характеристики, что повышает безопасность, масштабируемость и производительность, но проблема генерации случайных чисел может быть узким местом.

Гибридные алгоритмы (PoA, dBFT, F-BFT и т. д.) объединяют характеристики, что позволяет преодолеть ограничения, но могут ввести к новым рискам при обеспечении безопасности.

5. Цифровая валюта

Основные инвестиционные институты не признают криптовалюты и не считают Bitcoin активом (от англ. asset — финансовый инструмент с материальной стоимостью). Уоррен Баффетт, один из самых влиятельных инвесторов, назвал Bitcoin «крысиным ядом» (англ. rat poison), отражая свою позицию: он считает криптовалюты спекулятивным инструментом без внутренней ценности, сравнивая их с финансовой пирамидой.

Но некоторые институциональные инвесторы все больше признают Bitcoin как инвестиционный продукт, рассматривают инвестиции в Bitcoin – фьючерсы, фонды и банковские каналы для торговли.

Цена криптовалют зависит от двух групп факторов: особенности проектов (компетентность команды, активность сообществ, взаимодействие) и рыночные условия (макроэкономика, торговая активность, инсайдерство), определяющих волатильность и стоимость цифровых активов.

Частно-выпускаемые цифровые валюты: на основе публичной или гибридной цепочки.

Суверенные цифровые валюты – централизованные, используют блокчейн. Цифровая валюта центральных банков (Central Bank Digital Currency, CBDC) является цифровым аналогом национальной фиатной валюты разных стран, которую выпускает, регулирует и гарантирует центральный банк страны. В отличие от CBDC биткойн (или любая другая криптовалюта) является децентрализованной и не имеют регулирующего органа. При этом стоимость биткойна определяется разными факторами, например соотношением спроса и предложения, в отличие от CBDC, стоимость которой устанавливается центральным банком в фиатной валюте страны.

В качестве примера рассмотрим Китай. В Китае исследуется и продвигается цифровой юань (Digital Currency Electronic Payment, DCEP) [56]. Она проходит пилотный запуск, заменяет наличные юани. DCEP выпускается как в цифровом, так и в монетарном виде, а их учетом занимается Народный банк Китая (центральный банк). Пример взаимодействия между центральным банком и коммерческими банками/другими финансовыми учреждениями показан на рис. 6.

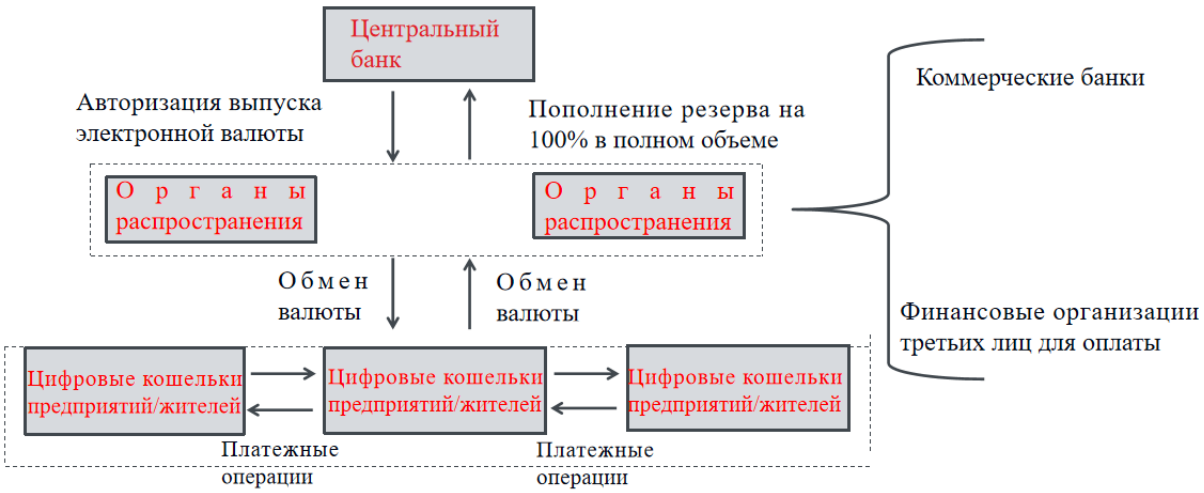

Рис. 6. Двухуровневая система операций между центральным банком и коммерческими банками/другими финансовыми учреждениями

Цифровой юань – это блокчейн-форма юаня, равнозначная юаню, законная валюта, относится к M0 и может быть отслеживаема. M0 – наличные в обращении (сумма денежных запасов организаций вне банковской системы и наличных у жителей). DCEP – фиатная валюта, Народный банк Китая гарантирует ее кредитоспособность (в отличие от Bitcoin и Libra).

Технологический процесс DCEP (рис. 7): Народный банк Китая генерирует цифровую валюту (создает фонд), хранит в своем репозитории [57]. По заявкам коммерческих банков ЦБ корректирует записи в их репозиториях. При заявке пользователя на вывод валюта из банковского репозитория идет в оборот и в цифровой кошелек пользователя. В обращении валюта перемещается между кошельками для платежей (онлайн- и офлайн-транзакции).

Алгоритмы шифрования (Hash, Fitzer и др.) обеспечивают безопасность DCEP. DCEP имеет исполняемые скрипты для будущей интеллектуализации.

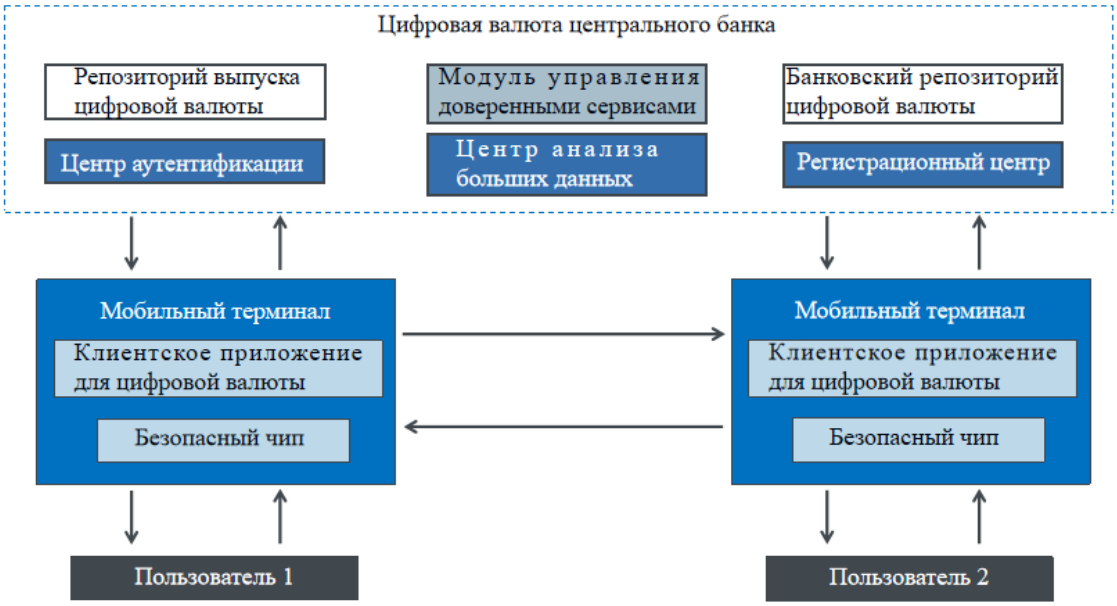

Рис. 7. Архитектура DCEP

Ключевые инновационные особенности DCEP включают «двойной офлайн» – оплату без сети, используя мобильные телефоны. DCEP имеет слабую связь с аккаунтом, можно передавать стоимость без банковского аккаунта с контролируемой анонимностью. DCEP обладает программируемостью, пользователи могут настроить скрипты для повышения эффективности оплаты.

Для оплаты пользователям нужен DCEP–кошелек с парами ключей. Открытый ключ для сертификатов, закрытый – для инициирования транзакций, которые записываются в центральном репозитории.

Заключение

Блокчейн-технология, воплощенная в Bitcoin как пионере децентрализованных финансов, и расширенная возможностями Ethereum для создания смарт-контрактов, заложила основу новой цифровой эпохи. Цифровые валюты, объединяющие передовые криптографические методы, экономики и программирования, трансформируют представление о деньгах, доверии и управлении активами. Несмотря на волатильность и регуляторные вызовы, их роль в глобальной финансовой системе продолжает расти, открывая перспективы для прозрачности, безопасности и инклюзивности. Будущее этой сферы зависит как от технологического прогресса, так и от гармонизации интересов пользователей, разработчиков и государств.

Литература

1. Накамото С. Bitcoin: A Peer-to-Peer Electronic Cash System / пер. с англ. А. Петрова. 2008. 9 с.
2. Бутерин В. Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform / пер. с англ. И. Смирнова. 2014. 36 с.
3. Национальный институт стандартов и технологий США (NIST). FIPS PUB 180-4: Secure Hash Standard (SHS). 2015. 33 с.

4. Антонопулос А. М. Mastering Bitcoin: Unlocking Digital Cryptocurrencies / пер. с англ. Д. Иванова. М.: O'Reilly Media, 2014. 298 с.
5. Narayanan A., Bonneau J., Felten E. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction // Princeton University Press. 2016. URL: https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies (дата обращения: 24.06.2025).
6. Decker C., Wattenhofer R. Information propagation in the Bitcoin network // IEEE P2P 2013. URL: https://doi.org/10.1109/P2P.2013.6688704.
7. Bitcoin Block Explorer (Difficulty Data). 2024. URL: https://blockchain.info/charts/difficulty (дата обращения: 24.06.2025).
8. Eswar Prasad. The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance. Cambridge: The Belknap Press, 2021. 342 с.
9. Бутерин В. Ethereum: Белая книга. Следующее поколение смарт-контрактов и децентрализованных приложений // Ethereum Foundation. 2014. URL: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Russian_Translation.pdf (дата обращения: 20.03.2025).
10. Ethereum Documentation: Smart Contracts. 2024. URL: https://ethereum.org/en/developers/docs/smart-contracts/ (дата обращения: 24.06.2025).
11. World Economic Forum. DeFi Beyond the Hype: The Emerging World of Decentralized Finance. 2022. URL: https://www.weforum.org/reports/defi-beyond-the-hype
12. Tether Whitepaper. Tether Limited. 2024. URL: https://tether.to/en/transparency#reports.
13. ERC-20 Token Standard. Ethereum Improvement Proposals. 2015. URL: https://eips.ethereum.org/EIPS/eip-20 (дата обращения: 14.03.2025).
14. ERC-721 Non-Fungible Token Standard. Ethereum Improvement Proposals. 2018. URL: https://eips.ethereum.org/EIPS/eip-721 (дата обращения: 24.06.2025).
15. SEC Report on Initial Coin Offerings (ICOs). U.S. Securities and Exchange Commission. 2019. URL: https://www.sec.gov/ICO (дата обращения: 24.06.2025).
16. SEC vs. Telegram Group Inc. Судебное дело № 1:19-cv-09439-PKC // Окружной суд Южного округа Нью-Йорка. 2020. URL: https://www.sec.gov/litigation/complaints/2020/comp-pr2020-48.pdf (дата обращения: 24.06.2025).
17. Lasla N., Al-Sahan L., Abdallah M., et al. Green-PoW: an energy-efficient blockchain proof-of-work consensus algorithm. Computer Networks, 2022, Volume 214, Issue C. https://doi.org/10.1016/j.comnet.2022.109118
18. Wei Y. K., An Z. X., Leng S. P., et al. Evolved PoW: integrating the matrix computation in machine learning into blockchain mining. IEEE Internet of Things Journal, 2023, 10(8):6689-6702. https://doi.org/10.1109/jiot.2022.3165973
19. nxt.org. (n.d.). Nxt Whitepaper. URL: https://nxt.org/nxt-whitepaper/ (дата обращения: 14.03.2025).
20. Zhao W. B. On NXT proof of stake algorithm: a simulation study. IEEE Transactions on Dependable and Secure Computing, 2023, 20(4):3546-3557.
21. Eyal I., Gencer A. E., Sirer E. G., et al. Bitcoin-NG: a scalable blockchain protocol // Proceedings of the 2016 USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2016:45-59.
22. Das D. Toward next generation of blockchain using improvized Bitcoin-NG. IEEE Transactions on Computational Social Systems, 2021, 8(2):512-521.
23. Kan J., Chen S. Z., Huang X. Improve blockchain performance using graph data structure and parallel mining // Proceedings of the 2018 IEEE International Conference on Hot Information-Centric Networking. Piscataway: IEEE, 2018:173- 178.
24. Yang F., Zhou W., Wu Q. Q., et al. Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE Access, 2019, 7:118541-118555.
25. Kim J., Oh S., Kim Y., et al. Improving voting of block producers for delegated proof-of-stake with quadratic delegate // Proceedings of the 2023 International Conference on Platform Technology and Service. Piscataway: IEEE, 2023: 13-17.
26. You L., Wang Z. B., Hu G. R., et al. An improved model on the Vague Sets-based DPoS's voting phase in blockchain. IEEE Transactions on Network Science and Engineering, 2023, 10(6):4010-4019.

27. Ongaro D., Ousterhout J. In search of an understandable consensus algorithm // Proceedings of the 2014 USENIX annual technical conference. Berkeley: USENIX Association, 2014: 305-319.
28. Tang H., Yi W. L., Zhao Y. D., et al. Improved raft algorithm for optimizing authorized nodes based on random forest // Proceedings of the 2022 XXV International Conference on Soft Computing and Measurements. Piscataway: IEEE, 2022:279- 282.
29. Yamashita A., Tanaka M., Bessho Y., et al. Improving raft performance with bulk transfers // Proceedings of the 2023 Eleventh International Symposium on Computing and Networking Workshops. Piscataway: IEEE, 2023: 38-44.
30. Liu Y. R., Shi T. J. Improved A-RAFT consensus algorithm based on sha256 encryption algorithm // Proceedings of the 2023 International Conference on the Cognitive Computing and Complex Data. Piscataway: IEEE, 2023:317-322.
31. Yang S. J., Tan P. L., Fu H. W. Improved raft consensus algorithm based on NSGA-II and K-Means++ // Proceedings of the 2024 International Symposium on System Security, Safety, and Reliability. Piscataway: IEEE, 2024: 383-390.
32. Castro M., Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.
33. Na Y. H., Wen Z., Fang J., et al. A derivative PBFT blockchain consensus algorithm with dual primary nodes based on separation of Powers-DPNPBFT. IEEE Access, 2022, 10: 76114-76124.
34. Sun H. F., Zhang W. F., Wang X. M., et al. A robust byzantine fault-tolerant consensus algorithm against adaptive attack based on ring signature and threshold signature. Acta Automatica Sinica, 2023, 49(7):1471-1482.
35. Jiang W. X., Wu X. X., Song M. Y., et al. A scalable byzantine fault tolerance algorithm based on a tree topology network. IEEE Access, 2023, 11:33509-33519.
36. Zhang M., Li S. W., Wu Y. T., et al. Research on Optimization of Reward and Punishment Mechanism of PBFT. Computer Engineering and Applications, 2024, 60(07):266-273.
37. Yin M. F., Malkhi D., Reiter M. K., et al. Hotstuff: BFT consensus with linearity and responsiveness //Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. New York: ACM, 2019:347-356.
38. Sui X., Duan S. S., Zhang H. B. Marlin: two-phase BFT with linearity // Proceedings of the 2022 Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE, 2022: 54-66.
39. Cheng T. N., Zhou W., Yao S. W., et al. Multi-pipeline hotstuff: a high performance consensus for permissioned blockchain // Proceedings of the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Piscataway: IEEE, 2022:1008-1019.
40. Gao M. G., Lu G. H., Wang Z. Y., et al. WPBFT: an improved consensus algorithm based on the hotstuff algorithm // Proceedings of the 2023 International Conference on Artificial Intelligence and Blockchain Technology. Piscataway: IEEE, 2023:56-59.
41. Gilad Y., Hemo R., Micali S., et al. Algorand: scaling byzantine agreements for cryptocurrencies //Proceedings of the 2017 Symposium on Operating Systems Principles. New York: ACM,2017: 51-68
42. Fooladgar M., Manshaei M. H., Jadliwala M., et al. On incentive compatible role-based reward distribution in Algorand // Proceedings of the 2020 Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE, 2020: 452-463.
43. Abbasi M., Manshaei M. H., Rahman M. A., et al. On Algorand transaction fees: challenges and mechanism design // Proceedings of the 2022 IEEE International Conference on Communications. Piscataway: IEEE, 2022: 5403-5408.
44. Abbasihafshejani M., Manshaei M. H., Jadliwala M. Detecting and punishing selfish behavior during gossiping in Algorand blockchain //Proceedings of the 2023 IEEE Virtual Conference on Communications. Piscataway: IEEE, 2023:49-55.
45. Shi Y., Luo T. Y., Liang J. W., et al. Obfuscating verifiable random functions for proof-of-stake blockchains. IEEE Transactions on Dependable and Secure Computing, 2024,21(4):2982-2996.
46. Chen L., Xu L., Shah N., et al. On security analysis of proof-of-elapsed-time(poet) //Proceedings of the 2017 Stabilization, Safety, and Security of Distributed Systems. Cham: Springer, 2017: 282-297.
47. Pal A., Kant K. DC-PoET: proof-of-elapsed-time consensus with distributed coordination for blockchain networks //Proceedings of the 2021 IFIP Networking Conference. Piscataway: IEEE, 2021: 1-9.

48. Bentov I., Lee C., Mizrahi A., et al. Proof of activity: extending bitcoin's proof of work via proof of stake. ACM SIGMETRICS Performance Evaluation Review 2014, 42(3):34-37.
49. Liu Z. Q., Tang S. Y., Chow S. S. M,et al. Fork-free hybrid consensus with flexible proof-of-activity. Future Generation Computer Systems, 2019, 96: 515-524.
50. Wang D., Jin C. G., Li H., et al. Proof of activity consensus algorithm based on credit reward mechanism //Proceedings of the 2020 Web Information Systems and Applications. Cham: Springer, 2020:618-628.
51. Wang D., Jin C. G., Xiao B. B., et al. Proof-of-activity consensus algorithm based on k-medoids clustering. Big Data Research, 2021, 26:100266.
52. Boreiri Z., Azad A. N. A novel consensus protocol in blockchain network based on proof of activity protocol and game theory // Proceedings of the 2022 International Conference on Web Research. Piscataway: IEEE, 2022: 82-87.
53. Wang Q., Yu J. S., Peng Z. N., et al. Security analysis on dBFT protocol of NEO //Proceedings of the 2020 Financial Cryptography and Data Security. Cham: Springer, 2020:20-31.
54. Coelho I. M., Coelho V. N., Araujo R. P., et al. Challenges of PBFT-inspired consensus for blockchain and enhancements over NEO dBFT. Future Internet, 2020, 12(8):1- 20.
55. Bogdanov, A., Degtyarev, A., Uteshev, A., Shchegoleva, N., Khvatov, V., Zvyagintsev, M.: A DLT based innovative investment platform. In: Gervasi, O., et al. (eds.) ICCSA 2020. LNCS, vol. 12251, pp. 72–86. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58808-3_7
56. People's Bank of China. (2021). White Paper on R&D Progress of China's Digital RMB. URL: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4293592/index.html
57. Bank for International Settlements. (2020). Central bank digital currencies: foundational principles and core features. URL: https://www.bis.org/publ/othp33.htm (дата обращения: 24.06.2025).

DIGITAL AND CRYPTOCURRENCIES IN THE FUTURE ECONOMY

Hu, Bitai

Saint Petersburg State University, Faculty of applied mathematics and control processes, postgraduate student
Saint Petersburg, Russian Federation
bitaihu@gmail.com

Khvatov, Valery Vladimirovich

DGT Technologies AG, chief technology officer
Toronto, Canada
valery.khvatov@gmail.com

Schegoleva, Nadezhda Lvovna

Doctor of technical sciences, associate professor
Saint Petersburg State University, Faculty of applied mathematics and control processes, professor
Saint Petersburg, Russian Federation
n.shchegoleva@spbu.ru

Abstract

This study examines the evolution of blockchain technology, from Bitcoin to Ethereum, highlighting their role in shaping a decentralized economy. Blockchain, as the foundation of the "internet of value," transforms asset management through cryptographic immutability, smart contracts, and tokenization. The paper systematizes key consensus algorithms (PoW, PoS, PBFT, etc.), their advantages, limitations, and the potential of hybrid models. Special attention is given to the digital yuan (DCEP), the first CBDC combining centralized control with innovations (offline payments, programmability). Despite technological advancements, challenges persist: regulatory uncertainty, energy-intensive mining, and the conflict between decentralization and governance. The research emphasizes the need to balance innovation, security, and international regulatory harmonization for the sustainable development of the digital economy.

Keywords

blockchain; Bitcoin; Ethereum; consensus mechanism; smart contract; digital yuan; decentralization; mining; Central Bank Digital Currency; CBDC; Decentralized Finance; DeFi; Digital Currency Electronic Payment; DCEP; Non-Fungible Token; NFT

References

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / per. s angl. A. Petrova. 2008. 9 s.
2. Buterin V. Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform / per. s angl. I. Smirnova. 2014. 36 s.
3. Nacional'nyj institut standartov i tekhnologij SSHA (NIST). FIPS PUB 180-4: Secure Hash Standard (SHS). 2015. 33 s.
4. Antonopulos A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies / per. s angl. D. Ivanova. M.: O'Reilly Media, 2014. 298 s.
5. Narayanan A., Bonneau J., Felten E. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction // Princeton University Press. 2016. URL: https://press.princeton.edu/books/hardcover/9780691171692/bitcoin-and-cryptocurrency-technologies (data obrashcheniya: 24.06.2025).
6. Decker C., Wattenhofer R. Information propagation in the Bitcoin network // IEEE P2P 2013. URL: https://doi.org/10.1109/P2P.2013.6688704.
7. Bitcoin Block Explorer (Difficulty Data). 2024. URL: https://blockchain.info/charts/difficulty (data obrashcheniya: 24.06.2025).
8. Eswar Prasad. The Future of Money: How the Digital Revolution Is Transforming Currencies and Finance. Cambridge: The Belknap Press, 2021. 342 s.
9. Buterin V. Ethereum: Belaya kniga. Sleduyushchee pokolenie smart-kontraktov i decentralizovannyh prilozhenij // Ethereum Foundation. 2014. URL:

https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Russian_Translation.pdf (data obrashcheniya: 20.03.2025).
10. Ethereum Documentation: Smart Contracts. 2024. URL: https://ethereum.org/en/developers/docs/smart-contracts/ (data obrashcheniya: 24.06.2025).
11. World Economic Forum. DeFi Beyond the Hype: The Emerging World of Decentralized Finance. 2022. URL: https://www.weforum.org/reports/defi-beyond-the-hype
12. Tether Whitepaper. Tether Limited. 2024. URL: https://tether.to/en/transparency#reports
13. ERC-20 Token Standard. Ethereum Improvement Proposals. 2015. URL: https://eips.ethereum.org/EIPS/eip-20 (data obrashcheniya: 14.03.2025).
14. ERC-721 Non-Fungible Token Standard. Ethereum Improvement Proposals. 2018. URL: https://eips.ethereum.org/EIPS/eip-721 (data obrashcheniya: 24.06.2025).
15. SEC Report on Initial Coin Offerings (ICOs). U.S. Securities and Exchange Commission. 2019. URL: https://www.sec.gov/ICO (data obrashcheniya: 24.06.2025).
16. SEC vs. Telegram Group Inc. Sudebnoe delo № 1:19-cv-09439-PKC // Okruzhnoj sud YUzhnogo okruga N'yu-Jorka. 2020. URL: https://www.sec.gov/litigation/complaints/2020/comp-pr2020-48.pdf (data obrashcheniya: 24.06.2025).
17. Lasla N., Al-Sahan L., Abdallah M., et al. Green-PoW: an energy-efficient blockchain proof-of-work consensus algorithm. Computer Networks, 2022, Volume 214, Issue C. https://doi.org/10.1016/j.comnet.2022.109118
18. Wei Y. K., An Z. X., Leng S. P., et al. Evolved PoW: integrating the matrix computation in machine learning into blockchain mining. IEEE Internet of Things Journal, 2023, 10(8):6689-6702. https://doi.org/10.1109/jiot.2022.3165973
19. nxt.org. (n.d.). Nxt Whitepaper. URL: https://nxt.org/nxt-whitepaper/ (data obrashcheniya: 14.03.2025).
20. Zhao W. B. On NXT proof of stake algorithm: a simulation study. IEEE Transactions on Dependable and Secure Computing, 2023, 20(4):3546-3557.
21. Eyal I., Gencer A. E., Sirer E. G., et al. Bitcoin-NG: a scalable blockchain protocol // Proceedings of the 2016 USENIX Symposium on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2016:45-59.
22. Das D. Toward next generation of blockchain using improvized Bitcoin-NG. IEEE Transactions on Computational Social Systems, 2021, 8(2):512-521.
23. Kan J., Chen S. Z., Huang X. Improve blockchain performance using graph data structure and parallel mining // Proceedings of the 2018 IEEE International Conference on Hot Information-Centric Networking. Piscataway: IEEE, 2018:173- 178.
24. Yang F., Zhou W., Wu Q. Q., et al. Delegated proof of stake with downgrade: a secure and efficient blockchain consensus algorithm with downgrade mechanism. IEEE Access, 2019, 7:118541-118555.
25. Kim J., Oh S., Kim Y., et al. Improving voting of block producers for delegated proof-of-stake with quadratic delegate // Proceedings of the 2023 International Conference on Platform Technology and Service. Piscataway: IEEE, 2023: 13-17.
26. You L., Wang Z. B., Hu G. R., et al. An improved model on the Vague Sets-based DPoS's voting phase in blockchain. IEEE Transactions on Network Science and Engineering, 2023, 10(6):4010-4019.
27. Ongaro D., Ousterhout J. In search of an understandable consensus algorithm // Proceedings of the 2014 USENIX annual technical conference. Berkeley: USENIX Association, 2014: 305-319.
28. Tang H., Yi W. L., Zhao Y. D., et al. Improved raft algorithm for optimizing authorized nodes based on random forest // Proceedings of the 2022 XXV International Conference on Soft Computing and Measurements. Piscataway: IEEE, 2022:279- 282.
29. Yamashita A., Tanaka M., Bessho Y., et al. Improving raft performance with bulk transfers // Proceedings of the 2023 Eleventh International Symposium on Computing and Networking Workshops. Piscataway: IEEE, 2023: 38-44.
30. Liu Y. R., Shi T. J. Improved A-RAFT consensus algorithm based on sha256 encryption algorithm // Proceedings of the 2023 International Conference on the Cognitive Computing and Complex Data. Piscataway: IEEE, 2023:317-322.
31. Yang S. J., Tan P. L., Fu H. W. Improved raft consensus algorithm based on NSGA-II and K-Means++ // Proceedings of the 2024 International Symposium on System Security, Safety, and Reliability. Piscataway: IEEE, 2024: 383-390.

32. Castro M., Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.
33. Na Y. H., Wen Z., Fang J., et al. A derivative PBFT blockchain consensus algorithm with dual primary nodes based on separation of Powers-DPNPBFT. IEEE Access, 2022, 10: 76114-76124.
34. Sun H. F., Zhang W. F., Wang X. M., et al. A robust byzantine fault-tolerant consensus algorithm against adaptive attack based on ring signature and threshold signature. Acta Automatica Sinica, 2023, 49(7):1471-1482.
35. Jiang W. X., Wu X. X., Song M. Y., et al. A scalable byzantine fault tolerance algorithm based on a tree topology network. IEEE Access, 2023, 11:33509-33519.
36. Zhang M., Li S. W., Wu Y. T., et al. Research on Optimization of Reward and Punishment Mechanism of PBFT. Computer Engineering and Applications, 2024, 60(07):266-273.
37. Yin M. F., Malkhi D., Reiter M. K., et al. Hotstuff: BFT consensus with linearity and responsiveness //Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing. New York: ACM, 2019:347-356.
38. Sui X., Duan S. S., Zhang H. B. Marlin: two-phase BFT with linearity // Proceedings of the 2022 Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE, 2022: 54-66.
39. Cheng T. N., Zhou W., Yao S. W., et al. Multi-pipeline hotstuff: a high performance consensus for permissioned blockchain // Proceedings of the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Piscataway: IEEE, 2022:1008-1019.
40. Gao M. G., Lu G. H., Wang Z. Y., et al. WPBFT: an improved consensus algorithm based on the hotstuff algorithm // Proceedings of the 2023 International Conference on Artificial Intelligence and Blockchain Technology. Piscataway: IEEE, 2023:56-59.
41. Gilad Y., Hemo R., Micali S., et al. Algorand: scaling byzantine agreements for cryptocurrencies //Proceedings of the 2017 Symposium on Operating Systems Principles. New York: ACM,2017: 51-68
42. Fooladgar M., Manshaei M. H., Jadliwala M., et al. On incentive compatible role-based reward distribution in Algorand // Proceedings of the 2020 Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE, 2020: 452-463.
43. Abbasi M., Manshaei M. H., Rahman M. A., et al. On Algorand transaction fees: challenges and mechanism design // Proceedings of the 2022 IEEE International Conference on Communications. Piscataway: IEEE, 2022: 5403-5408.
44. Abbasihafshejani M., Manshaei M. H., Jadliwala M. Detecting and punishing selfish behavior during gossiping in Algorand blockchain //Proceedings of the 2023 IEEE Virtual Conference on Communications. Piscataway: IEEE, 2023:49-55.
45. Shi Y., Luo T. Y., Liang J. W., et al. Obfuscating verifiable random functions for proof-of-stake blockchains. IEEE Transactions on Dependable and Secure Computing, 2024,21(4):2982-2996.
46. Chen L., Xu L., Shah N., et al. On security analysis of proof-of-elapsed-time(poet) //Proceedings of the 2017 Stabilization, Safety, and Security of Distributed Systems. Cham: Springer, 2017: 282-297.
47. Pal A., Kant K. DC-PoET: proof-of-elapsed-time consensus with distributed coordination for blockchain networks //Proceedings of the 2021 IFIP Networking Conference. Piscataway: IEEE, 2021: 1-9.
48. Bentov I., Lee C., Mizrahi A., et al. Proof of activity: extending bitcoin's proof of work via proof of stake. ACM SIGMETRICS Performance Evaluation Review 2014, 42(3):34-37.
49. Liu Z. Q., Tang S. Y., Chow S. M. et al. Fork-free hybrid consensus with flexible proof-of-activity. Future Generation Computer Systems, 2019, 96: 515-524.
50. Wang D., Jin C. G., Li H., et al. Proof of activity consensus algorithm based on credit reward mechanism //Proceedings of the 2020 Web Information Systems and Applications. Cham: Springer, 2020:618-628.
51. Wang D., Jin C. G., Xiao B. B., et al. Proof-of-activity consensus algorithm based on k-medoids clustering. Big Data Research, 2021, 26:100266.
52. Boreiri Z., Azad A. N. A novel consensus protocol in blockchain network based on proof of activity protocol and game theory // Proceedings of the 2022 International Conference on Web Research. Piscataway: IEEE, 2022: 82-87.
53. Wang Q., Yu J. S., Peng Z. N., et al. Security analysis on dBFT protocol of NEO //Proceedings of the 2020 Financial Cryptography and Data Security. Cham: Springer, 2020:20-31.

54. Coelho I. M., Coelho V. N., Araujo R. P., et al. Challenges of PBFT-inspired consensus for blockchain and enhancements over NEO dBFT. Future Internet, 2020, 12(8):1- 20.
55. Bogdanov, A., Degtyarev, A., Uteshev, A., Shchegoleva, N., Khvatov, V., Zvyagintsev, M.: A DLT based innovative investment platform. In: Gervasi, O., et al. (eds.) ICCSA 2020. LNCS, vol. 12251, pp. 72–86. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-58808-3_7
56. People's Bank of China. (2021). White Paper on R&D Progress of China's Digital RMB. URL: http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/4293592/index.html
57. Bank for International Settlements. (2020). Central bank digital currencies: foundational principles and core features. URL: https://www.bis.org/publ/othp33.htm (data obrashcheniya: 24.06.2025).