Архитектурные модели Web3

Д.Е. Намиот, В.П. Куприяновский

***Аннотация*—В настоящей статье рассмотрены основные архитектурные компоненты (модели) Web3. С последним обозначением в литературе существует некоторая неоднозначность. Web 3.0 еще соответствует семантическому вебу (как дальнейшему развитию подхода Web 2.0 – динамический контент, создаваемый пользователями сети). В данной статье технология Web3 рассматривается именно как децентрализованный веб. Основная идея Web3 заключается в том, чтобы посредством децентрализации вернуть пользователям право владения данными. Web3 должен позволить пользователям иметь полный контроль над данными и контентом, который они создают. Именно пользователи (владельцы информации) должны решать, кто может получить доступ к этой информации. Web3 достигает этого за счет децентрализованного хранения данных на основе технологий блокчейна и суверенной идентификации на базе DAO (децентрализованных автономных организаций). Базовая идея Web3 заключается в реализации бессерверного Интернета, то есть глобальной сети, в которой пользователи генерируют контент, принадлежащий им самим.**

***Ключевые слова*—блокчейн, смарт-контракты, DAO, DApps, DeFi.**

I. Введение

Идея нумерации веб-технологий восходит, скорее всего, к Тиму О'Рейли, который предложил (и, главное, популяризовал) термин Web 2.0 [1]. Соответственно, существовавшая до этого модель всемирной паутины, автоматически, получила нумерацию 1.0. Основная идея концепции Web 2.0. заключалась в динамических веб-страницах (CGI) и контенте, который создавался пользователями (UGC – User Generated Content). Как естественное развитие этого направления возникла концепция Web 3.0 (он же – семантический веб) – как научиться автоматически (программно) понимать (разбирать) этот самый UGC [2]. Таким образом, все эти "нумерации" существуют параллельно (очевидно, что и статические страницы Web 1.0 никуда не исчезли). И тут возникла еще одна идея – Web3 [3]. Авторство термина отдают Гевину Вуду, который был одним из соучредителей блокчейна Ethereum [4]. Он описывал свое предложение как децентрализованную экосистему на основе Ethereum [5]. Интересно, что автор использовал обозначение Web 3.0, а не Web3. Таким образом, на сегодня параллельно существуют эти два обозначения Web 3.0 и Web3. Поскольку, технологии вокруг блокчейн сейчас явно на слуху, во многих работах эти термины не различают, и все, что касается децентрализованного веба, называют Web3 или Web 3.0. Трудно сказать, как это будет обозначаться в дальнейшем, но, самое главное, понимать, что есть две разных технологии – семантический веб и децентрализованный веб. Кстати, семантический контекст нужен и в децентрализованных системах. На рисунке 1 показаны все перечисленные направления. В данной работе мы будем придерживаться термина Web3, описывая архитектуры соответствующих приложений.

Статья получена 15 декабря 2023.
Д.Е. Намиот – МГУ имени М.В. Ломоносова (e-mail: dnamiot@gmail.com).
В.П. Куприяновский – РУТ (МИИТ) (email: v.kupriyanovsky@rut.digital)

Централизация, действительно, является, как отмечается в некоторых работах, темной стороной современного веба. Большие Интернет-компании (Google, Facebook и др.) полностью контролируют все данные своих пользователей. Пользователи сети, в реальности, имеют очень мало контроля над контентом, который они создают, или даже над своими персональными данными в сети.

Основная идея Web3 заключается в том, чтобы и вернуть пользователям право владения данными посредством децентрализации. Web3 должен позволить пользователям иметь полный контроль над своими данными и своим (созданным ими) контентом. Сами пользователи (владельцы информации) могут решить, кто может получить доступ к этой информации, а кто нет. Этого можно достичь за счет децентрализованного хранения данных на основе технологий блокчейна и суверенной идентификации на базе DAO (децентрализованные автономные организации). Фундаментальная идея Web3 заключается в том, что он может реализовать бессерверный Интернет, то есть Интернет, в котором пользователи генерируют контент, принадлежащий самим пользователям.

Self-Sovereign Identity (SSI) — это альтернативный подход к управлению цифровой идентификацией. В соответствии с этим подходом, каждый человек или организация контролирует все аспекты своей цифровой личности, что гарантирует конфиденциальность и безопасность [7].

Использование Self-Sovereign Identity (SSI) может помочь сохранить конфиденциальность пользователей и защитить их право контролировать свои собственные данные. Этот подход также способствует демократическим процессам внутри DAO, поскольку участники могут использовать его для принятия решений и голосования. Например, в DAO каждый

участник может использовать SSI для участия в голосовании и других процессах принятия решений. При этом участник имеет полный контроль над своими данными и может решать, какими данными и когда делиться, без злоупотреблений и нарушений конфиденциальности [8].

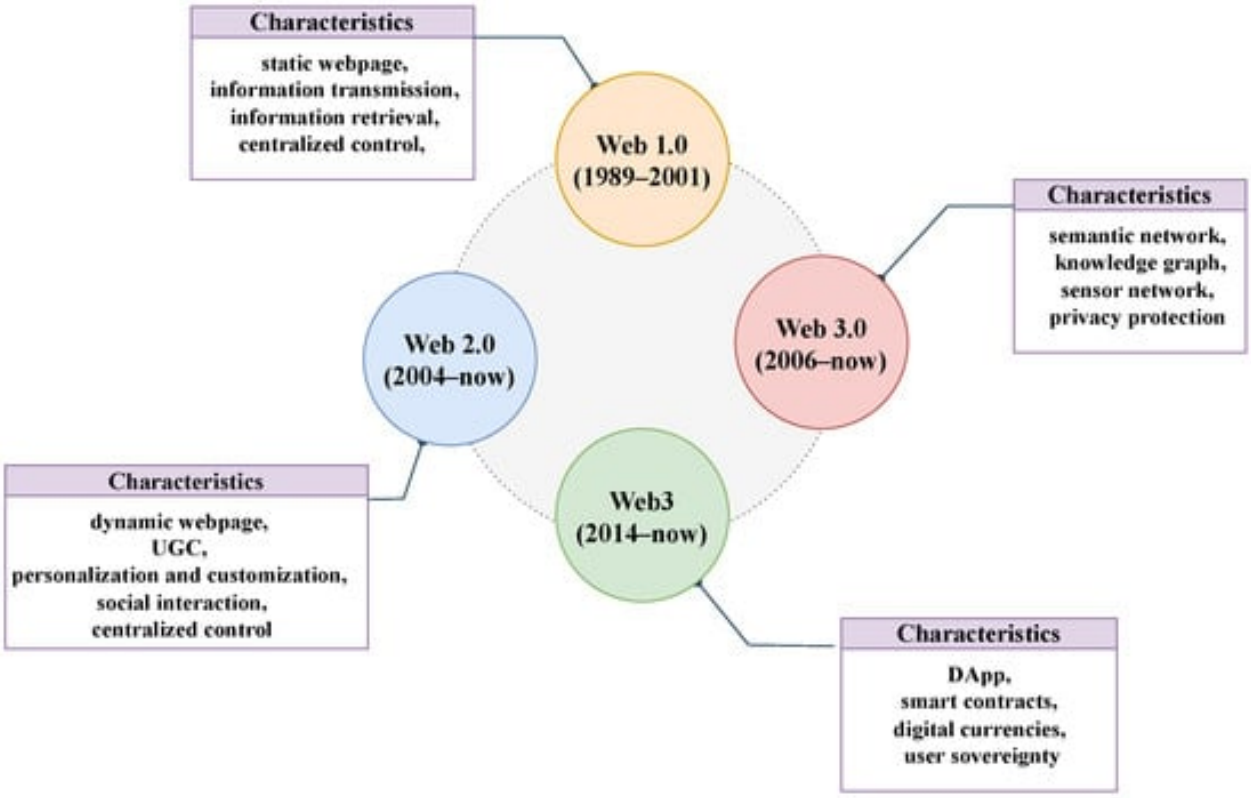

Рис.1. Эволюция веб [6].

Вообще говоря, использование блокчейн, конечно, не является обязательным условием децентрализованного веб. Например, основатель веб Тим Бернерс-Ли Бернерс-Ли, считает, что, поскольку данные блокчейна открыты и общедоступны, то всегда будут проблемы с конфиденциальностью. Соответственно, будет возможно отслеживать и анализировать данные и действия пользователей в новом веб. Заметим, что это является одной из проблем и в текущей сети. Другим возражением является дороговизна использования блокчейна. Каждая транзакция требует затрат [9]. Бернерс-Ли уже несколько лет работает над проектом Solid. Он построен с использованием стандартных веб-инструментов и открытых спецификаций [10].

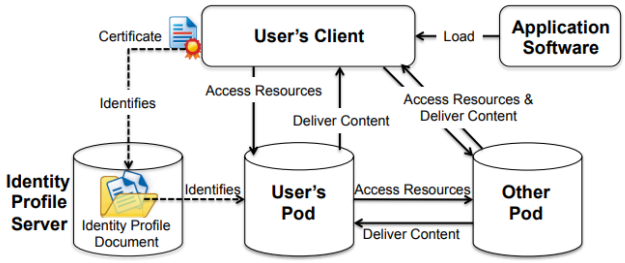

Рис.2 Архитектура Solid [10].

В этом проекте личная информация хранится в децентрализованных хранилищах данных, называемых коконами (pods). Они могут быть размещены где угодно, по желанию пользователя. Затем пользователи могут выбирать, какие приложения могут получить доступ к их данным (рис. 2). Идея этого проекта заключается в обеспечении совместимости, скорости, масштабируемости и конфиденциальности. Таким образом, здесь, как и во многих других областях Computer Science, необходимо учитывать, что помимо технических соображений есть еще и модные технологии.

Настоящая работа посвящена представлению основных архитектурных моделей Web3. Такие модели, а также связанные с ними вопросы кибербезопасности, рассматриваются в учебной программе магистратуры Кибербезопасность факультета ВМК МГУ имени М.В. Ломоносова [17]. Эта программа была создана при поддержке Департамента Кибербезопасности ПАО Сбербанк.

II Базовые положения

Согласно Гевину Вуду, «Web 3.0 — это не криптовалюта, блокчейн или токеномика. Web 3.0 – это децентрализация, открытость, и прозрачность» [11]. В 2017 году был создан консорциум Web3 Foundation [12], который, в частности, опубликовал и технологический стек (рис. 3) из 5 уровней.

Флагманский продукт находится на первом уровне (L1) – это платформа взаимодействия с нулевым уровнем доверия (сеть сетей) Polkadot. Согласно

заявленному описанию, Polkadot обеспечит полностью децентрализованную сеть, где пользователи будут контролировать ситуацию. Polkadot создан для соединения частных, публичных и закрытых децентрализованных сетей (отсюда – сеть сетей). Polkadot обеспечивает Интернет, в котором независимые блокчейны могут обмениваться информацией и транзакциями без доверия через ретрансляционную цепочку Polkadot.

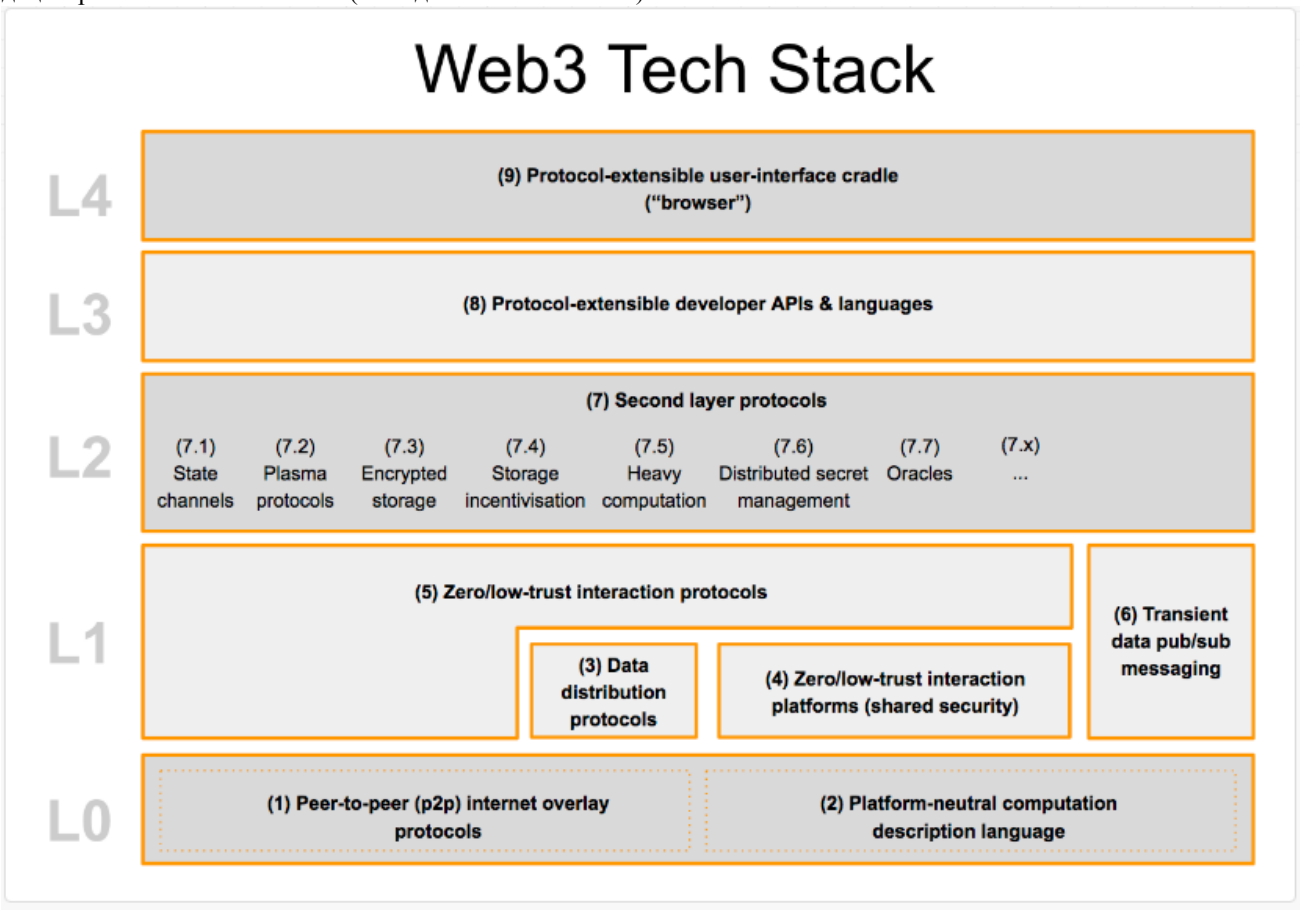

Рис.3. Web3 стек [13]

Блокчейны (блокчейны) облегчили развитие Web3, предоставив общедоступные и неизменяемые хранилища данных. Эти системы непрерывно развиваются. На рисунке 4 из работы [14] представлена архитектура блокчейн, где красными точками отмечено то, что не было частью исходного дизайна Биткойна (первого широко распространившегося блокчейна).

В целом, эти запланированные блоки и составляют основу современного развития инфраструктуры. Децентрализованная система без подобной структуры не будет функционировать должным образом, поскольку ее пользователи не смогут проверять состояние системы. В таких условиях пользователи системы, в лучшем случае, не будут уверены в том, что система эффективно выполняет запрошенные ими действия.

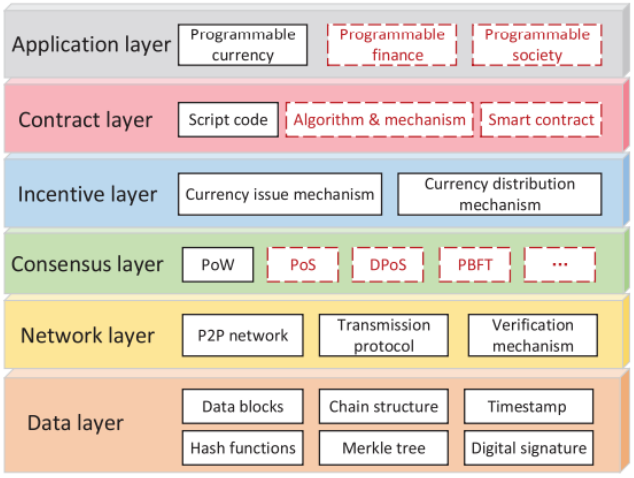

Рис. 4. Blockchain 2.0 [14]

Блокчейн — это база данных, которая используется в сети равноправных компьютеров. Он спроектирован как неизменяемая и допускающая только добавление структура. Без этого свойства прошлые транзакции (записи) могут быть стерты или подделаны, что приведет к полной неработоспособности системы. Блокчейны группируют транзакции в «блоки», где каждый новый блок соединяется с предыдущим, образуя «цепочку». Эта цепочка создается путем включения криптографического хеша предыдущего блока в данные

нового блока (рис. 5). Таким образом, если злоумышленник попытается изменить состояние блока (т. е. изменить предыдущую транзакцию), криптографический хэш блока изменится, поэтому его связь со следующим блоком будет нарушена. Таким образом, чтобы изменить предыдущий блок, злоумышленник должен обновить хэш-ссылку каждого последующего блока, чтобы создать действительную цепочку. Таким образом, безопасность блокчейна зависит от сложности создания и изменения блоков. Так, в блокчейне Биткойна используется протокол «доказательства работы», который включает в себя многократное вычисление криптографического хеша двух параметров — самого блока и сгенерированного числа — до тех пор, пока значение хеш-функции не станет меньше порогового значения. Установив достаточно низкий порог, сеть может предположить, что для нахождения этого числа был проделан значительный объем работы. Таким образом, злоумышленник должен потратить много времени на воссоздание всей цепочки после блока, который он хочет изменить. По этой причине блокчейн рассматривается как неизменяемая структура данных.

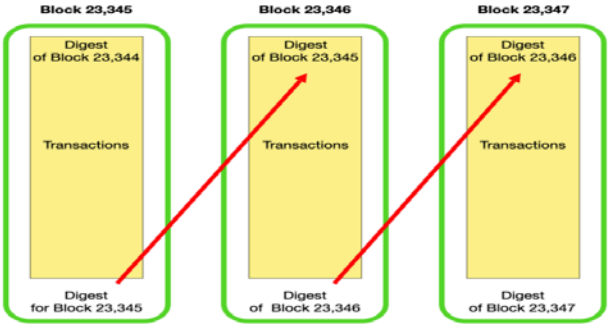

Рис. 5. Схема хранения

Блокчейн Биткойн был создан для одного применения: децентрализованной валюты. Децентрализация в этом контексте означает, что правительства не имеют контроля над предложением или состоянием валюты, и банки не нужны для завершения транзакций. Каждая транзакция Биткойн представляет собой передачу права собственности на цифровую монету от плательщика к получателю платежа. Для перевода монеты вычисляется хэш открытого ключа получателя платежа и предыдущего состояния монеты. Затем плательщик подписывает этот хэш своим закрытым ключом для подтверждения передачи права собственности [15]. Таким образом, посторонний может просмотреть предыдущее состояние монеты, чтобы убедиться, что текущее состояние было создано с использованием действительной пары открытого/закрытого ключей (рис. 6).

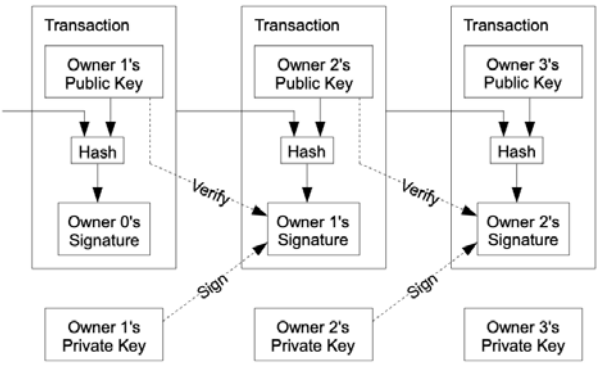

Рис.6. Транзакции в Биткойн [15]

Однако Web3 подразумевает децентрализацию всей сети, а не только небольшого подмножества ее приложений. Поэтому, вскоре после появления Биткойна, был создан еще один блокчейн, названный Ethereum [16], для обслуживания широкого спектра приложений. Блокчейн Ethereum изначально поддерживает смарт-контракты, которые позволяют пользователям писать код, который может храниться в блокчейне и выполняться при необходимости. Таким образом, пользователи могут написать любое приложение и запустить его на блокчейне Ethereum. Например, смарт-контракты могут быть написаны для создания субвалют, децентрализованных автономных организаций, систем репутации и многого другого.

Отметим, что концептуально, смарт-контракты можно рассматривать как аналоги триггеров в реляционных базах данных (автоматически исполняемый SQL-код, который хранится вместе с данными). Но есть одно важное исключение – триггеры выполняются в рамках транзакций базы данных, и все изменения могут быть отменены. Со смарт-контрактами в этом плане все хуже – поскольку блокчейн неизменяем, то все внесенные изменения – внесены. Да и сами контракты невозможно изменить после внедрения – они ведь также записаны в блокчейн. И это порождает массу проблем с аудитом (проверкой, верификацией) таких контрактов.

III Проблемы Биткойн

Основные проблемы, которые обсуждаются в связи с блокчейном Биткойн (и которые обуславливают дальнейшие разработки в этой области) следующие.

Во-первых, из-за больших накладных расходов, связанных с хранением и проверкой транзакций, Биткойн не может быстро справляться с большим количеством транзакций. Например, в [19] указывается, что Биткойн может поддерживать около 7 транзакций в секунду, тогда как платежная система Visa, например, обрабатывает около 47 000 транзакций в секунду.

Во-вторых, поскольку Биткойн использует вычислительно интенсивный и простой протокол доказательства работы, мощность майнинга будет определяться доступностью дешевой электроэнергии. В итоге, майнинг может сосредоточиться в определенных

местах, где такое доступно.

Разработка альтернативных блокчейн решений продолжается. Во-первых, можно упомянуть различные механизмы консенсуса: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Authority (DPoS), Practical Byzantine Fault Tolerance (PBFT) [18], которые имеют свои сильные и слабые стороны. Их применение варьируется в зависимости от целей, требований к производительности, соображений безопасности и желаемого уровня децентрализации в сети. Существуют и используются другие (помимо Биткойн) протоколы блокчейн. Например, Ethereum, Hyperledger, Multichain, Quorum, Corda [20]. Последний, например, аккредитован банковским консорциумом R3 (консорциум из 70+ крупных финансовых компаний в сфере разработки применения технологии блокчейн в финансовой системе) [21], что делает Corda синонимом для блокчейн-решений в области банковского дела.

Решения для масштабируемости предлагаются также на уровне L2 стека протоколов Web3 (см. рис.3) [22].

Важно также отметить, что Биткойн не предоставляет полностью анонимных транзакций. То есть, поскольку транзакции должны публично транслироваться, можно отследить транзакции Биткойн до их владельцев. Отслеживание транзакций, в частности, может привести к тому, что не все монеты будут взаимозаменяемы (например, если история некоторых из них приводит к пользователям с плохой репутацией и т.п.). Есть решения типа Zerocoin [23], которые решают проблему анонимности на основе концепции доказательств с нулевым разглашением [14].

IV Децентрализованные хранилища

Децентрализованное хранилище можно представить как сеть одноранговых серверов, которые хранят данные в глобальной сети узлов хранения. Таким образом, в действительно децентрализованной системе хранения децентрализованы и место хранения и управление хранилищем.

Общая модель хранения в Web3: метаданные – в блокчейн, сами данные – в децентрализованном хранилище.

Примером децентрализованного хранилища является IPFS (InterPlanetary File System — межпланетная файловая система) [24]. Это одноранговая распределенная файловая система, которая сочетает в себе важные свойства P2P, такие как распределенные хэш-таблицы (DHT), систему обмена файлами (BitTorrent), систему контроля версий (Git) и самосертифицированные файловые системы (SFS). IPFS обеспечивает контентно-адресуемую модель блочного хранилища с контентно-адресуемыми гиперссылками. Центральный принцип IPFS заключается в моделировании всех данных как части одних и тех же ориентированных ациклических графов Меркла - каждый узел графа имеет идентификатор, и это результат хеширования содержимого узла с использованием криптографической хеш-функции, такой как SHA256.

Самосертифицирующаяся файловая система (SFS) решает проблему управления ключами в криптографических файловых системах и отделяет управление ключами от безопасности файловой системы:

- Серверы имеют открытый ключ, и клиенты используют открытый ключ сервера для аутентификации сервера и установления безопасного канала связи.
- Чтобы позволить клиентам аутентифицировать серверы на месте, даже не зная о них раньше, SFS вводит концепцию «самосертифицирующегося пути» - он содержит хэш открытого ключа сервера, т.е. клиент может убедиться, что он действительно “общается” с законным сервером (рис. 7).

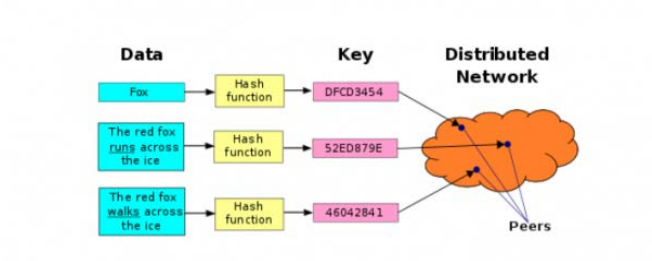

Рис. 7. Данные в IPFS

Было предложено расширение IPFS на основе блокчейна, называемое acl-IPFS [25], которое может обеспечить контроль доступа за счет использования смарт-контрактов Ethereum для обработки списка контроля доступа (пользователи могут регистрировать файлы, а также предоставлять или отзывать доступ к ним). Модель использования IPFS представлена на рисунке 8.

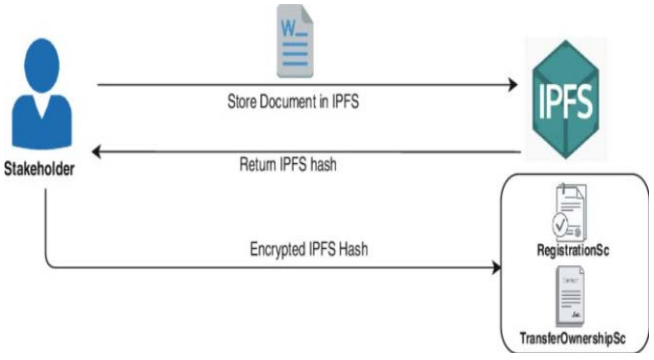

Рис. 8. Модель использования IPFS

Процесс децентрализованного хранения на основе блокчейна (выгрузка и загрузка файлов) в общем виде представлен на рисунке 9. Во время загрузки файлов система выполняет две основные задачи. Во-первых, загруженные пользователем данные подвергаются фрагментации, шифрованию и избыточной обработке по заданному алгоритму. Полученные избыточные срезы данных хранятся на нескольких независимых узлах сети,

в то время как метаданные файла одновременно записываются в блокчейн. Во-вторых, пользователи платят комиссию блокчейну, который вознаграждает их виртуальной валютой. В процессе выгрузки файла пользователи инициируют запросы к блокчейну, используя хеш-значение файла. Блокчейн в ответ на запрос предоставляет информацию о метаданных, позволяя пользователям извлекать файловые данные с узлов хранения в одноранговой сети. Эти процессы подчеркивают несколько ключевых характеристик децентрализованного хранилища, основанного на блокчейне:

- фрагментированные и зашифрованные файлы хранятся в виде зашифрованного текста в других узлах хранения, что позволяет получить доступ ко всем данным только ключу владельца данных;
- децентрализованная распределенная архитектура позволяет устройствам хранения данных быстро реагировать на запросы из нескольких мест, повышая эффективность системы; и
- выпуск виртуальной валюты на основе блокчейна предлагает жизнеспособное решение для стимулирования хранения.

К известным децентрализованным системам хранения, основанным на блокчейнах, относятся, например, Filecoin, Storj и Sia [6].

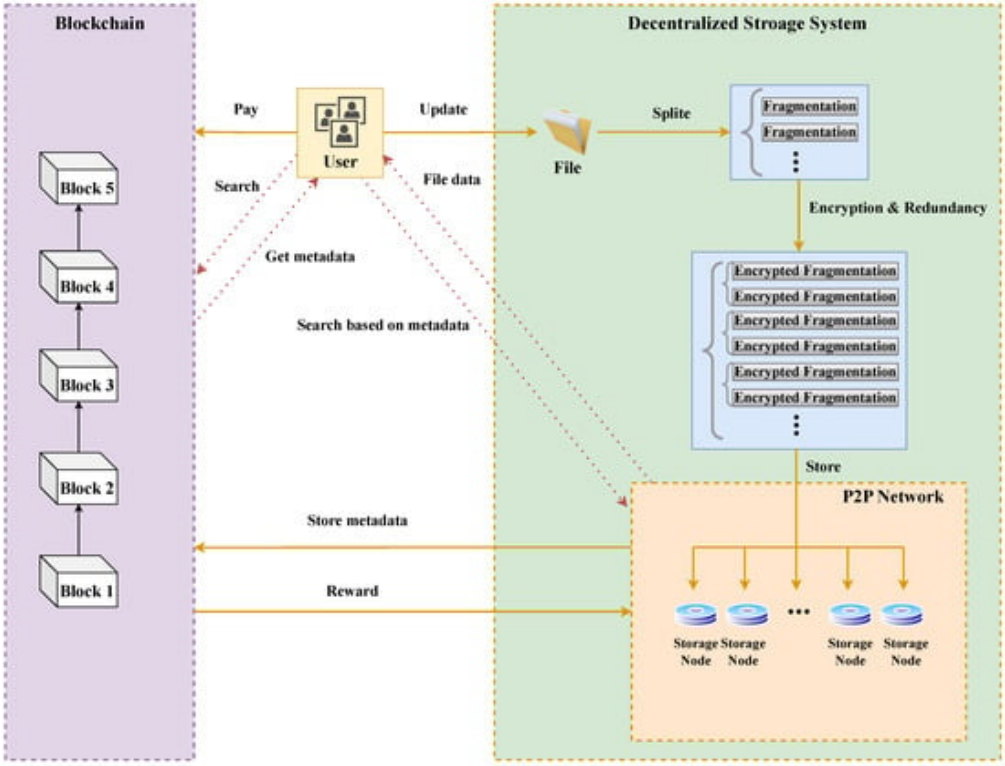

Рис.9. Децентрализованное хранилище [6]

V NFT

Термин «невзаимозаменяемый токен» (Non-Fungible Tokens - NFT) относится к незаменимому зашифрованному цифровому доказательству права собственности на основе блокчейна, в основном с использованием смарт-контрактов и технологии цифровой подписи [26]. В отличие от традиционных активов, таких как биткоин, каждый NFT имеет свой уникальный идентификатор и характеристики. Таким образом, каждый NFT уникален и отличается от любого другого. Более того, NFT неделимы, а это означает, что произведения NFT могут продаваться и циркулировать только в виде целого. NFT создается создателями или издателями цифрового контента с помощью смарт-контрактов на блокчейне. В процессе создания они могут указать атрибуты, метаданные и другую актуальную информацию NFT, чтобы обеспечить его уникальность и узнаваемость.

Модель использования NFT представлена на рисунке 10 [27]. Первым официальным стандартом NFT стал ERC721, который был предложен в 2018 году. Этот стандарт был новым стандартом блокчейна Ethereum в то время; С тех пор появился ERC1155, обладающий гибкостью и функциональными характеристиками, которых нет у ERC721 [28].

В настоящее время существует множество NFT-проектов, которые оказали значительное влияние на Web3, предложив следующие преимущества:

(1) благодаря связыванию уникальных NFT с цифровыми активами владение цифровым контентом и транзакции с ним становятся более прозрачными, безопасными и отслеживаемыми;
(2) пользователи могут гибко передавать свои NFT между различными платформами и использовать их в различных сценариях применения;
(3) создатели могут напрямую публиковать и продавать

свои работы в виде цифровых активов через NFT, что позволяет им получать вознаграждение;

(4) NFT предоставляют средства для обеспечения подлинности и отслеживания источника цифрового контента, связывая его с конкретным NFT [6].

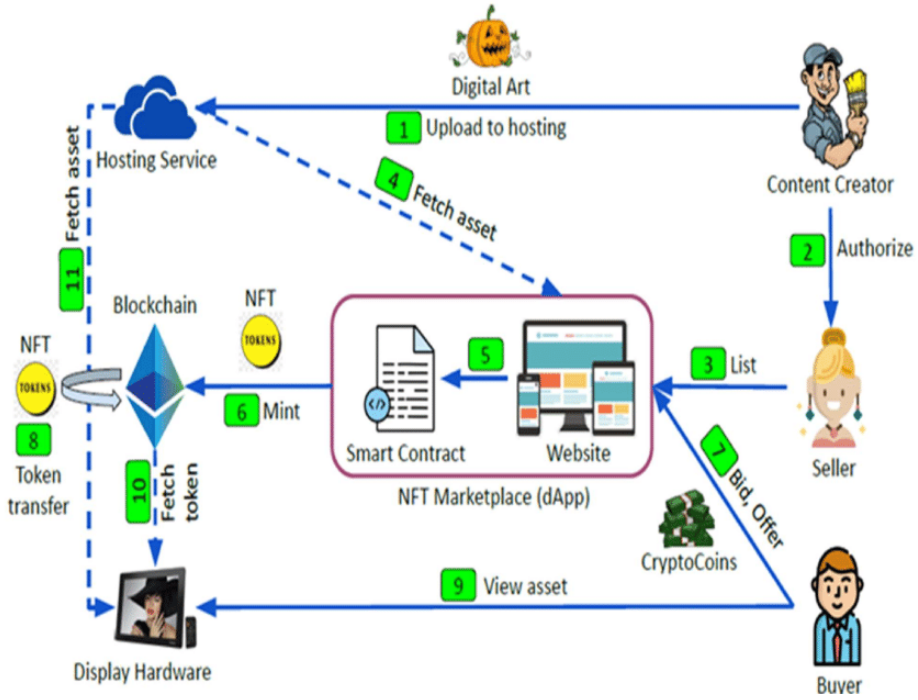

Рис. 10. Модель использования NFT [27].

VI DAO

DAO (Децентрализованная автономная организация) — это тип децентрализованной организации, которая работает через смарт-контракты в сети блокчейн, позволяя членам организации участвовать в децентрализованном принятии решений и управлении без необходимости в центральном органе или посреднике.

Другими словами, это организация, управляемая сообществом, которая использует технологию блокчейна для автономной работы, свободной от вмешательства централизованного органа. Участники могут предлагать решения и голосовать за них, а средства управляются прозрачно через блокчейн (рис. 11).

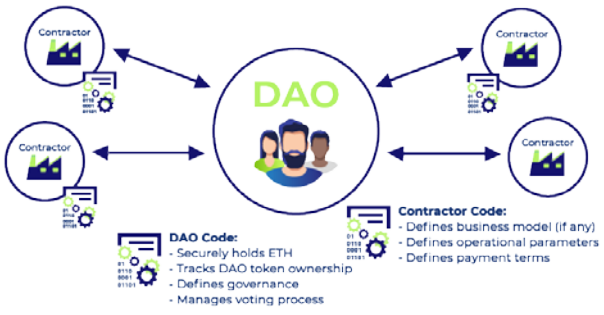

Рис. 11. Структура DAO

Новаторская организационная структура, концепция DAO построена на фундаментальных технологиях, таких как блокчейн, искусственный интеллект, большие данные и IoT [29]. Являясь фундаментальной организационной формой Web3, DAO позволяет своим участникам управлять своими собственными данными, эффективно предотвращая неправомерное использование информации о пользователях централизованными организациями. На практике DAO функционирует как органичное и прозрачное сообщество, участники которого разделяют общие цели. Каждый член имеет право участвовать в процессах принятия решений, коллективно формируя траекторию развития организации и извлекая выгоду из справедливых стимулов.

Базовая архитектура DAO проиллюстрирована на рисунке 12.

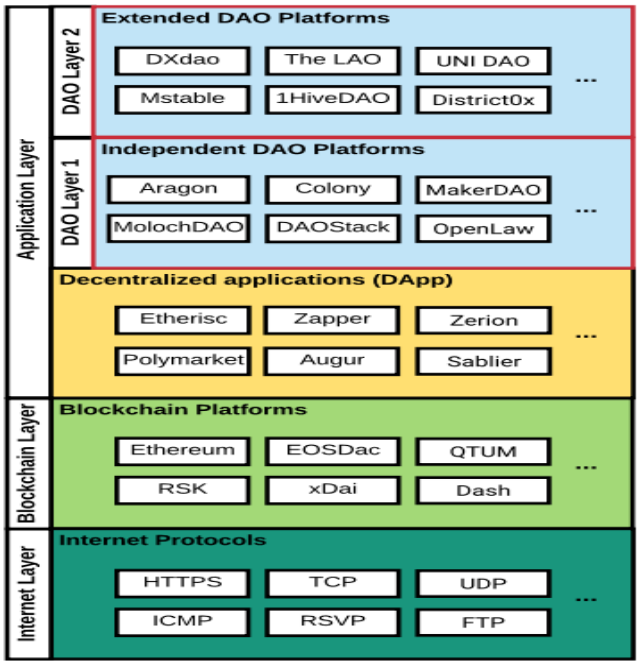

Рис. 12. Платформы DAO [31]

В основе проекта DAO лежит блокчейн, формирующий его фундаментальный слой. Средний уровень представляет собой протокол стека технологий проекта DAO, предоставляющий такие функции, как база данных распределенного реестра и API для внешнего доступа. Верхний уровень охватывает приложения, построенные на основе проекта DAO, что позволяет разработчикам реализовывать код на основе бизнес-логики приложения. Каждый слой выступает в качестве опоры для слоев, расположенных над ним, создавая целостную структуру. В работе [30] была предложена комплексная пятиуровневая эталонная модель DAO (рис. 13), которая обеспечивает всеобъемлющую основу для понимания и реализации DAO

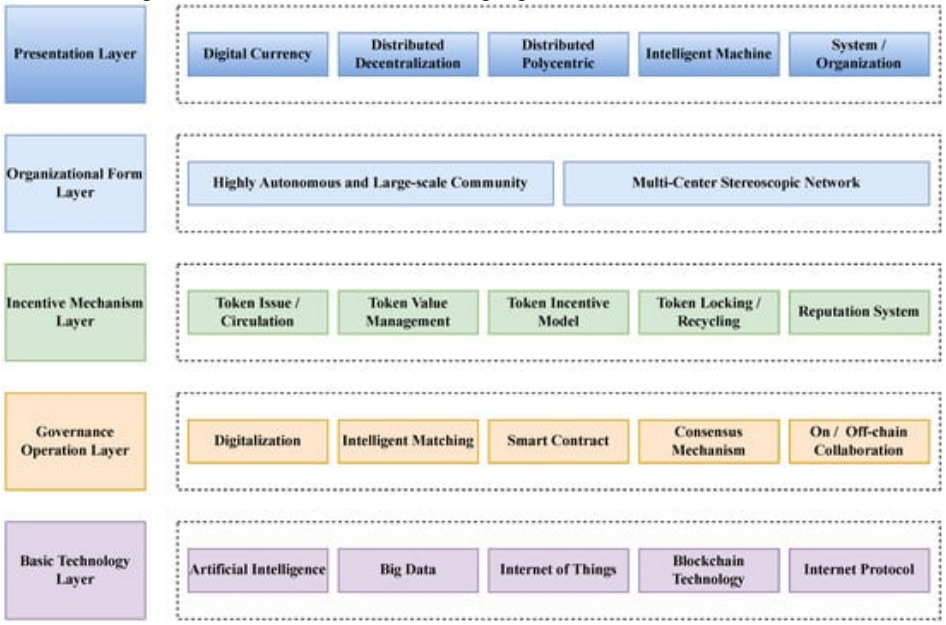

Рис. 13. Эталонная модель DAO [30]

Исходя из характеристик DAO и их модельной архитектуры, схему работы можно описать следующим образом:

1. Учреждение: создание DAO обычно начинается с начального этапа, на котором создатель или инициатор разрабатывает и публикует соглашение об управлении, смарт-контракты и связанные с ними правила и условия. Эти правила могут охватывать механизмы голосования, процессы управления, экономику токенов и другие аспекты.
2. Присоединение участника: любой желающий может свободно выбрать участие в DAO и стать участником, владея токенами DAO. Покупая токены, участвуя в обещаниях или делая другие взносы, участники приобретают права и привилегии в рамках DAO и получают возможность участвовать в процессе принятия решений.
3. Принятие решений: Принятие решений в DAO осуществляется путем голосования участников. Каждый участник имеет возможность проголосовать за или против конкретных предложений на основе своих токенов или другой назначенной доли. Эти предложения могут включать в себя важнейшие решения, включая распределение финансирования, изменения в правилах управления, направления развития проектов и многое другое. Процесс коллективного голосования гарантирует, что решения принимаются демократичным и прозрачным образом, отражая консенсус и предпочтения сообщества DAO.
4. Исполнение смарт-контрактов: протоколы управления и правила для DAO обычно реализуются в виде смарт-контрактов и выполняются на блокчейне. Решения, автоматически выполняемые в соответствии с результатами голосования участников, обеспечивают прозрачность, точность и устойчивость к взлому в процессе, который становится надежным и неизменным. Это устраняет необходимость в посредниках и обеспечивает надежную основу для принятия решений.
5. Управление и эксплуатация: члены DAO могут подавать предложения, обсуждать вопросы, участвовать в голосовании и контролировать работу DAO в процессе участия в управлении и эксплуатации. Управление и функционирование DAO может быть достигнуто с помощью регулярных голосований, обсуждений в сообществе, комитетов по управлению и т. д.
6. Распределение и вознаграждения: DAO могут мотивировать и вознаграждать вклады участников с помощью экономической модели токенов. Согласно правилам DAO, участники могут получать вознаграждения в виде токенов, дивидендов, прав на управление или других форм вознаграждений для поощрения участия и вклада.
7. Аудит и надзор: поскольку смарт-контракты и решения DAO являются открытыми и прозрачными, участники и другие соответствующие стороны могут проводить аудит и контролировать деятельность DAO, чтобы обеспечить ее соответствие, справедливость и прозрачность [6].

VII DAPPS

Децентрализованное приложение (DApp) — это тип распределенного программного приложения, которое

работает в одноранговой (P2P) сети блокчейна, а не на одном компьютере. DApps похожи на другие программные приложения, которые поддерживаются на веб-сайтах или мобильных устройствах, но их особенностью является поддержка P2P.

DApps могут работать автономно, обычно с использованием смарт-контрактов, на блокчейне или другой системе распределенного реестра. Как и традиционные приложения, DApps предоставляют пользователям некоторые функции или утилиты. Однако, в отличие от традиционных приложений, DApps работают без вмешательства человека и не принадлежат какой-либо одной организации, а распределяют токены, которые представляют собой право собственности [32]. Эти токены распределяются среди пользователей системы в соответствии с запрограммированным алгоритмом. Таким образом, приложение децентрализовано, поскольку система не контролируется каким-либо одним субъектом (рис. 14).

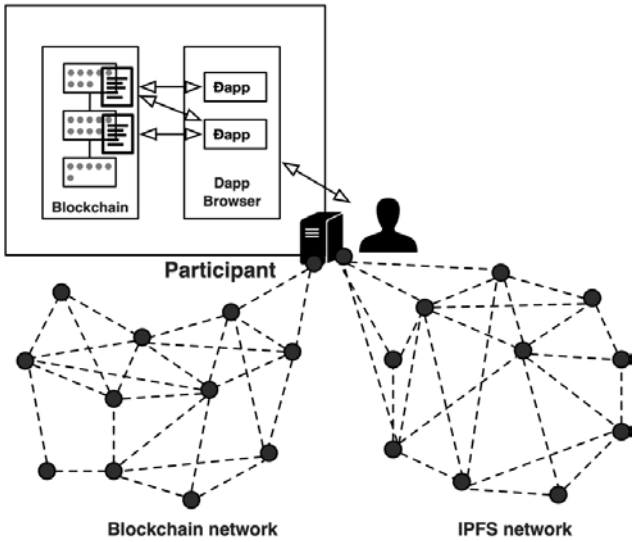

Рис. 14. DApps patterns [33]

VIII DeFi

Термин Децентрализованные финансы (DeFi) относится к финансовой системе и экосистеме приложений, построенной на технологии блокчейн [34]. Он направлен на демократизацию доступа к традиционным финансовым услугам и внедрение инновационных финансовых продуктов с помощью протоколов с открытым исходным кодом и децентрализованных сетей. С помощью DeFi люди могут беспрепятственно получить доступ к широкому спектру финансовых услуг, включая заимствования, страхование, управление капиталом и криптовалютные деривативы без необходимости в посредниках, что устраняет дорогостоящие комиссии. Используя возможности блокчейнов и смарт-контрактов, протоколы DeFi служат приложениями, которые используют распределенные записи транзакций, что приводит к расширенным возможностям обработки транзакций. Эта технология обеспечивает более быстрые, безопасные и прозрачные финансовые операции, предоставляя людям больший контроль над своими финансовыми активами и способствуя расширению доступа к финансовым услугам в глобальном масштабе.

В последние годы ландшафт DeFi превратился достаточно в сложную экосистему [6]. Как показано на рисунке 15, инфраструктуру DeFi можно разделить на три ключевых уровня. Каждый уровень выполняет жизненно важную функцию, облегчая работу и совместимость экосистемы DeFi.

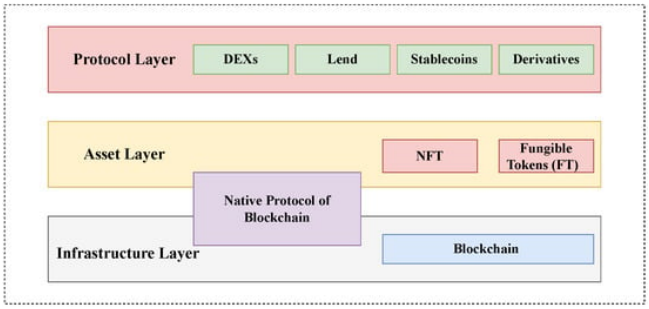

Рис. 15. Архитектура DeFi [6].

• Инфраструктурный уровень в основном состоит из блокчейна и лежащих в его основе протоколов, которые служат базовой инфраструктурой для верхних уровней. Этот уровень создает надежную и безопасную среду для транзакций, гарантируя, что переходы между статусами транзакций подтверждаются с помощью механизма консенсуса. Он обеспечивает надежный механизм хранения транзакций, гарантируя целостность и неизменность данных.

• Уровень активов в основном состоит из собственного протокола блокчейна и других протоколов активов, совместимых с базовой инфраструктурой блокчейна. Эти протоколы играют решающую роль в определении стандартов и правил обращения с различными типами активов в экосистеме. Они облегчают создание, передачу и администрирование различных цифровых активов, включая криптовалюты, токены, а также взаимозаменяемые и невзаимозаменяемые активы.

• Протокольный уровень устанавливает стандартизированные протоколы для транзакций, кредитования и криптовалютных деривативов в экосистеме DeFi. Он устанавливает правила и рамки для осуществления этой финансовой деятельности децентрализованным и не требующим доверия образом. Кроме того, разработчики создали различные интерфейсы пользовательских приложений, которые взаимодействуют со смарт-контрактами через веб-браузеры, позволяя пользователям получать доступ и использовать сервисы, предоставляемые этими протоколами.

В итоге, DeFi создал новую финансово-экономическую систему. Децентрализованная биржа (DEX) [35] в DeFi позволяет пользователям торговать собственными цифровыми активами без участия традиционных финансовых учреждений. Поскольку Web3 предоставляет DeFi основу децентрализованной системы идентификации и кредитования, пользователи могут использовать свои собственные цифровые удостоверения для аутентификации и изоморфные смарт-контракты для создания собственной кредитной

истории без необходимости оценки кредитоспособности традиционными финансовыми учреждениями.

VIII Заключение

В настоящей статье кратко рассмотрены основные архитектурные шаблоны Web3. Безусловно, Web3 предлагает собой весьма значительное изменение того, что сейчас представляет собой экосистема веб. Эти изменения затрагивают инфраструктуру, методы и подходы к разработке, инструменты разработки, бизнес-модели и, конечно, вопросы кибербезопасности. Последнее, безусловно, заслуживает отдельного рассмотрения. В частности, проблемы с безопасностью смарт-контрактов пока нигде не решены. Вопросам кибербезопасности Web3 будут посвящены отдельные работы.

Важным вопросом для дальнейшего рассмотрения является связь Web3 и Метавселенных. Последний термин относится к сгенерированному компьютером виртуальному пространству, состоящему из цифровых сред и виртуальной реальности. В Метавселенной виртуальные активы занимают центральное место. Пользователи Метавселенных могут создавать, покупать, продавать и владеть различными виртуальными активами, включая цифровые произведения искусства, виртуальную землю, игровой реквизит и многое другое. Кроме того, пользователи могут взаимодействовать, сотрудничать и общаться с другими через свои аватары в виртуальной социальной среде, предлагаемой Метавселенной. Примечательно, что транзакции с виртуальными активами в Метавселенной часто включают криптовалюты и смарт-контракты, создавая самоуправляемую экономическую систему. Метавселенная является важной областью применения Web3. Web3 включает в себя децентрализованную инфраструктуру, смарт-контракты и криптовалюты, обеспечивая децентрализованную, прозрачную и программируемую среду для Метавселенной. Децентрализованная технология Web3 обеспечивает подлинное владение виртуальными активами и дает пользователям автономию и контроль над Метавселенной. Кроме того, технология самоидентификации Web3 и токенизированных активов позволяют пользователям в Метавселенной по-настоящему выражать свою идентичность, а также владеть виртуальными активами и торговать ими. Пользователи могут взаимодействовать с другими участниками через свои цифровые удостоверения и проводить транзакции с виртуальными активами. В конечном счете, Метавселенная использует смарт-контракты и децентрализованные приложения на основе Web3 для реализации различных функций и сценариев приложений в виртуальном мире.

Благодарности

Здесь хотелось бы отметить базовые работы В.П. Куприяновского, которые и начали все направление цифровых преобразований в журнале INJOIT [36, 37]. Темы, связанные с блокчейн, также представлялись в журнале ранее [38, 39].

Библиография

[1] O'Reilly T. What is web 2.0. – " O'Reilly Media, Inc.", 2009.
[2] Hendler, Jim. "Web 3.0 Emerging." Computer 42.1 (2009): 111-113.
[3] G. Wood, “DApps: What Web 3.0 Looks Like,” Apr. 2014. [Online]. Available: http://gavwood.com/dappsweb3.html
[4] T. Gerring, “building the decentralized web 3.0,” Aug. 2014. [Online]. Available: https://blog.ethereum.org/2014/08/18/building-decentralized-web/
[5] S. Voshmgir, Token economy: how the Web3 reinvents the internet, 2nd ed. Berlin: BlockchainHub, 2020. [Online]. Available: https://github.com/sherminvo/TokenEconomyBook
[6] Lai, Y.; Yang, J.; Liu, M.; Li, Y.; Li, S. Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. Blockchains 2023, 1, 111-131
[7] Mühle, Alexander, et al. "A survey on essential components of a self-sovereign identity." Computer Science Review 30 (2018): 80-86.
[8] The difference between Web3 and Web 3.0 and the future of the Internet https://www.linkedin.com/pulse/difference-between-web3-web-30-future-internet-kirill-ostrovskii/ Retrieved: Jan, 2024
[9] Father of the Internet Says Web 3.0 Doesn’t Need Blockchain Technology https://beincrypto.com/father-of-the-internet-says-web-3-0-doesnt-need-blockchain-technology/ Retrieved: Jan, 2024
[10] Sambra, Andrei Vlad, et al. "Solid: a platform for decentralized social applications based on linked data." MIT CSAIL & Qatar Computing Research Institute, Tech. Rep. (2016).
[11] Korpal, Gaurish, and Drew Scott. "Decentralization and web3 technologies." Authorea Preprints (2023).
[12] Web3 Foundation https://web3.foundation/ Retrieved: Jan, 2024
[13] Web3 stack https://web3-technology-stack.readthedocs.io/en/latest/ Retrieved: Jan, 2024
[14] Zhang, Rui, Rui Xue, and Ling Liu. "Security and privacy on blockchain." ACM Computing Surveys (CSUR) 52.3 (2019): 1-34.
[15] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[16] V. Buterin, “Ethereum Whitepaper,” 2014. [Online]. Available: https://github.com/ethereum/wiki/blob/f83c4692be242ad350bef0c5f8757b7b3c27b2d9/%5BEnglish%5D-White-Paper.md
[17] Кибербезопасность https://cyber.cs.msu.ru/ Retrieved: Jan 25.2024.
[18] Xiao, Yang, et al. "A survey of distributed consensus protocols for blockchain networks." IEEE Communications Surveys & Tutorials 22.2 (2020): 1432-1465.
[19] J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” Jan. 2016. https://lightning.network/lightning-network-paper.pdf Retrieved: Jan 2024
[20] Top 5 blockchain protocols https://zebpay.com/blog/top-5-blockchain-protocols Retrieved: Jan 2024
[21] OPEN, PERMISSIONED DISTRIBUTED PLATFORM https://r3.com/products/corda/ Retrieved: Jan 2024
[22] Gangwal, Ankit, Haripriya Ravali Gangavalli, and Apoorva Thirupathi. "A survey of Layer-two blockchain protocols." Journal of Network and Computer Applications 209 (2023): 103539.
[23] Miers, Ian, et al. "Zerocoin: Anonymous distributed e-cash from bitcoin." 2013 IEEE Symposium on Security and Privacy. IEEE, 2013.
[24] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561 (2014).
[25] Steichen, Mathis, et al. "Blockchain-based, decentralized access control for IPFS." 2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData). IEEE, 2018.
[26] Wang, Qin, et al. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." arXiv preprint arXiv:2105.07447 (2021).
[27] Ahubele, B.O. & Okolai, B.D. (2022): A Formal Verification Model for Security Vulnerability in Non-Fungible Tokens (NFTs) Platform. Journal of Advances in Mathematical & Computational Sciences. Vol. 9, No. 2. pp. 61-74.
[28] ERC-20 vs ERC-721 vs ERC-1155 https://de.fi/blog/erc-1155-vs-erc-721-nft-standards#:~:text=ERC%2D721%20is%20a%20token,one%2Dto%2Done%20basis. Retrieved: Jan 2024

[29] Singh, Madhusudan, and Shiho Kim. "Blockchain technology for decentralized autonomous organizations." Advances in computers. Vol. 115. Elsevier, 2019. 115-140.
[30] Wang, Shuai, et al. "Decentralized autonomous organizations: Concept, model, and applications." IEEE Transactions on Computational Social Systems 6.5 (2019): 870-878.
[31] Research Summary: A Decision Model for Decentralized Autonomous Organization Platform Selection: Three Industry Case Studies https://www.smartcontractresearch.org/t/research-summary-a-decision-model-for-decentralized-autonomous-organization-platform-selection-three-industry-case-studies/1157 Retrieved: Jan, 2024
[32] Wu, Kaidong, et al. "A first look at blockchain -based decentralized applications." Software: Practice and Experience 51.10 (2021): 2033-2050.
[33] Decentralised Applications (DApps) https://research.csiro.au/blockchainpatterns/general-patterns/deployment-patterns/dapp/ Retrieved: Jan, 2024
[34] Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. "Decentralized finance (defi)." Journal of Financial Regulation 6 (2020): 172-203.
[35] Xu, Jiahua, et al. "Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols." ACM Computing Surveys 55.11 (2023): 1-50.
[36] Куприяновский, В. П., Д. Е. Намиот, and С. А. Синягов. "Демистификация цифровой экономики." International Journal of Open Information Technologies 4.11 (2016): 59-63.
[37] Куприяновский, В. П., et al. "Розничная торговля в цифровой экономике." International Journal of Open Information Technologies 4.7 (2016): 1-12.
[38] Намиот, Д. Е., et al. "Приложения блокчейн на транспорте." International Journal of Open Information Technologies 5.12 (2017): 130-134.
[39] Куприяновская, Ю. В., et al. "Умный контейнер, умный порт, BIM, Интернет Вещей и блокчейн в цифровой системе мировой торговли." International Journal of Open Information Technologies 6.3: 2018.

Web3 Architectural Models

Dmitry Namiot, Vasily Kupriyanovsky

***Abstract*— This article discusses the main architectural components (models) of Web3. There is some ambiguity in the literature regarding the latter designation. Web 3.0 still corresponds to the semantic web (as a further development of the Web 2.0 approach - dynamic content created by network users). In this article, Web3 technology is considered specifically as a decentralized web. The core idea of Web3 is to give data ownership back to users through decentralization. Web3 should allow users to have full control over the data and content they create. It is the users (owners of information) who must decide who can access this information. Web3 achieves this through decentralized data storage based on blockchain technologies and sovereign identity based on DAOs (decentralized autonomous organizations). The basic idea of Web3 is to implement a serverless Internet, that is, a global network in which users generate content that they own.**

***Keywords*— blockchain, smart contracts, DAO, DApps, DeFi.**

REFERENCES

[1] O'Reilly T. What is web 2.0. – " O'Reilly Media, Inc.", 2009.
[2] Hendler, Jim. "Web 3.0 Emerging." Computer 42.1 (2009): 111-113.
[3] G. Wood, “DApps: What Web 3.0 Looks Like,” Apr. 2014. [Online]. Available: http://gavwood.com/dappsweb3.html
[4]T. Gerring, “building the decentralized web 3.0,” Aug. 2014. [Online]. Available: https://blog.ethereum.org/2014/08/18/building-decentralized-web/
[5] S. Voshmgir, Token economy: how the Web3 reinvents the internet, 2nd ed. Berlin: BlockchainHub, 2020. [Online]. Available: https://github.com/sherminvo/TokenEconomyBook
[6] Lai, Y.; Yang, J.; Liu, M.; Li, Y.; Li, S. Web3: Exploring Decentralized Technologies and Applications for the Future of Empowerment and Ownership. Blockchains 2023, 1, 111-131
[7] Mühle, Alexander, et al. "A survey on essential components of a self-sovereign identity." Computer Science Review 30 (2018): 80-86.
[8] The difference between Web3 and Web 3.0 and the future of the Internet https://www.linkedin.com/pulse/difference-between-web3-web-30-future-internet-kirill-ostrovskii/ Retrieved: Jan, 2024
[9] Father of the Internet Says Web 3.0 Doesn’t Need Blockchain Technology https://beincrypto.com/father-of-the-internet-says-web-3-0-doesnt-need-blockchain-technology/ Retrieved: Jan, 2024
[10] Sambra, Andrei Vlad, et al. "Solid: a platform for decentralized social applications based on linked data." MIT CSAIL & Qatar Computing Research Institute, Tech. Rep. (2016).
[11] Korpal, Gaurish, and Drew Scott. "Decentralization and web3 technologies." Authorea Preprints (2023).
[12] Web3 Foundation https://web3.foundation/ Retrieved: Jan, 2024
[13] Web3 stack https://web3-technology-stack.readthedocs.io/en/latest/ Retrieved: Jan, 2024
[14] Zhang, Rui, Rui Xue, and Ling Liu. "Security and privacy on blockchain." ACM Computing Surveys (CSUR) 52.3 (2019): 1-34.
[15] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[16] V. Buterin, “Ethereum Whitepaper,” 2014. [Online]. Available: https://github.com/ethereum/wiki/blob/f83c4692be242ad350bef0c5f8757b7b3c27b2d9/%5BEnglish%5D-White-Paper.md
[17] Kiberbezopasnost' https://cyber.cs.msu.ru/ Retrieved: Jan 25.2024.
[18] Xiao, Yang, et al. "A survey of distributed consensus protocols for blockchain networks." IEEE Communications Surveys & Tutorials 22.2 (2020): 1432-1465.
[19] J. Poon and T. Dryja, “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” Jan. 2016. https://lightning.network/lightning-network-paper.pdf Retrieved: Jan 2024
[20] Top 5 blockchain protocols https://zebpay.com/blog/top-5-blockchain-protocols Retrieved: Jan 2024
[21] OPEN, PERMISSIONED DISTRIBUTED PLATFORM https://r3.com/products/corda/ Retrieved: Jan 2024
[22] Gangwal, Ankit, Haripriya Ravali Gangavalli, and Apoorva Thirupathi. "A survey of Layer-two blockchain protocols." Journal of Network and Computer Applications 209 (2023): 103539.
[23] Miers, Ian, et al. "Zerocoin: Anonymous distributed e-cash from bitcoin." 2013 IEEE Symposium on Security and Privacy. IEEE, 2013.
[24] Benet, Juan. "Ipfs-content addressed, versioned, p2p file system." arXiv preprint arXiv:1407.3561 (2014).
[25] Steichen, Mathis, et al. "Blockchain-based, decentralized access control for IPFS." 2018 Ieee international conference on internet of things (iThings) and ieee green computing and communications (GreenCom) and ieee cyber, physical and social computing (CPSCom) and ieee smart data (SmartData). IEEE, 2018.
[26] Wang, Qin, et al. "Non-fungible token (NFT): Overview, evaluation, opportunities and challenges." arXiv preprint arXiv:2105.07447 (2021).
[27] Ahubele, B.O. & Okolai, B.D. (2022): A Formal Verification Model for Security Vulnerability in Non-Fungible Tokens (NFTs) Platform. Journal of Advances in Mathematical & Computational Sciences. Vol. 9, No. 2. pp. 61-74.
[28] ERC-20 vs ERC-721 vs ERC-1155 https://de.fi/blog/erc-1155-vs-erc-721-nft-standards#:~:text=ERC%2D721%20is%20a%20token,one%2Dto%2Done%20basis. Retrieved: Jan 2024
[29] Singh, Madhusudan, and Shiho Kim. "Blockchain technology for decentralized autonomous organizations." Advances in computers. Vol. 115. Elsevier, 2019. 115-140.
[30] Wang, Shuai, et al. "Decentralized autonomous organizations: Concept, model, and applications." IEEE Transactions on Computational Social Systems 6.5 (2019): 870-878.
[31] Research Summary: A Decision Model for Decentralized Autonomous Organization Platform Selection: Three Industry Case Studies https://www.smartcontractresearch.org/t/research-summary-a-decision-model-for-decentralized-autonomous-organization-platform-selection-three-industry-case-studies/1157 Retrieved: Jan, 2024
[32] Wu, Kaidong, et al. "A first look at blockchain-based decentralized applications." Software: Practice and Experience 51.10 (2021): 2033-2050.
[33] Decentralised Applications (DApps) https://research.csiro.au/blockchainpatterns/general-patterns/deployment-patterns/dapp/ Retrieved: Jan, 2024
[34] Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. "Decentralized finance (defi)." Journal of Financial Regulation 6 (2020): 172-203.
[35] Xu, Jiahua, et al. "Sok: Decentralized exchanges (dex) with automated market maker (amm) protocols." ACM Computing Surveys 55.11 (2023): 1-50.
[36] Kuprijanovskij, V. P., D. E. Namiot, and S. A. Sinjagov. "Demistifikacija cifrovoj jekonomiki." International Journal of Open Information Technologies 4.11 (2016): 59-63.
[37] Kuprijanovskij, V. P., et al. "Roznichnaja torgovlja v cifrovoj jekonomike." International Journal of Open Information Technologies 4.7 (2016): 1-12.
[38] Namiot, D. E., et al. "Prilozhenija blokchejn na transporte." International Journal of Open Information Technologies 5.12 (2017): 130-134.
[39] Kuprijanovskaja, Ju. V., et al. "Umnyj kontejner, umnyj port, BIM, Internet Veshhej i blokchejn v cifrovoj sisteme mirovoj torgovli." International Journal of Open Information Technologies 6.3: 2018.