

УДК 347.73

ББК 65.3

DOI 10.24411/2073-3305-2021-2-139-141

ЦИФРОВЫЕ АКТИВЫ, ТЕХНОЛОГИЯ БЛОКЧЕЙН И СЕРВИСЫ ДЛЯ УПРАВЛЕНИЯ ЦИФРОВЫМИ АКТИВАМИ

Магомед Вахаевич АБУБАКАРОВ,

кандидат экономических наук, заведующий кафедрой
экономики и управления в образовании

Чеченского государственного педагогического университета

E-mail: magomed.abubakarov2015@mail.ru

Рецензент: М.-Р.Б. Хадисов, кандидат экономических наук

Аннотация. Цифровые активы, представляющие собой криптовалюты, созданные с применением блокчейн-технологии, применяются достаточно часто в финансовых отношениях. Сложившаяся ситуация на рынке заставляет обратить свое внимание на необычный вид активов даже самых больших гигантов классической финансовой системы. Изучение, применение или создание собственных инструментов для управления такими цифровыми активами становится основной деятельностью многих учреждений.

Ключевые слова: цифровая экономика; технологии блокчейн; криптовалюта; финансовые отношения.

DIGITAL ASSETS, BLOCKCHAIN TECHNOLOGY AND DIGITAL ASSET MANAGEMENT SERVICES

Magomed Vakhaevich ABUBAKAROV,

Candidate of Economic Sciences,
Head of the Department of Economics
and Management in Education,
Chechen State Pedagogical University

E-mail: magomed.abubakarov2015@mail.ru

Reviewer: M.-R.B. Khadisov, Candidate of Economic Sciences

Abstract. Digital assets, which are cryptocurrencies created using blockchain technology, are used quite often in financial relations. The current situation on the market forces one to pay attention to an unusual type of assets, even of the largest giants of the classical financial system. Studying, applying or creating custom tools for managing such digital assets is becoming the main activity of many institutions.

Keywords: digital economy; blockchain technologies; cryptocurrency; financial relations.

Чтобы дать определение цифрового актива, обратимся к Словарю банковских терминов, официально закрепленных и используемых в экономических отношениях и при разрешении правовых споров.

Цифровой актив — информационный ресурс, производный от права на ценность и обращающийся в распределенном реестре в виде уникального идентификатора.

Под управлением понимается возможность своевременно получать количественную инфор-

мацию об остатках или новых поступлениях, иметь возможность совершить операцию перераспределения средств между собственными кошельками, а также полное или частичное списание в пользу другого участника финансовых отношений. Другими словами, управление цифровыми активами позволяет полностью контролировать состояние этих средств и своевременно совершать различные операции обмена.

Блокчейн формально — это растущий список записей, называемых блоками, которые ис-

пользуют криптографию для обеспечения связей между собой. Данную технологию можно представить в виде алгоритмической структуры данных как хеш-дерево, или дерево Меркла. Одиночную цепочку блоков можно представить в виде связного списка, где связью будет хеш-сумма предыдущего блока [1].

На рис. 1 изображено схематичное представление цепочки блоков. Черным цветом изображена основная цепочка, которая содержит самую длинную серию блоков от первоначального блока (genesis), отмеченного светло-серым цветом. Темно-серым отмечены «осиротевшие» блоки, которые не получили достаточной длины блоков, чтобы стать основной цепочкой.

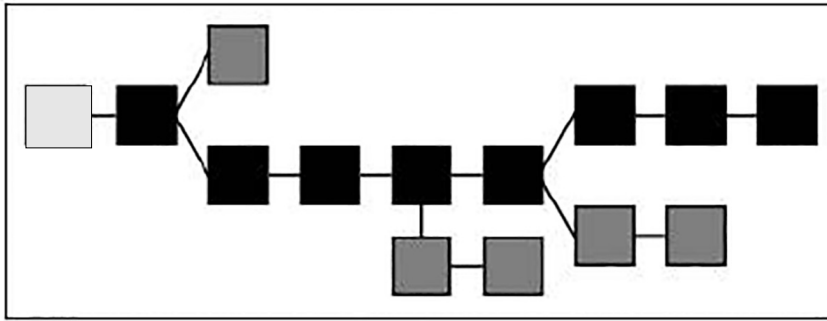


Рис. 1. Схематичное представление блокчейн

Блокчейн изначально проектировался невосприимчивым к изменению зафиксированных и подтвержденных в цепи данных. За счет хранения хеш-суммы предыдущего блока малейшее изменение данных заставит переписывать все последующие блоки цепи. Помимо этого, целостность гарантируется и проверяется всеми участниками распределенной сети. Блокчейн можно использовать в качестве распределенного регистра данных или как общую бухгалтерскую книгу, тогда все участники сети верифицируют новые блоки, рассчитывают хеш-сумму предыдущего блока и добавляют блок к основной цепочке. Если будет попытка подменить данные, то злоумышленник должен обладать 51% вычислительных мощностей всей сети, только тогда он сможет прикрепить неправильные данные к цепочке.

Необходимо разделять технологию блокчейн и основанные на ней криптовалюты, которые являются лишь частным применением технологии и не являются тождественными понятиями [2]. В России их упрощенно классифицируют на два вида — открытые и закрытые.

Чтобы совершать обменные операции в системах, построенных на блокчейн, необходимо иметь собственный адрес, на который будут зачисляться средства или списываться с него. Для подтверждения владения адресом необходимо иметь приватный ключ от этого адреса. В схожих с Bitcoin криптовалютах адрес — это хеш-

сумма публичного ключа, выведенного из приватного, хеш — сумма проходит через функции SHA256, а затем RIPEMD160. Для получения средств участие владельца адреса не требуется, а вот для перевода необходимо подписать транзакцию криптографическим ключом.

Необходимо также иметь доступ в децентрализованную сеть, чтобы отправить платежную транзакцию. Для этого можно запустить собственный узел, который будет полной репликой всей сети. Другим вариантом будет использование узла, открытого для общего доступа.

Зачастую многие сервисы отличаются способами взаимодействия с узлами, наличием ключей у пользователя и количеством поддерживаемых криптовалют. Клиентские реализации можно разделить на два вида:

1) толстые — требуют загрузку блокчейн-сети на клиентскую машину, чем занимают множество места на диске и времени на подготовку к работе;

2) тонкие — соединяются с удаленными серверами сервиса, как правило, по протоколу HTTP, которые сервисом передаются в узлы сети.

Blockchain Wallet, Coinbase — веб-клиенты, позволяют пользоваться криптовалютами кошельками как обычным интернет-банком, вся сложность взаимодействия с блокчейн скрыта от пользователя. В стандартном режиме работы не предоставляют пользователям приватные ключи от кошельков. Сервисы по-

добного типа являются условно бесплатными либо могут взимать дополнительную комиссию за совершение переводов, также собирают

пользовательские данные. Они ограничены по количеству валют в кошельках, предоставляют ограниченный Web API.

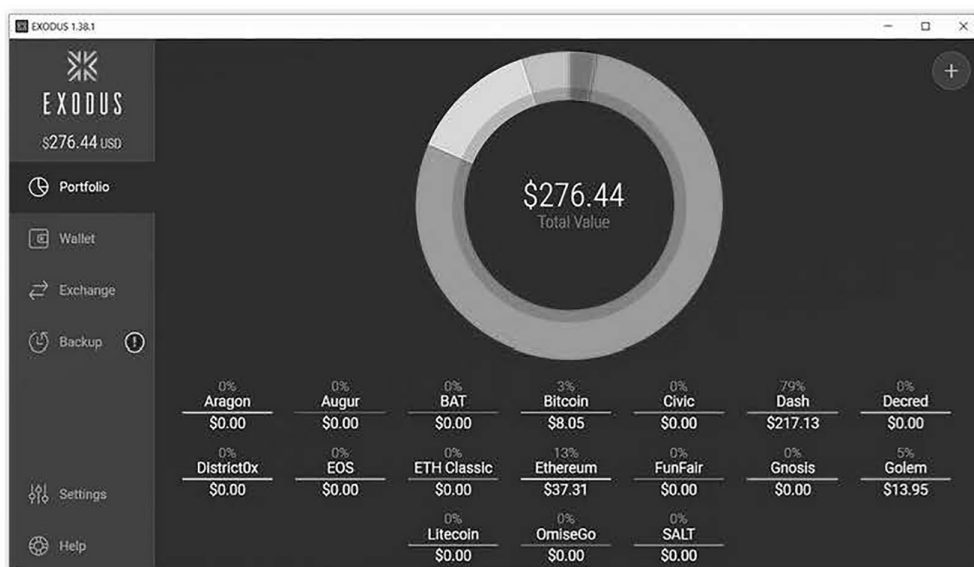


Рис. 2. Пример пользовательского интерфейса клиента Exodus

При взаимодействии в схеме, когда одиночный клиент совершает платежную операцию в пользу бизнес-клиента или, наоборот, ожидает получения средств, не проявляется никаких сложностей в управлении кошельками и их балансами. Достаточно использовать любой клиент- или веб-сервис в зависимости от целей сохранения приватности данных и желаемой валюты.

Если взаимодействие происходит между двумя бизнес-клиентами, то проблема групповых операций становится более актуальной, необходимо с нескольких кошельков сделать перевод на один адрес или несколько адресов, а также моментально отреагировать на поступление средств для своевременного начала выполнения обязательств со своей стороны. Таким образом, сервисы и инструменты, предназначенные для использования одиночными пользователями, плохо подходят к схеме.

Нами представлена краткая история развития цифровых технологий и приведены примеры возможных применений технологии вне экономической сферы. Перечислены самые известные, функционирующие на текущий момент криптовалюты с указанием их отличий друг от друга. В дополнение к этому представлены клиентские приложения и сервисы для взаимодействия с блокчейн-сетью и управления цифровыми активами. Описаны способы взаимодействия с различными типами клиентов.

Список литературы

1. Аксенов Д.А., Куприков А.П., Саакян П.А. Направления и особенности применения блокчейн-технологии в экономике. СПб., 2018.
2. Бенгли Д. Жемчужины программирования. 2-е изд. СПб.: Питер, 2019.
3. Донован А.А. Язык программирования Go. М.: Вильямс, 2020.