

КЛАССИФИКАЦИЯ БЛОКЧЕЙН-СИСТЕМ ПО ПОКОЛЕНИЯМ

Аннотация: данная работа описывает метод классификации блокчейн-систем, таких как криптовалюты, по поколениям. На сегодняшний день принято разделять блокчейн-системы на три поколения, однако достаточно редко приводятся конкретные признаки этих трёх поколений. Попытка это сделать была предпринята в данной работе. Описаны различия между блокчейн-системами 1.0, 2.0 и 3.0, приведены примеры каждого поколения.

Ключевые слова: блокчейн, криптовалюты, Bitcoin, Ethereum, Hyperledger.

Annotation: this paper describes a method of classifying blockchain systems like cryptocurrencies by generations. Today it is a very common opinion that blockchain-systems should be classified into three generations, but they're rarely described closely. The approach to this task was made in this paper. Differences between blockchain 1.0, 2.0 and 3.0 are described, instances of every generations are given.

Keywords: blockchain, cryptocurrencies, Bitcoin, Ethereum, Hyperledger.

Одной из актуальных проблем, которая сегодня стоит перед специалистами в области блокчейна, является классификация всех блокчейн-систем по различным признакам. Необходимо это для различных задач: с одной стороны, классификация необходима для построения определённой статистики (в какую сторону развиваются блокчейн-системы, как они трансформируются и т.д.), а с другой, она может помочь разработчикам создавать новые системы с

характеристиками, которые редко используются, но которые при этом потенциально интересны.

Одной из этих характеристик является поколение блокчейн-систем. Термин «блокчейн-системы» в данном тексте применяется неслучайно, так как на базе блокчейна сегодня создаются не только криптовалюты, но и другие распределённые приложения, напрямую не связанные с оборотом валюты [1]. Тем не менее далеко не в каждом поколении возможно использование блокчейна для создания именно распределённых приложений, о чём подробно рассказано ниже.

Принято считать, что поколения блокчейн-систем три: блокчейн 1.0, 2.0 и 3.0. К блокчейну 1.0 относят традиционные криптовалюты, которые чаще всего являются клонами Bitcoin, к 2.0 относят более новые Ethereum и Waves, а к 3.0 относят самые современные системы, такие как Ada, Tezos и другие. Но в чём их конкретное различие?

В блокчейне 1.0 все данные однотипны, а их структура, как и логика работы с ними, изначально заложены в систему. При этом считается, что системы, использующие такой блокчейн, могут быть исключительно платёжными, в которых оборачивается криптовалюта, что теоретически не совсем корректно, т.к. если разработать собственное нефинансовое приложение, использующее для хранения данных собственную реализацию блокчейна, то речь будет идти о блокчейне 1.0, т.к. в нём не используются смарт-контракты (которые будут описаны ниже). Тем не менее, при упоминании блокчейна 1.0 обычно подразумевается первое поколение криптовалют, в которых очень простой скриптовый язык, не позволяющий писать сложные программы для работы с данными в блокчейне [2].

К таким криптовалютам относятся Bitcoin, Litecoin, Dogecoin и другие. Первая система на базе блокчейна 1.0 – это Bitcoin, первая версия которой была выпущена в 2009 году.

Системы, использующие блокчейн 2.0, отличаются тем, что они поддерживают смарт-контракты. Автором идеи смарт контрактов был Ник Сабо,

который в 1994 году предложил использовать компьютерные алгоритмы с пользовательскими интерфейсами для проведения сделок в области электронной коммерции [3]. По задумке автора, описание условий контрактов должно было осуществляться с помощью математических инструментов и языков программирования. В качестве дани идеям Сабо сегодня практически любая программа, работающая на блокчейне, называется смарт-контрактом несмотря на то, что достаточно обширная часть из них не используется как деривативы.

Несмотря на то, что идея смарт-контракта на практике была частично реализована в системах блокчейн 1.0 (несмотря на то, что из соображений безопасности, а также по причине отсутствия полноты по Тьюрингу инструкции, позволяющие создавать смарт-контракты, не использовались), впервые смарт-контракты в современном понимании были описаны в проекте Ethereum в 2013 году, который и стал первым проектом блокчейн 2.0, реализованным на практике в ноябре 2015 года. В данном проекте были предложены языки программирования, обладавшие полнотой по Тьюрингу [4], одним из наиболее используемых из которых в конце концов оказался Solidity. При этом возможности языков позволяют создавать распределённые приложения, не связанные напрямую с платёжными операциями в сети (один из примеров – компьютерная игра CryptoKitties, работающая на базе блокчейна Ethereum).

Особенность систем блокчейн 2.0 заключается в том, что смарт-контракты отправляются в сеть как транзакции, таким образом они являются частью блокчейна и хранятся непосредственно в нём. Задача их выполнения лежит на узлах, поддерживающих сеть (т.к. Ethereum по аналогии с системой Bitcoin использует механизм консенсуса Proof-of-Work, эти узлы также называют майнерами). Таким образом, Ethereum можно назвать децентрализованной виртуальной машиной.

Что же касается систем, основанных на блокчейне 3.0, то единое определение их характерных признаков пока не было принято. Однако многие сходятся во мнении, что отличительная черта таких систем – это реализуемый различными методами отказ от хранения децентрализованных приложений и

токенов/информации в одном блокчейне. В случае с криптовалютами это позволяет таким системам работать с токенами, не являющимися частью системы (например, для написания смарт-контрактов в EOS можно использовать криптовалюту Bitcoin, а не только внутреннюю). В случае с децентрализованными приложениями, не являющимися криптовалютами, это позволяет полностью отказаться от оборота токенов в сети, если это необходимо. Во всех случаях цели у такой технологии общие – увеличить скорость работы таких систем, увеличить функциональность и обеспечить коммуникацию между несколькими блокчейнами.

На сегодняшний день это самое актуальное направление развития технологии. К блокчейну 3.0 можно отнести Lightning Network – сеть, работающая поверх других блокчейнов и призванная значительно увеличить скорость функционирования систем на их основе в случае, если это необходимо. На данный момент эта система активно используется в Bitcoin для решения проблемы масштабируемости криптовалюты. Также к блокчейну 3.0 можно отнести и проект Hyperledger Fabric, который использовался в данной работе для исследования рациональности использования блокчейна на предприятиях. При этом Hyperledger Fabric можно назвать первой системой блокчейн 3.0 – она появилась в 2015 году.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Чистяков М. «Hyperledger Fabric: особенности, сферы применения», Аллея Науки, No. 2 (18), 776-780 (2018).
2. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. / S.Nakamoto [Электронный ресурс]. URL: <https://bitcoin.org/bitcoin.pdf> (дата обращения: 21.03.2019)
3. Szabo N. Smart Contracts / N. Szabo, 1994 [Электронный ресурс]. URL: <https://web.archive.org/web/20011102030833/http://szabo.best.vwh.net:80/smart.contracts.html> (дата обращения: 24.04.2019)
4. Wood G. Ethereum: A Secure Decentralised Generalized Transaction Ledger / G. Wood [Электронный ресурс]. URL: <https://gavwood.com/paper.pdf> (13.04.2019).