

ЭФИРИУМ

Мамаева Н.В. Email: Mamaeva641@scientifictext.ru

Мамаева Наталья Владимировна – студент магистратуры,
кафедра прикладной математики и информатики, физико-математический факультет,
Марийский государственный университет, г. Йошкар-Ола, Республика Марий Эл

Аннотация: в статье описывается, что такое криптовалюта, рассматривается одна из наиболее популярных криптовалют – Эфириум. Также рассматривается технология блокчейн для использования смарт-контрактов. Описывается внутренняя валюта и основное горючее Эфириума. Далее излагается информация о двух видах сетей, тестовой и реальной, и объясняется написание и использование смарт-контрактов в данных сетях. После чего рассматривается алгоритм консенсуса Proof of Authority, а также компоненты Эфириума: кошелек, кран и интегрированная среда разработки.

Ключевые слова: Эфириум, смарт-контракт, «умный контракт», блокчейн, криптовалюта, валюта, газ, тестовая сеть, реальная сеть.

ETHEREUM

Mamaeva N.V.

Mamaeva Natalya Vladimirovna – Master's Student,
Department of Applied Mathematics and Informatics, Faculty of Physics and Mathematics,
Mari State University, Yoshkar-Ola, Mari El Republic

Abstract: in the article it is described what is the cryptocurrency, is examined one of the most popular crypto currency - the Ethereum. Also, the technology of blockchain for the use of smart contracts is being considered. Describes the domestic currency and the main fuel of the Ethereum. The information on the two types of networks is presented, test network and real network, and explains the writing and use of smart contracts in these networks. After that, the algorithm of consensus of the Proof of Authority is considered, as well as the components of the Ethersum: a wallet, a faucet and an integrated development environment.

Keywords: Ethereum, smart contract, blockchain, cryptocurrency, currency, Gas, test network, real network.

УДК 336.763

Криптовалюта – это цифровая (виртуальная) валюта, использующая криптографические технологии для защиты транзакций [1, с. 86]. Одной из самых популярных криптовалют является Эфириум. Эфириум (англ. Ethereum) является площадкой, на которой возможна разработка децентрализованных приложений, использующих технологию блокчейн, используя смарт-контракты. Блокчейн – представляет из себя децентрализованное хранилище информации, содержащую в себе сведения обо всех сделках, которые когда-либо проводили участники, подключенные к Эфириум. Сведения в структуре хранятся в виде цепочки блоков, в каждом из блоков указано определенное число сделок (транзакций). Смарт контракт – специализированное приложение, которое автоматически проверяет условия договора и реализовывает указанные в контракте договоренности. Смарт-контракт позволяет сторонам переговоров обмениваться между собой активами: акции, деньги или имущество без привлечения третьей стороны в качестве посредника [2, с. 6]. Эфириум – это общий децентрализованный виртуальный механизм, включающий в себя собственную виртуальную валюту для расчетов – «Ethereum» (ETH). Эфир является внутренней криптовалютой, ее добывают майнеры, что, в свою очередь, позволяет поддерживать сеть в работоспособном состоянии. Одна единица эфира разделяется на: Finney, Szabo, Gwei, Mwei, Kwei, Wei – самая маленькая часть эфира.

Таблица 1. Соотношение единиц эфира

Название	Количество эфира
Ether	1 (1:1)
Finney	0.001 (1:1000)
Szabo	0.000001 (1:1000000)
Gwei	0.000000001 (1:1000000000)
Mwei	0.000000000001 (1:1000000000000)
Kwei	0.000000000000001 (1:1000000000000000)
Wei	0.000000000000000001 (1:1000000000000000000)

Комиссия за сделку начисляется в газе, а уплачивается эфиром. Получается, что газ – это основное горючее Эфириума, которое расходуется на исполнение сделок, осуществление «умных контрактов»,

запуск «DApps» (децентрализованное приложение), а также для покрытия расходов на хранение данных. У газа имеется две составные части – это лимит и стоимость. Первая часть газа («Gas limit») – это самое большое значение газа, которым пользователь может расплатиться за осуществление умного контракта или для подтверждения сделки. Вторая часть газа («Gas Price») – объем Gwei, которое пользователь желает оплатить за каждую монету газа. Сеть Эфириум устроена таким образом, что чем больше газа не прочь израсходовать пользователь за осуществление транзакции, то тем выше по приоритету будет его сделка в сети «Ethereum», так как премия майнера будет больше.

Эфириум имеет два вида сетей: тестовую и реальную. В реальной сети для получения эфира придется заплатить реальные деньги. В свою очередь «эфир» в тестовой сети ничего не стоит и получить его не составляет никакого труда. Тестовая сеть создана для того что бы без рисков для сторон тестировать смарт-контракты перед их применением в реальной сети. Тест умных контрактов выполняется следующим образом: загружают в одну из тестовых сетей один контракт или контракты. Далее контракту присваивают тестовые параметры, отличающиеся от реальной сети, в которой будет работать контракт. А после, уже вручную, выборочно тестируют основные виды активности. В умных контрактах имеется математическая точность и логика работы, устанавливающая как методы должны менять условия контракта, какие должны выпускаться события, в каком случае, когда и кому нужно перевести активы, а когда наложить санкции на ту или иную сторону. В силу слабого развития инструментов отладки умных контрактов, на данный момент тестирование смарт-контрактов стало неотъемлемым этапом разработки. В случае если в смарт-контракте будет обнаружена ошибка, то уже будет невозможно как-то поменять и изменить код уже выполняющегося в реальной сети смарт-контракта, его можно будет только аннулировать и разработать новый. Потому тестирование проводят особенно внимательно и максимально подробно, особенно системы, связанные с платежами. Сейчас умные контракты находятся пока что на совсем раннем этапе развития, они постоянно дорабатываются и совершенствуются и, на деле, пока не используют весь свой потенциал [3, с. 11]. На данный момент существует три тестовые сети: Ropsten, Kovan и Rinkeby. Но использование собственной тестовой сети уменьшит время работы.

Сеть Эфириум использует различные алгоритмы консенсуса. Алгоритм Proof of Authority (POA) является относительно новой. В данном алгоритме транзакции проверяются определенным числом узлов, выступающих валидаторами системы. Любой новый узел, который необходимо добавить, должен быть проголосован утвержденным набором узлов. При удалении узла из сети также используется данный консенсус. Таким образом, Proof of Authority предоставляет множество преимуществ для сети: обеспечивает большую конфигурацию с точки зрения времени и задержки, является более безопасным из-за того, как происходит добавление узлов.

Сеть Эфириум имеет следующие компоненты:

- Ethereum Wallet (кошелек).

Ethereum кошелек – это программное обеспечение, которое позволяет хранить и управлять эфиром. С помощью данного кошелька возможно хранить валюту, проводить транзакции и проверять баланс.

- Ethereum Faucet (кран).

Для получения эфира возможно не только заниматься майнингом, но и применять краны эфира. Ethereum faucet – это интернет-ресурс, выдающий пользователям установленную правилами сайта, премию в криптовалюте. Выплата производится через определенные интервалы, от минут до часов.

- Ethereum IDE.

Ethereum IDE – интегрированная среда разработки, которая позволяет писать смарт-контракты на языке программирования контрактов Solidity, а затем развертывать и запускать смарт-контракты. Solidity – самый популярный язык программирования для написания смарт-контрактов Ethereum.

Список литературы / References

1. *Mamaeva N.V., Burkov A.V.* Comparative analysis of the cryptocurrency market // Scientific enquiry in the contemporary world: theoretical basics and innovative approach, 2017. № 11. С. 86–88.
2. *Мамаева Н.В.* Смарт контракты и их особенности // Наука и образование сегодня, 2018. № 2 (25). С. 6–7.
3. *Мамаева Н.В.* Смарт контракты // Наука и образование сегодня, 2018. № 4 (27). С. 11–12.