УДК 004.75

КРИПТОВАЛЮТА. ПРИНЦИП РАБОТЫ ТЕХНОЛОГИИ БЛОКЧЕЙН

Эфендиев Ш. И., Муравьева Э. А., студентки 2 курса факультета информационных систем и технологий
Научный руководитель – Горбоконенко В. Д., доцент
ФГБОУ ВО УлГТУ

Ключевые слова: *Криптовалюта, блокчейн, майнинг, блоки, Биткоин*

Статья посвящена исследованию инновационных цифровых валют – криптовалют. Рассмотрены принципы работы технологии блокчейн в криптовалютной системе Биткойн и механизам управления децентрализованной сети. Представлен разбор механизмов управления, позволяющих повысить уровень доверия к технологии.

Криптовалюта - это децентрализованная валюта с защитой от повторного использования, основанная на достижениях современной криптографии. Идея заключается в том, что каждая транзакция необратима и подтверждается вновь сгенерированными блоками, отвечающими специальным критериям. Блоки рассчитываются всем сообществом, объединяются в цепочку и доступны для просмотра всем как единую база данных. Процедура вычисления блоков - это майнинг [1].

Сеть построена так, что один блок майнится определённое время, независимо от вычислительной мощности — то есть сложность вычислений саморегулируется. В то же время, по мере роста сети, каждый вновь сгенерированный блок также содержит новые монеты. В случае биткоина и некоторых других видов криптовалют количество монет, которые могут находиться в обращении, ограничено на уровне протокола, а количество вновь добытых монет постепенно экспоненциально уменьшается, так что оно никогда не превышает заданного предела. Каждый пользователь, сгенерировавший блок, получает фиксированное вознаграждение, а также комиссию за транзакции, которые он подтвердил, включив их в блок [2]

Технология Биткоин - одно из первых успешных практических решений так называемой проблемы византийских полководцев. Вкратце она формулируется следующим образом: как установить доверие между сторонами, связанными только через канал связи, которому нельзя доверять? Одним из ключевых моментов в решении является криптографический метод proof-of-work- вычисления, которые должны выполняться длительное время, но доказательство того, что они были, должно легко проверяться.

Со временем размер базы данных будет только расти, как и емкость носителей информации. База данных - это блокчейн, цепочка блоков данных в формате JSON. Каждый блок содержит всю информацию, необходимую для работы сети, ее порядковый номер и хэш-сумму предыдущего блока. Естественно, в самом первом блоке такой хэш-суммы нет. К хэшу (шестнадцатеричному числу) предъявляются строгие требования: он должен начинаться с определенного количества нулей, а точнее, быть меньше специального параметра, называемого "битами". Обратно пропорциональный параметр называется сложностью. Этот механизм позволяет надежно хранить все остальные необходимые данные в распределенной сети, потому что, если вы измените хотя бы один символ в блоке, его хэш изменится полностью и все нули мгновенно исчезну

Несмотря на то, что хеш-функция вычисляется по строгому математическому алгоритму, брутфорс (полный перебор) нужный для того, чтобы найти красивый хеш, возможен благодаря параметру nonce (одноразовый код, выбранный случайным или псевдослучайным образом, который используется для безопасной передачи основного пароля, предотвращая атаку повторного воспроизведения). Программа майнера просто перебирает различные значения nonce одно за другим, вычисляет хэш блоки, и если в какой-то момент вам повезет и хэш удовлетворит параметру сложности, то вы получите вознаграждение в виде новых биткоинов и комиссий за все транзакции, входящие в блок [3].

Вывод

Доказательство работы (proof of work) — результат работы, которого трудно достичь, но легко проверить. Работа сети Биткойн основана на этом принципе. Вы можете проверить хэш за долю секунды. И требуется много работы, чтобы получить его.

Как только биткойн попадает на рынок, его стоимость определяется исключительно уровнем доверия к системе. Чем больше люди будут доверять, тем больше они будут покупать Биткойн, тем больше долларов они будут вкладывать в него и, как следствие, тем дороже будет биткойн.

Прежде чем люди смогут доверять Биткоину, они должны знать, обладает ли эта система достаточной степенью безопасности, а также может ли она использоваться в качестве денег. Чтобы узнать это наверняка, нужно вникнуть и понять принципы работы криптовалют.

Библиографический список:

1. Хачатурова Э. А. Блокчейн-технологии: перспективы развития и проблемы правового регулирования / Хачатурова Э. А., Макаревич М.Л. - журнал «Инновационная экономика: перспективы развития и совершенствования», 2018. - С. 25

2. Основные принципы работы самой популярной криптовалюты [Электронный ресурс] / журнал «Хакер», 2014 – Режим доступа: https://xakep.ru/ (дата обращения 23.04.2021).

3. Тестова А. «Криптография в блокчейнах»: о хеш-функциях, ключах и цифровых подписях [Электронный ресурс] / Тестова А. – Сообщество IT специалистов «Хабр», 2017 – Режим доступа: https://habr.com/ (дата обращения 23.04.2021).

CRYPTOCURRENCY. HOW BLOCKCHAIN TECHNOLOGY WORKS

Efendiev S. I., Muravyeva E. A.

Keywords: *Cryptocurrency, blockchain, mining, blocks, Bitcoin*

The article is about innovative digital currencies - cryptocurrencies. It includes review of the principles of the blockchain technology in the Bitcoin cryptocurrency system and the management mechanism of the decentralized network. There is presented the analysis of management mechanisms that allow increasing the level of trust in the technology.