7universum.com
UNIVERSUM:
ТЕХНИЧЕСКИЕ НАУКИ

UNIVERSUM:
ТЕХНИЧЕСКИЕ НАУКИ

Научный журнал
Издается ежемесячно с декабря 2013 года
Является печатной версией сетевого журнала
Universum: технические науки

Выпуск: 10(91)

Октябрь 2021

Часть 1

Москва
2021

УДК 62/64+66/69
ББК 3
U55

U55 Universum: технические науки: научный журнал. – № 10(91). Часть 1. М., Изд. «МЦНО», 2021. – 96 с. – Электрон. версия печ. публ. – *http://7universum.com/ru/tech/archive/category/1091*

ISSN : 2311-5122

DOI: 10.32743/UniTech.2021.91.10-1

Учредитель и издатель: ООО «МЦНО»

ББК 3

Содержание

РАБОТА С КРИПТОВАЛЮТОЙ

Имомова Шафоат Махмудовна
ст. преподаватель,
Бухарский государственный университет,
Республика Узбекистан, г. Бухара
E-mail: evrikiy@list.ru

Норова Фазилот Файзуллоевна
преподаватель,
Бухарский государственный университет,
Республика Узбекистан, г. Бухара

WORK WITH CRYPTOCURRENCY

Shafoat Imomova
Senior Lecturer,
Bukhara State University,
Republic of Uzbekistan, Bukhara

Fazilat Norova
Lecturer,
Bukhara State University,
Republic of Uzbekistan, Bukhara

АННОТАЦИЯ

По мере развития информационных технологий и электронной торговли создаются технологии для снижения затрат, связанных с денежными переводами. Сегодня предприятия готовы внедрять криптографию в бизнес-процесс, а крупные международные банки по всему миру активно изучают, как использовать криптографию и технологии блокчейн. В данной статье рассматривается практика работы с криптовалютами на примере криптовалюты Bitcoin, которая стала очень популярной в криптомире.

ABSTRACT

As information technologies and e-commerce develop, technologies are being created to reduce the costs associated with money transfers. Today, enterprises are ready to introduce cryptography into the business process, and large international banks around the world are actively studying how to use cryptography and blockchain technologies. This article discusses the practice of working with cryptocurrencies on the example of the Bitcoin cryptocurrency, which has become very famous and popular in the crypto world.

Ключевые слова: информационные технологии, криптовалюта, электронная коммерция, сеть, блокчейн-технологии, цифровая подпись, блокчейн, биткойн.

Keywords: information technologies, cryptocurrency, e-commerce, network, blockchain technologies, digital signature, blockchain, bitcoin.

По мере развития Интернета и электронной торговли людям приходилось платить электронными деньгами “дистанционно”. При этом дистанционно передавать деньги из рук в руки практически невозможно. Поэтому в процессе дистанционного перевода денег от одного человека другому придется прибегать к специфическим посредникам, то есть электронным платежным системам, банкам или курьерам. Любой посредник получает какую-то плату за свою транзакцию, процент которой зависит от количества денежных переводов, которые он делает, потому что никто не хочет работать бесплатно. Конечноже, чем больше сумма переводимых денег, тем больше вероятность потерять деньги из-за платежей посреднику. По мере развития информационных технологий и электронной торговли все больше людей задумываются над тем, как сократить расходы, связанные с денежными переводами и вести электронный бизнес, максимально увеличив коэффициент полезного действия денежных переводов на сто процентов?

Рассмотрим практику работы с криптовалютами на примере криптовалюты Bitcoin, которая стала очень известной и популярной в крипто-мире, и опишем ее. Потому что без какой-либо практики было бы намного сложнее понять, как работать в этой, казалось бы, не очень знакомой многим Вселенной. Любой пользователь, подключенный к сети Bitcoin, может сгенерировать в ней свой закрытый ключ, состоящий

Библиографическое описание: Имомова Ш.М., Норова Ф.Ф. РАБОТА С КРИПТОВАЛЮТОЙ // Universum: технические науки : электрон. научн. журн. 2021. 10(91). URL: https://7universum.com/ru/tech/archive/item/12357

из 34 цифр и символов, который является биткойн-адресом, и 64 цифр и символов, которые ему соответствуют. Один из таких биткоин адресов представлен ниже:

12a3rdfgdfhgjkgre4f6zrxter45hdfsfg

Закрытый ключ, соответствующий этому адресу, будет выглядеть следующим образом:

Kwfdg354j Jfshridg2Fl 2 A3 rdfgDfhg Jkgre4f6zrxt er45hdfsf g4cscsfgert176ge4gs

Только владелец того же закрытого ключа может отправлять биткойны с указанного выше адреса. Каждому биткойн-адресу соответствует только один закрытый ключ, и они связаны между собой чрезвычайно сложными математическими формулами. Зная адрес, найти подходящий ему закрытый ключ не представляется возможным ни теоретически, ни практически. Любой пользователь сети Bitcoin может самостоятельно и бесплатно создать любое количество биткойн-адресов и закрытых ключей. Так как вариантов возможных адресов очень много, то вероятность того, что вы дважды сгенерируете один и тот же адрес, практически равна нулю.

Например, участник сети по имени Равшан может отправлять деньги со своего биткойн-адреса на любой биткойн-адрес, не сообщая никому об этом закрытом ключе. Для этого он создает на своем компьютере необходимую транзакцию и подписывает ее закрытым ключом. Перед отправкой этой транзакции в сеть Bitcoin-программа на компьютере Равшана обрабатывает эту информацию с помощью нескольких математических формул и в результате генерирует специальный код, называемый цифровой подписью. Этот процесс будет выполняться автоматически, даже если компьютер пользователя не подключен к сети. Цифровая подпись будет уникальной для конкретной пары транзакций и закрытого ключа и будет выглядеть как подпись на банковском чеке. После этого Равшан отправляет цифровую подпись вместе с транзакцией в сеть Bitcoin. Компьютеры, имеющие открытый ключ цифровой подпис, не смогут найти соответствующий ему закрытый ключ, так как при создании цифровой подписи вычисления производятся с использованием очень сложных математических формул. Используя цифровую подпись Равшана и его биткойн-адрес, можно убедиться, что цифровая подпись была отправлена с использованием закрытого ключа, соответствующего адресу Равшана.

При криптографических операциях транзакции выполняются с обеих сторон: с одной стороны, генерируется цифровая подпись, а с другой стороны проверяется цифровая подпись, т.е открытому ключу должен соответствовать уникальный закрытый ключ. Все узлы сети Bitcoin должны проверять все транзакции, потому что нет другого центрального органа, который бы выполнял эти задачи. Убедившись, что у Равшана есть реальный закрытый биткойн-адрес, компьютерная система проверяет, есть ли деньги, предназначенные для отправки на этот адрес. Для этого узлы сканируют записи всех предыдущих биткойн-транзакций по адресу, указанному Равшаном. Сатоши Накамото, создатель сети Bitcoin, также хорошо понял, что могут возникнуть серьезные проблемы, если узлы записывают транзакции сразу после их получения. Поскольку, когда информация о каждой транзакции поступает на один узел раньше, а позже на другой, могут возникнуть недопонимания по поводу количества биткойнов, хранящихся на каждом адресе. Для решения проблемы сетевой синхронизации Сатоши предложил организовать хитрое соревнование, в котором может участвовать каждый узел сети. Узлы, участвующие в соревновании, собирают самые последние транзакции в списке, называемом блоками. После создания блока используется специальная криптографическая хеш-функция SHA 256. Эта хеш-функция может иметь любое значение и генерирует уникальное 64-битное значение на основе ссылки. Узлы, участвующие в соревновании, пытаются создать блок хеш-функций с некоторым количеством нулей в начале. Например, если условия соревнования требовали найти хеш-функции с пятью нулями в начале, то следующие две хеш-функции могут выиграть:

1) 00000dg4JJfshridg2F12A3rdfgDfhgJkgRe4F 6zrHHTer45HHDfSFg4KskS FgERT176Ge4Gs

2) 00000RT4Ge4GsQ'vfdg354JJfshridg2F12A3 rdfgDfhgJkgRe4F6zrHHTer45HHDfSFg4KskS

После применения хэш-функции невозможно ни теоретически, ни практически заранее узнать, какой блок даст результат с желаемым количеством нулей. SHA 256 и другие подобные хеш-функции всегда дают одинаковые результаты для одних и тех же входных значений. Поэтому каждый участник добавляет случайное число в конец блока. Криптографические хеш-функции разработаны таким образом, что любое малейшее изменение входных данных вызывает случайное изменение всех выходных данных – результата. Если первая попытка хеширования блока узлом не приводит к успеху с необходимыми нулями в хеш-коде, то узел меняет случайное число, добавленное в конец блока, на другое и снова хеширует блок.

Такие попытки повторяются до тех пор, пока не будет найден блок с нужным количеством нулей. Обнаружение такого блока, конечно, является случайностью, но только узел, который может хэшировать блоки быстрее, чем другие, будет иметь больше шансов на победу в соревновании (то есть тот, у кого более современный компьютер и работает быстрее, выиграет соревнование). Это похоже на лотерею: чем больше вы покупаете лотерейных билетов, тем выше ваши шансы получить выигрыш. Количество нулей в начале хеш-функции, которое позволяет выиграть соревнование, варьируется в зависимости от интервала между блоками. Если этот интервал сократится, программное обеспечение биткойнов автоматически изменит условия соревнования. То есть получить желаемый результат сложно - в блоках нужно иметь больше нулей. Если интервал между

блоками больше 10 минут, то сложность задачи снижается.

Узел, который получает желаемый результат и побеждает в соревновании, отправляет полученный блок другим узлам, чтобы указать, что проблема решена. Затем узлы добавляют выигравший блок в свою копию блокчейна вместе с транзакциями в нем. Этот блок будет официальной записью всех транзакций, выполненных с момента добавления предыдущего блока. Если в выигрышном блоке нет некоторых транзакций, отправленных в сеть в предыдущем раунде соревнования, они переходят к следующему раунду. Владелец узла (конкретное лицо или группа людей), нашедший необходимый блок, соответствующий условиям соревнования, получит определенное количество биткойнов в награду. Награда составила 50 биткойн-монет за первые четыре года существования биткойна. Чтобы получить эту награду, каждый участник должен будет добавить дополнительную транзакцию в список обрабатываемых транзакций. Это добавит немного биткойнов к вашей учетной записи. Когда конкретный блок выигрывает в соревновании и добавляется в цепочку блоков, новые биткойн-монеты будут отправлены на адрес, указанный в блоке. Если узел пытается добавить к нему больше биткойнов, чем текущее вознаграждение, то блок не будет распознан другими узлами. Это верно, даже если хэш узла имеет необходимое количество нулей.

Выше была рассмотрена практика работы с криптовалютами на примере криптовалюты биткойн, которая стала очень известной и популярной в мире криптовалют.

Список литературы:

1. Имомова Ш.М., Исмоилова М.Н. Численное решение смешанной задачи, поставленное на векторном волновом уравнении в области с углом // UNIVERSUM: ТЕХНИЧЕСКИЕ НАУКИ. №10(79), 2020. С. 22-25.
3. Имомова Ш.М., Исмоилова М.Н. Вычисление наибольшего собственного значения матрицы и соответствующего ей собственного вектора в среде Mathcad// ACADEMY. № 6(57), 2020. С. 9.
4. Имомова Ш.М., Норова Ф.Ф. Учебные методы организации спортивно-оздоровительных мероприятий в образовательных учреждениях// Вестник науки и образования, 2021. № 9 (112). Часть 2. С. 38.
5. Натаниэль Поппер. Цифровое Золото. Невероятная история биткойна или о том, как идеалисты и бизнесмены изобретают деньги заново, 2016, 350 стр.
6. Филиппов Е. Криптовалюта от А до Я. ST FOREX, 2017.
7. Назаров Ш.Э. Понятие электронной коммерции // Universum: технические науки. 2020. № 9-1 (78). URL: https://cyberleninka.ru/article/n/ponyatie-elektronnoy-kommertsii