ISSN 1609-1817

QazATK

М. ТЫНЫШБАЕВ атындағы
ҚАЗАҚ КӨЛІК ЖӘНЕ КОММУНИКАЦИЯЛАР АКАДЕМИЯСЫНЫҢ

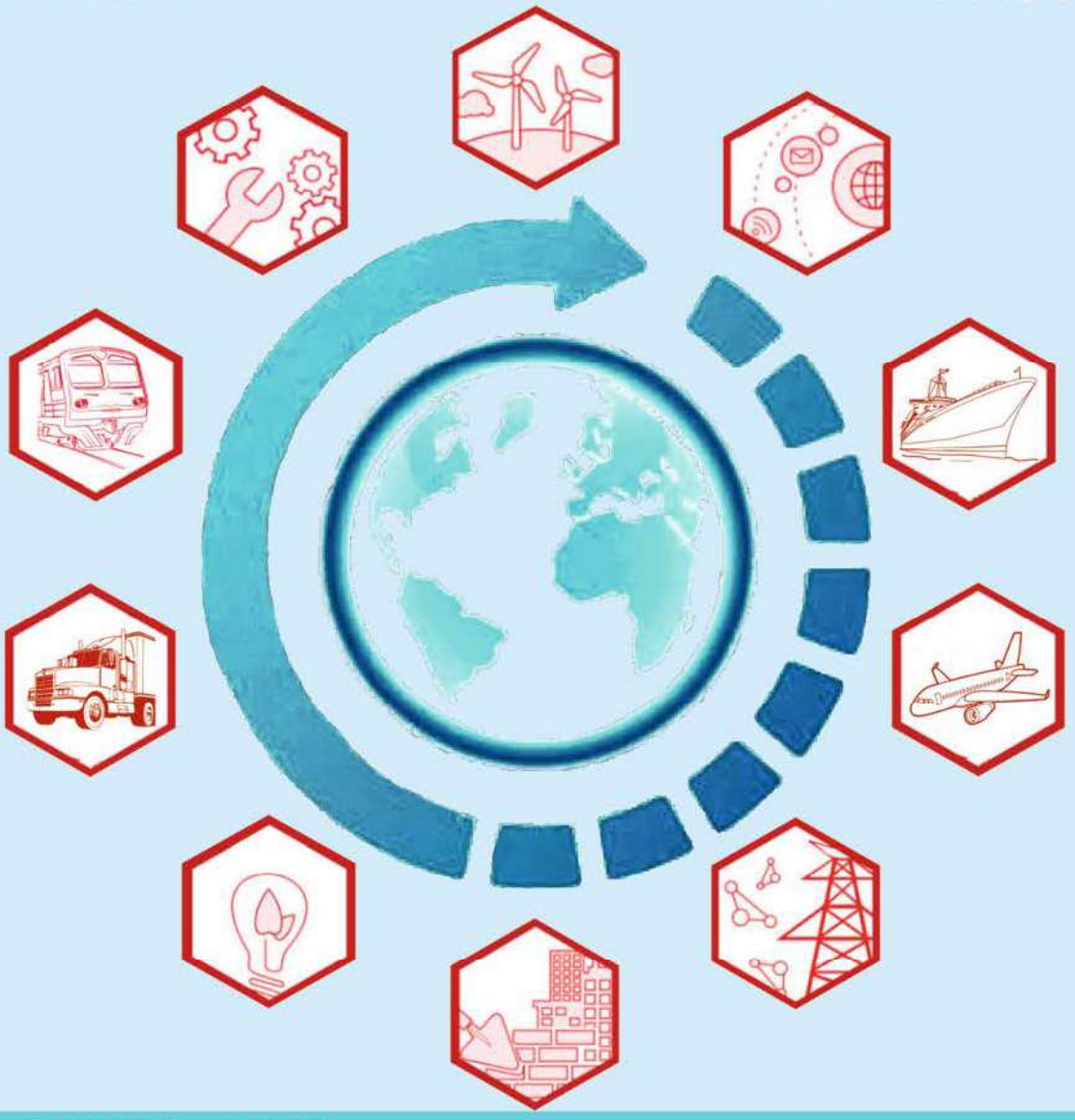
ХАБАРШЫСЫ

ВЕСТНИК

Казахской академии транспорта
и коммуникаций имени
М. Тынышпаева

The BULLETIN

of Kazakh Academy of Transport
and Communications named
after M.Tynyshpayev



№ 3 (110) - 2019

The Bulletin of Kazakh Academy of Transport and Communications named after M. Tynyshpayev
ISSN 1609-1817
Vol. 110, No.3 (2019), pp.208-214

USING BLOCKCHAIN TECHNOLOGY TO DEVELOP APPLICATION TO VERIFY PRODUCTS

Duisebekova Kulanda Seitbekovna, candidate of physical and mathematical Sciences, Associate Professor of «Information system» department, International Information Technologies University, dkulan@mail.ru.

Tukibayev Beibut Aidarovich, master student of the «Information system» department, International Information Technologies University, beibit.tukibaev@gmail.com.

Abstract. In this article, there was considered what blockchain term is and principles of its work. Also there were listed the spheres in which blockchain is widely used around the world nowadays.

Blockchain term was firstly introduced in the paper about bitcoin term, but its usage is not limited with cryptocurrencies and financial sphere. This technology is widely used in such areas as cybersecurity, healthcare, voting, land cadastres etc.

One of the most significant feature that blockchain provided is ability to securely store and share data across the network. There is a number of companies that offer user authentication or verify data verification, such as documents, files, user identities etc.

In this articles there was described process of application development that enables customers to validate certain products' identity. It uses public key infrastructure and cryptographic algorithms to store and append data to blockchain network. In order to add info about some product to blockchain, user has to generate public and private keys, which are interconnected so that information encrypted by public key can only be decrypted by private key. Any data to be added to blockchain contains digital signature, which is based on data content and private key. This signature is then used to validate user's identity.

Another cryptographic component that enables data consistency is hashing algorithm. It used to map data of arbitrary size onto data of a fixed size and allows one to easily verify whether some input data map onto a given hash value. If the input data is unknown, it is difficult to reconstruct it by knowing the stored hash value. This feature provides data immutability, because each block in blockchain network uses previous block's hash.

Key words: blockchain, hash functions, cryptography, public key, private key, digital signature, mining.

УДК 004.031.43.

К.С. Дуйсебекова[1], Б. А. Тукибаев[1]
Международный университет информационных технологий, г. Алматы, Казахстан

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ПРИ РАЗРАБОТКЕ ПРИЛОЖЕНИЯ ДЛЯ ВЕРИФИКАЦИИ ТОВАРОВ

Аннотация. В данной статье рассматривается понятие блокчейн, описывается принцип его работы, а также сферы применения данной технологии.

Впервые блокчейн был предоставлен вместе с биткойном, однако в данный момент сферы его применения не ограничиваются только криптовалютой. Свойство блокчейн безопасно хранить данные позволило создавать платформы для аутентификации и верификации пользователей и данных.

В статье описывается процесс написания приложения для верификации продуктов. С помощью инфраструктуры приватных и публичных ключей, а также криптографических алгоритмов было создано приложение для ввода данных о товаре, которое валидирует данные, а также добавляет их в сеть блокчейн. В свою очередь, мобильное приложение, подключенное к данной сети, позволяет пользователю проверить данные о товаре с помощью его штрих-кода.

Ключевые слова: блокчейн, хеш функции, криптография, публичный ключ, приватный ключ, цифровая подпись, майнинг.

В настоящее время применение технологии блокчейн становится популярным. Хотя о блокчейне начали говорить с появлением такого понятия как биткоин, данная технология находит свое применение в здравоохранении, государственных инициатив, земельном кадастре и других сферах.

Блокчейн (англ. «blockchain», «block» - блок, «chain» - цепь) является выстроенной по определённым правилам непрерывной последовательностью цепочек блоков, которые содержат некие данные. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров, серверов, не зависящих друг от друга. Основной особенностью блокчейна является использование криптографических алгоритмов, которые обеспечивают неподдельность и целостность данных [1].

О блокчейне впервые упоминалось в 2008 году в статье «Биткойн: цифровая пиринговая система платежей» (Bitcoin: A Peer-to-Peer Electronic Cash System) с авторством человека или группы лиц под псевдонимом Satoshi Nakamoto. В статье были описаны принципы построения одноранговой платежной системы с возможностью совершать электронные транзакции между участниками данной системы [2].

Главным преимуществом технологии блокчейна является безопасность осуществляемых транзакций (операций по добавлению данных). Все проводимые транзакции не только прозрачны и подвержены множественному копированию, а также являются объектом подтверждения каждого участника сети. Таким образом, у любого участника процесса имеется возможность просмотреть информацию других транзакций.

Актуальность. Свойство блокчейн хранить неподдельные данные открывает широкий спектр развития различных платформ для аутентификации и верификации.

В 2016 году началась разработка и тестирование первых решений, построенных на открытой платформе Ethereum, которая позволяла обойти ограничения Bitcoin-блокчейна.

Одним из первых решений в области применения блокчейн для верификации был сервис верификаций временных меток Acronis Notary. Технология была реализована в рамках функционала продукта для индивидуальных пользователей Acronis True Image 2017 New Generation. С его помощью можно проверять аутентичность хранящихся в резервных копиях данных. Например, музыканты или художники могут подтверждать дату и время создания своих произведений, предоставляя в качестве доказательства сертификат Acronis Notary с указанием данной информации, наряду с метаданными о самом произведении.

Другим сервисом, также предложенным Acronis Notary, является Acronis ASign. Решение открыло возможность электронного подписания резервных копий документов с автоматической нотаризацией. Пользователи загружают в облако Acronis, подписанные со своей стороны документы и рассылают другим подписантам электронные приглашения. Каждый из подписантов заходит в облако и с помощью специального интерфейса ставит свою электронную подпись на документе. Таким образом, между сторонами «подписывается» своего рода договор, который автоматически фиксируется в блокчейне.

На сегодняшний день существуют ряд решений и применений блокчейн-технологии для создания проектов для верификации продуктов. К примеру, сервис Blockverify предлагает производителям маркировать каждый продукт на этапе производства и поставки,

таким образом, что покупатель, в конечном итоге может проверить подлинность продукции, а также историю перемещений и поставки данного товара. Аналогичный сервис Orygene предоставляет возможность верифицировать товары, документы, а также посылки с помощью мобильного приложения на базе блокчейн.

Разработка. PKI (public-key cryptography) - это криптографическая система, которая использует пару ключей. Публичный ключ используется для распространения, в то время как приватный ключ известен только самому пользователю. Аутентификация данного пользователя проводится с помощью его публичного ключа, а приватный ключ используется для расшифровки данных, зашифрованных публичным ключом [3].

Хеш функцией называется функция, которая преобразует данные произвольного размера в данные фиксированного размера. Результатом хеш функций называются хеши. Такие функции используются для поиска дубликатов в больших базах данных, а также широко используются в криптографии. Криптографические хеш функции позволяют быстро проверить, соответствуют ли входные данные определенному хешу, однако проверить изначальное значение определенного хеша очень сложно. Важной особенностью хеш функций является то, что изменение одного байта входных данных может изменить весь результирующий хеш.

Для усложнения нахождения хешей биткойн и другие криптовалюты, основанные на блокчейне, используют добавочный параметр nonce. Данный параметр является неким числом, используя который требуется получить хеш с определенным свойством. К примеру, в биткойне необходимым условиям нахождения хеша является определенное количество нулей в результате хеш функции.

В блокчейне данные хранятся в блоках, которые, в свою очередь, хранят транзакции (данные). Чтобы добавить новый блок в блокчейн, нужно использовать хеш предыдущего блока. Таким образом, любые изменения данных в предыдущем блоке изменят хеш всего блока, на основе которого был создан следующий блок, что в результате приводит к невалидности всех последующих блоков данных.

Для работы в блокчейн сети пользователи данной системы необходимо сгенерировать публичный и приватные ключи.

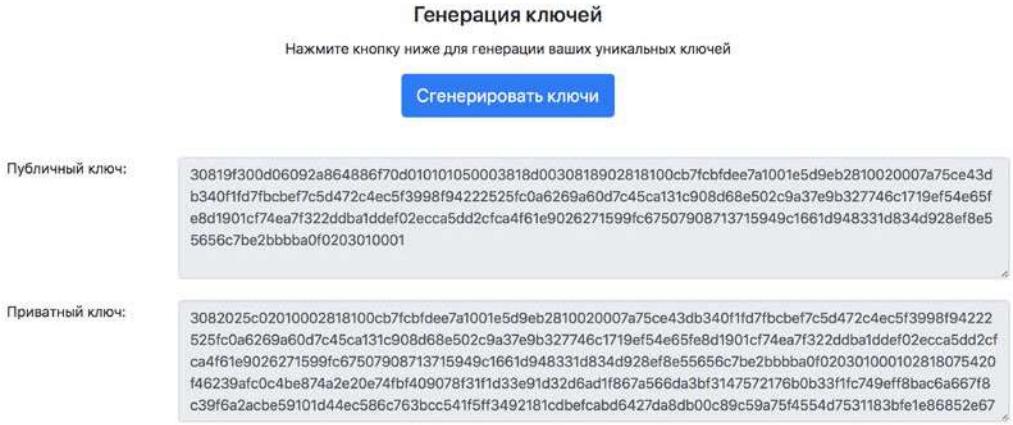


Рис. 1 – Генерация ключей
Fig. 1 – Keys generation

Далее пользователь вводит данные о товаре, а также свои ключи. На данном этапе от пользователя публичный ключ необходим для подтверждения цифровой подписи, которая, в свою очередь, формируется на основе приватного ключа пользователя.

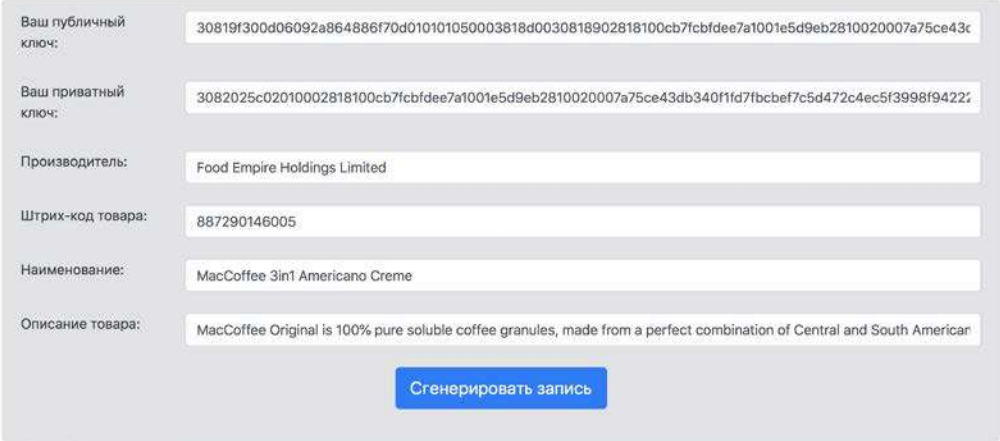


Рис. 2 – Ввод данных о продукте
Fig. 2 – Filling info about the product

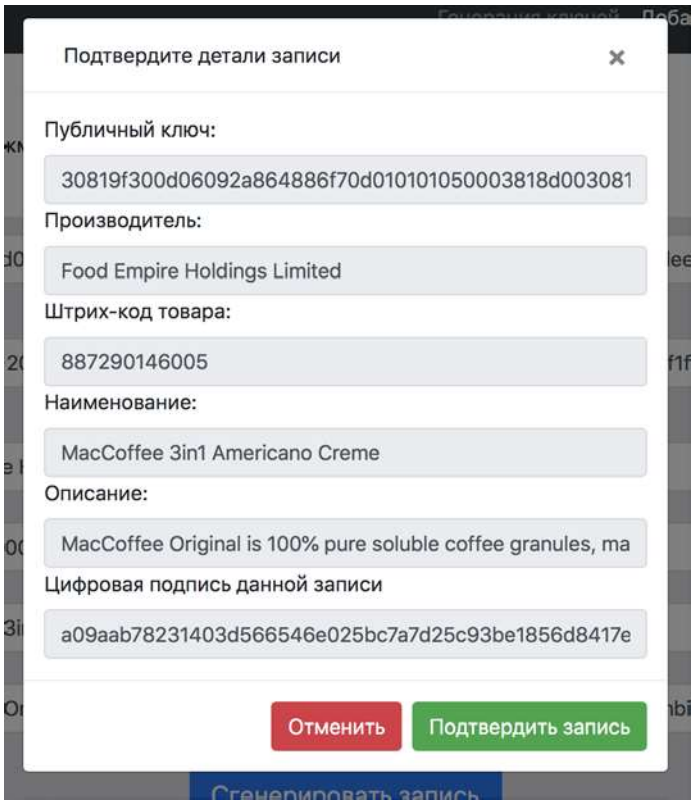


Рис. 3 – Подтверждение данных
Fig. 3 – Data confirmation

Затем формируется цифровая подпись, и наряду с публичным ключом, эти данные отправляются на майнинг. Майнинг - процесс добавления записи в блокчейн. В процессе майнинга производятся проверка валидности цифровой подписи, а также криптографические вычисления для обеспечения безопасности при добавлении записи в сеть блокчейн. Валидация подписи проходит с помощью предоставленного публичного ключа и данных о записи.

В мобильном приложении данного проекта пользователь может отсканировать штрих-код товара и произвести поиск по данном коду по всем записям данной блокчейн сети.

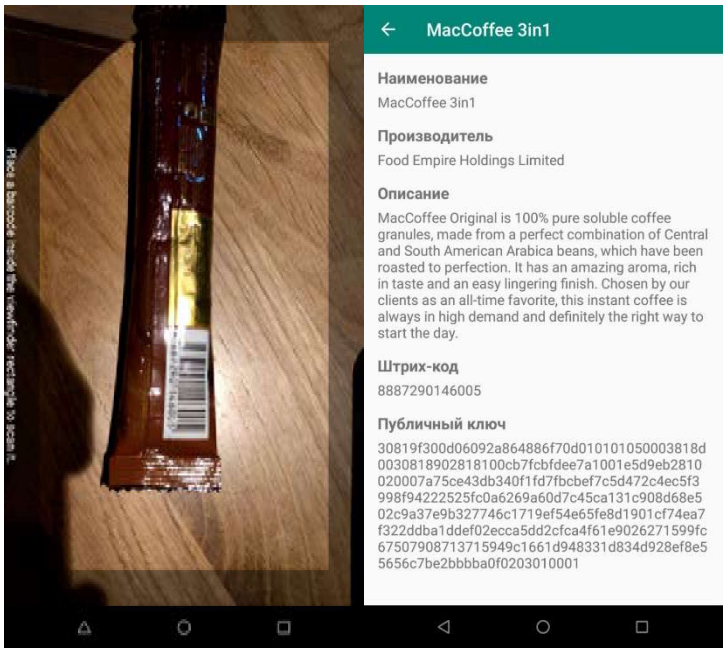
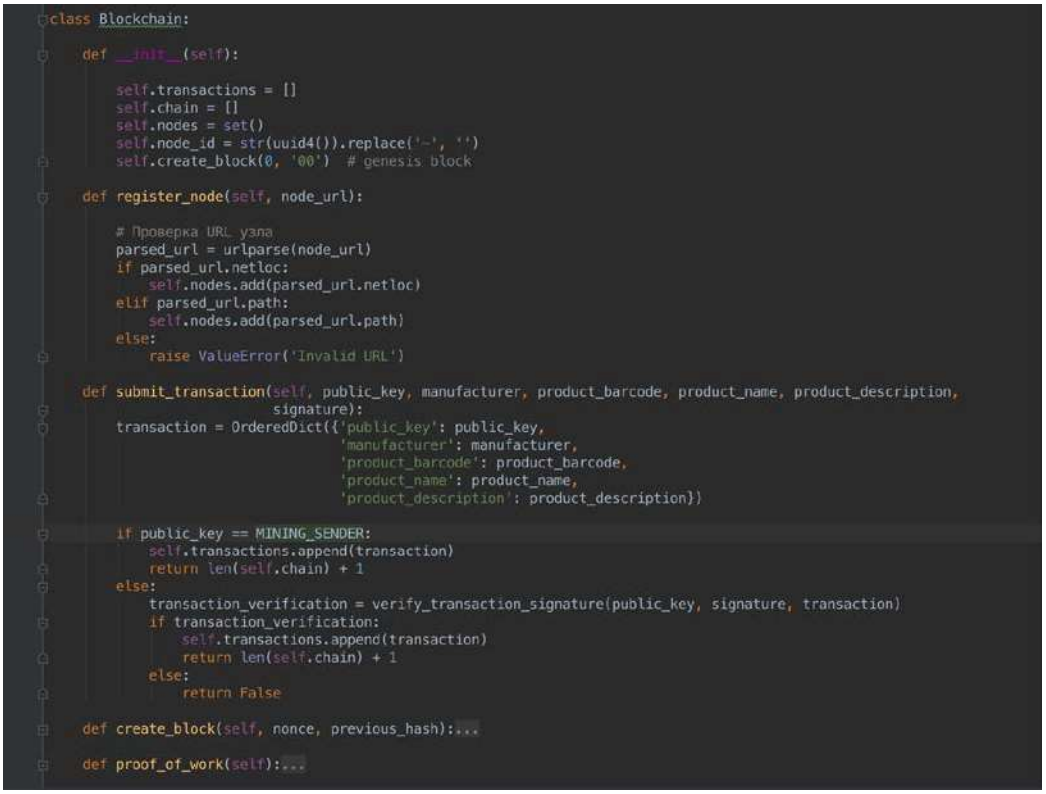


Рис. 4 – Сканирование и информация о продукте
Fig. 4 – Scanning and displaying information about the product

Ниже описывается код основной логики данного проекта на стороне блокчейн.

```python
def verify_transaction_signature(public_key, signature, transaction):
    public_key = RSA.importKey(binascii.unhexlify(public_key))
    verifier = PKCS1_v1_5.new(public_key)
    h = SHA.new(str(transaction).encode('utf8'))
    return verifier.verify(h, binascii.unhexlify(signature))


def hash(block):
    block_string = json.dumps(block, sort_keys=True).encode()
    return hashlib.sha256(block_string).hexdigest()


def valid_proof(transactions, last_hash, nonce, difficulty=MINING_DIFFICULTY):
    # Проверяется, подходит хеш под условия майнинга
    guess = (str(transactions) + str(last_hash) + str(nonce)).encode()
    guess_hash = hashlib.sha256(guess).hexdigest()
    return guess_hash[:difficulty] == '0' * difficulty


def valid_chain(chain):
    # Проверка на валидность блокчейна
    last_block = chain[0]
    current_index = 1

    while current_index < len(chain):
        block = chain[current_index]
        # Проверка хеша блока на корректность
        if block['previous_hash'] != hash(last_block):
            return False

        # Проверка доказательства работы
        transactions = block['transactions'][:-1]
        transaction_elements = ['public_key', 'manufacturer', 'product_barcode', 'product_name', 'product_description',
                                'signature']
        transactions = [OrderedDict((k, transaction[k]) for k in transaction_elements) for transaction in
                        transactions]

        if not valid_proof(transactions, block['previous_hash'], block['nonce'], MINING_DIFFICULTY):
            return False

        last_block = block
        current_index += 1

    return True
```

Рис. 5 – Код логики блокчейн
Fig. 5 – Blockchain logic code



```
class Blockchain:

    def __init__(self):

        self.transactions = []
        self.chain = []
        self.nodes = set()
        self.node_id = str(uuid4()).replace('-', '')
        self.create_block(0, '00')  # genesis block

    def register_node(self, node_url):

        # Проверка URL узла
        parsed_url = urlparse(node_url)
        if parsed_url.netloc:
            self.nodes.add(parsed_url.netloc)
        elif parsed_url.path:
            self.nodes.add(parsed_url.path)
        else:
            raise ValueError('Invalid URL')

    def submit_transaction(self, public_key, manufacturer, product_barcode, product_name, product_description,
                           signature):
        transaction = OrderedDict({'public_key': public_key,
                                   'manufacturer': manufacturer,
                                   'product_barcode': product_barcode,
                                   'product_name': product_name,
                                   'product_description': product_description})

        if public_key == MINING_SENDER:
            self.transactions.append(transaction)
            return len(self.chain) + 1
        else:
            transaction_verification = verify_transaction_signature(public_key, signature, transaction)
            if transaction_verification:
                self.transactions.append(transaction)
                return len(self.chain) + 1
            else:
                return False

    def create_block(self, nonce, previous_hash):...

    def proof_of_work(self):...
```

Рис. 6 – Код логики блокчейн
Fig. 6 – Blockchain logic code

Выводы. В данной статье было дано описание понятия блокчейн, были затронуты его преимущества, а также применение данной технологии в сфере аутентификации и верификации.

В информационный век безопасность и целостность данных играет большую роль. По этой причине, такие преимущества блокчейн как неизменяемость и распределенность данных активно применяются в разных сферах.

В статье описывается техническая сторона функционирования блокчейн на примере разработки приложения для верификации товара. С помощью инфраструктуры приватных и публичных ключей, а также криптографических алгоритмов было разработано мобильное приложение для проверки валидности товаров с использованием технологии блокчейн.

ЛИТЕРАТУРА

[1] Федотова В.В., Емельянов Б.Г., Типнер Л.М. Понятие блокчейн и возможности его использования. // European science №1 (33), 2018. С. 40-41.

[2] Nakamoto S Bitcoin: A Peer-to-Peer Electronic Cash System [electronic resource], 2008. – URL: https://bitcoin.org/bitcoin.pdf.

[3] Albarki A., Alzaid E., Gamdi F., Asiri S., Kar D. Public Key Infrastructure: A Survey // Journal of Information Security, 2015. С. 32-32.

REFERENCES

[1] Fedotova V.V., Emel'yanov B.G., Tipner L.M. *Ponyatie blokchein i vozmoznosty ego ispol'zovany*a. [In Russian: The concept of blockchain and the possibility of its use. // European Science] No. 1 (33), 2018.S. 40-41.

[2] Накамото С. Биткойн: электронная кассовая система [Электронный ресурс], 2008. – URL: https://bitcoin.org/bitcoin.pdf.

[3] Albarqi A., Alzaid E., Ghamdi F., Asiri S., Kar J. Инфраструктура открытых ключей: обзор // Журнал информационной безопасности, 2015. с. 32.