

## КРИПТОВАЛЮТА, РАЗРАБОТКА И ПРИМЕНЕНИЕ

*Шалупаев А. Д.*

*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»  
филиал «Минский радиотехнический колледж», участник Национального детского технопарка  
г. Минск, Республика Беларусь*

*Научный руководитель: Виничук О.Н., преподаватель первой категории дисциплин  
общепрофессионального и специального циклов, м.т.н*

**Аннотация.** На сегодняшний день мы стоим на пороге пятой информационной революции – введение технологий BlockChain в повседневную жизнь. В статье описываются принципы работы одной из технологий BlockChain – криптовалют (токенов), описывается их разработка и сферы применения.

**Ключевые слова:** криптовалюта, токен, BlockChain, распределенные системы, смарт-контракт

**Введение.** В данной статье описаны разработка BlockChain сетей, криптовалют и токенов и сферы их применения. Данная тема очень актуальна в наше время, в особенности в Республике Беларусь, так как Беларусь является первой страной легализовавшей операции с криптовалютами и первой страной, давшей юридическую силу смарт-контрактам. Поэтому на данный момент Республика Беларусь одна из лучших стран для развития и изучения технологий BlockChain.

BlockChain – выстроенная по определенным правилам непрерывная последовательная цепочка блоков, содержащих определенную информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит хеш-сумму предыдущего блока. Изменение любой информации в блоке изменит его хеш-сумму. Чтобы соответствовать правилам построения цепочки, изменения хеш-суммы нужно будет записать в следующий блок, что вызовет изменения уже его собственной хеш-суммы.

Криптовалюта – учёт внутренних расчётных единиц, который обеспечивает децентрализованная сеть BlockChain (нет внутреннего или внешнего администратора или какого-либо его аналога), работающая в полностью автоматическом режиме. Сама по себе криптовалюта не имеет какой-либо материальной или электронной формы – это просто число, обозначающее количество данных расчётных единиц, которое записывается в BlockChain. Все криптовалюты имеют свой собственный BlockChain в который записываются транзакции (запись о переводе криптовалюты со счета на счет).

Токен – это единица учёта, не являющаяся криптовалютой, предназначенная для представления цифрового баланса в некотором активе. Токены представляют собой запись в сети BlockChain. Управление токеном реализуется с помощью смарт-контрактов. Получить доступ к токену можно через специальные приложения, которые используют схемы электронной подписи. Основная часть существующих на сегодняшний день токенов формируется на протоколе BlockChain от Ethereum в соответствии со стандартом ERC-20.

Смарт-контракт – программа, предназначенная для формирования, управления и предоставления информации о владении чем-либо. Чаще всего речь идет о смарт-контрактах в сети BlockChain. В более узком смысле под смарт-контрактом понимается набор функций и данных, находящихся в сети BlockChain.

**Основная часть.** Разработка криптовалюты это сложный процесс, который требует знания принципов работы криптовалют и опыт в программировании на таких языках как C++, Python, Java. Работа криптовалюты основана на технологии BlockChain, поэтому для её разработки необходимо разработать распределенную систему BlockChain.

BlockChain состоит из блоков, блок можно представить в виде JSON-объекта, рисунок 1.

Но так как каждый блок содержит хэш-сумму предыдущего блока, то в первый блок, который называется генозис-блок, мы запишем единицу.

```
def create_block(self, proof, previous_hash, transactions=[]):
    block = {
        "index": len(self.chain) + 1,
        "timestamp": str(datetime.datetime.now()),
        "transactions": transactions,
        "proof": proof,
        "previous_hash": previous_hash
    }
    self.chain.append(block)
    return block
```

Рисунок 1 – Представление технологии BlockChain

Для работы BlockChain необходимо реализовать Proof of Work (PoW). PoW – это майнинг криптовалюты, а именно поиск какого-то числа, которое сложно найти, но легко подтвердить что оно является верным. Это необходимо для безопасности BlockChain. Это число подбирается случайным образом, до тех пор, пока не найдется число, удовлетворяющее каким-то требованиям, например произведение этого числа на доказательство предыдущего блока должно иметь хэш-сумму оканчивающуюся на три нуля. Чем больше нулей, тем безопаснее криптовалюта, но тем дольше проходят транзакции по сети.

После идентификации BlockChain необходимо сделать его децентрализованным (распределенным), если разработка производится на языке программирования Python, то используйте библиотеку PySyncObj. PySyncObj позволяет синхронизировать класс на языке Python с другими компьютерами в сети.

Теперь BlockChain готов, в нем можно совершать транзакции, тем самым переводя криптовалюту со счета на счет. Но в блоки можно записывать не только переводы криптовалюты но и документы, например: документы о приобретении частной собственности или свидетельство о браке. Таким образом BlockChain поможет безопасно хранить документы, создаст новый способ заработка для граждан – майнинг криптовалюты, подтверждая блоки, в которых содержатся документы.

Токены сильно отличаются в разработке, но имеют практически те же функции, что и собственный BlockChain. Разработка токена менее ресурсоемкая чем разработка BlockChain, но при выпуске токена необходимо заплатить за Gas (комиссию сети). Токен работает на основе смарт-контрактов, смарт-контракты имеют большую сферу возможностей, но чаще всего их используют для выпуска токенов. Токен – это доказательство владения чем либо, например криптовалютой.

Разработка смарт-контрактов в основном ведется на языке программирования Solidity, но можно использовать Python при помощи таких библиотек как: web3.py, Ape, Brownie и другие.

Так же необходимо выбрать сеть, в которой будет развернут (добавлен в BlockChain). Самые популярные сети: Ethereum, Binance Smart Chain, Polygon и другие. В разных сетях разная комиссия за запуск смарт-контракта, самая дорогая комиссия в сети Ethereum, но у этой сети больше пользователей и больше людей будут пользоваться разработанным смарт-контрактом.

Смарт-контракты работают по принципу запрос-ответ, для взаимодействия со смарт-контрактом необходимо отправить запрос на адрес в сети BlockChain, где лежит данный смарт-контракт. В смарт-контрактах реализованы функции, которые вызываются, обрабатывая отправленную информацию, после чего смарт-контракт выдает ответ.

Смарт-контракты не уступают BlockChain в своих способностях, но смарт-контракты легче разработать и запустить их работу.

**Заключение.** В ходе написания статьи была изучена заданная предметная область, были получены более глубокие знания в работе технологий BlockChain и разработке криптовалют и смарт-контрактов.

Итогом работы является закрепление полученных теоретических знаний и практических навыков, что помогает развить аналитическое мышление и повышает опыт решения логических задач.

UDC 004.75

## CRYPTOCURRENCY, DEVELOPMENT AND APPLICATION

*Шалунаев А. Д.*

*Educational Institution «Belarusian State University of Informatics and Radioelectronics»  
branch «Minsk Radio Engineering College»  
Minsk, Republic of Belarus*

*Scientific adviser: Vinichuk O. N., teacher of the first category of disciplines of general  
professional and special cycles, m.t.s*

**Annotation.** At the moment we are on the verge of the fifth information revolution — the introduction of BlockChain technologies into everyday life. The article describes the principles of operation of one of the BlockChain technologies – cryptocurrencies (tokens), describes their development and scope.

**Keywords:** cryptocurrency, token, BlockChain, distributed systems, smart-contract