Правительство Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет "Высшая школа экономики"

МИЭМ им. А.Н. Тихонова

Департамент прикладной математики

**ОТЧЕТ**

по курсовой работе по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Выполнил студент гр. СКБ183

Травкин Павел Андреевич

Тема работы: «Технология «блокчейн» - содержание, перспективы применения, проблемы безопасности»

Москва 2020 г.

**Содержание**

[Введение 4](#_Toc39868087)

[Основная часть 5](#_Toc39868088)

[Общее определение 5](#_Toc39868089)

[Техническое определение 5](#_Toc39868090)

[История происхождения технологии «блокчейн» 5](#_Toc39868091)

[Создание и первое применение технологии 5](#_Toc39868092)

[Сеть «Bitcoin» 6](#_Toc39868093)

[Концепция «Proof-of-Work» (PoW) 6](#_Toc39868094)

[Хеширование 7](#_Toc39868095)

[Блокчейн 7](#_Toc39868096)

[Определение 7](#_Toc39868097)

[Реализация технологии в рамках сети «Bitcoin» 7](#_Toc39868098)

[Майнинг 8](#_Toc39868099)

[Обеспеченность криптовалюты, как валюты 8](#_Toc39868100)

[Юридический статус криптовалюты в некоторых странах СНГ 9](#_Toc39868101)

[Перспективы применения технологии «Блокчейн» 10](#_Toc39868102)

[Дальнейшее развитие криптовалют 10](#_Toc39868103)

[Идентификация каких-либо товаров и ресурсов 11](#_Toc39868104)

[Интернет вещей и другие сети 11](#_Toc39868105)

[Энергетическая промышленность 13](#_Toc39868106)

[Проблемы технологии «Блокчейн» 13](#_Toc39868107)

[Проблемы с данными 13](#_Toc39868108)

[Проблемы безопасности 14](#_Toc39868109)

[Реализация технологии «Блокчейн» на языке python3.8 15](#_Toc39868110)

[Хеш-функция 15](#_Toc39868111)

[Алгоритм «Proof-of-Work» 17](#_Toc39868112)

[Криптовалюта и несколько транзакций 17](#_Toc39868113)

[Заключение 18](#_Toc39868114)

[Приложения 19](#_Toc39868115)

[Приложение 1 — hash\_function.py 19](#_Toc39868116)

[Приложение 2 — nickname\_base.txt 20](#_Toc39868117)

[Приложение 3 — transaction\_info.py 23](#_Toc39868118)

[Приложение 4 — PoW\_function.py 23](#_Toc39868119)

[Приложение 5 — blockchain.py 24](#_Toc39868120)

[Приложение 6 — main.py 25](#_Toc39868121)

[Список используемых источников 26](#_Toc39868122)

# Введение

# Основная часть

## Общее определение

«Блокчейн» — это основная технология для реализации криптовалют[[1]](#footnote-1), непрерывная цепочка пронумерованных блоков, содержащих в себе какую-либо информацию, связь между которыми обеспечена не только нумерацией, но и тем, что в каждом последующем блоке хранятся данные о предыдущем.

## Техническое определение

«Блокчейн» — связный список пронумерованных блоков, содержащих какую-либо информацию, собственную хеш-сумму[[2]](#footnote-2) и хеш-сумму предыдущего блока, более подробно технология будет описана далее.

## История происхождения технологии «блокчейн»

### Создание и первое применение технологии

В 1991-ом году учёные-математики Стюарт Хабер и У. Скотт Шторнетта разработали и реализовали систему временны́х штампов для цифровых документов, чтобы составитель файла не мог присвоить данным прошедшую дату. Система представляла из себя цепочку блоков, хранящих цифровой документ, дату внесения файла в систему и информацию о дате внесения в систему предыдущего документа. [2][3]

В 1992-ом году в систему была внедрена концепция деревьев Меркла[[3]](#footnote-3), что позволило собирать несколько документов в один. Это дополнение не принимало никакой роли в работе системы, однако обширно использовалось в последующем при работе с криптовалютой. [4]

### Сеть «Bitcoin»

В 2008-ом году неизвестный человек/группа людей Сатоши Накомото опубликовал статью под названием «Bitcoin: A Peer-to-Peer Electronic Cash System»[5] на сайте «mail-archive.com» в виде белой книги[[4]](#footnote-4). В документе была описана виртуальная валюта «биткоин», которую каждый желающий мог «добыть» и получить вознаграждение по системе «Proof-of-Work», которая будет подробно описана далее.

В 2009-ом году Сатоши Накомото «добыл» первый биткоин-блок и получил вознаграждение в размере пятидесяти биткоинов. Позже, в этом же году, была совершена первая транзакция — Накомото отправил 10 биткоинов американскому программисту Хелу Финни (Гарольд Томас Финни II).

## Концепция «Proof-of-Work» (PoW)

Алгоритм «Proof-of-Work» (алгоритм доказательства проделанной работы) — это криптографическая система, целью которой является защита каких-либо данных от спама и DOS атак. Простыми словами, чтобы получить доступ к данным пользователю необходимо вычислить сложную, но всегда решаемую функцию-ключ, проверить результат которой для системы не составляет большого труда. Например, в качестве функци-ключа используется сложное математическое выражение, даже численное вычисление которого занимает несколько минут, а для проверки достаточно подставить полученное решение вместо неизвестной.

На алгоритме PoW работают многие децентрализованные блокчейн-системы[[5]](#footnote-5), в том числе криптовалюты.

## Хеширование

Хеширование — это процесс превращения некоторых данных в битовую последовательность фиксированной длины (хеш-сумма). Функция, осуществляющая хеширование, называется «хеш-функция».

Необходимые свойства хеш-функции:

1. Работа за линейное время
2. Минимально возможное количество коллизий[[6]](#footnote-6)
3. При изменении одного бита во входных данных, хеш-сумма значительно меняется (необходимо для избегания коллизий, вызванных незначительной ошибкой при передаче данных)

## Блокчейн

### Определение

Блокчейн (цепочка данных) — способ хранения данных, в виде упорядоченного пронумерованного списка блоков, каждый из которых хранит в себе собственною хеш-сумму, хеш-сумму предыдущего блока и какие-либо данные.

### Реализация технологии в рамках сети «Bitcoin»

Сеть «Bitcoin» основана на технологии блокчейн. В качестве данных каждого блока выступают его собственная хеш-сумма, которая должна удовлетворять определённым требованиям системы. На компьютере каждого члена сети хранится полная копия всей цепочки, в которую приблизительно каждые 10 минут добавляется новый блок, защищённый технологией PoW. После создания нового блока, информация о нём поступает всем пользователям и проверяется каждым компьютером, подключённым к сети, отдельно.

Таким образом, чтобы подделать какой-либо старый блок, необходимо пересчитать хеш-суммы всех последующих блоков. Благодаря технологии PoW, такое вычисление занимает более 10-и минут, поэтому «догнать» сеть практически невозможно.

### Майнинг

Майнинг («добыча») — это процесс вычисления хеш-суммы нового блока в сети блокчейн методом перебора параметров хеш-функции. Этот перебор осуществляется до тех пор, пока полученная хеш-сумма не будет удовлетворять внутренним параметрам сети, которые были заданы разработчиками. Например, количество бит в хеш-сумме или степень отличия от предыдущего блока.

Принято считать, что вероятность сгенерировать новый блок первым приблизительно равна соотношению вычислительной мощности майнинг-фермы[[7]](#footnote-7) к суммарной вычислительной мощности всей сети.

На практике майнинг представляет из себя наибольшее возможное число параллельных проверок потенциальных вариантов хеш-суммы нового блока. Для это используются предварительно настроенные графические процессоры (GPU) и специальное программное обеспечение.

### Обеспеченность криптовалюты, как валюты

В отличии от большинства современных валют, криптовалята не является фиатными деньгами[[8]](#footnote-8), а значит напрямую обеспечена лишь доверием плательщиков и желанием последних ей расплачиваться (фиатальными деньгами, которые люди, желающие приобрести криптовалюту, отдают взамен на единицы этой цифровой валюты).[7] Однако, косвенно криптовалюта обеспечивается затратами на его «добычу» (стоимостью износа ресурсов, используемых для майнинга).

### Юридический статус криптовалюты в некоторых странах СНГ

В данной главе будет рассмотрен юридический статус криптовалют в нескольких странах СНГ, подход правительств которых к данному аспекту экономики, наиболее различен.

#### Российская Федерация

В 2014-ом году в Российской Федерации (далее РФ) впервые встал вопрос о легализации криптовалюты, однако Следовательный комитет (далее СК) РФ предложил ввести уголовную ответственность за использование биткоинов в связи с потенциальной возможностью вывода незаконных активов через данный вид валюты.

В 2017-ом году, по указанию Финансовой налоговой службы (далее ФНС) РФ, на Московской бирже была создана специальная платформа для обслуживания цифровых валют.

В 2018-ом году в Государственной Думе (далее ГД) РФ был принят закон «О цифровых финансовых активах», из которого позже, в этом же году, были исключены положения о криптовалюте.

На данный момент криптовалюта не имеет юридического статуса в РФ.

#### Республика Белорусь

В 2017-ом году в правительствен Республики Беларусь (далее РБ) был подписан декрет «О развитии цифровой экономики». [8] Согласно этому документу, физические лица[[9]](#footnote-9) имеют налоговые льготы на операции с криптовалютами до 2023-его года. Любая деятельность, связанная с цифровыми валютами, не считается предпринимательской, и доходы не нуждаются в декларировании. Юридические лица[[10]](#footnote-10), в свой очередь, получили право совершать операции с криптовалютой через операторов обмена.

#### Украина

Весной 2017-ого года глава Совета Национального банка Украины Богран Данилишин заявил, что криптовалюта является лишь денежным суррогатом[[11]](#footnote-11), который не обеспечен реальной стоимостью и не может быть использован, как платёжная единица.

В конце 2017-ого года в Верховной Раде Украины был зарегистрирован законопроект, приравнивающий криптовалюту к программному коду, являющемуся частной собственностью и облагающийся особым налогом.

## Перспективы применения технологии «Блокчейн»

### Дальнейшее развитие криптовалют

Первая и самая очевидная перспектива использования технологии «Блокчейн» — это развитие существующих и создание новых криптовалют. В современном мире, многие люди считают, что некоторые политики и крупные компании лоббируют свои интересы на финансовой бирже, а значит, имеют непосредственную власть над курсом той или иной валюты. Криптовалюта же, в свою очередь, является новой категорией денег, не подвластных государству или какому-либо третьему лицу, как например товарные деньги[[12]](#footnote-12), курс которых контролирует производитель товара. Таким образом, цифровые деньги имеют весьма обширную аудиторию фанатов.

### Идентификация каких-либо товаров и ресурсов

Ещё одной перспективой использования технологии «Блокчейн» является электронная идентификация каких-либо физических объектов. На данный момент существуют коммерческие версии подобных систем. Так, английская IT-компания «EverLedger» ведёт учёт бриллиантов всего мира с помощью блокчейн-системы. Представители лондонского холдинга также предлагают использовать их разработки для учёта премиальных алкогольных напитков. [9]

### Интернет вещей и другие сети

Существует также более глобальная перспектива развития технологии «Блокчейн» — внедрение подобных алгоритмов в интернет вещей[[13]](#footnote-13) и другие электронные сети, такие как Интернет (создание децентрализованных сетей).

В привычной нам централизованной сети, большинство данных хранится на серверах. Там же производится бо́льшая часть вычислений. Схема работы централизованной сети показана на рисунке 1.

Изображение выглядит как часы

Автоматически созданное описание

Рисунок 1 — схема работы централизованной сети

В децентрализованной сети, данные равномерно распределены между всеми пользователями, а вычисления производятся на устройствах, которые нуждаются в результате этих операций. Схема работы децентрализованной сети показана на рисунке 2.

Изображение выглядит как объект, часы

Автоматически созданное описание

Рисунок 2 — схема работы децентрализованной сети

Подобное решение также обеспечивает гораздо бо́льшую конфиденциальность, так как вся личная пользовательская информация храниться исключительно на конкретном устройстве.

### Энергетическая промышленность

Одной их потенциальных сфер использования технологии «Блокчейн» является отслеживание потребления электроэнергии. Учёные бельгийской компании «Scanergy» в 2018-ом представили работу под названием «The Transformation of the European Energy Industry through Digitalisation». [10] В документе подробно описана система учёта затраченного электричества. В качестве членов сети выступают счётчики электроэнергии.

## Проблемы технологии «Блокчейн»

Как и у любой технологии, у блокчейна существуют проблемы. Некоторые из них не решены на данный момент в виду малой распространённости технологии, другие ожидают блокчейн-системы в будущем.

### Проблемы с данными

#### Хранение данных

Одна из проблем, ожидающая блокчейн-системы — переполнение данными. В отличие от централизованных систем, в децентрализованных все данные системы хранятся одновременно на всех устройствах, а значит максимальное возможное количество информации, хранящейся в системе, ограничено памятью самого невместительного устройства системы.

Некоторые пользователи блокчейн-систем решают эту проблему, неравномерно распределяя данные по устройствам, но это нарушает концепцию децентрализованной сети.

#### Скорость доступа к данным

Ещё одна проблема, с которой по прогнозам экспертов предстоит встретиться блокчейну, это низкая скорость доступа к данным, содержащимся в длинных цепочках.

Со временем в блокчейнах накапливаться очень большие объёмы данных, тогда для доступа к последним можно использовать по крайней мере для способа: изменять тип контейнера[[14]](#footnote-14), так как поиск по односвязному списку[[15]](#footnote-15) (каким и является блокчейн) возможен только перебором всех элементов, либо копировать данные из цепочки в контейнер с произвольным доступом[[16]](#footnote-16), что является прямой угрозой безопасности информации, так как она более не защищена от копирования.

### Проблемы безопасности

Как таковых проблем с безопасностью у блокчейна пока не выявлено, но можно представить несколько специфических ситуаций.

#### Полный контроль злоумышленника над сетью

В случае блокчейна с маленьким количеством пользователей, например цепочка для учёта каких-либо корпоративных данных небольшой компании, возможна следующая ситуация: злоумышленник взломал и удалённо контролирует все устройства, подключённые к блокчейну, а значит преступник может внести свой собственный блок в систему, изменив алгоритм PoW сразу на всех устройствах.

#### Перехват и изменение пакетов

Также, в случае работы блокчейна через беспроводные сети, возможен перехват и изменение каких-либо пакетов. Например, злоумышленник может не давать некоторым устройствам отправлять их «согласие» на создание нового блока после проверки подлинности проделанной работы.

## Реализация технологии «Блокчейн» на языке python3.8

В этой главе будет подробно разобран прстой пример реализации криптовалюты на базе технологии «Блокчейн» на языке python3.8.

### Хеш-функция

В данной реализации приведена авторская хеш-функция. Она предназначена исключительно для демонстрации, вследствие чего, не является примером какой-либо хорошо защищённой от коллизий.

Длина хеш-суммы данной функции равна длине кодовой фразы (в данном случае это «primitive example of hash function by Pavel Travkin») и представляет из себя комбинацию побитовых операций, посимвольно применяемых к шифруемой информации и кодовой фразе.

#### Случай 1. Длина информации меньше или ровна длине кодовой фразы

В начале своей работы функция считает коэффициент, позволяющий значительно изменять хеш-сумму при незначительном изменении информации. ASCII-коды всех символов информации складываются, затем, в случае кратности суммарной длины длине алфавита хеш-суммы (латинские буквы верхнего и нижнего регистров и арабские цифры), из полученного числа вычитается единица (во избежание равенства коэффициента нулю).

Следящий шаг — формирование хеш-суммы. Он происходит в 2 этапа: 1. Увеличение информации до размера кодовой фразы, как показано в таблице

|  |  |
| --- | --- |
| Информация | information |
| Кодовая фраза | primitive example of hash function by Pavel Travkin |
| Дополненная информация | informationinformationinformationinformationinform |

Таблица 1 — способ расширения информации

2. Преобразование дополненной информации для значительного изменения хеш-суммы в случае незначительного изменения данных, и сопоставление полученного числа символу из алфавита. В таблице 2 показан пример данного алгоритма для одного символ информации.

|  |  |
| --- | --- |
| ASCII-код i-ого символа кодовой фразы | 112 |
| ASCII-код i-ого символа расширенной информации | 103 |
| Результат конъюнкции ASCII-кодов первых символов | 96 |
| Наше число, домноженное на коэффициент | 54048 |
| Остаток от деления полученного числа на длину алфавита | 46 |
| Символ хеш-суммы | ‘i’ |

Таблица 2 — подсчёт i-ого символа хеш-суммы

Затем, таким же способом подсчитываются все остальные символы хеш-суммы.

#### Случай 2. Длина информации превосходит длину кодовой фразы

В случае, когда размер информации превосходит размер кодовой фразы, иначе формируется коэффициент. А именно, от является суммой ASCII-кодов символов, номер которых в строке информации превосходит количество символов кодовой фразы.

При подсчёте посимвольной конъюнкции в качестве информации выступает первая её часть, равная по размеру кодовой фразе.

Реализация данной части системы продемонстрирована в приложении 1.

### Алгоритм «Proof-of-Work»

В данной реализации в качестве задачи PoW выступает поиск целого числа, являющегося значением многочлена от номера операции, методом перебора всех чисел от нуля. Система, в свою очередь, гарантирует существование ответа.

В качестве функции для разрешения взят многочлен

Для создания нового блока необходимо подобрать такое число, которое является решением данного многочлена при равном номеру транзакции.

Реализация данной части системы продемонстрирована в приложении 4.

### Криптовалюта и несколько транзакций

В приложении 5 представлена реализация блокчейна, хеш-функция и алгоритм PoW которой, был описан выше.

В приложении 6 продемонстрировано 40 случайных транзакции между виртуальными пользователями (никнеймы взяты из приложения 2).

# Заключение

# Приложения

## Приложение 1 — hash\_function.py

def hasher(str\_data):

alphabet = []

for i in range(48, 58):

alphabet.append(chr(i))

for i in range(65, 91):

alphabet.append(chr(i))

for i in range(97, 123):

alphabet.append(chr(i))

hash\_sum = "primitive example of hash function by Pavel Travkin"

result = ""

if len(str\_data) <= len(hash\_sum):

k = 0

for i in range(len(str\_data)):

k += ord(str\_data[i])

if k % (26 \* 2 + 10) == 0:

k -= 1

for i in range(len(hash\_sum)):

result += alphabet[(((ord(hash\_sum[i]) & ord(str\_data[i % len(str\_data)])) \* k) % (26 \* 2 + 10))]

else:

k = 0

for i in range(len(str\_data) - len(hash\_sum), len(str\_data)):

k += ord(str\_data[i])

if k % (26 \* 2 + 10) == 0:

k -= 1

for i in range(len(hash\_sum)):

result += alphabet[(((ord(hash\_sum[i]) & ord(str\_data[i])) \* k) % (26 \* 2 + 10))]

return result

## Приложение 2 — nickname\_base.txt

Randomizzze

Molodoy\_granit

Pelmeshek

Hodychii\_Mertvezz

Mr.Toretto

Zhivuchii

Vezunchikk

Castieeeel

Crazyman

Dilan

SuperGopnik

Pensioner

Tihaya\_gavan

Rozhdennyi\_v\_SSSR

Dzhentelman

Garfild

Hell\_Boy

Seeker\_of\_Truth

Tom\_Cat

Sedoy

\_Boolldozer\_

Light\_of\_Heaven

Shepard

Avtoritet

Sedrik

Brodyaga

Freeloader

Mordekai

Rastaman

Russkii\_Knyazzz

Znatok\_Lubvii

Mudryi\_Tigr

Viking

Harley.Davidson

Petrovich

Bad\_boy

Leningrad

Psichopat

Faraooon

Pryanik

Zapoinyi

Doberman

Kot\_begemot

Benediktovich

Scorpion

Hudozhnik

Major

Gospodin\_Bezymyannyi

Chernyi\_Bumer

Poseidon

Agressor

Gerakl

Illusionist

Improvise

Koluchii\_chemodan

Zloy\_kaktus

Kakoi\_to\_tip

Kirieshka

Psih\_is\_ada

Napaleon\_v\_trusah

Beshenyi\_orbit

Divnyi\_zezar

## Приложение 3 — transaction\_info.py

import random

class Transaction:

def \_\_init\_\_(self, sender, recipient, amount):

self.sender = sender

self.recipient = recipient

self.amount = amount

def data\_generate():

sender\_number = random.randint(1, 62)

recipient\_number = random.randint(1, 62)

while recipient\_number == sender\_number:

recipient\_number = random.randint(1, 62)

with open("nickname\_base.txt", "r") as f:

for i in range(sender\_number):

f.readline()

sender = f.readline()

with open("nickname\_base.txt", "r") as f:

for i in range(recipient\_number):

f.readline()

recipient = f.readline()

amount = random.randint(1, 100)

return [sender[:len(sender) - 1], recipient[:len(recipient) - 1], amount]

def transaction\_generate():

data = data\_generate()

return Transaction(data[0], data[1], data[2])

## Приложение 4 — PoW\_function.py

def math\_func(a):

return (a - 3) \*\* 5 - (a - 1) \*\* 3 + 40

def PoW(guess, PoW\_number):

if guess == math\_func(PoW\_number):

return True

else:

return False

## Приложение 5 — blockchain.py

import hash\_function

import transaction\_info

import datetime

import PoW\_function as PoW

class Block:

def \_\_init\_\_(self, counter, time, data, previous\_hash):

self.counter = counter

self.time = time

self.data = transaction\_info.transaction\_generate()

self.previous\_hash = previous\_hash

self.hash = self.hash\_block()

def hash\_block(self):

return hash\_function.hasher(str(self.counter) + str(self.time) + self.data.sender + self.data.recipient + str(self.data.amount) + self.previous\_hash)

def create\_genesis\_block():

return Block(1, datetime.datetime.now(), "Genesis Block", "")

def new\_block(last\_block):

i = 0

while not PoW.PoW(i, last\_block.counter):

i += 1

this\_counter = last\_block.counter + 1

this\_time = datetime.datetime.now()

this\_data = last\_block.data.sender + " send " + str(last\_block.data.amount) + " COINs to " + last\_block.data.recipient

this\_hash = last\_block.hash

return Block(this\_counter, this\_time, this\_data, this\_hash)

## Приложение 6 — main.py

import blockchain as bc

blockchain = [bc.create\_genesis\_block()]

previous\_block = blockchain[0]

num\_of\_blocks = 40

for i in range(0, num\_of\_blocks):

current\_block = bc.new\_block(previous\_block)

blockchain.append(current\_block)

previous\_block = current\_block

print("Block " + str(current\_block.counter) + " has been added\n")

print("Transactoin info:")

print("Sender - " + current\_block.data.sender)

print("Recipient - " + current\_block.data.recipient)

print("Amount of transaction - " + str(current\_block.data.amount))

print("\nHash - " + current\_block.hash + "\n\n\n")

# Список используемых источников

1. К вопросу о коллективных валютах или частных деньгах [Книга] / авт. Рисс Владислав Игоревич. - Пенза : "Наука и Просвещение" (ИП Гуляев Г.Ю.) , 2017.
2. Bitcoin and cryptocurrency technologies: a comprehensive introduction. [Книга] / авт. Narayanan Arvind [и др.]. - Princeton : Princeton University Press., 2016.
3. How to time-stamp a digital document [Книга] / авт. Haber Stuart и Stornetta W. Scott. - [б.м.] : Journal of Cryptology, 1991.
4. Improving the Efficiency and Reliability of Digital Time-Stamping [Книга] / авт. Bayer Dave, Haber Stuart и Stornetta W. Scott. - [б.м.] : CiteSeerX, 1992.
5. Bitcoin: A Peer-to-Peer Electronic Cash System [Книга] / авт. Nakamoto Satoshi. - 2008.
6. Writing White Papers: How to capture readers and keep them engaged [Книга] / авт. Stelzner Michael. - Poway : WhitePaperSource Publishing, 2006. - стр. 214.
7. ФИАТНЫЕ ДЕНЬГИ Аналитическая записка [В Интернете] / авт. Грищенко В. // Банк России. - Банк России, Август 2019 г.. - 1 Май 2020 г.. - <https://www.cbr.ru/Content/Document/File/79860/analytic_note_20190829_ddkp.pdf>.
8. dev by [В Интернете] / авт. Сергеенко Елена // decree\_mediakit\_ru. - 2017 г.. - 2 май 2020 г.. - <https://media.dev.by/decree_mediakit_ru.pdf>.
9. Экономика науки [Книга] / авт. Цветкова Л. А.. - Москва : Центр научно-технической экспертизы ИПЭИ РАНХиГС при Президенте РФ, 2017. - Т. III : стр. 278.
10. The Transformation of the European Energy Industry through Digitalisation [В Интернете] / авт. Nikolaus Mag. Dr. // ssc-rechtswissenschaften.univie.ac.. - Department of Innovation and Digitalisation in Law, Faculty of Law, 7 Январь 2018 г.. - 2 Май 2020 г.. - https://ssc -rechtswissenschaften.univie.ac.at/fileadmin/user\_upload/s\_rechtswissenschaft\_neu/Neu\_Versuch/Doktorat\_Expose/Expose1/Rechtsinformatik/The\_Transformation\_of\_the\_European\_Energy\_Industry\_through\_Digitalisation.pdf.

1. Криптовалюта — цифровая валюта, обеспечивающаяся автоматической децентрализованной платёжной системой (нет внутреннего и внешнего админестраторов). [1] [↑](#footnote-ref-1)
2. Хеш-сумма (хеш-код) — результат применения хеш-функции к каким-либо данным. [↑](#footnote-ref-2)
3. Дерево Меркла (дерево хешей) — полное двоичное дерево, в каждой вершине которого хранится хеш, построенный на базе хешей дочерних листовых вершин. [↑](#footnote-ref-3)
4. Белая книга (white paper) — официальное сообщение в письменном виде.[6] [↑](#footnote-ref-4)
5. Децентрализованная система (децентрализованная сеть) — это компьютерная сеть, где все пользователи имеют одинаковое количество прав, а все данные равномерно распределены между компьютерами членов сети. [↑](#footnote-ref-5)
6. Коллизия при хешировании — факт совпадения хеш-сумм для разных наборов данных, подвергнутых хешированию (если данных больше, чем возможных значений хеш-суммы, коллизии неизбежны) [↑](#footnote-ref-6)
7. Майнинг-ферма — это машина, вся вычислительная мощность которой направлена на майнинг. [↑](#footnote-ref-7)
8. Фиатные деньги — это деньги, стоимость которых установлена и гарантирована государством. [↑](#footnote-ref-8)
9. Физическое лицо — это гражданин Российской Федерации, иностранного государства либо лицо без гражданства, наделённое правами и обязанностями в силу самого факта существования. Иными словами, физическое лицо — это человек, который выступает в качестве субъекта правоотношений. [↑](#footnote-ref-9)
10. Юридическое лицо — это зарегистрированная в установленном законом порядке организация, фирма, компания, которая имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде. [↑](#footnote-ref-10)
11. Денежный суррогат — заменитель законного платёжного средства, такой как ценные бумаги, депозиты либо какие-либо запрещённые инструменты денежного обращения. [↑](#footnote-ref-11)
12. Товарные деньги — это деньги, в роли которых выступает какой-либо реальный товар, такой как драгоценные металлы. [↑](#footnote-ref-12)
13. Интернет вещей — это концепция вычислительной сети, включающей в себя несколько физических электронных устройств, каждое из которых принимает участие в равной степени в вычислениях для решения задачи, поставленной перед сетью. Также подобная система обязательно работает без участия человека. Пример: система «Умный дом». [↑](#footnote-ref-13)
14. Контейнер — это какая-либо структура данных, позволяющая хранить набор однотипных материалов. [↑](#footnote-ref-14)
15. Односвязный список — это контейнер, каждый элемент которого хранит какие-либо данные и позволяет перейти к следующему по порядку элементу. [↑](#footnote-ref-15)
16. Контейнер с произвольным доступом — это контейнер, который даёт пользователю возможность перейти к любым, содержащимся в нём, данным. [↑](#footnote-ref-16)