МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КОМИ

ГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ВОРКУТИНСКИЙ ПОЛИТЕХНИЧЕСКИЙ
ТЕХНИКУМ»

Индивидуальный проект по информатике на тему: «Электронные денежные системы. Криптовалюта»

Выполнила
студентка группы ПРУМ-22
Кузьмичева Т.А.

Преподаватель
Гейн П.В.

г. Воркута
2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ …… 3

ГЛАВА 1. История создания и развития криптовалют. …… 4

1.1. Предпосылки развития криптовалют. …… 4

1.2. Рождение и становление критовалюты Bitcoin. …… 5

ГЛАВА 2. Принцип работы криптовалют. …….. 8

2.1. Система prof-of-work. ……... 8

2.2. Хеширование SHA-256. …… 9

2.3. Транзакции. …… 11

2.4. Блокчейн. …… 12

2.5. Сложность. …… 13

2.6. Майннг. ……... 14

ГЛАВА 3. Основные «плюсы» и «минусы» криптовалют на примере Bitcoin. …….. 16

ГЛАВА 4. Роль криптовалют в современном мире экономики. …….. 19

ЗАКЛЮЧЕНИЕ …… 23

Список используемой литературы …… 24

ВВЕДЕНИЕ

Современный мир с каждым днём развивается всё больше, а, следовательно, всё изменяется в обычной жизни и деньги тоже приобретают новое значение. В интернете и даже по телевиденью все чаще можно услышать о новой виртуальной криптовалюте - **BitCoin** (Биткоин). Некоторые утверждают, что это валюта будущего. Другие, напротив, считают, что у неё нет будущего. И я решила узнать - Что это такое? Имеет ли криптовалюта будущее? И нужна ли она вообще?

На данный момент информации о биткоинах не очень много из-за того, что пока мало кто знает про них, но ее популярность быстро набирает обороты.

В этой работе я постараюсь рассказать на доступном языке, что такое ***биткоин***, как его можно добыть и конечно, рассмотреть другие вопросы связанные с этим.

Актуальность: Сегодня Bitcoin - современная цифровая валюта, которая прекрасно подходит для расчётов в сети Интернет. Простота и удобство открытия счета в биткойнах сегодня привлекают к этой цифровой валюте всё больше людей из развивающихся стран.

Гипотеза: Криптовалюта – деньги будущего и на мой взгляд она может использоваться в будущем наравне с другой «реальной» валютой.

Целью работы является выяснение вопроса, что такое криптовалюта и как работает биткоин?

Задачи:

1. Узнать историю создания и развития криптовалют.
2. Выяснить, что такое криптовалюта.
3. Понять принцип работы криптовалют.
4. Определить преимущества и недостатки криптовалюты.
5. Выявить роль криптовалют в мире экономики.

Объект исследования – Bitcoin (биткоин).

Метод исследования – поисково-аналитический.

ГЛАВА 1

1.1. Предпосылки развития криптовалют.

Еще в 60-х годах прошлого столетия профессиональные криптографы обсуждали возможность создания глобальной информационной сети. Первые практические шаги в этом направлении были сделаны в 80-е. При помощи инфосети начали производить обмен брокерскими данными, которые были нужны для торговли на биржах.

В это же время появилась идея цифровых денег. Основная ценность концепции сводилась к возможности быстрой покупки акций, различных финансовых активов и их деривативов.

В то время над реализацией идеи электронных денег работали американские криптографы Дэвид Чаум и Стефан Брэндс. Они описали принципы работы анонимной системы цифровых платежей, а также предложили первые протоколы «электронной наличности». В 1990 году Дэвид и Стефан создали компанию DigiCash, которая специализировалась на разработке и внедрении денежной системы eCash. У нее была функция поддержки конфиденциальности электронных платежей и присутствовала криптографическая защита данных.

Основным отличием eCash от современных криптовалют было централизованное управление. В 1998 году эта платформа обанкротилась. Но сама идея использования быстрых анонимных платежей была замечена многими шифропанками.

Немалый вклад в становление криптовалюты сделал Адам Баков. Именно он в 1997 году применил HashCash – технологию, устойчивую к спаму и DoS-атакам. Позже ее усовершенствованием занялся Хэл Финни. Ему удалось создать более совершенный алгоритм контроля электронных платежей. Суть улучшения сводилась к внедрению цепочки из хэш-блоков в работу с транзакциями.

Технология HashCash стала одной из ключевых концепций в процессе создания первого блокчейна. На ее основе в 1998 году двое разработчиков независимо друг от друга запустили свои цифровые проекты:

1. Вэй Дай – проект B-money.
2. Ник Сабо – проект Bit-Gold.

Каждый из них в качестве базы для работы системы использовал децентрализованный реестр. Фактически эти проекты Вэя и Ника стали прототипами криптовалюты. Позже Сатоши Накамото сошлется на B-money как на основополагающую технологию для разработки Bitcoin. Первая цепочка блоков была создана Хэлом Финни в 1998 году, а через некоторое время он тоже присоединится к проекту Bitcoin.

Таким образом, технология blockchain и криптовалюта – это результат усилий группы людей. Но финальный шаг в реализации идеи цифровых денег сделал анонимный разработчик под псевдонимом Сатоши Накамото (Satoshi Nakamoto).

1.1. Рождение и становление криптовалюты Bitcoin.

Кто именно скрывается под именем Satoshi Nakamoto — до сих пор достоверно не известно. Есть мнение, что этот псевдоним использовала целая группа специалистов. Все началось в 2007 году с формирования идеи децентрализованной цепочки блоков blockchain и криптовалюты биткоин версии 1.0.

Весь путь развития биткоина можно разделить на отдельные этапы.

2007 год.

В это время Сатоши начал работать над принципами построения распределенной сети — то есть системы без центрального управления.

2008 год.

Неизвестный человек или группа лиц под псевдонимом Satoshi Nakamoto опубликовали текстовый файл White Paper, в котором рассказали о том, что такое биткоин. В документе содержалось описание работы

цифровой платежной системы, а также информация о ключевых особенностях блокчейна и биткоина.

2009 год.

В январе этого года была произведена разработка первых клиентов Bitcoin 0.1/0.1.0/0.1.5.

После генерации начального блока «Genesis 0» были получены первые 50 BTC. Вскоре разработчики криптовалюты произвели тестовую транзакцию: Сатоши отправил 10 BTC другому участнику сети и тот их успешно получил. Презентованная в январе 2009 года версия блокчейна могла работать только на Windows 2000, Windows NT и Windows XP. Поэтому сразу после релиза первого клиента создатели этой технологии занялись доработкой блокчейна. В сентябре 2009 года впервые была выполнена покупка биткоина за фиатную валюту. Сумма сделки составила 5,02 USD. За эти деньги Марти Малми продал пользователю NewLibertyStandard 5050 BTC. Доллары были перечислены на счет в PayPal.

В ноябре 2009 года разработчики биткоина решили создать портал bitcoin.org. Сайт быстро привлек внимание тех, кто был заинтересован в криптовалюте. На площадку приходило много людей, то есть сформировалось первое криптосообщество. Чуть позже на базе этого портала был запущен форум Bitcointalk.org. Он сыграл одну из ключевых ролей в популяризации биткоина и дальнейшего развития сообщества.

В декабре 2009 года был выпущен клиент Bitcoin 0.2, который мог функционировать уже и на Linux. Новая версия децентрализованной сети позволяла запускать процесс генерации блоков несколькими параллельными потоками. Такое обновление ощутимо повысило эффективность майнинга. Поскольку добывать монеты стало проще, майнить криптоденьги массово начали обычные пользователи. Это привело к быстрому росту биткоин-сообщества. В этот же период разработчики приступили к реализации API-интерфейса JSON RPC. А сообщество, объединенное идеей криптовалюты, начало активно участвовать в разработке биткоина.

2010 год.

Летом этого года был выпущен Bitcoin 0.3. Сложность майнинга возросла. Но популяризация биткоина сделала свое дело – количество пользователей, добывающих криптомонеты, стремительно росло.

Из-за усложнения добычи разработчики посоветовали майнерам использовать видеокарты для ускорения вычислений. Пользователь под ником ArtForz оценил эту идею и решил создать первую криптоферму.

В августе 2010 года был обнаружен серьезный баг системы. Суть проблемы сводилась к тому, что перед добавлением сделок в блокчейн не проводился их анализ. Выявив это слабое место, неизвестные злоумышленники 15 августа произвели атаку на систему. Им удалось сгенерировать в одной транзакции 184 млрд монет и отправить их на 2 адреса.

Разработчики быстро исправили баг системы и отменили хакерскую транзакцию. Но пользователи были неприятно удивлены такой уязвимостью. Чтобы подобные истории не повторялись, сеть была переведена на новую версию протокола. Больше проблем с хакерами не возникало.

В ноябре 2010 года сформировался первый майнинг-пул под названием Slush’s Pool. Его появление было логичным, поскольку конкуренция в сфере добычи биткоинов постоянно росла. Обычным пользователям стало легче объединять усилия для генерации блоков сети. Так добыча монет становилась более реальной задачей, в сравнении с майнингом при помощи одного ПК. Впоследствии пулы стали популярны за счет обеспечения стабильного дохода от добычи криптовалюты.

В конце 2010 года была выпущена финальная версия клиента Bitcoin (0.3.9). В это же время человек (или команда людей), скрывавшийся за псевдонимом Сатоши Накамото, покинул проект без объяснения причин. До сегодняшнего дня было выдвинуто множество предположений о том, кто является создателем первой криптовалюты. Но однозначной версии нет до

сих пор. В дальнейшем разработчики, входившие в криптосообщество, начали работать над созданием других цифровых валют.

ГЛАВА 2

Биткойн сегодня обладает самой разветвленной и обширной сетью и является наиболее ликвидной криптовалютой. Биткойн нематериален и не обладает привязкой к каким - либо государственным валютам, драгоценным металлам или природным ресурсам. Курс Биткойн чрезвычайно подвижен и определяется исключительно балансом спроса и предложения. Оборот валюты не контролируется какими-либо органами, ведомствами или организациями и осуществляется только между криптокошельками участников сети. Отмена транзакций невозможна.

2.1. Система prof-of-work.

Концепция Proof-of-Work (англ. «Доказательство работы», дальше PoW) — алгоритм защиты распределенных систем от злоупотреблений (DoS-атак, спам-рассылок и тому подобного), суть которого сводится к двум основным пунктам:

1. необходимости выполнения определенной достаточно сложной и длительной задачи;
2. возможности быстро и легко проверить результат.

PoW-задачи изначально не предназначены для человека, их решение компьютером всегда достижимо в конечные сроки, однако требует больших вычислительных мощностей. При этом проверка полученного решения требует гораздо меньше ресурсов и времени.

Впервые концепция Proof-of- Work была описана в 1993 году в работе “Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology”. Хотя сам термин в статье еще не использовался, авторы предложили следующую идею: «Чтобы получить доступ к общему ресурсу, пользователь должен вычислить некоторую функцию: достаточно

сложную, но посильную; так можно защитить ресурс от злоупотребления».

В 1997 году криптограф и будущий основатель Blockstream Адам Бэк запустил проект Hashcash, посвященный защите от спама. Задача формулировалась следующим образом: «Найти такое значение x, что хеш SHA(x) содержал бы N старших нулевых бит».

Система предлагала хеширование частичной инверсии при отправке по электронной почте. Для расчета соответствующего заголовка требуется около 252 хеш-вычислений, которые надо пересчитывать для каждой отправки. И если для нескольких обычных писем дополнительные расчеты препятствий не создают, то массовую рассылку спама необходимость постоянного пересчета делает очень ресурсоемкой. При этом проверка корректности вычисленного кода осуществляется очень быстро: используется однократное вычисление SHA-1 с заранее подготовленной меткой.

Сам термин Proof-of-Work появился в 1999 году в статье ”Proofs of Work and Bread Pudding Protocols” (авторы — Маркус Якобссон и Ари Джуелс) в журнале Communications and Multimedia Security.

Сатоши Накамото использовал концепцию PoW в первой криптовалюте — биткоине. Он взял идею Hashcash, добавив к ней механизм изменяющейся сложности — уменьшение или увеличение N (требуемого числа нулей) в зависимости от суммарной мощности участников сети. Вычисляемой функцией стала SHA-256.

2.2. Хеширование SHA-256.

SHA 256 – это способ хеширования информации, использующийся в сети Bitcoin и многих других криптовалютах. Его название – это аббревиатура от Secure Hashing Algorithm. Создателем данной технологии

является подразделение Минобороны США по нацбезопасности. Ключевая задача алгоритма – преобразование информации в определенное значение конкретной длины, которая выступает в качестве идентификатора. Алгоритм хеширования SHA 256 позволяет контролировать эмиссию криптовалюты, поскольку является важной составляющей майнинга, а также обеспечивает максимальную защищенность сети. Чтобы заниматься добычей цифровых активов, нужно тщательно проанализировать особенности этой технологии, в частности понять, для чего она нужна и какие задачи способна решать.

Если упростить, то англоязычная аббревиатура SHA на русский переводится как «безопасный хеш-алгоритм». Это один из многих криптографических алгоритмов. Рассматриваемая хеш-функция является представителем класса SHA второго поколения. Впервые информация об этой технологии была опубликована NIST (Национальный институт стандартов США). Алгоритму был присвоен статус федерального стандарта.

SHA256 – алгоритм хеширования, использующийся для преобразования входной информации любого объема в строку фиксированного размера. Следовательно, он обеспечивает прием входа, а затем осуществляет выход четко установленной длины. Это и есть хеш. Совершенно неважно, пользователь вводит букву, слово или целую книгу – на выходе он получит код установленной длины.

Алгоритм преобразовывает информацию в 256-битный код, состоящий из 64 букв или цифр, составленных случайным образом. В результате генерируются практически уникальные комбинации, которые крайне тяжело расшифровать. Обратное преобразование невозможно, что, собственно, и делает SHA 256 одним из самых безопасных алгоритмов.

Детерминированность – еще одна важная особенность SHA, которую нельзя упускать. Сгенерированный код будет всегда одинаковым, если используют идентичные входные параметры. Эта характеристика

делает данную хеш-функцию идеальной для использования в пиринговой сети Bitcoin. Сегодня есть множество других способов хеширования, а у SHA 256 немало недостатков, но он продолжает пользоваться популярностью.

2.3. Транзакции.

Рассматривая понятие транзакции можно сказать, что данный термин обозначает проведение финансовой операции. На современном этапе существует множество видов транзакций в зависимости от вида деятельности и субъектов, которые их совершают. Но сегодня мы изучим относительно новый вид проведения финансовых операций, который относится к сфере криптовалютного мира.

Если разбираться в транзакциях криптовалют, можно сделать вывод, что это обычный процесс перечисления валютных единиц с одного счета на другой. Все финансовые операции перевода средств фиксируются в блокчейне. За счёт этих записей, пользователи могут свободно изучить информацию по любой проведенной транзакции.

Также, можно сказать, что скорость выполнения и подтверждения транзакций криптовалют намного выше в сравнении с теми же банковскими переводами, которые могут затягиваться до нескольких суток и создавать определенные неудобства для своих клиентов. Хотя в последнее время с криптовалютными платежами тоже начали возникать проблемы из-за огроНачнем с того, что для начала работы с криптовалютами, их покупки, продажи или обмена вам необходимо зарегистрировать свой специализированный кошелек. Для наилучшего понимания возьмем в качестве примера наиболее известный всем Bitcoin. Вы можете создать биткоин-кошелек прямо в онлайн сервисах либо установить ликальный кошелек на компьютер или мобильный телефон. После установки и регистрации, вы сможете провести транзакцию, то есть, например, перевести кому-либо часть своих активов.

Для осуществления транзакции вам будет необходимо указать следующие данные:

1. Номер биткоин кошелька, который будет получателем;
2. Сумма единиц валюты, которую вы намерены отправить;
3. Сумма комиссии майнерам за отправку транзакции.

Комиссию за перевод стоит обсудить отдельно. Дело в том, что вы сами можете определять сумму оплаты майнерам за проведение платежа, от этого будет в первую очередь зависеть каким в очереди будет ваш перевод. Именно майнеры принимают решение о выборе определенной транзакции и добавлении ее в ближайший блок. Поэтому транзакции с наибольшими комиссиями определенно будут иметь приоритетные позиции относительно других, не предполагающих вознаграждение за их выполнение. Поэтому величина комиссии может иметь существенное влияние на время выполнение транзакции. Из-за этого на рынке образовалась своеобразная конкуренция среди пользователей за право ускорить транзакцию.мной загруженности.

2.4. Блокчейн.

Блокчейн (от англ. blockchain — «цепочка блоков») — технология шифрования и хранения данных (реестра), которые распределены по множеству компьютеров, объединенных в общую сеть.

Блокчейн — это цифровая база данных информации, которая отражает все совершенные транзакции. Все записи в блокчейне представлены в виде блоков, которые связаны между собой специальными ключами. При этом каждый новый блок содержит данные о предыдущем.

Блокчейн применяется для хранения и передачи цифровых данных. Это могут быть как финансовые, так и нефинансовые активы (например, изображения или объекты индустрии видеоигр). Технология блокчейна позволяет присвоить активу уникальную информацию о его

принадлежности конкретному лицу. При этом такую информацию невозможно подделать, удалить или незаметно изменить.

Основные принципы блокчейна (распределенность и объединение данных о подлинности документа в блоки) были разработаны еще в начале 1990-х годов на основе еще более ранних математических концепций. В 1991–1992 годах американские ученые Уэйкфилд Скотт Сторнетта, Стюарт Хабер и Дэйв Байер описали технологию последовательного создания блоков данных, в которых с помощью криптографических алгоритмов и дерева хешей фиксируются сертификат подлинности и информация о дате генерации. Но технической возможности для практической реализации данной идеи тогда еще не было.

В 2004 году американский программист Гарольд Томас Финни II разработал систему RPoW, которая считается прототипом криптовалюты. В октябре 2008 года Сатоси Накамото (это псевдоним человека или группы людей) в научной статье, посвященной первой криптовалюте, биткоину, предложил использовать технологию блокчейна для создания децентрализованной и независимой платежной системы с ограниченным предложением активов. Разработка биткоина началась в 2007 году и завершилась в 2009 году.

Технология блокчейна стала актуальной тогда, когда появилась необходимость быстрой и надежной передачи цифровых данных.

Блокчейн позволяет каждому участнику сети иметь доступ к распределенной базе данных. При этом в блокчейне хранятся не сами данные, а записи о событиях (транзакциях) в их хронологической последовательности. Все новые записи проверяются на подлинность — для занесения в блокчейн их должны подтвердить большинство участников сети. Записи группируются в блоки, которые объединяются в цепочки. Данные, попавшие в блокчейн, нельзя изменить или удалить, не нарушив целостность цепи блоков.

2.5. Сложность.

Чем дольше добывается золото, тем труднее (затратнее по ресурсам) становится его добывать. Это гарантирует, что инфляция будет под контролем. В Биткойн похожее поведение достигается путем введения функции скорости суммарно добываемых монет от времени. Скорость добычи со временем падает и стремится к нулю, а объем эмиссии Биткойн ограничен общим числом монет в 21 миллион. Эмиссия криптовалют осуществляется посредством добычи, или майнинга, блоков. Периодически, через каждые 2016 добытых блоков, происходит корректировка сложности их добычи. Корректировка основывается на скорости добычи в последний период и нужна для сохранения среднего интервала добычи блоков у отметки в 10 минут.

2.6. Майнинг.

Слово «майнинг» пришло к нам из английского языка и в буквальном смысле означает добычу полезных ископаемых. В контексте финансов и информационных технологий таким «сырьем» считается криптовалюта.

Майнинг – это добыча цифровой валюты с помощью специального оборудования.

Если говорить на языке блокчейн-инженеров, майнинг представляет собой присоединение блоков, в которых хранится информация о проведенных транзакциях. В результате они образуют непрерывную и последовательную цепочку – блокчейн.

Чтобы присоединить блок, необходимо решить определенную математическую задачу, расшифровав алгоритм криптовалюты.

Собственно, этим и занимаются майнеры, а точнее их специальные устройства. Если оборудование находит правильный ответ, его владелец получает вознаграждение в виде цифровых монет.

При этом чем больше майнеров нацелены на решение задачи, тем больше усложняются поиски верного ответа и падает стоимость.

Существует три основных способа майнинга криптовалюты. Поговорим подробнее о каждом из них.

1. Облачный майнинг

Этот способ добычи криптовалюты считается самым простым и подходит для тех, кто только начинает майнить. Человеку не приходится самостоятельно заниматься покупкой, установкой и настройкой оборудования. От него требуется лишь одно – арендовать объем хешрейта на удаленном сервере.

Хешрейт (от англ. hashrate) – общий объем мощности, необходимый для добычи криптовалюты. Чем выше этот показатель, тем мощнее оборудование.

После этого всю работу по добыче цифровых монет берут на себя профессиональные майнеры. Человеку достаточно пополнять баланс в личном кабинете облачного сервиса и выводить полученные средства на свой кошелек. Обычно срок аренды хешрейта варьируется от одного до трех лет.
Важно оговорить, что даже самые проверенные дата-центры не могут стопроцентно гарантировать прибыль. Цифровой рынок имеет свойство проседать, а значит, в такие моменты доход с майнинга будет минимальным.
С этим связана высокая волатильность криптовалюты. Занимаясь майнингом, человек заранее соглашается с риском потерять вложенные средства.

Еще один недостаток подобного майнинга – большая вероятность того, что человек может нарваться на мошенников. Нередко злоумышленники пользуются доверием начинающих майнеров и оставляют их без денег.

2. Соло-майнинг

В этом случае майнер добывает криптовалюту в одиночку. Он самостоятельно собирает и настраивает оборудование, после чего пытается решить задачу.

С каждым годом майнить становится сложнее, поэтому майнеры используют более мощное оборудование. Сегодня соло-майнингом пользуются единицы, предпочитая объединяться в команды.

3. Майнинг в пуле

Пул (от англ. pool) – это сервер для коллективного майнинга.

Такой способ майнинга позволяет объединять мощности нескольких оборудований и быстрее находить решения задач. В основе пула лежит сервер, который рассылает участникам команды задачи с более простыми условиями.

ГЛАВА 3

Основные «плюсы»

Децентрализованность валютной системы. Все транзакции, включая выпуск новой денежной единицы, фиксируются в общей истории, доступной каждому пользователю. При желании можно проследить путь каждой единицы до момента её появления. Именно поэтому криптовалюту невозможно подделать, как нельзя полностью удалить историю транзакций, поскольку она одновременно сохраняется на компьютерах и серверах миллионов пользователей по всему миру; Открытый код криптовалюты и анонимность. Исходный код криптовалюты и теория Биткойна открыты. В Биткойне работают те же алгоритмы, которые используются в интернет-банкинге. Единственным отличием интернет-банкинга является раскрытие информации о конечном пользователе. В сети Биткойна вся информация о транзакции есть в общем доступе (сколько, когда), но нет данных о получателе или отправителе монет (нет доступа к персональной информации владельцев кошельков). Пиринговая сеть криптовалюты. В подобных сетях нет главного сервера, отвечающего за все операции. Протоколы работают как одноранговая сеть, наподобие торрентов. Обмен информацией (в нашем случае - деньгами) совершается между 2-3 и более программами-клиентами. Все установленные у пользователей программы-кошельки являются частью сети Биткойн. Каждый клиент хранит запись обо всех совершенных транзакциях и о количестве Биткойнов на каждом кошельке. Транзакции производятся сотнями распределенных серверов, их еще называют

"добытчиками". Ни банки, ни налоговые, ни государство не могут контролировать обмен денег между кошельками пользователей. Безграничные возможности транзакций. Каждый из держателей кошелька может платить кому угодно, где угодно и за что угодно. Транзакции невозможно проконтролировать или запретить, так что можно совершать переводы в любую точку мира, где бы не находился другой пользователь с кошельком криптовалюты. Криптовалюта работает как "живая наличка", сочетая в себе функции электронной коммерции. Очень низкие комиссии. Платежи с помощью криптовалюты на данный момент производятся либо без комиссии, либо с невероятно низкими комиссиями. Пользователи могут включать комиссии в транзакции, чтобы получить приоритет при обработке - это дает более быстрое подтверждение транзакций сетью. Кроме того, существуют процессинговые компании, которые помогают торговцам в осуществлении транзакций, переводя криптовалюту в фиатные валюты, которые отправляются напрямую на счета предпринимателей день-в-день. Так как эти сервисы основаны на Биткойне, они предлагают комиссии гораздо ниже, чем при использовании PayPal или пластиковых карт. Таким образом, криптовалюту целесообразно определить как особую разновидность электронных денег, функционирование которых основано на децентрализованном механизме эмиссии и обращении и представляет собой сложную систему информационно-технологических процедур, построенных на криптографических методах защиты, регламентирующих идентификацию владельцев и фиксацию факта их смены. При этом появление и популярность криптовалют обусловлены технологически, институционально и экономически. Между тем, в настоящее время функционирование криптовалют основано лишь на неформальных нормах. Несмотря на высокую популярность, законодательно проведение операций с криптовалютами не закреплено.

Основные «минусы».

Недостаточное распространение и признание. Несмотря на все свои преимущества, платежная система биткойн еще не получила масштабного распространения. Если вы зайдете в магазин и спросите, можно ли здесь рассчитаться биткойнами, вы увидите круглые глаза продавца. То есть, использовать биткойн для расчетов пока можно лишь в определенных сферах. Курсовые колебания. После стремительного роста курса биткойна осенью 2013 года, огромное количество охотников за легкими заработками начали скупать эту криптовалюту со спекулятивными целями, и все они "прогорели", потому что с тех пор стоимость биткойна до настоящего момента только снижается. Поскольку в системе биткойн выпущено еще довольно небольшое количество монет, то любые крупные сделки могут вызвать довольно сильные курсовые колебания, что опасно для других участников системы. Непредсказуемость. По сути, система биткойн - это своего рода стартап, и предсказать дальнейшее его развитие довольно сложно. Пока он успешно прошел только свою начальную стадию. Как будет происходить развитие системы далее можно только предполагать, и необязательно эти предположения окажутся верными. Это серьезный минус биткойна. Отсутствие гарантий. Владельцы биткойнов не имеют никаких гарантий, что они хотя бы смогут вернуть свои деньги, которые в них вложили. Курс биткойна устанавливается рынком, и при наступлении каких-то глобальных фундаментальных обстоятельств может даже упасть до нуля. Никто не может гарантировать, что такого не случится. Кроме того, биткойн как валюта ничем не подкреплен, кроме вычислительных мощностей, используемых для его создания. Государственные запреты. Разные государства по-разному относятся к платежной системе биткоин, и в любой момент могут ввести всевозможные запреты на ее использование, например, как средства оплаты за товары и услуги. Потеря монополизации роли эмиссии денег для государства будет означать потерю власти над людьми, поэтому они будут стараться не допустить этого, либо как-то взять систему биткойн под свой контроль. Это может вызвать быстрое и сильное

обесценивание криптовалюты. Оборот нелегальных товаров. Использование биткойнов в теневой экономике позволяет обеспечить неподконтрольность национальным органам власти торговлю такими товарами, как оружие, наркотики и т.д. В качестве примера подобной торговли СМИ чаще всего рассматривают историю интернет-магазина SilkRoad. При этом во время слушаний в Сенате США по поводу виртуальных валют отмечалось, что наличные деньги для нелегальных сделок используют гораздо чаще, но это не становится основанием для критики или запрета наличных.

ГЛАВА 4

Криптовалюта не являются долговым обязательством эмитента, что отличает их от электронных денег и безналичных расчётов. Котировка (курс) криптовалюты, напримербиткойна, формируется исключительно балансом спроса и предложения, не привязана к какой-либо валюте или другому активу. Также система "Биткойн" не принадлежит административному органу (центробанку или государству), который бы стремился обеспечить ликвидность на заданном уровне, обязался сам или обязывал других принимать оплату в биткойнах или мог бы изменить его покупательную способность путём волевого изменения суммарного количества биткойнов. Часто утверждается, что ограничение эмиссии является защитой от инфляции, так как предполагается, что ограниченное предложение обеспечит тенденцию к росту котировок. Это стимулирует спекулятивное накопление криптовалюты. Ряд авторов считают, что ограниченное количество криптовалюты не является достаточным условием для гарантирования тенденции роста курса, так как ещё одним необходимым условием для этого является увеличение объёма предложения товаров и услуг за криптовалюту и сервисов, связанных с ней. То есть неспекулятивная ценность криптовалюты напрямую зависит от объёма только тех товаров и услуг, которые можно будет за нее приобрести, а не общемировой товарной массы. С 2009 по апрель 2010 года биткойны лишь накапливались.25 апреля 2010 года

состоялась первая официальная продажа 1000 биткойнов по 0,3 цента, а в мае 2010 года за 10 000 биткойнов купили две пиццы. Лишь в феврале 2011 года за биткойн начали давать доллар или около того. Первая крупная статья о биткойнах в Forbes 20 апреля 2011 года пробудила более широкий интерес. К концу мая за биткойн давали почти 9 долларов, 9 июня 2011 года цена достигла 29,57 доллара, после чего пошла вниз примерно до двух долларов и вернулась только 19 февраля 2013 года. В середине ноября 2013 года цена превысила 1000 долларов. После череды всплесков и падений, с января 2014 года цена имела тенденцию к понижению. В январе 2015 года цена снизилась до 200 долларов, после чего начала колебаться в пределах 200-300 долларов. По данным 2017 года в ноябре биткоин достиг нового уровня - 7000 долларов. Первоначально криптовалюта, а именно биткойн, использовалась только ограниченным кругом людей, которые стояли у истоков его основания. Но затем за несколько лет превратился в гигантскую масштабную систему, охватывающую весь мир. На сегодняшний день операции с криптовалютами проводят не только на множестве бирж, обменников и других ресурсов в интернете, но и во многих оффлайнкомпаниях: магазинах, сервисных центрах и даже госучреждениях. Так, например, в США известны случаи выдачи зарплаты госслужащим в биткойнах, биткойн принимают к оплате во многих ресторанах, отелях, магазинах в ряде стран мира. В некоторых азиатских странах биткойны достаточно активно используются как альтернатива банковским счетам и пластиковым картам, поскольку банковское обслуживание в этих странах очень дорогое. Также Суд Евросоюза приравнял биткойны и другие криптовалюты к традиционным деньгам. Более того, суд в своем в решении от 22 октября 2016 года объявил, что сделки по обмену традиционной валюты на биткойны и другие криптовалюты не должны облагаться налогом на добавочную стоимость (НДС).

В России криптовалюты на данный момент не имеют широкого распространения.

Министерство финансов ужесточило подход к наказанию за выпуск и оборот криптовалют. Ведомство Антона Силуанова разработало поправки в Уголовный кодекс, по которым нарушителей будут сажать в тюрьму на четыре года. Ранее Минфин предлагал более мягкое наказание за выпуск и оборот криптовалют - штраф до 500 тыс. рублей или исправительные работы сроком до двух лет. Об этом "Известиям" рассказали в пресс-службе Минфина. В Минэкономразвития, которое поддерживает эту инициативу, отметили, что законопроект Минфина будет внесен правительством в Госдуму в ближайшие месяцы. В конце сентября 2015 года Минфин предложил ввести уголовное наказание за выпуск и оборот криптовалют в России, считая их денежными суррогатами (запрещены законом "О Центральном банке"). УК предлагалось дополнить новой статьей "Оборот денежных суррогатов": за изготовление, приобретение криптовалют в целях сбыта, а также за сбыт Минфин предлагал штраф в размере 500 тыс. рублей или в размере зарплаты, иных доходов осужденного за период до 2 лет, обязательные работы до 480 часов или исправительные работы сроком до 2 лет. Ведомство однозначно отнесло биткоины к денежным суррогатам, отождествив их оборот с незаконными финансовыми операциями.

Но, на конференции, которая проходила в Сочи 10 октября текущего года, Владимир Путин приказал разрешить криптовалюту и ввести налог на майнинг.

Возможно, к этому решению ведомство подтолкнули планы компаний по выпуску криптовалют. Qiwi в прошлом году объявила о разработке своего аналога биткоинов-битрублей. Уже битрублями можно расплачиваться за услуги (например, за мобильную связь) через Qiwi-кошелек. Гендиректор и совладелец компании Сергей Солонин сообщил, что при запуске будет использоваться криптотехнологияblockchain, на которой работает система Bitcoin. Представители Центробанка в прошлом году отмечали, что считают биткоины денежными суррогатами. Но первый зампред ЦБ Георгий Лунтовский объявил, что "нельзя отвергать этот инструмент, возможно, за

ним будущее". Резко против криптовалют выступают силовики: например, Федеральная служба по контролю за оборотом наркотиков (ФСКН) заявляла, что биткоины среди прочих платежных систем активно используются наркомафией в торговле наркотиками. Как отметили представители службы, позиция ФСКН по данному вопросу не изменилась. Против криптовалют выступают Генеральная прокуратура, Министерство внутренних дел и Федеральная служба безопасности. Источник, близкий к ЦБ, пояснил "Известиям", что окончательная позиция ЦБ прояснится по итогам анализа функционирования криптовалют рабочей группой ЦБ, в изучении этого вопроса принимает участие Росфинмониторинг. Близкий к этому ведомству источник отметил, что на повышенные риски оборота криптовалют указывает FATF (международная Группа разработки финансовых мер борьбы с отмыванием денег - FinancialActionTaskForce, участницей которой является и Россия). По словам собеседника, FATF считает, что главные риски связаны с анонимностью операций с криптовалютами. Источник говорит, что во всех последних отчетах FATF говорится об этой проблеме.

Среди противников криптовалют и Минэкономразвития.

По денежным суррогатам, в том числе криптовалютам, отсутствует обеспечение и юридически обязанные по ним субъекты, - сказала "Известиям" Елена Лашкина, помощник министра экономического развития Алексея Улюкаева. - Операции по ним носят спекулятивный характер, осуществляются на так называемых виртуальных биржах и несут высокий риск значительного изменения их стоимости. Использование денежных суррогатов, в том числе криптовалют, сопряжено с высоким уровнем рисков, прежде всего в связи с их необеспеченностью активами, отсутствием единого регулирования выпуска и юридически обязанного по ним субъекта. Анонимный характер деятельности по выпуску денежных суррогатов, в том числе криптовалют, неограниченным кругом субъектов создает предпосылки для вовлечения граждан и компаний в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем,

и финансирование терроризма. Елена Лашкина добавила, что использование денежных суррогатов, в том числе криптовалют, в качестве средства платежа и накопления может повлечь нарушение прав вовлеченных в их оборот добросовестных лиц, поскольку держатели денежных суррогатов ввиду их анонимности и виртуальности лишены возможности защиты своих интересов в судебном или административном порядке. Председатель правления агентства "Финансовые инновации" Роман Прохоров (ранее возглавлял департамент национальной платежной системы ЦБ) указывает, что единственный шанс для легального оборота криптовалюты в России - установление четких правил их обращения с ликвидацией анонимности.

ЗАКЛЮЧЕНИЕ

Сегодня криптовалюты продолжают свое развитие, число пользователей киберденьгами неуклонно растет. Популярность биткоина породила создание других криптовалют, которые развиваются наряду с биткоином, но их популярность и возможности пока намного меньше. В некоторых странах, в том числе в России, с криптовалютами начали бороться, объясняя это заботой о людях, предостережением их от вложения денег в “денежные суррогаты" и возможной их потери, в случае если наступит крах криптовалюты - биткойна. Однако, на самом деле, такая борьба, вероятнее всего, вызвана желанием сконцентрировать функции денежной эмиссии, а значит - и власть, в руках государства и не допустить образования альтернативных источников эмиссии платежных средств, тем более, не подвергающихся никакому государственному регулированию. Тем не менее, физически запретить операции с криптовалютами в Интернете практически невозможно. Можно ограничить их обмен на реальные деньги, запретив деятельность таких обменников, но чтобы запретить добычу криптовалют, в том числе биткойнов, потребуется возможность доступа к каждому компьютерному устройству, что пока запрещено законодательством

большинства стран, как вмешательство в личную жизнь. В конце октября 2017 года появилась новость о том, что разработан специальный вирус, который приводит к исчезновению уже приобретенных биткойнов. Вероятно, разработкой вируса занимались сами же разработчики биткойна.

Список используемой литературы

1. https://cryptos.team/blog/algoritm-sha-256-2022/
2. https://forklog.com/cryptorium/chto-takoe-proof-of-work-i-proof-of-stake
3. https://mining-cryptocurrency.ru/istoriya-kriptovalyut/#i-2
4. https://multiurok.ru/index.php/files/proekt-na-temu-kriptovaliuta.html
5. https://topuch.com/informaciya-i-informacionnaya-tehnologiya/index.html
6. https://sovcombank.ru/blog/umnii-potrebitel/chto-takoe-maining?utm_referrer=https%3A%2F%2Fyandex.ru%2F