

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

Сиракян Л.В., Степаненко И.С. Криптовалюта // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2021. – №5 (май). – АРТ 50-эл. – 0,3 п.л. - URL: <http://akademnova.ru/page/875550>

РУБРИКА: ЭКОНОМИЧЕСКИЕ НАУКИ

УДК 336.743.3

Сиракян Лиля Вачагановна

Студентка 3 курса, факультета экономики

Степаненко Игорь Сергеевич

Студент 3 курса, факультета экономики

Научный руководитель: Филимонцева Е.М.,

кандидат экономических наук, доцент кафедр экономики, финансов и природопользования

Южно-Российский институт-филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации

г. Ростов-на-Дону, Российская Федерация

e-mail: l-sirakanyan@bk.ru

КРИПТОВАЛЮТА

Аннотация: На протяжении истории люди использовали товарную валюту. Фиатная валюта появилась позднее, около 1000 лет назад, став на сегодня доминирующей. Криптовалюта – это не товарные и не фиатные деньги, а их новый, экспериментальный вид. Появление криптовалюты может быть или не быть, в конечном счете, успешным, но оно предлагает новое сочетание технических и денежных характеристик, которые поднимают различные экономические проблемы.

Эта статья объясняет, что такое криптовалюта, и начинает отвечать на вопросы, возникшие с ее появлением. Для того, чтобы понять, почему криптовалюта имеет особенные характеристики, важно понять какую

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

проблему призвано решить ее появление. По этой причине мы начинаем с проблем, которые преследовали цифровые деньги в прошлом, и технического прогресса, который делает криптовалюту возможной.

Ключевые слова: анонимность; биткоин; криптовалюта; криптография; задача византийский генералов; неопределенность обменного курса; деньги; новая денежная экономика; изменчивость.

Sirakanyan Lilya Vachaganovna

3rd year student, Faculty of Economics

Stepanenko Igor Sergeevich

3rd year students, Faculty of Economics

Supervisor: **Filimontseva E.M.**,

Candidate of Economic Sciences, Associate Professor of Department of
Economics, Finance and Environmental Management

YURIU The Russian Presidential Academy of National Economy and Public
Administration under the President of the Russian Federation
Rostov-on-Don, Russian Federation

CRYPTOCURRENCY

Abstract: Throughout history, people have used commodity currency. Fiat currency appeared later, about 1000 years ago, becoming the dominant currency today. Cryptocurrency is not a commodity or fiat money, but a new, experimental form of it. The emergence of cryptocurrency may or may not be ultimately successful, but it offers a new mix of technical and monetary characteristics that raises various economic concerns.

This article explains what cryptocurrency is and begins to answer the questions that have arisen since its inception. In order to understand why cryptocurrency has special characteristics, it is important to understand what problem its appearance is intended to solve. For this reason, we start with the problems that have plagued digital money in the past and the technological advancements that make cryptocurrency possible.

Key words: Anonymity; Bitcoin; cryptocurrency; cryptography; task of the Byzantine generals; uncertainty in the exchange rate; money; new money economy; variability.

Криптовалюта - это название системы, которая использует криптографию для обеспечения безопасной передачи и обмена цифровыми токенами распределенным и децентрализованным образом. Токенами можно торговать по рыночным курсам для фиатных валют. Первой криптовалютой стал Биткойн, который появился в январе 2009 года. С тех пор было создано множество других криптовалют, использующих те же механизмы, что и биткойн, но изменивших некоторые специфические параметры своих управляющих алгоритмов. Два основных новшества, которые ввел Биткойн, и то, что сделало криптовалюты возможными, было решением двух давних проблем в информатике: проблему двойного расходования и задачу византийских генералов.

Проблема двойного расходования

До изобретения Биткойна две стороны не могли совершать электронные сделки без привлечения доверенного стороннего посредника. Причиной стала задача, известная компьютерным специалистам как "проблема двойного расходования", которая преследовала попытки создания электронных денег с момента появления Интернета.

Для того чтобы понять проблему лучше, сначала стоит рассмотреть, как работают физические денежные операции. Предъявитель банкноты физической валюты может передать ее другому лицу, которое затем может подтвердить, что он является единственным владельцем этой банкноты, просто взглянув на свои руки. Учитывая это, наличные деньги позволяют различным сторонам, в том числе незнакомым, совершать сделки, не доверяя друг другу.

До недавнего времени, единственным способом преодолеть проблему двойного расходования было нанять доверенного стороннего посредника. В случае совершения сделки между двумя физическими лицами, они будут иметь учетную запись у третьей стороны, которой они доверяют, например, PayPal. Доверенные посредники, такие как PayPal, ведут бухгалтерскую книгу всех остатков на счетах и транзакций. Когда одна сторона хочет отправить другой денежную сумму, она сообщает об этом PayPal, который, в свою очередь, вычитает сумму с одного счета и добавляет ее к другому. В конце дня все переводы между всеми счетами сводятся к нулю. Заметим, однако, что в отличие от наличных денег сделки, в которых участвует посредник третьей стороны, не являются окончательными, поскольку сделки могут быть отменены третьей стороной.

В 2008 году Сатоши Накамото (псевдоним) объявил о способе решения проблемы двойного расходования без привлечения третьих лиц (Nakamoto, 2008). Его изобретение, Биткойн, по сути, является электронной наличностью. Он впервые позволяет осуществлять окончательную передачу, а не простое копирование цифровых активов таким образом, чтобы пользователи могли их проверить, не доверяя другим сторонам. Это достигается благодаря грамотному использованию криптографии с открытым ключом, одноранговой сети и системы проверки работоспособности.

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

Как и PayPal, биткойн-система использует бухгалтерский регистр, который называется блокчейн. Все транзакции в биткойн-экономике записываются и выверяются в блокчейн. Однако, в отличие от регистра PayPal, блокчейн не поддерживается центральным органом. Вместо этого блокчейн - это публичный документ, который распространяется одноранговым способом по тысячам узлов сети Биткойн. Новые транзакции проверяются по блокчейну, чтобы убедиться, что те же самые биткойны ранее не были потрачены, но работа по проверке новых транзакций не выполняется ни одной доверенной третьей стороной. Вместо этого работа распределяется между тысячами пользователей, которые работают на согласование и ведение книги блокчейн. По сути, вся одноранговая сеть занимает место одной доверенной третьей стороны.

По факту майнеры биткойна сталкиваются с проблемой двойного расходования. Решением в ситуации с Биткойном будет необходимость потребовать сопровождение решением математической задачи дополнений к бухгалтерской книге.

Новые блоки содержат в себе не только информацию о новых транзакциях, которые были транслированы в сети, но и транзакцию, которая присваивает победившему майнеру 25 вновь созданных биткойнов, что стимулирует их посвящать свои вычислительные мощности сети. Размер вознаграждения майнера, сопровождающего новые блоки, также уменьшается вдвое каждые 210 000 блоков (каждые четыре года). Вознаграждение начиналось с 50 биткойнов с каждого блока, когда сеть была запущена в 2009 году. Сегодня награда составляет 25 биткойнов и снова сократится вдвое до 12,5 в 2016 году. Это означает, что общее количество биткойнов, которые будет когда-либо существовать не более 21 миллиона. По мере того как вознаграждение за майнинг уменьшается, какой стимул будет у майнеров

предоставлять свои вычислительные мощности для проверки транзакций? Ответ заключается в том, что стороны транзакции могут включить плату за транзакцию, которая будет выплачена майнеру, который успешно добавит свою транзакцию в блокчейн.

Экономика криптовалюты

Управление

Криптовалюта не имеет центральных банков для регулирования денежной массы или надзора за финансовыми институтами, но при этом, нельзя пренебрегать важностью институтов управления криптовалютой. Мы сосредоточим наше обсуждение на двух отдельных, но взаимосвязанных способах управления.

Алгоритмическое управление

Понимание того, что действительно считается криптовалютными транзакциями, заключено в запущенном майнерами и пользователями криптовалют одноранговом программном обеспечении. Первый допустимый вид транзакций-создание монет из пустоты. Данную транзакцию не каждый может выполнить, за право выполнить одну из них на биткойне майнеры соревнуются каждые 10 минут.

Рост количества монет ограничен заранее просчитанным числом на блок. Транзакция, в которой майнер претендует на новые монеты, как и любая другая, должна соответствовать ожиданиям сети. Сеть отклонит блок, содержащий транзакцию, в которой майнер награждает себя слишком большим количеством новых монет.

В Биткойне заранее определенная сумма не должна быть постоянной с течением времени, а должна уменьшаться вдвое каждые 210 000 блоков или примерно каждые четыре года, как описано выше. Общий объем предложения биткоинов будет асимптотически приближаться к 21 миллиону, но никогда не

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

превысит его. Он достигнет 20 миллионов в 2025 году и полностью прекратит расти в 2140.

Открытое управление

Программное обеспечение Биткойна, которое помогает соблюдать определенные правила для действительных транзакций и скорости создания денег, появилась не просто так. Правила, заложенные в программное обеспечение, возникают из взаимодействия между лидерами проекта с открытым исходным кодом, который управляет так называемым "эталонным клиентом", другими разработчиками, майнерами, сообществом пользователей и злоумышленниками. Динамика между этими звеньями так же важна для понимания Биткойна, как и динамика центральных банков, традиционных денежных институтов и денежно-кредитной политики для понимания фиатной валюты.

Биткойн, как и все другие, даже умеренно успешные криптовалюты, является непатентованным проектом с открытым исходным кодом. Пользователи склонны с подозрением относиться к криптовалютным проектам с закрытым исходным кодом, которые имеют значительный предварительный майнинг для вознаграждения инсайдеров или имеют другие проприетарные функции. Другие ожидания сообщества пользователей также накладывают дополнительное давление на разработчиков. Например, жесткий предел в 21 миллион биткоинов, хотя он и может быть изменен с помощью обновления программного обеспечения.

Разделение программного обеспечения Биткойна на 'эталонный клиент' и так называемый 'альт-клиент' также имеет значение для развития Биткойна. Сообщество обращается к команде Bitcoin Core за лидерством в отношении направления развития сети. Альтернативный подход заключается в том, чтобы сообщество согласовало спецификацию для сети. Тот факт, что биткойн имеет

такого доминирующего референтного клиента, означает, что развитие может происходить быстрее, хотя оно также может иметь скрытые недостатки. Менее концентрированный подход к разработке криптовалют замедлил бы развитие, что предотвратило бы любые изменения в сети без полного обсуждения сообщества. Вполне возможно, что со временем Биткойн мог ближе продвинуться к этой модели, но на данный момент преимущества быстрой эволюции могут перевесить недостатки.

Майнеры также играют важную роль в управлении. Поскольку они криптографически защищаются от двойного расходования, их мнение относительно того, что считается действительной транзакцией, необходимо для функционирования криптовалюты. Майнеры также оказывают влияние через майнинговые пулы. Майнеры присоединяются к пулам, чтобы получить более последовательную выплату. Один майнер, работающий в одиночку, может не сразу обнаружить блок.

Майнинг-пулы часто вызывают осложнения. Например, самый большой пул майнинга биткойнов часто имеет треть или больше вычислительной мощности сети биткойнов. Если пул когда-либо получал больше половины вычислительной мощности сети, он мог тратить вдвое больше. Двойные расходы разрушат доверие к сети биткойнов и, скорее всего, приведут к резкому падению цен. Следовательно, мы наблюдаем некоторое саморегулирование со стороны майнинговых пулов, которые активно инвестируют в успех Биткойна. Всякий раз, когда верхний пул начинает приближаться к 40 процентам вычислительной мощности сети, некоторые участники выходят из этого пула и присоединяются к другому. До сих пор эта норма сохранялась, но многие в сообществе обеспокоены концентрацией майнинговых пулов. Недавно, майнинговый пул GHash.IO ненадолго превысил 50 процентов майнинговой мощности Биткойна. Нет никаких

свидетельств того, что пул использовал свое положение для удвоения расходов, но многие наблюдатели были встревожены тем, что это могло произойти.

В феврале 2014 года, когда Mt. Gox, старейшая и крупнейшая биткойн-биржа, заявила, что ее запасы биткойнов были исчерпаны. Остается неясным, были ли эти потери действительно вызваны атаками двойного вывода. Некоторые Биткойн-сайты временно приостановили вывод средств, в то время как проблемы были решены основной командой разработчиков, которая обновила программное обеспечение биткойна и помогла обучить сообщество об «изменяемости» транзакций, которая, при правильном понимании, является особенностью биткойна, а не ошибкой.

Сопrotивление анонимности и цензуре

Сеть биткойнов остается уязвимой для сложного анализа. Meiklejohn et al. (2013) смогли отследить биткойны от хорошо известных краж через сеть до централизованных сервисов, таких как биржи, которые в принципе могут быть вызваны в суд, чтобы раскрыть личности преступников. Они использовали только общедоступные данные; хорошо оснащенное охранительное агентство могло бы еще больше обезличить сеть.

Хотя транзакции не являются полностью анонимными, биткойн представляет собой значительный сдвиг в бремени принудительного исполнения для незаконных транзакций. Поскольку электронные платежи, не связанные с криптовалютой, проходят через финансовых посредников правительства могут вводить ограничения на транзакции, регулируя этих посредников. Наркоторговец, как правило, не может принимать платежи по карте, потому что Visa не одобрит торговца, чей бизнес связан с торговлей наркотиками. Незаконные транзакции биткойнов могут подлежать наказанию,

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

но они не подлежат предварительному ограничению посредством регулирования финансовых посредников.

Будущие разработки в области криптовалютных технологий могут принести полную анонимность биткоину или другой валюте. Zerocash-это одна из предлагаемых систем анонимизации, которая может быть либо добавлена в будущую итерацию биткойна, либо выпущена в качестве собственной валюты. Полная анонимность, обеспечиваемая Zerocash или аналогичной системой, может иметь значительные последствия для правительств, которые полагаются на контроль финансовой системы для обеспечения соблюдения законов.

Ценообразование и изменчивость

Биткойн впервые стоил выше \$1 в феврале 2011 года, \$30 в июне 2011 года, ниже \$7 в июле 2011 года, ниже \$2,50 в октябре 2011 года, поднялся до \$10 на Август 2012 года, до более чем 230 долларов США в апреле 2013 года, упал до уровня ниже 70 долларов США в течение недели и вырос до более чем 1100 долларов США в ноябре 2013 года, прежде чем снова упасть на несколько сотен долларов. Эта волатильная тенденция вызывает вопросы о цене криптовалют: какова фундаментальная ценность биткойна? Почему биткойн так не стабилен? Что может увеличить или уменьшить волатильность биткойна в будущем?

Поскольку биткойн не обеспечен активами, его ценность как валюты может заключаться только в его полезности в качестве средства обмена. Степень будущих сетевых эффектов остается неопределенной, что, возможно, является самой большой причиной изменчивости цен на биткойн. Некоторая часть этих проблем обязательно разрешится со временем, однако биткойн всегда, скорее всего, будет более волатильным, чем фиатные валюты,

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

поскольку у него нет центрального банка, а его предложение не реагирует на изменения спроса.

Криптовалюты также по-новому смотрят на вопросы неопределенности обменного курса. Как заметили Карекен и Уоллес (1981), все фиатные валюты одинаковы: клочки бумаги, которые ни на что нельзя обменять. При режиме плавающих обменных курсов и отсутствии контроля над капиталом, а также при условии, что существует некоторая версия паритета процентных ставок, существует бесконечное количество обменных курсов между любыми двумя фиатными валютами, которые составляют равновесие в их модели.

Вопрос о неопределенности обменного курса является одновременно более и менее важным для криптовалют, чем для фиатных валют. Бумажные деньги в основном одинаковы. Криптовалюты иногда имеют разные характеристики друг от друга. Например, алгоритм, используемый в качестве основы для майнинга, имеет значение – он определяет, насколько профессиональными становятся майнинговые пулы. Еще одним отличием является язык, используемый криптовалютой для программирования транзакций. Ethereum-это новая валюта, которая может похвастаться гораздо более надежным языком, чем биткойн. Zerocash-это еще одна валюта, которая предлагает гораздо более сильную анонимность, чем биткойн. В той мере, в какой криптовалюты отличаются друг от друга больше, чем фиатные валюты, эти различия могут быть в состоянии определить обменные курсы в такой модели.

С другой стороны, неопределенность обменного курса может быть более серьезной среди криптовалют, чем для фиатных валют, потому что легко просто создать точную копию криптовалюты с открытым исходным кодом. Есть даже веб-сайты, на которых вы можете создать и загрузить программное обеспечение для своей собственной криптовалюты несколькими щелчками

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

мышь. Эти валюты совершенно одинаковы, за исключением их названий и другой идентифицирующей информации.

Однако даже идентичные валюты могут отличаться с точки зрения качества управления. В настоящее время биткойн имеет высококачественные институты управления. Основные разработчики компетентны, а сообщества майнинга и пользователей серьезно относятся к тому, чтобы заставить валюту работать. Точному клону Биткойна, вероятно, будет трудно конкурировать с ним, если он не сможет обещать аналогичное высококачественное управление. Когда разразится кризис, пользователи идентичных валют захотят удержать ту, которая, скорее всего, выдержит его. Следовательно, между валютами с идентичными техническими характеристиками, мы считаем, что управление создает нечто близкое к рынку "победитель получает все". Сетевые внешние эффекты очень сильны в платежных системах, и вопрос управления в отношении криптовалют, в частности, усугубляет их.

Заключение

Криптовалюта - впечатляющее техническое достижение, но она остается денежным экспериментом. Даже если криптовалюты выживут, они не смогут полностью вытеснить фиатные валюты. Как мы попытались показать в этой статье, они дают интересную новую перспективу для рассмотрения экономических вопросов, связанных с валютным управлением, характеристиками денег, политической экономией финансовых посредников и природой валютной конкуренции.

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации Эл №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

Список используемой литературы:

1. Блэк, Ф. 1970. «Банковское дело и процентные ставки в мире без денег: последствия неконтролируемой банковской деятельности» 9-20.
2. Фама, Е. «Банковское дело в теории финансов. Журнал денежно-кредитной экономики», 6: 39–57.
3. Холл, Р. Е. «Монетарные тенденции в Соединенных Штатах и Соединенном Королевстве: обзор с точки зрения новых тенденций в денежно-кредитной экономике. Журнал экономической литературы, 20: 1552-6.
4. Карекен, Дж.и Уоллес, Н. «О неопределенности равновесных обменных курсов» Ежеквартальный экономический журнал.
5. Мейклджон, С., Помарол, М., Джордан, Г., Левченко, К., Маккой, Д., Фолькер, Г. М. и Сэвидж, С. 2013. «Пригоршня биткоинов»
6. Накамото, С. 2008. «Биткойн: Одноранговая Система электронных денежных средств»
7. Уоллес, Н. «Теория правовых ограничений спроса на "деньги" и роль денежно-кредитной политики» 1-7.

Дата поступления в редакцию: 18.05.2021 г.

Опубликовано: 18.05.2021 г.

© Академия педагогических идей «Новация».

Серия «Студенческий научный вестник», электронный журнал, 2021

© Сиракян Л.В., Степаненко И.С., 2021