МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСТИТЕТ

имени **М.В. Ломоносова**

Экономический факультет

Финансовый Институт Научных Исследований Современного Трейдинга

«ФинИст»

Конкурсная работа

«Криптовалюты: миф или реальность».

Выполнил: Ерёменко Никита Алексеевич

Научный руководитель: Попов Геннадий Алексеевич

Москва

2019

Оглавление

Введение

Даже в современном мире, с его постоянной изменчивостью, стремительным научным прогрессом, мгновенно рождающимися и забывающимися трендами, криптовалюты остаются очень новой и неосвоенной темой. Внимание, которое приковано к данной сфере жизни, крайне сложно переоценить. Криптовалюты обсуждают на самых высоких уровнях, от частного бизнеса, до правительства государств. Все больше государств явно выражают свою позицию в отношении новой, быстро развивающейся и расширяющейся технологии. Конечно, далеко не все они благосклонно относятся к данному нововведению. Некоторые, такие как Германия, Япония, Хорватия, уже придали им статус законного платежного средства на своей территории. Другие не считают криптовалюты деньгами, называя товаром, активом или имуществом. США, например, приняли ряд законов, обязующих граждан, использующих Биткоин, сдавать налоговую декларацию и платить налоги с осуществления операций с криптовалютой. Россия, Вьетнам, Киргизия – страны, которые пока относятся к криптовалютам крайне негативно. Российский ЦБ назвал Биткоин «суррогатом денег». Во Вьетнаме сразу восприняли криптовалюты как преступную инициативу и официально запретили любые операции с ним как на государственном, так и на частном уровне.

Тем не менее, криптовалюты все глубже проникают в нашу жизнь. Ещё в 2010 году состоялась первая бытовая сделка с криптовалютами: американский программист Ласло Ханьез приобрел за 10 тысяч биткоинов 2 пиццы. Тогда это было всего около 40-50$. Неизвестно, что стало с ним этой осенью, когда курс подскочил до 20’000$ за один биткоин. Отдать 200 миллионов долларов за пиццу сейчас было бы обидно… Тем не менее, прямо сейчас вполне реально купить пиццу за гораздо меньшую сумму, при этом, расплачиваясь криптовалютой. Например, в Лондоне пиццерия Papa John’s официально принимает к оплате Биткоин и Эфириум. Даже в России можно найти заведения, в которых в обмен на криптовалюту можно получить товар. Amazon и EBay уже довольно давно используют расчёты с помощью криптовалют. Ресторан «Valenok» предложит оплату в биткоинах, а добраться

домой поможет сервис такси «Wheely». Недавно с помощью криптовалюты был приобретена недвижимость на 6.5 миллионов долларов. Согласно американскому журналу недвижимости «The Real Deal», покупатель оплатил с помощью Биткоинов около 80% стоимости огромного особняка в Майами.

Но что же обуславливает подобное внимание к теме криптовалют, их быстрый рост и крайне высокую волатильность? Для ответа рассмотрим саму сущность криптовалюты. Мы знаем, что для обеспечения объективной устойчивости валютной системы необходимо, чтобы валюта обладала мерой стоимости. Это долго оставалось необходимым условием. Без этого доверие к валюте рано и поздно утрачивалось.

Но, например, золото обладает четко зафиксированной физической мерой стоимости, доллар США – нет. Он не привязан ни к какой ценности, кроме спроса на него самого по всему миру сейчас доверие к американской валюте фактически обеспечивается только отсутствием существенных конкурентов и крайне широким охватом доллара. Также, некоторые политологи склоняются к мнению, что ценность доллара поддерживается американской армией, которая располагает базами практически во всем мире. Можно, конечно, сказать, что рыночная стоимость доллара США как раз и состоит в затратах на поддержание боеспособности и развитие вооруженных сил, но сложно уловить какую-либо связь. Ничто не сдерживает правительство США от неограниченной эмиссии доллара.

В противовес подобной тенденции, в последнее время, используются альтернативные решения для создания новых криптовалют. Для них доверие является основополагающей характеристикой, при этом, они гораздо более стандартизованы и ближе к существовавшему в прошлом веке «золотому стандарту», чем тот же доллар. Подобным решением и стали криптовалюты. Идеологи криптовалюты, прежде всего, стремились к тому, чтобы полностью отделить новую денежную систему от государства, что гарантировало бы инициаторам транзакций с криптовалютой полную анонимность и неуязвимость.

Помимо определения базовых принципов, перед создателями стояла другая важнейшая задача: реализовать данные принципы на практике. Очень быстро

выяснилось, что ни защищенности, ни анонимности, с помощью существующей банковской системы и наличных расчетов не обеспечить. Иными словами, наличные деньги и деньги на банковских счетах легко отследить, они не анонимны, их возможно подделать, и они облагаются разнообразными комиссиями и налогами, находясь в зависимости от государственной политики. Поэтому основатели криптовалют и обратились к новому и на тот момент сравнительно малоизученному ресурсу: World Wide Web или, просто, Интернет.

Интернет позволил разработать систему, обеспечивающие не только базовые принципы, но целую экосистему, способную обеспечить работу криптовалют и выполнение всех операций с ними.

Таким образом, тема криптовалют является крайне интересной и актуальной. Она взаимосвязана со многими экономическими, правовыми, политическими и социальными аспектами. Именно рассмотрению данных аспектов и уделена большая часть данной работы.

Её цель – выяснить, являются ли криптовалюты комплексным явлением, работающим на практике, научным прорывом, который открывает нам будущее, либо это только искусственно созданный группой инвесторов шум, используемый для личного обогащения узкой группы лиц, состоящих в сговоре, простой миф?

Для достижения этой цели необходимо выполнить несколько задач:

1. Проанализировать различные аспекты проблемы

2. Выяснить, как можно применять криптовалюты на практике

3. Понять, есть ли у криптовалют перспективы, и какие они

4. Наконец, понять, принципы функционирования и отличия электронных денег от фиатных

Как же работает криптовалюта? Начнем с самого простого: структурных элементов технологии и того, как технология работает.

Во-первых, стоит разобраться в том, что такое блокчейн, технологии, которая обеспечивает работоспособность криптовалют. Блокчейн или цепочка блоков - это публичный коллективный регистр, на котором основана вся сеть криптовалют. Все операции и транзакции, одобряемые системой, немедленно внедряются в эту

цепочку блоков. Таким образом, пользователь может узнать, владельцем скольких денежных единиц он является, и какие операции он совершал. А система, в свою очередь, пользуясь данной информацией, способна рассчитать этот самый остаток и подтвердить, что участвующие в транзакциях деньги действительно списываются со счета их владельца. Целостность и хронологический порядок цепочки блоков основаны на надежной криптографии.

Транзакция - это передача средств между счетами клиентов. Информация о каждой такой операции включается в блокчейн. Счета клиентов, часто называемые «кошельками» содержат конфиденциальную информацию, которая называется «секретным ключом», которая используется как подпись человека под каким-либо официальным документом: для подтверждения авторства транзакций, предоставляя весьма достоверное, математическое доказательство того, что транзакция действительно одобрена тем, кому принадлежит «кошелек». Такая «электронная подпись» способна и заблокировать изменение транзакции уже после её выполнения и размещения в цепочке блоков. Все транзакции сразу разносятся по всей сети между другими клиентами, после чего осуществляется процесс подтверждения операции. Он занимает довольно продолжительное, впрочем, постоянно снижающееся время – около 10 минут. Это происходит за счет оптимизации существующей системы с помощью новых технологий. Процесс обработки транзакций в ходе проверки называется «майнинг».

Майнинг – это не только сам процесс, но и целая «распределенная» система, которая необходима для подтверждения транзакций и дальнейшего включения их в цепочку блоков. Именно он обеспечивает хронологический порядок операций в блокчейне, нейтральность этой сети, и, наконец, позволяет устройствам, составляющим систему определить общее состояние системы. Таким образом, чтобы транзакция была одобрена, её необходимо поместить в удовлетворяющий специфическим криптографическим условием блок, который затем будет проверен всей сетью. При этом сеть защищена от возможных ошибок и отклонений «правилом пятидесяти»: система не сочтет блок одобренным, если в ходе подтверждения его подлинность не заверят 50% всех устройств. Это правило, также не позволяет

вносить любые изменения в предыдущий блок, иначе все последующие блоки цепочки становятся «инвалидными», неподтвержденными. Более того, в ходе майнинга образуется, фактически, лотерея, которая исключает какую-либо возможность клиентских последовательных операций в цепочке, инициированных одним заинтересованным пользователем. В результате, никто не способен подчинить всю цепочку блоков или модифицировать её по частям для подмены транзакций или отказа.

1. История

1.1. Появление концепции криптовалюты

Итак, вернемся лет на 10 назад. Именно тогда привычные для нас деньги стали понемногу становиться «цифровыми», когда стало возможным практически повсеместно расплачиваться карточкой, вообще не имея наличных денег. Почти каждый банк теперь предлагает виртуальные счета, которыми можно управлять прямо со смартфона. Постепенно происходило развитие виртуальных платформ, валюты обзаводились своими интернет-формами, проникая в нашу жизнь глубже и глубже. Наконец, были изобретены полностью независимые от материального мира криптовалюты. Конечно, использовать криптовалюты не так просто, как «перекинуть» всю наличность на карточку Visa или MasterCard, и уж, тем более, сложнее, чем использование PayPal с Apple Pay. Ведь различия между используемыми сейчас сервисами платежей и криптовалютами настолько глубоки, что подчас не понятно, в чем состоит преимущество криптовалют.

Тем не менее, являясь Интернет-ресурсами, криптовалюты стремительно расширяют свое влияние и круг пользователей. Чувствуется и растущее воздействие криптовалют на материальный мир. Регулярно можно наблюдать основание новых сервисов, связанных с криптовалютами. Магазины, кафе, даже частные лица начинают принимать «крипту» в качестве оплаты. Вполне возможно, что настанет то время, когда мы будем рассматривать криптовалюты как нечто абсолютно обыкновенное и тривиальное.

1.2. История первых криптовалют

1.2.1. История «Биткоин»

Вокруг данной валюты за почти десять лет её существования сформировалась собственная субкультура, а само слово «Биткоин» стало нарицательным и приобрело практически сакральное значение. Думаем «криптовалюта», говорим «Биткоин». Да, мифология биткоина обзавелась огромным количеством знаковых людей и событий. Это и Сатоши Накамото – неизвестный создатель криптовалюты, которого никто никогда не видел, это и легендарная покупка пиццы за деньги, сравнимые с ВВП небольшой страны по текущему курсу биткоина, это и огромные колебания цен на валюту, неоднократно переживавшую резкие взлеты и периоды глубокой коррекции. Можно вспомнить и то, как обвалилась биржа «Mt.Gox», считавшаяся одной из самых важных на всем рынке криптовалют. Все это влекло кражи в колоссальных объемах. Были и комичные ситуации, вроде потери более чем семью тысячами биткоинов. Наконец, уже после ухода Накамото из проекта, участие в разработке ПО биткоина смог принимать практически любой желающий, разбиравшийся в принципах системы. Не стоит недооценивать и влияние нового интерфейса J, все растущее количество неподтвержденных транзакций и лихорадочный поиск альтернатив. Так и запомнилась в медиа-пространстве история валюты.

Но разберем все по порядку.

«Биткоин 0.1» впервые был опубликован 9 января 2009 года. Версии с 0.1.0 по 0.1.5 были доступны только для «Windows 2000», «Windows NT» и «Windows XP». Но практически сразу после релиза первой версии, Накамото выпустил несколько обновлений, призванных усовершенствовать систему, защитить её от сбоев и оптимизировать для стабильной работы. В результате его работы были исправлены несколько критичных ошибок системы, а также, благодаря, в том числе, сторонним программистам, клиентский интерфейс стал понятнее и доступнее в пользовании.

После этого, в 2009 году, Накамото выпустил релиз «Биткоин 0.2», адаптированный под ОС Linux. Данная версия вносила крупные изменения в процесс майнинга: раньше в биткоине использовалась монопоточная обработка генерируемых блоков, а с выходом новой версии она уступила место многопоточной. В результате, майнинг стал возможен не только теоретически, но и

практически с учетом всех возможностей современных многоядерных процессоров – Quad и Duo от Intel. Также, с этого момента SON RPC с использованием API-протокола. Данное нововведение разблокировало для служб, не входящих в систему, возможность подключиться к ней и взаимодействовать с ней. Биткоин тогда был известен только в узких кругах, но уже тогда наметились первые тенденции в росте: еще в августе 2009-го темпы роста валюты превысили темпы американской и европейской инфляции. В ноябре был сделан релиз Bitcoin talk – форума, на котором заинтересованные лица могли договариваться о транзакциях и обмениваться советами. В результате – всплеск популярности и основание множества инициативных групп программистов, желавших усовершенствовать систему.К сожалению, тогда же открылись и проблемы: Биткоин содержал в основе несколько уязвимостей, за что подвергся критике. Некоторые участники отвернулись от проекта и при обсуждении идеи комиссии за транзакции. «Биткоин 0.3» принес много важных обновлений: эффективную добычу блоков с помощью графических процессоров. Началось время «майнеров» Эти люди собирали из видеокарт своеобразную «ферму», использовавшуюся для получения биткоинов практически в промышленных масштабах. Тогда же обнаружилась и критическая ошибка: существовала возможность обойти проверку операций вместе с ограничениями системы на количество генерируемых биткоинов. Около 200 миллиардов биткоинов было похищено хакерами. Этот случай стал и до сих пор остается единственной уязвимостью, приведшей к реальному изменению структуры цепочки.

Другой стороной медали стала своеобразная лотерея майнинга: пользователи в азарте буквально боролись за право найти очередной блок, чего у некоторых не получалось неделями. Это привело к появлению своеобразных коалиций – «пулов», в которых распределение вознаграждение шло пропорционально. Первым из них стал Slus’s Pool.

Идея развивается и по сей день, оставаясь простейшей в своей сути: «майнить вместе выгоднее, чем по одному».

Перед наступлением нового, 2011 года, Сатоши Накамото выпустил «Биткоин 0.3.9», ставший прощальным подарком сети, которую он создал. Затем он буквально исчез из разработки проекта, временно создав небольшую панику среди разработчиков. Впрочем, они быстро преодолели этот кризис, и 2011 год принес биткоину множество экспериментов и улучшений. Сеть была и остается децентрализованной, но было принято предложение создать четкую структуру взаимодействия разработчиков, BIP. Автором этой идеи был Amir Taaki, написавший первый алгоритм 19 августа.

Впрочем, не все идеи было способно реализовать в рамках проекта. Начинается массовое создание валют, в которых создатели экспериментировали с основными параметрами выпуска блоков – их количеством, максимальным вознаграждением и скоростью выпуска. Тогда же был введен принцип PoW/PoS, позже развившийся в отдельную криптовалюту. Чуть позже, Алан Рейнер реализовал BIP 0010. Этот протокол описывал важное преобразование сети, предлагавшее транзакции, подписанные не одной, а несколькими крипто-подписями. Каждая должна была быть связана с уникальным хеш-ключом для обеспечения доступа нескольких клиентов к единовременной транзакции.

В 2012 году биткоин достиг широчайшего уровня известности. О нем заговорили на телевидении, политики начали обсуждать взаимодействие государственных систем с новой неиндексируемой криптовалютой.

Сам Биткоин, тем временем столкнулся с проблемой своего колоссального размера: ошибки, потери данных, неподтвержденные транзакции – всё это серьезно ограничивало стабильность системы. Решение было предложено в 16-м BIP. Пакет корректировок перекладывал ответственность за оформление условий сделки на самих клиентов. Это снизило нагрузку на сеть и увеличило скорость прохождения транзакций. Сторонние разработчики внедрились в Биткоин не только из числа энтузиастов, но и из крупного бизнеса: Программисты, юристы, экономисты - все они искали в Биткоин новую глобальную систему и желали вывести её на мировую арену. Именно в 2012 году Биткоин подошел ко множеству своих ограничений, не связанных с вычислительными мощностями, а с фундаментальными принципами.

Количество желающих войти в систему настолько превышало число доступных блоков, что курс стремительно пошел на повышение. Тогда же началась вторая волна создания альтернативных криптовалют, принявшая максимальные масштабы в следующем, 2013, году.

Хотя Биткоин и по сей день остается криптовалютой «номер 1», его положение нельзя назвать монополией: существует несколько крупных проектов, глубоко отличающихся от биткоина, но занимающие крупные доли рынка и привлекающие множество клиентов.

Сейчас один Биткоин можно приобрести за примерно 9500 долларов.

1.2.2. История «Ethereum»

Ethereum (эфириум в России) — это, на текущий момент, криптовалюта «номер 2». Она прочно заняла место за биткоином, оценочная стоимость капитализации – более 20 миллиардов $, что всего в 2 раза меньше суммарной стоимости биткоинов. «Эфир», или «Ether» - название одной единицы валюты. Проекту всего около 5-ти лет, но он уже составляет такую серьёзную конкуренцию и вышел в лидеры рынка. Как это возможно?

Рассмотрим историю проекта:

Виталий Бутерин – молодой человек, житель Коломны, представил проект в 2013 году. Он еще с самого зарождения Bitcoin интересовался проектом и даже являлся одним из основателей журнала «Bitcoin Magazine». Фактически, в проекте Ethereum он воплотил свое представление о 2nd-gen платформе криптовалют.

Особенностью платформы является хитрая платформа смарт-контрактов. Сам Виталий приводит такой пример: «рассмотрим простую ставку на спорт: допустим, два пользователя делают ставку на исход какого-либо футбольного матча. После его завершения выполняется смарт-контракт и происходит автоматическое распределение выигрышей, согласно заданному алгоритму».

Ethereum в 2014 году стал объектом масштабного крауд-сорсинга, в результате которого удалось собрать более тридцати тысяч биткоинов. Это позволило создателю собрать крупную команду и в 2015 году – 30 июня выпустить первый блок, ставший основой цепочки Ethereum. Эта цепочка имела первый номер и

называлась «Frontier». Ethereum не только добился признания среди пользователей, но и заинтересовал крупных инвесторов, вплоть до Microsoft.

К моменту введения новой цепочки, названной «Homestead», работавшей по новой схеме, эфир стоил уже в десять раз больше, чем на начало года: 14 марта 2016 капитализация всей сети оценивалась в 1 миллиард долларов.

Но Ethereum не был неуязвим: внутри системы организации сбора средств на развитие сети, которая подверглась атаке, в результате которой почти треть всех средств была переведена на счета хакеров. Курс немедленно отреагировал падением в полтора раза.

Существовало два пути: хардфорк (вскрытие алгоритма для внесения модификаций в уже записанные блоки) и блокировка средств фонда. Ethereum раскололся, так как часть пользователей не могла смириться с изменением оригинальной цепочки и считала это нарушением базовых принципов конфиденциальности, обвиняя не хакеров, а создателей в бездействии перед уязвимостью.

Хардфорк имел достаточно тяжелые для сети последствия: курс стал снижаться, достигнув в декабре 2016-го исторического минимума в 7 долларов.

К счастью, уже с 2017 года эфириум оттолкнулся от дна и вновь вернулся к стабильному росту. Особенно это было заметно на фоне кризиса Биткоин, страдавшего от неподтвержденных транзакций и 2-х дневного периода ожидания выполнения транзакций.

В результате Etherium поднялся до 200$, с 25 марта до 30 мая, увеличившись в 4 раза.

Теперь Ethereum готовится к очередной смене протокола: «Casper» станет новой вехой в истории эфириума, внося PoS метод в систему. В январе 2018 Etherium перешел барьер в 1000$ и достиг пика в 1386$, упав до 83$ на фоне хардфорка и общего спада всех криптовалют. Сейчас его можно приобрести за 175 долларов.

1.2.3. История «Ripple»

Ripple претендует на звание самой первой криптовалюты: его история разделяется на два крупных этапа. Первый – это этап создания проекта, начавшийся еще в 2004-м. Ripple был создан как новый способ осуществления расчетов, не проходящих через банковскую систему. Райан Фугерр оформил одноранговую сеть, в которой каждый участник мог проводить транзакции, основываясь на доверительной цепочке пользователей. Цепочка, в свою очередь базировалась на криптографическом алгоритме, генерировавшим цепь посредников случайным образом. При этом, существовала особенность в виде «кредитных линий» - прямая связь между пользователями, работающая без какого-либо влияния всемирной банковской системы. К сожалению, Фугерр не обладал достаточными инвестициями для пиара системы, и проект был практически забыт до 2011 года. Развитие Биткоина и его несовершенство привлекло внимание инвесторов к другим перспективным проектам, и Ripple снова оказался актуален. Он имел глубокие отличия от большинства криптовалют, торговавшихся на рынке. Огромные фонды, собранные инвесторами, целиком пошли на развитие системы. Это подарило Ripple фактически, «второе дыхание». Криптовалюта разработала собственную систему подтверждений – «Ripple protocol consensus». Партнерами Ripple сейчас являются крупнейшие банки Японии, ОАЭ, даже Google. Наконец – уникальной особенность Ripple является отсутствие майнинга – блоки вычислены и происходит исключительно их перезапись участниками, которым отдан карт-бланш на эмиссию собственных ripple-монет. Система очень интересна и самобытна. Ripple прочно занял место третьей криптовалюты после Bitcoin и Ethereum. Сейчас Ripple имеет капитализацию в 25 миллиардов $ и торгуется на уровне в чуть менее 4RPL за 1 доллар.

2. Цифровая основа криптовалюты

2.1. Блокчейн-технология

Blockchain – это цепочка блоков информации. Блоки имеют фиксированный объем данных. Каждый блок цепочки содержит определенную однородную информацию.

На практике система реализуется очень интересно: во-первых, она

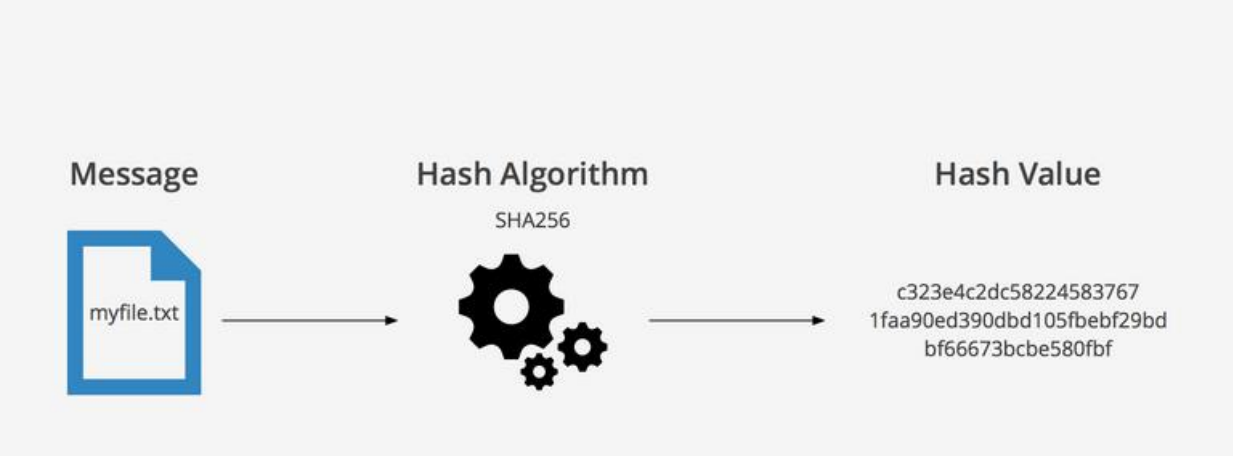
децентрализована. Вся цепочка есть у каждого пользователя системы. Это значит, что если происходит какое-либо изменение цепочки, оно происходит для каждого пользователя. В результате, у каждого клиента есть история всех транзакций системы. И один пользователь не сможет внести какие-либо изменения без одобрения остальных: он не сможет записать какие-либо данные в цепочку, чтобы данная операция не отразилась на блокчейне других пользователей. Разумеется, на практике одобрение операции производит не пользователь по собственному желанию, а компьютерный алгоритм, сверяющий параметры транзакции с определенными критериями. Соответственно, в разных алгоритмах, запись и проверка блоков Blockchain может осуществляться по категорически разным принципам.

2.2. Примеры алгоритмов реальных валют

2.2.1. SHA-256

Как происходит оформление нового блока? Существует стандартная Хэш-функция. На вход она получает блок, который содержит информацию. На выходе получается некое значение, которое невозможно предсказать и подвергнуть обратной операции. Функция подобрана так, что для нахождения аргумента функции можно использовать только подбор случайных значений. Этот аргумент и станет хэш-кодом.

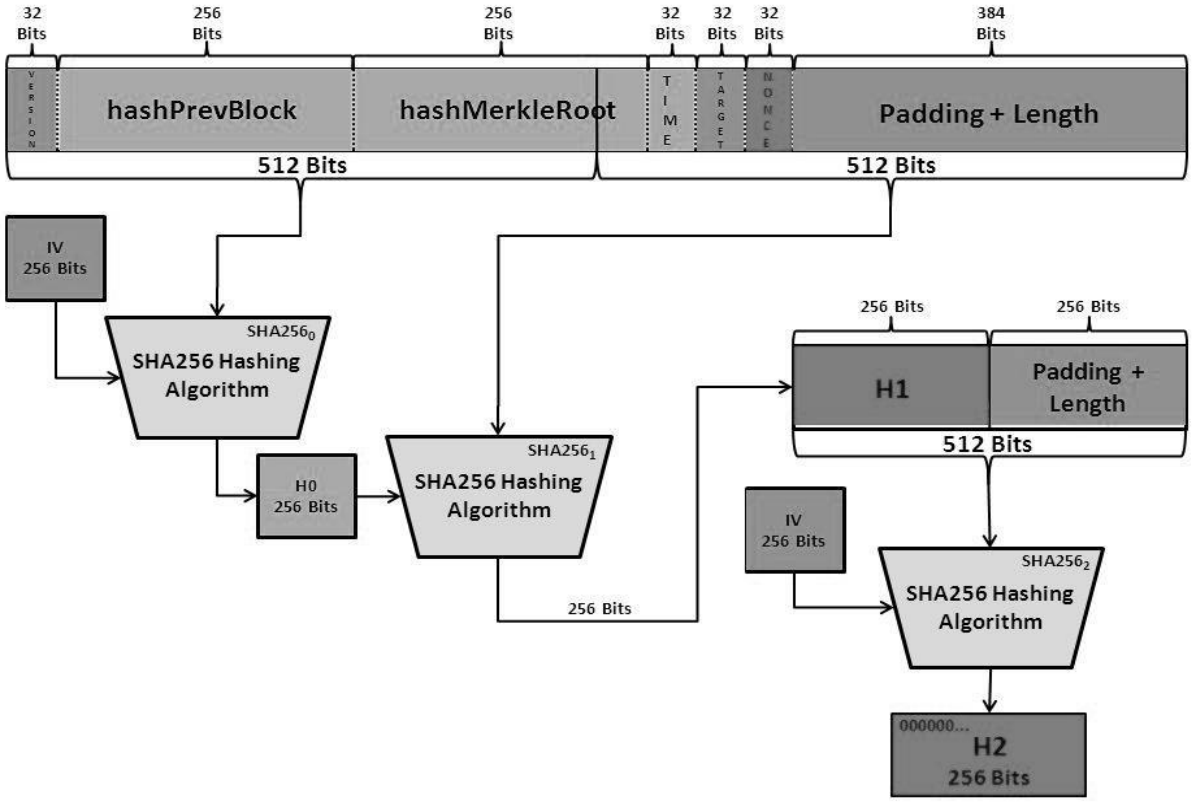
См. рис.1 – пример операции SHA-256. (www.slideshare.com/joejiang - implementation of BTC)



Одним из самых популярных методов дешифрации подобных блоков, считается SHA-256. SHA-256 получил широкое распространение в связи с использованием в Bitcoin.

Там используется специфический критерий: правильный хэш-код имеет некоторое количество нулей в начале. В результате, устройства для его поиска должны обработать 1.5*10^20 значений.

См. рис. 2 – схема работы SHA-256 (www.slideshare.com/joejiang - implementation of BTC)



Как можно видеть, протокол SHA с помощью хэширования производит преобразование 512 бит информации в 256 бит, являющиеся хэш-кодом. Алгоритм работает по принципу Меркла-Дамгарда: входящая информация делится на блоки информации, образующие «положение», а оно, затем, на 16 «слов».

Разработан алгоритм был в АНБ. Релиз первой версии состоялся в 2002 году. Затем, с учетом стандартов безопасности США была создана вторая версия, что произошло в 2005 году. Далее лицензия Royalty-free, распространявшаяся на это ПО в течение 3-х лет позволило пользователям использовать эти наработки для собственных проектов.

Интересен факт, что сейчас любой сайт, имеющий SSL стандарт безопасности, использует алгоритм SHA-256 и каждый является пользователем данного алгоритма в целях защиты собственных данных.

Характеристики алгоритма:

1. V блока – 512 bit
2. Длина сообщения – 33 byte
3. Длина внутреннего положения – 32 byte
4. V дайджеста сообщения – 32 byte
5. n итераций – 64
6. Скорость обработки – 8Mb/s

В чем же состоят недостатки такой, на первый взгляд, удачной системы? Ошибки не были обнаружены даже при тщательных исследованиях в Агентстве Национальной Безопасности. А уже в 2008 году индийские программисты отыскали критические схождения блоков в 22 итерациях алгоритма. Более того, усовершенствовав свой способ, они добились ошибки уже в 32 итерациях хеша.

Как же происходит такая проверка?

Алгоритм подвергают нескольким последовательным атакам: поиск формулы рехеширования – это нахождение прообраза аргумента функции по её хэш-коду, и поиск критических сближений – «коллизий» - практически идентичных выходных параметров при разных входных. В случае невыполнения одного или нескольких таких условий возникают возможности получить данные чужого положения и доступ к его информации.

В результате этого исследования, алгоритм хеша SHA-256 будет пользоваться другим протоколом. Его назвали «Keccak».

Анализируя текущее применение SHA-256 можно сделать вывод, что он не обеспечивает достаточной защищенности при текущих масштабах использования. Огромное количество «майнеров» сейчас зарабатывают биткоины, занимаясь взломом данного алгоритма, и основывают целые фермы, дающие намного более существенную эффективность. Эта практика угрожает базовым принципам децентрализованной сети, консолидируя крупные объемы «крипты» у основных

потребителей, в связи с чем увеличивается разрыв между начинающими майнерами и специализирующимися на этом индивидами и корпорациями.

По протоколу SHA-256 работает около половины рынка криптовалют. Он не является лучшим, но его сбалансированность, обилие применений и статус первого позволит ему сравнительно долго занимать эту существенную долю. Конечно, существуют и другие, более перспективные алгоритмы, которые тоже было бы неплохо рассмотреть.

2.2.2. PoW/PoS

Proof of Work и Proof of Stake никогда не были известны широким массам пользователей. Тем не менее, с ростом популярности криптовалют, эти методы становятся все более важны для потенциальных инвесторов криптовалютного рынка и специалистов, желающих разобраться в этом вопросе самому.

Proof of Work - это «доказательство работы», если переводить напрямую. Фактически, работой считается количество операций, которые устройство пользователя совершает в процессе вычисления блока. Соответственно Proof of Work – прямое условие того, что пользовательский ПК действительно совершил определенную вычислительную работу.

Сейчас этот протокол реализован в сети Bitcoin для подтверждения всех операций цепочки данных. Помимо биткоина, PoW лежит в основе алгоритмов майнинга огромной доли криптовалют на рынке.

Альтернативным решением является «Proof of Stake». Точного перевода найти нельзя, но Stake здесь – это процент, ставка или доля. Протокол подтверждает, что клиент обладает некой долей блоков и при прохождении транзакций по сети вероятность, что именно пользователь с более высокой долей получит новый блок и одобрит транзакцию, становится выше.

Протокол Proof of Work был запушен еще задолго до появления Bitcoin и даже Ripple. Он использовался для того, чтобы отражать различные хакерские атаки количеством однообразных запросов (DDos, спам). Вручную, отлавливать отдельные адреса и блокировать – невозможно. Но Proof of Work способен облегчить

эту задачу для сервера и позволить ему игнорировать запросы, не проходящие сквозь его алгоритм валидации.

Идея PoW была анонсирована аж в 1993-м. Авторами данной научной статьи были Синтия Диор и Моне Наор. Они предлагали ограничивать доступ к ресурсам до момента выполнения определенной задачи, требующей серьезного, сложного вычисления. Через 3 года Адамом Бэк реализовал программу Hashcash, защищавшую устройство или сервер от назойливых сообщений. В его интерпретации механизм должен был работать по следующему алгоритму: «Для запроса нужно найти аргумент функции SHA(x), результат которой содержит определенное количество пустых ячеек в начале».

Затем, в 1999 году был первый раз озвучен термин «Proof of Work» – Маркус Якобсон и Эри Джуэлс ввели его при написании статьи для издания Communications and Multimedia Security. Хэл Финни, в свою очередь, предложил монетизировать протокол Proof of Work. Именно этот человек осуществил первую транзакцию в сети биткоина. В результате работы RPoW «Reusable PoW», который он предложил, появлялось определенное вознаграждение пользователю, которое, затем, можно бы было конвертировать в деньги. Это довольно примитивная интерпретация функционирования современных криптовалют.

А уже потом на первый план выходит проект Satoshi Nakamoto, в чью основу легли все эти принципы. От работы протокола PoW зависит генерация каждого нового блока цепочки и защита всей Blockchain сети в целом.

Работает это так:

В блоках записан хеш-код, майнеры ищут аргумент функции. При этом, хэш-сумма кода всегда меньше аргумента, что является критерием для PoW. Пользовательский ПК осуществляет вычисления и алгоритм PoW, подтверждая эту работу, дает команду на запись очередного блока в цепь. Система также способна модифицировать уровень сложности вычислений: при добыче всех блоков в течение 2-х недель, сложность алгоритма увеличивается, чтобы снизить скорость добычи. С другой стороны – протокол Proof-of-Stake был анонсирован уже с изобретением криптовалют и в процессе их разработки и был сформирован. Это произошло на

мероприятии BitcoinTalk в 2011-м. QuantumMechanic – один из пользователей сети сделал релиз PoS в виде замены для Pow, используемого в blockchain системе биткоина.

Валюта Peercoin стала первопроходцем в области применения PoS. Несмотря на то, что PoW также имел в ней применение (во время предварительного распределения средств - при их обмене подключался PoS).

В PoS аргументом валидации транзакции служит размер доли «Stake», определяющий конкретный узел, получающий право на осуществление транзакции и вознаграждение за нее. В результате – пропуском в майнинг является количество коинов на счету.

В чем же вообще преимущество?!

Причина такого подхода – снижение использования ресурсов на обработку транзакций (значительно ниже PoW)

К тому же, в системе необходимо концентрировать не 51% вычислительных мощностей, а 51% всех средств в системе – что практически невозможно и безумно затратно. Даже при завладевании такими объемами, сеть будет нарушена и хакеры не смогут использовать ситуацию себе на пользу.

Наконец, комиссии в системе, особенно в длительном периоде должны сильно снизиться за счет низкой затраты мощностей и менее ресурсоёмких операций.

2.3. Возможные операции с криптовалютой.

Для понимания круга операций можно подробнее представить, чем является транзакция. Транзакция – разовая операция передачи пакета данных между пользователями сети.

Данные транзакции могут принимать практически любые виды. Большая часть транзакций – списание единицы валюты с одного счета и зачисление на другой. В результате процесса формируется и другая операция – снятие комиссии. Комиссия образуется за счет затраты некоторых пользователей сети вычислительных мощностей на обработку транзакции и её запись в блокчейн. Помимо транзакций и комиссий, сеть способна реализовать и передачу средств между платежными системами, странами, территориями и нейтральными водами. Деньги на вашей

карточке не способны быть переведены без крупной комиссии в банк другой страны. Вам или потребуется лично прибыть на место, либо заплатить обоим банкам за осуществление данного перевода.

Одной из главных операций над криптовалютами остается их хранение – средства для этого практически не затрачиваются, в то время, как курс большинства валют растет в разы быстрее темпов инфляции в большинстве стран (даже в Зимбабве, иногда). Это позволяет пользователям реализовывать накопительную функцию данных средств, что позволяет многим специалистам считать Биткоин и другие криптовалютами не деньгами, а активом, приносящем прибыль. Наконец, очень важной операцией остается майнинг. В ходе данной операции происходит создание нового валидного блока в цепочке данных. Соответственно, в ходе вычисления хеша определенного значения используется вычислительная мощность, которую предоставляет майнер, получая вознаграждение. При этом, в ходе данного процесса необходимо получить результат, который был бы меньше максимального возможного значения хеш-функции за вычетом значения сложности. Для этого на устройстве майнера происходит процесс подборки оптимального массива байт, получаемого из совокупности всех полей очередного блока, хеш-значение которого будет совпадать с известным значением у нового блока. В результате, в связи с равномерным распределением вероятности качественных хеш-функций данная операция может повторяться от одного до нескончаемого множества раз.

Тот же майнер, который нашел верный массив, немедленно включает блок со всеми его транзакциями в цепочку, тем самым рассылая его в системе, а сам получает вознаграждение и комиссию за транзакцию. Фактически, в самом блоке и будет закреплен владелец очередной награды с комиссией – ведь блок состоит не только из суммы, но и из электронной подписи создателя. В результате, майнинг незамедлительно вознаграждается системой, что сохраняется в цепочке блоков и учитывается в последующих её обновлениях. Вообще, с помощью майнинга пользователи обычно увеличивают свои счета и используют эти средства для вывода в материальный мир, о чем стоит подробнее рассказать в следующем пункте.

2.3. **Криптовалюта с точки зрения трейдера.**

Прежде, чем погружаться в использование различных криптовалют с целью получения прибыли, необходимо осознать, что, хотя цифровые деньги значительно отличаются от привычных биржевых товаров, они по-прежнему являются разновидностью финансовых активов.

Одной из ключевых особенностей данного инструмента до сих пор является низкая степень контроля за данным сектором торговых отношений и в целом невысокой проработкой вопроса в законодательстве, где многие термины оформлены неконкретно и расплывчато. Кроме того, на функционирование криптовалютных бирж в значительной мере влияет децентрализованность систем коинов, обращающихся на крипто-рынке.

В совокупности эти факторы могут стимулировать некоторых участников торгов на оппортунистическое поведение. Если на реальной бирже существует возможность оспорить правомерность сделки и доказать факт манипуляции, то на бирже криптовалют часто отсутствует сам регулятор, к которому можно обратиться с таким запросом. Ярким примером недобросовестного поведения контрагентов являются события, развернувшиеся на русской бирже Yobit вокруг Chill Coin, Magi Coin и UBQ: группа трейдеров по предварительному сговору скупают некоторые объёмы малоизвестных коинов, после чего параллельно начинают рекламную кампанию, создавая «хайп» и привлекая сторонних инвесторов, что взвинчивает цену на криптовалюту. После определенного уровня цены участники сговора избавляются от своих активов, прекращая информационную поддержку криптовалюты, после чего цена возвращается на изначальный уровень и в убытке оказываются инвесторы второй волны.

С другой стороны, именно криптовалюты являются самыми волатильными активами на сегодняшний день. Разницу может легко заметить даже далёкий от финансовых инструментов человек. За день курс валюты может меняться почти на 40% в зависимости от определенных условий, а колебания в пределах 10% вообще, фактически, нормальны, особенно не для основных коинов. Впрочем, волатильность в основном, необходимо учитывать либо в крайне краткосрочном периоде до 1-2 дней, либо уже в более долгосрочных периодах, начиная от одного месяца и более:

в рамках нескольких недель может наблюдаться однонаправленное изменение котировок исключительно за счет установившегося тренда. Таким образом, если мы желаем составить стратегию и просчитать прогноз, то лучше воспользоваться именно более длинные периоды, такие как квартал.

Волатильность зависит от множества показателей. Так для вычисления ожидаемой волатильности криптовалюты аналитиками используется текущая цена на коин, историческая волатильность, настроение на рынке криптовалют, капитализацию проекта, его доходность, ликвидность и актуальность, а также даже новости о рынке криптовалют в целом и выбранном коине в частности.

Хорошо это или плохо? Скорее, для долгосрочного инвестирования эффект будет негативным, оказывая эмоциональное давление на трейдера, для которого каждый день наблюдать изменение прибыли на десятки и, подчас, сотни процентов будет слишком волнительно. Но в краткосрочном периоде можно значительно изменить свое финансовое состояние благодаря столь резким колебаниям.

Проблемой для трейдера в данном случае будет информация. Всё, что даже косвенно касается криптовалюты может повлиять на её курс. Владельцу данного актива необходимо почти буквально «держать руку на пульсе» и обладать хорошей реакцией, усиленной стабильным интернетом. Обещания разработчиков могут подстегнуть криптовалюту на несколько процентов почти мгновенно, а в случае, например, хардфорка, котировки могут обрушиться меньше, чем за несколько минут после публикации сообщения.

Наконец, необходимо учитывать, что, если фиатная валюта обеспечивается показателями экономики страны-эмитента, либо драгоценными металлами, обыкновенная акция помимо реальных дивидендов даёт возможность влиять на деятельность компании, и даже фьючерс после истечения его срока может быть погашен с обменом на акцию, криптовалюта не имеет реального обеспечения. Её цена обуславливается исключительно доверием контрагентов к валюте и друг к другу. Соответственно, на неё проще повлиять различного рода сообщениями и новостями.

Стоимость криптовалюты, как таковая, тоже фактически не существует. Не существует никаких объективных свойств, которые обуславливали бы стоимость коина на бирже.

В итоге мы имеем высокорисковый, высоковолатильный, высокодоходный актив. Соответственно трейдер либо инвестор оценивает возможные преимущества и недостатки данных особенностей финансового инструмента. Очевидно, новичку, который желает иметь стабильный уровень прибыли со спекуляции на финансовом рынке подойдут разве только наименее волатильные и наиболее прогнозируемые из криптовалют. Тем не менее, по мере развития навыков трейдинга и приобретения опыта, придет и умение грамотно воспользоваться изменчивостью цены на актив, чтобы быстро заработать на столь активном рынке. Безусловно, рассматривая варианты инвестиций и получения прибыли за счет трейдинга, стоит обратить своё внимание на криптовалюту.

3. Взаимодействие криптовалют и материального сектора.

3.3. Использование криптовалют в странах мира

3.3.1. Национальные проекты криптовалют

Рынок криптовалют за последние несколько лет подрос в разы. Стремительное развитие и глубокие потрясения – это было характерно для большинства криптовалют на рынке. Постепенно государства осознали неоспоримые преимущества криптовалют, после чего во многих государствах появились проекты криптовалют, имевших Blockchain в базе системы и являющиеся, по сути, национальными аналогами всем известных Bitcoin, Ethereum, Ripple и другим.

Стоит заметить, что самое пристальное внимание к этой теме обращают страны, в данный момент находящиеся под санкциями. Условия международных санкций ограничивают экономические возможности государства, и решение данной проблемы может находиться в обходе данных ограничений с помощью криптовалют. Звучат и заявления, что развитие подобных решений в широком ряде стран способно инициировать масштабное преобразование международной

банковской системы. Причём ряд из них высказывают мнение, что реализация подобных инновационных цифровых проектов послужит толчком к бесповоротному изменению существующей международной валютной системы.

Например, недавно первый проект национальной криптовалюты был реализован президентом Венесуэлы – Николасом Мадуро. Валюта получила название «El Petro» и её интересной особенностью является факт, что каждая единица валюты имеет обеспечение в виде одного барреля нефти. Правительство считает, что подобная схема сможет разрешить зависимость Венесуэлы от долларов США и привлечь внешних инвесторов вкладываться в экономику страны. Согласно Николасу Мадуро, El Petro с самого начала продаж показала высокие показатели, и президент удовлетворен испытаниями. Таким образом, сейчас стоит проследить за развитием данного Blockchain проекта и удостовериться, что валюта действительно привлекает зарубежные инвестиции. Ведь при успехе El Petro действительно может послужить замечательным примером для остальных стран. О начале работ над схожими проектами заявили правительства Ирана и Турции.

В Швеции обнаружилась другая причина перехода на криптовалюту. Наличные деньги в стране практически не используются. В большей части сферы обслуживания наличность в принципе не принимают, т.к. комиссии весьма высоки. В той связи центральный банк Швеции рассматривает вероятность успеха собственной разработки - криптовалюты «E-Krona». Данная валюта призвана конкурировать с частными криптовалютами, распространенными на территории страны.

Россия же выводит идею криптовалюты на более глобальный масштаб: Центробанк Российской Федерации вступил в переговоры с Индией, Китаем, Бразилией и республиками средней Азии о разработке криптовалюты, которая будет использоваться в странах БРИКС и ЕАЭС. Данное предложение способно сильно поменять расстановку сил в мире, но, тем не менее, проект имеет смутные перспективы: Казахстан уже имеет проект национальной криптовалюты KZcash, который готов к размещению на международных биржах, а Китай имеет планы по выпуску валюты на базе Народного Банка Китая, совместно с ЦБ Китайской

Республики (Тайвань) и частным бизнесом. Это заявление было сделано Фан Ифеем, вице-президентом Народного Банка.

В чем польза национальных криптовалют для государств?

Существует и другой актуальный вопрос, имеющий тот же ответ: Можно ли считать валюты, принадлежащие правительству страны – настоящими криптовалютами? В базовых принципах криптовалют всегда называли анонимность и децентрализованность. Тем не менее, Blockchain не противоречит возможности сосредоточить управление криптовалютой в одном центре. Более того, государство будет способно очень четко проконтролировать эти деньги, так как каждая транзакция будет записана в цепочке блоков и доступна для контроля.

Таким образом, тенденция очень прозрачна. Национальные криптовалюты будут развиваться, за ними, возможно, и есть будущее: эти проекты сочетают в себе весомые преимущества как для государств, так и для пользователей. Ведь это позволит избавиться от возможности уклониться от уплаты налогов, взяток и разнообразных финансовых мошенничеств. Каждую транзакцию можно будет не только проверить, но и отменить в случае правонарушения. Другим примером применения национальной криптовалюты может служить её использование для обхода санкций частными компаниями и банками страны.

Глобальная финансовая система, сейчас испытывающее сильное влияние Запада, имеет основание в виде свода законов и правил, которые отлажены в течение многих лет на международной арене. Они четко регулируют осуществление торговли между странами и их экономические отношения. Если же многие страны будут переходить на собственные криптовалюты, то это подорвет влияние доллара США на международной арене, а вместе с ним и традиционных институтов мировой системы, например, Европейского Центробанка.

Таким образом, создание и развитие, проектов национальных криптовалют приведет в долгосрочном периоде к реформации всей мировой финансовой системы и появлению нового, полностью независимого принципа экономических взаимоотношений. Результатом столь глубоких преобразований станет падение

влияния Запада на отдельные экономики и позволит государствам индивидуально создавать свое будущее.

3.4. Правовое регулирование криптовалют

Несмотря на неоспоримые преимущества, для криптовалют все еще не определен их финансово-правовой статус. На этот счет существуют два противоположных мнения о ее сущности: либо это новый вид электронных денег, созданный в связи с реализацией технологий высококачественной трансляции информации, либо это лишь замена для денег, актив, имеющий доходность, являющийся временным экономическим феноменом и не имеющий особых перспектив в своем развитии. Определение направленности в данном вопросе приведет к одному из исходов: либо законодательное закрепление права выпуска данного денежного средства, либо запрет оборота на территории Российской Федерации во избежание негативных последствий использования криптовалют. Исходя из осмысления механизма функционирования и обращения криптовалют, для государств представляется целесообразным под «криптовалютой» понимать некий специфический тип электронных денег, которые являются определенной формой криптографических и информационно-технических операций, проводимых за счет децентрализованной системы эмиссии, защищенной крипто-протоколами, проводящих подтверждение аккаунтов пользователей и валидацию операций, совершенных от их лица. В текущих реалиях можно наблюдать достаточно неблагоприятное отношение Российской Федерации к криптовалюте. Согласно статье 27 Федерального закона «О Центральном банке Российской Федерации (Банке России)» выпуск на территории Российской Федерации «денежных суррогатов» не законен. Тем не менее, сравнительно недавно, в январе прошлого года прошла конференция: «Регулирование криптовалют в России: промежуточные итоги», в ходе которой представители различных секторов экономики выразили положительную оценку перспективы криптовалюты. Так, Ксения Осипова, которая является юридическим консультантом агентства «Deloitte» приводит в пример смену парадигмы отношений между государством и криптовалютами. Она показывает, что за последние три года в госструктурах был изучен вопрос установления для

криптовалют определенного финансового статуса, чтобы пресечь возможные схемы «отмывания» денег через них. Элина Сидоренко, профессор МГИМО, специалист в области уголовного права и директор университетского объединения по вопросам криптовалют, считает, что сейчас идет процесс, в ходе которого Россия изучает опыт других государств и готовится к ходу, который станет весьма радикальным решением вопроса, стремительно назревавшего с началом бума криптовалют в 2013-м году. Профессор также высказывает мысль, что в государственной думе сейчас относятся к криптовалютам относительно либерально, и готовятся к принятию законов соответствующей специфики.

Тем не менее, было бы ошибкой упускать причины столь противоречивого отношения мирового сообщества к криптовалютам. Одна из таких причин – широкое распространение криптовалют в теневой экономике.

3.5. Криптовалюты на теневом рынке

Резкий пик популярности Bitcoin и Ethereum был вызван их главными идеями: идеей децентрализованности и анонимности. Криптовалюты быстро приобретали новых сторонников, и к ним, вскоре, присмотрелись игроки криминального сектора, из-за чего криптовалюты быстро стали очень актуальными для черного рынка.

По словам Романа Янковского – сооснователя юридического агентства «Зарцын, Янковский и партнеры» - криптовалюты крайне распространены в современном мире как средство оборота наркотиков, а также иных нелегальных товаров и услуг, включая криминальное оружие, поддельные паспорта, личные данные частных лиц и т.п. Такой «бизнес» процветает благодаря невозможности отследить участников сделки – счета в сетях анонимны. Более того, сами транзакции практически не представляется возможным идентифицировать – для подтверждения факта транзакции от конкретного человека, необходимо напрямую подтвердить связь, между пользователем сети и определенным счетом в системе.

Наверное, самый известный пример подобной практики – блокировка огромной нелегальной торговой площадки «Silk Road». Она была открыта с 2010 по 2013 год по принципу другой, известнейшей платформы – eBay. Silk Road оперировала в своих транзакциях Bitcoin, объем оборота которых оценивается в

9500 тысяч биткоинов, а чистая прибыль за год составляла около пятнадцати миллионов долларов.

Пока, Bitcoin все ещё является лидером в глубоком интернете, но его уже начали теснить альтернативные криптовалюты. Они предлагают пользователям сравнительно большую анонимность и высокую скорость транзакций. Monero и Zcash только за 2016 год отбили 20% рынка у Bitcoin, а сейчас объем нелегальных транзакций оценивается в 225 миллионов долларов. Агентство «Chain Analysis» прогнозирует рост совокупного объёма теневых операций до 1 миллиада долларов только для Bitcoin, Ethereum и Monero.

Другая сфера применения криптовалют – «отмывание» денег и их вывод в офшоры. Множество стран инициировали запрет криптовалют именно по причине подобного использования. По оценке основателя банка Wirex, специализирующегося на криптовалютах, темпы - еще один теневой способ использования криптовалют – отмывание и вывод средств. «Вывод денег в другие юрисдикции – причина, послужившая толчком для запрета ICO в ряде стран. Это особенно наглядно проявляется на примере Китая и Южной Кореи. Судить об объёмах сложно, но если государство решило вмешаться в этот процесс, то речь может идти о сотнях миллионов долларов», отмечает сооснователь криптобанка Wirex Павел Матвеев.

Также, схожего мнения придерживаются и представители Центробанка РФ а также Министерства Финансов. Они выступают резко против криптовалют. Они многократно делали заявления, что анонимность нематериальных денег, а также невозможность их проконтролировать – может быть использовано злоумышленниками для проведения незаконной деятельности.

На настоящий момент, Россия не имеет сколь-либо четкого свода законов в области экономического и правового регулирования вопросов, связанных с криптовалютами. «Сегодня в России отсутствует регулирование рынка криптовалют. Отдельно от государственных финансовых институтов, блокчейн-валюты не могут быть однозначно расценены как положительное или отрицательное явление. В результате, некоторыми индивидами технология используется как

средства заработка или накопления, а другими – в качестве средства для осуществления противоправных действий. К сожалению, несмотря на светлую идею децентрализованной валюты, возможность использовать её незаконно «отбрасывает тень» на систему, хотя и, в свою очередь, является дополнительным двигателем их роста и расширения.

Согласно Яну Янковскому, большинство запретов Bitcoin, Ethereum, Ripple и т.д. непосредственно связано с их теневой зоной, обращающейся на черном рынке в значительных количествах. Многие частные компании, действующие легально, остерегаются вкладываться в криптовалюты из-за этого аспекта. Возможно, для решения данной проблемы могла бы стать разработка законных протоколов оборота криптовалют на территории страны.

Криптовалюта перестанет использоваться преимущественно в теневой зоне экономики только тогда, когда она сама выйдет из теневого рынка. При этом, для сокращения нелегального оборота криптовалют необходимы именно движения в сторону придания ей легального статуса.

Также, по мере развития сети криптовалют, будет совершенствоваться и криптография, и, собственно, технология Blockchain. Этот процесс отразится и на снижении доступности криминальных схем, связанных с применением виртуальных валют. Постепенно, будут реализованы схемы отслеживания и корректировки транзакций. Рынок криптовалют станет значительно безопаснее, обходя по этому параметру традиционные банковские операции.

3.6. Зависимость курса криптовалют от рыночных изменений/курсов других валют/ожиданий потребителей/политической ситуации.

Согласно утверждениям исследователей теории финансов, стоимостной эквивалент способен нести внутреннюю реальную стоимость, при условии существования определенного дефицита данного эквивалента. Существует ли дефицит криптовалют?

По усредненной оценке, на текущий момент, майнеры суммарно извлекают около 5000 битконов каждый день. Учитывая текущий курс валюты составляет около 9,5 тысяч долларов, Таким образом, каждый день сеть биткоина пополняется

средствами на сумму около $47,5 млн. Для обеспечения сохранения курса валюты при данных параметрах, данная сумма должна иметь за собой реальные средства, которые можно бы было обменять. И факт, что курс криптовалют только увеличивается, может свидетельствовать исключительно о высоком желании инвесторов приобретать новые монеты сети для дальнейшего обмена и спекуляций на курсе.

В альтернативных случаях, например, при остатке нереализованных монет, или при нежелании спекулянтов обменивать на монеты свои деньги, происходит падение курса. Это вызвано тем, что пользователи сети, зарабатывающие добычей валюты, снижают свои расценки на покупку монет, ведь им нужно отбивать затраты, которые они несут в процессе майнинга. В результате, курс следует вниз за ценой отдельных участников торгов.

Соответственно, в курсе валюты на определенный момент находят свое отражение ожидания пользователей, предполагающих рост или снижение цены на единицу криптовалюты. Однако, необходимо учитывать, что криптовалюты переживают постоянный приток пользователей, что придает многим из них сходство с схемами финансовых пирамид.

В результате – крайне сложно с какой-либо существенной вероятностью определить реальную стоимость одной монеты, например, Bitcoin, т.к. отделить её спекулятивную составляющую, быстро изменяющуюся и занимающую значительную часть стоимости практически невозможно.

Другой важной особенностью криптовалют, в отличие от материальных денег, является их бесконечная репликация. Или практически бесконечная: эмиссия биткоина прекратится только с достижением числа в 21000000 единиц. И последний биткоин будет выпущен не раньше следующего века… При этом, количество желающих приобрести валюту снижается гораздо более медленными темпами, чем уменьшение вознаграждения за майнинг, то есть медленнее, чем выпускаются новые монеты. Данная особенность также подогревает курс.

Разберемся в остальных факторах.

Первый из них – волатильность. Высокая волатильность всегда была характерна для криптовалют. Колебания цен на них в течение дня могут достигать 10-ти процентов. Если сравнивать с другими средствами, то у золота этот показатель составляет около полутора процентов, а у большинства стабильных валют – менее процента. Bitcoin в 2014 году достигал волатильности в 15%, а осенью 2017 побил и эти рекорды. Высокая волатильность демонстрирует, что носитель стоимости не является способом сохранения капитала, а служит в основном инструментом спекуляций на бирже.

Вероятно, это является следствием узкого распространения криптовалют: пользователи предпочитают не сохранять, а спекулировать на валюте.

Сейчас подавляющее большинство операций с криптовалютой является переводами между пользователями. Но этот факт не способен вызвать изменение курса на валюту в краткосрочной перпективе. А то, что криптовалюты редко используются клиентами в частной жизни, стимулирует их к выводу средств, которые они получили. Постоянный обмен между выводящими средства и желающими приобрести криптовалюту и формирует столь высокую волатильность.

Вред для системы от волатильности довольно заметен. Из-за быстрых и мощных колебаний невозможно установить единую цену для какого-либо товара или услуги: за день она может оказаться как слишком демпингующей, так и выпасть из рынка на несколько процентов выше максимума. Соответственно любые трейдеры, получая при продаже продукта криптовалюту, немедленно выводят средства в материальные деньги. А еще больше волатильность интересует спекулянтов, нередко недобросовестных, в результате чьей работы курс также получает дополнительный стимул к колебаниям. Волатильность крайне подвержена колебаниям от спекулятивных действий.

Другой фактор – количество транзакций. В сети Биткоина количество операций непрерывно увеличивается. При анализе этих операций, определяется соотношение спроса и предложения на рынке криптовалют. Для данного рынка, как мы уже выяснили, характерен положительный баланс. Например, для Bitcoin ежедневно происходит проведение транзакций в объеме до 200 миллионов долларов.

Больше половины из них – операции по переводу валюты на крупные обменные пункты с целью последующего вывода средств. При продаже биткоинов в обмен на реальные деньги создается негативное влияние на курс. С другой стороны, в этот же момент происходит покупка монет клиентом, входящим в систему. Это положительно влияет на курс и балансирует систему в целом.

Таким образом – баланс транзакций по покупке и продаже криптовалюты характеризует состояние спроса на неё, что и определят в конечном счете курс.

Отдельный фактор – законодательство. Законодательные нормы в отношении криптовалют индивидуальны для различных государств. Вероятно, одним из «камней преткновения» может служить анонимность большинства Blockchain-валют, с которых тяжело взымать налог. Например, в США Bitcoin считается не деньгами, а товаром. После получения легального статуса в столь крупной экономике, Bitcoin резко подорожал. Но, в качестве товара, криптовалюта имеет достаточно серьёзные ограничения, понижающие для пользователей её привлекательность.

Существует изрядное количество примеров, когда государства, оценивая своё взаимодействие с криптовалютами, переходили от резко негативного отношения до принятия разрешающих законов для торговли виртуальными деньгами. С другой стороны, немало и обратных примеров. Каждое изменение статуса криптовалюты в различных странах будет отражено на её курсе, так как от политических решений зависит охват аудитории валютой, а от этого, в свою очередь, и желание инвестировать в неё, напрямую изменяя курс.

Наконец, для криптовалют характерна и зависимость от отношения к ним средств массовой информации. На примере того же биткоина можно вспомнить, как после быстрого роста в 2014-м он подвергся резкой критике со стороны правительств многих стран, а после этого на криптовалюту обрушился поток негатива из СМИ. Пресса освещала новости, связанные с bitcoin предвзято, концентрируясь на проблемах, что отпугивало потенциальных пользователей. В результате, рост стоимости bitcoin резко замедлился.

Подобная информация до сих пор остается более доступна, чем сообщения о реальных процессах внутри структуры криптовалюты, что стимулирует вохможных инвесторов искать альтернативные пути. Тем не менее, некоторые вопросы, связанные, например, с безопасностью системы могут быть рассмотрены правильными людьми, которые попробуют их решить, что продвинет вперед развитие валюты. А развитие и широкое распространение отражает тенденции к падению волатильности, а также повышению «воспринимаемо ценности» криптовалюты.

Сегодня же, публикации в СМИ становятся более лояльными к новой технологии. Многие известные компании вкладываются в блокчейн и криптовалюты, дополнительно подогревая к ним интерес. В результате курс может вырасти.

Таким образом, криптовалюта – весьма молодой финансовый инструмент, ещё не получивший четких формулировок в отношении своего будущего. В силу своей относительно низкой распространенности, нестабильности и неопределенного правового статуса, они очень зависят от того, что происходит в мире и от отношения происходящего к криптовалютной сети.

3.7. Перспективы криптовалют, развитие технологий

Предельно ясно, что у рынка криптовалют есть большие перспективы к развитию. Сейчас рынок оценивается приблизительно в 200 миллиардов долларов, в то время, как объём рынка валют Forex составляет, согласно экспертным оценкам, не менее 5 триллионов долларов. Возможно ли для криптовалют достичь сопоставимых размеров?

Пока прогнозы благоприятные. Стоит обратить внимание на, например, темпы роста фондовых показателей. Возьмем 2017-й год. За год индекс ММВБ упал с 2263 до 2004 пункта, РТС – с 1176 до 1100, DOW J вырос с 19800 пунктов до 21800, а FTSE, принадлежащий Англии, с 7200 до 7350. А вот на рынке криптовалют изменения гораздо более масштабные: Bitcoin поднялся до 4300 пт., начиная с 905. Ethereum — торговался с 8,17 до 334 к концу года, а Litecoin вырос с 4,80 до 90 пунктов.

Какое развитие возможно для биржи криптовалют?

для многих из них основополагающими параметрами является эффективность и скорость информационных технологий, экспоненциально усложняющихся с течением времени. Поэтому данный фактор серьезно не ограничивает развитие платформ. А фактор их разрозненности и отсутствия стандартов – может. На рынке криптовалют нет лидирующей биржи, постоянно идет процесс открытия новых и закрытия старых. На Forex существует несколько лидирующих региональных платформ, осуществляющих более 75% всего оборота. Подобное положение дел не позволяет инвесторам концентрироваться на определенных ресурсах, осложняя их коммуникацию и не позволяя эффективно использовать свои возможности.

А каковы перспективы в России?

Тенденция к легализации криптовалют затрагивает и нашу страну. Вероятно, что вскоре будет введена система регуляторов рынка, которая будет иметь благоприятное влияние на развитии экономики в целом, количество иностранных инвестиций, а также создать условия для безопасного взаимодействия пользователей сети, в целях стимулирования легального использования криптовалют. Соответственно развитие криптовалют в российских реалиях зависит от слаженной работы ЦБ и Минфина, а также самих ресурсов рынка криптовалют.

3.8. Криптовалюты и квантовый компьютер

Технология квантовых компьютерных вычислений основывается на принципах «кубитов».

подобная ячейка из-за квантовых явлений принимает не только крайние значения 1 и 0, но и любые промежуточные, что повышает скорость работы квантовых систем относительно традиционных на порядок.

С другой стороны, технология пока крайне свежая и неотлаженная. Пока только одна компания, D-Wave, совместно с Google доложила об успешных испытаниях быстрого факторинга крупных чисел. Но уже этот факт является угрозой…

Биткоину неоднократно пророчили закрытие, исчезновение и взлом. Система, пусть и со скандальными расколами, хардфорками и огромной сферой противоречивой информации вокруг себя умирать пока не собирается. Но способен ли квантовый компьютер изменить это? Например, исследователи уверены, что, базируясь на алгоритмах, аналогичных D-Wave, новые компьютеры будут способны вычислить хэш-код пользователя, используя его публичный идентификатор всего за несколько минут.

В основном, подобные прогнозы базируются на том, что алгоритм ECDSA – «Elliptic Curve Digital Signature Algorithm» может быть взломан с помощью «брутфорса» квантовым компьютером, просчитающим абсолютно все конечное множество значений. Но, стоит заметить, что доступ к Биткоин-кошельку не ограничен одним хэш-кодом, а дополняется протоколами SHA-256 и RipeMD160, не поддающимися пока даже квантовым компьютерам.

Наконец, существует еще несколько важных вопросов, на которые необходимо дать ответы перед предсказанием взлома системы Bitcoin.

В случае создания квантового компьютера и его попытки использования в преступных целях, почему взлому может подвергнуться именно криптовалюта, защищенная гораздо сложнее, чем банковский и фондовый рынки? Их оборот составляет триллионы долларов, а криптовалюты не достигли пока 200 миллиардов $. В чем преимущество атаковать именно эту сферу?

Что, если квантовый компьютер, в силу новых обстоятельств действительно сможет взламывать защиту криптовалют. Но почему они не смогут начать использовать новые протоколы, такие как, например, IMSS – Improved Merkle Script Scheme, что примерно переводится как «улучшенная схема подписей Мёркле», являющаяся пост-квантовым алгоритмом, устойчивым к квантовым вычислениям за счет неограниченного множества вводных параметров. А даже в случае взлома-метод хардфорка может защитить систему от несертифицированных транзакций.

И, в случае взлома цепочки криптовалюты – как злоумышленник сможет реализовать то электронное золото, мгновенно оборачивающееся у него в руках черепками? Вряд ли найдется какой-либо инвестор, обменяющий колоссальные

суммы миллионов долларов на валюту, которая сразу же потеряет ценность после сделки. Такое применение квантового компьютера по сути будет являться кибер-терроризмом, обрушая рынки криптовалют без какой-либо выгоды.

3.9. Вывод об экономической сути криптовалюты

Анализируя то, как создавались первые криптовалюты, наблюдая за их развитием, осознавая, чем они являются сейчас, и что они будут представлять из себя в будущем, легко убедиться: несмотря на все заявления скептиков, это не явление «одного дня», напротив, это очень масштабное явление, способное не только приносить доход своим владельцам, но и развиться в полноценную международную систему, которая будет значительно отлична от той, которую мы эксплуатируем сейчас. Изменения в жизни людей из развитых и развивающихся стран будут сравнимы с переходом банков на безналичные системы расчета. Резко изменятся многие торгово-экономические отношения частного бизнеса, который станет практически независимым от государственных финансовых ограничений. Пробелы в экономическом праве заполнит значительное количество законов, призванных предотвратить махинации и систематизировать принципы использования криптовалют. Новый мир, который будет создан при повсеместном распространении криптовалют, полностью поменяет баланс сил и, вероятно, этот процесс перехода будет новым этапом «деколонизации» в истории, единственным отличием которого будет факт, что колонии в современном мире – не официально разделенные между крупными игроками территории, а сферы влияния, не обозначенные на картах.

Заключение

Таким образом, криптовалюты остаются экономическим явлением, крайне быстро развивающимся и изменяющимся, чтобы сделать однозначные выводы. Единственным гарантированным ответом будет то, что криптовалюты – это реальность. Они уже стали частью этого мира, пусть и не были достаточно исследованы. Возможно, поэтому в мире относительно немного стран, благосклонно принявших данные платежные системы и так мала доля людей, инвестирующих в криптовалюты. Возможно, сейчас люди только присматриваются к столь сложной и

непонятной технологической системе, и, вероятно, через некоторое время криптовалюты прочно войдут в жизнь каждого из нас, сокращая наши затраты времени и денег на привычные банковские расчеты. А пока – все, что в наших силах – это проинвестировать в будущее, найдя криптовалюту себе по вкусу и не забыть купить пиццу, которая по будущему курсу будет стоить целое состояние…

Список использованной литературы

1. Молчанов М.В. Криптовалюта: понятие и проблемы (Science Time) – 2014. – №7. – Вып. №10

2. Обозреватель блоков биткоин 2017: https://blockchain.info/ru/charts/market-price

3. Информационный сайт «Bitcoin – Frequently Asked Questions»: https://bitcoin.org/en/faq

4. Образцова В.В. Правовой статус криптовалют в России: Современные научные исследования и инновации. – 2017. – №1

5. Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн: Пресс-служба Банка России. – 2014: https://www.cbr.ru/press/PR.aspx?file=27012014_1825052.htm/

6. Конференция «Регулирование криптовалют в России: промежуточные итоги»: https://bitnovosti.com/2017/ 02/01/regulirovanie-kriptovalut-v-rossii/

7. Исследования Facebook и MasterCard: молодое поколение не доверяет банкам, предпочитая новые финтех-сервисы: http://forklog.com/issledovaniya-facebook-i-mastercard-molodoe-pokoleniene-doveryaet-bankam-predpochitaya-novye-finteh-servisy/

8. Возможности квантового компьютера при атаке на криптовалюты: https://golos.io/blockchain/@itsynergis/kvantovyi-kompyuter-protiv-bitcoin/

9. Влияние различных факторов на курс криптовалют: https://vc.ru/23946-cryptocurrencies/

10. Bank of England: «The emergence of digital currencies» – 2014. (в личном переводе)