ЦИФРОВАЯ КУЛЬТУРА
УНИВЕРСИТЕТ ИТМО

Цифровая экономика
Блокчейн

Высшая школа цифровой культуры
Университет ИТМО
dc@itmo.ru

Содержание

1 Технология распределенных реестров

Термин “Цифровая экономика” был введен в 1995 году Николасом Негропонте из Массачусетского университета.

Сегодня **цифровая экономика** включает в себя область электронных товаров и услуг. Например, телемедицина, дистанционное обучение, продажа медикаментов. Также она включает в себя производство с использованием цифровых технологий. Цифровая экономика основана на создании, обработке, хранении и передачи информации.

Многие считают, что Blockchain стал вершиной развития цифровой экономики. Уже сейчас эта технология повсеместно находит свое применение.

Но, справедливо сказать, о технологии распределенного реестра знали задолго до появления блокчейна и биткоина.

На самом деле, **blockchain** – одна из технологий распределенного реестра, но не единственная. В силу исторических обстоятельств блокчейн стал доминировать в общественном дискурсе во многом благодаря раскрученности Биткоина.

Первая же работа над криптографически защищенной цепочкой блоков была описана еще в 1991 году Стюартом Хабером и Скоттом Сторнеттой. Что же такое распределенный реестр? Распределенный реестр по сути это база данных, которая может быть распределена по множеству компьютеров в интернете. Все участники сети могут иметь свою собственную, копию реестра. Любые изменения в реестре отражаются во всех копиях в течение нескольких минут, а в некоторых случаях, секунд.

Безопасность и достоверность хранимых в реестре активов осуществляется криптографически с помощью "ключей"и подписей, которые контролируют кто и какие действия может производить в общем реестре. Записи реестра также могут быть изменены одним, несколькими или всеми участниками сети, в зависимости от принятых правил.

И все же, для многих блокчейн и есть та самая технология децентрализованных баз данных, которая может совершить переворот чуть ли не в каждой отрасли, начиная от денежных переводов и заканчивая интернетом вещей. На самом деле, таких технологий больше.

Одна из них – очень многообещающая технология Хешграф (Hashgraph), продвигаемая платформой Swirlds. В чем же особенность Хешграф, и каково отличие его алгоритма консенсуса от такового в блокчейне?

Можно сказать, что в отличие от блокчейна, где постоянно присутствует то ли лотерея, то ли состязание за право строить главный «ствол дерева», все ветки в Хешграфе получают право на жизнь и развитие, двигаясь параллельно. Также, в отличие от блокчейна, где транзакция может быть и не включена в блок, если так решит большинство, все транзакции в Хэшграфе

записываются в реестр, нравится это кому-то или нет. Единственный вариант не дать какому-либо участнику процесса записать свою транзакцию в реестр это «вырубить» ему интернет.

В Хэшграфе преимуществом является именно быстрый интернет – чем выше скорость соединения, тем больше шансов записать свою транзакцию первее. Скорость работы приложений на базе консенсуса Хешграф позволяет реализовать запись событий в распределенный реестр практически в реальном времени. Это означает, что могут быть построены быстрые и безопасные экосистемы интернета вещей и пространства рабочей среды, где по заявлениям Swirlds, даже распределенная работа с текстовыми документами становится возможной.

Для компаний, ведущих свою деятельность в стремительно разворачивающемся глобальном рынке интернета вещей разработана технология распределенного реестра Tangle от проекта IOTA.

Распределенный реестр IOTA, в отличие от традиционного линейного блокчейна, представляет собой направленный ациклический граф (DAG), с помощью которого система проводит транзакции без комиссий. Устройства, подключенные к Tangle, могут обмениваться ресурсами по требованию, а также сохранять в реестре данные сенсоров и сборщиков данных. DAG реализует механизм, когда каждая новая транзакция подтверждает одну или несколько предыдущих транзакций, в результате получается структура, являющаяся по своей сути направленным графом без циклов. То есть в DAG каждая транзакция ссылается на предыдущие (родительские), подписывая их хэши и включая их в свой состав. Таким образом формируется «дерево» транзакций, где каждая из них является подтвержденной и неизменной.

Еще одним примером использования технологий распределенного реестра можно назвать технологию KSI (Keyless signature infrastructure) используемую электронным правительством Эстонии , которая гарантирует неизменность данных, возможность их проверить в любой момент и избежать любых манипуляций с информацией. Записи не хранятся на блокчейне KSI — фиксируются лишь серии их хеш-значений, в которых и отображается информация об изменениях.

Инфраструктура KSI была реализована командой Guardtime и начала функционировать еще в апреле 2008 года, до появления блокчейна Биткойна.

В начале весны 2016 года проект Guardtime объявил о партнерстве с eHealth Foundation — Фондом электронного здравоохранения Эстонии. Цель проекта — защита свыше 1 млн медицинских записей. Согласно замыслу разработчиков Guardtime, реализованная ими инфраструктура KSI внедрена в ядро базы данных Oracle. Благодаря этой интеграции изменения в истории болезни пациентов можно увидеть в режиме реального времени. Один из проектов с которым Вы неизбежно столкнетесь изучая блокчейн – это

Hyperledger от Linux Foundation. Hyperledger– открытый исходный код, созданный совместными усилиями для продвижения кросс-отраслевых блокчейн технологий.

Проект представляет собой совместную работу по созданию открытой распределенной системы бухгалтерского учета (леджера), которая может быть использована для открытой разработки и внедрения блокчейн приложений и систем. Основной упор делается на создании и запуске платформ, которые поддерживают глобальные бизнес-транзакции. Проект также фокусируется на повышении надежности и производительности блокчейна.

Технологию уже начинают использовать. Так, "Sberbank CIB организовал выпуск корпоративных облигаций МТС на сумму 750 млрд. руб. с 6-месячным сроком погашения, используя смарт-контракты. Сделка проводилась на блокчейн-платформе Hyperledger Fabric 1.1.

2 Блокчейн

Самой известной технологией остается блокчейн. **Блокчейн** – одна из ключевых технологий позволивших существовать криптовалютам, избегая проблемы двойной траты. Это последовательность записей о транзакциях сети, распределенная и защищённая криптографическими алгоритмами.

Когда у вас есть биткойн, то он не хранится на вашем кошельке. Есть только запись о том каким приватным ключом можно авторизовать перемещение конкретной монеты. Каждое перемещение (транзакция) проверяется всей сетью и записывается в блокчейн становясь новой истиной для всей сети.

Блокчейн, по сути – цепочка блоков. Блок – функциональная единица блокчейна, набор записей о транзакциях произошедших в течение определенного времени, который математически сцепляется с базой данных, содержащей все предыдущие блоки и служит основой для следующего блока – так цепочка и растёт. За право создать новый блок конкурируют майнеры, работа которых мотивируется за счет эмиссии монет. Возможны и другие модели мотивации майнеров. Но для любого блокчейна должна быть предусмотрена мотивация участников, обеспечивающих работоспособность и отказоустойчивость сети.

Главное отличие блокчейна от других реестров транзакций в том, что он не хранится в каком-либо одном месте. Он распределен среди нескольких тысяч компьютеров в мире, которые выполняют задачу проверки и передачи транзакций, и автоматически получают обновления.

Blockchain полностью открыт. Каждый может просмотреть любую транзакцию и какой публичный адрес ее совершил. Конечно, можно зашифровать данные, сопровождающие транзакцию, но нужно помнить, что они хранятся

на тысячах компьютеров по всему миру.

Благодаря децентрализованной системе, блокчейном управляет сообщество разработчиков, майненеров и пользователей. Но стоит заметить, что есть несколько методов достижения консенсуса. Об этом мы поговорим позже.

Технология блокчейн нашла широкое применение. Например, такие характеристики blockchain, как прозрачность, неизменность и децентрализованность позволяет использовать технологию при проведении голосований на самых разных уровнях. Так, 7 марта 2018 года были проведены первые президентские выборы с использованием blockchain в Сьерра-Леоне. Техническую поддержку и реализацию инициативы обеспечил швейцарский стартап Agora. Фактически, эксперимент в Сьерра-Леоне стал первым шагом для масштабирования подобного опыта. Нужно отметить, что технология использовалась для передачи результатов голосования от избирательных участков в центральную избирательную комиссию.

Очень популярна технология blockchain в сфере здравоохранения. В апреле 2018, в России стартовал проект по по учету и выдаче лекарств с использованием технологии блокчейн. В пилотном проекте участвуют три отделения Новгородской областной клинической больницы.

Но это далеко не единственные направления, где можно использовать эту технологию. Логистика, хранение и передача данных, телемедицина, привлечение инвестиций, банки – лишь небольшой перечень, где уже сейчас работают над внедрением новой технологии. Пусть большинство существующих проектов находятся в стадии разработок и пилотов, тем не менее нельзя отрицать что технология становится все более востребованной.

Вы уже знаете что такое блокчейн. Но с чего все началось? А началось все с некого Сатоши Накамото – основателя первой по-настоящему цифровой валюты Bitcoin, которая не управляется ни одним из государств. До сих пор этот человек остается неизвестным. Сатоши Накамото — имя, которым подписаны научная работа, излагающая теоретические основы цифровой валюты

Статья о новой криптовалюте вышла в свет в 2008 году, и спустя несколько месяцев, было выпущено первое программное обеспечение, сразу запущенное в сеть. Сатоши Накамото, выступивший в роли разработчика Bitcoin, продолжил общение на веб-форумах со специалистами, заинтересованными в дальнейшем развитии системы. Однако постепенно контакт между ним и его командой стал ослабевать и весной 2011 года Сатоши объявил о своем уходе, как заявил сам разработчик: "Для занятий более важными делами". С тех пор о Накамото никто не слышал. Эта личность исчезла из информационных просторов также неожиданно, как и появилась.

Полный контроль над доменом Bitcoin.org он передал своим коллегам, в том числе Гэвину Андресену – одному из ведущих разработчиков Bitcoin.

Принципы работы первой криптовалюты Сатоши Накомото описал в документе, который назвал “Биткойн: система цифровой пиринговой наличности”. Он математически доказал возможность существования финансовой системы, которая не нуждается в управлении центральным органом и при этом остается безопасной.

Слово Blockchain впервые встречается именно в этом документе. Поэтому стоит подробнее остановиться на истории первой криптовалюты. Ведь если бы она не завоевала популярность благодаря своему стремительному росту и падениям, технология blockchain возможно не стала бы так популярна как сейчас.

3 История развития Биткоина

3 января 2009г. свет увидел первый блок Bitcoin (так называемый "genesis блок"). Было сгенерировано 50 биткоинов. Время: 18:15:05 (по Гринвичу). Блок имеет уникальный хеш заголовка следующего вида:
`000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f`

Генезис блок содержит сообщение в транзакции, которое гласит:
`Время 3/ Янв/ 2009, Канцлер на грани второго спасения банков.`

В 2010 году на форуме посвященном Bitcoin, пользователь laszlo предложил 10000 биткоинов тому, кто закажет ему две пиццы. Довольно быстро пользователь jercos откликнулся на предложение и заказал ему две пиццы, за что получил обещанные 10 тысяч биткоинов на свой счёт. Сегодня, это составляет 62 млн.долл.

Именно это событие и стало отправным пунктом в жизни Bitcoin как валюты.

В 2011 году начал работу Web-портал для торговли нелегальными товарами и услугами – “Silk Road”. Идеей платформы было сочетание технологии анонимного доступа к ресурсу через сеть Tor и анонимной оплаты товара с помощью Bitcoin. Товар, который можно было купить в “Silk Road” был почти весь нелегальным: наркотические вещества, пиратские программы, краденные вещи и др.

Цена Биткойна в эти времена падала с 31 до 2 долларов, но весь 2011 и 2012 год Silk Road только рос и развивался. На пике его популярности, оборот составлял до 2 миллионов долларов США в месяц. За 2.5 года, согласно данным ФБР, через сайт прошло в общей сложности 9.5 миллионов биткоинов.

На 23 июля 2013 в интернет-магазине зарегистрировались почти 1 млн человек. В общей сложности, оборот предприятия за два года составил 1.2 миллиарда долларов США. Доход организатора за этот период в виде комис-

сионных от продаж — порядка 80 миллионов долларов США."

Закончилось все арестом владельца торговой площадки – Уильяма Ульбрихта, также известного как Dread Pirate Roberts («Ужасный пират Робертс»), 2 октября 2013 года по обвинению в наркоторговле, хакерских атаках и сговоре с целью отмывания денег. С 29 мая 2015 года он отбывает пожизненное заключение.

После ареста Ульбрихта и закрытия "Silk Road" курс Bitcoin упал примерно на треть, но за неделю цена вернулась к прежнему уровню. А чуть позже начался рост. "Провал имени Ульбрихта"остается одной из точек отсчета для технического анализа на графике цены Bitcoin.

В ноябре 2013 года начались резкие скачки курса криптовалюты. В середине месяца стоимость 1 bitcoin превысила отметку 1000 долларов. Это случилось после того, как биткоин поддержал крупный американский создатель браузерных игр Zynga.

27 февраля 2014 года объявила о своем банкротстве крупнейшая биржа по торговле Bitcoin – MT. Gox. Чуть позже был опубликован документ в котором говорилось, что в результате хакерской атаки у биржи было украдено более 744 тысяч биткоинов. Закрытие биржи обвалило курс с 1000$ до 400$.

Популярность биткоина продолжала расти. Настоящий бум начался примерно с августа 2015 и продолжился до зимы 2016 года. В общей сложности с 2014 года более 50 именитых фирм инвестировали в технологию blockchain.

Тем временем, в Bitcoin сообществе произошел раскол. 14 января 2016 года разработчик Bitcoin Core Майк Хирн покинул сообщество и также продал все свои биткоины, предрекая провал цифровой валюты.

Группа, частью которой был Хирн предложила новый вариант ПО Bitcoin – "Bitcoin XT" – и столкнулась с сопротивлением другой части сообщества. Часть разработчиков отвергали предложенные Майком решения.

Камнем преткновения стал маленький размер блока. Сеть не справлялась с транзакционной нагрузкой, возлагаемой на нее, и почти все блоки получались максимального размера и выстроилась длинная очередь ожидающих транзакций.

Предсказанием Хирна не суждено было сбыться. Биткоин продолжил свой рост. А после хардфорка 1 августа 2017 года курс криптовалюты начал взлет и к концу года приблизился к отметке в 20 тыс. долларов.

Предпосылками к хардфорку стали рост числа пользователей сети Bitcoin и резкое увеличение количества операций. Объема блока Bitcoin в 1 МБ стало не хватать для записи всех транзакций.

Было предложено два решения проблемы: увеличить размер блока или же хранить часть информации вне блокчейна – согласно протоколу Segregated Witness, коротко – SegWit.

В итоге был предложен компромиссный протокол SegWit2x — часть ин-

формации хранить за пределами блокчейна и размер блоков увеличить до 2 Мб.

Первая часть решения по хранению информации вне блокчейна – SegWit – вступила в силу 1 августа 2017 года. Увеличение блока до 2 Мб было отложен на ноябрь. Тем не менее, последнее изменение было отменено общим решением разработчиков SegWit2x.

Группа разработчиков под руководством экс-инженера Facebook Амори Сечета объявила об отказе от SegWit2x, о сохранении прежней структуры блокчейна, но увеличении размера блока до 8 Мб.

Они реализовали эту идею, 1 августа 2017 года отделившись от блокчейна Bitcoin и назвав новую ветку Bitcoin Cash. Поддержали это предложение майнинг-пул viaBTC и майнинг-группа Bitmain.

С 2015г начали массово появляться различные блокчейн-сети и криптовалюты. из которых стоит отметить Ethereum, который помимо финансовых транзакций позволяет реализовывать смарт-контракты на Тьюринг-полном языке программирования. Т.е. появилась возможность писать программы, которые исполняются в децентрализованной сети, которую невозможно остановить. На сегодняшний день bitcoin является фактически резервной валютой интернета. Все криптовалюты торгуются в отношении к нему. Биткоин является доминирующей валютой как по общей капитализации так и по объему транзакций.

4 Основные понятия Blockchain

Вы уже много узнали о технологиях распределенного реестра и истории развития Биткоина. Давайте разберем основные понятия блокчейна, чтобы более осознанно оперировать ими.

Транзакция — это подтвержденная подписью секция данных, которая передается по сети. Набор транзакций собирается в блоки. Обычно она содержит ссылки на предыдущие транзакции и ассоциирует определенное количество Биткоинов с одним или несколькими публичными ключами.

Нода – компьютер с полной версией блокчейна, являющийся основной инфраструктурной единицей сети. Чем больше полных нод в сети, чем больше разных людей ими владеет, тем выше децентрализация, а как следствие – устойчивость сети.

Хеш-функция позволяет привести любой массив данных к числу заданной длины. Например, если любое число (любой длинны) начать делить много раз подряд на одно и то же простое число, то полученный в результате остаток от деления можно будет называть хешем. Для разных исходных чисел остаток от деления (цифры после запятой) будет отличаться.

Еще пример. Есть у вас текст в файле. Но на самом деле это ведь не текст, а массив цифровых символов.

Как вы знаете, в компьютерной логике используются двоичные числа (ноль и единица). Они запросто могут быть преобразованы в шестнадцатиричные цифры, над которыми можно проводить математические операции.

Применив к ним хеш-функцию мы получим на выходе (после ряда итераций) число заданной длины (хеш-сумму).

Если мы потом в исходном текстовом файле поменяем хотя бы одну букву или добавим лишний пробел, то повторно рассчитанный для него хэш уже будет отличаться от изначального. Доходит, зачем все это нужно? Ну, конечно же, для того, чтобы понять, что файл именно тот, что и должен быть. Это можно использовать в целом ряде аспектов работы в интернете и без этого сложно представить себе работу сети.

Майнеры. выполняют сразу несколько функций: поддержание сети и достижение консенсуса. Майнеры перебирают хеши, добавляя случайное число к вмещающимся в блок транзакциям.

Тот майнер, который подобрал Хеш с определенными значениями получает право на присоединение блока к цепочке и получение вознаграждения. Комиссия с транзакций, находящихся в блоке так же является вознаграждением майнера, присоединившего блок.

Может возникнуть ситуация, когда два майнера одновременно угадают нужный хеш. В этом случае, каждый из майнеров берет за основу любой из этих блоков и начинает подбирать хеш для следующего блока. Если майнеры разделились и присоединяют блок к разным предшественникам, тот блок, который присоединится первым будет валидировать конфликтный блок и сеть автоматически выберет самую длинную цепочку. А блоки из наименьшей цепочки будут считаться заброшенными.

Так как добыча криптовалюты сейчас находится на пике популярности для успешного майнинга уже не хватит одного компьютера со средней мощностью. Для решения этой проблемы необходимо иметь специализированное оборудование и вступать в пулы для майнинга.

Майнинговый пул представляет собой сервер, распределяющий задачу расчёта подписи блока между всеми подключенными участниками. Сервер получает решения от всех майнеров, которые подсоединены к нему и, если одно из этих многих решений оказывается правильным, пул получает вознаграждение за созданный блок. Это вознаграждение делится пропорционально вложенным майнерами усилиям и выплачивается на их кошельки.

Именно так достигается справедливое распределение добытых монет. Майнер с небольшой мощностью может работать очень долго, не найдя ни одного блока, но при этом получит свою долю общего пирога – ему платят за вероятность того, что именно одно из его решений окажется правильным.

Публичный адрес - криптографическая последовательность вроде той, что вы видите. Такой адрес можно без страха публиковать. Всё что он дает это возможность любому перечислить монеты и посмотреть остаток на счете и историю транзакций.

Приватный ключ. Криптографическая последовательность, похожая на открытый ключ. Зная приватный ключ вы можете распоряжаться всеми приписанными к нему активами. Хеш функция от него и является публичным адресом.

Токен – жетон, монетка, койн. Единица измерения криптовалюты. Могут быть сами по себе и работать на основе отдельного блокчейна, а могут быть выпущены и поддерживаться сторонним блокчейном. Так, например на блокчейне Биткоина можно выпустить "Цветные монеты" или на блокчейне Ethereum – "Токены". Токен биткойна – собственно биткойн. Токены могут делиться на части и объединяться, так что проблем со сдачей в магазине или нехваткой монет в обращении можно не бояться.

Форк – разветвление блокчейна на несколько версий, каждая из которых затем живёт своей жизнью. Чтобы внести изменения в блокчейн необходимо изменить его программу, что создаёт ответвление блокчейна – вилку. Разветвление может быть осуществлено как *хардфорк* – без обратной совместимости с базовой версией или *софтфорк* с которым сможет работать клиент предыдущей версии.

5 Алгоритмы консенсуса

Блокчейн представляет из себя базу данных, распределенную на множестве компьютеров. Должен быть метод принятия решения о том, какие данные учитывать, а какие считать неверными, т.е. участникам сети нужно договариваться друг с другом о том, что считать истиной. Общее согласие и называется консенсус.

Голосование является одним из методов достижения консенсуса, но самым нежелательным, т.к. оно учитывает исключительно интересы большинства и может быть использовано явно против лиц, не входящих в большинство. В анонимных системах, где каждый может стать участником, голосование легко взламывается простым накручиванием, когда каждый может зарегистрировать сотни аккаунтов

В любой блокчейн-сети передаются два основных типа сообщений — транзакции и блоки. Транзакции формируются участниками системы и к ним алгоритм консенсуса не относится. Для того чтобы отправить пару биткоинов, никакого соглашения не нужно, достаточно знать правильный ключ. Блоки — совсем другое дело. Они являются основным продуктом алгорит-

ма консенсуса и определяют, в каком порядке транзакции будут включены в базу данных. Существует проблема двойной траты средств.

Без согласования между узлами сети возможна повторная трата средств. Предположим, у вас есть 1 биткоин. Вы может сформировать две транзакции, согласно которым он переходит Алисе и Мише. Если Алиса и Миша никак не согласовывают свою историю транзакций, они оба примут ваш платеж, поскольку транзакции будут подписаны вашей электронной подписью, а до операции у вас действительно был этот биткоин! Если же Алиса и Миша согласовывают журналы транзакций, Миша увидит, что ваш биткоин уже принадлежит Алисе, если операция в ее адрес записалась в блок первой. То есть, выполнится только одна из транзакций, а вторая станет некорректной — ваши средства будут уже потрачены.

Задача распределенного консенсуса не специфична для блокчейна и имеет хорошо проверенные решения для многих других распределенных систем. Даже задача консенсуса, в котором узлы могут вести себя мошенническим образом, — задача византийских генералов— впервые была сформулирована в 80-х годах прошлого века, а методы ее решения появились в конце 90-х.

Рассмотрим подробнее эту задачу, чтобы пояснить что такое Византийский консенсус. Византия. В ночь перед великим сражением, Византийская армия содержит n легионов. Каждый из них подчиняется своему генералу. У всей византийской армии есть главнокомандующий, руководящий генералами. Империя находится в упадке и среди генералов, включая главнокомандующего, могут быть предатели. В течение всей ночи, каждый из генералов получает от предводителя приказ о действия на утро. Это может быть один из двух вариантов «атаковать» или «отступать». Если все честные генералы атакуют – они одержат победу. Если все отступят – им удастся сохранить армию. Если часть атакуют, а часть отступят – они терпят поражение. Если главнокомандующий предатель, он может дать разным генералам разные приказы, следовательно, его приказы не стоит выполнять беспрекословно. Если же каждый генерал будет действовать независимо от других, результаты битвы также могут быть плачевными. Поэтому генералы нуждаются в обмене информацией друг с другом, чтобы прийти к соглашению. Связь между ними осуществляется посредством надежной связи. Согласие заключается в том, чтобы все лояльные генералы узнали о численности всех лояльных армий и пришли к одинаковым выводам относительно состояния предательских армий.

Биткойн и другие блокчейны от предыдущих наработок отличаются условиями работы сети. В обычном алгоритме византийского консенсуса у узлов сети есть «личности», выражаемые через цифровые подписи, а сам список узлов известен заранее или меняется редко, но предсказуемо. В биткойн-блокчейне все наоборот. Участники сети не только заранее неизвестны, но и

могут свободно подключаться или отключаться от сети. Из-за этого обычные алгоритмы византийского консенсуса для блокчейна не подходят. Разработчики программного обеспечения для Блокчейн-сетей реализовали несколько различных методов консенсуса. Давайте подробнее поговорим о некоторых из них.

Proof-of-work – "Подтверждение выполнения", пожалуй самый известный способ подтверждения транзакций. В буквальном понимании, участники сети проделывают объем работы, который может быть быстро проверен другими. Узлы блокчейн сети, формирующие блоки проделывают просчет алгоритма, результат работы которого легко проверяется другими узлами сети. Если результат случаен, каждый узел имеет шанс выполнить работу первым. Вероятность будет тем выше, чем больше производительность.

Первый узел, который полностью провел необходимые вычисления — получает вознаграждение, формирует блок и рассылает его другим участникам на проверку. Все узлы борются между собой, чтобы оказаться тем самым, первым узлом, получившим вознаграждение. Большое количество узлов производят вычисления, но в результате только один проводит полезную работу и получает вознаграждение, таким образом, работа выполненная остальными узлами бесполезна. И так как скорость расчетов имеет значение, возникает гонка вооружений с целью получения вознаграждения. Это является недостатком данного метода. Например в для поддержания этого метода консенсуса в Биткоине, на сегодняшний день сжигается 71 Тераватт в час, что сопоставимо с энергопотреблением Чили.

И все же Proof-of-work решает главную проблему анонимных сетей — делает невозможной атаку, при которой злоумышленник создает множество фальшивых узлов, чтобы «задавить» получившимся большинством мнение остальных пользователей. Чтобы обладать мнением, нужно обладать реальной вычислительной мощностью, которую нельзя подделать, и которая не требует никакой дополнительной аутентификации — она сама по себе привязывает узлы к потреблению реальных ресурсов. Доказательство нельзя подделать и «перенести» на другие блоки. Таким образом, майнеры не могут воровать доказательства друг у друга. Более того, доказательства нельзя заготовить впрок — в каждый блок входит ссылка на предыдущий, поэтому начать работать над доказательством можно только после появления предыдущего блока в сети.

Proof-of-Stake – Доказательство доли владения. Популярный алгоритм консенсуса в блокчейн сетях. В этом алгоритме в формировании блоков участвую все или часть узлов. Вероятность, с которой узлы наделяются правом упаковки зависит от баланса на счете узла. То есть, участник, обладающий 1% всех монет сети будет подтверждать 1% блоков. Алгоритм Proof-of-stake решает проблему proof-of-work, связанную с большими затратами элек-

троэнергии. Вместо вычислительных мощностей участникам нужно определенное количество криптовалюты, находящейся у них на счету.

Основным недостатком метода можно назвать возможность концентрации средств в одних руках, что может приводить к централизации сети.

Одним из вариантов комбинированного применения Proof-of-Stake является Proof-of-Importance.

Proof-of-Importance – Доказательство важности. Алгоритм консенсуса используемый блокчейн платформой NEM. Значимость каждого пользователя в сети определяется, как количеством средств имеющихся у него на балансе так и количеством проведенных транзакций с использованием его кошелька, а также время его нахождения в сети. Таким образом, Proof-of-Importance учитывает как количество средств, так и активность пользователя в блокчейн сети..

Delegated Proof-of-Stake – еще одна из разновидностей алгоритма консенсуса Proof-Of-Stake, в которой блоки подписывают выбранные представители. Владельцы наибольших балансов выбирают своих представителей, каждый из которых получает право подписывать блоки в блокчейн сети. Каждый представитель, обладающий одним или более процентами от всех голосов попадает в совет. Из сформированного списка выбирается по очереди следующий представитель, который и подпишет следующий блок. В том случае, если по какой-либо причине представитель пропустил свою очередь в подписании, он лишается делегированных голосов и покидает совет, после чего на его место выбирается следующий кандидат. Владельцы балансов, делегируя свои голоса, не теряют над ними контроля, так как в любой момент могу их отозвать у своего представителя.

Leased Proof-of-Stake — еще одна модификация алгоритма Proof-of-Stake. В рамках этого алгоритма, любой пользователь имеет возможность передавать свой баланс в аренду майнинг-узлам, а за это майнинг-узлы делятся частью прибыли. Таким образом, данный алгоритм позволяет получить доход от майнинговой деятельности, не ведя самого майнинга.

Proof-of-Capacity – доказательство ресурсов. Алгоритм достижения консенсуса, при котором для добычи криптовалюты используется, например, память на жестком диске. Proof-of-Capacity дает возможность нодам в сети блокчейна задействовать для майнинга свободное место на жестком диске. Этот алгоритм предполагает создание списка возможных решений на жестком диске майнера еще до начала майнинга. Чем больше объем памяти жесткого диска, тем больше возможных решений на нем может храниться, что повышает шансы майнера найти в своем списке искомое значение хэша и получить награду за блок.

Proof-of-Authority – В этом алгоритме все блоки создаются одобренными аккаунтами. Такие аккаунты называют – Валидаторы. Фактически, Proof-of-

Authority – это модифицированная версия Proof-of-Stake, где доля определяется не счетом на балансе, а личностию Валидатора. Личность подтверждается идентификацией на платформе с учетом официальных документов, что позволяет избежать создание фейковые аккаунты. Таким образом, право подтверждать блоки выдается за добровольное раскрытие личности Валидатора. Все действия, которые совершаются Валидатором, становятся публичными. Таким образом, для сохранения репутации Валидорам следует придерживаться интересов сети.

Минусом данного алгоритма является то, консенсус достигается только благодаря работе валидаторов. Это прямо намекает на централизованность системы.

Преимущества Proof-of-authority перед Proof-of-work и Proof-of-Stake на лицо: новый блок создается всего за 5 секунд, комиссии предельно низкие, а масштабирование сети может происходить горизонтально, объединяя несколько сетей в одну. Как такового майнинга в Proof-of-authority нет. Транзакциями и блоками занимаются утвержденные валидаторы, а значит для подтверждения всех операций используются мощности их железа. Это позволяет существенно снизить затраты на обслуживание сети.

6 Смарт-контракты

На сегодняшний день, самой популярной платформой для написания и исполнения Смарт-контрактов является Эфириум – второй по популярности блокчейн после Биткоина. Запуск Эфириума состоялся 30 июля 2015 года. Основателем является программист Виталик Бутерин, проживающий в Канаде и имеющий русские корни. Именно он предложил инновационную идею, описал технологию работы новой криптовалюты – Эфира, и ее назначение. Совместно с ним в разработке криптовалюты и ее описании участвовал программист Гэвин Вуд.

Именно Эфириум дал возможность создавать смарт-контракты на блокчейне. Идея возникла благодаря повышенному интересу к теме финансовых контрактов на основе криптовалют. Базовым типом был «контракт на разницу цен» . В таком контракте, две стороны соглашаются внести на депозит некоторое количество средств и затем могут изъять их оттуда в пропорции, которая зависит от значения цены базового актива. Эти контракты позволяли людям как спекулировать на цене актива так и защищать себя от волатильности.

Эфириум развил эту идею и продвинул ее на шаг вперед. Вместо того, чтобы быть соглашением между двумя сторонами, которое имеет начало и конец, контракт в Эфириуме – это своего рода автономный агент, модели-

руемый блокчейном. Каждый контракт Эфириума имеет свой собственный внутренний программный код, и этот код срабатывает каждый раз, когда на данный контракт отправляется транзакция.

Основное преимущество Эфириума заключается в том, что на языке сценариев платформы может быть описан алгоритм любой сложности.

Чтобы понять, как устроены смарт-контракты, сначала надо разобраться с тем как работают аккаунты в сети Эфириум. Берем любой блокчейн, например Биткоин. У нас есть 2 аккаунта А и Б, на каждом по 10 биткоинов, каждый, конечно же, имеет свой уникальный адрес. Владелец аккаунта А пересылает 5 биткоинов на аккаунт Б. Балансы на аккаунтах меняются на 5 биткоинов и 15 биткоинов соответственно. Оба аккаунта контролируются приватными ключами, которые и дают доступ к ним. В сети Эфириум транзакции осуществляются по такому же принципу.

Но Эфириум предлагает второй тип аккаунтов. Кроме пользовательских аккаунтов с приватным ключом доступа, есть то, что мы называем “смарт-контракты”. Смарт-контракты имеют баланс и публичный адрес, также как и пользовательские аккаунты. Вместо же приватного ключа, смарт-контракт полностью контролируется программным кодом, который записывается на стадии создания. Никто и никогда не может изменить этот код. Нет какого-либо администратора, который сможет вмешаться в контракт и изменить его. Так что, если вы сделали опечатку или ошибку, то нужно создавать полностью новый смарт-контракт с новым балансом и адресом. Смарт-контракт имеет все те же функции, доступные пользовательским аккаунтам. Аккаунт Б может переслать 5 Эфиров на смарт-контракт, который, согласно прописанным с помощью кода условиям, пересылает, 1 Эфир на аккаунт А.

Итак, смарт-контракт – это аккаунт, контролируемый кодом, а не пользователем. В смарт-контрактах совсем не обязательно иметь положительный баланс. То есть можно хранить Эфир на балансе аккаунта, но совершенно не обязательно. Также, смарт-контракты могут взаимодействовать друг с другом, что применяется во многих децентрализованных приложениях.

Вот пример как работает смарт-контракт. Представим компанию с 5 работниками. Всем платим одинаково. У нас есть 10 Эфиров, которые мы хотим распределить между всеми работниками. Допустим, у нас есть менеджер, которого мы попросим это сделать. Мы доверяем ему перечислить по 2 Эфира каждому работнику. Действия менеджера могут опираться не только на поставленную перед ним задачу, но и на его личные отношения к каждому из работников, что может привести к неравному распределению. Такая ситуация может возникнуть и вследствие ошибки. Но что если заменить менеджера смарт-контрактом? Средства будут распределены согласно коду, прописанному в контракте, и каждый работник получит по 2 Эфира. В результате мы имеем смарт-контракт, хранящий адреса каждого из работников и условия

начисления оплаты, которые никто не может изменить, включая того, кто его создал.

Ранее мы упоминали Эфир. Это — внутренний токен блокчейна Эфириума, роль которого не ограничивается платежами. Он так же используется как топливо для работы смарт-контрактов. Т.е. чтобы контракт выполнил операцию, нужно заплатить небольшую часть Эфира за его работу.

Блокчейн Эфириума позволяет создавать и другие токены.. Для этого нужно опубликовать смарт-контракт, который будет управлять токенами.

Для того, чтобы с токеном могли работать кошельки и биржи, его нужно разрабатывать в соответствии со стандартами, которые базируются на протоколе внесения предложений по улучшению сети Эфириум – ERC – расшифровывается как Ethereum Request for Comments.

Например токен ERC-20, где 20 – уникальный идентификационный номер предложения. Технические спецификации для токенов, выпускаемых на блокчейне Эфириум, были опубликованы в 2015 году.. Токены, отвечающие этим спецификациям, известны как токены стандарта ERC-20 и фактически являются смарт-контрактами на блокчейне Эфириум. Несмотря на то, что токены ERC-20 функционируют в пределах рамок, установленных командой Эфириум, эти рамки достаточно широки, обеспечивая разработчикам большую гибкость при их создании.

Стандарт ERC-20 определяет набор правил, которые должны быть соблюдены для того, чтобы токен был принят и имел возможность взаимодействовать с другими токенами в сети. Сами токены представляют собой блокчейн-активы, которые могут иметь ценность, а также могут быть отправлены и получены как любая другая криптовалюта. ERC-20 на данный момент – самый популярный стандарт токенов на платформе Эфириум.

Вторым по популярности после стандарта ERC-20 можно назвать стандарт ERC-721. Известен он стал благодаря нашумевшей игре “CryptoKitties”. Эта игра точно войдет в историю не только благодаря своей идее. Еще она на несколько дней парализовала всю сет Эфириум из-за большого количества транзакций. CryptoKitties – игра, где можно покупать, продавать и выращивать виртуальных котиков. Каждый котенок в игре имеет уникальный набор характеристик. Именно эта уникальность делает CryptoKitties отличным объектом коллекционирования, ведь блокчейн позволяет доказать право владения цифровым объектом.

Стандарт токенов ERC-721 – был предложен Дитером Ширли в конце 2017 года. Этот стандарт позволяет смарт-контрактам работать как торговые токены похожие на токены ERC-20. Уникальность токенов ERC-721 в том, что они не взаимозаменяемы (Non-Fungible), т.е. каждый имеет набор неповторимых параметров.

Взаимозаменяемость (Fungibility) – характеристика денег или товаров,

означающая, что одна часть или несколько частей могут быть заменены другой равной частью при уплате долга или погашении счета.

Взаимозаменяемость может быть характеристикой актива или токена, которая определяет могут ли деньги или товары одного типа быть полностью равнозначны во время обмена или использования. Например, на 100-рублевую купюру можно купить лимонад в любом магазине. Она имеет ценность и может быть использована для приобретения товаров с одинаковой или меньшей ценностью. А вот если попробовать приобрести лимонад на, например, почтовую марку, продавец ее не примет.

Уникальные данные, которыми обладают и почтовая марка и рублевая купюра, нивелируют их взаимозаменяемость, так как оцениваются они по разному в зависимости от оценщика и не всегда могут быть равнозначны.

Токены ERC-721 можно использовать для обмена, но ценность их – в уникальности каждого токена. Все токены формата ERC-721 обладают собственными уникальным номером, что делает их невзаимозаменяемым и неделимым в отличие от токенов других форматов.

Успех игры с котятами привлек внимание компаний и разработчиков, которые видят в ERC-721 способ упростить использование криптоактивов. Будущее стандарта может быть, например, в инвентаризации ценных игровых предметов для многопользовательских онлайн-игр, таких как мечи, доспехи и амуниция, а также в облегчении отслеживания, торговли и управления активами реального мира, такими как недвижимость или автомобили. Новый стандарт открыл возможность для предотвращения подделки ценных вещей и упростил их передачу без посредников.

Например, при помощи технологии блокчейн произведениям искусства можно присвоить уникальные токены и ввести систему их совместной передачи, это станет доказательством подлинности и законного владения. Таким образом, даже в случае исчезновения предмета, реализовать его на черном рынке без привязки к определенному токену будет затруднительно. А получить токен без согласия владельца невозможно.

В мире, где мы все являемся владельцами уникальных предметов, начиная с игровых вещей и заканчивая недвижимостью, подобные токены найдут свое применение во многих сферах жизни, делая транзакции дешевыми, прозрачными и безопасными.

7 Регулирование криптовалют и ICO

В этом видео мы бы хотели более подробно рассмотреть государственное регулирование криптовалют и первичного размещения монет, более известного как ICO.

Технологии блокчейн привнесли в мировую экономику ряд изменений. Среди них – новые возможности инвестирования, криптовалютные биржи, торговля крипто активами. Экономики стран оказались не совсем готовы к стремительным темпам внедрения на рынки криптовалют и ICO. Многие столкнулись с проблемой отсутствия правового регулирования новых экономических взаимоотношений. Появились проблемы обеспечения безопасных финансовых сделок. Возникли угрозы финансовых махинаций. Именно поэтому возникла необходимость в методах регулирования криптовалют и ICO.

Основным вопросом стало, чем же считать криптовалюту? Платежным средством, цифровым активом, ценной бумагой, имуществом – существует много вариаций ответа на этот вопрос, который предлагают финансовые регуляторы разных стран. А все вопросы с регуляцией ICO упираются в то, что нужно не дать украсть средства инвесторов. К тому же большинство стран ведет активную борьбу с отмыванием денег. Через ICO можно привлечь серьезные деньги, вполне сравнимые с традиционным способами финансированием компаний. Между тем, особенность ICO в том, что весь бизнес здесь ведется в интернете и возможна смена юрисдикции, в которой происходит привлечение средств. Что в свою очередь дает возможность осуществлять разного рода махинации. Именно поэтому, государства активно разрабатывают способы регулирования ICO.

Одной из первых юрисдикций, принявших модель привлечения инвестиций через проведения ICO была Швейцария. В связи с резко возросшим количеством ICO-проектов Швейцарская служба по надзору за финансовыми рынками (FINMA) еще в сентябре 2017 года опубликовала Руководство для ICO. Формулировка и содержание изданного Руководства по ICO дает четко понять, что FINMA в крайней степени озабочена соблюдением Закона о борьбе с отмыванием денег. Внимание регулятора коснулось и законодательства по ценным бумагам. FINMA пришла к выводам, что токены представляют собой ценные бумаги и попадают под Закон о фондовой бирже, который регулирует создание и обращение ценных бумаг и их производные.

16 февраля 2018 FINMA опубликовала принципы, дополняющие предыдущий вариант Руководства для ICO, где были выделены три типа токенов:

- Payment tokens. Такие токены не имеют иной функции, кроме как платежное средство. Требования регулятора при использовании этих токенов сводятся к соответствию законодательству по борьбе с отмыванием денег. Payment tokens не считается ценной бумагой.

- Utility tokens. Они предоставляют доступ к приложению или сервису. Такие токены не считаются ценными бумагами. Важным требованием является возможность использования токена с момента его выпуска.

- Asset tokens рассматриваются как активы обеспечивающие получение дохода в виде, например, доли от будущих доходов компании. В этом случае они аналогичны акциям, облигациям или деривативам. Это значит, что торговля ими должна соответствовать нормам гражданского права, так же, как и требованиям Закона о ценных бумагах.

Опасения в отношении отмывания денег и использования криптовалют для мошеннических схем возникают и у Комиссии по ценным бумагам и биржам США. Джей Клейтон, председатель Комиссии по ценным бумагам и биржам в декабре 2017 года сделал публичное заявление, в котором предупредил, что Комиссия может быть не в силах обезопасить граждан от возникающих рисков в случае участия в ICO. Неамериканский эмитент может без труда продать токены в США, а все вырученные средства могут в ту же секунду покинуть сферу досягаемости американского регулирующего органа, возможно, не оставив инвесторам и регулирующим органам США инструментов для устранения последствий неправомерных действий со стороны подобного эмитента. Именно это побуждает финансовые регуляторы США ужесточить надзор на кпритовалютном рынке.

Ранее, в июле 2017 года Комиссия по ценным бумагам и биржам сообщила, что токены могут быть признаны ценными бумагами при наличии соответствующих условий (например, предоставление права голоса, доли в компании, обещание прибыли и т. д.). Для того чтобы определить, является ли токен ценной бумагой, применяются ряд специализированных тестов. А в конце декабря 2017 года президент Дональд Трамп подписал новый закон, согласно которому все сделки с криптовалютами будут облагаться налогом. Кроме того, стоит отметить что регулирование криптовалют в США может отличаться в разных штатах.

Несмотря на ужесточения, в июле 2018 именно в США была заключена первая в истории сделка по обмену BTC фьючерса Чикагской торговой биржи на биткоин, как физический актив. За этой формулировкой кроется событие, приближающее торговлю криптовалютами и производными от них к стандартным финансовым операциям.

Между тем азиатский регион демонстрирует огромный интерес к технологии блокчейн и криптоактивам. На Южную Корею приходится значительная доля мирового суточного объема криптовалютной торговли, Китай стремится быть лидером в области блокчейн-инноваций, Филиппины планируют использовать платформу для совершенствования системы сбора налогов, а центральный банк Таиланда ищет способы применения технологии. Япония, в свою очередь, также является одним из наиболее крупных криптовалютных рынков, а сами цифровые валюты в стране легализованы и используются в качестве платежного средства.

В Японии криптовалюта получила статус платежного средства 1 апре-

ля 2017 года. Согласно закону, криптовалюты могут быть использованы для взаиморасчетов. Криптовалютные биржи в Японии должны следовать стандартам обязательной верификации и противодействия отмыванию денег, используемых в других странах, получить лицензию на торговлю виртуальными валютами и иметь обязательную регистрацию в Агентстве по финансовым услугам Японии, – оно регулирует вопросы эмиссии национальной валюты. Если бирже отказано в лицензии, она должна прекратить свою деятельность на территории Японии.

Также, 18 июня 2018 года вступил в силу новый закон о введении запрета на анонимные криптовалюты из-за потенциальной возможности их использования в мошеннических целях.

Кроме того, власти Японии готовят изменения законодательства, согласно которым криптовалюты станут рассматриваться не как платежное средство, а как финансовый продукт.

Что касается регулирования ICO у Японии нет специализированных законов для первоначальных размещений монет, эта область регулируется действующим законодательством. Закон о платежных услугах в виртуальной валюте регулирует выпуск токенов. Так компания, выпускающая монеты должна зарегистрироваться в финансовом бюро по месту проведения ICO. Если же монеты, предлагаемые в рамках ICO, позиционируются как объект инвестиций, то вступает в силу Закон о биржах и финансовых инструментах и первоначальное размещение регулируется ним.

Тем временем в Китае все более усиливаются запретительные меры по отношению к криптовалютам и проведению ICO. 4 сентября 2017 года Центробанк КНР запретил проведение ICO, признал их незаконными и потребовал немедленно прекратить все операции и вернуть средства инвесторам. Все биржи получили указание о прекращении операционной деятельности в срок до 1 октября.

Тем не менее, эти события не привели к тотальному запрету на использование криптовалют. Закон, устанавливающий нормы для регулирования криптовалют в стране, вступил в силу 1 октября 2017 года. Согласно ему криптовалюты получили статус «виртуальной собственности», что позволяет владеть ими и использовать.

Власти Китая сотрудничают и с регуляторами Южной Кореи по вопросам совместного контроля за рынком криптовалют и ICO. Южная Корея как и Китай считается лидером в криптовалютной индустрии. Большие объемы криптовалютной торговли в Южной Корее означают, что любое событие на рынке этой страны отразится на мировой обстановке. Как и в Японии, власти Южной Кореи выступают против анонимности в криптоэкономике. В начале 2018 года были запрещены любые транзакции криптовалют с анонимных банковских счетов. Теперь все владельцы виртуальных кошельков криптова-

лют должны будут привязывать их к реальным банковским счетам. Помимо этого держатели таких кошельков должны пройти процедуру подтверждения личности.

Стоит отметить, что на майском саммите G20 в 2018 году, было принято решение классифицировать криптовалюты как финансовые активы, и Южная Корея должна соответствовать этому решению.

К первичному размещению монет Южная Корея относится более строго. И вслед за Китаем в сентябре 2017 года Комиссия по финансовым услугам Южной Кореи объявила о запрете всех форм размещения токенов. Данный закон вызвал широкий резонанс в криптовалютном сообществе. Кроме того, комитет Национального собрания по четвертой промышленной революции дал официальной рекомендации об отмене запрета на ICO. В сочетании с общим положительным настроением в мировом сообществе в отношении криптовалют, выраженном на собрании саммита большой 20-ки, закон о запрете первичного размещения монет может быть пересмотрен.

Что касается России, в соответствии с поручением президента к Правительству Российской Федерации и Банку России, 25 января 2018 года Министерство финансов и Центробанк представил законопроект “О цифровых финансовых активах”. Законопроект был принят Госдумой в первом чтении и отправлен на доработку. Он вводит определение цифровых финансовых активов, к которым относятся криптовалюты и токены, а также законодательно закрепляет новый вид договора, заключаемого в электронной форме – смарт-контракт. При этом цифровые финансовые активы не будут являться законным средством платежа на территории РФ. Все криптовалютные сделки могут быть осуществлены только через операторов обмена, которыми должны быть юридические лица, осуществляющие виды деятельности, определенные законами "О рынке ценных бумаг"и "Об организованных торгах".

Минкомсвязи в свою очередь подготовило законопроект о регулировании ICO в феврале 2018 года. Сейчас проект закона проходит общественное обсуждение, по результатам которого будет сделана экспертная оценка и он перейдет на рассмотрение Правительства. Согласно документу, для проведения ICO нужна аккредитация. Чтобы ее получить, нужно соответствовать нескольким условиям: наличие уставного капитала объемом не менее 100 млн руб. и лицензии на разработку, производство и распространение криптографических средств. Кроме того, у организатора выпуска токенов должен быть открыт банковский счет в российском банке для проведения операций с деньгами, которые получены в результате ICO. Организатора ICO обязывают выкупить токены по номинальной цене у любого предъявителя на основании так называемой безотзывной публичной оферты. Будет ли принят закон и какие правки будут внесены покажет время.

Стоит также отметить Беларусь. 21 декабря 2017 года был подписан де-

крет «О развитии цифровой экономики», который вступил в силу 28 марта 2018 года. Он легализует в Белоруссии майнинг, блокчейн, деятельность бирж криптовалют и прочие операции с криптовалютами. Гражданам Белоруссии декрет разрешает самостоятельно владеть криптовалютами, добывать их, менять, покупать и продавать за белорусские рубли и валюту, а также дарить криптовалюту и завещать. Причем ни одно из этих действий не будет считаться предпринимательством, а значит, его не нужно декларировать. Вместе с легализацией криптовалют было введено льготное налогообложение до 2023 г. Резиденты Парка Высоких Технологий за операции с криптовалютами не облагаются НДС и налогом на прибыль, физические лица – подоходным налогом, в том числе и за майнинг. Также в Парке высоких технологий могут быть созданы операторы ICO. Именно они будут запускать ICO-проекты своих заказчиков и рассматривать их с точки зрения легальности, структурирования и борьбы с отмыванием денег.

В Европе также можно ответить пристальный интерес к регулированию криптовалют и ICO. Например, Германия легализовала биткоин еще в 2013 году, обозначив его цифровой валютой. В 2017 году обозначение биткоина перешела в разряда “финансового интсрумента”. Также стоит обратить внимание, что в новых поправках к Банковскому кодексу помечено, что биткоин – это «частные деньги». И согласно Налоговому кодексу Германии, покупка-продаж биткоинов попадает под закон о “подоходном налоге”.

Если Вы хотите зарегистрировать ICO в Германии, то на данную деятельность Вам нужна будет финансовая лицензия Германии. А регулирование осуществляет Федеральное управлением финансового надзора.

В Эстонии ICO разрешено, но принимая во внимание разъяснения Финансового регулятора Эстонии, который считает, что при анализе токенов должны учитываться фактические обстоятельства, а содержание превалировать над формой. Эстония также рассматривает вопрос о создании национальной криптовалюты.

В Англии же регулирование деятельности относительно криптовалют законодательством не предусмотрено. Это связано с тем, что в Управлении по финансовому регулированию и контролю Великобритании Биткоин не считается ни денежными средствами, ни валютой. Англия — один из лидеров в сфере развития блокчейн-проектов и криптовалют, а также одна из самых благоприятных и удобных юрисдикций для ведения криптовалютного бизнеса. Государство открыто оказывает поддержку стартапам, которые связаны с цифровыми валютами. Все эти примеры доказывают общее лояльное отношения Европейских государств к криптовалютам и ICO.

Подводя итоги, можно сказать, что подход стран к регулированию криптовалют сильно разнится. Тем немее, нельзя отрицать что все игроки заинтересованы в новой технологии и возможностях которые она дает. А последнии

тенденции свидетельствую о рассмотрении регуляторами способов интеграции криптовалют в мировую экономику. Попытки тотального запрета лишь способ дать время разобраться в новых понятиях и разработать необходимые подходы к регулированию.

8 Обзор блокчейн проектов и их применение

Можно сказать, что сегодня в мире мы можем наблюдать настоящий бум всевозможных проектов заявляющих использование технологии блокчейн. В этом видео мы остановимся на самых популярных. Подробно рассмотрим особенности проектов, которые и сделали им имя в крипто мире.

Если уж и делать рейтинг блокчейн-проектов, то, конечно же, на первом месте будет – **Bitcoin**.

Это – пиринговая платёжная система, использующая одноименную единицу для учёта операций и одноимённый протокол передачи данных. Для обеспечения функционирования и защиты системы используются криптографические методы. Вся информация о транзакциях между адресами системы доступна в открытом виде. Уникальные особенности:

- Ограниченность ресурса. Общее количество биткоинов стремится к 21 миллиону. Чем больше людей добывает биткоин, тем сложнее это делать.

- Полная децентрализация. Нет центрального администратора или какого-либо его аналога. Необходимым и достаточным элементом этой платёжной системы является базовая программа-клиент с открытым исходным кодом. Запущенные на множестве компьютеров программы-клиенты соединяются между собой в сеть, каждый узел которой равноправен и самодостаточен. Невозможно государственное или частное управление системой, в том числе изменение суммарного количества биткоинов.

- Защищенность. Так так используется консенсус POW необходимы миллионы долларов чтобы получить ограниченный контроль над сетью.

- “Золотой эталон” для остальных криптовалют. Все существующие криптовалюты могут быть обменены на биткоины. Цена большинства криптовалют зависит от цены биткоина к фиатным валютам.

- Открытый исходный код. Разработка Биткойн ведётся с открытым исходным кодом и любой разработчик может внести свой вклад в проект. Также можно создать свою криптовалюту. Биткоин-клиент написан на

языке C++. Всё, что вам может понадобиться, находится в репозитории на GitHub. Ну и конечно, навыки программирования, так как изменением пары строчек кода не удастся создать новый форк Bitcoin, для этого понадобится гораздо больше времени и усилий.

На втором почетном месте проект – **Ethereum** Платформа для разработки децентрализованных приложений с использованием смарт-контрактов. На данный момент единственная готовая платформа, которая предлагает наиболее полный функционал для запуска проектов. Уникальные особенности:

- Можно запускать смарт-контракты на тюринг-полном языке. О них было рассказано подробно в шестом эпизоде лекции.
- Существует разные стандарты смарт-контрактов. В шестом эпизоде лекции мы говорили о двух самых популярных стандартах – ERC-20 и ERC-721. Помимо них, можно упомянуть стандарты ERC-223,-777,-621 и многие другие , исправляющий проблемы существующие в токенах ERC-20 или добавляющие новые функции.
- Для написание смарт-контрактов используется язык Solidity.
- Еще одной особенностью проекта можно считать самое большое количество разработчиков в среде блокчейн.
- А также большие планы по повышению скорости работы сети.
- Эфириум имеет открытый исходных код
- Используется алгоритм консенсуса – Proof-of-Work.

Один из проектов с которым Вы неизбежно столкнетесь, когда посещаете блокчейн конференции и отслеживаете новости о блокчейн – это **Hyperledger** от Linux Foundation.

Уже сейчас существует множество блокчейн-сетей и скоро назреет необходимость как-то взаимодействовать друг с другом. Возможность такого взаимодействия рарабочки Hyperledger и закладывают в свои разработки с открытым исходным кодом.

"Зонтичная стратегия"Hyperledger вынашивает и продвигает ряд бизнес блокчейн технологий, структуру, библиотеки, интерфейсы и приложение.

И, пожалуй, самым известным проектом является **Hyperledger Fabric**. Этим проектом руководит IBM. Fabric представляет собой подключаемый модуль и обыгрывает блокчейн технологию, предназначенную в качестве основы для разработки масштабируемых блокчейн приложений с гибким уровнем разрешений.

Уникальные особенности Hyperledger Fabric:

- Одной из особенностей является принципиальный отказ от создания собственных криптоактивов. Участники Hyperledger Fabric развивают проекты сугубо как информационную технологию. Тем не менее Hyperledger Fabric позволяет хранить информацию о физическом имуществе и обязательствах.

- Чейн-код. По сути это смарт-контракт. Но для программирования смарт-контрактов в Hyperledger Fabric используется язык GO и предусмотрена поддержка Java и Javascript. Приятный момент, ведь для написания смарт-контрактов на Ethereum приходится осваивать специальный язык Solidity.

- Сервисная служба. Именно она участвует в формирование новых блоков. Работа сервисной службы — одна из самых интересных технических деталей в Hyperledger Fabric. В отличие от других блокчейнов, здесь возможны разные механизмы достижения консенсуса.

Основным механизмом, который предлагают разработчики, является практический подход к византийской отказоустойчивости. Он обеспечивает устойчивость к двум типам ошибок распределенных систем: когда узел полностью выходит из строя и перестает откликаться и когда он продолжает работать, но выдает ошибки.

Устройство алгоритма основано на старой «Задаче византийских генералов», которое было рассмотрено в 5 эпизоде.

Алгоритм работает, предполагая, что из 10 узлов — скомпрометированы три. Алгоритм устойчивый, но с ростом количества узлов скорость достижения консенсуса в нем падает. Для случаев, когда это становится критичным, у Hyperledger Fabric есть другие механизмы. Это – кластер, называемый Kafka, в котором сервисные узлы вносят транзакции в строго заданной последовательности. Либо использование одного узла, который обеспечивает формирование блоков транзакций и консенсуса ему достигать ни с кем не нужно.

Также очень известен стал проект **Ripple**.

Криптовалютная платформа для платёжных систем. В данной технологии нет полной децентрализации, зато есть центры влияния в виде банковских ассоциаций и поставщиков ликвидности. По сути, это отдельная платформа, использующая только общие принципы блокчейна. Изначально создатели вообще не планировали делать из Ripple криптовалюту: создавалась глобальная платформа обмена ценностями в режиме реального времени. Основная разница с биткоином в том, что последний позволяет переводить ценности от одного человека к другому, а рипл дает возможность ценностями только банковским структурам. На сегодня у Ripple более 100 партнеров,

среди которых American Express, MoneyGram, UniCredit и многие другие известные банковские системы.

С Ripple уже сотрудничают Чикагская товарная биржа, Microsoft и технологическая корпорация Seagate. Официальные представительства команды разработчиков открыты в Сан-Франциско, Нью-Йорке, Сиднее, Лондоне, Токио, Мумбае, Люксембурге, Шанхае и других финансовых центрах мира.

Уникальные особенности:

- Межвалютная платёжная система. Ripple позволяет пользователям или предприятиям проводить межвалютные транзакции. Алгоритм поиска путей Ripple ищет самый быстрый и дешевый путь между двумя валютами. В случае если пользователь хочет отправить платёж из долларов в евро, это может быть путь в один шаг, в других случаях он может быть многошаговым, что позволяет найти самый дешевый способ обмена для пользователя.

- Высокая скорость обработки транзакций. За одну секунду в сети Ripple обрабатывается более 1,500 транзакций. А одна транзакция обрабатывается всего за 4 секунды. Это гораздо быстрее чем в сети Биткоин или Эфириум.

- Консенсусный реестр. Основой сети Ripple является «реестр» в виде распределенной базы данных. Этот реестр – общий между всеми серверами, то есть у каждого сервера своя копия базы, содержащая информацию о всех аккаунтах сети Ripple. При подтверждении сделок запрос обрабатывается всеми узлами, и если достигается согласие, операция подтверждается. При возникновении разногласий проводится повторный цикл, до тех пор, пока квалифицированное большинство не придёт к итоговому консенсусу.

Еще один известный проект, пришедший из азиатского региона **NEM**.

NEM может использоваться как система для платежей, голосования, для хешей файлов в блокчейне, для создания токенов, и для создание приватного блокчейна.

Очень популярен в Японии. С NEM Foundation сотрудничают: Mitsubishi, Hitachi, Toyota, Jaguar, правительство Японии, Сингапура, Малазии.

Уникальные особенности:

- Proof-of-Importance, о нем было рассказано в пятом эпизоде лекции.

- Mijing (Ми'инг) – платформа для создания приватного блокчейна. Каждый бизнес может создать свой блокчейн, который не будет ограничен по функциональности в сравнении с основной сетью. функционал

может быть расширен добавлением возможности создания и запуска смарт-контрактов. Такой подход несет в себе огромную пользу реальному сектору. Каждый бизнес может получить свой блокчейн, да еще и со смарт-контрактами и скоростью транзакции до 10 000 в секунду.

- Mosaic – платформа для создания токенов. Токены могут иметь свой набор функций. они могут быть делимыми и неделимыми, передаваемыми и непередаваемыми.

- Apostille – платформа для создания и хранения хешей файлов в блокчейне.

- Catapult – технология, которая позволяет синхронизировать приватный и публичный блокчейн NEM.

Не забудем и о новом проекте, который собрал больше всего средств на ICO – **EOS**.

Основная идея разработчиков – создать децентрализованную платформу с высокой пропускной способностью, функцией смарт-контрактов и минимальной комиссией. Программное обеспечение EOS предлагает иерархичне аккаунты, аутентификацию, базы данных, асинхронную коммуникацию и диспетчеризацию приложений на сотнях компьютерных устройств или кластерах. Итоговая технология представляет собой блокчейн-архитектуру, которая масштабируется до миллионов транзакций в секунду, устраняет пользовательские комиссии и дает возможность быстрого и простого развертывания децентрализованных приложений.

Уникальные особенности:

- Алгоритм консенсуса – Delegated proof-of-stake. Основной принцип работы – разделение голосующих и валидирующих участников. В итоге, участники сети, которые имеют право голоса в системе (держатели монет) не являются при этом валидаторами транзакций. Таким образом, одна группа участников выбирает другую группу, которая в свою очередь будет формировать блоки.

- Также, EOS предоставляет возможность пользователям создавать уникальные имена для своих аккаунтов длиною до 12 символов.

- Хранилище EOS – децентрализованная файловая система, предназначенная для хранения и размещения информации.

Возможную конкуренцию Эфириуму и EOS может составить проект **Cardano**. Платформа направлена на запуск смарт-контрактов, децентрализованных приложений, сайдчейнов и многопартийных вычислений.

Уникальные особенности:

- Алгоритм Cardano Proof-of-stake.

- Cardano использует новый алгоритм доказательства владения, называемый Уроборос, определяющий то, как отдельные ноды достигают консенсуса в отношении сети. Алгоритм является ключевой частью инфраструктуры, которая поддерживает криптовалюту ADA.

- В Cardano новые блоки генерируются случайным образом выбираемыми держателями монет; вероятность выбора того или иного пользователя пропорциональна размеру его депозита. Это реализуется через своего рода лотерею, которая определяет для держателей монет временные интервалы на то, чтобы они приступили к созданию нового блока для обновления блокчейна. Если пользователь не производит блок в рамках назначенного ему временного интервала, его очередь просто пропускается.

- Чтобы достигнуть хорошего уровня безопасности, Cardano использует математическое доказательство безопасности. По этой причине Cardano является одним из самых безопасных и масштабируемых блокчейнов на рынке.

А теперь немного уйдем в сторону от смарт-контрактов и рассмотрим проект **IOTA**, созданный как основа для развивающегося рынка *интернета вещей*.

IOTA – протокол распределенного реестра с открытым кодом, который выходит за пределы блокчейна при помощи его главного изобретения – безблочной технологии Tangle. IOTA Tangle – защищённый от квантового вмешательства направленный ациклический граф (DAG) без сборов за транзакции и без установленного ограничения числа транзакций подтверждаемых за секунду. Вместо этого, пропускная способность растет вместе с увеличением активности в сети: чем больше активность, тем быстрее работает сеть. В отличие от архитектуры блокчейна, у IOTA нет разделения между пользователями и валидаторами. Валидация здесь – внутреннее свойство работы с реестром, которое позволяет избежать централизации.

Уникальные особенности:

- Технология направленного ациклического графа (DAG) Tangle. О ней мы рассказывали в первом эпизоде лекции.

- Возможность совершать транзакции без подключения к глобальной сети.

Алгоритмы IOTA позволяют совершать платежи даже не имея подключения к глобальной сети, в отличие от биткоина и других классических криптовалют, которые требуют синхронизации со всей сетью. Устройства, отключенные от интернета, будут использовать локальную структуру хэшей и им будет достаточно подключаться к интернету не более 1-2-х раз в сутки. Это невозможно в традиционном блокчейне, так как будет являться форком, и подобные оффлайн транзакции будут отвергнуты сетью. Здесь же мы имеем абсолютную толерантность к ветвлению, что делает сеть пластичной и бесконечно масштабируемой. Если транзакция проводится в кластере, который не подключен к интернету, допустим в какой-то локальной сети, то его целостность сохраниться и после подключения к глобальному интернету.

Нельзя не отметить русский проект **Waves**, который представляет собой открытую блокчейн-платформа, которая берёт функционал биткоина и расширяет его за пределы простой передачи ценностей. Идея в создании платформы, на которой биткоин, криптовалюты, фиатные валюты и все типы активов реального мира можно будет выпускать, передавать и обменивать полностью децентрализованным способом. Платформа Waves также предоставляет краудфандинговое решение при помощи облегченного клиента.

Уникальные особенности:

- Алгоритм консенсуса Leased Proof Of Stake. Модификация консенсуса Proof-of-stake. Особенностью Leased Proof Of Stake является возможность для пользователей передавать собственные балансы полным узлам на правах аренды в обмен на часть прибыли от майнинга.

- Децентрализованная биржа DEX. Децентрализованная площадка для торговли криптовалютами, с возможностью обмена на фиатные валюты. Платформа предоставляет сервер, который принимает входящие заказы, но не имеет доступа к средствам пользователя. Пользователь постоянно имеет и не теряет полный контроль над своими средствами во время размещения их на бирже. Когда сервер находит подходящую пару для совершения сделки, он инициирует передачу средств и фиксирует в блокчейне перемещение. Правильность сделки проверяется и заверяется децентрализованным образом.

- Токенизация валюты. Пользователи могу легко конвертировать фиатные валюты в токены на блокчейне Waves. Эти фиатные токены можно передавать внутри блокчейна гораздо быстрее, чем это можно было бы сделать при помощи обычного банковского перевода, и за намного меньшую плату. После получения токенов пользователи могут обменять их на фиатные валюты. Прочие криптовалюты также можно токенизировать на платформе.

- При помощи удобного клиента и интегрированных фиатных валют Waves предоставляет новым пользователям доступ к миру технологии блокчейн и криптовалют. Пользователи могут работать с фиатными валютами или знакомыми им активами. Также пользователи могут инвестировать в акции компаний и активы при помощи краудфандинговой платформы Waves, благодаря которой разработчики и предприниматели могут привлекать необходимые для развития проектов средства.

Мы успели рассмотреть самые интересные проекты из среды. Но этим обзором история не исчерпывается. Существуют много интересных проектов, некоторые из которых находятся в стадии разработки. Вы можете узнать о них более подробно, изучив дополнительные материалы.