1.2. РАЗМЫШЛЕНИЯ НА ТЕМУ ТЕХНОЛОГИИ БЛОКЧЕЙН

Ерешко Ф.И., д.т.н., заведующий отделом информационно-вычислительных систем,
Вычислительный центр им. А.А. Дородницына ФИЦ ИУ РАН

Технология блокчейн предназначена для Проектов, где наличествует сообщество активных агентов, которые создают Коалицию для решения общей задачи, достижения общей цели и согласовывают механизмы ее решения. Поэтому всегда разработку Проектов нужно начинать с дескриптивной и теоретико-игровой моделей, а не с криптографии. И это представлено в обзоре уже существующих Цифровых платформ, среди них Эфириум, Мастерчейен и др. Эта схема приведена далее в тексте. Непременной составляющей всех Цифровых платформ является модель: одноранговая, многоролевая и т.д. Приводится описание варианта модели распространения информации в сети Проекта Биткоин, который принят как образец для иллюстраций и приложений. Отмечается, что имеется опыт построения подобных моделей и есть понимание, как в моделях учитывать технологию блокчейн. Предлагается создать математический прообраз для оценки возможного приложения технологии блокчейн для различных архитектур организационных систем и механизмов принятия решений.

Введение

Технология блокчейн – это специализированная информационно-коммуникационная технология (что эквивалентно определяется как приемы, способы и методы применения вычислительной техники[1]) для выполнения функций сбора, хранения, обработки, передачи и использования данных[2], обладающая специфическими особенностями. Две особенности отделяют технологию блокчейн от ряда технологий ведения распределенных баз данных: криптографическая защита данных и децентрализованная процедура обеспечения согласования интересов всех участников, т.е. достижения заданного консенсуса. Широкий интерес к этой технологии возник в последнее время в связи с ажиотажным спросом на криптовалюты и интересом к Проектам в этой сфере, выделим среди них Проект Биткоин и Проект Ethereum («Эфириум»).

Проект Биткоин по сути – это организация определенной экономической деятельности группы лиц, создававшийся первоначально, как платежная система для расчетов между ними, теперь обеспечивает увеличение богатства участников Проекта путем производства цифрового продукта(=биткоина). Как мы наблюдаем сейчас, цена биткоина в долларах стремительно возрастает, и тем самым возрастает богатство участников. Возможность обмена биткоина на фиатные деньги сделала привлекательным участие в Проекте.

В Проекте Биткоин принимает участие динамическая Коалиция (ее члены приходят и уходят). Каждый участник входит в Колицию, принимая условия членства в сообществе Проекта Биткоин. Он получает от Ядра.Биткоин исходное программное обеспечение, начинает его использовать для решения заданного скалярного неравенства и вычисления некоторого параметра. В случае успешного решения неравенства он получает стимулирующее право на увеличение количества условных монет в своей базе данных.

Современное развитие Проекта Биткоин вполне соответствует экономическому явлению, имманентно присущему рыночной экономике, которое носит название «пузырь». Термин «пузырь» (bubble) прочно вошел в научный и практический лексикон Западной науки и практики. Под «Пузырем» понимается чрезвычайно быстрый рост экономических показателей, например, цен, что предвещает, в силу объективных экономических законов, последующий спад.

Вот, что говорит главный финансовый мировой гуру Алан Гринспен[3], определявший длительное время направление развития мировых финансов, вообще о явлении «пузыря»:

> «*We, at the Federal Reserve…recognized that, despite our suspicions, it was very difficult to definitively identify a bubble until after the fact, that is, when its bursting confirmed its existence… Moreover, it was far from obvious that bubbles, even if identified early, could be preempted short of the Central Bank inducing a substantial contraction in economic activity, the very outcome we would be seeking to avoid*»[4]. Перевести на русский язык это можно так: «*Мы, в Федеральной резервной системе, осознаем, что, несмотря на наши подозрения, было очень трудно определенно идентифицировать «пузырь» до его факта, то есть до того, как он лопнул и тем самым подтвердил свое существование… Более того, далеко не очевидно, что даже если бы пузыри были вовремя распознаны, их можно было бы обезвредить посредством серьезных ограничений Центральным Банком экономической активности, и это привело бы именно к тому результату, к которому мы стремились*».

[1] https://ru.wikipedia.org/wiki/Компьютер
[2] https://ru.wikipedia.org/wiki/Данные
[3] Алан Гринспен – глава Федеральной резервной системы США на тот момент (30 августа 2002 г.)
[4] The Fed: A. Greenspan (Aug., 30, 2002)

Основная проблема состоит в понимании развития Проекта после прохождения пика сверхэкспоненциального роста: если наступит крах системы, и финансовые рынки рухнут, это означает, что «пузырь лопнул». Если происходит плавное снижение активности, то говорят: это было обычное циклическое развитие экономики. Схлопывание «пузыря» проявляется в форме социально-экономического кризиса и имеет разнообразные последствия, некоторые из них имеют положительное влияние на развитие общества и используется далее в жизнедеятельности.

Последние из кризисов – dot-com bubble и ипотечный кризис – оставили после себя широкое распространение информационных технологий и углубленное государственное регулирования ипотечных займов, опыт выхода государства из ипотечного кризиса. Значительный интерес к криптовалютам ввел в арсенал научных методологий и прикладных разработок технологию блокчейн, как одну из эффективных технологий поддержки коалиционных решений.

Есть принципиальное отличие в организации Проекта Биткоин от спекулятивных акций типа пирамиды. Но там и здесь задействован механизм ажиотажа, запущенный вне Проекта, и связанный с возможностью обмена криптовалют на фиатные деньги. Вот какое мнение Алана Гринспена о биткоине (2013 год):

> «*Я бы использовал аналогию с континентальным долларом. Он был выпущен в 1775 году без какого-либо обеспечения, в итоге к концу войны за независимость все «континентальные» доллары и доллары штатов не были погашены, и были выведены из обращения. Человеческая природа такова, что, если вы получаете что-то вроде биткоина, вы думаете, что он чем-либо обеспечен. Но биткоин больше похож именно на континентальный доллар, который не имел никакой ценности и служил только целям гражданской войны*» [5]. «*Биткоин не имеет фактической ценности. Вы должны действительно сильно пофантазировать, чтобы понять какова его истинная ценность. Я не смог этого сделать. Может быть, кто-то другой сможет*».

А вот каким стало мнение у Алана Гринспена в 2017 году:

> «*Биткоин – это восхитительный пример того, как люди могут создавать ценность, не руководствуясь при этом соображениями рациональности. В этом случае перед нами лежит нерациональная валюта*»[6].

Проект Биткоин – это рыночный механизм, но это не предмет наших текущих исследований. Наша задача, опираясь на идеологию системного анализа и теории принятия решений, исследования операций, теории игр провести анализ совокупности процедур, составляющих технологию блокчейн.

В исходной статье С. Накамото и в комментариях средств массовой информации в последующем превалирующее место занял процесс защиты данных на основе криптографических алгоритмов. Эта оригинальная конструкция, безусловно, имеющая фундаментальный характер, была использована в качестве главного аргумента для обоснования идеи защищенности частных денег и поддержала интерес к криптовалютам. Из этой идеи и всеобщего интереса выкристаллизовался рациональный элемент Проекта Биткоин – технология блокчейн.

Основная установка

В рамках системного подхода к исследованию явлений в природе и обществе и при проектировании прикладных систем предполагаются следующие этапы: содержательное изучение и осмысление конкретного объекта, построение моделей, определение информационных баз данных, реализация программного обеспечения, разработка сценариев и проведение вычислительных экспериментов в имитационном режиме. Тем самым первичны: постановка проблемы, описание Проекта, и построение соответствующей модели.

Общеизвестно, что модели могут быть эвристические, натурные (физические) и математические. Весь этот арсенал пригоден в данных ситуациях. В наших возможностях – использование информационных и математических моделей. Это обстоятельство вполне понимается разработчиками текущих цифровых платформ, что иллюстрируется на следующей таблице, где в каждом описании цифровой платформы присутствуют понятия Проект и Модель.

Для проблематики, связанной с использованием технологии блокчейн, исходным в постановке, безусловно, является сообщество активных агентов, каждый из которых имеет свои цели, ресурсы и информированность. Сообщество, образуя коалицию, вырабатывает общую цель, ради которой создается коалиция, и механизмы ее достижения. Сообщество может возникнуть стихийно, а может быть создано некоторым физическим или юридическим лицом, конструктором, Центром. Процедуры управления в коалиции могут быть централизованными либо децентрализованными. В общее Соглашение коалиции

[5] Бывший глава ФРС Алан Гринспен: Биткойн ничем не обеспечен, BITS MEDIA, 16.11.2017 // https://bits.media/

[6] Биткоин – это отражение нерациональной сущности человечества – экс-глава ФРС, TTRCOIN, 07.12.2017 // https://ttrcoin.com/

включается различные целевые условия, касающиеся функционирование сообщества в рамках коалиции, например, вопросы общей информированности, распределение достигнутого общего блага, частных и общих стратегий поведения и т.д.

Пример. Проект Биткоин: первичен был проект платежной системы, предложенный Сатоши Накамото, который дал в виде статьи описание Проекта создания аналога денег как обменного инструмента для некоторого сообщества лиц и создал первичное программное обеспечение. Затем возникла группа лиц, последователей, которая улучшила программное обеспечение и взяла на себя функции поддержки ПО, а затем возникла за счет стихийного интереса или организованной рекламной кампании сеть бирж для обмена права на монеты, обеспеченного согласием членов коалиции, на фиатные деньги, и коалиция стала разрастаться, и цена обмена увеличиваться.

Приведенное описание подчеркивает основную установку настоящего изложения: в основе всех Проектов использования технологии блокчейн исходно лежит идея создания коалиции. Следующим работоспособным примером создания коалиции с использованием технологии блокчейн для поддержания функционирования коалиции является Платформа Ethereum («Эфириум»).

Целевая установка коалиции сообщества в Проекте Ethereum («Эфириум») состояла в автоматизации процесса заключения контрактов между участниками, активными экономическими агентами.

В завершающем абзаце обзора[7], непосредственно посвященном проблематике использования технологий блокчейна в теории принятия решений, указывается, что децентрализованные приложения и децентрализованные организации на базе блокчейна могут создавать конкуренции правительственным организациям в исполнении управляющих и регулирующих функций.

Примеры разработок

Примеры реальных Проектов приведены в вышеописанной Таблице. Кроме того, задачи управления перечислены в Программе РФ по Цифровой экономике в разделах 10 и 12.

В работе [ШВАБ, 2016] приведена фраза: «*Дизруптивные изменения, которые несет четвертая промышленная революция, переопределяют деятельность государственных учреждений и организаций …*». Очевидны также перспективы применения технологии блокчейн в сферах банковской деятельности (организация фондов заемщиков, процессов кредитования), бизнесе (организация инвестиционных проектов), в государственном управлении, в строительстве организационных структур политических партий. Организационная архитектура блокчейнов может приспосабливаться к сложным системам управления и организационным структурам, наряду с плоскими схемами p2p, появятся иерархические блокчейны, матричные блокчейны и другие архитектурные формы.

Интерес к децентрализованной организации управления в Проекте Биткоин на основе технологии блокчейн для нас (исследователей операций, специалистов в теории управления) состоит в том, что перед нами разворачивается живой уникальный социально-экономический эксперимент, в котором реализуются различные механизмы управления. Имеется широкий простор для постановки различных задач, представляющих к тому же живой и обширный интерес во всем мире. Вот что говорит Стив Возняк о соперничестве блокчейна с бюрократией[8]:

> «*Сложно прогнозировать, достаточно ли силен блокчейн, чтобы изменить мир. Бюрократическая система сложна для понимания, особенно с точки зрения математической, логической систем. Технологии – это движение вперед, бюрократия – от желания контролировать. За блокчейн стоит бороться. Когда эта технология только появилась, мне понравилась ее математическая составляющая. Вот, скажем, биткоины. Мы живем в системе, где постоянно печатаются деньги. Биткоин – очень взвешенная система. В блокчейне отсутствует централизация, и это очень важно, он ведет к развитию горизонтальной связи. Блокчейн уже проникает в нашу жизнь, а в будущем точно будет в медицинской и банковской сферах*»

ОПИСАНИЕ ЭСКИЗА МОДЕЛИ

В той конкретной версии, с которой можно ознакомиться при описании Проектов Биткоин и Ethereum, технология блокчейн включает в себя последовательность действий для достижения консенсуса, т.е. достижения согласованного результата, оговоренного условиями вхождения участников в коалицию, принятию всеми участниками проекта (узлов сети) решений задач по поиску параметра nonce и подтверждения транзакций. Настоящая модель предназначена для анализа достижения консенсуса и угроз возникновения форков (разветвлений траекторий распространения информации в сети).

- Проект

Проект программного комплекса имитирует некоторые аспекты функционирования блокчейна. За основу взят биткоин. Моделируется часть тех процессов, которые составляют жизнь Биткоина. Основное внимание уделяется генерированию новых блоков с позиции угрозы возникновения форков (развилок). Модель создается для исследования форков и других вопросов, связанных с биткоином. Нижеследующее описание сделано в теоретико-игровой (субъектной) форме, в которой элементы, составляющие модель, выполняют отдельную самостоятельную работу. В окончательном виде, модель должна быть

[7] https://en.wikipedia.org/wiki/Decentralization

[8] Вячеслав Опахин, Мы никогда не полетим на другую планету, 07.10.2017, Новости Hi-tech, https://hi-tech.mail.ru/

реализована в виде программы, которая последовательно обрабатывает временные шаги модели и на каждом из них автономно модифицирует состояние каждого из элементов модели – узлов сети.

- Время дискретно

Строим модель с дискретным временем, т.е. потактовую. Шаги (такты) модели будем обозначать через t. Шаг модели – это довольно малая величина. Пока не определено, на какой стоит остановиться.

- Множество объектов

Рассматривается множество объектов, которые мы будем называть узлами Сети. Будем полагать, что все моделируемые узлы совмещают в себе майнинговые и коммуникационные свойства, это допущение. Число узлов сети обозначим N_t. Это величина переменная. С определенной заданной в модели вероятностью $\alpha^+(n)$ на каждом шаге модели может создаваться n новых узлов. И с вероятностью α^- любой из существующих узлов может аннулироваться. Появление узла означает, что он сразу начинает функционировать, работая с текущем состоянием блокчейна. Так как время от времени разные узлы могут поддерживать различные версии блокчейна, условимся, что новый узел принимает версию узла корреспондента с наименьшим номером. Варьируя значения α^+ и α^-, можно выбрать оптимальный для модели примерный максимальный размер сети. На практике уже существующие узлы могут временно отключаться и включаться вновь. Пока эту возможность можно не учитывать, так как нет смысла усложнять модель этим эффектом.

- Мощность узла

Каждому узлу n приписывается некоторая условная величина P_n, характеризующая мощность майнинг-оборудования. Эта величина выбирается вероятностным образом в момент создания узла. Полагаем, что она не меняется в продолжении всей жизни узла (*что. конечно, весьма условно)*.

ДУГИ (КАНАЛЫ) СВЯЗИ

Узлы сети связаны друг с другом двунаправленными дугами. Дуги моделируют каналы связи, по которым передается информация. Будем считать, что на каждом шаге t у каждого узла должно быть не менее, чем S^{min} каналов связи. Каналы выбираются случайным образом при создании узла и сохраняются. На шаге t узел n может иметь меньшее, чем S^{min} число дуг. Это возможно из-за прекращения работы узла-корреспондента. В этом случае для узла n случайным образом выбирается новый корреспондент. Новая дуга начинает функционировать с лагом времени t^s.

Комментарий. На практике узлы сами заботятся о наличии связей, делая соответствующие запросы, и только от их владельцев зависит, со сколькими другими узлами связаны их узлы. Так как корреспонденты выбираются случайным образом, в модели их число для отдельного узла может заметно превышать величину S^{min}.

ИНФОРМАЦИЯ УЧАСТНИКА (УЗЛА)

Опишем, какой информацией обладает участник (узел) n к моменту t.

Ему известна сформированная к этому моменту цепочка блоков. **Каждый блок характеризуется его номером и уникальным идентификатором (именем).** Он содержит пронумерованные имена предыдущих блоков и множество имен, включенных в него транзакций.

Комментарий. Имя блока моделирует хэш реального блока. В модели для создания имени можно использовать любую функцию, которая случайным образом выдает достаточно длинный набор символов. Можно использовать и хэш-функцию. Почему нет? На практике для проверки участником соответствия нового блока его версии цепочки достаточно хранить только ссылку на предыдущий блок. Это достигается за счет уникальности хэшей. Так как пока в модели хлопотный аппарат хэшей не предполагается как обязательный элемент, чтобы обеспечить проверку соответствия блока и цепочки, вводится сопровождение блока списком имен предшествующих блоков.

Реальный блок содержит набор данных, нужных для удобства работы сети и для защиты информации. Здесь, в этой модели пока все это не рассматривается. Предполагается, что информация в достаточной степени защищена криптографией от фальсификации. То же относится и к транзакциям, которые на практике содержат ключи, входы, выходы и всякую сопроводительную информацию. Пока все это в модель не включается. В модели предполагается, что каждую транзакцию отличает уникальный код (имя) (в реальности, по-видимому, хэш) и только.

ПУЛ НЕУЧТЕННЫХ ТРАНЗАКЦИЙ

Каждый участник поддерживает пул, неучтенных (еще не включенных в блокчейн, неподтвержденных) транзакций. Этот пул составлен из транзакций, полученных участником по сети от момента t' последнего включения участником блока в свою версию блокчейна, до текущего момента t, а также из транзакций, содержавшихся в пуле к моменту t' и не попавших в последний блок.

СОБЫТИЯ НА ШАГЕ t

На шаге t происходят следующие события.

t.1. С заданной вероятностью $\mu(k)$ узел n принимает к обработке k вновь созданных транзакций.

Комментарий. Это транзакции, созданные либо самим участником n, либо не представленными в модели, анонимными, держателями кошельков, которые, как подразумевается, напрямую коммутированы с узлом n.

Узел включает эти транзакции в свой пул неподтвержденных транзакций. Их же он передает по каналам связи коммутированным с ним узлам.

t.2 Кроме того, узел принимает от своих корреспондентов передаваемые по сети транзакции, которые поступили ранее на другие узлы. Время передачи пакета транзакций от узла к узлу будем считать постоянным и обозначим τ_1.

Комментарий. Быть может, имеет смысл положить его равным минимальному, т.е. 1, быть может, сделать пропорциональным числу передаваемых транзакций – пока не ясно

Участник проверяет, не содержаться ли эти транзакции в его пуле неподтвержденных транзакций. Те, которые еще не содержаться, он добавляет в пул, а также пересылает своим корреспондентам, если только они не были от них же получены.

t.3 Участник n на шаге t может получить от узлов-корреспондентов новый, очередной блок, созданный на одном из узлов сети. Получив новый блок, участник проверяет его номер. Если он меньше или равен номеру m, последнему в текущей цепочке участника n, то такой блок отвергается. Если этот номер больше или равен $m+1$ и не поступал на узел n ранее на шагах $\leq t$, то блок пересылается по сети корреспондентам участника n. Данные нового блока распространяются по сети со скоростью τ_2, т.е. узлы-корреспонденты получат этот блок на шаге $t+\tau_2$.

Комментарий. На шаге t один и тот же блок может прийти несколько раз от разных корреспондентов.

t.4 Если номер полученного блока равен $m+1$, и блок ссылается на блок m в цепи участника n как на предыдущий, то участник добавляет этот блок к своей цепочке.

t.5 Если номер полученного блока $m' > m+1$, то участник n делает (обратный) запрос к узлу, приславшему данный блок. Это запрос с требованием выслать цепочку блоков с номерами $m+1 \leq m' < m^{"}$. Он будет получен адресатом на шаге $t+1$.

t.6 Если номер полученного блока равен $m+1$, но указанное в нем имя предыдущего блока отличается от имени блока m в цепи узла n, то участник n сравнивает имена блоков в своей цепочке с их именами в полученном блоке и находит номер $\tilde{m}$, первый, где есть расхождение. Затем он на том же шаге t делает (обратный) запрос к узлу, приславшему данный блок, с тем, чтобы тот переслал ему все другие блоки, начиная с номера $\tilde{m}$.

t.7 Некоторое время у участника n уйдет на этот обмен данными и проверку присланной цепочки. Оценим это время как $q\tau_2+1$, где q – число запрошенных блоков. После этого узел n производит замену блоков своей цепочки с соответствующими номерами на полученные блоки и переходит к использованию нового экземпляра блокчейна.

Комментарий..Номер пришедшего блока может быть меньше ожидаемого в случае попытки фальсификации цепочки. Но он также может быть меньшим просто из-за более долгого пути по сети, чем путь для некоторого блока, созданного на другом узле почти одновременно с ним. Тогда участник n, получив более «близкий» блок переходит к ожиданию блока с номером на единицу большим.

Комментарий. Если структура сети не меняется и узел n на шаге t не находится в состоянии ожидания ответа на запрос от узла-корреспондента, то, по-видимому, невозможна ситуация, когда вновь пришедший блок имеет номер, больше, чем ожидаемый $m+1$. При появлении новых узлов такое, вообще говоря, возможно. Новый узел может начать функционировать, загрузив цепь до номера $m+1$. При этом на этот узел может очень быстро прийти информация о блоке $m+2$, которую он сразу передаст своим корреспондентам. Но пути, по которым движется информация к этим корреспондентам о блоке $m+1$ могут оказаться длиннее, чем новый путь, по которому прошла информация о блоке $m+2$. Впрочем, вся эта ситуация представляется весьма казуистической. В отличие от задержек, связанных с обратным запросом.

СИТУАЦИЯ ФОРКА

Комментарий Случай обратного запроса – это, как раз, ситуация форка. Представленный выше способ ее разрешения – допущение. Пока не удается обнаружить описание того, как именно действуют узлы в реальности при замене одной версии цепи на другую.

ВАЛИДАЦИЯ

Комментарий Валидация, т.е., в данном контексте, проверка корректности блока и блокчейна в целом, на практике включает в себя множество действий. Проверяются хэши блоков, заголовки, размеры блоков, сами транзакции. Пока моделировать все это не обязательно. Будем исходить из того, что все новые блоки корректны. Тогда валидация сводится к проверке номеров и имен блоков.

После валидации и добавления в блокчейн нового блока (или блоков, пришедших в ответ на обратный запрос), узел n сравнивает состав (набор транзакций) нового блока и своего пула неподтвержденных транзакций, оставляя в последнем лишь те, что по-прежнему не включены в блокчейн. После этого

участник немедленно, т.е. на том же шаге t, приступает к майнингу нового блока, включая в него все оставшиеся в пуле неучтенные транзакции.

ОГРАНИЧЕНИЯ ОБЪЕМА БЛОКА

Комментарий. На практике объем блока ограничен. Поэтому в новый блок включаются, вообще говоря, не все транзакции из пула, а согласно приоритетам.

Однако пока нигде не найдены объяснения, как решается проблема переполнения пула неподтвержденных транзакций. Поэтому принимается допущение, что объем блоков неограничен и, следовательно, в него майнером включаются все неучтенные к началу майнинга транзакции.

СОБСТВЕННЫЙ НОВЫЙ БЛОК

С некоторой вероятностью участник n на шаге t создает собственный новый блок. В этом случае он делает те же внутренние действия и распространяет этот блок по сети точно так же, как это описано выше для случая, когда корректный блок приходит со стороны. Вероятность создания нового блока на текущем шаге определяем формулой

$$\Omega_t^n = \frac{1}{T} \times \frac{P_n}{\sum_{k=1}^{N_t} P_k}$$

Здесь T – среднее время, выраженное в шагах модели, между появлением новых блоков.

Комментарий. На практике Блокчейн пытается поддерживать периодичность появления новых блоков, примерно, в 10 мин. Делается это несколько более сложным приемом – изменением трудности решаемой задачи, причем коррекция производится не на каждом шаге, а тоже с некоторой периодичностью. В данной модели не обязательно принимать это усложнение.

Литература

1. Satoshi Nakamoto (2009). Bitcoin: A Peer-to-Peer Electronic Cash System, www.bitcoin.org
2. Antonopoulos, Andreas M. Mastering Bitcoin. UNLOCKING DIGITAL CRYPTOCURRENCIES, O'Reilly Media, Inc., 2014, – 272 p.
3. Narayanan A., Bonneau J., Felten E., Miller A., Goldfeder S.. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton : Princeton University Press, 2016. – p.
4. Ерешко Ф. И. Теория иерархических игр в приложении к законотворчеству в цифровом обществе. Бизнес в законе. // Computational nanotechnolgy, 2017, №2, С. 52–58.
5. Равал С. Децентрализованные приложения. Технология Blockchain в действии. — СПб.: Питер, 2017. — 240 с.
6. Шваб, К. Четвертая промышленная революция / К. Шваб. - ЭКСМО, 2016, 230 с.

Ерешко Феликс Иванович

Ключевые слова

Блокчейн, хэш, коалиция, форк, биткоин

Ereshko Feliks,. Thinking about blockchain

Keywords

Blockchain, hash, coalition, fork, bitcoin

Abstract

Blockchain Technology is intended for Projects where there is a community of active agents who create a Coalition to solve a common problem, achieve a common goal and agree on mechanisms for its solution. Therefore, always the development of Projects should be started with descriptive and game-theoretic models, not cryptography. And it is presented in the review of existing Digital platforms, including Ethereum, Mastercar etc. This scheme is given later in the text. An indispensable component of all Digital boards is a model: peer-to-peer, multi-role, etc. A description of the version of the model of information dissemination in the network of the Bitcoin Project, which is accepted as a model for illustrations and applications, is given. It is noted that there is experience in building such models and there is an understanding of how to take into account the blockchain technology in the models. It is proposed to create a mathematical prototype to assess the possible application of blockchain technology for various architectures of organizational systems and decision-making mechanisms.

DOI: 10.34706/DE-2018-04-02