Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет информатики и радиоэлектроники

УДК 004.42

Бисярин

Георгий Александрович

БЛОКЧЕЙН ТЕХНОЛОГИИ: СУЩНОСТЬ И ОСОБЕННОСТИ РАЗРАБОТКИ

АВТОРЕФЕРАТ

на соискание степени магистра экономических наук

по специальности 1-25 80 04 «Экономика и управление народным хозяйством»

Научный руководитель
Беляцкий Николай Петрович
доктор экономических наук, профессор

Минск 2019

КРАТКОЕ ВВЕДЕНИЕ

За последние 10 лет, технология технология блокчейн продвинулась вперёд технологически. Что ещё более важно, данная технология является одной из самых перспективных и актуальных на сегодняшний день. Считается, что существующие реализации обладают явными преимуществами перед существующими решениями различных задач. Однако стоит акцентировать внимание на более детальных особенностях функционирования данных систем, а именно, как они работают.

Сегодня существует значительное множество литературы, описывающая понятие и экономическую сущность блокчейна. Но что касается материалов, описывающий технические особенности, то на данный момент они описаны лишь в статьях или так называемых «Yellow Paper» - это техническое описание функционирования существующих реализаций блокчейна. Однако последний даёт информацию «как есть», без описания процесса разработки и проблем, связанных с разработкой.

В рамках магистерской диссертации, будет описан путь реализации блокчейн-сети. Диссертация рассматривает компоненты, из которых состоит сеть. Параллельно с описанием назначения компоненты, перечислены некоторые подходы к их разработке, а также проблемы с их реализацией. Помимо технической сущности, работа описывает понятие ICO: как оно работает, зачем оно существует, что предлагается и как в данные предложения инвестируются.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью работы было исследование технических особенностей функционирования блокчейн-сети. Работа описывает процесс формирования блока, его согласования, протоколы коммуникации, синхронизации данных и многих других существующих компонентов.

Структурно работа поделена на три части:

– Теоретическая часть. Описывает теоретическое понятие технологии блокчейн, что это такое, чем она лучше, в чем её недостатки. Также приведены примеры существующих реализаций, их особенности и специфика работы

– Общее описание основных компонентов. Блокчейн есть совокупность технологических решений, совмещённых воедино. Часть работы освещает главные компоненты для функционирования блокчейн-сети.
– Подробное описание реализации. Здесь приведено пояснение реализации одной из блокчейн сети. А именно особенности реализации компонентов: какая задача стоит при проектировании, какие проблемы существуют при структурировании, какие варианты решений и их оценка.

В общем, магистерская диссертация открывает более глубоко детали реализации технологии блокчейн. Впоследствии, были выявлены текущие недостатки и направления, в которых данная технология должна развиваться. Исследованы новые перспективные векторы развития и технологические новшества, пока не получившие широкого распространения среди вендоров блокчейн-платформ.

Объём работы – 104 страницы. Из них 75 страниц есть основное описание работы, 29 страниц приложений.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В первом разделе приведена теоретическая информация о том, что собой представляет блокчейн в общем. Блокчейн – распределённый реестр хранения событий. Исторически блокчейн является сборкой многих технологий, разработанных в течении последнего столетия в области информационных технологий. А именно имеются в виду распределённые системы, компьютерные сети, криптография и т.п. Разработки в данных областях, в совокупности, решают одну задачу – надёжное хранение данных в децентрализованной среде.

Особое внимание уделяется финансовой области применения данной технологии, дающий определенные преимущества криптовалюте, по сравнению с фиатными валютами по следующим пунктам:

– Для начала, криптовалюта не регулируема определенным субъектом. Например выпуск токенов осуществляется исключительно за счет компьютерных алгоритмов.
– Также, благодаря блокчейну, нельзя отследить движение средств, т.к. в первую очередь, в сети нет информации, идентифицирующие владельца

кошелька. Имеется только некоторый набор символов, больше ничего. Более того, учитывая это, не существует связей между кошельками, т.е. вы не можете удтверждать, что имеются кошельки и они принадлежат одному пользователю. Текущая реализация криптокошелька построена так, что даже алгоритмически невозможно выразить это.

Также в первом разделе приведены примеры реализации блокчейн-сети. Первый описывается самая первая известная в мире система – биткоин, который имеет следующие особенности:

- Анонимность – другой участник транзакции будет знать только ваш Bitcoin-адрес или QR-код. Другие данные не разглашаются
- Децентрализованный характер системы – все участники сети равны и независимые
- Безопасность – взлом кошельков, подмена данных, перехват переводов невозможны
- Глобальность – биткоин позволяет быстро проводить транзакции между людьми с разных стран, часовых поясов
- Майнинг – существует самостоятельный способ добычи BTC, рассматриваемый многими в качестве заработка

Далее описывается эфириум. По сравнению с биткоином, это не просто финансовый инструмент обмена средствами. На самом деле это уже блокчейн-платформа, что является более широким понятием, ввиду того, что помимо платежей, пользователь имеет возможность осуществлять любого рода операции, благодаря существованию смарт-контрактов, которые, в свою очередь, предоставляют участнику изменять логику выполнения транзакции.

Предыдущие два примера есть два классических представления блокчейна как цепочки блоков. Однако в мире существуют и реализации с альтернативным представлением хранения информации. IOTA не похожа на биткоин или эфир, так как она фактически не использует блокчейн. Эта платформа использует специальный журнал Tangle, работающий на основе DAG – направленного ациклического графа. В блокчейн Bitcoin или Ethereum все держится на блоках, куда и записывается информацию о транзакциях. В Tangle IOTA блоков нет, а транзакции там связаны по своей особенной схеме.

Второй раздел перечисляет основные функциональные компоненты блокчейн-сети. Ведь распределённые системы, с одной стороны, есть создание блоков, хотя создание блока включает в себя использование алгоритмов шифрования. Блоки нужно каким-то образом передавать другим участникам сети и т.д. Описана структура основных сущностей в блокчейне, а именно блок и транзакция: какие поля каждая сущность хранит и как она калькулируется. Здесь же рассмотрен распространённый алгоритм консенсуса – Proof Of Work. Вообще, без консенсуса любая машина может в любое время сделать валидный блок, добавить его в цепь и получить награду за него. Но в определенный момент времени может претендовать одновременно несколько блоков. В таком случае, существует проблема выбора блока для добавления в цепь. Proof of Work усложняет задачу производства тем, что для генерации валидного хэша, нужно выполнить определенное количество работы, а именно получить хэш, удовлетворяющий условию, связанный с количеством нулей в начале. В биткоине существует понятие «сложность вычисления», определяющий количество нулей, которое должно присутствовать в начале результирующего хэша.

В третьем разделе была взята для исследования ещё одна реализация блокчейна, где более подробно описаны компоненты, задачи и проблемы при разработке сети. Описаны существующие реализации слоя коммуникации между участниками сети. Для начала были рассмотрены протоколы транспортного уровня: TCP и UDP. Оба являются приемлемыми для использования, однако имеющие свои особенности, определяющие для каждого разработчика выбор.

После обзора протоколов, более подробно описывается обработка сообщений на уровне приложения. На самом деле, один сервер с определённой спецификацией может функционировать эффективнее при использовании альтернативных подходов при работе сервера.

Важным компонентом сети является её инициализация: как участник подключается к сети, как он синхронизируется и т.п.

Рассылка сообщений по распределённому хранилищу также описана в третьем разделе. Существует наивный подход для рассылки – это подключиться ко всем известным машинам и отправить им сообщения. Однако в условиях, когда в сети находится очень много узлов, то время на

отправку будет расходоваться неэффективно, потому что одновременно с отправкой, нужно принимать и обрабатывать большое количество входящих сообщений.

Существует протокол, который произведёт рассылку быстрее, используя ресурсы всех участников сети – протокол Gossip. Пусть будет сообщение о том, что некоторый узел в сети произвёл блок. Он распространяет «слух» об этом своим подключённым узлам. Принявшие сообщения участники распространяют данное сообщение уже своим соседям и так до тех пор, пока о нём не узнают все участники сети. Таким образом, в условиях, когда все узлы подключены к 8 соседям, то количество принявших будет возрастать (8, 64, 4096 и т.д).

Определённо рассылку сообщений нужно остановить в определенный момент, а именно, если узел получает снова это сообщение, оно не должно больше рассылаться. Это логика описывается на бизнес уровне, т.е. если, например, блок с хэшем `x` существует в локальном хранилище, значит, что сообщение о блоке уже было принято в прошлом и он не нуждается в отправке.

Помимо Proof Of Work, существуют и другие алгоритмы консенсуса. На базе одной из реализации приведен детальный алгоритм Delegated Proof Of Stake. Здесь рассказывается про то, как можно удтвердить последовательность производителей блока, их время исполнения, условие добавления блока, рассинхронизации участника.

Вместе с рассинхронизацией узлов в сети, раздел описывает алгоритм синхронизации данных и времени.

Смарт-контракты также пояснены в разделе, с точки зрения реализации. Это более сложная задача для реализации и в работе приведены задачи, которые предстоят к решению.

ЗАКЛЮЧЕНИЕ

За время реализации магистерской диссертации были изучены аспекты, связанные с разработкой решений, в основу которых взята технология блокчейн. Описаны общие особенности, а именно положительные и отрицательные моменты существования данной технологии.

Перечислены некоторые существующие решения, основанные на блокчейне: их особенности, задачи, которые они решают. В рамках диссертации были приведены такие платформы как биткоин, являющимся первым рабочим вариантом реализации для финтех отрасли. Далее идёт эфириум, который выступает для сообщества не как обычное решение, осуществляющее перевод финансовых средств, но и как полноценная платформа, пресдставленная распределённой сетью узлов, хранящий события в блоках. И последним существующим примером является IOTA, который структурно имеет радикальные отличия по сравнению с классическим пониманием блокчейна, а именно в том, что события хранятся не в цепочке, а в ациклическом графе, что даёт определённые преимущества в скорости обработки событи, но, к сожалению, не удовлетворяет требования к безопасности.

В диссертации выполнена задача по выявлению особенностей разработки блокчейн-платформы. Для объекта исследования был выбран OPEN Chain со своими идеями и особенностями работы. В рамках него был детально описан процесс работы всех компонентов блокчейн-сети, а именно:

- Сетевая инфраструктура
- Алгоритм консенсуса
- Синхронизация данных
- Синхронизация времени
- Смарт-контракты

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

Бисярин, Грядовкин, Анализ эффективности разработки программных продуктов / Георгий Бисярин, Владислав Грядовкин // Молодой ученый №8 (246) февраль – 2019

Бисярин, Грядовкин, Анализ производительности подходов обработки информации на уровне веб-сервера и базы данных / Георгий Бисярин, Владислав Грядовкин // Молодой ученый №8 (246) февраль - 2019