Курс лекций «Одноранговые сети и технология блокчейн»

# БАЗОВЫЕ ПОНЯТИЯ И КОМПОНЕНТЫ БЛОКЧЕЙН

Профессор Часовских В.П.

2020

# КРИПТОВАЛЮТА

**Криптовалюта** (Bitcoins и прочие) была разработана как средство для осуществления электронных платежей без посредничества финансовых институтов. Часто рассматривается как одна из областей применения технологии blockchain.

Для использования в рамках цифровой экономики средство платежей (**криптовалюта**) должно обладать следующими свойствами:

- доступность и цифровая форма;

- признание во всем мире и в каждой стране в качестве средства платежа;

- свобода в движении от владельца к владельцу вне зависимости от их территориальной, национальной и иной принадлежности

- стабильная ценность и покупательская способность;

- надежность и конвертируемость; - отсутствие контроля со стороны какого-либо финансового института или государства.

# КРИПТОВАЛЮТА

В рамках технологии **blockchain** криптовалюта используется не только как электронное средство платежей, но и как средство для автоматизированного осуществления вознаграждений и штрафов участников за их вклад в развитие технологии:

- за вклад в обеспечение целостности технологии;
- за вклад в обеспечение открытости технологии;
- за поддержку распределенной природы технологии;
- за вклад в развитие философии технологии.

# Криптография

**Криптография** (крипто шифрование). Область знаний, которая при информационном взаимодействии дает возможность обеспечивать конфиденциальность (защита от просмотра третьими лицами), целостность (защита от стороннего изменения информации), аутентификацию (подтверждение подлинности сторон) информации, а также гарантирующая невозможность отказа сторон информационного взаимодействия от авторства. Является крайне важной составляющей. В рамках технологии **blockchain** осуществляется с помощью криптографических **хеш-функций.**

# Трансакция

**Трансакция** (transactions). В данном случае рассматривается как действие по передаче права собственности от одного участника технологии к другому. Каждая трансакция определяется следующими идентификаторами:

- идентификатор счета, владелец которого передает право собственности;

- идентификатор счета, владелец которого получает право собственности;

- количество товара (криптовалюты), на которое передается собственность;

- время, в которое должна быть осуществлена передача права собственности;

- комиссия, взимаемая за исполнение трансакции в рамках технологии;

- подтверждение согласия (подпись) передающего право собственности на осуществление трансакции.

# Хеш-функция

**Хеш-функция** (hash function) и хеш-значение (hash value). **Хеш-функция** – это алгоритм, позволяющий представлять данные любого типа, независимо от размера в виде числа фиксированной длины (**хеш-значения**).

Криптографические хеш-функции обладают следующими свойствами :

- быстрое вычисление хеш-значения для любых типов данных;

- детерминизм – обеспечение соответствия хеш-значения исходным данным;

– псевдо случайность – непредсказуемость изменений хеш-значения при даже незначительном изменении исходных данных;

– необратимость – невозможность преобразования хеш-значения в исходные данные;

– противоречиво устойчивость – низкая вероятность подбора двух различных значений исходных данных, для которых вычисляемое хеш-значение окажется одинаковым.

# Хеш-функция

Принимая во внимание перечисленные свойства, можно говорить о высокой надежности использования **хеш-функций** при идентификации исходных данных.

Поэтому **хеш-значения** активно используются в рамках технологии **blockchain** для идентификации данных, в частности для подтверждения согласия на осуществление **трансакции**.

# Структуры данных

**Структуры данных** (data structures). В общем виде структура данных представляет собой набор переменных, объединенных определенным образом. Также структура данных может быть определена как способ организации данных без учета их конкретного информационного содер- жания. В рамках технологии **blockchain** структура данных определяется как данные, структурированные в элементы, называемые блоками (**blocks**), связанные друг с другом по принципу цепочки (**chain**); из этого определения и происходит термин **blockchain**.

# Структуры данных

**Структуры данн**ых тесно связаны с алгоритмами, при помощи которых эти данные будут обрабатываться.

Под **алгоритмом** в технологии **blockchain** понимается последовательность операций, при помощи которых информационное содержание множества структур данных в распределенных пиринговых системах согласуется между собой подобно системе голосования.

# Целостность системы

**Целостность системы** (system integrity). Включает следующие составляющие:

- целостность данных (data integrity);

– обеспечение полноты, корректности и непротиворечивости создаваемых, корректируемых и хранимых в системе данных;

- целостность поведения системы (behavioral integrity) – гарантирование отсутствия логических ошибок при работе системы, полного соответствия поведения системы запланированным сценариям ее развития и использования;

- безопасность (security) – доступ к данным системы только для зарегистрированных пользователей, защита от несанкционированного использования данных системы.

# Распределенные системы

**Распределенные системы** (distributed systems), включая программные средства распределенных вычислений. В отличие от централизованной системы, в которой все данные хранятся на сервере, с которым связан каждый из пользователей системы, распределенные системы подразумевают порционное (распределенное) хранение данных на персональных компьютерах пользователей, связанных между собой и поэтому являющихся частью единой системы. Программные средства распределенных вычислений любой желающий может установить на свой персональный компьютер, тем самым вовлекая часть ресурсов своего компьютера в работу по проведению вычислений.

# Распределенные системы

В сравнении с централизованными распределенные системы обладают следующими отличительными чертами:

- Повышение вычислительной мощности.

- Снижение денежных затрат на эксплуатацию, однако увеличение расхода вычислительных мощностей и затрачиваемых усилий с целью координации системы в целом и для обеспечения коммуникаций внутри системы.

- Высокая надежность системы в сравнении с централизованными системами, но при этом повышенная сложность программного обеспечения, координирующего работу системы.

# Распределенные системы

- Способность развиваться естественным способом (путем включения новых пользователей в систему) и тем самым – почти бесплатно увеличивать вычислительную мощность системы, но при этом полная зависимость от работы сети и повышенные требования к безопасности в системе (чем проще осуществляется доступ к сети, тем выше требования к безопасности).

# Распределенные соглашения

**Распределенные соглашения** (distributed consensus) – «соглашения» между персональными компьютерами в рамках чистых распределенных P2P систем о том, какой вариант истории трансакций считать верным (истиным), а какой – ошибочным (ложным). Основное предназначение распределенных соглашений – предотвращение так называемой «двойной траты» криптовалюты, т.е. осуществления трансакции по передаче собственности на сумму криптовалюты, которой нет на счете отправителя трансакции или собственность на которую уже была передана.

# Распределенные соглашения

Осуществление выбора между истинным и ложным риантами истории трансакций осуществляется на основе подсчета агрегированной суммы вычислительных усилий, потраченных на создание истории трансакций. И основными критериями для оценки вычислительных усилий на создание истории трансакций являются:

- «Критерий длиннейшей цепочки», т.е. цепочка blockchain, состоящая из наибольшего количества блоков, соответствует большей агрегированной сумме вычислительных усилий по ее созданию, чем по созданию более коротких цепочек.

# Распределенные соглашения

- «Критерий длиннейшей цепочки», т.е. цепочка blockchain, состоящая из наибольшего количества блоков, соответствует большей агрегированной сумме вычислительных усилий по ее созданию, чем по созданию более коротких цепочек.

- «Критерий тяжелейшей цепочки». Агрегированный уровень сложности цепочки часто называется весом цепочки, отсюда и название «тяжелой цепочки». Цепочка blockchain, для которой агрегированный уровень сложности по добавлению блоков к цепочке является наибольшим, соответствует наибольшей агрегированной сумме вычислительных усилий по ее созданию, чем по созданию цепочек с меньшим агрегированным уровнем сложности.

# Распределенные соглашения

- Соответствие по одному из этих критериев в отдельности не является достаточным условием для решения об истинности рассматриваемой цепочки, поскольку уровень сложности при создании каждого блока различается, т.е. «длиннейшая цепоч- ка» не всегда требует наибольшей агрегированной суммы вычислительных усилий на ее создание. Аналогично, «тяжелейшая цепочка» (с наибольшим агрегированным уровнем сложности) не всегда является самой длинной. Однако соответствие цепочки blockchain обоим критериям в совокупности однозначно соответствует наибольшей агрегированной сумме вычислительных усилий и является достаточным условием для решения об истинности рассматриваемой цепочки.

# Пиринговые систем

**Пиринговые системы** (peer-to-peer systems, P2P). Частный случай распределенных систем. Это распределенные системы, состоящие из узлов (персональных компьютеров), которые предоставляют доступ других узлов системы к своим вычислительным ресурсам. P2P системы позволяют узлам системы взаимодействовать напрямую, без участия посредников. Также может рассматриваться как вид социальных коммуникаций, создаваемых на основе технологии web 2.0.

# Пиринговые систем

При функционировании системы P2P используют такие ресурсы персональных компьютеров, как:

- вычислительные мощности;
- память жесткого диска для хранения информации;
- пропускная способность данных;
- пропускная способность сети.

За счет использования перечисленных видов ресурсов системы P2P обеспечивают пользователей системы таким функциона лом, как:

- доступ к файлам;
- распределение контента (порционное хранение данных системы);
- защита данных.

# Пиринговые систем

Также существует отдельный подвид P2P систем – «централизованные пиринговые системы», имеющие центральный узел, который способствует взаимодействию между участниками системы (рядовых узлов – пиров), поддерживает директории с описанием сервисов, предоставляемых узлами системы, или выполняет поиск и идентификацию узлов системы.

Данный вид P2P систем позволяет комбинировать преимущества распределенной и цен- трализованной системы.

# Пиринговые систем

Таким образом, опираясь на вышеизложенные понятия, можно рассматривать технологию Blockchain как средство обеспечения целостности в распределенных системах. В частности, чистые распределенные P2P системы используют технологию Blockchain с целью достижения и обеспечения целостности. Как правило, основными угрозами целостности P2P систем являются недобросовестные узлы (пиры) и технические сбои, в то время как для обеспечения целостности P2P системы в качестве основных факторов используются сведения о количестве узлов в системе и сведения о надежности каждого из узлов системы.

# Пиринговые систем

Если мы знаем количество и уровень надежности всех узлов в системе, мы достаточно легко способны обеспечить ее целостность. Однако, если эти факторы не определены, во много раз возрастает сложность задачи обеспечения целостности.

В рамках цифровой экономики могут существовать, функционировать и взаимодействовать и централизованные, и распределенные системы.

# Пиринговые систем

Рассмотрим функционирование цифровой экономики на примере одного из ее процессов, а именно платежную систему, или «интернет-банкинг». Такая система должна обеспечивать конечного пользователя возможностями проверки баланса счета, перевода денег, оплаты услуг, размещения и снятия денежных средств со счета и т.д. Эти возможности могут обеспечиваться средствами как централизованных систем, так и распределенных систем.

# Пиринговые систем

Функционирование централизованной системы в данном случае предполагает создание на сервере баз данных, хранящих данные о пользователях, счетах и произведенных операциях. Любая операция, производимая пользователем со своим счетом, отражается в этих базах данных. Для взаимодействия с базами данных пользователи устанавливают на ПК специализированное программное обеспечение либо использует web-сервис, являющийся частью платежной системы, с помощью которого осуществляет ввод и первичную проверку данных о желаемой платежной операции.

# Пиринговые систем

Следующим этапом является верификация отправляемых пользователем данных и обмен данными с БД с помощью программ и алгоритмов взаимодействия с БД , установленных на том же сервере, что и СУБД. Любое взаимодействие между пользователями такой системы осуществляется через сервер-посредник.

В случае использования распределенной системы отсутствует сервер с централизованной БД и программами взаимодействия с ней. При этом ввод и первичная проверка данных о платежных операциях по-прежнему осуществляется посредством приложений, устанавливаемых на ПК пользователей системы.

# Пиринговые систем

Функции же верификации и хранения данных в данном случае возлагаются на программное обеспечение распределенных вычислений, которые осуществляют взаимодействие между пользователями системы (без сервера- посредника) и обеспечивают целостность и хранение данных в системе реестров, хранящихся на ПК тех же самых пользователей системы. То есть совокупность пользовательских приложений и программного обеспечения, осуществляющего хранение данных и взаимодействие участников системы, и получила название технологии blockchain.

# ЗАКЛЮЧЕНИЕ

Получено наиболее полное определение blockchain.

**Blockchain** – это чистая распределенная пиринговая система реестров, использующих программное обеспечение, которое состоит из алгоритмов, согласующих и объединяющих информационное содержание упорядоченных и связанных блоков данных в единое целое, на основе технологий криптографии и безопасности, с целью обеспечения целостности системы.

# ЗАКЛЮЧЕНИЕ

Приведено описание и схема функционирования технологии **blockchain**.

**Определена роль blockchain в цифровой экономике**. Она сводится к выполнению всех функций, связанных с хранением, изменением и доступом данных (т.е. функций, традиционно выполнявшихся сервером посредником в централизованных системах), а также функции взаимодействия между пользователями.

# ЗАКЛЮЧЕНИЕ

Определены отличия функционирования цифровой экономики на основе централизованных систем и распределенных систем. Использование технологии blockchain позволит сокращать затраты на использование (за счет отказа от использования серверов-посредников) и одновременно повышать платежных и иных систем (за счет выше описанных преимуществ технологии blockchain).

Применение технологии blockchain возможно в разных сферах и секторах экономики, и, с моей точки зрения, она весьма эффективна в вузовском образовании.

# ЗАКЛЮЧЕНИЕ

Подобная технология наилучшим образом подходит для организации синхронного и асинхронного взаимодействия преподавателя и студента университета в рамках электронно - образовательной среды вуза.