Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Селезнев М.Н., Воробьев Д.С. Применение технологии блокчейн как инструмента для открытого хранения информации о достижениях одаренных детей // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2018. – №5 (май). – АРТ 230-эл. – 0,3 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004

Селезнев Михаил Николаевич,
студент 2 курса магистратуры,
Национальный Исследовательский Ядерный Университет «МИФИ»
Воробьев Дмитрий Сергеевич,
студент 2 курса магистратуры,
Национальный Исследовательский Ядерный Университет «МИФИ»
*Научный руководитель***: Гусева Анна Ивановна,**
Профессор, зав. кафедрой экономики и менеджмента в промышленности.
Национальный Исследовательский Ядерный Университет «МИФИ»
г. Москва, Российская Федерация.
E-mail: seleminx@gmail.com

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН КАК ИНСТРУМЕНТА ДЛЯ ОТКРЫТОГО ХРАНЕНИЯ ИНФОРМАЦИИ О ДОСТИЖЕНИЯХ ОДАРЕННЫХ ДЕТЕЙ

Аннотация: В данной статье рассматривается подход к хранению информации с помощью технологии блокчейн, возможность его применения для хранения информации о достижениях одаренных детей. Приводится анализ возможных недостатков технологии.

Ключевые слова: технология блокчейн, алгоритмы консенсуса, структура блока, недостатки технологии блокчейн.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Seleznev Mikhail Nikolaevich,
Second-year master's student,
National Research Nuclear University MEPhI
Vorobiev Dmitry Sergeevich,
Second-year master's student,
National Research Nuclear University MEPhI
Supervisor: Guseva Anna Ivanovna**,**
professor, department chair of economics and management of industry.
National Research Nuclear University MEPhI
Moscow, Russian Federation.

APPLICATION OF BLOCKCHAIN TECHNOLOGY AS A TOOL FOR OPEN STORAGE OF INFORMATION ABOUT ACHIEVEMENTS OF GIFTED CHILDREN

Abstract: This article discusses the approach to the storage of information using blockchain technology, the possibility of its use to store information about the achievements of gifted children. The article provides the analysis of possible defects of the technology.

Keywords: technology of the blockchain, algorithms, consensus, structure of block, the disadvantages of blockchain technology.

Блокчейн является достаточно надежным методом хранения любой информации, которую необходимо записать и проверить. Начав завоевывать внимание разработчиков в 2008 году и став предметом научного интереса в 2017, когда был открыт первый институт исследований блокчейна в Торонто, сейчас технология проникает на новые рынки. Использующие ее проекты стремительно развиваются, специалисты все чаще рассматривают децентрализацию в качестве возможных решений.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

За прошедшие несколько лет было проведено множество исследований на тему того, в каких сферах данная технология может быть применима, и многочисленные тесты показали варианты ее применения в различных условиях. Потому, несмотря на новизну подхода, частные криптографические ключи и блокчейн – не всегда самый простой и правильный путь решения задачи. Многие указывают на перечень недостатков, часть из которых будет рассмотрена далее.

Суть технологии

Блокчейн – технологию подтверждения неких связанных действий, позволяющую при получении базы этих связанных действий от источника произвести проверку, действительно ли учащийся является единственным лауреатом всех приписываемых себе премий и наград. К каждому «новому кусочку» информации при этом приписывается хэш предыдущей транзакции какого-либо участника. Таким образом добавление новой информации будет зависеть не только от текущего шага, но и от всех предыдущих шагов.

Помимо этого, в базе также можно проверить не нарушает ли вся цепочка некоего правила – например, нет ли двух победителей одной олимпиады (в этом случае потребуются дополнительные проверки). С использованием алгоритмов консенсуса, позволяющих сети принять решение относительно того, какой из последующих блоков принять как следующий задача станет заметно упрощена. Необходимо будет лишь подобрать такой шаг, в результате которого хэш блока не перестанет удовлетворять определенному условию, однозначно вытекающему из состояния цепочки на момент принятия последнего блока. Если два узла одновременно выдают одинаковый подходящий блок, то цепочка этих самых блоков распараллеливается, один из них пропадет и узлы, которые

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

приняли блоки из удаленной ветви будут откинуты к моменту последнего нормального блока и автоматически получат самую длинную версию цепи.

При этом для участников будет достаточной проверка лишь последних транзакций (например, сразу по завершении конкурса или олимпиады), а вот если потенциальный работодатель изъявит желание проверить полную историю записей по конкретному человеку, потребуются большие вычислительные мощности, если база будет достаточно объемна.

По сути блокчейн позволит создать единый реестр достижений каждого человека и даст возможность любому желающему ознакомиться с этим реестром. Более того, потенциальным работодателям было бы удобно получать доступ ко всем участникам конкретных программ и конкурсов и быть уверенными в корректности полученной информации, ведь будет невозможным утверждение следующего блока транзакций в цепи без согласования каждого элемента со всеми ее участниками или внесение каких-либо изменений в уже утвержденный участок цепи.

Структура блоков

Структуры блока могут быть совершенно разными, однако есть перечень элементов, которые можно назвать обязательными [1]:

- Версия блока – по этому элементу возможно будет обратиться к конкретному кусочку всей цепи, не обновляя ее целиком;
- Хэш предыдущего блока – помогает произвести идентификацию родительского блока;
- Хэш всех транзакций в блоке – структура данных в виде бинарного дерева хэшей (Дерево Меркла);
- Временная метка создания блока;
- Список всех транзакций в блоке – позволяет определить состав блока;

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Этот список параметров образуют заголовок блока. По большому счету именно хэш заголовка и будет являться хэшем целого блока, а сами транзакции не принимают непосредственного участия в хэшировании.

Стоит упомянуть, что дерево Меркла используется для того, чтобы была возможность создания нод STV, синхронизирующих исключительно заголовки блоков, что позволяет всей цепи занимать куда меньшие объемы информации.[5]

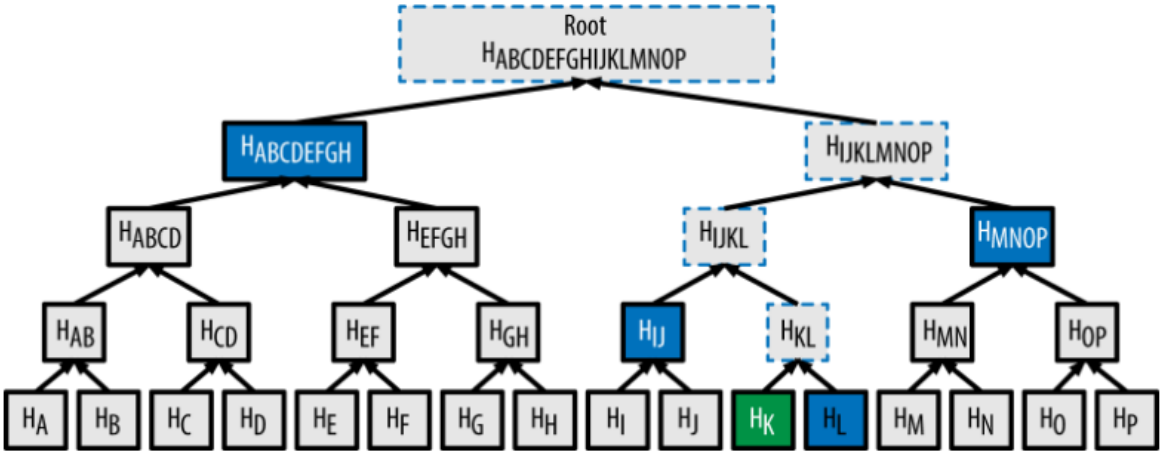

Рис. 1. Упрощенная верификация транзакций

Упрощенную верификацию транзакций можно описать следующим образом: например, у одного участника есть STV нода, а у второго вся цепочка блоков целиком. И для того, чтобы убедиться в существовании транзакции К ноде необходимо лишь предоставить хэши, отмеченные синим маркером на рис.7. Если после расчета хэша от суммы хэшей всех транзакций на каждом из шагов нода находит в своей цепи необходимый блок с таким же хэшем, то факт транзакции считается неоспоримым.

Касаемо временной метки создания блока можно отметить то, что обычно для проверки ее валидности создают два критерия:

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

1. Время сравнивается со средним арифметическим временем нескольких предыдущих блоков, при этом допустимой является небольшая погрешность в большую или меньшую сторону от времени последнего блока.

2. Значение временной метки должно быть меньше среднего времени по сети – проверка производится при получении нового блока путем сравнения среднего арифметического времени соседей по сети. При этом погрешность также допустима.

Структура транзакций

Опустившись на уровень транзакций, нельзя не упомянуть о том, что главными ее составляющими являются входы – транзакции, на которые ссылается текущая и выходы – их может быть несколько, однако для хранения информации о достижениях одаренных детей достаточно будет лишь одного. По большому счету транзакции ссылаются не друг на друга, а на конкретные выходы каждой из них и для этого внедряются параметры, хранящие в себе индекс и хэш выхода предыдущей транзакции [2].

Немаловажную роль в структуре транзакций играют и параметры, задающие условия, при котором выход в транзакции может быть использован либо возможности подтверждения того, что данное условие было выполнено. Например, для проверки закончил ли конкретный участник курсы, размещенные на портале, чтобы отправить ему соответствующий сертификат, создаются открывающий и закрывающий транзакцию скрипты. Когда учащийся успешно завершил курс, проверяется соединение обоих скриптов и если их исполнение валидно, то транзакция считается завершенной.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Недостатки технологии

Дополнительно стоит осветить несколько пунктов, которые многими рассматриваются в качестве отрицательных сторон технологии:

- Малая эффективность и медлительность, т.е. небольшое количество проведения транзакций при больших затратах мощностей и электричества, что является правдой лишь отчасти. Во-первых, не всем проектам, полностью работающем на блокчейне, либо реализующим отдельный бизнес-процесс с использованием технологии, необходима большая пропускная способность в единицу времени.[3]

Во-вторых, в зависимости от проекта и методики реализации, существует возможность настройки «собственного» канала между двумя или несколькими участниками основной сети, тем самым обмениваясь транзакциями изолированно от общей сети. После выполнения всех взаимодействий в рамках канала, он закрывается и в общую сеть пишется лишь результат данного взаимодействия. Скорость в данном случае ограничивается лишь ресурсами каждого из участников локального куска сети.

- Громоздкость, т.е. стремительно растущий объем цепи.

В основе своей, всем участникам не обязательно проверять всю цепь с самого начала, эта задача может решаться специализированными дата-центрами. Также проверить правильность цепи можно, используя тонкий клиент, смотрящий лишь на заголовки блоков. Даже в блокчейне больших объемов, заголовки занимают крайне малое количество памяти, исчисляющееся всего лишь несколькими десятками Мб.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

- Для цепочек блоков любой направленности необходимо, чтобы каждый из участников был заинтересован в записи блоков.

В действительности, с использованием метода Proof-of-Authority, можно предоставить возможность создания блоков только доверенным участникам с использованием собственного ключа для подписи. Открытость, являющаяся важнейшим свойством блокчейна, при этом будет сохранена.

- Блокчейн навсегда сохраняет все записи.

На самом деле, при росте цепочки блоков до гигантских масштабов, новые пользователи сети все реже будут испытывать желание качать полный клиент и проверять все блоки с самого начала, все чаще обращаясь к услугам сторонних сервисов или взращивая в себе желание хранить необходимую информацию на локальном узле. Но в данном случае каждому такому клиенту необходимо будет всецело доверять серверу, на котором записывается информация, не проверяя ее самостоятельно и по своей структуре такая архитектура будет представлять собой уже традиционную «клиент-сервер», а не одноранговый блокчейн.[4]

- Открытость информации самой по себе. В случае с финансовыми операциями это может быть как плюсом – потенциальный участник сделки видит, что у его контрагента достаточно средств на счету и его прошлые операции произведены корректно, так и минусом – для большинства компаний раскрытие информации обо всех закупщиках и клиентах, объемах продаж и счетов может стать большой проблемой.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

В зависимости от прикладной задачи, данная технология может быть оправданной или совсем неконкурентоспособной. Однако, в процессе развития как производительности оборудования, так и алгоритмов самой технологии, широта ее применения может стать неограниченной.

Так, в результате обзора технологии блокчейн, можно сделать вывод, что данный подход может быть использован не только в сфере банковских и вообще любых финансовых операций, на которые она опиралась при создании, но и, например, в сфере учета достижений одаренных детей.

Список использованной литературы:

1. David De Rossa “The Bitcoin Script language”, 2015
2. Jacob William Blockchain: The Simple Guide To Everything You Need To Know, 2016
3. Jeremy Clark Bitcoin, blockchain, cryptocurrency, cryptology» (A detailed and technical study of Bitcoin, blockchain, cryptocurrency, and cryptology), 2016
4. John W. Ratcliff “Documentation of the physical bitcoin blockchain”, 2014
5. William Mougayar «The Business Blockchain: a Primer on the Promise, Practice and Application of the Next Internet Technology», 2016

Дата поступления в редакцию: 18.05.2018 г.
Опубликовано: 18.05.2018 г.