УДК 004.7

ВОЗМОЖНОСТИ ТЕХНОЛОГИИ BLOCKCHAIN В ПРИМЕНЕНИИ ДЛЯ СОЗДАНИЯ РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ ДАННЫХ

А.И. Мартышкин
кандидат технических наук, доцент, доцент кафедры вычислительных машин и систем, ФГБОУ ВО «Пензенский государственный технологический университет», г. Пенза, Россия, e-mail: Alexey314@yandex.ru

Аннотация. В статье описывается возможность применения технологии Блокчейн (blockchain) для реализации распределенных реестров данных. приводится классификация распределенных реестров. Рассматриваются вопросы, касаемые устойчивости технологии блокчейн к попыткам подделки данных.

Ключевые слова: распределенные системы, блокчейн, криптовалюта, информационные технологии, реестр, токен, хэш-идентификатор.

OPPORTUNITIES BLOCKCHAIN TECHNOLOGY IN THE APPLICATION FOR CREATING DISTRIBUTED DATA REGISTRIES

A.I. Martyshkin
Ph.D. Associate Professor, Associate Professor of the Department of Computers and Systems, FGBOU VO 'Penza State Technological University', Penza, Russia, e-mail: Alexey314@yandex.ru

Abstract. The article presents the result of a study of the applicability of the Blockchain technology for the implementation of distributed registries of personal data, based on the example of the university student achievement register. The organization of interaction in the system is considered. An expression is provided to calculate the transaction hash.

Keywords: distributed systems, blockchain, cryptocurrency, information technology, registry, token, hash identifier.

Введение. Внимание к технологии Блокчейн привлекла возросшая популярность основанных на ней криптовалют. В 2009 году Сатоси Накамото опубликовал исходный код биткоина. На тот моментстоимостьэтой криптовалюты составляла 0,003 доллара за 1000 единиц. Спустя 9 лет она выросла в несколько сотен тысяч раз, пробив отметку в 20000 долларов за 1 единицу. Однако понятие и сферы применения блокчейна гораздо шире криптовалют. Особенности технологии распределенного реестра позволяют использовать его в большом числе отраслей.

Цель работы заключается в исследовании возможности технологии blockchain применененительно к созданию распределенных реестров данных.

Материал и результаты исследований. Новинки в сфере информационных технологий уже давно активно внедряются в различные сферы деятельности человека. Использование локальных и глобальных сетей продемонстрировало людям новые способы обмена информацией. Изначально такие сети проектировались для использования в специализированных целях (государственные, военные каналы и т.д.), но дальнейшее развитие сетей предоставило возможность использования Интернета как канала для хранения и передачи данных почти для каждого человека. Для записей данных таких как активы, деньги, имущество или любых других уже давно используются реестры. Однако сейчас технологии позволяют создавать цифровые распределенные реестры, которые обладают качествами, превосходящими традиционные бумажные реестры. Далее будут рассмотрены виды реестров.

Распределенный реестр. В базовом представлении являет собой БД, которая хранится, редактируется и обновляется независимо каждым участником (или узлом) в большой сети. Распределение уникально: записи не обмениваются через различные узлы центрального органа, а строятся и удерживаются каждым узлом независимо друг от друга. Это значит, что каждый узел в сети обрабатывает каждую транзакцию, делая свои выводы. По этим данным далее проводится голосование, с целью убедиться, что большинство участников сети подтверждают выводы. Все участники сети имеют полную, идентичную для всех, копию всех записей. Изменения в реестре повлекут изменения копий для всех участников сети в течение нескольких минут. Проверка достоверности записей в реестре происходит с использованием криптографических "ключей" и подписей, позволяющие управлять доступом к реестру. Права на изменения записей в реестре могут быть либо у всех участников, либо у нескольких выбранных, в зависимости от правил, принятых в сети [1].

Распределённый реестр может использоваться для выдачи паспортов гражданам и обеспечивать открытость, точность записей о государственной деятельности. Способы управления информацией, применяемые в наше время, предполагают её использование в каком-то отдельном учреждении. В связи с этим необходимо создание систем управления сетью, передачи сообщений и организации связи со внешними системами, которые увеличивают стоимость реализации и обслуживания всей системы в целом.

Системы, где используется централизованная модель обработки данных, при любом сбое потребует больших затрат для восстановления работоспособности системы. Они могут быть уязвимы для кибератак, а данные часто не синхронизированы, неактуальны или попросту некорректны. В распределённых реестрах вместо единой базы данных существует множество

копий реестра, а это значит, чтобы провести успешную атаку на распределённый реестр, нужно провести атаку на все копии, что крайне затруднительно. Технология распределенного реестра также устойчива от внесения подложных данных, так как участники сети в тот же момент обнаружат изменения в части реестра (рисунок 1). Кроме того, методы, используемые для защиты и редактирования информации, подразумевают, что участники сети делятся данными и могут быть уверенными, что все копии реестра совпадают друг с другом независимо от времени [1].

Но нельзя сказать, что распределённые реестры являются 100% защитой от кибератак. В случае, если злоумышленник найдёт способ “легально” внести изменения в реестр, то все копии реестра примут эти изменения.

Технология распределенного реестра предоставляет платформу для снижения объемов мошенничества, ошибок и стоимости процессов, интенсивно работающих с бумажными документами. Она обладает потенциалом на изменение взаимоотношений между государством и гражданином по вопросам совместного использования данных, точности и прозрачности. Также она применима и для частного сектора.

Неконтролируемые реестры, такие как Bitcoin, не имеют единственного владельца. В нем отсутствует возможность владения реестром. Для такого реестра характерна возможность любому лицу вносить в него данные и предоставлять возможность для тех, в чьем распоряжении находится реестр, получать его полные копии. Это предотвращает возможные попытки контроля данных. Никакой участник не может помешать добавлению транзакции в реестр. Игроки подтверждают точность информации в реестре с помощью достижения консенсуса в отношении его состояния. Неконтролируемые реестры могут используют для создания записей без возможности изменения данных. К примеру, для составления завещания или внесения других важных документов [1].

Контролируемые реестры имеют владельца. Их может быть один или несколько. При добавлении записи в транзакцию целостность реестра проверяется методом ограниченного процесса достижения консенсуса. Процесс осуществляют доверенные участники – к таким относятся государственные органы или банки. Это значительно упрощает поддержку совместной записи в отличии от процесса получения консенсуса, который используется для неконтролируемых реестров.

Контролируемые блокчейны предоставляют такие данные, которые легко верифицировать, поскольку процесс получения консенсуса позволяет создавать цифровую подпись, которую может быть проверена любой стороной. Необходимость валидации записей несколькими госорганами

предоставляет большую уверенность в ее безопасности. В отличие от текущих решений, когда организации зачастую обмениваются данными на бумажных носителях. Операции с применением контролируемого реестра часто исполняются быстрее, чем с применением неконтролируемого [1].

Теперь стоит рассмотреть вопрос, касаемый системы доверия в Интернете, где доверие базируется на двух требованиях: докажи мне, что ты тот, кем ты являешься (аутентификация); и подтверди, что у тебя есть необходимые права, для выполнения того, что тебе требуется (авторизация). В ответ я дам подтверждение, что мне можно доверять, и я могу предоставлять тебе услуги или продукты безопасно, эффективно и надежно. Аутентификация и идентификация связаны между собой, но есть различия. Первое не требует четко знать твою личность, но для нее необходимо, предоставление опознавательного ключа (токен), который точно связан с личностью. Это может быть PIN-код от банковской карты, отпечаток пальца и другие данные, связанные с личностью.

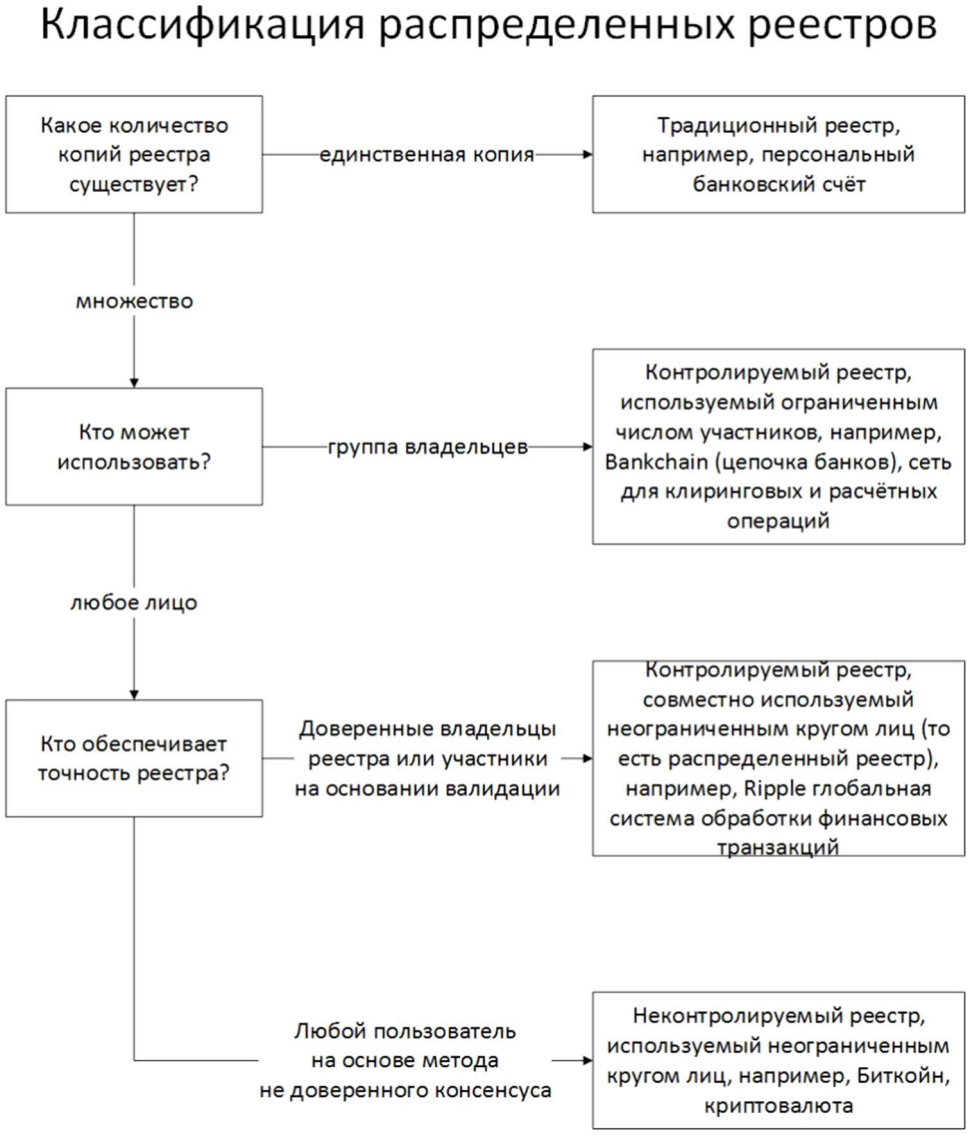

Рисунок 1 – Классификация распределенных реестров

А для предоставления опознавательного ключа нужны гарантии, что я предоставляю его нужному человеку или организации, то есть гарантии, что предоставляю тому, за кого себя выдают. Таким образом так же важно, чтобы организации предоставляли своим пользователям аутентификацию, как для физлиц, так и для юрлиц.

Блокчейн как технология передачи информации и совершения финансовых транзакций. Блокчейн – такой тип БД, где записи группируются в блоки. Блоки связаны друг с другом с использованием хэша. Таким образом Блокчейн можно использовать как распределённый реестр, доступ к которому устанавливается с учетом прав на запись или обновление. Есть немало способов достижения консенсуса. К примеру, для подтверждения записи в Bitcoin используется «майнинг». Реальная новинка Блокчейн в возможности устанавливать бизнес-логику непосредственно в самой транзакции. В этом её отличие от традиционных БД, в которых бизнес-логика задается в самой базе данных или в ПО.

Блок содержит в себе набор данных (рисунок 2). А новые блоки всегда включаются в конец цепочки [2].

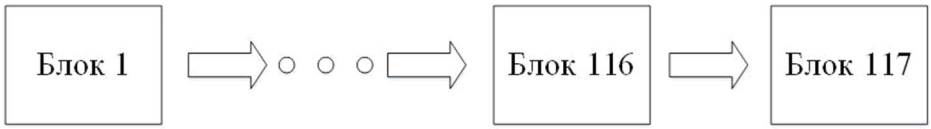

Рисунок 2 – Цепочка блоков

В Блокчейн используются 4 основных принципа.

Сверка данных с применением криптографии.

Различные учреждения обмениваются между собой сообщениями для передачи подробных сведений о транзакциях. После получения каждого такого сообщения организация обновляет свой реестр. К сожалению, пока нет быстрого и эффективного способа для обеспечения соответствия копий сообщений. Технология Блокчейн может решать эту задачу. Любые участники сети между собой приходят к достижению консенсуса в отношении записей в блоке с использованием различных алгоритмов достижения консенсуса (например, Proof-of-Work, Proof-of-Stake) [1, 3, 4, 5].

Распространение копий между различных участников.

Копия всех или определенной части записей передается всем участникам, что уменьшает возможность появления критической ошибки на одном из узлов. Одно из преимуществ применения Блокчейн заключается в том, что в случае повреждения в одной из копий, остальные копии не пострадают. Участники сети могут подтверждать возможные внесения определенных данных в ходе собственной проверки [1].

Децентрализованный контроль доступа.

В распределенных реестрах требуются "ключи" и подписи для предоставления определенным пользователям прав на создание, изменение, обновление или других действий в общем реестре. Возможно, регулятор будет иметь специальный "ключ для просмотра", который позволит ему видеть все транзакции своего учреждения, однако только в случае, когда этот ключ, который находится у законного владельца, дает регулятору разрешение (контроль) для выполнения таких действий.

Децентрализованная прозрачность и конфиденциальность.

Так как все стороны получают в свои базы копию реестра и выполняют верификацию каждой отдельной записи, общий реестр гарантирует повышенный уровень прозрачности. Это позволяет регулятору быть уверенным, что содержимое БД не было отредактировано или изменено мошенническим способом. Добавление записей происходит с применением уникальной криптографической подписи, которая подтверждает факт того, что данный участник внес запись согласно с применяемым правилам.

Блок в системе Блокчейн включает заголовок и тело блока (рисунок 3) [2].

Рисунок 3 – Структура блока

Тело блока содержит список транзакций. А заголовок блока формируется следующим образом. Блоки в системе Блокчейн связываются между собой при помощи хэша идентификатора блока. В каждом заголовке блока содержится хэш ID предыдущего блока. Это относительно несложное технологическое решение и создает защищенность и надёжность технологии Блокчейн (рисунок 4).

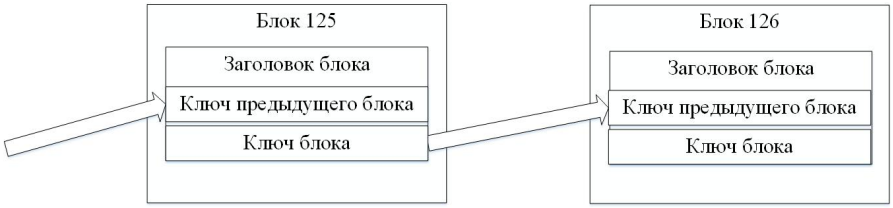

Рисунок 4 – Связь блоков

Хэш ID каждого блока цепочки вычисляется из кумулятивного хэша информации из всего блока и хэша ID предыдущего блокацепочки. Соответственно, в ID каждого блока кодируется информация о всех предыдущих блоках и данных (рисунок 5). Из этого следует, что нетрудно отследить хоть какое-либо изменение данных в любом блоке. При внесении изменений в данные в одном блоке пришлось бы пересчитать ID всех последующих, а это сделать довольно сложно [2].

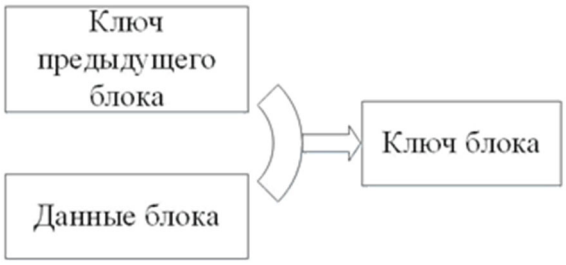

Рисунок 5 – Образование ключей

Соответственно, имея цепочку транзакций и ключ одного из блоков можно проверить: корректность информации в блоке, настоящая ли это цепочка, есть или нет пропущенные блоки, возможное наличие «левых» блоков в цепочке.

Достижение консенсуса относительно добавления изменений в цепочку транзакций происходит с использованием методов Prow-of-Work (PoW) или Proof-of-Stake (PoS).

Prow-of-Work – способ защиты распределенных систем отDDoS или иныхвозможных атак. Он основывается на выполнение одной стороной трудоемкой задачи, долгой по времени, а результат выполнения может быть оперативно проверен другой стороной. Расхождение затрат по времени даёт хорошую защиту. Хэш id блока должен соответствовать определенному условию, которое и задаёт сложность задачи. К примеру, в биткоине хэш id блока должен иметь в начале 10 нулей [3].

Proof-of-stake —Доказательство доли владения – способ защиты в криптовалютах. Основан на том, что вероятность создания участником очередного блока в блокчейне соответствует доле, которую составляют количество владеемой им криптовалюты от всего её объема. Такой способ защиты является альтернативой Prow-of-Work - подтверждения выполнения работы, у которого у обладателя более мощного оборудования более высокая вероятность создания очередного блока. В методе Proof-of-stake алгоритм формирования блока не зависит от мощности оборудования. Однако более вероятно, что блок сформирует тот участник, у которого баланс больше. Так участник, имеющий 1 % валюты от общего объема, в среднем сможет формировать 1 % новых блоков

Майнер – участник блокчейн-сети. Он выполняет создание и добавление новых блоков. Когда он получает записи от других участников сети, он составляет их вместе и пытается сформировать заголовок следующего блока. В этот момент он просчитывает хэш id блока. Допустим, по итогам первого просчёта был получен результат “57487654531244123274 9237564923”, но этот результат не соответствует условиям безопасности [2, 3]. Для возможности изменения результата вычисления, в блоке есть специальное поле nonce, по умолчанию оно равно нулю. Для получения такого результата, который соответствовал бы условиям безопасности, майнер производит перерасчет хэша, изменяя полеnonce, до тех пор, пока он не удовлетворит заданным условиям.

Чтобы найти такой хэш, майнеру требуется выполнить очень большое число расчетов. Как только подходящий хэш вычислен, блок сохраняется и передается остальным участникам сети. В итоге данные в блоке подтверждены и защищены, а внести изменения в предыдущие блоки почти невозможно [3].

Майнинг имеет следующую особенность. Независимо от количества перерасчётов, которые были исполнены, вероятность расчета необходимого хэша примерно равна. В свою очередь, становится невозможным провести предварительный расчёт или запись результата расчётов для последующего, возможно мошеннического использования. Поэтому все майнеры равноправны между собой.

За каждый созданный блок майнер получает небольшой процент. Это такое поощрение, за выполнение ресурсоёмкой задачи. Такой метод расчета хэша id блока намного усложняет создание поддельных блоков.

Устойчивость технологии Блокчейн к попыткам подделки данных.

К примеру, у нас есть цепочка блоков (рисунок 6).

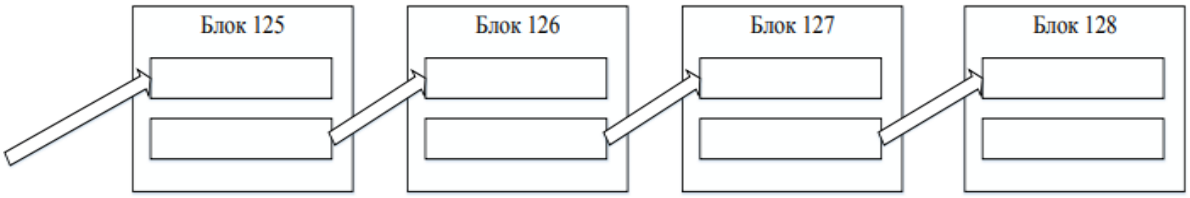

Рисунок 6 – Цепочка блоков

Мошенник пытается добавить фальшивый (поддельный) блок между двух неподдельных блоков цепочки (рисунок 7).

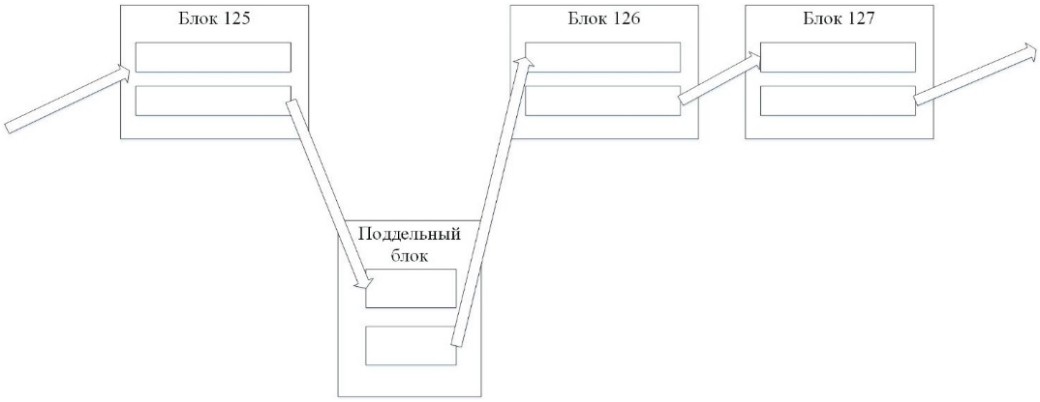

Рисунок 7 – Поддельный блок

В заголовок фальшивого блока он вписывает хэш id предыдущего блока и делает рассылку своего блока. Обман сразу же вскроется, так как в хэше блока 126 не закодирован поддельный блок.

Единственный способ провести такой вид атаки – это проделать майнинги всех блоков после поддельного, но это невозможно из-за Prow-of-Work, рассмотренного выше.

Так как поддельный блок внедрить не удалось, возможно получится подделать записи в блоке (рисунок 8).

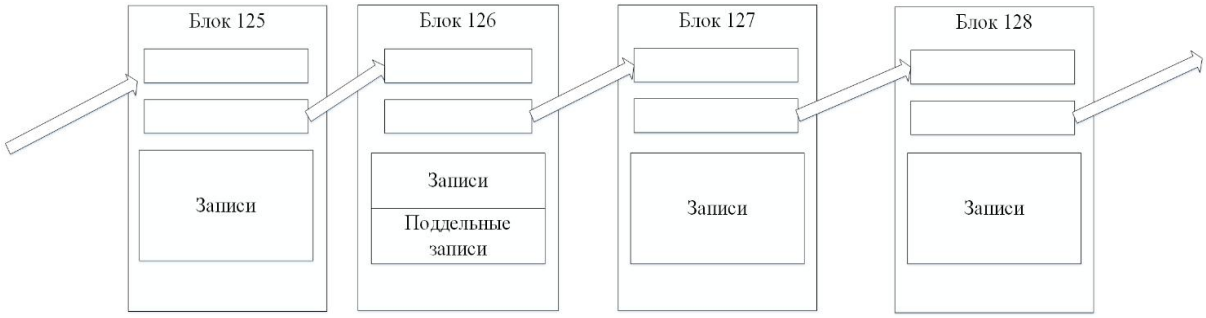

Рисунок 8 – Поддельные записи

Такой способ тоже не поможет, так как при внесении изменений в записи блока будет изменен и кумулятивный хэш. Вместе с ним меняется и хэш id блока. Только в цепочке уже зафиксирован верный ключ, а значит обнаружить поддельный блок будет легко обнаружить. Поскольку фальсифицировать данные невозможно ни добавлением блока, ни изменением данных внутри него, может есть возможность повлиять на правила? Раз пользователи равноправны, то один из них добавит запись “перевод всех средств пользователя Б на счёт пользователя А”. Блокчейн не позволит провести и такую ситуацию. Каждая запись имеет “начало” и “конец”.

Рисунок 9 – Источник и результат

“Начало” – это ссылка к предыдущей сделки. А “конец” – результат текущей сделки. Допустим, записана транзакция “перевод 50 рублей”. Результат сделки защищается уникальным ключом, известный только владельцу, которому был сделан перевод (рисунок 10). Только он в дальнейшем сможет по этому ключу создавать транзакции, ссылаясь в качестве “начала” на предыдущий перевод [6].

Рисунок 10 – Цепочка правил

В случае указания неправильного ключа, такая запись не войдет в блок и соответственно в цепочку блоков.

Вывод. В работе проведен обзор применения технологии Блокчейн для реализации распределенных реестров данных

Работа выполнена при финансовой поддержке гранта РФФИ «Конкурс на лучшие проекты фундаментальных научных исследований» (Грант № 19-07-00516 А).

ЛИТЕРАТУРА

1. «Как понять нужно ли интегрировать blockchain в ваш продукт?» URL: https://habrahabr.ru/company/web_payment_ru/blog/301972/ (дата обращения: 29.03.2019).
2. Как blockchain изменит нашу жизнь? URL: http://rb.ru/opinion/blockchain/ (дата обращения: 25.03.2019).
3. «Proof-of-Work» Proves Not to Work, Ben Laurie, Richard Clayton, 2004
4. Proof of work. URL: https://ru.wikipedia.org/wiki/ Доказательство_выполнения_работы (дата обращения: 28.03.2019).
5. Proof of Stake. URL: https://ru.wikipedia.org/wiki/Доказательство_доли_владения (дата обращения: 06.04.2019).

6. Peer-to-peer. URL: https://bitcoin.org/bitcoin.pdf (дата обращения: 08.04.2019).

УДК 519.711.3

АНАЛИЗ И МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЭФФЕКТИВНО ПРОВОДЯЩЕГО СЛОЯ В МАГНИТОСТРИКЦИОННЫХ ПРЕОБРАЗОВАТЕЛЯХ ПЕРЕМЕЩЕНИЙ

Ю.Н. Слесарев[1], А.А. Воронцов[2]

[1]доктор технических наук, профессор кафедры «Автоматизация и управление», федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный технологический университет», г. Пенза, Россия, e-mail: slesarevun@gmail.com

[2]кандидат технических наук, доцент кафедры «Вычислительные машины и системы», федеральное государственное бюджетное образовательное учреждение высшего образования «Пензенский государственный технологический университет», г. Пенза, Россия, e-mail: aleksander.vorontsov@gmail.com

Аннотация. В работе подробно рассмотрен явление, получившее название скин или поверхностный эффект, проявляющийся в протекании переменного электрического тока в поверхностном слое волновода, называемом также эффективно проводящим Zэ-слоем. Выполнен анализ основных факторов, влияющих на толщину поверхностного слоя. Проведено математическое моделирование поверхностного эффекта и оценка толщины Zэ-слоя при различных значениях частоты колебаний переменного электрического тока.

Ключевые слова: скин эффект, магнитострикционный преобразователь, эффективно проводящий слой, поверхностный эффект, моделирование скин эффекта.

THE ANALYSIS AND MATHEMATICAL MODELLING OF EFFECTIVELY CONDUCTOR LAYER IN MAGNETOSTRICTIVE CONVERTERS OF MOVEMENTS

Yuri Slesarev[1], Alexander Vorontsov[2]

[1]Dr., Ph.D., professor of Automation and Management department, federal state-funded educational institution of the higher education "Penza state technological university", Penza, Russia, e-mail: slesarevun@gmail.com

[2]Ph.D., associate professor "Computers and systems", federal state-funded educational institution of the highest education "Penza state technological university", Penza, Russia, e-mail: aleksander.vorontsov@gmail.com

Abstract. In work it is in detail considered the phenomenon which received the name the skin or a skin effect which is shown in course of alternating electric current in the wave guide surface layer called by also effectively carrying out Ze-layer. The analysis of the pacing factors influencing thickness of a surface layer is made. Mathematical modeling of a skin effect and assessment of thickness of a Ze-layer at different frequency rates of fluctuations of alternating electric current is carried out.