Инженерный вестник Дона, №3 (2019)
ivdon.ru/ru/magazine/archive/n3y2019/5801

Применение блокчейн-технологий в системах электронного документооборота: анализ и программная реализация

О.Ю. Пескова, И.Ю. Половко, А.Д. Захарченко

Южный федеральный университет, Ростов-на-Дону

Аннотация: В данной статье рассматриваются основные понятия в области технологии блокчейн, анализируются различные типы блокчейн и алгоритмы достижения консенсуса. Рассмотрены достоинства и недостатки различных технологий, определены их преимущественные области применения. Показано, как на основе проведенного анализа отобраны типы блокчейн и алгоритм достижения консенсуса, которые являются наиболее подходящими для реализации системы электронного документооборота. Представлено разработанное программное обеспечение, реализующее функции защиты документов с использованием технологии блокчейн.

Ключевые слова: блокчейн, транзакция, роли блокчейн-сети, патентное право, защищенный документооборот, классификация блокчейн, публичный блокчейн, приватный блокчейн, алгоритм консенсуса, неизменность данных

Технология блокчейн и ее применение

Блокче́йн (англ. Blockchain или block chain) — выстроенная по определённым правилам непрерывная последовательная цепочка (связный список) блоков, содержащих информацию [1]. Впервые термин появился как название полностью реплицированной распределённой базы данных, реализованной в системе Биткойн, из-за чего блокчейн часто относят к базовым технологиям криптовалют, однако система цепочек блоков может быть распространена на любые взаимосвязанные информационные блоки. и может использоваться в самых разных отраслях нашей жизни: управление поставками, логистика, защищенный документооборот [2].

Основная задача технологии блокчейн – доверительная передача собственности на цифровые активы в недоверительной сети без посредников. Ключевым понятием блокчейна является транзакция – единственный способ изменить состояние данных. Блок – это структура данных, позволяющая хранить список транзакций. Узлы блокчейн-сети создают транзакции, обмениваются ими и изменяют состояние блокчейн. Чаще всего копии цепочек блоков хранятся и обрабатываются независимо друг от друга на

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

различных компьютерах. Фактически, блокчейн представляет собой логику хранения данных, не зависящую от какого-либо центра – отдельного сервера или группы серверов.

Блокчейн отличают неизменность хранимых данных, которое достигается за счет приемов криптографии, а не за счет доверия к кому-либо. Два простейших криптографических алгоритма, используемых в блокчейне, — это хеш-функции и электронные подписи, обеспечивающие целостность транзакций и отвечающие за авторизацию.

Участники блокчейн-сети не являются равноправными: почти в любой реализации этой технологии введено следующее распределение ролей:

- валидаторы – участники, пишущие транзакции в журнал;
- аудиторы – участники, не записывающие транзакции, а только проверяющие их правильность;
- легкие клиенты – участники, не хранящие полные копии блокчейна, а взаимодействующие с сетью через другие узлы.

Глобальные вложения, связанные с блокчейн-технологиями, в 2021 году могут достичь 9,7 млрд долларов США. Размер рынка рассчитывается на основе прогнозируемых доходов от внедрения решений блокчейн, а также предоставления услуг и сервисов на его основе. При этом предполагается, что среднегодовой темп роста (CAGR) в период до 2022 года составит от 79,6% до 81,2%, однако ряд регионов будет наращивать темпы роста в области блокчейн-индустрии опережающим образом: Япония — 127,3%, Латинская Америка — 152,5% [3],

Анализ мировых трендов патентования технологий блокчейн за последние 5 лет выявил 2565 патентных документов, сгруппированных в 1804 патентных семейства. До 2013 года активность практически отсутствовала, начиная с 2014 года и далее, наблюдается увеличение количества поданных патентных документов. Согласно статистике,

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

приведённой Всемирной организацией интеллектуальной собственности WIPO, за 2014 год было сделано 84 запроса на патентирование блокчейн проектов, за 2015 год – 229 запросов, 2016 год – 455, ещё больше за 2017 – более 1500. Несмотря на непродолжительный период патентования технологий блокчейн, доля выданных патентов высока и составляет более 10%. Принимая во внимание, то, что более 75% патентных документов опубликованы после 2015 года, а также продолжительный срок экспертизы патентных заявок (около двух лет в Европейском патентном ведомстве и до нескольких лет в США), такая большая доля выданных патентов свидетельствует о зрелости и высокой значимости технологий [3].

Если теперь вернуться к областям применения блокчейн, то одной из наиболее перспективных представляется технология защищенного документооборота, который может стать намного безопаснее - в первую очередь за счёт ведения децентрализованного реестра документов, который невозможно изменить или подправить. Пользователи смогут работать с документами, имея полную уверенность в их авторстве и подлинности. Таким образом, решается множество проблем, связанных с несовершенством бюрократического аппарата, опасностью махинаций и подделки документов. На данный момент в мире уже существует множество реализаций подобной технологии, например, сервис BlockSign (США), разработанный Нью-Йоркской компанией Basno, представляющей собой общедоступный регистр, в котором хранятся, подписанные электронным способом, документы [4].

Классификация блокчейн-технологий

Наиболее полезной будем считать классификацию, данную создателем критповалюты Эфириум В.Бутериным, который выделяет 3 типа блокчейн [5]:

1) Публичные блокчейн с открытым доступом (Public blockchains)

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

2) Приватные блокчейн с открытым доступом (Consortium blockchains)

3) Приватные блокчейн с закрытым доступом (Fully private blockchains)

Разберём каждый из них более детально.

1. Публичные блокчейн с открытым доступом

Самым распространённым на данный момент является именно этот тип, использующийся в таких криптовалютах как Биткоин, Эфириум, Рипл и пр. Его особенностями являются:

1) Полная открытость блоков для всех пользователей.

2) Пользователям нет необходимости доверять друг другу.

3) Полная децентрализация и независимость от третьих лиц.

4) Защищённость сети за счёт криптографических алгоритмов и применения большого количества компьютерных систем.

Он в первую очередь хорошо подходит для применения в финансовой сфере, где необходима полная независимость от третьего лица, прозрачность операций и высокая надёжность системы.

2. Приватные блокчейн с открытым доступом:

Здесь право заверять транзакции, вести аудит безопасности, вносить изменения в программное обеспечение и изменять базы данных имеют только привилегированные пользователи, остальные получают доступ к файлам для чтения. Соответственно, такая система уже не является полностью децентрализованной и зависит от определённого круга лиц.

Ее основные свойства:

1) Наличие проверенных валидаторов.

2) Высокая скорость подтверждения транзакций.

3) Невозможность проведения атаки 51% (когда в распоряжении атакующего находятся мощности больше, чем у всей остальной сети).

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

4) Возможность удаления записей из цепи либо их изменения.

5) Более низкая стоимость транзакций за счёт отсутствия необходимости в применении больших вычислительных мощностей.

Учитывая перечисленные свойства, можно сделать вывод, что данная система может хорошо подойти для государственных структур (например, здравоохранение: привилегированными пользователями в таком случае могут быть медучреждения, которые будут вносить в цепочку данные о истории больных, а пользователи смогут всегда открыть свою историю).

3. Приватные блокчейн с закрытым доступом

Блокчейн данного вида обладает теми же свойствами что и предыдущие, но с условием, что простые пользователи не могут стать участниками сети без подтверждения валидаторов, а также не всегда имеют доступ к чтению файлов цепи. Таким образом, данная система полностью перестаёт быть открытой и независимой от третьих лиц.

Свойства данной системы:

1) Закрытость данных от непривилегированных пользователей сети.

2) Полная закрытость сети от неавторизированных пользователей.

3) Невозможность проведения атаки 51%.

4) Полная зависимость от круга привилегированных пользователей.

5) Высокая надёжность и стойкость сети при условии доверия к валидаторам.

Этот блокчейн уже больше похож на классические централизованные сети, однако, обладая свойством ведения цепи взаимосвязанных блоков, может удачно применяться для внутренних закрытых частных сетей и системах защищенного документооборота на предприятиях или государственных структурах где необходимо хранение служебной информации.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

Анализ алгоритмов достижения консенсуса

Рассмотрим теперь основные алгоритмы достижения консенсуса – математические алгоритмы, позволяющие всем пользователям системы прийти к общему согласию относительно определённого ключевого момента.

Впервые идея о доказательстве своей легитимности и наличия определенных прав с помощью выполнения трудоёмкой работы была предложена в статье Синтии Дворк и Мни Наор «Pricing via Processing or Combatting Junk Mail» 1993 г. [6]. В этой статье пользователям предлагалось вычисление трудоёмкой функции для доступа к определённым ресурсам, при этом такое вычисление должно легко проверяться, однако быть довольно трудоёмким, хотя и вычисляться в приемлемые сроки. Данная система могла оберегать корпоративные сети от DDOS-атак, т.к. распространение огромного числа писем с одного компьютера становилась физически невыполнимой [7, 8]. Четырьмя годами позднее Адамом Бэком был создан проект Hashcash, основной идеей которого было нахождение значения определённого числа X, хэш которого содержал бы N старших бит одного значения, к примеру, нулевого [9]. В 1999 году впервые был упомянут термин Proof-of-Work в статье «Proofs of Work and Bread Pudding Protocols» Маркуса Якобсона и Ари Джуелс [10]. Более широкую известность данный метод приобрёл после того, как был применен в криптовалюте Биткоин: здесь доказательство работы происходит путём нахождения хэша блока транзакций через функцию SHA-256, причём для такового существуют определённые требования, а именно - заданное количество старших бит должно заполняться нулями. Впоследствии данный метод стал распространятся на другие криптовалюты, такие как Litecoin, Ripple, swiftcoin, etherum и пр. Наиболее распространенными являются модели «Доказательство работой (Prof of Work - PoW)», «Доказательство долей (Prof of Stake - PoS)», «Делегированное доказательство долей (Delegated proof of

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

stake)», Гибридная система «Prof of Work/Prof of Stake», Система «Доказательство активностью (Prof of Activity)», «Доказательство сжигания (Prof of burn)», «Доказательство ёмкостью (Proof of Capacity)», «Доказательство хранения (Proof of Storage)» [11].

Рассмотрим основные алгоритмы более подробно.

1. Доказательство работой

Данная модель предполагает участникам подтверждать своё действие выполнением трудоёмкой работы, при этом работа должна требовать больших, но приемлемых по времени вычислительных затрат, и должен существовать способ быстро проверить выполнение этой работы.

«Суть заключается в поиске такого значения, чей хэш (например, SHA-256) начинался бы с некоторого числа нулевых битов. Требуется выполнить объем работы, экспоненциально зависящий от числа нулей, но для проверки найденного значения достаточно вычислить лишь один хэш.» [11] Таким образом, подобрать такую хэш функция для блока данных весьма проблематично, а вот проверить уже существующую не составит труда.

К плюсам данного метода можно отнести:

– Относительную стойкость системы. Злоумышленнику необходимо завладеть 51% всей мощности сети, чтобы изменить цепочку.
– Независимость от третьих лиц. Совершенно необязательно доверять кому-либо из пользователей сети, нет необходимости в третьих лицах для заверения сделки.

К минусам относятся:

– Бесполезное расходование вычислительной мощности всех компьютеров при доказательстве работы.
– Низкие скорости обработки транзакций внутри сети. На данный момент, криптовалюты, построенные по системе доказательства работы, отстают от других систем в скорости работы в 10 раз, из-за

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

необходимости заверения каждого блока сложными вычислительными процессами.

– Возможность объединения майнеров в сообщества (пулы) с дальнейшим наращиванием объёмов, что, в итоге, порождает монополию на процесс подтверждения работы крупными организациями которые в итоге могут заключить конгломерат и захватить 51% мощности всей сети.

2. Доказательство долей.

Данная модель подразумевает достижение консенсуса своего рода голосованием, на котором каждый в качестве доказательства приводит свои активы в качестве ставки. Таким образом, если предложенный вариант окажется неблагонадёжным, участник, предложивший свой вариант, потеряет все свои активы, и мошенничество становится невыгодным.

Преимуществом данной модели являются:

– Снижение затрат на поддержание системы. Для подтверждения транзакций мы не нуждаемся в сложных вычислительных процессах.

– Отсутствие необходимости постоянного улучшения вычислительной техники и наращивании технических объёмов.

– Атака на систему становится намного дороже, так как если злоумышленник захочет купить 51% монет, курс сразу же вырастет, да и вряд ли будет смысл скупать больше половины всей валюты ради махинаций в ней же самой.

Однако, данная система имеет ряд серьезных недостатков:

– Она мотивирует участников к накоплению большого количества средств, что ведёт к децентрализации самой системы.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

– Также, как и в доказательстве работой, группы участников могут объединяться в группы и создавать собственные финансовые силы путём давления на других участников сети.
– Возможность двойной траты, а именно: злоумышленник может выстроить собственную цепочку путём расходования несуществующих ресурсов (приватные ключи израсходованных денег), которая окажется длиннее легитимной, причём честные пользователи могут поддержать её, так как не используют подлинные ресурсы (атака «nothing-on-stake»).

3. Делегированное доказательство долей.

Модель похожа на модель доказательства долей, однако, отличием является возможность обладающих активами пользователей «сдавать в аренду» часть своих средств для проведения майнинга. Пользователь, у которого много валюты, может сдать часть своих денег другим, которые не могут тратить её, но могут использовать её для голосования за добавление блока в цепь. Данная поправка стимулирует большее количество пользователей заниматься майнингом, так как для это теперь нет необходимости иметь крупные суммы валюты.

4. Гибридная система «PoW/PoS»

Система совмещает как создание блоков и добавление их в цепочку с помощью майнинга (PoW), так и с помощью доказательства своими депозитами (PoS). Сама цепочка состоит из обоих типов блоков. Таким образом, переписать предыдущие блоки обманным путём, используя уязвимости Proof of Authority (PoA), становится намного сложнее, так как существуют так называемые «точки контроля» в виде блоков PoW. Также, благодаря майнингу блоков, возможно производить эмиссию денег по принципу стандартной PoW, а подтверждение блоков путём PoS можно использовать как дополнительный источник доходов.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

Однако, уязвимость типа «nothing-on-stake» всё же остаётся, так как есть возможность нахождения блоков PoS по всей длине цепочки и соответственно использование ключей израсходованных денег для подтверждения альтернативной ветки блока злоумышленника.

5. Доказательство активностью

Решением проблемы «nothing-on-stake» в гибридных системах может послужить использование для каждого блока как PoW-майнинга, так и PoS. На данный момент эта система существует только теоретически, однако, имеет огромный потенциал использования. Она предполагает, что участники PoS вступают в голосование только после того, как майнерами произведена определённая часть работы, т.е. даже если какой-либо пользователь будет владеть 51% монет, он не сможет единолично контролировать создание блоков.

6. Доказательство сжигания

Достаточно редкая и малораспространённая концепция, при которой пользователи отправляют монеты на адреса, с которых невозможно снять деньги обратно, т.е. своего рода «сжигание» средств ради получения права на пожизненный майнинг новых токенов. Эта модель является всего лишь теоретической и до настоящего момента не использовалась в крупных проектах.

7. Доказательство ёмкостью

Алгоритм представляет собой систему, подобную Доказательству долей, использующую в качестве показателя доверия не счёт вклада, а количество выделенных мегабайт на компьютере. Алгоритм построен таким образом, что создаёт на жёстком диске крупные блоки данных путём многократного хэширования ключа с некими случайными числами, и в конце каждого блока создаёт индекс-метку. Чем больше памяти выделено – тем

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

больше меток в наличии, соответственно, больше шансов на подтверждение блока цепи.

Преимуществами данного алгоритма являются:

– Защита от бот-сетей, т.к. довольно легко выявить внезапное переполнение жёсткого диска компьютера.
– Отсутствие необходимости траты энергии впустую, как при алгоритме Доказательства Работой.

Недостатки:

– Возможность атаки nothing-on-stake
– Возможная «гонка вооружений» в плане постоянного наращивания объёмов памяти.
– Не самая быстрая скорость работы из-за долгого отклика при обращении в HDD дискам.

8. Доказательство хранения.

Алгоритм достижения консенсуса схож с предыдущим, однако, основная идея в том, что выделенное дисковое пространство используется всеми участниками сети как облачное хранилище.

9, Доказательство компетентностью

Алгоритм, в котором все пользователи имеют свой ранг в сети, в зависимости от которого изменяется шанс заверения пользователем блока. К примеру, все пользователи могут делиться на обычных, экспертов и администраторов. Шанс майнинга блока для обычного пользователя может быть равен 1%, для эксперта 20%, а для администраторов 60%.

Проанализировав возможные варианты реализации блокчейн в зависимости от приватности пользователей и закрытости информации, можно построить график, изображённый на рис. 1.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

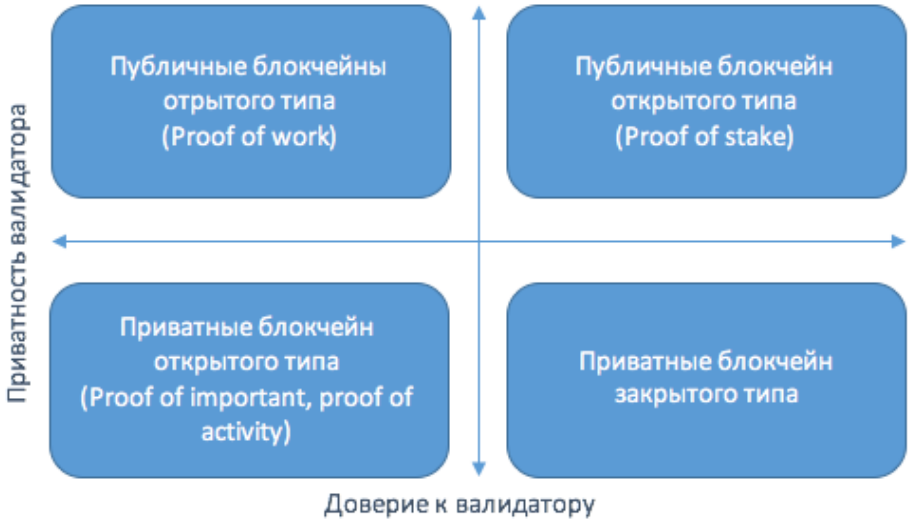

Рис. 1. – Классификация блокчейн по отношению к параметрам приватности и доверия

В итоге в левом верхнем углу, где мы получаем минимальное доверие к валидаторам и максимальную приватность пользователей, у нас располагаются публичные сети с открытым доступом. Для таких сетей преимущественно использование алгоритма достижения консенсуса Proof of work. Примером таких сетей выступают известные всем криптовалюты, такие как Биткоин, Рипл, и др.

В правом верхнем углу также максимальная приватность валидатора, однако существует доверие к валидатором. Для таких систем подходят алгоритмы Proof of stake, где нет необходимости публично открывать свою личность, однако, честность доказывается активами, вложенными в ставку на подтверждение блока. Над внедрением такого решения на данный момент работает криптовалюта Эфириум.

В нижней части оси ординат располагаются приватные блокчейн, так как в таких сетях отсутствует или почти отсутствует приватность валидаторов.

В левом нижнем углу располагаются приватные блокчейн открытого типа. В таких системах низкое доверие к валидатору, поэтому в них

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

повышенные требования к алгоритмам достижения консенсуса, примером таких могут быть Proof of important, proof of activity. Применение таких систем может быть обусловлено в медицинских учреждениях, где для ведения и внесения изменений в историю болезней человека медицинским центрам необходимо достигать консенсуса, не прибегая к очень сложным вычислительным процессам, а полагаясь на симбиоз авторитетности данного валидатора плюс выполнение небольшой работы по подтверждению и защите транзакций.

Последней областью таблицы является правый нижний угол, который приходится на приватные блокчейн закрытого типа, в которых все центры заверения транзакций являются открытыми, а доверие к ним очень велико. Таким образом, данный вид блокчейн скорее напоминает обычные централизованные иерархические сети, однако, может быть успешно использован на практике благодаря свойствам непрерывной цепи взаимосвязанных блоков информации.

Программная реализация системы защищенного документооборота на основе технологии блокчейн

На основании проведенного анализа нами были сформулированы следующие требования к разработке:

- Каждый авторизированный пользователь системы должен иметь доступ к документам.
- Несанкционированный доступ к документам должен быть невозможен.
- Изменять, подделывать или удалять документы из реестра не должно быть возможно.
- Каждый документ должен иметь автора и быть подписан.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

Исходя из требований, предъявляемых к системе, было признано целесообразным использовать следующий тип блокчейн: приватный закрытого доступа, так как блокчейн данного вида обладают условием, что простые пользователи не могут стать участниками сети без подтверждения валидаторов, а также не всегда имеют доступ к чтению файлов цепи.

В качестве алгоритма достижения консенсуса была выбрана гибридная система доказательства долей и доказательства работой – «Proof of Activity», так как она включает в себя все достоинства этих двух алгоритмов и является хорошим альтернативным решением для использования в нашей системе.

Был разработан соответствующий программный комплекс, были проведены эксперименты по подтверждению авторства документов, попытки удаления и изменения документов, а также попытки подмены авторства документа, которые подтвердили корректную работу системы.

Литература

1. Блокчейн: определение, блоки транзакций и применение вне сферы криптовалют // hr-portal.ru URL:hr-portal.ru/varticle/blokcheyn-opredelenie-bloki-tranzakciy-i-primenenie-vne-sfery-kriptovalyut

2. Генкин Артем, Михеев Алексей. Блокчейн. Как это работает и что ждет нас завтра. М.: Альпина Паблишер, 2017. 592 с. (ISBN 978-5-9614-6558-7).

3. Технологии Блокчейн: Современное состояние и ключевые инсайты // ФИПС, 2018 URL: new.fips.ru/vse-uslugi/patent-analytics/report-blockchain.pdf

4. BlockSigh: How it all works URL: blocksign.com/about

5. Vitalik Buterin On Public and Private Blockchains // Blog of Etherum 7.08.15 URL: blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

6. Cynthia Dwork, Moni Naor Pricing via Processing or Combatting Junk Mail // The Weizmann Institute of Science URL: wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf

7. Абрамов Е.С., Тарасов Я.В. Применение комбинированного нейросетевого метода для обнаружения низкоинтенсивных DDoS-атак на web-сервисы // Инженерный вестник Дона, 2017, №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4354

8. Георгица И.В., Гончаров С.А., Мохов В.А. Мультиагентное моделирование сетевой атаки типа DDoS // Инженерный вестник Дона, 2013, №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1852.

9. Adam Back Hashcash - A Denial of Service Counter-Measure // Hashcash URL: hashcash.org/hashcash.pdf

10. Markus Jakobsson Proofs of Work and Bread Pudding Protocols // Hashcash. URL: hashcash.org/papers/bread-pudding.pdf.

11. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System URL: bitcoin.org/bitcoin.pdf.

References

1. Blokchejn: opredelenie, bloki tranzakcij i primenenie vne sfery kriptovaljut [Blockchain: definition, transaction blocks and application outside the realm of cryptocurrencies]. Hr-portal.ru. URL:hr-portal.ru/varticle/blokcheyn-opredelenie-bloki-tranzakciy-i-primenenie-vne-sfery-kriptovalyut.

2. Genkin Artem, Mikheev Aleksey. Blokcheyn. Kak eto rabotaet i chto zhdet nas zavtra. [Blockchain. How it works and what a waits us tomorrow]. M.: Al'pina Pablisher, 2017. 592 p. (ISBN 978-5-9614-6558-7).

3. Tekhnologii Blokcheyn: Sovremennoe sostoyanie i klyuchevye insayty [Blockchain Technologies: Current State and Key Insights]. FIPS, 2018 URL: new.fips.ru/vse-uslugi/patent-analytics/report-blockchain.pdf.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019

4. BlockSigh: How it all works URL: blocksign.com/about.

5. Vitalik Buterin On Public and Private Blockchains. Blog of Etherum 7.08.15 URL: blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

6. Cynthia Dwork, Moni Naor Pricing via Processing or Combatting Junk Mail. The Weizmann Institute of Science URL: wisdom.weizmann.ac.il/~naor/PAPERS/pvp.pdf.

7. Abramov E.S., Tarasov Ya.V. Inženernyj vestnik Dona (Rus), 2017, №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4354.

8. Georgitsa I.V., Goncharov S.A., Mokhov V.A. Inženernyj vestnik Dona (Rus), 2013, №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1852.

9. Adam Back Hashcash - A Denial of Service Counter-Measure Hashcash. URL: hashcash.org/hashcash.pdf.

10. Markus Jakobsson Proofs of Work and Bread Pudding Protocols. Hashcash URL: hashcash.org/papers/bread-pudding.pdf

11. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System URL: bitcoin.org/bitcoin.pdf.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2019