Владимир И. Будзко[1], Наталья Г. Милославская[2]
[1]Федеральный исследовательский центр «Информатика и управление» РАН,
ул. Вавилова, 44, кор.2, Москва, 119333, Россия
e-mail: vbudzko@ipiran.ru, https://orcid.org/0000-0002-8235-0404
[2]Национальной исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

ВОПРОСЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ БЛОКЧЕЙНА

DOI: http://dx.doi.org/10.26583/bit.2019.1.04

Аннотация. С момента появления Интернета технологии блокчейна (ТБ) были признаны одними из самых взрывных инноваций начала XXI века, способными изменить как финансовые, так и нефинансовые приложения. В статье приводятся различные толкования блокчейна, иллюстрируется процесс включения нового блока, кратко рассматриваются вопросы стандартизации, новых технологий блокчейна такими организациями, как ISO и NIST, а также вводится базовое для ТБ понятие транзакции. Главная задача статьи – разобраться и показать, что должно записываться в общем случае в блок кроме его идентификатора и хэш-кода, связывающего каждый новый блок с его предшественником. Приводится пример учета и сохранения в целостном и хронологическом виде транзакций в блокчейне для случая его применения при управлении инцидентами информационной безопасности в компьютерных сетях. Представленные результаты могут быть распространены на предметные области, в которых возможно и обосновано создание блокчейна. В заключении определены направления последующих исследований в данной области.

Ключевые слова: технологии блокчейна, технологии распределенного реестра, стандартизация, транзакция, инцидент информационной безопасности, управление инцидентами информационной безопасности.

Для цитирования: БУДЗКО, Владимир И.; МИЛОСЛАВСКАЯ, Наталья Г. ВОПРОСЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ БЛОКЧЕЙНА. Безопасность информационных технологий, [S.l.], p. 36-45, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1178>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.04.

Vladimir I. Budzko[1], Natalia G. Miloslavskaya [2]
[1]Federal Research Center «Computer Science and Control» of Russian Academy of Sciences,
Vavilov str., 44/2, Moscow, 119333, Russia,
e-mail: vbudzko@ipiran.ru, https://orcid.org/0000-0002-8235-0404
[2]National Research Nuclear University MEPhI,
Kashirskoe shosse, 31, Moscow, 115409, Russia
e-mail: ngmiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

Issues of Practical Application of Blockchain Technology

DOI: http://dx.doi.org/10.26583/bit.2019.1.04

Abstract. Since the advent of the Internet, the blockchain technology (BT) has been recognized as one of the most explosive innovations of the early 21st century, capable of changing both financial and non-financial applications. The paper presents various interpretations of the blockchain, illustrates the process of inclusion of a new block into it, briefly discusses the issues of standardization of this new technology by organizations such as ISO and NIST, as well as introduces the basic BT notion for a transaction. The main task of this article is to give a generalized idea of the composition and structure of blocks of the blockchain, taking into account the identifier and the hash connecting each new block with its predecessor. It also provides an example of accounting and saving in a holistic and chronological form transactions in the blockchain for the case of its use in managing information security incidents in computer networks. The presented results can be extended to any subject area in which it is possible and reasonable to create a blockchain. In conclusion, the directions of subsequent research in this area are determined.

Keywords: Blockchain Technology, Distributed Ledger Technology, Standardization, Transaction, Information Security Incident, Information Security Incident Management.

For citation: BUDZKO, Vladimir I.; MILOSLAVSKAYA, Natalia G. Issues of Practical Application of Blockchain Technology. IT Security (Russia), [S.l.], p. 36-45, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1178>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.04.

Введение

Новые передовые технологии оказывают, как правило, огромное влияние на то, как бизнес внедряет инновации для улучшения своих конкурентных преимуществ. С момента появления Интернета технологии блокчейна (ТБ) были признаны одними из самых взрывных инноваций начала XXI века. Впервые они были упомянуты в 2008 году при появлении биткоина, связанного с псевдонимом его изобретателя С. Накамото [1]. Компания Gartner включила ТБ в Топ-10 стратегических технологических тенденций 2017 года [2].

Как технологии создания проверяемых цифровых записей ТБ в настоящее время используются в финансовых приложениях (например, для платежей, обмена валюты, денежных переводов и кошельков, торговых финансов, рынков, микросделок, инвестиции, брокерства, страхования и т.д.), а также в нефинансовых приложениях (например, управление идентификацией в электронном виде, аутентификация и авторизация, системы хранения и доставки данных в электронном виде, системы сертификации, смарт-контракты, разработка приложений, электронное голосование на выборах, управление медицинскими записями пациентов, распределение рабочей нагрузки для систем связи, компьютерные системы, которые должны соответствовать требованиям законодательства без вмешательства человека, интернет вещей и т.д.).

И все же применение блокчейна наиболее оправдано при решении задач, связанных в основном с обеспечением целостности сохраняемой информации. Прежде всего это закрепление в блоках цепи последовательности транзакций в их исторической очередности и сути совершенных транзакций, которые и составляют смысловую основу записываемой в блоке информации.

В данной статье ставится задача разобраться и показать, что же должно записываться в общем случае в блок кроме его идентификатора и хэш-кода, связывающего каждый новый блок с его предшественником. Именно этого понимания сейчас как раз и не хватает, судя по анализу многочисленных публикаций и выступлений на конференциях различного уровня – международных и отечественных, концептуальных и более технических. Все остальные вопросы ТБ в силу ограниченности объема статьи выходят за ее рамки.

1. Понятие технологий блокчейна

Прежде всего приведем наиболее часто цитируемые определения ТБ, чтобы на их основе сформировать собственное понимание этой технологии. Эти определения таковы:

- UK Government, 2016: “Технология распределенного реестра” [3];
- PriceWaterhouseCoopers, 2016: “Децентрализованный реестр всех транзакций в одноранговой сети, где участники могут подтверждать транзакции без участия центра сертификации” [4];
- Wilson, 2017: “Это не "машина доверия". Посредством протокола блокчейна она достигает консенсуса только в вопросе об одной специфической вещи – порядке входов в реестр, без какого-либо пристрастия” [5];
- OpenBlockchain, 2017: “Технология, обеспечивающая защищенное и устойчивое управление распределенными данными в сочетании с методами анализа данных, которые добавляют масштабируемость и гибкость” [6];
- Nielson, 2017: “Распределенная файловая система, которая хранит копии файлов участников, которые договариваются об изменениях по взаимному согласию, причем файл состоит из блоков и каждый блок имеет криптографическую подпись последнего блока, что делает запись неизменяемой” [7];
- Primechaintech, 2018: “Одноранговая сеть, которая ставит отметки времени в записи, связывая их хэш-кодами в непрерывную цепочку основанного на хэш-кодах доказательства выполнения работы, формирующая запись, которая не может быть изменена без повторного доказательства выполнения работы” [8];
- Draft NISTIR 8202, 2018: “Распределенный цифровой реестр криптографически подписанных транзакций, которые сгруппированы в блоки. Каждый блок криптографически связан с предыдущим после проверки и принятия консенсусного решения. По мере добавления новых блоков более старые блоки становится сложнее

модифицировать. Новые блоки реплицируются по всем копиям реестра в сети, а любые конфликты разрешаются автоматически с использованием установленных правил" [9].

Обобщая приведенное выше и учитывая многократно повторяющиеся свойства, в рамках данной статьи под блокчейном будем понимать особый тип защищенной распределенной структуры данных – базу данных (БД), которая без главного администратора и централизованного хранилища данных поддерживает постоянно расширяющийся список нередактируемых блоков/записей и устанавливает правила работы с транзакциями/событиями, записываемыми в блоках и привязанными таким образом к ним (в отличие от обычных БД, в которых правила часто устанавливаются для всей БД или приложения).

Такая БД совместно используется группой пользователей блокчейна – узлами, или нодами (англ. nodes) – сущностями в блокчейн-сети (транспортном уровне блокчейн-платформы), принимающими и обрабатывающими транзакции и делящимися информацией о потенциальной транзакции. Узел либо доказывает (публичный блокчейн) или проверяет (гибридный/частный блокчейн) транзакции и затем добавляет их в блок с уникальным хэш-кодом. Таким образом, среди узлов выделяются два особых типа: майнеры (англ. miners) и валидаторы (англ. validators). Майнеры ищут в системе (точнее, в соответствующих источниках данных) новые транзакции и криптографически доказывают, что транзакция реальна (действительна) для ее включения в блокчейн в составе новых блоков, используя такие доказательные средства, как доказательство выполнения работы/ресурса/состояния/активности и т.д., предлагают их. Валидаторы проверяют серии или отдельные транзакции на основе соответствующих средств их проверки (например, византийский механизм отказоустойчивости или «двойные расходы»).

В блок может входить одна или более транзакций, сгруппированных по определенному критерию. Новый блок будет включен в блокчейн на основе одного из применяемых способов достижения консенсуса, например, большинства узлов, которые согласны с тем, что все транзакции в нем являются действительными (законными, обоснованными) и этот правильно созданный блок может быть включен в блокчейн (рис.1). Определение того, что транзакция действительно имела место, очень важно. Просто потому, что если кто-то утверждает, что транзакция была, это не означает, что она действительно произошла. Транзакции подписываются и могут быть в любое время проверены с помощью пары открытого и закрытого ключей.

После того как новый блок утвержден и включен в цепочку, он не может быть удален или изменен. Блоки связаны друг с другом (как цепь) в хронологическом порядке. Таким образом, в блокчейне в блоках в защищенном виде хранится общедоступная история всех транзакций в какой-либо системе, для которой создается данный блокчейн.

Для самого блокчейна также в защищенном виде хранится история включения в него блоков. Эта история используется всеми пользователями блокчейна и является неизменной и проверяемой для записи истории транзакций, для чего используются различные протоколы. Различают четыре таких протокола: протокол транзакций, протокол для одноранговой коммуникации узлов с одинаковыми правами, протокола достижения консенсуса для обсуждения и достижения соглашения по соответствующим вопросам и протокол хранения данных для извлечения и отправки данных в БД.

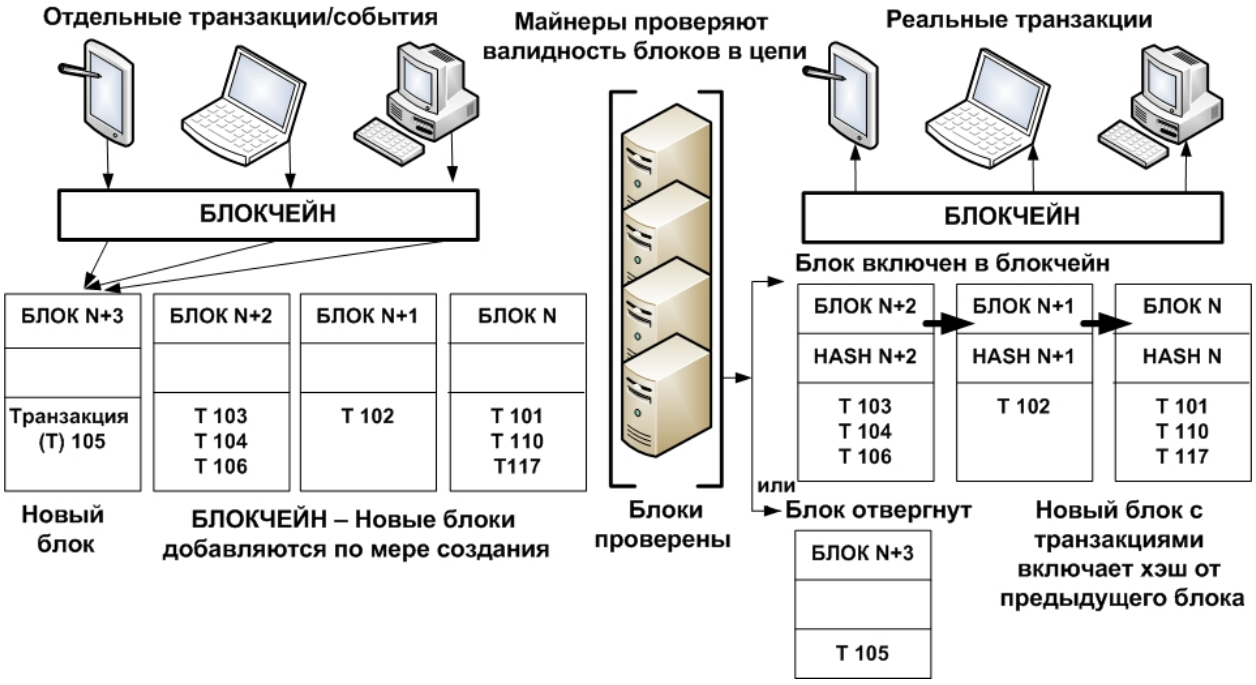

Рис. 1. Включение нового блока в блокчейн
(Fig. 1. Inclusion of a new block into the blockchain)

2. Стандартизация технологий блокчейна

Вопросами стандартизации новых технологий уже несколько лет занимаются ряд организаций.

В 2016 году был создан специализированный технический комитет ISO/TC 307 “Технологии блокчейна и распределенного реестра”. Его область действия была определена как стандартизация ТБ и технологий распределенного реестра (ТРР). ISO/TC 307 объединяет несколько специализированных и рабочих групп, а именно «Технологии блокчейна и распределенного реестра и технологии защиты ИТ», «Основы», «Примеры использования», «Безопасность, приватность и идентификация», «Умные контракты и их применение», «Управление системами технологии блокчейна и распределенного реестра» и «Интероперабельность систем технологии блокчейна и распределенного реестра». В настоящее время технический комитет работает над следующими десятью стандартами, посвященными ТБ и ТРР:

- ISO 22739 «Терминология»;
- ISO 23244 «Обзор приватности и защиты персональных данных»;
- ISO 23245 «Риски и уязвимости безопасности»;
- ISO 23246 «Обзор управления идентификацией с использованием ТБ и ТРР»;
- ISO 23257 «Эталонная архитектура»;
- ISO 23258 «Таксономия и онтология»;
- ISO 23259 «Юридически обязательные смарт-контракты»;
- ISO 23455 «Обзор и взаимодействие между смарт-контрактами в системах ТБ и ТРР»;
- ISO 23576 «Безопасность хранителей цифровых активов»;
- ISO 23578 «Проблемы обнаружения, связанные с интероперабельностью».

Большинство этих стандартов находятся на подготовительном этапе их разработки, и только два из них (22739 и 23455) имеют первые зарегистрированные проекты. Поэтому любое обсуждение их содержания преждевременно.

В июне 2017 года IEEE-SA начала подготовку стандарта IEEE P2418.1, посвященного использованию, внедрению и взаимодействию блокчейна при его применении в интернете вещей и ожидаемого к июню 2019 года. Разрабатываемая структура будет включать блокчейн-токены, смарт-контракты, транзакции, аутентифицированную сеть, открытый/публичный (англ. permissioned) и закрытый/частный (англ. permissionless) блокчейн для поддержки

децентрализованных, автономных одноранговых коммуникаций между потребителем и компьютером или между компьютерами без необходимости привлечения доверенного посредника. Эта архитектура решит вопросы масштабируемости адресов, интероперабельности, безопасности и приватности при использовании блокчейна в интернете вещей.

В проекте NISTIR 8202 «Обзор технологий блокчейна» [9] обсуждается, как работают ТБ, особенно при их применении к электронной валюте. В нем также показаны более широкие применения ТБ (банковское дело, цепочка поставок, страхование и здравоохранение, доверенная фиксация времени, энергетика) и выделены некоторые из ограничений, связанные с контролем блокчейна, злонамеренными пользователями, отсутствием доверия, использованием ресурсов, переносом бремени хранения учетных данных на пользователей, а также частной/открытой инфраструктурой ключей и идентификацией В этом проекте определяются высокоуровневые компоненты архитектуры блокчейна, такие как транзакции, блоки, хэш-коды, вилки и т.д. В нем описывается, как новые блоки добавляются в блокчейн и как модели консенсуса разрешают конфликты между майнерами. Определяются различные модели закрытого блокчейна и примеры их использования. Проект также охватывает смарт-контракты и платформы блокчейна, которые используются сегодня. Это единственный в настоящее время общедоступный документ по ТБ.

Данная ситуация со стандартизацией ТБ лишь доказывает, что остается еще много нерешенных вопросов их унификации. Назрела явная необходимость разъяснений в различных публикациях, не только как теоретически относиться к ТБ, но и как реализовывать их на практике.

3. Транзакции, записываемые в блоках блокчейна

В начале статьи сформулирован главный, интересующий в рамках данного исследования вопрос – что должно записываться в блок кроме его номера и хэш-кода, связывающего его с предыдущим блоком?

Данный вопрос неразрывно связан с другим важнейшим вопросом – что такое транзакция, которая помещается в блок и после этого становится общедоступной для определенного круга пользователей блокчейна (в зависимости от того, какой это тип блокчейна – открытый или закрытый)? Как описать транзакцию, чтобы размер блока был небольшим, что существенно влияет на производительность блокчейн-платформы?

В [9] под транзакцией понимается запись перемещения между взаимодействующими сторонами активов, например, цифровых денег, материальных ценностей и т.п. Транзакцией может быть событие проверки счёта, формируемое каждый раз, когда деньги вносятся на расчётный счёт или снимаются с него.

Как было отмечено выше, каждый блок в блокчейне может содержать одну или несколько транзакций. Рассмотрим пример обработки счетов. Отдельная транзакция, как правило, включает следующие информационные поля (хотя их может быть и больше) [9]:

- сумма – общая сумма цифровых активов, предназначенных для перемещения;
- входные данные – перечень цифровых активов, подлежащих перемещению (их общая стоимость равна сумме). При этом каждый цифровой актив имеет уникальный идентификатор и может иметь стоимость, отличную от стоимости других активов. Сами активы не могут быть добавлены или удалены из списка существующих цифровых активов. Но цифровые активы могут быть разделены на несколько новых (каждый с меньшей стоимостью) или объединены в меньшее количество новых цифровых активов (каждый, соответственно, с большей стоимостью);
- выходные данные – учётные записи, на которые перемещаются цифровые активы. Каждые выходные данные определяют стоимость для перемещения новому(ым) владельцу(ам), идентификатор нового(ых) владельца(ев) и набор требований, которым должен(ы) удовлетворять новый(е) владелец(ы) при получения указанной стоимости. Если цифровых активов больше чем требуется, то лишние возвращаются отправителю (этот способ называется «внесение изменений»);
- идентификатор/хэш-код транзакции – уникальный идентификатор каждой транзакции. В некоторых вариантах блокчейна используются идентификаторы, а в

других в качестве уникального идентификатора используется хэш-код конкретной транзакции.

Приведем другой пример – применение блокчейна для ведения домовой книги. В одном блоке можно фиксировать состояние всех квартир многоквартирного дома сразу или, что разумнее, только одной квартиры и тогда изменять цепь при изменении информации по одной квартире. Новый блок будет создаваться только тогда, когда изменится состояние любой квартиры, например, поменяется состав ее жильцов. Для данного примера транзакция должна включать номер транзакции, номер квартиры, дату изменения состава жильцов, основание для изменения этого состава и новый список жильцов квартиры с их установочными данными (фамилия, имя, отчество, дата рождения и пр.) и, возможно другие параметры.

Чтобы информацию в блокчейне можно было быстро обрабатывать, нужно оптимизировать размеры и состав полей, входящих в описание одной транзакции. Например, использование блокчейна – для записи действий всех участвующих сторон при работе с договорами.

В каждый записывать сам договор в блок не имеет смысла, поскольку во многих блоках он будет одним и тем же. Можно лишь указывать однозначно номер договора и соответствующую ему контрольную сумму (контрольная сумма текстового файла с договором), которая должна в защищенном блокчейне точно соответствовать его виду на момент создания блока. В случае работы с договорами на разных стадиях их жизненного цикла транзакции будут разными: на стадии разработки и согласования – кто и когда вносил какие изменения, на стадии исполнения транзакции будут отражать определенную последовательность действий, на стадии контроля – степень соответствия реальной ситуации требованиям договора и т.п.

4. Пример описания транзакций в блокчейне, применяемом при управлении инцидентами информационной безопасности

При управлении инцидентами информационной безопасности (ИБ) в сети организаций требуется сохранять последовательность и описание всех произошедших и приведших к инциденту событий ИБ [10]. Событие ИБ – это идентифицированное появление определенного состояния актива организации (системы, сервиса или сети), указывающего на возможное нарушение политики ИБ или нарушения в работе средств защиты либо возникновение ранее неизвестной ситуации, которая может иметь отношение к ИБ [11]. Инцидент ИБ – это появление одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операций и указывающих на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ для активов организации [11]. События ИБ можно рассматривать как часть инцидента ИБ, а сам инцидент ИБ как совокупность событий ИБ.

При такой постановке задачи закрытый (в рамках одной организации) блокчейн является идеальным средством сохранения событий ИБ в сетевой среде, поскольку блокчейн записывает и выстраивает их в строго хронологическом порядке. Таким образом, блокчейн в данном случае может рассматриваться как однонаправленная (без обратной связи) структура данных (цепь) со связанным списком блоков, каждый из которых ссылается на предыдущий, используя хранимые в заголовке блока хэш-коды-указатели. Один блок с уникальным идентификатором и криптографической ссылкой на предыдущий валидный блок объединяет транзакции – события ИБ, принадлежащие к одному и тому же инциденту ИБ (как его последовательные шаги). Создание повторяющегося блока (его содержимое аналогично одному из предшествующих блоков) с новым идентификатором означает наличие повторяющихся событий в сети, характерных, например, для атаки типа «отказ в обслуживании».

Все заранее предопределенные, надежные (доверенные) источники данных в виде агентов на каждом сетевом ресурсе, требующем мониторинга ИБ, собирают «сырые» (англ. raw) события, отбрасывают те, которые ни при каких обстоятельствах не могут повлиять на ИБ, и отправляют все оставшиеся события (подозрительные и точно относящиеся к ИБ, так называемые «чистые» события) в единую централизованную БД ожидающих решения событий (БДОРС), совместно используемую всеми источниками данных. В зависимости от политики организации любое событие в сети может быть классифицировано как не относящееся к ИБ,

подозрительное событие или событие/инцидент ИБ. Например, вход в систему с правильными учетными данными — это только событие. Любая попытка входа с неверными учетными данными является событием ИБ и может быть либо ошибкой пользователя, либо началом хакерской атаки. В последнем случае фактическая несанкционированная активность, приводящая в будущем к возникновению инцидента ИБ, может быть обнаружена, как правило, после такого события ИБ.

Источники данных могут просматривать только свои собранные данные в БДОРС. Из событий из БДОРС формируются блоки, которые затем после их обработки майнерами и валидаторами передаются в блокчейн. Существенные преимущества этого подхода состоят в том, что если один узел скомпрометирован (взломан), то остальные нет и общий блокчейн имеет высокую степень прозрачности для углубленного анализа инцидентов ИБ, если это потребуется позднее.

Формат записи о событии ИБ в блоке может быть взят из одной из спецификаций описания инцидентов ИБ, используемой в настоящее время производителями средств обеспечения сетевой безопасности (СОСБ). Чаще всего это спецификации компании MITRE Cyber Observable eXpression (CybOX) [12], Structured Threat Information Expression (STIX) [13] или Trusted Automated eXchange of Indicator Information (TAXII) [14], разработанные в 2013 году.

Создание блокчейна, содержащего только события ИБ из надежных источников данных, хорошо вписывается в ТБ. Один блок содержит одно подозрительное событие, одно событие ИБ или состоит из нескольких событий ИБ.

Примеры относящихся и не относящихся к ИБ событий на территории некоторой организации А с источниками данных о них и последующими действиями по записи информации о них в блокчейн представлены в табл. 1. Причем запись блоков с подозрительными событиями лучше всего осуществлять в «боковую» цепь (англ. Sidechain), из которой потом блоки можно перемещать в основную цепь (англ. Main chain) с «чистыми» событиями ИБ.

Каждый блок, передаваемый в блокчейн, должен включать ссылки на все исходные «сырые события», из которых было выведено его содержимое. Все источники данных, передающие данные о событиях в БДОРС, должны быть соединены друг с другом и синхронизованы, как правило, через процесс согласования. В этом случае один и тот же инцидент ИБ может быть задокументирован с разных точек зрения различными источниками данных. Вместо того чтобы СОСБ хранили и согласовывали свои собственные отдельные записи об одном и том же событии ИБ из своих отдельных, по-разному управляемых журналов, многие черты одного инцидента ИБ одновременно регистрируются в реальном времени в блокчейне, который является общим для всех источников данных. Блоки с «чистыми» событиями ИБ идут в основную цепь, а блоки с подозрительными событиями идут в боковую цепь для дополнительного анализа или ожидания прибытия в обе основную и боковую цепи блоков с событиями ИБ, которые подтвердят их статус как «чистый» инцидент ИБ. После этого блок будет перенесен в основную цепь.

Чтобы проиллюстрировать процесс формирования блока для дальнейшего включения в боковую цепь, рассмотрим, например, составное подозрительное событие из табл. 1 (строка 4). Вся деятельность работника после входа на территорию организации будет записана одним или несколькими соответствующими СОСБ. Эти действия будут записываться в журналы как отдельные необработанные события. Новый блок будет содержать все события, за исключением случаев повторного описания одного и того же события различными СОСБ (последние случаи), ссылки на все источники с исходными «сырыми» данными об этих событиях (в случае, если в будущем потребуется дополнительный анализ данного события) и время совершения/фиксации события (рис. 2).

Таблица 1. Примеры относящихся и не относящихся к ИБ событий в организации А

Тип события	***События***	***Источники данных***	***Последующие действия***
Не относящееся к ИБ событие	Единичное (атомарное) событие: работник (уборщик) вошел на территорию организации	Система контроля доступа (СКД)	Блок не формируется, но событие хранится в локальной БД СКД
Не относящееся к ИБ событие	Составное событие: • сотрудник ИТ-отдела вошел на территорию организации; • сотрудник ИТ-отдела вошел в свой офис; • сотрудник ИТ-отдела включил свою рабочую станцию; • сотрудник ИТ-отдела быстро и без ошибок ввел свои учетные данные; • сотрудник ИТ-отдела запустил авторизованное приложение	• СКД; • Система видеонаблюдения (СВ); • Система контроля включения питания компьютера (ВПК); • Система управления объектами и субъектами доступа (СУОСД); • Диспетчер задач	Блок не формируется, но отдельные события хранятся в отдельных БД СКД, СВ и т.д.
Подозрительное событие	Единичное (атомарное) событие: работник (уборщик) включил рабочую станцию	ВПК	Блок формируется для передачи в боковую цепь; событие хранится в БД ВПК; в блок вставляется ссылка на исходное событие
Подозрительное событие	Составное событие: • сотрудник ИТ-отдела вошел на территорию организации; • сотрудник ИТ-отдела вошел в свой офис; • сотрудник ИТ-отдела включил свою рабочую станцию; • сотрудник ИТ-отдела быстро и без ошибок ввел свои учетные данные; • сотрудник ИТ-отдела открыл документ Word, сделал скриншоты на каждой странице этого документа, сохраняя каждый на флэш-накопителе	• СКД; • СВ; • ВПК; • СУОСД; • Диспетчер задач, средство записи действий пользователя (СЗДП), DLP-системы	Блок формируется для передачи в боковую цепь; событие хранится в БД СКД, СВ и т.д.; в блок вставляется ссылка на исходное событие
«Чистое» событие ИБ	Единичное (атомарное) событие: работник (уборщик) сделал скриншоты невыключенного экрана компьютера в отсутствие его владельца	СЗДП	Блок формируется для передачи в основную цепь; событие хранится в БД СЗДП; в блок вставляется ссылка на начальное событие ИБ
«Чистое» событие ИБ	Составное событие: • работник (уборщик) включил рабочую станцию в одном из офисов в отсутствии его пользователя; • работник (уборщик) пытался методом грубой силы подобрать пароль, пока учетная запись не была заблокирована	• ВПК; • СЗДП	Блок формируется для передачи в основную цепь через узел; отдельные события хранятся в отдельных БД СЗДП и т.д.; в блок вставляются ссылки на начальные события ИБ

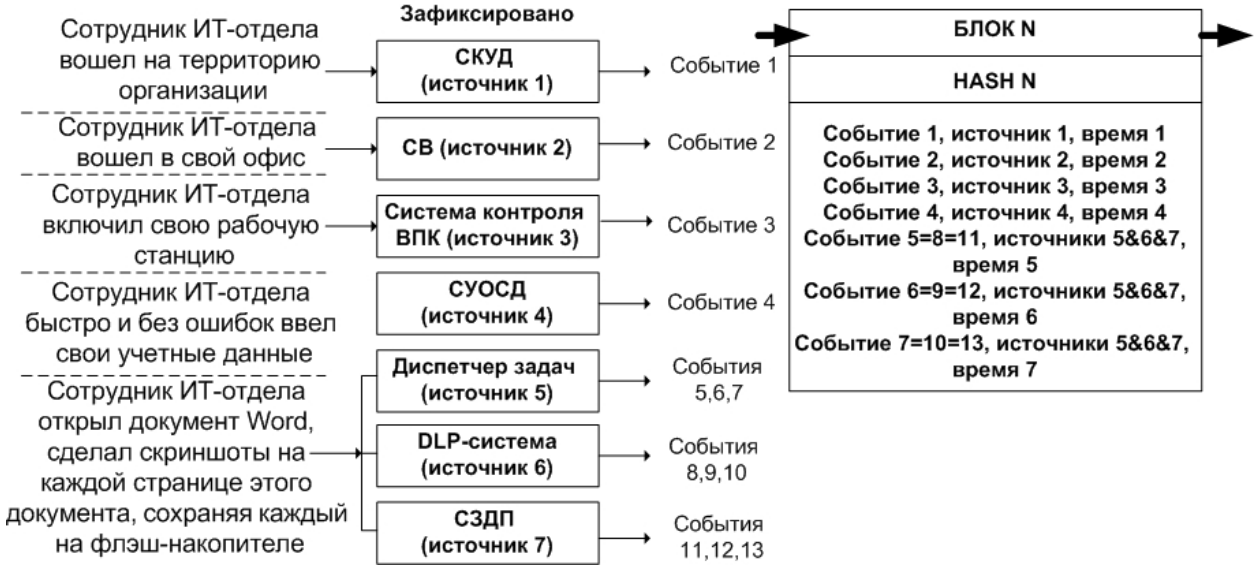

Рис. 2. Пример формирования блока для его включения в блокчейн
(Fig. 2. An example of the formation of a block to be included in the blockchain)

Представленный в этой статье блокчейн со временем потребует изменения, поскольку некоторые подозрительные события в будущем могут проявить себя как не имеющие отношения к ИБ. Этот вопрос требует отдельного детального рассмотрения и связан он с так называемым «сворачиваемым», или редактируемым, блокчейном, основы которого описаны в работах компании Accenture [15, 16].

Заключение

Широко распространенные и рекламируемые различными производителями варианты реализации технологии блокчейна пока не имеют единого стандарта (набора стандартов). Важно понимать, что эти технологии не составляют основы построения автоматизированной информационной системы (АИС), а лишь позволяют создать ее составной элемент, обеспечивающий неизменность реестров, в которых фиксируются определенные действия (например, факт заключения контракта и его важнейшие реквизиты, покупка с указанием суммы и идентификатора товара и прочее), для поддержки которых система создается. В данной статье было показано, что записывать в общем случае в блок блокчейна кроме его идентификатора и хэш-кода, связывающего каждый новый блок с его предшественником.

СПИСОК ЛИТЕРАТУРЫ:

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System (31 октября 2008 г.). URL: https://nakamotoinstitute.org/literature/ (дата обращения: 14.01.2019).
2. Gartner. Top 10 Strategic Technology Trends for 2017: Blockchain and Distributed Ledgers (21 марта 2017 г.). URL: https://www.gartner.com/doc/3647619/top--strategic-technology-trends/ (дата обращения: 14.01.2019).
3. Distributed Ledger Technology: Beyond Block Chain (Report). UK Government, Office for Science (2016). URL: https://www.gov.uk/government/uploads/ system/uploads/attachment_data/ file/492972/gs-16-1-distributed-ledger-technology.pdf (дата обращения: 14.01.2019).
4. Making sense of bitcoin, cryptocurrency, and blockchain. PriceWaterhouseCoopers (2016). URL: https://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html (дата обращения: 14.01.2019).
5. Wilson S. How it works: Blockchain explained in 500 words. URL: http://www.zdnet.com/article/blockchain-explained-in-500-words/ (дата обращения: 14.01.2019).
6. Researching the potential of blockchains. URL: http://blockchain.open.ac.uk/ (дата обращения: 14.01.2019).
7. Nielson B. Blockchain Solutions for Cyber & Data Security. – URL: https://richtopia.com/emerging-technologies/blockchain-solutions-for-cyber-data-security (дата обращения: 14.01.2019).
8. Blockchain Security Controls. URL: https://github.com/Primechain/blockchain-security-controls/blob/master/A.%20Introduction.md (дата обращения: 14.01.2019).
9. Yaga, D., Mell, P., Roby, N., and Scarfone, K. 2018. Draft NISTIR 8202 Blockchain Technology Overview. URL: https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/ documents/nistir8202-draft.pdf (дата обращения: 14.01.2019).

10. Miloslavskaya N. Designing Blockchain-based SIEM 3.0 System. Information and Computer Security (UK). Emerald Publishing. September 2018. Vol. 26, issue 4. P. 491 – 512. DOI: 10.1108/ics-10-2017-0075.
11. ГОСТ Р ИСО/МЭК ТО 18044–2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». М.: Стандартинформ, 2009.
12. Cyber Observable eXpression (CybOX™) Archive Website. URL: https://cyboxproject.github.io/ (дата обращения: 14.01.2019).
13. Introduction to STIX. URL: https://oasis-open.github.io/cti-documentation/stix/intro (дата обращения: 14.01.2019).
14. Introduction to TAXII. URL: https://oasis-open.github.io/cti-documentation/taxii/intro (дата обращения: 14.01.2019).
15. Accenture. Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World. URL: https://www.accenture.com/t20160927T033514Z__w__/us-en/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf (дата обращения: 14.01.2019).
16. Cocheo S. A blockchain you can edit? 2016. URL: http://www.bankingexchange.com/technology-channel/item/6492-a-blockchain-you-can-edit (дата обращения: 14.01.2019).

REFERENCES:

[1] Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System (31 Oktober 2008). URL: https://nakamotoinstitute.org/literature/ (accessed 14.01.2019).
[2] Gartner. Top 10 Strategic Technology Trends for 2017: Blockchain and Distributed Ledgers (21 March 2017). URL: https://www.gartner.com/doc/3647619/top--strategic-technology-trends/ (accessed 14.01.2019).
[3] Distributed Ledger Technology: Beyond Block Chain (Report). UK Government, Office for Science (2016). URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (accessed 30.11.2018).
[4] Making sense of bitcoin, cryptocurrency, and blockchain. PriceWaterhouseCoopers (2016). URL: https://www.pwc.com/us/en/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html (access: 30.11.2018).
[5] Wilson S. How it works: Blockchain explained in 500 words. URL: http://www.zdnet.com/article/blockchain-explained-in-500-words/ (accessed 30.11.2018).
[6] Researching the potential of blockchains. URL: http://blockchain.open.ac.uk/ (access date: 30 November 2018).
[7] Nielson B. Blockchain Solutions for Cyber & Data Security. URL: https://richtopia.com/emerging-technologies/blockchain-solutions-for-cyber-data-security (accessed 30.11.2018).
[8] Blockchain Security Controls. URL: https://github.com/Primechain/blockchain-security-controls/blob/master/A.%20Introduction.md (accessed 30.11.2018).
[9] Yaga, D., Mell, P., Roby, N., and Scarfone, K. 2018. Draft NISTIR 8202 Blockchain Technology Overview. URL: https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/ documents/nistir8202-draft.pdf (accessed 30.11.2018).
[10] Miloslavskaya N. Designing Blockchain-based SIEM 3.0 System. Information and Computer Security (UK). Emerald Publishing. September 2018. Vol. 26, issue 4. P. 491 – 512. DOI: 10.1108/ics-10-2017-0075
[11] GOST R ISO/IEC TR 18044–2007 Information Technology. Security Techniques. Information Security Incident Management. M.: Standartinform, 2009.
[12] Cyber Observable eXpression (CybOX™) Archive Website. URL: https://cyboxproject.github.io/ (accessed 30.11.2018).
[13] Introduction to STIX. URL: https://oasis-open.github.io/cti-documentation/stix/intro (accessed 30.11.2018).
[14] Introduction to TAXII. URL: https://oasis-open.github.io/cti-documentation/taxii/intro (accessed 30.11.2018).
[15] Accenture. Editing the Uneditable Blockchain: Why Distributed Ledger Technology Must Adapt to an Imperfect World. URL: https://www.accenture.com/t20160927T033514Z__w__/us-en/_acnmedia/PDF-33/Accenture-Editing-Uneditable-Blockchain.pdf (accessed 30.11.2018).
[16] Cocheo S. A blockchain you can edit? 2016. URL: http://www.bankingexchange.com/technology-channel/item/6492-a-blockchain-you-can-edit (accessed 30.11.2018).

Поступила в редакцию – 26 ноября 2018 г. Окончательный вариант – 31 января 2019 г.
Received – November 26, 2018. The final version – January 31, 2019.