УДК 681.518

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТЕХНОЛОГИИ БЛОКЧЕЙН

Виталий Витальевич Течиев
аспирант
г. Владикавказ
Северо-Кавказский горно-металлургический институт (государственный технологический университет) (Владикавказ, Россия)

Борис Дзамболатович Хасцаев
д.т.н., профессор
bordsamchas@rambler.ru
г. Владикавказ
Северо-Кавказский горно-металлургический институт (государственный технологический университет) (Владикавказ, Россия)

Аннотация. Статья посвящена задаче организации защиты информации на примере информационных транзакций по технологии блокчейна, главная цель которой – сохранение в большой секретности всей информации о проводимых транзакциях, а также поддержание в целостности всего массива информационных данных и дополнения этого массива новой информацией. Решение задачи основано на применении базовой концептуальной модели блокчейна, включающей в себя данные в виде последовательности записей с возможностью дополнения и хранения их вместе с вспомогательной информацией в блоках. Блоки, в свою очередь, хранимы как односвязный список. Анализируются преимущества от использования блокчейна в решении задачи обеспечения безопасности информационных транзакций – это прозрачность проводимых транзакций и множественное копирование всех этих транзакций таким образом, чтобы у каждого пользователя всегда была информация о каждом шаге всех партнеров. Примечательно то, что при этом у всех разный уровень доступа к файлам. Все пользователи могут наблюдать за перемещением средств, но доступ к самим средствам будет только у пользователя с необходимыми правами. Это обеспечивает должный уровень открытости сделки – вся цепочка транзакций дублируется и хранится в неизменном зашифрованном виде у каждого пользователя.

Ключевые слова: блокчейн, blockchain, криптография, транзакции, децентрализованная база данных, хеширование, защита информации, хэш-сумма.

Введение

Известно, что блокчейн (blockchain) – это выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащих информацию. Чаще всего копии цепочек блоков хранятся и обрабатываются на множестве разных компьютеров. Также можно отметить, что блокчейн – это журнал с фактами, реплицируемый на несколько компьютеров, объединенных в сеть равноправных узлов. Фактами могут быть различные операции, от денежных операций и до подписания контента. Члены сети — анонимные лица, пользователи, называемые узлами. Все коммуникации внутри сети используют криптографию, чтобы надежно идентифицировать отправителя и получателя. При необходимости добавления факта в журнал в сети формируется консенсус, задающий место появления факта в журнале. При этом консенсус принято называть блоком [1-4] . Таким образом, блокчейн – это последовательный набор блоков, каждый следующий блок в котором включает в качестве хешируемой информации значение хеш-функции от предыдущего блока.

Блокчейн используется для организации журналов транзакций, при этом транзакцией может называться любой из банковских событий: финансовая транзакция (перевод между счетами), события аутентификации и авторизации и т. д.

Организация безопасности информационных транзакций путем использования технологии блокчейна

Одним из важных путей организации безопасности транзакций является направление, предусматривающее применение технологии блокчейна для поддержания целостности и сохранности общего массива данных и дополнения его информацией. Развитию и исследованию этого направления и посвящена предлагаемая статья.

Определим, что блок транзакций — специальная структура для записи группы транзакций в определенной системе. Транзакция считается завершённой и достоверной («подтверждённой»), когда проверены её формат и подписи, и когда сама транзакция объединена в группу с несколькими другими и записана в специальную структуру — блок. Фрагмент блока с транзакциями приведен на рис. 1.

.

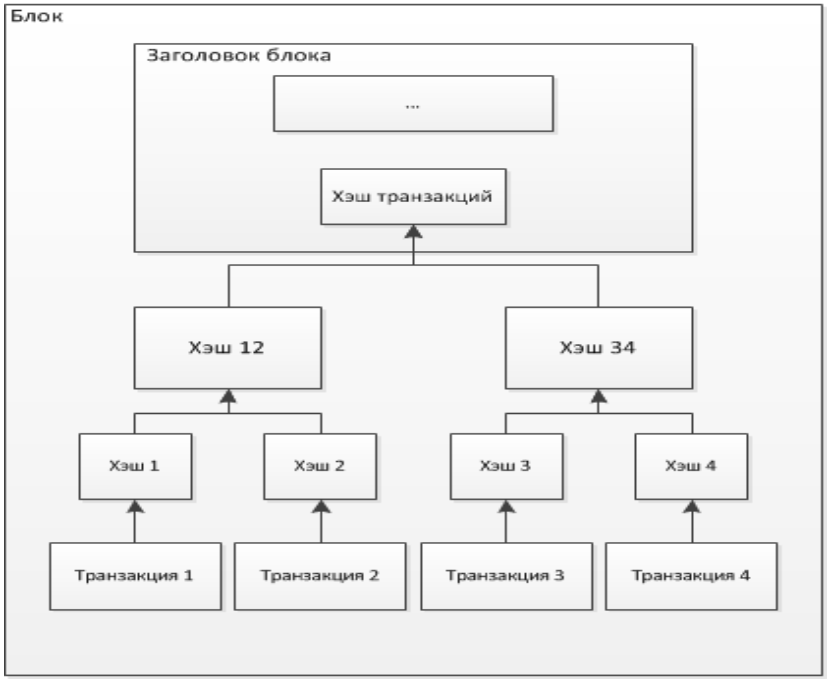

Рис. 1. Фрагмент блока с транзакциями

Содержимое блоков может быть проверено, так как каждый блок содержит информацию о предыдущем блоке. Все блоки выстроены в одну цепочку, которая содержит информацию обо всех совершённых когда-либо операциях в базе. Самый первый блок в цепочке — первичный блок. Он рассматривается как отдельный случай, так как у него отсутствует родительский блок. Блок состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой хэш, хэш предыдущего блока, хэши транзакций и дополнительную служебную информацию.

Если на основе технологий блокчейна организовать систему с обеспечением безопасности информационных транзакций путем использования технологии блокчейна, то такая система будет включать в себя три составляющих:

- источники событий (транзакций);
- источники блоков (в которых фиксируются транзакции);

- получатели (читатели) блоков и зафиксированных транзакций.

В зависимости от конкретной реализации системы, основанной на блокчейне, эти составляющие могут разными путями пересекаться, совмещая функции. Главное требование к журналам системы с обеспечением безопасности - неизменяемость: после добавления транзакции в журнал удаление или редактирование ее должны быть невозможными процессами. Но при этом возникают естественные вопросы, включая вопрос гарантии невозможности изменения информации внутри блока и вопрос гарантии невозможности перегенерирования с изменением информации в уже существующей цепочке блоков.

Ответ на первый вопрос – наличие в каждом блоке хэш-суммы от его содержимого и включение её же в следующий блок. Тогда, чтобы поменять что-то в блоке, не выдав это пользователям, нужно будет изменение сделать так, чтобы хэш-сумма от блока осталась прежней. Последнее невозможно выполнить, особенно, если механизм создания этого самого хэша криптографически стойкий, либо поменять в том числе и хэш-сумму блока. Тогда придётся менять и значение этой хэш-суммы в следующем блоке, что потребует изменений, в свою очередь, в хэш-сумме всего второго блока, а потом и в третьем, и так далее. Получается, что для того, чтобы поменять информацию в одном из блоков, нужно будет перегенерировать всю цепочку блоков, начиная с изменяемого. Для определения выполнимости этих процедур рассмотрим несколько вариантов реализации систем с базами данных.

Вариант 1. Централизованному блокчейну с доверенным центром поручается после определённого промежутка времени (или набора транзакций) формировать новый блок. Этот блок снабжается, кроме хэш-суммы, своей электронной подписью. Каждый клиент системы имеет возможность проверить, что все блоки в цепочке сгенерированы доверенным центром и никем иным и в предположениях, что доверенный центр не скомпрометирован и возможность модификации журнала злоумышленником отсутствует. Использовать технологию блокчейна в этом случае будет избыточной мерой. Достаточно будет обратиться к доверенному центру с целью подписания каждой транзакции, добавив к ней время и порядковый номер. Номер обеспечивает порядок и невозможность добавления (удаления) транзакций из цепочки, электронная подпись доверенного центра – невозможность модификации конкретных транзакций.

Вариант 2. При наличии централизованного блокчейна с недоверенным или с не полностью доверенным центром центру доверяется процедура фиксации транзакций в журнале при уверенности того, что выделенный центр не перегенерирует всю цепочку блоков, удалив из неё ненужные ему транзакции или добавив нужные. Для данного случая возможны следующие алгоритмы, предусматривающие:

- использование дополнительного доверенного хранилища. Оно предусматривает то, что после создания очередного блока отправку доверенным центром в доверенное и независимое от данного центра хранилище хэш-код от нового блока. Доверенное хранилище не должно принимать никаких изменений к хэш-кодам уже созданных блоков. В качестве такого хранилища можно использовать и децентрализованную базу данных системы, если таковая имеется. Размер хранимой информации может быть небольшим по сравнению с общим объёмом журнала;

- дополнение каждого блока меткой времени, сгенерированной доверенным центром временных меток. Такая метка должна содержать время генерации метки и электронную подпись центра, вычисленную на основании хеш-кода блока и времени метки. В случае, если «недоверенный» центр захочет перегенерировать часть цепочки блоков, будет наблюдаться разрыв в метках времени. Этот метод не гарантирует, что

«не совсем доверенный» центр не будет генерировать сразу две цепочки блоков, дополняя их корректными метками времени, а потом не подменит одну другой.

Вариант 3. При наличии децентрализованного блокчейна, при котором каждый участник может взять набор транзакций, ожидающих включения в журнал, и сформировать новый блок. В системах типа BitCoin такой участник ещё и получит премию в виде определённой суммы и/или комиссии от принятых в блок транзакций. Надёжность таких систем основывается на том, что новый блок нельзя сформировать быстрее, чем это задано системой. Для обеспечения безопасности система будет требовать введение информации, на введение которого в систему необходимо определенное время t. К примеру, зная суммарную вычислительную мощность блокчейн-сети, клиенты могут договориться о механизме изменения параметра t, о любом времени генерации нового корректного блока. Так, для обеспечения среднего времени генерации блока 10 минут сети Bitcoin параметр t пересчитывается каждые 2016 блоков. Такие время позволяет адаптировать сеть к изменению числа пользователей, их вычислительных мощностей, появлению новых механизмов вычисления хэш-функций. Кроме задания параметра t можно оперировать другими величинами, так или иначе относящимися к мощности вычислений. Они следующие.

- Hashrate — количество хэшей, которые считают за единицы времени конкретный майнер или сеть в целом. Например, в ноябре 2017 года общий hashrate для сети Bitcoin составлял примерно $7{,}7\times10^{18}$ хэшей в секунду.

- Difficulty — сложность поиска корректного блока, выражаемая как $d=d_{const}/t$, где d_{const} — некоторая константа сложности, а t — параметр-цель. В отличие от параметра t, который падает с ростом вычислительной мощности сети, d изменяется вместе с hashrate, что делает его более простым для восприятия и анализа человеком.

В случае, примерно одновременной генерации следующего блока двумя и более майнерами (когда информация о новом блоке публикуется вторым майнером до поступления к нему информации о новом блоке от первого) в направленной цепочке блоков происходит разветвление. Далее каждый из майнеров выбирает один из новых блоков (например – первый увиденный) и пытается сгенерировать новый блок на основе выбранного, продолжая «ответвление» в цепочке блоков. В итоге одна из двух таких цепочек становится длиннее (та, которую выбрало большее число майнеров), и именно она признаётся основной.

В случае нормального поведения системы на включение конкретных транзакций в блоки это влияет мало, так как каждый из добросовестных майнеров следует одному и тому же алгоритму включения транзакций в блок (например, в сети BitCoin – алгоритму максимизации комиссии за блок). Однако можно предположить, что какой-нибудь злоумышленник захочет «модерировать» распределённый блокчейн, включая или не включая в блоки транзакции по своему выбору. Предположим, что доля вычислительных ресурсов злоумышленника (направленных на генерацию нового блока) равна p ($0\% < p < 50\%$). В этом случае каждый следующий сгенерированный блок с вероятностью p будет сгенерирована мощностями злоумышленника. Это позволит ему включать в блоки те транзакции, которые другие майнеры включать не захотели.

Ситуация меняется, если мощности злоумышленника составляют больше половины от мощности сети. В этом случае, если после блока злоумышленника был с вероятностью $(1-p)$ сгенерирован «обычный» блок, злоумышленник его может просто проигнорировать и продолжать генерировать новые блоки, как будто он единственный майнер в сети. Тогда, если среднее время генерации одного блока всеми мощностями равно t, то за время T злоумышленник сможет сгенерировать $N_E=p*T/t$, а легальные

пользователи $N_L=(1–p)*T/t$ блоков, $N_E>N_L$. Даже, если с некоторой вероятностью легальные пользователи сгенерируют 2 блока быстрее, чем злоумышленник один, последний всё равно «догонит и перегонит» легальную цепочку примерно за время $t/(2p–1)$. Так как в блокчейне есть договоренность, что за текущее состояние сети принимается наиболее длинная цепочка, именно цепочка злоумышленника всегда будет восприниматься правильной, поэтому получается, что злоумышленник сможет по своему желанию включать или не включать транзакции в цепочки.

Возможны в реальности и другие варианты построения систем на основе блокчейна, наиболее интересной из которых является система с подходом «доказательство доли владения». Она используема в сетях Etherium и EmerCoin, в которых вероятность генерации блока пропорциональна количеству средств на счетах потенциальных создателей нового блока. Подход более эффективен, связывает ответственность за надёжность и корректность генерации новых блоков с размером капитала. С другой стороны, это даёт дополнительную мотивацию концентрировать больше капитала в одних руках, что может привести к централизации системы.

Рассмотренные примеры систем обеспечения безопасности информационных транзакций могут успешно применяться во многих сферах человеческой деятельности с целью автоматизации сохранности в секрете больших экономических информационных ресурсов.

Каждая из рассмотренных систем характеризуется и достоинствами и недостатками, фундаментальное исследование и анализ которых целесообразно привести в отдельной статье.

Заключение

Рассмотрено одно из важнейших направлений применения технологии блокчейна, которое связано с обеспечением безопасности информационных транзакций. Проанализировано несколько вариантов построения систем, способных с высокой надежностью выполнять функции обеспечения таинства информационных транзакций. Одновременно такие системы автоматизируют банковские операции, ускоряют платежи и денежные переводы, значительно снижая их стоимость. К примеру, системы на базе блокчейна в сети BitCoin позволяют, среди прочего, отправку практически мгновенных денежных переводов во все страны мира с мобильного телефона при комиссии не более 0,25% .

Список литературы

1. Свон М.Д. Блокчейн. Схема новой экономики. М.: Изд-во: Олимп-Бизнес, 2017.
2. Форк А.В. Bitcoin. Больше чем деньги. М.: Изд-во: Продюсерский центр, 2014.
3. Дон С.Е., Алекс В.Т. Революция блокчейн (BlockchainRevolution). М.; Изд-во: Эксмо, 2014.
4. Антонопулос А.В. Овладение Биткоином (MasteringBitcoin). М.: Изд-во O'Reilly Media, 2017.
5. Савельев И.Е. Технология blockchain и ее применение. М.: Изд-во: Синергия, 2016.

THE PROTECTION OF INFORMATION ON BLOCKCHAIN TECHNOLOGY

V.V. Techiev
graduate student
Vladikavkaz
The North Caucasian mining and metallurgical institute (state technological university) (Vladikavkaz, Russia)

B.D. Khastsaev
Dr. Sci. (Engineering), professor
bordsamchas@rambler.ru
Vladikavkaz
The North Caucasian mining and metallurgical institute (state technological university) (Vladikavkaz, Russia)

Abstract. The article is devoted to the problem of information security organization on the example of information transactions using blockchain technology, the main purpose of which is to preserve the secrecy of all information about the transactions, as well as to maintain the integrity of the entire array of information data and Supplement this array with new information. The solution of the problem is based on the application of the basic conceptual model of the blockchain, which includes data in the form of a sequence of records with the ability to Supplement and store them together with auxiliary information in blocks. Blocks, in turn, are stored as a single-linked list. The advantages of using blockchain in solving the problem of information transactions security are analyzed: transparency of transactions and multiple copying of all these transactions so that each user always has information about each step of all partners. It is remarkable that at the same time at all different level of access to files. All users can observe the movement of funds, but only the user with the necessary rights will have access to the tools themselves. This ensures a proper level of openness of the transaction – the entire chain of transactions is duplicated and stored in the same encrypted form for each user.

Keywords: blockchain, blockchain, cryptography, transactions, decentralized database, hashing, information protection, hash sum.

References

1. Svon M.D. (2017) Blokchei`n. Skhema novoi` e`konomiki [Blockchain. Scheme of new economy]. M.: Publishing house: Olympe-business.
2. Fork A.V. (2014) Bitcoin. Bol`she chem den`gi [Bitcoin. It is more than money]. M.: Publishing house: Production center.
3. Don S. E., Alex V.T. (2014) Revoliutciia blokchei`n [Revolution blockchain (BlockchainRevolution)]. M.: Publishing house: Eksmo.
4. Антонопулос A.V. (2017) Ovladenie Bitkoinom [Mastering Bitcoin (MasteringBitcoin)]. M.: O'Reilly Media publishing house.
5. Savelyev I.E. (2016) Tekhnologiia blockchain i ee primenenie [Blockchain technology and its application]. M.: Publishing house: Synergy.