Секция 4

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.056 DOI 10.17223/2226308X/14/26

О КОНФИДЕНЦИАЛЬНОСТИ ТРАНЗАКЦИЙ В ДЕЦЕНТРАЛИЗОВАННЫХ СИСТЕМАХ УЧЁТА ТОКЕНОВ

Л. Р. Ахметзянова, А. А. Бабуева, С. Н. Кяжин, В. А. Попов

Предлагается трёхуровневая модель функционирования децентрализованной системы, выделяется уровень, на котором выполняются протоколы формирования и валидации конфиденциальных транзакций. Приводится особенность обеспечения конфиденциальности транзакций в децентрализованных системах учёта токенов — потребность проверять выполнение различных условий для содержимого транзакций без получения доступа к нему. Выявляются классы неклассических (и нестандартизированных в России) криптографических механизмов, часто используемых в децентрализованных системах, в которых обеспечивается конфиденциальность транзакций. Показывается неуниверсальность существующих формальных определений таких систем, вследствие чего на текущий момент задача формализации свойства конфиденциальности транзакций в общем случае является открытой.

Ключевые слова: *децентрализованная система, конфиденциальность, токен, доказательство с нулевым разглашением, гомоморфное шифрование, обязательство, коллективная подпись, кольцевая подпись.*

Введение

Рассмотрим класс информационных систем с реестром, где под реестром понимается совокупность данных, структурированных и хранимых в целях их учёта, поиска, обработки и контроля [1]. Среди таких систем выделим те, для которых реестр представляет собой таблицу соответствия идентификаторов пользователей и цифровых объектов, удостоверяющих некоторые права этих пользователей. Такие цифровые объекты будем называть *токенами*, такие системы — *системами учета токенов*, изменения, предлагаемые к внесению в реестр (таблицу) — *транзакцией*.

Транзакция в системе учёта токенов может быть интерпретирована как выпуск, уничтожение или перевод токенов от одного пользователя к другому. Отметим, что токены могут быть взаимозаменяемыми (в таком случае можно учитывать не каждый токен в отдельности, а лишь их количество; если в системе обрабатывается несколько величин, принято говорить о типе токенов) или невзаимозаменяемыми. В качестве примера системы учёта токенов можно привести систему электронных платежей, где реестр представляет собой таблицу соответствия идентификаторов пользователей и цифровых объектов, удостоверяющих право требования денежных средств.

В соответствии с политиками (настройками) системы можно выделить следующие роли уполномоченных пользователей:

— регистратор — может вносить изменения в реестр;

— наблюдатель — может осуществлять чтение из реестра;
— валидатор — может подтверждать корректность транзакций.

Если в системе имеется единственный пользователь-валидатор, то при её использовании возникает *проблема доверия* к этому валидатору. Например, для упомянутой системы электронных платежей отправители и получатели денежных средств вынуждены доверять оператору электронной платёжной системы, который принимает решение о корректности предлагаемых изменений. В случае существования подобной проблемы доверия может быть целесообразным использование децентрализованной системы, в которой имеется несколько пользователей-валидаторов, которые совместно (согласно установленным алгоритмам) принимают решение о корректности транзакций. Тогда требование доверия перекладывается с одного уполномоченного пользователя на нескольких.

В общем случае для подтверждения корректности транзакций необходима проверка выполнения некоторых условий, зависящих от состояния реестра. Если в системе несколько пользователей-валидаторов, то у каждого из них может быть своя версия состояния реестра, для которой они проверяют выполнение соответствующих условий. Таким образом, возникает потребность использования распределённого реестра, т. е. реестра, который физически распределён между уполномоченными пользователями, и обеспечения при этом согласованности его состояния.

В настоящей работе предлагается выявить особенности обеспечения конфиденциальности транзакций в децентрализованных системах учёта токенов.

1. О систематизации свойств децентрализованных систем

Децентрализованные системы представляют собой распределённый программно-технический комплекс, внутри которого функционирует большое количество различных протоколов. Сложность таких систем приводит к тому, что задача их синтеза и анализа также становится крайне трудоёмкой. Для упрощения этой задачи целесообразно строить модели функционирования децентрализованных систем, позволяющие разделять сложную систему на отдельные блоки и анализировать части системы независимо, т. е. проводить так называемый модульный анализ. По этой же причине важна систематизация свойств, выполнение которых требуется от каждой отдельной части системы.

В литературе наиболее глубокие модели децентрализованных систем предложены в работах [2, 3], однако с точки зрения особенностей обеспечения конфиденциальности транзакций, на наш взгляд, они обладают избыточной детализацией. В настоящей работе предлагается следующая **трёхуровневая модель функционирования децентрализованной системы**:

— нижний уровень (уровень консенсуса);
— средний уровень (уровень транзакций);
— верхний уровень (уровень приложений).

Нижний уровень оперирует с реестром как с целостным объектом (набором данных, структура которого не имеет значения). Цель протоколов, функционирующих на нижнем уровне, — обеспечить согласованность состояния реестра между несколькими уполномоченными пользователями. На нижнем уровне выполняются протоколы достижения консенсуса.

Средний уровень определяет структуру реестра и, как следствие, структуру транзакции. На среднем уровне выполняются:

— протокол формирования транзакции (выполняется независимо от состояния реестра, часто используется термин «оффчейн»);
— алгоритм валидации транзакции (выполняется пользователем-валидатором локально с использванием имеющейся у него версии состояния реестра).

На **верхнем уровне** выполняются протоколы решения конкретных бизнес-задач, которые интерпретируют транзакции.

Таким образом, ограничение на класс систем, указанное во введении (системы учёта токенов), реализуется на среднем уровне.

Уровни взаимодействуют между собой следующим образом:

— выполняется протокол верхнего уровня, действия пользователей приводят к формированию входных данных для транзакции;
— на среднем уровне выполняется протокол формирования транзакции, а также алгоритм валидации транзакции, принимающий на вход транзакцию и состояние реестра, в результате формируется предлагаемое новое состояние реестра; транзакция является входными данными для протокола достижения консенсуса;
— на нижнем уровне выполняется протокол достижения консенсуса, в результате чего обновляется состояние реестра.

При этом подразумевается выполнение свойства инкапсуляции:

— обеспечение свойств системы на более низком уровне не зависит от обеспечения свойств на более высоких уровнях;
— обеспечение свойств системы на более низком уровне необходимо для обеспечения свойств на более высоких уровнях.

Стоит отметить, что при исследовании систем свойства протоколов одного уровня могут рассматриваться независимо от свойств протоколов другого.

Свойства протоколов верхнего уровня определяются бизнес-задачей, поэтому их можно рассматривать только для конкретных классов систем, решающих одинаковую задачу. На нижнем уровне существует множество протоколов достижения консенсуса (см., например, методические рекомендации [1] и обзорную работу [4]). Несмотря на различие этих протоколов, в [5] сформулированы единые (универсальные) свойства протоколов нижнего уровня: consistency, future self consistency, μ-chain quality, g-chain growth.

Для протоколов среднего уровня на текущий момент нет ни общего определения, ни строго определённых свойств безопасности. В литературе представлено большое количество самых разных протоколов, которые изначально разрабатывались под конкретные бизнес-задачи, накладывающие свои ограничения на вид этих протоколов и требуемые свойства.

Для класса систем с токенами можно выделить общие свойства корректности функционирования системы — **невозможность неполномочного выпуска, уничтожения и перевода токенов**. Для рассмотренного примера платежей это свойство можно интерпретировать как невозможность передать денежные средства, принадлежащие другому пользователю, а также создать или уничтожить их, не имея соответствующих полномочий. Существуют также свойства, которые не связаны напрямую с корректным функционированием системы. Например, может возникнуть потребность в обеспечении следующих свойств:

— конфиденциальность транзакции (содержимое транзакции неизвестно для пользователей-наблюдателей и пользователей-валидаторов, кроме тех, чьи идентификаторы входят в содержимое данной транзакции);

— анонимность участников (сторонний наблюдатель не может сопоставить участников протокола формирования транзакции и реальных пользователей системы).

Данные свойства могут быть связаны друг с другом. Для примера платежей содержимое транзакции может быть интерпретировано как «отправители», «получатели» и «суммы переводов». При этом пользователи, интерпретируемые как отправители и получатели, могут самостоятельно формировать транзакцию, то есть быть участниками протокола формирования транзакции. В таком случае, если будет обеспечено свойство анонимности участников, но не будет обеспечена конфиденциальность транзакций, то информация об отправителях и получателях из транзакции может быть полезной для злоумышленника с точки зрения нарушения анонимности участников.

Обеспечение свойства конфиденциальности транзакций в децентрализованных системах имеет следующую отличительную особенность. Поскольку для выполнения алгоритма валидации транзакции пользователям-валидаторам, как правило, необходимо знать о её содержимом, но при этом среди валидаторов могут присутствовать такие, которым, согласно свойству конфиденциальности, должны быть неизвестны указанные данные, то возникает потребность проверять выполнение различных условий для содержимого транзакций без получения доступа к нему.

Свойство анонимности участников представляет меньший интерес, поскольку протокол формирования транзакции выполняется «оффчейн» и никаких особенностей обеспечения данного свойства в случае децентрализованных систем не имеется.

2. О криптографических механизмах обеспечения конфиденциальности транзакций

Поскольку обеспечение конфиденциальности транзакций напрямую связано с изменениями алгоритма валидации транзакции, то свойство конфиденциальности транзакций нельзя рассматривать независимо от свойств невозможности неполномочного выпуска, уничтожения и перевода токенов. В связи с этим необходимо рассматривать не механизмы обеспечения конфиденциальности транзакций в отдельности, а системы, в которых обеспечивается конфиденциальность транзакций в целом.

Существует достаточно много систем, в которых конфиденциальность транзакций обеспечивается с помощью криптографических механизмов (например, zCash [6, 7], CryptoNote [8], RingCT [9], AZTEC [10], MW [11, 12], Zether [13], патент Alibaba [14]). Некоторые системы, кроме криптографических механизмов, используют доверенную вычислительную среду (например, Ekiden [15], HLF Private Chaincode [16]).

Несмотря на то, что данные системы необходимо анализировать как единое целое, в процессе исследования (как в рамках анализа, так и в рамках синтеза) систем возникает естественное желание декомпозировать системы на отдельные криптографические механизмы. В результате обзора систем удалось выявить следующие наиболее часто используемые классы неклассических криптографических механизмов:

— схема гомоморфного шифрования (в [13, 14] используется для сокрытия количества токенов);
— схема обязательства/commitment (в [6, 7, 9, 10, 11, 14] используется для сокрытия количества токенов);
— схема кольцевой подписи (в [8, 9] используется для «перемешивания» идентификаторов пользователей или токенов);
— протокол доказательства с нулевым разглашением (в [6, 7, 9, 10, 11, 13, 14] используется для валидации транзакции без доступа к ее содержимому);

— схема агрегируемой/коллективной подписи (в [11] является вспомогательным механизмом, позволяющим упростить использование других механизмов).

При этом стоит сделать замечания:

— указанный список не является полным, другие примеры систем могут использовать другие криптографические механизмы;
— использование перечисленных механизмов в системах, обеспечивающих конфиденциальность транзакций, косвенно подтверждает недостаточность использования классических криптографических механизмов (стандартизированных в РФ).

3. О формализации свойств децентрализованных систем

В связи со сложностью систем, в которых обеспечивается конфиденциальность транзакций, применение только методов криптоанализа, основанных на поиске методов взлома и обычно применяемых к базовым примитивам, становится недостаточным. В случае высокоуровневых протоколов, включающих в себя множество базовых криптографических механизмов, критичные уязвимости могут возникать не в базовых механизмах, а в порядке их использования.

В зарубежной литературе для анализа криптографических протоколов используются методы криптоанализа, основанные на теоретико-сложностных сведениях (парадигмы game-based [17], UC [18]) или применении автоматизированных средств формальной верификации [19]. Эти методы предполагают первоначальную разработку и формализацию моделей противника, включающих в себя описание угроз, возможностей противника и его ресурсов. Разработка релевантных моделей противника, наиболее полно с точки зрения практики отражающих аспекты свойств безопасности и возможностей противника, является одной из центральных задач данной области.

На текущий момент не существует устоявшегося формального определения системы, в которой обеспечивается конфиденциальность транзакций, и, следовательно, соответствующих общих формальных моделей противника для них. В литературе представлено много различных определений систем и моделей противника (например, [7, 12, 20, 21]), которые по-разному формализуют одни и те же свойства безопасности. Данное обстоятельство, а именно отсутствие единой системы оценивания криптографических качеств протоколов, приводит к снижению качества криптоанализа и увеличению риска появления уязвимостей в реальных системах.

Например, согласно [12], децентрализованная система учёта взаимозаменяемых токенов, в которой обеспечивается конфиденциальность транзакций, определяется следующими алгоритмами:

— Setup — алгоритм генерации общедоступных параметров системы, необходимых для её функционирования, и инициализации реестра;
— Mint — алгоритм формирования конфиденциальной транзакции выпуска токенов;
— Send, Rcv — алгоритмы формирования конфиденциальной транзакции перевода токенов (первый алгоритм выполняется отправителем, второй — получателем);
— Ldgr — алгоритм обновления состояния реестра, включающий в себя механизмы валидации транзакции.

В данном определении авторы разделили протокол формирования конфиденциальной транзакции на алгоритмы Send, Rcv. В общем случае это не всегда возможно — процесс формирования транзакции перевода зачастую предполагает выполнение протокола (может быть, интерактивного) между получателем и отправителем. Таким образом, приведённое определение не является общим и не позволяет явно разделить

систему на модули (подпротоколы) для анализа релевантности моделей противника и проведения теоретико-сложностных оценок. Итак, считаем необходимым сформировать универсальные строгие определения систем (возможно, отдельно для разных классов систем).

В работе [12] даются также формальные определения свойств невозможности неполномочного выпуска токенов, невозможности неполномочного перевода токенов и конфиденциальности количества токенов, участвующих в транзакции, и доказывается, что система MW удовлетворяет им. Однако поскольку определения свойств связаны с формальным определением системы, они также не являются общими.

Заключение

В работе показана актуальность задачи разработки децентрализованных систем учёта токенов, в которых обеспечивается конфиденциальность транзакций, несмотря на существование примеров таких систем.

Первоначальным этапом при решении этой задачи видится систематизация моделей противника, предложенных в [7, 12, 20, 21], путём выявления соотношений между ними, а именно: осмысление формально определяемых угроз и типов атак и определение того, какие модели являются более сильными, более слабыми или вообще несоотносимыми друг с другом (так как учитывают различные свойства безопасности). В силу того, что рассматриваемые системы и предложенные для них модели являются достаточно новыми и, как следствие, малоизученными, не менее важным представляется этап анализа моделей на предмет их релевантности и достаточности с точки зрения целевых свойств безопасности и при необходимости их дальнейшая доработка, например, путём расширения рассматриваемых типов атак.

После разработки релевантной модели противника необходимо проанализировать системы, предложенные в [6 – 16], на предмет выполнения свойств безопасности, соответствующих модели. Если среди перечисленных систем не окажется той, для которой выполняются данные свойства, то в качестве следующего этапа необходимо доработать эти системы, например, путем замены используемых криптографических механизмов на более эффективные/стойкие (при необходимости — разработать такие механизмы).

Например, предположим, что протокол MW является стойким в релевантной модели противника при условии использования стойких криптографических механизмов. В таком случае может потребоваться его адаптация к исследованным российским криптографическим алгоритмам. Так, в частности, актуальной становится задача разработки схемы агрегируемой/коллективной подписи на основе стандартизированной в РФ схемы подписи [22] (попытка построения такой схемы сделана в [23]) и анализ её стойкости в модели EUF-CMA.

ЛИТЕРАТУРА

1. Методические рекомендации ТК 26 МР 26.4.001-2018 «Информационная технология. Криптографическая защита информации. Термины и определения в области технологий цепной записи данных (блокчейн) и распределенных реестров». М.: Технический комитет по стандартизации «Криптографическая защита информации», 2018.
2. *Zhang R., Xue R., and Liu L.* Security and privacy on blockchain // ACM Computing Surveys. 2019. V. 52. No. 3. Art. 51. 34 p.
3. *Sai A. R., Buckley J., Fitzgerald B., and Le Gear A.* Taxonomy of Centralization in Public Blockchain Systems: A Systematic Literature Review. 2020. `https://arxiv.org/pdf/2009.12542.pdf`

4. *Nijsse J. and Litchfield A.* A taxonomy of blockchain consensus methods // Cryptography. 2020. V. 4. No. 4. Art. 32. 15 p.
5. *Pass R., Seeman L., and Shelat A.* Analysis of the blockchain protocol in asynchronous networks // EUROCRYPT 2017. Springer, 2017. P. 643–673.
6. Zcash Protocol Specification. 2021. `https://github.com/zcash/zips/blob/master/protocol/protocol.pdf`
7. *Ben Sasson E., Chiesa A., Garman C., et al.* Zerocash: Decentralized anonymous payments from bitcoin // IEEE Symp. Security Privacy. San Jose, CA, 2014. P. 459–474.
8. CryptoNote v 2.0. 2013. `https://cryptonote.org/whitepaper.pdf`
9. *Yuen T. H., Sun S.-F., Liu J. K., et al.* RingCT 3.0 for blockchain confidential transaction: Shorter size and stronger security // LNCS. 2020. V. 12059. P. 464–483.
10. AZTEC Protocol. 2018. `https://github.com/AztecProtocol/AZTEC/blob/master/AZTEC.pdf`
11. *Poelstra A.* Mimblewimble. 2016. `https://download.wpsoftware.net/bitcoin/wizardry/mimble-wimble.pdf`
12. *Fuchsbauer G., Orru M., and Seurin Y.* Aggregate cash systems: a cryptographic investigation of Mimblewimble // LNCS. 2019. V. 11476. P. 657–689.
13. *Bunz B., Agrawal S., Zamani M., and Boneh D.* Zether: Towards privacy in a smart contract world // LNCS. 2020. V. 12059. P. 423–443.
14. *Zhang W. and Ma B.* Blockchain Data Protection using Homomorphic Encryption. US Patent 2019/0253235 A1.
15. *Cheng R., Zhang F., Kos J., et al.* Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts // IEEE Europ. Symp. Security Privacy. 2019. P. 185–200.
16. *Brandenburger M., Cachin C., Kapitza R., and Sorniotti A.* Blockchain and trusted computing: Problems, pitfalls, and a solution for Hyperledger Fabric. 2018. `https://arxiv.org/pdf/1805.08541.pdf`
17. *Hevia A.* Introduction to Provable Security. Advanced Crypto School, Florianopolis, 2013.
18. *Canetti R.* Universally composable security: a new paradigm for cryptographic protocols // 42nd IEEE Symp. Found. Comput. Sci. IEEE, 2001. P. 136–145.
19. *Cremers C. and Mauw S.* Operational Semantics and Verification of Security Protocols. Springer Verlag, 2012. 174 p.
20. *Guan Z., Wan Z., Yang Y., et al.* BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs // IEEE Trans. Dependable Secure Comput. IEEE, 2020. `https://eprint.iacr.org/2019/1354.pdf`.
21. *Mitani T. and Otsuka A.* Confidential and auditable payments // LNCS. 2020. V. 12063. P. 466–480.
22. Межгосударственный стандарт ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи». М.: Стандартинформ, 2018.
23. *Молдовян Н. А.* Теоретический минимум и алгоритмы цифровой подписи. СПб.: БХВ-Петербург, 2010. 304 с.