

БЕЗОПАСНОЕ МАСШТАБИРОВАНИЕ ЭЛЕКТРОННЫХ БУХГАЛТЕРСКИХ КНИГ НА ОСНОВЕ ТАНГЛА*

*А. А. Грушо*¹, *А. А. Зацаринный*², *Е. Е. Тимонина*³

Аннотация: Рассматривается электронная бухгалтерская книга (ЭБК), основанная на концепции блокчейна. Развитием традиционного блокчейна стал тангл (tangle), который представляется ориентированным ациклическим графом (DAG — Directed Acyclic Graph) и который безопасно хранит информацию о транзакциях. Централизованный консенсус предполагает концентрацию функций контроля в едином органе. Масштабирование ЭБК в ряде случаев порождает угрозы коррупции и мошенничества. Рассматриваются три типа угроз, которые определяются коррупцией и сговором юридических лиц. Обеспечение информационной безопасности при масштабировании ЭБК — это направление, которое начинает развиваться в связи с ростом цифровой экономики.

Ключевые слова: информационная безопасность; тангл; блокчейн; угрозы коррупции и мошенничества

DOI: 10.14357/08696527210305

1 Введение

Электронная бухгалтерская книга основана на концепции блокчейна [1, 2]. Управление записями в блокчейне определяется консенсусом [3]. Все консенсусы можно разделить на централизованные и децентрализованные. С технической точки зрения централизованные и децентрализованные консенсусы схожи, так как каждый узел сети индивидуально ответствен за безопасность и хранение совместных используемых для ЭБК данных. Централизованный консенсус предполагает концентрацию функций контроля в едином органе. Это означает, что имеется единый контактный узел формирования и хранения блокчейнов.

Развитием традиционных блокчейнов стал тангл [4], который представляется ориентированным ациклическим графом (DAG) и который безопасно хранит информацию о транзакциях. Вершины (узлы) в DAG — это транзакции. Сеть тангла состоит из вершин, которые являются сущностями, отражающими транз-

* Работа частично поддержана РФФИ (проект 18-29-03124-мк).

¹Федеральный исследовательский центр «Информатика и управление» Российской академии наук, grusho@yandex.ru

²Федеральный исследовательский центр «Информатика и управление» Российской академии наук, AZatsarinny@ipiran.ru

³Федеральный исследовательский центр «Информатика и управление» Российской академии наук, eltimon@yandex.ru

акции и обеспечивающими валидацию транзакций с помощью ориентированных дуг.

Основная идея тангла состоит в том, что пользователи при регистрации транзакции как узла тангла должны провести определенную работу для «одобрения» других ранее определенных транзакций. Таким образом, каждый пользователь, создающий транзакцию, вносит вклад в безопасность сети. Узлы проверяют, чтобы «одобренные» транзакции были неконфликтными. Если узел выясняет, что транзакция конфликтует с историей в тангле, то этот узел не «одобрит» конфликтную транзакцию.

Для создания транзакций узел выполняет следующие действия:

- (1) выбирает две или более транзакций для «одобрения»;
- (2) проверяет непротиворечивость выбранных для «одобрения» транзакций;
- (3) использует криптографические методы для формирования специальных, сложно вычислимых данных из «одобренных» транзакций и собственной информации.

Первые транзакции в тангле называются генезисом. Все транзакции в тангле прямо или косвенно одобряют генезис.

Основой обеспечения юридической значимости электронного взаимодействия участников экономической деятельности служат договоры (соглашения, контракты), которые содержат три параметра:

- (1) задачу, которую надлежит решить;
- (2) цену решения задачи, которую надлежит решить;
- (3) время, за которое надлежит решить задачу.

Договор, как правило, связывает двух участников: заказчика и исполнителя. Это отношение можно отражать на отдельном графе в виде ориентированной дуги, на которой ставится метка в виде вектора из значений трех указанных параметров.

Результаты выполнения договоров также отражаются в тангле в форме транзакций. При выполнении договоров в транзакциях отражаются акты о решении задачи, документы на оплату выполненных работ или на предоставление авансовых платежей. Эти данные также можно отображать в виде другого ориентированного графа. Таким образом, электронное взаимодействие участников экономической деятельности цифровой экономики должно обеспечивать дистанционное заключение договора и юридическое подтверждение информации о выполнении или невыполнении договора.

Идея ЭБК состоит в том, что каждый субъект экономической деятельности обладает танглом, хранящимся у него и в узле, реализующем централизованный консенсус. В этом тангле фиксируются все договорные обязательства и результаты их выполнения. Основная идея бухгалтерской книги [5] состоит в двойной записи, которая отражена в главной бухгалтерской книге. В ЭБК каждая

транзакция должна найти отражение по крайней мере в двух танглах, которые принадлежат взаимодействующим участникам экономической деятельности. В этом состоит непротиворечивость транзакции, которая проверяется на узле, реализующем централизованный консенсус.

В рамках одной ЭБК вопросы взаимодействий и безопасности рассмотрены в работе [6].

2 Масштабирование электронной бухгалтерской книги

Масштабируемость ЭБК подразумевает взаимодействие нескольких ЭБК. В связи с этим рассмотрим новый вид консенсуса, который назовем сложным централизованным консенсусом (СЦК). Сложный централизованный консенсус предполагает взаимодействие нескольких ЭБК, каждая из которых организована на базе своего централизованного консенсуса.

Основная идея СЦК состоит в построении иерархии ЭБК. Предположим, что должен быть выполнен большой проект, создаваемый на основании нормативного акта (НА) и обеспечивающий выполнение проекта финансирования, которое определяется финансовым документом (ФД). Реализация проекта предполагает начальное участие организаций O_1, \dots, O_k , каждая из которых связана со своей ЭБК. Тогда можно создать новый тангл, генезис которого состоит из двух вершин НА и ФД, юридическая значимость которых может быть оформлена соответствующими документами и подписями. Этот тангл можно назвать коренным для проекта. Аналогично каждая ЭБК может создать коренные танглы в своих ЭБК, в которых генезисы будут определяться договорами об участии в проекте между коренным танглом проекта и коренными танглами организаций и соответствующими ФД. Вообще договор между коренным танглом проекта и танглом организации можно сразу создавать на основе уже сделанных ранее проектов организаций, хотя они относятся к разным ЭБК. Наличие общего удостоверяющего центра электронных подписей позволяет это сделать. Основная проблема состоит в обеспечении безопасности (контроля) при взаимодействии различных ЭБК при выполнении проекта.

В работе рассматривается ряд угроз, которые представляются существенными при реализации любого крупного проекта, и исследуется проблема мониторинга с целью выявления признаков реализации этих угроз. Исследование ограничено угрозами, связанными с организацией договорных отношений и финансирования этих отношений. Вопросы выполнения договорных отношений в этой статье не рассматриваются.

3 Угрозы безопасности при масштабировании электронной бухгалтерской книги

Рассматриваются три типа угроз, которые определяются коррупцией и сговором юридических лиц.

Первый класс угроз будем называть циклами. Пусть организация O_1 получила подряд на выполнение одной из задач T проекта с объемом финансирования F . В ходе организации субподрядных работ несколько юридических лиц O_2, \dots, O_k могут договориться о последовательном выполнении задачи T . Каждая из организаций O_2, \dots, O_k получает долю финансирования $\alpha_2 F, \dots, \alpha_k F$, где $\alpha_2 + \dots + \alpha_k = \alpha < 1$. При этом субподрядчики O_2, \dots, O_k не могут и не собирались решать задачу целиком, но договорились (за исключением некоторого процента от F) нелегально передать деньги O_1 , заключив договор между O_k и O_1 на решение исходной задачи T за объем финансирования $(1 - \alpha)F$. Получился цикл, в котором одну и ту же задачу T предлагается решать за различные деньги одной и той же организации O_1 . Этот цикл позволяет перераспределять или обналичивать средства, выделенные на проект. Сюда также входит схема отмывания денег с помощью фирм-однодневок.

Второй класс угроз будем называть коррупцией. Пусть организация O должна организовать решение задачи с трудоемкостью T и с объемом финансирования F , кратко (T, F) . Для решения задачи привлекаются две организации O_1 и O_2 . С первой организацией O_1 есть договоренность об «откате». Тогда распределение работы и финансирования можно организовать следующим образом:

- O_1 получает договор $(T/10, 9F/10)$;
- O_2 получает договор $(9T/10, F/10)$.

Третий класс угроз состоит в существовании первопричины задержки выполнения проекта хотя бы одним из критических узлов реализации проекта, которая позволит увеличить финансирование, требуемое на покрытие останова во время задержки.

Для выявления реализации этих угроз необходимо определить, как и какую информацию надо собирать и где ее обрабатывать. Кроме того, необходимо определить вспомогательную информацию для анализа данных мониторинга.

4 Вспомогательные данные для анализа данных мониторинга выполнения проекта

Пусть организация, обеспечивающая условия функционирования коренного тангла, является центром мониторинга безопасности реализации проекта. Для сбора, хранения и анализа данных мониторинга безопасности должен существовать вычислительный центр проекта (ВЦП), где в базах данных хранятся следующие вспомогательные данные.

1. При подготовке к реализации проекта должна быть разработана номенклатура задач, которые необходимо решить при реализации проекта, а именно: по каждой соответствующей задаче должны быть хотя бы ориентировочно указаны:

- разработка/цена/время;
 - готовое изделие/цена/время;
 - возможность совместимости/цена/время достижения совместимости.
2. Описание проекта:
- структурная модель;
 - разбиение на подсистемы;
 - цены/сроки/тестирование результатов.
3. Обновляемая база данных договорных отношений участников проекта (независимо от ЭБК), т. е. совокупность дуг между участниками договорных отношений с метками (задача/цена/время). Сообщения о закрытии договора при его выполнении. Эти данные обновляются и передаются в центр мониторинга организациями, поддерживающими централизованные консенсусы каждой ЭБК. При этом сами танглы экономических субъектов или их фрагменты не передаются, кроме как по отдельным запросам.
4. Средства интеллектуального анализа данных (ИАД).

Далее показано, что этих данных достаточно для выявления признаков реализации указанных выше угроз. Рассмотрим методы выявления признаков угроз.

5 Методы анализа безопасности при масштабировании электронной бухгалтерской книги

Рассмотрим методы выявления циклов. В поступающих данных обновлений договоров можно выявлять факты, когда субъект O заключает договор (исходящая дуга) и субъект O позже (сравнение меток времени) становится исполнителем (входящая дуга). Данный факт может считаться признаком возможного цикла. Тогда выделяются дуги, по которым можно построить ориентированные пути, исходящие из O , и ориентированные пути, входящие в O . Существование хотя бы одного пересечения на множествах этих путей означает существование цикла. Более того, построение всех циклов позволяет выявить все группы сговора с O . Детальный анализ меток на этих циклах позволит восстановить схему и причины образования циклов.

Рассмотрим методы выявления схем коррупции. Для каждой вершины, из которой выходят несколько договорных дуг, необходимо провести сравнение меток этих дуг. С этой целью надо использовать базу данных номенклатуры решаемых задач проекта. Если комплексная задача внесена в эту базу, то должно существовать разбиение этой задачи на подзадачи, иначе зачем нужны несколько субподрядчиков? Тогда подзадачи также должны присутствовать в номенклатуре задач проекта, для этого надо смотреть структурное описание проекта. Для

каждой задачи, по условию, есть данные о ее формулировке и ориентировочной цене. Это дает возможность сравнивать условия договоров субподрядчиков по сложности стоящих задач и цене за решение этих задач. Отсюда сразу можно увидеть следы коррупции. Если описания подзадач отсутствуют, то единственный способ их создать — это квалифицированная экспертиза. К сожалению, схем коррупции, подобной описанной, может быть много, но базовая основа у большинства таких схем одинаковая. Это позволяет априори создавать вспомогательные данные для выявления подобных схем.

Рассмотрим третий класс угроз, связанный с повышением цены проекта за счет задержек в решении отдельных задач. Проблема состоит в том, что существуют несколько способов прятать первопричину задержек и объяснять все «объективными» обстоятельствами. Самый простой способ состоит в формировании условий, когда отсутствует ответственность за порождение задержки. Пусть субъект O должен решить сложную задачу $T = (T_1, T_2)$, в которой T_1 состоит в создании софта для обработки данных в задаче T_2 . Субъект O , заинтересованный в создании задержки, распределяет задачи между субъектами O_1 и O_2 . Созданный софт тестируется в O_1 и показывает хорошие результаты. Однако в O_2 этот софт не работает. Выявление причин отказа работы софта и необходимые работы по модернизации порождают требуемую для O задержку. При этом O не несет ответственности за задержку, так как не участвует в разработке софта и его применении. Субъект O_1 отказывается нести ответственность, так как у него софт хорошо работает. Субъект O_2 отказывается нести ответственность за задержку потому, что софт создавал не он. В данном простейшем случае первопричину легко найти. Она состоит в том, что O некорректно поставил задачу и не организовал взаимодействие между O_1 и O_2 . Некорректность постановки задачи состоит в том, что в условии задачи T_1 должно присутствовать условие о необходимости использовать функционал софта в задаче T_2 , которая будет решаться в O_2 . Для этого тестирование софта должно вестись не только в O_1 , но также одновременно и в O_2 .

Рассмотрим, как можно выявить первопричину задержки на ВЦП. В рассматриваемом простейшем случае задержка проекта определяется невозможностью O решить сложную задачу T , но ответственность за задержку O не берет. Тогда по запросу ВЦП организации, реализующие централизованные консенсусы и имеющие копии танглов O , O_1 и O_2 , делают копии договоров и высылают ВЦП. Если ни в одном договоре не упоминается задача адаптации софта для решения задачи T_2 в O_2 , то ответственность за задержку ложится на O . Если O_1 проигнорировал требование адаптации в O_2 , то ответственность ложится на O_1 . Если O_2 декларирует неработоспособность софта, но O_1 показывает положительные результаты тестирования софта в O_2 , то ответственность за задержку ложится на O_2 . Идентификация ответственности влечет большие потери для ответственного за задержку (штраф, компенсация ущерба и т. д.). Тогда все звенья реализации проекта становятся заинтересованными в недопущении задержек выполнения проекта.

Рассмотренные простейшие примеры реализации угроз не исчерпывают всего многообразия конкретных сценариев реализации рассматриваемых угроз. Однако видно, что потенциальный доступ к танглам и имеющиеся вспомогательные данные в главном тангле позволяют эффективно вести анализ появления признаков реализации угроз. Наиболее часто встречается коррупция. Выявление коррупции не дает достаточной информации для выявления причин коррупции и заинтересованных лиц. Поэтому в работе рассмотрены задачи только мониторинга реализации проекта. Также не рассмотрены задачи поиска первопричин неявных сбоев [7–9], порождающих задержки. Такие сбои могут порождаться не только заинтересованными исполнителями проекта, но также наличием вредоносного кода в импортных программах [10] или даже скрытыми дверями (Backdoors), известными только противнику [11]. Например, при наступлении определенных событий возможен сброс конфигурационных параметров, используемых для согласованной работы различных приложений [12].

6 Заключение

Результаты, полученные в статье, являются развитием серии работ авторов [2, 6], посвященных построению ЭБК на базе централизованных консенсусов и танглов применительно к современным проблемам цифровой трансформации. Так, ЭБК на основе танглов служит, по существу, примером одного из возможных подходов к реализации цифровой экономики.

Показано, что обеспечение информационной безопасности при масштабировании ЭБК становится новым направлением, обусловленным интенсивным развитием цифровой экономики. При этом существенную роль играют блокчейн-технологии и их различные модификации.

В рамках масштабируемости ЭБК, состоящей во взаимодействии нескольких ЭБК, объективно возникает новый вид консенсуса, определенный как СЦК. Основная идея СЦК состоит в построении иерархии ЭБК.

Масштабирование ЭБК порождает в ряде случаев угрозы коррупции и мошенничества. Предложена классификация угроз выполнения крупных проектов, обусловленных коррупцией и сговором юридических лиц. Определены и формализованы три типа угроз.

Предложены методы анализа безопасности при масштабировании ЭБК применительно к трем типам угроз. Приведены простейшие примеры реализации угроз.

Литература

1. *Лелу Л.* Блокчейн от А до Я. Все о технологии десятилетия / Пер. с фр. — М.: Эксмо, 2018. 190 с. (*Leloup L.* Blockchain: La revolution de la confiance. Paris: Groupe Eyrolles, 2017. 160 p.)

2. Грушо А. А., Зацаринный А. А., Тимонина Е. Е. Электронная бухгалтерская книга на базе ситуационных центров для цифровой экономики // Системы и средства информатики, 2019. Т. 29. № 2. С. 4–11.
3. Wahab A., Mahmood W. Survey of consensus protocols. 2018. https://www.researchgate.net/publication/328160285_Survey_of_Consensus_Protocols.
4. Popov S. The tangle. 2018. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvslqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1.4_3.pdf.
5. Брыкова Н. В. Теория бухгалтерского учета: Баланс и система счетов. — 2-е изд. — М.: Академия, 2011. 80 с.
6. Грушо А. А., Зацаринный А. А., Тимонина Е. Е. Описание динамики цифровой экономики с помощью электронной бухгалтерской книги // Системы и средства информатики, 2020. Т. 30. № 1. С. 108–114.
7. Grusho A., Grusho N., Zabezhaiko M., Zatsarinny A., Timonina E. Information security of SDN on the basis of metadata // Computer network security / Eds. J. Rak, J. Bay, I. V. Kotenko, et al. — Lecture notes in computer science ser. — Springer, 2017. Vol. 10446. P. 339–347.
8. Грушо Н. А., Грушо А. А., Тимонина Е. Е. Локализация сбоев с помощью метаданных // Проблемы информационной безопасности. Компьютерные системы, 2020. № 3. С. 9–15.
9. Грушо А. А., Грушо Н. А., Забежайло М. И., Тимонина Е. Е. Локализация исходной причины аномалии // Проблемы информационной безопасности. Компьютерные системы, 2020. № 4. С. 9–16.
10. Грушо А. А., Грушо Н. А., Тимонина Е. Е. Методы защиты информации от атак с помощью скрытых каналов и враждебных программно-аппаратных агентов в распределенных системах // Вестн. РГГУ. Сер.: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность, 2009. № 10. С. 33–45.
11. Грушо А. А., Грушо Н. А., Забежайло М. И., Тимонина Е. Е. «Закладки» без вредоносного кода // Системы и средства информатики, 2021. Т. 31. № 2. С. 4–15.
12. Грушо А. А., Забежайло М. И., Зацаринный А. А., Николаев А. В., Писковский В. О., Тимонина Е. Е. Классификация ошибочных состояний в распределенных вычислительных системах и источники их возникновения // Системы и средства информатики, 2017. Т. 27. № 2. С. 29–40.

Поступила в редакцию 23.07.21

SECURE SCALING OF ELECTRONIC LEDGERS BASED ON TANGLES

A. A. Grusho, A. A. Zatsarinny, and E. E. Timonina

Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119133, Russian Federation

Abstract: The paper deals with an electronic ledger based on the concept of blockchain. The development of the traditional blockchain is the tangle (tangle), which is represented by an oriented acyclic graph (DAG — Directed Acyclic Graph) and which securely stores transaction information. A centralized consensus implies a concentration of control functions in a single body. The scaling up of e-books in some cases poses threats of corruption and fraud. Three types of threats are considered that are determined by corruption and collusion of legal entities. Ensuring information security when scaling electronic books is a direction that begins to develop in connection with the growth of the digital economy.

Keywords: information security; tangle; blockchain; threats of corruption and fraud

DOI: 10.14357/08696527210305

Acknowledgments

The paper was partially supported by the Russian Foundation for Basic Research (project 18-29-03124-mk).

References

1. Leloup, L. 2017. *Blockchain: La revolution de la confiance*. Paris: Groupe Eyrolles. 160 p.
2. Grusho, A. A., A. A. Zatsarinny, and E. E. Timonina. 2019. Elektronnaya bukhgalterskaya kniga na baze situatsionnykh tsentrov dlya tsifrovoy ekonomiki [The electronic ledger on the basis of the situational centers for digital economy]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 29(2):4–11.
3. Wahab, A., and W. Mahmood. 2018. Survey of consensus protocols. Available at: https://www.researchgate.net/publication/328160285_Survey_of_Consensus_Protocols (accessed April 24, 2021).
4. Popov, S. 2018. The tangle. Available at: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvslqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218elec/iotal_4_3.pdf (accessed August 24, 2021).
5. Brykova, N. V. 2011. *Teoriya bukhgalterskogo ucheta: Balans i sistema schetov* [Accounting theory: Balance sheet and system of accounts]. 2nd ed. Moscow: Akademiya. 80 p.
6. Grusho, A. A., A. A. Zatsarinny, and E. E. Timonina. 2020. Opisaniye dinamiki tsifrovoy ekonomiki s pomoshch'yu elektronnoy bukhgalterskoy knigi [Description

- of digital economy dynamics using an electronic ledger]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 30(1):108–114.
7. Grusho, A., N. Grusho, M. Zabezhailo, A. Zatsarinny, and E. Timonina. 2017. Information security of SDN on the basis of metadata. *Computer network security*. Eds. J. Rak, J. Bay, I. V. Kotenko, *et al.* Lecture notes in computer science ser. Springer. 10446:339–347.
 8. Grusho, N. A., A. A. Grusho, and E. E. Timonina. 2020. Lokalizatsiya sboev s pomoshch'yu metadannykh [Localizing failures with metadata]. *Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy* [Information Security Problems. Computer Systems] 3:9–15.
 9. Grusho, A. A., N. A. Grusho, M. I. Zabezhailo, and E. E. Timonina. 2020. Lokalizatsiya iskhodnoy prichiny anomalii [Root cause anomaly localization]. *Problemy informatsionnoy bezopasnosti. Komp'yuternye sistemy* [Information Security Problems. Computer Systems] 4:9–16.
 10. Grusho, A. A., N. A. Grusho, and E. E. Timonina. 2009. Metody zashchity informatsii ot atak s pomoshch'yu skrytykh kanalov i vrazhdebnykh programmno-apparatnykh agentov v raspredelennykh sistemakh [Methods of information protection against covert channels attacks and malicious software/hardware agents in distributed systems]. *Vestnik RGGU. Ser. Dokumentovedenie i arkhivovedenie. Informatika. Zashchita informatsii i informatsionnaya bezopasnost'* [RGGU Bulletin. Document Science and Archive Science. Informatics. Information security and information security ser.] 10:33–45.
 11. Grusho, A. A., N. A. Grusho, M. I. Zabezhailo, and E. E. Timonina. 2021. “Zakladki” bez vredonosnogo koda [Hidden impact without malicious code]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 31(2):4–15.
 12. Grusho, A. A., M. I. Zabezhailo, A. A. Zatsarinny, A. V. Nikolaev, V. O. Piskovski, and E. E. Timonina. 2017. Klassifikatsiya oshibochnykh sostoyaniy v raspredelennykh vychislitel'nykh sistemakh i istochniki ikh vozniknoveniya [Erroneous states classification in distributed computing systems and sources of their occurrence]. *Sistemy i Sredstva Informatiki — Systems and Means of Informatics* 27(2):29–40.

Received July 23, 2021

Contributors

Grusho Alexander A. (b. 1946) — Doctor of Science in physics and mathematics, professor, principal scientist, Institute of Informatics Problems, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119133, Russian Federation; grusho@yandex.ru

Zatsarinny Alexander A. (b. 1951) — Doctor of Science in technology, professor, principal scientist, Institute of Informatics Problems, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119133, Russian Federation; AZatsarinny@ipiran.ru

Timonina Elena E. (b. 1952) — Doctor of Science in technology, professor, leading scientist, Institute of Informatics Problems, Federal Research Center “Computer Science and Control” of the Russian Academy of Sciences, 44-2 Vavilov Str., Moscow 119133, Russian Federation; eltimon@yandex.ru