УНИВЕРСИТЕТ ИТМО
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
март–апрель 2021 Том 21 № 2 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
March–April 2021 Vol. 21 No 2 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)
НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2021-21-2-249–255
УДК 004.75

Модель устойчивого распределенного реестра для анализа безопасности многомерного блокчейна

Илья Михайлович Шилов[1]✉, Данил Анатольевич Заколдаев[2]

[1,2] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] ilia.shilov@yandex.ru✉, https://orcid.org/0000-0002-4019-0705

[2] d.zakoldaev@itmo.ru, https://orcid.org/0000-0002-2520-1998

Аннотация

Предмет исследования. Рассмотрена задача построения модели устойчивого распределенного реестра, предназначенной для доказательства безопасности многомерного блокчейна. К модели предъявляется ряд требований, наиболее существенными из которых являются совместимость с существующими моделями и поддержка внешних транзакций. **Метод.** Предложенный подход основан на анализе существующих моделей, построенных с использованием фреймворка универсальной композиции и с учетом выявленных достоинств и недостатков. В качестве основы для построения моделей используется фреймворк универсальной композиции. Рассмотрены две модели: устойчивого распределенного реестра и связанного с ней протокола поиска и верификации внешних транзакций, предназначенные для доказательства безопасности масштабирования и процесса регистрации при использовании многомерного блокчейна. Модель устойчивого распределенного реестра является расширением моделей, с помощью которых была доказана безопасность достижения консенсуса — доказательств работы и доли владения. Модель дублирует их функции и дополнительно поддерживает проверку корректности внешних транзакций. **Основные результаты.** Показана совместимость модели с существующими решениями. Модель протокола поиска и верификации блоков и транзакций реализует идеальный функционал, предназначенный для верификации внешних транзакций. Доказано, что предложенная модель не нарушает существенные свойства безопасности устойчивого распределенного реестра при наличии внешних транзакций. **Практическая значимость.** Доказана совместимость представленных моделей с существующими аналогами, реализующими устойчивые распределенные реестры. Совместимость позволяет использовать теорему универсальной композиции при построении доказательства безопасности многомерного блокчейна и протокола поиска и верификации. Рассмотренный метод расширения существующих моделей для доказательства безопасности может быть использован для создания новых моделей, включающих в себя дополнительные функции, не используемые при доказательстве безопасности многомерного блокчейна.

Ключевые слова

блокчейн, устойчивый распределенный реестр, многомерный блокчейн, фреймворк универсальной композиции, механизм достижения консенсуса, транзакции, доказательство безопасности

Благодарности

Работы выполнены при поддержке ФГБУ «Фонд содействия развитию малых форм предприятий в научно-технической сфере» (договор № 14492ГУ/2019 от 18.07.2019).

Ссылка для цитирования: Шилов И.М., Заколдаев Д.А. Модель устойчивого распределенного реестра для анализа безопасности многомерного блокчейна // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 2. С. 249–255. doi: 10.17586/2226-1494-2021-21-2-249-255

The robust distributed ledger model for a multidimensional blockchain security analysis

Ilya M. Shilov[1]✉, Danil A. Zakoldaev[2]

[1,2] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] ilia.shilov@yandex.ru✉, https://orcid.org/0000-0002-4019-0705

[2] d.zakoldaev@itmo.ru, https://orcid.org/0000-0002-2520-1998

Abstract

The paper considers the problem of constructing a model of the robust distributed ledger for security proof of a multidimensional blockchain. Several requirements for the model are imposed, among which most important are compatibility with existing models and presence of functionalities for external transactions. The authors present an approach to extending existing models based on the analysis of these solutions, their advantages and disadvantages. The model construction is based on universal composability framework. Two models are proposed: a model of the robust distributed ledger and a model of the search and verification protocol. These are meant to be used in security proofs for scaling and registration in a multidimensional blockchain. The proposed model of the robust distributed ledger is an extension of models used in security proofs for consensus mechanisms: proof of work and proof of stake. It duplicates their functions and additionally maintains external transactions. The model of the search and verification protocol implements ideal functionality used for external transaction verification. The results prove that the proposed model does not damage essential security parameters of the robust distributed ledger in presence of external transactions. The study confirms the compatibility of the proposed models with existing analogues implementing robust distributed ledgers. This fact allows using the universal composability theorem for constructing security proofs of multidimensional blockchain and search and verification protocol. The proposed method of extending existing models for security proofs can be used to create new models with additional functions not implemented for security proof of a multidimensional blockchain.

Keywords

blockchain, robust distributed ledger, multidimensional blockchain, universal composability framework, consensus mechanism, transactions, security proof

Acknowledgements

The research is supported by the Foundation for Assistance to Small Innovative Enterprises (FASIE) (contract No. 14492ГУ/2019, 18.07.2019).

For citation: Shilov I.M., Zakoldaev D.A. The robust distributed ledger model for a multidimensional blockchain security analysis. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 2, pp. 249–255 (in Russian). doi: 10.17586/2226-1494-2021-21-2-249-255

Введение

Многомерный блокчейн является продолжением развития концепции одномерного блокчейна. Эта технология предназначена для построения масштабируемого решения с сохранением всех преимуществ технологии блокчейн, а также для организации безопасной передачи данных между устойчивыми распределенными реестрами без посредников.

Одной из наиболее важных задач при проектировании распределенных технологий является доказательство их безопасности. Среди наиболее часто используемых подходов к доказательству безопасности выделяются подходы, основанные на методах теории вероятностей и построенные с использованием фреймворка универсальной композиции (Universal Composability framework). Для блокчейна Bitcoin и других протоколов, реализующих устойчивый распределенный реестр, предложены доказательства безопасности с использованием перечисленных методов, например, несколько моделей, основанных на фреймворке универсальной композиции и различающихся своей структурой. В работах [1–3] рассмотрены безопасность Bitcoin и соответствующий ему механизм достижения консенсуса — доказательства работы, в [4–6] — безопасность доказательства доли владения. Однако эти модели не совместимы с многомерным блокчейном, поскольку не предполагают межсистемного взаимодействия. По этой причине их использование при доказательстве безопасности многомерного блокчейна не представляется возможным.

Цель данной работы — построение модели устойчивого распределенного реестра, совместимой с существующими аналогами и поддерживающей межсистемное взаимодействие. Модель предназначена для доказательства безопасности многомерного блокчейна и обоснования предоставляемых им гарантий. Следовательно, необходимо показать, что она не нарушает свойства исходных моделей, существенные для корректности теорем и утверждений об их безопасности.

Существующие научные работы описывают конкретные протоколы (Bitcoin и Ouroboros), но фактически в работах доказывается безопасность механизмов достижения консенсуса, а не приложений на основе блокчейна [7]. Поэтому безопасность производных от Bitcoin криптовалют может быть доказана или опровергнута с использованием тех же теорем и умозаключений, что и в указанных работах.

Материалы и методы решения задач, принятые допущения

GUC-модели (Generalized Universal Composability framework models) представляют собой вычислительные системы, в которых осуществляется взаимодействие между интерактивными машинами Тьюринга. Можно выделить два наиболее существенных преи-

мущества моделей, построенных с использованием данного фреймворка. Во-первых, в моделях, которые используют идеальный функционал (ideal functionality) для представления протокола, реализующие его интерактивные машины Тьюринга могут быть заменены на примитивные узлы (dummy parties). Эти узлы только передают сообщения от окружения и атакующего идеальным функционалам. Доказательство корректности такой замены приведено в [8]. Во-вторых, теорема универсальной композиции позволяет заменять отдельные части протоколов на идеальные функционалы, которые их реализуют, что значительно упрощает процесс доказательства безопасности.

Существует две вариации UC-фреймворка (Universal Composability framework): стандартная и обобщенная [9]. В настоящей работе используется обобщенная версия, поскольку различные реестры могут использовать в своей работе общие настройки. Их наличие может влиять на порядок доказательства безопасности.

Как было отмечено в [10], многомерный блокчейн представляет собой обертку над функционалом одномерного блокчейна. Под «оберткой» (wrapper, wrapping functionality) понимается интерактивная машина Тьюринга, которая содержит другие интерактивные машины Тьюринга и код, расширяющий множество их функций. Следовательно, при формировании модели устойчивого распределенного реестра следует выполнять ряд требований:

— независимость от механизма достижения консенсуса;
— независимость от содержимого блоков (в существующих моделях для этого используется предикат Blockify [4, 11]);
— учет задержки передачи данных в сети;
— совместимость с одним из существующих доказательств безопасности.

При построении доказательства должны использоваться понятия стойкости (persistence) и живости (liveness) как обобщенные критерии признания реестра устойчивым. При этом их определение должно быть дано для каждой системы, входящей в состав многомерного блокчейна, а кроме того, должна быть оценена вероятность того, что эти свойства достигаются для такой системы.

Сравнительный анализ моделей

В научных публикациях встречается несколько различных моделей, реализующих одномерный устойчивый распределенный реестр. Эти модели развиваются с течением времени и основаны на различных принципах, однако при этом следуют общей цели и реализуют один и тот же функционал. В каждой модели присутствует окружение (environment) Z, которое используется для наблюдения за работой протокола, отправкой запросов и получения ответов от UC-модели. Исполнение реализуется в виде последовательности временных слотов, т. е. наиболее подходящим подходом является дискретизация времени.

Предложенная в [1] модель реализует одномерный устойчивый реестр, основанный на положениях UC-фреймворка. Атакующий — адаптивный, т. е. имеет возможность компрометировать узлы системы в процессе ее работы. Кроме того, атакующий не может изменять содержимое сообщений узлов, но может отправлять поддельные сообщения от их лица. Данное исследование посвящено безопасности доказательства работы. Этот механизм реализован в виде идеального функционала, к которому осуществляются запросы ограниченное число раз в каждом раунде. Сформулированы понятия Common Prefix Property и Chain Quality Property. В [2] рассмотрены аналогичная модель и аналогичные условия, однако доказательство осуществлено с использованием полученных в [3] результатов. Отличием является наличие CGP (Chain Growth Property).

Работа [3] основана на выдвинутых в [1] положениях. Отличительной особенностью является динамическое количество узлов в исполнении протокола. При этом изменяется сложность вычисления доказательства работы, а значит, и параметры модели. Количество активно участвующих в исполнении протокола узлов и доля атакующих динамически меняются. Также стоит отметить, что понятие BA-протокола (Byzantium Agreement Protocol) не используется в работе.

В [11] применена симуляция для доказательства безопасности протокола, лежащего в основе системы Bitcoin. Количество узлов изменяется динамически, для сети передачи сообщений характерны задержки, причем верхняя граница для допустимых задержек узлам неизвестна. Доказательство основано на симуляции.

В работах [4–6] введен новый теоретически обоснованный подход к построению протокола достижения консенсуса — семейство протоколов Ouroboros, реализующее доказательство доли владения. Работы [5, 6] практически полностью заимствуют ранее описанные модели, тогда как доказательство безопасности в [4] основано на новой GUC-модели, которая заимствует концепции [11].

Среди всех используемых моделей выделяются два общих подхода к построению доказательства. Первый подход (вычислительный) подразумевает построение модели для формализации доказательства методами теории вероятностей и математической статистики. Подход, основанный на симуляции, включает две разновидности. Во-первых, могут использоваться гибридные модели — когда части протокола заменяются на идеальные функционалы или наоборот, а для соответствующих исполнений доказывается идентичность [12]. Во-вторых, может использоваться симулятор. В этом случае исследователь строит интерактивную машину Тьюринга для протокола, которая симулирует действия атакующего идеальным функционалом узла [13]. Также может применяться обратный подход.

Модель устойчивого распределенного реестра

Для доказательства безопасности многомерного блокчейна необходима модель устойчивого распределенного реестра, входящего в его состав. Эта модель может отражать одномерный или многомерный блокчейн, а также любой другой способ построения устойчивого реестра, например, централизованный подход. Рассмотрим модель устойчивого распределен-

ного реестра, которая в дальнейшем будет применяться в качестве основы для доказательства безопасности многомерного блокчейна. В ее основе лежат модели реестров, построенные в [10, 11].

Модель включает в себя узлы, которые обычно используются в GUC-моделях при построении доказательства безопасности: G_{CLOCK} — часы для синхронизации времени, F_{CON} — функционал, который объединяет в себе необходимые для механизма достижения консенсуса методы (обертка над всеми возможными функционалами — такими как F_{KES} [11]), $F_{N\text{-}MC}$ — сеть передачи информации [14], P_i — узлы, которые предназначены для перенаправления сообщений от окружения функционалам или для исполнения исследуемого протокола, A — атакующий, Z — окружение (внешний наблюдатель).

Стоит отметить, что при реализации реестра идеальным функционалом подразумевается использование примитивных узлов (dummy parties), в задачу которых входит только передача сообщений от окружения к другим интерактивным машинам Тьюринга. В [8] доказано, что такая модель эквивалентна модели, в которой узлы выполняют полезную работу. При этом по аналогии с [11] узлы могут находиться в различных состояниях: вне сети, остановленные, в сети.

В соответствии с [11], модель принимает на вход набор алгоритмов: Validate, ExtendPolicy, Blockify, Predict-time. В отличие от моделей [10, 11] в ее основе лежит понятие состояния, а блокчейн рассматривается как конечный автомат, переходящий между состояниями посредством включения новых транзакций. Также в указанных работах атакующий предоставляет реестру собственное видение каждого следующего состояния, а алгоритм ExtendPolicy предназначен для контроля за деятельностью атакующего. При этом, поскольку целью является сопоставление поведения моделей с идеальным функционалом и без его использования, предполагается, что атакующий не будет намеренно создавать ситуацию, в которой ExtendPolicy сформирует собственное содержимое нового состояния. Псевдокод ExtendPolicy приведен в [10, 11]. Стоит отметить, что его работа зависит от используемого механизма достижения консенсуса. Аналогично заимствован алгоритм predict-time, который используется для того, чтобы исполнения моделей, используемых в доказательстве, не отличались друг от друга временными характеристиками.

Модель использует численные параметры windowSize (размер окна из [11]) и Delay (максимальное время синхронизации). Некоторые механизмы достижения консенсуса требуют использования дополнительных параметров.

Идеальный функционал поддерживает множество зарегистрированных узлов (P) и подмножество честных узлов (H), а также множество десинхронизированных честных узлов (P_{DS}). Дополнительно осуществляется хранение последовательности сообщений от честных узлов ($I_H{}^T$). Для каждого узла существует указатель и текущее состояние, хранимое этим узлом — *pt* и *state*.

Важным дополнением к ранее представленным моделям является вызов G_{VERIFY}. Этот идеальный функционал осуществляет верификацию транзакций, внешних для реестра. В случае многомерного блокчейна он реализуется с использованием протокола поиска и верификации блоков и транзакций. Новые внешние транзакции помещаются в специальный буфер (*ExtBuffer*) до момента их проверки и могут быть включены в *buffer* только после внешней проверки.

Для того чтобы не вводить в модель напрямую концепцию адресации, используется подход, в котором транзакции содержат транзакции из существующих моделей:

$$tx := (data, ext);\ ext \in \{\varepsilon, IN, OUT\},$$

где *data* — данные транзакции, а *ext* — флаг, который определяет, является ли транзакция внешней (принимает значения ε — внутренняя транзакция, *IN* — внешняя входящая транзакция, *OUT* — внешняя исходящая транзакция). При инициализации вызывается функционал F_{INIT}. Алгоритм работы модели при получении запроса.

1. Запрос к часам (CLOCK-READ), настройка временной метки: $\tau_L = \tau$.
2. $\hat{P} = \varnothing$; $P_i \in P_{DS}$: если $\tau' < \tau_L - Delay$, то $\hat{P} := \hat{P} \cup \{P_i\}$ и $P_{DS} := P_{DS} \backslash \hat{P}$.
3. Если запрос от честного узла, то запустить ExtendPolicy и обновить указатель на состояния. При наличии внешних транзакций — оповестить G_{VERIFY} и Атакующего: ($SUBMIT,sid,ledgerID,tx,|state|$).
4. Обновление G_{VERIFY}: ($STATE\text{-}UPDATE,sid,ledgerID,|state|,(pt_1,...,pt_l),P,H$).
5. Если запрос — добавление обычной транзакции, выполнить действия из [5].
6. Если запрос — добавление внешней транзакции, то добавить ее в *ExtBuffer* и оповестить узел: ($VERIFY,sid,ledgerID,tx$).
7. Если сообщение — *READ*, *MAINTAIN-LEDGER*, *NEXT-BLOCK*, *SET-SLACK*, то вызвать обработчик из [5].
8. Если сообщение — ответ от G_{VERIFY} ($VERIFY,sid,ledgerID,tx,flag$), если $flag = 1$, то переместить транзакцию из *ExtBuffer* в *buffer*.

Идеальный функционал поиска и верификации внешних транзакций

Для доказательства безопасности многомерного блокчейна требуется определить идеальный функционал для представления протокола поиска и верификации блоков и транзакций. Соответствующий ему протокол должен предоставлять узлам возможность находить узлы, поддерживающие другие реестры, и безопасно получать от них информацию о существовании транзакций при сохранении свойств стойкости и живости.

Кратко опишем работу идеального функционала. Он принимает на вход параметр Δ_{ext} — максимальное время задержки подтверждения внешней транзакции и значение γ — долю узлов, принимающих участие в проверке. Используемые переменные:

1. $attackDB := ((ledgerID_i, q_i))_{i=1,...,k}$,
2. $delayDB := ((ledgerID_i, \Delta_i))_{i=1,...,k}$,

3. *respnseDB:=(ledgerID,msg,τ′)*,
4. $stateDB:=((ledgerID_i,(pt_{i1},...,pt_{il}),|state_i|,|H_i|,|P_i|))_{i=1,...,k}$,
5. $extTX:=((ledgerID,tx_j,pt_j))_{j=1,...,z}$.

При инициализации также вызывается функционал F_{INIT}. Алгоритм работы модели при получении запроса.

1. Если запрос от часов, то настройка временной метки: $\tau_L = \tau$.
2. При получении внешней транзакции (*SUBMIT,sid,ledgerID,tx,pt*) сохранить ее в *extTX*, если ее там еще нет: *extTX:=extTX* || (*ledgerID,tx,pt*).
3. При активации проверить *extTX* и обработать записи, для которых $\tau_j \geq \tau_{now}$.
4. При получении запроса на верификацию внешней транзакции (*VERIFY,sid,ledgerID,tx*):
   1) если транзакции нет в *extTX*, прекратить исполнение;
   2) вычислить вероятность корректного ответа $\hat{p}$;
   3) принять решение об утвердительности ответа ($\hat{p} > 0{,}5$);
   4) сформировать ответ (*VERIFY,sid,ledgerID,tx,flag*);
   5) если в *delayDB* нет значения для целевого реестра, то отправить ответ, иначе: *responseDB:=responseDB* || *(ledgerID,message,*$\tau_L+\Delta'$).
5. При получении *(STATE-UPDATE,sid,ledgerID,* $|state|,(pt_1,...,pt_l),P,H$) обновить *stateDB*.
6. При получении от атакующего запроса (*SET-DELAY,ledgerID,*Δ') обновить соответствующее значение в *delayDB*.
7. При получении от атакующего запроса (*SET-VERIFY,ledgerID,p*) обновить соответствующее значение в *attackDB*.

Для того чтобы сделать модель реализуемой с использованием сравнительно простых протоколов, вводится ослабление — вероятностный ответ на вопрос о существовании транзакции. Вероятность зависит от предоставленной атакующим вероятности верного ответа и количества узлов, у которых запрашивается подтверждение. При этом под вероятностью, полученной от атакующего, понимается характеристика, отражающая количество подтверждений на запрос при опросе всех скомпрометированных узлов. Вероятность утвердительного ответа честных узлов определяется следующей формулой:

$$\forall pt_i \in PT: \theta_i := (pt < pt_i) \Rightarrow p := \sum_i \theta_i / |H|,$$

а общая вероятность утвердительного ответа:

$$\hat{p} := \frac{q \times \gamma \times (|P| - |H|)}{|P|} + \frac{p \times \gamma \times |H|}{|P|} = \gamma \times \left(q + \frac{(p-q) \times |H|}{|P|} \right), \quad (1)$$

где p — вероятность утвердительного ответа честных узлов; q — вероятность утвердительного ответа атакующим узлом; θ — случайная величина, принимающая значение 1 в случае, если индекс указателя для реестра превосходит указатель для состояния, в котором была принята транзакция.

Стоит отметить важную особенность работы данного идеального функционала. Решение о том, будет ли проверяемая транзакция объявлена верной, принимается в момент запроса и не изменяется в течение промежутка времени задержки. Данный подход отражает наихудший вариант развития событий при практическом использовании протокола, поскольку атакующий принимает решение об ответе на запрос однократно (этот параметр не зависит от времени запроса).

Доказательство применимости моделей

Утверждение 1. Модель устойчивого распределенного реестра совместима с моделями, представленными в [10, 11].

Истинность данного утверждения доказывается симуляцией. В случае, если идеальные функционалы одинаково реагируют на внешние воздействия и неотличимы для стороннего наблюдателя, они эквивалентны. Сообщения READ, MAINTAIN-LEDGER, NEXT-BLOCK и SET-SLACK обрабатываются одинаковым кодом. При отсутствии внешних транзакций отсутствует взаимодействие с G_{VERIFY}. В этом случае код моделей полностью совпадает за исключением дополнительных действий при инициализации, явно не влияющих на внешние взаимодействия. При наличии внешних транзакций их проверка осуществляется с использованием идеального функционала. В случае, если функционал работает корректно, внешние транзакции применяются аналогично встроенным — с дополнительной задержкой, необходимой для проверки, что влияет на живость транзакций, но не нарушает ее.

В отличие от моделей в [10, 11], в настоящей работе введена зависимость от функционала проверки внешних транзакций, которая не имеет значения при самостоятельном использовании многомерного блокчейна.

Кроме того, введен набор методов и вызовов для работы с этим функционалом, изменена семантика транзакций, добавлена их внутренняя структура. При этом не используются в явном виде понятия, характерные для механизмов достижения консенсуса. Дополнительно введены идентификаторы реестров для их совместной работы.

Стоит отметить, что в отдельных случаях в качестве реализующего функционал G_{VERIFY} узла может выступать централизованный сервис, которому доверяют остальные участники системы. Такой подход используется в системе Corda R3.

Утверждение 2. Свойства стойкости и живости не нарушаются при использовании предложенного идеального функционала поиска и верификации транзакций с вероятностью, пропорциональной γ.

Поскольку ответ о верификации внешних транзакций возвращается с задержкой, единственная возможность нарушить стойкость — включение в реестр внешней транзакции и ее обращение в исходном реестре. Все реестры в многомерном блокчейне являются стойкими по определению, поэтому такая ситуация теоретически возможна только тогда, когда исходящая транзакция обращается до ее погружения на безопасную глубину. Если $\gamma = 1$, это невозможно, исходя из принципа честного большинства (q меньше 0,5). Иначе вероятность прямо пропорциональна параметру γ в формуле (1).

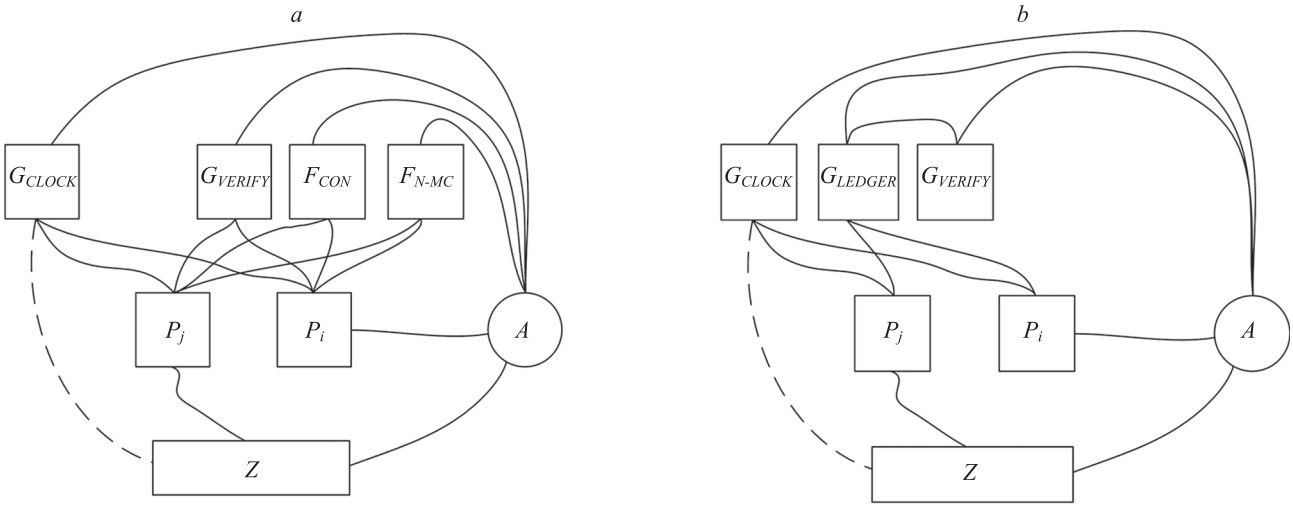

Рисунок. GUC-модель протокола, реализующего устойчивый распределенный реестр (*a*) и GUC-модель устойчивого распределенного реестра (*b*)

*Fig. G*UC-model of the protocol implementing the robust distributed ledger (*a*) and GUC-model of the robust distributed ledger (*b*)

При неправильном выборе параметра вероятность положительного ответа может превзойти 50 % даже в том случае, если не все честные узлы признали транзакцию свершившейся. Следовательно, при корректном выборе параметров стойкость не нарушается. Изучение вероятности атаки на протокол поиска и верификации является важным направлением для исследований по тематике: вероятно, возможно построение безопасных реализаций при значениях γ, меньших 1. Живость не нарушается по Утверждению 1.

На рисунке, *a* приведена модель для протокола, реализующего устойчивый распределенный реестр. Идеальный функционал F_{CON} используется для абстрагирования от механизмов достижения консенсуса [15]. На рисунке, *b* представлено схематическое изображение GUC-модели одномерного реестра, построенной с использованием идеального функционала для поиска и верификации блоков и транзакций. Целью построения доказательства безопасности протокола, реализующего устойчивый распределенный реестр является демонстрация эквивалентности приведенных моделей.

Заключение

В работе выполнен анализ моделей устойчивых распределенных реестров, построенных с использованием фреймворка универсальной композиции. Выявлены сходства и различия моделей, сформулированы требования к модели устойчивого распределенного реестра, предназначенной для доказательства безопасности многомерного блокчейна.

Построена модель идеального функционала для протокола поиска и верификации. Доказаны утверждения о корректности использования моделей при доказательстве безопасности многомерного блокчейна.

Согласно этим утверждениям, предложенная модель устойчивого распределенного реестра совместима с ранее созданными моделями и не нарушает свойства живости и стойкости при использовании приведенного идеального функционала поиска и верификации транзакций. Следовательно, модели могут использоваться для доказательства безопасности многомерного блокчейна с применением фреймворка универсальной композиции и теорем о безопасности, доказанных для этих моделей ранее.

Для доказательства безопасности многомерного блокчейна и функционирующего в его пределах протокола поиска и верификации блоков и транзакций необходимо построить аналогичную модель для многомерного блокчейна, построение которой является одним из направлений дальнейших исследований.

При этом анализ безопасности должен включать как вероятностную оценку сохранения свойств безопасности, так и доказательство с использованием симулятора или гибридных моделей.

Литература

1. Garay J., Kiayias A., Leonardos N. The bitcoin backbone protocol: Analysis and applications // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2015. V. 9057. P. 281–310. doi: 10.1007/978-3-662-46803-6_10
2. Garay J., Kiayias A., Leonardos N. The bitcoin backbone protocol: Analysis and applications [Электронный ресурс]. URL: https://eprint.iacr.org/2014/765.pdf, свободный. Яз. англ. (дата обращения: 15.03.21).
3. Garay J., Kiayias A., Leonardos N. The bitcoin backbone protocol with chains of variable difficulty // Lecture Notes in Computer

References

1. Garay J., Kiayias A., Leonardos N. The bitcoin backbone protocol: Analysis and applications. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9057, pp. 281–310. doi: 10.1007/978-3-662-46803-6_10
2. Garay J., Kiayias A., Leonardos N. *The bitcoin backbone protocol: Analysis and applications*. Available at: https://eprint.iacr.org/2014/765.pdf (accessed: 15.03.21).
3. Garay J., Kiayias A., Leonardos N. The bitcoin backbone protocol with chains of variable difficulty. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and*

Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. V. 10401. P. 291–323. doi: 10.1007/978-3-319-63688-7_10
4. Badertscher C., Gaži P., Kiayias A., Russell A., Zikas V. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability // Proc. 25th ACM Conference on Computer and Communications Security (CCS 2018). 2018. P. 913–930. doi: 10.1145/3243734.3243848
5. Kiayias A., Russell A., David B., Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. V. 10401. P. 357–388. doi: 10.1007/978-3-319-63688-7_12
6. David B., Gaži P., Kiayias A., Russell A. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2018. V. 10821. P. 66–98. doi: 10.1007/978-3-319-78375-8_3
7. Cachin C., Vukolić M. Blockchain consensus protocols in the wild // Leibniz International Proceedings in Informatics, LIPIcs. 2017. V. 91. P. 1.1–1.16. doi: 10.4230/LIPIcs.DISC.2017.1
8. Canetti R. Universally composable security: a new paradigm for cryptographic protocols // Proc. 42nd IEEE Symposium on Foundations of Computer Science. Newport Beach, CA, USA. 2001. P. 136–145. doi: 10.1109/sfcs.2001.959888
9. Canetti R., Dodis Y., Pass R., Walfish S. Universally composable security with global setup // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2007. V. 4392. P. 61–85. doi: 10.1007/978-3-540-70936-7_4
10. Шилов И.М., Заколдаев Д.А. Многомерный блокчейн и его преимущества // Информационные технологии. 2020. Т. 26. № 6. С. 360–367. doi: 10.17587/it.26.360-367
11. Badertscher C., Maurer U., Tschudi D., Zikas V. Bitcoin as a transaction ledger: A composable treatment // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. V. 10401. P. 324–356. doi: 10.1007/978-3-319-63688-7_11
12. Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts // Proc. 2016 IEEE Symposium on Security and Privacy. 2016. P. 839–858. doi: 10.1109/SP.2016.55
13. Pass R., Seeman L., Shelat A. Analysis of the blockchain protocol in asynchronous networks // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2017. V. 10211. P. 643–673. doi: 10.1007/978-3-319-56614-6_22
14. Hirt M., Zikas V. Adaptively secure broadcast // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2010. V. 6110. P. 466–485. doi: 10.1007/978-3-642-13190-5_24
15. Canetti R., Jain A., Scafuro A. Practical UC security with a global random oracle // Proc. 21st ACM Conference on Computer and Communications Security, CCS. 2014. P. 597–608. doi: 10.1145/2660267.2660374

Lecture Notes in Bioinformatics), 2017, vol. 10401, pp. 291–323. doi: 10.1007/978-3-319-63688-7_10
4. Badertscher C., Gaži P., Kiayias A., Russell A., Zikas V. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. *Proc. 25th ACM Conference on Computer and Communications Security (CCS 2018)*, 2018, pp. 913–930. doi: 10.1145/3243734.3243848
5. Kiayias A., Russell A., David B., Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10401, pp. 357–388. doi: 10.1007/978-3-319-63688-7_12
6. David B., Gaži P., Kiayias A., Russell A. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2018, vol. 10821, pp. 66–98. doi: 10.1007/978-3-319-78375-8_3
7. Cachin C., Vukolić M. Blockchain consensus protocols in the wild. *Leibniz International Proceedings in Informatics, LIPIcs*, 2017, vol. 91, pp. 1.1–1.16. doi: 10.4230/LIPIcs.DISC.2017.1
8. Canetti R. Universally composable security: a new paradigm for cryptographic protocols. *Proc. 42nd IEEE Symposium on Foundations of Computer Science.* Newport Beach, CA, USA, 2001, pp. 136–145. doi: 10.1109/sfcs.2001.959888
9. Canetti R., Dodis Y., Pass R., Walfish S. Universally composable security with global setup. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2007, vol. 4392, pp. 61–85. doi: 10.1007/978-3-540-70936-7_4
10. Shilov I.M., Zakoldaev D.A. Multidimensional blockchain and its advantages. *Information Technology*, 2020, vol. 26, no. 6, pp. 360–367. (in Russian). doi: 10.17587/it.26.360-367
11. Badertscher C., Maurer U., Tschudi D., Zikas V. Bitcoin as a transaction ledger: A composable treatment. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10401, pp. 324–356. doi: 10.1007/978-3-319-63688-7_11
12. Kosba A., Miller A., Shi E., Wen Z., Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. *Proc. 2016 IEEE Symposium on Security and Privacy*, 2016, pp. 839–858. doi: 10.1109/SP.2016.55
13. Pass R., Seeman L., Shelat A. Analysis of the blockchain protocol in asynchronous networks. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2017, vol. 10211, pp. 643–673. doi: 10.1007/978-3-319-56614-6_22
14. Hirt M., Zikas V. Adaptively secure broadcast. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6110, pp. 466–485. doi: 10.1007/978-3-642-13190-5_24
15. Canetti R., Jain A., Scafuro A. Practical UC security with a global random oracle. *Proc. 21st ACM Conference on Computer and Communications Security*, *CCS*, 2014, pp. 597–608. doi: 10.1145/2660267.2660374

Авторы

Шилов Илья Михайлович — научный сотрудник, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57199323605, https://orcid.org/0000-0002-4019-0705, ilia.shilov@yandex.ru
Заколдаев Данил Анатольевич — кандидат технических наук, доцент, декан, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57021875400, https://orcid.org/0000-0002-2520-1998, d.zakoldaev@itmo.ru

Authors

Ilya M. Shilov — Researcher, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57199323605, https://orcid.org/0000-0002-4019-0705, ilia.shilov@yandex.ru
Danil A. Zakoldaev — PhD, Associate Professor, Dean, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57021875400, https://orcid.org/0000-0002-2520-1998, d.zakoldaev@itmo.ru

Статья поступила в редакцию 02.02.2021
Одобрена после рецензирования 05.03.2021
Принята к печати 21.03.2021

Received 02.02.2021
Approved after reviewing 05.03.2021
Accepted 21.03.2021