УДК 004.75 **DOI** 10.15622/ia.20.4.2

И.М. Шилов, Д.А. Заколдаев

БЕЗОПАСНОСТЬ ПРОТОКОЛА ПОИСКА И ВЕРИФИКАЦИИ В МНОГОМЕРНОМ БЛОКЧЕЙНЕ

Шилов И.М., Заколдаев Д.А. **Безопасность протокола поиска и верификации в многомерном блокчейне.**

Аннотация. Проблема безопасного обмена информацией и проведения транзакций между устойчивыми распределенными реестрами является одной из наиболее актуальных в сфере проектирования и построения децентрализованных технологий. До настоящего времени были предложены подходы, ориентированные на ускорение проверки цепочки блоков для верификации транзакций в соседних блокчейнах. При этом проблема поиска ранее не затрагивалась. В работе рассмотрен вопрос безопасности обмена данными между самостоятельными устойчивыми распределенными реестрами в рамках многомерного блокчейна. Описаны принципы и основные этапы работы протокола, а также базовые требования, предъявляемые к нему. Предложены способы построения протокола обмена сообщениями для верификации внешних транзакций: централизованный подход, принцип подмножества и стойкий SVP. Доказана эквивалентность централизованного подхода идеальному функционалу поиска и верификации в GUC-моделях. Показана вероятность успешной верификации в случае использования подхода, основанного на подмножествах, при применении полного графа сети или эквивалентного подхода с полным графом между родительским и дочерним блокчейнами. Доказана небезопасность случая со связью 1 к 1 между родительским и дочерним реестром, а также небезопасность подхода, основанного на подмножестве узлов родительского и дочернего реестров. Предложен стойкий протокол поиска и верификации блоков и транзакций, основанный на свойствах стойкости устойчивых распределенных реестров. В значительной степени вероятность атаки определяется вероятностью атаки на процесс верификации, а не на процесс поиска. При необходимости защиты от атакующих, контролирующих до половины узлов в сети, предложен метод комбинации подходов для поиска и верификации блоков и транзакций.

Ключевые слова: протокол поиска и верификации, блокчейн, сайдчейн, многомерный блокчейн, GUC-фреймворк, устойчивый распределенный реестр.

1. Введение.

Многомерный блокчейн представляет собой один из подходов к построению устойчивого распределенного реестра. Эта технология основана на принципах работы обычного одномерного блокчейна и призвана решить основные проблемы работы одномерного блокчейна с сохранением гарантий безопасности и основных метрик его работы [1,2]. Наиболее существенными среди решаемых проблем являются проблема масштабирования устойчивых распределенных реестров и проблема безопасного обмена информацией между устойчивыми распределенными реестрами [3-5].

Внешние транзакции в многомерном блокчейне проводятся в два этапа (инициирования и акцепта), которые выполняются узлами в создавшем и принимающем транзакцию реестрах соответственно. Для успешной проверки существования и корректности транзакции в произвольном реестре предполагается использование специального

протокола. Он предназначен для достижения трех целей: поиска узлов, поддерживающих инициирующий реестр, запроса у них информации о корректности транзакции и принятия решения о допустимости принятия транзакции (выполнения фазы акцепта).

Представленный в предыдущих работах анализ многомерного блокчейна был посвящен технологии и ее безопасности в целом, без рассмотрения особенностей функционирования протокола поиска и верификации блоков и транзакций [1,6].

В работе [1] была сформирована концепция многомерного блокчейна, его структура и некоторые принципы функционирования (например, адресация). Были продемонстрированы его достоинства в сопоставлении с существующими аналогами, а также обобщенно показан подход к проведению внешних транзакций. При этом явным образом не рассматривалась безопасность технологии и подходы к организации взаимодействия между реестрами.

В работе [6] была построена модель устойчивого распределенного реестра с использованием фреймворка универсальной композиции (GUC, Generalized Universal Composability framework), GUC-модель, основанная на существующих моделях устойчивых распределенных реестров. Она предназначена для доказательства безопасности многомерного блокчейна. В работе явным образом введено понятие протокола поиска и верификации блоков и транзакций, однако в GUC-модели вместо реализаций данного протокола используется идеальный функционал, работающий по принципу черного ящика и предоставляющий необходимые функции узлам. Была доказана безопасность устойчивого распределенного реестра на основе многомерного блокчейна, построенного с использованием данной модели устойчивого распределенного реестра и идеального функционала проведения внешних транзакций. При этом возможные способы реализации протокола рассмотрены не были.

Корректное функционирование протокола поиска и верификации является основным условием корректности существующих утверждений, касающихся безопасности многомерного блокчейна. Поэтому актуальной представляется задача проектирования такого протокола, а также формального доказательства его безопасности, то есть сохранения свойств устойчивых распределенных реестров при его использовании.

В данной работе рассмотрен вопрос обмена данными между устойчивыми распределенными реестрами в пределах многомерного блокчейна. Авторами впервые предложены несколько подходов для организации такого обмена, а также произведена оценка их

безопасности. На основе полученных результатов предложен устойчивый протокол поиска и верификации блоков и транзакций, безопасность которого также проанализирована. Полученные результаты могут быть использованы как для реализации устойчивых распределенных реестров в пределах многомерного блокчейна, так и для организации взаимодействия между самостоятельными устойчивыми распределенными реестрами.

Работа состоит из восьми разделов. В начале кратко проанализирована проблема межсистемного обмена и предложенные ранее способы ее решения. Далее сформулированы базовые требования к протоколу поиска и верификации и рассмотрен порядок его работы. Затем рассмотрены различные подходы к построению протокола поиска и верификации блоков и транзакций, проанализирована их безопасность. В заключении произведена оценка полученных результатов и указаны перспективы для дальнейших исследований по тематике.

2. Анализ проблемы межсистемного обмена в распределенных технологиях. Понятие устойчивого распределенного реестра возникло сравнительно недавно, практически одновременно с возникновением понятия «блокчейн». Хотя методы решения задачи Византийских генералов рассматривались и ранее, существенных успехов удалось достичь лишь во втором десятилетии XXI века. Анализу безопасности устойчивых распределенных реестров и технологии блокчейн посвящено множество работ. Некоторые рассматривают безопасность конкретных систем (например, [2]), другие посвящены анализу безопасности механизмов достижения консенсуса [7-10]. Вопросы межсистемного взаимодействия изучены в меньшей степени, хотя проблема обмена информацией между устойчивыми распределенными реестрами неоднократно рассматривалась в научных публикациях.

Наиболее простым подходом является отслеживание всей цепочки блоков при верификации внешней транзакции [11]. Существенным недостатком данного подхода является скорость принятия решения о корректности транзакции: требуется запрос и проверка всей цепочки блоков. Одним из первых подходов к ускорению этого процесса является использование вложенных блокчейнов (interlink) [11]. Вместо проверки всей цепочки блоков проверяется цепочка блоков с хэш-суммами менее, чем $T / 2^i$ (T – целевое значение хэш-суммы для механизма достижения консенсуса). В результате сложность алгоритма проверки значительно уменьшается.

В работе [12] данный подход был усовершенствован. Предложенное решение упрощает проверку внешних транзакций, причем алгоритм имеет логарифмическую сложность относительно длины цепочки блоков в проверяемом блокчейне. Основным преимуществом является возможность верификации транзакции с использованием только одного запроса к целевому реестру. При этом доказывается уязвимость алгоритма из [11] к атаке со стороны участника системы, обладающего менее чем 50% вычислительной мощности. Также введены дополнительные предикаты, которые обобщают концепцию верификации, введенную ранее. Их особенностью является параметризация зависящим от конкретной реализации оператором сопоставления предоставленных доказательств, что делает решение независимым от конкретной реализации и особенностей конкретной системы. Тем не менее, стоит отметить, что данное решение подходит только для блокчейнов, использующих доказательство работы в качестве механизма достижения консенсуса.

В работе [13] рассмотрен подход, когда сайдчейны используются исключительно для создания усовершенствованных операций над токенами без изменения принципов функционирования блокчейна. Приведено интуитивное доказательство безопасности.

В [14] представлен обобщенный подход к построению сайдчейнов. Особенностью работы является ее направленность на системы, использующие доказательства доли владения. Кроме того, этот подход позволяет строить сайдчейны, поддерживающие метод GHOST [15]. Предложен новый криптографический примитив, направленный на проверку существования транзакции в сайдчейне. Отличительной чертой работы является формализация понятия сайдчейна без связи с конкретным механизмом достижения консенсуса.

Обзор многих современных технологий для построения привязанных сайдчейнов (pegged sidechains) приведен в [16]. Выделяются следующие способы организации сайдчейнов: централизованный посредник, федеративные сайдчейны, SPV (Simple Payment Verification). Описанные в работе решения основаны на концепции криптовалют, допускается лишь перевод части токенов между системами путем их заморозки в одной и создания в другой цепочке блоков. Также стоит отметить, что все рассмотренные в этой работе решения представляют собой лишь практические реализации.

Большинство рассмотренных методов посвящены обмену информацией о платежах в приложениях, реализующих криптовалюты. С одной стороны, этот подход позволяет узлам не отслеживать сторонние цепочки блоков, поскольку верификация основана на

методах криптографии и не подразумевает принятие решения на основе суждений узлов, поддерживающих внешний блокчейн, о корректности транзакции. С другой стороны, эти методы не могут быть использованы в сферах, отличных от криптовалют.

Еще одним недостатком сайдчейнов является необходимость использования общей формы хранения информации о транзакциях. В противном случае узлы обязаны обладать информацией о способе интерпретации структуры блоков в блокчейне-инициаторе транзакции. Поэтому существующие решения не подходят для построения взаимодействия между системами, реализующими разные приложения на основе устойчивых распределенных реестров. Иными словами, проблема заключается в том, что безопасность достигается проверкой цепочки блоков в соседнем реестре и не учитывает ответы поддерживающих его узлов.

Наконец, существенным недостатком является ограничение взаимодействия двумя реестрами. Поэтому важной особенностью перечисленных работ является отсутствие поиска узлов, поддерживающих внешний блокчейн. Обычно адреса для организации обмена предоставляются алгоритму в качестве исходных данных.

Рассмотренные проблемы существующих решений и работ, посвященных анализу их безопасности, подтверждают актуальность задачи и практическую ценность данной работы.

3. Протокол поиска и верификации. Основное назначение протокола поиска и верификации заключается в сохранении свойств стойкости и живости для самостоятельных реестров при использовании многомерного блокчейна [17]. Стойкость (persistence) может быть нарушена только при неправильном подборе параметров проверки внешних транзакций. В этом случае входящая транзакция, включенная в момент, когда она не перешла в неизменное состояние в исходном реестре, может быть исключена из исходного реестра после регистрации в реестре-приемнике. Узлы, поддерживающие целевой реестр, не смогут получить информацию об этом событии при отсутствии соответствующих механизмов в протоколе поиска и верификации блоков и транзакций. Поэтому либо должен быть включен такой функционал, либо протокол поиска и верификации должен явным образом предотвращать подобное поведение. Живость (liveness) может быть нарушена в том случае, если узлы, поддерживающие принимающий транзакцию блокчейн, не получат подтверждение корректности корректной транзакции. В этом случае применение транзакции к реестру не произойдет за конечное время.

Еще одно существенное требование, предъявляемое к протоколу поиска и верификации – сохранение децентрализованной структуры решения. Основное преимущество блокчейн решений – возможность достижения взаимопонимания между самостоятельными узлами, действующими в ненадежной среде передачи информации в присутствии атакующих. При верификации внешних транзакций этот принцип должен сохраняться, поскольку использование централизованного аналога сводит на нет получаемые от использования децентрализации преимущества.

Работа протокола поиска и верификации блоков и транзакций включает несколько процедур:

1. Процедура инициализации (initialization).
2. Процедура поддержания работы сети (maintenance).
3. Процедура поиска (search).
4. Процедура верификации (verification).

В рамках процедуры инициализации происходит настройка основных параметров функционирования протокола, устанавливаются необходимые соединения с узлами, поддерживающими другие реестры. Эту процедуру каждый узел выполняет каждый раз при запуске и начале работы с функционалом внешних транзакций. Основными параметрами данной подпрограммы являются: множество сетевых адресов соседних узлов для организации взаимодействия, минимально и максимально допустимое количество узлов при активном взаимодействии, количество узлов в родительском и дочерних реестрах для организации взаимодействия, а также флаг, определяющий участие узла в поддержании работы многомерного блокчейна. Кроме того, важным параметром является количество блоков, необходимых для приведения транзакции в необратимый вид. Этот параметр определяется для каждого блокчейна.

Процедура поддержания работы сети заключается в сохранении установленных соединений с узлами, поддерживающими различные блокчейны в пределах многомерного блокчейна, установлении новых соединений при нарушении работоспособности существующих, а также периодической ротации этих соединений. Данная процедура настраивается временными параметрами, определяющими период обмена сообщениями для поддержания соединений и период изменения набора взаимодействующих соседних узлов.

Процедура поиска выполняется каждый раз, когда требуется проверка внешней транзакции. Путем выполнения запросов к другим узлам, поддерживающим многомерный блокчейн, осуществляется поиск узлов, поддерживающих реестр-инициатор внешней транзакции.

Параметры для данной процедуры настроены на этапе инициализации. В процедуре верификации внешней транзакции осуществляется выбор узлов для запроса информации, получение информации и принятие на основе этой информации решения о корректности или некорректности входящей внешней транзакции. Параметром является требуемая доля утвердительных ответов, полученных от опрашиваемых узлов, для принятия внешней транзакции. Работа протокола поиска и верификации внешних транзакций продемонстрирована на рисунке 1.

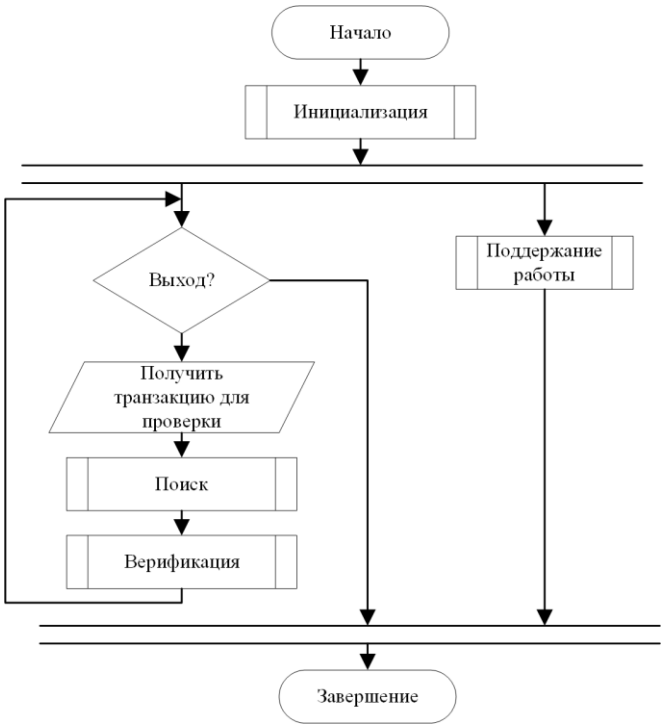

Рис. 1. Этапы работы протокола поиска и верификации

Возможны несколько подходов к построению протокола поиска и верификации блоков и транзакций:

1. Централизованный подход – проверка транзакций осуществляется с использованием единого узла или небольшой группы узлов, выступающих посредниками при проведении транзакций.

2. Подход, основанный на подмножествах – каждый узел поддерживает связь с некоторым подмножеством узлов в своем родительском блокчейне.
3. Стойкий search and verification protocol (SVP) – подход, основанный на свойствах устойчивого реестра и составляющий основной результат данной работы.

Рассмотрим предложенные подходы, выделим основные достоинства и недостатки этих подходов, а также произведем оценку безопасности каждого подхода.

3. Централизованный подход. Централизованный подход к построению протокола поиска и верификации подразумевает использование одного или нескольких узлов, совместно выполняющих работу по верификации транзакций. Они отслеживают состояние реестров в пределах многомерного блокчейна и предоставляют информацию о существовании или отсутствии транзакций при получении соответствующего запроса. Подобный подход используется в системе Hyperledger Fabric при создании и упорядочивании блоков: в качестве механизма достижения консенсуса используется получение подписей блоков со стороны удостоверяющих узлов.

Централизованный подход допустим в случаях, когда используются централизованные механизмы достижения консенсуса. Кроме того, иногда такой подход необходим, если транзакции между устойчивыми распределенными реестрами целенаправленно отслеживаются и анализируются контролирующими органами, и живость транзакций не является критически важным требованием. Стоит отметить, что аналогичных результатов можно добиться и в полноценно децентрализованном решении. Еще одним примером условий, при которых допустимо использование централизованного протокола поиска и верификации является ненагруженная система, в которой транзакции в каждом блокчейне сравнительно редки, и поддержание постоянных соединений для проведения внешних транзакций является избыточным.

Основным достоинством централизованного подхода является простота реализации, а также возможность выборочного блокирования транзакций в случае необходимости. Недостатками можно считать фактическое появление посредника при межсистемном обмене, что сводит на нет преимущества, предлагаемые многомерным блокчейном, а также достаточно низкую пропускную способность, поскольку количество запросов в единицу времени, которые может обработать единый узел, ограничено, что может привести к появлению дополнительной точки отказа.

Утверждение 1. Централизованный протокол поиска и верификации транзакций эквивалентен идеальному функционалу при условии, что узел, поддерживающий протокол честный.

Под честным узлом понимается узел, который не нарушает правила работы исполняемого протокола. В случае протокола поиска и верификации честность означает отсутствие действий, направленных на подтверждение несуществующих или отказ в подтверждении существующих транзакций. В этом случае централизованный узел поддерживает базу транзакций и отвечает на запросы по требованию, что полностью соответствует описанию идеального функционала, реализующего протокол поиска и верификации в GUC-моделях [6,18-21]. Следовательно, централизованный протокол UC-реализует протокол поиска и верификации при условии истинности предположений о его функционировании.

4. Подход, основанный на подмножествах. Иным способом работы с протоколом поиска и верификации является использование множеств. В этом случае каждый узел поддерживает взаимодействие с определенным подмножеством узлов, участвующих в работе многомерного блокчейна. Возможны четыре способа построения протокола поиска и верификации, основанного на подмножествах:

1. Способ, основанный на полном графе, когда каждый узел поддерживает соединение со всеми узлами системы.
2. Способ, основанный на полном графе, когда каждый узел поддерживает соединение со всеми узлами родительского реестра.
3. Способ, основанный на связи 1 к 1, когда каждый узел поддерживает связь только с одним узлом родительского реестра.
4. Способ, основанный на связи N к N, когда каждый узел поддерживает связь с набором узлов родительского блокчейна.

Второй и третий способы представляют собой граничные случаи подхода, основанного на подмножествах при взаимодействии только с родительским реестром, тогда как последний – промежуточный вариант. Рассмотрим каждый из описанных подходов. Далее под «соседними» реестрами понимаются реестры, находящиеся в отношении «родитель-дочерний реестр».

4.1. Способ полного графа сети со всеми узлами многомерного блокчейна. Способ, при котором узел поддерживает соединение со всеми узлами многомерного блокчейна, представляет собой вариант полного графа сетевого взаимодействия. Данный подход теоретически может применяться в сетях с небольшим количеством

узлов и редкими транзакциями, хотя его преимущества перед централизованным вариантом остаются предметом дискуссии. Фактически затраты на поддержание межсистемного взаимодействия могут превосходить затраты по поддержанию собственного реестра.

При проверке внешней транзакции узлы реестра-акцептора запрашивают информацию о существовании и корректности транзакции у всех узлов, поддерживающих реестр-инициатор, или у подмножества из k узлов. Поскольку стойкость реестра-инициатора постулируется по предположению, по принципу большинства верификация внешней транзакции гарантированно завершается успешно (поскольку честных узлов в стойком реестре большинство). При использовании подхода с запросом k узлов вероятность корректной верификации:

$$P = \begin{cases} \sum_{i=0}^{\left\lceil \frac{k}{2} \right\rceil - 1} C_k^i * q^i * p^{k-i}, \text{ если } z = \left\lceil \frac{k}{2} \right\rceil - 1 \le N_A; \\ 1, \text{ если } \left\lceil \frac{k}{2} \right\rceil - 1 > N_A, \end{cases} \quad (1)$$

где k – мощность подмножества, z – количество атакующих в подмножестве, N_A – общее число атакующих, P – целевое значение вероятности. В формуле высчитывается вероятность того, что не более половины из выбранных k узлов окажутся атакующими. Для этого суммируются все соответствующие вероятности, полученные по формуле Бернулли.

График изменения данной величины в зависимости от количества опрашиваемых узлов (k) приведен на рисунке 2. В качестве исходных величин использовались: количество атакующих 20, количество узлов 100, то есть атакующие исходно составляют 20% от общего числа узлов. С увеличением мощности множества вероятность успешной верификации стремится к единице. Поэтому при использовании данного подхода возможно достижение статистически безопасного обмена информацией о транзакциях даже при взаимодействии с подмножеством узлов.

Основные достоинства и недостатки этого подхода практически полностью повторяют достоинства и недостатки централизованного подхода. Хотя реализация такого подхода представляется задачей более сложной, чем реализация централизованного решения, пропускная способность в общем случае оказывается выше за счет параллельной обработки запросов.

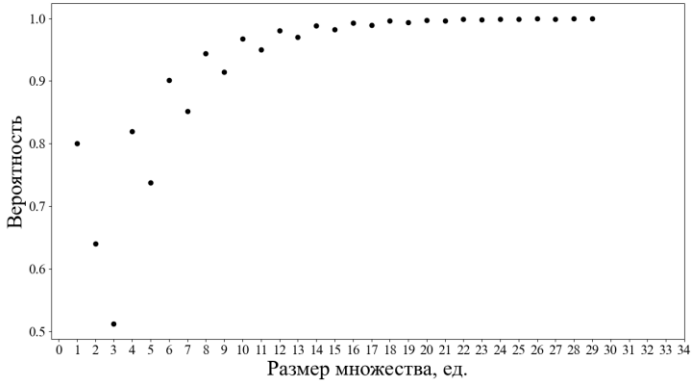

Рис. 2. Вероятность корректной верификации транзакций в полном графе

Утверждение 2. Протокол поиска и верификации блоков и транзакций, построенный на основе полного графа сетевого взаимодействия UC-реализует идеальный протокол поиска и верификации блоков и транзакций с вероятностью, указанной в Соотношении 1.

Поскольку Соотношение 1 выражает вероятность появления более половины честных узлов в выборке для запроса информации, оно отражает и вероятность принятия корректного решения по принципу большинства, что при исполнении прочих условий означает корректность реализации идеального протокола поиска и верификации. Результаты расчетов для $N = 100$ приведены в таблице 1.

Таблица 1. Вероятность успешной верификации

N	k	$q_1 = 0,5$	$q_2 = 0,4$	$q_3 = 0,3$	$q_4 = 0,2$	$q_5 = 0,1$
100	10	0,1719	0,3823	0,6496	0,8791	0,9872
100	20	0,2517	0,5956	0,8867	0,99	0,9999
100	30	0,2923	0,7145	0,9599	0,9991	1
100	40	0,3179	0,7911	0,9852	0,9999	1
100	50	0,3359	0,8438	0,9944	1	1

4.2. Способ полного графа между узлами соседних реестров. При использовании полного графа с родительским блокчейном необходимо рассмотреть безопасность как протокола верификации, так и протокола поиска. При поиске узлов целевого блокчейна для взаимодействия каждый атакующий узел может передавать

произвольное количество сгенерированных им узлов. В этом случае отсутствует контроль за количеством узлов, и атакующий может обеспечить себе сколь угодно большое преимущество перед честными узлами.

Поскольку анализ заведомо небезопасной реализации не имеет смысла, предлагается подход, защищающий систему от подобной атаки. Пусть при протоколе поиска на каждом уровне узлы получают от каждого узла перечень узлов его родительского или дочернего блокчейна, с которыми установлено соединение. Все узлы каждого реестра поддерживают соединение со всеми узлами соседнего реестра, поэтому для честных узлов предоставленные списки будут совпадать. Поскольку атакующий не контролирует большинство узлов, достаточно установить соединение с теми узлами, которые были найдены в более чем половине из предоставленных списков. Тогда в окончательном множестве по принципу большинства окажутся только узлы, с которыми установлено соединение честных узлов, то есть все узлы следующего блокчейна. Все остальные этапы взаимодействия эквивалентны случаю с полным графом и соединением «все-со-всеми».

4.3. Способ связи 1 к 1 между узлами соседних реестров. Это другой пограничный способ при построении взаимодействия с родительским реестром без учета особенностей его работы. Узлы для взаимодействия выбираются случайно. При этом возможно два варианта: либо узел, с которым установлено соединение, меняется в каждом раунде, либо соединения постоянны. Рассмотрим работу протокола в отдельно взятом раунде, поскольку в пределах одного раунда эти варианты идентичны, а вероятность выбора атакующего в наихудшем варианте постоянна.

Основным параметром в данной модели является расстояние между реестрами. Протокол поиска подразумевает последовательное взаимодействие с узлами всех реестров до корневого и далее от корневого до целевого реестра. Обозначим общее количество шагов d. На каждом уровне вероятность взаимодействия с атакующим совпадает с долей атакующих в реестре, с которым осуществляется взаимодействие – p_i. Если на каком-то промежуточном уровне начинается взаимодействие с атакующим, он может возвращать только подконтрольные атакующему узлы в следующих реестрах. Поэтому единственно безопасным исходом является взаимодействие с честными узлами на каждом уровне. Вероятность атаки на протокол поиска и верификации:

$$P = 1 - \prod_{i=1}^{d} (1 - p_i), \quad (2)$$

где p_i – вероятность взаимодействия с атакующим, d – число промежуточных блокчейнов. График вероятности атаки на протокол в зависимости от дистанции (для различных значений вероятности взаимодействия с атакующим на каждом шаге) приведен на рисунке 3.

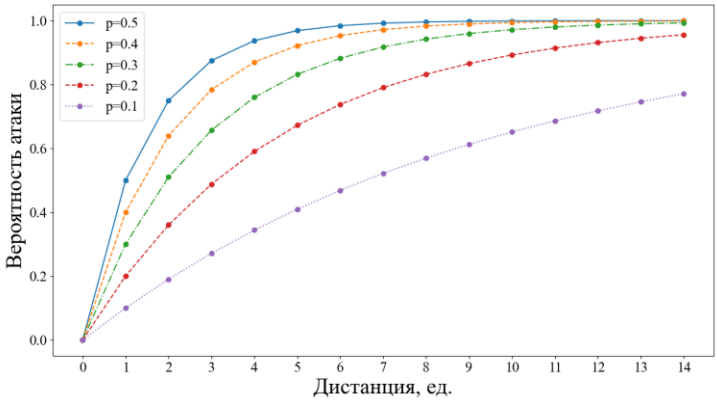

Рис. 3. Вероятность атаки на протокол в случае связи 1 к 1

Даже при незначительном количестве атакующих в каждом последующем реестре с увеличением количества промежуточных реестров вероятность атаки на протокол стремится к 1. Даже в случае, если количество атакующих составляет не более 10% в каждом реестре, при дистанции более 6 вероятность атаки превосходит 50%. Следовательно, подход с взаимодействием с одним узлом не является безопасным и не должен использоваться на практике.

4.4. Способ связи N к N между узлами соседних реестров. Данный способ является промежуточным и обобщенным вариантом, граничные варианты которого были рассмотрены ранее. Рассмотрим процесс поиска узлов реестра-инициатора при верификации внешней транзакции.

Каждый узел реестра-акцептора поддерживает связь с K узлами родительского блокчейна. При поиске следующего реестра у каждого узла запрашивается информация о смежных реестрах – связей аналогичным образом K. В наихудшем случае атакующий возвращает

информацию только об атакующих узлах в следующем реестре $(q=1)$. Если узел честный, то вероятность того, что он вернет атакующий узел:

$$p = \frac{N_A}{N}, \tag{3}$$

где N_A – количество атакующих в следующем реестре, N – количество узлов в этом реестре. Обозначим максимальное значение вероятности:

$$\max\{p_i\} = \phi, \tag{4}$$

где p_i – вероятность (3) для реестра с номером i.

Рассмотрим цепочку реестров от текущего до целевого и математическое ожидание количества атакующих, с которыми взаимодействует один узел на каждом шаге (M). Пусть общее число узлов – N. Математическое ожидание количества атакующих в первом реестре определяется долей атакующих узлов в реестре (N_A) и числом участвующих в поиске узлов (K):

$$E\left[M^1\right] = \frac{N_A^1}{N^1} * K. \tag{5}$$

Тогда количество выбранных атакующих во втором реестре:

$$\begin{aligned} E\left[M^2\right] &= \frac{E\left[M^1\right] * K + \frac{N_A^2}{N^2} * K * \left(K - E\left[M^1\right]\right)}{K} = \\ &= E\left[M^1\right] + \left(K - E\left[M^1\right]\right) * \frac{N_A^2}{N}. \end{aligned} \tag{6}$$

В общем случае:

$$\begin{aligned} E\left[M^i\right] &= \frac{E\left[M^{i-1}\right] * K + \frac{N_A^i}{N^i} * K * \left(K - E\left[M^{i-1}\right]\right)}{K} = \\ &= E\left[M^{i-1}\right] + \frac{N_A^i}{N^i} * \left(K - E\left[M^{i-1}\right]\right). \end{aligned} \tag{7}$$

Математические ожидания образуют последовательность, причем каждый член последовательности больше, чем предыдущий

(т. к. $K > E[M]$). Разность между последовательными членами последовательности:

$$E\left[M^{i}\right] - E\left[M^{i-1}\right] = \frac{N_A^i}{N^i} * \left(K - E\left[M^{i-1}\right]\right) > 0. \quad (8)$$

Поскольку каждый элемент последовательности больше предыдущего:

$$\lim_{i\to\infty}\left(\frac{N_A^i}{N^i} * \left(K - E\left[M^{i-1}\right]\right)\right) = 0. \quad (9)$$

Поэтому выполняется условие:

$$\forall \varepsilon > 0 \exists N(\varepsilon), \forall n, m > N(\varepsilon): \left|E\left[M^{n}\right] - E\left[M^{m}\right]\right| < \varepsilon. \quad (10)$$

Следовательно, последовательность сходится по критерию Коши. Рассмотрим предел последовательности в наихудшем случае – когда вероятность атаки на каждом шаге равна максимальной вероятности атаки (ϕ). Воспользуемся методом итераций.

$$E\left[M^{i+1}\right] = \phi\left(K - E\left[M^{i}\right]\right) = \phi * K - \phi * E\left[M^{i}\right] = \varphi\left(E\left[M^{i}\right]\right) \quad (11)$$

$$\begin{gathered}\lim_{i\to\infty} E\left[M^{i+1}\right] = \lim_{i\to\infty} \varphi\left(E\left[M^{i}\right]\right) = \varphi\left(\lim_{i\to\infty} E\left[M^{i}\right]\right) \Rightarrow \\ \Rightarrow \mathrm{M} = \varphi(M) = \phi * K - \phi * M \Rightarrow M = K.\end{gathered} \quad (12)$$

Следовательно, с увеличением количества шагов до целевого реестра доля атакующих в выборке стремится к 1, и использование этого протокола на практике недопустимо. Данная ситуация подтверждает возможность атаки, описанной при рассмотрении полного графа с родительским реестром, однако в данном случае защита на основе пересечения множеств неприменима, поскольку честные узлы в общем случае возвращают разный набор узлов для следующего шага, а подконтрольные атакующему узлы – один и тот же.

5. Стойкий протокол SVP

5.1. Описание протокола. Основным результатом работы является безопасный протокол поиска и верификации внешних

транзакций, основанный на свойствах блокчейна, реализующего устойчивый распределенный реестр:

1. Свойство общего префикса (CPP): для любых двух честных узлов цепочки блоков имеют общий префикс, получаемый отсечением k блоков.
2. Свойство качества цепочки (CQP): для последовательности из l блоков доля блоков, созданных атакующими, не превосходит μ.

При этом для свойства качества цепочки выполняются важные вспомогательные соотношения [10]. При этом доля блоков, созданных атакующим в худшем случае строго меньше 1:

$$\mu = \left(1+\frac{\delta}{2}\right)*\frac{t}{n-t} < 1-\frac{\delta}{2} < 1, \tag{13}$$

где t – число атакующих, n – число узлов, δ – преимущество честных узлов. В случае протоколов, реализующих доказательство доли владения [8-9,17] величина μ определяется как:

$$\epsilon \in (0,1), \beta \in [0,1], f \in (0,1] \Rightarrow \mu = \frac{\epsilon \beta f}{16} < 1, \tag{14}$$

где ϵ - качество концентрации случайных величин в «типичных исполнениях» (понятие установлено в [10]), β – ожидаемое число найденных атакующими решений задачи доказательства работы за раунд, f – общее ожидаемое число найденных решений за раунд.

Функционал многомерного блокчейна подписывается на обновления состояния в соседнем блокчейне. При этом отслеживаются последние $l+k$ блоков. Кроме того, по мере погружения блоков на безопасную глубину функционал устанавливает взаимодействие с узлами, создавшими последние l блоков, погрузившихся на достаточно безопасную глубину. Для упрощения рассмотрения и анализа безопасности не учитывается, что l и k отличаются для разных реестров – в реальности они выбираются на каждой итерации алгоритма. При запросе на верификацию транзакции осуществляется следующая последовательность действий:

1. Генерируется $l*l$ целых случайных чисел в диапазоне (0, N), где N – индекс блока на глубине k.
2. У каждого из l узлов, с которым установлено соединение, запрашивается l блоков и последовательность хэш-сумм от каждого блока до блока, созданного узлом в пределах l блоков.

3. Для каждого блока проверяется последовательность хэш-сумм. Если хотя бы для одного из блоков хэш-сумма некорректна, отбросить все результаты от узла-источника.
4. Из всех результатов выбрать l узлов. Для каждого блока запросить у узла-источника адрес узла, создавшего блок. Запросить у узла подтверждение создания блока – зависит от конкретного протокола блокчейна и структуры блоков. Если проверка осуществлена некорректно, заменить узел на случайно выбранный из полученного на шаге 3 множества.
5. Если полученные узлы не принадлежат целевому блокчейну, то перейти к шагу 1.
6. Иначе запросить у полученных l узлов верификацию транзакции и принять решение по принципу большинства.

Стоит отметить, что на практике оповещения о новых состояниях приходят с задержкой. Поэтому допустимо использовать окна большего размера – $k + \Delta k$, $l + \Delta l$.

5.2. Доказательство безопасности протокола. Утверждение 3. Протокол поиска и верификации позволяет корректно верифицировать внешнюю транзакцию с вероятностью, близкой к 1, при правильном выборе множества опрашиваемых узлов.

По определению многомерного блокчейна все реестры в его пределах являются устойчивыми. Реестр является устойчивым в том случае, если он выполняет требования к росту цепочки (CGP), общему префиксу (CPP) и чистоте цепочки (CQP) [10]. Параметром предиката CQP являются l – подпоследовательность блоков и μ – доля блоков, созданных атакующим в подпоследовательности. Параметром предиката CPP является k – глубина, на которой для всех честных узлов имеется общий префикс.

Алгоритм отслеживает блоки, погрузившиеся глубже, чем k. Следовательно, по свойству общего префикса у всех честных узлов цепочка длиной l совпадает. Кроме того, по свойству чистоты цепочки среди всех этих блоков есть как минимум один созданный честным узлом. Рассмотрим возможные атаки на протокол со стороны атакующего.

Событие 1 – Атакующий формирует блоки при запросе информации. Вероятность того, что произвольный блок был создан атакующим, совпадает с долей атакующих систему узлов (меньше 0.5). При попытке подделки цепочки заголовков от выбранного до текущего блока атакующий должен быстро построить новую цепочку, в которой именно он контролирует конкретный блок, что невозможно с вероятностью, близкой к 1 для блоков, находящихся достаточно

глубоко в цепочке блоков. Кроме того, эту задачу атакующий должен решить по несколько раз для получения большинства в множестве мощностью l^2.

Событие 2 – Атакующий не предоставляет информацию по запросу. Это событие игнорируется. Тогда окончательное множество имеет меньшую мощность, но доля атакующих в нем не изменяется.

Следовательно, атакующий не имеет возможности повлиять на соотношение блоков, созданных честными и атакующими узлами в выбранном множестве. Поскольку из полученного множества выбираются произвольные l узлов, доля атакующих по закону больших чисел будет приблизительно равна вероятности выбора атакующих, то есть строго менее 50% за счет принципа большинства честных узлов.

Аналогичным образом при завершении поиска информация о верифицируемой транзакции запрашивается у множества из l узлов, для которых выполняется принцип большинства честных узлов.

Вероятность атаки на протокол формируется из вероятности атаки на поиск и вероятности атаки на верификацию. Успешная атака на поиск возможна только в том случае, если все узлы в выбранном на некотором шаге множестве являются атакующими:

$$\phi = \max_{\mathrm{i}} \left\{ \frac{N_A^i}{N_i} \right\}, P_i^S = \phi^l, P_A^S = 1 - \left(1 - P_i^S\right)^d = 1 - \left(1 - \phi^l\right)^d, \quad (15)$$

где P_A^S – вероятность атаки на поиск, P_i^S – вероятность атаки на процедуру поиска в реестре с индексом i, d – расстояние до целевого реестра.

Вероятность атаки на верификацию аналогичным образом определяется соотношением честных и атакующих узлов:

$$\phi = \max_{\mathrm{i}} \left\{ \frac{N_A^i}{N_i} \right\}, P_A^V = 1 - \sum_{i=0}^{\left\lceil \frac{l}{2} \right\rceil - 1} C_l^i * \phi^i * \left(1 - \phi\right)^{l-i}, \quad (16)$$

где P_A^V - вероятность атаки на верификацию. Общая вероятность атаки:

$$P_A = P_A^V + P_A^S - P_A^V * P_A^S. \quad (17)$$

Примеры значений для данной вероятности приведены в таблице 2. Следовательно, длина пути верификации не оказывает значительного влияния на вероятность компрометации. При этом

основу вероятности компрометации составляет именно вероятность компрометации верификации, а не поиска, что соответствует результатам, полученным ранее при анализе вероятности успешной верификации для взаимодействия со всеми узлами целевого реестра.

Таблица 2. Вероятность атаки

l	d	$\phi_1 = 0,5$	$\phi_2 = 0,4$	$\phi_3 = 0,3$	$\phi_4 = 0,2$	$\phi_5 = 0,1$
10	5	0,8290	0,6179	0,3504	0,1209	0,0128
10	10	0,8298	0,6181	0,3504	0,1209	0,0128
15	5	0,8491	0,5968	0,2784	0,0611	0,0022
15	10	0,8492	0,5968	0,2784	0,0611	0,0022
20	5	0,7483	0,4044	0,1133	0,0100	ε
20	10	0,7483	0,4044	0,1133	0,0100	ε

Оценка максимальных возможностей атакующего должна осуществляться для каждого используемого на практике устойчивого распределенного реестра в отдельности.

Утверждение 4. Протокол поиска и верификации транзакций, основанный на свойстве чистоты цепочки, реализует идеальный функционал поиска и верификации с вероятностью соблюдения чистоты цепочки блокчейнами, входящими в многомерный блокчейн.

В предыдущих работах была представлена модель идеального функционала для протокола поиска и верификации блоков и транзакций [6]. Этот идеальный функционал получает оповещения о новых внешних транзакциях и отвечает с задержкой, устанавливаемой атакующим. При этом вероятность корректной верификации определяется долей узлов, участвующих в верификации. Покажем, что протокол, реализующий алгоритм, представленный в данной работе, GUC-реализует указанный идеальный функционал. Для этого кратко рассмотрим последовательные гибридные модели. Исходная и целевая модели приведены на рисунке 4.

HYB0 – исходная модель, внешние взаимодействия осуществляются с использованием идеального функционала для проверки внешних транзакций.

HYB1 – модель, в которой узлы самостоятельно обеспечивают работу с поиском реестров для взаимодействия. При этом все реестры по-прежнему оповещают идеальный функционал о внешних транзакциях. В результате каждый узел с использованием протокола поиска может гарантированно обнаружить подмножество узлов реестра-инициатора, то есть поиск осуществляется самостоятельно, тогда как верификация по-прежнему осуществляется с использованием

идеального функционала. Структурно модель не изменяется, а потому для внешнего наблюдателя эквивалентна HYB0.

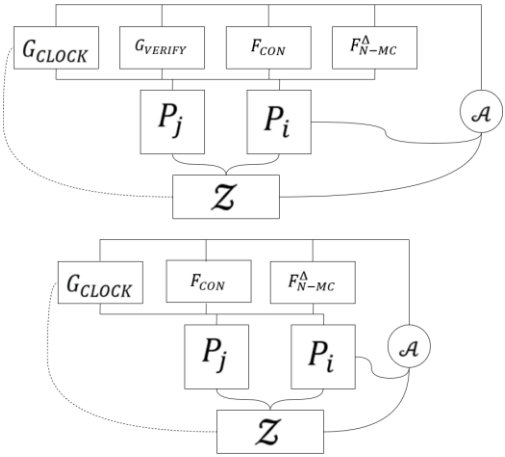

Рис. 4. GUC-модель: а) основанная на идеальном функционале; б) эквивалентная ей без данного функционала

HYB2 – разделение логики проверки транзакций. Вместо идеального функционала используется обертка, которая исполняет внутри себя набор идеальных функционалов, каждому из которых передаются запросы, связанные только с одним реестром. Внешние интерфейсы не изменяются, поэтому модель эквивалентна HYB1.

HYB3 – устранение обертки. Реестры самостоятельно взаимодействуют с идеальными функционалами. Запрос информации о том, у какого идеального функционала запрашивать верификацию, осуществляется у узлов, найденных через протокол поиска. Поскольку протокол поиска гарантированно находит узлы, поддерживающие реестр-инициатор, информация об идеальном функционале выявляется корректно с вероятностью, зависящей от доли честных узлов – Соотношение 6. При корректном подборе параметров эта вероятность стремится к 1. Стоит отметить, что вероятность некорректной верификации была учтена при построении GUC-модели для идеального функционала поиска и верификации транзакций (параметр γ).

HYB4 – запрос информации непосредственно у узлов. Аналогично HYB3 информация запрашивается у узлов, однако запрашивается именно информация о корректности транзакции. Вероятность корректной верификации при этом остается прежней,

поскольку честные узлы следуют протоколу и корректно верифицируют транзакцию. Эта модель эквивалентна протоколу поиска и верификации транзакций.

График для различных мощностей множества приведен на рисунке 5. За основу взята сеть, в которой присутствует 30 узлов. В качестве размера множества используется параметр l, введенный ранее. Следовательно, при незначительном оценочном количестве атакующих допустимо использовать как процедуру поиска, так и процедуру верификации предложенного протокола SVP. Однако, в случае если количество атакующих может достигать 50%, рекомендуется применять для процедуры верификации иные протоколы, то есть использовать комбинацию подходов.

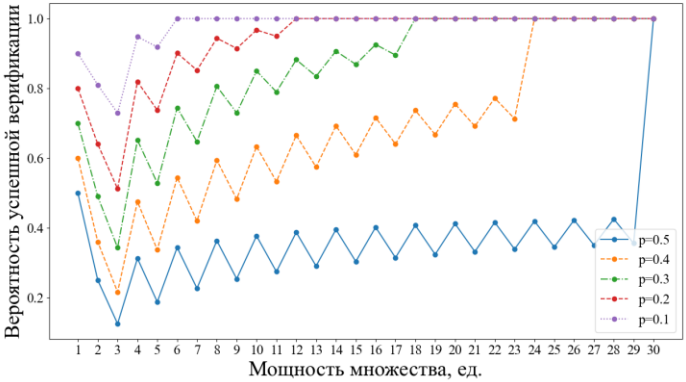

Рис. 5. Вероятность успешной верификации при различных размерах используемого подмножества

6. Комбинация подходов. Существует несколько возможных комбинаций подходов для различных условий работы многомерного блокчейна:

1. SVP и централизованный подход – в каждом реестре создается доверенный узел, отвечающий за верификацию внешних транзакций. В этом случае безопасный поиск осуществляется с помощью SVP, а верификация с использованием этого узла.
2. SVP и полный граф – если доля атакующих может достигать 50%, то допустимо организовывать поиск узлов с использованием протокола поиска и верификации, а затем – увеличить мощность опрашиваемого множества для повышения вероятности успешной верификации.

Стоит отметить, что полученные результаты не противоречат полученным ранее в иных работах, посвященных обмену информацией между блокчейнами [11-16]. Этап поиска завершается с вероятностью, близкой к 1. Этап верификации может быть завершен с вероятностью, близкой к 1 в случае, если количество атакующих сравнительно невелико (до 20%). Данные результаты схожи с результатами, достигнутыми в механизме достижения консенсуса Ripple. При использовании решений [5] или [11] возможно подтверждение корректности транзакций с вероятностью, близкой к 1, и за сравнительно небольшое время.

7. Обсуждение результатов. В работе было рассмотрено несколько подходов к построению протокола поиска и верификации блоков и транзакций. Основным результатом работы является протокол SVP, позволяющий осуществлять безопасный обмен данными между самостоятельными устойчивыми распределенными реестрами. Для всех рассмотренных подходов к построению протокола поиска и верификации проведен анализ безопасности. Рассмотрим основные отличия предлагаемого решения от существующих аналогов.

В работе [6] была рассмотрена модель многомерного блокчейна, использующая центральный модуль для верификации транзакций. Основным отличием предложенного подхода в части верификации является отсутствие требования к атомарности. Все внешние транзакции осуществляются в две фазы. Преимуществом данного подхода является независимость реестров друг от друга при принятии транзакций: реестр-акцептор принимает транзакцию в подходящий для поддерживающих его узлов момент времени.

Предложенные ранее в литературе подходы к обмену данными между устойчивыми распределенными реестрами [7-12] были предназначены для проведения платежей между криптовалютами, построенными на основе технологии блокчейн. Существенным отличием протокола поиска и верификации является независимость от приложения. Поэтому он может быть использован не только в сфере криптовалют, но и в любых приложениях, построенных с использованием технологии распределенного реестра.

Другое отличие от принципов, предложенных авторами работ, посвященных сайдчейнам, заключается в принципе отслеживания цепочки блоков соседнего блокчейна. В случае сайдчейнов создаются специальные контрольные точки, которые позволяют быстрее находить требуемые блоки, содержащие транзакции, и верифицировать их. В случае протокола поиска и верификации блоков и транзакций узлы

находятся в постоянном взаимодействии с узлами соседнего реестра и отслеживают цепочку из $2k$ последних блоков.

Отдельно стоит отметить, что предъявляемые к решению требования фактически совпадают с аналогичными требованиями, выдвинутыми в [5]. Решение удовлетворяет основным требованиям, предъявляемым к сайдчейнам и протоколам обмена информации между ними.

Ключевым преимуществом решения в сравнении с сайдчейнами можно считать возможность поиска узлов, поддерживающих реестр-инициатор. В случае сайдчейнов информация об узлах соседнего реестра подается протоколу на вход. В случае многомерного блокчейна (и протокола поиска и верификации блоков и транзакций) реестры находятся в иерархической зависимости, а потому могут находить узлы, поддерживающие произвольный реестр, по мере необходимости. Также благодаря использованию технологии в процессе проверки внешних транзакций может участвовать больше двух реестров.

Наиболее существенным достоинством предложенного решения является отсутствие необходимости в модификации реализации существующих решений (за исключением поддержки внешних транзакций и процедуры верификации). Подход не зависит от особенностей работы конкретных систем и позволяет им функционировать самостоятельно в пределах многомерного блокчейна. Существенной особенностью решения является отсутствие предикатов в отличие от рассмотренных существующих аналогов: у узлов сайдчейна запрашивается информация о корректности транзакции, а не доказательство корректности. Поэтому возможна работа с произвольными механизмами достижения консенсуса [22-24].

Стоит отметить, что при количестве атакующих, близком к 50% вероятность компрометации системы достаточно велика при опросе подмножества узлов. Поэтому в случаях, когда допустимое количество компрометаций не определено, процедура верификации должна быть построена на основе [5] или [11]. Иначе допустимо применение более простого подхода, рассмотренного в данной работе.

8. Заключение. В работе рассмотрена проблема безопасного обмена данными между самостоятельными устойчивыми распределенными реестрами в пределах многомерного блокчейна. Рассмотрены различные подходы к построению протокола поиска и верификации внешних транзакций. Для этих подходов произведена оценка безопасности. Предложен подход к построению безопасного протокола поиска и верификации транзакций, доказана его

безопасность и эквивалентность идеальному функционалу поиска и верификации транзакций.

Целью дальнейшей работы является построение новых механизмов для проведения внешних транзакций, оценка безопасности таких технологий, как кэширование, при их использовании в протоколе поиска и верификации блоков и транзакций. Кроме того, перспективным направлением для исследований является внедрение криптографии с нулевым разглашением в многомерный блокчейн и адаптация протокола поиска и верификации блоков и транзакций для проверки транзакций с нулевым разглашением. Также возможна адаптация криптографических алгоритмов с нулевым разглашением для проведения внешних транзакций.

Наконец, важным направлением для практических исследований является сопоставление многомерного блокчейна с другими технологиями с точки зрения различных характеристик работы. По результатам исследований должна быть произведена оптимизация характеристик и усовершенствование существующих протоколов для улучшения характеристик его работы.

Литература

1. *Шилов И.М., Заколдаев Д.А.* Многомерный блокчейн и его преимущества // Информационные технологии. 2020. Т. 26. № 6. С. 360–367.
2. *Badertscher C., Maurer U., Tschudi D., Zikas V.* Bitcoin as a Transaction Ledger: A Composable Treatment // Advances in Cryptology – CRYPTO 2017. 2017. pp. 324-356.
3. *Vukolic M.* Rethinking permissioned blockchains // Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017. pp. 3-7.
4. *Cachin C., Guerraoui R., Rodrigues L.* Introduction to Reliable and Secure Distributed Programming // Springer-Verlag, Berlin, Heidelberg. 2011. P. 279.
5. *Pease M., Shostak R., Lamport L.* Reaching agreement in the presence of faults // Journal of the ACM. 1980. vol. 27. pp. 228-234.
6. *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.
7. *Garay J., Kiayias A., Leonardos N.* The Bitcoin Backbone Protocol: Analysis and Applications // Advances in Cryptology - EUROCRYPT 2015. 2015. vol. 9057. pp. 281-310.
8. *Badertscher C., Gaži P., Kiayias A., Russell A., Zikas V.* Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability // ACM Conference on Computer and Communications Security – ACM CCS 2018. 2018. pp. 913–930.
9. *David B., Gaži P., Kiayias A., Russell A.* Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain // Advances in Cryptology – EUROCRYPT 2018. 2018. vol. 10821. pp. 66-98.
10. *Garay J., Kiayias A., Leonardos N.* The Bitcoin Backbone Protocol with Chains of Variable Difficulty // Advances in Cryptology – CRYPTO 2017. 2017. vol. 10401. pp. 291-323.

11. *Kiayias A., Lamprou N., Stouka AP.* Proofs of Proofs of Work with Sublinear Complexity // Financial Cryptography and Data Security. 2016. vol. 9604. pp. 61-78.
12. *Kiayias A., Miller A., Zindros D.* Non-interactive Proofs of Proof-of-Work // Financial Cryptography and Data Security. 2020. vol. 12059. pp. 505-522.
13. *Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timon J., Wuille P.* Enabling Blockchain Innovations with Pegged Sidechains. URL: https://blockstream.com/sidechains.pdf (дата обращения: 29.04.2021).
14. *Gazi P., Kiayias A., Zindros D.* Proof-of-Stake Sidechains // 2019 IEEEE Symposium on Security and Privacy (SP). 2019. vol. 1. pp. 677-694.
15. *Sompolinsky Y., Zohar A.* Accelerating Bitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains // IACR Cryptology ePrint Archive. 2013.
16. *Singh A., Click K., Parizi R.M., Zhang Q., Dehghantanha A., Choo K.K.R.* Sidechain technologies in blockchain networks: An examination and state-of-the-art review // Journal of Network and Computer Applications. 2020. vol. 149.
17. *Kiayias A., Russell A., David B., Oliynykov R.* Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol // Advances in Cryptology – CRYPTO 2017. 2017. vol. 10401. pp. 357-388.
18. *Canetti R.* Universally composable security: a new paradigm for cryptographic protocols // Proceedings 42nd IEEE Symposium on Foundations of Computer Science. 2001. pp. 136-145.
19. *Canetti R.* Universally composable signatures, certification, and authentication // Proceedings of 17th Computer Security Foundations Workshop (CSFW). 2014. pp. 219-235.
20. *Canetti R., Dodis Y., Pass R., Walfish S.* Universally Composable Security with Global Setup // Theory of Cryptography. 2007. vol. 4392. pp. 61-85.
21. *Canetti R., Shahaf D., Vald M.* Universally Composable Authentication and Key-Exchange with Global PKI // Public-Key Cryptography – PKC 2016. 2016. vol. 9615. pp. 265-296.
22. *Bentov I., Gabizon A., Mizrahi A.* Cryptocurrencies Without Proof of Work // Financial Cryptography and Data Security. 2016. vol. 9604. pp. 142-157.
23. *David B., Dowsley R., Larangeira M.* ROYALE: A Framework for Universally Composable Card Games with Financial Rewards and Penalties Enforcement // Financial Cryptography and Data Security. vol. 11598. pp. 282-300.
24. *Duan S., Meling H., Peisert S., Zhang H.* BChain: Byzantine Replication with Hight Throughput and Embedded Reconfiguration // Principles of Distributed Systems – OPODIS 2014. 2014. vol. 8878. pp. 91-106.

Шилов Илья Михайлович — научный сотрудник, Университет ИТМО. Область научных интересов: устойчивые распределенные реестры, многомерный блокчейн, анализ данных и математическая статистика в информационной безопасности. Число научных публикаций – 13. ilia.shilov@yandex.ru; Кронверкский пр., д. 49, г. Санкт-Петербург, 197101, РФ; р.т. +7(931)3604143.

Заколдаев Данил Анатольевич — к.т.н., доцент, декан факультета безопасности информационных технологий, Университет ИТМО. Область научных интересов: САПР, безопасность цифрового производства, аппаратные средства защиты информации, информационные технологии в образовании. Число научных публикаций – 200. d.zakoldaev@itmo.ru; Кронверкский пр., д. 49, г. Санкт-Петербург, 197101, РФ.

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

DOI 10.15622/ia.20.4.2

I. SHILOV, D. ZAKOLDAEV

SECURITY OF SEARCH AND VERIFICATION PROTOCOL IN MULTIDIMENSIONAL BLOCKCHAIN

Shilov I., Zakoldaev D. **Security of Search and Verification Protocol in Multidimensional Blockchain.**

Abstract. The issue of secure data exchange and performing external transactions between robust distributed ledgers has recently been among the most significant in the sphere of designing and implementing decentralized technologies. Several approaches have been proposed to speed up the process of verifying transactions on adjacent blockchains. The problem of search has not been under research yet. The paper contains security evaluation of data exchange between independent robust distributed ledgers inside multidimensional blockchain. Main principles, basic steps of the protocol and major requirements for it are observed: centralized approach, subset principle and robust SVP. An equivalence of centralized approach and ideal search and verification functionality is proven. The probability of successful verification in case of using fully connected network graph or equivalent approach with fully connected graph between parent and child blockchain is shown. The insecurity of approach with one-to-one links between child and parent ledgers or with a subset principle is proven. A robust search and verification protocol for blocks and transactions based on the features of robust distributed ledgers is presented. The probability of attack on this protocol is mostly defined by the probability of attack on verification and not on search. An approach to protection against an attacker with 50% of nodes in the network is given. It is based on combination of various search and verification techniques.

Keywords: Search and Verification Protocol, Blockchain, Sidechain, Multidimensional Blockchain, GUC-Framework, Robust Distributed Ledger.

Shilov Ilya – Researcher, ITMO University. Research interests: robust distributed ledgers, multidimensional blockchain, data analysis and statistics in information security. The number of publications – 13. ilia.shilov@yandex.ru; 49, Kronverksky pr., St. Petersburg, 197101, Russia; office phone: +7(931)3604143.

Zakoldaev Danil – Ph.D., Dr. Sci., Associate professor, Dean of Faculty of Secure Information Technologies, ITMO University. Research interests: CAD, cybersecurity, information security hardware, information technologies in education. The number of publications – 200. d.zakoldaev@itmo.ru; 49, Kronverksky pr., St. Petersburg, 197101, Russia.

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

References

1. Shilov I.M., Zakoldaev D.A. [Multidimensional blockchain and its advantages]. *Informacionnye tehnologii*. 2020. no. 6. pp. 360-367.
2. Badertscher C., Maurer U., Tschudi D., Zikas V. Bitcoin as a Transaction Ledger: A Composable Treatment. Advances in Cryptology – CRYPTO 2017. 2017. pp. 324-356.
3. Vukolic M. Rethinking permissioned blockchains. Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017. pp. 3-7.
4. Cachin C., Guerraoui R., Rodrigues L. Introduction to Reliable and Secure Distributed Programming. *Springer-Verlag, Berlin, Heidelberg*. 2011. p. 279.

5. Pease M., Shostak R., Lamport L. Reaching agreement in the presence of faults. *Journal of the ACM*. 1980. vol. 27. pp. 228-234.
6. Shilov I.M., Zakoldaev D.A. [The robust distributed ledger model for a multidimensional blockchain security analysis]. *Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki*. 2021. vol. 21. no. 2. pp. 249-255.
7. Kiayias A., Lamprou N., Stouka AP. Proofs of Proofs of Work with Sublinear Complexity. *Financial Cryptography and Data Security*. 2016. vol. 9604. pp. 61-78.
8. Kiayias A., Miller A., Zindros D. Non-interactive Proofs of Proof-of-Work. *Financial Cryptography and Data Security*. 2020. vol. 12059. pp. 505-522.
9. Back A., Corallo M., Dashjr L., Friedenbach M., Maxwell G., Miller A., Poelstra A., Timon J., Wuille P. Enabling Blockchain Innovations with Pegged Sidechains. URL: https://blockstream.com/sidechains.pdf (дата обращения: 29.04.2021).
10. Gazi P., Kiayias A., Zindros D. Proof-of-Stake Sidechains. 2019 IEEE Symposium on Security and Privacy (SP). 2019. vol. 1. pp. 677-694.
11. Sompolinsky Y., Zohar A. Accelerating Bitcoin's Transaction Processing Fast Money Grows on Trees, Not Chains. IACR Cryptology ePrint Archive. 2013.
12. Singh A., Click K., Parizi R.M., Zhang Q., Dehghantanha A., Choo K.K.R. Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*. 2020. vol. 149.
13. Kiayias A., Russell A., David B., Oliynykov R. Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. Advances in Cryptology – CRYPTO 2017. 2017. vol. 10401. pp. 357-388.
14. Canetti R. Universally composable security: a new paradigm for cryptographic protocols. Proceedings 42nd IEEE Symposium on Foundations of Computer Science. 2001. pp. 136-145.
15. Canetti R. Universally composable signatures, certification, and authentication. Proceedings of 17th Computer Security Foundations Workshop (CSFW). 2014. pp. 219-235.
16. Canetti R., Dodis Y., Pass R., Walfish S. Universally Composable Security with Global Setup. Theory of Cryptography. 2007. vol. 4392. pp. 61-85.
17. Canetti R., Shahaf D., Vald M. Universally Composable Authentication and Key-Exchange with Global PKI. Public-Key Cryptography – PKC 2016. 2016. vol. 9615. pp. 265-296.
18. Garay J., Kiayias A., Leonardos N. The Bitcoin Backbone Protocol: Analysis and Applications. Advances in Cryptology - EUROCRYPT 2015. 2015. vol. 9057. pp. 281-310.
19. Badertscher C., Gaži P., Kiayias A., Russell A., Zikas V. Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability. ACM Conference on Computer and Communications Security – ACM CCS 2018. 2018. pp. 913–930.
20. David B., Gaži P., Kiayias A., Russell A. Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain. Advances in Cryptology – EUROCRYPT 2018. 2018. vol. 10821. pp. 66-98.
21. Garay J., Kiayias A., Leonardos N. The Bitcoin Backbone Protocol with Chains of Variable Difficulty. Advances in Cryptology – CRYPTO 2017. 2017. vol. 10401. pp. 291-323.
22. Bentov I., Gabizon A., Mizrahi A. Cryptocurrencies without Proof of Work. *Financial Cryptography and Data Security*. 2016. vol. 9604. pp. 142-157.
23. David B., Dowsley R., Larangeira M. ROYALE: A Framework for Universally Composable Card Games with Financial Rewards and Penalties Enforcement. *Financial Cryptography and Data Security*. vol. 11598. pp. 282-300.
24. Duan S., Meling H., Peisert S., Zhang H. BChain: Byzantine Replication with Hight Throughput and Embedded Reconfiguration. *Principles of Distributed Systems* – OPODIS 2014. 2014. vol. 8878. pp. 91-106.