Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ ИУ «ИНФОРМАТИКА И СИСТЕМЫ УПРАВЛЕНИЯ»

КАФЕДРА ИУ7 «ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЭВМ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ»

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

НА ТЕМУ:

Методы решения задачи византийских генералов

Студент **ИУ7-55Б** _____ **О.Н. Талышева**

Руководитель _____ **А.С. Кострицкий**

2024 г.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Московский государственный технический университет имени Н.Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

УТВЕРЖДАЮ

Заведующий кафедрой ИУ7
(Индекс)
_____ И. В. Рудаков
(И.О.Фамилия)
«20» сентября 2024 г.

З А Д А Н И Е
на выполнение научно-исследовательской работы

по теме

Методы решения задачи византийских генералов

Студент группы **ИУ7-55Б**

Талышева Олеся Николаевна

Направленность НИР (учебная, исследовательская, др.): **учебная.**

Источник тематики (кафедра, предприятие, НИР): **кафедра.**

График выполнения НИР: 25% к 4 нед., 50% к 9 нед., 75% к 13 нед., 100% к 15 нед.

Техническое задание

Проанализировать предметную область: ввести основные определения, обозначить основные вехи развития. Формализовать задачу византийских генералов. Перечислить методы или группы методов решения, сформулировать критерии сравнения. Сравнить перечисленные методы по сформулированным критериям.

Оформление научно-исследовательской работы:

1. Расчетно-пояснительная записка на **12-15** листах формата А4.
2. Перечень графического (иллюстративного) материала (плакаты, слайды и т. п.): Презентация на **3** слайдах. В презентации должны быть отражены формализованная постановка задачи и результаты сравнения методов решения.

Дата выдачи задания «20» сентября 2024 г.

Руководитель НИР _____ **А. С. Кострицкий**
(Подпись, дата) (И.О.Фамилия)

Студент _____ _____
(Подпись, дата) (И.О.Фамилия)

Временная метка генерации: 24.11.24 г., 22:06:48

РЕФЕРАТ

Научно-исследовательская работа содержит 18 с., 1 рис., 1 табл., 10 ист., 1 прил.

Ключевые слова:

Византийские генералы, распределенные системы, консенсус, алгоритмы, отказоустойчивость.

Объект исследования:

Решение задачи византийских генералов — классической проблемы в распределенных системах, связанной с достижением консенсуса в условиях ненадежных узлов.

Результаты работы:

1. Изучена предметная область, определены основные понятия и рассмотрены исторические аспекты проблемы;
2. Сформулирована и формализована задача византийских генералов;
3. Описаны существующие методы решения проблемы;
4. Разработаны критерии для сравнения и оценки алгоритмов;
5. Проведён анализ различных методов с использованием предложенных критериев и сделаны выводы.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Современные распределённые системы играют центральную роль в различных областях информационных технологий: от баз данных и систем управления до облачных вычислений и криптовалют. Их широкое применение обуславливает высокие требования к надёжности, отказоустойчивости и согласованности между компонентами. Однако распределённая природа таких систем сопряжена с рядом фундаментальных проблем, одной из которых является задача достижения консенсуса в условиях ненадёжности некоторых узлов.

Проблема надёжного согласования в распределённых системах впервые была формализована в виде задачи византийских генералов (ЗВГ). Эта задача иллюстрирует ситуацию, в которой несколько сторон (узлов) пытаются прийти к единому решению, несмотря на то, что часть из них может вести себя некорректно — например, из-за сбоев, атак злоумышленников или неправильной конфигурации. Сам термин отсылает к историческим аллюзиям о коммуникации между военачальниками, пытающимися согласовать действия в условиях возможного предательства, что подчёркивает сложность задачи.

Развитие ЗВГ началось с работ Лесли Лампорта, Роберта Шостака и Маршалла Пиза в 1982 году, где была представлена теоретическая основа проблемы и предложены базовые алгоритмы её решения. С тех пор задача стала основой для разработки множества алгоритмов и протоколов, включая PBFT (Practical Byzantine Fault Tolerance), Raft и популярные механизмы консенсуса в блокчейне, такие как Proof-of-Work и Proof-of-Stake.

Задача ЗВГ имеет важное практическое значение. Она лежит в основе отказоустойчивости критически важных систем, таких как банковские платформы, авиационные и медицинские системы управления, а также распределённые реестры. Её решение позволяет минимизировать риски, связанные с несанкционированным поведением участников системы, и повысить уровень доверия в децентрализованных сетях.

Целью данной научно-исследовательской работы является исследование методов решения задачи византийских генералов.

В рамках работы были поставлены следующие задачи:

1. Провести анализ предметной области: дать основные определения, изучить исторические аспекты развития проблемы;
2. Формализовать задачу византийских генералов;
3. Перечислить существующие методы решения проблемы;
4. Разработать критерии сравнения алгоритмов;
5. Провести сравнительный анализ методов решения на основе сформулированных критериев.

1. Аналитиз предметной области

В данном разделе будут представлены основные определения, связанные с методами решения задачи византийских генералов, исторические вехи развития проблемы.

1.1. Основные определения

Распределённая система – совокупность взаимодействующих узлов, работающих совместно для достижения общей цели.

Отказоустойчивость – способность системы продолжать функционировать корректно при наличии сбоев.

Консенсус – соглашение между узлами системы относительно общего состояния или принятого решения. Основное требование консенсуса – выполнение двух свойств:

1. Согласованность (Agreement) – все честные узлы принимают одинаковое решение.
2. Достоверность (Validity) – если командующий честен, принятое решение совпадает с его предложением.

1.2. История развития проблемы византийских генералов

Формулировка проблемы

Проблема византийских генералов, концепция, имеющая ключевое значение в области информатики и распределённых систем, была впервые представлена в 1982 году Лесли Лэмпортом, Робертом Шостаком и Маршаллом Пизом [1]. В своей работе они описали сценарий, в котором несколько генералов должны согласовать стратегию атаки или отступления, несмотря на наличие предателей, которые могут распространять ложную информацию. Это постановка задачи является основой для разработки алгоритмов консенсуса в распределённых системах, где некоторые узлы могут быть ненадёжными или действовать злонамеренно.

Исследование получило широкую поддержку со стороны таких престижных организаций, как НАСА, Командование систем противоракетной обороны и Исследовательское бюро армии. Эти исследования подчеркнули значимость проблемы не только в военной связи, но и в широком спектре компьютерных систем. Вопрос достижения согласия между различными компонентами системы стал важной частью теории отказоустойчивости распределённых систем. Также проблема была рассмотрена в контексте новых подходов к дистрибуции вычислительных процессов и в применении для решения задач в распределённых вычислительных системах. [7]

Ранние подходы к решению

После публикации работы Лэмпорта, Шостака и Пиза начались активные исследования по решению задачи. Одним из важнейших результатов стало доказательство,

что для обеспечения консенсуса в византийской модели необходимо минимум $3f + 1$ узлов в системе, где f — количество потенциально ненадёжных узлов. Это открытие стало основой для ограничения разработок в области распределённых систем.

В ответ на вызовы, стоящие перед распределёнными системами, Лэмпорт предложил алгоритм, использующий гарантированную доставку сообщений для обеспечения согласованности. Однако такие методы оказались крайне затратными по вычислительным ресурсам и применимыми только для синхронных систем с заранее известными задержками.

Развитие BFT-протоколов

В 1990-х годах были разработаны более практичные алгоритмы византийской отказоустойчивости (BFT). Наибольшее внимание привлёк алгоритм PBFT (Practical Byzantine Fault Tolerance), предложенный Барбарой Лисков и Мигелем Кастро в 1999 году. Этот протокол был ориентирован на асинхронные системы с неизвестными задержками и позволил значительно повысить отказоустойчивость распределённых сетей, однако он столкнулся с проблемами масштабируемости.

Проблема в эпоху блокчейна

В 2008 году Сатоши Накамото предложил революционное решение византийской проблемы в децентрализованных сетях. Он представил алгоритм доказательства работы (Proof-of-Work, PoW), который стал основой для первой криптовалюты — Bitcoin. Этот алгоритм позволил достичь консенсуса в среде, где узлы не доверяют друг другу и могут быть ненадёжными. [7].

Накамото успешно объединил достижения из области децентрализованных технологий, предложив решение, которое устраняет необходимость в доверенных третьих сторонах и делает систему безопасной и масштабируемой.

Насущность в современности

Проблема византийских генералов остаётся важной задачей в области распределённых технологий. Современные исследования сосредоточены на разработке более производительных и энергоэффективных протоколов консенсуса, способных работать в условиях больших сетей и высокой нагрузки.

Алгоритмы византийского консенсуса нашли широкое применение в различных областях, включая блокчейн, распределённые базы данных, системы интернета вещей (IoT) и кибербезопасность. Эти алгоритмы продолжают служить основой для новых децентрализованных технологий, обеспечивая надёжность, безопасность и масштабируемость современных систем.

2. Формализация задачи византийских генералов

Византия. Ночь перед великим сражением с противником. Византийская армия состоит из n легионов, каждый из которых командует свой генерал. Также у армии есть главнокомандующий, которому подчиняются генералы. В то же время империя находится в упадке, и любой из генералов, а также главнокомандующий, могут быть предателями, заинтересованными в её поражении.

Ночью каждый из генералов получает от предводителя приказ о варианте действий в 10 часов утра (время одинаковое для всех и известно заранее): «атаковать противника» или «отступать».

Возможные исходы сражения

- Если все верные генералы атакуют — Византия уничтожит противника (благоприятный исход).
- Если все верные генералы отступят — Византия сохранит свою армию (промежуточный исход).
- Если некоторые верные генералы атакуют, а некоторые отступят — противник уничтожит всю армию Византии (неблагоприятный исход).

Графически задача представлена на рисунке 1.

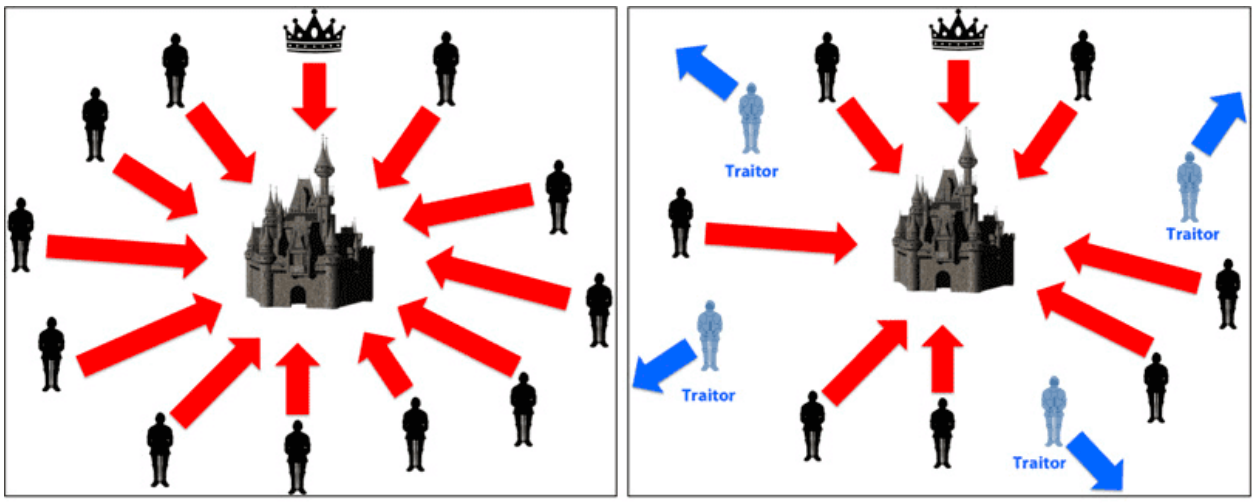

Рисунок 1 – Иллюстрация к «задаче византийских генералов»

Также следует учитывать, что если главнокомандующий является предателем, он может дать разным генералам противоположные приказы, чтобы обеспечить уничтожение армии. Следовательно, генералам лучше не доверять его приказам. Если же каждый генерал будет действовать полностью независимо от других (например, сделает случайный выбор), то вероятность благоприятного исхода весьма низка. Поэтому

генералы нуждаются в обмене информацией между собой, чтобы прийти к единому решению. [2]

Цель задачи:

Найти алгоритм, который позволит лояльным генералам достичь консенсуса, несмотря на присутствие m предателей, которые могут пытаться помешать принятию общего решения.

Задача византийских генералов является классической проблемой, моделирующей ситуации, где необходимо достичь согласия в условиях ненадежных участников и искажений информации.

3. Методы решения задачи византийских генералов

3.1. Классификация методов

Методы решения проблемы византийских генералов можно классифицировать на несколько категорий в зависимости от подходов к обеспечению консенсуса и требований к системе:

1. Детерминированные алгоритмы
   Эти методы основаны на чётко определённых правилах и последовательностях действий, например, алгоритмы, предполагающие гарантированную доставку сообщений. Примером является алгоритм Лэмпорта.

2. Статистические методы
   Используют вероятностный подход для достижения консенсуса, как, например, в алгоритмах, связанных с доказательством выполнения работы (Proof-of-Work, PoW).

3. Асинхронные протоколы
   Методы, позволяющие работать в системах с неизвестными задержками, такие как алгоритмы византийской отказоустойчивости (BFT, Byzantine Fault Tolerance).

4. Гибридные подходы
   Комбинируют детерминированные и статистические методы для достижения более высокой эффективности и отказоустойчивости. Эти подходы часто применяются в современных блокчейн-системах.

5. Алгоритмы с дополнительными доверенными узлами
   Включают использование специальных доверенных узлов (например, репутационных систем) для повышения безопасности.

Каждая из этих категорий находит применение в зависимости от особенностей системы и её требований к производительности и безопасности.

3.2. Описание методов

В этом разделе будут рассмотрены основные алгоритмы, применяемые для решения задачи византийских генералов.

3.2.1 Алгоритм Лэмпорта

Решение задачи византийских генералов (ЗВГ) зависит от того какой тип имеют сообщения — устные или подписанные. Устными считаются такие сообщения, содержимое которых находится под абсолютным контролем отправителя. Далее приведено решение в случае устных сообщений (OM – Oral Messages).

Теорема

1. Если число лояльных генералов $n \leq 2m$, где m — число предателей, то задача византийских генералов не имеет решения.

2. Если $n \geq 2m+1$, задача ЗВГ разрешима.

Доказательство теоремы можно свести к случаю $n = 3$, где один из генералов является предателем.

Предположения для устных сообщений

A1. Каждое посланное сообщение доставляется неповреждённым.

A2. Получателю сообщения известен его отправитель.

A3. Отсутствие сообщения может быть обнаружено.

Предполагается, что каждый генерал имеет возможность прямой связи с любым другим генералом. Если сообщение от генерала не поступило, по умолчанию считается, что его решение — «ОТСТУПАТЬ».

Алгоритм $OM(m)$ определяется индуктивно по $m \in \mathbb{N}$. Он задаёт правило, по которому каждый генерал передаёт своё решение другим генералам. Алгоритм основан на функции `majority`, которая определяется следующим образом:

$$\texttt{majority}(v_1, \ldots, v_{n-1}) = v_i \text{если большинство значений из } \{v_1, \ldots, v_{n-1}\} \text{ равно } v_i$$

Функция `majority` используется для достижения согласованности между генералами в условиях возможного наличия предателей. [8]

Алгоритм $OM(0)$:

1. Генерал посылает своё решение другим генералам.

2. Каждый генерал использует решение, переданное ему другим генералом, или принимает решение «ОТСТУПАТЬ», если сообщение не получено.

Алгоритм $OM(m)$, $m > 0$:

1. Генерал посылает своё решение другим генералам.

2. Каждый i-й генерал, получивший от другого генерала решение v_i (или, если решение не получено, считает его «ОТСТУПАТЬ»), высылает всем оставшимся $n-2$ генералам это решение, принятое по алгоритму $OM(m-1)$.

3. Для каждого i и для каждого $j \neq i$, пусть v_j — это решение, которое генерал i получает от генерала j на этапе (2) (используя алгоритм $OM(m-1)$), или считает этим решением «ОТСТУПАТЬ», если решение не получено. Генерал i принимает решение:

$$\texttt{majority}(v_1, \ldots, v_{n-1}).$$

3.2.2 Алгоритм Proof of Work

Главной идеей данного алгоритма является соглашение генералами выполнять заранее определенный протокол, который включает решение криптографической задачи. Решение этой задачи сложно для отправителя, но легко проверяется остальными участниками.

Пошаговый алгоритм:

1. Формирование сообщения
   Генерал создаёт план атаки и добавляет уникальный одноразовый номер (nonce):
   $$M = \text{plan} + \text{nonce}.$$
2. Решение криптографической задачи:
   (a) Генерал вычисляет хэш сообщения $H(M)$.
   (b) Проверяет, удовлетворяет ли $H(M)$ заданному условию (например, содержит k начальных нулей).
   (c) Если нет, увеличивает nonce и повторяет вычисления.
3. Отправка сообщения
   Генерал передаёт сообщение M остальным генералам.
4. Проверка
   (a) Каждый генерал проверяет, соответствует ли $H(M)$ заданным требованиям.
   (b) Если $H(M)$ некорректен, сообщение отвергается.
5. Принятие решения
   (a) Если большинство генералов подтвердили сообщение, план принимается.
   (b) Иначе сообщение считается недействительным.

Система устойчива до тех пор, пока злоумышленники не захватят более 50% вычислительных мощностей сети. [4]

3.2.3 Алгоритм Proof of Stake

Алгоритм Proof of Stake (PoS) можно представить как систему, где генералы принимают решения на основе зависит от процента их солдат в общей численности армии. Этот процесс позволяет получить консенсус, где вероятность принятия решения зависит от доли каждого генерала.

Пошаговый алгоритм:

1. Формирование ставки "Вес"каждого генерала определяется количеством солдат в его армии в зависимости от суммарного количества воинов. Эта доля будет влиять на его шанс быть выбранным для принятия решения или выдвижения нового плана.

2. Выбор генерала для выдвижения плана
   Выбор решения происходит случайным образом, но вероятность зависит от ставки, выдвинувших предложения по дальнейшим действиям генералов.

3. Предложение плана
   Генерал, выбранный для предложения решения, определяет атаковать или отступать. Этот план будет основой для дальнейших действий.

4. Проверка и одобрение плана
   Остальные генералы проверяют предложенный план и решают, поддержать его или нет. Каждый командир будет учитывать, насколько справедливым или правдоподобным кажется предложение, и, в зависимости от его ставки, может принять решение о поддержке.

5. Принятие решения
   Если большинство генералов (включая тех, кто имеет большую долю в войсках) поддерживают план, он принимается. Если же план не получает поддержку большинства, он отклоняется.

Таким образом, вероятность принятия решения зависит от доли каждого генерала в общей армии: чем больше у генерала солдат, тем выше вероятность того, что его предложение будет принято.

Эта система также устойчива, пока предатели не захватят более 50% доли в войсках. [9]

3.2.4 Алгоритм Delegated Proof of Stake

Алгоритм Delegated Proof of Stake (DPoS) можно представить как систему, где генералы достигают консенсуса путем делегирования полномочий наиболее доверенным из них. Этот процесс обеспечивает высокую производительность сети и одновременно поддерживает демократическое управление через голосование.

Пошаговый алгоритм:

1. Выбор делегатов (свидетелей)
   Все генералы голосуют за доверенных кандидатов, которые представляют их интересы. Голоса взвешиваются в зависимости от доли солдат генерала в общей численности армии. Топ-N кандидатов становятся делегатами.

2. Создание блоков

   Делегаты поочередно выдвигают решения (атаковать или отступать), создавая "блоки"предложений. Очередность делегатов заранее определена.

3. Валидация решений

   Остальные делегаты проверяют предложения на корректность: если более 2/3 делегатов поддерживают предложение, оно принимается.

4. Обновление списка делегатов

   Если делегат работает неэффективно или действует во вред сети, он может быть смещён голосованием генералов. Это обеспечивает динамическую адаптацию к изменениям в составе армии.

Таким образом, DPoS обеспечивает быстрое и эффективное принятие решений, сохраняя устойчивость системы, пока доверенные делегаты остаются лояльными. Эта модель позволяет обрабатывать большее количество транзакций в секунду (TPS) по сравнению с PoW и PoS. [10]

4. Оценка и сравнение алгоритмов

4.1. Критерии сравнения методов

Для сравнения алгоритмов решения задачи византийских генералов будут использоваться следующие критерии:

1. Тип системы: синхронная или асинхронная.
2. Устойчивость к предателям: минимальное количество лояльных узлов, необходимое для достижения консенсуса.
3. Эффективность: количество сообщений или вычислительных ресурсов, необходимых для работы алгоритма.
4. Масштабируемость: способность алгоритма функционировать с увеличением числа участников.
5. Обеспечение безопасности: устойчивость к различным видам атак.
6. Область применения: в каких типах распределённых систем используется алгоритм.

4.2. Сравнительный анализ

По сформулированным выше критериям была составлена таблица рассмотренных методов решения проблемы византийских генералов (см таблицу 1).

Критерий	Алгоритм Лэмпорта	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated Proof of Stake (DPoS)
Тип системы	Синхронная	Асинхронная	Асинхронная	Асинхронная
Устойчивость к предателям	$n \geq 2m+1$	$> 50\%$ вычислительных мощностей честных узлов	$> 50\%$ доли стейка у честных узлов	$> \frac{2}{3}$ голосов доверенных делегатов
Эффективность	Высокая (при малом n)	Низкая (энергоёмкость)	Средняя (меньше PoW)	Высокая (низкая задержка)
Масштабируемость	Ограниченная n	Ограниченная скоростью вычислений	Высокая	Очень высокая
Безопасность	Высокая	Высокая, но уязвима к 51%-атаке	Высокая (при распределённой доле)	Зависит от честности делегатов
Область применения	Надёжные синхронные сети	Криптовалюты, распределённые сети	Криптовалюты, DeFi	Высоконагруженные блокчейн-системы

Таблица 1 – Сравнение алгоритмов решения задачи византийских генералов.

4.3. Выводы

Благодаря проведённому анализу можно сделать следующие выводы:

1. Алгоритм Лэмпорта лучше подходит для небольших систем с гарантированной синхронностью.
2. PoW обеспечивает высокий уровень безопасности, но требует больших вычислительных затрат, поэтому подходит для систем, где приоритет — децентрализация (например, Bitcoin).
3. PoS улучшает энергоэффективность по сравнению с PoW, сохраняя безопасность, что делает его популярным выбором для современных криптовалют (например, Ethereum 2.0).
4. DPoS оптимален для высоконагруженных систем, где важна производительность и масштабируемость, но требует доверия к делегатам.

ЗАКЛЮЧЕНИЕ

В результате выполнения научно-исследовательской работы на тему "Методы решения задачи византийских генералов":

1. Был проведён анализ предметной области: даны основные определения, изучены исторические аспекты развития проблемы;
2. Формализована задача византийских генералов;
3. Перечислены существующие методы решения проблемы;
4. Разработаны критерии сравнения алгоритмов;
5. Проведён сравнительный анализ методов решения на основе сформулированных критериев.

Все задачи работы выполнены, цель достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems, 4(3), 382–401. SRI International. DOI: [Insert DOI if available].

2. Вахрамов, С. В. (n.d.). Решение «Задачи византийских генералов» с помощью принципов блокчейна Bitcoin. Факультет информатики и робототехники, Уфимский государственный авиационный технический университет. e-mail: s@vakhramoff.ru.

3. Инженерные классы Блокчейн. Лекция 4. Задача о византийских генералах и алгоритмы консенсуса [Электронный ресурс]. – URL: https://vk.com/@rtublockchain-lekciya-4-zadacha-o-vizantiiskih-generalah-i-algoritmy-konse (дата обращения: 05.11.2024).

4. Погорелов, А. М., & Михеенко, Д. С. (2022). Проблема византийских генералов в блокчейн-технологиях. Византийская отказоустойчивость. Основы алгоритмов консенсуса. Юный ученый, 3(55), 41–43. URL: https://moluch.ru/young/archive/55/2835/ (дата обращения: 12.11.2024).

5. Задача византийских генералов: история и решение. (2022). Education. Forklog. URL: https://hub.forklog.com/zadacha-vizantijskih-generalov-istoriya-i-reshenie/.

6. Разъяснение Задач Византийских Генералов. (2018). Binance Academy. URL: https://academy.binance.com/ru/articles/byzantine-fault-tolerance-explained (дата обращения: 12.11.2024).

7. Плизио. (2024, 11 января). Что такое проблема византийских генералов? Plisio. URL: https://plisio.net/ru/blog/what-is-the-byzantine-generals-problem (дата обращения: 13.11.2024).

8. Проблема византийских генералов. (2020, 30 июня). URL: https://vmath.ru/vf5/algorithms/bft (дата обращения: 05.12.2024).

9. Алгоритм консенсуса Proof-of-Stake (PoS): как он работает и почему так популярен. (2022, 03 октября). Forklog. URL: https://forklog.com/cryptorium/chto-takoe-proof-of-stake-pos (дата обращения: 10.12.2024).

10. Разъяснение Delegated Proof of Stake. (2018, 27 ноября; обновлено 2023, 20 апреля). Binance Academy. URL: https://academy.binance.com/ru/articles/delegated-proof-of-stake-explained (дата обращения: 11.12.2024).

ПРИЛОЖЕНИЕ А

Презентация к научно-исследовательской работе из 3-ёх слайдов.