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 **ИУ7-52Б** _____ **Е.Д. Пермякова**

Руководитель _____ **А.С. Кострицкий**

2024 г.

РЕФЕРАТ

Расчетно-пояснительная записка 14 с., 1 рис., 1 таблиц, 18 источников, 1 приложение.

ЗАДАЧА ВИЗАНТИЙСКИХ ГЕНЕРАЛОВ, КОНСЕНСУС, РАСПРЕДЕЛЕННЫЕ СИСТЕМЫ

Цель работы — рассмотрение методов решения задачи византийских генералов.

В рамках научно-исследовательской работы была формализована задача византийских генералов, были рассмотрены методы ее решения и проведено сравнение основных методов по критериям устойчивости алгоритма к византийским отказам и анонимности узлов распределенной системы.

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем отчете о НИР применяют следующие термины с соответствующими определениями

Блокчейн-технология – выстроенная по определённым правилам непрерывная последовательная цепочка блоков, содержащая информацию [1]

Отказ системы – поведение системы, не удовлетворяющее ее спецификациям [2]

Распределенная система – совокупность автономных вычислительных элементов, которая для его пользователей является единой связанной системой [3]

ВВЕДЕНИЕ

При создании распределенных систем важным является организации взаимодействия ее одновременно работающих элементов между собой и принятия ими единого решения, то есть достижения консенсуса, даже в ситуации, когда некоторые узлы системы начинают работать неверно, злонамеренно или в случае поломки [4]. Эта проблема формулируется как задача византийскиих генералов.

Целью данной работы является рассмотрение методов решения задачи византийских генералов.

Для достижения поставленной цели необходимо решить следующие задачи:

1) ввести основные определения;
2) обозначить основные вехи развития;
3) формализовать задачу византийских генералов;
4) перечислить методы решения;
5) сформулировать критерии сравнения;
6) сравнить перечисленные методы по сформулированным критериям;

1 Анализ предметной области

В данном разделе описывается изначальная постановка и формализация задачи византийских генералов, также рассматривается область ее применения.

1.1 Формализация задачи

Задача византийских генералов была сформулирована в 1982 году в исследовании Л. Лэмпорт, Р. Шостак и М. Пиз [5] и описывала ситуацию, в которой группа генералов византийской армии вместе со своими войсками расположена вокруг вражеского лагеря. Они могут общаться только через посланников и должны договориться об общем плане действий: отступать или нападать. Однако один или несколько из них могут быть предателями, которые попытаются запутать остальных, посылая при этом ложные данные. Проблема заключается в том, чтобы найти алгоритм, который обеспечит достижение согласия среди преданных генералов.

Формальное описание данной задачи заключается в том, что надо найти метод достижения консенсуса в распределенной системе, при условии, что некоторые ее элементы могут работать неверно. В качестве входных данных алгоритму подаются исправные и неисправные узлы системы. Выходными данными является единое решение, принятое для всех узлов в зависимости от функций, выполняемых самой системой.

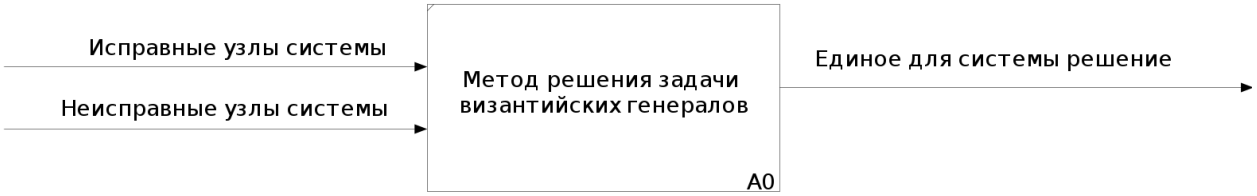

Рисунок 1.1 – Формализация задачи византийских генералов в нотации IDEF0

1.2 Область применения

Впервый задача византийских генералов была сформулирована в 1982 году в статье Л. Лэмпорт, Р. Шостак и М. Пиз [5]. В данной работе поднималась проблема взаимодействия элементов распределенной системы между собой,

которая иллюстрировалась на примере генералов, которым нужно договориться между собой о плане наступления.

На основе поставленной задачи в исследовании Барбары Лисков и Мигель Кастро [6] был предложен алгоритм практической византийской отказоустойчивость, актуальность которого заключалась в необходимости высоконадежных систем, которые обеспечивают корректное обслуживание без сбоев.

Следующим важным событием являлась публикация Сатоши Накамото в 2008 году идеи алгоритма достижения консенсуса в децентрализованных системах не требующих аутентификации ее узлов [7]. Данная реализация алгоритма доказательста работы, положила начало развития блокчейн-технологии.

В современном мире задача византийских генералов является достаточной актуальрой и рассматривается при реализации технологии распределённых реестров [8], одной из которых является блоекчейн, при созданиии распределенных операционных систем [2] или интернет протоколов [9].

2 Методы решения задачи византийских генералов

Существует большое количество алгоритмов достижения консенсуса в распределенных системах, обладающих византийской отказоустойчивостью. В данной научной работе рассматриваются основные из них, которые легли в основу создания всех остальных.

2.1 Практическая византийская отказоустойчивость

Метод практической византийской отказоустойчивости (Practical Byzantine Fault Tolerance, PBFT), предложенный в 2002 году Барбарой Лисков и Мигель Кастро [6], является алгоритмом основанном на передаче подписанных сообщений между репликами.

Подпись сообщений производится с использованием методов симметричной криптографии, для аутентификации самих узлов в системе.

При условии наличия в системе, состоящей из $3k + 1$ узлов, не более k неисправных, алгоритм гарантирует ее верную работу. [3].

Существует не малое количество модификаций данного алгоритма: метод sdBFT (stake distributed BET) [10], который позволяет увеличить количество узлов, участвующих в достижении консенсуса без потери скорости поступления транзакций; или семейство протоколов Internet Computer Consensus (ICC) [9], основным достоинство которого является скорость работы алгоритма равная скорости фактической сетевой задержки, а не с некоторой верхней границей сетевой задержки, в случае когда лидер честен.

2.2 Доказательство выполнения работы

Метод доказательства выполнения работы (Proof of Work, PoW), разработанный Сатоши Накамото [7],заключается в требовании от узла вычисления значения, «nonce», которое при хэшировании начинается с определенного количества нулевых битов, то есть вычислить значение хеша заголовка блока, который при этом может регулярно меняться.

После получения искомого значения остальным элементам сети надо взаимно подтвердить корректность полученного хеша. Таким образом транзакции, хранящиеся в новом блоке, проверяются в случае мошенничества.

При последовательном решении поставленной задачи честными узлами

образуется длинная цепочка связных блоков. И для изменения ее элементов необходимо будет повторить проверку его работоспособности и всех блоков после него, а затем догнать и превзойти работу честных узлов.

Алгоритм PoW обеспечивает безопасность системы, только когда мощность одного вычислительного узла не превышает половины мощностей всей сети [1].

Из-за необходимости произведения огромного количества математических операций в данном методе, а вследствие и большого потребления электроэнергии, был придуман более эффективный и экономичный алгоритм Proof of Stake (PoS), в котором для подключения к сети блока необходимо доказать владение определенным количеством валюты.

2.3 Сравнение методов решения задачи византийских генералов

В качестве сравнения рассмотренный методов решения задачи византийских генералов были выбраны критерии:

— анонимность узлов, так как в некоторых распределенных системах, например, в открытых блокчейн сетях, направленных на децентрализацию, требуется конфиденциальность элементов;

— уровень устойчивости алгоритма, который определяется отношением неисправных элементов системы(k) к исправным(n);

Таблица 2.1 – Сравнение методов решения задачи византийских генералов

	PBFT	PoW
Анонимность узлов	-	+
Уровень устойчивости алгоритма	$3k + 1 \leq n$	$2k \leq n$

При сравнении рассматриваемых методов, можно сделать вывод, что алгоритм PoW, основанный на доказательстве, хоть и сохраняет конфиденциальность своих узлов, но обладает меньшей отказоустойчивостью, чем алгоритм PBFT, основанный на подписях и опросе узлов.

ЗАКЛЮЧЕНИЕ

В ходе научно-исследовательской работы были рассмотрены методы решения задачи византийских генералов и проведено их сравнение по критериям устойчивости алгоритма к византийским отказам и анонимности узлов распределенной системы.

В процессе выполнения данной работы были выполнены все задачи:

1) ввести основные определения;
2) обозначить основные вехи развития;
3) формализовать задачу византийских генералов;
4) перечислить методы решения;
5) сформулировать критерии сравнения;
6) сравнить перечисленные методы по сформулированным критериям;

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Носиров З. А. Фомичев В. М. Анализ блокчейн-технологии: основы архитектуры, примеры использования, перспективы развития, проблемы и недостатки // Системы управления, связи и безопасности. 2021. № 2. С. 37-75. DOI: 10.24412/2410-9916-2021-2-37-75. URL: Режим доступа: https://sccs.intelgr.com/archive/2021-02/03-Nosirov.pdf (дата обращения: 17.12.2024).

2. В.А. Крюков. Операционные системы распределенных вычислительных систем. Лекции для 4 курса факультета ВМиК МГУ.

3. Стин ван М. Таненбаум Э. С. Распределенные системы. ДМК Пресс, 2021. с. 584. пер. с англ. В. А. Яроцкого.

4. Никольский И. М. Распределенная обработка данных: учебно-методическое пособие. Издательство Московского университета, 2023. С. 28, [1]. Электронное издание сетевого распространения. — (Библиотека факультета ВМК МГУ).

5. Leslie Lamport Robert Shostak, Pease Marshall. The Byzantine Generals Problem. 1982. URL: Режим доступа: https://lamport.azurewebsites.net/pubs/byz.pdf (дата обращения: 17.12.2024).

6. Research) Migel Castro (Microsoft, for Computer Science) Barbara Liskov (MIT Laboratory. Practical Byzantine Fault Tolerance and Proactive Recovery. 2002. URL: Режим доступа: http://vis.usal.es/rodrigo/documentos/papers/PBFT-Castro2002.pdf (дата обращения: 17.12.2024).

7. Nakamoto Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. URL: Режим доступа: https://bitcoin.org/bitcoin.pdf (дата обращения: 17.12.2024).

8. А.С. Тороев А.Б. Сизоненко. Алгоритм достижения консенсуса для распределённых систем обработки данных на основе технологии распределённых реестров. 2021. URL: Режим доступа: https://www.elibrary.ru/download/elibrary_46327552_80713174.pdf (дата обращения: 17.12.2024).

9. Jan Camenisch Manu Drijvers Timo Hanke Yvonne-Anne Pignolet Victor Shoup Dominic Williams. Internet Computer Consensus. 2021. URL: Режим доступа: https://eprint.iacr.org/2021/632.pdf (дата обращения: 17.12.2024).

10. А.П. Бардин А.В. Новицкий Ю.Ю. Шумилов. Обработка ошибочных ситуаций в больших блокчейн-сетях алгоритмом достижения консенсуса, основанном на решении задачи византийских генералов. Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение., 2021. URL: Режим доступа: https://cyberleninka.ru/article/n/obrabotka-oshibochnyh-situatsiy-v-bolshih-blokcheyn-setyah-algorit viewer (дата обращения: 17.12.2024).

Приложение А

Презентация к научно-исследовательской работе состоит из 3 слайдов.