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 «Информатика и системы управления»

КАФЕДРА «Программное обеспечение ЭВМ и информационные технологии»

# РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

## *К НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ*

## *НА ТЕМУ:*

## *«Аналитический обзор алгоритмов консенсуса в распределенных системах»*

Студент ИУ7-52Б (Группа) _____ (Подпись, дата) В. М. Короткая (И. О. Фамилия)

Руководитель курсовой работы _____ (Подпись, дата) К. А. Кивва (И. О. Фамилия)

*2022 г.*

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

Очередной этап технологической революции, происходящей в настоящее время в мире, влечет серьезные изменения в экономике, социальной структуре общества. Массовое применение новых технологических средств, на основе которых осуществляется информатизация, стирает геополитические границы, изменяет образ жизни миллионов людей. Вместе с тем, информационная сфера становиться не только одной из важнейших сфер международного сотрудничества, но и объектом соперничества.

Таким образом появляется возможность перехвата и подмены какой-либо информации в сети.

Для решения данной проблемы существует протокол TLS (Transport Layer Security), криптографический протокол, обеспечивающий защещенную передачу данных в сети Интернет.

Целью данной работы является обзор существующих версий протокола TLS.

Для достижения поставленной цели требуется решить следующие задачи:

- определить основные термины, связанные с протоколом TLS;
- рассмотреть существующие и актуальные версии протокола;
- выделить критерии классификации версий;
- провести классификацию версий.

# 1 Анализ предметной области

Приложения, работающие с большими объемами данных проникли во все сферы нашей жизни. Банковские системы, бронирование отелей, интернет магазинов — все они сталкиваются с задачами надежного хранения и обработки больших объемов данных.

## 1.1 Подходы к организации многосерверных систем

Существует 3 основных подхода к организации систем, состоящих из нескольких вычислительных машин[**burger2019distributed**]:

1. Централизованный
2. Децентрализованный
3. Распределенный

Наиболее простым в организации работы подходом является централизованный. При нем выделяется главный сервер, на который ложится ответственность за управление всем кластером. Зависимые сервера обмениваются сообщениями только с главным сервером и не общаются между собой. Такой подход порождает множество проблем: такими системы являются слабо масштабируемыми и обладают слабой отказоустойчивостью, ведь для приведения системы в неработоспособное состояние достаточно падения только одного главного узла.

Децентрализованный подход пытается решить проблемы централизованного подхода. При нем существуют несколько главных сервером, а так же зависимые от них. Каждых из зависимых серверов общается со своим главным сервером. Такая система является устойчивой к отказу в случае падения одного из главным серверов.

В распределенных системах все узлы системы являются равными, среди нет главных серверов. Каждый из узлов способен обрабатывать запросы. Такая система наиболее устойчива к падению и обладает наилучшей масштабируемостью.

Организация связей в данных подходах изображены на рисунке 1.1.

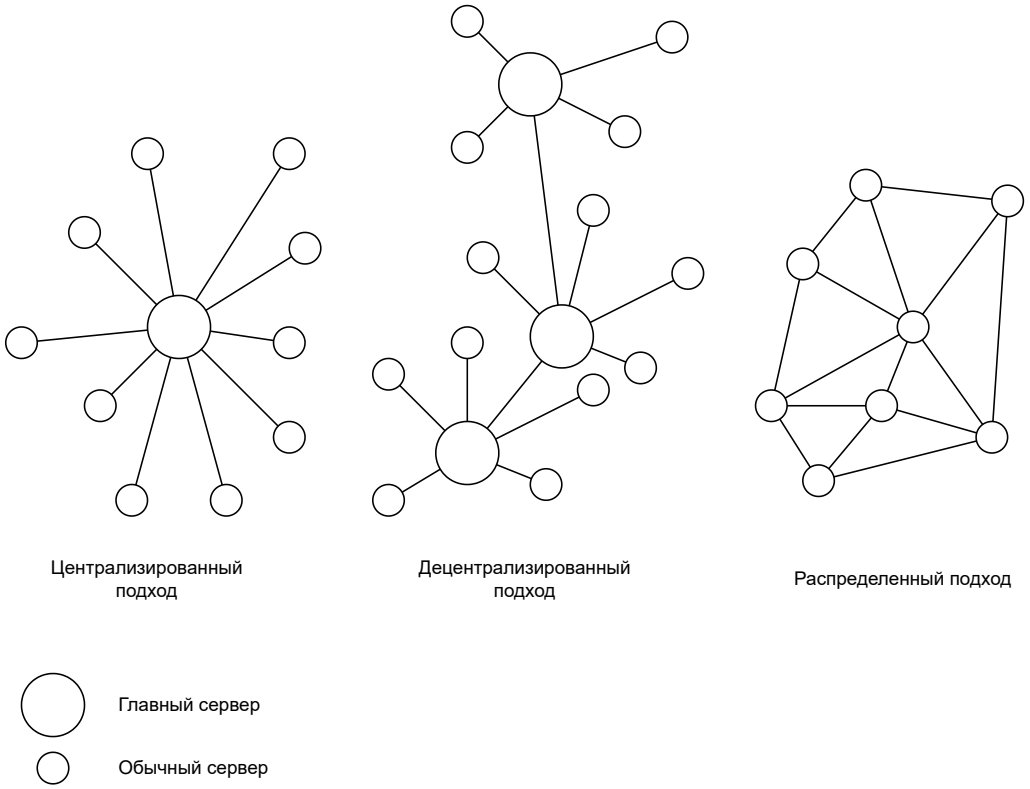


Рисунок 1.1 – Организация связей между серверами

## 1.2 Задача достижение консенсуса

Фундаментальной проблемой в распределенных системах является достижение общей надежности системы. Для ее достижения необходима координация процессов для достижения общего соглашения по поводу принятия или непринятия некоторого значения всей системой — задача консенсуса[**carlsson1992consensus**]. Примерами такой работы может являться соглашение по поводу некоторого единственного значения или задача репликации журнала[**panda2018efficient**].

### 1.2.1 Типы отказоустойчивости

В распределенных системах в работе участвует множество вычислительных машин, каждая из которых может выйти из строя. Рассматривают 2 типа алгоритмов достижения консенсуса по принципу отказоустойчивости:

- устойчивость к падению
- византийская отказоустойчивость

В первом случае рассматриваются сбои связанные с отказом оборудова-

ния, ошибки в программном обеспечении, сбои в сети. Алгоритмы устойчивые к падению не обрабатывают умышленные вредоносные действия в системе. Под византийской же устойчивостью подразумевается обработка в том числе и вредоносных действий узлов: посылка некорректных сообщений, посылка ложной информации, попытка вывести систему из согласованного состояния.

### 1.2.2 Эксклюзивные и инклюзивные алгоритмы

Алгоритмы достижения консенсуса классифицируются по модели обеспечения доступа к сети на следующие типы[**butun2020review**]:

- Эксклюзивные
- Инклюзивные

В эксклюзивных алгоритмах достижения консенсуса принимать участие в работе алгоритма могут только заранее установленные узлы в ограниченном количестве. В инклюзивных алгоритмах такое ограничение снимается, принимать участие в них может любой желающий узел.

## 1.3 Блокчейн

Важным толчком в развитии и разработке алгоритмов консенсуса послужило появление криптовалют, построенных поверх технологии блокчейна.

Блокчейн — выстроенная по определенным правилам непрерывная последовательная цепочка блоков (связный список), содержащих информацию. Связь между блоками обеспечивается не только нумерацией, но и тем, что каждый блок содержит свою собственную хеш-сумму и хеш-сумму предыдущего блока. Изменение любой информации в блоке изменит его хеш-сумму.

Пример цепочки блокчейна приведен на рисунке 1.2

## 1.4 Вывод

В данном разделе была обоснована актуальность поставленной задачи, определены основные термины, связанные с алгоритмами достижения консенсуса.

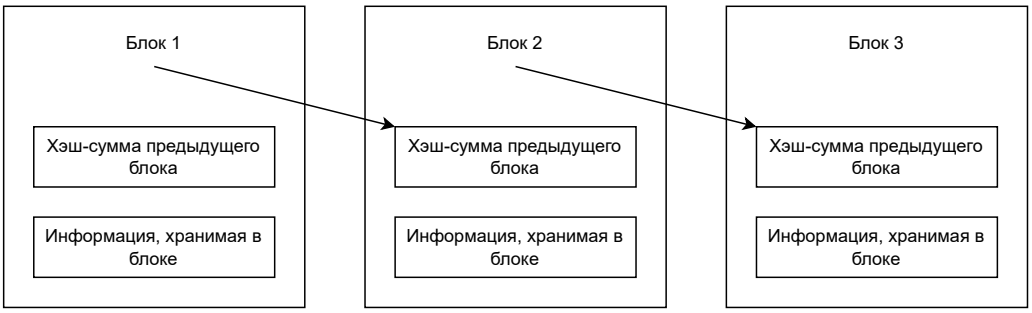


Рисунок 1.2 – Пример цепочки блокчейна