Методы и технологии испытаний информационных систем

Лекция 16

Архитектурные ограничения на тестирование и испытания

Овчинников П.Е.

МГТУ «СТАНКИН»,

ст.преподаватель кафедры ИС

Интернет: базы данных на клиенте

Web SQL (или **Web SQL Database**) — это API веб-страниц для хранения данных в веб-браузере на основе SQL

API поддерживается Google Chrome, Opera, Safari и браузером Android

Консорциум W3C прекратил работу над спецификацией в ноябре 2010 года, в качестве причины завершения спецификации ссылаясь на отсутствие независимых реализаций (т.е. систем баз данных отличных от SQLite в качестве внутреннего интерфейса), из-за чего спецификации этого API не входит в список рекомендованых W3C

IndexedDB — JavaScript интерфейс прикладного программирования (API) клиентского хранилища большого объема структурированных данных, в том числе файлы/blobs

Другими словами это NoSQL хранилище данные в формате JSON внутри браузера

Стандарт разработан W3C и внедрен в браузерах с 2011 года

Интернет: веб-сервер

Веб-сервер — сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медиа-потоком или другими данными.

Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер (см.: Сервер (аппаратное обеспечение)), на котором это программное обеспечение работает.

Веб-серверы могут иметь различные дополнительные функции, например:

- автоматизация работы веб-страниц;
- ведение журнала обращений пользователей к ресурсам;
- аутентификация и авторизация пользователей;
- поддержка динамически генерируемых страниц;
- поддержка HTTPS для защищённых соединений с клиентами.

В терминологии компьютерных сетей, **балансировка нагрузки**, или **выравнивание нагрузки** (англ. *load balancing*) — метод распределения заданий между несколькими сетевыми устройствами (например, серверами) с целью оптимизации использования ресурсов, сокращения времени обслуживания запросов

Интернет: сервер приложений

Сервер приложений (англ. *application server*) — это программная платформа (фреймворк), предназначенная для эффективного исполнения процедур (программ, скриптов), на которых построены приложения.

Сервер приложений действует как набор компонентов, доступных разработчику программного обеспечения через API (интерфейс прикладного программирования), определённый самой платформой.

Для веб-приложений основная задача компонентов сервера — обеспечивать создание динамических страниц. Однако современные серверы приложений включают в себя и поддержку кластеризации, повышенную отказоустойчивость, балансировку нагрузки, позволяя таким образом разработчикам сфокусироваться только на реализации бизнес-логики

В случае Java-сервера приложений, сервер приложений ведёт себя как расширенная виртуальная машина для запуска приложений, прозрачно управляя соединениями с базой данных, с одной стороны, и соединениями с веб-клиентом, с другой

Интернет: веб-служба

Веб-служба, *веб-сервис* (англ. *web service*) — идентифицируемая уникальным веб-адресом (URL-адресом) программная система со стандартизированными интерфейсами, а также HTML-документ сайта, отображаемый браузером пользователя

Веб-службы могут взаимодействовать друг с другом и со сторонними приложениями посредством сообщений, основанных на определённых протоколах (SOAP, XML-RPC и т. д.) и соглашениях (REST)

Веб-служба является единицей модульности при использовании сервис-ориентированной архитектуры приложения

В обиходе *веб-сервисами* называют услуги, оказываемые в Интернете. В этом употреблении термин требует уточнения, идёт ли речь о поиске, веб-почте, хранении документов, файлов, закладок и т. п. Такими веб-сервисами можно пользоваться независимо от компьютера, браузера или места доступа в Интернет

Интернет: сервер баз данных

Сервер баз данных (БД) выполняет обслуживание и управление базой данных и отвечает за целостность и сохранность данных, а также обеспечивает операции ввода-вывода при доступе клиента к информации

Архитектура клиент-сервер состоит из клиентов и серверов. Основная идея состоит в том, чтобы размещать серверы на мощных машинах, а приложениям, использующим языковые компоненты СУБД, обеспечить доступ к ним с менее мощных машин-клиентов посредством внешних интерфейсов

Систе́ма управле́ния ба́зами да́нных, *сокр.* СУБД (англ. *Database Management System*, сокр. DBMS) — совокупность программных и лингвистических средств общего или специального назначения, обеспечивающих управление созданием и использованием баз данных

СУБД — комплекс программ, позволяющих создать базу данных (БД) и манипулировать данными (вставлять, обновлять, удалять и выбирать)

Система обеспечивает безопасность, надёжность хранения и целостность данных, а также предоставляет средства для администрирования БД

Транзакции (информатика)

Транза́кция (англ. *transaction*) — группа **последовательных операций** с базой данных, которая представляет собой логическую единицу работы с данными

Транзакция может быть выполнена либо целиком и успешно, соблюдая целостность данных и независимо от параллельно идущих других транзакций, либо не выполнена вообще, и тогда она не должна произвести никакого эффекта

Транзакции обрабатываются транзакционными системами, в процессе работы которых создаётся история транзакций

Различают последовательные (обычные), параллельные и распределённые транзакции. Распределённые транзакции подразумевают использование более чем одной транзакционной системы и требуют намного более сложной логики (например, two-phase commit — двухфазный протокол фиксации транзакции)

Также в некоторых системах реализованы автономные транзакции, или подтранзакции, которые являются автономной частью родительской транзакции

Транзакция (информатика)

Транзакции (информатика)

Откат (англ. rollback)

Системы обработки транзакций обеспечивают целостность базы данных при помощи записи промежуточного состояния базы данных перед её изменением, а затем, используя эти записи, восстанавливают базу данных до известного состояния, если транзакция не может быть совершена.

Прогон (англ. rollforward)

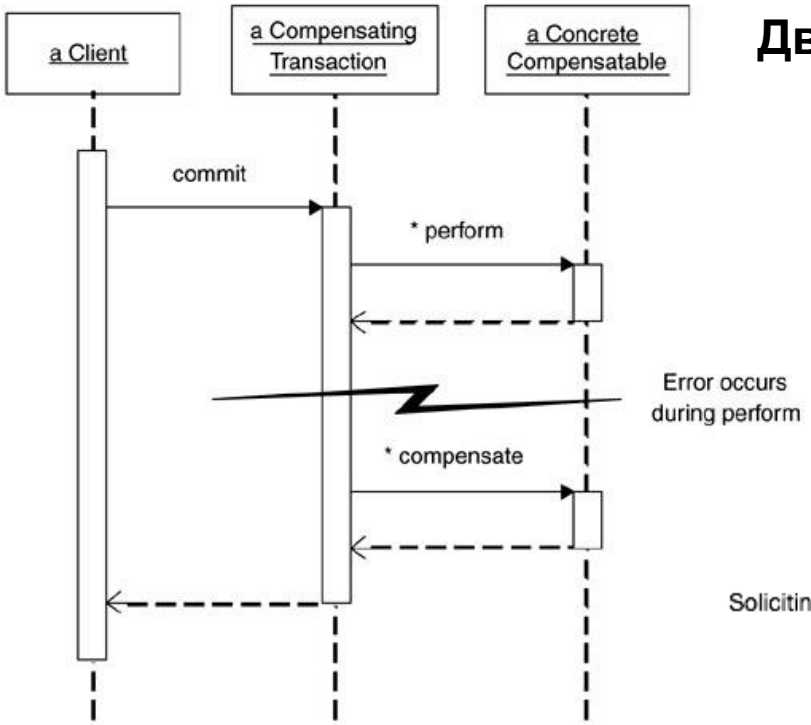
Кроме того, можно вести отдельный журнал всех изменений базы данных (иногда это называется after images); это не требует отката неудачных операций, но это полезно для обновления базы данных в случае отказа базы данных, поэтому некоторые системы обработки транзакций обеспечивают эту функцию.

Взаимная блокировка (англ. deadlocks)

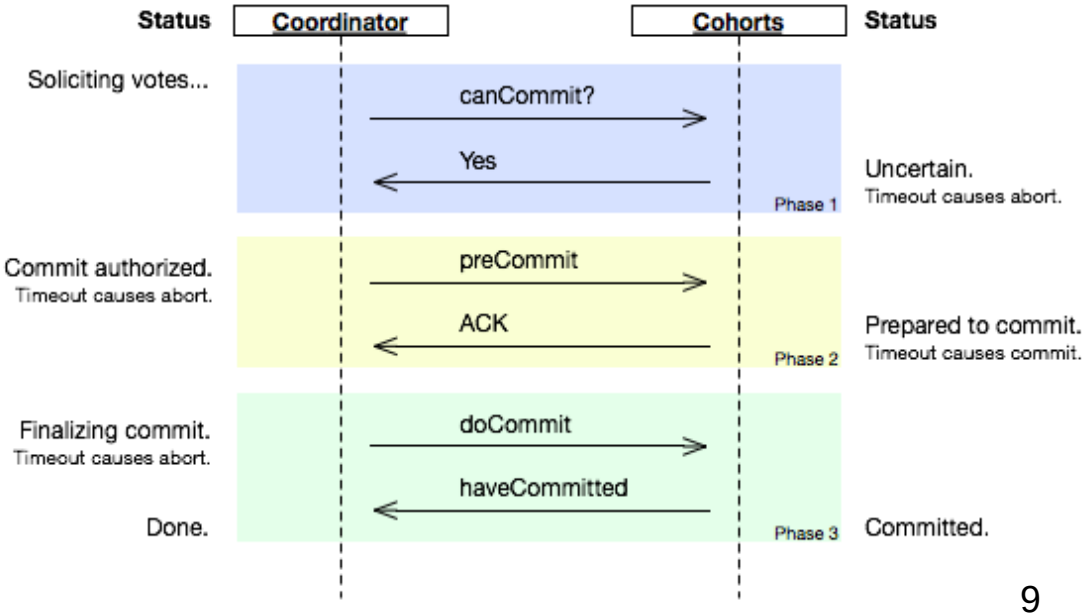
В некоторых случаях, две транзакции могут в ходе их обработки пытаться получить доступ к одной и той же части базы данных в одно и то же время, таким образом, что это будет препятствовать их совершению. Системы обработки транзакций предназначены для обнаружения таких ситуаций. Обычно обе транзакции отменяются и производится откат, а затем они автоматически запускаются в другом порядке, так что взаимоблокировка не повторится.

Многофазная обработка транзакций

Отмена (abort) и компенсация (compensation)



Двухфазная обработка



Трехфазная обработка

Распределенные реестры

Технология распределенных реестров (Distributed ledger technology, DLT)

это технология хранения информации, ключевыми особенностями которой являются:

- совместное использование и синхронизация цифровых данных согласно **алгоритму консенсуса**
- географическое распределение **равнозначных копий** в разных точках по всему миру
- отсутствие центрального администратора

Ключевая особенность распределенного реестра — отсутствие единого центра управления.

Каждый узел составляет и записывает обновления реестра независимо от других узлов. Затем узлы **голосуют за обновления**, чтобы удостовериться, что большинство узлов согласно с окончательным вариантом.

Голосование и достижение согласия в отношении одной из копий реестра называется консенсусом, этот процесс выполняется автоматически с помощью алгоритма консенсуса.

Как только консенсус достигнут, **распределенный реестр обновляется**, и последняя согласованная версия реестра сохраняется в каждом узле.

Распределенные реестры

Задача двух генералов — в вычислительной технике мысленный эксперимент, призванный проиллюстрировать проблему **синхронизации состояния** двух систем по **ненадёжному каналу связи**, в литературе также иногда упоминается как **задача двух армий**.

Определение: две армии, каждая руководимая своим генералом, готовятся к штурму города. Лагеря этих армий располагаются на двух холмах, разделённых долиной. Единственным способом связи между генералами является отправка посыльных с сообщениями через долину. Но долина занята противником и любой из посыльных может быть перехвачен. Проблема заключается в том, что, генералы заранее (пока была связь) приняли принципиальное решение о штурме, но не согласовали точное время штурма.

Задача византийских генералов (англ. *Byzantine fault tolerance (BFT), Byzantine agreement problem, Byzantine generals problem, Byzantine failure*) — в криптологии задача взаимодействия нескольких удаленных абонентов, которые получили приказы из одного центра. Часть абонентов, включая центр, могут быть злоумышленниками.

Распределенные реестры

Теорема CAP (известная также как **теорема Брюера**) —эвристическое утверждение о том, что в любой реализации распределённых вычислений возможно обеспечить не более двух из трёх следующих свойств:

- *согласованность данных* (англ. *consistency*) — во всех вычислительных узлах в один момент времени данные не противоречат друг другу;
- *доступность* (англ. *availability*) — любой запрос к распределённой системе завершается корректным откликом, однако без гарантии, что ответы всех узлов системы совпадают;
- *устойчивость к разделению* (англ. *partition tolerance*) — расщепление распределённой системы на несколько изолированных секций не приводит к некорректности отклика от каждой из секций.

Блокчейн

Blockchain — это один из видов **распределенного реестра**.

Они используют независимые компьютеры (ноды, узлы) для записи, совместного использования и синхронизации транзакций в своих соответствующих электронных реестрах.

Блокчейн организует данные в **блоки**, которые соединены вместе в режиме «**только добавление**».

- блок **не может конфликтовать** с другими данными, которые уже находятся в базе данных (непротиворечивость),
- это система Append-Only (неизменяемость — **нельзя изменить** какую-то часть внутри цепи (один блок), потому что другие блоки содержат информацию о нем),
- сами данные формируются их владельцем (контроль за собственной информацией — у создателя транзакции есть **приватные ключи**, их никто не знает),
- блокчейн можно **копировать** и **просматривать** некоторую информацию (прозрачность)

PKI

Инфраструктура открытых ключей (ИОК, англ. ***PKI*** - *Public Key Infrastructure*) — набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки **криптозадач** на основе **закрытого** и **открытого** ключей.

В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

- **закрытый ключ** (private key) известен только его **владельцу**
- **удостоверяющий центр** создает электронный документ — **сертификат открытого ключа**, таким образом удостоверяя факт того, что закрытый (секретный) ключ известен эксклюзивно владельцу этого сертификата, открытый ключ (public key) свободно передается в сертификате
- никто не доверяет друг другу, но все **доверяют удостоверяющему центру**
- удостоверяющий центр **подтверждает** или опровергает **принадлежность открытого ключа заданному лицу**, которое владеет соответствующим закрытым ключом.

Майнинг

Майнинг, также **добыча** (от англ. *mining — добыча полезных ископаемых*) — деятельность по **созданию новых структур** (обычно речь идёт о новых блоках в блокчейне) для обеспечения функционирования криптовалютных платформ.

За создание очередной структурной единицы обычно **предусмотрено вознаграждение** за счёт новых (эмитированных) единиц криптовалюты и/или комиссионных сборов. Обычно майнинг сводится к серии вычислений с перебором параметров для нахождения хеша с заданными свойствами.

Разные криптовалюты используют разные модели вычислений, но они всегда достаточно длительны по времени для нахождения приемлемого варианта и быстры для проверки найденного решения (см. Доказательство выполнения работы).

Такие вычисления используются алгоритмами криптовалют для обеспечения защиты от повторного расходования одних и тех же единиц, а вознаграждение стимулирует людей расходовать свои вычислительные мощности и поддерживать работу сетей.

ICO

ICO, ***Initial coin offering***, (с англ. — «первичное предложение монет, первичное размещение монет») — форма привлечения инвестиций в виде продажи инвесторам фиксированного количества новых единиц криптовалют, полученных разовой или ускоренной эмиссией.

Встречается также форма «первичного предложения токенов». Помимо этого термин ICO часто заменяется словом «краудсейл»

Токен — это единица учёта, не являющаяся криптовалютой, предназначенная для представления цифрового баланса в некотором активе, иными словами выполняющая функцию «заменителя ценных бумаг» в цифровом мире.

Токены представляют собой запись в регистре, распределенную в блокчейн-цепочке. Получить доступ к токену можно через специальные приложения, которые используют схемы электронной подписи. Основная часть существующих на сегодняшний день токенов формируется на протоколе Blockchain от Ethereum

Смарт-контракт

Смарт-контракт (англ. *Smart contract* — умный контракт) — компьютерный алгоритм, предназначенный для заключения и поддержания коммерческих контрактов в технологии блокчейн

Стороны подписывают умный контракт, используя методы, аналогичные подписанию отправки средств в действующих криптовалютных сетях. После подписания сторонами контракт вступает в силу. Для обеспечения автоматизированного исполнения обязательств контракта непременно требуется среда существования, которая позволяет полностью автоматизировать выполнение пунктов контракта.

Это означает, что умные контракты смогут существовать только внутри среды, имеющей беспрепятственный доступ исполняемого кода к объектам умного контракта. Все **условия контракта** должны иметь **математическое описание** и ясную **логику исполнения**.

IOTA

IOTA расшифровывается как Internet of Things Application. Это новая криптотехнология, которая облегчает **транзакции** между устройствами **в Интернете вещей** (IoT)

IOTA исследует транзакционные сборы и проблемы масштабируемости технологий блокчейн. Проект избавился от блоков и их цепи. Вместо этого, чтобы отправить транзакцию в публичный реестр IOTA, вы должны **проверить две другие предыдущие транзакции**. Этот метод проверки означает, что **нет центрального реестра** и нет необходимости в том, чтобы майнеры поддерживали сеть.

Поскольку вычислительная мощность в Tangle растет по мере роста сети, IOTA обещает бесплатные быстрые транзакции. Проект предназначен для обработки микроплатежей и платежей между устройствами, что облегчает создание микроэкономики в машиностроении.

Циклы ажиотажа

Hype cycle это графическое отображение проникновения, адаптации и социального влияния специфических технологий. Термин был введен Gartner.

С 1995 года последняя использует эту методику для описания и оценки энтузиазма, который вызывает у пользователей появление новых технологических решений.