Знакомство с блокчейн

Блокчейн – это распределённая база данных, которая содержит информацию обо всех транзакциях, проведенными участниками системы.



Блокчейн представляет собой последовательность блоков транзакций, связанных между собой криптографической хэш-функцией, где корректность каждого блока проверяется и подтверждается всеми участниками сети.

Банковская транзакция – это операция с денежными средствами: перевод вывод зачисление и т.д. т.е. любой процесс, связанный с использованием банковских счетов.

Транзакция блокчейна – это операция сохранения данных в блокчейне, в ходе которой происходит передача крипто активов или другой информации между адресами кошельков получателя и отправителя.

Отправка транзакции происходит после её создания и подписания цифровой подписью на основе закрытого ключа.

Крупные компании осваивают блокчейн для того чтобы снизить транзакционные издержки, ускорить прохождение транзакций, снизить риск мошенничества и устранить посредников.

Некоторые фирмы с его помощью пытаются перестроить устаревшие системные сервисы чтобы вывести их на следующий уровень.

Криптовалюта – это разновидность цифровой валюты. Базовый принцип криптовалюты заключается в том, что контроль над созданием каких-то новых транзакций или контроль над перемещением базируется на элементах криптографии.

Криптовалюты децентрализовано учитываются в противовес обычным цифровым. Все функционирование криптовалют основано на технологии блокчейн, которое использует криптографию.

Криптография в криптовалютах используется в основном для обеспечения неизменяемости базы самого блокчейна.

Происхождение блокчейна

Блокчейн впервые появился в криптовалюте в виде BTC в основу которой заложен блокчейн и тем самым представил.

Концепция децентрализованной цифровой валюты витала в воздухе десятилетиями.

Сатоши Накамото в 2009 году представил первую криптовалюту биткоин и тем самым представил практическую реализацию блокчейна.

Он объединил в себе уже известные на тот момент понятия:

1. Криптографическая система с открытым ключем
2. Алгоритм консенсуса Proof of work – данный алгоритм появился впервые как решение проблемы на электронной почте. Блокчейн стал той недостающей частью интернет революции, которая превращает уязвимую систему обмена ценностями в криптографический защищенную

Банковская система отстала от технологической революции. Банки создали централизованные организации, которые хранят транзакционные записи, контролируют взаимодействие, обеспечивают доверия и безопасность и регулируют всю систему. Вся коммерция опирается на эти финансовые учреждения, которые служат доверенными посредниками при обмене.

Что такое блокчейн?

Блокчейн – система записей о переносе любой ценности. Это означает что нет необходимости в посреднике, который служит доверенной третьей стороной при обмене ценностей.

Транзакции с использованием посредника

Транзакции с использованием блокчейна



Блокчейн – одноранговая система передачи ценностей без участия третьей доверенной стороны. Это общий децентрализованный и открытый реестр транзакций.

База данных реестра работает только в режиме добавления записей, и не может быть изменена или исправлена. Это означает, что каждая запись является постоянной и неизменяемой. Любая новая запись появляется во всех копиях базы данных, размещённых на разных узлах.

Нет необходимости, чтобы доверенные третьи стороны выступали в качестве посредников для проверки обеспечения безопасности и подтверждения транзакций.



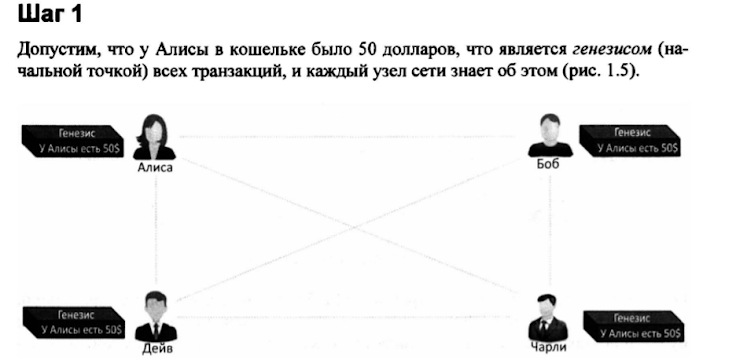
Первый блок цепочки – Генезис. Генезис-блок – самый первый блок распределительного реестра, который является основой и прототипом для создания всех остальных блоков.

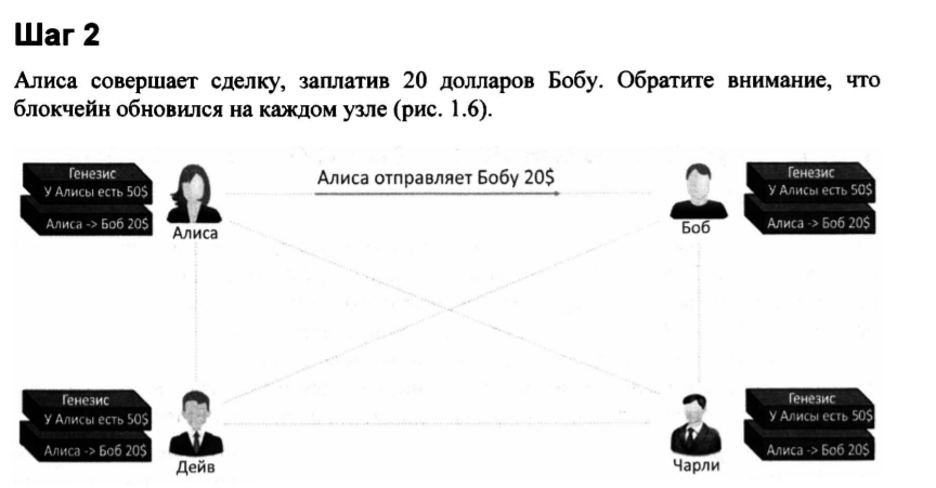
Блокчейн-сеть состоит из большого количества узлов. Каждый узел в сети имеет идентичную копию блокчейна. Каждый блок – совокупность транзакций и связь с предыдущим блоком.

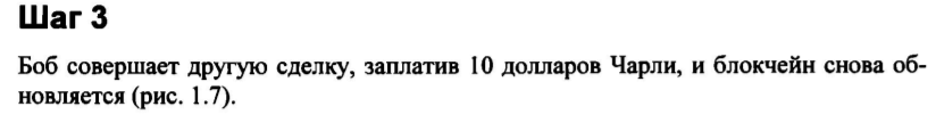
Каждый блок состоит из двух частей: заголовка и тела блока. Заголовок ссылается на предыдущий блок в цепочке. Каждый заголовок содержит хэш предыдущего блока. Поэтому никто не может скрытно изменить транзакцию в предыдущем блоке. Тело блока содержит список проведенных транзакций.

Пример:

Есть 4 участника, которые проводят транзакцию между собой в сети блокчейна.





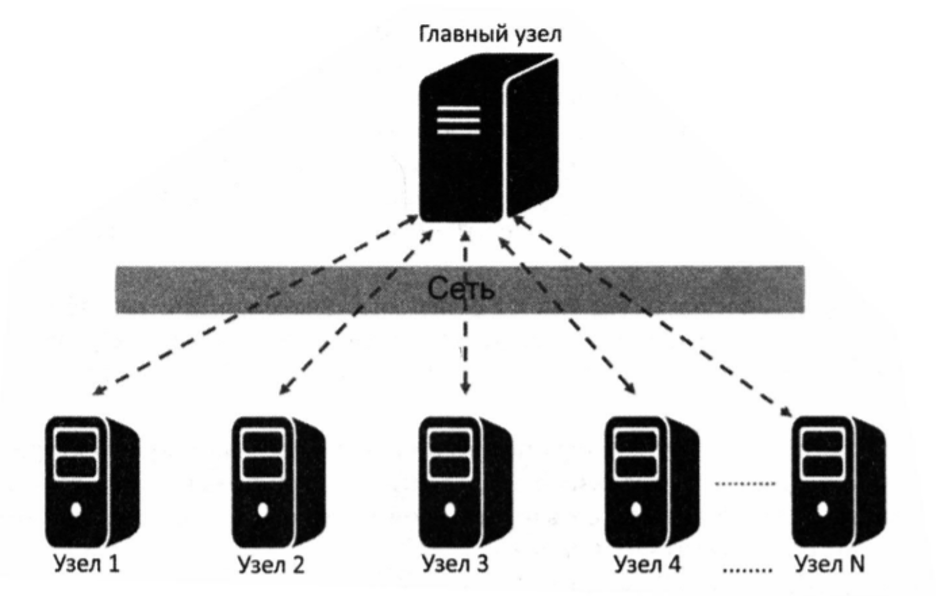


Данные транзакции в блоках неизменяемы. Все транзакции полностью необратимы. Любое изменение создаст новую транзакцию, которая будет подтверждена всеми участниками сети, а старая просто остается на месте. У каждого участника сети есть своя копия блокчейна.

Централизованные и децентрализованные системы

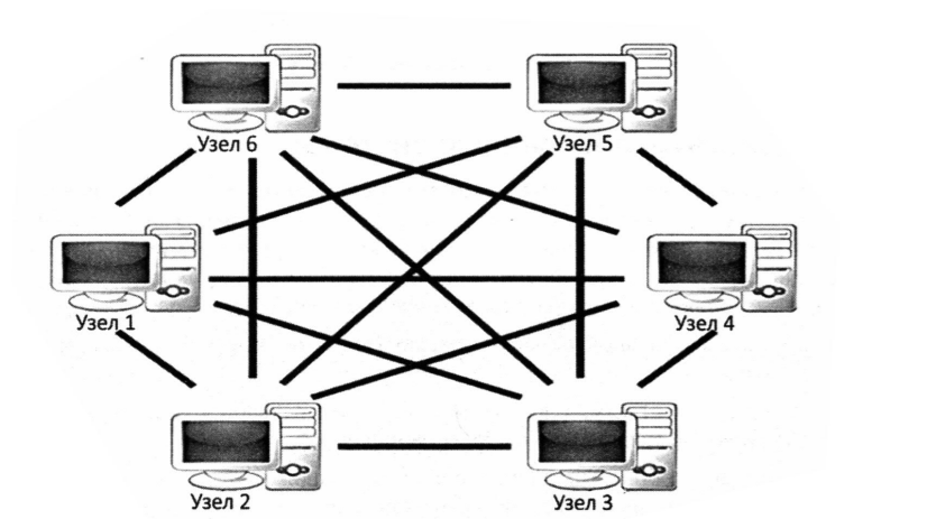
Независимо от того, централизована или децентрализована система – её все равно можно распределить.

Централизованная распределенная система – это такая система, в которой есть главный узел, ответственный за дробление задач и данных, а также распределение нагрузки между узлами.



Децентрализованная распределенная система – система, где нет главного узла как такового, но все же, вычисления могут быть распределены.

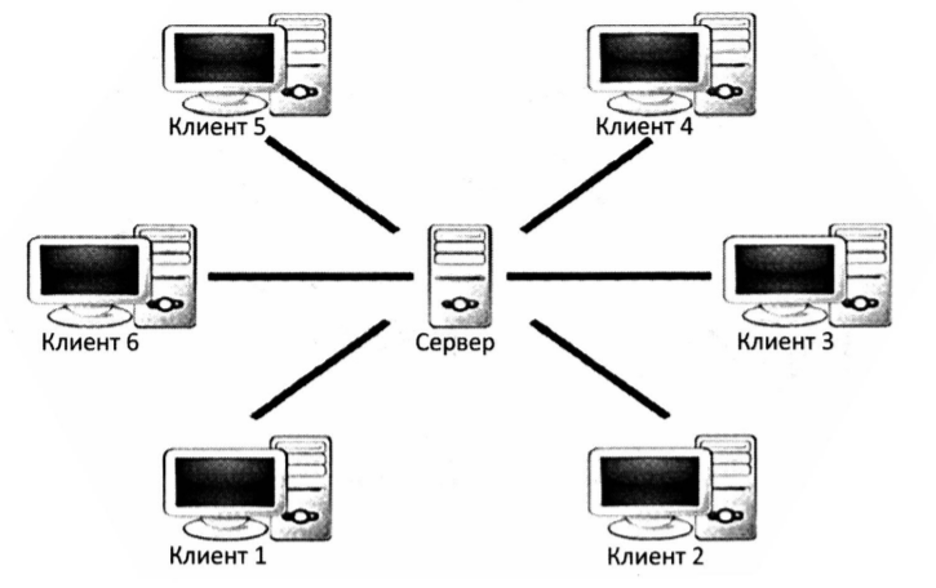
Децентрализованная система каждый с каждым



Централизованные системы

Централизованная система имеет централизованное управление со всеми административными полномочиями. Такие системы легко разрабатывать, поддерживать, навязывать им доверие и управлять ими. Но, они страдают от многих неотъемлемых ограничений. А именно:

1. У них есть центральная точка отказа, поэтому они менее стабильны.
2. Они более уязвимы для атаки, следовательно, менее защищены.
3. Централизация власти может привести к неэтичным действиям.



Децентрализованные системы

Децентрализованные системы не имеют центрального органа управления и каждый её узел равноправен. Такие системы сложно разрабатывать, поддерживать, управлять, или навязывать им доверие. Они не страдают от ограничений от ограничений обычных централизованных систем.

Преимущества децентрализованных систем:

1. Нет центральной точки отказа, поэтому они более стабильные и отказоустойчивы.
2. Устойчивость к атакам, так как они не имеют центральной точки, доступной для легкой атаки, следовательно, более защищены
3. Симметричная система с равными полномочиями

Ограничения централизованных:

1. Проблема доверия
2. Проблема безопасности
3. Проблема конфиденциальности

Преимущества децентрализованных систем:

1. Устранение посредников
2. Прозрачность
3. Проверка транзакций
4. Меньшие затраты и большая безопасность
5. Отсутствие уязвимого центра и неизменяемость

Двойное расходование (атака двойного расхода) – это повторная продажа одних и тех же активов. Заключается в том, что сначала продавец убеждается в проведении транзакций на оплату, после чего он передает свой товар, а после получения товара, покупателем создается новая транзакция, которая и принимается сетью вместо первой.

Атака 51% - это атака на блокчейн, где один субъект или организация захватывает наибольшую часть узлов, что может привести к нарушению работы сети. В такой ситуации у злоумышленника будет достаточно мощности, чтобы намеренно исключать транзакции или изменять их в порядке, а также изменять собственные транзакции, провоцируя проблему двойного расходования.

В системе биткоин нет понятия личного счета, это означает, что, когда кто-то совершает транзакцию, он использует одну из предыдущих транзакций, по которой получит как минимум ту сумму, которую тратит сейчас.

Новая транзакция должна быть проверена всеми узлами путем обхода предыдущих транзакций, чтобы определить, является ли она допустимой транзакцией.

В системе этериум имеется система балансовых счетов. После сделки будет обновлен счет того, кто отправил транзакцию, и счет того, кто её получил.

Смарт-контракты

Умный контракт – особый тип учетной записи с исполняемым кодом и частными состояниями. Состояние системы обновляется, если при получении транзакции сработал код умного контракта.

Блок обычно содержит несколько транзакций и несколько смарт контрактов.

В мире криптовалют смарт контракт – это приложение, работающее на блокчейне. Оно выступает в качестве цифрового соглашения, подкрепляемого набором правил. Эти правила определяются кодом, который копируют и обрабатывают все узлы сети (ноды).

Смарт-контракты позволяют создавать протоколы, не требующие доверия. Это означает, что обе стороны могут взаимодействовать без необходимости доверять друг другу. Участники процесса могут быть уверены, что несоблюдение условий контракта приведет к его аннулированию. Также, использование смарт контрактов избавляет от посредников и приводит к значительному сокращению расходов на операцию.

Блокчейн может вывести интернет на совершенно новый уровень, устранить препятствия в трех ключевых областях: управление доверие и ценность.

1. Управление

Блокчейн позволит распределить управление, сделав систему децентрализованной.

1. Доверие

Блокчейн представляет собой неизменяемый, защищенный от несанкционированного доступа. Это дает единый общий источник истины для всех узлов. Для совершения сделок с каким-либо неизвестным лицом или организацией больше не требуется доверие, так как оно заложено в саму сущность системы.

1. Ценность

Блокчейн позволяет обмениваться ценностями в любой форме. Можно выпускать или перемещать активы без центральных органов или посредников.

**Итог: все транзакции блокчейна криптографически защищены, независимо от их назначения. Используя криптографию, можно гарантировать, что лишь подлинный пользователь инициирует транзакцию.**

КРИПТОГРАФИЯ

Криптография – наука о методах обеспечения конфиденциальности, целостности данных, аутентификации и шифрования. Криптография является наиболее важной составляющей блокчейна. Это самостоятельная область исследования, основанная на передовых математических методах. Это самый важный компонент обеспечения безопасности в системе.

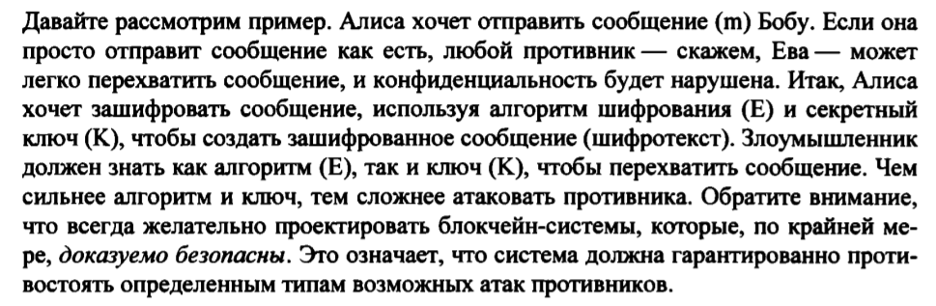
Из-за недостаточной криптозащищенности взломали много приложений, кошельков и обменных бирж.

Криптография существует уже более 2-х тысяч лет. Это наука о конфиденциальности с применением методов шифрования.

Способы использования криптографии:

1. Конфиденциальность – только предполагаемый или авторизованный пользователь может понять сообщение
2. Целостность данных – данные не могут подделаны и изменены злоумышленником или за счет ошибок. Целостность данных не может предотвратить изменение данных, она предоставляет средства проверки того, были ли данные изменены
3. Аутентификация – подлинность отправителя гарантированно проверяется получателем
4. Безотзывность – отправитель после отправки сообщения не может позднее отрицать, что отправил данное сообщение. Отправитель не может отказаться от ответственности за предыдущие обязательства или действия.

Любая информация в виде текстового сообщения числовых данных или программы может называться открытым текстом. Идея криптографии – зашифровать открытый текст, используя алгоритм шифрования и ключ.

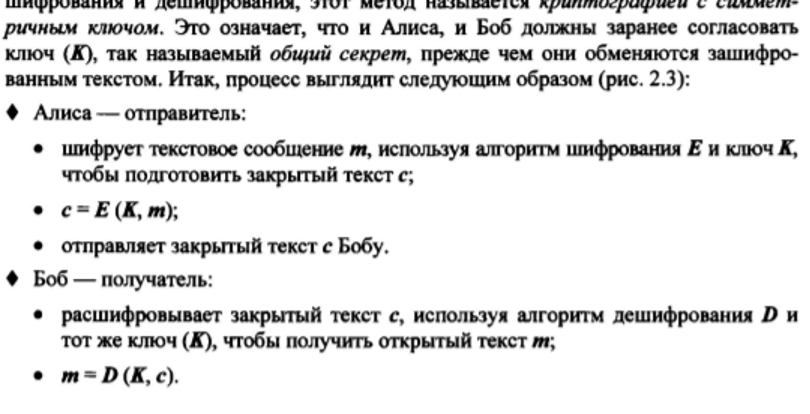


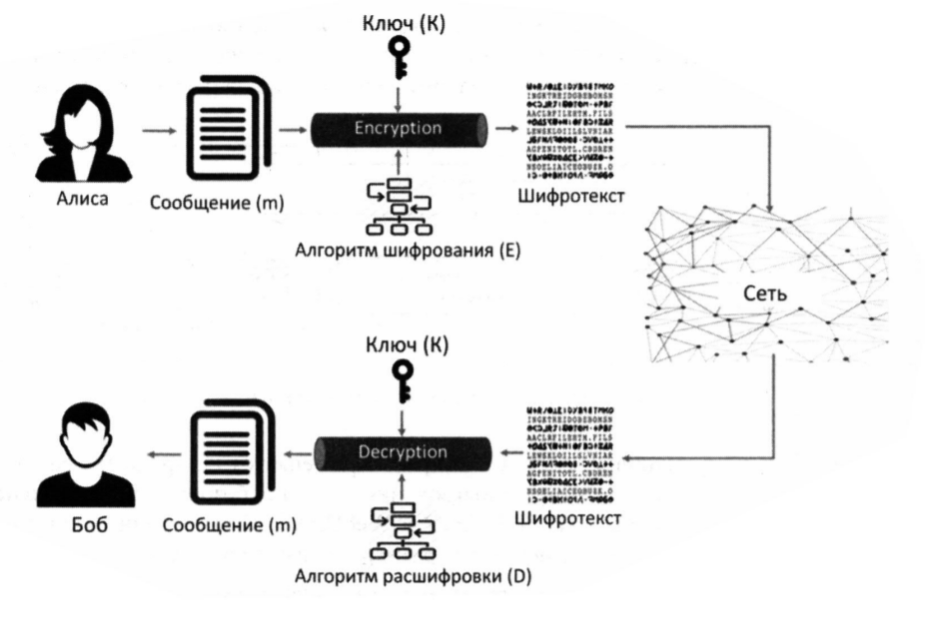
Существует два типа криптографии:

Криптография с симметричным ключом

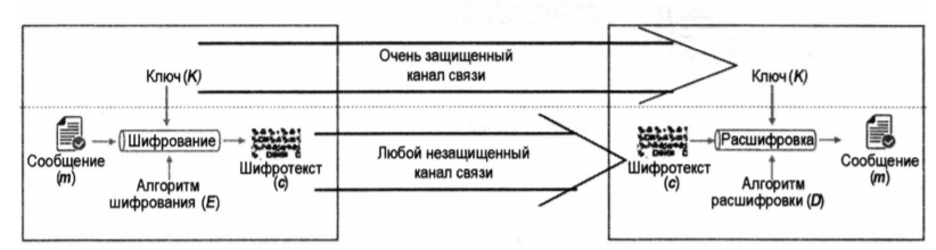
Криптография с ассиметричным ключом

Если один и тот же ключ используется для шифрования и дешифрования





Для обмена ключами нужен безопасный канал связи.



В криптографии с симметричным ключом есть некоторые принципиальные ограничения:

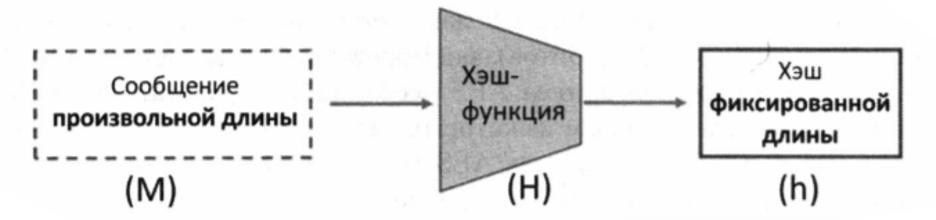
1. Ключ должен быть передан отправителю и получателю до начала сеанса связи. Для этого требуется защищенный механизм создания и доставки ключа.
2. Отправитель и получатель должны доверять другу т.к. они используют один и тот же ключ. Если злоумышленник взломал получателя, или получатель сознательно поделился с кем-то еще, вся система будет скомпрометирована (взломана).

Скомпрометированность – состояние объекта или субъекта, характеризующее падение уровня доверия. Рекомендуется постоянно менять ключ для каждого сеанса. Часто для эффективного управления ключами необходима доверенная третья сторона, что само по себе проблема. Большая сеть из N узлов требует управления N \* N-1 / 2 ключей.

Хэш – это уникальная строка фиксируемой длины, предназначенная для идентификации фрагмента данных.

Хэш-функция – это математические функции, которые относятся к наиболее важным криптографическим примитивам и являются неотъемлемой частью структуры блокчейна. Они широко применяются во многих криптографических протоколах и приложениях ИнфБез такие как цифровые коды и аутентификации сообщений.

Криптографическая Хэш-функция – это односторонняя функция, которая преобразует входные данные произвольной длины в выходные данные фиксированной длины. Вывод обычно называется хэш суммой.



Свойства хэш функции:

1. Входные данные могут быть любого размера
2. Выходные данные имеют ограничение
3. Хэш значение должно быть рационально-вычисляемым для любого данного сообщения
4. Одни и те же данные = один и тот же хэш
5. Нереализуемо восстановить исходное сообщения из хэш значения кроме подбора
6. Любое малейшее изменение в сообщение должно сильно влиять на выходной хэш
7. Хэш функции можно использовать для безопасной аутентификации пользователей без локального хранения паролей
8. Двумя наиболее важными приложениями являются цифровые подписи и коды аутентификации сообщений на основе хэшей (HMAC)

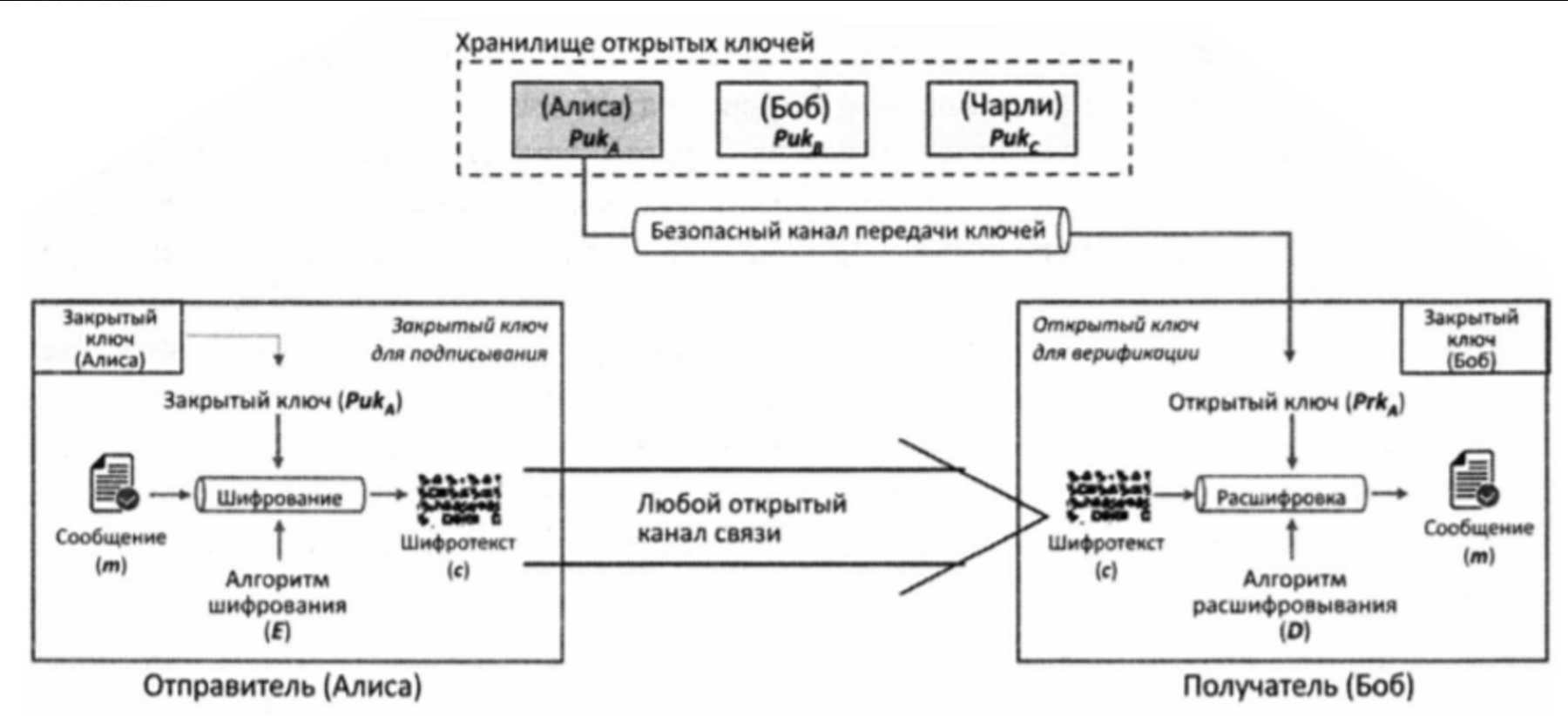
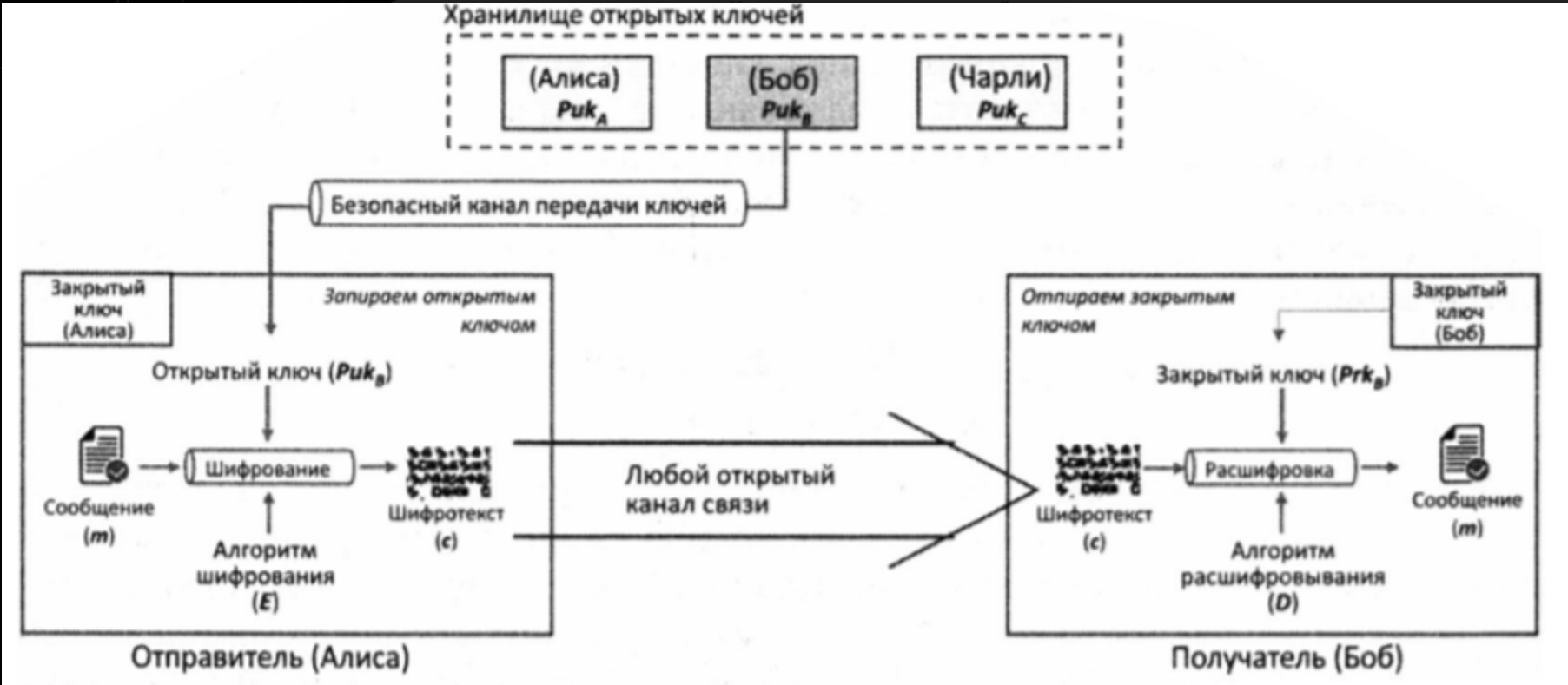
HMAC – это один из механизмов проверки целостности информации, позволяющий гарантировать то, что данные, передаваемые или хранящиеся в ненадежной среде не были изменены посторонними лицами

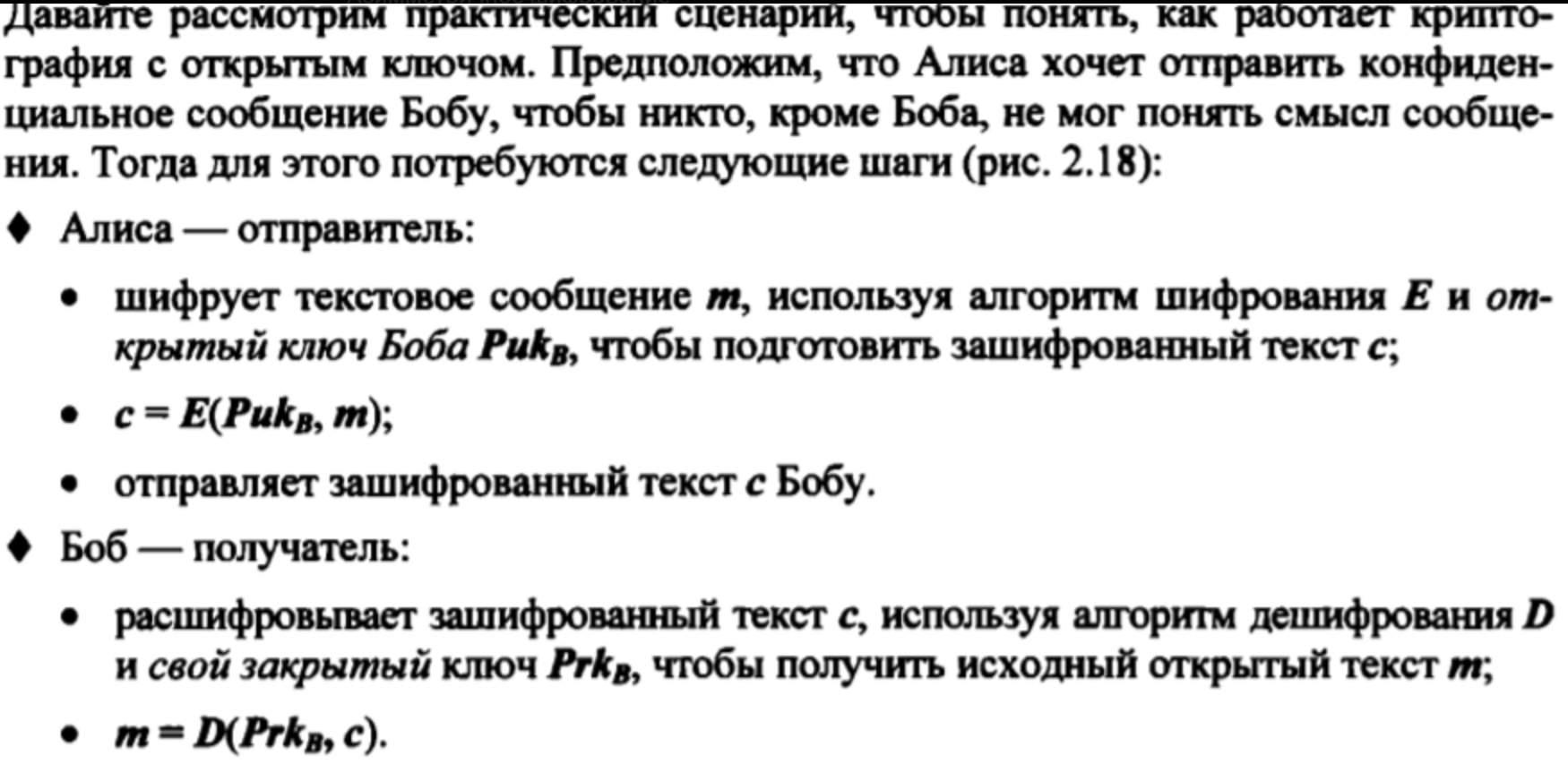
Криптография с ассиметричным ключом

Ассиметричное шифрование – это метод шифрования данных, предполагающий использование двух ключей: открытого и закрытого.

Открытый – для шифрования

Закрытый – для расшифровки



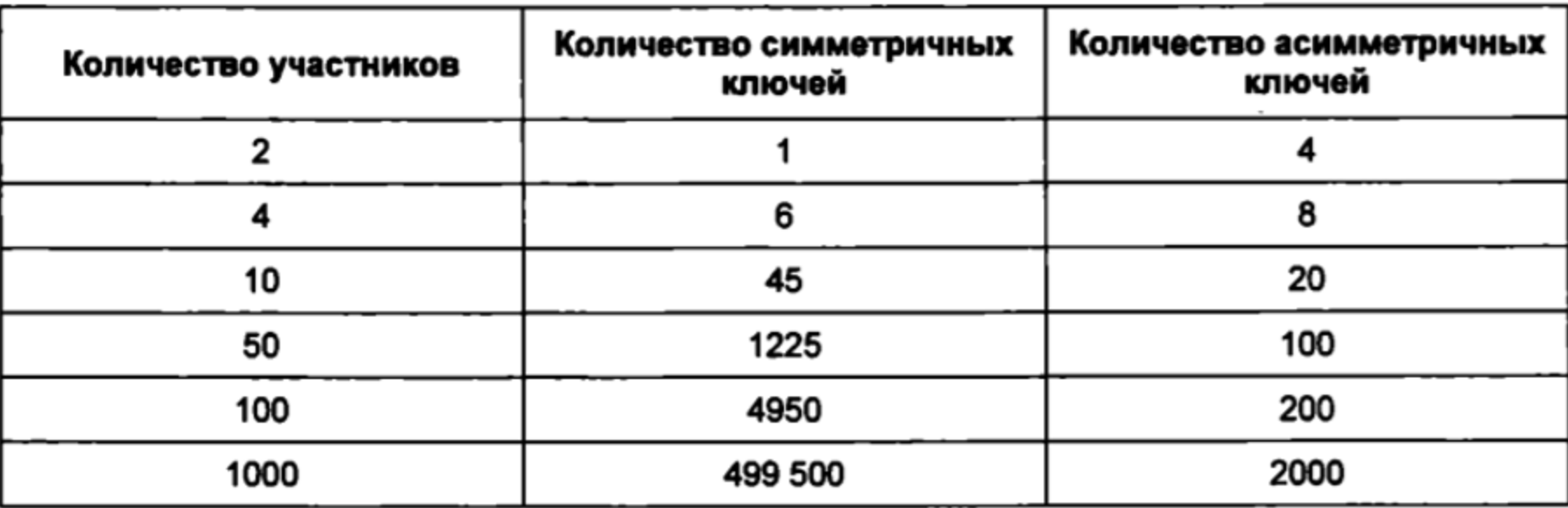


Открытый ключ должен храниться в доступном хранилище (открыт для всех). А закрытый ключ является тщательно охраняемым секретом. Криптография с открытым ключом также обеспечивает конфиденциальность. Получатель может проверить подлинность источника сообщений.

Свойства ключей:

1. Открытые ключи известны и доступны каждому, их можно использовать для шифрования сообщений или проверки подписей
2. Закрытые ключи являются исключительно секретными и принадлежать отдельным лицам. Они используются для расшифровки сообщений или создания цифровых подписей

Иногда, одновременно требуется и аутоинтефикация, и конфиденциальность. Для этого необходимо дважды использовать шифрование с открытым ключом. Сообщение должно быть сначала зашифровано с помощью закрытого ключа отправителя, для цифровой подписи. Затем сообщение должно быть зашифровано открытым ключом получателя для обеспечения конфиденциальности.



ОТКРЫТЫЕ И ЗАКРЫТЫЕ КЛЮЧИ

Закрытые ключи генерируются случайным образом. Открытый ключ создается путем криптографического преобразования закрытого ключа.

Чтобы получить адрес аккаунта необходимо хешировать открытый ключ, который создан на основе закрытого ключа, и взять оттуда последние 20 байт.

ХЭШ-УКАЗАТЕЛИ

Хэш указатель — это криптографический хэш, указывающий на блок данных, они указывают на предыдущий блок данных и предоставляют способы убедиться, что данные не были подделаны.

Назначение хэш-указателей состоит в создании устойчивого к взлому блокчейна.

Хэш предыдущего блока сохраняется в заголовке текущего блока, а хэш текущего блока, вместе с его заголовком, будет храниться в заголовке некст блока.

По цепочке ссылок можно пройти весь путь до первого блока. В такой схеме, где блоки связаны с помощью хэшей, практически невозможно незаметно изменить данные в любом блоке. Если данные будут изменены, то хэш-коды не будут совпадать.

СВОЙСТВА БЛОКЧЕЙН РЕШЕНИЙ

1. Неизменяемость — как тоько транзакция записана в риестр, она не может быть изменена. Если транзакции передаются в сеть, тто у каждого узла есть их копия. Со временем, когда в цепочку добавляется все больше и больше блоков, неизменяемость увеличивается и через неокторое время цепочка становится полностью неизменяема. Изменить данные такого колтичества блоков подряд практически невозможно, потому что они криптографически защищены. Таким образом любая транзакция, которая регестрируется в реесте, навсегда остается в системе в неизменяемом состоянии.

2. Стойкость к подделке — для обеспечения устойчивой системы к подделке могут использоваться цифровые подписи и криптографический хэш. Если мы совершаем транзакцию и подписываем её хэш, никто не сможет изменить транзакцию позже и сказать, что мы подписали другую транзакцию. Кроме того, позже мы не сможем утверждать, что никто не совершил транзакцию, потому что мы подписали ее.

3. Демократичность — у всех узлов есть равные права и своя копия блокчейна.

4. Согласованное состояние реестра.

5. Жизнестойкость — сеть должна быть достаточно устойчивой, чтобы выдержать временные сбои узлов, иногда недоступность некоторых вычислительных узлов, задержку в сети и потери пакетов, атаки с преднамеренной перегрузкой и т.п. затруднения.

6. Проверяемость — имела ли место транзакция в прошлом то проверка должна быть быстрой.

ТРАНЗАКЦИИ И БЛОКЧЕЙН

Как только пользователь совершает транзакцию, ему нужно сообщить об этой транзакции всей сети. Как только это произойдет, транзакция должна быть проверена несколькими узлами. После проверки, необходимо передать рассылку на всю сеть, чтобы транзакция была вклбчена в цепочку блоков. Транзакция проходит следующие шаги:

1. Каждая новая транзакция транслируется в сеть, чтобы все вычислительные узлы знали об этом факте в тот момент, когда она имела место быть.

2. Транзакции могут быть подтверждены или укланены узлами путем проверки поддленности.

3. Узлы могут группировать несколько транзакций в блоке для последующей обработки и включения в цепочку блоков.

4. Генерация новых блоков должна быть управляемой, но не централизованной и механизм управления должен быть таким, чтобы каждому узлу был присвоин равный приоритет. Согласие всех узлов по поводу блока, называется консенсусом.

5. Блоки имеют метки времени в порядке их поступления и добавления в цепочку блоков.

6. Как только узлы в сети или большинством голосов принимают в блок (приходит консенсусом), этот блок добавляется в цепочку блоков и к нему присоединяется хэш блока, созданного непосредственно перед ним. В результате блокчейн удлиняется на 1 блок.

МЕХАНИЗМ РАСПРЕДЕЛЕННОГО КОНСЕНСУСА

1. Доказательсво работы (PoW) — иедя алгоритма PoW заключается в том, что для блока транзакции выполняется определенная работа, прежде чем он будет предложен всей сети. Результат PoW представляет собой фрагмент данных, которые трудно добыть с точки зрения вычислений, но который легко проверить. Перед созданием блока необходимо выполнить некоторую сложную работу требующую большого объема вычислений если узел попробует внедрить мошенническую транзакцию в блок, то отклонения этого блока остальными узлами слишком дорого обойдется для мошенника (ведь вычисления, выполненные машенника для нахождения PoW, окажутся напрасными). Узел майнер (которое 1 нашел число Nonce) получает вознаграждение. Комиссия за транзакцию или генерация новых монет.

Одноранговый номер Nonce — это аббревиатура от числа, использованного только 1 раз, т.е. числа, добавляемого к хешированному блоку цепочки блоков, которые при повторном хешировании соответствуют ограничением уровня сложности.

Nonce — это число, которое майнеры блокчейн решают, чтобы получить криптовалюты.

Допустим, мы задали сложность такой, чтобы у хэша блока в начале было 4 нуля. Нам нужно знать хэш блока и прибавить к нему какое-то число и прогрнать это все через хэш-функцию. Если на выходе мы получаем хэш на выходе с 4 нулями, то блок сманен, он закрывается, а кто его находит получает вознаграждение за майн. Поиском числа Nonce одновременно занимаются все майнинг ноды сети.

Balance – общий баланс эфира на счету, а именно сумма денежных единиц на счету wei, принадлежащего нашему адресу.

1 эфир = 1018wei

Газ и стоимость транзакций

Транзакции в системе этериум работают на газе – фундаментальной единицы стоимости вычислений. Каждая транзакция должна иметь установленное значение газ-лимит и газ-прайс. Это выплачивается майнерам для компенсации их ресурсов.

Газ-прайс – это цена на один газ.

Газ-лимит – макс кол-во газа которое должно использоваться при выполнении транзакции. Обычно один вычислительный шаг стоит один газ.

Газ-прайс \* стоимость газа для комиссии. У майнера есть своя стратегия расчета минимальной приемлемой цены за газ. Майнер соглашается взять в обработку только те транзакции, которые ему выгодно.

Общая эфирная цена основана на двух фактах: использованный газ, цена газа.

Если общее кол-во газа, необходимое для вычислений меньше либо равно газ лимит то майнер принимает.

Если затраты газа превышают газ-лимит, то все изменения отменяются за исключением того, что майнер все равно может получить вознаграждение.

В начале обработки транзакции газлимит\*газпрайс списывается со счета отправителя транзакции.

Message – глобальный обьект в котором хранится инфа о транзакции в качестве сообщения.

Sender – свойство, которое вернет адрес отправителя транзакции.

Payable – свойство, которое позволяет указать что данная функция принимает средства.

Value – кол-во отправленной валюты.

Int64 – 2^64

Int8 – 2^8 = 256

Public – модификатор, при котором функция видна и в контракте, и за пределами контракта.

External – модификатор, при котором функция видна только извне, но не в контракте.

Internal – модификатор, при котором функция доступна только внутри контракта

Receive() – функция, позволяющая получать деньги на счет контракта без создания функций. Она обязательно должна иметь модификатор External и payable.

Fallback() – вызывается когда происходит вызов несуществующей функции.