# Знакомство с BLOCKCHAIN

Blockchain – это распределённая база данных, которая содержит информацию об о всех транзакциях, проведённых участниками системы.

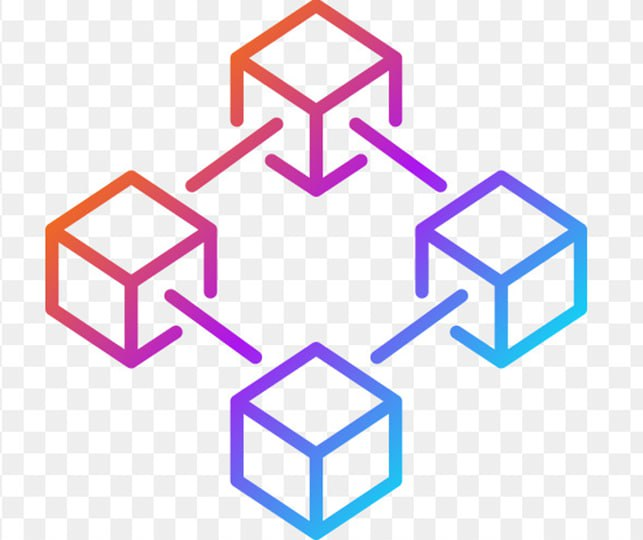


Рисунок 1

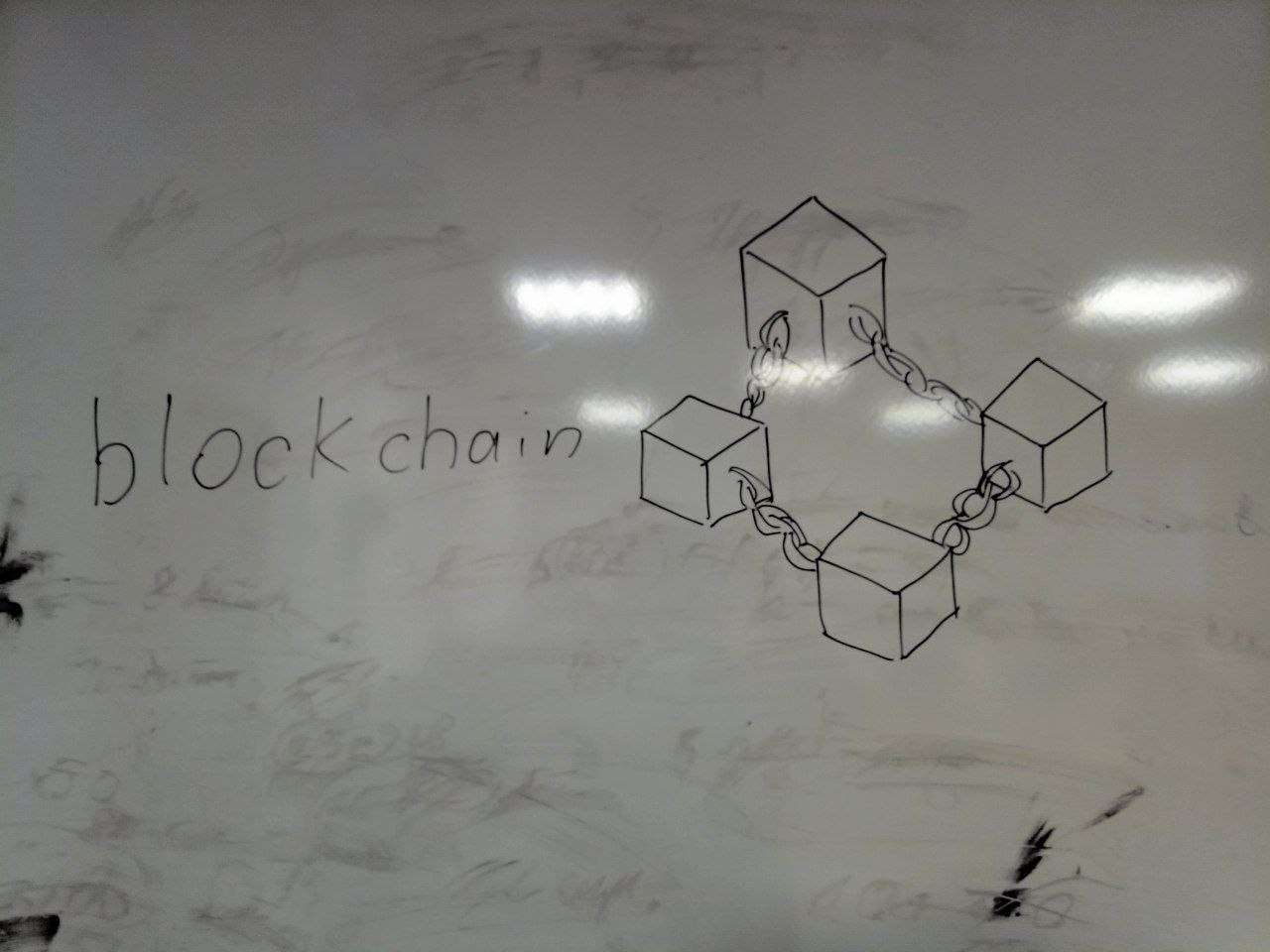


Рисунок – Мой рисунок)

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

Банковская транзакция – это операция с денежными средствами, перевод, вывод, зачисление и тд, любой процесс связанный с банковскими счетами.

Транзакция блокчейна – это операция сохранения данных 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 транзакции, снизить риск мошенничества и устранить посредников. Некоторые фирмы с его помощью пытаются перестроить устаревшие системные сервисы чтобы перевести их на следующий уровень.

Крипто валюта это разновидность цифровой валютой. Базовый принцип крипто валюты заключается в том, что контроль над созданием каких то новых транзакцией или контроль над перемещением. Криптовалюты децентрализовано учитываются в противовес обычным цифровым. Всё функционирование криптовалью основано на блокчейне, которая использует криптографию.

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

## Происхождение блокчейна

Блокчейн впервые появился в криптовалюте Bitcoin BTC в основе которой заложен блокчейн. Концепция децентрализованной цифровой валюты витала в воздухе десятилетиями. Satoshi Nakamono, в 2009 представил первкю криптоваюту Биткоин и тем самым представил реализацию Блокчейн.

Он объединил в себе уже известные на тот момент понятия:

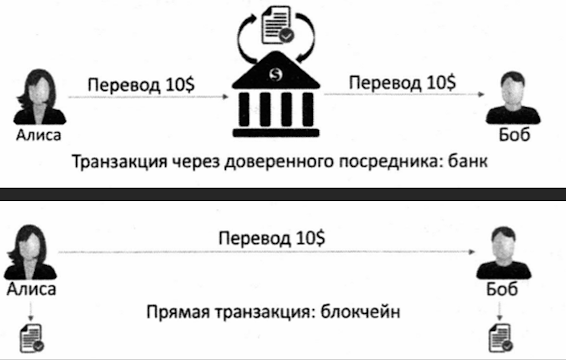
1. Криптографическая система с открытым ключом
2. Алгоритм консенсуса Proof of Work

Данный алгоритм впервые появился как решение проблеммы на электронной почты. Блокчейн стал той недостающей части интернет революции, которая превращает уязвимую систему обмена ценностями в криптографически защищёнными. Банковская система отстала от тех революции, банки создали централизованные организации, которые хранят транзакционные записи, контролируют взаимодействие, обеспечивают доверие и безопасность и регулируют всю систему.

Вся коммерция опираетс на эти финансовые учереждения, которые служат доверенными посредниками при обмене среди них.

## Что такое БЛОКЧЕЙН

Блокчейн это система записи по переносу любой ценности, это означает что нет необходимости в посреднике, который служит доверенный третьей стороной при обмене ценности.



Транзакции с использованием блокчейна и c посредником

Блокчейн – это одноранговая системма передачи ценностей без участия доверенности с третьей стороны.

1. Это общий децентрализованный открытый реестртранзакций.
2. БД реестра работает только в режиме добавления записей и не может быть изменена или исправлена. Это означает что каждая запись является постоянной и неизменяемой.
3. Любая новая запись появляется во всех копиях БД размещённых на разных узлах.
4. Нет необхоимости чтобы доверенные третьии стороны выступали в качестве посредников для проверки обеспечения безопасности и подтверждения транзакции.



1 блок цепочки является генезисом. Генезис блок жто самый первый блок распределительного реестра, который является основой и прототипом для создания всех основных классов.

Блокчейн сеть – сеть состоит из большого количества узлов, каждый узел в цепи имеет ту же копию блокчейна.

Каждый блок предстваляет совакупность транзакции и связь с предыдущим блоком.

Каждый блок состоит из 2х частей:

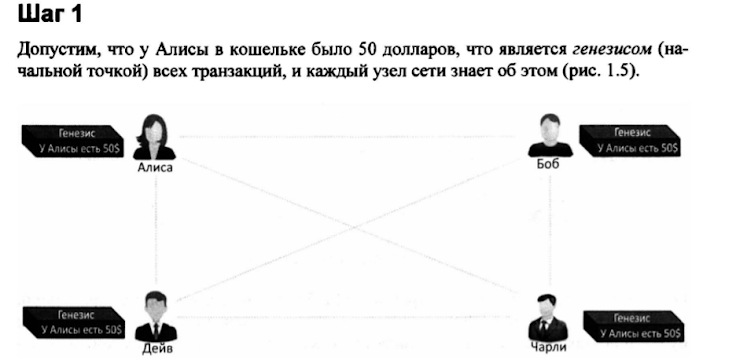
1. Заголовка
2. Тело блока

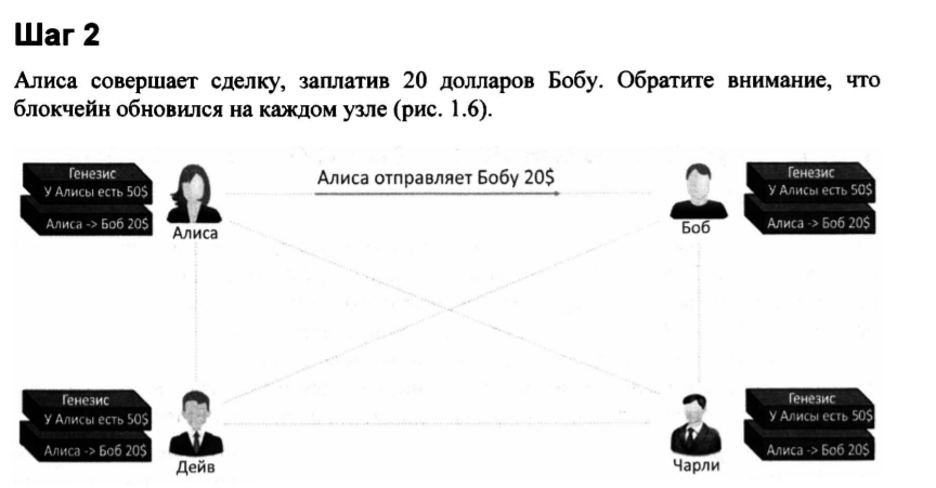
Заголовок ссылается на предедущий блок в цепочке. Каждый загаловок содержит хэш предыдущего блока, поэтому никто не может незаметно изменить транзакцию в предыдущем блоке.

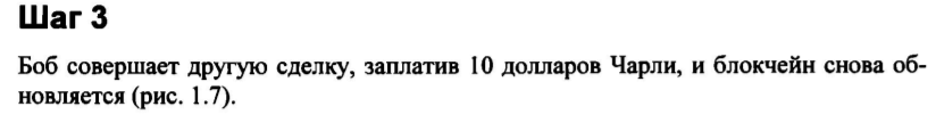
Тело блока содержит список проведённых транзакций

Пример:

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







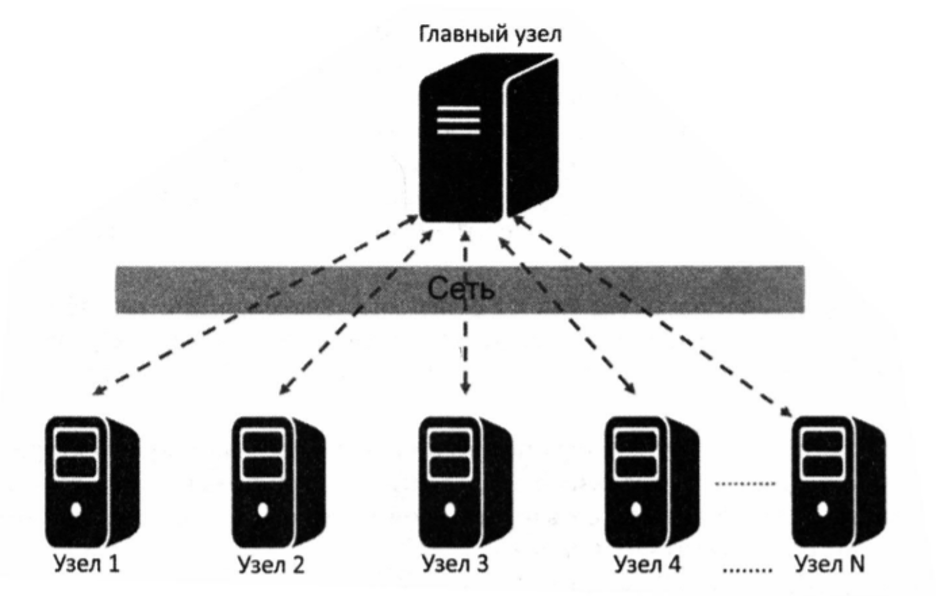


Данные в транзакциях блоков неизменяемые, все транзакции полностью необратимы. Любое изменение создаст новую транзакцию. У каждого участника ети есть своя копия блокчейна.

# Централизованная и децентрализованная система

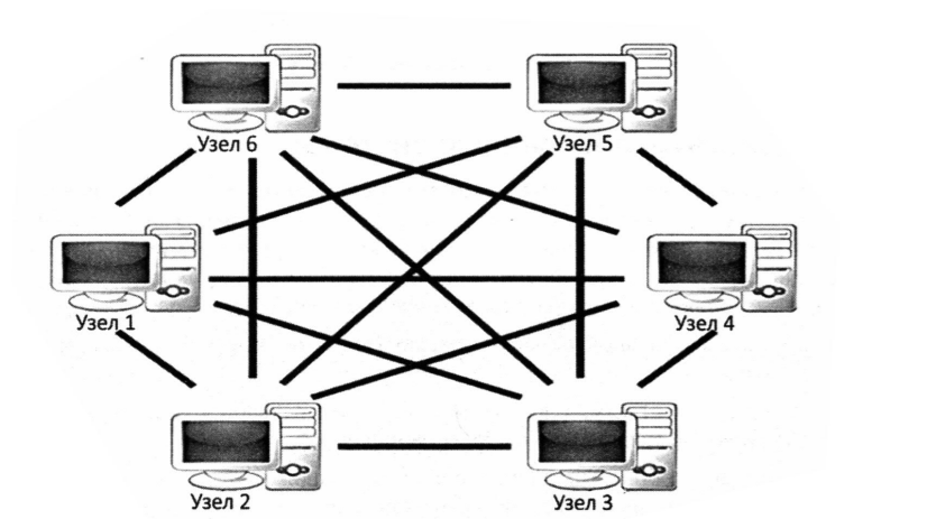
Независимо от того централизована или децентрализована система её всё равно можно распределить.

Централизованная распределённая система – это такая система в которой есть главный узел, ответственный за дроблением задач и данных., а так же распределение нагрузки между узлами.



Децентрализованная распределительная система – это такая система где нет главного узла как такового, но всё таки вычисления могут быть распределены.

Децентрализованая система каждый с каждым.

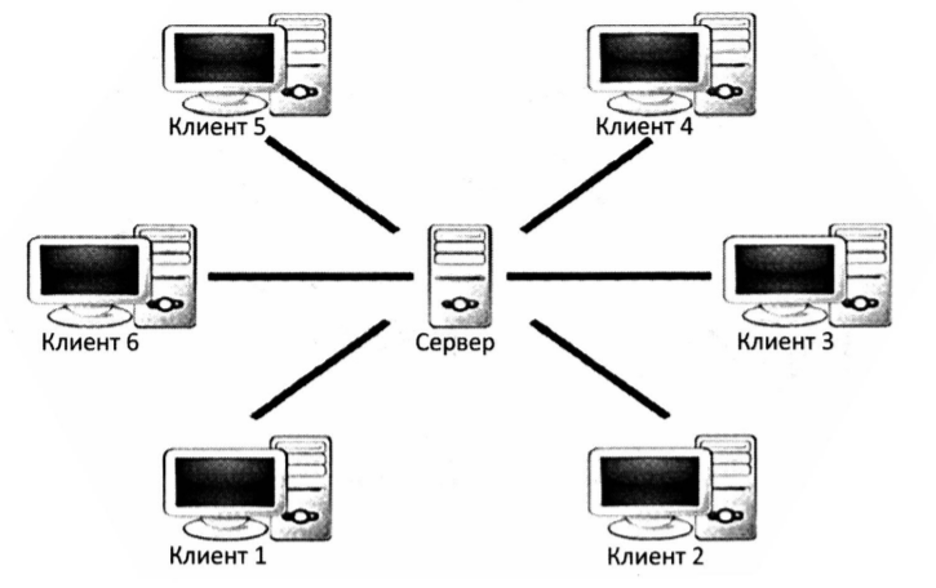


## Централизованные системы

Централизованная система имеет централизованное управление со всеми административными полномочиями. Такие системы легко разрабатывать, поддерживать, навязывать им доверия, но они страдают от многих неоемлимых ограничений, а именно :

1) У них есть центральная точка отказа, поэтому они менее стабильны. 2)Они более уязвимы для атаки и следовательно, менее защищены.

3) Централизация власти может привести к неэтичным действиям.



## ДЕЦЕНТРАЛИЗОВАННЫЕ СИСТЕМЫ

Децентрализованные системы не имеют центрального органа управления и каждый ее узел обладает равными полномочиями. Такие системы сложно разрабатывать, поддерживать, управлять или навязывать им доверие.

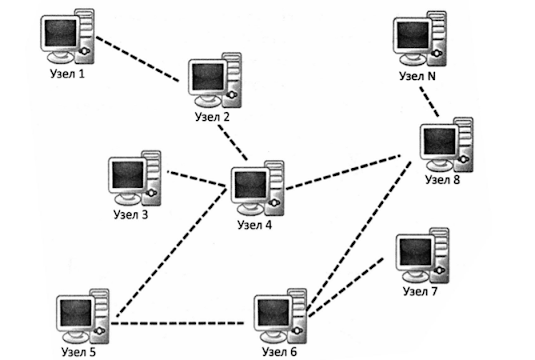
Они не страдают от ограничений обычных централизованных систем.

Децентрализованные системы имеют следующие преимущ

1) Они не имеют центральной точки отказа, поэтому они наиболее стабильные и отказо-устойчивые.

2) Устойчивость к атакам, так как они не имеют центральной точки, доступны для лёгкой атаки и, следовательно, более защищены.

3) Представляют собой симметричную систему с равными полномочиями для всех узлов.



Ограничения централизованных систем:

1) проблема доверия.

2) Проблема безопасности

3) Проблема конфедециальности

4) стоимость и временный фактор транзакций

Преимущество децентрализованных систем:

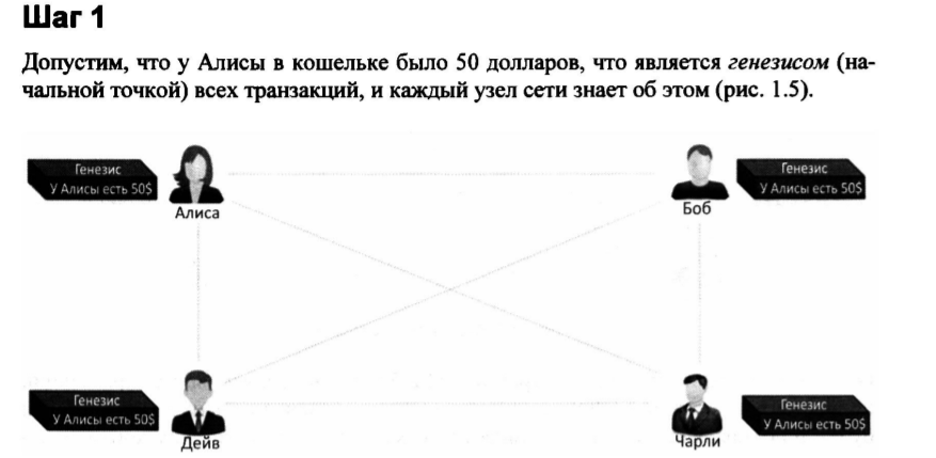
1) Устранение посредников

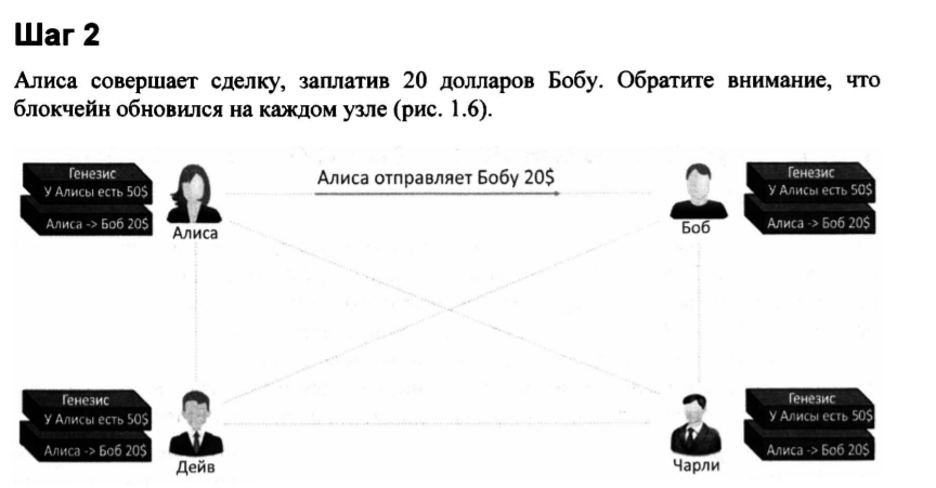
2) Проверка транзакций

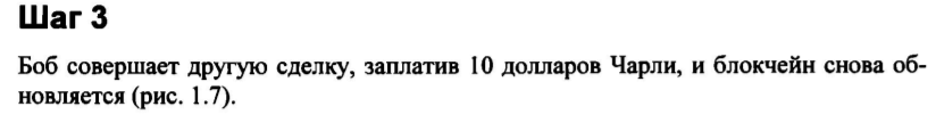
3) Повышенная безопастность с меньшими затратами

4) Прозрачность

5) Отсутствие уязвимого центра и неизменяемости.









Данные транзакции блоков не изменяемыми. Все транзакции полностью необратимы. Любое изменение создаст новую транзакцию, которая будет подтверждена всеми участниками, у каждого участника сети есть своя уопия блокчейна.

Центролизованные и децентрализованные системы

# Двойное расходование

Это повторная продажа одних и тех же активов заключается в том что сначала продавец беждается в проведении транзакции на оплату, после чего передаёт свой товар а после получения товара покупателем создаётся новая транзакция, которая и принимается сетью вместо первой.

## Атака 51%

Это атака на блокчейн где субъект или организация где захватывает наибольшую часть узлов, что может привести нарушения работы в сети, в таком случае у злоумышленника будет достаточно мощи чтобы намерено исключать транзакции или изменять их порядок, провоцирруя роблему двойного расходования

В системе биткоин нет понятия личного счета это значит что если 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.

# SMART контракт

Умный контракт – это особый тип учётной 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.

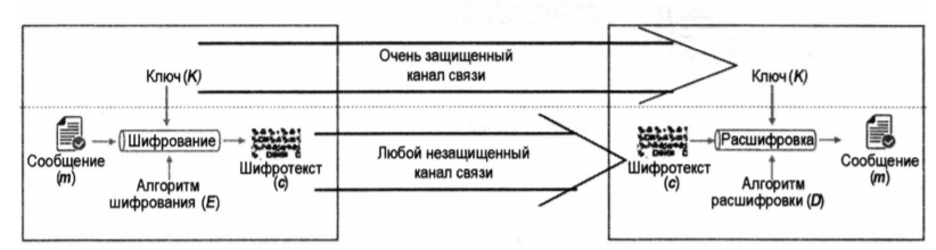
В мире криптовалют это приложение работающее на блокчейне. Оно выступает в качестве цифрового соглашения, подкриплённые правилами. Эти правила подкрипляются компьютерным кодом, которые копируют и обрабатывают все узлы сети.

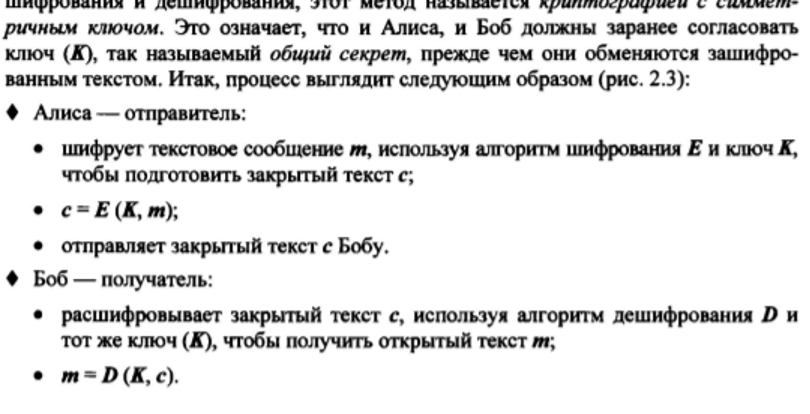
# Node

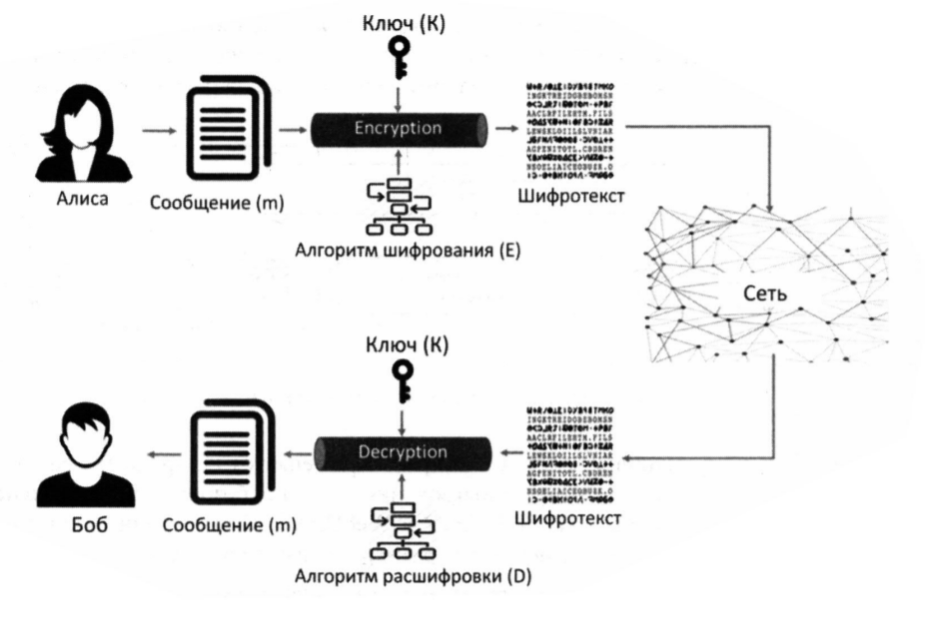
SMART контракты позволяют создавать протоколы, не требующие доверия. Это означает, что обе стороны могут взаимодействовать. Без необходимости доверять друг другу.  Участники процесса могут быть уверены, что не соблюдения условий контракта приведет к  аннулированию также использование избавляют от необходимости в посредниках (Значительно уменьшают расходы на операцию).

Существует два вида криптографии:

Симмитричный ключ



1



Хэш – это уникальная строка фиксированной длинны.

Это функция которая относит