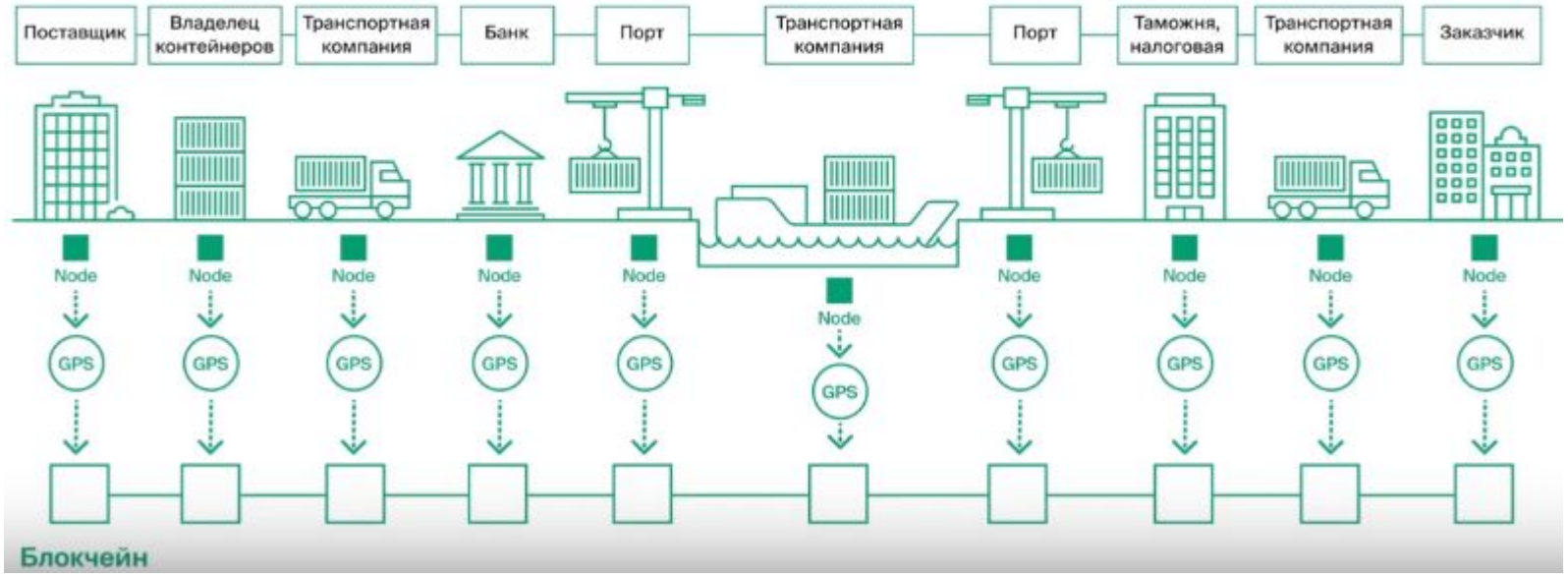
ЛЕКЦИЯ №2 ВВЕДЕНИЕ В БЛОКЧЕЙН

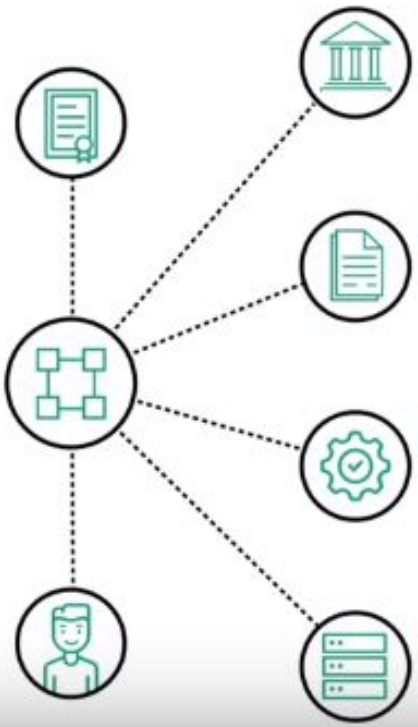
Москва, 2020

Система поставок на блокчейне



Ключевые преимущества

1. Легкая интеграция в существующий ИТ-ландшафт
2. Совместимость с любыми ИТ- системами
3. Развитие в виде маркетплейсов сервисов



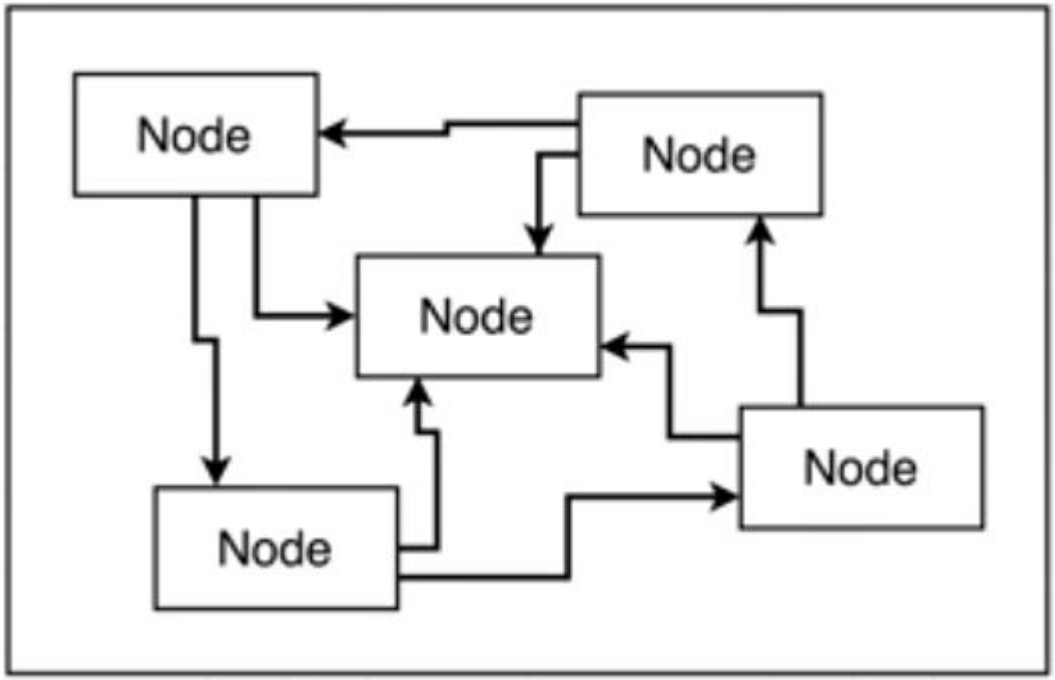
ERP Сведения о финансовых операциях, данных о персонале, данных операционного блока

ECM Данные из корпоративных систем документооборота, управление знаниями и контентом

MES Данные цехового уровня, связанные с производством на предприятии в целом

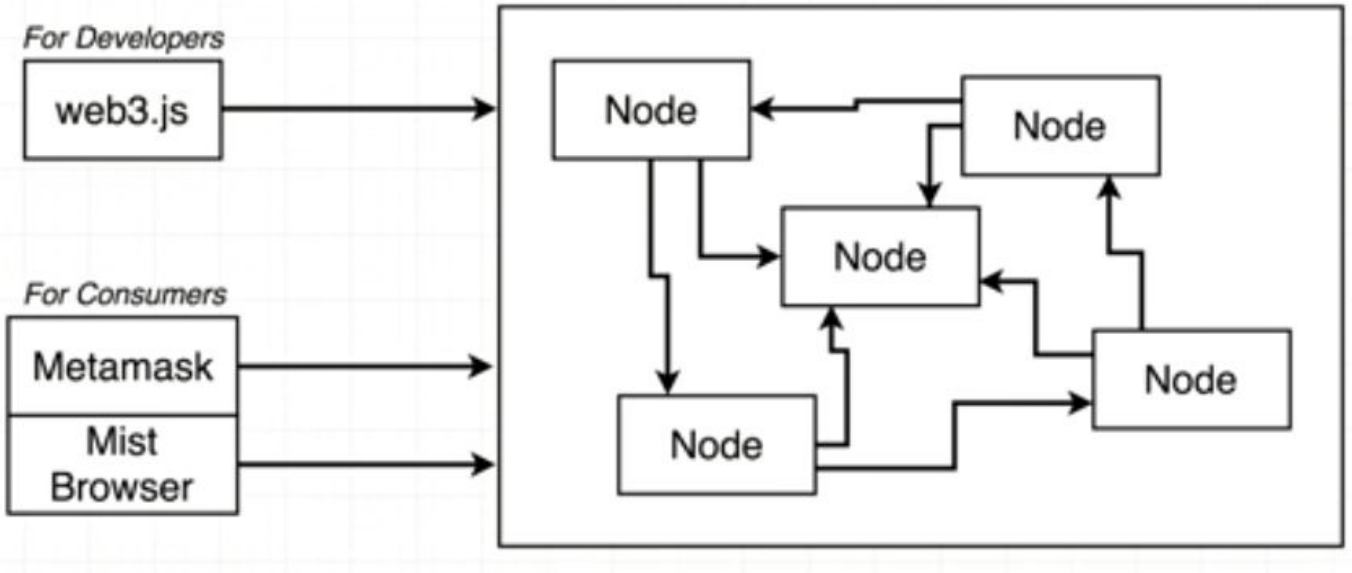
DW Интегрированные корпоративные хранилища данных для подготовки консолидированной отчетности

Эфириум



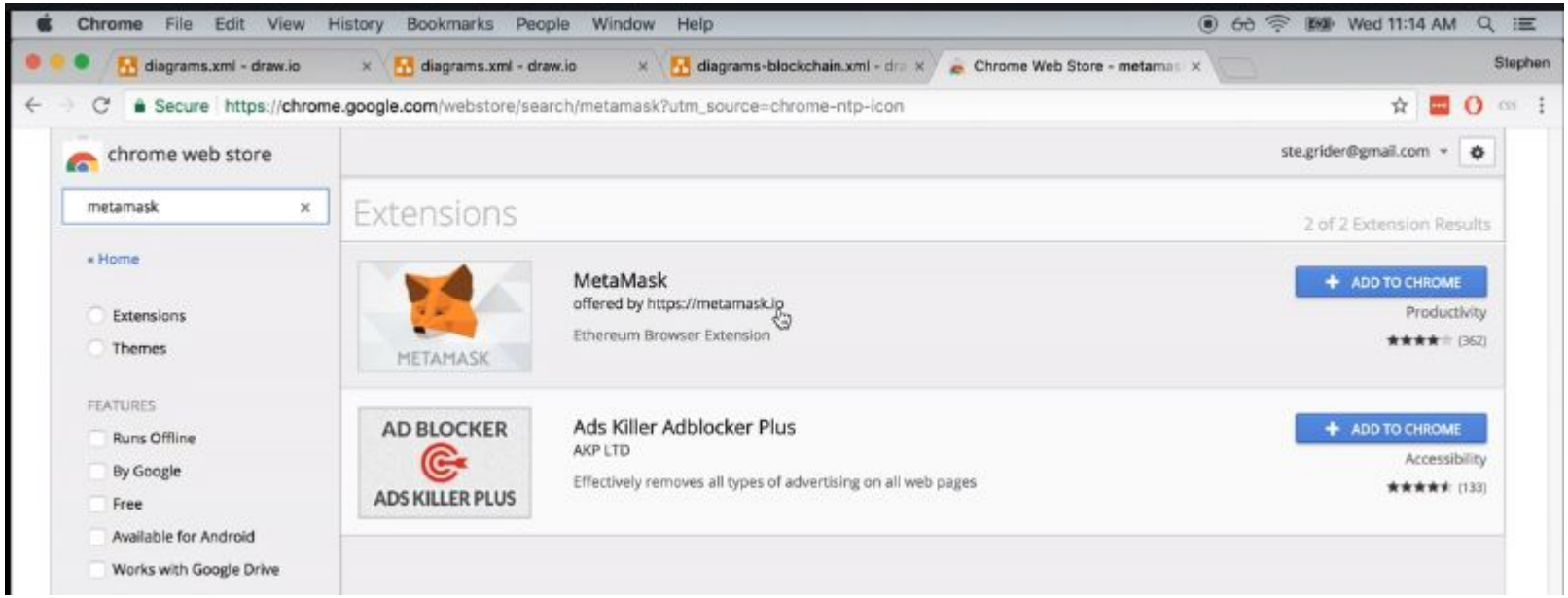
Эфириум используется для перевода денег и хранения данных.
Существует несколько различных эфириум сетей, сеть формируется один или множеством узлов
Любой может запустить узел
Каждый узел может содержать полную копия блокчейна.
Блокчейн - это база данных которая хранит записи в каждой транзакции которая имела место

Эфириум

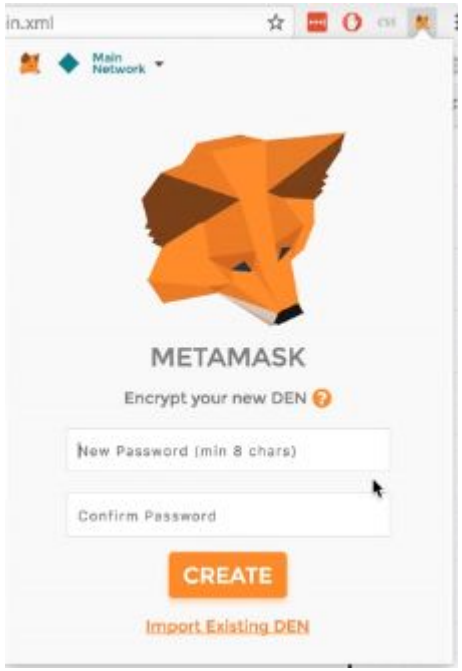

For Developers
web3.js
For Consumers
Metamask
Mist Browser
Node
Node
Node
Node
Node

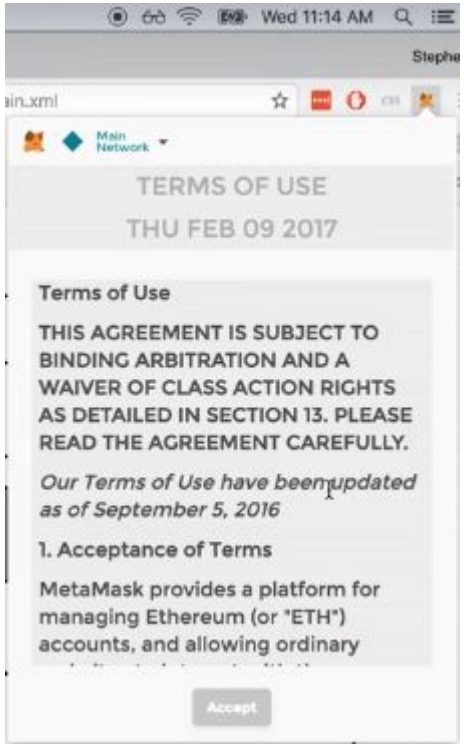
METAMASK INSTALLATION

METAMASK - ЭТО РАСШИРЕНИЕ CHROME ИЛИ РАСШИРЕНИЕ ДЛЯ БРАУЗЕРА, КОТОРОЕ ПОЗВОЛЯЕТ ЛЮДЯМ ДЛЯ ВЗАИМОДЕЙСТВОВАТЬ С СЕТЬЮ ETHEREUM



METAMASK INSTALLATION





METAMASK

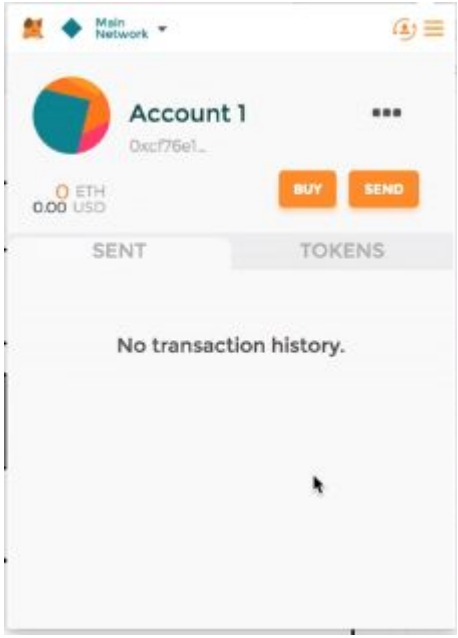
После этого мы подходим к главному экрану
Вы найдете раскрывающийся список, который говорит, что основная сеть.
Первая сеть, которая выбрана по умолчанию здесь, является основной сетью.

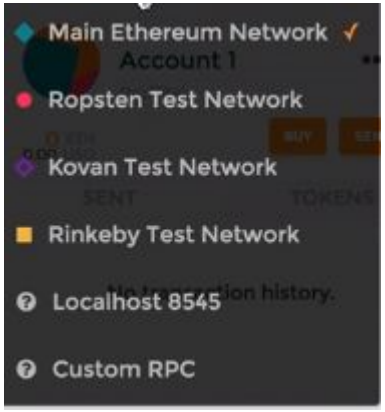
Основная сеть - это сеть, где монеты действительно чего-то стоят, и именно здесь мы разворачиваем реальные приложения.

Вы можете увидеть выпадающий список, который также показывает нам несколько других доступных сетей, три сети под основной.

Итак, это - все тестовые сети.

Эти сети используются для тестирования кода и получения бесплатного эфира для тестирования наших контрактов, с которыми мы собираемся в конечном итоге проделать большую работу.





Эфириум

Эфириум использует один аккаунт для всех сетей.

Он создал учетную запись, которая имеет три отдельные части информации - адрес учетной записи открытый ключ, закрытый ключ

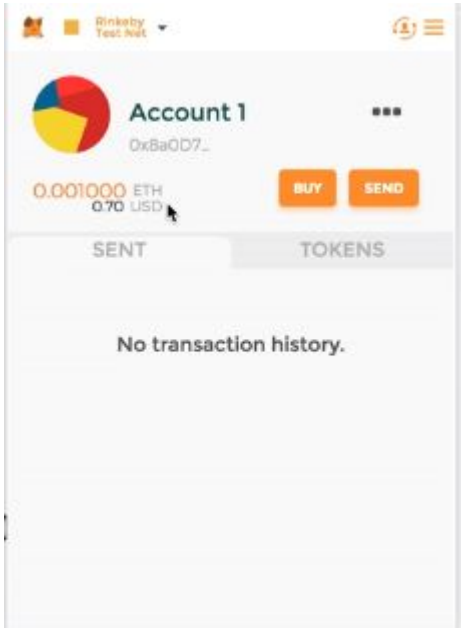
Это три части информации, которые составляют учетную запись и адрес может рассматриваться как адрес электронной почты.

ПОЛУЧЕНИЕ ЭФИРОВ

Это маленький веб-сайт, который будет принимать адрес
вашей учетной записи, и они отправят вам небольшое количество эфира

rinkeby-faucet.com

Для отправки денег из пункта А или со счета на счет Б. требуется некоторое время. Примерно через 30 секунд мы увидим сообщение:

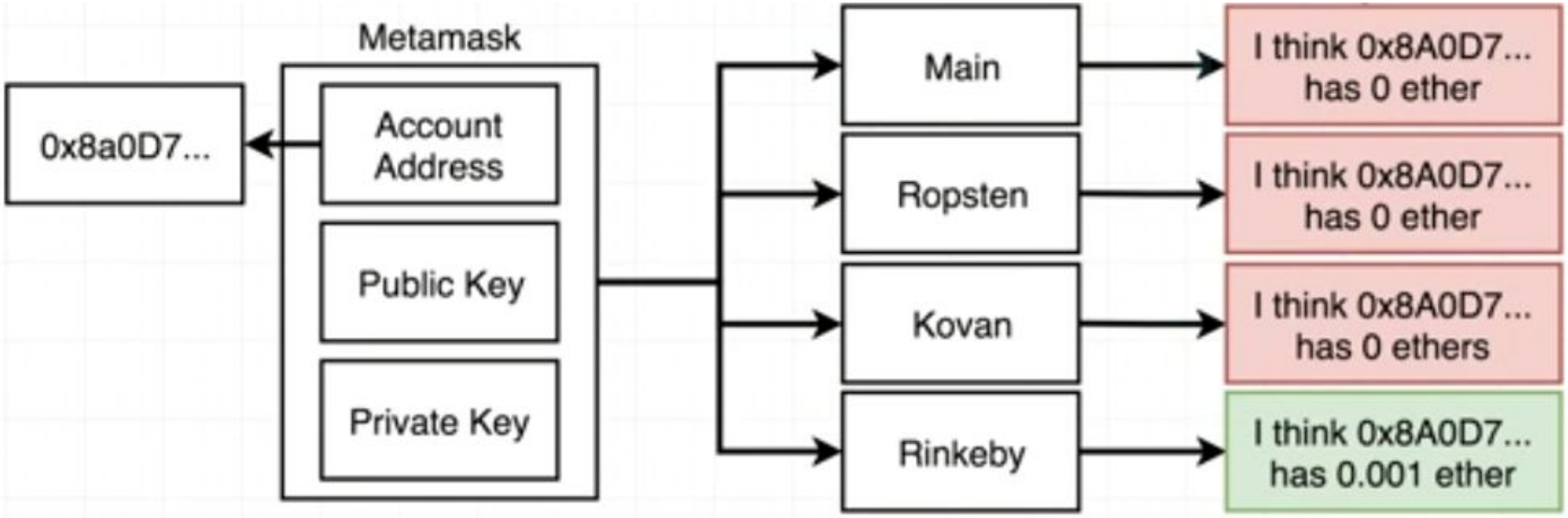


If you're curious, here is your transaction id:
0x3a7e14dc1a1de12217577f385f336c2c8627795da5d63a74a81f4af04744a132

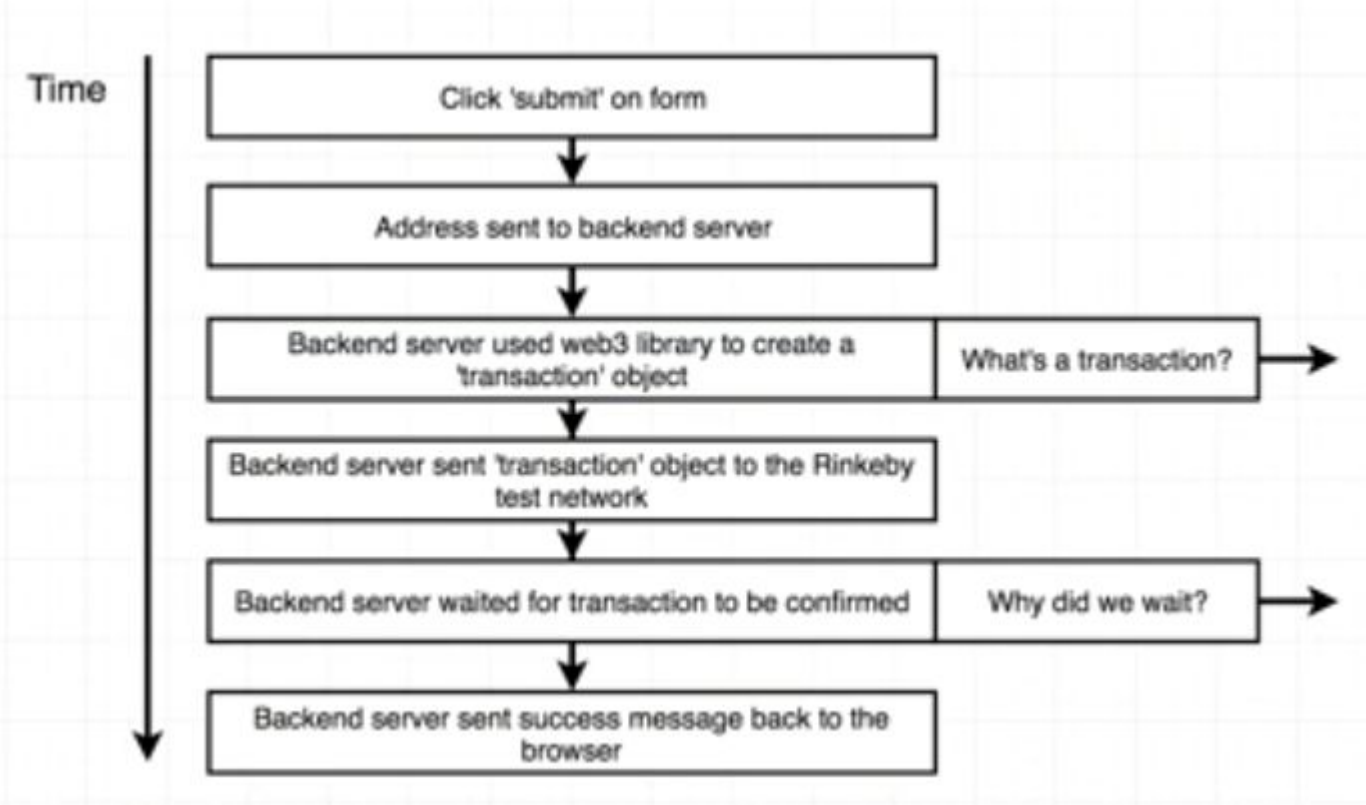
На самом деле есть еще один веб-сайт, очень похожий на этот

Перевод денег

https://faucet.rinkeby.io/
https://faucet.ropsten.be/



Перевод денег



ЧТО ТАКОЕ ТРАНЗАКЦИЯ ?

Транзакция - это запись, которая описывает одну учетную запись, которая пытается отправить деньги на другую учетную

Transaction

nonce	Сколько раз отправитель отправил транзакцию
to	Адрес счета, на который идут эти деньги
value	Количество эфира, отправляемого на целевой адрес
gasPrice	Количество эфира, которое отправитель готов платить за единичный газ эта транзакция обработана
startGas/gasLimit	Единицы газа, которые может потреблять транзакция
v	Криптографические фрагменты данных, которые можно использовать для генерации адреса учетной записи отправителя. Генерируется из личного ключа отправителя.
r	
s	

ЧТО ТАКОЕ
ТРАНЗАКЦИЯ ?

Транзакция создается в любое время, когда два счета обменивают определенную сумму денег. Поэтому, когда я только что отправил вам деньги, я создал объект транзакции, а затем отправил его в эфирную сеть для обработки.
Этому объекту присвоены различные свойства, которые вы увидите здесь с левой стороны.

Первое свойство, которое существует в объекте транзакции, это число, которое говорит нам, сколько раз отправитель отправил транзакцию.
Далее это значение это количество эфира, который мы хотим отправить

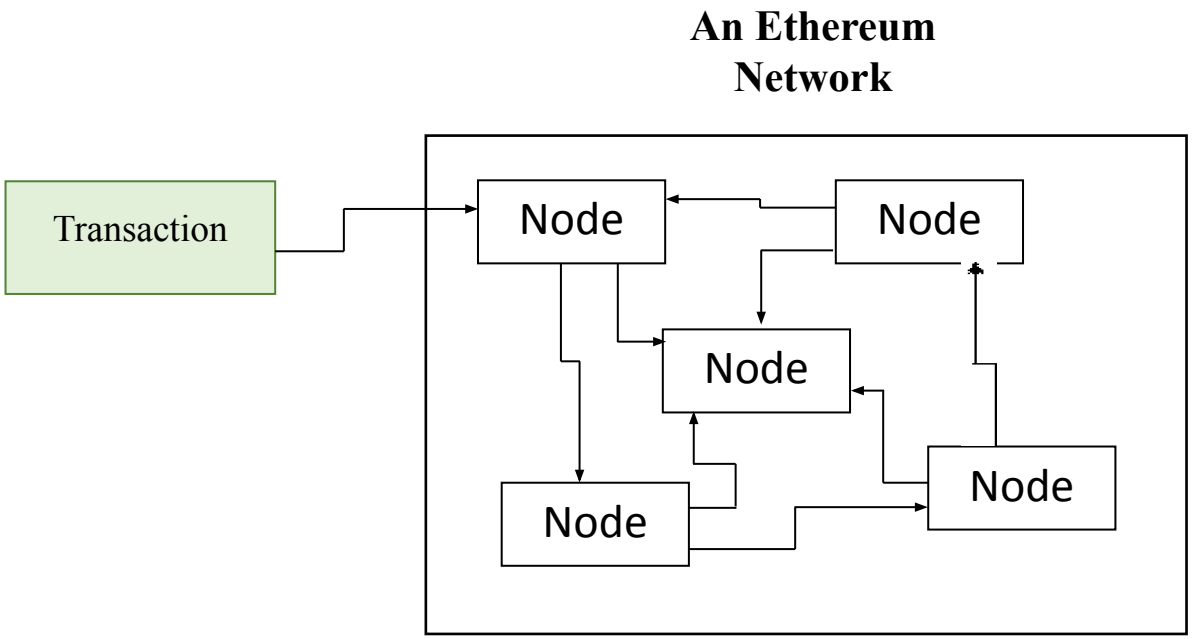
v r s свойства генерируются закрытым ключом этих центров. Так что центр возьмет свой закрытый ключ.
Они генерируют эти три значения. И эти три значения могут быть использованы для генерации адреса учетной записи
человек, который пытается отправить деньги.
Теперь генерируем R и S из закрытых ключей или из закрытого ключа.
Таким образом, если у вас есть закрытый ключ, вы можете сгенерировать V R и S, но если у вас есть r in s, вы не можете вычислить закрытый ключ.

ПОЧЕМУ ТРАНЗАКЦИЯ ЗАНИМАЕТ ВРЕМЯ?

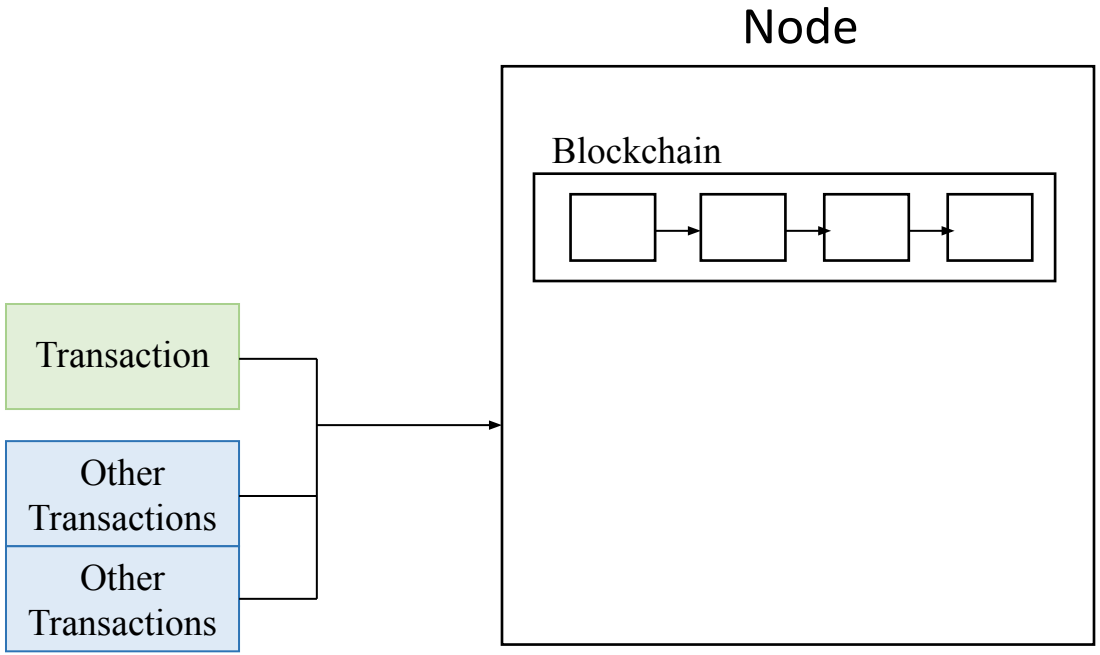
Таким образом, закрытый ключ используется один раз для генерации этих чисел и существования этих чисел.

Мы использовали библиотеку Web 3 для создания объекта транзакции. После создания этого объекта та же библиотека web 3 затем используется для отправки этого объекта транзакции в тестовую сеть.
Таким образом, транзакция отправляется в сеть, а затем мы ждем подтверждения транзакции.
Этот шаг, занимает около 30 секунд.

Транзакция идет к одному конкретному узлу.
Таким образом, наши приложения всегда будут взаимодействовать с одним узлом, и этот узел будет связываться с остальной частью сети



ПОЧЕМУ ТРАНЗАКЦИЯ ЗАНИМАЕТ ВРЕМЯ?



Узел имеет полную копию цепочки блоков.
В мире есть и другие люди, которые хотят отправлять транзакции.
Таким образом, возможно, в общей сложности три транзакции поступают в этот узел одновременно
Этот узел будет принимать эти транзакции

ПОЧЕМУ ТРАНЗАКЦИЯ ЗАНИМАЕТ ВРЕМЯ?

Block №
Nonce:
Data:
Prev
Hash:

Block №
Nonce:
Data:
Prev
Hash:

https://andersbrownworth.com/blockchain/block

Узел имеет полную копию цепочки блоков.

В мире есть и другие люди, которые хотят отправлять транзакции.

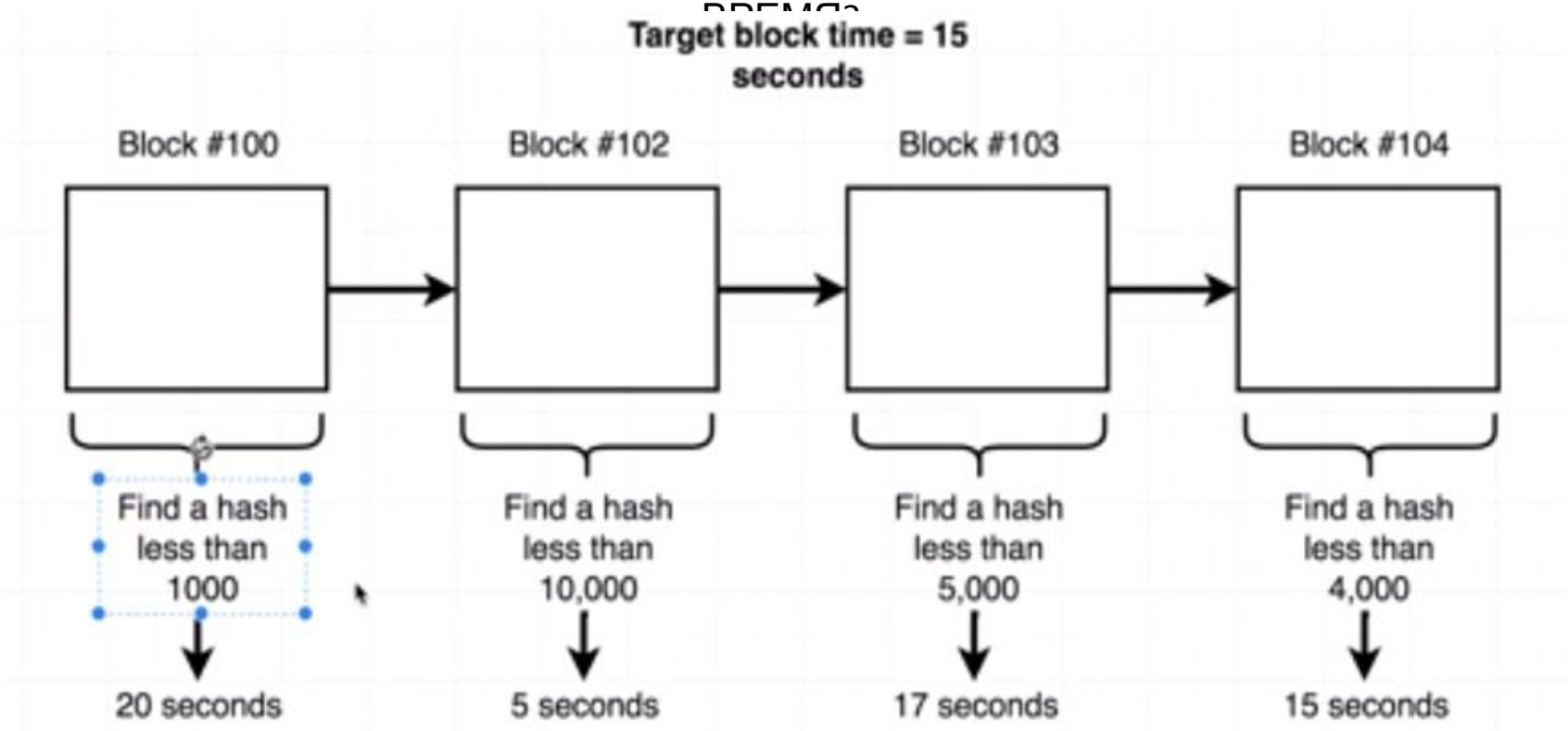
Таким образом, возможно, в общей сложности три транзакции поступают в этот узел одновременно

Этот узел будет принимать эти транзакции

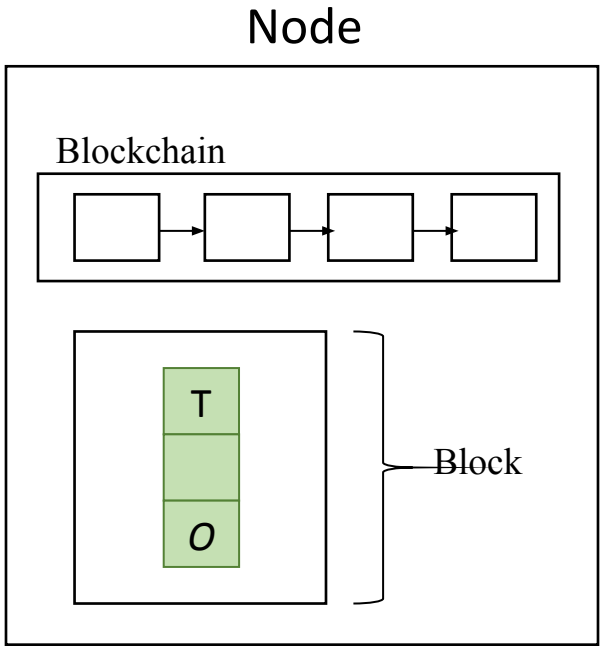
ПОЧЕМУ ТРАНЗАКЦИЯ ЗАНИМАЕТ ВРЕМЯ?

Data	+	Nonce	=	Output Hash	Output hash as a base 10 number	Is this less than 1000?
'Hi There'		0		a23042b2e	178917215	no
'Hi There'		1		cbc1491	29589283	no
'Hi There'		2		0ca24258	94869869	no
'Hi There'		3		d9eed91	13938166	no
'Hi There'		4		1488baec	419386918	no
'Hi There'		5		0077bbb	100	yes

ПОЧЕМУ ТРАНЗАКЦИЯ ЗАНИМАЕТ ВРЕМЯ?



ПОЧЕМУ ТРАНЗАКЦИЯ ЗАНИМАЕТ ВРЕМЯ?



Этот блок, что логика проверки - это то, что занимает 30 секунд.
долго, чтобы получить ответ к нам. Поэтому, когда эти транзакции собраны в блок, узел начинает выполнять некоторые вычисления в блоке.

И этот процесс называется майнингом.

Contract Account	
Field	Description
balance	Amount of ether this account owns
storage	Data storage for this contract
code	Raw machine code for this contract