、区块链开发者进阶知识：

evm虚拟机

合约吃透

uni1 2 3（uniswap 去中心化交易所协议）

bfc（BitFree Cash（简称BFC）Cuckaroo29算法）

撮合交易 合约交易 代码层（）

大姨父 yfi共识算法（YFI是yearn.finance的治理代币）（YFII续上）

dart（后端开发 对象语言）

--------------------------------------------------------------------------------

layer 2 的解决方案。

==============================================================

leon:

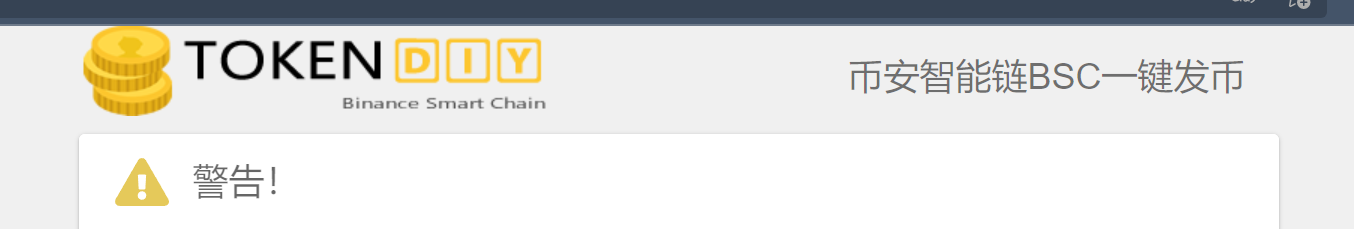
比如我发布一个游戏在BSC链上运行合约产生代币或者代币交易到钱包，这个费用有什么标准？或者在哪里可以查到这些开发约定的标准？

Devil:

发一个好像在几十块钱。

web3js 有个方法，estimateGas 搜下web3js

Devil:



这种有资产的就别去试，你写个合约调用一下就看到了

油管上教程很多

Devil:

0.0798美元 0.5人民币左右

打包就慢

转账快手续费就高

leon:

一般你们设置的这个数字，要多少秒能跑完？

Devil:

20s以内，一般几s

===========================================================================

 IPFS全称是Inter Planetary File System，直接翻译的话叫做“星际文件系统”，它由Protocol Lab提出，是一种点对点（P2P）的分布式文件系统。

目标是为了补充（甚至是取代）目前统治互联网的超文本传输协议（HTTP），将所有具有相同文件系统的计算设备连接在一起。

原理基于内容的地址代替基于域名的地址，无需验证发送者身份，而只需验证内容的哈希，通过这样 可以让网页的速度更快、更安全、更健壮、更持久。

IPFS的应用 2021-04-14 09:48

IPFS已得到全球认同，2019年，IPFS公共网络增长了30倍！每天有成千上万的节点参与IPFS网络！每周都有数百万用户访问IPFS HTTP网关！而在更广泛的IPFS生态系统中，有数百个dapp、工具和项目。

例如，IPFS已被德国航天中心用作遥测数据存储，全球第一大浏览器谷歌支持IPFS分布式协议，美国阿波罗登月使用IPFS保存机密文件，加拿大政府建立托管在IPFS上的以太坊浏览器等。随着Filecoin加入，IPFS的应用加快落地，并且越来越广泛。

Filecoin的应用

10月15日Filecoin主网上线，各路矿工纷纷进场。Filecoin，建立在IPFS上的分布式存储网络，新一代基础设施诞生，开启了人类文明存储的新时代。利用世界任何地方闲置的硬盘空间，在开放的市场中，提供数据存储和检索服务，从而使任何人都可以作为存储供应商，参与其中获利。

大量分布式应用Dapp使用filecoin做存储，filecoin成为去中心化生态重要的分布式存储网络基础设施。实现Filecoin的使命，为人类社会的信息奠定一个分布式的、高效且强大的基础。

分布式存储发展趋势可以依托“区块链”+“分布式存储”+“云计算” 构建下一代D-IaaS云服务基础设施；基于区块链和分布式存储软硬件创新研发，构建分布式大数据中心，提供更优质的服务，重构数字化底层产业生态。

2021-08

IPFS和区块链是完美的搭配，我们可以使用IPFS处理大量数据，并将不变的、永久的IPFS链接放置到区块链事务中，而不必将数据本身放在区块链中。毕竟，区块链的本质是分布式账本，本身的瓶颈之一就是账本的存储能力，目前大部分公链的最大问题是没法存储大量的数据在自己的链上。比特币至今全部的区块数据也才数百GB，以太坊这样可编程的区块链项目也只能执行和存储小段合约代码，DApp的发展受到了很大的制约。运用IPFS技术解决存储瓶颈是可行方案之一。

——本文节选自《IPFS原理与实践》

=============================================================================

2021-12-14

、IPFS存储原始数据，也是链上；

与主链没有任何联系，通过地址访问IPFS；

、SOL高玩平台，生态完善，高速；

、合约Owner可以自己赋权销毁币；

、游戏逻辑也写在合约上，跑在链上；

、赌博+挖币（发行）的简单游戏；

理解为提现到以太钱包即为铸币成功？此刻合约的运行产生了Gas费用，即发币代价，但是此币依然不可通兑；

游戏内代币可以认为是积分，不上链，积分兑换成自代币需要上链运行？

自代币再交易、兑换成公链币；

、发币成本就是合约执行成本；

（发币的合约，与游戏铸币的合约可以分开吗？）

、团队：全流程打通产品经理、合约编写，前端web3，专业推广的美术，市场沟通、……

、技术只占20%，社区公会是推广核心；

、专门公司测试上链前的智能合约；

、layer 2 可以认为是ERC2.0的侧链；

、分布式（链上）聊天工具？管理？

==============================================================

MetaMask钱包启动时不知为何锁定，需要解锁后才能启用测试网络，否则就只有Ethem一个网络可以用。

网络名称： BSC主网

新增RPC URL：https://bsc-dataseed1.binance.org/

链ID: 56

符号： BNB

区块浏览器 URL: https://bscscan.com/

Ropsten 测试网络

https://ropsten.infura.io/v3/9aa3d95b3bc440fa88ea12eaa4456161

3

ETH

https://ropsten.etherscan.io

Rinkeby 测试网络

https://rinkeby.infura.io/v3/9aa3d95b3bc440fa88ea12eaa4456161

4

ETH

https://rinkeby.etherscan.io

Goerli 测试网络

https://goerli.infura.io/v3/9aa3d95b3bc440fa88ea12eaa4456161

5

ETH

https://goerli.etherscan.io

Kovan 测试网络

https://kovan.infura.io/v3/9aa3d95b3bc440fa88ea12eaa4456161

42

ETH

https://kovan.etherscan.io

BSC主网

https://bsc-dataseed1.binance.org/

链ID: 56

符号： BNB

区块浏览器 URL: https://bscscan.com/

BSC测试：

https://speedy-nodes-nyc.moralis.io/03a2a57cae4f839aae2eb484/bsc/testnet

ID：97

BNB

https://testnet.bscscan.com/

=================================================================================

1.1、nodejs

前往nodejs官网（https://nodejs.org/en/）,选择下图左边的LTS版本下载，下载完成后傻瓜式安装。

1.2、truffle

npm install -g truffle

下载完成后查看版本信息：

truffle version

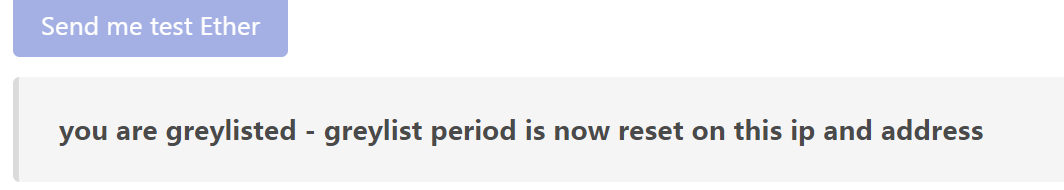
正常情况下返回如下信息：

Truffle v5.0.2 (core: 5.0.2)

Solidity v0.5.0 (solc-js)

Node v8.12.0

========================================================================



==============================================================================

精通以太坊HTML版链接：

<https://github.com/inoutcode/ethereum_book>

asciidoc文档

==============================================================================

以太坊的实时数据：

<https://bitinfocharts.com/ethereum/>

|  |  |
| --- | --- |
| [Block Time](https://bitinfocharts.com/comparison/ethereum-confirmationtime.html) [(average t](https://bitinfocharts.com/comparison/ethereum-confirmationtime.html)ime between blocks) | 13.4s |
| Blocks Count | 13,828,327 (2021-12-18 17:27:37) |
| [Block Size](https://bitinfocharts.com/comparison/ethereum-size.html) | 73.499 KBytes |
| Blocks last 24h | 6,450 |
| Blocks avg. per hour (last 24h) | 269 |
| Reward Per Block | 2+1.61+0.00356+0.09636-1.29 ETH ($9,482.68) |
| Reward (last 24h) | 12,900+10402+22.94+621.5-8299 ETH ($61,163,256.47) |
| [Fee in Reward](https://bitinfocharts.com/comparison/ethereum-fee_to_reward.html) [(Average Fee](https://bitinfocharts.com/comparison/ethereum-fee_to_reward.html) Percentage in Total Block Reward) | 6.28% |
| [Difficulty](https://bitinfocharts.com/comparison/ethereum-difficulty.html) | 11.456 P **-0.54%** in 24 hours |
| [Hashrate](https://bitinfocharts.com/comparison/ethereum-hashrate.html) | 903.864 Thash/s **-0.15%** in 24 hours |
| [Ethereum Mining Profitability](https://bitinfocharts.com/comparison/ethereum-mining_profitability.html) | 0.0677 USD/Day for 1 MHash/s |
|  |  |

===============================================================================

solidity学习链接：

<https://blog.csdn.net/weixin_45067603/article/details/105726491>

<https://www.bilibili.com/video/BV1St411a7Pk?p=1> 有65节课的详细教学

<https://www.bilibili.com/video/BV1NJ411D7rf/?spm_id_from=333.788.recommend_more_video.0> 九十课

<https://zhuanlan.zhihu.com/p/258512762> 知乎总结的视频收录

官方文档：<https://solidity-cn.readthedocs.io/zh/develop/>

学习游戏：<https://cryptozombies.io/zh/>

=============================================================

ubuntu系统搭建以太坊Geth私有链

1、安装curl、git

apt-get update

apt-get install git

apt-get install curl

2、安装go

（1）简便方式：

sudo apt-get install golang-go

（2）手动下载并编译方式：

curl -O https://storage.googleapis.com/golang/go1.5.1.linux-amd64.tar.gz

Unpack it to the /usr/local (might require sudo)

tar -C /usr/local -xzf go1.5.1.linux-amd64.tar.gz

建立软链接

sudo ln -s /usr/local/go/bin/\* /usr/bin/

3、配置go的环境变量

注意GOPATH是工作环境目录，不要跟GOROOT重复了；

（warning: GOPATH set to GOROOT (/usr/local/go) has no effect）

mkdir -p ~/go; echo "export GOPATH=$HOME/go" >> ~/.bashrc

echo "export PATH=$PATH:$HOME/go/bin:/usr/local/go/bin" >> ~/.bashrc

使修改生效：source ~/.bashrc

验证go :

go version

安装python：

依赖包：

yum -y install zlib-devel bzip2-devel openssl-devel ncurses-devel sqlite-devel readline-devel tk-devel gdbm-devel db4-devel libpcap-devel xz-devel

4、nodejs、npm

curl -sL https://deb.nodesource.com/setup\_4.x | sudo -E bash -

apt-get install nodejs

验证是否安装成功

node -v

npm -v

ubuntu库内直接安装：（版本比较旧）

sudo apt update

sudo apt install nodejs npm

5、安装以太坊环境

sudo apt-get install software-properties-common（OK）

sudo add-apt-repository -y ppa:ethereum/ethereum（OK）

sudo add-apt-repository -y ppa:ethereum/ethereum-dev（OK）

sudo apt-get update

sudo apt-get install ethereum（OK）

6、安装solc（solidity编译环境）

sudo add-apt-repository ppa:ethereum/ethereum（OK）

sudo apt-get update（OK）

sudo apt-get install solc（OK）

6.15、安装truffle：**sudo npm install -g truffle**

leon@ubuntu:~$ truffle version

Truffle v5.4.25 (core: 5.4.25)

Solidity v0.5.16 (solc-js)

Node v17.3.0

Web3.js v1.5.3

（单独安装web3：**sudo npm install web3**）这里不需要单独装。）

7、创建三个账户

连续输入三次命令：geth account new

得到三个公钥地址

8、编辑创世块文件（json）

将三个地址放入"alloc"中，

复制代码

{

"nonce": "0x0000000000000042",

"difficulty": "0x1",

"alloc": {

"0d2e08a2615d5c46734058f34b307db0eda5ba6e": {

"balance": "20000009800000000000000000000"

},

"1f9035c1ed2802fe7f96e8a28890d8816af14c9c": {

"balance": "20000009800000000000000000000"

},

"59b0a1db6b4de1d303d440da1d02fafd3f4f41af": {

"balance": "20000009800000000000000000000"

}

},

"config": {

"chainId": 15,

"homesteadBlock": 0,

"eip155Block": 0,

"eip158Block": 0

},

"mixhash": "0x0000000000000000000000000000000000000000000000000000000000000000", "coinbase": "0x0000000000000000000000000000000000000000",

"timestamp": "0x00",

"parentHash": "0x0000000000000000000000000000000000000000000000000000000000000000",

"extraData": "0x11bbe8db4e347b4e8c937c1c8370e4b5ed33adb3db69cbdb7a38e1e50b1b82fa",

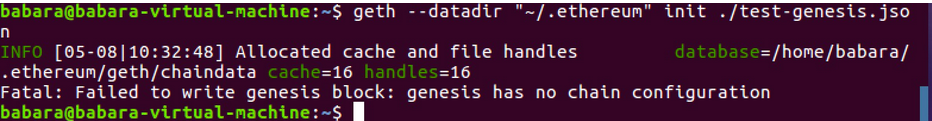
"gasLimit": "0xb2d05e00"

}

初始化创世块:

geth --datadir "./myblockchain" init genesis.json

注意：划线部分如果不添加，会出现以下错误：



9、配置自动解锁账号的脚本

在./ethereum下创建password文件，在里面输入密码，每个账号一行密码如：

123456

123456

123456

10、配置以太坊启动脚本private\_blockchain.sh(名字自取)

geth --rpc --rpcaddr="0.0.0.0" --rpccorsdomain="\*" --unlock '0,1,2' --password ~/.ethereum/password --nodiscover --maxpeers '5' --networkid '1234574' --datadir '~/.ethereum' console

每次启动geth节点时，只需要输入一下命令

bash private\_blockchain.sh

11、启动后，输入eth.getCompilers(),可能会出现一下情况

这是因为，安装以太坊环境时自动下载了geth客户端是1.6以上版本的，但是1.6版本客户端中没有getCompilers()函数，后续可能会开发别的方法来实现这个功能。

我的解决办法是下载geth1.5.9版本，覆盖掉原来的geth。

之后，输入eth.getCompilers()，会出现，
这是因为没有指定编译器，另开一个终端，输入which solc
之后，在geth终端中输入:

会出现这个是因为我用的ubuntu虚拟机，提示我虚拟机的内存不足，当我把虚拟机内存增加到2G后，这个问题就解决了。

再次输入：

大功告成！

===================================================================

Ubuntu安装以太坊开发环境 2020-11-11

3. 启动私有链

启动私链：(geth 1.10.13已不支持rpc等参数)

geth --identity "myethereum" --rpc --rpcaddr "127.0.0.1" --rpcport "7545" --rpccorsdomain "\*" --datadir ./myblockchain --rpcapi "db,eth,net,web3,admin,personal" --networkid 5777 console --allow-insecure-unlock

这里先介绍一下一些参数：

参数名 描述

identity 区块链的标识，用于标识目前网络的名字

init 指定创世块文件的位置，并创建创世块

datadir 当前区块链数据存放的位置

port 网络监听端口，默认30303

rpc 启动rpc通信

rpcapi 设置允许rpc的客户端，一般为db，eth，net，web3

rpccorsdomain 指定什么url能连接到你的节点执行rpc定制端任务，如果输入是“\*”，则任何url都可以连接到你的rpc实例。

rpcaddr 连接rpc的地址，默认为localhost，为了方便访问建议使用本机IP地址

rpcport 连接rpc的端口，默认为8545

networkid 设置当前区块链的网络ID，用于区分不同的网络，是一个数字，公链为1；这个和创世块文件的chainid没有直接关联（Leon认为这个值就是chainid）

console 启动命令行模式，可以再geth中执行命令

、geth控制台启动和退出

最简单的启动方式如下：

>geth console

启动成功之后可以看到输入提示符 >

退出 Geth 控制台也很简单，只要输入：

>exit

5. geth创建账号、启动挖矿、停止挖矿

、在geth终端，初始化后系统无账号，需要创建新账号，才能启动挖矿：

eth.accounts

由于我事先新建了两个账户，所以上图显示两个账户的地址；

、新建账户：

personal.newAccount("12345678");

、获取第一个账户的余额：

eth.getBalance(eth.accounts[0])

、开始挖矿：

miner.start()

、停止挖矿：

miner.stop()

geth常用操作

、解锁账户：

personal.unlockAccount(eth.accounts[0])

、交易池状态：

txpool.status

、区块总数：

eth.blockNumber

、获取交易：

eth.getTransaction("0x5cff7cd36fe841a7eb35ba30f99c8851a4e57715e4b648aeb341c3c2619879cd");

、获取第421个区块的信息：

eth.getBlock(421);

、连接到其他节点：

admin.addPeer();

、设置挖矿账户：

miner.setEtherbase(eth.coinbase)

、转账交易，要先解锁账户：

eth.sendTransaction({<!-- -->from:"0xe76c73baf75a67dd9637ad2da33d13288d73ee16",to:"0x62232534fda9ffe0c5f32cf6d48568a861065fea",value:web3.toWei(100,"ether")})

==============================================================

、初始化创世区块：

leon@ubuntu:~/ethmchain/consortium\_blockchain$

geth --datadir "./myblockchain" init genesis.json

**、启动此链命令：**

geth --identity "myethereum" --rpc --rpcaddr "127.0.0.1" --port 30304 --rpcport "7545" --rpccorsdomain "\*" --datadir ./myblockchain --rpcapi "db,eth,net,web3,admin,personal" --networkid 5777 console --allow-insecure-unlock

、本机可用：

**geth --datadir "myblockchain" --networkid 84348 console --nodiscover 2>output.log**

（–networkid 123 就是在genesis.json文件中配置的chainId；

–nodiscover是让控制台启动以后不去同步节点

（不加的话界面会显得比较繁琐复杂，一直在Looking for peers）

2>output.log就是将日志信息输出到当前目录下的output.log的文件里）

或写启动脚本：

运行这个指定目录下指定创世区块，好像就启动了链：

geth --datadir "./myblockchain" --networkid 84348

leon@ubuntu:~/ethmchain/consortium\_blockchain$ geth --datadir "./myblockchain" --networkid 84348

=============================================================================

以太坊**geth GPU挖矿**分析 天一生水water 2018-07-25 21:09:08

以太坊geth 默认是使用CPU挖矿，如果需要使用GPU 挖矿，需要单独的挖矿程序ethminer.exe

https://github.com/ethereum-mining/ethminer

**ethminer** 是一个独立的挖矿软件，可以连接geth 的rpc端口，通过getwork协议与geth交互。

geth中GPU挖矿主要通是通过miner包中的remote-agent.go来完成的。

-----------------------------------------------------------------------------------------------------------

（小白韭菜到币圈大佬)第三期、显卡挖矿：从入门到放弃

2018-3-

ETH挖矿软件主要有两个：

一是Claymore，地址是https://bitcointalk.org，特点是可以双挖，即挖ETH的同时还可以挖另一种币，缺点是要抽水1%，双挖抽2%。双挖费电费显卡，关键是总收益未必高，不推荐。

二是ethminer，地址是https://github.com/ethereum-mining/ethminer/releases，单挖效率超过Claymore，开源不抽水。

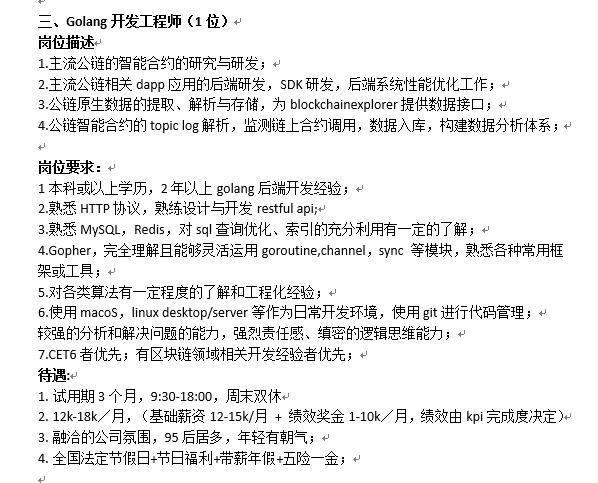
ETH矿池主要有两个，

https://ethermine.org/,总算力强劲，但在国外。

http://pool.ethfans.org/，在国内，总算力不如上面的。

------------------------------------------------------------------------------------------------------------------------

=======================================================================



陈鹿林(957284805)· 2021/12/4 23:44:56有智能合约玩的溜的大佬吗

南信芝麻糊 11:23:02

gamefi 25k少了点吧  我做defi的现在都30了

写rust也可以 只考虑40+的岗位   evm和dot都很熟悉  写过点substrate

=================================================================================