SimpleChain 联盟链（基础版）

开发者手册

目录

1 背景知识

SimpleChain 联盟链以简单高效的共识机制、高可用性和可扩展性、全方位的安全机制、简洁的合约设计、多角度的性能优化为设计目标，构建功能完善、技术成熟的联盟链底层架构，为上层业务应用提供标准化服务和技术组件。

1.1 联盟链简介

什么是区块链

对区块链最好的描述是将其描述为一个公共数据库，它由网络中的许多计算机更新和共享。

"区块"指的是数据和状态是按顺序批量或"区块"存储的。 如果你向别人发送交易，需要将交易数据添加到一个区块中才算成功。

"链"指的是每个区块加密引用其父块。 在不改变所有后续区块的情况下，一个区块的数据是不能改变的，这需要整个网络的共识。

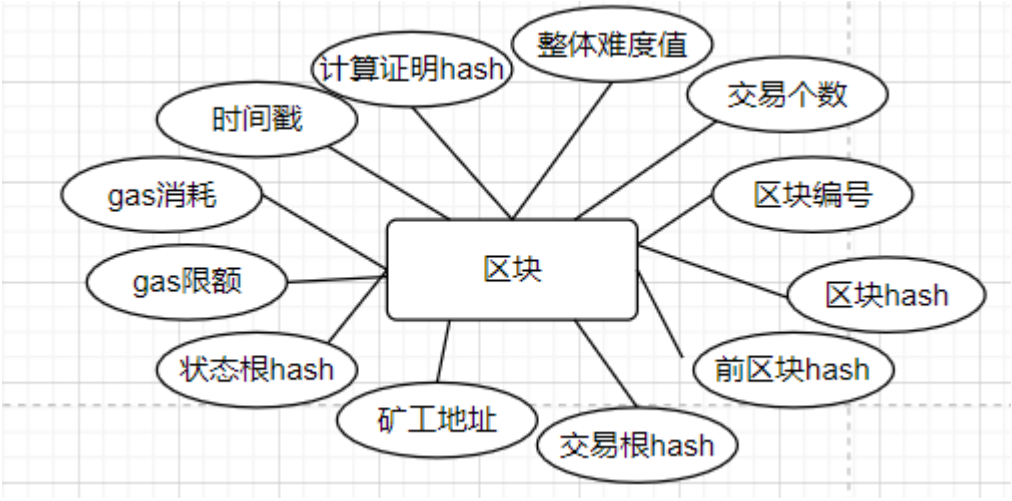
每一个新的区块和整个链必须得到网络中每个节点的同意。 这是为了让大家拥有相同的数据。 新的区块会被广播到网络中的节点，经过检查和验证，同步更新状态。

联盟链特点

- 高性能：不同于公有链，联盟链能够在短时间达成共识，大大缩短了出块时间。
- 高可靠 ：数据上链后，交易会被广播到各个节点中，达成共识后出块，保证了数据的准确和权威。
- 高隐私：数据不会默认公开，联盟链的数据只限于联盟里的机构及其用户才有权限进行访问。

1.2 区块

区块是指一批交易的组合，并且包含链中上一个区块的哈希。 这将区块连接在一起（成为一个链），因为哈希是从区块数据中加密得出的。 这可以防止欺诈，因为以前的任何区块中的任何改变都会使后续所有区块无效，而且所有哈希都会改变，所有运行区块链的人都会注意到。



什么是创世区块

区块链在网络初始组建时系统生成的第一个区块就称之为创世区块。

在 SimpleChain 联盟链中，创世区块被赋予了更多的含义。其中包括了出块时间设定，初始账户设置，共识算法等一系列重要信息。

SimpleChain 联盟链中创世区块的生成，请见《SimpleChain 联盟链（基础版）运行维护手册》

1.3 交易

交易是由账户发出，带密码学签名的指令。 账户发起交易以更新 SimpleChain 网络的状态。交易包括下列信息：

一旦您发送交易，加密算法生成交易哈希，例如下面的一串 16 进制的数字：

0x97d99i7fxh96j1111a21b12c933c949d4f31684f1d6954ff477j7g4s838ff017

然后将该交易转播到网络，并且与大量其他交易一起包含在一个集合中。您的交易还将得到一个区块确认号码。 该号码是包含了您交易的区块是自区块创建以来的第几个区块，并得到交易回执。

1.4 账户

在 SimpleChain 联盟链中，账户被定义为发送和接收交易的地址。它可以是一个由用户控制的实体，也可以是一个部署了智能合约的地址。

账户有四个字段：

- nonce – 显示从账户发送的交易数量的计数器。 这将确保交易只处理一次。 在合约账户中，这个数字代表该账户创建的合约数量
- balance – 显示账户的余额
- codeHash – 所有代码片段都被保存在状态数据库的相应哈希下，供后续检索。对于合约账户，合约代码经过哈希处理并存储为 codeHash。对于用户持有的账户，codeHash 字段是空字符串的哈希值。
- storageRoot – 有时被称为一个存储哈希。 Merkle Patricia 树的根节点的 256 位哈希，Merkle Patricia 树编码了账户的存储内容（256 位整数值键值对），256 位整数值的 Keccak 256 位哈希作为 Key，RLP 编码的 256 位整数值作为值。 此树编码账户存储内容的哈希，默认情况下是空。

账户的创建

创建一个账户，就是创建一个随机的公/私钥对。私钥由 64 个十六进制字符组成，可以用密码加密保存。

公钥是使用椭圆曲线数字签名算法从私钥生成的。 您可以将公钥的最后 20 字节前面添加 0x 来获得您账户的公共地址。

可使用 SimpleChain 的命令行接口执行下面的函数来创建一个账户：

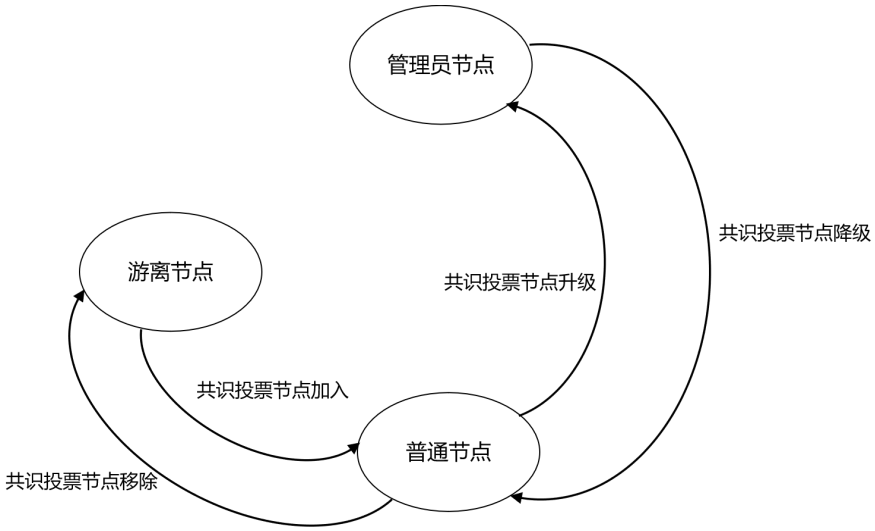
personal.newAccount()

1.5 节点

节点是区块链网络的构成元素，每一个节点计算机上运行着 SimpleChain 的节点软件——sipe 进程。

节点分类

从权限管理的角度，SimpleChain 联盟链分为三种节点类型：管理员节点、普通节点、游离节点，节点之间的角色转换参见《SimpleChain 联盟链（基础版）用户手册》。



还可以将节点分类为共识节点和非共识节点。共识节点参与共识协议、生成区块；非共识节点只能同步数据。

2 SimpleChain 联盟链的开发

SimpleChain 联盟链（基础版）提供两种方式的开发，一是用户编写智能合约，二是直接调用数据上链接口。

2.1 智能合约

智能合约是在 SimpleChain 联盟链上运行的可执行程序。SimpleChain 联盟链（基础版）的智能合约采用 Solidity 语言，是目前世界上最流行的智能合约开发语言，类似 JavaScript 的语法。

Solidity 语法文档请参照：https://solidity-cn.readthedocs.io/zh/develop/

2.1.1 智能合约的开发和部署

SimpleChain 联盟链（基础版）没提供智能合约开发的 IDE 环境，用户需要使用其他工具进行开发和调试，之后通过 SimpleChain 联盟链（基础版）的管理平台上传合约文件（.sol），管理平台会对上传的智能合约进行自动化编译和部署。

SimpleChain 联盟链（基础版）要求用户使用的 solidity 版本为 0.6.10 及以上。

2.2 数据上链接口

数据上链接口可以快速在链上进行数据的存证，与智能合约不同，智能合约的数据是保存在合约专属的状态（State）数据存储空间；数据上链接口将待存证的数据保存在每笔交易的数据字段中，速度快，而且方便使用管理平台的区块浏览器查看数据。

2.2.1 接口规范

Path：/v1/internal/upchain
Method: HTTP POST
接口描述：数据上链接口

请求参数：
Headers

参数名称	参数值	是否必须	实例	备注
Content-Type	application/json	是		

Body

名称	类型	是否必须	默认值	备注	其他信息

value	String	是		需要上链的数据	

返回数据

名称	类型	是否必须	默认值	备注	其他信息
tx	String	是		上链后的交易哈希	