第六届全国大学生能源经济学术创意大赛参赛作品

江 蘇 大 學

作品名称：区块链技术下的碳排放权交易的仿真研究

（研究论文类）

指导老师：

指导老师姓名	**工作单位**
卢娜	江苏大学财经学院

作者团队：

成员姓名	**学校**	**年级**
向致承	江苏大学	2018 级
张兆辉	江苏大学	2018 级
李伟	江苏大学	2018 级
汤培辰	江苏大学	2018 级

区块链技术下的碳排放权交易的仿真研究

指导老师：卢娜

摘要： 碳排放权交易是解决全球气候变化的重要途经，区块链技术具有去中心化、透明安全的特点，为碳排放权交易提供了重要的发展思路，本文通过使用 python 对区块链用于碳排放权交易进行仿真研究，首先从宏观角度设计交易框架，包括密码学原理、账户模型、交易流程、共识机制四个方面，然后建立区用 python 仿真实现整个框架，使用森林着火模型模拟区块链技术下的碳排放权交易对碳减排的作用。得出结论：（1）基于区块链的碳交易可以促进企业发展控排技术，进而减少企业碳排放。（2）区块链的完全透明性可以有效帮助监管部门监督碳市场，也帮助维护了市场秩序。（3）智能合约的调用具有强制性，开始调用之后就不可更改，因此有时人为的错误调用难以更改，这造成了一部分废单。（4）碳交易还处于初级发展阶段，区块链技术的使用还需要很多技术上的完善。

关键词：碳排放权交易，森林着火模型，仿真研究

1　文献综述

1.1　研究背景及意义

1.1.1　研究背景

随着经济的快速发展，我国的温室气体排放量也急剧增加，从 1980 年的少于 15 亿公吨到 2017 年超过 100 亿公吨。为了应对与日俱增的减排压力，加快向绿色和低碳经济转型的步伐，实现可持续发展，我国政府制定了一系列碳约束目标。在此背景下，我国的碳交易市场也逐步开始建设起来。

近年来，我国的碳市场建设经历了迅速的发展过程。2010 年 10 月，国务院发布的《关于加快培育和发展战略性新兴产业的决定》中首次提出，要建立和完善主要污染物和碳排放交易制度。随后，国家发展改革委陆续批准北京、上海、天津、重庆、湖北、广东和深圳等七省市开展碳交易试点工作。2012 年 6 月国家发展改革委印发《温室气体自愿减排交易管理暂行办法》，同年 10 月印发《温室气体自愿减排项目审定与核证指南》，两个规范性文件为国家核证自愿减排量（CCER）交易市场搭建起了整体框架，对 CCER 项目减排量从产生到交易的全过程进行了系统规范。2014 年 12 月国家发改委颁布了《碳排放权交易管理暂行办法》，明确了全国统一碳排放交易市场的基本框架。2016 年 1 月 11 日，国家发展改革委办公厅发布了《关于切实做好全国碳排放权交易市场启动重点工作的通知》，旨在协同推进全国碳排放权交易市场建设，确保 2017 年启动全国碳排放权交易，实施碳排放权交易制度。2017 年 12 月 18 日，国家发展改革委印发的《全国碳排放权交易市场建设方案(发电行业)》的通知，全国统一的碳交易市场正式启动。

1.1.2　研究意义

温室气体排放增加，全球气温升高，冰川融化、海平面升高，这种现象若是不加以遏制，多年以后地球上大部分陆地也将变成汪洋大海。但是按照目前全球碳排放水平的测算，必须将排放到大气中的二氧化碳控制在 3.2×10^{12}t 以内，实现哥本哈根协议中关于将全球气温升高控制在 2℃的要求，而目前留给我们的额度只剩下 1.2×10^{12}t。而碳排放权交易是目前相对而言能有效降低企业碳排放的措施之一，相比于传统碳市场交易方式，区块链技术下的碳市场具有以下几大优势[1]：

（1）没有中心化机构，不需要第三方机构监督管控，也不需要缴纳手续费，可以大幅度降低管理成本。

（2）整个系统信息公开透明，区块链数据对所有人开放，有利于未进入市场的企业充分了解市场概况，从而降低信息获取成本。

（3）所有节点可在系统内自由、安全地认证，可以降低目前碳市场配额认证成本。

（4）只要没有掌控 51%以上的数据节点，数据就无法被篡改，安全性极高。

（5）对于碳排放量未达标的企业，智能合约可以自动进行罚款，不存在讲人情的情况，有效提升政策执行力[2]。

1.2 国内外碳市场发展现状

目前，国内碳市场的运行机制分为两种。一种是基于配额的交易，即通过第三方机构发放配额，若各个碳排放企业或组织超过或者未达到既定的碳排放标准，可以通过现有的碳交易所进行碳排放权交易，并且对未达标的企业由有关机构对它进行认证和惩罚。另一种是基于项目的交易，即企业之间通过进行有关碳排放项目的合作，买方向卖方提供资金，从而获取温室气体减排额度的方法。

国内碳市场自从 2013 年到 2015 年的碳排放权交易试点以来，我国的碳市场建设正在稳步推进，到目前，已经取得了长足的发展。2018 年国内碳排放总量突破 100 亿，碳市场累计交易近 8 亿吨。2019 年中国碳排放总量接近 105 亿，占全球碳排放总量的 27.2%[3]。中国已经成为世界上碳排放量最大的国家，同时也是减排潜力最大的国家。

截至 2017 年 4 月，中国、欧盟和美国已经是全球温室气体排放量最大的三个国家或组织，其温室气体排放量占全球排放总量的一半以上，而更夸张的是，碳排放量排名前十名的国家或组织加起来大约占全球碳排放总量的 3/4[4]，因此，与其说是全球的碳减排行动，不如说是这些国家或组织的减排行动，只有当这些国家或组织起到了引领和模范作用，其他的国家将会纷纷效仿，全球碳减排以及碳市场才能得到有效的发展。

2 交易框架设计

2.1 密码学原理

2.1.1 哈希

延用传统区块链项目中运用到的哈希函数 SHA-256[5],主要运用其碰撞抵抗性、单向藏匿性、难题友好性三个性质，因为这个函数的输出空间足够大，所以即便有一个很好的随机源不断产生输入，也无法用高效的方法在改变输入的情况下维持输出不变，即难以产生碰撞。需要注意的是，即使这个碰撞抵抗性在实际运用中很好的保证了区块链运行的安全，但在理论上仍然无法证明，即便是已经人为

破解的 MD5，想要产生碰撞，实验环境依然很严苛。碰撞抵抗性结合单向藏匿性就可以用于数字承诺，给予承诺是一个很复杂的过程，类比预言术:若直接预言明天股票涨停或者跌停且广而告之，可能触发羊群效应，被其他人做多或者做空。若不将消息透露，则无人见证消息是否可信。而倘若将预言信息通过哈希运算得到的值传播出去，其他人无法直接算出预测信息，只有等到开盘当天将预测信息透露，则用户可以轻松鉴定预言是否正确。最后的难题友好性运用于挖矿中，在后文共识机制的选择上会详细叙述。

2.1.2 签名

因为对称加密存在对安全网络环境的高度依赖，非对称加密应运而生，消息发送方接收方用不同的密钥进行加密解密，给其他节点发送消息时需要用对方的公钥加密，对方接受消息用私钥进行解密，发起交易时用自己的私钥签名[6]，同时广播自己的公钥，网络中的其他节点监听到交易信息后用交易发起者的公钥验证签名。

2.2 账户

先由计算机随机产生公私钥，再由公钥哈希值的前 8 位(16 进制)加上身份信息得来账户，在整个碳排放权交易市场中，政府和企业等主体都需要创建账户，所以身份信息包含两部分，第一部分判断账户类型，第二部分为身份码，即政府或企业在该类节点中具体排上的编码，最后一部分是结束标识符以及账户内信息经过 json 序列化之后取哈希值。具体结构如图 1。

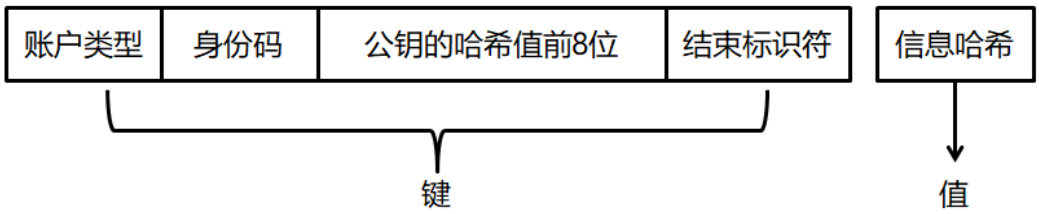

图 1

2.2.1 外部账户

政府和企业一开始创建的都是外部账户，创建的时候都需要进行认证，之后才可以获得使用和交易碳配额的权利，外部账户的账户内记录有账户余额，为了防止恶意节点对同一笔交易执行多次以额外获取未经对方许可的交易的费用，还需记录交易次数，这样通过查看账户就可以得知交易是该账户的第几笔交易，从而抵抗上述攻击，外部账户可以调用合约账户中的智能合约进行配额交易，也可以创建新的合约[7]。

2.2.2 合约账户

合约账户中记录的信息除了上述账户余额以及交易次数计数器，还有智能合约的代码，代码具有强制性，并不“智能”，准确来讲是“自动”。

2.2.3 存储和维护

账户的存储使用状态树，数据结构为默克尔前缀树(MPT)[8]，即把所有的账户状态排列起来组成字典树，再进行路径压缩成前缀树，每一次压缩都会形成共享前缀，同时产生叶子节点用于存储下属节点的哈希值。具体结构如图 2

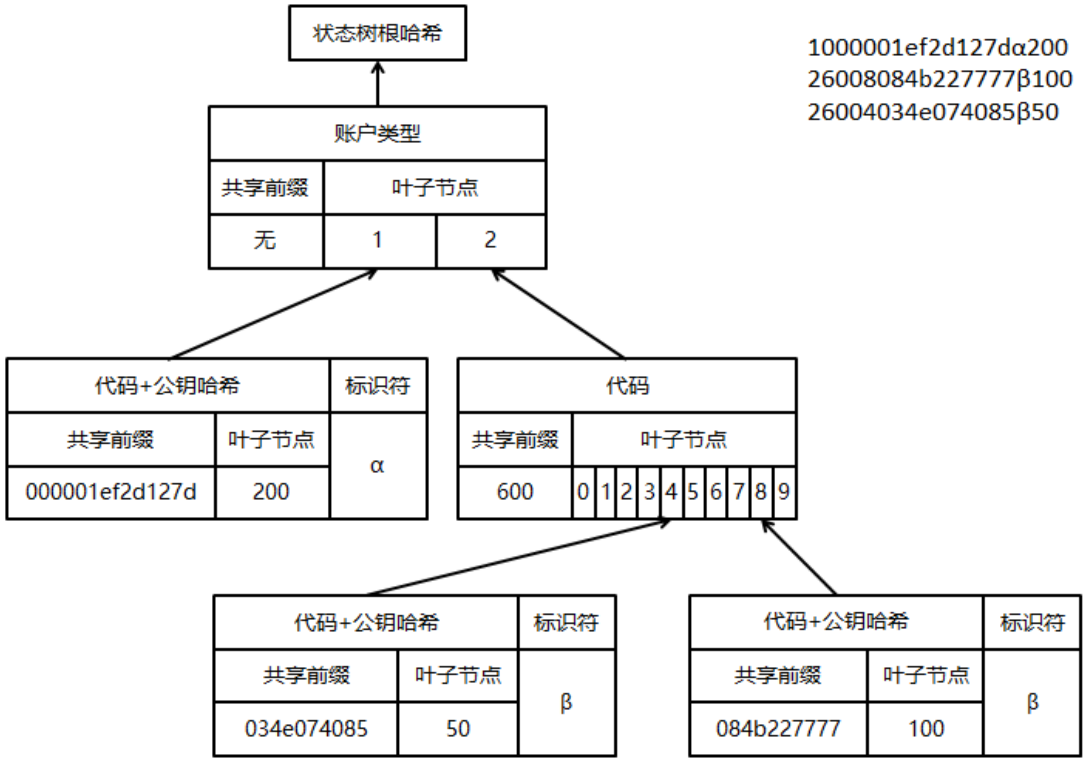

图 2

图 2 绘出 3 个账户组装为状态树作为简化的例子，此例包括 1 和 2 开头的两类账户，以及对应的 6 位身份码，公钥哈希前 8 位，结束标识符，账户状态用纯数字代替，每一次路径压缩产生的共享前缀就是有序叶子节点的开头公共部分，此例中后两个账户的代码公共部分是 600，其中每一个叶子节点处存储的都是后续节点的哈希值，结束标识符用于标识该节点的叶子节点处存储的哈希值是该账户的账户余额等信息 json 序列化之后取得的哈希值，哈希值一级一级传导计算，最终计算出一个根哈希值存储在区块中。

根哈希随着区块链的延续而更新，因为每一次更新并不是全部账户都需要更新，所以不变的账户就可以存储之前计算的哈希，即用哈希指针指向不变的账户状态，而变化的账户则继续路径压缩，在最低叶子节点处存储改动的新值。具体如图 3。

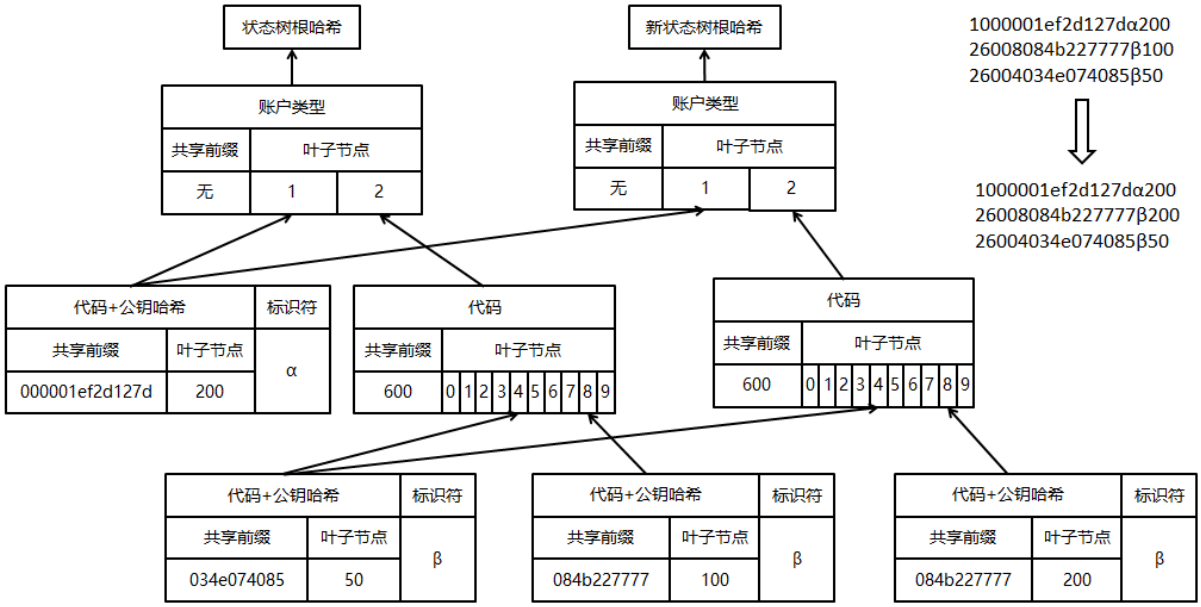

图 3

图 3 将图 2 中的例子做了改动，模拟账户的维护，可以看出本例只有 2600808 开头的账户状态值从 100 变为 200，因此其他账户不需要改动，改动的账户再经过一次次路径压缩后将新值 200 存储在叶子节点处替代原来的值，这样最终计算出来一个新状态树的哈希值放在发布的新区块中更新旧的账户状态。

2.3 交易流程

2.3.1 碳排放权交易

同股票和债券市场，我国的碳市场亦分为一级市场和二级市场[9]。其中，一级市场是发行市场，二级市场是交易市场。一级市场创造碳排放权配额和项目减排量两类基础碳资产，二级市场进行减排单位间的现货交易，交易产品包括排放权配额和经审定的项目减排量。目前，我国的碳交易市场仍以二级市场为主。具体的碳交易运行机制如图 4：

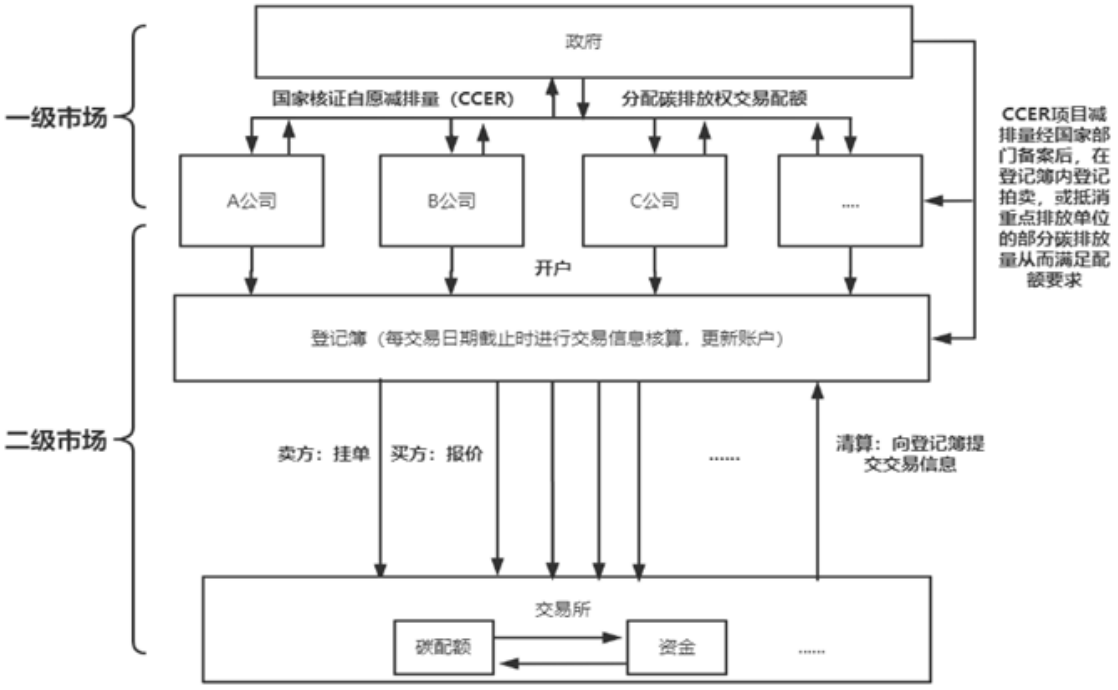

图 4

首先由政府免费向各减排单位分配碳排放权交易配额，减排单位可以根据自身实际的排放情况选择在交易所进行交易或参与国家核证自愿减排项目（CCER）。在交易所进行配额交易的单位应先在指定地区登记簿进行开户登记，达到指定要求即可开户交易。各单位间的配额交易需在交易日内将产品和价格由登记簿上传到交易所，在交易所内完成价值转移，在交易日截止时再由交易所将相关资金产品信息反馈给登记簿，由登记簿进行信息核查，完成账户更新。除此之外，减排单位通过 CCER 项目完成的减排量经过政府部门备案后，可在登记簿内登记拍卖，也可用于抵消 CCER 项目中某些重点排放单位部分已经确认的碳排放量，从而满足配额要求。

2.3.2 基于区块链的碳排放交易流程设计

基于区块链的碳排放交易的流程类比普通碳排放交易，首先是政府以及企业等所有节点在本地生成账户，然后广播自己的账户，政府节点监听到其他节点的账户之后检验并对企业节点进行认证，将合法节点加入本地保存的局域网内并对这个企业碳排放能力进行评估，然后核证自愿减排量，分配碳排放权交易配额，之后创建祖先区块记录已知账户组成的状态树的根哈希值，接下来就是企业之间

自由交易，争夺记账权。具体流程如图 5 所示。

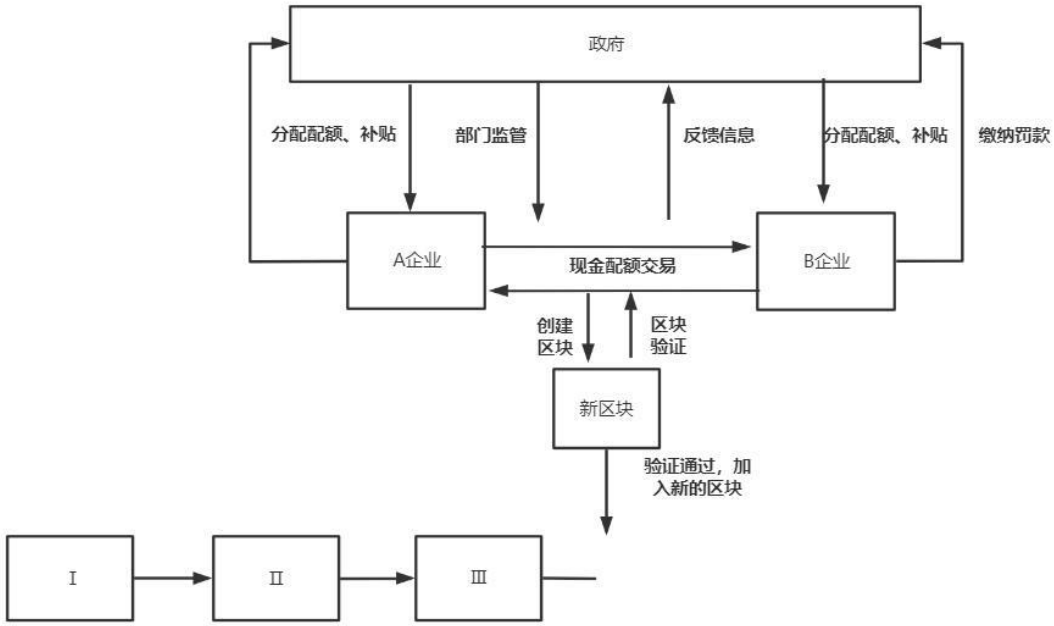

图 5

每一笔交易内的主要内容如图 6 所示。

参数	介绍
sender	交易发起方的账户
public_key	交易发起者的公钥
digisig	发起者的签名
receiver	接收方的账户
nonce	交易编号
data	调用的合约账户
value	交易需要花费的代币

图 6

2.4 公共账本

在一个分布式系统中，想要对于某一个公有的东西进行改变同时维护一致性，就需要一个完善的共识机制，在碳排放权区块链交易系统中，区块链作为公共账本来纪律碳排放权交易中的每一笔交易，每一个账户的状态等，每一次需要延续区块链时既需要记录交易，又需要更新账户状态树，共识机制的选择决定了系统的去中心化程度、安全性以及可扩展性[10]，此处参考比特币的工作量证明，沿用以来算力的难题友好型算法，调节随机数来计算哈希值，直到满足难度要求。

3 仿真与分析

3.1 初始设定

3.1.1 核心模块

核心模块及对应作用如图 7

模块	作用
account	定义账户类
block	定义普通块类以及祖先块
chain	定义链类
config	配置参数
digisign	产生签名
Minter	定义矿工类
route	调用端口
transaction	定义交易类
server	管理模拟的模型
agent	定义每一个模型中单元
model	定义模型

图 7

3.1.2 核心方法

核心方法及对应作用如图 8

方法	作用
compute_total_fee()	计算总的交易费
to_dict()	将块或交易信息以字典类型返回
verify_block()	检查块是否合法
register_node()	注册认证节账户
broadcast_transaction()	广播交易信息
broadcast_block()	广播区块信息
verify_chain()	检查链是否异常
resolve_conflicts()	选出最长合法链
verify_transaction()	检查交易是否合法
compute_balance()	计算账户余额
verify_signature()	检查签名是否合法

图 8

3.1.3 初始参数

设置 1 个政府节点，5 个企业节点，其中 1 个为重点企业，无控排情况下需要配额 100 个单位，其他 4 个企业节点需要配额 50，政府按照各企业无控排情况下的 80%发放免费配额，重点企业资金为 60 万，普通企业资金 30 万，在大力发

展控排技术之后重点企业可以将排放减少 10%，其他企业可以减少 5%，配额价格初始设为 3 万元每单位，企业节点之间交易期望价设为价格乘相应倍数，倍数在[0.75,1.25]之间取随机数，最终成交价为二者的均价，挖矿难度设为 16 进制数 $1*10^{57}$。

3.2 仿真程序运行流程

单个节点首先通过 config 模块配置初始参数，然后通过 account 模块以及 digisign 模块生成账户及对应签名，调用 webapp 占用端口，向外广播账户，并向政府节点取得认证及分配的配额，政府节点创造链上第一个区块，之后进行自由交易，监听到交易并验证后加入交易池中等待打包，监听到区块并验证后加入区块链链中，想要发布一个交易就调用 broadcast_transaction 广播交易等待其他节点验证并打包，发布区块同理，最后验证整个一条链是否合法，通过 chain 端口可以查看整条区块链。如图 9 所示。

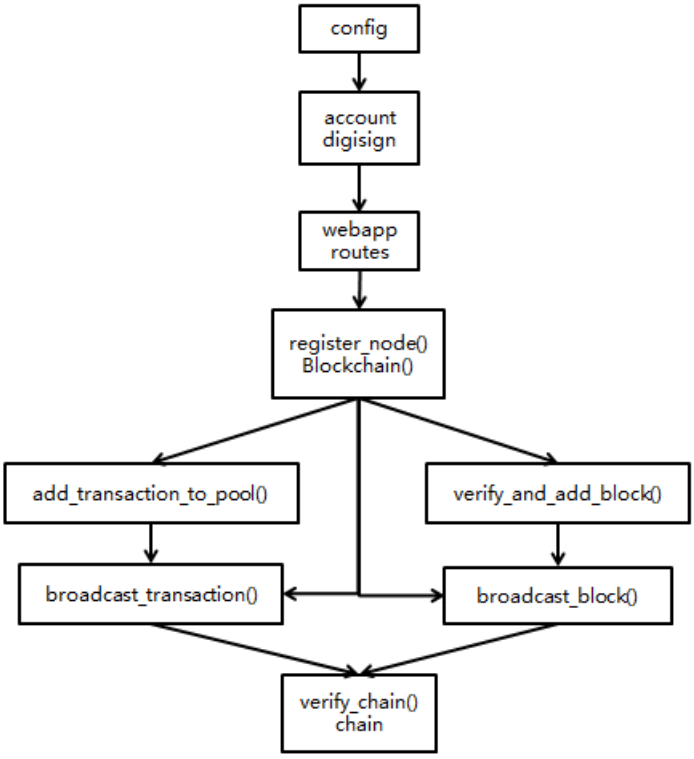

图 9

不同节点之间交互流程为：政府节点认证并广播企业节点的信息，企业节点之间交互价格进行交易，具体流程如图 10。

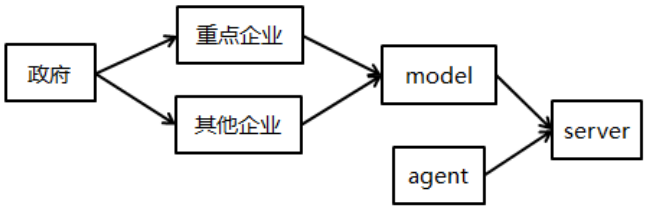

图 10

3.3 仿真结果分析

仿真模型的原型参考森林火灾模型[11]，将一些参数做了改动，模拟分布式网络，将原本的企业节点数放大为 45 个，初始状态如图 11，棕色节点为普通碳交易的节点，黄色节点为刚开始引入区块链的碳交易节点。运行一段时间之后如图 12，绿色节点为引入区块链的碳交易节点。两种节点的比例以及交易次数如图 13，可以看出一开始引入区块链的交易占比例并不大，慢慢的开始占大比例，并且碳交易量越来越小，可以看出基于区块链的碳排放交易可以促进企业发展控排技术，减少碳排放。

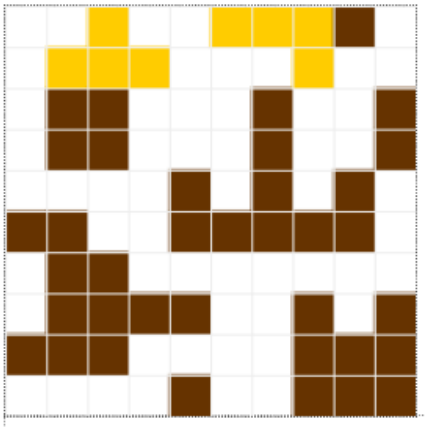

图 11

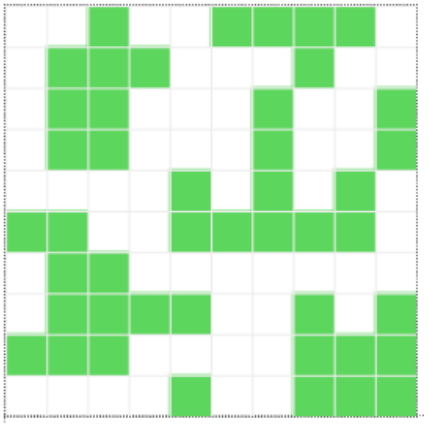

图 12

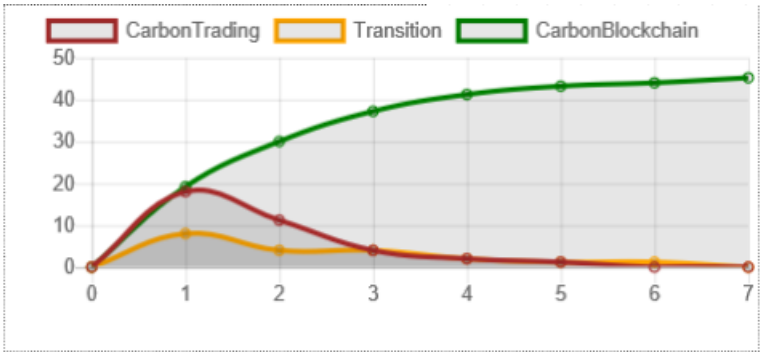

图 13

4 结论与建议

本文在设计出区块链用于碳交易的框架的基础上，应用 python 模拟森林火灾模型实现节点之间配额交易。研究结论如下：

(1) 基于区块链的碳交易可以促进企业发展控排技术，进而减少企业碳排放。

(2) 区块链的完全透明性可以有效帮助监管部门监督碳市场，也帮助维护了市场秩序。

(3) 智能合约的调用具有强制性，开始调用之后就不可更改，因此有时人为的错误调用难以更改，这造成了一部分废单。

(4) 碳交易还处于初级发展阶段，区块链技术的使用还需要很多技术上的完善，比如碳市场的初衷是碳减排，而传统的比特币挖矿会产生很多碳排放。

以上研究结论得出的政策建议如下：

(1) 由于区块链技术用途很广泛，科技政策的重心应该进一步聚焦于碳交易上，应该继续加入研发投入。

(2) 在应用区块链技术时，要考虑使用技术本身带来的能耗问题，要推动绿色低能耗的解决方案的发展。

(3) 政府充分发挥监管和调控作用，进一步完善和统一碳市场，促进区块链用于碳交易的健康可持续发展。

(4) 为了了解实际的区块链碳市场交易可行性，政府可借鉴碳交易试点经验，通过开放部分区块链碳交易试点，对实际运行中的问题进行查缺补漏，再进一步扩大试点范围，推进全国统一的区块链碳市场化发展。

参考文献

[1] 张琪.基于区块链的碳排放交易仿真研究[D].中国石油大学(北京),2018.

[2] 吴银海,黄妍,秦浩,鲍士婷.区块链技术在碳交易市场中的应用设想[J].全国流通经济,2019(06):99-100.

[3] 白雪楠,白昕,尤慧君.中国碳交易市场发展现状及问题分析[J].中外企业家,2020(14):100.

[4] 武旻华.全球碳交易市场环境下我国碳交易市场发展研究[D].青岛大学,2011.

[5] Alka Leekha,Alam Shaikh. Implementation and comparison of the functions of building blocks in SHA-2 family used in secured cloud applications[J]. Journal of Discrete Mathematical Sciences and Cryptography,2019,22(2).

[6] Electronic Signature and Records Association; New Members Join Electronic Signature and Records Association[J]. Computers, Networks & Communications,2016.

[7] 曹迪迪,陈伟.基于智能合约的以太坊可信存证机制[J].计算机应用,2019,39(04):1073-1080.

[8] Niloufar Shafiei. Non-blocking Patricia tries with replace operations[J]. Distributed Computing,2019,32(5).

[9] Wei Zhang,Jing Li,Guoxiang Li,Shucen Guo. Emission reduction effect and carbon market efficiency of carbon emissions trading policy in China[J]. Energy,2020,196.

[10]方响,马笛,侯伟宏,孙智卿,杨翾,刘剑.分布式新能源接入下的区块链共识机制研究[J].浙江电力,2019,38(07):1-6.

[11]唐勇,张晓碧,刘浩阳,郭慧玲.林火蔓延模型的改进及可视化验证[J].小型微型计算机系统,2020,41(04):893-896.