# 区块链供应链（卖鞋）

# 目录

[1 目录 1](#_Toc58969654)

[1. 区块链较传统互联网的优势 2](#_Toc58969655)

[2 区块链的五大特性 5](#_Toc58969658)

[3 当今市场环境 7](#_Toc58969667)

[4 真假区别 10](#_Toc58969673)

[5 市场份额 13](#_Toc58969673)

[6 区块链加卖鞋 15](#_Toc58969673)

[7 ERC721代币 15](#_Toc58969673)

[8 ERC721代币挂钩正品鞋 20](#_Toc58969673)

[9 区块链优势 22](#_Toc58969673)

[10 杜绝旧鞋翻新卖出 23](#_Toc58969673)

[11 交易流程 24](#_Toc58969673)

[12 钱款去向 26](#_Toc58969673)

[13 账户权限 28](#_Toc58969673)

[14 测试平台 31](#_Toc58969673)

[15 重要代码介绍 32](#_Toc58969673)

[16 实机演示 36](#_Toc58969673)

[17 前端代码演示 38](#_Toc58969673)

## 区块链较传统互联网的优势

当前，全球新一轮科技革命和产业变革持续深入，国际产业格局加速重塑，创新成为引领发展的第一动力。在这一轮变革中，信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最大的领域，是全球技术创新的竞争高地，是引领新一轮变革的主导力量。

区块链作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用，被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。区块链技术起源于化名为＂中本聪＂（Satoshi Nakamoto）的学者在2008年发表的奠基性论文《比特币一种点对点电子现金系统》。狭义来讲，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

目前，区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时，就像云计算、大数据、物联网等新一代信息技术一样，区块链技术并不是单一信息技术，而是依托于现有技术，加以独创性的组合及创新从而实现以前未实现的功能。

尽管区块链技术还存在可扩展性、隐私和安全、开源项目不够成熟等问题，但是已有的应用充分证明了区块链的价值。未来一段时间内，随着区块链技术不断成熟，其应用将带来以下几个方面的价值：

一是推动新一代信息技术产业的发展。随着区块链技术应用的不断深入，将为云计算、大数据、物联网、人工智能等新一代信息技术的发展创造新的机遇。例如，随着万向、微众等重点企业不断推动Baas平台的深入应用,必将带动云计算和大数据的发展。这样的机遇将有利于信息技术的升级换代，也将有助于推动信息产业的跨越式发展。

二是为经济社会转型升级提供技术支撑。随着区块链技术广泛应用于金融服务、供应链管理、文化娱乐、智能制造、社会公益以及教育就业等经济社会各领域，必将优化行业的业务流程、降低运营成本、提升协同效率，进而为经济社会转型升级提供系统化的支撑。例如，随着区块链技术在版权交易和保护方面应用的不断成熟，将对文化娱乐行业的转型发展起到积极的推动作用。

三是培育新的创业创新机会。国内外已有的应用实践证明，区块链技术作为一种大规模协作的工具，能推动不同经济体内交易的广度和深度迈上一个新的台阶，并能有效降低交易成本。例如，万向将结合＂创新聚能城＂建设，构建区块链的创业创新平台，既为个人和中小企业创业创新提供平台支撑，因为将来应用区块链技术奠定了基础。可以预见的未来是:随着区块链技术的广泛运用，新的商业模式会大量涌现，为创业创新创造新的机遇。

四是为社会管理和治理水平的提升提供技术手段。随着区块链技术在公共管理、社会保障、知识产权管理和保护、土地所有权管理等领域的应用不断成熟和深入，将有效提升公众参与度，降低社会运营成本，提高社会管理的质量和效率，社会管理和治理水平的提升具有重要的促进作用。例如，蚂蚁金服将区块链应用于公益捐款，为全社会提升公益活动的透明度和信任度树立了榜样，也为区块链技术用于提升社会管理和治理水平提供了实践参考。

随着新一轮产业革命的到来，云计算、大数据、物联网等新一代信息技术在智能制造、金融、能源、医疗健康等行业中的作用愈发重要。自＂十二五＂被确立为七大战略性新兴产业之一以来，我国新一代信息技术的发展迅速，逐步成为各行各业深化信息技术应用的方向。从国内外发展趋势和区块链技术发展演进路径来看，区块链技术和应用发展需要云计算、大数据、物联网等新一代信息技术作为基础支撑，同时区块链技术和应用发展对推动新一代信息技术产业发展具有重要的促进作用。

## 区块链的五大特性

当然区块链与传统互联网相比有着许多不同的特性，区块链是分布式数据存储，点对点传输，共识机制，加密算法等计算机技术在互联网时代的创新应用模式。虽然不同报告中对区块链的介绍措辞不尽相同，但“去中心化、开放性、自治性、信息不可篡改和匿名性”这五个基本特征得到了共识性。

一、去中心化，就是所有在整个区块链网络里面跑的节点，都可以进行记账，都有一个记账权，这个就完全规避了操作中心化的一个弊端。它不是一个中心化，它是一个去中介化。中心化就是，比如说现在40%的比特币掌握在美国人手里，（很有可能掌握在美国政府，当然了这只是一个猜测）它可以嫁接一个白手套来搅动整个市场。这个实际上还是有一个中心化运作体系的；以太坊大量持有在犹太人手里；EOS集中在21个超级节点那。他们只能叫做弱中心化；

二，开放性，这是针对区块链共有链来讲的，因为共有链的信息任何人都可以进去读可以进去写，只要是它整个网络体系的节点，有记账权的节点，都可以进行；

三、防篡改性，就是任何人要改变区块链里面的信息，必须要攻击网络里面的51%的节点才能把数据更改掉，这个难度非常非常大；

四、匿名性，它的匿名性基于它的算法实现了是以地址来寻址的 ，而不是以个人身份，这也是政府比较担心的。整个区块链里面有两个不可控，第一个是身份不可控匿名性，不知道是谁发起了这笔交易；第二个是它有一个跨境支付，这个牵扯到币的资金转移这一块；

五、可追溯性，他的机制就是设定后面一个区块拥有前面一个区块的一个哈希值就像一个挂钩一样，只有识别了前面的哈希值才能挂得上去，是一整条完整的链。可追溯性还有一个好的的特点就是便于数据的查询，因为这个区块是有唯一标识的，比如说之前往数据库里面去查询一个东西的话，是有很多算法去分块来找的，而这个区块链网络里面是以时间节点来定义找这个时间段的这个区块再去寻址，这就更方便。

在这五个特性中，最为重要也是区块链最具价值的就是可溯源性和防篡改，在区块链未应用之前，网络环境是非常不透明的，所有的数据都储存在一个中心服务器上，被掌控在少数人手中，用户们可查看的内容和控制的功能少之胜少，直到区块链的出现，区块链可溯源性和防篡改的特性使得网络环境变得更加公开和透明。

## 当今市场环境

2007年，美国警方在纽约查封了30多万双假耐克，涉案总值超过3100万美元。这些来自中国的假鞋惊呆了美国人，为此《纽约时报》的记者还专程跑到中国做调查采访。自此，福建莆田假鞋之名走出了国门，传遍了世界。虽然，我们常常把“莆田”和无良医院认知挂钩。但在福建莆田，造鞋才是当地的支柱产业。“让中国都穿得起名牌鞋”！这是“莆田鞋”广为人知的一句玩笑话，但这又何尝不是一种讽刺呢？

有媒体曾报道：国内市场上10双假鞋里，有9双从莆田发货。全球每3双耐克鞋中，便有一双是来自莆田的仿品。2017年年初，有媒体曝光了莆田一家假鞋门店，老板的电话和微信被无意中曝光。没想到他完全有恃无恐，甚至把这次曝光当成了免费宣传。“我莆田有10家店，曝光一个正常”。店主老板表示，店铺的销量一直很好，通过此次曝光，越来越多的人加他微信询价购鞋。“比如一双鞋子淘宝卖5000块，我去卖500块，马云还不马上给我封店啊，微信就挺好”。在老板眼里，封店是件小事，价格高昂的正品不如“高仿鞋”好买。微商大行其道后，让“莆田鞋”有了新的销售渠道，在淘宝上不好卖出的高价，可以通过一层层的朋友圈分销卖给消费者。

莆田鞋为什么生命力如此顽强？

除了多年的行业沉淀外，从产品到推广渠道莆田鞋业为了造假可谓花样百出。

网上有一个流传很广的视频：拿着莆田NB与正品NB进行正规质量检测，经过了耐磨测试、抗弯折测试和剥离测试后，真鞋和假鞋质量区别不大。“我妈花几千块买了一双真耐克，后来发现朋友圈的耐克只要几百。妈妈转头就把假鞋退回了专卖店，还没被专卖店发现。”这是网上流传的段子，似乎有的消费者对于便宜的假货并不反感。但并不是所有人都不反感假鞋，也不是所有人都能分辨假鞋。早时候，有很多人会把买回来的鞋放到虎扑上，求鉴定真假。最开始，莆田鞋在虎扑大神们的面前无从遁形。后来，莆田鞋竟然把虎扑大神们的鉴定意见慢慢接受了。根据专业意见，逐渐改良制鞋工艺。早在上世纪80年代，莆田与台湾隔海相望，因此吸引了大批台商来莆田创办制鞋厂。这些鞋厂最早为世界大品牌代工，鞋业逐渐成为莆田的支柱产业，甚至接近当地GDP的一半。随着订单越来越大，总会有滞销的鞋滞留在当地，这些鞋被当地人转卖，由于人工和土地成本低廉，当地人获利颇丰。越来越多的人发现了“卖鞋”有利可图，代工厂的工人开始往外偷图纸。从“假鞋”小作坊做到了大工厂，莆田慢慢变成“假鞋之都”。莆田鞋是随着电商平台一起崛起的。曾有媒体报道，有的人靠莆田鞋在“双11”一天赚了400多万。一双假的“耐克”成本不到100块，去除渠道费用，流入到消费者手里也远远低于正品售价。有关部门虽然多年打击“莆田假鞋”，但难从根本上遏制。

除去那些没什么钱想买假鞋装逼的人以外，人们拿着几千甚至上万的钱结果买到手的只是在莆田成本只有几十块钱的假鞋，不知道还好，知道的话不会直接吐血？特别是当代大学生，有句话说的特别好，“在球场上对人打击最大不是把别人打爆了，而是对人说你的Nike是假的。”如果还能拿得出证据那就真的是社会性死亡。

由此可见，现在的品牌鞋市场的混乱程度,全球限量100双，国内有10000双，莆田有9000双，甚至有的假鞋打出了“比真鞋质量还好，保证检验不出”的广告牌，进过了十几年的发展，假鞋市场已经与真鞋市场融为一体了。

就拿我身边的例子来说，我曾有幸去过莆田的鞋市，各种在外面市场上动则几百上千的球鞋、跑鞋、休闲鞋，在莆田的地摊市场上被随意摆放在一张简陋的垫子上，就跟夜市叫卖的人一样，外面买不起的鞋，这里只要百来块钱就能拿下，当然这种都是小工坊生产的鞋，与莆田的“高档鞋”的质量完全没办法比的，随着深入市场，进入了一家看似还不错的店面，当然的我是有人带的，这店面里才是最正宗，质量最好，最有代表性的“莆田鞋”，价格会比外面的鞋贵上许多，但正如他打出的广告一样，专家都难分辨的外观，比真鞋还好的质量，经过交谈得知，现在大多数的官方授权的工厂都在东南亚那边，论质量肯定没有“鞋都”——莆田做的好，国内许多实体店，授权点，甚至官方的店铺都会在他家拿鞋。在国内正规商场或者旗舰店买的鞋都有很大机率是莆田生产的。

## 真假区别

说说这两者的区别吧：

1、材料上的区别

首先不同质量等级的莆田鞋，用的材料也不同。比正品好的，有！正品用二层皮，莆田鞋用头层皮。莆田鞋比正品用料差的也多了去，正品用真皮，莆田直接用了仿皮。有的连皮都不是，直接用皮革，但是价格非常便宜。但是超好的用料跟正品是一模一样的。材料有好有坏，价格肯定也不一样的，莆田鞋更能体现一分钱一分货。但是千万别遇到那些忽悠，在这么多年做[鞋子](https://www.zzx8.com/xielei/)过程中，接触过各种人物，赚本份的，一双就赚20辛苦钱的很多。一双加价200或300的也大有人在。

总的来说：材料和正品比，无论鞋底，还是鞋面的用料，都有好有坏，有和正品一样的，你买要讲运气。

2、做工的精细

制造一双好鞋的关键工艺在于成型车间。成型车间就是把鞋面和鞋底组合起来的车间，一条长60米以上的普通流水线，就需要60多个工人。

普通莆田鞋工厂流水线和大的鞋厂的流水线是有区别的，莆田鞋好多小厂只有半条流水线。生产工艺虽然完全一样，但是缺乏严格的管理制度和品控。但是大的莆田鞋厂是具备这些条件的，他们生产鞋子的工艺跟正品是没有差别的。所以大厂生产的莆田鞋往往差在做工上，材料跟正品差别并不大。其实这些大厂很多都是正品的代工厂出生。

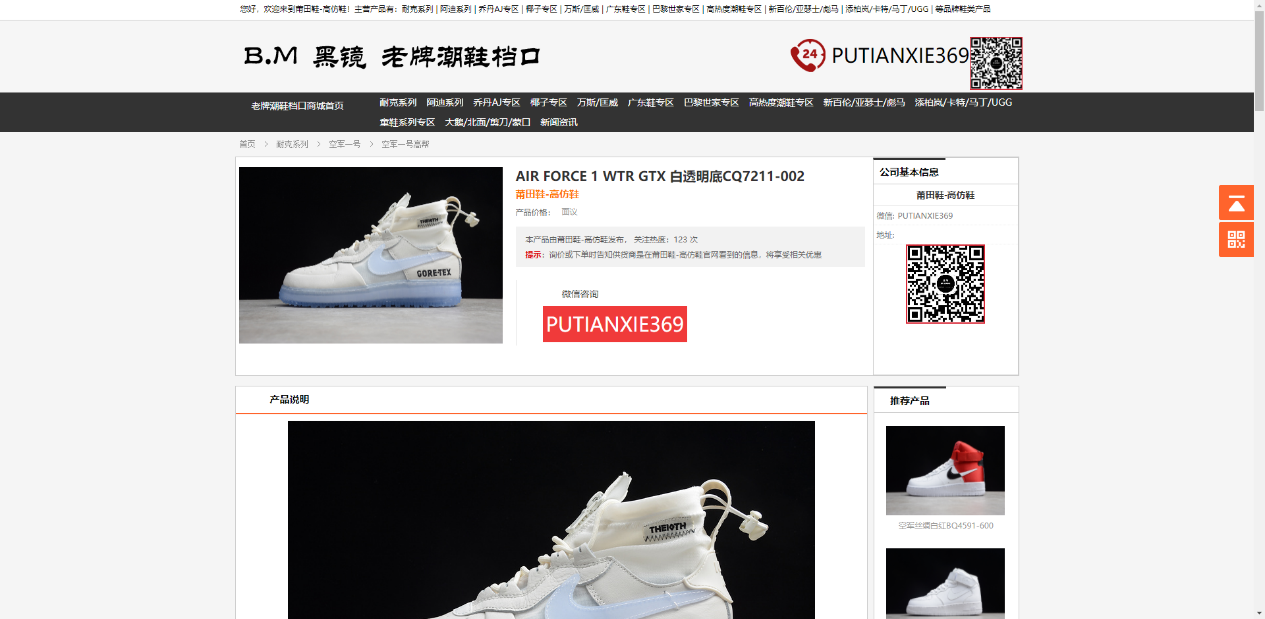
总之，不同等级的工厂生产的莆田鞋造就了不同品质的莆田鞋，正因为如此，才有了所谓的真标，公司级，纯原的分类。

我的建议，对于用于专业运动的，还是老实去买正品专业运动装备，哪怕是买国产[品牌](https://www.zzx8.com/bidu/637.html)的也行。经常会有人找我帮他们买乔丹篮球鞋，我都是建议他们：要用来打球的话就算了，这边的工艺真的没有想象中的那么强大，正品篮球鞋的鞋底要经过照射车间，流水线比普通的[运动鞋](https://www.zzx8.com/xielei/yundongxie/)流水线还要长。在很多细节的把控上，莆田鞋很难达到要求。当然，也有很多普通的流水线也生产正版的篮球鞋，但是超后的结果和品质有一定的差距。

莆田鞋平时穿，买来压压马路， 偶尔跑跑步这个没问题的，他的材料不差，做工也是可以，但是他的生产标准和品控制度不同，导致结果肯定有差距的。当然，你要看到正品的耐克也会觉得其实也就那么回事，正品的耐克开胶断线的太多了。但是在工艺细节方面，正品的工艺还是完全可以信任的。

在回过头来看市场现状，一双真鞋的利润是它造假的几倍甚至几十倍，细细想来更不要提假鞋的利润了，巨大的市场带来了巨大的利润，巨大的利润吸引了假鞋市场的各种商家，那些所谓的追求时尚的“潮儿”们不惜花几千上万的钱去买一双所谓的正版潮鞋，‘买点东西吃不好吗？’。同时也正是巨大的利润造就了鉴定平台的诞生，类如“得物”等等。起初这类平台还算良心，但是随着用户以及各种商家的加入，渐渐也变得不是那么像样了。

正所谓道高一尺魔高一丈，莆田鞋也打出了加价可以过各种检测平台，比真鞋还真的说法。总而言之，就我个人认为，现在的潮鞋市场，大家都只是加钱买个放心，你价格打的高的就相信你是真的，花钱买一种心理安慰罢了。当然这不是说不能买到真鞋，只是说现在买到假鞋的概率太大了。不知是国内的市场如此，国外的市场也同样如此，甚至在百度上直接搜索莆田鞋就有一推渠道，甚至还有完整的网站。

如下：

莆田鞋平时穿，买来压压马路， 偶尔跑跑步这个没问题的，他的材料不差，做工也是可以，但是他的生产标准和品控制度不同，导致结果肯定有差距的。当然，你要看到正品的耐克也会觉得其实也就那么回事，正品的耐克开胶断线的太多了。但是在工艺细节方面，正品的工艺还是完全可以信任的。在回过头来看市场现状，一双真鞋的利润是它造假的几倍甚至几十倍，细细想来更不要提假鞋的利润了，巨大的市场带来了巨大的利润，巨大的利润吸引了假鞋市场的各种商家，那些所谓的追求时尚的“潮儿”们不惜花几千上万的钱去买一双所谓的正版潮鞋，‘买点东西吃不好吗？’。同时也正是巨大的利润造就了鉴定平台的诞生，类如“得物”等等。起初这类平台还算良心，但是随着用户以及各种商家的加入，渐渐也变得不是那么像样了。正所谓道高一尺魔高一丈，莆田鞋也打出了加价可以过各种检测平台，比真鞋还真的说法。总而言之，就我个人认为，现在的潮鞋市场，大家都只是加钱买个放心，你价格打的高的就相信你是真的，花钱买一种心理安慰罢了。当然这不是说不能莆田鞋平时穿，买来压压马路， 偶尔跑跑步这个没问题的，他的材料不差，做工也是可以，但是他的生产标准和品控制度不同，导致结果肯定有差距的。当然，你要看到正品的耐克也会觉得其实也就那么回事，正品的耐克开胶断线的太多了。但是在工艺细节方面，正品的工艺还是完全可以信任的。莆田鞋平时穿，买来压压马路， 偶尔跑跑步这个没问题的，他的材料不差，做工也是可以，但是他的生产标准和品控制度不同，导致结果肯定有差距的。当然，你要看到正品的耐克也会觉得其实也就那么回事，正品的耐克开胶断线的太多了。但是在工艺细节方面，正品的工艺还是完全可以信任的。

在回过头来看市场现状，一双真鞋的利润是它造假的几倍甚至几十倍，细细想来更不要提假鞋的利润了，巨大的市场带来了巨大的利润，巨大的利润吸引了假鞋市场的各种商家，那些所谓的追求时尚的“潮儿”们不惜花几千上万的钱去买一双所谓的正版潮鞋，‘买点东西吃不好吗？’。同时也正是巨大的利润造就了鉴定平台的诞生，类如“得物”等等。起初这类平台还算良心，但是随着用户以及各种商家的加入，渐渐也变得不是那么像样了。

正所谓道高一尺魔高一丈，莆田鞋也打出了加价可以过各种检测平台，比真鞋还真的说法。总而言之，就我个人认为，现在的潮鞋市场，大家都只是加钱买个放心，你价格打的高的就相信你是真的，花钱买一种心理安慰罢了。当然这不是说不能

在回过头来看市场现状，一双真鞋的利润是它造假的几倍甚至几十倍，细细想来更不要提假鞋的利润了，巨大的市场带来了巨大的利润，巨大的利润吸引了假鞋市场的各种商家，那些所谓的追求时尚的“潮儿”们不惜花几千上万的钱去买一双所谓的正版潮鞋，‘买点东西吃不好吗？’。同时也正是巨大的利润造就了鉴定平台的诞生，类如“得物”等等。起初这类平台还算良心，但是随着用户以及各种商家的加入，渐渐也变得不是那么像样了。

正所谓道高一尺魔高一丈，莆田鞋也打出了加价可以过各种检测平台，比真鞋还真的说法。总而言之，就我个人认为，现在的潮鞋市场，大家都只是加钱买个放心，你价格打的高的就相信你是真的，花钱买一种心理安慰罢了。当然这不是说不能

光明正大的打出高仿的名号，成本不过百元，利润翻几番。

## 市场份额

说了这么多，说到底就是没有一个平台或者卖家能够保证他卖的鞋是百分之一百的真鞋，真鞋跟假鞋穿插在市场中，有可能你去专卖店买的鞋摆在外面给你看的是真鞋，从“仓库”拿出来的是假鞋，一真一假傻傻分不清，至少肉眼是无法识别出来的。

再说了，到底什么是真鞋？是贴了防伪的标签？还是质量好？或者说是价格高到离谱？就一定是真鞋吗？又或者是这些的勾好看，质量真好，我就认为是真的，那它就是真的了？还是说看什么所谓的“专家”说的玄乎其神的走线？再说了我打个比方，我有一双莆田鞋，我进价是200，质量超好，跟真鞋一摸一样，我在平台上按真鞋的价格能够卖到20000，你想买我的鞋，但跟我说要检测一下，我就找到了“专家”，分给他10000让他帮我作假爱，实际上他也看不出来，既然如此还不如拿了10000块说个谎，对大家都好，买家花钱买了个安心，卖家赚得盆满钵满，专家更是笑开了花。所以说所谓的渠道，路子，流程中拿到的鞋都没有百分百的保障。

说白了说到底什么是真鞋，从最最根本上来说就是从官方授权认证的工厂加工制造出来的就是真鞋，不是官方工厂出来的鞋就一律是假鞋，没有什么所谓的渠道，这是分辨真假鞋最粗暴最简单的方法，但是我们作为普通的消费者怎么可能看着鞋子从原材料进厂，全程盯着它一步一步从流水线出来然后直接交到你手上？先不谈有没有这个能力，就单说你愿意为了一双鞋子浪费巨额的金钱，和大把的时间吗？至少在我看来这是非常不切实际的东西。在现在的这种销售模式下，不论是线下还是线上都是不可能实现的，在线下买你不知道店员会不会骗你，在线上你不知道鞋子的来历，甚至拿到手之前都不知道是不是一双鞋子。

从现在的局面来看，在各大平台都只能提供部分保证的情况下，除了本来就想这要买假鞋的人以外，在价格远高于官方报价的情况下，还是有许多人愿意多花几百甚至上千元的“鉴定费”去各大平台上购买所谓的有保障的“真鞋”。就为了买一个心理安慰。到手的可能还是莆田做的高仿罢了。

这样看来假设有这么一个平台，能够提供百分之百的保障，那么就能得到消费者十足的信任，只要有了人气不想做大都难。

## 区块链加卖鞋

但是现在的传统互联网无法实现的事情，用区块链就可以非常好的解决这个问题，区块链的溯源和不可更改的特性在保真方面十分契合。既然从正规工厂出来的就是真鞋，非授权工厂出来的一律都是假鞋，那么只需要把工厂出来的每一双都上链，使用区块链透明公开，不可更改 ，完美溯源的特性来判断鞋子的真假简直再适合不过了。就相当于我从厂家拿出来鞋子卖，我还能拿出完美的证据，或者换一种说法，就等于你自己从厂家里拿出来的鞋子一样。保真度百分之一千。

## ERC721代币

讲到区块链加商品就不得不讲一下ERC721这个代币合约。首先什么是ERC721，ERC721是一种标准，只要是按照标准建立的“不可替代的代币”都可以称之为ERC721代币，这与目前主流的ERC20规格标准建立的代币不同。

ERC20 是目前最多人使用的以太坊代币主流规格标准，支持 Waltonchain、Storj，以及 Basic Attention Token 等在区块链上运行的代币。效用代币（utility token）是ERC20 代币的一种应用，可说是ERC20 使用的一个大宗，让创业家发行代币卖给使用者，使用者能用代币使用创业家开发的区块链服务。 ERC20 标准能够运行智能合约，能够在满足指定条件时用程式码对其进行编写程式。一个标准的 ERC20 智能合约需具备的函式有：

1.代币的全名

2.代币的缩写

3.代币的最小单位数值

4.代币的总量

5.查询帐户代币余额

6.转移代币

7.转移代币事件

8.从 A 地址转移代币给 B 地址

9.批准代币转移

10.A 地址批准给 B 地址的代币数量

11.代币批准触发事件

相较之下，ERC721 则是用于处理不可替换资产的另一种以太坊代币标准。可替换资产像是货币，它可以被其他任何平等单位替代，但诸如房屋、家具则属不可替换资产，它不能被替代，也不能被分割，这就是 ERC721 规格标准的主要效果。在 ERC721 标准下，能将资产转为唯一的、独特的 256 位元代币。而这种代币可以通过区块链上的智能合约追踪，从而建立数位化资产。

值得一提的是，因为 ERC721 标准是由 Axiom Zen 技术总监 Dieter Shirley 提出的，该公司风靡全球的游戏「谜恋猫」，也成为第一个采用 ERC721 标准的去中心化游戏应用。

ERC20 标准比起 ERC721 标准更早一些被提出，且很快的成为主流，目的是方便以太坊开发者为产品建立金融功能。而 ERC20 与 ERC721 的主要不同在于，钱包中的 ERC20 代币，只有数量的不同，代币之间是没有区别的。在 ERC20 标准下，关心的不是代币之间的区别，而是关心钱包帐号中的余额。 ERC20 代币被称作「可替换代币」，适用于可替换资产的价值。

另一方面，也因为有了主流 ERC20 规格代币，在以太坊平台下发行的代币多受限于可替换资产。但除了可替代资产，其实还有很多不可替换资产的部分。例如，特别稀有、可收藏的偶像签名海报、好友送的具有纪念价值的饰品等。因为不同的原因给物品赋予额外的、无法替代的价值，而这些价值似乎不是起初设计ERC20 所关心的主题，也因此有了ERC721 标准的出现，用于发行不可替换代币，补足ERC20 标准所缺乏的设计。

我们可以从 ERC721 标准规格内容中看到，兼容 ERC20 的方法有几个，包括代币全名 name、代币缩写 symbol、代币总量 totalSupply、代币余额 balanceOf。在 ERC721 标准中，可以看到开发者所增加的改进，让智能合约可以支持记录及转移代币所有权。 ERC721 规格内容中，新增的函式有：代币所有权发送 ownerOf、代币所有权提取 takeOwnership。此外，在 ERC721 规格中重写了代币批准授权 approve ，以及代币转移 transfer。 ERC721 和 ERC20 在记录所有权处理的方式不同， 在 ERC20 中，只需要知道帐户地址上有多少代币，而在 ERC721 中，则需要额外单独记录每枚代币的 ID。另外，ERC721 在转移代币所有权与 ERC20 中交易代币的过程相似，可以由使用者发起转移，另一位使用者接受转移，也可用代币转移 transfer 。

过去，因有以太坊 ERC20 标准，开发者可以发行应用产品中的专属代币，方便使用者使用应用中的金融服务。现在，有了时下流行的 ERC721 标准，预期将为以太坊应用领域创造新的局面，包括加密收藏品、虚拟物品、游戏宝物、游戏装备等等，期望再创新气象。未来将会出现越来越多的加密领域新兴应用，使用ERC721 代币确定真实世界中的房屋、土地、股票债券等所有权，利用ERC721 代币完成对这些资产的追踪、交易、审计，建造出一个活泼的新时代产权市场。

总而言之ERC721标准的代币适用于当今大部分的市场交易环境，特别是贵重的需要有标签防伪的商品，不但可以查看到商品的创造流程，交易流程，也可以查看商品的所有者，或者前所有者，这个道理就类似于古代书画收藏家，每收到一副名画都要在上面盖上自己的印章是一个道理，真迹传承下去久而久之就有许多名人的印章在上面，当然在古代人们可以仿造上面的印章，制造出假冒伪劣产品。但是在科技飞速发展的现在有了区块链这一项技术就不用担心了。

## ERC721代币挂钩正品鞋

之前我们浅谈了ERC721和区块链卖鞋的优点，接下来我想聊一下项目的设1计思路。

之前讲过，正规授权工厂出厂的鞋就是真鞋，其他的一律是假鞋，我的想法是运用ERC721代币，每一双鞋子出厂前都会有一个ERC721代币与之匹配，买家跟卖家都可以在区块链上查看到鞋子的信息。也可以查看鞋子之前的交易记录。

那么你可能就会有疑惑了，看来看去这只能保证“代币”的真实性，要怎么保证鞋子的真实性呢，就是说我拿一双假鞋一样也可以说这就是真鞋，一样上链，在交易的过程中把鞋子掉包一样无可以销售假鞋。说白了就是只能保证线上的真实性却不能保证线下的真实性。确实，那么就需要借鉴一下现在的防伪方式了，现在的传统防伪方法就是在鞋子内部和鞋盒上做防伪标志，我的想法是在鞋子的材料上做防伪，比如说通过在鞋底上做防伪标志，出场的时候就自带的，不知在看得见的外面做防伪，在看不见的内部也做好标志，而做了防伪标志的鞋子就只能在我们的区块链卖鞋平台上售卖，一旦卖出如果你不是拥有者就不能交易。

这样的话就有另一个问题，如果有人买了我的鞋子按照防伪做一双一摸一样的假鞋再拿出来售卖怎么办？但是我认为这是不现实的东西，如果你是商家，一个代币是一双鞋对应了一个唯一的防伪标签，一旦卖出了这双鞋，就不能再对这双鞋进行交易，就算造假一双鞋，一摸一样的，拿去别的平台上卖，但是又这种防伪标志的鞋之能在区块链上交易，别的平台也不会允许这种一看就是造假的行为。而且成本也非常的高，因为没双鞋都是不一样的标签，要做的话就赚不到什么钱，也是非常麻烦。更不用说个人买家了，买来做一双假鞋再交易真鞋出去，那么先不算你二手的差价，就说普通的个人卖家是不可能又能力自己作假的，有这能力还买什么鞋，直接自己做不就好了？

所以说还是相对来说比较好的解决方法，卖假鞋就是为了赚钱，如果从根本上不让他有利润可赚，甚至还有可能会亏本的话那么就别说卖假鞋了，造假鞋的鞋厂都会倒闭。

## 区块链的优势

说了这么多，跟区块链有个毛的关系，以前的互联网不能实现这种销售模式吗？我可以非常肯定的告诉你，不行！

以前各大厂商为了防伪也想出过各种花里胡哨，稀奇古怪的防伪方式，在没有互联网交易的时候有各种防伪，材料防伪啊，标志防伪啊，甚至还有鞋盒防伪。进入了互联网时代，就有各种官方鉴定网站，平台。但是最后还是被庞大的假鞋卖家趁虚而入。归根结底，传统互联网就算你做了防伪，你卖出去了，可是不知道是谁买的，不知道到底有多少，市场上依然会出现许多双一摸一样防伪的鞋子，就像我之前说的全球限定一百双，中国1000双，莆田900双。世界那么大你永远不知道有多少跟你一样的防伪鞋。

但是运用了区块链的技术就可以很好的解决，卖出去了就是卖出去了，你可以查，现在的所有人，卖家，鞋子的数量，只要你不是区块链上显示的所有人，你穿着跟链上显示一样的鞋子那么你的鞋子就肯定是假鞋。那我还要说了，我这鞋子是我爸给我买的，所有人是他不是我那我的鞋是假鞋吗。不用担心，就算你买鞋送人，我们的代币也是可以交易给他人的，只要你愿意，显示的拥有者就是你。

所有的一切都是公开透明的，可溯源可查，妈妈再也不用担心打球的时候别人说我的鞋是假的了，要是有人说你的鞋是假的，马上打开APP给他看，这就是老子的鞋，保真，不真不要钱。

## 杜绝旧鞋翻新卖出

还有些奸商为了赚钱，翻新旧鞋卖出‘旧鞋：一般指旧的真鞋’，这样既不会被别人说你的鞋是假的，也可以把一切售后问题都交给‘品控’来解释。这在现在是很难处理这种情况的。首先你如果怀疑这双鞋是翻新的，那么鞋的表面一定看不出来，如果要确定它是不是翻新就需要把鞋拆开，而拆开以后就很难再复原了，是翻新还好，如果是新的呢。就算你有证据我卖家一口咬死不承认，你也查不出什么东西来，没有足够的证据证明鞋子是卖家做旧的，那卖家还就有可能说是买家做旧的想骗钱。那真的是公说公有理，婆说婆有理了。

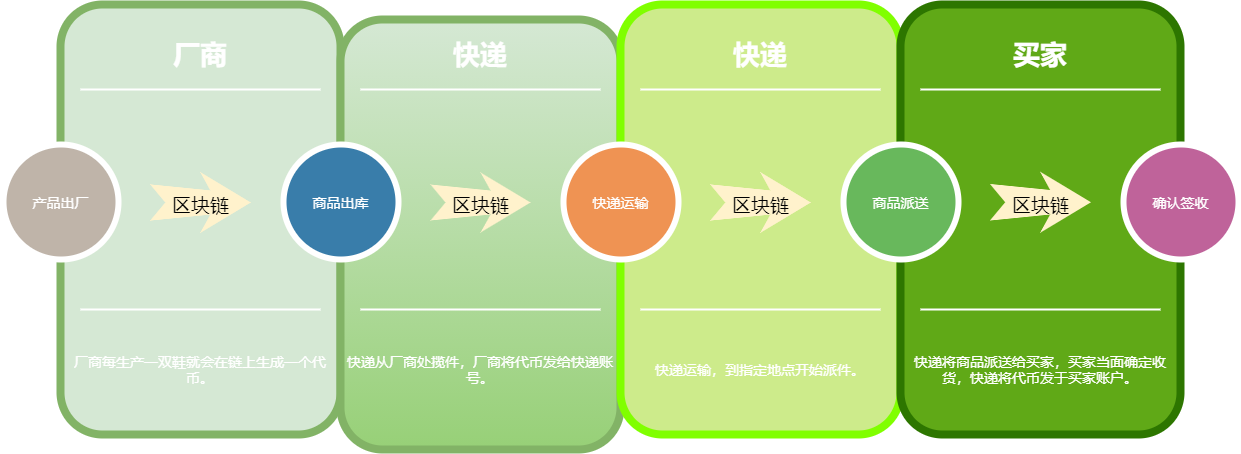
这时候区块链的优势就出来了，溯源性！可以通过事件来查看交易的记录。这种时候他想赖账也不可能了，只要一查都可以查到，想赖账只是搬起石头砸自己的脚罢了。

## 交易流程

首先，厂商每生产一双鞋就会在链上生成一个代币，同一款鞋就是由一个代币合约出来的。生产多少双鞋就有多少个代币，每一双鞋都有一个单独的特殊码，每一个单独的特殊码都可以在链上找到对应的一个721代币。

但是说到实际交易，那就不得不再引入一个中间账号了，快递的存在。因为如果仅有买家跟卖家的存在的话，那么居于现在的互联网交易方式，你在我的平台上买了东西，我是需要寄给你的，无论是现在的次日达，半日达，还是一小时送上门都是需要时间的，不可能你下了单下一秒就变给你，至少现在做不到这一点，如果只存在两个交易商的存在，那么你买了我的鞋，按照区块链的执行方式我就需要把代币发给你，可是你刚下单，我可能快递都没寄出去我代币发给你，你没拿到鞋，我也没有了代币，讲小了是时间问题，往大了说就是信用问题了，这就会牵扯到很多利益纠纷和民事问题。这时候就必须要快递这个中间人的出现了，买家购买了鞋以后，卖家把代币发给快递，再由快递寄给买家，买家当面验收以后，快递就把代币发给买家。这样就可以完美符合现在的交易逻辑，减少各种不必要的问题。

虽然运用了区块链实现了一种全新的交易方式，但是基于现实状况的考虑，不得不借用一下之前的网络交易方式了,所以到头来还是需要快递。

流程图：

Ps:当然中间也可以引入商家，商家的交易流程也是跟厂商一样的。

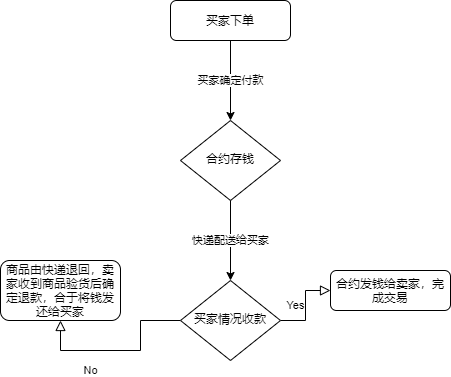
## 钱款去向

既然是要做一个基于区块链的平台,为了保证平台的可靠性，那么所有的交易都是要在区块链上进行，如果还是线下支付现金，或者线下转账不在区块链上做记录的话那么就跟现在的互联网模式一样，没有任何安全性和可靠性。

也就是说，既然一切都要在链上交易，每个交易对象都需要以太币(以太币是市值第二高的加密货币)，没有以太币如果想在基于区块链平台上交易的话只能先购买以太币再进行交易，虽说这无形之中增加了交易的总成本，但是从另外一个角度来看的话，成本的增加无形中也减少了许多黄牛以及一些中间商想要投机取巧的想法，变相保证了客户的纯正性，也使那些假鞋卖家想要在链上贩卖增加了许多成本。但是销量是完全可以保证的，毕竟现在各大平台上加价好几倍的都有。这多出来的一点成本价不算什么。

回归正题，首先由商家上架商品的同时不但在721代币中写入了产品的名称，同样也写入了产品的价格，点击购买按键时买家需要支付卖家设置的价格，这时钱转入合约中，当快递送货上门确认签收以后，买家通过确认收货按键，将合约中自己付的钱的金额转给卖家的以太坊账户。当然在买家支付完钱以后，在没有确认收款之前，卖家都可以在卖家界面查看到合约中的总金额。

这里就有点类似于jd自营的运营方式了，jd的自营产品都是由jd自己的快递运输的，当快递运给买家以后，买家收到快递，由快递员来点接受，买家不用额外确认收货的。其实最开始的想法是，由买家来点确认收货，然后再由合约调用方法将快递的代币转给买家，同时也将合约中买家支付的以太币转给卖家，但是转念一想这样买家的权限就有点大了，而且通过调用合约的方法来实现让买家操作快递方的以太币，首先快递要用方法给合约权限，指定该买家购买的以太币的转账权限，这样还是要快递先执行一手再由买家来执行，这样会造成没必要的gas消耗，也会造成交易过程的繁杂以及不必要的麻烦，引起没必要的人力消耗，同时代码量也会增加，不利于后期的维护以及运营。

在整个交易流程中，钱款去向是完全公开透明的，任何人都可以再链上查看到钱款的信息，这也是只有区块链这种交易模式能够做到的了，一切都运行在合约上，没有中间商或者服务器的存在，合约一经写好部署就无法改变，合约所有者只能拥有合约的权限，但是无法更改合约的数据。这打破了之前的互联网交易模式，这使得交易更加可信，在这种交易环境下每个人都是平等的。所有交易信息的公开透明使得所谓的暗箱操作，垄断，都无法存在。

## 账户权限

回看现在的互联网交易模式，发起一项交易，哪怕只是买一卷纸，或者是买一包牙签，都至少由4个交易方，商家提供牙签，获取利益，快递运输牙签，平台负责监管整个交易流程，买家购买牙签使用。

那你可能会认为这样看来区块链也是有4个交易方啊？但是区块链上的平台并不属于任何人，或者说并不归任何人管，只要给了权限就能使用合约的相关功能，没给权限就无法使用且一旦合约上链就无法更改。这跟现在的平台完全监管，权力中心化集中是完全不一样的。

这就需要讨论到一个账户权限的问题，所有的权限都写在合约中，那么要给谁权限，根据不同的身份来分配权限就变得极其重要以及合理。

厂商：首先考虑的也是最重要的就是厂商了，厂商作为商品的最初拥有者以及合约的所有人，权限自然就要大于他人。所以厂商就可以也只有厂家可以上架商品，和给予商品“出场价”。同时也可以查看合约中的以太币余额，和商品的总供给量(商品发布的总数)，当然也可以查看现在合约中鞋子的数量和价格。

如图：

快递：其次就是快递了，作为一个中转人来说，给的权限不需要太大，但想要在链上做交易就必须要给权限，所以快递的权限就仅限于查看自己账户中的代币(快递、鞋子)的数量以及代号，然后转账给买家的账户，或者授权给合约让合约对快递的代币进行操作(未完成)，当然也可以从界面上查看到合约的总供给量，获取厂商的总生产量，仅此而已。

如图：

买家：给买家权限就比较矛盾了，既不能触及到合约的核心权限，以保证合约的安全性，但也不能给过少的权限，这样不符合交易逻辑，为了保证交易的正常流程以及有序运行，买家可以操控“确认收款”：当买家收到款以后可以将自己付的钱的同等合约额度(合约中的额度)发送给商家，当然同时也要可以查看合约中的代币数量(鞋子数量)，来供买家挑选及购买，一样也可以查看总供给量，防止出现“全球限定100双，中国1000双，莆田900双的状况。”给他人同样的权限就是为了让合约中的所有人一起做监督者，最后也是最重要的就是购买键了，买家按下购买的同时，合约将购买的鞋子发送给快递，快递收到鞋子和代币开始运输，代币发送给快递的同时，也将买家彰化的钱发送对应鞋子价钱的以太币给合约。这样就既符合正常的交易思维逻辑，也符合合约的权限限制。

如图：

## 测试平台

### 开发环境的配置

|  |  |
| --- | --- |
| 类别 | 标准配置 |
| 计算机硬件 | Cpu:Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz 2.21 GHz  内存:16G , 硬盘:2.5T M.2 NVMe (1T+1T+500G) ,  显卡:NVIDIA GeForce RTX 2060 |
| 软件 | Draw.io 13.9.9 ; Geth 1.9.25 ; Web3js ; Google Chrome ; Remix ;  Microsoft Visual Studio Code ; Metamask ; Cmd ; Typora version 0.9.98 |
| 其它 | 配置好以太坊环境以及安装web3js，搭建本地链和可安装Metamask的浏览器。 |

开发配置基于本人笔记本配置而定，具体情况未知。

### 运行环境的配置

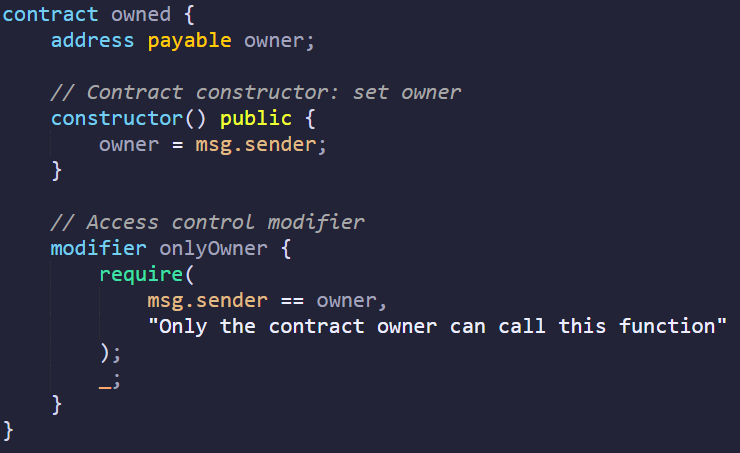
|  |  |
| --- | --- |
| 类别 | 标准配置 |
| 计算机硬件 | Cpu:Intel(R) Core(TM) i7-10870H CPU @ 2.20GHz 2.21 GHz  内存:16G , 硬盘:2.5T M.2 NVMe (1T+1T+500G) ,  显卡:NVIDIA GeForce RTX 2060 |
| 软件 | Google Chrome ; Metamask ; Web3js |
| 其它 | 配置好以太坊环境以及安装web3js，搭建本地链和可安装Metamask的浏览器。 |

运行配置基于本人笔记本配置而定，具体情况未知。

## 重要代码介绍

代码详见zzq.sol

1.代码截图：



文本代码：contract owned {

address payable owner;

// Contract constructor: set owner

constructor() public {

owner = msg.sender;

}

// Access control modifier

modifier onlyOwner {

require(

msg.sender == owner,

"Only the contract owner can call this function"

);

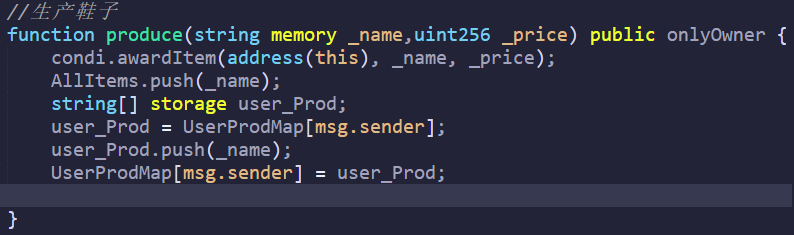
\_;

}

}

代码含义：设置合约的owner(所有人)。

2.代码截图：



文本代码：

function produce(string memory \_name,uint256 \_price) public onlyOwner {

condi.awardItem(address(this), \_name, \_price);

AllItems.push(\_name);

string[] storage user\_Prod;

user\_Prod = UserProdMap[msg.sender];

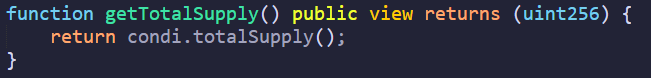
user\_Prod.push(\_name);

UserProdMap[msg.sender] = user\_Prod;

}

代码含义：生产鞋子的代码，输入名称和价格，onlyOwner只有合约所有人才能调用，调用condi中的awardItem方法，将名称绑定代币ID。

3.代码截图：



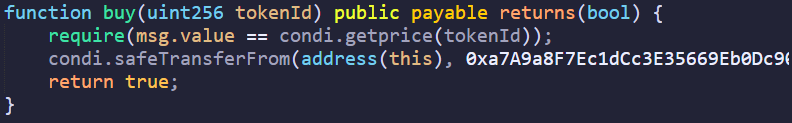
文本代码：

function getTotalSupply() public view returns (uint256) {

return condi.totalSupply();

}

代码含义：获取合约中的总生产量，返回condi中的totalSupply返回值。

4.代码截图：

文本代码：

function buy(uint256 tokenId) public payable returns(bool) {

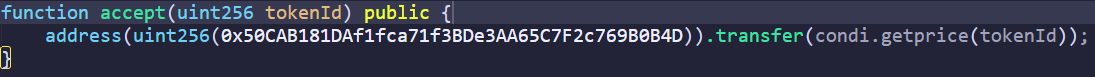
require(msg.value == condi.getprice(tokenId));

condi.safeTransferFrom(address(this), 0xa7A9a8F7Ec1dCc3E35669Eb0Dc90D2A589AF64eb, tokenId);

return true;

}

代码含义：用于提供给买家购买的方法，payable支付以太币，require查看支付的以太币是否等于商家设置的price然后发起转账合约将以太币从合约转给快递。

5.代码截图：

文本代码：

function accept(uint256 tokenId) public {

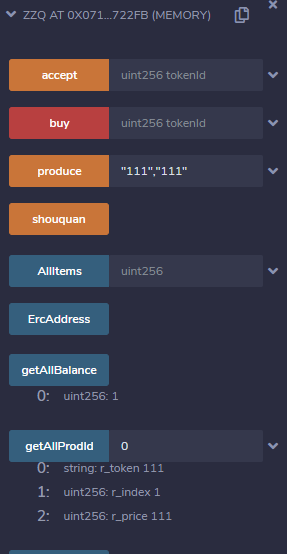
address(uint256(0x50CAB181DAf1fca71f3BDe3AA65C7F2c769B0B4D)).transfer(condi.getprice(tokenId));

}

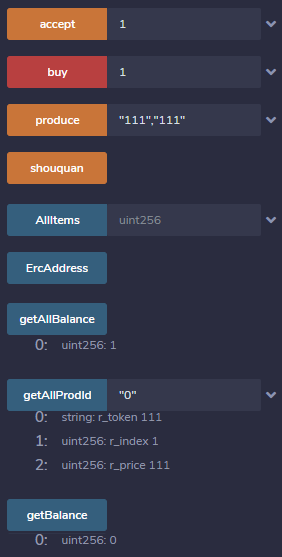
代码含义：买家确认收款，将合约中的钱发给商家。

## 实机演示

创建一个名字为111，价格也为111的鞋子，并且用getAllProdid方法查看。

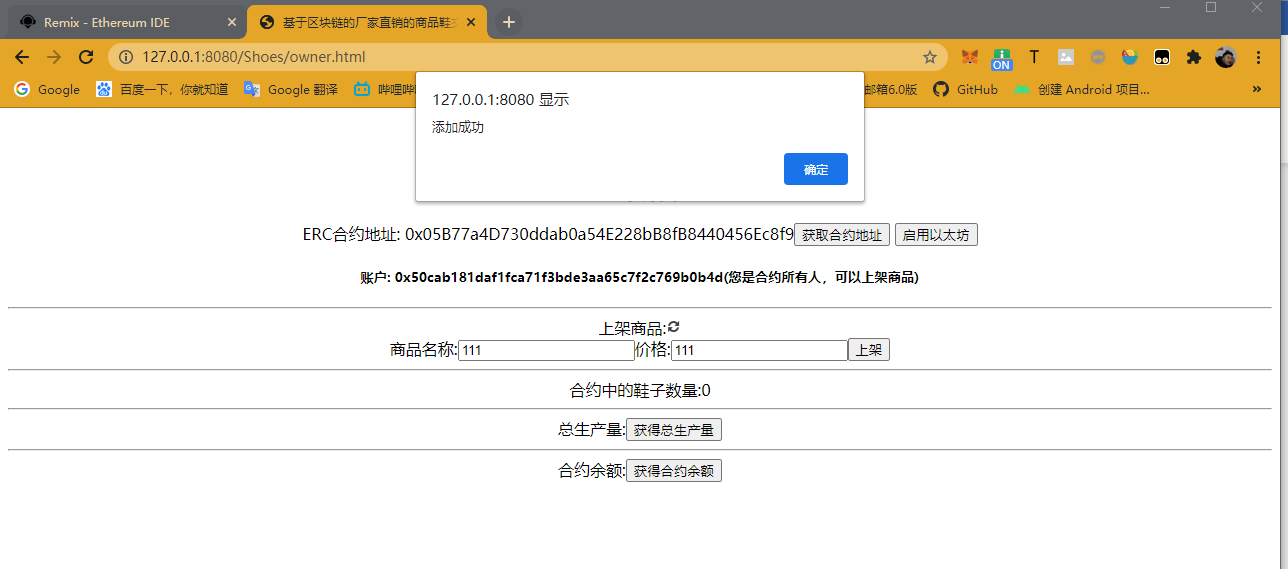
如图：

买家购买名为111的鞋并且支付111，通过查看合约中以太币余额确定买家是否付款。

最后确认收款，通过查看合约中的余额确定钱转给商家

## 前端代码演示

首先同样由商家在owner.html界面上架商品，比如我们上架一个名称为：111，价格也为：111.的商品，点击上架按键，弹出metamask认证要求再次确定，上架完成后会弹出一个弹窗提示上架完成，同时会显示出合约中的鞋子数量，以及总供给量和合约中的余额，但是这时买家还没购买鞋子，所以合约中的余额应当为0.

如图：

查询后应为：

这是代表商品已经上架成功，我们切换买家界面，同时metamask切换买家账号，通过买家的钱来进行购买。买家因为前面讲到的用户权限问题只能看到自己的鞋子数量以及合约中的鞋子数量及价格（也就是“可供购买的商品。”），并且同样可以看到总供给量。买家刚进界面应为：

买家确定购买以后点击购买按键，meta mask弹出认证，买家确定价格后点击确定购买，购买成功也会弹出一个弹窗提示购买完成，这是鞋子以及由合约发送给了快递。买家无需做更多的操作。只需等待快递的送达即可。

这时我们切换到快递的界面，同时也在meta mask中切换到快递的账号。因为快递只是一个中转人，所以他的权限并不多，只能支配他现在手上所拥有的鞋子（所对应的ERC721代币），同时为了起到公平公开的作用，所有人一起监督交易的运行，快递也可以查看到合约的总生产量。但是注意，快递是看不到每双鞋子对应的价格的。

所以当快递接收带代币时界面应为：



当快递运输到买家手上时，快递在接受人框中填写买家的账户地址，将代币转账给买家。这时会弹窗确认代币的id以及买家的地址信息，快递确认无误后在meta mask中再次点击确认，快递工作到此结束。

此时我们需要再切换会买家界面，进行“确认收货”环节，当快递运输给买家并且也将代币发给买家以后，这是钱还是存在合约中的，那么就需要买家手动确认收货了，同时记得再meta mask中切换回买家的账户。这是会看到，快递已经将买家购买的鞋子发送到买家的账户了，买家可以在用户界面中查看到我的鞋子数量，每双鞋子后面都有一个对应的确认收款按键，点击确认收款将钱款从合约中发送给商家，完成全部交易。

如图：

这时完整交易流程已经完成，所有交易以及操作都是在本人本地私链上运行。同时我也部署在了Ropsten测试网络中，部署Hash: 0x261ca102f455345f0A4371cB6518480B6324747a；

0x0eDF43349Ea20f6190769ce40151e96F7f1fe949

## 结语

以上就是我提出的基于区块链的卖鞋供应链，为一人独立完成，全部基于本地测试，未经公开测试，仅做参考。