**浅谈防伪溯源之区块链**

**---互联网的最后一块拼图**

**定义---------------------------------**

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的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法.

**本质----------------------------------**

是一个去中心化的数据库，分布式的公共账本(记录本).区块链是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一次网络数据交互的信息，用于验证其信息的有效性（防伪）和生成下一个区块,即是一种底层技术和基础架构.

(中心化案列:中心化交易模式

淘宝(中心)

平台收到钱了,

你可以发货了

我交钱了

买家 卖家

已发货

)

风险:

1:如果支付宝系统出了问题便会造成这笔交易的失败

2:你和卖家都要向第三方提供多余的信息,各方信息的安全性

3:支付宝跑路

**去中心化优势**:**---------------------------**

处理方式就要显得简单很多，你只需要和卖家交换钱和物品，然后双方都声称完成了这笔交易，就OK了。

去中心化是区块链技术的颠覆性特点，它无需中心化代理，实现了一种点对点的直接交互，使得高效率、大规模、无中心化代理的信息交互方式成为了现实

[狭义](https://baike.baidu.com/item/%E7%8B%AD%E4%B9%89" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)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](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E7%BB%93%E6%9E%84/1450" \t "https://baike.baidu.com/item/%E5%8C%BA%E5%9D%97%E9%93%BE/_blank)， 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、利用由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

**去中心化小模型**:**-----------------------------**

我们来看一个简单的去中心化模型：如果A借了B 100块钱，这个时候，A在人群中大喊“我是A，我借给了B 100块钱！”，B也在人群中大喊“我是B，A借给了我100块钱！”，此时路人甲乙丙丁都听到了这些消息，因此所有人都在小本本上默默记下了“A借给了B100块钱”。你看，这个时候一个去中心化的系统就建立起来了，这个系统中不需要银行，也不需要借贷协议和收据，严格来说，甚至不需要人与人长久的信任关系（比如B突然又改口说“我不欠A钱！”，这个时候人民群众就会站出来说“不对，我的小本本上记录了你某天借了A100块钱！”）

**防伪行业的痛点**：**----------------------------**

假货泛滥，防伪市场无序，安全性及信任度无法保障，缺乏统一的验证中心，防伪形式单一，衍生服务少,商家缺乏对商品的有效有力的管理，溯源手段。缺乏实用的商品和供应链金融工具.

在中心化账本模式下，谁作为中心维护这个账本变成了问题的关键。无论是源头企业保存，还是渠道商保存，由于其自身都是流转链条上的利益相关方，当账本信息不利于其自身时，其很可能选择篡改账本或者谎称账本信息由于技术原因而灭失了

区块链与防伪溯源**---------------------------**

把区块链技术应用在溯源、防伪、优化供应链上的内在逻辑——数据不可篡改和加盖时间戳.

比如我借钱的时候给我的钱写上标记（给我喊的那句“我是A，我借给了B 100块钱”标记时间1.这样以后在每一笔交易的时候，我在高喊“我借给了某某100！”的时候，会附加上额外的一句话：“这张100的来源是记为时间1的那条记录，我的这句话标记为时间2.这样就解决了伪造与溯源的问题。

**区块链防伪溯源商业案例------------------------**

**最成功案列之比特币,底层架构技术就是区块链**

1沃尔玛保障猪肉供应链安全:

中国是猪肉消费大国，猪肉消费量占到全世界的一半以上。做为最大的零售商，沃尔玛全球区块链计划的第一步始于保障中国市场的猪肉供应链安全。

此项目利用IBM基于Linux基金会旗下开源软件Hyperledger建立的区块链技术，可及时将猪肉的农场来源细节、批号、工厂和加工数据、到期日、存储温度以及运输细节等产品信息，以及每一个流程的信息都记载在安全的区块链数据库上。

通过该项目的实施，沃尔玛可随时查看其经销的猪肉的原产地以及每一笔中间交易的过程，确保商品都是经过验证的

2钻石防伪验证:

Everledger公司的工作重点是确保区块链上每颗钻石的来源，登记钻石身份和记录钻石流转过程。

Everledger的主要客户是承接钻石偷盗险的保险公司。保险欺诈是欧美保险公司最头疼的问题。美国和欧洲的保险公司因为保险欺诈每年要损失450亿英镑，经管保险公司的年度反欺诈支出高达2亿英镑，65%保险欺诈无法破案。这其中，每年约有1亿的金额被用于珠宝的失窃赔付。

Everledger正是瞄准了这样一个市场。通过和美国、安特卫普、以色列、印度等地的钻石鉴定机构合作，Everledger利用钻石的4C信息（颜色、切工、纯净度、克拉）外加14个特征数据，为每个钻石生成一个独立编号。通过在区块链上记录这一编号的流转过程，Everledger可以转载钻石的归属和所在地。当钻石不幸失窃时，保险公司在Everledger上将该钻石标记为被盗。这个钻石无法再次投保，如果被用于抵押也很容易被接受抵押的机构在Everledger上查找到，同时还为执法机构追寻赃物提供了方便

3京东防伪追溯开放平台

利用对产品防伪和全程追溯体系丰富的业务经验，针对每个商品，记录从原材料采购到售后的全生命周期闭环中每个环节的重要数据。通过物联网和区块链技术，结合大数据处理能力，与监管部门、第三方机构和品牌商等联合打造防伪，和全链条闭环大数据分析相结合的防伪追溯开放平台。

平台基于区块链技术，与联盟链成员共同维护安全透明的追溯信息，建立科技互信机制，保证数据的不可篡改性和隐私保护性，做到真正的防伪和全流程追溯

4**阿里巴巴**:

2017-11-08,阿里巴巴,蚂蚁金服与雄安新区签署战略合作协议,承建数字雄安区块链实施平台

**区块链行业效应------------------------------**

**1迅雷**

曾经是国民级PC应用的迅雷，装机量仅次于QQ，但在近十年的巨头混战中，它却一直扮演着安静的看客。一度沦落到靠甩卖业务、断臂求生的它，搭上区块链和共享经济这辆顺风车，在这云计算大战中，打了个不错的翻身仗。迅雷股价一日大涨30%

**2人人网**

蹭上了区块链的热点，人人网这家几乎已经被遗忘的公司，用2018年头两个交易日的大涨，再次回到了公众视野。人人公司的股价超过了52周高点，两日累涨76%

**3美图秀秀**

美图一则仅仅表示’有意’进军区块链的消息传出,仅1月5日一个交易日，美图公司就涨了11.01%

由以上动态来看不管是市场还是投资人都对区块链技术抱有极大的信心和投资热情,再加上防伪溯源与区块链理念完美契合,相信引用区块链是另一个比较好的发展方向.

**4香港UBI**

**只是因为在新改的名称中加入了区块链字眼,表示将要利用区块链技术为消费者追踪食品或药物源头,短短几日股价暴涨1108%**

**区块链和防伪溯源的契合点-----------------------**

（一）去中心/中介化的信任。系统自身保证其真实性，不需要外在信任背书主体介入。   
（二）其特征是它的稳定性、可靠性、持续性，因为它是一个分布式的网络架构，不存在单点故障，所以在整体的技术架构方面有着更强的稳定性、可靠性和持续性。   
（三）它安全的加密机制，共识机制不需要第三方的进入，而是通过技术中介，来达成整个交易。   
（四）因为链上数据只能增加，不能修改的特性，从而决定了交易的公开透明和不可篡改性。

**关于实施方案(大致)------------------------------**

**1技术原理:**

**A区块链是一个放在非安全环境中的分布式数据库（系统）。**

**B区块链采用密码学的方法来保证已有数据不可能被篡改。**

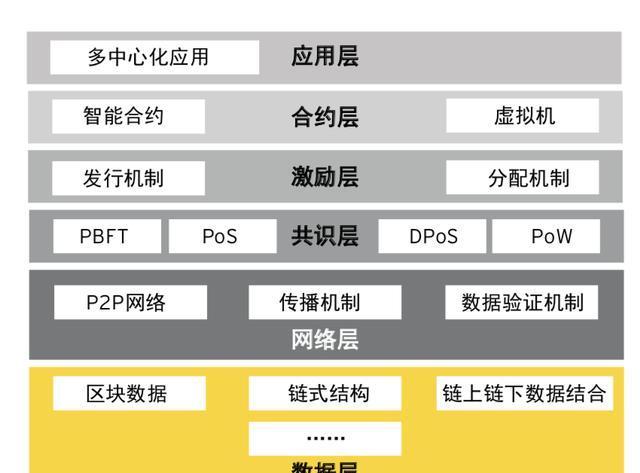
**C区块链采用共识算法来对于新增数据达成共识。**

**具有以上三个性质的系统，就是区块链**

------那么我们的区块链将提供的是一个由生产者、品牌商、经销商等各个节点去中心化(即每个节点都是中心)共同维护的记录本系统，包括生产、入库、出库、分销、零售等各环节都登记在区块链上，保证信息真实有效、无法篡改，以防作假。这样，品牌可以实现防伪，以达保护品牌的目的；保证整个防伪溯源过程的真实可靠，消费者更放心，生产商能获得更高的利润，各个环节也更规范,实现来源可查、去向可追，责任可究.

**2编程语言:C/C++,Nodejs/Javascript,Python**

**以下是国内首家区块链防伪架构----唯链**



**3**成型方案:

1利用第三方成熟框架完成公司架构设计开发(埃克森尔科技--Scry.info区块链开源社区)

2完全由技术人员全新开发一套属于自己的区块链技术架构与算法

3自有人才培养或者引进

4将防伪溯源与区块链结合的信息展示出来,广告打出来,让用户和投资人充满信心

---技术中心