加密权益证书商品防伪技术

作者：雷杰 JIEH.LEI@GAMIL.COM

Contents

1. 定义

假冒商品是商品在制造时，逼真地模仿其他同类产品的外部特征，或未经授权，对已受知识产权保护的产品进行复制和销售，借以冒充别人的产品。-- 百度百科定义

假冒与正品的根本区别在于是否获得知识产权所有者(IP owners)的授权。“授权”不是一个物理或化学特征，在数据类型上授权属于非结构化数据(Unstructured Data)。所以我们无法通过物理化学方法观察或测量授权，同时也没有预定的数据模型，不方便用传统数据库来处理授权数据。当前主流防伪技术对于鉴别及杜绝假冒效果不理想，原因是因为没有或者无法正确的处理授权信息。

2. 主流防伪技术

依照防伪逻辑我们可以将现有主流商品防伪技术分为两大类：物理防伪技术（Physical Authentication）以及追溯技术（Track & Trace Technology）。

2.1 物理防伪技术

物理防伪技术有着千年的历史，至今仍在推陈出新，但是它底层防伪逻辑并没有改变：具备验证元素（Authentication Element，防伪标签、特殊材料、特殊工艺…）的产品是正品，否则是假冒。它通过物理检测判断被甄别物体是什么。通过检测我们可以了解验证元素的机

械、分子结构，力学、光学、电子等特征，理想状态下可以推断出验证元素的生产厂家或者材料来源。然而我们无法通过物理化段获得授权信息，因为授权不是一个物理特征，它无法被观察或测量。而区别一件商品的真假的根本标准是该商品是否获得知识产权所有者的授权。

图 1 授权来源来自于商标的暗示

例如我们知道“莆田鞋”是高仿的代名词，它们的材质、外观、工艺水准比起正品都毫不逊色。得益于强大的供应链，“莆田鞋”的出货速度甚至优于正品。耐克东南亚代工厂疫情恶化导致工人流失及减产。假设今天耐克为获得既时产能，紧急授权“莆田鞋”工厂进行代工。那么同样的款式、材料、工艺及质量，此时“莆田鞋”就成了产地莆田的正品。而这前后的区别仅在于代工工厂有没有获得授权。

那么独门工艺是否能防止仿冒？答案是肯定的，前提是满足以下两个条件：

1. **工艺的保质期**。假设所有耐克鞋都采用量子油墨制作防伪标签，再假设量子油墨全世界目前只有 3M 的一间工厂能生产。那么是否究竟是由耐克决定什么是耐克正品，还是由 3M 量子油墨标签的产能决定？耐克如何确保 3M 不会超额生产量子油墨标签，因而可能被用到假冒品上？耐克又如何保证 3M 不会将量子油墨技术技术转让给第三方？第三方获得的量子油墨技术会不会被造假者出高价运用到未经耐克授权的防伪标签上？这些问题的答案都不在品牌的可控范围之内。
2. **没有信息差**。独门工艺有保质期，品牌企业需要不停的投入新技术，这又导致了信息差。举例来说，在只有前四套人民币鉴定知识的人眼里，第五套人民币是假币，因为很显然的第五套人民币无法通过他知识库里前四套人民币的防伪鉴定标准。同理一个茅台酒鉴定大师不经过系统学习大概率无法胜任五粮液的鉴定，更何况普通消费者面对五花八门的商品以及出不穷的物理防伪技术。而造假者正是利用信息差让假冒防不胜防。

利用物理特征与商标去暗示“授权”的存在，这无异于与虎谋皮，因为造假者大概率拥有同样的工艺与原料，还有信息差这个造假利器。

2.2 防伪追溯技术

防伪追溯技术有几十年的发展历史，是一个以数据为驱动的防伪技术。它记录每件商品从获得授权，到制造、集散、销售等过程的所有生产数据。通过分析这些数据得知一件正品应该或者不应该出现在哪。

防伪追溯技术的可见验证元素（Overt Authentication Element）是防伪码，通常以二维码、RFID、NFC 等物理载体形式出现；不可见验证元素（Covert Authentication Element）是关系数据库（Relational Database）数据。

图 2 克隆的防伪码可以指向相同的溯源数据

防伪追溯技术有几个缺点。首先它的初期投入较高。供应链上所有参与机构都必须在现有生产数据基础上进行额外的软硬件升级以及人员培训，以便衔接上下游的数据库以及服务额外的溯源数据库。其次庞大及分散的数据来源增加了采集成本也提高了数据造假的风险。假海外代购通过异地登陆物流系统对发货地点造假，就是一个有效记录虚假信息的例子❶。最后防伪追溯技术并没有内置的防伪逻辑，纯粹的数据没有权属，复制后可以被任意使用。造假者甚至不需要伪造数据库，只要复制防伪码即可。不论用什么物理载体去复制防伪码，它最终都会与正品一样指向数据库里同一套溯源数据。原装与复制防伪码解析结果没有任何差异。

一些防伪企业为了保障数据的排它性，采用统计防伪码被识读次数来判断是否出现假冒：防伪码被识读超过一次以上则判断出现仿冒（一物一码）。这个防伪逻辑有着天生缺陷，甚至会导致正品因为被反复扫码而被判断为仿冒。例如 2018 年茅台被内鬼泄露 700 万个防伪码，那么损人不利己者只要让茅台官方 APP 对这 700 万防伪码进行反复验证，那么最终都会因验证请求过多而被官方 APP 判断为假冒。

3 加密权益证书技术

这里我们看到物理防伪技术以及防伪追溯技术都没能从根本上甄别或者杜绝假冒，因为不能正确有效的确定、管理及保障“授权”数据的唯一性和独占性。品牌企业及消费者都需要一个全新的数据模型，以及一个全新的防伪逻辑来防止假冒。区块链技术的日益成熟让这个需求的实现成为可能。

基于区块链的权益证明（Blockchain based proof-of-ownership）概念最早于 2018 年被提出，在 CryptoC14、Arianee 等几个初创企业的开发和推动下，这个概念已经转化为加密权益证书商品防伪技术，并进入商业可实施阶段。

加密权益证书商品防伪技术利用区块链一个特殊的加密资产 NFT（Non-Fungible Token，非同质化代币）为每一件商品赋予一份授权。具有品牌企业赋予的加密权益证书 NFT 的商品是正品，否则是假冒。

NFT 是区块链上独一无二的加密资产，它具有唯一性及不可替代性的特性。NFT 所在区块链钱包的拥有者对 NFT 具有完全排它性的所有权力。NFT 可以理解为一个加密的权益证书（Crypto Certification of Ownership）。

加密权益证书与珠宝证书、房地产证等实体证书不同，实体证书只要能制造出来就可以被克隆或仿制。但是作为权益证书的加密载体 NFT，它的授权来源及本体都不可能被克隆或仿制，除非区块链的加密机制被解破。常见区块链采用的 SHA-256 加密算法，这个算法的解破成本

远高于商品造假获利，而且目前来看 SHA-256 算法在未来很多年都将会很安全。

3.1 方案的组成

加密权益证书商品防伪解决方案由实体商品、可见验证元素、不可见验证元素、分布式账本及应用 5 个部分组成。

- 不可见验证元素：保存于区块链上的 NFT。每一个 NFT 对应一个实体商品。这个映射由授权企业完成。 NFT 的生成以及所有权受到密码学的保障，不能被克隆也无法被伪造。
- 可见验证元素：NFT 编号。建议以条码、二维码形式附着于实体商品及包装上。亦可采用 RFID、NFC 等数据载体。条码、二维码具有成本低以及可以远程鉴定等优点，尤其适合当前网购的消费模式。CryptoC14 的 NFT 编号为 18 至 20 位的数字组合。
- 分布式账本（区块链账本）。授权数据通过 NFT 令牌化之后我们通过分布式账本去管理。授权是一个中心化行为，但是授权的转让通常在去中心化环境下完成。通过分布式账本与令牌模式获得数据写入权限是处理这个应用场景的最佳方式。分布式账本在防伪应用场景里有着中心化数据库无可比拟的优势❷。
- 智能终端。CryptoC14 为企业用户及消费者提供 WEB 应用，用户通过手机或桌面浏览器就可以进行真伪鉴定、申请加密权益证书、企业授权（生成 NFT）等活动。

3.2 挑战及解决办法

加密权益证书从概念到商用需要解决以下三个问题：

- NFT 与实体资产的绑定
- NFT 的生成、使用与管理成本
- 用户体验，可实施性

3.2.1 NFT 与实体资产的绑定

NFT 是实体资产的权益归属证明。NFT 由品牌企业利用自己的钱包密钥在区块链上锻造而成。每一个 NFT 都有一个独一无二的的 NFT 编号（NFT ID，例如 9990048413986158969）。NFT 通过将 NFT 编号附着到实体的方式绑定实体商品。NFT 编号只是起到一个指向的作用，真正的验证元素是保存在区块链上的 NFT。而 NFT 编号二维码标签主要是为了输入方便。NFT 与具有相同编号的实体资产形成了一对具有唯一性和独占性的资产组合。这个 NFT 编号我们称为防伪码。

注：NFT 编号及其物理载体并不具备排它性，任何人都可以将例如 9990048413986158969 这个 NFT 编号复制到他所偏好的任何物理载体上并呈现出来。但 NFT 的所有权需要它所在区块链钱包的秘钥来确认。这好比拥有房产证不等于拥有房产，拥有者要通过必要的身份确认才能证明拥有这个资产，才有交易的资格。

图 3 作为真正的验证元素，NFT 无法被克隆或伪造

如上图所示，造假者可以在物理实体以及防伪标签上做到完美仿制，但是加密权益证书 NFT 是储存于区块链上受到密码学保护的个体，它无法被克隆或仿制。获得正品 NFT 只有购买正品、通过回收以及窃取企业密钥三种途径。

窃取企业密钥：造假者与其买通品牌企业内部人员获得密钥，不如将精力花在仿制采用物理或者追溯技术的产品获利更有保障。品牌企业可以随时启用、作废密钥。并且还可以通过密钥分解加密技术，让生产部门及 IT 部门各掌握一部分加密后的密钥，而完整密钥是在计算机内存里动态复原。密钥分解加密技术既不会影响日常作业，也让日常作业员无法掌握完整的密钥。（当然企业还是要防范被植入恶意代码导出复原后的密钥。）

回收 NFT 是获得真品 NFT 的另一个方法。但是当一个供货商手里商品有大量回收的 NFT，那么消费者就需要谨防旧瓶新酒的造假方式，因为零星的退货不会导致单一供货商大量积累被回收的 NFT。NFT 是否经历回收会被应用发现，这在后文有详细描述。

作为比较，同为数据驱动类型的防伪追溯技术的防伪标签与溯源数据的组合并不具备独占性。只要复制了防伪标签里的防伪码，假冒品也同时获得了与数据库里真实的溯源信息的绑定。追溯技术缺乏内置的防伪逻辑，所以不得不采用缺点众多的统计防伪码被识读次数去判断真伪的办法。

3.2.2 NFT 的生成及使用成本

NFT 是区块链链上的一串数据，以加密资产的形式保存于拥有者的区块链钱包里。在适合的区块链平台上生成 NFT 并不会产生多少费用。事实上 NFT 的生成可以做到接近于零成本。NFT 是实体资产的权益证书，它本身并没有任何内在的价值。这就像房产证一样，房产有内在价值但是房产证并没有内在价值。证件的制作需要成本，但制作成本并不等于它具有内在价值。假设一个房地产证损坏了，花钱申请再制作一个副本就是。房产证的新旧以及是否原装并不会影响它所对应的房产的价值。一种例外是具有纪念意义的证书。例如某个历史阶段的第一本或者最后一本房产证，那么此时的证书本身具有内在的(收藏)价值。

数据采集是数据时代最大的成本组成部分之一。如何正确无误的将 NFT 转让给正品拥有者通常花费不菲。为了正确的转让 NFT，常见的做法是通过可信任第三方（trusted intermediary）收集的消费者信息，并正确的转让 NFT。授权企业将自己生成的 NFT 一层一层向下游转让，最后由零售商拥有。因为零售商直接面对消费者，所以能正确的将 NFT 转让给真正的消费者。这个过程与防伪追溯技术类似，需要供应链各个参与机构进行软硬件升级以及人员培训，初始投入很高。而且一旦发生 NFT 与实体资产异步流通就难以更正，因为每个 NFT 都是独一无二的，一旦发生流通异步，只能寄望无意获得 NFT 的钱包所有者归还 NFT，这种配合在实现中多数状况非常的耗时耗力。

CryptoC14 采用独家技术让 NFT 生成者（授权企业）与消费者直接建立信任，NFT 的转让不需要借助任何可信任的第三方进行。这样做不仅大幅减少数据采集的需求，也杜绝了数据造假的

可能。因为数据交换只发生在品牌企业与消费者之间，第三者没有机会介入，也没有机会造假。这个点对点传播信任的技术专利申请正在审核中，专利申请号 202010038768.3。

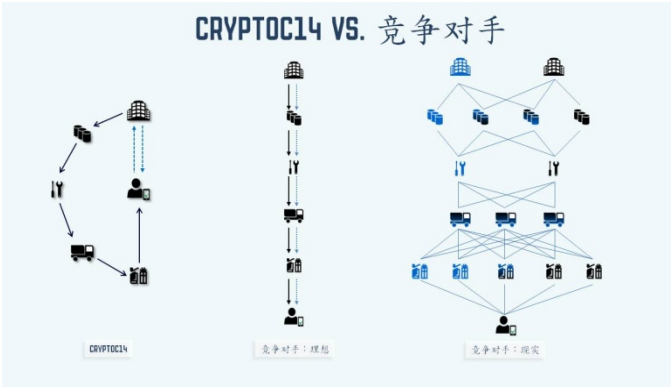


图 4 信任传递方式：点对点 vs. 链式的理想与现实状况

图左侧是 CryptoC14 的专利方法，这个方法不改变现有供应链流程，能最大程度的降低转换新技术的适配成本并杜绝数据造假。

图中间是理想状态下实体资产与 NFT 同步流通于一条可信任供应链上。

图右侧是现实中的供应“链”，一个配件能有几个供应商，同时向几个下游企业供货。NFT 的流通有无数多种方法与实体资产异步，从而导致隐藏成本上升。现实中数据网的带来的挑战。

3.2.3 用户体验

产品是否能成功很大程度上取决于用户体验。

消费者使用 CryptoC14.com 只需要扫描一个防伪码即能获得包括产品、授权企业、所有者、交易历史等数据以及最重要的购买建议。任何权益归属记录中的瑕疵都会导致应用发出警告，提醒消费者谨慎购买。见附图①②③。

消费者获得加密权益证书 NFT 只需要通过 APP 向品牌企业提供防伪码及注册码，企业官网核对无误后即会自动向消费者提供的区块链钱包地址转让加密权益证书 NFT。没有区块链钱包的消费者也可以通过 APP 实时生成一个新钱包⑥。

以上操作消费者只需要输入不超过三组数据即可在一、两秒钟内完成操作，而且不产生任何费用。整个过程比预约网约车或者订购外卖更便捷。消费者亦不需要编程、区块链或者物理/化学鉴定知识既能掌握。

消费者体验请访问：

http://www.cryptoc14.com/cn/index.html

以下是几个已经上链的防伪码，正品的加密权益证书由【演示企业】颁发：

- 9990048413986158969 - 已获生产授权并且已激活销售许可。
- 14980595911452706870 - 已获生产授权并且已激活，商品有召回记录。
- 9515666061890261866 - 已获生产授权但尚未激活销售许可。
- 16451992241381698202 -已获生产授权并且已激活销售许可，商品有已售记录。
- 8979558791471997978 - 曾经获得授权，但证书已被销毁。例如某藏品的完全损毁让拥有者决定销毁加密权益证书 NFT。
- 130725379765346402 - 未知钱包生成的 NFT，由于但无法伪造授权来源，所以不具备成为加密权益证书的资格。
- 1472173891428945831 - 错误的 NFT 编号，找不到相关记录。

品牌企业需要将授权令牌化，即为每件产品锻造一个 NFT。企业可以通过 CryptoC14 的【资产

管理】工具进行，激活或销毁 NFT 也可以通过这个界面进行。附图⑦⑧。作业员可以利用 CryptoC14 的 WEB 表格完成所以日常操作，无需编程知识。日常操作输入不超过三组数据即能进行批量处理，可以节省大量时间。

企业用户体验请访问：

http://www.cryptoc14.com/cn/issuance.html

目前提供能商用加密权益证书技术的公司只有 CryptoC14 和法国的 Arianee。Arianee 的分布式数据库基于以太坊开发，采用智能合约进行 NFT 的锻造、转让、销毁等操作。智能合约是一件商品一个 NFT，一个萝卜一个坑的逐步执行 NFT 操作。它的单页应用(Single page web applications) 全年 365 天/24 小时不间断运行可以执行 100 万笔 NFT 操作。因为一件商品必须有一次授权及一次转让的 NFT 操作。所以 Arianee 的单页应用一年最多只能给 50 万件商品提供防伪保护。CryptoC14 采用自主区块链公链以及 API 进行 NFT 操作，效率在 Arianee 的 30 倍以上。单页应用可达每年三千万笔操作。多个单页并行运行操作可以达每年 44 亿笔操作，即一条自主公链的理论上限。CryptoC14 会在适当实际启用更多的公链以提升并行处理能力。

有效使用和管理智能合约需要编程知识。当合约数量到达一定熵值之后管理需要投入的人力成本将大幅激升。而使用 CryptoC14 的应用作业员无需任何编程知识也能熟练掌握。同时可以结合传统数据库，电子表格这些办公环境常见的工具一起管理 NFT。这个两个特性使得普通知识储备的文员就能胜任日常操作，大幅降低企业采纳新技术的初期投资与营运成本。

3.3 弱点及隐患

任何技术都有弱点及隐患。加密权益证书技术的弱点及隐患表现在以下两个方面。

3.3.1 撞码

加密权益证书技术的编码通过计算得来，有一定的撞码几率。例如产生两个一模一样的防伪码。

CryptoC14 的防伪码是 64 个比特的十进制表达，大约是 20 位数的数字组合。64 比特撞码几率低于连中三个双色球头奖，撞码带来的不便可以忽略不计。防伪码需要附着到产品上，通常可供打印的空间不多。20 位数的防伪码即能保障极低的撞码几率，又不需要高精度的打印机即能胜任，同时还能保障很高的读码容错率。

CryptoC14 的注册码是品牌企业利用自己的密匙通过 AES-256 算法将防伪码加密得来。注册码需要打印的内容较多。但是因为注册码无需也不应该附着到产品上，而是以注册卡形式呈现给消费者，所以可以在不牺牲容错率的前提下预留出足够打印空间。企业也可以自行定义注册码的算法，进一步降低注册码的长度。

3.3.2 流程攻击

加密权益证书技术在消费者使用过程中分为购前鉴定与购后取证两个步骤。

购前鉴定：消费者在购物之前通过产品外包装或产品上附着的防伪码进行扫码鉴定，并根据应用的购买建议决定是否购买该商品。这个鉴定适用于消费者、执法者和供应链中所有下游企业。供应链中的下游企业可以视为上游企业的消费者，消费者对商品来源有任何疑虑的时候都应该进行购前鉴定。

购后取证：消费者拿到商品之后找到隐藏注册码，通过应用向品牌企业递交申请要求转让加密权益证

书 NFT。品牌企业解密注册码并与消费者递交的防伪码核对无误之后向消费者转让 NFT。

防伪码是明码，任何人都可以读取；注册码是暗码，只有支付以后才能获得。（参考刮刮乐，刮刮乐的兑奖号码也是暗码，只有付费之后才能刮去涂层获得。）正常情况下消费者不会购买状态更新为已售、遗失或损毁的商品，也不会购买没有涂层保护的暗码的商品。所以产品在销售许可被激活之后，以及完成转让权益证书前，造假者有一段时间窗口复制有效的防伪码，并争取在此期间将假冒品售出。

当然消费者拿到假冒品，在购后取证过程中还是会发现因为没有匹配的注册码所以无法获得 NFT。当每件正品都具备授权企业颁发的加密权证证书 NFT 的时候，无法获得 NFT 的商品就是未经品牌企业授权的商品，依照定义即是假冒品。此时消费者应向卖家发起维权，争取假一赔十。

消费者只要认真执行购后取证的操作，那么造假者的流程攻击就无法奏效。现实中消费者防伪扫码率极低。原因之一）传统防伪技术扫码并不能有效防伪，消费者对防伪码缺乏信心；原因之二）是否“正品”往往并不是消费者决定购买的主要原因，于是直接忽略真品鉴定。例如网红带货，让消费者做购买决定往往是因为人员而不是产品本身。

零售商与分销商应该承担更多的扫码鉴定的工作，它们也有必须这样做的理由：

1. 是否正品是进货的主要标准之一，卖家有足够的动力不以同样的进货价拿到假货。
2. 假一罚十的政策下，面对能百分百甄别出假冒品的加密权益证书技术，零售商与分销商都无法承受贩卖假货带来的惩罚。

另外品牌企业可以将加密权益证书与售后服务绑定，提高消费者获取 NFT 的意愿。即申请售后服务必须证明拥有相应的 NFT。这样做可以避免苹果被手机模型以及假 IMEI 号码欺骗造成损失事件的发生❸。

3.4 适用范围

加密权益证书技术使用任何品牌商品。也适用于个人创造，例如短视频、音乐小样、文本，当然也包括目前加密市场火热的美术作品。只是个人作品通常没有通用商品条码，所以原创者需要自行给作品编号，因为有了编号才能生成 NFT。加密权益证书同样可以运用到非实体资产上，例如新冠疫苗护照。

4. 防伪技术对比

加密权益证书技术可以理解为“一物一证”。对比物理防伪技术、防伪追溯技术，加密权益证书技术在有效性、安全性、便利性与成本上全方位领先。

防伪技术	物理防伪	防伪追溯技术（一物一码）	加密权益证明（一物一证）
可见验证元素	标签、材料、工艺…	二维码、RFID	二维码、RFID
不可见验证元素	-	溯源信息	NFT
鉴定工具	裸眼、专业设备…	手机	手机
专业知识	需要	不需要	不需要
可持续性	否	是	是
数据库类型	传统	传统、区块链	区块链
确定授权来源	不能	可以	可以
防伪造	不能	取决于生成方式	可以
防克隆	不能	不能	可以
防伪逻辑	陈旧无效	脆弱、负面效果	严谨有效
适配性	便利	困难	便利

图 5 物理 vs.追溯 vs.加密权益证书技术。（大图见附录）

下图是 CryptoC14 与同类产品竞争对手以及与传统的防伪追溯技术的比较。

防伪技术	权益证明技术			追溯技术
供应企业	CryptoC14	Arianee	Realitems	兆信、BATJ、3M
数据库类型	区块链	区块链	区块链	传统、区块链
个人隐私	匿名钱包	匿名钱包	绑定电子邮件	注册账号
可扩展性	便利	困难	困难	便利
编码生成效率	< 1 秒	~ 30 秒	~ 10 秒	< 1 秒
编码生成方法	API	智能合约	智能合约	自定义算法
适配性	便利	困难	困难	困难
标识独占性	有	无	无	无
用户体验	简便	复杂	复杂	复杂
数据采集方式	点对点	数据链	数据链	数据链

图 6 解决方案对比

5. 备注

❶ 有效记录虚假信息：是指数据由有效的账号写入数据库，但是写入的事件并没有真实发生。典型例子是假海外代购通过异地登陆物流系统，将没有发生的国外发货信息写入数据库。但真实的发货可能是在某个口岸城市，通过不诚实的节点将货物带入正常物流中。而物流系统往往只关注货物有没有支付运费，任务有没有完成，而不会关注货物进入物流系统的

时间和地点。对于已经支付但尚未完成的任务，物流系统会一直执行直到配送完成或被终止。

❷ 获得服务或者权限有以下两种方式：

A. 账号模式。用户需要完成账号注册才能获得相应权利。例如物流节点经过注册后获得物流数据库的写入的权利，用户账号认证是记录行为有效性的保障。另一个常见账号模式是微信支付、网络游戏、社交平台一类应用场景，用户同样需要注册才能进行操作。账号模式下用户在一定程度需要牺牲个人隐私，同时也面临隐私泄露的风险。
B. 令牌模式。邮票的使用是一种令牌模式。只要贴了邮票就能获得邮政系统提供的配送服务。像信件一类货物用户完全可以匿名进行。纸币与硬币的流通方式也是令牌模式。令牌模式使用便利，没有隐私泄露隐患，但容易受到假冒的攻击。

加密权益证书采用令牌模式。商品流通的全球性以及最终消费者的不可预知性，在加上日益受到重视的个人隐私保护，品牌企业没法做到为每一个产品去验证拥有者信息，并为拥有者设置一个账号。采用令牌模式加上区块链技术使得加密权益证书技术在不收集任何个人隐私的前提下也能保障权益的唯一性和独占性，并让所有者获得数据写入（区块）的权利。消费者拥有区块写入权利对于转让高附加值的收藏品交易尤为重要，因为涉及到在去中心化场景下更新所有权信息的操作。

❸ 苹果电脑手机模型欺诈事件

每个移动设备上都有一个 IMEI 号码，它是移动设备入网的必要条件。通过解析 IMEI 号码我们可以得知设备的授权企业、商品型号、保修期限等信息。

曾经有造假者利用免费的编码生成器生成有效的 iPhone IMEI 编码，然后将这个 IMEI 蚀刻到 iPhone 的模型上，最后以不能开机为理由向苹果申请退换。

手机模型具当然不能开机，但它的外观与手感与真机一模一样，苹果工作人员只能通过 IMEI 号码去核对保修信息。造假者利用这个方法成功的骗过了苹果客服，并对苹果造成 90 万美元的损失。而最后发现这个骗局的不是苹果电脑，而是美国海关。美国海关工作人员纳闷为什么有人进口那么多手机模型，因为在美国零售展台都是以真机在展示，而且美国本土并不生产 iPhone。那么大量进口 iPhone 手机模型的目的就值得怀疑了。

相关新闻链接 NPR。同样的欺骗手段在欧洲被重演了一次，受害者还是苹果电脑。

6. 附图 图中黄色高光部分由消费者输入。

①由商品条码获取的商品信息及图例

②加密权益证书的当前拥有者及授权企业信息

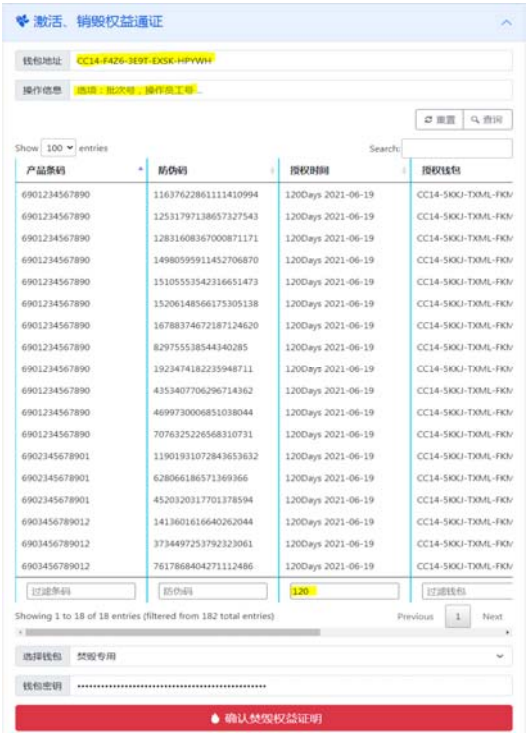
③应用根据权益调查结果提供的购买建议

④可提供与追溯技术一样完整的供应链信息

⑤区块链上未经解析的原始数据

⑥向授权者申请获得加密权益证书

⑦生成加密权益证书 NFT。黄色高光部填写内容分别是商品条码、作业员工号（选项）及授权数量。



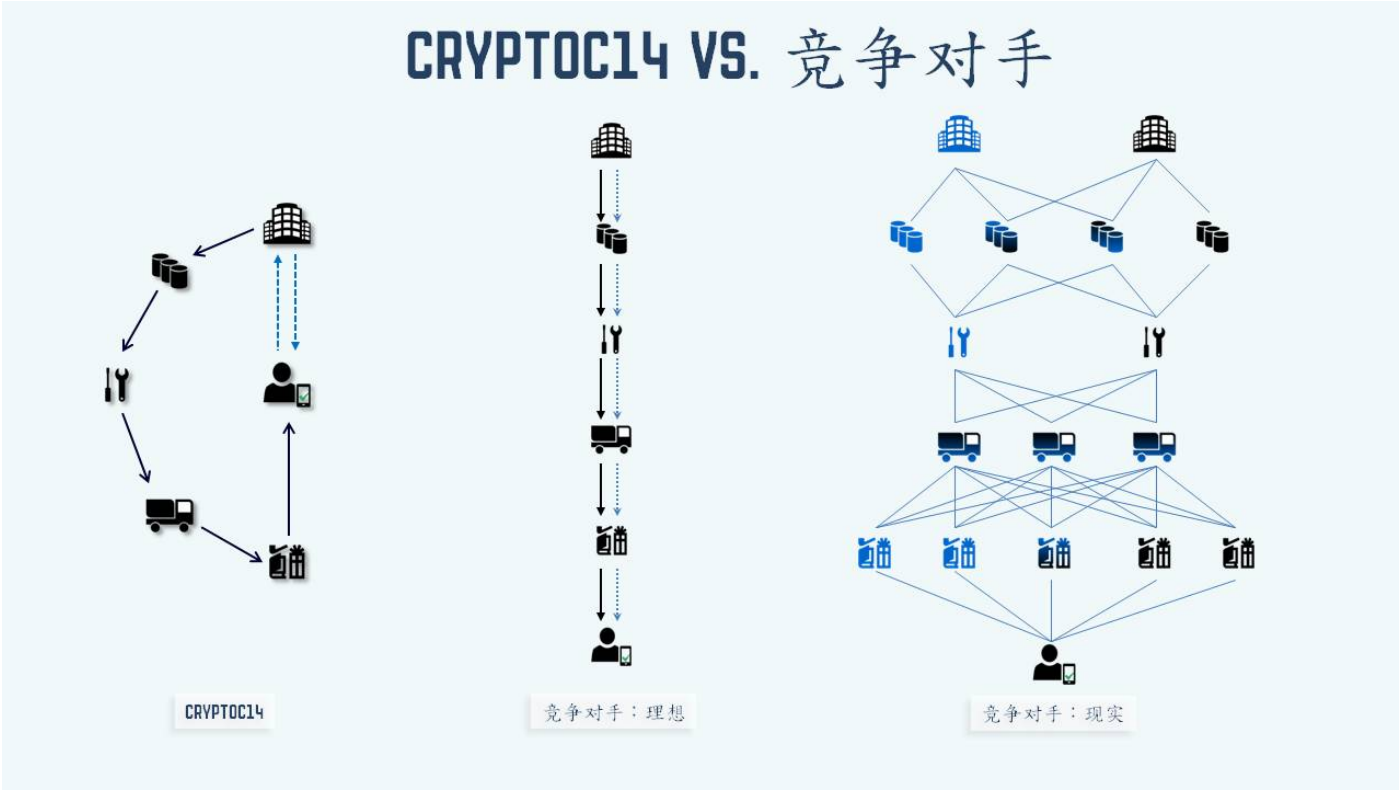
⑧图例中作业员根据企业操作手册将授权时间超过 120 天的加密权益证书 NFT 一批次销毁。销毁原因由企业制定，例如产品过期导致销毁。

验证元素并不能直接解析出授权来源，而是通过商品商标暗示，但伪造商标就是造假的基本手法之一。

复制的防伪码与原装防伪码指向同一套溯源信息。

物理实体与验证元素都很容易复制，但 NFT 无法复制或克隆。

防伪技术	物理防伪	防伪追溯技术 （一物一码）	加密权益证明 （一物一证）
可见验证元素	标签、材料、工艺…	二维码、RFID	二维码、RFID
不可见验证元素	-	溯源信息	NFT
鉴定工具	裸眼、专业设备…	手机	手机
专业知识	需要	不需要	不需要
可持续性	否	是	是
数据库类型	传统	传统、区块链	区块链
确定授权来源	不能	可以	可以
防伪造	不能	取决于生成方式	可以
防克隆	不能	不能	可以
防伪逻辑	陈旧无效	脆弱、负面效果	严谨有效
适配性	便利	困难	便利



点对点传输 vs.理想中可信数据链 vs.现实中的数据网

	权益证明技术			追溯技术
供应企业	CryptoC14	Arianee	Realitems	兆信、BATJ，3M
数据库类型	区块链	区块链	区块链	传统、区块链
个人隐私	匿名钱包	匿名钱包	绑定电子邮件	注册账号
可扩展性	便利	困难	困难	便利
编码生成效率	< 1 秒	~ 30 秒	~ 10 秒	< 1 秒
编码生成方法	API	智能合约	智能合约	自定义算法
适配性	便利	困难	困难	困难
防伪标签防复制	是	否	否	否
用户体验	简便	复杂	复杂	复杂
数据采集方式	点对点	数据链	数据链	数据链