(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109835084 B
(45)授权公告日 2021.07.16

(21)申请号 201711254446.7

(22)申请日 2017.11.27

(65)同一申请的已公布的文献号
申请公布号 CN 109835084 A

(43)申请公布日 2019.06.04

(73)专利权人 吴宁飞
地址 210036 江苏省南京市鼓楼区银城花园59号601室

(72)发明人 不公告发明人

(51)Int.Cl.
*B42D 25/36*(2014.01)
*B42D 25/405*(2014.01)
*B42D 25/318*(2014.01)
*B42D 25/21*(2014.01)
*B42D 25/22*(2014.01)
*B42D 25/23*(2014.01)
*B42D 25/29*(2014.01)
*B42D 25/24*(2014.01)

审查员 周文鑫

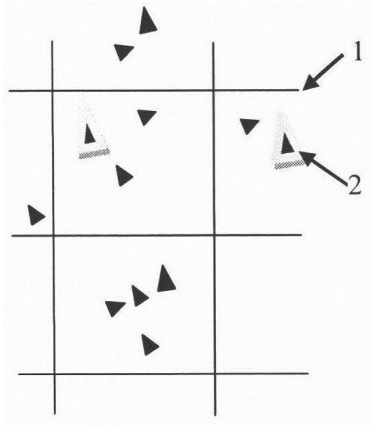
权利要求书3页 说明书41页 附图4页

(54)发明名称

新型防伪材料在防伪支付及货币防伪、银行卡等上的应用

(57)摘要

以往的防伪材料有一个致命缺陷:可能被仿制,对此我提出了1种新的防伪材料(不规则材料),它包含的信息量非常巨大,故难以完全复制。而验证时,只需对特定的位置进行查验,涉及的信息量较小,故易于操作。它不仅可用于商品的防伪,还可用于制造货币、银行卡、身份证件等。这种货币,数据不易灭失,远比目前的电子货币安全。这种身份证件,是线下验证身份的技术中最先进的。这种电子支付,采用真随机的口令,可抵抗量子计算的攻击。防伪支付指购买商品时,将货款的收款账号,确定为该种商品的真正的卖家的收款账号,则即使仿冒品被卖出,仿冒者也得不到钱,当然仿冒就无意义了。为防范一次性的仿冒,必须使用“不规则材料”。




CN 109835084 B

1.一种使用防伪材料的,鉴别商品的真伪与电子支付相结合的方法,其特征是,其步骤是:

代卖家完成商品的真伪鉴别的工作的支付平台,依序确定防伪码编号b,并针对该编号生成真随机的防伪码J1,加密为防伪码的密文J2;

所述的代卖家完成商品的真伪鉴别的工作的支付平台,找出一定数量的难以完全复制的防伪材料,随机确定查验位置,得出查验结果,记录所述的难以完全复制的防伪材料的编号x、查验位置、查验结果,并将该防伪材料的编号x与一定的防伪码编号b对应;将防伪码编号b、防伪码的密文J2、防伪材料的编号x复制到存储防伪信息的U盘中,记录U盘的编号及其中包含的防伪码编号b、防伪材料的编号x的范围,再派人将存储多个防伪码编号b、防伪码的密文J2、防伪材料的编号x的U盘,及相应的所述的难以完全复制的防伪材料,以线下的途径送至服务站,让各卖家派人领取U盘、所述的难以完全复制的防伪材料;卖家收到所述的代卖家完成商品的真伪鉴别的工作的支付平台送来的U盘后,工作人员将所述的存储多个防伪码编号b、防伪码的密文J2、防伪材料的编号x的U盘与设在卖家处的用于联系的终端连接,将数据载入,通过设在卖家处的用于联系的终端回传U盘的编号;

所述的代卖家完成商品的真伪鉴别的工作的支付平台,生成向所述的代卖家完成商品的真伪鉴别的工作的支付平台发出的用于表明买家身份的真随机的口令mk,并依序确定其编号,将口令mk及其编号复制到存储口令mk的U盘中,记录U盘的编号、U盘的包装的编号及其中包含的U盘的编号的范围,再派人将其以线下的途径送至服务站;服务站的工作人员将所述的存储口令mk的U盘与服务器连接,将数据载入;

买家在进行电子购物时,使用其手机或电脑,通过专用的软件登录到由用于控制防伪活动、支付活动的中央服务器提供或认可的购物平台,在所述的由用于控制防伪活动、支付活动的中央服务器提供或认可的购物平台上,提交要购买的商品的类别、用途,及商品的商标、商品名称、商品的规格、公司的名称、公司的地址方面的信息;

该购物平台返回一个该类别的商品的列表,其中列出相似的商标、商品名称、公司的名称,及产品的介绍、公司的地址、联系方式、卖家的用户名;

该买家根据该列表,确定其要购买的商品的卖家的用户名,再直接在该购物平台上针对该卖家的用户名提交订单;

买家提交订单后,该专用的软件记录商品的名称、商标、卖家的用户名、规格、款式、金额、单位、数量;

所述的用于控制防伪活动、支付活动的中央服务器收到订单后,对订单进行审核,若通过,向所述的代卖家完成商品的真伪鉴别的工作的支付平台发出划拨定金的指令,若该买家的用于完成防伪支付的账户内的资金不足,通知买家充值;

完成定金的划拨后,所述的代卖家完成商品的真伪鉴别的工作的支付平台,在该所述的设在卖家处的用于联系的终端当前未用的防伪码中,随机确定一个防伪码编号b,随机确定一个订单号H1并加密为密文H2,相应确定所述的难以完全复制的防伪材料的编号x,并将防伪码编号b、订单号的密文H2返回所述的用于控制防伪活动、支付活动的中央服务器;

所述的用于控制防伪活动、支付活动的中央服务器收到上述信息后,将订单信息及该防伪码的编号b、订单号的密文H2、及定金已支付的信息,发往所述的设在卖家处的用于联系的终端;

所述的设在卖家处的用于联系的终端收到订单信息后，检查商品的价格，若与预先设定的价格相符，向相关部门发出通知，找出、生产出、购进商品，若与预先设定的价格不符，提出异议；

在发出该商品时，所述的设在卖家处的用于联系的终端，根据收到的防伪码编号b，从U盘中调出数据，确定该商品使用的防伪码的密文J2，及所述的难以完全复制的防伪材料的编号x，将防伪码的密文J2加密为防伪码的密文J3，将订单号的密文H2 加密为订单号的密文H3，并在发货时，将防伪码编号b、防伪码的密文J3、订单号的密文H3、服务站的编号N、卖家的用户名C、买家的用户名Y打印在标签上，将相应的所述的难以完全复制的防伪材料置于包装上或交付物流公司；同时所述的设在卖家处的用于联系的终端，将防伪码编号b、商品的编号，加密发往所述的用于控制防伪活动、支付活动的中央服务器；

商品送到服务站后，由服务站的工作人员对商品进行检查，若该商品的买家的用户名Y，确实是该服务站所服务的买家的用户名，根据用户名，从服务器中调出相应的用户的手机号，将商品的种类、价格、卖家的用户名，附上一个流水号，加密发往该买家的手机；

买家的手机上的软件，将其与记录进行对比，并给出对比结果，如果对比结果是“该订单信息与记录相符”，同时显示“确认订单并开始验证”的按钮，如果对比结果是“该订单信息与记录不符”，不显示“确认订单并开始验证”的按钮，显示“否认订单”按钮；

如果对比结果是“该订单信息与记录相符”，买家在手机上点击“确认订单并开始验证”，手机向所述的用于控制防伪活动、支付活动的中央服务器发出验证请求信息，否则点击“否认订单”按钮，中止流程；

所述的用于控制防伪活动、支付活动的中央服务器收到该验证请求信息后，生成一个挑战请求，向买家的手机发出；

买家的手机，收到所述的用于控制防伪活动、支付活动的中央服务器发来的挑战请求后，生成一个真随机的A挑战值，将其发往所述的用于控制防伪活动、支付活动的中央服务器，同时，买家的手机由A挑战值也生成一个A应答值；

如果所述的用于控制防伪活动、支付活动的中央服务器收到二个或更多个不同的A挑战值，则向买家的手机发出“有敌手在攻击”的提示信息，并中止流程；

所述的用于控制防伪活动、支付活动的中央服务器收到A挑战值后，进行加密而生成一个A应答值，并发往该买家的手机；

如果买家的手机收到的所述的用于控制防伪活动、支付活动的中央服务器发来的A应答值，与A应答值不同，或收到二个或更多个不同的A应答值，则向所述的用于控制防伪活动、支付活动的中央服务器发出“有敌手在攻击”的信息，所述的用于控制防伪活动、支付活动的中央服务器收到该信息后，向相应的服务站、卖家发出“有敌手在攻击”的信息，向该手机发出“已中止流程”的信息，并中止流程；

如果所述的用于控制防伪活动、支付活动的中央服务器只收到一个A挑战值，也没有收到买家的手机发来的“有敌手在攻击”的信息，所述的用于控制防伪活动、支付活动的中央服务器向该买家的服务站发出包含上述的流水号的“开始验证”的通知信息；

服务站收到“开始验证”的通知信息后，由工作人员打开包装，找出防伪码标签，将防伪码编号b、防伪码的密文J3、订单号的密文H3录入服务器，服务器将订单号的密文J3加密为订单号的密文J4，将防伪码的密文H3加密为防伪码的密文H4，将防伪码编号b、防伪码的密

文J4、订单号的密文H4一起加密发往所述的用于控制防伪活动、支付活动的中央服务器，该中央服务器再将其转发给所述的代卖家完成防伪码验证的工作的支付平台；

由所述的代卖家完成防伪码验证的工作的支付平台完成防伪码编号、防伪码、订单号的验证，并向所述的用于控制防伪活动、支付活动的中央服务器返回验证结果，若验证通过，还同时向所述的用于控制防伪活动、支付活动的中央服务器返回相应的所述的难以完全复制的防伪材料的查验位置，该中央服务器再向相应的服务站转发该查验位置；

服务站收到查验位置后，得出查验结果，并返回所述的用于控制防伪活动、支付活动的中央服务器；

所述的用于控制防伪活动、支付活动的中央服务器再将其转给所述的代卖家完成防伪码验证的工作的支付平台；

所述的代卖家完成防伪码验证的工作的支付平台，根据记录进行验证，若验证结果是“通过”，所述的代卖家完成防伪码验证的工作的支付平台根据相应的订单的卖家的用户名，转换出该卖家的收款账号，并划拨余款及物流费用、代理费用；

若支付成功，所述的代卖家完成防伪码验证的工作的支付平台向所述的用于控制防伪活动、支付活动的中央服务器返回支付成功的应答，否则返回支付不成功的应答；

所述的用于控制防伪活动、支付活动的中央服务器收到支付成功的应答后，向相应的服务站返回上述的验证通过、支付成功的应答，也向相应的所述的设在卖家处的用于联系的终端发出上述的验证通过、支付成功的应答；

该服务站收到该应答后，向相应的买家传达该应答，并与买家约定送货时间、地点，录入服务器；

派出送货员前，由服务站的服务器，针对每一件商品随机生成用于确定买家的身份的验证码、开锁的密码；

服务站的工作人员再根据情况，人工指定送货员的编号、密码箱编号；

服务站的工作人员再调出相应的用于确定服务站的身份的口令，并打印出来；

服务站的工作人员再将货物，及打印出的相应的所述的用于确定服务站的身份的口令的纸质文件，一起锁在密码箱中，并根据服务器的指令，设定开锁的密码；

由服务器将所述的用于确定买家的身份的验证码、送货员的编号、密码箱编号、密码箱的开锁密码，一起发往相应的买家的手机；

送货员见到买家后，先出示标有送货员的编号的工作证，买家根据收到的送货员的编号，核实送货员的身份；

买家核实送货员的身份无误后，送货员再请买家出示所述的用于确定买家的身份的验证码、用户名、证明身份的证件，来核实买家的身份；

核实买家的身份后，送货员向其递交相应的密码箱，买家核实密码箱的编号后，用收到的开锁密码打开密码箱，用其手机扫描所述的用于确定服务站的身份的口令，进行核实，若该口令无误，再对货物进行核实，若货物无误，用手机生成一个用于表明送货工作已完成的验证码，由买家用手机将该验证码发往相应的服务站，也将其告诉送货员；

送货员回到服务站后，将用于表明送货工作已完成的验证码告知工作人员，如果其与记录相同，系统确认货物已送到。

# 新型防伪材料在防伪支付及货币防伪、银行卡等上的应用

## 技术领域

[0001] 本发明，涉及商品的防伪技术，与电子支付技术，以及货币防伪、银行卡防伪、身份的鉴别技术。更具体地说，是1种商品的防伪与电子支付相结合的技术和装置，以及使用不规则材料的货币防伪、银行卡防伪、身份鉴别技术。

## 背景技术

[0002] 以往，电子支付技术、防伪技术这2个领域内的技术人员，通常认为电子支付与防伪是2个不同的技术领域。电子支付有很多优点，如成本低、方便、到账迅速等，但最大的问题是安全性差。现在很多人不接受电子支付，主要原因之一就是其安全性不够。现在用户在很多支付平台上操作时，使用的口令都是固定(静态)的，这种口令很容易被盗。网银支付通常要使用U盾，其口令是动态的，但这种口令是使用特定的算法、密钥得出的，不是真随机的，故理论上也是可破的。而以往的电子支付所使用的密钥也常是固定的，这也是可能被破解的。电子支付在给人们带来方便的同时，也给不法分子带来了盗窃的便利，现在对电子支付的安全的最大的威胁来自网上。如何在给人们带来方便的同时又提高安全性，成了该领域的1个重要课题。

[0003] 现在量子计算的技术发展很快，一旦量子计算获得成功，破解密钥的速度将大幅提高，目前的大部分的密码体制都将是不安全的了，这引起了整个领域内的忧虑。这时就只有一次一密的密码体制，或是密钥的使用次数很少的密码体制，才可能保证安全。一次一密是最高级别的加密，在密码学中它被称为是完善保密的，即无法破解的。在支付中使用真随机的口令虽对口令的破解具有很好的防范效果，但最大的问题是：这种口令无法在异地用其他的硬件产生(以往称之为“同步”)，故只能通过网络或线下的途径传递。通过网络传递安全性较差，而简单地通过线下的途径传递成本较高难以实现。

[0004] 现在市场上有很多假货，这损害了消费者、生产商的利益，防伪工作对提高真实商家的效益是非常重要的。要鉴别商品的真伪，最可靠的方法，是对商品的物理特性、化学特性等进行考察，但这往往不仅麻烦、方法复杂，要耗费很长时间还成本较高，故并不常用。此外我们还可通过商品的包装等实体、防伪码(俗称为“电码”)等来间接地鉴别商品的真伪。使用包装防伪成本较高，但包装也还是容易仿冒的。而以往的防伪码技术虽成本较低，但更容易仿冒。

[0005] 而以往很多情况下防伪码是根据商品的序列号等数据通过特定的加密算法算出的，这就不需有较大的数据库，成本较低，但敌手若花费较长的时间，经过多次的运算，是可能破解的。而以往也有很多防伪码公司的内部人员，泄露加密算法、密钥的事情发生。

[0006] 而即使商品有真实的防伪标签也未必是正品，防伪标签是生产商为区别于仿冒产品而做的参照物，防伪标签能够证实该产品是这家企业生产的，但质量取决于该企业的质量管理。

[0007] 以往防伪技术与电子支付技术通常是分离的，人们认为它们是2个不相干的技术领域，但实际上它们是紧密相关的，在以往的传统的线下的贸易中，买家往往要在验明商品

的真伪后才肯付款，而在以往的电子支付中由于买家、卖家常相隔较远，故难以查验商品的真伪，故支付与防伪是分离的。若在付款前不能确定收到的货物的真伪，就不能很好地维护消费者的利益。

[0008] 防伪与电子支付的结合以往也有，但较简单，如CN102129637A基于安全机制的商品防伪方法，它实际上只是简单的拼凑，其中的安全隐患非常多，未将它们结合并发挥其益处。其收款账号的确定较简单，是由买家直接在网上提交，也没有严格的确认的环节；即使采用手机、电脑进行加密，其密钥也常常是固定的；而买家在支付平台上使用的口令也常常是固定的。而其付款账号也直接由买家在网上提交，手机、电脑，加密的密钥也常常是固定的。而这种方法的最容易攻击的弱点之一是在生产商完成防伪码的验证后，对验证结果的回传，敌手很容易伪造这种验证结果。这种方法中防伪与支付的结合较简单，仅是买家在看到POS机上显示商品为真品后，人工通过支付平台进行支付(提交、确认收款账号、付款账号)。

[0009] 现在手机、电脑上的软件常是直接在网上下的，而这些软件可能加入了非法程序并不可靠，而手机、电脑上也可能感染木马病毒等，使账号、口令等泄露。而POS机也可能感染木马病毒、安装不可靠的软件，这可能是被动造成的也可能是由安装POS机的商店所做的手脚。

[0010] 现在很多电码是通过生产商自己完成验证的，这可减少数据库的建设、维护等费用，防伪码不需线下传递，直接由生成防伪码的服务器验证防伪码，验证成本较低，但其安全性较低。而防伪码也可不由生产商生成防伪码，由防伪中心生成，这就不存在完成防伪码的验证后再将验证结果回传的环节，防伪码在整个使用的过程中是以明文的形式不变地存在的，容易泄密。

[0011] 此外以往的货币、银行卡、身份证，也有很多不足，这也可用1种新的防伪材料来解决。

## 发明内容

[0012] 发明内容分为防伪支付简述、防伪支付详述(包含对不规则材料的介绍)、货币、银行卡等多个部分，以下分别叙述。

[0013] 1.防伪支付简述

[0014] 1.1防伪支付

[0015] 以往，防伪技术，与电子支付技术，通常是2个不相干的技术领域，但将这2个方面的技术结合起来，这不只能维护消费者的权益(让消费者在确认商品的真伪后再付款)，还会产生很多的益处。这种防伪与电子支付相结合的支付方法，以下简称为“防伪支付”。确切地说，这不仅是1种支付的技术，也是1种防伪的技术，正因为是将防伪与支付相结合，它才会有下述的诸多益处，故既不能说它是1种支付技术，也不能说它是1种防伪技术。若将防伪与支付割裂开来，那么它的很多益处也就随之消失了，故其实它是1种新的概念的事物，1种以往没有的新的类型的技术，1种跨界的技术。但将商品的收款账号确定为特定的账号是1种商业方法，可能不能被授权，我提出的是提高防伪支付的安全性的方法。

[0016] 将电子支付与防伪结合可减少仿冒行为：在商品流通的过程中我们难以保证商品的唯一，对于同样的商品的序列号(以下也称为编号)、防伪码，相应的商品是可能被调换

的。但支付的唯一却是能做到的，我们可将特定的商品(特定的编号、防伪码的商品)的货款的收款账户，限定于特定的卖家的账户，这样支付就是唯一的。这样即使仿冒的商品被买家购买，货款也不能到达仿冒者的账户，这样仿冒就无意义了，故这可从根本上禁绝仿冒行为。以往的直接的防伪方法难以完全保证商品是真品，但通过电子支付来间接地防伪，效果好得多。这样通过电子途径购买商品，其真伪的可靠性就将远超过通过以往的实体的商店所买的商品。以往电子商务，尤其是网络拍卖等，被很多人不信任，但现在情况可以改变了。本发明主要针对网络购物，也包含针对线下购物的方法。

[0017] 而电子支付与防伪结合后，支付会更安全。电子支付的开始，往往是确认主体的身份，以往我们使用电脑登录支付平台，开始往往要输入(静态的)密码(密码学中称为口令)。而使用网络银行，往往要使用U盾，U盾也会发出口令，而这种口令是动态(变化)的。而我们可将防伪信息(防伪码等)，也作为支付的验证元素(口令、密钥)，而这种口令(防伪码)是一次一密级别的，其安全性远超过现有的电子支付技术，可抵抗量子计算的攻击。现在有的支付技术，将人脸、指纹等也作为验证元素，但实际上这些验证元素是静态的，也是容易复制的，只不过复制的难度大一些，其安全性远没有这种一次一密级别的支付技术高。以往电子支付中使用的口令、密钥，与收款账号、付款账号是不绑定的，故只要破解了口令、密钥，黑客就可随意地盗取资金。

[0018] 而采用了包装、包裹作为载体，口令、密钥就能随商品一起被运输，其传递口令、密钥的成本几可忽略不计，上述的一次一密的口令、密钥的传递困难的问题，就得到了解决。这种防伪码与支付的结合，是以往没有的。采用这些措施的成本，非常低，而攻击的成本却非常大，对于普通的商品进行攻击是根本不值得的。

[0019] 我曾提出1个名称为“1种通过专用的服务机构完成的电子支付系统与方法”的专利，它采用包裹来传递一次一密的支付口令，这是我提出本专利的基础，但其中的口令只用于支付，没有防伪的功能，它们之间有着本质的区别，且只采用了1个真随机的动态口令，较简单。

[0020] 而仅将防伪与支付结合在一起还远远不够，为提高安全性我还提出了下述措施：以往的防伪码常只和防伪码的编号捆绑(结合在一起进行验证)，防伪码标签可随意贴在任1商品上，但我们的防伪码，是与订单号、服务站号(线下的服务网点的编号)、编号等捆绑的，若有人将防伪码盗用在其他的商品上，就无法通过验证。即使防伪码被丢弃，也不怕别人盗用。以往的防伪与电子商务的结合不紧密，故不能与订单号、服务站号等捆绑。而这不仅是使验证信息的信息量增加，买家的用户名、服务站号等是会被买家、服务站(线下的服务网点)的人员亲自进行确认的，故很可靠。防伪码、防伪码的编号、商品的编号，都是可随便复制、更改的，而这些信息，买家、服务站难辨真伪。

[0021] 而在完成主体的身份的验证后，以往的电子支付的主要任务就是加密，主要是对收款账号、金额加密，这是要防止敌手篡改收款账号、金额。以往收款账号常是由买家个人提交给支付平台、银行的，而个人的力量是很单薄的。对此可由联控中心确定收款账号，即由卖家的用户名进行转换。而这种收款账号是不公开的，这样人们不能直接查询到它与用户名的关系。而买家确定卖家的用户名，是在特定的购物平台上完成的，而这种购物平台可根据买家提交的商品的种类、商标、用途等，列出真实、可靠的卖家(生产商)的列表，如此确定卖家的用户名可大幅减少卖家的仿冒。而这种卖家的用户名(及收款账号)，是在订购商

品的一开始就确定的，而以往的商品的销售，往往会经过多个环节，买家很难对大量的中间商的真伪做出分辨。而以往的实体的商业模式中中间商的数量更大，人们对这些中间商就更难辨真伪，只有采用电子商务才能在订购的开始就确定生产商，将防伪码与收款账号等绑定。以往人们对电子商务中的中间环节少，只知道这可降低成本、提高周转速度，而很少意识到这对防伪的作用。

[0022] 这种确定收款账号的过程分多个步骤：先由买家提交自己要购买的商品的用途、种类、商标等信息；再由特定的购物平台提供可靠的卖家的列表；再由买家确定卖家的用户名；提交订单后，卖家依照订单生产并将商品交付给买家；买家在收到商品时，对商品种类、卖家的用户名等进行核对，若他的确订购过该商品，通过其手机或服务站的设备，发出“真随机的防伪码”，以对卖家的用户名等进行确认；联控中心等再通过卖家的用户名转换出相应的收款账号。

[0023] 若买家订购过的商品较多，他可能记不清他订购过哪些商品及其金额等，这会使确认遇到困难，较可行的解决方法是：买家在手机或电脑等上安装相应的软件，订购商品的操作通过该软件在其手机或电脑上进行，确认订单后该软件记录商品的名称、商标、卖家名、金额等信息，商品送到服务站后，服务站向相应的买家的手机或电脑发出商品的信息，买家的手机或电脑上的软件，将其与记录进行对比，并给出对比结果(相符或不符)，买家根据该对比结果再确认订单、否认订单，由手机或电脑发出确认信息。为提高安全性，手机上记录的订单信息不能通过网络来访问，提交订单后订单信息不再输出，只输出对比结果，且只在对访问的主体(服务站或联控中心)的身份的验证通过后，才输出对比结果。

[0024] 这是通过1个系统来确认、转换出收款账号，虽较复杂但更可靠，也给消费者带来了区分卖家的方便，而以往没有这种帮助买家确定收款账号的系统是以前没有的。以往没有人用防伪码作为口令，也没有人用真随机的口令来完成支付。防伪与电子支付的结合以往已有，但它们的结合很不紧密，人们还没有深入地挖掘将它们相结合的益处，更没有在提高安全性上提出有效的措施，为提高支付的安全性、提高防伪工作的效果，我提出了以下的改进。

[0025] 1.2系统组成

[0026] 我提出了几种更完善的系统：我们设立1个控制防伪活动(验证防伪码、不规则材料等的活动)、支付活动的中央服务器(以下将该中央服务器及其管理机构简称“联控中心”)，它可包括支付平台(这样信息传递更直接，故安全性较高)，或与银行的服务器物理上相连(这样信息传递也较直接)，而由于支付牌照、投资等限制，通常它不包括支付平台。此外还需设立多个线下的服务网点(以下简称“服务站”，按照习惯服务站的主服务器也简称服务站)，用于完成各种事务。对于不会电子购物、电子支付的用户，服务站也可替他们完成电子购物、电子支付。这些鉴别商品的真伪、递交商品的服务站，与联控中心共同形成了1种新的商业服务体系。

[0027] 而目前很多单位没有自己的服务器、网站，无法自行完成防伪码的验证，我们可为它们提供代理服务(联控中心可向它们收取一定的代理费用)，即在联控中心外再增加1个用于代卖家完成防伪码、防伪材料(尤其是不规则材料)的验证等工作的模块，以下简称“代理模块”。再在卖家处设立用于联系的终端(用于接收订单、验证通过的通知、及对防伪码进行加密等的终端)，以下简称通知端。为便于区分，可将联控中心与代理模块等组成的整体，

称为“管理中心”。但在不会引起歧义的情况下，可将联控中心、管理中心，都简称为“管理中心”。当然有的单位有自己的服务器、网站，可自行完成防伪码的验证，对于这样的单位我们也可为他们提供防伪、支付的服务，不需使用代理模块，这种单位自己的服务器以下简称卖家端。

[0028] 任何个人要通过联控中心来验明商品的真伪、完成货款的支付，要在服务站通过线下的途径注册用户名(以下简称为个人名)，使用个人名(不用姓名)可防止隐私及支付账号的泄露，它必须是唯一的。它最好由服务站指定，这样不易重复、号码的位数较少。而用户在网上订货时，还需提交其服务站号，而服务站号是联控中心确定解密、加密的密钥的依据。

[0029] 任何单位要销售商品及通过联控中心来验明商品的真伪、完成支付也需注册用户名，以下简称单位名。单位名与公司名称不同，公司名称往往有很多个字，叫起来、输入麻烦，还易出错。各单位要向联控中心提交相关资料、通过审核，才能获得联控中心指定的单位名。单位名可用字母、汉字等来组成以便于分辨，而由数字组成不易分辨。使用单位名也有利于防止支付的账号的泄露。此外，买家的用户名，以下简称为买家名，卖家的用户名，以下简称为卖家名。而同1个单位，有时是卖家有时又是买家，故对于卖家、买家，我们可能不能区分他们是个人、还是单位，这时个人名、单位名都统称为用户名。

[0030] 当然我们也可在支付平台上增加这些功能(生成真随机的防伪码、密钥，及代卖家完成防伪码、防伪材料的验证等)，这种支付平台以下简称代理平台。以往电子商务网站进行支付时，常采用强加密的方法向支付平台发出支付指令，这不仅成本高还易被攻击。若由联控中心向代理平台发出真随机的口令(即防伪码)，这不需采用强加密的方法，不仅成本低还安全。使用代理平台完成防伪支付，比使用代理模块完成防伪支付更先进。

[0031] 当然我们还可再进一步，将代理平台与自有平台乃至于联控中心整合成1个平台，这样买家提交了订单后，自有平台可将订单的流水号，直接传输给代理平台，代理平台再根据流水号确定订单号(它是确定订单信息的重要依据)。这样订单的流水号，就可不暴露在公共网络上，敌手无法得知流水号、订单号，就无法伪装出合法的验证信息、盗取资金。这些功能分别由不同的模块完成，而这些模块都在物理上相邻，这就可省去联控中心与支付平台之间加密传输信息的环节，不仅能降低成本也可提高安全性。这种平台我称为综合性支付平台，简称综付平台，但建设综付平台投资较大，而仅将支付平台与代理模块进行整合较易，以下的论述主要针对代理平台而展开。而对每1个环节采用真随机的密钥进行加密的方法，可很好地保证安全。

[0032] 而在服务站中可能工作较繁忙，仅有1台电脑不能满足需要，对此可采用这样的局域网：设立1个主服务器，它与外界以有线或无线的方式连接。此外还采用若干台电脑，它们与主服务器以有线的方式连接，而不能直接与外界联系，每1台电脑都只负责特定的1种或多种任务。它们分为2类，1类负责买家的注册、收取包裹等较简单的任务，以下简称辅机。负责收费、录入交货时间、确定送货计划等较重要的任务的电脑，以下简称主机。各台主机、辅机的任务可由主服务器指定，如指定某1买家到哪1台辅机领取包裹。在这种局域网中主机、辅机都只是终端，而不是中心，其中的中心只有主服务器1台计算机，这样各计算机间易协调。在工作量较少时可只设1台主机，且也完成上述的主服务器的工作，即主服务器也是主机。服务站的工作人员以下简称柜员，操作主机的柜员以下简称主柜员，操作辅机的柜员以

下简称辅柜员。

[0033] 现在的防伪码应用有很多不足，有防伪标签的物品也未必是正品，防伪标签能证实该产品是这家企业生产的，但它生产的可能是伪劣产品。消费者常相信知名商标的商品，但现实生活中假冒的网站、卖家经常出现，让消费者防不胜防，仅凭防伪码还不足以证明商品的真伪，对此我提出了以下方法：联控中心提供1个购物平台或采用1个联控中心认可的购物平台，以下简称“自有平台”，该平台可与联控中心直接在物理上相邻，也可与联控中心距离较远。该平台包含1个专用的数据库，该数据库仅保存通过联控中心的认证的、可靠的卖家的名称(包括用户名、公司名称)，及其提供的商品的商标、名称、规格、用途及电话、地址等信息。以往的购物网站上，有很多的网络商店，而消费者是很难知道这些网络商店是否是可信任的。自有平台上通常只允许生产商和可靠的经销商销售商品，这样中间商的数量较少，这给消费者选择卖家带来了方便。以往在实体商业中同1种商品的经销商成千上万，故人们难以判断经销商的真伪。而在以往的电子商务中，同1个购物平台上销售同1种产品的网络商店，也如同大海般数量众多，这当然也会让消费者难辨真伪。我们也允许网络商店在自有平台上经销商品，但只有通过认证的网络商店才能在自有平台上销售商品，且严格控制其数量，在自有平台上也会明确标出这些卖家是网络商店而不是生产商，减少卖家的数量会给消费者选择卖家带来很大便利。自有平台上也允许较大型的商业企业经销某些类别(如化妆品、日用品等)的多种商品，消费者对一些大型的商业企业较信任，通过他们来选择商品是较可行的。以往的购物平台常简单地允许人们在其上开设网络商店，而对这些网络商店经销的商品不进行严格的检查、任其自生自灭，这是不当的，若不能为消费者提供更完善的服务，就会被消费者抛弃。

[0034] 买家在该平台上，可输入商品的用途、商标、名称、规格、卖家名等，进行搜索、选择后，直接在该平台上提交订单，该平台将订单转给联控中心，联控中心再根据卖家名，确定相应的卖家的联系方式等，将订单以可靠的方式(如加密发往通知端)告知该卖家。卖家收到订单后开始生产、发货。卖家收到订单后，可检查商品的金额，若低于预先设定的价格，可提出异议。

[0035] 这个平台掌握与商标、商品名称等相应的正确的卖家的名称及联系方式，这可防止假冒的卖家用类似的卖家的名称(尤其是网络商店、网站的名称)、及商标等来欺骗买家。为便于买家准确地分辨某1商品的生产商的真伪，可采用以下方法：首先买家在该平台上提交要购买的商品的类别，及商标、商品名称、规格、公司的名称、公司的地址等方面的信息；该平台再返回1个该类别的商品的列表，其中列出相似的商标(例如珠宝行业的老凤祥、宝凤祥，醋的恒丰、恒顺等)、商品名称、公司名称，及产品介绍、公司地址，为便于分辨真伪可对各卖家公布其销量、销量排名、好评数、好评率、差评数、差评率等，并可按销量、好评率、差评率等排序(销量较大的卖家通常是真实的卖家，而仿冒者的销量通常较少)；该买家再根据该列表确定其要购买的商品的卖家名，再直接在该平台上针对该卖家名提交订单(通常可在该卖家名后设1“加入购物车”按钮，买家点击该按钮即可进入订单编辑页面，再完成提交订单的各项操作)。

[0036] 我们对于同1种商品列出相似的多个商标，及详细的厂家、产品的介绍等，这便于买家进行分辨，不易被仿冒的商标欺骗。通过商标来确定卖家是很可靠的，商标法规定，未经商标注册人的许可，任何人都不能侵犯注册商标的专用权，在自有平台注册的卖家都需

提交营业执照等证件，而销售同1个商标的商品的代理人(卖家)，若不能提交商标注册人的许可材料，自有平台都不会允许其进行注册。而自有平台对同1生产商的代理人的数量，也有严格限制。

[0037] 而上述的方法，不能对自有平台之外的购物平台(以下简称“非自有平台”)所销售的商品，提供防伪、支付的服务，为便于向非自有平台提供防伪、支付的服务，我又提出了以下的方法：买家在非自有平台上选择知名的商标的商品，确定购买的商品的商标、卖家、商品名称、金额、数量等信息后，向平台确认订单，该网站再向该买家的邮箱(可由联控中心提供)发出经过编辑的订单信息，买家查看订单信息，对商标、卖家的名称、金额等都认可后，由买家提交给联控中心。联控中心由该卖家的名称，根据之前确认的卖家名称与其IP地址的记录转换出与之对应的真实的“IP地址”，再随机生成1个校验码，向其发出经加密的订单、及校验码，同时也记录下该订单的订单号、个人名、单位名、商品名称、金额等，用于完成之后的认证、支付(将订单号与该个人名、单位名建立绑定关系)。卖家收到该信息后，经解密得出订单、校验码，并向联控中心返回收到订单的信息，其中包含用特定的密钥加密的校验码。联控中心收到该信息后将解密得出的校验码与记录比对，若相符则返回验证成功的消息，否则返回验证失败的消息。卖家收到验证成功的消息，就可准备发货了。

[0038] 以往的电子支付中防止支付的金额的篡改的主要的办法，是对金额进行加密，而这里我们还可增加一些手段：买家从其邮箱中看到购物网站发来的订单后对金额进行检查，认为金额无误后，提交给联控中心。联控中心将其转发给卖家，卖家应当对收到的订单进行检查，若金额与商品的种类、数量相符，才向联控中心返回应答。而联控中心收到这1应答后，将其记录，支付时可将支付的金额与该记录比对，相符才会发出支付指令，否则就不发出相应的支付指令。

[0039] 联控中心事先在经过审核后，向合法的卖家(通过线下的途径)发放这种对订单信息、校验码进行解密、加密的密钥。只有真实的该卖家，才掌握该解密、加密的密钥，这可防止卖家的假冒。仅由买家去判断卖家的真伪是困难的，而通过联控中心判断卖家的真伪则可靠得多。让购物网站向买家发出邮件后，经买家的审核后再通过联控中心向卖家发出订单，防止了购物网站的作假。而仅凭返回的订单信息，就判定收到订单的卖家，是真实的卖家不可靠，因为订单信息之前可能在网上泄露，而该校验码是普通人难以从网上获得的，使用这种校验码可提高(验证卖家身份的)安全性。而让购物网站来编辑订单信息，是因为这些订单信息，往往包含数字、字母等，且字符较多，让买家自己编辑可能会让买家感到厌烦。而这比上述的使用自有平台(“购物”与“确认生产商的身份”2者结合)的方法的运行成本高。

[0040] 而买家的手机或电脑等，也是该系统的重要组成部分。而手机由于携带方便，是最适合的设备，故以下的论述主要针对手机，当然也可使用电脑等。

[0041] 上面提到了多种防伪支付的系统的组成方法，其中主要的1种由联控中心、代理平台、自有平台、买家的手机、通知端、主服务器、主机、辅机组成。也可由联控中心、代理模块、支付平台、自有平台、买家的手机、通知端、主服务器、主机、辅机组成。也可不使用代理模块，使用卖家端。也可不使用自有平台，而使用非自有平台。在这种系统中，服务站的服务器也是1个中心，而并非只有联控中心1个中心，而以往的电子支付常同只有支付平台1个中心。

[0042] 在防伪支付中1个易被攻击的弱点，是买家在购物平台上提交订单的环节，买家拥有的加密能力是较弱的，若敌手破解了某1买家的用户名、密码，就可在购物平台上提交伪造的订单，对此可让买家在领取商品时，向代理平台发出1个用于表明买家身份的真随机的口令(以下简称“买家口令”)以对订单表示确认。

[0043] 在这种电子支付中，收款账号不随意由买家直接确定、提交。而以往人们在网上购物时，可能是直接从网上得知卖家的收款账号，再通过支付平台完成支付，卖家收到货款后再发货，其收款账号由买家直接提交给支付平台；也可能是直接在购物网站上提交订单，再跳转到支付平台上完成电子支付；或者在收到商品后，通过担保支付平台在担保支付平台上，确认订单、收款账号，确认收到商品完成支付。这些方法较简单，存在很多的安全隐患。而以往的网购的付款账号的确定、提交、确认也较随意，这也给黑客的攻击带来了很多方便。以往人们在网购时，常是直接在支付平台上提交付款账号，通过用户名、支付密码来保证安全，这存在很多的安全隐患，对此我提出了以下改进：我们用完全随机的防伪码，作为支付的口令，这与以往的支付技术有着根本的不同，它可抵抗住量子计算的攻击。收款账号不直接由买家提交，由联控中心根据买家提交的订单中的卖家名转换出收款账号，并加密发往支付平台。对收款账号的确认，也不是直接由买家在支付平台上提交确认信息，而是通过较安全的渠道来完成(买家收到商品后，确认商品的种类、金额等无误后，发出防伪码、买家口令)，这也消除了重要的安全隐患。

[0044] 而收款账号通常不是网络商店的账号，而是生产商或可靠的经销商的管制账号(解释见下文)，而这种账号与生产商的关系是不直接在网上透露的，它通过联控中心等实现转换。其付款账号的确定、确认更完善，不随意由买家提交、确认，而是通过多次传递真随机的挑战值以及真随机的口令(买家口令)来确认(具体见下文)。正因为收款账号是确定的，故支付失败后，买家的资金还会保留在付款账户，而不会丢失。其对防伪码的正误的确认是直接进行的，即由服务站直接将防伪码发往联控中心，由联控中心或代理模块进行验证，这就没有卖家的服务器将防伪码的验证结果返回防伪中心的环节，消除了1个重要的安全隐患。

[0045] 我们通常只向真实的某1卖家，确定唯一的用户名，也只向它通过安全的途径发放真随机的防伪码及不规则材料，代理模块、代理平台也通过这种真随机的防伪码和防伪材料，来判定最终买家收到的商品的卖家的真实身份，这种判定是非常可靠的，是通过多个环节的紧密结合所形成的系统来实现的。而联控中心也可将用户数据转交给代理平台，这样代理平台可直接完成用户名与收款账号的转换，处理速度更快也更安全。

[0046] 卖家收到订单后，可检查商品的价格，若低于预先设定的价格，可提出异议。买家收到商品(信息)时，可通过手机或人工检查商品的价格，若高于预先设定的价格，可提出异议。在验证防伪码前，联控中心也可将商品的金额与记录比较，若不符可中止流程。而以往的第三方支付、网银支付，没有将金额与记录比较的环节。

[0047] 但仅有上述的措施，还不能保证绝对的安全，还必须与1种新的防伪材料结合才行，而这种防伪材料，不仅可提高电子支付的安全性，还可提高货币、银行卡等的安全性，以下详述之。

[0048] 2.防伪支付详述

[0049] 2.1不规则材料

[0050] 现在，1次性验证的防伪码的使用，已经很广，这可很好地防范复制，当然我们的防伪码也是1次性使用(验证后即失效)的，但这还是给敌手留下了1次仿冒的机会，对于珠宝等价值较高的商品，1次仿冒还是很有利可图的。即使将防伪与支付结合，使收款账号固定，敌手还是可对商品进行调包，并通过实体的商店销售真品以获利。以往的防伪码、防伪材料的最大的问题就是容易复制，对此我提出了1种难以复制的新的防伪材料(以下简称“不规则材料”)，它分为形状不规则材料(它以形状作为主要的查验的依据)、物理不规则材料(它以物理量作为查验的依据)等。而确切地说，若不是用于防范1次性的仿冒，就没必要采用不规则材料。现在，1次性的防伪码，使用得已经很多，其成本低得多。

[0051] 形状不规则材料分为1维、2维、3维3类。例如，将1根表面平直的塑料棒用1个表面不规则的锉刀以不规则的线路来锉，这就能形成1个不规则的表面。若这1不规则的表面凹凸不大，就可按照1条直线来查验各个部位，这种1维的不规则材料以下简称1维材料。若凹凸较大就不能按照1条直线来查验各个部位，若查验部位分布在1个平面上，这种不规则材料以下简称2维材料。若查验部位不是分布在1个平面上，而是立体的，这种不规则材料以下简称3维材料，它的仿制成本极高，但制造成本也较高。

[0052] 而查验不规则材料，是采用放大镜、显微镜等，按指定的位置(以下简称查验位置)进行的。可根据在指定位置查验到的图形，按照一定的规则(例如有转换为1、无转换为0，也可将灰尘等的坐标直接转换成数据，或将各个方格内的灰尘等的数量转化为数据，其方法是很多，本发明不对此进行严格限定)进行处理，可得出特定的数据，可根据这种数据来验证商品的真伪。这种数据及查验到的图形等，以下都统称为“查验结果”。而查验位置，是随机的、不规则的，可在发出不规则材料前，对其随机确定1或多组查验位置，并记录查验位置和查验结果。买家收取该商品时，在初步的验证(对防伪码、买家身份的验证)通过后，再向特定的人或设备(例如服务站的服务器)发出查验位置，再根据这些位置来查验，这样传输的数据量就较小。

[0053] 若由服务站发出查验结果、直接由卖家端完成不规则材料的验证，这对确定买家的身份较有利，但于确定卖家端的身份不利。若在卖家端发出查验位置前，先由卖家端向联控中心发出1个(以查验结果为源数据，用随机抽取几位数字等不可逆的算法生成的)校验值，再向联控中心发出查验位置，再让服务站向联控中心发出查验结果，联控中心也根据查验结果来生成1个校验值，并检查校验值是否相符，就可判断卖家的身份是否正确。而依据不规则材料来生成校验值，由于查验位置是不确定的，故敌手难以获得准确的查验结果，并生成校验值。用不可逆的算法生成校验值，可防止敌手推知查验结果。而以查验结果为源数据，比以往的生成动态口令的方法更可靠，因为其源数据是真随机的。若可由服务站发出查验位置(可从特定的1组位置中随机采用1个)，由卖家端发出查验结果(事先已经对多个特定的位置进行查验)，这对确定卖家的身份有利，但总体的安全性较差。

[0054] 而若通过代理模块(代理平台)完成不规则材料的验证，由代理模块通过联控中心发出查验位置，由服务站返回查验结果，安全性高得多。这样敌手就无法伪装成合法的卖家进行欺骗，也难以伪装成联控中心进行欺骗。联控中心向服务站发出的每1个请求，都会有记录，且有特定的流水号、编号等，还会对相应的应答进行核对，若敌手向服务站发出看似合法的信息，就将难以通过核查。

[0055] 制备不规则材料的方法很多，可以说是无限的。不仅是上述的用锉刀来锉的方法，

还可将纸等材料撕开、折断，断裂处的形状，往往是不规则的。我们还可制这样做，先用1个表面不规则的锉刀，以不规则的路线、速度，去锉1块表面平直的塑料；再以这样的塑料作为印版(以下简称锉纹印版)，在纸或塑料等材料上印刷；对印好的纸或塑料，可再印上1条直线或曲线，以便于针对这条直线或曲线上的图形进行查验。当然也可不印上线条，而是告知查验者进行查验所使用的线条的位置，这样敌手难以进行查验。也可按不规则的方向、位置，裁剪出材料，裁剪出的材料的1个侧边，是直的，而且位于印刷出的点、线较多的位置。这些不规则材料，以下简称锉纹材料。若这种材料的查验的部位，处于1条直线上，实际上它是1维材料。而我们不会对同1个锉纹印版，印刷出较多的锉纹材料，由同1个锉纹印版印出的锉纹材料，占总的锉纹材料的比例，都控制在一定的标准之下，这样我们通常遇到的锉纹材料，往往就是不同的。

[0056] 此外我们还可将不透明的灰尘(细小的固体颗粒)撒下，对承载灰尘的筛子，施以不规则的振动，以增加灰尘掉落位置的随机性，灰尘落在基材上之后，再予以固定。而对这种不规则材料(以下简称固粒材料)进行观察时，不易确定位置，对此可在其上印刷线条等来辅助定位，但常用的印刷技术所能印刷的线条最细只能达到0.06毫米，这对较小的区域较难以标记。还可印上相隔一定距离的、特定尺寸的色块(以下简称定位色块，它可类似于斑马线的样式)，用色块的边界作为确定位置的依据。我们还可在不规则材料上设置纤维(以下简称定位纤维)来辅助定位，这可更好地帮助定位，而在要求不高的情况下，我们也可不设纤维，以降低成本。还可使用粗细、或颜色不同的纤维，用来标记位置，粗纤维表示1，细纤维表示0，4根纤维为1组，就能表示15个位置。即使纤维的位置不太准确，也没关系，它本身就可成为1种位置不规则的标记。材料表面可标出正方向，以便于确定灰尘的坐标、确定查验的区域的位置。这样，固定、查验不规则材料时，首先要做的事，就是确定正方向。印刷的线条，可标出刻度等，以便于计算变形的比例等。还可在不规则材料上印出用于定位的点或其他形状的标志。

[0057] 具体地说这种材料可以是这样的(参见图1、2a)：用透明的强度较高的塑料、或玻璃等作为基材，这样材料不容易变形，也可在基材中加入或在基材下(外)粘上钢丝、塑料等材料以提高强度，这样材料又能适当地弯曲；先在基材的1面涂上透明的胶黏剂(通常是采用有机溶剂来稀释的)，待溶剂挥发干，在其上按一定距离间隔地放置定位纤维，将此面朝上，对承载灰尘的筛子施以不规则的振动，使灰尘从上方撒下，并用不规则的气流扰动，气流在较小的空间内的运动是很不规律的，这可使灰尘的运动也变得不规律。灰尘落下后，再在其上覆盖1层透明的保护膜。灰尘最好是形状不规则的，以加大复制的难度。基材的强度较高，可防止材料变形，但易被揭取。而基材的强度较低，可防止材料被揭取。若将用于加固的塑料等材料，粘在不规则材料的保护膜上，且宽度较大，坏人就可在这些地方下手，将不规则材料划开，实施盗窃，又不会破坏不规则材料，故应注意避免之。

[0058] 不规则材料的基材透明，便于用显微镜来直接观察，但若不规则材料贴在商品上，且商品是透明或半透明的，用放大镜、显微镜来直接观察，背景就可能对查验结果产生影响。对此可采用不透明的基材(参见图2b)，而且基材的颜色，需与灰尘的颜色不同，例如分别是白色、黑色，否则就会难以区分基材与灰尘。为便于观察，还可在胶黏剂下贴上金属膜，以反射光线。

[0059] 而随机确定查验位置，这些位置可能正好在定位纤维上；也可能在某些位置上，灰

尘过多，灰尘间没有明显的间隙；或是灰尘过少，一片空白，这些情况都会使转换出的数据缺乏随机性。可放弃这些位置，重新寻找其他的位置进行查验，直至找到合适的位置。

[0060] 此外还可用喷油漆、涂料、油墨等的方法来制备，即先将油漆、涂料、油墨等液体加压喷出，再用不规则的气流来扰动液滴，再使一部分液滴附着在塑料等基材上，待油漆、涂料等液滴干了，再覆盖上保护膜，这种不规则材料以下简称液滴材料。液滴材料与固粒材料，查验的方法是相同的，以下统称颗粒材料。干的液滴、灰尘等，都是不透明的细小的颗粒。

[0061] 此外我们还可制作这样的1种不规则材料(参见图3a、3b)：在基材的表面覆盖1层不透明的材料(例如油漆、涂料)，待其中的溶剂挥发掉，再用1或多个(钢)针(它们之间的距离是不相等的、不规律的)，以不规则的路径在材料的表面上移动(例如基材的运动由1个电动机控制，钢针的运动由另2个电动机控制，1个实现左右方向的运动，1个实现对安装钢针的部件的旋转，它们的运动速度都是不规则的)。这样，钢针划过的地方，就会没有油漆、涂料等(油漆、涂料等就会被刮掉)，这样就会在不规则材料的表面，形成不规则的图案。而钢针的尖端，是很小的，故它划出的痕迹就会很细，这样敌手就很难复制出同样的不规则材料。这种不规则材料以下简称“划痕材料”。为保护这层涂料，可在涂料的表面再粘上1层保护膜。为防止复制，可用粘度较大的不能用于印刷的涂料、油漆等涂在基材上，以往人们通常只能采用油墨等来复制图形。

[0062] 通常我们不需对所有的划痕都进行查验，只需对其中的1条进行查验就行了。而且我们不需对这1条划痕全部都记录数据，只需对一些部分进行查验就行了。我们只需对较小的部分，进行较精细的查验，这样数据量较小。而采用哪1条(划痕)，以下也简称为查验位置。通常我们可使用较粗的针，针的数量也不用太多，这样划痕较粗、较少，容易查验，标签的制作成本也较低，这适合于价值较低的商品。对于价值较高的商品，可使用较细、较多的针，以提高复制标签的难度、成本。它比颗粒材料查验容易，但较易复制。

[0063] 我们可采用这样的查验装置：1个凸透镜、1块用于确定不规则材料位置的玻璃板、1个照亮查验部位的光源、1块用于感光的CCD。CCD位于成像处，凸透镜、玻璃板、CCD的位置都固定，图像的放大倍率也固定。使用时，只要将不规则材料置于玻璃板处，就能生成放大的图像。玻璃板上可印上线条，以便于确定位置。而不规则材料可根据查验位置，进行移动。

[0064] 以往价值较高的商品的包装，大多都是1次性使用的，因为人们要通过这些包装来防伪。但采用了不规则材料后，防伪就不再依赖于包装了，这样包装就可较简单，也可回收了，这可大幅地降低包装成本，这是防伪技术的(支付之外的)另1个间接的益处。

[0065] 物理不规则材料也有很多种，例如我们可用颜色的深浅作为考察的物理量，先在1张白纸上喷上用易挥发的有机溶剂溶解的染料的液滴，再喷上无色的易挥发的有机溶剂的液滴，再通过加热、风吹等手段使溶剂迅速挥发，再覆盖上1层保护膜。这时染料还没有完全扩散，染料在各处的浓度差异较大。而纸是由纤维组成的，染料很容易通过毛细作用而迁移(俗称洇)，故纸上各处的颜色有很好的随机性，这种材料以下简称“洇染材料”。为防止染料的移动可在溶剂挥发后，再加入一些防止染料扩散的材料，例如喷上融化的蜡，待蜡冷却后，就会变成固体，阻止染料的扩散。但开发确定各处的颜色深度的技术较难，其成本也较高。

[0066] 我们还可用折光率作为考察的特性。例如我们可在透明的塑料中掺入一些可改变

光线的折射方向的物质(如其他种类的塑料或玻璃的碎屑,将玻璃进行粉碎得到的碎屑是很不规则的)。可先将盛放各种物质的碎屑的筛子(这种筛子可分成多个部分,参见图4)以不规则的速度转动、振动,再用不规则的气流来扰动碎屑的运动;达到一定的厚度后,再加热压制,使这些原材料形成1体。不应将这些材料完全混合均匀,否则对材料的各处进行考察得出的结果的随机性就会较差。虽其相关成本较高,但仿冒很难,用在国防、国家安全等领域,是很有前途的。

[0067] 我们还可将铅、锡、铜、铁、石墨等电阻率不同的粉末状的材料(应尽量采用电阻率相差较大的材料,以增加随机性)混合起来(方法同上),再加热压制成1体,其中可包含细微的气泡以增加随机性,这种材料以下简称电阻材料。而空气的气泡中含有氧气会使金属氧化,对此可在充满氮气等惰性气体的环境中来制造。电阻材料的查验方法很多,本发明对此不做出限定。若将1个电极置于固定的位置,再将探针置于不同的位置,就会形成不同的电阻。也可用2个探针,测量2者间的电阻,并通过一定的规则转换为查验结果,这2个探针间的距离应当较大,以提高攻击的难度。与2组位置的查验结果相关的电阻分布情况,比1组位置的查验结果相关的电阻分布情况复杂,4组就更复杂,16组就复杂很多,即使这些位置是很规律的(例如相邻各点间的距离相同)。2点间的电阻与多个位置的材料有关,这种关系是非常复杂的,很难通过计算来推导,若要复制电阻材料,1处的错误,就可能导致查验结果的不同。这种材料是非常难以复制的,且容易保存(不易损坏),查验的成本也较低,故很有前途。还可设2个电极,再测多处的电压、电阻等(这些探针、电极的位置,以下统称为查验位置,查验位置可以是1组位置,而不一定是单独的1个位置),这就更难仿制。而2个电极间的电流不同时,各处的电压等状况的变化是非线性的,故我们可在电流不同的情况下进行查验,还可在2个电极间的电压不同时进行查验,这些查验的条件以下简称查验条件。以现有的技术,要精确地控制电流成本较高,而测量电阻较为容易,故以下暂不讨论改变查验条件的查验方法。

[0068] 我们还可用磁介质来制作不规则材料,尽量使磁迹不规则,查验时使用较灵敏的磁头。

[0069] 不规则材料的特性是不规则的,理论上讲是无限的,这样敌手就难以完全复制。而按照指定位置来查验,又使传输的数据量较小,这样就容易查询。若不知道查验位置,即使敌手偷到了不规则材料也无法得出正确的查验结果。这种材料容易制作,却难以复制,复制的成本远超过制作的成本。当然在一定的技术条件下,查验不规则材料的精度是有限的,按照这种精度复制不规则材料也是可能的,但其成本通常是非常高昂的,因此是难以实现的。而不同的不规则材料复制的难度不同,就目前的技术而言,有的按一定的精度是无法复制的。

[0070] 对于价值较低的商品,只需在包装的封口处贴上用不规则材料制成的较小的标签(以下简称不规则标签),就足以防止坏人对商品进行调包,而对于价值较高的商品(例如钻石),坏人仍然可能从不规则标签之外的地方下手进行调包,并通过不正规的渠道将真品销售出去,故仅有防伪支付、不规则标签就不够了。对此也可使用较大的不规则材料,覆盖住商品的整个包装,以下简称不规则包装,它可有效地防止价值较高的商品被调包。不规则包装,通常可分为包装、封口2部分,当商品被装入包装后,再将用于封口的不规则材料,贴在封口处。包装部分可使用基材较坚固者,以便于重复利用;而封口处可使用基材强度较低

者，以防揭取。在基材较坚固的不规则材料被大量生产后，由于其数量较多，故回收后就很难再将它与其他的不规则材料区分开，故可多次回收利用，这样每次使用的成本就很低。每次用过，将商品及买家的编号等的字迹洗掉或撕掉，再用时再打印上新的编号，或贴上新的编号等的标签就行了。不规则包装的查验位置，必须覆盖封口处，以及其他的足够多的位置(查验位置之间的间隔不能大于货物的最小线度)，否则敌手就可能从中割开不规则包装，进行调包。而对不规则标签，则只需对经过封口处的位置，进行查验即可，故查验位置只需通过封口处即可。

[0071] 而查验不规则材料需使用专门的设备，故往往要在服务站完成其查验。若买家要求送货上门，可先将货物留在服务站，并通知买家商品已送到服务站，并告知商品的种类等信息，买家对商品信息进行核对后，若其的确订购了该商品则予以确认，系统核实过买家的身份后，由服务站向联控中心发出防伪码，防伪码的验证通过后，代理模块通过联控中心向服务站发出不规则材料的查验位置，服务站由此对不规则材料得出查验结果后，返回联控中心、代理模块，验证通过后，系统完成支付，服务站再向买家递交商品，这样买家对验证活动的启动有决定权，故易取得买家的信任，且不用送货员跑2趟；也可先将货物留在服务站，并将防伪码标签等递交给买家，由买家通过手机提交防伪码信息，防伪信息验证通过后，再由服务站对不规则材料进行查验，若验证通过再将货物递交给买家，这样送货员要跑2趟，且买家等待处理结果的时间较长。

[0072] 在货物的运输中，各个交接的环节是最容易出现问题的，而要保证最后买家收到的商品不被调包，就要使每1个环节都不出现问题，否则一旦发现货物被调包，之前的所有经手人，都可能是嫌疑人，难以准确地确定犯罪者。较简单的方法是，当货物足以用保险箱盛放时，货物用保险箱盛放，每到1个新的部门，将保险箱内的货物转移，或更改密码。这样转交货物之外的环节，都是较安全的，但转交的环节本身可能有问题。保险箱可能没问题，但货物可能被调换。

[0073] 更可靠的方法是，当保险箱被锁上时，就在箱门的门缝上，贴上1个不规则标签(以下简称交接标签)，并对特定的部位进行查验，记录查验位置、查验结果；货物到达下1个部门或单位时，上1个部门或单位告知其查验位置，得出查验结果后，再返回上1个部门或单位，上1个部门或单位根据记录进行验证，并将验证结果告知下1个部门或单位。若验证通过，则在上1个部门或单位贴的交接标签之外，再贴1个新的交接标签，再重复上述操作(对交接标签的特定的部位进行查验，记录查验位置、查验结果，货物到达下1个部门或单位时，上1个部门或单位告知其查验位置，得出查验结果后，再返回上1个部门或单位，上1个部门或单位根据记录进行验证，并将验证结果告知下1个部门或单位)。若验证未通过，则马上通知有关方面，停止货物的转移，这样犯罪可能发生的范围就较小，容易确定嫌疑人，这会对犯罪分子产生很大的震慑作用。交接标签，不像以往的防伪标签那样，容易仿制，故可大幅提高安全性。

[0074] 若商品较大、较多，不能用1个保险箱盛放，可制造1种较大的用于保管商品的箱子，以下简称“保管箱”，它可用以往的集装箱进行改造而成。保管箱被锁上时在箱门的门缝上，贴上1个交接标签，并在到达下1个部门或单位时再贴1个新的交接标签，并采用上述的验证方法。若条件允许，还可在保管箱的棱角等处，设置交接标签，以防商品被取出、调包。若某种商品(如手机等)的数量较多，发货单位也可用这种保管箱1次盛放多件商品，以降低

防伪成本。

[0075] 而若告知不规则材料的查验位置，是通过不安全的方法进行的(即较单纯地使用不规则材料)，就会给敌手以很多机会，使不规则材料的作用大打折扣。若敌手窃得了1个不规则材料，也知道相关的密钥等，就可伪造出验证请求，并获得查验位置，从而得出查验结果，故必须辅以其他的措施才能运用。我们应当使准确的人、设备，以可靠的方式获得查验的位置，才能够使不规则材料的作用得到真正的发挥，而通过防伪码来确认买家、服务站的身份，是较可靠的。

[0076] 验证不规则材料，放在最后，这样安全性最高。而最终的(联控中心生成的)支付指令的发出(或代理平台的支付操作的执行)，是经过了之前的多步的(防伪码、不规则材料等的)验证才做出的，这与以往的电子支付有很大的不同，以往的电子支付主要只是对发出请求者的身份进行验证、对支付信息进行加密，没有严格的对卖家身份、订单内容、防伪码、不规则材料的核查，没有对实物的核查。而设置了这些障碍，当然会给黑客以极大的困难，也使支付的安全性大大提高。以往，银行卡被盗刷的事件，非常多见，但采用了这样的支付方法，资金会安全得多。

[0077] 不规则材料，需与较可靠的身份验证、商品的防伪技术，紧密结合，才有运用价值，要将实体的防伪与数字的防伪相结合。若不能核实发出验证请求的人、实体的身份，随意地将查验位置透露出去，就没有什么安全可言了。故将不规则材料的使用，与防伪码的验证相结合是非常重要的。而这里的防伪码、不规则材料、买家口令，实际上也是验证买家身份的口令。

[0078] 而1个人的特征，也是无限的，不仅包括姓名、电话号码、密码、指纹、人像，还可包括很多内容，敌手是不可能完全复制它们的。我们完全还可这样做，设立线下的服务站，让买家亲自到服务站提货，提货前提供会员卡、U盾等介质，或输入密码，有条件的地方还可查验指纹等，来验明身份，这些线下的特征都是敌手难以复制的。这可放在开始(服务站向联控中心发出验证请求前)就进行，而仅是打了电话通知来提货，并不能保证来提货的人是真正的买家。

[0079] 当然使用不规则材料，较麻烦、成本较高，在要求不高的场合下，我们只需使用防伪码即可。而随着经济的发展，人们对商品品质的要求会越来越高，不规则材料的使用也会越来越多。

[0080] 若采用卖家端完成验证，若由服务站发出不规则材料的查验结果，可让卖家端认定该服务站、买家是真实的，便于联控中心确定服务站、买家的身份的真实，但于服务站确认卖家端的身份不利，敌手可伪装成某1卖家，并对收到的查验结果都返回验证成功的应答。

[0081] 2.2管制账号等

[0082] 这种支付中，收款账户，并不是由买家自己直接确定的(这其中没有买家对卖家的账号的确定的操作)，它是由1个功能较强的联控中心来确定的，而且这个联控中心与很多的实体的信息交流是很可靠的，收款账号绝不是黑客所能够轻易修改的。而这种付款账号与收款账号的绑定，是依靠支付平台或银行自身，所根本无法实现的。不仅如此，在这里，防伪码与该交易的买家、卖家的账号、订单号、商品的编号等也都是绑定的。为使这种绑定关系，较可靠，可让买家、购物网站、在确定订单后，向联控中心发出买家的用户名、卖家的名

称、商品的名称等订单信息。若之后的验证请求，不能找到与之相同的记录，就可给出验证失败的应答(这1验证请求可能是伪造的)。的确，这种绑定，不是由支付平台或银行直接完成的，而是由联控中心完成的，但这事实上形成了支付平台或银行中的相应的账户之间的绑定关系。

[0083] 而为保证买家的资金的安全，我们还可采取这样的措施：让买家在特定的(与联控中心有可靠的联系的，即采用可靠的密钥进行加密、解密的)支付平台上或银行中，开设唯一的专门用于进行防伪支付的账户(以下简称管制账户，其账号简称“管制账号”)，买家进行购物时只使用该账户来支付货款，将买家的用户名与其(该买家的)管制账号，建立绑定关系。而每1个卖家也在特定的支付平台或银行开设专门用于通过联控中心接收货款的唯一的账号，这种账号以下也简称“管制账号”。这样买家、卖家在其购物、支付的过程中，就可不使用(暴露)其支付的账号；联控中心在生成支付指令时，根据用户名与其账号的绑定关系，转换出相应的账号。由于在防伪支付中各卖家、买家的账号，只有1个，联控中心等在转换时，就不容易出错。而大型的生产商，管制账户的资金进出非常频繁，生产商不仅要获得资金，也要使用资金，为保证安全，可使其管制账户的转出账户只有1个，这样转出账户固定，资金的流向就容易掌控了。而同1个单位、人，可能在不同的情况下，既可能是卖家，又可能是买家，不但需付出资金，也要获得资金，故不能简单地限定管制账户只能接收资金或付出资金。

[0084] 为提高电子支付的安全性，可将转移的资金分为2类：有订单对应的资金(以下简称“有单款”，通常它就称做货款)、没有订单对应的资金(以下简称“无单款”)。联控中心只负责有单款的支付，而不参与无单款的转移。有单款有订单对应，可明确买家、卖家，而无单款的转移则不易控制，故将支付限定于有单款的转移是1种既简单又能提高安全性的方法。而对于个人来说，通常只会购买商品，而很少卖出商品，故对于个人，我们可限定其“管制账户”只能发出有单款、接收无单款，且只接受联控中心发来的付出资金的支付指令，不接受联控中心之外的机构发来的付出资金的支付指令。而对于单位来说，不只会卖出商品，也会买入商品，故对于单位，我们只能限定，联控中心只完成其“管制账户”的收入有单款、付出有单款的资金的转移，而不完成其“管制账户”的收入无单款、付出无单款的资金的转移。

[0085] 这种管制账号与用户名的绑定关系，是在网上不能直接查询到的，它通常存储在服务站、联控中心、支付平台或银行的服务器中。同1个买家在这个支付平台或银行上，可有多个账户，但联控中心所采用的只能有1个，这样才容易实现上述的绑定关系，即这种绑定关系，是由联控中心实现的，而非通过支付平台或银行实现的。为安全起见，将用户名与管制账号进行绑定的操作，应当在服务站完成，若直接由用户在公用网络上完成，信息可能泄露。

[0086] 而与支付的收款账户相应的用户名，是在购物开始时，由买家提交的订单所确定的，且在查验、收取商品时由买家、柜员亲自认定的，这对收款账户的范围有很大的限制，故黑客难以实现将买家的资金转至由其控制的账户；而支付需买家，在查验、收取商品(实物)后进行确认才能完成。黑客伪造1个订单、支付指令，就能盗取资金的事情，就难以发生了。

[0087] 而要求卖家的账户(收款账户)，只能是该卖家在联控中心所绑定的账户，也可进一步限制收款账户的范围，有利于保证买家的资金的安全。为限制收款账户的范围，对于每1个在联控中心注册的单位，联控中心对支付平台或银行发出的向其支付货款的支付指令

中采用的收款账号，最好都只采用1个，这样收款账号的范围就会较小，支付的安全性当然就会较高。而卖家在网上也不用(暴露)其收款的账号；联控中心在向代理模块发出支付指令(或向代理平台发出支付信息)时，根据卖家的用户名与其收款的账号的绑定关系，转换出相应的账号。

[0088] 开立以往的支付平台上的虚拟账户，申请较随意，不用经过严格的审核，同1个人也可开立多个虚拟账户。而管制账号，不能随便申请，要对身份等经过严格的审核，其账号必须与真实的姓名、名称绑定，而且1个个人，在1个联控中心上只能使用1个管制账户。这对保护买家的利益，是很重要的。而同1个单位，既需卖出商品，也需买入商品，其收款账户、付款账户，可以是同1个账户，也可分开，但买入商品、卖出商品都必须分别使用唯一的账户。

[0089] 以往人们常是直接使用账号来进行支付，而账号常是由无意义的数字组成的，不仅难以记忆，也难以人工识别，这给电信诈骗、黑客攻击带来了方便。通过卖家名来间接完成支付，就可改变这种状况。每1个卖家，在防伪支付中只使用唯一的用户名，而且由字母、汉字等组成，容易识别、记忆。而且卖家名与相应的单位的名称等的关系，可在网上进行查询，骗子无法遁形。而以往的银行账号，通常不能在网上查到其单位等信息，骗子就有机可乘。

[0090] 在这种支付活动中，只有货物被送到了服务站或买家手中，服务站的柜员、买家见到了货物，才可能完成支付，这也是1种货到付款的付款方式，故不会出现买家钱货两空的情况。在这种支付中，支付信息的确认，不是靠对订单信息的解密，而是由人(买家、柜员)执行的。只有买家认可了这1订单(尤其是收款者、付款者)，才可能完成支付。若买家发现货物不对，或是金额不对，任何时候买家都可提出异议、中止流程。若货物是正确的，通常买家都会承认订单是真实的，除非买家想反悔(因为觉得东西太贵了，或是付不起钱等原因，而允许退货，也是吸引顾客的1个重要手段，不允许退货是不对的)，但这些情况下，订单还是真实的，若买家与卖家事先曾经订过合同，或对交易的确认能提出什么证据，卖家都可依法争取自己的权益。这种确认订单的过程，完全不同于以往的机器对密文的处理，它不是1种可由机器自动完成的过程，它不但可靠，成本还低(不需进行复杂的加密、解密)。这种确认，是以特定的密钥(服务站与联控中心联系的密钥、服务站与买家联系的密钥)、口令、挑战值等来实现的。而货物的送到，本身就证明了该订单的存在，货物的种类，可由其自身来体现；它的生产商，可根据标签或货物的特征来确定；而该货物的买家，也可通过货物上的标签及之前的记录来确定，这些都是难以抵赖的，与该货物对应的订单的信息，都是货物本身就携带的，并不是非要用解密的手段才能得到。而且，若买家不承认该订单，他就不能获得该货物(柜员将不会向其递交该货物)，他原本是有着较强的意愿才决定要买下这1商品的，他可能的确非常需要这1商品，故反悔的几率较小。所以通过这种途径对订单进行确认，是非常可靠的。

[0091] 而这里的收款账户，是通过防伪码、校验码等，来确认其与订单、买家的用户名的绑定关系的。而以往买家开始订购时就向支付平台发出订单、收款账号等，这也可实现这种绑定，但个人所掌握的加密、解密的能力较有限，故安全性较差，不可取。卖家(或代理模块)根据防伪码，可确定买家是真实、准确的，这1交易是真实、准确的，这时表明自己的身份较好。卖家也害怕买家恶意骗取货物(收到货物后不付款)，而这种支付方法中，对买家也有严格的验证，故会大幅减少这种情况的发生。开始，购物平台、网站也可通过输入登录口令等

来判断买家的身份的真假。由于知道了真实的买家，即使出现不支付货款的情况，也很容易找到买家。

[0092] 1个更可靠的方法是，由联控中心事先通过线下的途径递交给卖家的U盘中，其中存储1项用于验证卖家的身份的数据(以下简称卖家口令)。在卖家对防伪信息进行验证后，若验证通过，由卖家向联控中心发出卖家口令，联控中心由此确认该信息是由该卖家发出的。而这种方法的成本较高，若卖家请代理模块完成验证、支付，就不需使用卖家口令了。

[0093] 以往的防伪码常以明文的形式传递，任何人都可轻易地得到它，这样防伪码就可能被坏人用在其他的商品上，这样买家获得的商品就未必是真的。而且以往用户往往因为怕麻烦、不愿意花上网费等原因，不进行防伪码的验证，还随意地丢弃防伪码，使防伪码很容易被泄露。我们可在线下设立多个为买家提供防伪码的验证的服务站，代买家来验证商品的真伪，这不仅方便了用户，也使防伪码的验证更可靠。我们可让超市等来加盟，这样就可减少场地、人工等费用。

[0094] 我们的防伪码，可使用真随机数发生器(例如蔡氏电路)来生成，这样虽成本稍高，但可根本上防止对防伪码的破解。防伪码在打印在标签上(或置于商品的包装上、内)时，可进行加密，这样当普通人获得这些防伪信息时，就难以获知真实的防伪码。

[0095] 若卖家有自己的服务器(即卖家端)，不通过代理模块完成验证，防伪码可由卖家端生成，加密后打印在标签上，置于商品的包装内。商品送到服务站后，打开包装，将防伪信息录入服务器，再加密发往联控中心。联控中心用相应的密钥解密后，得出防伪码的明文，再用特定的密钥加密(当然也可称为用特定的算法进行1次加密)，发往相应的卖家端，卖家端对防伪码验证后得出结果，并向联控中心返回经加密的验证结果。这里，防伪码共进行了3次转换，即卖家端的加密、服务站的加密、联控中心的加密，以下简称“3次加密”。而我们只向通过审核的单位(卖家)，发放(加密、解密的)密钥，这就能从源头上防范假冒。而这种(使用卖家端的)方法，不用线下(由联控中心向卖家)传递真随机的口令，成本较低，但安全性较差，只适用于金额较低的交易。其最容易被攻击的薄弱环节，是确认防伪信息正确后，卖家端向联控中心发出确认信息，若敌手破解了加密的算法、密钥，就可实施攻击。

[0096] 而目前很多单位没有自己的服务器、网站，无法完成上述的处理，对此我们可设立“代理模块”为它们提供代理服务，再在卖家处设立通知端，处理的流程是：代理模块生成防伪码(以下也记为J1)，加密后(以下也记为J2，下同)，将J2复制到U盘中，再派人将存储多个J2的U盘送给卖家；买家提交订单后，联控中心将订单发往通知端；通知端收到订单后，向仓库、车间等部门发出通知，找出、生产出、购进商品，在发出该商品时，通知端从U盘中(随机或依次序)调出J2，加密(为J3)后打印在标签上；货物送到服务站后，服务站的工作人员(以下简称柜员)将防伪码的密文J3及其编号录入服务器；服务站的服务器将其加密(为J4)后，发往联控中心，联控中心再将其转给代理模块，由代理模块完成防伪码的验证；若验证通过，联控中心向支付平台发出支付指令，完成货款的支付(划拨)后，支付平台返回“完成支付”的应答；联控中心也向通知端、服务站返回“完成支付”的应答。这里，防伪码也进行了3次转换(即代理模块的加密、通知端的加密、服务站的加密)，故以下也简称“3次加密”。

[0097] 此外我们也可通过代理平台提供服务，处理的流程是：代理平台生成防伪码(以下也记为J1)，加密后(以下也记为J2，下同)，将J2复制到U盘中，再派人将存储多个J2的U盘通过服务站送给卖家；买家提交订单后，联控中心将订单发往通知端；通知端收到订单后，向

仓库、车间等部门发出通知，找出、生产出、购进商品，在发出该商品时，通知端从U盘中(随机或依次序)调出J2，加密(为J3)后打印在标签上；货物送到服务站后，柜员将防伪码的密文J3及其编号录入服务器；服务站的服务器将其加密(为J4)后，发往联控中心，联控中心再将其转给代理平台，由代理平台完成防伪码的验证；若验证通过，代理平台完成货款的支付(划拨)，再返回“完成支付”的应答；联控中心也向通知端、服务站返回“完成支付”的应答。

[0098] 以往有的防伪系统中，也有防伪码的加密，其加密方法与3次加密相似，而3次加密不是本发明的重点。真随机的防伪码、买家口令及不规则材料的使用，才是本发明的重点。

[0099] 若要使用不规则材料，可采用卖家对不规则材料随机确定查验位置、得出查验结果后，将查验位置、查验结果加密回传给联控中心的方法。但这样卖家要自己设立服务器，这对于很多商家是不易实现的。我们还可采用另1种方法：代理平台事先对一定数量的不规则材料(其上标有编号)，随机确定查验位置，并记录查验结果，将不规则材料的编号及查验位置、查验结果、特定的防伪码及其编号一并记录，这些编号可存在U盘中，通过线下的途径传递给卖家。卖家在将不规则材料用在商品上(将小的不规则标签贴在封口处，或用多块不规则材料将商品全部包裹住)之后，将商品的编号与其上使用的不规则材料的编号，一起加密发往联控中心(使联控中心知道商品的编号与不规则材料、防伪码之间的对应关系)，再由代理平台完成验证。而在要求不高的情况下，我们可不将商品的编号与不规则材料的编号上传，以降低成本。这种方法的优点是，不需事先将查验位置、查验结果暴露在网络上，成本也较低，但缺点是不容易确定查验位置。为便于确定查验位置，可在不规则材料上，印上或标上较多的用于定位的标志(例如*号等)，通过这些用于定位的标志与查验位置之间的位置关系，来间接地确定查验位置。

[0100] 此外代理模块不仅可生成J1，及加密查验位置、查验结果的密钥，还可生成加密订单号、买家的用户名、商品编号等的密钥，它们都可打印在标签上，随商品一起被传递，服务站再以此对订单号等进行加密。而以往的加密，往往使用较固定的密钥，使用这些1次性的密钥，可使敌手难以对特定的买家的商品的支付(及真伪的验证)，生成正确的密文。由于订单号等信息，主要是由数字组成的，故敌手很难破解它。

[0101] 若联控中心与支付平台在物理上是相邻的，就不需使用复杂的加密来保证信息传输的安全。若联控中心与支付平台在物理上不相邻，就要使用复杂的加密来保证信息传输的安全，这样成本较高。这样就不会有上述的，确认防伪信息正确后，卖家端向联控中心发出确认信息的环节，被敌手攻击的情况发生。但这要线下传递防伪信息，成本较高。为降低运输成本，可通过服务站来间接递交U盘。先由代理模块生成真随机的防伪码等数据，存储于U盘(为区别起见这种U盘可称之为“防伪U盘”)中，再送到服务站，让卖家派人领取U盘。领取后，将其与通知端连接，将数据载入。通知端在第1次使用某U盘时，发出U盘的编号，这样代理模块就能知道卖家领取的U盘是哪1个。通知端可依J2的编号的顺序来使用J2，也可随机调取J2，后者安全性较高，但成本稍高。由于服务站的数量较多，且分布广泛，故卖家获取这种U盘很方便，而运输成本也较低。当然我们也可通过服务站来间接递交不规则材料，以降低成本。

[0102] 买家在购物平台上提交订单的环节，是很容易攻击的，若有敌手进行监听，就很容易破解出用户名、订单内容等(它们是确定转账信息的关键信息)。为提高安全性，可对买家的用户名、卖家的用户名、订单号进行加密，以增加攻击的难度。具体的方法是：代理平台送

给卖家的U盘中，再增加对买家的用户名、卖家的用户名、订单号进行解密的真随机的密钥这3项数据；买家提交订单后，代理平台确定订单号(当然订单号的明文之前不会在网上泄露)，并对订单号、买家的用户名、卖家的用户名使用真随机的密钥进行加密后发往联控中心；联控中心再将其加密发往相应的通知端；通知端收到信息后通知相关部门，发出商品时，通知端用U盘中的密钥，对买家名、卖家名、订单号进行解密(若条件允许，代理平台向通知端通过线上途径发出订单信息时，还可再增加1个对用户名、订单号进行加密的密钥，可简称为“网络密钥”，再使用网络密钥进行加密，可防范U盘中的信息泄露后敌手的攻击)，再将买家名、卖家名、订单号(可简单加密)与防伪码的编号等打印在标签上，但服务站号不能(强)加密，否则货物不能送至正确的收货地址；服务站收到货物后，向联控中心发出验证信息(用该服务站与联控中心联系用的密钥，对买家名、卖家名、订单号、防伪码的编号、防伪码等进行加密，一起发往联控中心)；联控中心再将信息转给代理平台，代理平台根据防伪码的编号、防伪码、订单号等完成验证，再根据买家名、卖家名，确定付款账号、收款账号，完成支付。

[0103] 由于加密订单号、用户名的密钥是随机的、1次性使用的，订单号、用户名(的明文)也是由数字等无意义的内容组成的，故敌手难以根据代理平台发出的密文破解出订单号、用户名。用户名是确定收款账号、付款账号的依据，若敌手掌握了用户名，就可能实现盗取。在信息技术日益发达的今天，最大的风险来自网上，故防范网上的攻击，比防范线下的攻击更重要。虽然我们也提供电子的途径的支付，但关键的因素都是通过线下的手段控制的。在以上的方法中，订单号的明文，在服务站发出验证信息前，一直没有在网上泄露。虽敌手可从线下的途径获得一些防伪信息，但效率较低、成本较高，很难大规模操作。

[0104] 而用户名是非常重要的，不知道卖家名，代理平台就不知道该向哪1个通知端发出信息；不知道买家名、服务站号，就无法对服务站发来的信息进行解密(因为不能确定解密的密钥)。故简单地采用以往的购物平台是不行的，至少应对其进行改造，让其掌握准确的卖家名、买家名，最好是将购物平台与支付平台进行整合。

[0105] 代理平台、通知端确定防伪码的编号，可根据同一个通知端收到的订单的次序来得出。而若订单由不同的购物平台生成，那么就必须针对不同的购物平台，分别计算同1个通知端收到的订单的次序，若1个购物平台，不能与代理平台有稳固的联系，就难以准确地确定同1个通知端收到的订单的次序，也难以准确地确定防伪码的编号，之后的验证也都会出现错误，故购物平台与支付(代理)平台的整合是非常重要的，简单地沿用以往的购物平台是不够的。依次序来确定防伪码，可不暴露防伪码的编号，这可提高安全性。

[0106] 此外为增加攻击难度，可不依序确定防伪码(的编号)、订单号。若防伪码、订单号依序确定，敌手就可根据顺序依次确定之。可这样确定防伪码：卖家收到代理平台送来的U盘后，由通知端回传U盘的编号，代理平台根据U盘的编号，确定其掌握的防伪码的编号。当买家在自有平台上提交订单并划拨定金后，代理平台在该通知端当前未用的防伪码中，随机确定1个(为便于操作，每次可对较小范围内的防伪码，如100个，进行选择)，并将该防伪码的编号发往通知端，通知端由此确定使用的防伪码，并将其打印(可简单加密)在标签上。

[0107] 确定订单号的方法可以是：代理平台送往卖家的U盘中，存有解密订单号的(1次性使用的)密钥，当买家在自有平台上提交订单后(可先生成1个流水号，以便操作)，代理平台在可用的订单号中随机确定1个，并根据防伪码的编号调出相应的加密密钥，将该订单号加

密发往通知端，通知端由此解密出订单号，并将其(加密)打印在标签上。在实际中，通常需将防伪码的编号与订单号的密文，1起发往通知端，否则通知端就无法确定防伪码的编号与订单号的关系。

[0108] 若在卖家包装商品时，使用哪1个不规则材料，完全由卖家直接确定，那么要完成验证，发出货物后，卖家需将查验位置、结果传递给联控中心。若通过线下的途径传递它们，效率低、成本高，对此我们可采用这种方法：代理平台传递给卖家1个U盘，其中储存用于加密查验位置、查验结果的密钥，使用这些密钥对信息进行加密后传输给联控中心，就非常安全了。由于查验位置、查验结果，都是无意义的数字，故只要对同1组查验位置、查验结果的数字使用1个密钥，就足以防止信息被破解(加密对象是真随机的、1次性使用的)。

[0109] 当然还可不由卖家确定使用哪1个不规则材料，即由代理平台先记录不规则材料的信息(在送出不规则材料前，记录其编号及查验位置、查验结果等)，1批不规则材料送到卖家处后，回传批号，代理平台就可确定该卖家拥有的不规则材料的编号等。防伪码的编号与不规则材料的编号可绑定，防伪码与不规则材料也一起传递、使用，这样不规则材料的编号就可不公开。

[0110] 卖家(通知端)收到订单信息(在本文中，订单信息也包括防伪码的编号、防伪码的密文、订单号的密文、商品的名称、买家的服务站号等，而不仅仅只包括商品名称、买家的用户名、服务站号等)时，依序采用1个不规则材料，用于某1商品上。即卖家依据收到的U盘中的防伪码的编号的次序，依次采用不规则材料(依次确定相应的不规则材料的编号)；代理平台依据发出的防伪码的编号的次序，依次确定相应的不规则材料的编号。举个简单的例子，例如，代理平台对发往某1通知端的第1个订单，采用第1个不规则材料(编号为1)；对发往某1通知端的第2个订单，采用第2个不规则材料(编号为2)……通知端对收到的第1个订单(为便于操作，可再采用1个流水号)，采用第1个不规则材料(编号为1)；对收到的第2个订单，采用第2个不规则材料(编号为2)……理论上讲，U盘的编号与不规则材料的编号的关系，是较固定的，可在代理平台送出U盘、不规则材料时，就确定U盘、不规则材料的关系，这样不需将相关信息暴露于网络上，但为操作方便，通常可由通知端或服务站来确定它们的关系(先向代理平台同时发出不规则材料的包装的编号、U盘的包装的编号，代理平台通过包装的编号确定使用的不规则材料的编号)，这样U盘、不规则材料送到服务站及递交给卖家的顺序有变化，也没有关系。但U盘中的防伪码的数量，必须与递交给卖家的不规则材料的数量相等，否则难以匹配。各个卖家的商品的销量，是预先难以确定的，将会使用的U盘等的数量也是难以预料的，故根据情况，在卖家领取U盘、不规则材料时，临时确定通知端的编号，及防伪U盘、不规则材料的编号的关系较方便。这种方法虽简单、方便，但若不规则材料的放置、使用顺序等有误，就会造成差错，对此可将不规则材料的编号与该商品的订单号加密回传给联控中心，以便完成验证。这样做的缺点是，订单号再次出现在公共网络上，这为破解订单号提供了可能。

[0111] 为防止破解订单号，可这样做：送给卖家的不规则材料，用特定的箱子盛放。装箱时，随机地(从回收的旧的不规则材料，或新的未用过的不规则材料中)采用不规则材料；各个不规则材料上，再依序贴上1个“流水号(它是依顺序排列的)”标签；再将不规则材料，按照流水号的顺序放置在箱子里，同时，记录流水号与不规则材料的编号的关系。若采用回收的旧的不规则材料，各不规则材料的查验位置，应当重新确定，并记录查验结果，因为数据

已经被泄露。

[0112] 联控中心向通知端发出订单信息时，针对每1个通知端，发出订单号、不规则材料的流水号(该流水号依序确定)。卖家发出商品时，针对各订单号的商品，使用相应的流水号的不规则材料。这样卖家就不需将不规则材料的编号与订单号，回传给联控中心。这其实是将不规则材料的编号进行随机的变换，敌手无法仅根据其流水号就推知其编号。而这种订单号与不规则材料的编号的关系，是由联控中心确定的，不需通知端再将这种关系回传给联控中心。

[0113] 而在这些环节中，防伪码的编号，通常都可采用明文或简单加密，故可作为确定订单号、防伪码、不规则材料等的较可靠的依据。

[0114] 实际中，卖家与买家可能不是同处于同1个城市，而是相距较远，这样就不能直接通过同1个联控中心来完成支付及防伪信息的验证，故需在各地(通常是以市为单位)设立多个联控中心、代理平台，以下简称分中心。还需要设立用来沟通、管理各个分中心的机构，例如可设立管理江苏省的各市的联控中心的机构，以下简称“地区中心”。还可设立用来沟通、管理各个地区中心的机构，例如可设立管理中国的各省的联控中心的机构，以下简称“总中心”。

[0115] 这样，验证的总的过程可以是：先由分中心A生成J1；再向其所属区域内的卖家甲，通过线下的途径传递J1的密文J2；卖家甲发出商品时，将J2的密文J3打印在标签上，置于商品的包装内。商品被运到另1个城市的相应的服务站后，服务站将J3加密发往其所属区域内的分中心B，分中心B再将其(直接或间接)加密发往分中心A。若分中心A、分中心B，是相邻的、或较近的，则它们可较容易地约定、更换联系中使用的加密、解密密钥，但若它们相距较远，则它们可能不能较容易地约定、更换联系中使用的加密、解密密钥，这时可通过总中心来中转信息。每1个分中心，只需有与总中心联系用的密钥就够了，而若要有与每1个分中心联系用的密钥，则要有很多组密钥。促进国际贸易是非常重要的，而以往仿冒国外的名牌产品的事件屡见不鲜，若能保证商品的品质，相关的商家的生意都会好做得多，我们可将防伪支付的服务机构，发展到国外，这样我们买到的国外的产品的品质就会有保证，我们的产品也会更容易卖到国外去。而这样代理模块、平台的编号的数量就会较多。

[0116] 而若不规则材料与货物分开放置、运输(货物、不规则材料上都标有编号、个人名等，用于确定它们之间的对应关系)，虽会增加验证的环节、降低工作速度、提高成本，但可减少信息泄露的机会，这对于某些价值较高、体积较大的商品是值得的，但对于体积较小、容易调包的商品则不适用。而对于价值较低、数量较大的商品(例如饮料)，通常是多件商品用托盘一起装载的，若接到了订货要求，再找出不规则材料、装箱，就会使交货时间推迟，较可行的方法是，先在各件商品上打印编号，并将多件商品装箱，在发货时，再另行打印编号、防伪码、用户名等(可简单加密)，并将不规则标签(可用密码箱锁起来)，与货物一起交给收货人(或分开传递)。

[0117] 当然，也可让不规则材料随货物一起运输(可事先记录不规则材料的编号、查验结果等，在发货时再对各件货物确定不规则材料)，而将印有防伪码等信息的标签与货物分开传递。这不仅使敌手难以获得查验位置，难以完成验证，又可防止调包，这其实是最佳的1种组合方法。

[0118] 而没有服务站，就难以实现可靠的加密、解密，也难以实现安全的，防伪信息与货

物的，分开运输，与集中验证。以往也已经有一些消费者的手机上安装了一些防伪的APP，但若软件可随意地从网上下载，会给敌手带来很大的方便。敌手可让买家下载含病毒、恶意程序的软件，以此来欺骗买家。我们可让买家直接在服务站下载软件，加注真随机的密钥，这就安全得多。

[0119] 普通人使用的传输信息的途径，是很容易被监听的，而服务站可使用强加密的方式来传输信息，甚至可使用专用的网络，当然安全性高得多。而通过服务站来加密，加密的成本也较低，因为同样的设备、装置可被多次使用，其成本可分摊到多个用户身上。例如，使用U盾，虽可提高安全性，但真正使用的人并不多，原因之1就是很多人不愿意花钱买。

[0120] 以往的防伪码的使用，较简单，它常常只和防伪码的编号捆绑(结合在一起进行验证)，防伪码标签可随意贴在任意1个商品上。但我们的防伪码，是与编号、订单号、买家的用户名、服务站号、商品名称、金额、购物时间等捆绑的，若有人将防伪码盗用在其他的商品上，就无法通过验证。即使防伪码被丢弃，也不怕别人盗用。而只有与电子商务结合，才能做到这些。而这种编号，是与原材料的批号、相应的工人的工号等相对应的，故不能随便乱贴的。以往，在生成新的防伪码后，系统要与数据库中的记录进行比对，只有与记录不同的防伪码才可被使用，以保证其唯一性。但我们的防伪码，是与防伪码编号、个人名、服务站号等捆绑的，故即使新生成的防伪码，与已有的防伪码相同，也没关系，故可省去这1比对环节。这可提高效率、降低成本。而防伪码编号、服务站号等，与防伪码可用不同的密钥、算法加密，以增加攻击难度。

[0121] 在实际情况中，商品的总量，是非常巨大的，若要让防伪码唯一，防伪码的位数，就必须很多，这会给扫描、包装、数据库带来很大的麻烦。条码占的空间较大，不仅会使包装较大，印刷成本也会较高，扫描时的识别也会较难，还可能要多次对不同的部位进行扫描，而数据库中存储的数据的信息量也会较大，传输的数据的信息量也会较大。防伪码与用户名等捆绑后，就可采用较少的位数，也使相关的多项成本降低。

[0122] 为提高安全性还可增加1个验证环节，代理模块对防伪码进行验证后，或在联控中心向卖家端发出加密的防伪码等后，若验证通过再由联控中心针对该防伪码的买家生成1个验证码(以下简称“交易验证码”)，以短信或微信等途径发到用户的手机上，再由用户将其返回联控中心；若验证未通过则直接向服务站返回“未通过”的信息，系统将由此启动报警程序(即通知相关单位、部门，并采取相应措施)，以短信或微信等途径发到用户的手机上。用户的手机号，可不透露给卖家，这可减少手机号泄露的机会。交易验证码的验证通过后，再向服务站或直接向买家的手机，返回验证成功的消息。这可防范仿冒的服务站欺骗买家，而且会增加用户的信任，因为只有自己参与了操作，才能完成验证，别人无法替代。而这些验证活动，都是以电子的方式完成的，其成本的增加也很有限。这不仅是使用SIM、USIM卡来验证买家的身份，也可通知买家，让其对该交易、支付知情。

[0123] 当然，现在SIM、USIM卡的复制，已很常见，故这还不够。若敌手知道了某买家的手机号码，再复制出同样号码的SIM、USIM卡，就可能伪装成合法的买家(尤其在发出信息时，敌手发出的信息不会被真正的买家的手机接收到)。在手机上安装APP，可防范上述攻击(不同手机上的APP可使用不同的密钥来传输信息)，但以往人们在手机上安装的APP与外界(例如支付平台)交流所使用的密钥，是根据一定的算法生成的，可能被敌手破解。对此我们可对APP(由服务站)通过线下的途径，加注真随机的(与服务站联系所使用的)密钥，这可使安

全性进一步提高。

[0124] 2.3挑战验证法

[0125] 而若买家的手机用固定的密钥与联控中心进行联系，敌手长期监听后，就可能破解出密钥，并伪造出正确的应答。对此，可让联控中心生成1个挑战请求，向买家的手机发出；买家的手机，收到该挑战请求后，生成1个真随机的挑战值(以下简称A挑战值)，将其发往联控中心；同时，买家的手机由A挑战值也生成1个应答值(以下简称B应答值，密钥可由联控中心直接通过公用网络加注，以防范服务站的作伪)，若联控中心收到2或更多个不同的A挑战值，就说明有敌手在进行攻击(这样敌手就无法向联控中心隐瞒其不法行为)，则向买家的手机发出“有敌手在攻击”的提示信息，并中止流程。联控中心收到A挑战值后，进行加密而生成1个应答值(以下简称A应答值)，并发往该买家的手机；若买家的手机收到的联控中心发来的A应答值，与由其发出的A挑战值生成的应答值(B应答值)不同，或收到2或更多个不同的A应答值，也说明有敌手在进行攻击，则向联控中心发出“有敌手在攻击”的信息，联控中心收到该信息后，向相应的服务站、卖家发出“有敌手在攻击”的信息，向该手机发出“已中止流程”的信息，并中止流程。而若一开始就先由买家的手机向联控中心发出挑战请求、挑战值，则不能产生这样的技术效果。这种通过真随机的挑战值来防范敌手的伪装的方法，是以往没有的。上述的使用A挑战值等来判断主体身份(是否有敌手在攻击)的方法，以下简称“挑战验证法”，它是1种原创的方法。而商品上的“不规则材料”，不仅可用来验证商品的真伪，也可用来验证买家的身份，这高度安全。挑战验证法与不规则材料是本发明中最主要的2个创新点。

[0126] 2.4站点口令等

[0127] 以往消费者在实体店里购物，店员向消费者递交商品是直接的，较简单、容易。但在电子商务中，很多顾客要求送货上门，递交商品就较麻烦，尤其是珠宝等价值高、体积小的商品更难保证安全。而顾客在服务站中自提商品，可直接完成验证操作(例如输入用户名、密码来登录系统)，较简单。但若是送货上门，顾客可能要求在家中完成验证操作(在手机上提交验证信息)，这些都对我们提出了更高的要求，我们只有提出适当的措施，才能达到这些要求。

[0128] 为便于买家确定送货员的身份及该送货员所属的服务站的身份，可在买家在服务站完成注册手续时，由服务站的服务器随机生成一定数量(例如100个)的用于确定服务站的身份的口令(以下简称站点口令)，并打印为纸质文件(二维码或一维条码)或用显示器显示出来，让买家用手机扫描之，并储存起来。这样买家在收货时，就可用手机扫描站点口令来确定为其服务的服务站的身份(是否正确)。站点口令的使用，是1次性的，这样安全性较高。而当站点口令快用完(例如剩下10％)时，可再由服务站的服务器随机生成一定数量的站点口令，并派工作人员上门递交。递交时，可出示之前还没有使用的1个(例如最后1个)或多个站点口令，来表明身份，买家用手机对其进行扫描后，得出验证结果，若验证通过，再扫描新的站点口令并储存之。站点口令，可防止假冒的网站、卖家、服务站欺骗消费者的情况发生，而它也是一次一密级别的，而且是线下传递的，故其安全性非常高。以往人们总认为线下传递一次一密级别的口令成本较高，而让用户、送货员顺带携带之，可使传递的成本较低。用无线、有线的的方式向手机传输站点口令，容易被黑客盗取，而通过纸质文件等线下的途径直接递交站点口令，较安全。当然，也可不使用手机来完成站点口令的验证，直接由

买家根据纸质文件人工进行核实站点口令，这样不会发生因手机丢失而造成站点口令丢失的情况，但较麻烦。

[0129] 我们在派出送货人员(以下简称送货员)前，由服务站的服务器，针对每1件货物随机生成1个用于确定买家的身份的验证码(以下简称取货验证码)，并发往买家的手机，送货员以此确定买家的身份。若同1个买家同时有多件货物要领取，可只生成、使用1个取货验证码。这样，只有向送货员出示取货验证码的所谓的“买家”，才能够得到相应的货物，不会送错。此外，我们在派出送货员前，由服务站的服务器向相应的买家的手机发出送货员的编号，这样，买家可通过送货员的编号来判断送货员的身份是否正确。为防止送货员在送货的途中，将货物调包，对于价值较高的商品，我们可采用密码箱来存放货物。在送货员出发前，由柜员确定使用哪1个密码箱(在密码箱上有标有编号的标签)，并将货物及相应的站点口令一起锁在密码箱中。开密码箱的锁的密码，由服务器随机生成，并由柜员设定。由服务器将密码箱的编号、开锁密码，发往相应的买家的手机。开锁的密码，不告诉送货员。取货验证码、送货员编号、密码箱编号、密码箱的开锁密码，可一起发送，也可分开发送。而买家收到货物，并核实货物无误后，可用手机生成1个用于表明送货工作已完成的验证码(以下简称工作验证码)。由买家用手机将该工作验证码发往相应的服务站，也将该工作验证码告诉送货员。送货员回到服务站后，将工作验证码告知柜员，若其与记录相同，系统确认货物已送到。以往，买家收货时，仅进行手工签名，而若送货员伪装成买家进行签名，不但难以确认，而且发现代为签名的时候往往较迟。

[0130] 上述方法中有1个弱点：买家在购物平台上提交订单的环节。对此可使用买家口令、送货口令：若买家在服务站领取商品，可直接在服务站确认订单，由服务站直接发出买家口令。若由送货员送货上门，服务站先生成1个真随机的口令(即送货口令)，加注到送货员携带的装置(如手机)，买家在家(或工作单位等处)领取商品时，由买家在送货员携带的装置上予以确认，由该装置发出送货口令，服务站对该口令的验证通过后，通过联控中心向代理平台发出买家口令。验证通过后，代理平台完成货款的支付。使用服务站及送货员的设备，是较可靠的。而真随机的口令，敌手是难以攻击的。送货口令，可由服务站的服务器生成，再加注到送货员携带的设备中，这样买家在家就能发出送货口令，而传递口令也较容易、成本较低。而让买家的手机1次下载较多的口令，不仅麻烦(让买家多次奔波)，还不安全。买家口令，可由代理平台生成，使用U盘(为区别起见可称之为“买家口令U盘”)来存储，并传递给服务站，服务站的工作人员再将其与主服务器连接，将数据载入。买家口令是真随机的，这就决定了它不能是时间同步式的，不能通过算法来得出，只能通过线下的途径来传递，它可以是事件式同步的，也可按照编号来同步。事件式同步(依次序来同步)，可就同1买家的订单来排序，也可按服务站发出验证信息的次序来同步，由于敌手不易掌握次序，故安全性较高，但这些方法的实施成本较高，还需将代理平台与购物平台整合。依口令的编号来同步(每次发出口令时，也发出其编号，可依发出验证信息的次序依次使用买家口令)，成本较低，容易实施，较可行。它可不与防伪码捆绑，这样不需将这种U盘与防伪U盘对应起来，操作较方便、成本较低。在要求不高的场合下，可不使用买家口令U盘、买家口令，以降低成本。而防伪U盘中也可仅包含防伪码及其编号，其编号来自于不规则材料的编号(2者相同)。服务站向卖家递交不规则材料的同时，也递交相应的防伪U盘，其中存有相应的不规则材料的编号，及相应的防伪码。联控中心向卖家发出订单时，不发出订单的流水号，而是发出相应

的防伪码编号，用防伪码编号作为订单号，并将订单流水号与防伪码的对应关系保存，这样成本是最低的。

[0131] 现在移动支付的应用越来越广泛，它给人们带来了很多方便，甚至很多人平时都不带钱包了。但移动支付的最大问题，是安全性不够，这是现在大部分人不接受电子途径的支付的主要原因。移动支付在给人们带来方便的同时，也给黑客带来了方便。要保证移动支付的安全，就必须使用动态的口令，最好使用真随机的动态口令。但要由支付平台直接向用户传递生成动态口令的装置(例如U盾)，是困难的，而且很不可靠。直接传递真随机的动态口令，更是难以实现的。只有设置大量的服务站，才能可靠、廉价地传递U盾、真随机的动态口令。上述的支付方法，高度安全，甚至超过银行系统的支付的安全性。而不会电子购物、支付的人，可在服务站由柜员代为完成操作，买家本身的操作较简单。故上述的技术的提出，可推进电子支付的推广。

[0132] 对于珠宝等价值较高的商品，若用户订购了商品，又中途反悔要求退货，会给卖家造成很大的损失。尤其是个性化定制的产品，退货后将很难再销售出去。对于这些商品卖家通常会要求买家先付定金后，订单才能够生效。对于这种情况，我们可在买家支付了定金后，再继续其他的流程(通知卖家等)。当然，对于价值较低的商品，可不设置收取定金的步骤。

[0133] 若只是简单地传递真随机的防伪码的明文，容易泄露、被人复制。通过联控中心，进行多次加密，可有效地防范加密订单号等的密钥的破解、防伪码的复制，但也不能根本地防止破解加密订单号等的密钥、复制防伪码(调包)。而不规则材料的使用，则可防范对3次加密的密钥的破解。使用不规则材料的电子支付的安全性，是现有的电子支付技术，所远远无法相比的。

[0134] 而这种真随机的口令，可只用于将该买家的与该订单相应的金额的货款，转至该卖家的特定的账户，这样若口令的验证成功，货款将划往该卖家；若口令的验证不成功，货款还在该买家的账户上，而不会不翼而飞。而以往的电子支付，常可随意地确定收款账户，这就给黑客带来了极大的方便。而确定了某1商品的买家、卖家，也使得对于仿冒行为，容易确定受害人、责任人，这也对防止仿冒有利。即使仿冒获得了成功、骗到了货款，也容易追查。

[0135] 不规则标签，可防范复制防伪标签，但还难以完全消除货物被调包。1次性验证的防伪码可很好地防范复制防伪码，但这还是给敌手留下了1次仿冒的机会。防伪与支付结合后，即使买家得到的是赝品，也付了款，货款也只能转往正确的卖家，而不会转给调包的敌手。而以往，大部分人购买商品，还是通过传统的线下的途径进行的，这样调包换出的商品就可能卖出去。但当大部分人都通过电子的途径购物后，敌手调包所换出的真品，也将难以卖出去，因为它没有合法的防伪码等。大的、知名的单位，不会接收这样的商品，而不知名的单位也很难将商品卖出去。要防止敌手通过有名的单位将调包的商品卖出去，生产商的认证非常重要，而以上的方法对生产商的认证远比以往的方法严格得多。

[0136] 上述的方法中，大部分的关键信息，都是通过线下的途径传递的(密钥、防伪码、不规则材料的传递，及买家输入密码等)，这大大增加了攻击的难度。

[0137] 我们只向真实的某1卖家，确定唯一的用户名，也只向它通过安全的途径发放真随机的防伪码，及不规则材料等，代理模块、代理平台也通过这种真随机的防伪码和防伪材

料，来判定最终买家收到的商品的生产商(卖家)的真实身份。这种判定，是非常可靠的，是通过一连串的多个环节的紧密结合所形成的系统来实现的，我们在可能的多个环节，都做了改进。而通过以往的传统模式的商业体系，我们根本不可能对商品的生产商的身份有如此准确的判定，因为商品经过的环节太多，而每1个环节都可能存在问题，仅凭单个的消费者的力量，是难以弄清这些经销商的身份、资质的。

[0138] 表面上看，使用真随机的口令、密钥、不规则材料，使成本较高，但在安全性提高后，贸易量会增加、整体的效率更高，故总收益更高，总成本会下降。而不采用这些方法的生产商，会失去人们的信任，采用这些方法的生产商，会提高美誉度。而生产商在这些方法开始使用时，积极参与这些活动，本身就是1种品牌营销。

[0139] 当然有的单位实力雄厚、销售额较大，也可不通过购物网站来销售商品，可直接通过其企业的网站完成商品的销售，这就可取消与购物网站进行交流的环节，具体的方法是：买家在其企业网站上订购商品，企业网站再向买家的联控中心中的邮箱发送订单，买家核实过订单后，提交给联控中心，联控中心再向该企业网站返回订单已核实、记录的应答……(以下都相同)。

[0140] 以往，价值较高的商品，人们大多还是到实体店中购买，因为人们认为，在网上买东西，出了问题，可能找不到相关的责任人，难以获得赔偿、售后服务等；而到实体店购物，即使商品出了问题，也能找到相关的责任人，容易获得赔偿、售后服务等。而实体店的经营者，由于难以逃避责任的追究，也会较认真地进行经营，不敢随意地销售假货。但使用了上述的方法，通过电子的途径购得的商品，真伪的鉴别的可靠性，就会远超过通过实体店。其原因不仅有3次加密、其防伪码是真随机的(可防范对防伪码的破解)、使用不规则材料(可防范防伪信息的复制)，还有很多：以往的商品的销售，大部分是通过实体的商店完成的，这种商业模式，难以对每1件商品都准确地确定其最终的买家(的所在地)。故防伪码标签往往可贴在同1批商品中的任何1件上，防伪码与“商品的编号”、买家是没有绑定关系的，甚至很多商品都不采用编号。这样同1个防伪码可能对应的商品的范围，就会较大，故出了问题很难追查。若其中有一部分商品，被人调换，或是防伪码被人复制，也很难发现，也很难认定责任人。某1防伪码所对应的商品，其运输、保存的途径、情况，是不确定的，这样就难以进行严格的管理、追查。而与电子商务结合后，我们就容易确定买家及货物的目的地。确定了目的地，对运输、保管就容易实现严格的管理。哪一些货物，在哪1个时段，应当位于何处，都能查得出，出了问题，就容易确定责任人的范围。而对商品记录其保存、运输的全过程，可使每1件商品的保存、运输的过程，都可追溯，这样责任人的范围就会小得多。

[0141] 而增加了用户名、服务站号等验证的要素，不仅可使真伪的鉴别更准确，更可缩小商品销售的范围。若发现1个防伪码，在其所属的服务站之外出现、要卖给别人，就可判定它是假货，并进行追查，查找出造假者。而确定了买家，若商品被调换，换出的真品就难以卖出去，因为它无法通过验证。这种商品的“实名制”，可大幅地提高防伪鉴别的可靠性。此外，在电子商务中，商品在从仓库出发到最终的买家手中，经历的时间较短。而在以往的商业活动中，商品从仓库出发到最终的买家手中，经历的时间较长，即使出了问题，也难以及时发现。而设立了服务点，就可对防伪码进行加密、解密，这也可防范防伪码的复制。即使有人盗取了防伪码或防伪码的密文，由于不掌握加密的密钥，故无法通过防伪码的验证。而正规情况下，这1商品，只能通过特定的服务站递交给相应的买家。造假者，难以将假货通过正规的渠

道销售出去。此外，设立了线下的服务站，也容易获得消费者的信任(因为出了问题，容易找)。

[0142] 而以往，消费者买到了商品后，由于怕麻烦等原因，经常不验证防伪码，还经常会随意丢弃防伪码，设立了服务点，就可采取这样的措施：不验证防伪码，不允许递交商品，防伪码也必须在验证后销毁。这些措施，都可大幅地减少仿冒、提高真伪鉴别的准确性。

[0143] 而若1个生产商，在1个地区，只通过这种服务体系来销售其商品，并且也向消费者广泛地宣传：在这1地区从某1时刻起所生产的产品都通过这种服务体系的服务站来销售。那么消费者就可很容易地(根据其生产日期、经销地点)认定：通过线下途径购买的所谓的这个生产商(在该日期后)生产的(在这些服务站之外的地点销售的)产品，通常都是假货。

[0144] 而一些实体的店铺，也经常会销售现货，在这种情况下，没有相应的订单，对此，可将为该店铺服务的服务站的编号(用户名)，作为买家的用户名，卖家的用户名还使用该卖家的用户名，订单号可根据出货单来确定。而在验证之前，卖家应当将相应的信息(买家名、卖家名、订单号、防伪码编号等)，提交给联控中心，并且可标上表示商品是现货的标志(例如增加1个字段，0表示商品需预订，1表示商品是现货)，否则就将无法通过验证。

[0145] 3.签名

[0146] 不规则材料，是在寻求商品防伪的方法的过程中被提出的，但很快我发现，不规则材料不只可用于商品的防伪，它还有很多用处。它也可作为1种安全性极高的签名。签名，是证明甲方、乙方对合同的认可的事物。手写的签名，可能被模仿。电子的签名，也不能保证绝对的安全，只要密钥被窃，或是被破解，谁都可能伪造出电子的签名。而使用不规则材料，则可靠得多。

[0147] 1个人对某1合同的条款认可后，可获取1个不规则材料，对其随机确定查验位置、记录查验结果；再将合同的文本、该不规则材料，一起交给可靠的机构(例如公证处)进行保存，这样普通人就难以再接触到该不规则材料；当需证明该合同的这个签署者，的确签署了该合同时，可让该签署者，告知其原先的对该不规则材料进行查验的查验位置及查验结果；该保存不规则材料的机构，根据这些查验位置，得出查验结果，并将查验结果进行比对，若2者相符，则可证明该合同的该签署者，的确签署了该合同，因为这1不规则材料是难以复制的，而普通人又难以知道查验的位置。若要多次证明该合同的该签署者，的确签署了该合同，可事先确定多组查验位置，并记录查验结果。

[0148] 4.信息的安全传输

[0149] 不规则材料还可用于信息的安全传输。信息的安全传输，是非常重要的。最安全的加密方法是一次一密，但密钥的传递往往很困难。而不规则材料可作为1种密钥的载体，而其包含的信息的数量，几乎可以说是无限的，故若不能知道查验位置，1个不规则材料所承载的密钥就无法解读出来，由此生成的密文也就无法破译。通常我们可将不规则材料，与查验位置的信息，分开传递，以防范敌手的攻击。具体的方法可以是：针对1个所述的不规则材料，随机地确定1组查验位置、得出查验结果，并根据查验结果，按照一定的规则转化为加密密钥；用这些加密密钥对明文进行加密，生成密文；将所述的不规则材料与查验位置、密文，分开传递；信息的接收者获得所述的不规则材料与查验位置、密文后，根据所述的不规则材料与查验位置，得出查验结果，按照一定的规则转化为解密密钥；用这些解密密钥对密文进行解密，生成明文。

[0150] 此外不规则材料还可用于承载密文，若对某1明文，将其与1个不规则材料对应起来，就可得出对不规则材料上的每1个位置的特征，应该采用何种密钥来解密。再将密钥，及查验位置，与该不规则材料，分别传递给信息的接收者。即使密钥、不规则材料中的1个，被敌手获得，也无法破解出明文。具体的方法可以是：针对1个所述的不规则材料，随机地确定1组查验位置、得出查验结果，并根据查验结果，按照一定的规则得出数据；根据这些数据，与明文，按照一定的规则，得出解密密钥；将所述的不规则材料与查验位置、解密密钥，分开传递；信息的接收者获得所述的不规则材料与查验位置、解密密钥后，根据所述的不规则材料与查验位置，得出查验结果，再使用这些解密密钥，按照一定的规则转化为明文。

[0151] 5.货币、票据

[0152] 不久我又发现了不规则材料的很多更重要的用途，现在实体货币的仿冒屡禁不绝，假币不仅对百姓造成了很大的危害，也对政府、国家财政造成了巨大的危害，防范仿冒使实体货币的制造成本非常高，而且为了防范仿冒，国家必须每隔一定的时间，就重新发行新的样式的货币，废止旧的样式的货币，这造成了巨大的浪费，但不规则材料的使用，完全改变了这些状况。

[0153] 现在对1元的货币的伪造日益多见，而国家对面额如此低的货币使用较高级的防伪技术，成本是难以接受的，故有的地方已开始拒绝使用1元的硬币，而不规则材料可改变这种尴尬。

[0154] 而很多银行，为避免用户将获得假币的罪责归咎于它，只能采用打印冠字号的方法。这不但麻烦，还不可靠。

[0155] 纸币的出现，就是为了降低制造货币的成本。中国人也往往以世界上第1个创造出纸币的国家为荣。但长期以来，中国的造币技术一直落后于西方国家，虽然我们的技术也在不断提高，但还是没有超过西方国家。若我们能创造出比纸币的成本更低、安全性更高的货币，以及新的查验货币的真伪的技术，将开启货币历史的新篇章，也给中国人再1次带来荣誉。

[0156] 我们可用不规则材料(电阻材料尤为合适)来制造实体货币，其制造成本很低，但仿制成本很高，远超过制造成本。这种货币以下简称“真密币”，意即使用真随机的密码(口令)的货币。

[0157] 现在，联网核查已在验钞机上使用，但使用范围较小，它对货币的防伪其实很重要。对于每1个实体货币都使用唯一的编号，并在每1次查验时，都上传货币编号、查验装置的编号，则只要同1个编号在多地同时出现，就足以判定有伪币存在。但伪币与原货币同时进行查验的可能性较小，只有同1编号在一定的时间内跨越的距离超过一定的标准，我们才能够较可靠地判定有伪币存在。时间超出标准、距离低于标准，我们就难以做出准确的判断。而且这对服务器的要求较高，要同时计算大量的编号出现的地点的空间跨度，及转移的速度，其实施成本很高。

[0158] 联网的记录，使货币的流向可追溯，这可一定程度上防范伪造货币、洗钱等行为，但还很不够，而且还有1个重要缺陷：当出现同1个编号在多地同时出现时，难以区分真伪。故联网核查必须与不规则材料的使用相结合。

[0159] 当有同1个货币编号在多地同时出现时，可这样分辨真伪：真密币可在正规的(得到认可的、可靠的)服务站(其服务器以下简称查验服务器，通常设在银行内，也可在银行

外)查验真伪,每1次查验时,用户将其插入专用的装置,该装置读取其编号,并向中央服务器发出验证请求(包括服务站号、货币编号等);中央服务器根据该货币编号,调出之前的对该货币进行验证的服务站(其服务器以下简称上1服务器)的编号,并向上1服务器发出验证请求(若是出厂后第1次验证,则直接将验证请求发往生产厂);该服务站返回与该货币编号相应的查验位置(可以是1个位置,也可是1组位置);中央服务器向查验服务器转发该查验位置;查验服务器根据该查验位置得出查验结果,并返回;上1服务器对查验结果进行验证,并将查验结果返回;若验证结果是通过,查验服务器重新随机生成1个或1组新的查验位置,并记录查验结果。下1次查验真伪时,由新的查验服务站向中央服务器发出验证请求(包括服务站号、货币编号等)……为提高安全性,中央服务器还可验证服务站的身份,以防范假冒的服务站盗取防伪信息。在条件允许的情况下,还可同时验证并记录持币者、付款者、收款者的身份(例如用户名、身份证号等)。这种方法中,系统不用存储大量的防伪信息,成本较低。而且,系统不需频繁地计算同1编号的移动速度,运算负担较小。以往,传递真随机的口令的成本较高,但上述的使用真密币的方法中,口令是由用户自己传递的,其成本是很低的。

[0160] 为提高安全性,可在每1次验证中,都先由中央服务器调出上1次验证时验证的查验位置,并发往查验服务器,并由查验服务器得出查验结果,若验证通过,再由中央服务器向上1服务器发出验证请求。由于该查验位置、查验结果已经在网络上泄露,故其价值已经降低。这样可提高对查验服务器的验证的可靠性,但会增加成本。由中央服务器记录查验位置、查验结果,会增加中央服务器的负担,但可降低服务站的负担、提高支付速度。

[0161] 在可能的情况下,可将货币编号与其所有者的用户名、账号等关联,若有同一货币同时属于1个以上的人的情况出现,则必有假币,只有与信息化、电子商务结合,这才可能实现。

[0162] 有时真密币上会有污物,对查验产生影响,若在此时就发出查验位置,可能泄露敏感信息。可先由查验装置对真密币进行检查,若发现较严重的污染,可发出警告,要求操作者对真密币进行清洗,只有符合标准时,才继续操作。

[0163] 上述的接力完成的验证方法非常安全,但服务站的数量毕竟是有限的,服务站外的小店使用的查验设备(以下简称简易终端)则不够可靠,也不能保证24小时在线,上述的接力完成的验证方法就不能使用。若简易终端重新随机生成1个或1组新的查验位置,并记录查验结果,下1次查验真伪时,数据可能被盗用。但小店通常只是收款,较少付出资金,收款是不存在使用假币的动机的,收款只会担心收到假币,故他们有很强的防范假币的意愿。而小店用的简易终端可很简单,通信功能可使用电脑、手机实现,故远比现在的验钞机便宜,易于推广。

[0164] 而小店卖东西通常要找零,为防止其付出假币,可在查验货币时,向中央服务器上传货币编号及终端编号、向买家的邮箱(可由系统免费提供)发出邮件,还可在货币上盖章等,这样假币被检出时,就可查出来源。此外还可在生产厂记录多个位置的信息用于验证。

[0165] 此外,消费者可能认为小店找出的用简易终端检验的货币不可靠,为提高安全性,可不由小店发出查验结果等,仅通过消费者的手机发出查验结果、向消费者返回验证结果。

[0166] 对于价值较低的货币,可这样来降低成本:省去向服务器索取查验位置的环节,直接由终端发出查验位置、查验结果,服务器只记录一些特定位置的查验结果,终端也只对这

些位置进行查验。为提高安全性，终端采用的查验位置是从这些位置中随机选取的。为提高处理速度，可每天或每批货币调整1次查验位置。为降低存储防伪信息的成本，可只存储小数点后特定位数(例如第3位)的数值。每1次验证时，可不验证多个位置的查验结果，可只验证较少位置的查验结果，这样成本较低。为增加攻击(敌手监听信息并进行复制)的难度，可使相邻的2次验证的查验位置不同。而且记录多个位置的查验结果会使复制成本很高，不值得复制。而若同时记录非常相近的多个位置的查验结果，会大幅提高复制难度，以现有的技术很难对这样的材料进行精细的复制。其实只要使复制成本高于币值就行了，故币值较小的真密币，只需记录、查验较少的位置的信息就够了，而币值较大的真密币只需记录、查验较多的位置的信息就够了。

[0167] 真密币的伪造，与传统货币的伪造，有很大的不同。同1个货币编号，只允许在1处出现。即使敌手复制出与原货币完全相同的货币，伪币也很难正式流通，记录查验设备的编号的做法也使伪币的流通很容易追查，这样伪造货币就是无意义的了。伪币很难转手，就不会有很多人愿意购买、接受伪币了。即使伪造者能够将伪币使用1、2次，成本也非常高，收益也很少。而以往的硬币的伪造成本，与政府的制造成本，是相近的，政府并不具有较大的优势，而真密币的仿制成本与生产成本的比值非常大。

[0168] 为阻止伪币的流通，我们还可制定这样的制度，真密币通常只能在同1个国家的1个省流通(可在编号的开头加上所属地区的编号)，出省、出国都需转换为其他省、国家流通的货币，即到外省、国前，将真密币存入银行(成为电子货币)，到外省、国后再兑换为实体货币；或将实体货币带至外省、国后，在正规的银行兑换为外省、国流通的实体货币，银行再将其集中转运至原先的省、国；相邻的省的货币，可直接由银行集中转运，不用兑换。这样，就可在不同的国家设立中央服务器，也在每个省设立服务器，这不但可减轻服务器的负担，还可避免因各省间有网络故障等原因造成的无法验证的情况发生。携带大量实体货币远行，以往也都是人们想尽量避免的，故上述措施并不会给人们带来太大的麻烦。而发行货币，可由省1级的机构完成，这就不用远距离运送实体货币，降低了运输成本。

[0169] 据纽约联储局报告称，全世界美钞约2/3在外国流通，因此其伪造的威胁，主要是在国外。而在境外使用的人民币，也越来越多。用传统的方法，很难对距离遥远的国家中使用的实体货币进行可靠的防伪。若直接在外国设立发行机构，并通过发行机构的服务器，联网验证真密币，鉴别成本可很低，效果也好得多。

[0170] 真密币的口令可分3类，1类是简易终端、手工终端等用的口令，1类是服务站用的口令，1类是核实用的口令。核实用的口令通常不使用，若出现口令与位置不匹配或其他的可疑情况再使用核实用的口令。确认其为真币后，可重新确定查验位置，记录查验结果，并改变货币编号。

[0171] 此外，我们还可对真密币定期(可按时间或使用次数来计量)改变编号，并重新确定查验位置、记录查验结果等，以下简称货币更新，这样可防范敌手伪装成合法的终端的攻击。其不规则材料可沿用，由于其信息是真随机的，新的查验位置也是真随机的，故改变了编号后，敌手很难确定新的编号的真密币的信息，这种改造的成本很低，但很可靠。在货币更新中，不仅可变更编号，还可改变不规则材料的位置，以增加攻击的难度(提高攻击的成本)。不能只是向左右方向移动，还应进行旋转。为便于移动，不规则材料的外缘，可增加一些用于固定的部件。查验的区域，也应小于整个的不规则材料的表面。固定不规则材料的边

框可用硬质的塑料，取出、安装不规则材料，可通过加热塑料来实现。为便于操作、降低成本，还可这样做：不规则材料不改变位置，而在真密币上增加1个部分，以下简称变换数据区，上面打印随机生成的查验位置的变换参数，每次查验时，根据参数对查验位置进行调整。其运算量很小，因此实施容易，这使得货币变更的频率可很高，不用成百上千次使用过后再变更，这对防范仿冒非常有效，而以往的货币是难以变更编号的。而变换参数来货币更新，不规则材料不用移动，这于制造有利。

[0172] 以往的实体货币的防伪特征、信息，往往是静态的，要防范仿冒只能不断地采用新的防伪技术，而这些新技术很快就会被敌手掌握。为防范可能出现的仿冒，政府往往只能按照一定的期限，提前开发新技术、淘汰旧技术，这种开发的费用是非常高的，而旧技术的淘汰也会造成巨大浪费。而以往也有多次印刷技术泄露的事件发生，其带来的损失是极为巨大的。而很多新的造币技术非常复杂，实施也较困难。例如新版美元自从2011年5月宣布当年10月发行，至2013年10月8日，经历了2年多时间，其间曾两度公布印制生产过程发生了重大质量问题，损失惨重。而上述技术完全改变了这种状况，同1个真密币，只要未损坏，就可一直使用下去(编号可变，不规则材料不用变)。而其使用的技术很简单，实施难度较小，成本很低，根本原因就在于，防伪信息是变化的、真随机的、而且是难以完全复制的。

[0173] 此外，与信息化的结合，也是非常重要的。以往的纸币的制造要求非常高，纸质、油墨等只要有细微的变化，就会导致不合格，故制造困难，成本高。尤其是变色印刷、光变油墨，其成本是非常高的。而真密币的制造成本，低很多。而各国常有新版纸币发行，以往的验钞机、ATM机很难适应这些变化，若只是图案等有变化，智能机可通过更新数据的方法来解决，但对新的类型的防伪特征就无能为力了，更换升级验钞机、ATM机的费用也是巨大的。而智能验钞机虽性能较强但较贵，而真密币的检验装置价格较低，但性能远超过之。

[0174] 真密币可以是这样的：为保护查验区域，可在电阻材料外设1护套，而包含电阻材料的部分，以下简称内芯，参见图5a。为便于查验，护套的形状可为长方形等，圆形不便于确定货币的方向。若长度与宽度相同不便于确定货币的正方向，长度可为宽度的1.5倍等。还可设1个孔，用于固定货币，以下简称固定孔。为降低查验成本，币值不同的货币，可采用相同的大小。币种不同的真密币，最好大小也相同。大小不同容易造成夹钞、漏钞等情况，给点钞机的设计带来了困难，也增加了金额统计错误的几率。而由于大小相同，将不同币值的真密币分开存放较容易。而以往的货币常常大小不同，故分拣较难。

[0175] 纸币的厚度很小，只能通过捻钞等方法将各张纸币分开，故常出现计数不准的情况，而真密币的厚度较大，容易分开，计数不准的情况将大幅减少。为减少存储空间，可使尺寸较小。

[0176] 纸币的使用寿命较短，1张纸币平均流通300次，仅是硬币寿命的1/100，很容易出现残、旧、烂、安全线脱落等情况。虽然硬币的使用寿命较长，但因为其硬度较大，在上面制作花纹、图案等很困难，故以往硬币的防伪较难，故仿冒行为也相对较多，硬币通常也只用在币值较小的货币。而对于政府，制造硬币的成本也较高，财政负担也较大。据英格兰银行披露，目前旧版的1英镑硬币，竟然超过2％是假币，现在英国在推出新版的1英镑硬币，回收旧版的硬币，其成本是非常高的，真密币可解决这些问题。

[0177] 为便于查验装置区分正反面、左右，可在护套的正反面的中间各设1个表示位置信息的条码或磁条、金属条等(例如正面从左到右是0123，反面是4567)，此外还需标注编号、

币值、币种等，承载这些信息的部分以下统称信息区。正反面都标有货币编号、变换参数(数值相同)等，可降低查验装置的成本，正反面各设1个感应装置成本较高。而信息区也可位于上下2个侧面及左右2个侧面，而币值的标记(正方形、星形等)的位置可随币值不同，颜色也可不同，这样币值更容易分辨，对快速统计总金额、区分币种及币值有利。自然情况下，货币存放时可能左右、上下颠倒，故币值标记应当2侧皆有。对于1摞真密币，可对其侧面拍照，对照片使用电脑、手机等中的软件就可自动统计，又快，又准。交账时，现金与账目可迅速地进行核对，即使不马上核对，只要将账目与这种照片一起交出，也足以证明操作者没有做伪。我们也可不使用传统的机械式的点钞机，借用电脑、手机的摄像头就够了，这些对以往的纸币都是不可想象的。这确切地说，也是一种条码技术，而以往的条码，还不能很好地适应这种情况，需要开发一种新的类型的条码。以往中国还没有主导开发过一种新的类型的条码，而这会改变历史。

[0178] 若货币较小，为便于人眼识别币值，可不使用条码(或用磁条、金属条等)来承载这些信息，而将显示币值的颜料涂在表面；也可在查验装置中增设1个放大镜，以便于读取条码，这样文字可较大，条码可较小。为防泄密，可对变换参数加密。信息区的空间非常有限，尤其是侧面的信息区，要在如此小的空间内表示这么多信息，并不容易，而货币的种类是较多的，因此必须制定1个标准，才能使各种货币都能被较容易地分辨。例如，表示币种的二维码，应该有多少个元素。而最早制定这种标准的国家，就可使用较易辨别、简单的编码。以往，不同的国家的货币的检验，要采用不同的验钞机，客户还经常对这些验钞机的性能存在疑虑，因其防伪特征有很大差异，而采用了上述技术，同一种验钞机就可检验不同的国家的货币，这可大大增加验钞机的功能，也降低银行、政府的成本，还对不同国家间的商贸有利。

[0179] 护套中间设1用于放置内芯的槽，护套上可设1个铁片(可不设在表面，以增加印刷币值的空间)，内芯上的相应位置设1磁铁，不查验时可将护套与内芯固定以保护内芯，查验时将内芯拉出。为便于拉出内芯，槽的开口处可留1缺口，电阻材料外设1个用于传动的部分，用胶轮与之接触，拉出、推入内芯。也可在内芯的末端设1凸起，用机械手拉出、推入内芯。为防内芯滑脱，可在内芯上设1凸起，在护套上设1阻挡物及1个相应的槽，以下简称防滑脱槽，参见图5b。内芯上也应当标上编号、币种等，这样护套上的编号等被损坏或护套被混淆时，可恢复数据，该部分以下也简称信息区。

[0180] 内芯的边，可用于确定查验位置，长边以下简称校准边，短边以下简称起始边。为提高强度，边缘可用钢片等材料，塑料容易磨损、变形。仅用普通的尺子不能准确确定探针的位置，其精度要求较高。我们可用游标卡尺来手工确定探针的位置，现在普通的游标卡尺只需几十元就能买到，故容易实现(可用于精密终端，参见下文)。而我们还需采用2个长方形的钢片，以下简称辅助片，其长边是直线(其精度要求较高)，与邻边垂直(其精度要求不高)。探针的位置可用x、y坐标来表示。先使游标卡尺的尺身与校准边平齐，量爪的左刃口与起始边贴合，用右刃口确定x坐标。当使读数与目标值相符时，将辅助片与右刃口贴合，并用紧固螺钉将该辅助片固定。由于游标卡尺的尺身和量爪的刃口是垂直的，故可用它使该辅助片的长边与校准边垂直。再在辅助片上量取与y坐标目标值相符的位置，再用另1个辅助片，与右刃口贴合，并用紧固螺钉将该辅助片固定。2个辅助片的边的交叉处，便是探针应在的位置。

[0181] 还可在内芯的2个边缘设2个V形的缺口，用2个缺口顶端的点来定位。可将查验位

置限定于缺口顶端的点的连线，这可提高定位精度、速度。每隔一定时间，可刻新的缺口，以增加攻击的难度。还可用不导电的涂料印上网格线等标记来定位，或在电阻材料外的不导电的材料表面印上金属线，用探针通过导电特性来定位。还可用氧化铁印上图案，并对其进行磁化，这就可用磁头来定位。若电阻材料的表面覆盖有钢铁，可直接对其进行磁化。以往的利用磁头来定位的技术，非常成熟，定位精度非常高，还价格低廉，故容易实现。而磁头可不与电阻材料接触，故不易磨损。

[0182] 对于币值较低的货币，可在内芯上设1定位用的衬有塑料的钢片(不衬塑料会改变电阻材料的导电特性等)，以下简称定位片，仅在其边缘上选择查验位置，这样虽会使查验位置的随机性下降，但定位精度较高，且定位速度较快，在要求不高的场合较适用。若用塑料制作定位片，它可能因温度变化而有较大的变形。可通过焊接、胶粘等方法，将定位片与内芯固定。每隔一定时间，可改变定位片的位置，以增加攻击的难度。定位片的位置，可不由计算机使用随机函数等随机生成，这样制造成本较低。

[0183] 当制造电阻材料的原料颗粒较小时，查验位置的细微变化，就会导致查验结果的较大变化，故需使定位精度较高。为降低定位精度、降低查验装置的成本、提高查验速度，可制作这样的双面电路板(以下简称靶板)：其1面有多个面积较大的扁平的(例如1平方毫米)的金属片(以下简称测靶)，参见图5c，其下端也有多个金属片(以下简称触靶)，有导线或过孔、金属箔等连接测靶与触靶，各测靶间是绝缘的，各触靶间也是绝缘的。在电阻材料的2面，分别装上1块靶板(上下方向相反)，这样探针只要接触到测靶即可进行查验，这可大幅降低定位精度要求。

[0184] 我们可这样制造靶板：制造多个横截面为长方形的塑料条，将其3面，用混合有铜(或其他金属，下同)粉的液体印刷上相隔特定距离的线条(为防氧化，铜粉可现做，可用铁轮磨粉，磨下的铁粉混进去也没关系)，再通过电镀的方法镀上较多的金属(形成较厚且强度较高的铜箔)，这样可快速、大规模地完成生产，这样形成的整体以下简称c板，参见图5d。这样每1条铜箔成c形，末端的2段，成为测靶、触靶，而测靶、触靶间有铜箔(以下简称导箔)连接，而各测靶、触靶间有足够的空间来绝缘。再将多个c板叠放在一起(可先涂胶)，再经加热、压制，形成一体，这就是一个有测靶、触靶、导箔的基板，而各测靶的位置、大小是特定的。

[0185] 我们还可这样做：制造多个横截面为长方形的塑料条，将其3面裹上铜箔，为使结合紧密可在塑料块上涂胶，再在其上压上网格状的橡胶，再浸入液体，将测靶等之外的部分腐蚀掉，再清洗干净，这就形成了c板。再将多个c板叠放在一起，再经加热、压制，形成基板。

[0186] 我们还可这样做：截取多个长方形的铜箔，再经过2次折压，形成c形，再切割下c形部分，中间放入塑料块(为使结合紧密可在塑料块上涂胶)，再切成(厚约1mm的)小块，再将多个这样的小块中塞上未裹上铜箔的小塑料块，组成1条，一起放至一定大小的塑料片上，这样也可形成c板，再将这些c板叠放在一起，经加热、压制形成一体。这种方法要多次切割，效率较低，我们还可使用多个刀片，1次切出多个小块。制造靶板的方法很多，我们还可用化学镀的方法在塑料条上镀上金属箔，其成本较高。当然也可在基板上钻孔，再在过孔上镀铜，成本较高，但过孔的位置可以是随机的，安全性较高。

[0187] 之后还可将测靶、触靶(露出表面的金属)再电镀上较多的铜、镍等金属以提高强度，可在这种基板上放置橡胶板，其上面有多个孔，被遮挡处不会镀上金属。镀过后，将该橡

胶板移除，橡胶板还可重复利用。触靶电镀用的橡胶板上的孔，可稍大于触靶，且形状各不相同，这可增加攻击的难度。之后还可对测靶镀锡等以防氧化。还可在表面粘上有多个孔的塑料膜来保护测靶，其孔的位置处于测靶之上，稍小于测靶。导箔的位置、形状固定虽对数据的随机性有害，但若测靶较多，查验位置的组合的数量也会非常庞大，就目前的复制技术而言，可近似地认为其接近于无限。

[0188] 为实现电阻材料与靶板的良好接触，可先在触靶上镀锡，加热、压制出电阻材料后，再将一定温度的电阻材料与靶板压在一起，这可使触靶上的锡(部分)融化，再冷却。也可在电阻材料被压制出后，待温度降低后，对其表面进行短暂的加热，再与靶板压在一起。这种融化的不确定性，也会对攻击带来很大的困难。触靶与电阻材料的接触处，是1个面，会使查验结果的随机性大幅提高，也使攻击的难度大幅提高。

[0189] 对币值较低的货币，可减少测靶的数量、增加各测靶的面积，以降低查验装置的成本、制造真密币(可采用丝网印刷的方法来印刷保护层，不用曝光)的成本等。测靶周围的绝缘部分较小，可使测靶的面积较大，探针碰到所要找的测靶的可能性会较大，但误碰到所要找的测靶周围的测靶的可能性也会较大，而且这会对印刷带来困难，使制造成本提高，故绝缘部分并不是越小越好，若其较大，可采用丝网印刷护膜，不用曝光，也不用清洗未曝光处，这对于币值较低的货币是较适用的。使用了测靶，我们就可不使用探针来进行查验，而探针的末梢较尖，容易损坏测靶，我们可用小的滚轮与靶板接触。此外，也可制作不采用靶板的不规则材料，其定位精度要求较高，故查验成本高，不易广泛采用，但对于银行卡、身份证等要求较高的场合适用。

[0190] 用电阻材料做货币，其硬度应较高，这才能寿命较长、不易变形，故厚度需较大。要用电阻材料做防伪标签，应能能进行弯折，因其粘贴处可能是不平的，这需将其厚度减少，且应减少石墨等不易弯折的材料、增加锡易弯折的材料。而靶板的基板，可选用易弯折的材料。

[0191] 查验真密币的装置以下简称查验机，通常它分4类，1类用于处理货币较多处，结构较复杂，以下简称网点终端；1类用于处理货币较少的小店等，只能对设有测靶的内芯进行查验，其结构较简单，即简易终端，其查验速度也很快；1类可由用户手工操作来进行定位，只能对设有测靶的内芯进行查验，以下简称手工终端，其成本很低，查验速度也较快；1类可自动或手工操作来进行定位，能对不设有测靶的内芯进行查验，以下简称精密终端，其成本稍高，查验速度慢，但精度高，可用于币值较高的货币及支票、银行卡等(见下文)。通常仅需使用设有测靶的内芯，只有对于币值较大等情况，才要使用没有测靶的内芯。个人收到货币，可能会怀疑其真假，即使是别人用查验机检验过也未必可靠，自己随身带1个手工终端就能放心了。

[0192] 网点终端分为分拣部分、查验部分等部分。分拣部分，分漏斗、传送带、机械手等，它可用单片机控制。通常可不用调整货币的方向。而网点终端的销量也较大，银行、大型商店等也很关心货币的真伪，其每天收到的货币数额巨大，即使假币的比例很低也会有很大的损失。货币从漏斗倒入，其横截面是三角形，1边垂直，下方有垂直、倾斜2条传送带，参见图7，若使用水平的传送带(齿状带)，货币容易卡在下方。漏斗下留有1个用于运出货币的V形的孔，高度可为1.4个货币的宽度，这样竖起的货币可被放倒，之后是1段水平的传送带，以下简称水平传送带，参见图8；其上有高约0.8货币厚度的齿，其前面有1个挡板，其空隙约

为1.5个货币厚度，这可使重叠的货币分开；2个齿的距离略长于货币的长度，故2个齿之间只有1个货币；其上方有1个可向后方旋转的刷子，使货币位于后面的齿前，这样可初步地确定货币的位置，便于处理。为便于机械手伸入抓在货币，可在牙上设空隙，传送带上也可设孔。

[0193] 实际中，客户投入货币时，投入的货币往往很多，不能马上查验完，需要先存储货币。此外查验货币常是先发出货币编号，再接收查验位置，之后才能得出查验结果，若对每1个货币都在发出编号后等待查验位置，会使处理速度较低，对此可先发出编号，再将货币存储，待收到查验位置再对相应货币进行查验。可这样存储货币：用类似子弹带的部件来存取货币，它是有多个孔隙的带状物，以下简称存取带，孔隙的大小、距离固定，参见图9，这样可随时在任何位置存取货币。存取货币的装置的结构类似于磁带，2端固定在2个卷轴上，再设置2个导辊，2个旋转方向分别用于存、取，参见图10。为便于确定存取位置，可在各孔隙旁设标记。为便于向孔隙中插入货币，可在存取带上设凸出部分。读取位置信息、货币编号、变换参数等的装置，可设在水平传送带上，若设在存取带等位置，会降低处理速度。

[0194] 查验货币时，先将内芯拉出，再利用内芯的边缘进行定位。之后根据货币的正反、左右，单片机对查验位置进行相应变换，再对探针调整位置，再进行查验。若货币是单面查验的则需调整货币的方向(双面查验不用，且探针位置的组合更多)，可用机械手分拣。为便于确定货币的方向，可在1角(如正面的左上角)设1孔，以下简称定向孔。水平传送带前面，是1个受币台，系统感受到有货币落入受币台，且基本到位后，4个推杆将货币准确地推至预定位置。根据定向孔决定旋转的方向。旋转部件分2部分，先是(对反面朝上者)垂直方向旋转的部分，之后是(对左右错误者)水平方向旋转部分，后者可向后方旋转，这样2者不会发生干扰。为使之不致相互妨碍，各只有2个夹子(如左与上、右与下)，工作完成后还需各自复位。正反左右皆错者，需进行2次旋转。仅需垂直方向旋转的货币，旋转后，可直接用机械手将货币送至上货口。通过机械手使货币处于特定的方向，成本高、处理速度较慢，故采用不调整方向的查验方法最好。

[0195] 对于手工终端、简易终端，可仅进行单面查验，先手工调整探针的位置，再将货币的内芯拉出，查验的1面朝下放入投币口，并调整位置。

[0196] 现在，电子货币(银行卡、虚拟支付账号所对应的电子形式的货币)的使用越来越多，因为其使用极为方便，而实体货币依然有一些优势，如价值可信(同1张银行卡所对应的资金的数额是不确定的，卖家不能确信其资金足以偿付货款)、不怕因中病毒或遭遇黑客攻击等原因使资金受损等，故依然有很强的生命力。尤其是在保护财产方面，其优势无可匹敌。银行看似强大，但其实非常脆弱，911事件中，很多银行都失去了客户数据。而建立灾难备份中心不仅费用高昂，还很难保证所有数据都准确无误。电子货币由于其自身形式的限制，很容易灭失、被篡改，而这些缺陷恰好可由实体货币来弥补。以往，实体货币很少有较大面值的，原因之1就是，这会激起极大的仿冒的欲望，而一旦仿冒成功，会造成巨大的危害，但现在情况变了，真密币的面值越大，保护财产的作用越大，完全可以面值1万、1百万，甚至根据客户的要求来确定面值(如235万)，这可弥补实体货币金额固定的缺陷。当然面值过大会不便使用，而随意确定面值会使安全性较低，需注意避免。真密币的使用(可与现在的实体的大额存单类似)，必须是联网的(而面值较大的真密币人们常会主动到可靠的服务站操作，而不会在路边的小店操作，故上述的接力的验证方法正好适用)，敌手不能直接使用它，

若其使用与操作者的身份验证相结合，则即使它被盗，小偷也不能使用它，这会暴露其身份，这是真密币的最重要的用处之1。

[0197] 为使用方便，可这样操作：各银行或央行，在每1个城市，设立1个专用的仓库(以下简称真密币库)，用户需存钱或付款，可向银行提出申请，真密币库将相应的金额的真密币的所有者改为当前的用户，再将这些真密币的新的查验位置、查验结果加密(为数字或二维码等)后，打印为纸质材料(以下简称证明材料，其作用类似于存单)，通过线下的途径递交给用户，用户可据此证明其为这些货币的所有者。为方便用户，纸质单据，可只存放于银行网点，用户可根据索引号来调取单据，也可使用U盾等进行远程操作。以纸质单据，作为根本的操作依据，大大减少了数据灭失的可能性。当然也可通过线上途径加密传输，由于加密对象是真随机的，即使简单加密也难以破解。证明材料可传递至相应的服务站，让用户自提。用户付款，需将原来的证明材料交付银行，就像兑付存单1样。证明材料是对真密币的1种凭据，通过它进行电子化的操作，较方便，若让用户亲自将真密币交付收款人，不仅麻烦，还不安全。让真密币位置不变，但权属改变，不仅方便还安全。而使用真密币的操作者，都需表明身份，并进行可靠的核查(例如使用银行卡、身份证等)，以提高安全性。以真密币作为代表价值的介质，比磁带、硬盘等(以往银行)用来存储数据的介质，可靠得多。以往的电子货币，数据很容易灭失。而真密币则不同，若真密币存于仓库里，真密币是不易损坏的，而用户保存的纸质凭证也不易灭失。若用户自己保存真密币，银行会保存纸质的凭据，或实时将数据刻录在光盘上，故不易灭失。实体货币、电子货币各有利弊，只有将实体介质与信息化合理地融合，才能够真正获得成功。

[0198] 很多人会不愿使资金闲置，要将资金存入银行，对此可将大额的真密币，作为存款的本金。若银行要对存款进行放贷，可用真密币为抵押来获得资金，并登记使用这些货币的人的信息。

[0199] 以往人们经常用支票、汇票等票据汇划资金，其实真密币也可起同样的作用，具体方法是：我们可生产查验真密币的精密终端等(其计算、联网等功能可借用客户的电脑、手机来完成)，由客户自行完成操作，这种终端的价格较低，故易于推广。客户先到服务站(以下简称出币点)领取若干真密币，出币点(可事先)随机确定并记录多组(用做口令、加密密钥、核对金额的密钥的)查验位置、查验结果，这些查验位置以下简称口令位置、加密密钥位置、核对密钥位置，并将真密币交给客户。客户要汇出资金时，取出1个真密币，并将其编号发给出币点，出币点返回口令位置，客户用精密终端据此得出口令，并返回出币点，口令验证通过后，出币点返回加密密钥位置、核对密钥位置，精密终端据此得出加密密钥，客户将收款人的账号、金额等信息输入电脑，将收款账号等加密发往出币点，出币点经过解密得出收款账号等，并用核对密钥将收款账号等加密返回，精密终端根据核对密钥位置得出核对密钥，将账号等解密后，与记录对比，若与之相符，向出币点返回验证通过的应答，出币点再完成资金的支付(例如向现代化支付系统发出支付指令等)，支付成功后返回支付成功的应答。此外真密币还可起以往的发票等的作用：税务局或银行向企业交付真密币，报税时企业用真密币完成操作。

[0200] 使用真密币传递口令、密钥，比用纸质单据、电子证书、U盾等安全得多，它集电子操作的便利，与实体介质的安全性于一身，因此价值很大，其作用可以说是很神奇的。

[0201] 当然，上述的防伪支付的方法，也可不用U盘来传递口令、密钥，而用不规则材料来

传递。

[0202] 6.会员卡、银行卡、身份证等

[0203] 不规则材料用于会员卡等，非常合适。会员卡通常只在同1个地点使用，这样每次验证后，可直接由同1个服务器随机生成新的查验位置，并记录查验结果，这样新的查验位置、查验结果就可不在网络上泄露，这就不需存储较多的防伪信息，故存储成本较低。

[0204] 不规则材料，也可用于制作银行卡，以下简称真密卡。以往的磁介质的银行卡，容易仿制，已被逐渐淘汰，人们开始用芯片卡来取代之，但芯片卡的生产成本较高、验证成本也较高，而且理论上只要破解了相关的密钥等(尤其是在量子计算的技术获得成功后)，芯片卡也是能仿制的，但真密卡的制造成本很低，仿制非常困难，验证成本也较低，因此优势很大。若真密卡仅在同1个地点使用，其使用方法可与上述的会员卡的使用方法相同。若在网上进行操作，为防不规则材料多次使用而使验证数据泄露，可再使用真密币发出口令来验证身份。

[0205] 若真密卡在不同的地点(银行网点或终端机)使用，可这样做：发行时在真密卡的发行单位(工厂或银行)对1张卡随机确定1个查验位置，并得出查验结果，再将该其与卡号存储于发行单位；第1个使用该卡的网点，向发行单位发出验证请求，发行单位收到该请求后，返回查验位置，该网点根据该查验位置得出查验结果，并返回发行单位，发行单位据此得出验证结果，并返回中央服务器，中央服务器再向该网点转发该消息，该网点收到该消息后，随机确定1个新的查验位置，并得出查验结果，再将其与卡号存储于该网点的服务器；之后，每次验证，都是向上1个网点发出验证请求，上1个网点返回查验位置，得出查验结果后，再由上1个网点完成验证，并返回验证结果；验证通过后，再生成新的查验位置，并记录查验结果。在每1次验证前，查验位置、查验结果是没有公开于网络上的，故即使真密卡被盗，敌手也无法得出有用数据，使用真密卡传递信息是高度安全的。而发出验证请求，必须标出网点的编号，真实的网点也会收到相关信息，并作出反应，故假的网点服务器很难实施欺骗(骗得查验位置、使用伪卡等)。

[0206] 真密卡也可用来传递密钥、口令等。当1张真密卡在1个可靠的网点验证通过后，该网点的服务器随机生成2个(组)新的查验位置(以下简称密钥位置、口令位置)，得出的查验结果经过一定的处理后(例如使数据的位数固定等)，分别作为密钥、口令。下1次用户使用真密卡时，用该密钥对转账的金额、账号等进行加密。该口令可用于服务器返回确认信息时，表明身份，防范敌手的伪装。

[0207] 若用户不想到银行操作，想在家完成操作，还可这样做：用户将其真密卡交给银行，银行的设备随机确定多个查验位置，并记录查验结果，用户回家，使用精密终端、手工终端完成操作。若同1个真密卡被多次使用，同1个查验位置被再次使用的几率就会较高，这会增加安全风险。对此，我们还可这样做；用户事先到出币点领取多个真密币，出币点将这些真密币的信息与该用户的账号绑定，用户回家操作时，先用真密卡来表明身份，再用真密卡进行加密等。这样可将电子支付的便利与实体介质的安全结合在一起，将可能使银行卡迎来1个新的时代。

[0208] 若用户没有手工终端等，可到服务点借用，为提高安全性，可不由服务点发出查验结果等，仅通过用户的手机发出查验结果等，这可防止敌手盗用查验结果(主要是加密密钥)等。

[0209] 相对于真密币(实体货币),真密卡的优势,在于支付数额可变。以往,现金往往用于小额支付,大额的支付很多采用电子途径(尤其是通过银行完成)。而也许,未来真密卡主要用在小额的(电子)支付,(实体的)真密币用在大额支付,正好与现在完全相反。

[0210] 现在,电子支付的使用越来越广泛,而很多电子支付是预储值支付(从预储值账户中划拨资金),每1次预储值支付可能是很安全的(例如上述的防伪支付的技术),但预储值账户内的资金通常要从银行卡中转入,这个环节是风险较大的环节,而一旦敌手能够得手,盗取的资金就可能非常多。以往还没有较完善的支付平台与银行系统之间进行转账的技术,而在这个环节使用不规则材料可大幅提高安全性。各银行可发行用不规则材料制作的充值卡,发出充值卡前随机确定多组查验位置并记录查验结果,将查验结果分别作为口令、加密充值金额的密钥、加密返回接收结果的密钥等(相应的查验位置以下简称为口令位置、充值密钥位置、返回密钥位置等),之后充值卡通过安全的途径传递给各服务站;用户充值时,先在服务站验明身份(可采用以往的技术,也可使用真密卡),再发出充值请求(包括卡号);银行根据卡号,调出口令位置、充值密钥位置、返回密钥位置,并发往该服务站;服务站根据这些位置,得出查验结果,并根据查验结果,对充值金额、相关账号进行加密,并发往银行;银行完成充值后,对充值金额用返回密钥加密并返回服务站;服务站根据返回密钥得出解密密钥,并对返回的密文进行解密,若金额与记录相符,向用户发出充值成功的通知。若有多个用户从同1个银行进行充值,可1次使用多个加密密钥。当然,也可直接使用真密卡来操作(不采用专门的充值卡),而以往所谓的银行卡,通常只用于银行间的转账,这种真密卡确切地说已不是银行卡。

[0211] 此外不规则材料,也可作为证明身份的证件。现在,在很多重要的场合,人们使用指纹作为判断个人身份的依据。但指纹是1种静态的事物,故敌手可使用橡胶等材料来复制指纹,进行欺骗。在更重要的场合,人们也使用智能卡来证明身份,它生成的口令是变化的,但其口令往往用固定的算法生成,是有规律可循的,故也可能被破解。若用不规则材料制作身份证明(以下简称真密证),则可使用直随机的口令、密钥,这样敌手就无法破解之。而它与智能卡的本质区别之1是,其数据是用特别的介质生成的,而这种介质是难以复制的,尤其在线下的验证场合中,敌手是根本无法通过以往的电子设备实施欺骗的,以往的黑客通过破解密钥等方法实施攻击的情况就不会发生了,这是目前在线下的环境中验证个人身份的最安全的技术,它将在国家安全、国防等领域有广泛而重要的应用。而以往的护照等成本高,真密证成本低很多。不规则材料,是1种新生事物,它的很多特性及用处,现在人们还很不了解。

## 附图说明

[0212] 图1部分的不规则材料的俯视图

[0213] 图2a基材透明的部分的不规则材料的剖视图

[0214] 图2b基材不透明的部分的不规则材料的剖视图

[0215] 图3a划痕标签的剖视图

[0216] 图3b划痕标签的俯视图

[0217] 图4分成多个部分的筛子的示意图

[0218] 图5a内芯拉出时的真密币的正视图

[0219] 图5b内芯的放大图

[0220] 图5c测靶的示意图

[0221] 图5d c板的结构示意图

[0222] 图6护套的横剖面图

[0223] 图7网点终端的漏斗的立体图

[0224] 图8水平传送带的示意图

[0225] 图9存取带的示意图

[0226] 图10存取货币的装置的结构的示意图

[0227] 图11一种商品的真伪验证、支付过程的方框图

[0228] 其中:定位纤维或印刷的线条1颗粒或涂料2透明的基材3胶黏剂4保护膜5不透明的基材6缺角6固定孔7护套8信息区9铁片10不规则材料11缺口12校准边13起始边14磁铁15传动部分16测靶17金属箔18防滑脱槽19放置内芯的槽20漏斗21 V形的孔22水平传送带23挡板24齿25空隙26刷子27凸出部分28孔隙29标志30卷轴31导辊32存取带33买家登录自有平台提交订单34自有平台向联控中心发出订单35联控中心收到订单后向代理平台发出划拨定金的指令36代理平台做出回应37联控中心收到上述信息后将订单信息等发往通知端38在发出该商品时,通知端将该商品使用的防伪码等打印在标签上,将相应的不规则材料置于包装上或交付物流公司39商品送到服务站后柜员将商品信息发往该买家的手机40买家的手机给出对比结果后买家在手机上点击“确认订单并开始验证”向联控中心发出验证请求41联控中心向买家的手机发出挑战请求42买家的手机将A挑战值发往联控中心43联控中心将A应答值发往买家的手机44若联控中心只收到1个A挑战值,联控中心向该买家的服务站发出“开始验证”的通知45服务站收到“开始验证”的通知后将防伪码等加密发往联控中心46联控中心将其转发给代理平台47代理平台完成验证后向联控中心返回查验位置48联控中心将其转发给服务站49服务站得出查验结果并返回联控中心50联控中心再将其转给代理平台51若验证结果是“通过”代理平台划拨余款及物流费用、代理费用并向联控中心返回支付成功的应答52联控中心向相应的服务站返回上述应答53该服务站收到该应答后向相应的买家传达该应答并派人将货物递交给买家54

## 具体实施方式

[0229] 以下提出1种防伪支付的流程,它通过代理平台进行防伪码的验证,使用不规则材料、挑战验证法,用户在家收取商品,参见图11。

[0230] 代理平台,依序确定防伪码的编号b,并针对该编号,生成真随机的防伪码J1,加密为J2;

[0231] 代理平台,找出一定数量的不规则材料,随机确定查验位置,得出查验结果,记录不规则材料的编号x、查验位置、查验结果,并将x与一定的b对应;将b、J2、x复制到防伪U盘中,记录U盘的编号及其中包含的b、x的范围,再派人将存储多个b、J2、x的U盘,及相应的不规则材料,以线下的途径送至服务站,让各卖家派人领取U盘、不规则材料;卖家收到代理平台送来的U盘后,工作人员将防伪U盘,与通知端连接,将数据载入,通过通知端回传U盘的编号;

[0232] 代理平台,生成真随机的买家口令mk,并依序确定其编号,将mk及其编号复制到买

家口令U盘中，记录U盘的编号，及(装有多个)U盘的包装的编号，及其中包含的U盘的编号的范围，再派人将其以线下的途径送至服务站；服务站的工作人员将买家口令U盘，与服务器连接，将数据载入；

[0233] 买家在进行电子购物时，使用其手机或电脑，通过专用的软件，登录自有平台(可手工输入用户名Y、密码登录，也可自动登录)，在自有平台上，提交要购买的商品的类别、用途，及商品的商标、商品名称、商品的规格、公司的名称、公司的地址等方面的信息；自有平台返回一个该类别的商品的列表，其中列出相似的商标、商品名称、公司的名称，及产品的介绍、公司的地址、联系方式、卖家名等；该买家根据该列表，确定其要购买的商品的卖家名，再直接在该平台上针对该卖家名提交订单(包括服务站号N、卖家名C、Y等，N可由联控中心自动填写，买家可修改之)；买家提交订单后，该专用软件记录商品的名称、商标、卖家名、规格、款式、金额、单位、数量、订单提交时间等信息；

[0234] 联控中心收到订单后，对订单进行审核，若通过，向代理平台发出划拨定金的指令，若该买家的防伪支付账户内的资金不足，通知买家充值；完成定金的划拨后，代理平台在该通知端当前未用的防伪码中，随机确定1个防伪码编号b，随机确定1个订单号H1并加密为H2，相应确定不规则材料的编号x，并将b、H2返回联控中心；联控中心收到上述信息后，将订单信息及该防伪码的编号、加密的订单号H2、及定金已支付的信息，发往通知端；

[0235] 通知端收到订单信息后，检查商品的价格，若与预先设定的价格相符，向仓库、车间等部门发出通知，找出、生产出、购进商品，若与预先设定的价格不符，提出异议；在发出该商品时，通知端根据收到的防伪码编号b，从U盘中调出数据，确定该商品使用的防伪码的密文J2，及不规则材料的编号x，将J2加密为J3，将H2加密为H3，并在发货时，将b、J3、H3、服务站号N、卖家名C、买家的用户名Y等打印在标签上，将相应的不规则材料置于包装上或交付物流公司；同时通知端将防伪码的编号、商品的编号，加密发往联控中心；

[0236] 商品送到服务站后，由柜员对商品进行检查，若该商品的买家名，确实是该服务站所服务的买家的用户名，根据用户名，从服务器中调出相应的用户的手机号，将商品的种类、价格、卖家名等，附上一个流水号，加密发往该买家的手机；买家的手机上的软件，将其与记录进行对比，并给出对比结果，若对比结果是“该订单信息与记录相符”，同时显示“确认订单并开始验证”的按钮，若对比结果是“该订单信息与记录不符”，不显示“确认订单并开始验证”的按钮，显示“否认订单”按钮；若对比结果是“该订单信息与记录相符”，买家在手机上点击“确认订单并开始验证”，手机向联控中心发出验证请求信息，否则点击“否认订单”按钮，中止流程；

[0237] 联控中心收到该验证请求信息后，生成一个挑战请求，向买家的手机发出；买家的手机，收到联控中心发来的挑战请求后，生成一个真随机的A挑战值，将其发往联控中心，同时，买家的手机由A挑战值也生成一个B应答值；若联控中心收到2或更多个不同的A挑战值，则向买家的手机发出“有敌手在攻击”的提示信息，并中止流程；联控中心收到A挑战值后，进行加密而生成一个A应答值，并发往该买家的手机；若买家的手机收到的联控中心发来的A应答值，与B应答值不同，或收到2或更多个不同的A应答值，则向联控中心发出“有敌手在攻击”的信息，联控中心收到该信息后，向相应的服务站、卖家发出“有敌手在攻击”的信息，向该手机发出“已中止流程”的信息，并中止流程；若联控中心只收到1个A挑战值，也没有收到买家的手机发来的“有敌手在攻击”的信息，联控中心向该买家的服务站发出“开始验证”

的通知信息(包括上述的流水号)；

[0238] 服务站收到“开始验证”的通知信息后，由柜员打开包装，找出防伪码标签，将b、J3、H3等录入服务器，服务器将b、J3、H3等一起加密(我J4、H4等)发往联控中心，联控中心再将其转发给代理平台；由代理平台完成防伪码编号、防伪码、订单号等信息的验证，并向联控中心返回验证结果，若验证通过，还同时向联控中心返回相应的不规则材料的查验位置；服务站收到查验位置后，得出查验结果，并返回联控中心；联控中心再将其转给代理平台；代理平台，根据记录进行验证，并将验证结果返回联控中心；若联控中心收到的验证结果是“通过”，联控中心根据相应的订单的卖家的用户名，转换出该卖家的收款账号，并向代理平台发出，划拨余款及物流费用、代理费用的支付指令；若支付成功，代理平台或银行向联控中心返回支付成功的应答，否则返回支付不成功的应答；联控中心收到支付成功的应答后，向相应的服务站返回上述的验证通过、支付成功的应答，也向相应的所述的设在卖家处的用于联系的终端发出上述的验证通过、支付成功的应答；该服务站收到该应答后，向相应的买家传达该应答，并与买家约定送货时间、地点，录入服务器；

[0239] 派出送货员前，由服务站的服务器，针对每一件商品随机生成取货验证码、开锁的密码；柜员再根据情况，人工指定送货员的编号、密码箱编号；柜员再调出相应的站点口令并打印出来；柜员再将货物，及打印出的相应的站点口令的纸质文件，一起锁在密码箱中，并根据服务器的指令，设定开锁的密码；由服务器将取货验证码、送货员编号、密码箱编号、密码箱的开锁密码，一起发往相应的买家的手机；送货员见到买家后，先出示标有送货员的编号的工作证，买家根据收到的送货员的编号，核实送货员的身份；买家核实送货员的身份无误后，送货员再请买家出示取货验证码、用户名、证明身份的证件，来核实买家的身份；核实买家的身份后，送货员向其递交相应的密码箱，买家核实密码箱的编号后，用收到的开锁密码打开密码箱，对站点口令进行核实，再对货物进行核实，若货物无误，用手机生成1个工作验证码，由买家用手机将该验证码发往相应的服务站，也将其告诉送货员；送货员回到服务站后，将工作验证码告知柜员，若其与记录相同，系统确认货物已送到。

[0240] 上述的流程，安全性非常高，对于价值较高的商品，是非常适合的，而对于价值稍低的商品，我们也可仅将不规则材料、真随机的防伪码、电子支付结合起来。而现在有不少人对手机不信任，在服务站完成操作，较容易获得信任。而防伪码是由买家直接提交，容易取得其信任。而加密用户名等的工作，可由其手机完成。

[0241] 而对于价值较低的日用品等，我们可使用更简单的流程，也可不使用不规则材料。

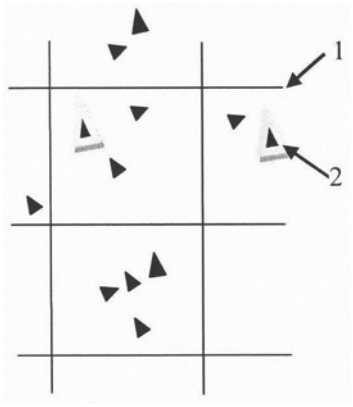



图1

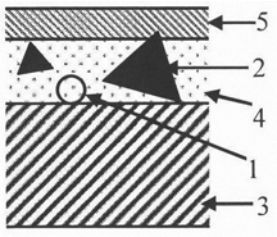



图2a

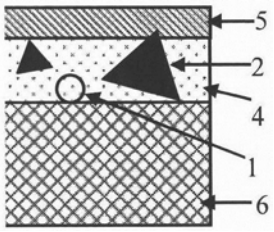



图2b

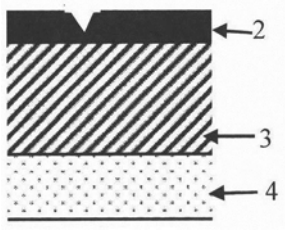



图3a

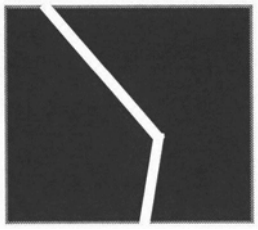


图3b

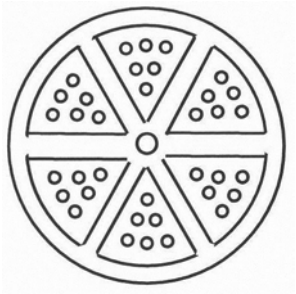


图4

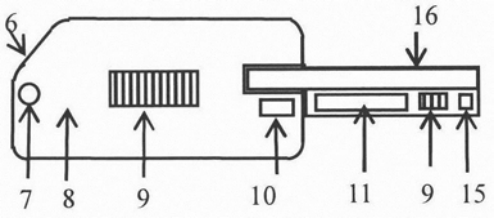



图5a

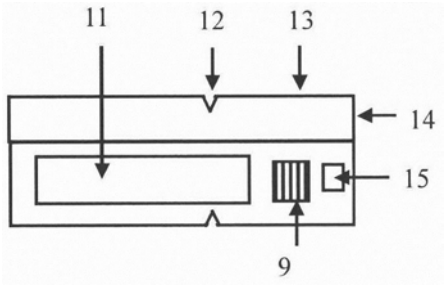



图5b

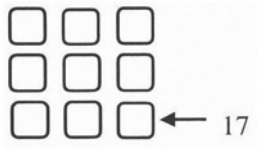



图5c

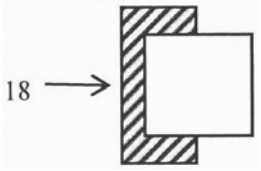



图5d

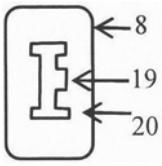



图6

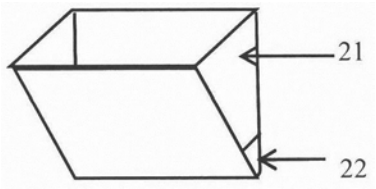



图7

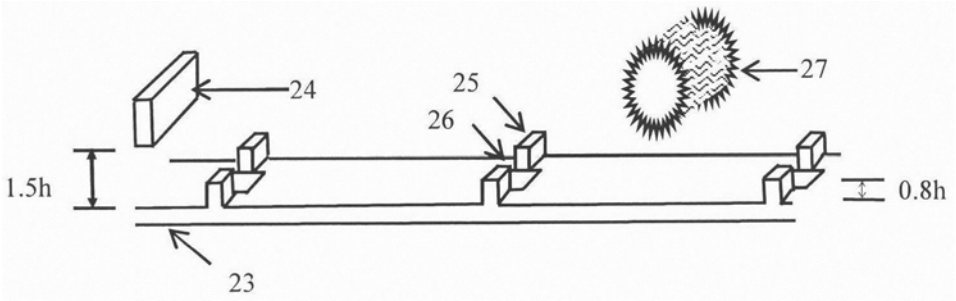



图8

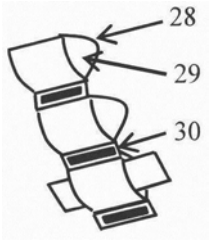

28
29
30

图9

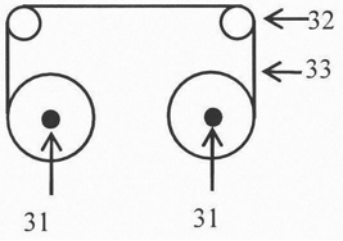

32
33
31
31

图10

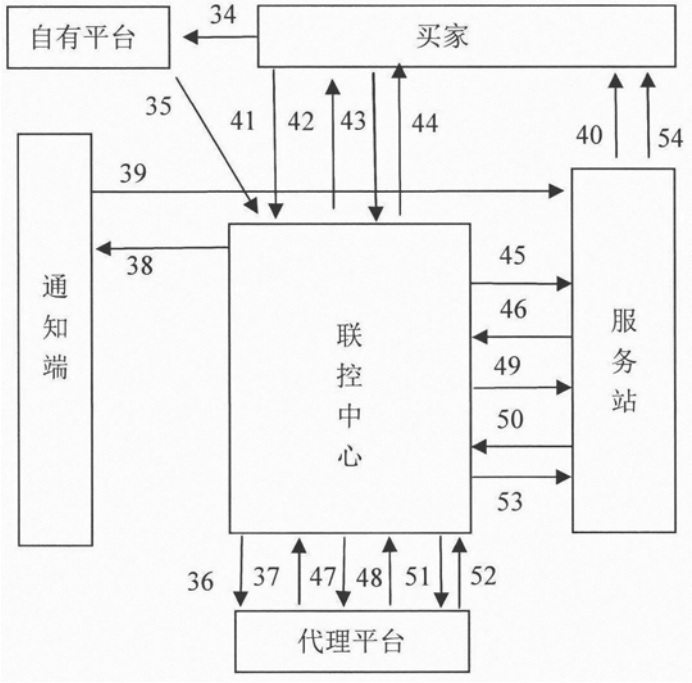

自有平台
34
买家
35
41
42
43
44
40
54
39
通知端
38
联控中心
45
46
49
50
53
服务站
36
37
47
48
51
52
代理平台

图11