**关于信息安全解决方案之一区块链技术的应用及扩展**

我国信息安全管理的现状

信息安全管理是随着信息和信息安金的发展而发展的。在信息社会中，一方面信息已经成为人类的重要资产，在政治、经济、军事、教育、科技、生活等方面发挥着重要作用，另一方面由于计算机技术的迅猛发展而带来的信息安全问题正变得日益突出。由于信息具有易传播、易扩散、易损毁的特点，信息资产比传统的实物资产更加脆弱，更容易受到损害，这样将使组织在业务运作过程巾面临巨大的风险。这种风险主要来源于组织管理、信息系统、信息基础设施等方面的固有薄弱环节和漏洞， 以及大量存在于组织内外的各种威胁， 因此对信启、系统需要加以严格管理和妥善保护，信息安全管理也随之产生。

解决方案之区块链技术

区块链技术中采用了密码学，这样也是保护数字资产不会被轻易窃取，当然目前区块链技术还不是很成熟，所以数字货币在安全方面也是值得推敲的，区块链技术也是一种高度密集工程，所以在运作的过程中也难免会出现错误，而且即便是理论上很完备的算法，也会有各种实现上的错误。区块链本身强大的信息存储和共享机制也是给信息安全带来了保障，密码学也为区块链在实际应用场景中解决了诸多了问题，所以区块链对于信息安全还是起到很大作用的，为了应用也会更加的广泛。

　　区块链对于信息安全行业的意义体现在以下三点：

**一、用户身份认证保护**

　　非对称式公私钥加密技术采用两套密钥系统，比对称式加密更安全，多数公钥加密在PKI平台上实施，易被黑客假冒身份，WhatsApp漏洞正是被黑客发送假密钥实施中间人攻击。

　　区块链则可以构建一个全新的身份管理系统，商务密邮采用的身份标识算法，让篡改难以隐匿，从而有效防范身份伪造。

**二、数据完整性保护**

　　传统的加密算法，一旦遭到中间人篡改攻击，网络中的参与者无法及时感知，在一些企业的交易邮件中时常发生类似的事情：发件人邮箱地址没有问题，但收款账户却被篡改了，而这种邮件诈欺通常在损失已形成后才被察觉。

　　美国国防部DARPA高级研究计划局正在考虑使用区块链来保护敏感的军事数据。区块链利用哈希算法存储数据，数据区块之间互为连结，某一处数据篡改，都会引起区块序列值的变更，再庞大的网络，也能轻易找到篡改来源。

**三、有效阻止DDoS攻击**

　　变本加厉的DDoS攻击令企业望而生畏，一场高级的DDoS攻击甚至可以轻松搞垮一家大型企业，这也正是黑客尝试进行大规模破坏的首选。

　　区块链的分布式存储架构则会令黑客无所适从，已经有公司着手开发基于区块链的分布式互联网域名系统，绝除当前DNS注册弊病的祸根，使网络系统更加干净透明。

　　区块链技术具备的出众安全特点，为巩固信息安全提供了全新的发展方向，区块链+商务密邮从数据本身进行源头处理，将传统邮件的单一边界式防护，升格为全网络数据节点共同防护的新型防泄密模式，结合国际级的加密算法，令企业用户的邮件安全得到更有效、更全面的保障。

以上就是关于区块链信息安全的相关介绍了，信息安全关乎我们的财产和生命安全，所以值得人人重视，区块链本来就是一个安全并且透明的生态环境，可以有效的遏制信息被泄露，这样我们的信息就像被放在了保险箱中一样，不用担心信息被盗用和窃取了。

区块链技术的应用场景

**一、应用场景：信息共享**

这应该是区块链最简单的应用场景，就是信息互通有无。

**1、传统的信息共享的痛点**要么是统一由一个中心进行信息发布和分发，要么是彼此之间定时批量对账（典型的每天一次），对于有时效性要求的信息共享，难以达到实时共享。

信息共享的双方缺少一种相互信任的通信方式，难以确定收到的信息是否是对方发送的。

**2、区块链 + 信息共享**

首先，区块链本身就是需要保持各个节点的数据一致性的，可以说是自带信息共享功能；其次，实时的问题通过区块链的P2P技术可以实现；最后，利用区块链的不可篡改和共识机制，可构建其一条安全可靠的信息共享通道。

也行你会有这样的疑问：解决上面的问题，不用区块链技术，我自己建个加密通道也可以搞定啊！但我想说，既然区块链技术能够解决这些问题，并且增加节点非常方便，在你没有已经建好一套安全可靠的信息共享系统之前，为什么不用区块链技术呢？

**二、应用场景：版权保护**

**1、传统鉴证证明的痛点**

流程复杂：以版权保护为例，现有鉴证证明方式，登记时间长，且费用高。

公信力不足：以法务存证为例，个人或中心化的机构存在篡改数据的可能，公信力难以得到保证。

**2、区块链 + 鉴证证明**

流程简化：区块链应用到鉴证证明后，无论是登记还是查询都非常方便，无需再奔走于各个部门之间。

安全可靠：区块链的去中心化存储，保证没有一家机构可以任意篡改数据。

**三、应用场景：物流链**

商品从生产商到消费者手中，需要经历多个环节（流程可能如上图所示），跨境购物则更加复杂；中间环节经常出问题，消费者很容易购买的假货。而假货问题正是困扰着各大商家和平台，至今无解。

**1、传统是防伪溯源手段**

以一直受假冒伪劣产品困扰的茅台酒的防伪技术为例，2000年起，其酒盖里有一个唯一的RFID标签，可通过手机等设备以NFC方式读出，然后通过茅台的APP进行校验，以此防止伪造产品。 咋一看，这种防伪效果非常可靠。但2016年还是引爆了茅台酒防伪造假，虽然通过NFC方式验证OK，但经茅台专业人士鉴定为假酒。后来，在“国酒茅台防伪溯源系统”数据库审计中发现80万条假的防伪标签记录，系防伪技术公司人员参与伪造；随后，茅台改用安全芯片防伪标签。

但这里暴露出来的痛点并没有解决，即防伪信息掌握在某个中心机构中，有权限的人可以任意修改。（备注：茅台的这种防伪方式，也衍生了旧瓶回收，旧瓶装假酒的产业，防伪道路任重而道远）。

2017年05月贵阳数博会上，小马哥就建议茅台防伪使用区块链；

**2、区块链+物流链**

区块链没有中心化节点，各节点是平等的，掌握单个节点无法实现修改数据；需要掌控足够多的节点，才可能伪造数据，大大提高伪造数据的成本。

区块链天生的开放、透明，使得任何人都可以公开查询，伪造数据被发现的概率大增。

区块链的数据不可篡改性，也保证了已销售出去的产品信息已永久记录，无法通过简单复制防伪信息蒙混过关，实现二次销售。

物流链的所有节点上区块链后，商品从生产商到消费者手里都有迹可循，形成完整链条；商品缺失的环节越多，将暴露出其是伪劣产品概率更大。

四、应用场景：供应链金融

**1、传统的供应链单点融资**

在一般供应链贸易中，从原材料的采购、加工、组装到销售的各企业间都涉及到资金的支出和收入，而企业的资金支出和收入是有时间差的，这就形成了资金缺口，多数需要进行融资生产。我们先来看个简单的供应链

**2、区块链+供应链金融**

面对，上述供应链里的中小微企业融资难问题，主要原因是银行和中小企业之间缺乏一个有效的信任机制。

假如供应链所有节点上链后，通过区块链的私钥签名技术，保证了核心企业等的数据可靠性；而合同、票据等上链，是对资产的数字化，便于流通，实现了价值传递。

如上图所示，在区块链解决了数据可靠性和价值流通后，银行等金融机构面对中小企业的融资，不再是对这个企业进行单独评估；而是站在整个供应链的顶端，通过信任核心企业的付款意愿，对链条上的票据、合同等交易信息进行全方位分析和评估。即借助核心企业的信用实力以及可靠的交易链条，为中小微企业融资背书，实现从单环节融资到全链条融资的跨越，从而缓解中小微企业融资难问题。

**3、应用案例**

比较成熟的还没看到，目前腾讯也已入局。

## 五、应用场景：跨境支付

**1、传统跨境支付**

跨境支付涉及多种币种，存在汇率问题，传统跨境支付非常依赖于第三方机构，大致的简化模型如上图所示，存在着两个问题；

流程繁琐，结算周期长：传统跨境支付基本都是非实时的，银行日终进行交易的批量处理，通常一笔交易需要24小时以上才能完成；某些银行的跨境支付看起来是实时的，但实际上，是收款银行基于汇款银行的信用做了一定额度的垫付，在日终再进行资金清算和对账，业务处理速度慢。

手续费高：传统跨境支付模式存在大量人工对账操作，加之依赖第三方机构，导致手续费居高不下，麦肯锡《2016全球支付》报告数据显示，通过代理行模式完成一笔跨境支付的平均成本在25美元到35美元之间。

**2、区块链+跨境支付**

这些问题的存在，很大原因还是信息不对称，没有建立有效的信任机制。

如上图所示，区块链的引入，解决了跨境支付信息不对称的问题，并建立起一定程度的信任机制；带来了两个好处。

效率提高，费用降低：接入区块链技术后，通过公私钥技术，保证数据的可靠性，再通过加密技术和去中心，达到数据不可篡改的目的，最后，通过P2P技术，实现点对点的结算；去除了传统中心转发，提高了效率，降低了成本（也展望了普及跨境小额支付的可能性）。

可追溯，符合监管需求：传统的点对点结算不能不规模应用，除了信任问题，还有就是存在监管漏洞（点对点私下交易，存在洗黑钱的风险），而区块链的交易透明，信息公开，交易记录永久保存实现了可追溯，符合监管的需求。

## 六、应用场景：资产数字化

**1、实体资产存在的问题**

实体资产往往难以分割，不便于流通

实体资产的流通难以监控，存在洗黑钱等风险

**2、区块链实现资产数字化**

资产数字化后，易于分割、流通方便，交易成本低

用区块链技术实现资产数字化后，所有资产交易记录公开、透明、永久存储、可追溯，完全符合监管需求

## 七、应用场景：代币

本来不像把代币加进来的，但说到区块链，始终绕不开代币；因区块链脱胎于[比特币](http://www.elecfans.com/tags/比特币/)，天生具有代币的属性，目前区块链最成功的应用也正是[比特币](http://www.elecfans.com/tags/比特币/)。

**1、传统货币存在的问题**

传统的货币发行权掌握在国家手中，存在着货币滥发的风险

元朝自1271年建立后，依然四处征战，消耗大量的钱财和粮食，为了财政问题，长期滥发货币，造成严重通货膨胀，多数百姓生活在水生火热中，导致流民四起，国家大乱，1368年，不可一世的元朝成了只有97年短命鬼，走向了灭亡。

1980年津巴布韦独立，后因土改失败，经济崩溃，政府入不敷出，开始印钞；2001年时100津巴布韦币可兑换约1美元；2009年1月，津央行发行100万亿面值新津元（如下图）加速货币崩溃，最终津元被废弃，改用“美元化”货币政策。2017年津巴布韦发生政变，总统穆加贝被赶下台。

**2、区块链如何解决这些问题**

比特币解决了货币在发行和记账环节的信任问题，我们来看下比特币是如何一一破解上面的两个问题。

滥发问题：比特币的获取只能通过挖矿获得，且比特币总量为2100万个，在发行环节解决了货币滥发的问题； 账本修改问题：比特币的交易记录通过链式存储和去中心化的全球节点构成网络来解决账本修改问题。

链式存储可以简单理解为：存储记录的块是一块连着一块的，形成一个链条；除第一个块的所有区块都的记录包含了前一区块的校验信息，改变任一区块的信息，都将导致后续区块校验出错。因为这种关联性，中间也无法插入其他块，所以修改已有记录是困难的。

而去中心化节点可以简单理解为：全球的中心节点都是平等的，都拥有一模一样的账本，所以，任一节点出问题都不影响账本记录。而要修改账本，必须修改超过全球一半的节点才能完成；而这在目前看来几乎不可能。 既然账本无法修改，那要是记账的时候作弊呢？ 首先，比特币的每条交易记录是有私钥签名的，别人伪造不了这个记录。你能修改的仅仅自己发起的交易记录。

其次，是关于记账权问题：比特币的记账权，通过工作量证明获得，可以简单理解为：通过算法确定同一时刻，全球只有一个节点获得了记账权，基本规律是谁拥有的计算资源越多，谁获得记账权的概率越大，只有超过全网一半的算力，才可能实现双花。

备注：比特币的模式是不可复制的，比特币已经吸引了全球绝大多数的算力，从而降低51%攻击发生等问题；其他的复制品基本无法获得相应的算力保证。

目前，比特币还存在着51%和效率低等问题有待解决，另外，关于交易本身的信任问题是个社会问题，比特币是没有解决的，也解决不了的。