基于网络交易的区块链安全技术研究

文丨焦锋

随着网络技术的发展，目前网络购物已经成为了一种趋势，基本上平均每周每人就会有一次网购，且网络支付也日益平常化。目前提倡无现金消费文化，年轻人出门带现金的习惯越来越少。因此，如何安全的进行网络在线支付是一个值得研究的问题。本文主要对当下比较流行的区块链技术进行研究。

一、引言

若干年前，比特币诞生了，当时的技术和经济环境还没有对它引起足够的重视，然而现在比特币的价值已经在3万元人民币一个左右。为什么它的存在能有这么大的价值，作为一种数字货币，它所存在的意义又是什么呢？比特币作为众多数字货币中的一种，之所以有这么大的价值，是因为它使用了一种可以代替第三方作为信任机构的技术，就是区块链技术。时下盛行的二维码支付，各种第三方网络支付机构的出现，无现金文化的提倡等等，涌现出了支付安全问题。区块链技术开始被人们所重视，尤其是京东、阿里这种巨无霸的网购平台。

二、网络交易存在的问题

从网购诞生到现在为止，站在人们面前最为严重的问题就是信任问题。为了解决这个问题，京东提出了自营策略，希望通过自身的信誉来解决客户的信任问题。阿里则通过支付宝第三方担保的手段，试图解决该问题。然而，这些方法无法从根源上解决信任危机。因此，就有了本文要研究的区块链技术，也就是当前最火的比特币所使用的技术。下面重点对区块链技术进行说明。

三、区块链技术

简单来说，区块链就是一种分布式的账本技术。它采用密码学的方法，确保自身的数据不会被篡改，然后又使用共识算法来对新增数据达成共识。

（一）区块链技术的性质

1、区块链是一个放在非安全环境中的分布式数据库

首先，这是一个分布式的，去中心化的系统。所以，有一个中心服务器或者节点的，不是区块链。节点都是安全的，无恶意的，这也不是区块链。同理，从应用的角度讲，如果你的应用必须要使用中心节点（例如要用超级计算机做深度学习）或者没必要考虑节点不安全的情况（例如某个安全的工厂里的传感器），那么并不需要考虑区块链技术。

至于后面的词“数据库”，目前大部分成熟的区块链都是数据库，例如比特币就是一个分布式账本，而账本其实就是数据。然后，根据数据的格式，又可以分三种：1，数据是完全不相关的，只是达成的共识，没有有效无效之分；2，数据有某些逻辑结构，例如账本中，一笔交易实际上除了金额，还有输入和输出，连接到之前的交易，这些数据需要通过逻辑验证（例如交易中，节点需要验证输入的交易是否有效）；3，数据拥有图灵完备的逻辑，而验证的时候需要通过节点使用算力运算，每笔交易可以有不同的输出和状态，每个节点要做的不仅仅是验证交易的真实性和输入的正确性，还要根据交易里的逻辑读入数值，进行验算然后再验证结果。比特币的系统就是第二种，又叫分布式账本；以太坊是第三种。第三种可以支持智能合约。用比特币举例的话，它是一个完全去中心化的系统；它放在一个非安全的环境，并不要求所有使用比特币的人都没有恶意。

2、区块链采用密码学的方法来保证已有数据不可能被篡改。

这个部分的两个核心要点是：密码学哈希函数；非对称加密。两个都是密码学的基础概念：

（密码学）哈希函数：一个函数Y=H(X)，有如下性质：有X可以很容易算出Y；有Y不可能算出X；有Y不可能找到另一个X'使得H(X')=Y；如果X和X'相差很小，H(X)和H(X')则完全不相关。这东西主要用于验证信息完整性——在一个信息后面放上这个信息的哈希值，这个值很小，例如256bit，而且计算方便。收到信息之后收信人再算一遍哈希值，对比两者就知道这条信息是否被篡改过了。如果被篡改过，哪

怕只有1数字1bit，整个哈希值也会截然不同。而根据哈希函数的性质，没有人能够伪造出另一个消息具有同样的哈希值，也就是说篡改过的数据完全不可能通过哈希校验。

非对称加密：这东西很好理解——对称加密就是有个密钥，可以理解成保险箱钥匙，你把消息加密变成密文，没有人能看懂这是啥，然后同一把钥匙解密成原来的消息。非对称加密就是有两把钥匙，一把叫公钥，一把叫私钥，用其中一把加密的话，只能用另一把解密，反之亦然。另一个重要的性质是，给你密文，明文和其中一把钥匙，你还是解不出来另一把钥匙是啥。原理基本上是基于一些困难数学问题，例如因数分解和离散对数，常用的有RSA，Diffie-Hellman和ECC（椭圆曲线），比特币用的是椭圆曲线。非对称加密除了和对称加密一样用于信息加密之外，还有另一个用途，就是身份验证。因为通常情况我们假设一对公私钥，公钥是公开的，而私钥只有本人有，于是一个人如果有对应的私钥，我们就可以认定他是本人。其中一个重要的应用就是数字签名——某个消息后面，发信人对这个消息做哈希运算，然后用私钥加密。接着收信人首先对消息进行哈希运算，接着用相应的公钥解密数字签名，再对比两个哈希值，如果相同，就代表这个消息是本人发出的而且没有被篡改过。

区块链把交易（数据）写在区块里：第一个区块叫创世区块，内容随意。从第二个区块开始，每个区块的第一部分有前一区块的哈希值。此外，区块里的每一笔交易（数据），都有发起人的数字签名来保证真实性和合法性。于是，先前区块里的任何数据都不可被篡改。这个数据库并不是静止的啊。数据库的数据是会增加的，而每次增加的数据，就是一个区块，于是这些生成时间不同的区块，就以这种形式链在一起了。

3、区块链采用共识算法来对于新增数据达成共识。

共识算法的目的，就是让所有节点对于新增区块达成共识，也就是说，所有人都要认可新增的区块。对于有中心的系统，这事很简单，中心说什么大家同意就好了，但是放到去中心化系统里，尤其是当有些节点有恶意的时候，这东西非常复杂，计算机科学里有个相应的问题，叫做“拜占庭将军问题”或者“拜占庭容错”（BFT）。

公有链，以比特币，以太坊和所有虚拟货币为代表，都采用比特币共识，共识算法基本上都采用工作证明机制，也就是挖矿，这种机制其他回答里已经讲得够清楚了。工作证明机制一切都好，除了费电……费多少电呢？比特币的话，差不多和一个百万人级别的城市那么多。此外以太坊的创始人特别喜欢权益证明，似乎很快要小范围投入使用（100个区块里一个用权益证明）。但是目前为止，大家对它的可靠性还持观望态度。

私有链和联盟链。以IBM的hyperledger-fabric，以及一大堆其他的类似于tendermint，甚至R3 corda和ripple为代表，都用BFT共识。其实这方面的应用已经很多了，问题是，目前基本上所有应用给人的感觉都还是为了做区块链而区块链，真的觉得这东西好到不可或缺的应用还基本没有。

（二）区块链技术的优点

安全且没有中央大账本，所以无法销毁（不是一台电脑可以控制的），无法作弊，每个人都有相同的账本，能确保账本记录过程是公开透明的。

全民记账效率也会提高没有中心化的中介机构存在，让所有的东西都通过预先设定的程序自动运行，能够大大降低成本，提高效率。

解决了中介信用的问题以前两个人合作，若是不信任对方，就必须依靠第三方，就像转账必须通过银行。但通过区块链技术，人们就可以实现在没有中介机构的情况下双方相互转账，比如比特币，它就是区块链的实际应用之一。

（三）存在问题

区块链的主要技术应用就是在金融上，然而还是存在不少的问题需要去解决：

1、区块链作为一个记账系统，如何解决金融体系的底层线下摩擦。

2、比特币在支付方面，当前比特币网络确认的交易是每秒最多7笔，而支付宝每秒则达到上万笔的交易确认。便捷性上来看，的确不如微信和支付宝，这个毋庸置疑，不过侧链和闪电网络正在攻克这些技术问题。

3、银行开户的成本是比较高昂的，但也无法避免。因为涉及到跨境支付，像目前对于不同的机构，做账对不上这些问题，其实都会涉及到支付成本。而区块链要怎么给出实际的解决方法，都是很

现实的问题。

四、结语

区块链技术虽然目前被看好，然而由于是新技术，且成熟案例非常有限，可借鉴的案例几乎没有，因此，还需要不断的去探索和尝试，解决所遇到的各种坑和一些现实问题。

作者单位：湖南省汽车技师学院

网络信息安全中加密算法及应用研究

文丨任一新

在社会经济和科技的不断发展下，人类社会进入到信息社会时代，信息对人们生活的方方面面都产生了深刻的影响。在人们的生活和工作中，他们依赖计算机来处理各种数据。在这些数据中包括国家机密、科研成果、商业机密、个人隐私等。在应用处理这些信息的时候，受计算机系统特殊性和复杂性的影响，数据信息的安全难以得到有效的保护。在这样的情况下，人们对数据加密技术和加密算法的要求。通过加密算法和加密技术的应用能够有效解决应用层数据在传输过程中的被窃听和修改的问题。为此，文章重点从理论和实践两个方面对网络信息安全中的加密算法展开研究。

一、加密算法概述

（一）术语介绍

加密是指将明确的可读信息转变为密文，即不可读信息的过程。解密是将已经加密的密文信息重新恢复成明文信息的过程。密钥是密码算法中的一种以特定方式进行运行的特定密文数值。

（二）对称加密算法

对称加密算法是一种传统的加密算法，加密和解密操作应用的都是同样一组密钥，在进行信息通信的时候需要双方拥有同样的密钥。数据加密标准（DES）是一种分组密码运算，在应用操作的时候能够实现多次的交换和应用，密钥长度是64位。这种算法在应用的时候需要经过16次的更迭，在这个过程中密文解密需要应用同一个密钥，过程和加密操作相似。

（三）非对称加密算法

非对称加密算法在加密和解密的时候需要应用不同的密钥，每个使用用户在应用的时候都需要保存一对密钥（公钥PK和私钥SK）。在非对称加密算法应用中，PK是一种公开性的信息，主要用来对密钥进行加密处理，SK则是由用户个人自己保管。公钥PK和私钥SK往往是一起出现的。在非对称加密算法中RSA是公开密钥加密系统中最著名的算法，是一种数据公开加密处理的标准，是基于一个难解的数学问题，应用操作的可变动性小。

二、网络信息安全中加密算法的选择和应用

（一）安全通道

在企业专用的信息网络的服务器和客户间建设安全通道，应用安全通道来进行数据信息的传输。比如在客户机和服务器之间经过协商来交换彼此加密公钥，之后将彼此所交换的数据信息加密之后进行传送。双方在接收到数据信息之后会应用各自的私钥加密来得到明文。

（二）安全网络隧道

在安全通道跨越两个远程网络的时候，需要应用加密路由器、隧道协议在远程网络上建立一种私有的网络通路。

（三）网络登录和认证

在企业的专用网络中一般是通过授权等级来对各