北斗区块链项目白皮书

Beidou Blockchain White Paper

张蕾

Email: zhanglei@huasystem.com Weixin: 161555

2017/11 V1.0

摘要

本文提出了一种基于地理信息的安全增强型交易架构，将交易的地理位置植入到交易的数据结构中。这种结构既可以在交易之前或交易过程中，作为交易的约束条件，防止某些交易风险的发生；也可以在交易以后，针对恶意交易的排查和追踪提供有效的技术手段。

1、背景

比特币[1]自 2009 年出现以后，为我们带来了一种新的“去中心化”的交易模式，这种模式的核心就是通过技术手段构建一个“最小信任”系统，从而提高交易的效率和安全性。比特币底层的区块链就是这种技术的具体体现。

比特币之后，又出现了上百种替代币（Altcoins）和其他区块链平台（代表性的有 Nxt、Bitshares、Ripper、Ethereum 等）。这些项目都对比特币的区块链提出了技术改进，改进的方向主要有三种：1）安全性的提升（如 Zerocoin）；2）交易效率的提高（如闪电网络、侧链等）；3）智能化交易功能的扩展（如 Ethereum 的智能合约概念）。其中，安全性的技术改进的速度最慢，但却是商业

应用最关心的。

当前，区块链远没有达到大规模、主流商业应用的要求，安全性不足是主要原因之一。下面介绍一种基于地理信息的安全增强型交易架构。

2、地理信息对交易安全的重要性

地理信息在传统交易中的应用场景

地理信息一直在传统交易中发挥重要的作用，在一些重要的商业合同中，都会约定“合同签署地”，并约定合同仲裁机构的所在地（城市），因为不同的交易地址，适用的法律条款可能不一样（比如在美国等地区，各州的地方法律差别很大）。

地理信息在恶意交易的追踪方面也发挥重要的作用。比如银行卡盗刷案件，公安机关的侦查通常是从交易地点开始，锁定提款的 ATM 所在的城市或区域（通常是异地），缩小侦查范围，提高破案的效率。

地理信息在新型交易中的应用场景

地理信息在新型交易中，同样发挥着重要的作用。比如在“共享汽车”这样的互联网交易场景中，交易通常是客户通过手机扫描二维码的方式开启的，运营方希望客户（及其手机）和实体资产（共享汽车）应该是在同一个地理位置上，防止客户将二维码照片发送到远程，由第三人协助开启交易，这与国家对共享汽车的“用户真实身份认证”的要求是相违背的。同时，在交易执行过程中，也就是客户使用车辆过程中，系统侦测到客户与汽车发生了位置偏离，那么交易应该取消或者暂停。这些地理信息为整个交易安全提供了强有力的保障。

地理信息在区块链交易中，也将发挥重要的作用。比如在区块链的供应链系统中，我们希望利用区块链的技术特性，实现追踪溯源、防伪鉴真的功能，但是如果供应链信息向区块链录入时就发生了错误，那么区块链的数据安全特性就没有任何意义。在一个绿色食材的供应链区块链网络中，我们要求“采集”的流程必须发生在食材的原产地，“进出仓库”的流程必须发生在指定的冷库中，“终端消费”的流程必须发生在特定的超市中，这些要求都需要地理信息的参与或者约束。

除了上面两种应用场景，地理信息在交易中的重要性还表现在：

1）交易位置的不同，适用的法律条款将产生差异；

2）交易位置的不同，相应的征税主体和税收政策也将产生差异。

因此，将地理信息整合到交易的基础属性中，将是必然的一种市场需求。

3、北斗区块链

简介

北斗区块链，简称“北斗链”，是世界上首次将地理位置信息与区块链交易结合的一种尝试。项目前身是“积分币”：一个商业积分交易平台。在实际运行中，商户提出了有关交易的地理位置方面的要求，比如要求某种积分只能在特定的场所（主要是门店）进行交易和赎回，从而更好地实现积分兑换对门店销售的促进作用。在此基础上，我们将地理信息整合到区块链核心的交易结构中，提出了升级版本的“北斗链”。

北斗链跟中国北斗卫星导航系统（BeiDou Navigation Satellite System，BDS）并没有直接的关系。北斗链的取名表明了我们对北斗精神的敬意，同时也突出了我们在地理信息方面的技术特点。

北斗链在系统运行中，会涉及到卫星导航模块和芯片。我们并没有仅仅限定于北斗系统，而是同时适配美国的 GPS、俄罗斯的 GLONASS 等系统，以达到更好的平台兼容性。

北斗链中提出包含地理信息的交易的标准结构（Geographic Transaction Standard, GTS），一个标准的交易信息，至少应该包括：

[发送人][接收人][交易资产][数量/金额][交易时间][交易位置]

其中交易位置的标准为：

城市英文或拼音名称[IP 地址][地理经纬度]，经纬度采取 WGS84 坐标系

实例：SHANGHAI [58.33.219.255] [N31.46E121.29]

城市名称便于在应用系统中做显性识别，网络 IP 地址和地理经纬度至少有一项不能为空。由于 IP 地址可能伪造，而定位信息也可能被模拟，所以北斗链在后续的技术升级过程中逐步提高对地理经纬度的要求，并对网络 IP 地址与地理经纬度进行交叉验证。

针对使用终端：如果用户使用网络钱包或通过交易所发出交易指令，系统将获取用户浏览器的 IP 地址；如果用户使用手机 APP 等移动终端，系统将要求用户手机开启定位功能，以获得精准的卫星定位数据。

针对矿工和交易所等完全节点，系统将强制服务器安装卫星导航模块，从而同时获得服务器所在的 IP 地址和卫星定位数据。

技术实现

区块链使用了一种 per-output 的交易模型，每一个交易结构都有若干个输入（inputs）和若干个输出（outputs）构成，每一个输入都要匹配（实际含义是消费）前一个交易中的一个输出。所有的交易历史就构成另一个多路、相互连接的结构，被称为“交易链”。这种结构在计算机科学中有一个专有名词叫“有向无环图 DAG”。最终这个交易链在货币初次发行的、被称为“coinbase” 交易的地方结束。

比特币区块链中的交易安全机制，分为“交易安全”和“区块安全”两个层次。

区块层面的安全措施，主要由矿工来维持，保证一个输出只能跟一个输入进行“匹配”，从而避免了“双重消费”的风险。

交易层面的安全措施，主要是两个方面，首先是数量控制，也就是所有输出的金额的总和必须等于所有输入的金额总和。其次是身份控制，要求输入提供有效的签名，完成与上一个输出的“匹配”。所谓匹配，就是说这个输入有权力对输出中包含的货币及其金额进行合法的支配。

区块链中的输出并不仅仅是货币接受者的钱包地址，也不是地址进行哈希运算后的公匙，而是一段代码，被称作 scriptPubKey。输入其实也是一段代码来代替签名，被称作 scriptSig，如下图所示。两段代码碰到一起，运行后没有错误，

就表示匹配成功。

图：一个真实交易中的 scriptPubKey 和 scriptSig

比特币中这种脚本代码，被称作 Script，它是一种简单的、基于堆栈的编程语言。Script 存在的价值，一方面是为交易提供更高的安全保证，另一方面为交易提供了更多的灵活性。北斗链的增强功能就是基于 Script 的扩展来实现的。

功能特点

北斗链的增强功能，主要表现在以下几个方面：

1）地理信息植入

所有交易发生时的位置信息将作为核心要素整合到交易的数据结构中，同时地理位置也可以作为一种交易约束条件，整合到 Script 中，并接受矿工的验证，提高交易的安全性。

2）继承比特币的优点

继承比特币的安全特性，包括交易结构、加密算法、多签名审核等。

3）增加交易约束机制

区块链中用户可以使用加密学的算法随机产生一对公匙和私匙，通常公匙用做用户的识别（地址）来接受货币或资产，用户发起一个用私匙签名的交易就可以控制这些货币和资产。除了直接交易，用户也可以通过发送一段私匙签名的消息，来证明自己对某个地址（公匙）的控制权。

北斗链就是利用这种特性，构建一个交易约束的列表，每一个交易执行前，双方先通过签名消息的方式，验证交易约束是否生效。

北斗链初期设计的交易约束有：网络连接、交易发送、交易接受、挖矿约束等。用户可以通过构建 pay-to-script-hash(P2SH)交易的方式，实现更复杂的交易约束。

4）支持智能资产

目前区块链上承载的资产通常有两种，一种是比特币方式的本地化货币（Native Currency），另一种是令牌化资产（Tokenized Assets）。本地化货币通常只能有一种；而令牌化资产并不会受到区块链网络层面的验证，因此计算令牌化资产的数量必须要回溯到所有的相关的交易历史。在区块链中令牌资产属于“二等公民”。

北斗链中的智能资产(Smart Asset)，是在区块链底层交易之上构建的一种新的结构。不仅可以同时发行多种资产，而且每种资产的身份识别和数量，通过扩展 Script 的功能，都会编码到交易的输出中。交易验证的规则也将扩展：输出中与输入中，不仅每一种资产的数量都必须相等，而且所有资产的总和也必须

相等。这种验证规则，相比比特币的验证规划更加严格，因此安全性更高。

在北斗链上，智能资产的种类和数量可以无限多。

5）支持原子交易

原子交易是指区块链上，两笔交易（特别是两种资产相互兑换时）应该同时完成或者同时失败，原子交易是交易安全的一种必要的手段。北斗链通过扩展 Script 中的 OP_CHECKSIG 函数 [3] 的功能来实现原子交易。原子交易中也可以加入交易位置信息作为参数条件。

6）适合快速部署

针对企业级应用场景，只需要 2-3 步就可以快速部署一条区块链或者加入一个已有的区块链。

7）支持数据流媒体

在区块链上构建 key-value 风格的数据流媒体存储机制，通过 API 调用屏蔽对区块链底层数据的直接调用，降低数据存取风险。

8）提供丰富的开发接口

针对开发人员提供丰富的 API 接口，并且最大程度兼容比特币的接口规范，支持 JAVA、PHP 等主流开发语言编写应用层代码。

9）平台定制化部署

针对不同行业的需求，可以灵活定制区块链的运行参数，不需要加密学知识。

挖矿及共识机制

挖矿的主要任务是维护“完全节点”，从而保证整个区块链的交易安全和数据安全。

北斗链中的矿工采取“雇佣制”，也就是有条件地、面向全球招募矿工，矿工入选必须具备一定的条件，主要是地理区位、服务器性能等指标。矿工选择时尽量分散以获得更高的安全保障，但是不提倡使用性能过高的设备而引起的“军备竞赛”。

北斗链上线一年内，计划招募的矿工数量在 200 名左右。具体的招募时间和细则，请关注项目官网。

北斗链的共识机制，没有采取比特币等其他区块链常用的 POW 机制（工作量证明机制），尽量减少能源的浪费和不公平竞争。在雇佣制矿工的基础上，北斗链采取 POWT 机制（工作时间证明机制 Power of Work Time），基于矿工当时的服务器性能和网络通信状态，尽可能平均分配挖矿任务。

4、北斗链的定位及发展愿景

北斗链是一个区块链底层框架，而不是一个应用系统。它继承比特币区块链的优秀的特点，在此基础上针对交易的安全性进行了功能增强，更适应未来大规模主流商业应用的需求。

北斗链希望成为继 Ethereum 和 Hyperledger 之后，另一个被世界广泛认可和接受的区块链框架，在某些特定行业，比如供应链管理、共享经济等领域，成为主流的基础开发平台。

北斗链将以开源、开发的模式，通过社区建设，构建智能资产交易的生态。

5、关于我们

华工咨询

北斗链的技术研发实体是郑州华工企业管理咨询有限公司。

华工咨询是一家区块链科技企业，致力于企业级区块链应用开发。自 2012 年进入数字加密货币领域，已开发出咔咔积分（通用积分平台）、珠宝溯源系统、北斗链（区块链底层平台）等多个区块链相关项目。

核心团队

张蕾 CEO，创始人

毕业于北京大学，20 多年的技术研发管理经验，长期从事 IT 架构设计、IT Consulting 工作。近几年，专注与数字货币和区块链的商业模式研究，首次提出了“区块链业务分析”的概念，并对外提供咨询和培训服务。

2017 年“中国云计算大会上” 区块链技术峰会演讲嘉宾.

王彦涛 CTO，核心开发者

毕业于解放军信息工程大学，曾任华为高级研发经理，大河网技术部经理。精通 JAVA 等多种开发语言。

＊＊＊ 密码设计，核心开发者[4]

本硕毕业于西安电子科技大学密码学专业，长期从事 Hash 函数的设计和攻击、安全加密芯片的软硬件算法设计。

6、类似项目介绍

Niantic 公司开发的著名的网络游戏《口袋妖怪 GO》中，地理位置是不可或缺的一个重要内容，游戏中的交易功能（互相交换精灵）就是基于地理位置进行的。游戏中引入了一个虚拟交通运输系统，比如虚拟飞机、虚拟火车、虚拟公共

汽车等，甚至已经规划好了虚拟线路。玩家之间的交易就需要基于这个虚拟交通系统完成。根据 Niantic 公司申请的专利文件显示，在交易的时候，玩家需要走到公交站、地铁站或是飞机场等交通站点发起交易，而对方也同样需要在对应的站点才能进行精灵接收。

参考：

[1] 比特币白皮书 http://bitcoin.org/bitcoin.pdf
[2] ERC20 标准 https://theethereum.wiki/w/index.php/ERC20_Token_Standard
[3] OP_CHECKSIG 函数 https://en.bitcoin.it/wiki/OP_CHECKSIG
[4] 作为几个加密算法的设计者，特殊身份，隐藏信息

版本

2017 年 6 月 Draft Version
2017 年 7 月 V0.9
2017 年 10 月 V1.0