DPC

基于北斗卫星技术与区块链底层技术的去中心化平台

V1.0.0

Dipperchain.com
2017/9/5

目录

DPC（北斗链）

0.引言：

比特币自 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。

本项目提出了一种基于北斗导航和位置服务的安全增强型交易架构，将交易的LBS位置信息和AI大数据挖掘运算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.项目介绍：

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。我们提出了一种基于LBS位置信息服务，并融合人脸识别技术、语音识别技术等生物特征识别技术的安全增强型交易架构。

北斗区块链，简称“DPC(北斗链)”，是世界上首次将地理位置信息、生物特征识别技术与区块链数据服务结合的一种尝试。以区块链技术+目标识别+地理位置服务的底蕴，运用AI运算和大数据挖掘的区块链技术,致力于北斗卫星精准定位和空间信息数据服务应用，融合人脸识别、语音识别等生物特征认证识别，设计一套高性能的数据分布储存和跨平台并发处理，确保采集传输、交易服务等数据安全；打通各个应用单元的信息孤岛、深化各个应用单元的数据开放、提高数据服务的安全、效率和便捷性；在实际运行中，第三方提出了有关数据服务、数据交易等场景的精准地理位置方面的要求，因此我们将精准地理信息整合到区块链核心的数据服务结构中，提出北斗区块链(DPC)。DPC在系统运行过程中，会根据应用场景选择GPS、北斗等不同的定位模式，以确保数据实时性和完整性；

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北斗卫星导航模块，从而同时获得服务器所在的IP地址和卫星定位数据。

2.位置信息服务对交易安全的重要性：

基于位置的服务，是指通过电信移动运营商的无线电通讯网络或北斗定位方式，获取移动终端用户的位置信息，在GIS平台的支持下，为用户提供相应服务的一种增值业务。

（1）签到（Check-In）模式：

主要是以 Foursquare 为主，还有一些国外同类服务还有 Gowalla、Whrrl 等，而国内则有：嘀咕、玩转四方、街旁、开开、多乐趣、在哪等几十家。

（2）大富翁游戏模式：

国外的代表是 Mytown，国内则是 16Fun。主旨是游戏人生，可以让用户利用手机购买现实地理位置里的虚拟房产与道具，并进行消费与互动等将现实和虚拟真正进行融合的一种模式。这种模式的特点是更具趣味性，可玩性与互动性更强，比 Check-In 模式更具粘性，但是由于需要对现实中的

房产等地点进行虚拟化设计，开发成本较高，并且由于地域性过强导致复盖速度不可能很快。在商业模式方面，除了借鉴 Check-In 模式的联合商家营销外，还可提供增值服务，以及类似第二人生（Second Life）的植入广告等。

（3）周边生活服务的搜索：

以点评网或者生活信息类网站与地理位置服务结合的模式，代表 大众点评网、台湾的“折扣王”等。主要体验在于工具性的实用特质，问题在于信息量的积累和复盖面需要比较广泛。

（4）与旅游的结合：

旅游具有明显的移动特性和地理属性，LBS 和旅游的结合是十分切合的。分享攻略和心得体现了一定的社交性质，代表是游玩网。

（5）会员卡与票务模式：

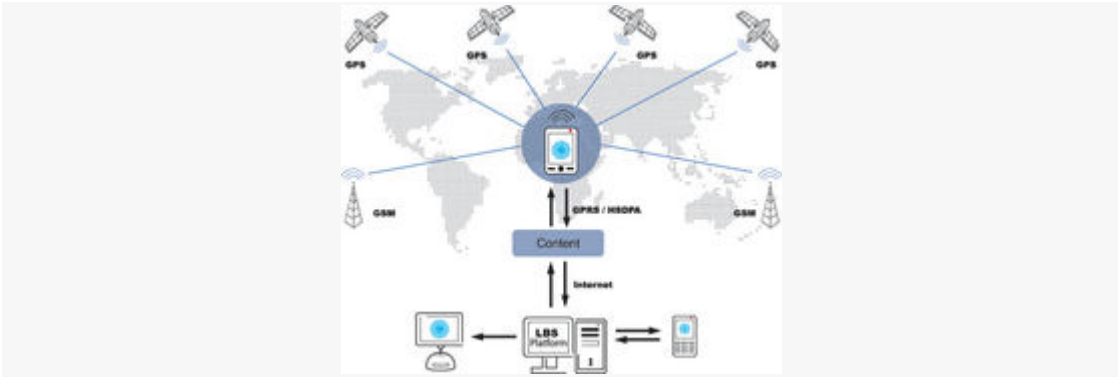
实现一卡制，捆绑多种会员卡的信息，同时电子化的会员卡能记录消费习惯和信息，充分的使用户感受到简捷的形式和大量的优惠信息聚合。代表是国内的“Mokard（M 卡）”、还有票务类型的 Eventbee。这些移动互联网化的应用正在慢慢渗透到生活服务的方方面面，使我们的生活更加便利与时尚。

（6）地点交友，即时通讯：

不同的用户因为在同一时间处于同一地理位置构建用户关键，代表是兜兜友。

（7）以地理位置为基础的小型社区：

地理位置为基础的小型社区，代表是“区区小事”



（8）LBS+团购 ：

两者都有地域性特征，但是团购又有其差异性，如何结合？美国的 GroupTabs 给我们带来了新的想象： GroupTabs 的用户到一些本地的签约商家，比如一间酒吧，到达后使用 GroupTabs 的手机应用进行 Check In。当 Check In 的数量到达一定数量后，所有进行过 Check In 的用户就可以得到一定的折扣或优惠。

Getyowza 就为用户提供了基于地理位置的优惠信息推送服务,Getyowza 的盈利模式是通过和线下商家的合作来实现利益的分成。

（9）店内模式:

ShopKick 将用户吸引到指定的商场里，完成指定的行为后便赠送其可兑换成商品或礼券的虚拟点数。

3.技术实现：

操作指令信号输入后，通过数据服务模式或交易模式，一对一的匹配相应输出结果，并且输入指令都要匹配前一次服务的输出，构建多路、多链接网状的数据链。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。

服务层面的安全措施，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，融入人脸识别、语音识别等最新人工智能技术，对人脸特征和声纹特征数据采集，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。两段代码碰到一起，运行后没有错误，就表示匹配成功。

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。DPC的增强功能就是基于Script的扩展来实现的。

4.项目亮点：

（1）引入地理位置服务和导航技术

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）融合语音、图像识别等人工智能技术

交易过程融合语音识别、图像识别等人工智能技术和大数据挖掘运算技术，通过交易过程的身份认证和身份识别，保障

了交易的高效安全性；

（4）支持智能资产

DPC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。

（5）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。

（6）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。

（7）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。

（8）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。

5. 代币及激励机制：

DPC 中的基础货币，叫做“北斗币”。北斗币跟比特币系统中的原生货币（native currency）的概念不同，它是一种智能资产（smart asset）型货币，兼容 ERC20 标准。在交易过程中，智能资产同比特币一样要接受矿工的验证，因此，北斗币可以获得与比特币一样的交易安全保证。

6.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。

DPC 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，不会因为使用性能过高的设备而没有安全保障。

DPC 上线一年内，计划招募的矿工数量在 500 名左右。具体的招募时间和细则，请关注项目官网。

DPC 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，DPC 采取轮询式共识机制（round-robin schedule），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。矿工挖矿不能自动获得北斗币，矿工的工作通过“工资”的方式获得补偿。

7.应用场景：

（1）移动互联网领域：

随着手机智能化水平的提高和移动互联网的普及，我国移动互联网发展进入全民时代。DPC技术渗透到移动终端、接入网络、应用服务、安全与隐私保护等移动互联网各个方面，在商业服务和交易过程中，带有北斗导航地图和位置信息分享的区块链技术有力的保证了服务和交易过程的安全、便捷和效率。

（2）互联网金融领域：

互联网理财用户规模不断扩大，理财产品的日益增多、产品用户体验的持续提升，带动大众线上理财的习惯逐步养成。目前已经推出DPC技术可直接融入到众筹、P2P、第三方支付、数字货币等互联网金融的安全、信用、支付、理财等多种不同类型，大大提高互联网金融风控水平。

创始团队来自中国原始技术、University of Pennsylvania、University of Edinburgh等科研院所及一流企业的技术研究团队。有着多年网络传输、数据加密和北斗导航位置服务等领域的深厚技术和ICO运营经验。能够完整的在基于AI运算的区块链技术服务过程中实现去中心化、程序化以及自动化储存、交易。

（3）公共安全应急管理：

通过采集事件发生地的位置信息数据，融合事件的目标识别技术，确定事件地点和目标特征，由此将采集数据加密技术传输给中心控制系统，指挥调度相应地理信息的应急人员、应急物资及应急车辆，确保事件处理及时高效，将风险降到最低。

（4）国防军工领域：

通过远程监测和识别目标特征，确定目标所在的精准地理位置信息，融合图像识别和目标位置跟踪技术，实时确定目标的位置移动轨迹，将监测数据加密传输到指挥控制中心系统，由语音技术和人脸识别技术发出操作指令，确保高效安全的调度命令指挥系统，保障国防安全和人民生命财产安全。

（5）智慧城市领域：

区块链技术去中心化、信息不篡改等技术特征，保证数据服务和交易的安全性，同时数据节点之间的传输和服务，可通过LBS位置信息和人脸识别、语音识别等技术嵌入，保证数据存储、采集、传输、调用和交易过程的高安全性，维护智慧城市数据运营安全运行，保障城市公共安全和政务管理效率提升。

（6）共享单车监控管理：

“共享单车”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，分享北斗位置信息数据，并从大数据挖掘和机器学习算法，提高车辆的安全、效率和便捷性，提供更多的产品服务；对共享单车的“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。

（7）食品安全溯源管理：

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。

8. DPC 的定位及发展愿景：

DPC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。

DPC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、公共安全等领域，成为主流的基础开发平台。

DPC将以开源、开发的模式，通过社区建设，构建智能资产交易和数据服务的生态体系。

（1）产品上线：

DPC底层平台架构设计、代码开发及压力测试，完成产品内部小范围试用，通过平台代码开源管理，逐步完善产品并推出产品上线。

（2）示范应用：

基于DPC的商业应用的开发，首先在共享经济领域，把北斗导航和位置服务信息融入商业交易服务中，建立DPC应用示范项目，树立DPC应用的标杆。

（3）大规模商业化应用：

由共享经济领域的示范应用、技术积累及产品成熟，逐步推向在食品安全、智慧城市、智慧社区、城市安全及国防安全等各个领域的规模应用，实现DPC规模化商业化应用价值。

9.：关于我们

创始团队来自中国原始技术、University of Pennsylvania、University of Edinburgh等科研院所及一流企业的技术研究团队。有着多年网络传输、数据加密和北斗导航位置服务等领域的深厚技术和ICO运营经验。能够完整的在基于AI运算的区块链技术服务过程中实现去中心化、程序化以及自动化储存、交易。