深化电子发票应用　践行新旧动能转换

—— 区块链技术服务于纳税遵从

区块链技术的可能

从2017年开始，国家税务总局已经开始了区块链技术的研究，以区块链技术促进纳税遵从成为了近期税务工作深化改革的重点。

1、区块链技术概述

（1）区块链技术原理

区块链是一种大型、分布式、多方共享的数据库。它基于密码学技术，通过特定的算法记录每一个交易事项，交易的每一个后续变化都可在连接和可追溯的链条下游创建另一个数据区块，并且在交易的每一个环节都实时复制一定时间内全部的交易数据，具有无与伦比的可靠性和安全性，使交易数据几乎不可能被伪造或销毁。

（2）区块链技术特点

区块链特殊的数据库组织形式，使得区块链技术具有四个特点：去中心化、公开透明性、可追溯性以及智能合约机制。

（3）区块链技术中的财税理念

区块链技术的特点与财税理念在很大程度上类似，详细见下表：

区块链技术与财税理念对比表

特点	区块链技术	财税理念
去中心化	各个节点地位相同	财务部门、管理层、治理层、税务部门信息对称
公开透明性	单一节点无法篡改数据	财税数据不可篡改、真实有效
可追溯性	数据按时间顺序冗余保存	会计记账的不可逆、增值税抵扣链条完整
智能合约机制	自动执行条款	收入确认、纳税义务发生及时确认

2、区块链技术促进纳税遵从的应用分析

区块链技术的核心功能就是去中心化，运用分布式记账功能实现交易的去信任化。这在纳税遵从中有着积极意义。区块链技术在纳税遵从中的应用探索可从纳税遵从因素和纳税遵从成本两方面来归纳分析。

（1）区块链技术可以减少纳税不遵从的因素

a. 区块链可以大幅度减少税收争议；

b. 区块链技术可以减少自私性纳税不遵从；

c. 区块链技术可以减少无知性或懒惰性纳税不遵从。

（2）区块链技术可以降低纳税遵从成本

a. 区块链技术可以减少纳税遵从货币成本和时间成本。

b. 区块链技术可以减少纳税遵从非劳务成本。

3、在实践中可能的应用

比如区块链技术在纳税信用公示系统、增值税管理系统两个方面的应用。

（1）纳税信用公示系统

区块链技术能够搭建一个全方位、数据更为详细的纳税信用公示系统。具体而言，区块链网络将给予纳税人唯一的纳税人识别号，并加盖时间戳记。每一次产生纳税信用信息和重大税收违法案件信息，都将被实时记录进区块链网络，并且不可篡改。

区块链技术可以真正实现**“让守信者一路畅通，让失信者寸步难行”**，提高了纳税不遵从的声誉损失成本，进而促进纳税遵从。

（2）增值税管理系统

区块链技术与增值税管理系统具有高度的契合性。它通过使用加密技术和由防篡改分布式记账启用的分布式信任系统来记录和验证交易，可以实现对某一商品从生产到最终到消费者手中的全部过程中所有交易事项的所有信息的详细记录。该交易记录不可以篡改，且不可逆。

区块链技术用于增值税管理，会使增值税管理系统更加透明和高效、增值税抵扣链条更加准确和完整，可以大幅度降低财务风险和税务风险，使人为主观因素对财务数据的影响大幅下降，会计计量更为公允，进而促进纳税遵从。

另外，在增值税管理环节，区块链技术还有助于识别骗取出口退税，并能有效缓解纳税人运营资金的压力，进而更好地促进纳税遵从。

总体技术方案

现在就全面推进区块链技术在纳税遵从方面的应用是不切实际的，而围绕着目前我们在电子发票的推广应用中碰到的瓶颈问题，着力以共享模式加持区块链技术的方法，打破瓶颈、深化应用不失为一条好的发展思路。

1、技术设计原则

区块链技术的颠覆性在于：让公众“不再依赖任何的中心机构，就能实现完全可信的交易或共识”，人人可以公平、公正地拥有和使用信息！

因此，我们参照“比特币社会实验”的成功经验，充分结合信息技术的最新发展成果，确定了方案的技术设计原则：

- 开源实现
- 信息资产化
- 严格保护隐私
- 功能模组化，可动态配置和扩展
- 操作智能化
- 资源共享接入
- 全云化

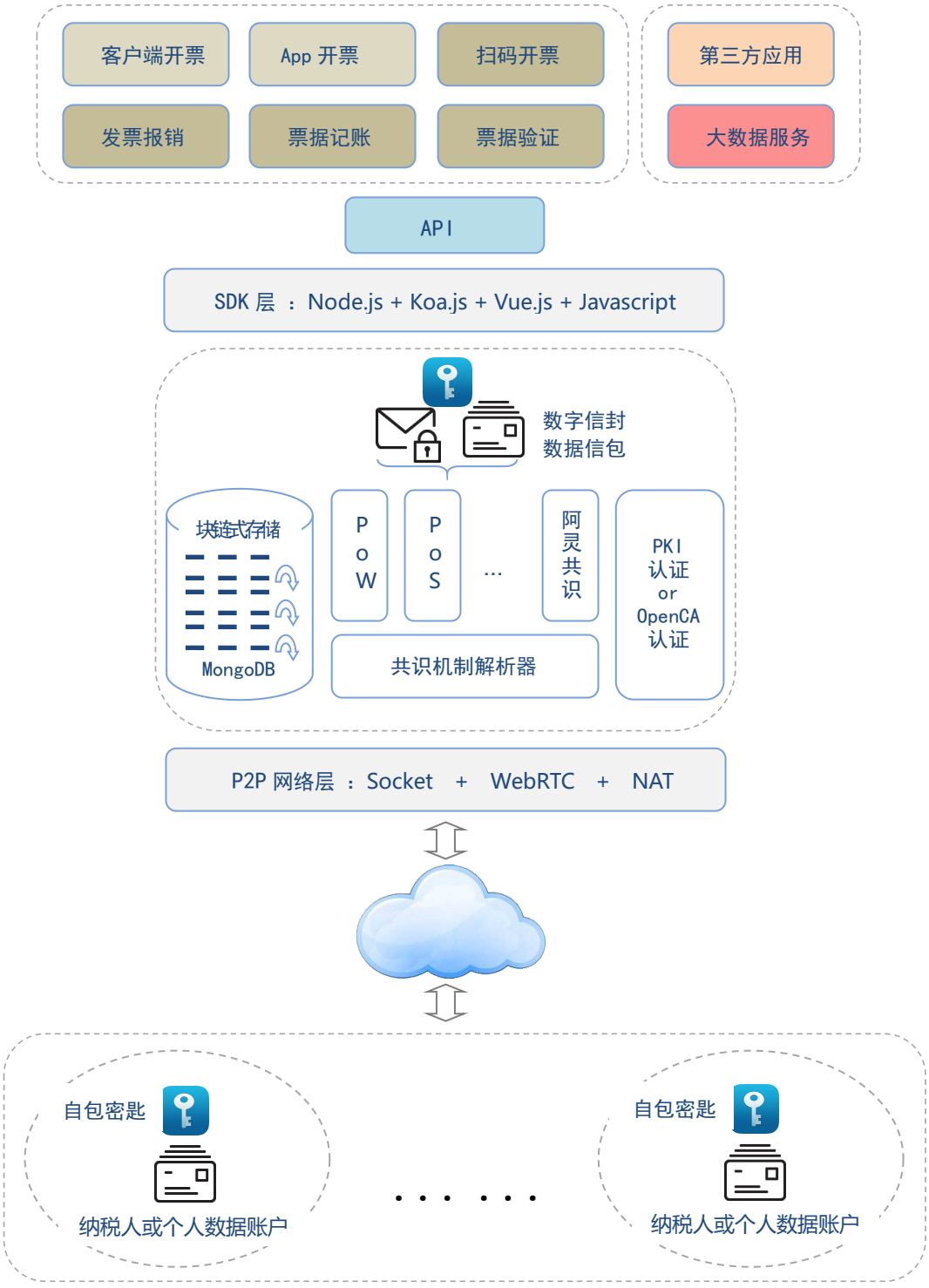
2、总体框架设计

我们为每户纳税人和每位消费者创建强加密保护的数据账户，并将其账户信息资产化。然后以此为基础，在云环境中用创新的区块链技术平台，将电子发票的开票、验票、报销、记账以及大数据服务，统一到区块链技术加持的系统中来。

按照区块链技术应用于纳税遵从的思想，使得每户纳税人和每位消费者无论是开票、验票、报销和记账，都全部记入云端分布式存储的“全民账簿”中，籍此实现了涉及电子发票及其未来拓展的各项涉税事务的可追溯、不可篡改和客观公正。

整个系统中全面使用自包密匙、数字信封和数字信包，在公开、透明的纳税遵从中，充分保障了纳税人和消费者的信息隐私。

具体的设计见下面的《总体框架设计图》。



总体框架设计图

其中，P2P 的分布式对等网络，通过 WebRTC 开源协议可实现点对点的包括实时音视频直播的数据传输；通过 NAT 可实现在用户使用内部网络（如：公司局域网，家庭 WiFi 路由内部网）时都能完成点对点的内外网穿透，保障数据传输的畅通。

整体项目的开发，除需特别优化之外，均统一在前后端使用 JavaScript 语言进行开发，全部使用开源的、优选的 SDK 工具，进行项目的开发、调试、测试、部署、维护和迭代升级。其中，选用 Node.js 作为代码运行平台，服务端框架使用 Koa.js，前端框架使用 Vue.js；建议统一使用 Visual Studio Code 作为集成开发工具（IDE），或者使用 WebStorm、Visual Studio 2017。

技术架构上将 API 集完全独立，便于应用层的功能扩展，还支持第三方开发基于本系统的应用，也支持各类应用模块的动态配置（包括对实验性质应用的支持）。

上述的的各类技术和工具要求必须支持 Linux、Windows 和 macOS 操作系统，移动端必须支持 Android 和 iOS。

注意一点，目前区块链技术的应用，存在多种实现共识机制的算法或方法。一则是不同的用户认同或偏好不一样，二则是更多、可能更好的算法或方法还不停地在产生，所以我们的技术架构中使用了共识机制解析器，来像支持插件一样地支持不同的共识机制在一个系统中的共存。

3、关键技术和难点

在目前全世界都还没有真正成功落地的区块链技术应用的背景下，我们系统实施的难度是可想而知的。而且，系统一旦上线成功，用户对系统的访问量是海量级别的，这对系统的健壮性、可扩展性、可维护性都有着极高的挑战。

所以，我们有必要把可能设想到的技术重点和难点提前进行梳理。

系统技术重点

(1) 基于开放式网络的数据访问和操作规范

纳税人和消费者的账户信息要成为资产，就必须是在整个开放的环境中被准

确识别和理解，还包括在授权许可下能够被无歧义地操作。从另一个角度讲，就是必须在开放的环境下消除“信息孤岛”，才能真正释放信息的价值。

系统必须在资产化信息都经过强加密的情况下，采用 RESTful（Representational State Transfer，简称 REST）规范，统一以 JSON 为基础数据格式，来进行全网络的数据访问和操作，以实现可重用性、简单性、可扩展性和组件可响应性的清晰分离，最大化地展现数据价值，并最终大幅优化全网的数据冗余。

（2）全程的透明与开源

区块链技术对最佳“信用”的实现，其实是依赖于公开、透明的原则来达成的。理解了这一点，就要求我们在整个项目中要做到：从数据、数据操作到业务逻辑的执行，从开发架构、开发工具到运行的源代码都要做到公开、透明。

所以，在我们采用的技术架构里就已经全部选用了开源实现的数据库和一系列的开源 SDK 工具；同样的，我们整个系统也将总体采用 MIT 的开源协议进行开源。

不仅如此，为充分地体现公开、透明原则，项目中还会在多个层面和必要的功能中向用户提供开放的数据查询和验证服务，也籍此强化系统“信用”驱动的本质。

另外，借助设计良好的技术架构，在全程的透明和开源条件下，系统还要为各种可能的用户共享提供便利的实现，以达到最大化推动“共享”实现的目标。

（3）支持多种共识机制的实现

区块链项目的开发、实现，不能违背去中心化的本质。绝不能像今天的虚拟货币一样，各自搞一套虚拟币的实现方式或标准，希望大众以后都以他的币种为中心来完成交易，即他们都想干掉了原有世界的货币中心，自己成为未来全球唯一的中心。

果真如此的话，中本聪肯定是非跳出来不可的啦！（^_^～^_^）

有鉴于此，更主要的是为了支持信息尽可能无障碍地传输和交互，尽可能地实现信息价值的最大化，我们要通过底层平台实现“共识机制解析器”的方式，将不同的、各家的共识机制作为插件一样地纳入到系统中来，从而打破中心化共识机制的瓶颈。

这样实现的另一大好处是：通过“共识机制解析器”的多插件设置，利用 Node.js 的单线程、异步、非 IO 阻塞特性，就可以突破现存的区块链技术不能满足高性能应用的弊端，为每秒提供数百万次甚至更高频次的交易创造条件。

（4）结合大数据和 AI

系统在本质上的主营业务是数据处理，而且它一旦能够成功上线，用户累积的数据量是惊人的。并且我们支持“信息资产化”和公众信息的关联，这样就会更加放大项目的数据量规模。

但是，光有数据量并没有什么价值，系统必须要利用大数据技术，为用户挖掘海量数据形成后的关联关系价值。

在此之上，AI 人工智能又有了用武之地。我们将使用商务智能技术（Business Intelligent，简称：BI），并借助 Google 旗下的 DeepMind 公司开源的 AlphGo 和 AlphGo Zero，为用户的海量数据不断迭代全新的价值。

（5）跨平台和跨终端的用户体验

系统将为用户提供不同终端的便利工具，这就包括了基于 PC 的应用软件，基于手机、平板等的移动 App。这些用户端的应用工具，主流的就涉及 Windows、Linux、Android、macOS、iOS 五种操作系统和众多的不同版本；同时，适合不同系统的开发语言、开发工具以及开发圈子又都完全不一样。虽然有“全栈式开发”的办法可以基本统一在一套开发体系里来完成，但在移动端，特别是最大用户群的 Android 和 iOS 端，“全栈式开发”目前还很难为用户提供极佳的操作性能和体验。

这就迫使我们，在开发和发展上选择分步走的路线：

① 用户端开发分两步走：全栈式 Web + 原生开发；

② 优先解决 Web 的实现；

③ 在 Web 实现的基础上，用“全栈式”的工具先为移动端提供先期的应用；

④ 在系统发展已经蓬勃之时，再全力开发 Android 和 iOS 的原生应用。

近期，应该组织力量学习和操练 Kotlin 和 Swift 这两种新兴的语言和开发工

具，未来用它们作为 Android 和 iOS 移动端开发的主流语言。

系统技术难点

(1) P2P 对等网络的实现

系统要面对全球的用户实现分布式点对点通信，要传输的数据中还可以包括视频和音频，所有数据在传输中还必需保持密文状态；为达到高性能的要求和好的用户体验，传输的性能和质量都面临极高的要求。

系统将主要参考 BitTorrent 和 WebSocket 的架构和实现方法，研究了现在多家虚拟货币的实施效果，确定以更基本的、得到大多数开发语言和平台支持的 Socket 为基础，使用 Google 开源的 WebRTC 来实现 P2P 的对等网络功能。

WebRTC 确实集成得很完备，性能也完全满足项目要求，但毕竟是很新的框架，开发文档不多，运用上有一定的难度。另外，NAT 的配置和架设需要大量的实际验证、测试和优化，才能覆盖广泛的用户群体。

所以，P2P 对等网络的实现是项目的一个技术难点。

(2) 强加解密的性能和可靠性保证

目前我们可以放心使用的，不惧怕黑客攻破的加解密方案是使用非对称加解密的 RSA2048、对称加解密的 AES112 以及 Hash 散列值的综合方案。

就当前来讲，至少到 2030 年前，这个方案是稳定、可靠的。但是，我们的项目要求，任何的传输和存储中都一律使用加密后的密文，那么在大量的实时查询中，就需要动态地执行对密文的解密计算，所以应用中的性能是一个很大的技术难题。而且，纯算法上是不具备改善条件的，只有在各种具体的功能实现上去找到理想的办法来克服大量的解密性能问题。

再有就是，量子计算离现实可用已经越来越近，所以我们设计的加解密方案还必需是可无缝过渡的。这一点，也加大了加解密方案实现好的性能和可靠性的实现难度。

（3）函数式编程和 ES6

其实任何的区块链技术应用项目都是一个庞杂的体系，所以我们才在技术架构和实现方案上进行了大量的统一、区隔和可扩展工作。比如说，统一开发语言为 JavaScript 就是这样。

但是，JavaScript 并不是一种强约束语言，而且它的发展历程和分歧就非常多。这就导致，我们在开发上能够更贴合项目实际的函数式编程在 JavaScript 上就不好掌握，团队在使用中会耗费很多的学习时间，也会产生很多的开发障碍；要不就会牺牲代码的开发时间或稳定性。

同样的原因，还产生了对最新的 JavaScript 标准 ES6 的支持问题上，统一一个标准，许多浏览器和第三方工具不支持；不统一又会导致工作量和可靠性的牺牲。

这些，都是我们在开发过程会面对的技术难题。需要充分重视，妥善解决。

比如，像这样的一些函数柯里化的 ES6 标准的编程方式：

```
var compose = (f, g) => (x => f(g(x)));
var add1 = x => x + 1;
var mul5 = x => x * 5;
compose(mul5, add1)(2);                    // =>15
```

这样的编程方式非常的简洁、高效，而且运行时可以发挥异步并行的极高性能；同时还具有极好的隔离性，不会导致模块间的交叉感染和错误。可是，转换编程思维的学习曲线就相对很抖了。

系统功能设计

在全新的区块链技术支持下，系统将为纳税人和消费者提供创新的各类涉税应用，同时也支持第三方通过开放的 API 接口提供更多的涉税应用。

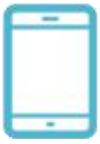
下面简单说明一下系统基本的一些应用。

1、开票应用

支持线上、线下的实时开具发票，发票数据经过签名、加密，开票方式多种多样，便捷、安全。

客户端开票

客户可安装 PC 端的开票软件，支持各种格式的票据信息导入、导出



App 开票

支持 iOS、Android 设备的开票，随时随地同步涉税信息

扫码开票

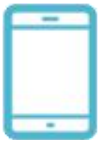
消费者可自行扫码开票，并支持各类分享推送

2、验票

提供各式发票的实时验证和后台自动验证，并可核查开票业务的相关信息（除公开信息外，访问涉密信息需有授权）。

客户端验票

客户通过 PC 端软件可以实时验票或在后台自动验票



App 验票

支持 iOS、Android 设备的验票，也可选择实时或后台自动验票

3、报销

支持各式发票的快捷报销，在区块链云上、PC 端和移动端同步报销的发票、流程和单据，提供多样化的报销及费用报表。

客户端报销

客户通过 PC 端软件可实现便捷报销，统一报销的财务接口

App 报销

支持 iOS、Android 设备的快捷报销，与纳税人财务统一报销凭证

4、记账

提供各式发票报销和记账的流程整合，彻底告别报销和财务记账分离导致的错漏、繁琐年代！

报销记账整合

纳税人可以在终端上实现报销和记账的流程整合，自动、智能地处理票证记账工作

5、大数据服务

纳税人和消费者不断地使用系统，海量的数据就会记入云端分布式存储的“全民账簿”中，这些数据在经过去结构化后，纳税人和消费者的隐私信息将被完全地剔除。对这些海量的、动态更新的数据应用大数据技术进行分析和挖掘，并予以可视化呈现，就能够不断地为政府和各类机构提供高价值的信息服务。