OpenAuditable 架构白皮书

一种可以取代区块链技术的新架构

作者：陈德伟
2018 年 11 月

1. 为啥要发明新的轮子

区块链技术这几年实在是太火了，大家都在学习和讨论区块链。但是区块链技术目前正在成功的应用只有比特币等虚拟货币。最近阿里巴巴发布了“相互保”产品，获得广泛的支持，我本人也加入了。说实在的，尽管“相互保”有阿里的信用进行背书，我比较放心，我还是担心有人可以以权谋私。尽管网上说“相互保”采用了区块链技术，加上网上公示，应该万无一失了吧。我百度了一下“相互保公示”，没有找到入口。即使我找到了公示入口，我也难以找到有效的手段对数据进行核实，或者核实的成本太高。它采用的区块链技术能真的保证其数据不可篡改吗？其实是值得怀疑的。区块链这种数据结构只是提高了修改数据的难度，而不是不能。以比特币来说，只要你拥有超过 **51%**的算力，你就可以控制比特币记账，这是常识。比特币之所以让人比较放心，是因为拥有超过 **51%**的算力成本太高。尽管我没有仔细研究“相互保”的技术实现，但是有理由相信：因为数据和算法都在阿里的控制下，阿里其实是可以随心所欲的修改数据的。

总而言之，区块链技术的设计思想是通过提高数据篡改的成本来保证数据的可信度。难道提高数据的可信度只有这一种方法吗？本文提出一个新的提高数据可信度的方案，成本更低，可操作性更强。它核心思想是通过降低数据验证的成本来提高数据的可信度。

2. OpenAuditable 架构的工作原理

以阿里“相互保”产品为例，如果任何人可以方便且低成本地审核“相互保”的数据，而且审核方法可以自定义，审核的内容包括数据是否被篡改、记录对比等。如果再加上有专门的有公信力的审核机构参与审核。应该可以说，“相互保”的可信度比采用区块链技术更高吧。

下图（**Figure 1**）列出了这个系统的工作方式，图的上半部分是需要获得可信度（或者公信力）的系统，它们都需要实现了 **OpenAuditable** 接口（**Figure 2**），图的下半部分是开放验证生态系统。为了后面叙述方便，把实现了 **OpenAuditable** 接口的系统简称为“可信系统”，“开放验证生态系统”简称为“验证系统”。

可信系统把数据以安全的方式提供给验证系统。验证系统把数据数据保存起来，为以后验证数据是否被篡改提供依据。如果可信系统提供的数据是加密的，它们应该提供相应的软件包来操作加密数据。为了便于验证，可信系统提供的数据应该是部分加密。

以“相互保”为例来说明系统的工作原理：

1.第一步，“相互保”实现 **OpenAuditable** 接口，比如开放 **RestApi**。通过这个 **API**，任何人（也可以限定为参保人）可以获取“相互保”的可验证数据，比如参保人名册，保险发放记录等。数据建议采用部分加密的方式。比如参保人姓名和省市区等非敏感信息明文存储，身份证及联系方式等信息以加密形式存储。

2.第二步，验证系统可以根据 **OpenAuditable** 接口进行验证。验证系统包括开源社区和各种社会组织和个人，他们可以开发各种验证算法和验证工具，比如可以开发手机 **App** 或者网站，考虑到存储容量的限制，手机 **App** 验证算法倾向于基于部分数据来验证，比如随机抽样的方式。个人验证者最感兴趣和可行的验证方式是核对自己或朋友的部分信息。当然，任何人都可以进行求和等统计操作，也可以提出对某条记录的质疑（验证系统可以提供质疑支持，比如投票，公告等）。

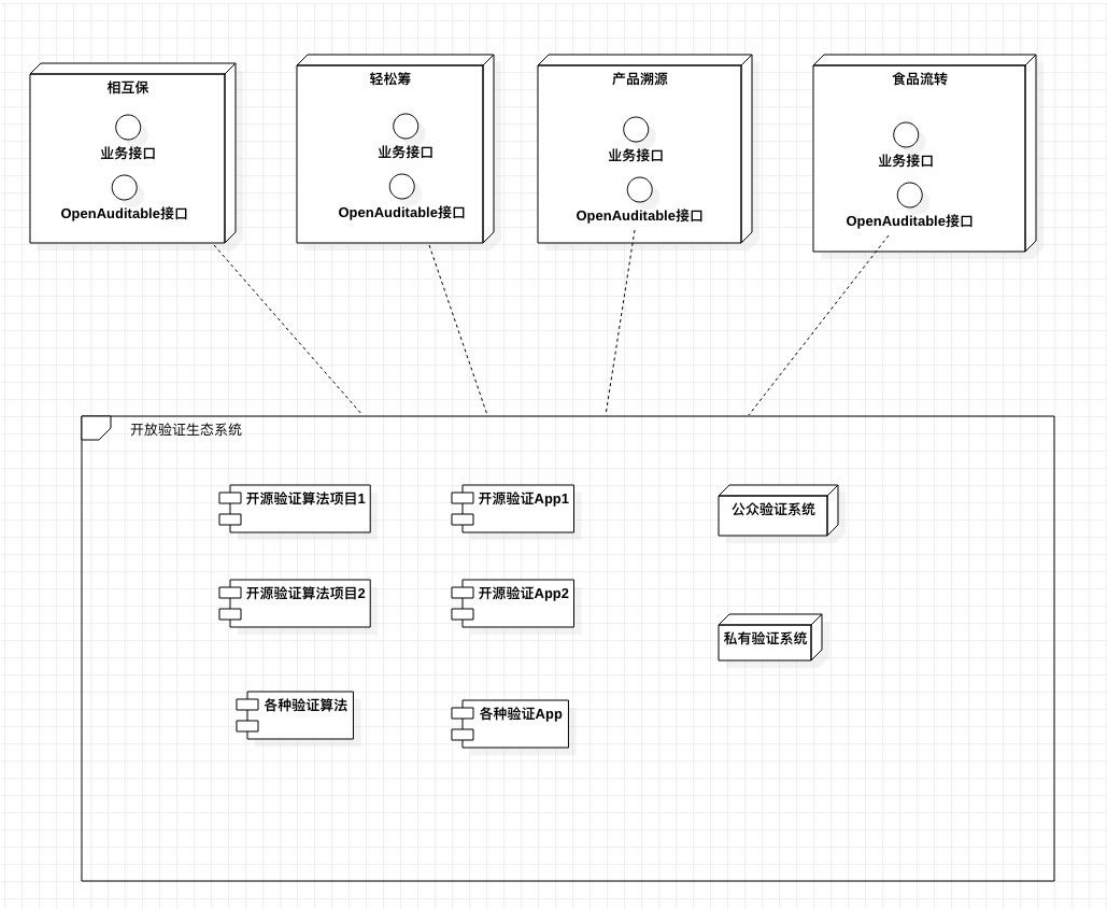

Figure 1OpenAuditable 系统组成

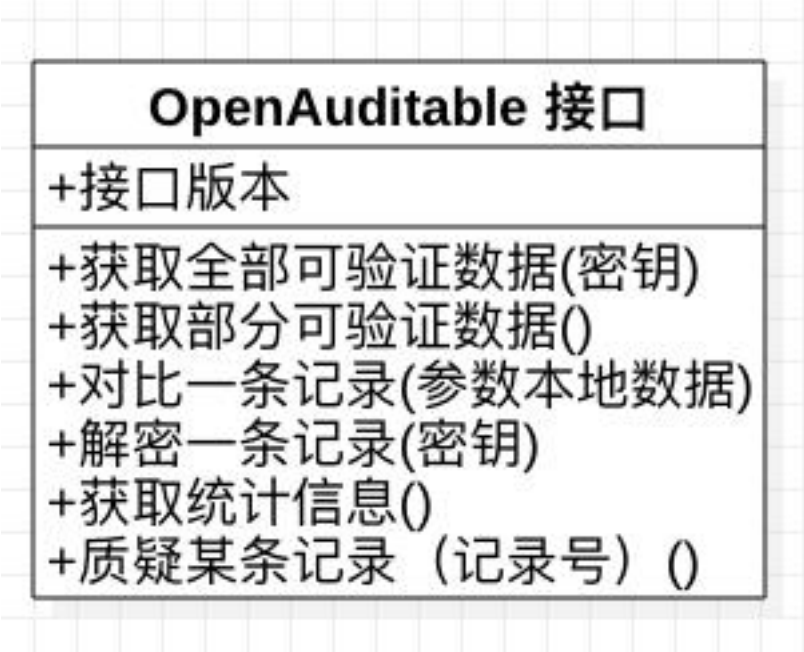

Figure 2OpenAuditable 接口

3. OpenAuditable 生态系统如何建立

OpenAuditable 架构成功的关键有两个：

1. 有大量软件实现 **OpenAuditable** 接口

如果这个架构获得社会认可，大量系统将实现这个接口是可以预期的。区块链技术之所以获得广泛关注和支持，就是他提供了一种建立信任的机制。如果 **OpenAuditable** 架构的成本更低，没有理由不被广泛接受，这个问题会在下面章节进行论证。

2. 验证系统建立起来并有效运转

开源社区参与验证算法和软件的开发是可以预期的，看看 **github** 上大量的开源项目我们就可以坚信，只要是社会需要的，就有优秀的程序员去实现他。另外，开发和运营验证软件也是有利可图的，即能提高组织或个人的知名度，也可以在 **App** 或网站里嵌入广告来获利。

4. OpenAuditable 架构有何优势

OpenAuditable 架构比区块链技术的优势有以下几个：

1. 验证系统是基于开放标准的中立系统，比起“相互保”这类靠自律的系统，更加可信。况且任何人都可基于标准制作自己的验证算法和工具，
2. 一个算法或软件可以验证多个或所有可信系统，节约了社会资源
3. 比特币每秒能够进行大约 **7** 笔转账（**2017** 年数据），而支付宝每秒可以完成 **10** 万笔交易。基于区块链技术的分布式系统，性能是个严重瓶颈。**OpenAuditable** 架构是在现有的中心化系统上加上开放和中立的验证系统，可以在不降低中心化系统的处理效率的前提下，提高系统的可信度。

5. 如何参与改善 OpenAuditable 生态系统

OpenAuditable 开放标准是系统核心，本作者创建的开源项目：https://github.com/dwchen1999/OpenAuditable，希望和众多参与者一起制定接口。希望更多开发者参与开源系统的验证算法和软件。