基于秘密共享的多方协作撮合服务系统设计

第 1 章 绪论

1.1 系统开发背景

信息技术不仅提升了工业效率，而且改变了团队合作的方式和合作理念。例如，人们可以在几分钟内通过发送电子邮件或更新到云服务器来提交作品，而不是乘坐出租车，花几个小时到达目的地，并将文件交给对方。另外，如果人们想建立一个网站作为他们公司的门户网站，他们可能不需要聘请一个正式员工来建立这个网站，而是可以在网上咨询自由职业者或者相关服务供应商。因此，限制员工时间和空间的传统工作形式将会逐渐消失，一种全新的合作方式将取代它。这样一来，每个参与者都可以专注于自己的专业知识，而不用将重点放在克服物理限制和就业人事关系等事务上。人们通过自己的专业技能和知识为需求而工作和努力，让平台服务管理人事关系，从而淡化雇主和雇员之间的界限概念。

目前来看，互联网上的“Elance”，“Odesk”和“Freelancer”等现有平台提供的众包服务，不利于保护用户的创意、隐私等重要信息。尽管这类平台造就了蓬勃发展的市场和互联网社会关系，但仍然存在一个重要问题需要解决：如何在保障用户信息安全的前提下，提升创造者和创新者的团队建设工作的效率和成功率？本文试图为解决该问题提出一个可行的解决方案并实现一套服务系统。

由于中心化设计本身存在难以解决的信任风险问题，本文会基于目前已经拥有成功实践经验的去中心化技术，设计新的平台结构，提供一个在具有去信任前提的同时也能够保障用户信息安全，且能够为需求供需双方提供可靠匹配服务的解决方案。

1.2 国内外现状

关于提供服务供需双方匹配的服务，国内业务和技术都比较成熟是“猪八戒网”以及“商理事”两大平台。其中“商理事”是基于企业资源共享和 SaaS 模式的企业合作撮合服务平台，运用企业智能、大数据技术以及云计算技术以尝试重构商业合作营销方式，以“企业网” 、“资源网”、“BD 网” 三网为中心，不同于传统的人工获取销售合作线索和粗颗粒度营销合作方式，融合商机搜索引擎、

商业数据库、商业资讯以及活动等功能，通过主动查询和智能推送为商业从业者提供企业资源服务。“猪八戒网”是服务众包平台，创办于 2006 年。涉及的服务交易品类涵盖创意设计、网站建设、网络营销、文案策划、生活服务等多种行业。“猪八戒网”有大量服务商为企业、公共机构和个人提供定制化的解决方案，将创意、智慧、技能转化为商业价值和社会价值。

与以上平台专注业务类似的国外服务提供商有以“Elance”为代表的大量外包网站，也有像“MatchPool”这样的创新类用户匹配服务网站。其中“Elance”是国外成熟的一套业务外包平台，外包项目类型以软件和网站为主，这个平台上包含平面和动画设计，网站设计，软件编码设计，商业计划寻找技术合作商等各类需求。其主要业务和模式都与国内的“猪八戒网”相似。而“MatchPool”则基于虚拟货币以及区块链等技术，加之新的匹配机制和算法，提供一个去中心化的用户社交匹配服务方案。

1.3 解决的问题

首先，创新创业者和普通社会公司员工之间的对于合作需的求的差异在于创新者通常需要保护他们重要的创意和资料，在寻找合作伙伴时不被能泄漏和被盗。因此，收集大量用户信息和私有数据的通用服务模式（集中式）具有严重的数据安全问题。一方面，创新创业者会考虑避免上传数据安全性重要的文件，因此很难获得一个找到合作伙伴的好机会。另一方面，即使有很多用户在网站上公开他们的想法，以吸引好的合作伙伴，很有可能使网站成为一个免费创意的搜索引擎，无法响应用户的期望。用户上传他们的信息和资料到网站，是因为用户相信它。但是，如果网站的运营商私下背叛用户，使用这些用户数据获得更高的黑色利润呢？没有人可以给出一个肯定的承诺，这样的问题不会在集中式技术中发生。因此，去中心化的解决方案能有助于我们找到一种相对正确的方法来保护用户的数据安全并保持服务的可信度。本论文提出的主要框架是设计为去中心化的分布式解决方案。它使用一些 Peer-to-Peer（以下称 P2P）技术和秘密分割加密来确保网络中没有包含所有或大部分用户数据的节点，用户可以自由选择多个节点来存储其信息片段。设计的算法和结构保护用户的信息片段不被恢复，除非相反是真正的潜在合作伙伴。

其次，大部分众包网站都像中介机构一样工作，其重点是把工作伙伴介绍到一起，但对于后续工作漠不关心。用户来到网站，使用其服务寻找好的合作伙伴。但他们的最终目标不是合作伙伴。他们想找到合作伙伴，是为作出一些作品或工作。最终的目标是让合作者们一起成功地完成一个工作。本论文希望通过使用智

能合约技术，让解决方案能够支持后续跟进工作。智能合约是一基于块链的概念和技术，它们像标记化程序一样运行，它们像网络上的任何其他东西一样具有公钥，但是它们具有代码，可以像存储过程那样“处理”业务。运用这样的技术可以通过规则的手段让供需双方签署生效的协议不受人为干扰地自动执行，最大化地保证了协议的公平性和严格性。

第 2 章 系统使用的概念和技术

2.1 中心化概念

在网络当各节点之间中有着明显从属关系或服务于客户关系的结构都可以考虑成一个中心化设计。其特点是所有的客户节点主要负者提出服务要求并接受和处理由服务端返回的数据，而服务端主要负责处理来自客户端的请求。网络当中存在一个中心节点或中心节点群，中心内的服务节点与中心外客户节点是对称但不对等的关系。所有的客户节点必须按照与服务节点的通信协议才能正常地工作。而且往往重要的数据都存储在服务端，从而导致大量的信息安全问题。

中心化架构并不意味着只有一个数据中心，它也可以是多数据中心的，如下图：

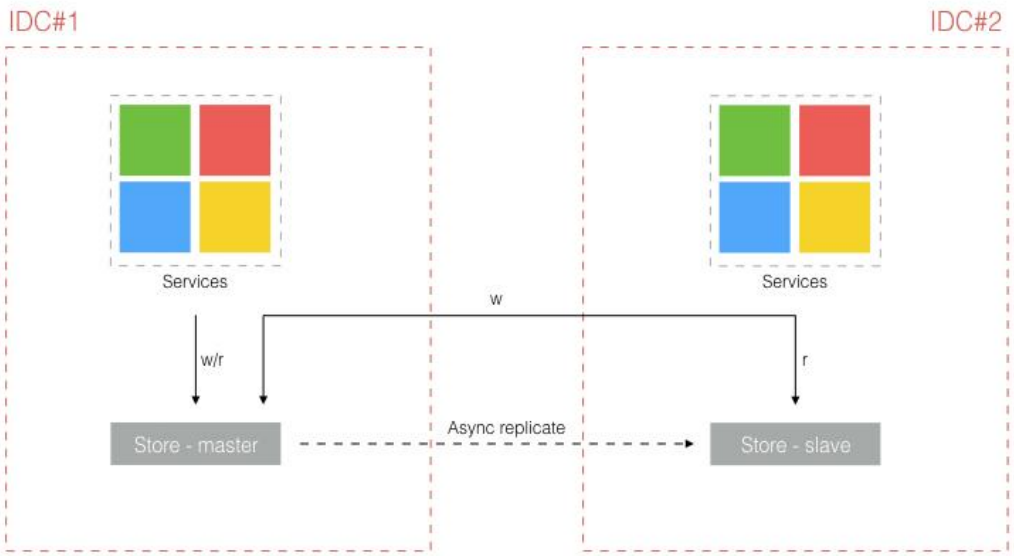

图 1：一个中心网络可以不仅仅只存在一个物理节点，服务器之间可以有从属关系，在保持对外抽象的一致性的同时提高服务处理能力和运算规模。

之所以说它是中心化架构，关键特征是其存在共享的数据存储。部署在两个

数据中心的应用需要共享访问统一的数据存储，而这种共享访问实际是依赖数据中心之间的专线连通，这样的架构也限制了能选取的数据中心地理位置的距离。而实现去中心架构的关键点就在于规避跨数据中心的共享存储访问，使得应用在其自身数据中心实现访问闭环。

2.2 去中心化概念

在具有许多节点的系统中，每个节点具有高度的自主性。节点可以互相连接，形成连接单元。任何节点都可能成为系统的中心，但不具有强制性的中央控制功能。节点和节点之间的关系将通过网络形成非线性因果关系。这种开放、平等和扁平化的系统现象或结构，我们称之为去中心化，它必须存在于具有大量节点或一组个体的系统中。

去中心化的系统中，通常每一个节点都平等地存储数据，而且相互之间存在一定的共识机制。同时，去中心化网络结构中的身份认证往往是匿名的、去信任的，从而保证每一个用户在保护自身信息安全的同时也能够与其他用户进行可信任的数据来往。

2.3 秘密分割方案

秘密共享（也称为秘密分割）是指在一组参与者之间分配秘密的方法，每个参与者分配一部分的秘密。只有当足够数量的可能不同类型的秘密碎片结合在一起时，才能还原秘密。个别碎片自身是没有意义的。

在一种类型的秘密共享方案当中，有一个分配者和 n 名共享人。分配者给予共享人一个秘密的碎片（也称为影子）。但是只有当具体协定的条件得到满足时，共享人才能从碎片中还原秘密。如果，分配者通过给予每个共享人一个秘密碎片，使得任何一组 m（阈值）或更多的共享人可以一起还原秘密，但是没有达到 m 名共享人则不能还原这个秘密。这样的方案被称为（m，n）阈值方案（有时它也被记为（n，m）阈值方案）。

秘密共享方案是存储高度敏感和非常重要的信息的理想选择。典型的示例有：加密密钥，导弹发射代码和银行账户编号等。这类信息中都必须保持高度的机密性，因为它们被曝光之后产生的影响是巨大的。但保证信息保密的同时也保证信息不被丢失是一件非常重要的问题。传统的加密方法不适合同时满足高水平的机密性和可靠性。这是因为当存储加密密钥时，必须选择在单个位置保存单个密钥副本以获得最大的保密性，再者是在不同的位置保留密钥的多个副本以获得更高

的可靠性。通过存储多个副本来提高密钥的可靠性的同时降低了机密性，而提高机密性则会降低可靠性。秘密共享方案成功地解决了这个问题，并且能够满足任意级别的机密性和可靠性。

2.4 非对称加密技术

对称加密算法加密和解密相同的密钥，而非对称加密需要两个密钥来单独加密和解密。非对称加密能为数字签名提供良好的安全保证。例如，若要在区块链的地址中操作比特币，则必须通过数字签名的验证。在比特币中，算法采用了椭圆曲线密码学（ECC）。用户可以通过 ECC 生成自己的私钥，再通过私钥可以生成相应的公钥。数字签名需要私钥进行签名处理，此证书和公钥将发送给收件人进行验证。在比特币的 PoW 协议区块链中，接收者是参与到区块链维护的挖掘节点，每个节点也维护着整个区块链数据的数据。对于交易的验证，它需要使用接收的公钥进行检查，验证其是否由私钥持有者发送，并且公钥可以通过两次特殊的哈希生成唯一的地址。验证完成后，地址中的比特币就可以运行。每个用户在比特币钱包应用程序中都有自己的私钥，而且私钥不会在网络上传播，它可以生成独特的相应公钥，公钥可以生成唯一对应的地址。整个区块链数据是公开的，任何人都可以查看块中的数据。想要操作比特币就必须知道相应的私钥。而使用不同明文数据进行安全哈希运算得到相同哈希值的概率非常低，所以几乎不可能获得与其地址对应的私钥。

2.5 区块链技术

区块链本质上是一个简单的链式数据结构。具有点数量具有随时间增加、数据不可修改、开放且支持匿名等诸多特点。每一个区块与特定信息相互捆绑，整个区块链是分布式、P2P 和去中心化的。当前已经成功应用了区块链技术的案例有“比特币”（Bitcoin），“以太坊”（Ethereum）等虚拟货币，以及由微软的身份认证服务为代表的区块链 2.0 技术支持的产品。

区块链可以被看作是一个数字账本，并且其区块和支链的维护需要通过多个节点合作进行。在“比特币”的应用中，每个矿工计算机都是一个有效节点，每个节点都在本地存储整个区块链的数据并一直更新。对于一个新的事务（我们把所有的数据操作称为区块链的交易，对应于比特币则是一个输入和输出的数据流），许多节点都需要进行检查其是否有效的确认工作，这需要节点之间建立安全合理的共识机制。

区块链采用匿名的方式存储和访问数据。以“比特币”为例，每个比特币都有其唯一的地址，也就是区块当中的一个标记。这种地址是经过安全哈希变换后的哈希值字符串。虽然地址是开放的，但为了能保证匿名功能的同时具有极强的安全性，不可或缺的就是非对称加密技术及其签字技术来支持比特币地址的相关操作。

第 3 章 系统需求分析

2.1 系统概述

2.1.1 总体描述

本论文中的提出的系统主要面向既有合作需求也需要保证自身信息安全的网络用户，作为一个完整的解决方案，同时也是一个应用平台，解决社会当中安全合作过程的关键问题。从而试图推进一个更好的合作模式，让用户可以无需顾虑过多的信息安全问题，同时也能大大提高匹配服务的成功率。

目前市场上已有的此类系统基本存在着以下问题，也正是本论文需要解决的问题：

1）中心化服务导致的集中化管理数据的方式不可避免地存在一定的信息安全问题，易被盗取、篡改和滥用。

2）合作撮合的准确度不高。采用搜索引擎方式进行合作信息查找，有效的匹配结果出现的概率并不高。

3）合作进行过程当中的信用度不能保证，存在单方面诈骗行为的可能。

本论文设计的系统适用于任何具有合作、撮合需求的人群，无论是公司的大型项目、还是个人的创意想法，都可以在我们的平台上寻求合适的合作；而且该平台更擅长支持对合作内容对保密需求、撮合准确度需求有一定高度要求的一类用户提供更好的服务。

用户无论在公司还是家中，通过浏览器即可打开我们的平台主页，我们的平台具有良好的交互性来为有需求的客户提供服务，其操作方式尽量相似于传统的撮合平台使用户更好的上手使用。

2.1.2 业务描述

合作需求者（即用户）将自己的需求通过入口网站发布在我们的平台，而我们的寻求合作者，通过将自己所具有的能力指标提供在我们的平台之上，后台通过一系列的匹配、认证来进行合作撮合，我们会验证合作者与被合作者的需求和要求是否具有一致性，在不具有这样的一致性时，双方的信息都不会被对方直接搜索出来，这样的方式尤其对于对自己个人信息、项目信息有特殊安全性、保密性要求的用户提供可信的服务，同时我们能够提供更加准确、有意义的撮合结果。

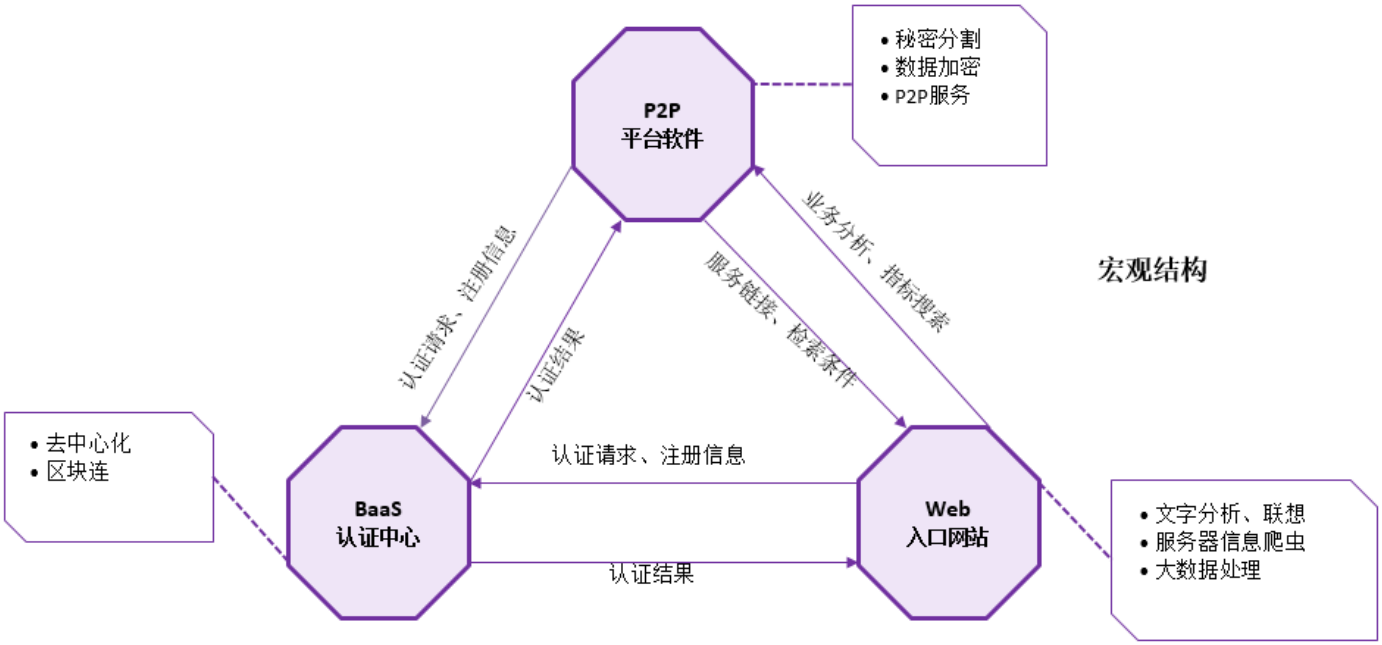

图 2：