┊┊┊┊┊┊┊装┊┊┊┊┊┊┊订┊┊┊┊┊┊┊线┊┊┊┊┊┊┊

**大连海事大学**

**毕 业 论 文**

**二○一七年六月**

基于秘密共享的

多方协作撮合服务系统设计

|  |  |  |
| --- | --- | --- |
| 专业班级： | 软件工程3班 |  |
| 姓 名： | 廖 添 |  |
| 指导教师： | 李 志 淮 |  |

信息科学技术学院

**摘 要**

目前来看大部分合作平台倾向于尽可能地收集用户信息，将其加入到搜索引擎的资料库中，以便其他用户进行匹配。这种简单直接的服务模式虽然能够在一定程度上解决不同用户之间寻求合作的需求，但还不够理想。本论文所设计的系统更专注于寻找和设计一个有效的解决方案，提供精细化、智能化的合作匹配服务。旨在严格保护用户个人信息的同时，更能够非常准确的匹配出一个合适的合作结果。而且相较于目前流行的中介服务模式，更加安全和智能。

系统为用户提供的所有服务都围绕着四个基本原则进行设计：1.严格地保护用户信息安全；2.使用分布式计算结构将服务分散化；3.允许具体服务具有多版本，能够精细化、快速演进迭代；4.支持模糊计算、同时可将服务智能化。通过保证这四个基本设计原则，能够有效地保证系统在设计和开发的过程当中始终不偏离最初的设想和要求。

本论文先从阐述设计一个安全的合作撮合系统的必要性和相关背景开始。介绍系统使用和依赖到的若干关键基础技术，并举例其典型的应用方式和案例。然后再描述系统方案的需求分析、概要设计和详细设计，逐渐地绘制一个清晰完整的系统轮廓。最后展示系统的原型和相应的测试用例。具体以若干完整的假设用户和场景，通过数据和结果来论述系统的功能和效果。

**关键词：合作；匹配；信息安全；P2P；秘密分割；区块链**

**ABSTRACT**

At present, most of the cooperation platform tends to collect user information as much as possible, add it to the search engine database, so that other users can use them to match their requirements. This simple and straightforward service model, although able to a certain extent, to solve the needs of different users to seek cooperation, but not ideal. The system designed in this paper is more focused on finding and designing an effective solution to provide a meticulous and intelligent partners matching service. Designed to strictly protect the user's personal information at the same time, more able to match the exact match with a suitable result. And compared to the current popular intermediary service model, more secure and intelligent.

All services provided by the system are designed around four basic principles: 1. Strict protection of user information security; 2. Use of distributed computing architecture to decentralize services; 3. To allow specific services with multiple versions, to refine, fast evolution iterations; 4. Support fuzzy computing for providing intelligent services. By ensuring these four basic design principles, can effectively ensure that the system in the design and development process which does not always deviate from the original ideas and requirements.

This paper begins with the necessity and background of partners matching services. Introduce the key technologies used by the system and rely on, and give examples of its typical application and case. And then describe the requirements of the system program analysis, summary design and detailed design, and gradually draw a clear and complete system profile. Finally show the prototype of the system and the corresponding test cases. Specifically with a number of complete assumptions on the user and the scene, through the data and results to discuss the system functions and effects.

**Keywords: Cooperation, Matching, Information Security, P2P, Secret Sharing, Blockchain**

目录

**未找到目录项。**

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。

下面列举分析现有网络平台所存在的问题：

1) 集中化存储个人用户信息，信息泄露风险高，并且存在平台私自利用用户信息进行保密协议外其他用途的可能风险。仅中国范围内，据中国互联网协会的一项调查报告，国内网购用户的规模已高达约4.8亿人，其中过半在网购过程中经历过个人信息泄露的不幸遭遇，而由此造成的经济损失每年高达915亿元。

表1：近年发生的用户数据泄露事件举例

• 雅虎，时间2016年9月，受影响用户数量至少5亿；

• 英国宽带服务提供商TalkTalk，时间2015年10月，受影响用户数两至少400万；

• 智联招聘，时间2014年12月，86万条求职者简历数据泄露。

对于信息安全敏感的创新创业者和自由工作者们来说，采用数据集中化管理办法的平台不能给予他们足够的安全需求（至少在现今的安全环境之下）。假如为了保证用户信息安全而又过度封闭用户信息又将导致另外一个重要矛盾的产生：寻找到一个合适的合作伙伴需要逐渐地互相公开一定的敏感信息。这也是我们要描述的第二个问题。

2) 信息公开与封闭的矛盾致使现有平台表面上来看能够解决合作伙伴的寻找问题，不过实际运用当中会发现：很多有价值的项目或创意急需有能力和相同志趣的人与之合作，但要想寻找到这样的合作伙伴若不公开一部分项目核心内容是不可能轻易完成的任务，而公开项目核心内容于互联网中是显然绝对不可行的办法，剽窃和抄袭等问题会将无法解决。

本论文的目标正是力图为致力于创新创业事业的用户们提供一个能够保障信息安全的、合作撮合高效的网络平台。一直以来创新者都处在一个比较尴尬的合作困局当中，即拥有独特创新的想法和理念，甚至是一个成熟的设计方案，但在现代社会当中抛弃合作仅凭一己之力是几乎不可能成功完成一项合格的创新创业事业；然而如果选择合作，又面临着不方便过度透露自己的创意以防止知识剽窃行为，但若不透露关键信息又难以寻找到真正的合作伙伴。如此矛盾的合作撮合困境可能在无形当中抹杀了许多非常优秀的创意创造走向实现道路的机会。

该解决方案不同于以往的传统网站平台，而是采用去中心化设计的方式尽最大可能保证用户信息的不受制于任何一个特定的运营商；同时，通过我们设计的解决方案，创客双方根据自身的技术能力与合作需求能够更准确的将自己的部分信息公开与需要与之公开的可能合作对象，避免了无关人士对于重要信息的访问，从而在一定程度上保证了创客们的创意与技术秘密的安全；而且鉴于用户账户注册数据集中化之后产生的安全问题，该解决方案将采用区块链即服务(BaaS, Blockchain-as-a-Service)的技术制作认证服务平台以担任整个方案中的认证任务。

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：

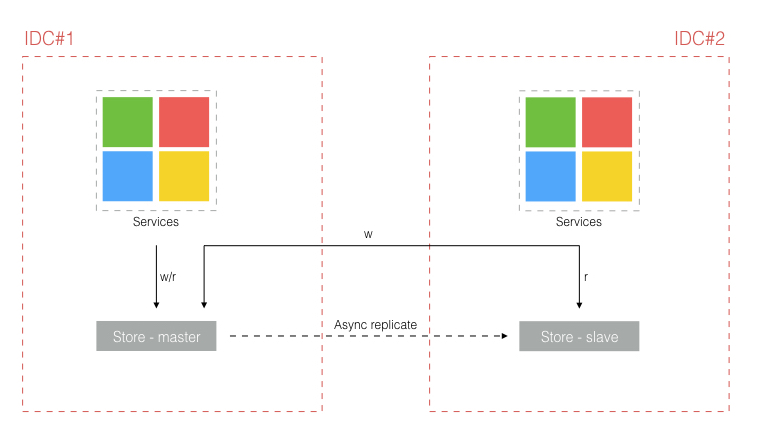


图2：一个中心网络可以不仅仅只存在一个物理节点，服务器之间可以有从属关系，在保持对外抽象的一致性的同时提高服务处理能力和运算规模。

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相关操作。

第3章 系统需求分析

2.1 系统概述

2.1.1 总体目标

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，通过浏览器都可以访问打开系统的网页，因为系统平台具有良好的移动性和交互性，利用Web服务无需提前下载应用的优势，尽最大努力为有需求的客户提供便利的服务。其前期操作方式与传统的平台相近，因此有利于用户从其他传统平台迁移到该系统提供的平台上。

系统的基本目标以及要求有：

1）保证用户在寻找合作伙伴过程中使用的数据和信息的安全。通过去中心化的设计，防止数据的存储、管理、收集的权利过于集中，防止任何一方滥用侵犯个人隐私和威胁数据安全大数据技术。

2）设计对使用者、开发者、客户端用户、服务用户均友好的交互方式。既要保证健全的开发接口、调试接口和配置空间，也要为客户端用户提供能够简单上手、低学习成本的交互方式。因此，所有核心操作都由命令行风格的程序完成，而客户端单独设计具有图形化界面的工具，辅助用户进行操作。

3）用户账户使用匿名的方式，采用基于区块链的身份认证方案，必要情况下考虑集中化的用户开户审核方式。最大化地保证用户在进行数据交换时的身份确认建立在由密码学保证的去信任环境上。

2.1.2 业务描述

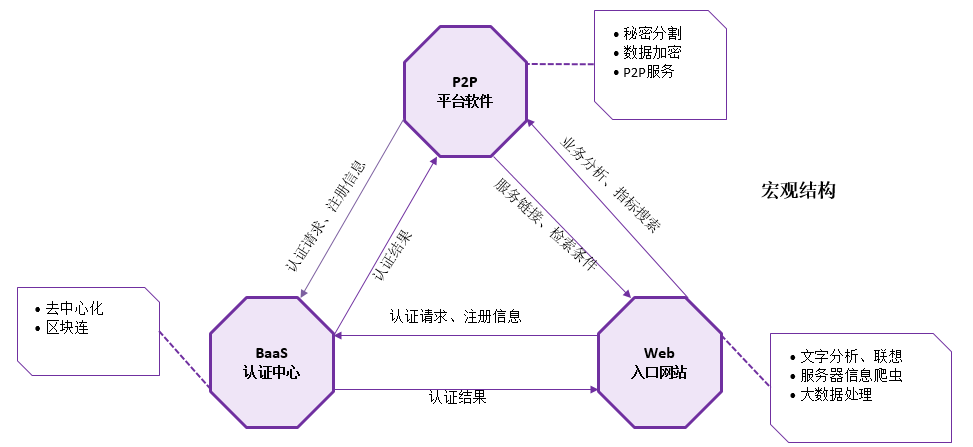


图2：整个系统的工作需要三个相对独立的模块（或称角色）互相提供支持才能为用户提供合作伙伴的匹配服务。

系统的主体业务是帮助合作供需双方能够安全地寻找到合适的合作者。首先一方合作寻求者将自己的信息资料通过不同的需求和要求标准发布至平台，以供系统进行用户匹配。系统会根据合作寻求者的要求，如指标数据，来按照不同服务器自定义的算法进行双方或者多方匹配。整个匹配过程只有进行匹配运算的服务器和提交指标数据的用户知道详细的指标数据和算法，其他无关匹配和信息服务器无法通过正常方式窃听到有关信息，从而最大化地保证了用户信息的安全。然后，当有另一个合适的合作寻求者向平台提交其合作需求和指标时，系统就会将其匹配出来。当每个匹配服务成功匹配出一对指标时，匹配服务器将把当时双方提交的信息资料的碎片发送到对方。当获得到的信息碎片数量满足还原条件时，原始的信息将会被用户在本地计算还原。此时服务双方的撮合任务就完成了。如果双方选择在特定的业务按特定的规则开始合作，则平台可以开始后续的合作跟进服务。

为在本论文当中更好地描述业务流程以及系统参与者的动作、属性和任务等各项特性，现使用若干角色代表不同的用户、程序和服务器，明确地分配业务内容和阐述业务关系。这些角色有：

1）终端用户角色。即用户，是系统提供的主要服务的最终使用者。

2）服务供应角色。为终端用户提供指标服务，主要负责用户数据存储，指标匹配以及服务映射功能。

3）搜索引擎角色。针对用户提供的简单需求描述，尽可能地提供最符合用户需求的服务供应条目以供用户选择，从而提高系统的使用效率、降低使用门槛和学习成本。

4）身份认证平台。对各个角色的身份进行管理和认证，以保证系统的安全运行。

5）保险柜角色。针对个人用户的私钥存储问题，提供一个保险柜平台帮助用户管理私钥。



图3：目前互联网中的主要角色及其结构的简单图示。

互联网本身是去中心化的结构，每一个网站都是相对独立的，每一个用户也不例外。为了让用户更容易、更简单地访问到合适的网站，一个被称为“搜索引擎”的角色的网站出现，为用户分析其访问需求，并提供经过筛选的合适的网站链接。这样一个结构非常稳定和安全。因为去中心化的结构，保证了没有任何一个搜索引擎、网站、用户对于整个网络来说是必不可少的。例如，没有“Google”用户仍然可以使用微软的“Bing”或是百度来代替它。

类比这样的结构，本论文所设计的系统在网络当中的存在形式及其相似，如图4。



图4

其特点是：

1）去中心化的服务结构。整个解决方案当中没有任何一个独立节点能够收集用户的完整信息。

2）与现有网络运行模式相兼容，不存在重新建设基础网络设施的成本。

3）面对用户拥有一致的用户接口，降低普通用户使用该解决方案的学习成本，具有快速推广的潜力。