基于区块链技术的股权众筹模式构建

韩笑天　马超群（湖南大学工商管理学院　长沙　410082）

中图分类号：F830　文献标识码：A

内容摘要：当前环境下，我国的众筹是以众筹平台为中心进行的募资、运作模式。在该模式下，存在着监管难、信用缺失、欺诈风险等问题。而比特币的底层技术——区块链技术具有着去中心化信用、不可篡改、可编程的特点，日益成为学界和产业界研究的热点。本文基于区块链技术提出一种去中心化的股权众筹架构，在该架构下可以起到降低交易成本、便利监管、去中心化等作用。但由于区块链网络建设的工作量庞大，本文建议以政府为主导，建立起全社会可使用的区块链网络。

关键词：比特币　区块链技术　去中心化　股权众筹架构

众筹的概念及发展现状

众筹（crowd funding）是2009年出现的网络商业模式，是基于互联网平台的融资创新，由发起人、跟投人和平台三部分构成。其显著特征包括低门槛、创新性、众包交互等。基本模式是通过互联网平台，由发起人向整个平台用户展示项目，用户通过查阅发起人公布的信息决定是否参与投资。

近年来，众筹发展迅速，以众筹方式在全球募集的资金总额逐年上升。Massolution研究报告指出，2013年全球总募集资金已达51亿美元，其中90%集中在欧美市场。世界银行报告预测到2025年总金额将突破960亿美元，亚洲占比将大幅成长。

众筹融资发展迅速，但仍有诸多问题难以解决。首先，众筹依托于平台进行融资，每个平台在融资过程中收取手续费作为平台运营成本，以人人投股权众筹平台为例，该平台将收取总融资额的5%作为手续费，变相地增加了众筹融资的交易成本。其次，众筹平台作为中心化机构，起着担保项目真实性的职能，然而面对互联网的纷繁信息，依靠平台审核，效率低下。此外，众筹过程中的欺诈行为同样难以防范，在众筹平台上，投资者之间没有个人联系，对拟投资的项目也缺乏实际了解，地理分隔也使投资者难以去监督所投项目的业务运营状况，这些诸多因素增加了众筹欺诈的风险。

众筹及区块链技术研究现状

（一）众筹的研究

国内诸多学者对于众筹的研究主要集中于众筹商业模式的探讨以及规避风险的措施。刘明（2015）研究了美国《众筹法案》的集资门户的法律问题，对众筹平台的监管有着借鉴意义。胡吉祥、吴颖萌（2013）探讨了众筹融资的发展及监管，指出了当前众筹行业存在的诸多难题并给出了解决手段，然而这些手段可实施性差、生效慢，难以根除问题。李雪静（2013）研究了众筹融资模式的发展，从历史角度对众筹融资进行了解析。杨东、苏伦戛（2014）研究了股权众筹平台的运营模式及风险防范，该文详细地阐述了发起人创办项目、投资人投资项目、后续资金跟进等一系列流程，并介绍了以平台为中心机构的信用认证过程。范家琛（2013）则主要研究了众筹商业模式，指出众筹平台起着价值匹配的职能，并依靠该职能进行商业盈利。

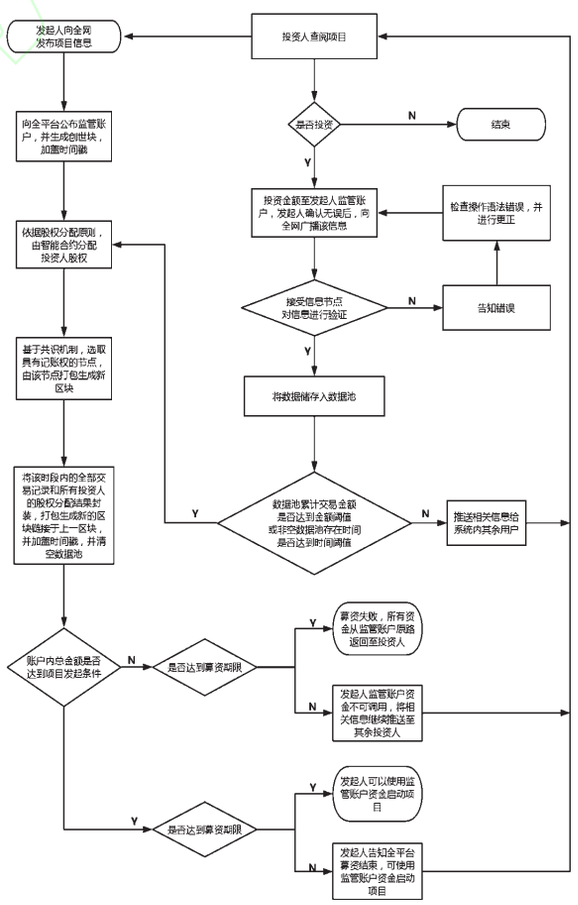

图1　基于区块链技术的股权众筹项目募资流程图

现今的众筹大部分仍是依靠一个中心化的平台，并通过平台审核的方式为项目进行担保，平台除了信息匹配之外，也起到一个中心信用机构的作用。而在众多研究中都囊括了众筹的风险问题，不难看出，即便是有一个中心化的信用机构，风险规避仍是一个大大的难题。

（二）区块链的研究

区块链是比特币的底层核心支撑技术，具有去中心化的核心优势。区块链运用数据加密、时间戳、分布式共识和经济激励等手段，在节点无需互相信任的分布式系统中实现基于去中心化信用的点对点交易、协调与协作， 从而为解决中心化机构普遍存在的高成本、低效率和数据存储不安全等问题提供了解决方案。随着数字货币的快速发展，区块链技术也获得了国内外诸多学者的关注。袁勇、王飞跃（2016）详细地介绍了区块链技术，对区块链系统中的六个层次即数据层、网络层、共识层、激励层、合约层和应用层，进行了详细的剖析。蒋润祥、魏长江（2016）探讨了区块链的应用进展与价值，并在文中展示了区块链运用的诸多实例。陈一稀（2016）则讨论了区块链技术的不可能三角问题，认为在区块链发展中需要在高效低能、去中心化、安全三个层面上进行平衡，是一个在实际应用中值得思考的问题。任安军（2016）则思考了在票据市场上运用区块链技术的可能性，对本文有启示作用。

区块链技术本质内涵及功能

（一）区块链定义

区块链缘起于比特币，虽然外界对于比特币的观感起起落落，但作为底层技术之一的区块链却日益受到重视。在区块链技术中，区块（block）是一个储存单元，分为区块头和区块体两个部分。其中，区块头封装有当前的版本号、前一区块地址、当前区块哈希值、共识过程以及时间戳等信息；区块体则包含当前区块的交易数量以及经过验证的、区块创建过程中生成的所有交易记录。外界通过访问一个区块的区块体就可以获得生成该区块时间内的所有交易记录；通过访问区块头中的时间戳就可以获知创建区块的时间；通过不断访问前一区块的地址，就可以追溯整个系统中所有的交易记录。每一个区块通过地址与前一区块进行链接，因此形成了区块链系统。

（二）区块链是如何记账的

除了区块链中记录数据的数据层外，网络层起着在系统内起到连接网络、传播数据消息和数据验证的功能。每当一笔新的交易发生，将会在全网进行广播，收到消息的节点将对数据进行验证，对无效数据将会舍弃，如果数据有效则将对未写入区块的数据建立储存池并继续向系统中的其他节点进行广播。在网络层进行充分传播之后，全网将对储存池中的所有有效数据进行认证并打包生成一个新的区块链接到区块链系统中，依据不同的共识机制有不同的认证方法，例如比特币中的 PoW 共识、类似于董事会决议的DPoS共识、权益值最高用户认证的PoS共识等机制。在不同的机制下，对承担起打包数据生成区块链的用户和承担认证数据职能的节点，区块链网络中通常会通过给与奖励的方式进行激励，例如在比特币中，优先解出 PoW 共识的节点用户将会获得比特币奖励。

（三）区块链安全性

1. 用智能合约解决实际问题。区块链系统还支持智能合约，所谓的智能合约是由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的计算机程序，能够实现主动或被动的处理数据，接受、储存和发送价值，以及控制和管理各类链上智能资产等功能。在合约层中写入智能合约的方式，让机器代替人类起到监督系统各方面的作用，并自动分配股权收益，只需要及时对智能合约进行修改、补充，便可以大大地降低众筹过程中的操作风险。

2. 区块链加密技术。由于每个区块均与前一区块相连，并加盖有时间信息的时间戳，因此网络中的任何用户都可以访问到自创式区块开始的所有记录，这也意味着对数据进行篡改需要同时篡改区块链系统中的所有区块，过高的篡改成本有效地规避了风险的发生。同时，每一笔交易数据都需要经过几乎全网所有节点的验证，作假成本同样高昂。通过非对称加密技术、哈希函数等方式，在信息共享的环境下依旧能够有效地保护节点用户的隐私以及个人资产安全，并且区块链作为去中心化的机构，自然而然地起到了降低交易成本的作用。此外，通过全网认证、数学加密的手段，在去中心化的系统中保证项目的信用。因此，区块链技术应用于众筹领域，能够有效地规避众筹风险，降低交易成本，促进众筹行业的更快发展。接下来，本文将提出一种基于区块链技术的众筹模式。

基于区块链技术的股权众筹模式

（一）众筹模式：募资

第一，基本流程。首先由项目发起人向整个平台发布项目的相关信息，该项目可以在区块链平台中被所有用户检索并查看相关信息。当投资人查阅信息之后，若对项目产生投资意向，即可对项目进行投资，在线上投资人在区块链平台中提交自己的投资信息，在线下投资人打款至发起人向系统提供的监管账户。接着，当发起人确认资金信息无误后，发起人将向全平台广播该信息，接收到该信息的节点将对该信息进行验证，主要验证在投资过程中是否合规以及是否存在系统语言错误。若检验通过，则将该信息储存入节点的数据池，并继续向邻近节点转发该信息。

由于在募资过程中只存在投资过程，不存在其他交易行为，因此当数据池积累的募集资金数据达到金额阈值或者非空数据池存在时间达到时间阈值之后，将会对信息进行打包并进行封装。设置金额阈值是为了避免产生过多的数据区块来增加系统的可读性难度；设置时间阈值则是为了避免数据池存在过长时间从而导致交易信息无法及时写入系统的弊端。

当数据池达到阈值之后，将由共识机制决定记账权的归属，由具有记账权的节点对数据池中的数据进行封装打包。基于不同的共识机制有不同的归属方式，在比特币系统中是采用 PoW 共识机制——高度依赖节点算力的工作量证明，即最先解出哈希函数的哈希值的节点将具有记账权并获得比特币奖励。由于 PoW 机制过度依赖于强大的算力，在一定程度上造成了资源的浪费，故不适用于众筹模式下的区块链系统。本文建议在区块链系统初期采用 PoS 共识机制进行记账权确定，在用户节点增至足够多了之后采用 DPoS 共识机制来进行记账权确定。

第二，PoS 共识机制和 DPoS 共识机制。PoS 共识机制：赋予全网的最高权益用户记账权而不是全网最高算力的用户。什么是最高权益，在 PoS 共识机制中引入了“币龄”的概念，币龄是特定数量的币与其最后一次交易的时间长度的乘积。用“币龄”去衡量用户的权益，譬如一个用户在众筹过程中为项目投资了 1 万元人民币，则十天后该用户的“币龄”为 1*10=10。越早进入的用户将获得更多的币龄，投资额越多的用户也将获得更多的币龄，因而越早、越多的用户将具有更高的权益。由权益最高用户行使记账权具有一定的可靠性。DPoS 共识机制：当进入项目的用户足够多了之后，将由 PoS 机制转变为 DPoS 机制，类似于权利从独裁转向民主。DPoS 共识机制类似于民主投票，系统中的所有节点将自身的股份权益作为选票进行投票，获得票数最多且有意愿的节点将进入“董事会”，按照一个既定的时间表依次行使记账权，并对生成的新区块进行签署。此外，在每一个成员行使记账权时，必须验证前一个区块已被签署。被票选出来的节点必须对整个系统中的其他用户负责，如果某个授权节点错过了其本该签署的区块，则系统内的其他用户将收回自己的选票并剥夺该用户的记账权。

基于 PoS+DPoS 共识机制，合理、有效地解决了记账权归属问题，从而避免了重复记账问题。在进行记账时，将由区块链系统对系统内所有用户的投资额进行汇总，更新每个用户的股权份额。该过程可以由内置的智能合约来完成，由于项目的不同，股权分配的原则也不尽相同。

第三，判定过程。当决定生成区块时，数据池中的所有募资记录将会被打包封装进一个新的区块。值得一提的是，区块并不会直接储存原始的数据或是交易记录，而是将其编码成特定长度的由字母和数字组成的字符串后记入区块链，该过程也被称为生成哈希函数。在比特币区块链系统中，采用的是双 SHA256 哈希函数，该哈希函数具有巨大的散列空间（2 的 256 次方）和抗碰撞特性（不同的输入值不会生成同样的哈希函数），哈希函数广泛的映射空间足可以胜任在众筹过程中庞大的记录工作。区块链还采用非对称加密技术给与每个用户一个公钥和一个私钥，全网用户可以依据公钥获取该节点加密的信息但不具有修改权，只有具有私钥的用户才具有修改权。而所谓的非对称加密，则是指无法通过公钥来反推出私钥，该项技术在区块链的应用场景主要包括信息加密、数字签名和登录认证等。对数据封装完成之后，对区块加盖时间戳并签署个人签名，链接到上一区块。通过访问一个区块，就可以获得上一区块的地址，层层递推就可以获得所有的交易数据，不仅方便节点用户获知项目状况，也便于监管机构的有效监督。同时，如果要对区块链进行篡改，则需要对所有区块的数据进行篡改，而每个区块是由不同的节点进行签署的，这就意味着篡改数据需要知道所有具有记账权节点的秘钥，进而进行修改。如此高的作弊成本成为了一道无形门槛，降低了众筹集资环节的风险。

在生成了一个新的区块后，系统将进行两次判定，即当前募资金额是否已达项目开始条件及是否达到募资期限。若金额已足够且已达募资期限，则发起人可以使用监管账户来实践自己的项目，发起人将向全平台进行公告终止募资；若金额已足够且未达募资期限，则发起人向全平台公告募资已达标，终止募资，并可以使用监管账户来实践项目；若金额不够且已达募资期限，系统宣告该项目募资失败，投资金额从监管账户原路返回至投资人账户；若金额不够且未达募资期限，则发起人无法使用监管账户内的资金，平台将继续推送该项目的信息给平台内的其他投资人。图 1 用流程图的方式解释了区块链股权众筹模式的过程。

（二）项目运作模式及盈利流程

1. 运作项目形式。在项目运作过程中，发起人每调用一笔监管账户内的资金，需要向区块链平台提交包括金额数目、金额用途、金额去向等信息，并在全平台进行广播。接收到该信息的节点主要检查信息的语法、合规的问题，如果发生信息打包语法错误或者不合规的问题，则发起人需要修改信息。值得一提的是，本步骤只是保证程序合法，并不能由系统自发地查出发起人的欺诈行为，但由于银行在监管账户的公信力和区块链平台的不可篡改的属性，资金流动可见，监管部门的监督是非常便利且有效的。当信息无误后，信息将会被存入数据池中，当数据池积累的募

集资金达到金额阈值或者非空数据池存在时间达到时间阈值之后，将会对信息进行打包并进行封装。接着是决定记账权归属问题，由授权节点打包生成区块链，该过程既可以采用 PoS 共识机制，也可以采用 DPoS 共识机制，视整个系统的大小及投资人的投资额度而定。在记账过程中，同样地采用哈希函数对该时段内的所有交易信息进行封装打包，生成新的区块并链接于上一区块，加盖时间戳并由授权节点进行签署。该过程就是基于区块链技术的股权众筹项目运作流程。

2. 项目盈利后的分红部分。在项目盈利分红部分，首先由发起人将盈利资金存入监管账户并注明盈利资金，接着由之前向平台提交相关数据，由智能合约计算分配额，并依照合约计算结果由监管账户向投资人账户汇款。接着，收到分红的投资人向全平台广播分红信息。接收到该信息的节点主要检查信息的语法、合规的问题，如果发生语法错误或者不合规的问题，则需要修改信息。当信息无误后，信息将会被存入数据池中。当数据池积累的分红资金达到金额阈值或者非空数据池存在时间达到时间阈值之后，将会对信息进行打包并进行封装。同样，可采用 PoS 共识机制或者 DPoS 共识机制来决定记账权归属，产生授权节点并对数据池中的盈利金额、红利分配结果、盈利来源等信息进行封装打包生成新的区块，并链接于上一区块，加盖时间戳并由授权节点进行签署。该过程就是基于区块链技术的股权众筹的盈利分红流程。

区块链技术的优势及不足

（一）区块链技术的优势

本文基于区块链技术，提出了一种基于区块链技术的股权众筹项目的架构。在区块链技术下，股权众筹可以做到去中心化，脱离众筹平台来进行众筹，降低了众筹过程中的交易成本。同时，由于信息的公开和日益先进的加密技术，用技术来作为信用凭证而不是由一个中心化的机构来为信用担保，降低了信用风险，更加地可靠。由于区块链的发展尚处于起步阶段，因此采用监管账户，在线下借用银行的中心信用来加强区块链的安全性。区块链的数据和监管账户的流动记录，为区块链股权众筹提供了双重保险。在交易过程中，由系统内置的智能合约和预先编写好的代码来执行操作，降低了人工操作中可能存在的操作风险。同时，对于监管部门而言，通过遍历区块链中的所有区块，就能够获得所有的交易数据，并依据时间戳在数据中引入了时间维度，配合监管账户在监管层面将更加地便利和易于审计。此外，区块链系统还支持智能合约应用，通过编写不同的智能合约，区块链系统可以适应于各种环境下的不同众筹需求。

（二）区块链技术的不足

区块链技术作为时下的热门技术，仍存在着诸多不足之处。譬如 PoW 共识机制过于苛求节点的算力，造成了一种资源浪费，而每个节点逐一查验，从宏观角度浪费了全网的资源，因此存在着高效低能的弊端。正如陈一稀（2016）在文中所指出，“安全”、“去中心化”和“高效低能”是一组不可能三角，区块链技术做到了前两项，在第三项不可避免地产生了某些缺陷。另外，随着数学、密码学、超级计算机的不断发展，区块链的非对称加密算法也存在着被破解的可能，需要不断地更新区块链加密算法以规避潜在的破解可能。同样，尽管加密算法在现今难以被破解，也存在着用户私钥保存不当被黑客盗用的危险，这是互联网时代无法避免的风险之一。但正如银行遭遇抢劫不能否定整个货币体系，私钥被盗风险也不能成为否定区块链的理由。此外，虽然有以太坊此类的开源的区块链平台可以直接用于股权众筹区块链网络的架构，但从信息安全和促进国内经济发展的角度考虑，我国应尽快构筑我国的区块链平台。尽管可以通过维护、更新等措施从技术角度向全网用户收取一定资金作为运营成本，但区块链平台的架构仍是一件费时费力的事情，还需要完成诸如账户对接、写入协议、系统维护等多项职责，作为未来可能覆盖全球的一项技术，任何个人或企业都难以承担起如此庞大的职责，最好的方式莫过于由政府主导来完成区块链平台的构筑。

结论

由于区块链技术具有的去中心化信用、不可篡改、可编程等特点，区块链技术逐渐成为学术界和产业界的热点研究课题。本文基于现有的区块链技术理论，提出了一种基于区块链技术的股权众筹项目架构。然而，现今的区块链技术研究仍存在着诸多不足，将该技术直接应用于社会服务仍有诸多问题需要去解决。本文构想了一种区块链技术的实际应用，以期为未来的发展提供有用的启发与借鉴。

参考文献：

1. 橘子打造创业团队强力后盾 推出募资平台“群募贝果”. 番薯藤，2014-09-30

2. 刘明 . 美国《众筹法案》中集资门户法律制度的构建及其启示 [J]. 现代法学，2015（1）

3. 李雪静 . 众筹融资模式的发展探析 [J]. 上海金融学院学报，2013（6）

4. 胡吉祥，吴颖萌 . 众筹融资的发展及监管 [J]. 证券市场导报，2013（12）

5. 杨东，苏伦嘎 . 股权众筹平台的运营模式及风险防范 [J]. 国家检察官学院学报，2014（4）

6. 范家琛 . 众筹商业模式研究 [J]. 企业经济，2013（8）