拉手互助

白皮书

版本：1.0

智能坊

2016.05

摘要

本文主要讲述了一种在互不信任的匿名网络中，如何利用区块链（Blockchain[1]）的不可篡改特性与智能合约[2]（Smart contract）的可自动执行特性来实现正和博弈[3]的必要条件（1.信息对称；2.规则全部强制执行；3. 收益合理分配），最终实现群体利益最大化。具体实施规则：通过将数字资产存放于区块链/消除不必要的中间环节/使非法挪用成为不可能/资金划拨将通过智能合约来实现/操作流程公开透明/无任何暗箱操作的机会/实现正和博弈的必要条件。通过不断优化规则实现帕累托最优[4]解。

前言

随着互联网+浪潮的强劲来袭，加之 P2P 分享经济[5]概念的悄然兴起，传统保险业的高成本弊端愈发显露无遗，而互助保险[6]这一新型互助模式的出现将从一定程度上有效降低保险行业的整体成本。

但这种基于中心化的互助保险模式仍旧存在一些通过传统方式无法逾越的难题：互助保险平台虽然在竭尽所能地公示着各种信息，但是这些“公开的”信息依然可以轻易地造假，也就是说，平台无法自证清白，加之近几年屡屡出现的捐款去向不明及 P2P 理财平台跑路等恶性社会事件，更是充分暴露了人们在当前社会信任感严重缺失的环境下的无力感。那么，是否有一个有效且可行的办法来帮助我们自证清白呢？ 如果有，那么其势必将为整个互助保险业带来更加富有颠覆性的变革浪潮。

在国际领域， 智能合约的概念正在如火如荼地席卷资本市场，智能合约项目“以太坊 DAO”的项目前期众筹甚至已超过一亿美金[7]，这无疑让众多业外人士感到瞠目结舌，资本市场的疯狂追逐，也似乎能说明智能合约确实是一项真正具备点福利的和潜在价值性的技术。 不过， 由于开发难度及其它相关配套条件无法及时跟进等因素的制约和束缚， 迄今为止的智能合约仍处于概念性阶段而

让人难以真切触碰，真正落地的实际型应用更是可望而不可及。

值得庆幸的是，国内顶级的智能合约应用开发者们已经在这一领域里走在了世界的前列，智能坊团队[8] 经过长期的潜心调研与实践，最终发现了智能合约与区块链技术在传统互助保险领域里蕴含的机会，并准备将这一崭新的技术——“区块链+智能合约”应用到互助保险这样一个新兴的领域，此举有望完美解决传统保险行业遗留下来的信任相关的难解问题且又能完整保留传统互助保险的优势。由此，“拉手互助”的基础设想和构架诞生了，它将是由智能坊所主导的第一款有望真正造福社会的、区块链相关的落地型智能合约应用。

一、简介

1、产品概述

拉手互助是基于区块链智能合约系统开发的一款针对重大疾病的非盈利型互助保障平台，利用区块链的不可篡改及去信任化的特性，把保障规则和赔付执行流程用智能合约的形式予以固定。拉手互助项目有望在很大程度上高效解决社会现存的信任危机，从而为广大民众提供更加低成本化的高额人身社会保障。

值得一提的是，由于智能合约系统与生俱来的去信任化特性，用户甚至可以通过加密技术来进行匿名投保，购买一定数量的数字资产（见章节八）即可正式成为拉手互助的会员。遵守会员规则，即可按照规则获得相应的平台互助资金（资金由拉手互助平台内所有注册会员进行分摊捐助）。

2、产品特性

传统互助也在试图实现正和博弈，但囿于其无法完整实现正和博弈的三个必要条件：信息对称、规则全部强制执行、收益合理分配，故很难实现其最终目的，更是无法达到帕累托最优；

而拉手互助通过区块链和智能合约技术的特性，基本实现了正和博弈的三个必要条件，从而可以实现正和博弈。

拉手互助特性如下：

1） 只需极低的成本即可获得高额的保障；

2） 资金流向公开、公正、透明，可以做到无需预存费用，即用即扣；

3） 维护运营成本较低；

4） 信息对称，且不可篡改，从而保证信息的可靠性（区块链提供的特性）；

5） 赔付审核的过程与结果透明可查。用户可以随时加入或者退出，方便快捷且无需负担其他额外的费用；

6） 合约代码强制执行并开源，合约的可靠性和有效验证。

二、流程架构

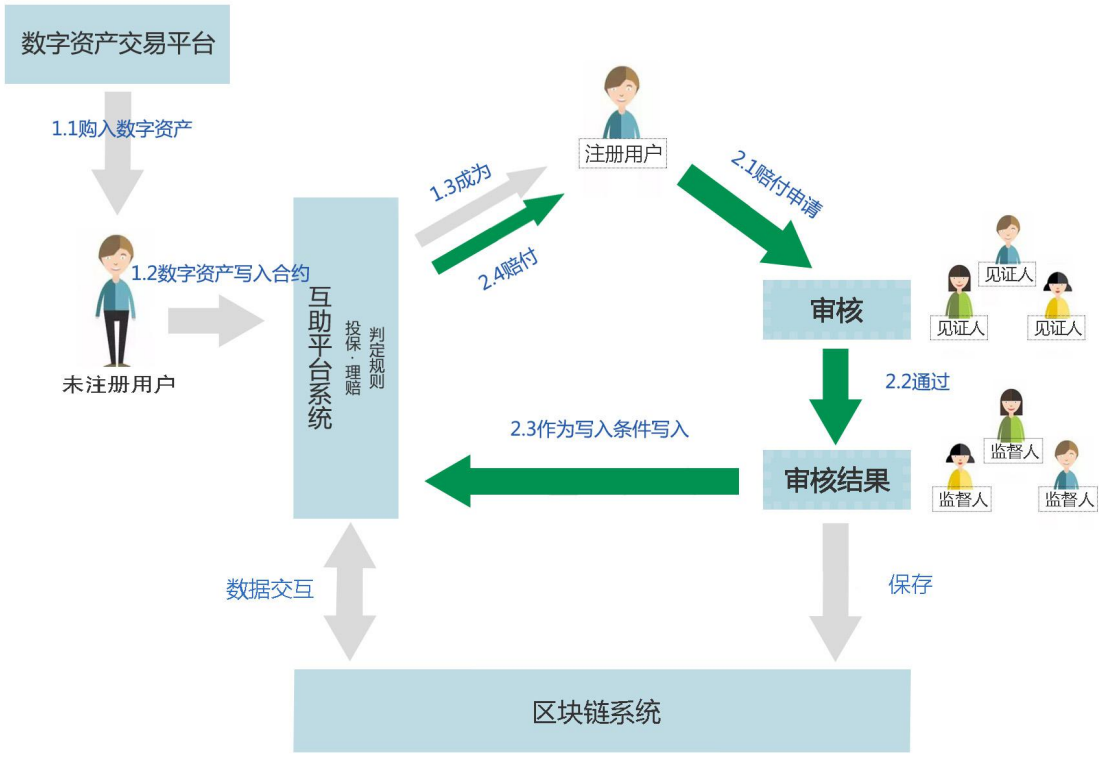

图 1

通过智能坊提供的“区块链+智能合约”平台，遵循一系列既定的智能合约规则就可以有效的运行拉手互助平台，具体流程见图 1。

流程详解：

流程 1. 成为注册用户：

（1.1）未注册的用户可通过购买相应数字资产；

（1.2）预存到智能合约系统中；

（1.3）成为正式注册用户。

根据预先设定的条件可进行相应的扣除操作，此举可免除人工操作的环节；

流程 2.赔付流程：

（2.1）如注册用户中有用户遭遇重大疾病的状况，则允许其提出赔付申请；

（2.2）在平台进行相关的审核后，再由多位见证人（详见章节五）进行共同审核，通过审核；

（2.3）后得出审核结果，并写入区块链数据库中，将结果在一定时间范围内公示；

（2.4）如果审核结果不存在异议，则将其相关信息写入智能合约，进行合约的判断，验证通过后，系统将对申请赔付用户进行付款操作。

结果公示过程中或者公示后，监督人（详见章节六）均可在系统界面提出异议，并由运营公司启动事后调查流程；

三、规则

1、互助重疾保障规则

——参加互助大病保障，须经过一段时间观察期[9]（观察期内无法获得帮助，但此期间一旦出现其它会员罹患重大疾病的情况，处于观察期的会员仍需分担费用）；

——有人求助而不助人，则视为自动退出互保公社；

——不设立基金，会员捐助是 p2p 的，通过支付工具从捐助人直接到受捐人，无需担心第三方从中截留；

——根据成员数量实现动态的捐助金额；

——成员患癌后的病情是需公示且经过公证的；

——成员随时可以选择退出，放弃捐助即可自动退出互保公社，权利与义务同时中止，跟道德及诚信无关。

2、 智能合约规则

——参与者把身份证号码和姓名（或者其他可以作为唯一标识身份的信息）加盐后 hash 存放于区块链里（保护隐私）。

——每个参与者购买一定数量的、价值稳定的数字资产写入智能合约里（任何人都无法挪用）。

——患病会员通过某些流程，可申请资助，进而激活合约运行条件，从每一个参与者的账户中自动扣取相应的费用（资金流向和过程在区块链上如实记录，有绝对的可靠度和不可篡改性）。

四、申请资助流程

提交相关诊断证明，经过公证人公证，并将证明文件 hash 存入区块链。

患者可以发布信息，请相应的见证人（共计 3 个），前往见证。

信息公示一定的期限后，如期间无人提出异议，则智能合约自动将相应数额的数字资产打入病患会员账户，见证人也将收到相应的佣金。

五、见证人

任何人在缴纳一定的数字资产押金后，都可以自动成为见证人，患者在提出救助申请后，智能合约会根据特定公开的随机算法（为防止见证人作弊）提供优选见证人，选择见证人后，见证人需与患者见面，并审查相关信息，如无问题则签名确认，并可以获得一定的费用奖励。

如果在后续流程中发现患者造假，而见证人未能及时觉察，见证人押金将被没收，并被分配给所有注册用户。

见证人在经济利益的驱动下将为合约各方提供准确可靠的信息输入，可极大地保证合约的公平且有效执行。

六、监督人

任何人一旦发现骗保情况，即可通过匿名的方式抵押一定的数字资产，举报骗保行为，运营公司将如实调查，一旦查实，则给予举报人丰厚的奖励，如果举报有误，则将举报者抵押的数字资产作为运营公司的调查费用予以没收，上述的每一个流程都将在区块链上留下相应的 hash 记录。

监督人在巨大利益的驱动下平衡了见证人的权力，可有效震慑见证人合伙骗保的行为，其作为合约的最后一道把关，可更加有效地保证合约的公平执行。

七、骗保处理

对于被举报并经运营公司查实的骗保案例，将按照赔偿金的一定比例额度奖励举报者。

对于被查实的骗保行为人，将通过法律手段向骗保人追讨赔偿金，同时扣除见证人的保证金，上述的每一步流程都会在区块链上留下不可篡改的记录。

八、数字资产

当前，市面上的普通数字资产往往价值波动幅度较大，将其作为保险支付手段，显然会存在非常大的不确定性，因此有必要使用某种价值稳定的支付介质。

可考虑根据二元期货的理论原理，在价值波动的虚拟货币系统里运行一种具备稳定价值的数字资产，这其中较为成功的案例有：比特股、太一元。

我们将在智能合约系统上开发一种价值稳定的数字资产，作为支付媒介。

九、智能合约运行平台

国内版本运行于智能坊平台，国外版本运行于以太坊平台。

十、用户体验

基于区块链的应用，由于其分布式存储数据的特性，将不可避免地遇到区块链同步迟缓的问题，后期加入的用户会明显感到数据同步的过程异常漫长难耐，从而导致用户体验不佳。因此，可设计一款融合了中心化服务的优势且又能保留区块链优势特征的产品，以提供可媲美中心化平台的用户体验。

十一、 结论

我们在此提出了一种可靠的系统，它借助于区块链技术的不可篡改性和智能合约的可自动执行的特性来系统地设计参保规则、赔付规则、见证人和监督人激励机制、事后追查机制，发行稳定价值的数字资产作为支付媒介，从而基本实现了正和博弈的 3 个必要条件（1. 信息对称；2. 规则全部强制执行；3. 收益合理分配），使团体利益值最大限度接近帕累托最优。

参考资料

[1]. Blockchains: The great chain of being sure about things". The Economist. 2015-10-31.

https://en.wikipedia.org/wiki/Block_chain_(database)#cite_ref-te20151031_2-2.

[2].https://en.wikipedia.org/wiki/Smart_contract.

[3].http://baike.baidu.com/link?url=UglhCZyu9-4Dk5y2qrsXVGxP7NGEoyQTakl9miAlTwRGlOrdzTweCBMNhEFFtkUg6UiRYXGlpWs_onDuV3JjKK.

https://en.wikipedia.org/wiki/Cooperative_game.

[4].https://en.wikipedia.org/wiki/Pareto_efficiency.

[5].http://theory.people.com.cn/n1/2016/0307/c49154-28177876.html.人民网.

[6].http://money.163.com/15/0916/11/B3KLT6I100253B0H.html.

[7].https://daohub.org/.

[8].http://www.dacrs.com/portal.php?mod=view&aid=4.智能坊.

[9].http://baoxian.pingan.com/tiaokuan/yinianqizhongjibaoxiantiaokuan.shtml#a.