唐盛链白皮书

中国第一个实现自主知识产权的区块链底层框架协议

与您共同打造数字金融新生态

（V1.0）

发布：唐盛（北京）物联技术有限公司

北京唐盛区块链技术研究院

编制：唐盛（北京）物联技术有限公司

2017 年 8 月

编委会成员

顾问：王连洲

审核：乔盖乔、王雅妮

撰写：孙文、解旻、乔盖乔、曲云潇

工程实现：解旻、王彦忠、肖尊平、李梦杰、李盈辉、陈洪智、尹伊波、秦川、谢军兴、朱帅、郑自胜、黄点点、崔延聪、谭银鹏

前　言

近两年，区块链技术已成为信息技术产业最炙手可热的概念之一。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式，被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新，很可能在全球范围引起一场新的技术革新和产业变革。

区块链技术具有去中心化、时序数据、集体维护、可编程和安全可信等特点，特别适合构建编程的货币系统、金融系统乃至宏观社会系统。这一随着比特币等数字货币的日益普及而逐渐兴起的全新去中心化基础架构与分布式计算范式，目前已经引起政府部门、金融机构、科技企业和资本市场的高度重视与广泛关注。

放眼全球，联合国、国际货币基金组织，以及美国、英国、日本等国家对区块链的发展给予了高度关注，积极探索推动区块链的应用。我国也非常重视对区块链及其应用的研发，积极展开布局。目前，随着国内外对区块链研发水平的不断提高，这一技术的应用范围已延伸到物联网、智能制造、供应链管理、数字资产交易等多个领域。

从应用市场的角度来看，数字金融市场正是区块链技术落地的最佳场景。2015 年，中国战略文化促进会与西南财经大学互联网研究中心在联合发布的《中国数字金融发展报告》（以下简称“报告”）中提出：数字金融的出现意味着极大的机遇和挑战，网络技术以及互联网精神的渗入，正在极大地改变金融领域。

报告描述，数字金融是网络技术与金融的深度渗入和融合。一是网络技术对金融的渗入：网络技术能降低金融交易成本和信息不对称，提高金融资源配置效

率，改变金融交易的组织形式和市场结构，拓展交易的可能性；二是互联网精神对金融的渗入：互联网精神的核心是开放、共享、平等、普惠，数字金融反映了社会组织和网络平台在金融业的兴起，金融分工和专业化将会被淡化，而金融的普惠性将增强。

因此，数字金融对当前大环境下各个领域的重要性是不言而喻的。推动数字金融不断完善的动力是使之与先进技术有效结合，并在各个行业中推广和实施战略。

区块链技术是互联网技术的升级版，从比特信息传输升级为价值传输，其对数字金融的意义非常重大，将成为下一代数字金融应用的基础设施。唐盛链正是在这样的大环境下孕育而生，抓住下一代金融基础设施建设的机遇，希望可以为数字金融的持续稳定发展奠定基础。

目录

一、 背景概述

1.1 公司简介

唐盛（北京）物联技术有限公司（简称“唐盛物联”）是一家从事区块链自主知识产权研究、专注于区块链技术应用开发及资产数字化的科技公司。公司自成立以来不断储备区块链专业技术人才，申请了多项专利，先后获得国家版权局颁发的多个软件著作权证书，并自主研发了基于区块链的资产数字化交易基础设施——唐盛链。

“唐盛链”是利用双核心币机制实现公私链融合并打通现实世界资产和数字资产的区块链底层框架，是公司投入大量研究经费，通过长期科技攻关收获的研发成果，具有自创共识机制（GEAR）、应用场景融合（公链、私链、联盟链应用融合）、智能合约法律效力化等独创特点，拥有现实世界资产数字化和价值流通的能力，是构建区块链落地应用的不二选择。该底层的问世，预示着我国拥有了自主知识产权的可实际落地的区块链底层，为区块链应用在我国快速落地打下了坚实基础。

公司发展至今，已在“唐盛链”的基础设施之上开发了“唐贝”、“DICO”等优质项目，并完成了 3000 万天使轮融资。未来，公司将专注于区块链在各应用领域的研发，让各行业机构通过“唐盛链”打通数字和现实世界，共同打造“唐盛链”数字金融新生态。

1.2 研发背景

1.2.1 数字金融市场前景

数字金融是网络技术与金融的渗入和融合。它并不是简单的“互联网+金融”，也不是复杂到与传统金融没有关联，更不是在现有金融体系之外的一个异生物或类生物。它是金融行业与互联网技术和精神相结合的新兴领域，是将互联网“开放、平等、协作、分享”的精神渗入传统的金融行业，在金融上所表现出的新特征、新技术、新平台、新模式和新形式。

可以说，目前互联网金融行业中活跃度较高的 P2P、第三方支付、网络银行、众筹等均属于数字金融的范畴。中国信息通信研究院研究发表的《2017 年中国数字经济发展白皮书》显示：2016 年我国数字经济规模达到 22.6 万亿，同比增长 18.9%，占 GDP 比重达到 30.3%，其中，互联网理财和信贷用户人数分别为 4.4 亿和 1.3 亿，平台数量达到 2448 家，网络资管资金规模约 2.8 万亿，网络信贷规模达到 1.2 万亿，网络众筹规模超过 200 亿，数字支付金额达到约 111.5 万亿。从数据可以看出，虽然 2016 年，国家出于金融安全的考虑，开始收紧数字金融行业，对 p2p、第三方支付、众筹等平台实行强力的监管措施，但是数字金融更加健康稳定的发展，促进了行业长久持续的增长。

从目前的情况看，全球数字金融市场仍在高速发展和持续孕育中，然而中心化的数字金融服务由于信息安全、资金安全、信用缺失等问题，已经到达一定的发展瓶颈，市场急需新的模式和生态以满足民众持续增长的金融生活需求。

1.2.2 现有区块链底层框架的问题

区块链技术的发展为数字金融的突破和创新提供了新的思路和模式，并终将引领新一轮的数字金融模式创新。

目前应用较为广泛的区块链底层技术主要有 Bitcoin，Ethereum，Graphene 和 Fabric，以他们为底层的应用虽然解决了很多问题，但是由于数字金融领域应用对安全、法律效力、兼容性等的要求相对较高，这些底层都存在一定的局限性。

a) Bitcoin

比特币是区块链技术最早也是目前最稳定的应用，该框架实现了基本的 UTXO 模型、区块链数据结构和 P2P 网络通信，并使用 POW 共识机制，共识节点通过计算一个特定格式的 hash 值来争夺记账权。该框架在控制代币发行量、交易透明等方面很有优势，也是目前使用最广泛的区块链底层框架。但目前来说，比特币底层由于确认效率慢、数据吞吐量低、能耗大等问题，并不适用于数字金融领域，仅能作为最基本的存证或货币交换平台，不能满足数字金融领域高复杂性、高实时性、高兼容性的需求。

b) Ethereum

以太坊作为智能合约在区块链上应用的先行者，为区块链技术提供了更多的发展方向和前景。其图灵完备的智能合约虚拟机，可以帮助应用开发者构建自己的区块链应用。但作为数字金融系统，图灵完备而没有任何形式化证明的智能合约，给应用带来了很多的安全隐患，the DAO 事件就是一个典型的例子。同时，由于其仅通过代币来控制智能合约的部署和调用，导致门槛过低，大量低质量的应用占用公链资源，无法形成数字金融生态。

c) Graphene

石墨烯底层框架开创性地使用 DPOS 作为共识协议，极大提高了系统吞吐量和交易确认速度，在此基础上开发的比特股、steemit 等应用，都能很好体现该框架的特点。但该框架本身并不支持智能合约，可定制化的程度较低；同时，由于其记账人数量的限制、投票意愿和代币集中的问题，导致了一定程度的中心化。

d) Fabric

Fabric 是目前联盟链使用最广泛的底层框架，实现了类似智能合约的 Chain Code，可以快速构建验证区块链应用。目前的问题是 1.0 版本之前无法支持动态添加删除节点，新发布的 1.0 版本没有采用任何拜占庭共识算法，其安全性和可扩展性的表现并不适合大型数字金融应用的构建。

1.3 唐盛链定位

基于现有区块链底层在数字金融领域可能存在的问题，唐盛物联于 2015 年开始研发适用于数字金融领域的新底层框架——唐盛链，希望首先构建数字金融行业的基础设施，并以

数字金融为切入点，进而满足其他领域的变革需求。

唐盛链的自创共识机制（GEAR）、应用场景融合（公链、私链、联盟链应用融合）、智能合约法律效力化等独创特点都是为了这一目标而设计的，所以唐盛链对于构建数字金融新生态有其独特的优势。

二、 唐盛链架构设计

2.1 设计理念

“安全、融合、可信”是唐盛链架构设计的原则。唐盛物联充分利用区块链技术“去中心化、信任强化、分布式共识、不可篡改”的特点，深挖数字金融应用场景，独创多项专利技术，并着力于实现普惠可用的落地应用。

为了全方位解决中心化数字金融中的一系列问题，唐盛物联提出了以融合区块链技术和可验证、可法律效力化的智能合约为基础的解决方案，并使用双核心币机制，满足数字金融市场不同的记账需求。同时，还希望通过盲签名方法帮助用户实现加强的隐私保护。

2.2 名词解释

2.2.1 系统名词

区块链：就技术而言，区块链是指用散列算法链式关联数据块，多节点验证存储从而使数据无法被篡改的分布式数据存储技术；**从应用系统角度来看**，一个区块链系统是指利用区块链数据存储技术和博弈论建立强化信任机制，在所有节点均不可信的网络中实现数据一致性的通信系统。

数字资产：以数字化的形式登记注册在区块链网络中的可流通有价物。

资产数字化：将拥有的有价物通过价值转换和评估服务转化为数字资产。

可赎回资产：资产数字化并在区块链网络中流通后，可通过出售时的智能合约在特定条件下赎回的有价物。

共识节点：区块链网络中通过共识机制产生并同步数据区块的程序及其运行环境。

轮转记账：唐盛链共识中，常规时间内，区块产生的方式。由票选胜出的共识节点在共识时间内等概率获得记账权。

价值评估：唐盛链中通过集体决策方式确定资产价值并数字化的共识模型。

唐贝（TangCowry）【简写 TCY】：唐盛链双核心代币之一，可赎回资产数字化后的数字资产。

唐宝（TangShell）【简写 TSL】：唐盛链双核心代币之一，锚定接入唐盛链应用项目和中小企业股权的集合价值。

唐币（TangCoin）【简写 TCN】：法币资产通过透明网关数字化后的数字资产。

2.2.2 系统参与者

治理委员会：由持有核心代币的投资用户、唐盛物联官方、国家监管机构组成，主要负责费用参数调整、唐盛链重大变更决策，以及对金融服务商、透明网关、水龙头服务的认证和监督，具体治理架构见 5.2 小节。

透明网关：法币资产和数字资产交换机构，法币资产可以通过透明网关兑换数字资产（唐币）；反之，数字资产也可以通过透明网关兑换成法币。每笔兑换成功后，该服务收取固定的服务费。该服务采用透明机制公示每一笔兑换交易，并使用银行或第三方支付作为资金冻结通道，以保证承兑。

水龙头：提供推荐注册和 KYC（Know Your Customer）服务。普通用户在钱包中生成公私钥后，只能通过水龙头上传公钥并注册到区块链中。在以后的用户交易中，水龙头收取一定的交易费，并对治理委员会的风控和监管提供 KYC 服务。

金融服务商：运行共识节点的可赎回资产数字化服务机构，可根据自身业务范围认证和托管抵押资产，收取认证托管服务费，将抵押资产数字化为唐贝，并生成可赎回智能合约。其签发的唐贝在区块链中发生交易，该机构可以收取一定比例的交易佣金。

普通用户：使用钱包客户端提供的功能，通过唐盛链中的资产数字化服务生态，将个人持有的有价资产数字化并利用唐盛链的分布式撮合交易能力和可验证的安全智能合约实现数字资产的登记与流通。

轮转记账人（ROTATE WITNESS）：唐盛链底层网络的核心维护者。首先在共识网络中拥有账户体系（公私钥对）以及稳定运行一个绑定了账户体系的共识节点；然后接受普通用户使用代币投票选择，票选数的前 3/4 可以成为轮转记账人，参与 GEAR 共识中的等概率轮转记账。

价值评估人（VALUER）：在价值评估事件发生时由轮转记账人转化而来，通过对某项数字资产估值的加权平均的接近率抢夺一次额外记账机会。

2.3 系统架构描述

2.3.1 总体生态网络拓扑

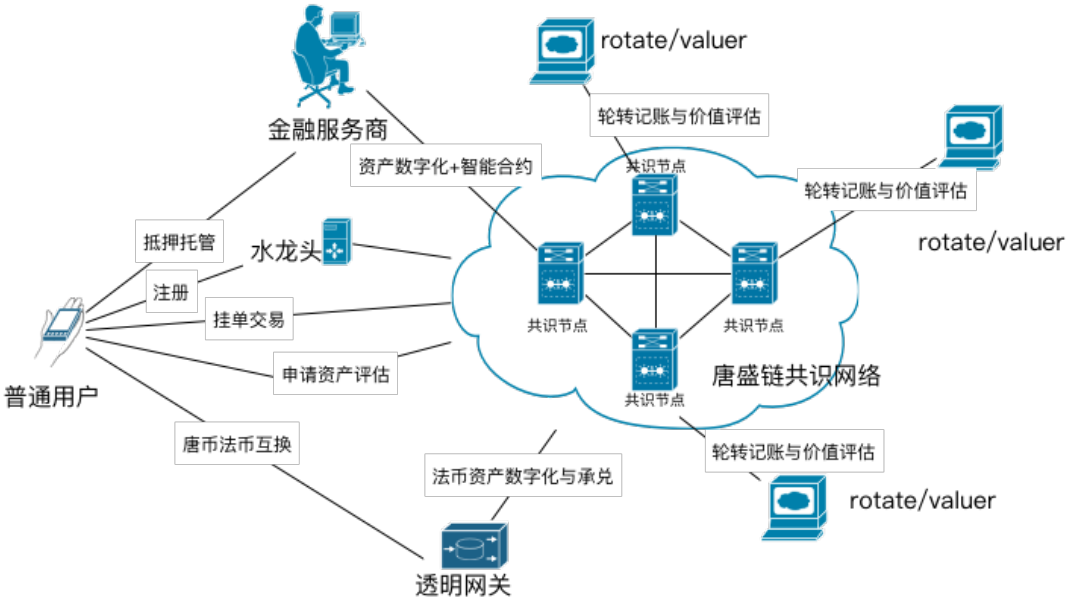

图 1 唐盛链总体生态网络拓扑图

如图 1 所示，唐盛链总体架构，包括唐盛链共识网络、服务生态、移动客户端三部分。

唐盛链底层共识网络提供基本的区块链网络系统，并提供撮合交易、智能合约执行等基础服务。控制共识节点的账户可以通过客户端实现价值评估等共识操作。

唐盛链的服务生态包括金融服务商、水龙头服务商和透明网关。其中金融服务商作为共识节点加入到唐盛链共识网络中，为用户提供可赎回类资产数字化服务，并发起服务相应的智能合约；水龙头服务商作为用户身份认证服务，为用户提供“一次一密”、盲签名等隐私保护服务，为相关部门提供监管服务；透明网关作为法币资产数字化服务，为用户提供资金的存管和兑换服务，保证用户资金与业务分离，并为监管部门提供资金端监管服务。

移动客户端钱包通过简单操作，实现数字资产登记、认证、兑换和流转。

2.3.2 逻辑架构

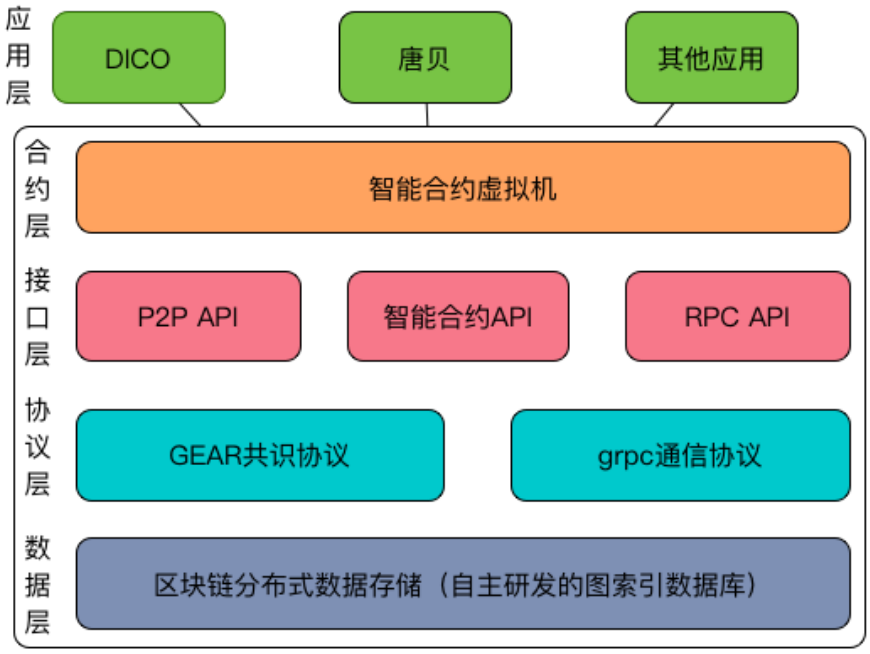

图 2 唐盛链逻辑架构图

如图 2 所示，唐盛链及其应用采用五层逻辑架构设计：数据层、协议层、接口层、合约层和应用层。

数据层：唐盛链数据层实现了基本的区块链数据结构存储，并自主研发了图索引数据库实现对区块数据的快速检索和查询。

协议层：在共识协议方面，唐盛链采用自主研发并拥有自主知识产权的 GEAR 共识协议；在数据通信方面，唐盛链采用 grpc 框架，grpc 是 google 开发的一个高性能、通用的开源 RPC 框架，基于 HTTP/2 协议标准而设计，基于 Protocol Buffers 序列化协议开发。

接口层：基于 grpc 框架，接口层对外提供节点间通信的 P2P API、节点与钱包客户端通信的 RPC API，以及智能合约虚拟机可调用的智能合约 API。

合约层：合约层为智能合约执行提供运行编译和运行环境。

应用层：通过调用接口层和合约层，可以实现各类应用模式。

2.3.3 金融服务商架构

金融服务商由共识节点、钱包程序、服务商后台组成，通过共识节点参与网络的数据维护，并通过钱包和服务商后台完成认证资产、抵押托管、签发数字资产等业务。金融服务商架构如图 3 所示。

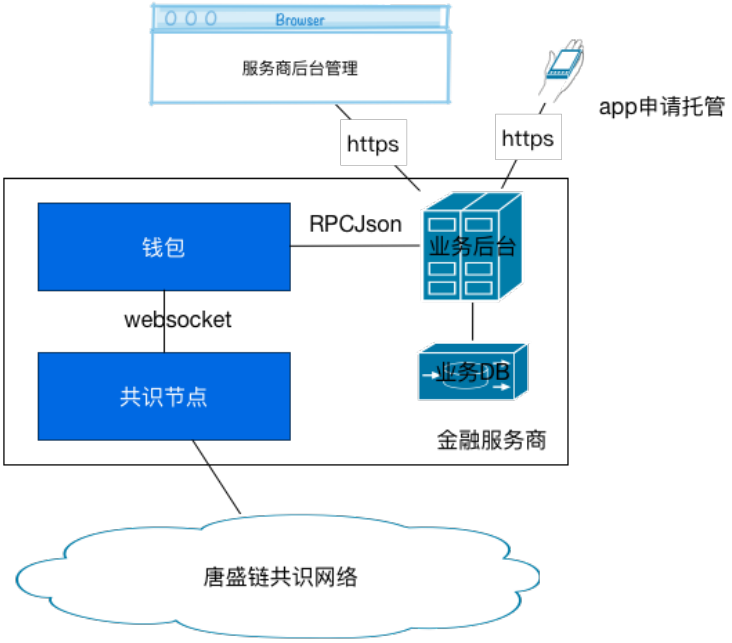

图 3 金融服务商架构图

2.3.4 透明网关架构

透明网关服务由钱包程序、转账程序和托管程序组成，唐币与法币资产相互兑换通过透明网关实现，资金托管由第三方支付或银行提供，实现资金与业务分离以及资金流向监管。透明网关架构如图 4 所示。

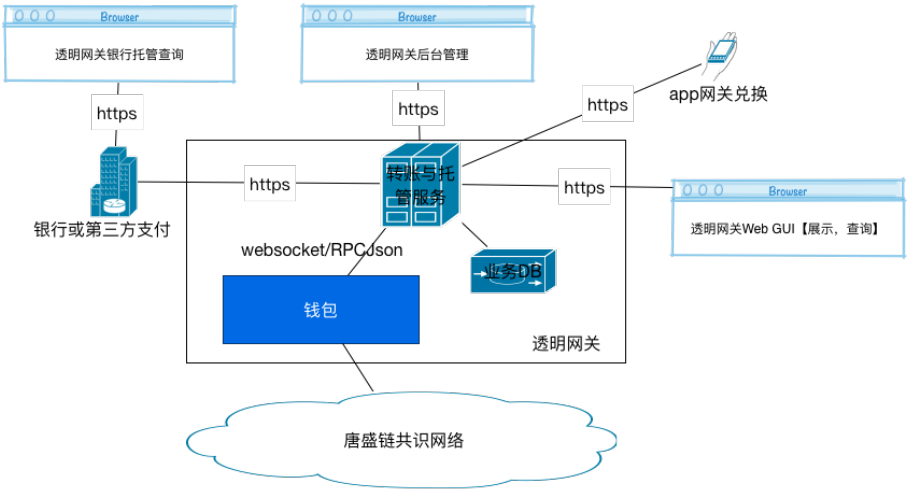

图 4 透明网关架构图

2.3.5 水龙头服务架构

水龙头服务由钱包程序和 adapter 服务组成，向所有其他系统参与者提供注册服务。钱

包程序用于水龙头账户和区块链底层交互，adapter 服务用于转发接口、实名认证、KYC 等。用户通过向水龙头服务上传用户名和公钥地址完成注册。水龙头服务提供实名认证和用户监管服务，是控制用户质量和 KYC 的关键服务模块。用户的账户体系由通过 secp256k1 算法生成的公钥和私钥组成，用户自己保留私钥用于电子签名，公钥作为验证和交易地址，通过水龙头服务注册到唐盛链中，在保证用户账户安全和链中交易隐私的同时实现认证监管。水龙头服务架构如图 5 所示。

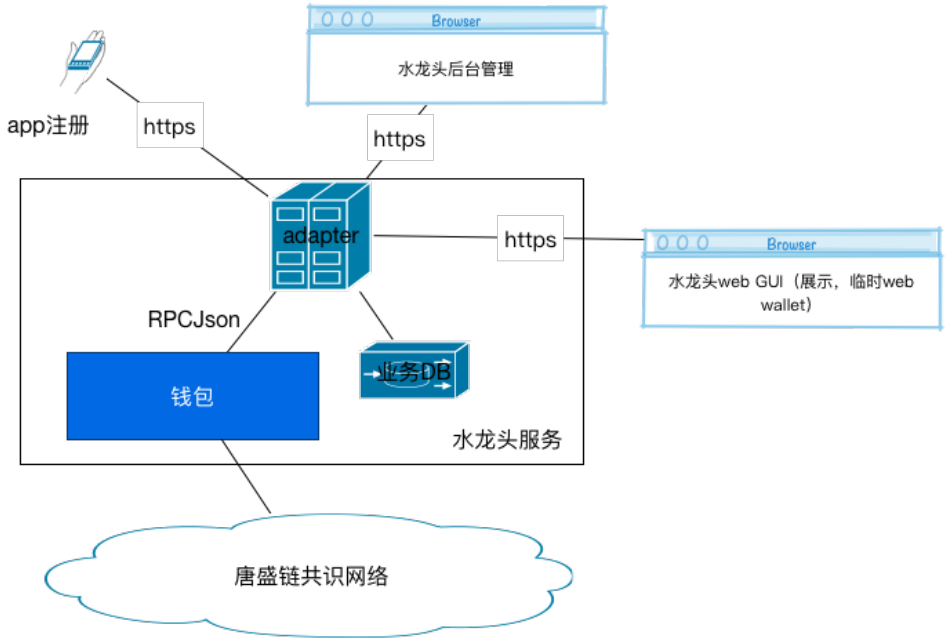

图 5 水龙头服务架构图

三、 唐盛链技术特点

3.1 自主研发共识机制——GEAR

GEAR 共识协议，全称是集体评估和轮转记账（Group Estimate and Rotate）共识协议，是适用于区块链结构数据的点对点传输和同步协议。该协议由轮转记账（rotate），集体评估（group estimate）和齿轮共识路由（gear）三个子协议组成，结合区块链数据结构和点对点网络通信的特点，实现安全、高效、去中心化、应用场景灵活的数据同步共识。

3.1.1 共识网络结构

共识网络由若干可动态加入和删除的共识节点组成，节点之间具备两两互联的能力，但不必完全两两相联。

基于 grpc 的数据通信模块保证数据同步的广播能够被足够多的节点接收；底层数据存储模块保证区块链数据结构的完整性和可验证性；共识协议模块实现了 GEAR 共识的数据处理程序，能够按照 GEAR 共识协议校验和同步数据。

3.1.2 轮转记账

轮转记账子协议主要包含两个部分，成为轮转记账人和等概率记账。

1）成为轮转记账人

成为轮转记账人首先要成为轮转记账候选人，成为轮转记账候选人的基本要求是在共识网络中拥有账户体系（公私钥对）以及稳定运行一个绑定了账户体系的共识节点。

成为候选人后，可以通过网络推送、社区宣传等方式为自己拉票，一级集体评估人（普通用户）通过手中所持选票（代币或数字股权）选举轮转记账人。得票数排在全网候选人前3/4 的候选人，可以成为当前记账轮次的轮转记账人。

2）等概率记账

候选人被集体评估机制评选为轮转记账人后，这些轮转记账人所运行的共识节点可以每隔 5 秒以等概率签名产生新区块，并广播到网络中的其他共识节点中，其他共识节点验证区块数据并存储新区块。超过 50%以上的共识节点确认新区块后，区块中数据被确认。

当一个等概率记账的新区块被网络确认后，产生该区块的轮转记账人可以获得一次 5 个唐宝代币的奖励。

3.1.3 集体评估

集体评估是 GEAR 共识协议中非常重要的子协议模块，也是通过集体决策机制实现资产数字化的主要手段，对数字金融领域的应用有基础性的支撑作用。集体评估子协议包含两个独立的过程，分别是：

一级集体评估

一级集体评估人由所有持有代币或数字股权的账户组成，负责以所持代币或数字股权数量为权重投票选择轮转记账人。一个评估人只允许投一次票，选择轮转记账人完毕即代表自己所有权重票投予该轮转记账人。

评估共识

价值评估人是评估共识的参与者，在成为价值评估人之前，首先要成为轮转记账人。

评估共识的流程如下：

1） 共识网络通过预置或智能合约定义一系列评估事件（如外包工作酬劳、公司股权估值、抵押物价值评估等），这些事件通过提案的方式广播到共识节点中；

2） 期望参与估值的轮转记账人在规定时间内对事件进行评估，按照所持选票（一级集体评估人所投）的权重，给出评估数值；

3） 该轮转记账人通过 RSA 加密算法，生成一对临时公私钥对，使用公钥加密后，广播到网络中；

4） 网络在评估事件到期前，估值对所有人不可见；

5） 在评估事件到期后，估值参与人将估值对应的临时私钥广播到网络中；

6） 当所有估值得到解密后，按照加权平均的原则去掉最高最低两个估值，得到一个最终的评估数值，该估值确定成为该轮评估事件的最终估值；

7） 参与该轮评估共识的轮转记账人中估值最接近最终估值的，可以在下一次轮转记账共识直接获得 100%概率的产生新区块机会；

8） 由评估共识产生的新区块被确认后，区块奖励为估值的一定比例数量的代币或数字股权。

3.1.4 共识路由

以 GEAR 共识网络作为主干网，其他共识机制网络可以通过 GEAR 共识节点中的齿轮共识路由模块，实现与 GEAR 共识网络的互联互通。

1）POW/POS 与 GEAR 互通

由于 POW 与 POS 协议是依赖于代币激励机制的共识机制，所以齿轮共识路由提供代币估值与转换接口，并对接各大交易所的实时数据，自动完成代币价值的转换。

2）类 PBFT 与 GEAR 互通

类 PBFT 的共识机制不依赖代币，主要是数据的交换和存储，齿轮共识路由通过智能合约的方式实现主干网与类 PBFT 共识网络的数据互通以及主干网数据的分片存储。

3.2 更安全的智能合约

为了保证唐盛链上应用的安全和高效，唐盛链中并不实现图灵完备的智能合约虚拟机，也并不实现可以自由部署的智能合约。

智能合约对区块链来说是把双刃剑，它扩展了区块链的功能、充分发挥了区块链可信数据的特性，但同时，未经过形式化验证和安全验证的智能合约，也为区块链系统带来了安全隐患，一些不规范的合约代码也会给区块链的存储和记账效率带来不良的影响。

因此，对于一个着力于打造数字金融新生态的区块链系统来说，需要一种智能合约部署和执行的新方式，能够在满足数字金融高扩展性需求的同时，不影响安全性和效率。

唐盛链中的智能合约使用以下四个方式满足以上要求：

1） 合约模板

合约模板是唐盛链中对智能合约的约束。一个有智能合约需求的应用，首先需要编写合约模板，合约模板由一段 golang 脚本组成，暴露一个不重名的调用方法，参数包含合约执行方和数量参数。

2） 智能合约治理委员会

智能合约治理委员会是唐盛链合约模板的管理机构，负责对用户提交的合约模板进行形式化验证和安全验证。有智能合约需求的应用首先需要编写“合约模板”，编写完成后，向智能合约治理委员会提交合约模板并一次性缴纳 99 个唐宝作为管理费，由治理委员组织进行形式化验证和安全验证，确认通过验证后，部署到区块链网络中，并分配智能合约调用地址。

3） 智能合约+NLG 电子协议

应用得到智能合约调用地址后，可以在程序中以 API 接口的方式调用合约模板，

传入参数后，生成一份智能合约，并通过 NLG（自然语言生成）算法，生成内容对应的合约参与方电子签名的电子协议，在区块链网络中存证。

4） 节点自动执行机制

与以太坊等智能合约不同，唐盛链智能合约都存储于区块数据中，每轮共识发生时，获取记账权的节点通过图索引查找到符合执行条件的智能合约（时间、价格等），自动执行该合约中约定动作。

3.3 分布式撮合系统

使用分布式交易所的方式进行撮合交易，卖方挂单和买方挂单缓存在网络中。当共识节点记账时，自动匹配撮合买卖挂单，将账单广播到网络中，在 51%以上的节点验证通过后，完成交易。

分布式撮合交易的好处是每一笔交易都有据可查，每一笔交易都得到了最广泛节点的确认，在提高交易记录安全性的同时增加了庄家操纵交易盘的难度。

3.4 基于盲签名的隐私保护

对于现金交易来说，最重要的性质是匿名性——当你从银行取出现金时，银行是不知道你要买什么的；而当你消费时，商家也不知道你是谁。相比之下，当你用信用卡在线购物时，必须告诉信用卡公司你是谁、在哪里消费——正因为如此，隐私的入侵是随时随地的。唐盛链为了更好地保护用户隐私，在转账功能中加入了盲签名协议，用户在进行转账操作时，可以选择使用盲签名转账协议。

唐盛链中的盲签名方案主要使用事前限制性盲签名算法，在保护隐私的同时最大程度地防止双花。

基本现金系统包括了三个参与实体，它们是银行 B(唐盛链共识数据)，用户 U，以及商店 S。盲签名过程主要包括五大步骤——系统建立、开户、取款协议、付款协议、存款协议，具体描述如下：

3.4.1 系统建立

1） 银行 B 随机产生一组生成元 (g,g_1,g_2)，和一个数 $x \in_R Z_q^*$；

2） B 选择两个合适的单向 H 函数 H,H_0，满足：

H： $G_q \times G \times_q G_q \times G_q \times G_q \to Z_q^*$

以及，满足：

H_0：$G_q \times G_q \times SHOP-ID \times DATE/TIME \to Z_q$

3） B 公开对 G_q 的描述，(g, g_1, g_2)，H, H_0，$h = g^x$，$h_1 = g_1^x$，$h_2 = g_2^x$ 对密钥 x 保密。

4） 每个商店 S 都有一个独一无二的账号，它至少被 B 和 S 所知。$DATE/TIME$ 是一个代表交易时间和日期的数值，这个数值保证了同一个 S 对于不同的交易生成的相应数据也是不同的。

5） 签名 $Sign(A,B)$ 包含了一组参数 $(z,a,b,r) \in G_q \times G_q \times G_q \times Z_q$，满足：

$g^r = h^{H(A,B,z,a,b)} a$ 和 $A^r = z^{H(A,B,z,a,b)} b$

一项电子现金是由 A，B 和 $Sign(A,B)$ 构成的，如果一个账户持有者知道对应于 (g_1, g_2) 的 A 和 B 的表达形式，那么可以说他知道了电子现金的表达形式。

3.4.2 开户

当用户 U 在 B 处开一个账户时，B 需要 U 通过一定的方式证明自己的身份（如通过身份证或护照等证明身份）。然后 U 产生一个随机数 $u_1 \in_R Z_q$，计算 $I = g_1^{u_1}$。如果 $g_1^{u_1} g_2 \neq 1$，那么 U 将传递给 B，保密 u_1，B 把 U 的识别信息和账号 I 保存到账户数据库中。账号 I 必须是独一无二的，因为这样可以使得银行在发现重复花费后唯一地识别出用户来。

B 计算得到 $z = (Ig_2)^x$ 并把它发送给 U，因为 B 公开了 $h_1 = g_1^x$，$h_2 = g_2^x$，所以 U 可以自己计算得到 z 的值。

系统参数：g，g_1，g_2；

用户参数：私钥 u_1，公钥/账号 $I = A_O g_1^{u_1} = g_1^{u_1+O_1}$，$Ig_2$，$z = (Ig_2)^x$ $= g_1^{x(u_1+O_1)} g_2^x$；

银行参数：私钥 x，公钥 $h = g^x$，$h_1 = g_1^x$，$h_2 = g_2^x$；

监察器参数：私钥 O_1，公钥 $A_O = g_1^{O_1}$。

3.4.3 取款协议

Step1：首先 O 随机生成 $O_2 \in Z_q$，发送 $B_O = g_1^{o_2}$ 给 U，虽然这个步骤包含在协议中，但是 O 可以在 Step3 之前的任何时间发送 B_O 给 U；

Step2：B 随机生成 $w \in_R Z_q$，传递 $a = g^w$ 和 $b = (Ig_2)^w$ 给 U；

Step3：U 选取随机数 $s \in_R Z_q^*$，$x_1, x_2, e \in_R Z_q$，计算 $A = (Ig_2)^s = g_1^{s(O_1+u_1)} g_2^s$ 和 $B = g_1^{x_1} g_2^{x_2} A_O^{se} B_O = g_1^{x_1+seO_1+O_2} g_2^{x_2}$，$z' = A^x = z^s$。U 再次生成两个随机数 $u, v \in_R Z_q$，得到 $a' = g^{wu+v} = a^u g^v$ 和 $b' = A^{wu+v} = b^{su} A^v$，同时计算 $c' = H(A, B, z', a', b')$，将 $c = c'/u$ 发送给 B；

Step4：B 返还 $r = cx + w(\mathrm{mod}\, q)$ 给 U。

U 接收 r，当且仅当满足 $g^r = h^c a$ 和 $(Ig_2)^r = h^c$，计算得到 $r' = xH(A, B, z'.a', b')$

$+(wu+v) = ru + v \bmod q$

最后用户得到的电子现金为：

$(A, B, Sign(A, B))\ Sign(A, B) = (z', a', b', r')$；$g^{r'} = a' h^{H(A,B,a',b')}$，$A^{r'} = b' z'^{H(A,B,a',b')}$

3.4.4 付款协议

当 U 需要使用电子现金在商店 S 进行付款时，就会执行下列付款协议：

Step1：U 发送 $(A, B, Sign(A, B))$ 给 S；

Step2：如果 $A \neq 1$，S 计算 $d = H_0(A, B, I_S, date/time)$，并将其发送给 U；

Step3：U 发送 $d' = s(d + e)$ 给 O；

Step4：如果内存中还保留着 O_2，则 O 计算 $r_1' = d' O_1 + O_2$ 并把它发送给 U(如果 O_2 已被删除，O 自动停止运行)，然后把 O_2 从内存中删除；

Step5：U 验证 $g_1^{r_1'} = A_O^{d'} B_O$，如果满足，则计算 $r_1 = r_1' + d(u_1 s) + x_1$ 和 $r_2 = ds + x_2$，

并传递(r_1,r_2)给 S。

S 接收(r_1,r_2)，当且仅当$Sign(A,B)$是(A,B)的合法签名，以及满足$g_1^{r_1}g_2^{r_2}=A^dB$。

3.4.5 存款协议与双花追踪

存款协议和基本现金系统的相关内容是一样的，在此不再累赘叙述。这里使用了存款协议：$(A,B,Sign(A,B),(r_1,r_2),date/time)$。

由于在此方案中引入了监察器，于是追踪协议为：

$(A,B,Sign(A,B),(r_1,r_2),date/time)$和$(A,B,Sign(A,B),(r_1',r_2'),date'/time')$

$$u_1=\frac{r_1-r_1'}{r_2-r_2'}-O_1=\frac{(d-d')(u_1s)}{(d-d')s}-O_1\Rightarrow I=g_1^{u_1}$$

3.4.6 协议分析

事前防止重复花费的体现：在付款协议中监察器在计算出r_1'之后删除了O_2，若出现重复花费，则在第二次的付款中，由于没有了与对应现金的O_2，为了进一步执行付款协议，监察器产生了一个O_2'，而这个O_2'与$B=g_1^{x_1}g_2^{x_2}A_O^{se}B_O=g_1^{x_1+seO_1+O_2}g_2^{x_2}$中的$O_2$是不同的，因此，它不能通过在 S 处的检验$g_1^{r_1}g_2^{r_2}=A^dB$，也就无法和商店 S 之间实现交易。

由此可见，监察器通过删除O_2，在用户企图重复花费之前，阻止了他的行为，实现了事前防止重复花费。

3.5 基于一次一密的钱包备份

在传统中心化系统中，用户的安全信息都存储在服务器上，信任成本过高。在而后出现的区块链钱包技术里，将用户钱包保存在用户本地，服务器只保存能验证用户身份的用户公钥，虽然解决了信任危机以及数据不透明问题，但是仍然具有以下缺点：

1）用户需要承担备份钱包任务

用户钱包文件需要用户自己保存，一旦钱包文件丢失，用户就无法使用账户，更别提拿回账户里的钱了。

2）用户需要承担忘记口令风险

用户需要记住钱包口令,一旦用户忘记口令，用户就取不到证明其身份的密钥，用户账户的钱就只能看着取不出来。

3）用户口令存在暴力破解危险

用户口令校验为本地校验,且无次数限制,黑客可以通过暴力破解的方式强行试出口令,用户的数字资产就可能遭受损失。

本方案解决了上述问题，用户不用担心钱包备份和信息安全问题，一次一密的用户密码在首次注册时由水龙头发送短信得到。每次注销时生成新的密码（由两串随机字符串组成）和 rsa 公私钥对，将私钥裂变为两个私钥组合，将其中一串随机字符串通过 rsa 公钥加密，连同一半裂变私钥发给水龙头；登录/交易时，发送手机号和另一半裂变私钥给水龙头，水龙头解密后，取出随机字符串短信验证码方式发送给用户，用户输入短信验证码，和本地存储的另一个随机字符串一起组成解密密码，取出私钥。

用户在操作链上数据的情况下，app 钱包需要输入密码，在接收到验证码并输入验证之后，需更换钱包密码，并向水龙头调用钱包备份和更换密码接口，传递下次登录短信验证码的线索，用于下次操作链上数据时短信验证码的获取。

使用类似于 IPFS 分布式云存储服务用于钱包文件备份，备份的钱包文件是加密的。备份的钱包文件恢复时，服务器会发送备份的钱包文件给用户设置好的救援邮箱中。

四、 唐盛链应用简介

作为区块链技术在数字金融领域的先行者，唐盛物联在专注于底层技术的基础上，非常重视落地应用。唐贝钱包是唐盛链上的第一个官方落地应用，解决了普惠金融领域目前存在的一系列问题，现在已经可以下载使用；DICO 将作为唐盛链上的第二个官方落地应用，为数字资产、股权等的众筹提供一个可评估、可交易的平台。

4.1 唐贝钱包——全球首个普惠金融领域区块链落地应用

4.1.1 应用背景

普惠金融（Financial Inclusion），也称作“金融包容”或“包容性金融”，最早由联合国在 2005 年提出。上世纪 90 年代以来，普惠金融问题逐渐受到国际普遍关注。国际上先后成立了普惠金融联盟（AFI）、二十国集团普惠金融专家组（FIEG）、全球普惠金融合作伙伴组织（GPFI）等机构，着力于推动普惠金融发展。

2013 年 11 月，党的十八届三中全会在《关于全面深化改革若干重大问题的决议》中，就明确提出了“发展普惠金融”。时至今日，在我国普惠金融发展取得阶段性成效的同时，我们也要清醒地认识到,我国金融业在服务覆盖率和渗透率方面仍然存在一些薄弱环节和制约因素。

数字金融的发展，尤其是 P2P 网贷、小微金融等传统中心化数字金融服务的兴起大大提升了普惠金融服务的覆盖率和渗透率，但同时，受限于中心化服务存在的问题，滥用信用、跑路、资金流向不透明等情况严重打击了投资人的信心，也阻碍了普惠金融的进一步发展。

在传统的业务模式中，普惠金融平台开展业务面临很多困难，资产是否优质、资金是否充足、获客成本是否可控、技术是否持续可维护都是平台是否能稳定运行的关键。同时，由于监管的诸多限制，多数平台已无法满足一些中小企业的融资需求，“钱、人、信”三大难题仍是中小企业在融资过程中面临的关键问题。唐贝的出现，能帮助网贷平台更好地拥抱监管、践行合规，帮助网贷机构健康发展。

4.1.2 应用说明

唐贝钱包是一款基于区块链技术开发的普惠金融领域的落地应用，旨在将传统网贷平台的角色从“信息中介”转换为“资产数字化”金融服务商。唐贝可以通过价值锚定、评估托管等方式，帮助平台将借款用户所持有的真实资产转化为区块链网络中的数字资产唐贝，从而让平台在唐贝自由流通的过程中获得交易手续费。

在唐贝钱包应用中，所有的交易都在由区块链技术搭建的分布式交易所中完成，金融服务商无需再承担中介撮合的成本、技术维护的成本和其他隐性成本。通过区块链，接入的金融服务商客户资源、风控数据实时共享，一定程度上解决了获客和风控的难题。此外，借款用户和投资用户利用唐贝代表资产在区块链中进行交换、流通，也能够体验到更加便捷、丰富、安全的金融生活。

通过唐贝钱包，**一个完整的可赎回资产数字化流通过程可分为以下四步：**

金融服务商认证：通过委员会认证后，金融服务商可以作为共识节点加入到记账网络中，并生成金融服务商公私钥和账号。

可赎回资产数字化：借款人通过 app 向某一个金融服务商登记资产申请融资，金融服务商验证并托管资产后，向借款人签发唐贝及赎回智能合约。

唐贝流通：借款人向区块链网络发布唐贝售卖并签署智能合约，投资人通过透明网关将法币资产兑换为唐币，向区块链网络中发布唐贝购买并签署智能合约，由共识节点记账时产生撮合交易。投资人获得唐贝后也可向区块链网络发布二次售卖。

智能赎回合约执行：智能合约到期，由共识节点自动执行，以约定回购价格转移借款人提前兑换的唐币给持有该抵押资产唐贝的投资人，投资人账户中唐贝转移给借款人，借款人凭全部唐贝向金融服务商申请资产解押并燃烧唐贝。如果借款人账户没有足够的唐币，则由金融服务商账户唐币补全，抵押物资产自动转移到金融服务商名下。如果金融服务商没有补全唐币，则在区块链网络中留下不可篡改的不良记录。

以上过程如图 6 所示：

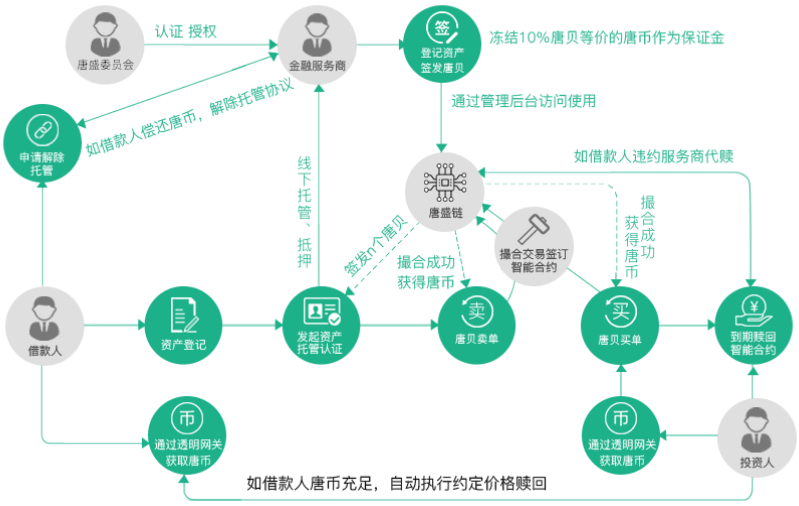

图 6 唐贝总体流程图

综上，唐贝给受益者提供的服务有：

1）为金融服务商提供认证、接入、智能合约定制、大数据等服务，接入唐贝的各类金融服务商可享受大数据资源；

2）为资产抵押/出售方提供注册、推荐、资产数字化、信息咨询等服务，接入唐贝的资产抵押/出售方可安全、透明地进行交易；

3）为投资用户提供注册、推荐、信息咨询等服务，接入唐贝的投资用户可以放心地选择任意一家接入的认证金融服务商进行投资，无需担忧财产安全

唐贝已于 5 月 26 日正式上线公测运营，现招募广大金融服务商加入公测，如有意向请致电 400-001-9593。唐贝 APP 可通过唐盛云官网 www.tangshengyun.com 直接扫描二维码下载，或在 360 手机助手、App Store 搜索关键词“唐贝”下载。

4.1.3 应用特性

具体来说，唐贝的开发解决了以下问题：

1）解决传统技术手段效率低下、安全性缺陷等问题；

2）基于委员会尽调、押金冻结、风险维权基金等多层次智能化风险控制措施，结合区块链固有的不可篡改、可追溯、交易签名等特点，解决可赎回资产流通中的信任问题；

3）解决传统业务模式中资产流通范围局限、流通成本高昂的问题；

4）解决现实世界资产变现难的问题；

5）解决传统模式中交易不透明、资金缺少保障的问题。

相对于传统普惠金融服务，基于唐盛链底层开发的唐贝系统，拥有以下特性：

1）基于智能合约的金融服务商垫资机制——无赎回风险

2）通过透明网关服务锚定法币——稳定

3）基于区块链的数据记录——防篡改、透明

4）到期约定价格赎回的法律化智能合约——便捷可信

5）网络直接撮合交易，没有信息或信用中介——效率高、没有中介成本

6）透明网关法币兑换透明化、资金与业务分离——资金安全

7）金融服务商业务标准化，只需关心资产和风控——降低技术和运营维护成本

8）所有接入服务商贡献并共享区块链中的可信数据和用户——消除信息孤岛、风控透明、无地域限制

9）提供水龙头和透明网关的监管服务——无需合规成本

4.2 DICO——公开透明的分布式 ICO 平台

4.2.1 ICO 现状

现如今，加密数字货币领域正上演着疯狂的资本游戏：比特币、以太币等加密数字货币价格近期攀升至高峰后持续下跌；与此同时，ICO 却开始火爆，但野蛮生长中种种乱象也逐渐浮出水面。

ICO 是 Initial Coin Offering 缩写，指首次公开募币，是区块链项目首次发行代币、通过比特币等虚拟货币募集资金的行为，这一概念源自股票市场的首次公开发行（IPO）。这个与 IPO 有着类似逻辑的区块链领域的融资方式，正迅速从极客的世界走向普通投资者的视野。

ICO 目前基本不受监管，参与门槛较低，投资人得到的是代币而非股权。融资成本低、效率高且无需让渡股权等优势，为许多不具备上市资格、没有银行贷款资质或缺少风投资源的企业提供了新的融资渠道。由于技术性较强，投资人对项目的真实运营情况和盈利前景判断不足，投资往往出于跟风追捧，这使得该市场鱼龙混杂、项目良莠不齐。有些 ICO 项目最终成为圈钱工具，甚至有些项目起初就有非法集资嫌疑。

从投资的角度看，有些 ICO 项目动辄筹集数千万甚至上亿人民币（以比特币或以太坊折合人民币计算），但从业内估算来看，白皮书宣称要做的事情无需如此规模的资金。另外，当前 ICO 泛滥，项目上线缺乏有效审核，透明度极低、资金流向极其不透明，所筹资金有很大嫌疑进了私人腰包，甚至中心化 ICO 平台本身也有卷钱跑路的风险。

基于唐盛链底层的 DICO 平台，是唐盛物联团队开发的第二款落地应用，专注于解决股权众筹、代币众筹等数字金融新兴领域中存在的问题。以该应用为基础的参赛项目——唐宝，在中国首届区块链技术创新应用大赛上，斩获创新创意和创意类三等奖两项大奖。该项目预计在 2017 年 10 月正式上线公测。

4.2.2 DICO 流程

DICO（Distributed ICO，分布式 ICO）平台是唐盛链底层架构上致力于利用区块链技术解决中小企业权益资产数字化流通的项目，该项目旨在通过区块链技术解决传统融资模式的“钱、人、信”三大难题，从而实现中小企业、金融专业人员及投资者三方共赢。

DICO 应用支持两类 ICO：初创 ICO 与集合股权 ICO。下面将分别介绍两类 ICO 的流程。

初创 ICO：

作为具有去中心化交易撮合能力和资产数字化能力的区块链底层，唐盛链内盘提供了“交易撮合”和“资产发行与管理”这两种公共服务架构，每一个想进行 ICO 的初创企业都可以在唐盛链内盘发行相应资产（积分、代币、实物资产等）作为自己的 ICO 标的物，并根据自己的 ICO 策略编写智能合约。该智能合约定义了一种用户自定义数字资产，并约定了该资产流转的权利和义务，智能合约通过审核后，融资方发起一轮价值评估事件，系统中的轮转记账人参与价值评估，通过 GEAR 协议中的价值评估子协议完成数字资产的定价，用户使用唐宝购买数字资产后完成 ICO。

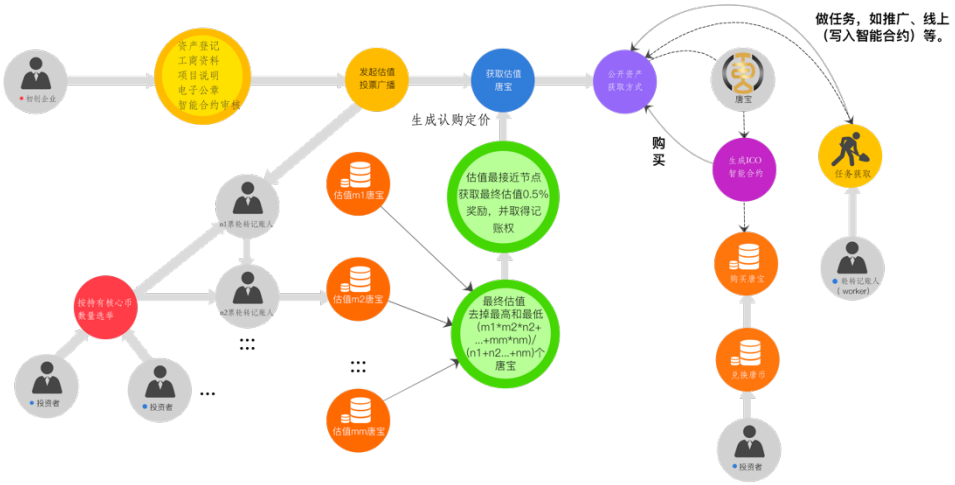

图 7 一个典型的初创 ICO 流程

如图 7 所示，一个典型的初创 ICO 流程可描述为如下几步：

1）初创企业（融资方）发行资产，撰写资产绑定的合约模板；

2）向智能合约治理委员会提交合约模板，等待审核通过；

3）合约模板审核通过后，得到分配合约地址和接口；

4）初创企业选择融资估值方式：如果选择自行估值，可以直接路演公示后挂单售卖；如果选择价值评估，则进入第 5 步；

5）在唐盛钱包中提交资产评估申请，等待轮转记账人参与评估共识；

6）在线上线下社群进行路演和公示，争取更准确的价值评估；

7）评估共识结束，资产获得最终定价，评估共识过程参见 3.1.3 小节；

8）融资方按照定价将资产挂单交易，投资人用唐宝作为基础代币进行投资认购。

集合股权 ICO：

在 DICO 平台进行过初创 ICO 的企业，在连续三年达到盈利指标（指标由持币人大会决议）后，可以申请参与集合股权 ICO，经过公示、路演和尽调后，发起集合股权价值评估，经过一轮价值评估后，企业的股权数字化为唐宝，并发行至企业账号中。

值得注意的是，此处的唐宝相当于所有参入企业的集合股权，也就是说每一个企业进入后的股权估值，都是按照当前唐宝的价格来计算发行的数量。例如企业 A 申请集合股权 ICO 时的唐宝价格为 1 元人民币/个，集体评估人如果认为该企业股权价值 1 亿元人民币，则评估值为 1 亿个唐宝；当企业 B 申请集合股权 ICO 时，如果集体评估人评估该企业也价值 1 亿元人民币，而当前唐宝价格为 10 元人民币/个，则评估值为 1 千万个唐宝。

图 8 为一个典型的集合股权 ICO 流程。

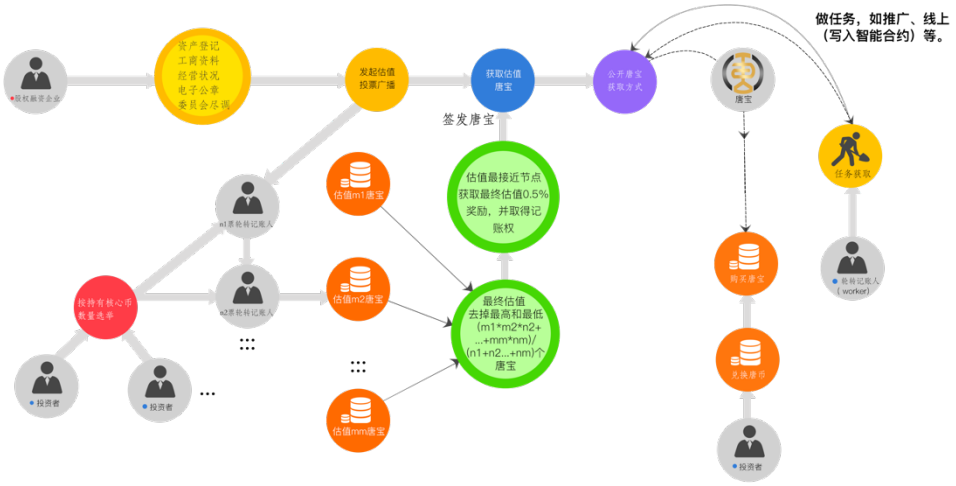

图 8 一个典型的集合股权 ICO 流程

4.2.3 唐宝（TSL）的意义

唐盛链的核心代币——唐宝，作为唐盛链接入企业集合股权背书的数字货币，其意义和目前只有单纯数字的其他虚拟货币完全不同。它是一种集合股权价值背书的创新货币，它的价值是对整个**唐盛链生态生产总值**（Gross TangshengChain Product，**简称 GTP**）的正反馈。

唐宝作为货币，既可以衡量整个唐盛链生态的发展状况，又可以参与市场交换，还能够代表集合发展企业的股东权利，可以说涵盖了数字金融的所有基础需求，具有开创的意义。

唐宝总量固定 30 亿枚，但不会随意地大量发行。大部分唐宝会在企业集合股权价值评估事件发生时产生，少部分的唐宝由轮转记账人奖励获得，具体分配情况参见 8.1 小节。

4.2.4 应用特性

相比传统方式，在唐盛链上进行分布式 ICO 有以下优势：

成本低，唐盛链已经为希望 ICO 的初创企业提供了一个现成可用的用户社区，如果仅进行线上宣传和路演，成本极低；ICO 进行时，其费用只是一些唐盛链交易操作的微量手续费。

资金透明，基于区块链的 ICO，可以有效地监督资金流向，让项目进程和花费有据可查，让 ICO 项目不再脱离投资人的监管。

估值合理，基于 GEAR 共识机制的集体评估，可有有效防止项目虚报价值，同时，由于激励奖励、加密评估、匿名评估等机制的存在，有效降低了价值评估人联手压价的可能性。

ICO 资产直接交易，因为依托于唐盛链去中心化撮合交易能力，所以原则上用户在 ICO 过程中得到的资产可以即刻在唐盛链内盘挂单交易，其它用户也可以即刻购买这些“二手”的原始资产，某种意义上说，这是个一二级市场融为一体的资本市场，当然，项目团队可以通过智能合约规定二级市场的行为，比如白名单、黑名单、T+?等等。

满足企业各个阶段的融资需求，DICO 不仅给初创企业提供了融资渠道，还可以给运转良好、有持续盈利能力的企业提供集合发展的机会。

集合股权背书的货币，货币价值是 GTP 的直接反应，可以在合理区间内波动，不存在单个企业股权、代币发行时的庄家操控价格的问题。

共享唐盛链发展，对于符合数字金融生态，符合唐盛链发展方向的团队，在实现连续三年盈利指标后，可以直接在唐盛链中以集合股权的形式上市融资，与唐盛链生态共同发展。

4.3 “唐小恋”智能投顾——数字资产配置智能优化

4.3.1 我国投顾现状

我国传统投资顾问一直无法获得大规模发展的原因，一是覆盖的用户有限，管理收费较高，主要面对小部分的机构投资者或高净值客户；二是资源配置效率低，获客成本较高；三是理财顾问能力参差不齐，知识结构单一；四是传统投顾服务有较高的道德风险，大部分理财经理不希望客户长线持有单一的理财产品，以免佣金收入下降。

这些原因导致当前投顾市场处在一种极度稀缺又极度混乱的状态。一方面，中证协和中证登方面的数据显示，投资者和协会注册投顾的比例高达 3138：1，投顾极度稀缺；另一方面，民间咨询泛滥，甚至很多人打着投顾的幌子行非法荐股和无牌照代销之事。

随着数字金融的发展，“智能投顾”的出现正在缓解投顾市场的混乱状态。智能投顾是指利用大数据分析、量化金融模型以及智能化算法，根据投资者的风险承受水平、预期收益目标以及投资风格偏好等要求，运用一系列智能算法、投资组合优化等理论模型为用户提供投资参考，并监测市场动态，对资产配置进行自动再平衡，提高资产回报率，从而让投资者实现“零基础、零成本、专家级”动态资产投资配置。

虽然目前智能投顾极大提高了用户投资理财的体验，一定程度规范了市场行为，但仍然存在以下问题：

1） 仍然以销售产品为主，投顾结论很难让人信服；

2） 资产配置结构单一，无法满足多元化投资需求；

3） 对投顾建议没有直接的奖励或惩罚机制；

4） 过程不透明，缺少信任机制；

5） 虽然降低了投资门槛，但是门槛过低会引发不必要的社会问题。

4.3.2 投顾模型

“唐小恋”智能投资顾问是唐盛物联开发的第三个官方落地应用，依托唐盛链撮合交易大数据和智能合约，通过独创的量化模型实现投资理财人工智能。其利用唐盛链可信数据、匿名化、强化信任的特点，可以解决中心化智能投顾系统目前遇到的问题。

根据用户历史交易数据、全链数字资产交易情况等，为用户定制智能投顾合约，相当于每一个投顾建议都是一份智能合约，合约根据风险等级配置不同的数字资产，当市场条件触发时，自动执行相应的买卖条款。

举例说明：根据唐盛链底层提供的正确、无差错和无歧义的可信数据，“唐小恋”利用机器学习分类模型自动分析得出某用户可承受高风险且资金供应量充足。于是，“唐小恋”会自动撰写一份智能合约，该合约根据用户持有的数字资产按高风险比例（4：6~2：8 的优先劣后比）自动在分布式交易市场寻找优化配置资源，随着市场条件的变化，自动执行数字资产的买卖。

“唐小恋”智能投顾因为没有传统的投顾成本，所以不收取任何交易佣金，仅收取为用户所赚利润的固定比率的数字资产管理费。同时，智能合约与交易公开透明，有效避免了交易道德风险。

4.3.3 分布式智能投顾的优势

与中心化智能投顾系统相比，基于唐盛链的分布式智能投顾系统——“唐小恋”具有以下优势：

1） 结合全链数据的投资推荐，让投资者更加信服；

2） 结合唐盛链 DICO 和唐贝的能力，可配置的数字资产将非常丰富；

3） 投顾成本降低，根据市场情况自动调整投顾策略，没有利润的情况下不收取任何费用；

4） 合约、交易过程透明，用户可随时终止投顾策略；

5） 只有在唐盛链中产生过交易数据且达到一定量的用户才能使用“唐小恋”，一定程度上提高了准入门槛，将合适的资产配置给合适的用户。

4.4 其他第三方应用

由于唐盛链在数字金融领域突出的适用能力，有很多第三方应用希望借助唐盛链的底层

基础设施和区块链设计理念，实现全新的数字金融模式。目前，已经确认进入开发阶段，并将于 2018 年先后上线的项目包括农业金融新模式——嗨农宝，以及艺术品流通新模式——艺公盘。

4.4.1 嗨农宝

“唐盛庄园农业资源数字化流转平台”（www.tangshengmanor.com）是唐盛庄园（北京）资产管理有限公司旗下专注于解决“三农”金融问题的在线平台。团队有丰富的互联网、农业及品牌推广经验，依托于母公司玖玖投资集团强大的资金及渠道资源，在有机农产品领域，开创了“金融+科技+三农”的创新模式，推动农业产业转型升级。

该团队在福建省漳州市南靖县政府的大力支持下，依托当地林果及其他农业及生态资源优势建立了唐盛庄园-土楼生态庄园。目前，该庄园拥有蜜柚树类 20000 余棵、高海拔茶园 1000 多亩，持有中国驰名商标“睿轩佳香源”，原始自然环境保护良好、野生动植物资源丰富。未来，该庄园将立足天然、健康、有机的生活品质，发展成为集农业生产、果品加工、高端茶叶生产、特色生态旅游于一体的大型自然生态庄园。

与此同时，唐盛庄园-土楼生态庄园还以园区内蜜柚树、茶叶等农产品的“综合收益权”，作为农业资源数字化标的进行价值评估，利用先进的计算机软件技术，将农业资源数字化并实现自由流通转让，成功打造了“唐盛庄园农业资源数字化流转平台”。

唐盛庄园运用大农业、大健康的前沿理念切实解决了“三农”问题，实现了农业生产者、消费者和社会各界的普惠共赢，并通过“唐盛庄园农业资源数字化流转平台”实际项目的投入响应了国家号召，以“金融+科技+三农”的手段优化了农村经济作物产业链条。这一系列的创新实践，是对国家“鼓励农村金融创新”、“深化农村集体产权制度改革”的切实探索，是对时下金融+科技热之于“三农”的新实践、新突破。

“嗨农宝”是“唐盛庄园农业资源数字化流转平台”的升级品牌，在原有流转模式的基础上，利用区块链技术“去中心化、信任强化、分布式共识、不可篡改”的特点提升资金安全，实现交易透明。

唐盛链底层去中心化撮合交易和独特的共识机制非常符合“嗨农宝”的需求，双方将携手用金融科技助力“三农”发展。

4.4.2 艺公盘

德艺公盘电子交易中心（以下简称“艺公盘”，www.yigongpan.com）隶属于山西德艺公盘文化艺术品股份有限公司，是经山西省文化厅批准成立的艺术品经营机构，旨在建立全国性的、专业性的、公开透明的艺术品交易平台，挖掘价值、体现价值、分享价值，实施艺术品产业化运作，致力于为广大投资者提供艺术品投资增值服务，是国内首家由艺术、传媒、互联网等多家机构跨界投资组建，倡导价值型投资理念的艺术品交易及增值服务平台。

艺公盘希望借助唐盛链完成艺术品确权、溯源、防伪和流通，打造中国艺术精品投资平台，打造面向时代、面向生活、面向大众的艺术精品、艺术衍生品、限量文创产品消费平台，

从而推动艺术精品的大众化消费，推进大众生活艺术化发展。

五、 唐盛链治理架构

5.1 治理机制说明

虽然目前唐盛链的研发和维护主体是唐盛物联，但唐盛物联作为一家科技公司，始终积极践行“分享、开放、共赢”的原则，在 DICO 项目完成上线后，将开放所有底层源代码，以 GEAR 共识机制为治理基础，推进唐盛链开源社区的建设，吸纳专业人才治理和维护社区，同时让投资人真正拥有主权，让每一个参与者都能基于自身的能力和权利，为社区贡献自己的力量并获得应得的收益。

为了达成以上目标，唐盛链对分布式自治机构的治理提出开创性的运营方案，我们设计了专业执行权、监督权、主权“三权分立”的管理机制，在该机制下，管理主体主要由持币人大会、专业治理委员会和风控委员会组成，下面将做详细介绍。

5.2 治理组织架构

图 9 唐盛链治理组织架构

如图 9 所示，唐盛链的治理组织架构由三个互相配合、互相制约的组织构成。

持币人大会由唐宝和唐贝的持有用户组成，是唐盛链的最高决策机构。该机构主要通过线上社区组织，持币用户在大会上根据自己所持代币进行投票，决定唐盛链中的重要功能更改或参数调整，提名选举专业治理委员会和风控委员会主席团成员，并拥有对专业治理委员会成员和风控委员会成员的弹劾权。

轮转记账人委员会和价值评估委员会是在 GEAR 共识基础上产生的轮转记账人（ROTATE WITNESS）和价值评估人(VALUER)组成的机构，分别负责轮转记账和评估共识中可能涉及的参数调整或重大决策。

专业治理委员会主席团成员由持币人大会提名投票选举，两年一换届、一年一调整，负责执行持币人大会决议和唐盛链社区日常维护工作。主席团设主席一名，副主席四名（分管

技术、财务、智能合约和合规）。主席团下设四个专委会，采用聘用制管理:技术专委会主要负责根据持币人大会的决议更新迭代开源代码;财务专委会负责整个治理架构工作所涉及的财务收入和支出；智能合约治理委员会负责智能合约模板的审核、形式化验证、安全验证、部署上链工作；合规专委会主要负责相关法律条文拟定、国家政策把控、链上数据存证等工作。

风控委员会主席团成员由持币人大会提名投票选举，两年一换届、一年一调整，负责对持币人大会决议进行法律风控层面的审议、监督专业治理委员会工作、风险基金的管理以及日常法务尽调等工作，该委员会拥有对持币人大会决议的一票否决权。主席团设主席一名，副主席四名（分管风险基金会、日常监管、尽调、法务等工作）。主席团下设四个分支机构，采用聘用制管理:唐贝风险基金会主要管理唐贝交易中收取的手续费和金融服务商接入费用，基金可以用来购买 CDS 服务并抵御系统性偿付风险;监管常务理事会负责对专业治理委员会工作的监督，金融服务商、水龙头、透明网关的审核与监管以及向国家监管部门提供唐盛链监管服务；ICO 尽调委员会主要负责参与 DICO 平台项目的尽职调查并对持币人大会出具尽调报告、风险说明等；法务部负责内部各个委员会成员工作合同的拟定以及唐盛链对外的法务合作和法律事务。

六、 唐盛物联核心团队介绍

总顾问-王连洲：被业内誉为基金业之父。清华大学中国经济研究中心副主任、全国人大财经委办公室副主任，北京唐盛区块链技术研究院名誉院长、专家委员会主席。1983 年调任全国人大财经委员会，先后担任办公室财金组副组长、组长，办公室副主任，经济法室副主任，研究室正局级巡视员，是中国《证券法》、《信托法》、《投资基金法》起草工作小组组长。着重研究宏观经济问题，计划与市场关系问题，企业财产制度问题，非国有企业问题等。现任北京大学国际投资管理协会名誉会长、人民大学信托与基金研究所理事长、华夏基金管理有限公司独立董事等职。

CEO-孙文：玖玖投资集团董事局主席、普盛商业保理有限公司董事长、中财汇基金创始合伙人兼风险控制委员会主席。现任中国私募投资行业联合会特邀专家、北京唐盛区块链技术研究院院长、中国区块链协会筹备组组长。

原国家发改委中国投融资专业委员会会长，在信托投资、证券投资以及地方政府城投债方面具有较深的研究；VC/PE 投资方面专家，具有丰富的政府引导基金投资经验，在私募股权投资基金领域有独到见解，管理经验丰富，是“打造中国私募股权国家队”理念的提出者和倡导者。

CTO-解旻：北京唐盛区块链技术研究院副院长、研究员，北京邮电大学信息安全博士，在密码学算法、高级持续性威胁建模与评估、安全协议设计等领域有深入的研究，曾在国际权威期刊和会议上发表多篇论文，并被 SCI 和 EI 收录。

技术总监-王彦忠：北京唐盛区块链技术研究院副研究员，曾任职于酷六网、新浪乐居等大型知名互联网公司，有丰富的网站前端开发和管理经验，在产品的交互设计和用户体验

方面有独特的创新理念。2013 年起担任创业公司联合创始人兼技术总监，负责研发基于 O2O 的大型项目管理系统及人民银行大数据挖掘系统。主要涉及的技术有 PHP、Node. js、Android、IOS、C#等。比特币早期投资者，多个开源项目的参与者。

区块链工程师-肖尊平：精通 C++、Golang 等语言，精通 Android Native Interface，JAVA Native Interface 开发，熟悉常用的算法、一般的图形图像处理算法、分布式架构设计、网络开发、数据库开发（sqlite3、mysql、sql server、redis、mongodb）、UI 开发（GDI、GDI+）、OpenGL、webkit，以及 Windows、Linux、Android 系统，在网络安全、跨平台开发、P2P 网络开发、机器学习算法与结构设计等方面有着丰富的经验。2013 年起开始关注比特币及区块链技术，对 graphene、bitcoin 等开源区块链项目底层代码非常了解。

区块链工程师-李梦杰：长期从事系统架构、算法分析、数据挖掘相关技术岗位，擅长业务数据建模、加密算法编写、分布式编程等。持续关注以太坊、比特股技术发展，曾为社区论坛源码做出贡献。近几年致力于区块链技术的研究跟进，曾带领团队搭建面向互联网保险业务的私有链并进行智能合约的设计研发。

全栈工程师-张烨：拥有 10 年 IT 行业开发工作经验。精通 C/C++、PHP、Java、Node. js 等语言，能够游刃于多种计算机语言、数据库和 Linux 系统之间，快速完成技术的整合与成

型。熟练应用分布式内存、分布式数据库、分布式计算框架完成业务的开发与迭代。2014 年开始关注区块链技术，对其所涉及 P2P 网络技术和信息加密算法颇有研究，并对区块链的应用有所了解。

测试工程师-李盈辉：8 年测试行业经验，曾在多家大型科技公司担任核心测试岗位以及测试管理岗位，具有丰富的测试理论知识与项目实测经验。

副总经理-张亚涛：多年证券行业营销管理及人力资源管理实战经验，精通营销管理、人力资源规划、组织架构设计、团队建设、领导力及企业营销策划，2014 年起开始关注区块链及其应用。

金融顾问-林叶晴：华瑞金融创办人及董事长。澳大利亚太平绅士（新南威尔士州），澳大利亚金融信贷协会（MFAA）成员，澳大利亚信用监督服务协会会员，曾获得澳大利亚信贷专业领域 100 强经纪人华人女性第一位、澳新银行卓越表现奖、Connective 联邦银行最佳信贷经理奖、澳新银行优质贷款经理奖。

法务顾问-Andrew Lin：美国加州大学戴维斯分校法学博士，纽约州执业律师，曾任 Unite Investing, LLC 区块链合规负责人，精通多国金融法案和知识产权保护。

七、 项目里程碑

2017.01 唐盛链内测
2017.02 唐贝内测
2017.03 唐贝金融服务商接入商务计划开启
2017.04 DICO、智能投顾项目启动
2017.05 唐贝上线公测
2017.06 唐贝白皮书发布，获得七项软件著作权，申请五项专利
2017.08 唐盛链白皮书发布
2017.09 唐盛链众筹路演开启
2017.10 唐盛链众筹开始，唐宝首次发售，DICO 内测
2017.11 DICO 上线公测、唐贝正式上线试运营、发布 DICO 白皮书
2017.12 智能投顾上线公测，发布智能基金白皮书
2018.01 DICO 正式上线试运营，开放源代码，治理架构各岗位组建完毕
2018.03 智能投顾正式上线试运营
2018.05 DICO 至少接入 10 家初创 ICO 项目，唐贝至少接入 200 家金融服务商
2018.06 召开首次持币人大会，治理架构任命，商讨唐盛链生态的持续发展

八、 唐盛链资产管理

8.1 分配比例

唐盛链中的原生资产有两类：用抵押物背书的债权类核心代币——唐贝（TCY），用企业集合股权背书的股权类核心代币——唐宝（TSL）。

唐贝由金融服务商签发，代表了融资人的抵押物价值和借款需求，不存在发行量和分配比例的问题。

唐宝由 GEAR 共识产生，总量固定为 30 亿个，四位有效精度。其中 9 亿个作为风控基金锁定在唐盛链网络上，当出现系统性风险时作为抵御手段放出；对外公开的总发行量为 21

亿个。

对外公开发行的 21 亿个唐宝，分为两个部分：1）初始阶段，以 DICO 项目股权作为背书，估值 5 亿个唐宝进行预分配，其中天使轮私募认购 2.9 亿个，公开众筹 2.1 亿个；2）共识挖矿阶段，由共识机制发行 16 亿个唐宝，包括：由每轮轮转记账产生 5 个唐宝奖励给记账成功的共识节点，以及由每轮集合股权价值评估产生相应股权价值的唐宝。随着唐宝发行数量的增加，轮转记账产生唐宝的数量按照一定比例逐渐降低。

唐宝的具体分配比例如图 10 所示。

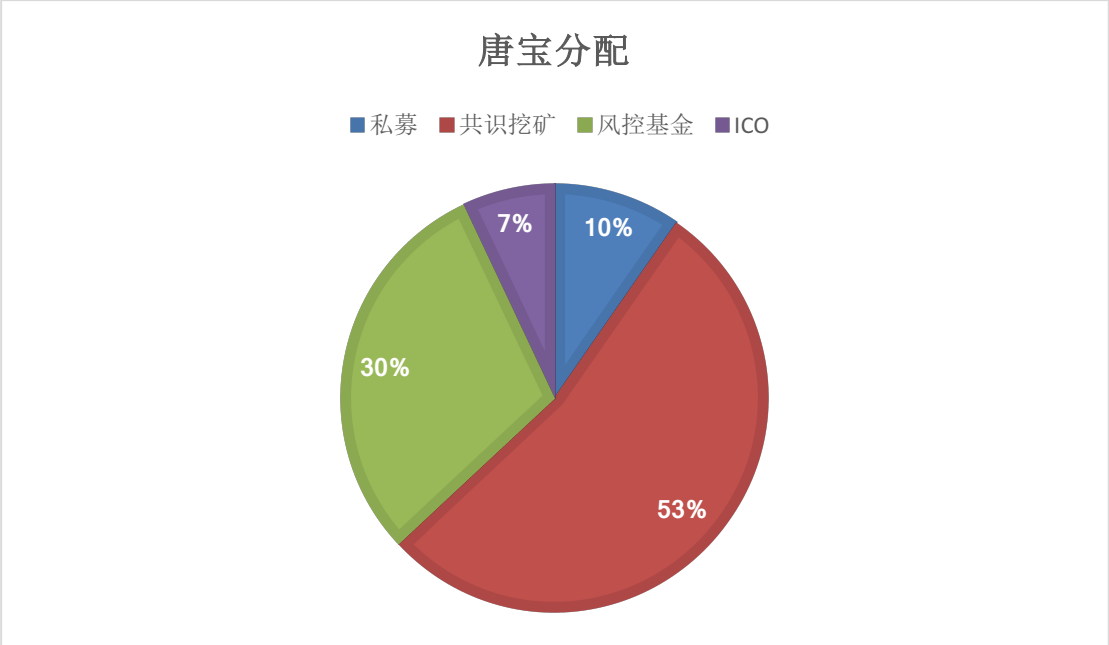

图 10 唐宝分配比例

8.2 经济模型

唐盛链生态生产总值（GTP）是整个唐盛链生态经济的参与者在一定时期内生产的所有最终产品和劳务的市场价值。提供资产数字化服务的金融服务商、透明网关可以为 GTP 贡献来自现实世界的真实资产价值，这部分价值称为链外生产总值(Gross Outer-chain Product，简称 GOP)，主要包括唐贝和唐币价值；参与 DICO 的企业可以为 GTP 贡献来自企业本身所创造的价值，这部分价值称为链内生产总值（Gross Inner-chain Product，简称 GIP），是唐盛链最重要价值来源，主要表现为由评估共识节点产生的唐宝数量与唐宝价值的乘积。

设唐贝价值为 $V^{tcy}{}_i$，唐贝数量为 $N^{tcy}{}_i$，唐贝利润率系数为 k_i，总共有 n 类唐贝，唐币数量为 N_{tcn}，唐宝价值为 V_{tsl}，唐宝数量为 N_{tsl}，GTP 的值可以使用公式 1 来计算：

$$GTP = GOP + GIP = \sum_{i}^{n} V_i^{tcy} \times N_i^{tcy} \times k_i + N_{tcn} + V_{tsl} \times N_{tsl} \qquad \text{公式 1}$$

其中唐宝的价值与 DICO 项目和企业的发展状况之间是正反馈的关系，当唐宝价值增长时可以有效促进企业和初创项目的进展，当企业和初创项目进展良好时，可以正向影响唐宝价值，同时控制唐宝流通量，从而给予 GIP 一个正向反馈。

8.3 财务计划

收入：维持唐盛链项目运作的资金主要来源于众筹、私募、交易手续费、金融服务商接入费。除去众筹和私募所得款，根据第七章项目里程碑，预计 DICO 和智能基金项目上线运营后年收入可达 1 亿元人民币以上。

支出：唐盛链治理结构中，主要支出为专业治理委员会和风控委员会的聘用薪资、办公场地与用品、宣传推广活动费用等。众筹所得款的具体支出比例见表 1。

用途	支出比例
技术研发	50%
审核风控	30%
办公场地	3%
办公日常开支	1%
运营推广	10%
媒体公关	5%
商务活动	1%

表 1 众筹所得支出比例表

唐盛链资产管理由治理专业委员会中的财务专委会负责，纳入全面预算管理，根据实际运营情况编制财务收支预算。年度财务收支预算报持币人大会审议，月度财务预算由专业治理委员会主席团审议。在官网 www.tangshengyun.com 披露每个季度的财务报告，由风控委员会的监管常务理事会监督唐盛链的财务运作，进行资金审计和提供审计报告。

九、 总结

数字金融是未来数年内区块链技术最重要的落地应用领域，该领域有很多痛点可以在唐盛链上得到解决。同时，由于唐盛链的可扩展性，该底层也可以很好地适用于数字金融之外的领域。

如果说区块链的世界是共产主义或者无政府主义，那我们要做的就是将现实世界和区块链世界打通，探索一条通过科技来实现的社会主义道路——这是唐盛链的目标，也是唐盛链的使命。我们期待，唐盛链通过技术手段打通现实资产和数字资产，打破传统金融市场藩篱、重构金融产业结构，最终形成健康稳定的数字金融新生态。

法律声明：

参与唐盛链众筹的购买者，请仔细阅读唐盛链白皮书，全面认识唐盛链的风险收益特征和唐盛链技术特性，并充分考虑自身的风险承受能力，能够承受唐宝的价值波动和唐贝的偿还风险，理性判断、审慎决策。

有关唐盛链的所有消息以唐盛云官网（www.tangshengyun.com）发布的公告为准，唐盛（北京）物联技术有限公司对本白皮书拥有最终解释权。唐盛链唯一官方 qq 群为 197109866，唯一官方公众号为“区块链技术资讯”（微信号：tangdaijinfu），请注意识别。如需商务合作，请联系 010-82858368。