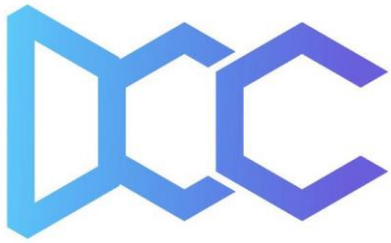
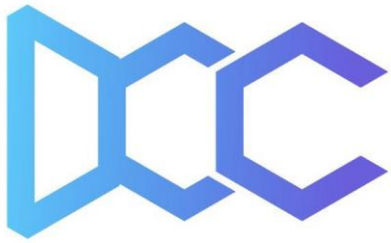




Distributed Credit Chain WhitePaper

Cyber Sheng Foundation
2018

目录

1. 简介

随着世界数字化进程的不断加速，互联网传输速度的不断提升，分布式计算资源的不断积累，数学和密码学技术在数字化时代的大量实用，我们预见未来通过基于区块链去中心化、开放、自治、不可篡改、保护隐私等特性建设的适用于分布式征信、分布式债权登记、分布式财富管理、分布式资产交易的底层公链，会让全球不同国家、地区、商业场景的参与者具有简便的提供金融服务的能力。这时候基于区块链技术的新型虚拟机构“分布式银行”就此诞生，分布式银行不是传统银行，而是分布式金融业务的集合生态。

立意上，通过公平的金融服务能力，打破传统金融机构的垄断，将金融服务的收益返还给所有参与金融服务的提供者、使用者手中，让每个参与者都分享生态成长的回报，真正做到普惠金融。

生态上，通过去中心化思维，改变传统金融业务的参与方合作模式，构建新的点对点、全联通的跨地域、跨领域、跨主体、跨账户的合作模式。

业务上，改变银行负债业务、资产业务、中间业务的业务结构，以分布式财富管理替代负债业务、以分布式征信、分布式债权登记替代资产业务，以分布式资产交易替代中间业务。将传统银行树状的管理结构演进到分布式银行扁平化的管理结构，建立各个业务的分布式标准，提高业务处理效率。

分配上，去中心化就是去中介化，打破原来由于中介导致的信息不对称带来的超额溢价，将这些溢价反馈回生态的参与者手中，达到生态价值的再分配，通过数字化的共识算法，达到参与方的分配公平。

监管上，区块链不可篡改的登记所有的记录，将给监管带可以实时穿透底层资产的能力，大数据分析机构也可以根据区块链数据分析，帮助监管更快的了解行业风险作出适当的应对。在区块链分布式银行的管理制度上编制新的“巴塞尔协议”。

我们将发起建立一条基于区块链技术的主链“Distributed Credit Chain”以下简称DCC，在这条主链上为各种不同的分布式金融业务建立业务标准、达成账本共识、部署业务合约、执行清结算等服务。

分布式银行体系的建立需要一个漫长的过程，可能是 5 年或者 10 年才能完全建立，我们希望经过一段时间的建设，分布式银行发展成为新金融的重要节点，传统业务通过分布式银行进入分布式商业生态中。

我们首先会在 DCC 上开展信贷业务，通过去中心化思想和分布式技术重构传统信贷的业务生态，下面我们具体在介绍分布式银行在信贷领域的变革。

2. 分布式银行从改变信贷业务开始

2.1.传统信贷业务

信贷业务的定义：是一种是货币持有者将约定数额的资金按约定的利率暂时借出，借款者在约定期限内，按约定的条件还本付息的信用活动。信贷业务作为金融市场最重要的金融活动之一，其有序发展对于社会的发展具有巨大的积极促进作用。

信贷市场的基础功能是调剂暂时性或长期的资金余缺：在经济生活中，资金盈余个体有多余的资金，而它们又并不想在当前作进一步的开支；而赤字个体想作更多的开支，但又缺少资金，计划不能实现。资产和资金在此过程中达到了良好的配置作用，对经济体系的顺利运转具有重要意义。

信贷行业历史非常之悠久，在人类文明起初，自美索不达米亚的 3000 年历史的书面贷款合同，显示出信贷制度的发展，并纳入了利益的概念。就已经体现了这种有酬的经济活动的实际应用。

如果没有信贷，人类文明的巨大扩张和进步是不可能的。比如，贷款支持西班牙对新世界的探索，使美国的殖民化成为可能进而推动了工业革命。贷款对社会的效用巨大而美丽，带来了人类已知的一些最伟大的项目。

直到到十八世纪，贷款人仍然使用抵押品，主要贷款类型转为契约贷款。

19 世纪初期开创了一个新的贷款时代，一个更公平的平台， 1816 年 12 月，费城储蓄基金协会是许多储蓄和贷款协会的第一家，其目的是为美国一般的美国人提供一个储蓄和贷款资源，这是一个非常中心化的金融中介。

今天近 90%的贷款人使用 FICO 评分，联邦国家抵押协会(称为联邦抵押协会)和 Freddie Mac 则推荐 FICO 评估抵押贷款。到 1959 年，贷款人正式开始使用 FICO 分数做出明智的信贷决策。

随着移动互联网的发展，通过大数据决策信贷业务，快速的在美国以至于全球市场展露头角。其占领市场主要的方法有三点：

第一，数据挖掘，数据监测，数据对比和差异化竞争；

第二，基于实验和数据提供分析决策；

第三，基于大数据的营销和修正；

基于数据驱动的信贷业务，给我们带来了很多启发，能够大幅的提高效率。但是我们发现在任何一个国家的信贷业务中，还有很多很多的问题，比如说权益不清晰、业务成本高、作业效率低、凭证不可信、隐私泄露等等各种信贷环节问题。

这些问题最大的祸源在于割裂的组织通过各种中心化的系统在提供服务：首先系统是中心化的，有太多了不稳定和造假的可能；其次系统之间是割裂的，相互的校验和信任成本大幅提升；最后数据在传递的过程中并没有很好的加密、使用过程也没有得到用户的真正授权，隐私被滥用。

随着人类的经济活动越来越发达，我们相信信贷产业会更加蓬勃的发展，而随之对信贷的效率要求、隐私的保护以及成本的降低诉求会越来越高，我们相信区块链技术的去中心化思想以及公开的共识机制会是一种更好的解决方案。

2.2.中心化的信贷服务

以提供信贷服务中介机构为例，许多的信贷机构已经陷入了一场可怕的危机。大量的网络信贷机构，通过信息不对称，成为了中心化暴利的行业。为何有如此暴利？透过数据我们发现，在收入中占比最高的是资金利息差。在某发展中国家从全行业来看，银行收入中利息差贡献了 80%。某央行规定的存贷利息差可以达到 3%-5%。关键是这个还只是名义上的，只有大企业才能享受得到。对于大部分普通中小企业来讲，存贷利息差能达到 7%。

中心化的信贷模式让更多的中心拥有了垄断性的优势，放款人和贷款人在信息不对称下，失去了直接交易的机会。有没有一种可能，有一种没有中间商赚差价的信贷服务，让放款人，借款人，风控模型方，催收业务单元，保险机构一起来参与，参与者以服务为目的，在共识的基础上，放款人和和借款人达成借贷平衡。

2.3.中心化带来的信贷困境

成本

信贷机构的核心成本在于通过收取能够还钱的“好人”的费用，来分摊那些不能获得借款（获客、数据、信审等）以及不能偿还贷款（坏账）的成本。

很显然这一成本分摊的方式是极其不合理的，对于借款人来讲，他们额外承担了成本。对于信贷机构来讲，他们的利润空间始终有限但是成本管理难度变大，效率被拉低，利润率却无法进一步提升。

从全行业角度来看，那些投入巨大科技力量在算法算力方面的工程成本被重复的支出，因为几乎每一家金融机构都是为了判断几乎相同的一群人的借款需求而重复的投入科技成本建设系统。

效率

从借款人角度来说，大多数国家的消费金融市场借款人对于申请条件、自己的信用情况和可能获得的服务几乎一无所知，这催生了大量的服务机构和贷款中介，如美国 CreditKarma 通过帮助借款人查询自身的多家信用评分来为借款人推荐消费信贷及信用卡产品，这无疑拉长了借贷申请的链条，降低了获得服务的效率。

从信贷机构的角度来说，消耗了大量的时间和精力在那些可能本身并不符合自身风险偏好的客群身上，使得资源投入浪费的同时，信贷机构的效率也被大幅度降低。

借款人权益

从借款人的角度来说，缺乏自证信用的能力，这使得在消费信贷实操中贷款中介的群体显得愈发“重要”，我们抛开资料造假不谈，仅看正常的业务办理，不论是消费信贷发达国家还是不发达国家，都存在专业的贷款中介/经纪或者客户经理帮借款人

组织证明自身“信用能力”的材料，尤其是那些数据征信体系不发达的国家中，借款人办理贷款的额度高低受到资金准备资料的影响显著。

这使得借款人权益并不能被借款人本人所知悉，也使得借款人并不能有效的完成自身的信用积累，比如在中国有超过半数的年轻人办理信用卡的第一目的是“建立信用记录”。

共债

世界各国征信发展水平不均衡，部分国家和地区的征信建设相对落后，具有信贷记录的客群数量不足，这也催生了世界范围内近几年互联网金融通过服务那些没有信贷记录的客群的创业浪潮。

但是这一浪潮之下，共债问题却成为了扼杀行业发展，引发社会关注的一大诱因。从借贷发生的角度来看，债务信息被各个信贷机构“散列”的记录，但是没有人比借款人更清楚自己的借贷还款历史，通过设立中心化机构完成个人征信的实施成本高昂。

暴利

中心化的信贷模式让更多的中心拥有了垄断性的优势，而太多金融机构已经忘记服务初衷。他们以利润为目的，一方面克扣存款人，一方面压榨贷款人。通过规模化不断放大自己的利润。如果这些利润被释放，我们相信会促进更多产业的良好发展，他们可以招聘更多的人，更好的投资技术，给更好的福利。

2.4.去中心化区块链对于信贷业务的价值

2.4.1.打破垄断和暴利

“人人”都可以选择放贷对象，市场在去中心化的服务情况下百家竞争，把定价权交给市场双方而不是交给中介机构，市场参与主体通过在区块链上提供算法和算力获取回报，重新分配数据的价值。

2.4.2.合理保护隐私

个人原始信息和非脱敏数据不应长期被第三方机构所缓存，个人的数据保存在用户处是最为合理的方式，存储的方式可以是个人本地存储，可以是加密存放在云上通过本地寻址方便的取回。

个人传递数据通过加密通道点对点的传输给数据接收方，只有数据接收方可以对数据进行处理，处理完毕后数据接收方理论上可以不保留数据。或者数据以零知识的证明的方式提供给数据需求方，通过不泄露信息本身原文的情况下，证明数据的真实性和所有权完成业务需求。

2.4.3.打破数据垄断

让个人拥有数据的所有权和使用权，传统的方式中由于无法验证个人持有数据的真实性，个人拥有数据只有所有权，没有使用权，使用权需要个人授权机构提供证

明才能获得，区块链技术打破数据在第三方机构集中存放、证明带来的数据价值溢价，也避免了数据被第三方机构滥用和泄露。

2.4.4.提高数据验证效率、降低使用数据的成本

个人的数据可以被自动验证正确、并且根据数据类型可以多次被使用能显著降低数据使用机构在使用数据过程中的成本。无需每个使用机构在每次使用用户数据过程中去重复获取用户的授权，重复调用获取数据。

2.4.5.构建数据超市

建立标准数据超市帮助数据认证机构更好的营销自己处理过的数据标准，建立大数据处理的品牌和价值高地，通过数据被使用频率和反馈数据给数据平台进行定价。金融机构也可以更便捷的看到数据超市有多少数据模板可以被使用，推动自身 IT 系统对接更有价值数据。

2.4.6.AI 风控

通过深度学习和人工智能风控系统在链上提供反欺诈和模型算法，帮助金融机构处理个人数据，但又不存储个人数据，合规的帮助金融机构提升风控能力。

通过提供加密算法将风险策略进行发布服务，让借款人通过链上的风险策略服务，基于算法供应商以及信贷机构发布的算法进行申请校验，对于可以获得的借贷服务进行主动筛选，而无法获得机构借款的客户则选择不与该机构发生借贷申请，避免个人信息重复的多家提交。

这使得信贷机构的交易效率得到了大幅度的提升，而交易成本进一步下降，不再为了获取那些原本无法提供服务的借款人分配算力资源，也不再支付成本。

2.4.7.借贷行为公开

借贷双方将双方认可的借贷发生过程数据开放给其他需要获得数据的机构，通过在区块链上创建信贷历史报告，帮助放贷机构有效避免多头借贷、重复试探借贷等问题。

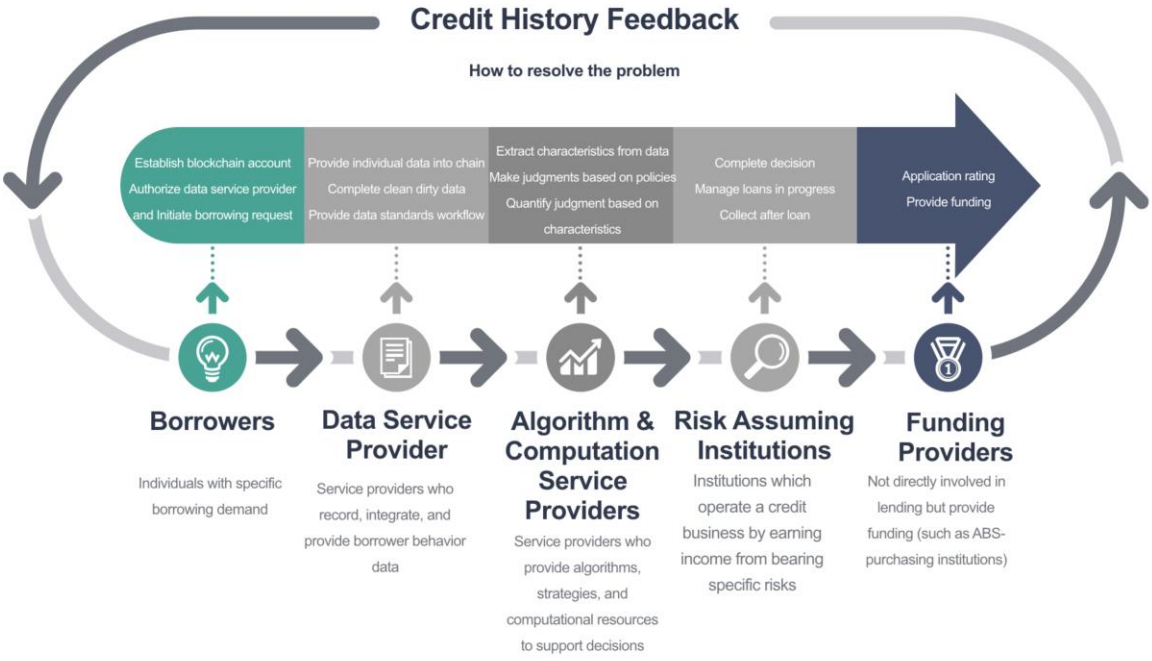
2.4.8.数据正向反馈

借贷数据能够被除了借贷方使用可以帮助多机构全局的分析借贷人行为和借贷结果，给单次借贷非参与方建立起对个人更全面的信用评价。

通过部分公开的数据可以让更多审计机构、监管机构更有效的评估系统风险。

Distributed Credit Chain 将以上解决方案落地到实际的业务场景中，建立和进化为一个全新的、服务于全球的超级信贷生态。

3. 分布式信贷如何解决信贷中心化问题

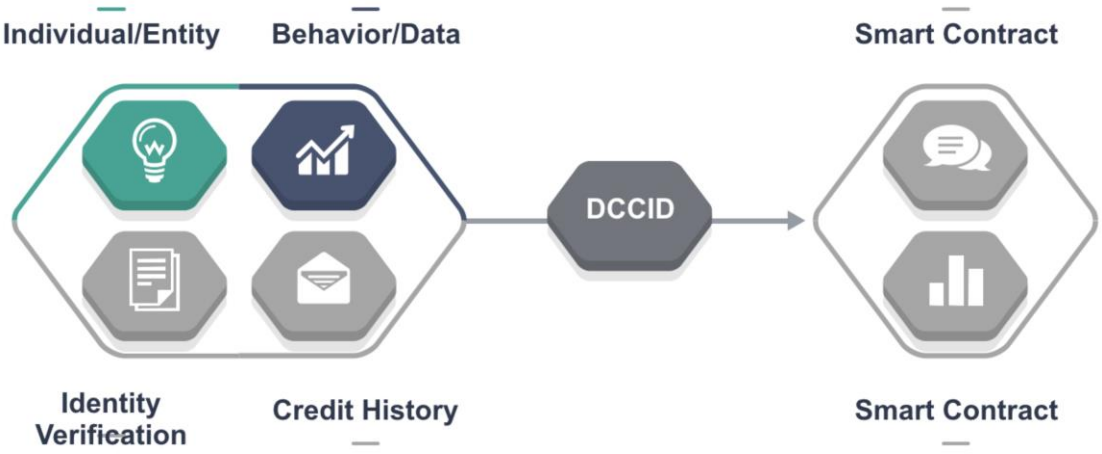


3.1.用户账户标识体系

DCC 中每个个人或者机构有用一个 DCCID，DCCID 通过公私钥对的方式生成，形成一个 address。这个 address 就如同传统互联网系统中的 Memberid，标识和关联各种现实世界的属性，比如：实名认证、持有的银行卡、拥有几套房产，也标识和关联在信贷链上的信息，比如：一次借款请求、一次借款、一次还款等。

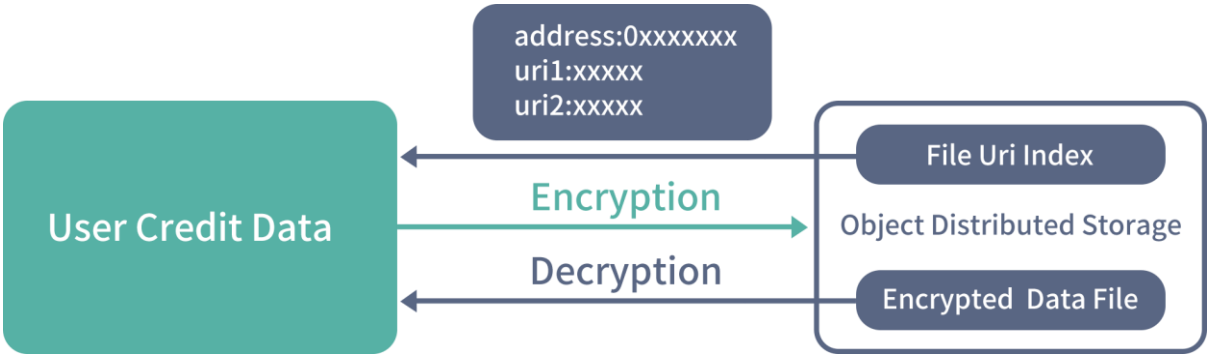
DCCID 是一个去中心化的账户系统，他的生成不依赖 DCC 任何节点，任何人、组织、公司可以离线的生成该 DCCID，在有信息需要被关联到 DCC 上时才在 DCC 生态上留存信息。

DCC 在数据交互中全面采用数字签名方式，全面保障个人或者机构与链交互数据的不可抵赖性。



DCC 将提供一个基于特定云存储服务商的开源个人信用数据管理框架 DCDMF（Distributed Credit Data Management Framework），开发者可以根据 APP 研发需要使用 DCDMF 快速的重建用户的个人征信数据。拥有 DCCID 的用户可以通过导出自己的钱包地址在多个使用 DCDMF 的 APP 中进行数据互通。

DCDMF 采用 AES 的对称加密方式，以 DCCID 的私钥为种子和自己输入的密码（盐）对数据进行加密，并且通过 DCCID 的钱包 address 在云服务商形成数据索引，用户通过 DCCID 的 address 可以方便的在任何时刻获取这份数据索引，也可以利用自己的密码快速的从云端获取明文数据。

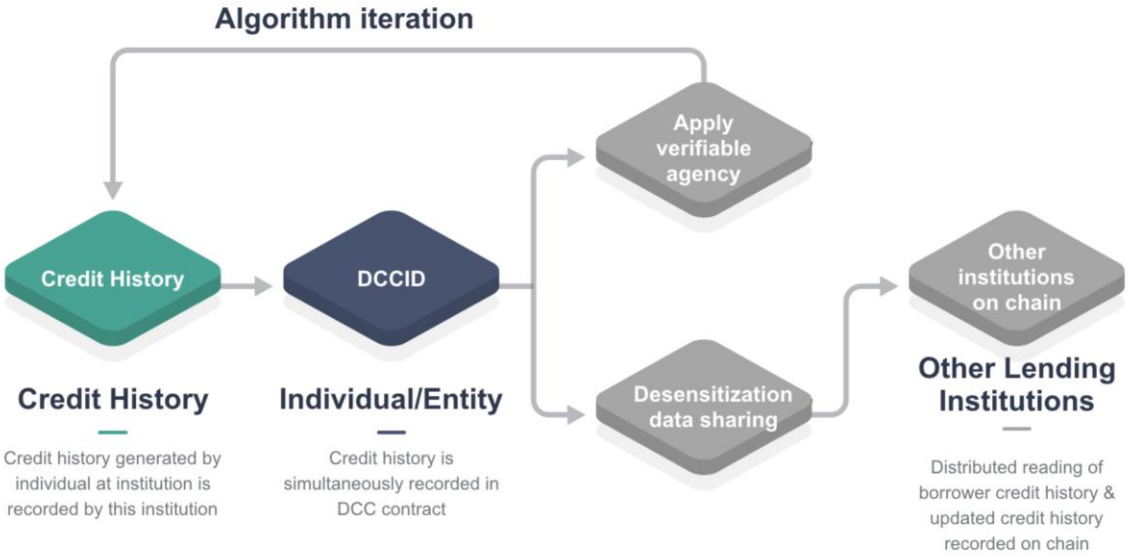


3.2.分布式信用维护体系

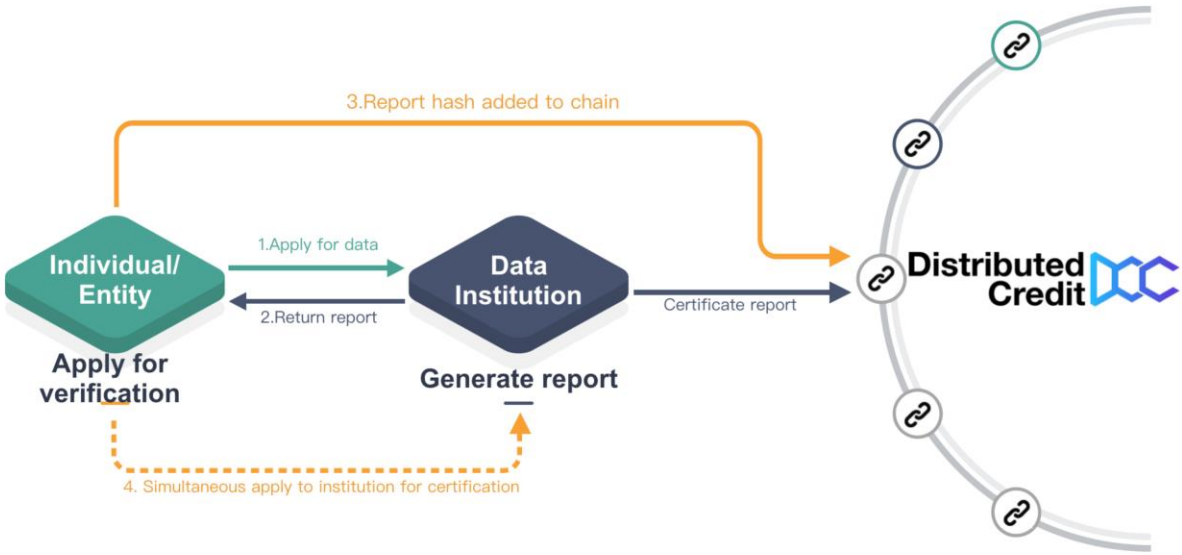
DCC 重新定义了个人信用交换过程。个人通过 DIV（Distributed Identity Verification）系统掌握了数据的所有权，个人数据的存储、展示、使用都由个人可以主导，数据服务机构通过专业的能力不再是缓存和滥用数据获得利益而是通过给个人提供优质的数据服务来获得收益。

Data in the DCC is stored distributed in the hands of users, thereby "returning control of credit to customers"

DIV 系统通过数字签名、数据摘要的方式保证数据在流转过程中防篡改和防欺诈，DIV 的机制优势在于数据机构直接给用户提供数据验证服务，数据不会被第三方机构持有，这种机制给原来只愿意给自身客户提供数据的机构数据分享提供了底层支持。



这一切都源于去中心化，将掌握数据的中心从原来的数据寡头变成了个人，分散的数据被保存在分散的个人手中，在 DCC 上保存产生和证明该数据正确存在的不可抵赖证明，如下图：



个人将数据发送给数据机构进行数据处理，数据机构处理完毕后的标准化数据成为数据报告返回给个人，个人一方面将数据报告保存在本地或者加密存储在云端作为个人数据资产，再对报告进行 HASH 摘要后向 DCC 系统的数据验证智能合约发起认证申请，同时向原认证机构申请进行链上认证，认证机构校验原始报告后如 HASH 一致，在链上对个人此条数据打上被认证过的标签并记录有限时段。

由于该认证的数据在认证过程中只在个人和数据机构中传递，因此数据泄露的风险已被控制在最低的程度，在链上认证采用数字摘要算法是不可逆的，因此在链上没有数据被破解的风险。

通过 DIV 交互架构，个人与个人、个人与数据机构、数据机构与数据机构间广泛的可以建立去中心化的对等认证体系，一个实体被越多的实体认证，拥有越多的数据资产，那么该个人的信用画像越全面，对金融机构判断信贷风险提供了多维度丰富的数据支撑。

个人获得的数据报告又被用作是新的数据资产丰富自身的数据积累，可以再次被数据机构使用，如此循环生成更多的数据验证。DIV 的机制降低了大数据公司和 AI 数据加工公司参与用户数据服务的门槛，为更广泛的场景快速使用用户数据提供了底层支持。

金融机构在使用个人数据资产时，只需要个人自主提交金融机构需要的个人数据报告，通过 DIV 框架能非常快速的认定报告的真实性和有效性。

这是一个打破国家界限、场景界限的征信系统，在任何场景下只要拥有 DCCID 的个人可以提供借贷机构需要的数据，即可完成征信。

总结：通过 DCC 的 DIV 框架，实现了个人数据从中心化征信机构管理向去中心化个人分散持有的转变，彻底改变了原来由每个国家、地区形成的中心化征信系统来维护个人征信信息的格局，将不同国家、地区、语言的信用记录在一个 DCCID 下得到整合，通过去中心化的无数个人和参与机构共同搭建一个不干预敏感数据交互的平台，

是一个真正意义上去中心化的独立征信体系。该征信系统能够服务于世界任何个人和机构、能够提供任何需要信用数据的业务场景。

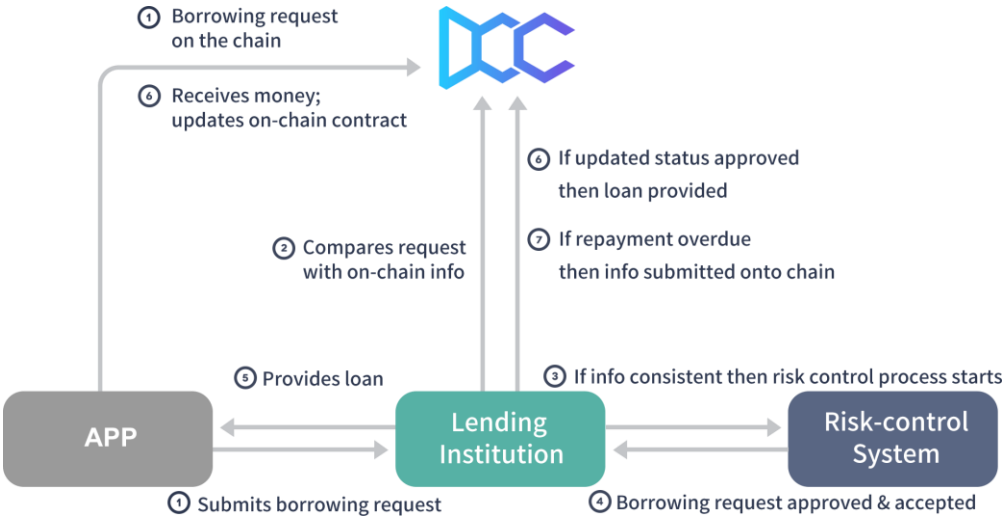
3.3.基于区块链开展借贷业务

3. 3. 1. 数据进件

通过 SDV（Submitting Data Validation）开源框架，借贷机构可以很方便的将用户的数据接入到现有风控系统，SDV 根据 DCCmarket 中的数据提供方持续更新数据解析和验证的模板库，用户数据进入该框架后，SDV 根据 DCCID 的数字签名和提交数据摘要生成风控系统可使用（被验证为本人提交和未篡改过的有效数据）的进件数据。

3.3.2.借贷流程

DCC 建议借贷机构以链数据为驱动来维护借贷流程，用户的借贷申请直接由用户通过签名方式提交到链上，借贷机构通过 SDV 获得进件数据后把审批结果更新到对应



的订单中。

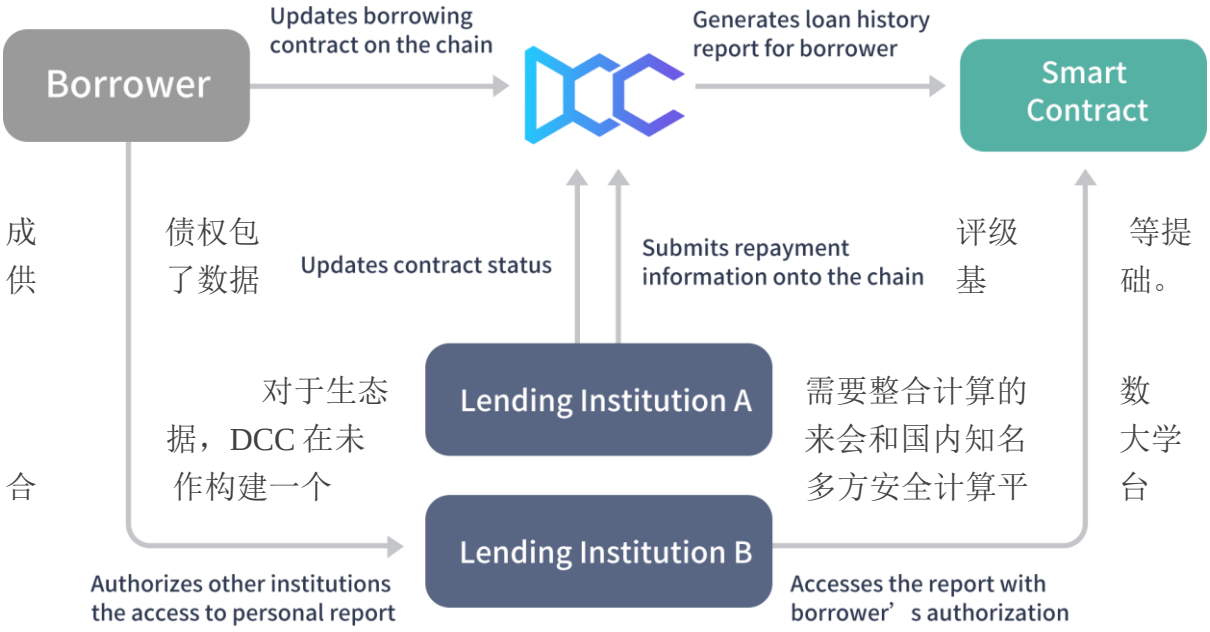
3.3.3.借贷报告

通过 DCR（Distributed Credit Report）合约，将记录个人从申请借款、审核借款、还款、逾期、催收、坏账的全生命周期状态，在 DCC 系统中生成一张借贷历史索引列表。这张索引列表加上个人手中拥有的实际借贷合同明文数据构成个人在 DCC 系统中借贷历史报告，这也是 DCC 系统“将数据还给个人”的目标的体现。

DCR 中的每条记录只有借贷双发持有明文数据，在 DCR 中只记录索引列表，因此虽然记录索引共享在区块链上，但是对于第三方该记录几乎没有价值。这种机制也保障了借贷机构的之间共享数据可以在保持自身隐私的前提下开展。

DCR 机制的实施成本相对低廉，同时对于信贷机构而言、应用一条本身即具备信贷**风控数据**的区块链价值巨大，可以有效且低成本的解决信贷生态共债问题。

DCC 上的数据被不可篡改的留存，这也为后续资产证券化过程中债权确权、通过算法算力完



成 债权包 评级 等提
供 了数据 基 础。

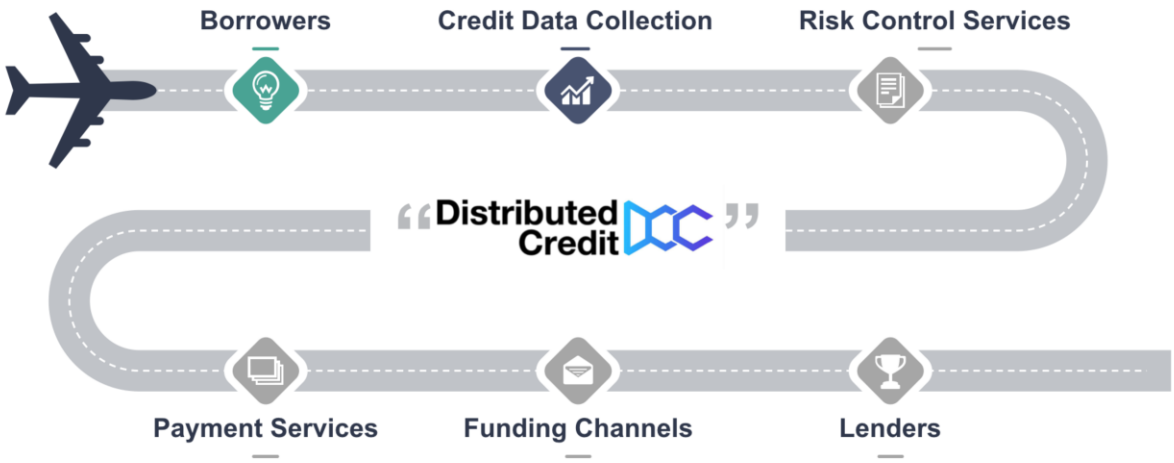
对于生态 需要整合计算的 数
据，DCC 在未 来会和国内知名 大学
合 作构建一个 多方安全计算平 台

（Multi-party computation,MPC）,由 DCC 系统利用此系统将多个参与方的数据无需归集后分析，而是数据保存在本地进行协同计算，这样多参与方不用担心自己的数据被第三方滥用、又可以在相同的计算分析场景下共享数据，真正的达到保护隐私的合作。

DCR 的去中心化传递模式会大大的降低借贷信息中介机构的利润，真正让利给信贷需求方和资金方，让生态的竞争更加市场化，降低参与者进入该市场的信息门槛，提高风控能力对业务的影响力，真正促进利率市场化。

3.4.参与方的非合作博弈

DCC 通过区块链将原来串联的、由多个中心化系统构成的信贷生态关系展开成一个由区块链智能合约为共享媒介的各参与方互相平等的平面型信贷生态新关系。



DCC 生态的开放性让每个参与者独立对等的开展合作，任何合作关系间的再合作对原合作关系没有依赖，使得各个参与方在生态中的决策可以不依赖任何其他参与方，真正构建一个非合作博弈的环境。

这种**独立的双边合作模式会大大降低系统对接的复杂度，信贷系统技术服务商可以更简单的标准化信贷服务的模块，提供出可快速部署的信贷标准系统。**

DCC 系统基于 DCC 这种开放性，因此对任何信贷生态参与方的接入都是无门槛的，并且已经在各个基础服务领域与世界上部分优秀的服务机构达成合作意向。

3.5.生态优势

- ✓ 唯一、不可篡改的身份体系
- ✓ 无数据孤岛和数据垄断的征信体系
- ✓ 处理高效、成本低廉的借贷业务系统
- ✓ 跨任何实体的、永久的数据保存和共享的债权记录
- ✓ 极佳流动性的资产证券化
- ✓ 市场化的利率形成机制

4. 产品场景

4.1.借贷登记服务

借贷登记模式服务于 C2C 个人间的借贷行为，一般分为定向借款和不定向借款两种类型。

定向借款是由出借人与借款人线下就借款问题达成一致后，双方分别下载借条软件并添加彼此的认证，在超信链上完成借款电子合同签订，链上的支付合作方同时提供资金流转服务，用户可以选择通过超信链服务完成借款本金和利息的划扣，也可线下双方自行转账。

不定向则是借款人在没有指定出借人的情况下，通过超信链上的 DAPP，在链上发起借款申请（可匿名），申请中将包含借款金额、期限、利率、还款方式以及、数据服务商为借款人整合并存放在链上的不可篡改个人数据，通过在链上的算法服务商的算法及算力而生成的信用评估等信息，其一度好友（好友可通过 DAPP 授权自动添加和双方在链上主动添加）可看到借款人的申请，并决定是否出借，如确认出借则双方签订电子借款合同以及链上的借贷合约，资金一般通过链上的支付合作方（合作的三方支付机构）完成流转。如借款人个人信用情况不足，还可通过链上的他人提供担保来进行增信并获得借款。

4.1.1.消费贷款

消费贷款也叫消费者贷款，主要指的是用于留学贷款、房屋装修、购买耐用品乃至买车等方面的个人贷款。

C 端申请人将个人申请信息通过超信链发送给 B 端金融机构、或者将自己的数据先行测试各类金融机构的筛选算法，符合条件的申请人可与对应金融机构线上签署电子合约，获得金融机构的借款，该资金用途限定于偿还指定信用卡，

由于区块链的跨地域性，C 端申请人可以是某个急需装修房屋的非洲国家普通劳动者，他在当地有较好的信用记录，但是由于每个国家的信贷发展不平衡，他在当地银行借钱的利率高达 8%年化。而通过 DCC 的去中心化征信数据的共享，一家加拿大的银行评估了这个劳动者的借款风险和使用场景，通过消费场景的增信，银行愿意通过区块链网络给他以 4%年化发放这笔贷款。这样的应用场景在传统的银行网络是不可想象的， 但是在区块链的分布式架构中将时时刻刻在发生。

4.1.2.消费分期

消费分期一般指消费者与商家签订商品分期购买协议，在商家交付商品后，消费者则按照合同约定在一定期限内分次付清货款。

在超级信贷链中，消费者可上传个人数据至链并生成信用评估报告，发生购买行为时，可授权商家查看个人数据和信用报告，了解和评估消费者的信用情况，并决定是否进行分期赊销。

在某些消费商业场景中，传统银行由于本身贷款资金的限制无法给足够的消费场景提供分期服务，此时通过 DCC 合约集，商家可以组织用户建立对应消费场景的虚拟资金池，这些资金池的资金仍然通过 DCCID 账户存放在个人用户手中，当消费产生时，通过区块链的大数据风控模式和不同虚拟资金池的风险偏好，快速的匹配对应的资金，通过多个人分散投资的方式既解决了消费过程中的资金需求，又合理的降低了每个人承担的风险。

例如现在满街的快递外卖小哥，他们每天需要更换 3 次-4 次电瓶车电池，但是如果这些电池都是他们自己购买那么成本极高利用率极低，如果这些电池通过换电站提供，换电站需要在业务开展初期采购大量电池投入成本很大，并且存在业务链接上的风险，DCC 提供一个定制的分期计划，可以让参与的小哥们一起集合资金进行投资，这些资金用来定向的采购电瓶并且进行代币化，在后续的电瓶使用中，业务收入可以被投资的小哥们再进行公平的分享，这样的自给自足的金融体系在传统的金融生态中是不可想象的，但是 DCC 的生态中，开展的非常顺利和自然。

4.1.3.区块链信用卡

基于 DCC 合约集，各种个人、金融机构可以在 DCC 上给特定的用户进行授信，授信金额被维护在链上，通过零知识认证和同态加密的方式，多家授信机构可以在不互相泄露授信金额的前提下，判断具体的消费是否允许进行透支， 透支消费记录也会被保存在链上作为用户的征信数据被生态使用。

基于 DCC 的信用卡还可以方便的整合各个授信机构的额度，进行组合消费。因为合并的信用卡透支识图，通过 DCC 系统提供的分布式征信数据系统，提供信用卡代偿业务的机构也可以用更低的成本对客户进行服务，这种成本降低不但体现在获客数量、单个获客成本，还体现在降低违约率和缩短逾期时长上。通过区块链技术，DCC 有望发展成全世界最大的自己不发行信用卡的信用卡组织。

4.1.4.数字资产借贷

目前在数字资产借贷上，由于数据资产世界和传统世界缺乏有效的个人信用信息关联，导致没有历史信贷积累，在贷前、贷中、贷后处理上都缺乏有效规避风险的手段，DCC 分布式征信系统可以帮助基于区块链的借贷平台打通征信环节、进行贷前风控、管理贷中表现，将数字资产的借贷市场培育壮大。

设想，拥有不同类型数字资产的人，通过借贷链质押自己的数字资产，通过征信数据和信贷记录的支持，从不同的人手中借入 ETH,BTC 等主流数字资产用于再投资，这样的借贷市场会给数字资产交易市场创造出更大的流动性，也可以提供更多的金融衍生产品。

4.2.助力资产证券化

4.2.1.抵押债权登记

在资产证券化过程中，由于资金的提供方并不是资产的拥有方，对于资产的合法合规性、资产历史表现的真实性存在天然的不信任，这也导致其花费大量的成本聘请外部机构对于这些进行验证。很多时候，即使有外部机构的尽调，资产的历史数据仍然不被信任，如果项目发起机构的主体存续时间较短或者评级不够，就很难发行成功。

通过 DCC 上 DCC 合约集，基础资产的权属可以被明确的通过各律所、认证机构、公证机构等在链上进行登记、例如房、车、销售合同、票据等。在这些资产被再次使用时使用方可以很廉价和很高效的在链上确认整个资产的生命周期，有效的避免重复抵押融资的情况。

在资产证券化业务中，原始权益人作为发起方，将资产所有权转让给 SPV 后，只作为劣后级产品投资人，原则上资产后续服务应该由第三方机构完成，包括对还款的回收、逾期资产催收、不良资产处置等。在中心化世界里，这些工作经常还是由原始权益人来承担，再由原始权益人将这些工作自己组建团队或者分包出去，由于原始权益人通常情况下同时也是劣后级产品持有人，整个数据闭环都不对任何人公开，就存在道德风险。

通过 DCC 维护整个 ABS 的分销过程可以有效杜绝了此类问题，在原始权益人和 SPV 中形成实时的共享数据，资产处置的结果穿透。

4.2.2.ABS 资产分销

在 DCC 生态中通过 DCC 系统形成的借贷合同，由于具有去中心化、不可抵赖、不可篡改的特点，同时由于去中心化征信系统的形成，赋予了此类资产极好的分割性和流动性。资产证券化过程中，不再严格需要由单一权益人来出让资产，而会出现新型的技术投资机构，通过甄别、筛选、组合、结构化等手段对整个 DCC 中保存的借贷资产进行打包销售。

通过 DCC 资产打包的 ABS 产品穿透性好，还款回收、预期催收、不良资产处理的结果清晰，验真成本及其低廉，会对整个资产证券化市场带来全新的产品。这些资产证券化产品未来会通过 DCC 的 AssetManage 服务对外提供分布式资产管理能力。大大的提高整个资产管理生态的技术含量和流动性。

5. 生态经济模型

5.1.DCC——估值生态的凭证

DCC 是 DCC 中用来支付劳动力(Pay for Jobs)的凭证，DCC 中任何的劳动都需要支付 **DCC** 作为工作的报酬。**DCC** 的余额管理由 **DCC**token 合约进行维护，**DCC** 总量固定，随着 DCC 中金融服务系统的增多，分布式商业场景嵌入的越来越多，使用越来越频繁，流动性会大福增加。

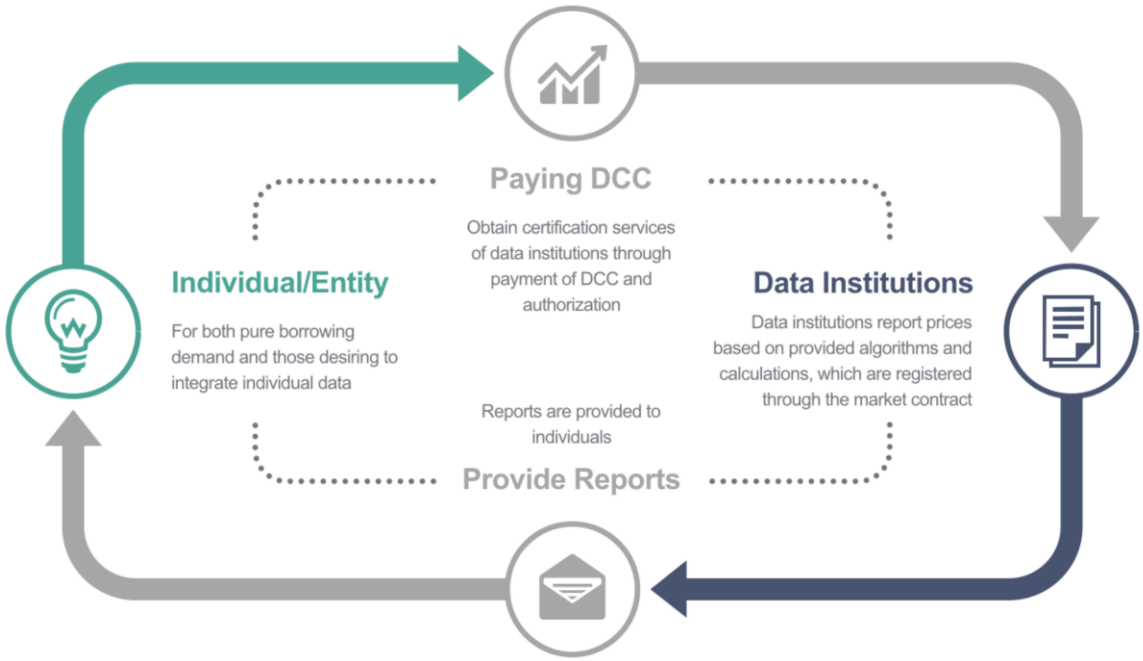
DCC 的支付由 **DCC**payment 合约维护负责多收付方参与情况下的 **DCC** 支付规则。

5.2.生态贡献的好处

DCC 作为生态贡献的重要价值指针，当基于 DCC 开展的金融系统遇到危机时，DCC 作为贡献值可以在生态参与方中作为优先享受金融流动性支持的凭证。这种流动性支持会帮助基于 DCC 开展业务的金融机构对抗流动性风险，创建一个基于贡献的金融生态保护机制。

5.3.DCC 在 DCC 系统中的使用

5.3.1.用 DCC 重构信用成本



在 DCC 系统中，个人要从数据机构获取数据报告需要向数据机构支付 **DCC**，通过 **DCC** 的支付改变了原本数据服务机构获取收入的方式，从原来收集用户数据处理倒卖信息牟利转变为更好的服务客户获得收入。

信贷机构在验证数据的有效性时也需要支付给认证机构 **DCC**，但是由于数据机构收入构成的变化，验证成本会大大降低，这种成本后置将进一步降低借款人的综合成本。

DCC 的劳动力市场由 **DCC**market 合约维护，负责 DCC 系统中提供服务机构以 DCC 计价的报酬登记、变更、删除，通过链下 AI 分析手段给个人或者机构推荐最合适的合作方，有效的维护市场的公平和透明，服务对于 **DCC** 的标价形成也避免了 **DCC** 在二级市场价格波动导致对借贷生产产生不良影响，各参与方在开展业务的过程中不需要关注 **DCC** 在二级市场的价格表现，简单的判断服务对应的本国法币价值即可决定是否使用该服务。

5.3.2.用 **DCC** 重新分配生态利益

在 DCC 系统中，个人申请借贷需要支付 **DCC** 给申请合约，其中一部分比例（例如：50%）按照信贷机构使用数据验证服务的权重进行分配给数据机构作为验证费用，一部分比例（例如：2.5%）作为信贷激励损耗进入当日信贷激励池，一部分（例如：7.5%）会被燃烧回收以确保 **DCC** 总量的持续释放。一部分（例如：40%）作为信贷结果奖励进行分配，如果审核放款成功，借款人主动确认借贷合同该奖励返还给借款人，如果在 1 天内未主动确认借款合同或者借款申请被拒绝则该笔奖励分配给借贷机构。

申请借贷支付的 **DCC** 由借款人自行决定，信贷机构可以设定最低的 **DCC** 门槛和处理借款人申请的优先级，原则上信贷机构会优先处理 **DCC** 支付较多的借款人。

通过此类更多的去中心化交易模型的建立，动态的调整整个生态的利益分配格局，达到信贷处理资源向拥有更多 **DCC** 的个体（对生态贡献越多的个体）倾斜，使生态保持持续的活力。

5.3.3.用 **DCC** 激励信用积累

在 DCC 系统中，借贷申请过程中的一部分比例（例如：2.5%）转化进入当日信贷激励池，和生态固定激励形成总激励池，由 **DCC**reward 合约进行维护在 T+1 日对 T 日按时还款的借款人均分奖励池奖励。在 DCC 生态中，未来不同的业务会形成不同的 reward pool，生态参与者可以在使用和贡献不同生态时获得不同 pool 种的奖励。

每日固定激励按照基金会根据生态发展需求动态调整，每日固定积累最终不会 **DCC** 总量，当没有可以挖出的 **DCC** 时不发放奖励。

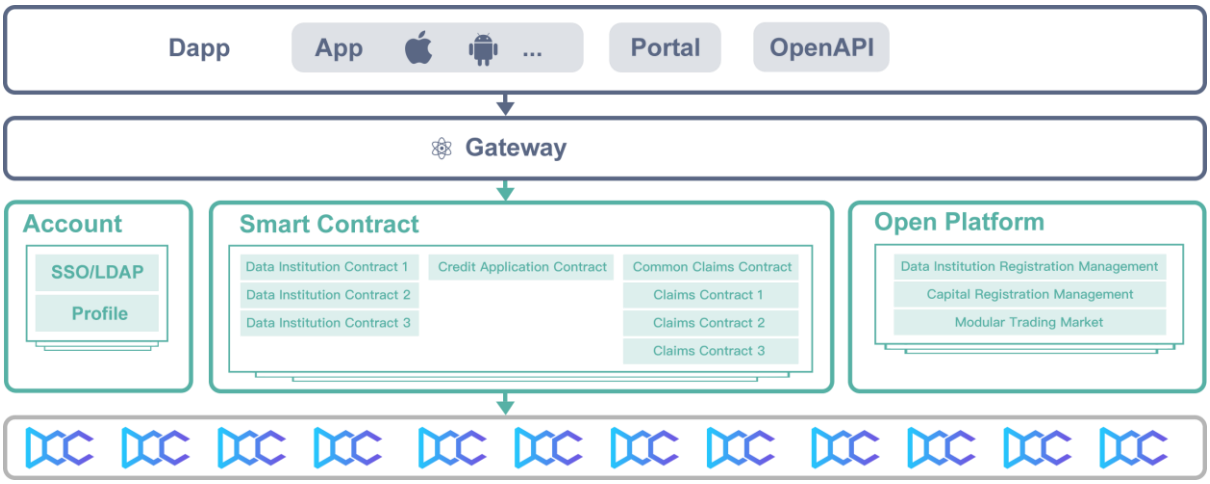
DCC 激励机制保障良好的借贷行为获得更多的借贷便利，激励每个人建立自己良好的信用。

5.3.4.跨越国界的借贷凭证

由于 DCC 系统提供的是一个跨国、跨场景、跨法币数字资产的信贷服务，**DCC** 可以在各个国家对应不同服务于借贷的法币价值，这给借贷服务机构的跨国业务提供了极大的便利。

DCC 随着使用者的越来越多，有望成为跨国借贷生态服务的锚定货币，打通各国借贷生态服务者的价值互换。一个国家或者场景的用户可以通过 **DCC** 购买另外一个国家或者场景的数据提供方提供的数据报告，也可以通过 DCC 系统申请各个国家借贷机构的贷款。**DCC** 在各个国家不同交易所对应不同法币的交易可以提供跨国结算服务的开展。

6. 技术实现



6.1.系统架构

6.2.Dapp

DCC 是一个去中心化信贷开放系统，任何有流量的和场景的平台只要基于 DCC 的标准都可以提交自己的 Dapp 应用到 DCC，生态早期为了保证生态系统的健康稳定，采用基金会审核模式审批 Dapp 的发布申请，Cyber Sheng Foundation 非常欢迎各类场景平台利用 DCC 系统接入 DCC 生态提供互联网消费金融场景。

DCC 研发团队会和 App 研发团队合作早期提供 Dapp 的定制开发服务，帮助借贷机构封装发布使用 DCC 底层技术的借贷客户端，借贷机构利用此客户端开发客户，完成客户注册、维护、数据采集、风控、贷中和贷后管理等功能。

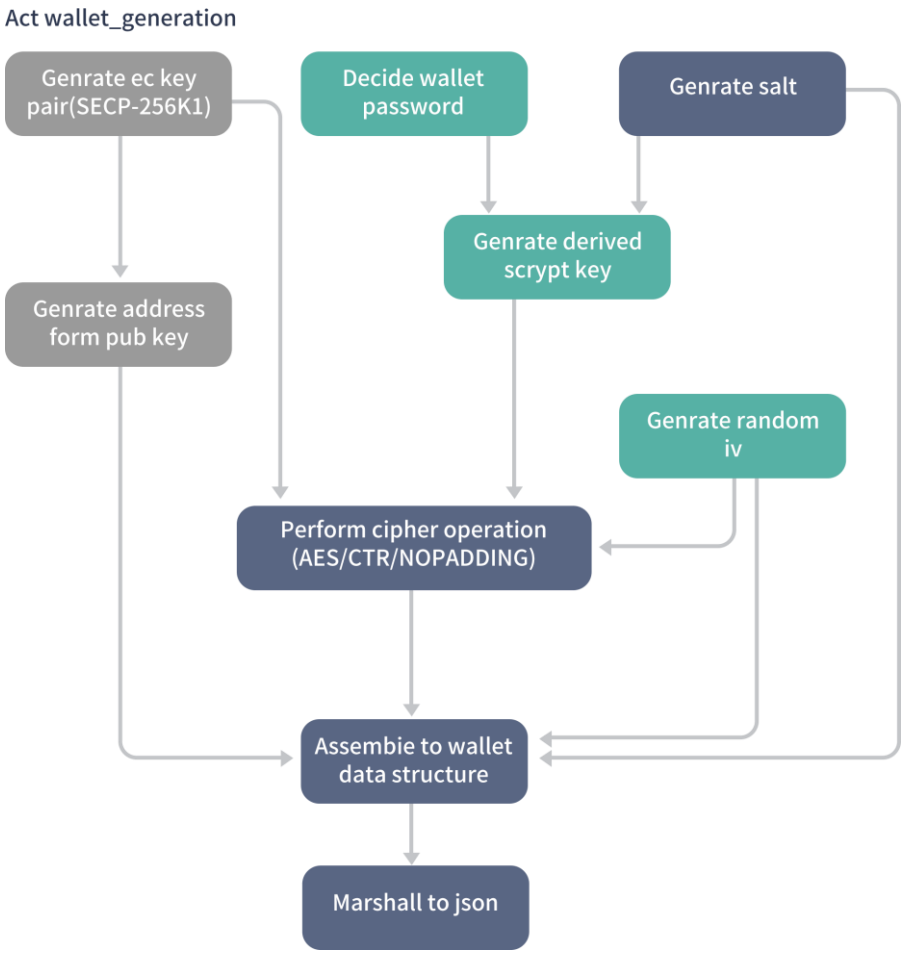
通过定制 App 创建的客户地址在未来可以被客户导出和导入到 DCC 提供的通用 Dapp 或者其他开发者开发的 Dapp 中，这些通用 Dapp 可以使用 DCCmarket 的所有服务结构来给客户提供借贷服务，这样有利用借贷机构和数据服务机构的价格竞争，为客户提供更好的借贷利率。

6.3.账户(钱包)系统

DCCID 采用和以太坊钱包相同的生成机制，钱包由私钥、公钥、地址组成。

DCCwallet 采用“椭圆曲线算法”生成公私钥对，椭圆曲线算法是一种非对称加密算法，相比常用的 RSA 算法有更高的安全性、更快的速度、占用空间小的特点。

每一个钱包账户包含一份密钥对，即私钥与公钥。私钥（k）是一个数字，随机选出的，然后使用椭圆曲线乘法这个单向加密函数生成一个公钥（K），通过公钥（K），再使用一个单向加密哈希函数生成该账户地址（A）。



DCCwallet 使用 Private Key 和 Keystore & Password 的方式保存私钥，私钥可以保存在 Dapp 中也可以被备份导出另行存放。

```
ECKeyPair ecKeyPair = Keys.createEcKeyPair();
byte[] salt = generateRandomBytes(32);

byte[] derivedKey = generateDerivedScryptKey(password.getBytes(UTF_8), salt, n, R, p, DKLEN);

byte[] encryptKey = Arrays.copyOfRange(derivedKey, 0, 16);
byte[] iv = generateRandomBytes(16);

byte[] privateKeyBytes = Numeric.toBytesPadded(ecKeyPair.getPrivateKey(), Keys.PRIVATE_KEY_SIZE);

byte[] cipherText = performCipherOperation(Cipher.ENCRYPT_MODE, iv, encryptKey, privateKeyBytes);

byte[] mac = generateMac(derivedKey, cipherText);
WalletFile walletFile = new WalletFile();
walletFile.setAddress(Keys.getAddress(ecKeyPair));

WalletFile.Crypto crypto = new WalletFile.Crypto();
crypto.setCipher(CIPHER);
crypto.setCiphertext(Numeric.toHexStringNoPrefix(cipherText));
walletFile.setCrypto(crypto);

WalletFile.CipherParams cipherParams = new WalletFile.CipherParams();
cipherParams.setIv(Numeric.toHexStringNoPrefix(iv));
crypto.setCipherparams(cipherParams);

crypto.setKdf(SCRYPT);
WalletFile.ScryptKdfParams kdfParams = new WalletFile.ScryptKdfParams();
kdfParams.setDklen(DKLEN);
kdfParams.setN(n);
kdfParams.setP(p);
kdfParams.setR(R);
kdfParams.setSalt(Numeric.toHexStringNoPrefix(salt));
crypto.setKdfparams(kdfParams);

crypto.setMac(Numeric.toHexStringNoPrefix(mac));
walletFile.setCrypto(crypto);
walletFile.setId(UUID.randomUUID().toString());
walletFile.setVersion(CURRENT_VERSION);
```

在 DCCwallet 版本迭代过程中，在安全验证的前提下，会结合 MPC 平台推出多方协作的分布式秘钥恢复中心服务，私钥客户被分开保存在多家独立机构，独立机构无法独立恢复密码，当秘钥需要被恢复时，通过多家机构协同进行秘钥恢复，帮助用户更安全的的储存秘钥。

6.4.网关服务

网关服务是一个中心化系统，主要用来服务没有能力通过 RPC 接入 DCC 的生态参与机构。机构可以通过 DCC 提供的 Gateway 通过 openapi 方式访问 DCC 系统，大大缩短了业务的对接时间。

DCC 系统也会在 Gateway 服务的基础上提供 SDK 等接入手段，来便于生态扩展，提供简便的享受 DCC 上信贷服务的方式。

6.5.开放平台

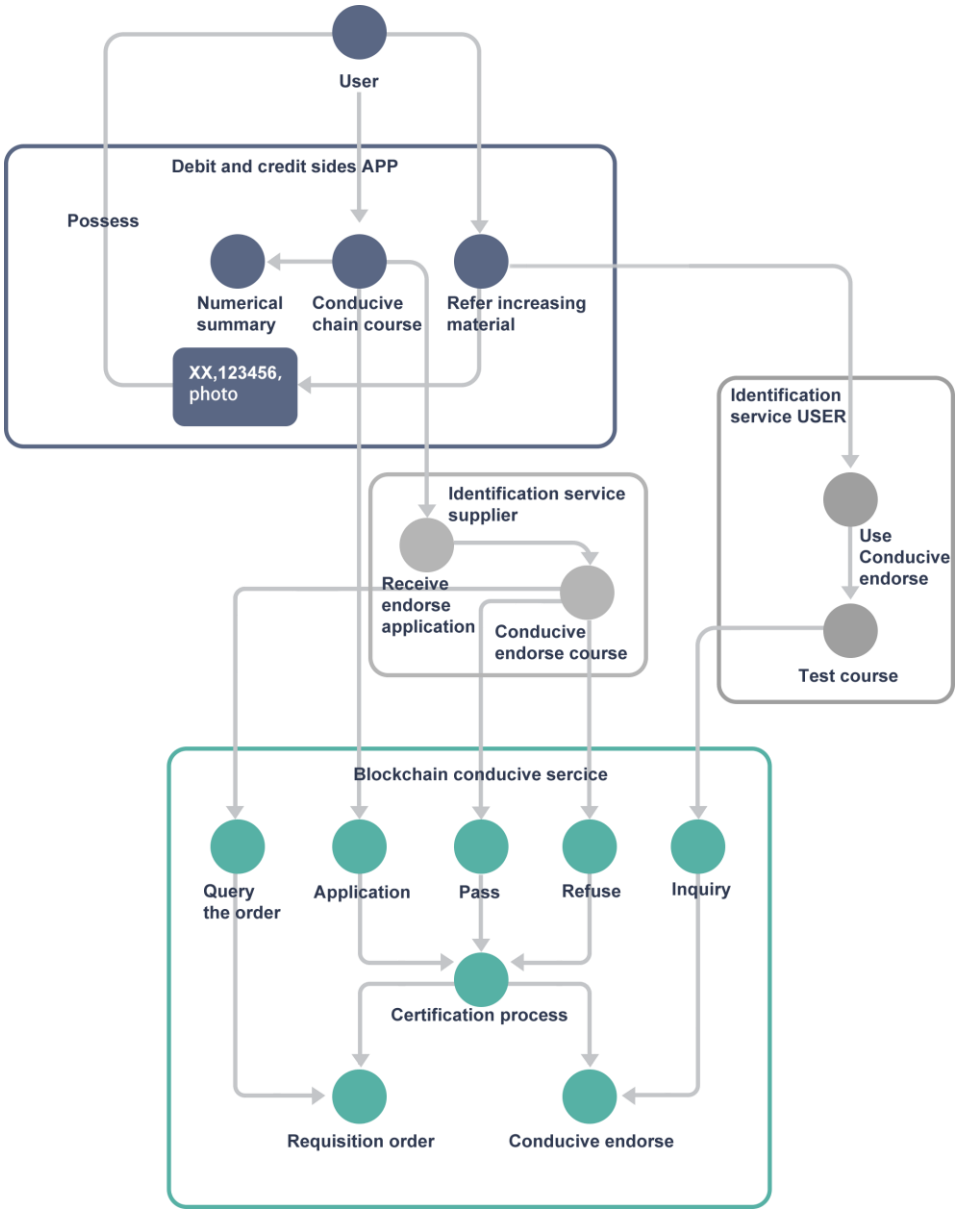
开放平台是一个中心化系统，主要提供数据、服务市场功能，该交易市场服务于数据机构、AI 风控算法服务商、信贷结构等机构合作者，机构合作者在使用链上服务的同时通过该平台可以查看、筛选、接洽自己需要的其他合作机构，利用 DCC 达成合作。

开放平台对接 DCCmarket 合约，所有合作机构以此平台发布劳动力成本，这些数据会被处理和分析后推送给用户，提供用户、机构选择各自所需要服务的价格依据，通过实时报价的方式润滑整个机构服务市场的信息交互。

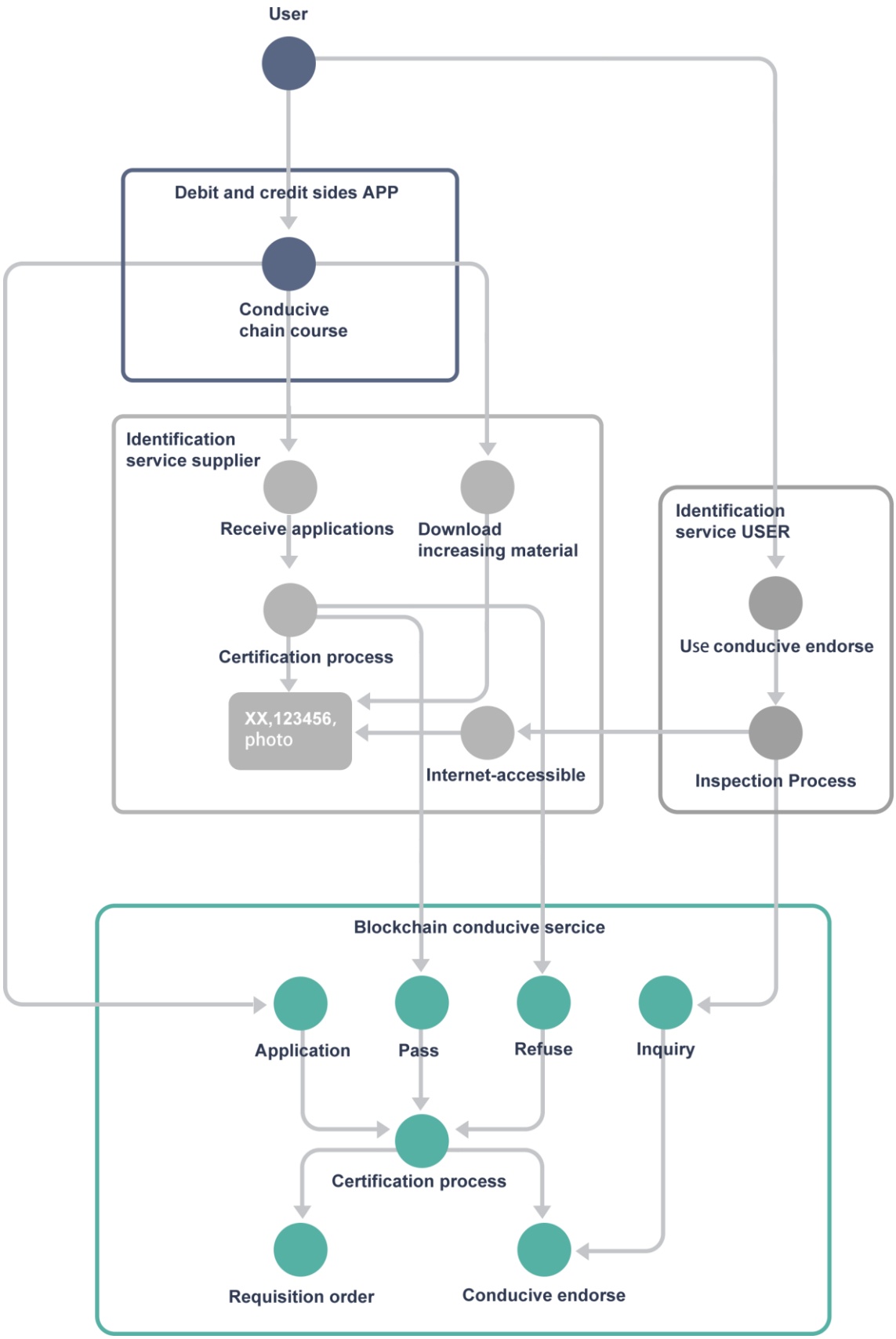
开放平台会提供区块链浏览器，查看所有 DCC 的节点运行情况、出块请款、交易流水等区块链基本信息。

6. 6. 开源**框架**

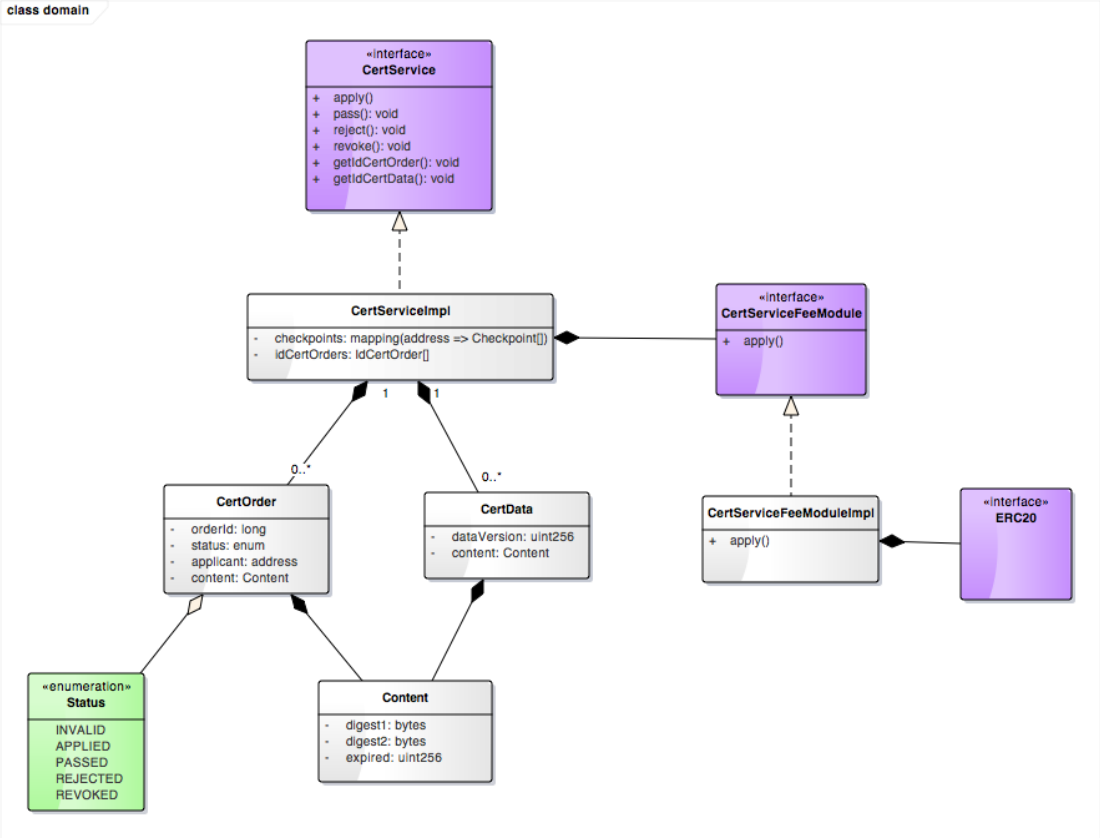
DCDMF、DIV、SDV **等框架我们将会在** github **上进行开源，欢迎合作伙伴根据这些框架进行修改提供更加定制化的服务。**



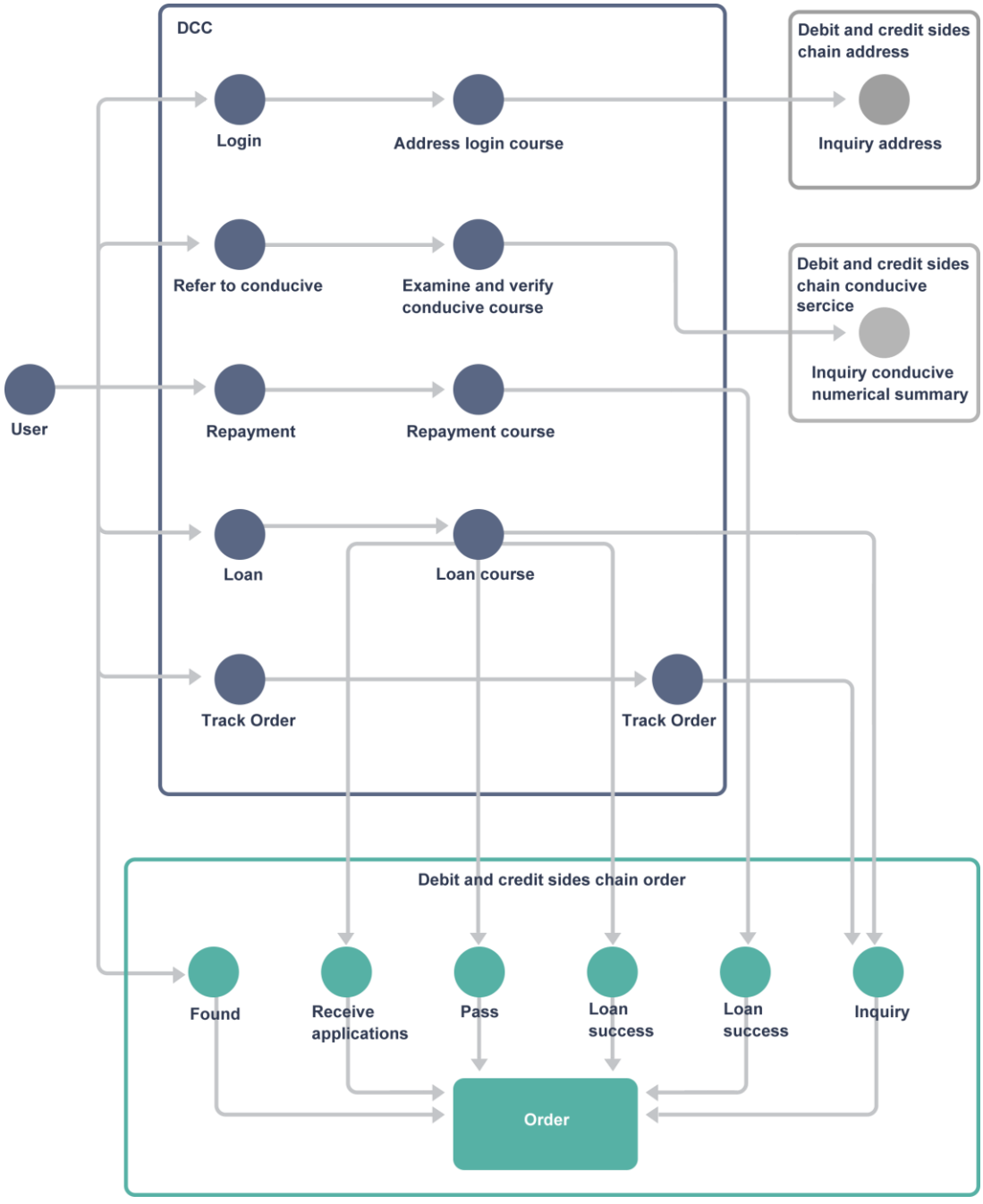
DIV **框架的流程示意**

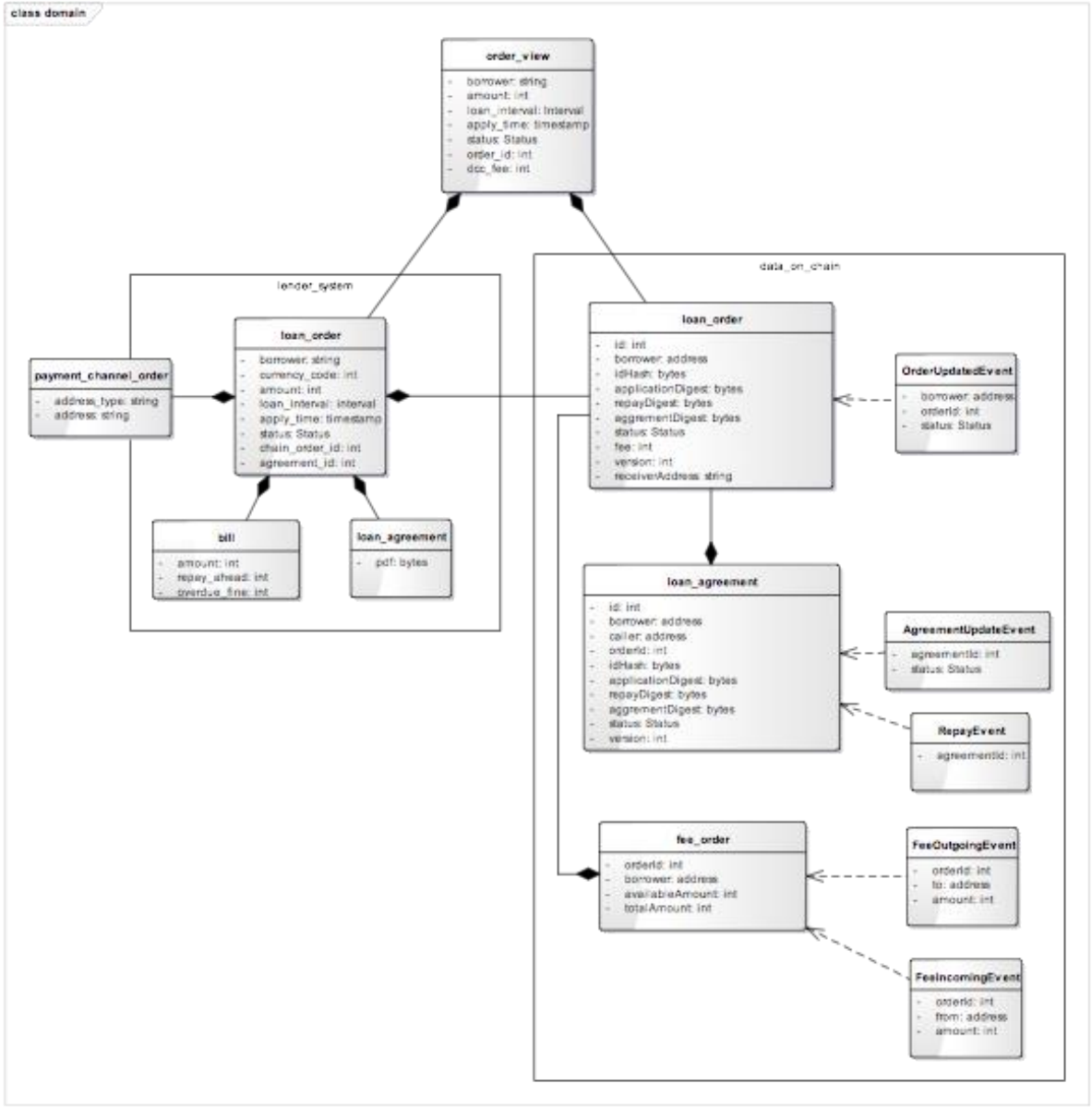

User
Debit and credit sides APP
Conducive
chain course
Identification
service supplier
Receive applications
Download
increasing material
Certification process
XX,123456,
photo
Internet-accessible
Identification
service USER
Use conducive endorse
Inspection Process
Blockchain conducive sercice
Application
Pass
Refuse
Inquiry
Certification process
Requisition order
Conducive endorse

领域模型设计：


class domain
«interface»
CertService
+ apply()
+ pass(): void
+ reject(): void
+ revoke(): void
+ getIdCertOrder(): void
+ getIdCertData(): void
CertServiceImpl
- checkpoints: mapping(address => Checkpoint[])
- idCertOrders: IdCertOrder[]
«interface»
CertServiceFeeModule
+ apply()
1
1
0..*
0..*
CertOrder
- orderId: long
- status: enum
- applicant: address
- content: Content
CertData
- dataVersion: uint256
- content: Content
CertServiceFeeModuleImpl
+ apply()
«interface»
ERC20
«enumeration»
Status
INVALID
APPLIED
PASSED
REJECTED
REVOKED
Content
- digest1: bytes
- digest2: bytes
- expired: uint256

SDV 框架流程设计


DCC
Login
Address login course
Debit and credit sides chain address
Inquiry address
Refer to conducive
Examine and verify conducive course
Debit and credit sides chain conducive sercice
Inquiry conducive numerical summary
User
Repayment
Repayment course
Loan
Loan course
Track Order
Track Order
Debit and credit sides chain order
Found
Receive applications
Pass
Loan success
Loan success
Inquiry
Order



领域模型设计：

详细的开源信息请访问 https://github.com/DistributedBanking/DCC **查看**

6.6.区块链和智能合约

6.6.1.联盟链治理架构

DCC 是一个逐步开放的区块链系统，随着生态的逐步稳定，DCC 完成自我从联盟链转向公链的进化。（DCC 主链上线运行后，所有的代币可以通过 1:1 平移的方式以太坊 ERC20 合约中被兑换到 DCC 主链的钱包中。）

生态的第一阶段，DCC 以联盟链的方式存在，接入的记账节点分配“记账节点”和“非记账节点”，一个记账机构可以申请一个或者多个节点，也可以申请任一类型的节点。

申请机构通过质押一定比例的 DCC 获得成为记账节点的资格，向 Cyber Sheng Foundation 发起申请，在 Cyber Sheng Foundation 通过对节点可用性、稳定性、机构资质的审核后，成为记账节点，记账节点质押的 DCC 不会增加，生态不会提供记账节点记账奖励，记账是参与生态机构公益性劳动。DCC 不是联盟链共识代币，因此在交易共识过程中不消耗 DCC，联盟链阶段所有的记账都是公益的。

DCC 将和提供可信计算的软件服务商一起合作，通过在记账节点中部署持续免疫插件，进行可信计算节点认证，只有当记账节点在满足可信认证的情况下才允许参与记账，一旦被可信认证节点发现运行异常进行或者操作，就会被取消记账权。该系统完成部署和上线后，Cyber Sheng Foundation 将取消质押 DCC 获取记账权的策略，逐步开放公开记账节点加入。

任何申请机构都可以申请成为非记账节点，并且节点没有限制。Cyber Sheng Foundation 承诺在最长一周内完成对非记账节点的接入审批，并逐步开放非记账节点的代码公开化和提供自助部署引导流程。

生态第二阶段，DCC 将根据分布式银行业务共性，定制业务开展最合适的共识算法，从联盟链治理架构进化到公链架构，任何个体都可以申请加入记账节点进行记账，目前世界上的共识算法暂时都不具备承载信贷链业务的能力，因此 Cyber Sheng Foundation 会根据算法技术的不断发展适时的推出进化计划。

进入公链阶段，DCC 会重构账户体系，使用比 ECSDA 更安全的 Schnorr Signature 进行生成，并且在账户默认数据结构上进行扩展，在链上通过零知识证明的方法维护基本的数据结构，让用户可以直接对其进行访问，便于金融业务的后续开展。

在数据保存、合约部署、共识节点开放性上，充分参考 HyperLedger、DFINITY、Zilliqa、Stellar 等项目的经验，结合分布式银行不同业务开展的需要，通过不同的业务 channel 开展业务。

将 DCC 的清算服务下沉到区块链底层逻辑中，更加平滑的插入到各个 channel 的业务生态中，将金融业务和共识更加紧密的结合起来。

DCC 团队和基金会聘请的专家将在迁移改造中提供技术服务，构建主链并且开放记账，重新设定公链记账的激励机制，迁移原联盟链数据到公链中等，平滑的保障该工程顺利远程。

6.6.2.共识算法

共识机制是 DCC 维护数据正确性、一致性、持续性的重要机制，DCC 依据目前的生态需求采用 PBFT 算法作为共识算法。

PBFT 算法的特性包括：

- 共识节点轮流出块，具有同等的记账权，体现了参与者的对等性，且防止个别记账者作恶。
- 秒级出块，满足交易短时间内影响的需要。
- 支持 1/3 容错，整个系统中少于等于 1/3 数量的节点出现故障或作恶，均不影响共识进行。
- 在区块同步的过程中严格校验签名，保证数据的安全性。

PBFT 共识具有高一致性、高可用性，抗欺诈能力较强的特点，被广泛的应用在其他联盟链项目中，较为稳定成熟。

6.6.3.智能合约

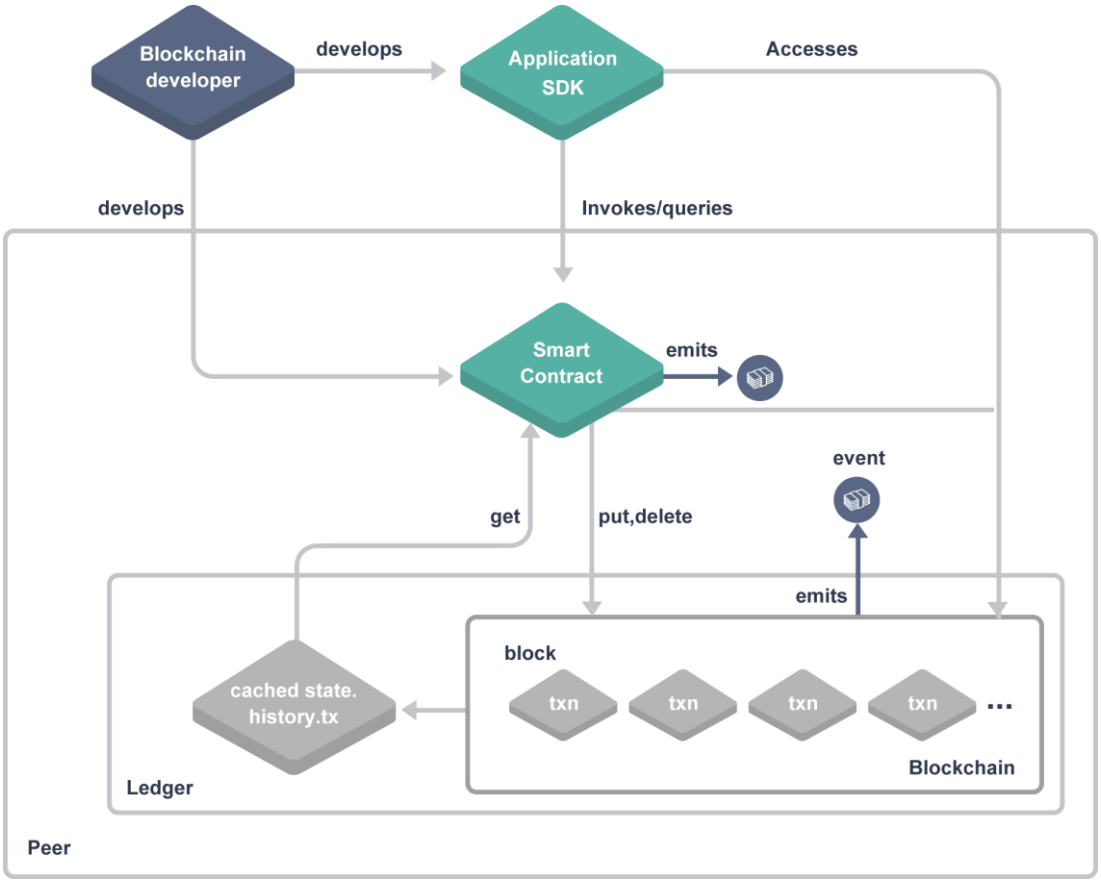
智能合约是部署在 DCC 上的 chaincode，是一段包含业务逻辑的代码。

DCC 生态第一阶段将采用兼容以太坊的 evm 容器作为执行智能合约的容器，DCC 使用 solidity 语言进行开发。

由于生态第一阶段 DCC 采用联盟链架构，因此加入成员在达成共识出块环节不需要支付任何成本，因此合作机构的智能合约必须在开放平台提交到 Foundation 进行审核，并在测试环境验证通过后进行链上部署。

智能合约的代码类似下图：

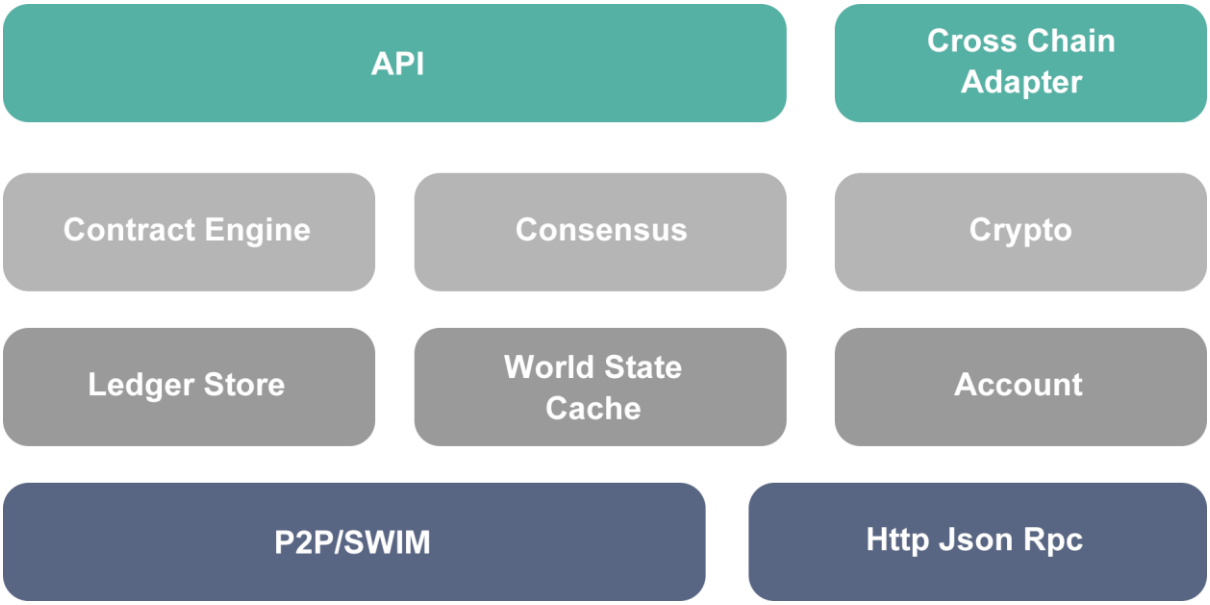
```
function CertService() public {
    insertOrder(address(0), Status.INVALID, Content("", "", 0));
}


function apply(bytes digest1, bytes digest2, uint256 expired) public returns (uint256 _orderId){
    require(digest1.length > 0 && digest1.length <= 100);
    require(digest2.length <= 100);
    require(expired > 0);

    return insertOrder(msg.sender, Status.APPLIED, Content(digest1, digest2, expired));

}

function insertOrder(address applicant, Status intialStatus, Content icc) internal returns (uint256 _orderId){
    uint256 orderId = orders.push(Order(applicant, intialStatus, icc));
    orderUpdated(applicant, orderId, intialStatus);
    return orderId;
}

function revoke(address applicant) public onlyOperator returns (uint256 _orderId) {
    require(applicant != address(0));

    Checkpoint memory cp = getCheckpointAt(applicant);

    //表示有有效的验证信息
    require(cp.content.digest1.length > 0);

    //插入订单
    Content memory icc = Content("", "", 0);
    uint256 orderId = insertOrder(applicant, Status.REVOKED, icc);

    //压栈
    appendElement(checkpoints[applicant], orderId, icc);

    return orderId;
}

function pass(uint256 orderId) public onlyOperator {
    audit(orderId, Status.PASSED);
```


Blockchain developer
develops
Application SDK
Accesses
develops
Invokes/queries
Smart Contract
emits
event
get
put,delete
emits
block
txn
txn
txn
txn
...
Blockchain
cached state. history.tx
Ledger
Peer

智能合约的流程：

6.6.4 公链架构

6.6.4.1 系统架构



6.6.4.2 网络层

我们选用 SWIM 作为网络层协议，SWIM 是 Scalable ,Weakly-Consistent,Infection-Style,Processes Group Membership Protocol 的缩写。他的特点如下：

1、可伸缩，可用于构建数以万计的大规模 P2P 网络

2、弱一致性，节点的成员关系视图不追求强一致性，通过信息交换，达到最终一致性，对一致性的妥协加强了整个网络的可用性，保证大规模组网的可行性。

3、病毒传播，通过 gossip 风格的消息交换协议，快速全网传播信息。

4、分离故障检测与会员关系更新传播，通过特定的故障探测算法，避免了传统 Gossip 心跳检测在大规模网络下不可用的缺陷。

在 SWIM 协议维护会员关系的基础上，我们提供 HTTP Json RPC 组建供节点交换服务协议数据。

6.6.4.3 核心层

账本存储

我们提供一个插拔式的账本存储接口，以适配不同的账本存储实现。我们提供基于嵌入式 K-V 数据库、嵌入型关系数据库以及独立的各种 Sql/NoSql 数据库的账本存储实现。

世界状态缓存

区块链上的交易，本质上是对当前区块链状态进行计算，已获得下一个新的区块链状态的过程。账本存储完整的、不可变的保留了所有的状态的变更，因此是不可抵赖的。

为了提高获取当前世界状态的效率，我们将当前状态的快照保存在高速缓存中，供快速的读取。同时缓存可根据账本存储重建，因此世界状态缓存不影响整个网络的可用性。

函数式智能合约引擎和虚拟机

与其他智能合约引擎有所区别的是，我们认为金融的智能合约是一段纯函数 F，假定当前世界状态为 S，则有：S'=F(S) ,S'为合约执行后的状态。

以纯函数的角度去看待智能合约将得到以下好处：

1、易于测试，因为是纯函数，无副作用，合约可不依赖区块链环境即可进行测试。

2、合约即算法，合约回归规则仅用于描述业务规则，不对区块链产生副作用，提高了区块链的稳定性。

3、易于成本测量，由于仅仅描述业务规则，因此对于智能合约成本的测量复杂度极大地降低了，无需考虑存储、IO 等副作用产生的成本。

4、可靠重放，由于是纯函数，相同的 S'重复执行，得到的结果是相同的 S，也即支持幂等性。

我们将使用 JAVA 为核心智能合约开发语言，目前 JAVA 是金融后端系统较为常用的开发语言。我们用 JVM 作为运行智能合约的容器。

账户

内置账户体系，包含支持多种原生 token。

加解密组建

DCC 公链使用 ECDSA 进行数字签名和验证，使用 ECDH 交换秘钥进行加密通讯。

共识算法

DCC 公链是开放性加入的公链，任何人都可以加入 DCC 公链作为记账节点，我们提出一种 REBFT 的算法，通过在全网节点中随机产生 N 个通信速度较快的节点参与

共识，其他节点为 Follow 节点进行同步，完成一轮共识之后，重新选择下一轮的 Leader 节点。

6.6.4.4 交互层

OpenAPi

DCC 公链将提供大量开源 API 接口提供给参与者进行调用，并且提供一些开发 SDK 便于移动 APP，WEB 进行链交互开发。

跨链适配

DCC 公链通过研发跨链适配器机制，兼容目前的主流主链，如 bitcoin、ethereum，来进行跨链的资产交换和支持数字资产的金融服务开展。

DCC 的公链研发也将在 github 进行开源，欢迎研发者参与到 DCC 公链的研发中来，Cyber Sheng Foundation 将提供开发者应对的 DCC 奖励。

9. 发展计划

2017 年 **8** 月	**DCC** 项目组成立
2017 年 **9** 月	基于以太坊测试网络构建统一身份标识系统
2017 年 **10** 月	搭建底层测试联盟链
2017 年 **12** 月	基于底层测试链部署上线信用声明合约
2018 年 **2** 月	代币互换
2018 年 **3** 月	推出首个基于 DCC 系统的借贷 Dapp
2018 年 **4** 月	上线 DCC 开放平台
2018 年 **5** 月	对接超过 5 家借贷、数据提供、风控机构
2018 年下半年	开放 DCC 系统的自主加入 API
2018 年下半年	建立 DCC 的统一 MPC
2018 年底	进入印尼借贷市场
2019 年上半年	进入越南借贷市场和更多东南亚市场
2020 年	进化平台到公链体系
2020 年	基于公链开发 AssetManage 系统 开发 Settlement 系统

10.

10. Cyber Sheng Foundation

Cyber Sheng Foundation 是一个在新加坡成立的非盈利性组织。基金会致力于在 DCC 生态建设的第一阶段维护整个生态的健康成长，在生态进入到公有链阶段，基金会开始逐步退出生态维护，维护权移交给公有链治理架构治理。基金会在维护生态过程中不获得任何生态收益，不从 DCC 生态中获取任何收益。

Cyber Sheng Foundation 组成由 DCC 初创团队、核心合作伙伴、早期投资人共同组成（如参与方为机构则由机构指派人员），负责 DCC 生态的日常运营。DCC 的决策权重由组成成员只有的 DCC 多少决定，每年排名在 DCC 持有榜最高的 30 个主体有权申请加入基金会由原基金会成员 50%以上同意后加入，原基金会成员如持有 DCC 份额不在最高的 30 个主体中则必须退出基金会。基金会成员不少于 3 人，不多余 7 人。

基金会在 DCC 初创中持有的 DCC，在经过基金会成员投票决策后可用于支付技术团队激励、增加生态奖励、开拓服务机构等有利于生态的用途，此用途需要被审计机构出具审计报告。

核心团队

Stewie Zhu

DCC 创始人兼 CEO，既是成功创办多家互联网和金融科技公司的企业家，同时也是一位资深学者，拥有多个全球最具声望学府的高等学位。创立 DCC 之前，Stewie 曾担任同牛科技 CEO，带领团队将其一手打造成中国领先的消费金融 SaaS 系统服务商，所开发的互联网信贷系统服务于 10 余家信托公司，每年帮助信托公司发放的贷款额超过数十亿美元。

南京大学电子工程学士学位，统计学硕士学位

耶鲁大学金融经济学硕士

牛津大学博士（候选人），伦敦政治经济学院金融系

研究侧重于金融和博弈论

Vanessa Cao

拥有在红杉资本（Sequoia Capital）工作的多年经验，关注金融科技行业的早期项目。

凯思博投资管理公司（KEYWISE CAPITAL）董事。

美桥投资集团（Bridge Capital ）合伙人，负责中国 A 股上市公司的并购事宜（主要是科技金融公司）。

清华大学，工商管理硕士，注册金融分析师 。

Vanessa 主要关注 DCC 项目的生态系统发展。

Daniel Lu

美国耶鲁大学数学博士；金融工程博士后，主要在德国莱比锡大学研究表象理论

大型商业银行投资银行和资产管理负责人，财务部总经理

国内外多年金融机构工作经验，先后就职于德意志银行总部以及一家股份制银行总部财务部。

具有扎实的专业知识和研究能力，曾受邀在国内外学术会议和金融会议上做主题演讲。专门研究资本和资本市场业务，资产管理，银行资产和负债管理，内部资金转移定价，产品定价，市场风险管理和建模，金融衍生产品定价，以及投资银行/商业银行中的巴塞尔新资本协议。

Daniel 主要负责 DCC 项目金融产品创新和设计。

Stone Shi

摩根大通量化研究副总裁，专注于衍生产品定价和定量模型风险

计算机科学与应用数学专业电信工程师

南京大学电子科学与工程专业

Stone 主要负责 DCC 项目的技术和研发

顾问

陈宇

网名“江南愤青”

聚秀资本合伙人；著名天使投资人；投资近 200 家互联网公司

中国金融领域畅销书《支付革命》和《风吹江南之互联网金融》作者

连续五年入选“中国互联网金融人物 50 强”

2016 年和 2017 年获胡润新金融年度风云人物

郭宇航

星合资本董事长，点融网创始人兼联席董事长

曾是沪上知名律师事务所的管理合伙人，具有十余年律师从业经验。2012 年成立点融网，3 年打造成独角兽企业

2016 年成立星合资本，专注金融科技早期投资

曾荣膺新华社与上海权威金融监管机构评比的“2015 年沪上金融行业领袖”和“2015 上海十大互联网创业家”等称号

姚明

中诚信征信副总裁兼首席技术官

早年就职于贝尔实验室（Bell Labs），后从业于移动互联网和金融行业，在大数据技术领域具有丰富的经验，并长期致力于探究金融大数据技术的创新与应用

2014 年加入中诚信征信，帮助公司完成了个人征信牌照准备工作，筹建了万象信用互联网大数据征信平台。领导团队自主研发了大数据反欺诈、大数据信用评估等多项核心技术并取得成功应用，成为国内最早一批践行大数据征信之路的人员之一，并被多家大型银行聘为外部技术专家

2016 年以来专注于金融领域区块链、机器学习和人工智能等技术的应用和创新，致力于推动智能信用评估

陈志武

前耶鲁大学金融经济学教授（1999-2017），现任香港大学亚洲环球研究所所长，香港大学经济及工商管理学院冯国经冯国纶基金教授（经济学）。兼任北京大学经济学院特聘教授。

中国证监会国际顾问，中国民生投资公司全球咨询委员会委员，IDG 能源投资集团有限公司、交通银行和诺亚财富独立董事。陈教授曾任耶鲁大学雅礼协会理事，北京市十二五及十三五规划专家咨询委员会委员，中央电视台纪录片《华尔街》和《货币》学术总指导。陈教授于 2007 年中国投资有限责任公司（CIC）创建之时，曾担任筹备专家小组成员；于 2011 至 2017 年间出任中国石油股份公司独立董事；于 2007 至 2015

年间出任诺德基金管理有限公司独立董事；于 2011 至 2012 年担任世纪佳缘网独立董事；于 2002 至 2005 年担任中国 Eagle 证券董事。

斑马资本管理（Zebra Capital Management）基金管理公司创始人

2012 年，全球咨询公司 Burson-Marsteller 在其 “G20 Influencer Report”（G20 国家最具影响力人物报告）中将陈教授列为“中国最具影响力的十人”之一。

研究获奖包括格雷厄姆•都德奖（2013）、Pacesetter 研究奖（1999）、默顿•米勒研究奖（1994）和芝加哥期权交易所研究奖（1994）。陈教授的著作《金融的逻辑》曾获 23 项最佳年度图书奖。

1983 年获中南工业大学计算机科学学士学位，1986 年获国防科技大学管理学硕士学位，1990 年获耶鲁大学金融经济学博士学位。

曹辉宁

著名金融经济学家，现任长江商学院金融学教授，金融 MBA 学术主任

金融俱乐部成员，加州大学伯克利分校、北卡罗来纳大学 Chapel Hill 分校前教授

发表过多篇论文，被《金融期刊》、《金融研究评论》和《金融经济学期刊》等国际知名期刊广泛引用

1998 年和 2000 年两次获得《金融期刊》最佳论文提名；获北方金融协会评选的新兴市场领域最佳论文奖；获西方金融协会评选的最有投资价值最佳论文奖；在 2004 中国金融国际年会上获得最佳论文三等奖

《经济与金融年刊》编委会成员，《国际金融评论》和《中国金融评论》主编

Matthew Chang

Matthew Chang 现任 KKR 私募股权投资中国团队董事总经理，此前曾担任 KKR 凯普斯通中国区负责人。Chang 先生在中国大陆、欧洲和北美等众多公司（例如初创企业、跨国公司和专业服务公司）拥有超过 20 年的工作经验。

在加入 KKR 凯普斯通之前，Chang 先生曾在罗兰·贝格国际管理咨询公司（RolandBerger Strategy Consultants）担任全球高级合伙人，主要负责亚洲地区的业务和重组业务。

在早期职业生涯中，Chang 先生曾担任艾睿铂公司（Alix Partners）中国区总经理，麦肯锡公司（McKinsey Company）副董事，以及帝亚吉欧公司（Diageo PLC）亚洲战略总监。

Chang 先生拥有瑞士国际管理发展学院（IMD International）工商管理学硕士学位，以及寇伊学院（Coe College）和纽约州立大学（State University of New York）数学与物理学学士学位。

合作伙伴

同牛科技

同牛科技是中国领先的 SaaS 金融科技公司，致力于向信托、银行和小额贷款公司等持牌金融机构提供消费者融资 SaaS 系统服务。同牛科技在中国信托业市场份额中排名第一。在建立 DCC 分布式信贷链的过程中，同牛科技将为历史积累的数据提供历史信用数据应用支持。

矩阵元

矩阵元是全球分布式账本技术的领导厂商，致力于在数字化时代提供分布式数据交换及协同计算服务，为数据的流动提供全方位的治理服务，让数据交换与协同更加简单、安全、高效。

矩阵元基于完全自主开发的数据交换基础设施技术平台，集成了分布式账本、安全多方计算、可插拔密码学框架、面向未来的密码学算法与协议，以及适配软硬件一体的解决方案。矩阵元为金融、交通、物流、航空服务、智能制造、物联网、健康医疗等领域提供基础技术平台级服务，并与全球领先的云平台全面合作，为面向分布式的行业应用提供完备的解决方案。

作为 DCC 联盟链阶段中的重要技术服务提供商，矩阵元将在联盟链的构建阶段提供全面的技术支持。

Deepfin

Deepfin 是基于区块链的去中心化资产证券化平台。在 Deepfin 中，不同链上的数字资产（例如版权、文章、流量等）持有人都可以轻松地完成资产抵押与募资，通过量化分析工具和服务对于不同链上的不同资产进行定价，打通不同链上的数字资产，让不同社区中有融资需求的用户均可轻松地通过自己持有的数字资产获得融资。利用区块

链技术对传统 ABS 业务进行改造，低成本高效率地完成资产确权、数据验证等真实性验证工作。

WXY

WXY 是高价值数字项目的一站式全球营销和商业咨询服务平台，总部位于新加坡，业务涵盖品牌名称、媒体推广、全球流量访问、商业咨询、资本对接等。WXY 由前奥美高管、前氪市场副总裁、前花旗集团营销和金融投资银行高管、媒体和基金等核心资源组成，是当今货币市场中最正式和专业的营销平台。

投资人

BTX Capital

BTX Capital 是一家专注于区块链行业的全球加密货币基金。BTX 通过技术咨询、投资和资源对接，不断推动有价值的互联网组织采用区块链技术，促进区块链价值的认识和实现。与传统的风险投资股权投资或其他纯数字货币基金不同，BTX Capital 专注于不同场景下的复杂互联网平台。BTX 通过帮助他们将区块链应用于商业，寻求重塑商业生态系统，改善生态合作环境，扩大实体经济，促进技术进步，用区块链技术振兴互联网产业。

核心团队包括红杉资深投资人、上市公司高管，以及耶鲁大学、牛津大学、伦敦政治经济学院等大学金融学博士。BTX 得到了许多金融机构资深高管以及顶级金融机构背

后项目来源的支持，并与硅谷和欧洲的大学展开深入技术合作，为项目合作伙伴提供专业人才支持。

胡森

创业家，前 Google 员工

中国科学技术大学计算机系学士，获郭沫若奖学金；耶鲁大学计算机系硕士；读博期间创办并经营风云广播和章鱼 TV；2015 年，章鱼 TV 被乐视收购。

因创立云成互动的杰出成就，2014 年入选福布斯“中国 30 位 30 岁以下创业者”，2016 年入选福布斯“亚洲 30 位 30 岁以下创业者”

Zhao Zimai

Telegram-Ton 基石投资者

区块链实验室 MathTrust 联合创始人

MathTrust 是由多家世界知名大学共同建立的实验室，专注于对区块链共识机制的理论、逻辑和实践进行研究和实验。MathTrust 提出的最新理论模型——区块链是智能合约序列链。其共识机制研究所涵盖的主题包括但不限于智能合约担保、节点生态相关漏洞识别以及基于节点的安全解决方案。

AbilityChain 联合创始人

AbilityChain 是一个基于区块链的全球教育底层应用平台。AbilityChain 是基于全球开发者社区共同建立的公共链，由 MathTrust 发起，AbilityChain 及其股东均为非营利组织。

飞跃教育创始人

飞跃教育是中国第一所面向基础教育的双语教育机构。飞跃教育采用其完全自主研发的基于理解的教学法和核心课程。

Risk Statement

Disclaimer

This document is for informational purposes only and is for reference only. It does not constitute advice, invitation, or solicitation of any investment in the sale of stocks or securities in the personal digital currency and its related companies. Such invitations must be

made in the form of a confidential memorandum, subject to relevant securities laws and other laws. The contents of this document may not be construed as compelling any participation in the exchange. Nothing in this white paper may be considered as participation in the exchange, including the requirement to obtain a copy of this white paper or to share this white paper with others. Participating in the exchange means that the participants fulfill appropriate age criteria and possess full capacity for civil conduct. Contracts with DCC are real and effective. All participants voluntarily sign such contract and possess the clear and necessary understanding of individual currency before signing such contracts.

The team will continue to make reasonable attempts to ensure that the information in this white paper is true and accurate. During the development, the platform may be updated, including but not limited to platform mechanisms, tokens and their mechanisms, and token distribution methods. Portions of this document may be adjusted in the new white paper as the project progresses, and the team will release updates by posting a notice or a new white paper on the site. Please be sure to obtain the latest white papers, and make timely adjustments to your decisions based on such updates. The DCC team expressly disclaims all liabilities to participants for any loss resulting from (i) reliance on the contents of this document, (ii) inaccuracies of the information in this document, and (iii) any actions caused by this document. The team will spare no efforts to achieve the goals mentioned in the document, but due to force majeure, the team cannot fully promise to fulfill such promises.

DCC is an important tool for platform performance but not an investment product. Owning DCC does not confer any ownership, control, or decision-making rights over the DCC Platform. DCC, as a digitally encrypted currency, does not fall into one of the following categories: (a) currency of any kind; (b) security; (c) equity interests in legal entities; (d) stocks, bonds, notes, warrants, certificates or other grant, or any instrument granting any right. The value added of personal DCC depends on the laws of the market and the application requirements after implementation, which may not have any value, and the team does not promise any value creation, and is not responsible for the consequences of any increase or decrease in value. To the extent permitted by law, for the damages and risks including, but not limited to, direct or indirect damages, loss of business profit, loss of business information, or any other economic damages arising from interests in connection with the particular purpose, the team takes no responsibility. The DCC Platform will comply with any regulatory regulations conducive to the development of the credit industry and industry self-declaration. Participants and their representatives will fully accept and abide by any such inspections. At the same time, all information disclosed by participants to accomplish such inspections must be complete and accurate. The DCC Platform has clearly communicated possible risks to participants. Once participants engage in the exchange, they

confirm and acknowledge the terms said conditions and rules, accept the potential risks of this platform, and agree to bear the consequences.

Risk Warning

There are a variety of risks involved in the DCC ecosystem, which require participants to carefully assess and be aware that such risks are borne by themselves:

Policy Risks: At present, the regulatory policies for the blockchain project and financing of the exchange are still unclear, so there is a possibility of participants suffering losses due to policy reasons. For the market risk, if the overall value of the digital assets market is assessed at a high value, then the risk of investment will increase, and participants may be subjected to overly optimistic valuation estimates, which may not be realized.

Regulatory Risks: Digital asset transactions, including personal digital currencies, are highly uncertain. As there is currently no strong regulatory regime in digital asset trading, there is a risk that e-tokens will skyrocket and be subjected to market manipulation by bankers. If individual participants lack experience after entering the market, it may be hard to resist the asset shock and psychological pressure brought about by market instability. Although academics, the government, media and so forth have suggested cautions from time to time, no official written supervisory methods and provisions have been released. Therefore, it is difficult to effectively circumvent such risks. It is undeniable that in the foreseeable future, official regulations will be introduced to constrain the blockchain and electronic token markets. If competent entities regulate the sector, the tokens purchased during the swap may be affected, including but not limited to fluctuations or limits in price and marketability.

Team Risks: The current blockchain technology team is engaged in many projects. Market competition and project operating pressures are strong. Whether the DCC project can stand out among those projects and be well-acknowledged depends on the team’s own capabilities, vision, planning and other aspects, and also on competitors in the market and even oligarchs. During this process there exists the possibility of vicious competition. Based on the contacts accumulated by the founders for many years, DCC brings together a team with both vitality and strength, one which has attracted experienced practitioners in the blockchain industry and experienced technical developers. The stability and cohesion within the team are crucial to the overall development of this personal currency. In the future, we do not rule out the possibility of core personnel leaving or conflicts within the team, which will negatively affect the overall project.

Coordination Risks: The founding team will spare no efforts to achieve the development goals set out in the white paper, and to extend the project. However, given the unforeseen factors in the industry development trends, the current business model and the overall plan may not cohere with market demands, resulting in unmanageable earnings. Also, since this white paper may be adjusted as the details of the project are updated, if the updated details of

the project are not readily available to exchange participants or the public is not aware of the latest progress, information asymmetry will result, affecting follow-up development.

Technical Risks: First, this project is based on a cryptographic algorithm. The rapid development of cryptography will inevitably bring about the risk of cracking. Second, where technical support such as blockchain, distributed ledger, decentralization, tamper-proof records, and other such core technologies sustain the business development of the project, the team cannot fully guarantee complete implementation. Third, during the project update, you may discover that loopholes exist, which may be fixed by releasing patch, but we cannot fully guarantee that no impact will be caused by such vulnerabilities.

Security Risks: In security, the number of individual supporters is small, but the total number of users is huge. This also places high requirements on project security. Electronic tokens are anonymous and difficult to trace, so they can be easily used by criminals and hackers, or may be used in transferring illegal assets.

Current Unknown Risks: As blockchain technology and the overall industry continue to evolve, the DCC project may face unforeseen risks. Before participants make decisions, we invite them to fully investigate and understand our team’s background, gaining a full understanding of the project and its framework and goals, and reasonably adjust their own vision to rationally participate in the exchange of tokens.