AdvancedCreditChain — 加密征信系统白皮书

2017 年 2 月

“我们的论点并不是简单的循环逻辑，其背后有着独到之处。”

—Willard van Orman Qui

Content

摘要

本白皮书向您介绍 AdvancedCreditChain(ACDC),一个通用的加密征信系统。

商业方面，ACDC 着眼于东南亚及非洲等较不发达地区，旨在为中小企业出征打下牢固基础。技术方面，ACDC 的最大优势是可以吸收任何一种基于区块链的征信系统好的方面，其将常规区块链上的各种操作以单纯的功能模块的方式实现。通过网络壳(Shell)利用这些操作处理网络层任务。

更重要的是，ACDC 支持元数据升级:即可以通过自我修正代码进化协议。为此，ACDC 从一个种子协议开始定义一整套流程来让持币的用户来对代码进行修正，以及修正这套流程所必须的投票体系本身。这和哲学家 PeterSuber 的 Nomic[3]博弈观点不谋而和，该观点的博弈构建主要围绕一整套内省规则。

除此之外，ACDC 的种子协议被放在一个纯粹的股权证明系统(POS)上，支持图灵完备的智能合约。ACDC 通过 OCaml 语言进行实现，该语言是一套功能强大的函数式编程语言，提供高速，非歧义语义和语法以及整个生态系统。所有的这一切让 ACDC 成为一个形式化正确性证明的很好的候选者。

以下的白皮书要求读者要对比特币协议的一定程度的了解并已理解基本的加密学知识。

1.传统企业征信

1.1 传统企业征信评估

随着各行各业规模日益发展壮大，行业内各企业规模飞速成长，透明化，规范化的征信系统已逐渐成为提升企业效率及效益的重要因素。使用征信系统的根本任务是要发现存在于现实中的信用风险形成规律并揭示信用风险，因此，必须把影响债务偿还能力的主客观因素

作为研究对象，分析不同债务主体信用风险形成因素的特殊性，研究其普遍性，这是形成评级原理的物质基础和思想源泉。信用风险形成因素是相互联系和交织的，我们要从联系的视角发现信用风险形成因素的内在逻辑和运动规律。信用风险形成因素的矛盾运动必定有主要因素和主要因素的主要方面起着决定性作用，以信用风险形成因素普遍联系为认识基础，发现主要风险因素及其地位与作用，能够使评级原理源于现实、高于现实、用于现实。正是运用辩证唯物主义思想方法使大公能够深入到极为复杂的信用风险体系内核，发现信用风险的形成机理。

传统的企业征信评估一般基于以下几方面：

(1) 企业的资金及财务状况

财务状况是指一定时期的企业经营活动体现在财务上的资金筹集与资金运用状况，它是企业-定期间内经济活动过程及其结果的综合反映。 企业财务状况是企业一定日期的资产及权益情况，是资金运动相对静止状态时的表现。 财务状况是用价值形态反映的企业经营活动的状况，通常通过资金平衡表、利润表及有关附表反映，是企业生产经营活动的成果在财务方面的反映。 在美国会计界，常常将资产负债表称为财务状况表（Statement of financial position）。在当前公认的资产负债表定义中，也常常认为资产负债表是反映企业某一特定时点财务状况的报表。显然，这里的"财务状况"指的是资产负债表状况，也就是指资产负债表所包括的所有内容。

(2) 经营状况

主要包括了经营信息，合同履约，缴税信息及员工的待遇保障。一般指现在劳动法所规定的劳动保障和社会保障。合同履约能力是企业诚信度最直接提现，税务信息也可看出诸如企业经营状况等诸多方面的信息。现在的福利待遇指企业为了保留和激励员工，采用的非现

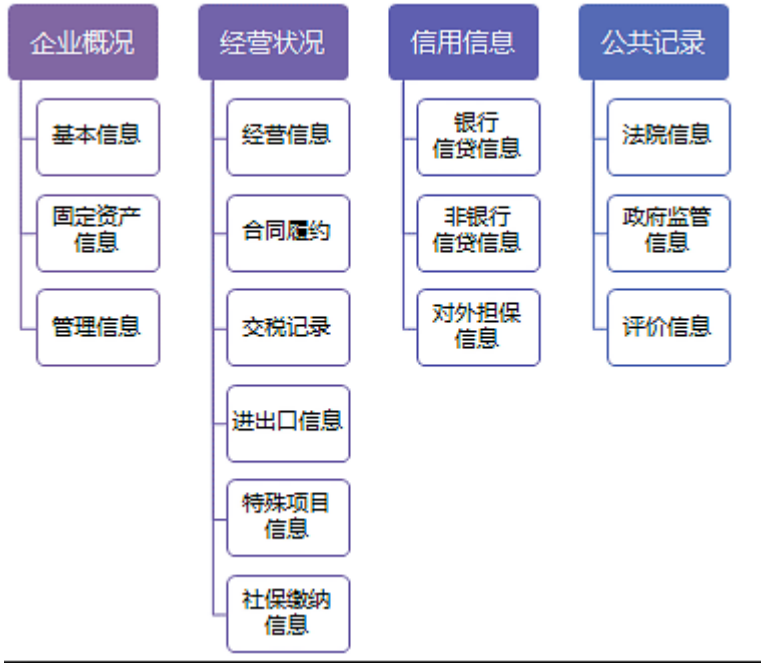
金形式的报酬，福利的形式包括保险、实物、股票期权、培训、带薪假等等，系统中列出的金额是从公司成本角度考虑的，折合成金额后进行展示的。

(3) 信用信息

主要是企业的借贷信息。企业借贷融资主要是指金融机构与非金融机构之间的资金融通活动，简称借贷融资，它是历史最悠久、使用最广泛的一种融资手段。借贷融资的形式很多，按照不同的分类标准分为很多种类。而对外担保则指我境内机构向境外机构或境内外资金融机构承诺，一旦债务人不能按约偿还债务时，将代为履行偿还义务。

(4) 公共记录

主要强调企业的合法合规性。 主要对企业和企业主的合同审查、法律事件处理等记录，合规审查要更为复杂。对于合规审查来说，除了需要面对静态的国家法律外，还要接受监管机构动态的严格监管。一着不慎，就有遭受法律制裁或监管处罚之虞，从而导致重大财务损失乃至声誉损失。合法合规会涉及环境保护问题、安全生产问题，甚至 9 月份的新《广告法》里都会存在合规问题，比如什么样的人可以作为企业代言人，范围越来越广；其次，在反商业贿赂过程中，企业要应对一系列的司法调查问题，对于没有任何司法权限的企业法务来说，调查工作会是一个很大的挑战；再者，从跨国公司到国企，以及民营企业中的金融企业，都有应对监管措施的需要。



而在企业征信审计调查阶段，调查者与企业之间往往也存在着一定程度上的问题。 首先，以上所述的企业合法合规审查，弹性很大。严格遵守企业与勉强合规企业，其实际执行过程中存在着非常大的差距。再者，审计当中很多信息不透明，使得审计机构本身的信用变得非常重要；最后审计材料的可信度也成为了审计中的一个难题。部分企业存在着弄虚作假，篡改记录等行为，如果这些行为不被发现，将直接影响评定结果。

1.2 传统征信业的痛点

目前，由于投资者与经营者之间存在着信息不对称，因此会形成两个问题：第一是逆向选择；第二是道德风险。解决这两个问题的一个有效办法就是信用评级。信用评级不但为资金供需双方的信息缺口开辟通道，使资本市场不至于收敛于因信息不对称而无法发挥资金中介的功能，使资金需求者能取得所需资金从事其各项牛产经营活动，使资金供给者的投资拥有适合其风险偏好的标的，也使金融机构的管理效率得到提高，从而增强了资本市场的整体

效率。然而，信用评级是否合理，评级结果是否准确， 很大程度上取决于评级方法的科学性。

而目前企业评级的主要障碍如下：

⑴企业信用评级尚未得到全社会的认可。目前我国经济正处于转型期，原有计划经济的观念和旧的习惯依然存在，有的还根深蒂固，一些人还停留于过去国家财政统配资金，不拿白不拿 ，甚至"赖债"、"逃债"得益的陈腐观念中。信用评级又起步较晚，近两三年来在部分省市开始， 也还是处于"点"的状况。目前企业，也包括政府对信用评级不了解，或知之甚少，或存有种种偏见， 尚处于十分艰难的推动阶段。

⑵法律依据不足。企业信用贫农国际行业管理与业务规则基本空白，法律责任条款也不完善。目前只有 1999 年 9 月发布的《中共中央关于国有企业改革和发展若干重大问题的决定》、《企业债券管理条例》，已经存在的中国人民银行《企业信用评级管理办法》等规章体制。中国人民银行的企业评级还停留在部门规章的层面上。贷款人的管理、评级过程及评级结果还未提出规范。信用评级的业务规则、从业人员的资质相应的法律责任等都都尚未纳入立法范围，理发层次较低，内容过于单薄，达不到强制性效果。

⑶信用评级的基本职能与社会"需求"存在差异，特别是市场推动之初矛盾尤均突出。信用评级是揭示市场风险的一种有效手段， 其基本职能是通过综合考察分析受评经济组织的信用状况，揭示风险，公开发布，为社会提供公众信息， 满足投资者和监管部门需求的中介服务， 其评级结果和质量，也就是第一位的经营目标，是投资者和监管都门对评级结果的使用和信任，为其提供决策参考。目前的状况是受评企业对级别期望值很高，大有"没有 AAA 不罢休"之势。究其原因，一是受评企业的错误认识；二是存在客观原因：目前全国评级业务没有全面铺开，走正门的反而成了"低级别"，一旦进入招投标市场，没有"高级别"无法入围，从而严重影响了企业的正常经营与发展。

(4)出介机构自身素质不高，尤其在"僧多粥少"的情况下，自律性更差，甚至提级压价，存在道德风险。

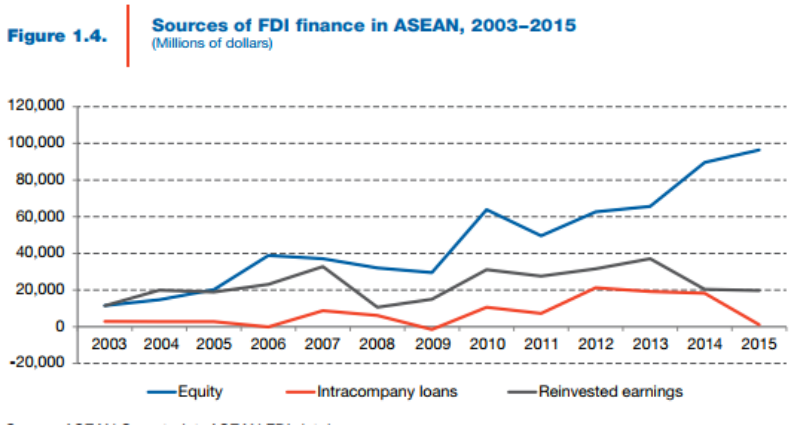
中国征信基数庞大，但数据缺乏共享，征信机构与用户信息不对称。征信机构与征信机构、征信机构与其他机构等缺乏有效的共享合作，信息孤岛问题严重，无法实现征信业内高质量的数据流通及交易，造成征信机构与用户信息不对称。征信机构间信息孤岛问题严重，金融业内信贷机构、消费金融公司、电商金融公司等机构的海量信用数据尚未没有发挥其应有的价值，金融业外信用信息割裂在法院、政府部门、电信运营商等机构手中。究其原因，主要是各国数据归属权尚未确立，处于隐私保护的顾虑，各机构宁愿握紧手中的数据画地为牢，没有额外的积极性进行数据交换共享。除体制机制原因外，传统征信业也由于技术架构的问题无法在各机构、行业间安全地共享数据，使得传统征信工作中数据孤岛障碍的问题迟迟得不到解决。

正规市场化数据采集渠道有限，数据源争夺战耗费大量成本。信用数据不同于其他行业数据，所属用户是最为重要的数据标签，涉及到企业和个人的切身利益，因而无法通过传统数据交易平台进行共享交换，导致正规市场化采集信用数据渠道极其有限。传统征信机构通过自挖、合作、购买等方式，主动对接相关的部门与机构，从有限的场景中整合数据，抢占征信业发展的高地与先机。因此关于数据源的竞争尤为激烈，这也直接使得传统征信机构在采集数据上耗费了大量成本，导致用于数据分析及征信产品研发的资金比例缩水，征信机构无法过多关注征信产品的质量，继而影响了征信机构的水平与信誉。

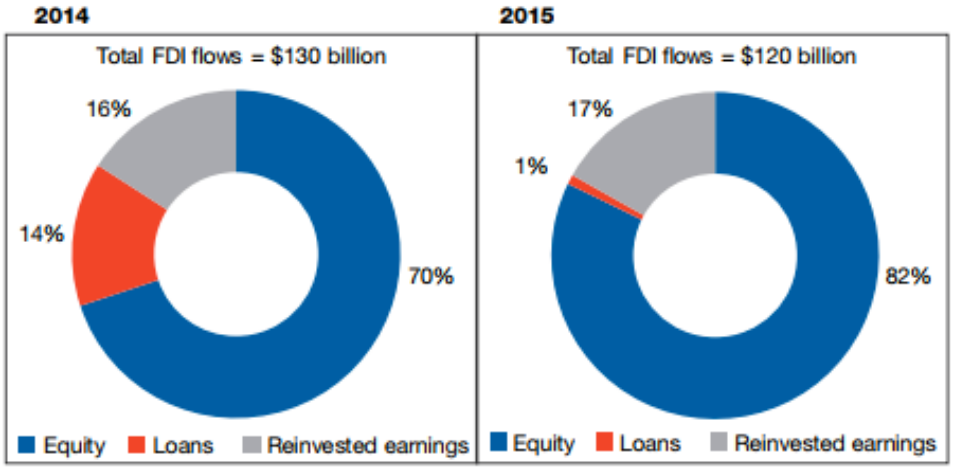
数据隐私保护问题突出，传统技术架构难以满足新要求。大数据时代下的征信业对隐私保护和数据安全的要求更高。央行对下发个人征信牌照非常谨慎，说明监管机构对于正式放开个人征信领域还存在疑虑，隐私信息保护、个人信用评价指标不统一等问题仍是央行最主要的担忧。此外，"暗网"中的个人信息交易灰色产业链，以其多样性、隐蔽性与复杂性成为

监管部门查处的痛点与难点。为此，中国人民银行征信管理局明确指示要加强隐私保护，要求征信机构采集使用用户信息应当经信息主体同意，并明确告知可能产生的影响等事项，信息主体有权要求征信机构将其纳入拒绝用于营销的范围内。然而，传统征信系统技术架构对用户的关注度较低，并没有从技术底层保证用户的数据主权，难以达到数据隐私保护的新要求。

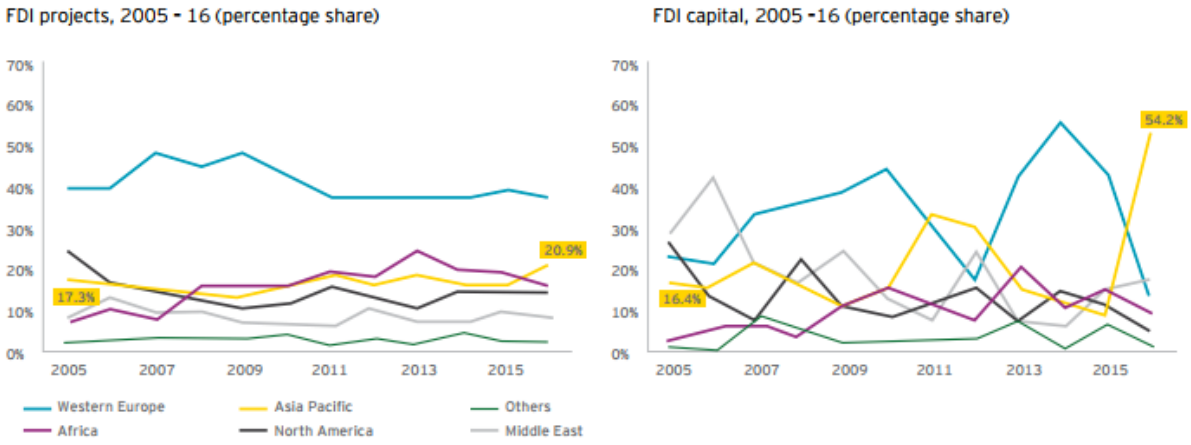
1.3 东南亚及非洲投资与征信概况



可以看到，东南亚市场吸引外资的能力也越来越强，有 5 个国家将在 2016 至 2018 年成为跨国企业的全球投资预期目的地。在这份全球首要投资目的地排行榜中，印尼、马来西亚和越南的排名升高，而菲律宾和缅甸首次入榜。2015 年，流入东南亚的外来直接投资（FDI）为 1260 亿美元，较上年增加 1%。



而东南亚投资的主要资金来源中，股份制占了绝大部分。这与东南亚国家的对外招商引资政策相关。与前几年相比，2015 年直接投资者在利用股权资本为东盟投资项目融资方面更为活跃。 相比之下，外国直接投资的公司内部贷款部分则从 2014 年的 14%大幅下降到 2015 年的 1%，导致外国直接投资流量下降 100 亿美元。 公司内部贷款（偿还贷款或向关联公司和母公司提供新贷款）的流出额大于东盟，特别是新加坡和泰国子公司的内部贷款流入量。公司内部贷款的部分外流支持了其他东盟成员国投资联属企业的融资。 在新加坡，公司内部贷款净流出到了东盟以外的目的地。



非洲投资者多元化的迹象是，2016 年亚太地区对非洲的投资创下了历史新高，占项目总数的五分之一以上，占资本投资的一半以上。来自亚太地区的公司也是向非洲直接投资工作的最大贡献者。近年来，中国和日本一直在与包括美国在内的其他西方国家竞争，在这个大陆上建立影响力。源于中国的对非洲的外商直接投资在 2016 年大幅增加。随着项目的跃升 106%，中国成为该大陆的第三大投资者。事实上，自非洲吸引力计划开始以来，这是所有三个指标（即项目，资本投资和就业）中来自中国的最高水平。中国近四分之一的 FDI 项目是针对埃及的。 2016 年 1 月，中国国家主席习近平访问埃及，埃及承诺向埃及国家银行贷款 7 亿美元。中国还计划在埃及的 15 个电力，基础设施和交通项目中投资 150 亿美元.8 在非洲，2016 年，中国投资者在 TMT，汽车和商业服务领域发挥了积极的作用。

在这两个地方，中资企业主要靠中国进出口银行及中信保担保，对方企业一般由国家进行直接担保。这导致在很多领域，只有大公司能够有能力进行输出，中小企业很难的到保障。其根本原因在于中小企业资源匮乏导致的信用评价低。而建立以套公开透明的征信系统来共享数据，能够非常是中小企业站到台上竞争，从而增大了其在当地成事的机会。

征信查询方面，不论中国、东南亚还是非洲，目前信贷机构所需的主要黑名单数据，来源于政府官方征信机构，银行和民间私营征信数据公司三种渠道。但通常情况下，一家信贷机构都需要对接多家黑名单数据供应商，对接流程复杂、成本高，并且要给相应的机构支付黑名单查询费用。且这些数据很大程度上成为一些公司的核心竞争力。 ACDC 看到了这种现象，就希望在未开化市场先入为主，将一套信用体系在很早期建立起来，这有利于提升整个区域的效率。

1.4 区块链征信的可行及必要性分析

传统数据中心，通常是将数据储存在一个中心节点上。这个中心节点完全由数据中心控制，数据中心可以随意的修改，删除这些数据。数据中心出于利益原因，完全可以出售假数据，篡改或者删除数据当前的数据。联盟的模式一般是多个小型数据中心依附于一个大型数据中心，小型数据中心和大型数据中心进行数据互换。这种模式小型数据中心之间无法互相信任，所有的数据经过大型数据中心交换。最终结果是，大型数据中心将所区块链是一种去中心化的分布式数据存储技术。它的核心价值是创造一个安全可信的体系，可以让互相不信任的机构或者个人。所以区块链技术的引入，将很好的解决上述问题中的一些痛点。首先，从企业层面来说，区块链能帮助我们确立自身的数据主权，生成自己的信用资产。这是个人信用生产的基础，也是我们将来的重要资产来源及保障，同时也有利于征信机构信用生产成本的降低。现在，除征信中心外，用户数据的所有权几乎全是是错配的，它们被掌握在各大互联网公司手中，所以我们难以控制自己的私人数据，更不用说作授权了。并且，这些大互联网公司各自垄断了一个市场，形成一个个相互封闭、隔绝的数据孤岛，从而征信数据难以充分地发挥其共享价值。

其次，受益于密码学的诸多成熟技术，对征信数据进行加密处理，或者直接采用双区块链链的设计来确保用户征信数据安全，确保征信数据在区块链上绝对安全。这样，个人征信数据直接可以在区块链上做安全交易，那么我们的交易数据将来可以完全存储在区块链上，成为我们个人的信用，所有产生的交易大数据将成为每个人产权清晰的信用资源。不止于此，区块链还在人与人之间公开透明地收集和共享数据。这样，就可以将散落在私有部门及公共部门的"全部"个人数据充分地聚合起来，取之于用户而用之于用户，促进数据的开放共享与社会的互联互通。

2. AdvancedCreditChain 产品概况

2.1 AdvancedCreditChain 业务简报

在 Advanced credit chain system（简称 ACDC 系统）中，各用户可将核心数据保存在自己的内部链上，将少量摘要集索引信息提供至 CreditChain 的公共区块链上。有查询请求的用户通过 ACDC 公共区块链转发到原始数据提供方（另一个用户）查询，这样各用户既可以查询到海量的资料，又不用担心泄露自己的商业数据。每一次查询都会被视为一次交易并向全链广播，ACDC 运用区块链不可篡改的特性构建了可行的技术框架基础。

- 不共享原始数据的情况下，做到多方数据共享，放大数据价值。
- 数据真实有效且无法被篡改。
- 参与者不是被动的提供数据，而是主动参与。
- 被查询公司可获得部分收益。
- 提供的数据越新越有价值。
- 提供信用调查与风险防范的数据支撑。

2.2 AdvancedCreditChain 征信系统功能简介

2.2.1 统一的数据共享注册规则

使用更加直接的合作形式收集所需的数据、对必要的数据包和分类与标签达成一致、准备联合提交的数据常常是更为实际的做法。这可能会涉及所有现成可用数据（包括公开可得

的数据）的联合审核。这种更完全的交流方式使得参与者们能够决定分类与数据并达成一致。因此，ACDC 在现有信息（包括公开可得数据）和数据需求的确认、新信息的生成、联合注册等方面同步进行工作。

2.2.2 区块链公钥加密保证数据可靠性

公开密钥加密（Public-key cryptography），也称为非对称加密（英语：asymmetric cryptography），是密码学的一种算法，它需要两个密钥，一个是公开密钥，另一个是私有密钥；一个用作加密的时候，另一个则用作解密。使用其中一个密钥把明文加密后所得的密文，只能用相对应的另一个密钥才能解密得到原本的明文；甚至连最初用来加密的密钥也不能用作解密。使用此技术应用于区块链，可以进一步保障数据本身的安全。

2.2.3 无偿提供数据查询

在系统数据库建立起来之后，任何机构及第三方企业可以选择对他人进行查询请求。在系统内查询任何数据都是无偿的，这意味着任何参与的机构及企业可以看到完整、公开、透明的企业信用数据。

2.2.4 共享的数据广播

在 ACDC 内部，每一次交易（修改）均广播全链，确保数据不可篡改。广播基于现有的区块链模型，使用分布式账本存储。针对点对点之间广播传输进行优化，且在传播策略上对信息量及频率进行权衡。

2.2.5 通过黑名单系统甄别共享数据真实性

建立黑名单机制，在全链公开失信人信息。黑名单失信数据分为公开数据、详细信息两部分。公开数据为数据当中的部分详细信息。可以类比法院系统发布失信人"老赖"名单，是一种有效监督并规范企业信用体系的方式。

2.2.6 引入整套成熟的信用评价体系

ACDC 引入专业的信用评价团队以及完整的信用评价体系。针对本产品特定的商业模型进行定制与优化。着重突出征信系统中影响权值较大的部分，对繁杂而低效的评估内容及体系方法进行直接的删除。在确保效率的同时也保证了数据的准确性。

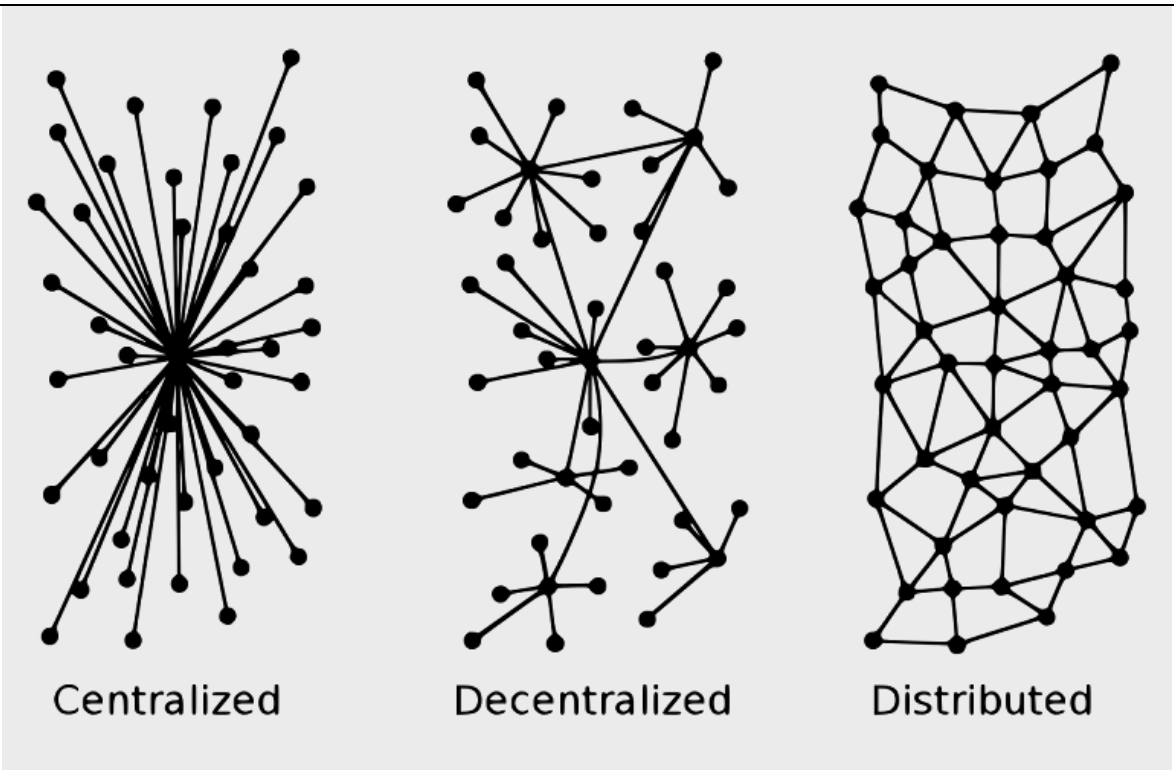
2.3 AdvancedCreditChain 征信系统技术特性

- 去中心化：原始数据单点存储，摘要信息区块链账本共享。
- 币天销毁：币天销毁等于每笔交易的金额（币）乘以这笔交易距上一次交易所积累的时间（天）。
- 数据交易授权。 建立起一套完整公平的数据交易授权模型。
- 智能合约：提出独有的全新智能合约模型。
- 公钥加密：加密数据提交副本到区块链，确保数据无法被篡改。
- 私钥解密：用户通过私钥授权查询操作。
- 不可更改：每一次查询及更新均视为一次不可逆的交易，交易广播至全链。
- 有偿服务：查询用户需要支出，被查询用户获得收入。
- 准确机制：提供保证金机制提升数据准确性。

- 仲裁机制：当出现异议时启动仲裁程序。
- 开放式接口（API）:主要数据查询接口全部对外开放，使系统更加方便快捷的被应用到其他社交、信息平台。

3.去中心化

传统数据中心联盟的模式一般是多个小型数据中心依附于一个大型数据中心，小型数据中心和大型数据中心进行数据互换。这种模式小型数据中心之间无法互相信任，所有的数据经过大型数据中心交换。最终结果是，大型数据中心将所区块链是一种去中心化的分布式数据存储技术。它的核心价值是创造一个安全可信的体系，可以让互相不信任的机构或者个人，在没有权威中心机构统筹下，还能彼此信任地进行信息和数据的交互。同时区块链通过密码学、分布式一致性协议、共识协议、点对点网络通讯等技术手段，实现了数据不可篡改性和不可删除。 去中心化"是一种现象或结构，其只能出现在拥有众多用户或众多节点的系统中，每个用户都可连接并影响其他节点。通俗地讲，就是每个人都是中心，每个人都可以连接并影响其他节点，这种扁平化、开源化、平等化的现象或结构，称之为"去中心化"。



同时"去中心化"是区块链的典型特征之一，其使用分布式储存与算力，整个网络节点的权利与义务相同，系统中数据本质为全网节点共同维护，从而区块链不再依靠于中央处理节点，实现数据的分布式存储、记录与更新。而每个区块链都遵循统一规则，该规则基于密码算法而不是信用证书，且数据更新过程都需用户批准，由此奠定区块链不需要中介与信任机构

区块链所解决的都是一个核心的问题，即信任问题，来自多方的数据，比如供应链金融的货押业务，就会涉及金融机构、企业、仓储、服务提供方、仓储监管方等五方，包括企业那边可能还有买方和卖方，在这当中获取数据和数据之间的来回确认相对会比较麻烦，由于他们各自都有信息记录的方式，所以五方一起去对账非常繁琐。

产业之间本身也有上下游的关系，比如原材料和化工，和日化品的品牌商、汽车的主机厂和汽车零配件的产业就是一个上下游，这也会有相关的纵向的协同。更好的方式是大家各自都往区块链记载分布式的账本，大家最终又有一个能够达成的共识，所以，区块链解决的就是供应链金融在非信任的体制下怎么达成一个信任关系。

传统的供应链金融因为存在着核心企业沟通，操作成本高昂，贷后管理复杂等等一系列问题，结果就是花费很大精力却无法产生合理收益，金融科技的发展将真正改变传统供应链金融，不只是简单在线化，而是通过交易征信、大数据和区块链等技术推动供应链金融更加自动化和智能化，为实体经济创造更大价值。

区块链上的征信只基于直接的数据本身，即交易数据，而不需要综合不同维度的信息。因为区块链的交易带有时间箭头，重复消费的边际成本不再等于零，而是正比于币天销毁。

4. 币天销毁

币天销毁（Coin Days Destroyed）是区块链的一个非常重要的概念，顾名思义，币天销毁等于每笔交易的金额（币）乘以这笔交易距上一次交易所积累的时间（天），比如用户花了一笔 100 天以前收到的 10 数字货币，这笔交易的币天销毁就是 1000 币天。

将币天销毁作为区块链交易的信用评价权重因子，既可防止刷客在两个账户之间反复转账以刷信用，又可以防止差评师进行大量小额交易以恶意差评。这是因为在一次交易中，销毁的币天越多，则信用评价的权重越高。当刷客试图给用两个账户反复交易而刷好评时，第一次交易的评价是有效的，但历史上累积的币天在交易完成之时便已销毁，当进行第二笔交易时，由于发生在第一次交易后不久，币天积累非常之小，相应地，对信用评价的贡献微乎其微，其后所有交易的币天销毁之和同样也非常之小，用户利用同一笔钱反复给自己刷好评，不管进行多少次，其最终效果与第一笔交易所带来的信用评价几乎一样。同样，将差评师试图通过大量小额交易对用户以恶意差评时，由于信用评价正比于币天销毁，由于交易的额度太小，同样也几乎不能对用户的信用造成影响。

4.1 传统信用评价模型（累加模型）

累加模型系指在原有的信用积分基础上直接进行加减，其模型表示如下：

$$R_n = R_{n\text{-}1} + r_n$$

$$r_n \in \{\text{-}1,0,1\}$$

其中：Rn、Rn-1 分别表示用户截止到第 n、n-1 次交易之后所获得的信用得分，

$$r_n \in \{\text{-}1,0,1\}$$

表示{差评，中评，好评}，即当获得"差评"时在原来信用积分的基础上加上"-1"分，当用户获得中评是就在原来信用积分的基础上加"0"分，当用户获得好评时在原来信用积分的基础上加"+1"分。此评价模型能够较直观的呈现出交易者的信用积分并且操作起来也较为方便简单，在一定范围内为交易双方提供了信用参考。但是由于没有考虑到交易金额大小，导致用户刷信用行为泛滥，同时由于没有考虑区块链时间戳等其他因素，使得交易的边际成本接近于零，刷客可以在短时间内制造大量虚假交易，使得诚实交易者不能在一个公平的交易环境中竞争。由于刷信用、刷差评这两种行为模式的普遍存在，此模型很难反映区块链交易者的真实信用值。

4.2 基于币天销毁的权值模型

权值模型系指用用户所得的信用评价得分乘以该次交易的币天销毁再获得用户的最后信用值，其模型如下：

$$R_n = \sum_{i=1}^{i=n} R_i * W_i$$

$$W_i = C_i * D_i$$

$$R_i \in \{-1,0,1\}$$

$$i, W_i, C_i, D_i \in (0, +\infty)$$

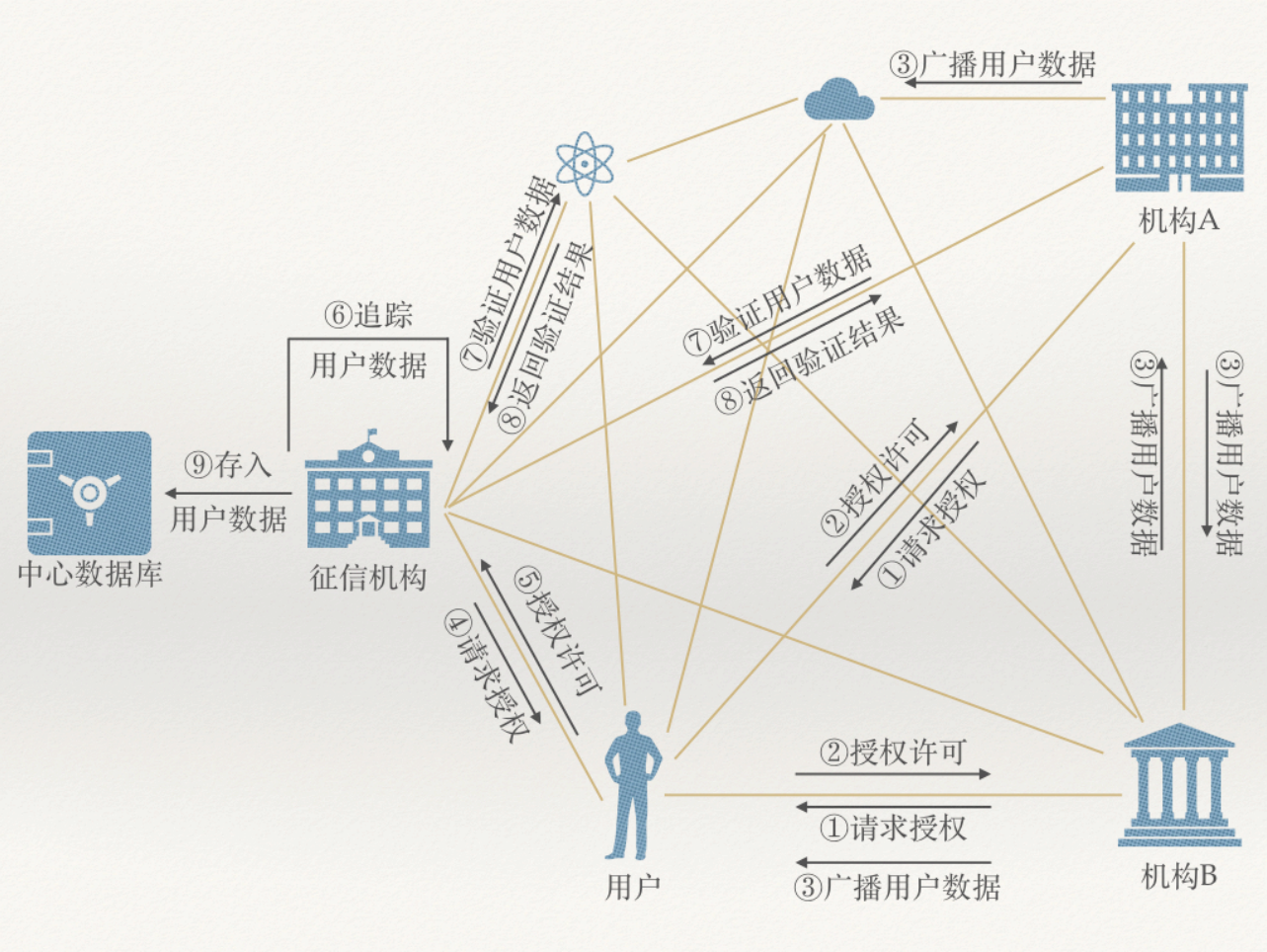
Rn 代表用户的信用值得分，Ri 为第 i 次交易时用户所得的信用值，Wi 为第 i 次交易时的币天销毁，Ci 为第 i 次交易时的金额，Di 为第 i 次交易距离上一次交易所积累的时间。

这里我们规定把币天销毁作为信用评价因子，在一次信用记录中，销毁的币天越多，则信用评价的权重越高。当刷客试图给用两个账户反复交易而刷"好评"时，第一次交易的评价是有效的，但历史上累积的币天在交易完成之时便已销毁，当进行第二笔交易时，由于发生在第一次交易后不久，币天积累非常之小，相应地，对信用评价的贡献微乎其微，其后所有交易的币天销毁之和同样也非常之小，用户利用同一笔钱反复给自己刷好评，不管进行多少次，其最终效果与第一笔交易所带来的信用评价几乎一样。同样，将差评师试图通过大量小额交易对用户以恶意差评时，由于信用评价正比于币天销毁，由于交易的额度太小，同样也几乎不能对用户的信用造成影响。

在现实的信用体系认知中，人们过去总是把信用当成一个道德问题，试图从道德层面约束交易行为，淘宝们设计了极其复杂的信用体系，试图区分真实的交易行为与作弊交易行为，并通过大数据分析，结合用户的社会关系、职业、收入甚至公共事业缴费单，来评价一个人的信用高低。

然而在区块链的信用评价中，信用其实是一个数学问题，在刚才的例子中我们看到，用户的交易行为不再被区分为作弊交易与真实交易，所有的交易行为一视同仁，通过数学赋予交易以成本（币天销毁），便可以使信用评价结果准确地反映用户的真实信用。作弊是允许的，但即使你作弊，也不会对任何人的信用产生影响。

5. 征信数据交易授权介绍



①其他机构 A、B 向用户请求授权，②经过用户授权许可后，③将各个环节关于用户的数据进行广播添加到区块链中，在链上显示的这些数据只有用户的地址属性，并不会泄露用户隐私。④征信机构向用户请求授权，⑤经用户授权许可后，在自身节点中对这些数据进行追踪，获知用户过往的贷款记录、还款记录、逾期记录、当下大致的债务情况等数据。⑦⑧征信机构在区块链中验证得到数据的真实性，⑨存入中心数据库，继而对其信用状况进行分析判断。

在该模型中，机构及用户（企业）都最大限度的参与到了评价之中。该模式主要特点有二：良好的加权及多元的验证。在该模型中，不同的机构及企业得到了很好的加权，极大的

弱化了"头部效应"造成的信用体系失衡，实现了"强者不霸道，弱者不畏缩"的授权及验证模型。并且该模型中信用数据是可以多源交叉验证的。可以看到任一方数据的发出都会经过第三甚至四方的验证及授权，因此数据真实性有所保证，且无法被企业或者个人篡改。

6 智能合约

6.1 合约类型

和比特币的 unspent 输出不同，CreditChain 使用有状态的账户。当这些账户规定了可被执行的代码时，它们也就成了广泛意义上的合约。征信系统本身也是一种合约，只是没有可执行的代码。

每一个合约都有一个管理者，对于账户而言，这个管理者就是它的拥有者。如果这个合约标识为可以被花费的，那也意味着管理者可以花费与这个合约相关联的资金。此外，每一个合约都可能会规定一个公钥的哈希用来签署或者挖 POS 协议内的区块。私钥可由或不由管理者控制。

一个合约可以正式表示为:

```
type contract = {counter: int; (* counter to prevent repeat attacks *)
manager: id; (* hash of the contract's manager public key *) balance: Int64.t; (* balance held *)
signer: id option; (* id of the signer *)
code: opcode list; (* contract code as a list of opcodes *) storage: data list; (* storage of the contract *)
spendable: bool; (* may the money be spent by the manager? *) delegatable: bool; (* may the manager change the signing key? *)
}
```

一个合约的句柄是初始内容的哈希值。试图创建的合约的哈希不能与已经存在的相同，否则将不会被包含在一个有效区块内。

该数据表示为一个 union 类型。

```
type data =
| STRING of string | INT of int
```

这里 INT 是一个有符号的 64 位整数，string 是一个 1024 字节的数组。存储空间上限为 16384 字节，将整数以八字节计数，strings 则以它们的长度计数。

6.2 起源

起源操作可以用来创建一个新的合约，主要是合约代码和合约存储的初始内容。如果该句柄已经是一个已存在的合约的句柄，那么起源操作将被拒绝。(除非是因为错误或恶意，否则基本不会发生。)

合约需要最低 1 余额来保证其正常运行。如果这个余额低于这个数字，该合约就会被销毁。

6.3 交易

交易是从一个合约发至另一个合约的消息，可表示为:

```
type transaction = {
amount: amount; (* amount being sent *)
parameters: data list; (* parameters passed to the script *) (* counter (invoice id) to avoid repeat attacks *)
counter: int;
destination: contract hash;
}
```

如果交易使用管理者密钥签名，或者以编程的方式通过合约中的程序代码执行，那么交易将从合约发出。当这个交易被接收，该交易金额就被加入目的合约的余额中，并且执行目的合约代码。该代码可利用接收到的参数，对合约存储进行读写，改变签名密钥，以及发送交易至其它合约。

计数器的作用是防止中继攻击。当合约的计数等于交易的计数的时，该交易才是有效的。一旦交易被确认，计数器就会增加 1，防止该交易被重用。

该交易也包含客户端认为有效的最近区块哈希值。如果攻击者成功地迫使一个分叉进行长重组，这些交易将不能被整合入区块链，使得分叉显得明显伪造。这也是安全的最后一道防线，虽然 TAPOS 是有效防止这种长重组的伟大的系统，但是该系统对于防止短期双花并不是十分有效。

一个 (account_handle, counter) 对和比特币中未被花掉的输出几乎等价。

6.4 存储费用

存储是网络上最重要的成本之一，在存储上每增加一个字节大约最低的费用为 1 ACDC。例如，如果交易执行后，一个整数被添加到存储中，并且在已经存在的存储的字符串上增加 10 个字节，那么 18 ACDC 将从合约的余额中取出和销毁。

6.5 代码

该语言是基于栈的且具有高级的数据类型和严格的静态类型校验。设计的灵感来自 Forth, Scheme, ML 和 Cat。它有一个完全描述的指令集，详细描述了指令集，类型系统，以及词法和语义。这也意味着一个精准的完全参考指南，而不是一个简单的介绍。

6.6 交易费

到目前为止，这个系统和以太坊处理交易的方式很类似。然而，我们在处理交易费方面却很不同。在以太坊上用户只要支付随程序执行时间线性增长的费用，就可以运行任意长的

程序。虽然这种方式提供了矿工验证交易的经济动机，但并不能给同样参与交易验证的其他矿工相同的动机。在实践中，大多数用智能合约编写的程序都是非常短的。因此，我们通过在程序的执行步骤上加上一个硬性的帽子来简化构建过程。

如果该帽子对一些程序而言被证明是紧上界，他们可以在多个执行步骤上中断并采取多个交易完全执行的方式。正是因为 CreditChain 是自我进化的，这个帽子在未来可以改变，或者引入更多的高级原语。

如果账户同意，签名密钥可以通过发起签名信息请求修改。

7. AdvancedCreditChain 商业优势及发展规划

7.1 ACDC 的波特竞争力优势分析

根据迈克尔·波特(Michael Porter)于 80 年代初提出的五种竞争力分析模型 Michael Porter's Five Forces Model，我们全方面的对 ACDC 进行了深入的分析。对竞争力产生影响的主要有以下五种力量，分别是同业竞争者、购买者、供应者和替代者，针对 ACDC，同业竞争者和替代者是产生主要影响的力量。

在企业征信行业中，更多的竞争者来自传统的企业征信中介机构，但其中数据缺乏共享，征信机构与用户信息不对称、同业机构间缺乏有效共享合作，各机构互相隔绝征信信息，造成严重的信息孤岛问题，加之体制机制原因和征信业技术架构问题，致使传统的征信机构虽然掌握海量征信数据却一直无法真正高效利用。此外，由于传统征信企业之间存在激烈竞争，在面对客户对“AAA”评级的渴求时，各家征信评级企业难免出现道德风险，刻意或无意的忽略一些潜在因素，从而给到客户满意的评级。我团队顾问 Rayloard 先生在实际的公

司债券发行工作中已经将某些评级机构给予的企业评级自行进行降级处理，并且此类情况在中国投资银行实际业务中有大量的实例可追溯。相比同业竞争者，ACDC 征信系统通过去中心化让互相不信任的机构和个人在没有权威中心机构统筹下，彼此通过安全加密的区块链技术进行信息和数据的交互。辅以币天销毁的手段，赋予信用交易成本，准确反映客户真实信用，从数学上解决作弊手段对信用产生的影响。

在如今的区块链行业中，新概念在提出后短时间内将要面对具有相似功能的新进入者的威胁，因此我们在设计 ACDC 伊始就设计了完善的数据共享规则、可靠的公开密钥加密、无偿的数据查询、共享的数据广播、真实的可共享黑名单和高效成熟的信用评价体系。具备了较高的技术壁垒，替代者想要达到替代 ACDC 理论上是存在可能性的，但需要付出高昂的时间成本和研发成本，外加 ACDC 的原生属性——支持元数据升级，自我修正代码进化协议，可以吸收任何一种基于区块链的征信系统的优点，将其常规区块链上的各种操以单纯的功能模块方式实现，从而使得替代者的功能优化不仅不会威胁到 ACDC，反而会不断推动 ACDC 功能升级，达到一种在中国古代武侠文学作品中"小无相功"的效果。

显而易见的，对于功能全面、技术突出、解决痛点的 ACDC 来说，来自同业竞争者和新进入替代者的竞争力量不仅对其产生的负面影响较小，而且可以促使其进化升级，因此 ACDC 具有独特且不可忽视的竞争力。

7.2 ACDC 的资源优势分析

1997 年，提斯（Teece，1997）等学者提出了动力能力理论，认为资源可以分为四个层次：

第一层，是获得的公共知识。ACDC 加密征信系统通过将密码学应用在征信领域，通过网络壳（shell）处理网络层任务。

第二层是专有资产，如商业秘密、生产秘诀和特殊功能等，由于融入了企业的无形知识，因而非常难以复制和模仿。ACDC 通过团队的艰苦研发，具备可靠的共享规则、加密技术和无偿的黑名单查询，搭建了独特信用评价体系和技术壁垒。

第三层是管理团队的能力和外部资源，即将生产要素和专有资产有机地整合起来的组织惯例和管理活动，对于那些与竞争对手比有显著优势的能力就是竞争优势的主要来源。著名的"潘罗斯效应"。（ Penrose，1959）认为，规模不能从大小上去比较，关键是取决于企业管理者拥有的知识和管理能力，虽然 ACDC 目前市场规模仍在萌芽状态，但我们的团队有顾问 A，顾问 B，（你加点顾问的技能，突出下相关研发实力之类的就行）具有优秀的管理能力，将会为 ACDC 后期的发展带来持续不断的动力。

第四层是动力能力，强调为适应不断变化的外部环境，必须不断取得、整合内外部的社会组织、通过资源整合能力打造专有资产，例如专有技术资产、声望资产、和市场资产等，ACDC 团队除了在研发技术上具有非常高的水准，在声望方面也有突出的进步。目前团队与越南政府、贝宁政府和传统征信企业之间有着紧密合作和联系。事实上，ACDC 已与越南政府及贝宁政府达成了初步共识，越南通信部队总司令暨越南陆军足球队经理 Hồ Tri Liêm 先生表现出了对 ACDC 项目理念的高度赞赏。贝宁总统 Patrice Talon 先生同样表达了对于 ACDC 的强烈兴趣，并表示会对 ACDC 项目落地提供必要的帮助。与此同时，ACDC 团队也在积极与新加坡、日本、意大利、莱索托等国相关部门洽谈，为其带来全新的征信系统，解决现有痛点。

综合对 ACDC 动力能力四层的深入分析，我们可以发现 ACDC 在资源优势方面具备较大提升潜力，在扩大声望和影响后这种优势会加速凸显。

7.3 发展规划

虽然相比传统征信行业，ACDC 具备鲜明的特点和突出的优势，但毕竟 ACDC 是全新的系统，并且由于去 ACDC 的中心化势必触动传统征信行业机构利益，在推行过程势必会有阻碍，但 ACDC 带给行业的竞争并非破坏性的，而是促进性、改善性的。在有效的沟通后团队相信可以集结行业内外的精英力量，辅之以国家政府的无间协作，ACDC 团队有强大的信心将项目顺利推进，为引入 ACDC 的国家创建一个透明健康的商业环境并且提供对社会发展与稳定至关重要的公平与正义。目前我团队正与中国一领先的金融科技企业沟通，在未来会深度运用其目前已有的中国 17000 家信用主体的财务信息、评级历史与股价表现数据。

有了 ACDC 这一切将会更加容易的实现，这也是多名关心国家社稷的政要高度看好 ACDC 的一个重要因素。在未来，ACDC 将会与风险控制公司、猎头公司、会计与审计公司以及背景调查公司进行深度合作，将传统征信系统化繁为简，为征信行业插上区块链科技之翼。

8. 引用

. [1] Vitalik Buterin. Slasher: A punitive proof-of-stake algorithm. https://blog.ethereum.org/2014/01/15/ slasher-a-punitive-proof-of-stake-algorithm/, 2014.

. [2] Ariel Gabizon Iddo Bentov and Alex Mizrahi. Cryptocurrencies without proof of work. http://www.cs.technion.ac.il/~idddo/CoA.pdf, 2014.

. [3] Peter Suber. Nomic: A game of self-amendment. http://legacy.earlham. edu/~peters/writing/nomic.htm, 1982.

. [4] Jérôme Vouillon. Lwt: a cooperative thread library. 2008.

. [5] Tezos project. Formal specification of the tezos smart contract language. https://tezos.com/pages/tech.html, 2014.

. [6] Lending Relationships and Credit Rationing: The Impact of Securitization. Santiago Carbovalverde, Hans Degryse, Francisco Rodriguezfernandez

. [7] Bitcoin and the Blockchain: a coup d'état in Digital Heterotopia? Donncha Kavanagh, Gianluca Miscione

. [8] Collaborative Filtering on the Blockchain: A Secure Recommender System for e-Commerce. Remo Manuel Frey, Dominic Worner, Alexander Ilic

. [9] An Analysis of the Cryptocurrency Industry. Ryan Farell

. [10] Blockchain Demonstration Shows Potential Loan Market Improvements. Credit Suisse

. [11] Integrating blockchain and artificial intelligence into the accounting curriculum. Sean Stein Smith

. [12] THE AFRICA INVESTMENT REPORT 2016

. [13] ASEAN Investment Report 2016，Foreign Direct Investment and MSME Linkages

. [14] EY’s Attractiveness Program Africa