



定义去中心化金融服务

基于区块链和多方安全计算技术，
服务东南亚市场 20 亿人

目录

Defi 项目背景	01
数据越来越重要，但也面临着重重问题	01
信用数据市场的现状导致信用评分仍处于欠发达状态	01
Defi 项目的愿景与使命	02
东南亚市场与 Defi 项目存在特别的关联	03
Defi 产品介绍	06
B2B 产品：跨企业数据协作	06
产品 1：联合风控平台	07
黑名单共享服务	07
多头借贷监测服务	07
产品 2：信用评分平台	09
产品 3：联合营销平台	10
沉睡用户激活	10
精准营销	10
B2C 产品：基于个人数据钱包的应用	11
产品 1：块点投 /Coinsta	11
产品 2：CreditMe	12
Defi 核心技术	13
高阶架构设计	13
核心技术	13

分布式账本	14
可信计算环境	14
数据加密及混淆	14
零知识证明	14
数据检索与搜索	14
不对称加密	14
差分隐私	14
联邦计算	15
技术流程	16
GDPR 合规	17
Defi 项目计划	18
Defi 通证：DEFI	19
项目治理	20
项目团队	21
顾问团队	22



Defi 项目背景

数据越来越重要，但也面临着重重问题

如今，数据不间断的产出和记录，并呈现出爆发式的增长趋势。据国际数据公司（IDC）最新的数字研究，到 2020 年每人每秒会产生约 1.7 兆数据信息。

数据被广泛应用于我们生活的各个场景中：互联网巨头应用数据向我们提供个性化的产品和服务，例如基于数据分析向我们推荐视频和商品。数据协作和共享的需求也越来越强。哈佛商业评论最近的一项研究发现，已经有三分之二的组织机构试图将五到十五个数据源混合起来进行分析。更多前沿科技的发展也扎根于大量数据输入，例如基于大数据的人工智能，随着逐渐成熟将应用于医疗、交通等多个行业。

随着数据价值被更多人认可，以及被更深层次的挖掘，数据应用中存在的种种问题也浮现出来：数据泄露，数据被滥用，个人隐私被侵犯等等。因此全球监管机构对数据使用的监管也变得越来越严格。《通用数据保护条例》（GDPR）（欧盟）2016/679 是欧盟数据保护法中的一项条例，它不仅保护了欧洲联盟 (EU) 和欧洲经济区 (EEA) 内所有个人的隐私数据，也解决了在欧盟和欧洲经济区以外的个人数据输出问题。GDPR 的主要目的是给予公民和居民个人数据控制权，并对欧盟内部的业务实行统一监管，以简化国际监管环境。

信用数据市场的现状导致信用评分仍处于欠发达状态

回顾历史，信用评级始于银行和商户之间收集和分享多样化的数据。在 20 世纪下半叶，二战后返回家园的美国人对住房和抵押贷款产生了巨大的需求，在接下来的几十年里，这种趋势促进了市场的整合和技术的进步，信用报告公司开始在全国范围内开展业务，通过更先进的建模技术和客观的信用评分，帮助企业评估风险并做出更快、更便宜、更可靠的决策，从而取代了人工主观的决策过程。

尽管 FICO 评分仍是被普遍采用的方法（约占 90% 的市场份额），但从近几十年来经济活动的变化上看，FICO 的评分已经过时。自 1956 年 FICO 问世以来，受电子商务和基于互联网的社交应用的普及推动，许多关于借款者的新型经济行为数据已成为可用数据，但是 FICO 系统内并不包括这一类数据。

除了传统的评分模型，大数据信用评分正在兴起。大数据信用评分依赖于比传统信用评分多 10 至 100 倍的数据集，并使用包括机器学习在内的新兴先进技术。多样地信用评分方式进一步探索了非传统数据的预测能力。信用相关数据是信用评分的基础，但目前的数据收集过程也存在成本高、效率低、隐私泄露等各类问题：



1. 由于缺乏有效的数据共享机制，许多贷款机构会将时间和金钱花费在收集关于同一借款人的重复数据上，与此同时，大部分人口的信贷数据仍然处于缺失状态；
2. 数据获取成本昂贵，并且获取过程经常涉及到在发展中国家的黑市上买卖个人数据，大家对于安全和隐私方面非常担忧；同时，从黑市甚至是中央信用局获得的许多数据都是片面或不准确的，无法对贷款人的信用状况提供有效的支持。低质量的数据还使得信贷市场信息失真，损害了消费者的权益。
3. 个人数据资料的使用者每年可从这些资料中赚取巨额利润，但数据提供者并没有因此获利。

尽管在构建共享数据库方面有巨大的潜力，但是现有的数据所有者与大部分公司机构都不愿意或无法互相合作，原因如下：

1. 安全问题以及对竞争对手数据控制权的顾虑；
2. 缺乏对早期参与者的激励措施：数据共享的好处是由网络效应驱动的，因此对早期参与者的激励措施有限
3. 技术无法实现大规模实时数据交换的吞吐量需求

因此直到今天，信用评分系统仍然将数十亿人视为“隐形人”，这其中包括快速增长的千禧一代、移民和许多低收入家庭，他们现在仍然无法从企业或者银行获得需要救急的资金。

Defi 项目的愿景与使命

Defi (Decentralized Finance, 去中心化金融) 的技术核心是基于区块链的安全多方计算系统，我们相信 Defi (区块链 + 可信计算) 是即以太坊 (区块链 + 智能合约) 之后行业最重要的一次范式转移。

Defi 认为，基于区块链的数据协作协议在提取数据价值方面具有天然优势，也能够激励人们参与到数据贡献中来。基于区块链的系统不但能够记录数据的所有权，还可以更好的保护安全和隐私。基于区块链的数据交换与计算系统可以通过对原始数据的混淆处理，降低数据泄漏的可能性，使数据变得更安全。这种体系结构可以应用高级加密和数据处理技术，包括零知识证明、隐私差异、非对称加密和数据混淆。

最终，当安全和激励问题都得到解决时，一个更全面、更准确的数据网络将为释放人工智能最大潜力提供强有力的基础。

Defi 项目的目标是凭借全球领先的技术和工程化能力，从分布式的芝麻信用，走向区块链上的蚂蚁金服，服务东南亚 20 亿尚未被传统金融服务覆盖的普通人，回归区块链 serve the next billion 的初心。



Defi 为新时代的消费者提供了一个更公平、更高效、更全面的金融服务市场。分布式数据协作协议允许参与者提高数据质量，降低数据获取成本，扩大数据覆盖范围，最终通过人工智能创建更好的信用评分模型。

通过建立在 Defi 协议之上的 Defi 生态系统，我们可以看到能够大幅改善多个金融服务垂直领域的巨大潜力，包括：

- 通过普惠金融，推动社会公平和经济发展。世界银行认为，改善信贷获取渠道促进了社会公平，是推动经济发展和减轻贫困的最佳做法之一。
- 促进消费信贷体系发展：菲律宾、泰国和印度尼西亚等发展中国家必须从基础设施投资驱动型增长模式转向消费驱动型增长模式，以实现可持续发展。全面的消费信贷体系正是这种经济转型的基础。
- 通过扩大信贷市场和消费市场的份额，向大众提供信贷覆盖可以创造非常大的利润价值。这样的增长刺激可以激励更高质量的借贷、支出和投资。

东南亚市场与 Defi 项目存在特别的关联

大多数东南亚国家还未充分释放其经济潜力，这些国家占据着人口众多、人口结构优越、科技和互联网普及率高、金融科技空间发展迅速等独一无二的优势，这些都为东南亚经济发展提供了机遇。除此之外，有两个因素的存在也使得 Defi 在东南亚地区存在的意义得以凸显。

首先，东南亚国家政府在数字转型和金融普惠方面都有宏大的目标。印度尼西亚到 2020 年希望成为全球最大的数字经济国家，达成创建 1000 家科技初创企业的目标，同时将每年的电子商务交易额提升至 1300 亿美元。为了实现金融普惠，推动金融服务业的创新，菲律宾最近推出了一套支付系统，目标是将公司目前只占 4% 的数字支付交易率增加到至少 20%。越南希望到 2020 年，能够将银行普及率从目前的 59% 提高到 70%，同时将现金交易降低到不足 10%。泰国非常重视利用区块链等技术来改善国内的金融服务，创造一个良好的金融科技生态系统，并且积极欢迎来自其他国家的众多金融科技初创企业驻扎。为了促进数字转型，马来西亚也在推动开放 API 等多项举措，并邀请更多行业人士参与 P2P 贷款等领域，他们认为开放 API 将彻底改变该国金融科技生态系统。新加坡拥有对包括金融科技在内的科技公司最友好的生态系统，这使得该国成为东南亚地区金融科技公司数量最多的国家之一。

在高度重视推动地区金融科技创新的情况下，亚太地区具备引领下一轮革命的良好条件。随着该地区的监管机构通过诸如东盟金融创新网络 (AFIN) 这样的平台拥抱开放的银行体系——东盟金融创新网络是世界上第一个将银行与金融科技公司联系起来以提高金融包容性的跨境开放式架构平台——Defi 在东南亚的重要性将不断增加。Ernst & Young 对东盟金融科技的一项研究显示，该地区的金融机构正在寻求 AFIN 的支持，



以优先将金融科技服务纳入包括信用评分、KYC、中小企业贷款解决方案等领域的沙盒，所有这些都与 Defi 的核心业务范围有关。

其次，互联网普及率的快速增长，为多方数据协作提供奠定了基础。菲律宾移动互联网用户正以 1.5 倍（或每年 3000 万）的速度增长。泰国互联网用户比例从 2017 年的 67% 上升到 2018 年的 84%；印度尼西亚拥有超过 1.43 亿的互联网用户，是东南亚地区互联网用户最多的国家之一；在过去的十年里，越南的互联网用户数量几乎翻了一番。马来西亚和新加坡已经有约 85% 的人口在使用互联网。

互联网在东南亚地区的迅速普及意味着通过社交媒体、流媒体服务、电子商务等媒体产生的数据量会更高，但是，这些数据目前还处于一种封闭状态，还未出现以安全的方式多方协作共享数据的实践案例。

示例：东南亚国家的互联网普及率和银行存款人口

国家	互联网渗透度	金融服务覆盖人群
印度尼西亚	55%	49%
菲律宾	63%	31%
越南	54%	59%
泰国	84%	97%
马来西亚	85%	85%
新加坡	84%	98%

Defi 可以从两个角度帮助东南亚金融机构扩大市场、降低风险，同时帮助普通消费者获得更好的服务：

对于互联网渗透率较高，但金融体系不完善的东南亚国家（如印度尼西亚和菲律宾），Defi 可以帮助没有满足银行最低要求的人们提供信贷。通过多方数据贡献和安全计算，银行可以获得关于个人的信用数据和画像，



甚至可以为那些没有任何银行和信用记录的人提供信贷。经济体中更多的信贷供应将进一步导致消费增加，并推动经济增长。

对于金融体系相对成熟的东南亚国家（如马来西亚、新加坡和泰国），Defi 可以提供一个更安全的数据合作框架，通过多方数据输入，实现更好的风险评估模型。这将帮助金融机构改进风险评估模型，并使他们能够更全面地了解借款者的行为。对于拥有大量银行存款用户的经济体来说，这将会让其信贷违约率大幅下降。



Defi 产品介绍

Defi 通过以下方式定义最先进的普惠金融体系：

- 扩大获取信贷的渠道：大多数国家，特别是发展中国家，由于缺乏数据，人们获得信贷的机会仍然有限。没有相关数据，金融机构无法对风险进行评估和控制，因此金融机构多数都不愿提供相关金融服务。Defi 旨在鼓励机构和个人之间的数据合作，并帮助每个人获得信贷。
- 增强数据的可迁移性：即使在当今世界，数据也是无法迁移的。数据通常都被抓取和存储在不同的公司和组织，假设你从一个国家搬到另一个国家，那么你必须从头开始建立新的个人信用体系。Defi 的目标是通过完善的金融数据管理工具和平台来解决这个问题。
- 身份证明：这是构建共享 KYC 流程，使得金融机构和个人受益。Defi 旨在应用新技术和数据来创造一个去中心化的自主身份身份，它可以帮助金融机构更好地识别和认证客户，降低金融诈骗风险，促进普惠金融。
- 隐私保护计算：在涉及数据传输和处理的场景中，数据隐私是企业和个人最关心的问题。Defi 将安全和隐私放在首位，采用创新技术确保所有数据处于安全的环境下，并且这些数据只有授权方才能访问和使用。

通过 Defi 网络，数据提供者可以在不公开原始数据的情况下协作 3000 多种类型的数据；模型提供者提供分析模型（例如信用评分）作为服务；个人用户可以查看自己的数据档案，对其进行纠错及管理，并建立一个更全面的数据档案以获得奖励；数据使用者（例如金融服务提供者）购买计算结果（例如信用评分），或构建去中心化应用（如贷款、资产支持证券和保险）。

为了在全球范围内得到机构和个人的广泛使用，我们设计了 Defi 安全多方数据协作协议：

- 公开、公平、高效的数据交换：所有的交易历史都被永久地记录到区块链中；所有交易都由智能合约自动代理、执行和强制执行。
- 低延时性：与直接交换数据相同的性能。
- 可扩展性：可以支持成千上万的参与者，支持任何规模的数据交换，吞吐量 >1k TPS（初始阶段），>100k TPS（未来），可以在一些人口稠密国家的极端情况下提供支持。
- 可靠性：全冗余结构，无单点故障，可以抵御分布式攻击。



- 数据安全和隐私保护：通过零知识证明请求数据，受非对称加密和数据混淆保护的数据传输，分散、加密的数据存储，不公开披露个人身份信息。
- 合规性：遵守所有国家的法律法规以及全球主要市场的政策条例，符合 GDPR 要求。
- 真实性：数据来源于多个提供方，不断相互校验，并对数据质量评级所有提供方不断认证和评级。

B2B 产品：跨企业数据协作

产品 1：联合风控平台

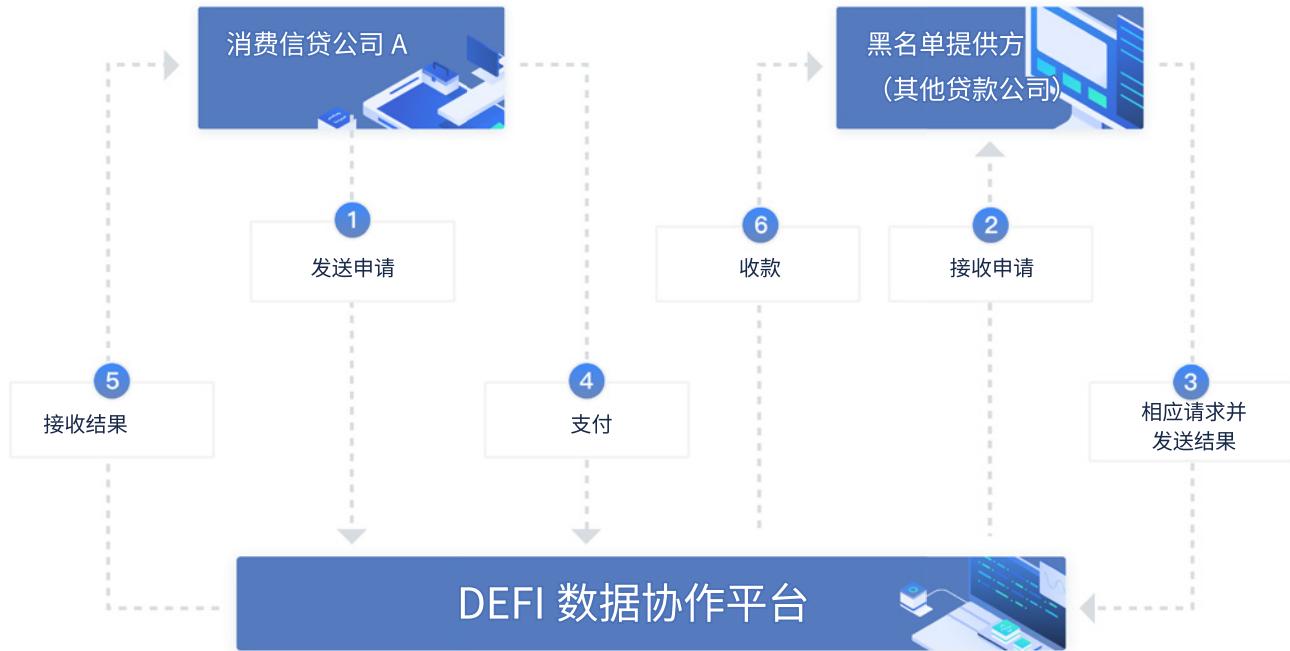
通过 Defi 安全多方计算技术，不同金融机构可以共同建立安全的风险数据联盟。这是打造一个安全的数据协作环境的创新之举，不仅能为用户提供更严格的隐私保护，还能提供让用户在数据中创造额外价值的机会。金融机构可以上传、分享、联合计算信用数据，通过相互合作创建一个更有效率、更健康的信贷市场。

黑名单共享服务

消费信贷公司拥有自己的黑名单，包括之前违约或参与欺诈活动的客户。然而这类的黑名单既不共享也不公开。一个消费信贷公司需要一段时间的时机贷款业务来积累这样一个黑名单列表，过程中会发生实际的损失。Defi 黑名单共享服务的目标是消除信息孤岛，使贷款机构能够合作抵制有问题的借款人。其中，消费信贷公司可以同时担任数据提供者和数据使用者的角色：

作为数据请求者，消费信贷公司可以用包括银行账号、手机号码和身份证件等数据信息来检查用户的个人信用，是否曾经在其他公司由于欠款未还而在黑名单之中。这有助于消费信贷公司更好地确定个人信用风险，降低运营风险水平，从而提升利润率。

作为数据提供方，消费信贷公司可以将自己的黑名单数据放入网络中。如果其黑名单数据被其他公司查看使用过，提供数据的公司就可以从中获得相应报酬。通过使用 Defi 技术，这些数据将不会泄露给其他公司。以下是 Defi 黑名单共享服务的工作流程：



1. 消费信贷公司 A 在评估贷款风险时，通过 Defi 平台发起信用欺诈检测请求
2. 其他贷款公司收到请求
3. 匹配到黑名单信息的数据提供者（其他贷款公司）处理并将结果发送到 Defi 平台
4. 信贷公司 A 通过 Defi 平台进行支付
5. 信贷公司 A 收到结果
6. 黑名单信息提供者获得相应收益

多头借贷监测服务

一些借款人通过多个借贷平台申请贷款，使他们的个人债务增加到他们无法偿还的水平。一项调查显示，如果申请人从多个来源借款，他 / 她的逾期率是平均水平的 3~4 倍。拒绝这种类型借款人的借贷申请，将有效降低违约风险。

借助 Defi 安全多方数据协作技术，借贷平台可以发起对贷款人个人信息的查询请求，例如借款数量、借款金额、逾期历史、逾期金额等。这些信息将使贷款公司能够在发放贷款前作出更明智的决定。



产品 2：信用评分平台

Defi 信用评分与评估平台提供了一个可以容纳所有现有的信用评分方法和参与者的框架。这样的设计反映了 Defi 的信念：在一个活跃的市场中，广泛的服务提供者可以最大限度地提高效率，并为消费者带来最具竞争力的产品。

Defi 将利用协议中的数据来计算信用评分，数据包括申请人、征信 / 信贷局、电信、移动使用数据、社交网络、电子商务交易、金融交易等数据。

目前有三种信用评分方法：传统信用评分法、大数据信用评分法和替代信用评分法。

只使用信用记录数据的传统的信用评分法仍然是现如今最被广泛使用的方法。FICO 是该领域的领导者，拥有 90% 的市场份额。除了 FICO，许多商业银行的内部团队也在使用传统的信用评分方法。Defi 网络通过为这些模型用户提供 api 来贡献和获取数据，从而支持传统的信用评分法。

大数据信用评分正在快速增长中。大数据信用评分方法使用了更广泛的信用评分变量，通常结合了教育、就业、工资、电子商务购物、在线社交网络连接、社会保障和医疗保险以及资产持有情况等数据。此外，Defi 协议 api 将允许这些模型提供者使用 Defi 网络计算信用评分。

替代信用评分探索出了许多进行信用评估的新方法。这些新的方法包括将借款人行为数据作为一个因素，并依赖于直接从用户那里获得数据。Defi 有足够的灵活性来整合这些替代方法。

Defi 信用评分模型将提供由内部信用评分模型支持的 Defi 评分：Defi Score Basic 使用的是经过金融行业测试并得到广泛应用的一流评分模型。

$$p = \frac{\exp(\beta_0 + \beta_1 \cdot x_1 + \dots + \beta_n \cdot x_n)}{1 + \exp(\beta_0 + \beta_1 \cdot x_1 + \dots + \beta_n \cdot x_n)}$$

据上图：

p 是违约概率

x_i 为解释因子 i

β_i 是解释性回归系数因子 i

n 是解释变量的个数



Defi Score Plus 融入了创新的评分理念，包括斯坦福大学张首晟教授提出的“Zhang Rank”。Zhang Rank 通过合并时间戳和赋予最近数据更多权重进一步提高相关数据排名。Zhang Rank 在基于区块链的信用评分系统中至关重要，因为它极大地降低了贷款人随着时间的推移利用信用评分系统进行一些诈骗行为的风险，并且 Zhang Rank 强调的是信用记录集合，贷款者滥用系统将变得不可行。

受 Word2Vec 在自然语言处理方面的启发，Defi 正在开发的下一代信用评分方法，Person2Vec，它将为整个信用评分网络做出贡献。Person2Vec 将基于不同场景动态地选择最佳变量来描述贷款用户的信用价值。

在目前的体系下，信用评分无法在各国之间无障碍传递，这给机构和个人带来了很多不便，并导致机会流失。基于区块链的 Defi 协议具有可跨境传递的特征，它允许个人和机构最大限度地利用其信用数据进行评分，而不必考虑国家界限，这有益于东南亚国家朝着区域内更深层次的经济一体化迈进。

除上述模式外，Defi 信用评分平台欢迎社会各界建立和贡献有效的信用评分模式。一旦验证了模型的有效性，科技公司、经济学家和数据科学家就可以利用简单易用的工具在网络上贡献自己的信用评分模型，并从中获利。我们相信这样的市场环境和 Defi 协议所带来的大量高质量数据的结合，将为不同场景和不同领域的信用评分模型带来持续的优化与进步。

产品 3：联合营销平台

沉睡用户激活

沉睡用户激活可以大大增加公司的收入，并提高客户生命周期价值。无法激活沉睡用户的通常是因为公司缺乏相关信息，无法了解用户的最新情况，从而无法开发更定制的产品或更有效的营销策略。但沉睡用户激活具有深远意义：

首先，沉睡用户的转化率高于活跃用户。从了解产品到购买产品，最大的障碍在于公司和消费者之间缺少了解与信任。沉睡用户因为曾经购买过公司产品，因此比新用户更可能购买相关产品。

其次，通过对沉睡用户的进一步了解，公司可以创造出更多量身定制的产品以增加销量。例如，一家消费信贷公司可以使用 Defi 的数据协作协议来查找曾经服务过的客户的属性，并为他们提供与其新属性相匹配的其他金融产品和相关服务。这将重新吸引沉睡顾客再次购买公司产品，带来更多利润。

精准营销

Defi 的安全多方计算框架可以帮助营销团队使用创新策略，通过分析特定用户群的特定需求、兴趣和行为模式，帮助品牌更好地满足个体群体的需求，并显著提高营销传播的成功和有效性。



精准营销针对现有客户，可以鼓励品牌忠诚度，刺激购买行为。精准营销会减少业务对广告的依赖，创造能够吸引现有客户的交易和优惠来替代广告。为了做到这一点，精准营销在很大程度上依赖于来自多个数据提供商来创建客户档案，通过了解每个客户的独特需求，制定更明智的策略来保持他们的忠诚度。

通过数据交易流和加密机制，Defi 协议可以促进多方数据协作，显著提高广告定位和推荐引擎的准确性，在不公开任何原始数据的情况下实现数据共享，从而更好地对目标用户进行分析。

B2C 产品：基于个人数据钱包的应用

数据可以完整的描述个人信息，目前急需更好的管理方式。个人数据钱包帮助个人存储和管理个人数据，如身份信息、教育背景、消费历史、财务记录、社交媒体行为等等。通过对数据的管理和授权，用户的个人数据可以帮助他们获得更好的服务，甚至给他们带来盈利。

Defi 确保个人的数据是安全的，并且归属权只在于用户个人。通过使用先进的技术，我们确保用户的数据存储在个人设备中，只能在用户自己的授权下请求和使用。数据传输和处理过程是加密的，并且是在可信的执行环境中进行的。这可以防止任何第三方实体入侵用户的数据或损害用户的隐私。

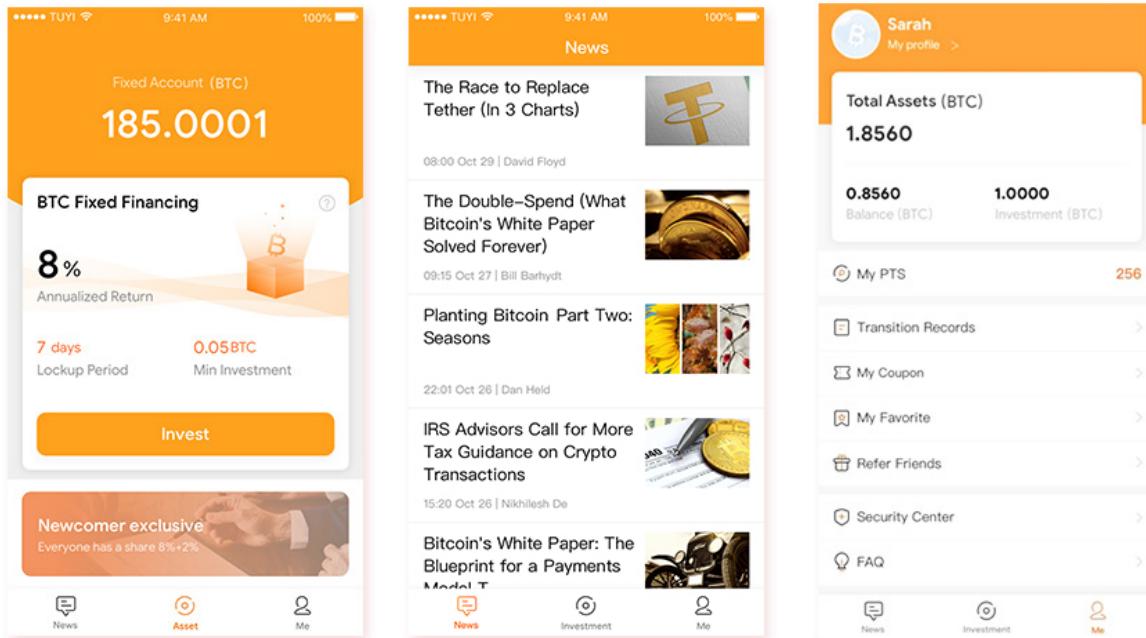
Defi 是探索个人数据钱包用例的先驱，并且 Defi 现已推出了两个应用程序，帮助用户管理数据，以获得更好的金融服务和奖励。

产品 1：块点投 /Cointsta

块点投 /Cointsta 提供一站式数据资产管理服务，包括加密货币、区块链新闻以及个人数据，是新一代的数字钱包。

块点投 /Cointsta 提供 BTC 理财产品，这些产品由专业管理团队管理，通过量化交易产生稳健的收益。块点投 /Cointsta 还为数字货币投资者提供个性化的聚合新闻推送，使他们能够阅读相关的加密数字货币新闻、监管新闻或与区块链初创企业相关的最新消息。

同时，块点投 /Cointsta 让用户能够更有效的使用他们的个人数据。块点投 /Cointsta 鼓励用户在数字身份管理界面中贡献自己的个人数据，用户可以以此换取积分，因块点投 /Cointsta 使用了 Defi 协议，用户最后还可以用这些积分兑换 Defi Token (DFT)。



产品 2：CreditMe

据世界银行统计，世界上有 24.5 亿人没有银行存款，同时还有 9.75 亿人无信贷资格，这意味着世界上 34.2 亿人（占世界成年人口的 72%）被定义为“无信贷价值”。世界上 70% 以上的欠发达地区都没有信贷业务，近 60% 的全球人口需要增加信贷额。

CreditMe 帮助用户根据自己的个人数据获得最合适的个人信用贷款和其他金融服务。通过用户所提供的身份、教育、工作信息以及其他综合数据，CreditMe 会编译一个独特的、可以被金融机构接受个人信用档案。用户提供的数据越多，则其信用档案就越准确。信用档案越准确，金融机构就越有可能批准此用户的贷款或信用卡，甚至提供更好的利率。分布式去中心化的数据协议保证了用户对其个人数据的所有权及控制访问权，这保护了用户个人数据隐私安全，解决了数据泄漏等问题。

此外，如果个人授权他 / 她的消费数据、社交媒体数据和其他相关数据，CreditMe 的算法和模型能够生成更全面的用户个人资料。CreditMe 还可以根据用户的个人兴趣及行为历史推荐相关的金融产品。例如，如果用户的数据显示他 / 她对电子设备很感兴趣，那么当新一代 iPhone 问世时，CreditMe 可以为此用户推荐最合适的个人消费贷款。



Defi 核心技术

高阶架构设计



Defi Protocol 的基础设施包括区块链和数据安全传输服务。区块链用作分布式账本和智能合约平台。Defi 的技术可以架在任何区块链上，第一个应用于 Defi 战略合作伙伴 Ontology 合作。数据安全传输服务可以保证数据通过加密的、分布式的方式完成交换。

在此基础上，Defi 开发了包括数据浏览器、委托服务、数据注册表、可信计算环境的基础服务，保证数据提供方可以方便、安全的接入，同时实现产品的性能、可扩张性和稳定性。

核心技术

分布式账本

区块链就是一种分布式账本。Defi 的产品和技术可以嫁接在任何区块链上，第一个应用于战略合作伙伴 Ontology 合作。Defi 的机制在保证公平的情况下兼顾效率，最大化的利用了区块链分布式、匿名性且不可篡改的优势特点。



智能合约

智能合约可以实现程序化、自动化的执行相关的交易，同时这些交易可以被追踪但无法被篡改。通过使用智能合约，Defi 可以打造一个开放、公平和高效的数据市场。数据需求方可以通过智能合约的方式广播数据需求，数据提供方可以自行应答。整个过程都在区块链上自动执行，确保程序公平，且不受人为因素影响。

可信计算环境

可信计算环境（TEE）是一个独立的执行环境，可以保证其中的数据和程序的安全和一致性。通过搭建可信计算环境，Defi 确保数据和模型在沟通和计算流程中的安全性，进行全过程的监测和控制，防止被第三方攻击。

数据加密及混淆

数据加密和混淆技术可以更好的保护数据安全。在数据加密的过程中去掉与身份相关的敏感数据，可以实现数据与来源无法对应，实现更好的安全性。Defi 在数据传输和计算过程中运用数据加密技术，帮助客户防止数据泄露，提升数据的安全性。

零知识证明

零知识证明可以在不暴露原始数据的情况下验证对方知道具体的数据。Defi 应用零知识证明技术，保护用户心思数据不泄露，同时证明用户确实拥有该项数据，解决网络中各个参与方互相不信任的问题。

数据检索与搜索

Defi 平台上有多方参与数据合作。通过数据检索，每个参与方可以更高效的贡献、交换和使用数据，提升平台的整体性能。因为数据存储在分布式账本中，Defi 支持用户从不同的数据源搜索数据，以提升效率。

不对称加密

不对称加密中存在两个密钥：公钥可以广泛传播，而私钥掌握在所有者手中。这样的加密方式可以更好的保障数据真实和安全，因为公钥可以确保数据已经发出，而只有私钥可以解码该数据。

Defi 在数据传输过程中运用不对称加密技术，确保没有第三方可以获得数据。参与数据传输的两方可以建立私有的安全通道，即使面临攻击，原始数据也无法被解码。

差分隐私



差分隐私的通过模糊非关键信息，在确保数据质量不受影响的情况下减少原始信息暴露。Defi 运用差分隐私技术，确保数据提供方在参与多方计算时，原始数据无法被追溯并解码。

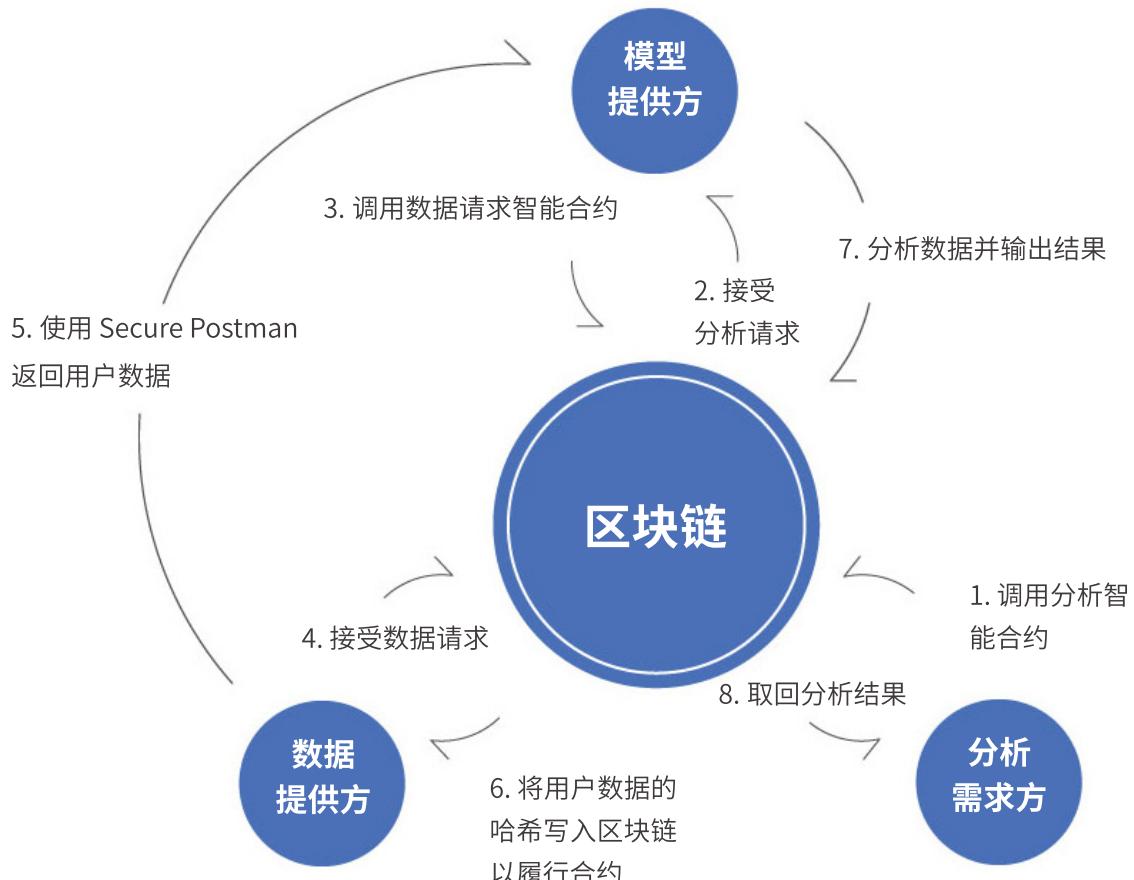
联邦计算

联邦计算可以使得移动设备共同学习和分享预测模型，同时数据保存在每个设备本地。这个技术可以使得每个设备仅掌握和使用本地数据，但可以共享大数据训练的模型成果。

实现流程上，你的手机从云端下载现有的模型，基于你手机上的数据优化模型，将优化点总结后通过加密技术上传到云端。每个设备的优化点会被纳入整体考虑，进而优化整体模型。整个过程中，你的个人数据都没有离开你的设备，保证了数据安全。



技术流程



网络中存在三个角色，数据提供方，模型提供方和数据需求方，分工如下：

- 数据提供方：提供数据，收取通证。提供的数据类型包括：公开数据（如房产、车辆信息等）、聚合数据、其他数据（如通信记录、健康报告等）。同时，个人也可以成为数据贡献者，授权并管理相关的数据。
- 模型提供方：接受分析需求，从数据提供方抓取数据，输出分析结果。在 Defi 网络中将存在不同的模型提供方，以满足各个行业和业务场景的分析需求。
- 数据需求方：提出分析需求。

举例如下：某消费信贷公司在收到贷款申请后发起对借款人信用评分的查询需求。Defi 收到需求后从模型库中选择合适的信用评分模型，向数据提供方收集模型所需的各项参数，计算结果后返回消费信贷公司。



GDPR 合规

GDPR 是目前对个人数据保护力度最严格的的法律法规。如果合作伙伴有相关要求，Defi 可以实现完全的 GDPR 合规，因为 Defi 平台有以下特点：

- 数据提供方拥有数据，平台不存储数据
- 所有的数据处理行为都记录在区块链上，Defi 将提供 API 供用户查阅
- Defi 将要求所有合作方在处理欧洲用户数据时，遵守 GDPR 相关规定



Defi 项目计划

Defi 项目开发计划如下表所示：

时间	项目产出
2019 年一季度	<ul style="list-style-type: none">· 上线黑名单共享服务，签约首批东南亚消费信贷公司· 发布块点投 /Cointa App
2019 年二季度	<ul style="list-style-type: none">· Defi 平台支持多币种转换及 token 支付· 上线多头借贷监测服务· 发布 CreditMe App
2019 年三季度	<ul style="list-style-type: none">· 上线信用评分平台，实现分布式的多方数据安全计算
2019 年四季度	<ul style="list-style-type: none">· 上线保护数据隐私的模型训练服务· 在生态伙伴之间实现不暴露原始数据的数据交换
2020 上半年	<ul style="list-style-type: none">· 上线联合营销平台，与客户联合开发营销场景，如老用户唤醒、精准营销等
2020 下半年	<ul style="list-style-type: none">· 持续扩大 B 端伙伴和 C 端用户人数· 鼓励生态伙伴基于 Defi 的多方安全计算框架开发更多应用



Defi 通证：DEFI

DEFI 在 Defi 生态系统中扮演着重要的作用，总计数量 100 亿枚，没有通胀。

在 B2B 场景中，Defi 将支持使用 DEFI 作为支持手段进行联合风控服务（包括数据、模型和安全计算算力）的调用，同时，平台也接受法币支付，法币部分的收入会对 DEFI 进行定期的回购。

在 B2C 场景中，Coinsta 和 CreditMe 内部均支持数据贡献挖矿系统，同时可以兑换包括会员升级、理财升息券、借贷降息券等产品和福利。



项目治理

Defi 项目由 Defi Foundation Ltd. 治理。Defi Foundation Ltd. 是注册于新加坡的法律实体，致力于建立并维持 Defi 产品和生态系统的开发和持续运营。

为了达到管理目标，Defi Foundation 承诺将作出以下管理举措：

- Defi Foundation 将每月发布项目进展，与社群同步消息。
- Defi Foundation 将举办年度大会，邀请社区用户参加，对 Defi 项目发展献计献策，大会支持互联网远程参加。

Defi Foundation 将成立委员会，监督 Defi 相关业务的进展，并提供技术支持。我们致力于聚集世界级的跨学科人才，将经济、计算机与管理融合，打造新一代的金融服务基础设施和商业应用。



项目团队

CEO - Katherine Shen

Katherine 兼具深刻的技术洞见和丰富的东南亚市场拓展经验。她曾任小米新加坡和马来西亚国家总经理，是前 Google 副总裁 Hugo Barra 执掌小米国际业务后的重要爱将，负责小米在东南亚市场的拓展，对东南亚市场和用户有全面的认识和丰富的运营经验。

Katherine 家学深厚，毕业于全球图灵奖得主最多的卡内基梅隆大学计算机系，对区块链和其他前沿科技有深刻的理解，并曾在微软、Hulu 等企业负责过包括搜索引擎在内的多个大型系统工程开发。

技术负责人 - Yupeng Liao

Yupeng 毕业于清华大学，拥有 10 年软件开发和架构设计经验，跟踪记录以构建可扩展且安全的架构，支持 10 亿级日常交易。

产品负责人 - Pillie Wang

Pillie 曾任职于网贷天眼等国内领先的互联网金融机构，拥有 8 年传统及互联网金融产品及后台设计经验，负责的产品曾经每年交易量超过 10 亿人民币。

运营负责人 - Vincent Lu

Vincent 曾任职于小米国际部和 Keep，擅长用户运营和流量运营，曾从零开始搭建团队，开展商业化业务，经历了收入从零到过亿、产品月活从百万到千万的全过程，积累了 A 至 C+ 轮融资的互联网运营经验。

生态合作负责人 - Summer Zhang

Summer 在德勤咨询和玖富集团积累了丰富的金融行业经验，曾在玖富负责战略投资，在区块链行业布局多家公司，并以顾问身份帮助区块链项目进行战略规划。同时，Summer 对东南亚互联网金融行业和产品有深刻的理解，尤其在印尼市场掌握大量消费金融公司资源。

市场负责人 - Lynne Zhang

Lynne 曾任 dApp store 币用宝（已被波场收购）运营合伙人，实现币用宝从 0 到百万注册用户的流量冷启动突破。同时，Lynne 曾担任第一财经周刊市场经理，在传统媒体和区块链媒体方面都有丰富的资源。



顾问团队

Bin Zhang:

- 中诚信征信前董事长兼 CEO，百行征信（即信联）董事会成员。中诚信征信是中国最大的全国信用评级公司之一，百行征信的 8 家股东之一，以及央行审核通过的八家个人征信试点机构之一
- 前联动优势创始人和 CEO。联动优势是中国最大的第三方支付公司之一，合作方及客户包括全国 110 多家金融机构、3000 多家大型企业、70 万家的中小企业用户。联动优势也是 Hyperledger 项目最早的中国地区成员之一

Jason Lu:

- 蚂蚁金服前全球首席风控官，负责蚂蚁金服在全球的欺诈风险控制、加密安全、大数据分析、生物 AI 识别等部门；蚂蚁金服是全球最大金融科技公司，拥有 4.5 亿用户
- Paypal 前全球风控产品研发高级总监，负责其风控技术和数据科学
- 路透、UBS 等多家全球金融机构前风险技术高管，在开发实时金融服务的系统产品方面，有 20 余年的一线经验

Ding Fei:

- Ledger Capital 创始人，Kakao 等区块链明星项目的投资人，帮助币安推进国际化业务
- 前华平投资执行理事，负责中国和东南亚市场 TMT 投资，投资 Go-Jek 等明星项目

Sarah Zhang:

- 曾任 Tim Draper 加速器增长黑客，从 2014 年起接触区块链行业
- 小米生态链企业 Ninebot 机器人业务前 COO，亚马逊前高级产品经理
- 哈佛商学院 MBA，哈佛肯尼迪学院公共政策硕士，任哈佛商学院学生会副主席，肯尼迪政府学院学生会副主席
- 清华大学区块链公开课讲师，中国通信学会第一届区块链委员会委员