Calorie Chain
技术白皮书

为企业政府提供专业可定制区块链解决方案

让区块链商业应用真正安全 隐私 稳定

V1.3

目录

第一章 前言和概述 4

第二章 Calorie介绍 6

2.1 去中心化技术与隐私问题 6

2.2 区块链支付手段的局限性 7

2.3 Calorie Chain框架概述 9

第三章 Calorie的设计 11

3.1 设计原则 11

3.2 实现方案 12

3.3 行星链安全性保护措施 13

3.4 智能合约3.0 15

3.5 获取链外数据源 16

3.6 虚拟机的使用 17

第四章 解决方案示例 19

4.1 供应链 19

4.2 内部专用行星链 19

4.3 游戏领域 20

4.4 教育部门在线课堂版权 20

第五章 激励的经济模型 20

5.1目前现状概括 22

5.2 Calorie的经济网络结构 22

5.3 Calorie的经济设计 23

第六章 路线图 24

6.1 苏格拉底 24

6.2 柏拉图 25

6.3 亚里士多德 26

第七章 初创团队 28

第八章 须知 29

8.1 风险提示……29

8.2 免责声明……30

第一章 前言和概述

区块链技术近年来越来越受欢迎。 它以一种“去中心化信任”的机制，为人类提供了一种全新、高效的合作机制。 区块链在金融和商业领域的应用带来了最多的关注，也是最大的期待。 目前，各种数字货币已经具备了价值传递和价值分配的基本功能，但离现实世界所需要的功能齐全的金融服务还差很远，这也是为什么区块链在金融和商业领域的应用只闻雷不见雨的原因。 为了尽快实现区块链价值互联网时代，人们需要基于区块链技术的新一代基础设施，该基础设施具有完整的金融和商业功能，能够连接不同的社区和代币，能够弥合中心化和去中心化组织之间的鸿沟。融合是包容的，它应该整合目前存在的和未来将推出的加密货币，连接集中和分散的组织，容纳认证机制和匿名交易机制，并引入链上数据和链外数据。

如果你快速环顾一下办公室或家里，你周围的大部分物品，都是通过某种形式，通过不同地区、国家甚至全球供应链而来的。但是这些产品是如何流向你的，你可能一无所知。不仅是你，就连生产这些物品的企业和厂家，也面临着提高供应链透明度的难题。 而这些难题的根本，就在于整个供应链上共享数据的能力非常有限。

几年之前，有一些企业采用了这样的解决方案：在来自全国各地甚至全世界各地的零件上面，贴上专属的二维码。当这些零件抵达目的地，准备进行组装之前，只需扫一扫二维码，就能追溯每个零件的来源和物流信息。这种解决方案，在一定程度上提高了供应链上的信息透明度。但与此同时，这种解决方案，也使生产环境面临着信任危机。因为这一切都可以造假。二维码可以造假，来源可以造假，物流信息也可以造假，因此这种解决方案在实际上并不可取。

除了供应链透明度问题，根据Payoneer公司的2019年全球支付报告，2019年跨境支付流量为209万亿美元。 如此庞大的支付流量导致了高昂的交易和汇款成本，这一成本每年都在增长，预计2025年将达到300万亿美元。 对于较小的交易，通常是中小微企业的情况，这种影响更大。 金融运营研究所2018年9月关于跨境支付前景的调查明确指出，跨境支付交易的高成本降低了利润率。现有的金融支付系统不能完全满足这种日益增长的支付需求，导致全球贸易和经济发展机会的巨大损失，需要创新金融支付机制来补充传统金融。

而区块链技术，就提供了建立一个公共的、分布式的数据库或交易组的方式，这些记录或交易，在本质上是加密安全和不可逆的。 它们在网络的节点之间使用分布式共识机制，以进行或验证对记录区块链所做的任何更改，以确保网络中的节点是同步的，并且始终保证区块链的最新状态。 区块链网络的分布式去中心化特性及其共识机制，确保了系统中没有中心故障点。 由此可以看出，金融的演变与区块链技术之间有着密切的联系。

但与此同时，又产生了一个新的矛盾点。就是当企业和政府想选择一种区块链技术，来解决自己面临的难题时，通常会遇到以下问题：在当前市面上错综复杂的公链中，应该选择哪一条？在错综复杂的数字货币中，应该选用哪种作为支付手段?

的确，目前各种各样的公有链百家争鸣，各种各种的数字货币百花齐放。区块链技术的出现，本身就是为了解决信任危机，但是在目前区块链技术市场鱼龙混杂的情形下，作为企业和政府，应该选用哪一条链，哪一种币，这本来就又带来一种信任危机。因为一条公有链的安全性和稳定性，直接决定了企业和政府数据的安全性和稳定性。同时，一种数字货币在支付时的畅通性，也直接决定了企业和政府在金融支付中资产的安全性。因此，选择至关重要。

而2014年的以太坊，提出了erc20代币的概念，使发行代币变得便捷，政府企业和个人想拥有专属的代币，也不再是难以克服的技术鸿沟。在一定程度上，以太坊的erc20代币解决了政府企业和各个机构，选择某种数字货币作为各自市场流通手段的难题。因为他们已经完全可以发行自己的代币，使用自己的代币作为流通和支付手段。他们无需再在市面上成百上千种数字货币中挑选和抉择，也不用再担心自己选择的数字货币，在未来有没有可能出现各种难以预知的问题。代币概念的出现，让选择区块链技术作为解决方案的政府企业和机构，自己对于流通手段的掌控度大大提高。

但与此同时，这种解决方案也面临着一个问题。代币的掌控权虽然在自己的手里，但是代币是基于第三方公链发行的，说到底还是别人的技术，在使用别人的技术底层时，还是会面临着信任危机。

转眼间来到了2020年，如今的区块链发展更加迅猛，人们对于区块链技术的认可程度更加提升。当企业政府和各种机构，打算采用区块链技术解决自己面临的难题时，就更想对这一技术的掌控度进一步提升，更接近底层。

这时，我们Calorie Chain，一种全新的解决方案便应运而生——“**行星链**”。

行星链，又名并行链。在以往的区块链和公链技术中，只允许用户基于公链发行自己的代币，且代币仅有流通功能。代币的转账操作，完全由所属公链处理和操控，用户没有任何其它权限。而在Calorie Chain中，用户可以在网络上搭建和创造自己的“行星链”，“行星链”之间互相独立，拥有其专属的共识权。此时Calorie Chain就可以比作网络中的那颗“恒星”。“行星”之间有自己特定的运行轨道，互不干扰。

在Calorie Chain之前，若将过去的时代称为“发币时代”。

则如今，“发链时代”，即将到来。

第二章　Calorie介绍

2.1　去中心化技术与隐私问题

随着贸易的全球化和供应链复杂性的日益增加，进一步加剧了信息不对称的程度，使得信息在供应链中参与的利益相关者之间分配不均。当参与的利益相关者来自不同公司，就更没有统一的提供完整信息的激励政策，就更加剧了信息的不对称。

因此，产品的最终购买者没有合适的途径去验证他们所购买的产品，这就为欺诈行为创造了条件。 比如市场上假冒商品泛滥，安全问题，违反劳工标准等等。

供应链不仅仅指生产资料的供应，也包含互联网上的信息数据供应。例如Facebook曾因2018 年3月发生的大规模隐私泄露事件，使得公司市值在短短两天时间里，蒸发了数百亿美元。

互联网之所以会带来信息泄漏，是因为用户的所有数据，都储存在提供网站或者APP的公司的中心化服务器里。并且由这些公司自己的服务器来储存和处理信息。而区块链网络的诞生，就旨在建立一个去中心的平台来储存和处理信息，来保护用户的隐私。但是像比特币或以太坊这类可定制性很低的区块链网络中，作为企业政府和机构在使用这些网络时，没有办法完全根据自身需求区定制功能，这本身就会造成用户隐私泄漏。

举个最简单的例子，若使用比特币或以太坊等可定制性较低的区块链网络来解决支付问题，那或许你的每一笔线下购买记录、网购购买记录，都直接被公布在区块浏览器上，任何人都可以看到，每个人都可以查到你什么时间花了多少钱购买了什么物品。这本身在某种角度上就是一种泄漏用户信息的行为。

区块链网络中数字资产及其交易记录，这其实本身就属于比较私人和敏感的信息，如果对所有人透明，并且无法删改，那么设想一下，当区块链在生活中进行大量的应用落地时，对于绝大多数时候的普通生活场景需求来说，自己的交易和支付信息被公之于众，这无疑是令人难以接受的。

因此，我们可以得出这样一个结论。我们只有特定的需求，需要用到区块链技术去解决，需要实现透明和不可篡改。同时，也有一些场景，我们并不希望做到信息透明，比如以下几种情况。

* 某家公司并不想让竞争对手了解到自己供应链信息；

* 某些富有的人，不希望被外界得知自己的具体财富；

* 基金公司、证券公司等，不希望被其它人看到自己的具体交易记录，防止被别人预测出自己的交易意图，影响操盘和盈利。

在传统的区块链网络中，所有的信息都是透明和不可删改的，这显然和企业、政府和各种机构的实际应用场景相违背，阻碍了区块链技术应用落地的进一步发展。

因此，他们需要一种可定制度高、各种模块可插拔、可按需进行搭建的一个共有网络。Calorie Chain就是这样的一个网络。

Calorie Chain是一个高度模块化的公有链底层，也是非常适合用来二次定制的开发框架。“行星链”可拓展性强，且支持部署自己的共识和应用生态。任何企业、政府和机构，都可在Calorie Chain中进行按需搭建，拥有高度的自主权和掌控权。主链也就是“恒星链”，只负责运行核心功能来保证安全性，而复杂的功能都放在“行星链”上进行开发和运行，既互相独立，同时互相互补。

2.2 区块链支付手段的局限性

在全球范围内，造成贸易与融资发展效率低下的原因，主要是不同企业间的内部系统不衔接，有时需要手工处理，有多个中间人，以及当事方之间的信任环境。

若企业政府想采用数字货币作为支付手段，虽能一定程度上解决上述问题，但也同时会引入其它问题。如：数字货币种类也极其繁多，且绝大多数无法跨链转账。又如：数字货币价格波动大，若交易时间较长，容易在金额上产生纠纷等等。

Calorie Chain为解决以上局限性，从互操作性、可拓展性、可用性三个方面入手改进。首先是互操作性。不同的区块链、中心组织和数据中心中，都对某一事物的价值有着不同的定义。而如果想做到价值统一，就需要公链能够沟通不同的区块链、不同的中心化组织、不同的数据源，并且不仅能够传递价值，还能够运行其它智能合约。 其次是可扩展性，需要能够用于不同的场景，包括金融，制造业和政府管理等等。最后是可用性，需要有资源丰富的生态，需要让多种DAPP流畅运行，让开发者高效开发应用，让用户轻松使用应用。

* Calorie Chain跨链原子交易。

价值网络不仅需要跨链的通信，还需要与现有的中心化机构和外部数据源进行通信。当前区块链还不能与其他区块链互操作（同步其它网络的区块），不同区块链上的代币不能相互交易。且目前区块链无法与外部中心化机构互操作，使得链外资产难以映射到链上。 由于当前区块链无法读取链外数据，这使得当前区块链的“智能”合约变得难以落地应用。以跨链技术为例，跨链交易目前难度极大，更不用说开发跨链智能合约。 目前已经有上千个代币，但每个代币只能在单种区块链上自由移动，只能形成自己的钱包、自己的智能合约等生态系统，现有的区块链生态系统实际上都是孤岛生态，还远未实现真正的互通。

而原子交易技术则为此种现象提供了解决方案。具体实现技术途径将在下一章节详述。

* 智能合约的增强

关于可扩展性，很多链外动作的场景映射到区块链上目前依然很难的。之前通过ERC20等协议，便可以在公链上进行ICO项目。但金融、实物资产，投资的各种衍生品仍难以映射到区块链上。并且很多离链交易场景，只要涉及到繁重的计算，离链数据的需求仍然无法映射到区块链上。许多项目正在进行相关的努力，但由于缺乏高效的跨链通信解决方案，这一进程受到严重阻碍。

对此，Calorie Chain增强了主网上的智能合约，实现了多方数字资产之间的应用，并且具有多种触发机制以有效获取链外数据的输入，以嵌套的方式或并行的方式调用多种其他智能合约，提升了可拓展性。

* 模块可插拔性

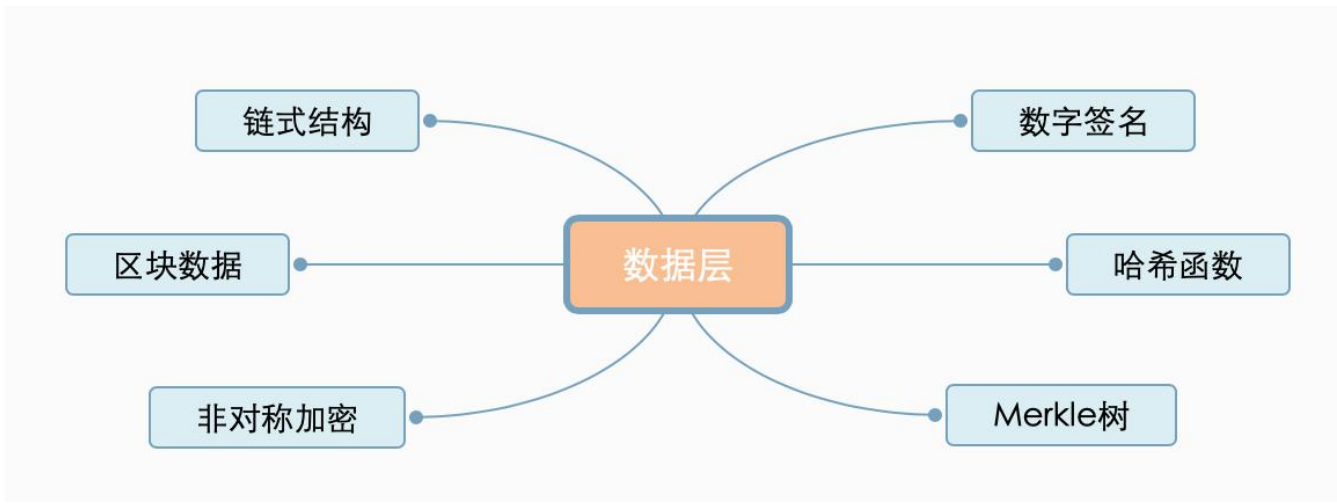
根据之前章节的讲述，要想使区块链技术真正应用到现实生活中，区块链网络就必须拥有高度的可定制性，必须根据具体的应用场景进行具体的分析和具体的开发。在Calorie Chain网络中，将主网分为六大模块： wallet、p2p、block、store、mempool以及rpc。开发人员可按需进行选用和组合，实现自己的实际需求，极大提升了区块链技术在实际生活中的可用性。

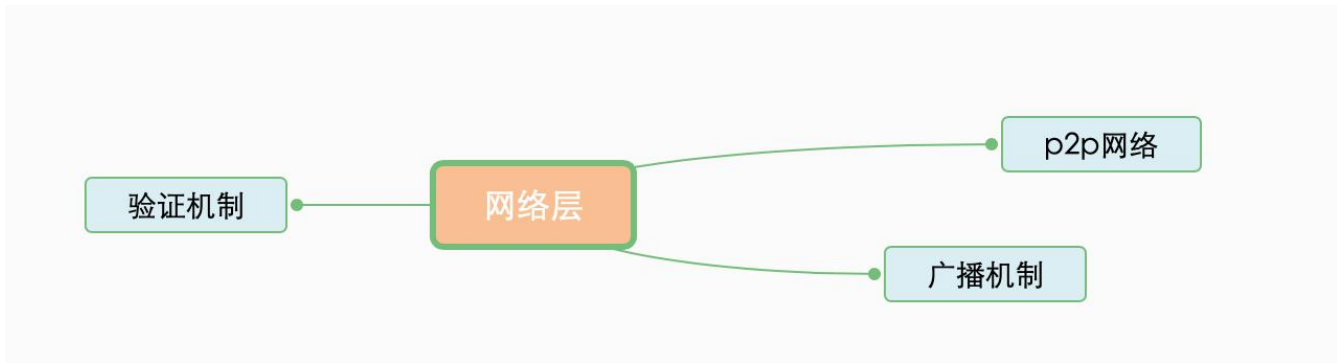
2.3 Calorie Chain 框架概述

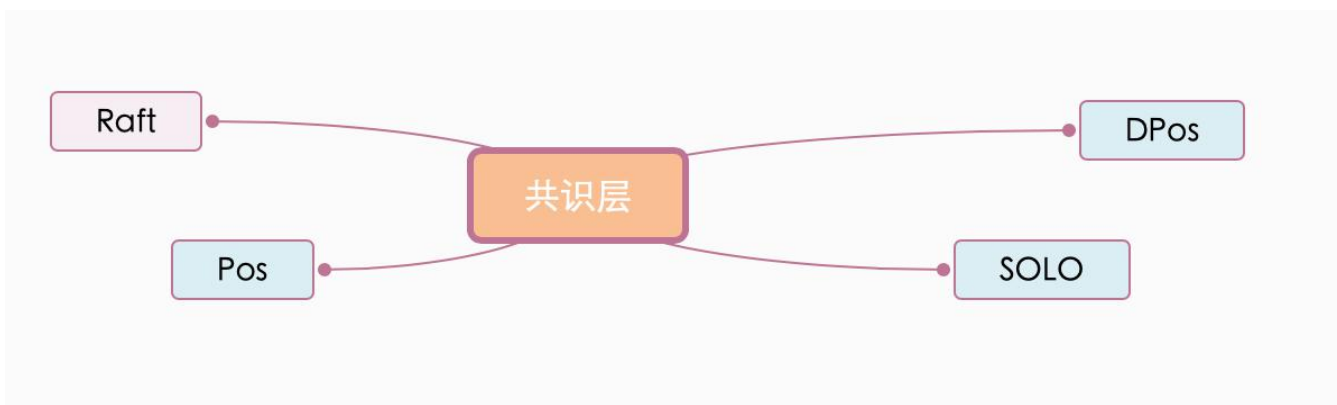
Calorie Chain使用Golang开发。

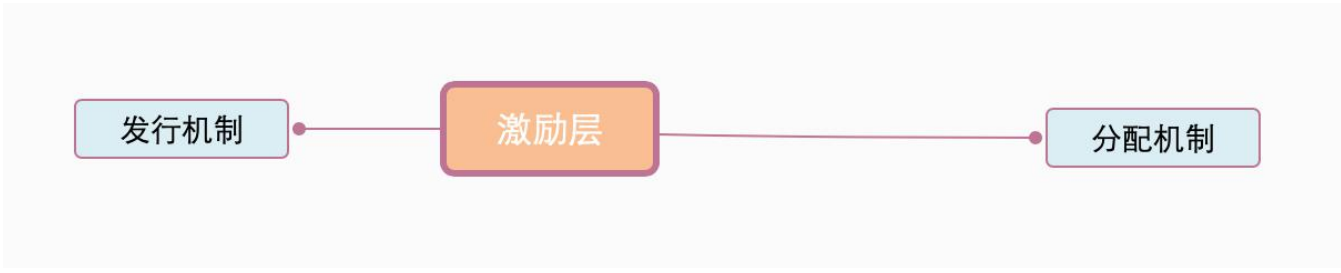
架构如下图所示

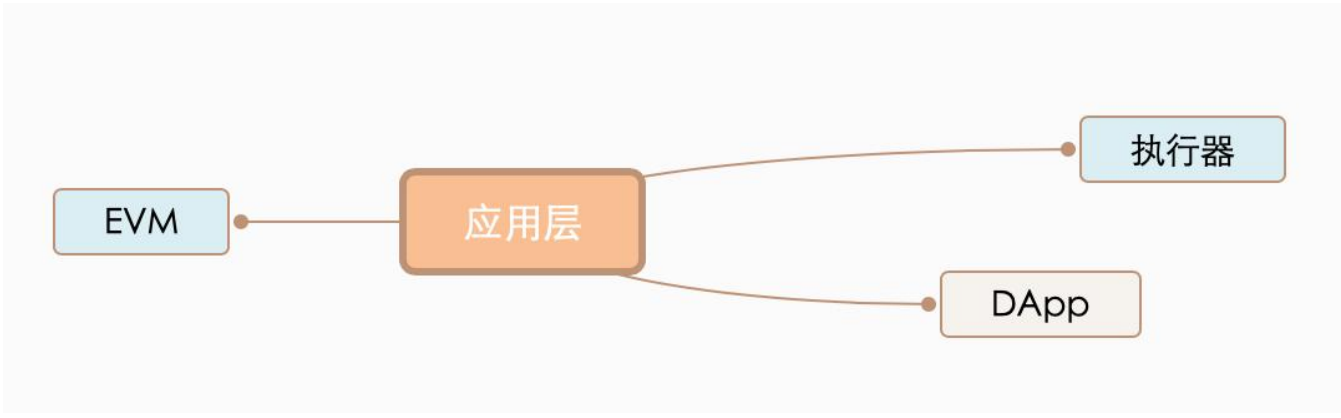
应 用 层
激 励 层
共 识 层
网 络 层
数 据 层








发行机制
激励层
分配机制


EVM
应用层
执行器
DApp

第三章 Calorie的设计

3.1 设计原则

从以上分析我们可以看出，区块链的兴起让人们看到了互联网的前景，区块链在一定程度上代表了互联网的未来。 然而，互联网在互操作性、可扩展性，可用性等方面仍存在瓶颈，使得当前的区块链网络难以支持跨链价值转移、跨链智能合约或跨链应用程序。

由于区块链网络资产是以代币的形式呈现的，只要能够实现多代币智能合约，就可以极大地增强区块链网络的互操作性，并且使可扩展性变得更加容易。目前的跨链技术一般是侧链技术，通过双向打包将交易移至侧链，然后通过多重签名实现从侧链的退出。这样的途径只能实现同网络转移，并且性能一般。

而如果采用“行星链”（即并行链）解决方案，只在“恒星链”（即主链）上运行核心功能，而虚拟机、智能合约等复杂功能放在“行星链”上去解决，不仅可以减少数据处理量，“行星链”还能拥有完全的区块链生态。

区块链网络上的经济活动才刚刚开始。 虽然近年来加密货币已经开始渗透到生活的方方面面并迅速增长，但其总价值只有区区几千亿美元，与现有的全球金融规模相比，可谓杯水车薪。 全球的土地和房地产市场、股票市场、商品市场、外汇市场、债券市场以及各位衍生品市场，总市值可以是几十万亿，几百万亿，甚至上千万亿。

行星链技术可极大减少数据上链的成本。一旦完整的区块链生态形成，链上的数据就会更加多元。只需要在并行链上设计好流通的token，更多的数据就能映射到区块链网络上。大量有价值的事物，如土地、房屋、艺术品、智力劳动等有价值的东西，如今仍然没有很好地在链上表现出来。 而随着并行链的和“代币化技术”的不断发展，资产代币化将成为一个全新的产业，越来越多的价值将在链上流通。

3.2 实现方案

以跨链技术为例，跨链互通目前难度极大，更何况开发跨链智能合约。 目前已经有上千种token和coin，但每种代币只能在单条公链上自由转账，形成自己的钱包、智能合约开发工具等生态系统。

现有的区块链生态系统实际上都是孤岛生态系统，区块链网络的价值还远未实现真正的互通。

* 跨链原子交易（以跨BTC网络为例）

（1）启动锁定请求

用户A通过使用钱包中的锁定接口向Calorie发起10个BTC锁定请求。

（2）启动私钥

锁定请求操作触发启动锁定智能合约，进行私钥初始化过程。所谓私钥化，就是以分布式的方式生成一个私钥。在此过程中，智能合约将完成密钥分片和密钥碎片的分布式存储。私钥的初始化为以后密钥的存储和使用奠定了基础。

（3）将记账权交给节点管理

此后将在比特币网络上生成一个地址，用户A将把他的BTC转移到此地址。用户转移操作将由Calorie的接口初始化一个广播，Calorie节点检查转移的完成情况。

在收到交易广播后，行星链上的节点会通过接口检查交易是否在比特币网络上得到确认。如果结果显示成功地将10个BTC转移到锁定生成的地址，则将记账权移交给节点管理。

（4）映射token

在确认记账权转移后，智能合约会在Calorie上更新用户A的账户状态。锁定记录将被节点打包并记录在行星区块中。此时，完成对用户A的10个BTC锁定请求。

同样，用户锁定请求也是通过调用相关程序接口在钱包中发起的。 用户使用钱包的体验类似于任何代币转账。 锁定实施过程具体步骤如下:

（1）启动锁定请求

用户A操作钱包向Calorie之外的比特币地址发起10BTC的转账交易，这将被视为锁定请求。

（2）检查，锁定，生成交易记录

交易触发Calorie上的锁定智能合约。 该合约将首先检查用户A在Calorie上的资产状态，

并锁定用户A在Calorie账户中映射的10个比特币的状态，然后生成一个带有用户A签名的交易请求以寻址。

（3）节点签名

行星链上的节点接收到事务请求，并开始根据其存储的密钥碎片进行计算和比较。如果结果是肯定的，节点将签名并广播结果。

同时，每个节点收集签名。当交易签名达到3时；交易由节点发送到比特币网络，10BTC交易的转移就完成了。

（4）分解节点控制权

Calorie上的节点会通过比特币对应的接口检查交易是否在比特币区块链上得到确认。 在达成交易共识确认后，用户A的10BTC将节点控制权中被拆解。

（5）释放token映射并销毁

智能合约会同步用户在Calorie账户上的状态，释放被锁定的10个BTC映射，并销毁映射。 同时，锁定记录被打包到行星区块中。此时，用户的锁定请求完成。

参与跨链发起交易、确认交易和验证交易签名的节点，都将按照给定的激励机制获得相应的奖励。

3.3 行星链安全性保护措施

账户系统

账户系统私钥的使用是通过分布式密码计算实现的。 当一个事务签名验证被广播时，节点可以根据它所保存的碎片来计算和比较它。当验证成功时，节点签名并广播其分片的验证结果。

目前，Calorie团队通过代码分析得出结论，hash256和椭圆曲线算法能够支持私钥分片和分布式计算。对于一些原链，在算法不支持分片计算的地方，会考虑采用同态加密的方法来实现密钥的计算，而不会泄露密钥。

共识系统

共识算法的安全性取决于生成每个块的节点的随机性。当恶意节点通过控制算力无法获得连续区块的生成权时，共识算法的安全性就可以得到保证。

Calorie对记账权的随机性设计类似于“彩票”，即通过一定的算法，将大量“开奖”的随机性赋予“中奖”节点的过程，保证每个节点的结果都是不可预测的。这种共识机制被称为“PoS”。

下面是选取记账节点使用的方法:

首先若想成为拥有记账权的节点，节点账户中必须存有Calorie Coin。参与记账的节点是基于PoS共识算法生成的，持有币量更多、持币时间更长的节点更容易成为记账节点。

然后对节点进行分组，通过计算前一个区块的hash值和另一个输入值来生成结果，之后通过一个预设的函数进行分组。 分组过程是一个随机过程，与持币量和币龄无关。

最后根据算力选出打包节点。PoS机制鼓励记账权竞争者拥有一定的算力，但不鼓励他们拥有过多算力。同时，该机制保证了打包节点生成的随机性。当然，掌握网络最高算力的节点会有更多机会，但因为随机性仍然难以保证频繁“中奖”。

综上所述，尽管一个节点为了实现更多的记账机会而花费一定成本保持其股权或增加其股权，但并不能保证其“中奖”的机会维持在一个固定值。 同时，我们通过调整组数，通过我们的随机化和分布式机制，对于没有持有大量权益或拥有绝对算力优势的节点，仍然有足够的机会获得记账权。 这样，更多的节点往往会得到更理性的对待，最终，节点大多处于平均状态。 并且，随着网络节点数量的增加，这种平衡不会有任何显著的变化。

因此，Calorie Chain将始终保持高度的随机性。

高度的随机性还可以体现在第二步的分组上。假设A组中的节点想要得到B组交易的打包权。那么首先它将面临与B组节点的竞争，并且不能保证该节点在竞争中一定能够胜出。并且即使该节点成功成为B组的获胜节点，当B组交易提交给A组之前，会先提交给特定的智能合约，会被合约踢出并丢弃。

因此，在这种情况下，A节点做了一个无用的努力。 同样，一个恶意节点也无法以这种方式控

制连续的两个区块来执行一次恶意分叉。

同时，Calorie又进一步增加随机性。 特定的智能合约可以将n个组中的一个组设定为游走节点，将所有交易分成n+1个组。 所谓游走节点，就是这些节点被赋予了选择任何一个组加入的权利。

假设整个网络中的节点本身都是诚实节点，游走节点的存在必然会进一步增加节点记账权的随机性，导致结果更大的不确定性。

这些不确定性，增加了恶意节点通过攻击该节点来获取打包权所需付出的代价，而且即使获得了前一个块的打包权，也不保证能够获得下一个块的打包权。要攻击和控制太多的节点是非常困难的，因为节点的数目至少等于组的数目，而这已经是一个非常大的数目，将引起整个监控系统的关注。

分层系统

分层系统体现在打包区块的工作中。它将其分为两个阶段，分别对应着两层的处理。

第一层是应用程序执行层，它记录应用程序的执行结果并提交给第二层。 第二层是区块生成层，将第一层提交的结果打包，形成链上的区块记录。

在第一层即应用计算层，由行星节点完成当前所有事务的处理，以实现当前所有事务的并行计算。 此外，事物的处理权，由每轮随机选择的节点进行打包，从而增加了算法的安全性和扩展性。

3.4 智能合约3.0

资产代币化实际上是将链外价值转化为数字资产，同时使这些资产去中心化、数字化和可编程化的过程。 而代币化的过程以及代币在区块链网络上的整体交易，都属于加密金融的范畴。

加密金融最重要的特征是资产和价值主要表现在区块链上，其产权主要由私钥控制，交易活动主要通过区块链上的智能合约完成。

由于智能合约的优越性，它将对现有的金融运行方式产生冲击。 链外资产将被代币化，变为加密金融资产，智能合约可以调用不同地址中的“加密数据（余额）”，因此智能合约可以相互嵌套来表达复杂的金融逻辑，并形成传统金融无法实现的应用。

跨链智能合约调用规则

在Calorie Chain网络里的智能合约的代码中，增加了调用其它公链智能合约的预置条件判断和预置条件规则，并创建了目标智能合约地址索引的参数。 条件判断的依据来自于Calorie智能合约被触发时数据的输入以及对数据进行计算的结果。 如果满足预设条件，节点将下载其它公链智能合约并执行。

对调用条件的描述有两个部分:规则和定时。规则是事先写在智能合约中的计算函数。 定时条件可能是智能合约中的预设条件，也可能是定期检查智能合约状态的实时条件。

跨链智能合约调用过程

假设Calorie网络中智能合约为A，其它公链中的只能合约为B。

i.当智能合约A被触发时，它会根据预设的调用条件，判断是否需要执行智能合约B。

ii.当满足调用条件时，执行预设的计算函数，计算的结果将作为智能合约B的输入。

iii.执行过智能合约A的节点将智能合约B下载到本地，输入上一步计算的数据作为智能合约B输入的数据，开始执行智能合约B。

以上步骤可以完成智能合约A对合约B的调用，由于智能合约B是基于智能合约A的状态作为触发器和输入数据，所以我们将它们之间的逻辑关系称为智能合约的衔接调用。

Calorie提出的智能合约3.0，不仅在其合约内根据自身的逻辑做出判断，还会通过预设的条件调用其他智能合约。 通过这种方式，就可以在不同的智能合约之间构建网络状的调用关系，它为建立相互关联的金融应用程序以及其它复杂应用程序提供了可能性，可以通过智能合约之间的衔

接调用构建复杂的金融和供应链服务。

3.5 获取链外数据源

链外数据源接口调用

智能合约3.0在触发条件上，也可以使用链外数据。 通常，这种数据获取是通过第三方提供的标准http或基于SOCKS的API进行的。 例如，一个第三方接口调用函数，通过http获取目标URL的地址，并得到一个JSON数据包。

这种接口方法也适用于Calorie来获取其他区块链上的信息，例如查询和确认另一个链上的某一笔交易是否被所在区块确认。同样也可以用于传输第三方数据，例如股票指数，足球比赛结果，天气数据等。

Calorie智能合约3.0将利用基础数据来识别第三方接口，并形成相应的第三方接口供智能合约调用。

在以往的区块链落地应用中，需要解决以下几个核心问题：

怎样能保证数据的真实和一致性？当出现不一致的时候以哪个为准？当需要读取数据时，是走链上，还是链下？什么数据上链，什么数据不上链？

根据以上问题，在Calorie网络中，两端都将数据做一次hash，可以快速对比是否数据一致。同时前端通过链上，后台通过数据库，前端是为用户提供服务的，所以要走链上数据，后台是管理的，可以直接走数据库，然后保证数据库与区块链数据一致。

最后共享数据上链，私有数据不上链，在并行链链系统中，需要共享给其他成员数据时，之前只能采用 Api接口，而有了区块链技术后，就更好地解决了资源共享问题。

如需记录多媒体数据，如图片、音频与视频等，可以将它集成到采集终端上，然后异步上传到去中心化的分布式文件系统中。去中心化的分布式文件系统能实现，将每一份图片或者音频对应着独一无二的hash值，之后便可通过hash值访问图片，图片被同步到相邻节点实现去中心化。如图片被修改，则hash值会随之变化，数据随之无效。

多种类触发识别

现有的智能合约只能被动地等待交易的触发，只能由链上交易执行。Calorie加入了链外信息的关键词识别触发功能，相关的智能合约将由多个触发器自动运行，使得智能合约能够在不需要人为的情况下陆续被激活。 因此，多方可以通过智能合约的代码相互信任，完成各种复杂的金融功能。以借钱参与ICO的应用为例，Calorie智能合约可以通过编程实现借代币，还新币和支付利息。 以基金应用为例，Calorie平台上的智能合约可以自动管理一笔基金，将各种代币投资各种数字资产，产生管理费，支付分红等，同时可以接受保证金，并通过外部数据源的触发器实现调整保证金、清算结算等功能。

3.6 虚拟机的使用

在编程语言方面，Calorie使用的是go语言，开发者可使用go语言进行现有智能合约的快速移植。

今后我们还会提供不同语言的编译器来支持更多的智能合约。

在虚拟机方面，由于Solidity是目前开发智能合约最常用的语言，因此Calorie最初使用EVM来兼顾兼容性。

从长远来看，我们将使用JVM中更多的开发资源。同时，对于暂时无法熟练使用区块链虚拟机的开发人员，我们也提供了封装好的java、php、python等常用语言的接口，供开发人员前期调用，以便更快地上手。通过这种方式吸引越来越多的开发人员加入Calorie的开源社区，共同打造应用生态，促使更多的精品DApp落地应用。

第四章 解决方案示例

4.1 供应链

物流企业正面临着一个前所未有的变革时代，数字化正在占据主导地位，客户的期望也在不断提升。 区块链技术正在实现更高的效率和更便捷的协作模式，保证了交付时的真实性，确保透明度并提供即时结算的功能。

利用Calorie Chain，可以在供应链的参与方之间，使用预先根据支付条款制定好的智能合约进行协作。 可使用物联网和其他实时监控技术跟踪交付情况，并可实时更新访问状态。在成功交货后，智能合约可以根据约定的付款条款同时向所有供应链参与者发放付款。 使用区块链，各方可以确保交货和付款的透明性。通过透明的智能合约及时向物流服务商付款，运输成本可以降至最低。评级系统可以进一步提升智能合约解决方案的实用性，可以跟踪供应链参与者在一段时期内的真实表现。

除此之外，所有员工记录都可以保存在公司、银行和选定供应商之间的指定账本上。 使用区块浏览器可以在任何时候实时查看交易，从而消除了从供应商处获取所提供服务的每日报告的需要。 当员工的请求和供应商响应中的识别字段达成匹配时，交易被批准并上载到区块链上，也消除了人工对账的需要。 这种安全和简化了的流程最大限度地减少了人工干预和处理成本，可以为客户节省大量费用。

4.2 内部专用行星链

公共区块链和公有链的缺点之一就是信息的绝对开放性，这意味着交易的隐私性很差。很多时候企业和政府部门，只需要交易数据对内部绝对透明，同时对外部绝对保密。

公共区块链和公有链的另一个缺点就是需要大量的算力来实现共识。 这些因素使得它们不适合商用和政用，特别是涉及支付和结算的用例。

Calorie的行星链可定制性很高，企业和政府部门可以通过行星链创建私有网络。 通过创建专用私有网络，能够让内部人员进行安全和私密的连接， 能够让在私有网络下进行的交易不为外界所见，从而使敏感的金融信息和交易信息绝对地安全和保密。 例如，银行机构可

以用区块链技术简化对账流程和业务流程，包括支付服务、融资贷款组合、资产融资、股权等等衍生工具和其他复杂产品。银行内部可以共同使用一条行星链，该链只对内部人员开放读取和记账权限。虽然数据和状态变化都记录在区块链网络上，但内部人员之间的任何交易，外界都不可见。

4.3 游戏领域

网络游戏领域，是目前最需要公开化和透明化的领域之一。很多对游戏了解的人，都玩过“私服”，也就是私人搭建的服务器。在私服里，管理员可以任意修改游戏里人物的属性和金钱，也可以任意修改怪物的属性，权力高度集中。

同样，即使不是在私服里玩游戏，而是在官方推出的服务器里。这种“暗改”的现象，也屡见不鲜。

比如，服务器里可能会有内部人员，俗称“托”，管理人员能够偷偷修改他们游戏里的金钱余额，来达到刺激真实玩家充值的效果。再比如，游戏的管理员，为了达到某种目的，也经常会偷偷暗改游戏难度，比如增加怪物的攻击、血量等等。

总而言之，游戏领域的权力高度集中化，对于玩家非常不公平。

但是，游戏领域，也是非常适合用区块链技术去解决痛点，比如人物属性、包裹金额、怪物数值等内容就非常适合上链，来保证数据的透明性和公开性，提升对于所有游戏玩家的公平性。

如今，Calrorie的并行链，又可以把区块链技术更好地应用在游戏领域中。通过创造多条不同分工的并行链，可以实现掉落装备立即上链、人物升级立即上链、人物状态改变立即上链、目前通过了的关卡层数实时上链等.....这将完全保证所有玩家的公平，没有任何中心化的管理员可以暗改数据，同时也不可能存在玩家恶意攻击中心服务器来篡改数据。

4.4 教育部门在线课堂版权

网上课堂和在线教育是一种趋势，据2018年Youtube统计，有73%的中小学生都使用在线教育听过网课，平均每月观看网上课程的时间超过50小时，每年花费在网课上的费用平均超过200美元。在线教育平台是即将到来的风口，即将迎来爆发点。

但是与之相应的，是网上课程的版权问题。盗版现象十分严重，一套网课，被转手一层层上传到不同的在线平台多次，很难追溯到原作者是谁。并且同样一套网课，不同平台价格差距大。这使得教育部门无法高效率地规范和管理网课市场，错失了拓宽当地学生们学习渠道的途径，网上教学资源和用户需求严重不符。

而Calorie的行星链解决方案，可以为当地学生指定使用的每一个网课平台分别搭建一条行星链。每一部原创的网课视频，都会有唯一与之对应的hash值。当这部视频首次上传到某条行星链时，hash值便会被恒星链记录，上传者将获得一定数量的token作为激励。当同一部视频被上传多次，恒星链检查到重复的hash值，便会通过智能合约驳回将视频上传至行星链的请求。同时，学生们也是通过支付token的方式购买网课，token实时按照一定的奖励分成转入网课原作者的区块链钱包中。比例分成写死进智能合约，任何人无法修改，也从根本上杜绝了平台私扣工资或拖延工资的行为，从而激励更多网课创作者上传更多高质量网课。

第五章　激励的经济模型

5.1　目前现状概括

若把市面上的绝大多数公链比作一块商圈，则它们首先做的，就是划定自己商圈地皮的范围。但是经过一段时间后，地皮上并没有什么建筑、商场或者娱乐设施，十分荒凉。

而Calorie的经济模型，则是首先在地皮上建设建筑、商场和各种娱乐设施，等到这些设施建造起来之后，商圈的范围就会自然而然地形成，甚至是无限地往外延展。

5.2　Calorie的经济网络结构

一个理想的区块链经济模型，应该包括了公链和Coin并由多个层次组合而成。Calorie运用了“行星链”的理念，致力于打造一个可信网络。Calorie的网络结构主要分为三大层，分别为信任层（账本层），构建层与合约层，同样每一层都有着对应的经济模型。

1. 信任层：信任层即账本层，对外提供最基础的共识服务，比如行星链的每笔交易将会做两次共识，第一次在主链，第二次在并行链本身，因此行星链的安全性由其并行链和主链保证。其中在做第一次共识时，将会消耗Calorie作为代扣手续费和燃料，这将会增加Calorie的稀缺量和需求量。

2. 构建层：构建层主要包括虚拟机服务和并行链搭建服务。并行链在发行时，为了防止日后产生恶意分叉的情况，需要提交一定量的Calorie作抵押。

3. 应用层：应用层主要包括各种智能合约和去中心化PaaS，同时可对外提供封装好的交易接口，加快Calorie的流通和交易频率。

Calorie网络通过以上三层架构，为现实中的政府和企业计算提供可信的服务平台和生态系统。

5.3 Calorie的经济设计

Coin名称：calorie

共识机制：PoS

发行总量：1亿

出块时间：6s

爆块奖励：6calorie

区块减半高度：9413191

- 从Calorie生态建设的角度，因为区块链提供的平台是一个公平的价值流通平台，所以在平台上产生经济行为的成本仅有交易成本，在Calorie Chain上产生经济行为时，消耗的就是calorie。calorie币100%完全由矿工挖矿获得，人人参与机会平等，并保证绝对公平。

第六章 路线图

我们以古代最著名哲学家作为版本发布代号。
他们在自己的领域之中，凭借着专注的精神和执着的习惯，为世界作出了伟大贡献。

6.1 苏格拉底

此阶段为Calorie的第一阶段，主要围绕着底层技术和公链技术开发展开。

2019.3 Calorie 测试网络发布

* 完成Calorie主链底层架构
* 支持Blockchain、共识、逻辑执行器、p2p、Mempool、状态树储存、列表储存、rpc等区块链底层支撑模块
* 支持共识协议可插拔，使Calorie既是个公链系统，也可以作为联盟链和私链
* 支持多种执行器，有系统自定义，也支持用户可拓展

2019.5 Calorie 正式网络发布

* 支持将以太坊EVM虚拟机融合进Calorie系统，支持多种储存方式，数据库可插拔
* 支持交易隐私保护

2019.9 行星链测试网络发布

* 支持行星链技术，并支持主链和行星链跨链，以及行星链之间的跨链资产交易。

* 智能合约代缴手续费

2019.11 行星链正式网络发布

* 支持将wasm虚拟机融入行星链

* 实现Saas和Lass的基础框架

6.2 柏拉图

本阶段为Calorie的第二阶段，主要围绕着生态建设和社区建立展开。

全球化节点部署

* 核心代码github开源

* 可挖矿钱包上传github供用户下载及部署

* 初步形成全球矿池规模

开源工具包上线

* 支持可视化引导式发布token

* 支持用户引导式部署私有链及行星链

* 原子交易（去中心化闪兑）功能上线

* 去中心化聊天功能上线

生态软件上线

* 支持实现供应链金融SaaS平台和IaaS系统，打造供应链金融完整生态软件

* 实现和挖掘Calorie商用价值，商用并行链达到10条以上

* 与多家中心化组织和数据源合作，将多家链外数据提供商的数据写入链上，让越来越多的价值得以在平台上运行

接口标准化

* 通过发起“区块链接口标准化运动”，解决Calorie网络在互操作性上的瓶颈。

* 通过接口标准化，可完全实现Calorie与其它公链的跨链交互，实现Calorie智能合约与其它区块链网络智能合约的互相调用，极大提升Calorie在实际落地应用上的可用性和可拓展性。

6.3 亚里士多德

本阶段为Calorie的第三阶段，主要围绕着未来区块链技术发展的前景展开。

并行链产权登记平台

* Calorie在使用区块链技术上的最大优势，在于其并行链技术上登记信息的便捷性和低成本性。每一类需要登记的信息和产权，都可以搭建一条并行链区去登记和记录。社会上的产权类型一直都因为登记成本的存在，而受到严重制约。若通过Calorie并行链技术，把登记的成本压到极低甚至降为0，此后定将出现很多新的产权类型出现并登记于链上，产权类型的不断丰富与扩张，提高了人类的“智力”劳动地位的进一步提升，不仅为人类社会做出贡献，甚至可能改变经济运行的模式。

混合区块链架构

* Calorie混合架构建立在联盟区块链的范例之上，它不同于传统的私有/联盟区块链以及公共区块链。 Calorie混合网络的公共状态有不同类型的组成部分，由所有参与节点共享。 节点组可

* 以进一步形成具有自己的私有状态的网络，该私有状态仅对授权成员访问。私有网络状态在其各自的网络中维护，但是交易和智能合约的记录（散列）被存储在区块链的公共状态上。公共状态可用于跨Calorie网络安全透明地共享其他数据，而私有状态可以用来保护敏感

* 数据和金融数据不受外界干扰。Calorie混合架构可以彻底解决区块链的透明化与匿名私有化的矛盾。

第七章 初创团队

Bernoulli区块链智能实验室

Bernoulli Blockchain & Intelligence Lab.

实验室是由来自学术界与工业界尖端人士组建的一支科研团队。实验室成立于2015年，成立以来长期致力于研究基于区块链的安全解决方案和基于区块链的应用系统研发，同时担任着多家企业网络计算和物联网的设计工作，已落地多个区块链应用场景并积累了丰富的区块链技术实现经验。

Bernoulli区块链智能实验室于2018年利用区块链开放平台，成功将智能泊车系统与区块链技术相结合，通过去中心化的方式，将车位数据上链，终结了以往只能通过第三方机构储存数据和调用数据的弊端。保证了平台内车位的真实性和泊车成功的准确性，并使泊车数据可溯源。

实验室同时兼顾学术的科学研究与技术在产业的可用性，在进行深层次理论研究的基础上，完成实际应用的实现。实验室利用大数据和区块链技术进行驱动，长期探索金融和数据科技的变革和创新。

第八章 须知

8.1 风险提示

系统性风险:是指由于全局性的共同因素引起的收益的可能变动，这种因素以同样的方式对所有证券的收益产生影响。例如政策风险，目前国家对于区块链项目的监管政策尚不明确，存在一定的因政策原因而造成参与者损失的可能性；市场风险中，若数字资产市场整体价值被高估,那么投资风险将加大，参与者可能会期望项目增长过高，但这些高期望可能无法实现。同时，系统性风险还包括一系列不可抗力因素，包括但不限于自然灾害、计算机网络在全球范围内的大规模故障、政治动荡等。

监管缺场风险：包括Calorie在内的数字资产交易具有极高不确定性,由于数字资产交易领域目前尚缺乏强有力的监管，故而电子代币存在暴涨暴跌、受到庄家操控等情况的风险，个人参与者入市后若缺乏经验，可能难以抵御市场不稳定所带来的资产冲击与心理压力。虽然学界专家、官方媒体等均时而给出谨慎参与的建议，但尚无成文的监管方法与条文出台，故而目前此种风险难以有效规避。

监管出台风险：未来可能会有监管条例出台以约束规范区块链与电子代币领域。如果监管主体对该领域进行规范管理，所购买的代币可能会受到影响，包括但不限于价格与易售性方面的波动或受限。

团队间风险：当前区块链技术领域团队、项目众多，竞争十分激烈,存在较强的市场竞争和项目运营压力。Calorie项目是否能在诸多优秀项目中突围，受到广泛认可，既与自身团队能力、愿景规划等方面挂钩,也受到市场上诸多竞争者乃至寡头的影响，其间存在面临恶性竞争的可能。

项目技术风险：首先,本项目基于密码学算法所构建，密码学的迅速发展也势必带来潜在的被破解风险；其次,区块链、分布式账本、去中心化、不可篡改等技术支撑着核心业务发展,TRON团队不能完全保证技术的落地；再次,项目更新调整过程中，可能会发现有漏洞存在，可通过发布补丁的方式进行弥补,但不能保证漏洞所致影响的程度。

黑客攻击与犯罪风险：在安全性方面，单个支持者的金额很小，但总人数众多,这也为项

目的安全保障提出了高要求。电子代币具有匿名性、 难以追溯性等特点，易被犯罪分子所利用，或受到黑客攻击，或可能涉及到非法资产转移等犯罪行为。

目前未可知的其他风险：随着区块链技术与行业整体态势的不断发展， Calorie可能会面临一些尚未预料到的风险。请参与者在做出参与决策之前，知晓项目整体框架与思路，合理调整自己的愿景，理性参与。

8.2 免责声明

本文档仅作为传达信息之用，文档内容仅供参考，不构成在Calorie的任何投资买卖建议。

本文档内容不得被解释为强迫参与。任何与本白皮书相关的行为均不得视为参与 ,包括要求获取本白皮书的副本或向他人分享本白皮书。

参与项目则代表参与者已达到年龄标准,具备完整的民事行为能力

社区将不断进行合理尝试,确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。团队概不承担参与者因依赖本文档内容、本文信息不准确之处，以及本文导致的任何行为而造成的损失。

团队将不遗余力实现文档中所提及的目标,然而基于不可抗力的存在，团队不能完全做出完成承诺。

Calorie作为Calorie Chain的官方代币，是平台发生效能的重要工具，并不是一种投资品。Calorie作为在Calorie Chain中使用的加密代币，均不属于以下类 别： （a）任何种类的货币； （b）证券;（c）法律实体的股权； （d）股票、债券、票据、认股权证、证书或其他授与任何权利的文书。

Calorie的增值与否取决于市场规律以及应用落地后的需求，其可能不具备任何价值，团队不对其增值做出承诺并对其因价值增减所造成的后果概不负责。

在适用法律允许的最大范围内,对因参与项目所产生的损害及风险，包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失，本团队不承担责任。

Calorie平台明确向参与者传达了可能的风险，参与者一旦参与项目，代表其已确认理解并认可细则中的各项条款说明,接受本平台的潜在风险，后果自担。

Calorie Chain