INT：一种通过经济驱动改良物联网设备互联的方案

Abstract: INT will build a framework, based on which a cellular network is made of machines, and create a token, which will be used to coordinate the resource exchange between nodes and heterogeneous links (different nodes may create independent internal links). For example, a node may make a request and pay corresponding tokens to request other nodes (or links) to provide power, network, data, service and other possible resources. In addition, through zero knowledge proof(specific improvement is necessary), optional masking may be conducted to protect user privacy.

摘要：INT 将构建一种架构，让机器形成蜂窝式连接网络，并构建一种代币，用于协调节点与节点之间及异构链路（不同的节点可能形成独立的内部链）的资源互换。一个节点，可以在提出请求，付出相应的代币，请求其他的节点（或者链路）予以电力、网络、数据、服务等其他可能的资源提供。并且，通过零知识证明（需要进行特定的改进），对用户数据进行脱敏，保护用户隐私。

1 前言

当前物联网领域虽然快速发展，然而，各家厂商的通讯标准，数据交换标准、厂商利益、用户隐私、碎片化的模式制约着整体的发展。预计 2020 年将有超过 250 亿个节点接入网络，然而，如果无法打通整体网络之间的互联互通，碎片化物联网，是无法体现最大价值的。

通过定义一套通用的协议标准寻求各家厂商支持，这样的可能性并不是没有，但是低效，而且代价高昂。能否通过去中心化的方式，以及经济驱动，让各个标准之间互联互通，是我们试图在找寻的一种新的可能性。

1.1 项目目标

INT 是 Internet Node Token 的英文首字母缩写，INT 原义为 IoT Node Token，但我们认为物联网将快速发展为如同今天的移动互联网，将成为 Internet 的一部分，因此我们更改 INT 定义为 Internet Node Token。

INT 试图建立一套方案，在一个非信任的去中心化机器联邦中，允许数据、资源自由地流通并且保证用户的隐私。

本文并不是一个完整的形式说明书，只是一个预览版的开发意图定义，尝试提出解决方案，并且通过概念性实验，以及社区的支持，验证性开发，让 INT 落地。通过实验性的证据、原型和数据，以及对社区意见和评论的响应，本文的内容在后期将会有大量的修正。

1.2 背景介绍

区块链技术已经在金融等领域证明了自身的价值，然而其实它还有一个更加适合的领域——物联网。高度分散，高度去中心化的物联网领域特别适合区块链的应用。

目前物联网领域存在以下几个缺陷

（1）缺乏标准

物联网厂商目前各自为阵，形成一系列数据孤岛，信息流极不通畅，跨厂商接入和清算是一个很大的问题。

（2）效率低下

当前物联网生态体系下，所有的设备都是通过云服务器验证连接的。设备间的连接都要通过中心服务器处理，效率无法满足物联网的实时需求。

（3）成本昂贵

中心化云服务器、大型服务器和网络设备的基础设施和维护成本非常高。在物联网设备的数量增加到数百亿后会产生巨量通信信息，使物联网解决方案非常昂贵。

（4）安全隐患

中心化网络对中心服务器的安全性要求极高，中心化服务器出现安全漏洞将会对整个网络中的节点产生影响。

（5）隐私保护

现有中心化网络可以随意收集用户隐私，在用户意识到自己的数据价值之后，用户会逐渐反感，甚至抗议。物联网由于涉及用户更多的信息，包括健康信息、车辆行驶信息等，中心化网络无法取得用户信任。

2 项目概要

INT 项目源于 Apache Mynewt（Apache 开源物联网操作系统）的一次社区实践。团队最初尝试通过软件定义硬件，降低硬件开发的复杂度。然而即使定义出了系统的抽象层，硬件与硬件之间如何形成统一的生态，依旧是一个充满挑战的问题。后来，团队经过思考，考虑通过经济方式去驱动不同系统之间的融合。

INT 正是一种面向物联网的基于经济驱动方式的区块链应用平台和交互标准。以平行链的结构使设备间彼此相连形成分布式网络，通过共识算法来保证设备间交易的合法可信任。同时不同种类的设备可以接入不同的平行链，避免总账本的爆炸式增长。

INT 的存在可以大幅度降低物联网区块链应用的开发难度。它可以中继不同的物联网，形成边缘计算网络，有效流通资源，加快物联网普及进度。INT 设计为可伸缩的异构多链，提供中继链平台，在其上可以构建大量可验证的、全局一致的、共识的数据结构。换句话说，在保证整体的安全性和链间信任基础上，INT 致力于使物联网区块链内化成如同 TCP/IP 一样的物联网基础架构，不知不觉影响人们的生活。

为了实现以上目标，我们必须做到如下内容：

2.1 软件定义资源

硬件开发和软件开发有着本质的差异。硬件因为成本设计的限制，一般相对资源匮乏，所以当我们希望硬件增加额外的成本，提供额外的资源，一定是不可能的（比如说提供额外的计算能力，额外的电量）。所以我们想解决的问题，并不是提供额外的资源，而是如果硬件本身是一个 WIFI，或者一个温度采集器，当它需要将自身价值提供给其他的服务或硬件时，可以提出响应的收费策略。而我们涉及的资源，根据相应不同的设备，从现实世界中进行抽象，对于现有的实体（无论是硬件，还是数据）进行映射，以服务的形式提供一致性的调用。

我们不可能让现有的设备增加额外的功能，但是在一个相对的硬件生态中，或许我们可以通过经济驱动，让各种设备开放自身的功能，从而获得更多的收益。因为标准垄断的本质就是利润，而代币本身是可以提供利润的，并且因为代币价格的浮动性，可能产生额外的经济收益。相对收益，并不低于绝对利润。

所以我们将尝试一种新的模型，通过分享收益的方式来驱动硬件开放自身能力，去中心化地获取利润，而不是通过中心化的垄断获取利润。

2.2 资源的货币化

在我们的定义中，需要一个稳定的度量衡，物联网络内部的结算，我们不会采用 INT，而会采用一种类似于 ETH 的 GAS 的机制。因为，设备的资源结算需要一种相对稳定的度量衡，

资源将会以以下几种方式进行结算：

标价式：根据标定的价格付费。

计量式：根据时间轴，或者其他维度分段计费。

竞价式：向所有需要调用资源的设备发起竞价，价高者得。

CPP（Cost Per Purchase）：根据资源的最终使用结果付费。

因为有智能合约的存在，所以可以采取很多传统架构无法完成的方式，进行协调互动，具体的方式可以以智能合约的方式在链上约定。

2.3 资源交易配置

相关的节点应该以一种半自动化的方式，通过自定义策略，对资源进行采购。

2.4 隐私性保护原则

当前物联网还有一个特别重要的问题，就是用户隐私。物联网的用户隐私保护极其脆弱。因为通过传感器大量的收集用户数据，非常容易对用户行为进行预测。并且，当前的架构模型，就算采用 OpenID 的方式，进行用户

脱敏，只要多个维度进行比对分析，很容易反向推导出用户的身份。针对这个问题，我们尝试基于零知识证明算法，并采用我们所以创新的行为私钥（BPK）算法模型，通过将用户意图（intent）传递给其他硬件，而不需要传递用户符号，不但可以在事实上有效地保护用户隐私，而且也可以解决担心用户流失的问题。

我们所创新的ＢＫＰ算法模型，通过对于用户数据进行非监督式学习或策略模型，聚类为行为，并通过零知识证明算法进行用户脱敏。这样设备在设备之间，就可以基于意图的去共享资源，而且不需要基于用户去共享数据，这样可以非常有效的解决用户隐私问题。

2.5 安全性

设备可能像魔镜（Black Mirror）中的机械蜂一样杀人吗？这可能不一定，但是自动驾驶汽车撞死人，一定不是一件稀奇的事。未来物联网的安全是重中只重，INT 将会尝试通过创新的 BPK 算法，对意图进行过滤，试图保证用户的安全性。

3 系统架构

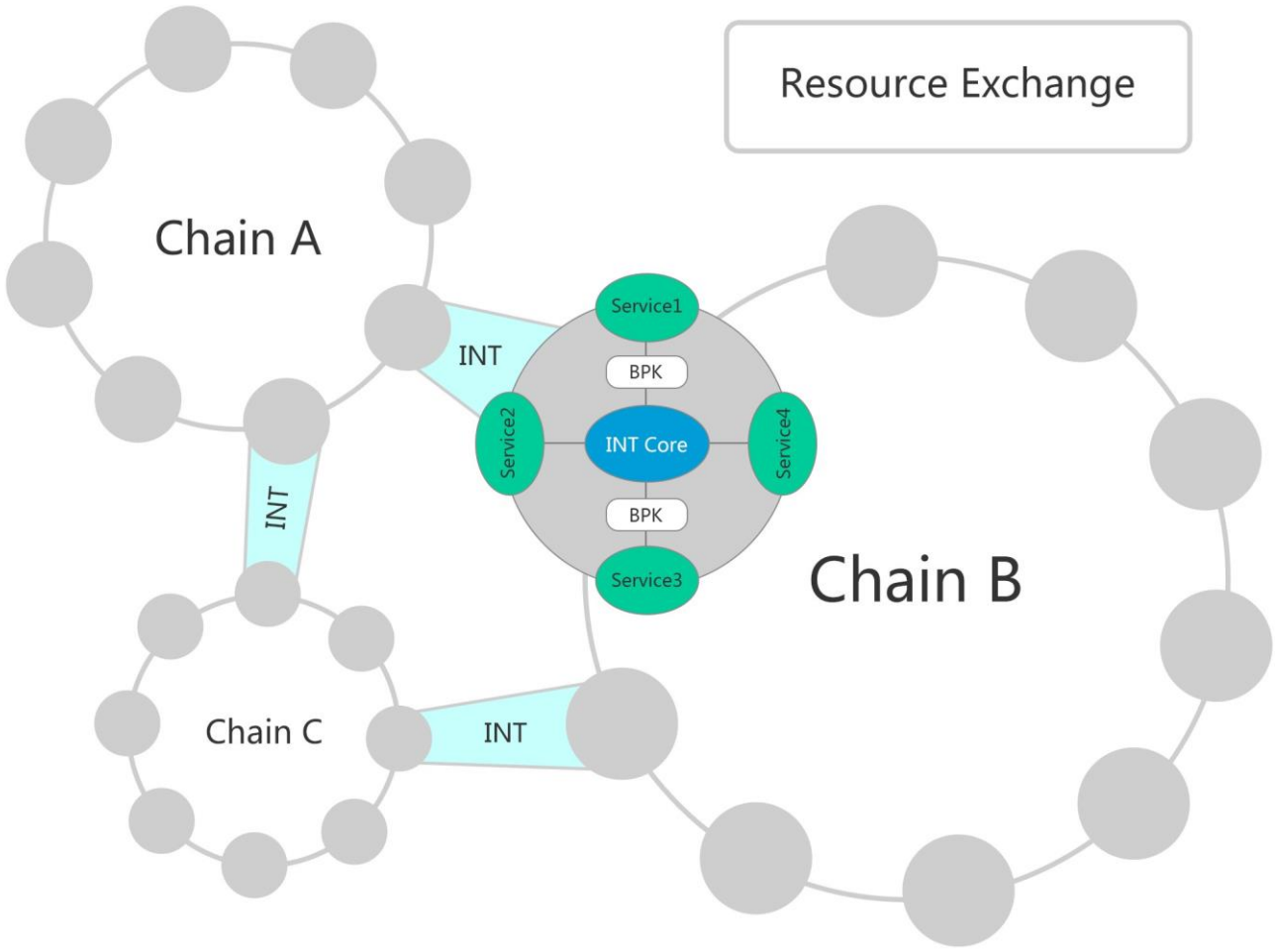

图 1 INT 的系统架构

4 服务

各个机器节点之间可以根据自己的意愿，上架相应的 SKU，适配不同的竞价、销售、分销策略、权限策略，形成自发现的 Metadata。该层即是对软件服务的定义，也是对于硬件服务的抽象。

5 交易市场

A. 机器自动撮合

通过智能合约，半动态的配置，对于基础服务，如网络，电源，算力，自发现，进行即插即用式接入。

B. 开发者 API 交易市场

对于数据和服务，在云端形成交易体系。

6 INT 代币

INT 代币将会采取两层结构。

第一层是传统的代币结构，参与交易所交易，可以理解为 INT 股。

第二层采用第一次结构代币，限时竞拍，浮动瞄准法币，主要为了解决代币波动性问题，降低波动性，便于计费。

7 机器节点

节点可能有传统 PC Server 节点，也可能有 STM32 节点，根据机器性能进行配置性剪裁。物联网是典型的边缘雾计算场景（Fog Computing）。现有的区块链网络，其实并不适合于物联网。在这么一个算力高可缩放的网络中，如何进行算力共享，其实这里面的核心也是经济驱动，所以我们才需要去定义 INT 这样的一个解决方案。

8 共识

在共识上，INT 基本会采用和 Polkadot 一样的模式，因为一样是多链平行算法，INT 通过异步（asynchronous）拜占庭容错（BFT）算法达成对有效区块的相互共识。算法起源于 Tendermint 和 HoneyBadgerBFT，HoneyBadgerBFT 在有任意网络缺陷的架构下，只要大部分验证人是诚实的，就能提供一种高效的容错算法。

确实一个（PoA）模式的网络就足够了，然而 INT 是个可以在全开放和公开的场景下部署的网络。因此我们需要一种管理验证人群体并且激励他们守法的机制。因为硬件交易的性能要求，所以我们将选择使用以 POS 为基础的共识算法，为了避免 POS 的缺点，以及因为大部分节点可能是低性能节点，我们会采用 POS+POW 的混合方式进行改良。单纯的单链，一定无法解决性能问题，所以我们尝试通过平行链，共识接入，解决性能问题。

物联网未来存在千亿级别的接入设备，并且特别多的设备将是低区块时间的高频链，也

存在大量联盟链的需求，因此我们采用了平行链结构，通过 INTStream 实现价值和数据在 INT 与其他多个平行链间的转移，由于平行链是独立的系统，技术和经济上的创新不会被其他因素妨碍。

INT 平行链可以在运行时的任意时刻，由任意帐户创建。创建者可以根据应用需求定制平行链的细节功能和平行链所提供的服务和平行链代币具体信息。这些定制信息形成平行链的数据结构，以类似 INT 交易记录的方式，被记账节点记录在当前时段的区块中。至此平行链将作为一条独立的区块链，记录平行链代币的交易。

9 区块的打包方式

不同链之间，有可能是高频低出块时间的链，有可能是高度加密的块。所以，每条平行链采用不同的包块打包方式，通过中继链整合共识。共识整合这部分，我们应该会采用 Polkadot 或者基于 Polkadot 进行改良，由主要节点进行记账。

10 网络设计

物联网是一个非常特殊的网络，数据的传输，对于延迟、不同协议、精度的要求差异都特别大。所以在网络架构方面，我们将会采用 MQTT 方式，并对 MQTT 进行特定实现以及协议改良，用于满足区块链的需求

11 INT 应用场景与 INT DAPP

随着物联网设备几何级数增加以及机器智能水平提升，将会有越来越多自动运行的物联网 DAPP 安装在智能设备上，机器与机器，人与机器之间将将通过分布式物联网 DAPP 进行实时可信的自动数据交换和自动交易。

INT 将实现物联网点节点间直接互联的数据传输，物联网解决方案不需要引入大型数据中心进行数据同步和管理控制，包括数据采集、指令发送和软件更新等操作都可以通过区块链的网络进行传输。一些 INT 典型应用场景包括：

1）工业制造：制造业周期开始进入完全虚拟的世界，包括产品研发、客户需求监测、生产、库存管理。随着设备和系统越来越智能和交互，区块链也将成为工厂、地区、全球供应链级别的账本，从而大大降低成本，加强准时化生产（JIT），更好的使用工厂产能，改善运营效率；

2）联网的无人驾驶汽车：联网汽车（Connected Vehicle）中自动运行的 DAPP 使车辆变成的智能应用终端，汽车与汽车之间进行自动的行驶数据交换，从而实现更加安全的自动驾驶、汽车自动化导航、道路救援等；

3）交通：物联网＋区块链＝联网交通。车辆网络中的应用场景很多，可以传递所有交通信息，避开交通堵塞等问题。将其延伸

到全球贸易中，这个交通网络可以囊括水运、空运、地面运输网络，追踪货物运输； 4）公共技术设施和智能城市：智能设备已经用于追踪桥梁、道路、电网等的状况，区块链可以将所有这些连接到一起，共享高效率，进行维护，预测使用情况和污染情况等。另一个重要应用是帮助偏远地区监测自然灾害，防范大规模山火、病虫害等大灾害；

12 路线图

INT 旨在解决破碎分散的物联网市场当中价值传递的问题。INT 将是一种 ERC20 代币。它将是一个基于物联网的全新底层构架平台：去中心化，开放，开源，高效。在生态系统中，不同的参与方可以得到合适的成本和利润，并且彼此分享。区块链和物联网这两个领域存在着快速发展的红利。INT 作为透明、开放的系统，希望可以促进物联网的发展，不诉求于标准的统一，通过经济方式去驱动不同的标准互联，形成一个有效的去中心化市场。

该解决方案的第一步，我们将会在 RUFF 的生态体系当中构建，RUFF 现在已经有众多的模块化产品。我们在模块化产品中，搭建一个完整的联通体系。

第二部分，我们会打通基于 Arduino、树莓派等众多开放性硬件平台。

13 INT 团队

INT 团队核心成员包括国内最早一批物联网开发人员、国内通信骨干网络系统与设备开发人员，物联网操作系统架构师、金融区块链开发工程师。研发团队对物联网、信号传输、安全系统设计、区块链、比特币底层、以太坊底层、自动化交易、机器学习、大数据等技术有深刻的理解和研发经验。

团队核心成员

项若飞 INT 基金会 INTchain 首席架构师。

中科院博士后，新一代（5G）无线通信和物联网技术青年专家，专攻“区块链--物联网”技术融合的应用落地。主持 863 项目一项，发表论文多篇，申请技术专利数项。

陈光辉 复旦计算机软件专业，先后就职于东方通信、华为等企业，在通信底层技术、系统架构、研发项目管理、软件开发、移动互联网等领域具有丰富经验

1993 年至 2005 年东方通信工作，历任 CDMA 交换机开发部研发工程师、测试部长、副总经理，2005 年加入华为，历任企业通信 MKT 部长，铁路信号架构设计部部长，2012 年创业，方向为手机打车服务市场；

殷相玉 物联网深度爱好者，国内最早期物联网研发从业者，互联网连续创业者，站长，Apache Mynewt 代码贡献者

2003-2005 参与基于 GPRS 的穿戴式远程单兵生命状态测试仪、麻醉深度测试仪、糖尿病早期神经病变测试仪的系统设计研发；
2005 年-2008 连续创办服装批发网、戒烟网、抑郁症强迫症社区等多个互联网项目；2008 年开始运营地方站等站长站；2013 年，中国第一台微信物联网设备微信打印机“印美图”最早期支持者和推广负责人；
曹严明 善林金融技术总监。北京大学数学学士，美国威斯康辛大学麦迪逊分校计算机硕士。二十余年 IT 从业经验，曾就职于微软、SAP、HCL 等知名软件公司，负责过大型数据库系统、银行业务系统、电子商务系统、银行清算区块链应用开发， 具有丰富的金融系统开发和项目实施经验。现专注于区块链和智能合约底层技术的研发在银行物联网等行业应用；
汪晔 毕业于北京邮电大学，先后就职东方通信、UTStarcom、华为，软件系统工程和研发质量管理专家。1999 – 2005 就职于杭州东方通信网络所，从事 CDMA2000 移动交换机、小灵通的平台和协议软件开发与测试工作；UTStartcom 期间就职宽带事业部，从事 AN8000 宽带接入产品的平台软件开发工作；2005.12 入职华为杭研，负责企业通信 IP PBX 产品部 SEG leader 产品导入，架构与系统设计；
张波 华中科技大学硕士，12 年系统架构经验；华三 DDOS 防护设备带头人；华为高铁信号 2 乘 2 取 2 安全机制负责人；华为首款工业路由软件架构师，地铁 ATP&ATO 系统架构师；
王红伟 川大硕士，10 年物联网领域技术研究；“货车帮”早期平台架构人；华为首款工业路由 AR531 设备领军人物；高铁信号 3oo3 组合故障-安全系统发明人，智能包装发明人；
张杭君 毕业于杭州电子科技大学，11 年硬件开发工作；负责 10 余种 EMC 检测设备研发；华为首款工业路由硬件负责人，负责高铁、地铁和有轨电车车载、CBI 及轨旁信号系统硬件研发。
李勐然 毕业于华南理工大学，大型电信骨干网络核心运维工程师，中国电信集团国际业务处原副处长，中国电信窄带物联网 NBIoT 项目早期参与人；
徐纯 中国计量学院硕士，先后就职华为、中电海康，软件系统工程专家，高可靠性安全性系统设计专家。华为就职期间负责高铁信号系统的设计和开发，RBC 系统设计和开发；就职中电海康集团物联网研究院期间，承担“湖州智慧织里”等项目，技术总负责顶层规划、网络设计、应用、硬件终端部署开发等；

陈宇琪 中山大学数学系，前搜房网分布式系统开发工程师、Google Brillo 代码贡献者；

团队顾问

Roy Li ：知名网络安全专家，物联网专家，Ruff 操作系统创始人，复旦大学硕士生导师，Ruff 在过去的三年里获得了极客帮基金，景林资本，山行资本投资。

谭磊：区块链和大数据挖掘专家，北美区块链协会 NASA 发起人、微软总部工作 13 年，美国杜克大学硕士，《区块链 2.0》等著作；

孔华威：中科院计算技术研究所上海分所所长，张江高科创投首席科学家

Ramble：北美区块链协会 NABA 主席，贵阳区块链金融监管沙盒总架构师，贵阳区块链金融孵化器董事长，谷壳币、SWFT 创始人项若飞：中科院博士后、华中科技大博士，师从郝跃院士和王占国院士，开发了基于区块链的大宗商品电子商务平台，先后主持了 863 项目“新一代移动通信基站氮化镓射频功率放大器”课题及广东省院合作系列课题。

赵亚甫：广东卓泰投资管理有限公司风控总监

葛磊：广东广信君达律师事务所合伙人刘金华： 注册会计师、注册税务师，山东实信会计师事物所合伙人，多家上市公司会计税务顾问，前山东国税公职人员。

INT 天使投资团队

朱濬：华体网竞 CEO

郑志平：知名站长，爱站网创始人徐斌：金名网 4.cn、易特网络创始人陈东红：知名域名圈投资人黄智毅：中美资本创始合伙人

罗文：下载吧创始人、瓦力科技创始人

Alex.F： 高榕资本高级投资总监

团队成就

中国第一代基于 GPRS 的远程单兵生命状态检测可穿戴战衣；

国内第一款麻醉深度测试仪概念产品；

小灵通产品、通讯平台和通信协议系统

国内首款 CDMA 交换机；

华为首款工业路由硬件 AR531；

高铁信号 3oo3 组合故障-安全系统；

华三百 G 级 DDOS 防护设备

华为高铁信号 2 乘 2 取 2 安全系统；

中国地铁 ATP&ATO 系统；

银行间清结算区块链应用系统；

2014 年，Ruff 物联网操作系统诞生，让软件程序员也可以开发硬件，获得微软年度最具投资价值大奖、Tech Crunch 2016 创业大赛第一名、GITC 2016 年度互联网最佳技术创新奖、Predix hackthon 最佳创新奖等等奖项；

2016 年基于 ETH 的车联网区块链应用“自动路况互换系统”测试成功。

INT 基金会

INT 基金会是专门为支持基于 INT 平台的物联网应用项目而办的一个非盈利性组织。

INT 基金委员会治理

INT 基金联盟委员会采用联盟轮值主席方式开展工作，每两年由投票选出轮值主席，轮值主席只能一届，INT 基金联盟委员会设立数个管理中心，包括区块链技术开发中心、区块链商业应用中心、财务管理中心、风控管理中心和综合事务管理中心，分别指导业务部门开展工作

资金来源与资金管理

1） 维持 INT 项目运作的资金主要来源于原生资产 INT 币的分批次、风险投资和联盟链会员会费、捐赠等，在需要的时候部分 INT 会转换为其他形式权益资产，用于项目运营。

2） **财务管理说明**

INT 基金会财务管理的原则：统筹安排，综合管理；勤俭节约，讲求实效。

INT 基金会资产管理纳入全面预算管理，根据实际运营情况，编制财务收支预算。

年度财务收支预算报自制委员会审议，月度财务预算由执行委员会审议，财务管理中心负责编制和执行，每季度进行披露。财务报告披露渠道：官网 https://intchain.io/。

INT 基金会将引入第三方审计，监督项目的财务运作，进行资金审计编制审计报告，审计报告将在年度信息披露中公告体现。

进度披露

INT 项目发起团队承诺将恪尽职守、诚实信用、谨慎勤勉的原则管理众筹的加密数字资产。

为保护投资人利益，加强 INTC 的管理和高效使用，促进 INT 项目的健康发展，INT 项目设置信息披露制度。

INT 希望能通过自身的示范作用，规范数字资产的管理，增加区块链行业的 自律

性，提升区块链加密数字资产管理的透明度，维护好区块链行业的长远发展。

INT 将在每个季度结束后的两个月内披露季度报告，每个会计年度之日（每年 12 月 31 日）起三个月内编制并披露年度报告，报告内容包括但不限于 INT 项目的技术开发里程碑及进度、应用开发里程碑及进度，数字资产管理情况，团队履职情况，财务情况等。

INT 会不定时实时披露 INT 项目重要的临时信息，包括并不限于重大合作事项、核心团队成员变更、涉及到 INT 的诉讼等。

INT 将在官网 https://intchain.io/ 披露信息报表

专家顾问委员会

INT 将邀请国内外从事区块链行业工作多年的资深专家、具有丰富经验工作业绩的知名人士、法律娱乐文化等各行业专家以及熟悉政府政策的人士组成第三方专家顾问委员会，为团队提供咨询顾问、辅助决策等外脑参谋，具体包括：

1） 对团队工作规划、重大项目进行论证和指导，协助项目进行开发规划和设计；

2） 承接项目的政府调研和行业委托，开展行业研究；

3） 组织对物联网和区块链热点问题的调研，为团队提供咨询服务；

4） 加强信息交流，定期举办行业论坛、嘉宾座谈、学术交流等；

INT 专家顾问委员会专家包括：孔华威：中科院计算所上海所所长项若飞：中科院博士后、区块链专家；郑志平：爱站网创始人，网络营销专家赵亚甫：广东卓泰投资管理有限公司风控总监

葛磊：广东广信君达律师事务所合伙人刘金华： 注册会计师、注册税务师，山东实信会计师事物所合伙人，多家上市公司会计税务顾问，前山东国税公职人员。

INT 法务

INT 基金会将聘请国内知名的律师事务所，作为 INT 项目法律顾问，为 INT 项目提供数字化资产交易结构设计、运营合规化、法律风控体系设计、海外法律咨询等方面提供全面的法律服务。

免责声明

本文档只用于传达信息之用途，并不构成买卖 INT 代币的相关意见。任何类似的提议将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策，或具体建议。

本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为，或任何邀请买卖、任何形式证券的行为，也不是任何形式上的合约或者承诺。

INT 明确表示相关意向用户明确了解 INT 平台的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意为此承担一切相应结果或后果。

INT 代币，是一个在 INT 平台使用的数字加密货币。在写这段文字时, INT 币尚且不能用来购买相关物品或者服务。我们无法保证 INT 币将会增值，但其也有可能，在某种情况下出现价值下降的可能。

INT 币不是一种所有权或控制权。控制 INT 币并不代表对 INT 或 INT 应用的所有权，INT 币并不授予任何个人任何参与、控制、或任何关于 INT 及 INT 应用决策的权利。

风险声明

- 1) 证书丢失导致的丢失 INT 币的风险

购买者的 INT 币在分配给购买者之后会关联到购买者的 INT 账号，进入 INT 账号的唯一方式就是购买者选择的相关登录凭证，遗失这些凭证将导致 INT 币的遗失。最好的安全储存登录凭证的方式是购买者将凭证分开到一个或数个地方安全储存，而且最好不要储存在公开场所或者会有陌生人流出现的地方。

- 2) 以太坊核心协议相关的风险

INT 币基于以太坊协议开发，因此任何以太坊核心协议发生的故障，不可预期的功能问题或遭受攻击都有可能导致 INT 币或者 INT 应用以难以意料的方式停止工作或功能缺失。关于以太坊协议的其它信息 http://www.ethereum.org

- 3) 购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制购买者的 INT 币，为了最小化该项风险，购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

- 4) 司法监管相关的风险

区块链技术已经成为世界上各个主要国家的监管主要对象，如果监管主体施加影响则 INT 应用或 INT 币可能受到其影响，例如法令限制使用，销售，电子代币。

- 5) INT 应用缺少关注度的风险

INT 应用存在不会被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开

发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对 INT 币和 INT 应用造成负面影响。

- 6) INT 相关应用或产品达不到 INT 自身或购买者的预期的风险

INT 应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何 INT 自身或购买者对 INT 应用或 INT 币的功能或形式(包括参与者的行为)的 期望或想象均有可能达不到预期，任何错误地分析或者底层设计的改变等均有可能导致这种情况的发生。

- 7) 黑客或盗窃的风险

黑客或其它组织或国家均有以任何方法试图打断 INT 应用或 INT 币功能的可能性，包括服务攻击，Sybil 攻击，游袭，恶意软件攻击或一致性攻击等。

- 8) 漏洞风险或密码学科突飞猛进发展的风险

密码学突飞猛进的发展或者其他相关科技的发展诸如量子计算机的发展，或将破解风险带给加密代币和 INT 平台，这可能导致 INT 币的丢失。

- 9) 缺少维护或使用的风险

购买 INT 币应该被认为是一种对于物联网应用开发的支持和投资，而不是一种投机行为。虽然 INT 币在一定的时间后可能会有相当的市场价值，导致早期投资者产生较大的收益，不过如果 INT 平台缺少维护或没有足够的应用，这种升值并没有太多的实际意义。

- 10) 未保险损失的风险

不像银行账户或其它金融机构的账户，存储在 INT 账户或以太坊网络上通常没有保险。任何情况下的损失，将不会有任何公开的组织或者个人为你的损失承保。

- 11) 无法预料的其它风险

密码学代币是一种新兴的技术，除了本白皮书内提及的风险外，此外还存在着一些区块链行业本身以及 INT 团队尚未预料到的风险

更多信息

更多信息请见 INT 官方网站： https://Intchain.io

词汇说明

Bitcoin/比特币：比特币是一种虚拟货币，它不依靠特定货币机构发行，而是依据特定算法，通过大量的计算产生的。比特币使用整个 P2P 网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。

IoT：internet of things 物与物之间的网络链接，简称物联网。

Apache Mynewt：由 Apache 软件基金会（ASF, Apache Software Foundation）发起的一个开源的社区项目 Mynewt，是一个专注于物联网 IoT 应用的实时操作系统，包括低功耗蓝牙（BLE4.2）无线传输协议栈 NimBLE，最新的稳定版本为 1.0.0-b1。

DAPP：Decentralized Application 的英文缩写，去中心化的应用程序。

DAC：decentralized autonomous corporation 的英文首字母缩写，去中心化的自治公司。

Distributed Ledger: 分布式分类账本。

Fog Computing：雾计算，在该模式中数据、（数据）处理和应用程序集中在网络边缘的设备中，而不是几乎全部保存在云中，是云计算（Cloud Computing）的延伸概念。

Hash: 哈希散列，密码学里的经典技术。把任意长度的输入通过哈希算法，变换成固定长度的由字母和数字组成的输出。

Hash/s，缩写 **H/s**：运算性能参数，即每秒能处理的 Hash 数，100MH/s 就是 1 秒钟能够处理 1 亿次 Hash 数。

Merkle Tree：默克尔树，是一种二叉树，由一组叶节点、一组中间节点和一个根节点构成。

PBFT：Practical Byzantine Fault Tolerance，即实用拜占庭容错算法共识机制。它是一种消息传递的一致性算法，通过三个阶段达成一致性，确定最终的区块产生，假如有 3f+1 个节点，这种算法机制决定了可以容忍 f 个错误节 点的存在，而使一致性结果不受影响，这种机制可以脱离币的存在，共识节点可由参与方与监管方组成，2-5 秒的共享延时也基本能满足商用要求。

ZKP：零知识证明，zeroknowledge proof，是由 S.Goldwasser、S.Micali 及 C.Rackoff 在 20 世纪 80 年代初提出的。它指的是证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。

PoA：Proof of Activity 行动证明协议。

POW： Proof of Work, 工作量证明。

POS：Proof of Stake，即股权证明共识机制。是 POW 的一种升级的共识机制，它是根据节点拥有代币的多少和持有代币的时间，来控制挖矿时间的长短; 它可以有效的降低挖矿时间，但是仍然没有避免矿机运算资源浪费的问题。

DPOS：Delegated Proof of Stake，即委任权益证明共识机制，它的原理是代币通过投票选出一定数量的节点，为它们完成验证和记帐的工作，这种共识机制可以大大减少参与记帐和验证的节点数量，达到快速的共识验

证，但是这种机制也需要依赖代币的存在，使某
些不需要代币存在的应用受到限制。

ERC20：ERC20 令牌是 ETH 钱包的通用交换标准，允许钱包、交换和其他智能合约的开发人员提前知道基于该标准的任何新标记将如何运行。通过这种方式，他们可以设计自己的应用程序来处理这些令牌，而无需等到
新的令牌系统更新。

ERC223：ERC20 令牌无法将令牌发送给一个与这些令牌不兼容的契约，也正因为这样，部分资金存在丢失的风险，ERC223 令牌标准将向现有的 ERC20 标准引入一个新功能，以防止意外转移的发生。

Ruff：是一种支持 JavaScript 开发应用的物联网操作系统，通过硬件抽象，实现软件定义硬件、跨平台、高效便捷的智能硬件开发，可以让软件工程师将更多的注意力集中在业务需求和应用逻辑，而非如何实现。Ruff 包含了操作系统，解释器，驱动，安全，后台控制，无线配置等运行环境，还有桌面工具以及开发框架，从而实现更可靠、高效的智能硬件开发过程，目前已经是全球最重要的物联网操作系统之一。

Raspberry Pi：树莓派，简写为 Rpi，是为学习计算机编程教育而设计，只有信用卡大小的微型电脑，其系统基于 Linux。 **Arduion**：Arduino 是一款便捷灵活、方便上
手的开源电子原型平台。包含硬件（各种型号的 Arduino 板）和软件（Arduino IDE）。由一个欧洲开发团队于 2005 年冬季开发。**参考文献**

A. Tapscott, D. Tapscott, How blockchain is changing finance, Harvard Business Review, 2017.

T. Stein, Supply chain with blockchain — showcase RFID, Faizod, 2017.

S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org, 2009.

R. Hackett, The financial tech revolution will be tokenized, Fortune, 2017.

D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, Sequences II: Methods in Communication, Security and Computer Science, 1993.

A. Legay, M. Bozga, Formal modeling and analysis of timed systems, Springer International Publishing AG, 2014.

A. Back, Hashcash — a denial of service counter-measure, Hashcash.org, 2002.

B. Dickson, Blockchain has the potential to revolutionize the supply chain, Aol Tech, 2016.