Ruff 物联网公有链白皮书 [1]

Working Draft, October 2017, Rev. 0.7.1

摘要

Ruff 是一个结合物联网和区块链的架构，它包含一个分布式操作系统和一条开放式的主链，从而将虚拟世界的点对点网络及共识机制扩展到线下，实现信息流推动原子流。 在 CAP 三角的选择中，传统区块链是放弃可用性从而强化一致性和分布式容错性，而 Ruff 通过边缘计算和区块链的结合，强化了可用性，从而满足物联网对实时性的弹性需求。

我们要解决的核心问题是不同体系 IoT 设备之间的可信互操作，有偿互操作问题。用来构建开放的 Ruff 生态。

背景

物联网往往是割裂的封闭的体系，广域物联网和局域物联网不能发生交互，私有化部署的工业系统和IDC为基础的IT网络难以连接。然而物联网的数据往往需要较高的一致性和安全性，这是任何一个中心化体系下的技术难以解决的问题。现代的物联网技术往往伴随着冗余性的节点，混合云等技术，然而在一致性和安全性问题上，区块链提供的是最终的解法。可惜的是，区块链的存在着基础设施匮乏，技术门槛较高，技术风险过大的问题，如常被诟病的扩展性问题至今没有较为成熟的解决方案，使得目前的分布式应用稀少且停留在虚拟层面，并不能和真实世界发生交互。

碎片化

从物联网诞生的那一天起，它就是碎片化的。街上随处可见的共享单车，不同类别的车你需要不同的手机应用才能打开，这些节点并不等价，没有标准，是碎片化的。 任何品牌的手机都可以通话、联网以及交换数据，为什么交通工具却不行?

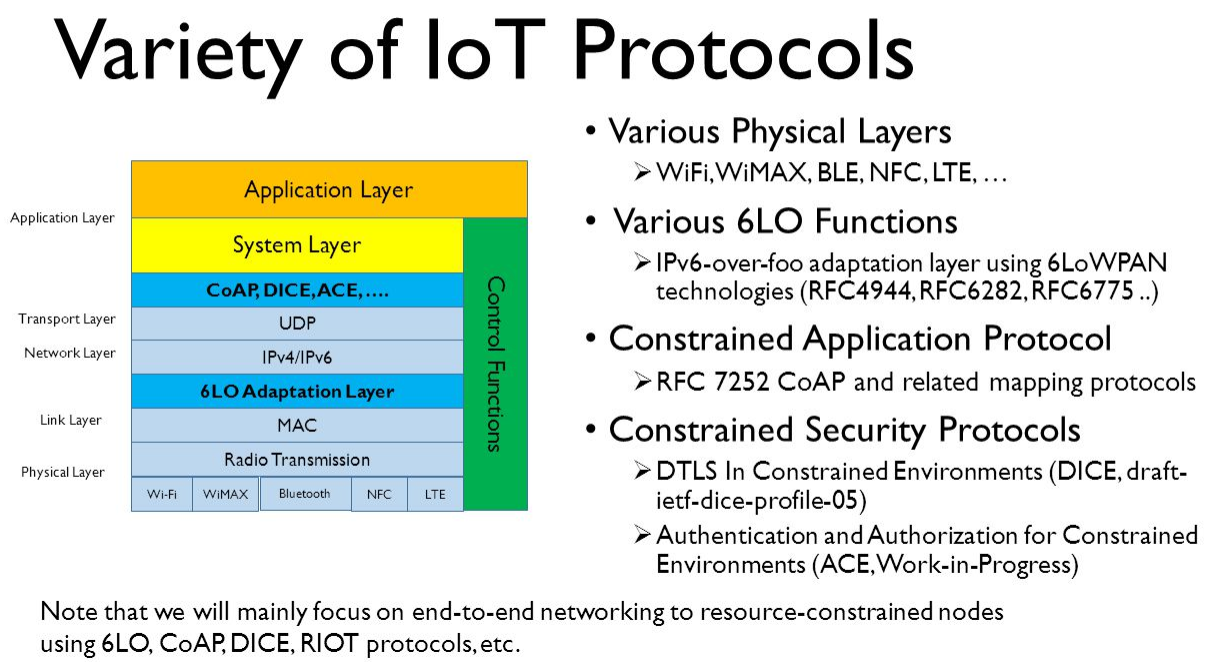
其实不止是交通工具，那些看起来已经联网的门，灯，报警器，咖啡机等等，他们所连接的网络都是割裂的，封闭的。同样类型的产品都是碎片化的，更不要说不同类型的产品了。物的种类已经多到数不过来，而几乎每一种物都很难像个人电脑或是手机那样同质化。

碎片化的问题可以不解决吗？答案是否定的。而解决碎片化的一种方式需要引入操作系统以及中间件的概念，兼容碎片化的硬件设备，并提供统一的编程接口。

标准

IT技术是标准化的，个人电脑通过 http 协议和服务器进行交互，在浏览器上呈现出来，这是一种标准化。比特币节点之间的全网广播，也是标准化的。 只有将碎片化的产品不断标准化，才有可能将节点统一起来，或是让节点之间形成一种共识。

在标准化这件事上整个物联网行业尝试了有二十多年，在物理层标准上有 WiFi, BLE, Zigbee 等，工业网络有Modbus, Profibus, 工业以太网等，尽管不同标准之间不能兼容，然而应用层的标准却一直没有推行起来， Machine B 和Machine B 连接成功，但 MachineA 却并不知道任何操纵或是请求 MachineB 的指令。更要命的是，同样是一种设备，不同的驱动，不同软件商的私有协议各不相同，难以交互。



易用性

指令有的时候是没有可读性的， GPIO_14号高电平变低电平的这个操作，能否和别的串口兼容，对开关的作用具体是什么，有的时候是未知的。你往往需要下面这样的定义。

```
RCC_APB2PeriphClockCmd(RCC_APB2Periph_GPIOB, ENABLE);
GPIO_LED.GPIO_Pin = GPIO_Pin_1 | GPIO_Pin_11 | GPIO_Pin_14 | GPIO_Pin_15;
GPIO_LED.GPIO_Mode = GPIO_Mode_Out_PP;
GPIO_LED.GPIO_Speed = GPIO_Speed_50MHz;
GPIO_Init(GPIOB, &GPIO_LED);
```

但是这种做法很难在互联网应用工程师群体里被推广起来，它的门槛不低，很容易写出bug，而且可读性依然不高。他们更喜欢如下这样的编程方式：

```
$('led-green').on();
$('led-red').off();
```

上面的这一段就是使用 Ruff OS 编程的代码，更多的可以在 http://www.ruff.io 中查找。截止 2017 年 12 月，全球已有 13521 名工程师在 Ruff 社区注册，其中一半以上都购买了 Ruff 开发板并部署过代码。

当节点之间有了应用层协议的标准，节点之间的通信就停留在了设备抽象之间的交互，可以是支付，请求，验证等，当多个设备组成阵列的时候，抽象级别会高一级，成为应用和应用之间的交互。

标准在应用层的统一，会是物联网当下最需要解决的问题，也是未来万物互联互通的重要基础设施。

物联网的标准不会在中心化的云端实现，而是在边缘计算的可编程开始，摒弃传统的模块 + 云的模式，应用逻辑会在固件之外，形成统一的编程模型。

不同品牌 IoT 设备之间的可信互操作

每个智能设备有一个地址，出场的时候商家把这个地址写入硬件，并在硬件的包装盒内放置该地址私钥的二维码。 控制中心通过获得私钥后发送给设备一条绑定命令（使用该私钥签名），拥有该硬件的完整控制权。绑定后控制中心可以删除设备的私钥，只需保存控制中心自己的私钥即可

- 点对点控制：控制中心通过给设备发起一条带自己签名的控制 TX，来操作设备。（并不需要链的参与，但要求控制时，控制中心和设备均在线）
- 基于链上状态的控制：当控制端无法和设备建立点对点连接时，可以让控制端消费一些 Token，在链上写入一个“状态改变” TX，或“控制命令” TX 来操作目标设备（这些 TX 一样需要有）。目标设备可以直接从链上同步状态或控制命令，或则通过一个可信轻节点（比如一个网桥设备）同步状态或控制命令。区块链解决了所有设备都连上云后，云的运维成本和稳定性问题。
- 自动化控制：并不需要使用合约来设置“气温低于 15 度则关闭空调”的逻辑，这些自定化控制逻辑可以用传统的开发语言在控制端（一个 App)里实现，降低了设备支持合约所需要的硬件成本，同时也减少了主链因为运行合约带来的可能的卡死。

可以基于上述设施，多厂商共同构建一个开放的 Ruff 生态。

时序数据

物联网的数据大多是以时间为序列的，和区块链有天然的结合。盖上时间戳的数据，本身就可以防止重放攻击，解决并发导致的死锁等问题。这些数据在过往割裂的中心化网络中并没有有效地被结合起来，解决数据在流通中的最终一致性问题。我们常见的如产品溯源的场景，往往在产品生产、存储、流通过程中，数据反复被 ERP, MES, WMS 等不同中心化的系统录入，整个环节的一致性是完全没有保障的。

Ruff 的边缘计算节点会以同步的时间戳为核心，控制局域网络内的业务逻辑。时间戳在整个区块链网络是同步的，追溯同一时刻整个网络各节点的行为可以还原网络某一时刻的状态。

共识机制

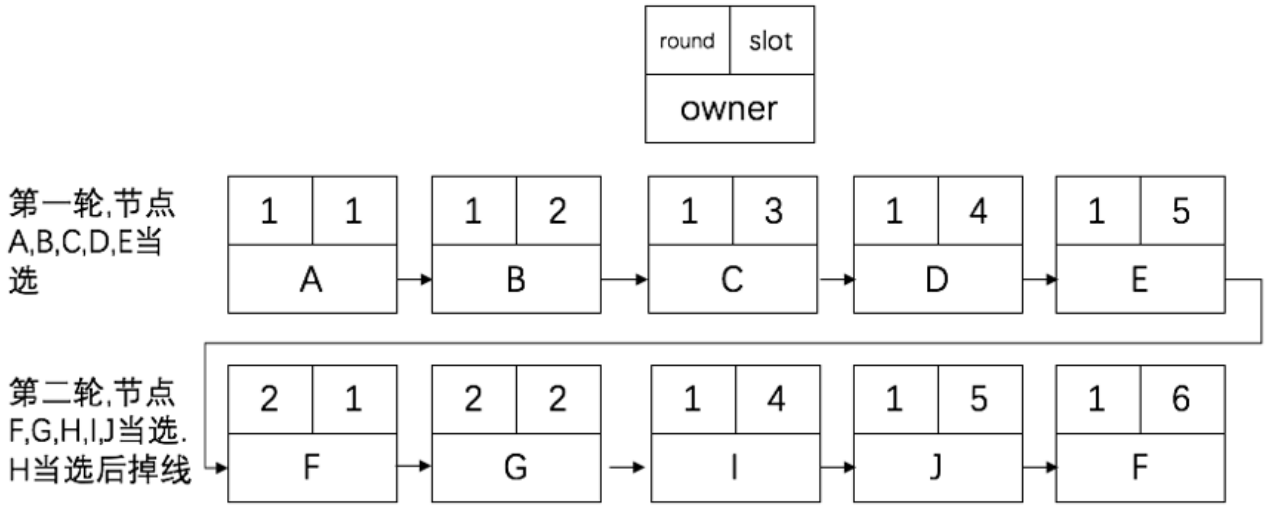
考虑到物联网里主控设备的计算能力，我们选择 DPoS 作为共识算法。

根据这种算法，全网持有代币的人可以通过投票系统来选择区块生产者，一旦当选任何人都可以参与区块的生产。

系统预计每 9 秒生产一个区块。任何时刻，只有一个生产者被授权产生区块。如果在某个时间内没有成功出块，则跳过该块。

任何全节点都可以通过一个特定的TX成为候选人。系统通过投票机制从候选人中产生 105 个代理人。

下图演示了代理人总数为 5 情况下的出块情况：



网络上的资源不是免费的，在任何个包含了多笔物联网合约交易的区块诞生之时，系统将奖励打包区块者。

在我们的架构中区块产生是以 105 个区块为一个周期。在每个出块周期开始时，从候选人人中选取 105 个代理人的过程称做一个 Round。在一个 Round 中有固定 105 个 Slot，会出 105 个块 在这些块中,所有的候选人都可以进行投票（VOTETX），选出下一轮的代理人。每个 Block 除了有高度外，还包含自己的 Round 号和 Slot 号。Round 号是连续的， Slot 号不一定连续。

候选人在一个轮次中都必须发起一次 类型为 Vote 的 TX ,在一个有效的候选人列表中选出 x 个代理人（如果候选人总数超过 318，那么代理人不允许连任）

当本轮的块 Slot 到达 105 时

- 如果 Vote 交易的数量不够法定数量，那么本轮的所有代理人都获得连任，开始下一个轮次
- 如果 Vote 交易的数量达到法定数量，那么计票得出获得最高票的 105 个代理人，开始下一个轮次

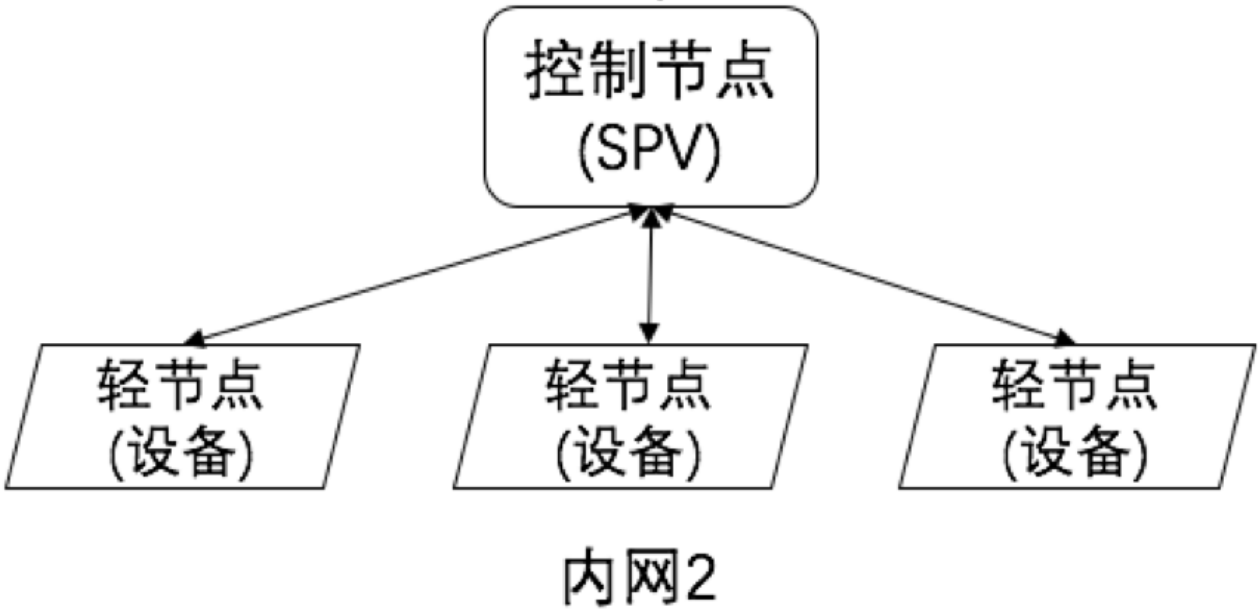
根据上一个轮次的最后一个 Slot 块的 Hash ,可以得到一个确定的本轮代理人出块顺序列表。

然后每个块，由该 Slot 负责的代理人出块，时间间隔为9秒。其它代理人在未轮到自己出块时，也要负责收集TX,并在轮到自己出块时，优先放入未包含的 TX（ TX 的收集是按 Round 来的）

如果轮到 n 号代理人出块，但该代理人节点掉线。那么他的下一个代理人会在 18 秒后自动出块。本轮的 Slot 号出现空缺。本轮的出块数依旧要满足 105 块.

通过分析链上的 Vote 交易和块的 Slot, Round 值。可以知道哪些候选人没有好好的工作。在一个轮次中，代理人可以发起投票取消某些候选人的资格。如果发行代理人没有按时出块，并且在此后的 24 小时里，该代理人都没有再次出块。那么所有的候选人都会投票要求取消该候选人的资格。

链下控制



在上图的典型结构中，轻节点和控制节点处于同一内网。在轻节点已经绑定控制节点的情况下，允许控制节点脱离主链对轻节点进行控制。

我们使用命令签名技术来达到链下控制的目的。

- **设备初始化：**

轻节点的设备生产商会在设备中写入一个密钥对的公钥，然后把该密钥对的私钥印刷在设备的说明书或包装盒内（二维码的形式）

- **设备绑定：**

将轻节点与控制节点放置在可互相通信的网络环境，然后控制节点发起一条绑定命令，该命令包含控制节点的公钥。命令创建后要求输入待绑定设备的私钥来对该绑定命令进行签名。签名完成后命令发送给设备。设备收到该绑定命令后对签名进行验证，验证通过将控制节点的公钥记录下来。控制节点可以不再保存轻节点的私钥

- **控制命令验证：**

轻节点收到的命令，只要有其记录的控制节点的签名，就会通过身份认证，同意执行该命令。

- **历史命令上链：**

在必要的情况下，控制节点会记录所有已经发送的控制命令，在与主链通信恢复后，把历史记录和控制结果记录发布到主链上。

基于类闪电链的差评机制

控制节点可以在主链上通过一个 TX:CreateContract 创建一个固定格式合同。合同的内容一般是“如果你给我多少 token，我就允许你在什么限制下使用下列命令”。合同成功创建后会返回保存合同的 Block 高度和该 TX 的 Hash (合称 Contract Addr)

用户可以创建一个 TX:Call 指向一个合同地址。把该TX保存到主链后，控制节点会不断的检测是否有 Call 自己创建合同的TX. 一旦检测到该TX,控制节点会检查用户是否有足够的 Token。如果有，则交易成功，创建 TX:Return，该 TX 中包含合同执行的结果，以及一个未提交的编码后的 TX:Review.Review 是一个设置了 seq 的多重签名TX.

TX:Return 被主链确认后合同执行成功，用户的 Token 会被真正的转入控制节点的账户。在一段时间后，如果用户觉得该硬件没有正确的处理后续的命令，那么就可提取出 TX:Return 中预签名的 TX:Review，签上自己的数字签名，并把 TX:Review 提交到主链，差评生效。由于该 TX 带有 seq，所以用户无法在短时间内立刻进行差评。

如果一个合同有大量的相关产品，那么当后续用户打算执行该合同时，控制 App 会通过交互提示用户该合同有大量差评。

节点分类

物联网的节点往往是非常小的运算单元，由于对体积功耗往往都有要求，它们的算力很低，内存很小，MCU 不会超过 512kb, Linux 版本的节点也就是路由器的级别，存储也很小，MCU 的只有 1M 的 Flash，这样的节点参与共识是非常困难的。 所以物联网的结构一定是由多个节点组成一个网络，这个网络里会有一个或是多个应用，应用通过应用接口和链发生交互，而本地应用所需的计算能力来自边缘计算单元，可以是网关或是路由器。应用可以使用中心化或是去中心化的方式管理局部网络，并和链发生交互。根据这个特点，我们把 Ruff 生态里的节点按下图进行分类：

轻节点（执行者）

应用控制物的接口，请求网络获取认证信息，核对正确后执行合约给使用者，比如释放物权。 轻节点可由无存储能力的简单设备承担，成本可低至几美金。

全节点（记录者）

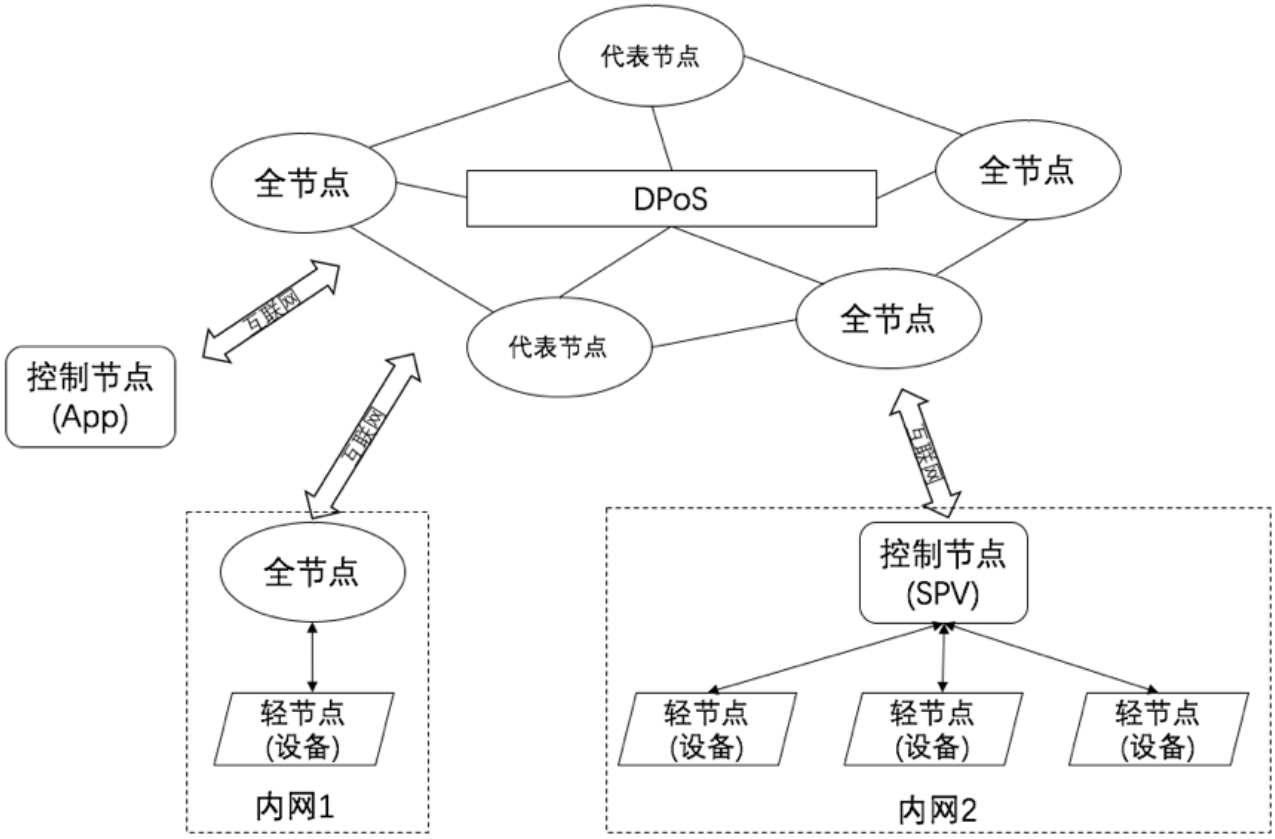
记载全部的信息，参与事件登记或是更改的广播，可将票投给其他节点。 并能成为代表节点。由网络里性能较强的设备扮演。由于未使用 PoW 的共识算法，对全节点的算力要求较低，200 美金的 HTPC，高度路由器，NAS 等家用智能设备均可扮演。

代表节点（仲裁者）

全节点中得票最多的 105 个节点，投票节点要承担坚守规则，打包区块的职责，一旦被发现有恶意行为则会被投票者抛弃，失去代表资格。代表节点可以通过出块获得挖矿收入。

控制节点（SPV钱包）

有一定的计算能力，能保存所有的区块的头部快速验证一个指定的交易是否上链，能使用 P2P 协议安全的发起一个交易。相对于全节点，不用 24 小时保存在线。一般由智能手机上的 App，或则没有足够存储空间的家用智能设备扮演（比如低端路由器，智能家居的网桥等设备）



物的合约（Smart Contract of Things）

物的合约建立在物被抽象的基础上，Dapp 通过 Ruff OS 和物件的抽象进行交互，并和 Ruff Chain 进行链上的交互，这二者相结合，就可以令智能合约在真实世界中执行。比如线下物权的交易就可以通过这样的方式，酒店和房东的门锁，租赁设备的使用开关都可以被合约控制。

除了物的使用权，生产资料产生的价值也可以进入合约，如发电、挖矿、制造等。

【描绘一下生产资料如何进入合约】

常见的 Dapp 场景可以是融资租赁，资产证券化，资产质押，供应链金融，物权登记和交易等，传统的区块链技术并不能将物的使用权和生产能力放入合约。

【举例说明描绘一下如何使用Ruff Chain辅助资产证券化】

应用场景

物权转让和租用

控制端可以允许绑定到一个定制的智能合约上，用来实现设备**使用权的认定**。 这类合约的结构类似格式化合同“如果付我 50 个 Token，那么未来 1 个小时内，我会接受你发送的下列控制命令。”，“如果付我 100 个 Token，那么未来 3 个小时内，我会每 10 分钟扣除你 1 个 Token。”链上支持不更新扩张这类格式合同。比使用智能合约更适合区块链的商用项目。

在控制端使用了这类合同后，还会得到一个用来做质量反馈的预签名 TX。

开放数据交易

产品、项目的全生命周期管理，产业链上下游可共享实时数据，从而实现如溯源、质量追踪、产能预测和分配等功能。

资产管理和证券化

资产产生的价值可以被交易，如发电机、矿机、充电桩、共享单车、零售设备等，预计产生的收入可以被证券化，进入流通环节。需要消耗耗材的设备及供应链管理也可以使用这种机制进行反向流通。

企业通过物联网设备的状态以融资租赁资产为载体，发行融资租赁集合信托计划。融资租赁公司利用自身在租赁业务当中的专业优势，完成租赁项目后，将融资租赁资产通过信托形式转让出去；同时委托人基于对信托投资公司的信任，将自己合法拥有的资金委托给信托投资公司，由信托投资公司按委托人的意愿以自己的名义，为受益人运用于该融资租赁业务。因此，它本质上是一种指定用途的资金信托和专门投资于融资租赁债权的金融产品。

所有权与收益权分离，发行融资租赁资产收益权信托计划。融资租赁公司将融资租赁项目租金收取权进行分离或重组，然后委托给信托公司，由其在金融市场上向特定投资者出售，投资者在信托期间享有融资租赁租金受益权。信托公司将投资者的购买金交付给融资租赁公司，融资租赁公司将应收租金折现，消除了其资产负债表上相应项目的融资负债，实现表外融资，既解决了融资租赁公司融资问题，又可以使资产出表，达到调整业务资产结构的目的，同时另外，该项目的融资租赁手续费等相关费用已经收取，融资租赁公司收益快速实现。同时对于信托公司而言，也找到了与融资租赁公司合作的载体和模式，有利于提高信托公司的租赁专业技能。

租赁公司可以考虑把信托公司发行产品作为一条固定的融资渠道，在融资项目调研的同时，与信托公司进行沟通，项目完成后即可同步发行信托产品，减少自有资金占用时间，同时又可以收取相关的费用收益，打造时间短、收益快的新盈利模式。例如，在 Ruff 与某光伏运维企业的合作中，光伏企业生产电能可以被实时被数据化监控并证券化。企业可根据光伏发电情况实时了解设备状态及资产生产效率，同时开放相关数据给用户，获取更加透明和更有公信力的产品信息。

0.00%

实时发电率

当前发电功率: 0.00W

累计发电量（度）

267,906

首页

我的

●●●●● 中国联通 上午9:58

测算结果

电站概况

装机容量	25.44kWp
月平均发电量	2157.31度
自发自用比例	5.10%

电站成本

建设成本	20.35万元
回本年限	8.30年

电站收益

年化收益率	12.04%
政府补贴	0.52元/度
余电上网电价	0.4153元/度
月平均收益	2042.23元
CO_2月减排	1978.47kg

我要装电站

我要装电站

评价机制

当合同执行完成后，用户并未得到预想的结果时，可以收手工提交合同返回的预签名 TX，来发布一个差评。 比如一个自动贩卖机，在扣除了用户的 Token 后，由于机械故障并未给出饮品。用户可以在一定时间内和自动贩卖机的销售方联系，如果问题位解决，就可以通过预签名TX来发表一个差评。 当用户执行的合同差评很多时，控制端会弹出提示。

代币的使用

Ruff 公有链内置虚拟货币：Ruff 币，由虚拟货币合约实现。Ruff 币是 Ruff 公有链生态系统内激励、消费和交易的基准。

代币的机制

在 Ruff 生态内，会产生一种代币或多种代币（token），作为一种结算标准。消费者在物权或是数据交易过程中会消耗代币。设备使用权和设备产生数据的交易也都会使用代币来结算。任何基于 Ruff 的智能合约都可以声称自己用于结算的代币。然而物联网生态内通过提供相应的节点资源，参与验证、记账等行为的生产者，其获得的代币会使用默认的 Ruff 币，消费者部署合约以及消耗资源所结算的也会是 Ruff 。

举例：用户A 需要向节点B请求获得资源或是使用权，则需要支付一定数量的某种token，同时将该交易打包的代表节点C也将获得奖励，该奖励为 Ruff 。

隐私与安全性

由于边缘计算单元承载了绝大多数数据，上报的数据是由应用决定的，应用开发者大部分逻辑都是离线的，在线部分数据的脱敏则由开发者自行控制。

Ruff 的本地自组网也是去中心化的，在一个本地应用网络中，一旦主要应用节点发生故障，应用逻辑会漂移到另一个节点继续完成，从而保障了本地应用网络一致性的问题。

物联网本身的安全性是由 OS 本身保证的， Ruff 采用对称密钥，密钥在网络中不传输。 此外链网络释放基于时间戳的一次性 token 到应用网络，可对抗重放攻击。

关于 Ruff

Ruff 成立于 2014 年，以边缘计算为核心，替代了原有的嵌入式操作系统，目前拥有上万开发者，是业内最通用的物联网操作系统。团队成员除技术过硬外，还有包括2017年福布斯中国30位30岁以下精英获奖者等殊荣的团队成员，负责项目对外的商务及市场推广。

成立至今，Ruff 获得了广泛的行业的认可度：

- 微软加速器 上海，一期企业
- 2017 GE Predix Hackathon 最佳创新奖

- 2016 Tech Crunch Beijing 创新大赛总冠军
- 2016 GiTC 最佳技术创新奖
- 2016 微软创新峰会最具投资价值奖

合作伙伴

Ruff 成立至今获得与诸多知名企业达成了合作关系。包括并不限于：

- 微软中国
- 施耐德
- 百度云
- muRata

技术团队

Roy Li： 知名网络安全专家，物联网专家，复旦大学硕士生导师。曾任诺基亚（北美）技术总监，负责OVI开发平台及Symbian操作系统的研发。为Symantec、VeriSign等安全公司提供安全咨询服务。TNB, RealChain, AIDOC 顾问。

Alex Goh： 前360云总裁、惠普中国副总裁、复星投资东南亚负责人。

投资人团队

- 极客帮基金
- 景林资本
- 戈壁资本
- 边江 原百度产品总监，盛大副总裁；WeXFin 创始人 & CEO，洪泰基金 Aplus 管理合伙人
- 孔华威 中科计算所上海分所所长
- 王岳华 德丰杰龙脉基金合伙人

路线图

Ruff 将是一个基于物联网的全新底层构架平台，有去中心化、开放、开源和高效的特点。在生态系统中，不同的参与方可以通过提供资源获取代币回报，或是消费代币获取资源，并且彼此分享，形成一个经济驱动的自治体。

Ruff 公有链开源计划

在我们完善了产品的基础框架之后，我们会对我们的核心模块逐步开源，让更多的研发者们加入。

日期	开源内容
2017年12月	超大规模、超低延迟的共识算法
2018年04月	超大规模区块链账本算法
2018年10月	智能合约架构算法
2019年03月	Ruff 公有链 平台

---

1. THIS DOCUMENT AND ANY OTHER DOCUMENTS PUBLISHED IN ASSOCIATION WITH THIS WHITE PAPER RELATE TO A POTENTIAL TOKEN OFFERING TO PERSONS (CONTRIBUTORS) IN RESPECT OF THE INTENDED DEVELOPMENT AND USE OF THE NETWORK BY VARIOUS PARTICIPANTS. THIS DOCUMENT DOES NOT CONSTITUTE AN OFFER OF SECURITIES OR A PROMOTION, INVITATION OR SOLICITATION FOR INVESTMENT PURPOSES. THE TERMS OF THE CONTRIBUTION ARE NOT INTENDED TO BE A FINANCIAL SERVICES OFFERING DOCUMENT OR A PROSPECTUS. THE TOKEN OFFERING INVOLVES AND RELATES TO THE DEVELOPMENT AND USE OF EXPERIMENTAL SOFTWARE AND TECHNOLOGIES THAT MAY NOT COME TO FRUITION OR ACHIEVE THE OBJECTIVES SPECIFIED IN THIS WHITE PAPER. THE PURCHASE OF TOKENSREPRESENTS A HIGH RISK TO ANY CONTRIBUTORS. TOKENS DO NOT REPRESENT EQUITY, SHARES, UNITS, ROYALTIES OR RIGHTS TO CAPITAL, PROFIT OR INCOME IN THE NETWORK OR SOFTWARE OR IN THE ENTITY THAT ISSUES TOKENS OR ANY OTHER COMPANY OR INTELLECTUAL PROPERTY ASSOCIATED WITH THE NETWORK OR ANY OTHER PUBLIC OR PRIVATE ENTERPRISE, CORPORATION, FOUNDATION OR OTHER ENTITY IN ANY JURISDICTION. THE TOKEN IS NOT THEREFORE INTENDED TO REPRESENT A SECURITY INTEREST.↩