The decentralized and distributed characteristics of blockchain share similar commonality with the distributed characteristics of IoT. According to a report issued by IBM, IoT may be the best application scenario of blockchain technology.

Among the current blockchain projects in the IoT field, the most famous one is IOTA. As a well-known thousand-times currency, its present price has soared by some 5000 times over its original crowd-funding price 15 years ago. Then, as a bottom-layer distributed operating system, what new differences has Ruff Chain brought to IoT?

Ruff Chain is an architecture integrating IoT with blockchains, composed of a distributed operating system and an open main china. The core issues to be addressed by Ruff Chain are the trusted interoperability and paid interoperability among IoT equipment and devices in different systems, for, at present, IoT is a separated and closed system.

Then, how can Ruff Chain realize trusted interoperability among IoT equipment and devices of various brands?

Firstly, each smart device has an address, which is written into the hardware by the supplier when sold, with the two-dimensional code for this address private key put in the hardware package box. Through acquiring the private key, the control center sends a binding instruction (with this private key signature) to the device and gains entire control of this hardware. After binding, the control center may delete the private key of the device and only needs to save the private key of control center itself.

In such a way, all the equipment and devices in the IoT can be controlled point to point, namely, the control center operates the device by sending a control TX with its own signature to the device. Besides, control can be achieved based on chain status. When the control end can not establish point-to-point connection with the device, the control end may consume some tokens and write a “Status Change” TX into the chain or “Control Command” TX to operate the target device. The target device may directly synchronize the status or control command through the chain, or synchronize the status or control command through a trusted light node (e.g. a bridge device). The blockchain has addressed the issues of cloud operation and maintenance costs and stability after all equipment and devices are connected to the cloud.

Lastly, all the IoT node devices are automatically controlled, with no need for the use of contract to set up the logic of “shutting down the air conditioner when the air temperature is below 15 degrees”. These automatic control logics can be realized at the control end (an app) with the traditional development language, reducing the hardware costs needed for devices’ support of contract and also decreasing the possibility of main chain crash due to contract operation.

In addition to the utilization of blockchain technology to realize trusted interoperability among IoT devices, Ruff Chain also offers time sequence data, consensus mechanism and lightning-chain-like-based negative review mechanism.

● Time Sequence Data: Most IoT data are time sequences, with natural bonds with blockchains. Data affixed with time stamps can, by themselves, prevent replay attacks and avoid dead locks due to concurrency. These data are not effectively integrated in previously separated centralized networks to address the final consistency of data in flow. In scenarios common to us, such as product source tracing, data are often repeatedly input into centralized systems like ERP, MES and WMS in product manufacture, storage and circulation, and the consistency of those links is totally un-guaranteed. Edge calculation nodes in Ruff Chain take synchronized time stamps as the core, for controlling the business logic within the LAN. Within the entire blockchain network, time stamps are synchronized, and, by tracing the behavior of all network nodes at one moment, the status of network at that moment can be restored.

● Consensus Mechanism: Considering the computing capacity of IoT main control equipment, we choose DPoS as the consensus algorithm. Based on this algorithm, token holders in the entire network can select block producers through the voting system; once selected, anyone can participate in block production.

● Lightning-chain-like-based Negative Review Mechanism: A control node can create a fixed-format contract at the main chain through a TX: CreateContract. Common contract contents include: “If you give me certain tokens, I’ll allow you to use the following command on condition that …”. After a contract is successfully created, the height of block saving the contract and the hash of that TX (collectively, Contract Addr) will be returned.

Ruff Chain can strongly withstand replay attacks in terms of privacy and security, since the local ad hoc network of Ruff Chain is decentralized. Once any fault occurs at a main application node in a local application network, the application logic will drift to another node to continue completion so as to guarantee the consistency of local application network.

The security of IoT itself is guaranteed by OS itself. Ruff Chain adopts symmetric keys, and keys are not transmitted in the network. Besides, the chain network releases time-stamp-based one-time tokens to the application network, so as to withstand replay attacks.

In future, Ruff Chain will be a brand new IoT-based underlying architecture platform, characterized by decentralization, development, open source and high efficiency. In ecosystem, different participants may provide resources to acquire token returns or consume tokens to acquire resources and share resources to form an economically-driven autonomy.

Click to know more about Ruff Chain ⤵️  
Website: RuffChain.com  
Twitter: [https://twitter.com/Ruff\_Chain](https://twitter.com/Ruff_Chain" \t "https://medium.com/ruffchain/_blank)  
Facebook: [https://www.facebook.com/RuffChainProject/](https://www.facebook.com/RuffChainProject/" \t "https://medium.com/ruffchain/_blank)  
GitHub [https://github.com/RuffNotes/RuffChain](https://github.com/RuffNotes/RuffChain" \t "https://medium.com/ruffchain/_blank)

# ****Ruff Chain：实现区块链与物联网的深度融合****

区块链的去中心化和分布式特性与物联网的分布式特性具有相似的共性。根据 IBM 发布的报告，物联网可能是区块链技术的最佳应用场景。

目前物联网领域的区块链项目中，最著名的就是IOTA。作为家喻户晓的千倍币，它现在的价格比15年前的众筹价格飙升了近5000倍。那么，作为底层分布式操作系统，Ruff Chain给物联网带来了哪些新的不同？

Ruff Chain是物联网与区块链相结合的架构，由分布式操作系统和开放的主链组成。Ruff Chain要解决的核心问题是不同系统的物联网设备和设备之间的可信互操作和付费互操作，因为目前物联网是一个分离的封闭系统。

那么，Ruff Chain如何实现物联网设备与各品牌设备之间的可信互通呢？

首先，每个智能设备都有一个地址，供应商在销售时将其写入硬件，并将该地址的二维码私钥放入硬件包装盒中。通过获取私钥，控制中心向设备发送绑定指令（带有该私钥签名），从而获得对该硬件的全部控制权。绑定后，控制中心可以删除设备的私钥，只需要保存控制中心自己的私钥即可。

这样，物联网中的所有设备和设备都可以实现点对点控制，即控制中心通过向设备发送带有自己签名的控制TX来操作设备。此外，还可以根据链的状态进行控制。当控制端无法与设备建立点对点连接时，控制端可能会消耗一些令牌并将“状态更改”TX或“控制命令”TX写入链中以操作目标设备。目标设备可以直接通过链同步状态或控制命令，也可以通过可信轻节点（如桥接设备）同步状态或控制命令。区块链解决了所有设备设备都上云后的云运维成本和稳定性问题。

最后，所有的IoT节点设备都是自动控制的，不需要通过合约来设置“气温低于15度关空调”的逻辑。这些自动化控制逻辑可以用传统的开发语言在控制端（app）实现，降低设备支持合约所需的硬件成本，也降低了合约运行导致主链崩溃的可能性。

除了利用区块链技术实现物联网设备之间的可信互操作外，Ruff Chain还提供时序数据、共识机制和基于闪电链的负面评价机制。

● 时序数据：大部分物联网数据都是时序数据，与区块链有着天然的联系。带有时间戳的数据本身可以防止重放攻击并避免由于并发导致的死锁。这些数据没有有效地集成到以前分离的集中式网络中，以解决流中数据的最终一致性。在我们常见的场景中，比如产品溯源，在产品制造、存储、流通等环节，数据往往会重复输入到ERP、MES、WMS等中心化系统中，这些环节的一致性完全无法保证。Ruff Chain 中的边缘计算节点以同步时间戳为核心，用于控制局域网内的业务逻辑。在整个区块链网络中，时间戳是同步的，通过跟踪所有网络节点的行为，在某一时刻，

● 共识机制：考虑到物联网主控设备的计算能力，我们选择DPoS作为共识算法。基于该算法，全网代币持有者可以通过投票系统选择区块生产者；一旦被选中，任何人都可以参与区块生产。

● 基于类闪电链的负面审查机制：控制节点可以通过一个TX：CreateContract在主链上创建一个固定格式的合约。常见的合约内容包括：“如果你给我某些代币，我将允许你使用以下命令，条件是……”。合约创建成功后，会返回保存合约的区块高度和该笔交易的哈希值（合称合约地址）。

由于 Ruff Chain 的本地 ad hoc 网络是去中心化的，因此 Ruff Chain 在隐私和安全方面可以很强地抵御重放攻击。一旦本地应用网络中的主应用节点发生故障，应用逻辑将漂移到另一个节点继续完成，以保证本地应用网络的一致性。

物联网本身的安全性是由操作系统本身来保证的。Ruff Chain采用对称密钥，密钥不在网络中传输。此外，链网向应用网络发布基于时间戳的一次性代币，以抵御重放攻击。

未来，Ruff Chain将是一个全新的基于物联网的底层架构平台，具有去中心化、开发、开源、高效的特点。在生态系统中，不同的参与者可以通过提供资源来获取代币收益，也可以通过消耗代币来获取资源并共享资源，形成经济驱动的自治。