使用 CITA 的通信加密

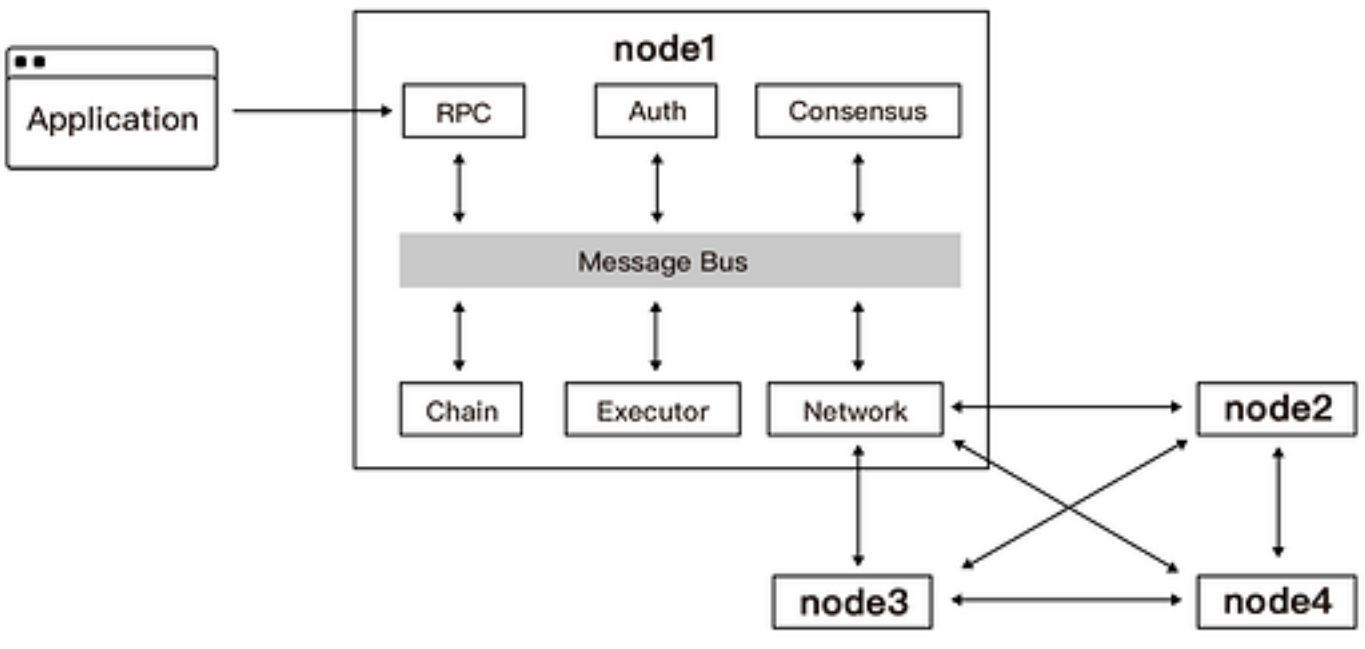
李耀荣 溪塔科技 2月4日



本文是溪塔科技区块链开发者李先生的「带你玩 CITA」的区块链技术分享，从一个一线开发者的角度来谈谈区块链技术的方方面面。本文是「李先生带你玩 CITA」系列第三篇文章，在本文中，李先生将和大家交流通信加密二三事。

本文转自 CITAHub 开源社区，略有删改。

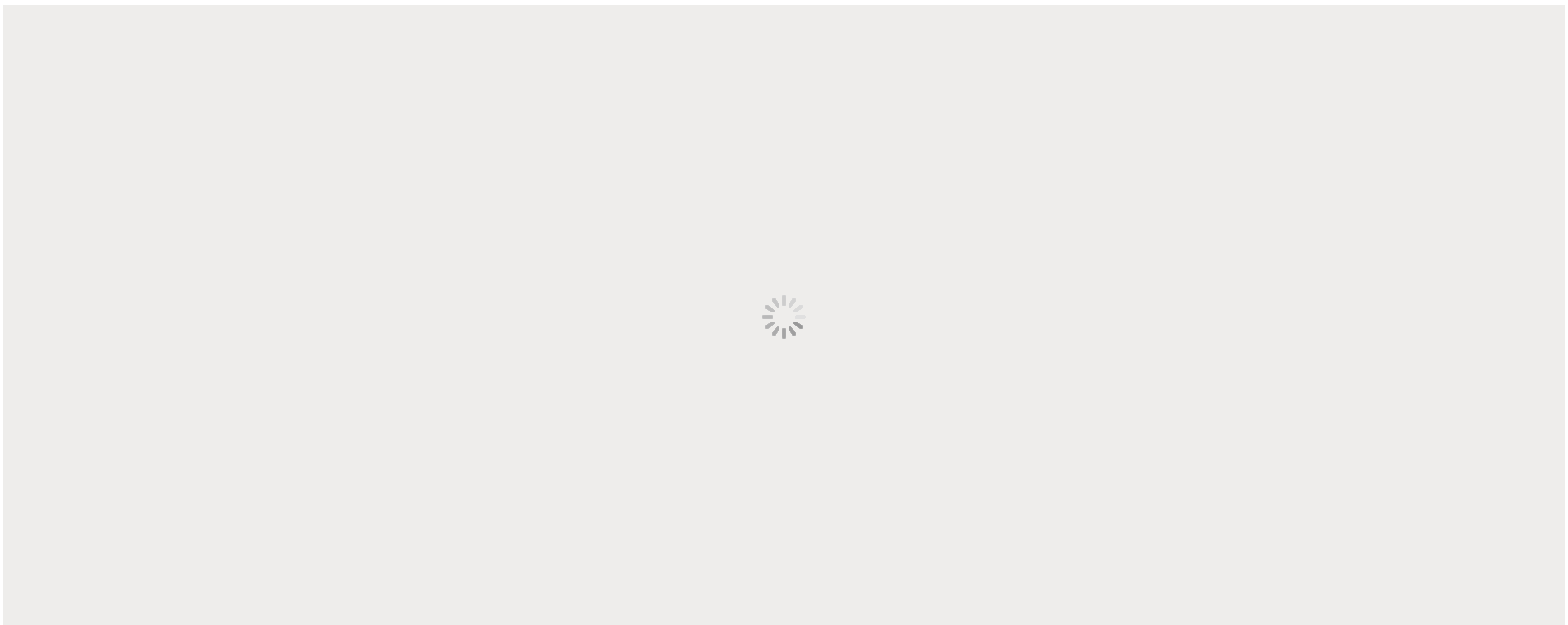
为了客户的数据安全，我强烈推荐大家在生产境中部署 CITA 时，考虑使用 CITA 的通信加密。首先，从 CITA 的系统架构图可以看到，在 CITA 系统中，主要有两部分是跨网络的通信：



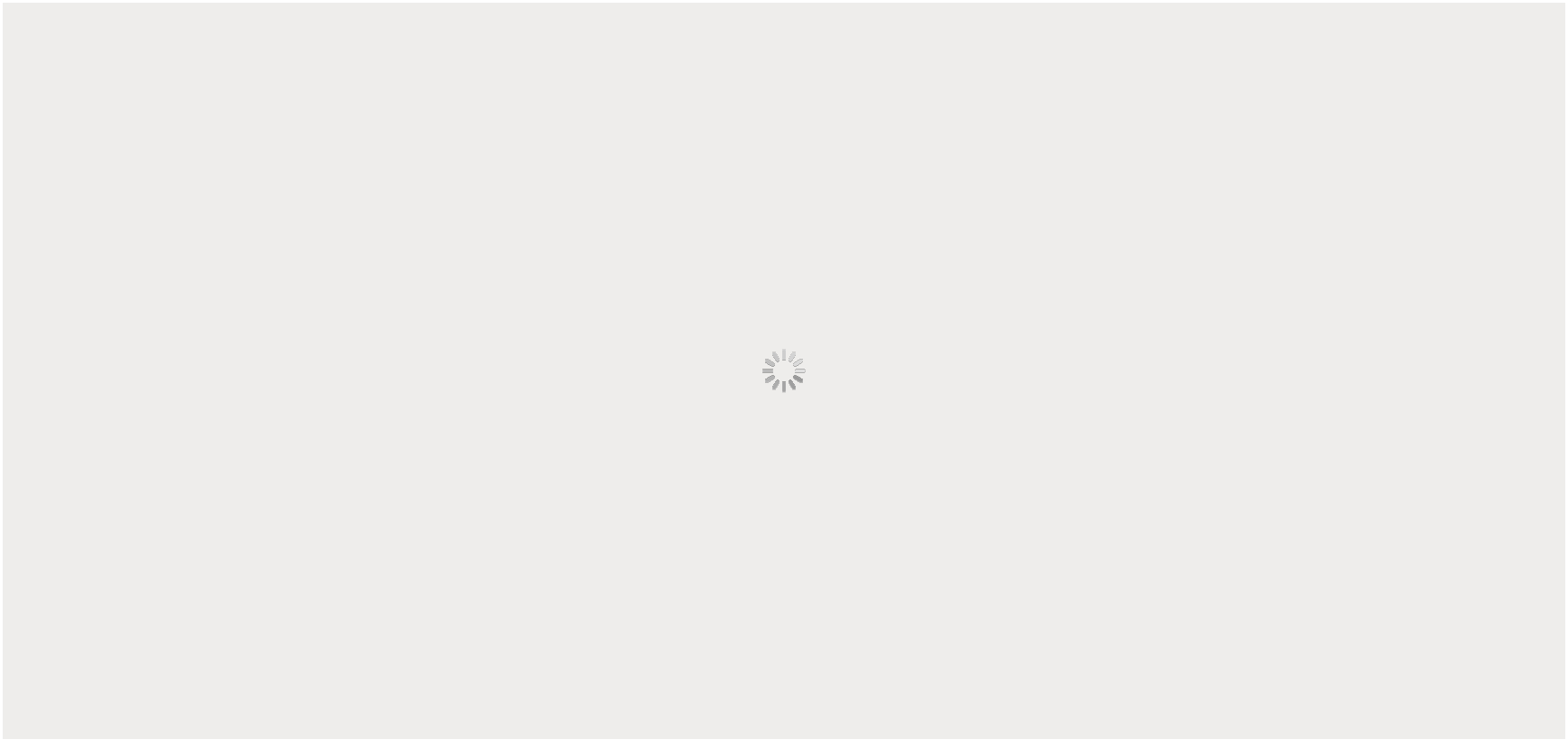
1. Application <-> RPC， 即应用与 RPC 的通信。
2. node <-> node，即 CITA 节点间的通信。

节点间通信加密

可以网络抓包与分析工具 （我这里使用 tcpdump 与 wireshark）先看一下，使用了通信加密与不使用通信加密的差别。



上图是在节点间没开启通信加密抓到的数据包，可以看到，里面的信息是明文，很容易被工具读取并分析。那接下来再看看开启了通信加密后，同样相近的数据包是怎么样子:



可以看到，里面的通信信息经过了加密，抓包工具是不可读取并分析里面的数据的。

如何开启节点通信加密

可以在创建网络 （ create ）或添加节点（ append ）时传入选项 --enable_tls 来开启。如

创建网络：

```
$ bin/cita create --enable_tls --super_admin "0x37d1c7449bfe76fe9c445e626da06265e9377601" --nodes "127.0.0.1:4000,127.0.0.1:4001"
```

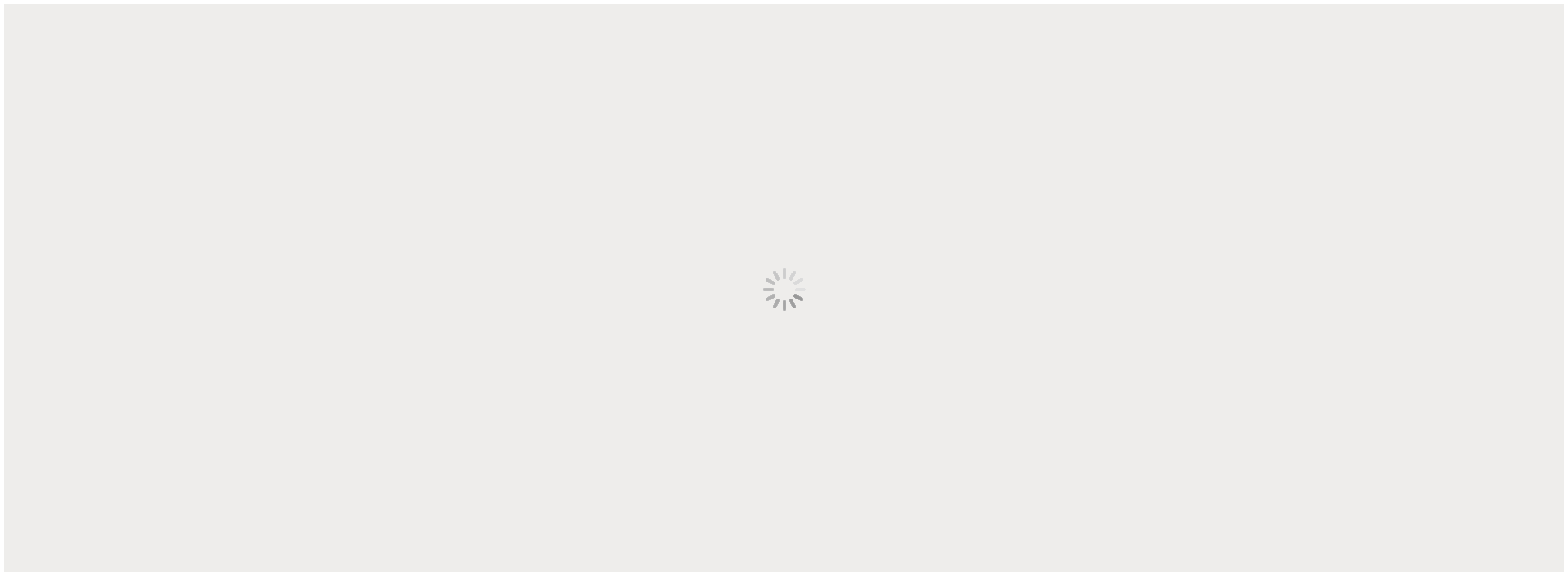
添加节点：

```
$ bin/cita append --chain_name test-chain --enable_tls --node "127.0.0.1:4004"
```

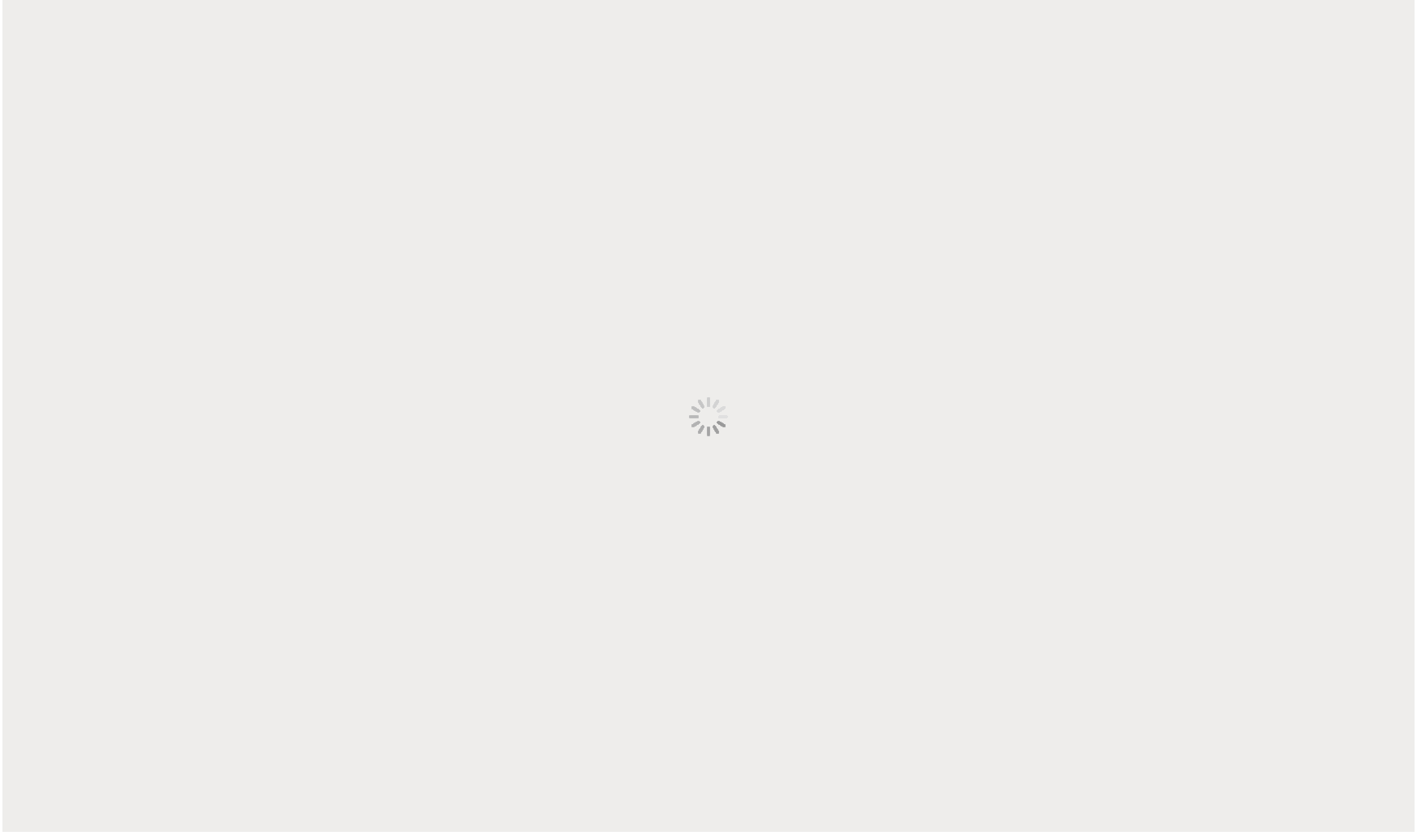
应用与 RPC 通信加密

首先，也先看一下添加通信加密与没有通信加密的情况下的数据包情况，大家有个直观的感受。

没有通信加密的数据包情况：



有通信加密的数据包情况：可以看到，有通信加密时的数据包完全不可读！



如何开启应用与 RPC 间通信加密

由于 RPC 是 http 协议，所以只需要使用 Nginx 将 http 反向代理成 https 就可以了。然后应用使用 https 与 RPC 进行加密通信。大家可以看到，现在 CITA 的测试链（访问地址 https://node.cryptape.com 1）访问就是使用了这个技术进行通信加密。

关于如何配置 Nginx ，网络上有很多材料，在此不打算展开描述。

关注公众号：溪塔科技，回复“交流群”，加入到区块链开源社区 CITAHub 大家庭中。 开源企业级区块链内核 CITA 点赞地址：https://github.com/citahub/cita

延展阅读

[研报] 存证将成为区块链的一个大规模应用场景

[研报] MakerDAO 深度报告

[研报] 隐私币应用全景观察

[研报] 区块链正在重塑法律

[研报] 控制个人数据滥用，谁是更好的答案?

[观点]溪塔科技联合创始人姚文婉：打造可分层数据治理网络基础设施

[观点] 区块链行业发展现状与解决方案

[观点] 任何公司都能用上区块链吗?

[观点] 区块链的价值在于分工与积累

[合作] 溪塔科技与北斗区块链达成战略合作

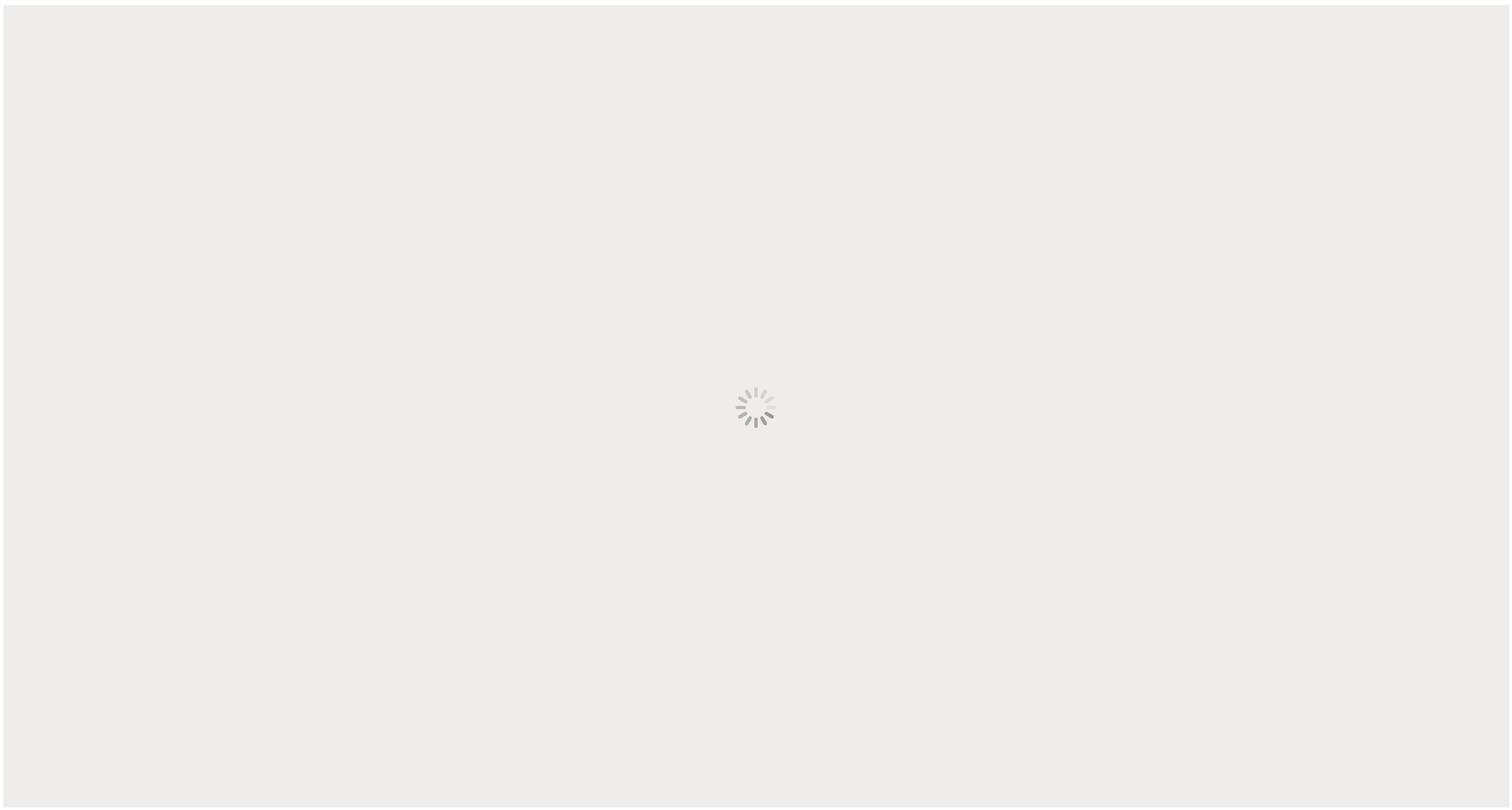
[合作] 区块链工程实训基地落户广州 溪塔科技等多方共建

[合作] 蓝亚科技、锌链接、法捕快、零识区块链等 4 家企业机构加入 CITAHub

[合作] CITA v1.0.0 正式发布！溪塔科技等多家核心企业共同维护后续开发

[合作] 溪塔科技宣布正式成立，助力数字时代企业间合作

更多咨询请关注溪塔科技公众号↓



阅读原文