BBChain 对数字雷亚尔采用背后的技术背景的看法

M. G. B. de Avellar[1], ⁎, A. A. S. Junior[1]•, A. H. G. Lopes[1]○, A. L. S. Carneiro[1]◇, J. A. Pereira[2]⋆ 和 D. C. B. D. da Cunha[2]‡

[1]BBChain | 儒塞利诺·库比契克大道 1327 号，4 楼 – 41 号套间 CV 1152 – 新康塞桑区 邮编：04543-011 – 圣保罗州圣保罗市[2]微软公司 |儒塞利诺·库比契克大道 1909 号，16 楼 - 新康塞桑区 邮编：04543-900 - 圣保罗州圣保罗市

⁎ marcio.g.avellar@bbchain.com.br.
• alexandre.junior@bbchain.com.br
○ andre.lopes@bbchain.com.br◇
carneiro@bbchain.com.br⋆
jopereira@microsoft.com
‡ davicunha@microsoft.com

arXiv:2304.04833v1 [cs.DC] 10 Apr 2023

摘要

本文以 Microsoft 的 CCF 框架为例，探讨了机密计算在央行数字货币背景下的应用。通过开展实验，并比较不同方案的性能与安全指标，我们旨在评估机密计算在提升央行数字货币的隐私、安全性和性能方面的有效性。我们的初步研究结果表明，机密计算可能是应对央行数字货币所面临技术挑战的一种有前景的解决方案。在 Hyperledger Besu 等分布式账本技术中实施机密计算，并使用 CCF 等框架，可以增强交易的机密性和隐私，同时保持全球数字金融体系所需的可扩展性和互操作性。总之，机密计算有望在央行数字货币的开发和部署中发挥关键作用，助力金融市场迈向更安全、更私密、更高效的未来。

关键词： 数字雷亚尔；机密计算；CCF

本sse 文章属于以下专题子领域：信息技术，并提交至征文启事 | 金融代币化：从加密资产到央行数字货币。

1. 引言

巴西中央银行于2023年3月6日启动数字雷亚尔试点阶段。数字雷亚尔是巴西雷亚尔（巴西法定货币）的代币化版本(Sciarretta 2023；Banco Central do Brasil 2023*a*)。预计到2024年底，数字雷亚尔将面向特定领域推出。数字雷亚尔是一种央行数字货币（中央银行数字货币），即由一国中央银行发行、旨在作为国家货币数字形式的数字货币，因此受政府监管。央行数字货币不同于稳定币，稳定币的价值与某种参考资产挂钩，由金融机构发行；央行数字货币也不同于加密货币，例如比特币(Nakamoto 2009) 和以太坊(Buterin2014)，它们可由任何实体发行，其价值浮动，随市场力量而变化。

这一倡议紧随全球金融市场中一场大胆的创新浪潮而来，有望彻底革新并推动数字经济发展，降低对中介机构的需求，同时实现即时支付（如PIX[1]）、更快的速度、更低的交易成本、更高的可扩展性以及更大的金融包容[2]。总体而言，如果央行数字货币得到采用，减少洗钱和腐败也将是值得期待的潜力。已有十一个国家

[1] 如今，PIX 已拥有超过 1.22 亿活跃用户，占巴西人口的 57%。得益于这项创新，40% 的用户完成了他们的首次电子转账，这表明该技术在促进金融包容方面具有巨大的潜力。 (Valente andTeixeira 2022)。[2] 这对于巴西而言是一个重要问题，因为巴西拥有数量众多的“功能性未银行化人群”。尽管巴西有 1.89 亿公民与国家金融体系（SFN）存在关系，但其中很大一部分人口无法获得信贷，也没有进行大额金融活动，例如投资及类似业务。请参阅(Banco Central do Brasil 2023*b*）以了解这些统计数据。

拥有其法定货币的数字版本，另一些则处于研究或开发阶段。请参见，例如，**Atlantic Council CBDC tracker**。

然而，央行数字货币的部署并非没有技术挑战。主要的技术顾虑与网络攻击及其他安全漏洞有关，例如交易这些资产的用户或实体的数据隐私。隐私面临的潜在威胁在于，中央银行原则上可以监控和追踪个人或机构的所有金融交易；而对于网络攻击，人们担心一旦成功攻击央行数字货币，可能会导致大量法定货币被盗，进而造成严重的经济 disruption。

多家以专业能力著称的国内外企业专业能力**(Mancini 2020；Gartner 2020)**一直在研究这些问题，并启动了一系列机密计算应用研究实验和项目，以解决这些问题。**(例如，参见Microsoft | Research 2022；Microsoft| Confidential Consortium Framework 2023*b*；BlockchainLab *by BBChain* | Research Division 2023)**。

在本文中，我们将介绍有望解决这些问题的新技术方案，深入探讨分布式网络框架 和 Microsoft 的 *Confidential Consortium Framework*中的机密计算概念。

我们将特别讨论其中一项实验——与一位保密合作伙伴共同开展的实验——在该实验中，创建了一个基于 Hyperledger Besu 的应用，用于处理数字资产的买卖，并使用法定数字货币的类似物作为支付手段，换言之，即央行数字货币 **（BlockchainLab *by BBChain*| ResearchDivision 2023）**。

2. 隐私、保护与机密计算

央行数字货币通常使用区块链或分布式账本技术[3], 去中心化且安全的技术来执行交易、记录和验证数字资产。这些技术创建由分布式节点网络维护和验证的共享交易数字记录。安全性通过密码学技术得到保障，例如数字签名和哈希。

为了保护机密性和隐私，例如会使用仅限授权成员访问的私有网络、数据加密，以及对参与者身份进行假名化。不过，还必须兼顾隐私、安全性与可用性，因为没有任何系统是百分之百安全的。

通常情况下，敏感数据加密只能在数据需要处理之前提供保护；一旦需要处理，数据就会被解密并暴露于威胁之下。正因如此，以及其他原因，央行数字货币和稳定币等数字货币需要采取额外的数据安全措施，尤其是在金融机构大规模采用的情况下。

机密计算是一种范式，在不受信任的环境（如公有云或共享数据中心）中处理敏感数据时保护它们 **（例如，参见Costan and Devadas 2016；*Confidential Computing Consortium* 2023）**。BBChain 是探索这一计算范式的企业之一，旨在提升其解决方案的安全性，同时建议金融机构采用这一框架 作为 基准 来衡量数字资产。

2.1. *ConfidentialConsortium Framework*(CCF)

机密计算利用 可信执行环境(TEEs)，例如英特尔 SGX **(英特尔公司 2023)** 或 AMD SEV **(AMD | 开发者中心 2023)**，创建 Enclave，使敏感数据能够在安全且隔离的环境中进行处理。**图 1** 阐释了 Enclave 的概念。

Enclave是计算机内存中的特定区域，敏感数据可以在其中进行处理，并完全免受外部威胁的侵害，例如恶意软件或网络攻击。具体而言，设备启动时，处理器会分配一部分内存，将其与任何其他进程隔离，并专用于某个应用程序及其数据。Enclave 中的数据会被加密，以

[3] 实际上，区块链是分布式账本技术的一种。请参阅 **Anwar (2019)**，以详细了解分布式账本技术的类型和类别，以及它们的相似之处与差异。

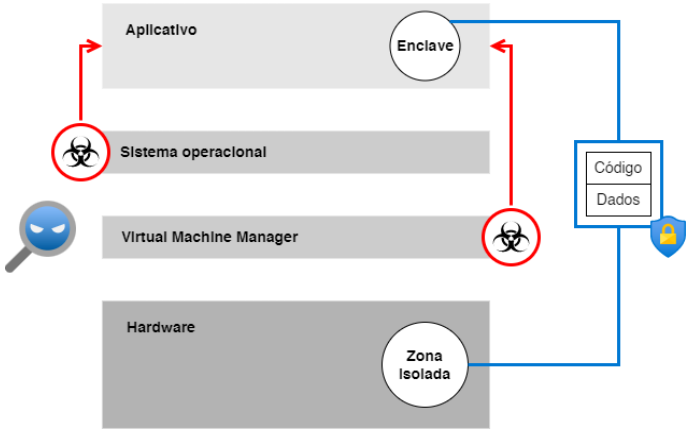


图1 创建飞地时所提供保护的抽象示意。处理器分配一部分内存，将其与任何其他进程隔离，专用于应用程序及其数据。飞地中的数据经过加密(**BlockchainLab** 由 *BBChain* 提供| **研究部门 2023**)。

避免遭受间谍活动或信息泄露，即使是在应用程序处理数据时也是如此。因此，即使操作系统或虚拟机监控程序遭到入侵，在 Enclave 中运行的应用程序和数据仍然安全。

由于这一基本特性，机密计算的应用领域包括医疗、金融、供应链和政府。在区块链/分布式账本技术等分布式环境中，这一范式非常有用，因为并非所有参与者都相互信任。

BBChain 是区块链/DLT 解决方案公司之一，一直在其解决方案中探索机密计算，开发了多项概念验证（PoC）和实验，以满足部署 CBDC 系统的功能性和非功能性要求，而数字雷亚尔正是拟议中的此类系统。因此，相关研究一直在使用 *Confidential Consortium Framework*（Microsoft（**Microsoft | Confidential Consortium Framework 2023*a*, *b***）。

CCF 是一个 开源框架 用于有状态高可用服务，将集中式计算的易用性和性能与去中心化的信任相结合。它允许在无需参与者之间相互信任的情况下，对机密数据执行可审计操作。

图 **2 展示了** CCF 如何结合中心化网络与去中心化网络的特点，而**表 1** 比较了三种实现方式。

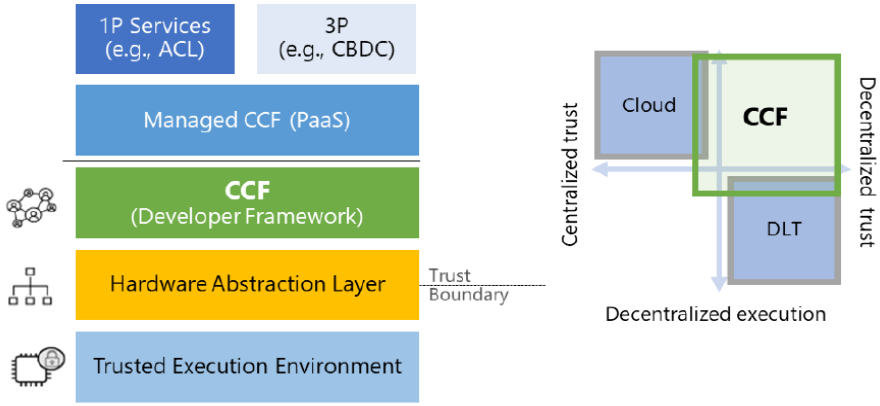


图 2 左侧为执行堆栈中的 CCF；右侧为 CCF 与其他分布式账本技术及中心化系统的对比**Microsoft | 研究 (2022)**。

传统数据库	许可型 DLT	Microsoft CCF
机密性		
• 传统的访问控制 基于角色的方式用于 私有数据。 • 节点运营商需要 值得信赖。	• 所有执行节点都能看到 所有交易。 • 需要昂贵的加密技术 来隐藏机密数据。 • 节点运营者通常 需要可信赖，才能保障 隐私。	• 对.....的可编程控制 在账本中是私有的。 • 只有治理机构 需要值得信赖，才能保护 隐私。 • 节点运营者默认不会获得 读取权限。
去中心化（网络安全）		
• 集中式治理带来 赋予运营商巨大的权力 nós. • 很多时候，力量源于纽带 更弱。攻破一个节点 可能就足够了。 • 节点的运行必须是一个 高权限。	• 通过复制 交易执行。 • 每个参与者都必须运行 一个执行节点。 • 可容忍最多 1/3 的节点 损坏。	• 通过治理， 管理机构控制获准的代码、 应用程序以及 节点运营者。 • 可验证的收据能够识别 恶意行为者。 • 在多个 TEE 平台，以限制¯奇米 硬件信任。 • 节点的运行是一个 无冗余含义的简单 нөкумити 特殊权限的简单 冗余。
可用性（韧性）		
• 需要热备份，并且 在许多情况下需要同步 交易。 • 不存在拜占庭故障场景。	• 所有部分节点 可靠的机密性和 完整性。 • 难以从故障中恢复 拜占庭式。	• 不可信节点运营者 以确保机密性/完整性。 • 灾难恢复， 依靠 HSM 或 成员共享。
性能		
• 交易的可扩展性没有上限， 无论是交易本身还是交易数据。 • 交易只执行 一次。 • 吞吐量和 延迟表现出色， 副本和分区。 • 最多可达到 5 万每秒交易数。	• 吞吐量和 延迟设置得不合理 参与者数量。 • 所有节点执行所有的 交易。 • 20.000 每秒交易数，无保护措施的 隐私。	• 无可扩展性限制 在治理联盟中。 ～ 已达到60.000每秒交易数。 • 吞吐量和 延迟可随副本数量 完美扩展。 交易只会 执行一次。 • 分区需要一个 会导致.....的特殊逻辑 性能权衡。
可审计性		
• 有必要创建一个 特殊验证机制 审计。无法保证这些数据的可用性。 违规证明 • 即便如此，运营者们的 节点必须值得信赖。	• 所有交易都是 可在账本中验证；若不可篡改 达成共识。 • 需要验证 至少获得 2/3 节点的一致同意，以 证明一笔交易曾经被 已执行。	• 所有交易，包括 a 治理，在账本中可验证。 • 通用离线收据 可验证，并具备证明保证 遭到违规侵害。
灵活性		
• 更适合该模型的#+#+#+#+ 账户。UTXO 需要表示法 复杂，且对 来源的验证会使操作 变得非常缓慢。	• 更适合 UTXO 模型。	• 支持 UTXO 和账户模式。

表 1 传统数据库、许可型分布式账本技术与 CCF 的比较 (Microsoft 丨 Research2022)。

CCF 具有与分布式账本技术相似的特点，例如由受章程约束的成员组成的联盟进行治理，以及由节点构成的网络。节点必须在 TEE 上运行，以确保去中心化和安全性。CCF 采用的共识协议是基于 Raft 的崩溃容错（CFT）。

更具体地说：

• **治理：** CCF 网络由受《宪章》约束的成员联盟治理。《宪章》就像一个通用智能合约，由一组最精简的 JavaScript 组成，构成一个模块，而该模块随后会被记录在账本本身中。《宪章》规定了网络在交易、智能合约等方面的规则。总体而言，成员负责治理网络，其公开身份会记录在框架中。成员与运营者有本质区别：运营者负责网络的运维工作，例如添加或移除节点，而其身份不会记录在 CCF 中。

• **节点：** 节点构成 CCF 网络。其含义与我们谈到区块链或 DLT 时相同。这些节点是有正当利益在网络内进行资产交易的自然人或法人。不过，这些节点的特殊之处在于，每个节点都必须运行在 TEE 上，也就是说，运行在一个 Enclave 中。因此，该网络是去中心化的。所有节点都运行以 JavaScript 或 C++ 编写的相同应用程序。

• **共识协议：** 区块链和分布式账本技术支持许多类型的共识协议，例如工作量证明、权益证明、权威证明以及许多其他协议。CCF 作为一个需要确保信任的去中心化网络，支持崩溃故障容错（CFT）。CFT 基于 Raft，但存在一些关键差异。也可以实现拜占庭容错（BFT）协议。

启动 CCF 网络涉及生成身份、初始化初始节点及其他节点，并提出网络开放提案。网络治理通过章程确立，章程由 JavaScript 脚本构成，这些脚本导出验证、解决和应用函数。

图**3 和 4 展示了如何初始化 CCF 网络以及将节点加入网络。借此，我们介绍了 CCF 机密计算的基本概念；事实证明，它适用于金融资产交易。**

```
{
  "enclave": {
    "file": "/opt/ccf_sgx/lib/libjs_generic.enclave.so.signed",
    "type": "Release",
    "platform": "SGX"
  },
  "network": {
    "node_to_node_interface": { "bind_address": "127.0.0.1:8081" },
    "rpc_interfaces": {
      "main_interface": {
        "bind_address": "0.0.0.0:8080"
      }
    }
  },
  "command": {
    "type": "Start",
    "service_certificate_file": "/home/myadmin/ccf-app-template/workspace/sandbox_common/service_cert.pem",
    "start": {
      "constitution_files": [
        "/home/myadmin/ccf-app-template/workspace/sandbox_common/validate.js",
        "/home/myadmin/ccf-app-template/workspace/sandbox_common/apply.js",
        "/home/myadmin/ccf-app-template/workspace/sandbox_common/resolve.js",
        "/home/myadmin/ccf-app-template/workspace/sandbox_common/actions.js"
      ],
      "members": [
        {
          "certificate_file": "/home/myadmin/ccf-app-template/workspace/sandbox_common/member0_cert.pem",
          "encryption_public_key_file": "/home/myadmin/ccf-app-template/workspace/sandbox_common/member0_enc_pubk.pem"
        }
      ]
    }
  }
}
```

图 3 使用“Start”命令演示配置文件(**BlockchainLab** 由 *BBChain* 提供 **研究部 2023**)。

3. 机密计算的研究与开发

A **图 5** 展示了本文所讨论实验的高层架构 (**BlockchainLab** *by BBChain* **研究部门 2023**)。该实验涉及发行用于批发买卖的证券

```
{
  "enclave": {
    "file": "/opt/ccf_sgx/lib/libjs_generic.enclave.so.signed",
    "type": "Release",
    "platform": "SGX"
  },
  "network": {
    "node_to_node_interface": { "bind_address": "127.0.0.1:8082" },
    "rpc_interfaces": {
      "main_interface": {
        "bind_address": "0.0.0.0:8083"
      }
    }
  },
  "node_certificate": {
    "subject_name": "CN=CCF Node",
    "subject_alt_names": ["iPAddress:127.0.0.1", "dNSName:ccf.dummy.com"],
    "curve_id": "Secp384R1",
    "initial_validity_days": 1
  },
  "command": {
    "type": "Join",
    "service_certificate_file": "/home/myadmin/ccf-app-template/workspace/sandbox_common/service_cert.pem",
    "join": {
      "retry_timeout": "1s",
      "target_rpc_address": "127.0.0.1:8080"
    }
  }
}
```

图 4 使用“Join”命令展示配置文件（**BlockchainLab** 由 *BBChain* 提供 **研究部 2023**）。

金融机构之间。

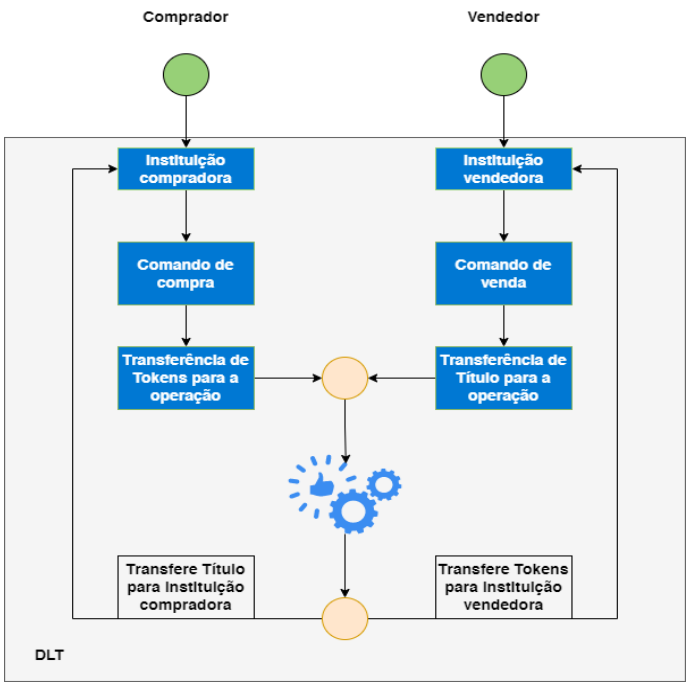


图 5 模拟数字货币使用场景的资产买卖应用（**BlockchainLab** 由 *BBChain* 提供 **研究部 2023**）。

该实验采用 Hyperledger Besu 模型，并在其上运行智能合约。这项开发将证明，该 DLT 及其创建的系统适用于此类资产交易，例如涉及政府债券以及稳定币/央行数字货币的交易。

机密计算是与 Hyper- 实验同步并行的一条研究路线。

使用 *Confidential Consortium Framework*– CCF 的 Besu 账本。

在当前研究阶段，目标是开发一项新实验，以实现批发型央行数字货币的间接模式；该架构模式是国际清算银行设想的四种模式之一 (**Auer andBöhme 2021**)，如**图 6**所示，摘自上述文章。

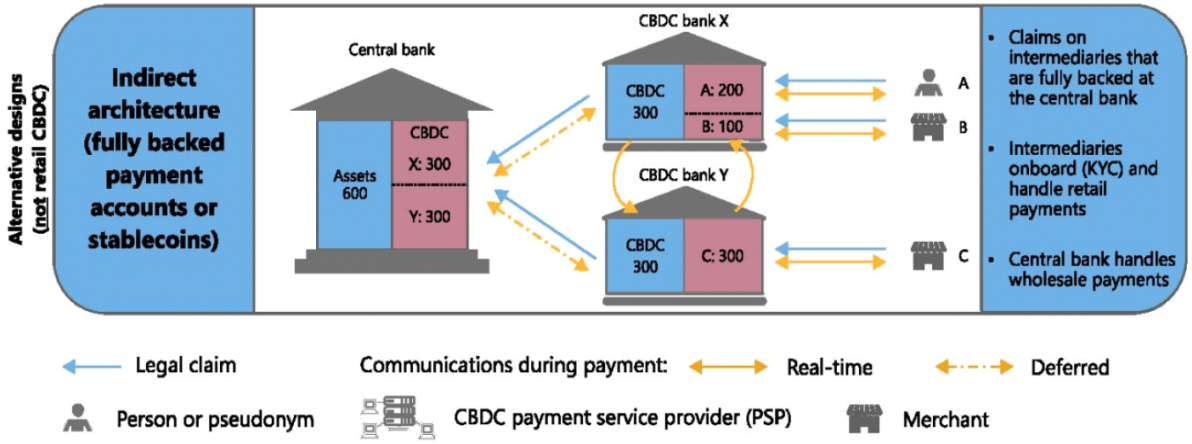


图 6 在间接架构中，CBDC 仅由中央银行发行和赎回，但这通过中介机构间接完成。中介机构则向消费者发行债权。中介机构必须以其在中央银行持有的 CBDC 全额支持每项债权。中央银行仅运营批发支付系统(**Auer 和 Böhme 2021**)。

因此，该设想是利用CCF 来模拟这一架构，鉴于巴西中央银行正在朝着CBDC 迈进，以及其他机构在稳定币方面的动向。

基于这项研究，我们希望对各种方案的表现进行量化，并将 CCF 作为一种市场选项纳入技术路线图中 (**BlockchainLab** *by BBChain* | **Research Division 2023**)。

3.1. 方法论

问题定义：使用分布式账本技术进行金融数据交易，需要采取额外措施，以确保隐私、交易安全、机密性和性能达到令人满意的水平，具体而言，应排除货币当局（例如中央银行）追踪已识别个人金融交易的可能性。

假设： 在分布式账本技术上实施机密计算将解决隐私和安全问题，因为即使在可信执行环境（TEEs）中处理数据时，数据也会保持加密状态。

具体的研究设计：

- 在 Hyperledger Besu 实验中启用对 TEE 的支持，将机密计算直接集成到该 DLT 中；
- 修改 Hyperledger Besu 实验，将 CCF 纳入机密计算场景；重构智能合约，确保其与 CCF 兼容（架构和功能）。
- 使用性能指标（KPI）比较两种场景：交易吞吐量；延迟；计算资源消耗；可扩展性。
- 安全指标的使用：抵御攻击的能力；

隐私保障；处理阶段的数据机密性。

- 解决方案对比：基于 HyperledgerBesu 且不具备机密计算能力的解决方案；基于 HyperledgerBesu 且具备机密计算能力的解决方案；与 CCF 集成的解决方案。
- 指标分析。

3.2. 进展到目前为止

Hyperledger Besu 环境功能正常且运行稳定，其中部署了通过央行数字货币的模拟形式进行资产买卖的应用程序。

正在实施于**BlockchainLab** 一个使用 CCF 作为概念验证的机密计算环境中，最初通过 你好，世界风格的应用，验证所有治理与审计流程(**BlockchainLab** 由 *BBChain* | **研究部门 2023**)。

如 **图 7 和 8** 所示，**BlockchainLab**系统中的节点数量有所增加。

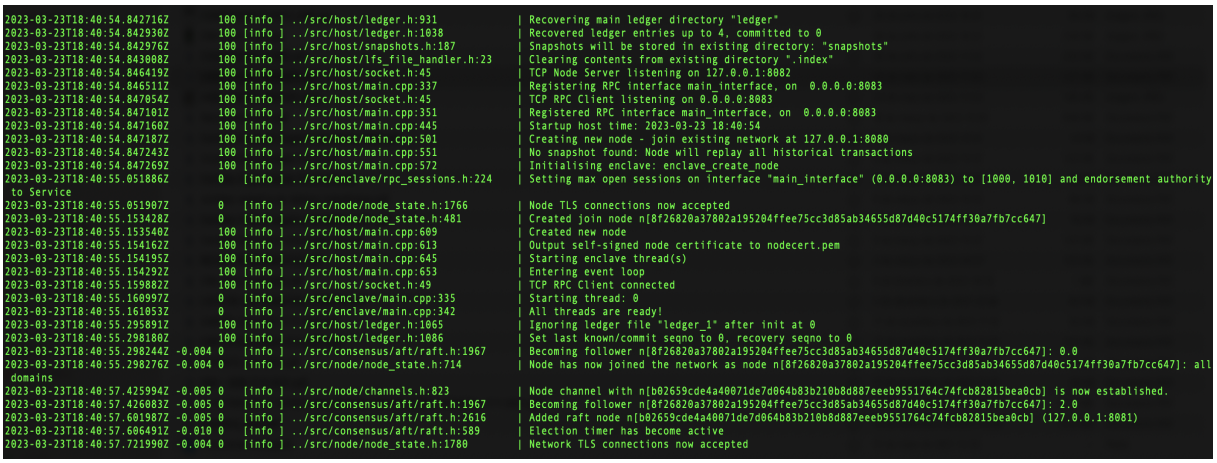


图7 节点进入 在网络中作为领导者 (**BlockchainLab** *by BBChain* | **研究部门 2023**) .

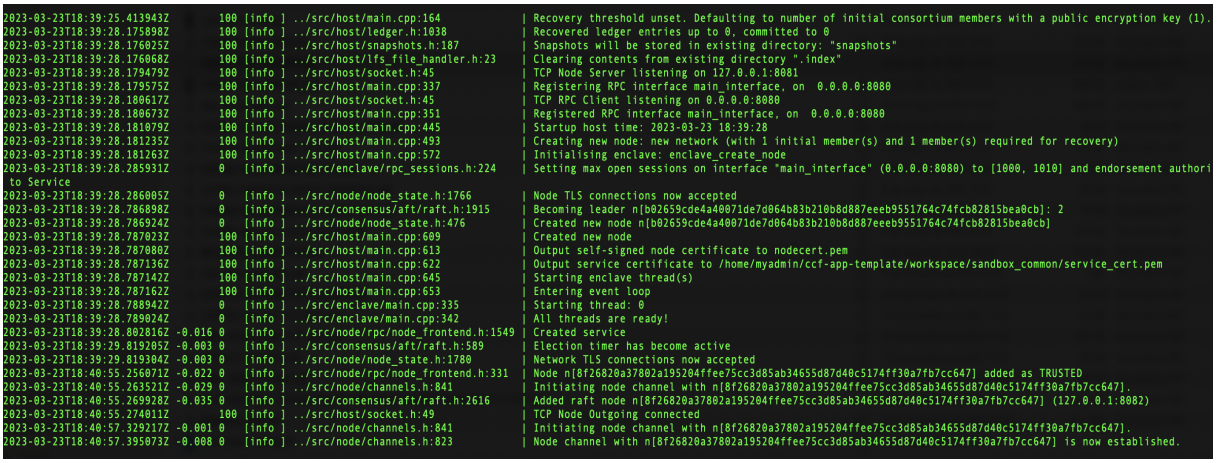


图8 节点作为跟随者 (**BlockchainLab** *by BBChain* | **研究部门2023**)。

研究团队的下一个目标是构建资产买卖应用程序，并将其作为案例研究，与在 Hyperledger Besu 上运行的应用程序进行比较。通过这项研究，我们将能够在类似情境下评估各类环境的优缺点，帮助所有相关方选择最适合自身需求的框架 。

4. 结论与展望

机密计算及其框架 代表着数据和代码保护与共享方式的一大进步。它们的潜在应用涵盖多个行业领域，例如金融市场、医疗行业和政府部门。

尤其是在金融和数字经济领域，机密计算将通过支持交易的安全执行，并确保个人及机密数据绝不会被任何未经明确授权的主体访问（包括 Microsoft、Google、AWS 和 Meta 等大型服务提供商及数据托管方），从而提升央行数字货币的安全性和隐私保护。

机密计算在央行数字货币应用背景下还有两个重要方面：一是与其他系统和平台的互操作性——例如与 PIX 等其他支付方式互通，甚至可实现更快捷、更安全的国际交易；二是合规监管。政府对此尤为关注，因为该系统从机制上便符合反洗钱（AML）和“了解你的客户”（KYC）规则。

巴西中央银行，正如我们已经提到的，已启动在 Hyperledger Besu 上实施数字雷亚尔的试点阶段(**巴西中央银行 2023*a***)。

Hyperledger Besu 根据技术标准被选为底层技术，但并不要求使用机密计算来保护交易的信息和数据。这种安全保障应采用其他网络安全技术。

在巴西中央银行的初始架构中，数字资产将通过数字雷亚尔的央行数字货币，在商业银行等金融机构之间进行批发交易。

因此，随着数字经济不断扩展，社会将面临一个关于数字货币未来的关键抉择：必须在主权货币形式与非主权货币形式之间作出选择。主权货币包括中央银行的货币（央行数字货币）、商业银行的货币，以及由受监管的金融或非金融机构发行的电子货币；所有这些形式都被归类为受监管的负债(**Kerigan 等，2022**)。

通过采用共享账本技术，这些法律工具可以在不对现行规则和法规作出重大改变的情况下得到呈现，从而有望解决该行业的一项重大挑战：缺乏全球性、多币种、多资产的金融结算系统。

这一基础为一种名为监管责任网络（RLN，英文缩写）的新型金融市场基础设施（FMI）提案铺平了道路。RLN 将运行一个共享账本，用于记录、转移和结算中央银行、商业银行及受监管机构的受监管负债。例如，随着稳定币 在部分司法管辖区被认可为一种受监管负债，它们也可以接入该网络，从而与其他形式的代币化货币实现互操作性，尤其是央行数字货币。

RLN 的主要目标是为主权货币体系建立一个持续运行、可编程且支持多资产的共享账本基础设施。该网络将促进参与机构之间以主权货币进行结算的“链上”最终交割，同时遵守所有现行规则和法规(**Kerigan 等，2022**)。

正是在这一背景下，CCF可能找到其最大的适用性。简而言之，RLN是这样一种概念：参与者网络遵守监管机构制定的具体规则和法规。这些网络通常处理敏感数据，要求参与者之间进行安全通信，同时还具备追踪和审计交易的能力。

因此，我们设想 CCF 可以通过以下方式帮助推动 RLN 概念的发展。 s:

- 更高的隐私性和安全性：在 RLN 中，TEE 将大有裨益，因为隐私和安全至关重要。
- 增强的信任与合规性：CCF 能够创建具有高度信任度的去中心化应用，因为参与者可以在 TEEs 内部验证代码的正确执行。

- 可扩展性和性能：CCF 经过设计，可提供高吞吐量和低延迟，使其适用于大规模 RLN。此外，该平台能够在不牺牲性能的情况下处理大量交易，这有助于推动 RLN 中去中心化应用的采用。

- 互操作性：CCF 可以与多个区块链平台及其他分布式账本技术集成，实现不同系统之间的无缝交互。这种互操作性将促进 RLN、监管机构及生态系统中其他利益相关者之间的协作。
- 审计与监控：CCF 的集成功能（例如防篡改日志）可实现高效且透明的审计流程，使 RLN 自动满足监管要求，并为持续改进提供信息。
- 灵活的治理模式：CCF 可以适应不同的治理结构，使 RLN 能够根据其监管和组织需求实施定制化的治理模式。

互操作性尤其有助于与巴西的 PIX 等其他电子支付系统集成；此外，巴西中央银行还选择了 DLT Hyperledger Besu 作为数字雷亚尔试点项目的平台。

总而言之，CCF 可以为受监管责任网络的发展作出重大贡献，提供更高的隐私、安全性和合规性，同时促进可扩展性、互操作性和灵活的治理模式。

巴西企业一直在大力投资培养能够改进区块链/DLT 技术并在巴西实施具有重大社会影响力系统的人才**(BlockchainLab** *by BBChain* **| 2023 年研究部门)**以及在世界各地。

尤其是，像**BlockchainLab**[4]，凭借其技术多样性和治理即服务，处于分布式账本技术的前沿，并紧随新的计算范式。

5. 致谢

作者感谢 BBChain 的鼓励，并感谢 Microsoft 提供的机会。作者还感谢 Microsoft 的 Davi Castelo Branco Dias da Cunha 对本文的审阅。

6. 利益冲突

就这项研究而言，不存在利益冲突。

[4] 如需了解有关**BlockchainLab**及其能力、创新和构思流程的更多信息，请参阅**de Avellar（2023）**在坎皮纳斯州立大学科学与技术政策系技术创新战略管理专业课程中提交的专著。

参考文献

AMD | Developer Central（2023），《AMD 安全加密虚拟化（SEV）》。网址：https://developer.amd.com/sev/，访问于 09/03/2023。Anwar, H.（2019），《分布式账本技术：技术革命由此开启》，101 Blockchains。网址：https://101blockchains.com/distributed-ledger-technology-dlt/，访问于 21/02/2023。Auer, R. 和 Böhme, R.（2021），《中央银行数字货币：探索最低侵入性的技术》，BIS 工作论文第 948 号。网址：https://www.bis.org/publ/work948.pdf，访问于 21/02/2023。巴西中央银行（2023a），《数字雷亚尔新闻发布会》。网址：https://www.youtube.com/watch?v=LCycE9mfH2U，访问于 17/03/2023。巴西中央银行（2023b），《涉及的关系、CPF 和 CNPJ 统计数据》，巴西中央银行 | 信息公开，金融系统客户登记 | CCS CCS 统计数据。网址：https://www.bcb.gov.br/acessoinformacao/ccsestatisticas?page=1.，访问于 22/02/2023。BBChain 的 BlockchainLab| 研究部（2023），《BlockchainLab 路线图》。Buterin, V.（2014），《以太坊白皮书：新一代智能合约与去中心化应用平台》，Ethereum Org。网址：https://ethereum.org/en/whitepaper/，访问于 22/02/2023。Confidential Computing Consortium（2023）。网址：https://confidentialcomputing.io/，访问于 17/03/2023。Costan, V. 和 Devadas, S.（2016），《Intel SGX 详解》，IACR 密码学电子印本档案 2016，86。网址：https://eprint.iacr.org/2016/086.pdf，访问于 17/03/2023。de Avellar, M. G. B.（2023），《BlockchainLab：商业模式创新史》，科学与技术政策系 |坎皮纳斯州立大学（Unicamp）。Gartner（2020），《2020 年区块链技术炒作周期》。网址：https://www.gartner.com/en/documents/3987450，访问于 17/03/2023。Intel Corporation（2023），《Intel 软件防护扩展（Intel SGX）》。网址：https://www.intel.com/content/www/us/en/architecture-and-technology/software-guard-extensions.html，访问于 09/03/2023。Kerigan, N., Kohli, V., Lau, V., Left, P., Low, M., Marroitt, L., McLaughlin, T., Prendergast, J., Shepherd, M., Swanson, C. 和 Ward, J. C.（2022），《受监管负债网络》，《受监管负债网络：数字主权货币》。网址：https://regulatedliabilitynetwork.org/wp-content/uploads/2022/11/The-Regulated-Liability-Network-Whitepaper.pdf，访问于 23/03/2023。Mancini, C.（2020），《BBChain 是 Gartner 最佳区块链公司榜单中唯一一家来自拉丁美洲的企业》。网址：缩短链接：https://bityli.com/wzl7vb，访问于 17/03/2023。Microsoft |Confidential Consortium Framework（2023a），《基于共同可信数据源，在多方之间构建企业级应用》。网址：https://ccf.microsoft.com/，访问于 09/03/2023。Microsoft | Confidential Consortium Framework（2023b），《什么是 CCF？》。网址：https://microsoft.github.io/CCF/main/overview/what_is_ccf.html，访问于 09/03/2023。Microsoft | Research（2022），《Microsoft 对数字货币格局的看法》。Nakamoto, S.（2009），《比特币：一种点对点电子现金系统》。网址：http://www.bitcoin.org/bitcoin.pdf，访问于 21/02/2023。Sciarretta, T.（2023），《巴西中央银行启动测试并确定数字雷亚尔架构》，Valor Econômico | 加密货币。网址：https://valor.globo.com/financas/criptomoedas/noticia/2023/03/06/bc-inicia-testes-e-define-arquitetura-do-real-digital.ghtml，访问于 09/03/2023。Valente, R. 和 Teixeira, L.（2022），《巴西有望通过在 2024年 实施中央银行数字货币赢得经济领导地位》，COINTELEGRAPH BRASIL。网址：https://cointelegraph.com.br/news/brazil-could-cement-its-status-as-an-economic-leader-thanks-to-2024-cbdc-move，访问于 09/03/2023。