

# Hacash L3: 一种将健全货币接入日常经济的多链系统

作者: Hacash.com团队(2022)

本白皮书是由 Hacash.com 团队提议的 Hacash 三层多链、多账本、多技术扩容和可编程经济平台 ( 简称 L3 ) 的生态建构和应用场景说明文档。

L3 技术实现方面的细节描述和代码证明将在下一篇《Hacash L3 技术黄皮书》中给出。

## 以 Hacash 健全货币为基础

HACASH(ㄗ) 是一个去中心化加密货币系统 ( L1 ) , 目标是成为最健全、稳定的用于日常支付和长期持有的货币。它由三个具备不同目标的PoW币组成, 分别简称为HACD ( 钻石 ) , BTC ( 单向转移)和HAC。HACD和BTC可以自动化调节HAC的供应量。他们可以在Hacash上进行点对点转移或去中心化互换。Hacash是由一个未知的人或团队在2018年发明的, 并在2019年由社区开发并上线主网。另外, Hacash的白皮书详细描述了一种实现HAC和BTC大规模支付和实时结算的方式: 通道链网络 ( L2 ) 。

Hacash 网络上的 BTC 由 Bitcoin 主链通过单向转移技术移动过来, 并不是通过跨链桥等方式间接映射的另一种代币, 而是直接、真实的BTC。Hacash 的其中一个重要使命就是通过单向转移技术兼容、继承比特币, 纳入比特币和HACD、HAC一起组成一个系统化、互为补充的健全货币体系。

Hacash追求的唯一目标是为人类实现更健全的加密货币, 而不是为区块链技术寻找更多别的应用场景。货币问题是区块链和加密技术最重大和最迫切需要解决的问题。对货币哪怕是微小的优化都能带来整个社会经济效率的巨大提升。

L3 以 Hacash 健全货币系统 ( L1 和 L2 ) 为基础, 实现了更高层级的可编程、可跨链、可定制的多链协议扩容网络。

# 目录

- 什么是 Hacash L3 ?
  - 扩容
  - 资产
  - 可编程
  - 跨链
  - 隐私
  - 可定制
  - 应用
- Hacash L3的应用场景
  - 支付
  - 稳定币
  - 可编程积分和股票
  - 资产映射及交易
  - 社区通证和NFT发行
  - 金融衍生品
  - DeFi创新探索
- Hacash L3的商业机会
  - 云服务
  - 账本和交易审计
  - 钱包和数据浏览器
  - 去中心化交易所
  - 加密支付
- Hacash L3 的主要缺点
  - 账本安全审计支出增大
  - 可组合性和互操作性降低
- 总结

## 什么是 Hacash L3 ?

Hacash 的白皮书描述了一条用于货币创造、分发和结算的核心主链 ( L1 货币层 ) 和一个用于大规模实时结算的通道链支付网络 ( L2 支付层 ) ，以此两层为基础，本白皮书提出了可编程的第三层扩容多链系统 ( L3 应用层 ) 。从本质上来看，L3 类似于Polkadot 或 Cosmos 的跨链/多链系统，但技术适配和可选择程度更高，且不具备任何代币预分配机制或官方对协议的控制。

以下将从 7 个维度介绍 L3 的功能和特性：

### 扩容

Hacash 的主网负责货币的创造、分发和结算，为了维持高度的去中心化，区块大小和出块间隔时间均受到限制，平均 TPS 在 20 左右。通道链结算网络通过将货币支付场景放入 L2 层来解决大规模的实时支付问题，技术上实现了资金无托管、交易无安全问题，理论上做到了无上限扩容。但通道链存在主网开启通道、收款方保持在线和通道支付限额这三个不方便使用的问题。L3 将从去中心化程度等其他方面进行取舍，在做到无上限扩容的情况下，解决 HAC 和 BTC 支付的便捷性问题，成为小额、可编程的多样化支付平台，进一步提升 Hacash 系统吞吐量的可扩展性。

### 资产

基于控制总账本的规模、排除无效历史数据以保持严格去中心化，Hacash 主网不支持自定义资产发行。真实的经济体离不开各种资产的自由发行和大规模交易，L3 将承担扩充 Hacash 经济系统的资产类别的职能。以通用的、可一键部署的基础协议为支撑，通过多账本、多链的方式为每一种资产的发行、维护和交易提供可靠的技术环境。

### 可编程

为了保持 Hacash 货币核心层极致的安全性、稳定性和高效性，以及考虑到全节点设备的轻量级、嵌入式、移动性等多样化需求，主网不支持图灵完备的智能合约。L3 的多账本、多链系统刚好能将智能合约的安全性问题置于“防火墙”之下，某局部用户业务出现漏洞，不影响 L1 货币层和 L2 支付层的安全运行。既可灵活探索各类可编程货币和金融需求，又可将风险隔离在有限范围之内，且可做到渐进式、不停机修复漏洞。

## 跨链

L3 本质是一个多链系统。每一项资产、每一个组织、每一种技术创新都能单独发一条链来接入 Hacash 丰富多样的经济体系。链与链之间、账本与账本之间将有一套资产跨链、通信跨链和合约调用跨链的基础协议和接口规范。做到多链互通、万链互联。

## 隐私

一方面，我们喜欢区块链的去中心化和公开透明等特点；另一方面，我们也希望自己的财产以及信息隐私可以得到保护。而这两者在一定程度上略显矛盾，由此我们需要一种可选择的隐私支持。L3 将不仅仅用于扩容，服务于隐私等非扩展性需求也可以发挥重要作用。L3 可以支持各种隐私技术，例如混币和零知识证明。

## 可定制

L3 并不是“一条链”，而是一整套可定制的协议标准。用户可在基础的通用协议之上，按照接口规范，选择不同的技术或现有的模块，组合出定制化的解决方案或技术创新。可选择完全不同的编程语言、合约类型、合约虚拟机、共识机制、账本种类等自由定制每一条链，在安全性、去中心化程度、需求独特性等因素之间权衡，来满足特定的需求。

## 应用

如果我们可以为每一项的 Web3 应用都发行一条单独的链并只在相关者之间共享和审查账本，并且可以在底层协议支持的基础上为应用定制更多的高阶技术模块，这会带来极大的技术灵活性和数据可掌控性，功能和安全都将得到平衡。

## Hacash L3 的应用场景

L3 并不预设任何演进方向或应用场景，而是作为一套技术上中立的、底层的多链协议，支撑多种多样的、持续发展变化的业务需求，以达成将 Hacash 健全货币接入真实经济的目标。

### 支付

L3 作为 Hacash 的扩容层，可容纳更大规模、可编程的货币支付需求，例如小微支付、流式支付等，且同时支持 HAC 和 BTC。

### 稳定币

L3 作为 Hacash 的资产层，支持任何种类的资产的发行和管理，其中包括抵押型稳定币（例如 USDT）或算法稳定币。稳定币在 Hacash 体系中可作为法定货币和以法币计价的资产的中间渠道和过渡，帮助传统经济世界渐进式迁移到加密经济体系。

### 可编程积分和股票发行

在日常经济中，主要的经济主体（企业）一般会发行两种类别的资产：1) 积分（面向客户，回馈老客户或提升顾客忠诚度）；2) 股票（面向股东，代表公司所有权和利益分配权）；L3 通过独立账本的形式支持企业发行和管理这两种资产。采用开源的技术方案和通用资产标准协议，可极大的简化、降低资产管理的复杂度和成本，且能实现不同类型资产间的互通互联。

### 资产映射及交易

土地、房产等不动产，艺术品、珠宝以及已经发行的股票、债券等资产，在大型股票、债券和商品、期货交易所之外的资产都可映射注册到 L3 上以独立账本的形式进行确权和交易。

## 社区通证和NFT

加密社区 DAO 组织或社区可低成本发行内部通证，并且可选择性地开放部分信息或者完全保持私密。NFT也可以发行在 L3 上，通过基础协议进行交易，或采用更多定制模块管理资产。

## 金融衍生品

以 HAC、BTC 为货币基础，联合更多发行的资产类别，如稳定币、债券等资产，创造出更多的金融衍生品，如永续期货或期权等，让不同风险偏好的市场参与者都能参与赚取利润或对冲风险。

## DeFi 创新探索

Hacash 认为加密领域的最大应用是健全货币，以及由此货币为基础衍生的开放金融需求。L3 可用于构建这种开放式金融产品的协议、平台、应用程序和工具，生态系统。L3 希望通过分布式开源协议建立一套具有透明度、无门槛和包容性的点对点金融系统，将信任风险最小化，让参与者更轻松、更便捷地获得各类金融支持。

## Hacash L3 的商业机会

一个长期有效的经济体内，既有服务需求方，也有产品供应方。L3 在满足更多用户的开放金融需求的同时，亦产生了许多可以盈利的商业机会。

## 云服务

L3 中每一种代币、每一项需求都可以独立创建一个账本或一条链，而大部分的账本或链的需求和功能都是大致相同的。就像如今的云计算创造的价值一样，L3 的用户虽然可以自己在任意计算机上创建账本或运行全节点，但对商业服务的开发方以及某些非技术背景的普通用户来说，使用云上一键部署的账本或链将极大的减轻它们的操作负担。

## 账本和交易审计

L3 并不是“一条链”，而是一个多链系统。这在某种程度上会带来账本审计的独立化，也就是每链都需要单独做审计，而不像那些在 L1 扩容的链，只需要一个性能满足要求的高级计算设备就能审计所有交易和状态。L3 经济体内将有可能产生独立的、有信誉的第三方链上审计机构，为多数不便于自己审计账本的客户id提供可信赖的一次性审计服务，或者作为一个第三方节点来做持续性区块链审计。

## 钱包和数据浏览器

根所有公链一样，L3 是一个单独的协议和接口标准，需要单独开发来支持 L3 的钱包和区块数据浏览器。简单来说就是，我们需要 L3 版本的 MetaMask 和 Etherscan 服务。

## 去中心化交易所

L3 上可以发行丰富多样的各类资产，这些资产可以通过跨链协议进行链间转移或原子互换，但这些都只是在协议层面的接口支持。对于大多数用户来说，它们无法直接和代码调用接口打交道，而必须有更加便捷的用户操作界面。更早提供这个界面的产品将成为更多用户使用的去中心化交易所，成为资金流动的入口。

## 加密支付

无论对于 HAC、BTC 等加密原生货币还是 USDT 等稳定币来说，支付需求都是十分重大的需求。通过 L2 通道链支付网路或者 L3 层支付都可以进行支付，但对普通用户来说，很难精确这其中的技术差别和注意事项。熟悉这些技术规范的加密支付公司将代替用户处理这些技术细节，提供更加便捷、人性化的支付服务。

## Hacash L3 的主要缺点

L3 是 Hacash 的第三层多链网络，做到了无上限扩容、图灵完备的智能合约、可定制的技术模块以及可控的风险隔离等优点。但它并不是100%完美的，也存在一些技术上的权衡，在安全支出和可组合性两个维度上有所取舍。

## 账本安全审计支出增大

理论上 L3 可以创造无数个账本、无数条区块链，每一条链的安全性只与这条链的利益相关者（持币者）有关，缺乏一个全局的、整体的矿工或验证者群体。这带来了无上限扩容的能力，同时，也导致用户必须审计与自己有关的那些账本。对普通用户来说，这种分散化的验证增加了自己的成本。解决这个问题的关键在于第三方运营的云基础设施能帮助用户“一键同步”账本，减少这种自主验证的复杂性。

## 可组合性、互操作性降低

所有多链系统（包括分片扩容系统）都有可组合性的弱点，L3 也不例外。Hacash 的目标是健全货币，以此为基础的 L3 的目标是开放金融，它的适用场景更多需要与日常经济行为相结合，而不仅仅只是在封闭的链上不断创造相互嵌套的“DeFi乐高”。一套基础跨链协议可以满足 L3 用户的资产转移、原子互换和充提币需求，做到底层相互连接，而上层风险隔离。

## 总结

本白皮书论述了 L3 的定义、应用场景、商业机会和潜在缺点，这一多链架构解决了当今区块链领域面临的许多问题，包括可扩展性、技术定制性、风险隔离性以及无缝更新性，为优质的加密健全货币提供开放的经济生态发展基础。