Qredo

# QREDO 简版白皮书

## 为数字资产所有权和区块链互操作性而生的全新基础设施

QREDO FINANCE LTD 版权所有 2021

# 目录

1. 前言
2. 简介
3. 挑战
4. QREDO是什么？
5. 领导团队
6. 未来发展
7. 去中心化
8. QRDO 代币
9. 产品用例
10. 行业领袖感言

# 网络即金库™

QREDO FINANCE LTD 版权所有 2021

# 前言

要为数字资产托管带来更深的流动性和更高的资本效率，我们需要一种崭新的方法。

这种方法需要去中心化、互操作性，以及开放的网络。

## 由多方计算（MPC）保障安全性的去中心化的托管网络

### 功能特点

跨平台信贷和流动性

跨链原子互换和结算

满足治理与合规需求

机构级的安全和控制

互操作性和开源代码

QREDO FINANCE LTD 版权所有 2021

全球金融的未来，取决于去中心化市场的力量。Qredo 的志向是推进去中心化，并以此为指导原则。我们所服务的，是那些热切希望参与加密资本市场下一轮进化的先驱者和远见者。

Qredo 已在主网上推出了去中心化托管协议的 1.0 版本，提供无任何对手方风险的 Layer-1 数字资产的去中心化原子交换。该协议的 2.0 版本正在开发中。2.0 版在安全性、可扩展性和去信任化方面有重大改进，我们将在本文档中详述。

目前，我们的 1.0 版本主网部署六个验证者节点上，它们分布于各地的 Equinix 数据中心。节点中包括一个多方计算 (multi-party computation, MPC) 集群，确保用户存款钱包和 Layer-1 交易的安全。所有 MPC 节点都部署在防篡改的硬件安全模块（HSM）中。这种架构允许我们在一个无限扩展的低延迟网络上，提供机构级别的安全防护。目前，我们正在引入那些准备好体验一种全新方式来保管、质押和交易自身资产的企业客户。所有网络参与者都通过一个独特的委托持股证明（DPoS）协议获得交易费返利。

随着 2.0 版本协议的推出，Qredo 将开始加入独立的第三方验证者。他们将首先协助测试网络的运作，最终用于主网 2.0 的启动。随着我们走向完全去中心化的模式，社区最终将通过一个去中心化的自治组织（DAO）来实现治理。

QREDO FINANCE LTD 版权所有 2021

# 简介

## 愿景

Qredo 正在为多链世界重构数字资产所有权和区块链间的连接方式，并采用一种全新的方式为区块链经济带来流动性和资本效率。

Qredo 开创了第一个适用于金融机构的治理和合规流程的、去信任化的去中心化托管网络，由多方计算（MPC）保障其安全性，实现了**去中心化的托管、跨链原子互换、跨链信贷设施和流动性接入。**

## 我们的使命

Qredo 工作在网络安全和区块链行业的最前沿。我们使用最新的密码学和分布式账本技术构建了一个强大的全球网络，保障数字资产可以进行安全的托管和交易。

我们的使命是为先驱和具远见者建立一个去中心化的基础设施，从而创造一个为所有人服务的开放网络。

QREDO FINANCE LTD 版权所有 2021

# 挑战

## 碎片化的市场

数字资产经济中，存在着许多本行业特有的结构性问题。这些问题导致了流动性缺失，阻碍了金融市场的正常运转。交易确认时间过长，导致所有的交易和信贷活动都需要高达 100%的锁定资本；交易费用高得令人望而却步；除此以外，行业还受到普遍的黑客攻击和安全漏洞的影响。

尽管大型资本市场玩家不乏参与的热情，但他们往往由于缺乏企业级加密货币基础设施而无法投身其中。这些基础设施包括支持跨资产结算和跨平台流动性的内置审计跟踪、治理及合规机制。

而 Qredo 解决了以上所有问题。

*安全性低下*

**19亿美元**

总值的数字资产
在2020年被盗或被黑

中心化的私钥
管理会产生
交易方风险

*资产超额抵押*

**100%+**

预备资金、贷款和借贷
需的抵押品比例

资本被锁定在不同
的交易场所，造成
资本效率低下

*对DEFI内的资产*
*没有控制权*

**5亿美元**

总值的资产在 2020 年
从 DEFI 协议被盗

DeFi协议中的资金
损失归咎于对私钥
的控制不足及繁琐
的程序

*糟糕的跨链/*
*跨平台互操作性*

**1300美元**

2021 年 因"泡菜溢价"
而出现的比特币价差

流动性被困在协议
和平台之间，参与者
无法进行套利

*延迟结算*

**30分钟**

平均确认时间
（3次确认）

区块链结算速度慢
网络费用高

QREDO FINANCE LTD 版权所有 2021

# QREDO 是什么?

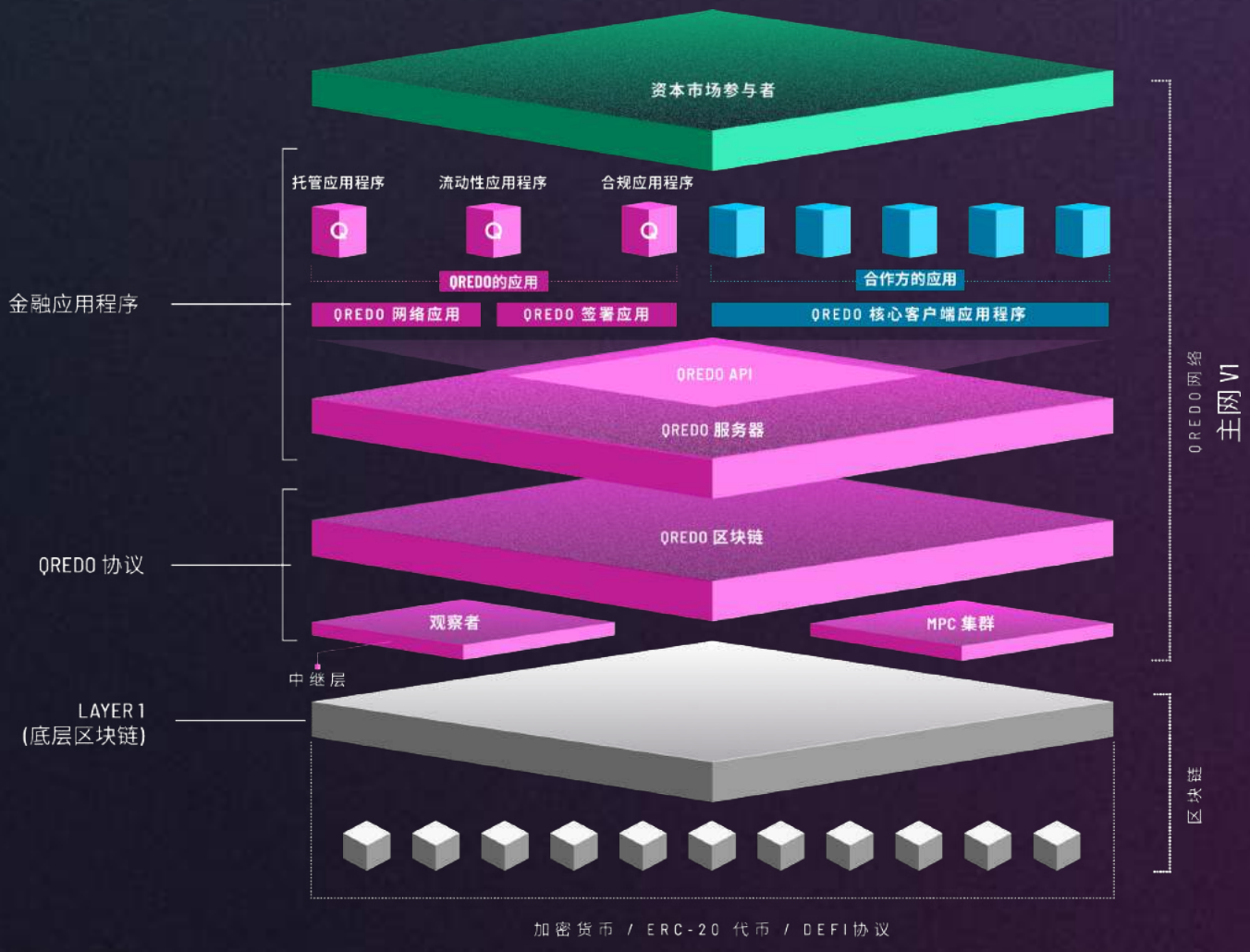
Qredo 是一个在共识机制中内置合规和治理控制的 Layer 2 去中心化托管协议。在 Layer 2 之上，还存在一个 Layer 3 的去中心化的通信层，使对话能够即时被复制到所有端，同时提供内置的端到端加密以保证隐私和安全。对话可以发生在机器与机器间，也可以发生在机器与人，或人与人之间。

Qredo 的理念是，如果能够利用分散的通信协议（Layer 3）作为一个独立的层来为 Layer 2 卸下任何不相干的通信，Layer 2 协议就能充分发挥自身的潜力。如果一个 Layer2 服务希望为那些感兴趣参与或开发 DeFi 协议的传统金融机构提供高性能的解决方案，这是至关重要的。

Qredo 协议利用多方计算（MPC, multi-party computation）来生成相互隔离的存款地址，并消除私钥被盗的风险。多方计算节点签署交易时需要依循一个由共识驱动的、无需中心化私钥存储的安全工作流程。

从共识层到数字资产和经济安全设计，Qredo 协议的设计都是为了在「网络即金库」的前提下为流动性提供者、做市商和交易者的消除所有交易方风险。所有的存款和持股都会 1:1 映射到底层的 Layer 1 区块链上，并可以通过 Qredo 区块浏览器查看。

QREDO FINANCE LTD 版权所有 2021




## QREDO 网络架构

QREDO FINANCE LTD 版权所有 2021

# 核心技术特色

## 最终性快速确认的区块链

Qredo 的 Layer 2 网络能快速确认交易最终性，从而可应对每秒数千笔的交易量。

Qredo 的 Layer 2 可跨越不同的 Layer1 区块链记录流动性网络内的资产所有权。

## 多方计算(MPC)共识网络

由共识驱动的多方计算（MPC）网络消除了数字资产的被盗风险。

Qredo 为机构交易提供内置安全机制、可编程的治理和工作流程。在确保最大安全性的环境下，用户还可访问 DeFi 智能合约。

## 加密的信息传输

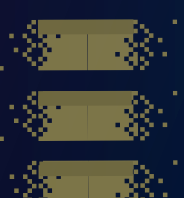
Qredo 的 Layer 3 传输层允许用户在其加密且去中心化的消息网络中广播询价，并使交易前的谈判简单易行。

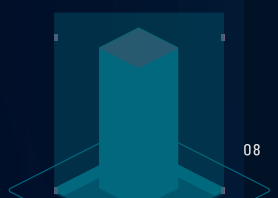
Qredo 的 Layer 3 对所有传输的信息和交易进行加密绑定，从而符合 FATF 的「旅行规则」(Travel Rule) 监管要求。

## 客户端及合作方接口

Qredo 集成运行库与 Qredo 客户端接口（API）相连，使市场参与者能够将 Qredo 集成到他们的中台和前台应用程序中。

合作伙伴还可定制开发集成了 Qredo 网络的应用程序，从我们灵活的架构和对多种用例的支持中受益。





QREDO FINANCE LTD 版权所有 2021

# 关键功能

## 可控的去中心化托管

- 自助管理功能、支持第三方托管
- 企业级授信和分级控制
- 多类型资产资金管理
- DeFi 操作面板

## 去中心化询价系统和信贷设施

- 跨链原生原子交换
- 即时转账
- 自动净结算
- 点对点和点对池的（P2P/P2Pool）交易员加密聊天（trader chat）
- 访问流动性池
- 原生的跨链去中心化交易所（DEX）连接性

## 去中心化合规

- 符合FATF 「旅行规则」反洗钱监管要求
- 自动化、可自定义报告机制
- 交易和沟通记录存档且不可篡改
- 已审计、已认证、已保险

## 已审计、已认证、已保险

已通过安全审计: NCC Group, Quantstamp

正进行安全审计: Trail of Bits & Marsh McLennan

已通过渗透测试: Zokyo

已经同行评审: Dr Michael Scott

已投保: Lloyds of London, Marsh

QREDO FINANCE LTD 版权所有 2021

# 市场定位

## QREDO 与市场竞争者对比

与目前市场上的任何解决方案相比，Qredo 提供了最佳的跨链互操作性和最安全的去中心化托管。

尽管其他项目也在使用多方计算（MPC）技术，但 Qredo 的 多方计算是目前世界上唯一的由共识驱动的多方计算。

## QREDO 的优势

因其独特的实现方式，Qredo 具有三大明显优势：

**1）去中心化的安全保障**
Qredo 协议不会将资产所有权信息存储在中心化数据库中，而存储在去中心化账本中。由共识驱动的多方计算（MPC）网络消除了私钥被盗的风险。

**2）跨链互操作性**
Qredo 通过无摩擦的跨链原子互换，以及跨链信贷设施，支持跨链加密市场的发展。

**3）自动交易和执行安全**
Qredo 有内置的隐私和安全协议，确保 Qredo 网络上的任何对手方都无从知晓你的策略。交易将不受抢先交易、矿工可提取价值（MEV）破坏等恶意活动的影响。

QREDO FINANCE LTD 版权所有 2021

资产跨链
协议

多方计算技术
的托管服务

QREDO FINANCE LTD 版权所有 2021

# 发展历史

## Q4 2018
**QREDO 成立**

Anthony Foy 与 Brian Spector 联合创立 Qredo

## Q1 2019
**前种子轮融资**

Qredo 完成 290 万美元前种子轮融资

## Q4 2019
**首个MVP产品发布**

首个去中心化托管 MVP（最小可用产品）发布

## Q1 2020
**APACHE MILAGRO**

向 Apache Milagro 孵化项目承诺专利

## Q2 2020
**测试网 1.0 发布**

由共识驱动的多方计算网络1.0 版测试网发布

获得种子轮投资，来自
Gumi Crypto Capital , G1 Capital 和 Maven 11

## Q3 2020
**主网 1.0 发布**

主网1.0版本上线，实现 BTC 的去中心化托和即时传输

## Q4 2020
**支持以太坊**

支持即时兑换 BTC 和 ETH

## Q1 2021
**完成 1100万美元种子轮融资**

主要战略投资人包括：Celsisus, Deribit, Wintermute, GSR, CMS Holdings 等知名机构。
开始支持 USDT、USDC 和20种主流 ERC20 代币，支持多用户控制的企业账户操作。

## Q2 2021
**与HEDGEGUARD 推出联合产品**

发布流动性中心和交易员聊天功能 MVP
为前10名的 ERC20 代币提供即时支持

QREDO FINANCE LTD 版权所有 2021

# 领导团队

## ANTHONY FOY

### CEO 首席执行官

科技行业老兵及连续创业者

20年+风险投资支持的成长型公司工作经验

4次成功退出

## BRIAN SPECTOR

### CPTO 首席隐私技术官

网络安全专家和连续创业者

20年+高级密码学专业经验

拥有5项专利

3项在申专利

## JOSH GOODBODY

### COO 首席运营官

15年+从业经验

曾负责世界最大加密货币交易所（币安、火币）全球业务增长

曾任金融市场律师

## DUNCAN PAYNE-SHELLY

### CFO 首席财务官

高成长企业资深高管

20年+金融从业经验，曾任四大会计师事务所 FCA（英格兰及威尔士资深特许会计师）

包括 13年并购业务经验

进入科技/科技金融领域10年

## BEN WHITBY

### REGULATORY AFFAIRS 合规专家

合规技术负责人，曾任

Capital Markets, MiFID, Dodd Frank 专家

2001年曾开发全球首个利率互换交易平台

自2013年以来一直是加密行业的倡导者

QREDO FINANCE LTD 版权所有 2021

# 技术路线图

| | 数字资产 | 平台及功能 |
|---|---|---|
| **已完成**<br>现已上线 | **大市值资产**<br>原生加密货币<br>Bitcoin BTC<br>Ether ETH<br>稳定币<br>Tether USDT<br>USD coin USDC<br>市值前20<br>ERC-20 代币 | **LAYER 2 核心**<br>✓ Layer 2 交易及清算<br>✓ 去中心化托管<br>✓ 企业级加密钱包<br>✓ 跨链互换和流动性中心 |
| **进行中**<br>2021下半年 | **中等市值资产**<br>原生加密货币<br>Algorand ALGO<br>Solana SOL<br>Binance Smart Chain BSC<br>Polkadot DOT<br>市值前 60<br>ERC-20 代币 | **LAYER 3**<br>交易员加密聊天<br>「旅行规则」合规<br>DeFi 中心 |
| **计划中**<br>2022上半年 | **中小市值资产**<br>NATIVE<br>Cardano ADA<br>Stella XLM<br>市值前 100<br>ERC-20 代币 | **市场增值模块**<br>自定义保险<br>加密货币市场 |

QREDO FINANCE LTD 版权所有 2021

## 通往去中心化之路

目前，Qredo 已经部署了 1.0 版本主网，由 Qredo 有限公司担任去中心化架构的唯一运营商。Qredo 的认证节点运行在一个低延迟的网络中，由分布在全球的 6 个数据中心托管。在 2021 年下半年，Qredo 将在 2.0 版本测试网发布时进入联合运行模式。在联运模式下，一组准备好的第三方验证者将开始运行认证节点。2022 年初，联运阶段完结后，如果所有的运营测试和安全评估都表明没有重大风险和缺陷，Qredo 将增加第三方验证者的数量，以实现完全去中心化。

Qredo 协议和代码不属于任何一方。Qredo 网络是一个社区，将以去中心化自治组织（DAO）的最佳运作模式进行治理。Qredo 网络将由一个开放的、分布式的 Qredo 认证节点网络来保障，这些认证节点通过运行多方计算（MPC）协议保护存款、管理参与者的市场活动、验证交易和票选新区块。

Qredo DAO 的运作将独立于任何中心化机构。相反，组织将以“一 QRDO 代币一票” 的形式作出集体决策。一般来说，如果一项改进提案获得了足够多的支持，就会进入投票阶段。投票将通过以太坊上的智能合约进行。DAO 的智能合约定义了组织的规则，并持有该组织的资金。智能合约一旦在以太坊上线，任何人都不能改变其运行规则，除非有新的投票得以通过。Qredo 已经开发了这些智能合约，目前正在进行安全审计。Qredo 将修复已发现的问题，并且在二次审计没有问题的情况下发布这些智能合约。

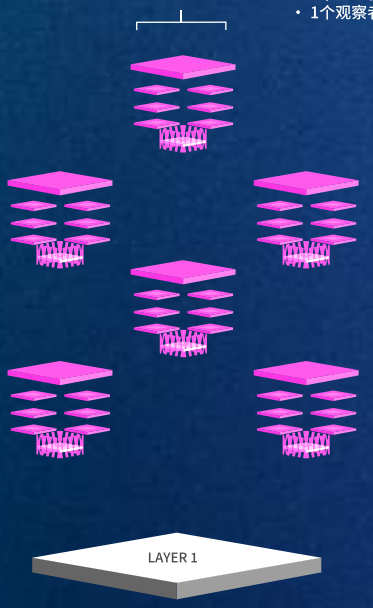
QREDO FINANCE LTD 版权所有 2021

# 现在

## 中心化

QREDO 全球运行
6个数据中心

每个数据中心都有：
- 1个认证节点
- 6个MPC集群
- 1个观察者

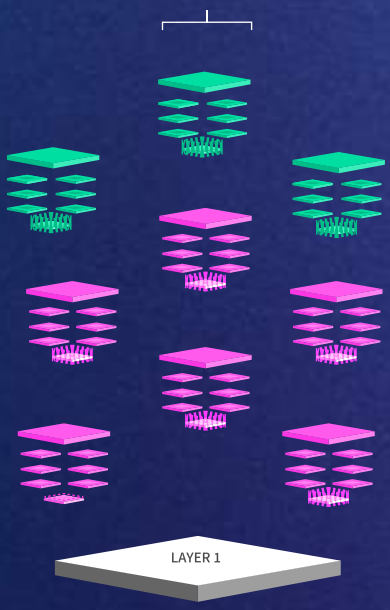



QREDO 认证节点
QREDO 多方计算
QREDO 观察者

# 2011下半年

## 联合运行

合作伙伴验证者




合作方 认证节点
合作方 多方计算
合作方 观察者

# 2022年

## 去中心化

独立验证者

独立的 认证节点
独立的 多方计算
独立的 观察者

QREDO FINANCE LTD 版权所有 2021

# 代币经济学

**QRDO** 是 Qredo 网络的应用和治理代币。我们设计了一个「以用户为中心」的激励结构，从经济上鼓励用户积极参与到 Qredo 网络中来，以建立网络效应和推动大规模采用。因此，该激励措施的设计考虑到了每类参与者，其中包括：验证者、流动性提供者、交易者以及托管用户。

## 以用户为中心的奖励机制

### 交易挖矿

激励用户使用 Qredo 网络交易手续费返还最高可达 100%

### 托管挖矿

在网络内存放资产的用户可获得通胀奖励

### 验证节点奖励

高回报模式，来自于交易和托管费，以 QRDO代币形式支付

### 流动性挖矿

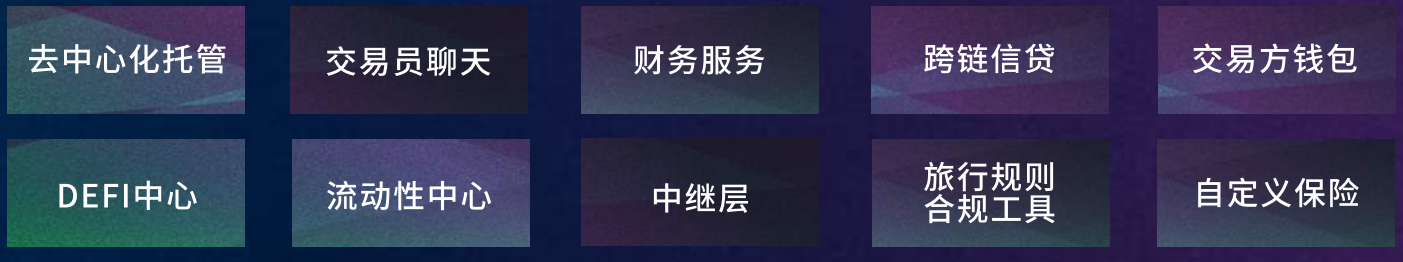
流动性提供者不需支付任何费用，并可获得 L1 和 QRDO 代币作为提供流动性的奖励。

QREDO FINANCE LTD 版权所有 2021

## 产品用例

市场对具备企业级风控体系的去中心化托管服务有着强烈的需求，正是这一需求激发了 Qredo 的设计灵感来创造一个能支持最先进的加密交易应用的网络。

- **去中心化托管**：支持企业级控制以及多用户接入的托管服务，包括自存管和第三方托管。
- **交易员聊天**：一个为OTC交易沟通而设的即时通讯应用，采用点对点加密技术，可用于交易前的谈判、询价和清算。
- **金库管理服务**：例如本地会计软件的平台插件。
- **跨链信贷服务**：使跨链套利或跨链流动性挖矿策略的利润最大化。
- **交易方钱包**：允许交易者汇集自身保管的资金来参与中心化交易所和DeFi上的交易，而无需提前进行资金的汇集工作。
- **DeFi 中心**：提供跨链的DeFi智能合约协议供接入。
- **流动性中心**：扩展了现有的多交易商 P2P 暗池，留存完整并可审计的交易历史记录。
- **中继层**：为经纪人类型用例（例如报价）提供向第三方支付功能。
- **自定义保险**：一款综合型保险产品，提供灵活、可定制的、可以根据业务所需量级扩展的保险方案。
- **「旅行规则」合规工具**：一种利用 Qredo 网络来接受、拒绝交易、验证交易方，同时与第三方合规系统完全互通的合规性工具。




QREDO FINANCE LTD 版权所有 2021

# 行业领袖感言

「我们欣喜地看到 Qredo 为 DeFi 带来更好的速度、安全性和合规性，并为机构提供了参与加密市场的新方式。」

**ALEX MASHINSKY,**
CEO 首席执行官
Celsius Network

「我们期待看到 Qredo 建立丝滑流畅的托管服务……我们从未如此接近专业化的 DeFi、适用于 Web 3.0 的更上层楼的金融服务。」

**JOHN JANSEN,**
CEO 首席执行官
Deribit

「Qredo 为机构提供了一种更有效的方式来管理和交换他们的原生资产，且不论存在何处都可无缝接入 DeFi 协议。」

**JOE DETOMMASO**
投资组合经理
CMS Holdings Network

「我们投资 Qredo 是因为其崭新的基础设施与我们的目标不谋而合，那就是让加密货币交易和投资更容易、更公平、更高效。」

**JACK TAN**
联席CEO和联合创始人
Kronos Research Network

「若机构持有和交易加密资产，Qredo 的去中心化基础设施将迅速成为他们数字资产生态必不可少的一部分。」

**CRISTIAN GILLOMMASO**
联合创始人
GSR

「Qredo 是加密行业进化的一部分；一个适合机构的，能协助数字资产迈向主流及更广泛应用的基础设施。」

**MILES PERRY**
托管业务负责人
Genesis

QREDO FINANCE LTD 版权所有 2021

# 免责声明

本文由 Qredo Finance Ltd（「Qredo」）编写，仅供参考，不应视为购买或出售或认购任何加密代币、证券、金融工具或任何其他权利或产品的要约或邀约。特别是，本文不构成在英属维尔京群岛（「BVI」）或此类要约或邀约为非法的任何司法管辖区出售证券的要约或邀约。

Qredo 没有在英属维尔京群岛或其他地方的任何金融监管机构注册或获得许可。因此，没有英属维尔京群岛或其他金融监管机构通过本介绍的内容或购买 QRDO 代币的优点，也没有向任何英属维尔京群岛或其他金融监管机构备案或审查本文件。QRDO 代币没有在任何金融监管机构注册。本文件并非针对任何司法管辖区的任何人士，而该司法管辖区（因该人士的国籍、居住地或其他原因）禁止发表或提供本文件。对其适用此类禁令的人不得查阅本文件。在不限制上述规定的一般性的前提下，本文件不针对也不应由位于美国、中国或任何其他禁止这样做的司法管辖区（各为 「受限制司法管辖区」）的人员访问。本文件仅供专业和商业投资者使用，并不打算构成招股说明书或其他营销文件。在已实施招股说明书指令的欧洲经济区成员国（各为 「相关成员国」），本文件仅针对招股说明书指令意义上的 「合格投资者」人士。就这些目的而言，「招股说明书指令」 是指 2003/71/EC 号指令（及其修正案，包括在相关成员国实施的 2010/73/EU 号指令），并包括相关成员国的任何相关实施措施。

根据英国《2000 年金融服务和市场法（修订版）》第 21 条，本文件未经授权人批准。因此，本文件仅面向以下合格投资者分发：

(i) 符合英国《2000 年金融服务和市场法》（金融推广）2005 年法令（「法令」）第 19(5)条规定的投资专业人士；或

(ii) 符合法令第 49(2)(a)至(d)条规定的高净值实体，或

(iii) 其他可合法传达的人（所有这些人统称为 「相关人士」）。

不属于相关人员类别的人不应根据本文件采取任何行动，也不应采取行动或依赖本文件。本文件中的信息仅用于讨论，潜在的购买者应仅根据 Qredo 在适当时候公布的进一步信息中的信息购买代币。

QREDO FINANCE LTD 版权所有 2021

Qredo

# 网络即金库™

QREDO FINANCE LTD 版权所有 2021