Libra

笔记本： 区块链
创建时间： 2019/10/29 22:50 **更新时间：** 2019/11/2 15:50
作者： jyyhermance@163.com
URL： https://libra.org/zh-CN/white-paper/?noredirect=zh-Hans-CN#introducing-libra

---

目的：建立一套简单的、无国界的货币和为数十亿人服务的金融基础设施

可靠的数字货币+金融基础设施 -> 让更多人享受到金融服务
（徘徊在传统金融体系之外的人，拒绝开立银行账户的原因：手续费，银行距离过远，办理手续繁琐。对银行不信任？）

I. 建立在安全、可扩展和可靠的区块链基础上

区块链要求：

- 能够扩展到数十亿帐户，这要求区块链具有极高的交易吞吐量和低延迟等特点，并拥有一个高效且高容量的存储系统
- 高度安全可靠，可保障资金和金融数据的安全
- 足够灵活，可支持 Libra 生态系统的管理以及未来金融服务领域的创新

为此采取了：

- 新的编程语言，Move
- LibraBFT共识协议，拜占庭容错
- Merkle树，匿名原则（单一的数据结构，长期记录交易历史和状态？）

以许可型区块链起步，逐步过渡到非许可型区块链
无论是在许可型还是非许可型状态下，Libra 区块链都将向所有人开放：任何消费者、开发者或公司都可以使用 Libra 网络、在这个网络上构建产品以及通过它们的服务实现增值

II. 以赋予其内在价值的资产储备为后盾

Libra 完全由实物资产储备提供支持。对于每个新创建的Libra 加密货币，在Libra储备中都有相对应价值的一篮子银行存款和短期政府债券，以此建立人们对其内在价值的信任。
Libra 储备中的资产将由分布在全球各地且具有投资级信用评价的托管机构持有，以确保资产的安全性和分散性。

III. 它由独立的 Libra 协会管理，该协会的任务是促进此金融生态系统的发展。

Libra协会理事会成员共同对网络和储备的管理制定决策。
只有 Libra 协会能够制造 (mint) 和销毁 (burn) Libra。
只有当授权经销商投入法定资产从协会买入 Libra 币以完全支持新币时，Libra 币才会被制造。
只有当授权经销商向协会卖出 Libra 币以换取抵押资产时，Libra 币才会被销毁。
由于授权经销商始终能够将 Libra 币以等于篮子价值的价格卖给储备，因此 Libra 储备承担着“最后的买家”的角色。

LibraBFT共识协议：

- 恶意节点小于1/3时安全
- validators从客户接收事务，互相分享（mempool protocol）。每轮有一个validator担任领导，打包事务，提出下一个要创建的区块，其他validators查询规则决定是否投票，最后领导者统计票数，形成QuorumCertificate，证明超过2/3的validators投票，最后广播给所有validators

- 3-chain commit rule - 第k轮提交的区块，被确认过3次，在k+2轮以后才算committed
- 基于Hotstuff协议 - modules for safety and liveness
- 改进 - validators签署的是区块的状态而不是交易顺序；pacemaker发出显式超时，提醒进入下一轮；VRF选举每一轮领导
- 聚合签名 aggregate signatures - 保护签名的validator信息
- 长时间掉线的节点，需要借助外部可信的checkpoint，来同步信息