G G F B

白皮书

澳大利亚区块链技术联盟（GGFB）

目录

GGFB 简介

澳大利亚金融业巨头组建区块链联盟 GGFB，是总部位于墨尔本的区块链创业公司，其核心职能是制定银行业区块链技术开发的行业标准，以及探讨实践用例，并建立银行业的区块链组织。

至今，区块链联盟 GGFB 已经成功吸引了 60 多家知名银行及金融机构加入，其中包括花旗银行、丹麦银行、德意志银行、汇丰银行、澳大利亚联邦银行、美国合众银行、加拿大皇家银行、法国巴黎银行、高盛集团等。GGFB 所倡导的区块链技术将很快在国际金融支付和清算领域中进行实际应用，而这一应用最先颠覆的将是当前金融领域中现有的支付系统。

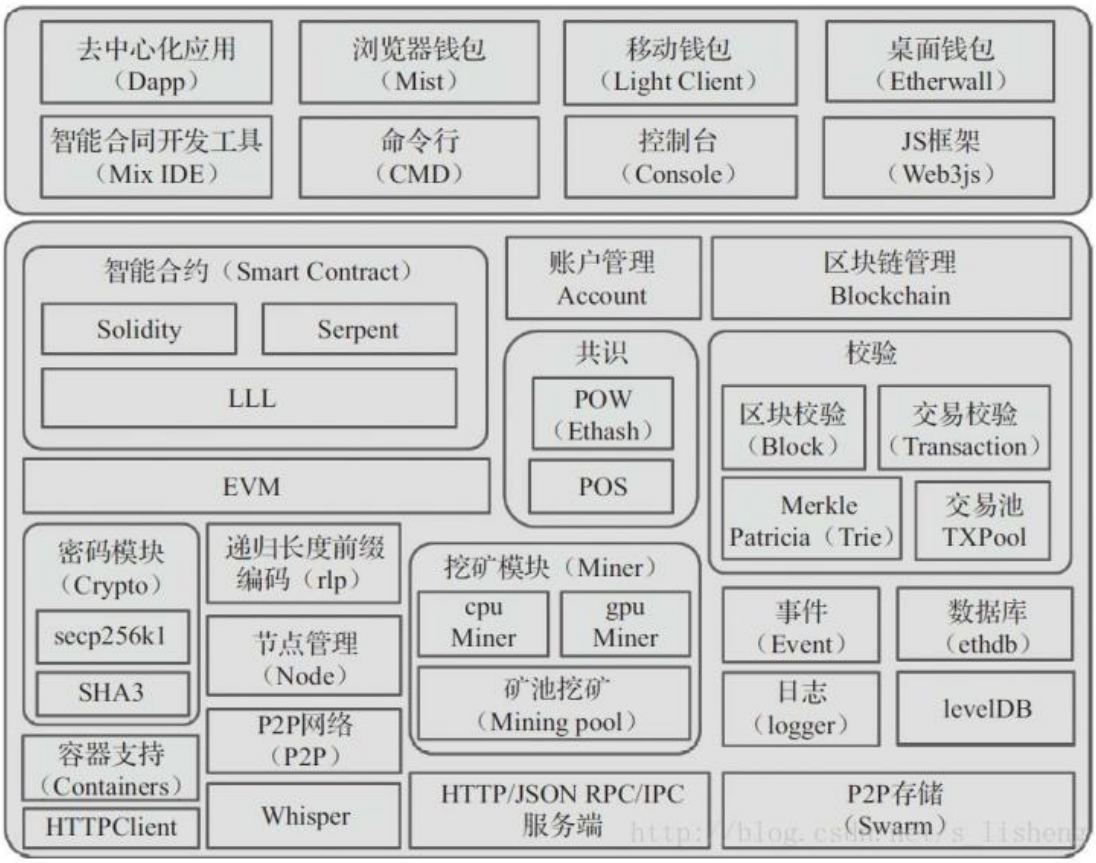
区块链联盟 GGFB，采用区块链 2.0 技术架构 ERC2.0 发行代币 GGFB，总发行量为 300 亿枚。

区块链 2.0 是数字货币与智能合约相结合，对金融领域更广泛的场景和流程进行优化应用，其最大的升级之处在于有了智能合约。

智能合约是上世纪 90 年代由尼克萨博提出的理念，几乎与互联网同龄。由于缺少可信的执行环境，智能合约并没有应用到实际产业中，自比特币诞生后，人们认识到比特币的底层技术区块链天生可以为智能合约提供可信的执行环境。

所谓智能合约，是指以数字化形式定义的一系列承诺，包括合约参与方可以在上面执行这些承诺的协议。智能合约一旦设立制定后，能够无需中介的参与自动执行，并且没有人可以阻止它的运行。可以这样通俗的说，通过智能合约建立起来的合约同时具备两个功能：一是现实产生的合同；另一个是不需要第三方的、去中心化的公正、超强行动力的执行者。

基本架构



专用开发语言

Serpent(类 python)

Solidity(类 JavaScript)

Mutan(类 Go)

LLL(类 Lisp)

技术特点

智能合约（smart contract）：存储在区块链上的程序，由各节点运行，需要运行程序的人支付手续费给结点的矿工或权益人。

叔块（uncle block）：将因为速度较慢而未及时被收入母链的较短区块链并入。使用的是有向无环图的相关技术。

权益证明（proof-of-stake）：相较于工作量证明，可节省大量在挖矿时浪费的电脑资源，并避免特殊应用集成电路造成网络中心化。

闪电网络（lightning network）：可提升交易速度、降低区块链的负担，提高可扩展性。

开发社区稳固，不断成长，勇于使用硬分叉（hard fork）。

GGFB 的独特性

1、目标清晰，致力于全球第三方支付。

2、币值相对稳定，具有较高的安全度。

3、具有稳定的用户群体及广泛的应用场景。

4、实时对接线下实物资产，持续保值增值。

5、具有更高的稳健量化增值可能性。

应用场景

第一类是金融应用，为用户提供更强大的管理和参与合约的方法。GGFB 定位于支付领域的未来发展，致力于为全球用户提供手续便捷、成本低廉的国内及跨境第三方支付，此外包括子货币、金融衍生品、对冲合约、储蓄钱包、遗嘱及一些全面雇佣合约等其他金融应用。

第二类是半金融应用，这里有金钱的存在但也有很大比重的非金钱因素，一个完美的例子是为解决计算问题而设的自我强制悬赏。

第三类是非金融应用，例如在线投票和去中心化治理等。

去中心化存储

在过去的几年里出现了一些大众化的在线文件存储初创公司，最突出的是 Dropbox，它寻求允许用户上传他们的硬盘备份，提供备份存储服务并允许用户访问从而按月向用户收取费用。然而，在这一点上这个文件存储市场有时相对低效；对现存服务的粗略观察表明，特别地在“神秘谷”20～200GB 这一既没有免费空间也没有企业级用户折扣的水平上，主流文件存储成本每月的价格意味着在一个月里支付整个硬盘的成本。以太坊合约允许去中心化存储生态的开发，这样用户通过将他们自己的硬盘或未用的网络空间租出去以获得少量收益，从而降低了文件存储的成本。

这样的设施的基础性构件就是我们所谓的“去中心化 Dropbox 合约”。这个合约工作原理如下。首先，某人将需要上传的数据分成块，对每一块数据加密以保护隐私，并且以此构建一个默克尔树。然后创建一个含以下规则的合约，每 N 个块，合约将从默克尔树中抽取一个随机索引（使用能够被合约代码访问的上一个块的哈希来提供随机性），然后给第一个实体 X 以太以支撑一个带有类似简化验证支付（SPV）的在树中特定索引处的块的所有权证明。当一个用户想重新下载他的文件，他可以使用微支付通道协议恢复文件；从费用上讲最高效的方法是支付者不到最后不发布交易，而是用一个更合算的带有同样随机数的交易在每 32k 字节之后来代替原交易。

这个协议的一个重要特征是，虽然看起来像是一个人信任许多不准备丢失文件的随机节点，但是他可以通过秘密分享把文件分成许多小块，然后通过监视合同得知每个小块都还被某个节点的保存着。如果一个合约依然在付款，那么就提供了某个人依然在保存文件的证据。

去中心化自治组织

通常意义上“去中心化自治组织（DAO, decentralized autonomous organization）”的概念指的是一个拥有一定数量成员或股东的虚拟实体，依靠比如 67%多数来决定花钱以及修改代码。成员会集体决定组织如何分配资金。分配资金的方法可能是悬赏，工资或者更有吸引力的机制比如用内部货币奖励工作。这仅仅使用密码学块链技术就从根本上复制了传统公司或者非营利组织的法律意义以实现强制执行。至此许多围绕 DAO 的讨论都是围绕一个带有接受分红的股东和可交易的股份的“去中心化自治公司（DAC，decentralized autonomous corporation）”的“资本家”模式；作为替代者，一个被描述为“去中心化自治社区（decentralized autonomous community）”的实体将使所有成员都在决策上拥有同等的权利并且在增减成员时要求 67%多数同意。每个人都只能拥有一个成员资格这一规则需要被群体强制实施。

更先进的组织治理机制可能会在将来实现。现在一个去中心化组织（DO）可以从去中心化自治组织（DAO）开始描述。DO 和 DAO 的区别是模糊的，一个大致的分割线是治理是否可以通过一个类似政治的过程或者一个“自动”过程实现，一个不错的直觉测试是“无通用语言”标准：如果两个成员不说同样的语言组织还能正常运行吗？显然，一个简单的传统的持股式公司会失败，而像比特币协议这样的却很可能成功，罗宾·汉森的“futarchy”，一个通过预测市场实现组织化治理的机制是一个真正的说明“自治”式治理可能是什么样子的好例子。注意一个人无需假设所有 DAO 比所有 DO 优越；自治只是一个在一些特定场景下有很大优势的，但在其它地方未必可行的范式，许多半 DAO 可能存在。

代币发行及基于 PoS 的挖矿

GGFB，总发行量为 300 亿枚，计划分 30 年发行完毕，每年发行 10 亿枚。

为保证币值的相对稳定，系统设置每日的币值涨跌幅为≤±10%，用户不能超出该波动范围进行交易，以此保护用户的财产安全。

对于矿工，按其挖出的区块难度值同比例进行奖励，难度越大、奖励越大，以此作为对矿工的激励。

通过各种技术措施，保证 GGFB 产出曲线相对平滑，以避免人为地动摇市场。

利息币

PoS 区块将根据在币利交易中所消耗的币龄产生利息币。设计时设定了每 1 币一年将产生 12 分（即年利息为 12%），以避免将来的通胀，同时也是对用户持有 GGFB 进行奖励。

虽然我们在造币时保留了 PoW，使最初的造币更加方便，但是可以预料到的是在一个纯粹的 PoS 系统里，最初的造币可以种植在创世区块里，形式类似于现实证券市场中的 IPO。

区块签名及双重权益协议

每个区块都必须由其拥有者签名，以避免同一 PoS 受到复制并被攻击者使用。

为了抵御攻击者使用单个 PoS 来产生多个区块进行 DOS 攻击，我们在设计上采用了双重权益协议。每个节点都会收集其接触到的（核心，时间戳）配对的所有利息币交易信息。假如一个已接收到

的区块包含与其它之前收到的区块中的配对信息（核心，时间戳）是重复的，我们会忽略此区块直到后者被孤立(orphaned)出去。

获取 GGFB

用户可通过以下方式获取 GGFB：

1、原始代币发行（ICO）

所有资料写入区块链中，通过公示期，GGFB 开始产生并启动 ICO。用户可通过官方平台、ICO 平台、数字货币交易所以及数字资产交易所参与，并使用比特币、以太币等数字货币购买 GGFB。ICO 结束后，GGFB 将会被释放。

2、数字货币交易所、数字资产交易所及平台

ICO 结束后，通过数字货币交易所、数字资产交易所及平台可继续购买 GGFB。

3、全球超级节点

为进一步的快速扩张与发展，GGFB 的超级节点网络正有计划地进行全球部署，届时任何节点均可购买 GGFB。

4、数字资产混合型 ETF 基金

国际基金经理将会以 GGFB 作为主要资产发行数字资产混合型基金。用户可作为有限合伙人 LP 参与基金投资 GGFB。

5、挖矿奖励及利息奖励。

退出机制

用户可通过以下方式使用 GGFB：

1、持有 GGFB 作为投资。由于 GGFB 的价值已与地产价值及其他资产价值相关联，用户可直接受益于相关资产的升值。

2、购买房产、车辆及其他商品。用户在积累一定数量的 GGFB 后，可以选择数字资产交易所及平台提供的房产、车辆及其他商品，购买退出。

3、交易。用户可在数字货币交易所及平台卖出 GGFB 或者进行其他代币的交易。

4、其他购买交易。GGFB 的生态圈正在生成，未来将有无数的应用场景使用 GGFB 支付各类商家的商品及相关服务。

进一步的应用

1、储蓄钱包。

2、购买保险。

3、一个去中心化的数据发布器。

4、云计算。

5、点对点赌博。

6、预测市场。

7、链上去中心化市场。