



亿书白皮书

亿书团队
v1.4
2016.5.1

（本版作者：Imfly Tailor Cob Mojie）



目录

1. 介绍.....	2
(1) 什么是亿书.....	2
(2) 场景描述.....	2
(3) 核心目标.....	2
(4) 技术选型.....	2
(5) 关键创新.....	3
(6) 亿书组成.....	3
(7) 亿书资源.....	3
2. 共识机制.....	4
(1) 委托人.....	4
(2) 网络费用.....	4
(3) 点对点网络.....	5
3. 客户端.....	5
(1) 全客户端.....	5
(2) 轻客户端.....	5
(3) 移动客户端.....	6
4. 核心功能.....	6
(1) 自定义用户名.....	6
(2) 联系人列表.....	6
(3) 多重签名.....	6
(4) 多功能编辑器.....	7
(5) 去中心化博客.....	7
(6) 自出版平台.....	7
(7) 版权签名与验证.....	8
(8) 去中心化存储.....	8
5. 侧链功能.....	8
(1) 虚拟机.....	8
(2) Dapp 开发.....	9
(3) Dapps 运算.....	9
(4) Dapps 共识算法.....	9
(5) Dapps 主节点.....	9
(6) Dapps 分发.....	9
(7) Dapps 资金存取.....	9
(8) Dapps 代币.....	10
6. 参考信息.....	10



1. 介绍

(1) 什么是亿书

亿书，是一个去中心化的出版平台。由新一代加密货币驱动，安装使用零门槛，是颠覆当前中心化的博客和传统出版机构的创新产品。具备侧链功能，方便第三方开发者无缝集成，开发出各类去中心化的应用（Dapp^[1]），打造立体的生态系统，构建覆盖全人类的智能网络。

亿书，英文名 **Ebook**，底层加密货币中文名“亿书币”，英文名“**Ebookcoin**”，简称：**EBC**。知识是人类进步的阶梯，亿书以让积累知识、分享知识更简单作为终极目标，给人类创作注入新动力。

(2) 场景描述

对普通人而言，亿书与日常使用的办公软件（word，wps 等）相似，是一款简单的文字写作工具，具备安装简单、编辑可视、互动协作等功能，还可直接获得海量书籍。

对于博客爱好者，它可以安装在服务器端，绑定域名，提供公开访问的能力，大大简化博客安装、个性化与维护的难度。

对于专业作者，它的电子书编辑、一键发布、版权保护与交易等自出版功能，具备强大吸引力。

对于企业或社区，它的多节点协作、互动等功能，可方便地用于集体创作、版本控制等，对撰写员工手册、说明文档、研究报告等，可大大提高工作效率。

对于出版社等企业用户和第三方开发者，可以基于亿书强大的网络和市场，使用亿书侧链、智能合约、云存储和计算节点，构建、发布个性化的去中心化软件，货币化一切有形或无形资产，并从中盈利。

(3) 核心目标

亿书的核心目标是让“写作/协作”更简单、让知识有价值，为知识创作和积累注入新动力，进而建立覆盖全人类的 P2P 网络，改善人类使用网络的体验，打造包括电子商务在内的融合社会化、信息化、商业化、物联网的新一代网络。

(4) 技术选型

亿书完全基于 Node.js^[2]平台研发，后台使用 Express.js^[3]框架，前端使用 Ember.js^[4]框架，客户端使用 Electron^[5]框架，数据库使用 SQLite^[6]，前后端统一使用 Javascript 脚本语言，界面使用 HTML5 和 CSS3。



（5）关键创新

技术优势。Nodejs 是一款服务器开发处理平台，其天生的异步处理机制和强大的网络开发能力，非常适合基于事件的、实时交互的加密货币应用，为亿书高性能的即时通讯提供了坚实的技术保障。

社区优势。前后端统一的技术架构，大大降低了亿书及其侧链开发难度，任何熟悉 JavaScript 和 Node.js 的开发者，都可以快速参与进来，促使亿书形成良好的生态系统。我们做过细致调研，在《Nodejs 开发加密货币》^[7]一书里论述了 Nodejs 在开源社区的使用情况，结果是超过 70% 的开源项目都是基于 Nodejs 的。未来，会有大量开发者加入亿书开发行列。

产品优势。亿书目标明确，能让读者、创作者、开发者，基于这个网络，做一切他们想做的事情——写作、设计、开发、交易等。读者可以快速找到最专业、最系统的文章、书籍和服务，创作者可以随时、安全的出售自己的研究成果，开发者可以使用侧链开发电子商务、游戏、物联网等各类商业化软件并从中盈利。

团队优势。亿书面向未来，全面打造专业技术团队。亿书结合开源团队的特点，按照核心团队、贡献者团队、支持社区三个层面，逐步打造出一个实力雄厚、操作规范、运转高效的技术团队。核心团队成员全球控制在 57 人以内，全部来自于贡献者，贡献者产生于支持社区，从而确保每一位开发者都经过长期检验和历练，都被社区高度认可。

管理优势。亿书把贡献作为唯一考量标准，构建了独特的激励机制，并写入区块链，覆盖了团队管理、产品推广和交易计算的每一个环节。对团队管理和产品推广，按照时间和贡献两个纬度设计，坚持先贡献先得且多得、多贡献多得、不贡献不得的原则，给予 EBC 奖励，逐步扩大团队和社区规模。对网络存储、计算和交易等给予固定的 EBC 奖励，促进用户、委托人维护好亿书节点网络，保证网络安全。

对于读者、作者和开发者而言，亿书就是一个知识宝库、巨大市场和一站式解决方案，是一个加密货币驱动的相互促进、互为所用、共享共赢的生态系统。

（6）亿书组成

- ❖ 新一代极具创新精神的加密货币；
- ❖ 新一代强大的高性能对等网络；
- ❖ 面向未来的去中心化的存储和计算；
- ❖ 面向未来的易用易扩展的可编程侧链功能；
- ❖ 简单易用的可视化编辑器；
- ❖ 清晰稳定的 API 接口；
- ❖ 针对主流开源产品的官方插件；
- ❖ 面向第三方开发者的开发工具包 SDK。

（7）亿书资源

- ❖ 亿书官方网站，<http://ebookchain.org>；



- ❖ 《Nodejs 开发加密货币》，详尽的开发文档，<http://bitcoin-on-nodejs.ebookchain.org>;
- ❖ 亿书币核心代码，及其辅助开发包，<https://github.com/Ebookcoin>;
- ❖ 亿书客户端源码，及为第三方提供的各类插件，<https://github.com/Ebookchain>;
- ❖ 区块链俱乐部，亿书社区，团队管理，<http://chainclub.org>

2. 共识机制

亿书基于 DPOS^[8]（授权股权证明机制）共识算法，该算法是由 BTS 团队创造，是被广泛证明更加安全合理的共识机制。

DPOS 是由委托人来创建区块。委托人是被社区选举的可信帐户，得票数排行前 101 位。其它得票排名未进入前 101 名的委托人帐号被列为候选人，当从其它 EBC 持有者那里得到足够多的投票并且排名进入前 101 名后，将成为正式委托人。

所有 EBC 用户均有 101 张选票来推举他们所喜爱的委托人进入前 101，每个用户根据自己持有的 EBC 数量占总量的百分比来投票，得票总数以百分比的方式展示在委托人名单里，比如持有 100 万 EBC 的人投的票，票值就是 1%。

当 101 个区块生成周期完成后，委托人排名前 101 名的代表就会重新调整，排名下降的则被降级到候选人。每个周期的 101 个区块均由 101 个代表随机生成，每个块的时间为 10 秒，新创建的块被广播到网络上，并被添加到区块链里，在得到 6-10 个确认后，交易则被确认，一个完整的 101 个块的周期大概需要 16 分钟。

在 DPOS 里，可以发生分叉，但较长的分叉获胜。委托人必须保持在线，且有足够的在线率。在线率是用来衡量节点稳定性的一个参数，当节点错失区块创建时，就会减少在线率。用户给 101 名委托人投票是基于多因素的，在线率是影响用户是否投票的关键因素，如果委托人的在线率下降到一定程度，用户就有可能取消给他的投票。

（1）委托人

想成为委托人，用户需要注册委托人帐户，可以通过任意版本的客户端进行注册，但只有全客户端才具有创建区块的功能，也就是说用户可以通过轻客户端注册委托人帐户，但只能使用全客户端来开启锻造区块的功能。所有 EBC 帐户都可以注册成为委托人。

新的委托人都是从候选人开始的。候选人从得票率 0 开始，候选人必须到社区拉票，以使自己能挤身前 101 个委托人。前 101 的委托人在候选状态下，是无法创建区块的。注册为委托人要支付一定的网络手续费。

（2）网络费用

所有网络中的有效事务都必须被处理，委托人处理交易并把交易存储在新创建的区块里，为此委托人要收取该区块中所有交易的手续费。所有网络中的交易都必须包含手续费，以防止洪水式垃圾交易攻击。



EBC 默认的发送交易手续费为 0.1%，例如：发送 100 个 EBC，需要包含 0.1 个 EBC 做为手续费，所以实际花费为 100.1 个 EBC。

以下是不同类型的交易所需要的费用：

- ❖ 发送交易手续费 0.1%；
- ❖ 注册成为委托人手续费 100EBC；
- ❖ 注册一个侧链应用手续费 500EBC；
- ❖ 注册一个多重签名，每名会员 10EBC；
- ❖ 用户注册实名认证信息免费，修改或删除手续费 50EBC；
- ❖ 用户出售商品（电子书等），实名认证的用户交易手续费远低于未实名认证的手续费，费率由具体交易决定，不超过 5%；

委托人代表团收取每一轮（101 个块）的所有交易费用，并且平分给该轮里有创建区块的所有委托人，在该轮里没有成功创建区块的委托人则不参与分配。

（3）点对点网络

亿书使用的是一个建立在 HTTP 协议之上的标准的对等网络（点对点网络^[9]），它使用 JSON 进行数据通信，P2P 模块包含了以下节点数据。

- ❖ 版本
- ❖ 系统
- ❖ IP
- ❖ 端口号

3. 客户端

（1）全客户端

全客户端是针对委托人和开发者的最佳解决方案，具有亿书全部功能和 API，可用于 windows，Mac OS 以及 Linux。为了运行委托人节点，需要运行在 Linux 上。全客户端通过点对点网络，从其它全客户端节点下载完整的区块链。

（2）轻客户端

轻客户端适用于普通用户，只通过 HTTP 连接到其它的节点，就像一个个性化的浏览器，轻松管理帐户、撰写和发布文档、管理远端博客、买卖书籍、管理各类第三方开发的去中心化应用等，支持 Windows，Mac OS 和 Linux。

与全客户端相比，轻客户端不下载区块数据，会一直保持较小的体积。它不向网络广播密钥，所有数据在本地签名，可以做所有类型的交易。缺点是无法铸币。



(3) 移动客户端

移动客户端，核心功能与桌面版相同，允许用户通过移动终端来操作自己的帐户。亿书提供苹果与安卓两种版本，可通过苹果应用商店和安卓应用商店下载安装。

它采用响应式设计，适配各类移动终端屏幕。它充分利用移动设备的特殊功能，如：指纹扫描及视网膜扫描验证来增加帐户的安全性，语音输入提高输入体验，GPS 定位查找附近好友等。

4. 核心功能

(1) 自定义用户名

亿书允许用户注册一个用户名，它相当于是用户帐户的一个别名，其它用户可以直接向该用户的用户名付款（类似于人们常用的支付宝帐号），而与该用户名相关联的帐户就会收到对应的交易，用户不再需要记下一长串的加密货币地址。

每个用户名都是唯一的，用户名的长度不得超过 16 个字符，而且，用户名注册后无法更改或删除。

亿书鼓励用户添加真实姓名和国家身份 ID，这非常有利于版权认证和保护。对于不提供真实信息的存储、交易和验证，将会收取相对较高的费用。

(2) 联系人列表

亿书允许用户维护一个联系人列表，该功能可用来存储一些常用帐户，包括合作者、客户、读者或朋友。这是一项社交功能，是亿书协作功能的基础，它类似于社交网站的关注功能。

一个用户被添加到某人的联系人列表，那在该用户的客户端里面，会显示一个待处理的联系人请求，不管该用户是否接受该请求，他都会显示在别人的联系人列表上，而如果该用户接受该请求，那他们双方都会添加对方到自己的联系人列表里。

每一个用户都会优先看到在线联系人的各类公开状态，并可直接访问该用户博客页面，阅读或购买该用户的书籍，向该用户直接发送消息等。用户的动态会推送给联系人列表里的所有人，增强用户互动性。

(3) 多重签名

亿书允许用户创建一个多重签名钱包。一个多重签名钱包就是指一个钱包有多个持有人共同持有并管理。多重签名钱包的交易必须是由数位，或者是全部持有人共同签署的才会有效。多重签名基于 M/N 架构，其中，多重签名钱包的所有者数量 N 最多不超过 16 个，当签署交易时，至少要有 M 个所有者进行签名。M 必须大于 1 且小于等于 N 的数量。



一旦你从多重签名钱包发起一笔交易，所有钱包拥有者都会看到该条待处理的交易，并可决定是否要同意或者拒绝，一旦达到需要的签名数量，那钱包就会允许该交易被提交到网络，并广播全网，打包进下一个区块中。多重签名钱包的所有者可以在获得 M 个所有者同意的情况下，随时更改多重签名的规则。

亿书基于多重签名，实现电子书籍利益分享。用户作为一本书籍的核心创作者，可以创建一个多重签名钱包，将书籍的销售分成比例与合作者的贡献比例对应分配，然后发布出售。这样，每一个购买交易，都会自动按照设定的比例分配给合作者。每笔交易包含一定手续费。

（4）多功能编辑器

亿书提供面向普通用户的可视化编辑器，具有一般编辑器的易用性，后台使用 Markdown 标记语言，可方便的导出导入 Html、Word、PDF 等各类格式。

亿书编辑器具有强大的互动协作功能，可以忠实记录每一处修改细节，自动显示合作伙伴的修改信息，即时显示读者的评论等反馈信息。具备强大的辅助编辑功能，通过简单拖拽，就能把零星记录的灵感组合成文。

亿书编辑器兼具阅读器的功能，可以添加批注、评论，信息直接反馈给版权所有，与作者进行直接互动。

（5）去中心化博客

亿书全客户端集成了一个内容管理系统（CMS^[10]），可以简单的展示用户撰写的博客文章，用户能够方便的改变页面主题，控制文章发布状态。其他用户能够通过用户名直接进行访问，阅读和评论。

用户可以在服务器上安装全客户端，绑定域名，供全世界用户访问浏览。同时，在本地使用轻客户端进行管理，将本地客户端与远程节点同步，从而实现远程控制，大大减少博客维护难度。

（6）自出版平台

亿书可以帮助用户，把自己平时积累写作的文章，方便的处理成电子书。用户可以设置封面、插页等信息，直观地设置出售的价格，与合作者的利润分成比例等。电子书的出售，要支付一定的交易费用，最高不超过 5%。

用户也可以把自己联系人列表里好友的文章，直接拿来聚合成书，亿书会自动记录版权信息，提供详尽的贡献者名单和贡献比例。这对那些开源社区、企业或团队更加方便，协作建立各类专业文档更加简单直接。

用户可以选择一键发布到自己的博客节点主页，也可以选择在线即时交易，更可以发布或出售给第三方平台，即便用户不在线也能在线出售，供其他用户购买使用。



（7）版权签名与验证

亿书自动对发布的文本、电子文档、图片等进行哈希运算，并将运算结果、概要、用户名、作者真实信息、时间戳等写入区块链。如果是多人合作并设置了权益比例，那么每个人的个人信息、贡献比例和权益比例也会一并写入区块链。

亿书可以方便的查看和验证一部作品的版权信息，只要用客户端打开文档，就能直观的检索出来。亿书可以根据用户对版权的要求，做出加密、隐藏、公开、授权等各种版权保护处理。亿书独创多重加密算法，针对文档内容，亿书可以检索区块链记录，罗列全部版权更新情况，实现版权信息追溯验证。

亿书提供各类插件或扩展，为著名的博客、论坛等软件提供支持，把亿书网络之外的文档纳入管理。提供简单易用的 API，鼓励第三方扩展，实现对文件、图片、音频、视频、甚至包含海量数据的文件等进行版权签名和验证，从而为传统出版社等企业用户提供强大技术支撑。

（8）去中心化存储

用户在使用亿书过程中，会产生大量数据，包括各类文本，聚合的各类电子书，及其导出的 PDF 等格式的文档，图片，视频等，还有第三方开发的去中心化的应用数据，这些文件需要安全存储，快速分发。

亿书采用星际文件系统（IPFS^[11]）作为底层存储方案。IPFS 是分布式文件系统的超媒体协议，它可以让用户的数据分布存储于网络的各个节点。当用户浏览其他用户的博客时，或下载安装第三方 Dapp 时，他的节点在下载的同时会向其它节点扩散。这意味着他的博客被越来越多的人浏览，数据会越多的分布于亿书网络。

这样做的好处有很多，数据分布于网络中成千上万的节点上，攻击者想要阻止其他人访问是不可能的。用户不必全天候的运行自己的节点（虽然这么做有助于网络安全），商户在关闭这个亿书客户端的时候，他的博客或书籍在网络中依然可以访问。类似于 BitTorrent，访问和下载的人越多，速度会越快，用户体验越好。

5. 侧链功能

亿书具备强大、易用、可编程的侧链（Sidechains^[12]），可为第三方开发者或出版设等企业用户，提供简单快捷的扩展服务，开发设计出适合企业业务流程的个性化的 Dapps，让亿书这个生态系统更加安全，业务范围更加广泛。主要特点是：

（1）虚拟机

亿书采取沙箱机制，通过虚拟机来运行未经验证的 JavaScript 代码。该虚拟机是一个 Node.js 的分支，通过 API 与亿书主链、比特币区块链进行连接。



Dapp 在虚拟机中运行，使用亿书的算法做为它的共识算法，这种机制能够阻止许多可能的攻击，使用户更加安全的在本机运行 **Dapp**。用户可以在全客户端或者轻客户端上运行 **Dapps**。

（2）Dapp 开发

亿书虚拟机 API 简单易用，开发者可以选择任何 **NPM** 库^[13]，使用所有 **JavaScript** 的异步编程能力，构建基于亿书的任何应用代码。

（3）Dapps 运算

亿书实现了一个可依时间计费的系统，亿书虚拟机可以追踪运行一个 **Dapp** 所使用的 **CPU** 时间，因此，节点所有者可以通过运行 **Dapp** 主节点来赚取 **EBC** 或者 **BTC** 作为收益。

亿书鼓励节点所有者通过提供 **CPU** 计算，内存，存储和其它资源来获取报酬，促进亿书网络覆盖面更广、更强大、更安全。

（4）Dapps 共识算法

Dapp 的所有者可以跟踪自己的 **Dapp** 被使用的情况。**Dapps** 内的交易是由主节点处理的，主节点是由 **Dapps** 所有者运行的，**Dapp** 所有者必须拥有一个亿书帐号，这个帐号类似多重签名的帐号，它的主要任务是在 **Dapp** 主节点创建共识并签名新的区块。

一旦一个新的 **Dapp** 区块被创建，并且在主节点内被签名，这个区块需要被转换成 **SHA256** 哈希。然后 **Dapp** 所有者提交这个哈希值给亿书区块链，亿书则存储该哈希值为 **Dapp** 区块。一旦亿书区块链收到一条包含 **Dapp** 哈希值的交易，就经由委托人对这条哈希值与上一个哈希值，并将它保存。

（5）Dapps 主节点

Dapp 主节点是指安装了该 **Dapp** 并且针对该 **Dapp** 开放了区块创建功能的亿书节点，只有多重签名 **Dapp** 帐户的所有者可以通过使用密钥来运行主节点，主节点是该 **Dapp** 系统的核心，主节点处理交易并且创建新区块，然后由亿书区块链或者比特币的区块链来保证其安全性。

（6）Dapps 分发

Dapps 采用去中心化的存储方案（**IPFS**），存储为一个 **ZIP** 文件包，包括了 **node.js** 安装包，该 **zip** 包的 **json** 文件包含了安装信息，开发者可以使用其 **Dapp** 帐户更新安装包，多重签名的 **Dapp** 帐户会按其多重签名的设定，要求其签名授权对 **Dapps** 的更改。

（7）Dapps 资金存取

开发者可以使用 **EBC** 和 **BTC** 来作为其 **Dapp** 的货币。使用 **Dapp** 时，用户需要存入或者取出资金。当 **EBC** 或者 **BTC** 被发送到 **Dapp** 时，资金会在其 **Dapp** 的帐户内出现，用户便可在 **Dapp** 内使用该资金。**BTC** 与 **EBC** 的存入方式是一样的。



Dapp 的帐户就是 Dapp 的 BTC 或 EBC 地址，由 Dapp 的作者创建，所有存入的 EBC 或者 BTC 都将被存储在这里，考虑到安全性，Dapp 帐户应该是多重签名账户。

从 Dapp 取款是由主节点负责处理的，当有人发送一条取款请求，Dapp 主节点就会处理它并且把资金从 Dapp 的地址上移出到亿书区块链上或者比特币区块链上。

(8) Dapps 代币

开发者可以在自己的 Dapp 里面发行代币，使用代币作为该 Dapp 的流通货币，这些代币在该 Dapp 内可像 EBC 或者 BTC 一样使用。但是，它不能直接从一个 Dapp 转移到另一个 Dapp，必须通过亿书主链来转移。

6. 参考信息

^[1] [Decentralized Applications.]:

<https://github.com/DavidJohnstonCEO/DecentralizedApplications>

^[2] [Node.js 官方网站]: <http://nodejs.org>

^[3] [Express.js 开发框架]: <http://expressjs.com/>

^[4] [Ember.js 开发框架]: <http://emberjs.com/>

^[5] [Electron 官方网站]: <https://github.com/atom/electron>

^[6] [Sqlite 官方网站]: <http://www.sqlite.org/>

^[7] [Nodejs 开发加密货币]: <http://bitcoin-on-nodejs.ebookchain.org>

^[8] [Bitshares DPoS.]: <http://wiki.bitshares.org/index.php/BitShares>

^[9] [Peer-to-Peer Wikipedia Article]: <https://en.wikipedia.org/wiki/Peer-to-peer>

^[10] [CMS]: https://en.wikipedia.org/wiki/Content_management_system

^[11] [IPFS]: <https://ipfs.io/>

^[12] [Sidechains.]: <https://www.blockstream.com/sidechains.pdf>

^[13] [NPM 官网]: <https://www.npmjs.com/>

^[14] [Factom 白皮书 v1.0]:

https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf

^[15] [Crypti 白皮书 v2.1]: <https://crypti.me/crypti.pdf>

^[16] [Bitcoin 白皮书]: <https://bitcoin.org/bitcoin.pdf>