firefly

萤火

去中心化的数字资产跨平台支付系统

2018年4月28日

V0.1

免责声明

本白皮书仅供参考，不能根据本文陈述的内容作为投资决策依据。萤火团队（Firefly）不做任何声明或保证（不论明示的还是隐含的），并且不承担本白皮书所述内容引起的一切责任。萤火团队不接受任何对 XFF 和未来业绩与回报的任何陈述的约束。本白皮书中提出的“路线图与进展计划”可能会视具体情况有所调整，本项目的实际结果和表现有可能与白皮书的内容存在不符。本白皮书的出版、发行或传播并不意味着适用您所在地区的法律、法规或相关规定，特别提醒：本项目涉及的 XFF 的兑换对象不面向中国、南非和美国公民。有关参与数字资产初次公开兑换的相关条款和条件，请详细阅读数字资产发行章节与法律文件。

本文仅作为传达信息之用，既不组成也不理解为提供任何买卖行为或邀请买卖任何形式证券的行为，更不是任何形式上的合约或者承诺。除非你本人了解本项目及发展情况，否则不建议您兑换本项目的数字资产。相关意向用户需明确了解相关 的风险，投资者一旦参与投资即表明承诺了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。团队既不承诺也不承担任何因参与本项目造成的直接或间接的资产损失，投资者无权对本项目团队的任何成员追究任何法律责任。

概要

随着区块链的爆发式增长，出现了越来越多的虚拟资产，现如今已达数千种。在可预期的现在与未来，个人、组织甚至以及机器拥有数种甚至数百种链上资产会成为普遍模态。但由于链与链之间的跨平台合作性能差，不同数字货币之间的自由兑换出现了严重的发展瓶颈。

基于此，我们开发了萤火平台。萤火（Firefly）是基于恒星网络协议构建的一个去中心化认证与授权框架及基于支付场景的开放第三方应用平台。

萤火采用社区化方式运营，构建区块链跨链生态，创建开发者社区与用户社区。萤火会不断的加大推广力度，吸引优质的社区成员共建开放、公平、健康的社区，打造用户与链之间的有效协作与沟通。

XFF 作为萤火社区的权益证明，是萤火生态的重要沟通桥梁及价值体现，包括社区交流平台所使用的积分、打赏、管理激励等均由 XFF 实现；为促进社区发展，以 XFF 分发形式，鼓励轻应用的开发，社区内权益的流转也将通过 XFF 予以体现；作为社区权益的体现，社区成长带来的增值均分配到 XFF 持有者手中；同时萤火作为链上资产入口，糖果分发也体现在 XFF 持有者手中。

目录

链上资产

随着区块链的爆发式增长，出现了越来越多的虚拟资产，现如今已达数千种涵盖金融、供应链、清算结算、房屋租赁、法律等各个行业。同时，也有许多传统行业机构与人员正在酝酿或者布局，力图将更多的传统资产在特定的区块链上发行，即所谓的“资产上链”。

在可预期的现在与未来，个人、组织甚至以及机器拥有数种甚至数百种链上资产会成为普遍模态，但现行的链上资产管理方式，一般针对某种特定资产，如脑钱包，纸钱包等，同时，资产管理的方式也需要革新与迭代，这为新世代的资产管理带来新的需求与挑战。

同时，现行区块链世界，链条数量众多，特性迥异，链与链之间的交互性差。如果个人拥有多种链上资产，其资产所有权的转移（transfer）容易实现，但币与币之间的交换（exchange）则严重依赖数字资产的交易所。支付（payment）的实现则各自为战，在让普通民众/商家尝试接受时遇到挑战，难以实现大规模、高频次的数字资产转移与交换，这就引发了如 Stripe 作为传统金融变革者也停止了比特币支付的尝试。

去中心化认证

账户是用户在数字世界的通行证，是用户的身份标识。传统的用户身份存储于中心化的网站服务器中，用户的身份信息保存、修改、验证，均依赖于中心化服务器的安全和可信，而中心化的服务面临着服务器被攻击的风险，用户的信息随时可能被泄露、篡改，

同时，用户的身份依赖于中心化服务商的存在，由于政治、经济、竞争、利益驱动等原因，中心化服务商存在着各种风险；同时由于安全及成本原因，中小服务商无力设计或采购较高防护等级的认证体系，而采用委托方式进行。

不同于中心化账户系统将用户的身份信息和验证过程完全依赖于中心服务器，在去中心化的身份验证体系中，用户的身份信息和凭证不属于任何机构所有，真正完全掌握在用户自己手中，账户完全归用户所有。用户自由创建一个或多个包含身份信息的账户，而信息的查验需要用户明确授权。信息的更新与删除都可由使用私钥进行管理。否则，第三方无法访问和修改或删除数据。而基于区块链建立去中心化鉴权系统，也有很多机构在尝试。比如微软发起的 ID2020 项目。基于有账户系统设计的公有链，来创建去中心化的鉴权系统也似乎水到渠成。将用户的身份 ID，与公链地址予以一一映射，作为用户身份和资产归属的唯一标示，实现基于公链地址的去中心化账户系统。验证过程在区块链网络进行，通过数字签名，实现用户的身份获得，身份验证和资产所有权的拥有及转移功能。

传统的身份认证是将用户信息存放在一个独立的系统中，可能是目录服务器，数据库，本地文件系统或自定义的系统。认证时，用户提供用户名和密码，与用户信息系统进行核对，确认用户是否合法。而区块链系统将无需这些繁琐验证，即可证明身份。

开发者与区块链的对接

传统开发者在面对区块链系统时仍有较高的认知成本与学习成本存在。部分开发者认为区块链仅仅是现有技术的整合，在使用时作为强一致性数据库来使用，并没有意识到区块链应该是在思维和理念上的改变继而导致业务模式的改变。

“机器经济”的到来不可避免。在不久的未来，机器支付将会得到长足发展，区块链技术的出现给了机器支付必要的支撑。机器支付可能的形态是小额，快速支付，以及较小的计算能力需求。目前区块链应用限制该类支付的主要痛点则为拓展性以及交易费用。开发者需要改变方式，转而编写适用于机器支付的业务系统。

而目前流行的 DAPP 方式，将运行逻辑提交固化到与区块链紧密集合的虚拟机中，每个节点（某些系统为部分节点）都需运行该逻辑。同时逻辑代码不可更改，即使开发者拥有较高的开发水平，仍不能保证运行安全。某些“智能合约”逻辑在运行时出现较大事故，间接导致世界级项目的分裂以及理念上的争论，影响至今。这也导致某些代码范式的产生，以降低编写“智能合约”的难度。

而在部分商业场景中，逻辑无需提交上链，亦或有随时更新改进的需求，开发者需要随时根据需求进行调整。开发者只需要将逻辑运行结果上链。

为什么萤火选择恒星协议

恒星网络是恒星发展基金会（Stellar Development Foundation）于 2014 年发起的一个项目。恒星网络协议具有以下特点：

业界内较快的支付速度。

采用联邦拜占庭理论形成的 SCP 算法，可以（较为）快速地在『平均 3-5 秒』时间内完成共识过程。业务处理速度与现有中心化电子支付工具如支付宝相比处于同一量级。

安全稳定的账户体系

恒星采用 ED25519 算法作为签名算法，兼顾安全及效率。并且计划支持更多算法。

网络协议为小额支付设计，基础费用低廉。

目前每个操作仅需花费 0.00001 个 xlm，10 万次操作花费约合 0.3 美元。

可扩展性强。

官方宣传在 10 亿账户级别下可达到 1000TPS 的能力。同时认为还仍存在优化空间。现在闪电网络正在研发中，可进一步提升处理能力。

具备简单的智能合约功能。可以根据多重签名，时间，序列以及批量执行等能力来编写可自动执行的协定。

为资产上链管理优化，相对于其它平台安全，且费用低廉。

实现了原子交换（Atomic Swap）协议。这为跨链交易打下基础。

精简的协议簇

恒星发展基金会维持了一个精简的协议簇，专注于网络的开发与推广，更多的使用场景等工作，则交给合作伙伴来完成。在其官方愿景中有所表述。

萤火生态

萤火（Firefly）是基于恒星网络协议构建的一个去中心化认证与授权框架及基于支付场景的开放第三方应用平台。萤火的设计理念为社区化开发与运营，最大程度上调动社区参与者的力量，通过服务萤火社区用户以及恒星社区用户，吸引开发者，达到普及区块链技术，让区块链为用户更好服务的目的。

萤火致力于建立可支撑高频次、多平台交易的生态体系。萤火将构建体系的基础设施与底层协议标准，开发者将可即刻开始发挥自己的创造力，开发不同行业不同业务场景的应用。

通用支付标准

目前典型的支付场景中，传统开发者开发的应用，可以由用户自由选择支付手段并调用相应的支付 App 进行支付，并在支付完成后进行跳转与支付结果确认。

萤火会撰写相关支付标准，并开发相关接口，允许应用开发者调用，在主流移动平台（android，iOS）上开放，使得用户可以利用链上资产进行支付。

由于恒星网络协议的特性，开发者可以指定接收的资产类型如欧元资产，而用户可以支付其所拥有的资产如比特币（即所谓的路径支付 Path Payment），这为跨资产，跨地域支付的应用带来极大的便利。

去中心化认证与授权

区块链技术具备透明性，去中心化、不可篡改、共同记账等特点。恒星网络是区块链技术的最佳应用之一。其建立的账户体系可以由萤火进一步扩展，用以实现去中心化的认证与授权系统。

每个账户及其拥有的资产通证都可以用于确定其身份并允许使用私钥方式进行验证与登录。基于恒星网络，萤火将可以提供简单的 API，允许应用获取账户信息作为用户身份，在必要时使用私钥签名以登录应用，以使用应用的一些服务及保存数据。用户可主动决定是否提供账户信息以及使用该应用。由于区块链技术的透明性，在用户明确授权后，应用可以自然而然的获取账户信息，并根据账号信息，来确定用户权益。

用户亦可透过萤火管理已登录过的应用，并对不再使用的应用撤销权限。一切结果均可保存在区块链中，从而实现去中心化的认证与授权管理。

基于此，可以拓展更多服务场景。比如将一些身份信息（非账户信息）保存在第三方应用中，如有其它应用需要调用身份信息时，该应用可查看用户的授权信息，并根据列表信息予以授权，亦或拒绝。

轻应用

目前基于区块链的 DAPP 发展迅速，但如前文所述，DAPP 开发仍具备较高的门槛；同时期微信小程序，支付宝小程序等发展势头迅猛，对开发者相对友好，且其随用随开用完即走的概念也是得到很多人的青睐。工具型，娱乐型轻应用占据大部分使用场景。如同大部分开发者并不会创建自己的开发框架一样，开发者也不会选择创建全新的区块链

以进行开发。萤火选择采用轻应用的模式，合理利用现有技术，降低开发者进入区块链开发领域的复杂度。

萤火会创建与维护 SDK，用于应用通过框架，获取一系列与设备与用户深度交互的能力。最典型的 API 即是支付 API。

使用提供的 SDK，开发者可以简单变身区块链开发者，构建多种形态的轻应用。萤火鼓励开发者在萤火框架内构建轻应用，并会制定奖励措施，以繁荣生态。

开发者中心

为降低开发者进入区块链开发的难度，萤火需要创建一个开发者中心，一方面供开发者进行 SDK 以及其它区块链开发相关知识的学习，一方面供开发者之间进行交流。

运营良好的开发者中心可为生态繁荣创建基础。开发者中心的运营工作也会是萤火社区活动内容的重点。

轻应用市场

萤火将会为所有基于萤火 SDK 开发的轻应用提供一个场所。基于区块链技术构建的分布式应用（即轻应用），以及链上资产的概念普及到更多用户人群需要互相促进。萤火需要帮助用户发现更多有价值的应用，也要帮助应用抵达更多用户。因此我们将建立简单高效的轻应用市场，为用户和开发者提供应用交流，感受反馈等功能。

社交与聊天

社交是人类天性。基于区块链的去中心化网络，建立可信的社交网络也是水到渠成。在以往的社交网络中，社交网络提供者拥有网络的控制权限。而基于区块链的公私钥设计，端对端加密通讯也具备极好的基础条件。萤火计划在后期增添社交功能以及加密通讯的底层支持。

基于社交和支付，可以衍生出很多场景，比如典型的知识付费，在萤火提供底层 SDK 支持后，会诞生伟大的应用。

跨链资产管理

链上资产的管理也是萤火将重点发展的内容。随着区块链的发展，个人甚至机器拥有链上资产将逐渐普及。但是众多链上资产的管理和支付亦会是个难题。

随着原子交换技术的成熟，结合恒星网络的快速支付功能，萤火会开发跨链资产管理功能，兼顾安全和快速支付功能。

数字资产 XFF

XFF 用途

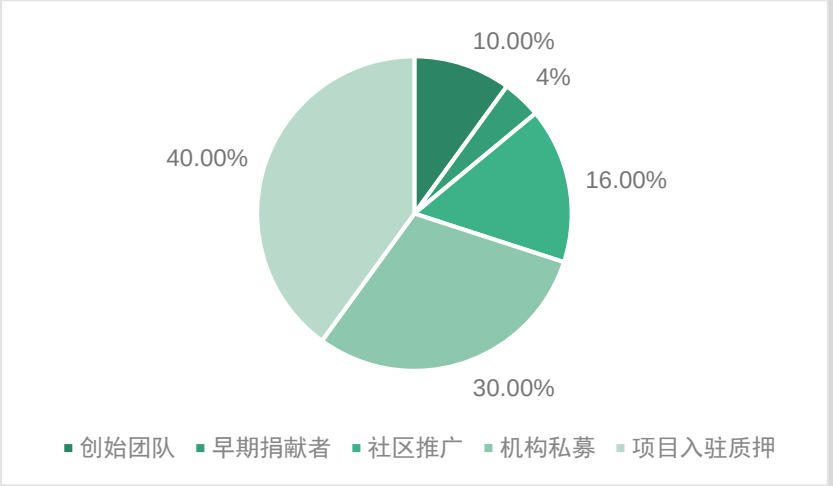
萤火将使用 XFF 作为社区权益证明，在社区内部流通。XFF 在社区中扮演重要角色，拥有广阔的使用场景。

XFF 的设计使用场景如下：

- 社区交流平台所使用的积分、打赏、管理激励等均由 XFF 实现。
- 为促进社区发展，以 XFF 分发形式，鼓励轻应用的开发
- 社区内权益的流转也将通过 XFF 予以体现。
- 作为社区权益的体现，社区成长带来的增值均分配到 XFF 持有者手中。
- 萤火作为链上资产入口，糖果分发也体现在 XFF 持有者手中。
- XFF 代表萤火重大事件的投票权。每个 XFF 权重为 1 票。包括但不限于上下币等。

分配方案

XFF 总量为 2.1 亿。分配方案如下：



10%　创始团队

4%　前期捐赠者。

16%　用于社区推广及早期轻应用开发者奖励

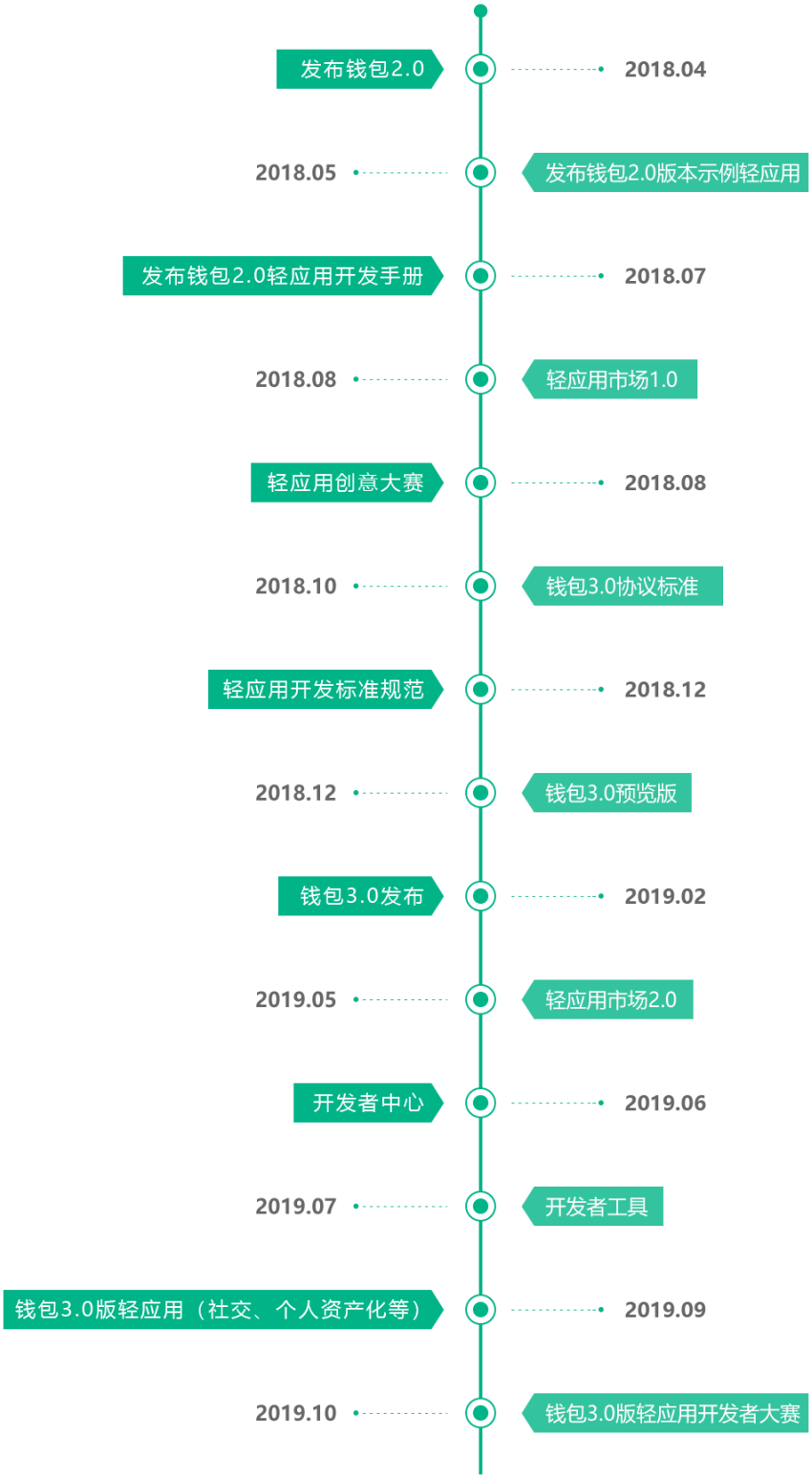
30%　机构私募

40%　项目池（待定、不流通、不参与社区增值分配）

资金用途

募集资金主要用于萤火社区的搭建和系统的运行，这些费用将会为萤火的发展提供有力的支持。同时，部分用于开发团队与社区运营，市场营销以及相关法律财务等部分，。萤火定位为全球化发展的产品，可以帮助萤火更加平稳更加迅速的发展。

项目路线图


发布钱包2.0
2018.04
2018.05
发布钱包2.0版本示例轻应用
发布钱包2.0轻应用开发手册
2018.07
2018.08
轻应用市场1.0
轻应用创意大赛
2018.08
2018.10
钱包3.0协议标准
轻应用开发标准规范
2018.12
2018.12
钱包3.0预览版
钱包3.0发布
2019.02
2019.05
轻应用市场2.0
开发者中心
2019.06
2019.07
开发者工具
钱包3.0版轻应用（社交、个人资产化等）
2019.09
2019.10
钱包3.0版轻应用开发者大赛