Opes Protocol

Enabling Decentralized Digital Assets Management and Investment

去中心化数字资产管理的驱动者

White Paper Draft Version 0.9.7

OPX Foundation

这是一个数字资产管理的开源协议，驱动去中心化的资产管理生态，为上层应用开发者和参与者进入分布式生态所需遵守的一组约定或标准。实现在以太坊区块链上的数字资产管理协议和工具集，为数字资产提供当下最需要的基础金融服务。为个人投资者提供高效、透明、安全的数字资产投资服务，为金融企业降低区块链技术与数字资管应用门槛，打造可信的数字金融资管底层操作基础，使其成为一个更加透明、稳定和高效的市场，最终形成全球化的数字资产可信任金融生态。

目录

I .摘要

2008 年，金融危机席卷全球，导致金融市场的透明度和信任度降至冰点。因此，华尔街或者欧洲乃至亚洲金融服务行业的监管和监督力度得到了增强,但是并未改变资金资产供应链的上下逻辑和透明度。[1] 一切的一切都在循环。因此，参与者越来越希望分布式账本技术发展成为一种开放、安全、可扩展且透明的方法，从而可以满怀信任且自信地进行交易。

区块链的根本是通过分布式账本技术，带来去中心化交易中信任建立的可行性。 对于几乎所有供应链结构的行业来说，无论是药品物流、医疗记录、食品加工、稀有矿物甚至大额固定资产（例如房产），其能稳定运行并逐步扩大影响力的关键是在于参与者的可审核性和去中心化的透明性、可靠性。以此为出发点，我们可以将金融产品看作一级投资市场和二级投资市场的供应链，一方面为现金流转供应链，另一方面为股票、金融衍生品的资产供应链。区块链的终极目标就是通过透明的方式兑现这个承诺。似乎，监管机构的梦想就要实现了。[1]区块链技术可以构建一个高效可靠的价值传输系统，在互联网思维基础上结合区块链新的数据组织结构，推动互联网成为构建社会信任的网络基础设施 Baas（区块链即服务 Blockchain as a services），实现价值的有效传递，并将此称为价值互联网。[3]我们注意到，区块链提供了一种新型的社会信任机制，为数字经济的发展奠定了新基石，“Blockchain Plus”应用创新，昭示着产业创新和公共服务的新方向。

区块链的诞生，标志着人类开始构建可真正信任的价值互联网!

在传统金融的资产管理行业，不论是银行家还是基金管理人，都被老百姓看为金融剥削者，而互联网升级了整个投资理财的交易方式，但只是通过互联网技术解决了在线交易的问题，赚钱的成了平台，腾讯、蚂蚁金服、京东金融、百度金融等巨头都是千亿估值，有的公司甚至年毛利达几百亿，估值上万亿。互联网反而通过流量的集中成就了更大的金融平台。

互联网已经偏离了他原来的样子，而互联网金融也不在是那个的“P2P 乌托邦”的模样。

那么 Opes Protocol 想做的就是先去中介化，让数字货币投资理财真正做到点对点交易，让投资用户清楚的知道自己投资的项目、基金组合潜在风险、实际回报率、服务商的收费标准、抽佣比例，让投资者的利益最大化。

区块链最早的应用场景就是比特币（BTC），以太坊的智能合约时代给了各个领域金融自治权的机会，如果说区块链是一个颠覆中心化互联网的机会，或者说是互联网价值 2.0 时代，那么最应该被颠覆的就是数字资产投资领域；如果连最基础的投资还是中心化，多层级中介，多层级监管的形态，从行业的最源头都没有颠

覆或者说升级，又如何去颠覆其他行业的生产关系呢？ “区块链+Token” 最大的魅力就是自带金融属性和分布式。

Opes Protocol 要做的就是在区块链+金融这个行业率先做到“去巨头”化，让信息更透明，让生态自治，在互联网金融的基础上做进一步升级改造，让过去优秀的“金融民工”做到有一个平台直接对话服务投资者，让投资者真实的跟踪自己投资资产的实时状况。

Opes Protocol 希望更多的数字货币投资者一起来构建一个自治的区块链金融生态。

II .Opes Protocol 介绍

OPES Protocol（OPES 协议）取自拉丁文的财富一词。用区块链技术为数字资产投资行业赋能，以 Token 经济助力上下游资源高效自由流通，打造高效透明的去中心化数字资产投资生态。OPES 协议的区块链项目由 OPES 基金会管理（Blockchain OPES Foundation），

2.1. 相关市场

截至 2017 年底，加密数字货币的总市值从 2017 年初的 177 亿美元增长到 7000 亿美元。与成熟的金融资产相比，加密数字货币这样一个新兴金融资产的发展还处于早期。目前全球股市价值约 73 万亿美元，债券市场价值 215 万亿美元，衍生品价值总量为 544 万亿美元。按此估算全球虚拟货币市场总量（2017 年 12 月数字统计约 7000 亿美元）还不到全球金融市场总量的 0.5%，加密数字货币及相关服务市场拥有巨大的发展空间。

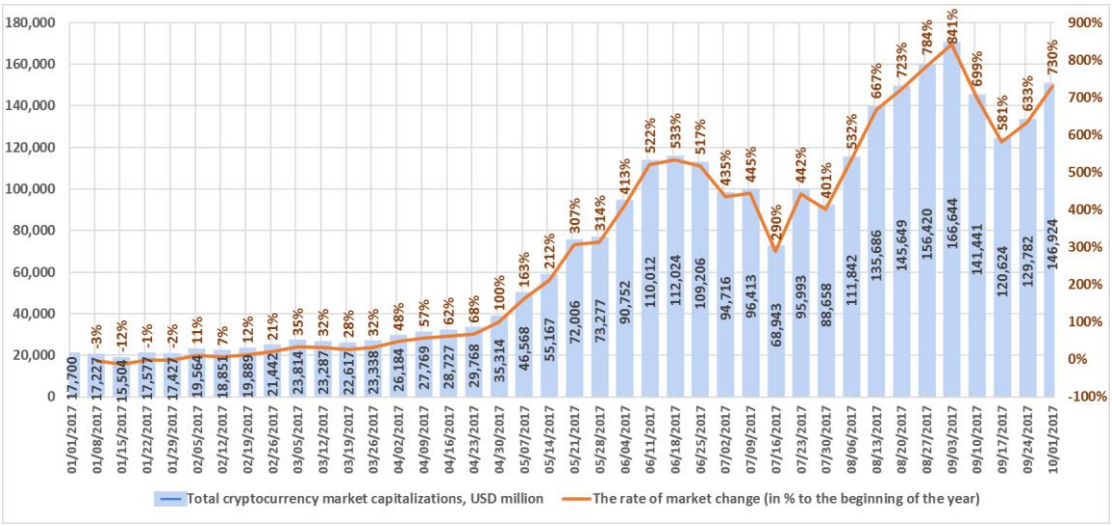


Figure 1 虚拟货币市场总量增长曲线 注：2017/1~2017/10

加密数字货币投资及金融理财市场刚刚兴起，整个行业发展还处于萌芽阶段。目前整个加密数字货币投资市场主要以散户投资者为主，未来将会逐步呈现出一级市场以投资机构为主，二级市场投资散户及部分专业团队的现状。

目前全球数字货币市值高达 4000 多亿美元，随着全球加密数字货币投资市场的发展，越来越多的机构个人开始配置加密数字货币资产投资，越来越多的各类衍生品及量化工具不断涌现。 目前传统金融市场的投资

机会逐渐减少，传统金融的投资收益逐渐在下降。优秀的传统金融年收益大约在 10%，而加密数字货币资产的月获利甚至周获利都很容易超过 10%。加密数字货币投资的高回报收益正在吸引更多的专业投资者、基金量化团队等参与其中。

事实上，几乎所有的大型金融服务公司都在探索并且积极参与加密数字货币及虚拟资产的研究。同时，全球超过 40 个国家建立了 320+的虚拟货币交易所来承接全球的虚拟货币投资者。与此同时日本，加拿大等国家都在探索国家级的区块链和虚拟货币战略为加密数字货币的合规化提供支持及政策规范。未来数字货币资产将是我们重要的新型资产，更好的研究数字货币资产的价值，更好的建立数字货币资产管理及投资生态，与各行各业共同拥抱迅速崛起的数字货币资产经济。

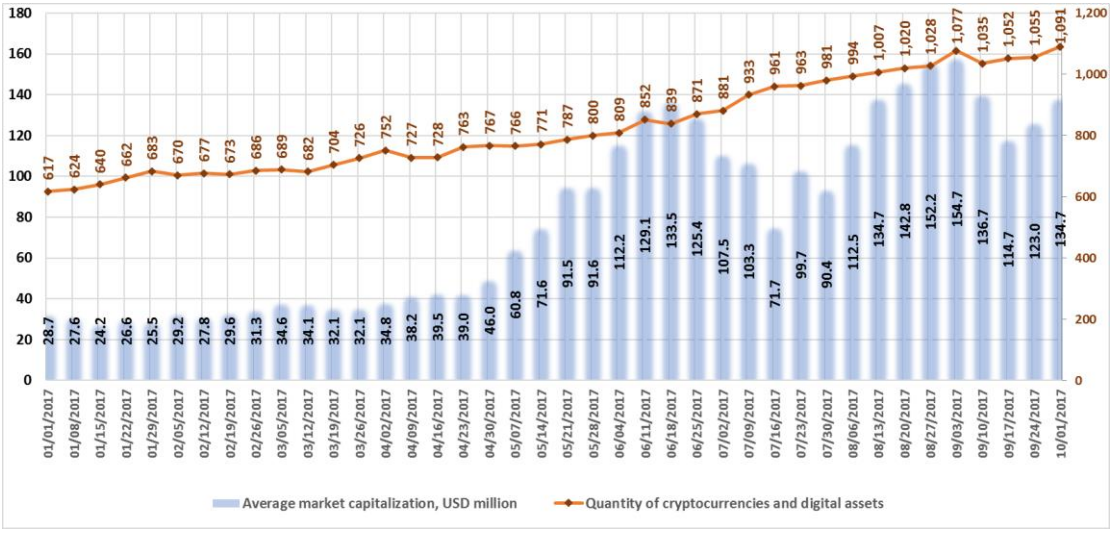
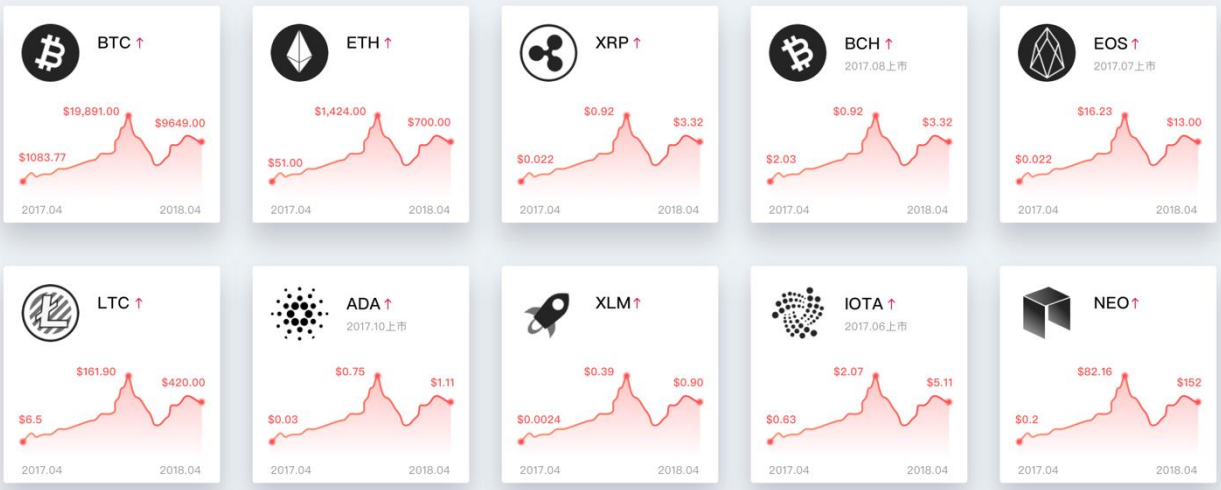


Figure 2 虚拟货币数量及资产量[5]

2.2. 行业百态和挑战

加密数字货币在早期发展阶段行业爆发的红利为众多个人投资人带来百倍甚至千倍的回报收益。目前数字货币市场目前大约有 1000 多种代币，包括比特币（Bitcoin）、以太坊（Ethereum）、瑞波币（Ripple）、莱特币（Litecoin）等主流货币。以太币从 2016 年年底 8 美元一枚单价，一度上涨到 2018 年 1 月份最高 1400 美元，目前也维持在 700 美元左右，涨幅将近百倍；莱特币 2017 年 1 月 1 日莱特币单价只有 4.51 美元，2017 年 12 月莱特币单价一度飙升到 340 美元，暴涨了八十倍。

一年内前十名主流币种价格增长情况



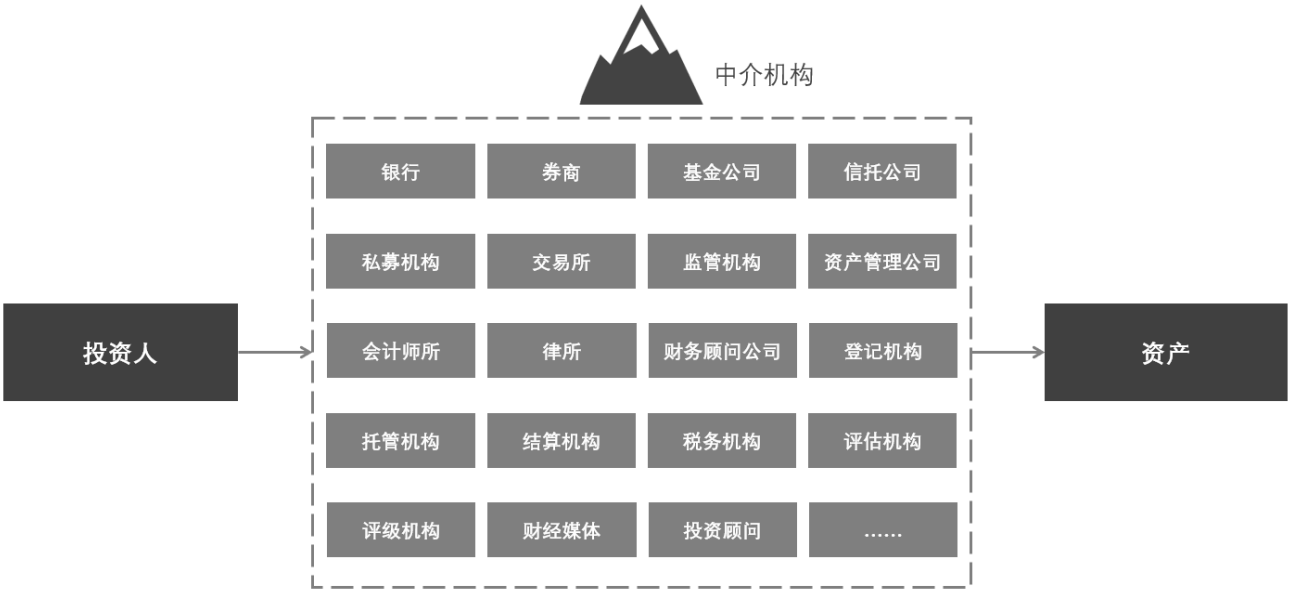
不过随着 2017 年末比特币冲击 2 万美元高点失败后带来的不断下跌，ICO 红利戛然而止。德勤调查了全球最大的社交编程及代码托管网站 GitHub 网站上的将近 86000 个区块链项目发现，如今存活的项目大约只有 5%，90%的项目处于非活跃状态。据同步财经统计，2018 年后登陆各大交易所的 247 种虚拟货币中，有 87.5%长期处于破发状态，算上曾登陆交易所破发后，二次上大交易所压低价格的币种，这一比例接近 90%。真正达到 10 倍以上收益的不到 3%。（数据来源：coinmarketcap 及同步财经数据库）

2018 年 2 月份以来，整个加密数字货币市场投资的专业性和难度逐步体现出来，整个投资市场也出现明显的收益两极分化、流通性不足等诸多特点。整个加密数字货币资产投资市场无论是个人投资者还是专业机构投资者都面临着一些限制和痛点，同时更多的未进入加密数字货币资产市场的个人和机构更需要合适的方式和引导参与进来。

对于个人投资者而言，缺乏加密数字货币的行业知识，对数字货币的甄别和选择能力不足，数字货币二级操作技能匮乏，面临着高风险低收益的困境。个人投资者一方面没有充足的时间和足够的量化交易工具在加密数字货币资产 7*24 小时的高频、大波动的交易中博弈；另一方面，在多个交易所账户注册、KYC 认证、去中心化钱包、冷钱包以及加密数字货币金融衍生品的操作过程中，会面对高门槛、专业且复杂的流程及操作要求；

对于专业的数字货币投资机构而言，加密数字货币资产目前流通性差，配套的相关量化开发工具、资产管理产品等十分缺少。相比传统的金融市场，整个加密数字货币资产市场缺少策略编写、回测、量化算法等工具，大量传统金融从业人员无法在数字货币资产市场充分发挥从业技能；同时目前专业投资机构和个人投资者逐渐缺乏足够的信任和连接。加密数字货币资产的特殊性，资金托管及真实业绩表现等都难以做到透明和信任。

对于传统投资个人和机构，现有的资产管理模式中面临着股权投资规模大估值高，投资金额大，投资周期长，募资渠道和来源相对单一等问题。当代资产管理体系的基础架构源自荷兰，几百年来虽然交易规则不断演化，各种信息技术的持续引入，但依然没有质的改变；“古典”资产管理生态演化到今天，最根本的困局是最初的投资人与最终的资产越来越远：



目前“古典”资产管理信息越来越滞后，并且变得残缺、失真、被篡改，权力在被不断剥夺，利益在被不断降低，主要的痛点如下：

1、 投资人知情权得不到保障，信息在传递过程中不断的被“后期处理”；

2、 未经同意的将投资人进行分类管理，实施人为操纵的“类型隔离”；

3、 所谓的评级机构，以保护投资人的名义，对各类资产进行打分，但结局总是让最大众的投资人为最有毒的资产买单；

4、 投资人的所有权在各种所谓法律的“保护”下，被不断演化出来的中介机构反复盘剥，变得所剩无几；

5、 投资人的决策权在层层代理机构的隔绝下，经常是“被代表”的角色；

6、 投资人的隐私权变得无足轻重，反而被任意的公示，检查；

7、 原始的资产管理生态，让绝大部分资产变成“牢笼”，投资人都身处于“围城”之中，外面的人想过去，里面的人变出来，但往往又无法实现；

8、 投资人沦落为永远是后知后觉，只能被动的接受经营结果。应有的经营权和监督权消失殆尽。

区块链技术的运用为投资者增添了全新的投资标的。资产管理指资产管理人根据资产管理合同约定的方式、条件、要求及限制，对客户资产进行经营运作，为客户提供证券、基金及其他金融产品，并收取费用的行为。“区块链+数字资产管理有两个维度，第一个是用区块链来改造基金管理的模式，另一方面是投资于区块

链上的数字资产，比如比特币、以太坊、EOS 等等。缺乏标准让传统基金的表现对比起来非常困难，并且基金审查也不透明；其次，成立和运行一个对冲基金非常消耗时间和资金成本，这就限制了只能在一个小范围内选择对冲基金经理，也因此限制了对冲基金的竞争性和可能的优秀表现；同时,还在用陈旧的技术架构投资对冲基金，造成很多低效性。“

2.3. What Opes Protocol are

Opes Protocol（Opes 是最古老拉丁语系中财富一词，为人带来财富）是一套去中心化数字资产投资生态的解决方案，包含了多种数字资产投资的协议。OPX 通证是 Opes Protocol 生态的基础，正如拉丁语的财富赐予数字资产生态新的生命一样，OPX 通证为 Opes Protocol 的金融生态系统提供动力，以协助维持网络的透明性和完整性并认证交易，同时以激励模式来回馈参与者，为 OPX 网络带来持久的稳定性。

协议，即为达成某个目的（如实现去中心化的加密货币基金生态），上层应用开发者以及相关参与者需要遵守的一组约定。如怎样建立一个加密货币基金，资金如何管理，如何实现去信任化等等。协议往往分为多个层次定义，如 Opes 协议逻辑上分为技术层的技术标准和去中心化生态层的参与者的行为规范。协议最终体现为某个产品的代码实现和应用落地，协议本身并不关心底层（公链）的技术细节以及上层应用的具体实现方式。

Opes 协议理论上可以支持任何智能合约平台，并不限制底层公链。Opes 将基于相对成熟的以太坊技术栈给出协议的一个实现，并研发相关的落地 DApp 和开发工具包，搭建投资者和基金管理员社区，验证经济体系的可持续性和相关协议的鲁棒性，并不断对协议本身进行更新迭代。

当前区块链应用面临很多实际问题，诸如公链吞吐量差，智能合约占用资源过多，单个爆款 DApp 堵塞整个网络，开发门槛较高，生态不开放不收敛等。Opes 选择不盲目相信和过度依赖未来的技术迭代，理智地选择当前被证实的技术路线，并认清当前的技术局限，在去中心化和效率间作出合理妥协，并开源核心代码，实现去信任化和高效的数字资产投资生态。

Opes 将运用通证的激励经济理念重组数字资产投资行业成本结构，增进投资人和优质基金管理人的自由对接。利用智能合约实现数字资产基金产品和金融衍生品的发行、认购、份额转让、赎回、分红、手续费计算等，同时利用区块链公开透明不可篡改的特性，记录操盘人的全部实盘操作、收益率以及客户评价，并进行加密存储，既保证投资人的资金安全，也能保护基金管理人的利益，使得好的投资策略可以公正地展示给投资人，为投资人带来合理收益。

Opes 的愿景：用区块链技术为数字资产投资行业赋能，以 Token 经济助力上下游资源高效自由流通，打造

高效透明的去中心化数字资产投资生态。

2.4. “区块链+金融”爆发期中 Opes 协议的表现

Opes 协议首先不仅仅是区块链金融的一个运用，更多的是一个用于区块链资产管理行业的协议。它为区块链金融生态中的场景应用提供协议层，并赋予被验证无误的扩展性和可靠性。

在整个生态里的早期位置是：Ethereum 区块链提供计算功能，ipfs 区块链提供数据存储功能，Opes 协议利用两者实现一些数字货币资产管理市场的基本功能，完全开源；然后数字货币资产管理行业的开发者和基金从业人员，比如基金平台（对应余额宝），股权众筹平台(对应 Kickstarter)或者任何点对点的交易的金融业态；都可以直接利用 Opes 协议提供的算法实现具体的去中心化的管理商业模式。没有 Opes 协议之前，每一个互联网金融的应用必须从以太坊最底层开始实现，比如怎么创建账号，怎么投资交易，非常复杂。现在有了 Opes 协议提供这些基础功能，开发者只需要把注意力集中到具体的商业逻辑就可以了。而基金经理则可以在基础之上把更多的精力放在自己所投资组合的回报上。协议层是现在区块链投资最关注的领域，没有好的协议层，即无法构建真实的应用；而建立优质高效协议层的技术门槛很非常高，必须要有非常出色的开发者团队。

然后为了能快速的推进数字资产管理行业的快速发展，Opes 协议还提供资产管理行业完整的区块链解决方案，Opes 协议将打造一个完整的系统生态，其中从底层操作系统的数据上链，资产管理垂直领域的智能合约体系，对数字货币这个去中心化的资产管理行业从发行、管理、托管、财务、清结算、审计以及监管、争议仲裁等提供全方位的系统支持。

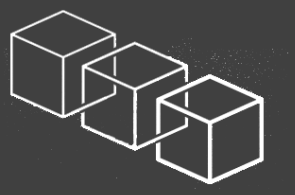
Opes 协议将支持一个开放式、高扩展的生态体系，我们将与行业其他生态进行深度合作，包括身份认证、内容传播、预测市场、资产借贷、可信数据验证、跨链协议等等，共同搭建起数字金融领域的基础设施。

OPES 将通过区块链的技术创新，金融规则的创新，以及上下游生态的建设，逐步去解决数字金融领域的存在的问题，永远站在投资者的立场上去对互联网金融体系做升级，以保证投资者资产安全，利益最大化。

OPES 希望用区块链技术去重塑一个蚂蚁金服生态。

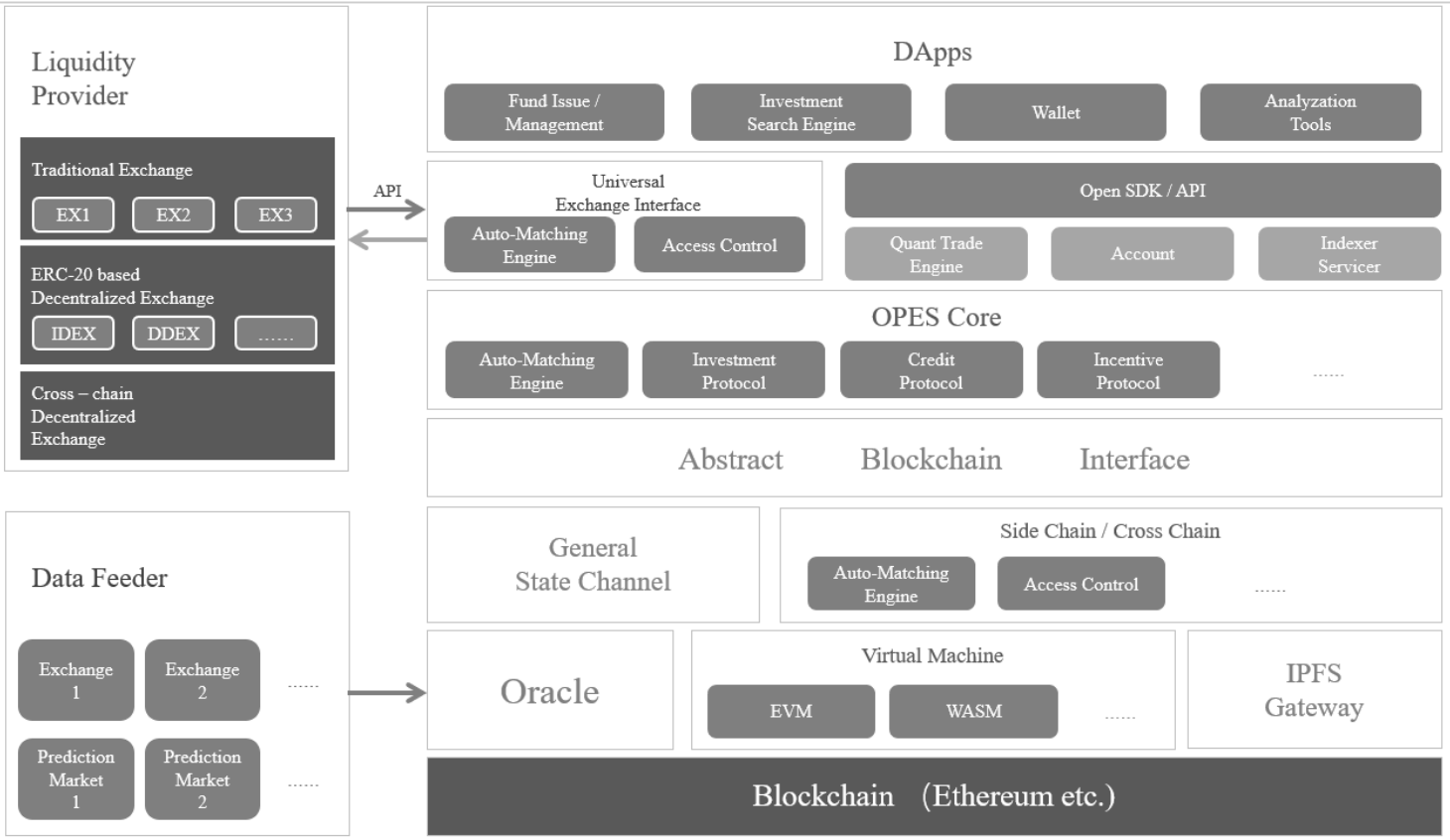
III.Opes 协议和技术架构

OPES Protocol（OPES 协议）是为解决去中心化数字投资的协议集，为各类 DApp 或第三方数字货币金融平台提供协议层支持。



Opes 协议建立在许多现存的开源项目、协议以及分布式系统之上。正是由于这些前人的工作，Opes 才变得有可能实现。Opes 协议将包含一套智能合约的接口，通过在具体的智能合约平台实现这些接口，来完成实际的业务逻辑。

技术架构图



3.1. 设计理念

Opes 协议理论上可以支持任何智能合约平台，并不限制底层公链。Opes 将基于相对成熟的以太坊技术栈给出协议的一个实现，并研发相关的落地 DApp 和开发工具包，搭建投资者和基金管理人社区，验证经济体系的可持续性和相关协议的鲁棒性，并不断对协议本身进行更新迭代。

Opes 将所有资产管理人的投资操作、充提币操作、基金当前状态等都记录在链上，一切行为公开透明。

核心关键的数据之外的数据，如描述文字、图片、评价、信用等信息将被保存在 IPFS，并与相关智能合约建立链接。如此可以实现更好的可扩展性，并减少不必要的燃费损失。当前端 DApp 创建了一个数据对象，并保存在 IPFS，一个唯一的 hash 将被建立引用该数据对象。随后，此 hash 将被保存至区块链。

Opes 既期待以太坊上面 Plasma 协议和 sharding 的技术突破，也期待 IPFS 上 Filecoin 的流通以及整体网络效率的提升。在未来逐步完善 Opes 平台的同时，Opes 将不断接纳最新的经过验证的技术。

综上，Opes 在架构设计上有 3 个重要的原则：

1. *Opes 力求去中心化和去信任化。Opes 不希望有任何单一的中心化节点，包括 Opes 运营团队自身，控制整个网络。*
2. *Opes 希望一直能站在巨人的肩膀上，不重新发明轮子。*
3. *Opes 会努力保证计算性能和用户体验的平衡。*

3.2. 核心组件

3.2.1 智能合约组

一套 Solidity 写成的智能合约。

Opes 将通过智能合约保存核心数据，同时实现资金的募集，投资，分红，手续费计算等自动执行。

Opes 将使用“抽象智能合约层”来实现合约代码的部署和升级。所有合约都将有一个封装合约，封装合约将一直指向最新的代码。之前旧版本的合约将被映射在某个版本控制合约中，如果有必要可以直接进行访问。所有的基金合约将在注册表合约（registry smart contract）中登记。

3.2.2 前端 DApp

Opes DApp 将会是一个开源的 React 应用或 JavaScript 应用，它将与以太坊网络、IPFS 网络、索引服务器进行交互。

DApp 将为用户提供一个友好的智能合约交互界面，来提供基金发行、资金调配、认购、分红等功能。Opes DApp 将使用 js-ipfs 来与 IPFS 网络交互，同时使用 web3.js 来通过 MetaMask 等钱包客户端与以太坊网络进行交互。Opes 鼓励开发人员可以基于 Opes 的合约来写出用户体验更好的 DApp。

一次经典的合约交互过程如下，资金管理人通过创建基金合约发行一个新的数字资产基金的时候:

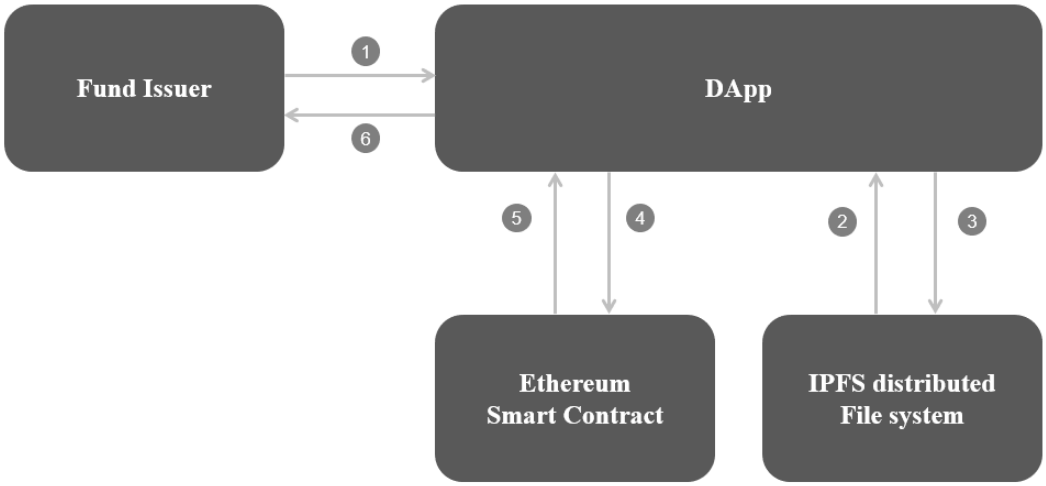


Figure 3 合约交互流程[6]

1. 资金管理人连入 Opes DApp。
2. DApp 通过与资金管理人的交互，生成了一个包含了各类基本信息的 JSON 对象（样式后面具体有阐述）。DApp 验证了此 JSON 对象符合标准式样，并上传至 IPFS。
3. IPFS 返回上传内容的 hash。
4. DApp 将返回的 hash 发送给智能合约工厂。
5. 智能合约工厂返回一个 txid。
6. DApp 将监视这条未完结交易，并在交易成功后通知用户。

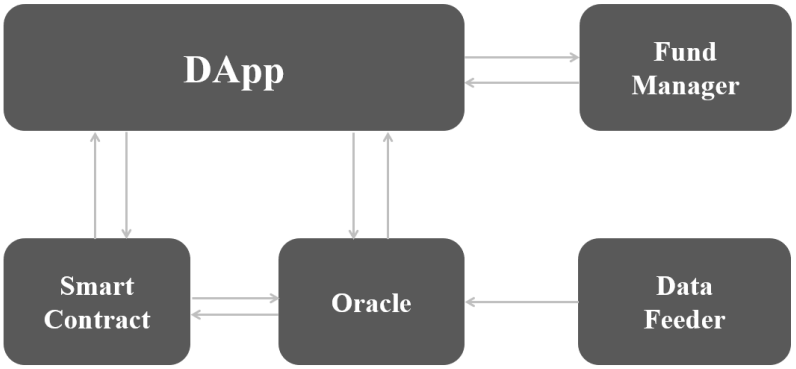
3.2.3 索引服务器

索引服务器是开源的服务器端的应用，它不断读取注册表合约中最新的基金合约信息，同时从 IPFS 上获取相关合约的文件和数据，并将读取的数据缓存加索引，以便实现 DApp 的快速搜索和条件过滤功能。

索引服务器在网络可扩展方面作用至关重要，Opes 索引服务器将为平台提供基本的搜索和过滤功能。Opes 将鼓励开发者分叉源码，开发自己的高效可扩展区块链应用。

3.2.4 预言机（Oracle machine）

预言机是一种可信任的实体，它通过签名引入关于外部世界状态的信息，从而允许确定的智能合约对不确定的外部世界做出反应。预言机具有不可篡改、服务稳定、可审计等特点，并具有经济激励机制以保证运行的动力。



Opes 数字货币基金智能合约执行分红的情况下，需要计算当前的收益情况，就要获取数字货币的市场价格（如 ETH/USDT），现在有一个第三方系统（预言机）可以提供权威准确、不可篡改、稳定、并可接受审计的市场价格查询接口，包括查询 ETH/USDT 的行情，在执行分红智能合约时会自动触发该预言机，预言机获取行情信息后，就向区块链发送一笔交易，交易的数据块携带了 ETH/USDT 的行情，随着每个矿工节点区块的同步，就保证了执行分红合约的共识。

Opes 协议需要的数据，除了交易所之外，另一个重要的来源是预测市场。预测市场的数据本质上来自于人，而非机器，比如那些博彩，下注，竞猜等一切与比赛结果相关，并捆绑了自身利益的人，都可以成为预测数据的提供者，因为他们捆绑了自身利益，他们不会牺牲自身利益提供虚假数据，从而有效地保证了数据的可靠性和真实性。

在绝大部分情况下，一台预言机已经足够，但在处理重大资产时，常常一台预言机并不能保证完全可靠，有人提出了多台预言机的解决方案，比如设置 5 台预言机，如果其中有 3 台或 3 台以上给出的价格一致，则向区块链发起一笔携带此价格备注的交易。这种由多台单一预言机组成的多重模型又被称为预言机网络。

3.2.5 状态通道

状态通道是一种进行链下交易和其他状态更新的一种技术。在一个状态通道内发生的事情保持着非常高的安全性和不可更改性：如果出现任何问题，Opes 可以选择回溯到链上交易中，关闭通道，并释放锁定的

资产。

支付通道的概念已经存在多年，如比特币区块链上的闪电网络。而状态通道不仅可以用来进行支付，还可以用来在区块链上进行任意的状态更新，就像改变智能合约的内部状态。2015 年，杰夫·科尔曼首次详细描述了状态通道。

✧ **资金管理人 Alice 的例子**

资金管理人 Alice 在 Opes 平台创建了基金合约，操作得当的话可以拿到分红。要做到这一点，最简单的方法就是在区块链（以太坊）上创建一个智能合约，它可以实现基金操作的规则，并跟踪管理人的操作。每次管理人进行一次操作的时候，他们向智能合约发起一个交易。当交割分红的时候，智能合约就给 Alice 支付一定量的分红。

这是可行的，但是效率低下、速度慢。Alice 让整个以太坊网络处理这个基金合约，这明显多于她的需求。每次 Alice 想要进行操作的时候，她都必须支付 gas 费用，而且必须等几个块被挖出后才能采取下一步行动。

相反的，Opes 可以设计一个系统，让 Alice 尽可能少地进行链上操作的情况下来做资金操作。Alice 能在链下更新基金合约的状态，同时操作资金，并仍然有充分的信心，如果有必要的话，他们可以恢复到区块链（以太坊）主链的状态。Opes 把这种系统称为状态通道。

✧ **Opes 基金合约应用和限制**

状态通道在需要频繁合约交互的应用中非常有用，它们在执行链上操作方面有严格的改进。对于一个 DApp 是否适合通道化会有如下一些权衡:

a. 状态通道依赖于有效性

如果通道参与者在挑战期内丢失了网络连接，则可能无法在挑战期结束前做出回应。不过，参与者可以让他人保留自己的状态副本，并支付一定费用，来保持有效性。

b. 基金管理人将在很长一段时间内交换许多状态更新

在部署法官合约时创建的状态通道有一个初始成本，不过一旦部署完毕，在该通道内每个状态更新的成本就会非常低。

c. 基金管理人在单一合约中相对固定

法官合约必须始终知道作为通道的一部分的实体（即地址）。Opes 可以添加和删除成员，但每次都需要更改合约。

d. 基金管理操作需要强大的隐私性

因为一切都在参与者之间的通道“内部”发生，而不是广播和记录在链上。只有最初和最后的交易必须公开。

e. 状态通道具有即时终结性

只要基金合约的参与者多方都签署了一个状态更新，这个状态就可以被认为是最终状态。双方对此都有很高的保证，如果有必要，他们可以“强制执行”将此状态放到链上。

3.2.6 跨链

Opes 协议要实现的去中心化/去信任化的投资生态，包含了两个层面的问题，一是对资金管理人的去信任化，二是对资金安全的去信任化。而彻底实现基于智能合约的资金（可能是来自多条链上数字资产）的管理/流动/分红，就需要跨链技术带来的去中心化币币交易。终极的状态，是跨链智能合约。

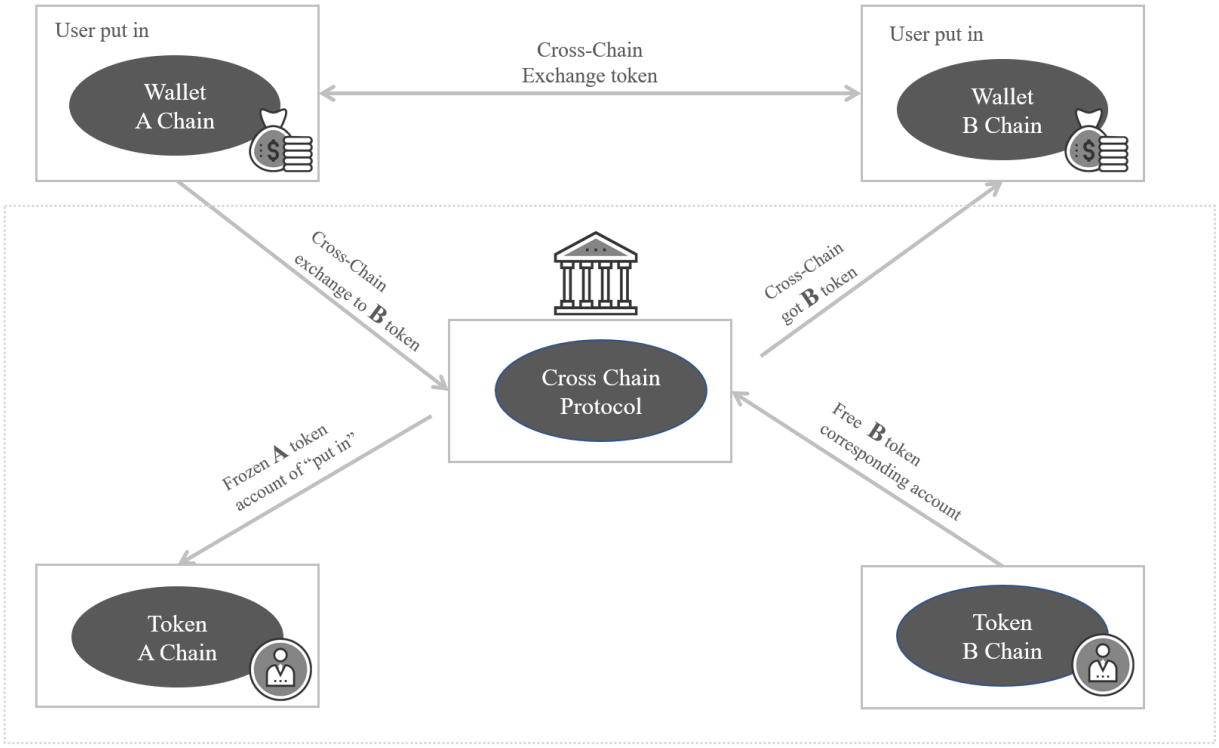
目前主流的跨链技术包括：

1、 公证人机制（Notary schemes）

2、 侧链/中继（Sidechains/relays）

3、 哈希锁定（Hash-locking）

去中心化的跨币交易所是最基础的跨链模式。无论跨链实现方式如何复杂，跨链的本质都是如下图所示：



基础的跨链实现有下面五个步骤：

1. 用户使用 A 链币向跨链协议发起兑换 B 链币的请求；
2. 跨链协议锁定用户 A 链币；
3. 跨链协议锁定等额数量的 B 链币；
4. 将 B 链币发到用户 B 链钱包地址，同时拿走用户锁定的 A 链币；
5. 用户 A 链钱包币转走，对应获得 B 链钱包等额币。

真正去信任化的跨链数字资产交换想要自动运作必需要上面三种技术方案配合来实现，然而 Opes 想要实现基金合约的跨链资金管理，就需要实现：

1. 便携式资产（Portable assets）：资产可以多链之间来回转移和使用。
2. 满足原子性交换（atomic swap）：跨链资产兑换是安全的而且同步发生的。（不同链上的两位用户可以发起两笔传输交易，要么在两个账本上一起执行，要么两个账本都不执行，即原子性）
3. 带有跨链互通性，具备他链信息和事件的读取和验证能力（Cross-chain oracle issues）：在某些情况下，一个链（如 A 链）的智能合约执行机制可能是依赖另一个链（B 链）的条件触发，所以 A 链要能获得 B 链的所有相关条件状态，即 c 具备他链信息和事件的读取和验证能力。
4. 资产留置权（Asset encumbrance）：在某些情况下，相关联的两个链资产同时需要被锁定，如抵押品或者法院强制执行的扣押等。
5. 跨链执行合约（General cross-chain contracts）：例如根据链 A 的股权证明在链 B 上分发股息等。

跨链所涉及到的技术点非常多，很多细节实现难度很大，目前牺牲一部分效率验证跨链 SPV 的情况下基本可以实现跨链的去信任化币币资金操作，而且这也要面临流动性的问题：基金合约管理的资金可能数额较大，依赖去中心化跨币种交易可能无法满足必要的流动性。

跨链的基金智能合约则面临更多的技术难点，Opes 将可能在多重签名公证人机制（Multi-sig Notary Schemes）以及分布式私钥控制技术（Distributed Private Key Control）方向上投入更多精力，最终实现 0 信任的资金流动。

3.2.7 流动性供应方（Liquidity Provider）

Opes 作为去中心化、去信任化的数字资产基金投资平台，需要时刻保证智能合约自身掌握基金中的实际资金的核心控制权。如资金的流动、交易、监控和分红等。

✧ 3.2.7.1 宿主链去中心化交易所

智能合约本身可以自然地（natively）处理宿主区块链（如以太坊）上的数字资产，典型地场景是，Opes 引入一个基于 ERC20 数字资产体系的去中心化币币交易所，如 IDEX、DDEX 等。理论上 Opes 基金合约（锚定币种为 ETH）可以去信任化地完成一笔资金的操作，当前去中心化交易所越来越受到行业参与者的重视，去中心化交易所（Decentralized Exchange，DEX）可以提供越来越多的流动性。

✧ 3.2.7.2 跨链去中心化交易所

基于中继/侧链技术的 Polkadot 和 COSMOS，以及基于分布式私钥控制技术的 WanChain 和 Fusion 都将有基于各自跨链技术的跨链去中心化交易所。随着技术的进步和万链互联（Internet of Blockchain）的思想深入人心，去中心化跨币交所或将为 Opes 提供更多的去信任化流动性支持。

✧ 3.2.7.3 中心化交易所

去中心化方式无法消化的流动性由传统中心化的交易所解决，Opes 将与多家流动性较大的中心化交易所达成战略合作，开设特殊的保险账户，联合多家保险公司保障资金安全，同时支持较大宗的下单操作。Opes 将为这些交易所账户保留较大的资金池来保证流动性。

✧ 3.2.7.4 场外交易（Over The Counter, OTC）

场外交易会增加古典机构与虚拟资产机构的之间的互动，体现在增加流动性和数字资产的灵活性中。Opes 协议会支持 OTC 的业务模式，对资产的清结算进行支持和管理，以此来增加 Opes 生态中的金融场景与传统资产的关联度。

3.3 Opes 数字资产基金协议

数字资产基金产品是 Opes 的核心，一切其他的环节都要围绕基金智能合约来展开。本节详细介绍相关的智能合约设计、数据结构设计以及交互接口设计。

3.3.1 智能合约接口（Smart Contract Interface）

Opes 基金的发行和管理将基于智能合约进行，注重合约本身的逻辑和关键数据保存，真实资金的流动将依据具体情况进行去中心化/去信任化的管理。

接口包含基金的关键属性和核心操作，Opes 将给出接口的多种类型和基本模版，作为具体实现的基础，同时给出自定义接口甚至开发者代码接口。下面是基金合约接口的伪代码，使用 Solidity 语言编写：

```
contract FUND {
    // 基金名
    string public constant name = "TO THE MOON 005";
    // 结算币种
    string public constant base = "ETH";
    // Balances 保存投资人投资额
    mapping(address => uint256) balances;
    // 基金发行者（操作资金的权限）
    address public manager;
    // 基金监管者（监理权限）
    address public observer;
    // 硬顶
    uint256 public constant hardcap = 1000;
    // 实时市值（按结算币种和市场价计算）
    uint256 public cap;
    // 投资对象币种级别限制
    // level1: cap larger than 1b USD
    // level2: cap below 1b but larger than 100m USD
    // level3: cap lower than 100m USD
    uint8 public constant level = 1;
    // 状态 0:created，1:open, 2:operating, 3:closing, 4:closed
    uint8 public status;
    // 操作列表对象索引：保存于 IPFS（如"cc3bef279ae8"）
    string public ipfs_op_list_object;

    // 获取总投资额
    function totalInvestment() constant returns (uint totalInvestment);
    // 获取投资者的初始投资额
    function balanceOf(address _ investor) constant returns (uint balance);
    // 基金进入分红阶段后可以进行利益分配
    function withdraw() returns (bool success);
    // 如果是 ETH 则可直接接受充币，同时记录投资人投资额
    function() payable;
    // 调仓。"EOS/ETH", "BUY", "200"。配合 Oracle 服务和交易所 API 操作下单
```

```
    function operate(string pair, uint8 op_type, uint256 amount) returns (bool success);
    // 通过 Oracle 更新实时市值
    function refreshCap() returns (bool success);
}
```

3.3.2 数据结构（Data Schema）

✧ 3.3.2.1 基金操作列表

本节定义了用于保存基金中具体资金操作的对象数据结构。实际的数据对象将保存至 IPFS，其 hash 将保存至智能合约中作为索引。

```
"op_list": {
    "id": "cc3bef279ae8",
    "fund": "e3fd8a426bc",
    "tx": {
        {
            "op_count": "0",
            "op_type": "BUY",
            "pair": "EOS/ETH",
            "amount": "208.482",
            "price": "50.42",
            "time_stamp": "201806170612482",
            "fee": "8.32 OPX",
        },
        ...
    }
}
```

IV.基于 Opes 协议的产品设计

OPES Protocol（OPES 协议）是为解决去中心化数字投资的协议集，为各类 DApp 或第三方数字货币金融平台提供协议层支持。

Opes Protocol 是解决区块链数字资产管理的协议层解决方案。在讨论技术之时，我们面对的根本问题还是采用区块链的技术去解决问题：投资门槛高、稳定性不足、中介过多、流程不透明性、去人为因素，同时通过信任机制获得更多的流动性和流量。我们的目的不仅仅是虚拟货币的投资者，我们还需要面对更广大的传统投资者和投资服务者。

区块链开发的长周期和技术的不确定性，我们会按照应用落地原则进行项目的整体推进：

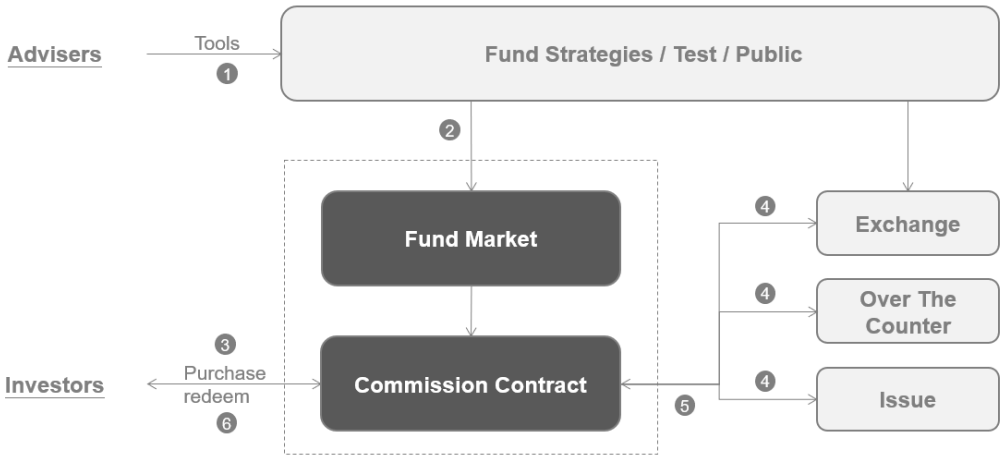
1、 *开发完成“基金投资功能 DApp（区块链应用）”；*
2、 *投资者社区的建设和运营，完成投资者从“加密货币价格投资”转向“数字资产专业投资”的角色转变；*
3、 *通过 DApp 对 Opes Protocol 概念验证（PoC）；*
4、 *基于 Opes Protocol 的资产管理平台；*
5、 *Opes protocol 的协议栈；*
6、 *基于 Opes 的生态，Opes 团队仅仅作为技术和治理提供方提供服务；*

4.1.数字资产投资 DApp

无论是早期的 Opes DApp 应用还是未来的平台产品乃至整个生态我们首先解决的问题还是如下三条：

- 虚拟货币及资产更低的投资风险，更好的投资收益。
- 真正公平和透明化的投资
- 数字资产投资在整个金融体系中的合规性

Opes Protocol DApp 的产品业务流程：



1. 顾问通过协议工具消耗 OPX 完成基金策略、回测、发布等工作;
2. 相关基金及金融衍生品通过智能合约完成合规后在基金市场上的推广展示同时消耗 OPX 示
3. 投资者通过 ETH、OPX 等 token 进行申购
4. 智能合约通过限制条件及合约条款进行操作
5. 数字资产市场对基金的到期清结算
6. 投资者对投资的赎回

角色（特点）	*Opes Protocol DApp*
各个环节参与方（信息披露完整/信息公开透明）	*全网交易打包写入区块链（时间戳），通过区块链披露资产、融资机构全生命周期的信息* *全网节点参与几张，分布式数据存储*
投资人（资产不可篡改）	*关键信息计入区块链通过共识机制、非对称加密技术保证数据库真实、不可篡改和销毁。保障资产可靠性及降低风险。*
融资人（提高优质标的物融资效率）	*智能合约计算机自动执行，合规法律机构进驻；可替换纸质合同，减少线下审批环节。*

4.2. Alpha-Investor 社区运营计划

区块链世界的共识来自于社区的形式，社区就是我们孕育用户、培养用户、倾听用户的地方。

Opes Protocol 作为一个去中心化数字资产投资生态的协议栈，是为了让数字资产在可控安全的环境下去发展，集合更多金融领域的专家和更多的非专业投资者，为数字金融提供更多的可操作性和流动性。

我们鼓励整个社区一起加入和参与，开发过程中需要由这些需求者和参与人不断的探索。与此同时，吸引社区中更多人参与，然后需求又向着更完善的方向发展，并进一步推动技术进步。

我们的社区会聚集:

- 对项目感兴趣的技术工程师、极客或区块链爱好者
- 专业的投资顾问，提供金融专业知识
- DApp 的服务提供方，例如中心化或去中心化交易所、借贷平台、票据市场等金融服务提供方
- 参与我们的节点的人或机构
- DApp 应用的使用者
- 代币的投资者，包括基石机构、私募机构、早期投资者和潜在的未来投资者
- 其他，培训机构、媒体、监管机构等

我们谋求的是区块链应用的真实可落地，并且希望社区投资者会逐步成为我们应用的实际用户、开发者和治理者。

4.3. 基于 Opes 的数字金融资产管理平台

Opes 协议是一套去中心化数字资产投资生态的解决方案。Opes Protocol 包含了多个协议来帮助建立不同“特点和属性”的资产管理平台和数字金融平台来帮助更多的投资。

- *数字资产发行协议*
- *基金份额交易协议*
- *登记结算协议*
- *去中心化的基金市场协议*
- *多侧链和可扩容协议*
- *数字货币金融产品设计协议*
- *量化投资开发接口协议*

- *数据持久化协议*
- *公正收益排行和评价体系协议*
- *生态激励和动态调整协议*

Opes 协议理论上可以支持任何智能合约平台，并不限制底层公链。Opes 将基于相对成熟的以太坊技术栈给出协议的一个实现，并研发相关的落地 DApp 和开发工具包，搭建投资者和投资顾问社区，验证经济体系的可持续性和相关协议的鲁棒性，并不断对协议本身进行更新迭代。

因此，为了让 Opes Protocol 更好的服务市场并获得市场的认同，我们同样也会建立真实可操作的工具和平台*"数字资产管理平台"*为 Opes Protocol 获取更多的技术样本。

A. 基金的发行和销售

多种条件的智能合约可以支持基金的自动化发行。基金发行和智能合约提供金融产品的定价、交易规则、交易所信息、交易执行、数据访问、费率设置和分红计算。优秀的算法交易员和资产管理人可申请发行基金和资产管理产品，为用户的数字资产保值增值，同时收取服务佣金。平台也会提供较为稳健的金融衍生品，包括主要虚拟货币的投资组合、Index 指数基金、ETF 等。

平台基于实盘情况和信用记录为基金市场的从业人员发行基金，基金发行后的执行和结算会依托场内交易和场外交易引擎。

针对场外交易买卖：多种资产将会涉及场外的到期结算和申购，通过智能合约对基金进行限定条件的结算和申购。

针对场内交易撮合：投资者将数字货币转入多方管控的智能合约账户并获取对应的基金份额，同时限定交易所账户只能将数字货币提现到该智能合约账户，保障投资者的资金安全。**针对去中心化交易撮合**：通过基于 Opes 协议智能合约在撮合引擎中自动执行，整个投资与清结算过程利用跨链技术和多侧链技术。

B. 量化投资开发者工具

构建量化交易策略会参考多种算法包括曾经的 FranklinAllen 使用遗传算法来找出最优的交易规则[7]，Tak-chungFu 从众多技术指标中找到最优的入场组合，以及使用遗传算法来进行最优品质组合配置[8]，Jiah-JenChang 考虑风险的情况下利用遗传算法来筛选技术指标[9]。Opes 平台的开发者可以基于 Opes 协议开发不同的投资组合、交易策略、趋势分析等，所有的投资均可以有不同的风险偏好或者收益预期，例如货币组合、摆单交易、对冲交易、货币合约等。开发者工具也提供各类投资策略的回测环境进行实盘模拟验证，为开发者提高量化策略的可靠性和有效性。

关于高频交易策略的例子，用于工具开发逻辑：

1、 通过制造流动性来获得盈利的交易策略

2、 猎物算法交易策略需要对历史数据进行充分研究和挖掘。通过人为操纵使得买入价格提高或者卖出价格降低，从中进行获利的交易手段

3、 做市商交易策略，通过联系不断地向交易所提供某一特点的买卖价格，并且有能力在特定价位上满足众多投资者的买卖要求，利用自由资金与投资者进行交易。

C. 基金市场

平台会挖掘优质的策略发布者（机构/个人），对于发布策略/基金业绩提供多维度评估：复合收益率、阿尔法系数、最大回撤等。发掘具有成长潜力和投资价值的策略和基金组合，对有潜力的、优质的基金（策略）给予多维度支持；根据惯例规模、策略数量、策略容量等因素综合的考量，给予资金支持；纳入代销观察池，酌情降低机构代销的背景调查要求；优质基金需要的其它支持等。

D. 风险建模工具

基于数字资产的投资特点提供多种建模环境和影响因子的引入。

关于的收益与收益均值的例子：

设 X 是描述投资基金组合损失的随机变量，F(x)是其概率分布函数，置信水平为 a，

则：$VaR(a)=-\inf\{x|F(x)\geqslant a\}$

平台会提供对应的建模工具和 API 接口供第三方，为风险计算提供可操作的模型设计工具。

E. 数字身份识别和匿名

数字身份系统工具是通过可验证的匿名和加密签名技术，完成匿名的声誉评级，不需要提取用户身份即可完成评价，该规则可以让优质用户提高平台忠诚度和使用频次。

- 避免恶意刷分行为
- 避免用户信息泄露行为
- 提高评级可靠性及真实性，让身份规则为生态提供良性的循环

F. 审计和合规智能合约

账户细节安全编译可以涉及每笔交易账户信息完整度和历史记录（收寄细节、标的物信息、托管信息、实体信息等）相关的规则进行汇编。可以为智能合约提供数据支持，一旦超越合约阈值即可进行合约审计调研（非人为）的发起，对应的数据即可向数据持有者申请开启并作为评判的依据。

平台不持有数据，但是智能合约会限制制约不合规的条件，让金融体系可以在规则下运行。在有必要的时候智能合约可以验证其源头和个人、企业、子实体之间的关联关系。

由于所有涉及特定客户的交易都能自动追溯，这些记录将作为银行按照反洗钱要求行事的证据，使之迅速实现与监管要求的合规性。

G. 其他的服务类功能

为资产委托方、管理方、托管方、代销方在资产变动、投资明细等信息操作的工具性服务类功能，包括存管机制、分账户系统、风险管理系统、结算系统、投研系统、交易系统和业绩监控系统等。

4.4. 基于 Opes Protocol 的生态

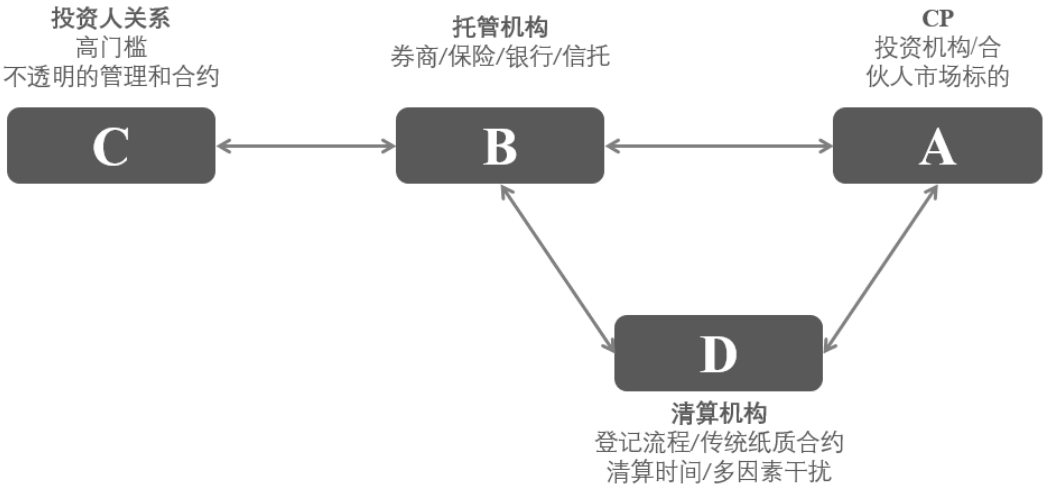
构建一个自治的区块链金融生态，去通道化去中介化，回归资产管理本质。

Opes Protocol 的愿景是用区块链的技术特点打破传统金融中“ABCD”的固化结构，互联网已经解决了一部分工作但是根本的问题还需要分布式共识的思维去解决。

我们可以了解到投资者、融资方乃至监管方的意图，其本质还是在于资产管理行业的整体生态再造，金融监管的协同化将不断压缩不同主体的套利空间，对资金池业务的严格控制和对投资组合集中化风险的详细规定都有助于金融合规及风险的控制。

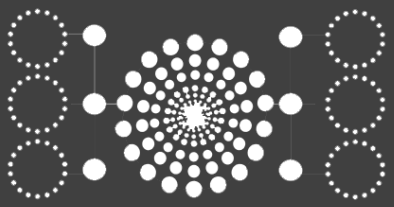
向前看，未来各类资产管理机构都将不能继续仰赖“红利”而从事信息不对称的业务，主动管理业务的能力将成为资产管理机构的核心竞争力所在。资产管理业务的“去中心化”最终也将解决当前过度金融化的问题，事

实上将使得优质项目乃至实体经济受益。



V.组织模式

我们需要考虑一个组织是什么。从结构角度看，组织是不同参与者和实体（例如，人员，其他组织，机器）之间的一组协议。这些协议采用合同和内部规则，正式和非正式协议，准则，流程和程序的形式。总的来说，治理规定了不同组织实体（如管理层，员工，所有者）明确责任，财产权，付款和组织运作的其他要素。



在分布式资产管理的生态中，我们需要基于区块链的智能合约来自动执行的协议，这些协议（即 Opes protocol）是开放的，安全的，并提供问责制度和透明度。此外，每一方都可以确信承诺会得到真实地保留。因此，我们结合区块链智能合约和中心化的高效管理方式确立了分布式资产管理的治理模式——*"四权分散式组织"*

*"四权分散式组织"*的治理概念的根本目标是形成高效安全可靠的分布式投资模式。

Organization 1：决策权组织

即拥有投资决策权力的组织（个人），可以进行金融衍生品的挖掘开发，资产组合的配置，投资行为的计划。决策权组织仅有决策权，无法接触到资金。

Organization 2：执行权组织

即根据决策权组织的投资决策进行实际资金操作权的组织（个人）。由于资金存储在智能合约中，资金的执行权是由机器和组织共识执行。执行的过程中会牵扯各个执行组织的权重、资质、信息等，同时机器执行会采用多种侧链、跨链和接口进行自动操作。

Organization 3：监督权组织

即拥有监督资金流转权的组织（个人），可以对资金和账户等进行冻结、审计等操作。资产管理是一套完整的金融生态，需要监管进行风险防范和合规性监督，一旦出现问题会形成系统性风险。无论在早期还是在中后期监督权组织都会需要。

Organization 4：运营权组织

即拥有基础设施运营权的组织（个人）。其提供投资服务的基础功能，技术服务，新功能开发等，不会参与任何资金相关的行为，不涉及资金的沉淀和管理。分布式资产管理平台和治理模式形成，所有的数据和功能均在分布式服务器上，没有任何人可以关闭它，最终可实现自运行的投资产管理服务。

这里必须要提到的是，每一类组织都是分布式的形态，进行相互博弈和共识。组织之间也可以进行转换，组织内共识之后进行组织间共识。组织的转换可以让资源充分在治理过程中体现价值，组织内部和组织间的以此来保证共识的高效性、有效性和安全性。等待区块链的 TPS 到达百万级别，治理的模式可以完全向 DAO 过渡。

Opes Protocol 的“四权分立”的治理模式既要依托于区块链智能合约，还要依托于中心化的组织（个人），其介于 DAO（分散自治组织）和中心化组织之间。在金融的世界，风险是第一位，我们需要落地和实现真实的资产流转需要在中心化和去中心化取得平衡并取得支持，之后逐步走向真正的分布式自治。

VI.核心团队

传统金融资产管理的业务已经有上百年的历史，他们的经验依旧需要延续和传承。团队均来自于金融投资行业和资产管理行业的资深人士和区块链行业的专家。

CEO 龙小波

毕业于上海复旦大学，从事金融市场投资及管理工作长达 20 余年，熟悉中国内地及香港的资本市场，多家券商和公募基金公司的创始人，擅长于资产管理、证券投资、收购兼并、公司改制及财务顾问咨询业务。

曾任大鹏证券副总裁，负责投资银行和海外市场业务。

曾任大成基金管理有限公司首任总经理，大成基金成立于 1999 年，是中国首批获准成立的“**老十家**”基金管理公司之一，具有全国社保基金投资产管理及境外配售产品管理人资格、基本养老保险基金证券投资产管理业务资格、受托管理保险资金、保险保障基金投资产管理、特定客户资产管理和 QDII 业务资格。

现列席多家国内外上市公司董事及总经理，以及柏恩投资、柏坊资产管理的总经理。

投资案例包括：奇虎 360、分众传媒、国泰君安、长城证券、北京银行、成都商业银行、南京天数等

Co-Founder & Operation Director Leslie Van

英国 Coventry University MBA 金融硕士，投资人，ChainBANK Capital 合伙人。主要研究方向：金融、证券、股权投资、上市辅导等领域，成功投资多家企业在德国、国内 A 股及创业板上市。近年来主要研究区块链在新金融领域的投资方向，力图在区块链场景应用投资方面有较大突破。区块链项目投资案例：OMG，EOS，兰花协议等。

CTO Wentao Zheng

南京大学计算机本科和硕士，计算机方面的专家

任职于谷歌美国超过 8 年，负责多个项目包括 Google Cloud、Google X（Confidential Project）等项目的技术负责人和架构师。为谷歌的核心项目设计整体技术架构：包括存储、同步协议、服务器到客户端推送和跨平台的共享数据层等。曾就职于 IBM 研究院，负责研究智能人机交互和信息可视化并设计开发

其拥有 7 篇研究性论文和 3 篇专利。

CRO 邢毅

原就职于各类大型金融机构，曾担任中金（香港）高管和柏恩投资副总负责整体投行业务。

邢毅先生擅长风控及投资管理，曾处理百亿级投资管理和前期风控的安全管理。任职期间金融投资业绩优异，投资案例包括：奇虎 360、分众传媒、成都银行、国泰君安证券、北京银行等

CMO Mia Shang

美国东北大学金融学士

前 DAppLabs CMO，加速及推广超过 20+海外优质区块链项目

曾任职毕马威会计师事务所咨询部门，就职期间曾担任浦发银行及多家大型上市公司风险咨询顾问。曾任职于腾讯系富途证券行情及社区部门。曾担任 MIT Chief 中国创新与创业论坛融资经理。

专注于通证经济如何变革金融领域的生产关系

Investment Director VICTOR.LAU

加拿大劳里埃大学 MBA 学历，曾担任加拿大显达理财集团投资经理、深圳盈信创投公司投资经理，具有超过 25 年国内外基金管理经验，熟悉全球证券市场和投资产品，有扎实的经济理论及数理估值建模功底，具有全球市场联动性的深刻洞察力。刘先生投资信仰价值投资，投资风格保守稳健，对港股 TMT、消费电子、保险、医药、教育等行业有较深的认识，是相关行业的选股高手。刘先生于 2012 年 7 月至今负责管理龙动力基金，2013 年获得中国海外对冲基金第二名（私募排排网评选），管理期间总收益超 231.52%，年复合回报率 26.6%。

Finance Director TIGER.WU

前高盛财务总监，跨国集团公司金融及财务相关工作从业经历 20 年以上，主要围绕证券和期货公司。曾担任 Qiankun Futures 公司 CFO，大鹏证券、银泰证券和可口可乐财务经理，乾坤期货财务部总经理。

Business Development Director 慕亦凌

链银资本创始人，BitAlpha 行情社区联合创始人，ElevenEX 数字交易所投资合伙人，长期深度参与区块链行业中的各项业务，多个项目早期投资人。毕业于澳大利亚知名大学 Swinburne University，也曾在海外参与 Whitehorse 等早期知名区块链自媒体的发展。

Product Director Simon Mao

前万向区块链实验室产品业务总监，负责区块链产品应用框架的设计，专注于溯源、物流、能源、供应链金融领域。曾任世界 500 强公司分布式能源高级咨询顾问，曾担任某物联网企业联合创始人。专长于分布式治理模式的研究和区块链产品应用框架。

VII.顾问委员会

朱菁

资产管理投资公司董事长，资产管理行业大咖。

朱菁先生现任富坤投资董事长兼总经理。

朱菁先生曾任深圳证券交易所上市总监，哈佛大学客座研究员、深圳市新财富多媒体经营有限公司副董事长。现任深圳市富坤创业投资有限公司、上海富堃投资管理有限公司董事长，南京南农高科技股份有限公司董事、上海财大金融学院兼职教授等职。具有超过 18 年的证券从业经历，熟悉国内外资本市场运作，具有丰富的股权投资和企业投融资策划及实际运作经验。

朱菁先生曾获复旦大学经济学博士学位，以及高级经济师资格

薛蛮子 Charles Xue

著名天使投资人，奇虎 360 董事长周鸿祎称他为“中国天使投资第一人”。曾担任中国电子商务网 8848 董事长、中华学习网董事长等职务。目前活跃在中国的创业圈，所投项目包括汽车之家、点融网、驴妈妈、265、雪球财经、美豹金融、51 信用卡、神策数据、帝科思跨境电商、火炬租房、易思汇留学平台等众多项目。薛蛮子是传统投资界最早关注数字货币和区块链投资的投资人之一，2017 年投资了 20 个区块链项目。

李云鹏

南京天数润科创始人&CEO。毕业于南京大学计算机系、美国威斯康辛州大学麦迪逊校区硕士，曾任美国甲骨文公司数据库部门研发总监，带领跨过团队为 Oracle Database 11g、12C 和 Exadata 做出卓越贡献。专长于研发体系的组织和管理以及智能系统架构设计。

陈怡仲 Jeremy Chen

在大型国际金融机构历练多年，包括美国花旗集团与渣打银行集团，拥有丰富的投资银行与商业银行经验。在渣打银行直接投资部中国总部负责另类投资业务多年。

芝加哥大学布斯商学院 MBA（荣誉成绩毕业）

2012 至今：中富資源有限公司 Deputy CEO/执行董事/法人代表（HK.0274）

2010 - 2012 年：渣打銀行直投部門另類投資

2000-2010：花旗集团亚太区总部特殊资产管理、花旗集团上海和花旗集团台湾的企业金融和全球交易银行。在银行交易金融（包括電子商務和電子支付），企業金融，另類投資，資產重組，財務顧問，借款融資，特殊資產管理等方面擁有超過 17 年的經驗。

孙祺扬(孙强)

前海知行资本 CEO，香港公开大学 MBA，现就读 BSN（荷兰国际商学院）DBA，十多年股权投资领域从业经验，熟练掌握企业战略规划、资本运作等相关知识，曾担任福建知名国有创投“火炬创投”总经理、董事长，曾被评为 2015 年福建十大投资人，2017 年获评金汇奖最受母基金青睐创始合伙人 TOP100，兼任深圳上市公司并购协会副会长等多项社会职务；投资参与上市项目三十多个，并参与多个区块链项目投资。

Jessica Luo

毕业于清华五道口金融专业，暨南大学 MBA

Canada Sunrise Metal Recycling Ltd. 公司联合创始人，Sunrise (Hong Kong) group limited 公司创始人

深圳市兴为通科技股份有限公司创始人，链众资本联合创始人，曾参与投资：Ripple、QASH、CyberMiles、SmartMesh、ObEN PAI、RSK 等项目

周冰阳

现为相对论资本创始合伙人，车联集团董事长，VOS 汽车链联合创始人，车金互联创始人，东南大学区块链研究中心副主任，东南大学区块链研究院有限责任公司合伙人，曾参与投资过 pst，beechat，rct，HMC，btm，ulsee，XMX，VOS 等项目

谢正伟博士

现北京大学物理学院定量生物中心博士，加州大学旧金山分校联合培养博士，北京大学博士后。

2016 至今，作为 Tenure-track 特聘研究员，北京大学医学部基础医学院和系统生物医学研究所进行研究工作。学术方向：医学大数据，金融物理，人工智能，生物信息学，系统生物学

Celilia Wang

北京航空航天大学计算机本科及分布式计算硕士。基金投资经理，一级市场投资孵化及技术顾问，主要负责区块链项目投资及孵化，Voyage 项目技术顾问；参与孵化 ULSee、Tube、DAC、WEtoken、Crptube 等等；

区块链项目早期投资人，曾投资 Cortex、Elf、ONT 等；

Ⅷ. Opes Protocol 通证的分配方案

Opes Protocol 的通证定义为 OPX

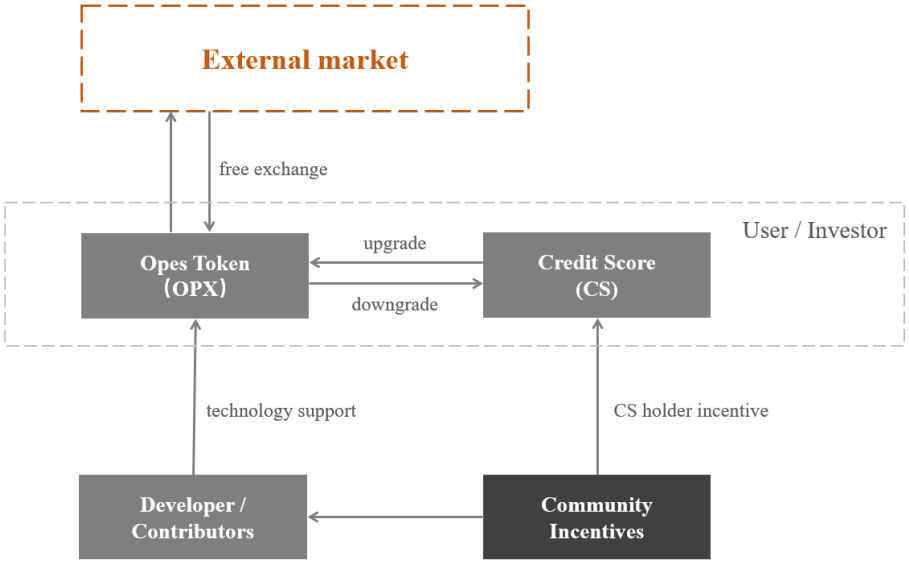
8.1. OPX 的使用场景及经济激励机制

Token 的用途:

1. 发行各类数字货币资产衍生品及服务的抵押金
2. 投资者可直接参与以 OPX 代币为结算单位的各类数字货币资产衍生品及服务
3. 投资者向资金管理者支付管理佣金及收益奖励
4. 用于购买 OPX 平台的第三方服务业务，比如财务审计、安全审计、法律合规服务等
5. 可购买使用 OPX 量化及相关资产管理工具，例如模型、回调测试等
6. OPX 协议及 SDK 调用手续费

社区激励的 OPX 分配

1. 奖励 OPX 生态中 Credit Score 的持有者
2. 奖励 OPX 生态中 Investment Ability 指数高
3. 奖励 OPX 社区开发者及突出贡献者



8.2. Credit Score 的计算

我们用$f_s(x)$代表 Credit Score

$$f_s(x) = f(x_{act}, x_{tra}, x_{amo}, x_{num}, x_{eva})$$

$$= \lambda_1 x_{act} + \lambda_2 x_{tra} + \lambda_3 x_{amo} + \lambda_4 x_{num} + \lambda_5 x_{eva}$$

x_{act}：用于衡量在整个生态中的行为操作

x_{tra} ：用于衡量在整个生态中的交易次数

x_{amo}：用于衡量在整个生态中的交易总额

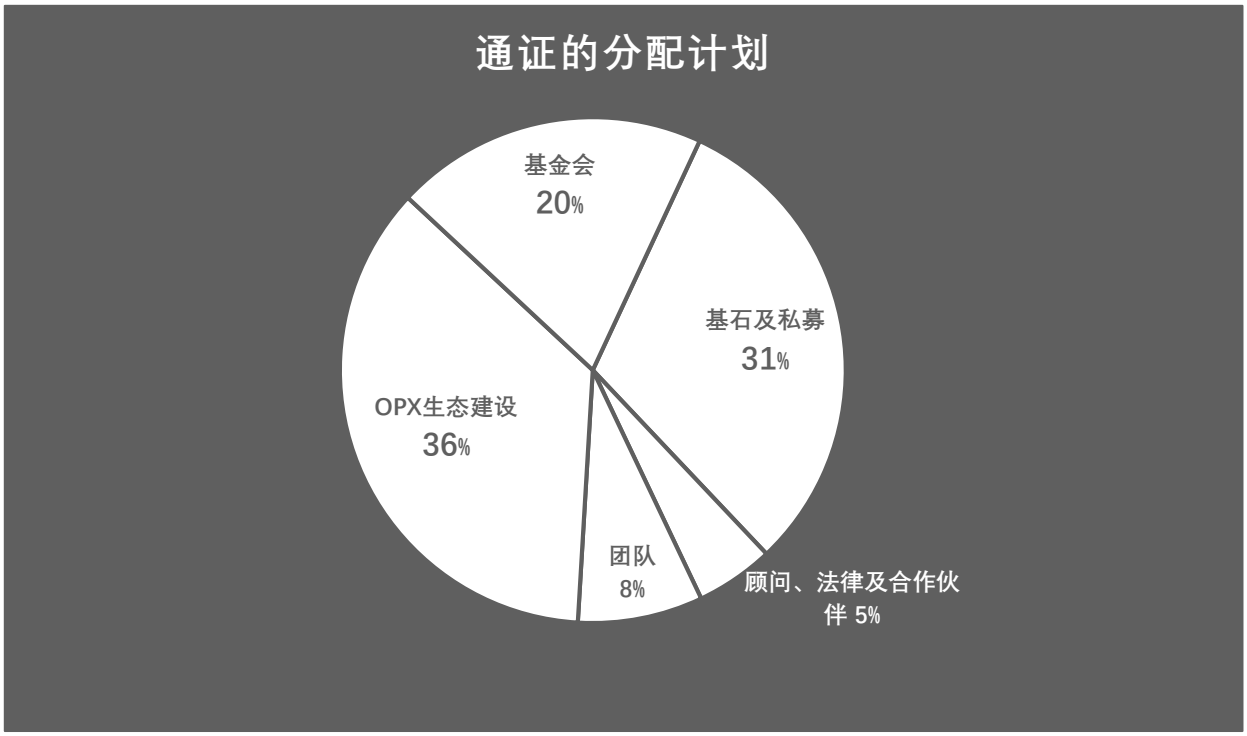
x_{num}：用于衡量在整个生态与其他生态角色互动的频率

x_{eva}：用于衡量来自生态系统中其他角色的评价

λ_1，λ_2，λ_3，λ_4，λ_5 为相关比例因子，会根据生态反馈数据进行调整确定。

8.3. 通证的发行与使用计划

初始分配比例 Opes 创始区块（Genesis Block）会按照计算机时间生成总量 200 亿枚的 OPES，其中：



31%：为基石投资者和社区私募所有，其中 5%为基石投资机构或者个人（锁仓六个月）；26%用于私募轮的众筹（部分直接发放部分锁仓）。所获募资用于 OPX 团队的早期运营、社区创始开展、团队协议层开发、团队应用开发，还包括市场、虚拟资产业务等；

5%： 为顾问、法律及合作伙伴。OPX 作为金融资管项目，金融顾问和法律类专家是不可或缺的力量，也将为区块链资产进行标准化的设计和指导；

8%：用于回报创始团队以及开发团队在发展过程中做出的持续贡献（锁仓三年）；

36%：用于 OPX 生态建设，对产品运营及社区建设的工作，金融数字资产生态的激励，帮助金融数字资产生态的形成。数字金融及资产管理关联 DApp 应用的激励，包括优质策略提供者、开发者和行业领导者（企业高管、董事、大学教授、前沿极客等）作为重点开拓目标和商业场景的拓展开发及资助，来帮助 Opes Protocol 的 DApp 迅速占领市场获得先机。目标：回馈 OPX 资产管理社区，创造有效的流动性；方式：相关渠道空投、开发者激励、社区运营激励和生态建设激励。

20%：OPX 基金会，区块链开发及场景应用深度合作，包含支持基金会运营、商业生态建设、前沿研究、虚拟资产研究的交叉持币。

IX. 路线图

2017-Q1Q2	（Done）区块链技术在金融场景的基础设施原则研究 （Done）资产管理行业分析
2017-Q3	（Done）金融合规分析 （Done）投资人场景研究和产品规划
2017-Q4	（Done）协议层框架设计 （Done）虚拟货币市场行为研究和分析
2018-Q1	（Done）市场调研及数据获取 （Done）金融合规设计 （Done）区块链解决资产管理问题的概念验证
2018-Q2	（Done）数字资产在金融体系中的合规验证 （Done）金融合规设计 （Done）白皮书准备 （Done）产品概念验证 （Done）白皮书发布
2018-Q3	（Ongoing）项目募资 （Ongoing）合规性设计文本 • DApp 产品设计及开发 • Opes 协议栈部分协议开发
2018-Q4	• Opes 工程文件发布 • 测试网部署 • 基于 Opes 协议的 DApp 应用 Alpha & Beta 版本完成及 UAT 测试 • DApp 上线发布 • Opes 协议开发及部分协议验证
2019-Q1	• Opes 协议开发及部分协议验证 • 基于 Opes 的资产管理平台的产品设计 PRD • 平台产品设计验证 • Opes 协议开发及部分协议验证 • 数字资产管理平台开发
2019-Q2	• 数字资产管理平台开发完成部分功能 • Opes 协议开发及部分协议验证

2019- Q3	• 平台测试网部署 • 数字资产管理平台 Alpha 版本发布及 UAT 测试
2019-Q4	• Opes 协议发布，提供基于区块链技术的资产发行、资产管理、资产托管等功能

X.白皮书声明

重要：请务必完整阅读如下声明：

a) 证书丢失导致的丢失加密数字货币的风险

购买者的加密数字货币在分配给购买者之前很可能关联至一个账号，进入账号的唯一方式就是购买者选择的相关登录凭证，遗失这些凭证将导致加密数字货币的遗失。最好的安全储存登录凭证的方式是购买者将凭证分开到一个或数个地方安全储存，且最好不要储存、暴露在工作的地方。

b) 以太坊核心协议相关的风险

加密数字货币和应用程序基于以太坊的协议开发，因此任何以太坊的核心协议发生的故障，不可预期的功能问题或遭受攻击都有可能导致加密数字货币或应用以难以意料的方式停止工作或功能缺失。此外，以太坊协议中账号的价值也有可能以加密数字货币相同方式或其它方式出现价值上下降。

c) 购买者凭证相关的风险

任何第三方获得购买者的登录凭证或私钥，即有可能直接控制购买者的加密数字货币，为了最小化该项风险，购买者必须保护其电子设备以防未认证的访问请求通过并访问设备内容。

d) 相关的政策风险

区块链数字资产已经成为世界上各个主要国家的监管主要对象，如果监管主体采取或施加影响则导致区块链数字资产的缩水或不稳定。例如政府限制使用或销售加密数字货币（或相关数字资产），整个区块链数字资产市场有可能受到限制、阻碍甚至直接终止区块链应用的发展。

e) 应用缺少关注度的风险

平台应用存在没有被大量个人或组织使用的可能性，这意味着公众没有足够的兴趣去开发和发展这些相关分布式应用，这样一种缺少兴趣的现象可能对加密数字货币和应用造成负面影响。

f) 相关应用或产品达不到标准的风险

平台自身或购买者的预期风险应用当前正处于开发阶段，在发布正式版之前可能会进行比较大的改动，任何自身或购买者对应用或加密数字货币的功能或形式(包括参与者的行为)的期望或想象均有可能达不到预期，任何错误地分析，一个设计的改变等均有可能导致这种情况的发生。

g) 漏洞风险或密码学科突飞猛进发展的风险

密码学的飞速发展或者科技的发展诸如量子计算机的发展，或将破解的风险带给加密数字货币和平台，这可能导致加密数字货币的丢失。

h) 加密数字货币挖矿攻击的风险

就如其它去中心化密码学的加密数字货币一样，用于应用的区块链也容易受到挖矿攻击，例如双花攻击，高算力的比例攻击，“自利”挖矿攻击，过度竞争攻击，任何成功的攻击对应用加密数字货币来说都是一种风险，尽管行业内非常努力地提升系统的安全性，但以上所述的攻击风险是真实存在的。

i) 缺少维护或使用的风险

加密数字货币不应该被当作一种投资，虽然加密数字货币在一定的时间后可能会有一定的价值，但如果缺少维护或使用的话，这种价值可能非常小。如果这种情况发生，则可能没有这个平台就没有后续的跟进者或少有跟进者，显然，这对加密数字货币是非常不利的。

j) 应用存在的故障风险

平台可能因各方面的原因故障，无法正常提供服务，严重时可能导致用户加密数字货币的丢失。

k) 无法预料的其它风险

加密数字货币是一种全新且未经测试的技术，除了本白皮书内提及的风险外，还存在着一些团队尚未提及或尚未预料到的风险。此外，其它风险也有可能突然出现，或者以多种已经提及的风险以组合的方式出现。

l) 其他说明

充分了解运营平台的发展规划以及清楚区块链行业的相关风险。

免责声明

该文档只用于传达信息之途，并不构成本项目买卖的相关意见。以上信息或分析不构成投资决策。本文档不构成任何投资建议，投资意向或教唆投资。任何与本白皮书相关的行为均不得视为参与互换，包括要求获取本白皮书的副本或向他人分享白皮书。

Opes 团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括 DApp 开发，合规性文件发布，OPX 平台开发，Opes 协议开发等。

本文档不构成或理解为任何买卖证券的操作建议，也不是任何形式上的合约或者承诺。相关意向用户明确了解本项目的风险，投资者一旦参与投资即表示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。运营团队不承担任何参与本项目造成的直接或间接的损失。

参考文献

[1] https://www-935.ibm.com/services/cn/gbs/ibv/pdf/Unblocking_the_blockchain.pdf

[2] Baker, Jessi."Trust in the Digital Age."Provenance News.October 13, 2016. https://www.provenance.org/news/movement/trus t-digital-age/

[3] 我们把互联网的发展定义为三种：信息互联网即解决信息互通互联的根本问题及基础建设，数据互联网即信息化数据的有效关联，价值互联网即数据的 P2P 可信任及区块链化的数据组织再造

[4] http://www.the-blockchain.com/docs/JP-Morgan-Juno-Distributed-Cryptoledger.pdf

[5] http://www.coindesk.com/jpmorgan-juno-hyperledger-blockchain/

[6] S. Shalunov, G. Hazel, J. Iyengar, and M. Kuehlewind.
Low extra delay background transport (ledbat). draft-ietf-ledbat-congestion-04. txt, 2010.

[7] Franlin Allen，Risto Karjalainen. Using genetic algorithms to find technical trading rules[J] Journal of Financial Economics, 51(1999): 245-271

[8] Tak-Chung Fu，chi-pang chung，Fu-lai Chung.Adopting genetic algorithms for technical analysis and portfolio management[J].Computers and Mathematics with Applications,66(2013):1743-1757.

[9] J.Chen Essentials of Technical Analysis for Financial Markets[J].Wiley,2010

[10] Gorgulho,Neves,Horta N.Using Gas to Balance Technical Indicators on Stock Picking for Financial Portfolio Composition in Proceedings of the GECCO. Montreal[J].Canada,2009;2041-2046

[Other]

- Bitcoin: A peer to peer electronic cash system" at https://bitcoin.org/bitcoin.pdf
- "A protocol for interledger payments" at https://interlegder.org/interledger.pdf
- "Ripple – key feature" at https://ripple.com/technology
- B. Cohen. Incentives build robustness in bittorrent. In Workshop on Economics of Peer-to-Peer systems, volume 6, pages 68{72, 2003.
- 丁鹏 量化投资=策略与技术[M] 北京：电子工业出版社，2012