InvestDigital

白皮书

数字货币一站式投资服务平台

目录

摘要

全球加密数字货币市值不断增长，市场对加密数字货币资产投资需求旺盛，传统金融领域的专业投资人（如基金经理、量化交易员等）开始进入这一领域。为了建立普通投资者与数字资产管理人之间的连接,并解决普通投资者对资产管理服务的信任问题，我们提出了 InvestDigital——数字货币一站式投资服务平台。

InvestDigital 致力于建设数字货币投资的完整生态,为目前处于无序状态的数字货币市场搭建金融服务基础设施。InvestDigital 将为加密数字资产管理人提供一站式解决方案，帮助他们方便地创建和安全地管理加密数字货币基金。通过 InvestDigital,普通投资人可以选择符合自己风险偏好与收益预期的基金产品完成一键直投。InvestDigital 生态还引入工具提供者与数据提供者，为算法交易员提供适用于数字货币市场的量化工具与数据服务，帮助他们更好地制定投资策略。

白皮书阐述了 InvestDigital 的市场需求、产品与服务、商业模式、技术路线以及代币机制。

第一章　加密数字货币投资

1.1 加密数字货币发展迅猛

随着区块链技术的飞速发展，以比特币为代表的加密数字货币在市值、交易量上迎来了井喷。目前，全球加密数字货币整体市值已经突破 3000 亿美元，单日交易量在 2017 年 11 月 12 日迎来了历史峰值——260 亿美元。华尔街传奇投资经理 Michael Novogratz 预测，全球加密数字货币市值将在五年内达到 5 万亿美元。加密数字货币正在越来越多的被传统投资行业关注。日前，芝加哥商品交易所（CME）和芝加哥期权交易所（CBOE）宣布计划于 2017 年第四季度推出比特币期货。随后，纳斯达克交易所亦宣布计划于 2018 年推出基于比特币的期货合约。

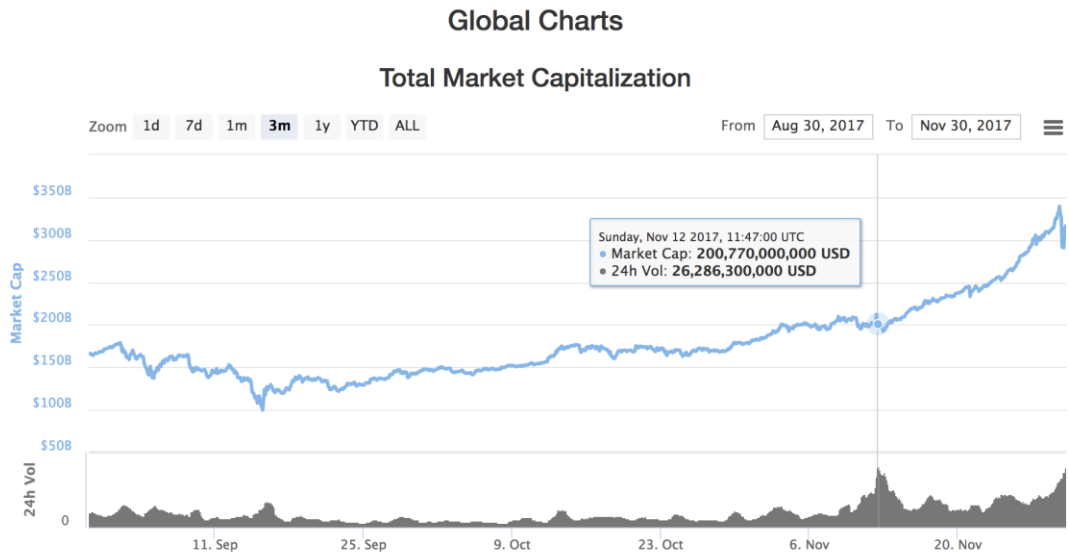

图 1.1 全球数字货币发展趋势

1.2 加密数字货币投资市场及趋势

目前加密数字货币投资刚刚兴起，散户投资者占据了大部分比例，随着其进

一步发展成熟，越来越多的专业投资者参与其中。类比成熟市场，专业投资者是市场的主体，普通投资者更倾向于把资金交给专业的基金管理者进行投资。以美国股票市场为例，根据 2016 年的数据，在资金规模上，股市整体规模接近 25.2 万亿美元，股票型基金的基金规模约为 9.8 万亿美元，基金市值占比达 38.9%，在成交额上，机构占比更是超过 70%。据此推算，加密数字货币投资市场走向成熟后，数字货币基金规模将超过 1 万亿美元。有理由相信，随着全球加密数字货币投资市场各类衍生品和量化工具的日益丰富，专业投资者将成为加密数字货币投资市场的主导。

1.3 加密数字货币投资市场需求

加密数字货币属于新生事物、投资专业性强，加密数字货币投资正处于从初级逐步走向成熟的过渡发展阶段。在这一阶段，普通投资者和专业投资者在加密数字货币投资市场都受到了多个方面的制约。

对于普通投资者，缺乏加密数字货币投资的知识和技能，急需专业资管服务。一是知识匮乏，加密数字货币种类繁多，投资者不仅要了解其基本原理，还要掌握钱包管理、交易所开户、处理交易等繁琐操作，导致大量的潜在投资者望而却步；二是投资技能不足，不掌握程序化交易工具难以应付 7x24 小时交易，不掌握期货合约等衍生品工具难以对冲高波动风险；三是数字货币资产管理服务和社区尚未发展，普通投资者没有可靠途径发现专业的数字货币资管服务，很难对数字货币市场、金融投资知识、自身风险承受能力三个方面都有清晰认知，因此寻求资产管理机构的专业服务也是个人投资者的现实需求。

对于专业投资者，缺乏连接普通投资者的渠道、量化工具，并且难以取得投

资者信任。一是缺乏渠道，难以建立与普通投资者之间的链接，许多优秀的投资策略难以募集足够资金；二是缺乏针对加密数字货币投资的策略编写、回测与实盘交易工具，传统算法交易员难以进入数字货币这一新兴市场；三是缺乏市场监管，基金真实业绩表现、资金账户安全托管等难以自证清白，无法与普通投资者之间建立信任。

因此，加密数字货币投资市场需要一个满足普通投资者和专业投资者需求的一站式服务平台，帮助广大参与者快速发现并实现数字货币投资价值。

1.4 InvestDigital 的使命

作为全球加密数字货币智能投资生态的建设者，InvestDigital 致力于打造数字货币一站式投资服务平台，是实现在 EOS 区块链上的数字资产管理协议和工具集，为目前正在飞速扩容的数字货币市场提供当下最需要的基础金融服务，打造从内容/工具（投资讨论），到投资策略（投资组合），再到金融产品（各类基金）的完整生态，使其成为一个更有效的市场，助力把有限的金融资源最有效地分配到能产生最大效益的投资中，从而提升整个生态的公共福利。

第二章　InvestDigital 产品和应用

2.1 量化投资开发者工具

InvestDigital 提供丰富的策略开发工具和回测环境，开发者可以基于 InvestDigital 开发不同投资风格、不同风险偏好、不同收益预期的数字货币交易策略，诸如单一品种的数字货币投资、对冲、套期，多个数字货币品种的投资组合（如 ETF），数字货币合约、期货等，并利用交易所数据进行回测，在可信环境下模拟实盘验证，提高量化策略的有效性，丰富数字货币量化投资生态。

2.2 数字货币投资交流社区

InvestDigital 提供一个基于用户间 follow 关系的投资交流社区，能满足投资者对投资资讯的个性化需求，帮助投资者发现有价值的交易策略和资管产品，帮助投资者消除信息死角和思维盲区，降低投资决策时的不确定性。

投资交流社区能产生有效的内容和社交关系，社交关系进一步促进交易；同时，社交关系会产生信用，信用可以应用在金融交易上，进一步保证交易的可靠性。用户在 InvestDigital 浏览每个投资产品的页面，都可以看到投资者围绕它产生的海量内容，这些内容能够把投资产品的收益、风险等特征提炼出来；用户在 InvestDigital 浏览每个投资者的页面，都可以看到他关注哪些基金，交易风格是怎样的。如果投资产品的特征和投资者的偏好能够匹配，则交易有可能撮合成功。

2.3 数字货币基金发行工具

优秀的算法交易员和资产管理人可利用 InvestDigital 申请发行基金和资管产

品，为用户数字资产保值增值，同时收取服务佣金。InvestDigital 提供一系列的智能合约，完成基金的自动化发行，这能够大大缩短基金成立所需时间，降低基金成立和运行所需成本。基金发行和管理智能合约提供产品定价、交易规则、交易所信息、交易执行、链下数据访问、投资组合相关数据等的储存，以及管理费设置和分红计算等。

2.4 数字货币基金加速服务

InvestDigital 为规模较小的基金（如低于 1000 万美金的基金）提供业绩展示服务，帮助他们在平台上获得资金，找到潜在资源。当基金规模发展到 1000 万美金之后，单纯一个一个去拉客户非常困难，InvestDigital 将筛选能力强、回报多样性高、市场相关度小的基金进行更深度的推广。InvestDigital 将举行基金大赛，对报名参赛基金的业绩进行一段时间的观察。观察期后，InvestDigital 会和合作方对初选出来的基金进行尽调，与基金经理进行交谈，给出最后结果。对基金的支持包括但不限于：进行持续的线上线下媒体宣传、品牌推广；根据惯例规模、策略数量、策略容量等因素综合考虑，给予资金支持；纳入代销观察池，酌情降低机构代销费用等。

2.5 数字货币基金市场

InvestDigital 提供一个数字货币基金市场，为平台上优秀的基金提供产品展示和销售服务，让投资者可以看到更多基金的竞争性和优秀表现，从而在更大范围内选择投资标的。同时，InvestDigital 也为其它平台外基金提供展示和代销服务。

InvestDigital 也是数字货币基金投资入口，投资者根据自身投资需求进行匹配

并参与投资，获得以智能合约形式生成的收益权凭证。产品运营期间，数字货币量化产品在 InvestDigital 智能交易系统中自动完成交易，并在交易过程中根据市场变化动态调整策略交易参数，实现资产增值的目的，待产品到期后投资者自动获得投资收益。

2.6 多样化数字货币投资产品

InvestDigital 将致力于提供或开发丰富的智能数字货币投资组合，加快数字货币成为传统金融机构、Fintech 公司、高净值投资者资产配置的重要选项的进程，成为数字货币投资浪潮的推动者。

2.6.1 数字货币 ETF

针对被动型投资者和配置型投资者资产配置的需求，InvestDigital 及其开发者生态将致力于制作数字货币指数（Index），跟踪多支数字货币的市场表现，并开发丰富的数字货币 ETF 产品，诸如数字货币 A50 基金、数字货币稳健型基金等，填补数字货币市场基金产品空缺。

2.6.2 数字货币 FOF

为了降低资产配置风险和主动管理风险，进而降低投资门槛，InvestDigital 及其开发者生态将致力构建 FOF 的投资组合。通过对基金净值、持仓进行科学的业绩归因，筛选合适的子基金，并开发配置方案和投资策略形成 FOF 产品。运营过程中通过持续监控，确保当前的母基金的持仓和对冲配置的方案不发生大的偏移，从而保证母基金的整体风险的稳定性。

第三章　InvestDigital 概览

3.1 业务模型

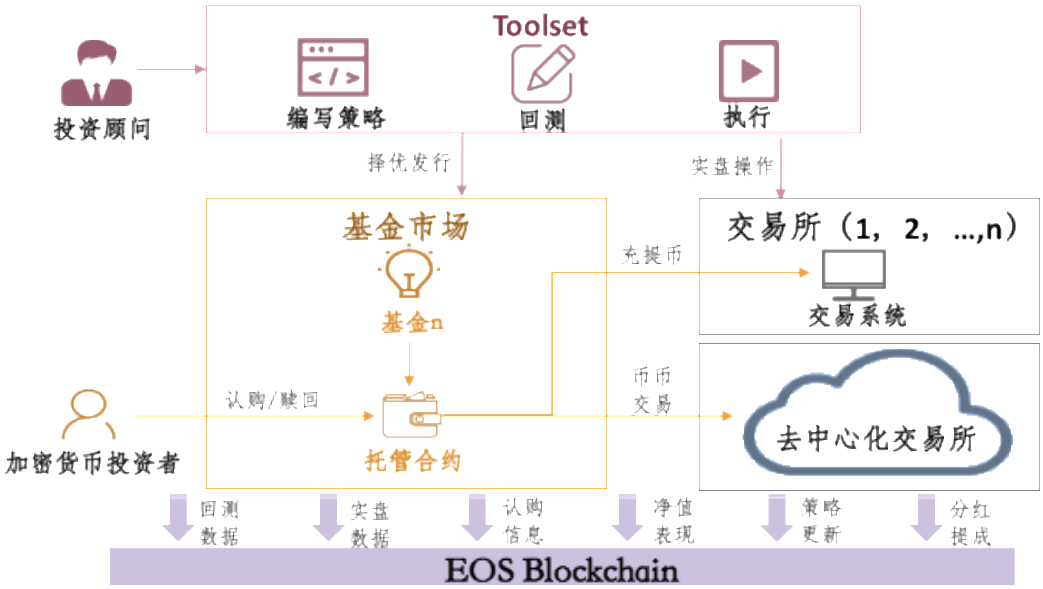

图 3.1 InvestDigital 业务模型

InvestDigital 提供数字货币基金的完整生命周期服务。算法交易员通过工具集编写、回测、实盘执行自己的投资策略。InvestDigital 会基于策略的实盘业绩甄选出表现优异的策略，形成基金产品发行到基金市场上，同时对有潜力的策略提供基金加速服务，保证优秀的策略可以得到充分的推广，帮助他们获得充裕的资金。InvestDigital 基金市场将以基金的净值表现，最大回撤等技术指标为基础，提供基金排行榜，对加密数字货币有兴趣的投资者可选择适合自己风险偏好与收益预期的基金产品进行投资。

整个过程中，策略的回测结果、实盘数据、净值信息等都将通过 EOS 预言机记录到区块链上，保证数据的真实有效，不可篡改，使投资者免受欺诈；算法交易员对策略的更新与修改也将写入区块链，防止恶意操作；同时，基金的申购，

赎回与分红都将通过经过形式化验证的智能合约去执行，保证资金的安全与投资的公平；最后，交易员的历史业绩数据，交易员与投资者的评价也将记录在区块链上，从多方约束的角度促进生态的发展。

3.2 InvestDigital 代币

InvestDigital 将发行统一代币——IDT（InvestDigital Token）以激励并维护生态健康发展，通过 IDT 使社区多个参与方之间形成有机的流转。IDT 是 InvestDigital 生态系统的本地货币，基于以太坊 ERC20 代币标准，待 EOS 主网上线后，将 IDT 代币转换到 EOS 上。其使用场景如下：

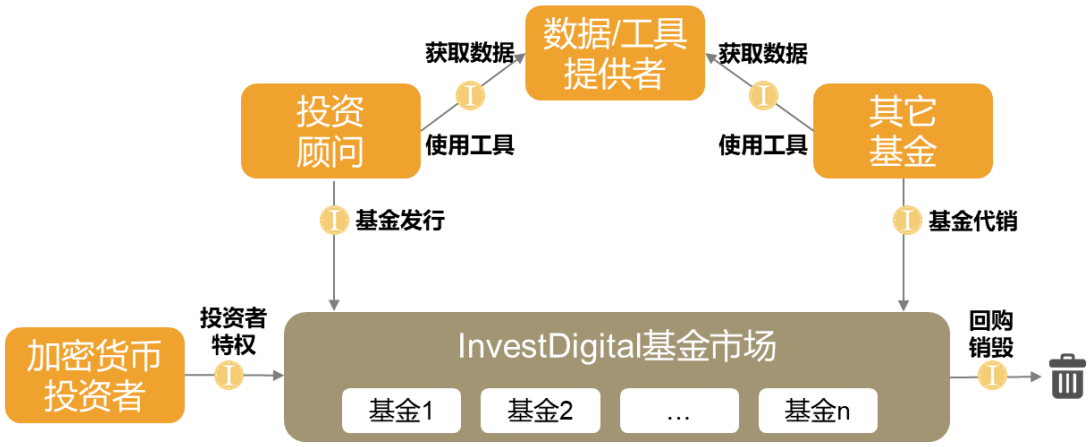

图 3.2 InvestDigital 代币流转

1. 算法交易员：使用 InvestDigital 的相关数据服务和工具集将消耗 IDT 代币；在 InvestDigital Marketplace 上发布基金，将消耗 IDT 代币；参与社区管理、展示和推广自己的策略以及创建私密群聊将消耗 IDT 代币；
2. 数字货币投资者：投资者可使用 IDT 代币获得 InvestDigital Marketplace 上的投资者特权，如产品推荐，投资研报，专线服务等；
3. 数据服务和工具提供者：InvestDigital 社区的数据提供者、工具集提供

者和智能合约形式化验证提供者将获得 IDT 代币奖励，以鼓励他们提供高质量的服务；

4. 数字货币基金管理者：数字货币基金通过 InvestDigital Marketplace 进行业绩展示和销售将消耗 IDT 代币奖励；

5. 回购和销毁策略：InvestDigital 团队将每季度拿出季度利润的 20%用以 IDT 的回购，并进行销毁，直到 IDT 的总量减少到一半为止，保证 IDT 流通量减少，相对价值提升。整个回购销毁过程将记载到区块链上，保证过程的公开透明。

第四章　技术架构

4.1 技术架构

InvestDigital 构建在 EOS 区块链基础设施之上，主要包括 Oracle Machine Data Feeder、InvestDigital Core、InvestDigital Auditor、InvestDigital Marketplace 和 Toolset。

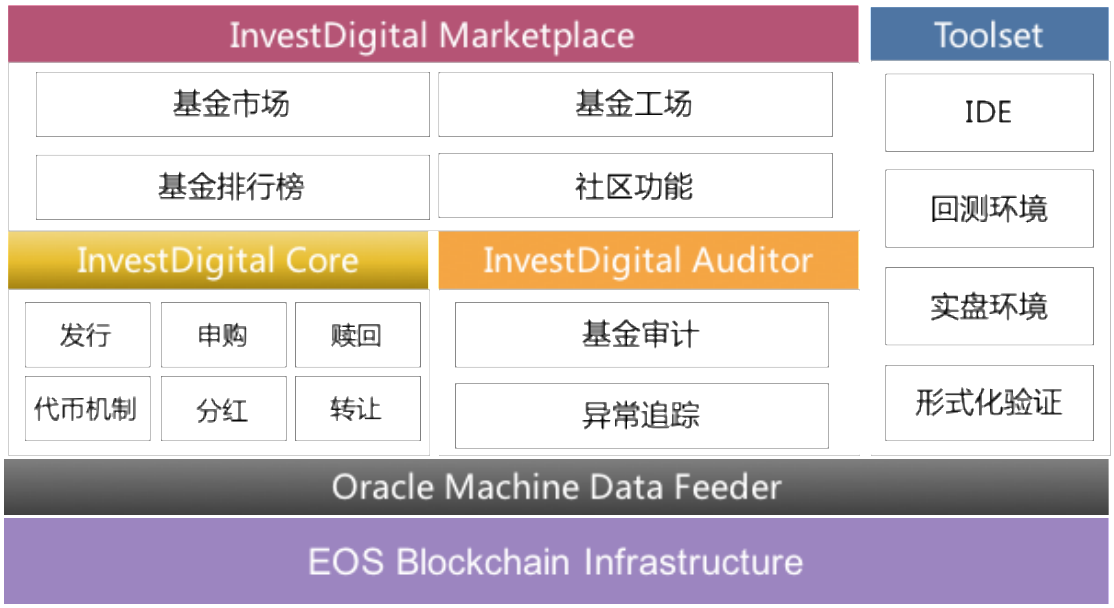

图 4.1 InvestDigital 技术架构

4.2 Oracle Machine Data Feeder

Oracle Machine Data Feeder 是一个可靠的数据获取服务。它通过建立多形态预言机，算法交易员可以获取交易所公开数据、去中心化的预测市场数据、加密数据等。这些数据能够帮助算法交易员优化投资组合和投资策略；数据提供者也可以获得经济奖励（代币）和内部评级提升，激励其不断提供高质量的数据。

4.3 InvestDigital Core

InvestDigital Core 提供基于智能合约的数字货币基金产品认购、份额转让、赎回、分红等服务，以及交易员的管理费计算等功能。

4.3.1 基金发行

InvestDigital 将允许实盘业绩良好，无不良信用记录的交易员在基金市场上发行自己的基金。

针对中心化交易所：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。

针对去中心化交易所：随着去中心化交易技术的不断完善，利用去中心化交易所低延迟，低费率的特点，InvestDigital 也将支持基于去中心化交易所的基金产品。整个投资与分红过程利用跨链原子交换技术，通过一组智能合约在去中心化交易网络自动执行。

4.3.2 申购

针对开放式基金，股份总额不固定，投资者们可以根据自身情况随时进行申购操作。我们通过对份额的生成来对应申购。每个投资者在给定基金的份额占比可以用下面公式表示：

$$\text{Proportion} = \frac{\text{Holding Shares}}{\text{Total Shares}}$$

基金 m 在 t_i 时刻的股价$p_m^{t_i}$以基金中给定的投资货币为单位(如 BTC，EOS 等)，

由基金 m 所包含的投资组合中的虚拟资产在当前时刻的价格向量$\begin{pmatrix} p_{a_1}^{t_i} \\ \vdots \\ p_{a_n}^{t_i} \end{pmatrix}$所决定，$p_{a_k}^{t_i}$表示数字货币$a_k$在 t_i 时刻针对基金给定投资货币的价格。当投资者在基金 m 中投入 N 个给定投资货币时，InvestDigital 将为该用户生成 $Q=\frac{N}{p_m^{t_i}}$个份额。

InvestDigital 支持投资者基于多种主流数字货币一键直投。InvestDigital 原创基于公平交换协议的跨链原子交换技术,保证互不信任的多个主体之间按约定规则完成不同区块链系统之间的资产互换，保证基金申购便捷。

4.3.3 赎回

我们通过销毁投资者的份额实现赎回操作，投资者申请赎回时，将获得 $N=Q*p_m^{t_i}$个投资货币，由于股价（数字货币价格）$p_m^{t_i}$是动态变化的，所以投资者赎回获得的 N 也将是变化的。同时，InvestDigital 会将该投资人之前所持有的 Q 个份额销毁（更新赎回后的基金份额），保证市场的动态平衡。基金 m 在某一时刻的净值$V_m^{t_i}$可通过用如下公式进行计算：$V_m^{t_i}=\sum_{k=1}^{n} p_{a_k}^{t_i} h_{a_k}^{t_i}$,其中，$h_{a_k}^{t_i}$表示该基金在 t_i 时刻持有的数字资产a_k的数量。

策略执行过程中，交易员可根据外部环境的情况动态对策略进行调整与更新，同时通过 EOS 预言机服务记录到 EOS 区块链上，并定期对外公示净值等指标，保证基金股价的正确。

4.3.4 分红

InvestDigital 将通过智能合约去执行基金分红，以通过 EOS 预言机提供的可信基金净值和投资者份额为输入,自动将收益分配到各个投资者。对于投资经理，

将会获得管理费和业绩提成，管理费由所管理的资金规模决定；业绩提成将由所管理的基金业绩决定。提成的计算方法一般有以下两种模式：1.高水位提成法：只有在基金的表现不低于基金成立时给定的基准时，投资经理才可以获得提成；2.阶梯提成法：可以将基金的表现划定区间，根据不同区间，投资经理可以获得不同比例的提成。除此之外，InvestDigital 也支持由投资经理和投资者约定的分成方式。

4.3.5 份额转让

针对封闭式基金，一旦达到限定总额，将对投资者关闭，投资者们无法进行申购与赎回操作，为了提供便利，InvestDigital 内部将提供份额转让功能，提供一个 C2C 的平台，让投资者之间可完成基金份额与数字货币的交易。

4.3.6 代币机制

在 InvestDigital 中，IDT 代币作为平台内流转的本地货币，是保障整个模式持续运转的基础，同时也是社区治理内的一个重要凭证。通过支付 IDT，数字货币投资者，量化交易员，基金经理可以获取 InvestDigital 内一系列功能模块的使用权；社区内部将根据 IDT 的持有情况，分配各种提议的决策权。同时，IDT 作为一种经济学激励的货币，将不断激励数据提供者与工具提供者提供更优质的服务。

4.4 InvestDigital Marketplace

InvestDigital Marketplace 是 InvestDigital 生态的门户，提供策略/基金排行榜、基金工场、基金市场和投资社区等多类服务。

4.4.1 策略/基金排行榜

InvestDigital 对发布的策略/基金业绩表现提供多个维度的排行榜功能，支持按照策略/基金各项评价指标（包括绝对收益、最大回撤、夏普比率等），展示策略/基金的业绩。帮助不同需求的投资者，快速发现最适合自己的基金。同时利用区块链技术透明不可篡改的特性，保护优秀交易员的利益，使得好的策略，好的投资技巧能够公平公正地展示给大众。

4.4.2 基金工场

InvestDigital 联合多家投资机构发掘具有成长潜力和投资价值的投资经理和基金（策略），对有潜力的、优质的基金（策略）给予多维度支持，包括但不限于：进行持续的线上线下媒体宣传、品牌推广；根据惯例规模、策略数量、策略容量等因素综合考量，给予资金支持；纳入代销观察池，酌情降低机构代销尽调要求；优质基金需要的其它支持等。

4.4.3 基金市场

通过 InvestDigital 基金市场，建立了投资者与基金之间的无障碍链接。基金市场提供不同种类，不同组合的基金产品，投资者可以一键直投心仪的基金，而 InvestDigital 强大的技术体系与安全的智能合约则充分地保障了投资者的利益不会受到侵害。投资经理通过基金市场实现了“用业绩说话”,快速获客。InvestDIgital 先进的评价与仲裁体系也免去了很多不必要的麻烦，即使出现争端，也可以做到公平快速的解决。InvestDigital 基金市场优秀的交易员们发行自己的基金，同时也欢迎其他基金机构展示、销售自己的基金产品。我们致力于打造一个真正意义

上的安全互信多元化的数字货币投资平台。

4.4.4 投资社区

InvestDigital 旨在提供数字货币投资的完整生态，因此在发展过程中，也将不断滋生对数字货币投资的讨论需求，为了使用户投资者可以找到一个公平开放、质量优良的信息互通载体，使投资经理与工具/数据提供者能快速了解到市场需求与用户反馈，InvestDigital 将提供一个基于用户间 Follow 关系的讨论社区。同时，针对 InvestDigital 产品的讨论，将通过标签的方式自动与相关产品进行关联：用户在浏览社区时，可通过内容进入产品详情页面；内容在浏览产品时，也可查看到社区内的相关讨论。

目前的数字货币投资市场，消息会在很大程度上左右投资者的投资思维。由于投资类社区的特异性，投资者往往无法立即判断接收信息的价值，而需要结合市场后续走势作出准确判断，单纯的通过流量（阅读量，点赞数，评论数，转发数等）去判断内容的价值往往是不可信的。然而，在投资类社区内，往往存在着大 V 喊单，并雇佣网络水军干扰投资者判断的情况，不仅造成了内容污染，更会侵害到投资者与其他投资经理的利益。InvestDigital 将利用基于可验证洗牌和关联环签名的匿名声誉机制去构建内容评价体系与信用评分体系，对社区内的用户的长期关联身份进行信用评分，在匿名评价的前提下防止了恶意差评与刷量好评，将此类现象的影响降低到最低。

除此之外，用户可通过 InvestDigital 社区创建私密群聊，保护用户在安全隐秘的环境下，对项目前景以及投资策略进行讨论与分享。

4.5 InvestDigital Auditor

4.5.1 基金审计

由于目前针对数字货币投资的监管还不完善，为保证投资者的权益，InvestDigital 将提供基金审计服务，对异常交易情况进行及时发现和告警。审计服务包括事前审计与定期审计。

事前审计：对于通过平台发行基金的投资经理， InvestDigital 将对其进行完善的尽职调查，在背景、市场风险、管理风险、技术风险和资金风险等方面做全面深入的审核，同时会结合投资经理的历史业绩与评价形成完整的尽调报告；对于通过 InvestDigital 销售基金的其他基金，InvestDigital 将对其真实性、正确性、合规性、合法性进行审查和监督。

定期审计：在基金运作过程中，InvestDigital 将定期对基金进行审计。审计内容包括内部情况与外部情况。内部情况审计主要基于基金的表现情况；外部情况审计主要将对基金经理所处的外部环境进行调查，同时对基金经理与投资者进行回访。

4.5.2 异常追踪

虽然基于形式化验证的智能合约能从根本上保证投资与分红过程的公平性，但却无法在根本上对一些不法行为做出约束：比如投资经理在基金申购过程中通过抬高数字资产价格恶意拉升基金股价误导投资者；或者在数字货币交易过程中存在买卖老鼠仓行为。InvestDigital 将追踪到这些行为，并及时处理，保证投资者权益不受侵害。

4.6 InvestDigital Toolset

Toolset 是支持 InvestDigital 的一系列工具，包括策略开发与回测框架、实盘交易工具和形式化验证服务。

4.6.1 策略开发与回测框架

策略开发与回测框架是提供给量化开发者的策略编写与回测工具集。开发者无需在本地搭建任何环境，即可通过 Web IDE 完成策略的编写与编译。InvestDigital 将同时提供一系列的策略模版与范例算法，大大减少开发者的工作量。InvestDigital 后续也将提供 IFTTT（If This Then That）的友好操作界面，比如，如果低于 15 日均线就卖出，帮助不懂代码的用户也能轻松编写量化策略，真正意义上实现技术与业务的解耦。

对于编写好的策略，InvestDigital 将提供交易所历史数据用于回测，可根据选择的日期区间，形成包括回测收益、回测年化收益、最大回撤、Alpha、Beta、夏普比率等指标的回测结果。支持生成收益曲线，支持同一图表内与基准收益、其他策略收益直观对比。回测结果也支持从交易详情、持仓情况等多重维度进行拆分，帮助量化交易者不断完善自己的策略算法。

4.6.2 实盘交易工具

由于滑点、幸存者偏差等客观因素，以及编写时使用未来函数等主观因素的制约，回测结果只能用于参考，不能反映基金在实盘环境下的交易业绩。同时，对于有意向发行基金的投资经理，通过“晒单”的方式并不能令人信服，也需要一个提供可信结果的业绩展示渠道。InvestDigital 充分考虑到上述需求，将连通

多个交易所的接口，让交易员在实盘环境下既可以执行算法策略，又可以完成人工下单交易，交易结果基于 EOS 预言机服务提供可信的业绩展示。

4.6.3 形式化验证服务

The DAO 事件给我们的最大启示是要特别重视智能合约的安全性。在 InvestDigital 生态中，由于基金申购、赎回、分红等直接关系到资金和资产操作都通过智能合约自动执行，因此智能合约的安全性是整个体系的立足之本。InvestDigital 将使用形式化验证技术去检测和避免智能合约可能存在的漏洞。我们将利用模型检测和定理证明等形式化验证技术手段，保证 InvestDigital 智能合约代码的正确性和安全性，最大程度上减少智能合约遭受攻击的可能性，保障投资人的资金安全。

第五章　技术创新之处

5.1 首个基于 EOS 区块链的智能投资协议

InvestDigital 是区块链技术和数字资产管理的结合，也是首个基于 EOS 区块链的加密数字货币智能投资协议。EOS 区块链平台是基于经过普遍证实、并通过长期实践考验的概念来设计的，代表着区块链技术的根本性进步。借助于 EOS 的高吞吐率和高效预言机等优良特性，可以为 InvestDigital 提供智能合约高处理能力和低延迟的数据服务。基于 EOS，InvestDigital 未来可支持百万级别用户、轻松 Bug 恢复和升级、以及良好的可扩展性。

5.2 首个 EOS 预言机服务的可信资产管理

InvestDigital 致力于打造可信资管平台，也成为了 EOS 预言机服务的首个真实落地场景。InvestDigital 通过 EOS 预言机机制实现链外业务流程和链内智能合约的结合，即链内链外数据的互通。通过把实盘数据、基金净值、历史交易数据等链外金融系统里的信息引入 EOS 区块链系统，实现资产管理数据的真实性和不可篡改。保证交易记录和结果可溯源，策略人工干预过程透明，一旦发生违规行为可追溯。

InvestDigital 的数据服务基于 EOS Oracle 预言机完成数据的采集、取信和共享，主要包括公开数据、预测市场数据和隐私数据这三大类数据。

公开数据：主要通过 Oracle 预言机的 data feeder 经过社区的投票等一系列过程把链外数据（如交易所数据等）导入链内；

预测市场数据：金融市场本身就是对未来的预测，目前主要的市场分析与

预测未来金融方面的关系是由少数使用大致相同信息的专业人士所创造的，我们相信更多人参与的预测市场会带来更为丰富的信息和更强大的群体智能。我们将通过建立去中心化的预测市场来获得高质量的数据集，帮助分析师、交易员和基金经理在这些数据基础上编写投资策略。

私密数据：我们充分理解分析师和交易员对 InvestDigital 平台的潜在的不信任，不愿意与策略相关的私密数据分享到平台上。我们将通过多方计算技术建立一个强制隐私保护的数据分享平台，使投资人可以观察策略的回测输出（资金账户的净值，最大回撤等）技术指标，而隐藏了策略本身细节。

针对以上三类数据，可以借由 EOS Oracle 预言机提供多种形态的预言机服务来实现，比如完全借由链上数据实现数据服务的链上预言机、信任某个链外数据源提供服务的中心化预言机、由区块链上各参与主体共同提供服务的去中心化预言机和综合以上多种形态的混合预言机等等。

5.3 首个采用形式化验证技术的投资平台

The DAO 智能合约遭遇攻击，以及最近的 Parity 多签名钱包智能合约遭遇攻击，都表明智能合约安全的重要性。新加坡国立大学和康奈尔大学研究团队对以太坊区块链上的智能合约进行了检测，发现大约 44%的智能合约存在安全风险。

形式化验证（Formal Verification）是使用数学方法来验证一个系统的否满足某种安全性的方法，主要分为模型检测和定理证明。其中模型检查将软件构造为状态机或者有向图等抽象模型，并使用模态/时序逻辑公式等形式化的表达式来描述安全属性，而后对模型进行遍历以验证软件的这些安全属性是否满足；定理证明将待验证问题转化为数学上的定理证明问题来判定程序是否满足特定安全

属性。

InvestDigital 非常重视智能合约的安全，我们建立了一套基于形式化验证技术的智能合约验证理论体系，并提出了自动化验证工具解决方案，主要解决主要确保基金认购、分红智能合约的正确性、安全性和合规性。

5.4 首个支持匿名特性的声誉评价机制

为了解决投资交流社区中恶意差评与刷量好评等问题，维护良好的社区讨论环境，InvestDigital 通过声誉机制实现带有奖励和惩罚的激励。声誉系统的一大优势是基于可验证洗牌和关联环签名技术，可以完成匿名的声誉计算，不泄露用户真实身份，提升用户的参与程度和忠诚度。

声誉系统工作机制由多轮消息的发送和反馈构成。在每轮的开始，服务器维护包含所有客户端的长期数据库身份和各自的加密声誉分数。在每轮中，服务器依次运行基于可验证洗牌协议的调度算法，把声誉列表变成基于一次性假名的匿名排列列表和对应的明文信誉评分。我们采用去中心化的调度协议，服务器和客户端（所有者除外）均不能将一次性假名和长期身份相关联。客户端使用一次性假名匿名发布消息。服务器可以关联这些消息与他们相应的声誉评分，而不会了解到客户端的敏感信息。接下来每个客户端会对其它用户的发布的消息提供反馈（例如投票）。每个投票都采用关联环签名进行签名，使服务器能验证每个客户只投票一次而不透露哪位客户提交了每一票。这个设计使服务器在统计正面和负面投票时不能将投票与长期身份相关联。最后，服务器根据一次性假名的反馈信息更新信誉评分，然后执行“反向调度”，将这些一次性假名及其更新的声誉恢复到原来的长期身份和他们的加密更新的声誉评分。

第六章　InvestDigital 实施及迭代

6.1 发展路线图

InvestDigital最初的设想始于The DAO事件，创始团队成员中的几名信息安全领域专家想要提供一种基于安全的智能合约的数字资产投资方案,并对智能合约的形式化验证进行深入研究。在与多位智能投资领域专家探讨和充分的市场调研后,InvestDigital 团队意识到数字资产的智能投资平台将会成为一个新的需求点，并拥有宽阔的市场前景，于是在2017年初，InvestDigital团队便开始项目规划，并在以太坊上完成关键技术验证。随着EOS的发展与不断成熟，InvestDigital团队意识到具有更好吞吐的EOS平台对于高频、快速交易具有更好的适应性与可扩展性，因此，InvestDigital将基于EOS平台打造数字资产投资和交易生态。

我们预计在2018年Q1开始开发第一个原型系统,主要包括InvestDigital Toolset和InvestDigital Marketplace的Demo版本,并在Q2接入测试网络进行测试。计划2018年Q3、Q4开始支持基于中心化交易所的基金发行、认购等服务，同时不断完善项目细节,准备在EOS主网上线。在去中心化交易所逐渐成熟后,InvestDigital也将接入去中心化的交易所,拓展落地渠道。在整个项目研发过程中,InvestDigital团队会紧密追踪 EOS 项目的开发进度,同步推动项目前进。随着EOS生态的不断完善，InvestDigital将陆续接入基于EOS其他多种应用，提高用户体验，成为EOS生态内首个落地、最专业、最具前瞻性的多元化数字资产智能投资平台。

版本	里程碑时间	代号	实现功能
1	Q1 2018	Armadillo（犰狳）	InvestDigital Marketplace ● 策略排行榜 ● 基金排行榜 InvestDigital Toolset ● 支持Python编写IFTTT类型投资策略，支持客户端回测 InvestDigital Core ● 代币机制 Oracle Machine Data Feeder ● 链外公开数据获取 EOS Blockchain Infrastructure ● 测试网络上线
2	Q3/Q4 2018	Echidna（针鼹）	InvestDigital Marketplace ● IDT代币激励机制 ● 支持在中心化交易所发行基金 ● 支持基金认购 InvestDigital Toolset ● 完善的Web-based IDE和回测环境 InvestDigital Core ● 基于中心化交易所的基金发行、申购、赎回、分红、转让机制 Oracle Machine Data Feeder ● 获取预测市场信息 EOS Blockchain Infrastructure ● 主网上线
3	Q1 2019	Kookaburra（笑翠鸟）	InvestDigital Marketplace ● 举办量化交易大赛 InvestDigital Toolset ● 为算法交易员提供预测市场数据 InvestDigital Core ● 基于去中心化交易所的基金发行、申购、赎回、分红、转让机制 InvestDigital Auditor ● 基金审计 Oracle Machine Data Feeder ● 支持数据隐私
4	Q3 2019	Platypus（鸭嘴兽）	InvestDigital Marketplace ● 支持基金孵化和加速 InvestDigital Toolset ● 支持IDT代币激励的高级数据服务

			InvestDigital Core ● 支持基金发行和管理收取IDT代币 InvestDigital Auditor ● 支持异常跟踪
5	Q4 2019	Quokka（短尾矮袋鼠）	InvestDigital Marketplace ● 发行更丰富的量化投资产品 InvestDigital Toolset ● 为智能合约提供形式化验证工具 InvestDigital Core ● 支持ETF、FOF等多类产品 Oracle Machine Data Feeder ● 去中心化交易所数据获取

6.2 生态圈建设

作为 EOS 平台上第一个数字资产策略市场，本身将为数字资产投资者与投资经理人们提供一个良好的平台，促进数字资产快速多元化的发展，同时 InvestDigital 将致力于打通，丰富、完善上下游应用。InvestDigital 将吸引更多的上游数据提供者，工具开发者们提供优质，及时，可靠的数据与便捷，安全，高效的工具；同时，InvestDigital 的不断发展，也将为数字资产资讯，预测市场，社交，去中心化交易所等应用的落地与完善起到促进作用。同时为了丰富社区生态，InvestDigital 也将不定期举办线上线下的活动，例如比赛、沙龙等，并对比赛优胜者以及对活动提出好的建议的用户，以 IDT 代币形式提供奖励，鼓励社区内每一个用户积极参与到整个项目的管理与运作上。

第七章　团队

7.1 核心团队

项目核心团队由来自于世界顶尖科研机构的计算机技术专家以及知名券商的投资专家组成，具备国际化的跨行业经验。在区块链及其安全、量化交易、资产管理、投资社区运营等领域具备强大的科学研究，工程研发和市场推广能力。

1. Daniele Bernardi，负责 InvestDigital 商业生态的顶层设计和战略。他是一位不断寻求创新的企业家，担任 Diaman SCF 的创办人兼首席执行官，INVESTORS' Magazine Italia 杂志主席。他致力于开发高回报的投资战略，他提出的面向数学模型的定量方法开发等研究成果能减少投资选择中的情感因素影响及其带来的风险，从而改善结果并增加客户满意度，简化投资者和家族企业的决策过程，减少投资风险。他领导的 Diaman SCF 在改变客户金融工具需求和制定动态投资策略方面处于领先地位。

2. Hugo Gong，负责 InvestDigital 产品设计与运营。伦敦大学学院区块链研究中心研究员，中英区块链协会秘书长，伦敦大学学院金融数学博士，研究项目包括联合国食品署数字身份计划、ICO 监管及挑战和用于数字货币基金的套利策略等，研究方向为算法和高频交易，包括交易策略研发和订单执行等，拥有丰富的数字货币金融产品设计经验。

3. Riaz Ahmad，InvestDigital 首席科学家。伦敦大学学院和牛津大学客座教授，应用数学家，国际数量金融工程认证 CQF 的创始人和 CQF Faculty 负责人，研究兴趣包括金融衍生工具的数学和计算方法，特别是随机波动率、跳跃扩散模型、奇异期权和利率模型等。Ahmad 教授拥有伦敦大学学院数学博士学位。

4. 晁辉，负责 InvestDigital 系统架构。资深互联网技术和产品技术管理专家。早年进入北京大学攻读理学博士学位，后离校创业。曾在雪球网担任高级总监，在阿里巴巴支付宝担任资深架构师，拥有十五年大型金融和互联网系统研发和管理经验。

5. 张力，负责 InvestDigital 市场推广与社区建设。方正证券资产管理分公司权益投资经理，北京大学博士，量化交易专家，资深证券投资专家。证券从业经历 8 年，金融信息化研究经历 13 年，拥有丰富资产管理经验和客户资源。

6. 王前锋，负责 InvestDigital 项目投资策略和产品风控。泰康资产高级产品经理，香港中文大学金融工程硕士，智能投顾专家。曾参与沪港深投资产品、MSCI 指数产品、量化策略产品等的开发和发行，著有智能投顾专著《量化大类资产配置》。

7. 唐聪，负责 InvestDigital 区块链和密码学技术架构。北京大学理学博士，纽约大学访问学者。原北信源（300352）产品总监，区块链和分布式账本技术专家，网络和信息安全领域专家。有丰富的区块链架构设计与系统开发落地经验。主持研发供应链金融、产品追溯和医疗健康等多个行业区块链产品和应用。

8. 孟宏伟，负责 InvestDigital 产品架构和协议设计。北京大学理学博士，高级工程师。长期从事大型信息系统顶层设计，拥有大型系统研制和管理经验。未来互联网体系结构专家、密码学和区块链专家，对区块链架构、共识算法、智能合约有深刻理解。

9. 胡成建，负责 InvestDigital 区块链系统开发。高级软件工程师，北京大学工学硕士。开发了基于改进 BFT 共识机制的高速私有区块链（北航链），是国内最早的区块链参与者和开发人员。

10. 刘晗，负责 InvestDigital 智能合约形式化验证。清华大学博士，加州大学戴维斯分校访问学者。主要研究领域为软件缺陷检测及漏洞分析、软件测试等。主持和负责 DATE：Java 程序动态分析及测试平台项目，开发了多个软件安全验证和自动化测试平台，包括 Closure*工具，Tsmart-SiRi 异步嵌入式系统的建模、验证工具，Tsmart-Edola 同步系统集成开发平台。

7.2 顾问团队

1. OracleChain（http://oraclechain.io/）。作为全球第一个在 EOS 生态圈上构筑的应用，OracleChain 将解决该生态的 Oracle（预言机）需求，实现区块链技术服务和现实生活中的多种需求场景直接高效对接。作为一个基于 EOS 的去中心化的 Oracle 技术平台，OracleChain 采用自主的 PoRD 机制，将现实世界数据引入区块链，并将此作为基础设施为其他区块链应用提供服务。OracleChain 的使命是“让世界与区块链互联”，立志打造未来区块链世界中最高效的获取链外数据的服务提供平台。

2. Ennan Zhai，耶鲁大学博士、博士后，耶鲁大学副研究员。主要研究方向为声誉系统和大规模分布式系统，研究重点是利用分布式系统，编程语言和密码学等领域的技术构建安全可靠的计算机系统。目前工作包括使用高效、准确和深入的审计技术来提高大型分布式系统的可靠性和安全性，以及 PriFi：第一个低延迟和抗跟踪的匿名通信系统。他的博士论文工作着重于构建云计算的可靠性审计系统，该系统可以主动检测可能导致云规模相关故障的深层原因和异常依赖关系。

3. 关志，北京大学副研究员，德国曼海姆大学访问学者，主要研究方向为密码学和安全协议，著名国密算法开源项目 GmSSL 的主要开发者和社区领袖，

研发了 Hyperledger Fabric 国密算法套件，培养了多名区块链方向硕士研究生。在椭圆曲线加密算法性能优化与安全增强领域有丰富研究和工程实践经验。

4. 陈宇，中国科学院信息工程研究所信息安全国家重点实验室副研究员、硕士生导师，主持国家自然科学基金两项。入选中国科学院青年创新促进会会员，担任中国密码学会青年工作委员会委员。主要研究方向为公钥密码学、可证明安全理论、基本密码组件等。近年在密码学领域高水平期刊 Design, Codes and Cryptography 等及国际会议 CRYPTO、PKC、SCN 等上发表学术论文多篇。