开源生态白皮书

稳定 | 安全 | 实用 | 快捷

2021 年 1 月

1 概述

MACD 的定义

1.1.1 MACD 是基于区块链技术+文创产业+通证等进行文创产品保真、查询、消费等而开发的应用;通过点对点进行文创作品登记、发行、转让、交易、清算、交割等保真查询及金融业务的去中心化网络协议的区块公链，是一个用区块链技术打造的开源式综合去中心化应用平台。运用区块链、大数据、人工智能、密码学、5G 等融合技术，打造一个安全、合规、高效、专业、自治、稳定、易用、透明的价值交换新体系，通过节点商业的多元化激励机制让所有商业活动的参与节点都能充分发挥其内在价值，推动节点商业的价值最大化。

1.1.2 MACD 是致力于设计和打造基于私域流量的分布式节点商业新联盟。在此基础上 MACD 还将建立一套标准化节点商业评估体系，应用于文创产业的溯源保真查询。

1.1.3 MACD 应用于文创产业的溯源保真查询，构建全球文创产业生态链，所有跟文创产业有关的平台、开发者以及爱好者都可以参与其中，共建价值生态以及节点商业服务体系。生态服务的主题包罗万象，涉及区块链生态的各个环节，从区块链爱好者，个人投资者，咨询服务商，到区块链专家，文创产品创作者等；不仅有区块链项目的创业者们，还有寻求通证化解决方案、实现新增长的传统行业壁垒，价值应用和场景增多，良好的生态环境将是用户体验的根本所在，包括用户如何在其中享受区块链技术带给其生活、工作方面的便利。活跃用户等如何利用好自身影响力去实现个人价值最大化。

为解决当前文创产业发展中存在的突出问题，MACD 将从基础设施公链，价值开放平台，节点识别入口，节点管理平台，节点商业体系等多个维度展开具体研究与实践。

1.2 区块链说明

区块链是一种以密码学技术为基础，以去中心化的方式，对大量数据进行组织和维护的数据库结构，适合用作数字货币或数字资产的账本。区块链上的交易数据全部都附有交易者的数字签名，不可伪造。

此外，区块链还具有完全公开透明、交易可靠、即时交割、无需信任等诸多特性。以区块链技术构建的财务和交易系统相对于传统金融机构和商业体有具备巨大的竞争优势。区块链技术在未来将成为金融网络的主流底层技术，应用于难以公开透明计数的交易领域中。

1.3 应用场景

MACD 专注于数字货币的金额快捷支付，可以被广泛应用于区块链商城、餐饮、酒店、生活缴费和旅游等日常生活新零售交易。

1.3.1 MACD 区块链商城进行时时支付

通过区块链技术框架可以实现功能完善的商城应用。用户可以自由的建立商家界面，出售商品，也可以使用法币或其他 MACD 网络认可的虚拟币种进行消费。所有交易具备自由、公开、可靠、低手续费、可溯源、去信任等优点；同时，用户将享有平台发展所带来的更多收益。

1.3.2MACD 区块链交易餐饮，超市和酒店落地扫码支付

MACD 将首次实现，当我们在餐厅用完餐或者便利店购完物后直接用数字资产进行面对面支付，而且首次让区块链资产达到即时交易，体现数字资产在实体应用中的真实价值，并且不仅仅局限于自主平台用户。用户可以任何互联网的地方下载 MACD 钱包进行跨国界，跨地域即时付款和收款，远程支付等，不需要任何第三方机构确认。

1.3.3MACD 应用于文创产业应用支付

MACD 应用在线上平台及线下拍卖行于文创产品进行拍卖，用户抢拍标的后直接用数字资产进行面对面支付，而且首次让区块链资产达到即时交易，所拍文创产品具有保真查询功能，实现文创产品能够追溯起源。

1.3.4MACD 区块链增值共享价值

MACD 指标首次推出存币付息机制，让更多的前期 MACD 用户享有更多的数字资产增值带来的长期稳健收益，首期只微量发行份额币，复息分发释放子币的增值模式，让更多的爱好者享有量变和价变的双增值发行模式。让区块链的增值更有普惠性。区块链首次采用了小额支付确认模式，防止大资金进入爆炒带来的暴涨暴跌风险，会让 MACD 真正更具备货币流通价值相对稳定的属性，量变保持数字资产增值性，价格相对稳中上涨，保障实体商家结算热情，建立货币流通产生价值的增值属性，MACD 带领数字加密资产真正走入全实体落地交易结算。

1.3.5 其他

MACD 的用户同时可以确认其它所有数字资产的区块链功能， 金融合约功能等；去中心化，衡量发行，既有超强的收藏价值和交易价值。

1.4 设计规划

1.4.1 权力以及具体事务的自治和去中心化

对财产的支配将逐步走向自治与去中心化。比特币通过公钥体系和 PoW 体系， 实现了数字资产权利自治和去中心化的第一步。然而如果按照确定性的规则，以可追溯的方式，进行没有具体复杂上限的简单事务。例如，开源程序就并不要求每个人都独立编写源代码，而是提供已编译的程序供用户下载，只需少数人进行编译验证即可。
如果能够将区块链的记账系统设计成一种确定性的，作恶会留下密码学证据的简单事务，那么这样的记账体系就可以不追求完全的去中心化，从而获得更高的效率。
MACD 中的记账人的权力等同于比特币矿工，记账是一种确定性的简单交易事务。通过这样的设计，MACD 可以做到一秒内区块查新及清算确认时间，保证了交易的即时性。

1.4.2 区块链类型的进化

Ripple、Bitshares、Counterparty 等区块链是一种记录型区块链，所有的用户行为都记录进了区块链。例如在基于比特币区块链中发送一个挂单指令，要 10 分钟后才能确认挂单成功（不是成交），并且还要支付比普通银行转账还高的手续费。
MACD 的设计理念为保真查询及清算型区块链。简单地说，保真查询及挂单、撤单等不产生资产变更的日志型交易不需要写进区块链。区块链仅用作登记发生资产变更的交易。清算型区块链虽然牺牲了一部分非关键性的信息记录，但获得了更好的交易效率、交易承载量、灵活性和用户体验。

1.4.3 全新的金融体系

比特币的机制使用户可以匿名的进行转账、收款，矿工可以匿名的进行记账，但同时带来了法律法规保护方面的不足，是一个独立于真实世界的金融系统。然而， 平行金融系统将存在难以对接具体的实物资产的问题。
MACD 的目标用户是整个现有的互联网金融受众，需要接入大量实体性的金融资产。因此 MACD 的设计充分考虑了合规方面的要求，定位为一个对接实体金融和商业的区块链系统，同时又保持了极高私密性。

1.5 特点

1.5.1 对接实体金融

如上所述，与真实世界充分兼容是 MACD 的最大目标。MACD 为个人和公司用户都提供了多个国家法律认可的认证方案。通过身份认证的账户所参与交易的电子签名受相应法律法规的认可和保护，等同于实名签章。用户股权、债券等资产的转让和交易，等同各方签署电子合同，受多国《合同法》的认可和保护。

1.5.2 点对点场外交易

通过 MACD 独有的去中心化“点对点场外交易”，用户能够以全新的方式完成去中心化交易。用户无需向交易所充值，就可以在交易所进行挂单。挂单成交后，交易所将成交的交易信息直接写入区块链。
例如某用户通过“点对点场外交易”卖出某公司债权，该用户无需通过充值或其他方式把债权转入交易所。只需要在本地通过私钥对委托单进行签名，就可挂卖。成交后，对方的货币款项将直接进入此用户的钱包，无需通过交易所中转。
点对点交易因为无需管理用户的资产，所以在增加信任度的同时，提高了交易效 率。这种新的交易方式--平台只负责信息的撮合，区块链负责财物的交割安全， 将带来包含网上商城、新零售、旅游、远程支付的巨大变革。

2 系统说明

2.1 用户界面说明

私钥：一个系统生成的随机数，由用户保管且不对外公开。私钥是用户账户使用权以及账户内资产所有权的证明。
公钥：每一个私钥都有一个与之相匹配的公钥。可由私钥通过单向、确定性的算法生成。
地址：将一组公钥的有序排列得到的脚本，通过单向、确定性的算法生成。
账户和账户地址：账户是指一定数量（1-16 个）的公钥的组合。最基本的账户由一个公钥组成，其账户地址就是其 1-of-1 多重签名地址。更高级的设计中， 账户可以由两个公钥组成，这两个公钥所生成的 2-of-2 多重签名的地址为账户地址。

2.2 身份认证

用户（个人或机构）可以以匿名的方式使用 MACD 平台及其对应服务，也可以申请身份认证，以便于在交易中提供身份信息。申请认证时，用户提供所需身份证明材料，并以对应私钥签名。核实无误后，用户获得一份数字证书，该证书内包含了用户的公钥和身份信息，用于证明该公钥和用户身份的对应关系。
用户在使用 MACD 时，可使用对应的私钥对交易进行签名。该签名符合各国《电子签名法》中“可靠电子签名”的定义，具备法律效力。
包含用户身份信息的数字证书由用户自行保存，不存储在 MACD 区块链上。因此， 除非用户主动向他人提供数字证书，任何第三方均无法获知其身份信息。

2.3 技术优势

MACD 将运用最新的 Masternode 主节点技术，在基础的区块链结构上，向用户（开发者以及支付金融用户）提供更多的服务，包含：匿名、隐私的交易；即时交易；加强的去中心化管理；去中心化的预算系统；不可逆的投票表决系统等。

3 MACD 资产类别

MACD 资产可以分为原始资产和用户发行资产。原始资产是 MACD 协议权益的载体， 用户发行资产是代表用户使用 MACD 平台所发行的资产或权益的载体。

3.1 MACD 原始资产

3.2 MACD 发行总量为 2600 万枚，代表了 MACD 协议的所有权及使用权，总量恒定，不可增加。
分配方式为：100 万枚原始股东及投资人， 400 万枚分配给技术团队，2100 万枚币量通过持有、复息、分配的方式，逐步释放给 MACD 的爱好者和市场推广者及矿工，以此保持结算价格的相对稳定及逐步上涨。

MACD 所代表的的主要权益为：

a)持有权

b)分红权

c)记账人决策权

MACD 的主要用途为：

a)支付 MACD 的服务费

b)支付 MACD 的区块链使用费（挖矿）

c)流通交易的媒介

3.3 用户发行资产

任意用户均可发行资产。区块链数字资产通过平台进行创建与交易。

3.3.1MACD 货币网关

MACD 以网关的形式引入外部法定货币，以 MACD 作为交易支付媒介对同种或不同种货币进行转账和接收货品和实物。
用户可通过 MACD 平台将货品和实物数字资产化，再以整体或分拆的形式进行转让或交易。

3.3.2 股权资产

股权资产指用户以公司股权（或股份公司股票）为标的物在 MACD 系统中发行资产。

3.3.3 债权资产

债权资产指用户以个人或组织机构的货币性债务为标的物在 MACD 系统中发行资产。

3.3.4 其它资产

其它类型资产，资产发行者可自行定义。

4 交易类型

交易是指 MACD 系统中引起资产的权益发生变化的事务，包含以下类型的交易。

4.1 资产创建

用于创建一个新的用户资产。用户可以自定义资产的类型、名称、总量、单价等， 并指定资产的管理者。此项操作需要消耗一定数量的 MACD 作为服务费。

4.2 资产转移

用于资产的出售、赠与、继承、接收等。

4.2.1 合同交易

指定参与方的交易，并可以根据参与交易的资产类型判断是否要求对方确认接受。对手方可以选择确认接受（签名）或拒绝（忽略）。

4.2.2 委托交易

不指定对应方，但指定一个代理人的交易。由代理人负责撮合交易的对应方。“点对点交易”即通过委托交易这种交易类型来实现。

4.4 交易费用

交易费用分为区块链使用费和服务费，均以 MACD 支付。其中，区块链使用费则被支付给记账人（节点）作为记账奖励。

4.4.1 区块链使用费

区块链使用费是因交易占用包括传输带宽和区块链字节等区块链资源所产生的费用，由记账人收取。记账人可自行决定是否收取以及费率标准。

4.4.2 服务费

服务费是使用 MACD 协议完成某些高级功能而需支付的费用。目前需要支付服务费的交易包括资产创建、资产变更、资产注销、资产冻结、候选记账人登记等。

5 记账机制

5.1 区块链记账

MACD 使用区块链来记录数据。区块链可以被看做一本账本，每个区块就是此账本里的一页账目，每页账目里包含了一个预设时间段里的所有交易。
MACD 的区块链约每 30 秒生成一个区块。新区块附加于前一个区块之后，形成一个链的结构。每个区块内包含了 30 秒内所发生的交易信息，以及其他必要的检索和校验信息。
一个完整的区块链包含了自创世块以来的所有交易信息，代表了当前的所有资产的归属和状态。MACD 区块链可以以极低的成本完成传统中心化数据库的等量事务。

5.2 区块链共同确认

共同确认是指运行 MACD 协议的各节点对当前区块链状态达成一致意见的机制。MACD 通过 MACD 持有人持有，来决定记账人及其数量；被选出的记账人进行对每个区块内容进行共识，来决定其中所应包含的交易。

5.2.1 记账规则

MACD 的区块链可以做到：

a)30 秒一个区块，交易达到一秒以内结算

b)单个记账人不能拒绝包含某笔交易进入当前区块

c)每个确认由全体记账人参与，六个确认就是完全确认

d)“点对点交易”机制，记账人不能虚构交易

5.2.2 记账人

持有 MACD 一定权益量的人可以按 POS 参与记账，记账人通过提供实体服务器提供算力支持，同时获得相应记账奖励。

5.2.3 区块交易的确认

在每次交易提交时，记账人将广播其认为应该写入本区块的每笔交易的散列值。其他记账人接收到此项信息后，检查自己是否有该交易散列值的对应数据。当区 块随机数产生后，每个记账人合并所有第一步广播中的交易（剔除只有散列值但无法获得交易数据的交易），并签名。获得 6 个记账人的签名，则本区块完成； 否则，本区块的本轮共识失败，退回第一步再次尝试进行确认。

5.2.4MACD 分配的确认

每个区块中除了用户发起的交易外还有一笔特殊的交易用于将 MACD 分红。其算法是根据区块随机数，以持币量为权重，按一定算法发送给 MACD 持有人。

6 分配机制

6.1MACD 分配方案

用户通过参与前期推广交易所购买、场外转让等方式获得 MACD。MACD 代表了 MACD 协议这个网络的所有权。

6.2MACD 分配机制

创世块中，根据一定算法，每个块向持有者按比例概率分配 MACD。具体分配方案详见后续说明文件。

7.MACD 生态链

7.1 交易方式

MACD 可以在例如中心化进行交易，也可以在 MACD 的区块链上以点对点交易的形式交易。目前交易所的大量成本耗费在资产和货币的充值提现上。点对点交易所不需要参与资产的交割，大大减轻了运营成本，同时也降低了用户的交易成本。

7.2MACD 钱包

MACD 平台提供专用的钱包，向用户提供多方的服务。同时，自由开发者及服务商可以通过默认 API，来鼓励 MACD 的持有人选举钱包服务商成为记账人。记账人可以获得 MACD（区块链使用费）作为经济回报。为服务商运营好钱包服务提供了额外的经济激励。

7.3 新零售、众筹、商城、跨国支付及其他商业应用

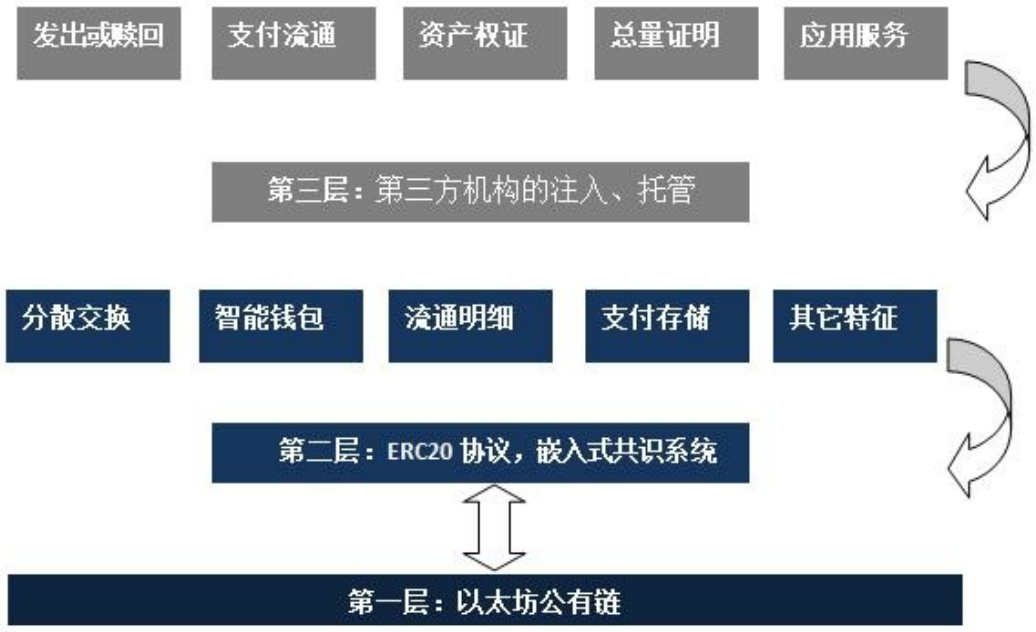
MACD 用户（个人或机构）可通过平台发起众筹，并可以使用 MACD 作为其平台众筹 项目的股权管理系统；即满足了用户对众筹的各项需求，也合乎监管规定。MACD 的资产数字化、区块链交易功能可以帮助用户实现实物以及数字产品的登记、转 让、出售、购买等功能，并在这一过程中降低了运营成本，极大地提高了效率。MACD 的快速支付功能以及 MACD 作为支付媒介的属性，使跨国交易、法币兑换变得快捷简单。此外，用户可自定义数字资产这一特性，使个人品牌、小额风投成为可能。

8.MACD 公有链技术

8.1 第一层是区块链

通过嵌入的共识系统以太坊，MACD 交易分类帐被嵌入以太坊公有链中作为元数据。

MACD 完全基于以太坊公有区块链，其流程架构图：



8.2 第二层是全层协议。

以太坊公有链是一项基础技术，可以：

a) 授予（创建）和撤销（销毁）表示为以太坊公有链中嵌入的元数据的数字令牌。

b) 通过以太坊公有区块链完成跟踪和报告 MACD 的流通情况。

c) 允许用户支付或存储 MACD 和其他资产。

d) 数字货币支付在点对点、匿名、加密环境中进行。

e) 开源、基于浏览器、加密的网络钱包。

f) 支持多签名和离线冷存储

8.3 第三层是 MACD 限制，我们的业务实体主要负责：

a) 接受资产并注入发行相应的 MACD；

b) 发出或赎回相应的 MACD；

c) 保管法定资产权证，支持所有流通的 MACD；

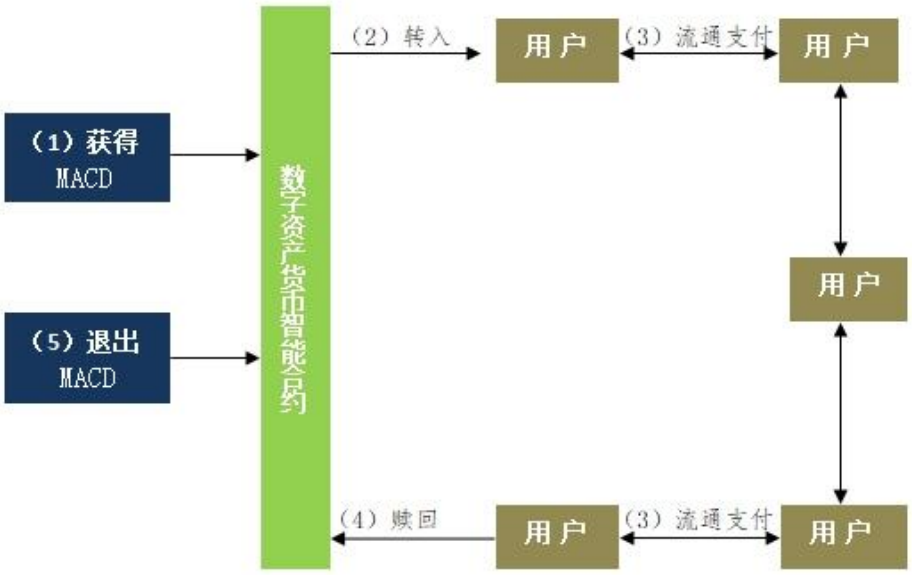
d) 公开报告准备金和其他法定资产审计结果的证明；

e) 启动和管理与现有区块链钱包、交易所和商家的流通支付；

f) 允许用户方便地发送、接收、存储和转换 MACD。

8.4 生命周期

MACD 的生命周期有五个步骤，流程图：



a) 用户通过其他资产或货币获得 MACD。

b) MACD 生成并转入用户的数字区块钱包帐户，MACD 进入循环。

c) 用户进行交易。用户可以通过点对点、开放源码、匿名、基于以太坊的平台来传输、交换和存储 MACD。

d) 用户将 MACD 放在数字区块钱包账户上，通过交易所、点对点多种通道，以便兑换成法定货币。 用户也可以通过直接交换或其它方式获得上述过程之外的 MACD。每一个 MACD 进入流通，它就可以在任何企业或个人之间自由交易。