米优速区块链

MIUSU

米优速

WHITE PAPER

MIUSU

目录

米优速

第一章 背景

1.1 行业概述

区块链技术本质是一种分布式数据库技术。所谓的分布式数据库，指的是把数据分别存储在通过互联网相连的多台计算机上，用户可以通过整个互联网访问和修改数据的数据库组织形式。再通俗一点说，区块链的核心就是一个建立在共识模式之上的共享数据库，无论是要添加新的数据库，还是调用已有的数据库，都需要达成共识，并且这些数据交易记录对于系统内部来说永久透明。基于区块链技术的应用通常会呈现出五个特征：去中心化（Decentralized），集体维护（Collectively Maintenance），去信任（Trustless），信息不可篡改（Unchangeable Data），匿名性（Anonymity）。总而言之，区块链的出现，利用其分布式的公共账簿记账方式，实现了在没有第三方参与的情况下，双方可以互相信任且顺利地完成交易行为，这是一种公信力表达方式的变革。

美国学者 Melanie Swan 在其著作《区块链：新经济蓝图及导读》中将区块链技术带来的对各个应用领域的颠覆影响分为三个时代：区块链 1.0（可编程货币）、区块链 2.0（可编程金融）和区块链 3.0（可编程社会）。区块链 1.0 时代主要是数字货币时代，是加密货币的应用，它构建了去中心化的数字交易系统，实现了快捷的货币交易、跨国交易等多样化的金融服务，它的主要代表是比特币。区块链 2.0 时代主要是智能合约的应用，主要领域扩展到金融领域，是智能资产、智能合约市场的去中心化，可作货币之外的数字资产转移，区块链在市场和金融的应用中更加广泛。区块链 3.0 主要是区块链的全面应用时代，区块链技术以去中心化的方式配置全球资源，进一步延拓到货币、金融和市场以外的领域，其潜在的应用领域包括选举、医疗、公证、公益、版

权以及网络安全、汽车租赁和学历鉴定等。目前，区块链已经历了区块链 1.0 时代，正处于区块链 2.0 时代，正在向区块链 3.0 时代稳步迈进。有学者预言 2019 年将完全进入区块链 3.0 时代。

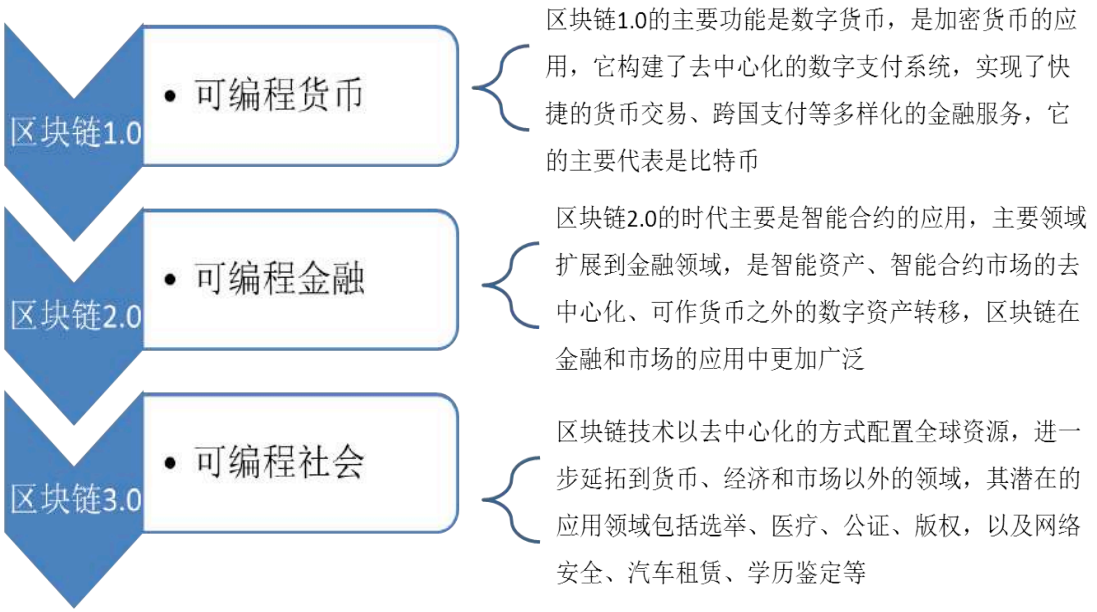


图 1 区块链的发展历程

目前，区块链技术正处于区块链 2.0 到 3.0 的过渡阶段，其应用领域也从最初的数字货币扩展到更广泛的金融领域，并且逐渐向其他众多领域延伸，其中金融领域应用最为广泛和成熟。区块链的一些典型的应用领域包括: 金融、教育、医疗、物联网、物流供应链、通信、社会公益、共享经济、大数据、人工智能、投票、审计、拍卖和彩票等。总之，区块链以其去中心化、去信任化、可追溯性、集体维护性、安全性和不可篡改性、开放性、匿名性等独特优势正逐渐运用到社会经济生活的各个领域，解决各个行业的难点、痛点问题，最终达到节约中介成本、建立信任关系、便于追踪、保证信息安全完整透明和保护隐私等目的。

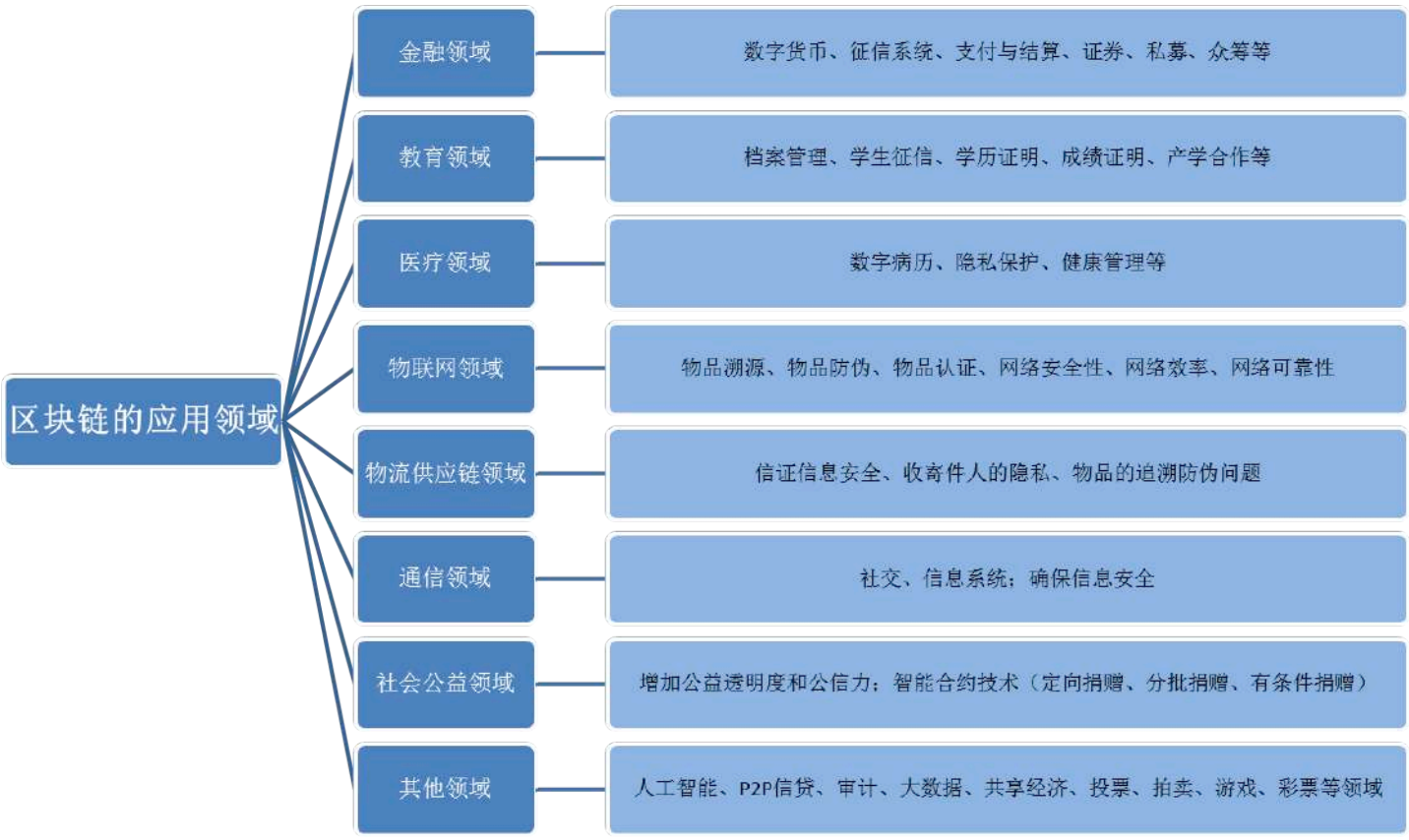


图 2 区块链的应用领域

区块链技术的出现，使得互联网上的数字资产确权成为可能。其经济意义在于数据自带程序。首先，数字确权实现低成本化，人类将进入数字资产时代。在这样一个时代中，人类的主要资产将是由数字构成的，其比重甚至超过实物。试想一下，当你在朋友圈发的一张过年的照片被意大利一位开民宿的摄影爱好者看中，而通过区块链的交易，你将照片的版权卖给了他，而换来旅游时一夜的住宿权，这样的全球小贸易是不是格外的方便而有趣呢？

其次，数据带程序使得资产、合约合二为一。在区块链技术的前提下，不对称加密进行数据确权，一个用户除非掌握全网超过 51%的计算能力，否则无法篡

改信息，数据在全网记账并且盖时间戳进行唯一合法转移，违反协议者出局，这就是区块链共识协议。换句话说，这个程序本身就是一种合约。

再则，人类将进入智能经济时代，实现经济 2.0。区块链在金融领域可以构建智能合约机制，私钥的条件一旦达成，程序代替合约直接开始执行。比如说，我们在网购时，通常是借助 Paypal 或者支付宝来进行转账的，如果应用了区块链技术，同一个链上的资产就自动兑付了，可谓是真正的“一手交钱，一手交货”。这种无需第三方的经济模式，非但没有降低交易的安全性以及私密性，反而提高了交易的保障性、及时性和广泛性。另外，基于区块链的数字资产也带给了每个人变现自己未来的机会。所谓变现未来，指的就是我们可以利用已经确权的数字资产获得具有全网公开认证的估值，从而完成交易。

未来关于区块链的研究会更多地集中在区块链存在问题的解决方案、区块链的应用研究即将区块链技术付诸实践的研究以及相关法律法规和监管问题。随着区块链技术的成熟以及人们对区块链认识的不断深入，区块链问题终会得到解决，当成熟的区块链技术广泛应用于各个领域时，“区块链 + ”时代随之而来。有专家预测， 在未来的 10 至 20 年几乎所有的企业都会利用区块链技术来设立公司、签合同、登记数字资产，管理供应链、物流、销售、融资、财务、交税 等各项业务，以此获得更大的竞争优势，就像今天的所有企业都在用互联网产品一样，没有利用好区块链技术的公司无论目前多大多强，都会有被淘汰的可能性。米优速团队希望能帮助大家最快最好地将区块链应用场景落地，迅速跟上时代的步伐。

第二章：项目概述

2.1 米优速区块链介绍

基于区块链技术的米优速使用由分布式账本和分布式计算机组成的智能合约，使数字货币更加透明，其生态适用于大部分应用场景。

2013 年 12 月，Vitalik Buterin “V 神” 提出了以太坊（Ethereum）区块链平台，除了可基于内置的以太币（Ether）实现数字货币交易外，还提供了图灵完备的编程语言以编写智能合约（Smart contract），从而首次将智能合约应用到了区块链。然而，现在的以太坊存在交易成本高和交易速度慢等问题，对于那些对交易成本控制非常严格和那些需要高效的交易速度的商业模式，今天的以太坊是无法支撑的。

首先，交易成本非常高。交易手续费近来成为了困扰虚拟货币投资者的新问题。在两三年前当以太币的价格不足一美金的时候，以太坊的交易手续费十分低廉，几乎可以忽略不计。这也是该数字货币的支持者经常强调的其主要卖点之一。时至今日，以太坊的价格已经超过了 600 美金，涨幅 600 多倍，这也代表手续费也随之翻了很多倍。为了确保快速完成交易，以太坊交易手续费在高峰期通常可以超过数美元。因此，在交易费用持续上涨的时候，那些对转账时手续费非常敏感的商业项目势必要寻找替代品，否则无法持续发展。

其次，交易速度较慢。2017 年，最常出现在人们视线里的新闻除了以太币价格的狂飙，便是以太坊交易网络的时常拥堵。据外媒报道，这是由于以太坊的网络收费结构竞争激烈，延迟时间相对较长造成的。按照今天的标准，以太坊的区块运行时间的确较慢，高费的 GAS 往往也需要花费 2 - 3 分钟才能完成确认，低费的 GAS 则需要 10 几分钟以上。虽然它的速度相较于比特币的区块链已经有了很大程度的优化，在今天也仍然算快，但无法达到即时的程度。以太坊是目前市场上最成功区块链 2.0 项目，有数以千计的智能合约搭载在其区块链之上，2018 年 6 月份 “V 神” 表示，以太坊将采用 Sharding 和 Plasma 等第二层解决方案，以此能够达到每秒处理 100 万次交易，甚至有潜力到达 1 亿次，但是许多业界人士对此表示不太看好，因为以太坊船大难调头，很多东西都已经成为定式，比如社区的共识，矿机的生态，底层的技术都不是那么容易改变的。所以很多人认为，一定会有一个公链替代以太坊，如果把以太坊比做是计算机的 dos 系统，下一代 windows 是谁 ,我们不得而知。这也是我们要做米优速区块链的主要原因，做出一个基于以太坊的公链模型为基础，能顺应市场需求而演变的区块链，因此只要有在以太坊上开发过的程序员都能马上适应米优速的区块链开发。保持以小

船的韧性姿态将区块链技术落地到实体项目，让区块链技术能够融合到日常生活的方方面面。米优速团队坚信，入市才是现在区块链公司的重心之重。个人和企业在区块链真正的落地面临三难：应用场景难，找到懂区块 链技术的开发团队难，实现区块链安全难，特别是在欧洲，这几个问题更是严重。米优速希望能提供类似 SaaS(软件即服务)的方案，帮助欧洲企业解决这三个区块链落地的难题。个人和企业不需要支付昂贵的开发费用，米优速团队会按照客户的需求帮其打造区块链项目，让客户可以享受安全的区块链服务。现在市场上的区块链人员是比较稀缺的，因此很多想要对接区块链技术的商业项目没有合适的技术支撑，无法做好项目策划和后期跟进。很多公司甚至都区块链基础技术的概念都是模糊的，更别说智能合约运行的原理。这有点像互联网初期，很多人觉得与自己的行业无关，却不知之后互联网将重塑所有的商业模式。区块链技术也是一样，有着能够重塑现有的中心化的互联网商业模式的力量。大家可以想象一下：去中心化的支付宝或者 Paypal，去中心化的博彩赌球公司，去中心化的众筹平台，去中心化的共享经济平台等等。很多商业模式在完成去中心化的阶段之后，将会给供应者和需求者留下前所未有的利益分配红利。米优速将会把大部分筹集的资金用于社区的开发，对社区项目的扶持，为社区提供从资金到资源的支持，从概念普及到到技术落地，帮助孵化更多的链上项目，努力打造一个完整生态环境。

在未来，尽管米优速的交易费用可能也会随着其代币价格的增长而增长，但是增长速度较慢，而且船小易掉头，如果未来米优速决定采用 Sharding 和 Plasma 等第二层解决方案，应该会比以太坊更容易实施落地和达到效果。由于米优速新型的网络设置，其交易费用几乎可以忽略不计，而且交易达成几乎是即时的。因此，可预见短期内米优速将可以覆盖现在因为以太坊高额交易费用和缓慢

交易速度而不得不离开以太坊的商业项目，或者那些未对接区块链的商业项目，许多这方面的项目是高频率的项目，比如说小额支付等金融类业务，高频的项目汇集会使米优速的区块链代币 MIU 拥有良好的市场价值增值空间，对于人们来说会是不错的投资。

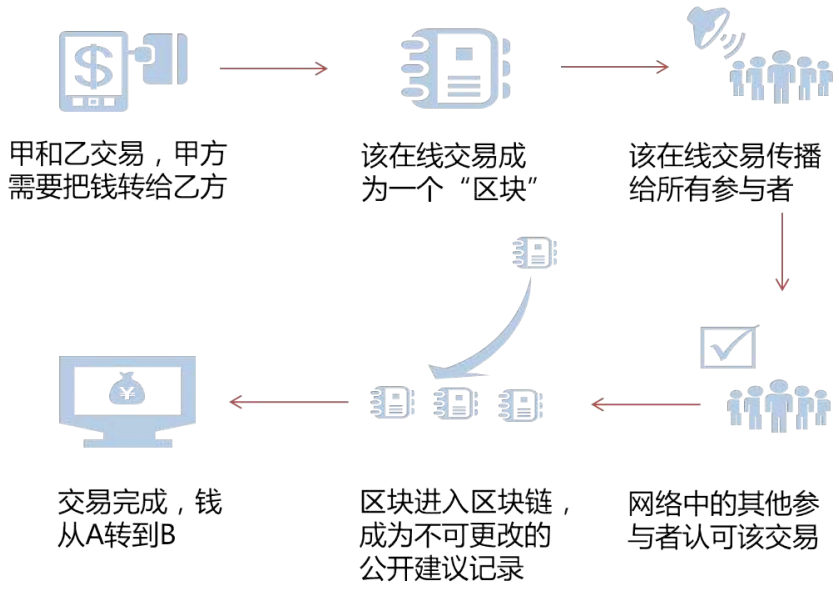
此外，米优速拥有良好的社区资源，将与多家交易所展开合作，方便用户可以快速将米优速上的代币兑换成政府支持的货币，如兑换成欧元或美元。米优速区块链和以太坊一样，将会产生一个使用加密认证技术和去中心化共识机制共同维护的完整的、分布式的、不可篡改的服务社区，通过区块链发行的数字货币将所有用户紧密地联系在一起。

首先，用户自行完成交易，无需中间商插手。区块链在米优速的真正价值在于促进用户根据供需自行达成协议，交易双方无需第三方的认证和监管即可互相信任，自行选择完成交易。用户信息、交易信息等作为数据通过分布式账本技术储存在全球网络上的各个节点，当达成共识以后会被盖上时间戳储存在区块链中，因此这些数据不可篡改且公开透明。

其次，基于区块链的去中心化特性，整个米优速系统的运作是公开透明的，采用“签名”机制和利用“少数服从多数”方式，从而能够从机制上保障信用。统一的交流平台使得全球用户能够基于区块链获得真实有效的交易信息，避免信息造假，避免上当受骗，并且可以使各种商业资讯快速地传播开来。

最后，统一数字货币连接全世界的交易。随着交易全球化的推进，其变得越发频繁，然而各个国家之间汇率的换算阻碍了国与国之间的交易发展。米优速发行的代币在平台之间进行流通，不受用户国籍和各国汇率的限制，只要是米优速用户都可以使用代币进行交易，这进一步避免了用户的许多麻烦，避免了因外汇

而带来的市场动荡，从而能够吸引更多的全球用户在此平台交易，也因此能够促进全球交易的发展。中国是世界上最大的贸易出口国，华侨也遍布在世界的每一个角落，区块链技术可以作为一个良好的外汇解决方案。



作为能在全球范围内使用的平台，米优速背后的区块链技术可以让消费者在面对不同的消费需求和应用场景而要进行交易时，既无需付出过高的交易成本，也无需等待过长的交易时间，从而提高消费者使用米优速的积极性。

区块链将改变人们的生活方式，米优速也将参与这场革命。智能合约将变为一种安全、透明、便捷的机制，降低交易的风险和繁琐程度，让交易活动更加迅速简单。米优速的自治合约能为很多应用场景提供新的机会，让人们获得更多的便利进而提高其生活质量。此外，米优速能提供“完全的透明性”，以解决交易者之间的信任缺失问题。米优速的透明度是公开的，任何用户都可以查阅。任何基于它的系统都是完全透明的。米优速账本不需要第三方，因此它降低了相关成本，也消除了对第三方的依赖，并使交易变得开放，其可以为建立信任带来显著的好处。其次，米优速结合虚拟与现实提供了一种可代表任何资产的方式，这些

资产可以是有形的，也可以是无形的。在这种方式下，所有权状态可在任何时间点被确认，同时能够与交易机制完全兼容。

米优速通过区块链技术记录交易信息，区块链技术使得交易记录永不可更改。米优速上记录的数据具有公允性，而且持续有效。此外，通过技术的迭代可让更多的交易信息记录到米优速上，实现匿名共享，可靠传递。此外，米优速促进大数据价值流通。流通使得大数据发挥出更大的价值，类似交易管理系统的区块链应用，可以将交易大数据作为数字资产进行流通，实现大数据在更加广泛的领域应用及变现，充分发挥大数据的经济价值。基于去中心化的米优速区块链，能够打破各用户之间的数据壁垒，从而使得用户的消费数据得到最大价值的发挥。

2.2 系统设计体系介绍

2.2.1 智能合约系统

和以太坊的一样，米优速的智能合约编程语言是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。智能合约就像一台基于区块链的自动贩卖机，购买者将硬币投入机器，而机器对硬币进行验证，然后做出回应（分配产品）。发展至今，智能合约可以简单的概括为：它是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值。它更像是一个系统的参与者，可以把它想象成一个绝对可信的人，他负责临时保管你的资产，并且严格按照事先商定好的规则执行操作。具体的合约式交易流程如下:

智能合约生命周期管理：智能合约自动化的特性使得米优速在处理数字货币交易时显示出了突出的优势。当交易的两端对合同约定事项的执行达成共识后，智能合约平台可自动触发交易、结算等行为，同时将相关信息记录在区块链中。智能合约的加入使数字货币交易的效率大大提高，同时由于智能合约能够自动执行，可以极大程度地减少人力成本的投入。米优速借助基于区块链技术的智能合约不仅可以发挥在速度、成本效率方面的优势，而且可以避免恶意行为对数字货币交易正常执行的干扰。米优速将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障存储、读取、执行整个过程透明可跟踪、不可攥改。同时，由区块链自带的共识算法构建出一套状态机系统，使得智能合约能够高效地运行。智能合约的生命周期管理功能包括创建、调用、升级、销毁。用户可以升级智能合约和迁移数据，但是要依照原智能合约设定的升级规则。

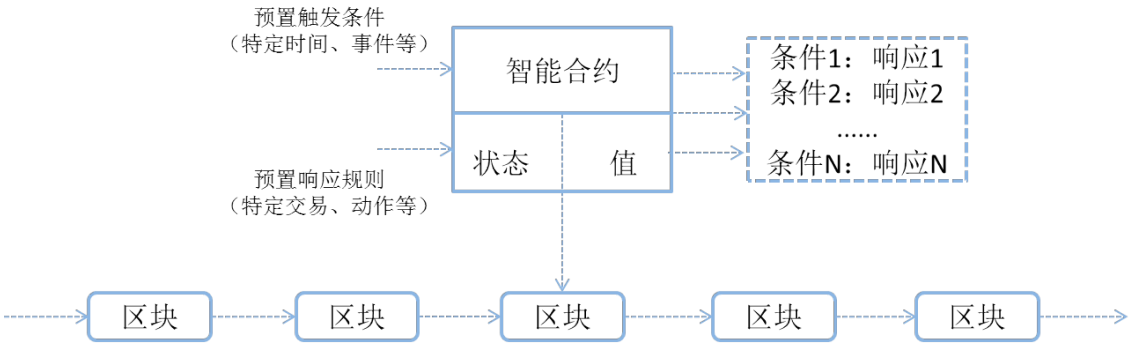


图 3 智能合约的运作机理

智能合约组合服务：已有的一个或多个智能合约可以通过组合来创建新的服务功能。米优速为服务使用者设计集成的接口使其能访问多个区块链系统服务功能。

智能合约测试服务：通过对区块链系统中实现的组件功能进行测试，可以确保这些组件完整并正确地实现了服务功能。此外，通过测试也可以检测这些组件

的系统安全性与健壮性、确保服务功能接口的互操作性以及测试宜覆盖区块链系统中的服务部署节点。

智能合约模板服务：米优速系统在链上业务的支持方面采用目前主流的虚拟机机制，目前支持的是兼容米优速的虚拟机，可直接部署、运行 Solidity 智能合约。并在积极研发更贴近环境净化行业应用的其他虚拟机实现，以方便快速开发、定制链上业务逻辑。智能合约的模板服务可以使用户快速使用米优速系统，针对一些常见的业务场景，米优速系统预先开发了多个可直接使用的链上业务合约，集团可根据实际需求直接选择部署、使用即可。

2.2.2 账户模型和账户体系

米优速的账户模型和以太坊的一样，为了支持更多类型的行业应用，米优速区块链平台采用了基于账户的模型，从而可方便地查询交易余额或业务状态数据。智能合约也更适合于在基于账户的模型之上构建，其针对状态数据更易处理复杂的业务逻辑。米优速下的账户分为外部账户（Externally Owned Account）和合约账户（Contract Account）两种类型。外部账户用于表达一个普通账户的米优速代币余额，合约账户用于表达一个米优速智能合约，普通账户中的余额、智能合约中的状态变量都属于米优速状态数据。下图描述了米优速账户的状态转换过程，状态反映了账户中各属性的当前值，涉及账户的一笔交易发生时，会引起账户状态的变化。外部账户和合约账户在米优速下用同一数据结构表示，其包含 Balance、Nonce、Code Hash 和 Storage Root 四个属性，Balance 是账户中的米优速代币余额；Nonce 是对账户发送过的交易的计数，用于防范重放攻击；当账户被应用于智能合约时，Code Hash 为合约代码的哈希值，Storage Root

是合约状态数据的 Merkle Patricia 树根。米优速的交易包含 To、Value、Nonce、gas Price、gas Limit、Data 及交易签名七个属性。To 是接收者的账户地址 ,Value 是转账的米优速代币金额，Nonce 是发送者对本次交易的计数，gas Price 是交易时 Gas 的米优速代币单价 ,gas Limit 是执行该交易所允许消耗的最大 Gas 数额，Data 是调用智能合约时的消息数据，交易签名是发送者对交易的 ECDSA 签名。

2.2.3 账户地址生成规则

对于用户通过交易和米优速区块链互动来说，账户是必不可少的。账户代表着外部代理人（例如人物角色、挖矿节点或是自动代理人）的身份。账户运用公钥加密图像来签署交易以便米优速虚拟机可以安全地验证交易发送者身份。每个账户都由一对钥匙定义，一个私钥和一个公钥。账户以地址为索引，地址由公钥衍生而来，取公钥的最后 20 个字节。每对私钥/地址都编码在一个钥匙文件里。钥匙文件是 JSON 文本文件，可以用任何文本编辑器打开和浏览。钥匙文件的关键部分是账户私钥，通常采用用户在创建帐户时设置的密码进行加密。

米优速涉及的安全加密算法及相关定义如下：

对称加密：对称加密是最快速、最简单的一种加密方式，加密（encryption）与解密（decryption）用的是同样的密钥（secret key）。对称加密通常使用的是相对较小的密钥，一般小于 256 bit。密钥的大小既要照顾到安全性，也要照顾到效率，是一个 trade-off。

非对称加密：非对称加密为数据的加密与解密提供了一个非常安全的方法，它使用了一对密钥，公钥（public key）和私钥（private key）。私钥只能由一

方安全保管，不能外泄，而公钥则可以发给任何请求它的人。非对称加密使用这对密钥中的一个进行加密，而解密则需要另一个密钥。

私钥（private key）：非公开，是一个 256 位的随机数，由用户保管且不对外开放。私钥通常是由系统随机生成，是用户账户使用权及账户内资产所有权的唯一证明，其有效位长足够大，因此不可能被攻破，无安全隐患。

公钥（public key）：可公开，每一个私钥都有一个与之相匹配的公钥。ECC 公钥可以由私钥通过单向的、确定性的算法生成，目前常用的方案包括 secp256r1（国际通用标准）、secp256k1 和 SM2（中国国标）。

Hash 算法：通常 Hash 算法是指安全散列算法 SHA（Secure Hash Algorithm），该算法是美国国家安全局（NSA）设计，美国国家标准与技术研究院（NIST）发布的一系列密码散列函数，包括 SHA-1、SHA-224、SHA-256、SHA-384 和 SHA-512 等变体。除 PoW 外，其余 Hash 算法均指 SHA-256。

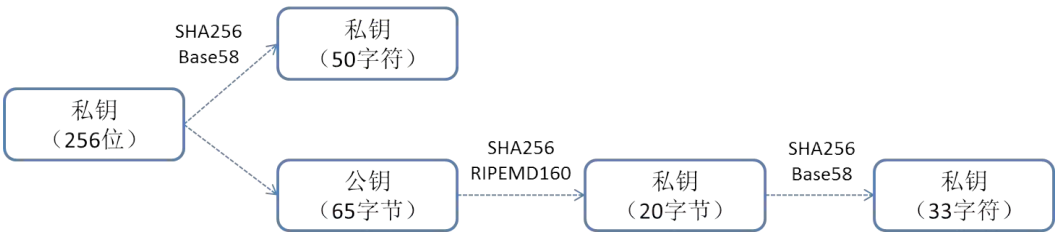


图 4 隐私保护

2.3 米优速区块链交易系统

区块链将许多跨领域技术凑在一起，包括演算法、数学、密码学与经济模型，并结合点对点（P2P）网路关系，利用数学基础就能建立信任效果，成为一个不需基于彼此信任基础、也不需依赖单一中心化机构就能够运作的分散式系统，用来实现一个可去中心化，并确保交易安全性、可追踪性的数位货币体系。

当前所有者利用私钥对前一次交易和下一位所有者签署一个数字签名，并将这个签名附加在数字货币的末尾，制作成交易单。一笔新交易产生时，会先被广播到区块链网络中的其它参与节点。当前所有者将交易单广播至全网，每个节点会将数笔未验证的交易 Hash 值收集到区块中 ,每个区块可以包含数百笔或上千笔交易。最快完成 PoW 的节点，会将自己的区块传播给其他节点。每个节点通过相当于解一道数学题的工作量证明机制，从而获得创建新区块的权力，并争取得到数字货币的奖励。各节点进行工作量证明的计算来决定谁可以验证交易，由最快算出结果的节点来验证交易，这就是取得共识的做法。当一个节点找到截时，它就向全网广播该区块记录的所有盖时间戳的交易，并由全网其他节点核对，其他节点会确认这个区块所包含的交易是否有效，确认没被重复花费且具有效数位签章后，接受该区块，此时区块才正式接上区块链，无法再窜改资料。全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块。所有节点一旦接受该区块后，先前没算完 PoW 工作的区块会失效，各节点会重新建立一个区块，继续下一回 PoW 计算工作。每个区块的创建时间大约在 12 秒，随着全网算力的不断变化，每个区块的产生时间会随算力增强而缩短，随算力减弱而延长。

第三章：设计原则

3.1 应用

米优速之上可以搭建三种应用，和以太坊一样。第一类是金融应用，包括金融衍生物，hedging 合同，存储钱包。第二类是半金融应用，一部分需要钱，而一部分不需要钱，如矿工通过计算解决问题获得奖励。此外，第三类是非金融应用，例如线上投票和分散治理等。

金融衍生物和稳值货币。金融衍生物是智能合同的最常见的应用，但金融合同是最主要的挑战是需要提供一个外部价格作为参考。最简单的方法是通过数据反馈合同，合同包含特殊的官方机构可以提供价格。那么当一方有能力去更新合同并且会提供一个窗口允许其他合同发送消息给他并回复。给出对冲合同的重要部分：1) A 方输入 1000 数字货币；2) B 输入 1000 数字货币；3) 记录 1000 数字货币的美元价值，这是通过反馈合同的数据计算得到的，并存储记录为 x $。若干天后，允许 A 或 B 重新要回价值 x ¥（由合同返回的新价值计算），然后将剩下的给另一方。最重要的问题就是价格波动大，提出的解决方案是发起者背后的支持方案。发行人创建了一个子货币，其有权发行和撤销货币单位，并提供一个单位的货币给任何一个给他们离线提供了能与一个单位的货币对应的基础资产（如黄金，美元）的人。比如由 Tether 公司发行的锚定美元的 USDT 代币，或者

由 Joppay 公司发行的锚定欧元的 EURP 代币，发行人则承诺发送回一个单位的保密资产而提供的法定资产。通过银行转账进行交易对于很多人来说会缺乏隐私性，而且在欧洲美国等发达国家税务的检查和私人银行的流水直接挂钩，使用现金又会碰到携带，远程交易和人身安全等问题，使用比特币等虚拟货币却又有价格浮动太大的问题，所以如果能够将一个锚定法定货币的代币在民间应用起来，可以把现金虚拟化，那么使用的频率和可覆盖的市场将会很大。

米优速区块链拥有和以太坊一样的身份认证和信誉系统，搭建分散自治组织（DAO）的可能性，和搭建各种领域的应用，比如实现云计算（证明的计算环境）、点对点打赌（可以赌下一个区块的哈希值与猜测值之间的差异）、预测市场、链上的分散市场（利用身份和信誉系统为基础）。

3.2 资产流通以及管理

数字资产是米优速的血液，它为生态的各个部分提供动力，数字资产是整个系统运行的基础，也是米优速正常运营的保障。无论是算力组还是应用层，都需要得到数字资产的支持，用户想真正使用米优速应用，也需要数字资产来帮他实现。只有各个部分互相帮助，协同进行，才能使米优速像一个有机生命体一样充满活力和生命力。

3.3 多重签名

在米优速公链上，公钥是标识和区分一个用户的唯一方法。为了保障交易安全性，需对每笔交易都进行签名与验证，签名算法使用了椭圆曲线数字签名算法（ECDSA）。

米优速货币基于账户的模型，其交易数据中只包含了发送者的 ECDSA 签名，并不包含发送者的公钥和发送者的地址，因为基于 ECDSA 签名、原始交易数据和椭圆曲线参数可以恢复出发送者的公钥，然后对公钥进行 SHA3 哈希运算，即可计算出发送者的账户地址。如此设计可减少每笔交易的字节数，从而减少交易数据在存储和网络方面的开销。

第四章：实现方案

4.1 米优速区块链公链

米优速区块链是公有链，对所有人开放，任何人都可以发送交易且交易能获得有效确认的、共识过程的区块链，共识过程决定哪个区块可被添加到区块链中和明确当前状态。公有链一旦发布运行，程序开发者无权干涉用户，所以区块链可以保护使用他们开发的区块链的用户。任何拥有足够技术能力的人都可以访问，也就是说，只要有台能够联网的计算机就能够满足访问的条件，对节点没有太大限制。没有准入门槛，虽然对容量和性能改善造成比较大的困扰，但全民参与大大增强了区块链的透明度和信任度。

4.2 共识机制

4.2.1 PoW 共识机制

作为区块链技术的开创者比特币使用的共识机制就是基于工作量证明的共识机制，并且这一机制在其他公链环境下的区块链系统中也得到广泛应用。在 PoW 机制中，每一个参与算力竞争的节点叫做矿工，求解随机数的过程叫做挖矿。每一个矿工当接收到交易或者有新的区块成功添加到区块链上，会进行新一轮的挖矿。挖矿过程是求解一个数学难题的过程，将该矿工正在生成区块的区块头信息

进行哈希，由于区块头中包含唯一标示该区块的信息，因此矿工的每次挖矿中区块的哈希值一定各不相同。在每次挖矿前，会计算出一个目标值，该目标值与难度系数相关，矿工的每次挖矿过程就是生成一个随机数，并将这个随机数与唯一标识区块的哈希值进行双 SHA3 哈希，并将生成的结果与目标值进行比较，如果小于目标值则认为挖矿成功，否则将重新生成随机数继续运算直到小于目标值为止。整个过程由于双 SHA3 是不可逆哈希过程，对于求解小于目标值的过程只能通过不断计算获得，整个过程只与计算能力相关，因此可以通过求解的速度来判断算力。挖矿过程虽然耗时，但校验过程却异常简单，只需要将随机值与区块头哈希重新进行一次双 SHA3 哈希并判断是否小于目标值即可。通过 PoW 共识机制，全网共同竞争求解随机数，倘若某些矿工想使区块链发生错误只有汇集全网超过 50%的算力进行挖矿才可以办到，而这对于公链来说是近乎不可能完成的，因此 PoW 共识机制可以维持全网节点的一致性。中本聪将 PoW 共识机制与奖励机制结合，促使全网共同挖矿，这一新的理念可以说是真正意义上实现了去中心化。但是通过算力竞争实现分布式系统的一致性代价很大，以比特为例，在 2016 年比特币全网的算力要比全球前 500 的超级计算机算力总和还要多。因此米优速的区块链社区可以在后期按照整体社区的发展，投票决定是否要从现有的 PoW 的共识机制转换为 PoS 的共识机制。

4.3 去中心化钱包

米优速拥有网络版去中心化钱包，和移动客户端钱包，分别有 IOS 和安卓两个版本。米优速的钱包除了应有的发送、接收、地址簿、数字资产的信息展示、查询交易 ID 功能之外，未来将为用户开发用于落地应用场景的功能，这些功能将会接入钱包移动客户端当中，比如上述的不同的虚拟货币兑换功能，对接第三方的去中心化博彩竞猜应用，嵌入区块链游戏，区块链金融，众筹 ICO 等服务。

4.3.1 兑换服务

米优速的 App 钱包里有 Swap 兑换功能，能够实现用户使用米优速的一些代币和其它货币进行双向兑换，比如和比特币 BTC，以太坊 ETH 等等。

4.3.2 ICO 众筹平台

ICO (Initial Coin Offering) 是当前很多区块链项目筹集资金的主要方式。通过这项功能，米优速能够扩张自己的用户基础，帮助社区良性发展，帮助孵化更多的米优速社区项目。这方面的成功案列有中国的 ImToken 钱包，欧洲的 Eidoo 钱包等。

第五章：米优速区块链经济生态

5.1 米优速区块链币的用途和价值

米优速区块链币基于区块链技术，所有的数据点交易都会被区块链记录下来，以实现整个交易系统的公正、公开与透明。过去数年，以比特币和以太坊为代表的数字货币的发展，即用过去的事实，印证着区块链技术和加密数字货币的价值，让以米优速区块链币为介质的经济得以实现。

米优速区块链币的用途和价值：

1. 稀缺性：由于米优速可以引入各种应用，其用户量基本上都在百万级或者更多。代币的分发将会迅速进行，而随着挖矿难度的增加，免费获得代币的渠道将会减少，从而促使用户通过二级市场进行交易。

2. 流通性：百万级用户的引入和各种主流消费场景（金融、博彩、游戏、电商、广告、电子书、打赏等）的引入将大大提升代币的流通性，和社区一起打造”区块链+”的时代。米优速贷币还将登录国内外各种主流交易所，进一步提升流通性。

3. 系统发展带来的升值：数字货币的市值将跟其米优速系统的发展有正比的关系，在各种应用进入到米优速区块链后，米优速区块链代币的市值将会得到不断地提升。

米优速将会把大部分筹集的资金用于社区的开发，对社区项目的扶持，为社区提供从资金到资源的支持，从概念普及到到技术落地的完整生态环境。

5.2 发行计划

5.2.1 发行细则

MIU 米优速代币分布与预算分配

MIU 是基于 Miusu 米优速公有链自生成的代币，并且是公有链唯一的基础支付媒介，用来作为社区奖励、结算、交易以及公链智能合约履约使用。MIU 的数字代币共发行 100 亿枚，在第一阶段由创世区块一次性创设出来，之后平均 12 秒左右出一个区块，每出一块奖励 3 个 MIU 代币给矿工，一年大概新增 788 万枚代币。

1）MIU 米优速代币分布与预算分配:

- 5% 的 代币将预留给早期基石投资者
- 10% 的 代币将预留给早期私募投资者
- 20% 的 代币将用于众筹 ICO
- 15% 的 代币将预留给顾问 Advisor
- 25% 的 代币将预留给创始团队成员
- 25% 的 代币将由基金会用于扶持社区和链上项目发展，后期如果项目多的话，可以通过用 MIU 代币的公众投票机制决定所要扶持项目。

2）筹集的资金用途：

- 20% 将用于产品开发
- 35% 将用于运营
- 10% 将用于法务
- 20% 将用于营销
- 15% 将作为储备

团队锁定期:团队持有 25% 的 MIU 代币，其中 20% 用于现有团队成员激励，5% 用于后期引进新的团队成员激励，以确保团队的开发、运营实力。 团队持有 MIU TOKEN 锁定期三年，从第四年开始每 6 个月解锁一次，单次解锁 MIU TOKEN 量不超过当期剩余可用于团队激励 MIU TOKEN 总量的 30%。

MIU 的代币私募发售共分为两轮: 私募对象仅面向特定机构或合格投资者，募集币种为以太坊(ETH)，投资者在投资时需根据当天 ETH 价格与 USDT 或者 EURP 价格进行换算， 再使用 ETH 兑换相等价值的 MIU。

- 基石轮： 一个 ETH 兑换 750.000 MIU
- 私募轮： 一个 ETH 兑换 500.000 MIU
- ICO 众筹：一个 ETH 兑换 250.000 MIU

MIU 代币的锁仓机制: 私募期间通过智能合约锁仓奖励锁定相应的 MIU 代币，锁仓时间是 12 个月。

第六章：发展规划

现时 MIUSU 米优速的区块链平台已经搭建完成，主网已经上线，有网络钱包和移动端 App 钱包。资金募集到位后，接下来必须要使平台面向用户，开发应用，发挥其价值，因此必须要进行平台的推广使用。我们坚信，入市才是现在区块链公司的重心之重。因此所募集的一部分资金将被用于孵化社区的一些优质项目在米优速区块链上的搭建，运营和推广。米优速将持之以恒的进行区块链技术的深度开发，将“区块链+”的模式落地到各种领域。第一年我们将会把主要精力集中在欧洲地区，主要开发金融领域和博彩竞猜领域的 DAPP。

第七章：团队介绍

米优速创始团队：

胡允键 Jerry

“米优速”创始人

现任【聚付宝】CEO，1996年来到欧洲，毕业于意大利都灵经济大学，人称网红「小胖Jerry」。2016年创办了聚付宝，投资了呱呱到家等互联网平台。

Aurelio Mustacciuoli

“米优速”联合创始人

现任 【FinTier】集团的CEO，Mobilmat联合创始人，拥有20年金融和支付领域管理经验，曾任 IW Bank的总经理，Banca IMI 的CFO。

陆未

“米优速”联合创始人

现任【呱呱到家】CEO，8年系统平台、电子商务运营经验，呱呱到家O2O平台创始人。

第八章 免责声明

本白皮书只用于传达信息之用途，不构成任何投资建议，投资意向或教唆投资。本白皮书不组成也不理解为任何买卖行为，或任何邀请买卖、任何形式证券行为，也不是任何形式上的合约或者承诺。

Mjusu

第九章：风险提示

本数字资产项目净值会因为市场波动等因素产生波动，募集者须承担相应的募集风险。本数字资产项目募集中的风险包括：因整体政治、经济、社会等环境因素对数字资产市场产生影响而形成的系统性风险。

募集者参与募集本项目并不等同于将资金作为存款存放在银行或其它存款类金融机构，不保证盈利，也不保证最低收益。投资有风险，投资者募集本项目时应认真阅读本白皮书。

提醒募集者“募者自负”原则，在作出募集决策后，该项目运营状况与该项目净值变化引致的风险，由募集者自行负担。

Miusu

第十章：附件专业术语

1、米优速是一个基于公链的分布式计算平台，并提供了一个去中心化虚拟机，该虚拟机可以执行图灵完备的脚本语言。

2、米优速是由智能合约层、激励层、共识层、网络层和数据层构成，其中数据层中包含了米优速中最基本的数据结构和账户加密算法，这也是米优速的基础组成部分；

3、网络层中主要包含米优速中各节点的数据传输校验机制；

4、共识层中米优速采用基于工作量证明的共识机制；

5、激励层则将奖励机制包含进来，主要用来激励节点自主挖矿，维持米优速运行。

6、数据层、网络层、共识层、激励层也构成了基本的区块链结构。智能合约层可以说是米优速特有的，智能合约层封装了可以执行图灵完备的脚本语言的虚拟机，可以通过编写脚本语言作为智能合约部署到米优速区块链中实现应用的去中心化。

MIUSU

米优速白皮书 V1.0版