MIT 项目白皮书

version 1.6

2018 年 7 月

免责声明

请仔细阅读本免责声明。如果您对所采取的行动有任何疑问，请咨询您的法律，财务，税务或其他专业顾问。

这是一份概念性文件（「白皮书」），用来解释并说明我们所提出的 Mundellian Infrastructure Technology 平台与 MIT 代币。这份文件可能会随时受到修改或置换。然而，我们没有义务更新此份白皮书，或提供给读者任何获得额外资讯的渠道。读者请注意下列事项：

并非开放给所有人：Mundellian Infrastructure Technology 平台和 MIT 代币并非开放给所有人。参与平台和代币发售可能需要完成一系列的步骤，其中包括提供特定信息与文件。

在任何司法管辖区内不提供受管制产品：MIT 代币（如本白皮书所述）无意构成任何司法管辖区内的证券或任何其他受管制产品。本白皮书不构成招股说明书或任何形式的要约文件，也无意构成任何司法管辖区内的证券或任何受管制产品的要约或招揽。本白皮书并未经过任何司法管辖区的监管机构审查。

不提供任何建议：本白皮书并不构成关于您是否应参与 Mundellian Infrastructure Technology 平台或购买任何 MIT 代币的建议，也不应作为任何合约或购买决定的依据。

无任何声明或保证：对本文中描述的讯息，声明，意见或其他事项的准确性或完整性，或以其他方式传达与计划相关的讯息，我们不给予任何声明或保证。情况下，我们不对任何前瞻性或概念性陈述的成就或合理性给予任何声明或保证。本文件中的任何内容，均不得作为对未来的承诺或陈述之依据。在适用法律上允许的最大范围内，尽管有任何疏忽，违约或缺乏关注，任何因本白皮书的任何相关人员或任何方面而产生或与之有关的任何损失（无论是否可预见），其所有责任均可免除。但无法完全免除的责任范围，仅限于适用法律所允许的最大限度。

其他公司：除了 MIT 基金有限公司（「基金会」）及 Mundellian Infrastructure Technology 有限责任公司之外，使用任何公司及/或平台名称及商标，并不意味着与任何一方有任何关联或认可。对特定公司和平台的引用仅供说明之用。

1 前言

1.1 综述

在经济学中，有一个理论称作三元悖论（Mundellian Trilemma），也称三难选择(The Impossible Trinity)，当前的区块链也遭遇到同样类似的困境，即不可能同时具备以下三个条件：

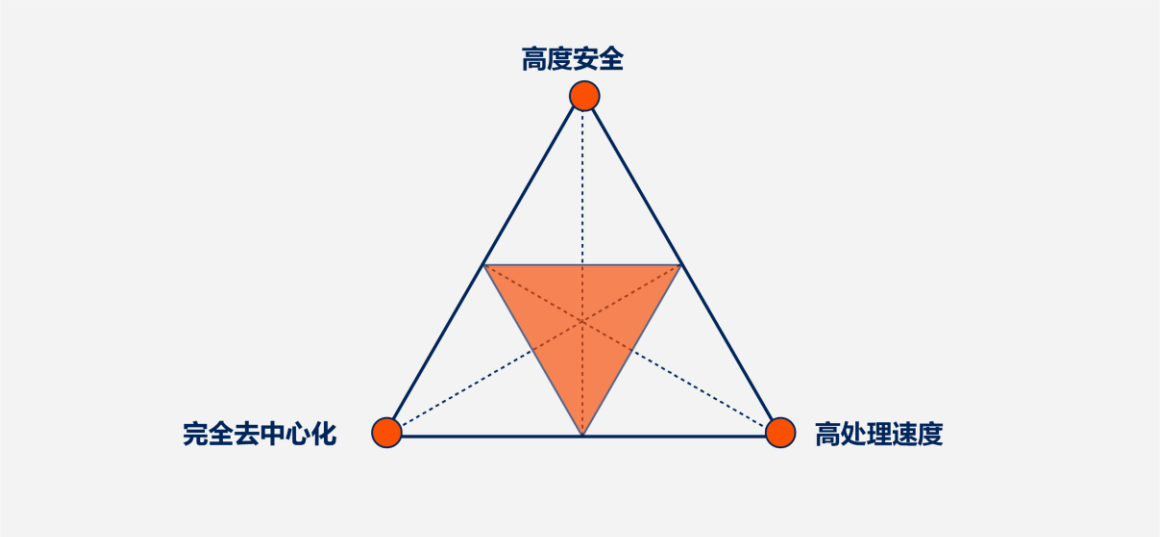

图1 区块链三元困境

比特币：完全去中心化，高度安全，但是TPS小于10；

以太坊：高度去中心化，安全性一般，发生过DAO安全事件，TPS只有20左右；

EOS：号称处理速度上百万，但是弱中心化，因为建立了21个中心化的超级节点；

根据三元悖论理论，任何新的区块链技术试图创新，要么需要限制TPS，要么弱中心化，要么降低整个系统的安全性，能否获得一个合理的平衡，甚至是兼而有之?

基于区块链技术特点，去中心化，可追朔，价值传递等，MIT将从体系架构、共识机制、分布式协议等多方面进行重大创新和改进，塑造一个全新的区块链系统。

1.2 技术背景

自从 2008 年 10 月 31 日，Satoshi Nakamoto 公布比特币（Bitcoin）白皮书[1]以来，比特币作为第一代区块链技术最大的应用，开启了比特币网络作为一种点对点的价值交换网络蓬勃发展的时代，带来了去中心化的加密数字货币，提出了建立不需要第三方介入的点对点信任关系的解决方案；

以太坊 (Ethereum) [2]作为第二代区块链技术, 包括资产数字化和智能合约，建立世界计算机，带来了去中心化的应用平台，解决了比特币区块链脚本语言过于简单的问题，代表技术是 EVM 以太坊虚拟机技术和合约编程语言，伴随创新的是大量去中心化应用的诞生，这是 DApp 阶段；

MIT 区块链提出了全新的下一代区块链底层基础性架构，建立起一个均衡扩展性、安全性、效率性等的高性能区块链平台，并形成一套自己的跨链协作技术和协议体系，以实现点对点的价值传递和链与链的协同工作。通过这些核心技术加上区块链技术本身特性去中心化，不可篡改等的特点，我们的系统将服务于供应链金融，数字资产，股权债券，供应链产品朔源，金融信贷等等各行各业。

2 MIT 综述

2.1 MIT 区块链设计动因

当前主流的区块链技术面临的主要问题：

1. 无法进行高频交易
2. 缺乏新型的智能合约平台, 目前现有的智能合约平台主要是基于 Proof of Work（POW），而 POW 的共识机制尤其高耗能，而且出块间隔较长，使得 TPS 很低，很难应用于真正的商业环境。

3. 不同区块链技术之间的兼容性，比如基于 UTXO 模型的比特币生生态和基于 Account 模型的以太坊生生态很难有兼容性。

4. 共识机制本身身缺乏灵活性，因为参与者的不同，在公有链中和联盟链中，对共识机制的要求是不一样的。

5. 数据爆炸，目前以太坊全数据已经超过 200GB，并且还在快速增长，使用压缩，扩大区块大小或采用轻节点，并不能彻底解决问题。

6. 现有区块链系统具备很大的封闭性，目前大多数的智能合约的触发条件来自于区块链系统本身，很少有来着外界的触发条件，缺乏与现实世界的交互。

针对这些当前区块链行业的挑战，MIT 链在区块链技术和理念上进行了一系列的创新：其中多侧链多子链节点群架构、模块化可替换自适应共识机制、基于分片动态权重共识算法、独立 DAG 分布式文件系统、分布式跨链通讯协议等，使得 MIT 链成为现实商业世界提供一个可以支持大规模商业应用的新一代的将人工智能最新算法和区块链技术相结合的生态世界。

2.2 核心目标

1. 提出一个解决区块链最大问题之一数据爆炸的方案

采用一个全新的框架结构多侧链多子链节点群，将应用逻辑，事务数据和生产数据进行三层隔离。主链负责 token 流转、侧链创立、及其应用逻辑运行在侧链之上的 DAPP，生产数据和业务数据的 HASH 值保存在子链中用于验证，生产数据和业务数据保存在云端或其他传统数据库上比如 DB2，MySQL，MongoDB 等。

2. 支持百万级别以上的用户群

目前像 Taobao，Facebook，Twitter，eBay 这样具有海量并发的应用，需要能够处理数以千万甚至亿计的日活跃用户的区块链技术，比如双十一的购物狂欢，非常短的时间内产生了巨大的交易量，系统可能无法正常工作甚至

瘫痪，因此提供一个可以处理大量用户并发请求的平台至关重要。

3. 支持复杂商业逻辑和用户友好的智能合约

当下主流的以太坊智能合约，支持图灵完备的合约编程语言 Solidity，并提供 GAS 消耗机制来防止死循环，但是对于复杂商业业务逻辑的支持不尽如人意，而且使用、部署和实施也非常不方便，因此 MIT 将要实现目标是：支持完备业务功能、清晰合约结果、合理的安全检查、完善的调试部署升级方案、对客户友好，开发者友好和企业友好的全新智能合约平台。

4. 基于 AI 的智能合约

MIT 区块链将目前已经获得成功的一系列 AI 规则知识库、交易模型识别、语义分析等等算法结合霍尔逻辑 (Hoare logic) 形式验证用于智能合约的设计，确保智能合约的安全性、可靠性和易用性。

5. 全新的智能合约代币消耗机制

不同于以太坊智能合约中使用消耗 GAS 的复杂计算机制，MIT 区块链采用一种全新的解决方案，即锚定一个基本稳定的参照物比如 USDT 作为计算智能合约中代码执行成本计算的方式，即定义每个指令的执行成本以法币计，消耗代币的数量=指令成本×指令数量×代币市场价格，避免了的以太坊设计两套 ETH 和 GAS 机制的复杂方案。

3 MIT 区块链系统架构

MIT区块链的架构是基于分层、模块化和微服务群。系统分为五层：

第一层是应用层

封装了区块链的各种应用场景和案例，比如搭建各类区块链应用，钱包，区块浏览器，Dapp等等都是基于Json RPC的交互API库，基于Json RPC,我们还可以创立Dapp或系统子链侧链的时候，使用弱耦合组件化可插拔可替换加微服务群的方式来搭建系统。

第二层是中间层

提供API，SDK,CLI，允许外部系统或人工智能代理进行访问和操作。区块链的各种业务合约（合约流程，合约服务）信息，区块链的各种交易结果，当前流程状态，资产状态，或者区块链的交易发生证明，资产存在证明，链上治理接口，也都可以API的方式向外部系统提供。通过API接口，也可以进行各种业务合约的操作，如人工处理的提交，合约动作交易的提交等。

第三层是区块链核心层

包含了MIT区块链的AI服务群和最重要的逻辑部分，如，共识模块，加密安全模块，存储管理模块，智能合约服务包括虚机、合约注册，生命周期管理，节点注册，账户管理，代币管理模块等等；

第四层是网络层

P2P网络协议最底层是一些通用的基础模块，比如基础加密算法，网络通讯库，流处理，线程封装，消息封装与解码，系统时间等；

第五层是硬件基础设施层

包含存储数据的硬件基础设施可以是传统的数据库SQL SERVER, DB2等，也可以是存储云或是最新的星际文件系统IPFS。底层数据区块的链式结构就封装和保存在其中，这是整个区块链技术中最底层的数据结构。

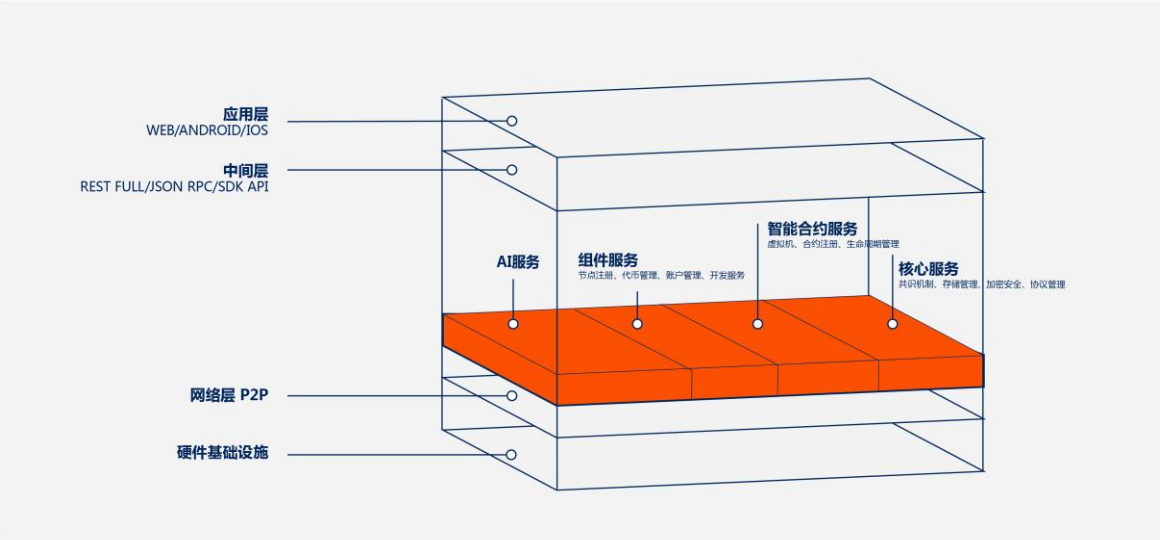

图2: MIT区块链系统架构场

4 区块链 – 技术方案

4.1 多侧链多子链群

MIT 区块链通过多侧链多子链群提高 TPS 处理速度，可以实现超过每秒 100000 次事务处理能力，同一个节点可以参与多个链,也可以同时执行多个事务,并行执行和异步通信,可以同时支持多个商业级应用，同时隔离不同的业务流程，以确保业务安全和数据安全。

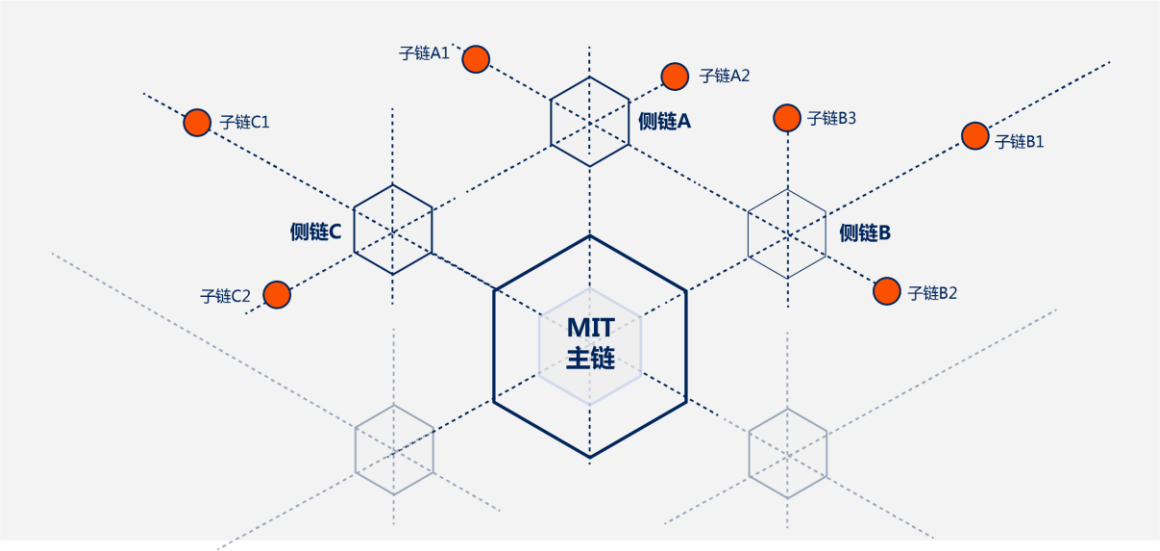

图 3： MIT 区块链网络结构图

侧链

在 MIT 区块链设计中, 每一个应用开发 DAPP 都是对应一个侧链 (Sidechain), 并且系统提供 API 来创建侧链。侧链本身在技术上是一个完全独立的区块链，可以选择自己的共识机制，数据库，交易类型以及账户系统，依据其业务逻辑决定是否发行自己的 token，承载应用的全部商业逻辑，但不保存生产数据，事务数据。

子链

子链是 Subchain，不同于侧链,子链可以作为保存各种数据的仓库，也可以

是公共服务提供者，比如可以部署 IPFS 子链，时间戳子链，真随机数子链等等。

如果应用的数据量巨大，比如很多朔源系统，需要查询商品的朔源报告，但很多商品是有时效的，例如海鲜、进口水果、红酒等等，而区块链的特性之一就是不能修改和删除数据，所以对于这类应用，MIT 区块链采用区块链加云端或其他传统数据库相结合的方式，即商品的完整朔源报告保存在传统数据仓库中，但是对其进行 HASH 计算，将 HASH 值保存在子链的区块链上，当需要验证的时候分三步，一是从外部传统数据仓库中获取完整朔源报告并计算 HASH 值；第二步是从子链上获取该商品的 HASH 值；第三步进行比对并返回验证结果。

链路间路由

MIT 区块系统中有两种链路间路由，一种是侧链之间的网络路由，另一种是子链间的路由。通信规则是：

- 侧链之间可以直接通信；
- 基于同一个侧链的子链可以相互通信；
- 目前不支持跨侧链的子链间通信，因为这会极大的降低处理速度和带来安全隐患。

4.2 代币流转机制

MIT 除了支持区块链重要的特征之一价值传输以外，不同于以太坊复杂的 GAS 机制，MIT 区块链提供一个新创的解决方案，即代码执行的成本是以一个基本稳定的参照物比如 USDT 币定价，这样即使 MIT 代币市场价格剧烈波动，每个智能合约执行成本是不变的，只是需要支付的代币数量随行就市，避免的以太坊在一个系统内设计和维持两套代币的做法。

	GAS PRICE	
PARAM	Computed	Actual
DUP	3	3
SWAP	3	3
PUSH	3	3
ADD	3	3
MUL	3	5

表 1：以太坊智能合约指令 GAS 价格

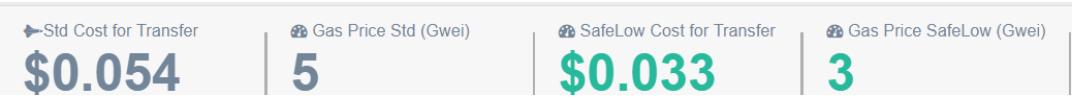

图 4：以太坊 GAS 和 ETH 之间价格汇率

例如执行一个指令成本定义为 0.00001 个 USDT，智能合约含有 1000 条指令，当前市场 MIT 对汇率价格是 1 个 MIT 对 10 个 USDT，那么整个智能合约执行共需要：0.00001×1000×10=0.1USDT，约合 0.01MIT，如果市场波动剧烈变为 1 个 MIT 对 0.001USDT，执行同样的智能合约对应的 USDT 币成本不变，但是需要支付的 MIT 数量变为 100 个 MIT。

	指令	价格(USDT)
1	ADD	2×10^{-8}
2	MUL	6×10^{-8}
3	MOD	5×10^{-8}
4	SHA3BASE	25×10^{-8}

表 2: MIT 区块链智能合约指令价格

4.3 可替换模块化的自适应共识机制

MIT 区块链系统的侧链和子链对共识机制设计是模块化，可替换的，目前绝大多数区块链系统都将共识算法固化在底层代码库中,而主流的各种共识算法,都各有优缺点。自适应是指针对不同信用等级距的节点，系统自动为其选择共识机制，以达到最优配置。

比如针对不同的子群使用不同的共识算法，例如在高度可信子链内，比如金融机构，银行等，可使用 PAXOS 或者 RAFT；在一般信任子链内，比如企业组织或银行联盟，可使用 SDWBFT，PBFT；在公链内，可使用 SDWBFT,POS，DPOS, Ripple 共识等； 开发子链内，可以不选任何共识算法，关注于业务开发。

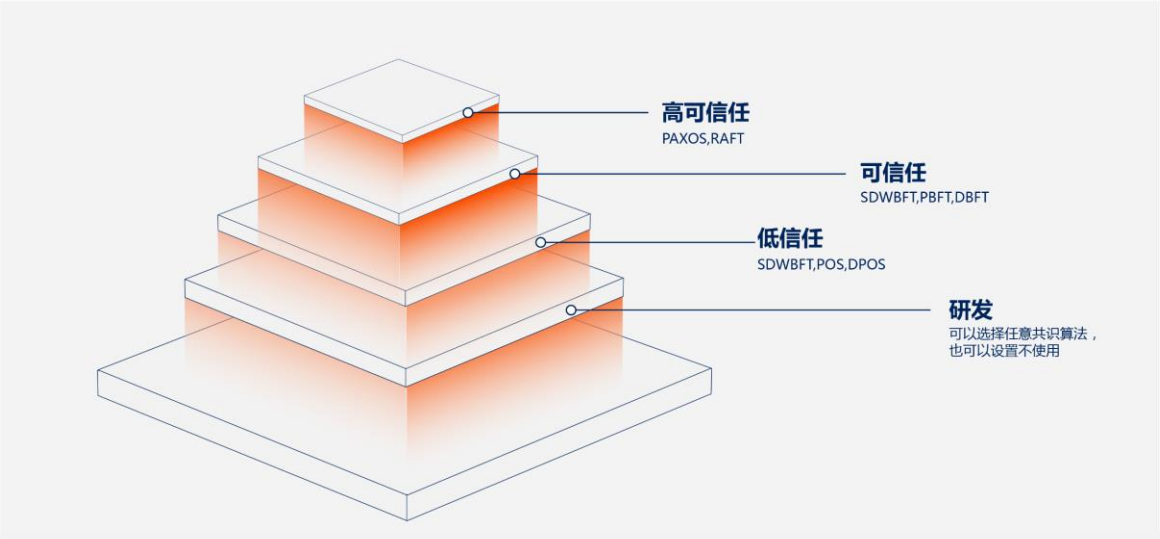

图 5: 模块化可替换机制

5 MIT 区块链技术介绍

5.1 公链共识算法

比特币网络的共识算法中由于 PoW 资源消耗过大，并且算力也越来越集中，因此 Dan Larimer 在 2014 年作为比特股的首席开发者时提出了一种快速、安全且能源消耗比较小的授权股权证明(DPoS)共识机制。DPoS 在最小化网络成本的同时，赋予每个持股人一定的投票权，由他们投票产生“超级节点”代表。最后由获得票数最多的一定数量的超级节点轮流平等地产生区块。在比特股中 Dan Larimer 选择了 101 个超级节点，但在 EOS 中选择了 21 个超级节点，主要有两方面原因：一是由于用户很难对较多数量的超级节点充分了解，所以过多的超级节点会降低用户投票的活跃度;二是规模为 20 的节点数目可以在拜占庭问题中以更低的资源成本来获得高效的共识。但是股份证明非常容易产生大股东作恶的委托而使用超级节点违背了区块链去中心化的原则，MIT 区块链采用一种新创的基于三个维度权重计算的共识算法：分片动态权重共识机制(Sharding Dynamic Weight Consensus，SDWC)：

- 节点负载；
- 网络质量；
- 节点信用；

权重计算公式。

$$W_{1,\ 2,\ 3} = W_1X_1 + W_2X_2 + W_3X_3;$$

W = 相对权重（%）

X = 归一化后数值

指标名称	权重	数值范围	说明
节点信用	80%	0-100000	越大越好
节点负载	10%	0-1000	越小越好
网络质量	10%	0-1500	越小越好

表 3: 权重示例表

信用数值归一化公式

$$x' = \frac{(x+1) - min}{max - min}$$

*X 为数据原值

负载和网络质量归一化公式

$$x' = \frac{1}{Log\,(x+1) + 1}$$

*X 为数据原值

节点选择分配原则：

- 80%节点从权重分值最高节点中选择
- 20%节点随机从低权重的节点中选择
- 百分比动态可调节

信用积分原则：

- 每次被选中节点按时间出块，则增加信用
- 节点作恶信用清零
- 节点未按时间出块，信用降低

SDWC 算法的优势：

- 平衡全网算力即避开高负载节点，优先让负载低的节点来验证和出块
- 鼓励新加入节点，采用更好的硬件和高速稳定的网络
- 选择 20%新节点是为了奖励和鼓励新注册节点，从而防止老的节点垄断铸币。
- 防止恶意节点，防止 51%攻击，防止大股东作恶。

在确保共识过程公平的前提下，平衡处理速度，安全，去中心化，提供一个高效，高可用性的共识机制。MIT 区块链之所以不采取超级节点的做法是因为，建立超级节点本身就有违区块链去中心化的初衷，如果超过 10 个超级节点被伪冒或入侵，系统就彻底瘫痪或被劫持。

5.2 基于 AI 的智能合约

5.2.1 当前智能合约技术缺陷

以太坊为代表的智能合约，从用户角度来讲，实际上是一个无人值守、程序执行、具备自动担保的状态机，只是当特定的条件满足时，能够自动释放和转移资金。智能合约从技术层面来讲就是一种网络服务，是通过区块链共识，完成特定的合约程序执行。由于是共识，区块链上的任意智能合约代码和状态必然都要公开，都要经受公开的检验。在软件开发行业平均每 1000 行就含有一个安全漏洞，而以支持图灵完备的以太坊智能合约为代表的新新事物，虽然具有完备性和灵活性，但是代码的可靠性和安全性却成为很大问题，例如发生在 SMT 的加法溢出漏洞和 BEC 的乘法溢出，导致黑客利用智能合约漏洞窃取巨额数字货币。

当前以太坊的智能合约主要缺点:

- 代码容易产生漏洞，缺乏安全保障
- 智能合约不够智能，非常不易用
- 不能获得外部信息，无法和外界安全有效沟通。

5.2.2 MIT 区块链智能合约设计原理–人工智能局限性

目前 AI 技术依然处于弱人工智能时代，当前市场上各种人工智能的项目层出不穷，但是各种夸大其词以至于大众对 AI 有些脱离实际的期望。

但是 MIT 区块链项目是着眼于可以实现的，为当下大规模商业应用提供可以落地的区块链技术基础性框架结构。通过广泛的调研和深入的探索，我们认为以当前的 AI 技术水平试图对一个图灵完备的编程语言通过无论是基于“机器学习”，“神经网络语义分析”等等算法产生一个类似“全自动编程”功能完全自动的智能合约验证，目前是不可能实现的。

所以现阶段试图对以太坊（Ethereum）的智能合约语言（Solidity）进行形式验证，号称要用严密的数理逻辑方法，全自动的验证以太坊智能合约的正

确性，有效性和安全性，是不切实际的。

基于以上判断，MIT 区块链提供一种解决方案，创造一种新的非图灵完备的合约语义处理语言（CLP），让人工智能系统接触各种不同合约。一旦系统掌握了某个合约术语，训练人员就会指出其他需要识别的概念。CLP 技术让算法识别概念成为可能，即使这些概念以（系统）前所未见的方式出现，为此，MIT 区块链采用了概念+断言（关键词）监测的办法。人工智能可以识别某个概念，无论这个概念以何种方式表达出来或者出现在何处，如此以来，MIT 区块链的人工智能系统就能以一种远比关键词搜索更为成熟的方式运行。

5.2.3 MIT 区块链智能合约设计原理–霍尔逻辑形式验证

基于非图灵完备的 MIT 区块链独有的 CLP（合约语义处理语言），MIT 区块链系统将采用霍尔逻辑（Hoare Logic），又称弗洛伊德–霍尔逻辑（Floyd—Hoare logic），是一种形式验证（formal verification）的方法。这个系统的用途是为了使用严格的数理逻辑推理来替计算机程序的正确性提供一组逻辑规则，霍尔逻辑的中心特征是霍尔三元组（Hoare triple），其提供了如下公理和推理规则：

部分正确性（Partial Correctness）

- 空语句公理

  $$\frac{}{\{P\}\ \mathbf{skip}\ \{P\}}$$

  如果 P 在一个空语句之前成立，那么在执行这个空语句之后也是成立的。 ”skip”在这里表示空语句（Empty statement）。

- 赋值公理模式

  $$\frac{}{\{P[E/x]\}\ x := E\ \{P\}}$$

  对赋值右端的变量的以前为真的任何命题在赋值之后仍然成立

- 顺序规则

  $$\frac{\{P\}\ S\ \{Q\}\ ,\ \{Q\}\ T\ \{R\}}{\{P\}\ S;T\ \{R\}}$$

- 条件规则

$$\frac{\{B \wedge P\}\, S\, \{Q\}\,,\ \{\neg B \wedge P\}\, T\, \{Q\}}{\{P\}\ \textbf{if}\ B\ \textbf{then}\ S\ \textbf{else}\ T\ \textbf{endif}\ \{Q\}}$$

- 推论规则

$$\frac{P' \rightarrow\ P\,,\ \{P\}\, S\, \{Q\}\,,\ Q \rightarrow\ Q'}{\{P'\}\, S\, \{Q'\}}$$

全部正确性（Total Correctness）

- 全部正确性的 While 规则

$$\frac{\{P \wedge B \wedge t = z\}\, S\, \{P \wedge t < z\}\,,\ P \rightarrow t \geq 0}{\{P\}\ \textbf{while}\ B\ \textbf{do}\ S\ \textbf{done}\ \{\neg B \wedge P\}}$$

为解决智能合约的安全性和有效性问题，结合霍尔逻辑的形式验证给出三步解决步骤：

- 前置分析（Pre-Condition）：合约编写过程中的规范化与合约发布的漏洞分析检查；
- 执行和验证：在 MIT 智能合约虚拟机中完成合约命令的执行，以及动态安全和有效性验证；
- 后置检测（Post-Condition）：对智能合约执行结果进行后置分析及审计，确保执行结果必须落在智能合约所指定的结果范围内，而不会出现偏差。

5.2.4 MIT 区块链智能合约技术实现

MIT 区块链将人工智能中多种技术应用于智能合约的设计，并给出解决当前智能合约各种缺陷的对策，主要包括：

- 基于规则知识库的语法检查

将合约文本文件，通过内置编译工具，将对合约构建一棵基于 BNF 范式基础上的抽象语法树（AST），通过该语法抽象树，便可以对合约内容展开语法识别，进行简单的合约安全识别。目前建议按照递归下降分析的方法，对语法抽象树进行基于知识规则库的检查，从而确定是否存在安全隐患。

- 基于语义分析 NLP 的交易模型识别与安全检查

基于语法的安全检查规则仅能静态识别合约缺陷，而基于语义分析的交易模型识别与安全检查，则主要通过上下文相关审查，确定智能合约中不满足规则或者不安全的操作。目前支持的安全检查包括：类型检查，控制流检查和一致性检查。

通过上述静态语义分析，能够基本排除由于人为书写智能合约带来的各种表层的逻辑缺陷，但尚不能解决动态执行过程中出现的各种逻辑问题。

- AI 辅助的形式验证以及动态约束

在合约验证上，采用基于 AI 辅助的形式验证以及动态约束检查的方法，解决上述安全问题。其核心思想包括：利用模式匹配获得用户真实需求约束、对静态语义分析形成的抽象树，按照贝叶斯分类器进行模型分类，确定树中的各段分支属于对应的类属，根据模式匹配结果和人工智能分类结果，获得当前合约的全部静态与动态约束，基于该约束即可生成合约代码的断言，并基于该结果进行形式验证和动态验证。

- 基于 AI 形式验证的智能合约安全性检查

MIT 区块链使用形式验证技术对智能合约的安全性进行自动化检查。其中，形式验证模型使用 F*函数程序语言（Functional Programming Language）建立，该语言整合了 Z3 求解工具，输入格式是 SMT-LIB2.0 标准，拥有丰富的类型和条件检查功能。

使用人工智能方法自动识别程序语义并发现其中的典型模式，从而根据模式自行产生为了满足安全要求而需要的属性。当用户提供智能合约以及翻译后的执行代码后，MIT 的 AI 引擎将自动完成代码的局部相似性匹配和全局相似性匹配，从而推测代码的行为模型。根据 AI 获得行为模型，生成对应的形式验证约束，从而进行深层次的行为验证，实现代码安全性。

5.2.5 虚拟机和沙盒

沙盒(Sandbox)是一种按照安全策略限制程序行为的执行环境。早期主要用于测试可疑软件等，比如黑客们为了试用某种病毒或者不安全产品，往往可以将它们在沙箱环境中运行。经典的沙箱系统的实现途径一般是通过拦截系统调用，监视程序行为，然后依据用户定义的策略来控制和限制程序对计算机资源的使用，比如网络调用，IO 读写等等。

MIT 区块链系统设计了全新的 MVM (MIT Victual Machine) 实现沙箱机制。MVM 包含了调用 AI 微服务的分析模块，和文本语义智能合约翻译模块，以及执行翻译后的智能合约的引擎，可以用来执行翻译后字节代码，使用系统层的 API, 比如网络传输相关的模块, 但是不允许第三方库, 这就需要 DAPP 的开发者使用 MIT 提供的 SDK 包通过网络协议的方法为从安全的侧链获取信息，这样兼顾了安全性与功能的完备性。

5.3 分布式跨链协议

MIT 区块链的跨链协议（Cross Blockchain Protocol）主要包括两个部分：消息地址和消息包。协议地址包括消息来源链的链标识（srcChainID）和当前链高度（Height）。消息包则由两个部分：消息包头（MessageHeader）和消息体（MessageBody）组成。其中，消息头包括了，起始链标识（srcChainID)，目标链标识 (destChainID)，消息状态 (MessageStatus)，消息有效时间（MessageValidDuration)，触发交易等。

消息状态对应的是网络消息协议中的消息状态机制。当一个消息包被发送的时候，消息状态是“接收待定”。当接收方收到消息，会返回给发送方一个消息包，其中消息状态为“发送成功”，若发送方收到了含有“发送成功”标识的消息包，发送方会再回复给对方一个含有“接收成功”标识的消息包。以上便是一次成功消息的。如果过程中，有消息包接收失败，如，接收方一直不回复“发送成功”，则发送方会在一定时间后重发交易，试图再次建立通信。

除上述状态外，我们还规定了“连接超时”状态。当一笔交易从侧链 A 发往侧链 B 时，会标明其指定的以链路由区块高度为准的消息存活时间。在到达消息存活时间之前，链路由会将消息结果的状态返回给侧链，若超过消息存活时间，则链路由直接返回给发送方“连接超时”状态。发送方侧链将该次消息记录为消息失败。

6 MIT 区块链应用领域

目前 MIT 区块链分成两个部分，第一是区块链底层基础架构；第二是上层针对多个行业的应用，MIT 区块链将与世界上多个行业的多个企业和机构合作开发并落地多个基于 MIT 技术的实际项目，并将对相关行业进行深入挖掘和拓展，为各行各业提升效率和降低成本提供一个坚实的区块链基础架构。以下是几个即将在 MIT 区块链上的应用案例。

6.1 供应链金融

供应链金融是一个具有十万亿级别规模的巨大市场，从国家统计局的公开数据来看，2017 年年末我国工业类企业的应收账款余额为 13.48 万亿元人民币，2016 年年末我国工业类企业的应收账款余额为 12.58 万亿元人民币，同比增长 8.5%。从近 5 年的全国工业类企业应收账款的年末余额来年看，每年的期末余额都呈递增的趋势，无论是前景还是成长空间都足够高。目前行业痛点主要是：

- 中小企业融资困难，成本高；
- 金融汇票流通困难；
- 信任风险始终存在，风控成本高；
- 核心企业角色太重，议价能力太高。

供应链金融是典型的需要多方参与和合作，但是受制于整个供应链行业对外的低透明度，以及信息不对称，信用机制不完善等，而且又没有一个传统中心化的机构在治理，因此借助 MIT 区块链、大数据、人工智能、物联网等新一代信息技术的发展推动传统供应链金融向数字化、智能化的转型，更好的将信息流、资金流、物流整合分析，建立动态信用评价体系，从而实现资金的高效率、高质量投放。供应链金融将走向以数字化的形式，智能化的方式，并依托于区块链的范式，协助构成未来的产业生态。

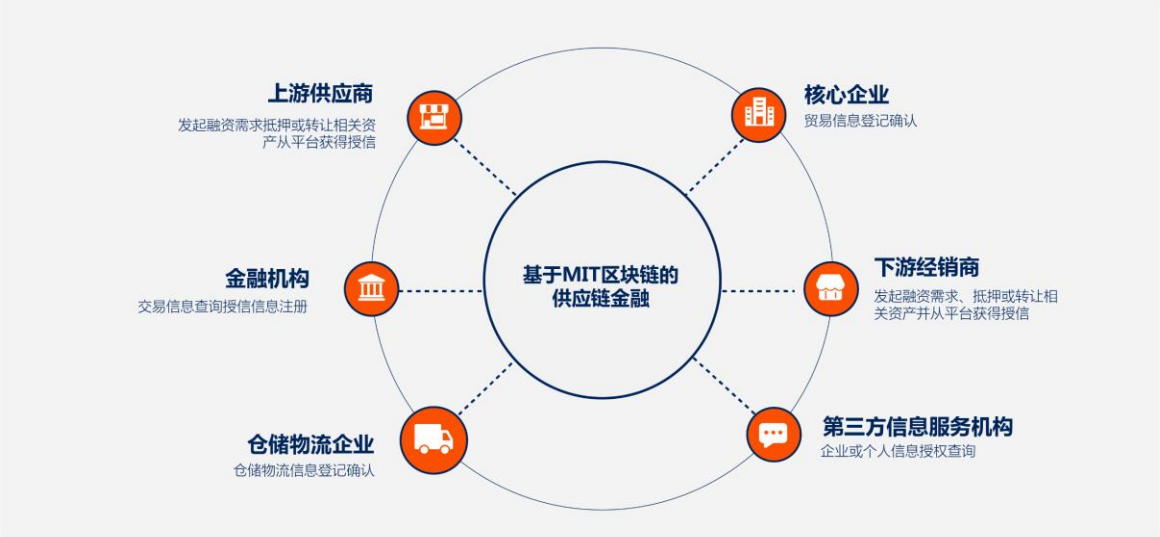

图 6: 供应链金融业务架构

6.2 资产数字化

相比于传统中心化系统， 区块链应用于数字资产领域的优势在于：资产一旦在区块链上发行，后续流通环节可以不再依赖发行方系统， 在流通中，资产由单中心控制变成社会化传播，任何有资源的渠道都可能成为资产流通的催化剂。因此，区块链能极大地提升数字资产流通效率真正达到“多方发行、自由流通“。

传统的资产服务，需要相应中间商如资产所有者证明、真实性公证等均需要第三方的介入才可以完成整个流通过程。在目前的模式中存在以下几个痛点：

（1）资产进入流通后，仍必须依赖资产发行方系统才能完成使用、转移，这就将资产流通范围限制在发行方系统用户群内；

（2）传统的资产流通渠道有限，几乎都依赖于大渠道 ，行业大渠道由于垄断地位大幅增加费用，从而导致流通，成本显著提高，小渠道及个人难以在流通环节发挥作用。

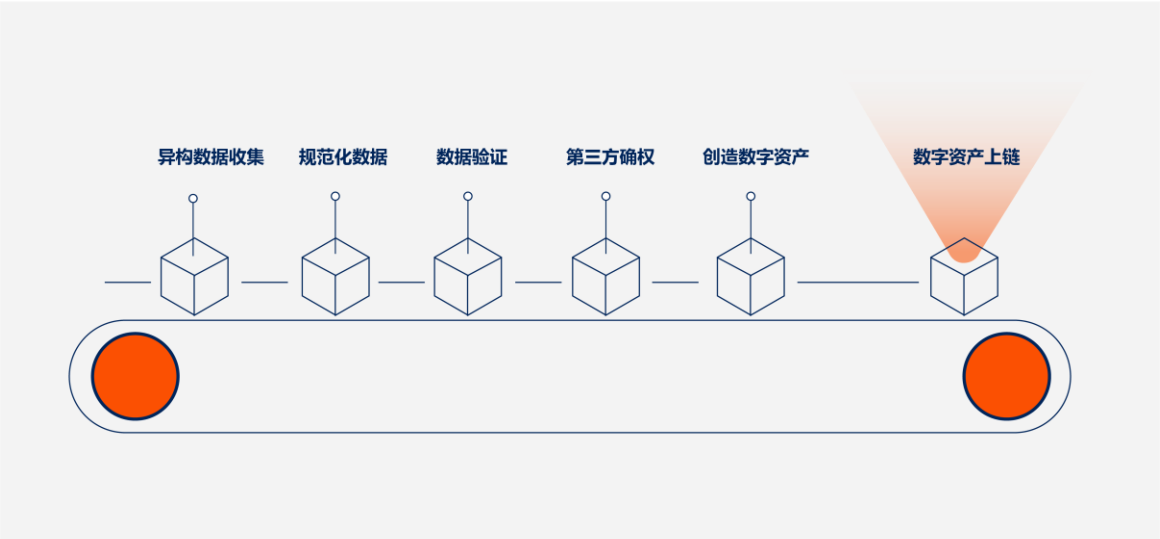

图 7：资产数字化流程

6.3 产品朔源

目前市场上假冒伪劣产品越来越多，如地沟油，毒豆芽，假奶粉，各大电商 XX 优品也频频传出假冒商品。受害最大的自然是消费者，特别是买到假冒伪劣的食品药品，会对我们的人体产生危害。同时对企业声誉也会产生危害，被假冒的品牌，销量将会大幅下降。因此溯源在社会生活中起着重要作用，能够实现产品从原料、生成加工到物流、销售等整个供应链上的追溯功能，一旦发生相关事故，监管人员就能够通过该系统判断企业是否存在过失行为，企业内部也可借助该系统查找是哪个环节、步骤出现了问题，使问题得到更快解决。MIT 区块链将物联网，区块链，智能防伪等技术进行有机结合，利用区块链公开透明、无法作弊、不可篡改、信息安全等技术特性，解决各行各业供应链信息不透明的问题，从源头解决消费品信任问题，保障消费者利益的同时实现目标客户的品牌价值增长。

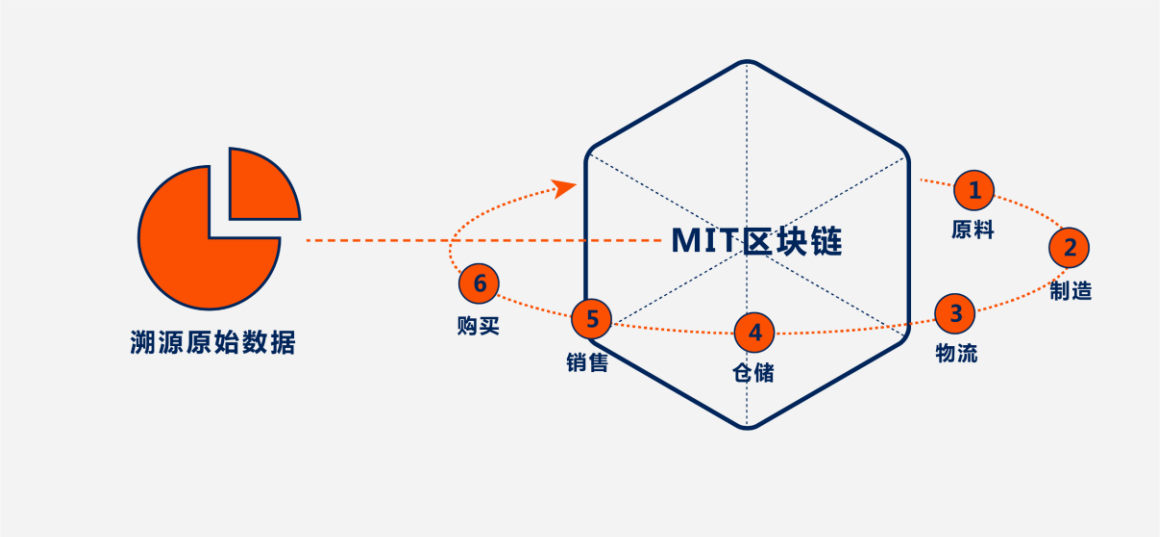

图 8: 产品朔源业务流程

7 MIT 团队核心及顾问

Jason Huang

CEO 首席执行官

清华大学计算机软件专业博士

曾任职于朗讯、CA、微软等知名科技企业

区块链领域优秀的技术专家，十多年从事分布式系统、云计算及通信标准设计开发。2006 年通过 BSIS 算法创造 PennySort 世界排序大赛世界纪录，并由美国工程院士 Jim Gray 和中国工程院院士孙家广亲自颁奖。

Adam Mallet

CTO 首席技术官

计算机科学硕士

澳大利亚昆士兰大学

曾任职于 IBM 和惠普. 高级架构工程师.

区块链领域技术专家. 2010 年加入 BTC 社区.

Si Wei

CIO 首席信息官

AI 人工智能博士

澳大利亚国立大学

NASA 资深技术专家

在 NASA 主导全球顶尖数据溯源标准 PROV3.0 并主导开发 PROV4.0 标准.

Richard Fang

COO 首席运营官

昆士兰大学金融硕士，银行金融硕士；

数家供应链、生鲜冷链企业创始人、经营者，资深投资人；从事供应链行业十余年，拥有丰富的行业经验，对整个行业的运营细节具有深刻独到的见解。

Alexander Kristensen

首席顾问

工商管理硕士

英国爱丁堡商学院

计算机科学及 MBA 专业，斯堪的纳维亚银行高级风险控制顾问，对冲基金模型设计专家

8 路线图 Road Map

2018 Q1	2018 Q2	2018 Q3	2018 Q4	2019 Q1	2019 Q2	2019 Q3	2019 Q4
塑链项目开始启动	为塑链项目选择和设计公链技术路径	塑链技术白皮书完成	基于CLI的PC端钱包	基于IOS的移动钱包	MIT主链pre-α版本	MIT主链α版本上线	MIT主链β版本上线
研究和分析现有各个公链的优缺点	开始技术白皮书撰写	项目网站v1.0完成	MIT区块链浏览器	基于Android的移动钱包	将共识引擎结合共识算法进行联调	包括CBP分布式跨链协议验证和实现	包括实现主链分片和轻节点
	确定战略合作方	为项目通证创建基于ERC20的Solidity脚本并执行	分片动态权重共识算法验证和实现	MIT区块链主链内核开发	MIT网络文件系统	跨侧链间路由协议验证和实现	实现基于语义分析 NLP 的交易模型识别与安全检查
			Github上发布开源代码并持续更新	P2P网络协议开发	MIT主链部署，调试和回滚机制	跨子链间路由协议验证和实现	通过Z3 和使用 F* 函数程序语言，实现霍尔逻辑的形式验证
				账本数据块存储底层开发	MIT侧链验证和开发	非图灵完备的CLP（合约语义处理语）验证和实现	Dapp集成开发环境
				运行环境开发	多侧链支持	实现通过基于BNF范式基 础上的抽象语法树（ AST ）	可插拔和模块化的各种共识算法
				测试网络开发	MIT子链验证和开发		
				共识算法测试	多子链支持		
				共识引擎设计和验证			
				共识引擎实现			

9 TOKEN 分配计划

MIT 总计设置 100 亿枚，分配计划如下

比例	分配对象	用途及说明	冻结及限制
40%	众售	项目开发，运营及投资者回馈	无冻结无限制条件
10%	早期投资机构	早期投资人和投资机构	冻结一年，第二年起每月最多出售总量的2%
10%	创始及开发团队	开发团队	冻结一年，第二年起每月最多出售总量的1%
		管理委员会	
10%	投资人及项目保障	为保障投资人及项目支持者利益，提供的奖励或共享	不出售，无偿奖励
10%	合作机构	鼓励合作商业机构及社区	不出售，无偿奖励
20%	商业落地及推广	用于项目应用及商业推广	不出售，无偿奖励

10 风险披露

货币监管风险

各国政府仍在设计关于将加密货币作为一种贸易结算形式进行监管的公共政策。对本地商业使用加密货 币扩散的政府可能会发布法律和法规，认为使用密码币是一项受规管的活动。近几周来，中国和韩国等 国家已经发布了禁止代币销售的规定或声明，而其他国家则试图将代币销售作为证券发行监管。这可能 导致 MIT 代币的持有人在 MIT 代币未进一步推进合规性的情况下未来无法使用他们的 MIT 代币。

与代币/众筹销售有关的风险

MIT 代币不是投资产品。确切的说，MIT 代币可以在 MIT 系统中提供特定的功能。如果没有 MIT 代币，普通大众可能无法访问 MIT 系统。MIT 代币也未

见未来的利润或收益。由于这些原因和其他原因，我们认为，MIT 代币的销售并不构成符合公开发行募股说明书注册要求的证券。然而，代币销售的公共政策正在发生变化，而且可以想象，监管机构未来可能会扩大代币销售的监管范围。这可能使代币销售受到美国和类似司法管辖区的注册要求。如 MIT 代币销售受到注册要求的限制，这可能会耽搁或无限期推迟所提出的 MIT 代币的销售。

税务风险

使用 MIT 代币作为一种结算货币可能会受到当地所得税，资本利得税，增值税或其他形式的税收的限 制。税收立法的这种不确定性可能会使商家和客户面临与使用 MIT 代币作为结算货币和/或代币交易或 Well 代币资本利得有关的不可预见的未来税收问题。

资本控制风险

许多司法管辖区，如中国，对跨境资本的流动实施了严格的控制。MIT 代币持有人可随时会受到这些规定和/或被强制执行此类规定的约束。这会使把 MIT 代币从某些司法管辖区转移到海外交易所成为一种会使 MIT 代币的使用者受到政府处罚或其他监管制裁的非法活动。

CTF 和反洗钱条例

美国已经出台了一系列打击恐怖主义融资和洗钱活动的规定。许多其他国家已经制定了类似的法律来控制这些非法活动的资本流动。在这种情况下，任何 MIT 代币的非法使用（如被不法分子用于洗钱活动）都可能严重影响 MIT 网络在国际上的声誉。这可能会导致 CTF 和反洗钱监管机构的审查，并可能对 MIT 生态系统中的代币和 MIT 代币的分配和流通造成重大的负面影响。

区块链风险

在以太坊网络中，由于出块时间是由工作量证明决定的，因此出块时间是随机的。买方确认并理解，以太坊智能合同可能不会在买方预期的时间打包买方的交易，而且买方不会在买方发送 ETH 的同一天收到了 MIT 代币。 以太坊区块链可能会出现周期性的堵塞，在这种情况下，交易可能会延迟或丢

失。个人也可能故意作乱堵塞以太坊网络以在购买 MIT 代币上获利。买方承认并了解，以太坊矿工可能不会在买方想要的时候打包买方交易，或者根本就不会打包买方的交易。MIT 代币可能会丢失和/或被盗。黑客或其他恶意团体 或组织可能会尝试以各种方式干扰 MIT 网络或 MIT 代币的发放和流通，包括但不限于恶意软件攻击，拒绝服务攻击，基于共识的攻击，Sybil 攻击， smurf 攻击和电子欺诈。此外，由于以太坊平台依赖于开源软件，而且 MIT 网络也基于开源软件，因此，以太坊智能合约可能会包含有意或无意的漏洞或弱点，这可能会对 MIT 代币产生负面影响，或导致买方的代币丢失，买方丧失访问或控制其购买的代币的能力，或者买方帐户中的 ETH 丢失。如果出现这样的软件错误或缺陷，公司可能无法提供任何补救措施，并且公司不能保证 MIT 代币的持有人会获得任何补救措施，退款或赔偿。该白皮书中提出的所有事项都是全新的且未经测试的。因此，该项目可能无法完成，实现或启动。 即使项目已经完成，实现并启用，它可能不会按照预期的方式运行，并且任何与采用该项目的区块链相关的代币可能不具备预期的功能或价值。而且，由于技术发展迅速，所以 MIT 网络或代币可能会过时。加密货币，数字资产和区块链技术的监管状况在许多司法管辖区尚不清楚或不明确。所以很难预测政府当局将如何对这些技术进行监管，以及政府当局是否会对影响加密货币，数字资产，区块链技术及其应用的现有法律，法规和/或规则进行任何修改。这种变化可能会以各种方式对 MIT 网络和代币产生负面影响，其中包括例如确定代币是受管制的金融工具，需要注册。如果政府行为使其不合法或继续经营项目 在商业上不可取，公司可能会停止发放 MIT 代币以及项目的开发或停止项目在某个管辖区的运营。

商业风险

公司计划在收到足够的资金后停止代币的销售。如果公司从销售 MIT 代币中筹集的金额少于一定数额，本公司可能没有足够的资金来实现其商业计划，而且购买代币的买家所面对的投资风险将更高。

本公司保持竞争力的能力可能一部分取决于其开发新产品和/或增强现有产

品或服务，并及时以一种性价比高的方式推出这些产品或服务的能力。此外，本公司竞争对手产品和服务的推出，增强或其他技术的使用可能会导致本公司现有产品和服务的销售或市场接受程度的下降。 我们不能保证公司能在选择，开发和推广新产品和服务，或者增强现有产品或服务方面取得成功 。如果不成功，可能会对公司的业务，财务状况和运营业绩产生不利影响。

公司实现目标的能力取决于其吸引和留住更多高质量人才的能力。对于这些人才的竞争是十分激烈的，而且 我们不能保证公司的业绩不会因无法吸引和/或留住合格人才而受到不利影响。

公司所在的行业是全新的行业，可能会受到高度的政府监督和审查，包括调查或执法行动。我们不能保证政府机关不会审查公司的运营情况和/或对公司采取执法行动。此类政府活动可能或可能不是特别针对公司的结果，但所有这些活动都可能导致公司受到判决或处罚，或公司重组其业务和活动，或停止提 供某些产品或服务，所有这些都可能会损害公司的声誉或提高公司的运营成本，而且可能对 MIT 代币和/或项目的开发产生重大的不利影响。

12. 联系我们

您可以通过以下方式联系我们，以随时获得有关 MIT 平台及其代币发售的最新资讯。

官方网站：　MIT.club

邮箱：　info@MIT.club

微信：　MITclub

Telegram：　Blockchain MIT@mitblockchain

Facebook：　MIT Club

Twitter：　Mitclub

Github:　MITFC

13. 参考文献

[1] S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, Bitcoin.org, 2009.

[2] Buterin, V. (2014). A next-generation smart contract and decentralized application platform.

[3] T. Stein, Supply chain with blockchain — showcase RFID, Faizod, 2017

4. R. Hackett, The financial tech revolution will be tokenized, Fortune, 2017.

[5] D. Bayer, S. Haber, W.S. Stornetta, Improving the efficiency and reliability of digital time-stamping, Sequences II: Methods in Communication, Security and Computer Science, 1993.

[6] A. Back, Hashcash — a denial of service counter-measure, Hashcash.org, 2002.

[7] B. Dickson, Blockchain has the potential to revolutionize the supply chain, Aol Tech, 2016.

[8] KCDSA Task Force Team, The Korean certificate-based digital signature algorithm, IEEE Standard Specifications for Public-Key Cryptography, 1998.

[9] R. T. Clemen, Incentive contracts and strictly proper scoring rules. Test, 2002.

[10] J.-Y. Jaffray, E. Karni, Elicitation of subjective probabilities when the initial endowment is unobservable, Journal of Risk and Uncertainty, 1999.

[11] Blockchain Luxembourg S.A., https://blockchain.info.

[12] J. Gong, Blockchain society — decoding global blockchain application and investment cases, CITIC Press Group, 2016.

[13] D. Johnston et al., The general theory of decentralized applications, Dapps, 2015.

[14] P. Sztorc, Peer-to-peer oracle system and prediction marketplace, 2015.

[15] R. Hanson, Logarithmic market scoring rules for modular combinatorial information aggregation, Journal of Prediction Markets, 2002.

[16] Goldman Sachs report Blockchain Putting Theory into Practice, EQUITY RESEARCH | May 24, 2016.

[17] IBM 区块链技术（Blockchain）简介---z Systems China Client Council, for ICBC, Mar. 2016