# MATRIX，开启区块链 3.0 时代

## MATRIX 项目白皮书

【MATRIX 是新一代的区块链技术，它创新性地将人工智能技术引入了区块链产业，将而这两者紧紧地结合在一起，打造出跨时代的产品。】

MATRIX 项目理事会

www.MATRIX.space

# 版权声明

**本白皮书由 MATRIX 团队编写，严禁抄袭，如需转载，请注明出处。同时本白皮书中所涉及到的所有的产品设计理念、技术设计方案以及技术解决方案，其知识产权，均属于 MATRIX 团队，团队已对核心的技术方案部分申请知识产权保护，对于任何侵犯 MATRIX 团队知识产权的行为，本团队将通过法律手段保护我们的权益，望周知。**

**MATRIX 项目理事会**

# 内容摘要

MATRIX 是一个跨时代的区块链产品，团队作为人工智能区块链的首创者和践行者，历史性地将人工智能技术和区块链技术结合在一起，目标是用 MATRIX，来正式定义下一代区块链技术。在我们看来，要成为符合时代应用及技术发展需求的区块链 3.0 技术，需要具有以下四个特点：量化处理定性问题的能力、广泛为一般用户接受和使用的能力、自然进化的能力以及将算力公益化的能力。

与传统区块链技术不同，人工智能技术的介入，让 MATRIX 真正拥有了生命力，“他”将不断地通过学习和应用实践，来进化自己的算法和体系，从而不断地升级，这种自然进化的能力，将让 MATRIX 永远可以适应时代的需求，领先技术的潮流。

MATRIX 通过人工智能技术，大幅提升了智能合约的可用性和适用范围，让智能合约在本质上进行了升级，同时人工智能的介入，可以自动地对合约条款进行升级和纠错，大大提升了合约的合理性和安全性。在 MATRIX 网络中，智能合约已经不是处理简单的一般性条款的计算机语言，而是真正地拥有了面向用户为用户提供安全、智能的协同服务的能力，我们把这个全新的功能，称为“安全智能协同”。

在“自然进化”和“安全智能协同”作为核心功能的基础上，MARTIX 打造了一个完整的生态，“他”不仅是一款能够在区块链上实现智能协同、开源的底层系统，同时打造了一个平台并提供了相应的编程语言，使开发人员能够利用人工智能算力和区块链技术来建立和发布下一代分布式应用，也为每一个普通用户提供了方便地使用智能协同功能的开放式工具。从 MATRIX 开始，区块链技术将真的开始可以为每一个人服务，全民受惠于区块链技术的时代将正式拉开序幕。

# 目录

# 1 前言：MATRIX，开启区块链 3.0 时代

**比特币：区块链 1.0——加密货币时代**

2009 年 1 月 3 日，区块链技术的创造者——中本聪先生发布了开源的第一版比特币客户端；同日，世界上第一个比特币区块链诞生、首批 50 比特币同时被创造出来，这标志着比特币网络的正式成立，作为比特比的底层技术——区块链也作为下一代的网络技术正式登上历史舞台。比特币网络开创了一个全新的时代，中本聪先生用超越时代的理念建立了一个去信任化、去中心化、分布式自治的网络社会。比特币可以称为区块链的开山鼻祖，也可以看做区块链 1.0 时代的里程碑——加密货币时代。虽然有着远超于所在时代的智慧和理念，但中本聪先生创造技术仍然拥有相应的局限性，例如在设计比特币的时候，中本聪先生并没有想到区块链会成为一项划时代的技术，在未来被如此广泛地商业化应用，所以比特币网络从这个角度来看，在现在已经无法满足时代的需求，无法真正地为大规模商业化应用提供支持，但尽管如此，比特币仍然是作为加密货币核心价值定位的标杆。

**以太坊：区块链 2.0——规模应用时代**

2013 年年末，以太坊创始人 Vitalik Buterin 发布了以太坊初版白皮书，正式拉开了区块链 2.0 时代的序幕。与初期目标只服务于加密货币的比特币不同，以太坊引进了智能合约的概念，从真正意义上可以满足商业化应用发布的需求：以太坊可以用来编程，分散，担保和交易任何事物，如：投票、域名、金融交易所、众筹、公司管理、合同以及大部分的协议、知识产权以及各种得益于硬件集成的智能资产。以太坊可以看做是区块链 2.0 时代的标志。

**MATRIX：区块链 3.0——区块链全行业、平民化应用时代**

随着近年来区块链技术的爆炸性增长，以及更广泛的被各行各业所应用，同时无论是 DAO 事件，还是以太坊前段时间的大规模阻塞，都在提醒我们当前区块链技术的不足，区块链产业再次来到十字路口：区块链的下一步怎么走？如何定义区块链 3.0 时代？

随着 AlphaGo 战胜了当前人类围棋第一人——柯洁，人工智能时代正式拉开大幕，两个划时代的技术同时走上时代舞台，我们认为这并不是巧合，于是我们选择将这两个炙手可热的技术结合在一起，让区块链技术插上 AI 技术的翅膀，正式开启区块链 3.0 时代。

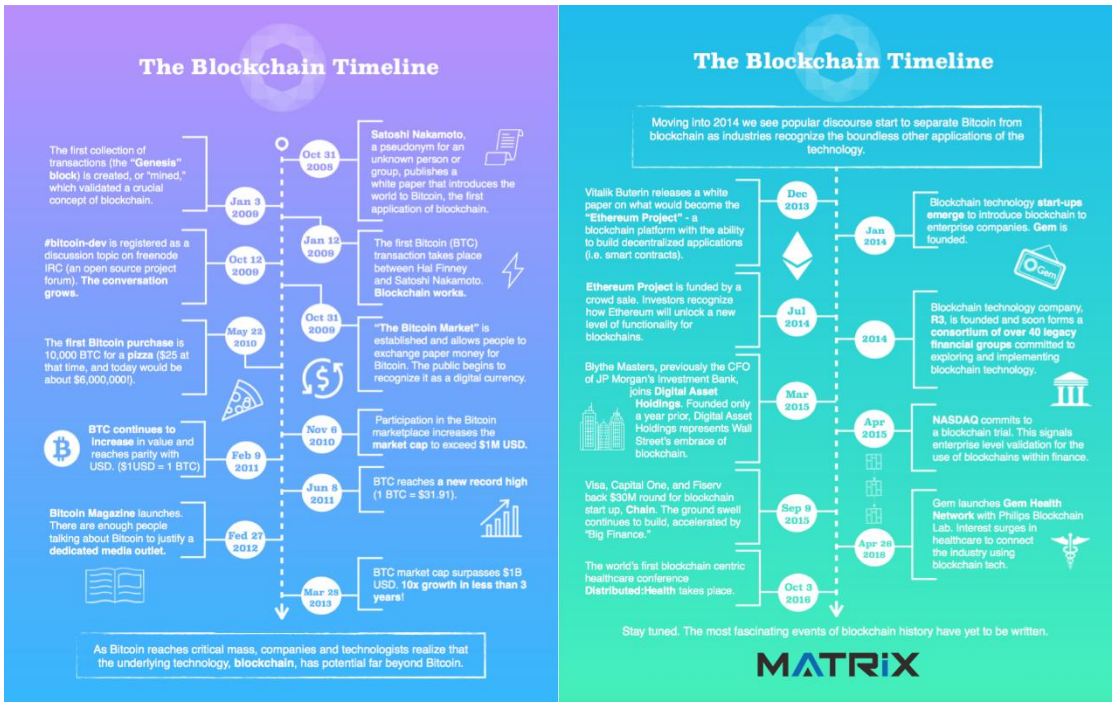


图 1 区块链技术发展简史

# 2 MATRIX，有生命的区块链

## 2.1 什么是区块链 3.0

在正式介绍 MATRIX 之前，为了帮助大家更好地理解 MATRIX，我们有必要先介绍一下什么是区块链 3.0。就每项技术的演进历史而言，每一次的技术大版本的革新，都是基于对前一代技术的痛点完美升级而诞生的。在我们看来，真正地区块链 3.0 的技术标准，应该具有以下几个特征：

**定性的问题定量化**：作为第二代区块链技术的典范，以太坊虽然提供了智能合约，但目前的以太坊智能合约只能解决简单的线性问题，无法解决更复杂的合约条款，也就是无法将定性的条件定量地转为计算机语言，这也大大限制了区块链的交易和应用的空间和范围。所以为了区块链可以更广泛地商业化应用，第三代区块链技术必须具备可以将定性的问题定量化的特征。

**智能合约平民化**：作为第二代区块链技术的核心，智能合约可以说大大提升了区块链的应用范围和想象空间，但目前智能合约（以以太坊为例）必须由少数熟悉代码的技术人员来提供技术上的服务与支持，你不懂计算机语言的话，对不起，你无法主动、方便地使用智能合约。所以如何让智能合约平民化，真正成为人人都可以应用的工具，将是区块链技术真正渗透到每个人生活的一个重要条件，也是第三代区块链技术必须具备的一个重要特征。

**与时俱进的特性**：传统的区块链技术都受限于其研发的时代，也就是“发布即定型“，然后逐渐会被时代淘汰，今天的比特币技术就是个很好的例子。在过去，几乎所有的技术都具有这样的特点，无论是曾经的互联网霸主雅虎，还是摄影行业的龙头科达，无数科技巨头都难逃无法与时俱进而被淘汰的命运，但在技术高速发展的今天，尤其是区块链这种并未成为主流的新技术，几年一次的更新换代，会给几乎所有的应用开发者和使用者都带来不同程度的困扰，尤其是对于金融类行业这种在未来会成为区块链行业最大使用场景产业来说，频繁地更换底层技术或者是主链条，对于银行、券商这种巨型的、内部运营结构精密复杂的公司来说，简直是一场灾难。所以如果区块链本身具有进化的可以做到与时俱进的特性，是区块链在更多行业尤其是国企或大型跨国企业种广泛使用的的基础，这毫无疑问应该成为下一代区块链不可或缺的一个标准。

**算力公益化**：众所周知，PoW 是当前区块链行业最主要的一种共识机制，而目前大多数的挖矿型加密货币都是在无社会意义地浪费算力和资源，如比特币，大量的电力和算力被用来计算毫无意义的 hash 值。虽然这个值是这个链条上很重要的一个组成部分，但这个数值本身对整个社会来说，毫无意义。如何充分利用这些算力和资源，来为公众做更多的有益的事，即算力公益化，成为我们要在下一代区块链技术中思考的一个重要问题。

当然，更高的交易效率、更好的安全性等等，都会是下一代区块链的重要特性，但这些都是会随着技术的线性化发展即可得到解决的技术问题，上述四点特性却是真正地需要质变产生的特性，所以我们把他们定义为区块链 3.0 最重要的 4 项技术标准。

## 2.2 MATRIX 的设计哲学

每一个跨时代的产品的诞生，都基于一个深刻的哲学思想。如比特币，中本聪先生是比特币的创造者，其去中心化、去信任化、社区自治的产品特性后面，隐藏着的是西方主流的“自由、平等”的哲学思想。

MATRIX 也一样，MATRIX 最核心的哲学思想，来自于拥有光辉璀璨的 5000 年历史的中华民族——“知行合一”。“知行合一”是 500 年前，伟大的心学创始人——王阳明先生提出的哲学思想，其核心是客体顺应主体，知是指思想和理论，行是指实践，知与行的合一，既不是以知来吞并行，认为知便是行，也不是以行来吞并知，认为行便是知。

对于当前所有的区块链产品中，“行”都是产品或者生态的主体，应用（即实践）都是每一个区块链产品的主要目标。在没有“知”的情况下，“行”自然缺少了行为准则，或是具有了很大的局限性。在 MATRIX 中，我们创造性地将“知”的概念引入区块链，让区块链自身具有感知世界的能力，真正的拥有了思想和生命。

在“知行合一”的方法论之下，MATRIX 除了拥有了思想和生命，还真正拥有了自然进化的能力：通过“知”来指导“行”（在人工智能的指导下运作和应用），然后在“行”中感知世界（通过运转和应用不断学习），提升“知”的境界（在学习中提升自己的思维能力和认知范畴），之后更好地“行”（提升运作效率，扩展应用范围），这是一个不断演进，自我提升，与时俱进的良性循环。

区块链是这个时代迄今为止最新的技术，这是我们追随痴迷这个方向的重要原因，同时我们也希望“知行合一”这个古老的思想，能为这项最新的技术带来不一样的生命和活力，也让中华民族的伟大的智慧结晶，可以在这个全新的世界中光荣绽放，让所有人为之获益。

## 2.3 MATRIX，区块链 3.0 时代的里程碑

在确定了区块链 3.0 的标准以及设计 MATRIX 的哲学思想之后，我们开始思考如何打造一个真正符合这些标准的区块链技术体系，仅仅依靠区块链技术本身，是很难真正达到 3.0 的标准，所以我们必须引入强大的辅助技术，结合区块链技术一起，来创造下一代的区块链技术。

### 2.3.1 什么是 MATRIX

MATRIX 是新一代的区块链技术，它创新性地将人工智能技术引入了区块链产业，将而这两者紧紧地结合在一起，打造出的跨时代的产品。MATRIX 并不是一个机构，而是一款能够在区块链上实现智能协作、开源的底层系统，它打造了一个平台和提供了相应的编程语言，使开发人员能够利用人工智能算力和区块链技术来建立和发布下一代分布式应用，也为每一个人提供了方便地使用智能协同功能的开放式工具。

### 2.3.2 为什么叫 MATRIX

和大家的想像不同，MATRIX 的核心团队并不是一群像美剧《生活大爆炸》中一样，只知道钻研技术和打游戏的的科学家，我们除了是一群技术极客之外，还是狂热的电影爱好者。而《黑客帝国（The MATRIX）》这部作品更是被我们奉为经典，同时为我们展现了一个人工智能发展到极致的未来的场景。

图 2 电影《黑客帝国》海报

在电影《黑客帝国》中，MATRIX 是一套复杂的模拟系统程序，它是由具有人工智能的机器建立的，模拟了人类以前的世界，用以控制人类。在 MATRIX 中出现的人物，都可以看做是具有人类意识特征的程序。这些程序根据所附着的载体不同有三类：一类是附着在生物载体上的，就是在矩阵中生活的普通人；一类是附着在电脑芯片上的，就是具有人工智能的机器；这些载体通过硬件与 MATRIX 连接。而另一类则是自由程序，它没有载体，诸如特工、先知、建筑师、梅罗文加、火车人等。电影中所展现出来的很多未来场景，以及贯穿整个电影的哲学思想，都与我们设计这个产品的理念不谋而合，所以我们把我们的产品也命名为“MATRIX”，一个结合人工智能的分布式区块链网络。

与此同时，“MATRIX”一词本身的含义代表“矩阵”，矩阵本身的数学含义中透露出来的分布式哲学思想，与区块链的理念很好地契合，同时矩阵的两个维度正好对应我们产品中的人工智能与区块链两条主线。

所以，我们是“MATRIX”，我们是区块链 3.0。

### 2.3.3 MATRIX 的特点

MATRIX 链的特点如下：

**M**echanized Network – 机械化网络：与传统区块链不同，MATRIX 不再是一个纯软件的底层技术网络，越来越多的机械化元素将会加入这个网络，如具有人工智能算法的新型芯片、具有人工智能解决方案的贝叶斯推理机，MATRIX 将通过软硬件结合的方式，大大提升区块链本身的效率、实用性和可扩展性。

**A**utomated – 高度自动化：由于引入了人工智能技术，而语义识别作为 MATRIX 的最基本的一项技术特性，在未来，智能合约不再只为少数懂得计算机编程语言的人服务，而是每一个使用 MATRIX 的用户，只要输入自己的交易目的和交易条件，MATRIX 会通过人工智能自动生成对应的智能合约，通过高度自动化让智能合约真正意义上可以为每一个人服务；

**T**argeted Calculations – 目标性计算：与其他 PoW 型的区块链网络不通，MATRIX 的算力体系不再会计算单纯的对社会本身没有实际贡献的 hash 值或其他加密数字，MATRIX 将在链上部署具有人工智能计算能力的机器作为矿机，或者让加入网络的算力习得人工智能算法，通过人工智能来解决各种需要算力的问题来获得奖励（例如帮助大数据公司通过人工智能算力处理数据），让电力和算力真正用到对社会有实际价值的事情上；

**R**isk Aversion – 规避风险：MATRIX 具有自我进化后不断寻找合约漏洞及应用程序漏洞的能力，任何在链上进行的交易或发布的程序，都会在人工智能的帮助下趋近完美从而规避风险，让每一个用户更加安全；

**I**ntelligent – 高度智能化：MATRIX 通过自我学习和进化，具备处理更加复杂的交易条件的能力，让智能合约不再仅限于处理定量的条件，MATRIX 的超级智能合约具有

高度智能化的特点，可以将很多定性的条件定量化，从而处理更多复杂条件的交易，如投资对赌协议等等，这将大大提升智能合约的可应用行业空间，我们把这种超级智能合约，称为“**智能协同**”；

**X** for Future – 未来成长性：和前两代区块链技术不同，引入了人工智能技术的 MATRIX，并不会存在“发布即定型”的局限性，MATRIX 具备了自我学习而不断进化的能力，由于我们自身的历史局限性，我们现在还无法准确地描绘出第 X 代的区块链技术的特性，但是 MATRIX 会通过自我进化一直与时俱进，成为适应当前时代的区块链解决方案。


图 3 MATRIX 的含义拆解

MATRIX 的这 6 个特点，正好组成了 MATRIX 这个单词，也是我们产品的名称，它贯彻了我们设计 MATRIX 的核心理念和思想，完美地诠释了区块链 3.0 标准并提供了完备的解决方案，所以，我们希望可以通过 MATRIX，正式拉开区块链产业的下一个时代的序幕。

## 3 MATRIX 的生态环境

MATRIX 有一个完整的生态环境，其中包括公有链主体、算力组、应用层、用户组及数字资产代币五个组成部分，这五个部分共同依存、相互作用，形成了 MATRIX 的完整的生态环境：

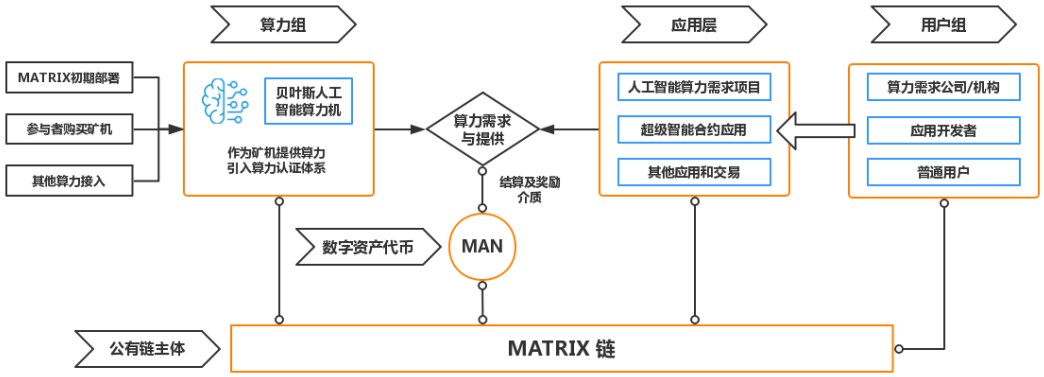


图 4 MATRIX 生态

## 3.1 公有链主体——MATRIX 链

MATRIX 链是 MATRIX 生态的身体，也是生态中其他组成部分存在和行动的基础，整条链将采用 PoW 的共识机制。

## 3.2 算力组

算力组可以说是整个 MATRIX 链的大脑，也是整个 MATRIX 生态最与众不同的部分，MATRIX 的算力组将为 MATRIX 这条链带来生命力，让 MATRIX 不断地进化，与时俱进。

我们并不打算打造一个只有驱壳没有灵魂的存在概念上的 AI 网络，所以在一开始，我们就要赋予这个网络灵魂，在最初团队会部署一定数量的贝叶斯人工智能算力机到网络中，让整个网络在一开始就具备了可以自我学习和进化的能力，在完成初期的自我学习，让整个网络真的具备了人工智能的基础之后，我们会开放算力的接入，届时每一个希望可以通过分享算力而获益的社区参与者，都可以将他们的算力接入到这个网络，在经过我们的人工智能算法优化后，开始为这个全新的世界做出贡献。

## 3.3 应用层

应用层是 MATRIX 生态的骨骼，所有的功能的具象化和真正为用户服务，都是通过应用层来实现的。MATRIX 的主要应用层将分为三类：

1. 需要专业的人工智能算力的项目和应用，比如大数据的深度分析和挖掘，又抑或希望通过人工智能不断学习提高 AI 水平来陪人类游戏的棋牌类游戏；
2. 需要使用超级智能合约的应用，如全程无人参与的房产中介；
3. 常规交易，所有希望通过超级智能合约实现的交易和协议，都可以通过 MATRIX 来实现，这也将是 MATRIX 链上个体用户最多的应用部分。

### 3.4 用户组

用户组是 MATRIX 生态的肌肉，无论是需求人工智能算力的公司或机构（如大数据公司），还是应用开发者，抑或是普通的个人用户，都可以自由地使用 MATRIX 来给自己的生活带来各式各样的便利，有用户的存在，才可以真正驱动 MATRIX 上的应用，从而让整个 MATRIX 生态活跃起来。

### 3.5 数字资产

数字资产是 MATRIX 生态系统的血液，它为生态的各个部分提供着动力。无论是算力组还是应用层，都需要得到数字资产的支持，用户想真正使用应用，也需要数字资产来帮他实现。我们在 MATRIX 上发行的代币简称是“MAN（MATRIX AI Network）”。我们也希望我们的 MATRIX 生态可以真正地像一个人一样，有思想、有行动、有生命力。

## 4 MATRIX 的技术设计理念

MATRIX 作为新一代区块链，核心思想是构建一个具备自然进化能力的区块链，能够充分利用人工智能构建一个用户友好、面向云服务、与 AI 紧密融合的生态系统。

传统的区块链解决了在不可信信道上传输可信信息、价值转移的问题，而共识机制解决了区块链如何在分布式场景下达成一致性的问题。共识机制在去中心化的思想上解决了节点间互相信任的问题；以太坊智能合约 2.0 的推出，则使区块链技术更加接近现实，延伸到了社会生活和商业；而 MATRIX 则在区块底层引入人工智能，从方方面面让人工智能（AI）参与更多以前需要人类能完成的“判断”和“执行”，并引入“集体智慧”和“合约宪法”，同时利用 AI 自身的学习能力，不断进化区块链本身，实现一个具备真正人类意识与思维的区块链生态。

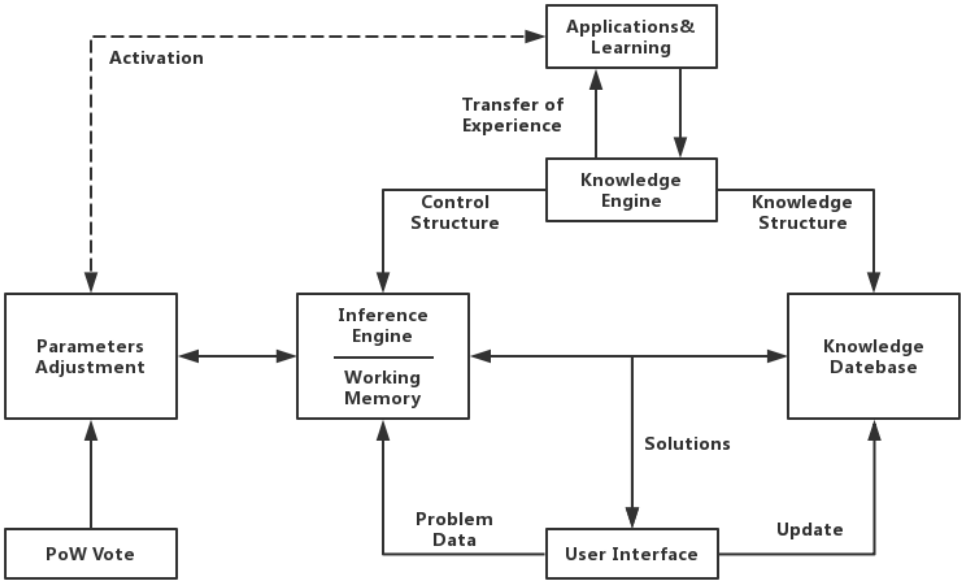


图 5 MATRIX 的人工智能进化设计理念

MATRIX 相对于传统区块链的核心特点包括：

- 系统自然进化（Evolvable）
- 个体可延展性（Extensibility）
- 交易可管理化（Transactions Manageability）
- 交易智能化（Transactions intelligentized）
- 人工智能服务化（AI as a Service）

## 5 MATRIX 引入 AI 的目的以及解决的问题

MATRIX 引入 AI 的目标包括以下几点：

（1） MATRIX 自然进化：通过对 MATRIX 的 AI 辨识与推理，实现 MATRIX 对外部环境变化的系统主动优化和个性化扩展；

（2） 矿机优智化：区别于传统矿机由无意义的 HASH 运算，MATRIX 链解算实际 AI 问题，矿币具备现实价值锚点；

（3） 合约人性化：利用 AI 引擎执行合约，支持利用 AI 解决智能合约中的漏洞与陷阱，并提供仲裁手段；交易方既可以选择基于 AI 保护的交易模式，也可以选择传统无歧视交易方式；

（4） MATRIXAI 服务（AI as a Service）：MATRIX 全网均具备 AI 能力；在系统框架上全方位支持 AI 云服务，支持链上链下的多形态 AI 服务整合，实现数字新财富与传统财富的对接。

以上述目标为基础，MATRIX 将构建丰富的生态系统，引入多种基础服务模式，实现“区块链即服务”的愿景。

## 5.1 什么是 AI

人工智能（英语：Artificial Intelligence, AI）亦称机器智能，是指由人工制造出来的系统所表现出来的智能。通常人工智能是指通过计算机来实现的智能。人工智能的研究是高度技术性和专业的，各分支领域都是深入且各不相通的，因而涉及范围极广。

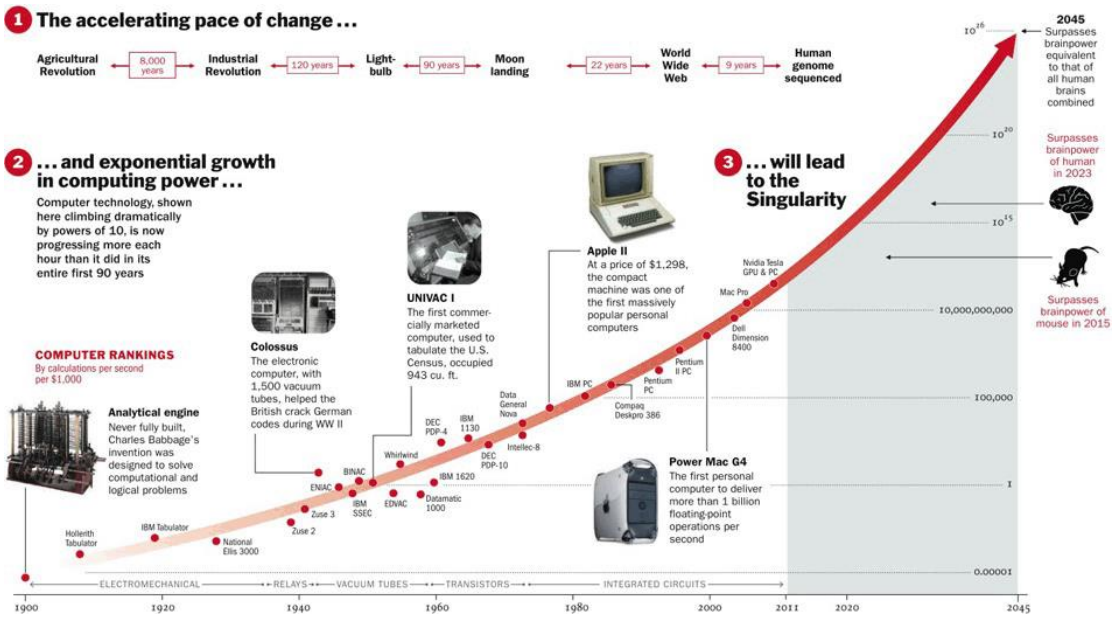


图 6 人工智能发展简史及未来预测

人工智能的研究可以分为几个技术问题。其分支领域主要集中在解决具体问题，其中之一是，如何使用各种不同的工具完成特定的应用程序。AI 的核心问题包括推理、知识、规划、学习、交流、感知、移动和操作物体的能力等。强人工智能目前仍然是该领域的长远目标。目前比较流行的方法包括统计方法，计算智能和传统意义的 AI。目前有大量的工具应用了人工智能，其中包括搜索和数学优化、逻辑推演。而基于仿生学、认知心理学，以及基于概率论和经济学的算法等等也在逐步探索当中。

人工智能的定义可以分为两部分，即“人工”和“智能”。“人工”比较好理解，争议性也不大。有时我们会要考虑什么是人力所能及制造的，或者人自身的智能程度有没有高到可以创造人工智能的地步，等等。但总括来说，“人工系统”就是通常意义下的人工系统。

关于什么是“智能”，就问题多多了。这涉及到其它诸如意识（consciousness）、自我（self）、心灵（mind），包括无意识的精神（unconscious mind）等等问题。人唯一了解的智能是人本身的智能，这是普遍认同的观点。但是我们对我们自身智能的理解都非常有限，对构成人的智能必要元素的了解也很有限，所以就很难定义什么是“人工”制造的“智能”了。因此人工智能的研究往往涉及对人智能本身的研究。其它关于动物或其它人造系统的智能也普遍被认为是人工智能相关的研究课题。

## 5.2 MATRIX 的人工智能体系

MATRIX 选择了贝叶斯决策理论，作为其人工智能体系的基石。

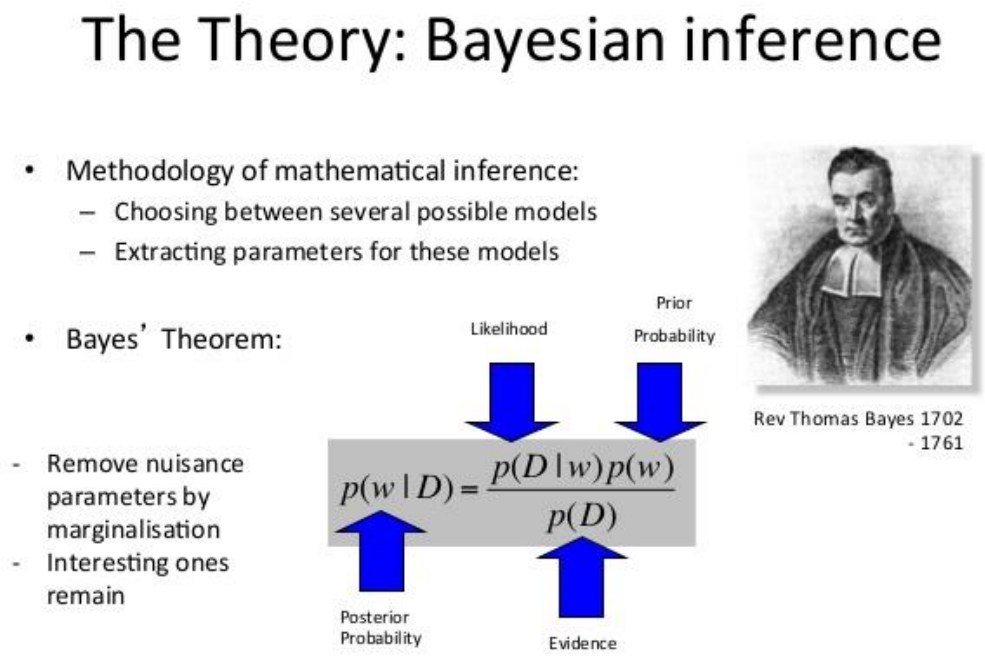


图 7 贝叶斯——MATRIX 人工智能体系的基础

自从其诞生之日起，贝叶斯理论就被认为是概率论和统计科学的一个重要分支，被誉为『永远不死的理论』。20 世纪 80 年代以来其重要性进一步提高，很多数学家认为可以把贝叶斯理论作为基础从而重新构造整个概率论和统计科学。贝叶斯的思想是把概率作为一种信念，通过观测现象、结合基于历史经验的先验概率，反向对端最

可能产生观测结果的假设，并且根据以上推理不断更新先验概率。因此，该理论完美的整合了概率、学习和推断等机器学习的关键概念，已经在机器学习众多领域获得了广泛应用，并且被认为能够解释人脑认知行为的关键理论。从机器学习的角度看，贝叶斯理论具有以下重大优势：

1. 贝叶斯理论能够以非常自然的方式处理机器学习问题中常见的不确定性，并且能够根据观测结果不断减小不确定性；
2. 贝叶斯理论能够构造生成式模型，即能够捕捉学习对象的动态特征，特别是具有寻找因果关系的能力， 这一点与区分式模型具有重大区别，后者能够对识别对象进行区分，但不能捕捉其产生数据的过程；
3. 贝叶斯理论支持复杂过程的推理和认知，更偏向于人的高层次认知行为，例如概念认知、归纳、推理、感知-运动集成等；
4. 通过将贝叶斯计算的基本模式 ——蒙特卡洛马尔可夫计算提供了构造具备普适应用价值的挖矿机制的重要手段；
5. 贝叶斯机器学习拥有重大应用，包括基因与生物表现型相互作用的分析、医学诊断、经济获得分析和金融预测等。

贝叶斯理论具有深度学习具有相辅相成、互为补充的关系。比较而言，贝叶斯学习和推断适用于先验概率准确度较低（不确定性更高）、样本较少、 认知行为更加复杂的问题，而深度学习适合于不确定性较低、样本量大、输入输出关系明确的问题。参数优化是贝叶斯理论最直接的应用之一，能够直接应用于区块链性能调优。同时，贝叶斯增强学习可以逐步减小不确定性的影响，适合于在样本相对有限的情况下对区块链参数进行迭代优化。另一方面，贝叶斯理论与深度学习并不矛盾。首先，深度信念网络和有限玻尔兹曼机就是两者贝叶斯理论与深度学习的产物。其次，当前以及取得巨大成功的卷积和递归神经网络更加适合于识别和分类，这些网络提取的特征为贝叶斯技术进行高层次认知和推理提供了巨大的机会。实际上，贝叶斯理论与深度学习的集成和综合是通向强人工智能的有力途径。

## 5.3 MATRIX 自然进化

MATRIX 作为新一代区块链，通过引入人工智能，动态更新各项区块链参数，实现自然进化演进。通过自然进化，目前 MATRIX 能够解决当前区块链设计固定、不灵活、各种区块链参数不能动态调整的问题。MATRIX 内置开源 AI 引擎，通过对各个区块链参数的学习获得训练参数，从而判断当前区块链参数配置是否进入不合理区间。通过 AI 学习结果，确认是否发起参数修订，并获得最佳修订参数，并通过全网智能投票确认参数修订。修订确认的参数则通过全网广播形式，发送到各个节点，完成区块链的全局更新，从而实现 MATRIX 的智能进化。

目前区块链核心参数包含以下几类：

（1） 区块的存储格式配置类，包括区块大小、数据记录方式、交易列表、以及填充随机字等；

（2） 区块链的共识机制与算法类，包括 PoW 及附带的完整性保护方法（SHA256、SCRYPT 等）、PoS、pbft 等以及未来可能出现的新方法；

（3） 区块链的网络模型，包括 P2P 协议方法、新交易的广播方式、投票表决机制等；

（4） 区块链的激励机制，包括挖矿以及关联的矿币分配协议、智能合约的交易费用、红利、彩票收益等等；

（5） 区块链的安全加密算法，包括基于公钥的签名方式、Merkle 树及压缩算法等；

（6） 区块链的交易模型：包括智能合约方案、钱包设计、身份隐私设计、支付模型等。

（7） 区块链的附属模型：包括可信网关、隐私数据保护池等针对现有区块链不足而添加的附属模型。

通常情况下，当一条链确定以后，其核心参数也固定了。但随着服务对象变化以及外部环境的变化，很多参数都将变为瓶颈。例如，比特币由于将区块大小设定为 1Mbyte，单次挖矿时间设定为 10 分钟，初期比较条件宽松，当在 2016 年以后，在线交易十分拥挤，大部分商业密集交易活动均不适合在比特币上开展。

目前，MATRIX 将对区块的存储格式配置类、区块链的激励机制、区块链的安全算法以及完整性算法、区块链的交易模型这四项参数，进行在线监控，并通过本地内置 AI 模型，从而辨识出是否处于瓶颈或是否可以优化。当本地 AI 判断可以进入优化后，将发起 AI 参数优化交易，并进入区块链 AI 记录区，其余节点将对该 AI 参数优化交易进行辨识和判断，并发起投票；当投票结果满足一定规则后，将启动该 AI 参数更新。

此外，MATRIX 内嵌支持区块链的共识机制与算法类、区块链安全加密算法的更新，通过 AI 智能投票与选择机制，保证此类区块链核心参数能够平滑进入未来的 MATRIX 中，避免各种区块链的硬分叉。

对于区块链的附属模型，MATRIX 将保留一定的扩充能力，通过模型标记语言描述其能力；通过安全智能合约表述其操作流程以及行为模型；通过添加模型附属的 AI 参数，实现对象模型的持续优化。

### 5.3.1 MATRIX 参数的 AI 辨识

MATRIX 中各个参数均存储在专用的区块中，但由于区块链很多的参数实际属于隐藏变量，例如交易活跃度，用户可信度等。因此，MATRIX 通过建立贝叶斯网络模型，

利用结构学习算法，识别各个隐藏参数之间的依赖关系和程度。一个典型的 AI 参数辨识过程如下，目前准备在专门的矿机芯片中内置该算法实现参数的动态调优。

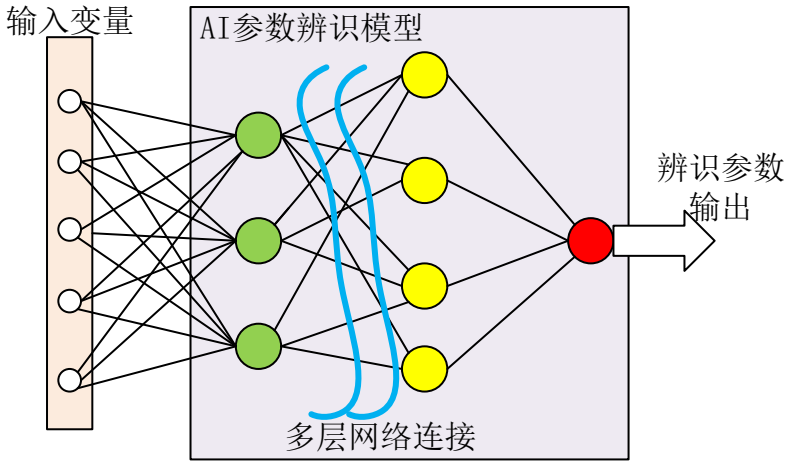


图 8 MATRIX 参数辨识模型

MATRIX 中，将对每个 AI 显式参数进行统计，例如区块大小等；而对影响 MATRIX 性能的每一个隐式参数，建立一个基于 AI 的辨识模型。当上述参数进行统计与辨识后，将通过标准优化算法，实现参数最优化。

### 5.3.2 MATRIX 参数的 AI 优化

MATRIX 参数的 AI 优化法则包含以下几条：

（1） 保证 MATRIX 能够延续生存，并获得最大化的货币收益；

（2） 保证 MATRIX 可用 AI 服务最大化；

（3） 保证 MATRIX 所有节点的算力话语权以及活跃度；

（4） 保证 MATRIXAI 参数配置的优先级。

上述每项原则均可用一个可量化的目标函数进行评估。例如 MATRIX 的生存原则以及最大化货币收益原则，可以通过预先配置参数，评估全网的交易频度、电费以及交易网络开销，挖矿所得、AI 服务所得，确定当前时刻的收益。

$$Principle_1(Time_N) = Income(Total_{Miner}) + Income(AI_{service}) - Cost(Power_{Matrix}) - Cost(TranscationGas_{Matrix}) - Cost(Tradeoff_{Matrix})$$

根据该目标函数$Principle_1(Time_N)$，内置的 AI 优化引擎将评估各个区块链参数是否配置合理，并通过动态寻优，预估本时间段内的最佳参数配置。

目前 MATRIX 的参数优化模型采用贝叶斯增强式学习算法，预印本将公布在 arXiv 上。参数的 AI 优化原理如图 9 所示。其基本思路是把参数优化作为一个决策过程，其

中 MATRIX 的状态在外界输入和模型参数的变化下不断进行状态更新。优化算法利用贝叶斯原理在观测奖励的基础上寻找优化策略，从而使得参数得以优化。为了保证系统稳定，实际上优化过程中的模型不直接与环境交互，而是利用 MATRIX 网络中采集的历史数据进行批量优化。

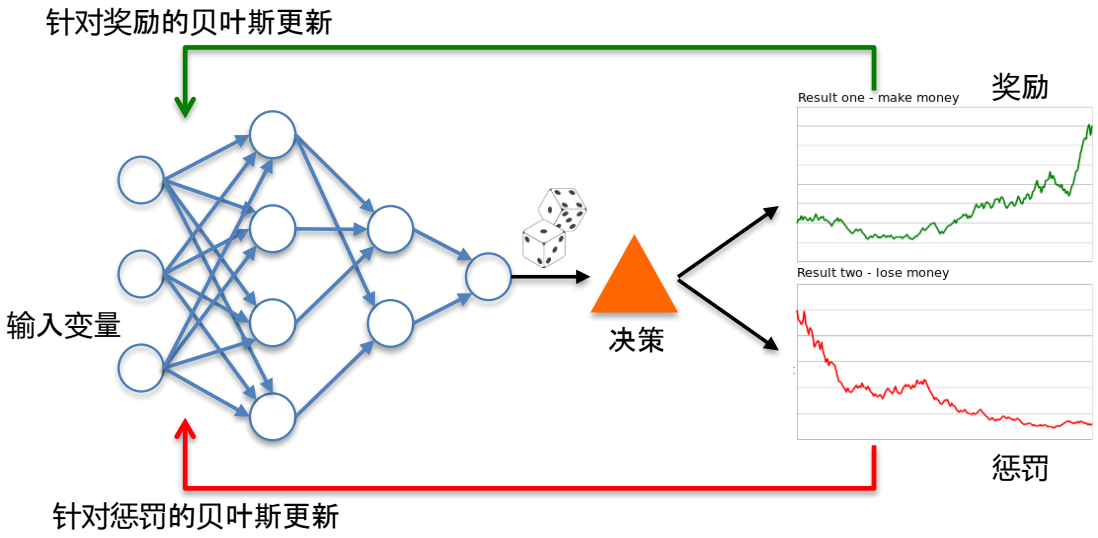


图 9 基于贝叶斯增强学习的参数优化

### 5.3.3 MATRIX 的链式结构

由于 MATRIX 设计为具备自然进化的区块链，因此需要设计专有 Block，用于表征 MATRIX 的自然进化过程，并表述整个 MATRIX 的特征形态和行为参数。基于区块链分布式基础上，结合“管理控制与数据分离”， MATRIX 将整个区块划分为独立的两类：分布式协同管控区块与数据区块。分布式协同管控区块可以组成为一条分布式控制区块链，该链包括整个系统区块链系统信息描述、以及对应数据链的 AI 参数描述、AI 模型描述、交易模型描述等控制信息；而数据区块则根据分布式控制区块的指示进行数据编码、配置 AI 模型、并获得交易信息。可以认为 MATRIX 是一条具备自然进化能力的软件定义区块网络。

MATRIX 在初始阶段，仅包含一条分布式控制区块链与一条数据区块链，其区块结构定义为如图 10 所示。在实际应用中，控制链与数据链既可以设计为时分复用的一条区块链，也可以设计为两条联系紧密，但独立运行的区块链：

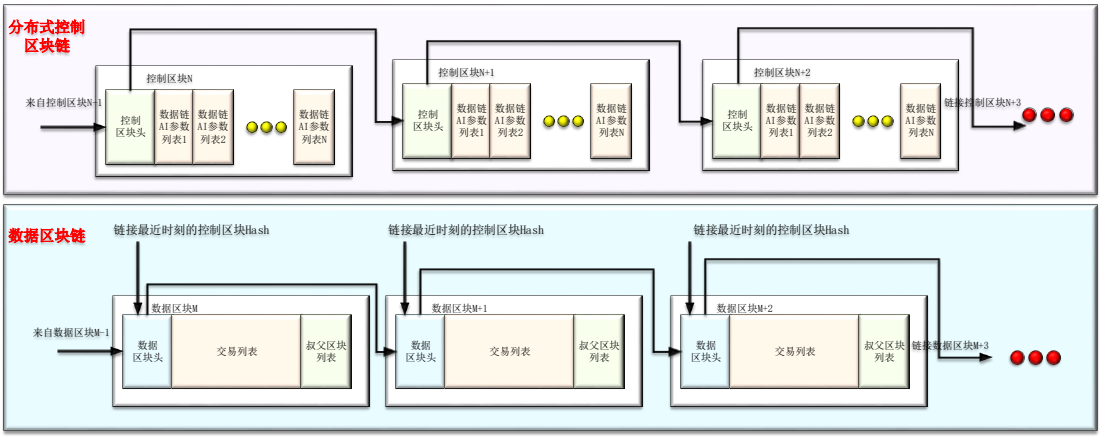


图 10 MATRIX 的结构

事实上，随着 MATRIX 区块链 AI 服务内容的增多，为保障业务的开展，MATRIX 区块将会形成更多的区块链条，其中一条作为控制区块链，其余的多条数据区块链则按照控制区块链的指示进行链接组合。每条数据区块链采用的共识机制与算法、各项区块链参数都可能存在相当的差异。这种做法的核心思想是：针对每一项服务提供最定制化、最智能的区块链。

由于数据链的参数均由控制链定义，因此，每一条数据链区块可以呈现出截然不同的风格和特色。此外，随着时间推移，各个数据链与控制链也会利用 AI 进行各种优化，因此，单条数据区块链在不同时刻，也同样存在不同的风格差异。

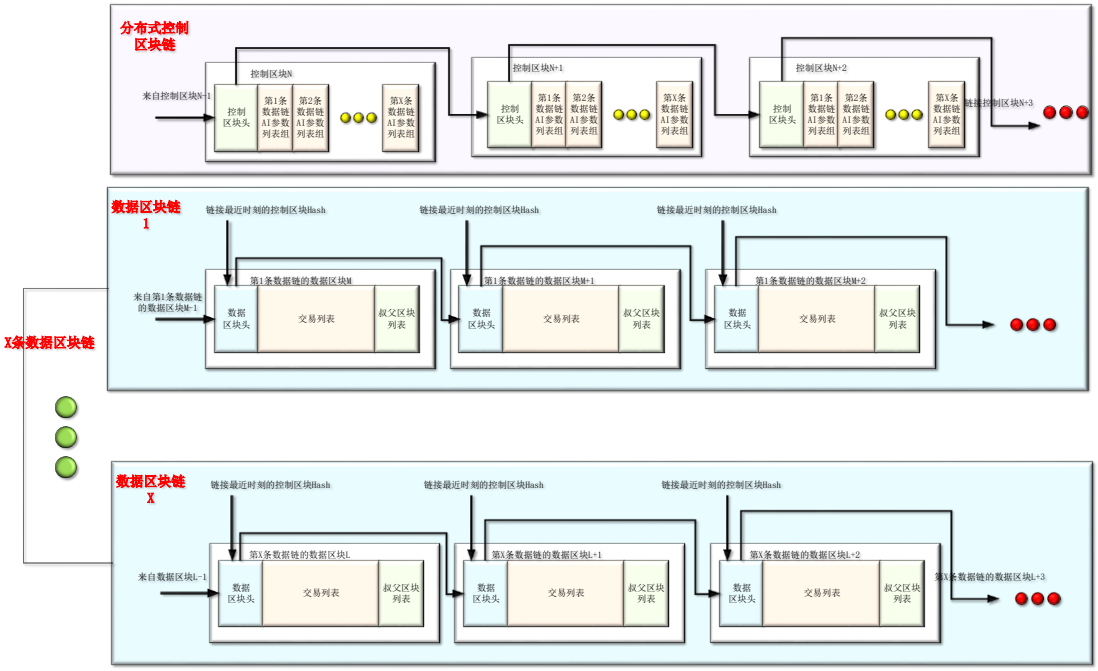


图 11 MATRIX 基于多数据链的结构

当 MATRIX 区块链的 AI 服务进一步增多时，可以将多链进化为多条交织的区块网络，各条链中的区块，通过分布式控制链的定义方法，支持链条间的数据路由以及跨链交易执行。此时，MATRIX 将进化为真正的区块链网络。而进一步的进化，则在未来更新的版本中发布。MATRIX 的自然进化过程如图 12 所示：


图 12 MATRIX 的自然进化过程

由于 MATRIX 采用控制与数据分离的设计思想，每条数据区块链均通过分布式控制区块动态描述。因此，在未来的 MATRIX 中，可以通过控制链定义一条支持比特币的数据链，也可以定义一条以太坊数据链，而这两条链中的数据可以通过控制参数定义，实现多链交互，对应的币值和数据也可以通过 MATRIX 设计的安全智能合约进行交易互换。

事实上，MATRIX 作为一个开放性的平台，在满足共识机制的前提下，任何节点都可以按照约定规则，通过合约方式，创造新的附属数据链条。新添加的附属数据链将拥有独立的控制参数配置与数据结构，其链条货币价值独立，需要通过控制链合约与 MATRIX 原生货币进行兑换。

### 5.3.4 MATRIX 链参数更新过程

MATRIX 中在控制链区块中通过标准模型描述语言，定义了控制区块链与数据区块链的模型与 AI 参数。在更新数据区块链参数时，可以通过配置生效时间确定参数更新，例如当前控制区块产生后的第五个数据区块生效，即 N=5 的方式。数据区块的更新过程如图 13 所示：

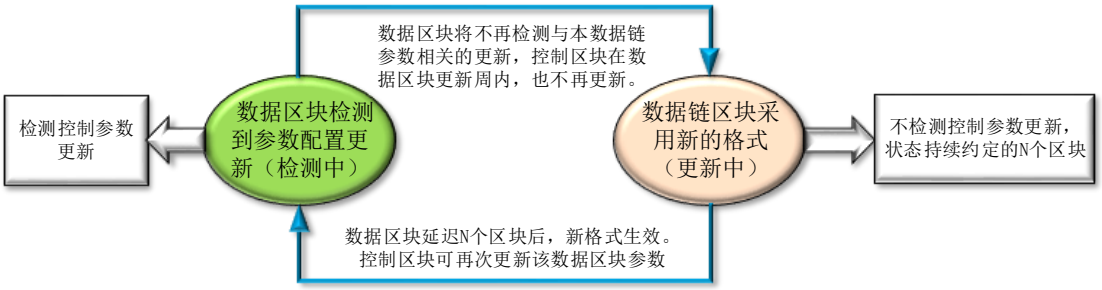


图 13 数据区块的更新过程

目前 MATRIX 的分布式控制区块结构包含两种：

（1） 采用自解释结构，每个区块的内容均能独立解码。

（2） 采用关联解码结构，当前区块的内容解码与前面区块具备相关性。

考虑到更新参数会影响大量的连锁反应，因此分布式控制区块重新定义参数时，仅采用了自解释结构。具体而言，当现在的控制区块包含控制区块参数更新时，所有的更新参数将会在下一个控制区块生效。

MATRIX 还有一个重要特点是：分布式控制区块包含了完整的 AI 模型描述。由于 AI 模型描述通常比较复杂，模型存在超出单个控制区块数据区的容量可能性，因此 AI 模型描述存在跨区块的问题。对此，MATRIX 采用跨区块归集技术：仅在当前区块不存在未完结模型描述时，启动支持新一次跨区。数据区块在对应控制区块模型完整发布后，才能使用该模型。

为了激活 MATRIX 个体业务的繁荣，促进多种业务的开展，MATRIX 在初始设计中，就支持用户定制化任务发布系统。任何 MATRIX 用户，只要承担部分费用后，可以根据自身需求，通过控制区块发布个体交易模型参数与 AI 参数，并基于此定义智能合约。

当用户定义的智能合约通过全网广播和消息确认后，MATRIX 分布式控制区块将记录该用户的 AI 参数和交易模型，当取得全网共识后，MATRIX 将写入分布式控制区块，并支持用户基于该模型参数启动智能合约，实现定制化智能合约发布。而当用户需要更新 AI 参数与交易模型时，需要首先撤销所有与之相关，且尚未完成的智能合约。当撤销完毕后，才能再次发布新的模型参数。需要明确的是，当智能合约明确为不可撤销，则用户必须等待合约完成后，才能更新相关参数与交易模型。

单用户通过 MATRIX 节点发布个性化参数与更新过程示意图如下：

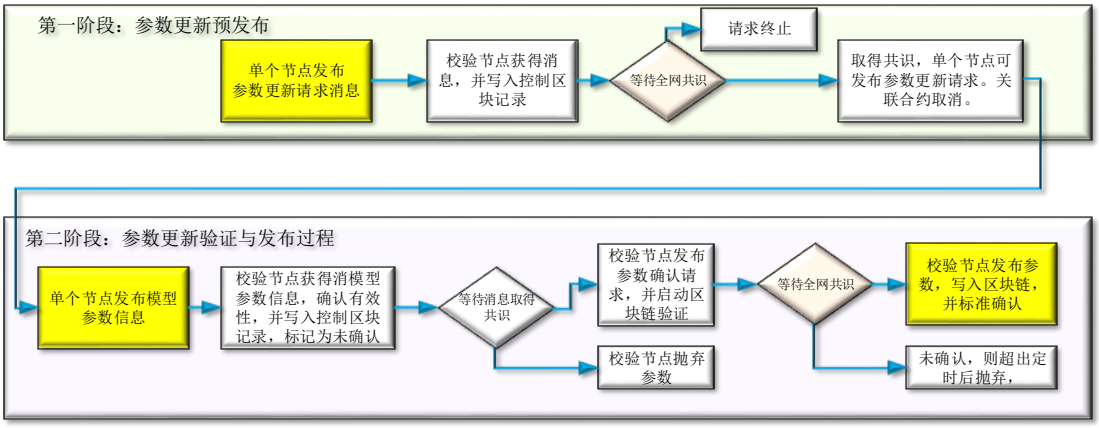


图 14 用户个性化模型与参数更新过程

## 5.4 矿机优智化

对任何密码货币系统来说，挖矿具有两重意义。首先，挖矿是产生货币供应的基本过程，而货币供应是矿工们的根本动机。其次，挖矿过程实际上是对交易数据的完整性进行加密处理，从而形成一个 checksum，因此也是保护货币信用、防止欺诈的核心手段。

### 5.4.1 挖矿计算要求

密码货币的加密计算包括两个方面的内容：1）公钥系统实现数字签名，2）单向加密实现交易记录的完整性计算。矿机主要负责后者的计算。交易数据的完整性计算通过特定数学函数实现，现有系统普遍采用以 SHA 及其变种的 Hash 函数，该函数需要满足以下三个要求：

1. 压缩性：把任意长度的交易记录计算为为一个较短的、具有固定长度的字符串；
2. 隐藏性：计算具有单向性，即从计算结果很难推出原文，这里需要考虑当前正在高速发展的量子密码技术，基于数论的密码系统在量子计算面前是脆弱的；
3. 计算性：计算过程需要一定的、可以证明的工作量，其计算强度（体现为计算时间）相对可控。

除了上述条件以外，如果挖矿计算能够完成超越加密货币之外的应用（例如科学计算和机器学习），那么伴随矿机网络强大计算能力的硬件损耗和电力消耗就具有挖矿之外的价值，反过来也提升密码货币的价值。

### 5.4.2 MATRIX 矿机算法思想

区块链需要一定的工作量证明（Proof of Work，PoW）机制，其目的在于防止所谓的『区块链分叉（forking the blockchain）』或者 51%攻击，即矿工需要极大的运算

能力才能成功篡改账本。目前最常见的 PoW 机制是哈希函数，旷工把交易记录整合到一个区块之后，需要对区块内容进行哈希运算，该运算结果首先是记录内容完整性的一种表征。其次，哈希计算结束后，矿工检查结果是否满足特定条件（例如小于某个阈值），如果不满足，则再次进行同样的哈希计算，直至满足阈值为止。这样，矿工必须完成一定计算量，才能提交区块。基于 PoW 的矿机算法，通常可以归纳为如下的实现方式：

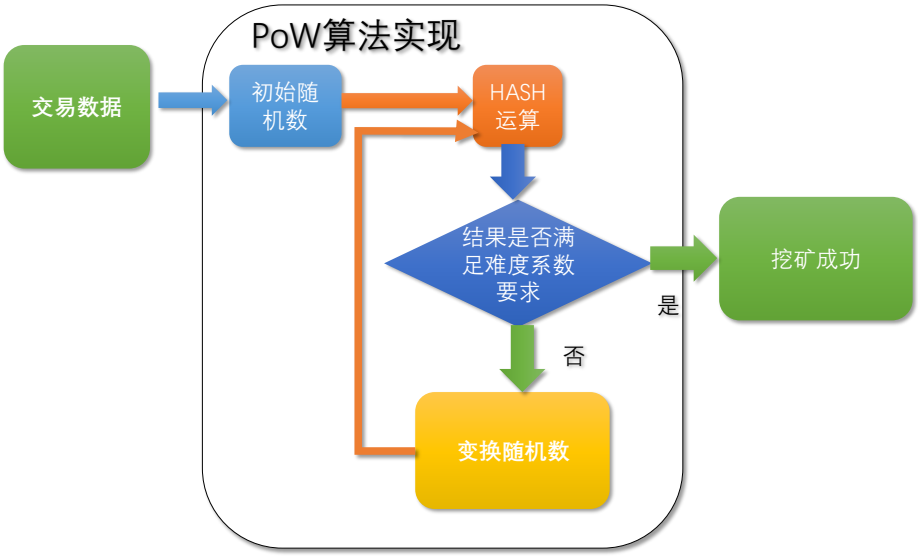


图 15 传统 PoW 的执行方式

PoW 机制对区块链的安全性具有重要意义，然而其计算结果对人类其它方面的生活全无意义，这也是比特币和其它加密货币受到诟病的一大原因。

MATRIX 区块链的核心技术之一是将具有附加值的 PoW 计算机制，通过将贝叶斯核心模式 ——蒙特卡洛马尔可夫（Monte Carlo Markov Chain，MCMC）计算引入 PoW，从而保证计算过程能够产生针对其它领域的应用价值，这也是区块链 3.0 建造虚拟货币和人类社会现有财富之间桥梁的重要一环。

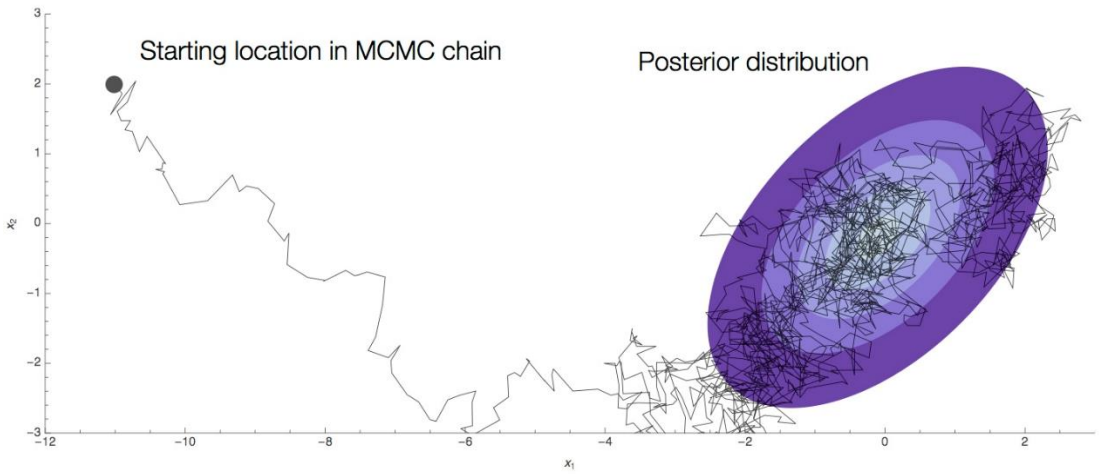


图 16 MCMC 算法的执行过程

MATRIX 链的 PoW 模型构造方式如下：

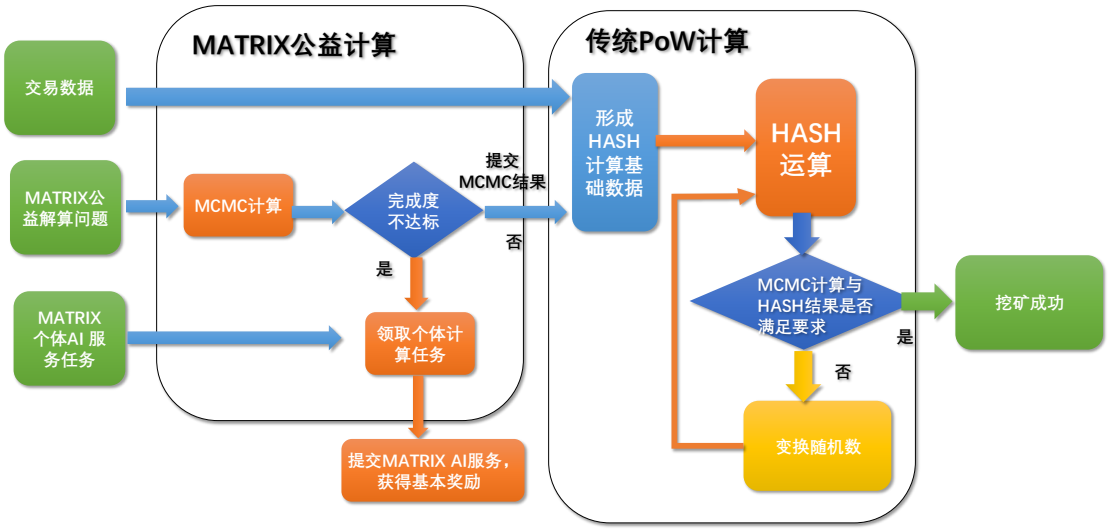


图 17 基于二阶段 PoW 的挖矿计算原理图

MATRIX 的 PoW 实际包含两部分，（1）MATRIX 公益计算阶段；（2）传统 PoW 阶段。

在公益计算阶段，每个节点将根据共识获得的随机数，选择 MATRIX 链公益计算问题之一进行解算，该问题包含了一系列候选 MCMC 问题，必须通过长时间的拟合计算才能逼近某个结果，且问题属于初始条件敏感算法。当在规定的时间内，拟合目标不达标，则节点被取消进入下一步传统 PoW 计算的资格，将进入个体任务领取状态；通过计算 MATRIX 链发布的 AI 服务获得基本奖励。当拟合完成度达标的节点，则进入传统的 PoW 解算阶段。

在 PoW 解算阶段，每个合格的节点将对交易区块以及本次 MCMC 参数的提交结果进行完整性校验，获得规定难度以内的随机值。当获得该随机值后，将迅速全网发布。而收到发布结果的节点将验证 MCMC 的难度以及 HASH 校验值是否满足要求。如果满足则迅速转入下一区块计算，否则继续本地 PoW 计算。

上述实现方案的核心在于：（1）通过 MCM 计算，确定基础 PoW 候选者，没有在规定时间内的候选者，最佳选择是进行公益计算，获得个体服务收益。（2）PoW 将 MCM 计算结果作为验证依据；但由于 MCM 与 HASH 运算通常属于独立的两类计算方式，因此二阶段的 MCM 计算能力，同样可以作为公益计算，获得个体服务收益。

MATRIX 链通过参数配置，既可以选择仅支持二阶段运算，也可以选择支持全部阶段运算。

### 5.4.3 MCMC 算法特点

MCMC 是通过随机采样构造满足细致平稳条件的马尔可夫过程，使得样本分布任意逼近目标函数。贝叶斯后验概率的计算通常依靠 MCMC，常见采样算法有 Metropolis-Hastings （MH）、Gibbs 和 Slicing 等。其中 MH 算法被认为是二十世纪十大算法之一，其基本思想是根据似然概率比值决定是否接受样本，图 16 是从随机起点起步逐步采样的过程， 右半部分采样结果的分布就是目标分布。MCMC 算法具有这样一些特点：

1. 计算量大：复杂分布经常需要上百万次甚至更多次数的采样，计算时间极大；
2. 并行度低：经典的 MCMC 算法采样过程中，先后产生的样本具有顺序依赖性，难以并行化；
3. 应用广泛：MCMC 是贝叶斯计算的核心模式，在金融、生物、分子动力学等领域具有重要应用；
4. 易于评估：虽然 MCMC 的计算过程复杂，但是相对容易评价计算结果的质量，例如可以通过似然函数进行评价。

按照 PoW 设计初衷，任何一个 PoW 计算既要具备一定强度，也要鼓励接受最好的结果（这里『好』的标准是计算结果与目标分布的接近程度 ）。而 MCMC 的优势在于，以上两个要求都可以通过收敛性进行衡量。收敛性的评估方法极多，其中稳态测试是比较有效的方法。常见稳态测试算法（也常被称作收敛性诊断算法）如表格 1，MATRIX 区块链采用其中算法的组合对收敛性进行评估。

表格 1 MCMC 稳态测试算法

| 评价方法 | 使用范围 | 概述 |
| --- | --- | --- |
| Gelman-Rubin | 多马尔可夫链（初始值不同 ） | 比较链内和链间方差 |
| Heidelberg-Welch | 单马尔可夫链 | 对半数样本使用 Cramer-von Mises 方法估计后验分布（即目标分布）均值 |
| Geweke | 单马尔可夫链 | 比对前一半样本和后一半样本均值的相似程度 |
| Raftery-Lewis | 单马尔可夫链 | 估算以某种概率到达某个阈值数据的迭代次数 |

MCMC 作为 PoW 的另一个好处是计算过程中矿工并不知道最终的分布是什么，即只能看到当下的计算结果，也可以知道自己确实在走向收敛目标，但并不知道最终的分布是什样子，因此难以造假，即伪装自己拥有较好的计算结果。

### 5.4.4 MATRIX 的交易者获益模型

MATRIX 节点获得收益的方法包括以下几类：

（1） 挖矿收益；

（2） 执行合约收益；

（3） 寻找优化区块链 AI 参数，并获得区块链认可；

（4） 为其它用户执行任务获得收益；

（5） MATRIX 红利收益；

（6） 基于合约的随机彩票奖励

MATRIX 单个节点支出的费用包括以下几类：

（1） 发送交易与提交合约的费用；

（2） 合约调用 AI 的费用；

（3） 合约执行计算步骤的费用；

（4） 合约执行内存的费用

（5） 合约嵌套调用其它合约的费用（含步骤与内存费用）；

（6） 调用密码运算与安全钱包的费用；

（7） AI 托管的费用；

（8） 发布 AI 任务费用以及后续执行费用；

（9） 参与随机彩票的基础费用。

### 5.4.5 MATRIX 的特色交易

MATRIX 通过引入人工智能以及配套的多种 AI 模型，能够支持现有金融系统中出现的各种合约交易行为，典型的行为包括：期货保值交易、商品对冲交易、远期合约锁定等。另外，还通过可信网关与各种 AI 插件，实现 MATRIX 上与 MATRIX 下的各种智能合约交易。

作为一个特色，MATRIX 引入基于彩票的奖励机制，鼓励用户参与交易。典型的奖励机制实现流程如下：

（1） MATRIX 上的彩票 AI 模型确定本次开奖的区块交易起始位置与候选长度，并写入控制链区块，因此各个节点和参与用户均可以可等效换算出彩票开始与结束区块，并确定奖励机制与开奖规则；

（2） 在开奖期间内，每个用户完成一次交易后，将获得对应份额的奖励彩票；

（3） 当区块达到彩票结束区块位置后，将以当前区块的 Hash 值作为中奖函数的随机种子，获得中奖号码以及奖励分配方式。

（4） 本次开奖结束后的下个区块将本次开奖结果，按照开奖规则分配到各个用户钱包中。

上述交易的目的主要是鼓励用户交易。

上述方案的核心是开奖区块的 Hash 值足够随机，事实上，如果当利益足够大的时候，矿工可以选择欺骗，或者使得竞猜结果有利于自己。典型的，如果矿工挖矿成功，但使用其它 Nonce 值带来的预期收益高于当前收益，矿工可以选择欺骗。

因此，MATRIX 可以选择第三方监督方案，即在彩票发行过程中，开奖的随机种子由第三方私钥和最后一个开奖区块的 Hash 值共同产生。监督员将产生一对公钥与私钥，其中公钥提前公布，用于验证私钥的可靠性，而私钥作为最终使用的随机种子之一。

第三方监督模式的奖励流程如下：

（1） 上述交易在启动彩票活动后，将随机选择一个在线第三方，并由第三方随机生成一对公钥密钥。在彩票结束区块前，由第三方公布公钥。若第三方不公布公钥，则重新选择新的第三方，并延迟开奖。

（2） 开奖时，将由第三方在彩票结束后的第一个区块中公布私钥，并利用私钥和彩票结束区块的 Hash 值进行彩票专用 Hash 函数处理后，作为中奖函数的随机种子。如果该用户未公布私钥，则延迟开奖，重新进入步骤（1），直到最后开奖区块满足要求。

所有用户可以通过验证私钥与公钥对，确认本次交易的公正性。在 MATRIX 中，既可以按照上述随机模式，也可以选择可信的在线第三方提供公钥与私钥，从而避免延迟开奖的发生。

上述，彩票奖励的流程如下所示：

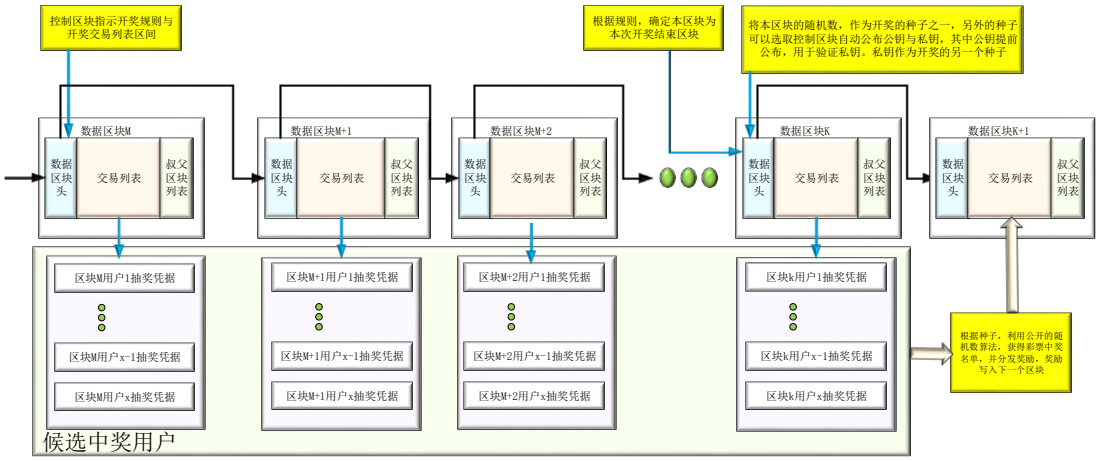


图 18 MATRIX 的彩票交易奖励

## 5.5 安全智能合约

MATRIX 针对现有交易合约存在的开发难度大、编码调整非结构化、无安全审查机制等弱点，通过引入人工智能和安全可信执行机制，并基于 AI 虚拟机，设计了新一代的安全智能合约。在支持无歧视原则基础上，合约用户能够选择基于 AI 模型作为基础保障，实现更加安全可靠、更加灵活开放的交易。

安全智能合约可以定义为：由事件驱动、能够通过 MATRIXAI 审查、支持 AI 托管和裁决、能够持续状态保持、运行在一个复制的、分享的账本（The Replicated, Shared Ledger）之上的、且能够保管账本上资产的程序，该程序能够支持通过 MATRIX 指定的接口方式和可信网关，获得外部数据。可以认为安全智能合约真正实现了具备法律框架的智能金融。

在 MATRIX 系统中，智能合约是一个包含代码、数据存储以及指定 AI 参考模型与 AI 判决规则的链上对象。合约拟定者可以通过语言描述合约条款，明确合约的 AI 规则与 AI 参考模型，设定执行条件，以及达到执行条件后执行的操作，参与接口等。在合约拟定者将合约注册到 MATRIX 上后，其他用户将通过调用接口参与合约。

### 5.5.1 智能合约 2.0 的缺陷

传统的智能合约交易，当前还处于野蛮生长阶段，每次交易都类似于一次“丛林冒险”。目前基于以太坊的智能合约项目非常多，比较有名的有 Augur、TheDAO、Digix、FirstBlood 等。很容易发现，这些传统智能合约非常复杂繁琐，很容易出现逻辑漏洞。例如在 TheDAO 智能合约中，通过非常繁琐的步骤，才避免了“多数抢劫少数”的情况；如果用户经验不足，此类事件极容易发生。造成此类现象的本质在于：区块链设计为无需信任的环境，不具备中心化的裁决机构，因此无法实施“事后申述并进行仲裁”的机制，这意味着只要错误发生，就无法改正。

例如，在区块链中，如果将货币发送到某个地址，这个操作是无法撤销的。因此，当交易方将货币发送到某个错误的地址时，由于交易无法撤销，相应的损失将无法挽回。

同样，类似互联网上的钓鱼交易，也能够在区块链中发生，欺诈方通过在合约中埋下特定的陷阱或者钱包地址，实现合约的漏洞执行，此类交易同样无法执行。

另外，当合约中存在漏洞，例如当前交易执行完毕却忘记撤销交易钱包，此时货币将无法转移到指定的钱包。

在现实生活中，上述交易能够通过中心化的系统来撤消。但是如果是去中心化的系统，按照传统合约方式，则只能由交易方自己承担风险。

此外，还有一种可能性：用户在编写合约过程中，人为出现失误。常见的人为失误包括：股市交易中的乌龙指操作；外汇交易中的错误报价方式：例如将 USD/RMB 报价为 RMB/USD。上述交易必然导致严重损失。

因此，对现有智能合约进行兼容性改造，通过某种机制实现对合约的逻辑行为进行智能分析与缺陷预防，最终达到漏洞概率最小化，是非常有必要的。

MATRIX 的安全智能合约致力于解决上述需要传统中心化交易才能解决的问题。安全智能合约在无歧视原则基础上，引入 AI 模型，自动判断交易模型的合理性，并自动嗅探交易漏洞，实现合约交易的文明化。另外，通过内置 AI 交易模型，在用户许可下，自动拒绝不合理交易，实现 MATRIX 的交易立法。但如果用户舍弃 AI 保护，也可以完成交易，但出现的后果需要用户自行承担。

安全智能合约相对智能合约 2.0，增加了如下几项功能包括：

- 利用 AI 确定交易数据风险与可能的漏洞；

- 提出修改建议，并推荐生成新的交易合约；
- 金融衍生品交易的 AI 制度保障；
- 用户合约执行中的各种边界条件的自动补充；
- 用户合约的 AI 安全托管，主要用于期货与长时段金融衍生品交易。

此外，MATRIX 的合约工具能够提供以下几类功能：

- 为用户提供各种高层次交易模型，模型已经通过 AI 安全审查；
- 针对用户合约，进行交易漏洞嗅探与提示；
- 对交易对象提供的交易合约进行机器码层面安全审查，确认交易风险。

事实上，MATRIX 的安全智能合约，能够充分描述合约参与方的目的，嗅探其中的风险，并在进入合约执行前进行充分审核，确保交易安全。相对传统的智能合约，MATRIX 在合约执行过程中，为用户提供了充分的安全保护；而在执行完毕后，MATRIX 还将通过 AI 模型对合约执行过程与结果进行分析，并提交质量评估，从而促进安全优化与交易品质提升。

另外，当前的智能合约 2.0 还有一个关键性的缺陷：区块链运行 DApp 应用程序的能力非常有限，无法实现人工智能的语义理解、多层神经网络、机器学习等 AI 能力。而 MATRIX 每个节点原生支持 AI 虚拟机，既能支持传统的 DApp 应用，也能直接实现基于人工智能的语义理解、基于 RNN/DNN 的神经网络等先进的 AI 功能，整体计算能力强大，支持大量的 DApp 并发运行。

### 5.5.2 基于 AI 的交易模型

安全智能合约向下兼容传统的智能合约 2.0，支持基于脚本和支持利用 AI 辅助完成交易，也支持 AI 托管交易。

#### （1） 智能合约 2.0 的执行

MATRIX 上的节点通过 AI 虚拟机，以兼容形式执行该类型的合约。智能合约 2.0 执行过程如下：

首先，多方用户共同参与制定一份智能合约，该阶段属于合约拟定阶段：

i. 合约执行方（用户）注册成为区块链的用户，并由区块链返回给用户一对公钥和私钥；公钥做为用户在区块链上的账户地址，私钥做为操作该账户的唯一钥匙。

ii. 两个以两个以上的用户根据需要，设计一份合约，通过程序化条款，确定了相关承诺，承诺中包含了双方的权利和义务；这些权利和义务以电子化的方式，编程机器语言；参与者分别用各自私钥进行签名；以确保合约的有效性。

iii. 签名后的智能合约，将会根据其中的承诺内容，上传至区块链网络中。

其次，当用户提交智能合约至区块链后，将进入有效性验证阶段。该阶段将完成以下操作：

i. 合约通过 P2P 的方式在区块链全网中扩散，每个 MATRIX 节点都会收到一份；区块链中的验证节点会将收到的合约先保存到内存中，等待新一轮的共识时间，触发对该份合约的共识和处理。

ii. 当共识时间达到时，验证节点会把最近一段时间内保存的所有合约，一起打包成一个合约集合（set），并计算出合约集合的 Hash 值，最后将这个合约集合的 Hash 值组装成一个区块结构，扩散到全网；其它验证节点收到这个区块结构后，会把里面包含的合约集合的 Hash 取出来，与自己保存的合约集合进行比较；同时发送一份自己认可的合约集合给其它的验证节点；通过这种多轮的发送和比较；所有的验证节点最终在规定的时间内对最新的合约集合达成一致。

iii. 最新达成的合约集合会以区块的形式扩散到全网，每个区块包含以下信息：当前区块的 Hash 值、前一区块的 Hash 值、达成共识时的时间戳、以及其它描述信息；同时区块链最重要的信息是带有一组已经达成共识的合约集；收到合约集的节点，都会对每条合约进行验证，验证通过的合约才能最终写入区块链中，验证的内容主要是合约参与者的私钥签名是否与账户匹配。

最后，当区块链写入通过验证的合约后，将启动智能合约的自动执行过程，包括如下步骤：

i. 智能合约会定期检查自动机状态，逐条遍历每个合约内包含的状态机、事务以及触发条件；将条件满足的事务推送到待验证的队列中，等待共识；未满足触发条件的事务将继续存放在区块链上。

ii. 进入最新轮验证的事务，会扩散到每一个验证节点，与普通区块链交易或事务一样，验证节点首先进行签名验证，确保事务的有效性；验证通过的事务会进入待共识集合，等大多数验证节点达成共识后，事务会成功执行并通知用户。

iii. 事务执行成功后，智能合约自带的状态机会判断所属合约的状态，当合约包括的所有事务都顺序执行完后，状态机会将合约的状态标记为完成，并从最新的区块中移除该合约；反之将标记为进行中，继续保存在最新的区块中等待下一轮处理，直到处理完毕；整个事务和状态的处理都由区块链底层内置的智能合约系统自动完成，全程透明、不可攥改。

典型的以太坊智能合约 2.0，从编译到执行的过程如图 19 所示，可以发现传统的智能合约 2.0，其实只是一个自动化程序，并不具备任何智能。

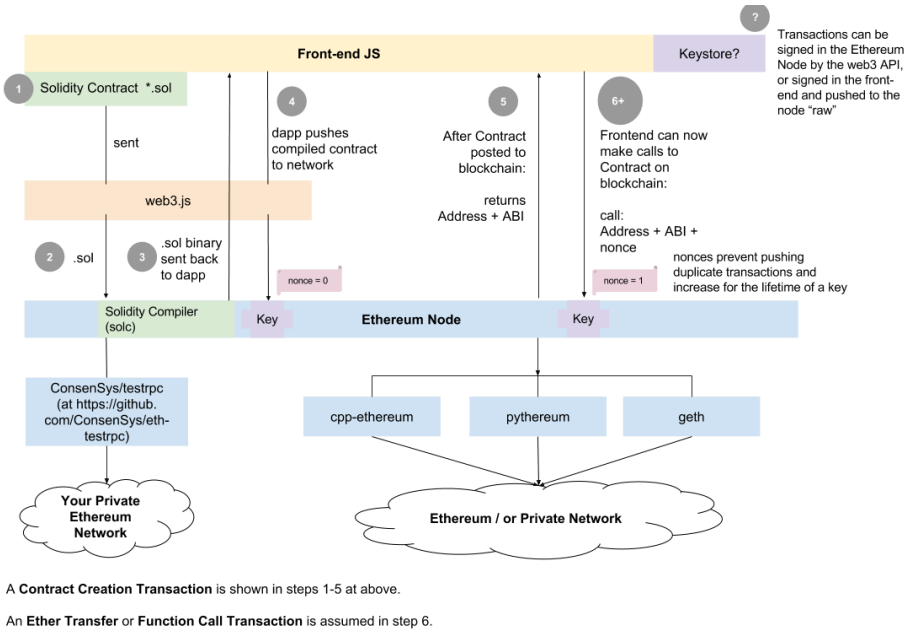


图 19 典型的智能合约 2.0 创建与执行过程

### （2） 基于 AI 辅助的安全智能合约执行

针对智能合约 2.0 的各种缺陷，MATRIX 采用基于 AI 辅助的合约执行机制，合约执行过程不仅自动化，而且真正具备智能化：

（1） 在合约拟定阶段，参与合约的双方将通过控制链公布的安全 AI 模型以及 MATRIX 提供的智能合约安全助手软件，审查合约是否存在缺陷，并根据审查结果进行修改，自动生成双方“权利”与“义务”的代码，直到合约完成满足安全审查规范为止。

（2） 在有效性验证阶段，由于该合约需要全网达成共识确认；此时的合约外部条件可能发生变化，因此每个验证节点的 AI 虚拟机除了确认合约签名一致性外，将额外审核合约是否满足要求，保证各种执行条款与条件选项满足完备性，并具备可执行性。如果合约方支付额外的费用，校验节点可以启动额外的条件审查与预执行功能，动态嗅探合约中新出现的各种漏洞。当合约有效性验证通过后，将写入区块链，并进入自动执行阶段。

（3） 在合约自动执行阶段，通常会出现各种由于无法预见未来，而产生的各种漏洞，此时执行合约的 AI 虚拟机节点可以通过 AI 自动判决机制，并基于 MATRIX 制定的规则条款，对出现的漏洞进行弥补，确保合约顺利执行。另外，当参与方产生矛盾，智能合约无法正常执行时，MATRIXAI 虚拟机将通过内置 AI 模型提供解决方案，并协助解决。

当智能合约执行完毕后，MATRIX 附属的智能工具可以对合约中间步骤以及对应的事务处理与状态进行分析。用户可以将该合约执行的结果，进行模型行为归纳和优

化，并通过节点提交。如果 MATRIX 的各个节点对该模型取得共识，该模型将写入区块，并作为用户模型发布，从而丰富 MATRIX 的合约模型库。

对于合约执行阶段出现诸如“钓鱼”欺骗的行为，则可以通过两种途径解决：

（1） 通过 AI 训练，获得相关欺骗行为的预警，并在形成共识过程中，针对这一行为进行识别，从而拒绝合约执行。

（2） 对钓鱼欺骗行为，由被欺诈方提供 AI 模型，对欺诈方进行行为模型和钱包地址标记，实现类似信用评价的体系。后续 AI 将自动判别该行为特征，从而阻止再次发生。

对于合约执行阶段出现无法转账等行为，则在合约挂起一定时长后，校验节点执行 AI 审查，确定合约的可执行性，并通过内置 AI 模型规则，推进合约的执行。而此类基于 AI 判断的合约执行，需要通过全网 AI 共识完成。

详细的基于 AI 辅助的智能合约执行过程如图 20 所示：

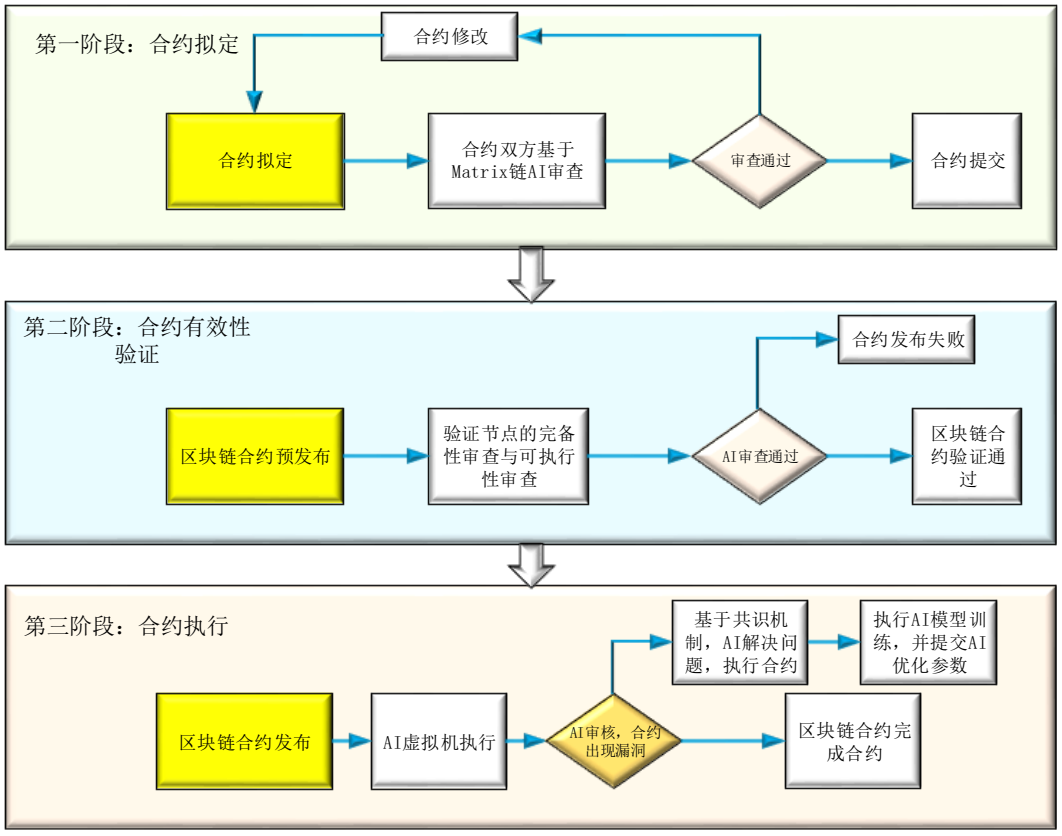


图 20 基于 AI 辅助的智能合约执行过程

### （3） 基于 AI 脚本模型的安全智能合约

智能合约 2.0 实际是一个支持字节操作码的有限状态机，通常需要用户描述交易模型的参数细节以及执行过程，很容易出现问题。即使后续发明了多种高级语言，通

过编译形成对应的字节码，用户仍然需要编写相关的模型描述。由于用户人工描述模型的不准确性和不完备性，往往各种漏洞就在其中发生。而在智能合约执行过程中，即使用户发觉这种漏洞，也无能为力，无法申述。MATRIX 则是通过事先在模型中引入 AI 判决模型，并支持模型更新的方式，解决这一问题。但如果能够直接避免漏洞，则对用户更加友好。MATRIX 通过引入基于 AI 脚本模型的智能合约解决这一问题。

当用户准备发起一个安全智能合约，可以通过查找 MATRIX 的智能合约基础模型库，匹配当前需要发布的智能合约以及任务。如果没有完整匹配的模型，则 AI 通过模型组合完成基础匹配，剩下的未匹配部分，则由用户通过 AI 脚本胶合。

当用户提交基于 AI 脚本模型的智能合约后，AI 虚拟机将对用户合约进行分析。对于直接调用智能合约基础模型库的部分，AI 按照 MATRIX 定义执行；对于脚本部分，则通过解释器进行安全审查后再执行。所有执行行为均需要通过 AI 辨识，确认行为规则，防止恶意攻击。这种执行方式的好处在于用户无需关注模型的描述，而是关注于模型的目的，从而简化开发。

由于基于 AI 脚本模型的智能合约需要大量的基础安全模型，因此 MATRIX 将初期内置部分交易模型，后期通过用户主动提交安全交易模型方式，完善整个模型库。每个个体用户提交的模型在完成共识审查后，将获得以 Royality+Option 方式分配的 MATRIX 货币奖励，用于鼓励用户积极发布自定义模型。

基于脚本的模型构架如下：

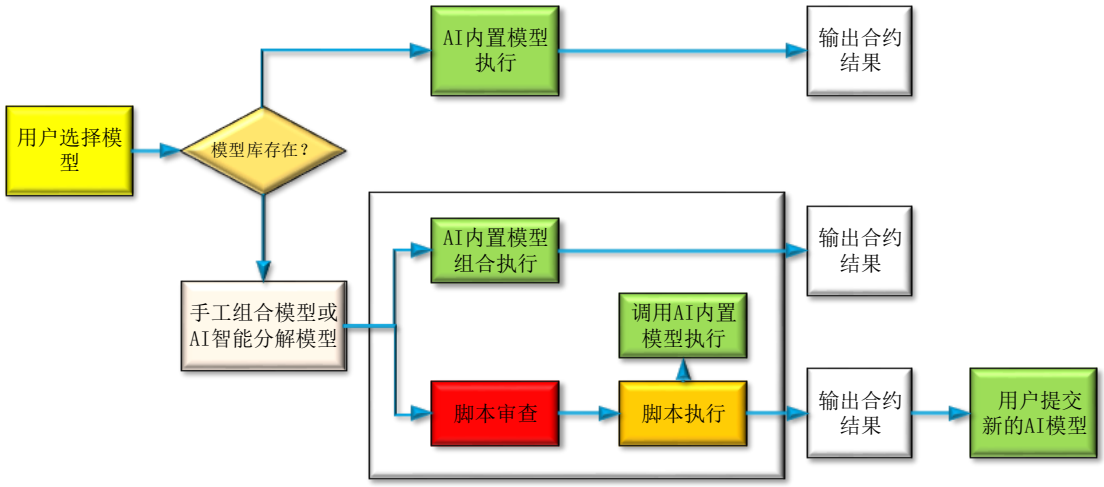


图 21 基于脚本的 AI 模型执行

### (4) 基于 AI 的托管交易

智能合约 2.0 十分依赖于发送给它的信息的质量。通常，智能合约 2.0 通过各种情况选择和分支帮助解决问题，本质上是一种“预言机”，必然会出现“预言机”无法面对的情况，例如信息源消失，或者新的更好的信息源出现，或者判断条件改变等。出现上述现象的根本原因在于：智能合约 2.0“无法预见未来”。因此，安全智能合约设计了基

于 AI 的托管交易，实现在未来时刻，人工智能按照用户目标要求，通过训练模型和函数约束，执行合约代码。

用户在使用托管交易时，仅提供目标要求，而实现细节和交易代码以及中间的执行过程，均由 AI 完成。

### （5） 基于 AI 的多路撮合交易

传统的智能合约通常需要严格匹配，才能完成交易，正常情况下不能拆单，也不能支持多方交易，存在诸多限制。例如，用户 A、B、C 存在一个连环交易合约。

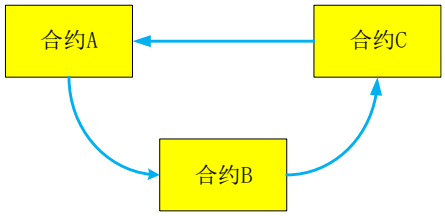


图 22 合约的撮合交易示意图

因此，用户往往通过中心化的交易所完成类似拆单和多方交易的活动，甚至简单交易也通过交易所完成。但交易所通常要求用户将法币或者代币充值到交易所的银行账户或区块链地址中，然后用户利用交易所虚拟地址进行 IOU 记账。而执行合约时，用户实际是基于 IOU 基础上进行交易。用户需要通过交易所申请 IOU 兑换成法币或区块链代币，并获得通过，才能完成整个交易。在交易过程中，交易所替用户保管资产的能力是用户最大的风险；同时用户还需承担交易所运营者商业道德带来的其它风险。

MATRIX 针对上述交易模型，建立一个基于 AI 的智能合约撮合系统。验证节点在验证合约集的同时，对用户发送的合约集合进行扫描与分析，并确定各种交易环路；在执行过程中则进行动态撮合，寻找最大的交易环路，并寻找到最低的交易成本，实现多个对手方的多个订单成交，避免中心化交易所带来的弊端。典型的撮合交易示意图如下：

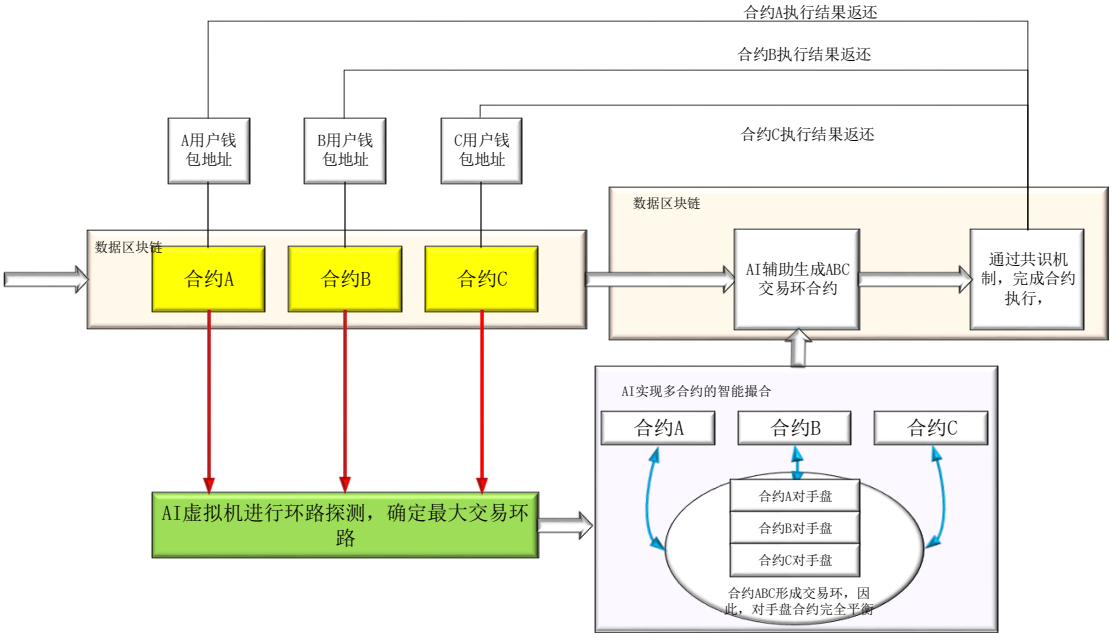


图 23 基于 AI 的多合约撮合系统

### 5.5.3 安全智能合约的基础实现

由于安全智能合约的核心思想是通过建立各类 AI 模型，完成合约的审查，并保障合约执行。因此，如何将这些基础 AI 模型粘连（glue）形成用户最适宜的模型是 MATRIX 考虑编程语言的重点。

目前，MATRIX 采用 Lua 作为安全智能合约使用的默认编程语言。Lua 是一种轻量小巧的脚本语言，满足图灵完备的要求，采用标准 C 语言编写并以源代码形式开放，其设计目的是为了嵌入应用程序中，从而为应用程序提供灵活的扩展和定制功能。

Lua 的核心特点包括：

- 轻量级：它用标准 C 语言编写并以源代码形式开放，编译后仅仅一百余 K，可以很方便的嵌入其它程序中。
- 可扩展：Lua 提供了非常易于使用的扩展接口和机制，MATRIX 设计的各种 AI 模型及功能，Lua 可以很方便的调用。
- 其它特性：
  - 支持面向过程(procedure-oriented)编程和函数式编程(functional programming)；
  - 自动内存管理；只提供了一种通用类型的表（table），用它可以实现数组，哈希表，集合，对象；

- ✧ 语言内置模式匹配；闭包(closure)；函数也可以看做一个值；提供多线程（协同进程，并非操作系统所支持的线程）支持；
- ✧ 通过闭包和 table 可以很方便地支持面向对象编程所需要的一些关键机制，比如数据抽象，虚函数，继承和重载等。

因此，MATRIX 将设计一套支持 Lua 的脚本解释器与编译器的 AI 虚拟机，以完成 Lua 的字节码的解释执行。此外，AI 虚拟机将添加 Lua 的 AI 模型调用接口。在 MATRIX 中涉及到智能合约的操作或块同步验证中，节点将从区块中取出对应的合约字节码，并利用 AI 虚拟机执行对应的代码，并通过参数调用 AI 模型，从而获得合约字节码的运行结果。AI 虚拟机的执行结果与相关上下文状态变化将被区块链使用。

需要说明的是，由于 MATRIX 提供了对智能合约 2.0 的向下兼容性，因此在 MATRIX 的节点上，将通过 AI 虚拟机以字节解释器方式对对智能合约 2.0 进行模拟执行。

### 5.5.4 安全智能合约对数字资产的支持

绝大部分的区块链应用是围绕数字资产展开的，而用户通常愿意创造自己的资产类型，并利用智能合约来控制它的发行和交易逻辑。但在传统区块链设计中，每一种数字资产都需要自行开发一套基于智能合约的业务流程，这种方式类似于“每个人都重复发明一遍轮子”，该实现过程是极其低效，且容易出错的。

在安全智能合约中，MATRIX 利用 AI 技术创建了大量基于数字资产的交易模型与业务流程。任何一个用户在创建自己的数字资产时，仅需调用相应的 MATRIX 内置资产合约接口，即可生成完备的数字资产体系；对应的数字资产交易逻辑，既可以用户自行开发，也可以通过 MATRIX 的各种 AI 模型生成，还可以直接继承 MATRIX 定义的数字资产模型特性。

在保证安全前提下，MATRIX 能够便捷的创造用户自定义数字资产，这就意味着 MATRIX“自金融”时代的到来。每一个用户均在 AI 审查合格的前提下，能够按照合约方式，将自身的某项属性按照代币形式发售，并在 MATRIX 上安全可靠的交易。例如，某个创业者将自身的创意在 MATRIX 上以代币形式发售，同时按照智能合约的方式进行各种权属的交易与变现，从而获得足够的支持；而购买创业者创意的用户则能够享受对应的权益。用户创造的数字资产通常情况下只能是线上资产，无法通过传统的智能合约与线下资产与行为关联互动。而 MATRIX 通过各种扩展，引入 AI 判决机制与可信网关设备，实现线上与线下的联通与互动。

### 5.5.5 安全智能合约的扩展

所有传统区块链存在的问题包括以下几类：

（1） 智能合约需要根据一些外部事件，作为合约依据，改变自己的行为；

（2） 智能合约执行过程中从外部服务获取数据，并以此作为下一步执行的依据；

（3） 智能合约试图直接完成线上线下的交易。

（4） 智能合约中无法隐藏机密数据；

其中问题（1）（2）的实质是要求区块链外部的数据源能够对所有节点要求保持一致。站在区块链的角度，外部数据源实际是不可控的、未来的行为也是未知的。因为，数据源可能会在收到不同节点请求时，给出不同的响应、甚至暂时不可用。这意味着：区块链获取的外部数据是不确定的。而区块链的根基在于共识机制，而共识机制的基础在于区块链上所有发生的事情必须是确定的。因此，当外部数据源行为不可控时，必然带来共识机制的混乱，整个区块链就崩溃了。

问题（1）（2）的出发点实际是为了解决线上（区块链）与线下（外部世界）的互联互通问题。因此，MATRIX 通过引入 AI 审核与多个独立可信网关解决上述问题。具体执行步骤如下：

步骤（1）：当智能合约需要读直接调用数据时，AI 虚拟机将进行智能审核，并确定该合约需要读取外部数据以及对应的安全性。当安全性不通过时，AI 虚拟机将按照预定规则进行后续流程处理，如果通过，则进入步骤（2）。

步骤（2）：当确认需要读取外部数据源时，将通知 MATRIX 上所有可信网关进行外部数据提取；可信网关将读取外部数据，并将该数据写入到公开账本中。

步骤（3）：AI 虚拟机将对各个可信网关提供的数据进行审核，并进行数据置信度分析；例如对总是提供一致性数据的网关给予奖励，对于提供错误数据的网关则给予惩罚。

步骤（4）AI 虚拟机将审核通过的数据写入独立的区块链数据区域，并作为链上合约执行的依据。

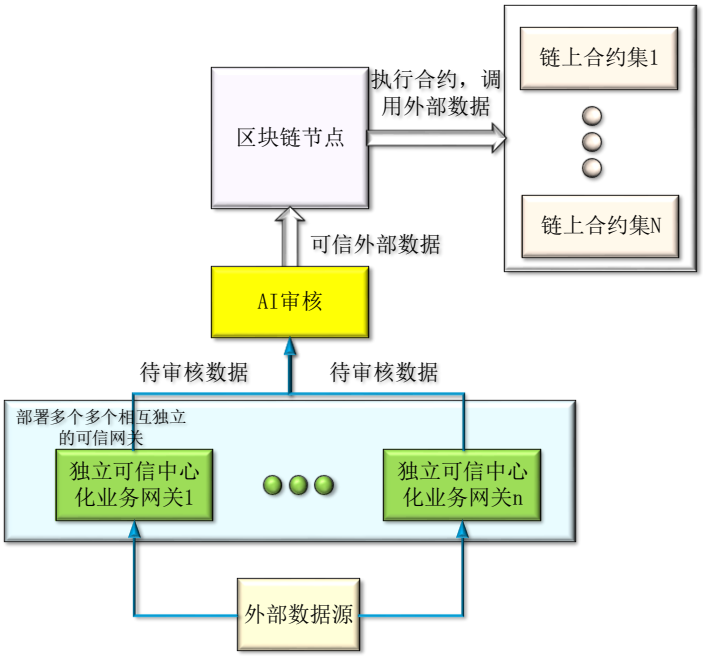


图 24 智能合约与外部数据源的交互

通过上述架构，MATRIX 很容易打通线上与指定的线下交易系统，展开各种交易方案。典型的，例如某个合约要求指定英超足球的比赛结果作为合约指定的依据；又譬如，指定 Nasdaq 特定日期的指数作为合约依据等等。因此，问题（3）也相应解决。

而问题（4）的实质是要求智能合约支持数据保密，其它非相关用户不能获知该数据的细节。这实际是一个两难问题，如果智能合约不公开，则全网无法达成共识；而公开数据，则因为着无法隐藏机密数据。传统的区块链通常通过部分共识机制，或者通私有合约方式，实现仅特定获得私钥的参与方能够访问机密数据的要求；但上述模式实际是对区块链安全机制进行了修订，其中的典型包括摩根大通“Quorum”区块链项目。

对于问题（4）,MATRIX 同样采用可信网关处理的方式。所有的机密数据均通过加密方式，提交给可信网关，并由可信网关存储于 MATRIX 的机密数据区；同时这部分数据的完整性验证与摘要内容则写入区块中。智能合约将这部分加密数据作为可信外部数据源处理。在合约执行过程中，任何节点均可以验证数据的存在性和可靠性；但只有得到授权的特定用户才可以通过可信网关验证加密数据。上述模式下，区块链的共识机制没有受到任何损害，同时客户的隐私也得到了保护。政府如果对某些特定数据进行监管，也可以采用类似机制完成。

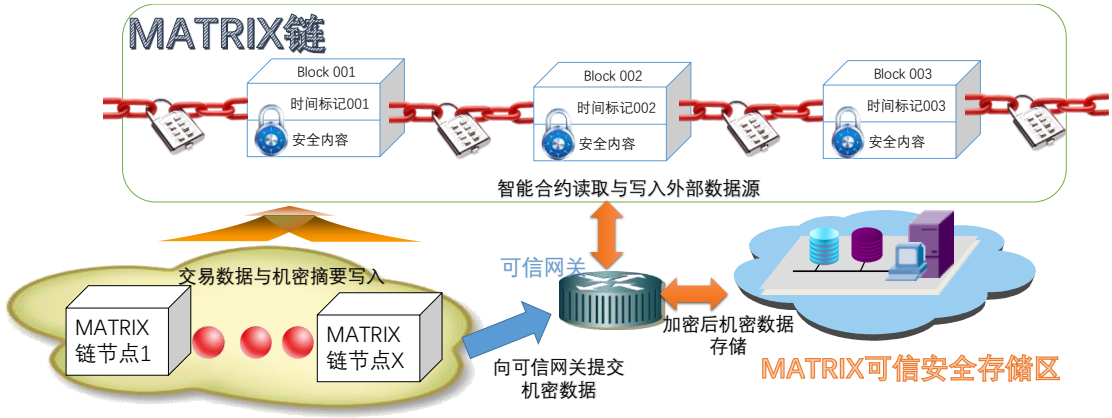


图 25 MATRIX 链可信网关与机密数据的处理

由于，MATRIX 引入可信网关加 AI 审核机制，因此面临着海量的外部数据接口需求。对此，MATRIX 建立了 AI 插件机制，由合约用户编写和使用插件，通过开放编程接口，经过共识审核，实现外部世界与区块链数据定制化链接。通过共识可信机制，实现外部数据与区块链数据共享。典型的执行方案如下：

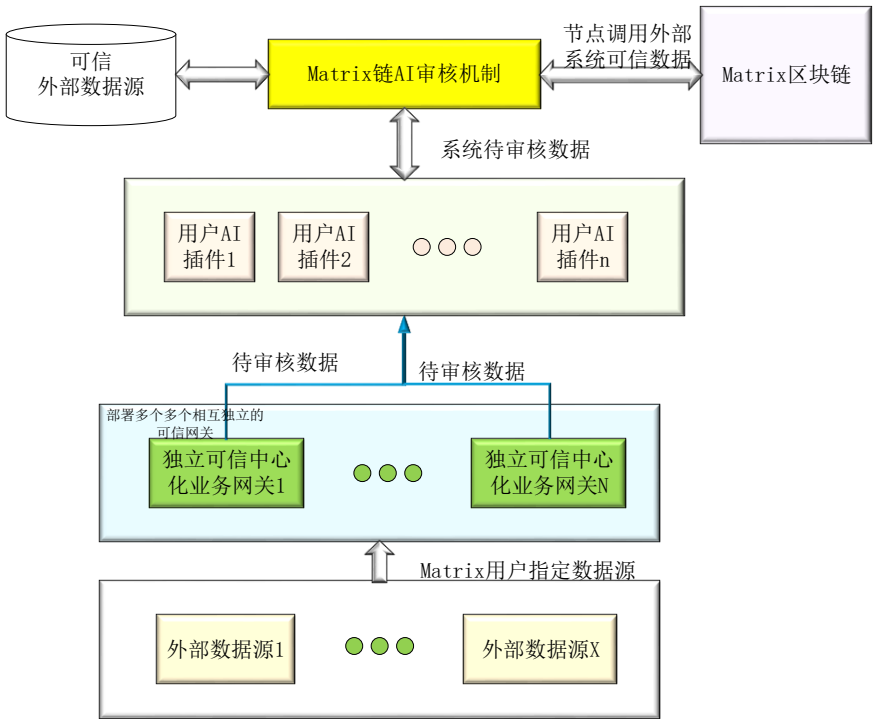


图 26 MATRIX 的 AI 插件机制

通过上述方式，每个用户均可以编写或者使用特定的 AI 插件，实现个性化的外部数据交互。例如，某个用户编写了 NBA 的每场比赛结果插件，相关用户可以通过 MATRIX 插件调用规则，即可实现基于 NBA 比赛结果的智能合约。

通过 MATRIX 的安全智能合约，用户可以非常便捷的创造自己独特的资产；通过 MATRIX 引入的可信网关与 AI 审查机制，MATRIX 打通了线上与线下，支持外部数据源与内部智能合约的交互；通过 MATRIX 的可信网关与 AI 插件机制，用户可以创造各种自定义的线上线下交易模式；因此 MATRIX 的业务创新与金融创新可以层出不穷。结合 MATRIX 独有的 AI 进化机制，可以确定未来业务模式无比精彩。

### 5.5.6 安全智能合约为新手提供的保护

为吸引更多的用户使用和完善 MATRIX，MATRIX 为用户友好和保障用户安全，做出了大量的预设性设计，目前主要包含三个方面：（1）预设模型：根据常规交易模型，设计大量的交易模板，并在模板中设计保护机制；（2）预设保护：对用户完成的交易脚本，根据用户意愿，自动链接保护脚本，确保用户不会因为自身失误，导致严重损失；（3）用户定制模型：在用户知情且同意前提下，根据用户行为习惯，推荐设计 AI 合约，并支持 AI 托管服务。

#### （1） 预设模型

按照“二八定律”，80%的交易往往发生在 20%的模型上。因此，MATRIX 在开始阶段，将提炼用户交易行为，重点设计大量的常用交易模型，保证用户基本能够匹配这些交易模型。新手用户在交易时，仅需选择模型，并输入自己的需求与许可条件即可，后续的交易实现细节以及智能合约发布，均由智能交易助手完成。由于采用预设模型，对应的合约漏洞与陷阱相对较少，同时由于 AI 的存在，能够不断修正模型，实现交易模型库的完善。

另外，MATRIX 的预设 AI 会根据交易列表进行分析，并通过内置训练方案，实现新手交易模型的动态扩展与更新，促进 MATRIX 易用性与安全性的平衡发展。

#### （2） 预设保护

对于部分用户个性化定制交易的意愿，MATRIX 提供全方位的安全支持。用户在编写脚本阶段、合约有效性验证阶段、合约执行阶段，均有安全审核与安全建议机制。

在编写脚本阶段，MATRIX 的开发向导将通过语法分析确定基础漏洞；通过 AI 的语义分析，确定用户行为合理性，提出改进操作；通过静态边界检查，确认用户设定边界条件的合理性；通过动态随机测试，并根据约束条件和 AI 分析合约运行结果，确定用户动态运行漏洞。

在合约有效性验证阶段，验证节点将对合约进行合法化检查，通过 AI 审查嵌套合约是否存在安全陷阱或执行费用缺陷等问题；通过合约双方行为分析，排除钓鱼以及非法利用 AI 虚拟机本身漏洞的可能性；通过 AI 审查智能合约调用外部数据源与用户 AI 插件可能存在的问题。当验证节点对合约合理性评分低于一定程度时，将发出合约需要改进的消息，并拒绝合约共识。

在合约执行阶段，则重点确保合约的安全执行，并在合约方发生冲突时，利用 AI 模型进行分析，确定冲突化解规则。在合约执行完毕，但存在缺陷时，例如钱包无法转账时，则利用 AI 进行值守，确定最终的合理解决方案。

再次强调：所有的保护机制与保护原则，均是在用户自愿的情况下启动并生效。MATRIX 的设计原则是无歧视原则，任何合法代码均可运行，只要用户支付相应的费用即可。

#### （3） 用户定制模型

MATRIX 在用户许可情况下，将通过 AI 分析用户的交易记录，并进行模型辨识，从而获得对应的行为特点。当 MATRIX 辨识出用户行为后，将在用户交易时，定制化保护机制，优化对应的交易速度，并在用户确定交易成本的基础上，选择最佳的交易方案。

后续，MATRIX 将持续对用户定制化模型方案进行改进。

### 5.5.7 AI 交易模型的演进

MATRIX 的 AI 交易模型通常由用户提出。个体用户或 MATRIX 友好用户，将通过对交易数据的分析与实际训练，获得各种合适的 AI 交易包含模型与 AI 收益模型。上述模型将通过 AI 模型消息提交，并通过全网投票表决，从而纳入系统交易模型库中。

对于优秀的交易模型，在采纳超过一定门限后，系统将在交易系统中发放奖励，促进友好用户对 MATRIX 改进的鼓励。

## 5.6 MATRIXAI 服务

由于 MATRIX 内置原生的 AI 功能，并具备通用的 AI 执行引擎，因此在 MATRIX 上，每个节点均具备独立执行 AI 任务的能力；而通过 MATRIX 专有的控制区块链，各个分布的节点能够结合起来形成一个整体，以便于执行各类大型或巨型 AI 任务。

更进一步，由于 MATRIX 具备强大的控制区块链，很容易就能实现多个 AI 服务相互协作、相互调用的问题。在 MATRIX 中，用户通过简单的安全智能合约机制，就能定制一个多点多任务协作服务。

在 AI 服务架构中，MATRIX 可以承担两种角色：（1）AI 服务供应商；（2）多个外部 AI 服务的协作商。

第一种角色很容易理解：MATRIX 自身即为一套大规模 AI 基础设施，并具备丰富的 AI 服务模型。 MATRIX 的控制链运行机制也决定了，MATRIX 上的 AI 服务还能与专有 AI 服务云结合，实现更加丰富的 AI 服务。

第二种角色则是 MATRIX 具备将多种外部服务整合运行的能力。MATRIX 能够通过安全智能合约，将外部不同的 AI 服务连接到一起；并利用外部服务接口，实现用户与各个外部服务之间的清算。

### 5.6.1 单个节点的 AI 服务

由于 MATRIX 是建立在 AI 基础上的交易链，因此任何一个 AI 节点均具备一定的 AI 算力。在 MATRIX 上的单个节点既可以选择挖矿实现自身收益，也可以选择通过对外提供 AI 服务实现收益。

单个节点的 AI 服务，通常需要节点响应 MATRIX 上的 AI 服务合约请求，并完成合约解析。当节点确认参与 AI 服务合约后，将通过控制链检索对应的 AI 参数，并通过数据链获得服务数据。当单个节点执行 AI 服务合约，并输出对应结果后，由 MATRIX 进行合约结果检查，中间可能需要调用可信中心服务进行验证。当 MATRIX 确认 AI 服务完成后，将通过一系列流程完成最终合约。对应的，单个节点也能获得相应服务收益。

### 5.6.2 多节点协作 AI 服务

当单个节点提供 AI 服务能力不够时，可以通过 MATRIX 内置的控制链，实现多个节点协作并提供 AI 服务。

常规的区块链签署多方合约后，很难实现灵活的用户参与与退出机制。MATRIX 通过 AI 模型，智能管理合约，能够支持多用户灵活 AI 服务。当用户希望临时加入时，AI 将临时切割部分服务任务给对应的用户，并利用控制链参数通知。对应的，智能合约也能通过 AI 分析，进行细分切割。当用户希望中间退出时，AI 可以收回对应的任务，并利用控制链参数进行调整。对应的，智能合约也能进行相应的调整。当且仅当原始智能合约可分割时，AI 节点服务能够在中间阶段获得收益；当不支持时，任何中间加入和退出的用户必须等待合约整体完成后，才能获得收益。

上述多节点协作 AI 服务，能够有效实现多种形态的服务。

典型的实现案例包括：MATRIX 通过 AI 参数配置，发布一个以太坊挖矿的智能合约，各个节点可以通过协作方式，完成以太坊的挖矿任务，而参与节点可以随时进入，也可以随时退出。在完成一定任务后，各个节点均能获得收益。

另外一个典型案例包括：某个用户以代币形式发布一个全网人脸识别的智能合约时，传统的区块链往往需要通过一系列的操作，通过调用外部专业的 AI 服务完成该任务。而在 MATRIX 中，当某个独立个体用户认为当前任务能够通过调用 MATRIX 其它用户的 AI 能力完成，并能够获得收益时，就可以对此做出响应。该独立用户将基于原有任务，发布一个新的协作智能合约，通过协作多个 MATRIX 节点的 AI 算力，完成原始的全网人脸识别任务。

因此可以认为：MATRIX 的任何一个节点都具备多节点 AI 协作服务能力合约；而任何一个用户均可以利用 MATRIX，透明享受多点 AI 服务。

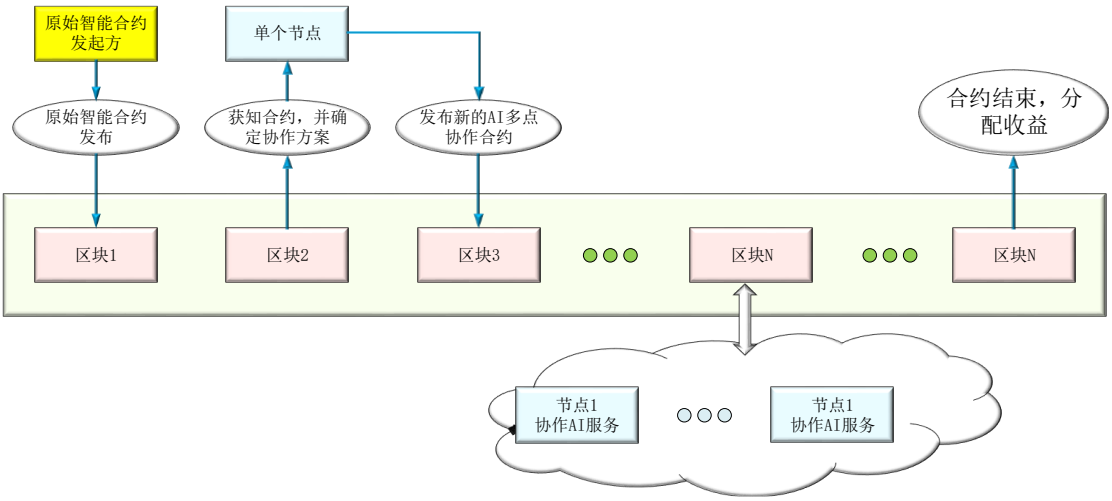


图 27 MATRIX 的多点协作 AI 服务

### 5.6.3 MATRIX 提供的接入服务

作为 MATRIX 附属的基础设施，MATRIX 将在云端部署大量的服务节点。该节点将为 MATRIX 的使用者提供一个简单访问本区块链的方法。使用者无需拥有 MATRIX 的节点，仅仅需要提供接入认证，即可链接到 MATRIX 的云端接入服务节点。用户在云端服务节点上，能够启动各种智能合约交易，也可以享受整个 MATRIX 的服务。

一个典型的应用场景包括：例如某个用户希望通过 MATRIX AI 矿机完成智能代币交易。此时，用户仅需要安装一个 MATRIX 的微信小程序或 APP。当用户激活微信小程序或 APP 后，用户可以选择登录到特定的服务节点，然后将该服务节点作为获得区块链服务的锚点。当用户锁定锚点后，可以基于该锚点获得专有的 AI 云服务。

上述实现的典型示意图如下所示：

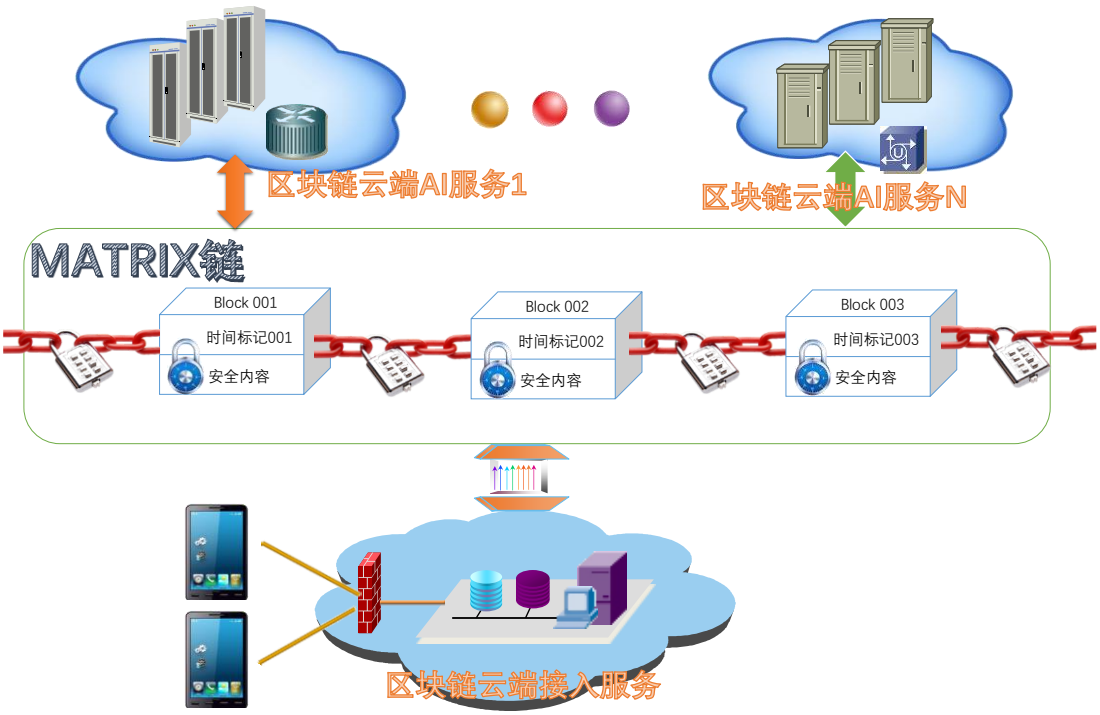


图 28 MATRIX 的 AI 接入服务示意图

### 5.6.4 MATRIX 对外部 AI 服务的整合

MATRIX 不仅自身可以提供 AI 服务外，还可以作为 AI 集成服务商，通过智能合约集整合多个外部的 AI 服务。MATRIX 整合外部 AI 服务的核心在于通过安全智能合约，能够动态协调各个外部的 AI 协作关系，支持多个 AI 服务之间相互调用。

对用户而言，MATRIX 则是一个支持海量 AI 服务的接入端服务器与应用服务器，任何的 MATRIX 上各个 AI 服务器协调调用以及费用结算，用户无需了解。用户只需与 MATRIX 专用部署的 AI 接入服务节点，签署智能合约即可享受服务。

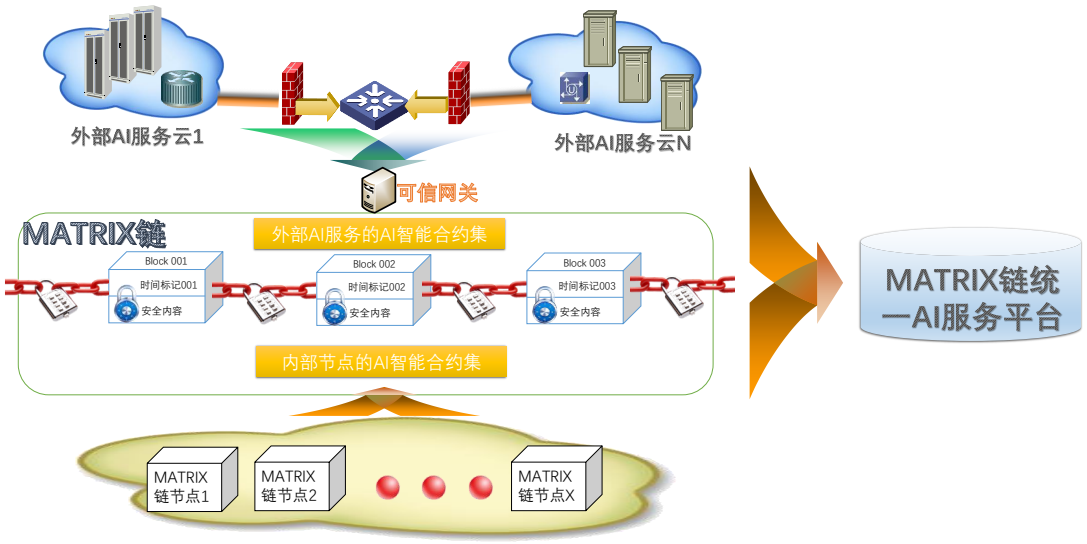


图 29 MATRIX 整合外部服务后的统一 AI 服务平台示意图

一个典型的应用例子，就是基于 MATRIX 的智能投顾。

传统的投资顾问服务，由于很难定性量化，因此采用长期趋势预测、中期数据报告、短期预警等模糊的报告方式，客户很难实时更新信息，并基于此进行对应的操作。而 MATRIX 上，将利用人工智能，建立一个实时开放的智能投顾服务。该服务将利用贝叶斯推理机与 DNN 数字神经网络对过去的投资产品，进行各种时间维度的序列分析与深度学习，形成 AI 模型。当用户签署智能投顾服务的智能合约后，就可以使用 MATRIX 上的各项智能投顾服务。

当客户群体规模急剧扩大，瞬时峰值需求超出 MATRIX 的专用 AI 服务器能力时，MATRIX 将通过控制区块链，发布内部智能合约服务，从而获得 MATRIX 部分节点的响应支持。响应智能投顾服务的 MATRIX 节点，将利用自身的 AI 能力为智能投顾服务。

当 MATRIX 内部 AI 能力无法满足要求时，MATRIX 将通过可信网关，导入外部的各种 AI 服务基础设施，并通过预定义的协作模式实现 AI 服务操作。

## 6 MATRIX 设计概要

MATRIX 初始版本包含两类区块：（1）分布式控制链区块，该区块包含标准参数区块表头、数据块链格式定义、公共 AI 模型参数列表、AI 参数扩展数据块指示、用户 AI 模型参数列表；（2）数据链区块，该区块结构与以太坊类似，包含标准的数据区块头、交易列表、叔父列表。

MATRIX 中的分布式控制链区块按照固定速率生成，自身行为独立，不依赖于其它数据链；而数据区块链则需要对最新生成的控制链区块进行解析，从而确认新的数据区块更新频率以及对应的参数设置。常规情况下，每个数据区块链参数在较长时间内处于稳定状态，除非 MATRIX 区块参数的 AI 模型，判断现有的数据区块链需要及时优

化，或者 MATRIX 本身受到了非法攻击，因此需要改变参数，保证整个 MATRIX 的生存优化。

MATRIX 直接定义了创世控制区块和第一个数据区块，然后按照定义的时间顺序，依次创造后续的控制区块与数据区块。

## 6.1 MATRIX 的分布式控制链区块头结构

MATRIX 的分布式控制区块头（Block header）结构如下 ，这一结构主要用于指定 AI 参数列表，并内置添加用于 AI 服务的模型参数与更新 AI 模型参数的功能。由于 MATRIX 支持多数据链结构，因此该控制区块头属于动态可变类型，通过内置的数据区块链 AI 参数指示数量 AIChainNumber 来确认区块大小。

| Bit 位宽 | 字段定义 | 字段说明 |
|---|---|---|
| 32 | nVersion | MATRIX 版本号 |
| 256 | HashPrevBlock | 前一个区块头的 Hash 值，目前基于 RNN 算法得到。 |
| 32 | AIChainNumber | 本区块包含的区块链数量，该数量将指定本区块头中包含有多少个区块链 AI 参数列表组。在 MATRIX 仅设定一条数据区块链时，AIChainNumber 为 1。当数据区块链包含多条时，则 AIChainNumber 设定为当前准备更新的参数链大小。因此区块头大小是动态可变的。从维护和实现角度，目前建议单个区块头中中 AIChainNumber 不大于 16。 |
| 32* AIChainNumber | AIchainSN[AIChainNumber] | 用于指示后面对应的 AI 参数作用于哪一个数据链编号。目前存在 AIChainNumber 条需要指示的数据链 |
| 256* AIChainNumber | HashSystemAIParameterList [AIChainNumber] | 用于指示对应数据链编号对应的本次标准 AI 参数更新列表 Hash 值 |
| 256* AIChainNumber | HashSystemTransModelList [AIChainNumber] | 用于指示对应数据链编号对应的本次新增 AI 交易模型列表 Hash 值 |

| | | |
|---|---|---|
| 256* AIChainNumber | HashUserAIParameterList [AIChainNumber] | 用于指示对应数据链编号对应的新增用户定义 AI 参数列表 Hash 值 |
| 256* AIChainNumber | HashUserTransModelList [AIChainNumber] | 用于指示对应数据链编号对应的新增用户定义 AI 交易模型列表 Hash 值 |
| 256 | nNonce | 随机数，比特币是 32 位，MATRIX 为 256 位，用于保证整个区块满足 RNN 算法校验 |
| 32 | nTime | 更新时间，32 位 |
| 32 | nBits | 当前运算难度，32 位 |

参数的详细说明如下：

- nVersion，区块版本号，升级时改变。
- AIParameterVersion，本次区块定义的 AI 参数版本号，若当前没有更新系统 AI 参数或新增系统交易模型，则参数版本不变化。
- hashPrevBlock，从前一区块获得。
- AIChainNumber，数据区块链 AI 参数指示数量。
- HashSystemAIParameterList，本字段包含当前区块 AI 参数列表的 Merkle 树计算。通过该字段列表能够调整后续数据区块的字段配置与参数配置，是本区块链能够自主进化的典型标志。
- HashSystemTransModelList，本字段包含当前区块系统交易模型列表的 Merkle 树计算。通过该字段列表能够不断丰富系统的交易模型，并能完成各种交易缺陷弥补。
- HashUserAIParameterList，本字段包含当前区块用户 AI 参数列表的 Merkle 树计算。通过该字段列表，单个用户能够自定义交易的 AI 参数配置，从而保障用户交易的安全可靠性。此外，用户也可以通过该字段上报自身的 AI 能力，方便 AI 服务或其它节点调用。
- HashUserTransModelList，本字段包含当前区块用户自定义交易模型列表的 Merkle 树计算。通过该字段列表，单个用户能够发布自身的 AI 模型，并通过 AI 控制链发布，从而实现付费购买 MATRIX 其余用户的 AI 算力，或有偿开放自身 AI 算力。
- nNonce，MATRIX 提供了 $2^{256}$ 种可能取值，而比特币提供 $2^{32}$ 种。

- nBits，由全网算力以及分配给 AI 的服务算力计算获得。目前，由 AI 参数决定如何动态调整难度，最小调整间隔为 16 个区块 1 次，最大为 2048 个区块调整一次。（比特币每 2016 个区块调整，以太坊每个区块调整一次）。
- nTime，基本取机器当前时间轴。

由于 AI 参数的重要形，矿工通常需要最大限度的包含系统 AI 参数列表、系统 AI 交易模型列表、用户自定义 AI 参数列表、用户自定义交易模型列表，如果不能包含，则按照上述顺序，进行优先级排列。对于列表内部，矿工则可以自由选择排布，并删减部分内容，从而形成最终的控制区块。

控制区块的头的构造过程如下：

1. 选择待确认各个 AI 参数列表，因为矿工可以从交易中获得手续费，所以一般构建区块时会选择尽可能多的交易，但是不能超过当前控制区块设定的容量上限。
2. 确定 Coinbase，这里记录假如该区块构建成功，矿工将获得的收益（手续费+奖励）。控制区块不支持幽灵协议。
3. 构造各个集合参数列表信息的 Merkle 树，然后根据 DNN 算法生成随机数 nNonce，写入其他参数。
4. 最终构造 MATRIX 控制区块头。

## 6.2 MATRIX 的分布式控制链区块内部结构

MATRIX 的控制区块单个区块链的结构提由两部分组成：

1. 控制链区块头；
2. 控制链参数与模型列表。

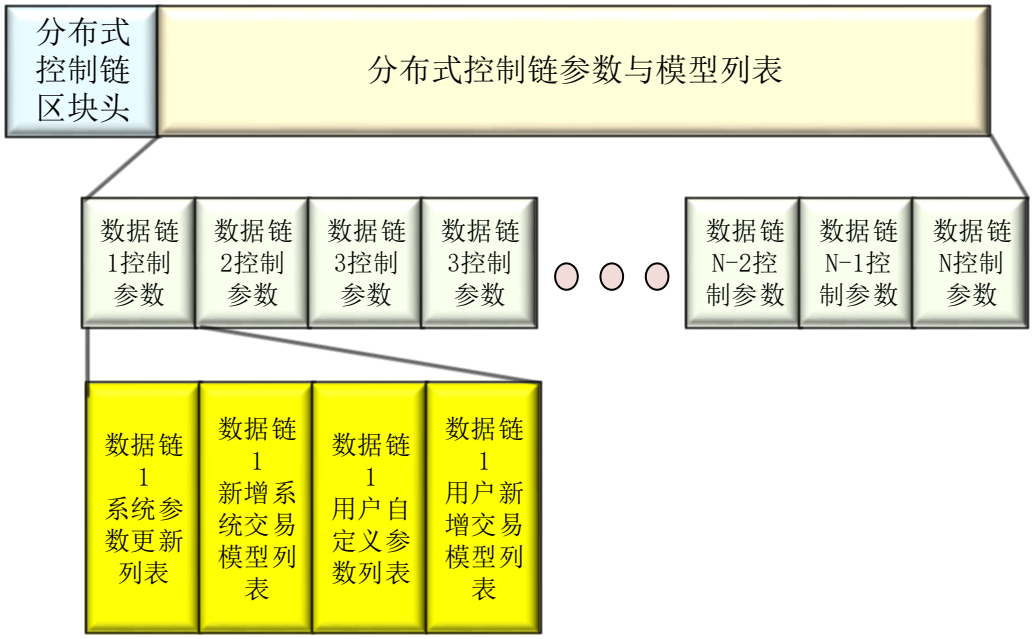


图 30 MATRIX 控制区块内部结构图

其中：

MATRIX 控制区块，将尽可能的容纳多条数据链的参数配置。当某个区块存在容量问题时，将采用 Round Robin 算法，保证每个数据链参数配置的公平性。

目前的参数配置方式如下：

DataChainParameter_list = [

DataChainParameter 1,

DataChainParameter 2,

...

]

而对应的每条数据链的参数配置，则采用如下方式定义：

DataChainParameter=[

SystemAIParameterList

SystemTransModelList

UserAIParameterList

UserTransModelList

]

另外，考虑减少数据链的参数解析运算量，促进新加入用户快速进入挖矿进程，MATRIX 将周期性的提供每一条数据链的完整参数，并设定对应的标志。

## 6.3 MATRIX 的数据区块头结构

MATRIX 的数据区块头（Block header）结构如下 ，这一结构与以太坊区块头类似，差异在于 Hash 算法采用 RNN 算法实现，同时引入 AI 参数版本。

| Bit 位宽 | 字段定义 | 字段说明 |
|---|---|---|
| 32 | nVersion | MATRIX 版本号 |
| 32 | AIParameterVersion | MATRIX 使用的 AI 参数版本号 |
| 256 | HashPrevBlock | 前一个区块头的 Hash 值，目前基于 RNN 算法得到 |
| 256 | HashTransListMerkleRoot | 交易记录的 Hash 树值，256 位值 |
| 256 | HashUncleBlockHeadRoot | 叔父节点区块的 Merkle 树值，256 位值 |
| 256 | nNonce | 随机数，比特币是 32 位，MATRIX 为 256 位，用于保证整个区块满足 RNN 算法校验值 |
| 32 | nTime | 更新时间，32 位 |
| 32 | nBits | 当前运算难度，32 位 |

参数的详细说明如下：

- nVersion，区块版本号，升级时改变。
- AIParameterVersion，当前交易使用的 AI 版本号，通过该版本号，能够通过控制区块链获得各种 AI 参数以及 AI 对应模型。
- hashPrevBlock，从前一区块获得。
- HashTransListMerkleRoot，本字段由矿工自行调整，变化来自于对包含进区块的交易进行增删，或改变顺序，或者修改 Coinbase 交易的输入字段。
- HashUncleBlockHeadRoot，本字段根据当前是否支持幽灵协议，即叔父节点是否能够取得矿币来决定，该参数由 AI 参数控制；当支持叔父列表时，将对所有叔父节点进行 Merkle 树计算，从而得到本字段；如果不支持，则该字段直接置零。

- nNonce，MATRIX 提供了 $2^{256}$ 种可能取值，而比特币提供 $2^{32}$ 种。
- nBits，由全网算力以及分配给 AI 的服务算力计算获得。目前，由 AI 参数决定如何动态调整难度，最小调整间隔为 16 个区块 1 次，最大为 2048 个区块调整一次。（比特币每 2016 个区块调整）。
- nTime，基本取机器当前时间轴。

一般来讲，HashTransListMerkleRoot 和 nNonce 是发挥挖矿自由度的地方。而 MATRIX 数据区块头构建的过程也与比特币类似：

1. 选择待确认的交易，因为矿工可以从交易中获得手续费，所以一般构建区块时会选择尽可能多的交易，但是不能超过 AI 参数设定的容量上限。
2. 确定 Coinbase，这里记录假如该区块构建成功，矿工将获得的收益（手续费+奖励），同时按照是否支持幽灵协议，分配部分奖励给叔父节点。
3. 构造集合交易信息的 Merkle 树以及叔父节点区块头的 Merkle 树，然后根据 RNN 算法生成随机数 nNonce，写入其他参数。
4. 最终构造 MATRIX 数据区块头。

## 6.4 MATRIX 的数据区块内部结构

MATRIX 的数据区块单个区块链的结构提由三部分组成：

1. 数据区块头；
2. 交易列表；
3. 叔父区块头列表。


图 31 单个数据区块的构成

其中：

交易列表包括尽可能多的交易信息，类似：

transaction_list = [

transaction 1,

transaction 2,

...

]

uncle list = [

uncle_block_header_1,

uncle_block_header_2,

...

]

## 6.5 MATRIX 的共识机制

区块链的价值锚点在于链条自身的消耗与产出。当区块链选择 PoW 作为共识机制时，每一次区块的生成消耗的算力都将成为其价值的基石。另外，在 MATRIX 上，每个节点都具备解决现实环境问题的能力，并能对外提供各种 AI 服务。如果 MATRIX 上的节点能够参与实际问题的解算，整个区块链条就具备了现实的产出价值。因此，为保证区块链自身价值最大化，MATRIX 控制链与每一条数据链将默认选择基于 PoW 的共识机制。

但由于 PoW 具备交易速度较慢等显性缺陷，因此在 MATRIX 中，除初始的数据链与控制链强制采用 PoW 外，后续的数据链，其共识机制将被设计成模块化的，可以通过控制链参数进行配置，能够动态适用公链和私链的不同应用场景。

目前，MATRIX 对后续数据链共识机制，支持 PoW、POS、DPOS、BFT 等。MATRIX 链的 AI 优化系统将针对数据链本身的应用场景和交易情况，选择合适的共识机制，确保各个分布式节点通过算法取得数据的一致性。

## 6.6 MATRIX 的安全加密算法

MATRIX 链的安全加密算法，是基于采用传统的比特币加密方式上的改进。MATRIX 链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（比特币标准）和 SM2（中国国标）。MATRIX 控制链与初始数据链选择 secp256r1 作为密钥方案。

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。目前比特币采用 SHA-256 算法。MATRIX 除 PoW 外，其余 Hash 算法均指 SHA-256。

## 6.7 MATRIX 随机数的产生

MATRIX 链的随机数产生包含两种方式：

（1） 基于共识的随机数

（2） 二阶段产生的随机数

其中，基于共识的随机数将当前区块的 Nonce 作为种子之一，与未来某个区块的 Nonce 共同组成随机数种子（Random Seed），通过随机数发生器，获得真正的随机数。

二阶段随机数，则将随机数的产生分为两个阶段，核心是避免矿工由于自身利益，隐藏当前区块的 Nonce 作为随机数种子。因此，第一阶段先随机抽取一个在线第三方，第三方可以与当前区块的 Hash 有关联，并确定未来某个区块的 Nonce 作为随机种子之一。这个第三方也可以直接选择可信第三方。第三方生成一对公钥与私钥，并公布随机种子的区块公布公钥，并在后续的一个区块公布私钥。私钥与随机种子的区块 Nonce 共同组成了随机数发生器的种子，并由此产生基于全网共识的随机数。

## 6.8 MATRIX 的难度调整实现

MATRIX 的难度调整遵循："按照难度比例来分配币的奖励"的原则。这可以让加密货币的挖矿与真实世界的挖矿更加相似，并保证算力较低的矿工也能获得合理的收益。

低级矿工的生存法则：

（1） 挖矿，但越来越难

（2） 基础红利，收益恒定

（3） AI 服务，收益恒定

（4） 彩票收益，随机化

**MATRIX 的挖矿难度公式如下：**

difficulty = maximum_target / current_target

(target is a 256 bit number)

**难度在区块中的储存方式：**

每个块存储一个打包（pack）过的十六进制表示的 target. 这个 target 能够使用预定义的公式推断出来. 例如，在 block 中被打包的 target 为 0x1b0404cb，那么这个十六进制的 target 即是：

0x0404cb * 2**(8*(0x1b - 3)) =

0x00000000000404CB000000000000000000000000000000000000000000000000

请注意，这个 0x1b0404cb 是一个有符号数据. 最大的合法值为 0x7fffff，最小的正的合法值为 0x008000.

最高（位）的可能难度被定义为 0x1d00ffff，它的 16 进制表示为：

0x00ffff * 2**(8*(0x1b - 3)) =

0x00000000FFFF0000000000000000000000000000000000000000000000000000

**MATRIX 中算力和给定难度的相关性：**

MATRIX 会根据网络中当前算力、资源耗费及实际工作情况，实时调整挖矿的难度；假设每过 N 个区块后（N 值为人工智能算法根据当前参数需要计算生成确定），难度就会调整，依据是前面完成这 N 个区块的实际消耗平均时间。按照产生 N 个区块之前算法中，会对这 N 个区块产生的平均时间有个预算，预估值为 $T_0$。

如果前面的 N 个区块平均时间 T 超过预估值 $T_0$，难度会降低。反之，难度升高。难度的调整多少与之前的 N 个区块块花费时间的方差正相关。

在 MATRIX 的体系中，每一个数据链均由其难度设计思想，但多种链均会采用一个统一的难度调整策略。

但控制链需要专用的设计思想。

## 6.9 MATRIX 的 P2P 协议

MATRIX 上，每个节点（客户端）均采用 P2P 协议进行消息广播交互。对于 MATRIX 的数据区块，采用的 P2P 协议是标准的以太坊加密货币协议，该协议的核心特点是引入“幽灵“协议。而 MATRIX 的控制区块则，采用标准的 P2P 协议，不支持“幽灵“协议。

MATRIX 的客户端通常工作于守护状态。该状态下，客户端执行的工作包括：（1）调用网络守护进程维护连接及定期发送消息；（2）获取当前区块信息以及关联区块信息；（3）获取 AI 参数，并对 AI 参数按照标准模型分析，确定是否提交更新的参数。

当客户端收到一个消息时，它将执行以下布骤：

1. 对该消息进行 Hash 处理，并确认该数据与其 Hash 值是否已经接收过，如果是，退出，否则将数据发送给数据分析器。

2. 确认该消息的数据类型。目前包含 4 种情况：（1）交易信息；如果该信息为非法合约，则直接不将该信息加入本地交易列表；否则，进一步判断用户是否选择 AI 保护，如果不是，则直接将其加入本地交易列表，否则判断该合约是否通过 AI 审查，如果通过，则加入本地交易列表，否则拒绝加入列表；当交易消息列入列表后，将当前数据区块并发布至网络。（2）如果该数据项是一个消息，作出回应。（3）如果该消息为 AI 参数与 AI 模型，则将该消息加入到对应的 AI 列表，并写入即将发布的控制区块种，并在规定时刻发布至网络。（4）如果该消息是一个区块，转入步骤 3。

3. 检查区块中的“父区块“参数是否已存储于数据库中。如果没有，退出。

4. 当前区块为数据区块时，检查该区块头以及其“叔区块列表”中所有区块头中的工作量证明是否合法，如有任意一个非法，退出。当前区块为控制区块时，则跳过检查“叔区块列表”步骤，进入检查区块时间戳步骤。

5. 检查“叔区块列表” 中每一个区块的区块头，以确定其是否以该区块的“祖父区块”为父区块。如有任何否，退出。注意叔区块头并不必须在数据库中；他们只需有共同的父区块并有合法的工作量证明。

6. 检查区块中的时间戳是否最后至未来 15 分钟并且在其父区块的时间戳之后。检查该区块的难度与区块号码匹配。如任何检查失败，退出。

7. 由该区块的父区块的状态开始，加上该区块中的每一笔合法交易。最后，加上矿工奖励。如果结果状态树的根哈希与区块头中的状态根不匹配，退出。如匹配，将该区块加入数据库并前进至下一步。

8. 根据参数设定，确定是否需要更新区块难度。当新区块需要调整难度时，则启动难度调整，否则维持难度不变。

9. 如果新区块被改动，向其中加入交易列表中的所有交易，废除交易列表中的所有变为不合法的交易，将该区块及这些交易向全网重新广播。

“现区块”是由矿工存储的一个指针；它指向矿工认为表达了最新的正式的网络状态的区块。所有索要平衡账目，合约状态等的消息都通过查询现区块并计算后回应。如果一个节点在挖矿，过程有一点轻微的改动；在做上述所有步骤的同时，该节点同时在现区块挖矿，将其自己收集的交易列表作为现节点的交易列表。

# 7 MATRIX 系统模型

对于 MATRIX 而言，系统设备包含几类：

（1） 标准 MATRIX 节点；

（2） 云接入节点；

（3） 云存储节点；

（4） MATRIX 可信网关

（5） 外部数据源存储池

（6） AI 服务设备；

标准的 MATRIX 节点，可以认为是一个支持 MATRIX 控制链与至少一条数据链，支持相关链的数据存储，且能执行对应数据链智能合约的基础网络设备。该设备应当具备运行 AI 虚拟机的能力，并能执行 AI 控制链与对应数据链定义的 AI 模型功能。

云接入节点，则是 MATRIX 为方便各个移动端设备而开发的节点，该节点能够为各个接入的对象提供 MATRIX 节点的能力。任何一个移动端客户都可以安全加密方式，通过登录该云接入，并获得 MATRIX 节点的各种能力。


图 32 MATRIX 的手机客户端接入链上所有应用服务示例

云存储节点，则是 MATRIX 在云端实时备份的 MATRIX 区块数据，该数据是由 MATRIX 创世节点实时写入云端；该数据仅为方便用户进行离线查阅，不作为所有节点的共识基础，属于 MATRIX 的附属工具。用户可以通过获取整个数据校验与签名，离线验证数据链的有效性。由于云存储节点数据无需按照区块链顺序存储，因此可以按照传统数据库方式存储，例如 MySQL 等格式，从而方便用户离线查询验证。

MATRIX 可信网关，则是用于沟通外部数据源的主要设备。该设备将通过 AI 获得 MATRIX 所需要的外部数据源，并通过 AI 审核，确定置信度。MATRIX 节点在使用该数据时，将根据各个独立节点的一致性，确定最终数据的可信度，并给出各个节点的信用评价。另外，可信网关能够支持 MATRIX 的扩展，也能支持用户插件，实现线上线下的更深层次融合。

外部数据源存储池，该数据源存储内容为可信网关获取的外部数据，所有数据均通过 AI 审核。该存储池也将用于用户私密数据的存储，通过安全加密保证只有特定用户才可以访问。存储池中的任何文件，都可以在不直接读取内容情况下，通过内置引擎，验证文件签名，从而确定文件是否被篡改。由于该存储池的重要性，MATRIX 将部署多个分布式存储池，各个池之间按照数据区块链方式进行组织，只有各个分布式存储池数据内容达成一致，才能完成写入区块。

AI 服务设备，该设备包含两个功能：（1）能够服务于整个系统结构以及各个 AI 模型参数的优化；（2）发起 MATRIX 上的各种 AI 服务，既能够将 MATRIX 作为一个整

体，为外部用户服务，也能够调用 MATRIX 中的节点，为各类用户服务。AI 服务设备是 MATRIX 的附属设备，任何节点也可以自建该设备。

典型的部署方案如下：

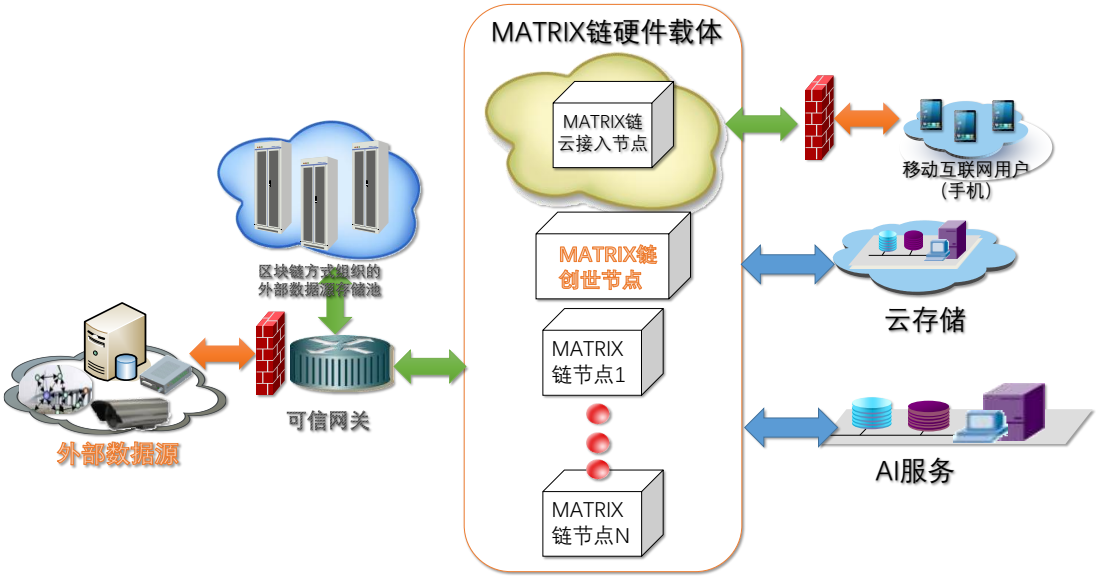


图 33 MATRIX 的系统结构与部署模型

## 8 MATRIX 的商业生态拓展

**链上持续发行资产和应用：**

James F.Moore 在 1996 年提出了“商业生态系统”的概念，目的是力求在商业实践中“共同进化”。

所谓的商业生态系统，就是由组织和个人所组成的经济联合体，其成员包括核心企业、消费者、市场中介、供应商、风险承担者等，在一定程度上还包括竞争者，这些成员之间构成了价值链，不同的链之间相互交织形成了价值网，物质、能量和信息等通过价值网在联合体成员间流动和循环；他们是共生关系，多个共生关系形成了商业生态系统的价值网。

商业生态系统也是一种网络，是“一个介于传统组织形式与市场运作模式之间的组织形态”，但它不是一般的企业网络，它强调以企业生态位的思想来看待自己和对待他人。无论是哪一种企业网络，它们共同的目标都是在一个不断进化和变化的环境中求得生存。要达到这个目标，一个企业网络必须能够快速准确地感知到环境的变化，明白其所处的状态，并制定出一套可行的方案。不仅如此，它还应当展现出其良好的学习行为。

MATRIX 项目在其基金会领导下，位于多条价值链的交叉位置，从而将存在于多个商业生态系统中：

1. 由于 MATRIX 自身拥有的 AI 特性和区块链技术，其中的 AI 算法迭代和进化应用前景的价值链和区块链 3.0 价值链将毫无疑问在 MATRIX 上重叠并生产几何级数的价值提升。

2. MATRIX 的 AI 化挖矿机云应用，是将 POW 算力需求通过 AI 智能合约在云上发布给相关的挖矿机系统进行 POW，提升了挖矿机挖币的成功率并生产出对应的虚拟币价值，这将打破现有各种区块链挖矿算力的隔阂，并由此产生各种虚拟币价值链在 MATRIX 上的交叉重叠。

3. MATRIX 项目可以接入其它区块链发布的任务，通过其自身的 AI 算力，产生相应的虚拟币而产生价值。

4. 在智能合约处理方面，基于 AI 算法机制生成的编码语言有别于传统智能合约（Smart Contract）的编码语言，能防止合约中的缺陷和陷井，降低交易风险和区块链使用门槛。这样 MATRIX 项目可快速部署于金融领域中，特别是证券、债券、信用评级等。如此，MATRIX 将位于金融价值链的覆盖范围内，并具有核心应用价值。

5. 区块链智能合约的最大优势之一就是不可中断的执行一段程序，可由 MATRIX 链上 AI 智能合约选举出来的账户执行收集信息并执行链下共识过程后，获取外部符合 AI 条件的信息和数据,而由此获得的数据是可信的、及时的第三方数据。 当 MATRIX 使用于此类包含对赌要求应用环境时，可大大提高对赌达成概率。在此类应用中，MATRIX 被包含于保险、彩票价值链中。

6. MATRIX 项目带有区块链特有的云化应用、分布式存储的、类去中心化的基因，当把 AI 算力结合云化分布后，主要分层节点将由 AI 自主控制，而各个 AI 可根据业务要求进行不同主业设计（算法一致），再根据 MATRIX 智能合约揉合各个 AI 结果以达成目标商业目的。在物联网和物流领域价值链中，MATRIX 可根据其物品所在的不同业务阶段设置 AI 自主控制、本地高效数据处理、类去中心化智能合约执行而体现其价值。

在未来，MATRIX 除了发展自身技术，保持足够的竞争力，维持行业标准地位之外，也会积极地拓展自身的商业生态：

**链上持续发行资产和应用：**

和以太坊一样，MATRIX 上线之后，除了不断加强 MATRIX 的技术领先性以外，我们也会不断在链上发布新的资产和应用，全面拓展 MATRIX 的生态结构和丰富 MATRIX 的生命力。

**行业标准：**

将 MATRIX 打造成智能合约区块链的标准，成为未来新技术发展和新应用发布的基础。

**技术的扩展性应用：**

在 MATRIX 保持技术领先性的情况下，MATRIX 的开源代码将会成为很多未来项目的底层技术，包括政府的项目。

**矿机销售：**

在未来,MATRIX 上矿机的销售将会成为 MATRIX 财务收入的重要组成部分。

## 9 MAN（MATRIX AI Network）公开售卖（ICO）

MATRIX 未来发行的代币简称为“MAN (MATRIX AI Network)”，预计总计生成 10 亿个 MAN，代币的发售细则将会在未来公布，请关注 MATRIX 的官网及白皮书更新情况。

## 10 MATRIX 产品研发计划


图 34 MATRIX 产品研发计划

我们会根据项目的实际情况不断更新产品的研发和推出进展，具体时间表也会根据我们的研发情况进行相应的调整。

## 11 MATRIX 的核心团队与顾问团队

一个真正意义上改变世界的充满创造力的产品，是需要一个极其出色以及配置合理的团队来打造的：需要顶级的科学家来创新、来探索，他们是这个团队的灵魂，决定了这个产品的上限；需要顶级的工程师来执行、来实现，他们将组成这个团队的躯干，决定了这个的品质；另外需要顶级的产品专家来负责用户体验，他们是这支团队的外表，决定了这个产品的体验 。MATRIX 就是这样的一支团队，一群中国的顶级科学家和工程师因为相同的理想和理念走到一起，用共通的“知行合一”的产品哲学思想，设计了这个标志区块链 3.0 时代的产品——MATRIX。核心团队 Leader 如下：

| 姓名 | 简介 |
| --- | --- |
| **邓仰东** | MATRIX 首席人工智能科学家，清华大学副教授，知名人工智能学者科学家，1995 和 1998 年在清华大学电子工程系取得学士和硕士学位，于 2006 在靠计算机及机器人专业享誉世界的卡内基－梅隆大学(Carnegie Mellon University)取得博士学位。2004 年起（博士毕业前）即已在美国 Incentia Design Automation 公司担任资深工程师，2006 年 1 月加入美国 Magma Design Automation 公司担任咨询级研究员，2008 年 3 月回国担任清华大学微电子学研究所副教授。现任清华大学软件学院副教授，主要研究方向为人工智能、电子设计自动化、并行算法和图形处理器架构。曾为中国高铁设计及研发了人工智能预警安全解决方案。著有《结构化集成电路设计和高层次综合》等多本知名高校教材，在各种一流期刊上发表论文超过 20 篇，曾带领团队在 Pascal 人工智能国际大赛上斩获第一名。邓老师将带领团队负责 MATRIX 项目中整体人工智能部分的算法设计、人工智能硬件部分的设计与研发以及下一代人工智能芯片的设计。 |
| **李庆华** | MATRIX 首席网络架构科学家，国内顶级芯片设计专家，作为主设计师，设计了国内第一款 WiFi 芯片；同时作为总工团队成员和基带项目总师，设计了中国首个大型水面舰艇的通信调度指挥系统。个人主导设计了多款量产商用芯片，并多次获得省部级科学技术奖励。作为多项芯片专利的发明者，著有《通信 IC 设计》一书，京东同类书籍销售排行榜第一名，作为北邮等一流高校研究生芯片设计课程的教材。李老师将带领团队负责 MATRIX 项目中区块链的架构及与人工智能结合的设计，通信架构设计以及软件与硬件结合的架构设计。 |
| **时昕** | MATRIX 首席矿机及芯片科学家，中国科学院博士，曾任 AMD 公司计算平台与方案部负责人，负责 GPU 显卡在下一代计算平台的应用开发及生态系统建设。时博士曾在多家国际领先的半导体及 IP 公司担任重要技术职务。时博士将带领团队负责 MATRIX 项目中矿机的设计和研发，以及下一代人工智能芯片的研发。 |
| **田国斌** | MATRIX 首席研发工程师，毕业于北京大学，曾就职于 MicroSoft，担任 Senior R&D Engineer，曾主持及参与开发多个大型软件系统及计算平台。田国斌将带领团队负责 MATRIX 项目中区块链部分及各个公用化开放接口的研发工作。 |

# 12 结语

互联网技术的兴起，给这个世界带来的巨大的变革，中国成为了这场革命的最大受益者，于是在互联网 2.0 时代，中国第一次在一个新兴技术及商业化领域走在了世界最前端，但究其根本，无论是互联网 1.0 万维网时代，还是 2.0 的移动互联网，所有的世界通用标准和协议，都与中国无缘。目前区块链技术将拉开互联网 3.0 革命的的序幕，在这场革命里，MATRIX 首当其冲将走在最前线，这个产品，对我们意义重大，不仅他将改写区块链技术的历史，成为区块链 3.0 时代的标志，更重要的是，我们相信，MATRIX 将让中国，第一次真正意义地在一个新兴的技术领域，拥有自己的标准和话语权。

与此同时，我们也真正希望 MATRIX 将成为“中国质造”转为“中国创造”的起点，在 MATRIX 中，渗透了中华民族伟大文化中的哲学思想，拥有了以华夏文化为核心理念的灵魂，拥有了中国文化为灵魂的产品，才真正意义上是“中国创造”。

GO MATRIX, GO CHINA!

# 13 附录：参考文献

1. E. T. Jaynes and G. Larry Bretthorst, "Probability Theory: The Logic of Science," 1st Edition, Cambridge University Press (June 9, 2003).
2. Christian P. Robert, "The Bayesian Choice: From Decision-Theoretic Foundations to Computational Implementation," Springer Verlag, New York; 2nd edition (June 1, 2007).
3. Brenden M. Lake, Tomer D. Ullman, Joshua B. Tenenbaum, and Samuel J. Gershman, “Building Machines That Learn and Think Like People,” Behavioral and Brain Sciences (2016): 1-101.
4. David C. Knill, and Alexandre Pouget, “The Bayesian brain: the role of uncertainty in neural coding and computation.” TRENDS in Neurosciences27, no. 12 (2004): 712-719.
5. Yufei Ni, Yangdong Deng, Fei Gao, Jjin Huang, and Leibo Liu, “Accelerator for Bayesian Cognition (ABC): A Stochastic Computing Platform for Cognition Computing,” https://arxiv.org/submit/1974875/.
6. Konrad P. Körding and Daniel M. Wolpert, “Bayesian integration in sensorimotor learning,” Nature, 244-247, 2004.
7. Brenden M. Lake, Ruslan Salakhutdinov, and Joshua B. Tenenbaum, “Human-level concept learning through probabilistic program induction,” Science 350, no. 6266 (2015): 1332-1338.
8. Joshua B. Tenenbaum, Charles Kemp, Thomas L. Griffiths, and Noah D. Goodman, “How to grow a mind: Statistics, structure, and abstraction,” Science 331, no. 6022 (2011): 1279-1285.
9. André M.M. Sousa, Kyle A. Meyer, Gabriel Santpere, Forrest O. Gulden, Nenad Sestan, “Evolution of the Human Nervous System Function, Structure, and Development,” Cell, Volume 170, Issue 2 July 13, 226–247, 2017.
10. Radu V. Craiu and Jeffrey S. Rosenthal, “Bayesian Computation Via Markov Chain Monte Carlo,” Vol. 1:179-201, 2014.
11. W. R. Gilks, S. Richardson and D.J. Spiegelhalter, “Markov Chain Monte Carlo in Practice,” Chapman and Hall, 1996.
12. Doron Avramov and Guofu Zhou, "Bayesian Portfolio Analysis," Annual Review of Financial Economics Vol. 2:25-47, 2010.

13. Simon Jackman, “Bayesian Analysis for Political Research,” Annual Review of Political Science, Vol. 7:483-505, 2004.

14. Sanjib Sharma, "Markov Chain Monte Carlo Methods for Bayesian Data Analysis in Astronomy," Annual Review Astronomy Astrophysics. 55:1–49, 2017.

15. Chris J Needham , James R Bradford, Andrew J Bulpitt, and David R Westhead, "A Primer on Learning in Bayesian Networks for Computational Biology," PLoS Computational Biology, Vol. 3, No. 8, 2007.

16. Jin Huang, Yangdong Deng, Qinwen Yang, Jiaguang Sun, An Energy- Efficient Train Control Framework for Smart Railway Transportation: IEEE Transactions on Computers 65, no. 5 (2016): 1407-1417.

17. Y. Deng and J. Huang, “GPU Machine Learning,” China Machine press and Elsevier Publishing Company, in press.
18. Y. Deng, M. Zhu and C. Liu, “Introduction to OpenCL Programming for Heterogeneous Processors,” China Machine press, 2016.
19. Y. Deng, Y. Ni, Z. Li, S. Mu S. and W. Zhang, Toward Real-Time Ray Tracing: A Survey on Hardware Acceleration and Microarchitecture Techniques, ACM Computing Surveys. Accepted.

20. Z. Li, L. Liu, Y. Deng, S. Yin, Y. Wang, and S. Wei, Aggressive Parallelization of Irregular Applications on Reconfigurable Architectures, 44th International Symposium on Computer Architecture (ISCA), Toronto, Canada, 2017.

21. Jin Huang, Qingmin Huang, Yangdong Deng, and Ye-Hwa Chen. "Toward Robust Vehicle Platooning With Bounded Spacing Error." IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 36, no. 4 (2017): 562-572.

22. Yangdong Deng, Shuai Mu, “A Survey on GPU Based Electronic Design Automation Computing,” Foundation and Trends in Electronics Design Automation, Now Publishers, pp. 1-180, 2013

23. K. Fang, Y. Ni, J. He, Z. Li, S. Mu, and Y. Deng, FastLane: An FPGA Accelerated GPU Microarchitecture Simulator, IEEE International Conference on Computer Design, 2013. (**Best paper award**).

24. Y. Zhu, B. Wang, and Y. Deng, “Massively Parallel Logic Simulation with GPUs,” ACM Transaction on Design Automation of Electronics Systems, Vol.16, No.3, June, 2011.

25. Y. Deng, B. Wang, and S. Mu, Taming Irregular EDA Applications on GPUs, IEEE/ACM International Conference on Computer-Aided Design, Nov. 2009.

26. Coulouris, Geroge; Jean Dollimore; Tim Kindberg;Gordon Blair,Distributed System:Concepts and Design(5th Edition)
27. Stefan Thomas & Evan Schwartz, A Protocol for Interledger Payments,Ripple.com,2015
28. Vitalik Buterin. Merkling in Ethereum.http://blog.ethereum.org/2015/11/15/
29. Ethereum WiKi, Patricia Tree.http://github.com/ethereum/wiki/
30. Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System.” 2008.http://bitcoin.org/bitcoin.pdf
31. “Genesis block” http://en.bitcoin.it/Genesis_block/.May,2015.
32. William Mougayar. “The Business Blockchain” April,2016
33. Roger WAttenhofer. “The science of the Blockchain” Oct,2016
34. James F.Moore ,A thousand business ecosystems，a worldwide connected community,and the future, May,2013
35. 博弈论与信息经济学，张维迎，6,1996
36. Microslav Kubat, An introduction to machine learning, Nov,2016
37. S. Russell and P. Norvig. Artificial Intelligence: A Modern Approach.Prentice Hall,2002
38. 区块链定义未来金融与经济新格局，张健，6，2017
39. Lamport L, Shostak R, Pease M. The Byzantine general problem.ACM Trans. on Programming Languages and Systems,1982,4(3):382-401
40. Fischer, M.J., Lynch, N.A., Paterson, M.:Impossibility of distributed consensus with one faulty process.J. ACM 32(2),374-382(1985)
41. Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery.ACM Trans. on computer System,2002,20(4)
42. 范捷，易乐天，舒继武。拜占庭系统技术研究综述。软件学报，2013,24(6)
43. Ongaro D, Ousterhout J. In Search of an Understandable Consensus Algorithm. In: Proc. Of USENIX Annual Technical Conference 2014
44. Garay, J.A., Kiayias, A., Leonardos, N.:The Bitcoin Backbone Protocol:Analysis and Application.IACR Cryptology ePrint Archive 2014