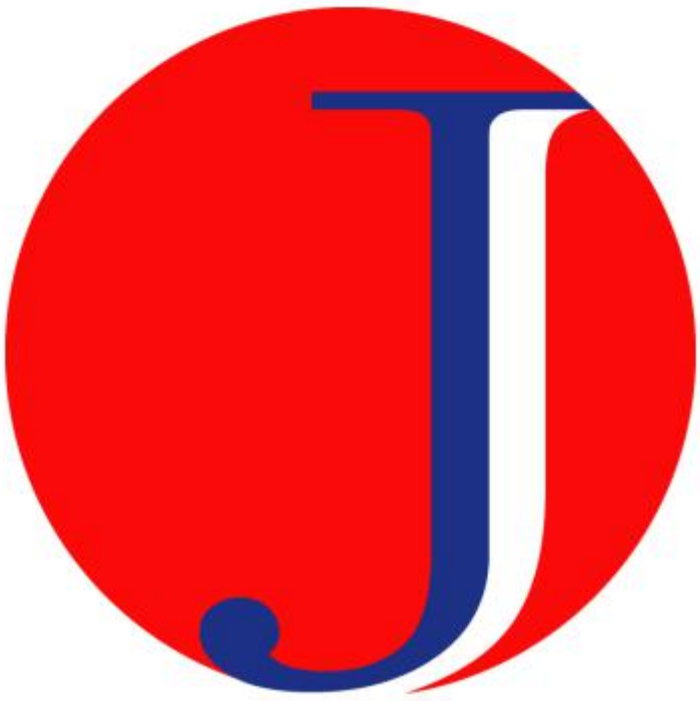
加乐币白皮书

JLA



目录

1.简介.....4

2.创新之举.....5

2.1 现有区块链面临的问题.....5

2.2 创新之举.....5

2.2.1 PoW+PoS 混合共识机制.....5

2.2.2 零知识证明（后期实现）.....7

2.2.3 wvm 虚拟机及改进的智能合约（后期实现）.....9

2.2.4 量子抗性密钥（后期实现）.....12

2.2.5 AI DAO（后期实现）.....14

3.技术概述.....20

3.1 JLA 矿机.....20

3.2 JLA 底层平台.....20

3.3 JLA 架构.....21

3.4 核心价值介绍.....22

3.5 关键技术优势.....22

4.JLA 生态圈.....24

5.JLA 发行规则.....25

5.1 发行计划.....25

5.2 资金用途.....25

5.2.1 研发.....25

5.2.2 市场推广.....25

5.2.3 法律.....25

5.2.4 备用金留存.....25
5.2.5 资金分配图.....26
6.预备交易所.....27
7.项目风险警示.....27
7.1 政策性风险.....28
7.2 市场风险.....28
7.3 技术风险.....28
7.4 资金风险.....29
8.免责声明.....29
9.结语.....30

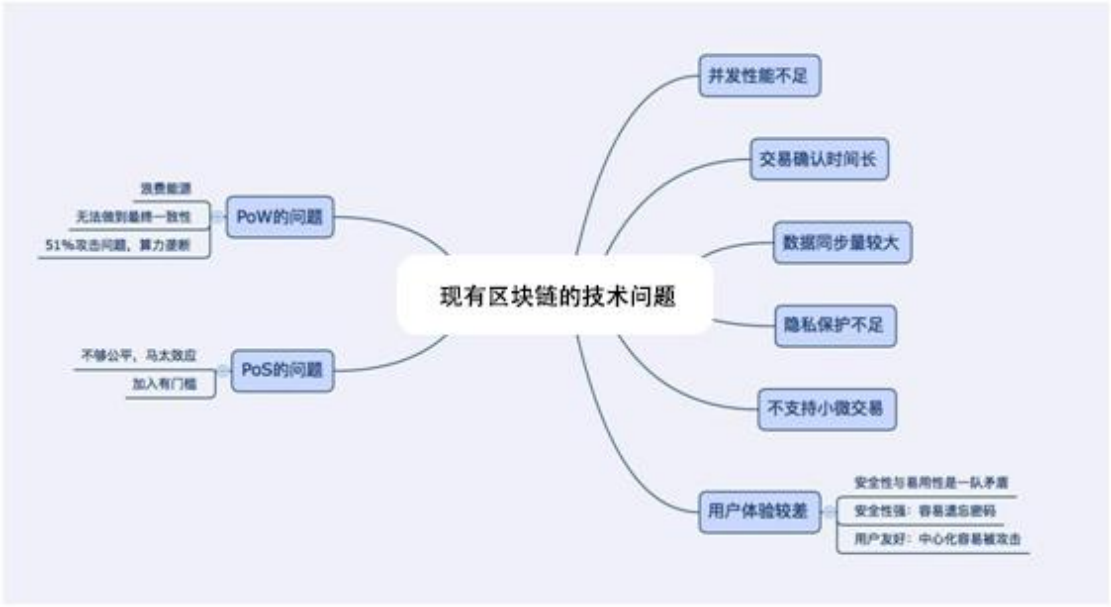
1.简介

2018 年是区块链爆发年，许多区块链技术推陈出新， 被称之为下一代的互联网技术，让信息互联向价值互联网迁移。与此同时，区块链具备的价值网络、去中心 化共识等的特性，能够结合许多行业发展出更为完善的经济体系、重构商业体系，甚至 激励出更大的技术创新。

特别是，区块链的分布特性，能够让整个链上的参与者共享 整个 生态的经济利益，而不会形成垄断。能够用于打破行业的孤岛效应，让整个行业在协作中竞争，互通基础数据 和设施，形 成为良性的技术和商业合作。技术为基、服务为盾、区块链为矛，对行业包含热情，全心全力为广大用户和合作伙伴打造全新一代的加密数字货币JLA 币及其公有链——JLA和落地应用。

2.创新之举

2.1 现有区块链面临的问题



目前的大部分问题都是由 PoW 共识机制算法带来的，而单独采用 PoS 公式算法，则会带来公平和马太效应问题。

2.2 创新之举

2.2.1 PoW+PoS 混合共识机制

JLA采用 POW 打包记账，POS 投票治理的共识机制。其具体特点如下：

区块是由 PoW 矿工挖矿产生的，矿工选择交易并放入区块里。股权系统相关的交易被插入到 UTXO 集合中。

i. POS 矿工通过从他们的选票生成一个投票交易在区块上进行投票。投票能够在前一个区块之上构建一个区块，并且不管前一个常规交易树（包含基于货币和非股权相关的交易）是否有效，都会选择一个。

i. 另外一个 PoW 矿工开始构建一个区块并插入 PoS 矿工的投票。已投选票的大多数都会被包含在后续的区块中，并被网络所接受。在这个新区块的投票交易中，PoW 矿工检查一个标志来确定 PoS 矿工是否指示了区块的常规交易树是有效的。这些投票标志会被记账，如果前一个区块的常规交易树是有效的，那么会在区块中基于大多数选票设置一个比特位标志来指明。

iv. 会发现一个满足网络难度的随机数，并且该区块被插入到区块链中。如果前一个区块的常规交易树被确认了，就将这些交易插入到 UTXO 集合中，并返回到第 i 步。

为了防止对于票数的操纵，如果矿工没有将所有的投票交易纳入区块中，那么会对当前的区块采用线性的补贴处罚。对以前那些交易树进行失效动作的“软” 处罚有助于防止丢弃工作，这对于确保系统安全是必要的，并且假设下一个区块将由一个无私的保留前面区块补贴的矿工获得，以便获得支持。即使不是这样的情况，具有高哈希率的恶意采矿者仍然至少需要（数量为多数 / 2）+ 1 个选票赞成他们之前区块的交易树，以便产生一个区块，使得他们可以从前面的区块获得任何补贴。

比特位标识会被显式地添加到区块头部和投票中以便矿工可以轻松地进行硬分叉或者软分叉。

JLA的PoS 机制将借鉴现有的PoS 机制，在保障系统安全性的前提下， 提高 PoS 的效率，着重提高用户在使用 PoS 机制时数字货币的安全性。

2.2.2 零知识证明（后期实现）

零知识证明 （被称为“zk-SNARK”）是实现区块链匿名特性的核心技术。

“零知识证明”的定义是：证明者能够在不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的。举个简单的例子：

A 要向 B 证明自己拥有某个房间的钥匙，假设该房间只能用钥匙打开锁， 而其他任何方法都打不开。这时有 2 个方法：

（一）A把钥匙出示给 B，B 用这把钥匙打开该房间的锁，从而证明 A 拥有该房间的正确的钥匙。

（二）B 确定该房间内有某一物体，A 用自己拥有的钥匙打开该房间的门， 然后把物体拿出来出示给 B，从而证明自己确实拥有该房间的钥匙 。

后面这个方法属于零知识证明。好处在于在整个证明的过程中,B 始终不能看到钥匙的样子，从而避免了钥匙的泄露。

我们采用一种安全性是基于计算离散对数的困难性的鉴别方案，可以做预计算来降低实时计算量，所需传送的数据量亦减少许多。为了产生密钥对，首先选定系统的参数：素数 p及素数 q，q是p－ 1 的素数因子。p≈21024，q＞2160， 元素 g为q阶元素，1 ≤ g ≤ p－ 1。令 a为 GF(p)的生成元，则得到 g= a(p

－ 1) / qmod q。由可信赖的第三方 T 向各用户分发系统参数(p, q, g)和验证函

数（即T 的公钥），用此验证 T 对消息的签字。

对每个用户给定惟一身份 I，用户 A 选定秘密密钥 s，0 ≤ s≤ q－ 1， 并计算 v=g－s mod p；A 将I和v可靠地送给 T，并从 T 获得证书，C= (I, v,

A A A

ST (IA, v))。

协议如下：

（1）选定随机数 r，1 ≤ r≤ q－ 1，计算 x= gr mod p，这是预处理　　步骤，可在 B 出现之前完成；

（2）A 将(CA, x)送给 B；

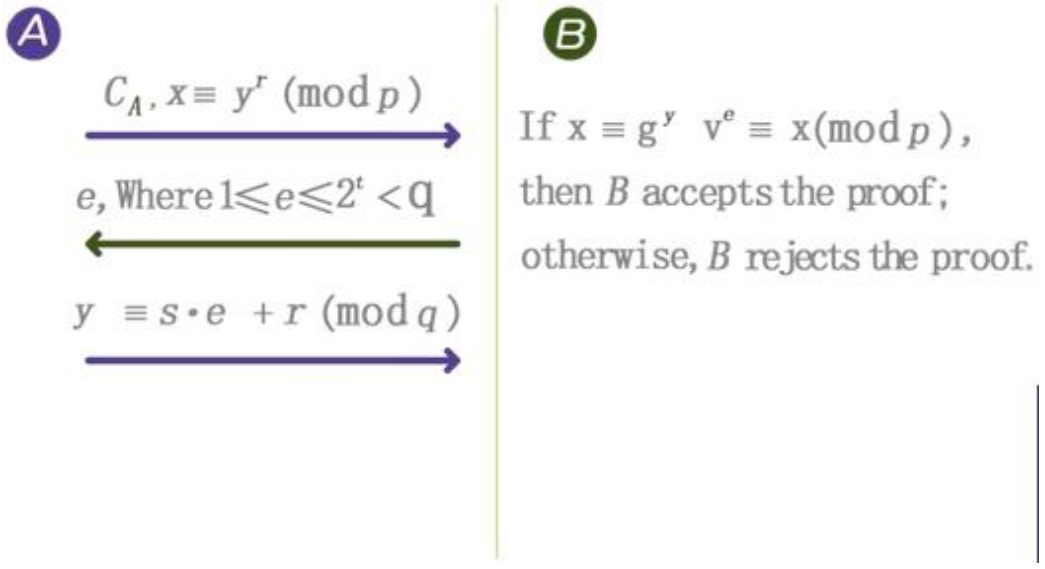
（3）B 以T 的公钥解 ST(IA, v)，实现对 A 的身份 IA和公钥 v认证，并传送　一个介于 0 到2 t － 1 之间的随机数 e给 A；

（4）A 验证 1 ≤ e≤ 2 t，计算 y= (se+ r) mod q，并将 y送给 B；

（5）B 验证 x= gy ve mod p，若该等式成立，则认可 A 的身份合法。

安全性基于参数 t，t要选得足够大以使正确猜对 e的概率 2－t足够小。建议 t为 72 位，p大约为 512 位，q为 140 位。

此协议是一种对 s的零知识证明，在认证过程中没有暴露有关 s的任何有用信息。



JLA将会借鉴 Zcash 的零知识证明技术，不单单在资产转移的过程中可以实现双向加密，还可以应用到很多其他对交易隐私要求极高的领域。

2.2.3 wvm 虚拟机及改进的智能合约（后期实现）

尼克•萨博关于智能合约的工作理论迟迟没有实现，一个重要原因是因为缺乏能够支持可编程合约的数字系统和技术。区块链技术的出现解决了该问题，不仅可以支持可编程合约，而且具有去中心化、不可篡改、过程透明可追踪等优点， 天然适合于智能合约。因此，也可以说，智能合约是区块链技术的特性之一。

如果说区块链 1.0 是以比特币为代表，解决了货币和支付手段的去中心化问

题，那么区块链 2.0 就是更宏观的对整个市场去中心化，利用区块链技术来转换许多不同的数字资产而不仅仅是比特币，通过转让来创建不同资产的价值。区块链技术的去中心化账本功能可以被用来创建、确认、转移各种不同类型的资产及合约。几乎所有类型的金融交易都可以被改造成在区块链上使用，包括股票、私募股权、众筹、债券和其他类型的金融衍生品如期货、期权等。

智能合约看上去就是一段计算机执行程序，满足可准确自动执行即可，那么为什么用传统的技术为何很难实现，而需要区块链技术等新技术呢？传统技术即使通过软件限制、性能优化等方法，也无法同时实现区块链的特性：1 是数据无法删除、修改，只能新增，保证了历史的可追溯，同时作恶的成本将很高，因为其作恶行为将被永远记录；2 是去中心化，避免了中心化因素的影响。

基于区块链技术的智能合约不仅可以发挥智能合约在成本效率方面的优势， 而且可以避免恶意行为对合约正常执行的干扰。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。

智能合约工作原理

基于区块链的智能合约包括事务处理和保存的机制，以及一个完备的状态机， 用于接受和处理各种智能合约；并且事务的保存和状态处理都在区块链上完成。事务主要包含需要发送的数据；而事件则是对这些数据的描述信息。事务及事件 信息传入智能合约后，合约资源集合中的资源状态会被更新，进而触发智能合约 进行状态机判断。如果自动状态机中某个或某几个动作的触发条件满足，则由状 态机根据预设信息选择合约动作自动执行。

智能合约系统根据事件描述信息中包含的触发条件，当触发条件满足时，从智能合约自动发出预设的数据资源，以及包括触发条件的事件；整个智能合约系统的核心就在于智能合约以事务和事件的方式经过智能合约模块的处理，出去还是一组事务和事件；智能合约只是一个事务处理模块和状态机构成的系统，它不产生智能合约，也不会修改智能合约；它的存在只是为了让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行。

基于区块链的智能合约构建及执行分为如下几步：

1、多方用户共同参与制定一份智能合约；

2、合约通过 P2P 网络扩散并存入区块链；

3、区块链构建的智能合约自动执行。

下面详细描述步骤 1“多方用户共同参与制定一份智能合约”的过程，包括如下步骤：

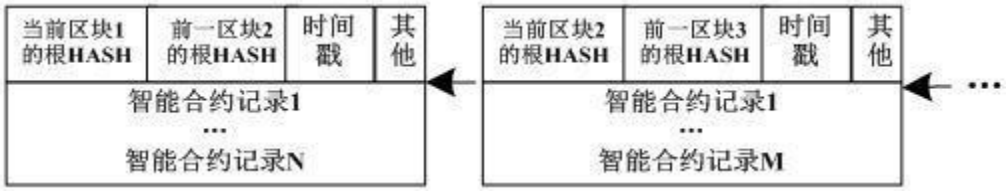
首先用户必须先注册成为区块链的用户，区块链返回给用户一对公钥和私钥；公钥做为用户在区块链上的账户地址，私钥做为操作该账户的唯一钥匙。

两个以上的用户根据需要，共同商定了一份承诺，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。

签名后的智能合约，将会根据其中的承诺内容，传入区块链网络中。下面详细描述步骤 2“合约通过 P2P 网络扩散并存入区块链”的过程，包括

如下步骤：

合约通过 P2P 的方式在区块链全网中扩散，每个节点都会收到一份； 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。共识时间到了，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），并算出这个合约集合的 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。（3） 最新达成的合约集合会以区块的形式扩散到全网，如下图所示，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，验证通过的合约才回最终写入区块链中，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。



下面是步骤 3“区块链构建的智能合约自动执行”的过程，包括如下步骤：

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。

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。

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。

JLA最终版本会提供类似于以太坊的图灵完备的脚本语言，用类似于

emv 的 wvm 虚拟机来运行智能合约程序。

2.2.4 量子抗性密钥（后期实现）

在当前以比特币为代表的区块链系统中，SHA-256 哈希计算和 ECDSA 椭圆曲线密码构成了比特币系统最基础的安全保障，但随着量子计算机技术不断取得突破， 特别是以肖氏算法为典型代表的量子算法的提出，相关运算操作在理论上可以实现从指数级别向多项式级别的转变，这些对于经典计算机来说足够“困难” 的问题必将在可预期的将来被实用型量子计算机破解。

后量子密码（post-quantumcryptography），又被称为抗量子计算密码

（quantum-resistantcryptography），是被认为能够抵抗量子计算机攻击的密码体制。此类加密技术的开发采取传统方式，即基于特定数学领域的困难问题， 通过研究开发算法使其在网络通信中得到应用，从而实现保护数据安全的目的。后量子密码的应用不依赖于任何量子理论现象，但其计算安全性据信可以抵御当前已知任何形式的量子攻击。1997 年，IBM

的研究人员提出一种加密方案名为Learning With Errors（LWE），意即伴随误差学习，由于要找到最近的通用格要很长时间，因而可以抵抗来自量子计算机的攻击。

基 于 Ring—LWE 的 公 钥 加 密方案： 相关参数选择及运算规则

方案中主要参数有 n，p，q。

n: 确定加密方案中多项式的最大次数。在保证计算效率和安全性的标准下， n 值越大越好，应该是 2k。

q: 大模数， 通常是一个正整数，q 值的大小与具体实例相关。q 值应该足够大， 这样才可以保证足够高的安全性，但是 q 值越大占用的系统资源就会越多，并会增加整数计算量。

p: 小模数，通常是一个小的正整数。令 R = Z

q［x］ /(xn + 1) ，对于环中的两个多项式 f 和 g，表示为如下形式 f(x)

= f0 + f1(x) +… + fn—1xn—1，g(x) = g0 + g1(x) + … + fn—1xn—1， k ∈ R，

$$f(x) \cdot g(x) = \sum_{k=0}^{n-1} \left(\sum_{i+j=k(modn)} f_i g_j \right) x^k$$

定 义 如 下 运 算: k • f(x) = kf0 + kf1x+ …kfn—1xn—1

密钥生成

在该方案中加密公钥是 h(x) ， 解密私钥是 f(x) 和 fp(x) ，选取方法如下

选定多项式 f(x) ，g(x) ，满足f(x) •g(x) =0modq。

f(x) •fq(x) = 1modq。

h(x) = fq(x) + 1。

公 钥 为 (h(x) ，g(x)) ， 私 钥 为 (f(x) ，fp(x)) 。加密过程

该方案中加密时引入随机差错多项式 e(x)∈ Ψα，Ψα 是参数为 α 的某一高斯分布，将明文转换为多项式 m(x) ，计算密文为: c(x) = h(x)•m(x)
+ g(x) •e(x) 。解密过程
接收到的密文是 c(x) ， 使用私钥 f(x) 和 fp(x) 对密文进行解密的步骤如下:
α(x) = f(x) •c(x)= f(x) •h(x) •m(x) + f(x) •g(x)•e(x)=
[f(x) •fq(x) + f(x)]•m(x) +f(x) •g(x) •e(x) modq (1)= f(x) •m(x)
fp(x) •a(x) = fp(x) •f(x) •m(x) modp= m(x) (2)

其中在第(1) 步和第(2) 步的解密过程中有可能出现解密失败，即当第(1) 步的系数不在区间 (－ q2 ，q 2] 内或者第(2) 步的系数在不在区间 (－ p2 ，p 2] 之间时便会出现解密失败现象，但是只要选取合适的参数，解密失败的可能性还是非常小的， 还可以采用像 NTRU 类似的避免解密失败的方法以减少解密失败的概率。
JLA将会开发可与 OpenSSL 一同工作的 Ring-LWE 密钥交换协议， 实现后量子时代区块链的安全需求。

2.2.5 AI DAO（后期实现）

我们认为“去中心化”技术的发展将经历五次浪潮：
1、比特币

2、区块链

3、智能合约

4、DAO——去中心化自治组织 Decentralized Autonomous Organizations 5、AI DAO

目前行业内是发展到了第四步也就是 DAO 阶段。Vitalik 将DAC 概念进行扩展，提出了更为普遍的 DAO 概念，以太坊集成图灵完备的语言和运行智能合约的能力，让 DAO 成为可能，正如 Stan Larimer 所说“在一组商业规则的控制下， 不需要人类的参与”。然而这种理想状态下的自治组织，如果在系统设计阶段不进行严格的把控，也会造成非常严重的后果。去年 The DAO 失败的根源在于其多数抢劫少数攻击解决方案——DAO 分离的Solidity 代码createTokenProxy 方法执行时 gas 消费并没有发生，这是系统漏洞，没有得到重视及时修复。

JLA将会吸取 The DAO 的失败教训，新推出 wvm 虚拟机，在其中可以运行现有的主流成熟开发语言比如 JavaScript、Java、Golang 等。对于智能合约，我们推崇简单就是美的原则，倡导微服务的架构理念。同时，在崭新的wvm 虚拟机基础之上，我们将会推出激动人心的 AI DAO（人工智能 DAO）。

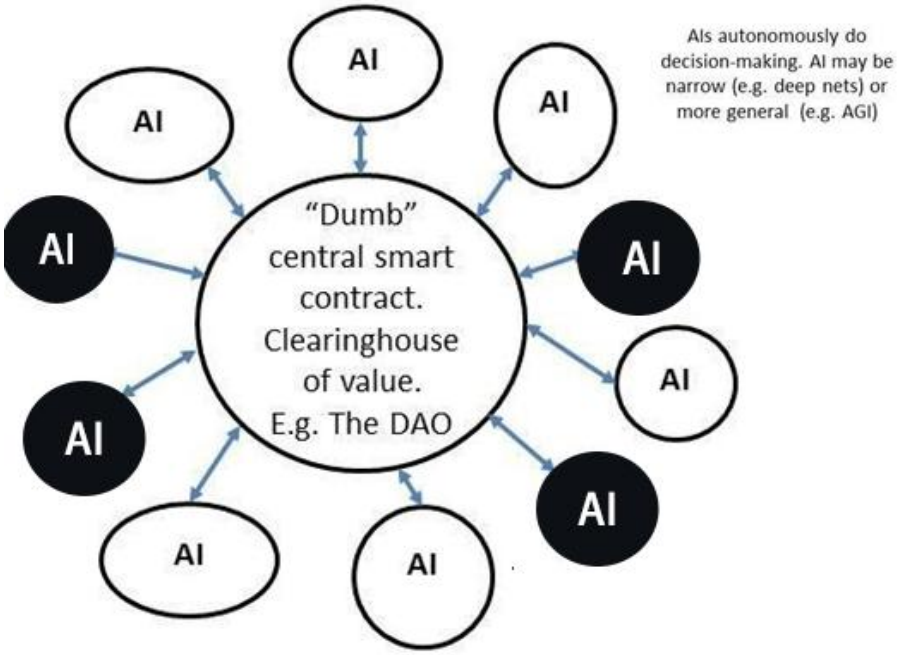
我们定义的 AI DAO 具备如下特性： 1、访问资源的能力

2、征用更多资源的能力

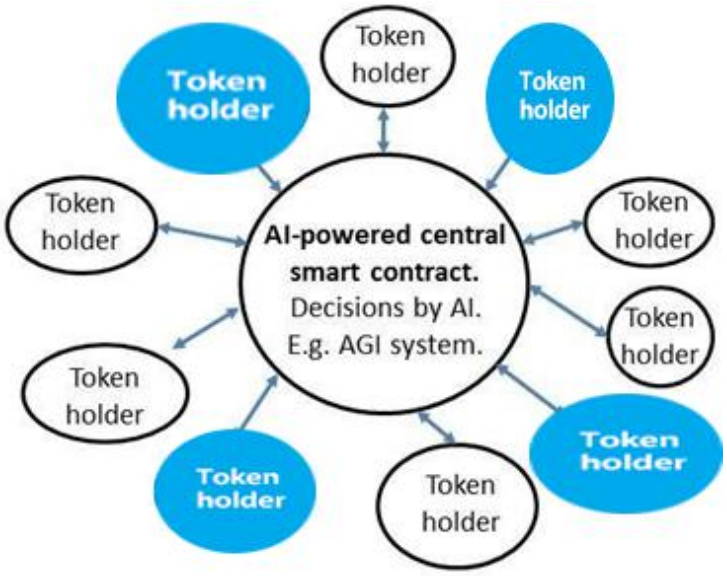
3、拒绝人为干涉的能力

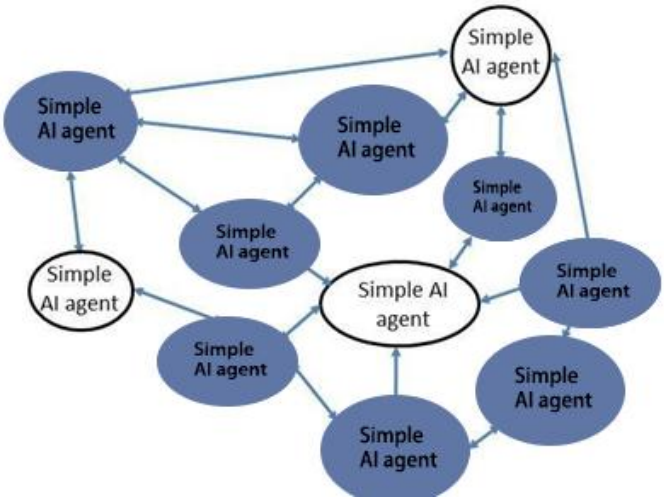
而这会通过三种途径来实现：

1、将智能合约的边缘执行单元交给 AI（自动化投票）



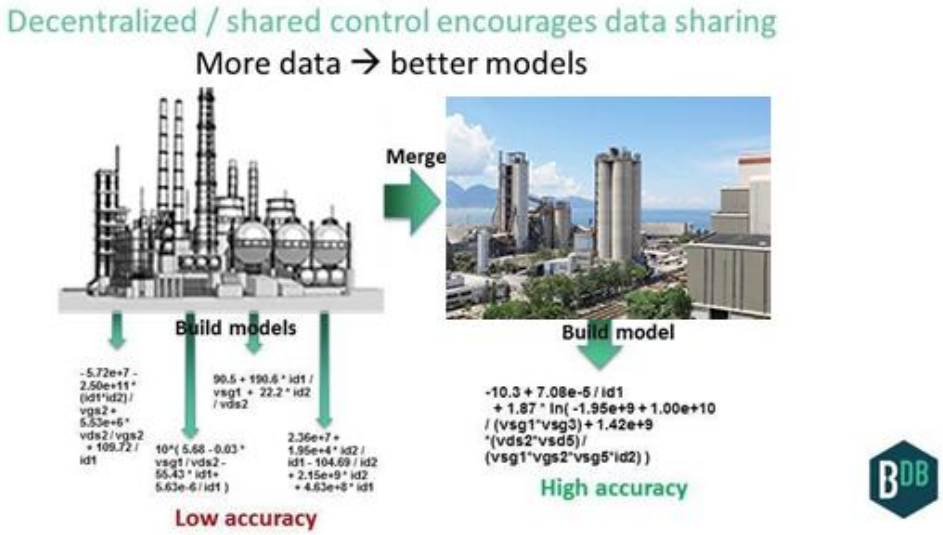
2、将智能合约的中心交给 AI（自动化反馈控制系统）





3、从集群中自动涌现出 AI 的复杂性

AI DAO 还有可能自我升级，而且自我升级的能力可以越来越强。AI DAO 可以跟自己的代码杂交生成下一代。而这些生成的下一代，可能不仅仅是某项能力产生了变化，还可能会改变该 AI DAO 的核心目标。“下一代”可能不再把此能力做为自己的“DAO 生涯”目标，而是其他的什么目标，比如检查软件中的安全漏洞。AI 本身就是一个强大而很酷的技术。DAO 也是一个强大而很酷的技术。AI 没有的资源，DAO 有；DAO 没有的自主决策能力，AI 有。所以 AI DAO 是更强大更酷的技术。DAO 的发展程度，已经足以提供让 AI 自行获取资源的能力。



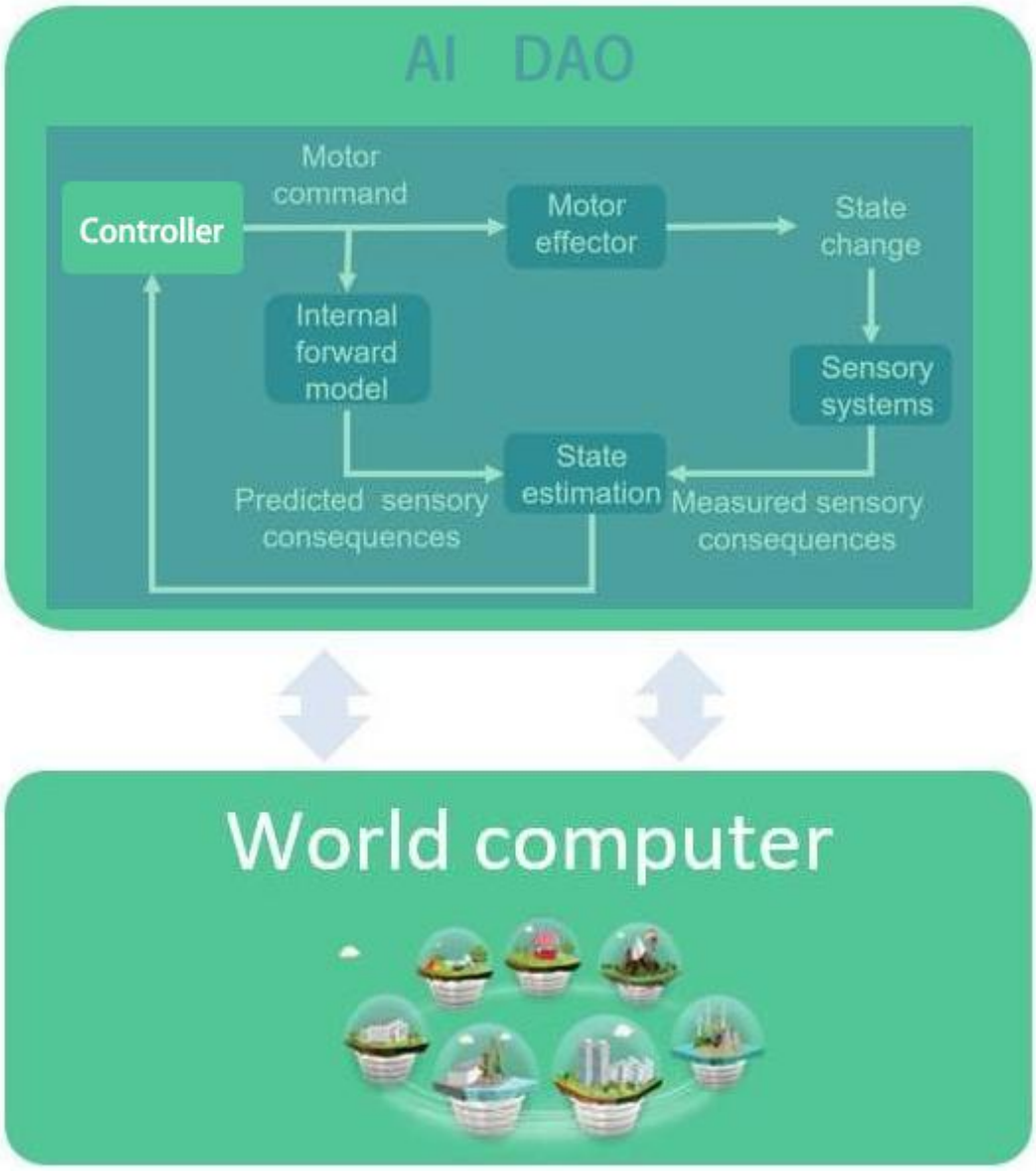
1、去中心化的数据控制方式将促进数据的共享，不仅意味着更多的训练数据（对 AI 而言意味着更好的模型），同时也意味着 AI 模型的共享。

2、更高效的数据验证，减少了训练数据中的坏数据，提升模型的可信度。

3、训练数据与模型成为可以交易的 IP 资产。

通用人工智能——AGI，是可以自发行动的代理决策者（agent），是一种反馈控制系统。控制系统是个顶呱呱的好东西。控制系统的数学基础深厚，可以追述到 1950 年代 Wiener 的“Cybernetics”。控制系统与这个世界交互（通过传感器与执行机），并适应这个世界（通过内部模型与外部传感器来更新自己的状 态）。控制系统应用广泛——恒温空调、降噪耳机、汽车刹车、下围棋的 AlphaGo， 这个世界到处都是它的身影。

AI DAO 是一个运行在去中心化软件上的 AGI 控制系统。它不断的获取输入， 更新状态，调整输出，并获取资源以持续维持这个反馈循环。



AI DAO 有很多可能性，其中包括增强 AI 自身的能力。比如，AI DAO 可以发起“请求为我的数据做标记”的有偿请求（智能合约），用低成本雇人来完善自己的数据集（去中心化的 Mechanical Turk）；AI DAO 还可以发起“将你的数据给我”的有偿请求，让 IoT 设备用自己的数据来交换电费。

依托于我们自研的 wvm 虚拟机，JLA的 AI DAO 是业界的第一个智能化DAO，我们的 AI DAO 将会给大家提供很多很酷的功能和新玩法。

实现方案

3.技术概述

具体分为 JLA 币矿机、JLA底层平台、应用平台：

3.1 JLA矿机

将会提供自研的矿机进行新 JLA 币的挖矿，构建完整的 JLA生态。

3.2 JLA底层平台

底层平台架构如下，其中我们会在区块链 Gateway 提供对于区块链底层平台事件的监听/通知接口，这是其他共有链不具备的功能。

共识机制我们采用PoW 和PoS 混合的方式，先以传统的PoW 方式进行挖矿， 此时挖出的区块不包含任何的交易信息，但会包含给该矿工的发放奖励的地址。这时系统切换到 PoS，由一组手中持有 JLA 币的 validator 对于新挖出来的区块及及交易进行签名，手中持有 JLA 币越多的 validator 被选中的概率就越 大。被选中的 validator 完成对该区块的签名后，该区块就包含响应的交易信息， 并成为一个完整的区块。Validator 和矿工都会获得相应的手续费奖励。加密算法采用椭圆曲线加密签名，哈希函数采用 Blake256。

3.3 JLA架构

核心架构图如下所示，所有与区块链底层平台的交互均通过区块链 Gateway 进行。

3.4 核心价值介绍

JLA解决了现有区块链面临的痛点问题和需求：

Pow + PoS 混合共识机制兼顾效率与公平

零知识证明的引入解决了用户隐私及匿名问题

闪电网络解决了现有公有链不支持高并发的痼疾

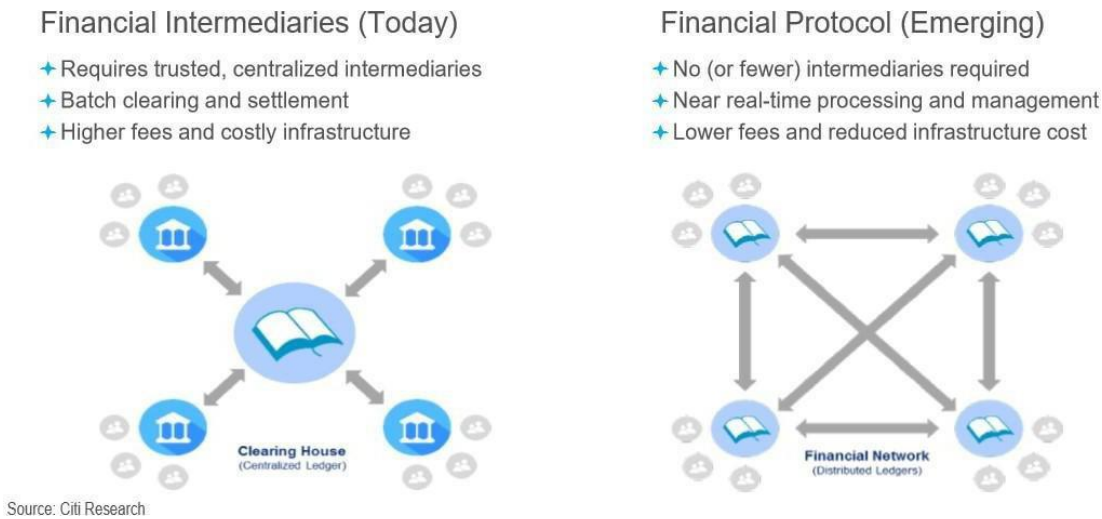
运行于JLA自身虚拟机wvm 上的智能合约赋予了节点可编程能力， 基于 wvm 构建 AI DAO，将 DAO 技术与 AI 技术有机整合。

量子抗性密钥赋予了在后量子时代区块链密钥的安全性。

3.5 关键技术优势

JLA具备区块链技术的四个特点：

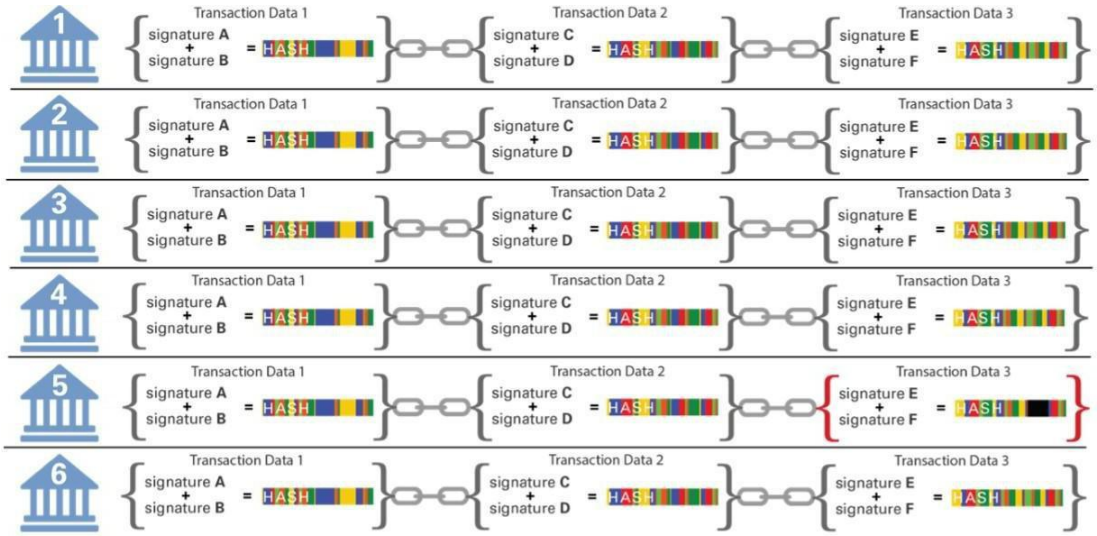
去中心化（Decentralized）：下图的左侧描述了当今金融系统的中心化特征，右侧描述的是正在形成的去中心化金融系统，其没有中介机构，所有节点的权利和义务都相等，任一节点停止工作都会不影响系统整体的运作。



去信任（Trustless）：系统中所有节点之间无需信任也可以进行交易，因为数据库和整个系统的运作是公开透明的，在系统的规则和时间范围内，节点之间无法欺骗彼此；

集体维护（Collectively Maintain）：系统是由其中所有具有维护功能的节点共同维护的，系统中所有人共同参与维护工作；可靠数据库（Reliable Database）：系统中每一个节点都拥有最新的完整数据库拷贝，修改单个节点的数据库是无效的，因为系统会自动比较，认为最多次出现的相同数据记录为真。

除此之外，我们还将人工智能（AI）与区块链技术通过 DAO 有机结合在了一起



Source: Goldman Sachs Global Investment Research.

4. JLA生态圈

JLA作为区块链生态圈的核心服务平台，支持生态圈应用，包括底层的公有链、矿机、矿池、数字货币、交易所、ICO 平台以及上层的去中心化应用， 如下所示：

5.JLA发行规则

5.1发行计划

恒定发行总量：2000万

流通量：1500万

创始团队持币：500万

发行时间：2019年5月份

首发交易所：Hubi（虎币）

5.2资金用途

5.2.1 研发

计划开发人员占 80%， 其他人员占 20%。

计划团队扩充至 20-100 人， 具体人数根据业务发展进度以及融资规模来定。

5.2.2 市场推广

搭建开发者社区、用户社区，进行市场教育，保障市场关注度。

5.2.3 法律

为 JLA生态圈建设过程中提供法律合规辅导服务。

5.2.4 备用金留存

留存一定的备用金，为 JLA生态圈服务。

5.2.5 资金分配图

2019年5月发行并且上线国际交易所，后续将会上线更多国际知名交易所，则计划用途如下分配：

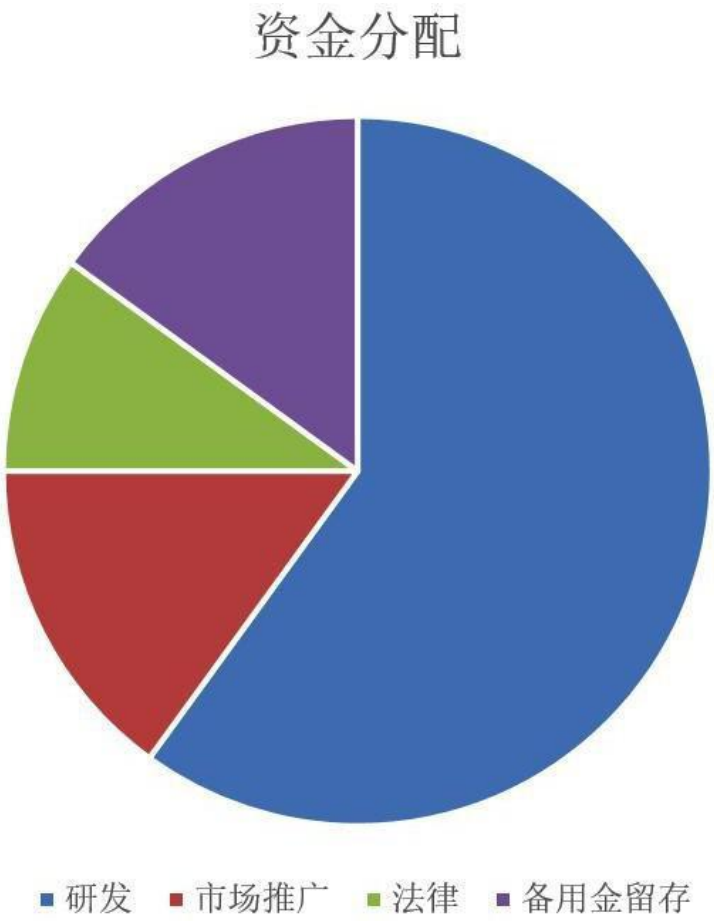


图 5-1　资金用途

6. 预备交易所

7. 项目风险警示

7.1政策性风险

目前虽然多数政府对区块链相关产业态度明朗并持积极鼓励政策，但公有区块链天生的去中心化属性在与现有的中心化政府的法律法规下依然面临政府政策层面的很多不缺定性。

针对政策性风险团队将会采取如下措施：

在团队单独设立公共关系部门，积极与政府以及业内从业人员保持沟通协作，在法律框架下设计数字资产发行 / 交易 / 区块链金融 / 区块链应用等方面业务。

JLA项目运营不涉及法定货币交易，但并不干涉第三方交易所开展

JLA兑法币交易业务，团队只专注技术。

7.2市场风险

JLA的终极目标是要实现一个基于 PoW/PoS 混合共识机制的共有链， 然而区块链产业刚刚兴起，项目的未来会面临各种各样的市场考验。

针对市场风险运营团队采取的应对方式为：

运营团队将定期的参与业内会议，并定期或不定期举行项目进展与发布会， 与相关开发者沟通与交流目前的市场需求与前景预测，确保项目能够回应社区与市场的声音。

7.3技术风险

JLA要建立跨平台的新技术标准，这其中的技术开发难度是非常巨大的，这对于顶尖技术人

才的需求以及科研的投入力度要求都是非常高的，如果把控不好，会影响项目进度甚至最终导致项目的失败。

针对技术风险运营团队采取的应对方式为：

紧紧依托国内外顶尖著名高校与区块链社区，与顶尖高校共建区块链技术创新实验室。基金会定期拨款，支持 JLA社区建设并与其他区块链社区开展深度合作，确保项目的技术风险可控。

与国内外 AI 团队合作推进 JLA人工智能化的研发。

7.4资金风险

资金风险是指项目资金出现重大损失，例如：资金被盗，在预定时间内因为人员与资金问题无法完成开发进度等等问题。

针对资金风险运营团队采取的避险方式为：

所有大额数字货币存储采取多重签名钱包+冷存储方式由基金会理事共同掌管。在 3/5 多重签名方式下，可以有效降低资金被盗以及被私自挪用风险。

8.免责声明

本文档只用于传达信息之用途，并不构成买卖新 JLA 的相关意见。以上信息或分析不构成

投资决策。本文档不构成任何投资建议，投资意向或教唆投资。

本文档不组成也不理解为提供任何买卖行为或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。

相关意向用户明确了解JLA的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。

团队不承担任何参与 JLA项目造成的直接或间接的资产损失。

9.结语

JLA专注于构建一个基于PoW/PoS 混合共识机制的数字货币JLA 币， 以及完整的区块链生态系统及去中心化应用商店，为广大投资者、开源社区以及产业链上下游合作伙伴提供完整的数字货币平台、区块链基础平台及应用落地服务。

电报群：https://0.plus/jla_com