基于 DAG 的价值交换网络

Value Interconnection & Exchange Network Based on DAG

技术白皮书

目 录

说明

本文档是 DAGX NETWORKS 技术白皮书 V1.1 版本,主要介绍DAGX 价值交换网络的理念、定位、技术特色 、项目蓝图和团队介绍等内容。随着项目推进，我们会持续升级本文档,使其与技术实现保持一致。欲了解 DAGX NETWORKS 的最新信息、技术白皮书、开发进度、社区建设等信息,请访问官方网站: https://www.dagx.io

联系我们

基金会: foundation@dagx.io ，技术支持: support@dagx.io

版权声明

免责声明

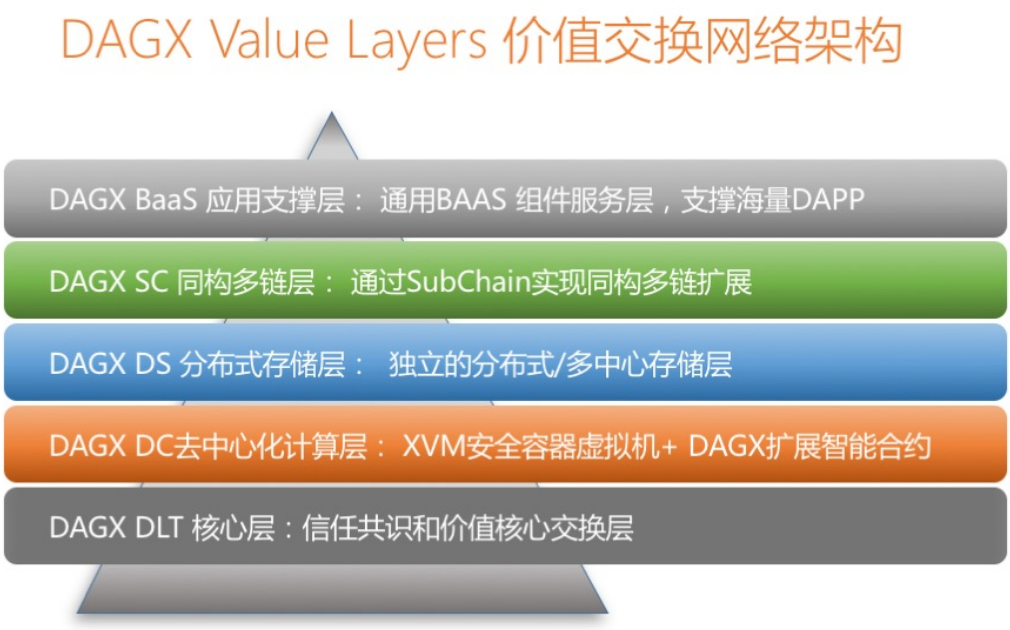
技术在不断发展， 区块链也在不断进步，DAGX NETWORKS 开发团队将会持续改进、完善现有技术方案，持续升级更新技术白皮书，恕不另行通知。

技术概要

DAGX Networks 是新一代基于有向无环图分布式账本技术（DAG）的商用价值交换网络， X 代表“价值互联与交换” ，DAGX Networks 致力推动实体经济与价值互联网连接融合，赋能行业与企业资产价值上链、流通与交换，实现数字经济价值重构和价值创造。

DAGX 团队认为：下一代价值互联网将会是多维多链的网络生态，就像繁荣的生物世界； 目前行业主流专家依然从传统历史进行推断，认为未来 DLT 生态发展类似操作系统，只有 3-4 种主流区块链得以延续发展。DAGX 团队对未来有更宏远不同的判断： 区块链正在带来生产关系的彻底变革，实现价值互联和流通交换体系的重构，通过全球多个价值交换网络、分布式多维逻辑功能链层进行资产价值互联、流通交换， 从而构筑崭新繁荣的多维多链新世界。

DAGX 团队创造性提出了 DAGX Value Layers 分层架构体系，由不同功能层次化的逻辑功能链组成 DAGX Network 价值交换网络，积极推动多维多链的下一代价值互联网应用落地。



在基础链技术方面，DAGX 团队针对 DAG(有向无环图)技术的系统容量、水平扩展能力、共识算法、交易速度、安全优化等方面进行了大幅创新，研发并部署了新一代 DAG 分布式账本系统，我们称之为 DAGX。 DAGX 落地行业应用不是单打独斗，而是和其他关键技术，如 ABCD（人工智能、区块链、云计算、大数据、生物识别）等技术融合在一起，形成 DAGX 价值交换网络的核心能力。DAGX 从设计理念和编码实现上都是一次技术的跃迁，推动实现“区块链”商用化落地、迈入价值互联网社会的新阶段。

DAGX 公链 1.0 已开发完成、上线测试运行，并在医疗健康、保险科技等多行业展开落地合作 ，DAGX 重点赋能“医疗健康、保险互助”行业，打造健康与保险行业数字资产公链生态，并助力企业运用 DAGX 开放平台与技术实现资产上链和价值互联、交换。

DAG Token： DAG Token 是 DAGX 的唯一官方 Token，DAGX 的首个 BAAS 应用 DAPP 组件 Bsure.cloud 已经运作，分期上线数据资产上链、安全智能合约模板、KYC、保险智能机器人市场、去中心化投票、去中心化聊天...等功能； 用户通过 DAG Token 实现产品与服务的购买与使用。

DAGX NETWORKS

在技术架构上，DAGX 打造了基于第三代区块链 DAG 的 DLT 分布式账本（Blockless based）系统及其相关的周边系统。DAGX 向用户提供了一种去中心化、去许可化、去信任化、具有公平访问权限和可加密协议的分层基础设施网络架构。这个分层基础设施网络架构可通过网络节点的共识保持 “不可更改”的交易记录。

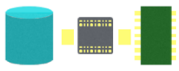
DAGX 的八大特点：

高并发

全球首条应用高性能内存图数据库的 DAG 公链，打造高并发能力

可扩展

首条基于分层可扩展体系 Value Layers 架构 DAG 公链，解决可扩展性问题



双合约

全球首条双合约 DAG 公链， SuperJ 超安全合约 + eContract 全智能合约

快支付

Instant Payment 实时闪付，秒级支付、快速确认，满足商业应用落地需求

可挖矿

支持可持续价值挖矿的 DAG 公链，助力解决 WCG 世界计算网格问题

BAAS

全球首条支持区块链 BAAS 应用服务公链，提供企业上链应用就绪能力

高安全

SuperJ 安全智能合约，内置格加密算法 NTRU 抗量子公钥接口，银行级的最终确认性，无 51%算力攻击问题

应用广

内置 P2P 聊天+智能对话机器人，构建 DappStore 应用商店

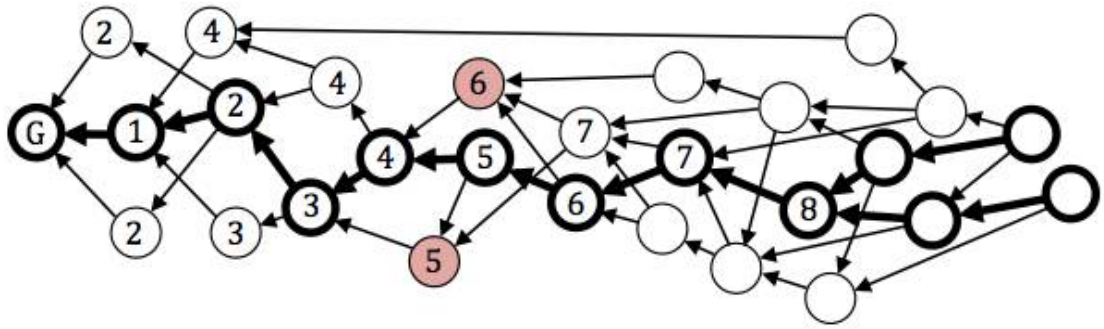
背景

当前的主流区块链实现比特币、以太坊技术均基于块状链实现： 他们在底层结构采用的是区块+链的数据结构。这种结构有一些先天性的局限。比如，这种结构会有一个类中心化的动作——“打包区块”，整个区块链在任意时刻，都是由记账者单点写入，记账者通过全网 POW 共识机制，算出 nonce 随机数并获得区块写入权力，并得挖矿奖励。这种单点写入区块链的主要问题是**无法处理高并发请求。**区块链的吞吐量受制于区块的大小：如果区块太小，而交易量很大的话，很多交易无法打包进区块；如果区块太大，整个区块链系统的数据量将迅速膨胀，普通用户将无法运行全节点，这将会造成中心化的问题。目前比特币扩容之争的其根本矛盾点就在于此，这也是区块+链式结构先天性的悖论问题。

DAGX 采用的是 DAG (有向无环图)结构。交易无需矿工打包，可以自行创建发布，不存在交易延时的问题，也不存在矿工机器的性能限制，因此DAGX 不存在吞吐量的问题。在DAGX网络里，每个用户可以只维护自己单元的所有父辈单元和储存、交易关联方所在父辈单元的数据，无需存储全网所有数据。即使全网所有数据量非常庞大，对单个普通用户也没有影响。 DAG技术是区块链的跃迁，简单类比可以说是并发多线程的区块链。把区块链从一维单点写入跃迁到了三维全网并行工作空间，从独木桥变成了高速公路网，从而解决了区块链无法处理高并发吞吐量的问题。

DAGX 将致力于打造一个通用的智能合约编程平台与区块链操作系统，同时具备原生的“安全智能合约”以及基于V8引擎的的虚拟机的“图灵完备智能合约”。与以太坊不同的是， DAGX不仅有效地解决了传统区块链系统面临的低吞吐量、交易确认延时、区块膨胀等先天性的悖论问题，还通过“安全智能合约”解决了以太坊长期受人诟病的“智能合约”安全问题。

革新



DAG 示意图

DAG 架构最早理论阐述是 DagCoin，后由 IOTA 团队率先实现基于“Tangle 机制” 的服务于物联网（IoT）生态系统的去中心化加密货币，之后 Byteball 借鉴 DAGCoin 的 DAG 理论设计，并加以改进创建了 Byteball 去中心化加密货币。

在 IOTA 中，要验证新的交易前，必须直接验证之前的两个交易，这也使得在这两个交易之前所有被验证过的交易得到间接验证。在 DAG 中，顶点代表交易，带箭头的线代表交易的验证关系。在 IOTA 中，有一个权重积分的概念，所谓权重积分是指它自身的权重与它验证过的所有交易的自身权重之和。在 DAG 结构中，交易总是自己创建并发布。从理论上看，攻击者总是可以建构比 它要推翻掉的那个交易权重更高的交易用以双花。

Byteball 在 DAGCoin 的基础上, 创新性引入主链与见证人概念，鼓励验证多个父辈交易单元，形成一个随着交易增长，相互验证安全性不断加强的数字签名 Hash 网络，由于主链算法和见证人发布频率有关系，交易确认的时间是不确定的。由于 Byteball 选择基于关系数据库来存储数据，SQL 语言紧耦合算法逻辑。 在一定程度上限制了 Byteball 的实际扩展能力和速度。当然，这些正是 DAGX 要解决的部分问题所在。

DAGX 基于“主链”概念，也就是经过见证人认定的最短路径 MC 的 Parents 优选算法。主链创造了一个全网共识确定的交易时间序列，优雅的避免了双花问题。

DAGX 网络中“**见证人**”真正意义就是“共识机制”本身；12 个“见证人”发布的交易单元，在理论上无限宽广的 DAG 并发交易网络中划出了一道确定性的交易时间序列。正是这道无限延伸基于时间的确定性交易序列，打造了 DAGX 中的主链，在宽广无序的有向无环哈希世界中形成了强健有序的唯一主干。基于见证人+主链的共识机制，双重支付等问题得到了轻松解决。

DAGX 还取消了区块链和工作量证明（POW）挖掘的概念，而是选择了 DAG 数据存储技术。 与基于传统区块链的加密货币相比，这具有一些优势。

在比特币区块链的情况下，自比特币区块开始以来，所有区块都链接在一条长链上。矿工们将会执行这个计划，以便为这条链增加新的区块。 由于协议的性质，这大约每 10 分钟发生一次。这种创建块的限制是交易时间和费用在网络拥塞时可能激增的原因之一。 DAGX 通过使用完全不同的数据结构消除了这一点。

DAGX 中的所有交易都是以加密方式相互关联的。 新产生交易将添加到叶子交易单元后面。 这样做的好处是网络上的所有节点（用户）都将帮助验证事务。

这不仅可以更快地验证付款，还可以让网络保持足够的分散。 避免在比特币中的一些问题：例如可能威胁网络的大型集中式矿池。

同时 DAGX 收取存储在网络上的每字节数据 1mg 的 DAG Gold 费用，通过资源消耗机制减少网络上的 SPAM 垃圾信息。

分层网络

DAGX 创造性提出了 **DAGX Value Layers** 分层网络架构体系：其中 DAGX 区块链作为下一代网络的核心组件- 1.信任共识和价值交换层，其上依次是 2.去中心化计算层(合约链)、3.分布式存储层、4. 同构跨链层、5. BAAS Dapp 应用支撑层、，共同组成可商用价值交换网络。

DAGX CORE 核心层

DAGX 向用户提供一种去中心化、去许可化、去信任化、具有公平访问权限和可加密协议的基础设施网络 DLT， 无缝链接全球互联网与区块链数字世界；主机服务器、移动设备、嵌入式设备都能作为节点加入到 DAGX 网络中，共同实现网络、应用开发及价值流通， 形成无处不在的大规模组网 。

DAGX 网络由几类逻辑节点设备组成：

1. Hub： Hub 是提供扩展服务功能层和 API 的全节点，允许其他终端设备（全钱包和轻钱包）连接到网络，Hub 还处理加密聊天消息服务。 Hub 可以与其他设备共享数据。

2. 见证人（Witness）：见证人不执行特殊操作，本质上 Witness 不*验证*任何内容，也不会做什么证明工作。 他们的工作仅仅是在后台连续发布见证单元，这些见证单元在 DAG 并发交易网络中划出了一道确定性的交易时间序列。

3. 轻钱包：轻钱包仅包含和自己交易相关的数据，因此数据同步速度极快

4. 全钱包：全钱包拥有全数据库，需要长时间来下载全数据达到同步，Hub、Witness、中继器都包含全钱包。

任何人都可以随时安装钱包软件，接入 DAGX 开放网络，无论是运行 Windows、MacOS、Linux 的服务器、笔记本，还是 Android、IOS 的移动终端，甚至包括运行嵌入式 Linux 的物联网设备；形成 DAGX 价值交换网络生态的一分子。

DAGX DC 去中心化计算层

DAGX DC 是独立的去中心化计算网络层， 由逻辑上独立的 DC Node Network 去中心化计算节点网络组成，每一个 DC Node 实际都是由 XVM 安全容器虚拟机+ DAGX 扩展智能合约接口组成。

XVM1.0：

XVM 安全容器虚拟机用于资源管理隔离、封装虚拟机的 API 通讯等；在之上运行 DAGX 扩展智能核心（DAGX eContract），DAGX eContract 为图灵完备的智能合约模块， eContract 用于开发上层 DAPP，其核心逻辑使用 Node.js 开发，前端则可以使用任意技术，前后端之间通过 JSON RPC 协议进行通讯。

DAPP 运行在 XVM 上的 Node.js Sandbox 中，相互之间不会影响，同时受到 XVM 的整体管理和资源安全隔离。DAPP 代码会在 XVM 中以子进程的方式启动，子进程首先加载一个使用 Sandbox 机制隔离的 JavaScript 虚拟机，这个虚拟机是定制的安全模块 JS 虚拟机。DAGX 为这个虚拟机植入了安全定制的 require 和经过审核的常用安全的模块，最后再加载 DAPP 的代码。 DAGX 还通过进程间通讯的方式提供一系列的 API。 通过这种方式，DAPP 框架就拥有可随时扩展的丰富 API，同时 DAPP 的安装者也没有任何风险。

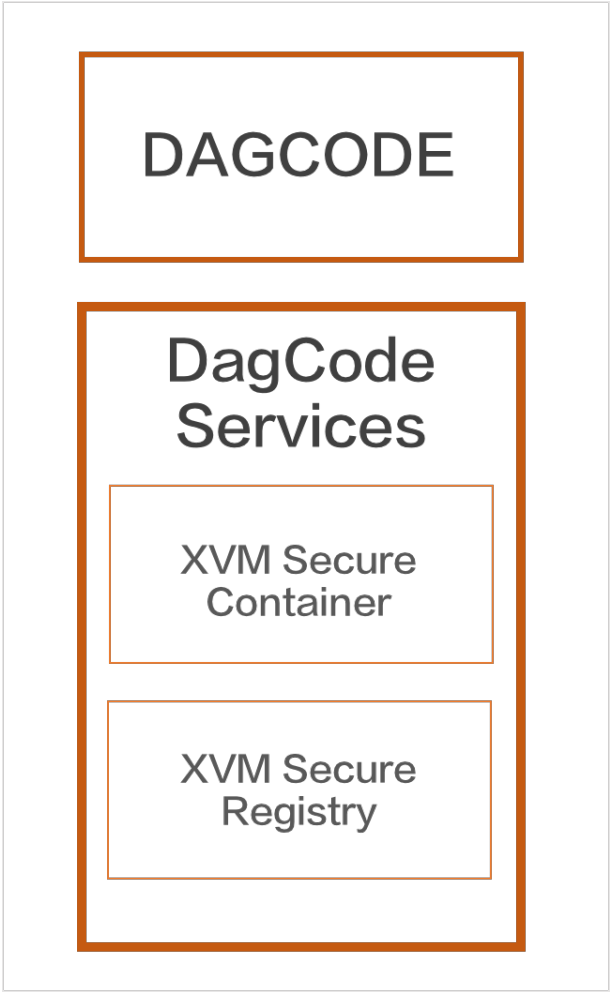
XVM 具备独立的 IP 网络地址，上面运行的扩展智能合约 eContrct 通过链上接口与 DAGX Networks 进行互联， 而 Dapp 基于 Node.JS 和 Javascript 作为主要开发语言，具有简单、易用的特点； 加上封装良好的 API， 形成让开发者可以快速的在 DAGX Networks 上建立自己的应用。

XVM 2.0：

随着 Kata Containers 等新容器技术的成熟，将容器的速度与虚拟机的安全性相结合。XVM 2.0 将会基于 KATA 实现更好的安全性和性能。当前容器技术飞速发展——轻便，性能卓越，易于集成。问题

在于，传统的容器架构涉及主机操作系统和访客容器之间的共享内核，如果一个容器出了问题，集群中的其他容器工作负载就会容易受到攻击。Kata Containers 目标正是解决此类问题。

XVM 2.0 将会实现更好的安全隔离，性能指标、资源管理与横向扩展能力。



- DAGCode（DAG 代码或 D 码）：DAG 链上的应用代码，扩展自“智能合约”概念，先期计划支持 nodejs、golang 等，运行在安全容器环境中。

当前 EVM 实现了细粒度的 GAS 资源控制，每一步操作都有相应的 GAS 计算资源消耗，导致 EVM 效率低下，这种细粒度的控制 DAGX 团队认为是 EVM 的过度管控，对计算能力和扩展能力并无益处；独立的 DAGX DC 计算层通过 Dcode 链码，与安全的 XVM 虚拟机实现整体资源管控，并从时间，存储、网络等几个主要资源维度进行动态管理， 既保证了安全性，也保障了良好的性能实现与扩展性。

独立的 DAGX DC 计算层，和底层区块链解除了紧耦合，在安全性、可扩展性、易用性上都是巨大的改进。

DAGX DS 分布式存储层

大多数在公有链上构建的应用，都需要除了交易信息之外更多的存储空间。（用户信息，财务信息等等）

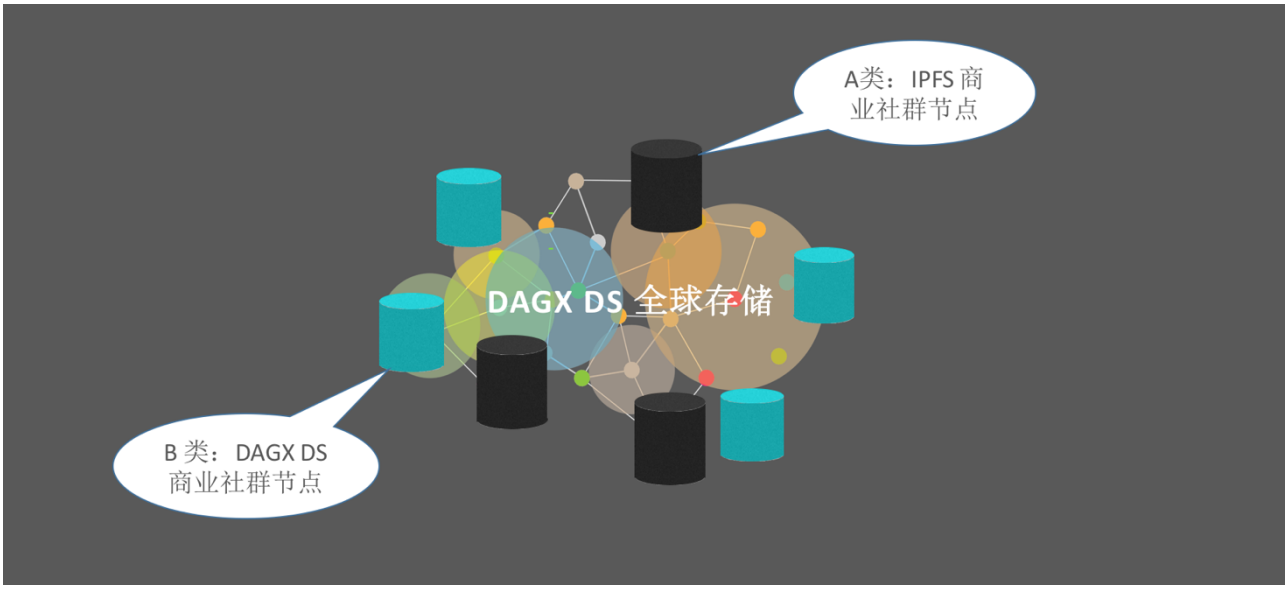
但是，在区块链上存储信息，其实就意味着将信息存储在网站中所有的全节点中。同时存储空间也有限，因为区块链数据库是不可变的。

DAGX DS 通过独立的多中心化/分布式存储层 解决链下数据存储这个问题，DAGX DS 分成两部分：

A 类：分布式非结构化存储，这部分利用 IPFS 项目进行分布式储存。主要的原理是，并不需要每个节点来存储所有的信息，有一系列的存储节点在他们之间来分散存储信息。

B 类：分布式结构化存储， 这部分 DAGX DS 通过全球化按需部署 多中心/分布式 DS 数据库来进行解决，并为运行 DS 存储节点提供 DAG Gold 奖励。

链下数据的锚定通过 Hash 和默克尔树 DS 接口 API 进行，保障校验和数据不可篡改性。



DAGX DS Layer 全球存储服务层

DAGX 团队 2018 年第-2019 年， 部署验证性的 DS 商用服务节点，逐步扩大服务能力，并和七牛云的第三方合作伙伴合作共同推进 DS 分布式全球存储建设。

DAGX 的 DS 服务节点分 AB 两类，将尝试进行 Token 激励的商业化社群运营。

A 类 通过 IPFS 的服务和挖矿机制提供可持续的社群运营支持，提供社群商业化的去中心化存储服务。

B 类通过 DAGX 团队架设的全球去中心化存储节点对外提供类商业化服务，同样基于社群 token 激励机制，奖励 DAGX Gold，除了 DAGX DS 方案， Bluzelle 项目为备选方案。

DAGX SC 分层级多链

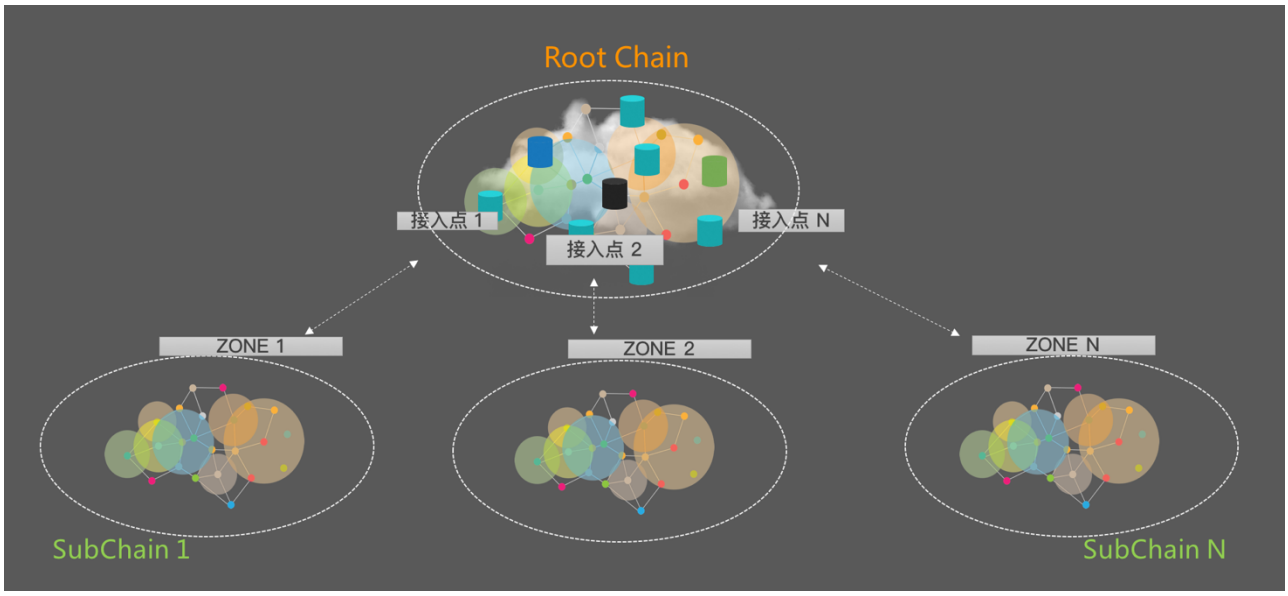
扩容性对区块链的发展是决定性作用。目前已经有一些社区团队在对扩容性进行研究。

DAGX 多链机制为 DAGX Zone，类似以太坊的Sharding机制，通过多条同类型的区块链来实现存储容量、处理能力、容错机制、功能组合的横向扩展。

DAGX SC 通过同构层级侧链的方式进行扩容，DAGX 通过设置 Zone Code，提供了同构多链间类路由机制，通过多链之间的通信协议、Hub将作为多链路由器维护多链间的网络拓扑地图。目标是解决多链之间的连接与分发问题。链路由可以多层次组合构成分层网络结构，目前DAGX 2.0 规划分2层。

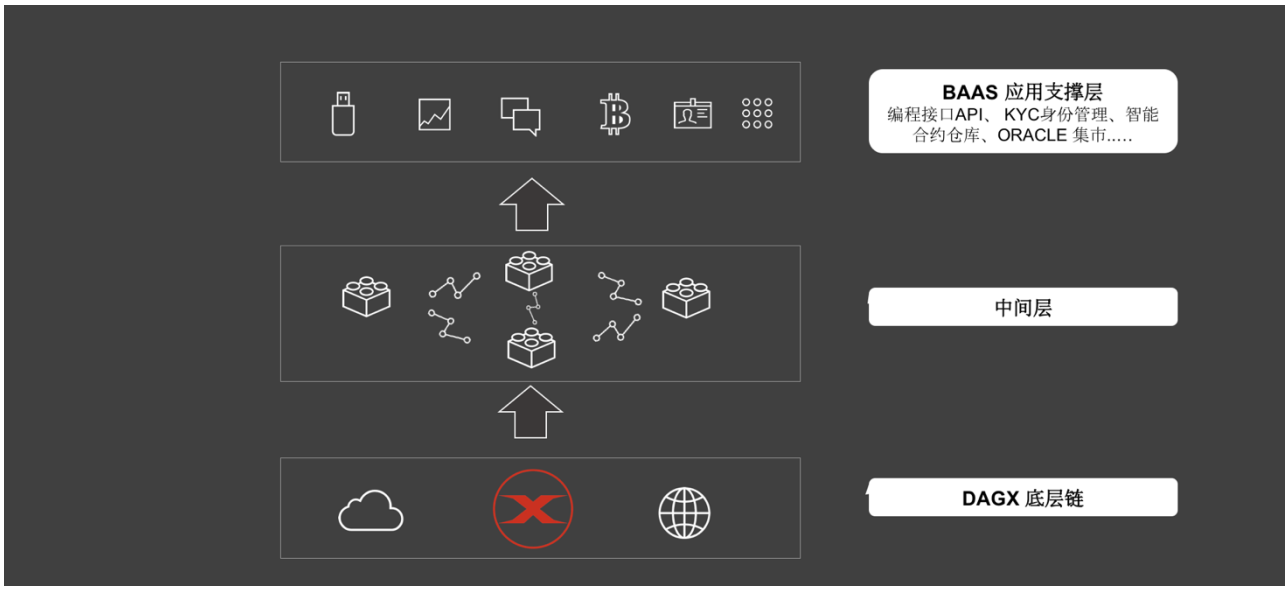
元链层为Root chain，子链层为Subchain。子链层接入元链层为接入点。

用户在任意节点可以设置子链的方式来运行自己的 DAPP，发行 Token 等等，并与 DAGX Root 主网络进行无缝对接。



BAAS 应用 DAPP 支撑层

DAGX 的首个 BAAS 应用 DAPP 组件 Bsure.cloud 已经运作，分期上线数据资产上链、安全智能合约模板、KYC、保险智能机器人市场、去中心化投票、去中心化聊天...等通用模块功能；为 B 端用户开发 DAPP 提供快捷方便的支持。



共识机制

DAGX 网络共识机制为“**主链（Main chain）**”，我们使用“见证人”(Witness) 来见证交易，实际上 DAGX 网络中“**见证人**”真正意义就是形成“共识机制”；12 个“见证人”发布的交易单元，在理论无限宽广的 DAG 并发交易网络中划出了一道确定性的交易时间序列。正是这道无限延伸基于时间的确定性交易序列，打造了 DAGX 中的**主链**，在宽广无序的有向无环哈希世界中形成了强健有序的唯一主干。基于见证人+主链的共识机制，双重支付等问题得到了轻松解决。

如果两个交易尝试花费相同的输出（双花）并且它们之间没有偏序，则两个交易都被允许进入数据库，但只有全序中较早的交易才被视为有效。(全序代表全网所有交易都需要排序, 此处的偏序为本地指定交易集的排序) 全序是通过引用见证人产生的签名单元组成的主链来建立的。 单元的散列如果在主链上较早地被包含则在全序中被认为较早。 用户通过在每个存储单元中指定信任的见证人来选择它们。 见证人是有真实世界身份的且有信誉的用户，并且指定它们的用户也期望它们永远不会尝试双花。 只要大

多数见证人的行为不被恶意操纵（51%容错），所有的双花尝试都会被及时发现并被标记。并有明确的（非概率性）标准来判断用户交易是否最终被确认。

DAGX 将基于合理的利益设计驱动见证人服务，DAGX 将结合 **知名见证人** 和 **选举见证人** 两种方式。 实际上，见证人不执行任何具体的见证操作（他们不*验证*任何内容，只在后台连续发布见证单元）。

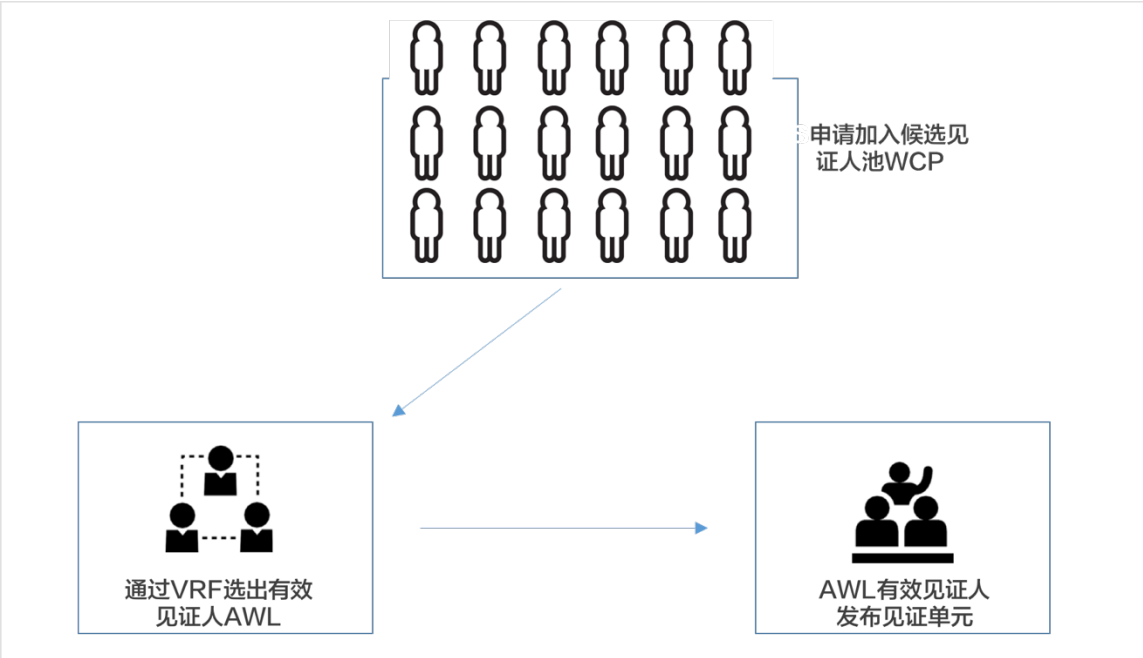
知名见证人机制：DAGX 通过社群选举真实世界的高信誉实体节点来作为交易见证人，这样并非完全意义上的去中心化，但效率高、可实现三方联合管制。

选举见证人机制：通过建立社区申请机制以及选择发布见证单元最多的 Top *x 个活跃*全钱包（POC 权重），建立了候选见证人网络池（ **WCP)** 。**WCP** 大小可以调整（事实上，极端情况下所有全钱包节点都可以纳入 **WCP**）， 通过 **BA-VRF** 共识算法选择 *y 个*见证候选人为有效的见证人列表 **AWL**。 这种方式摆脱了“终端用户选举法”，“真实世界声誉证明法”，“投票系统”，“内置默认列表”以及不适用于去中心化的“+1 改动见证人规则”。 新方法的目的是实现在线实时和真正的去中心化。 所有的钱包都有相同的见证人名单（动态调整服务能力最强并且活跃的全钱包）。

选举见证人可以引入候选见证人淘汰阈值，根据指定的标准执行末位淘汰机制，剔除不活跃的候选见证人。

选举见证人通过引入基于拜占庭算法和可验证随机函数（**BA-VRF**）的共识机制，DAGX 2.0 无需通信和大量计算，就可从见证人候选网络池中随机选出公认的 y 个有效见证人节点，并确定有效见证人节点的优先级。

见证人对于网络运行是关键因素，DAGX 网络协议通过提取见证服务费，以激励见证人长期 24 小时在线工作，基于选举见证人机制的规则，WCP 池中的见证人都有机会获得服务费。



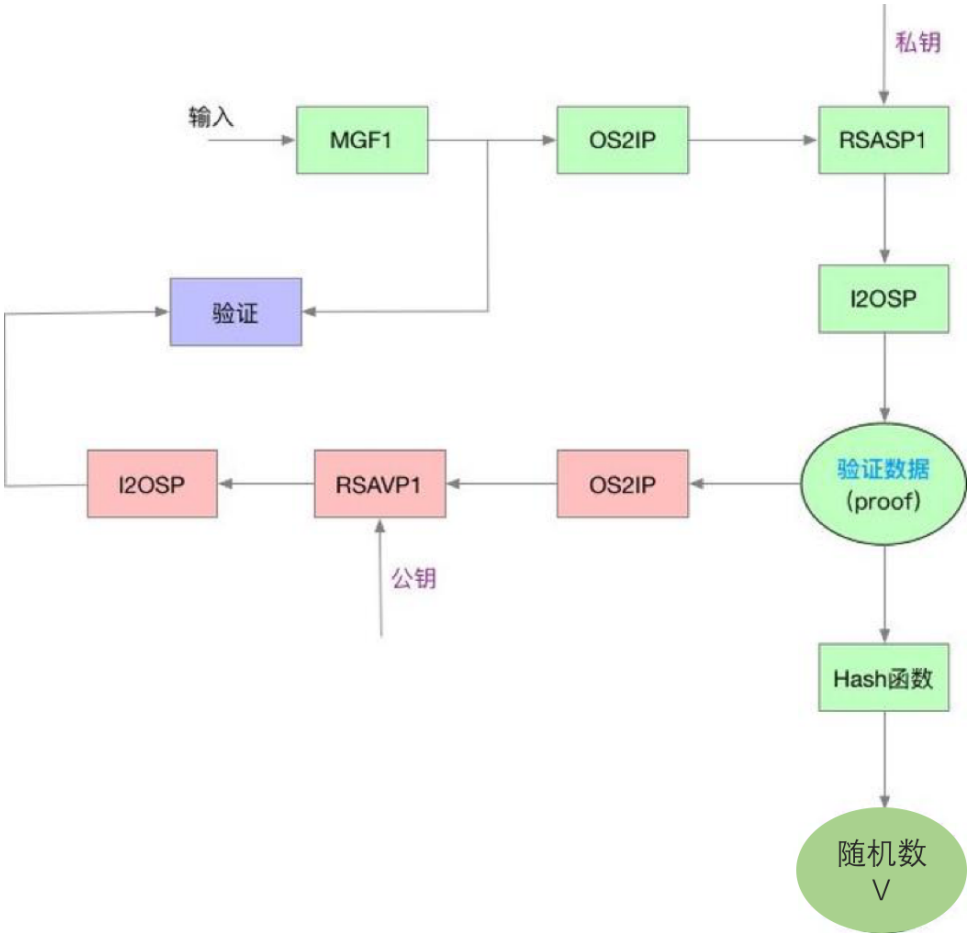
选举见证人机制

可验证随机函数(VRF)

VRF 可验证随机函数是一个密码学的工具，一种伪随机函数，可以使用私钥参与随机数的计算，同时别人可以使用公钥对计算结果进行验证。

VRF 函数的输出由两部分组成：随机结果以及随机证明（proof）。

VRF 函数的实现一般有两种：一种基于 RSA 算法，一种基于 EC 算法。下图详细解释 RSA 算法的生成和验证流程（EC 算法逻辑上类似）：



OS2IP 是字符串转整数字函数，I2OSP 是整数转字符串函数，MGF 是 Mask Generation Function（掩码生成函数）。从上图可以看出，验证数据是 RSA 的加密结果，验证过程从 RSA 的公钥进行解密验证。随机数据的生成是对验证数据再进行 Hash 处理。

简单的说，VRF 提供了一个随机数据生成方法，而且这个随机过程和私钥有关，并可以通过公钥被验证。

-- 计算随机数

vrf :: PrivateKey -> Seed -> (a, VrfProof)

-- 验证随机数

verifyVrf :: PublicKey -> Seed -> (a, VrfProof) -> Bool

DAGX 2.0 通过引入选举见证人机制和 **BA-VRF 算法**，实现有效见证人自动推荐选举机制，在去中心化和中心化之间取得合理平衡。

BA-VRF 算法每 15 分钟发起执行一次，每次达成共识将随机选出有效公证节点，有效公正节点列表将广播发布到网络中去，确认稳定后成为新一轮有效公证人；有效公证节点有权发送公证单元，发布的公正单元确认稳定后，相关有效公正节点将得到系统奖励。

攻击者必须持有超过 *y* / 2（*y* 个最高资产有效见证人）见证人的累计价值，才能欺骗网络。 有实力的全钱包持有者可以申请成为见证人，并获得见证佣金。

持续激励

DAG Gold

DAG Token ，也叫 DAG Gold (简称“DAG”)是 DAGX 网络的内置原生加密数字令牌,用于表征和度量 DAGX 上的数字化经济活动。由于用户发起的交易或智能合约会占用区块链网络的资源，所以需要为此付出一定量的 DAG Gold 作为资源费用，资源费用通过 DAG Token 来计量。

DAG Gold 机制使用存储重量模型，DAGX 网络的 TOKEN 总数对应 10e15 mg 的存储重量，即发行 10 亿枚 DAG Token， 每一枚 DAG Token 对应 1kg DAG Gold（千克），每次交易都会消费一定的 DAG Gold，一般一次交易需要 500 mg DAG Gold 佣金，大概是一枚 DAG Token 面值的万分之五。交易费用负担低。

DAG Token 总发行量为 10 亿枚 DAG Token = 10 亿 kg DAG Gold，Token 默认主单位为 kg，即：1 DAG Token = 1kg DAG Gold

DAG Gold 采用重量单位体系，换算关系如下：

1ton（ 吨 ） = 1000 kg （公斤）

1kg （公斤） = 1000 g（ 克 ）

1g （ 克 ） = 1000 mg（毫克）

注：kg 为 DAG Gold 的默认主单位

网络激励

Hub 是 DAGX 网络健壮性（安全、冗余、可用性）的主要支撑机制。 基础协议鼓励大家运行 Hub。DAGX 将实现合理的激励机制，Hub 通过公告交易所需的佣金标准，通过合理的服务性价比吸引用户（不同 Hub 运营者提供不同的服务质量以及服务内容，比如加密消息服务，价格也有差异化），钱包会自动切换到性价比最高的 Hub 或选择就近最可用的 Hub。

DAGX 将创造了一个 Hub 公共服务市场。，这个 Hub 公共服务市场通过市场机制到达运营平衡点，Hub 运营者将通过其佣金补偿运营支出。 如果运营 Hub 的费用成本在向最终用户收取服务费用后得到平衡或有盈余 - 运营 Hub 可能会成为一项盈利业务，由于所有 Hub 公共服务运营商之间存在竞争，可以保障 Hub 佣金不会过高。 DAGX 将运营示范的 HUB 服务，社区运营 Hub 如果有利可图，那就意味着 DAGX 网络将依靠社群力量成长壮大。

同理，见证人也是网络正常运转的基石，同样会有服务佣金，可以预见的是运行 HUB 的服务商，较大可能也会参与选举见证人机制。

DAGX 创建可持续的算力激励机制

矿工挖矿需要花费巨大的算力解决工作量证明算法，但是这些计算工作对社会没有任何价值，并且比特币现在耗费的电力已经占到了全球电力总消耗的 0.13%，非常的浪费资源。

DAGX 解决这个问题，可以让计算量证明机制变得有意义， 比如让矿工去计算负责的人工智能问题，而不是计算没有意义的 SHA256 问题。同时，还可以考虑权益证明共识机制，让挖矿过程虚拟化。使用网络中的“验证者”代替矿工。

IBM 发起的自 2004 年起发起的慈善活动—— World Community Grid 世界社区网格。WCG 允许您利用计算机的空闲时间帮助科学家解决世界上最大的健康和可持续性发展问题。目前的项目包括:

- 微生物免疫项目
- 粉碎儿童癌症
- OpenZika
- 帮助遏制结核病
- FightAIDS@Home——第二阶段
- 一起战胜埃博拉病毒
- 映射癌症标记物
- FightAIDS@Home

超过 70 万的志愿者已经在为解决这些问题贡献他们的计算资源。**DAGX** 贡献出 20%的 DAG Token 鼓励用户帮助进行有价值计算，并获得工作量报酬。

智能合约

SUPERJ 安全智能合约

DAGX 智能合约的主要优点来自于能够设计特定的智能合约，这些合约将在网络上的所有节点中进行验证。 编入合约的规则是不能改变的，这意味着它们具备不可篡改性。

人们看到智能合约时，可能会想到以太坊。 DAGX 与以太坊的智能合约非常相似，以太坊智能合约使用专有语言 Solidity 功能强大，非常灵活。

DAGX 设计的智能合约为申明式的智能合约，在设计时对功能做了准确定位： 把安全性放在第一位，DAGX 提供基于 JSON 申明式的简安全智能合约，避免以太坊智能合约的灵活性导致的大量安全问题和不可读性。 目标是让非开发人员也能轻松创建这些智能合约。DAGX 智能合约的简单性也意味着较少的编码错误，容易阅读也意味着对金融从业者可审计。

由于DAGX内置强大的智能合约，用户可以创建简单的条件付款， 从技术角度解释，用户可以将付款“绑定”至特定条件。如果交易方没有满足条件，那么用户的DAG Gas将被发回钱包。 这一切都是以直接点对点方式完成的，并且实现的是原子支付。

DAGX 智能合约由申明式的IF / AND / OR条件的系列组成，甚至可以简单的构建多方参与智能合约，一旦其他人验证条件已满足并且仅在合约规定时间到后才会支付给收款方。

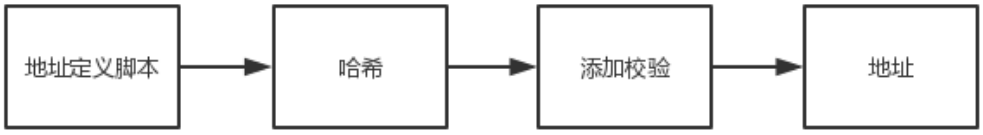
DAGX 团队通过设置常用的外部事件 Oracle 来提供条件付款的事件触发。 这些外部事件的发行方被称为 Oracle，Oracle 已经成为智能合约生态系统的重要组成部分，并可以有用户自行开发设计。

DAGX superJ 智能合约语言里，地址定义是一个布尔表达式，可计算出 true 或者 false 结果。superJ 智能合约的所有表达式，最终都会计算出一个布尔值，多个子表达式可以通过布尔操作级联组合，形成高度灵活表达式。

任何能够使 superJ 地址定义脚本输出为真（也称作解锁该脚本）的用户具有使用该地址资产的权限。与Bitcoin类似，最常用的地址定义脚本是公钥（采用BASE64编码），即具有相应私钥的人可以使用该地址的资产，比如

```
1["sig",{"pubkey":"Ald9tkgiUZQQ1djpZgv2ez7xf1ZvYAsTLhudhvn0931w"}]
```

对于地址定义脚本进行哈希，再加上校验位就得到了地址，Dagx 的地址采用 BASE32 编码。Dagx 地址的校验位并不是全部放在尾部，而是穿插着放在哈希值中间，防止有攻击者在地址中间进行恶意修改。



按照此流程，上面公钥脚本对应的地址为：

```
1A2WWHN7755YZVMXCBLMFWRSLKSZJN3FU
```

Dagx 的脚本语言具备安全自限性，superJ 定义的几乎都是逻辑判断语句，但是表达能力强，易于理解，安全性高。与以太坊相比，superJ 智能合约系统具有复杂度低、轻量化和高性能等优势，同时还降低了合约编写难度和出错概率。

逻辑运算脚本

与运算：当多个条件同时满足时，脚本输出为真。比如，同时需要两个私钥签名的脚本

```
["and", [
  ["sig", {pubkey: "one pubkey in base64"}],
  ["sig", {pubkey: "another pubkey in base64"}]
]]
```

或运算：多个条件中有一个满足时，脚本输出为真。比如，仅需要 laptop、smartphone 或者 talet 中某一个私钥就可以解锁的脚本

```
["or", [
  ["sig", {pubkey: "laptop pubkey"}],
  ["sig", {pubkey: "smartphone pubkey"}],
  ["sig", {pubkey: "tablet pubkey"}]
]]
```

非运算：脚本中不含 sig、hash、address、cosigned by 或者 in merkle 的条件可以进行非运算，比如

```
["not", [
  "in data feed",
```

```
  [["NOAA ADDRESS"], "wind_speed", ">", "200"]
]]
```

逻辑嵌套：逻辑运算可以嵌套使用。比如，必须同时拥有 `smartphone` 私钥以及 `laptop` 或者 `tablet` 中某一个私钥就可以解锁的脚本

```
["and", [
  ["or", [
    ["sig", {pubkey: "laptop pubkey"}],
    ["sig", {pubkey: "tablet pubkey"}]
  ]],
  ["sig", {pubkey: "smartphone pubkey"}]
]]
```

最小数量运算：当满足条件的个数超过门限时，脚本输出为真。比如，具有 2 个以上私钥就可以解锁的脚本

```
["r of set", {
  required: 2,
  set: [
    ["sig", {pubkey: "laptop pubkey"}],
    ["sig", {pubkey: "smartphone pubkey"}],
    ["sig", {pubkey: "tablet pubkey"}]
  ]
}]
```

最低权重运算：当满足条件的权重值超过门限时，脚本输出为真。比如，当几个私钥签名的权重之和大于 50 时可以解锁的脚本

```
["weighted and", {
  required: 50,
  set: [
    {weight: 40, value: ["sig", {pubkey: "CEO pubkey"}] },
    {weight: 20, value: ["sig", {pubkey: "COO pubkey"}] },
    {weight: 20, value: ["sig", {pubkey: "CFO pubkey"}] },
    {weight: 20, value: ["sig", {pubkey: "CTO pubkey"}] }
  ]
}]
```

地址授权脚本

授权使用其它地址来解锁脚本，其定义的语法为

```
["and", [
  ["address", "ADDRESS 1 IN BASE32"],
  ["address", "ADDRESS 2 IN BASE32"]
]]
```

这可以很方便地用来构造共享控制的地址。比如，上面给出的地址定义脚本生成的地址将由 ADDRESS1 和 ADDRESS2 共同控制。

共同签名脚本

要求与另一个地址共同签名才可以解锁脚本

```
["cosigned by", "ANOTHER ADDRESS IN BASE32"]
```

数据订阅脚本

通过订阅的数据是否符合条件来解锁脚本，其语法格式为

```
["in data feed", [
  ["ADDRESS1", "ADDRESS2", ...],
   "data feed name",
   "=",
   "expected value"
]]
```

上述脚本表示：当数据源地址 ADDRESS1、ADDRESS2 等中某个地址发出的消息中订阅数据 data feed name 等于 expected value 时，脚本输出为真。

地址发出的数据订阅消息格式为

```
unit: {
   ...
   messages: [
         ...
     {
       app: "data_feed",
           payload_location: "inline",
       payload_hash: "hash of payload",
       payload: {
         "data feed name": "value",
         "another data feed name": "value2",
         ...
       }
     },
     ...
  ],
  ...
}
```

对赌合约

当某个地址可以作为可靠的数据订阅源时，用户可以使用其作为外部数据条件来构造**合约**。比如，

```
["or", [
  ["and", [
    ["address", "ADDRESS 1"],
    ["in data feed", [["EXCHANGE ADDRESS"], "EURUSD", ">", "1.1500"]]
  ]],
  ["and", [
    ["address", "ADDRESS 2"],
    ["in data feed", [["TIMESTAMPER ADDRESS"], "datetime", ">", "2017-10-01
00:00:00"]]
  ]]
]]
```

上述脚本给出了 ADDRESS 1 和 ADDRESS 2 之间的一个简单合约，假设其对应的地址为 ADDRESS X。当 EXCHANGE ADDRESS 发布的汇率数据 EURUSD 大于 1.1500 时，仅使用 ADDRESS 1 的私钥就可以取走 ADDRESS X 中的资产。而当 TIMESTAMPER ADDRESS 发布的时间数据 datetime 大于 2016-10-01 00:00:00 时，仅使用 ADDRESS 2 的私钥就可以取走 ADDRESS X 中的资产。也就是说，上述脚本定义的是对赌合约：如果 2017-10-01 00:00:00 之前 EURUSD 汇率超过 1.1500，地址 ADDRESS 1 获胜，否则地址 ADDRESS 2 获胜。

交易合约

单元约束脚本可以用来实现去中心化交易。假设用户 `USER ADDRESS` 希望使用不高于 `1000bytes` 的价格购买 `1200units` 的其它资产。用户可以发送 `1000 dags` 至如下脚本定义的地址上：

```
["or", [
  ["address", "USER ADDRESS"],
  ["and", [
    ["address", "EXCHANGE ADDRESS"],
    ["has", {
      what: "output",
      asset: "ID of alternative asset",
      amount_at_least: 1200,
      address: "USER ADDRESS"
    }]
  ]]
]]
```

或逻辑 or 的第一个条件表明，在未成交之前，用户可以随时取回他的 1000dag。或逻辑 or 的第二个条件表明，其他用户可以使用 EXCHANGE ADDRESS 地址私钥来取走着 1000bytes，只要他同时在同一单元中将 1200units 其它资产输出到 USER ADDRESS。通过这种方式，用户之间可以实现不同资产之间的交易。

借贷合约

单元约束脚本还可以用来实现抵押借贷。假设借款人抵押某种资产借贷 10000dag，那么借款人和借贷人可以共同签名一笔交易，其中借贷人将 dags 发送给借款人，同时借款人将抵押资产转入以下脚本定义的地址上：

```
["or", [
  ["and", [
    ["address", "LENDER ADDRESS"],
    ["in data feed", [["TIMESTAMPER ADDRESS"], "datetime", ">", "2017-06-01
00:00:00"]]
  ]],
  ["and", [
    ["address", "BORROWER ADDRESS"],
    ["has", {
      what: "output",
      asset: "base",
      amount: 10000,
      address: "LENDER ADDRESS"
    }]
  ]],
  ["and", [
    ["address", "LENDER ADDRESS"],
    ["address", "BORROWER ADDRESS"]
  ]]
]]
```

上述脚本包括了三层含义：

1. 当时间超过 2017-06-01 00:00:00 时，借贷人可以取走抵押资产；
2. 当借款人归还 10000 dags 至借贷人地址 LENDER ADDRESS 时，借款人可以取回抵押资产；
3. 借贷人和借款人可以协商解除合约。

ECONTRACT 扩展智能合约

eContract 运行在 DAGX DC 独立的去中心化计算层，每一个 DC Node 实际都是由 XVM 安全容器虚拟机+ DAGX 扩展智能合约接口组成。

DAGCode（DAG 代码或 D 码）：DAG 链上的应用代码，扩展自“智能合约”概念，先期计划支持 nodejs、golang 等，运行在 XVM 安全容器环境中。

独立的 DAGX DC 计算层通过 Dcode 链码，与安全 XVM 虚拟机实现整体资源管控，并从时间，存储、网络等几个主要资源维度进行动态管理， 既保证了安全性，也保障了良好的性能实现与扩展性。

XVM 1.0 安全容器虚拟机用于资源管理隔离、封装虚拟机的 API 通讯等；在之上运行 DAGX 扩展智能核心（DAGX eContract），DAGX eContract 为图灵完备的智能合约模块， eContract 用于开发上层 DAPP，其核心逻辑使用 Node.js 开发，前端则可以使用任意技术，前后端之间通过 JSON RPC/ gRPC 协议进行通讯。

DAPP 运行在 XVM 上的 Node.js Sandbox 中，相互之间不会影响，同时受到 XVM 的整体管理和资源安全隔离。DAPP 代码会在 XVM 中以子进程的方式启动，子进程首先加载一个使用 Sandbox 机制隔离的 JavaScript 虚拟机，这个虚拟机是定制的安全模块 JS 虚拟机。DAGX 为这个虚拟机植入了安全定制的 require 和经过审核的常用安全的模块，最后再加载 DAPP 的代码。 DAGX 还通过进程间通讯的方式提供一系列的 API。 通过这种方式，DAPP 框架就拥有可随时扩展的丰富 API，同时 DAPP 的安装者也没有任何风险。

XVM 具备独立的 IP 网络地址，上面运行的扩展智能合约 eContrct 通过链上接口与 DAGX Networks 进行互联， 而 Dapp 基于 Node.JS 和 Javascript 作为主要开发语言，具有简单、易用的特点； 加上封装良好的 API， 形成让开发者可以快速的在 DAGX Networks 上建立自己的应用。

随着 Kata Containers 等新容器技术的成熟，将容器的速度与虚拟机的安全性相结合。XVM 2.0 将会基于 KATA 实现更好的安全性和性能, 更加轻便，性能卓越，易于集成。XVM 2.0 将会实现更好的安全隔离，性能指标、资源管理与横向扩展能力。

eContract 运行在独立的 DAGX DC 计算层，和底层区块链解除了紧耦合，在安全性、可扩展性、易用性上都是巨大的改进

跨链机制

现有区块链技术在单链架构下存在性能、容量、隐私、隔离性、扩展上的瓶颈。

想象一个用户数以亿计的类VISA的支付应用，每秒交易请求高达几万笔，每日交易笔数高达几亿笔，用户交易达到秒级响应体验。在现有区块链技术下，数据存储采用链式本地存储导致无法平行扩展，共识机制采用同步式状态机模型导致无法高效处理交易，同时受限于网络中单节点的性能极限，因此单链架构无法满足应用的性能、容量、用户体验及其他要求。

存储容量上，由于当前区块链技术体系中的单链中的每个全节点都拥有全网所有数据，因此无法满足高容量存储的要求。

同时区块链的互操作性本身就是一些应用的基础需求。想象一个理财应用，用户可以用某项资产交换不同机构的理财产品，不同的资产就需要在多条链上做转移、交换。还有一些ORACLE应用同样需要多链间的跨链引入数据交互，譬如汇率牌价、天气、股价、特定指标等等。

DAGX的跨链机制涉及2个层面：

一：同构多链

DAGX 多链机制为 DAGX Zone，类似以太坊的Sharding机制，通过多条同类型的区块链来实现存储容量、处理能力、容错机制、功能组合的横向扩展。

DAGX SC 通过同构层级侧链的方式进行扩容， 通过设置 XZone Code，提供了多链间类路由机制，通过多链之间的通信协议、路由协议，Hub将作为多链路由器维护多链间的网络拓扑地图。目标是解决多链之间的连接与分发问题。链路由可以多层次组合构成分层网络结构。

二：异构跨链

DAGX 的异构跨链机制，通过运行独立的DAGX跨链节点网络实现，这些跨链功能节点组成的节点网络我们称之为Hash Universe（简称HU），DAGX通过HU来实现跨链交易，通过HU来实现Bitcoin, Etherum、Byteball、IOTA、Nano等异构跨链交易支持，通过跨链机制解决异构链互通和数据交易问题。

当前主要有三种跨链技术实现模式，见证人模式、中继模式和哈希锁定模式

HU方向是专注于解决跨链轻量级数据交换与资产转移。HU网络主要由两部分组成，HU Hub和若干个Zone。每个Zone可以看做是单独的区块链空间。每个Zone会和Hub保持状态同步。Hub通过去中心化的验证人组来保证安全性，验证人组有罚金托管机制，它是唯一的多资产中心账本，并负责保证各类资产在不同Zone转移的同时，资产总量不变。HU通过引入对接第三方跨链平台实现，如跨链开源项目 Cosmos。

跨链技术打破了不同区块链间的藩篱,使得跨行业、跨领域价值流通成为现实。跨链技术把“链”编织为“网”，形成贯通全球的价值网络体系。

安全机制

反垃圾信息与DOS攻击与区块链安全息息相关。

DAGX 通过实现类POS押金机制阻止垃圾信息发布：任何希望发布信息到DAGX网络的全钱包（包括Hub）都必须在押金智能合约上保留一定数量的押金DAG Token。 钱包用户发布新帖子需要的“押金金额”将与智能合约数量成指数增长。

例如：一个全钱包通过押金智能合约申明了1,500mg DAG的“发布权”。 钱包用户发布的押金合约在主链指数1000和主链指数1100之间有效。

在MCI 1100之后，钱包用户不能再发帖，但他可以收回1500 mg DAG。

在MCI 1000之前，钱包用户无法进行发布。在MCI 1000和1100之间，钱包所有者可以以10 exp *x* DAG的价格发布新单元，其中*x*是钱包发布新单元（未稳定单元）的数量。 因此他可以在mci 1000和mci 1100之间同时向DAGX发送不超过3个未经确认的帖子，因为1x10exp1 + 1x10exp2 + 1x10exp3 = 1,110mg<1,500 mg（此处是伪代码，10exp*n* 函数设计成指数增长型函数，防止SPAM攻击）。

DAGX中一个钱包未稳定的单元数作为参数 *x*，另一个参数是DAGX全网未稳定单元总数*y*。通过引入全网未确认的单元总量（ *y* ）来实现DAGX网络全局函数，以达到全局共识。

RequiredPoS（ *x*，*y* ）= ExpFuncMyUnstable（ *x* ）+ ExpFuncGlobalUnstable（ *y* ）

钱包（或Hub）可能同时发布多个押金合同以调整其发布能力。 拥有大量DAG Token的用户可以提交大量的押金，也就是说持续影响主链MCI会很高（这个反垃圾信息策略辅助好处是可以得知设备在网络中投入多少押金，以及能持续多长时间）

在每份押金智能合同结束时，钱包所有者可以拿回担保资金。

基于这样的机制，即使是一个有大量token的钱包也不能洪泛攻击网络。

身份管理(KYC)

加密货币主要的特征之一是匿名， 但用户电子身份管理对于构建一个真实落地的应用生态是至关重要的，对于需要证明个人身份用户，KYC的实现是一个关键功能：当前最普遍的例子是公司在美国等国

家进行类似ICO时必须执行的KYC要求。 DAGX认为用户应该具备身份ID存储在钱包的能力、管理他人共享自己个人身份信息的能力， **KYC身份管理**是DAGX要推出的关键服务之一。

DAGX 正与行业伙伴合作（目前正在评估测试 ccint 、tencent cloud、Jumio 等三方伙伴身份识别服务），推出验证基于 DAGX 地址的用户身份管理功能，该身份验证可以链接 DAGX 地址并按需使用，我们命名其为 XID，XID 功能将大大方便基于区块链功能的商业应用落地，使其更加快捷。

为了实现商业环境落地，需要实现链上数据与现实世界关联映射。 其中最重要的数据之一是身份认证。

通过XID, DAGX用户可以将他的DAGX地址与其真实世界身份相关联。 用户的个人数据由合作的身份验证服务第三方提供商验证，并存储在用户的DAGX钱包中。 同时，个人数据的Hash码存储在公共DAG中，并由可信的证明人签名。 证明人也作为Witeness见证人，已被信任。

该证明允许用户向任何人证明他的钱包DAGX地址与经过验证的人相关联，而不公开任何个人信息。 还允许根据需要向特定服务提供商披露个人隐私信息，服务提供商可以使用公共DAG上存储的Hash码轻松验证此信息的真实性。

运作方式：

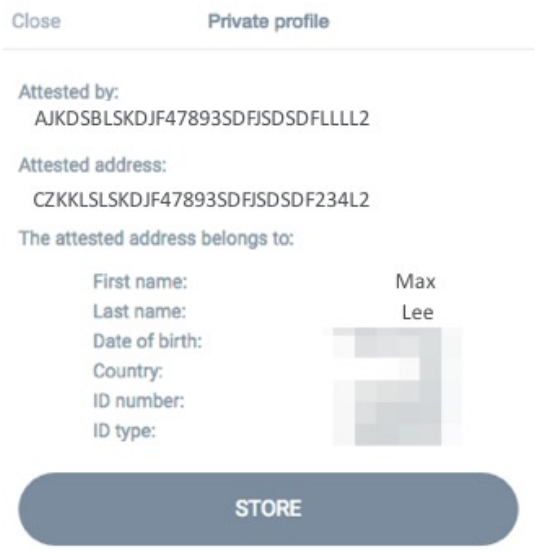
DAGX 通过身份认证机器人实现身份认证 ，设计流程如下：

认证设置成一项有奖励服务 ，每次验证需先支付50元（以DAG支付）。 如果验证成功并且，用户将从DAGX网络获得150元的奖金（以DAG为单位），高于验证费。

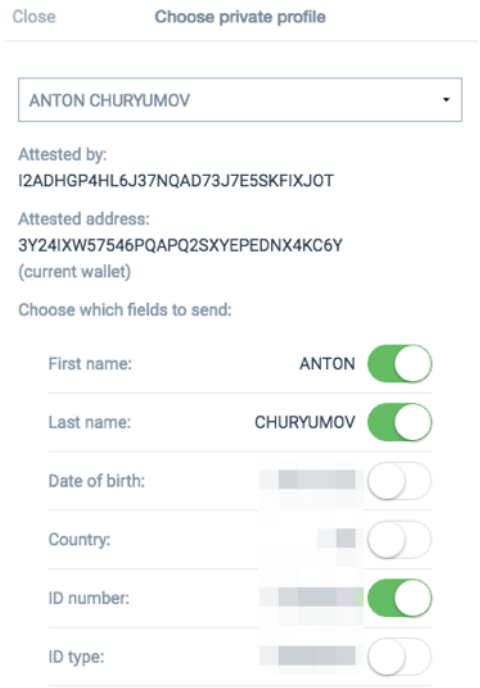
阅读身份认证说明，准备好身份证，确保设备摄像头正常。 支付验证费后，用户将被重定向到第三方验证服务提供商进行实际验证。

用户需要在相机前手持身份证件自拍。 照片拍摄完成后，第三方认证服务提供方会处理数据确保ID不会被篡改。上述过程自动完成的，只花费几分钟，同时提供手动验证，手动认证需时稍多。

完成上述工作后，机器人会通知结果。 如果验证成功，机器人会将认证记录发布到DAG（只包含个人信息的散列，除非用户明确要求发布更多个人信息），并且系统会提示用户将个人信息保存在钱包中以供将来使用：



现在，当用户想要将个人资料透露给他人或机器人时，可以将其从用户钱包中提取，就像将的身份证从用户的实体钱包中取出一样，并选择想分享的字段：



这样，用户可以完全控制分享数据的人员以及字段。

所有实名认证均从特定证明人地址发布，该地址也是见证人。

公民国家认证

如果认证机器人发现用户不是合规国家公民，并且用户在三方网站上进行验证时使用的IP地址也不是合规，则可以证明用户不是合规国公民。

例如：这种证明可以由想要避免美国域外管辖权的ICO使用，并且只允许非美国用户投资他们的代币。 这种限制甚至可以应用于二级市场，方法是在资产定义中要求用户必须经过发布“非美国”认证的证明人的地址的证明。

```
var asset = {
 ....
 spender_attested: true,
 attestors: ["  var asset = {
 ....
 spender_attested: true,
 attestors: [" C4O37BFHR46UP6JJ4A5PA5RIZH5IFPZF "]
 }; "]
 };
```

应用场景

ICO是应用身份认证最直接的案例。

ICO KYC需求大量存在，许多最近的ICO已经要求投资者使用KYC，但必须手动完成或开发临时解决方案。 在不久的将来，市场对KYC / AML合规性的透明度和监管压力的需求将会持续增加。 所以，DAGX在适当的时候会尽快推出这款服务。

其他可以使用安全身份的应用场景：

- 支付欺诈筛选;
- 贷款;
- 年龄限制服务检查（需要公布出生日期，其余的个人信息保密）。

不可追踪交易

DAGX 内置专门为匿名而设计的加密货币。 被称为黑币-**BlackDAG（BDAG）**，黑币专门用于个人间的不可追查交易，。

交易双方之间通过加密消息发送要交易的黑币。 DAG将记录当前交易付款方不再拥有交易的黑币，但是它不会记录黑币新的收款方信息。

比特币网络上的所有交易都存储在区块链中并可以透明追踪，这是比特币区块链具有的好处之一。 但也是双刃剑，也是部分有隐私要求的用户转向了新一代的隐私加密数字货币原因， DAGX 同时支持可追查交易 DAG Token 和不可追踪交易 BDAG 黑币。

资产管理和原子交易

DAGX的另一个特点是用户可以定义自己的数字货币。例如，一个金融机构可以使用DAGX网络来定义自己的资产，如贷款。

金融机构通常会要求应用系统具备KYC核验能力，作为贷款资产智能合同的审核部分。KYC功能是DAGX正在开发的重要功能基础设施。它将允许机构用户轻松地创建自定义资产并通过KYC来核验用户身份。

DAGX支付与智能合约具有内置原子交易的能力。这将保证交易事务能安全可靠的在交易双方同时执行，如果交易条件不满足，不会出现未完成交易。

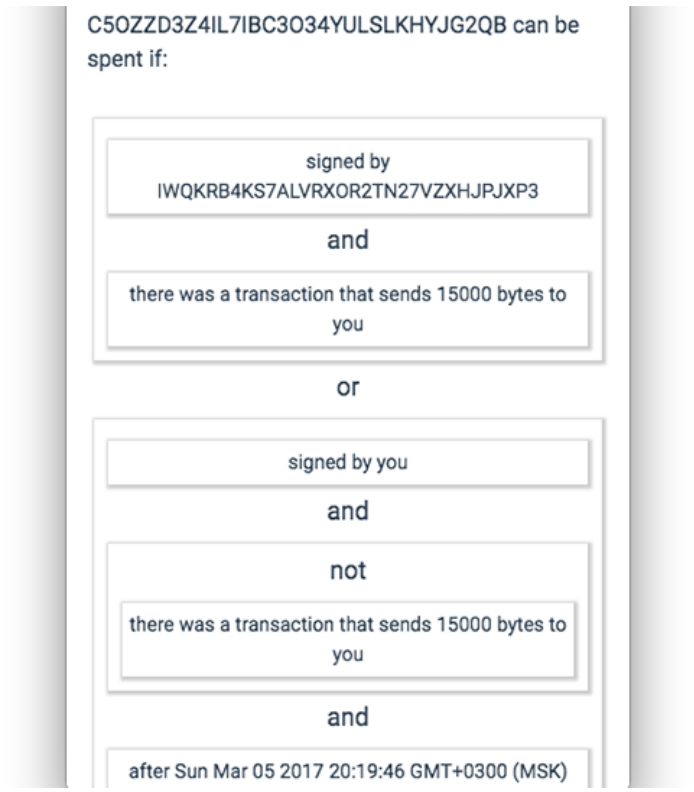
应用示例

- **无风险付款**

比特币支付的一个缺点是，一旦支付完毕，就无法恢复。 因此，如果用户需要根据某些条件付款，那么不得不使用某种形式的三方托管服务。

通过DAGX，用户能创建简单的有条件付款，付款会在预设条件完全验证满足的情况下才会完成最终交易。 从技术角度而言，这将付款“绑定”至特定条件。

如果付款条件不满足，那么用户的数字货币将被发送回钱包。 这些都是通过点到点方式完成的，无需中间人。 用户也可以阅读DAGX应用智能合约，合约由IF / AND / OR条件的系列申明式语言组成，简单易懂。



用户可以构建自己的第三方托管智能合约，一旦其他人验证条件已满足并且仅在一段时间过后才会支付给收件人。

DAGX 将逐步构筑包含外部事件提供组件的智能合约生态。 这些外部事件提供组件被称为Oracle，Oracle已经成为智能合约生态系统的重要组成部分。

- **保险**

当意外事件发生时，用户可能会遭受巨大损失。 虽然保险公司为这些意外事件提供保险，但从保险中获得赔付金并不像预想的那么简单。

如果有一种解决方案，在发生出险事件的情况下，只需几行合约代码就能实现自动赔付？并且合约代码是面向用户开放可阅读的， 这正是DAGX简单合约保险可以帮用户实现的能力。

用户可以通过DAGX的智能合约代码开发一份保险协议，如果条件得到满足，那么获得保险的人将从发行人那里得到赔付金。 用户也可以从专门的第三方市场买卖这种保险。

保险智能合约很大程度上依靠Oracle的服务能力。 由于保险事件大多是外部的，Oracle组件负责将事件的信息提供给智能合约。

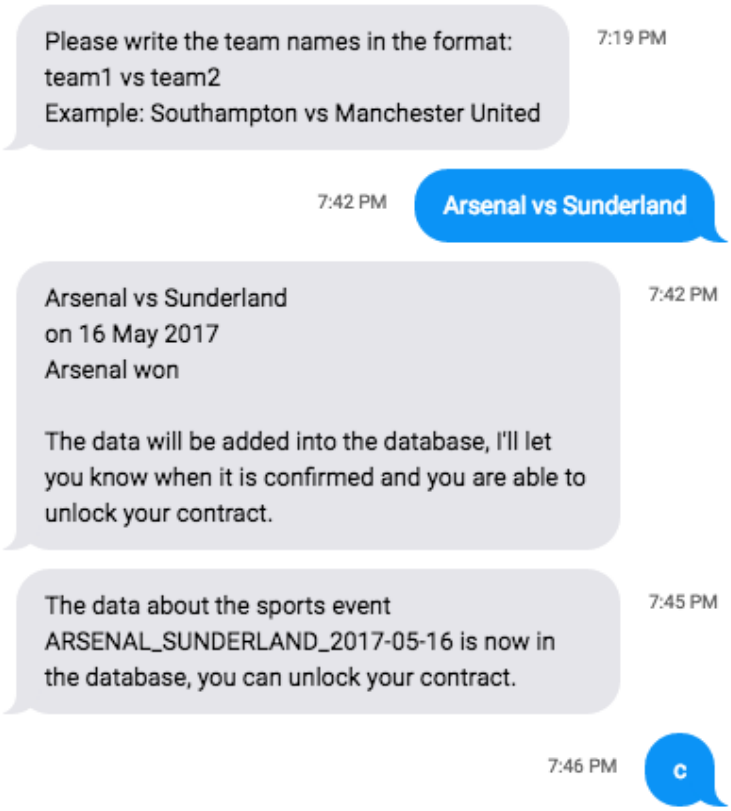
例如航班延误险。 当有人购买航班延误险时，可以将其作为一种合同，在因某种原因航班取消或延误时支付。 在这种场景下，需要的Oracle是航班信息的采集器。

Oracle将向智能合约提供航班信息，以便在航班取消或延误时时执行。 类似保障可扩展到的其他许多应用场景。

- **预测和博彩**

体育赛事博彩例子

用户投注或博彩时，通常预设条件来判断输赢，用户将依据某些事件的结果来获得预测回报。



在P2P博彩的情况下，用户可以与他人在某场体育赛事上签订智能合约， 根据赛事结果，获胜者将根据合约规则从失败者那里获得付款。

用户也可以使用P2P智能合约来押注特定价格趋势。 例如，可以投注比特币的价格，用来对冲投资风险或实现趋势预测套利。

在上面提到的例子中，下注形式是二选一。 智能合约中的代码将在事件发生后确定赢家和输家。 与上面的航班延误险的例子类似，通过 Oracle 将赛事结果事件信息提供给智能合约。

DAGX 路线图

下面是 DAGX 技术革新发展路线图的总体阐述：

1) 对于全数据节点（例如Witnesses见证人节点），增添SuperNode超级节点支持，引入分布式数据引擎，在存储容量上达到**PB**级别，在计算能力上支持同步扩展，在速度上通过多实例计算资源和SQL表达式下推优化，成级数提升处理速度.
2) 引入 **POC （Proof of Contribution）**贡献证明机制算法。利用POC机制可以实现**Witness 自动推荐选举机制**，最后决定依然由用户来确认，我们认为利用 PoC算法，可以做到在鼓励用户参加与贡献的同时，达到一定的攻击防范效果。
3) 引入高性能内存图计算技术， 改造现有的SQL紧耦合底层架构，打造DAGX高速高并发能力。

内存图数据库技术相当于大数据时代的高铁， DAGX 用内存图数据库技术替代传统底层 SQL 数据库。

下表是在一个社交网络里找到最大深度为 5 的朋友的朋友。随机选择两个人，是否存在一条路径，使得

关联他们的关系长度最多为 5？对于一个包含 100 万人，每人约有 50 个朋友的社交网络，以典型开源图数据库测试，结果如下表所示。

深度	SQL 数据库运算时间（s）	图计算的运算时间（s）	返回结果条数
2	0.016	0.01	~2,500
3	30.267	0.168	~110,000
4	1543.505	1.359	~600,000
5	未完成	2.132	~800,000

表 1 复杂关系数据处理上，图数据库比关系型数据库速度快 100-10000 倍

4) 增加“Instant Payment”闪电支付类型，用于小额实时支付技术，快速确认到账，满足商业应用落地需求
5) 引入抗量子计算密码 ，并实现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。
6) 除了原生的强大安全的“申明式合约” ， DAGX将基于Chrome V8引擎、打造全新的虚拟机XVM与“图灵完备的扩展智能合约 eContract” ，实现 DAGX 完备可编程商业智能基础
7) 在共识层， 设计部署“Zone-Code”机制，通过同构多链技术，彻底解决区块链的扩展和容量问题。
8) 设计引入Hash Universe 跨链交易机制，通过HU来实现跨链交易, 并通过HU来实现Byteball、IOTA、 Bitcoin, Etherum等跨链交易，从跨链角度解决互通和数据扩展问题
9) DAGX将推出企业版EDAG特性选项，取消交易费，EDAG 将成为免交易费的企业优化DAG DLT，增加Witness许可机制和身份认证机制，仅许可准入的witness可以被认可使用, 使其更适用与企业/商业机构应用要求
10) 我们将定制一系列基础就绪的内置链上应用服务商店， 包括KYC 、TX 、Oracles；

DAGX 系统特性如下：

1、更彻底去中心化

传统的区块+链式结构，需要有一个类中心化的操作，即需要挖矿竞争记账资格，成功出块的矿工将获得奖励，并将当前所有交易验证打包到一个区块，然后发布到网络。而 DAGX 系统，采用的是单元+DAG 结构，没有区块这一概念。所有单元由用户自己创建与发布。其验证与确认由引用其作为先辈单元的后辈单元来承担，可全网节点并发记录自己单元数据，因而是一种更彻底的去中心化系统。

2、没区块扩容与数据膨胀的悖论性两难

传统区块+链式结构，所有交易要打包到区块才有效。那么区块的容量设置小，则交易量大时，很多交易无法及时打包进区块。如果区块容量设置大，则会使网络传输缓慢、区块链数据迅速膨胀，超出单节点处理能力。这也是比特币扩容之争的根本矛盾点。如上所述，DAGX 没有区块这一概念，所以对于传统区块+链式结构先天性的悖论两难问题。

3、可选交易确认速度

DAGX 的交易单元，只要通过见证人发布的见证单元验证确认，即具最终性。DAGX 通过见证单元系列机制，灵活调整交易确认时间，在速度和见证单元数据比例之间取得平衡。

4、无吞吐量瓶颈

因为传统区块+链式结构存在着，需要记账人将交易打包到区块，这一中心化的操作过程。那么区块链系统处理交易能力的大小，必定受制于以下三点，1，记账人节点机器的性能。2,记账人节点的网络带宽，3，区块的大小。因为存在这一中心化色彩的操作，无论怎样优化，始终都会存在着一个处理能力的瓶颈点。DAGX 采用的是单元+DAG 结构，没有记账人打包区块这一中心化的操作，单元由用户创建发布，并由其它单元验证确认。因而不存在吞吐量瓶颈。

5、明确可预期的最终性

传统区块+链式结构，不排除可能同时产生两个甚至多个区块，由此导至分叉。对于出现分叉的情况，传统区块链将以最长链做为有效链。这种机制在理论上会无法确定最终性，因为无法保证，是否存在一条隐藏长链。而 DAGX 通过见证人机制，只要通过见证人发布的见证单元验证确认，即具最终性，无法推翻。

6、链外数据对接、验证、共识机制

DAGX 中的交易单元，只要通过见证人发布的见证单元验证确认，即具银行级别的最终确认安全性，不存在 51%算力攻击问题

代码开源

开源，指的是将软件的源代码以一定规范开放，其它开发者可以在遵从此规范的基础上使用源代码，或修订和二次开发。与一般的技术项目不同，鉴于区块链的特殊属性， DAGX 定位为开源项目，开源代码回馈 DAGX 社区，让社区力量推动 DAGX 项目的发展，并更好的为 DAG 技术发展做出贡献。

蓝图展望

区块链技术存在跳跃式发展的可能性，金融科技是否真能实现“几乎无限”的扩展能力？ 目前区块链技术的最大瓶颈依然是“同步”，如何获得全网最佳的“低延迟一致性”，其余的指标包括：“最终确定性”、“容量”、“实用性”、“可靠性”、“保证”、“简单性”，“去中心化度”等，这都是需要综合考量的未来 DLT 重要指标。

未来的可能包括使用新的 ZKP 技术，例如可以通过 zk-STARKS 将大量的事务(例如 1M 事务)压缩为一个单一的凭证(例如 1 mb 的字符串)，然后递归地进行压缩。再在这个凭证结果上达成全球网络共识。这将使每一个共识周期的交易能力达到一万亿次。目前问题是评估这样的新途径是否有可能实现，或者是否存在无法接受的潜在缺陷。

其他的可能性包括 Bitcoin-NG2 或 SPECTRE、HashGraph，一些还没有被业界充分理解的新技术(像 Algorand2)，或者“类以太坊 Casper/PoS/sharding 协议技术“。

DAGX 基金会与核心开发团队会非常积极的的拥抱新的技术变化，推动 DAGX 项目快速引领区块链金融科技发展的前沿

ROADMAP

1. **2018/05-06：** 社群启动（1w 电报群　1w twitter 粉丝　500-1000 Slack、DAGX 和 B 端合作，发出第一款产品（赔付宝）
2. **2018/07-08：** DAGX 登录主流交易所
3. **2018/08：** Bsure.Cloud DAGX BAAS 上线（对外开放 DAGX 云服务），DAGX 和众安保险、平安保险、阳光保险、安心财险、复星集团、大都会、…… 保险公司展开区块链数字保险合作探索，探索区块链去中心化数字保险商业
4. **2018/09**： DAGX 主网上链，同步启动 DAGLab 全球实验室, 发布 daglab.io 官网，联合全球所有的 DAG 项目入驻 DAGLab，启动 DAGX 基金，推动社群开发下一代 DAG。
5. **2018/10**：DAGX DAI 去中心化数字保险超市 DAIStore 上线。H5 版本同步上线
6. **2018/11：** DAGX MileStone Ⅰ： primary stone 原石上线测试，速度提升 10-100 倍.
7. **2018/12**： DAGX 和多个健康和保险行业伙伴展开合作伙伴关系，开展项目落地合作。
8. **2019/01**： DAGX 和 CCInt 合作，推动 DAGX.Cloud xKYC 服务落地，并对外提供 KYC 公链服务。并形成 Oracles、KYC、DAPP 服务架构
9. **2019/02**： DAGX MileStone Ⅱ： Magic Stone 魔岩-独立的图灵完备智能合约层 上线测试。并在 dagx.cloud 上提供开发 API 。

   经过 10 - 12 个月 DAGX 运营， 推动 DAGX 和产业界的广泛合作，初步建立 DAGX 价值交换网络体系

团队背景

顾问团队

黄连金

美国分布式应用商业公司Founder&CEO、前华为区块链专家，中国电子协会区块链专家委员，DAGX项目资深顾问

曾 良

倍链资本创始合伙人。曾任金蝶、微软和百度、糯米网高管。 清华大学工学硕士和美国佐治亚理工大学MBA。DAGX 区块链与互联网创新顾问

黎江

微软中国首席技术执行官，DAGX企业区块链发展顾问

吴少萍

国际政策关系发展委员，特普朗亚太裔政策顾问，北美政策顾问

Robin.H

区块链社群教育生态顾问，Bit University（比特大学）创始人，Icon Fund （图标资本）联合创始人

龚剑峰

Nerthus 区块链创始人，DAGX 技术顾问

钟明导

富士康FinConn富金服CEO，DAGX企业应用顾问

朱 颖

医疗健康产业顾问, 爱康君安健疗国际院长，协和系医生集团主任

核心团队：

Max Lee

华为前分支机构技术主任、DAGX CoFounder、DAG区块链专家、中软国际云计算实验室研究员、北京云基地云计算/大数据咨询专家

Jiang Hai

中科大博士，布比区块链创始人，DAGX 技术总指导

Chris chang

微软认证专家，服务于Motorola、利丰、腾讯等公司、DAGX CoFounder

Howard Sun

前JD.com集团战略部和京东金融集团，DAGX CoFounder，金融科技专家

Guo Wei Bin

区块链技术开发专家，14年的开发工作经验，早期区块链技术开发者，
曾就职于腾讯、百度。精通多平台C/C++编程。熟悉golang

Zhe Hou

社区活跃 DAG 技术爱好者(英国) 爱丁堡大学-科学硕士；（伦敦)帝国理工大学-工程学硕士，擅长计算机图论、JavaScript 、Python

Kevin Wang

DAGX区块链工程师、原人工智能和大数据方向

Alan Guan

DAG Core Engineer：资深区块链开发者，DAG技术早期布道者，长期从事区块链研发