B A X

目录

第一章 前言介绍.....3

区块链概述.....3

1.1 共识机制.....4

1.2 传输协议.....4

1.3 数据块.....5

第二章 BAX 阐述.....6

2.1 区块链协议&芯片.....6

2.2 区块链网关.....7

2.3 平台型应用.....8

2.4 交互性应用.....10

2.5 共识算法.....11

2.6 BAX 治理.....12

2.7 BAX 区块链的价值效应.....14

安全优势.....15

无限扩容.....15

第三章 BAX 技术架构.....18

3.1 产品模型及设计原则.....18

3.2 POP 算法架构.....19

3.3 技术架构.....20

3.4 底层架构.....21

3.5 经济模型.....22

3.6 性能扩展支撑.....23

第四章 发展路径.....24

风险声明.....24

第五章 团队核心成员.....25

第一章 前言背景介绍

区块链行业近期的主要发展趋势将会是底层链技术的创新，我们也一直在关注从技术上如何实现更大尺度的去中化。在工信部指导发布的《中国区块链技术和应用发展白皮书》里是这样解释区块链的：广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。区块链作为最颠覆性的创新技术其主要有以下几点特性：

1.1 共识机制

计算机领域成熟的技术（如：P2P 通信，密码学，块链数据结构等）创新的组合在一起，形成了一种去中心化、非信任和基于博弈的自治体系---区块链。随之以以太坊为代表的系统提出了具有图灵完备性的智能合约概念，使区块链既能实现价值的传递，又具有一定的逻辑判断和处理能力。自此以后，越来越多的人意识到区块链技术的巨大价值和潜力，开始关注和研究区块链技术，促进了区块链的基础设施的持续发展。

但是我们看到由于当前区块链平台的局限性，还很少有区块链系统实现和现实社会的连结，在各实体行业的广泛应用仍然受限：区块容量受限，难以处理和记录海量交易，容易造成系统拥塞；共识机制本身缺乏灵活性，无法随意在共识机制中引入不同的因素以动态的衡量用户的贡献力；同时现有区块链系统具备很大的封闭性，目前大多数智能合约仅接受链上数据作为触发条件，缺乏与现实世界的交互。

BAX致力于构建一个全新的区块链生态系统，把区块链技术推向更高维空间的进化和演变，使其最终作为未来世界可选的互联网价值传输协议。通过对分布式技术、P2P 通信、共识机制和智能合约的创新，在芯片物理层及协议层上进行革命，最终使得BAX成为区块链世界连接现实世界中的桥梁。

1.2 传输协议

在传统的中心化网络中，对一个中心节点进行攻击就有可能破坏整个系统，而去中心化的网络采用分布式记录、分布式存储和点对点通信，任意点的权利和义务都是均等的，系统中的数据块由所有节点共同维护。这样就避免了被某个人或机构操纵，无论任一节点遭受攻击或停止工作，都不会影响整个系统的运行。当人们在讨论软件的去中心化时，实际上在讨论的，是三个独立的中心化或去中心化的轴。在没有另一个同在的情况下，很难看清现在的这个事物是中心化还是去中心化的。一般来说，中心化和去中心化互相独立，而这三个轴如下：

a. BAX驱动的雾联网采用去中心化的架构。基于去中心化的需求，BAX重新设计了传统区块链中的一些元素：

b. 共识机制中引入了设备计算能力、存储能力及通信能力的贡献度。

c. 全新的合约设计，链下和链上数据的共同输入作为触发条件，实现线上线下的价值交换。

d. 引入新的交易费率机制，实现区块链社区资源的最优分配。

e. 新的加密结构和访问权限，设备可开放链上数据给指定用户。

f. 广泛集成现有的如分布式文件系统、分布式数据库等第三方软件，将他们的优点和区块链技术结合，取长补短。

g. 优化了和硬件连接的接口，允许不同特性的硬件无缝接入BAX。

h. 在协议层内置币币互兑系统，方便运行在雾联网中的不同 DeOS

i. 政治上的（去）中心化—非单个人和组织控制的去中心化政治体系，比如 AWS 就是一个典型由公司控制的非去中心化云计算服务平台；

j. 逻辑上的（去）中心化—系统呈现和维护的接口和数据库结构像是非结构群体，如果把这个系统的使用方和提供方一分为二，他们还能作为完全独立的单元保持运行显然在任何一个维度上，我们都无法定义究竟节点（决策者）小于多少就是“中心化”的，或者节点（决策者）大于多少，系统就是完善“去中心化”的。

1.3 数据块

在区块链系统中，节点之间无需任何信任也可以进行交易，因为整个系统的运作规则是公开透明的，所有的数据内容也是公开的。而在现实生活中，两个完全陌生、没有信任的人或机构要进行交易，需要依赖第三方权威机构（比如银行）作为信用背书，凭借对第三方机构的充分信任来完成交易。区块链所有节点都必须遵守同一交易规则来运作。这个规则是基于密码算法而不是信任，因此在系统指定的规则范围和时间范围内，节点之间是不能也无法欺骗其它节点，自然无需任何第三方介入。

通过这些创新，人与人、人与物、物与物的相连不通过中心服务器而在BAX所架构的分布式结构里完成，前面所述的中心化问题均可以得到完美的解决，并最终发展成为一个软硬一体的生态：所有运行在BAX共识机制上的设备或系统都可视为BAX里的公民：他们向其他个体购买生产资料；他们贡献自己的生产力获取报酬；他们缴纳一定的税收；他们在法规的约束中博弈。

社区建设和代码开源：BAX致力于通过社区、第三方开发者和技术上的创新，打造一个在全球具有影响力的开源社区生态，通过开源鼓励第三方的开发者一起推动BAX技术渗透不同的应用和产业。最终目的是将区块链融入万物相连的世界，成为现实世界个体信息传递和价值交换的媒介。

雾联网基金会：为实现BAX的可持续性发展，避免散沙式的发展结构和 底层构架分化，BAX基金会将制定完善的治理架构，对一般轶事、代码管理、财务管理、薪酬管理和特权操作范围等事务进行管理。同时，治理架构会随着 基金会和社区的发展不断更新，并引入监察和监督功能，规则制定和变更控制 管理等。

商业应用：BAX基金会通过与合作伙伴的通力合作，将企业、商界、技术和政府等多方面资源进行整合，最大化实现资源共享，最高效利用资源，实现社会协同发展。

第二章 BAX 阐述

2.1 区块链协议&芯片

BAX区块链协议旨在定义一个雾联网（即未来的区块链网络）的运行模式，其中主要包含治理模式、共识机制、价值传递规范等，并通过开源的芯片解决方案，为区块链的广泛应用提供有力的基石。

区块链协议将提供一系列的关键性规范文件，是形成所有共识的基础，基于协议之上采用层次结构，可以很容易的讨论和学习协议的规范细节，并创建了一个更好的互连环境，降低了整个雾联网的复杂度，使共识更容易达成，发展及进化的速度更快。

而专业的可编程区块链芯片，将共识机制从应用程序层下沉到芯片内核层， 使BAX在性能及安全性上更能发挥价值。

BAX 结合分布式存储、智能合约、分布式人工智能、多重签名等技术连接用户、银行、券商、基金、信托、P2P 平台等，通过共识激励体系让生态参与者自发的维护 BAX 生态的可持续发展。BAX 的生态主要由传统商业银行的业务演化而成的基于区块链的新型数字化生态。BAX 生态最主要的目的是解决传统金融行业的透明度、公信力、数据传输和隐私保护得不到保障的问题。BAX 生态中会出现在大量可扩展的延伸业务，通过 Dapp 实现更多创新型业务结合区块链技术来解决金融行业遇到的更多问题。

BAX 是一个开放的金融行业的平台，支持多种 Dapp 的开发和上链，帮助所有参与者灵活参与生态。参与者可以通过技术服务者快速开发数字资产托管、数字资产清算、数字资产交换、数字指数投资、资产证券化等多种适用于不同玩家需求的不同功能的应用。BAX 生态通过区块链技术保障各方参与者的利益。促进整个金融行业数据上链，多方维护，打破传统金融行业各环节的壁垒，提高金融行业价值传递的效率，建立一个自由、平等、安全、可信、开放、共享的金融行业新生态。

2.2 区块链网关

对于普通用户而言，区块链似乎是一个高深的技术，同时，到目前为止，普通用户几乎没有接触过区块链应用（除 Token 外）。

BAX区块链网关的出现，革命性的降低了普通用户使用享受区块链所带来的改变，使得普通用户获得了一把开启通往区块链世界之门的钥匙。

数字资产清算业务是 BAX 生态里最为基础的应用，在 BAX 生态中所有的用户，包括金融机构、上下游企业、券商、信托、基金等，涉及到交易的行为都会经过 BAX 数字资产清算应用进行资产清算。BAX 用户首先需要自己对数字资产和数字货币进行数字资产登记，交易的买卖双方通过智能合约进行合约化交易以及资产的自动化结算。

玄尺对于衡量BAX和雾联网的性能，增强BAX的安全性和稳定性起到关键作用。玄尺在链上度量的性能有：BAX中区块大小、区块生成时间、矿工的参与度等；玄尺在链下度量的性能有：雾联网中设备 P2P 传输时延、设备带宽、设备存储空间、设备负载和业务能力等；雾联网上应用的稳定性、应用的使用频度、应用的传播性、应用中价值流动的频次和规模。基于上述指标， 玄尺对获取的数据进行分析和处理，然后提供给玄规。

玄规获取玄尺提供的数据之后，着手构筑BAX的价值体系，建立更完善的模型，挖掘更多元的价值维度，采用更加节能环保和稳定的共识机制。玄规在确定BAX价值体系的变化之后，可以向社区提议进行BAX升级。

2.3 平台型应用

BAX 生态可以实现数字资产间的交换，BAX 将会支持数字资产与传统资产之间的交换，比如说股票、仓单、票据、库存、厂房等实物资产可以在 BAX 生态中进行资产数字化，确定相应的价值，通过使用 BAX 来进行相应价值的结算，兑换成相应的数字资产。同时，这些数字资产可以在二级市场进行交易买卖。

我们把类似于 Windows、Linux 等系统对于电脑芯片而言的区块链操作系统类应用模式称之为“平台性应用”。

在遵循BAX雾联网协议的基础上，任何区块链底层操作系统均可以运行于BAX系统之上，比如现在的比特币网络、以太坊、EOS 等，只要愿意遵循BAX的共识机制或互操作协议，那么也可以运营在BAX里面，并使用、调度链上资源。

此类平台性应用我们称为“DeOS”。

2.4 BAX 区块链价值效用

我们把具有低延时高可靠性要求的应用称之为交互型应用。主要包括车联网、Mesh 组网、医疗诊断、安防报警等。此类应用的服务需要在较低（可能在毫秒级）的时延内获得确认，确认时间远远小于目前一般区块链技术的区块确认时间。在 BAX 生态里，用户可以通过使用 BAX 购买股票类、数字货币类、大宗商品类等，通过用户自己选择设定的时间（时间设置多久由用户自己决定），到期后 BAX 通过清算系统自动进行结算，并且判断用户的盈亏并形成报表提交给用户自己查阅。

在 BAX 生态体系中，通过对参与者的有效活动进行 Token 奖励的激励机制，更好的激发了参与者的主观能动性和积极性，并通过区块链去中心化和数据公开透明的特性，来解决价值信任问题，形成可靠的数据流闭环。BAX 生态体系构建了一个新的金融环境和商业关系，改变了市场的观念以及彻底颠覆了传统金融行业的价值流动和分配模式。BAX 作为 BAX 生态里的唯一支付手段。对于生态里的各个参与者的业务往来，通过智能合约的形式实现 BAX 的流通，BAX不仅仅是支付工具，还可以成为激励手段，BAX 的高流通性是 BAX 生态里实现高活跃度的有力保证。

2.5 BAX 区块链价值效用

BAX 生态是一个并行多主链的结构。其中最重要的主链是 BAX 主链，它是维持整个系统生态运转的核心，BAX 主链除了承担交易记录、用户体系以及跨公链资产交换的功能以外，还记录了生态中所有其他链的信息，基于BAX 主链可以实现天然的跨链资产交换。在 BAX 多链生态里，其他主链的底层代码和 BAX 主链几乎是一致的，不同的在于其

他主链的代币情况和共识算法的区别。其他主链在fork 了BAX 主链的代码以后，可以部署到自己的节点独立运行，这种情况下该主链相当于一条独立的区块链，和主链的生态没有产生直接的关联。

如果一条基于BAX 代码运行的主链想要加入到BAX多链生态的话，他该如何操作呢？BAX 多链会提供一个统一的客户端。这个客户端可以看做是其他主链和 BAX 主链进行连的入口。其他主链可以在这个客户端里提交自己的主链信息，包括部署节点、代币名称、代币数量以及共识算法等信息。在向 BAX 主链注册成功以后，这条主链就可以共享 BAX 多链技术生态的资源了。

每一条基于 BAX 代码运行的主链都需要有自己的代币，即所谓的“一链一主币”。主币可以充当该链上的交易手续费。另外由于 DApp 开发也可以基于主链，是主链的上层应用。主币的功能及消费都可以在 DApp 里进行定义。

安全优势

公链是区块链发展的前提基础，也是区块链行业未来发展的核心保障。而目前区块链的发展现状是，底层公链的性能尚未发展起来，在其上构建的各类 DApp 严重受限于性能，各种共识算法都有不完美之处，安全问题也令人堪忧。由于智能合约一旦上传，即公开且不可更改，因此大多“区块链 2.0”项目有安全性验证的需求。一些团体也开始致力于应用形式化验证技术，为智能合约和区块链生态提供安全保护。将智能合约转化为数学模型，通过逻辑上的推理演算来验证模型，从而证明智能合约的安全性。

但由于智能合约是“不可变更的”。一旦部署，它们的代码是不能更改的，导致无法修复任何发现的 bug。在潜在的未来里，整个组织都由智能合约代码管控，对于适当的安全性需求巨大。过去的黑客如 TheDAO 等漏洞事件提高了开发者们的警惕，可见我们还有很长的路要走。

一个保障每个合约都能正常运行的公链。这一创新极大程度上简化了架构，降低了数据处理压力，确保一条链上流量激增不会影响到另一条链的效率，在链上进行的任何业务都不会收到其他业务干扰，有效实现了资源隔离。

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喂入交互，譬如汇率牌价、天气、股价、特定指标等等。区块链的某些应用在单链上无法完整实现，需要在多链架构下的可扩展性、隔离性、高性能、互操作等特性的帮助下实现。

在 BAX 中 Token 链是一个并行多链的结构，多链多共识，共享用户基础。BAX 的 Token 是链上的一个属性，就像使用了 UTXO 模型的链 UTXO 有其他 Token 一样，我们的转账事件也是内置的。BAX 提供了一套底层的区块链机制，其他的区块链项目可以很容易的基于 BAX 的主链代码部署一套自己的主链。BAX 开发者可以轻易的开发一个DApp，其他的交给 BAX 来处理， BAX 的“一链一主币，多链多共识”的机制为后来的区块链项目开发提供了很大的便利，可以使用于任何区块链适用的应用场景，而互不影响的 DApp 多链系统，可以一直横向扩展，也就带来了事实上的无限扩容。

第三章 技术架构

3.1 产品模型及设计原则

设备节点可以衡量自身对于设备资源，如 CPU,内存，带宽和存储空间的占用，和事务属性等定时以合约的形式记录到链上。事务属性是为了表示事务的紧急和重要程度。

共识算法会以这些数据为依据，对不同节点的贡献度排名，挑选出区块验证者。即使两个节点的资源贡献完全相同，但是不同的事务属性也会导致两个节点的贡献度不同。

BAX 基于区块链技术打造安全、可信、共享的金融行业新生态。BAX 底层提供了完整的分布式账本体系，包括完整的智能合约体系和系统安全体系等等。同时 BAX 支持各类主要应用协议、多维认证协议和各类跨链协议。

BAX 还提供了包括数据分布式存储、跨链智能合约、安全多方计算、可信数据交换等技术体系。BAX 基于 Javascript+PostgreSQL 开发完成，包括区块浏览器、轻钱包都是使用 Javascript+Node.js+Nginx 搭建而成。

在此基础上，BAX 提供了一系列应用框架，通过通用 API、SDK 以及各种应用功能组件，进一步支持各类上层应用的实现。BAX 的速度目前能达到10000TPS，已经足够金融行业的各种业务使用，未来，随着更多节点的加入， BAX 的速度会随之而增加。

3.2 PO P 算法

在 PoP 共识机制中，系统将首先选取 态中广泛的具有代表性的账户作为候选账户。选择候选账户时，系统同时考虑多种因素：如，账户的地域分布；账户的业务类型；和此账户关联的设备贡献度。候选账户是具有广泛的代表性， 这个方法非常接近于人民代表大会制度，每个人民代表具有相同的投票权力， 而他们又是各自的省份和各自行业中的佼佼者。

社区对系统生成的候选账户进行投票，按照所得票数的多少，系统从中按照概率挑选总共 N 个账户作为区块生成者,其中 N 由社区投票决定，并被写入到BAX玄规中（第 1.2.6.1 章节）。候选账户所获得的投票数越多，被选中成为区块生成者的机会就越大。因此最终所选取的区块生成者既具有了广泛的代表性，又拥有社区的共识。通过社区投票可以剔除那些虽然具有设备贡献力，但是却对社区建设不够活跃的或者恶意破坏BAX生态的账户。

BAX 区块链由区块组成，区块由标题和已确认交易列表组成。代理分配一个插槽并且有一个节点正在运行时，该委托会生成下一个块并确认来自交易池的多达 51 个交易。这些确认的交易将被添加到该块的有效负载中，并随后被登录到该块中。

于标识块的版本；块创建时的 32 位时期时间戳；前一个块的 64 位 ID；与块中处理的交易数相对应的 32 位整数；一个 64 位整数，对应于传送的 BAX 总量；一个 64 位整数，对应与该块关联的总费用；代表的 BAX 奖励相对应的 64 位整数；有效负载长度相对应的 32 位整数；有效载荷的 256 位散列；生成该块的代表的 256 位公钥。BAX 使用 DPoS 共识在 BAX 网络内每隔 8 秒发生一次块生成。代表是一个账户，有权通过其他 BAX 持有者的选举过程产生屏蔽。区块生成需要 51% 的同行维持 broadhash 共识。一旦建立 broadhash 共识，节点将使用区块中描述的技术生成一个块。密钥对：密钥对由私钥和公钥组成。私钥是只有密钥所有者才知道的一条信息。公钥是从私钥导出的，可用于验证私钥是否属于所有者，但不提供对所有者私钥的访问。椭圆曲线密码术用于生成密码安全密钥对。用于生成密钥对的过程在以下假设下运行：当用户创建一个帐户时，为用户生成 BIP39 助记符（密码）。使用 SHA-256 哈希函数将该密码散列为 256 位字符串。该散列随后被用作 ed25519 中的种子来生成私钥 ks 并导出其公钥 kp。这个私钥，用户可以将交易签署到交易对象中并将该对象广播到网络。公钥包含在事务中，接收事务的节点能够使用 kp 来验证签名的有效性。这为用户和网络提供了有效的安全性，因为 ks 只

为用户所知，kp 可以验证签名是有效目的。

BAX 为用户提供了额外的安全层，使用特定类别的交易，用户可以注册与秘钥相关联的第二密码，设置第二密码需要收取一定的手续费（目前暂定为5BAX），这种关系要求所有后续交易都要使用第二个密码进行签名才能被视为有效，设置第二个密码的时候，用户可以直接通过钱包设置。

多重签名：

对于需要更高安全性的用户，BAX 支持多重签名帐户作为另一个安全系统。多重签名账户是一个需要多个签名者提交签名交易的账户。任何用户都可以通过发出一个特殊的交易来在他们的账户上启用多重签名，指定一组 ksn 和确认交易有效的所需的最小签名数量。然后在区块链中规定，在处理来自该账户的任何交易之前，源自该账户的任何交易必须由最小法定数量的相关账户签署地址：

BAX 地址或钱包 ID 是从公钥导出的，使用 SHA-256 散列公钥，然后颠倒散列的前 8 个字节。帐户 ID 是这 8 个字节的数字表示，以 M 字符开头。

3.3 技术架构：

为了维护区块链生态的健康，区块链中交易的过程一般需要支付一定量的手续费，手续费是对矿工在区块链中处理交易所占用资源的一种补偿。发起交易的账户需要指定自己愿意为这笔交易支付的手续费；而矿工则可以指定自己愿意处理的最低的交易手续费，只有手续费高于这个最低值的交易才会被该矿

工处理。矿工会优先打包交易手续费高的交易，如果一笔交易所愿意支付的交易手续费过低，这笔交易可能要等很久才会被打包确认。交易费的设计可以鼓励更加高效的合约代码，减少不必要的计算，避免系统遭受攻击，毕竟攻击者要为他们消耗的资源付出一定的代价。

从经济学的角度来讲，交易的发起者们通过竞价向矿工购买了确认交易的服务，而矿工通过价高者得的原则销售自己的服务。因此我们可以通过经济学中的机制设计理论(Mechanism Design) 来指导矿工费率的设计。简单的讲，经济机制设计理论是研究在自由选择、自愿交换、信息不完全及决策分散化的条件下，设计一套机制(规则或制度)来达到既定目标的理论。

图 阐述了矿工在处理交易时的两种不同情况。图中矿工对所收到的交易的价格从高到

底排序为 ！＞ ！＞… ＞ ！ ＞… ＞ ！，每个区块最多可以容纳 笔交易合成一个包来工作。然后该捆绑包按照每隔 5 秒指定的时间间隔向网络广播。除了广播对象之外，该组件还有一个中继限制以防止过度广播数据。在当前的实现中，中继限制被设置为2，这意味着每个数据包将从始发节点广播一次，并且从接收节点多出两次。

3.4 底层架构

BAX 采用双链架构设计，双链架构分为用户链（UBC）和交易链（TBC）， BAX 分别在两条链中做优化，不仅可以保障用户隐私，还能够节省大量算力。双链架构是负载均衡的，既可以并行计算又可以串行计算，拥有良好的扩展性能， 因此只要增加服务器就能够增加区块链速度。

并发共识是指并行的拜占庭算法（PBFT），能够确保用户隐私不泄露。拜占庭算法分为三轮投票，每一轮均按照 N 的 2 次方这种广播式投票，三轮投票后达成共识才能够建块。与传统的耗费巨大计算力的拜占庭算法不同，BAX 的算法在不简化任何一轮投票的基础上，将交易与投票并行，因此纵使投票过程复杂度增加，整体的交易与投票过程不需要彼此等待，提高了交易速度。

3.5 经济模型

BAX 系统是基于JavaScript 开发而成，在架构上内置了区块链防火墙，这个防火墙接口来自全球顶级安全公司 Mcafee。BAX 以后的所有应用及软件都将结果 Mcafee 审核，最大化安全防范。

少被攻击成功的几率。

BAX 官方将在全球部署大于 200 台的节点服务器，这些服务器将通过mcafee 解决方案进行的安全硬件设置（防火墙、路由器、服务器、设备），我们经过验证的网络防火墙与最高效的下一代入侵防御系统 (IPS) 及高级恶意软件防护 (AMP) 完美融合在一起不仅能拒大多数黑客与门外，同时也有效提高整个生态环境的安全性。

分布式数据存储

BAX 提供了安全加密的分布式数据存储能力，BAX 构建数据块的分布式哈希表（DHT），用户访问数据时根据DHT 找到数据所在的块节点列表，然后取回并验证数据。当其他用户访问文件时，需要被用户授权得到密钥后才能查看数据。

当用户将数据存储到 BAX 时，BAX 会对数据进行分片并使用户密钥对数据进行加密，

然后在 P2P 网络上进行分块传输，因此 BAX 存储加密的分布式数据区块，保护用户隐私和数据安全。

安全多方计算

安全多方计算（SMC）是解决一组互不信任的参与方之间保护隐私的协同计算问题，SMC 要确保输入的独立性、计算的正确性、去中心化等特征，同时不泄露各输入值给参与计算的其他成员。主要是针对无可信第三方的情况下，如何安全地计算一个约定函数的问题，同时要求每个参与主体除了计算结果外不能得到其他实体任何的输入信息。

区块链的数字签名、不可篡改、可追溯、去中心化，安全多方计算的输入隐私性、计算正确性、去中心化。区块链技术和安全多方计算的结合，多方安全计算作为区块链数据加密和验证机制的组成部分，而区块链技术又作为云计算、AI 等基础设施平台的组成部分，结合零知识证明和其他密码学技术，构成了下一代通用计算服务平台，具有去中心化、数据保护、联合计算等特点，对上层业务形成新的支撑。

3.6 性能扩展支撑

传统区块链上所有的交易都被记录在公链上，所有的用户都可以查询到每一笔交易的来龙去脉，这种机制确保了交易的公开和透明，对金融应用更是极大的推进。但是在BAX和雾联网的应用中，并非所有的数据都是公开的，某些数据属于用户个人所有。这也是我们把物联网改变成雾连网的初衷之一，把属于用户的数据从服务提供商归还给用户。

以此为出发点，我们设计了全新的用户访问权限。在BAX设备中，每个用户的数据都用自己的密钥加密存放，同时受BAX访问权限的保护，在用户没有授权的情况下，其他人无法破解。而用户对服务商或其他用户的每次授权都被公开保存在BAX上，这样可以用BAX的不可逆特性记录他人对用户数据的访问，确保安全性。

数据所有者在BAX上授权他人访问自己的数据主要分两步：第一步，数据所有者发送一个交易，里面包含了数据的 ID（数据摘要的哈希值），把当前 已有数据注册到BAX上；第二步，如果数据所有者要把数据授权分享给他人， 他再发送一个交易，交易里面包括了数据流的 ID 和用被分享人的公钥地址。BAX 生态涉及多种数字金融场景，通过 DAI 可以对各种数字金融服务进行智能匹配。结合区块链和 DAI 技术可以更好的实现数据价值保护和传递。

第四章 发展路径

2018 第二季度——BAX 技术团队成立

2019 第三季度——*PoP* 共识机制基本完成，*BAX*代码开源

2019 第四季度——测试主网上线& 标准白皮书上线

2020 第一季度——全球首款支持 *PoP* 共识机制的区块链网关（雾联网节点）发布

2020 第二季度——全球*BAX*开发者社区对外正式开放，雾联网联盟启动

2020 第三季度——支持数据库输入，主网链接

2020 第四季度——接入宁波城商行系统测试

2021 第二季度——主网测试，DOPS机枪池攻击算力试行

风险声明

本白皮书只用于传达信息之用途，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。

本白皮书不组成也不应理解为提供任何买卖行为，或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;

BAX 基金会相信，在 BAX 及其他加密货币和区块链系统的开发、维护和运营过程中存在着无数风险，这其中很多都超出了基金会的控制。除本白皮书所述的其他内容外，每个 BAX 购买者还均应细读、理解并仔细考虑下述风险。

投资者应明确了解 BAX 代币的风险，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;

BAX 团队不承担任何参与 BAX 项目造成的直接或间接的资产损失;

每个 BAX 的购买者应特别注意这一事实：BAX 只存在于网络虚拟空间内， 不具有任何有形存在，因此不属于或涉及任何特定国家。

第五章 团队核心成员

张太云 创始人

POP技术专家，马来西亚华裔、具备千万级代码运营经验，具有着丰富的数据与互联网经验，

Mr Ma 联合创始人

分布式计算专家，连续创业者，曾在排名前十金融类媒体、互联网营销等领域就职和连续创业。

Mrs Liu

技术合伙人，在数值优化、数值线性代数、线性/非线性规划、稀疏矩阵、迭代求解器、约束优化、稀疏线性方程组、稀疏最小二乘法等领域具备领先技术水平。

张爱男 COO

纷纷传媒创始人，曾任职传媒中心数据实验室首席，具备金融数据传媒和实战经验。