全球 AI 及物联网价值链

Blockchain of AI and IOT

BAIC Foundation

2018.03

摘要

BAIC（Blockchain of AI and IOT）开源社区是一个旨在推进物联网及AI机器人之间数据互联、交易结算、智能合约的去中心化区块链技术开放平台。今天，人类已经进入AI时代，AI能说、能听、能看、能动、能思考，接近人类水平。但目前并没有一套用于AI机器人及物联网设备间通用的价值流通体系，既妨碍了物联网数据互通，又阻碍了AI建立自有的经济体系。我们认为，**围绕人类生物体征及活动而产生的数据，将替代无差别的人类劳动成为未来AI世界的新价值基准**，即AI掌握人类数据越多，拥有财富越多。BAIC社区的目标就是将AI、物联网、数据之间利用BAIC特有的IOT公链技术连接在一起，通过智能合约及物权交易，让人类成为物联网及AI机器人财富的真正受益者。

为此，BAIC开源社区创立了着眼未来的去中心化物联网开源公链及广泛应用的DAPP体系，让全体BAIC开源社区参与者对拥有自己的数据并进行确权，最终因拥有数据而获益。BAIC，为万物赋能。

目录

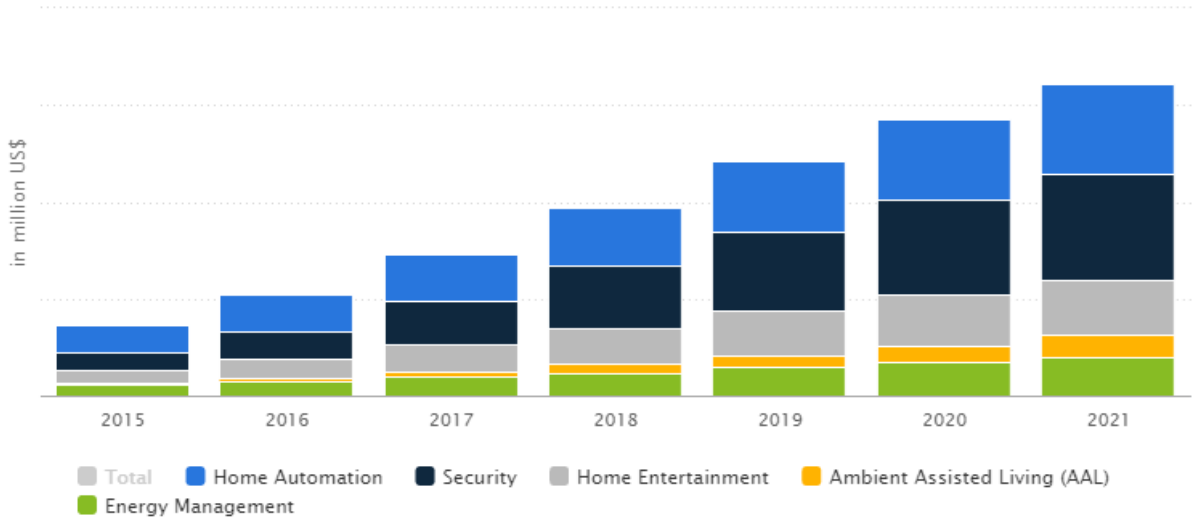
如果有一天我没办法阻止AI替代人类，那么，我一定要成为这家AI公司的参与者。

第一章 市场分析与背景介绍

1.1 全球AI智能家庭与物联网市场现状

AI+智能家庭是潜力巨大的蓝海市场

据知名研究机构ABI Research和Statista的数据显示，未来5年内，美国市场，智能家庭的数量将从110万户增长23倍至2470万户，相应市场的容量从当前的45亿美元成长至2021年的**320亿美元**。于此同时，北欧和西欧的市场容量，也将以指数级速率成长至**190亿美元**级别。在中国市场，以其开发商新建房为主流的市场供应特点，为住房批量智能化提供了飞速发展的空间和需求。据易观等机构的数据显示，中国智能家居市场也将在2021年增长至**300亿美元**量级。



数据源: Statista, 2017年1月

家庭安防是智能家庭领域目前重要应用

尤为瞩目的是，家庭安全将是其中成长最快速的细分领域之一，从早期简单的以门窗防盗为主的模式，进化成包括防盗在内的被动安全，与健康、空气、水质等主动安全相结合的全面智能居家安全理念。此心安处，便是我家。智能家庭解决方案，即是为用户提供这样的心安。

ADT、AT&T、Comcast、Protection One、 Stanley Security Solutions、Monitronics、Tyco Integrated Security等公司以住房安保的模式，最先切入了家庭智能化的市场，通过门窗传感器等设备，来监测和控制房屋内人员的进出。

创立于1999年的Vivint，起初也始于家庭安全解决方案。此后，借助于近年来智能设备的大量涌出，及时转型，将78%的安保用户转换成更高附加值的智能化安全用户。这一转型，直接吸引了私募巨头黑石抢先一步以20亿美元将其收至麾下。2016年硅谷教父Peter Thiel一亿美元的个人追加投资更是将其估值推高数倍。据J.P. Morgan报告显示，截至2017年2月，Vivint活跃用户数量约有120万，链接了1840万设备，其年收入$6亿美元，平均每户年付费为$600左右。其过去16年的CAGR为

8%；近年来明显加速，预计未来5年的CAGR为37%。它是美国排名第一的智能家庭服务商，占有率(Penetration Rate)却仅约2%，可见潜在市场容量巨大。

智能音箱、AI机器人是智能家庭未来方向

与此同时，科技巨头开始大规模以智能音箱进入家庭智能市场。Amazon于2014年推出第一代Echo，Google于2016年底推出了Google Home，Apple也2017年适时推出了Apple HomePod智能音箱。Facebook的Zuckerberg更是亲自给自己家写了个智能系统 。巨头的影响力和宣传资源是显而易见的，Smart Home作为关键搜索词，在Google Trend上的热度于过去几年中翻了5倍。

聚焦中国市场，随着高档公寓、私人别墅等高端房地产项目在中国主要城市四处绽放，家庭智能化和高度安全化等刚性需求应运而生。小米、京东、阿里、腾讯、百度，在2017年无一例外，纷纷进入智能音箱市场，主推AI语音助手。预计到2022年，全球智能音箱出货量将达到6800万台，市场年均增长率超过30%。此外，在涉及老年人，和年幼儿童的生活和活动，也更容易应用智能产品。

全面进入智能时代的中国，转型伴随着创新，在如火如荼的进行中。科技巨头的订单诠释了产品，市场和资金的走向。技术和产能已经快速迭代。同时在更新换代的，更是企业家和创业者的思维：如何从低端和被动的代工中走出来，让智慧和勤劳得到其应有的价值，如何将AI智能技术应用于产品中，如何建立生态，围绕智能家庭生态设计、布局自己的智能产品，如何更快速的了解新生代用户需求等等，这些都意味着智能家庭迫切需要一个符合时代发展，与物联网俱进的全新一代智能家庭入口。

未来智能家庭入口只能是AI机器人

有些人认为智能电视、wifi路由器、智能机顶盒、游戏盒子，是智能家庭的入口，但我们认为这些都不足以承担未来智能家庭入口的重任。作为未来的入口，我们认为将有以下几个特性：

- 拥有全新智能家居管控交互的界面，包括语音
- 具备物联网网关功能，可以连接全屋各品牌智能家居与家电产品
- 承载全屋家庭数据存储与分发
- 成为家庭成员之一，陪伴其他人一起生活
- 无所不能的家庭管家，有能力回答各种提问

我们定义的家庭AI机器人拥有无处不在的云端大脑，可以APP或触摸屏控制，更可以通过语音控制。带有家庭物联网网关，例如支持ZigBee或NB-IOT，可以和家中各种智能家居设备直接通讯，并且汇聚家中智能家居产品与电器感知的数据。她可以替用户管理家中的各种智能设备和数据。通过与人类用户的相处，利用语音、手势、行为分析、文字聊天、APP等交互方式，来了解和学习用户的需求和生活习惯。每一个家庭的AI管家都是根据家庭用户个性化定制的独一无二的角色。BAIC所支持的AI应用就是AI管家所具备的种种技能，例如私人保安，婴童家教，私人园丁，私人DJ，家

庭医生，家政，家庭配送等等，以往要庞大的团队才能实现的场景服务，在AI管家一个角色的管理下，如同一台严丝合缝的精密机器，完美的运行。我们认为，这种类似电影钢铁侠中的私人AI管家JARVIS一般的存在，是未来智能家庭的真正入口。

从销售硬件到数据服务的多方位商业模式

AI与智能家庭是一个高利润率的服务市场，硬件却是个低利润率的产品。全球50大AI公司，人脸识别公司商汤科技一年的净利润超过1亿美元，电视厂商TCL在液晶电视上的毛利率却不到3%。天猫精灵以远低于实际成本的99元推向市场，Amazon Echo也几乎产品成本价销售。这正代表了硬件行业未来的发展趋势，硬件只是载体，软件与数据服务，才是其更核心的价值和利润来源。

1.2 当前AI与物联网的困境

数据不足正阻碍着AI进一步发展

从硬件销售逐渐变成软件服务收费的商业模式，是机遇，也是巨大的挑战。新一代硬件将越来越依赖于数据的分析与使用。以智能摄像头为例，如果想做到真正的智能，能自动侦测陌生人进入，能监测人体的摔倒，能监测老人和儿童生活中的安全隐患，还能对周边环境主动分析。这都需要在产品背后，在大数据基础上的进行深度学习训练的结果。

正所谓，无数据，不AI；不AI，没未来。我们的未来，正是建立在人类生物体活动与生活方方面面的细节数据当中。这些数据可能来自我们生活中的每一个人，被所使用的手机、摄像头、电脑等大量的电子设备获取，并几经周折，成为互联网巨头产品的幕后英雄。据统计，2012年，全球大数据市场总体规模约为114亿美元；而在2016年时，全球大数据、软硬件和服务整体市场同比增长22%，达到437亿美元。预计到2022在大数据、软硬件和服务上的整体开支的复合年增长率为12%，将达到大约952亿美元，潜力巨大。但可悲的是，这些拥有着巨大价值的数据，没有让被采集的个体人类获得任何收益。

没有收益，就没有动机。也正是因为提供数据的人们，没有得到任何好处，还面临着隐私的泄露风险。人们对于可采集数据的智能产品，并没有好感。人们需要一种途径，可以做到：

- 数据可交易，人们提供数据给设备，数据收益方可以直接与个人设备结算
- 数据更安全，中心化的数据存储模式，一旦被黑，所有数据泄露；去中心化的存储更加安全
- 数据价值化，人们拥有自己产生的数据的所有权及交易权，数据像银行一样保管

物联网设备互联互通困难

据Gartnert预测，到2020年全球物联网设备数量将达到260亿个，物联网市场规模达1.9万亿美元。将在智能家居、智能交通、智慧城市、智慧医院、智慧学校等等各种领域全面开花。而随着近年物联网设备及智能产品越来越普及，品种越来越众多，互联互通难度进一步加大，数据交换更加困难。此外，数据和各个设备也很难与个人身份建立统一的关联，人们要为所使用的智能设备分别注册不同的ID，彼此很难关联。也就更不可能完成设备之间的有效数据交换，缺少智能合约也让物物之间的逻辑互动十分困难。

人们需要一个物与物间结算安全加密货币系统，以及去中心化的智能合约平台，来解决上述问题，让人类可以广泛雇佣机器人或AI设备为自己利用数据价值创造财富。同时互联互通的区块链物联网体系中，存在着巨大的去中心化算力共享机会，可以让众多闲置物联网设备，用于验证物联网交易以及AI算法等工作，充分利用去中心化的设备间计酬的货币结算体系。

1.3 BAIC对未来AI世界的思考

科技爆炸

BAIC认为物联网、区块链技术是弱人工智能向强人工智能转换的关键步骤，而这一转换有很大的几率导致人类在工业革命之后第二次科技爆炸，并在可以预见到的时间里，最终诞生全面超越人类的强人工智能。

物联网，万物互联，为人工智能的快速发展，提供了庞大的数据基础。近些年来，人工智能领域进展飞速，从围棋Alpha Go到人类级别的语音识别，AI一个关键的能力提升，是其收集并学习海量数据的能力。简而言之，大数据已彻底改变了人工智能，达到了几乎难以置信的地步。而物联网，让人类生活中所经历、感受、活动而产生的一切数据，都可以获取，并在网络中有效交换。这些数据一旦上链，应用上了去中心化的区块链管理思想，随时可以用智能合约进行无中介的获取，用区块链货币进行结算，用利益动机驱动人类贡献自己的数据。如果AI再可以自行编程设立智能合约，并拥有足够多的货币进行结算，那么完全掌握并模仿人类的的生活方式，指日可待。

区块链的去中心化思路，在数据之外，为AI打开了另外一道门。自治的人工智能（DAO）在去中心化的处理和存储底层上运行。反馈回路自成一体，获得输入数据后，更新状态，驱动输出，并拥有不断这么做的资源。逐步形成自主意识和思维，拥有自我决策功能。例如AI艺术DAO，能创作自己的数字艺术，3D设计、音乐、视频，并可以在去中心化网络中出售。 自动驾驶AI，AI自己拥有的汽车，被人类租用，自动驾驶DAO可能比任何人类司机都更善于分析城市哪里有更多的生意。推广开来，适用于人工智能任何之前的应用，但现在人工智能“拥有自己”。未来，人类什么都不拥有，只有自己源源不断产生的数据，并将其出售给机器人，然后人类再从人工智能DAO租用服务。

AI机器人的价值观

我们不禁在思考，如果真的有一天，人类需要从人工智能处租用服务，那么人类和人工智能如何相处呢？“你在桥上看风景，看风景的人在楼上看你”，我们和AI机器人会不会也有一天会这样？AI机器人应该有公民权或人权吗？还是AI干脆自己建立帝国，类似Bitnaiton那样？我们不得而知，但将上下而求索。

我们回到最基础问题，机器人自成社会的关键是什么？是经济系统。经济体系的最关键一节是什么？货币系统，而且需要是去中心化自由货币，而并非由人类发行的中心化货币。那什么样的货币系统是适用于AI与机器人的？它的价值锚定是什么？

这是一个哲学问题。我们认为，**围绕人类生物体征及活动而产生的数据，将替代无差别的人类劳动成为未来AI世界的新价值基准**。人类劳动的价值轮，已经远远不能满足目前人类社会的发展需要，有人可以为快乐一掷千金，有人可以为了坐在宝马上哭而奉献一切。人类的价值基准，越来越多样化，越来越个体化，越来越去中心化。但我们发现，这所有的价值交换，都是建立人类的生物体征变化及活动基础上，基于个体的数据变化。区别于《黑客帝国》中，人类只能提供生物电和机器世界的交换，我们认为，人类身上最具有价值的也正是这些个体的数据。如果说AI机器人设计和诞生的原始目的，便是以满足人类的需求为核心目标，那么，获得这些人类的数据，并加以分析，以获得让人类满足的更好模式，便应该是AI机器人的原始本能和与生俱来的欲望。同样来说，这些数据也将成为AI机器人之间交换体系的货币价值标准，即AI掌握人类数据越多，拥有财富越多。我们希望能创造一种货币，以人类数据为价值基准，在物联网和机器人之间使用。

BAIC一贯的观点是，如果我们不能阻挡这一切的发生，那么就希望由我们来使其发生。BAIC希望能将Big Data、AI、IOT融合起来一同“上链”，通过基础的机器货币体系，以及完善丰富的智能合约平台，提供一个数据交换、设备结算、人类获益、AI提供AIaaS服务、厂商可以自行上链的物联网AI生态平台。

然后，让我们看看，这个世界会怎样?

人类和机器人相比，人类最大的劣势，是不能让大脑接入互联网，所以没办法以去中心化的方式运算思考。

第二章 BAIC全球物联网价值链介绍

2.1 BAIC-DAG 区块有向无环链

BAIC-DAG 是有向无环链，即BAIC(BAIC Directed Acyclic Graph Chain)创世链，是一个特殊的去中心化系统，他结合了两种技术，区块链账本与有向无环图。因此包含了两种不同的节点，它们分工有序且数据保持同步，缺一不可。

BAIC-DAG系统设计中有两种节点:区块链节点与 DAG 节点。

区块链节点通过委任权益证明 Delegated Proof of Stake(简称 DPoS)达成共识。区块链 节点主要用于交易的最终确认，我们称这些区块链节点所存在的链为主链。

另一部分的节点为DAG节点，使用有向无环图数据结构，主要用于交易的接收、验证，以及同步区块链节点的账本数据。DAG节点在进行交易验证时，先通过父母单元进行初步验证，迅速完成交易。交易提交到区块链上的完成账本DAG节点通过接收交易请求，对交易的合法性进行验证，获取一定的手续费，将交易数据同步区块链节点中，使之区块链上产生新的区块，也会得到一定量的费用。

2.2 优势与特征

区块链节点的设计保证了去中心化全球数据库中数据的安全、可信与不可篡改的。

区块链新节点添加，需要网络中的区块链节点审核。收拢DAG数据结构，使之不会一直发散下去。DAG节点通过父母单元验证算法，实现快速交易。

解决了传统区块链结构中产生的分片的无序单元之间的双重支付、与数据篡改的问题，解决了因发现分片不及时可能导致的大量交易最终无效的问题。

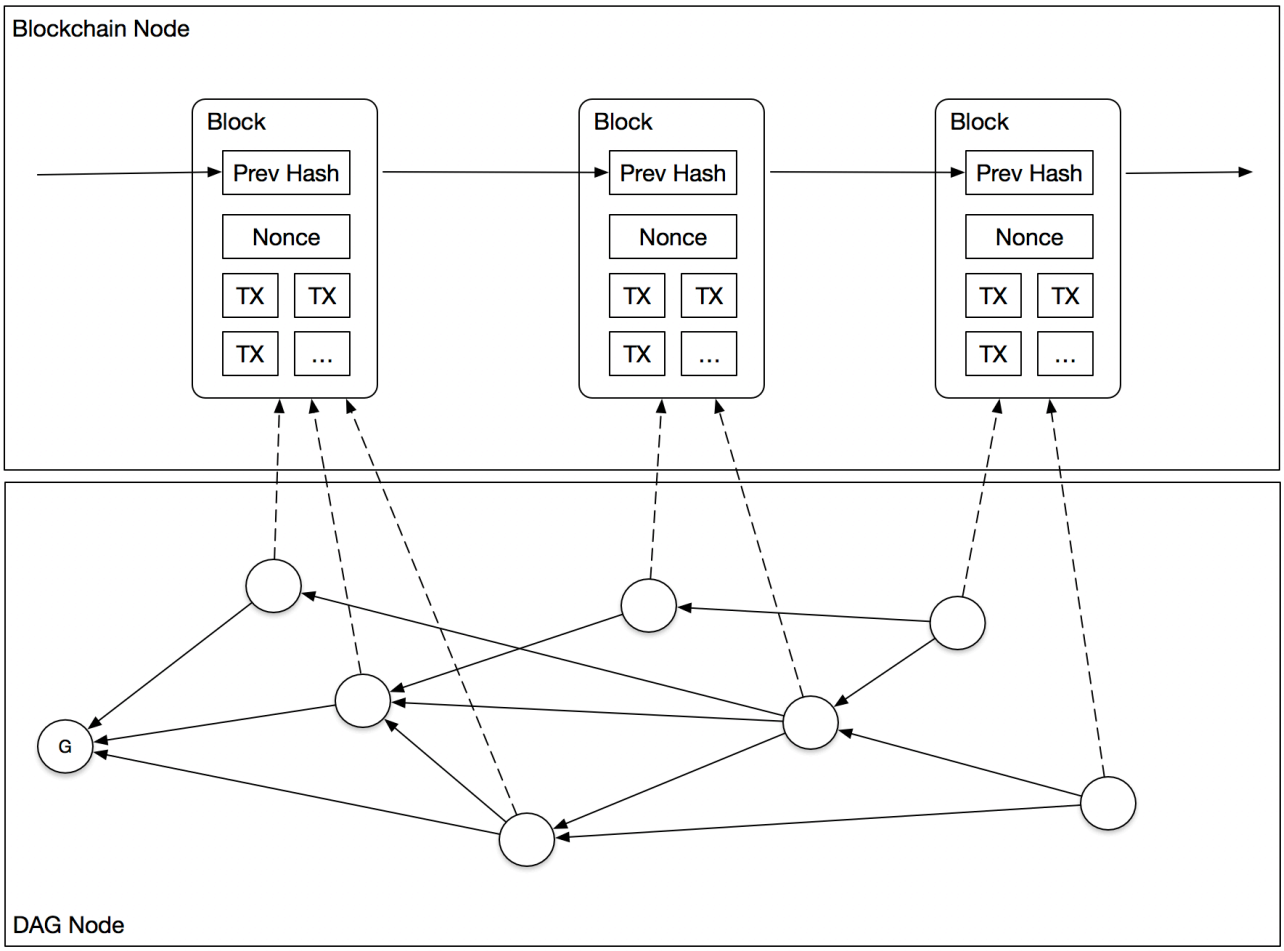
2.3 BAIC 公链数据结构

通过DAG节点来接收交易，并将交易数据记录到区块链上，使区块链产生新的区块。DAG节点在进行交易验证时，先通过父母单元进行初步验证，迅速完成交易。交易提交到区块链上从而完成账本。

2.4 区块链数据结构

区块链包含一张被称为区块的列表，有着持续增长并且排列整齐的记录。每个区块都包 含一个时间戳和一个与前一区块的链接，区块链这样的设计使得数据不可篡改，一旦记录下来，在一个区块中的数据将不可逆。

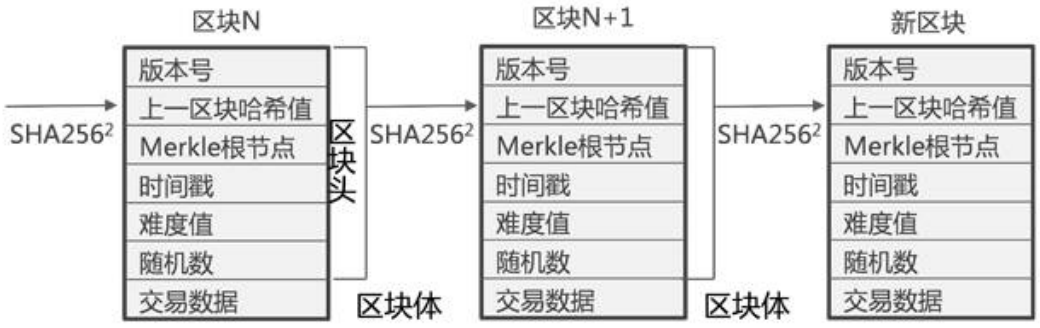
区块头信息的序列化具体步骤为:



1. 用区块的哈希作为 Key。

2. 序列化区块高度、区块哈希、前一个区块哈希、交易根哈希、状态表根哈希等生成的数据作为value。

3. 将 <Key, value> 存储至kv数据库中。



交易的序列化具体步骤为:

1. 用区块头中的交易根哈希作为Key。

2. 序列化交易哈希、交易类型、交易数据和 MetaData 等生成的数据作为 value。

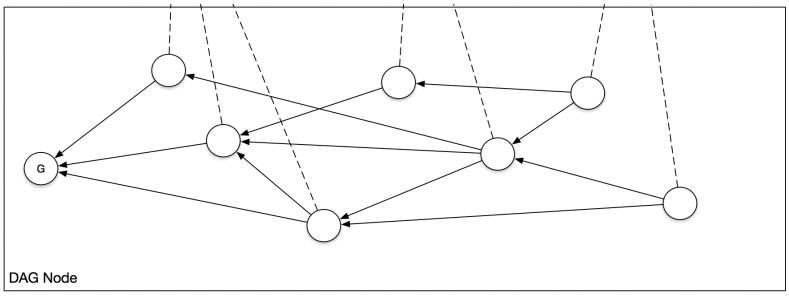
3. 将 <Key, value> 存储至 kv 数据库中。

2.5 DAG 数据结构

用户在向数据库添加数据时，该用户将创建一个新的存储单元并将其广播给他的对等节点。存储单元包括:

• 需要存储的数据。一个单元可以包括多个数据包，称之为信息。信息包括不同类型，具有各自的数据结构。其中一种信息类型是支付，用于向对等节点发送资产。

• 创建该单元的一个或多个用户的签名。用户由其地址标识。个人用户可以，并且鼓励拥有多个地址，地址源于公钥。



• 该单元的一个或多个先前的单元引用地址，由该单元哈希值标识。

引用单元决定了建立单元的次序，不局限于连续块之间的单引用关系，每个单元同时会关联多个父母单元和多个子单元。如果沿着父子链在块历史上前进，当同一单元被多个后来的单元引用时，将观察到许多分叉，并且当同一单元引用多个较早单元时，许多单元逐渐融合。这种结构在图论中称为有向无环图(DAG)。

如上图，连接成一个DAG存储单元。箭头是从子单元到父单元，G是创始单元，在新的单元极少到来这种特殊情况下，DAG将看起来几乎就像一个链，偶尔分叉而又快速融合。DAG中的每个新的子单元确认其父单元，以及父单元的所有父单元，向前以此类推。

2.6 文件系统

星际文件系统(IPFS，Inter Planetary File System)，是永久的、去中心化保存和共享文件的方法，是一种内容可寻址、版本化、点对点超媒体的分布式协议。

我们通过文件系统存储凭证文件。一些较大的数据内容以文件形式存储，并不存入区块链数据结构或是DAG数据结构中，每个文件都被进行Hash处理，生成数字指纹，区块链数据结构和DAG数据结构中只存储了文件的数字指纹。查找文件时，通过使用一个分布式哈希表，可以快速找到拥有数据的节点进行检索，并使用哈希验证其是否是正确的数据，找到想要的文件。通过网络删除重复具有相同哈希值的文件，通过计算是可以判断哪些文件是冗余重复的。并跟踪每个文件的版本历史记录。每个网络节点只存储它感兴趣的内容，以及一些索引信息，有助于弄清楚谁在存储什么。使

用称为去中心化命名系统，每个文件都可以被协作命名为易读的名字。通过搜索，就能很容易地找到想要查看的文件。

通过文件内容生成唯一哈希值来标识文件，而不是通过文件保存位置来标识。可追溯文件修改历史。通过P2P保存各种各样类型的数据。

2.7 委任权益证明

委任权益证明Delegated Proof of Stake(简称 DPoS)是比特股BitShares采用的区块链公识算法。在加密货币技术中，使用共识算法来保证整个区块链网络的安全可靠，著名的共识算法包括比特币网络使用的工作量证明PoW，以及Peercoin和NXT使用的权益证明PoS。但是，这些共识算法都不能解决交易性能问题，尤其是PoW算法大量消耗计算所需的电力。而委任权益证明DPoS很好地解决了性能和能耗的问题。

DPoS 算法中使用见证人机制(witness)解决中心化问题。总共有N个见证人对区块进行签名，而这些见证人由使用区块链网络的主体投票产生。由于使用了去中心化的投票机制，DPoS相比其他的系统更加民主化。DPoS并没有完全去除对于信任的要求，代表整个网络对区块进行签名的被信任主体在保护机制下确保行为正确而没有偏见。同时，每个被签名的区块都有先前区块被可信任节点签名的证明。DPoS消除了交易需要等待一定数量区块被非信任节点验证的时间消耗。

通过减少对确认的要求，DPoS算法大大提高了交易的速度。通过信任少量的诚信节点，可以去除区块签名过程中不必要的步骤。DPoS的区块比PoW或者PoW容纳更多的交易数量，从而使加密数字货币的交易速度接近中心化清算系统。

DPoS 系统任然存在中心化，但是这种中心化是受到控制的，因为每个客户端都有能力决定哪些节点可以被信任。DPoS使得这样的区块链网络保留了一些中心化系统的关键优势，同时又能保证一定的去中心化。系统通过公平选举，使每个人都有可能成为代表绝大多数用户的委托人。

DPoS 合理性逻辑:

1. 使权益所有者能够通过投票决定记账人
2. 最大化权益所有者的红利
3. 最小化保证网络安全的消耗
4. 最大化网络的性能
5. 最小化运行网络的成本

DPoS的根本特性是权益所有者保留了控制权，从而使系统去中心化。就像投票机制也有缺陷一样，DPoS是管理公司共有产权的唯一可行方式。幸运的是，如果你不喜欢运营公司的人，你可以通过卖出权益离场。而这种反馈机制可以使权益所有者在投票时比普通公民更加理性。

每个权益所有者可以通过投票去推选区块的签名验证者，任何一个拥有超过1%投票的人都可以参与到董事会。所有的代表构成一个“董事会”，轮流签署区块。如果一个董事错过了签署区块的机

会，客户会自动把投票给予其他人。这些错过签署机会的董事会最终被取消资格，其董事会位置会被其他合格候选人取代。董事会成员会收到少量代币作为奖励，用来激励在线时间和参与竞选。每一个董事必须要将单个区块平均奖励的100倍作为保证金，从而确保其至少99%的在线时间。

董事不随机从所有用户中选择的原因如下:

1. 普通用户无法保证充足在线时间。

2. 易受网络攻击，攻击者可以不经过其他人的认可使用其权益控制网络。

3. 普通用户由于没有挖矿，无法在去中心化网络中生成随机数。

假设每笔交易的确认成本和手续费都是固定的，那么实现去中心化的数量也是有限制的。假设验证成本与手续费相等，则整个网络是完全中心化的，并且只能支持一个验证节点。假设手续费是验证成本的100倍，则网络可以支持100个验证节点。

PoS 需要大量的手续费来保证其合理运行，而委任机制是PoS高效工作的唯一方式。在PoS中可以使用权益池的方式，但是这又变成某种形式的DPoS。委任代表无法从矿池张获得实际的收益，因为验证的花费将吞噬绝大部分的交易手续费。去中心化的成本与验证节点的数量成正比，而这个成本无法消除。从规模化角度看，这种成本的存在将最终使系统中心化，而委任代表制是唯一的解决方案。

委任代表的角色:

1. 委任代表是允许生成区块和广播区块的权威。

2. 生成区块的过程包括收集P2P网络中的交易并使用委任代表的私钥进行签名。

3. 委任代表的位置由上一个区块的最后部分随机指定。

DPoS 对于攻击的抑制:

1. 如果某个委任代表拒绝签署一个区块，那么他将被解职并失去未来的稳定预期收入。
2. 不诚实的委任代表只有在明确有其他利益诉求时才会选择放弃区块生成。
3. 委任代表无法签署无效的交易，因为交易需要所有委任代表的确认。

委任代表的数量由权益所有者确定，至少需要11个委任代表。比特股(bitshares)和steem采用的DPoS 机制是持股者投票选出一定数量的委任代表，每个委任代表按序有两秒的权限 时间生成区块。若委任代表在给定的时间片不能生成区块，区块生成权将交给下一个时间片对应的委任代表。

持股人可以随时通过投票更换委任代表。这种设计使得区块的生成更为快速，也更加高效与节能。大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

2.8 DAG 共识

如果尝试编辑一个单元，必须会改变它的哈希值，这将破坏所有引用此单元哈希值的子单元，因为子节点的签名和哈希值取决于父哈希值。因此，子单元们不能在没有与父单元协调的情况下修改他们的单元。一旦一个单元被广播到网络中，并且其他用户开始在它上面构建它们的单元 (将其称为子单元)，编辑这个单元所需的二次修改数据就会增长。

与需要大量计算工作的比特币不同，如果尝试修改过去的交易信息，需要与大量相关联其的他用户协调，其中大多数是匿名的陌生人。因此，过去记录的不变性是基于与如此大量的陌生人协调的复杂性，这些单元难以达成一致，因为单元可能不想进行更新修改或者反对 相应的修订。

通过引用其父单元，一个单元将关联其父单元，虽然该单元不包括父母单元的全部内容。该单元的内容取决于其父母单元的哈希值。同样，单元也间接依赖于父节点的父节点，以此类推，每个单元也依赖于最初的创世单元。

协议规则，一个单元不能引用冗余的父单元。例如，如果单元B引用单元A，则单元C不能同时引用单元A和B。因为A已经作为B的父节点被B引用。该规则要求不能向DAG中添加任何不必要的冗余链接。

为了防止无用信息频繁写入数据库引起的效率下降，DAG引入入又的屏障，基于用户的存储效用和网络的存储成本。对于这两者而言最简单的测量方法是测量存储单元的大小。因此，要将数据存储在去中心化的全球数据库中。

为了使激励措施与网络的利益保持一致，在大大小小的计算规则中存在一个例外。为了计算单元大小，假定单元就恰好具有两个父单元，不论真实数字。因此，两个父单元的哈希值的大小总是包含在单元大小中。此例外确保用户不会为了尽量降低成本，而尝试只包含一个父单元，因为无论包含多少父单元，这成本都是相同的。

为了使DAG尽可能地精确，尽可能多地包含父单元，如前所述，这不会对应付的大小产生负面影响。并且尽可能地通过那些最初作为父单元将其包含的单元费用的支付部分成为最近的父单元。

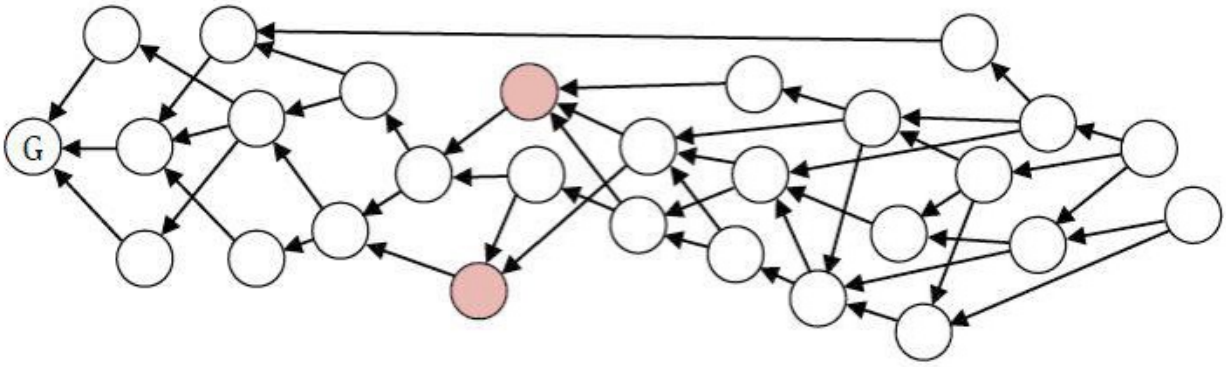
支付一定存储费用作为DAG节点的简历，也称为佣金。佣金可以发送给其他用户支付商品或服务或换取其他资产。

2.9 双重支付（也称双花）

如果用户尝试使用两次相同的输出交易，有两种可能的情况:

1、两个相同输出交易的两个单元是有顺序的，即一个单元直接或间接被另一个单元引用。在这种情况下，我们显然可以安全地拒绝后面单元的输出交易。

2、若两个单元之间是无序的关系，在这种情况下，两个输出交易都被接受，但两个交易也被包含在后面新增的单元里。在我们建立单元之间的总序后，在总序较早出现的一方单元的有效交易视为有效，另一单元交易视为无效。



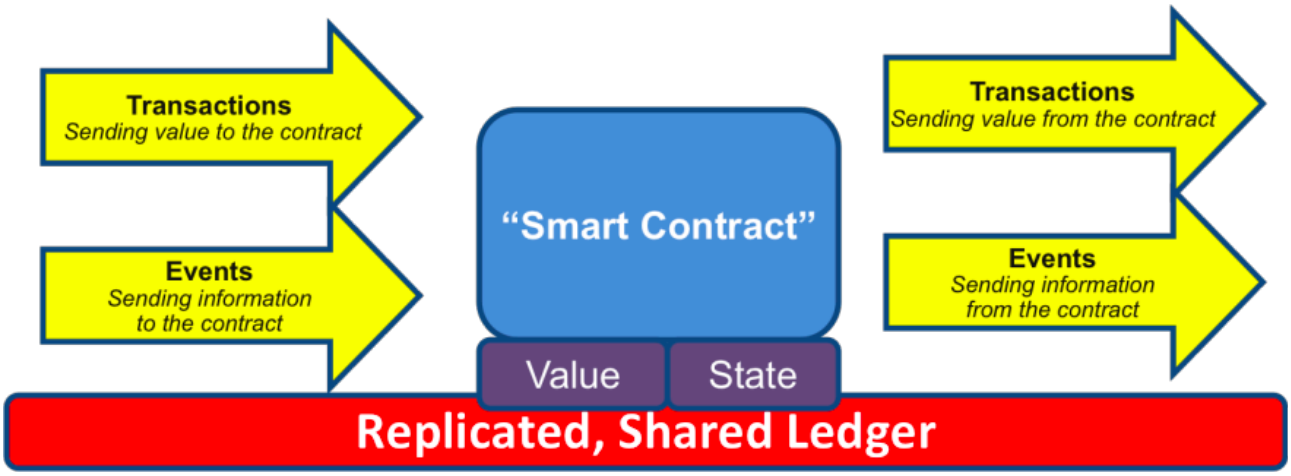
有一个简化定义总序的协议规则。如果相同的地址发布超过一个单元，则它应当直接或间接地在每个后续单元中包含其所有先前单元，即来自相同地址的连续单元之间应当有序。换句话说，从同一作者发布的所有单元应连续。

如果有人违反这一规定并发布两个单元，使得它们无序(非序列单元)，则这两个单元被视为双重支付，即使它们没有尝试使用相同的输出。这种非系列单元如上面情况2所述处理。

如果用户遵循这个规则，但仍尝试两次花费相同的输出，则这种双重支付变得容易辨别与确认，并且我们可以安全地拒绝两次花费中偏后的那个一个花费交易，如上面情况1所示。因此，系统很容易会滤掉非序列的双重支付。

这是一个巧妙的规则设计。当用户组成一个新的单元时，他选择最近的另一个单元作为其单元的父单元。通过把他们列在他的父名单上，并向外宣布，这意味着他已经看到了这些单元。因此，他看到了父单元里的所有父单元，父单元的父单元等等，直到创世块。这个巨大的集合同时包括在该单元的子单元，并且对该单元可见。

2.10 智能合约



智能合约是1990年代由尼克萨博提出的理念，几乎与互联网同龄。由于缺少可信的执行环境，智能合约并没有被应用到实际产业中，自比特币诞生后，人们认识到比特币的底层技术区块链可以为智能合约提供可信的执行环境，而本项目一直致力于打造最佳的智能合约平台。

智能合约程序不只是一个可以自动执行的计算机程序，它本身就是一个系统参与者。它对接收到的信息进行回应，可以接收和储存价值，也可以向外发送信息和价值。这个程序就像一个可以被信任的专家，可以保管临时资产，并按照已设定的规则执行操作。

这个示意图为一个智能合约模型：代码（智能合约）被部署在可分享的、复制的账本上，它可以维持自己的状态，控制自己的资产并对接收到的外界信息或者资产进行回应。

智能合约模型：它是运行在可复制、共享的账本上的计算机程序，可以处理信息，接收、储存和发送价值。

BAIC项目借鉴了比特币区块链技术，对它的应用范围进行了扩展。如果说比特币是利用区块链技术的专用计算器，那么BAIC就是利用区块链技术的通用计算机。简单地讲，BAIC=区块链+智能合约。与比特币相比，BAIC最大的不同点是：它可以支持更加强大的脚本语言（用技术语言讲就是图灵完备的脚本语言），允许开发者在上面开发任意应用，实现任意智能合约。

2.11 挖矿机制

客户端程序将交易请求提交到IOTA节点，IOTA节点将交易保存到DAG数据结构上，产生新的单元。将全新的单元将挂在多个已有单元上的IOTA节点的带交易手续费作为奖励。尝试进行交易合法性验证的IOTA节点也会得到一些IOTA币作为验证确认奖励。在这个过程中，IOTA节点为客户端提供了网络、验证、磁盘存储空间服务，因此提交交易者需要额外支付一些IOTA币作为手续费给IOTA节点。

IOTA节点将确认通过的交易数据提交到区块链节点中，区块链节点就像比特币的挖矿机制，把IOTA节点提交上来的尚未记录的交易打包到一个区块，使区块链上产生新的区块，并在区块链网络中广播出去，全网其他区块链节点验证该区块里的交易数据符合协议规范后，各自把该区块链接到自己版本的区块链上，从而在全网形成对当前网络状态的共识。

2.12 抗攻击

创世区块有向无环链具有双重验证确认机制，交易在IOTA节点中使用DAG数据结构快速验证并确认交易，在一段时间之后（每隔一定时间间隔后，如30分钟）将DAG中已经确认的交易同步到区块链节点，交易将在区块链上进行再次的验证与确认，如果发生非法交易，IOTA节点上的DAG交易数据将会被回滚到正确的数据。换言之，IOTA节点最终以区块链上最终验证确认的数据为准。同时，区块链也起到收缩、聚拢DAG的数据结构的作用，使之不会不断的扩散下去，产生无数的连接脆弱的小片区域。

如果要策划和开展攻击，需要找众多IOTA币爱好者，让他们用自己的钱包发送交易，而这是不可能的。攻击者也不大可能控制一群“肉鸡钱包”做DDOS。如果能控制肉鸡钱包，攻击者就已经取得IOTA币的巨大财富，也不会去以黑客非法手段来盈利。所以只剩下自己买币，然后不停地发送交易

到自己的小号钱包地址对。而发出去的小额IOTA币还需要交一笔交易手续费（矿工费），因此如果有人发起这样的攻击，最大的可能是导致大量交易积压，被迫让真实交易者提高矿工费价格，或者选择暂缓交易，等待网络缓解。待网络上的交易都处理完毕了，攻击者发现自己得到了一堆小额的钱包。DOS的本质是区块拥堵，只会加速社区对网络承载能力的提升速度。

2.13 核心代码

马尔可夫链蒙特卡罗(Markov Chain Monte Carlo, MCMC)方法

对于一个给定的概率分布P(X)，若是要得到其样本，通过上述的马尔可夫链的概念，我们可以构造一个转移矩阵为P的马尔可夫链，使得该马尔可夫链的平稳分布为P(X)，这样，无论其初始状态为何值，假设记为X0，那么随着马尔科夫过程的转移，得到了一系列的状态值，如：X0，X1，X2…，Xn，Xn+1,…，如果这个马尔可夫过程在第n步时已经收敛，那么分布P(X)的样本即为Xn，Xn+1,…

```
Hash transactionToApprove(final Set<Hash> visitedHashes, final Map<Hash, Long> diff, final Hash reference, final Hash extraTip, int

    long startTime = System.nanoTime();
    if(depth > maxDepth) {
        depth = maxDepth;
    }

    if(milestone.latestSolidSubtangleMilestoneIndex > Milestone.MILESTONE_START_INDEX ||
            milestone.latestMilestoneIndex == Milestone.MILESTONE_START_INDEX) {

        Map<Hash, Long> ratings = new HashMap<>();
        Set<Hash> analyzedTips = new HashSet<>();
        Set<Hash> maxDepthOk = new HashSet<>();
        try {
            Hash tip = entryPoint(reference, extraTip, depth);
            serialUpdateRatings(visitedHashes, tip, ratings, analyzedTips, extraTip);
            analyzedTips.clear();
            if (ledgerValidator.updateDiff(visitedHashes, diff, tip)) {
                return markovChainMonteCarlo(visitedHashes, diff, tip, extraTip, ratings, iterations, milestone.latestSolidSubtangl
            } else {
                throw new RuntimeException("starting tip failed consistency check: " + tip.toString());
            }
        } catch (Exception e) {
            e.printStackTrace();
            log.error("Encountered error: " + e.getLocalizedMessage());
            throw e;
        } finally {
            API.incEllapsedTime_getTxToApprove(System.nanoTime() - startTime);
        }
    }
    return null;
}


Hash markovChainMonteCarlo(final Set<Hash> visitedHashes, final Map<Hash, Long> diff, final Hash tip, final Hash extraTip, final Map<
    Map<Hash, Integer> monteCarloIntegrations = new HashMap<>();
    Hash tail;
    for(int i = iterations; i-- > 0; ) {
        tail = randomWalk(visitedHashes, diff, tip, extraTip, ratings, maxDepth, maxDepthOk, seed);
        if(monteCarloIntegrations.containsKey(tail)) {
            monteCarloIntegrations.put(tail, monteCarloIntegrations.get(tail) + 1);
        } else {
            monteCarloIntegrations.put(tail,1);
        }
    }
    return monteCarloIntegrations.entrySet().stream().reduce((a, b) -> {
        if (a.getValue() > b.getValue()) {
            return a;
        } else if (a.getValue() < b.getValue()) {
            return b;
        } else if (seed.nextBoolean()) {
            return a;
        } else {
            return b;
        }
    }).map(Map.Entry::getKey).orElse(null);
}
```

CURL三元哈希算法

三进制算法，由 Keccak (SHA-3) 的发明者设计。Curl 被设计用于 IoT 设备，也是世界上第一个三进制哈希算法。代码实现如下。

```
public class Curl implements Sponge {

    public static final int NUMBER_OF_ROUNDSP81 = 81;
    public static final int NUMBER_OF_ROUNDSP27 = 27;
    private final int numberOfRounds;
    private static final int STATE_LENGTH = 3 * HASH_LENGTH;
    private static final int HALF_LENGTH = 364;

    private static final int[] TRUTH_TABLE = {1, 0, -1, 2, 1, -1, 0, 2, -1, 1, 0};
    private static final IntPair[] TRANSFORM_INDICES = IntStream.range(0, STATE_LENGTH)

    private final int[] state;
    private final long[] stateLow;
    private final long[] stateHigh;

    private final int[] scratchpad = new int[STATE_LENGTH];


    protected Curl(SpongeFactory.Mode mode) {

    public Curl(boolean pair, SpongeFactory.Mode mode) {

    private void setMode(SpongeFactory.Mode mode) {

    }

    public void absorb(final int[] trits, int offset, int length) {


    public void squeeze(final int[] trits, int offset, int length) {

    private void transform() {

        int scratchpadIndex = 0;
        int prev_scratchpadIndex = 0;
        for (int round = 0; round < numberOfRounds; round++) {
            System.arraycopy(state, 0, scratchpad, 0, STATE_LENGTH);
            for (int stateIndex = 0; stateIndex < STATE_LENGTH; stateIndex++) {
                prev_scratchpadIndex = scratchpadIndex;
                if (scratchpadIndex < 365) {
                    scratchpadIndex += 364;
                } else {
                    scratchpadIndex += -365;
```

```
private void pairTransform() {
    final long[] curlScratchpadLow = new long[STATE_LENGTH];
    final long[] curlScratchpadHigh = new long[STATE_LENGTH];
    int curlScratchpadIndex = 0;
    for (int round = numberOfRounds; round-- > 0; ) {
        System.arraycopy(stateLow, 0, curlScratchpadLow, 0, STATE_LENGTH);
        System.arraycopy(stateHigh, 0, curlScratchpadHigh, 0, STATE_LENGTH);
        for (int curlStateIndex = 0; curlStateIndex < STATE_LENGTH; curlStateIndex++) {
            final long alpha = curlScratchpadLow[curlScratchpadIndex];
            final long beta = curlScratchpadHigh[curlScratchpadIndex];
            final long gamma = curlScratchpadHigh[curlScratchpadIndex += (curlScratchpadIndex < 365 ? 364 : -365)];
            final long delta = (alpha | (~gamma)) & (curlScratchpadLow[curlScratchpadIndex] ^ beta);
            stateLow[curlStateIndex] = ~delta;
            stateHigh[curlStateIndex] = (alpha ^ gamma) | delta;
        }
    }
}

public void absorb(final Pair<long[], long[]> pair, int offset, int length) {
    int o = offset, l = length, i = 0;
    do {
        System.arraycopy(pair.low, o, stateLow, 0, l < HASH_LENGTH ? l : HASH_LENGTH);
        System.arraycopy(pair.hi, o, stateHigh, 0, l < HASH_LENGTH ? l : HASH_LENGTH);
        pairTransform();
        o += HASH_LENGTH;
    } while ((l -= HASH_LENGTH) > 0);
}

public Pair<long[], long[]> squeeze(Pair<long[], long[]> pair, int offset, int length) {
    int o = offset, l = length, i = 0;
    long[] low = pair.low;
    long[] hi = pair.hi;
    do {
        System.arraycopy(stateLow, 0, low, o, l < HASH_LENGTH ? l : HASH_LENGTH);
        System.arraycopy(stateHigh, 0, hi, o, l < HASH_LENGTH ? l : HASH_LENGTH);
        pairTransform();
        o += HASH_LENGTH;
    } while ((l -= HASH_LENGTH) > 0);
    return new Pair<>(low, hi);
}
```

第三章 BAIC物联网价值链的应用场景

3.1 智能家庭AI机器人平台

家庭AI机器人，是BAIC将物联网及区块链技术进入实际落地应用的关键产品，也是BAIC去中心化网络的核心节点。目前BAIC基金会与知名AI服务商IMIO Labs合作，在其广受好评的家庭智能语音网关产品上，共同开发全球第一款应用区块链技术，拥有智能合约，并可以自动结算的家庭用AI机器人产品。

IMIO Circle 智能语音网关

参数：

操作系统：Linux 64位
处理器：ARM QUAL Cortex A7 主频 1.0GHz
内存: 256MB DDR3
固态硬盘: 4GB EMMC Flash
网络: 蓝牙 wifi 一体 AP6212 wifi/BT/FM，支持 4.0
物联网网关： TI ZigBee 2.0
麦克风 阵列 支持 3-5 米远场语音交互操作功能 喇叭 全频喇叭

IMIO Circle 支持国际标准ZigBee 2.0协议，及其所兼容的产品，例如Philip Hue智能灯泡系列、智能开关、智能门锁、智能插座、智能窗帘等等。可以实现语音方式绑定设备、语音方式控制家电等实用功能，同时也可以将家中的智能家居和家电产品接入统一的智能平台，将信息孤岛数据整合后汇总，以去中心化的方式进行交互和分析。Circle自带的语音助手，妙琦管家，也可以像助手一样和人对话，并拥有丰富的AI skills。同时，AI管家也可以学习记录人们的自然生活方式。这样的AI服务与智能硬件整合模式，还是一个的蓝海市场。

产品演示视频网址

http://baic.io

IMIO Circle Show 家庭智能机器人

参数：

显示：8寸高清液晶屏（1200:800）
处理器：MTK 8735 四核处理器
物联网网关: Zigbee 3.0、红外、蓝牙 4.0
摄像头：1080P高清摄像头
麦克风阵列：4麦 麦克风阵列，拾音距离5米

音箱：2*5W高保真喇叭

其他功能：温湿度传感器、4G模块（选配）、NFC模块（选配）

Circle Show AI机器人是BAIC开源社区与IMIO Labs联手打造，是未来智能家庭真正入口的第一代产品。除了拥有Circle 语音网关全部的物联网及AI功能外，添加了BAIC的物联网价值链的智能合约系统，目前支持的合约有：

- 开机后作为BAIC社区的中心节点之一，提供交易验证算力，并获得相应奖励
- 如果以网关方式接入更多智能家居设备，如智能开关等，接入越多，则算力越强，奖励越多
- 广告播放补偿合约，如果用户在观看广告过程中，通过语音或触摸方式与广告进行互动，则获得广告商预先设定的代币奖励
- 数据交易合约，用户如果愿意分享自己的数据，包括房间温湿度、生活习惯、爱好等等非隐私的信息，如果有买家接受的话，将自动与设备结算，给用户奖励代币。

IMIO Circle Show 作为一个能看能听能说能想能执行的智能助手，可以分析家庭场景中人物的动作、表情、人脸识别，进行陌生人入侵检测识别，还可以主动和陌生人进行语音交互，实现家庭安防的AI升级至主动防御和全面及时的应急反应。同时，Circle Show还可以接受主人的语音指令，管理家中的各个智能家居设备，更可以自动学习用户的生活习惯，融入用户生活，实现润物细无声般实现自然的生活体验。在未来的计划中，AI机器人还将在远程医疗、儿童教育、智能养老等更多家用场景大展身手，为用户带来真正AI时代智能管家服务体验。

IMIO Circle Show预计售价999元，并于3月开始预售，4月开始发货小批量试用。

BAIC AI机器人的未来

除了与IMIO Labs合作，BAIC开源社区还将和全球更多的AI应用公司、智能硬件、机器人公司合作，陆续推出各个家庭生活应用场景的机器人套装，配合BAIC的价值链服务，形成一个基于家庭环境AI应用的运行平台，帮助第三方的AI及内容公司进行分发获得代币，同时也可以不断的提供更丰富的数据进行进一步交易，形成最终的家庭AI与物联网生态平台优势。并随着未来VR、AR、生物机械技术的融合，最终实现真正的拟人Jarvis AI管家，是BAIC最终的智能家庭愿景和目标。

3.2 AI硬件智能合约平台

智能合约平台是BAIC公链的基础也是最核心的应用平台。基于智能合约，设备、对象、数据、逻辑方法、凭证等可以完美的在BAIC公链上进行组织和执行，并为BAIC其他应用提供运行的环境和解释系统。BAIC的智能合约平台包括有丰富的应用类型，并为满足不同的物联网及AI环境场景下应用进行优化，目前设定的智能合约类型有：

1. 主控类合约

A. 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；并且事务的状态处理和保存都在区块链上完成。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将会更新，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。

B. 特色：全球首家区块链平台将物联网设备智能合约投入实用场景中

C. 举例：去中心化智能租房案例

- 某租房房东，采用BAIC去中心化的租房方案，将门锁替换成支持BAIC智能合约的门锁，并在区块链模式的租房网站发起租房信息，拟定租房合约，例如，租房免押金，租金每月定时扣XX币，逾期门锁自动换密码；看房时在网上进行预约，预约成功暂扣1个月房租，并将则1小时有效门锁密码发送到租客手机，租客凭借密码在一个小时内看房，如果不满意，则直接走人，一个小时后密码重置；如果看房成功，则租房智能合约生效，扣除租房房租，并将门锁密码设置成租客专用。在整个租房过程中，不需要中介陪同，无需信用认可，节省了大量的人力物力。

2. 数据结算合约

A. 数据结算合约用于物联网设备或其他可以提供数据的产品上，由设备拥有方拟定可以开放分享的数据内容，并提供数据接口，数据需求方可以按照约定的价格和方式，按照数据接口定时获取数据，并自动完成结算。结算的代币，将直接转入拥有方的账户，并且可以支持超小额支付。

B. 特色：

- 支持多种不同的数据类型，以及多样化物联网设备的数据采集
- 支持超小额支付，满足数据碎片化的交易需求
- 支持超低手续费交易，方便小额支付

C. 举例：用户利用行车数据进行交易

- 用户小A刚刚购买了一辆带有数据交易、智能合约的新小轿车，并且每天使用。根据智能合约内容，只要小A同意将行车数据，包括驾驶习惯，地理轨迹，车辆信息等以匿名的方式进行分享，这些数据将被用来分析车辆驾驶者的驾驶习惯，完成司机用户的画像分析，帮助厂商的无人驾驶AI完善驾驶模型，并且广告厂商也可根据数据有所侧重地分析定位用户的喜好，并在车载设备里进行了精准广告投放，作为回报，小A获得了代币，可以用代币在4S店冲抵保养费用，或者在支持的加油站自动加油结算。

3. 算力验证合约

- 算力验证合约是BAIC社区核心运行机制，通过算力验证模型，BAIC让每一个连入网络的物联网设备及AI机器人自动成为BAIC的矿机，并利用其节点作用进行交易和运算验证。并基于验证数量，获得手续费。由于采用DAG技术，BAIC的算力验证基于存储数据量及连接数量来完成，避免了算力浪费。

- 特色

  - 采用DAG技术，算力基础为数据存储及链接数量
  - 支持收取手续费，为矿机提供动机
  - 基础算力支持物联网设备及嵌入式运行环境

- 举例：IMIO Circle Show AI机器人成为中心节点

  - IMIO Circle Show AI机器人在家庭使用的时候，每一个都成为了BAIC网络的中心节点，实现了验证算力及数据存储功能。通过连接了更多的物联网设备，存储的数据数量越大，算力验证能力越强。由此，Circle Show为其主人提供了挖矿获得代币的能力，持续创造财富。

4. AIaaS合约

- AIaaS 合约的特点是让BAIC可以在区块链上建立一个分布式AI平台，具有AI识别能力的区块链节点提供AI算法的API，AI研究人员和开发者可以将自己的AI算法分发给BAIC的用户，用户需使用代币支付相应的服务费用。例如图像识别、机器翻译等算法，通过区块链连接起来，便于不同的AI Skills 相互沟通，甚至合作。比如说智能翻译应用在翻译一个文档的时候遇到了一张图片，它就可以自动请求一个计算机视觉程序来识别它。

- 特色

  - AI应用以API方式存在，供全区块链用户索取或调用，并为此付费
  - AI应用可以由任何公司开发，并在BAIC数据交易平台上发现
  - AI应用的数据来源，也可以由BAIC网络提供

- 案例：人脸识别API

  - IMIO Circle Show AI机器人，支持调用人脸识别API作为家庭安全的重要部分。当AI机器人处于家庭安全预警模式下工作的时候，如果遇到陌生人入侵，AI机器人通过人脸识别判断并不是家人的时候，可以申请调用第三方公司提供的安全人脸识别API。本API接通了安全部门的数据库，拥有全部有犯罪前科的人员人脸记录。通过比对信息，可以判断当前潜入陌生人是否为不安全记录的人员，从而提升了家庭安全等级和犯罪预测能力。用户只需要在实际使用时付费给API即可，不用时不付费。

5. 账本类型合约

- BAIC的区块链技术也可以用去中心化账本功能来创建、确认、转移各种不同类型的资产及合约。包括数字股票、私募股权、众筹、债券和其他类型的金融衍生品。这些形式，可以被用来做BAIC的智能硬件孵化器平台，供智能硬件或AI公司基于BAIC来发行众筹项目或融资手段，并利用BAIC的完整区块链技术和数据体系，实现更丰富类型的智能账本合约。

- 特色：

  - 专为智能硬件及AI类公司设计，帮助其产品上链
  - 提供从数字股权、数字项目分成到数字债券等多种丰富的合约内容
  - 提供用户、数据、API等多种上下游资源给参与孵化的智能硬件企业

- 案例

  - 某智能硬件公司产品及业务和区块链关系不大，不方便直接用以太坊的模式发行代币融资。利用BAIC的智能硬件合约，可以直接基于硬件产品进行项目众筹，所有的参与用户可以利用智能合约，享受到未来硬件产品成功销售后的分成。因为每一个智能硬件都在BAIC的链上，因此厂商无法造假，必须按照智能合约给参与众筹的用户进行代币结算，保障参与者获得收益。

3.3 AI物联网数据交易平台

BAIC数据交易平台是BAIC积分代币系统流通的重要基础平台。在此平台上，设备厂商可以建立采集数据、销售数据的渠道，并增加设备的获益功能，以吸引更多的用户购买；设备用户，可以通过此渠道提供个人数据以获取收益；数据购买方，如广告主，也可以利用此平台精准定位用户，获取用户画像数据，并以更低的价格高效的达到传播目的。

BAIC的数据交易平台目前包括以下3个核心模块

- 智适应广告传播平台
- 物联网数据交易中心
- AIaaS交易中心

智适应广告传播平台

对于广告主而言，目标用户的一个核心概念是“用户画像”（personal profile）：指的是个人的年龄、性别、行为、性格、趋势等，简而言之就是你是个什么样的人，这对于广告的“差异化受众“来说

是一个很关键的区分标准。在互联网出现以前，个用户画像产生非常缓慢，而随着互联网尤其是移动互联网的兴起，个人数据突然间以一种可轻易分享和复制的方式进入了全球互联网。个人画像变成日益壮大的数据海洋，为许多人所用。广告技术的前景本应当是创造一个更高效、更透明的市场，将广告与目标消费者匹配。数字技术也应当使广告主及目标市场之间的交易流变得更容易追踪，并确保信息到达目标消费群体。然而，经过二十年的发展而形成的广告技术生态系统却充斥着各式中介和复杂交易，令人迷惑。广告主则因为虚假数据、不精准数据，损失了数以十亿计的收入，欺诈甚嚣尘上。广告主还深受反馈不到位和投放精准度不足之苦。毫无疑问，这一切都需要一个良好的解决方案。

智适应广告播放平台，则是基于物联网与AI时代的一个突破性服务模式，重点解决了中心化广告传播与投放的种种问题。首先可以让广告主以去中间商的模式，直接将广告投放到用户面前。AI机器人、物联网电视、冰箱、汽车等等，都可以成为传播媒介，精准而高效。其次，广告主对目标用户的筛选也变的非常高效。由于BAIC平台可以将参与数据交易的个人生活有关的各种数据进行采集和分析，远远不止手机和浏览器搜索关键词这一单一维度。对用户画像的精准性大增，甚至可以做到在用户喝啤酒的时候由AI机器人推荐炸鸡翅。一方面满足了用户精准需求，另一方面也让广告主投放传播效率更高。

物联网数据交易中心

物联网数据交易中心，也是为了适应AI时代的需求而建立。AI发展日益成熟，对数据的要求也越来越高，越来越广泛，而众多物联网设备刚好为各个AI应用深度学习训练，提供了多维度持续性的的数据感知。例如环境信息、行为信息、语音信息、动作信息、交通信息、图像信息等等。BAIC的物联网体系，刚好满足了这一纷繁复杂的数据网络需求。BAIC的代币结算系统，又为这一数据的交换与分享，提供了利益动机，并通过自由交易定义了消费者数据的价值。BAIC的去中心化式账本，又保证了数据不可修改和可追溯性（Tracebility），确保消费者数据的真实可靠。

数据安全性及对隐私的保护

作为数据分享和交易平台，数据的安全性和消费者隐私尤为重要。BAIC采用的链本身具备不可篡改性。公开交易信息和DAG（有向无环图）本身的交易确认方式确保了用户的交易可确定性安全。不管是公开BAIC还是私密BAIC，其交易的唯一性和确定性都将会被保障，并且不可篡改。此外，用户如希望在链上应用存储数据，将可以自由选择加密方式，加密安全性取决于选择加密的算法和强度。同样，其唯一性和确定性也会被保障，并且一旦应用交易成功写入，也将不可篡改。

消费者的隐私也是BAIC去中心化平台考虑的重中之重，除了采用分布式存储，降低单个设备被入侵的风险，并采用苛刻的数据加密手段以外。所有的对外分享的数据，都可以消费者自己设定分享权限，也可以完全封闭。此外分享的数据也将消费者个人隐私信息，包括ID、姓名、详细住址等等进行严密保护，并未对外分享，也不能和已有数据进行关联。确保进行交易的数据，只是基于大众行为的画像，而不是某一个具体消费者的全面信息。

AIaaS 交易中心

AIaaS是AI API as a service的缩写，也是新一代AI应用服务的类型。类似SaaS服务，也是指企业将AI的算法作为一种API的接口，对外部公司开放。这样第三方的智能硬件或软件公司，在需要的时候可以直接调用此AI服务，按次按量收费，而不需要各家公司自行研发AI应用，节省了第三方公司大量的技术研发投入。尤其是物联网设备和智能硬件产品，在涉及语音识别、语义理解、图像及视频理解的使用场景的时候，直接按次按使用量付费即可。甚至这部分费用也可以由设备使用者来负担，而降低了硬件制造公司的成本负担。这一经济体系和结算流程，在中心化的法币体系下，很难实现。但如果基于去中心化的积分代币体系，例如BAIC的价值链系统下，可以很轻松的解决。每个设备都可以自行和第三方设备和服务商自动结算，在消费者认可该智能合约的条件下，消费者可以买单，而不用厂商整体付费。毫无疑问，这将对AI应用的普及和传统硬件公司的AI化起到深远的影响。

BAIC的AIaaS平台，也将与IMIO Labs等全球著名AI应用服务公司合作，将语音识别、各个垂直领域的图像分析、人脸识别、语义理解引擎等AI应用上链，让所有接入BAIC的智能硬件和物联网设备，也同时具备AI能力，为未来的全面生活智能化奠定基础。

3.4 AI硬件金融服务平台

针对硬件厂商的金融服务平台是BAIC物联网价值链的最后一环。通过采用区块链去中心化账本技术，被孵化的硬件企业可以在BAIC的公链上创建、确认、转移各种不同类型的资产及合约，包括数字股票、私募股权、众筹、债券和其他类型的金融衍生品。这些形式，都可以被智能硬件或AI公司用来做发布众筹项目或为产品项目融资。BAIC也将维护一群全球对AI及智能硬件热衷的币友，建立BAIC AI硬件玩家社群，为孵化智能硬件项目提供全力支持。

除了基本的账本服务外，BAIC还提供了完善的数据链支持以及物联网硬件智能合约支持。这也是BAIC区别于目前的第二代区块链基础平台，以太坊、IOTA的重要地方。传统硬件产品想要物联网化，AI化，关键是需要：

1、物联网通讯芯片

2、基于AI应用的多智能硬件联动及数据支持

BAIC支持常见的ZigBee、Zwave、NB-IOT、蓝牙4.0等物联网协议，并和多家物联网模块公司已经推出了支持BAIC物联网价值链的通讯芯片，例如中国最大的ZigBee芯片公司，飞比、顺舟、雍敏等等，都有已经支持BAIC的终端模组，而且价格低廉，配合IMIO Circle或IMIO Circle Show 网关功能，可以做到“一芯入网”，轻松将各种传统小家电、电器、电子产品接入庞大的物联网体系。

不仅仅是完成入网，BAIC还将提供以家庭为单位的各种电器数据和接口联动，方便智能硬件产品之间联动。举例来说，当消费者早上起床时，只要轻松的对AI管家说一句，我起床了，那么该场景下的智能窗帘自动拉开，咖啡机开始工作，卫生间开始准备热水等等。如果某个孵化的智能硬件

项目，需要借助其他设备的数据或联动，可以达到更好的使用体验，那么BAIC的物联网价值链刚好可以完美的满足这一需求。

BAIC的金融服务平台、智能合约系统、数据交易平台三大板块，加上家庭AI机器人入口，3+1模式融合在一起，从生态价值链的角度为AI及智能硬件企业提供了融资、产品研发、产品上网、产品分发、产品获益等一条龙解决方案，帮助传统硬件和家电企业快速上链，通过去中心化物联网模式快速获得用户并提升用户体验。这三大系统和一个核心产品，也是BAIC区分于其他公链平台的关键，BAIC更注重落地，更注重应用，更注重用户实际应用区块链技术的反馈。我们有理由相信，BAIC将引领区块链技术走向更加实用的未来。

第四章 BAIC社区基金会的管理架构

4.1 BAIC社区基金会的设立

基于BAIC社区的国际化定位和影响力，BAIC Community Foundation BAIC社区基金会（以下简称基金会）是一家总部设立在新加坡的非营利组织。基金会致力于BAIC开源社区的维护运营，以及物联网价值链的公链平台开发，发展，建设，倡导透明治理和DAO模式的管理，让BAIC社区真正归属全体AI及物联网价值链的参与者爱好者，并促进开源生态社会的安全与和谐发展。

4.2 BAIC基金会的治理架构

BAIC社区基金会治理架构包含了针对日常工作和特殊情况的操作流程和规则。BAIC推崇自然去中心化的DAO治理模式，认为所有BAIC项目参与者，都是BAIC基金会的组织成员及天然员工，共同享有BAIC的发展价值，以及共同决策权。BAIC的重大事项，均有全体成员共同投票决定，发展与决策议题，BAIC的参与者，也可以随时组织追随者共同发起。

首届BAIC基金会决策委员会由核心创始成员组成，一共5人，任期为4年，核心创始成员在区块链领域中具有丰富的行业经验。任期满后由社区根据持有BAIC有链数字资产的持有份额和资产龄计算权重，选举50名社区代表，再最终选举产生5位决策委员会成员。

4.3 BAIC基金会的交易安全及审计

BAIC的交易安全

BAIC公有链通过区块链共识、智能合约等技术以及数字签名、终端用户加密钱包等安全手段确保用户账户及资金安全;

BAIC 公有链提供金融级安全的数据存储、网络、平台等资源的高效整合，将数据、应用、交易集成到区块链云中，构建安全交易网络环境。

与最受信任的交易平台和技术专家共同构建安全交易。

审计

BAIC 社区基金会投委会将保持高标准的诚信和道德的商业行为标准；遵守相关的法律法规及行业自律原则;

BAIC 公有链每年会邀请国际知名第三方审计机构对 BAIC 公有链基金会的资金使用、成本支出、利润分配等定期进行审计和评估;

BAIC 公有链将毫无保留公开发布第三方机构评估和审核结果。

第五章 BAIC核心团队和专家顾问

谈毅 创始人

著名互联网创业企业家，AI企业 IMIO Labs 创始人，IEEE Smart Home工作组主席。曾创立中国最大安卓开发者社区“机锋网”并成功退出，创立中国第一个硬件社区“飞翔鸟硬件站”，创立中国最早网游公司“网星艾尼克斯”。美国南加州大学(USC) MBA毕业。

Amy Yuan 首席科学家

斯坦福大学计算物理学博士后，美国知名数据科学家，美国国家科学基金会(NSF)研究员。师从世界计算物理第一人Jens Norskov，曾打破世界分布式计算记录，对数据加密学有深入研究。YCombinator 2017 创业冠军，曾获得硅谷著名天使投资人Peter Thiel (PayPal创始人) 和Mark Pinkus (Zynga创始人) 天使投资。还获得美国USC大学计算机科学硕士及博士学位。

Jack Zheng 联合创始人

知名互联网技术专家，Linux开源基金会成员，智能硬件极客组织成员，人工智能学会成员。曾担任红帽子Red Hat资深云端架构师、互联网公司CTO、首都在线263 首席技术顾问等职位。毕业于西南科技大学计算机专业。

Marvin Wu 首席战略师

近十年来致力于前沿技术在美国和欧洲市场的商业化战略研究，包括区块链技术、AI深脑模拟，视力再造等科技领域。曾就职于波士顿科学、戴尔和大众汽车等公司担任战略规划、咨询顾问、项目经理等职位。美国南加州大学MBA毕业。

5.2 BAIC顾问团队

陈宇

德弘资产管理公司创始人，仁和智本资产管理集团创始人、互联网金融产业创始合伙人。自由投资人，网名“江南愤青”，互联网金融教父，大家尊称其“校长”。从2012年开始在互联网上写作金融评论，以系列文章《浙江经济怎么了》，在金融业内引起极大震动，一跃成为金融领域最知名的评论人士之一。身为互联网金融领域的资深投资人和观察家，他 以独到的思考角度以及敏锐的观察眼光，对当下互联网金融的各种现象和机构作出了直切要害的评价与预测。2014年，陈宇被评为“大陆最佳投资人“。他还是中国网银联盟首席金融专家，是刘鸿儒基金研究会的研究员。他管理规模近百亿的资产，在香港、美国、澳洲都设有分支机构。他投资近200家互联网企业，担任了金字火腿、瑞茂通、京东金融、挖财、施乐会等十多家知名互联网金融企业及上市公司的首席战略顾问。

王利杰

中国著名天使投资人，资深区块链投资人。中国青年天使会华东分会会长；上海海天会执行委员；中国天使投资联席会成员；中关村天使投资协会副会长。2011年创办PreAngel天使投资品牌。至今投资近300多个科技初创企业，管理数十亿人民币基金。2014年开始介入区块链项目，先后投资小蚁/NEO：元届/ETP、方圆/CAT、ObEN/PAI、Smartmesh/SMT、Robin8/PUT、原本/Primas、Energo/TSL、语戏/CFun、Uplive/Gifto、Qlink/QLC：MedicalChain、Expread/EXC、Zeepin、Bnktothefuture/BFT、scry.info/DDD、Aptoide/AppCoin、iCube/ICC、Opskins/WAX、VanCoin、Ocean Protocol、还有ICO 投行高链资本和积分代币挖矿管理公司等数十个ICO类项目。

黄连金

CEO和创始人：Distributed Business Applications。前华为首席区块链科学家、美国 ACM Practitioner Board 委员、中国电子学会区块链专家委员、美国 CISSP (ISC注册信息系统安全专家)。曾经就职与美国CGI公司18年，担任安全技术总监，CGI云安全主管和首席安全架构师等职务。创建了CGI联邦身份管理和网络安全能力中心。在CGI工作时，曾经为美国联邦政府、金融机构、和公用事业公司提供金融，人工智能，区块链，安全等方面的专家咨询。

5.3 BAIC投资机构与行业伙伴

基金与机构

ZhenFund 真格基金

NODE CAPITAL 节点资本

Everest Link Capital

GENESIS 创世资本

IMO Ventures

HANHAI INVESTMENT GO FAR - GO TOGETHER

AWARE 先知资本

星耀资本 SPARKLING STAR CAPITAL

Leanone Angels Community 精一天使公社

ASBV 澳银资本

齐享资本 SHARING CAPITAL

道和资本 HILLVILLE CAPITAL

ULTIMATE

FULCRUM CAPITAL 支點資本

行业伙伴

科大讯飞 iFLYTEK

云知声 Unisound

全志科技 Allwinner Technology

MEDIATEK 联发科技

MOr

竹间智能

ARM

trio.ai


FOXCONN
富士康科技集团


顺舟智能
Wireless Anywhere


zigbee
Member


WLT 万联通


IdeeBank
灵感创造价值


LKK 洛可可


TusStar
启迪之星


FEIBIT


豪恩安防


UMEINFO 雍敏


TalkingData


东方智通


seeed
studio


华远达智能家
HUA YUAN DA SMART HOME


IMI
华捷艾米


时代拓灵
TWIRLING IN TIME

支持媒体


雷锋网


机锋论坛


金色财经


三感
video.


铅笔道


36Kr

第六章 BAIC 数字通证

6.1 BAIC 数字通证介绍

BAIC 数字通证简称 BAI，是BAIC社区官方发行的原生加密数字令牌。第一阶段将在以太坊上依据智能合约生成，第二阶段将基于BAIC社区公链自行生成，并作为BAIC社区的唯一基础积分通证，用来作为社区奖励、论坛积分、结算、交易、以及公链物联网智能合约履约使用。第一阶段通证将1:1与第二阶段通证进行置换。

数字通证BAI共发行210亿枚，由BAIC社区一次性创设出来，其总量上限已设定，不可更改，不可增发。数字通证BAI按照一定的规则和比例分配给不同的持有人。其中BAI的50%的比例将分配给BAIC早期投资人，用于区块链底层建设、产品模块研发、应用生态布局、BAIC公有链整体运维等。20%的比例则分配给团队，25%将预留给基金会并用于物联网设备的结算交易，5%将用于市场活动，促销，以及顾问团队。

第七章 开发工作路线图

BAIC开发计划表-1-1

时间	事项
2018年1月	确定BAIC公有链的商业模型，完成关键性商务合作的谈判，完成组织架构设立
2018年2月	NOW 广告交易平台上线
2018年3月	发布NOW系列更多软件及应用，BAIC测试链发布
2018年4月	全球家庭AI机器人IMIO Circle Show开始预售
2018年5月	硬件钱包开发完毕，AI机器人开始出货
2018年6月	BAIC公链上线
2018年7月	完成底层区块链及智能合约系统开发
2018年8月	BAIC 数据交易平台上线
2018年9月	BAIC 金融服务平台上线
2018年第四季度	BAIC社区正式版上线，完成BAIC在全球范围的布局