AVADAR
阿瓦达
——基于区块链技术的社交信息平台

1. 摘要

当今大多数社交信息分享平台都是中心化实体，近年来随着比特币、以太坊等加密数字货币开启了信息时代的经济革命大门，世界进入了价值互联网时代。AVADAR 将社交信息革命引领到一个新的水平。

AVADAR 是基于区块链技术的去中心化社交信息平台，任何个人或者组织均可以在 AVADAR 平台上快速建立去中心化社交应用，例如区块链论坛、区块链图片社交、区块链直播、区块链微博、区块链音乐分享等。未来平台将采用人工智能自动分析社交信息。AVADAR 平台内部集成智能合约技术，AVA 是 AVADAR 平台的内生数字资产，AVADAR 平台的任何价值信息分享者将获得 AVA 数字资产作为回报。AVADAR 平台让分享创造价值，让分享获得回报，让分享更自由。

目录

2. 时代背景（Blockchain）

Satoshi Nakamoto 于 2009 年创造了去中心化数字货币比特币，他的出现使人们对于财务的认识发生了惊人的变化。相对于传统银行，比特币具有更加高效的清结算速率并且消耗更加低廉的成本，但不幸的是，虽然比特币已经面世 8 年有余，由于其架构设计方面的缺陷，他未能在其他去中心化应用大幅度推广。比如比特币 7TPS 的交易处理能力的限制，每隔 10 分钟的交易确认等；另外，比特币协议里使用了一套基于堆栈的脚本语言，这语言虽然具有一定灵活性，使得像多重签名这样的功能得以实现，然而却不足以构建更高级的应用。这些缺陷使得比特币无法满足中高频交易的处理。

因此，比特币被看作区块链技术的先行者，同时也是一个满怀众多天生缺陷的区块链应用。2013 年年末，以太坊创始人 Vitalik Buterin 发布了以太坊初版白皮书，启动了项目。随着以太坊技术的流行，吸引了大量开发者以外的人进入以太坊的世界。以太坊是一个平台，它上面提供各种模块让用户来搭建应用，如果将搭建应用比作造房子，那么以太坊就提供了墙面、屋顶、地板等模块，用户只需像搭积木一样把房子搭起来，因此在以太坊上建立应用的成本和速度都大大改善。具体来说，以太坊通过一套图灵完备的脚本语言（EthereumVirtual Machinecode，简称 EVM 语言）来建立应用，它类似于汇编语言，我们知道，直接用汇编语言编程是非常痛苦的，但以太坊里的编程并不需要直接使用 EVM 语言，而是类似 C 语言、Python、Lisp 等高级语言，再通过编译器转成 EVM 语言。上面所说的平台之上的应用，其实就是合约，这是以太坊的核心。作为去中心化去信任不可篡改的分布式账本，区块链技术号称继信息互联网后又一大 IT 技术创新——价值互联网。

3. 基于区块链的社交信息平台

当今大多数社交信息分享平台都是中心化实体，由运营者决定社交信息平台由谁使用和如何使用。例如用户使用社交信息平台首先必须同意其条款声明，通常都会失去对所发表内容的所有权、收益权等，并且中心化社交信息平台有权对各种创意社交信息进行内容修改、编辑或者将其完全删除。例如 FaceBook、Twitter 等社交信息平台。

在中心化社交信息平台实体中，作者和读者之间缺乏直接的交流关系，而且这些充满创意的作者也没有机会将其价值信息货币化。这些价值信息也无法被准确评估其价值，因此一般情况下，作者要产生盈利，那得借助中间人，例如特殊的出版机构、专业的有价问答社区、专业的有价培训社区或者机构、社交信息平台中的特殊热贴等。

以上提到的问题没有一种综合性的解决办法，因此我们提出了一种能解决所有问题的开放平台构想，AVADAR 是一种基于区块链技术的分布式自助运行组织（DAO），不受任何第三方平台的干预。它是专门针对社交信息，用内生的数字资产激励用户的区块链社交信息平台。

4. AVADAR 的价值

4.1. 社交信息价值

社交信息平台作为开发者的天堂，使用者的乐土。开发者可以用智能虚拟机来定义新社交信息应用并且确定利益分配规则。社交信息平台为创作价值内容提供对应的报酬等（创意作者提交价值内容，会收到相应的报酬；会获取读者的（评价）打赏报酬或者限制性阅读报酬等）

4.2. 内建及广告价值

社交信息平台也可发布广告或者需要提高知名度的创意内容。读者每读取或者评价对应的内容都会收到报酬。

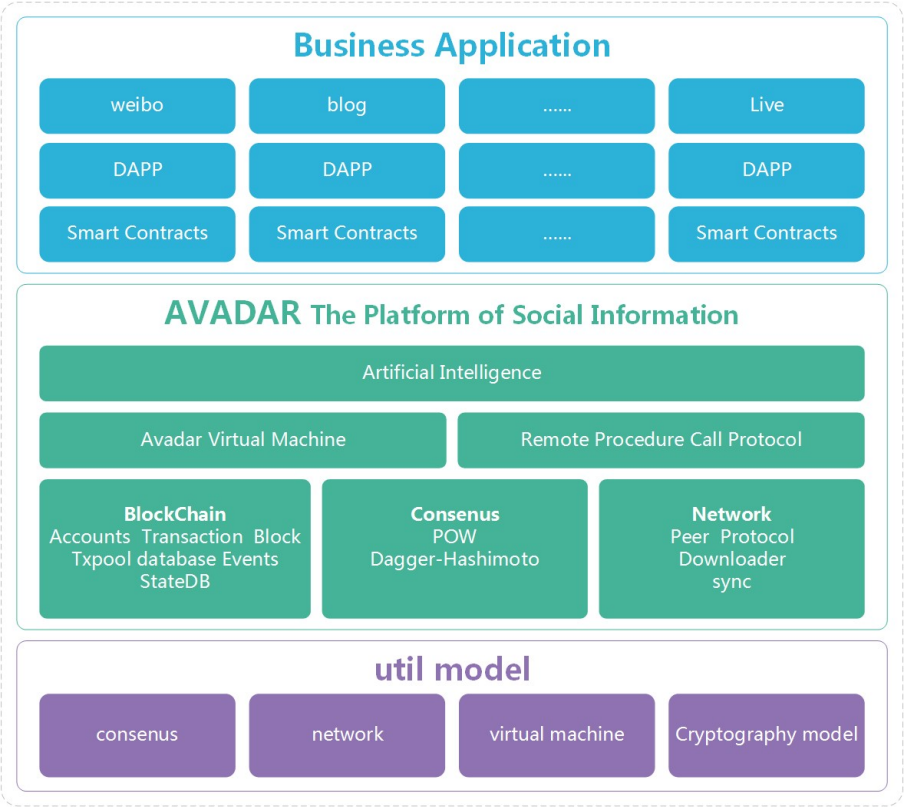
广告或者需要提高知名度的创意内容想发布在社交信息平台上必须付费，并且配置每次发出去的费用量。

4.3. 跨应用交易

不同应用之间的智能合约资产可以相互交易或者转账，AVA 作为社交信息内生数字资产是各个应用之间的转账或交易标杆以及交易费。

5. AVADAR 的核心技术

AVADAR 将是一个完备的社交生态体系，其主要由 AVADAR 社交信息平台、人工智能、多种去中心化商业应用几大模块构成，系统具体逻辑图如下：



基础工具模块包括共识算法、网络模块、虚拟机、加密算法；

AVADAR 社交信息平台包括区块链（账户、交易、区块、交易池、数据库、事件）；共识（proof of work）；网络（节点、协议、下载、同步）；AVADAR 虚拟机和 RPC 接口等。

人工智能模块：人工智能模块是未来 AVADAR 社交信息平台的特殊功能，其主要的作用是自动分析用户的喜好和关注，从广博的社交信息海洋中向用户推荐合适合理的社交信息，同时向用户推荐感兴趣的广告或者付费创意信息，让用户获取对应的点击广告或者付费创意信息收益。

商业应用模块：任何使用 AVADAR 社交信息平台的第三方组织或者个人均可以按照 AVADAR 提供的接口、虚拟机、应用框架快速创建自己的去中心化社交信息商业应用。

5.1. 共识与激励

5.1.1. 共识算法

AVADAR 的算法，AVADAR hash（Dagger-Hashimoto 改进版），是基于一个大的、瞬时的、任意生成的、形成 DAG（Dagger-part）的资料组规定，尝试解决它一个特定的约束，部分通过区块标题散列来决定。

它被设计用于在一个只有慢 CPU 的环境中来散列快速验证时间，但在被提供大量高带宽内存时，为挖矿提供大量的加速。大量内存需求意味着大规模矿工获得相对少的超线性利益。高带宽需求意味着从堆在很多超速处理单元、分享同样内存的加速在每个单独的单元给出很少的利益。

AVADAR，和所有区块链技术一样，使用激励驱动的安全模式。共识基于选择具有最高总难度的区块。矿工节点生成区块，其他节点检测有效性。

AVADAR 挖矿使用的工作量证明(POW)算法叫 AVADAR_hash（Dagger-Hashmoto 算法的改进版本），包括找到算法的随机数输入以使计算结果低于特定的难度阈值。工作量证明算法的意义在于，要找到这样一个随机数，没有比列举可能性更好的策略，找到随机数的耗时取决于难度阈值。这使得只通过调整难度来控制找到新区块的时间成为可能。

正如协议中所描述的，难度动态调整的方式是每 30 秒整个网络会产生一个区块。我们说网络用 30 秒区块时间生产一个区块链。这个"心跳"基本上主要强调系统状态同步，保证不可能维持一个分叉（允许 double spend）或被恶意分子重写历史，除非攻击者有半数以上的网络挖矿能力（即所谓的 51%攻击）。任何参与到网络的节点都可能是矿工，预期的挖矿收益和他们的（相对）挖矿能力成正比。

AVADAR hash 工作量证明是具备内存难解性，需要选择依靠随机数和区块标题的固定资源的子集合。这个资源（几十亿字节大小的数据）叫做 DAG。每 600 个区块的 DAG 完全不同，25 小时的窗口叫做 epoch（大约 1.04 天），需要一点时间来生成。由于 DAG 只由区块高度决定，它可以被事先生成，如果没有被事先生成，客户端需要等到进程最后来生产区块。如果客户端没有预生成并提前缓存 DAG，网络可能会在每个 epoch 过渡经历大规模区块延迟。注意不必要生成 DAG 以验证工作量证明，它可以在低 CPU 和小内存的状态下被验证。

在特殊情况下，从零开始创建节点的时候，只有在为现存 epoch 创建 DAG 的时候才会开始挖矿。

5.1.2. 挖矿奖励

获奖区块的成功工作量证明矿工会获得：

"获胜"区块的静态区块奖，包含 8.0（8 个）SOC。

区块内支出的 gas 成本——一定数量的 SOC 币，取决于当前 gas 价格。叔伯块的额外奖励，形式是每个叔伯块包含额外的 1/32，在区块中执行所有交易所消费的、由获胜矿工提交的 gas 都由每个交易的发送者支付。已发生的 gas 成本归到矿工账户作为共识协议的一部分。随着时间变化，这会使数据区块奖变得矮小。

5.2.价值交易系统

5.2.1. AVA 账户

在 AVADAR 系统中，状态是由“账户”对象和在两个账户之间转移价值和信息的状态转换构成的。AVADAR 的账户包含四个部分：

（1）随机数，用于确定每笔交易只能被处理一次的计数器

（2）账户目前的余额

（3）账户的合约或者虚拟机代码（默认为空）

（4）账户的存储

AVA 是 AVADAR 内部的主要加密燃料，用于支付交易费用。一般而言，AVADAR 有两种类型的账户：外部账户（由私钥控制的）和合约账户（由合约代码控制）。外部账户没有代码，人们可以通过创建和签名一笔交易从一个外部账户发送消息。当合约账户收到一条消息，合约内部的代码就会被激活，允许它对内部存储进行读取和写入，和发送其它消息或者创建合约

5.2.2. AVADAR 交易系统

AVADAR，作为一个整体，能被看成是一个基于交易的状态机：我们开始于一个创世块（“Genesis”）状态，然后伴随着执行交易的写入到最后的状态。这个最后状态是我们能接受的权威的版本在 AVADAR 社交信息区块链平台世界。这个状态保存了一下信息，比如账号的余额、名誉度、信誉度、

和附属的现实世界的数据。总而言之，最近能被电脑描绘的任何事都是合理的。因此，交易就代表了两个状态的有效桥梁；这个“有效”是很重要的－因为这里存在无效的状态改变远远超过有效的状态改变。举一个例子：无效的状态改变可能是这里减少了一个账号的余额，但是没有在其它任何账号上加上同等的额度。然而，一个有效的状态转换是来自一个交易。公式上：

（1） $\sigma(t+1) \equiv \gamma(\sigma\ t, T)$

其中γ是 ETH 的状态交换函数。在 ETH 中γ与σ是相当地强大超过现存任何的类似系统；γ允许部分成分去实现特有的计算，相比下σ允许部分成分存贮特有的状态在交易间。

交易是被校对在区块中；区块采用一种密码学的哈希值（hash）作为参考方法被“链子”链接起来。区块充当一个日记，记录着一系列与之前区块的交易和鉴定最后一个状态（虽然它不能通过自己存贮最后状态－因为这个区块链会一直增加）。他们也标记这些交易系列为了激励节点去挖矿。这样的激励作为状态转换函数发生，同时增加相应的价值到一个特定的账号。

挖矿是一个奉献努力的过程，这个过程是为了维持交易链（区块链）在任何一个潜在的竞争块中。它是由于一种密码学上安全证明的方式被实现。这个工作量证明的体制（POW）是众所周知，会在 11.5 小结讨论更多的细节。

公式上，算式张开成：

（2） $\sigma(t+1) \equiv \Pi(\sigma\ t, B)$

（3） $B \equiv (\cdots, (T0, T1, \cdots))$

（4） $\Pi(\sigma\ t, B) \equiv \Omega(B, \gamma(\gamma(\sigma, T0), T1)\cdots)$

其中Ω是区块完成状态转换函数（这个函数是奖励一个特有的团体）；B 是这个区块，它包含了某些成分中的一系列交易；Π是区块等(“block-level”)状态转换函数。

5.3. AVADAR 虚拟机

AVADAR 是一个可编程的区块链。AVADAR 允许用户创建他们自己的去中心化应用，这些应用可以任意复杂。这样，AVADAR 成为了多种不同类型去中心化区块链的服务平台，包括但是不限于加密货币。

AVADAR 的核心是 AVADAR 虚拟机，AVADAR 虚拟机可以执行任意算法复杂度的代码，AVADAR 虚拟机是图灵完备的，但是为了限制逻辑代码的无限制执行，采用最大执行燃料限制其逻辑代码的复杂性或者基本操作数。

与其他区块链系统一样，AVADAR 同样包括了一个点对点（P2P）协议。AVADAR 区块链数据库由连接到网络的多个节点维护和更新，这个网络上的每个节点都运行 SVM 并且执行相同的指令。这种在整个 AVADAR 网络上进行大规模并行计算并不是为了获得高的效率。而是每个 AVADAR 节点运行逻辑是为了在区块链中保持一致。去中心化一致性使得 AVADAR 具有非常高的容错性，而且使存储在区块链上的数据永远不可改变。

AVADAR 平台自身不提供功能和价值。就像编程语言及其编译器一样，由企业或开发者来决定 AVADAR 未来的应用。但是，比较明确的是不同的应用类型从 AVADAR 得到的好处是不同的。比如那些在点对点市场进行协调的应用程序，或者自动化执行复杂社交游戏合约的应用程序。理论上，社交互动或者任意复杂性的交易都可以由运行在 AVADAR 上的程序自动并且可靠地实现。除了社交游戏应用程序之外，任何需要信任、安全和永久存储的社交信息应用都可能受到 AVADAR 平台的巨大影响，例如微博、博客、问答等。

5.4.artificial intelligence （人工智能）

5.4.1. 数据管控

AVADAR 社交信息内容一直为人类所掌控，但 AI 的出现正在改变这一切。利用 AI 管控信息，让社交信息内容中的暴力和色情等非法内容无处遁形，并且减少对青少年的伤害。

很多高科技公司正致力于利用机器学习来解读社交信息的内容和图片信息，部分科技公司已经掌握了相关技术，能够实时分析社交信息和图片信息中的情色信息。这类社交信息软件已经投入使用，对 Facebook 等发布的社交信息进行监测，过滤暴露的情色内容。

5.4.2. 推荐系统

随着 AVADAR 社交信息平台的发展，其规模将越来越大，广告业务和付费创意信息也将越来越多，完全靠人工分拣社交信息不太现实，而且对于想建立一个公正公平的社交信息生态体系也无甚益处。

确定型人工智能可以帮助社交信息生态体系处理大量的业务匹配分析,通过将大量的决策制定和数据分析自动化，社交信息生态体系可以降低监管风险并提高效率。另外，确定型人工智能可以通过控制个体偏见和误差以提高决策制定时的一致性。

背景：什么是业务匹配？

业务匹配是用来决定一个广告业务是否适合某位用户的分析过程。它既适用于用户市场（如：查看广告的个人），也适用于特定兴趣用户市场（如：在复杂的广告市场中挑选适合自己风格的广告业务，并且无缝结合或者过度）。

我们为什么需要业务匹配？为了证明公平性和最大化各方收益。

业务匹配被用于证明公平性。广告主或者付费创作者在将广告业务或付费创意信息推广给用户时需要充分了解每位用户的关注领域和兴趣，这样才能做到公平对待用户,这个过程也为广告主或者付费创意者控制了风险。为了证明公平性，社交信息生态体系使用“合理”这个词，审查常常建立在定量和结构化的数据之上；为了在实际决定中避免依赖于特定的个人或者有赖于用户当天的处理。决策制定也受到个人偏见或者个人错误的影响——我们毕竟是普通人。换句话说，传统用户匹配分析的质量参差不齐。通过运用“确定型人工智能”来进行用户匹配分析，将会扭转当前这种分析质量不稳定的情况。

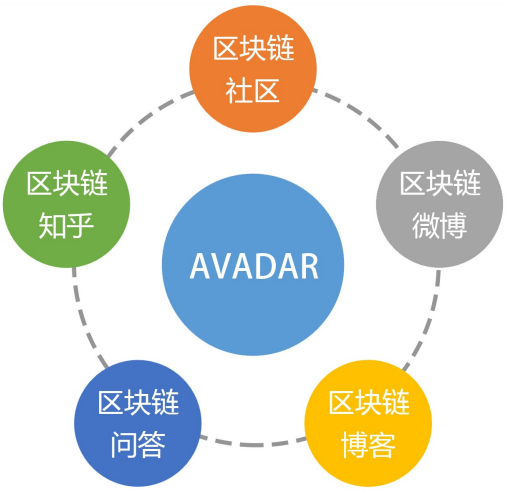
运转中的确定型人工智能与用户匹配。这个平台将会处理和总结定量数据，共同地，社交信息生态体系中的用户将他们的专业能力集合在一起，共同决定发行的广告对于用户是合适的。

通过“机器间对话”和“人机对话”，确定型人工智能只将所需数据加总，将最佳的决策制定过程应用到相关情景中。

6. AVADAR 的生态系统

AVADAR 社交信息平台的目标是系统化建立社交信息区块链底层平台，用 AVA 数字资产作为 AVADAR 区块链系统的生态系统的支付方式。

任何具备开发能力的组织或者个人都可以基于 AVADAR 社交信息平台完成去中心化微博、去中心化博客、去中心化图片等应用。AVADAR 的社交生态信息体系如下图。



AVADAR区块链社交生态体系

6.1. 多 DApp 支持

AVADAR 钱包包括一个专用定制的客户端内核模型，使得用户可以运行各种各样的基于 AVADAR 的 DApp。这一内核模型非常易于使用，所以 DApp 和相关的智能交易模型能够被大量用户使用。从降低用户使用门槛角度而言，这个内核模型是一项突破性成就。 它的作用等同于浏览器之于互联网。内核模型具有特殊的安全层、密钥管理、去中心化用户账户地址管理（即用户帐户由用户拥有并控制，而不是第三方机构），这一切使得这个定制内核成为用户运行或者管理 AVADAR 平台去中心化应用不可或缺的工具。

6.2. 快速创建 DApp 支持

AVADAR 社交信息平台致力从技术层面全方位支持社交信息去中心化应用，将不同的 DApp 线路产品化，使普通互联网用户可以真实感受到区块链技

术带来的价值。 面对不同行业，不同线路的去中心化应用，可以把区块链技术带给更多的用户。例如去中心化的产权社交，去中心化的社交信息流转和去中心化的社交聊天等，通过激励机制的引入，将更深入利用共享社交经济的理念，改变现有的 APP 市场的商业模式。 区块链技术为搭建去中心化应用提供基础架构，在 AVADAR 中，通过完善的 AVADAR API 设计，简化开发者的前期工作，开发者可以快速切入。

7. AVADAR 的数字资产 AVA

AVADAR 社交信息平台的内生数字资产 AVA，中文名阿瓦。AVA 被用来支付交易费，以及奖励创意作者的作品和经常评价作品的用户等。AVA 是所有基于 AVADAR 社交信息区块链平台应用的通用数字资产，从而实现不同的社交信息平台应用之间的价值转换。

8. AVADAR 发展规划

AVADAR 社交信息平台是由 AVADAR 团队组织创立的非营利性项目。该组织不从该项目中收取任何经济效益。该组织所扮演的主要角色是开发基于区块链的社交信息平台，为创建去中心化社交信息应用提供一种快速的途径；提供 AVA 数字资产的发行、管理和 AVADAR 平台未来发展方向的确定。AVADAR 社交信息平台的开发现在已经开始，相应内容及进度将在 ICO 活动中介绍。下面是我们的开发进度规划:

2016 年 10-12 月　项目调研，资料收集整理
2017 年 1 月　组建项目团队
2017 年 2 月　项目基础工具模块开发、测试
2017 年 3-6 月　底层区块链开发,测试
2017 年 5-6 月　AVADAR beta 版钱包开发、测试
2017/8/1　中文官网上线，发布技术白皮书
2017/8/2　AVADAR 钱包 beta 版本上线
2017/8/3　ICO 第一期启动
2017/8/28　ICO 第一期结束
2017/9/2　区块链浏览器开发、测试
2017/9/5　AVADAR 正式版钱包上线；AVA 币上线，英文官网上线；
2017/9/6　启动 AVADAR 平台 beta 版开发、测试
2018/3/6　AVADAR 平台 beta 版上线(虚拟机、内核模型、RPC 接口等)
2018/5/6　AVADAR 平台正式版上线

9. AVADAR 众筹方案

9.1. AVADAR 分配方案

AVA 币总量共 2.5 亿枚,团队预挖 2.2 亿枚,3000 万枚后期挖矿产出。
AVA 币总量的 40%共 1 亿枚将用于 ICO;
AVA 币总量的 20%共 5000 万枚将分配给创始团队和开发团队，将用于 AVADAR 社交信息平台的开发和运营，奖励给开发人员和运营人员，冻结周期为 3 年;
AVA 币总量的 12%共 3000 万枚用于私募投资人、战略投资人以及业界知名人士的天使轮融资，（招募 10 人，每位投资人最低持有 150 万枚，最多持有 300 万枚），招募的投资人将进入团队管理层，参与项目未来的运营、管理以及决策;
AVA 币总量的 8%共 2000 万枚用于 AVADAR 社交信息平台奖励、第三方合作、社会公益以及宣传推广等;
AVA 币总量的 8%共 2000 万枚用于商业合作，任何在 AVADAR 平台上建立去中心化社交信息应用的组织或者个人，均可根据贡献获取对应的奖励;
AVA 币总量的 12%共 3000 万枚用于 AVADAR 社交信息平台挖矿。

9.2. AVADAR 众筹时间表

阶段	开始时间	结束时间	BTC	ETH	奖励
天使轮	2017/7/29 15:30	2017/8/3 15:30	128123	10343	0
早鸟阶段	2017/8/3 15:30	2017/8/7 15:30	85415	6895	15%
第一阶段	2017/8/7 15:30	2017/8/14 15:30	85415	6895	10%
第二阶段	2017/8/14 15:30	2017/8/21 15:30	85415	6895	5%
第三阶段	2017/8/21 15:30	2017/8/28 15:30	85415	6895	0

9.3. 资金使用

- 技术开发： 50%
- 商业运营： 18%
- 法律与合规性： 2%
- 储备金： 30%

10.联系我们

官网：www.avadar365.com
微信：
QQ 群：251889046
公众号：
Twitter:
Facebook：