ZOZ公链白皮书

2019.07.12

ZOZ公链白皮书

目录

摘要

自创世区块诞生以来，比特币已经有了近十年的历史，比特币以耀眼的方式吸引着全球注意力，逐渐形成了集支付、储备、数据库等功能于一体的区块链平台。 与此同时比特币也存在耗能严重，算力易集中被操控，效率低下，对智能合约与DAPP 开发不友好等问题。为此本白皮书提出基于比特币的分叉技术 ZOZ（Virtual-GoodsToken），针对当前比特币面临的问题，提出新的分叉币案例尝试。由于高功率采矿硬件最终拼的是电力，工作量证明采矿在环境上是不可持续的。ZOZ 利用节能的 DPOS 算法，可以在任何计算机上开采，并且永远不需要专门的采矿设备，同时基于 DPOS 共识机制出块时间短、高效、强健的特性，ZOZ 可实现高效的交易确认。ZOZ 作为去中心化的全球价值互联网传输协议，以 Satoshi Nakamoto 对比特币的愿景为蓝本。ZOZ 协议为比特币可持续发展问题提供了一个简单的解决方案，并通过VVM(ZOZ VM) 智能合约虚拟机来对进行智能合约代码运行，提供了更快， 更具可扩展性的区块链平台，更适合日常交易使用。ZOZ 是一种可持续的去中心化点对点交易通证，具体应用包括点对点支付以及去中心化数字资产交易等。任何接受ZOZ协议的用户都可以几乎免费的使用 ZOZ 来保证交易的实时性与安全性。借助于强大的网络吞吐能力与智能合约，ZOZ 可为快速点对点支付、去中心化交易平台、比特币联储等开发及使用需求提供充分性能支撑。

ZOZ 公链除了 ZOZ 币外，还推出基于 Ominlay 的稳定币 USDTB。本白皮书将详细讲解这些理念。

《1》设计背景

1.1 行业背景

比特币由 Satoshi Nakamoto 于 2009 年创建，是世界上第一个区块链技术应用的实施。比特币网络是由互联网连接的全球计算机网络，每台计算设备都称为节点。当有人发送一些 BTC 时，交易将被广播到所有节点，每个节点可以独立地验证交易的真实性。比特币系统将每隔几分钟发生的所有事务都打包在一起为一个区块，为了完全处理事务区块并将其添加到所有历史有效事务的区块链或公共分类帐中，节点间需要竞争解决困难的数学问题，率先完成正确解的幸运节点首先获得新比特币的奖励，并且其区块被添加到区块链中。通过解决困难数学问题，即计算密集型数学问题的过程称为POW 工作量证明，POW 是比特币网络安全的共识机制。

从货币角度来讲，比特币是目前为止规模最大的数字货币，它是区块链 1.0 时代的一个重要应用，是区块链的首次应用：比特币在去中心化的前提下，实现了数字货币在发行、支付、流通等阶段的职能，这是一种全新的支付手段。 从区块链角度来讲，随着比特币的关注度逐渐增大，区块链作为它的底层技术也越来越被大众所熟知， 区块链开始逐渐脱离数字货币，渗透到许多商业领域，不同行业都希望能够将比特币这个技术应用到我们的现实生活中去，通过各式各样的应用场景，让我们获得更好的体验。

Satoshi Nakamoto 对比特币的愿景是允许跨境点对点支付和创建世界上第一个真正去中心化的价值转移网络，这无疑是革命性的。同时比特币的底层区块链技术直接导致许多去中心化的网络的建立，如 ETH、EOS 等，这些网络允许智能合约，身份保护，知识产权管理，供应链管理以及众多其他前所未有的创新。

1.2 需求和痛点

随着公众对比特币和区块链技术的认识的提高，加密货币市场的估值也在加。随着越来越多的投资者和投机者开始了解区块链技术的真正潜在价值， 主流加密货币价格稳步上涨。尽管区块链技术很有前途，但如何确保加密货币生态系统的长期可持续性，可扩展性和良性发展。比特币和其他工作量证明等区块链耗能网络从长远来看是不可持续的。比特币的能源消耗正在快速增长，因为它使用了一种非 常低效的POW共识机制来保护其网络。比特币的全部目的是让人们在一个不需要中间人的、去信任、去中心化的网络中，快速、廉价、 匿名地进行价值传递。比特币充分利用了密码学技术来保证比特币系统的运作安全，其中主要采用的密码学原理是：哈希算法和非对称加密。哈希算法，简单理解，就是将一切的交易信息给 “代码化"，它是单向性的，通过全网公开的交易信息也不会查到交易者的个人信息。哈希算法可以说是贯穿了整个比特币的运作，无论哪个环节都离不开哈希算法。非对称加密，实现了在没有中心化机构（银行）的情况下，交易双方的信息安全、资产安全。尽管理论上，这些密码学原理能够保证比特币作为一个 “去中心化货币”基本职能的实现，但比特币却也存在一些问题，这些问题使得比特币的发展与其目的相佐。

1.2.1 处理交易的速度太慢

比特币系统里面，一秒钟最多处理 7 笔交易，显然这个速度是无法满足正常的交易需求的。要知道我们现在用的支付宝、淘宝、微信，每秒能处理几十万甚至上百万的交易，一笔交易只需要 1-2 秒就处理成功，如果比特币拿来做日常货币使用，那么我们在微信上付一次款，起码要 1-2 天才能处理成功，是很难让人接受的。

1.2.3 比特币挖矿消耗的电量太大

挖矿需要专业矿机，专业矿机的算力很高，但是消耗的电量是巨大的，而且以现在的行情来看，买一台矿机挖矿一年很难回本。比特币现在年挖矿消耗的电量已经高达 2900 亿千瓦时，超过了 159 个国家消耗的电量。因此，就有人怀疑：消耗这么大的电力去维护一个交易速度如此之慢的系统，是能源浪费和不可持续的。

1.2.4 对智能合约与DAPP开发不友好

比特币系统只能进行简单的 Script 编程，Script 是比特币协议中用于事务处理的基于堆栈的脚本编程语言。Script 编程语言不是图灵完备的，缺乏现代编程语言的功能，如循环，只能进行有限的应用编程。Bitcoin 需要开发通用的脚本语言来支持丰富功能的应用开发。

1.2.5 作为货币存在通货紧缩的情况

货币被视为比真实财富更重要，比特币作为加密货币存在通货紧缩的情况，因为比特币一共才 2100 万枚，流动性不足导致比特币生态发展受限，我们需要足够供应的货币使我们能够按照我们的选择进行交易。

1.3 ZOZ方案

ZOZ（ZOZToken，中文表示虚拟货品通证）致力于解决比特币系　统存在的许多局限性，作为一种交易性的日常使用货币，旨在提供比特币的可扩展和可持续的替代品。ZOZ 利用节能的 DPOS 算法，可以在任何计算机上开采，并且永远不需要专门的采矿设备，同时基于DPOS共识机制出块时间短、高效、强健的特性，ZOZ 可实现高效快捷的交易确认。并通过 (ZOZVirtual Machine)智能合约虚拟机来对进行智能合约编码运行，提供了更快，更具可扩展性的　区块链平台，更适合日常交易使用。通过 USDTB 通证来应对通货紧缩的情况。

《2》ZOZ项目介绍

2.1 比特币点对点电子现金系统

比特币一种完全通过点对点技术实现的电子现金系统，它使得在线支付能够直接由一方发起并支付给另外一方，中间不需要通过任何的金融机构。虽然数字签名（Digital signatures）部分解决了这个问题，但是如果仍然需要第三方的支持才能防止双重支付（double-spending）的话，那么这种系统也就失去了存在的价值。比特币白皮书提出一种解决方案，使现金系统在点对点的环境下运行，并防止双重支付问题。该网络通过随机散列（hashing）对全部交易加上时间戳（timestamps），将它们合并入一个不断延伸的基于随机散列的工作量证明（proof-of-work）的链条作为交易记录，除非重新完成全部的工作量证明，否者已经形成的交易记录将不可更改。最长的链条不仅将作为被观察到的事件序列（sequence）的证明，而且被看做是包含 CPU 最大计算工作量的链。只要绝大多数的 CPU 计算能力都没有打算合作起来对全网进行攻击，那么诚实的节点将会生成最长的、超过攻击者的链条。这个系统本身需要的基础设施非常少。信息尽最大努力在全网传播即可，节点（nodes）可以随时离开和重新加入网络，并将最长的工作量证明链条作为在该节点离线期间发生的交易的证明。

中本聪的“去中心化”背后的潜台词是“大多数人诚实”，共识机制是比特币的核心理念。建立一套“去中心化的 P2P 支付系统”，没有中心（中介）的支付系统，要避免“双花”（双重支付），该如何进行账目记录。答案是通过共识机制：用密码原理和工作量证明 (Pow) 代替中心化权威信用。产生一条新的交易记录时永远有先后顺序，即便是双花也总有先后顺序，同一用户不可能同 时创造两笔交易。比特币首先引入了基于时间戳的随机散列，让其形成前后相 关的序列，比特币的交易记录就是一个时间序列的链条。这就是为什么称之为 区块链的原因。要避免双花，只需要证明其中一条链有效即可，并且将其记录 到交易链条上，其他的交易就是无效的了。要证明其中一条是有效又不允许中 心化从存在，只有一个办法：发动所有人参与这项活动，进行 “多数人见证”。

POW 共识算法正是为了解决谁是大多数的问题，“大多数”的决定表达为最长的链。新区块进行节点广播，一旦有节点收到了这个区块的广播，会按照“当 且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才 认同该区块的有效性”的规则进行验证。验证通过后，这个节点就不会再接受别的节点的同样区块了。同时这个节点会终止自己正在进行的包含同样交易的区 块 计 算，节点在这个区块基础上启动新的交易区块计算，如此往复，形成链条。由于网络延迟，如果同时有几个节点互相收到交易区块，记录同样的链条（分叉），该僵局的打破要等到下一个工作量证明发现。通过一段时间运行，总有一条区块链时序最长， 作为最终被认可的链条。比特币区块链就是在不停的分叉、抛弃、又分叉、又合并的过程（这里的分叉都是暂时性的软分叉）。共识机制替代中介信任，设计者同时智慧地引入矿工奖励机制，即依赖矿工供算力构筑比特币信任的城墙，进而通过不可逆地凝结算力这一方式，从无到有创造了一个全球性

电子现金系统所需要的关键元素，那就是信任。比特币现金系统是一种对互联网通信协议进行变革的技术，它将创建出新的信任网络，促成巨大的经济生态系统，和产生持久的长久价值。某种意义上来说，构建牢固且不断累积增长的信任。
才是比特币协议设计思想核心的核心。

2.2 ZOZ的分叉法方法

比特币分叉，广义上指比特币区块链在拓扑结构上的分裂，在较短时段内形成两条链共存的情况；但在比特币共识机制的作用选择下，区块链最终会恢复到唯一链的共识状态。狭义的分叉一般指代人为导致协议变动带来的硬分叉， 因共识的分裂造成比特币网络在多套不同的共识群体环境下运行，形成若干独立 的区块链协议。比特币至今已有多个仍在成功运行的分叉协议版本，不同的协议版本针对比特币存在的缺陷或局限出了各有侧重的解决方案。ZOZ 通过发起对原始比特币协议的硬分叉，成为比特币的一个实现版本，ZOZ 可以被认为是对比特币协议的一种诠释方式，亦应当被认为是点对点电子现金系统的一个落地 方案。ZOZ 采用基于 UTXO 的 DPOS 共识机制，目的是作为主网长期稳定的运行。

ZOZ 认为，一个真正的点对点支付系统，需要满足以下条件：

（1） 运行成本足够低廉，大大低于该系统功效所产生的社会总效用；

（2） 高效的 TPS，足以应对高频小额支付交易；

（3） 系统应有稳定运行的 Token 经济系统，引入适当的角色以支持系统的可扩展性、并平衡其中的利益关系；

（4）有可行的方法进行协议的自我更新，使得系统能够不断进化、引入新的特性以适应环境

ZOZ 的分叉方法论：1)ZOZ 希望实现比特币点对点现金系统的设计初衷，通过改造比特币协议，建立一个技术上可行的、全球共享的点对点现金系统；2) 在点对点现金系统的基础上，要求协议能够承载一定的经济活动功能，简便、安全、人人可用；3)ZOZ 认可原始比特币协议的价值与地位，复用和借鉴了原始比特币协议所产生的数据以及大部分重要设计思想； 4)ZOZ 对比特币协议进行的上述改进和创新，既要在根本上解决构建点对点现金系统所必须面对的技术及经济问题，又要尽可能地引入已经被验证成熟的技术和模式，确保系统的稳定性、用户可接受性以及长期可持续性。

为了平衡 TPS 以及控制运行成本的矛盾，ZOZ 引入高效的 DPOS 共识机制，保证 3 秒稳定出块、具备不可逆转块设计，不仅使得点对点支付得到技术性能上的支撑，也为内置 dApp、链上治理、智能合约等复杂链上行为和功能供了充分可行性。其次，针对协议的可维护性、可持续性以及长期创造性解决问题的能力要求，ZOZ 构建了有自身特色的治理哲学，引入了兼顾公平与效率的链上治理体系，鼓励社区对链上事务的参与及促进参与群体对环境变化的响应，因而协议能够快速更新迭代，成为能够自我运营、自我更新进化的比特币协议。而针对协议功能对经济模型中复杂系统角色的需求，ZOZ 的链上治理体系和 VDEX 体系引入了节点、分享治理委员会、交易网关、承兑网关等经济行为角色，权力结构上实现了记账权与治理权的两权分离，在链上治理的民主实践中迈出创造性的一步。同时整合 IPFS，为ZOZ 的生态应用提供更为广泛的应用支持。

2.3 比特币发展与其原始设计目的的偏离

中本聪设计比特币的初衷，本来就是为了追求相对的公平，追求不被操纵的货币体系。

中本聪创建比特币的初衷：建立一个不依托于政府信用、去中心化的电子货币系统。比特币，作为一种加密货币，逐渐背离了它被设计的初衷。比特币虽然具备了法币的大部分特征，但是在稳定性这方面，确实是比特币广泛流通的一个大坑。虽然国家法币之间的汇率常有波动，但却不太影响消费者的日常使用。而比特币的价格波动，却让它只能出现在 K 线图上。比特币在某些方面确实具有货币的一些属性，但是就目前的情况来看，稳定性和流通性是两个硬伤， 而这两个硬伤也是阻碍比特币平民化的主因。同时虽然比特币在设计上保证了去中心化、 点对点的电子现金系统的技术可行性，但这并不意味着比特币的发展路径完全符 合白皮书的设计初衷。有货币的一些属性，但是就目前的情况来看， 稳定性和流通性是两个硬伤，而这两个硬伤也是阻碍比特币平民化的主因。同时虽然比特币在设计上保证了去中心化、点对点的电子现金系统的技术可行性， 但这并不意味着比特币的发展路径完全符合白皮书的设计初衷。

比特币存在耗能严重，算力易集中被操控，效率低下，对智能合约与DAPP开发不友好等问题，比特币暴露了作为点对点现金系统的诸多弊病，并且在市场影响下选择了偏向于储值资产的自我定位。如前文所言，一个真正的点对点支付系统，1）运行成本足够低廉，大大低于该系统功效所产生的社会总效用；2）高效的 TPS，足以应对高频小额支付交易；3）系统应有稳定运行的Token 经济系统，引入适当的角色以支持系统的可扩展性、并平衡其中的利益关系；4）有可行的方法进行协议的自我更新，使得系统能够不断进化、引入新的特性以适应环境。

此外，比特币的治理机制依赖的是最为原始的链下治理，治理内耗极为严重、无法实现快速响应，这应当是众所周知且一度影响比特币生死存亡的大难题。又因比特币对路线的选择，导致比特币开发组对协议的变动和升级极端保守化， 这一切使得比特币并不适合作为点对点现金系统这样一个偏向于支付应用的系统。

比特币虽然构建了可以持续运营的矿工体系，但是对于点对点支付系统这样偏向于实际应用、功能设计更为复杂的系统来说，矿工体系显得过于简单低级。而且目前主流论调普遍认为，可以从数学和经济原理上证明，在POW机制下矿工与用户、开发者的利益是不可协调的。比特币体系无法给出一种很好的可以让复杂的链上系统经济角色（ 例如网关 ）产生收入并平衡各方利益的解决方案，也无法做到记账权与治理权的两权分离，极大地阻碍了比特币适应复杂经济活动的能力。

2.4 ZOZ分叉信息

分叉时间：计划为北京时间 2019 年8 月8 日；

分叉块高： 555555；

共识机制：基于 UTXO 的 DPOS 共识算法；

ZOZ 代币发放总量：1 亿枚；

出块间隔：固定 3 秒，可动态调整；

添加 VVM 虚拟机功能；

区块体积：最大可达 128M，可动态调整；

发行稳定币 USDTB(1：1 方式与美元锚定）

添加重放保护；

支持 CPU 挖矿；

支持智能合约编程；

整合 IPFS 星际文件系统。

《3 》ZOZ公链背后的技术

3.1 ZOZ作为价值互联网协议

在互联网这样一个大模型中，区块链是应用层里面的一个价值点对点传输的协议 ，它的价值与信息互联网中 HTTP 协议的价值一样。没有 HTTP 协议，就不可能有互联网的存在；没有区块链协议，在没有中介帮助的情况下，也不可能点对点地在互联网上完成价值传输。区块链本身就是一个互联网协议，这就是区块链在整个互联网模型中所处的地位。ZOZ 是一个互联网价值传输协议， 所谓价值传输，指在特定协议框架下可以实现的价值表达、传递和信用构建， 以及基于此的所有经济金融活动，具体可能包括转账汇款、数字资产互换，法币与数字资产交换、信用背书的数字资产发行与交易、去中心化交易所、交易与承兑网关等一系列具备现实功能与社会效用的应用。ZOZ 协议的设计核心是：通过选用适当的技术架构去保证 ZOZ 有足够的能力担当全球互联网价值传输的载体系统。ZOZ 协议是实现价值传输的基本框架，即一切链上经济行为的载体。ZOZ 协议基于 UTXO 的 DPOS 共识机制，通过不可逆转块、时间戳共识、Cache 中间件等来平衡 UTXO 与DPOS 的性能与可靠性，实现了一个比原始比特币更为贴近点对点现金系统设计初衷的协议版本。ZOZ 价值互联网协议网络超越了社交网络的层次，实现了人与人之间的价值联接。从联接本质上看，网络通过协议让子系统分布式主体之间形成关系，从而实现子系统或结点与其他子系统或结点的交互。联接无处不在，联接使要素交互成可能，交互又形成了经济。

3.2最有效的共识机制DPOS

DPOS（委托权益证明）特点：出块时间超短，效率高，几乎不会分叉。这种特点，使得 DPOS 在未来相当长的一段时间内，都具有独特的优势，是目前相对先进的共识模式。ZOZ 便采用了 DPOS 这个机制。DPOS 保障了投票权在持币人手中，因此持币人将可以通过投票选择是否通过议案，从而决定项目的发展方向。这同时也意味着，项目的发展方向取决于关心项目本身的人群手中， 众智的力量将推动项目更好地发展。同时 DPOS 机制的优点还有不存在算力攻击、严格遵守时间出块和节约资源等。

3.2.1 DPOS 共识机制优点

（1）低功耗

DPOS 机制将节点数量进一步减少的同时，将节点间的相互关系从竞争改为合作，避免了不必要的算力竞争和互相攻击等无谓的损耗，在保证网络安全的前提下，整个网络的能耗 进一步降低，网络运行成本最低。

（2）高效能

更快的确认速度：以 ZOZ 为例，每个区块的时间固定为 3 秒，一笔交易（ 在得到 6-10 个 确认后 ）大约消耗 1 分钟，完整的区块生产周期仅需 5 分钟；每 1-2 个周期即可以生成 作为确认点的不可逆块。而在 PoW 机制下，以比特币为例，产出一个区块需要约 10 分钟，而确认一笔交易（ 得到 6 个确认 ）至少需要 1 小时。

（3） 鲁棒性

在整个过程中，任何人都可以通过观察见证人的参与率来监测网络健康状况。如果在某个 时候见证人的参与程度都低于一定水平，那么整个区块链交易网络用户可以被允许用更多 时间进行交易确认，而且还会提醒用户需要对他们的网络状况保持高度警惕，可以在出现 问题后的 1 分钟内提醒用户区块链网络上可能存在潜在的问题。DPOS 机制最早由 BM 应用在 BTS 项目中。BM 的其他明星项目 STEEM、EOS 同样沿用了这一 共识机制。DPOS 自诞生以来一直都是高性能、高效率、高灵活性的代名词，众多项目的 长期实践也证明了 DPOS 机制的这些优良特性。

（4） 高效治理

只要利益相关方批准，开发人员可以实施他们认为合适的任何更改。这项政策不仅可以保 护开发者，同时它还可以保护利益相关者，并确保没有任何人单方面控制区块链网络或让 区块链网络失控。硬分叉如同替换了 51% 的见证者，因此利益相关者参与的越多，其对应 的选举证人越多，那么整个系统的安全性就越高。

3.3最安全的会计模型UTXO

UTXO 代表 Unspent Transaction Output，即未花费的交易输出，它是比特币交易生成及验证的一个核心概念。交易构成了一组链式结构，所有合法的比特币交易都可以追溯到向前一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。UTXO 模型中，交易只是代表了UTXO 集合的变更。而账户和余额的概念是在 UTXO 集合上更高的抽象，账号和余额的概念只存在于钱包中。基于 UTXO（BTC）交易规则：1）除了coinbase 交易之外，所有的资金来源都必须来自前面某一个或者几个交易的UTXO，就像接水管一样，一个接一个，此出彼入，此入彼出，生生不息，钱就在交易之间流动起来了。2）一笔交易可以有多个输入或多个输出，但任何一笔交易的交易输入总量必须等于交易输出总量（加上过程中产生的总交易费用），等式两边须配平。

Bitcoin 的设计初衷是点对点的电子现金系统，在比特币中，每个交易消耗之前交易生成的 UTXO 然后生成新的 UTXO，账户的余额即所有属于该地址的未花费 UTXO 集合，Bitcoin 的全局状态即当前所有未花费的 UTXO 集合。在过去10 年中，比特币中使用的 UTXO 数据模型已被证明是创建稳定可靠数字货币的可靠方式。货币最重要的功能是成为一种交换媒介，而 UTXO 模型可以很好地做到这一点。UTXO 模型的核心思想就是保证已经写入的数据不可变，链式的UTXO基于这一核心思想，通过哈希指针连接不同交易的输入和输出，保证所有交易的合法性，实现 UTXO 的可溯源性。通过分叉继承这一点对 ZOZ

来说至关重要。UTXO 以币为中心，而不是以人为中心，资产便于监管和统计。UTXO 的这种以资产为中心的设计模式，是很适合 ZOZ 上面的资产管理。就在交易之间流动起来了。2）一笔交易可以有多个输入或多个输出，但任何一笔交易的交易输入总量必须等于交易输出总量（加上过程中产生的总交易费用），等式两边须配平。

3.3.1 UTXO 模型优点

（1）一次性

UTXO模型中的每一笔交易都是由多个交易输入组成的，这些输入其实就是 UTXO + 签名。每一个交易输出（Transaction Output）只有两种状态，已花费和未花费。如此确保了每 个 UTXO 仅能被花费一次，抗双花攻击能力极高。

（2）隐匿性

对比起账户模型，UTXO 更加私密。前文已知，每个 UTXO 都是“一次性”的。用户要是每 笔交易都换一个地址，那么就很难找到其中两个地址的相关性，保证了交易的隐匿性。如果还有需要进一步提高这种隐匿性，亦可以考虑使用环形交易签名对、交易要素混用等技 术手段。

（3）可靠性

在一个区块结构体中，previousblockhash 和 merkleroot 是两个最重要的字段，都起到 了防止交易信息被篡改的可能性。UTXO 模型的核心思想就是保证已经写入的数据不可变，链式的 UTXO 基于这一核心思想，通过哈希指针连接不同交易的输入和输出，保证所有交 易的合法性，实现 UTXO 的可溯源性。

（4）可并行性

UTXO 模型被公认具有潜在的可扩展性，因为 UTXO 允许交易的并行化处理。当一个交易发 送者发送两笔独立的交易时，花费独立的 UTXO 也可使交易用任意次序处理。这样可以使 一个人的资金分离，在保证隐私的同时具有并行处理交易的能力。比特币的 UTXO 模型经过了多年较为稳定的运行和测试，性能和安全性都有较大的优势。ZOZ 作为比特币的分叉币，采用 UTXO 模型，对于 ZOZ 来说是对其底层技术的一种继承。ZOZ 采用比特币核心代码为基础进行开发，也是较为谨慎的选择。UTXO 的安全性和并行交易特点也将给 ZOZ 带来更高效率的可能。

3.4 Omni 协议

Omni 协议是一套非常完整的协议实现，它完全利用了 UTXO 模型的特点，在不更改共识和协议的情况实现 Token 的管理。同时，Omni Layer 也秉承了开源运动的精神，采用了 MIT 许可证，是我们可以实现无许可创新的重要基础。ZOZ 通过 Omni 协议进行 USDTB 稳定币的发行。

3.4 智能合约虚拟机VVM

通过独立的虚拟机架构（ZOZ Virtual Machine，简称 VVM），ZOZ 能够实现智能合约。通过VVM实现智能合约的好处是，可以在需要时增加新的功能，运行多个不同区块链的虚拟机。VVM 智能合约体系能够支持更多编程语言。现阶段，ZOZ 发展 VVM 主要有两个阶段的计划。第一阶段，兼容以太访虚拟机（EVM）。因为EVM是智能合约最初的实现平台，VVM要能在代码微调的情况下，运行现有 EVM 上的智能合约。 第二阶段，ZOZ 计划动态调整 EVM 代码，使ZOZ 的代码更接近本机代码，并支持更多的编程语言。

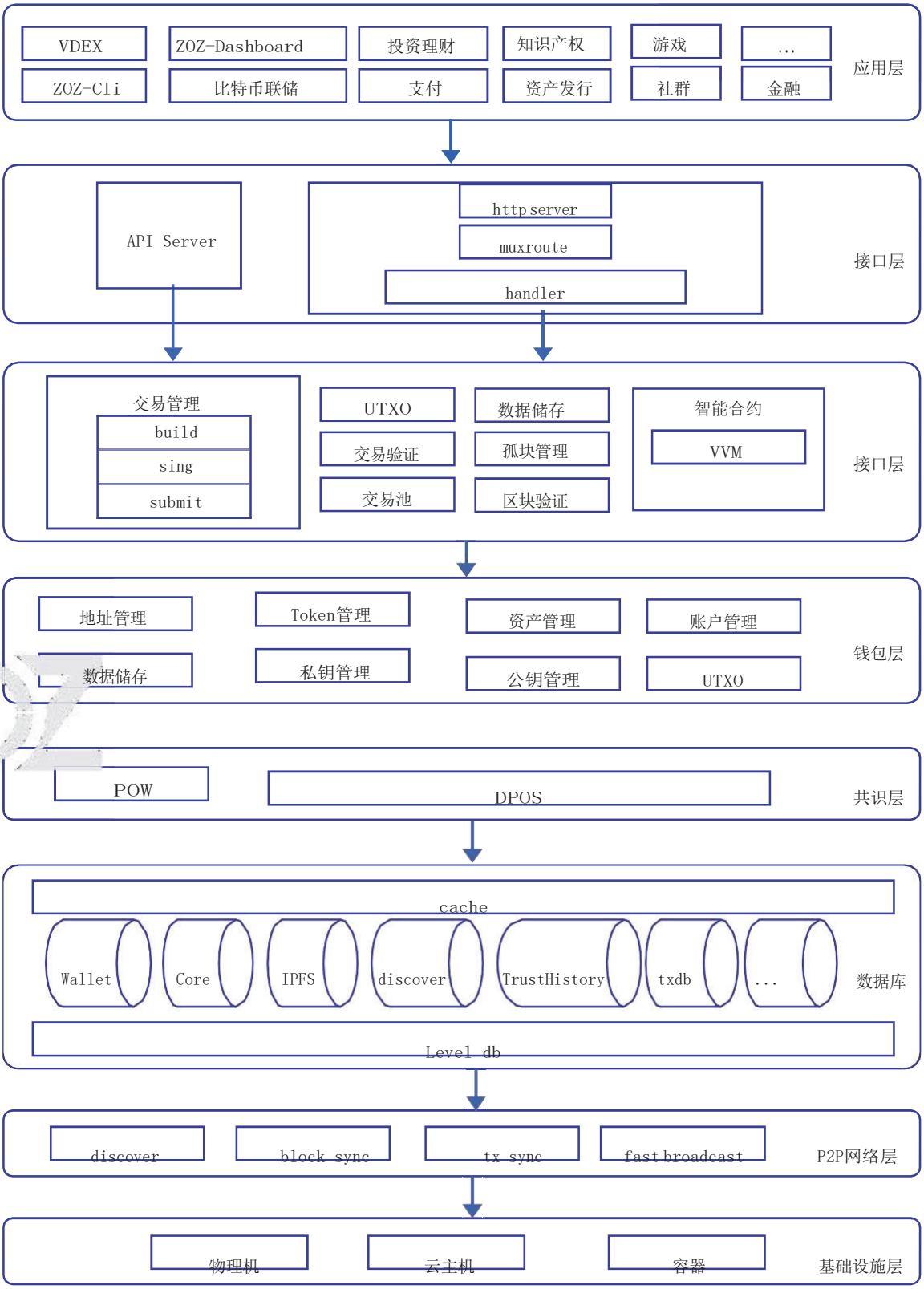
3.5 星际文件系统IPFS

IPFS 主要基于 Merkle DAG 的原理，引入了 “基于内容的寻址” 的概念。在请求特定资源时使用基于内容的寻址，用户无需指定位置，只需指定所需内容即可，每个文件都有一个唯一的哈希值，可以将其视为文件的指纹或标识。如果要访问特定文件，只需向网络询问具有指定哈希值的文件副本即可。请求完成后，IPFS 网络上的某个人将提供用户请求的资源。用户将下载该资源，并将副本保存到用户的 IPFS 缓存中，当另一个人来并请求相同的文件时，用户将能够通过哈希链接提供给他们。IPFS 是点对点的超媒体协议，可以让网络更快、更安全、更开放。它是一个面向全球的、点对点的分布式版本文件系统，试图将所有具有相同文件系统的计算设备连接在一起。

IPFS 与区块链技术的整合似乎是一个完美的选择。在区块链事务中使用 IPFS，可以放置不可变的永久链接。时间戳可以保护用户上传的数据，而无需将数据内容实际存储在链上，从而减少区块链膨胀，并为安全的脱链解决方案提供了一种方便的方法来帮助区块链扩展。

ZOZ 将增加对 IPFS 的支持。文件共享平台允许任何人上传由 IPFS 协议和 ZOZ 区块链支持的媒体文件。由于 IPFS 集成，ZOZ 文件用户可以上传比之前的 128m 或更低限制更大的文件，从而使平台能够支持更丰富的 DAPP 应用。可以将 200MB 文件上载到 IPFS，将文件的 IPFS 哈希链接保存在 ZOZ 上。ZOZ 平台将为上传到平台的 MP3，WAV，文本和图像文件添加文件预览支持。

3.6 ZOZ公链整体技术架构



（ZOZ 技术架构图）

ZOZ 公链技术架构如上图，从下至上一个分基础设施、P2P 网络、数据库、共识、钱包、内核、接口与应用等几个层次。基础设施可以是物理机，虚拟机（云） 以及容器都可以；P2P 网络层主要功能是节点发现、区块及事务同步、事务广播等；数据库层包含多种不同用途的数据库，最主要的有 Core，用来存放所有主区块信息与交易信息，还有 IPFS, IPFS 主要用来进行文件共享平台的支持，另外还有 Wallet 钱包数据库等；共识层主要是指 ZOZ 进行比特币硬分叉采用的 DPOS 共识算法，高效稳定；钱包层的功能主要进行公私钥及地址管理，同时对账户、Token 管理及 UTXO 维护等；再就是内核层，是整个 ZOZ 的核心， 最主要的功能是交易管理，交易构建、交易的签名及交易提交，同时包括智能 合约及其运行环境 VVM 等；接口层包括 API Server 服务，主要接收应用层工具的请求和处理请求，这一次主要针对 ZOZ 公链生态系统的开发人员；最后我们来说一下应用层，应用层包含两种用户交互工具 ZOZ-Cli 与 ZOZ-Dash- board, 以及各种 DAPP 应用。

ZOZ 生态应用主要有比特币联储、VDEX（去中心化交易所），其它的如投资理财、金融、支付、游戏、社群、资产发行及知识产权等。

《4》通证及主要应用场景

4.1 通证ZOZ与USDTB

4.1.1 ZOZ 通证

ZOZ 是 ZOZ 公链的原生币，ZOZ 的总发行量为1 亿枚，其中有 200万枚 ZOZ提供给B58的持有者，分发按空投的方式，运营与技术准备金 280万，交易所750万， 其余 8770万枚 ZOZ 将自动转入社区奖励池作为挖矿奖励。与 BTC 一样， ZOZ的特点是去中心化、匿名、只能在数字世界使用，不属于任何国家和金融机构，并且不受地域的限制，可以在世界上的任何地方兑换它。使用者可以用 ZOZ购买一些虚拟物品，比如网络游戏当中的物品，只要有人接受，也可以使用 ZOZ购买现实生活当中的物品。ZOZ 继承自 BTC，ZOZ的目的不是要取代 BTC，而是增强BTC的信用，改善比特币系统的不足，致力于实现区块链技术的现实应用。这包括以其革命性的特性既支持日常生活使用，又充当全球金融和支付系统的补充，同时通过智能合约的方式进行各种可编程经济，打造可编程的商业社会。ZOZ经济使用整个 P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付，同时确保了货币所有权与流通交易的匿名性。

4.1.2 USDTB稳定币

ZOZ 为了生态系统的稳定与繁荣，同时也为了应对通货紧缩的情况，推出USDTB（USD Offering）稳定币，USDTB 与美元 1：1 进行锚定，其发行机制是以比特币作为信用背书， 平台存储有多少比特币， 就会发行相应比例数量的USDTB。平台比特币存储地址公开，任何人都可以在平台上公开查询，存储的比特币价值大于发行的 USDTB， 不存在超发的情况。在没有风险的情况下USDTB 与美金 1：1 的锚定汇率使得它能被理解成法币变种，价格波动相对数字货币来说几乎为零。

4.2 VDEX(ZOZ Decentralized Transaction Platform)

在中心化交易所情况下，所有的用户用来参与交易的资金都保存在同一个地方。用户的资金直接存储在交易所中，它不仅负责匹配订单，并保持当前的订单簿和存款者的资金处于正确的状态。由于所有用户的私钥保存在一起，交易所系统可被侵入而导致所有用户失去所有资金。交易所使用去中心化的方式可以避免许多用户的资产卷入因入侵者带来的危险而引发的问题。为此ZOZ 推出去中心化的交易所VDEX(ZOZ Decentralized Transaction Platform)，管理个人代币资产 ，进行点对点代币交换。在 VDEX 下交易订单时，用户可以指定交易对象，仅允许指定的账号吃单。这一功能很适合双方直接交换不同代币，保证交易双方 “一手交钱、一手交货”。

USDTB 可作为 VDEX 的流通代币，可以作为交易媒介，支付相应的费用，当数字资产在 VDEX 上交易时作为相应的折扣或奖励等。VDEX 应用支持各种

以及各种虚拟货币的交换。未来，公链计划支持 USDTB 与合法虚拟货币之间的交换，以及大宗商品和其他实物资产或其相应数字资产的交换。我们计划基 于为 VDEX 开发的最高性能稳定 P4P 技术支持的基础技术开发超高性能平台，支持高速交换和清结算操作。

4.3 比特币联储BFR(Bitcoin Federal Reserve)

比特币是基于区块链技术的最成功数字资产之一，凭借不可篡改、去中心化等特点，实现极高的安全性，不容易被盗。但因为比特币的拥有只有特定的 秘钥来保管，所以可以说谁有了这个秘钥就相当于拥有了这个钱包里的所有比 特币资产。所以比特币的被盗事件也是层出不穷。早在 13 年 11 月份就有比特币被盗事件的发生，损失了约 4100 个比特币，当时价值约合 110 万美元。随后 12 月在 OKcoin 交易所上也发生了比特币的突然消失，损失达到 64 万人民币。14 年2 月，著名的 “门头沟” 事件爆发，当时世界上最大的比特币交易所被盗， 近85 万个比特币被盗一空，有人称这是监守自盗。3 月份，美国 poloniex 交易所发布了一个声明，损失了约 12.3% 的比特币。16 年 5 月，香港数字货币交易所 Gatecoin 也遭到了黑客的攻击，损失高达 200 万美元。还有除了这些被盗走的比特币，据 Chainalysis 表明 30% 的比特币可能已经丢失，而这种丢失的比特币是无论如何都不能找回的。这一系列事件的爆发，都说明了数字资产安全性上存在着巨大的漏洞，如何找到一个低成本、高效的解决措施成为了当务之急，数字资产托管成为了各方寄予厚望的选择。

资产托管服务，是现代金融不可或缺的重要一环。随着资产体量的增大、资产组合复杂度的提高等原因，越来越需要专业人士或机构提供服务在减少与拥有资产相关的运营负担的框架下进行，从而保管委托人价值数万亿美元的资产。随着数字资产投资的越来越兴起，以及一些交易所跑路、黑客攻击等事件的频繁发生，投资者对数字资产托管服务的需求也越来越迫切。为此 ZOZ 推出比特币联储 BFR（Bitcoin Federal Reserve）的应用，即用户可以将他们的比特币以数字资产托管的方式存储在比特币联储，平台会进行安全的保管，同时奖励相应比例的 ZOZ。比特币联储的数字资产安全是有保障的，首先平台自身会存储相当比例的比特币，如果用户的比特币在比特币联储丢失，平台将会以相应价值的 USDTB 进行赔偿。

《5》ZOZ 生态治理

5.1 区块链治理中待解决的问题

（1）消极贡献问题

此处所讨论的贡献积极性包括开发的积极性与投票的积极性。积极性与激励直接相关，尤其是经济激励与权力激励；在相应激励缺失的情况下，积极性问题 是大概率出现、且非常难以解决。在历史上，某些积极性问题被行业爆发 的整体环境带来的心理冲击所掩盖；而在区块链项目竞争加剧的未来，这一问题很可能大规 模爆发。贡献积极性是关乎区块链项目生死存亡的问题。例如比特币的开发者保守 化问题，导致比特币社区旷日持久的大争论（ 有关扩容等 ）； EOS的投票积极性问题导致 EOS主网推迟上线。如何重构区块链的激励机制， 平衡系统关键角色的权责义务，是区块链项目面对的至关重要的问题。

（2）角色对立问题

角色对立问题从某种意义上与消极贡献问题是同源的，皆可归因于激励这一治理要素。

在区块链生态中，普通用户、开发者、矿工，甚至与更复杂的委托权益人、受托权益人等，其权利义务存在较强的不对等性。例如在常见生态中，开发者与普通用户往往都不享有直 接经济激励，只能从 Token 价格的上升中获取收益，

但是开发者承担的责任缺远远大于普 通用户；理性的治理机制不可能指望开发者仅仅出于兴趣或责任来完成开发工作，因此开 发者有可能选择淡出社区或成为普通用户。

以上例子是一个权责不对等的情形，往往不至于导致角色严重对立；若考虑到利益冲突的 情形，就更易引发直接的对立。例如在常见的 POW 生态中，矿工有高交易手续费率、高 Token 价值的动机，而用户有降低交易手续费率、降低 Token 价值的动机（ 需注意：用户不一定是持币人 ），两者将完全处于对立面。历史上多次出现 POW 矿工恶意打包空交易、引发网络堵塞的案例，印证了利益冲突引发角色对立的逻辑。

（3）Token 流动性匹配问题

Token 流动性匹配问题是指在区块链生态体系中，Token 的分配、锁定、发行等影响流通 量的环节出现了失衡，导致 Token 价值的不正常波动，以及利益相关方受损的情形。Token 流动性匹配问题的本质是供需关系失衡。例如增发量过大的 Token 系统，可能引起系统内通胀、减损早期用户积极性的问题； Token 过度锁定与抵押的系统，可能引起价格失真、货币供给不足的问题。长期来看， 经济模型设计以及供需关系调节机制存在瑕疵的 Token 系统，尤其是整体平衡性弱、政策极端的系统，极易被自身的设计所反噬。

5.2 ZOZ治理定义

（1） 治理活动的核心：角色

角色可能包括：用户、受托权利人、委托权利人、开发者等

（2） 治理的基本要素：激励、协作机制

激励：决定组织（ 社区 ）形成的结构基础与运行驱动力。协

作机制：决定组织（ 社区 ）运作的效率。

（3） 治理的具体表现领域：Consensus、Voter、Voting Area、协议升级与变动。

Consensus：决定参与记账和出块的权利义务、决定 Block reward 利益的分配、是 形成链上权责的客观基础。

Voter：决定谁有权利参与与影响治理活动

Voting Area：决定链上治理涉及的领域，哪些事务可以被投票决定协

议升级与变动：如何决定协议的升级与变动，以及协议如何进行更新

5.3 系统角色定义

（1）用户

分为 ZOZ 用户、ZOZ 上建生态用户。原则上，凡持有 ZOZ 的用户，都可以通过 ZOZ 平台行使社区治理权利。

（2）委托权利人

ZOZ 社区是一个由 Token 控制并实施治理的系统；因此，ZOZ 的委托权利人是所有 ZOZ 持有者。ZOZ 持有者是 ZOZ 治理系统里面最基本、最广泛存在的参与者，也是 ZOZ 治 理的最终目的。持有者参与 ZOZ 治理系统的方法很简单，但是当众多持有者参与治理的 时候，他们的意愿会变成最终的行动指南。持有者可以将他们的投票权代理给节点。持有者选择他们信任的、理念相同的节点，将自 己的权限交由他们使用，大量持有者推选出的节点来执行用户的意志。持有者也可以选择 喜欢的钱包、矿池直接托管自己的代币，获取自己的收益。持有者可以将自己的议事权代 理给理事会，来参与到 ZOZ 未来发展的共同规划中。

（3）受托权利人

记账权的受托权利人是出块节点；议事权的受托权利人是理事。ZOZ 的节点与理事分别代表系统的记账权、议事权， 是 ZOZ 实现高效治理的核心。ZOZ 的节点与理事通过不同的方式进行选举，两者没有必然身份联系。

（4）开发者

开发者是 ZOZ 生态的基石；ZOZ 将把对开发者的奖励纳入 ZOZ 链上治理体系，直接升到协议层面的高度。ZOZ 系统就其形式来说是一个代码维持的程序，代码的质量决定了系统的性能，代码更新进度决定了它进化的速度。开发者是维护系统程序最重要的力量，程序的开发和维护因为特有的技术门槛， 所以不需要也不可能由全员来共同完成。所以需 要特定的开发者团队来完成开发和维护工作，并因此得到奖励——这样才能更好地激励开 发者的工作效率。

（5）链上 Oracle

在 ZOZ 生态系统中，链上 Oracle 将成为链上网关、去中心化交易所的重要角色。链上 Oracle 也属于 ZOZ 用户， 但不同于普通用户的是， 链上 Oracle 会以服务供方、资产承兑方等功能性角色的形式存在。

（6）钱包和矿池

钱包和矿池是由社区或者其他第三方做的应用，方便用户托管和使用他们的代币。它们可以用用户的代币来竞选节点和获取收益，但这些权力本身是属于原本的用户的，钱包和矿 池必须将这些权力再归还给用户，将获取的收益分给用户，按照用户的意愿进行投票。钱 包和矿池帮助用户实现他们应有的投票权，仅此而已。

（7）ZOZ DAO 基金

基金是由 ZOZ 社区领导者组建的，由理事会代为管理的，用以维护 ZOZ 系统发展的组织

5.4 ZOZ节点要求和选举规则

节点是 ZOZ 治理系统里最重要的一个环节，是直接参与 ZOZ 治理的代理者。节点的主要 任务是负责产生、确认、记录区块信息，忠诚的节点会得到区块奖励，而作恶的节点会失 去奖励。但是想要成为节点，不仅需要有足够性能的设备支持一个节点服务，保证产生区 块的准确率，同时还需要获得广大代币持有者的支持。

节点由用户选举产生，代表着选举他们的用户。节点在参与 ZOZ 链上治理的时候可以投 出重要的一票，但是如果违背了多数用户的意见，节点就会逐渐失去他的选票，并最终失 去成为节点的资格。

每个节点可以在自己的主页展示自己的技术、团队、理念等信息，吸引代币持有者的投票。作为最普遍存在的代币持有者，他们有权选出心中合格的， 符合自己诉求的节点，然后给 他们投票。每个代币持有者可以给信任的节点投票， 最多可以选择 51 个节点，每一个节点都会获得这个代币持有者所有的投票。

每个周期系统会自动统计选票数，选出获得投票数前 101 的节点候选人成为节点。

5.5 ZOZ理事会规则和条例

（1） 理事与理事会的定义

ZOZ 理事会（ 简称理事会 ）是 ZOZ 社区执行议事职能的专设机构。理事会负责主网协议 参数维护更新与日常社区事务管理。ZOZ 理事（ 简称理事 ）是代表 ZOZ 社区行使议事权职能并处理事务的人员，同时也是 ZOZ 协议以程式化形式法定的链上职能角色。

（2） 两权分原则

理事会与 DPOS 记账节点独立，不对记账以及记账节点的选举行为负责。

（3） 理事资质

任何 ZOZ 地址持有人可以成为节点。理事需要通过 KYC 认证，为有完全行为能力的自然人或组织团体。ZOZ 理事会初期设立 7 个理事名额；随着社区规模扩大，可以适当增加理事会规模，但不得低于 7 人。因为理事会特殊的重要程度和贡献度，理事会不仅需要有足够的技术水准，还需要有有一定的社区支持，了解社区的现状与民意。所以理事会的 7 名成员中暂定的 4 名由ZOZ

开发者社区推选出来，三名由社区内部竞选选举出。理事要求至少持有 20,000个ZOZ，理事也可以同时兼任节点。

（4） 选举方式

理事通过链上理事选举决定。该选举活动是一项独立的、不同于 DPOS 节点选举活动的行 为，于每季度举行一次。任何 ZOZ 持有人都可以在钱包内委托选票给理事候选人。选举结束后，根据委托选票的数量决定前 7 名候选人正式成为理事。在选举前，理事候选人应当正式在社区平台公开自身信息、治理计划等，已获得社区的公开支持。

（5） 理事的职能与权力

1) 决定 ZOZ 主网的可变参数；

2) 审核并讨论社区意见预案与开发者案；

3) 讨论涉及主网协议更新的事项；

4) 讨论并组织社区事务；

5) 讨论并决定当期 DAO 基金会划拨款项以及其他公共资金的安排；

6) 讨论 ZOZ 治理体系涉及的规则条款的变更。

（6） 经济激励

ZOZ 将在基金会中划拨特定数量的款项到理事会激励基金，作为对理事的经济补偿。(开发者奖励机制，推广运营活动奖励)

（8）社区全员投票机制

所谓社区全员投票，是指针对某项理事会决议，要求社区全体成员以 ZOZ 进行投票，并根据投票结果进行最终的民主式决议。

社区全员投票是特定情况触发的，而非法定发生。理事会决议对社区公开后， 社区成员可以在 ZOZ 钱包或项目主页中对决议进行反馈投票 （ 即可以以自身ZOZ投票，表达反对 ）； 如果某项决议获得 ZOZ 流通总量 1/5 以上选票反对， 就自动触发社区全员投票。社区全 员投票需经参与投票的 ZOZ 数量 67% 以上支持方可通过；对于触发了社区全员投票且没 有得到通过的理事会决议，当即自动失效。

5.6 ZOZ DAO 基金

基金是由 ZOZ 社区领导者组建的，由理事会代为管理的，用以维护 ZOZ 系统发展的组织。由于整个 ZOZ 的发展更像是一种公共事业，系统升级能惠及每一个参与者，然而每个个 体都不愿意为此付费——如果其他使用者可以免费地搭便车的话。这样就需要一个组织，他们向所有参与者收取费用 （ 并不是直接收取，而是从其他的代币中收取部分比例 ），用 来支持系统的升级维护。基金的角色在整个治理中是极为重要的，但并不是统治性的，基 金会同样只是用户权利的代行者，帮助整个系统维持进化。

我们将从长期无人确权的 ZOZ 池中拿出一部分，分批释放给基金会。基金会负责奖励对 ZOZ 生态系统做出贡献的人，增加所有系统参与者的贡献动力，使得整个生态系统形成 一个闭环。基金会属于整个 ZOZ 社区， 日常任务由 ZOZ 理事会代为管理，重大事项则由 所有参与者共同决定。基金会将负责下列具体事由的奖励发放：

理事会奖励：为理事会作出的日常管理工作给予的奖励

开发者奖励：奖励开发者做出的代码升级或者新协议的开发

社区贡献：奖励社区成员给出的议案、资源或者其他贡献

其它奖励

每一次释放到基金会之前，会由基金会预先发起议案，确定释放代币的数量 和时间，并由理事会投票，获得赞同后推行方案。

5.7 ZOZ 协议的自我进化

ZOZ 协议是一个自我进化的协议，在现行版本的基础上，由所有参与者共同决策共同推行升级。社区的成员可以将想法交给理事会，可以是管理体系的改动，可以是未来发展路线，甚至是一个简单的建议。只要出想法，理事会将考虑是否为好的建议，是否值得 升级，然后在将建议反馈给开发者社区。

《6》愿景

我们的愿景是创建一个比特币白皮书所倡导的点对点的电子现金系统，为用　户提供方便、快捷、安全的服务。

我们的目标：

建立一个强大而负责任的社区；

创造一个前景光明的高端货币；

建立一个光明前景的比特币联储，增强 BTC 的信用；

创造一个稳定的去中心化加密数字资产交易所；

创建支持加密货币的环境，避免未来的争议；

使其广泛采用开源和去中心化；

用户可以完全匿名，无需为其交易或持有 ZOZ 而共享其身份。

《7》路线图

ZOZ 团队已经为未来的愿景和路径提供了明确的支持，以支持网络和参与社区的用户。我们已经计划并制定了我们的路线图，并将其视为数字货币和去中心化的未来。

2019 年 Q6
ZOZ 项目组成立，项目架构设计

2019 年Q7
白皮书撰写，筹备资源

2019 年Q7
测试网开发完成，进行数据上链测试

2019 年 7 月
筹备启动各地路演

2019 年7 月
Demo app 上线

2019 年 7 月 上线交易所

2019 年 9 月
王网上线。支持开发者链上开发

2019 年11 月 钱包上

2019 年 12 月
第一款官方 DAPP ZOZ 宠物游戏上线，
激活存量数据，链上用户高达 1500 万

2019 年12 月
第二款官方 DAPP 比特币联储上线
链上用户达 5000 万，开始引流企业用户

2020 年 Q1
第二款官方 DAPP VDEX 上线
链上用户大 1 亿

2020 年Q2
第四款官方 DAPP 金融端上线

2021 年
整合生态，形成基于用户生态数据
的完整数字经济国

《8》法律

在过去一年中，美国，新加坡，中国，瑞士和德国的金融当局收紧了对加密代币众售的政策或发出警告，因为通证越来越多地被归类为证券。ZOZ 通证销售承认并将遵守几个主要司法管辖区的安全法规，并遵守 KYC 和AML 法规。详细地说，这意味着如下几点：

8.1 证券法规

请仔细阅读本部分。如果您对您应采取的行动有任何疑问，我们建议您咨询 您的法律，财务，税务或其他专业顾问。

本文档中列出的信息可能并不全面，并不代表合同关系的任何要素。本文档不代表投资，税务，法律，法规，财务，会计或其他建议，也不能作为可能参与ZOZ 生态系统支持和开发的唯一理由。在做出决定之前，潜在买方必须咨询其法律，投资，税务会计和其他顾问，以确定此类交易的潜在利益，限制和其他后果。

公本文件的任何部分均不是发行招股说明书或要约，其目标不是作为证券要约或在任何类型的司法管辖区内以证券形式进行投资的要求。本文档未按照任何司法 管辖区的法律或法规编制，该法律或法规禁止或以任何方式限制与数字代币或 其使用的任何形式有关的交易。

8.2 KYC和AML

了解用户的客户（KYC）和反洗钱（AML）法规在技术细节方面因国家 / 地区而异，但它们都需要根据恐怖主义，禁运和政治暴露人士（PEP）的各种清单对客户的身份进行核实和核对。ZOZ正在与专业服务提供商实施此流程。在向人群进行投融资的流程中，身份验证和 AML 检查之后将检查投资者类别。如果仍有疑问，则会进行人工调查。从加密到法定货币的交换将由受监管的经纪人 / 交易所进行，银行将获得 KYC 和 AML 报告。

8.3公司治理

公司准备聘请一家国际会计师事务所来评估 ZOZ 通证经济模型及流程，审计其会计，并提供有关其如何遵循其指导方针的报告。

《9》常见问题

什么是区块链？

区块链是最简单的形式，是一种独立，透明，安全和永久的数据库，共存于多个地点，并由社区共享。

区块链的神奇之处在于数据库不存储在一个地方或由任何特定的主体管理。相反，它被称为分布式，存在于多个计算机或节点上，同时以任何有兴趣的人可以维护它的副本的方式。

此外，验证系统提供安全性，确保没有人可以篡改数据库中的记录。旧事务将永久保留，新事务将不可逆转地添加到分类帐。网络上的任何人都可以检查分类帐并查看与其他人相同的交易历史记录。

区块链涉及哪些领域？

区块链涉及到的领域比较杂，包括分布式、存储、密码学、心理学、经济学、 博弈论、网络协议等。从技术角度讲，区块链核心技术包括：分布式、共识机制、 密码学、Merkle Tree、智能合约等。

区块链的发展状况？

区块链发展如火如荼，世界各国的政府，企业，创业公司纷纷布局，唯恐错过这场足以改变世界经济格局的技术。世界经济论坛在一份报告中称，科技革新在过去 50 年里大幅推动了金融服务业的变革。而区块链可以算是开启下一次科技革命的领导型技术之一。然而，目前没人可以预知区块链的未来发展前景，正 如在上世纪 90 年代初我们无法预测互联网的未来一样。但是可以肯定的是，这项技术将会对世界经济发展产生巨大的影响。区块链就像当年的互联网，正处于 获得广泛接纳和应用的临界点上。区块链提供一种在不可信环境中，进行信息与 价值传递交换的机制，是构建未来价值互联网的基石。

什么是加密货币

加密货币是一种使用密码学原理来确保交易安全及控制交易单位创造的交易介质。加密货币是数字货币和虚拟货币使用密码学及数字散列而成并与智能合约 的绑定之下的新型通证。比特币在 2009 年成为第一个去中心化的加密货币，这之后加密货币一词多指此类设计。

什么是比特币？

比特币是一个共识网络，促成了一个全新的支付系统和一种完全数字化的货币。它是第一个去中心化的对等支付网络，由其用户自己掌控而无须中央管理机构或中间人。从用户的角度来看，比特币很像互联网的现金。比特币也可以看作是目前最杰出的三式簿记系统。

谁创造了比特币？

比特币是第一个实现了 “隐秘货币” 概念的货币。1998 年，Wei Dai 在 cypherpunks 邮件列表中首次阐述了 “隐秘货币” 的概念，即：一个采用密码学原理控制货币的发行和交易、而不是依赖于中央管理机构的全新的货币形态。2009 年，中本聪（Satoshi Nakamoto 化名）在 cryptography 邮件列表中发表了第一个比特币规范及其概念证明。2010 年年底，中本聪离开该项目，关于他的身份没有透露太多。此后，众多开发人员致力于比特币的项目，比特币社区迅速成长起来。 中本聪的匿名身份经常会引起毫无根据的忧虑，其中很多是与比特币开放源代码特性的误解有关。比特币的协议和软件都是公开发布的，世界各地的任何开发人员都可以查看其代码，或者开发他们自己修改过的比特币软件版本。 就像目前的开发人员，中本聪的影响仅仅局限于那些他做出的被其他人采纳的改 动 ，因此，中本聪并没有控制比特币。那么，在今天，关于比特币的发明者的身份问题可能和纸张发明者的身份问题一样。

谁在控制比特币网络？

没有谁拥有比特币网络，就像没有人拥有电子邮件背后的技术一样。比特币由世界各地所有的比特币用户控制。开发者可以改善软件，但他们不能强行改变比特币协议的规则，因为所有的用户都可以自由选择他们想用的软件。为了相互之间保持兼容性，所有用户也需要选择遵循相同规则的软件。只有所有用户达成完全一致的共识，比特币才能正常地工作。因此，所有的用户和开发者对接受和保护这一共识很有动力。

比特币是如何运作的？

从用户的角度来看，比特币就是一个手机应用或电脑程序，可以提供一个个人比特币钱包，用户可以用它支付和接收比特币。这就是比特币对于大多数用户 的运作原理。 在幕后，整个比特币网络共享一个称作 “块链” 的公共总帐。这份总帐包含了每一笔处理过的交易，使得用户的电脑可以核实每一笔交易的有效性。 每一笔交易的真实性由发送地址对应的电子签名保护，这使得用户能够完全掌控 从他们自己的比特币地址转出的比特币。另外，任何人都可以利用专门硬件的计算能力来处理交易并为此获得比特币奖励。这一服务经常被称作 “挖矿”。你可以查阅专用页面 和 原始论文来了解更多有关比特币的信息。

真的有人使用比特币吗？

是的，越来越多的企业和个人在使用比特币。这既包括像饭店，公寓和律师事务所那样的传统企业，也包括像 Namecheap，Overstock.com，和 Reddit 这样的流行在线服务。虽然比特币仍然是一个相对较新的现象，但它发展迅速。2013 年 8 月底，流通中的比特币总值超过了 15 亿美元，每天都有价值数百万美元的比特币在进行兑换。

还有其他加密货币吗？

比特币是最大和最成熟的加密货币。截至 2020 年 1 月 7 日，互联网上有 1384 种加密货币。

政府对加密货币的态度是什么？

在最极端的层面，中国和韩国都禁止在自己的市场上使用加密货币对普通民众进行融资。就中国而言，值得注意的是，加密代币首轮融资和加密货币的去中心化性质削弱了中央政府对国内经济各方面的监管程度，其中已有一些欺诈活动。另一方面，在俄罗斯，莫斯科证券交易所正在开发基础设施以允许加密货币的合法交易，而在爱沙尼亚，政府正在考虑使用其本国货币的加密经济体系建设。

许多其他监管机构采取了更多的观望态度：

在新加坡，MAS 将加密货币归类为资产，虽然交易不受监管，但 KYC 和反洗钱都受到监控。

瑞士金融市场监管局已将加密货币列为资产，但公司不需要特定许可或批准 来运营。

在美国，美国证券交易委员会已决定，如果通证销售代表证券销售，则此类加密代币融资行为应受联邦和州法律的约束，尽管他们也在考虑更灵活的立法。

加密货币的积极因素是什么？

为没有其他现成资金的有前景的项目或任何广泛接触的平台提供机会。

作为一种去中心化的货币，加密货币避免控制货币流动的中间人以及与该货 币内的交易相关的费用。

避免通过其他更成熟的筹款方式随着时间推移而产生的不必要的文书工作，其中大部分都没有什么实际价值。

《10》免责声明

请仔细阅读本 “通知和免责声明” 部分的完整内容。此处不构成法律，财务，商业或税务建议，您应该在参与任何与此相关的活动之前咨询您自己的法律，财务，税务或其他专业顾问。

白皮书仅用于一般信息目的，不构成招股说明书，要约文件，证券要约，投资邀请或任何产品，项目或资产（无论是数字还是其他）的要约。此处的信息可能并非详尽无遗，并不意味着合同关系的任何要素。无法保证此类信息的准确性或完整性，也不保证或声称提供此类信息的准确性或完整性。如果白皮书包含从第三方来源获得的信息，则基金会，分销商和 / 或ZOZ 团队尚未独立验证此类信息的准确性或完成情况。此外，白皮书可能随项目发展进行更新或更正与此相关的文本文件。

本白皮书的任何内容均不构成基金会，分销商或团队出售 USDTB 或 ZOZ（如本文所定义）的任何要约，也不得将其或其任何部分或其陈述的事实构成基础， 或依赖于任何合同或投资决定。本白皮书或本网站中包含的任何内容均不得或可 能作为对 ZOZ 平台未来业绩的承诺，代表或承诺。就任何买卖 ZOZ 或 USDTB 而言，经销商与您之间的协议仅受该协议的单独条款和条件的约束。

发行和销售 ZOZ 或 USDTB 的经销商应为基金会的附属机构。所有贡献将用于促进，促进研究，设计和开发以及倡导基于区块链的平台，该平台将连接全球黄金购买者 / 持有者以及行业用户，创造可靠且有限的黄金代币供应，这些数字资产代表了获取实物黄金的权利，从而为全人类创造了一个可靠和透明的通用价值交换平台，该平台基于最古老的实物产品（黄金）和最前沿的未来技术（区块链技术）。基金会， 经销商及其各个附属公司将开发， 管理和运营 ZOZ 和USDTB 平台。

基金会，分销商和 ZOZ团队不会也不会声称对任何实体或个人作出任何陈述，保证或承诺，并且不作任何声明（包括但不限于对其准确性，完整性，及时性或可靠性的保证）。白皮书或网站的内容，或基金会或经销商发布的任何其他材料）。 在法律允许的最大范围内，基金会，分销商，其关联公司和服务提供商不对任何类型的侵权，合同或其他方面的任何间接，特殊，偶然，后果性或其他损失承担责任（包括但不限于，因使用白皮书或本网站或任何其他公布的材料而导致的任何责任，收入，收入或利润损失，使用或数据丢失等引起的任何责任。或其内容（包括但不限于任何错误或遗漏）或以其他方式产生的内容。ZOZ 或 USDTB 的潜在购买者应仔细考虑和评估与 ZOZ 或 USDTB 代币销售，基金会，分销商和 ZOZ 团队相关的所有风险和不确定性（包括财务和法律风险和不确定性）。

白皮书和网站中列出的信息仅供社群讨论，不具有法律约束力。任何人不得就收购 ZOZ 或 USDTB 订立任何合约或具约束力的法律承诺，且不得在白皮书或网站的基础上接受任何虚拟货币或其他付款方式。ZOZ 或 USDTB 的买卖协议和

/ 或继续持有 ZOZ 或 USDTB 的协议应受一套单独的条款和条件或令牌购买协议（视情况而定）规定，并规定此类购买条款和 / 或或继续持有 ZOZ 或USDTB（条款和条件），这些条款应单独提供给您或在网站上提供。如果条款和条件与白皮书或网站之间存在任何不一致，则以条款和条件为准。

没有监管机构审查或批准白皮书或网站中列出的任何信息。根据法律，监管要求或任何司法管辖区的规则，不会或将会采取此类行动。白皮书或网站的发布， 分发或传播并不意味着已遵守适用的法律，法规要求或规则。

此处列出的信息仅是概念性的，并描述了要开发的 ZOZ 平台的未来发展目标。白皮书或网站可能会不时修改或更换。没有义务更新白皮书或网站，或向收 件人提供超出此处提供的任何信息的权限。

此处包含的所有陈述，新闻稿中的陈述或公众可以访问的任何地方以及基金会，分销商和 / 或ZOZ 团队可能作出的口头陈述均可构成前瞻性陈述（包括有关意图，信仰的陈述或市场条件，业务战略和计划，财务状况，具体规定和风险管理实践的当前预期。谨请阁下不要过分依赖这些前瞻性陈述，因为这些陈述涉及已知和未知的风险，不确定性和其他可能导致未来实际结果与此类前瞻性陈述所描述的实质性不同的因素，以及没有独立第三方审查任何此类陈述或假设的合理性。这些前瞻性陈述仅适用于白皮书中提出的日期，基金会，分销商以及ZOZ团队明确表示不对这些前瞻性陈述的任何修订发布任何责任（无论明示或暗示）反映此日期之后的事件。

在此使用任何公司和 / 或平台名称或商标（除了与基金会，分销商或其附属公司有关的那些）并不意味着与任何第三方有任何关联或认可。白皮书或网站中 对特定公司和平台的引用仅用于说明目的。

白皮书和本网站可能被翻译成中文以外的语言，如果中文版本与白皮书的翻 译版本之间存在冲突或含糊不清，则以中文版本为准。您承认您已阅读并理解白 皮书和中文版本。

《11》参考文献

1、 Maymounkov, P. and Mazieres, D. (2002). Kademlia：a peer-to-peer information system based on the XOR metric, International Workshop on Peer-to-Peer Systems, 53-65.

2、 Naor, M. and Rothblum, G. N. (2009). The Complexity of Online Memory Checking. Journal of the ACM (JACM), 56(1).

3、 Back, Adam, et al. "Enabling blockchain innovations with pegged sidechains." URL： http：//www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged- sidechains (2014).

4、 Bentov, I., Gabizon, A. and Mizrahi, A. (2016). Crytocurrencies without Proof of Work. International Conference on Financial Cryptography and Data Security. 142-157.

5、 Kshemkalyani A D, Singhal M. Distributed computing：principles, algorithms, and systems[M]. Cambridge University Press, 2011.

6、 朱立，《详解最近大热的闪电网络、雷电网络和 CORDA》，2016 年 6 月 12 日，http：//www.8btc.com/ln-rn-corda

7、 马龙，《柔支付：基于 2-of-2 多重签名实现的类闪电支付》，2016 年11 月6 日， http://idgui.com/RouPay.com

8、 Vitalik Buterin，翻译 Hell_Q，《中本聪的天才：比特币以意想不到的方式躲开了一些密码学子弹》，2013 年10 月28 日，http://www.8btc.com/satoshi-is-genius-unexpected-ways-in-which-bitcoin-dodged-some-cryptographic-bullet

9、 Bandara, H. M. N. D. and Jayasumana, A. P. (2012). Collaborative Applications over Peer-to-Peer Systems Challenges and Solutions. Peer-to-Peer Networking and Applications. arXiv：1207.0790.

10、中本聪，《比特币：一种点对点的电子现金系统》，2008 年11 月1 日，http://www.8btc.com/wiki/bitcoin-a-peer-to-peer-electronic-cash-system

11、 LBTC White Paper (English Version) ，2019 年 4 月 17，https://lbtc.io/web/viewer.html