ZG BLOCKCHAIN

智能资产发行交易生态公链

PUBLIC BLOCKCHAIN FOR THE ISSUANCE AND TRANSACTION OF SMART ASSETS

目 录

1. 背景

1.1 区块链技术

1991 年， Stuart Haber 和 W. Scott Stornetta 第一次提出关于区块的加密保护链产品，随后分别由 Ross J. Anderson 与 Bruce Schneier & John Kelsey 在 1996 年和 1998 年发表。2008 年 10 月，在中本聪(Satoshi Nakamoto)的原始论文《比特币：一种点对点的电子现金系统》中，出现了“区块”和“链”两个关键词，而后该技术被广泛称颂后被合称为区块链。比较确切的说，区块链诞生自中本聪团队发明的比特币。2009 年以来，出现了各种各样的类比特币的加密货币或虚拟资产，都是基于类似的公有区块链。

区块链技术是一种分布式的数据流通和共享的技术方案，利用去中心化方式维护一个可信数据账本，因此区块链技术也被称为分布式总账技术（DLT，Distributed Ledger Technology）。区块链技术在技术层面上解决了多方信任的问题，构建了一个可信的价值自由流通的基础设施。

区块链起源于分布式数据存储、点对点传输、共识机制、加密算法等计算机技术，是一种全新的应用模式和协议。一般说来，区块链系统由数据层、网络层、共识层、激励层、合约层和应用层组成。 其中，数据层封装了底层数据区块以及相关的数据加密和时间戳等基础数据和基本算法；网络层则包括分布式组网机制、数据传播机制和数据验证机制等；共识层主要封装网络节点的各类共识算法；激励层将经济因素集成到区块链技术体系中来，主要包括经济激励的发行机制和分配机制等；合约层主要封装各类脚本、算法和智能合约，是区块链可编程特性的基础；应用层则封装了区块链的各种应用场景和案例。该模型中，基于时间戳的链式区块结构、分布式节点的共识机制、基于共识算力的经济激励和灵活可编程的智能合约是区块链技术最具代表性的创新点。

区块链技术诞生初期主要被应用于私人数字货币领域，进入 2.0 时代落地了防伪溯源、数据存证、保险、供应链金融、慈善公益等领域的试点应用，3.0 时代区块链被期许作为新时代大规模协作商业应用的信用平台。根据调研，目前主流的区块链体系都在解决区块链上交易速度、安全性、智能合约、跨链及侧链等技术问题，出现了例如 EOS、RSK、LSK、NEO 等公有链项目，也出现了基于区块链概念打造的新型技术形态-DAG 技术，这种技术

甚至摒弃了区块的概念，不过仍是围绕区块链倡导的“分布式账本，去中心化网络”的思想在发展。整体来看，2017 年以来，区块链技术的发展呈现百花齐放的姿态。

ZG BLOCKCHAIN 团队认为，目前公有区块链体系的发展依然是行业的重中之重，众多应用型项目的商业化发展离不开高性能的底层公有链技术，也离不开完善、简洁易用的商业应用基础设施。ZG BLOCKCHAIN 团队在区块链的技术领域选取了智能资产的高并发撮合匹配作为技术的突破口，试图解决区块链上高并发问题，以实现实体资产与数字资产的结合，实现实时快速的交易，这种技术理念在传统互联网领域已经得到实践和证实，也将首次在 ZG BLOCKCHAIN 公有链中应用。

1.2 ZG BLOCKCHAIN 的由来

区块链数字资产上链是区块链链接实体经济最为核心的一个技术环节，一直以来，围绕资产上链的问题争议颇多。那么到底什么是资产上链呢？我们可以把资产上链看作是一种“登记制”，即把资产的信息、权益和流通映射到区块链上。通俗来讲，就是用区块链技术去登记资产的信息、产权以及交易方式，从而把资产与区块链上的 Token(通证)进行一个有效连接。

由于现实中的资产流通存在登记确权等种种问题，使得人们想要过户个房子或者专利过程都异常复杂。资产上链就是要利用类似于比特币等通证的特性来解决这些问题，其核心为将链下资产映射到链上。资产上链主要是解决交易过程中存在的流转记账和防伪溯源的问题。但是如果仅仅是将资产登记在链上，而没有后续的交易、结算、支付上的便利性，那么这种资产上链的意义有限，与互联网时代把资产登记到网上，比如把专利登记到专利局，房产登记到房产局并没有本质区别。登记是为了确权，确权是为了交易，交易天然就是资产的属性。举例说明，由极客钱包技术支持的头道原浆白酒资产上链项目，借助区块链本身的算法达到去信任效果，增加了商品的交易便利性，降低了商品流通的成本，同时，还赋予了交易过程中的金融属性。购买头道原浆白酒 Token(通证)的持有者，可以选择提取实物，也可以在价位合适的情况下在二级市场上再次交易获利，还可以转赠他人。如在一年内即不提取实物也没有二次交易，Token(通证)发行方可以支付一定的资金使用利息。所以说，资产上链给实体经济扩宽了交易场景还增加了融资的金融属性。

在现行经济结构下，资产上链的优势很明显，结合区块链最突出的特点——去中心化、点对点网络、分布式账本、时间戳、信息透明且不可篡改等，资产上链将会有以下几个优势：

（1）消除信任问题，降低沟通成本

区块链的本质是去信任，通过技术来解决两者之间的信任问题。信任问题一旦解决，陌生人之间的交易就会变得更为容易，整个资产流通系统的效率随之增加，不需要周边熟人介绍或者第三方中介平台进行“牵线搭桥”。区块链上的每个节点都保存了数据副本，单个节点试图修改链上资产信息的为可被有效防范，从可以确保链上资产信息的真实有效性，降低信任险。

（2）去中介，降低交易成本

传统的资产交易过程中，涉及的环节非常复杂。除了需要政府等权威部门进行资产认证或背书外，还需要结算系统来进行结算，需要银行来处理资金转账，政府相关部门进行资产交割转让等等，用户在这过程因此付出了较大的成本。通过区块链的方法，整个交易流程完全在链上完成，所有数据都同步在全网各个节点上，实时更新交换数据，使得整个过程更加清晰透明，无需外部第三方机构的介入，不仅成本大幅度降低，效率也显著提高。

（3）提高资产流通效率

传统资产交易流通平台相互孤立，各自为营，这就导致了整体的用户规模受限，从而导致资产流通的效率低。在区块链领域也会出现同样的问题，目前各主链之间也相互独立，但是可以通过跨链技术，实现各链之间相互连通的状态，各链用户和流通资产相互共享，从而促进了整体的资产流通效率。

（4）防止资产“双花”

区块链的跨链技术，可以有效的将各个主流链连接起来，各链之间的信息实时同步，有效解决各链之间的价值孤岛的问题，并给可以有效避免用户同一个资产分别在不同的链上进行上链交易的弊端，有效监测和杜绝同一资产在多条链上的双花问题。

虽然资产上链有诸多好处，对于区块链智能资产去中心化发行交易管理而言，诸多先行者做过的实践也印证了一些存在的问题，最为核心的技术问题是资产交易管理的效率和质量问题。目前比较知名的数字资产发行管理公链 Binancechain 目前在专注于解决上链的问题，没有注重交易效率的提升以及 DAPP 的友好支持度。目前比较主要的去中心化交易协议包括：0x、Kyber、Airswap，还有 stex、Loopring、Etherdelta 等。除 Etherdelta 早期有一定交易规模外，大多数都还处于早期开发阶段，也就是说距离成熟的模式还需市场的探索。仅从目前用户体验来看，Etherdelta 跟中心化交易所差距还很远。

其实,从用户需求的角度,交易所是不是用区块链,是中心化还是去中心化都不是核心,核心是交易体验和资金安全。

首先，速度要快，不用等太长时间；其次，要有交易量，可以快速成交；再次，是有合适的成交价格；最后是资金安全和可信任；当然这四者在每个人心目中的排序是不同的。中心化交易所目前在前三个方面有绝对优势,比如中心化交易所在撮合交易对象和完成交易结算方面都具有速度优势，都是在链外的订单簿匹配和链外结算。

而目前全球去中心化交易所主要有三类：一类是 relayer 托管订单簿的模式，以 0x 为代表；一种是储备池的模式，以 kyber 为代表；还有就是 p2p 交易协商的模式，以 Airswap 为代表。

0x 是一个可以在以太坊区块链上进行 ERC20 代币对等交易的开放式协议。该协议旨在成为通用开放标准，作为可与其他协议组合的基本模块，用以驱动越来越复杂的区块链应用程序。由于它使用的是以太坊的智能合约系统，因此可以作为各种 dApps 的共享基础架构。而从长远来看，开放式技术标准相比封闭模式具有更大的优势，随着每个月有更多的资产在区块链上被代币化，也有更多的 dApps 需要使用这些不同的代币，开放式标准也因此变得更加重要。此外，由 dApps 耦合到其底层协议所导致的智能合约冗余也是未来区块链协议开发的主要障碍，因此在标准化之余，我们还需要一个合适的解耦方式。0x 协议试图将信息交换功能从应用层拉到协议层，推动 dApps 之间的互操作性。

0x 协议中，参与交易的用户通过 ERC20 协议将自己的代币委托给以太坊上的去中心化交易所智能合约。订单的 Maker 将自己的订单请求在链下广播，订单的 Taker 在通过链下 Order 转发服务找到理想的订单，并向区块链发出请求，并最终完成交易。

Kyber 是个专注于链上资产去中心化互换的交易所。它的目标是解决中心化的风险、即时交易、交易品种繁杂等等问题。但在具体实现上它和传统交易所有很大的不同，它强调的是基于代币储备库的兑换而不是挂单交易的处理。

Kyber 引入了储备贡献者的角色为代币储备库提供代币，引入了储备库管理者来管理运营储备库。每个储备库都由对应的储备管理者来运营，由其负责周期性设置储备库兑换率，并利用储备库对普通用户提供的兑换折价来获取利益,该利益由储备管理者和储备贡献者共同分享。储备库与储备库之间是互相竞争关系，以保障给用户提供最优的兑换价格。KyberNetwork 为储备库管理者提供平台,并设有 KyberNetwork 的全局运营者对所有储备库、储备库管理者进行集中管理维护。

Kyber 基于储备库的基础上支持了去中心化的各类自由兑换的即时支付 API，强调了流动性保证。但这些也是有前提的，就是代币要有充足的储备库。

P2P 模式主要是直接进行点对点的价格协商，可以做到个性化沟通，但因为有协商，找交易方,协商价格和数量等步骤,交易速度也会随之变慢,也存在如何确定交易价格的问题。其他模式的去中心化交易所,包括订单簿模式和储备池模式都是以来订单簿价格或储备池价格做参考。当然，前提是交易量要足够，否则很难有一个可参考的最优交易价格。而 P2P 模式一般来说，会依赖第三方，比如大的中心化交易所价格作为参考。

Swap 采用了 indexer 来匹配交易双方，Oracle 提供价格建议，最后通过智能合约完成结算，速度核心在于协商时间，当然这也是它优点，可以做到个性化。

Loopring 是类 0x 的去中心化的交易协议，从整体思路上与 0x Project 是非常类似的，也主要是受到 0x 的启发。Loopring 与 0x 一样的地方是，链上智能合约负责资产托管、实施撮合成交，链下负责订单匹配。具体技术实现上的不同点，其一是，Loopring 将撮合扩展到了多币种多订单上，既白皮书所说的链上交易环路撮合技术，鼓励交易所匹配最大折扣的成交路径，为用户节省交易成本的同时交易所也有利可图。但另一方面也增加了智能合约的复杂度和以太坊交易的执行成本，在实际应用中效果如何还有待观察。其二是，设计了经济激励机制，提倡交易所从交易手续费为主的模式转变为成本节约分润为主的模式。其三是，交易所之间是互相平等竞争的关系，用户的订单可以选择发送给一个或多个交易所，甚至为了快速达成，可以发送给全网所有的交易所，尽管这样会给市场深度带来好处，让成交更快更有效，但对于交易所而言也会带来抢单的问题，因为理论上大部分交易所对于链上订单合约的变更的感知速度是一样的，因此对于同样的订单匹配，不同交易所就会各自发送相同的撮合请求到链上，造成大量无效的撮合交易。

综上而述，从目前来看，还没有一个去中心化交易系统是完美的，都有各自的优缺点，都需要在实践中不断模式完善。

ZG BLOCKCHAIN 团队在 2015 年就关注去中心化交易及智能合约，并在 2017 年启动 ZG BLOCKCHAIN 区块链智能合约平台开发。结合团队在商业场景领域的积累以及对技术商业化的理解，ZG BLOCKCHAIN 初始的想法就是要建立商业易用的智能资产发行交易生态平台，让资产上链以及流转更友好。

2. ZG BLOCKCHAIN 的定位

ZG BLOCKCHAIN 定位于提供智能资产交易发行整体解决方案，依托 ZG GROUP 集团生态打造去中心化交易生态圈。

我们可以把资产上链看做是一种“登记制”即把资产的信息、权益和流通映射到区块链上。通俗来讲，就是用区块链的技术去登记资产的信息、产权以及交易方式，从而把资产与区块链上的 Token(通证)进行一个有效连接。

ZG BLOCKCHAIN 解决了资产上链后几个主要的问题：

（1） 通过丰富的智能合约组件，完成链上资产的分类管理

ZG BLOCKCHAIN 提出了一套自己的应用开发框架，可以让开发，测试，部署合约能够一行命令完成。它的作用是帮助开发者在区块链上部署智能合约，替换更新合约，以及在已经部署的合约上挂载前端等功能，简化了开发流程。

ZG BLOCKCHAIN 团队会将开发框架集成为一个客户端，来降低 ZG BLOCKCHAIN 应用开发的门槛，同时会配套开发框架的操作文档，提高效率。只需要开发者安装客户端，配置运行环境就可以开始 ZG BLOCKCHAIN 开发之路。提供应用开发框架后，开发者可以直接通过集成的客户端去部署合约，会提供两个网络资源，首先是测试网络，开发过程中，可以使用测试网络去调试，其次是正式网络，那时你的 ZG BLOCKCHAIN 会使用正式网络上部署的合约。可以直接通过 UI 根据智能合约的模板去写入自己的智能合约。集成的客户端还需要有良好的兼容性，适用于各种环境，后端集成时，可以集成不同的环境的客户端。

资产上链后，通过 ZG BLOCKCHAIN 的各类简易智能合约组建，实现资产的分类和细化管理，使之实现与中心化管理平台同等的用户体验。

（2） 高并发支持，让资产流转更便捷

总的来说，区块链技术的发展面临很多的挑战，目前人们已经广泛认识到区块链技术巨大的应用价值，特别是区块链上不可篡改的特性，适用于很多业务场景，但是区块链的技术发展却还没有到达成熟阶段，尤其是将区块链应用到企业级应用方面，区块链的交易并发能力、数据存储能力、通用性、功能完备性、易用性都还存在明显不足。

目前开源的区块链系统的高并发交易能力普遍不高，其中，共识算法是制约性能的重要方面。制约性能的另一个重要因素就是链的底层结构。目前典型的区块链的底层结构是单链

结构区块，意味着从全局来看所有的交易都只能顺序地被处理。由于交易处理缺少并行度，因此难以获得接近传统中心化系统的性能表现。

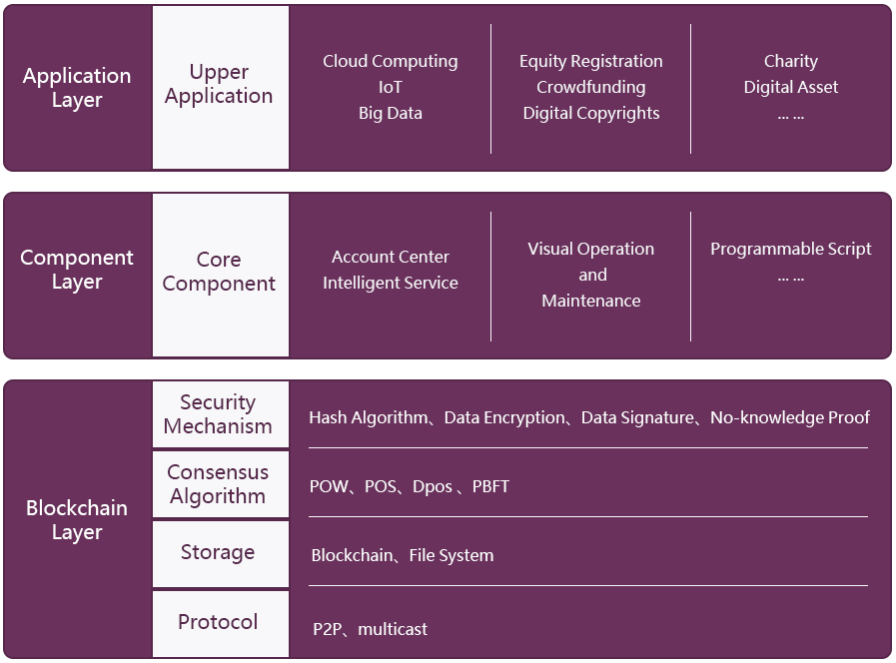
大型交易场景下的交易并发量通常要求在每秒处理数百至数千笔以上的交易，远高于目前典型区块链的表现，而且还要求区块链的性能表现可以随着业务规模的增长而动态伸缩。因此，现实和目标之间存在着巨大的差距，需要持续优化和提升区块链系统高并发交易性能。

（3） 周边生态的支持（交易保险和征信）

区块链行业建立黑名单机制一直是一个紧迫的问题，黑客层出不穷，黑钱泛滥，交易网络有必要建立一张去中心化的信用网络，对于在交易网络出现违约风险的个体列入征信黑名单，共享给整个区块链网络，并且实现防篡改。对于区块链智能资产交易，如果出现恶意行为，可以实行互助保险合约机制，确保风险分散化，避免系统性风险。

3. 技术架构

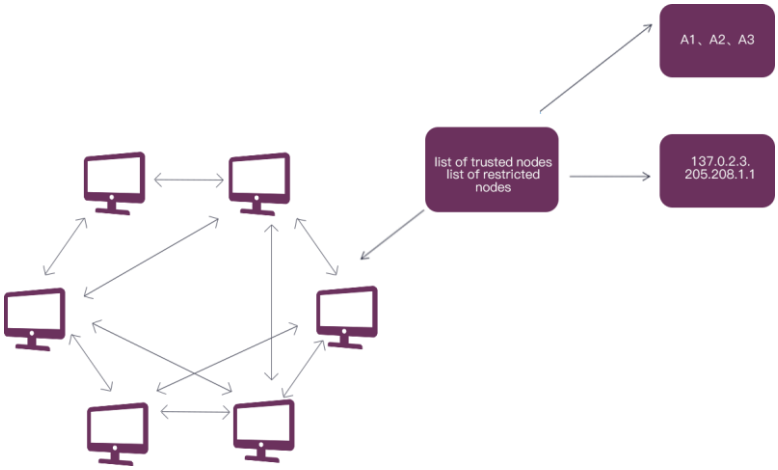
ZG BLOCKCHAIN 系统分为三部分：一是底层的 ZG BLOCKCHAIN 区块链服务，一是中间层的 ZG BLOCKCHAIN 组件层，一是上层的 ZG BLOCKCHAIN 应用层。底层提供完善的区块链服务，包含网络协议，数据存储，共识机制，安全机制四方面；中间层提供区块链开发套件，将区块链封装，方便上层应用对区块链服务进行调用和监控，以及构建智能合约；上层基于业务场景构建可信应用，以实现智能资产上链、发行交易以及管理。



3.1 区块链服务

3.1.1 网络协议

网络协议基于成熟的 P2P 组网协议实现，节点维护邻居节点列表，以自组织形式动态组网。除此以外，添加了可信节点列表，IP 限制等安全措施，增强网络协议安全性和健壮性。



网络协议安全机制说明

3.1.2 共识机制

ZG BLOCKCHAIN 团队在共识机制上的研究方案主要用于解决网络节点一致性信任问题，同时需要保证能抵抗恶意攻击。ZG BLOCKCHAIN 支持 PoW 和 PoS 算法，未来考虑开发支持多种共识算法，包括 DPoS，PBFT，DBFT 等。

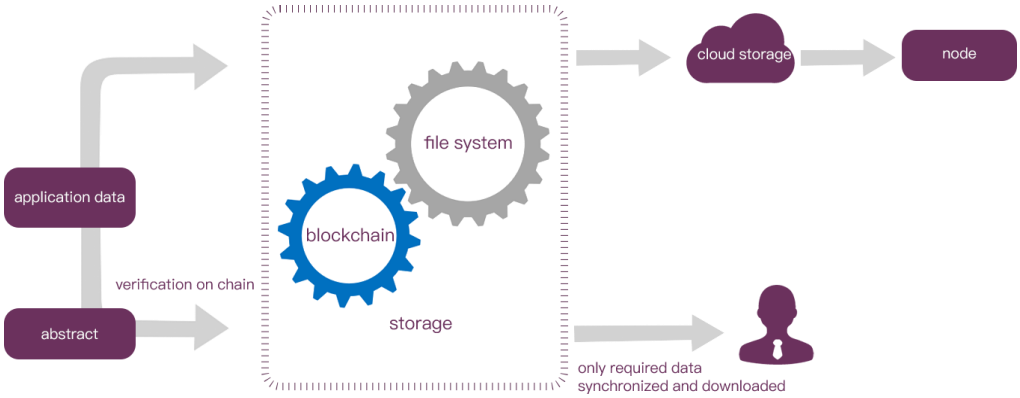
3.1.3 数据存储

数据存储包含两部分：区块链和文件系统。数据存储是区块链底层核心技术，包括数据格式定义，以及数据读写方式。区块链数据依然存储在链式数据结构之上，应用数据则存储在文件系统里，但是应用数据摘要会保存到区块链之上用于可信验证。

由于区块会不断的增长，导致应用数据所占用的空间也会不断的变大，普通电脑根本无法保存那么大的数据量。实际上，大部分用户并不需要存储全部数据，只需要下载可供基本验证的区块数据即可，大部分应用数据不必保存到本地。我们提出的解决思路是数据分片+云存储方案，具体思路如下：

数据分片：把数据分为热数据、冷数据，必需数据、非必需数据，普通用户只需下载必需数据即可快速参与区块链验证工作。

云存储：将历史数据保存到云端，并分发到世界各个节点，实现去中心化，并通过 CDN 加速，用来解决大量历史区块的存储问题，以及同步数据的效率问题。



数据分片+云存储方案

3.1.4 安全机制

通过对网络层的改造，ZG BLOCKCHAIN 设计了一套安全的加入机制，可限制了非授权用户的连接，从而增加区块链的安全性；这将意味着上新加入者需要通过现有区块链维护者超过一半（可设置）的授权允许，才能加入该网络，有点类似于投票，只不过投票人是现有区块链网络维护人。

对于私有链、联盟链来说，这是极其有用的。只有这个联盟里面的超过一半的人允许新节点加入，这个新节点才能连接到该区块链网络，并参与挖矿。

3.2 组件服务

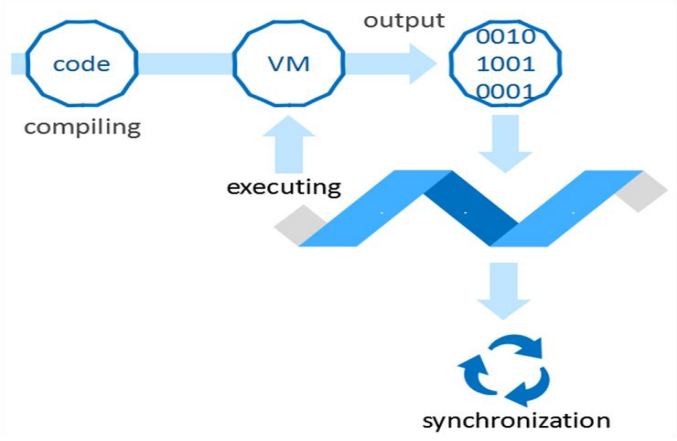
3.2.1 账户中心

提供了公私钥生成、管理功能，可使用私钥对交易进行签名、交易验证、多重签名；支持地址实名认证，同一用户支持多个地址；可针对特定用户开放高级功能权限，实现审计监管；提供应用层地址与区块链地址的映射，对于应用来说，不需要知道用户真正的区块链地址，只需知道应用的地址即可。

3.2.2 智能合约

ZG BLOCKCHAIN 合约层为上层应用提供更高层的基础组件,支持应用资产发行。开发者可基于现有区块链发行应用内部代币，并可实现应用代币跟区块链货币之间的互转。

ZG BLOCKCHAIN 可以提供商业化的大型智能合约应用服务。智能合约其实就是预先定义好的一段脚本，在发布之后就无法修改。在智能合约中支持自定义数据结构，实现复杂的业务逻辑，并通过跟自定义资产或区块链货币结合，开发出各种去中心化的应用。智能合约提供对数据进行加密处理，只有数据相关人才能看得到数据，并支持可拔插的应用共识机制，实现特定领域的特殊共识需求；开发者只需要将开发好的智能合约部署到区块链，用户即可使用该合约。



智能合约实现模型

为了更好的适应未来的区块链环境，我们系统的设计考虑到不同区块链的互通问题，考虑将其作为一组基础服务提供给开发者，实现区块链之间的资产转移，交叉验证。

3.2.3 运维中心

提供多种可视化区块链管理工具，对区块链进行监控。支持区块链参数配置;支持在线分叉投票；支持区块浏览器，可查看实时区块数据，节点分布情况，整个区块链网络运行情况；提供多维度的数据分析，可及时发现区块链异常情况，并发出警报。

3.2.4 可编程脚本

为了更方便开发者基于区块链进行智能合约编程，我们对区块链底层进行改造抽象，提供了一种更简单的方式进行编程，那就是利用脚本语言。

智能合约代码会运行在脚本虚拟机中，实现了脚本运行时的隔离，以控制脚本权限，并通过将区块链数据注入脚本虚拟机中，实现脚本可访问区块链数据实现智能合约逻辑。

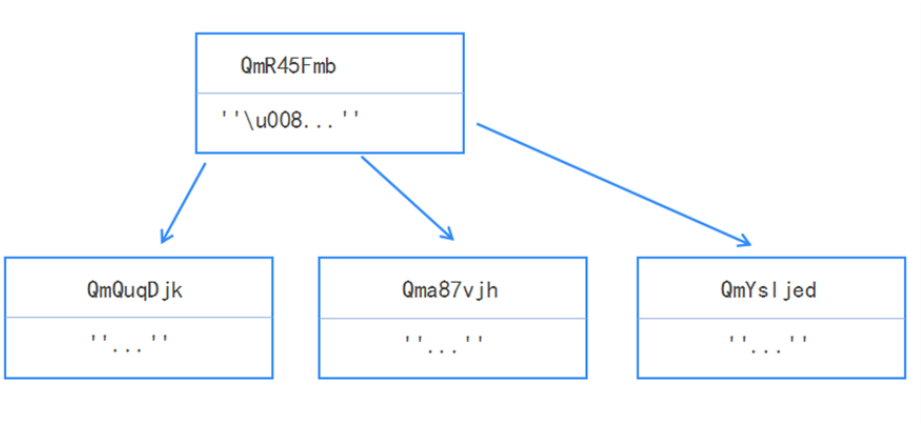
脚本语言因其语法简单，易用的特性，受到广大开发者的喜爱。以语言的通用性、易学性作为考量标准，决定前期采用 lua、javascript 这两种语言作为智能合约开发的脚本语言。未来我们可能会支持更的语言供开发者选择。

3.2.5 数据分层机制

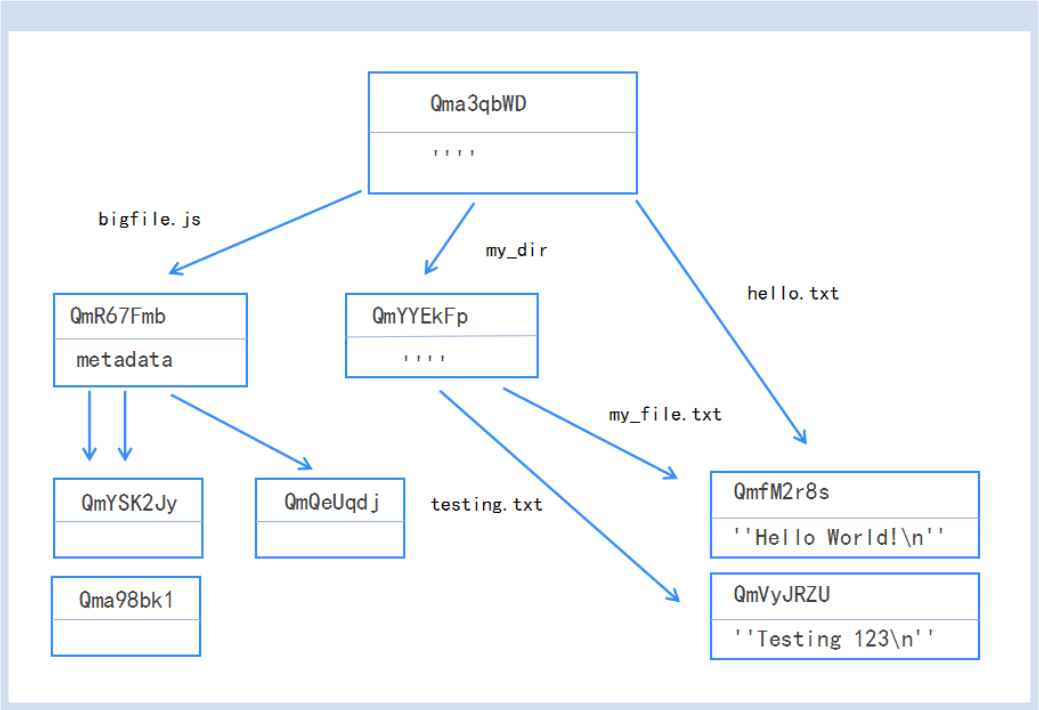
数据分层通过数据的重要性分为以下两层:

第一层，基础账户数据。基础性数据包含用户的账户、合约、交易等，通过基于位运算的交易分类算法(Based bit- Operation Transaction - Classification Algorithm)分类,存到提前划分好的重要数据存储的块中。

第二层，应用数据，各种应用产生的数据比如文字、图片、声音、视频等数据。
这些场景数据量巨大，所以选择采用 IPFS 存储方式，先将数据打散，然后分片存储，文件名和文件内容强关联起来（文件名是文件内容的 hash）。在任意终端上，相同文件内容的文件其名称也一定相同。文件内容的 hash 存储在矩阵的每条子链中，然后将内容打散存储在提供存储的节点上，将文件名和 link 存储在子块中，使单位存储数据变小。如下图所示:



当产生一个数据时，先我们判断这个数据的大小，当小于等于一定值时，我们直接将数据存储在子链中，此时这个数据中就只有一些基本数据信息，存在一个 link 字段，但是值是空字符串。当大于一定值时，子链中只存储数据的基本信息和 link 值，数据中的 link 字段指向其包含的文件和目录，通过这个 link 最后可以找到完整的数据，如图中，通过 link 的指向去查找，最后可以找到完整的文件。



上面就是公有链底层的存储机制，这样的存储机制，可以不用像比特币那样，发生存储瓶颈时，去增加区块的大小。这样的存储机制，不需要协同矩阵中的子块有多大的容量，只需要设定好激励机制，让更多的节点参与到存储共享中来，这样就不会产生由于数据增长，导致一些存储方面的问题。简单的说就是，用户和用户之间遵守一定的系统规则，相互存储数据碎片，存储人想要得到完整的数据时的时候，系统会把碎片收集组合起来，数据的主人

用密钥才能打开。就比如说，现在一个节点上传了一个视频进入系统，节点创建时，会有自己的私钥等等各种信息，系统将文件打散，打散后，存储在提供共享存储的节点上，然后系统显示产生一笔数据，但是具体的内容只有当节点需要完整的数据时，系统再通过 link 去向下查找，组合起来完整的视频，然后节点通过自己的密钥去打开这个视频。

以前的公有链上的数据指的是一笔交易，所以对于数据的定义还是比较简单的，但是我们现在的存储机制是可以接受任何类型的数据，所以我们对于数据的定义做了修改：

由于区块链现在上面的数据类型,都是以交易为单位,所以里面会包括一些交易相关的数据，数据定义的伪代码：

Transaction {

nonce *//发送者发送交易数的计数*

gasPrice *//发送者愿意支付执行交易所需的每个gas的Wei数量*

gasLimit *//发送者愿意为执行交易支付gas数量的最大值*

to *//接收者的地址*

value *//从发送者转移到接收者的Wei数量*

data *//消息通话中的输入数据(也就是参数)*

chainId *//当前区块的id*

}

ZG BLOCKCHAIN上面数据定义的伪代码：

Link {

Name *//link的名字*

Hash *//数据的加密哈希*

Size *//数据的大小*

}

Object{

link [ ] *//link数组*

data [ ] *//数据内容*

}

从两段伪代码可以看出，对交易的定义，就是一笔交易的内容，这样就限定了数据的类型，格式。这样的定义，显然不能接受其他格式的数据，所以我们通过下面的方式来定义，

这样的定义形式，没有限制数据的字段和内容，也就是说，应用可以随意定义自己的数据的类型和结构，灵活度非常的大。

3.2.6 DAPP 分发服务

随着区块链的发展，将出现各种各样的应用落地，不止金融方面，会出现各种类型的 DAPP，ZG BLOCKCHAIN 得益于无限制的底层数据存储和数据的定义，可以对接多种 DAPP，这种情况下 ZG BLOCKCHAIN 就是一个应用商城。DAPP 应用商城具有普通应用商城的功能，对商品进行上架、下架，展示应用的活动、优惠等信息，通过排名算法展示 DAPP 的排名前后,用分类算法给应用分类展示。在去中心化的 P2P 网络里面，应用影响力的传递，是通过用户之间的消息传递进行的，分发模式可以多种多样，ZG BLOCKCHAIN 通过先将 DAPP 分类然后采用 DAPP 排名的方式，提供应用分发服务。以下具体介绍分类算法和 DAPP 排名算法。

◆ **分类算法**

此算法从数据分析的角度，给出一个更准确、细致的分类方法。

记 Ω 为分类的样本 DAPP 集合，距离 $d(,)$ 是一个 $\Omega\times\Omega\to R^+$ 的一个函数，满足条件：

1) $d(x,y)\geq 0$， $x,y\in\Omega$；

2) $d(x,y)=0$ 当且仅当 $x=y$（即为同一个 DAPP 时）；

3) $d(x,y)=d(y,x)$， $x,y\in\Omega$；

4) $d(x,y)\leq d(x,z)+d(x,y)$， $x,y,z\in\Omega$。

现在将 DAPP 分为 p 类，则每个 DAPP 可以看作为 R^p 中的一个点，Minkowski 距离:

$$d_q(x,y)=\left[\sum_{k=1}^{p}|x_k-y_k|^q\right]^{\frac{1}{q}},\quad q>0$$

通过将 DAPP 的内容和属性标准化，计算两个 DAPP 的距离，得到最后的分类结果。

◆ **DAPP 排名算法**

算法通过收集一个 DAPP 被调用的账户的数量来对 DAPP 进行排名，定义 DAPP 的合约地址与其它地址之间的关系的带权邻接矩阵 $G=(g_{ij})$，其中如果账户 i 调用了 DAPP j，

则G对应的有向图中存在从j到i的弧，此时$g_{ij}=1$，否则$g_{ij}=0$。若账户i调用了 DAPP j，设i的重要性为q_i，i调用的 DAPP 的数量为n_i，则j从i分到的重要性为q_i/n_i。

现设有M个节点，节点的重要性根据节点地址的重要性来判断。地址的重要性根据其转账记录多少、交易是否频繁、数额大小来衡量。优秀程度越高，排名越前，活动信息和优惠信息位置越重要，将交易历史生成交易拓扑图，然后根据 LeaderRank 算法，得到每个地址的得分。

设有m个 DAPP，将他们的重要性分别记为$r_1, r_2, r_3, \cdots r_m$，令$\sum_{j=1}^{m} r_j = 1$，$G_m = \frac{g_{ij}}{n_i}$，DAPP j存在调用账户的概率为$p\ (p<1)$，则：

$$r_j = \frac{(1-p)}{m} + p\sum_{i=1}^{M}\frac{g_{ij}}{n_i}r_i$$

最后得到每个 DAPP 的重要性的值，排名即可。

4. 应用场景

ZG BLOCKCHAIN 作为智能资产领域解决信任问题的技术中介，在诸多应用领域可以发挥作用，将包括数字资产发行交易，区块链交易网络征信共享，去中心化竞价及投票，信息公示，区块链交易互助保险等。下面将挑选几个应用场景说明 ZG BLOCKCHAIN 如何应用。

4.1 数字资产发行管理

金融数字资产发行在区块链上具有如下优势：总量恒定，资产自由流通，流向可溯源追查，参与者共同维护资产的可信性。传统的股票，债权，收益凭证等都可以整合到区块链上，发行相应数字资产。

发行者将资产凭证登记在区块链上，发行自己的数字资产。一旦发行完毕，该数字资产维护将不再只受发行方控制，而是由数字资产持有方和参与方共同维护，真正达到社会化运营。区块链作为一个价值自由流通的网络，数字资产可以通过这个网络在节点间自由流通交

换。任何新的机构或者用户想参与进来，只需要将系统对接该数字资产的区块链系统或者成为区块链网络一个节点，这样增强了数字资产流通渠道的多样性。而资产的价值由参与该数字资产运营的机构或者用户共同决定，真正通过社会化流通实现价值定位。

4.2 去中心化数字资产的交易

传统的资产交易过程中，涉及的环节非常复杂。除了需要政府等权威部门进行资产认证或背书外，还需要结算系统来进行结算，需要银行来处理资金转账，政府相关部门进行资产交割转让等等，用户在这过程因此付出了较大的成本。通过区块链的方法，整个交易流程完全在链上完成，所有数据都同步在全网各个节点上，实时更新交换数据，使得整个过程更加清晰透明，无需外部第三方机构的介入，不仅成本大幅度降低，效率也显著提高。

另外,对于目前市场推崇的资产证券化以及 token 经济学,区块链之所以重构生产关系，最主要成就和价值，不是因为单纯的技术突破，而是站在前人的积累下，建立一套围绕“token”的激励系统。这套激励系统有非常广泛的普世性应用，会给各行各业带来了生机和活力。传统行业会寻求升级，而许多之前难以想象的新型行业会崛起。Token 的流转和交易成为“token 经济学”之中很为关键的环节，市场对于 token 的交易效率要求也非常高，提供一套去中心化的高并发交易系统能够加速“交易创造价值”。

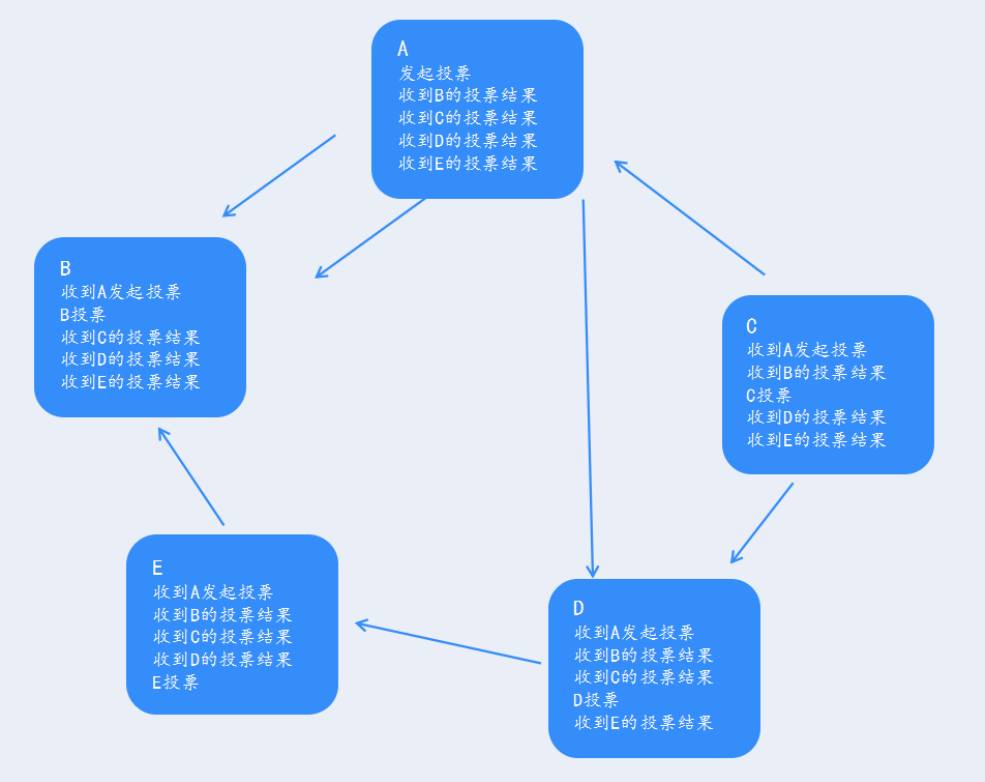
4.3 去中心化竞价及投票

传统投票活动中存在不公开、不透明、投票作假或更改、随意更改投票结果等问题。这些投票系统封闭性，所以会存在刷票、后台篡改数据、黑客攻击等问题，其安全性更是令人担忧。由于区块链技术的不可篡改、高透明度等特性，基于 ZG BLOCKCHAIN 之上提出了提供公正投票的服务应用。利用区块链技术，投票人的任何投票记录，一旦写入到区块链，都将被永久保留且无法被篡改，事后还可以随时提取投票数据作为证据，从而确保投票人的权益不受损害或破坏。

为了避免刷票这种情况的出现，采用如下模式投票：投票发起人发起一次投票，必须生成足够多的票发放给参加投票的人,有票的人才能给本次投票。票是一种锁定了多个代币（该数量可以投票表决之后变更）的数字资产，因而发起人发起投票时要计算需要参与投票的人员的数量，有多少参与投票的人就要准备多少个代币。投票过程中这些代币被锁定，不得用

来支付，直到该次投票结束票释放后，这些锁定的代币将回到投票人的手中。这样首先只有持有代币的人才能参加投票，而且这样的设置限制了刷票的可能。

公证投票的使用范围很多，下面通过区块链投票上币来说 DAPP 在公证公开投票上的应用。首先交易系统服务商在 DAPP 上写入候选代币的名单发起投票，并且设定投票时间，投票资产，用户参与，时间截止，选出热度最高的项目上线。在 DAPP 上投票的好处就是，投票的进度和结果每个参与者都可见，不可篡改，保证了投票上币的公正、公平、公开性。以下是投票过程的简单流程图：



4.4 交易征信上链

在数字资产交易征信领域，普通交易所由于缺少大量数据来源，其自身拥有的数据无法精确绘制用户征信图像，只得依赖于这些大型机构。这种单中心的征信模式，往往需要依赖于企业的规模效应。对于提供征信服务的企业而言，其信息采集和维护成本也是极其高昂的。这使得征信服务往往具有垄断性。

基于 ZG BLOCKCHAIN 的互联网征信则是一个开放共享的服务模式，可以看做是一个交易行业内的联盟链。区块链数据的不可伪造，不可篡改属性也增强了企业间信任，参与维护这个联盟链的企业需要将数据共享在区块链上，所有企业共同参与维护和验证。

这种基于区块链的数据共享方式，也丰富了征信数据来源，增强了征信服务可靠性。多个企业共同参与维护征信系统，降低了企业成本。

4.5 信息公示

现有的信息公示模式下，信息的权威性完全来自于公示主体，这种公信力的证明方式恰恰容易滋生诸多内幕交易。

区块链数据的不可篡改、无法抵赖的属性极大地满足了公示领域要求。在区块链上实现信息公示，其可信性不再来自于单一机构，而是来自于大众节点的认可。一旦为大众认可的信息才会被记录在区块链上，然后公示于众。一旦被公示的信息，是无法被任何单一机构或者个人所篡改的。区块链从技术层面上，保证了公示信息的可靠性。ZG BLOCKCHAIN 打造的区块链信息公示系统用于实现对项目信息披露的内容做永久存证，以防止欺诈行为。

4.6 去中心化交易网络互助保险

随着互联网互助保险业务放开，越来越多平台开始开展互助保险业务。互助保险业务其核心行业痛点在于资金流向不透明问题和赔偿标准问题。现有互联网保险模式，其资金流向是无法受到公众，尤其是投保用户监控的，容易出现平台挪用现象。

基于 ZG BLOCKCHAIN 开展互助保险业务，将用户投保资金以及资金流向记录在区块链上，投保用户可以查看到自己投保资金流向。如果权限允许，甚至可以申请查看所有投保资金流向，这无形中增强了平台的公信力。

一旦出现赔付事件，可以由投保用户投票决定该事件是否应该赔付，以及赔付额度。这样可以避免大的赔付纠纷，降低平台运营风险。

前期，ZG BLOCKCHAIN 主要定位于区块链数字资产交易市场的互助保险服务，对于黑客攻击等不可控事件实施互助保险，确保降低系统性交易风险。

5. 代币 ZGT

5.1 价值

传统互联网商业世界，信任来源于中心化平台；ZG BLOCKCHAIN 将信任问题去中心化，将信任确定问题交给系统参与者共同决定，参与者可以获得相应资产奖励。在 ZG BLOCKCHAIN 的区块链生态体系中，虚拟世界的信任被赋予了价值。

在 ZG BLOCKCHAIN 体系里，资产奖励以及价值体现的媒介就是 ZGT 代币（ZG BLOCKCHAIN TOKEN），ZGT 是 ZG BLOCKCHAIN 生态系统中唯一一个系统代币，充当了虚拟世界价值衡量尺度的类货币。在 ZG BLOCKCHAIN 生态中，不同的应用可以依托 ZGT 发行不同的资产代币,这些代币根据应用的特定需求在 ZG BLOCKCHAIN 生态系统中流转，充当应用的价值媒介或者权益凭证。

总结来看，ZGT 主要用作系统燃料、区块链应用价值转移媒介。具体来说是，

系统燃料：ZG BLOCKCHAIN 是一条公有链，基于其来开发部署的智能合约均需要消耗一定量的 ZGT。

价值转移媒介：作为 ZG BLOCKCHAIN 生态系统的唯一代币，ZGT 充当了价值媒介，在链上展开的智能合约应用可以基于 ZGT 进行交易、清算和结算，所有交易可溯源、防篡改。

ZG BLOCKCHAIN 公链体系将以交易为中心，立足于打造综合性智能合约应用生态，服务好智能资产用户，未来，更多的应用也将基于 ZGT 来开展。

5.2 初始分布及销毁情况

在 ZG BLOCKCHAIN 体系中，ZGT 会恒量发行，永不增发。ZGT 代币总量 2 亿枚，无公募，无私募，初始流通的 ZGT 将全部以赠送的方式流通，ZGT 整体分布情况如下：

比例	数量	分配方式/用途	锁仓计划
10%	0.2 亿枚	超级节点及战略投资机构	锁仓 12 个月，12 个月后分 12 个月等比例释放
20%	0.4 亿枚	购买手续费点卡免费赠送	不锁仓
20%	0.4 亿枚	R&D 研发基金	锁仓 12 个月，12 个月后 10 年线性释放
10%	0.2 亿枚	市场拓展资金，用于奖励、空投以及市场合作等	从第一年起，分 10 年线性释放
20%	0.4 亿枚	生态基金，支持区块链生态产业	锁仓 12 个月，12 个月后 10 年线性释放
20%	0.4 亿枚	团队所有，支持后续运营支出，系统升级以及团队激励	锁仓 12 个月，12 个月后 10 年线性释放

说明：ZG BLOCKCHAIN 项目是一个社区型公有链项目，ZG BLOCKCHAIN 基金会会全面负责项目的推广和商务合作等，基金会持有的份额会用于支持媒体、第三方合作以及后续会员招募、后续战略投资方引进等。

销毁情况：

由于 ZGT 的交易回购销毁机制，截止到 2021 年 3 月份，团队已经累计销毁了 6,435,298 枚 ZGT。为了进一步降低 ZGT 未来的流通量，进一步提升 ZGT 的稀缺性和内在价值，基金会决定于 2021 年 5 月份一次性销毁 1 亿枚 ZGT，即研发基金、团队以及市场拓展资金部分的 1 亿枚 ZGT 悉数销毁。生态基金以及超级节点战略投资的这部分 ZGT 依然按照原有解锁模式分批解锁，约在 11 年后完全解锁完毕。

销毁完成后,ZGT 的理论最大流通量为约 9300 余万枚,由于长达十年的线性锁仓机制，ZGT 的释放极为缓慢，截止到 2021 年 5 月，ZGT 的流通量不超过 5000 万枚。

6. 团队及投资机构

核心团队

Chao Qian	*创始人*
Gang Jin	*CPO&CMO*
布哈斯赫--如玉饭	*政府公共事务负责人*

基石投资机构

比特时代（bwfund 基金）、达摩资本、华尔资本等。

合作生态

黑钻评级、黑钻财经、灯火区块链、ZG.news、ZG GROUP、AEX.com、时代学院、金色财经、火星财经、币看 bitkan、币小白、布洛克财经、深链财经、链向财经等。

7. 风险提示及免责声明

该文档只用于传达信息之用途，并不构成买卖 ZG BLOCKCHAIN 股份或证券的相关意见。 任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策或具体建议。本文档不构成任何关于证券形式的投资建议，投资意向或教唆投资。本文档不组成也不理解为提供任何买卖行为或任何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。 ZG BLOCKCHAIN 明确表示相关意向用户了解 ZG BLOCKCHAIN 市场的风险，投资者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。ZG BLOCKCHAIN 明确表示不承担任何参与 ZG BLOCKCHAIN 项目造成的直接或间接的损失，包括:

1）因为用户操作带来的经济损失;

2）由个人理解产生的任何错误、疏忽或者不准确信息;

3）各类区块链资产带来的损失及由此导致的任何行为。

ZG BLOCKCHAIN 公链生态流通证 “ZGT”，是 ZG BLOCKCHAIN 唯一内置核心资产。ZGT 不是一种投资，是一种使用凭证。我们无法保证 ZGT 一定会增值，在某种情况下也有价值下降的可能，没有正确使用其 ZGT 的人有可能失去使用 ZGT 的权利，甚至会可能失去他们的 ZGT。ZGT 不是一种所有权或控制权。 控制 ZGT 并不代表对 ZG BLOCKCHAIN 的所有权，ZGT 并不授予任何个人任何参与、控制，或任何关于 ZG BLOCKCHAIN 决策的权利。

风险提示：许多数字资产市场因为安全性问题而停止运营。我们非常重视安全，但世界上不存在绝对意义上的100%安全，例如:由于不可抗力导致的各种损失。我们承诺尽一切可能确保您的安全。