



YDS

YDS

项目白皮书





# 目录

## 摘要

一、项目背景

二、设计理念

三、整体架构

四、技术支持

五、核心优势

六、项目愿景

七、代币分配

八、工作线路

九、创始团队

十、风险提示与免责声明

## 摘要

YDS Blockchain (以下简称 YDS) 致力于打造一个无边界的区块链世界。区块链自 21 世纪初期发展起来, 是目前全世界认为最有潜力、最具想象力的一种技术革新。在人类的发展史上共经历过三次工业革命, 第一次以蒸汽机的发明为标志, 让机器代替了手工劳动; 第二次以电能的突破、应用和内燃机的发明为标志, 直接推动人类进入电气化时代; 第三次以电子计算机、核能、空间技术、生物工程的发明和应用为标志, 不仅推动人类社会的巨大变革, 更深刻地影响了人类的生活和思维方式。每一次工业革命都带来生产力的巨大提升, 而作为生产要素之一的生产关系, 改变并没有那么巨大, 依旧是自上而下、金字塔层级的中心化组织。组织的业务越复杂, 层级越多, 效率提升就越困难。区块链是去中心化、去信任化的网络, 可以实现点对点价值交换, 被人们称之为价值互联网。YDS 认为区块链技术最有可能改进当前的生产关系。在 YDS 的帮助下, 我们可以创造这样一个世界——一个人和人直接相连, 去信任化的, 在社区或者社会共识下, 相互协作、点对点相互交换、价值驱动的世界。

YDS 将分三个阶段来实现上述目标。首先, 我们利用模块化的设计方法构建安全稳定的区块链网络, 这一阶段即可实现智能合约及数字资产, 同时我们将引入智能沙盒——一个可以智能化测试和监测合约运行的环境, 沙盒可确保即将正式运行在链上的合约足够安全,

避免类似 DAO 事件的发生。接下来，我们利用区块链分叉来满足不同的商业诉求，如保险、电子文档、数字货币、溯源追踪、个人信用记录等。这一阶段将实现一个不断进化、容易使用、低成本的、适度定制化的区块链网络。最后，通过价值交换协议（Value Exchange Protocol，以下简称 VEP），我们将这些已经分叉的、仍然活跃的网络连接在一起，甚至与其他网络（可能是非区块链的）打通数据交互，构建出一个相互连接、多维度数据相互关联的网络世界。利用多维度数据，如个人信用、资产、生产和消费数据，可以更好地将社区共识、个体行为、价值交换有机地整合在一起。Token 承载生态中的价值，YDS Blockchain 将它命名为 YDS，持有 YDS 将获得合约发布、网络分叉等区块链基础服务。

为构建上述生态，YDS 在设计上把安全性、稳定性、可扩展性放在首位。YDS 作为一个公有链，我们选取了更实用、占用资源更少的委托权益证明（Delegated Proof of Stake，以下简称 DPOS）共识机制。DPOS 更有利于提升整个网络的交易性能，结合对网络其他参数的整体优化，理论上可达到甚至超过 1000TPS（transaction per second）。

YDS 区块链将使人类以无地域限制的、去信任的方式来进行大规模协作。未来已来，变革在即。



# 一、项目背景

## 一、项目背景

1969年10月29日，阿帕网加州大学洛杉矶分校（UCLA）第一节点与斯坦福研究院（SRI）第二节点连通，标志着人类开启了互联网时代。以互联网为代表的信息技术，在其蓬勃发展的近50年时间里，不仅主导了第三次工业革命，更成就了如Amazon、Google、Facebook、Alibaba等伟大的互联网企业，让人们又一次看到技术改变世界的力量。

2008年10月31日，中本聪发布了比特币白皮书——《一种点对点的电子现金系统》，宣告了价值传输网络的到来。比特币有许多值得称赞的设计，如：防篡改，数据备份，参与者相对匿名，无其他信任方等。但其本身的交易性能和工作量证明（Proof of Work，简称POW）共识机制也逐渐暴露出问题。区块链技术从比特币衍生而来，近些年，人们主要围绕区块链的交易性能、共识算法、安全匿名进行创新，如：石墨烯、闪电网络对交易性能的提升；权益证明（Proof of Stake，简称POS）、委托权益证明（DPOS）、实用拜占庭容错（Practical Byzantine Fault Tolerance，简称PBFT）对共识算法的丰富和改进；零知识证明（Zero-knowledge Proof，简称ZKP）、混币提升交易安全等。

### 1.1 市场环境

为什么会出现区块链，我们真的需要吗？YDS Blockchain作为

区块链早期的参与者和见证者，认为这一创新不可逆转更不会昙花一现，原因有两个。

其一，人们需要真实、有价值的信息、够降低信任成本。计算机和互联网让信息分享更加便宜、更加便捷，利用信息透明，优化价值链，提升协作效率。但是，无法杜绝的虚假信息、违约行为也让人头疼不已，基于互联网的传播和复制也极为容易，人们为信任所投入的成本已经越来越大，必然阻碍效率的进一步提升。

其二，人们需要一个将共识、行为和价值激励相互连接的生产关系网。相比工业革命带来生产力巨大飞跃，生产关系的改变就不那么巨大。人类的生产活动以组织为中心开展，依旧是自上而下、金字塔层级的中心化结构。组织业务越复杂，层级越多，要实现客观公正的利益分配就越难，因此，效率提升也就难上加难。区块链将分布式存储、加密技术、P2P网络等技术融为一体，有去中心化、去信任化的技术优势，被人们称之为价值互联网。区块链最有可能解决人与人之间的信任问题，并缔造出新的生产关系网络——点对点价值交换。

## 1.2 主要问题

比特币自2008年诞生以来，以此为原型衍生出区块链技术，无数技术爱好者参与贡献，发展方向百花齐放。有专注于去中心化平台

的以太坊 (Ethereum)、发展数字货币为主的比特币 (Bitcoin)、莱特币 (Lite Coin)，以信息存档为方向的公证通 (Factom)，为保护用户隐私目的的 Zcash 和 Dash，专注于去中心交易所的比特币股 (Bitshare)，甚至是 R3CEV 力推的分布式账本平台 Corda。

尽管行业发展生机勃勃，但区块链无论从技术创新还是商业应用，还面临很多挑战。

(1) 智能合约仍存在安全隐患，黑客可利用漏洞盗取用户的数字资产；

(2) 以不同应用目标而建立的区块链平台，彼此之间存在兼容性问题。尽管人们已经发现并尝试特定链之间的信息交互，但这种局部的解决方案还不足以支撑整个区块链生态发展；

(3) 区块链缺少和现实物理世界的交互，让许多应用创新不得不流于形式，如商品溯源；

(4) 目前，区块链应用仍有较高的技术门槛，导致大规模商用的成本太高；

(5) 存在性能瓶颈，目前分布式系统的性能还难以赶超中心式系统，或者说，分布式系统还难以实现大规模商用。

## 1.3 YDS Blockchain 的必要性

YDS Blockchain 在设计上把安全性、稳定性、可扩展性放在第一位。通过引入模块化的虚拟机、智能沙盒、价值交换和分叉机制，从而创造出一个不断进化、容易使用、低成本的、适度定制化的区块链网络。此外，YDS Blockchain 通过对出块间隔、区块容量、共识算法的优化，理论上可达到 1000TPS 的可用性能。YDS Blockchain 相信，通过技术创新将能够解决人与人之间的信任、也能缔造一个新的生产关系网络，更好地将社区共识、个体行为、价值交换有机地融为一体。



## 二、设计理念

## 二、设计理念

### 2.1 稳定性

稳定性是确保 YDS Blockchain 可用的必要条件。区块链自带去中心化特征，去中心化网络通常较复杂并充满不确定性。因此，我们借助模块化设计工具对区块链进行抽象和简化，通过单独构建模块化虚拟机——Lua Virtual Machine（以下简称 LVM）运行智能合约，这样的设计可带来两个好处。一是优化 LVM 性能直接提升合约执行效率，减少系统耦合带来的干扰因素；二是弱化区块链网络与智能合约运行状态的相关性，即便合约执行出现问题，或虚拟机运行异常，区块链网络的稳定性依然能够保证。

### 2.2 安全性

PoW 曾对比特币网络的安全贡献功不可没，但由于日益增长的挖矿需求和算力难度提升，几乎所有权利都集中到矿工和矿池手中。通过专业合作，他们事实上已经成了高度中心化的“中央服务器”。如果联合超过 51% 的算力，理论上就能够控制大多数比特币交易，如我们熟知的 DOS（Denial of Service）攻击。此外，高昂的电力消耗也同样让人诟病。相对于 POW 模式来说，POS 模式仍在发展，这些发展方向主要立足于安全和应用。POS 模式比 POW 模式在安全上有很大优势，但前提是吸引到足够的持有者来进行 POS 挖矿，才能充分的发挥出安全的优势。DPOS 是 POS 的改进，而 YDS Blockchain 创新出更具商业普适意义的 RDPOS 共识机制。与 DPOS

同等安全的情况下,理论上可提高出块响应,增加网络的稳定和安全。除此之外,YDS Blockchain 创新性地提出智能沙盒机制。任何人发布的合约,首先要在智能沙盒中试运行,YDS Blockchain 会对其进行全路径自动化测试,并持续监控其运行状态,若健康程度恶化,或发现漏洞。网络自行判断将其终止,避免问题合约对区块链生态造成破坏。

### 2.3 可扩展性

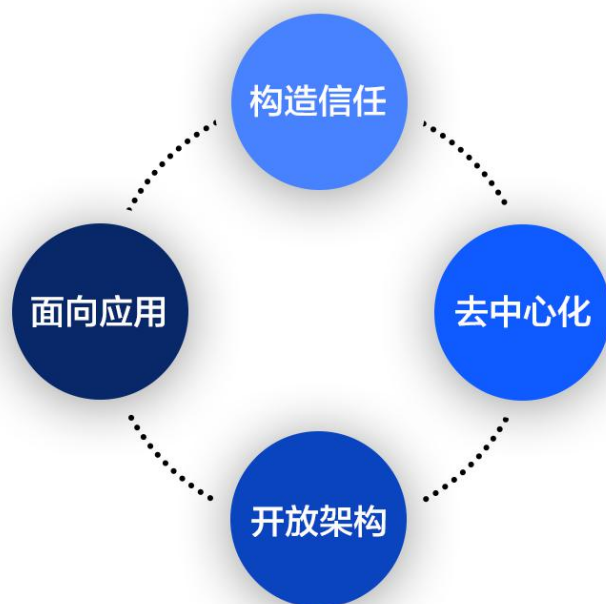
可扩展性的提出,为了解决区块链彼此不兼容的信息孤岛问题。首先,我们认为升级、分叉是网络进化的有效途径之一,分叉后形成一个主链和若干子链。主链和子链从技术角度看完全对等,只是基于社区共识给它们设置不同的标识。每一条子链可根据不同的商业应用做适度化定制,通过在子链之间构建 VEP,其工作方式类似于网关,子链之间通过 VEP 可交互信息和交换价值。通过这样的协作可形成多应用的区块链生态。不仅如此,非区块链的线上数据也将纳入 YDS Blockchain 生态,辅以智能合约,可对现实世界中的事件做出响应。

### 2.4 易用性

YDS Blockchain 通过两方面来实现易用性。一是提供区块链即服务平台 (Blockchain as a Service, 简称 BaaS) 来降低企业及个人的使用门槛。通过网络分叉、数据定制、智能合约发布和升级、资产交易监控等并辅以可视化功能,让区块链应用变得简单易用。二是 YDS Blockchain 提供多种语言支持,从 Lua、C++到 Java,让不

同平台的开发者都可以便捷地开发。

### 2.5 YDS 系统设计原则



#### YDS 系统设计原则关系图

**构造信任**：这是区块链的核心使命，系统设计的目的就是为应用构建一个可信任的系统；

**去中心化**：是区块链的核心特征，是构造信任的根本手段；

**开放架构**：开放是去中心化的必要条件，开放意味人人平等、代码开源、设施平民化；

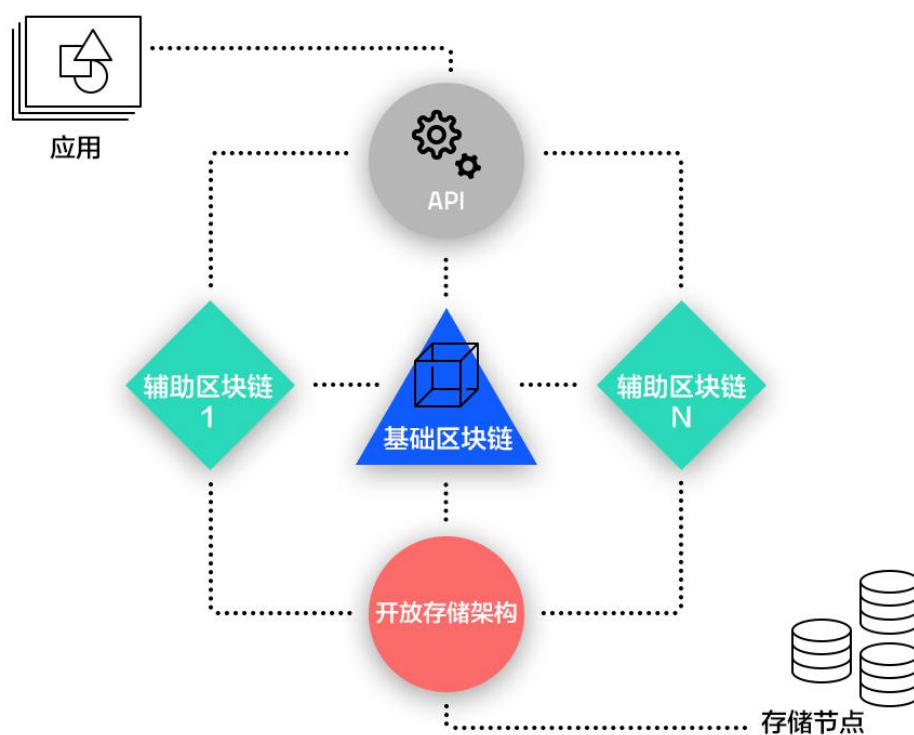
**面向应用**：开放架构导致平等参与、平等使用，互不信任的参与者需要信任机制保证。



## 三、整体架构

### 三、整体架构

YDS Blockchain 由三部份构成：基础区块链(Foundation Blockchain)、辅助链(Annex chain)及开放存储架构(Open Storage Architecture) ,是根据矛盾错位机制建立在统一底层协议与共识机制核心规则基础上的开放经济生态的组成部份，分别执行不同的功能，整体上相互协作、相互验证，构成完整的信任保证及价值维护机制，解决了去中心化、可扩展性、安全性三者不可兼得的难题。



YDS Blockchain 总体逻辑架构



## 四、技术支持

## 四、技术支持

### 4.1 YDS 数据格式

YDS 中的所有数据都以“递归长度前缀编码 (recursivelengthprefixencoding,PLP)”形式存储,这种编码格式将任意长度和维度的字符串构成的数组串接成字符串。

### 4.2 YDS 创新型共识机制

YDS 创新型共识机制：采用 TPOS(SuperProofofStake)+POW+DPOS 的全新机制。相较于传统 POS/POW/DPOS 机制,大大提高了系统效率,交易处理能力,实现了商业级的提高;基于过去多年数字货币的经验,发现的一个对于工作量证明功能很重要的特性是“内存困难”--合法的工作量证明不仅需要大量的计算,同时需要大量的内存。

如今,存在两个主要的“内存困难”功能类别-scrypt 和质数币挖矿,但二者都不完美;没有一个需要理想的内存困难功能可能需要的内存,二者都会遭受时间-内存置换攻击,攻击中攻击者可以牺牲一些计算效率为代价以远低于算法要求的内存大小完成合法工作量证明。使用一个替代的名为“短剑”的算法,一个基于适度直连的无环图的内存困难的工作量证明机制,它虽然远非最佳,但却有远较现存其它算法为强的内存困难性。哈希算法将任意长度的二进制值映射为较短的固定长度的二进制值,这个小的二进制值称为哈希值。哈希

值是一段数据唯一且极其紧、凑的数值表示形式。如果散列一段明文而且哪怕只更改该段落的一个字母，随后的哈希都将产生不同的值。要找到散列为同一个值的两个不同的输入，在计算上是不可能的，所以数据的哈希值可以检验数据的完整性。

一般用于快速查找和加密算法，字符串随机生成代码如下：

```
#include<stdio.h>#include<stdlib.h>#include<string.h>
#include<ctype.h>#include<time.h>#defineSTRINGSIZE10#d
efineSTRINGCOUNT1000//如果是在一个程序的循环中不断调用
这个函数,那么是没有效果的虽然也是使用的系统的时间函数来初始
化随机数发生器,但程序的执行速度太快了,可能执行1000次循环
返回的秒数都是一样的time返回
时间戳/*voidget_rand_str(chars[],intnum){
//定义随机生成字符串表char*str=
"0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefg
hijklmnopqrstuvwxyz";inti,lstr;
lstr=strlen(str);//计算字符串长度
srand((unsignedint)time((time_t*)NULL));
//使用系统时间来初始化随机数发生器
for(i=0;i<num-2;i++)
//按指定大小返回相应的字符串{s[i]=str[(rand())%lstr];
}s[i++]='\n';s[i]='\0';printf("%s",s);}
```

```
*/  
  
intmain(){FILE*fp1;  
  
//定义文件流指针，用于打开读取的文件 char text[10];  
  
//定义一个字符串数组，用于存储读取的字符 inti=0,j=0,lstr;  
  
char*str="0123456789ABCDEFGHIJKLMNPOQRSTUVWXYZ  
Zabcdefghijklmnopqrstuvwxy";lstr=strlen(str);  
  
//计算字符串长度  
  
fp1=fopen("d:\\test.txt","r+");  
  
//只读写方式打开文件 a.txt  
  
//while(fgets(text,1024,fp1)!=NULL)  
  
//逐行读取 fp1 所指向文件中的内容到 text 中  
  
srand((unsignedint)time((time_t*)NULL));  
  
//使用系统时间来初始化随机数发生器  
  
for(j=0;j<STRINGCOUNT;j++){  
  
for(i=0;i<STRINGSIZE-2;i++)应的  
  
//按指定大小返回相字符串  
  
{text[i]=str[(rand()%lstr)];text[i++]='\n';text[i]='\0';fputs(t  
ext,fp1);  
  
//将内容写到 fp1 所指向文件中  
  
}fclose(fp1);  
  
//关闭文件 a.txt，有打开就要有关闭  
  
}
```

## 4.3 YDS 智能合约技术

很多区块链正在整合一种通用的脚本语言去定义所有的操作。这些设计终将业务逻辑处理器定义为一个虚拟机，而所有的交易被定义为由这个虚拟机运行的脚本。这个方案有一个在真实处理器上的单线程性能极限，并且由于将所有东西强制通过一个虚拟处理器去执行，让问题更严重了。一个虚拟处理器即使用上了实施编译技术(JIT)也总会比一个真正的处理器要慢，不过计算速度并不是这种“任何东西都是一个脚本”方案的唯一问题。当交易被定义在这么低的层次上，意味着静态检查和加密算法操作还是会被包含到业务逻辑处理的环节里，这也让会让整体的吞吐量降低。一个脚本引擎永远不应该要求执行一个加密算法签名检查的请求，即使这个请求是通过原生的机制实现的。

## 4.4 交易快速确认

YDS 采用高效自适应的共识算法，保证了共识完成即交易确认，并且对交易确认过程中的其他环节，如签名算法、账本存储方式等进行了优化，实现了毫秒级确认交易。

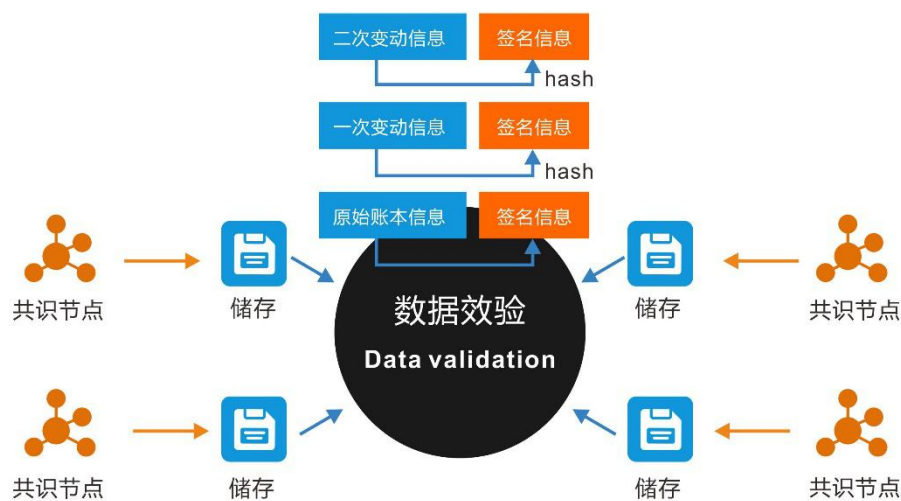
## 4.5 海量储存及高并发支持

YDS 支持本地数据库存储、文件系统存储以及云存储多种方式。本地存储实现冷热分离，数据库存储使用分库分表的模式，云存储支持按照云的集群规则扩展。

## 4.6 可靠一致的记录存储

YDS 通过非对称加密的数字签名保证业务请求在传输过程中不

能被篡改，通过共识机制保证各节点的数据一致的存储。对于已经存储的数据记录通过节点内的自校验性和准实时多节点数据校验来保证已经存储的数据记录不能被修改。节点的自校验性：采用块链结构存储数据记录，其中部分记录的修改会破坏块链结构的完整性，可以快速校验出来并从其他节点将数据恢复。另外 YDS 每个记账节点都有自己的私钥，每个区块头中包含了本节点私钥的签名，区块内数据的修改都可以通过签名校验出来。多节点准实时的数据校验：当节点的私钥被盗取，恶意用户是存在修改账本链上所有数据的可能性的，YDS 提供了多节点间准实时的数据对比机制，可以及时发现某个节点账本数据被篡改的情况。



## 4.7 用户隐私和交易保密

YDS 中用户信息和区块链地址是隔离的。从各节点的记录存储中，无法获取到相关联的用户信息。用户信息存储有权限控制，访问认证，加密存储等多层保护。对交易保密程度较高的用户还可以选择

交易不相关性机制,同一个用户的每次交易都映射到区块链上不同的地址上,从而保证了在交易账本上无法获取一个用户的多笔交易的关联性。

### 4.8 安全的密钥管理体系

在 YDS 的密钥管理解决方案中,提供了密钥保险箱和用户账户委托的功能来保证密钥的安全。密钥保险箱使用用户信息对密钥加密并分割存储在多个不同的节点上,正常业务流程下不会访问密钥保险箱,当用户密钥丢失后,可以通过对用户信息认证之后将密钥找回。YDS 所有委托账户操作会独立记录在区块链上,并且对委托账户的操作有严格的频度限制和独立的风控策略,可以严格控制委托账户的操作风险。



## 五、核心优势

## 五、核心优势

在“稳定、安全、可拓展、易用”的设计理念下，YDS Blockchain 具有以下核心优势：高性能、高安全性、高速接入、高效运营。

- 1、高性能：依托 YDS 区块链技术的海量并发经验，交易支持秒级确认；提供海量数据存储，具备每秒万级的处理能力；
- 2、高安全性：提供丰富的权限策略、安全的密钥管理体系和用户隐私保密方案，保障数据安全。
- 3、高速接入：丰富的应用开发框架和灵活的部署方式，方便不同类型的用户快速接入，构建应用；
- 4、高效运营：提供全面、实时、可视化的运维管理系统，快速识别系统状态，满足多个层级的运营管理需求。



## 六、项目愿景

## 六、项目愿景

发达国家积极布局区块链，在金融、支付、审计、物联网等领域多点开花。目前国际相关机构产业投资力度较小，过往产业内投资多集中在挖矿、报价、信息咨询等领域，技术含量低且商业模式单一。有深入商业模式研究及一定规模的应用项目比较匮乏。

近两年行业内开始呈现出向区块链商业应用和深度探索的发展和投资趋势，但体量较小且缺乏大型金融机构及政府支持。随着各国政府对区块链重视程度加深，全球最新科技进展的溢出效应，以太坊作为区块链技术标准的逐渐确认，以及区块链应用的更加成熟和可投资标的的增加，区块链有望成为“互联网+”之后的下一个热捧对象。这将激发创业者和应用者的热情，从而形成国际区块链发展的良性之路。

区块链并不是一次技术炒作。2017年是区块链的元年，特别是从下半年开始，区块链概念迅速崛起，全球金融机构和区块链相关的新闻层出不穷，不断看到有更多的机构和企业开始拥抱区块链技术。这不仅仅是欧美对于技术热点的短期追捧，从需求层面来看，区块链技术是有真实的市场需求的。尽管重构所有互联网应用的理想似乎过于远大，但在金融领域，已经可以观察到传统金融机构对于区块链的趋之若鹜。区块链技术实际上赋予传统金融机构一个全新互联网的工具，传统金融机构迫切的需要借助区块链改造原有的业务流程，降低

运营成本和提高经营效率。从产业层面来看，2016 年区块链产业将从概念逐步走向落地。2015 年，金融机构以及初创企业开始陆续完成对于区块链的相关应用的概念证明以及试点。2016 年，随着大量资本的入场，有望迅速催熟产业；同时，金融机构本身对于区块链技术的重视程度不断的提高也将加快区块链技术的产业化道路进程。

部分去中心化在金融领域率先展开，优化传统金融机构的业务流程，提高整体的经营效率；而完全去中心化将成为互联网行业新的演进方向，YDS Blockchain 实质上是一种中心化的组织网络，可以利用大数据再现计划经济。

未来，YDS Blockchain 技术最终将塑造一个去中心化、自治的网络组织，实现市场无形之手的互联网化表达，实现更彻底的共享经济范式。并依托 YDS 区块链底层技术将业务拓展到全球各行各业，真正意义上实现人类以无地域限制的、去信任的方式来进行大规模协作。

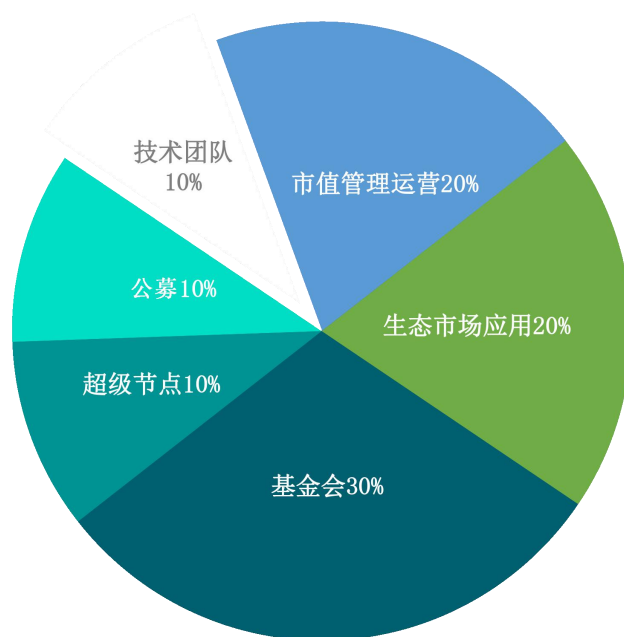


## 七、代币分配

## 七、代币分配

数字货币 YDS Coin 简称 YDS，是 YDS 官方发行的原生加密数字令牌，基于 POW、POS 技术开发。第一阶段将在以太坊上依据智能合约生成，第二阶段将基于自己的公链自行生成，并作为 YDS 公链的唯一基础数字货币，用来结算、交易、以及智能合约履约使用。

数字货币 YDS 持有人可以参与投票产生记账人，还可以共同参与决定基金会及 YDS 公有链平台等相关重大事项。



数字货币 YDS 共发行 6.8 亿枚，由 YDS 基金会一次性创设出来，其总量上限已设定，不可更改，不可增发。数字货币 YDS 按照一定的规则和比例分配给不同的持有人，首期流通 1.36 亿。10%超级节

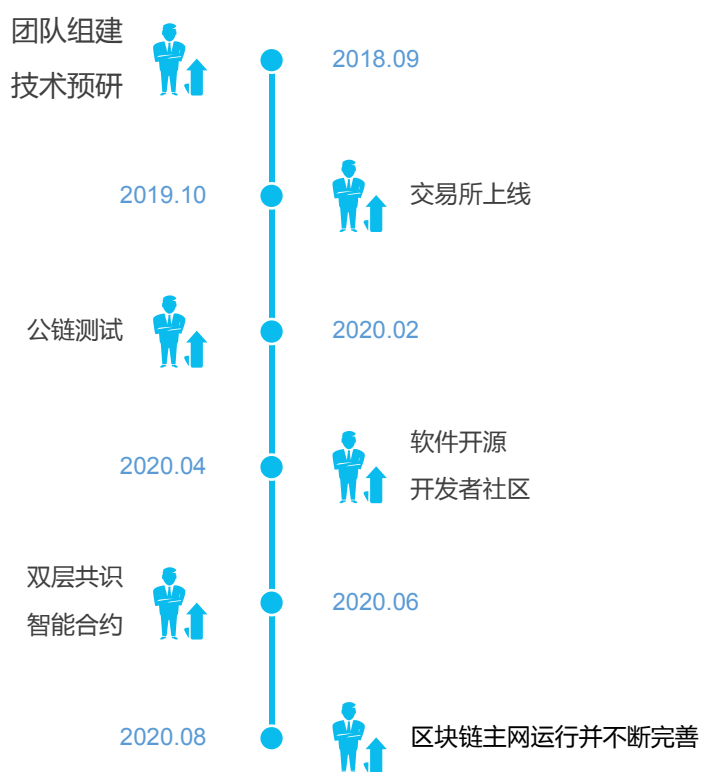
点锁仓收益，100 个超级节点，一个节点配送 68 万枚 YDS，3 万 USDT 一个超级节点；公募 10%，6800 万枚 YDS，价格 0.1USDT；技术开发团队 10%，2021 年开始释放。元道基金会，华谊资本，壹点资本 30%；市值运营管理 20%；生态市场激励 20%。



## 八、工作线路

## 八、工作线路

随着区块链和智能合同的成熟和普及，YDS Blockchain 的总体开发过程将是短期建设与长期开发相结合的过程。我们将逐步完善以下战略步骤：





## 九、创始团队

## 九、创始团队

YDS 项目团队成员均为行业相关领域资深专家，而且有丰富的资源和经验。而且项目前期已经开展了大量的工作，成绩斐然。具体情况如下：



Taylor Smith (CEO)

美国康奈尔大学的金融管理学硕士，曾就职于摩根士丹利投资银行，在支付领域有自己独特的见解，美国先锋集团股东一，2012 年开始布局区块链，认为区块链是金融颠覆式创新技术，致力要打造一个区块链领域的商业帝国。



Richard Marx (CTO)

毕业于美国常春藤名校波士顿学院，计算机专业硕士，在著名社交通讯公司 Facebook 有 5 年的工作经历，掌握社交应用的核心技术，在职期间参与了新一代加密通讯的底层架构，系统维护和软件研发工作。



Alfredo Aguirre Valdez ( 开发工程师 )

原特斯拉软件工程师，在不同业务领域的软件开发超过 13 年。从金融到物流行业，在不同的开发环境，如 PHP，Python、iOS、Android 以及微软协议栈等均有过开发经验。客户包括美国运通和 BBVA 罗盘等。他的个人项目包括苹果 App Store 中的多个应用程序，在 GitHub 的开源库中有 4K 以上下载，Facebook APP 月综合浏览量超过 270 万。



Genevieve Leveille ( COO )

爱沙尼亚国家区块链区块链技术顾问、数字货币影响力机构创始人。毕业于美国哥伦比亚大学，具有在信息技术和服务行业工作的经历。有较强的创业精神，擅长现金、市场风险、流动资金管理、金库和业务转型。



Alexander von Preysing (金融顾问)

曾任德意志交易所高级副总裁、发行服务部总裁。2002年加入德意志交易所，先后负责多个部门，精通债券、私募基金、风险管理、IPO等业务，并作出良好的业绩。



## 十、风险提示与免责声明

## 十、风险提示与免责声明

### 10.1 风险提示

#### 由于用户个人错误行为造成的风险:

##### 1)由于私钥遗失带来的风险

在 YDS Token 分配给参与者前,参与者会获得和 YDS Token 相关联的公钥账户, YDS Token 公钥账户可以通过参与者随机分配的私钥进入, 私钥遗忘将可能失去在相关联公钥账户的 YDS Token。建议多练习如何操作以便于参与者能够安全的将私钥在多个本地设备中备份, 最好在非网络环境进行操作。

##### 2)由于私钥泄漏给第三方的风险

任何第三方的个人或机构在获得了参与者的公钥账户的私钥后, 有可能就会处理其相应账户的 YDS Token。建议参与者保护好相关的设备, 防止未授权登陆, 降低风险几率。

##### 3)由于参与投票可能会出现的风险

YDS Token 持有者在参与投票中, 由于恶意或者不负责任的投票行为, 极有可能导致 YDS 丢失。

#### 由于在使用 YDS Token 期间网络安全相关的风险:

##### 1)基于以太坊网络协议带来的相关风险

YDS 在初期会发行基于以太坊协议开发的 ERC20 代币, 以太坊

协议上的任何故障和未知的功能，都有可能导致 YDS 出现未知的不希望发生的情况。以太坊和基于以太坊协议的本地单元账户，有可能会像 YDS 一样失去任何价值。

## 2)非官方的 YDS 网络替代的风险

在 YDS 网络系统开发出来后，由于是开源的代码和协议极有可能存在被其他人抄袭并建立类似的网络系统。官方的 YDS 网络系统有可能需要同这些抄袭的网络系统竞争，由此带来对 YDS 网络系统的负面影响需要所有用户承受。

## 3)来自恶意第三方的不法入侵的风险

黑客、其他团队或机构等恶意第三方，可能会试图干预 YDS 网络系统的发展，可能会采用但是不限于以下的方式：DDOS、Sybil、spoofing、smurfing 或者基于共识机制的攻击等。

## 4)由于 YDS 网络系统存在基础设施软件安全漏洞的风险

本网络系统是一个开源的系统，存在 YDS 的员工或者其他第三方机构有意或无意引入 bug 到网络核心系统中去，如此会导致 YDS 的使用风险和损失。

5)密码学领域的重大技术突破会造成隐藏的弱点被挖掘和利用的风险

密码学技术是区块链技术的重要部分，密码学的进步或其他高科技技术的发展，可能会对 YDS 网络系统和 YDS Token 带来被盗或者丢失的风险。

#### 6)YDS 网络系统故障的风险

YDS 网络作为比较高新的系统，可能会产生让人不能够接受或意想不到的网络故障，同时也有可能导致 YDS Token 消失的风险或其他对市场造成波动的风险。

#### 7)YDS 可能会因为其高价值出现被挖矿攻击的风险

对于很多去中心化的密码学代币和虚拟货币，YDS 网络系统的区块链技术生成的 YDS 有被挖矿攻击的可能，其中包括并不局限于双重攻击、大矿池攻击、“自私挖矿”攻击和竞争条件攻击等，也可能出现未知的更新颖的挖矿攻击，对 YDS 网络系统的运行带来巨大的风险。

#### **由于市场的不确定性造成的风险：**

##### 1)YDS 系统用户量少的风险

YDS 系统会随着时间产生相应的价值，如果 YDS 网络系统不被更多的商业、个人或者其他机构使用，不能够产生更多的公众关注度对其发展造成使用人数少的影响，可能会限制或降低 YDS 的使用和价值。

## 2)YDS 来自交易所造成的流动性不足的风险

目前 YDS Token 还未在交易所进行交易，如果在交易所开放交易后，很有可能会因为交易所比较新对于各种法律法规了解的少，比起那些成立时间久声望好有其他成熟虚拟代币正常交易的交易所来说，新交易所很容易出现欺诈和失败的可能。交易所的问题可能会造成有很大一部分 YDS Token 交易陷入欺诈或其他运营风险问题，如此会导致 YDS 的价值和流动性降低。

## 3)YDS 网络系统的发展跟不上 YDS Token 持有者预期的风险

YDS 网络系统当前还处于开发阶段，而且在对外正式发布前可能会有很大的变化，参与者对 YDS Token 或者网络系统的预期可能跟实际的发布时间会不同，同时也可能会在设计和执行上的实际情况的变化导致不能按计划发布。

## 4)参与者在面对损失时无法得到保险的风险

YDS Token 公钥账户和银行账户、其他金融机构账户或者其他社交服务账户不同，YDS 基金会通常不会对网络系统购买保险。当出现 YDS 丢失或者网络系统失去价值时，不会有任何保险机构可以对 YDS 的持有者提供索赔服务。

## 5)YDS 项目解散的风险

YDS 项目会存在各种因素，比如比特币、以太坊的价值大跌、

商业运作失败或者因为知识产权索赔等，YDS 项目或许会无法继续运营从而导致不能成功发布或者团队解散。

## 6)相关地区和国家的司法或行政部门的监管政策的风险

区块链技术目前在世界范围内都获得了支持或认可，但是同时也受到了各种监管部门的仔细审查。YDS 网络和 YDS 的功能可能会受到部分监管政策的影响，其中包括但是不限于限制使用或者拥有 YDS Token，由此可能会阻碍或者限制 YDS 网络系统的发展。

## 7)其他未知的风险

区块链技术和相应的数字货币技术 是相对比较新的并且未经完全验证的科技，可能会出现更多无法预测的风险，风险可能会以更多的方式出现。

这份文件可能随时会被修改或者置换，然而我们没有任何义务更新此版本白皮书，或者提供读者额外资讯的渠道。

## 10.2 免责声明

本声明不涉及与证券招标以及承担 YDS 经营性的相关风险

不涉及任何在司法管制内的受管制产品：本文件是项目阐述的概念性文件【白皮书】，并非出售或者征集招标与 YDS 产品及其相关公司的股份、证券或其他受管制产品。根据本文件不能作为招股说明

书或其他任何形式的标准化合约文件，也并不是构成任何司法管辖区内的证券或其他任何受管制产品的劝告或征集的投资建议。本文件不能成为任何销售、订阅或邀请其他人去购买和订阅任何证券，以及基于此基础上形式的联系、合约或承诺。本白皮书并没有经过任何国家或地区的司法监管机构审查。

**不作为参与投资的建议：**在本文件中所呈现的任何信息或者分析，都不构成任何参与代币投资决定的建议，并且不会做出任何具有倾向性的具体推荐。您必须听取一切有必要的专业建议，比如税务和会计梳理相关事务。

**不能构成任何声明和保证：**本文件用于说明我们所提出的 YDS 平台与 YDS Token，但是 YDS 基金会明确表示：1)对于本文件中描述的任何内容的准确性或完整性，或者以其他方式发布的与项目相关的内容，不给予任何声明和保证；2)在没有前提条件的情况下，不能对任何具有前瞻性、概念性陈述的成就或合理性内容给予任何声明和保证；3)本文件中的任何内容，不作为任何对未来的承诺或陈述的依据；4)不承担任何因白皮书的相关人员或其他方面造成的任何损失；5)在无法免除的法律责任范围内，仅限于所适用法律所允许的最大限度。

**不是任何人都可以参与项目：**YDS 的网络系统和 YDS 并不是任

何人都可以参与，参与者可能需要完成一系列的步骤，其中包括提供表明身份的信息和文件。

非授权公司与该项目无关：除了 YDS 基金会和 YDS 之外，使用其他任何公司或者机构的名称商标，并不说明任何一方与之有关联或认可，仅供说明相关内容之用。

与 YDS Token 相关的注意事项：“YDS Token” 或 “YDS ”，是 YDS 区块链网络的虚拟密码学代币。

YDS 不是虚拟货币：在本文件未完成期间，YDS 不能在交易所兑换物品、服务和交易，也不能在 YDS Token 网络以外使用。

YDS 不是投资品：没有任何人能够保证，也没有任何理由相信，你所持有的 YDS Token 将会一定升值，甚至有可能存在贬值的风险。

YDS 不是所有权证明或具有控制权：持有 YDS Token 并不是授予持有者所有权以及 YDS 和 YDS 网络系统的股权；也并不是授予其直接控制或者替 YDS 和 YDS 网络系统做任何决策的权利。