华资基金集团

Company introduction

ZHSH

白皮书

基于第二代区块链技术商业应用生态模式

Based on the second generation block chain technology, a commercial application ecological mode.

版权声明

- Copyright declaration -

本白皮书由 ZHSH 团队编写，严禁抄袭，如需转载，请注明出处，因此本白皮书中所涉 及到的所有的产品设计理念、技术设计方案以及技术解决方案，其知识产权，均属于 ZHSH 团队所有，团队已对核心的技术方案部分申请知识产权保护，对于任何侵犯 ZHSH 知识产权 的行为，将通过法律手段保护我们的权益，望周知。

目 录

Contents

前 言

随着新一轮产业革命的到来，云计算、大数据、物联网、区块链等新一代信息技术在智能 制造、金融、能源、旅游等行业中的作用愈发重要。而在此轮产业革命中，区块链信息技术的 发展尤为迅速， 逐步成为各行业深化信息技术应用的方向。目前发展趋势和区块链技术发展演 进路径来看，区块链技术和应用的发展需要云计算、大数据、物联网等新一代信息技术作为基 础设施支撑，同时区块链技术和应用发展对推动新一代信息技术产业发展具有重要的促进作 用，这恰好正是这场技术革新风潮奠基了一个历史前提。

基于此前提背景下，区块链众所周知的技术特性:以其可信任性、安全性和不可篡改性， 让更多数据被解放出来，推进数据的海量增长。区块链的去中心化特性使得数据从采集、交易、 流通，以及计算分析的每一步记录都可以留存在区块链上，使得数据的质量获得前所未有的强 信任背书，也保证了数据分析结果的正确性和数据挖掘的效果。区块链能够进一步规范数据的 使用，精细化授权范围。对于数据交易流通，则有利于突破信息孤岛，建立数据横向流通机制，并 基于区块链的价值转移网络，逐步推动形成基于全球化的数据交易场景，顺应此场景，商业链领域亦 由此进入了区块链应用时代大潮。

商业产业链是一个门槛极高的产业领域，所针对的群体是由政府、地产、产业上下游等巨头所组 成，领域内涉及到生活类消费、线上结合交易、互联娱乐消费、线下交易消费以及一系列链条式产业， 因此，对安全系数、保密性、契约精神等方面，有着极为严苛的技术要求，而如何借助当前大数据的 浪潮下推进业态发展，借助区块链不可篡改的、全历史的数据库存储技术成为了历史进程的重要助推 动力，巨大的区块数据集合包含着每一笔商业产业链下的业务全部历史，随着区块链的应用迅速发展，

数据规模会越来越大，不同的业务场景也催生了区块链。

PART 01 背景介绍

ZHSH Background

一、背景介绍 ZHSH Background

作为技术创新的区块链

1.1 区块链 1.0 阶段——数字货币

2009 年初，比特币网络正式上线运行。作为一种虚拟货币系统，比特币的总量是由网络 共识协议限定的，没有任何个人及机构能够随意修改其中的供应量及交易记录。在比特币网络 成功运行多年后，部分金融机构开始意识到，支撑比特币运行的底层技术——区块链实际上 是一种极其巧妙的分布式共享账本及点对点价值传输技术，对金融乃至各行各业带来的潜在影 响甚至可能不亚于复式记账法的发明。

以区块为单位的链状数据块结构:区块链系统各节点通过一定的共识机制选取具有打包交 易权限的区块节点，该节点需要将新区块的前一个区块的哈希值、当前时间戳、一段时间内发 生的有效交易及其梅克尔树根值等内容打包成一个区块，向全网广播。由于每一个区块都是与 前续区块通过密码学证明的方式链接在一起的，当区块链达到一定的长度后，要修改某个历史 区块中的交易内容就必须将该区块之前的所有区块的交易记录及密码学证明进行重构，有效实 现了防篡改。

1.2 区块链 2.0 阶段——智能合约

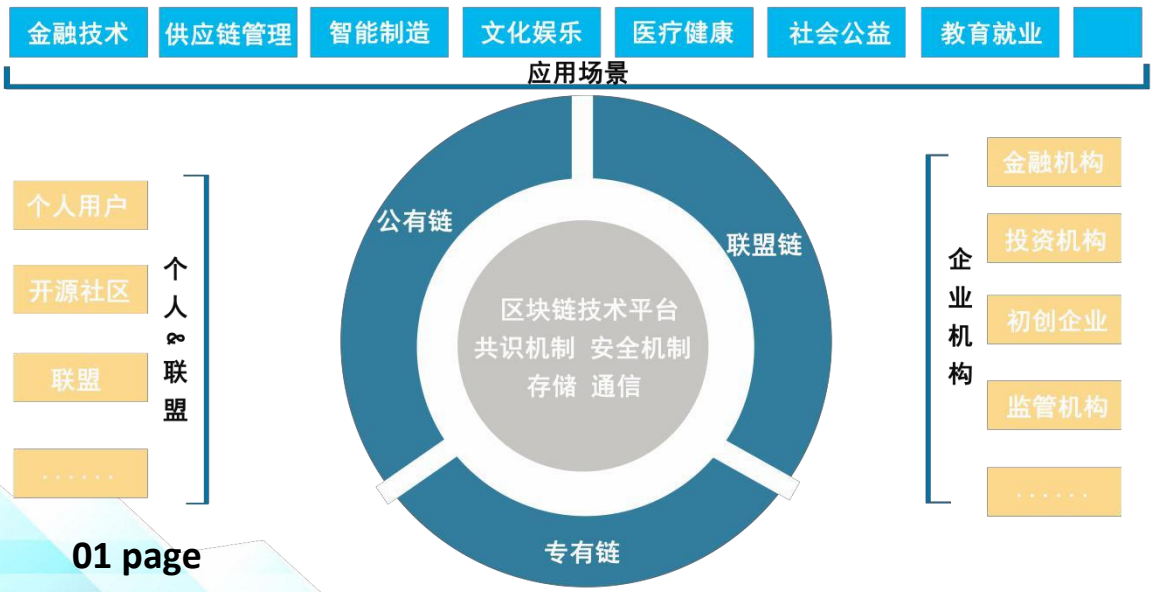
2014 年前后，业界开始认识到区块链技术的重要价值，并将其用于数字货币外的领域， 如分布式身份认证、分布式域名系统、分布式自治组织等。这些应用称为分布式应用(DAPP)。 用区块链技术架构从零开始构建 DAPP 非常困难，但不同的 DAPP 共享了很多相同的组件。区 块链 2.0 试图创建可共用的技术平台并向开发者提供 BaaS 服务，极大提高了交易速度，大大 降低资源消耗，并支持 PoW、PoS 和 DPoS 等多种共识算法，使 DAPP 的开发变得更容易。

随着区块链技术和应用的不断深入，以智能合约、DAPP 为代表的区块链 2.0，将不仅仅只 是支撑各种典型行业应用的架构体系。在组织、社会等多种形态的运转背后，可能都能看到 区块链的这种分布式协作模式的影子。可以说，区块链必将广泛而深刻地改变人们的生活方式。 区块链技术可能应用于人类活动的规模协调，甚至有人大胆预测人类社会可能进入到区块链时代，即区块链 3.0。

1.3 区块链 3.0 阶段——新商业产业链下的区块链应用

ZHSH 是一个基于以太坊的去中心化、社交性的、全开源的、数字资产与其他资源、并有 娱乐消费集合为一的综合性平台。设计发布的开源软件是 ETH 网络的一个分支，是一种 P2P 形式的数字货币。与大多数货币不同，ZHSH 不依靠特定货币机构发行，它依据特定算法，通 过大量的计算产生。ZHSH 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 Token 来人为操控币值。基于密码学的设计可以使 Token 只能被真实的拥有者转移或支付，这同样确保了货币所有权与流通交易的匿名性。基于智能手 机的无处不在、以及频宽的成长。

1.4 区块链：产业数据化的技术



新商业产业数据化的技术在区块链技术的应用下产生了实际场景的变迁，新商业产业数据 化的技术在传统意义上泛指契约型金融机构在内的大部分产业链机构运作下的相关业务，是指 以契约方式在一定期限内从合约持有者手中吸收资金，然后按契约规定向持约人履行赔付或资 金返还义务的金融机构。包括后商业市场的各种线上消费、线下支付、娱乐互动、生活类交易 和买卖契约等。这类机构的特点是资金来源可靠而且稳定，资金运用主要是长期投资，契约型 金融机构是资本市场上重要的机构投资者。

随着全球商业的发展，商业市场的行业痛点及改革方向，一定是从产品因素向以 人的因素 为主转移，人的因素会更多显现出来。为了解决这一难题，ZHSH 与多家商业机构达成战略合 作，并率先规模化推出“ZHSH 智慧全球应用计划”项目，一种基于商业习惯、线上消费、线 下支付、生活类交易、娱乐互动、金融运作等使用和消费习惯数据样本为基础的区块链模式。

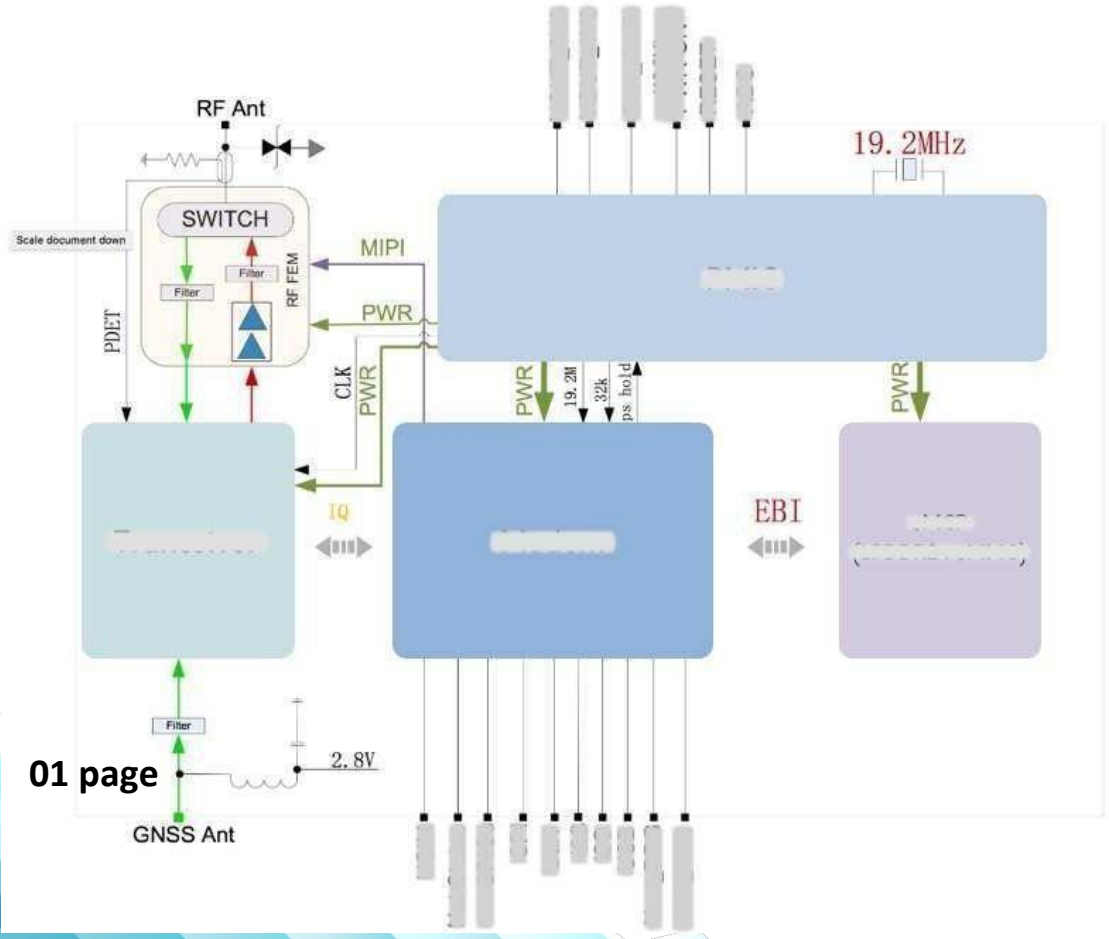
如今有了区块链的发展和技术广泛应用，让“商业产业+科技”的状态向 “商业产业数据 化的技术”演化，在商业产业链内的应用区块链技术，彻底改变商业购买前后的业务中合作体 系的实际需求，从而解决了交易中的信任和安全问题，成为未来 ZHSH 未来发展趋势。通过区 块链，交易双方可在无需借助第三方信任中介的条件下开展业务活动，从而降低资产能够在全 球范围内线上交易、线下支付、生活类

应用、娱乐互动、等成本和资金运转的速度，以技术促 进商业产业的优化进程。

1.5 区块链在支付消费领域的应用场景

现如今区块链成为各种科技领域的大热门，区块链技术在各个行业领域有着广泛的应用。 那么，“商业产业下区块链+ZHSH 数字钱包支付”这个组合是否具有可行性，是否能达到人们的预期，还要进一步验证。未来区块链在该领域的模式中应用与发展，是否有发展前景呢?

“谁拥有用户的数据?谁应该使用这些数据?”现在这些问题不再头疼，因为区块链 可以解决这些问题并可以借助区块链来创建商业数据市场的机制。对于消费方来说，一 方面可以通 过 ZHSH+区块链结合的产品与服务，享受智能时代下，商业支付带来的全球智慧生活，获取基 于消费行为的区块链奖励收益，另一方面，在商业方面，区块链技术更有补充现有金融服务体 系内的不足，继而形成更多的金融产品满足商业的消费群体实际需求。



1.6 区块链技术将解决哪些问题

1.6.1 信息安全性问题

在信息存储方面，层出不穷的黑客攻击以及信息盗窃，用户的信息安全问题成 了信息存储 的重要问题，以往中心化的信息流通模式让信息数据的安全性降低， 一旦黑客攻克了一个中心 数据库，与之相关的所有数据就会泄露，对企业或者个人而言，有着不可估量的损失。而区块 链分布式记账方式让信息安全得到更加牢靠的保护。

1.6.2 信息数据的真实性

在企业信息系统上，数据造假也屡有发生，被篡改的数据将会给企业或个人带来严重的后 果，而区块链不可修改性则杜绝了此类情况，在区块链技术中，除非同时控制系统 50%以上的 有效节点，才能修改数据，而随着区块链的应用，越来越多的数据节点将纳入区块链的运行系 统中，而控制全球 50%以上的节点更是不可能的事。数据的真实性将得到保证。

1.6.3 信息数据的高效流通

在传统的信息传输中，无法避免的一个问题就是中心化问题，用户之间的信息传播必须先 经过中心节点，才能传达到另一个用户手中，传输过程极大的耗费用户的时间，而去中心化， 就实现了信息流的直接传输，点到点的运行系统，让用户间的信息沟通更加快捷。

PART 02 ZHSH 阐述

ZHSH This paper

二、ZHSH 阐述 *ZHSH This paper*

2.1 什么是 ZHSH?

ZHSH 团队致力于打造全球最具有竞争力的商业市场应用链——在商业联盟区域内的消 费场景。团队在 2018 年 2 月基于第二代加密技术运用并优化其功能，计划于 2018 年下半年开 始向市场发行 ZHSH，总量为 1.3 亿枚，均以计算机和手机移动客户端挖矿式流通，同时保持 永不增发的政策以维持数位货币的价格稳定性。

与大多数货币不同，ZHSH 不依靠特定货币机构发行，它依据特定算法，通过大量的计算 产生。ZHSH 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。基于密码学的设计可以使 ZHSH 只能被 真实的拥有者转移或支付，这同样确保了货币所有权与流通交易的匿名性。

2.2 ZHSH 生 态

ZHSH 生态建设基于以太坊去中心化、智能合约技术，建设支付系统应用全球性，其应用 包括直营+联营 B2B、B2C 商城平台、直播线上消费、签约商家线下消费、平台生活类缴费。

2.2.1 商业应用

ZHSH 区块链技术则去除了对中央权威机构的依赖。由于区块链技术是以点对点的方式处 理交易，分布式的结构使其不需要第三方机构来对交易进行记录和结算。因此，建立在区块链 基础上的应用系统有着“去中介化”的特征。这可能改变现有以集中清算为特征的应用系统。

2.2.2 创造直接价值

ZHSH 区块链在线上、线下、娱乐、商城支付领域目前是其技术应用中进展最快的，区块 链技术能够避开繁杂的系统，在付款人和收款人之间创造更直接的付款流程，不管是境内转账 还是跨境转账，这种方式都有着低价、迅速的特点，而且无需中间手续费。区块链技术初级应 用体现在跨境支付的分布式账本中，如今的跨境支付网络是分散和孤立的，造成了成本缺乏竞 争性、结算时间长以及用户体验糟糕的情况。跨境支付必须靠不同的消息传递协议和结算协议 利用各种代理银行关系进行处理，统计显示，这些低效率问题每年令生态系统中所有的参与者共 耗费 1.6 万亿美元。

ZHSH 是结合线上、线下支付应用平台、其利用通用的全球基础架构将这些孤立的网络连 接起来，以分布式账本做到实时结算、确保交易的确定性，并减少风险，以此提高金融结算效率。

2.2.3 除去中心化间点

ZHSH 应用系统则可省去第三方金融机构的中间环节，让双方跨境网络支付结算交易通过 点对点的方式快速、自由地完成;同时还能全天候支付、实时到账、提现简便且没有隐性成本。 不仅如此，因为区块链安全、透明、低风险的特性，还可提高国内

/跨境支付、的安全性，并 加快结算与清算速度，大大提高资金利用率。根据麦肯锡的测算，从全球范围看，区块链技术 在 B2B 国内/跨境支付与结算业务中的应用，将可使每笔交易成本从约 26 美元下降到 15 美元。

2.2.4 ZHSH 的庞大应用

在当前线上、线下交易场景中，加密货币并没有被广泛使用。随着加密货币的用途和理念 日益普及，相信在不久的将来，加密货币也会融入到我们的日常生活与消费中。例如:每年， 在消费者和商家之间产生的消费规模预计达 22 万亿美元。人们用当地货币支付所有的消费， 从每天早上的一杯咖啡到每周的购物。ZHSH 正在推动线上、线下、生活缴费、娱乐全面接受 加密货币。通过利用现有的 ZHSH 生态系统，ZHSH 将会大大加速加密货币的大众化过程。

ZHSH 全球支付将要实现的是创造一个全球通用并且可以代替传统银行的业务。通过使用 ZHSH 您可以安全存储资金，并随时随用任何货币进行交易，包括加密币。所有的操作都可以 通过全球商家上安装的 ZHSH 平台网络节点应用程序完成。ZHSH 创建的数字钱包，可以代替 传统的商业支付模式，使您能够在世界任何地方，用任何类型的货币完成付款交易。

2.3 ZHSH 的算法描述

发行名称:ZHSH(简

称:ZHSH) 数量:恒定 1.3

亿枚

机器运行区分:手机客服端和计算机客户端

机器运行计划:2018 年 7 月 1 日开放运行苹果 APP 和安卓 APP 客户端，

2019 年 10 月 10 日

前配合上交易所时间开放运行电脑客户端。 目标:打造全球最具有竞争力的商业市场应用链——在联盟区域内的消费场景，均可用

ZHSH 进行消费。在 ZHSH 的平台内，每一位用户可以自由注册一个独立的分布式账户，你获 得多少货币，取决于你挖矿贡献的有效工作。

ZHSH 钱包的算法方式主要是采用 POW 模式(工作证明)，根据用户持有的 ZHSH 矿机算 力的大小，分配相应币数，在 POW 模式下，每个 ZHSH 数字资产钱包可享受到挖矿带来的算力 收益，直至全部产完。

2.3.1 分配方案

团队与基金会占有 3000 万枚币，公开发行数量为 2800 万枚币 矿机挖矿产生 7200 万 枚 币

2.4 ZHSH 的价值

在 ZHSH 的平台上，具有的价值表现在以下几个方面:

一是高效率性；去传统中心转发架构后支付时间由分钟缩减至秒级；

二是高可用性；分布式架构任一个节点出故障不影响整个系统的运作；

三是高安全性；处于一个私有链封闭的网络环境中报文难篡改难伪造；

四是高扩展性；新的参与者可以快速便捷地部署和加入至系统中；

五是全球化应用：在全球范围落地支付、数字化资产支付让全球世界资产形成一个庞大的商业帝国；

六是全球交易集点；随着全球资产的无现金化规划、全球支付将集点以点对点支付方式，全部必须通过 ZHSH 支付平台;

七是国内唯一性；国内唯一在世界商业行业有话语权的区块链商业资源综合流通技术;

八是商业生态圈；世界商业资源综合利用、运输、发展的迫切需求和全力以赴的技术基础；

九是三链结构；唯一的商业资产资源产业链和消费链，应用支付链完美结合的三链并融的系统架构。

PART 03 ZHSH 技术构架

ZHSH Technical architecture

三、ZHSH 技术构架 *ZHSH Technical architecture*

3.1 平台设计

3.1.1 共识机制——POC

ZHSH 的模块化设计，支持共识机制在内的所有核心功能模块的替换与插拔。主链默认采 用信用共识机制 POC(Proof-Of-Credit)。任何人都可以参与到区块链网络，每一台设备都能作为 一个节点，每个节点都允许获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争 计算共同维护整个区块链。任一节点失效，其余节点仍能正常工作。

共识机制是区块链技术的一个核心问题，它决定了区块链中区块的生成法则，保证了各节 点的诚实性、账本的容错性和系统的稳健性。基于区块链技术的不同应用场景，以及各种共识 机制的特性，主要可以从性能效率、资源消耗、容错性、监管水平等几个方面进行评价和比较；共识机制功能组件具备以下功能：

(a) 支持多个节点参与共识和确认;

(b) 支持独立节点对区块链网络提交的相关信息进行有效性验证;

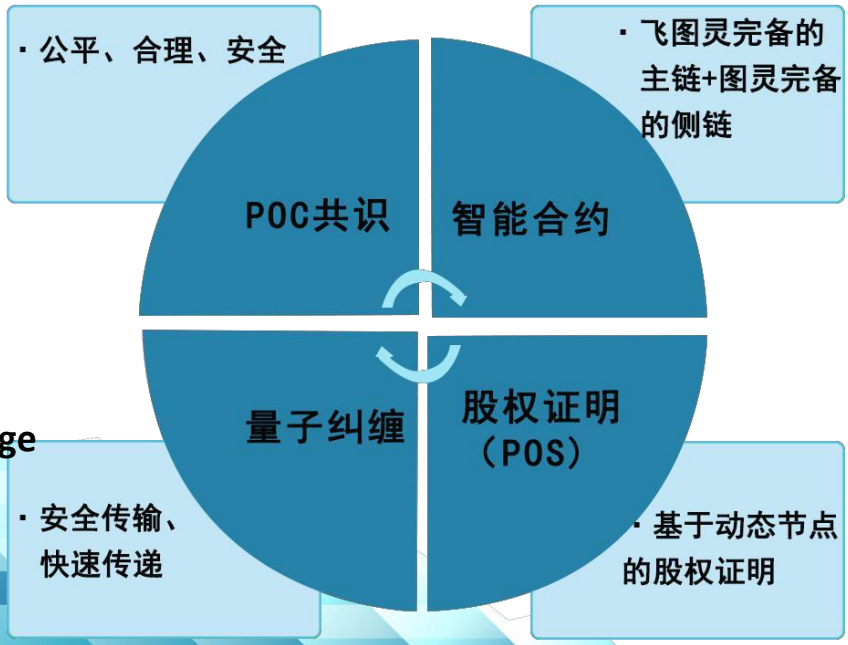
(c) 防止任何独立的共识节点未经其他共识节点确认而在区块链系统中进行信息记录或 修改;

(d) 应具备一定的容错性，包括节点物理或网络故障的非恶意错误，以节点遭受非法控 制的恶意错误，以及节点产生不确定行为的不可控错误。

3.1.2 股权证明——POS

POS 也称股权证明，类似于财产储存在银行，这种模式会根据你持有数字货币的量和时 间，分配给你相应的币。简单来说，在股权证明 POS 模式下，有一个名词叫币龄，每一个币 每天产生 1 币龄，比如你持有 100 个币，总共持有 30 天，那么你的币龄是 3000，这个时候， 如果你发现了一个 POS 区块，你的币龄就会被清空为 0，你每被清空 365 币龄，你将获得从区 块中获得 0.05 个币，那么在此案例中，利息=3000*5%/365=0.41 个币，这样让持币有利息，POS 模式下还有一大好处就是节省资源，仅需较低的算力就能维持整个区块链网络的运作，有的甚 至通过前期的短时间挖矿阶段直接进入纯 POS 模式，实现后期无需挖矿仅靠运行钱包客户端 就能确认全网交易。

POS 相对于 POW 是种完全不一样的机制，POS 不需要大量的算力来维持网络安全，只是需 要每个参与者打开自己的钱包在线增加网络权重，同时获取相应的奖励，也就是 POS 机制本 身所说的利息。



3.1.3 智能合约

ZHSH 打造的是非图灵完备的主链和图灵完备的侧链相结合的智能合约。智能合约是编程 在区块链上的汇编语言。通常人们不会自己写字节码，但是会从更高级的语言来编译它，例如

用 Solidity，Javascript 类似的专用语言。这些字节码确实给区块链的功能性提供了指引，因此 代码可以很容易与它进行交互，例如转移密码学货币和记录事件。代码的执行是自动的:要么 成功执行，或者所有的状态变化都撤消。这是很重要的，因为它避免了合约部分执行的情况(例 如，在证券购买交易中，证券所有者已经转移发送了证券，但是密码学货币的支付转移却失败 了)。在区块链环境中， 这尤为重要，因为没有办法来撤消执行错误所带来的不好的后果(而 且如果对手不配合的话，根本就没有办法逆转交易)。

基于区块链的智能合约不仅能发挥智能合约低成本高效率的优势，而且可以避免恶意行为 对合约的正常执行的干扰。将智能合约以代码化的形式写入区块链中，利用区块链技术实现数 据存储、读取及执行过程可追踪透明化且不可篡改。此外利用区块链的共识算法构造的状态机 系统能使智能合约高效的运行。

3.2 智能合约的功能组件包括

A 开发运行环境，包括:

（1）提供编程语言支持，必要时可提供配套的集成开发环境;

（2）支持合约内容静态和动态检查;

（3）提供运行载体支持，如虚拟机等; (4)对于与区块链系统外部数据进行交互的智能合约，外部数据源的影响范围应 仅限于智能合约范围内，不应影响区块链系统的整体运行。

B 存储环境，包括:

（1）防止对合约内容进行篡改

（2）支持多方共识下的合约内容升级;

（3）支持向账本中写入合约内容。

3.1.4 量子纠缠加密技术

ZHSH 采用是量子纠缠技术，是安全的传输信息的加密技术。与超光速传递信息相关。这些粒子之间“交流”的速度很快，利用这种联系以如此快的速度控制和传递信息。 同时区块链中也使用非对称加密的公私钥对来构建节点间信任。

非对称加密算法由对应的 一对唯一的密钥(即公开密钥和私有密钥)组成，任何获悉用户公钥的人都可用用户的公钥对 信息进行加密与用户实现安全信息交互。由于公钥与私钥之间存在依存关系，只有持有私钥的 用户本身才能解密该信息，任何未经授权的用户甚至信息的发送者都无法将此信息解密。加密 功能组件具备以下功能:

支持国际主流加密算法，如 AES256 等对称加密算法和 RSA、ECC 等非对称加密算法;

支持商密算法，如 SM4、SM7 等对称加密算法和 SM2、SM9 等非对称加密算法;

应具备明确的密钥管理方案，确保区块链底层安全机制正常运行;

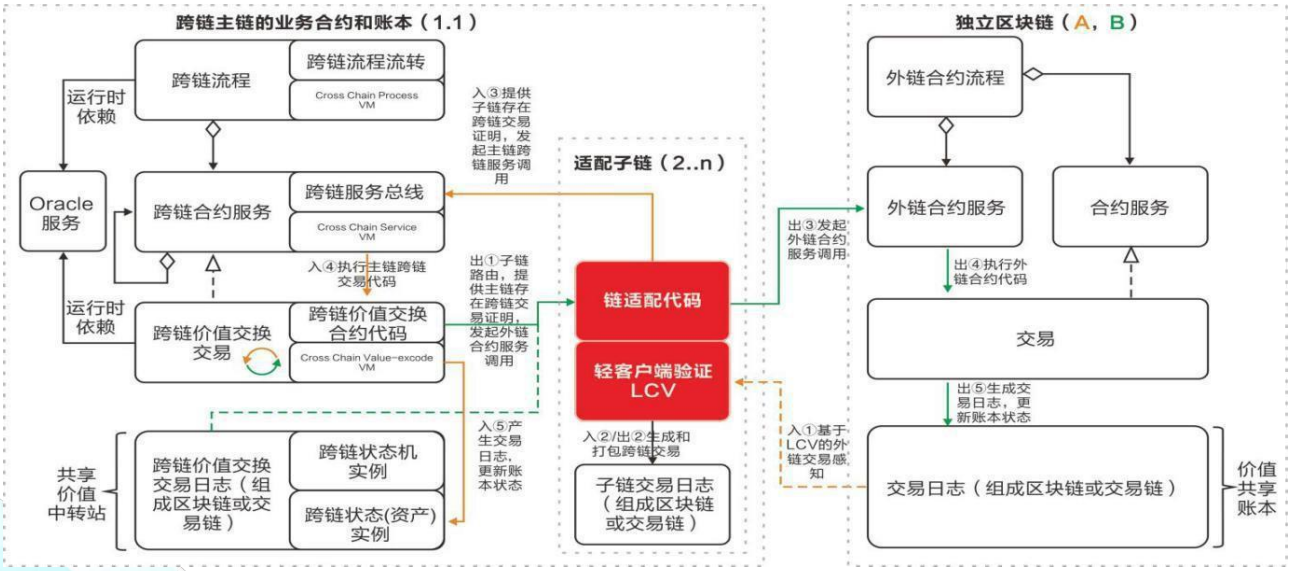
加密算法应具备抵御破解的能力，宜定期审核加密算法的安全性，必要时采用更高 破解计算复杂性的加密算法。

3.1.5 多链(主链-子链--子链)

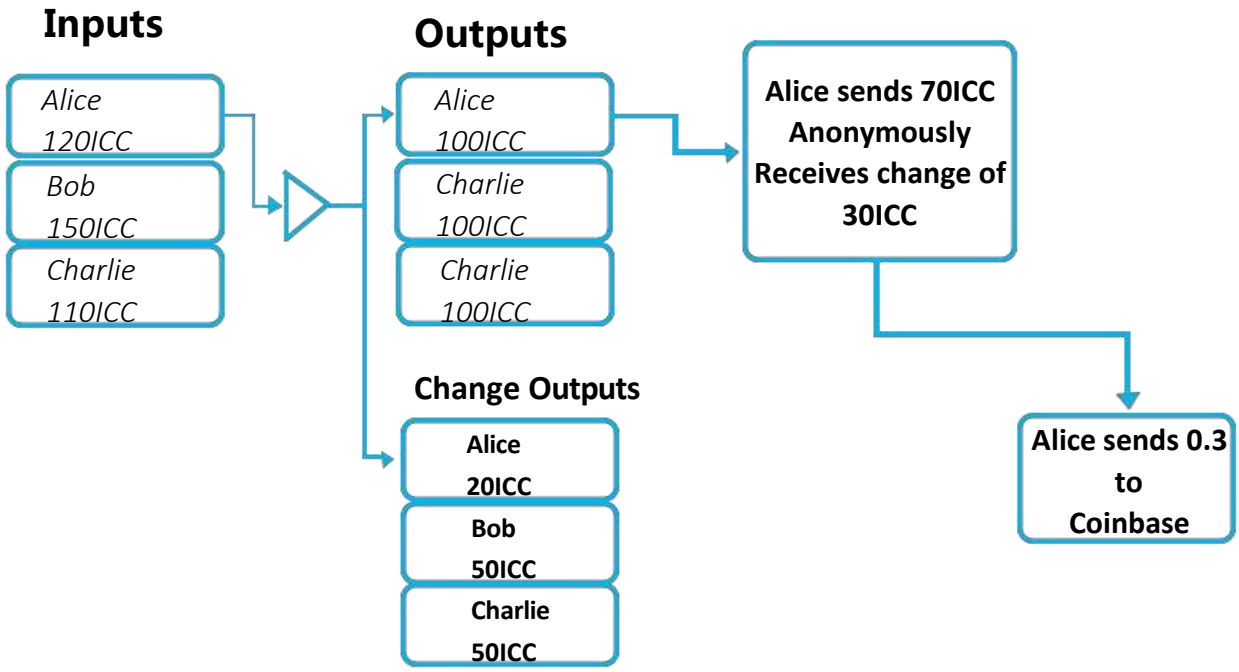
独立区块链完成相关性较高的业务领域的价值生产，要实现社会化商品和价值 大流通，就需要跨链交易市场，通过跨链提供的跨链价值交换市场满足价值在不同 主体自由等价流通。跨 链具有兼容性，可以与现有、未来各种区块链兼容;跨链具有开放性，跨链具备让任何区块链 接入的能力;跨链具有标准化潜力，让任何区块链接入，会渐渐形成一种接入标准，有助于推 动区块链协议的标准化。

根据业务功能、隐私保护、数据隔离、或者性能容量扩展的需求，ZHSH 建立多个独立的 链并行工作，链和链之间可以通过跨链服务进行交互，如发送交易，查询交易结果，读取配置 数据等。不同区块链间的智能合约数据交互，使得区块链之间构建了互操作性，在复杂的业务 场景下，可以设计出细粒度运作的独立子链(逻辑/物理)，并通过母-子智能合约满足不同的 业务需求，提升了全局“臃肿”账本的灵活度。

ZHSH 通过跨链技术，将商圈型私有链/联盟链融入到主链的共识网络中去，同时又能保 有私有链/联盟链的隐私和许可的防护措施。根据业务功能、隐私保护、数据隔离、或者性能 容量扩展的需求，建立多个独立的链并行工作，链和链之间可以通过跨链服务进行交互。其他 数字资产连入 ZHSH，首先需要在 ZHSH 上完成注册，可通过自主开发或定制开发，接入 ZHSH， 实现互通互联。



在 ZHSH 区块链网络中:“主链”构成了信息主干道，不同的母链之间通过链路由协议交换信 息。同时，一个主链上承载着不同的同构子链，这些子链是某个垂直领域或多个异业集群的分 布式账本实现。子链间的通信则由跨链通信协议实现。通过区块链的分片，提高区块链系统的



交易处理能力。相较于一条单独的区块链系统，链集群系统可以通过连接多条子链的方式在交 易处理能力上直线增长。交易的请求通过链路由的分配进入不同子链，可以有效规避针对一条 子链的集中请求。此外，我们可以在链路由上部署同构子链的不同节点数的集群，对于同构链 而言，多节点数量的集群会有相对较高的安全性，少节点集群的处理速度则更快。此外，根据 节点数量，地理位置，业务分类等不同需求，部署不同的链集群，对应不同需求将请求分发到 合适的集群之中处理，帮助链网络根据业务需求灵活部署，为用户提供更高质量的区块链服务。

3.1.6 非对称性加密

椭圆曲线加密法(ECC)是一种公钥加密技术，以椭圆曲线理论为基础，在创建密钥时可 做到更快、更小，并且更有效。ECC 利用椭圆曲线等式的性质来产生密钥，而不是采用传统的 方法利用大质数的积来产生。椭圆曲线加密法 ECC(EllipticCurveCryptography)是一种公钥加 密技术，以椭圆曲线理论为基础，利用有限域上椭圆曲线的点构成的 Abel 群离散对数难解性， 实现加密、解密和数字签名，将椭圆曲线中的加法运算与离散对数中的模乘运算相对应，就可 以建立基于椭圆曲线的对应密码体制。椭圆曲线是由下列韦尔斯特拉斯 Weierstrass 方程所确 定的平面曲线:

$$E:y2+a1xy+a3y=x3+a2x2+a4x+a6$$

椭圆曲线加密算法以其密钥长度小、安全性能高、整个数字签名耗时小， 使其在智能终端 应用中有很大的发展潜力，比如掌上电脑、移动手机等都能有更好的表现。而在网络中，ECC 算 法也保证了其协同工作的实时性， 使用 ECC 算法加密敏感性级别较高的数据(如密钥)，速度 上能够满足大数据量要求，而且安全性高，能很好地保障系统的安全。

3.2 ZHSH 区块链的技术架构

3.2.1 复制证明与时空证明

在 ZHSH 协议中，存储供应商必须让他们的客户相信，客户所付费的数据已经被他们存 储。在实践中，存储供应商将生成"存储证明"(POS)给区块链网络(或客户自己)来验证。

在本节中，我们介绍和概述在 ZHSH 中所使用的“复制证明”n (PoRep)和“时空证明”(PoSt) 实现方案。

1. 动机

存储证明(POS)方案类似“数据持有性验证”(PDP)[2]和“可恢复性证明”(PoR)[3,4]方案。 它允许一个将数据外包给服务器(既证明人 P)的用户(既验证者 V)可以反复检查服务器是否 依然存储数据 D。用户可以用比下载数据还高效的方式来验证他外包给服务器的数据的完整 性。服务器通过对一组随机数据块进行采样和提交小量数据来生成拥有的概率证明作为给用户 的响应协议。

PDP 和 PoR 方案只保证了证明人在响应的时候拥有某些数据。在 ZHSH 中，我们需要更 强大的保障能阻止作恶矿工利用不提供存储却获得奖励的三种类型攻击:女巫攻击(Sybil attack)、外包攻击(outsourcing attacks)、代攻击(generation attacks)。

女巫攻击:作恶矿工可能通过创建多个女巫身份假装物理存储很多副本(从中获取奖 励)，但实际上只存储一次。

外包攻击:依赖于可以快速从其他存储提供商获取数据，作恶矿工可能承诺能存储比他 们实际物理存储容量更大的数据。

代攻击:作恶矿工可能宣称要存储大量的数据，相反的他们使用小程序有效地生成请求。 如果这个小程序小于所宣称要存储的数据，则作恶矿工在 ZHSH 获取区块奖励的可能性增加 了，因为这是和矿工当前使用量成正比的。

2.复制证明

“复制证明”(PoRep)是一个新型的存储证明。它允许服务器(既证明人 P)说服用户(既 验证者 V)一些数据 D 已被复制到它唯一的专用物理存储上了。我们的方案是一种交互式协 议。当证明人 P:(a)承诺存储某数据 D 的 n 个不同的副本(独立物理副本)，然后(b)通 过响应协议来说服验证者 V，P 确实已经存储了每个副本。据我们所知 PoRep 改善了 PDP 和 PoR 方案，阻止了女巫攻击、外包攻击、代攻击。

PoRep 方案使得有效的证明人 P 能说服验证者 V，数据 D 的一个 P 专用的独立 物理副 本 R 已被存储。PoRep 协议其特征是多项式时间算法的元组: (Setup, Prove, Verify)

PoRep.Setup(1λ, D) → R, SP，SV，其中 SP 和 SV 是 P 和 V 的特点方案的设置变量，λ 是一个安全参数。PoRep.Setup 用来生成副本 R，并且给予 P 和 V 必要的信息来运行 PoRep.Prove 和 PoRep.Verify。一些方案可能要求证明人或者是有互动的第三方去运算 PoRep.Setup。

PoRep.Prove(SP，R, c) → πc，其中 c 是验证人 V 发出的随机验证，πc 是证明人产生的 可以访问数据 D 的特定副本 R 的证明。PoRep.Prove 由 P(证明人)为 V

(验证者)运行生成 πc。PoRep.Verify(Sv，c, πc) → {0, 1}，用来检测证明是否是正确。 PoRep.Verify 由 V 运行和说服 V 相信 P 已经存储了 R。

3.时空证明 存储证明方案允许用户请求检查存储提供商当时是否已经存储了外包数据。我们如何使用

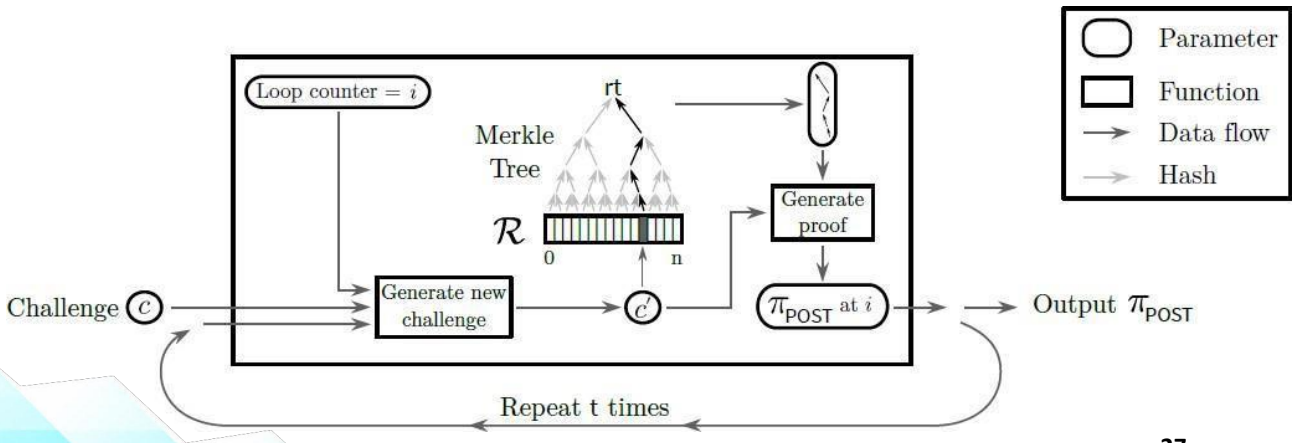
PoS 方案来证明数据在一段时间内都已经被存储了?这个问题的一个自然的答案是要求用户 重复(例如每分钟)对存储提供商发送请求。然而每次交互所需要的通信复杂度会成为类似 ZHSH 这样的系统的瓶颈，因为存储提供商被要求提交他们的证明到区块链网络。

为了回答这个问题，我们介绍了新的证明，“时空证明”，它可以让验证者检查存储提供商 是否在一段时间内存储了他/她的外包数据。这对提供商的直接要求是:(1)生成顺序的存储 证明(在我们的例子里是“复制证明”)来作为确定时间的一种方法 (2)组成递归执行来生成简单的证明。

4.PoRep 和 PoSt 实际应用

我们感兴趣的是 PoRep 和 PoSt 的应用构建，可以应用于现存系统并且不依赖于可信任 的第三方或者硬件。我们给出了 PoRep 的一个构建(请参见基于密封的复制证明[5]),它在 Setup 过程中需要一个非常慢的顺序计算密封的执行来生成副本。

PoRep 和 PoSt 的协议草图在图 4 给出，Post 的底层机制的证明步骤在图 3 中。



5.构 建 加 密 区 块

防碰撞散列 我们使用一个防碰撞的散列函数:CRH：{0, 1}* → {0, 1}O(λ)。我们还使用了 一个防碰撞散列函数 MerkleCRH，它将字符串分割成多个部分，构造出二叉树并递归应用 CRH， 然后输出树根。

zk-SNARKs 我们的 PoRep 和 PoSt 的实际实现依赖于零知识证明的简洁的非交互式知识, (zk-SNARKs)[6,7,8]。因为 zk-SNARKs 是简洁的，所以证明很短并且很容易验证。更正式地， 让 L 为 NP 语言，C 为 L 的决策电路。受信任的一方进行一次设置阶段，产生两个公共密钥: 证明密钥 pk 和验证密钥 vk。证明密钥 pk 使任何(不可信)的证明者都能产生证明证明 π， 对于她选择的实例 x，x∈L。非交互式证明 π 是零知识和知识证明。任何人都可以使用验证 密钥 vk 验证证明 π。特别是 zk-SNARK 的证明可公开验证:任何人都可以验证π，而不与产 生π的证明者进行交互。证明π具有恒定的大小，并且可以在| x |中线性的时间内验证。

可满足电路可靠的 zk-SNARKs 是多项式时间算法的元组:(KeyGen, Prove, Verify)KeyGen(1 λ,C)→ (pk, vk)，输入安全参数 λ 和电路 C，KeyGen 产生概率样本 pk 和 vk。这两个键作为 公共参数发布，可在 Lc 上用于证明/验证。Prove(pk, x, w) → π 在输入 pk、输入 x 和 NP 声 明 w 的见证时，证明人为语句 x∈LC 输出非交互式证明π。Verify(vk, x, π) → {0, 1} 当输入 vk，输入 x 和证明 π，验证者验证输出 1 是否满足 x ∈ LC。

通常而言这些系统要求 KeyGen 是由可信任参与方来运行。创新的可扩展计算完整性和隐 私(SCIP)系统[9]展示了在假设信任的前提下，一个有希望的方向来避免这个初始化步骤。

6. 密封操作

密封操作的作用是(1)通过要求证明人存储对于他们公钥唯一的数据 D 的伪随机排列副本 成为物理的独立复制，使得提交存储 n 个副本导致了 n 个独立的磁盘空间(因此是副本存储 大小的 n 倍)和(2)在 PoRep.Setup 的时候强制生成副本实质上会花费比预计响应请求更 多的时间。有关密封操作的更正式定义，请参见[5]。上述的操作可以用 SealτAES−256 来实现， 并且 τ 使得 SealτAES−256 需要花费比诚实的证明验证请求序列多 10-100 倍的时间。请注 意，对 τ 的选择是重要的，这使得运行 SealτBC 比证明人随机访问 R 花费更多时间显得更加 明显。

7.P o R e p 构 建 实 践

创建副本 Setup 算法通过密封算法生成一个副本并提供证明。证明人生成副本并将输出 (不包括 R)发送给验证者。

Setup inputs:

–prover key pair (pkP ,skP)

–prover SEAL key pkSEAL

–data D

outputs: replica R, Merkle root rt of R, proof πSEAL 证 明 存 储 Prove 算法生成副本的存储证明。 证明人收到来自验证者的随机挑战， 要求在树根为 rt 的 Merkle 树 R 中确认特定的叶子节 点 Rc。证明人生成关于从树根 rt 到叶子 Rc 的路径的知识证明。

Prove inputs:

7.P o R e p 构 建 实 践

创建副本 Setup 算法通过密封算法生成一个副本并提供证明。证明人生成副本并将输出 (不包括 R)发送给验证者。

Setup inputs:

–prover key pair (pkP ,skP)

–prover SEAL key pkSEAL

–data D

outputs: replica R, Merkle root rt of R, proof πSEAL 证明存储 Prove 算法生成副本的存储证明。 证明人收到来自验证者的随机挑战， 要求在树根为 rt 的 Merkle 树 R 中确认特定的叶子节 点 Rc。证明人生成关于从树根 rt 到叶子 Rc 的路径的知识证明。

Prove inputs:

8.在 ZHSH 的应用

ZHSH 协议采用”时空证明“来审核矿工提供的存储。为了在 ZHSH 中使用 PoSt，因为没 有指定的验证者，并且我们想要任何网络成员都能够验证，所以我们把方案改成了非交互式。 因为我们的验证者是在 public-coin 模型中运行，所以我们可以从区块链中提取随机性来发出 挑战。

9. ZHSH:DSN 构 建

ZHSH DSN 是可升级，可公开验证和激励式设计的去中心化的存储网络。客户为了存储数据和检索数据向矿工网络付费。矿工提供磁盘空间和带宽来赚取费用。矿工只有在网络可以审计他们的服务是否正确提供的时候才会收到付款。

3.2.2 环境

1.参与者

任何用户都可以作为客户端、存储矿工和/或检索矿工来参与 ZHSH 网络。客户在 DSN 中 通过 Put 和 Get 请求存储数据或者检索数据，并为此付费。

存储矿工为网络提供数据存储。存储矿工通过提供他们的磁盘空间和响应 Pug 请求来参与 ZHSH。要想成为存储矿工，用户必须用与存储空间成比例的抵押品来抵押。存储矿工通 过在特定时间存储数据来响应用户的 Put 请求。存储矿工生成"时空证明”，并提交到区块链网络来证明他们在特定时间内存储了数据。 假如证明无效或丢失，那存储矿工将被罚没他们的 部分抵押品。存储矿工也有资格挖取新区块，如果挖到了新块，矿工就能得到挖取新块的奖励 和包含在块中的交易费。检索矿工为网络提供数据检索服务。检索矿工通过提供用户 Get 请求所需要的数据来参与 ZHSH。和存储矿工不同，他们不需要抵押，不需要提交存储数据，不需要提供存储证明。 存储矿工可以同时也作为检索矿工参与网络。检索矿工可以直接从客户或者从检索市场赚取收益。

2 .网络

我们将运行所有运行 ZHSH C 全节点的所有用户细化为一个抽象实体:网络。该网络作为 运行管理协议的中介。简单的说，ZHSH 区块链的每个新块,全节点管理可用的存储，验证抵 押品，审核存储证明已经修复可能的故障。

3.账本

我们的协议适用于基于账本的货币。为了通用，我们称之为“账本” L。在任何给定的时 间 t(称为时期)，所有的用户都能访问 Lt。当处于时期 t 的时候，账本是追加式的，它由顺 序的一系列交易组成。ZHSH DSN 协议可以在运行验证 ZHSH 的证明的任意账本上实现。在 第六节中我们展示了我们如何基于有用的工作构建一个账本。

4.数据结构

碎片是客户在 DSN 所存储数据的一部分。例如，数据是可以任意划分为许多片，并且每片都可以有不同集合的存储矿工来存储。

扇区是存款矿工向网络提供的一些磁盘空间。矿工将客户数据的碎片存储到扇区，并通过他们的服务来赚取令牌。为了存储碎片，矿工们必须向网络抵押他们的扇区。

分配表式衣柜数据结构，可以跟踪碎片和其分配的扇区。分配表在长辈的每个区 块都会更新，Merkle 根存储在最新的区块中。在实践中，该表用来保持 DSN 的状态， 它使得在证明验证的过程中可以快速查找。

订单式请求或提供服务的意向声明。客户向市场提交投标订单来请求服务(存储数据的存储市场和检索数据的检索市场)，矿工们提交报价订单来提供服务。订单数据结构如图 10 所示。市场协议将在第 5 节详细介绍。

订单簿是订单的集合。请查看第 5.2.2 节的存储市场订单簿和第 5.3.3 节的检索市场订单簿。

抵押是像网络提供存储(特别是扇区)的承诺。存储矿工必须将抵押提交给账本，以便能在存储市场接受订单。抵押包括了抵押扇区的大小和存储矿工的存放的抵押品。

3.3 ZHSH 区块链的架构层

先前我们提到，区块链技术更象是一个采用了不同的技术综合而成的技术架构。在广义的区块链技术架构中，可以粗分为三个层次:

协议层:在这一个层次当中，代表着区块链核心的内容。也就是目前市场上 所泛称的底层技术。里面包含了数据存储的结构、共识算法、加密机制、网络通讯协议等等。这一切的内容都被包覆到这层当作进行运作，并且以 API 或者服务的形式提供上层调用。

扩展层：扩展层比较象是传统 MVC 架构中的 V 层，处理部分业务逻辑。智能合约就是建构在这个层上的。因此在这个层，我们可以通过智能合约将区块链技术延伸到各种不同的场景中，例如 AI 人工智能、VR/AR、 物联网<IOT>、ERP/MES、大数据<Bigdata>、云平台<Cloud>， 都可以在这里进行实现。

应用层：应用层面向最终用户，对于有接触过虚拟货币的人来说，各种不同的“电子钱包” 就属于这个层。不过在实际应用中，由于区块链技术本身的限制。应用层的开发除了要面对使用者的需求之外，同时也要兼顾扩展层与协议层的逻辑与技术要求。这导致一个区块链开发项 目，将会需要更为复杂的团

从以上的架构可以发现，区块链技术在每一个架构层当中都可能是不同的编程语言与各自独立的运算逻辑。同时要配合业务自身的加密算法要求等等，这会 形成一个复杂的协作过程。 在其背后更是需要完整的业务逻辑，才能迎合市场的真实需求。

3.4 技术特点

ZHSH 技术总体特征是公开、透明、可验证，或者至少在一定范围的具有这些特征。而从 效果上看，则是不可篡改与可追溯。项目应该会选择开放程度较高的类似于公有链的架构，因 为项目对各方隐私的要求高，反而对于流程透明性有极强的需求。

当然，项目以太坊 2.0 区块链技术，但从目前技术能力和跨国支付的需求上来看，不排除 项目中会搭建新的链和共识机制，就好如 ZHSH 的共识机制。

这样做的优势在于既不会像当前比特币区块链那样依赖大量算力消耗能源的工作量证明， 又能将数据公开程度及影响面设定在可控范围内。通过大数据能够对支付用户节点的行为作为 有效判断的依据，而不至于像 The DAO 那样出错之后，却由于节点行为不可控而造成的解决 方案难以统一的问题。当然，自有区块链在相关延展性也更适合项目根据自身发展需要量体裁衣。

PART 04 虚拟货币发行规则介绍

Introduction of virtual currency issuance rules

四、虚拟货币发行规则介绍

Introduction of virtual currency issuance rules

4.1 虚拟货币说明

ZHSH 是一种基于以太坊实现的结算虚拟货币，用于在 ZHSH 系统平台上兑换、结算其他 货币。ZHSH 在 ZHSH 系统平台为用户交易提供的交易媒介。

ZHSH 是整个生态系统的母链唯一虚拟货币，任何跨子链的数据交互及资产交换都需要消 耗母链虚拟货币，当生态系统形成后，跨链数据交互变成高频事件，此时各方面对 Token 的需 求量不断提升。虚拟货币持有者拥有母链发展方向的原始分配权。

和以太坊一样，ZHSH 上线之后，除了不断加强技术领先性以外，也会不断在链上发布 新的技术和应用，全面拓展生态结构和丰富生命力，实现私链到平台再到公链的属性切换。

ZHSH 的出现将重新定义跨境金融支付业务的全新行业标准:打造成金融支付合约区块 链的标准，成为未来新技术发展和新应用发布的基础。

在 ZHSH 保持技术领先性的情况下，开源代码将会成为很多未来项目的底层技术，包括 各国实际应用场景下的政府、企业、个人项目。

4.2 运行规划

阶段	说明
第一阶段	打通全过个地区的第三方保险公司的战略合作
第二阶段	实现通过保障计划，进行保底，购买保险的方式来进行商业的流通
第三阶段	对接商业应用、和商城、实体产业的商品以物置物
第四阶段	实现面对面的支付流通体系，面对面的收款，OTC 的方式
第五阶段	路线开发基于 token 生态的直营项目/50 个联营项目
第六阶段	研发硬件钱包，让 token 的应用在生活各个方面都具备快速的接入

PART 05 ZHSH 远景规划

ZHSH vision

五、ZHSH 远景规划 *ZHSH vision*

5.1 ZHSH 的商业模式规划

区块链技术之所以那么火热，是因为它能解决人们在互联网世界里微弱的隐私权，又能帮助企业解决众多难治的痛点。把它放在金融领域，能解决交易的安全问题；放在文化领域，能解决侵权问题；放在制造业，能降低运营成本；放在供应链上，能根除产品在流转过程中出现的成本流通、商品运输等现象。

5.1.1 ZHSH 的应用性

1 第三方管理模式:

（1.1）以太坊技术层次管理;透明供应链平台、解决运营方、消费方、信用征信、 自由交易。

（2.2）合作品牌管理；合作方通过平台区块链注册，可以通过区块链，面向全球 发布自己的产品

信息，可以进行管理，交易由平台流通，做到公正，公平。

2 分布式共享数据库:

区块链具备对点价值转移、去中心化特性、所有信息公开记录在公共账本。区块链，商家信息、客户信息、商品信息、数据透明、不能篡改、每个人都可以随时查看。

5.1.2 ZHSH 的核心竞争力

区块链智能合约；平台信息流通、信用透明、第三方平台系统管理、交易或者物 流、成本核算、都有智能合约保证。

效应智能物流；ZHSH 区块链智能、产品信息、物流动向、消费者能通过平台查询、解决 商品送达，买家与物流时间逆差。

5.1.3 ZHSH 的关键应用

ZHSH 区块链；引入 RFID 和 FWC 电子标签技术。以 RFID 技术植入商品 ID 身份。客户可 以通过手机平台扫描，得知商品一切资讯。

唯一 ID 身份；通过产品生产，标签管理、每一件商品都是独一无二、不可篡改、不可造假、商品所有信息都可通过手机平台查询。

5.2 ZHSH 商业模式落地实施

基于区块链技术，ZHSH 能够做到全球产业数据化，其中产业包括(互联网娱乐行业、时 尚奢侈品行业、金融行业、广告行业、实体行业)有如搭积木的应用模式，采取全球商业数 据，一步步数字化到区块链，如此形成一个商业资产王国。比如;生产方在 ZHSH 上传数据营 销，消费者在于 ZHSH 数字钱包购买消费，就是基于区块链基础的技术上，做到第三方管理(第三方也就是区块链系统)，通过系统应用运作，做到各自信用，自由交易，资产信任等。

5.2 .1“区块链+ZHSH 支点塑造商业链”

ZHSH 的供应链，在商业行业能够解决价格乱象、做到信息流通，公正，真假难辨的根本问题。在商业市场，消费者可以通过 ZHSH 来辨别 ZHSH 商业资源的生态、来源，以及信息不透 明导致市场的乱价现象损害消费者的利益。

5.2.2 公开透明，数据可溯源

ZHSH 底层基于 RFID 底层链技术，它能追踪辨别商品的生产地点、生产时间、运输直到销 售终端的整个过程，消费者能在手机上查看每一笔消费信息。

5.2.3 ZHSH 社交生态系统

ZHSH 将在全球以每个地区自主成立社区，共同打造商业数字资产技术应用和商业支付应 用社交共赢生态圈。在此过程中，每个成员都有机会通过 ZHSH 机制获得奖励，这种模式能最 大程度地发挥全体社区成员的积极性、创造性，从而提升 ZHSH 社区影响力。

5.2.4 大数据的溯源平台建设

ZHSH 将与全球商业资产产业生态以及商业营销商合作，发起成立 ZHSH 商业 RFID 溯源技 术研究中心，通过对全球商业资产产业链数据各个环节跟踪采集，创建 ZHSH 大数据平台。

5.2.5 QSC 的信用体系建设

通过区块链的去中心化特质，节点之间通过数字签名技术进行数据交换，无需互相信任， 而且在智能合约的前提下，合约双方无法进行欺骗，只有当合约条件满足时，程式就会释放或 转移资金。在这样的体系下，买到全球商业资产资源的成本将大幅度降低。

5.2.6 推动秸秆级别标准化体系建设

利用区块链技术产生信息流、资金流、大数据链等，先建立 ZHSH 社区内部自己独有的商 业资产级别标准化体系，最终借助 ZHSH 市场化运作手段促进和帮助政府建立全球商业资产级 别标准化体系。

5.3 ZHSH 最终生态系统建立

ZHSH 和以太坊以及其他区块链数字资产都是基于去中心化、P2P 网络技术、分布式记账、 共识机制技术、不可篡改的智能合约的区块链区底层技术。

ZHSH 是由自己的区块链技术开发团队独立原创开发的源代码结构，是完全适合“全球资产商业产业区块链技术白皮书”的要求而量身打造的大数据系统，是首家直接应用于商业资产产业资源支付、消费利用“全球性商业生态资产产业”为架构方向的区块链应用模式，该模式涉及拥有了全面融合及商业资产产业综合商业资源流通特性所具有的前端供应链、中期消费、 支付链、后期消费、支付、金融综合利用链、全程交易环节到最终销售环节(线上线下)的数 据采集、区块标识、合约由分散到统一，又从统一到分装、有效期管理、溯源、分单以及所涉 及的上中下游企业的同步管理、结算、统计等的全部功能，是全国甚或全球唯一可以依托全球行业产业基础、数据基础、管理基础、集中程度而具备可行性落地条件的数字资产，同时，ZHSH 还兼具了主流数字资产所共有的“智慧钱包、智能合约” 系统，将会为打造合伙人财富 体系、数字资产反哺资源商业资产，改善综合商业资产利用基层工作者收益、提升商业资产产业综合利用的资产再生、打造商业资源全球综合商 业利用的架构体系而做出卓越的贡献。

在应用层面 ZHSH 以实体为依托、以行业权威优势为基础、以三大战略、九大布局为支撑、 用场景为基点，横向开拓区域，纵向打通商业资产资源产业链条，在网络与现实的深度融合、 精准对接中实现流通，实现“ZHSH”稳定的价值增长。

5.3.1 ZHSH 应用落地

ZHSH 是商业产业链产售供应全程、综合利用商业资产资源综合利用、以制作商品销售的 全程以区块链去中心化特性、基于商业应用技术制作、流通、运输至全球销售、消费交易、支 付、结算全场景应用。 (1)以去中心化特性，基于商业资产采集、存储加工、运输、流通全球应用、做到资产流通 全球综合利用;

(2)ZHSH 及商业产业资源利用、资源再生利用、基于去中心化应用全球性应用资源链; (3)资源交易、储存、资源利用、输运、销售等五项应用场景; (4)合伙人之间、合伙人对企业、企业对企业数字资产交易等三项场景;

(5)ZHSH 数字资产国际大盘交易、应用、结算等三项应用场景; (6)合伙人数字钱包与主要国际货币结算、兑付应用场景一项。

PART 06 主建团队

The main team building

六、主建团队 *The main team building*

Hendricks Founder

创始人兼CEO

国籍：美国 U.S.A

介绍：*Hendricks is the Founder of Pied Piper, and after a brief hiatus, is once again CEO.*

While Richard has worn a few different hats at Pied Piper, his compression algorithm — an algorithm some have called a game-changing technology worth seeing through to its greatest potential to impact the world — has always been his guiding light. He is now focusing on a new project. He still can't go into specifics at this time, but let's just say it's going to be pretty big, and not crazy.

Richard first moved to Silicon Valley to study computer science at Stanford. He left four credits shy of graduation to concentrate on his true passion: compressing data. He created Pied Piper to pursue that passion and bring his middle-out algorithm to all. He and his team launched the Pied Piper platform earlier this year, which didn't quite catch on with the public, but that was no reflection on the tech. The tech remains revolutionary.

Dinesh

高级程序员兼技术总监

国籍：印度 India

介绍：*Over his career as a programmer, Dinesh has brought his talents to many promising startups. He briefly served as CEO of Piper Chat, Pied Piper's video chat offshoot. Following Hooli's acquisition of Piper Chat, Dinesh gracefully parted ways with the company and thinks it's best not to talk about it too much anymore. Dinesh has also contributed to a pioneering image classification project at Periscope, scraping the internet of inappropriate content. He doesn't like to talk about that too much, either.*

Prior to working in Silicon Valley, Dinesh received degrees in information theory and computer science from Yale, Caltech, and Oxford, and published several books on advanced Java tools. (Signed copies available upon request.) When he's not coding or kicking it with his boys, Dinesh enjoys online solitaire and the occasional karaoke session.

Nelson "Big Head" Bighetti

首席运营官兼多数投资者

国籍：保加利亚Bulgaria

介绍：*Nelson was sort of one of the founders of Pied Piper, or was at least in the same house when it got founded. In the past, he rose from doing data entry at Hooli to being a SVP there, and eventually became Head Dreamer of HooliXYZ. He is currently a co-principal at Bachmanity Enterprises, which is now the principal owner of Pied Piper. Is that weird, using the word "principal" like that twice in the same sentence, but in kind of two different senses? It feels weird. Anyway, Big Head is just three credits shy of an undergraduate degree in computer science from the University of Oklahoma. He used to own a boat. He likes soda and cannons.*

Jared

首席财务官

国籍：美国U. S. A

介绍：*Ared's early life is best passed over, and parts of it he cannot legally discuss because of non-disclosure clauses in settlements. Yet he managed to rise above it thanks to a series of largely well-meaning foster parents and went on to receive a B.A. from Vassar College in Economics. During those happiest of years, he sang second alto with the Joyce Carol Notes A Capella Confrontation and was both coxswain for Women's Heavyweight Crew and co-founder of Take Back Take Back the Night. After college, he worked for Google, Congresswoman Nancy Pelosi, and Hooli, but now he is a Pied Piper man through and through.*

Monica Hall

基金会主席

国籍：美国 U.S.A

介绍：*Monica hails from Baltimore, Maryland and earned her A.B. in Economics from Princeton University. There she was President of the Tigerlilies a capella group and a member of the Ivy Club. She went on to receive her M.B.A. at the Stanford Graduate School of Business. Notably, she delivered the most efficient TALK in GSB history, narrating her life story in just under twelve minutes.*

After business school, Monica worked as a consultant at McKinsey & Company before getting recruited to the venture capital world. She served as associate partner at Raviga Capital, founded by the late Valley legend Peter Gregory. Later, she and colleague Laurie Bream exited Raviga to launch their own fund, Bream-Hall, where they championed investments in K-Hole Games, Everglade, and, of course, Pied Piper.

PART 07 法律事务与风险提示

Legal affairs and risk tips

七、法律事务与风险提示 *Legal affairs and risk tips*

7.1 法律事务

ZHSH 项目会成立一家设立在海外的 BVI ，即 ZHSH 基金会。该基金会将作为独立的法律 主体，全权负责组织团队来开发、推广和运营 ZHSH 项目，并承担所有相关责任。

ZHSH 基金会将严格按照 BVI 所在地法律法规，以恰当方式面向特定人群进行互换，并给 与数字货币 ZHSH。出于有法律限制的国家公民或群体限制，数字货币

ZHSH 将不在某些国家地 区进行公开众筹或公开募集等行为。 数字货币 ZHSH 作为一种具有实际用途的虚拟商品和使 用，不是证券，也不是投机性的投资工具。

ZHSH 基金会在数字货币 ZHSH 互换中所获的收入，将由 ZHSH 基金会主要将用于技术开发、 市场营销、社区建设、财务审计、商务合作等用途。

ZHSH 平台依然很有可能会在全世界不同国家受到主管机构的质询和监管。为了满足和遵守当地的法律法规 ZHSH 平台可能会在有些区域无法提供正常的服务。

7.2 风险提示

本项目在售卖之前和进行中，不会在任何媒体组织任何公开的宣传及广告推介活动，平台团队也没有组织任何 Facebook、SNS 群等社交媒体，邮件列表进行推介， 请大家参与前谨慎判别。

本文档只用于传达信息之用途，并不构成未来买卖原生数字资产的相关意见或投 资意见，也不是任何形式上的合约或者承诺。

本项目所涉及的原生数字资产是一个在平台上使用的加密数字编码，并不代表平台项目的股权、债权、收益权或控制权。

同时 ZHSH 基金会在此明确不予承认和拒绝承担下述责任:

(1) 任何人在互换数字货币 ZHSH 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求;

(2) 任何人在购买数字货币 ZHSH 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求， 以及由此导致的无法使用或无法提取数字货币 ZHSH;

(3) 由于任何原因，数字货币 ZHSH 的互换计划被放弃;

(4) ZHSH 的开发失败或被放弃，以及因此导致的无法交付或无法使用数字货币 ZHSH; (5) ZHSH 公有链开发的推迟或延期，以及因此导致的无法达成事先披露的日程;

(6) ZHSH 源代码的错误、瑕疵、缺陷或其他问题;

(7) ZHSH 的故障、崩溃、瘫痪、回滚或硬分叉;

(8) ZHSH 未能实现任何特定功能或不适合任何特定用途;

(9) 对数字货币 ZHSH 计划所募集的资金的使用;

(10) 未能及时且完整的披露关于 ZHSH 公有链开发的信息;

(11) 任何参与者泄露、丢失或损毁了数字货币 ZHSH 的钱包私钥;

(12) 第三方分销平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误 操作、 不当行为、失误、疏忽、破产、清算、解散或歇业;

(13) 任何人与第三方分销平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾;

(14) 任何人对数字货币 ZHSH 的交易或投机行为;

(15) 数字货币 ZHSH 在任何交易平台的上市、停牌或退市;

(16) 数字货币 ZHSH 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、 商业票据、流通票据、投资品或其他事物，以至于受到禁止、监管或法律限制;

(17) 本白皮书披露的任何风险因素，以及与该等风险因素有关、因此导致或伴随发生的损害、损失、 索赔、责任、惩罚、成本或其他负面影响。

华资基金集团

Company introduction

THANK YOU FOR WATCHING

基于第二代区块链技术商业应用生态模式

Based on the second generation block chain technology, a commercial application ecological mode.