



# ZITCOIN

# 项目白皮书



**重塑Layer 2标准 定义区块链新纪元**

**ZTC优化共识算法确保比特币网络高效稳定运行**



# 目录

<b>01/引言 .....</b>	<b>4</b>
<b>02/驱动背景 .....</b>	<b>6</b>
2.1 比特币网络的挑战 .....	6
2.2 Layer 2 解决方案的兴起 .....	6
2.3 ZTC 创新点 .....	6
<b>03/ZTC 使命 .....</b>	<b>8</b>
3.1 显著提升比特币网络性能 .....	8
3.2 去中心化安全性 .....	9
3.3 引入 Layer 2 技术创新应用 .....	10
<b>04/ZTC 技术解决方案 .....</b>	<b>11</b>
4.1 技术概述 .....	11
4.2 Layer 2 二层扩容 .....	12
4.3 并行处理与交易速度优化 .....	13
4.4 ZTC 聚焦状态通道侧链 .....	14
4.5 高性能共识算法 .....	14
4.6 数据隐私保护 .....	17
4.7 智能合约支持 .....	19
<b>05/技术架构与实施 .....</b>	<b>22</b>
5.1 ZTC 系统架构详解 .....	22
5.2 共识算法 .....	25



5.3 数据隐私与安全 .....	27
5.4 智能合约平台 .....	32
<b>06/应用生态 .....</b>	<b>34</b>
6.1 应用场景分析 .....	34
6.2 商业应用实例 .....	35
6.3 生态系统建设 .....	36
<b>07/经济生态 .....</b>	<b>36</b>
7.1 发行方案 .....	36
7.2 ZTC 价值 .....	37
7.3 ZTC 激励 .....	38
7.4 ZTC 完全去中心化公平发射台 .....	38
<b>08/发展路线图 .....</b>	<b>38</b>
<b>09/项目团队 .....</b>	<b>41</b>
9.1 基金会 .....	41
9.2 团队成员 .....	41
<b>10/免责声明 .....</b>	<b>44</b>



# 01/引言

在数字化浪潮的席卷下，区块链技术凭借其去中心化、透明、不可篡改的特性，已然成为推动全球技术革新的重要引擎。随着比特币等主流加密货币的普及和应用场景的不断拓展，区块链网络面临的性能瓶颈问题愈发凸显，成为制约其进一步发展的关键因素。为解决这些挑战，ZTC 项目应运而生，立志通过前沿的 Layer 2 解决方案，为比特币及其他区块链网络注入新的活力，引领区块链技术的革新与发展。

## ZTC 概述

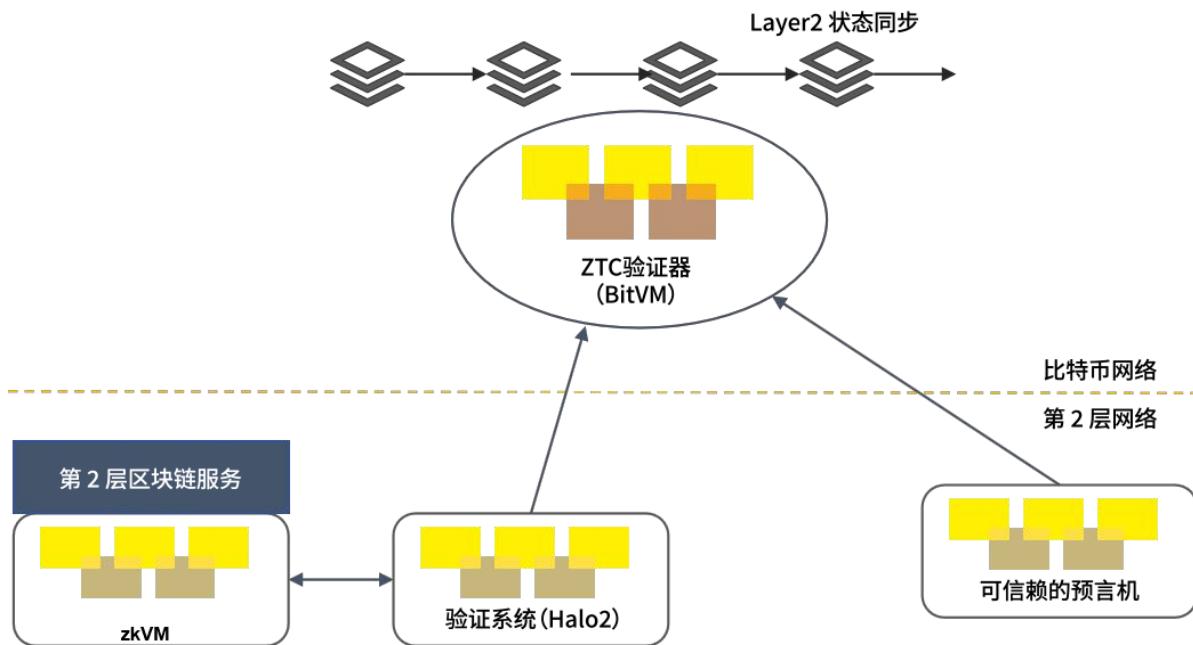
ZTC (Zitcoin) 是一个基于 Layer 2 架构的区块链创新项目，旨在通过技术创新优化和扩展现有区块链网络，为比特币等主流区块链提供高性能、低成本的 Layer 2 扩展解决方案。ZTC 通过集成零知识证明 (ZKPs) 和量子密码学等前沿技术，在不牺牲系统安全性和去中心化特性的前提下，显著提升区块链的交易速度和吞吐量。

在 ZTC 的 Layer 2 架构中，采用了账户模型来管理区块链的状态。为验证整个区块链的状态，ZTC 运用基于 Halo2 证明系统的 zkVM (零知识虚拟机)。这种验证方式确保了 Layer 2 状态与比特币主网络之间的同步，并且所有的 Layer 2 状态更新都通过由 BitVM 实现的零知识证明 (ZKP) 验证器进行验证。

在追踪和管理所有的 Layer 2 状态中，ZTC 使用了一个统一的 UTXO (未花费交易输出) 模型。此外，ZTC 还引入了一个可信的预言机机制，确保只有符合 Layer 2 协议规范的锁定/解锁脚本的输入/输出被允许，从而维护了系统的安全性和稳



定性。



### ZTC 公链计划:

- **ZTC V1 (侧链版本)** : 在 V1 版本上线的过程中, ZTC 公链将重点关注侧链的性能、安全性和易用性。通过不断的测试和优化, 确保侧链能够满足用户的需求, 并为开发者提供丰富的开发工具和 API 支持。
- **ZTC V2 (UTXO 客户端验证版本)** : V2 版本的上线将进一步提升 ZTC 公链的性能和用户体验。通过 UTXO 客户端验证, 用户可以更加快速、安全地进行交易, 享受更加流畅的区块链体验。同时, ZTC 将继续优化和完善 UTXO 客户端验证机制, 确保其在各种场景下的稳定性和可靠性。

ZTC 公链分阶段上线计划旨在逐步验证和完善其区块链技术, 为用户和开发者提供更加成熟、稳定的区块链平台。通过 V1 和 V2 两个版本的迭代和优化, ZTC 将不断推动区块链技术的发展和应用, 为整个区块链生态的繁荣做出贡献。



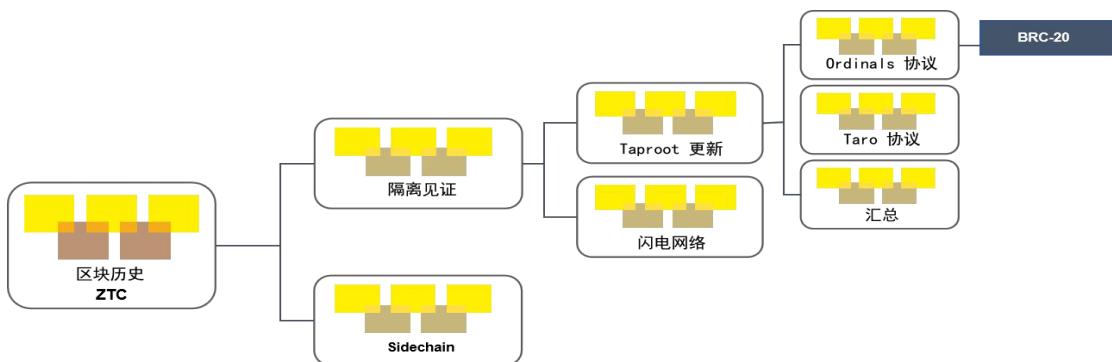
## 02/驱动背景

### 2.1 比特币网络的挑战

随着比特币网络的发展，其面临的性能问题愈发严重。交易速度缓慢、吞吐量受限、区块确认时间过长以及网络拥堵等问题，不仅影响了用户体验，也限制了比特币在更广泛领域的应用。这些问题迫切需要得到解决，以推动比特币及整个区块链行业的持续发展。

### 2.2 Layer 2 解决方案的兴起

Layer 2 作为区块链技术的重要创新，通过在主链（Layer 1）之上构建扩展层，实现交易速度和吞吐量的提升，同时保持主链的安全性和去中心化特性。这种方案无需对主链进行大规模修改，即可有效解决比特币面临的性能问题。Layer 2 解决方案的兴起，为区块链行业带来了新的发展机遇和可能。



### 2.3 ZTC 创新点

ZTC 在 Layer 2 解决方案的基础上，引入创新技术，以实现更高的性能和更好的



用户体验：

- ✓ **高性能共识算法**: ZTC 引入了并优化了最新的共识算法，如 StarkNet 的 STARKs 等，以确保交易的高速处理和低延迟。这些算法能够大幅度提升交易的确认速度，为用户提供更加流畅的区块链体验。
- ✓ **隐私保护技术**: ZTC 充分利用零知识证明 (ZKPs) 等先进的隐私保护技术，保护用户的交易隐私和匿名性。这些技术能够确保用户的交易信息不被泄露给第三方，满足用户对隐私保护的高要求。
- ✓ **去中心化预言机 (Decentralized Oracle)**: ZTC 的去中心化预言机系统确保了链上数据与链下实时信息的无缝对接。通过多个独立的预言机节点提供的实时数据，ZTC 提高了智能合约的可靠性和灵活性，为开发者提供了更丰富的应用场景。
- ✓ **SWAP (Swap Protocol)**: ZTC 支持 SWAP 协议，该协议允许用户在链上进行资产的无缝交换，无需第三方中介的参与。这不仅提高了资产流通的效率和安全性，还为用户提供了更加便捷的交易方式。
- ✓ **UTXO 客户端验证 (UTXO Client-Side Validation)**: 在 ZTC 的后续版本中，将引入 UTXO 客户端验证机制。这种机制允许用户在本地验证交易的有效性，降低了对中心化验证服务的依赖，进一步提高了系统的安全性和隐私性。
- ✓ **POS+POW 共识节点 (Proof of Stake + Proof of Work Consensus Nodes)**: ZTC 采用了 POS 和 POW 混合的共识机制。POW 确保了网络的安全性和去中心化特性，而 POS 则提高了交易速度和能源效率。这种混合机制使得 ZTC 在性能和安全性之间达到了良好的平衡。ZTC公链采用双GAS模型，V2版采取BTC和ZTC双GAS消耗模型，用户可自主选择，很好的帮助BTC生态和ZTC完成通缩模型。



✓ **双GAS模型**：ZTC公链采用双GAS模型，V2版采取BTC和ZTC双GAS消耗模型，用户可自主选择，很好的帮助BTC生态和ZTC完成通缩。

**ZTC 项目成功实施，将为比特币及其他区块链网络带来革命性的变革，推动整个区块链行业的持续发展。ZTC 期待与各方携手合作，共同开创区块链技术的新篇章。**

## 03/ZTC 使命

### 3.1 显著提升比特币网络性能

在数字货币和区块链领域，性能一直是衡量一个网络成功与否的关键因素。ZTC 的首要使命便是显著提升比特币网络的性能，以满足日益增长的用户需求和应用场景。

#### 3.1.1 提升交易速度吞吐量

当前，比特币网络面临着交易速度和吞吐量上的限制，导致用户在高峰时段需要支付高额的交易费用并等待长时间的交易确认。ZTC 通过引入先进的 Layer 2 技术，如状态通道（State Channels）和侧链（Sidechains），将大部分交易转移至链下处理。这种方式可以极大地减轻主链的负担，从而显著提升交易速度和降低交易成本。ZTC 将不断优化共识算法，确保网络即使在交易量激增的情况下也能保持高效稳定的运行。

#### 3.1.2 链下处理扩展性

ZTC 通过链下处理，将复杂的交易逻辑和数据处理移至链外进行，从而提高交易速度，降低网络拥堵的风险。链下处理还为开发者提供了更大的灵活性和创新空



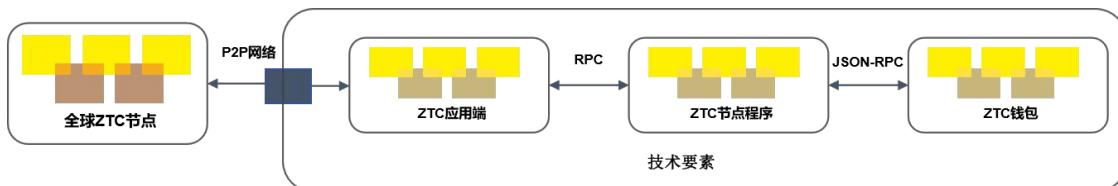
间，使得更多复杂的应用场景得以实现。ZTC 还将积极探索其他扩展性解决方案，如分片（Sharding）等，以进一步提升网络的性能。

## 3.2 去中心化安全性

在区块链技术中，去中心化和安全性是两个至关重要的原则。ZTC 在设计和实施过程中，将始终遵循这两个原则，确保网络的稳定运行和用户的资产安全。

### 3.2.1 去中心化原则

去中心化是区块链技术的核心优势之一，比特币网络能够持续发展的基础。在设计和实施过程中，ZTC 始终遵循去中心化的原则，确保网络的稳定运行不依赖于任何中心化的机构或个体。通过采用分布式账本和共识算法等技术手段，ZTC 确保网络的去中心化特性，防止单点故障和权力集中等问题。



### 3.2.2 安全性保障

在安全性方面，ZTC 采用最新的密码学技术和安全机制来保障交易的安全性和数据的完整性。通过引入先进的加密算法、数字签名技术和隐私保护技术等手段，确保用户的交易信息不被泄露给第三方，并防止任何形式的攻击和篡改。ZTC 建立严格的安全审计和漏洞奖励机制，鼓励用户和安全专家积极参与网络的安全维护和改进工作。



### 3.3 引入 Layer 2 技术创新应用

ZTC 积极探索引入 Layer 2 技术的创新应用，以丰富比特币网络生态和为用户提供更多的价值和便利。

#### 3.3.1 跨链交易与互操作性

通过 Layer 2 技术，ZTC 实现不同区块链网络之间的跨链交易和互操作性。打破区块链之间的壁垒，促进不同网络之间的资源共享和合作，为用户提供更加灵活和便捷的跨链服务。例如，用户可以在不同的区块链网络之间无缝转移资产、进行交易和访问智能合约等。

#### 3.3.2 去中心化金融（DeFi）

DeFi 作为区块链领域的一个重要分支，正在逐渐改变金融行业的格局。ZTC 积极引入 Layer 2 技术来推动 DeFi 的发展和创新。通过构建去中心化的借贷、交易、保险和资产管理等平台，为用户提供更加安全、透明和高效的金融服务体验。同时，与 DeFi 领域的优秀项目合作，共同推动整个生态的繁荣和发展。

#### 3.3.3 资产代币化

资产代币化是区块链技术的另一个重要应用方向，可以将各种实体资产转化为可交易的数字资产。ZTC 探索资产代币化的应用场景和解决方案，为用户提供更加便捷和高效的资产管理和交易方式。降低资产代币化的成本和门槛，吸引更多的用户和机构参与其中。与相关行业合作，共同推动资产代币化的规范化和标准化发展。



# 04/ZTC 技术解决方案

## 4.1 技术概述

### 4.1.1 Layer 2 可信预言机

ZTC 的 Layer 2 架构依赖于一个由被选中的用户组成的节点，负责监督整个网络的运行状况。在协议遇到问题时，有权介入并暂停协议，以保护所有用户的资产。此外，引入可信预言机来验证输入/输出 UTXO 和脚本的正确性，确保 Layer 2 交易的有效性。

### 4.1.2 第一层到第二层交互

在 ZTC 中，通过创建一个单一的 Taproot 地址来代表 Layer 2 协议。当 UTXO 被转移到这个 Taproot 地址时，实际上是完成了从比特币主网到 Layer 2 的“充值”过程。只有协议、可信预言机或委员会账户拥有对存入 UTXO 的“转移”权限。可信预言机确保所有权转移交易中的 UTXO 脚本准确无误。

### 4.1.3、同步到比特币主网区块

Layer 2 网络的状态更新将以区块的形式同步到比特币主网。每个区块包含交易记录、新账户状态、新 UTXO、比特币网络区块信息以及零知识证明（ZKP），用于验证状态转换的正确性。这些状态更新被记录在 UTXO 交易历史中，确保 Layer 2 的透明性和可追溯性。

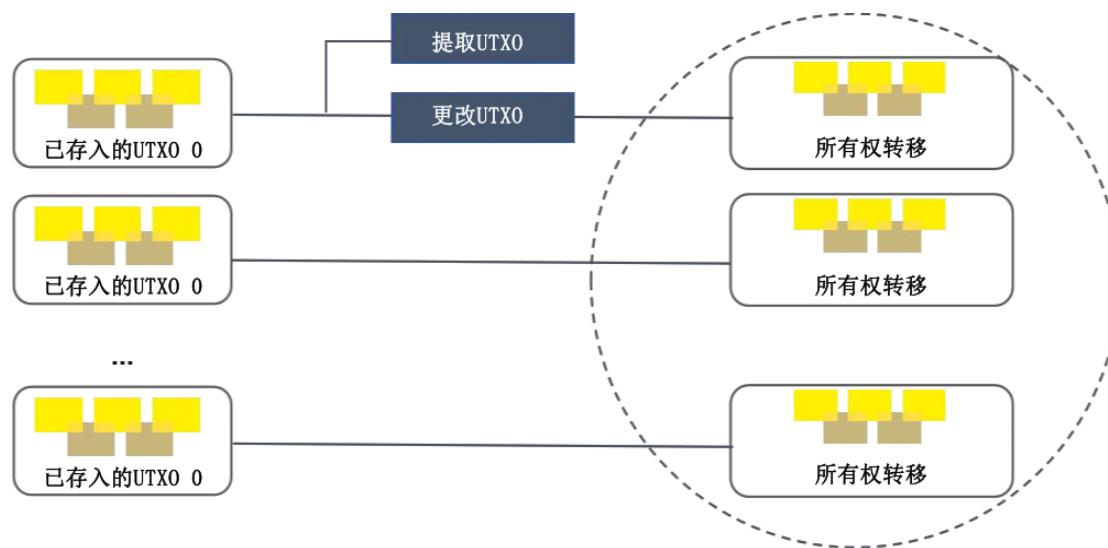
ZKP 被用于验证 Layer 2 的正确性，包括交易签名验证、账户状态正确性、充值交易处理以及 UTXO 分配的准确性。为确保区块信息的准确性，ZTC 采用挑战



和响应方案，并结合 ZKP 电路和 BitVM 进行验证。每个 Layer 2 区块都有唯一的二进制电路承诺，由可信预言机检查公共输入的正确性。

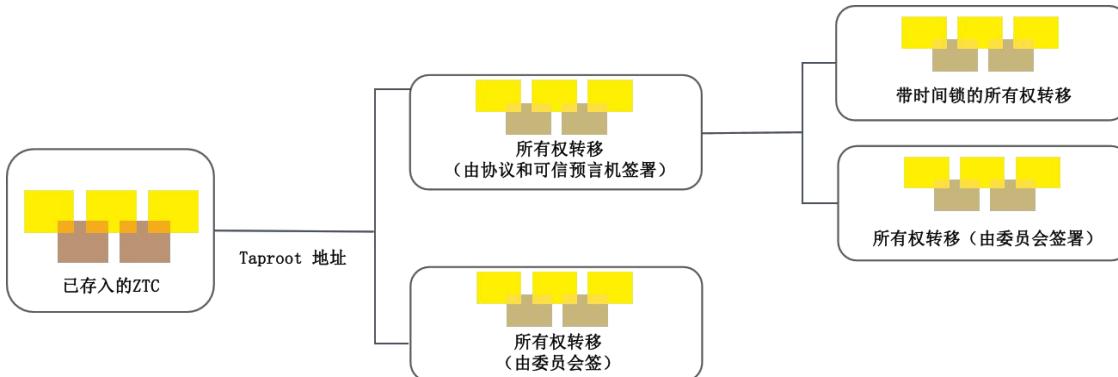
#### 4.1.4 退出机制

资产可以从 Layer 2 转移到比特币主网，主要通过两种方式实现：提现 (withdrawal) 和强制提现 (force-withdrawal)。提现交易由 Layer 2 触发，使用 ZKP 电路进行验证，确保资金的安全转移。而强制提现交易则由比特币网络发起，并在下一个区块状态更新中反映。



## 4.2 Layer 2 二层扩容

Layer 2 技术，亦被业界广泛认知为二层扩容技术，其核心理念在于对现有的区块链主链（Layer 1）进行性能增强。通过构建在链下的附加层，Layer 2 技术能够在确保主链安全性和去中心化特性的前提下，显著提升区块链网络的交易速度和吞吐量，有效降低交易费用。



## 原理探究：

Layer 2 技术通过将大量交易在链下进行处理，将交易结果或状态更新提交至主链进行验证和确认。这种方式有效避免了主链因处理大量交易而产生的拥堵和延迟，从而实现了交易速度的大幅提升。同时，由于链下处理的交易数据并未直接写入主链，因此也显著降低了交易费用。

## 前沿优势：

- 可扩展性：** Layer 2 技术通过链下处理大量交易，有效扩展区块链网络的能力，使其能够支持更多的应用场景和用户需求。
- 去中心化与安全性的保障：** Layer 2 技术在提升性能的同时，并不牺牲主链的去中心化和安全性。所有链下处理的交易结果或状态更新仍需通过主链的验证和确认，确保了整个系统的安全性和可信度。
- 交易速度的优化：** 通过链下并行处理交易，Layer 2 技术显著提高了交易速度，降低了交易延迟，为用户提供了更好的使用体验。

## 4.3 并行处理与交易速度优化

ZTC 充分利用 Layer 2 技术处理能力，实现交易并行化执行。构建多个链下通道



和侧链，将交易处理分散到这些通道或侧链中进行。通过并行处理，ZTC 能够同时处理更多的交易，从而显著提升交易速度和吞吐量。交易排序和批量处理机制。对交易进行优先级排序和批量处理，ZTC 能够进一步优化交易速度，降低交易延迟。确保了高优先级的交易能够得到及时处理，提高了整个系统的处理效率。

## 4.4 ZTC 聚焦状态通道侧链

经过深入研究和评估，ZTC 重点关注状态通道（State Channels）和侧链（Sidechains）这两种成熟且广泛应用的 Layer 2 技术。

对于状态通道（State Channels），ZTC 优化其关闭机制。传统状态通道在关闭时需要提交大量数据到主链进行验证和确认，这可能导致较高的关闭成本和较长的关闭时间。为了解决这个问题，ZTC 引入先进的压缩技术和验证机制，降低关闭成本并提高用户体验。

对于侧链（Sidechains），ZTC 探索新的构建方式。传统侧链通常与主链存在较弱的耦合关系，这可能导致跨链交易安全性和稳定性问题。为了解决这个问题，ZTC 研究更加紧密的跨链协议和机制，确保侧链的稳定性和安全性。探索跨链资产的互操作性，为用户提供更加灵活和便捷的跨链服务。

## 4.5 高性能共识算法

### 4.2.1 STARKs 技术应用

ZTC 采用 STARKs (Scalable Transparent ARgument of Knowledge) 技术作为 Layer 2 解决方案的核心技术。STARKs 允许在不透露具体输入或计算过程的情况下，验证比特币及其他区块链网络上交易的正确性，从而为 ZTC 网络提供



了高效的验证机制。

### 原理简述：

在 ZTC 项目中，利用 STARKs 技术将交易移至链下执行，并通过数学证明的方式验证交易的有效性。交易的执行结果或状态更新被编码为一个数学证明，这个证明可以被任何拥有适当验证密钥的节点验证。由于 STARKs 的透明性和可验证性，以及高效的验证速度，ZTC 项目能够支持大规模的交易处理和验证。

### 特性分析：

- **高效性：** ZTC 项目通过 STARKs 技术，实现了链下交易的快速验证，大大减少了主链上的计算负担和交易延迟。
- **隐私保护：** 利用零知识证明技术，ZTC 项目能够在验证交易的同时保护用户的隐私和数据安全。
- **可扩展性：** 由于 STARKs 的架构优势，ZTC 项目具有强大的扩展能力，能够支持不断增长的交易需求。

#### 4.2.2 算法优化

为了进一步提高 ZTC 项目的性能和稳定性，将对 STARKs 技术进行以下优化和改进：

- **并行化处理：** 通过优化算法架构，实现交易的并行化处理，提高交易验证的效率和速度。
- **验证效率提升：** 引入先进的验证技术和算法，降低验证过程的复杂度和计算量，进一步提高验证效率。
- **安全性增强：** 密切关注最新的安全漏洞和攻击手段，及时采取相应的安全措



施和防护措施，确保 ZTC 项目的安全性。

### 4.2.3 性能与安全性分析

#### 性能分析：

- **交易验证速度：** 通过模拟不同规模和复杂度的交易场景，测量 ZTC 项目中验证单个交易所需的平均时间。
- **吞吐量：** 测试 ZTC 项目能够处理的交易数量，以评估系统的扩展能力。
- **延迟：** 测量从交易发起到被验证并确认在区块链上的时间间隔，以评估 ZTC 项目的延迟性能。
- **系统资源消耗：** 监控 ZTC 项目在运行时对计算资源、存储资源和网络带宽的消耗情况。

#### 安全性分析：

- **STARKs 技术安全性：** 评估 STARKs 技术在 ZTC 项目中的应用是否存在已知的安全漏洞或攻击手段。
- **隐私保护：** 分析 ZTC 项目在验证交易过程中是否能够有效保护用户的隐私和数据安全。
- **抗攻击能力：** 模拟各种可能的攻击场景，以测试 ZTC 项目的抗攻击能力。

代码审计和漏洞扫描：委托专业的安全团队对 ZTC 项目的代码进行审计和漏洞扫描，确保其安全性和稳定性。



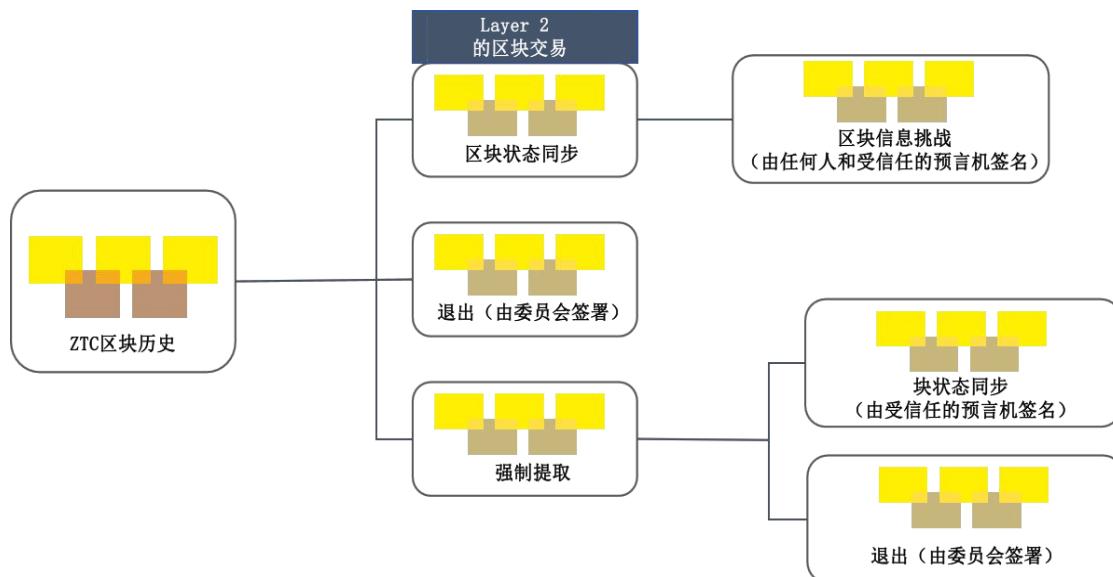
## 4.6 数据隐私保护

### 4.3.1、隐私保护技术深度集成

在 ZTC 的构建中，数据隐私与保护被视为至关重要的核心要素。深入研究集成多种前沿的隐私保护技术，以构建一个安全、可靠的区块链网络。

#### 1. 零知识证明 (ZKPs) 技术

ZKPs 是 ZTC 实现隐私保护的核心技术之一。通过 ZKPs，将交易信息转化为数学证明问题，而无需公开交易的具体内容。采用 STARK (Scalable Transparent ARguments of Knowledge) 作为零知识证明的实现方式，具有高效性，能够在保证验证过程透明度的同时，实现交易的隐私保护。



#### 2. 同态加密 (Homomorphic Encryption)

同态加密技术允许在加密数据上进行计算，而无需解密数据本身。在 ZTC 中，利用同态加密技术对用户的交易数据进行加密处理，确保在交易过程中数据的隐



私性和安全性。同态加密还提供了在加密数据上进行验证和计算的能力，进一步增强了 ZTC 的隐私保护能力。

### 3. 安全多方计算 (MPC)

安全多方计算技术允许多个参与方在不泄露各自秘密输入的情况下，共同计算一个函数。在 ZTC 中，利用 MPC 技术来实现节点间的协同验证和计算。通过 MPC 技术，可以确保在多个节点之间安全地共享和验证交易信息，同时保护用户的隐私和数据安全。

#### 4.3.2、ZKPs 在隐私保护中应用

ZTC 应用 ZKPs 技术来保障交易的隐私性，基于 ZKPs 的隐私保护交易协议，该协议将交易信息转化为数学证明问题，通过 ZKPs 技术验证这些证明的正确性，可以在不泄露交易具体内容的情况下，实现交易的验证和确认。

还利用了 ZKPs 技术的可扩展性和灵活性，优化算法参数和改进数据结构等方式，进一步提高了 ZKPs 技术在 ZTC 中的性能和效率。

#### 4.3.3、加密技术与匿名性

应用加密技术来保护用户的交易数据，结合匿名性技术来进一步增强用户的隐私保护能力。先进的加密算法对用户的交易数据进行加密处理，确保数据在传输和存储过程中的安全性。同时，环签名和混淆网络等匿名性技术来隐藏用户的真实身份和交易路径，防止用户的隐私被泄露或追踪。

加密技术与匿名性的完美结合，使得 ZTC 在保障用户隐私和数据安全方面达到了一个新的高度。



#### 4.3.4、隐私保护机制

##### 1. 隐私保护智能合约

随着智能合约在区块链上的广泛应用，ZTC 设计实现了隐私保护智能合约，使得智能合约的执行过程和结果能够在不泄露用户隐私的前提下进行验证和记录。通过结合零知识证明、同态加密等隐私保护技术，确保智能合约的隐私性和安全性。

##### 2. 隐私保护跨链交易

随着区块链技术的不断发展，跨链交易成为了实现不同区块链之间价值流通的关键技术。然而，跨链交易中的隐私保护问题也愈发凸显。ZTC 提出了隐私保护跨链交易机制。通过利用零知识证明技术，实现在不同区块链之间进行隐私保护的跨链交易，确保交易过程中用户的隐私和数据安全。

##### 3. 隐私保护节点协作

在 ZTC 网络中，节点之间的协作是保障网络正常运行的关键。然而，节点之间的协作也可能带来隐私泄露的风险。为了解决这个问题，通过利用安全多方计算技术，确保在多个节点之间安全地共享和验证交易信息，保护用户的隐私和数据安全。这种机制不仅提高节点协作的效率和安全性，进一步增强 ZTC 的隐私保护能力。

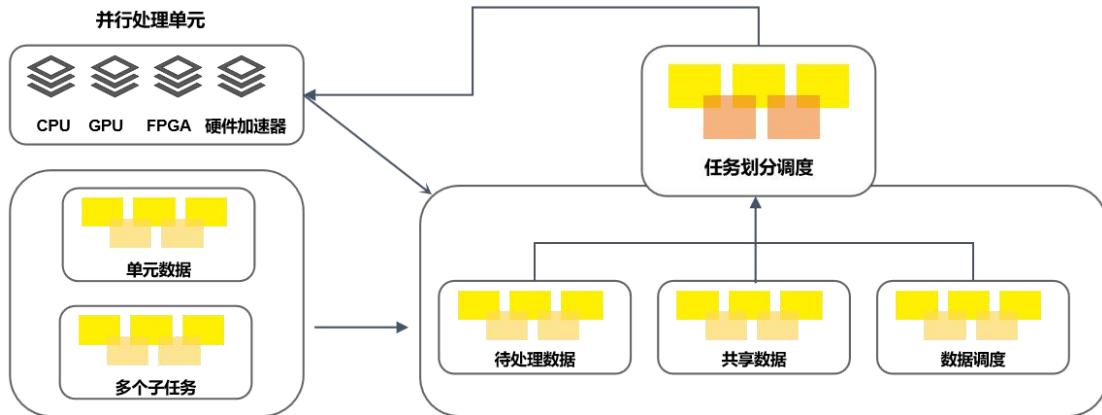
## 4.7 智能合约支持

#### 4.4.1、Layer 2 的实现

认识到 Layer 1 主链的性能限制，ZTC 选择在 Layer 2 层实现智能合约。Layer 2 解决方案，如状态通道 (State Channels)、侧链 (Sidechains)、分片 (Sharding)



和 Rollups 等，允许大部分计算和数据处理在链下进行，仅将关键数据或状态更新提交到 Layer 1 进行验证和记录。



**这种架构的主要优势在于：**

- 1. 性能提升：**由于大部分计算和数据处理在链下进行，Layer 2 可以支持更高的交易吞吐量和更快的合约执行速度。
- 2. 成本降低：**由于 Layer 2 的链下交易无需支付高昂的矿工费用，因此可以显著降低智能合约的执行成本。
- 3. 用户体验优化：**更快的交易速度和更低的成本将带来更好的用户体验，特别是在需要频繁交互的智能合约应用中。

#### 4.4.2、并行执行环境在智能合约执行中的应用

ZTC 采用并行执行环境 (Parallel Execution Environment, PEE) 技术。允许同时处理多个智能合约的调用和状态更新，从而实现高效的合约执行。具体实现方式包括：

- **状态分片：**将区块链的状态数据分成多个分片，每个分片由一个或多个节点



并行处理。智能合约的执行可以在不同的状态分片上并行进行，从而显著提升吞吐量。

- **智能调度：**系统根据合约的优先级、资源需求和其他因素智能地调度合约的执行顺序，确保资源的有效利用和合约的快速响应。
- **轻量级虚拟机：**采用优化的轻量级虚拟机技术，减少执行智能合约所需的计算和存储资源，提高执行效率。
- **事务流水线：**将智能合约的事务处理过程分解为多个阶段，并在不同的处理单元中并行执行，形成事务流水线，以最大化资源利用率。

#### 4.4.3、跨链智能合约

随着区块链互操作性的需求日益增加，ZTC 将支持跨链智能合约的部署和测试。跨链技术允许智能合约在不同区块链网络之间无缝互操作，扩展智能合约的应用范围和灵活性。

- **跨链桥接：**构建连接不同区块链网络的桥接协议，实现跨链通信和数据传输。这可以基于现有的中继链（Relay Chain）或侧链（Sidechain）技术。
- **跨链共识：**设计跨链共识机制，确保跨链交易的一致性和安全性。这可能涉及多个区块链网络之间的共识算法协调和验证过程。
- **跨链验证：**提供跨链验证机制，确保跨链智能合约的正确性和安全性。这可能包括跨链事务的验证、状态数据的同步和验证等。



# 05/技术架构与实施

## 5.1 ZTC 系统架构详解

### 系统整体架构概览

ZTC 整体系统架构是基于分层设计思想构建的，以实现高性能、高安全性、高扩展性和高互操作性的区块链服务。该架构自底向上依次包括：底层基础设施层、网络层、共识层、Layer 2 扩展层、智能合约层和应用层。



### 各层次组件的功能与交互

- **底层基础设施层:** 提供硬件和软件基础设施支持，包括分布式存储系统（如



IPFS、Swarm 等)、网络通信协议 (如 Libp2p、gRPC 等) 和加密技术 (如椭圆曲线加密算法、哈希函数等)。通过分布式存储确保数据的冗余性和持久性，网络通信协议保障节点间的通信效率和安全性，加密技术则保护数据的机密性和完整性。

- **网络层**: 负责节点之间的通信和数据传输，实现信息的实时、高效和可靠的传播。通过点对点 (P2P) 网络通信、节点发现、数据验证和同步等机制，确保网络的稳定性和安全性。
- **共识层**: 采用高性能的共识算法 (如 STARKs、Rollups 等)，确保网络中的交易数据得到公正、可靠和一致的验证和确认。通过验证者节点之间的协作和竞争，实现交易数据的快速确认和全网同步。
- **Layer 2 扩展层**: 通过状态通道 (State Channels)、侧链 (Sidechains)、分片 (Sharding) 等技术实现链下交易处理，提高交易速度和吞吐量，降低交易费用。状态通道允许交易双方建立私有的通信通道，进行高频、小额的交易，而无需每次都写入主链；侧链则作为与主链分离的区块链，通过跨链桥接实现与主链的互操作性；分片则将主链拆分成多个子链，并行处理交易数据。
- **智能合约层**: 支持智能合约的编写、部署和执行，实现去中心化应用的开发和运行。智能合约是基于区块链技术的自动执行程序，包含一组条件和操作的规则集合。开发者可以使用 Solidity、Vyper 等编程语言编写智能合约，并通过编译器将其转换为字节码部署到区块链上。
- **应用层**: 为用户提供丰富的区块链应用场景和服务，如支付、资产交易、去中心化金融 (DeFi) 等。调用智能合约的接口，实现各种区块链应用的业务



逻辑和数据处理。

## 底层技术栈的选择与配置

ZTC 的底层技术栈主要基于广泛应用的区块链技术栈，包括：

- **加密库**：如 OpenSSL、libsodium 等，用于提供加密算法和哈希函数等安全功能。
- **共识算法库**：如 StarkNet 的 STARKs 算法、Optimistic Rollups 算法等，用于实现高效、安全的共识机制。
- **网络通信库**：如 Libp2p、gRPC 等，用于实现节点间的通信和数据传输。

根据实际需求选择适合的技术栈，并进行相应的配置和优化，以确保系统的稳定性和性能。

## Layer 2 扩展技术的实现

实现 Layer 2 扩展技术以提高交易速度和吞吐量：

### ◆ 状态通道 (State Channels)：

状态通道允许交易双方建立私有的通信通道，并在该通道内进行高频、小额的交易。只有最终的结算结果才会被提交到主链上进行验证和记录。

实现高效的交易处理，同时降低交易费用。但是，用户需要确保通道的安全性，并管理通道的生命周期和状态。

### ◆ 侧链 (Sidechains)：

侧链是与主链分离的区块链，具有自己的区块参数和共识模型。侧链可以独立运行，并支持更多复杂的应用场景。



通过跨链桥接技术，实现主链和侧链之间的互操作性。部署到主链的智能合约也可以部署到侧链上，并在侧链上执行。  
侧链的引入可以扩展 ZTC 的应用范围，并提高整个系统的吞吐量和性能。

## 5.2 共识算法

### STARKs 算法实现

为了追求极致的交易性能和安全性，ZTC 选择了 STARKs (ZK-SNARKs/ZK-STARKs) 的共识算法。这类算法的核心思想是通过数学证明来验证交易的正确性，而无需公开具体的交易内容，从而实现高效且无需信任的交易验证和确认。

### 算法原理

STARKs 允许交易在链下进行，将压缩后的交易证明（即零知识证明）提交到链上进行验证。这种设计使得大量的交易可以在链下并行处理，从而极大提高了交易速度和吞吐量。

交易双方首先在一个离线的、可信的环境（称为“验证器”）中执行交易，并生成相应的交易证明。然后，这个证明会被发送到链上，由其他节点进行验证。由于零知识证明的特性，验证节点无需知道具体的交易内容，只需要验证证明的正确性即可。

### 具体实现

- ❖ **验证器部署：**在网络中部署一定数量的验证器节点。这些节点负责在链下执



行交易，并生成相应的交易证明。

- ❖ **交易执行与证明生成：**当用户发起交易时，验证器节点会执行该交易，并生成一个包含交易执行结果的零知识证明。这个证明会被发送到链上。
- ❖ **链上验证：**链上的节点接收到证明后，会使用 STARKs 的验证算法来验证证明的正确性。如果验证通过，则该交易将被视为有效，并被添加到区块链中。
- ❖ **欺诈检测与惩罚：**如果验证器节点被发现生成了错误的证明，系统将对其进行惩罚，以确保系统的安全性和可信度。

## 性能测试与安全性验证

为了确保 STARKs 在 ZTC 中的有效性和安全性。

性能测试将关注以下关键指标：

- ✓ **执行速度：**验证器节点执行交易并生成证明的速度。
- ✓ **吞吐量：**系统单位时间内能够处理的交易数量。
- ✓ **延迟：**从交易发起到被确认并添加到区块链中的时间间隔。

使用专业的性能测试工具和方法，对 ZTC 进行详细的性能测试，并根据测试结果进行相应的优化和改进。

## 安全性验证

安全性验证将关注以下方面：

- ✓ **抗攻击能力：**系统是否能够抵御各种网络攻击，如双重支付攻击、51% 攻击等。
- ✓ **证明的正确性：**验证器节点生成的证明是否能够被正确验证，且不存在被篡改。



改的风险。

- ✓ **欺诈检测与惩罚机制：**系统是否能够及时发现并惩罚欺诈行为，确保整个系统的安全性和可信度。

## 5.3 数据隐私与安全

### 5.3.1 隐私保护技术的具体应用

ZKPs 是一种允许一方（证明者）向另一方（验证者）证明某个陈述为真，而无需透露任何额外信息的技术。这种技术特别适用于区块链场景，因为它可以在不泄露具体交易数据的情况下验证交易的有效性。

- **在 ZTC 中的应用：**我们将利用 ZKPs 技术实现隐私交易。具体来说，交易双方可以生成一个 ZKPs 证明，证明交易是有效的，然后将这个证明提交到区块链上进行验证，而无需公开具体的交易内容。
- **部署与测试：**在部署阶段，我们将选择合适的 ZKPs 算法，如 zk-SNARKs 或 zk-STARKs，并根据 ZTC 的具体需求进行参数配置和环境设置。在测试阶段，我们将重点关注算法的执行效率、正确性和安全性，确保其在 ZTC 中的有效应用。

### 5.3.2 同态加密技术

同态加密是一种允许在加密数据上进行计算并得到加密结果的加密技术。这种技术可以在不解密数据的情况下对数据进行处理和分析，从而保护数据的隐私性。利用同态加密技术实现敏感数据的隐私处理。例如，在智能合约中，可以使用同态加密技术对用户的资产进行加密处理，然后在加密状态下进行资产转移和计算，

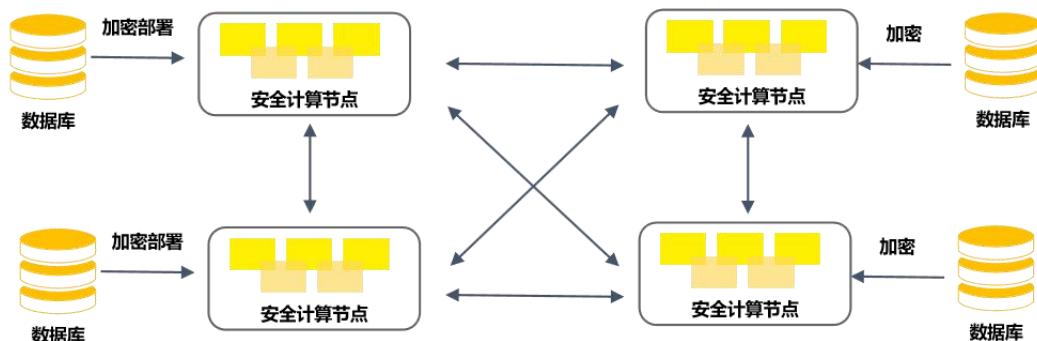


从而保护用户的资产隐私。

### 5.3.3 安全多方计算 (MPC)

MPC 允许多个参与方在互不信任的情况下共同计算一个函数的技术。每个参与方只能看到自己的输入和输出，无法获取其他参与方的输入信息。这种技术特别适用于需要多个参与方共同处理敏感数据的场景。

利用 MPC 技术实现跨链交互和多方协作。例如，在跨链交易中，使用 MPC 技术来确保交易双方在不泄露各自资产信息的情况下完成交易。在多方协作中，确保各方在不泄露各自敏感信息的情况下共同完成某项任务。



MPC 技术的部署和测试将关注其在 ZTC 中的实际应用效果。选择合适的 MPC 协议和算法，并进行参数配置和环境设置。在测试阶段，对 MPC 协议的性能、安全性和易用性进行全面评估，并根据测试结果进行相应的优化和改进。

### 5.5.4 ZKPs 算法

- **选择合适的 ZKPs 算法：**根据 ZTC 的具体需求选择合适的 ZKPs 算法，如 zk-SNARKs 或 zk-STARKs。



- **配置参数和环境：**根据所选算法的要求配置相应的参数和环境设置。
- 编写测试用例：编写涵盖各种场景和边界条件的测试用例以全面评估算法的性能、正确性和安全性。
- 执行测试：使用自动化测试工具或手动执行测试用例以获取测试结果。
- 分析测试结果：对测试结果进行详细分析以识别潜在问题和改进点。
- 优化和改进：根据测试结果进行相应的优化和改进以提高算法的性能和安全性。

### 5.5.5 匿名性实现细节

实现隐私交易和匿名性时我们将采取以下措施：

- **加密用户身份和交易信息：**使用先进的加密算法对用户身份和交易信息进行加密保护以防止未经授权的访问和泄露。
- **采用匿名交易协议：**设计并实现匿名交易协议以隐藏交易双方的身份和交易金额等敏感信息。这可能涉及使用混币技术、环签名技术或其他匿名化技术。
- **验证和审计机制：**建立严格的验证和审计机制以确保交易的真实性和合法性同时防止欺诈行为的发生。

### 5.5.5 安全性审计

为确保 ZTC 的安全性我们将进行定期的安全性审计和漏洞管理：

- **安全性审计：**定期对系统进行全面的安全性审计以发现潜在的安全漏洞和风险点。这可以通过内部安全团队、外部安全顾问或自动化安全扫描工具来完成。



- **漏洞管理：**建立有效的漏洞管理机制以确保漏洞的及时发现、报告、修复和验证。这可能涉及设置漏洞奖励计划、建立漏洞响应团队和制定漏洞修复流程等措施。

### 5.5.7 监控和日志记录

监控和日志记录是确保系统安全性和稳定性的重要组成部分。通过实时监控系统的运行状态和记录关键事件，可以及时发现潜在的安全问题、性能瓶颈或错误，并采取相应的措施进行修复和优化。

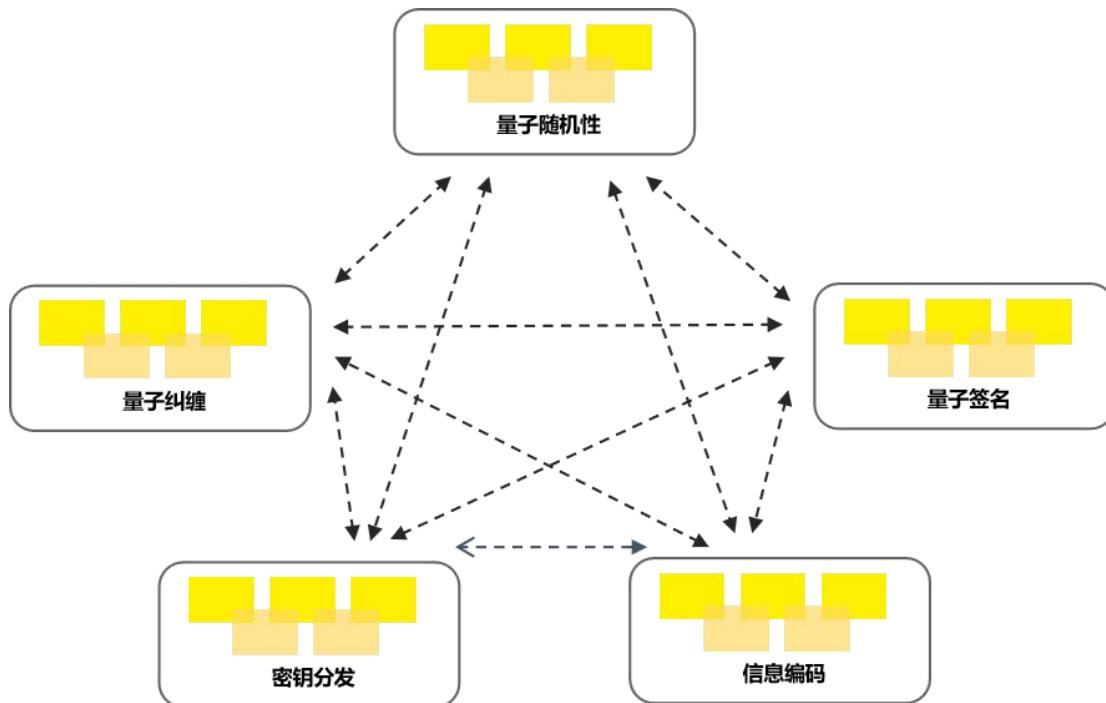
**系统状态监控：**监控节点状态、网络连通性、系统资源利用率等关键指标，确保系统稳定运行。

- **交易监控：**监控交易的创建、验证、执行和确认过程，确保交易的正确性和及时性。
- **安全事件监控：**监控异常行为、潜在攻击等安全事件，及时报警并采取应对措施。
- **详细日志：**记录系统运行的详细日志，包括交易日志、节点日志、安全日志等，以便后续审计和故障排查。
- **加密存储：**对敏感日志进行加密存储，确保数据的安全性和隐私性。
- **日志分析：**利用日志分析工具对日志数据进行挖掘和分析，发现潜在的安全风险或性能瓶颈。

### 5.5.8 量子密码学应用

**算法选择：**选择经过广泛研究和验证的后量子密码学算法，如基于格的密码学算

法、基于哈希的密码学算法等。



**密钥管理:** 设计并实现安全的密钥管理方案，确保后量子密码学算法中的密钥的安全性和可用性。

**逐步迁移:** 逐步将传统的密码学算法替换为后量子密码学算法，确保系统的平稳过渡和安全性。

**定期评估:** 定期对系统的安全性进行评估和测试，确保后量子密码学算法在系统中的有效性和安全性。

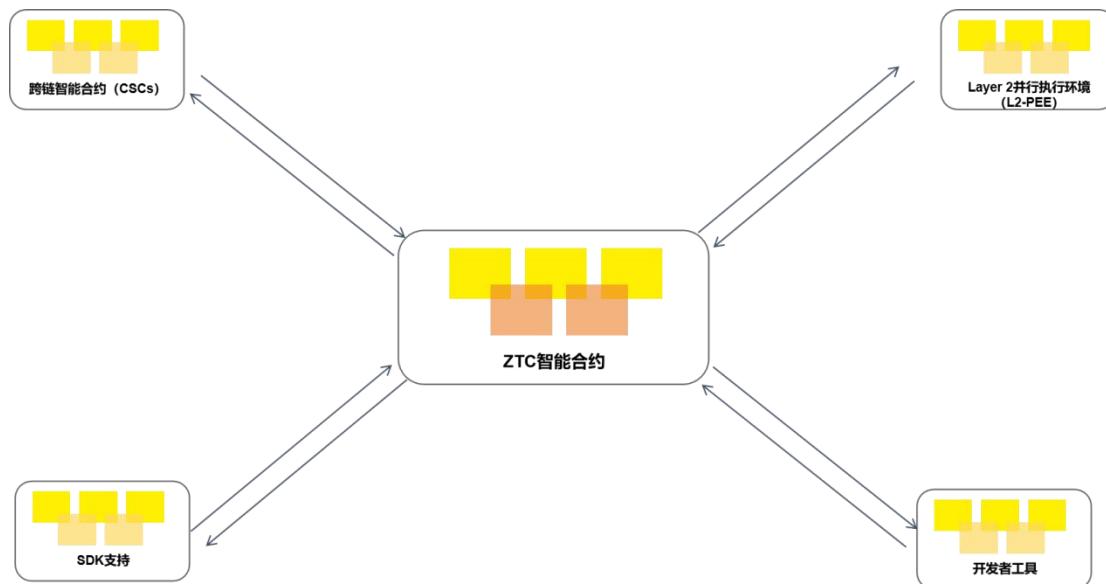
**持续改进:** 根据评估结果和最新的研究进展，对后量子密码学算法进行持续的改进和优化。



## 5.4 智能合约平台

### 5.4.1 智能合约平台的搭建

ZTC 的智能合约平台基于 Layer 2 解决方案，支持多种智能合约编程语言 Solidity 并提供丰富的工具链支持，如 Truffle 为开发者提供极大的便利。平台采用模块化设计，可以轻松扩展和集成新的功能和组件，以满足不断增长的业务需求。



### 5.4.2 Layer 2 并行执行环境配置

提高智能合约的执行效率，ZTC 项目引入了 Layer 2 并行执行环境（Layer 2 Parallel Execution Environment, L2-PEE）的概念。L2-PEE 通过优化算法和分布式计算技术，使得多个智能合约能够并行执行，从而显著提升交易速度和吞吐量。ZTC 项目将选择经过严格测试和优化的 L2-PEE 实现，进行精细的配置和调



整，确保其在 ZTC 中的稳定、高效运行。

### 5.4.3 跨链智能合约的开发与测试

在不同区块链网络之间的互操作性，ZTC 项目将深入研究并开发跨链智能合约（Cross-chain Smart Contracts, CSCs）。这包括开发一套完善的跨链智能合约开发框架和工具链，以及设计跨链通信协议（Cross-chain Communication Protocol, CCP）和跨链适配器（Cross-chain Adapter, CA），为开发者提供一站式的解决方案。ZTC 项目将建立跨链智能合约的测试环境，对 CSCs 的正确性、安全性和性能进行全面的测试，确保其在实际应用中的稳定性和可靠性。

### 5.4.4 开发者工具与 SDK 支持

降低开发者在 ZTC 上进行智能合约开发的门槛，ZTC 项目将提供一套功能强大、易于使用的开发者工具和 SDK 支持。这些工具包括智能合约的集成开发环境（Integrated Development Environment, IDE）、调试工具（Debugging Tools）、测试框架（Testing Framework）以及详尽的文档和示例代码。ZTC 项目团队将定期更新和维护这些工具，确保其与 ZTC 的最新版本保持兼容，为开发者提供持续、稳定的技术支持。



# 06/应用生态

## 6.1 应用场景分析

### ❖ 高性能交易与支付

ZTC 以其高性能架构为基础，为交易与支付领域带来了革命性的变革。通过其优化的共识算法和分布式账本技术，ZTC 能够实现低延迟、高吞吐量的交易处理，为零售支付、跨境支付和证券交易等高频次交易场景提供了理想的解决方案。在零售支付领域，ZTC 的即时确认和低成本特性使得消费者和商家能够享受更加流畅和高效的支付体验。在跨境支付领域，ZTC 的去中心化特性消除了传统跨境支付中的中介环节，降低了交易成本和风险，同时提高了交易速度。在证券交易领域，ZTC 的高性能和可扩展性能够满足大规模交易的需求，为投资者提供更加便捷和安全的交易环境。

### ❖ 去中心化金融 (DeFi) 应用

ZTC 的智能合约平台为 DeFi 应用提供了坚实的基础。通过其高效、可扩展的智能合约执行环境，ZTC 能够支持各种 DeFi 应用，包括借贷、资产交换、衍生品交易等。在借贷领域，ZTC 的智能合约可以确保借贷过程的透明性和公正性，同时提供低利率和灵活的还款方式。在资产交换领域，ZTC 的智能合约可以实现去中心化的资产交换，为用户提供更加便捷和安全的交易方式。在衍生品交易领域，ZTC 的高性能和可扩展性能够满足复杂衍生品交易的需求，为投资者提供更加丰富的交易策略。

### ❖ 隐私保护与资产安全

在区块链领域，隐私保护和资产安全一直是用户最为关心的问题。ZTC 通过采用



先进的隐私保护技术，如零知识证明（ZKPs）和混币器等，为用户提供了强大的隐私保护能力。这些技术可以在保护用户隐私的同时，确保交易的透明性和公正性。此外，ZTC 还采用了高度安全的共识算法和加密技术，如基于分片技术的共识算法和先进的加密算法，以确保区块链网络的安全性和稳定性。这些安全措施使得用户可以放心地在 ZTC 上进行交易和资产管理，无需担心隐私泄露和资产安全问题。

## 6.2 商业应用实例

### 具体的商业用例分析

- **零售支付：**ZTC 作为一种新型的数字货币支付手段，可以与现有的零售支付系统无缝集成。通过集成 ZTC 支付功能，零售商可以为用户提供更加灵活和便捷的支付方式，同时降低交易成本和提高支付效率。例如，在线商店可以接受 ZTC 作为支付方式，从而吸引更多的数字货币用户；实体店铺也可以安装支持 ZTC 的支付终端，方便消费者进行数字货币支付。
- **跨境支付：**传统的跨境支付存在诸多痛点，如成本高、速度慢、风险大等。ZTC 通过其去中心化的特性和智能合约技术，为跨境支付提供了全新的解决方案。通过智能合约和去中心化网络，ZTC 可以实现快速、低成本、安全的跨境支付。例如，两个不同国家的商家可以通过 ZTC 进行跨境交易，无需经过繁琐的银行转账和货币兑换过程，大大提高了交易效率和降低了成本
- **DeFi 借贷：**ZTC 的智能合约平台可以支持去中心化借贷应用。用户可以将自己的资产作为抵押品在平台上发布借款需求，并通过智能合约实现自动化审批和放款。这种借贷方式具有低利率、高透明度和灵活性等优点，为用户



提供了更加便捷和安全的借贷服务。同时，智能合约还可以确保借贷过程的公正性和透明性，避免了传统借贷中的欺诈和违约风险。

### 合作伙伴与集成案例

ZTC 将与多个合作伙伴建立紧密的合作关系，共同推动区块链技术的应用和发展。与金融机构、支付平台、DeFi 项目等建立合作关系，通过集成 ZTC 的技术和服  
务，为用户提供更加全面和优质的区块链服务。

## 6.3 生态系统建设

ZTC 将建立一个活跃的开发者社区，为开发者提供丰富的资源和支持。提供详尽的开发者文档、强大的 SDK、示例代码、教程和在线支持等，帮助开发者快速上手并高效开发基于 ZTC 的应用。

# 07/经济生态

## 7.1 发行方案

**ZTC 发行方案**

**代币名称：ZTC**

**总量：233 亿枚 ZTC**

**分配方案：**

- **ZTCY 铭文兑换 (10%)**: 初始的 10% ZTC 将通过 ZTCY 铭文进行兑换。
- **投资人产生 (20%)**: 20%的 ZTC 将通过投资产生，包括来自风险投资 (VC) 和直接用户投资。

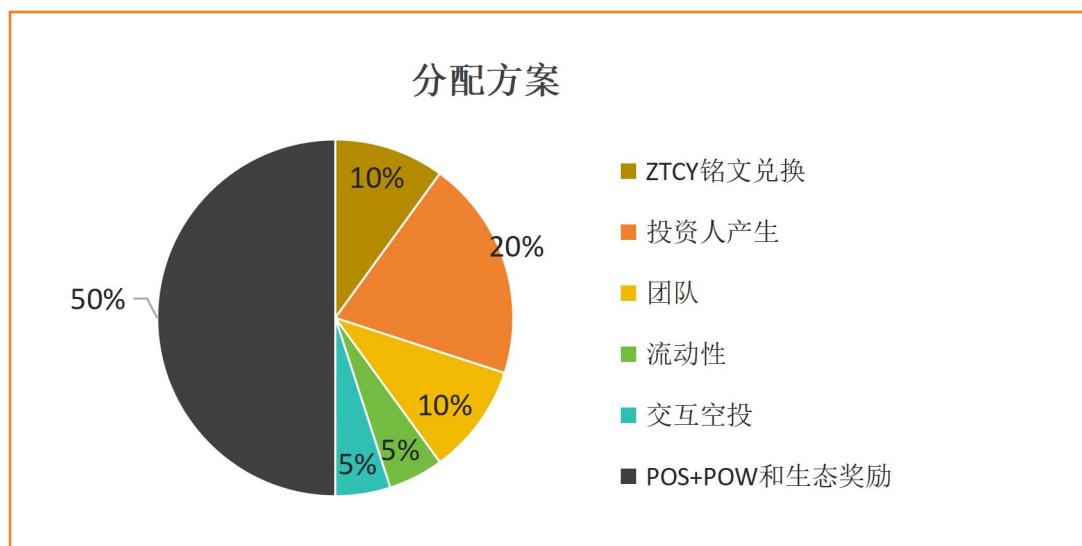


**团队预留 (10%)**: 团队将预留 10% 的 ZTC 用于项目运营和团队薪酬。这部分代币将在 5 年内逐步解锁，每年解锁 2% 以确保团队的长期参与和稳定性。

**流动性 (5%)**: 为了确保代币在市场上的流通性，将预留 5% 的 ZTC 用于市场流通和交易。

**交互空投 (5%)**: 通过交互空投活动，用户获得额外的 ZTC 奖励。

**POS+POW 和生态奖励产出 (50%)**: 剩余的 50% ZTC 将通过 Proof of Stake (POS) 和 Proof of Work (POW) 机制生态奖励产出。



## 7.2 ZTC 价值

ZTC 的价值源于其独特的分配方案、广泛的生态策略以及深远的影响力。将总量设定为 233 亿，恰好对应全球 233 个国家和地区，这一设计不仅体现了 ZTC 的全球化视野和包容性，更预示着其在全球范围内的广泛应用潜力。结合技术创新、满足不断增长的生态需求，以及社区成员的共识与支持，ZTC 展现出了显著的价值增长潜力。这种全球性的布局和定位，使得 ZTC 有望成为连接世界各地、推动区块链技术普及和应用的重要桥梁。



## 7.3 ZTC 激励

ZTC 将采用多种激励机制，包括节点奖励、开发者奖励和社区贡献奖励，以吸引和激励更多的用户、开发者和合作伙伴参与 ZTC 生态的建设和发展。这些激励措施将促进生态的繁荣和多样性，为投资者和社区成员带来长期稳定的回报。

## 7.4 ZTC 完全去中心化公平发射台

ZTC 作为一个完全去中心化的公平发射台，旨在通过其独特的设计和机制，防止 LP（流动性提供者）跑路和老鼠仓风险。在区块链和数字货币领域，LP 跑路和老鼠仓风险一直是投资者和社区成员关注的焦点。ZTC 通过其去中心化的特性和公平的发射机制，为投资者提供了一个安全、可靠的平台，从而降低了这些风险。

# 08/发展路线图

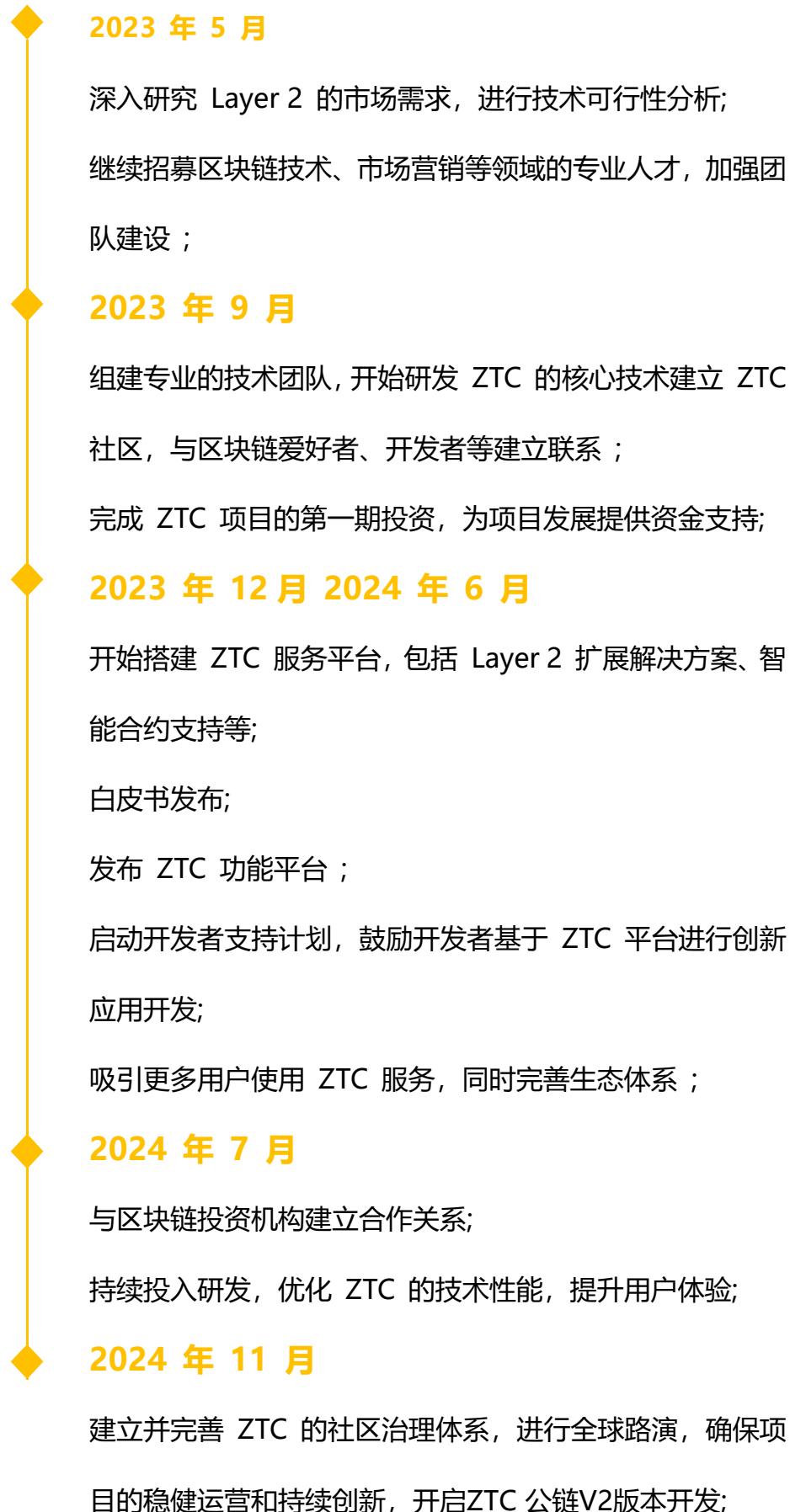


2022 年 6 月

ZTC 概念首次由 ZTC 创新实验室提出，作为基于比特币 Layer 2 的创新区块链解决方案；

2022 年 12 月

ZTC 项目团队成立，开始详细讨论并立项；  
开始建立合作伙伴关系网络，涵盖 Layer 2 技术提供商、  
区块链开发机构等；





- 2025 年 1 月**  
在主流交易所上线 ZTC 代币 (ZTC)，启动全球运营策略；  
拓展市场，与更多品牌和企业建立合作关系，提升 ZTC 的  
品牌影响力；
- 2025 年 6 月**  
与更多区块链项目、技术供应商建立合作关系，共同推动区  
块链行业的发展；  
开展用户教育活动，提升用户对 ZTC 的了解和使用能力；
- 2025 年 8 月**  
研发 V2 ZTC Layer 2 技术，持续优化 ZTC 的性能和安全  
性；  
探索更多 ZTC 的应用场景；
- 2026 年-**  
制定全球扩张策略，在更多国家和地区设立办事处，扩大市  
场覆盖范围；  
与现有合作伙伴深化合作关系，共同推动 ZTC 在全球市场  
的发展；  
参与社会公益事业，提升 ZTC 项目的社会影响力和品牌形  
象；  
开展跨行业合作，探索 ZTC 在更多领域的应用和可能性。

Zitcoin



# 09/项目团队

## 9.1 基金会

ZTC 基金会是一家在新加坡注册的非营利性组织，专注于推动 Zitcoin (ZTC) 区块链项目的发展和应用。作为 ZTC 项目的核心支持机构，基金会致力于通过资金支持、技术研发、社区建设等多方面的努力，为 ZTC 项目的长远发展提供坚实保障。基金会的成员由区块链领域的专家、技术开发者、金融从业者及热心于区块链技术发展的各界人士组成，团队成员共同致力于打造一个安全、高效、可扩展的区块链生态系统，为全球用户带来更加便捷、安全的金融服务体验。

## 9.2 团队成员

ZTC 团队共有 20 多位成员，以下是其中部分成

### YC - CEO

YC 现任 ZTC 的首席执行官，负责公司的整体产品发展与战略规划。他拥有超过 10 年的团队管理经验和超过 12 年的创业 经验，精通区块链金融、金融科技及互联网金融等新兴产业。 YC 曾在世界知名公司任职高管，于 2016 年涉足区块链领域，并成功参与多家区块链产品的上市。

---

### Victor Ma - COO

Victor Ma 现任 ZTC 的首席运营官，负责全球市场运营及业务发展规划。他根据公司的总体战略规划，组织制定中长期发展计划，并推动全球战略和项目的落地实施。Victor Ma 拥有超 5 年的运营管理经验，专注互联网和区块链领域，



擅长处理 复杂的运营问题， 并与各类金融机构建立了良好的合作关系。Victor Ma 本硕毕业于中国清华大学五道口学院， 曾在全球顶级券商任职管理。

---

### **Anthony - CTO**

Anthony 现任 ZTC 的首席技术官， 负责区块链技术的架构设计和开发工作。他精通各类主流共识算法， 熟练掌握区块链系统开发语言。Anthony 拥有超过 10 年的互联网游戏 开发和区块链技术经验， 成功参与多家交易所和数字钱包项目 目的上市。

---

### **Richie -CFO**

Richie 负责 ZTC 的财务工作， 他具备多年的财务管理经验， 毕业于全球知名的财校， 擅长财务增长以及与各国政府机构建立了良好的合作关系， 目前专注区块链行业的投资机会发掘。曾在全球 TOP5 的会计师事务所任职。

---

### **Rison- MM**

Rison 负责 ZTC 的全球营销策略。他具备超过 3 年的 公司营销管理经验， 擅长洞察市场机会并制定营销策略， 以提升品牌影响力和产品推广。Rison 精通互联网、电 商及金融科技领域的品牌管理， 曾帮助多家创业公司成功转型品牌形象。具备丰富的实战经验和成功塑造品牌影响力的能力。

---

### **Austin koch- LIA**

Austin koch 负责 ZTC 的风险投资和新业务投资。在加入 ZTC 之前， Austin



koch 参与超过 10 种数字货币的设计， 并发现若干安全漏洞，是数字货币社区中值得信赖的成员。此外， 他还参与多个加密货币项目的开发工作。

---

### **Louis Hu- PM**

Louis Hu 负责 ZTC 的合作伙伴关系管理，包括与投资组合公司、子公司、投资者及广泛网络之间的合作。他凭借在风险投资和非营利性技术倡导领域的丰富经验， 为团队带来宝贵的数据、研究和社区组织支持，以推动新兴技术的发展。 Louis Hu 对商业运营模式有深入研究和独到见解，并具备专业的金融知识和丰富的经验。

---

### **Alexander ingold- BD**

Alexander ingold 是一位经验丰富的区块链开发者和爱好者，毕业于全球 QS100 院校计算机系。Alexander ingold 的专业知识和经验为 ZTC 项目的设计提供了宝贵的意见。

---

### **Luca-SE**

Luca 是一位经验丰富的区块链开发者和爱好者，曾经任职于全球知名的游戏公司，自 2016 年起投身于区块链行业，并参与了多个加密货币项目的开发工作。 Luca 的专业知识和经验为 ZTC 项目 提供了宝贵的技术支持。

---

### **Bella-CD**

Bella 是一位经验丰富的设计师，从事设计行业数年，她参与超过数十种数字货币



币的设计，负责组织 ZTC 审核设计方案，明确设计要点和市场设计需求，协调其它相关部门，推动 ZTC 项目目标的实现。

---

## 10/免责声明

---

本文件仅作为信息传达之用，其内容仅供参考，不构成对 ZTC 平台及其相关公司股票或证券买卖的建议、诱导或要约。本文件并不构成任何形式的交易行为、合约或承诺。

鉴于不可预见的情况，本白皮书中列出的目标可能发生变化。尽管我们团队将竭尽所能实现白皮书中的所有目标，但所有购买 ZTC 的个人和团体应自行承担风险。随着项目的进展，文件内容可能会在新版白皮书中进行相应调整，团队将通过网站公告或新版白皮书等方式，将更新内容公之于众。

本文件仅供主动寻求项目信息的特定对象使用，不构成任何投资建议，亦非任何形式的合约或承诺。

ZTC 明确声明不承担由参与者造成的直接或间接损失，包括但不限于：

1. 参与者一旦参与 ZTC 代币分发计划，即表示已充分了解并接受项目风险，并愿意自行承担一切后果。项目团队明确声明不提供任何回报承诺，也不承担由项目直接或间接导致的任何损失。
2. 本项目涉及的代币仅为交易环节中的虚拟数字编码，不代表项目股权、收益权或控制权。
3. 鉴于数字货币本身存在众多不确定性（包括但不限于各国对数字货币的监管环



境、行业内的激烈竞争、数字货币技术漏洞等)，我们无法确保项目的绝对成功，项目存在一定失败风险，且代币价值可能归零。

团队将全力以赴实现文档中提及的目标，但鉴于不可抗力的存在，无法做出完全保证。在法律允许的最大范围内，对于因参与本项目所产生的任何损害及风险，包括但不限于直接或间接的个人损害、商业利润的丧失、商业信息的丢失或任何其他经济损失，团队不承担任何责任。