



HAICHAIN.IO

全球首家商业区块链双通证模型

# | 01 | 概述



## 1.1 项目简介

---

Haichain 项目是全球第一个使用双通证模型来服务产业的区块链项目

Haichain模拟传统经济的投资和生产的关系，设计了双链及双通证。

既为权益记账，同时也为商品和服务做记账，我们将这种特殊分布式记账技术，引入商业生态，让价值在商业体系中自由流转，以此打造一个崭新的，诚信的，去中心化的商业社区生态。

# 1.2

## 幸福链双子星

### Haicoín和Galtcoin概述

为了对Haichain分布式商业平台的所有参与者、贡献者进行记账和资格准入，我们设计了Haicoín和Galtcoin两个通证，即幸福链双子星。

Haichain的双子星，Haicoín，Galtcoin，分别代表着权益标准币和商品（和服务）标准币。

#### 1.2.1 代表产业节点权益的Haicoín

在产业经济体系下，有多个参与角色，比如：平台方、金融机构、技术提供方、运营方、供应商、销售商、消费者等，他们一起为整个产业的建设做出贡献，在Haichain幸福链的规划中，以Haicoín的数量来记录各个产业节点的参与度和贡献，并设定准入门槛。比如，商家持有有一定量的Haicoín就可以入驻通证商场；运营推广做得好直接奖励Haicoín。

#### 1.2.2 代表产业链上商品和服务积分的Galtcoin

在产业链上，Galtcoin是幸福链产业上各种产品和服务的商品积分，用于记账，可以通过Galtcoin在流通领域来享受产品、服务或抵扣现金。

#### 1.2.3 Haicoín和Galtcoin

Haicoín是基础的无记名权益（证券），易流通和交易。Galtcoin是基础的商品加密货币，其80%会在社区经济体流转，和Haicoín是子母币关系，根据Haicoín量，进行权益的按比例分红，分配Galtcoin，即权益挖矿。目前，每5个Haicoín一年产生1个Galtcoin

我们认为在产业链内流通的加密通证而言，转账如果收取手续费会影响通证的广泛使用，带来负面效果的经济激励，所以Haicoín和Galtcoin取消所有交易费用，为所有持有者带来零成本的交易环节，以促进经济发展。

## 1.3 Haichain幸福链解决的问题

---

让区块链技术服务于实体经济是国家，社会以及个体的迫切需求。 但是目前实体企业，初创企业都面临诸多的挑战，

第一，融资困难问题

第二，产品和服务的营销问题 第三，消费群体粘度问题

初创企业的资金门槛越来越高，股权融资，众筹，借债的方式已经无法满足他们的需求。

对于投资者来说，以上的投资方式，在高通胀的时代，他们很难在1-3年内看到投资回报。投资者的权益的欠流通性，无法更好的价值流转。

Haichain 公链将为初创企业，投资者做基本的保证和桥梁。

Haichain 通过双链双币的模式，帮助企业孵化，加速，以及今后的规模化发展。

## 1.4 Haichain幸福链的愿景

---

目前，区块链技术除了深入的应用在了金融服务行业外，还在进一步扩展到其它行业。就像20世纪90年代互联网出现大繁荣，随之而来的技术将彻底改变商业游戏规则一样，区块链正在逐步改变行业的运行规则。

对Haichain幸福链来说，我们践行“区块链+”战略，打造Haichain分布式商业服务平台：将区块链和通证引入商业体系，构建诚信的、去中心化的商业体系，激活产业链的上下游，促进实体经济的发展，助力产业重构和升级，共建产业互联网。

## 1.5 我的解决方案

---

我们设定的双链双币，一种是权益通证和一种商品通证，两者同时在生态中流通，可以帮助企业融资和发展币改。

初创企业可拟定商业智能协约（投资，运营和回报等），申请进入Haichain生态系统，经过Haichain系统的社区投票，投注，最后得到众多商业节点的融资，营销，以及消费的支持和监督，初创企业通过原定的智能合同给商业节点分红。

企业需要进一步规模化发展，可以在Haichain平台发币，对自己的商业节点和有粘度用户，发自己的权益币及商品币，将原先占用经济体的Haicoi和Galtcoin币映射成自己的代币，由我们的Haichain主网支持。而发币之前，Haichain通过双币为企业提供充分的支持。

不仅如此，Haichain平台还为企业提供了商业智能协约上链，资产上链，运营记录上链，促进了其价值流转，让投资，生产和消费链上结合的社区型商业节点式经济体，这是一种「去中心化经济模型」。企业的运营和账目对投资的节点，相对公开和透明。

Haichain 通过双链双币的模式，不仅解决了企业的资金问题，还可以利用社区资源帮助它健康发展，是初创企业的孵化器，加速器，甚至帮助他们今后的规模化发展。Haichain 这种新型的生产关系和价值体系，有助于产业的重构和升级。

# | 02 | 系统模型



## 2.1 Haichain 系统模型概述

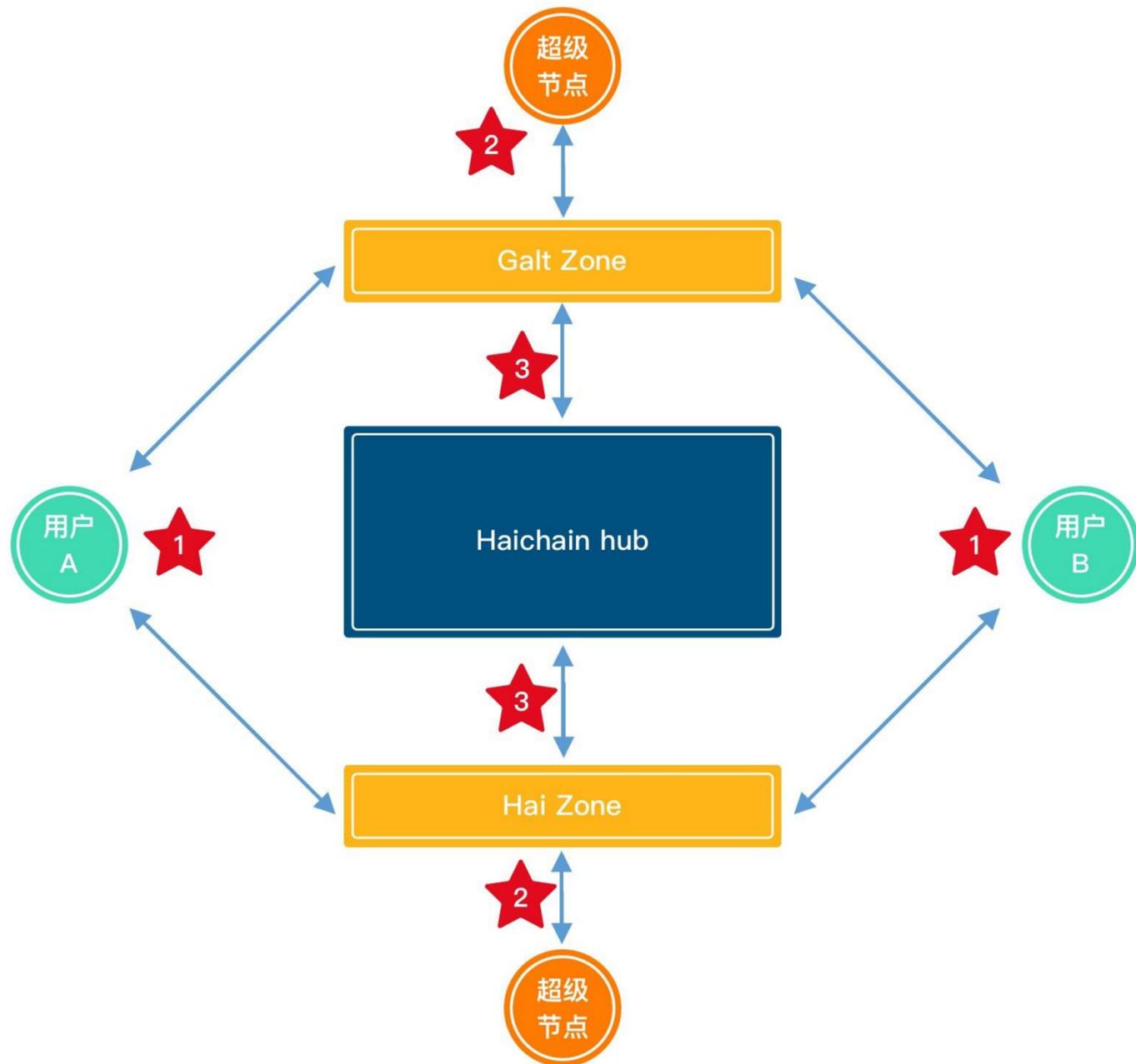
Haichain团队有着多年的建设“区块链+”产业互联网产品的设计，研发和运维的经验。

我们对需求进行了分类，归纳和整理。

完成了以下6大系统模型，该模型把实体经济的需求，系统设计，链下服务和区块链的技术有机结合在一起。

能够提供一站式的服务，便于其他现在系统整合到我们的模型中，有助于发展cosmos区块链网络的生态节约开发成本，提高开发效率。





## 2.2 资产发布模型

资产发布模型主要用于用户资产的发布，该流程如下：

1. 用户在Galt zone或者Hai Zone上发布资产
2. 超级节点负责资产的审核和确认
3. 资产发布成功的话，就可以在Galt zone， Hai Zone以及通过Haichain Hub在各大公链上流通。

补充：

1. 资产的类型包括

*Galtcoin* 资产：以Galtcoin标价的资产 *Haico*in 资产：以Haico

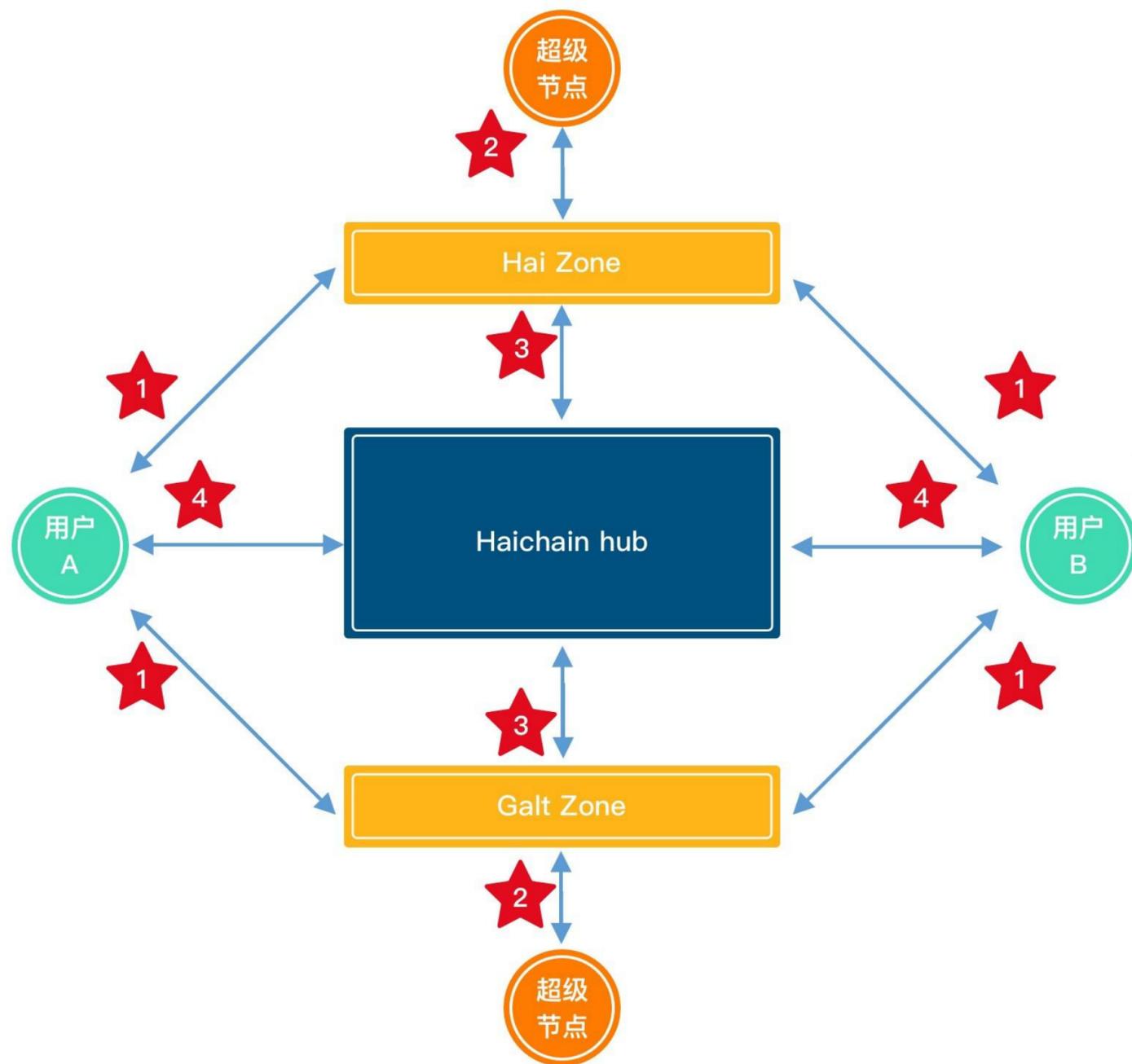
- *Galt*chain上发布的token *Haizone* 资产：在Haichain上发布的token

2. *Hai* Zone 和 *Galt* Zone 的双链架构

- *Haico*in 代表权益标准币，由于其资产的金额较大，其对资产的安全性要求较高，运行效率要求不是那么高。

*Galtcoin* 代表商品（和服务）标准币，由于其资产的金额较小，其对资产的安全性要求相对不那么高，但是对运行效率要求比较高。

正是由于业务逻辑的不同，导致系统模型设计是需要有两种zone



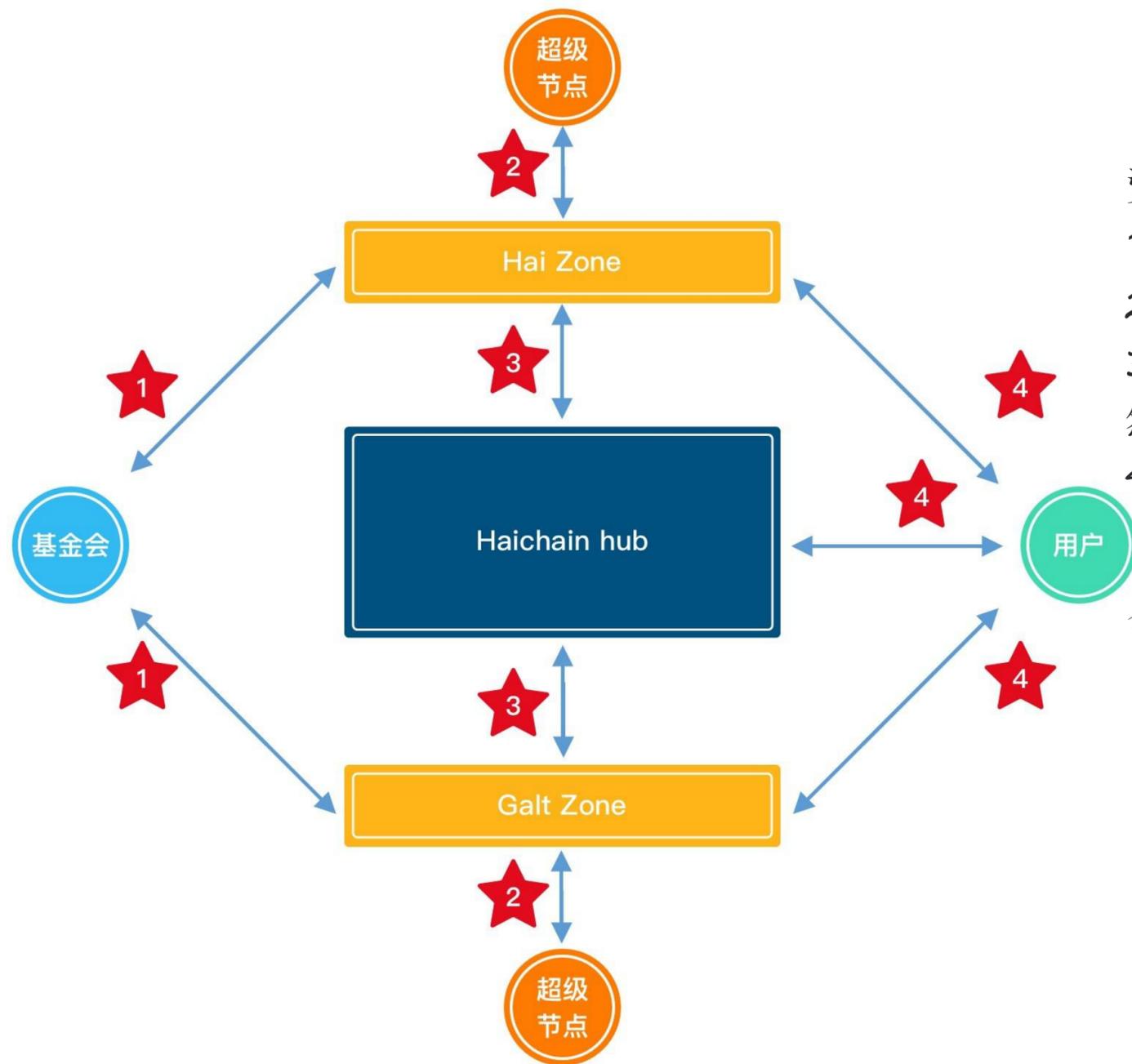
## 2.3 资产锁定模型

资产锁定模型主要用于用户资产的锁定和质押，该流程如下：

1. 用户把资产锁定在Galt Zone或者Hai Zone上
2. 超级节点负责锁定资产的确定，作为后期系统激励的凭证
3. 已锁定的资产不能通过Haichian Hub流通。
4. 用户可以按时从Haichain Hub获得系统激励。

补充: 锁币的权益

- 资产锁定的激励跟锁定资产的金额和时间有关
- 根据锁币金额和时间，可以优先申请超级节点
- 锁币期间，用户可以用锁定的币进行投票等操作



## 2.4 资产销毁模型

资产销毁模型主要用于销毁现有的token以保证它的价值，该流程如下：

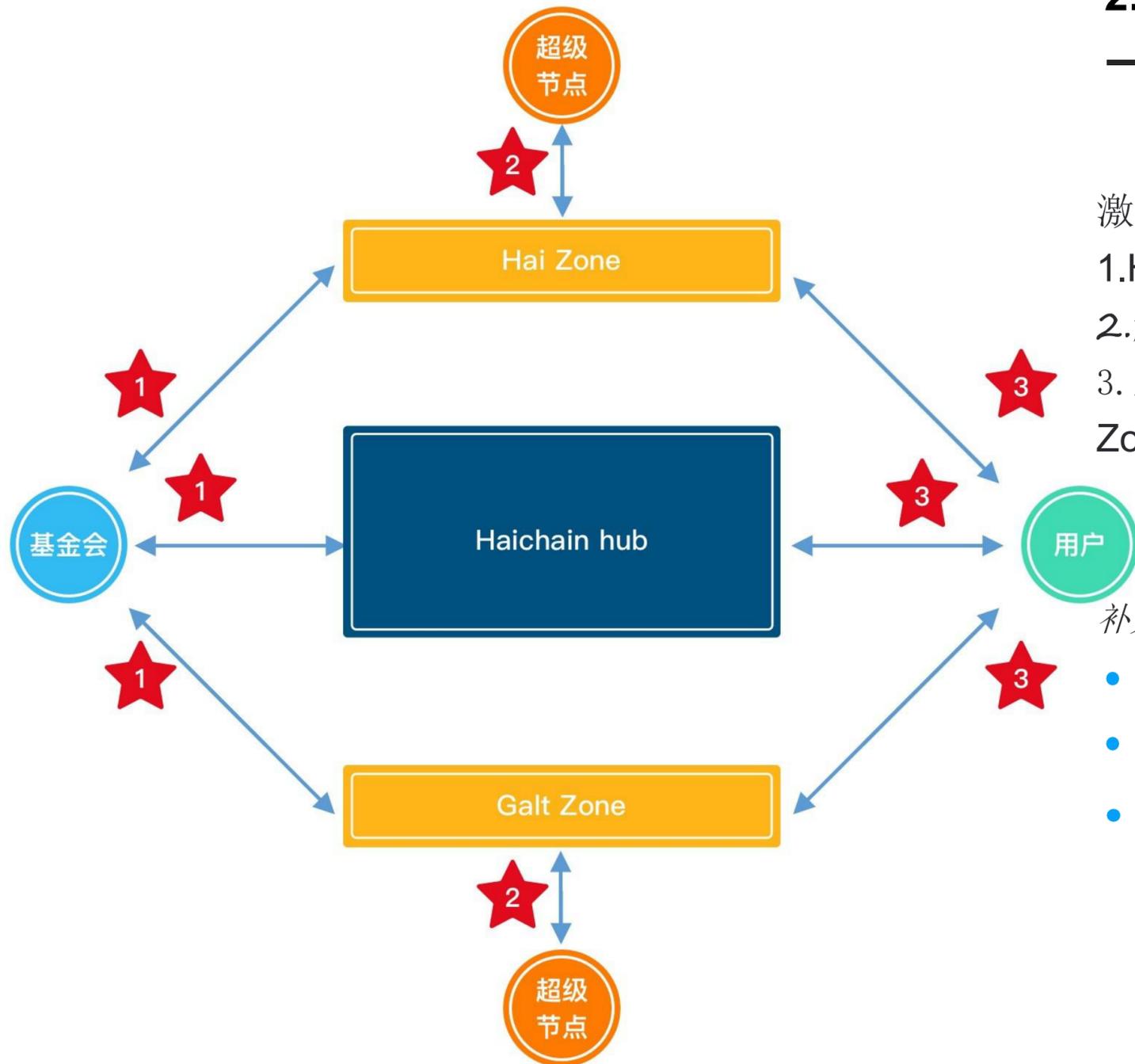
1. HaiDAO根据具体情况，销毁部分token
2. 超级节点负责审核和监督token的销毁情况
3. 由于Haicoins能产生Galtcoin，因此Haicoins的销毁会影响Galtcoin，反之亦然。
4. 每次币的销毁，需要告知用户

补充:token销毁的条件

定期检查币的总量和价值，发现币的总量过多是会销毁 当实体项目失败时，公链的价值下降，相应的币会被销毁

如果galt zone和hai zone上发行的token数量或者总量过大，需要销毁

- 
- 
-



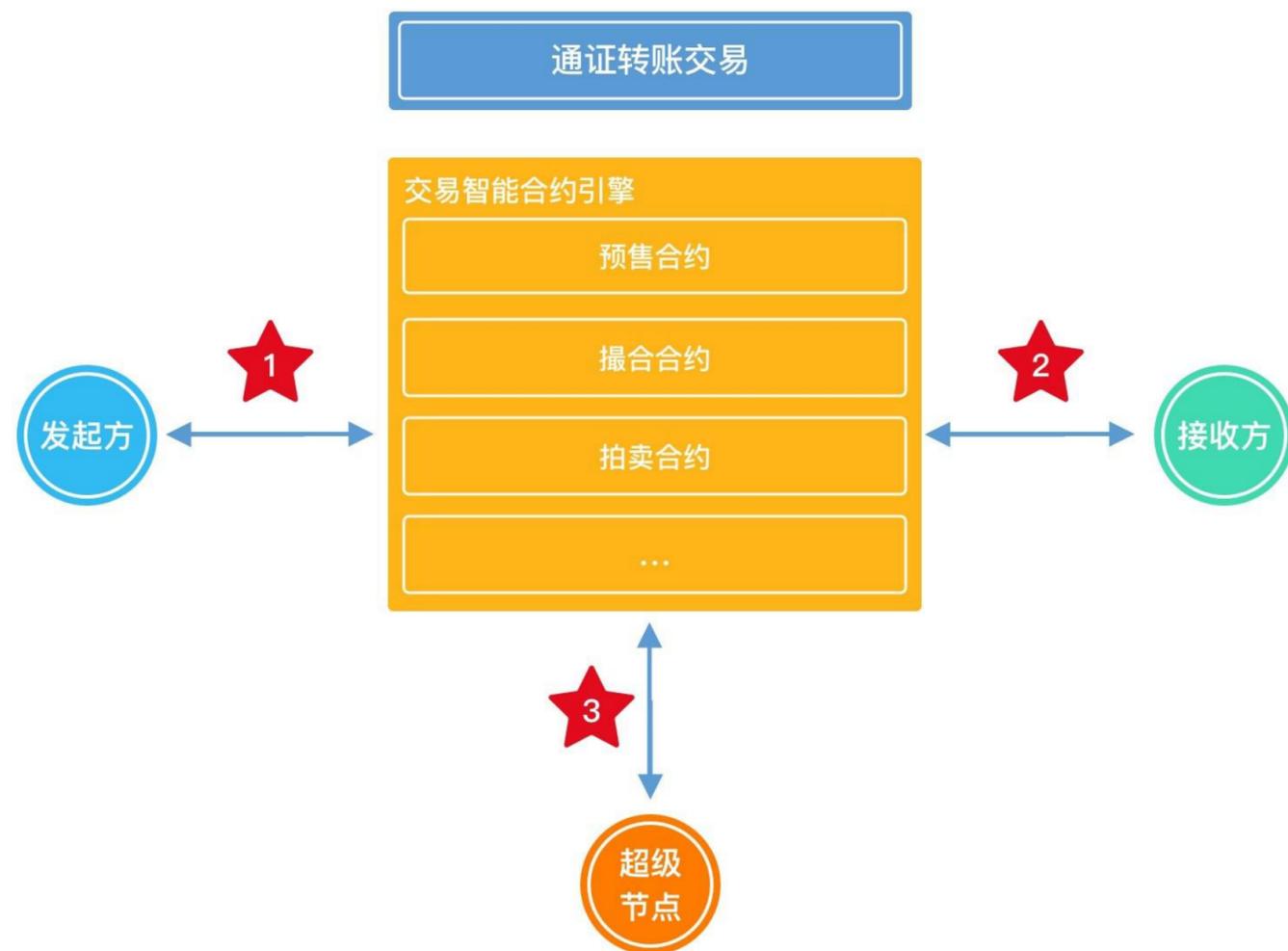
## 2.5 资产激励模型

激励模型主要用于对公链做出贡献的用户给予奖励，该流程如下：

1. HaiDAO(也可以是超级节点)根据具体情况，设置激励的规则
2. 超级节点负责审核和监督激励的执行
3. 对奖励对公链有贡献的用户(包括超级节点),激励主要包括Hai Zone, Galt Zone和Haichain Hub上流通的各种token

补充:激励的来源

- 出块的激励(coinbase) 交易费
- HaiDAO给予做出贡献的用户的奖励
-



## 2.6 交易模型

交易模型主要是完成Haichain, Galtchain以及跨链的交易, 主要包括如下类型:

一.交易的类型

1.通证的转账交易:是指Haicoín, Galtcoin和在此公链上发行的各种通证的转账。

2.交易智能合约模板:是指公链上的智能合约模板引擎, 具体包括

1. 预售合约

2. 撮合合约

3.拍卖合约等。 二.交易的实现

3. 发起方发起交易, 可以发起上述的[通证转账交易]或[交易智能合约]

4.接受方接受发起方的交易金额

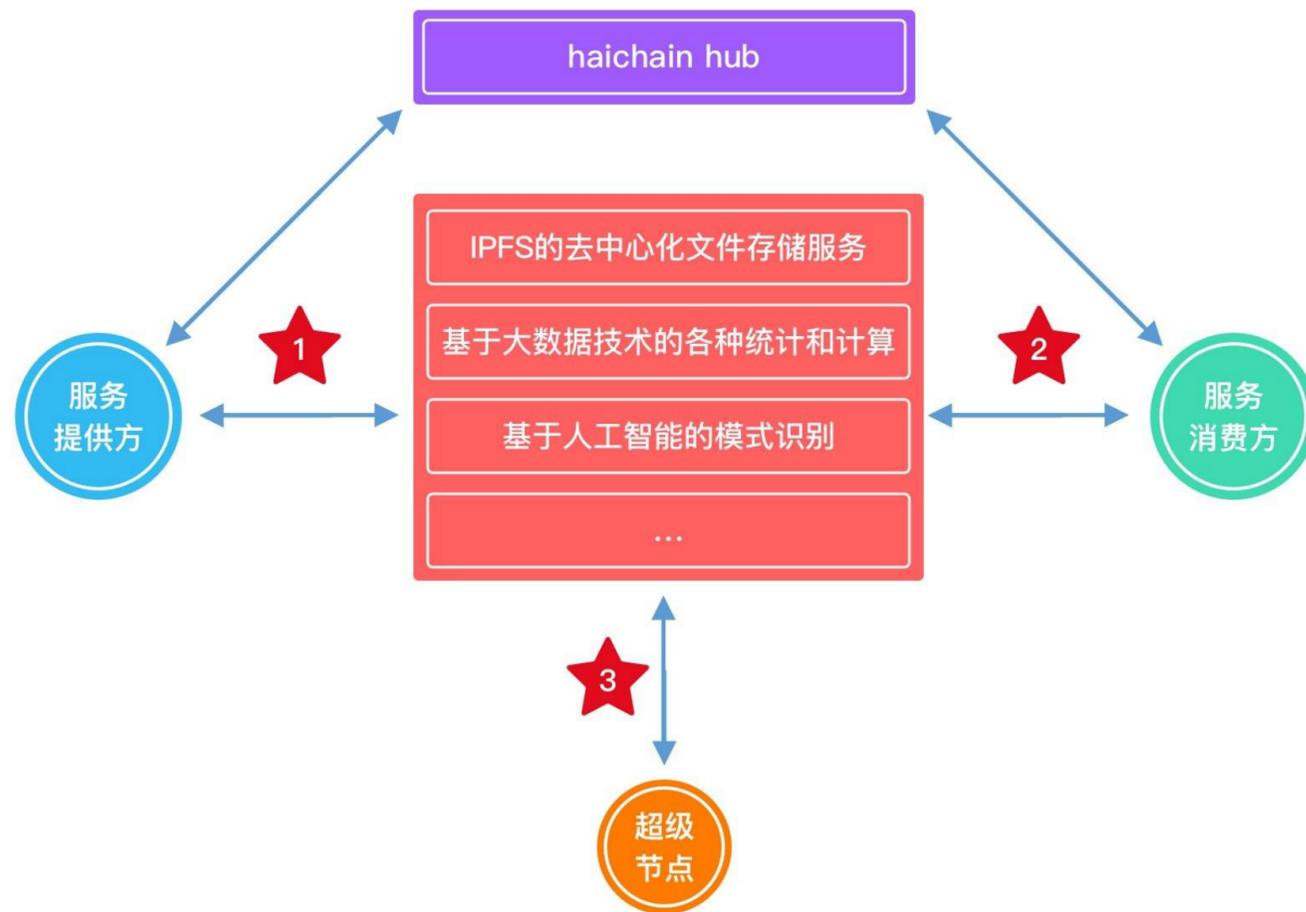
5.所有交易均在超级节点上执行, 因此超级节点拥有记账权, 可以获得交易费

补充:交易的跨链

上述的交易模型和相关智能合约均支持跨链交易 跨链交易主要是采用的cosmos的跨链协

- 议
- 关于跨链的实现, 在后面的技术实现中详细介绍
-

## 2.7 通用服务模型



在产业互联网的系统模型中，区块链不能解决所有的问题，需要各种链下的服务去完成相应的业务逻辑。

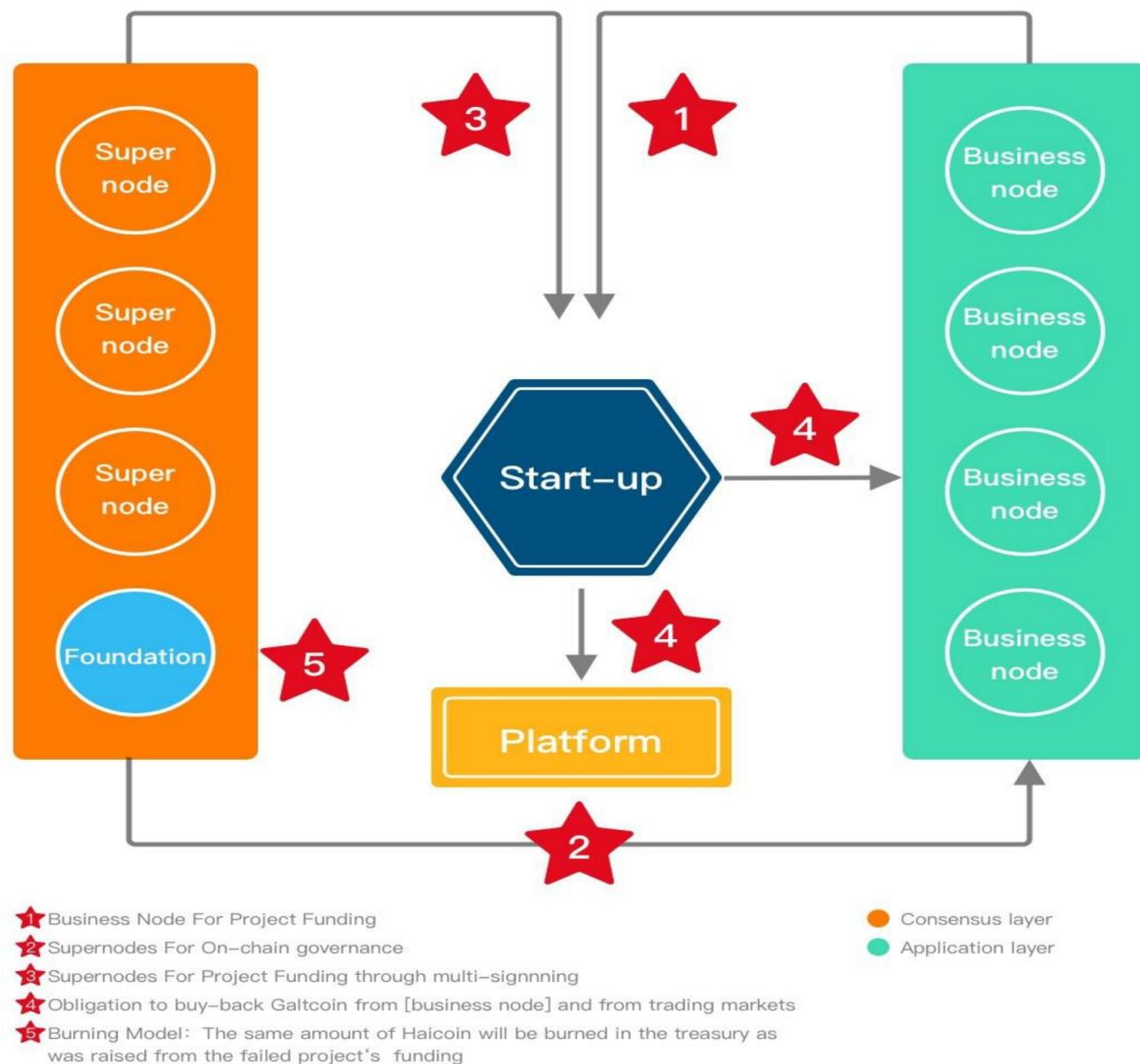
包括人工智能，大数据在内的各种链下服务是Haichain系统的重要补充，同时各种链下服务通过Haichain实现其价值计量和变现。

通用模型的实现步骤如下：

1. 服务提供方提供链下的服务，并且通过Haichain Hub对服务进行标价。默认支持Haicoín和Galtcoin的计价方式。
2. 各种经过认证的服务，需要部署到超级节点上，超级节点将会审核和监督服务的执行，同时获得一点的管理费用。
3. 服务消费者对消费的服务支付费用。默认通过Haicoín或者Galtcoin支付。

## 2.8 系统模型的应用

Haicoín&Galtcoin Use Case



左图是系统模型具体应用的例子，过程如下：

- 1.[业务节点]为[项目方]提供投资,[项目方]通过[资产发布合约]把资产发布到Haichain上。
- 2.超级节点，审核和确定资产的发布情况并且通过[资产激励合约]由投票决定，给投资人的奖励。
3. 该投资地址为多签地址，根据时间周期，按照一定的规则给[项目方]拨款，并且根据[资产锁定]合约，对项目的资产做监督和管理
4. 项目方按照提交的PB合约模板，回购从【业务节点】和【平台】Galtcoin。并且通过[通证交易合约]完成资产的流通
- 5.如果项目失败，[HaiDAO]根据[资产销毁h合约]负责销毁[项目方]已经获得的融资的等价值Haicoín

## 2.9 小结

6大系统模型，主要通过智能合约模板库实现，跨链交易部分通过cosmos的底层协议完成。

另外通过长时间的实践，我们发现基于cosmos的基于产业互联网跨链垂直行业的服务和协议，有很大的商业价值，而且能够繁荣cosmos生态。但是，区块链毕竟不能解决所有的问题，很多中心化的服务也必不可少，比如：大数据分析服务，智能匹配等  
因此，我们的在设计架构上，把链上和链下服务做了有机的结合。

NO	模型名称	技术实现方式	说明
1	资产发布	智能合约	实现包括haichain, galt和第三方通证的资产上链, 发布和确权
2	资产锁定	智能合约	实现包括haichain, galt和第三方通证的资产锁定
3	资产销毁	智能合约	实现包括haichain, galt和第三方通证的资产销毁
4	节点激励	智能合约+激励层	对包括超级节点在内的公链贡献者进行奖励
5	通证交易	智能合约+cosmos跨链技术	跟其他公链的token(包括btc,eth和eos等主流数字货币)进行跨链交易, 每个超级节点都可以作为跨链交易的交易所
6	链下通用服务	链下服务	提供包括以下功能的链下服务, 并且通过区块链完成其服务的价值变现 1.IPFS的去中心化文件存储服务 2.基于大数据技术的各种统计和计算 3.人工智能的模式识别 等等

# | 03 | 技术实现

```
Name={styles.container}>  
  
Avatar && (  
  DetailsCardOnHover  
  user={user}  
  delay={CARD_HOVER_DELAY}  
  wrapperClassName={styles.avatarContainer}  
  
  Avatar user={user} />  
  DetailsCardOnHover>
```

```
name={classNames(  
  styles.linkContainer,  
  inline && styles.inlineContainer
```

```
DetailsCardOnHover user={user} delay={CARD_HOVER_DELAY}>  
  link  
  to={{ pathname: buildUserUrl(user) }}  
  className={classNames(styles.name, {  
    [styles.alt]: type === 'alt',  
    [styles.secondaryLink]: !secondaryLink,  
    [styles.inlineLink]: inline,  
  })  
}
```

```
children || user.name}  
link>
```

```
secondaryLink  
  null  
  <a  
    href={secondaryLink.href}  
    className={classNames(styles.name, {  
      [styles.alt]: type === 'alt',
```

```
155 <ul class  
156 </ul class  
157 {this.r  
158 {this.r  
159 {this.r  
160 {this.r  
161 {this.r  
162 {this  
163 {this.r  
164 {this.r  
165 </ul>  
166 </div>  
167 );  
168 }  
169  
170 renderWhatsNewI  
171 return (  
172 <li classNa  
173 <a  
174 href={t  
175 target=  
176 rel="no  
177 >  
178 {title}  
179 </a>  
180 </li>  
181 );  
182 }  
183  
184 renderFooterSub  
185 return (  
186 <div classNa  
187 <Link to=  
188 <Icon  
189 type=  
190 classN  
191 />  
192 </Link>  
193 <span clas  
194 </div>  
195 );
```



## 3.1 公链与技术研发

幸福链社区的技术研发方向基于TaaS(Token as a Service, 通证即服务)的设计理念, 解决数字经济的通证化问题。

通证(Token)的本质就是通过技术进步让每一个人都可以用自己的信用做背书或资产抵押来发行通证, 募集生产资料去创造自己的商业价值。所有的价值, 应该都是基于人和人、人和机器之间形成的共识, 通过算法予以确认。

通证化被定义为三个层次:

(1)

**TokenCurrency**  
(通证代币化能力)

价值上链, 构筑我们在区块链场景中的一般等价物, 能直接通过网络来跨国界、快速、低成本进行资产交易与转移。

(2)

**TokenFinance**  
(通证金融化能力)

构建通证在场景内的流通模式, 借助于Token对现有资源进行重新整合之后, 增加资产的流动性, 达到价值和利润的高效流通。

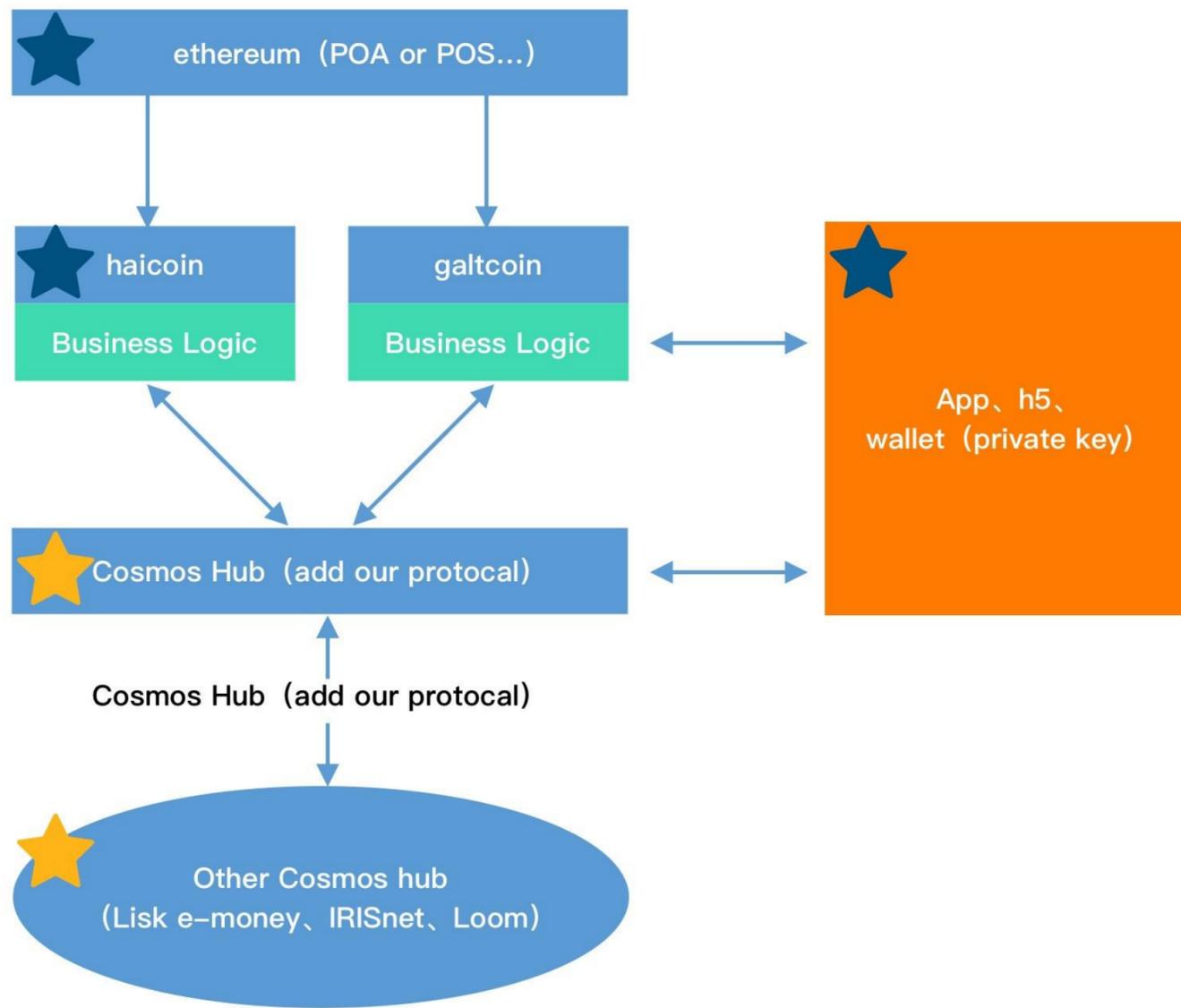
(3)

**TokenAsset**  
(通证资产化能力)

以资本的形态对Token的价值再次升级, 衍生出更为结构化、更新形态的流动形式。

Haichain幸福链区块链设计上强化对TokenFinance和TokenAsset的支持, 作为整个生态下的基础服务资源, 形成一个完整的多链并行的应用和服务平台, 解决各类“资产上链”、“资产流通”面临的各类问题。

### 3.2 整体技术架构图



Haichain 2.0的技术架构兼容以太坊的智能合约和evm虚拟机，并且通过cosmos的底层技术实现跨链通信。

具体的实现如下：

1.集成以太坊的虚拟机，能够完成兼容以太坊的所有智能合约，能够高效地开发出实用，安全的智能合约。应用到系统的业务逻辑层(Business Logic)

2.Haicoins和Galtcoins通过cosmos Hub完成内部和外部公链数据的通信。包括通比特币，以太坊和EOS等主流币的转账，智能合约的执行等操作。

3.另外在应用层，基本不需要更改原有的业务逻辑，就行比较容易的移植到Haichain2.0的公链架构。

### 3.3.1 智能合约

---

Haichain幸福链平台中，将通过一系列的智能合约来将目前中心化商业模式涉及到的利益分配和权益归属相关的问题进行程序自动化执行，这些智能合约由商家和用户的互动行为直接触发，保证公开透明。

#### HaichainCode机制

Haichain幸福链提倡使用简易的智能合约，通过链下的数据和网络输入作为触发条件，完成合约的执行。以太坊中智能合约的编写和执行简单得益于以太坊的合约执行环境 **EVM**，但由于所提出的“代码即合约”的策略，也导致一系列合约安全性问题。在Haichain幸福链也采用虚拟机机制，但是整个合约是被运行在独立于主链运行生态外的虚拟机体系内，主要作用是缩减因合约解析而带来的时间消耗成本以及链上规则安全性问题。

#### 智能合约审计

Haichain幸福链中包含对智能合约的自动化审计以及形式化验证的保护性机制，这样可以降低上传的智能合约出现代码逻辑漏洞的概率，减少用户的损失，加强系统的可用性。

#### 异构智能合约

Haichain幸福链可以使用异构智能合约。不同的节点将采用逻辑相同但是编写语言不同的智能合约，在这些智能合约中，对于相同的输入将得到相同的输出，攻击者要想完成对智能合约的攻击，必须找到所有智能合约的漏洞，完成对所有智能合约的攻击。

#### 采用**Affordances**范式设计的全新合约语言

为了更好的解决智能合约的安全性问题，Haichain幸福链将采用一种全新的强类型的、使用了**Afforances**范式设计的新语言。**Afforances**范式可以给基于区块链的合约提供额外的安全性。

### 3.3.2 交易智能合约引擎库

Haichain zone里面集成有完整的交易智能标准，类似于以太坊的ERC系列标准，Haichain的智能合约引擎库能够做到跨链，计划支持包括以太坊，EOS等主流的智能合约。通过Haichain zone智能合约引擎库，可以使得基于Haichain开发的应用和服务，能够更加的规范，方便和快捷。

同时能够通过合约模板库能够吸引大量的开发者，参与Haichain的应用和开发。这样Haichain的模板库就会成为产业互联网的行业规范和标准，最终提升Haichain的价值。

根据业务的也需要，目前准备集成如下的合约模板库：

- 资产发布引擎库 资产锁定引擎库 资产销毁引擎库
- 资产激励引擎库
- 通证交易引擎库
- 
-

## 3.3 跨链

### 3.3.1 从传统互联系统到区块链智能合约

跟其他业务系统一样，中心化的系统到了一定的规模，会出现技术上的瓶颈。比如，网络的访问量，系统的安全性，社区的建设和治理等等。

根据不断的探索和研究，我们发现区块链是解决这些问题的最佳方案。我探索使用以太坊的智能合约，把数字内容资产化，通过合约完成交易和资产流通。但是当业务量扩大时，以太坊容易出现网络拥堵，手续费高等问题。

### 3.3.2 从智能合约到跨链服务

幸运的是出现了，cosmos等跨链技术，可以实现[万链互联]。我们现有的系统，如果能使用cosmos跨链协议，那很多问题就迎刃而解了。比如网络拥堵，手续费等，最重要的是能比较容易地跟其他区块链系统实现资产交换和数据的交互。

### 3.3.4 从跨链服务到垂直行业的通用协议

然而，因为cosmos开始发展的初期，而且其本身不会太专注于某个垂直领域，所以还是需要投入比较多开发人力和其他资源。

因此我们一直想把Haichain的设计成从业务中抽象出来的模型，让其具有高通用性，良好的扩展性和容开发性。

### 3.4 跟Cosmos和Tendermint 和其他项目的关系

Cosmos 想要建立“区块链的互联网”。这是由许多被称为分区“Zone”的独立区块链构成的互联网络，每个分区都由经典的拜占庭容错（Byzantine fault-tolerant, BFT）共识协议（如Tendermint）提供支持。

Tendermint提供了一个高性能、一致的、安全的BFT共识引擎，严格的分叉问责保证能够控制作恶者的行为。Tendermint非常适合用于扩展异构区块链，包括公有链以及注重的性能的许可链/联盟链，像Ethermint 就是一次对Ethereum以太坊POS机制的快速实现。使用Tendermint在许可/联盟链域中的成功案例包括Oracle，CITA 和Hyperledger Burrow 等。

Tendermint作为共识协议用于在Cosmos Hub上构建第一个分区。Cosmos Hub可以连接到许多不同类型的分区，并且通过一种相当于区块链之间的虚拟UDP或TCP的IBC协议（Inter-blockchain Communication, IBC）实现跨链通信。通证可以安全地通过Cosmos Hub从一个分区转移到另一个分区，而不需要在分区之间的交易所或受信任的第三方。

Haichain是建立在Cosmos网络之上的，为了避免“重新发明轮子”，我们也会使用Cosmos生态中所有好技术和实现方法，同时会把Haichain的项目开源出来，让其他项目也能使用我们的技术，这也体现了“区块链精神”。

### 3.5 共识机制

---

共识机制是区块链系统的根本，业界在共识机制上做了大量的讨论和实践，由最初Bitcoin的POW(Proof of Work)，到后面的POA(Proof of Authority)、POS(Proof of Stake)、DPOS(Delegated Proof of Stake)、PBFT (Practical Byzantine Fault Tolerance) 以及基于信任网络的Obelisk算法等等，其本质都是解决分布式系统中如何通过算法保证一致性问题。

不同的共识算法有不同的适应场景，Haichain作为一个产业区块链平台和并行的多链体系，共识是可扩展的：

Haichain幸福链主链使用高效和安全的改良DPOS+PBFT共识算法。

Haichain幸福链上的各个子链，可以由客户在子链发行时由发行方自行设定共识模式、节点支持等参数，并记录到子链的创世区块中，以满足客户实际应用场景的需要。

### 3.6.1 超级节点

---

在DPOS共识算法中，区块链的正常运转依赖于见证人(Delegates)，见证人是由全网节点投票产生的，见证人也是记账节点的实际控制人，也即是Haichain的超级节点。

见证人在完成打包交易的同时可以领取区块奖励和交易的手续费，并且可以执行社区投票的提案，所以DPOS共识算法不仅仅是算法，而是一个包含了协作治理关系的共识机制。

DPOS是通过被社区推选出来的可信账户（又被称之为“受托人”）来创建区块。其特点是出块时间短，效率较高，几乎不会分叉。

网络中所有持有代币的用户通过投票选举的方式，推选出153个可信账户来替他们做决策，并充当的是区块生产者的角色。获票数最多的前51位自动当选。

被选中的超级节点将为Haichain网路提供算力和带宽支持，他们的主要任务就是收集交易信息将其打包进区块，并将区块广播给其他节点，通过验证后再将区块上传至区块链，获得相应的奖励。当一个排名前51的节点超过24小时没有产生任何区块，那么它将被移出超级节点的名单。

### 3.6.2 超级节点的贡献度计算

超级节点为平台源源不断提供计算、带宽、存储底层资源，对平台上的内容和服务起着至关重要的作用，平台会拿出较大的比例投入到超级节点的贡献奖励

要运行超级节点，系统需对设备配置并进行监测，达到准入门槛并抵押一部分通证才能加入资源型节点网络。加入网络的资源节点根据其硬件设备配置的差异，通过 Docker 部署执行不同功能的软件，初期超级节点承担的角色有：

**计算：**承担 CPU 密集型工作，比如音视频文件的转码工作。

**分发式存储：**承担视频、文件、分布式网站的持久化存储和内容分发 CDN 工作。

**网络：**两种类型的超级节点都需要由良好的网络链路质量，系统将通过 ping-pong 操作监测接入点与相邻节点间的数据丢包率和网络延迟，对不合格的节点或上线后超出阈限的将停止资源贡献奖励。

**硬件配置准入：**超级节点需要较高的服务器硬件配置，比如 1T 以上存储空间、较高的 CPU 型号和主频，一定的内存空间、带宽等；重点监测 CPU 能力，若节点附带显卡 GPU 能力则会有更高的得分；重点监测存储的 IOPS。

$$c = \lambda_h * h + \lambda_s * s + \lambda_b * b + \lambda_d * d$$

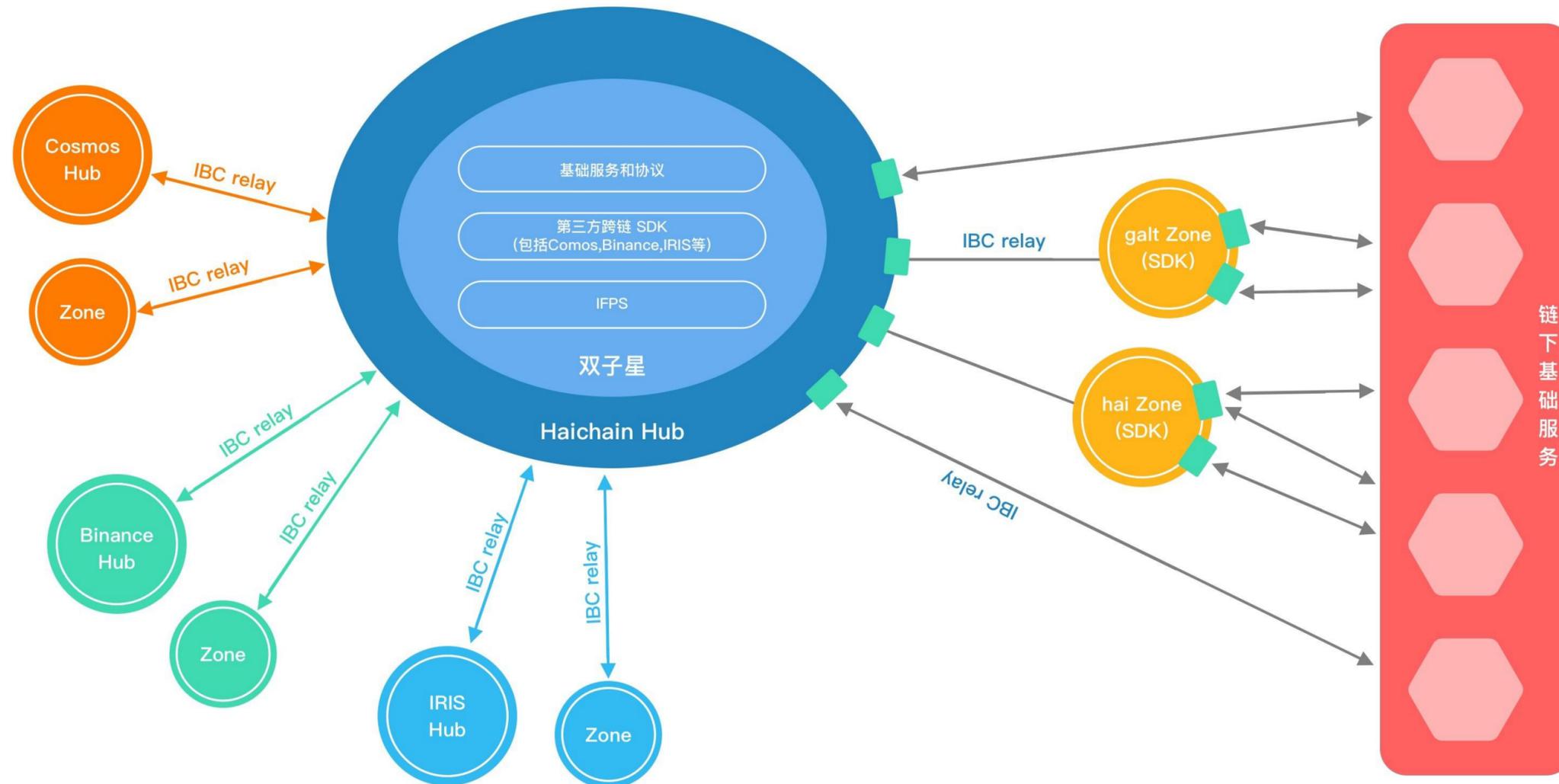
那么，在该数字证明期间，节点 i 能够获得的奖励  $m_i$  就为当前发行总量乘以该节点资源贡献度占总体贡献的比例，即：

$$m^i = \frac{m c^i}{\sum_{k=1}^n c^k}$$

### 3.7 网络架构

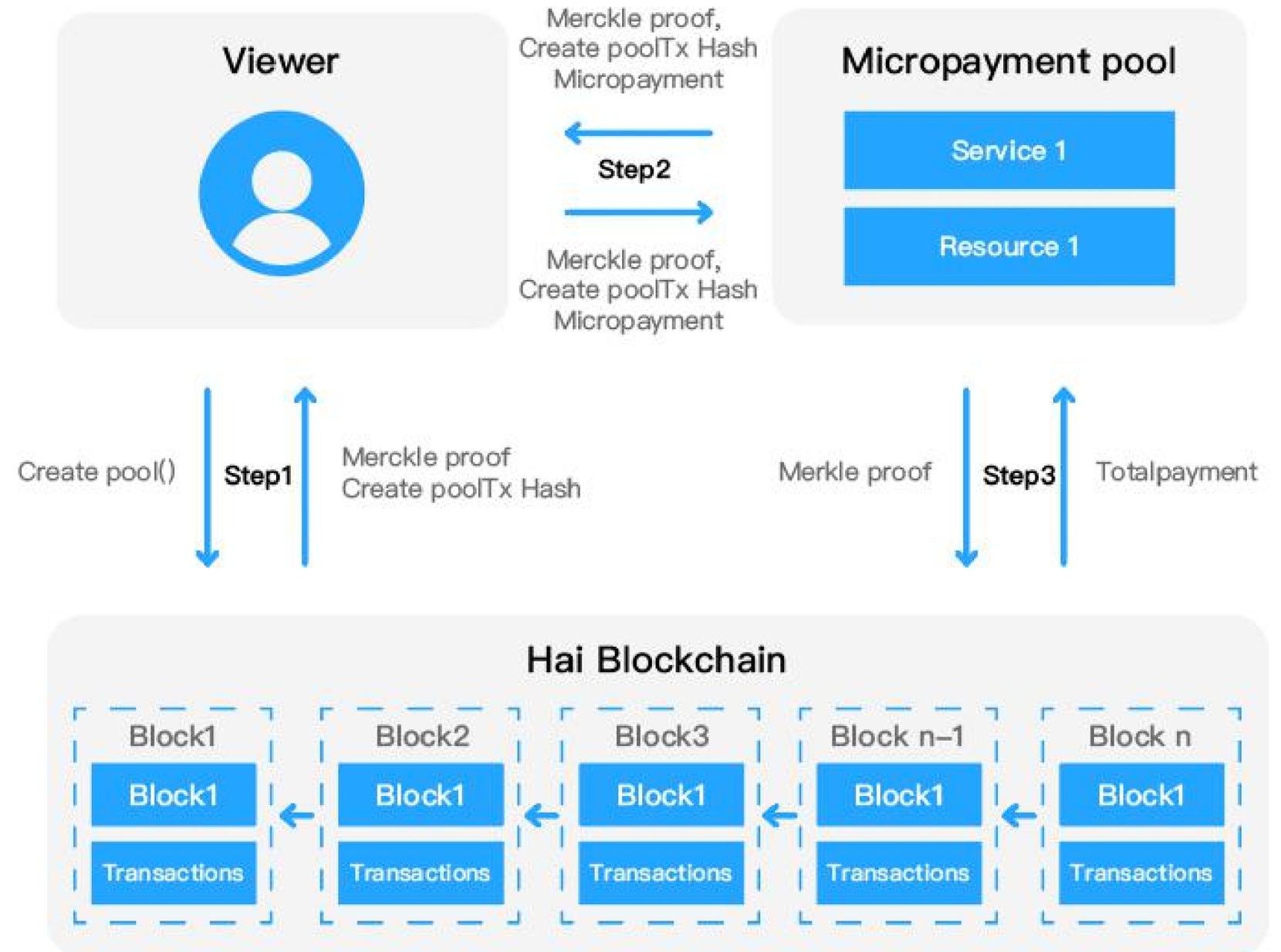
如上图所示，Haichain网络在设计上与Cosmos网络具有相似的拓扑结构。我们计划将[Haichain Hub]作为Cosmos众多分区和区域型Hub之一与Cosmos Hub连接起来。

[Haichain SDK]本身就是计划对Cosmos SDK的扩展，由[Haichain SDK]开发的Haichain全节点旨在提供一个服务的基础设施，并在内部集成了分布式文件系统IPFS（InterPlanetary File System,IPFS），也计划兼容各种其他Cosmos生态的项目(比如:Binance,IRIS等)。



### 3.8 离链微交易池

在真实的互联网应用中，会出现大量的针对同一个资源的重复性交易，比如粉丝经济中对同一个主播重复的打赏、评论、刷礼物等。为满足这个场景的需求，我们将分布式系统的账户数据进行网络切片和交易切片。针对特定资源的海量微小交易将存储在特定的超级节点，交易完成后由这些节点一次性提交到总账本，其结构如下



### 3.9 创新点

Haichain的目标是为了构建去中心化产业互联网生态系统的跨链服务和协议，把现有传统系统改造成去中心化的跨链服务进而成为整个行业的标准协议。

我们的主要工作在于：

1.建立了跨链的系统模型根据我们的业务实践，定制了包括[资产发布，[资产锁定],[资产销毁],[激励]和[通证交易]在内的系统模型，并且将模型跟Cosmos的分区(zone)一一对应，这样可以使不同的公链处理不同的业务内容。因此把有相同业务逻辑放在一个zone(公链)上能够方便开发，让zone（公链)能够处理自己擅长的事情，把自己能力范围以外的事情，放到别的zone去处理，这是我们设计模型的根本出发点。

2.链上和链下相结合区块链有其不可被替代的作用，同时现阶段也不能用区块链解决所有问题，特别是有些业务逻辑已经有比较成熟的解决方案和实现代码，协同链上的处理与链下的业务逻辑的执行能够提高工作效率，降低开发成本。具体实现方式请参考[链下基础服务设计]。

3.定制化的跨链协议对于跨链通信，Cosmos IBC(链间通信协议:Inter-Blockchain Communication Protocol)定义了一个协议用于将价值从一条链上的某个帐户转移到另一条链上的某个帐户的协议。业务需求的特殊性，扩充了IBC协议，以允许利用IBC协议完成具体的业务逻辑。我们认为这种能力在构建可扩展的业务应用程序时非常重要。

4.兼容性的思考我们的垂直行业(数字内容)的服务和协议，因此必须考虑到跟各种公链的兼容性。虽然cosmos使得跨链的交互变动更加容易，但是需要复杂的业务和各种公链的结合，需要有很多工作需要完成。

5.一站式服务我们还会开发方便易用的SDK和各种小工具和模板库，让用户(包括企业用户)能够很方便的使用Haichain，让他们只关注业务本身而不需要关注太多底层技术的实现。

## 3.10 可扩展性

Haichain的扩展性，主要体现在以下几个方面:

### 1. 组件化结构:

采用全组件化结构设计，每个组件都被独立地实现，并通过标准接口联系在一起。每个功能组件在功能上独立，同时可根据用户需求灵活配置、组合，实现平滑升级扩容，功能实体可使业务和开发人员根据具体使用要求增加或减少系统应用模块。

### 2. 分层架构设计:

采用横向分层和纵向分割架构设计。将层与层之间相互分离，每层的应用和服务，采用独立的模块开发和部署，模块间交互标准化，新增功能模块分解到各层，以插件形式加入原系统，既不影响整体架构，也不影响本层功能提供，具备高模块化设计，保证了系统功能的可扩展性。

### 3. 部署和升级的扩展性:

系统采用的软件开发技术都属于开源系统项目，软件系统可运行于通用的主流硬件平台上，不依赖于特定的、专用的硬件设备或者系统软件。

### 4. 区块链应用（状态）与底层进行了分离:

核心代码涵盖了可重用可配置的共识和网络层功能，同时它还定义了一组 **ABCI(区块链应用接口:Application BlockChain Interface)** 回调接口与应用层进行交互，应用逻辑可以用你熟悉的任何语言来写。

## 3.11 去中心化

Haichain的去中心化商业模式，主要是通过以下的几方面来保证。

### 1.共识机制:

Haichain底层的共识机制(DPOS+PBFT)保证了系统是去中心化的，DPOS的保证所有的决策来自于超级节点参与进行投票，各个超级节点都独立的节点，不存在唯一的中心。PBFT是一种状态机制副本复制算法，即服务作为状态机进行建模。状态及在分布式系统不同节点进行副本复制。这样就算某些节点出现问题，只要不超过1/3的节点。就能保证系统正常运行。

### 2.激励机制:

传统我们靠中心化的体系来赋予我们个人激励的动力，但是显然存在两个问题:频次不够，奖金没有增值功能。现在在通证机制下，只要个人对社区产生贡献，就可以给与通证激励，在这种机制下，激励的频次提升，通证还有升值潜力。特别是Haichain的双币机制，每个Haicoine能够定期产生Galtcoin。

### 3.数据和信息存储:

分布式的账本解决了数据和信息账本的去中心化，IPFS (InterPlanetary File System,星际文件系统)解决了文档信息存储的去中心化，这些技术保证了Haichain的数据不是存在在一个中心，而是各个服务器上。既保证了数据的安全性，又保证了中心化节点无法篡改系统数据。

## 3.12 安全性

Haichain在系统的安全性方面做了以下这几方面的工作，来为其商业模式能够正常实行提供有效保障。 1.信息加密

信息的加密是区块链的关键环节，主要是哈希函数和非对称加密两部分的算法。其中，非对称加密部分使用私钥证明节点所有权，通过数字签名实现；使用哈希散列（hash）算法，把任意长度的输入变换成固定长度的由字母和数字组成的输出，具有不可逆性，实现不可篡改。

### 2.P2P网络

全节点与内网的出块节点同步后，组成一个全节点网络，通过 P2P 端口为外提供区块同步功能。我们需要对外界 TCP 流量进行合理分流，对被攻击的机器进行有效隔离，避免影响其他节点同步。

### 3.安全审计 3.1)超级节点

超级节点与其他节点在内网直连，管理员可以通过堡垒机（security administration 模块）连接，除此无其它对外暴露的通信接口。此节点存放着节点私钥，所以所有操作都需要安全审计，并且私钥会由 key admin 定期维护更新。

### 3.2)智能合约

智能合约本质是一段运行在区块链网络中的代码，它完成用户所赋予的业务逻辑。但我们也知道，只要是由人编写的程序，就一定会出现错误和缺陷。如果智能合约存在安全漏洞问题，攻击者就可以通过发布包含恶意代码的“智能合约”，经过一系列操作，控制区块链网络中的所有节点，进而对项目造成毁灭性打击。因此，Haichain在智能合约上线之前，对其进行全面深入的代码安全审计，尽可能的消除漏洞，降低安全风险。

# | 04 | 案例介绍



# 4.1

## 经济生态扩展计划

### 4.1.1 商品和服务扩大承兑场景

为Galtcoin长期发展商品承兑场景是一项重要的使命。传统互联网以单一吸引流量的方式增加用户使用APP的粘度，而Galtcoin仅仅给可以溯源的真实商品提供价值流动，社区HaiDAO管理团队优先的任务是寻找原创、优质、真实的商品加入我们的Galtcoin承兑体系，让持有者可以享受到这个体系带来的便利。

### 4.1.2 去中心化电子商城与社交

过去，传统互联网发展带来社会繁荣的同时，也让世人看到了互联网大型企业是如何垄断社交、通讯、搜索、电商、支付、大数据以及社会生活的各个方面。互联网急剧发展的同时，也使得互联网用户生活在一个完全没有隐私和真正价值分享的世界中。幸福链将从去中心化商城与社交软件入手，将互联网平台还与社会每一个参与者

幸福链的商城和社交平台将没有侵权式的大数据收集，没有中心化的支付交割系统，不会存在账期延长的情况，无论作为商家与消费者而言，这都是一项福利。社交软件方面，在可以实现原有互联网社交软件的功能与效率的同时，我们会实现更为重要的隐私保护；这一愿景并非需要来自HaiDAO或技术团队的承诺，这就是区块链技术的真正进步，使社交真正实现隐私保护而无需任何中心化机构的承诺。



## 4.2 应用体验馆及共享办公

---

幸福链将在多个城市建成Haicoín和Galtcoin的应用场景体验馆。体验馆将主要用于体验区块链科技与应用场景，以及去中心化价值流动的实际场景和AI技术的成果展示。

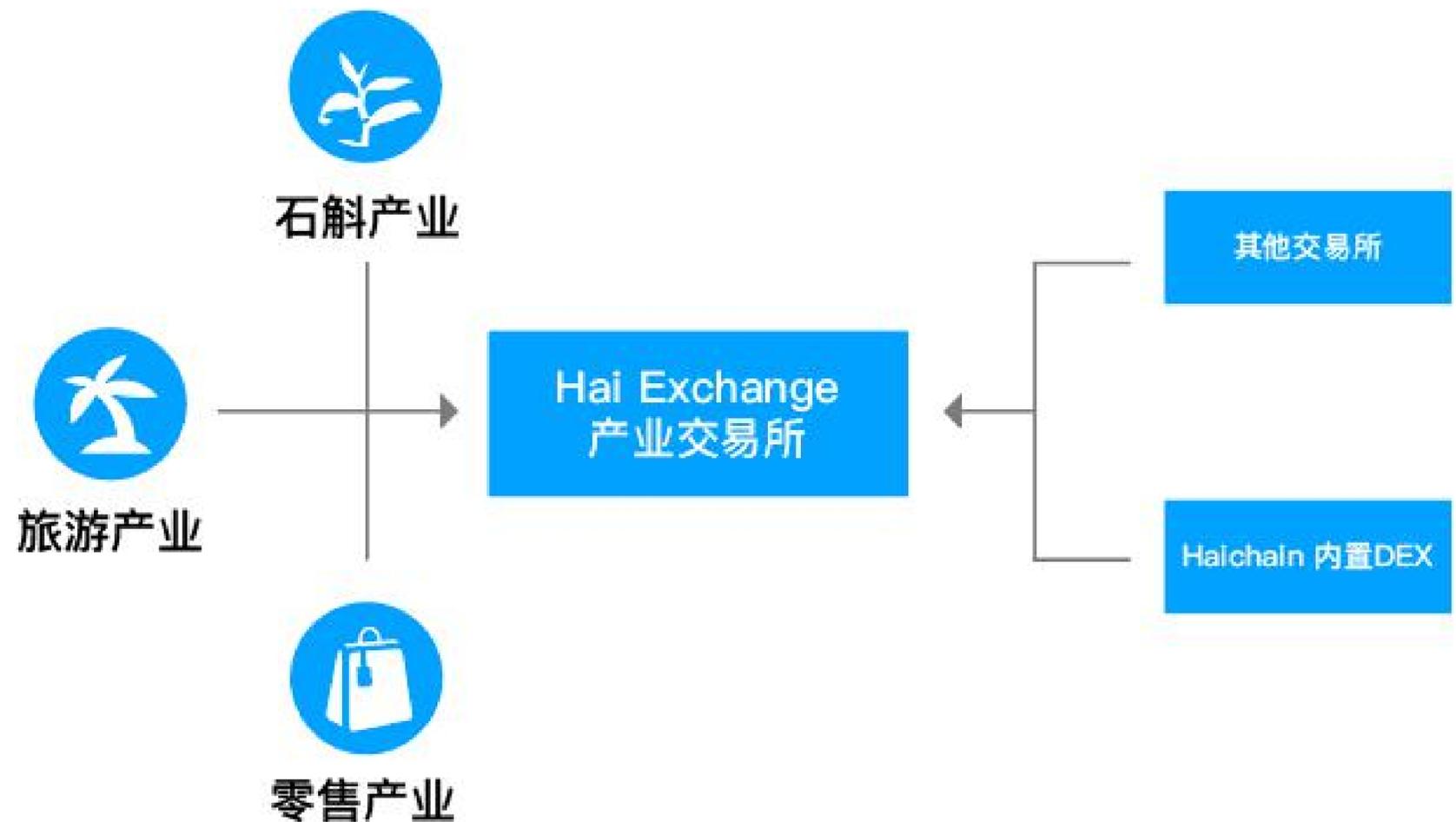
体验馆同时也是去中心化共享办公的场所，这里将进驻参与应用的社区成员的企业；体验馆同时也是项目孵化器驻地，Haichain幸福链自主研发的项目。技术成果作为公开的信息演示给进入体验馆的所有人，体验馆的目标就是让更多的人了解技术和应用如何为生活和价值提供推动力。



### 4.3 Haichain幸福链产业交易所

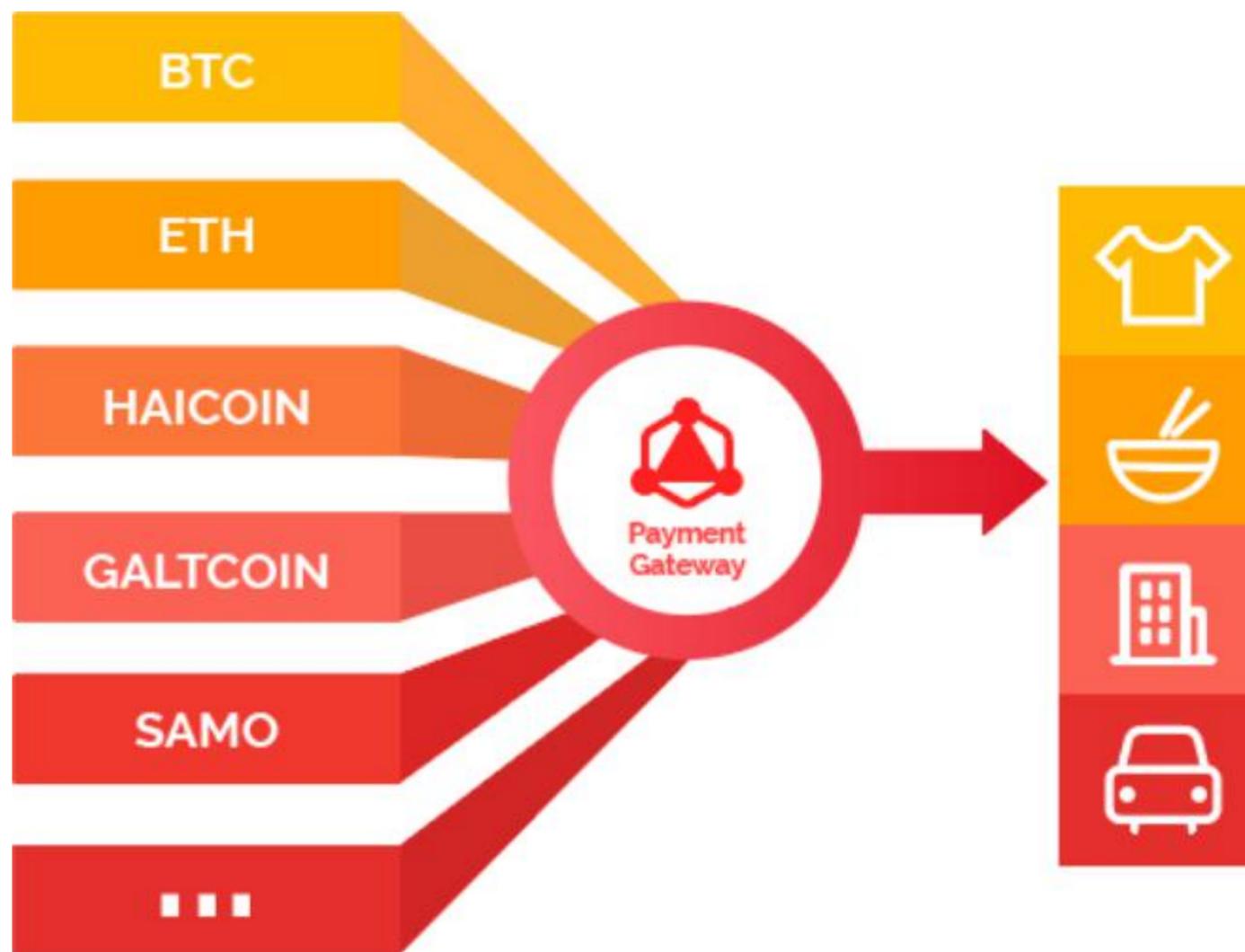
Haichain幸福链的目标是为实际的产业服务，每一个产业都拥有一条独立的链。为了促进资产流通，使中小企业有能力构建自有的生态体系，Haichain幸福链会建设一个分布式的资产流转平台，包括且不限于分布式交易所。

Haichain幸福链和第三方交易所合作，在自己的移动钱包中嵌入交易所功能，同时在Haichain幸福链的公链上将内置分布式交易所功能，促进整个链上资产的流通。



#### 4.4 Haichain幸福链支付网关

在购买和享受虚拟和实际商品服务的过程中，为了最大化客户群，我们将整合主流数字通证和法币成为一个独立的支付网关，让法币用户和数字通证都能无缝的享受整个Haichain幸福链社区的各类服务。



## 4.5 Haichain幸福链隐私保护存储网络

---

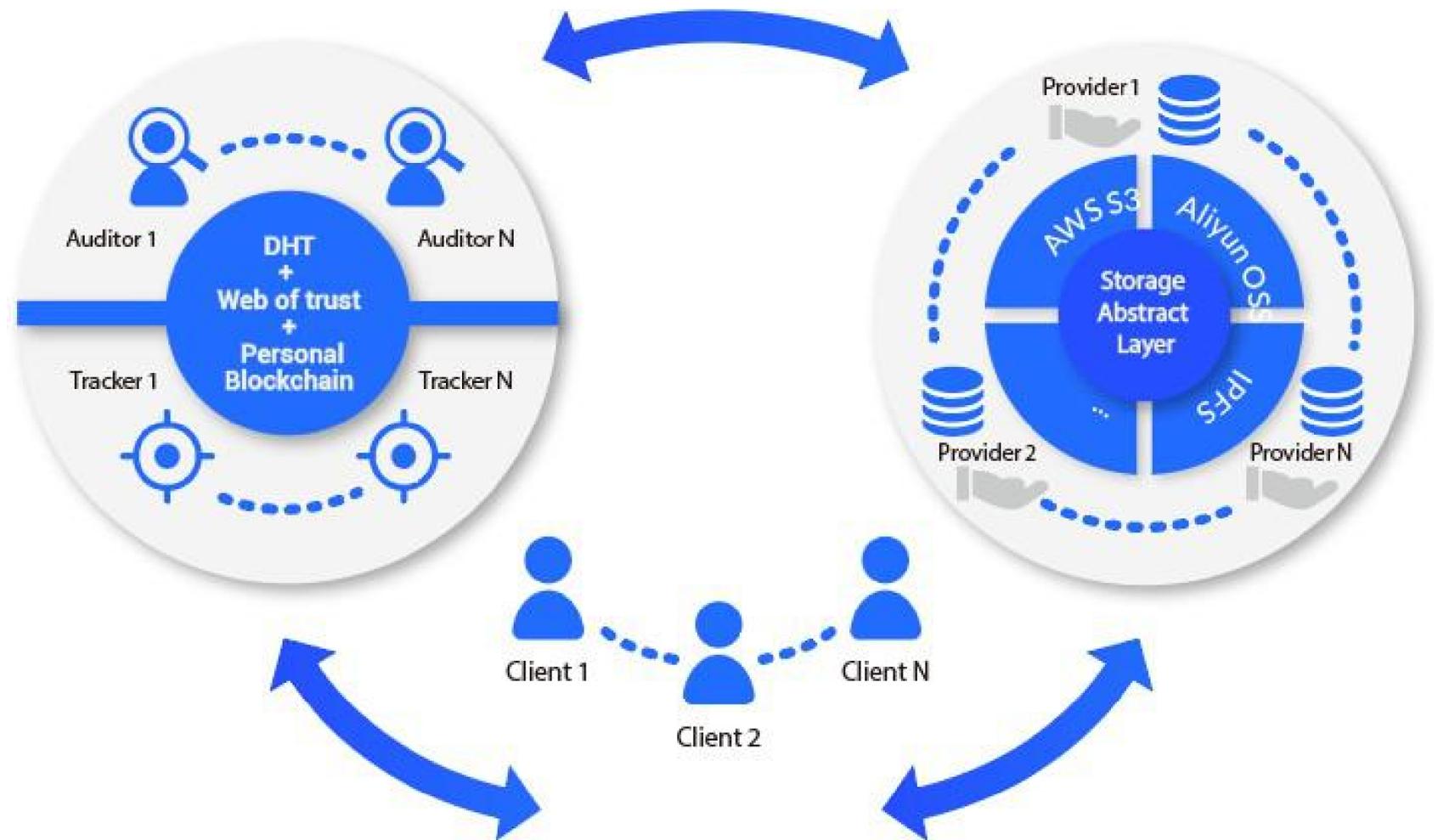
如前文所述，存储是去中心网络底层基础设施之一，为了构建起整个Haichain经济体，最大程度的保护好Haichain经济体里面数字公民的数据安全和隐私保护，需要给整个Haichain经济体产生的各类数据提供一个安全的分布式数据存储网络。

## 4.6.1 安全的数据存储和隐私保护存储网络

为了达到数据安全存储和隐私保护目的，我们采取了以下措施：

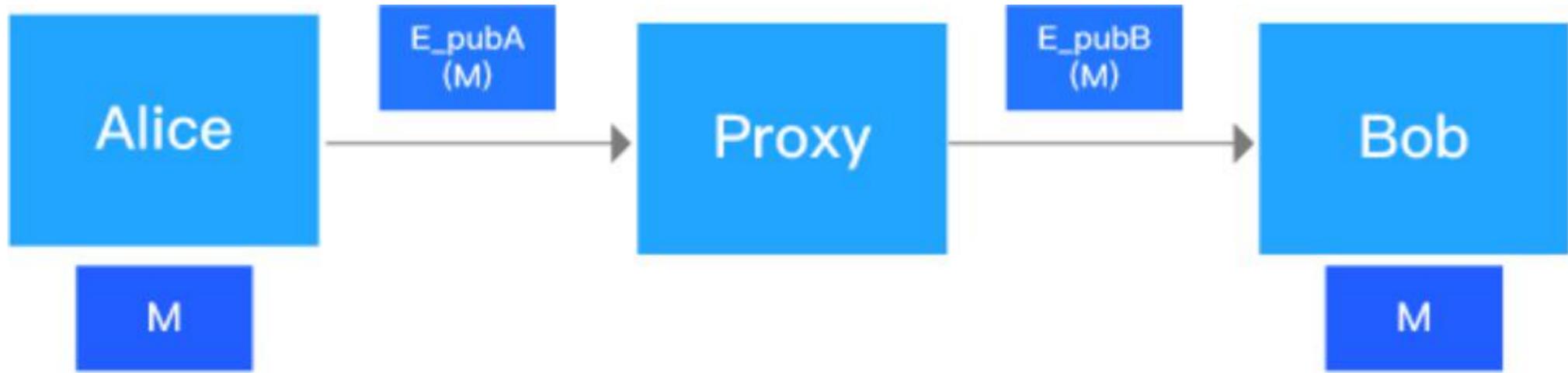
- 所有隐私数据都进行端到端的强加密
- 数据都是分片后加密存储的，任何存储提供方都没有完整的加密数据
- 任何存储提供方都是存储的加密后的数据
- 数据的分享使用代理重加密，杜绝隐私数据泄露
- 存储证明使用基于BLS签名的PDP机制，将烦琐的数据审计任务交由Auditor节点完成

该系统我们已经开发并上线测试运行，其简化逻辑架构如右：



## 4.6.2 基于代理重加密的文件共享

为了解决隐私文件的安全分享问题，我们设计了代理重加密的方式进行加密信息共享：也就是原本我们公钥加密后的密文，只有我们的私钥才能解开，转化为对方私钥也能够解开，这个过程就是代理重加密，其过程概要描述如下：



## DAO社区投票决定新的商业准入



## 4.7 系统模型的应用

DAO(Distributed Autonomous Organization), 翻译成中文的意思是"分布式自治组织"。只要满足分布式、自治的组织都可以被称为DAO。

区块链中的DAO, 简单说就是一个应用程序, 但是它是基于区块链技术实现的应用程序。分布式自治组织和区块链技术没有耦合的关系, 区块链中的分布式自治组织只是基于区块链技术实现。

Haichain的DAO社区投票机制, 主要包括一下几个步骤

- 1.企业根据自身的情况, 向社区递交[商业计划书]。
- 2.社区成员根据[投票]机制, 确定该项目的[风险评级]。
- 3.通过[风险评级]的项目, 社区成员会对该项目进行 [签名验证]
- 4.社区成员会对该项目进行投资, 也即是进入[投注阶段]

## | 05 | 产品生态

为了达成Haichain幸福链经济体系的目标，我们将提供一系列跨终端的应用产品，包括WEB站点、移动终端APP、桌面应用、移动商场、聚合支付、资产流转系统等。

当前产品主要包括以下几个方面：



### 移动钱包

多币种 的移动钱包  
并整合点对点聊天  
资产交易功能



### 移动商场

基于积分兑换的商  
场，用于兑换各类  
积分



### 资产发行和流转

提供Haichain幸福链体系  
下自定义数字资产、实物  
抵押资产的发行、流转功  
能

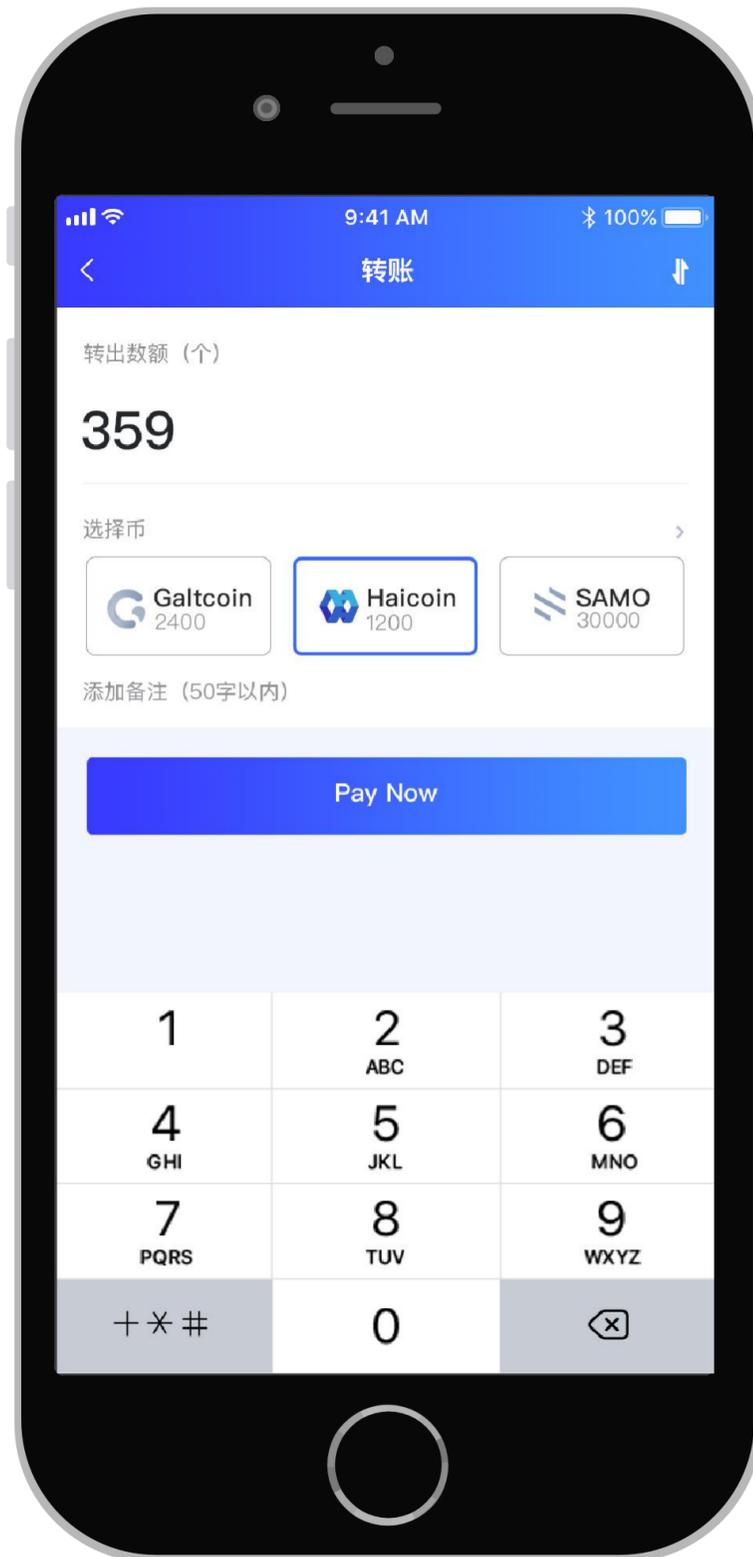
未来我们将根据Haichain幸福链经济体的建设情况，不断的扩大和丰富产品体系，全面满足作为Haichain幸福链体系下数字公民的需求。



## 5.1 移动钱包

---

移动钱包是一个基于通证的类似支付宝和微信的平台，可以同时支持Galtcoin，Haicoín，Skycoin和Samos等多个币种。在移动钱包里面，未来会整合聊天、个人转账、群红包等功能。



”

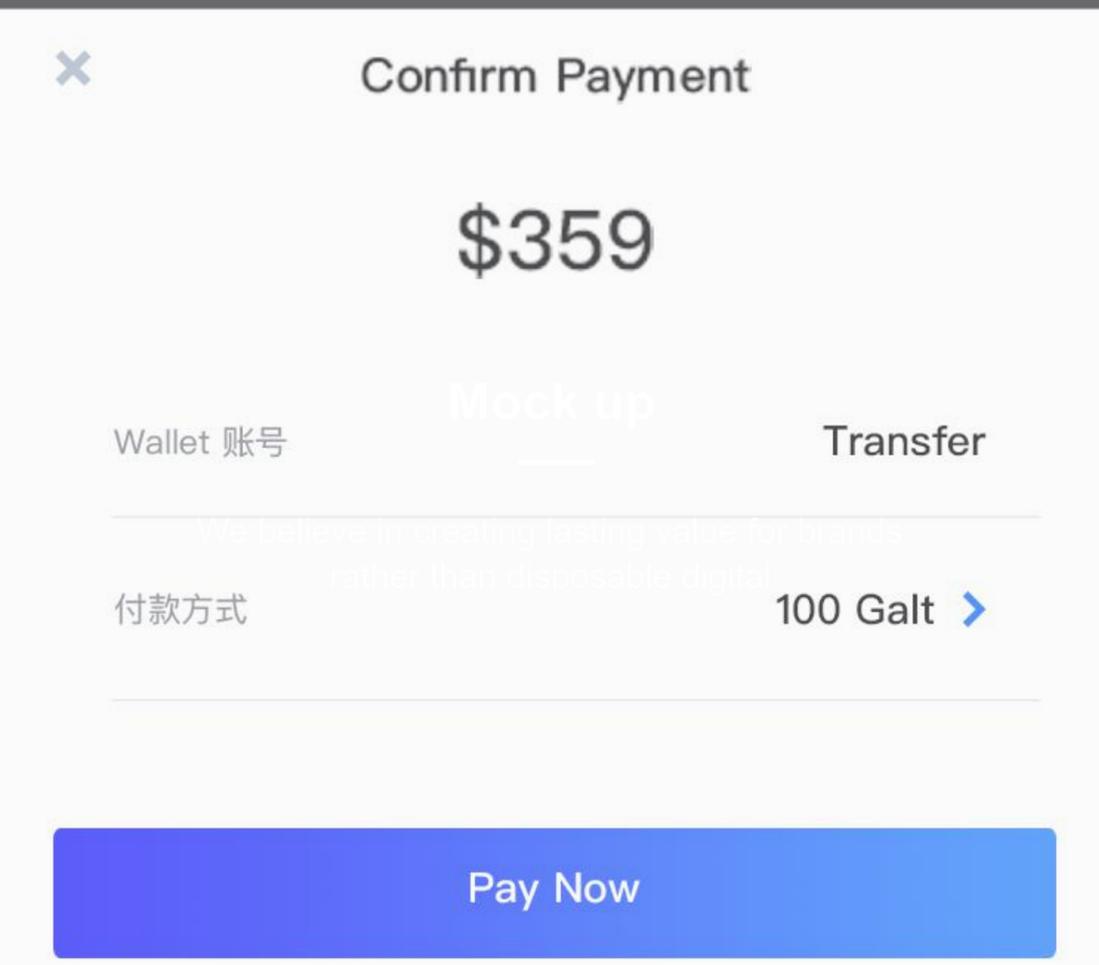
移动钱包是一个基于通证的类似支付宝和微信的平台，可以同时支持Galtcoin, Haicoín, Skycoin和Samos等多个币种。在移动钱包里面，未来会整合聊天、个人转账、群红包等功能。



## 5.2 移动商场

Haichain幸福链的移动商城，是基于区块链的新一代去中心电商平台，为基于Haichain幸福链的商业结构专属打造。

基于区块链和去中心化技术将商场本来的主人还给用户本身，结合大数据，分享经济，社区运营，以线下实体店为依托，消费者、商场用户、数字通证人群组成一个共同体，让区块链技术真正落地应用。

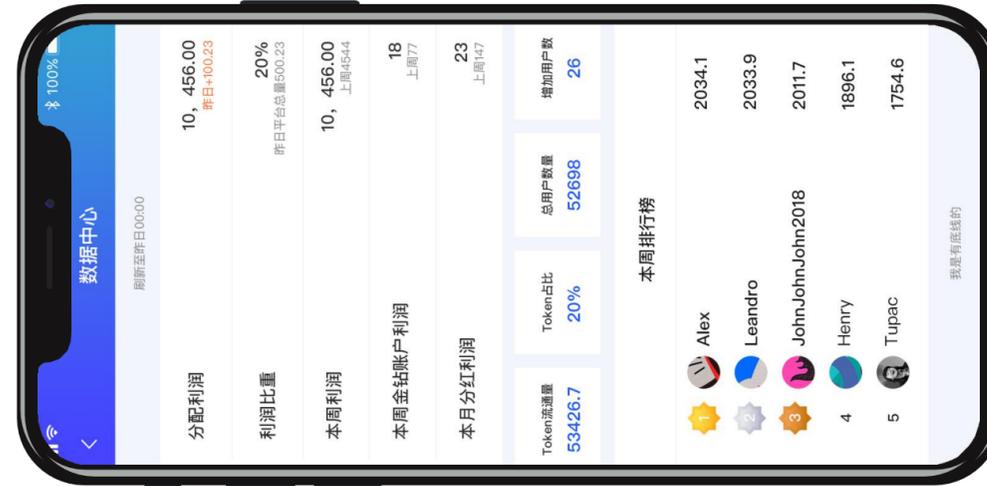


## 5.2.2 卖家中心

卖家中心表示的是商场里面的商家，里面有商品管理订单管理，资产管理等，所有功能非常简洁，用手机即可以完成全部操作。

## 5.2.3 数据中心

数据中心让每一个用户对商场经营了如指掌，每日利润，分配利润，贡献排行，总用户量等全部显示，实现去中心化管理，没有暗箱操作。



## 5.3 资产发行和流转

让企业和普通用户可以通过简单的配置即可发布自己的数字资产，资产可以进入Hai Exchange进行自由流转：



## 5.4 产品生态一览



已经接入生态的企业有包括共享打印，农业，生物科技，旅游业以及百余种商品。目前，我们的产品除了代币之外还有，具有红包功能的畅聊，自动售卖系统，OTC交易系统，拍卖系统，正在开发众筹系统，Hai商城，游戏软件等

和10家企业合作，其中初始项目方和投资方在南宁结合的项目有30多种产品，目前还结合有万印宝的共享打印，黄山多维农业，生物科技，灵山果园民宿，还有百余种商品。

## | 06 | 展望

我们使用Haicoin和Galtcoin为基础来建设“区块链+”产业互联网，针对这个数字化的产业经济体，我们提出了如下的产业经济学愿景。



## 6.1 Haichain幸福链产业经济体愿景

---

纵观历史发展，科技进步让人类社会不断向前发展，也让更多的人享受到了更优质的生活，在这个进程中，经济框架也在不断随之发生变化，促进资源不断突破旧的桎梏，形成了更加有效的配置，经济不断得到进一步的发展。资本、人力、技术，这是影响经济长期发展的三大要素，然而归根到底是人和资源这两大基本要素在驱动经济的发展。过往经济制度的变化就是不断激发人的创造力和优化组织结构、更加有效利用和各类资源的过程。

对于Haichain幸福链来说，我们认为当前经济正处于一个新的变化节点，经济正朝着更加网络化和数字化的方向演变，而我们的传统经济体制仍步履蹒跚，依然有诸多不公开、不透明、不有效的因素在制约经济更快的发展。Haichain幸福链希望利用新一代区块链技术，创造出一种适应数字化社会的新型产业经济体系，进一步优化经济资源的配置方式，打破当前阻碍经济要素最优化配置的障碍，从而激发经济进一步增长的活力，也让经济体内的分配更加公平。

在Haichain幸福链产业经济体内部，资源配置能够以点对点的形式进行高效运作，这种去中心化的经济架构能够避免中介机构形成垄断，从而避免对上下游的消费者进行价值剥削。我们相信最好的产业经济体制应该能够回馈真正对经济发展做出贡献的参与者：包括投资者、商家、技术提供方、消费者等等。

## 6.2.1 提升产业经济配置效率

---

产业经济体的核心在于经济资源的有效配置。产业经济资源的高效配置包括更灵敏的价格体系、更快的需求响应、更低的流通成本、更充分的竞争、更低的信用成本等等。**Haichain**幸福链将利用区块链技术配合大数据、人工智能来构建纯数字的产业经济体。

## 6.2.2 数据驱动

---

我们认为数据将是新经济时代——也就是数字化时代最根本的基础资源，如同石油资源之于当前世界经济的地位一样。未来的科技提升将极大的依赖于数据本身的发展。因此在**Haichain**幸福链经济体系中，我们格外重视数据资源的积累，尤其是特质数据的积累。我们将在**Haichain**幸福链经济网络中设置数据奖励机制，同时致力于提升经济体的**数据密度比**，即数据总量/经济总量。我们认为，更多更优质的数据资源将成为未来经济体快速扩张和解决人力资源成本的一个关键因素。大量的数据使得我们能够运用最好的**AI**技术去学习重复性活动，从而能够低成本、快速、大量的复制经济活动节点，为**Haichain**幸福链的经济网络的扩张带来充分的动能。而数据的积累也将为资源的最优配置提供科学的决策依据。

## 6.2.3 数据共享

---

对于网络中至关重要的数据资源，我们认为整个网络的基础设施，也是经济网络效率提升、降低信任成本的关键。为了实现真正的数据驱动经济体，在**Haichain**幸福链网络中，所有公开活动产生的数据、网络运行的基础数据，都会进行签名存储、开放共享。

## 6.2.4 公开透明

---

对于任何一个经济体来说，资源有效配置的一个关键在于信息的公开透明。相比传统经济体中由于信息的不对称导致的资源浪费、分配不公、权利寻租等问题，使用新型技术的**Haichain**幸福链数据驱动经济体将进行自动统计，无需传统的国家统计局进行采集和编制，从而实现宏观经济体的透明公开。

除了整个经济体运行状况的公开透明外，**Haichain**幸福链网络将对具有系统重要性的服务机构进行自动的定期审计信息披露，杜绝数据造假可能性，降低**Haichain**幸福链经济网络中的信任成本。



### 6.3.1 打破粘性价格

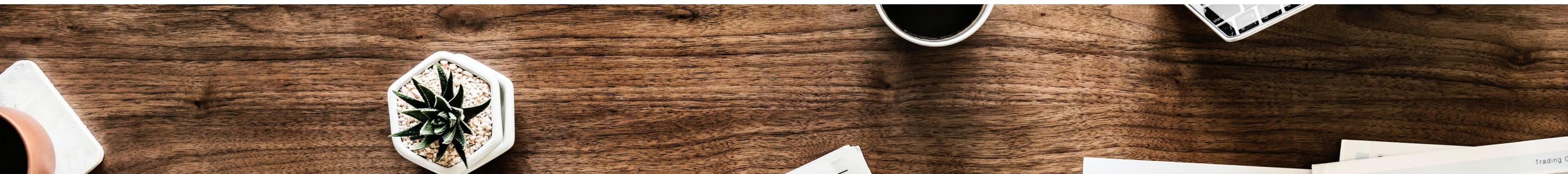
---

传统经济网络中存在摩擦，价格变动往往滞后于经济变动，从而不能实现整个网络中的最优资源配置。在Haichain幸福链网络中，数字化、数据化的经济网络模式使信息能够最快速的传达到网络中的每个节点，而数字化、社区化的管理方式将使得价格灵活调整的成本足够低，从而不会产生粘性价格的问题。

### 6.3.2 打破信息不对称

---

在中心化的经济结构中，中心信息机构占据信息优势，从而能够实现对上下游机构的价值压榨。在Haichain幸福链网络中，信息公开透明、无法篡改，不存在由信息不对称带来的价值挤占甚至欺诈行为。



# 6.4

## 金融效率

### 6.4.1 资产流动性

Haichain幸福链经济网络的财富将以通证的形式进行分配，而通证资产的流动性对于经济网络的效率至关重要。为了提升通证的流动性，我们将作出以下安排：

- OTC场外交易，做市商激励机制。
- 上交易所，设定算法交易激励机制
- 提供多个网络服务市场，提供服务撮合交易。
- 拓展各类应用场景，扩展通证的使用范围。

### 6.4.2 资产市场深度

Haichain幸福链经济网络的资产深度最终将由整个经济体的实际经济活动深度作为支撑。Haichain幸福链网络将会提供移动钱包、移动商城、聚合支付等一系列真实经济活动必须的基础技术设施，并通过网络激励的方式鼓励大家来共建基础设施，Haichain幸福链的合作伙伴会把相应的业务活动在Haichain幸福链网络中进行开展。

Haichain幸福链网络对个人隐私和安全进行极大强化，作为网络服务提供方也无法窥探用户真实数据，无法进行数据伪造和注入，会吸引全球真正对个人隐私和安全关注的用户。



## 6.5 社区效率

---

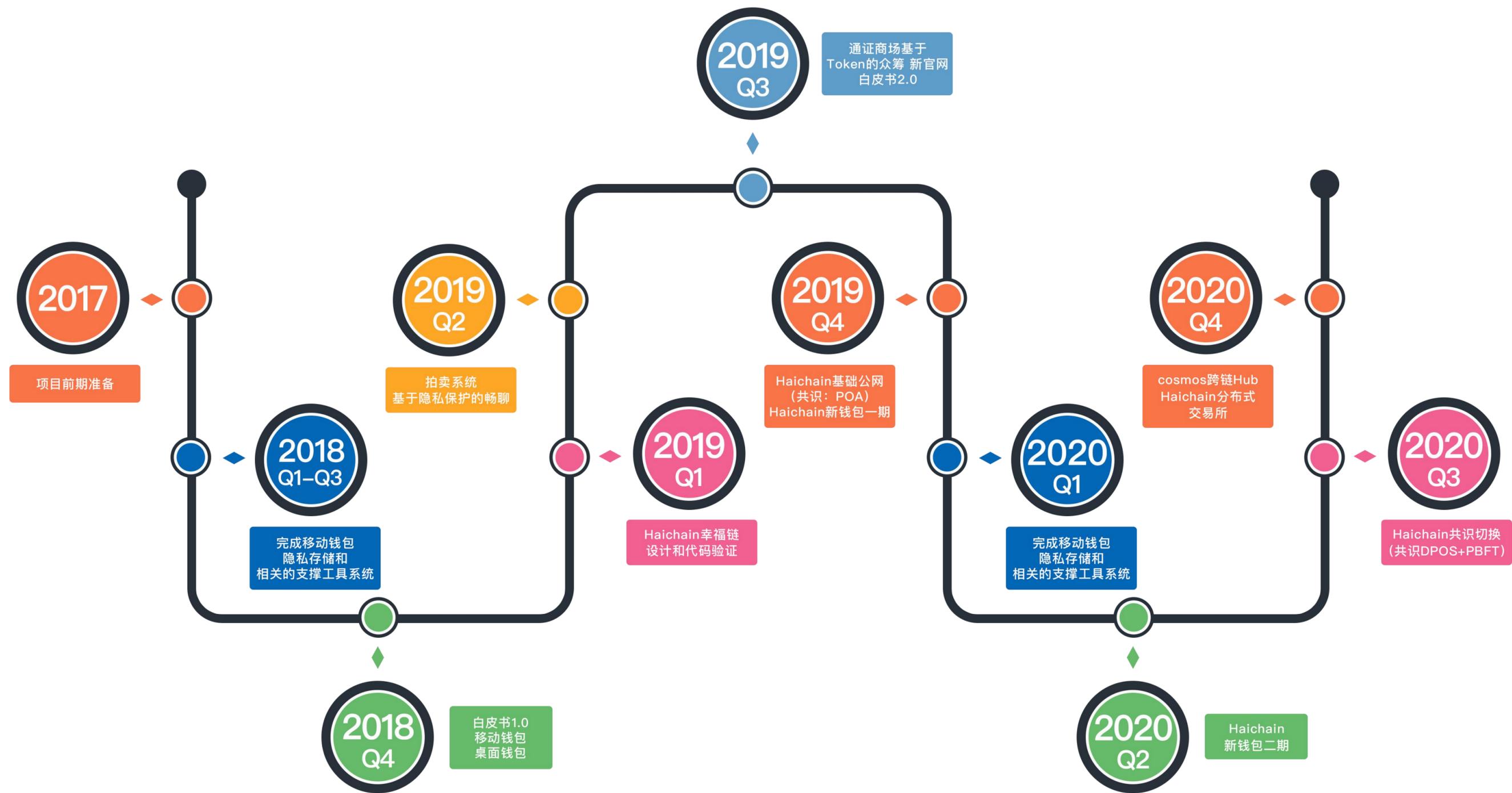
Haichain幸福链认为应对竞争最好的方式就是竞争本身。在数字经济体的世界，未来将会有多种另类币。另类币长期最大的风险之一就是被其他性能更优的另类币打败。因此，我们将激励重点放在提升Haichain幸福链性能和网络效率的关键算法上。我们鼓励最优秀的算法工程师为Haichain幸福链提供服务，我们将会设置开放透明的竞争系统，让算法工程师享受到最大的利益。

从短期来看，在技术差别不大的情况下，各类另类币之间的竞争凸显于使用基数上。由此，在短期竞争中我们将激励基于真实应用场景、能够获取更多用户的真实应用。



# | 07 | 开发计划

Haichain幸福链已经完成了大量的前期技术准备和开发工作，在未来重点完成公链、分布式电商平台、隐私保护网络的建设等。



## | 08 | 初始团队和主要节点



HaiDAO

# | 09 | 初始团队和主要节点

技术支持



Haichain 开发团队



C2CX开发团队

# | 10 | 风险与免责

## 10.1 风险提示

为了达到数据安全存储和隐私保护目的，我们采取了以下措施：

- 政策与监管风险

区块链项目以及数字资产交易领域目前尚未有非常明确的政策监管,全球范围内各国的政策与监管差异较大。我们相信在不久的未来,全球各国家都会出台明确的针对区块链项目及数字通证资产的监管政策,但不能否认至少在当前,该领域将存在因政策监管原因导致参与者财产损失的可能性。

- 市场风险

目前阶段数字通证存在暴涨暴跌、易受消息影响等情况,若参与者缺乏市场经验,易受到市场不稳定带来的财产损失

- 执行风险

目前阶段数字通证存在暴涨暴跌、易目前全球范围内,区块链创业团队和项目雨后春笋,其中不乏全球巨头的参与,在可见的未来竞争将十分激烈和残酷,故该领域虽然处于刚起步阶段,但依然存在强劲的市场、运营竞争压力。本项目基于区块链技术和密码学,不能完全排除黑客攻击的安全风险。消息影响等情况,若参与者缺乏市场经验,易受到市场不稳定带来的财产损失

# | 10 | 风险与免责

## 10.2 免责声明

本白皮书只用于传达信息之用途,不构成任何投资建议,投资意向或教唆投资。本白皮书不组成也不理解为任何买卖行为,或任何邀请买卖、任何形式证券行为,也不是任何形式上的合约或者承诺。

区块链作为新兴的行业,目前阶段具有极高的投资风险和技术风险。虽然Haichain会尽力去实现本白皮书中所描述的所有目标,但我们无法保障通证Haicoïn和Galtcoin的增值,故所有参与Haichain的人都将自担风险。

参与Haichain项目者,即无条件的认为已经充分仔细阅读了本白皮书,全面认了Haichain的项目规划,技术特征及上述提到的各项风险特征,并已经充分结合自身的风险承受能力,了解并接受该项目风险,并愿意为此承担一切相应结果或后果。

# 11 | 主要参考文档

Bitcoin: <https://bitcoin.org/bitcoin.pdf>

Cosmos: <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md> ZeroCash:  
<http://zerocash-project.org/paper>

Tendermint, <https://tendermint.com/docs/>

Ethereum: <https://github.com/ethereum/wiki/wiki/White-Paper> TheDAO:  
<https://download.slock.it/public/DAO/WhitePaper.pdf>

Segregated Witness: <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>

BitcoinNG: <https://arxiv.org/pdf/1510.02037v2.pdf>

FLP Impossibility: <https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf> PBFT:  
<http://pmg.csail.mit.edu/papers/osdi99.pdf>

Interledger: <https://interledger.org/rfcs/0001-interledger-architecture/>

LibSwift: <http://www.ds.ewi.tudelft.nl/fileadmin/pds/papers/PerformanceAnalysisOfLibswift.pdf>

Thin Client Security: [https://en.bitcoin.it/wiki/Thin\\_Client\\_Security](https://en.bitcoin.it/wiki/Thin_Client_Security)

Ethereum 2.0 Mauve Paper: [http://vitalik.ca/files/mauve\\_paper.html](http://vitalik.ca/files/mauve_paper.html) DLS:  
<http://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf> ABCI:

<https://github.com/tendermint/abci>

Stellar: <https://www.stellar.org/papers/stellar-consensus-protocol.pdf>