超导链（SCT）技术的碰撞

创新性的联盟链与公链的结合

同构多链 . 创造未来

Super Conductor Token

V1.1

1.摘要

超导链致力于解决商户间沟通、协作的问题，具有通用区块链账本功能，基于多链混合共识算法，图灵完备的智能合约体系，基于 solidity 语言，在进行超导链设计时即创新性的提出联盟链与公链的结合。

联盟链易于搭建和接入并且兼具联盟币创建及发放功能，主链支持联盟币和主链币的自由交易，钱包支持一键创建联盟币，并且可以对接交易所。

联盟链作为联盟内部的权益、价值的交换，其具有灵活的联盟权限，高效的运行机制，尊重商户数据权益，保护商户个人隐私。公链则作为我们超导链中各个联盟间的价值与权益交换的核心平台。通过超导公链，用户可以将联盟内 coin 与公链 coin 做出价值兑换，使得在联盟内的收益可以转换为其它价值。

超导链拥有区块链从业多年的技术开发人员，从用户角度出发，满足超导用户的各种场景，不仅在共识，虚拟机，DAPP 等方面有着深度考量与实践，特别在公链与联盟链的交互上深入研究。我们希望超导链不仅可以满足用户的需求，成为金融底层基础设施的技术，同样可以像互联网一样走向大众，服务生

活。

1.技术概述

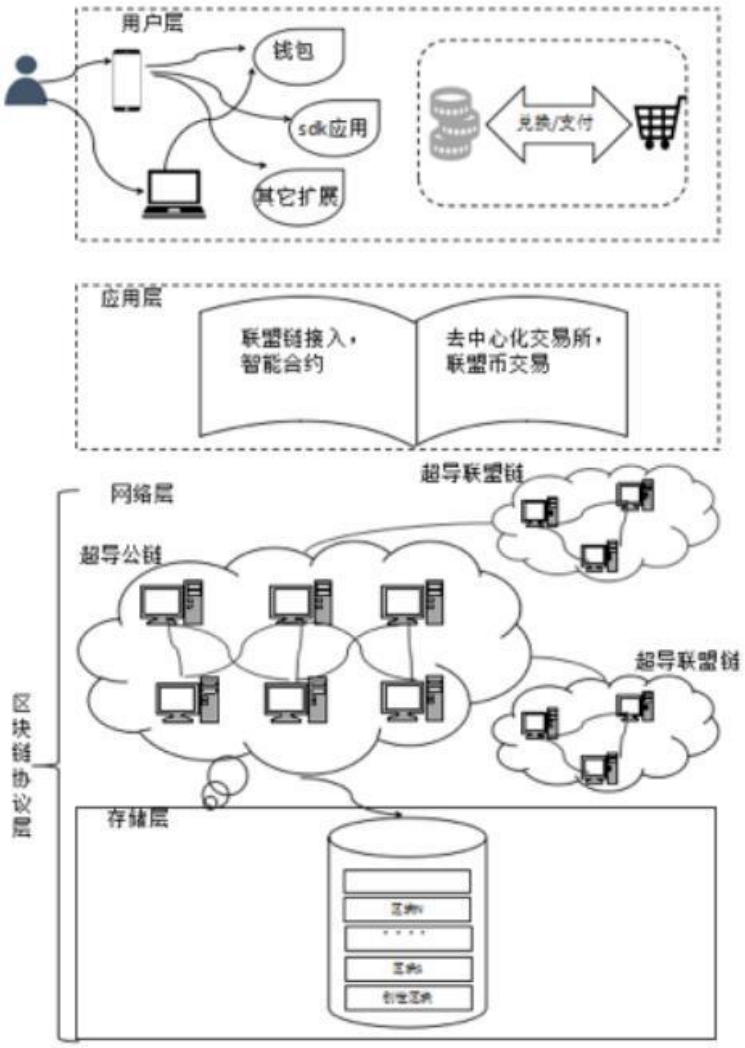
超导链致力于解决商户间沟通，协作问题，在进行超导链设计时即创新性的提出联盟链与公链的结合。联盟链作为联盟内部的权益、价值的交换，其具有灵活的联盟权限，高效的运行机制，尊重商户数据权益，保护商户个人隐私。公链则作为我们超导链中各个联盟间的价值与权益交换的核心平台。通过超导公链，用户可以将联盟内 coin 与公链 coin 做出价值兑换，使得在联盟内的收益可以转换为其它价值。

超导链拥有区块链从业多年的技术开发人员，从用户角度出发，满足超导用户的各种场景，不仅在共识，虚拟机，DAPP 等方面有着深度考量与实践。特别在公链与联盟链的交互上深入研究。我们希望超导链不仅可以满足用户的需求，同样可以在技术上引领时代。

1. 技术架构

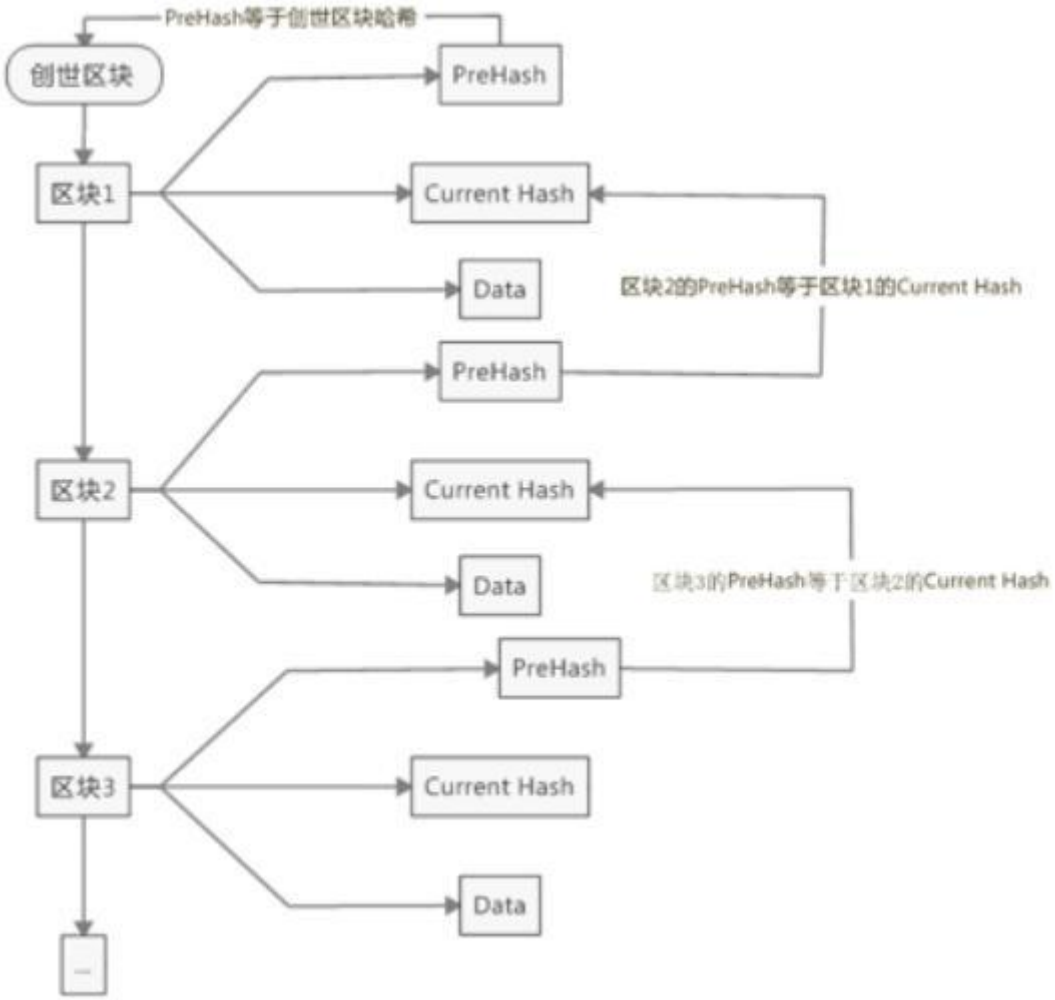
超导根据自身技术经验设计出全新的超导区块链架构，使其在技术底层为用户提供高可靠的存储、交易保障，同时用户提供便捷接入服务。超导链根据实际情况设计超导区块链。

技术架构如下图所示：



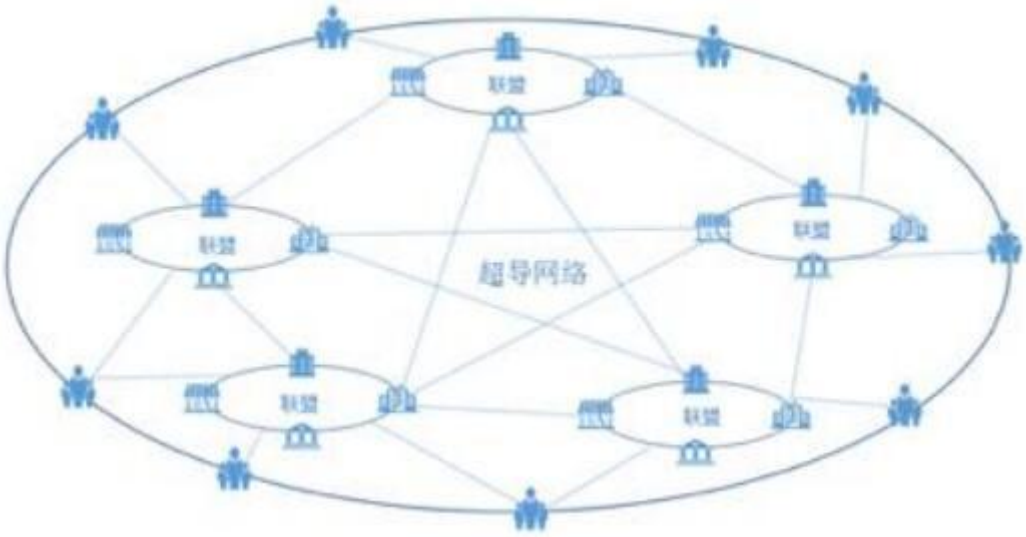
存储层：超导针对存储，提供插件机制，灵活接入多种存储引擎，对于不同的存储场景提供合适的存储机制。保证存储的高效、安全。

超导的区块链存储继续沿用了数据区块化，链式结构，哈希函数，默克尔树的重要特性。



网络层：超导对超导公链与联盟链在网络层进行深度优化。对区块广播， 交易广播，共识交互，公链与联盟链交互进行全新设计。保证网络的快速、稳定。

超导链由公链和联盟链组成，多个联盟链和公链无缝连接。好下图所示：



应用层：超导为用户提供完善的应用生态，方便用户创建超导 DAPP。超导同时内置了去中心化交易所，为超导 Coin 与各联盟 Token 进行便利汇兑。

用户层：超导从用户角度出发，超导钱包为提供公链与各联盟链的便捷接入服务。

2. 账户模型

超导链从技术架构角度划分，将帐户分为公链帐户和联盟链帐户。 超导各个联盟作为超导生态的一部分。为了方便各个联盟与公链的交换。超导为各个联盟链与公链提供统一账户功能，用户在任意一条链中创建用户即在其它联盟链中拥有相同账户。为便于操作，我们对钱包进行了改进，对同一个钱包账户可以公链与联盟链之间切换，方便用户对各链资产进行操作。

超导链公链帐户和联盟链账户的生成都使用了 ECDSA-secp256k1 数字签名算法，EC 是椭圆曲线的简称，椭圆的形状由 secp256k1 参数决定，DSA 是数字签名算法的简称。

超导链的公钥是通过私钥推计算出来的，而超导链帐户可以由公钥经过一系列

哈希和变换，再通过 Base58 编码生成的字符串。

3. 超导链的交易

超导链的交易类型有多种类型，如下图所示：

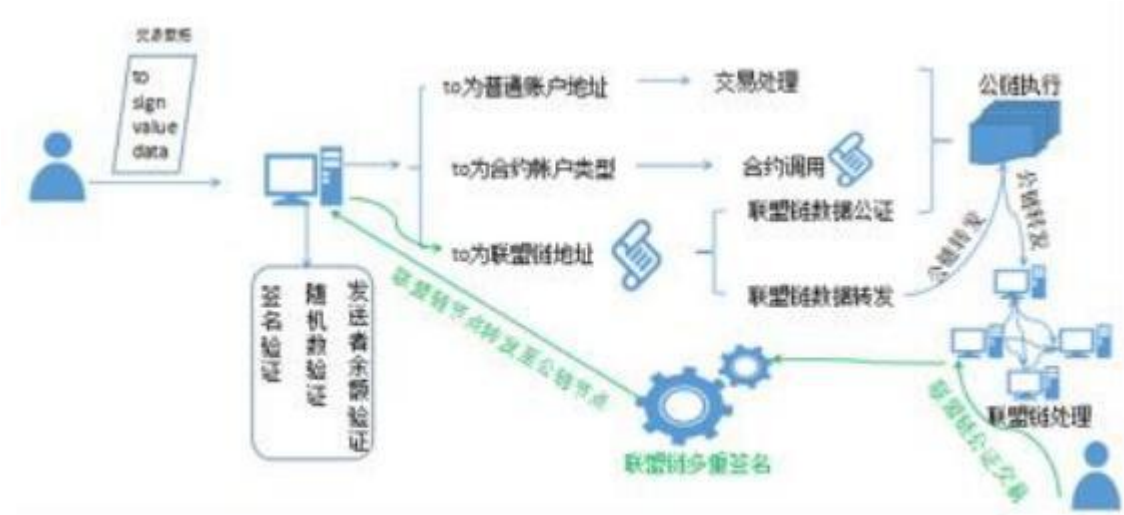
超导链的转帐交易：超导链任意公链节点接受到发送代币转帐交易，即可在公链执行。

超导链合约创建：即向超导链发送新合约，发生时即将合约 Code 发送至任一公链节点，校验无误后即可在公链执行。

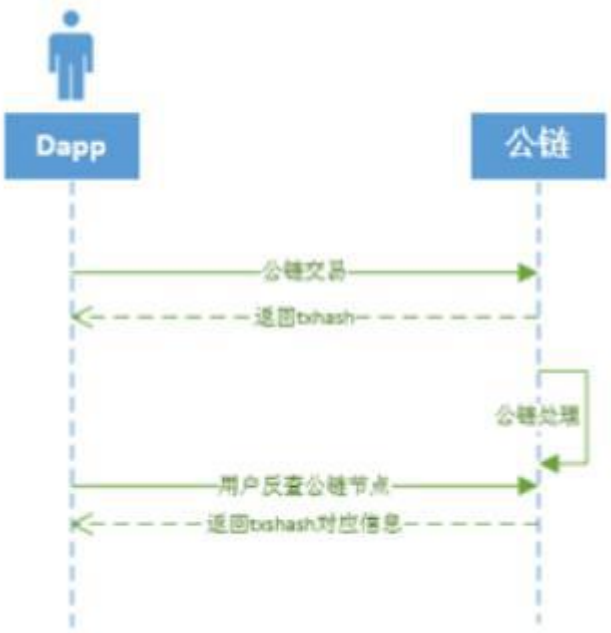
联盟链存证交易：当联盟链内有用户需要将数据转移至公链存证时，可以由用户发起，经联盟链各节点公证后转发至公链节点，并在公链执行。

联盟链内部交易：交易为联盟内运行的交易，该交易只需要在联盟链内部共识即可。

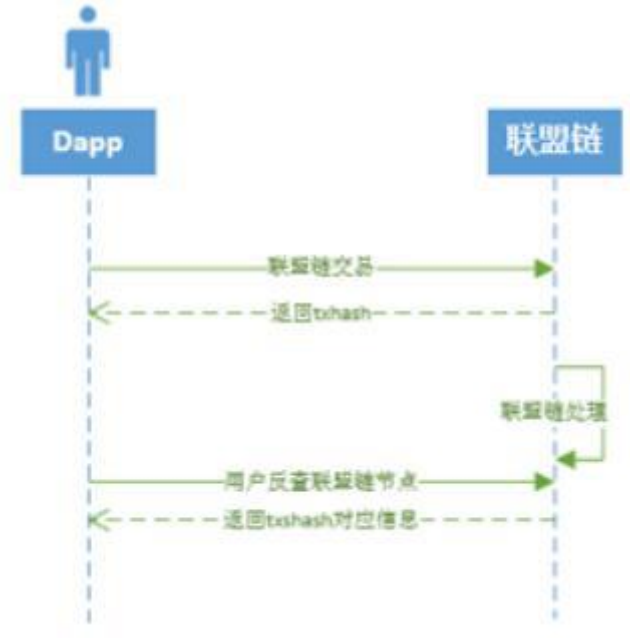
联盟链接入交易：这是一个特殊的交易，交易内附带了联盟链的一些创世块参数信息，会创建联盟链的路由等信息。



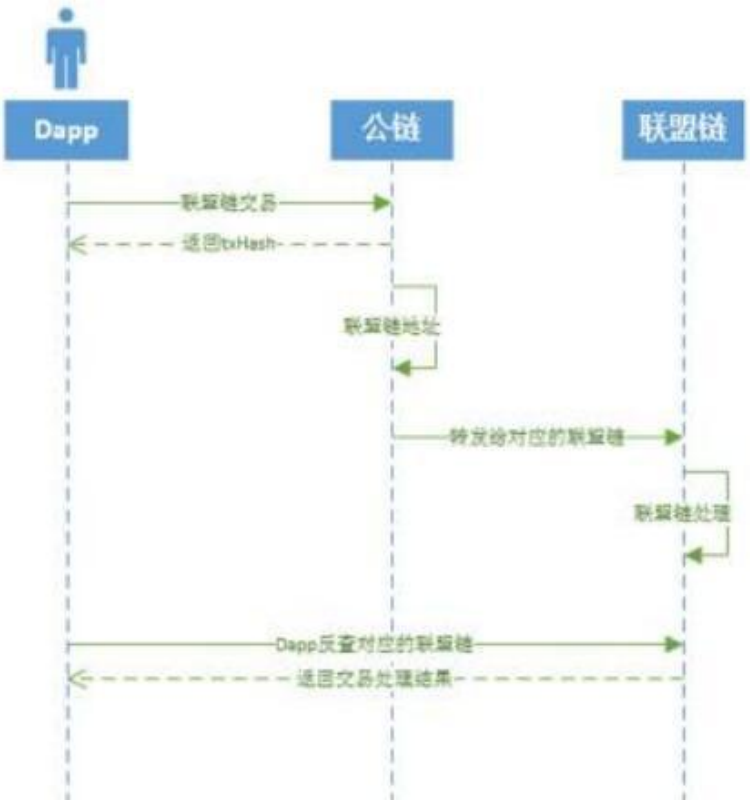
公链交易时序图：用记将交易发送到公链节点，公链返回交易凭据，公链处理完毕后，Dapp 反查公链节点交易处理结果。



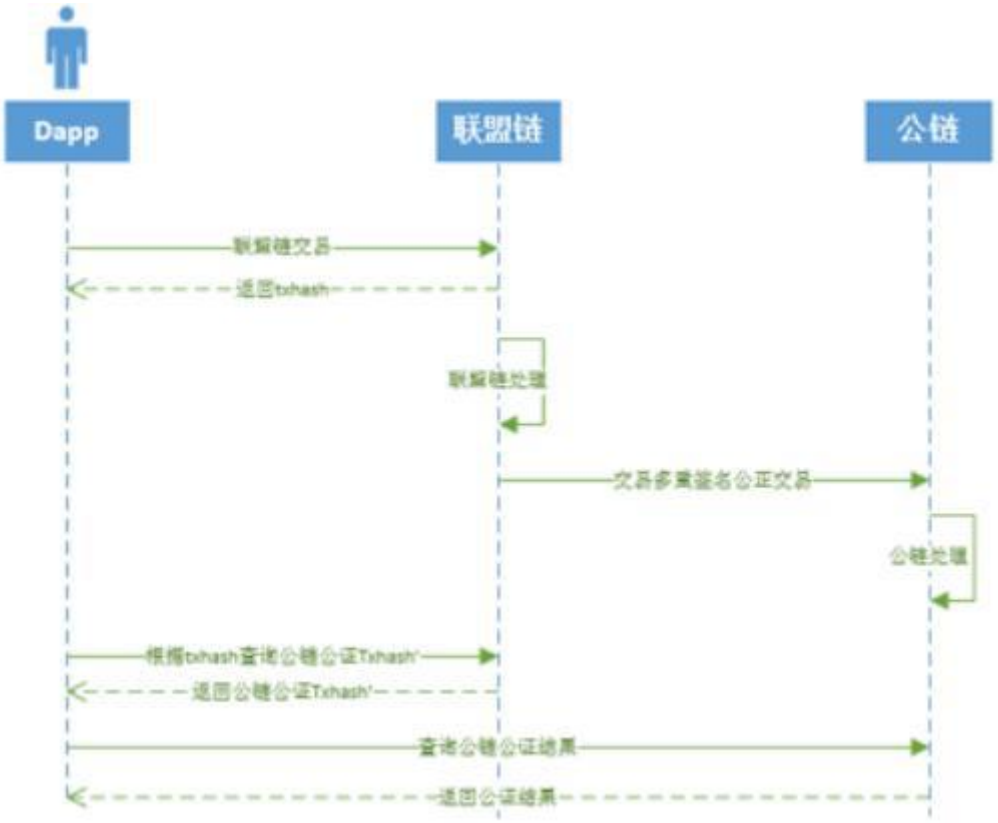
联盟链交易时序图：直接发送交易至联盟链时



联盟链交易发送到公链：当联盟链交易发送至公链时，公链执行转发，联盟链处理交易，结果只能从对应的联盟链反查，或去对应的联盟链浏览器上查询。这样有利于某些环境连接不上联盟链接点时，直接使用公链来广播交易。

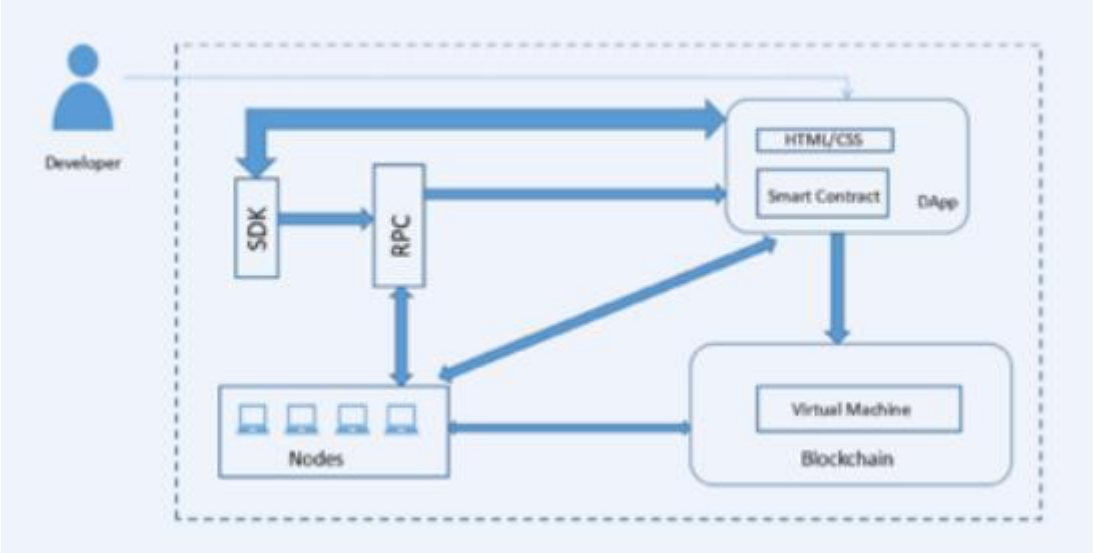


联盟链交易公证：当联盟链有交易请求公链公证时，联盟链先处理请求，然后转发至公链，再经公链公证。



4. 虚拟机与智能合约：

超导作为新一代区块链，同样支持智能合约来丰富我们的超导生态。超导对市面上的合约虚拟机进行研究。发现 Solidity 语言在智能合约领域占有很高的比重。为了便于已有智能合约的移植和使开发人员快速开发。超导同样采用 Solidity 语言来作为我们超导智能合约的开发语言，超导同样把 EVM 移植到我们的超导链里面。但 EVM 在执行效率上相比于传统语言的虚拟机性能存在较大差异。超导开发团队同样在虚拟机领域进行探索，考虑引入 X86 虚拟机与操作系统、硬件结合更为紧密，解决虚拟机性能问题将作为我们后续工作的重要内容。



5. 共识算法：

共识作为区块链的‘灵魂’，不停的有新的算法在创新。超导链同样对共识同样有着深度的研究。不同的共识可以引导社区、引导整个生态的生态模式，创建不同的社区文化。超导追求公平，自由的理念。超导希望利用超导共识解决整个生态价值交换，经济激励的问题。超导链有两类共识组成，公链共识、联盟共识。意在解决商户与用户间的快速价值交换，达到甚至超过传统应用架构的用户体验，同时解决掉联盟间商户的登记，公证，价值转移问题。

超导公链共识兼具普通矿工与持币用户权益，而联盟链侧重快速确认及数学完整性验证，并且有多种联盟链共识算法适应不同应用场景。

2.联盟链与公链资产转移

超导链是联盟链与公链的多链架构，超导技术团队根据超导自身特点，设计出多链资产转移（MCTA)方案。

MCTA 方案中联盟链需要向公链进行资产的质押，该资金用来进行超导 Coin 与联盟 Token 的汇兑。该资金通过 PAPC（公链资产合约）来进行存储。使用该合约进行转移资产时需要联盟链中参与者进行多重签名来解锁里面资产，以保证资产的安全。

针对联盟链中的节点，每个联盟链中共识节点都会拥有其他共识节点的代理签名。利用代理签名拥有很多好处：

1.不可伪造性: 除了原始签名者，只有指定的代理签名者能够代表原始签名者产生有效代理签名。
2.可验证性: 从代理签名中，验证者能够相信原始签名者认同了这份签名消息。
3.不可否认性: 一旦代理签名者代替原始签名者产生了有效的代理签名，他就不能向原始签名者否认他所签的有效代理签名。
4.可区分性:任何人都可区分代理签名和正常的原始签名者的签名。代理签名者的不符合性(proxy signer’s deviation) 代理签名者必须创建一个能检测到是代理签名的有效代理签名。
5.可识别性: 原始签名者能够从代理签名中确定代理签名者的身份。

通过代理签名方案，我们很容易识别出是谁签发的交易，在出现作恶时可以根据此信息进行追溯。

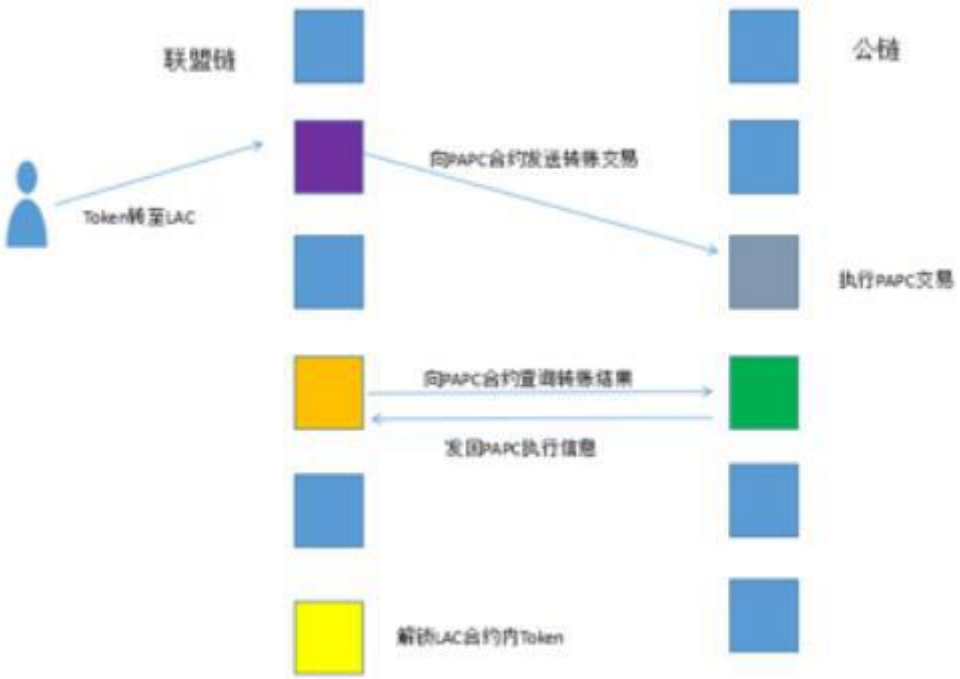
公链与联盟链之间会建立 LPC 双通道，分别作为向联盟链先公链发送转账交易和获取公链转账交易的执行结果。通道完全采用拉取的方式，即联盟链主动向公链进行请求。这种设计主要目的是减少公链网络，性能负但。

联盟链中有 LAC（联盟资产合约），用户希望进行资产汇兑时，需要将联盟 Token 转至此合约内。联盟链内只有通过获取到指定 PAC 转账结果信息才能从 LAC 合约中把用户的 Token 转移出去。

在公链中同样有 PAC（公链资产合约）。用作公链用户向联盟链资产汇兑，进行汇兑前，公链用户需要将公链 Coin 转至此合约内。

联盟 Token 兑换公链 Coin

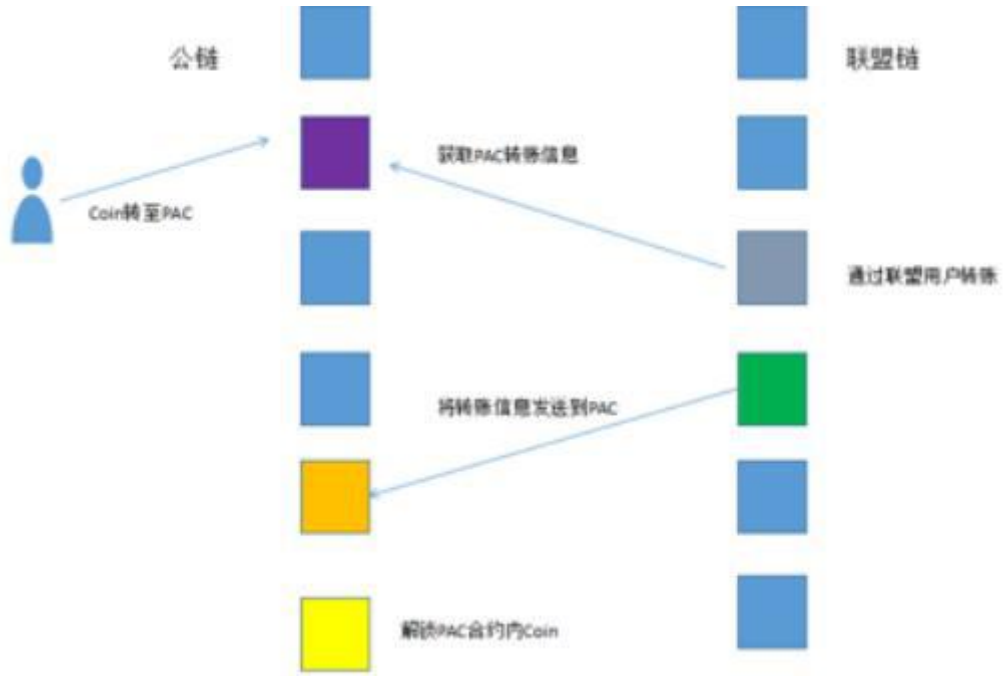
1. 用户向 LAC 合约内转入 Token
2. 联盟平台向公链向 PAPC 合约发起转账请求，请求中包含 LAC 交易 hash, 用户签名和平台签名（代理签名）等信息
3. 公链将从 PAPC 合约内转出 Coin 到指定用户账户
4. 联盟链通过 LPC 通道获取公链交易执行信息。成功后通过交易执行信息对 LAC 内资产进行解锁转移



公链 Coin 兑换联盟 Token

1. 用户向公链合约 PAC 转入 Coin
2. 联盟平台收到 PAC 执行结果即向用户转入 Token

3. 平台通过用户签名与联盟内交易执行结果等信息发送至公链 PAC
4. 公链进行验证操作对资金进行解锁转入联盟平台账号



3.去中心化交易

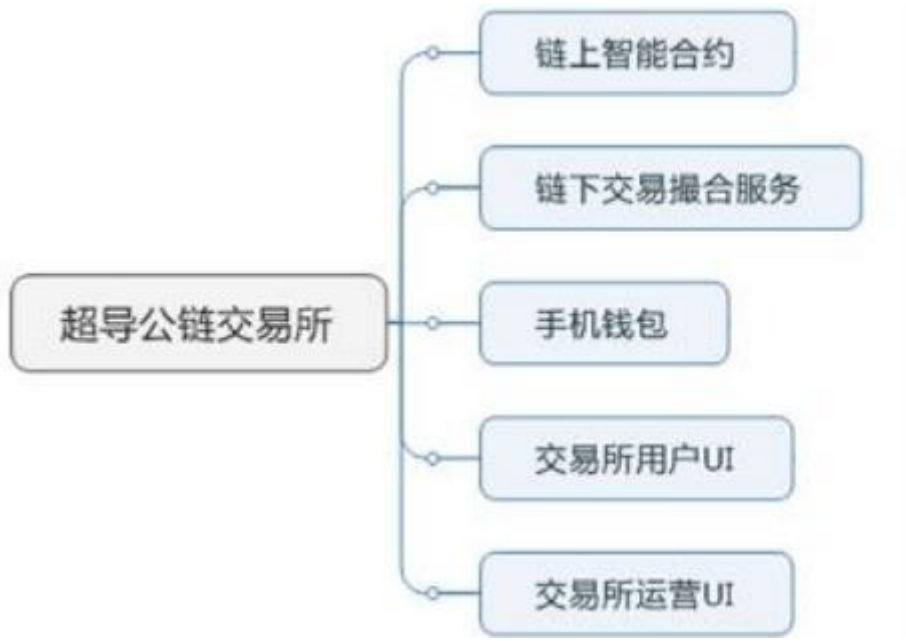
超导链公链创世区块内置去中心化交易所，其核心逻辑在于智能合约，交易所以智能合约的形式在超导链上执行代码块，有分布式不可变更及可追溯的特性。

资金的管理

交易所将资金管理权完全交给用户，用户在使用交易所时，需将资产转入智能约中，资金全部在超导链区块链帐本上。在任何时候，任何情况下用户可以不需要任何第三方协助提取或充值资产。

交易所交易的币种分两类，超导链 Coin 和联盟链在公链的映射 Token，超导链 Coin 做为计价币，存入合约时以 0x0000000000000000000000000000000000000000 标识，其它联盟链 Token 以各自联盟链帐号地址为标识。

交易所主要分为链上智能合约，交易撮合服务，手机钱包，用户 UI，运营 UI 这五个部分。



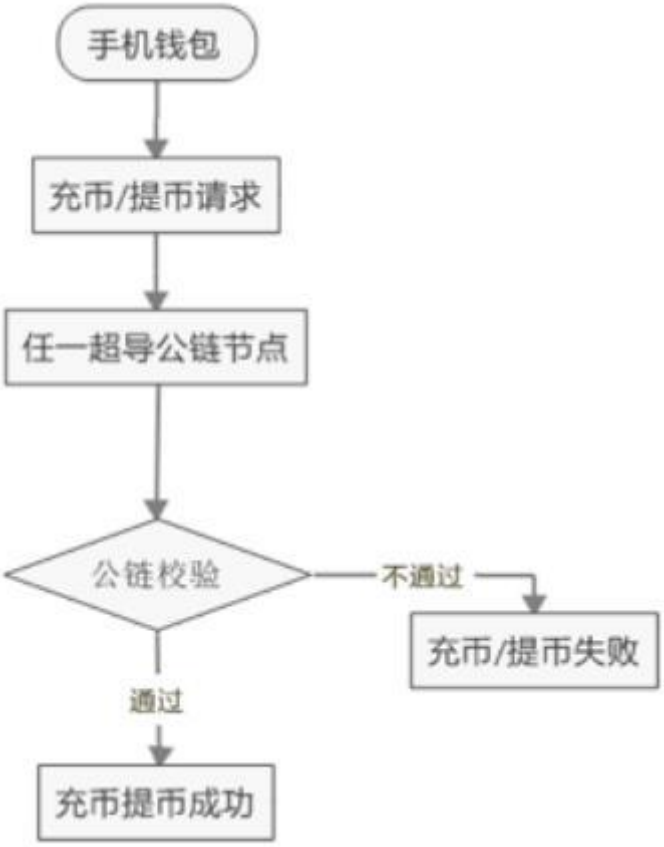
链上智能合约：交易所的核心处理，包含资金管理，身份验证，充币，提币，记帐等功能。

撮合服务：考虑智能合约的运行效率，超导撮合服务使用链下系统完成，在由公链验证身份验证之后，再由之撮合，再调用超导链上智能合约完成。

手机钱包，交易所用户 UI，运营 UI 为使用者和运营者提供了必要的便利。


交易所撮合系统
买卖单登记
资金变更
用户
充提买卖交易
超导公链
交易所智能合约

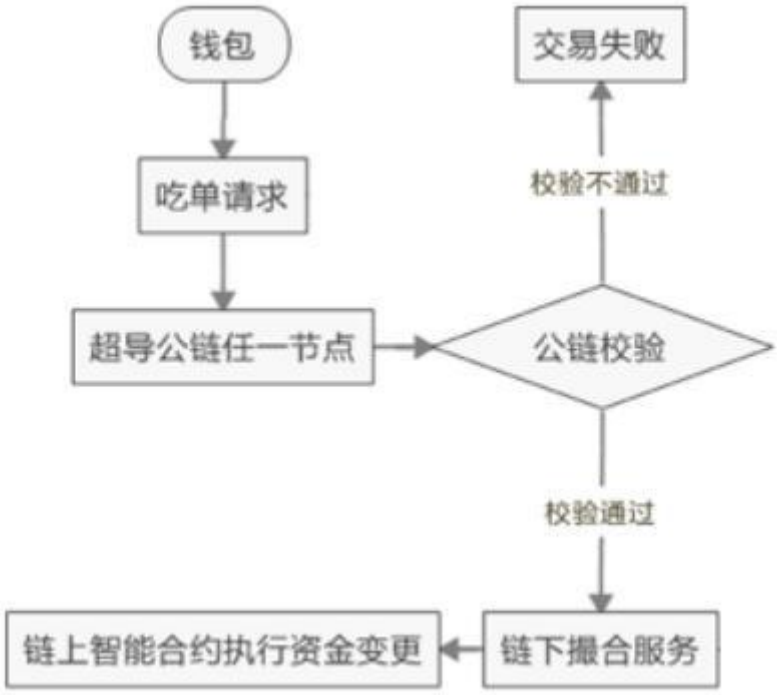
充提币流程


手机钱包
充币/提币请求
任一超导公链节点
公链校验
不通过
充币/提币失败
通过
充币提币成功

挂单流程


钱包
挂单请求
超导公链任一节点
公链校验
不通过
挂单失败
通过
公链返回事件
撮合服务新建订单

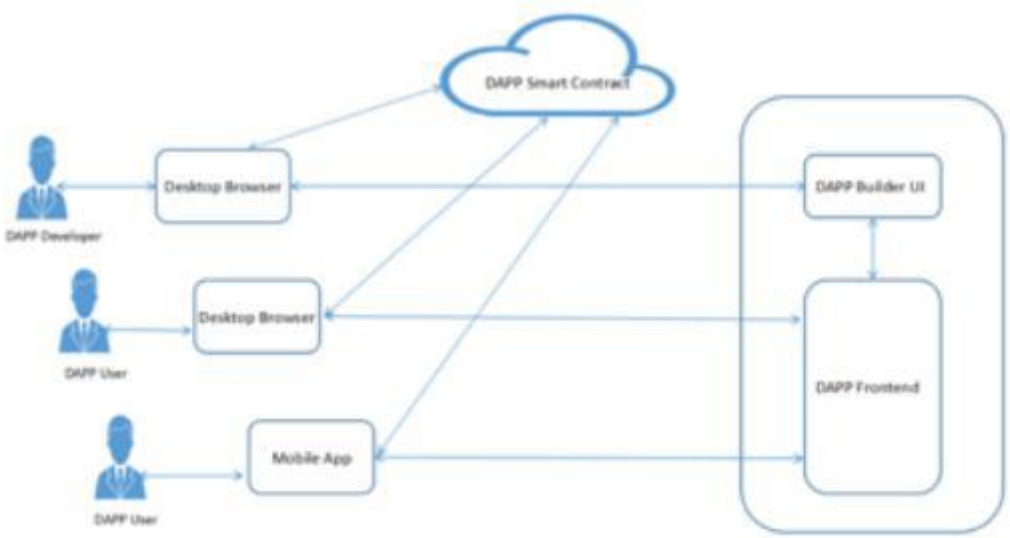
吃单流程


钱包
交易失败
吃单请求
校验不通过
超导公链任一节点
公链校验
校验通过
链上智能合约执行资金变更
链下撮合服务

4.DAPP 应用

超导链致力于创建共享联盟生态，DAPP 作为用户与超导链的桥梁扮演着至关重要的角色。通过移动端 DAPP 开发策略，把区块链的技术优势带给不同行业联盟应用者和普通用户。通过超导 DAPP Store 的高效和快捷的分发，促进超导链走进更多的普通互联网用户。

Dapp 架构如下图所示：



5.项目背景

SCT 超导链发展历程

区块链是一门融合型技术，大类上包含分布类存储，信息传输，密码学，匿名技术，经济学等多领域学科，可谓博采众长，2009 年区块链技术第一次以比特币的身份出现，到 2017 年底比特币创造了一个金融界的神话涨幅两千多万倍，之后的几年区块链的底层应用一直围绕着硬件，流量入口，支付功能展开，从比特币到莱特币包括瑞波币等皆是如此，直到 2015 年以后以太坊的出现，以太坊是第一个提出以区块链公链，智能合约的形式创建代币，这个时候就诞生了区块链应用，从最早的支付层面跳出来作为应用。

2015 年 SCT 超导链同构多链概念诞生

SCT 超导链是在 2015 年在以太坊出现之后诞生的一个理念，以太坊最大的一个特点是智能合约与在以太坊公链上无限发币，但是无论以太坊的发币应用或者智能合约这两大特色，对于实体企业或实体经济商业应用领域上起到的价值作用并不显著，就是基于这么一个服务于实体经济，促动商业应用领域里面， 2015 年澳大利亚的一支技术团队提出，以公链无线创建链、以链发链，让区块链技术更好的运用到实体经济的概念由此产生，实现造链平民化，切实服务于实体经济与普通老百姓。

2016——2017 年搭建底层架构

2016 技术团队着手搭建 SCT 超导链底层架构、公识算法、协议机制的处理等，2017 搭建开发完成架构应用等复杂程序。

2018 年 底层架构搭建成功正式上线

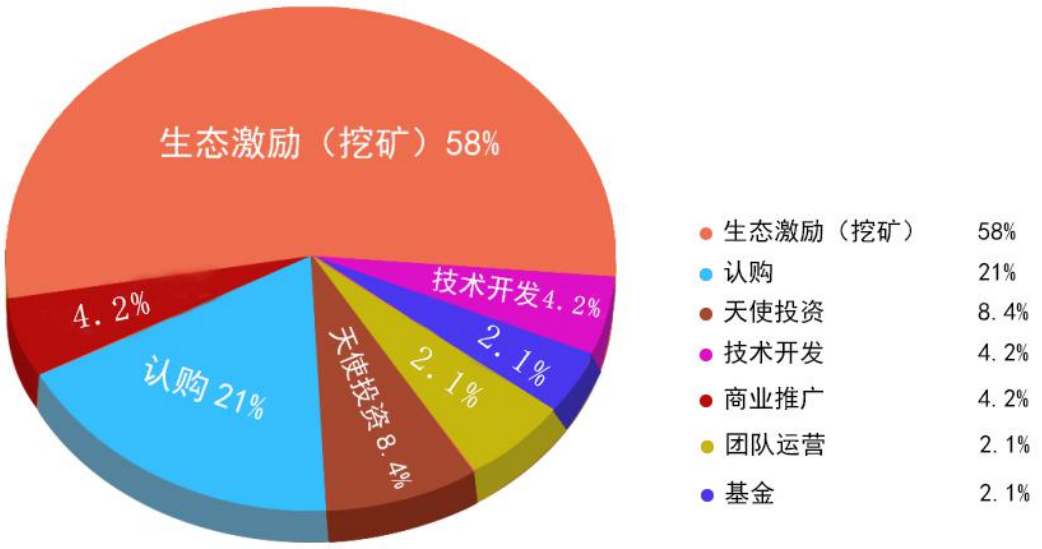
直到 2018 年的时候超导链同构多链 (1+N) 的底层架构完全搭建成功，于 2018 年 4 月 2 日超导链 SCT 正式问世上线。

2019 年完善同构多链技术、DAPP 钱包等投入应用

超导联盟链无限发链的形式与 DAPP 钱包一键 Token 等应用经过不断测试，修改升级到了 2019 年均已完善，正式投入商业应用场景。

SCT 超导链代币分配

SCT 总量预设为 5 亿，伴随超导链创世区块一次性设 2.1 亿枚。后期社区激励【挖矿】2.9 亿枚，预计 142 年到 148 年产出。总量的 4.2 %技术开发， 2.1 %基金， 2.1 %运营团队， 4.2 %商业推广， 8.4 %天使 投 资，21 %认购，官方持有锁仓 3 年，3 年后按季度释放、如图：



在超导链 SCT 上无需官方自行可开发创建联盟，通过 SCT 超导链公链无限扩充联盟链的架构特点每开发一种应用，需要向链上提交一定数量的 SCT 作为费用，系统机制会自动燃烧销毁，采用前期销毁、后期压制的机制。

6.结论

SCT 超导链底层平台在架构上设计并实现灵活、高效、可靠、安全的并行计算和可扩展能力技术的“颠覆性”和业务的“实用性”，同构多链的技术架构为目前

区块链商业场景应用拥有着不可替代的作用，也是全球首屈创新，是真正意义上的未来商业之链，价值之链！

扫码关注公众号