DC技术白皮书

1. 概述

1.1 去中心化系统和云计算服务的新机遇

去中心化账本技术指的是交易记账由分布在不同地方的多个节点共同完成，这些节点都可以参与监督交易合法性，同时也可以共同为其作证。区块链是分布式账本技术的一种形式，区块链分布在点对点网络上并由其管理。由于它是一个分布式账本，因此可以在没有中央服务器管理的情况下运行，并且可以通过数据库复制和信任计算来维护其数据质量。但是，区块链的结构使它有别于其他类型的分布式账本。区块链上的数据被分组并以块的形式组织起来，这些块按照时间顺序依次连接形成一条链，并使用密码学技术对其进行安全保护。基于区块链这种分布式数据结构，可以为零信任的去中心化网络带来共识。

能否解决实际社会问题，以及能否真正提升社会生产活动的效率，是技术能否持续发展和普及的关键衡量标准。信息技术对于社会生产关系与生产效率的影响是已被验证的，且正处于持续深化的进程中，而存储和计算恰是信息技术生产力革命的两大核心基础要素。因此，区块链技术不仅需要提供凝结共识、去信任化的机制（即“价值去中心化”），也应当为存储、计算两大核心生产要素提供去中心化的基础设施（即“存储去中心化”与“计算去中心化”）。纵观现有的主流去中心化共识机制，区块链技术被广泛用于信任凝聚（生产关系）基础设施，并且往往伴随着大量算力以及存储资源的消耗，而对存储和计算去中心化的支撑则相对空缺。

现有的存储和计算场景广泛地承载于中心化的云计算平台，计算服务与存储服务是云服务市场最重要的两大组成部分。中心化的云服务中将算力以及云存储都汇聚到中心化服务器以及磁盘阵列上，使用者可以在任何时间、任何地方，透过任何可联网的装置连接到云上获取计算能力并方便地存取数据。但是，在这种中心化服务的方式下，存在服务稳定性不足、网络带宽成本高、数据传输能力有限等问题。更加致命的是，当中心化的平台出现运行问题，就会殃及几乎所有被服务方——中心化云计算的规模做得越大，这种运行方面安全问题的隐忧就越大。本项目旨在以区块链的信任凝聚出发，通过技术的创新优化，从去中心化云服务场景切入，进而实现可信、可靠、高效、泛在的去中心化云服务生态。

1.2. **DC** 概述

DC（Decentralized Cloud）本质上是DePIN(Decentralized Physical Infrastructure Networks)。和现有的云计算最大不同，DC是分散的，没有中心的，不被个人或机构统一控制。任何人都可以参与，在任何地方都可以运行节点，自动入网。借助区块链提供的共识服务，每个节点都可以单独对外提供云计算服务,并且与**DC**网络中的其他节点互为备份。相对云计算来说，**DC**不是一朵云，也不是一片云，而就是云本身。**DC**是为开发人员提供非常便利的去中心化网络基础设施，使他们能够利用他们传统的互联网开发经验来开发去中心化应用程序。**DC**从技术上为激励层（共识）+ 网络层 + 持久层（存储）+ 应用层（计算）的全栈生态进行了实现。基于**DC**的DApp的用户体验就像使用传统的互联网应用程序一样。

2. **DC**的技术目标

DC主要目标是为用户提供去中心化的云服务,并通过全新的技术方案为Web3.0行业带来革命性的改变。

- 消除用户使用Web3.0应用的门槛
- 消除企业和开发者开发Web3.0应用的门槛
- 消除当前Web3.0业务存在的性能瓶颈
- 消除当前Web3.0生态中数据存储瓶颈
- 突破当前Web3.0应用业务场景的限制

- 为AI时代个性化应用提供基础设施

3. DC的共识机制

通过将TEE技术与NPOS共识机制结合，**DC**网络旨在提供一个既安全又高效的区块链解决方案，克服了传统技术在处理速度和数据存储能力方面的限制。这种创新的组合共识机制为DC网络的发展和应用提供了坚实的基础。

3.1. 可信执行环境（TEE）

可信执行环境（TEE）是一种安全技术，它基于硬件安全模块来提升计算和通信系统的安全性。TEE技术的发展已经从传统的硬件芯片安全模式转向更为高级的实现方案，如Intel的SGX技术和基于ARM的开源框架TrustZone。这些技术通过以下五个核心规范来确保安全：

a. 签注密钥（Endorsement Key）
签注密钥必须随机生成并且不能被改变。其中私有密钥必须被安全保存，除了指定接口可以通过黑盒子方式使用，无法通过任何方式获得。而公共密钥用来认证及加密待发送的敏感数据。

b. 安全输入输出（Secure Input and Output）
输入输出是指用户与系统之间的交互，其途径包括键盘、外设、网络接口等。安全输入输出是指，从系统用户到访问的进程间存在一条受保护的路径。

c. 储存器屏蔽（Memory Curtaining）
储存器屏蔽拓展了一般的储存保护技术，提供了完全独立的储存区域。即便是操作系统自身也没有屏蔽区的完全访问权限，因此入侵者即便控制了操作系统，运行时（Run Time）的数据也是安全的。

d. 密封存储（Sealed Storage）
密封存储通过把私有信息和用户使用的平台环境配置信息捆绑在一起来保护私有信息。意味着被密封存储的数据只能在相同的安全环境下读取。

e. 远程认证（Remote Attestation）
远程认证是指，由签注秘钥生成当前系统的软件证明书，系统上的任何改变可以通过证明书被远程授权方感知和校验，从而使得系统的执行逻辑安全可信。

DC的局部共识和数据安全方案主要集中在服务端，采用基于 Intel SGX的TEE技术作为其首个解决方案。与复杂的算法解决方案相比，基于TEE的解决方案在实现逻辑上更为简单而有效。随着技术的快速发展，TEE拥有了强劲的发展动力和技术生态，支持复杂计算逻辑的可信执行，并满足完整的云计算能力需求，从而使**DC**能够创建去中心化的云服务生态。

3.2. NPOS共识

NPoS（Nominated Proof of Stake，提名权益证明）是Polkadot基于PoS算法设计的共识算法，验证人（Validator）运行节点参与生产和确认区块，提名人（Nominator）可以抵押自己的通证获得提名权，并提名自己信任的验证人，获得奖励。**DC**集成了Polkadot的NPOS算法。 验证人选举算法是NPoS机制的核心，选举过程要具有公平代表性和安全性，NPOS为此设计了Phragmén算法,确保每次选举都具有这种性质, 确保任何节点池既不被选出的验证人过度代表，也不被选出的验证人过低代表，而是与它们的质押成比例的。

在NPoS中，每个验证者节点分配到的奖励是一样多的，提名者根据自身在支持的验证节点的质押量比例来分配该验证节点获得的奖励。这样一来，如果有太多的提名者投票给了质押总数较多的验证者节点，对于他们来说就很不划算了，所以需要他们调整票仓，将通证投票给质押总数更低的一个或者多个验证者节点。

这样的机制会激励提名者寻找质押通证更少的验证者节点，这样会使他所质押的通证占比变得更大，在分配中更有优势。也正因为如此，才能保证验证者都有差不多平等的质押量，使网络足够去中心化。

3.3. DC的组合共识机制

DC的共识分为由链下共识及链上共识两部分组成。链下共识主要负责**DC**的云服务节点的运行逻辑共识,包括云服务节点的入网、退网、质押、举报、节点间数据同步以及对外服务等机制;链上共识主要用于维护**DC**的账号体系、激励机制以及数据索引机制等。

链下共识主要基于TEE技术实现,TEE技术保证了云服务节点的运行逻辑的安全性,同时也保证了云服务节点的运行逻辑的可信性,杜绝了运行非授权程序的云服务节点入网,从而确保**DC**中的云服务节点都按既定业务逻辑对外提供服务;链上共识主要基于NPOS共识机制实现,**DC**的NPOS共识机制保证了**DC**的账号体系、激励机制以及数据索引机制的公开、公正、可靠以及参与者自由出入的能力。

4. DC的架构

DC是一个无限横向扩展，节点可以自由进出的的P2P对等网络。通过将TEE技术与NPOS共识机制结合，**DC**旨在提供一个既安全又高效的区块链解决方案，克服了传统区块链技术在处理速度和数据存储能力方面的限制。这种创新的组合共识机制为**DC**的发展和应用提供了坚实的基础。

DC主要由**DCChain**以及**DCNode**两部分组成,**DCChain**是一个区块链网络,负责维护**DC**的账号体系、激励机制以及数据索引机制等;**DCNode**是一个云服务节点,多个**DCNode**组成了**DC**的云服务网络,通过**DCChain**提供的账号体系、激励机制以及数据索引机制为**DC**的用户提供去中心化的云服务。

4.1. DCChain

DCChain是一条基于Substrate开发的公共区块链，采用统一账户体系,统一了以太坊EVM和Substrate两个系统的账户和签名(即公钥和私钥) ,兼容以太坊钱包及DApp的接入。它是**DC**的大脑，它为**DC**生态的所有参与者营造一个高度可信、公平、可靠且透明的共识机制，为整个**DC**网络提供以下几方面的共识能力：

4.1.1. 为DC维护账号体系

- 为整个网络生态中的用户提供身份共识，为**DC**的所有业务操作的提供用户识别和标识；
- 支撑**DC**网络生态独有的、用户体验与现有互联网应用账号登录一致的账号、密码体系；
- **DC**中的用户账号的主权属于用户自己,可以自由转让,为了更好区分于区块链上的ERC20格式的账号,我们将**DC**网络中用于结合密码登录的用户账号称为NFT账号;
- 用户通过**DC**的NFT账号与密码在网络生态中进行登录时，**DCChain**提供NFT账号到用户基础信息存储和备份节点的索引，引导登录请求发送到对应的**DC**节点为用户提供登录响应，最终通过登录的NFT账号提取出对应的**DCChain**应用签名账号的私钥。用户登录成功后，即可利用获取到的**DCChain**的应用签名账号进行后续业务操作。

4.1.2. 作为DC的激励层

DC根据参与者的贡献程度，发放对应数量的DCT通证的方式进行奖励。

1. **DC**网络贡献者
    - 云服务空间供应商（运行**DC**云服务节点）
    - **DCChain**验证人及提名人
    - 基于**DC**的DApp开发者

2. **DC**对贡献者的的奖励来源
    - **DC**根据通胀率增发的**DCT**通证 增发的**DCT**通证按一定比例奖励给区块链验证人(含提名人)和云服务空间供应商
    - DApp用户用于兑换云服务空间所消费的**DCT**通证 DApp用户消费的**DCT**则按一定比例奖励给DApp开发者以及云服务空间供应商
3. 保障利益分配的公平性
   DC将网络贡献者、贡献程度、增发规则已经用户**DCT**通证消费信息等数据记录到区块链上，保障**DC**经济生态的公开、公正、可靠以及参与者自由出入的能力。
4. 恶意行为的惩罚机制
   DC通过**DCChain**记录的数据，可以对DC网络中的恶意行为进行追踪，对恶意行为者进行惩罚,主要包括对链共识的破坏和所存储数据的损毁。

4.1.3. 作为DC网络的数据索引层

DCChain将**DC**中的数据索引信息记录到区块链上，为**DC**的数据存储层提供数据索引服务，保障**DC**数据存储层的可靠性和可用性。数据索引主要包括:

- 数据存储位置索引 DApp可以根据文件或者数据库的的CID快速定位到存储了文件或数据库信息的云服务节点信息列表,快速取回数据。
- 云服务节点索引 DApp可以从**DCChain**上快速获取云服务节点的基本信息,包括入网状态、存储容量以及访问可达的互联网地址。
- 用户信息索引 DApp可以根据NFT账号快速定位用户信息所在的云服务节点,为用户NFT账号密码登录逻辑提供快速引导服务,详情可以参考[DC网络的账号体系](## 4)。

4.1.4. 作为DC的智能合约层

DCChain支持智能合约的开发和部署，为**DC**的DApp提供智能合约的支持。**DCChain**完全兼容EVM,任何跑在以太坊的DApp都可以原封不动的迁移到**DC**中。

4.2. DCNode

DC的云服务节点网络由很多个自组网的**DCNode**组成，负责为**DC**的用户提供云服务,每个**DCNode**都运行在TEE环境中,确保数据绝对私密安全。**DCNode**通过**DCChain**提供的账号体系、激励机制以及数据索引机制为**DC**的用户提供云服务。**DCNode**的主要功能包括：

1. 基础数据存储 **DCNode**利用IPFS网络为用户提供文件类数据存储服务，用户可以通过**DC**的DApp将文件存储到**DCNode**提供的云服务空间中，**DCNode**会根据用户的存储需求提供相应的存储空间,并确保**DCNode**中数据备份的数量不少于3份,确保数据的可靠性和可用性。
2. 数据库存储 **DCNode**提供独特的多线程分布式数据库存储服务，允许DApp将允许多终端并发访问的数据库存储到**DCNode**提供的云服务空间中，**DCNode**会根据用户的存储需求提供相应的存储空间,并确保**DCNode**中每个数据库数据备份的数量不少于3份,确保数据库数据的可靠性和可用性。
3. 社交路由 **DCNode**提供独特的社交路由服务，允许DApp将用户自身的基本信息、社交关系以及社交过程数据加密存储到**DCNode**提供的云服务空间中,方便开发者可以快速开发出Facebook、Twitter、Linkin等类似的社交DApp。
4. 消息缓存 **DCNode**为用户提供长达10天的点对点消息缓存服务,确保用户在离线时也不错过其他用户或平台发送给自己的消息。

5. DC网络云服务节点组网机制

DCNode是一个自组网的节点,它运行在TEE环境。**DCNode**之间通过P2P网络互联,并利用**DCChain**提供的共识机制进行数据同步,确保整个DC的数据一致性。

5.1. 节点入网机制

1. 运行**DCNode**节点程序,获取节点的PeerId和节点Erc20账号(注意:该Erc20账号私钥加密存储在节点的TEE环境中,任何人无法获得)。
2. 通过**DC**门户或者兼容以太坊的钱包,向节点的Erc20账号转入少量的**DCT**用于节点向链**DCChain**提交事务时的手续费消耗。
3. 将节点PeerId绑定到用户拥有所有权的用于质押的Erc20账号上,并将绑定的Erc20账号转入质押所需数量的DCT用于质押。
4. **DCNode**节点程序,在检测到质押成功后,将自动发起携带TEE远程证明的入网申请,并等待**DCChain**的共识机制的确认。
5. 其他已经入网的一组随机**DCNode**节点,在检测到新节点的入网申请后,将自动发起对新节点的TEE远程证明进行验证,如果该TEE远程证明验证失败,则向区块链提交举报请求。
6. 新申请入围的**DCNode**节点在等待300个区块后,再次发起入网申请,**DCChain**将判断新节点的入网申请是否已经通过其他已入网节点的TEE远程证明验证,如果通过,则新节点入网成功,否则新节点入网失败,并会扣除对应数量已质押的**DCT**通证。
7. **DCNode**节点入网成功后,开始为**DC**的用户提供云服务,并担负起头节点发起携带TEE远程证明的验证任务。

5.2. 节点退网机制

1. 节点拥有者可以在**DC**门户随时发起退网申请,**DC**在收到对应**DCNode**的退网申请后,会自动开启该节点上所存数据的备份任务(此时节点可以离线,因为DC网络本身就存在多分数据备份)。
2. 如果节点拥有者,直接停止**DCNode**节点程序,并在7天内都没有主动发起退网申请,则**DC**将扣除一定数量该节点质押的**DCT**通证,作为惩罚。

6. DC网络的账号体系

DC用户的NFT账号与密码与用户的应用签名私钥建立对应关系，即每个**DC**的NFT账号与密码对都会对应一个区签名私钥或助记词信息。由于NFT账号密码登录必须支持跨终端登录Web3.0应用，为实现这一特性，**DC**实现了以下几点：

1. 将NFT账号密码对应的账号私钥信息的存储到**DC**中
2. 存储在**DC**中的私钥信息以及用户基本信息完全私密，无法被用户以外的任何人解密
3. NFT账号密码登录时，可以安全的从**DC**中快速提取出对应的应用私钥信息
4. 存储在**DC**中的应用私钥信息只能被同时拥有NFT账号与密码的用户提取出来，且整个登录与信息提取过程全程加密。

具体实现流程如下：
与现有的Web3.0一致的步骤：

1. 用户本地自动生成一个应用账号,包括私钥或派生助记词
2. 引导用户记录助记词
3. 完成去中心的链上应用账号生成,同时通过助记词派生出ERC20格式的链上账号

DC网络NFT账号独有相关步骤：

4. 引导用户输入NFT账号与密码等基本信息
5. 在 **DC** 中查询NFT账号是否被注册，已注册则引导用户重新输入其他NFT账号
6. 检查用户的链上账号是否有余额，如果没有余额引导用户在链上账号中存入余额。（建议应用开发商在应用推广前期自行建立一个水龙头服务，为新注册账号的用户自动转入可绑定账号用的余额）
7. 链上账号向DCCHain为用户的应用账号订阅云服务空间
8. 向 **DC** 提交应用私钥或助记词与NFT账号的绑定关系（如果提交过程中，账号被其他人绑定或者余额不足，则重新回到前面第4步）
9. 用户可以直接用NFT账号与密码在任何终端进行登录
10. 用户可以根据需要修改登录密码

6.1. **DC**账号安全设计

由于存储了用户账号信息的节点列表都可以通过NFT账号检索到，因此必须对存储在**DCNode**的用户信息进行安全防护，**DC**针对用户信息的安全防护主要由以下几点来保证：

1. 基于AES256加密区块链账号私钥
   利用NFT账号与密码再通过一系列加密处理组合生成加密绑定的区块链账号私钥的AES256密钥，确保只有同时知晓了NFT账号与密码才能解密出绑定的应用账号私钥相关信息。
2. 加密后的区块链账号私钥只会存在在已入网的**DCNode**中
   客户端SDK确保客户端应用在将加密的应用账号私钥只存储在已经入网且在线的**DCNode**中，由于每个已入网的**DCNode**都是已经由网络通过基于TEE的远程证明技术认证，确保节点上的程序都是未经任何修改、合法的且运行在TEE环境的程序，因此数据存储在入网节点上是安全、私密以及可靠的。
3. **DCNode**通过TEE封装存储加密后的区块链账号私钥
   DCNode将使用TEE封装技术对存储在节点上的加密后的区块链私钥进行封装存储，确保**DCNode**物理设备拥有者也无法提取出加密后的区块链私钥。
4. 登录过程加密处理的key中，不包含完整的账号密码信息
   请求信息中的提取NFT账号的Key参数生成算法进行了安全设计：

- 通过账号与截取部分密码各自HASH，并进行分解与截取后再组合生成，多重HASH算法确保无法通过Key来反向退出账号密码；
- 密钥截取部分后参与计算，以及HASH后再截取部分来进行二次HASH确保不能通过暴力枚举来获取准确的NFT账号与密码

5. 登录过程全程加密，确保通信安全

- 客户端向**DCNode**发送登录请求时，通信过程使用**DCNode**的公钥进行加密，只有被请求的**DCNode**程序才能解开（所有**DCNode**的私钥都是随机生成后，利用TEE技术进行封装后进行保存，节点拥有者也无法获取）；
- 反馈数据也通过登录请求过程协商的密钥进行加密，确保只有请求发起方才能解密。

6. **DCNode**对登录失败次数进行窗口控制，拒绝超出窗口限制的登录请求
   DCNode对用户发起NFT账号与密码登录请求进行登录失败窗口控制，确保同一个NFT账号在一定时段内只能请求有限次数，阻止黑客通过接口暴力方式提取出加密后的区块链私钥
7. 引入Bcrypt算法，降低AES256密钥生成速度，阻止离线暴力破解请求key
   NFT账号与密码生成AES256密钥过程中引入Bcrypt,并加以改进，确保加密盐值可以由NFT账号密码通过特定算法导出。利用Bcrypt的慢速HASH算法原理（cost设置为12，后面可以根据设备性能普遍提升后进行加大），黑客即使获得加密后的区块链私钥后也无法进行离线暴力破解。

7. **DC**的安全机制

DC安全分为两大部分,一部分是**DCChain**的安全机制,另一部分是**DCNode**网络的安全机制。

7.1. **DCChain**的安全机制

DCChain的安全机制主要包括以下几个方面：
1. 共识机制
DCChain的共识机制采用NPOS共识机制,最大程度的吸引了生态用户的参与网络共识,确保**DC**的安全性。
2. 治理机制
DC具有一个去中心化的治理结构，允许通证持有者投票决定网络升级和变更。这种机制可以迅速响应安全威胁和漏洞，及时进行修复和升级，从而维护网络的安全性。
3. 运行时升级
DCChain允许无需硬分叉即可升级区块链的运行时逻辑。这意味着如果发现安全漏洞或需要改进安全措施，可以迅速且无缝地部署更新，从而增强整个网络的安全性。
4. 抗拒绝服务攻击（DDoS）
DCChain机遇Substrate开发,网络设计考虑到了抗DDoS攻击的需要，通过各种机制（如限制请求率、选择性接受连接等）来减轻潜在的拒绝服务攻击。

7.2. **DCNode**网络的安全机制

DCNode网络的安全机制主要包括以下几个方面：
1. 节点入网质押机制
所有**DCNode**入网前需要质押一定数量的**DCT**通证, 当节点出现恶意破坏网络或损毁数据时,将会被罚没。
2. 节点代码逻辑管控机制
DCNode的代码全部运行在TEE环境中,因此**DCNode**节点只能运行**DC**认证过的代码逻辑,确保**DCNode**的业务逻辑透明可控,无法造假。
3. 节点入网冷静期机制
DCNode节点在发送入网申请后,需要等待300个区块的冷静期后,才能正常入网.在冷静期内入网的**DCNode**节点会对新入网节点的TEE远程证明进行校验,所有校验通过后,才能入网。
4. 节点签名私钥TEE封装机制
节点用于与区块链交互的签名私钥,利用TEE进行密封,任何人都无法获得,保证了已入网节点的所有数字签名都是按预定的代码逻辑执行,不受任何人干扰。
5. 用户交易安全机制
所有涉及用户交易相关的事务,都必须携带用户数字签名,并校验通过后,才提交到区块链上,确保用户交易的安全性。
6. TEE 远程证明机制
所有涉及到**DC**安全性的事务,都必须携带**DCNode**节点的TEE远程证明后再提交到区块链,接受其他**DCNode**节点的远程证明校验。

8. DC数据存储及安全机制

DC的文件存储机制主要包括以下几个方面：

- 数据存储及传输机制
  DC通过IPFS协议为用户提供数据数据传输及存储服务。
- 数据存储位置索引
  用户数据存储信息与PeerId的绑定关系记录到**DCChain**上,方便快速检索。
- 数据存储备份机制
  DC确保用户上传的数据至少备份3份(用户账号信息至少备份5份),确保数据的可靠性和可用性。
- 存储权限控制机制
  DC会根据对数据的所有权进行管理,确保数据只能被拥有主权的用户操控。
- 数据安全检查机制
  DC的每个**DCNode**节点都会对存储在节点的数据进行监控,一旦发现数据被篡改或者损坏,将会自动通知网络,并开启备份数据的任务。
- 数据加密机制
  DC中所有敏感数据都是加密存储,除拥有数据主权的用户外,对任何人不可见。
- 数据存储位置可控
  DC中用户可以指定数据存储的位置,确保数据存储在用户信任的节点上。
- 数据删除机制
  DC中用户可以随时删除自己的数据,确保数据的隐私性。
- 数据备份数量可控
  DC允许用户为重要的文件单独增加备份数量。

9. DC去中心化数据库机制

DC对ThreadDb进行改造后,再结合**DCChain**的索引功能打造了类似关系型的去中心化数据库存储机制:主要包括以下几个方面：

- 去中心化
  利用了IPFS的去中心化特性，允许数据分布在多个节点上，这增强了数据的持久性和抗审查性。
- 数据同步
  它支持数据在不同设备或用户之间的实时同步，这对于构建协作应用和社交网络类应用尤为重要。
- 用户控制
  用户完全控制自己的数据，可以选择共享和同步的数据范围。这与传统的中心化服务不同，用户通常对自己的数据控制权有限。
- 隐私和安全
  数据可以加密存储，确保即使在公共或半公共环境下也能保护用户的隐私。
- 多节点备份
  DC确保数据库数据在整个网络中至少备份3份,确保数据的可靠性和可用性。

10. DC的去中心化社交能力

DC打造去中心化社交能力的目的是为了让用户在**DC**中可以自由的建立社交关系,并在社交关系中进行数据的共享和传递,不在受到中心化社交平台的控制。**DC**的去中心化社交能力主要包括以下几个方面：

- 用户信息存储
  DC将用户的基本信息、社交关系以及社交过程数据加密存储在**DCNode**节点中,确保用户的隐私安全。

- 用户路由
  DC通过**DCChain**提供的数据索引机制,为用户提供快速的用户路由服务,确保用户可以快速找到自己的好友。
- 主题路由
  用户可以通过**DC**快速的路由到对应社交主题所在的**DCNode**节点列表,并可以快速找到自己感兴趣的社交主题。
- 用户社交过程数据存储
  用户不论是基于社交主题还是与好友间的社交过程数据多是加密存储在**DC**中,任何无关人员都无法访问。
- 消息缓存
  DC为用户提供长达10天的点对点消息缓存服务,确保用户在离线时也不错过其他用户或平台发送给自己的消息。

11. **DC**的服务能力提供机制

DC支持基于智能合约模式以及非智能合约模式的DApp,并提供了一套完整的服务能力提供机制,主要包括以下几个方面:

- 基于智能合约模式的DApp的支持
  DC兼容以太坊的智能合约,任何以太坊的DApp都可以无缝迁移到**DC**中。
- 基于非智能合约模式的DApp的支持
  DC允许任何人都可以开发无中心化服务器的DApp,并通过**DC**的云服务节点为用户提供服务。
- 云服务节点的服务能力方式
  为了普通开发者都能快速开发出DApp,**DC**为开发者提供了基于类似中心化云服务的RPC接口以及高度集成化的SDK,功能覆盖用户信息管理、文件存储、数据库同步、消息通信、社交服务等。

12.DC网络云服务用户消费机制

DC是一个基于用户付费的网络,用户可以通过**DCT**通证来为使用**DC**的服务,根据用户对**DC**的使用方式不同,也有不同的付费方式,主要包括以下两种方式:

- 用户的业务操作直接与区块链交互
  这种操作方式下,用户可以通过**DCT**通证来为自己的业务操作付费,包括用户直接调用**DCChain**上的接口进行DCT通证转账或者调用链上的智能合约功能等。
- 用户通过DApp与云服务节点交互
  这种模式下,用户不需要直接和**DCChain**进行交互,所有业务操作都与云服务节点交互,涉及需要上链的业务请求,在用户生成Ed25519的签名后,由云服务节点代用户向DCChain发送上链请求,同时用户也无需支付任何区块链交互手续费。但是用户在与**DCNode**交互前,需要使用**DCT**通订阅对应期限的**DC**云服务空间,这种方式好比用户采用包月乃至包年的方式来使用DC网络的服务。这种方式下,用户与**DCNode**的业务交互都是实时和确定性的,用户无需等待区块链的确认时间,也无需支付区块链交互手续费。

(**注意: DC**经过特殊设计,在线的**DCNode**与**DCChain**交互时,大部分情况下也无需支付手续费。)

第一种方式是现在通用区块链的操作方式,我们之所以引入第二种方式,是因为现在通用区块链网络的模式下,所有操作都需要在链上进行操作,这样注定无法发展超级应用,因为链上操作gas费用再低,也需要费用,用户只会为产生最终价值的这一步操作付费,这样必然导致很多业务逻辑无法实现,**DC**将那些非决定性的也不能提现或产生价值的业务逻辑由云服务节点提供类似中心化的服务支持。另外,区块链的业务排序以及区块确认逻辑,不会随任何业务需求发生改变,导致DApp在用户提交业务请求后,无法明确的确定需要多长时间能对该业务请求进行响应。因此如果DApp的业务操作逻辑过多的与区块链直接交互,将严重影响用户体验。**DC**除了用户

间**DCT**通证转账以及云服务空间订阅等必须需要进行链上操作的逻辑外,其他与区块链交互的业务逻辑全部交由**DCNode**代为处理,由**DCNode**给用户提交的业务请求作出快速的响应,确保用户侧体验的连贯性,并确保业务上需要涉及上链的数据正确上链。

13. 基于**DC**云服务的应用开发实践

开发者可以基于**DC**开发基于链上智能合约的DApp,这部分功能和传统区块链项目基本一致;**DC**真正的创新点在于开发者可以基于**DCNode**的开发性能、用户体验及业务场景覆盖范围不属于传统互联网应用的DApp.开发者根据自己的业务需求,可以选择以下几种方式进行开发:

- 基于**DC**客户端SDK开发
  为了减轻开发者的开发难度,**DC**为开发者提供了一套完整的开发工具链,包括覆盖移动端及PC端的多开发语言支持的SDK,以及基于Docker的开发环境.在这种方式下,开发者可以充分利用自身的开发经验和技术栈,快速的开发出DApp,而开发者自身甚至无需具备任何区块链的相关知识储备。

- 基于**DC**入口应用开发
  DC提供单独的入口应用,它类似Web3.0的钱包应用,但是除了钱包的基本功能外,它最主要的能力是为轻应用提供部署及运行环境,任何基于H5或Python的轻应用都能通过入口应用具备去中心化的数据存储以及轻用户间信息交互的的能力,同时任何人可以基于这个入口应用一键发布应用,供其他用户使用。这是一种崭新的应用开发模式,它将为用户提供更多的创新空间,让每个人都能随时随地的发布应用,在即将到来的AI时代,可以让每个人都能参与到应用的开发定制中来,从而更好的满足用户的个性化需求。

- 基于**DC**的RPC服务开发 **DC**提供了类似中心化云服务的RPC接口,开发者可以通过RPC接口访问**DCNode**,为用户提供服务,这种方式下,更加灵活,但是对开发者要求更高,需要开发者具备去中心化相关的知识储备,并对整个**DC**的运行机制非常熟悉。

14. 技术实现

DC的技术实现主要包括以下几个方面:

14.1. **DC**中的TEE远程证明(Remote Attestation)

DC的远程证明(Remote Attestation)基于SGX DCAP(Data Center Attestation Primitive), 主要用于解决了软件执行的可靠性问题，是 TEE 抵御恶意行为的重要功能。在**DC**中，远程证明同样是去中心化网络组建的核心。被节点通过在远程验证的过程中嵌入当前运行 TEE 的公钥，将节点的身份、执行逻辑以及平台参数与 TEE 公钥在区块链上 关联起来。远程证明在节点向**DCCHain**提交的涉及网络安全的相关事务中被携带,由**DC**中随机的一组已入网的节点进行验证，先后要求被校验者证明:

- 节点的身份
- 节点运行的逻辑未被篡改
- 节点在一个正版平台上运行，并且启用了英特尔SGX

DC中远程证明应用的基本流程为:

1. 每个节点都会配置运行PCCS（Provisioning Certificate Caching Service）服务，该服务会根据需要从Intel PCS(Provisioning Certification Service)同步硬件证书到本地,用于验证其他节点的远程证明是否有效;
2. 根据业务逻辑设计,节点向**DCCHain**提交携带了远程证明的事务(如节点入网申请、节点举报异常节点);
3. **DC**会随机选择一组已入网的节点,并要求这些节点对远程证明进行验证;

4. 如果有节点对远程证明验证失败,则会进入节点异常举报流程(举报事务自身会携带远程证明,供**DC**验证);
5. 如果举报节点异常的数量超过一定比例,则会对被举报节点进行处罚,包括扣除质押的**DCT**通证、暂时禁止入网等;

远程证明机制确保了代码逻辑不能被修改,它为**DC**解决了以下几个关键问题:

- 保证了节点的身份,确保了节点的可信度;
- 从根源上避免了女巫攻击、生成攻击、资源攻击以及数据篡改等恶意行为;

14.2. 空盘证明

为了度量节点的存储供应量，我们定义了空盘封装机制，使得节点可以在 TEE 内有效地追踪节点声明的存储空间。节点封装文件由很多1G大小的封装文件组成,每个封装文件以以下方式生成:节点以封装在TEE环境的加密密钥与文件名经过一系列的HASH处理后生成对应文件名的封装文件的长度位256的种子,再以这个种子通过链式形式生成完整的1G封装文件，这种模式下可以确保节点的存储空间是真实的，而不是虚假的,因为可以抽查文件的任一位置都能验证文件的完整性。

14.3. 基于TEE的**DCNode**升级

Substrate 框架提供了很强大的无分叉升级机制，但**DC**的**DCNode**主要运行在TEE环境,因此这部分不能直接的适用这个机制。

DC团队根据Substrate链和TEE的特性，将**DCChain**的升级使用Substrate的无分叉升级机制，而**DCNode**的升级则使用TEE的升级机制,通过引入同样运行于TEE的**DCUpgrade**应用来辅助升级,**DCUpgrade**应用主要用来将旧版本**DCNode**TEE环境中的密钥传递到新版本**DCNode**TEE环境中,确保新版本**DCNode**节点能够解封旧版本的数据。升级流程如下:

1. 运行在TEE环境的**DCUpgrade**节点程序会定期监控**DCChain**上最新的**DCNode**程序的版本号,如果发现有获得的DC网络签名确认的新版本,则会自动下载新版本的**DCNod**e程序;
2. **DCUpgrade**向正在运行的**DCNode**程序申请应用密钥;
3. 运行中的旧版本**DCNode**程序向**DCUpgrade**发起携带随机数的TEE本地证明挑战请求;
4. **DCUpgrade**节点根据挑战请求中的随机数以及**DC**对自身EnclaveID签名一起组合后生成TEE本地证明,并将证明发送给**DCNode**;
5. **DCNode**验证**DCUpgrade**节点的证明,并确认DC网络对**DCUpgrade**的EnclaveID的签名有效后,将应用密钥发送给**DCUpgrade**;
6. **DCUpgrade**将应用密钥封装在TEE环境中,并关闭运行中的**DCNode**程序;
7. **DCUpgrade**启动新版本的**DCNode**程序;
8. 新版本的**DCNode**程序向**DCUpgrade**申请应用密钥;
9. **DCUpgrade**向新版本的**DCNode**程序发起携带随机数的TEE本地证明挑战请求;
10. **DCNode**验证**DCUpgrade**的证明,并将应用密钥发送给**DCUpgrade**;
11. **DCUpgrade**验证**DCNode**的本地证明,并确认**DCNode**是经过**DC**签名后,将应用密钥发送给运行中新版本的**DCNode**;
12. 新版本的**DCNode**开始接管旧版本的**DCNode**的工作,完成升级。

15. 攻击与威胁

15.1. SGX 的侧信道攻击

Intel SGX技术是基于硬件的可信执行环境实现。即使是攻击者获得OS，hypervisor,BIOS 和 SMM 等权限，也无法直接攻击 Enclave。因此，攻击者往往通过侧信道攻击，比如页表、Cache、DRAM 等攻击面。侧信道攻击主要手段是通过攻击面获取数据，推导获得控制流和数据流信息，最终获取 Enclave 的代码和数据信息，比如加密密钥，隐私数据等等。

在DC网络框架下，受到侧信道攻击威胁的是节点 TEE 中的核心敏感数据，也就是 TEE 的私钥。一种可行的抵御侧信道攻击方法是在程序的源码层面引入增强的密码学算法，比如使用增强的椭圆曲线和 AES 算法等。基于以上源码层面的增强实现数据流和控制流的隐藏，可以有效地保护节点 TEE 内敏感数据。

15.2. SGX-ROP 攻击

ROP 全称为 Return Oriented Programming（面向返回的编程）是一种新型的基于代码复用技术的攻击，攻击者从已有的库或可执行文件中提取指令片段，构建恶意代码。通过扫描已有的动态链接库和可执行文件，攻击者提取出可以利用的指令片段(gadget)，这些指令片段均以 ret 指令结尾，即用 ret 指令实现指令片段执行流的衔接。进行 SGX□ROP 攻击，需要将恶意程序加载进入 TEE 下执行，从而对主机造成破坏，并且恶意程序防护软件无法从 SGX Enclave 扫描到有用信息。

DC是一个开源框架，社区内发布的任何程序代码和来源均可以被审查，因此从根本上杜绝了恶意代码破坏节点主机的可能性。与此同时，ROP 攻击主要针对本地系统，如果节点 TEE 内嵌入恶意代码，则无法生成被DC网络认可的远程证明,它将无法通过入网校验，整个网络不会受到影响。

15.3. PlunderVolt、VoltPillager 攻击

PlunderVolt 和 VoltPillager 分别从软件和硬件对 SGX 的加密秘钥进行攻击，这种攻 击本质上都是通过操控处理器电频电压，对Intel高级加密指令注入可控的硬件故障并导致其错误的输出，使得攻击者可以在 enclave 之外恢复加密秘钥。DC的工作量上报机制、文件封装机制以及 MetaData 封装保存都依赖于 ECC、AES 等加密算法。为了避免节点通过 PlunderVolt 或 VoltPillager 攻击获取到私钥从而进行工作量报告伪造，DC将整个DCNode作为单独的Enclave运行,使得攻击者即无法操控输入,也无法获得任何输出,从根源上了避免了PlunderVolt、VoltPillager 攻击。

15.4. 最坏情况

DC可以抵御目前已知的 SGX 安全漏洞，但对未来潜在的威胁也有一定的防治策略。我们假设最坏情况发生（虽然目前并没有发生的征兆），某个恶意节点攻破 SGX 并获取到了节点私钥，这就意味着节点可以随意伪造 TEE 软件和硬件环境证明。

- 工作量伪造：可能伪造文件完整性校验信息，导致**DC**数据没有被真实存储。
- 假节点入网：可能进行虚假验证，从而导致包含恶意代码的节点加入网络。

应对方案

1. 设定一个合理的单点存储上限
   通过限制单节点存储量达到限制虚假算力，从而控制有效的恶意攻击对网络的影响
2. 基于 RICS-V 的 TEE 解决方案
   目前主流 TEE 解决方案因为不开源而遭受挑战。不开源，意味着可能的漏洞和后门，而 RICS-V 开源指令集架构则可以从根源解决这个问题。随着基于 RICS-V 的TEE 解决方案的不断成熟，**DC**未来也将支持基于 RICS-V 的 TEE 解决方案。

16. 技术演进

DC着力于协议的制定和持续完善，并对新技术和新参与者保持开放的态度。 除了前文提及的技术实现，还有一些工作可以为**DC**带来成长，这些工作包括但不 限于：

- 支持多种TEE解决方案: **DC**早期主要基于Intel SGX技术，未来**DC**将会通 过TEE抽象层接入各种解决方案，比如ARM芯片的 rustZone、AMD的SEV、基于 TPM 模块的 Software TEE 以及未来的基于RICS-V的TEE方案。
- 支持计算的量化: 基于 TEE 的支持，比如基于 TEE的代码混淆算法，一些类似 FaaS 任务的去中心化执行可以被量化。
- 支持完善的链上治理: 为了更好的满足技术和生态的进步，**DC**将会开放公平高效 的去中心化的链上治理。
- 接入Web3生态: **DC**可以解决Web3生态中的所有去中心化云服务场景，同时也将 获得Web3生态带来的生态加速。