

极数链(Extreme Data Chain)白皮书

高性能、高安全、支持大数据协作共享的新型分布式网络

极数链团队

V1.0

2018 年 1 月 30 日

目录

1 项目背景	1
2 竞争优势	2
2.1 支持高速率交易的创新体系架构	2
2.2 具有更高安全性的新型共识机制	2
2.3 安全的异构智能合约	3
2.4 完善的分布式大数据协作共享机制	3
2.5 国际一流的抗量子密码算法	3
2.6 友好的应用生态体系	4
3 总体实现方案与关键技术	4
3.1 总体实现方案	5
3.2 XDC 体系结构与共识机制	6
3.2.1 XDC 体系结构	6
3.2.2 交易模式	7
3.2.3 XDCM 共识机制	9
3.2.5 运行实例	13
3.3 智能合约体系	14
3.3.1 虚拟机机制	14
3.3.2 智能合约审计	14
3.3.3 异构智能合约	15
3.4 基于风筝模型的存储与计算	18
3.5 抗量子密码算法	19
4 效能分析	20
4.1 交易性能分析	20
4.2 安全性能分析	20
4.2.1 双花攻击	20
4.2.2 Sybil 攻击	20
4.2.3 预先生成攻击	21
4.2.4 >50%攻击	21
4.2.5 其他攻击	21
4.3 性能安全度分析	21
5 极数链应用场景及生态构建	22
5.1 大数据领域	22
5.2 物联网领域	23
5.3 其他领域	23
5.4 应用生态体系	24
6 极数链开发线路图	25
7 经济激励模型	25
7.1 激励原则	25
7.2 发行细则	26

7.3 筹集用途及相关计划	28
8 发行团队	28
8.1 发起人团队	28
8.2 投资人	29
8.3 法律顾问	29
8.4 产品技术团队	30
9 参考文献	33

1 项目背景

区块链技术有望成为继蒸汽机、电力、信息和互联网科技之后，最有潜力触发新一轮颠覆性革命浪潮的技术。区块链引领我们敲开了“价值互联网”的大门。互联网的出现，使信息传播手段实现了飞跃，信息可以不经第三方、点对点的实现在全球范围的高效流动。而价值传递的效率，却还没有得到同步的提升。区块链的诞生，正是人类构建对等于信息互联网的价值互联网的开始。价值互联网将为整个人类社会进入透明的、可靠的信用社会奠定基础。

区块链展现出巨大的应用潜力，越来越多的区块链底层基础设施产生，也有部分应用开始落地，但是区块链的应用仍然存在很多技术瓶颈。其中，应用数据的存储和交易吞吐率(其指标为 **Transactions Per Second ,TPS**)以及系统的安全性威胁是三大主要瓶颈。以比特币为例，目前比特币区块链上的交易数据已经超过 **130G**，比特币上节点想要完成验证其他节点交易的任务，正常情况下，此节点需要存储至少 **130G** 的数据，这会对节点造成很大的压力。比特币上的数据还仅仅是简单的转账交易数据，数据格式统一，如果区块链中的应用数据更加多样化，无疑会对验证节点造成更大的压力。同样，交易吞吐率也严重制约区块链应用落地，例如在基于以太坊的 **CryptoKitty** 游戏出现的时候，以太坊网络出现了严重的拥堵，导致很多笔交易长时间无法得到确认，严重影响了用户的体验。当区块链中同时有多个大规模的应用接入时，现有的区块链模式显然是不能胜任的。

国内外众多团队在这些方面进行了深入研究，取得了一定的成果，但是并没有带来实质性的改变，这也是目前缺少区块链杀手级应用的重要原因。传统的公有链，无论采用工作量证明(**Proof of Work, PoW**)共识机制，股权证明(**Proof of Stake, PoS**)共识机制，还是授权股权证明(**DPoS**)共识机制等其他共识机制，受到记账人节点机器性能、记账人节点的网络宽带、区块容量等固有条件的限制，很难达到现实应用的要求。有向无环图(**Directed Acyclic Graph, DAG**)为解决传统区块链面临的问题提供了思路。**DAG** 以单笔交易作为出发点，以网络结构代替链式结构，交易可以并发产生，同时交易的验证也可以并发进行，理论上可以满足现实应用的要求。但是目前以 **DAG** 为组织结构的公有链系统中或多或少都存在

问题，其中安全性和中心化问题是主要的问题。在这种情况下，XDC 应运而生。XDC 是高性能、高安全、支持大数据协作共享的新型分布式网络，提供公有链底层基础设施。在 XDC 中，DAG 作为系统的底层交易组织形式。在此基础上，通过创新的极数共识机制，以动态分层、异构冗余的思想，达到对交易的快速确认，同时保证系统的安全性。XDC 拥有一个自有的分布式大数据协作共享生态，打造新的基于公有链技术的数据处理生态，同时能够为通过 XDC 公有链技术进行的数据操作进行安全保护。XDC 的愿景是成为一个区块链商业场景落地的基础设施，同时成为区块链 3.0 生态的有力竞争者。

2 竞争优势

2.1 支持高速率交易的创新体系架构

XDC 交易模型采用被动 DAG 架构，交易可以并发进行。同时交易的验证与共识同时并发进行，按照主动 DAG 架构，交易速度可以满足目前应用的需求。目前比特币理论上每秒最多可以处理 7 笔交易，以太坊可以每秒处理 15 笔交易，而实际上，这两个系统真实处理交易的能力远远达不到理论值。而目前采用 DAG 结构的新型区块链系统，尽管理论上可以每秒钟处理上万笔交易，但是受到其他条件的限制，例如 IOTA 受到中心协调器的限制，byteball 受到主链以及见证者的限制，其实际的交易处理速率也比较慢。XDC 采用创新的体系架构，利用新型的共识机制和交易发送机制，理论上每秒交易处理数量可以至少达到万级，且随着接入节点的增多，交易处理能力会进一步增强。并且 XDC 实际交易处理速率在目前的区块链系统中是最优的。

2.2 具有更高安全性的新型共识机制

目前采用 PoW 的比特币等典型区块链具有较好的安全性。而采用 DAG 模式的新型区块链系统面临着中心化以及严重的安全性问题。XDC 采用分层动态共识机制，同时结合随机、异构、冗余的思想，利用工作量证明初步共识，防止垃圾交易。然后利用改进的动态异构的投票共识机制对系统的记账权进行投票表

决。可以同时防御系统接入节点的内部攻击和系统外部的黑客攻击，比单纯采用 PoS、DPoS 的区块链系统或者现在 IOTA、Byteball 等 DAG 结构的系统具有更好的安全性。

2.3 安全的异构智能合约

智能合约扩展了区块链的应用宽度，加速了区块链应用的落地。但是智能合约的安全问题也制约了区块链的进一步发展，例如以太坊中 THE DAO 事件,多重签名钱包 Parity 事件等都对以太坊区块链造成了巨大的损失。因此 XDC 重点考虑了智能合约的安全问题，研究得到目前大多数区块链中的智能合约都采取“开放”的策略，用户可以自己随意提交智能合约，缺少对提交的智能合约的代码审查。之前智能合约出现的问题大多都是代码问题，因此 XDC 首先加入了智能合约的审查模块，对提交的智能合约进行安全审查，初步拒绝存在安全漏洞的智能合约。并且重点增加了智能合约的形式化验证模块，从根本上确定提交的智能合约的安全性。其次我们在系统中增加了异构的智能合约体系，从代码异构的角度进一步增加了攻击者的攻击难度。

2.4 完善的分布式大数据协作共享机制

XDC 支持基于用户权益凭证的大数据协作共享的应用场景。XDC 采用数据和区块的松耦合涉及原则，采用远程锁定的方式支持多方数据的协作和共享。实现基于用户权益凭证控制数据的访问。将应用数据从区块链中剥离，保留了区块链系统安全、去中心化的特征的同时，又减少了区块大小，提高了系统的可扩展性。相对于增加区块容量的数据存储方案，XDC 节点存储门槛低，降低了系统维护成本，便于 XDC 在各种不同的设备部署。

2.5 国际一流的抗量子密码算法

量子计算机的出现将对传统密码带来致命的打击。区块链的安全很大程度上取决于公钥密码体系的安全性，因此一旦量子计算机能够实用化，区块链的安全性将受到致命的威胁。目前的抗量子密码算法，主要有基于 Hsah 函数的数字签

名方案、基于纠错码的密码和基于格的密码等。这些密码体制大多依赖于复杂的计算结构，对计算能力的要求较高，并且时间复杂度很高，对区块链的性能带来较大的影响。但是考虑到量子计算机的出现将是瞬间的操作，因此为了应对量子计算机的威胁，我们必须提前布置抗量子计算密码。XDC 采用敏捷加密的技术内嵌抗量子计算密码模块，可以随时代替现有的公钥密码模块，并且不需要重写其他事务。

在抗量子签名算法中，基于格上带错误学习的困难问题（LWE）的签名算法具有更好的安全性和效率。为了进一步提高效率，我们基于 LWE 提出了格上的新概念，用于规范构建格上密码体制。以此为基础的抗量子密码算法能够无缝对接到 XDC 的体系结构中。

2.6 友好的应用生态体系

为了更友好的支持商业场景落地，满足未来商业场景的需要，XDC 从接入体验到底层平台均采用 API 级别设计。用户通过 SDK&API 可以实现快速接入区块链。XDC 友好的底层平台完全支持全世界知名的云计算平台的开发架构，简化了商业场景下的应用开发难度。与 EOS 或以太坊、比特币等其他公链平台不同，为了满足不同行业的需要，XDC 内置了多种固定模块，给用户提供最基础的配置资源，其中包含共识算法、数据结构、基础带宽、网络服务、代币配置系统、业务接入系统，并且灵活可配置，用户可以直接进行配置实现，使用区块链上的服务。

3 总体实现方案与关键技术

XDC 公有链将成为新生代互联网大数据的协作共享生态系统，通过完善的设计，来实现和比特币、以太坊一样的长期技术演进，以及与以太坊虚拟机相兼容的特性。除此之外，XDC 系统注重去中心化应用的开发，通过吸引第三方开发者加入，一起为普通用户提供移动端的去中心化应用，所有根据 XDC 底层分布式存储系统开发的第三方应用，XDC 将通过完善的评价体系，给予开发者激励。

XDC 系统的初始设计目标是:构建一个超级友好的区块链公有链系统来为大数据分布式存储与应用进行构建,让全世界的第三方开发者、行业用户、普通用户共建 XDC 平台和生态系统。

目前采用 PoW 或者 PoS 等共识机制的传统区块链面临着共识耗时长等问题,而采用 DAG 模式的新型区块链系统,解决了共识耗时长的问题,但是同时也带来了相关的安全性问题以及中心化问题。

XDC 借鉴了 DAG 模式中的核心思想,同时利用动态、异构、冗余的思想,结合 Hashgraph 的技术特点,在进一步提高共识速度的基础上,比现有 DAG 模式的区块链具有更强的安全性。

3.1 总体实现方案

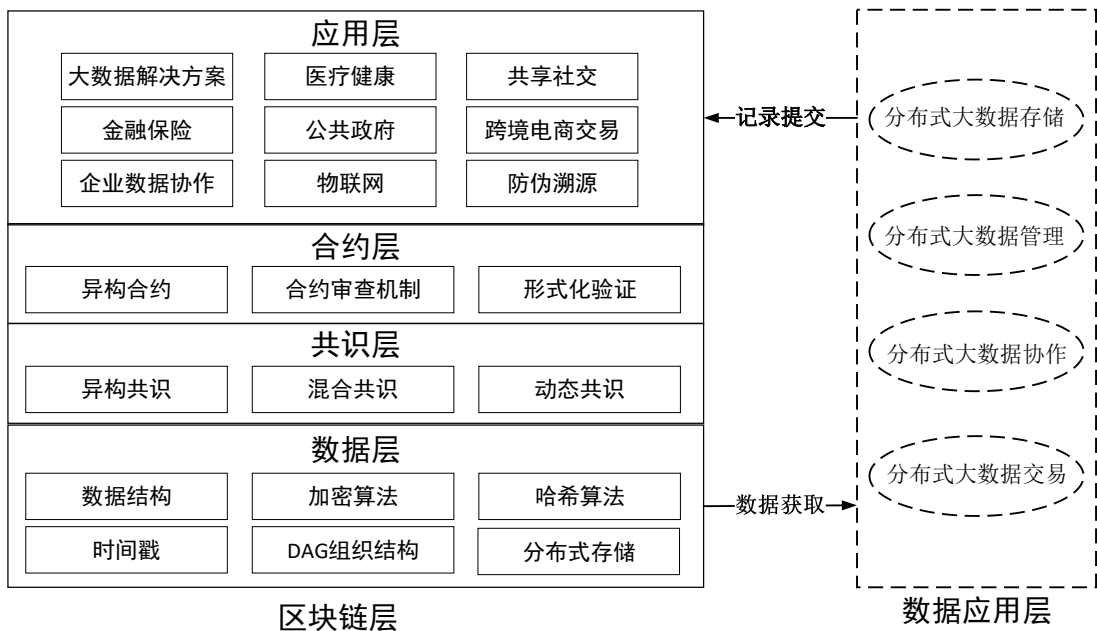


图 1 XDC 体系架构

图 1 给出的 XDC 体系结构由数据层、共识层、合约层、分布式大数据存储层和应用层构成。在数据层中,数据结构是对系统中交易信息的组织结构,因为 XDC 面向不同的应用领域,对数据的组织结构要求不同,因此数据层中包含多种类型的数据存储格式,且面对用户接入应用的特点,自动分配合适的数据结构。加密算法主要包块交易发送与接收过程中的交易信息的加密,同时还包含对大数据分布式存储与应用过程中数据的加密,主要是公钥密码体系,同时以敏捷加密的技术内嵌着抗量子加密模块。哈希算法主要完成对数据的压缩,完成区块链上

的记录以及大数据的索引操作。时间戳是为了对系统中的操作进行时间映射，以便完成校验与溯源。DAG 组织结构是整个系统的核心，以交易为出发点，并使得对系统交易网络进行拓展。在共识层中，混合共识与异构共识的加入，使得共识过程更加安全同时更加快速。在合约层中，异构智能合约和智能合约审查机制以及形式化验证机制使得智能合约的使用更加安全。

3.2 XDC 体系结构与共识机制

3.2.1 XDC 体系结构

XDC 的体系机构主要由交易发行和交易验证构成，交易验证的过程也就是 XDC 的共识过程。体系架构如图 2 所示。

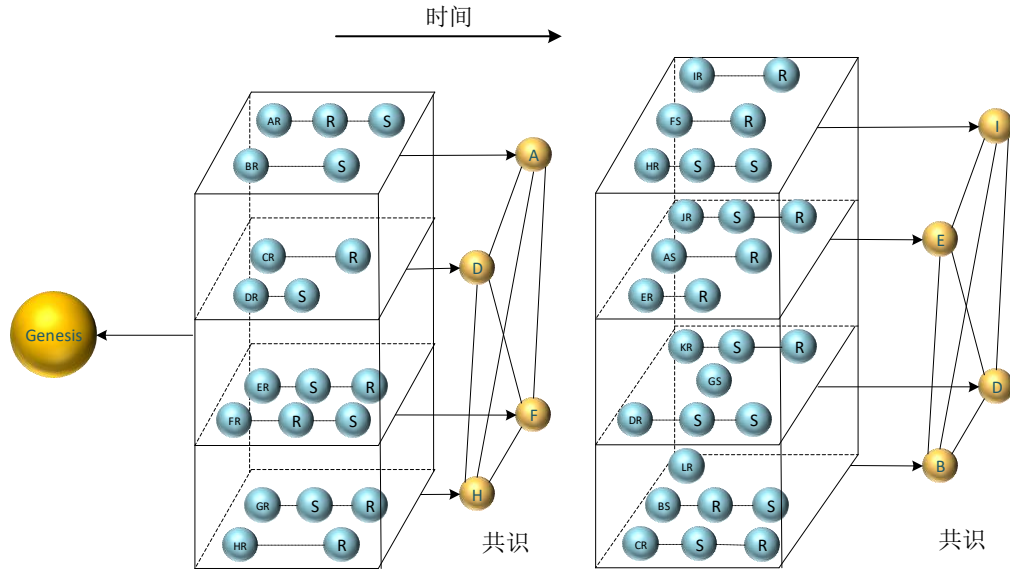


图 2 XDC 体系架构

图中蓝色的球表示进行的交易，系统中总的节点总数为 n 。每一条虚线代表一个节点，节点的交易包含收入(R)和输出(S)，具体交易模式在 3.2.1 节介绍。每一个分长方体表示一个分组，分组总数为 m 。分组规则在 3.2.2 节介绍。分组情况在一定时间后会进行一次调整，由于分组的过程由密码学安全的函数控制，因此在分组产生之前，任何人都无法知道具体的分组情况，增强了系统抵御黑客攻击的能力。黄色的球代表当前轮的共识代表，共识代表的产生同样在 3.2.2 节介绍。

令系统中的所有参与节点为 $P_i (i=1,2,\dots,n)$ ，共识代表为 $Cr_j (j=1,2,\dots,m)$ 。

节点 P_i 发出的交易为 $Tr_i^j (j=1,2,\dots,n_i; i=1,2,\dots,n)$, 交易 Tr_i^j 历经的验证次数为 TN_i^j , 交易 Tr_i^j 发出时, 节点 P_i 所在的层为 $L_i^{i_k} (1 \leq i_k \leq m)$, 交易 Tr_i^j 的认可值为 $V_i^{i_k}$, 交易认可阈值为 Th 。系统的参数表示为:

$$S = \left\{ \left[P_1 \left(Tr_1^1 (TN_1^1, L_1^1, V_1^1), Tr_1^2, \dots, Tr_1^m \right), P_2, \dots, P_n \right], [Cr_1, Cr_2, \dots, Cr_m], Th \right\}$$

当节点 P_i 发出一笔交易时, 首先将交易发送给 $Cr_{L_i^{i_k}}$, 然后 $Cr_{L_i^{i_k}}$ 将接收到的交易消息按照 3.2.2 给出的顺序传递算法, 参照 HashGraph 的传播原则, 对交易集合进行验证, 验证流程同样在 3.2.2 节进行介绍。

3.2.2 交易模式

在传统的区块链中, 数据的存储代价是交易验证者面临的一个重要难题。以比特币为例, 目前比特币的全网交易数据已经超过了 130G, 如果一个节点想要参与比特币中交易的验证, 那么正常情况下, 此节点需要存储超过 130G 的数据, 这无疑会带来巨大的开销。而 XDC 面向的是多种表现形式的大数据的多态应用, 无疑会在数据规模、数据类型上远远超过比特币, 因此如果 XDC 采用传统的区块链结构, 会对交易的验证者带来巨大的挑战, 影响系统的性能与安全。

XDC 中交易发行传播采用 DAG 的组织形式, 交易模式采用传统的余额模式, 一个账户向另一个账户进行转账时, 首先需要完成一定的工作量证明, 这里的工作量证明是为了防止垃圾交易, 难度很低, 普通节点也可以轻松完成。交易中主要包含输入地址, 输出地址, 交易值, 交易时间戳, 输入地址对应的前一笔交易的哈希值, 输入地址对应的余额, 输入地址对应的用户的签名, 以及交易的哈希值。交易模式如图 3 所示。

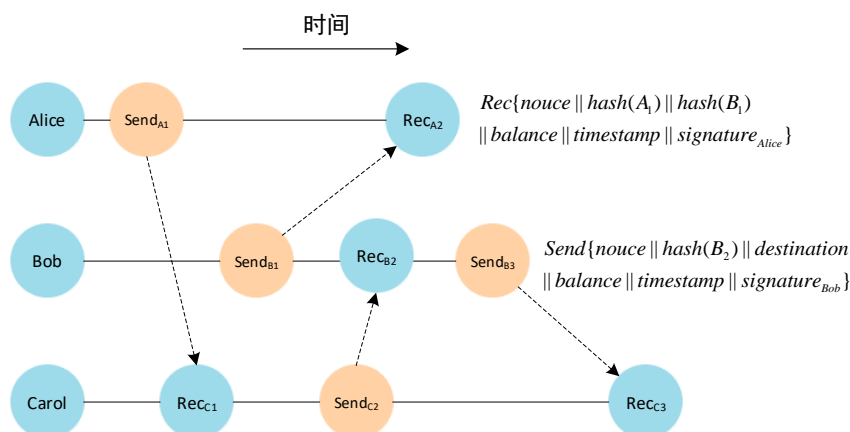


图 3 交易结构

当 Alice 给 Carol 发送一笔交易时，Alice 的账本中产生一个发送交易，而 Carol 产生一个接收交易。同时 Alice 将交易发送给 Alice 所在层当前轮的验证代表。其他的交易按照相同的模式进行。

核心代码

```
//
//filename: dag.go
package core
import (
    "errors"
    "xdc/go-xdc/common"
    "xdc/go-xdc/core/types"
    "xdc/go-xdc/core/state"
    "xdc/go-xdc/rpc"
)
// 定义图的一个节点
type Node struct {
}
// 定义图的一条边
type Edge struct {
}
// 定义 DAG 图的节点和边
type DAG struct {
}
// 给 DAG 增加一个节点
func (d *DAG) AddNode(n Node) (err, errors) {
}
// 给 DAG 增加一条边
func (e *DAG) AddEdge(e Edge) (err, errors) {
}
```

3.2.3 XDCM 共识机制

XDC 中交易采用 DAG 的组织形式，由于缺少集中竞争的共识模式，容易出现双花、伪造交易等情况。极数共识机制采用动态分层的共识策略，并且结合随机、异构、冗余的思想。每层的共识代表在某段时间内是保持不变的，当需要对共识代表进行调整时，在每一层中都存在一个判断函数，函数以此时的系统参数等其他对象作为输入，对于每一次输入，判断函数都会输出一个值，这个值决定了此轮共识本层的共识代表。由于这个判断函数是密码学上安全的，因此在共识开始之前，包含攻击者、诚实者，甚至将要参与共识的节点本身都不知道具体参与共识的节点，因此可以在很大程度上解决外部黑客对共识算法的攻击。并且，为了进一步增加系统的安全性，XDC 采用了异构的思想，在某一轮中，参与共识的所有 n 个节点按照 m 种不同的选取规则分成 m 组，在每一组中，按照某种规则，选取 1 个代表，所有选出的 m 个代表对交易进行投票，且这 m 个共识代表分别由 m 个不同的密码学上安全的函数决定。

XDC 的共识机制被设计成模块化，是可以扩展和插拔的分层组件。目前存在的公有链很难适应多个大规模的应用，共识成本过高、51%攻击问题、存在的分叉可能等问题也影响了公有链系统的安全性和可用性。XDC 采用的极数共识机制，一方面可以在接入多个大规模应用的条件下，良好运行。另一方面系统可以在安全的前提下高速完成共识。

XDC 共识代表产生规则中，共识代表的产生是由当前轮本层的节点的地址集合、随机数 $n_i (i=1,2,\dots,m)$ 以及 q 个接入应用和系统的参数以及判断规则产生。这里的判断规则主要包括节点的信誉值、节点拥有的币龄值、节点的活跃度等。当在某一轮共识过程中，某个共识节点没有完成自己共识，或者有恶意行为，此节点相应的特征值会得到大幅度降低，从而降低了这个节点再次参与共识的可能性。共识节点产生过程由式(1)给出

$$\begin{cases} Cr_1 = P_1 \xrightarrow{f_1\left(\left\{P_{t_1}^1, P_{t_1}^2, \dots, P_{t_1}^{n_1}\right\}, n_1, r_1, r_2, \dots, r_q, w_1\right)} Cr'_1 = P'_1 \\ Cr_2 = P_2 \xrightarrow{f_2\left(\left\{P_{t_2}^1, P_{t_2}^2, \dots, P_{t_2}^{n_2}\right\}, n_2, r_1, r_2, \dots, r_q, w_2\right)} Cr'_2 = P'_2 \\ \dots \\ Cr_m = P_m \xrightarrow{f_m\left(\left\{P_{t_m}^1, P_{t_m}^2, \dots, P_{t_m}^{n_m}\right\}, n_m, r_1, r_2, \dots, r_q, w_m\right)} Cr'_m = P'_m \end{cases} \quad (1)$$

为了更好的体现共识产生规则的随机性，随机数 $n_i (i=1,2,\dots,m)$ 的选取很重要。之前在很多区块链社区，有人讨论过使用比特币每个区块的区块头部的 Hash 值来构建随机数。但是，当比特币网络的出块时间有大幅抖动时，构建随机数的过程将变得复杂。在 XDC 中，随机数的产生采用两阶段公布随机数的方案，通过引入激励机制，利用承诺协议(Commitment Protocol)和多阶段交和博弈机制，来保证随机数产生的公平性。

当产生交易时，交易发起者首先将交易发送给自己所在组的共识代表，此共识代表按照某种顺序将自己收集的所有交易按照一种顺序传送算法进行传送。

顺序传送算法：

令交易产生的节点所在的层数为 $L_i (i=1\leq i\leq m)$ ，交易已经历的验证次数为 $N_j (j=1\leq j\leq m)$ ，则下一次交易传送的层数为 $L_i + N_j + 1 \bmod m$

在验证的过程中，如果共识代表认可收到的交易（可能是一笔交易，也可能是多笔交易），则共识代表对其进行签名，此时，这部分交易的认可值相应得增加共识代表所持有的权重。如果共识代表不认可收到的交易，则不进行签名，交易的认可值不变。如果某笔交易的认可度在共识过程中超过了某个阈值，则认为这笔交易共识成功，否则，当所有 m 个共识代表表决完成之后，判断交易共识失败。其过程如图 4 所示。

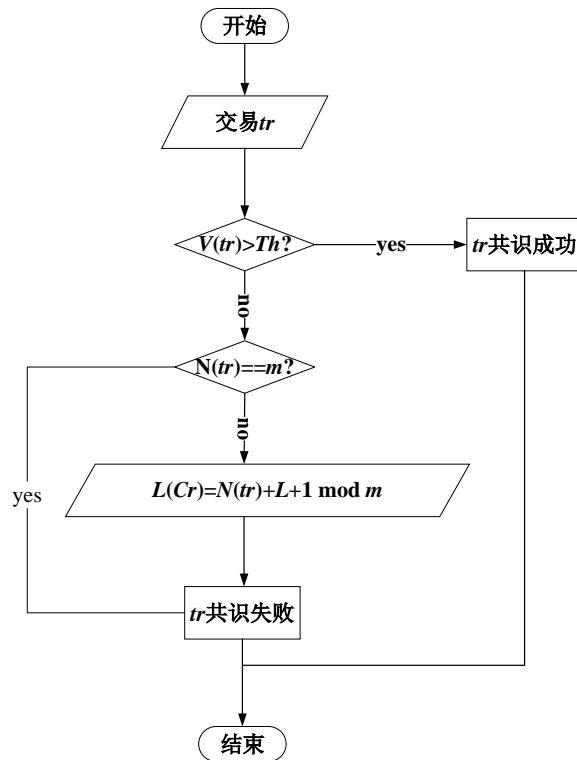


图 4 XDC 交易共识流程

核心代码

```

//
//filename: certificate.go
package kite
import (
    "errors"
    "xdc/go-xdc/common"
    "xdc/go-xdc/core/types"
    "xdc/go-xdc/core/state"
    "xdc/go-xdc/rpc"
)
// 凭证
type Certificate struct {
}
// 用户
type User struct {
}
// 检查凭证的有效性
func (c *Certificate)Verify(c Certificate) (err errors){
}
// 检测数据块能否被授权
func (c *Certificate)Authorize(u User) (err errors) {
}
// filename: consensus.go

```

```
package consensus
import (
    "xdc/go-xdc/common"
    "xdc/go-xdc/core/types"
    "xdc/go-xdc/core/state"
    "xdc/go-xdc/rpc"
)
// 定义访问 DAG 图的 method 集合
type DAGReader interface {
    // 获取 DAG 的配置信息
    Config() *params.GraphConfig
    CurrentHeader() *types.Header
}
// Engine 适用于异构 XDCM 算法引擎
type Engine interface {
    // Verify 用于检查该引擎是否匹配 XDC 共识的规则
    Verify(reader DAGReader)
    SelectbyStack(reader DAGReader)
    SelectbyActivity(reader DAGReader)
    SelectbyPow(reader DAGReader)
    APIs(reader DAGReader) []rpc.API
}
//
//filename: xdc.go
package consensus
import (
    "errors"
    "xdc/go-xdc/common"
    "xdc/go-xdc/core/types"
    "xdc/go-xdc/core/state"
    "xdc/go-xdc/rpc"
)
// Verify 用于检查该引擎是否匹配 XDC 共识的规则
func (f *Engine) Verify(reader DAGReader) (err errors) {
}
// 基于股权的代表选择
func (f *Engine) SelectbyStack(reader DAGReader) (err errors) {
}
// 基于活跃度的代表选择
func (f *Engine) SelectbyActivity(reader DAGReader) (err errors) {
}
// 基于算力的代表选择
func (f *Engine) SelectbyPow(reader DAGReader) (err errors) {
}
```

```
// 执行 XDCM 操作
fucn (f*Engine) Execute(readr DAGReader) (err errors) {
}
```

3.2.5 运行实例

假设 $n=100$ ，即系统中共有 100 个节点， $m=3$ ，即系统被分为 3 层。

第一步：对 100 个节点利用分层规则函数进行分层。得到集合 $\{L_1(P_1^1, P_1^2, \dots, P_1^{s_1}), L_2(P_2^1, P_2^2, \dots, P_2^{s_2}), L_3(P_3^1, P_3^2, \dots, P_3^{s_3})\}$ ，其中 $s_1 + s_2 + s_3 = 100$ 。

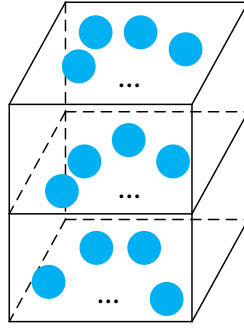


图 5 系统分层

第二步：得到共识代表。在每一层中利用不同的判断函数选取 1 个共识代表，记为 Cr_1, Cr_2, Cr_3 。

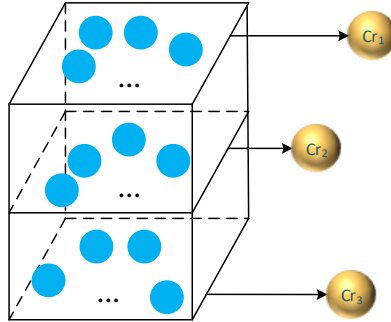


图 6 共识代表产生

第三步：假设 L_1 中 P_1^1 发出交易 Tr_1^1 ， P_1^2 发出交易 Tr_1^2 ， L_2 中 P_2^1 发出交易 Tr_2^1 ， P_2^2 发出交易 Tr_2^2 ， L_3 中 P_3^1 发出交易 Tr_3^1 ， P_3^2 发出交易 Tr_3^2 。则 Tr_1^1, Tr_1^2 首先发给 Cr_1 ， Tr_2^1, Tr_2^2 首先发给 Cr_2 ， Tr_3^1, Tr_3^2 首先发给 Cr_3 。 Cr_1, Cr_2, Cr_3 分别进行判别之后， Tr_1^1, Tr_1^2 发给 Cr_2 ， Tr_2^1, Tr_2^2 发给 Cr_3 ， Tr_3^1, Tr_3^2 发给 Cr_1 。然后 Tr_1^1, Tr_1^2 发给 Cr_3 ， Tr_2^1, Tr_2^2

发给 Cr_1 , Tr_3^1, Tr_3^2 发给 Cr_2 。在此过程中，一旦某笔交易的认可值超过阈值，则断定此交易共识成功，并不再继续进行共识过程，否则共识结束，判断此交易共识失败。

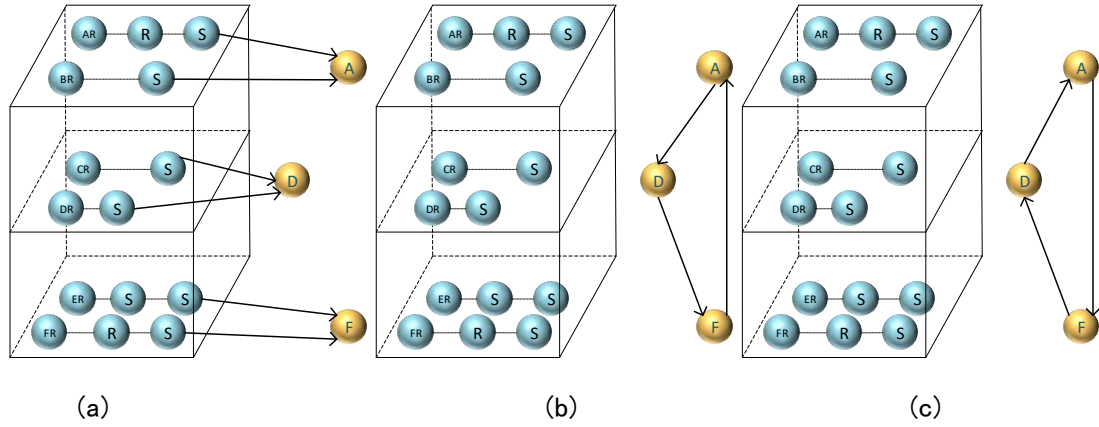


图 7 交易共识

第四步：分层调整。假设目前已有 200 个节点，对 200 个节点利用分层规则函数进行分层。得到集合 $\{L_1(P_1^1, P_1^2, \dots, P_1^{s_1}), L_2(P_2^1, P_2^2, \dots, P_2^{s_2}), L_3(P_3^1, P_3^2, \dots, P_3^{s_3})\}$ ，其中 $s_1 + s_2 + s_3 = 200$ 。在每一层中利用不同的判断函数选取 1 个共识代表，记为 Cr_1, Cr_2, Cr_3 。在第一步和第四步之间新加入的节点暂时采取随机选取的规则，加入某一层。

3.3 智能合约体系

3.3.1 虚拟机机制

XDC 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。在 XDC 系统中，我们同样采用虚拟机机制，XDC 合约解析器类似于以太坊网络的 EVM，主要作用是简化因合约解析而带来的时间消耗成本以及链下规则确定执行的成本。

3.3.2 智能合约审计

XDC 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。

3.3.3 异构智能合约

目前 80-90%的合约都使用 solidity 语言编写，XDC 的智能合约主要采用 solidity 语言编写，可以运行在属于 XDC 自己的虚拟机上（SVM），并且符合 ERC20 标准，支持跨链执行。ERC20 让 XDC 区块链上的其他智能合约和去中心化应用之间无缝交互。在一些对安全性要求高的场景中，XDC 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。

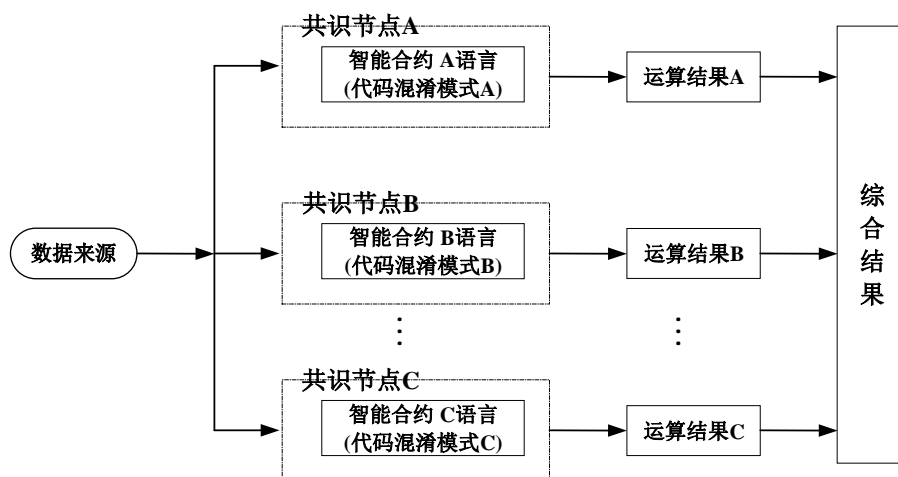


图 7 异构智能合约

核心代码

```

/**
 * 合约解析器
 */
package com.xdc.contract.analyzer;
public class AnalyContract {
    /**
     * 执行者
     */
    public static void executor() {
        // 目前主流合约编写语言建议使用 solidity,且符合 erc20 标准，这样可以和以太坊合约无缝兼容；
        // 解析合约字节码
    }
}

```

```
package com.xdc.contract.compiler;
/**
 * 编译器
 * 基于公链的虚拟机执行编译
 */
public class CompileContract {
    /**
     * 执行者
     */
    public static void executor() {
        // 根据区块链的虚拟环境，编译当前合约
    }
    public static void audit() {
        // 基于形式化验证的审计
    }
}

package com.xdc.contract.deploy;
/**
 * 部署管理中心
 */
public class DeployContract {
    /**
     * 启动、激发部署
     */
    public static void executor() {
        // 将当前合约部署到区块链的虚拟环境中
    }
    public static void Heterogeneous() {
        // 异构智能合约部署
    }
}

package com.xdc.contract.executor;
/**
 * 合约执行官
 * 基于公链虚拟机
 */
public class ExecutorContract {
    /**
     * 对于合法合约启动执行
     */
    public static void executor() {
        //在虚拟环境中执行该合约
    }
}
```

```
package com.xdc.contract.interceptor;

/**
 * 对于交易中产生的税费、收益、权益等的计算和记录
 */
public class Balance {

    /**
     * 税相关计算
     */
    public static void gas() {
        //1 不同的合约类型，有不同的 gas 点；
        //2 根据当前的合约类型，进行 gas 收取；
    }

    /**
     * 资产收益相关计算
     */
    public static void profit() {
        //1 根据本金，周期，收益率进行计算；
    }
}

package com.xdc.contract.interceptor;

/**
 * 根据业务拦截
 * 做税收、收益等处理
 */
public class Interceptor {

    public static void interceptor() {
        Balance.gas();
        Balance.profit();
        //... ...
    }
}

package com.xdc.contract.transaction;

/**
 * 合约交易管理者
 */
public class Transaction {

    /**
     * 执行者
     */
    public static void executor(){
        transaction();
        calculation();
        //... ...
    }
}
```

```

/**
 * 账户地址数据传输
 */
public static void transaction() {
    //... ..
}
/**
 * 转账计算
 */
public static void calculation() {
    //1 对双方进行转账计算;
    //2 A to B, 增减处理;
}
}

```

3.4 基于风筝模型的存储与计算

XDC 中将数据实体与 XDC 链分离，所有的数据在本地进行加密和签名，进行逻辑或物理分块，将数据块的大小、存储地址（URL 表示）、所有者签名等信息产生哈希凭证。XDC 首先将数据块头信息及其哈希凭证存入链，作为数据完整性和数据产权的凭证。XDC 链控制数据块就像是在放风筝，XDC 根据数据凭证访问云端的数据，像是手握着风筝线，控制着在云端的数据实体。

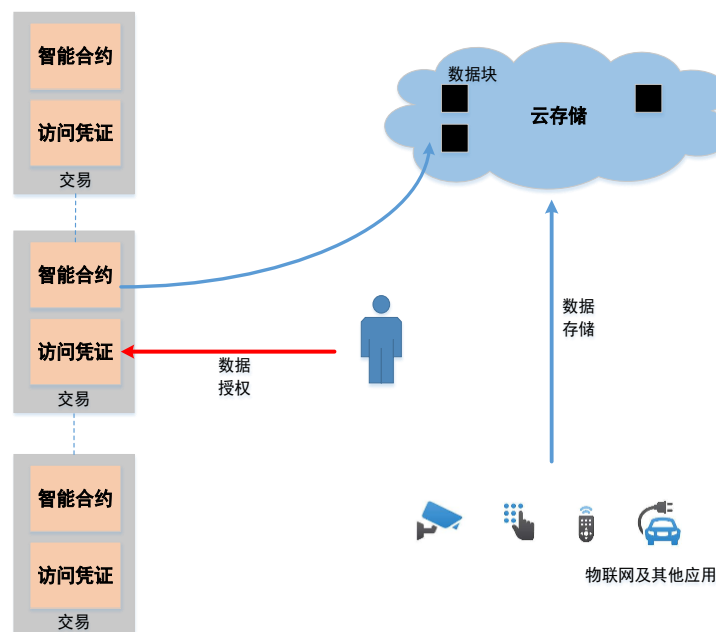


图 8 基于风筝模型的存储与计算

XDC 所支持的多方数据共享协作以保护数据产权为基础。在每一次数据块

的访问中，区块链的智能合约会检查合约方对数据块的访问凭证，只有其访问凭证中包括了数据所有者的授权凭证，交易才能被授权，数据访问才有可能。

为了提升数据访问的性能，提升数据访问的带宽，在 XDC 的数据共享的架构中采用快访（CACHE）和多强度加密两种技术。数据块凭证的 CACHE 机制，对近期访问的数据块的凭证做快速缓冲，智能合约在访问数据块时，先访问 CACHE，如果缓冲击中，则直接访问。由于数据之间往往存在紧耦合的特征，只要参数合理，CACHE 能以较大的概率被击中。此外数据块的加密和解密往往占用较大的带宽，对系统的性能要求较高，在 XDC 中，根据应用场景的要求，可以采用不同强度的密码，对于重要的数据，采用强度高计算量大的密码，对于普通数据采用轻量级密码，提高访问速度。

3.5 抗量子密码算法

目前，后量子时代的到来被认为是一个时间问题，IBM 和 Microsoft 的工程师预计大规模量子计算机有望在未来 15-20 年的时间出现。特别地，IBM 计划在未来几年内建立一个 50 量子比特系统。XDC 为了保证安全，将在量子计算机威胁现有非对称密码体系之前，部署高速抗量子密码模块。

XDC 生态要求签名算法性能不能成为短板。在抗量子密码的分支流派中，基于理想格和 RLWE 的密码方案具有显著的效率优势，在相同的安全级别下，基于 RLWE 的密码方案的效率甚至优于目前的椭圆曲线密码方案。模格是介于一般格和理想格之间的一种格，XDC 的抗量子密码算法 SKE 就是基于模格的密码算法。

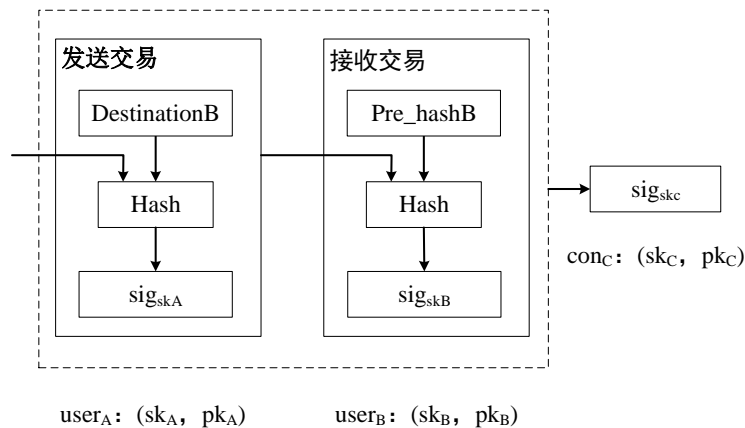


图 9 XDC 抗量子密码模块

用户根据 SKE 自发生成公私钥对，公布公钥和根据公钥生成的地址。每个地址代表一个节点，每个节点产生交易时，需要用私钥对交易全部内容进行签名。节点若被选为共识参与方，则投票信息和转发的验证包也需要节点签名。XDC 抗量子签名算法的出现使得其他人无法通过量子计算机根据公开信息还原私钥，从而保护节点账户的安全。

4 效能分析

4.1 交易性能分析

XDC 采用基于 DAG 的架构，其架构体现了充分的并行性。不同于比特币等链式的区块模型，节点在挖矿竞争的过程中，算力很大程度上被浪费，而且也带来系统交易吞吐率低、确认时间长等问题。XDC 工作量的证明轻量的工作量证明和异构动态投票的混合共识机制，实现高效能的交易吞吐率。

4.2 安全性能分析

像所有的去中心化的加密区块链系统一样，XDC 也会遭到各种攻击，企图获取利益或者使系统奔溃。本节讨论可能遇到的典型攻击场景，以及 XDC 机制中相应的防范措施。

4.2.1 双花攻击

双花 (double spend) 是任何区块链交易系统要解决的重要的安全问题，和现在主流 DAG 的系统不同，XDC 在共识算法上并非由新参与者进行验证，而是采用异构方式在诚实节点中选择投票者，用投票验证的机制保障系统交易信息可信，从而预防双花攻击。

4.2.2 Sybil 攻击

Sybil 是指攻击者创建或控制了众多的 XDC 节点，试图通过投票机制控制系统。由于在 XDC 中的异构投票共识，系统的多种投票机制并行发挥作用，因此

额外增加的节点并不会使得攻击者增加投票权重，Sybil 攻击者不会获得任何额外的优势。

4.2.3 预先生成攻击

由于 XDC 系统采用了轻量算力累加机制，攻击者可能会预先生成连续的区块，并向网络中倾注这些事先生成的交易来执行拒绝服务攻击。XDC 采用两种机制来防范这种攻击，其一是由于系统存在交易费用限制攻击者；其二是每笔新产生的交易都要求包含已经产生的其他交易。

4.2.4 >50%攻击

在比特币的 POW 机制下，如果攻击者控制了 50%以上的算力，从理论将控制整个系统。在单一的 DPoS 机制下，如果攻击者能获得超过 50%的投票权，就会导致网络震荡，甚至系统崩溃。在 XDC 中，采用异构混合 XDCM 投票机制，即共识代表的产生由密码学安全的函数所产生，单一在某方面超过 50%的优势，不会给系统带来震荡。

4.2.5 其他攻击

系统还可能遇到饱和攻击等其他攻击方式。例如攻击者可以在其控制的账号下发送大量合法但确是不必要的交易，试图使得系统饱和而阻塞正常用户的交易。由于 XDC 在交易的过程中使用 gas 作为交易费用，且每次交易需要工作量证明，也限制了攻击者在没有充分的算力资源保障的情况下发起大量的交易。

4.3 性能安全度分析

在类分布式账本的技术中，交易吞吐率和交易安全是两个重要的指标。传统的比特币采用经典 POW 的共识机制，安全性能高但是交易吞吐率低；而现有的基于 DAG 的系统，为了提升交易吞吐率而牺牲了系统安全性。

本文以对系统的攻击成功率来度量安全率 S ， S 的取值范围为区间(0,1)；以归一化的系统吞吐率度量性能 T ，表示本系统的交易吞吐率与已知公认最高的交易

吞吐率的比值。分布式账本的性能安全度 P :

$$P = \frac{T}{S} = \frac{\text{归一化的交易吞吐率}}{\text{安全率}}$$

XDC 所采用的系统构架和安全机制，其宗旨是在保证系统安全性的前提下，构建性能安全度极高的系统。

5 极数链应用场景及生态构建

5.1 大数据领域

大数据是信息化发展的新阶段。随着信息技术和人类生产生活交汇融合，互联网快速普及，全球数据呈现爆发增长、海量集聚的特点，对经济发展、社会治理、国家管理、人民生活都产生了重大影响。世界各国都把推进经济数字化作为实现创新发展的重要动能，在前沿技术研发、数据开放共享、隐私安全保护、人才培养等方面做了前瞻性布局。可以看到，大数据正在成为数字社会治理的基础性战略性资源，但现阶段大数据发展正面临数据开放共享流通难、数据安全与隐私保护难等挑战。区块链是一种不可篡改的全历史数据库存储技术，包含着每一笔交易的全部历史，随着区块链的应用迅速发展，数据规模会越来越大，不同业务场景区块链的数据融合进一步扩大了数据规模和丰富性。但是，区块链提供的是账本的完整性，数据统计分析的能力较弱。大数据具备海量数据存储技术和灵活高效的分析技术，极大提升区块链数据的价值和使用空间。由上可见，区块链技术特点决定其正是大数据资源流通、隐私保护的重要支撑，大数据又是挖掘利用块数据价值的技术手段，区块链 + 大数据，是区块链技术 with 大数据开放共享、个人数据隐私保护等特性的有效融合，真正破解大数据在城市治理中的应用痛点，助力大数据在数字雄安的建设过程中发挥真正价值。

传统的区块链系统在数据存储能力、数据存储灵活度上都存在较大的缺陷，导致区块链+大数据的方案实施面临着诸多技术挑战。并且，传统区块链中数据处理能力很弱，且数据处理代价大，区块链很难进行复杂的数据处理。XDC 内置大数据存储机制，且配置数据处理模块，很好的促进了区块链+大数据的发展。

5.2 物联网领域

物联网(Internet of Things,IoT)是信息领域的一次重要变革,它融合了计算机技术、网络技术、通信技术、传感技术等多种技术。物联网链接智能设备,进行信息的传递和共享,对数据进行智能处理。目前的物联网系统大多采用中心化的模式,存在个人隐私、数据价值、商业模式、连接成本等多种问题。

区块链为物联网的发展带来了新的机遇。利用区块链的去中心化、去信任等特点,基于区块链的物联网平台可以有效解决中心化服务器的问题,拜托“数据孤岛”难题。在个人隐私方面,可以有效解决中心做坏、黑客攻击的问题,用户可以掌控自己的个人数据,保护个人隐私与权益。在数据价值方面,在区块链中,所有的节点都可以利用系统中公开的数据,完成数据分析与利用,实现数据价值的传递。在商业模式方面,在基于区块链的物联网平台中,用户不仅仅是系统的使用者,也可以自主完成其他的角色功能,可以吸引更多的用户接入系统。在连接成本方面,基于区块链的物联网平台是一个集体维护的平台,系统不需要为每种设备提供不同的接口,可以显著降低物联网的连接成本。

目前出现的区块链底层平台在解决物联网问题方面存在几个关键的问题,其中最关键的是数据存储代价高,在以太坊等其他公有链系统中,数据存储能力很弱且存储代价高,并不能满足物联网对数据存储的要求。另外一个共识效率低,无论是采用 PoW 共识算法还是 PoS 共识算法,都需要大量的计算消耗,由于接入物联网的设备大多是轻量级的设备,缺乏足够的计算能力,因此完成共识的效率较低。导致高吞吐量和高并发性的应用并不适合在传统区块链中应用。

XDC 采用 DAG 的组织结构和混合共识机制,可以满足物联网的高并发性和高吞吐量,实现超短时间内的共识并需要的计算能力很低。并且内置的大数据存储机制可以低成本存储物联网产生的数据。

5.3 其他领域

- ◆ 医疗大健康:个人医疗健康解决方案,医药供应链解决方案、医疗数据解决方案、运动健康解决方案;
- ◆ 共享社交:社交解决方案、共享经济解决方案、众筹解决方案;

- ◆ 金融保险：证券交易解决方案、票据解决方案、金融反欺诈解决方案、互
- ◆ 互联网金融监管解决方案、保险解决方案、金融小贷解决方案、数字货币解决方案、供应链金融解决方案；
- ◆ 公共政府：资源共享解决方案、教育就业解决方案、精准扶贫解决方案、公益解决方案、企业征信解决方案、智慧出行解决方案；
- ◆ 电商交易跨境：房地产交易解决方案、电商交易解决方案、跨境交易解决方案；
- ◆ 科技技术：智能制造解决方案、物联网解决方案、投票解决方案、DNS（域名解析）解决方案、游戏解决方案、人工智能解决方案；
- ◆ 防伪溯源：文化娱乐版权解决方案、实物防伪版权解决方案、新媒体确权解决方案、物流供应链解决方案。

5.4 应用生态体系

XDC 团队坚持技术和产业生态同步发展的理念。XDC 作为下一代价值互联网的基础设施，提供了多种不同行业领域的区块链应用级别解决方案，企业可以接入平台快速落地应用。

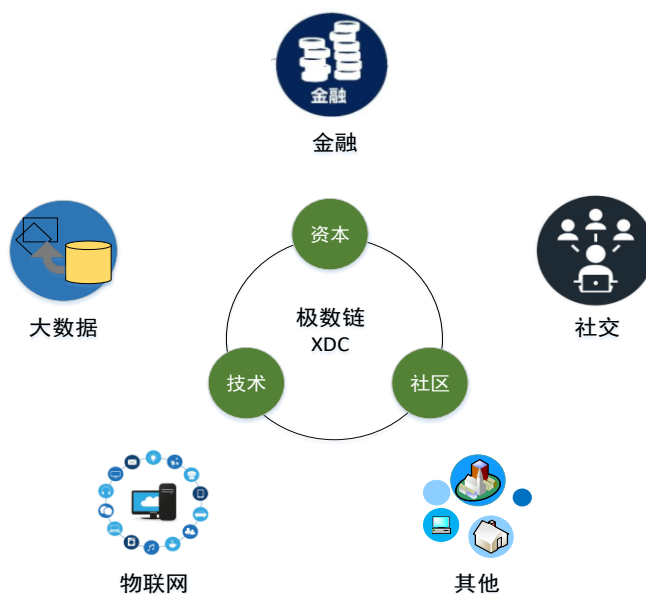


图 10 极数链的应用生态

XDC 以其高效的系统吞吐率和基于数字权益凭证的数据协作技术，并且提供了方便的 DAPP 的开发支持库，方便用户构建基于 XDC 的应用系统。此外，XDC 的开发团队也密切关注创新型去中心化的应用场景和概念，支持这样的应用在 XDC 链上落地。

6 极数链开发线路图

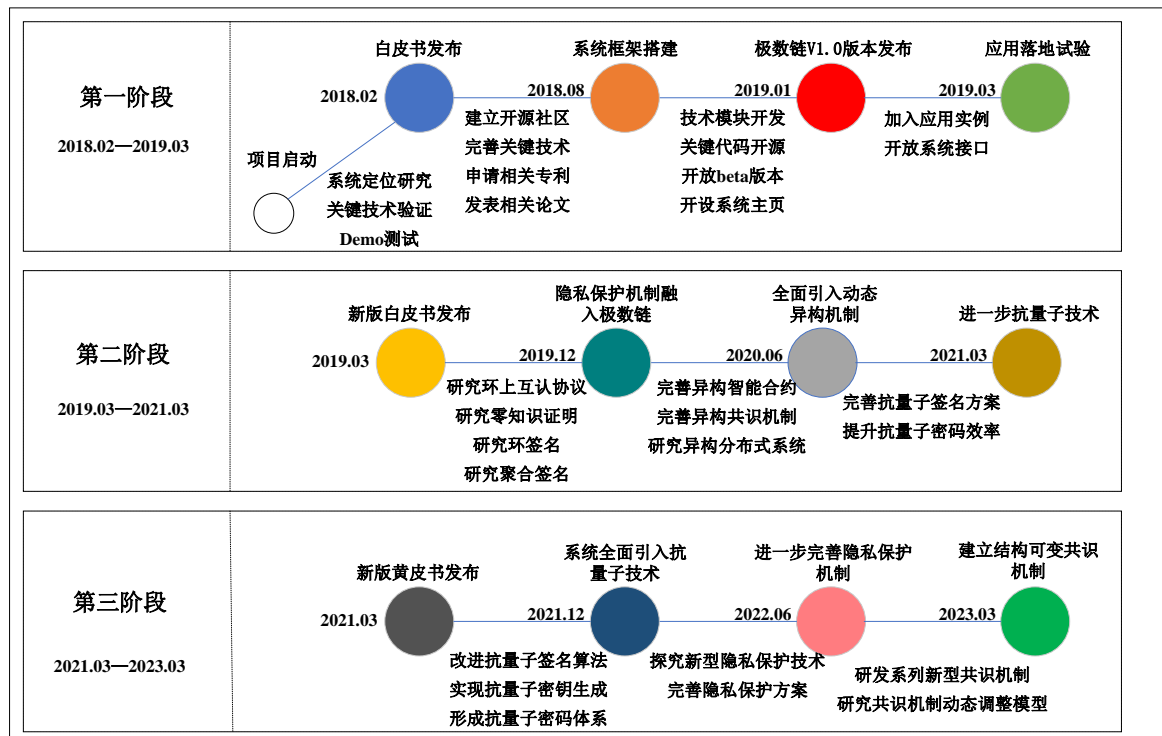


图 11 XDC 开发线路图

7 经济激励模型

7.1 激励原则

- 极数链发币包括“初始发币”和“确认交易奖励”（本文简称挖矿）两个部分；
- 极数币总量控制 ≤ 10 亿个
- 挖矿数量按每年 $\frac{1}{8\sqrt{n}}$ 模型递减， 2019 年 $n=1$, 2020 年 $n=2$, 以此类推。

- 每个系统用户都有机会参与挖币
- 挖币的数量和用户贡献大小成正比

用户的贡献包括 3 个维度：股权数量 x_1 、交易活跃度 x_2 和安全积分 x_3 。贡献函数为 $y = f(x_1, x_2, x_3)$ ，初始阶段 $y = \frac{1}{2}x_1 + \frac{1}{4}x_2 + \frac{1}{4}x_3$ ，由于挖矿的总量为 2 亿个 XDC 币，每年挖掘的数量由下表所示：

表 1 XDC 挖矿比例明细

年度	挖币份额
2019 年（第 1 年）	$\frac{1}{8}$
2020 年（第 2 年）	$\frac{1}{8\sqrt{2}}$
2021 年（第 3 年）	$\frac{1}{8\sqrt{3}}$
...	...
2041 年（第 23 年）	$\frac{1}{8\sqrt{23}}$

节点每次确认交易时，系统会奖励共识节点 XDC 币和交易发起者提供的 gas 费用。

$$\text{由于 } \frac{1}{8} + \frac{1}{8\sqrt{2}} + \frac{1}{8\sqrt{3}} + \dots + \frac{1}{8\sqrt{23}} = 1.0033 \approx 1$$

因此，23 年后挖币完毕。在挖矿完毕后，参与共识的节点收益为用户的交易费用。XDC 中 gas 的价格为动态可调整，交易发起方可以动态设置其价格，系统统计所有用户设置的 gas 价格，以月为单位进行调整。

7.2 发行细则

极数链发行 XDC 币，发行总量 10 亿枚，初次生成即 8 亿枚，剩余 2 亿枚，依照发行曲线，通过系统运行和生态激励规则进行分配，随着数据的积累和生态的生长会逐渐增多，直至增长到 2 亿枚 XDC 币。这 2 亿枚 XDC 币会持续进入到生态中激励所有链接到极数链上的商业化的产品。

使用方	占比	用途	锁定期
私募	25%	用于支撑项目运营，	无锁定期

		包括发行、开发、市场拓展、法律咨询、资源型顾问、发行渠道、pr 等	
市场推广	15%	用于用户推广	无锁定期
基石投资人	10%	早期投资者对团队建设、平台运营等方面做出的贡献。	锁定 100%，每月解锁 5%，20 个月解锁完毕
创始团队	20%	创始团队中的核心人员，核心人员是项目发展中起到至关重要的人员，锁定期三年，逐步释放。	锁定期一年后释放 10%，第二年分四次解锁 20%，第三年分四次解锁 70%。
社区奖励奖	5%	励社区内的优秀代码贡献者；推广社区生态服务志愿者	无锁定期
系统运行	20%	用于交易验证奖励	无锁定期
生态激励	5%	用作基金会正常运营的费用，用于支持极数链在实体企业中的快速应用	逐月解锁，每月解锁 5%，20 个月解锁完成

XDC 行数量为：

总募集 ETH

币种	类型	数量
ETH	认购	
ETH	基石	

兑换比例

币种	兑换比例
ETH	

7.3 筹集用途及相关计划

所筹集的所有 ETH，将用于下面几个方面的支出：


- 1) 支撑极数链团队的运转以完成极数链底层技术平台的开发建设，基于极数区块链的联盟链建设和垂直行业商业场景方案的落地。
- 2) 购买或参与重要区块链商业方案应用；
- 3) 搭建区块链咨询师团队尽快推进所有区块链商业场景落地；
- 4) 扶持区块链商业场景应用的相关项目发展。

极数链时间计划，分为三个阶段进行。即私募阶段、发行代币、交易所交易（以下时间节点随时可能发生变化，请留意白皮书变更）。具体包括以下 5 个时间节点：

- 1) 2018 年 2 月 3 日，正式公布极数链（XDC）全球白皮书，同时启动极数链第一轮私募（基石）。
- 2) 2018 年 2 月 4 日 - 2018 年 2 月 6 日，极数链私募完成。
- 3) 2018 年 2 月 12 - 2018 年 2 月 14 日，所有代币参与者发放代币
- 4) 2018 年 2 月 22 日，正式登陆交易所

8 发行团队

8.1 发起人团队

<p>中国联合发起人</p>  <p>Tom Z Qi</p>	<p>毕业于美国亚利桑那大学，专业计算机、数学、金融。毕业后从事十多年大宗商品交易工作，曾任瑞士摩科瑞能源集团铁矿石业务亚洲区总裁。2014 年戚先生退出大宗商品行业，建立国内第一家硬科技创新人才社交平台 Xtecher，发展至今以成为国内最专业的产业科技创新服务平台之一。</p>
--	---

<p>中国联合发起人</p>  <p>Shephor Gan</p>	<p>毕业于浙江大学通信与信息系统专业，获工学博士学位。从 2002 年开始从事密码算法、高性能计算和网络安全领域的研究工作。主持并参与了国家和军队多项重大科研项目，全球网络攻防领域顶级专家。在并行计算、软件脆弱性分析、区块链中的共识算法和智能合约技术领域有极深入研究，在全球范围内具备绝对领先的技术优势。</p>
<p>法国联合发起人</p>  <p>Eric Caudal</p>	<p>ELICO 公司总裁，专注企业信息化技术咨询及开发 20 年经验。币圈资深人士</p>

8.2 投资人

8.3 法律顾问

<p>蔡汉强</p>	<p>法律顾问</p>	<p>英国及香港律师 伦敦大学法律硕士，中南财经大学法学教授，美国美科律师事务所顾问</p>
------------	-------------	--

8.4 产品技术团队

<p>首席科学家顾问</p>  <p>Chris Wood</p>	<p>Chris Wood 曾担任西班牙 URV 大学研究主任，目前是中国顶级大学教授。他的主要研究领域是应用密码学、区块链与密码货币以及云计算安全，拥有 30 多项发明专利，发表论文 130 余篇，包括 IEEE / ACM ToN, TIFS, TDSC, TC, TITS, TVT, Eurocrypt, Asiacrypt, ESORICS 等顶级期刊与会议论文 40 余篇。他获得 IET Information Security 杂志 2016 年度最佳论文奖，ACISP 2017 最佳论文奖，他指导的学生获得 ProvSec 2017、是 SOCO, JCIN 和 TDP 等国际期刊编辑。他在 CACR 担任青年工作委员会副主任，是密码协议专委会委员，密码学应用专委会委员，是 CZE 区块链专家委员会委员，CCF 区块链专委会发起人之一。</p>
<p>首席科学家顾问</p>  <p>Andrew Chiu</p>	<p>Andrew Chiu 曾担任惠普欧洲研究院（英国）密码学和可信计算研究科学家，目前是中国顶级大学教授。他的主要研究领域是密码协议理论及工程、共识机制与密码货币、后量子密码技术。在国际密码学会旗舰期刊《Journal of Cryptology》，密码学和信息安全顶级会议 EUROCRYPT、ACMCCS 等发表论文 60 余篇。获得美国和中国发明专利 10 余项，研究成果得到了大规模实际应用。他担任 CACR 理事、是密码协议专委会委员，密码学应用专委会委员，是 CZE 区块链专家委员会安全隐私工作组副组长，和 CCF 区块链专委会发起人之一。</p>
<p>首席科学家顾问</p>  <p>张云泉</p>	<p>张云泉，博士，中科院计算所并行软件实验室主任，研究员，博士生导师，国家超算济南中心主任。2000 年中国科学院软件研究所计算机软件与理论专业硕博连读，获工学博士学位。主要研究方向为大数据并行处理、并行程序设计和性能评价、并行计算和并行编程模型等。已在国内外学术刊物上发表论文二百余篇，出版专著一部，译著七部。获得中科院软件所首批杰出青年人才专项计划支持。曾获国家科技进步奖二等奖一项，获</p>

	中科院科技进步二等奖一项，2016 年中国计算机学会科学技术二等奖，2017 年中科院科教成果一等奖，2017 年中科院杰出科学与技术成就奖，2017 年度国际艾奇奖商业创新影响力人物。中国大数据产业应用协同创新联盟执行理事长，中国软件行业协会常务理事，中国计算机学会常务理事/高性能计算专业委员会秘书长,大数据专家委员会副秘书长。中国高性能计算机 TOP100 排行榜创始人和发布者。IEEE CSE 2010、IEEE HPC 2013、FCST2015，NPC2015 和 HPC China 2016 等程序委员会共同主席。
Chester Yuang	研究方向密码学与区块链。曾获国际数学建模最高奖多次，acm 程序设计竞赛最高奖多次。主要研究区块链安全及底层架构，熟悉比特币、以太坊等区块链底层架构。在国际重要期刊上发表过多篇区块链领域的文章。
Michelle Hsu	熟悉区块链多种隐私保护技术，以及主流区块链的底层架构，尤其对密码货币各种体系有深入研究。曾获国际密码、数学等竞赛奖项多项。在国际重要期刊发表区块链领域文章多篇。
温德亮	原阿里云架构师，蜜芽宝贝架构总监，多年区块链技术和人工智能研究经验，16 年即参与到区块链项目中实践，具备丰富的区块链架构经验
Male	核心开发者 俄罗斯 National research university 毕业，前任职俄罗斯 Jincor CTO ，技术战略开发框架选择，区块链技术设计架构研究、学习、开发、代码质量控制，前端/后端服务开发、测试和部署自动化，参与 Jincor 全流程 pre ICO 白皮书和 yellowpaper 开发
Paul	原百度高级产品经理，多年百度数据存储、分布式、智能匹配产品经验，主导过一线百度云存储产品。资深比特币玩家，代币玩家。对区块链产品有深入了解。
苏海江	原阿里云高级架构师，十年以上的互联网开发经验互联网云存储分布式专家，先后任职用友、阿里云、美团等知名一线互联

	网公司负责底层存储架构，技术擅长互联网分布式系统开发，高可用应用架构，区块链技术等系统研发架构
米凯	十年以上的互联网开发经验，先后任职用友、阿里云等知名互联网公司，阿里云分布式存储高级技术专家对区块链有深入研究。
于姜萍	十年以上前端技术开发经验，前端技术高级专家，先后任职联想、阿里云、淘宝擅长多种类高精尖的前端技术

9 参考文献

1. <https://en.bitcoin.it/wiki/Category:History>
2. <https://panteracapital.com/wp-content/uploads/The-Final-Piece-of-the-Protocol-Puzzle.pdf>
3. <https://github.com/bitcoinbook/bitcoinbook>
4. <https://github.com/ethereum/wiki/wiki/White-Paper>
5. S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system, 2009, <https://www.bitcoin.org/bitcoin.pdf>
6. Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform, 2013, <http://ethereum.org/ethereum.html>
7. Paul Sztorc, Peer-to-Peer Oracle System and Prediction Marketplace, 2015, <http://bitcoinhivemind.com/papers/truthcoin-whitepaper.pdf>
8. PriceFeed Smart Contract, 2016, <http://feed.ether.camp/>
9. V. Costan and S. Devadas, Intel SGX Explained, 2016, <https://eprint.iacr.org/2016/086.pdf>
10. E. Shi. Trusted Hardware: Life, the Composable Universe, and Everything. Talk at the DIMACS Workshop of Cryptography and Big Data, 2015
11. <http://ethdoc.cn/>
12. Iddo Bentov and Ranjit Kumaresan, How to Use Bitcoin to Design Fair Protocols, 2014, <https://eprint.iacr.org/2014/129.pdf>
13. Marcin Andrychowicz et al., Secure Multiparty Computations on Bitcoin, 2013, <https://eprint.iacr.org/2013/784.pdf>
14. Ranjit Kumaresan and Iddo Bentov, How to Use Bitcoin to Incentivize Correct Computations, 2014, <https://people.csail.mit.edu/ranjit/papers/incentives.pdf>
15. Aggelos Kiayias, Hong-Sheng Zhou, and Vassilis Zikas, Fair and Robust Multi-party Computation Using a Global Transaction Ledger, 2016, http://link.springer.com/chapter/10.1007%2F978-3-662-49896-5_25
16. Guy Zyskind, Oz Nathan, Alex Pentland, Enigma: Decentralized Computation Platform with Guaranteed Privacy, 2015, http://enigma.media.mit.edu/enigma_full.pdf
17. Joseph Bonneau et al., On Bitcoin as a public randomness source, 2015, <https://eprint.iacr.org/2015/1015.pdf>
18. Dennis Mckinnon et al., RANDAO, 2014, <https://github.com/dennismckinnon/Ethereum-Contracts/tree/master/RANDAO>
19. Dennis Mckinnon et al., RANDAO, 2015, <https://github.com/randao/randao/blob/master/README.en.md>
20. Marcin Andrychowicz et al., Secure multiparty computations on Bitcoin, 2014, <https://eprint.iacr.org/2013/784.pdf>
21. Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies, 2016, <http://www.theblockchain.com/docs/Princeton%20Bitcoin%20and%20Cryptocurrency%20Technologies%20Course.pdf>
22. Matt Springer, Is Bitcoin Currently Experiencing a Selfish Miner Attack?, 2014, <http://scienceblogs.com/builtontfacts/2014/01/11/is-bitcoin-currently-experiencing-a-selfish->

- miner -attack/
23. Edward Felten, Game Theory and Bitcoin, 2013, <https://freedom-to-tinker.com/blog/felten/game-theory-and-bitcoin/>
 24. Litecoin, 2011, <https://litecoin.info/>
 25. RaiBlocks: A Feeless Distributed Cryptocurrency Network
https://raiblocks.net/media/RaiBlocks_Whitepaper__English.pdf
 26. The Tangle Serguei Popov https://iota.org/IOTA_Whitepaper.pdf
 27. Byteball: A Decentralized System for Storage and Transfer of Value Anton Churymov
<https://byteball.org/Byteball.pdf>
 28. 《区块链革命》 唐塔普斯科特
 29. 《区块链:定义未来金融与经济新格局》 张健
 30. 《区块链:将如何重新定义世界》 唐文剑, 吕雯
 31. 《区块链革命:比特币底层技术如何改变货币、商业和世界》 唐·塔普斯科特、亚力克斯·塔普斯科特著
 32. 《全球政府区块链技术应用一览》 胡宁
 33. 《区块链应用的经济学原理》 WEMONEY
 34. 《各国政府对区块链都持何种态度?》 徐利
 35. 《中国区块链技术和应用发展白皮书(2016)》, 工业和信息化部信息化和软件服务业司
 36. 《分布式账本技术:超越区块链》, 英国政府首席科学顾问报告, 万向区块链实验室编译
 37. 《中国区块链技术和应用发展白皮书(2016)》, 工业和信息化部信息化和软件服务业司
 38. 《英国将区块链列入国家战略部署, 并制定详细战略实施规划》, 蔡维德、赵精武, 中国信息化百人会
 39. 区块链铅笔, chainb.baijia.baidu.com
 40. 36Kr-区块链研究报告
 41. 2016 年区块链市场调研分析报告
 42. 2017 年中国区块链行业市场调研及投资前景评估报告
 43. 2017 年版中国区块链市场调研报告
 44. “宜人智库” 区块链技术商业机会研判
 45. 《蚂蚁金服在大数据合作上的创新实践》 周卫林
 46. 德勤: DLT (区块链) 技术使用调查报告 (中文版)
 47. 高盛: 区块链, 将理论付诸实践报告 (英文版)
 48. 麦肯锡: 区块链, 银行业游戏规则的颠覆者
 49. 普华永道: 2017 年全球金融科技调查——保险科技 (InsurTech) 调查报告
 50. 区块链数据库-东南大学崇志宏
 51. 腾讯研究院: 2017 数字经济白皮书
 52. 中国区块链技术市场调研报告目录
 53. CSIRO: 区块链技术潜在用途研究
 54. <https://bitcoin.org/bitcoin.pdf> 中本聪论文
 55. 一文读懂区块链产业生态、存在问题及政策建议 中国电子银行网