DotKey

DotKey

DotKey：基于波卡生态的区块链权益证明金融架构系统

DotKey Team

PUBLISHED BY DOTKEY FOUNDER TEAM

DOTKEY.LIVE

本文档为中文社区成员自发翻译，仅供参考，如与英文版文档有出入之处，请以英文版文档为准。

First Publish, February 2021

Contents

行业概况

1. 区块链技术

区块链(Blockchain)是一种将数据区块有序连接，并以密码学方式保证其不可篡改、不可伪造的分布式账本(数据库)技术。通俗的说，区块链技术可以在无需第三方背书情况下实现系统中所有数据信息的公开透明、不可篡改、不可伪造、可追溯。区块链作为一种底层协议或技术方案可以有效地解决信任问题，实现价值的自由传递，在数字货币、金融资产的交易结算、数字政务、存证防伪数据服务等领域具有广阔前景。

1.1 数字货币

在经历了实物、贵金属、纸钞等形态之后，数字货币已经成为数字经济时代的发展方向。相比实体货币，数字货币具有易携带存储、低流通成本、使用便利、易于防伪和管理、打破地域限制，能更好整合等特点。

1.2 金融资产交易结算

区块链技术天然具有金融属性，它正对金融业产生颠覆式变革。支付结算方面，在区块链分布式账本体系下，市场多个参与者共同维护并实时同步一份“总账”，短短几分钟内就可以完成现在两三天才能完成的支付、清算、结算任务，降低了跨行跨境交易的复杂性和成本。同时，区块链的底层加密技术保证了参与者无法篡改账本，确保交易记录透明安全，监管部门方便地追踪链上交易，快速定位高风险资金流向。证券发行交易方面，传统股票发行流程长、成本高、环节复杂，区块链技术能够弱化承销机构作用，帮助各方建立快速准确的信息交互共享通道，发行人通过智能合约自行办理发行，监管部门统一审查核对，投资者也可以绕过中介机构进行直接操作。数字票据和供应链金融方面，区块链技术可以有效解决中小企业融资难问题。目前的供应链金融很难惠及产业链上游的中小企业，因为他们跟核心企业往往没有直接贸易往来，金融机构难以评估其信用资质。基于区块链技术，我们可以建立一种联盟链网络，涵盖核心企业、上下游供应商、金融机构等，核心企业发放应收账款凭证给其供应商，票据数字化上链后可在供应商之间流转，每一级供应商可凭数字票据证明实现对应额度的融资。

1.3 数字政务

区块链可以让数据跑起来，大大精简办事流程。区块链的分布式技术可以让政府部门集中到一个链上，所有办事流程交付智能合约，办事人只要在一个部门通过身份认证以及电子签章，智能合约就可以自动处理并流转，顺序完成后续所有审批和签章。区块链发票是国内区块链技术最早落地的应用。税务部门推出区块链电子发票“税链”平台，税务部门、开票方、受票方通过独一无二的数字身份加入“税链”网络，真正实现“交易即开票” “开票即报销”——秒级开票、分钟级报销入账，大幅降低了税收征管成本，有效解决数据篡改、一票多报、偷税漏税等问题。扶贫是区块链技术的另一个落地应用。利用区块链技术的公开透明、可溯源、不可篡改等特性，实现扶贫资金的透明使用、精准投放和高效管理。

1.4 存证防伪

区块链可以通过哈希时间戳证明某个文件或者数字内容在特定时间的存在，加之其公开、不可篡改、可溯源等特性为司法鉴证、身份证明、产权保护、防伪溯源等提供了完美解决方案。在知识产权领域，通过区块链技术的数字签名和链上存证可以对文字、图片、音频视频等进行确权，通过智能合约创建执行交易，让创作者重掌定价权，实时保全数据形成证据链，同时覆盖确权、交易和维权三大场景。在防伪溯源领域，通过供应链跟踪区块链技术可以被广泛应用于食品医药、农产品、酒类、奢侈品等各领域。

1.5 数据服务

区块链技术将大大优化现有的大数据应用，在数据流通和共享上发挥巨大作用。未来互联网、人工智能、物联网都将产生海量数据，现有中心化数据存储（计算模式）将面临巨大挑战，基于区块链技术的边缘存储（计算）有望成为未来解决方案。再者，区块链对数据的不可篡改和可追溯机制保证了数据的真实性和高质量，这成为大数据、深度学习、人工智能等一切数据应用的基础。最后，区块链可以在保护数据隐私的前提下实现多方协作的数据计算，有望解决“数据垄断” 和“数据孤岛”问题，实现数据流通价值。针对当前的区块链发展阶段，为了满足一般商业用户区块链开发和应用需求，众多传统云服务商开始部署自己的 BaaS (“区块链即服务”)解决方案。区块链与云计算的结合将有效降低企业区块链部署成本，推动区块链应用场景落地。未来区块链技术还会在慈善公益、保险、能源、物流、物联网等诸多领域发挥重要作用。

2. 市场痛点

区块链自比特币诞生至今产生出现了无数的公链，其中主流公链有Omni、ETH、EOS等，更小的垂直应用公链更不计其数。这些公链都是独立运行的，而上面的资产也都独立存在，想将一条链上资产转移到另一条链上更是困难重重。DotKey基于波卡生态，为跨链工具波卡生态提供流动性，将跨链基础设施金融化，使得基础设施和服务的提供者可以获取收益，从而成为跨链的润滑剂。

DotKey：区块链基础设施的金融化

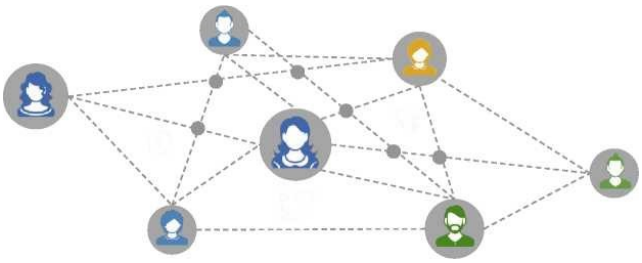
3. DotKey平台

为将区块链资产资金融化，最大程度地提高共识效率和促进链上应用程序使用，DotKey提出一种区块链解决方案。DotKey建立了一个金融渠道，将区块链资产转化为灵活可交易的金融产品。通过DotKey的财务渠道，个人既可以从权益奖励中受益，也可以通过参与区块链应用程序获得收益。节点运营商可以发行衍生品，在一定期限内通过衍生品出售抵押资产。因此，该财务协议为首例允许用户同时通过抵押和应用两个途径获得收益。基础资产衍生品的发行使区块链更加灵活，从而促进区块链行业的金融化进程。

3.1 DotKey背景

抵押资产的总价值已从 7.41 亿美元增至 47 亿美元，总增长率为 533%。随着新型 PoS 网络的兴起以及现有区块链向 PoS 的迁移，预期资产总值会进一步增长。但是，权益证明要求投资人将其资产在一定时期内在区块链内锁定，不能投放允许短期内交易盈利的二级市场。所有类型的区块链目的都是为了创建一个数据库系统，各方可以以去中心化的方式共同维护和编辑数据库，任何一方无法进行中心化控制。在区块链经济中，去中心化操作会影响代币代理人的的商业动机和操作惯例。在标准的权益证明系统中，越多人持

股，就有越多的代币处于非流通状态。这看似有利于代币价格上涨，但多数情况下，流动性不足会阻碍整个金融网络的发展。充足的流动性对于支撑金融网络而言是十分必要的。流动性不足会影响需求，因为此种情况下一旦出现需求的小幅上涨趋势，就可能导致价格急剧上升，甚至可能超过应用程序买家所能承受的最大倾向范围。如果交易对价格的影响过大，退出系统的成本也会增加，最终影响数据提供方的收益。由于交易买卖引起的价格变动称为滑点，滑点的起伏不定是各方都不希望的结果。 DotKey计划创建一个连接协议层和应用程序层的财务渠道。PoS 代币持有者可将本地代币存入权益合同并获得与原代币具有同等价值的合成代币。持有人可以使用合成代币在二级市场上交易，也可进入链上应用程序，例如 defi。持有人通过自由使用代币，实质上就是在权益证明链上的抵押池中通过已经抵押的代币获得报酬。相反，对于正在运行具有大量抵押资产的抵押节点运营商，他可以通过DotKey的财务渠道进行抵押拍卖，发行由自己抵押资产做保的金融衍生产品。衍生产品采用代币形式，拍卖竞标者可以在应用程序或交易中自由使用这些衍生代币。DotKey的金融渠道建立在Polkadot 上，由基层开发者开发后连接到平行链。财务层是一个包含了各种金融模型优化智能合约层。智能合约在 polkadot 区块链上运行，可以加强合约性质，以一种编程和自动算法的形式促进货币和有物品价值所有权的交易。即使在某些情况下，智能合约需要由中心化数据端执行，去中心化的共识记录也可以使合约和执行方面的摩擦相对减少。智能合约可以提高某些意外情况的合约约束力和执行力。



4. DotKey金融架构

4.1 权益衍生品发行

DotKey提出一种权益拍卖机制，在此机制中，利益相关者可以拍卖所抵押的资产。买家可以竞标拍卖的一部分，即一部分的抵押资产权益。买家也可以大量购入，生成以抵押为基础的衍生工具。治理方面，首先将验证资产抵押方的有效性以及拟发行衍生品的抵押资产的数量。衍生产品合约的定价由发行人确定，但DotKey有一个基准框架，可为发行人设定要价提供参考。DotKey首先定义股份合同的特征，如下所示：

每个抵押合同的标准符号：

- 权益年回报率：$k\%$；
- 抵押期：T；
- 到期时间：τ；
- 合约大小：C；
- 当前代币价格：S；
- 抵押合同的当前价值：$V = S*(1+k\%)^{\tau/T}$。

如果市场上有 n 个合约交易，所有符号都用 i 标记。假设 $0=\tau 0<\tau 1<\cdots<\tau n$，则代币的（连续复合）返回率应为时间$[\tau i-1]$，$\tau i$ 上的分段常数 ri。这些回报率应满足

$$\begin{cases} e^{r_1*\tau_1} = \frac{(1+k_1\%)^{\tau_1}}{V_1/S} \\ e^{r_1*\tau_1}e^{r_2(\tau_2-\tau_1)} = \frac{(1+k_2\%)^{\tau_2}}{V_1/S} \\ \vdots \\ e^{r_1*\tau_1}e^{r_2(\tau_2-\tau_1)}\cdots e^{r_n(\tau_n-\tau_{n-1})} = \frac{(1+k_n\%)^{\tau_n}}{V_n/S}. \end{cases}$$

因此我们得到：

$$\begin{cases} r_1 = \frac{1}{\tau_1}[\tau_1\ln(1+k_1\%) - \ln(V_1/S)] = \ln(1+k_1\%) - \frac{\ln(V_1/S)}{\tau_1} \\ r_2 = \frac{1}{\tau_2-\tau_1}[\tau_2*\ln(1+k_2\%) - \tau_1*\ln(1+k_1\%) - \ln(V_2/V_1)] \\ \vdots \\ r_n = \frac{1}{\tau_n-\tau_{n-1}}[\tau_n*\ln(1+k_n\%) - \tau_{n-1}*\ln(1+k_{n-1}\%) - \ln(V_n/V_{n-1})] \end{cases}$$

现在，如果要评估具有到期时间和收益率 k%的抵押合同，则其价值应为：

$$
\begin{aligned}
V &= e^{r_1*\tau_1} e^{r_2(\tau_2-\tau_1)} \dots e^{r_i(\tau_i-\tau_{i-1})} e^{r_{i+1}(\tau-\tau_i)} \\
&= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(e^{r_{i+1}(\tau_{i+1}-\tau_i)} \tau_{i+1}^{\tau-\tau_i} \tau_i \right. \\
&= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{V_{i+1}/S} / \frac{(1+k_i)^{\tau_i}}{V_i/S_i} \right)^{\frac{\tau-\tau_i}{\tau_{i+1}-\tau_i}} \\
&= \frac{(1+k_i)^{\tau_i}}{V_i/S} * \left(\frac{(1+k_{i+1})^{\tau_{i+1}}}{(1+k_i)^{\tau_i}} \frac{V_i}{V_{i+1}} \right)^{\frac{\tau-\tau_i}{\tau_{i+1}\tau_i}}
\end{aligned}
$$

在此定价指导下，发行人可以评估其衍生产品的当前价格并公开拍卖抵押资产。

4.2 ETF的发行

DotKey还提供获得多种 pos 奖励的合成金融投资产品，该产品可以通过一种最简单方法，让用户选择最优质的的权益证明协议下进行长期交易。持有人持有的每一枚代币都可以获得抵押资产的最优回报。DotKey会根据市值和日交易量筛选 POS 资产的资质，然后通过抵押率和奖励率等因素对这些资产进行排名。然后，DotKey将筛选出排列前三位的代币作为合成组合，并每月进行市值加权和重新评估。

4.3 共识和协议

DotKey使用基于Polkadot 的权益证明共识算法，该算法是一种混合共识模型，用于区块创造，而不用于确定区块的最终性质。DotKey的网络具有多种类型的节点：勤奋节点、挖掘节点和权益代理节点。勤勉节点除具有区块生成功能外，还具有投票和渠道维护的权利。当勤奋节点达到投票阈值时也将成为区块生成节点。挖掘节点生成区块，在投票方面更具吸引力。权益代理节点从块生成节点筛选得出。勤奋节点，挖掘节点和权益代理节点必须具有相同的网络访问环境和计算功能。尽管勤奋节点不需要产生区块，但是有必要创造真实节点来传输规律性的交易数据。节点的区块创造、区块丢失、节点掉落或其他恶意行为将受到惩罚，同时扣除节点的自抵押资产和用户所等待的奖励。利益主体节点将获得额外的利益收益；违反收益合同的条款将受到相应的惩罚。罚金将转入议会资金，随后进行全民公决决定如何处理。

节点注册和应用程序向所有用户开放。设置节点服务器后，即可开始运行。DotKey使用一点一票模型来防止暗箱操作。所有用户都可以使用 BNC 进行节点投票选举。为保证网络稳定运行，同步节点和块生产者节点需要支付相同的成本。因此，同步节点和块生产者节点将获得相同的收益。权益代理节点将成为我们多链生态系统的重要组成部分，负责产生生态系统的收益。除大宗节点的收入外，权益代理节点还将获得收益产生的股息。运行环境作为链的重要组成部分，比智能合约更底层。运行环境由各种运行时模块组成。运行时区块包括帐户、余额、抵押、智能合约、交易过渡、治理和共识等模块。模块可以彼此独立，同时允许模块相互调用。该链的大多数代码逻辑都在运行时环境中运行。

运行环境允许每个运行模块独立升级，而它的一个重要功能是没有硬分叉升级。现有区块链系统升级时，由于每个节点的运行版本不一致，存在造成整个链条硬分叉的风险，严重影响了整个生态系统的健康发展以及节点和用户的利益。每次升级模块，DotKey都会生成两个版本：本地版本和 WASM 版本。当运行时环境确定更新的模块的版本与当前本地版本一致时，为获得最快的运行效率请直接运行本地版本代码。

用户通过跨链将资产锁定在主链内，这部分资产经过签订多重托管合同，托管合同由多个见证节点共同管理。通过去中心化治理机制，见证节点由各节点参与方投票选出并定期轮换。同时，当主链托管合同持有的资产太大时，可以将其拆分为多个托管合同，出于安全性考虑，会引入更多的托管节点组进行托管。

4.4 保险与安全

通过存入DotKey的平台代币并指定某些关键参数（例如基础资产、预购价、到期日等），期权程序开发者可以制造称为 DTokens 的任意可替代期权代币。出售 DTokens 代币使开发者赚取溢价，最终通过自有的抵押资产创收。然后，买家可以购买这些 DToken，这些DToken 在 0x 或 Uniswap 等交易所进行交易，从而确保市场流动性。除此框架所支持的可互换、可自由交易的 ERC20 期权合约之外，买家还可以特别关注存款保险的保护性看跌策略（例如，保护代币市场的用户，如复合货币用户免受黑客入侵和流动性危机影响）以及保护用户避免 DAI 价值崩溃风险。我们还考虑其他一些情况，比如希望提供风险保护期权卖方可以采取措施，使用一种不同于与以行使价计价的资产（例如美元）的另一种抵押类型（例如 ETH）。

4.5 财务审计

审计师采用区块链技术上策略是互补和调整性的，因为在处理多审计师共同参与的交易项目时，越多审计师采用区块链技术，那么审计的损失代价就越小。但如果审计客户宁愿冒着被查办的风险还是倾向谎报数据的话，此时客户往往宁愿选择不用区块链技术的审计师，即使这类审计师的收费更低。因此，如果其他审计师没有使用该技术，那么审计师往往同样不会使用，因为不仅利润上不划算，还可能造成客户丢失，最终不如传统审计师。但总体而言，区块链有三个有利于审计的技术特征：

- 去中心化：区块链的点对点设计，无需受有信用度的数据中心的要求限制；
- 加密性：零知识证明支持加密通信，保护数据隐私；
- 不可篡改：一旦审核员通过联合区块链请求信息，任何审核员或外部黑客都很难有意修改或删除该信息，除非能够做到修改联合区块链上绝大多数的节点信息。我们将建立去中心化的财务审计系统，以监督权益拍卖的权益交易人拍卖完成后的活动。

5. 经济原理

DotKey拥有用于金融渠道的本地代币。此种代币可为DotKey的渠道获取链上价值。DotKey的代币的主要功能如下：

服务：DotKey提出一种代币锁定奖励模型，该模型使用户可以通过锁定代币来奖励协议贡献者，而无需花费自身代币。此过程类似于锁定代币：原理是由加盟者根据已签署的条款将其锁定在代币中。衍生产品发行人必须就所需的代币和时间长度进行协商，允许DotKey 的财务渠道为其协议作公开记录。一旦确定条款，衍生产品发行人就会按照其协议条款将交录入区块链。DotKey将此交易称为协议交易。衍生发行人需要抵押一定数量的平台代币以获得拍卖许可。

ETF 发行：DotKey将分配平台代币池来发行权益ETF。DotKey新发行的代币价值将紧跟通过算法管理的透明化 POS 代币配餐。由DotKey新发行的代币跟踪的基础资产产生的奖励将用于回购和销毁。

保险：保险的概念来自过去，人们集中资源来保护彼此抵抗所有人所面临的风险。我们意识到，DotKey可以在一个平台上建立一个共同体，在此平台上，个人只需要信任系统，而无需信任每个人。此举目的是为DotKey的用户提供更简单、透明、可访问且更优惠的财务保护措施以防范风险。DotKey的平台代币将有一组保险资金池来为链上活动提供保护。DotKey 提供衍生品担保业务，为权益人和权益购买方防范价值存储的过程的黑客入侵风险。

购回及销毁：DotKey将通过财务渠道的运营从交易和服务中产生费用收入。所有收入将用于回购代币，DotKey将回购的代币销毁，作为所有代币持有者的权益保障。

DotKey项目技术实现与发展

6. DotKey项目技术实现与发展

DotKey的初始版本是基于ERC20开发的代币体系。代币（Token）是区块链中定义价值的方式，用于标定金融或数字资产。在ETH链上，代币使用相同的标准，这样代币之间的兑换和DAPP支持就会变得容易。

7. 区块链技术应用

区块链在本质上是一种分布式的交易数据库，所有在网络中的节点分享数据。这是比特币的技术创新，它在这种交易过程中担任着公共分类账目的角色。系统中的每一个节点都拥有现存链上的区块副本，其中包含了所进行过的一切交易数据，每个区块以哈希值与前一个区块相连，这些相连的区块就形成了区块链。每个区块链都包含四个维度，数据层、共识层、应用层三个水平维度以及一个垂直的治理维度。

7.0.1 数据层

作为底层水平维度，被记录的交易在节点间广播，完整的节点产生区块。作为区块链的基础，在区块链中发生数字资产与其伴随的价值的传输，通过椭圆曲线密码、哈希函数、默克尔树算法等加密手段实现账户安全。

7.0.2 共识层

共识层是区块链的中间水平维度，体现区块链点对点式的特征。在此层中，网络中所有节点通过工作量证明算法（PoW）、权益证明算法（PoS）或其变体、拜占庭容错算法（BFT）或其变体等技术对链的内部状态达成共识。区块链的可扩展性主要受共识层影响。通常认为，PoW（工作量证明算法）在扩展性方面不及PoS（权益证明算法）。此外，双重支付问题和区块链可能遭受的状态篡改攻击还会直接影响共识层的安全性。

以上两个水平维度构建了区块链的基本构架，而应用层对于区块链的实际应用至关重要，影响到包括区块链可扩展性和可用性的问题。举例来说，波场使用的智能合约具备可编程性，使得个体能依靠分布式的“全球计算机”执行合约条款。侧链技术与合并挖矿也极大地推进了可编程性的发展。闪电网络所代表的二级协议发展状态通道技术，进一步加强了区块链在此层面的可扩展性。此外，应用工具、软件开发工具包、框架结构、图形用户界面对区块链的可用性也尤为重要。应用层为开发者提供开发去中心化的应用软件(DApps)的平台，这是区块链实现其使用性和价值的重要环节。

7.0.3 治理层

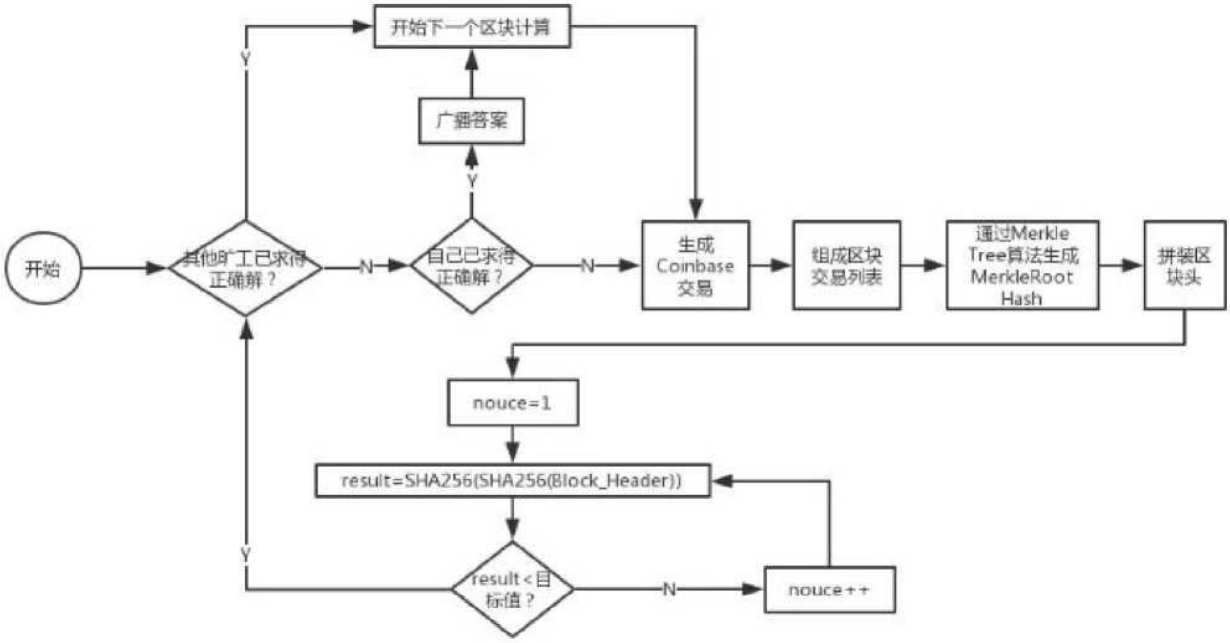
与任何有机体一样，成功的区块链也将是环境的最佳适应者。在区块链系统只有通过演化才能生存的前提下，初始设计固然重要，但在足够长的时间段里，可变化的机制无疑

是最重要的，此机制就是我们所说的垂直层面治理。

7.1 共识机制

7.1.1 PoW

PoW(ProofofWork),即工作量证明，闻名于比特币，俗称“挖矿”。 PoW是指系统为达到某一目标而设置的度量方法。简单理解就是一份证明，用来确认你做过一定量的工作。监测工作的整个过程通常是极为低效的，而通过对工作的结果进行认证来证明完成了相应的工作量，则是一种非常高效的方式。 POW有去中心化、安全性高等优点，但是浪费了



算力，消耗了大量的资源，网络性能较低，算力集中化等缺点明显。

7.1.2 PoS

PoS（Proof-of-Stake）即权益证明，可看其为PoW的替换，其解决了PoW中的一些问题，但也出现了新的问题。其设计理念是区块记账权的抉择是根据不同节点的股份和占有时间来进行随机选择的。它解决了比特币随着矿工积极性的下降从而使矿工人数的减少，造成的整个网络可能陷入瘫痪的问题，也增加了安全性，因为破坏成本不光是51%的算力，而且还需要51%的持有量。

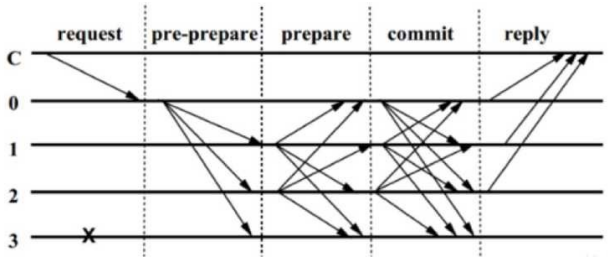
PoS更加节能、去中心化、避免通货膨胀。PoS的基本思想是随机选择一组节点对下一个区块投票，并根据它们的资金量大小（即权益）对他们的投票进行加权。如果某些节点行为不当，系统可能会没收其链上的资金。藉由这种方式，不用通过高计算成本的PoW，区块链依旧可以更高效地运行，除此之外可以实现链上的经济稳定性：参与者拥有的权益越多，其维护账本共识机制的动机就越大，其节点行为不当的可能性也就越低。

7.2 实用拜占庭容错算法

实用的拜占庭容错算法(PBFT)是Castro和Liskov在1999年提出的一种有效的抗攻击算法，用于在分布式异步网络中达成协议。我们计划使用PBFT作为我们DPoS共识机制的基础投票算法，因为它是一种简洁而且研究得非常好的算法，它提供了快速的结算性，这对于构建高效与可扩展的区块链至关重要。正如Castro和Liskov的原始论文所证明的那样，只要低于三分之一的网络节点出现故障或恶意行为，PBFT就可以为链提供可用性和安全性；同时，PBFT的网络成本非常低，仅为未复制网络系统成本的3%。PBFT是一种状态机副本复制算法，即服务作为状态机进行建模，状态机在分布式系统的不同节点进行副本复制。每个状态机的副本都保存了服务的状态，同时也实现了服务的操作。将所有的副本组成的集合使用大写字母R表示，使用0到$|R|-1$的整数表示每一个副本。为了描述方便，通常假设故障节点数为f个，整个服务节点数为$|R|=3f+1$个，f是有可能失效的副本的最大个数。尽管可以存在多于$3f+1$个副本，但额外的副本除了降低性能外不能提高可靠性。

所有的副本在一个被称为视图(*view*)的轮换过程中运作。在某个视图中，一个副本作为主节点(*primary*)，其它的副本节点作为备份节点(*backup*)。视图是连续编号的整数。主节点由公式$p=vmod|R|$计算得到，v是视图编号，p是副本编号，$|R|$是副本集合的个数。当主节点失效的时候就需要启动视图轮换过程。

PBFT算法实现流程如下:



IV

DotKey发行

8. 代币发行

8.1 项目角色

- 直接建设者：负责研发Dotkey 公链底层技术的基金会及创始团队和支持创始团队运营的「基金」；
- 系统维护者：维护 Dotkey 系统运转和系统安全性的「矿工节点」；
- 生态建设者：持续为Dotkey 生态创造价值的「社区用户」。

从这些生态成员的角度出发，Dotkey的经济模型将根据不同阶段采取不同的激励模式，使整个 Dotkey 生态从初始运行平稳过渡到成熟发展

8.2 项目运行阶段

- 初始阶段：通过激励直接建设者和生态建设者，解决系统的冷启动问题
- 运行阶段：通过持续激励系统维护者，推动系统实现持续升级；通过市场化系统资源，促进Dotkey 的系统资源实现自适应配置

8.3 代币分配

为有效激励社区建设，实现DotKey生态的增长和繁荣，DotKey发行平台发行通证token——DotK。总发行量为1亿，永不增发，实行通缩机制，保证币价有效上涨。DotKey分配用途如下：

- 10%: 首轮投资者：首轮投资者会获得 10% 的创世通证激励，该部分通证及时流通；
- 36%: 基金会团队及创始团队：基金会团队及创始团队将获得 36% 的创世通证激励，此部分将作为资金池持续发放。该部分通证会于 4 年内解锁；
- 12%: 社区基金：12% 的创世通证会用于激励普通社区用户，鼓励社区用户早期投入到 Conflux 的生态建设和维护中。该部分通证将于 4 年内解锁；
- 42%：生态基金：42% 的创世通证会用于激励社区开发者并孵化支持Dotkey 生态中的 DApp 项目。该部分通证会于 4 年内解锁；
-
- 公共基金：初始阶段将不会分配额外额度到DOTKEY公共基金账户

V

附录

9. 附录

9.1 法律声明

DotKey的销售内容仅作为针对特定面向的人群或参与者的交换媒介，也不是任何形式的招股说明书或要约文件，也不打算构成任何形式的证券要约、商业信托中的单位、集体投资计划中的单位或任何其他形式的投资，或任何司法管辖区中任何形式的投资的要约。没有监管机构审查或批准本白皮书中列出的任何信息。本白皮书尚未在任何管辖区的任何监管机构注册。通过访问和/或接受拥有本白皮书或其部分（视情况而定）中的任何信息，默认您符合以下条件：

1. 您不在中华人民共和国境内，也不是中华人民共和国的公民或居民（税收或其他方面），或居住在中华人民共和国境内；
2. 您不在美利坚合众国，也不是美利坚合众国的公民、居民（税收或其他方面），或居住在美利坚合众国；
3. 根据您所在地区的法律、法规要求或规则，您不在禁止、限制或未经授权以任何形式或方式出售令牌的司法管辖区内，无论是全部还是部分；
4. 您同意符合以上让所有人条件限制和约束。

9.2 风险提示

本白皮书并不代表投资建议、或同意销售的许可，以及引导和吸引任何的购买行为。任何类似的提议或征价将在一个可信任的条款下并在可应用的证券法和其它相关法律允许下进行，以上信息或分析不构成投资决策，或具体建议。本白皮书不构成任何关于证券形式的投资建议，投资意向或教唆投资。本白皮书不组成也不理解为提供任何买卖行为，或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。DotKey明确表示相关意向用户明确了解DotKey的风险，投资者一旦参与投资即表示了解并接受该项目风险并愿意个人承担一切相应结果或后果。DotKey明确表示不承担任何参与币市项目造成的直接或间接的损失,包括：

- 因为用户交易操作带来的经济损失；
- 由个人理解产生的任何错误、疏忽或者不准确信息；个人交易各类区块链资产带来的损失及由此导致的任何行为。

DotKey不是一种投资，我们无法保证DotK一定会增值，在某种情况下也有价值下降的可能性，没有正确使用DotK的人有可能失去使用的相应权利。