Dipper Network：开放金融网络

目录

摘要

比特币的诞生开创了一个全新的时代，其以点对点网络和去中心化的思想，解构了传统金融，实现了支付、清结算等基础功能，而这只是区块链伟大愿景中的第一步。在当今社会的经济领域中，尤以借贷、理财、保险和衍生品交易最为活跃，然而传统金融服务的准入门槛高、中间成本高昂、资金透明度低、侵犯信息隐私等问题，增加了金融运行成本，降低了资金利用效率。

针对当前传统金融存在的问题，本文以开放式金融（Decentralized Finance，简称DeFi）为蓝图探寻解决方案。我们设计了一系列的基础金融协议，其中DipBank是一个简单易用的借贷类应用，提供了高度流动性和多样化的借贷服务，使用了新型的经济模型和开放的治理模式，从而减少交易摩擦，提高资金利用率。

与此同时，主流公链的架构、设计与性能参差不齐，资产分布在异构网络之中，无法互通互联。基于此我们设计了Dipper Network——去中心化的金融网络，专注于构建跨链生态的金融中心，通过设计与实现完善的基础金融协议，全面提高资产的流转效率。在未来，我们认为区块链将承载着越来越多的资产，而跨链网络是价值的中转和汇聚之地，Dipper Network旨在通过植根于跨链生态，打造全新的金融枢纽，为DeFi带来更大的想象空间。

1.简介

1.1 驱动因素

金融体系自文明开始就存在，随着时间的推移，它们经历了大量的转变，改变了互动的形式和原则。金融系统从非正式的储蓄和贷款团体开始，逐渐演变出合作社、互助保险和合作银行等形式，这些机构通过几个世纪的增长、兼并和收购，成为了当今大众所熟知的商业和零售银行。当前的金融系统存在不透明、低效[1]而且规模庞大，一旦出现风险将造成极大的社会影响[2]。

近些年兴起的金融科技（Fintech）变革旨在通过改良金融市场和创建以社区为中心的新模式来降低上述影响。Fintech搭建专用程度很高的软件，软件和软件执行需要建立在信任的基础上，而且会受到限制和审查。交易的最终结算层是某个体制，而非代码。其没有使用加密方式确保交易的不变性，整个系统存在很高的体制性风险。

区块链使得任何人都可以在开放网络中拥有和转移资产，而无需信任第三方。与现有的Fintech架构不同，区块链在全球范围内自由且同样可用，这促使区块链上存在大量且迅速增加的数字资产。但是，这些区块链资产面临借贷机制有限而导致的错误定价以及存储成本和风险导致的负收益率等问题。

DeFi用开源软件进行搭建，关键逻辑的运行在免信任的加密网络上，搭建者不会受到金融框架或技术上的限制，尤其是优化了传统借贷服务存在的不足：它们都有着更加易于理解和操作的客户端交互界面；实时可访问的可变利率；允许用户与区块链进行交互，为交易过程带来了更高的透明度。

尽管如此，DeFi也面临着一些显著的问题：首先在生态上面，资金利用率低，缺乏保险机制；其次其主要构建于以太坊网络，存在网络拥塞、高额的交易成本和分片带来的不确定因素等问题；最后，各个区块链自成体系，彼此无法安全的互通互联，形成一座座价值孤岛，难以形成完整的价值互联网。

1.2 前人工作

我们分别介绍在近年来区块链技术的最新进展和DeFi的发展状况。

首先，受限于公链的性能，最近几年业内在公链扩容领域做了很多工作，其分为链上Layer 1和链下Layer 2扩容。最早期的Layer 1方案是比特币的隔离验证（SegWit[11]），近期以太坊准备开始在casper中实施分片（Sharding[12]）；推进Layer1方案在知名的项目是比较困难的，涉及到安全性和多方利益博弈，因此Layer 2方案获得了较大的关注，其主要包括状态通道（State Channel）和侧链（Side Chain）两种解决方案。典型的状态通道有比特币上的闪电网络和以太坊上的雷电网络（Raiden Network[13]）；侧链方案中，Polkadot[14]提供了高度安全的跨链方案，其方案中包含平行链和中继链，并设计了动态验证者和赏金猎人等博弈机制；Cosmos[15]在多方跨链资产转移方面做了充实的工作，每个Hub blockchain作为各个Zone blockchain通信的枢纽，它基于拥有高性能的Tendermint共识算法；Plasma[16]是Vitalik Buterin等提出的，是一种具备资产安全撤回机制的侧链，满足高性能和低安全性应用的需求，主链负责安全和状态验证。

其次，DeFi构建在区块链之上，目的在于提供一个人人皆可参与的、无门槛且无中心的金融服务体系。其实质上是独立于平台的，从应用数、交易量和锁定价值三个维度来看，DeFi类应用几乎全部基于以太坊开发和使用，其累计锁仓资产价值超过5亿美金。闪电网络（Lightning Network[3]）是运行在比特币网络上的DeFi应用程序，截至2019年7月5日，闪电网络的锁仓价值约为800万美元。EOSrex[4]发布后一个月共计锁仓了9000万个EOS，它使用户能够借贷EOSIO资源，比如CPU、内存和带宽等。EOS上还包括一个无需许可的货币市场协议——BUCK Protocol[5]。以太坊上第一DeFi应用是Maker[6]，它是区块链上的央行，每个人都可以通过将ETH存入其抵押债仓（CDP）来借用与美元挂钩的Dai，其挂钩目标价值为每个代币1美元。Compound[7]是一种借贷协议，称为以太坊上自动化商行，每个货币市场

都关联到一个充当协议上借出资产的中介cToken（比如cBAT），通过cToken，出借方可以获得随时间而累加的利息。Dharma[7]提供固定利率的固定期限贷款，贷方的存款只会在借款人使用资产时赚取利息，该平台可以手动处理和匹配交易，而无需在任何时间点担任托管人，用户可以请求借出资产，然后只需等待他们的请求被匹配，支持的资产包括ETH、USDC和Dai。BlockFi[8]提供的是最传统的借贷产品，用户可以抵押加密货币获得法币(上限由抵押金额决定)，用于日常金融交易，比如还抵押贷款、买车等等。BlockFi还可以从其发放的贷款中获得更大的利润，因为它的贷款额度更大。Nexo[9]是一种更传统的新型加密货币借贷工具。它的功能与信用卡的功能几乎完全一样，就是让那些持有加密货币的人可以通过抵押他们的加密资产换取法币信用额度(目前支持不限于45种法定货币)。Nuo[10]的功能与Maker非常相似——它提供了一种加密货币借贷协议，用户可以通过抵押一种加密货币来借另一种。与Maker不同，Nuo并不特别关注稳定性和降低市场波动的影响。

2.Dipper Network

开放金融系统需要一个高效和安全的区块链作为基石，为了提高吞吐量，以太坊引入分片方案，跨片交易是一个设计复杂、尚需时日完善的解决方案。我们因此提出并设计了Dipper Network，这是一个支持跨链技术的高性能公链，将连接到Cosmos Hub并接收来自Cosmos生态中其他类型的资产。未来Dipper Network将通过多种跨链技术去连接更多的区块链，包括Polkadot、Ethereum、Cardano等，在安全的前提下，接收、处理各类区块链资产，真正地实现价值的无缝流通。为了进一步支持高性能应用和提高网络的安全性，我们分层设计，采用Layer2方案，使Dipper Network得以承载更高频、复杂的计算。

2.1 系统架构

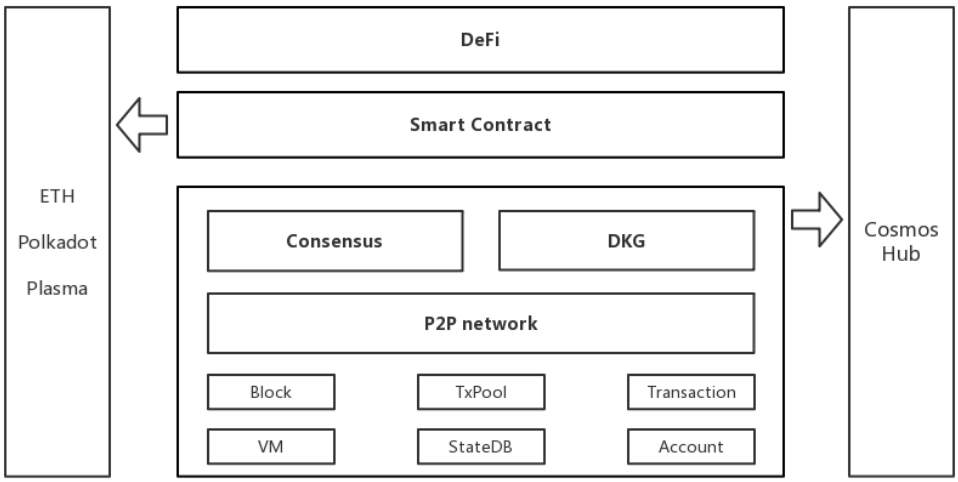

图1.系统总体架构

2.2 关键设计

2.2.1 状态模型

当前主流的区块链协议中，每个节点都需要处理所有的交易并存储所有的状态(余额、合约代码和存储等)。这种方式保证了网络安全的同时，也极大地限制了区块链的可扩展性，即一个区块链网络无法处理比单个节点更多的交易，这一点极大的降低了区块链的性能。

通过研究分层网络模型[19，20，21]，我们提出全新的状态模型：每一笔交易（transaction）包含事件（event）、状态（state）和证明（proof）。通过将计算和状态分离，在链下完成状态生成，在链上进行状态验证，通过使用零知识证明（例如zk-STARK[17]），在状态模型中实现通用的可验证计算，减少了链上验证的计算量，大大提升网络的交易处理能力。Dipper Network的状态模型如下图所示：

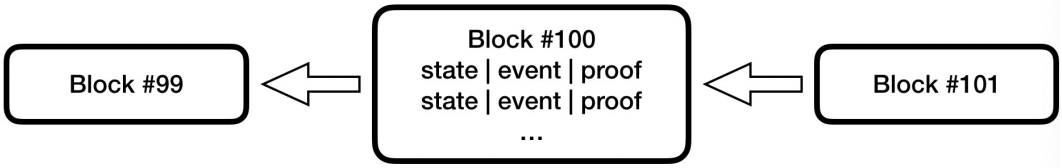

图2 状态模型

2.2.2 随机数

将随机数引入到共识算法中，为了实现记账的随机性，从而提高节点记账的公平性和网络的安全性，我们在共识算法中增加完全公平的随机数方案。共识过程中的区块提议者，由共识节点共同参与生成的随机数来决定。每一轮都会通过基于BLS的门限签名算法生成区块的最终签名，将其作为随机数并取模，将得到的值映射在基于节点权益和记账效率的序列中，从而得到完全随机的下一轮区块提议者。

随机数生成方案，将使用分布式密钥生成协议（Distributed Key Generation，简称DKG），即允许一组多方成员共同生成多项式，每一方都得到无偏差的随机密钥。DKG协议的运行结果是每一方能获得一份密钥对，并共享一个公共公钥。

2.2.3 共识算法

Dipper Network将基于Tendermint[18]共识算法结合DKG引入随机数，具备以下特性：

1）实现快速的交易确认

2）解决区块链的分叉、交易回滚问题

3）达到更高的网络吞吐量

4）生成公平的随机数

5）实现记账的公平

Tendermint作为一种优化的PBFT算法，只需要两轮投票即可达成共识。同时可以抵御双重攻击，并且能够容忍网络中一组高达1/3的拜占庭节点。Tendermint共识算法的分叉问责制，避免了传统POS算法的无利害关系问题，减少了节点恶意分叉的风险。为了最大限度地提高安全性和拜占庭容错能力，Dipper Network可以与Cosmos Hub共享相同的验证人集合。

Tendermint共识算法中，网络中主要有两种参与者：

1）验证人，参与共识过程中的投票，验证人的记帐权重各不相同；

2)提议者，使用公平的随机算法从验证 人集合中选出。验证人的记账权重越大被选为提议者的概率越高。

2.2.4共识过程

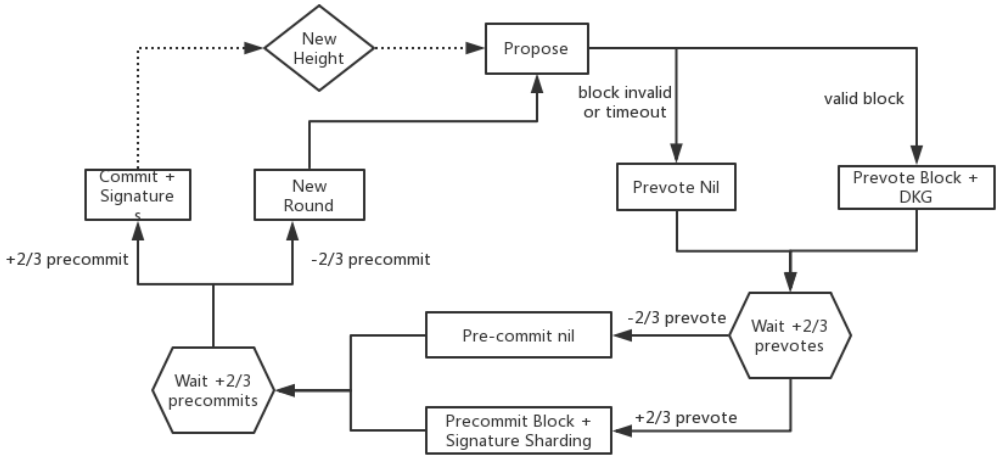

图3 共识算法流程

每一轮开始，验证人对新一轮的区块进行提议(Propose)。合法的提议区块，先经过一轮的预投票(Prevote)，在提议区块获得2/3以上的预投票后，进入下一轮的预提交(Precommit)，同样是获得2/3以上的验证人预提交后，被提议区块被最终确认。

我们在初始化过程中引入DKG，以便生成各方共享的密钥；在预提交阶段，我们使用上述共享的密钥基于BLS的门限签名算法生成签名分片（Signature Sharding），在最终提交的区块中合并成一个最终签名。利用这样的多方共同生成的签名来生成随机数，具有均匀性、相互独立和不可预测性，才能作为公平的链上随机数。

2.3 跨链方案

Dipper Network将仅通过区块链协议本身实现资产跨链，而不需要第三方（如中心化交易所）介入。目前Cosmos和Polkadot是最具前景的区块链跨链项目，两者多年深耕跨链领域，在去中心化社区中拥有良好的声誉。Dipper Network将打通Cosmos、Polkadot以及更多的区块链，让各类加密资产能高效流通起来，充分的发挥其金融价值。

2.3.1 Cosmos跨链

Dipper Network支持Cosmos生态内的资产跨链，通过IBC 连接Cosmos Hub，进而实现与以分区的形式连接到 Cosmos Hub的Zone blockchain通信。Dipper Network同时将实现Peg Zone允许实时的区块链（如以太坊）连接到Dipper生态内。

以Dipper Network与以太坊的跨链为例，分为2个过程：PegZone和以太坊跨链转Cosmos
体系内IBC跨链。图4描述了PegZone和以太坊跨链转账的流程，该案例中Alice通过以太坊公链将10个Eth转移到PegZone区块链，在PegZone中将等值的4个Eth资产CEth转账给Bob，Bob在PegZone区块链上执行了赎回交易，PegZone公链，Signer，Layer组件对Bob的赎回操作执行验证，签名，通知以太坊智能合约，在以太坊智能合约经过验证签名和交易等操作释放了4个Eth给Bob。

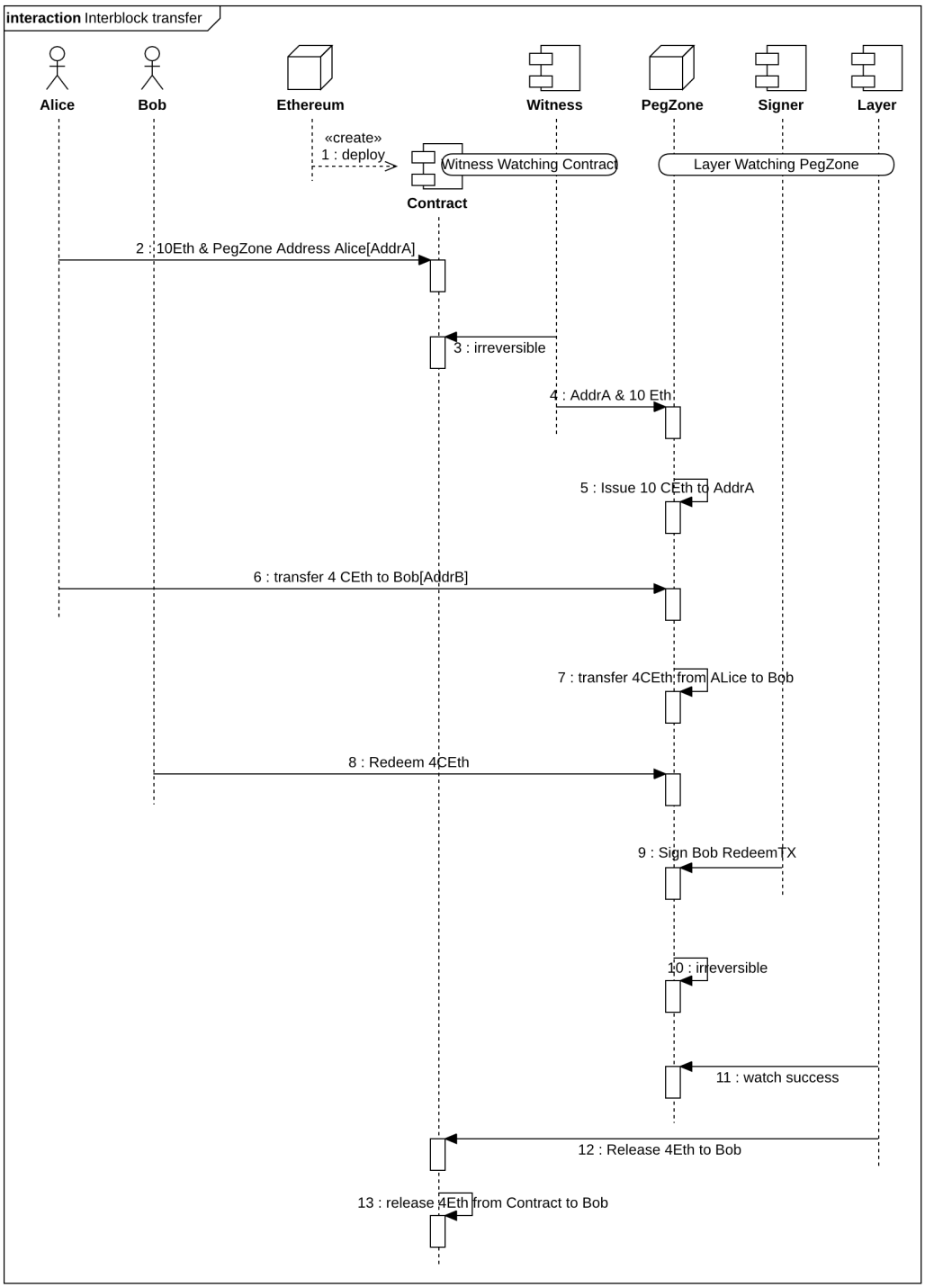

图4. PegZone和以太坊垮链转账的流程

1）Dipper Network在以太坊创建智能合约，用于记录和处理Eth在跨链转移的逻辑和数据

2）Alice通过以太坊智能合约执行跨链转账操作，转移10Eth到其在PegZone公链的地址

3）PegZone相关的Witness组件监听到该交易，继续监听直到该交易在以太坊公链不可逆

4）Witness将ALice的跨链转账请求发送到PegZone

5）PegZone验证转账通过后，向交易请求中的地址（这里指Alice在PegZone的地址，可以是任意地址）发放10个CEth表示收到了10个Eth价值的资产

6）Alice得知跨链转账成功后通过PegZone向Bob的地址转账4个CEth

7）PegZone验证交易并执行Alice的请求

8）Bob收到了Alice的转账后，开始执行赎回（表示从PegZone链赎回资产到以太坊）请求

9）Signer组件监听到Bob的赎回请求后，对交易进行签名并发送自己的交易请求到PegZone

10）Layer监听Signer的交易，直到2/3+的投票确认该交易

11-12）Layer确认赎回交易请求不可逆后开始执行转发交易请求到以太坊智能合约（调用以太坊智能合约接口）

13）智能合约根据逻辑释放4个Eth到Bob的以太坊地址。

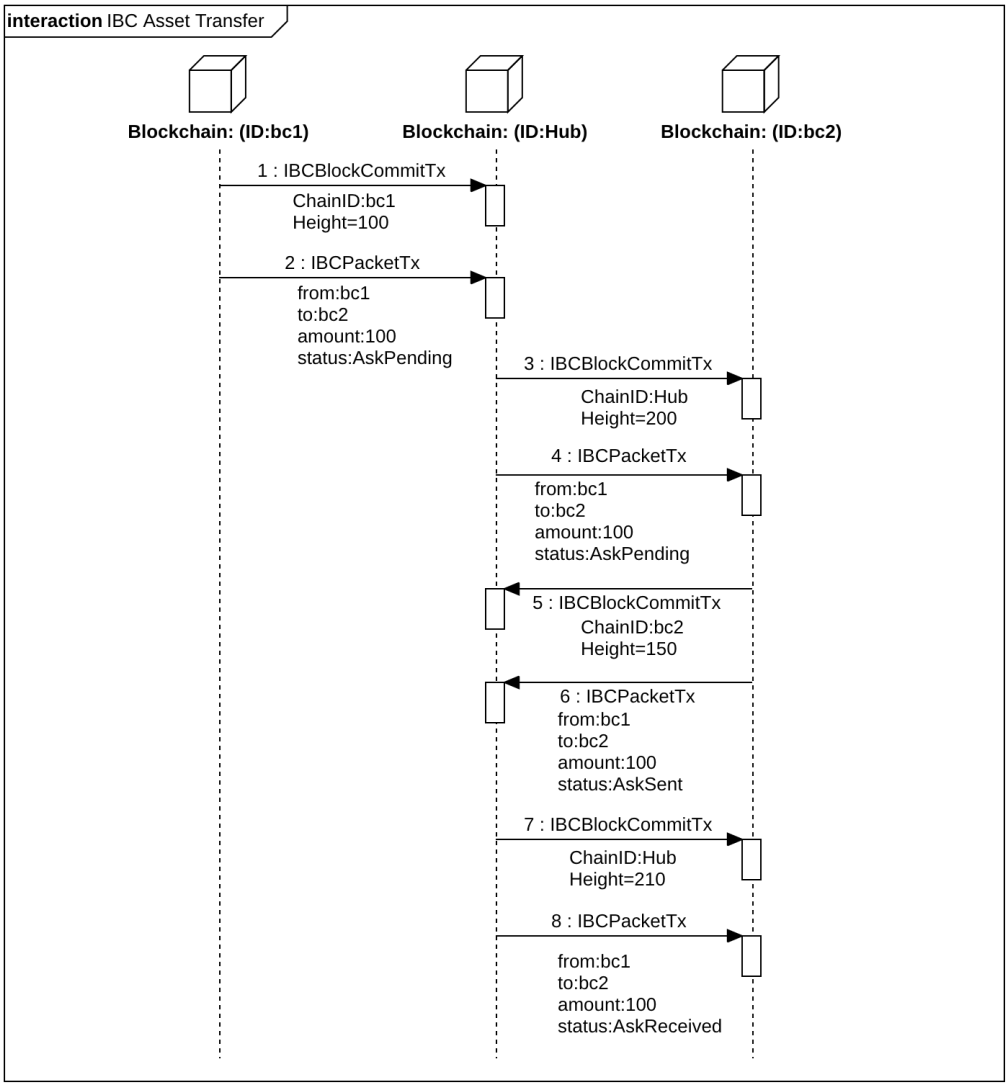

图5. Cosmos体系内IBC跨链转账流程

1）bc1链将区块高度信息发送给Hub链

2）bc1链发起跨链资产转移交易，资产转移方向为bc1-->bc2，资产数量为100个单位，交易的状态是AskPending，bc1验证交易成功后会将交易请求放到面向Hub的交易通道，中继程序监听到交易通道的交易请求生成Merkle Proof作为IBCPacketTx的payload发送到Hub

3-4）Hub验证step2中收到的IBCPacketTx，验证通过后以step1-->step2的逻辑步骤发送Hub的区块高度信息和跨链转账交易到bc2

5-6）bc2收到Hub的交易请求后，验证交易，验证成功后同步区块高度和确认可以接受转账请求交易到Hub

7-8）Hub发送区块高度并执行资产转移交易将相应数量的资产转移到bc2，完成跨链转账业务。

2.3.2 Polkadot跨链

Polkadot 作为一种区块链间协议，允许各个独立的区块链通过异构多链的架构以“无信任”的方式无缝地进行交易和信息交换。Dipper Network通过转接桥+中继链的跨链方式，打通Polkadot网络。当Dipper Network节点向其他区块链发送信息时，数据将通过Bridge（桥接器）传递到Relaychain（中继链），中继链再经过几次路由后，最后找到正确的Parachain（平行链），再由 Validator（验证者）验证，计算处理信息。

每个平行链拥有相同的完全节点来具体负责一个平行链，被称为*核对人（collator）*。这些*核对人*收集并验证来自用户的交易，然后将验证后的交易传输至负责*中继链（Relay chain）*的参与者--*验证人（validator）*，他们在*中继链*上运行相当于轻节点的节点，负责验证和广播发送自核对人的区块。为了确保*验证人*做出正确的行为并且不广播无效的交易，引入另一类参与者，称为*钓鱼（fisherman）*。他们只要证明*验证人*的错误行为，就会获得高额报酬。

交易由一个平行链到另一个平行链的工作流如下：

a）用户在*平行链* A上创建一个交易以向*平行链* B发送信息。

b）该交易被发送至*平行链* A的一个核对人。

c）该*核对人*确保该交易有效，并将其包含在一个区块中。

d）该*核对人*向*平行链* A的一个*验证人* 展示这个区块以及一状态转变证明。

e）该*验证人*验证得出该接收到的区块只包含有效的交易并抵押出他们的 DOT 代币。

f）当有足够的*提名人*抵押他们的 DOT 并提名*验证人*时，向*中继链*广播其区块将得到授权。

g）该交易被执行，同时，来自A的数据被发送到B。

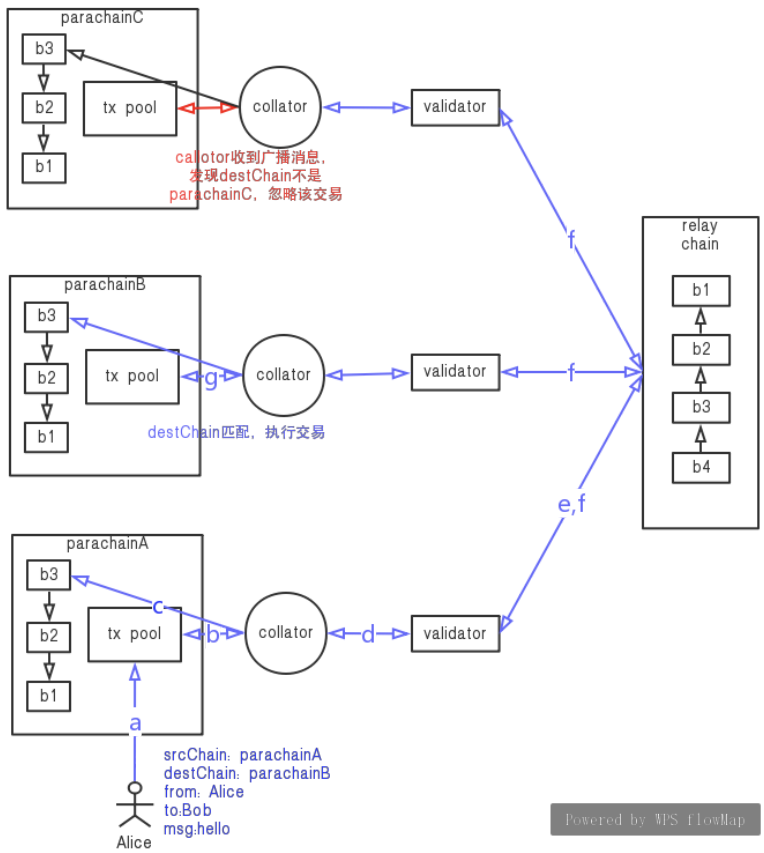

图6. Polkdota跨链通信流程

2.3.3 Layer2

当前公有链的交易处理能力面临着很大的性能瓶颈，即便是Cosmos， 在未来也将难以满足不断增长和多样的商业级应用。当前的主流方案包括在基于Layer 1的sharding和基于Layer 2的状态通道、Plasma等。sharding设计复杂，容易引起网络分区等安全性问题且跨片交易有诸多限制。因此我们选择Layer 2方案，对共识进行分层，在Layer1上专注安全和状态验证；在Layer2上专注性能和状态生成，这样可以实现更高的业务并发和安全性。

Dipper Network 将基于Plasma实现Layer 2方案：在root chain上部署Plasma合约来定义充值、提现、提交区块证明和欺诈证明等规则。当检测到side chain有恶意行为发生时，用户可以调用Plasma合约安全地在root chain上取回资产，side chain运行者将受到惩罚。针对各种作恶情形，Plasma设计了一系列经济博弈机制，比如设置取款延时、取款提以及交欺诈证明都需抵押资金等。其整体流程如下：

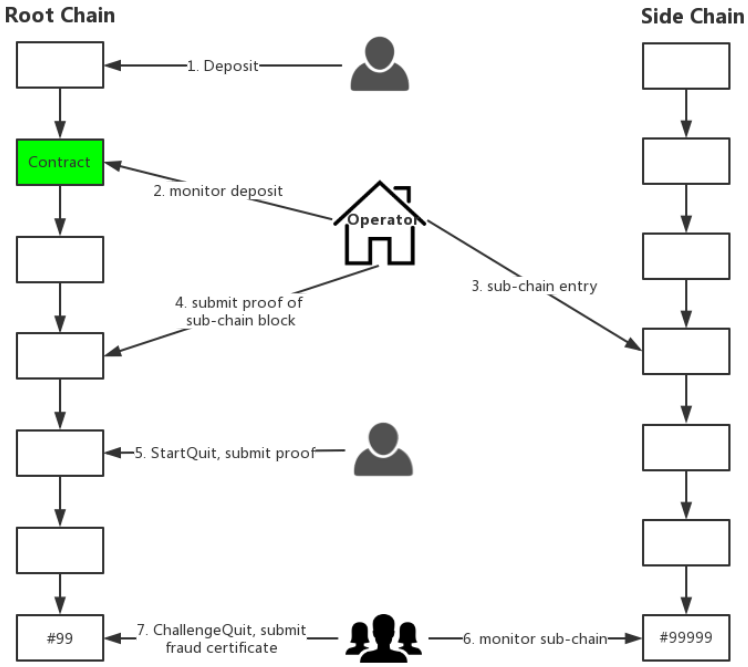

图7. Dipper Network的Layer 2流程图

1) root chain用户调用Deposit向Plasma合约充值，合约锁定将资产锁定在合约里面；

2-3) operator监听合约，检查合约内的资产锁定证明，在子链上为对应的用户入帐；

4) operator定期向Plasma合约提交side chain的区块证明，任何用户都可以向Plasma合约提交欺诈证明，合约验证通过并在在约定的争议期结束之后，撤销operator提交的区块，并对其进行惩罚；

5) 用户可以在任何时刻退出子链，调用StartQuit来执行取款操作，取回合法资产，这里有一个争议期（7天）。

6-7) 在争议期期间任何其他的用户可以调用ChallengeQuit发起挑战。若挑战成功则挑战者获取用户的退出保证金，用户退出失败并扣除退出保证金；若退出成功，Plasma合约发送合法资产至退出请求的用户。

3.DeFi Dapps

3.1 DipBank

DeFi生态中的借贷类应用，主要分为两种主流模式：资金池和P2P模式。资金池模式以Compound最为显著，动态的设置利率，提供了良好的流动性，但其可抵押通证的种类偏少，且使用会计准则无法保持先发优势；Dhrama则是P2P模式中最为活跃的应用，模拟传统的借贷模型，提供多样通证的90天定期借贷业务，但币价信息来源、利率的确定以及平台开发和更新过于中心化。基于以上思考，我们综合了两者的优势，设计了DipBank：一个功能完备、简单易用的借贷应用。一方面，它具备活期和定期两种服务，最大限度的提高资金利用率同时确保安全性；另一方面它拥有全新的Token激励机制并促进了DIP的有效均衡分发。详细设计如下：

3.1.1 贷出资产

1）在活期产品中，为了提供高效的资金流动性，我们设计了资金池，借贷双方无需设计贷款合约或者等待贷款到期。用户可以调用saving tokens来存入系统支持的资产，成为一种可替代资源，用户调用borrowing tokens借入资产。

2）在定期产品中，为了满足固定利率的投资需求，用户可以调用createFund tokens来创建，设置周期、利率和金额等信息，其他用户可调用supplyFund tokens来参加定期理财产品。

在系统中以dToken来代替用户资产，在活期产品中，随着货币市场来产生利息，用户的dToken的数量会相应增加。

3.1.2 借入资产

使用dTokens作为抵押品，用户可以从DipBank中借入资产转移到Dipper网络的任何地方。与提供资产类似，每个货币市场都有一个由市场力量设定的浮动利率，这决定了每种资产的借贷成本。借入资产一共分为两种模式：

1）在活期产品中，希望借入并且具有存储在DipBank中足够余额的用户可以在MoneyBank合约上调用marketBorrow。此函数调用检查用户的帐户值，并给予足够的抵押品，将更新用户的借入余额，将token转移到用户的Dipper地址，并更新货币市场的浮动利率。借款以与3-3中计算的余额利息完全相同的方式产生利息；借款人可随时调用repayBorrowMoney来偿还未偿还的借款的本金和应计利息。

协议持有的资产（由dToken的所有权代表）用作从协议借用的抵押品。每个市场都有一个抵押因子x，范围从0到1，表示可借入的标的资产价值部分，根据资金的流动性，我们设定不同资产的抵押因子x，后续的参数设计由管理委员会来设定。用户的借贷能力等于资产余额价值之和乘以抵押因子。

2）在定期理财产品中，借款人在MoneyMarket合约上调用marketFund（资产地址，金额，利率，期限）。此函数会调用检查用户的账户余额，并给予足够的抵押品，设置用户的借入金额。借款的利率是用户自由指定的，借款人在给定期限结束之后将自动偿还未偿还的贷款。如果借款人提前偿还贷款，将支付给定期限的利息。

如果用户的整体账户价值由于其抵押品价值变化（例如，用户持有DIP作为借入以太币的抵押品并且DIP显著降低价值）而低于清算比率，那么我们就有一个公共函数liquidateBankBorrow用于调用者的资产来交换借用者抵押品，比低于市场5-10%的价格。

3.1.3 账本和利率模型

DipBank的活期产品借鉴Compound，使用了业界主流的国际会计准则，对于每个货币市场均有一份完整且可审计的资产负债表和分类账：

$$Supply + Equity = Cash + Borrows \tag{3-1}$$

在定期产品模式中，由借款方自定义。在活期产品模式中，使用动态利率。根据经济学理论，利率应当在需求高时增长，在需求低时下降，使用资金利用率来衡量需求强弱程度。

$$userRatio = borrowingBalance / (borrowingBalance + cash) \tag{3-2}$$

$$borrowInterest = P1 + userRatio*P2 \tag{3-3}$$

$$lendInterest = borrowInterest*userRatio*P3 \tag{3-4}$$

P1，P2，P3将由治理委员会投票决定。每次交易发生，都会更新资产的利率，以复合自先前指数以来的利息，使用以每个区块利率计算的r * t计算的期间利息：

$$Indexn = Index(n-1)*(1 + r*t) \tag{3-5}$$

市场的未偿还借款总额更新为包括自上次指数以来累计的利息：

$$totalBorrowBalance_n = totalBorrowBalance_{(n-1)}*(1 + r*t) \tag{3-6}$$

3.1.4 市场状态

每个市场（由资产定义）包含三个状态：准备，运行或暂停。如果出于任何原因，必须改变市场的状态，相应的提案将由治理委员会讨论并作出决定，在此之前为用户提供重要的准备

时间。暂停的市场不允许用户继续供应或借入资产（尽管用户仍可以撤回或关闭借入的头寸）。

1）准备：每个市场都将以准备的方式开始，并可能转换为支持的状态。一旦成为支持状态的市场，任何用户都可以如上所述从市场供应或借入。

2）运行：市场在这个状态下正常运行，支持供应和借入资产。运行状态将会在出现借贷对价格出现可预见性风险的时候，由治理委员会决定是否需要转变为暂停状态。

3）暂停：一旦市场暂停，无论借款人的抵押品健康状况如何，该资产的所有借款都可以按标准折扣进行清算。

3.1.5 治理

从最初的阶段，DipBank即由的Dipper network选举的DAO来控制。 DAO将采用智能合约的形式，通过提案和投票，可以调用以下相关的功能。 协议中的以下权利由管理员或治理委员会控制：

1）选择新的委员会成员
2）设置市场的利率模型
3）准备，暂停或取消市场
4）选择Oracle价格来源
5）激活市场全局清算
6）是否接受合约更

3.1.6 风险和清算

我们设定抵押率是150%，DIP持有者可以投票决定每种类型的资产的抵押率。当发生借款时会出现以下三种情况：

1）当抵押率高于150%时，系统正常运行；

2）当抵押率低于150%时，触发清算机制，抵押的资产dToken将当前市场价格减去清算折扣进行清算；这种激励是套利者的生态系统快速介入以减少借款人的风险，并消除协议的风险。

有资格关闭的比例是一个紧密因素 ，是借入资产的一部分已偿还，范围从0到1，例如25%。 可以继续调用清算过程直到用户借款少于借款能力。拥有借入资产的任何地址都可以调用清算功能，将他们的资产换成借款人的dToken抵押品。 作为用户，资产和价格都包含在Bank协议中，清算不依赖于任何外部系统或订单簿。

3）在发生极端的事件中，抵押率在瞬间低于100%，系统将暂停市场并启用预设的风险储备金补贴用户。

3.1.7 Token激励和分发机制

我们设计了借贷激励算法：贷出和借入行为除了应获得和支付利息，还将获得DIP作为激励，DIP将根据利率同时补贴给借贷双方。通过token激励来促进借贷，有利于促进Dipper network的正向循环，提高网络的使用率和安全性，从而形成稳定的经济闭环。

3.2 基础金融协议

我们将进一步在Dipper netowrk上构建完整的基础金融协议：稳定币DipUSD，提供流动性的去中心交易所DipDex，重要的衍生品市场DipDER，合成资产DipSYN，完善的资产保险服务DipINS，提供可靠外部信息的预言机DipORC等。

4.经济模型

经济模型是公有链的灵魂。通过引入经济激励，比特币第一次解决了开放网络上的共识难题。每一个区块链网络都是一个通过经济激励结合在一起的自治共同体。一个优秀的经济激励

制度应该引导区块链的参与者为这个自治共同体作出贡献，最大化区块链的效用，激励用户、开发者和节点运行者合力为共识的形成与保存贡献力量。

Dipper network同时支持智能合约和多通证模型，通证将保存在各个区域，并可通过Dipper Network从一个区域移动到另一个区域。在最初的阶段，有两种类型的通证可以支持Dipper网络的操作：Staking token和Fee token。

4.1 Staking token

采用与Cosmos网络[15]类似的质押机制设计，Dipper network拥有自己的特殊本机通证用于质押，该通证将被称为“DIP”。DIP可以用在多种情形之中，比如：

1）通过验证器和委托人系统将DIP令牌集成到Dipper network的共识引擎验证器中；

2）投票权参与Dipper网络的治理；

Dipper Network的安全程度与共识节点抵押的代币数量息息相关，共识抵押代币越多，节点作恶成本越高，整个系统也更加安全。DIP也代表着Dipper Network上的存储资源，拥有的DIP越多对应更多的状态空间，以有效的应对状态爆炸问题，这样有助于系统的长期运行，有效地捕获链上生态的价值。

4.2 Fee token

网络费用令牌用于防止垃圾邮件，并在维护分类帐时向验证人付款；Dipper network旨在支持来自Cosmos网络的所有列入白名单的费用令牌，例如Photon，以及IRIS令牌。

当前主流用户难以使用区块链的一个重要原因是，交易手续费必须以原生代币进行支付，由此要求用户在使用服务之前自行寻找方法先获取原生代币，提高了使用门槛。另一方面，用户已经习惯了基本服务免费，增值服务收费的商业模式，无论做什么都要收费也不符合主流用户习惯。我们计划采用Cosmos的功能，支持各种列入白名单的费用令牌，它可以为网络参与者提供增强的体验。在Cosmos中，对于网络费用令牌，每个验证器都有一个配置文件，用于定义他们对每个费用令牌的价值的个人权重。

系统手续费的分配比例由投票决定，收入的大部分由出块节点获得，剩余的部分将用于支持Dipper网络的开发、研究、运营等工作，以保证网络的持续良性发展。

5.路线图

Dipper Network的路线图包含如下几个阶段：

第一阶段，Dipper Network测试网上线

第二阶段，Dipper Network正式网上线

第三阶段，DipBank、DipDEX等上线

第四阶段，定制IBC协议和异构网络跨链方案

第五阶段，构建完备的基础金融协议

第六阶段，全面的普惠金融服务

结论

我们认为在区块链扩容以支撑商业级应用的潮流之下，任何一条公链无法有效承载所有的价值，头部公链之间会形成自己独有的业务聚集地，而跨链将作为一个核心桥梁的存在，连接各类公链，汇聚价值从而产生规模效应，因此我们将Dipper Network构建于跨链生态之中，专注于金融应用，重新定义去中心化金融，让金融真正地惠及每一个人。

我们通过DipBank为加密资产创造了正常运作的货币市场，每个货币市场的利率都是由货币的供需决定；当借入资产的需求增加或供应降低时，利率上升，激励额外的流动性，用户可以向货币市场提供代币以赚取利息，而无需信任中间方，用户可以使用协议中的余额借用代币（使用，出售或再出借）。我们设计了创新的token分发机制来补贴用户，构建网络经济生态，从而避免冷启动，同时设计完全中心化的机制，让token持有者深度参与治理。

在未来的工作中，我们将在以下几个方面展开。首先是深入研究跨链机制，综合各种跨链方案的优势提高安全性；其次是构建完备的基础金融设施并设计标准接口，让各种类型应用的高效组合使用；第三，深入研究零知识证明，实现通用型的可验证计算；第四，增强可扩展性，优化Layer2解决方案；第五，支持隐私交易，比如实现mimblewimble协议；第六，优化加密经济设计，让链上资产与底层公链更好的锚定起来。

团队

核心成员

黄志勇	CEO	前公信宝首席研究员，前中移杭研工程师，连续创业者
罗田佳	CTO	高街时尚技术总监，前华为优秀工程师，连续创业者
朱礼廷	Conselor	前公信宝首席架构师，Graphene社区开发者，全球石墨烯区块链应用中心技术顾问
Joy	Operator	国际知名教育机构COO， IB国际教育认证专家
侯晋炜	Bussiness	知名社群运营推广者，连续创业者

致谢

Dipper的设计经历了多次迭代和演变，每次都是基于Dipper Labs开发者的工作，我们要感谢所有人在设计过程中所做的出色贡献。感谢Ethereum社区、Cosmos开发人员及其社区以及Polkadot社区的工作。

让我们共同携手创建美好未来!

术语表

DeFi	一个由建立在无需许可的区块链、点对点协议和去中心化网络上的应用所组成的生态系统，用于促成借贷行为或金融交易。
Plasma	是一种实现区块链链下扩容的方案，通过创建经济激励来实现自动和链上状态的持久化，而不需要合约创建者的状态转换管理。
DKG	Distributed Key Generation，分布式密钥生成算法，用于在分布式系统的节点中生成共享密钥。
BLS	短签名算法，主要思想是待签名的消息散列到一个椭圆曲线上的一个点，并利用双线性映射e函数的交换性质，在不泄露私钥的情况下，验证签名。BLS的算法在签名合并，多签，m/n多签有丰富的应用。
MPSS	Mobile Proactive Secret Share，移动主动密钥分享算法，用于在不同的节点分组之间动态的更新和转移密钥。
VRF	Verifiable Random Function，可验证随机函数，由Micali，Rabin和Vadhan提出，是一种伪随机函数，可以提供其输出正确性的公开可验证的证明。
VC	Verifiable Computation，可有效验证结果数据是否按照原始数据依照指定逻辑计算而来。
Zkp	Zero-Knowledge Proof，零知识证明，证明者让验证者确信某个事实的正确性，并不泄露其他任何信息（零知识）。

参考文献

[1] TresuaryDirect. The data on total public debt outstanding 1993-2019.
[2] The coming pension crisis. Citi GPS: Global Perspectives & Solutions, 2016
[3] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. Tech. rep. Technical Report (draft). https://lightning.network, 2015.
[4]https://eosrex.io/
[5]https://medium.com/@dmitry.yunodo/buck-protocol-is-live-fef2cf5765d7
[6]Maker Team. The Dai Stablecoin System (2017). https://makerdao.com/whitepaper/DaiDec17WP.pdf
[7]https://www.dharma.io/
[8]https://blockfi.com/
[9]https://nexo.io/assets/downloads/Nexo-Whitepaper.pdf?n=2
[10]https://www.nuo.network/
[11] Eric Lombrozo, Johnson Lau, Pieter Wuille. Segregated Witness (Consensus Layer). https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. 2015.
[12] Sharding FAQ. https://github.com/ethereum/wiki/wiki/ShardingFAQ, 2016.
[13] "Micro-raiden: A payment channel framework for fast and free off-chain erc20 token transfers." [Online]. Available: https://raiden.network/micro.html
[14]Gavin Wood. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK. https://github.com/w3f/polkadot-white-paper/raw/master/PolkaDotPaper.pdf, Nov 2016.
[15] Jae Kwon jae, Ethan Buchman. Cosmos: A Network of Distributed Ledgers. https://cosmos.network/cosmos-whitepaper.pdf, 2016.
[16] Poon J, Buterin V. Plasma: scalable autonomous smart contracts. See https://plasma.io/plasma.pdf. 2017.
[17] Eli Ben-Sasson, Iddo Ben-Tov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. https://eprint.iacr.org/2018/046.pdf, 2018.
[18]J. Kwon. TenderMint: Consensus without Mining, August 2014.
[19] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Jonathan Katz and Hovav Shacham, editors, CRYPTO 2017, Part I, volume 10401 of LNCS, pages 357—388. Springer, Heidelberg, August 2017.
[20] Will Martino. Kadena: The first scalable, high performance private blockchain, http://kadena.io/docs/kadenaconsensuswhitepaper-aug2016.pdf, 2016.
[21] Jan xie. Nervos CKB: A Common Knowledge Base for Crypto-Economy.

法律声明

Dipper Network Tokens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:

(a) 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;

(b) 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)或绿卡持有者，或居住在美国;

(c) 根据您所在地区的法律律、法规要求或规则，您不在禁止止、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；
(d) 您同意符合以上描述的条件限制和约束。

风险提示

本信息并不代表投资建议、或同意销售的许可，以及引导和吸引任何的购买行为。