Galileo 新一代区块链跨链开发平台（技术简要）

一、引言

比特币的诞生，也是第一代加密数字货币的出现，区块链技术得以发展起来，当前阶段区块链有无数众多不同的链，链与链之间的数据隔离形成了区块链不同公链之间的价值分离。从技术的角度，token 是区块链的价值载体，token 本质上是加密的数字信息，token 执行信息流的传递过程与价值的传输过程，在单一用户前提条件下，如何实现区块链上两种不同属性的分布式账本之间的价值信息流的同步协作问题。跨链不仅仅是信息的传输过程，它是链与链之间的信息互动融合的过程，跨链也不只是技术层的传输交互协议，从能量守恒推出价值守恒定律，区块链的本质是不同链之间的信息价值流的流动过程。

当前区块链跨链机制有：公证人机制、侧链/中继人、哈希锁定、分布式私钥控制等技术，早期跨链技术包括以瑞波和 BTC Relay 为代表，它们更多关注的是资产转移，现有跨链技术以 Polkadot 和 Cosmos 为代表更多关注的是跨链基础设施。我们现在提出一种分布式的跨链交互机制，可实现多链多共识下的信息价值流之间的流通。基于分布式私钥控制技术的解决方案，通过对节点实时数据的解析服务，新一代的分布式众源数据交互协定，可以完成不同分布式账本之间的连接与价值传输过程。Galileo 致力于打造未来全球化的区块链基础设施，开创分布式智能经济新生态。

二、概述

Galileo 是新一代分布式跨链数据交互架构，基于高性能的区块链 DAPP 开

发平台的定位，Galileo 首次引入以主动式安全为核心兼具高性能的友好型的智能合约机制，我们提供新一代智能合约开发语言 NAM 与模块化（BAAS）开发平台，开发者可根据自己的应用需求进行个性化定制智能合约，智能合约的运行环境为 NAM VM，通过 VM 的本地运行环境，提升开发的高效性。

Galileo 的分布式跨链交互架构提供了发行数字资产的权限与兼容不同主链之间的相关智能合约协议机制。不同链之间的价值信息流可以通过 Galileo 的分布式众源数据交互协议与分布式私钥控制技术可以在不同主链之间进行数据交互，未来将兼容更多的应用场景 DAPP 进行跨链数据的交互支持。

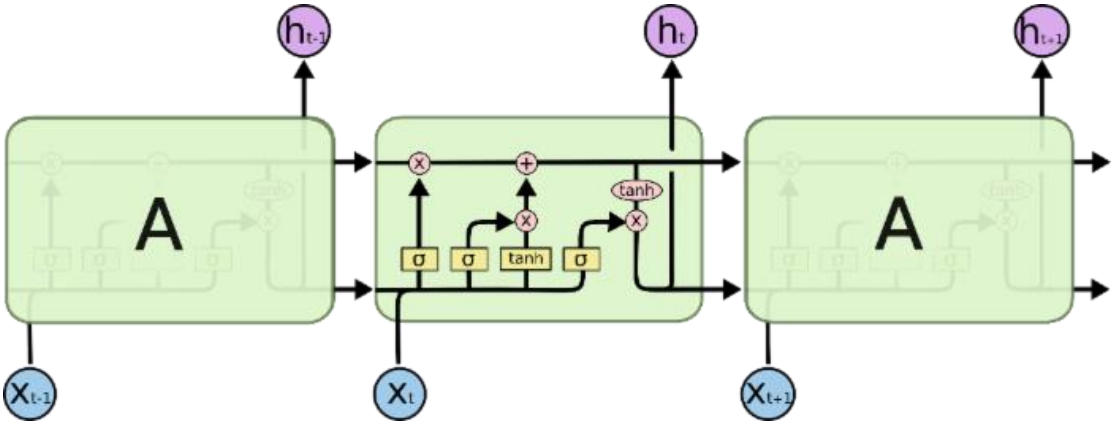
Galileo 的分布式跨链交互机制，们认为跨链的实质意义在于提供了一套链与链之间的清算机制，也是一种分布式精确记账。跨链是当前区块链行业急需的基础设施之一，区块链构筑的分布式智能经济协作新模式的高速公路需要跨链的桥梁进行嫁接。

Galileo 主链提供统一的跨链交互的 API 与 SDKS，不同主链（联盟链、私链）、DAPP 应用层等都可以通过 MDA 机制进行不同业务需求的数据存储、验证与确认，未来将支持更多的应用场景下的 DAPP 的跨链的数据需求。用户可以在不同链之间进行价值信息流的 DAPP 进行切换，使用与开发成本进行降低，主链支持主动式安全防护机制的智能合约，通过算法升级模式，可支持抗量子支持等算法。

三、共识机制

Galileo 采用主链+子链的设计方案，采用基于 Network of Neuron 的新一代共识机制——超级共识机制 L—DPOS+DBFT（lstm 深度学习优化共识算法）。

LSTM 网络（Long Short Term 网络）：



LSTM 网络

LSTM，全称为长短期记忆网络(Long Short Term Memory networks)，是一种特殊的 RNN，能够学习到长期依赖关系。LSTM 在设计上明确地避免了长期依赖的问题，循环神经网络都有着重复的神经网络模块形成链的形式。

在公有链主链中，我们采用 PBFT 共识算法(Practical Byzantine Fault Tolerance，实用拜占庭容错算法)维持基础交易的合法性。PBFT 共识在保证灵活性和安全性的前提下提供了(N-1)/3 的容错性，它使用加密技术防止欺骗攻击和重播攻击，以及检测被破坏的消息。每一个 Message 包含了抗量子公钥签名(RSA256 算法)、消息验证编码(MAC)、无碰撞哈希函数生成的消息摘要(Mes- sage Digest)等。

在子链中可采用 DPOS 共识机制，对 Galileo 主链数据业务层面进行验证管理。DPOS 通过投票选举中的超级节点完成交易确认，可大幅提高交易并发规模和确认速度，通过签名的可信任记账人证明，消除了交易等待验证的时间消耗，便于 Galileo 用户快速提交业务请求，同时降低了交易手续费成本。

为了提升交易确认的时间我们通过 Dpos（股份授权证明机制），大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

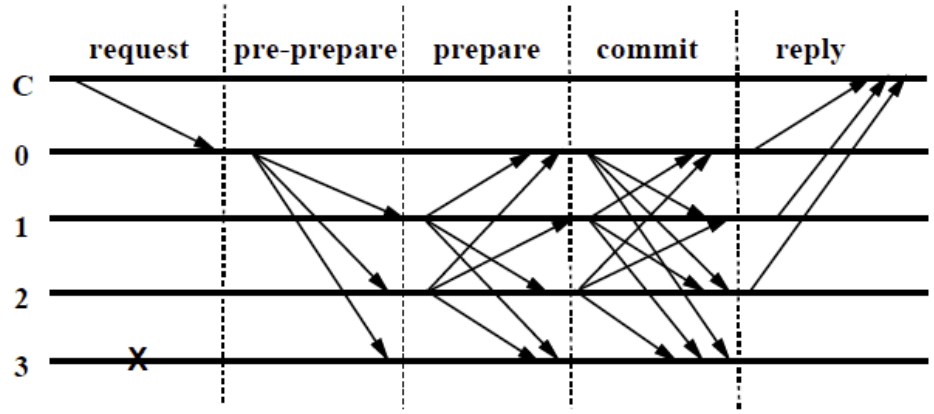
DPOS+PBFT，DPOS 是一种更为去中心化，也更节省资源的共识机制，

PBFT 则解决了 DPOS 的安全隐患，有效降低了分叉的风险，使系统更加安全。

- 在主链中采用 PBFT 共识机制：共识效率高，可实现高频交易。

假设节点总数为 3f+1，f 为拜占庭错误节点：

当节点发现 leader 作恶时，通过算法选举其他的 replica 为 leader。leader 通过 pre-prepare （第一个协议阶段）消息把它选择的 value 广播给其 replica 节点，其他的 replica 节点如果接受则发送 prepare（第二个协议阶段），如果失败则不发送。一旦 2f 个节点接受 prepare 消息，则节点发送 commit（第三个协议阶段）消息。



当 2f+1 个节点接受 commit 消息后，代表该 value 值被确定 如下图表示了 4 个节点，0 为 leader，同时节点 3 为 fault 节点，该节点不响应和发出任何消息。最终节点状态达到 commited 时，表示该轮共识成功达成。 注：预准备阶段（pre-prepare）： 主节点分配一个序列号 n 给收到的请求，然后向所有备份节点群发预准备消息，预准备消息的格式为<<PRE-PREPARE,v,n,d>,m>，这里 v 是视图编号，m 是客户端发送的请求消息，d 是请求消息 m 的摘要。 准备阶段（prepare）：如果备份节点 i 接受了预准备消息<<PRE-PREPARE,v,n,d>,m>，则进入准备阶段。在准备阶段的同时，该节

点向所有副本节点发送准备消息<PREPARE,v,n,d,i>，并且将预准备消息和准备消息写入自己的消息日志。如果看预准备消息不顺眼，就什么都不做。确认阶段（commit）：当(m,v,n,i)条件为真的时候，副本 i 将<COMMIT,v,n,D(m),i>向其他副本节点广播，于是就进入了确认阶段。

- 在子链中采用 DPOS 共识机制，在 Galileo 主链上共有 21 个节点维护网络的运转。

DPOS 工作原理:

```
for round i
    dlist_i = get N delegates sort by votes
    dlist_i = shuffle(dlist_i)
    loop
        slot = global_time_offset / block_interval
        pos = slot % N
        if delegates[pos] exists in this node
            generateBlock(keypair of delegates[pos])
        else
            skip
```

Galileo 的主链共识机制为 PBFT，子链采用了 DPOS，但是其他主链可以通过 Galileo 提供的分布式跨链交互机制，自由的定制其他共识机制，比如 POW、POS、Paxos 等。

四、主要核心技术创新点

高并发

新一代超级共识机制 L—DPOS+DBFT (lstm 深度学习优化共识算法)，基于 Network of Neuron 的数据底层的结构优化，将提升 TPS 的计算瓶颈，未来在 DAPP 的高性能运算需求，基于软硬件结合的思想来搭建高并发的应用开发平台。

可拓展性

创新的智能合约的机制设计，首次引入主动式安全为核心兼具高性能的友好性智能合约机制，Galileo 的可拓展性可支持不同应用场景的 DAPP 的部署。新一代智能合约开发语言 NAM 与模块化（BAAS）开发平台，开发者可根据自己的应用需求进行个性化定制智能合约，智能合约的运行环境为 NAM VM，通过 VM 的本地运行环境，提升开发的高效性。

跨链数据交互协议

通过分布式私钥控制技术与基于分布式众源数据（MDA）交换协议，可支持 25+主链上数据的存储、验证与确认，未来将支持更多的应用场景下的 DAPP 的跨链的数据需求。

分布式众源数据交换协议

- 基于区块链上的可量化的多维数据源(POI/ROI)，进行 节点地址解析服务，通过内置智能合约机制为不同 场景应用需求提供数据分布式存储、节点数据验证、 交易与共享等功能；
- 通过轻量化的开发框架与应用部署，分布式的节点 确保量化的数据

源的安全性，推动可信编程化社会 的到来。

分布式节点机制

基于区块链/分布式节点部署的链网体系，从单个节点的建设贯彻去中心化的思想。通过节点的优化设计，高性能的低延迟效率，Galileo 预计在 0.5S 完成交易的确认环节，相比之下比特币和以太坊分别需要 60 分钟和 120 秒的时间来完成。

实用性

Galileo 网络上采用极低的运算费用来设计架构 DAPP 的应用层设计，通过节点的竞选机制和民主投票机制，充分了解用户的期望与需求，进行商业化产品更加便捷。

分布式存储

分布式节点组成的链网体系，数据库复制成 多份保证冗余性，然后分成很多个小部分， 分散存储到网络的众多节点上，这样只要有 足够多的节点运作正常，数据就是安全的。 冗余系数、分割的份数、是否加密存储以及 由哪些节点还是全部节点负责存储，由具体 的应用决定。

分布式云存储

去中心化的源码托管服务

分布式数据存储管理平台

五、原生开发语言 NAM

为了方便开发者基于 Galileo 开发符合自己实际需求的智能合约。我们设计了一门新的智能合约开发语言：NAM。NAM 是一个事件驱动的语言。事件分为两种类型：用户事件和系统事件。用户事件是指 DApp 客户端的调用。经过 DApp 的共识之后，DApp 客户端会发送一个事件到智能合约。系统事件是指区块完成打包、某个交易处理完成或者智能合约订阅的一些其他事件。另外 NAM 也支持面向对象的编程，开发者可以使用面向对象的思想来进行开发。另外，我们后期还会增加对主流编程语言如 Java、nodejs、Python 等的支持，方便开发者快速开发自己的 DAPP。

1.NAM 的特点

事件驱动。NAM 是一个事件驱动的语言。它与一般语言(比如 C/C++、Java、Golang 等)不同，NAM 没有 main 函数，所有的代码都是围绕事件去执行。

面向对象。NAM 支持面向对象的编程范式。它是一个天然支持模块化设计的语言。开发者可以把一些常用的结构体封装成一个对象，然后在对象里封装一些方法。在事件驱动的函数里可以对对象的属性和方法进行调用。

模块化设计。在 NAM 中，我们鼓励开发者把不同模块的代码放到不同的包中，方便上层调用。

2.NAM VM

我们为 NAM 语言设计了一个执行环境。这个环境就是 NAM VM。和以太坊的开发语言 Solidity 难以调试不同，NAM VM 可以让开发者方便的在本地运行和调试 NAM。 另外 NAM VM 还会提供 API 来让开发

者模拟事件。用户可以很容易的使用 Python、Java 或者 JavaScript 等语言编写测试用例，用来测试智能合约是否可以满足需求。

3. 原生函数

在 NAM 的底层中，有许多基础库可以调用。这些基础库也会不断完善。以 NAM 支持的原生数据库操作函数为例，在 GALILEO 系统中， 智能合约封装在底层的磁盘操作之上，可以直接操作数据库。NAM 为开发者提供了三种方式的数据库操作：SQL、文档型（类似 MongoDB）和 KV 型。开发者只需要导入响应的包即可完成响应的操作。这些方式可以极大的提高开发者的开发效率，降低开发难度。

六、相关接口：

1、API

提供 API 网关服务

2、应用开发程序包（SDKS）

应用程序开发包（Application Software Development Kit） 是基于不同开发语言对区块链操作和功能的综合性服务包，提供加密、数据签名、交易生成等综合性服务功能接口，可以扩展集成特定业务逻辑功能，无缝支持各类语言业务系统的集成与功能扩展。将支持 Java、JavaScript、.NET、Ruby、Python 等多种语言 SDK。

3、DAPP

DApp 分为 DApp 服务端和 DApp 客户端两个部分。DApp 服务器就是智能合约，利用 NAM 语言编写完成，后期也会对主流语言如 Java、nodejs、Python 等进行支持。DApp 客户端是基于 JavaScript 的一个框架，用户可以

根据自己的需求利用这个框架实现客户端的功能。

Galileo 在设计智能合约之处就考虑到了现有智能合约的缺陷，比如上手难度大、与业务无关操作较多等。通过 Galileo 提供的 NAM 智能合约开发语言和 NAM VM 虚拟机，开发者可以只关心业务逻辑，进行基本的学习就可以快速上手。

4、模块化 BAAS(Blockchain As a Service)开发平台

通过 BAAS 模块化平台，普通开发者可以个性化定制自身需求的区块链分布式 DAPP。

5、基于 FPGA 的软硬件结合高性能应用场景解决方案。

通过软件优化与硬件通过 CPU、基于 ARM 的 GPU 的硬件加速模式驱动在针对 DAPP 应用场景有更高需求，可支持十万级 TPS 的运算处理需求。

七、应用场景

分布式交易：

分布式交易所、分布式场外交易、

中心化竞价撮合与分布式清结算混合模式的交易所。

数字金融创新与可拓展应用场景

金融行业

交易领域

财富管理

衍生品交易

批押品管理

供应链金融

支付

小额支付

B2B 国际汇款

税务申报与统计

了解您的客户

反洗钱

保险

索赔申请

索赔处理与管理

欺诈检测

远程信息处理和评级

数字认证

物联网

支付设备

自动化操作

电网管理

智能家居管理

办公室管理

消费行业

共享经济

供应链管理

药物跟踪

农业食品认证

物流管理

媒体

数字版权管理

艺术认证

广告刊登

广告点击的真实统计

正版资产的转售

软件开发

微粒化工作

人工支付

面对开发者的直接付款

API 接口平台

公证和认证

医疗卫生

病历共享

处方共享

多重认证

个性化医疗

DNA 测序

资产标的

钻石

设计师品牌

汽车租赁和销售

住房抵押

土地所有权

实体资产数字化

社会管理

投票

车辆登记

福利分配

版权保护

教育和认证