**上海大学“区块链”课程论文考试**

**ChainLink项目分析**

姓名：**刘斯祺** 学号： **21121678**

**字数：4678**

**摘 要：**

由于智能合约无法访问现实世界中的数据，这时预言机作为连接链上和链下的重要工具便显得十分的重要。而ChainLink作为预言机中最重要也是最有影响力的项目，本人认为具有分析的价值。作为重要的数据传输节点，保证数据的安全与真实性是重中之重。还有一点值得讨论的是一旦这个项目实现落地我们是否需要将所有的数据传输到区块链上，或者有哪些数据需要传输，哪些数据不能传输，这都是本篇论文重点讨论的地方。

**关键字：**数据安全、去中心化、预言机

**论文评语：**

成绩： 任课教师：吴建刚

1. 经济模型分析

1.1项目介绍

ChainLink是2017年6月由旧金山的一家金融科技公司SmartContract推出的项目，是区块链系统中第一个去中心化的预言机，ChainLink可以算得上是预言机概念中的龙头项目，旨在为智能合约提供可验证的真实数据。

ChainLink本质上是一个为区块链网络和链外提供服务的分布式预言机网络，通过智能合约，区块链网络上运营着各种各样的Dapp，但是这些Dapp不仅需要区块链上的数据，还需要区块链以外的数据。打个比方，用户在区块链上开了一个电商平台，除了需要用户上传到电商平台上的商品图片、商品评论等链上数据外，用户还需要调用顺丰、中通等快递服务的数据，而这些数据属于链外的，那么这个时候就需要ChainLink这种预言机系统来打通链上链下数据。

1.2项目团队

ChainLink的联合创始人兼首席执行官Serge Nazarov，中文名为：谢尔盖·纳扎罗夫，他在启动SmartContract之前，曾担任安全资产交换公司(Secure Asset Exchange)的创始人，这是一个类似于ShapeShift的交换网络。

ChainLink的联合创始人兼首席技术官史蒂夫·埃利斯，曾与Sergey Nazarov合作进行安全资产交易，曾在Pivotal Labs担任软件工程师。

顾问团队：康奈尔大学科技计算机科学教授和IC3主任阿勒·朱尔斯，伊利诺伊大学计算机科学副教授安德鲁·米勒和一个爱心基金会的主要成员哈德森詹姆森。

从该项目的项目团队可以说是十分有实力，无论是从技术上还是资金上都有很好的支持。尤其它的首席执行官曾创办了安全资产交换公司，在安全产业方面应具有丰富的经验。

1.3项目目标

ChainLink的目标是构建一个完全去中心化的预言机网络，其主要想法是为预言机打造一个可信的市场，有良好行为的预言机节点会受到激励，其表现和声誉会公之于众反之有恶意行为的节点会受到惩罚（起到大众监督的作用）。

用ChainLink官网的说法就是：智能合约本质上是与世隔绝的（区块链是非常安全可靠的价值交换网络，但却无法安全防篡改的获取链下数据或将数据发送至链下系统），ChainLink预言机将智能合约连接至链下数据、事件、支付等，并保障防篡改性和可靠性。这将有利于扩展区块链的功能。

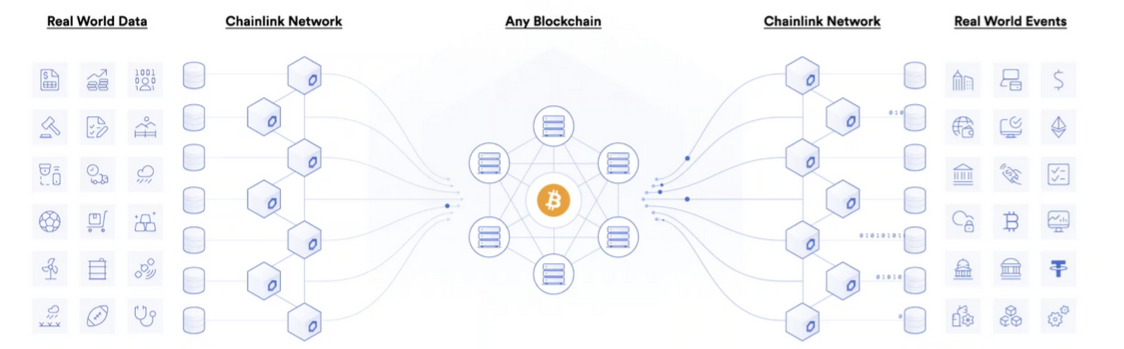


图1.ChainLink想实现的终极目标

在2021年，ChainLink在官网上发布了最新一版的白皮书，并发文详细的说明其计划

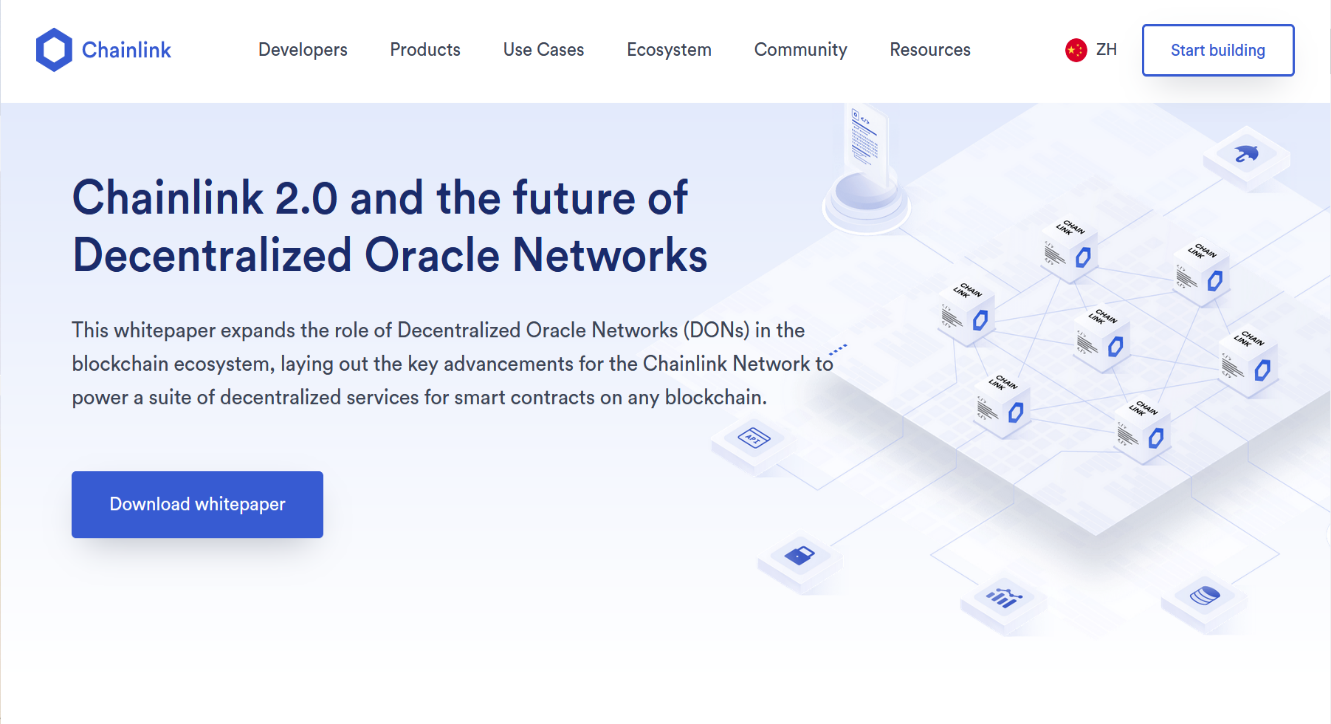


图2.ChainLink官网推出白皮书2.0版

ChainLink作为加密世界的预言机已经得到了巨大的发展，但预言机本身的限制，似乎有限制到ChainLink网络的多元化，所以在白皮书2.0里可以看到ChainLink有向更加广泛的加密货币网络发展的思路。在白皮书2.0中ChainLink将着眼于创建用于计算的Oracle网络。ChainLink联合创始人Sergey Nazarov表示，新的Oracle网络将继续专注于区块链甚至第二层网络无法实现的功能，未来ChainLink的混合智能合约将定义行业的未来。

在预言机的传统理解里，通常认为这是一种外部数据上链的安全可靠的方式。而ChainLink白皮书2.0创建了一个用于多个互操作的去中心化Oracle网络(DON)的框架，每个网络都由节点的集合组成，这些节点可以双向传输数据并使用各种共识协议执行去中心化的链下计算。与第2层技术类似，Chainlink DON锚定到现有的区块链上，以便定期同步数据输出和状态变化计算出的链外状态，以及建立强制执行正确Oracle报告和仲裁链下Oracle争端。

白皮书中描述的更高级的链外计算使DONs可以为智能合约提供一个通用的与区块链无关的网关，不仅可以访问任何链外资源，还可以使用链外计算环境来执行无法执行的代码。

ChainLink网络中的DONs是安全、灵活的全栈解决方案，用于创建依赖现有链上代码并将其与关键链下计算相结合的混合智能合约。这些混合智能合约使去中心化应用程序能够实现可扩展性和机密性的重大升级，这对于大规模采用区块链至关重要。

扩展性：

DONs将链下计算oracle结果和部分合同执行，同时与现有的区块链网络或第二层定期同步。这使ChainLink分散式Oracle网络可以实现为区块链，第二层网络甚至传统Web 2.0系统提供服务所需的低延迟和高吞吐量性能。

机密性：

DON允许多种形式的机密性，例如链上和链下系统之间的保留机密性的连接器，以及智能合约和Oracle数据的机密计算。

通过DON带来的增强功能将使ChainLink能够支持为下一代智能合约用例提供支持的各种去中心化服务。此外，通过DON提供的优势，将进一步增强ChainLink Network今天提供的oracle服务。这些高级去中心化服务的简要清单包括：

1.可以无缝连接到所有必要的链下资源的混合智能合约，同时保留更高级别的隐私。

2.增强的ChainLink数据反馈，提供更高频率的更新，隐私保护查询和多区块链交付，这些都降低了成本，并为DeFi应用程序提供了更加安全可靠的外部数据源。通过OCR已经使ChainLink数据Feed更具可扩展性。

3.增强的ChainLink VRF，具有增强的安全性，加密经济安全性和成本效率，可支持更安全的游戏，NFT铸造以及任何其他需要安全随机源以实现端到端安全性的应用程序。

4. ChainLink Keepers可为关键智能合约功能（例如收获收益和触发清算）提供分散且高度可靠的自动化维护，目前已投入生产并由顶级项目进行了测试。

5. ChainLink公平排序服务（FSS），使用DON来排序区块链上的用户交易，以减轻前向运行，后向运行和其他相关攻击的手段，以及其他类型的交易，例如可截取价值（MEV）。

6. ChainLink去中心化身份，其中保护隐私的oracle协议以向后兼容的方式与现有系统进行互操作，可开辟新的用例，例如基于链式信用的借贷。

从ChainLink的最新白皮书上看来ChainLink在未来的大规模应用上有着不可估量的前景，而且它的机密性也得到了提升，未来在去中心化金融上也会有更大的应用价值。

1.4代币机制

在ChainLink网络中的主要代币是Link币，Link是ChainLink网络的主要资产，Link币用于支付节点运营商的服务费用。以太坊等网络中的智能合约如果要使用ChainLInk节点，就需要使用Link币付款给为他们提供服务的ChainLink节点，节点根据用户对它们服务的需求量以及其他类似数据源的供应量来定价。

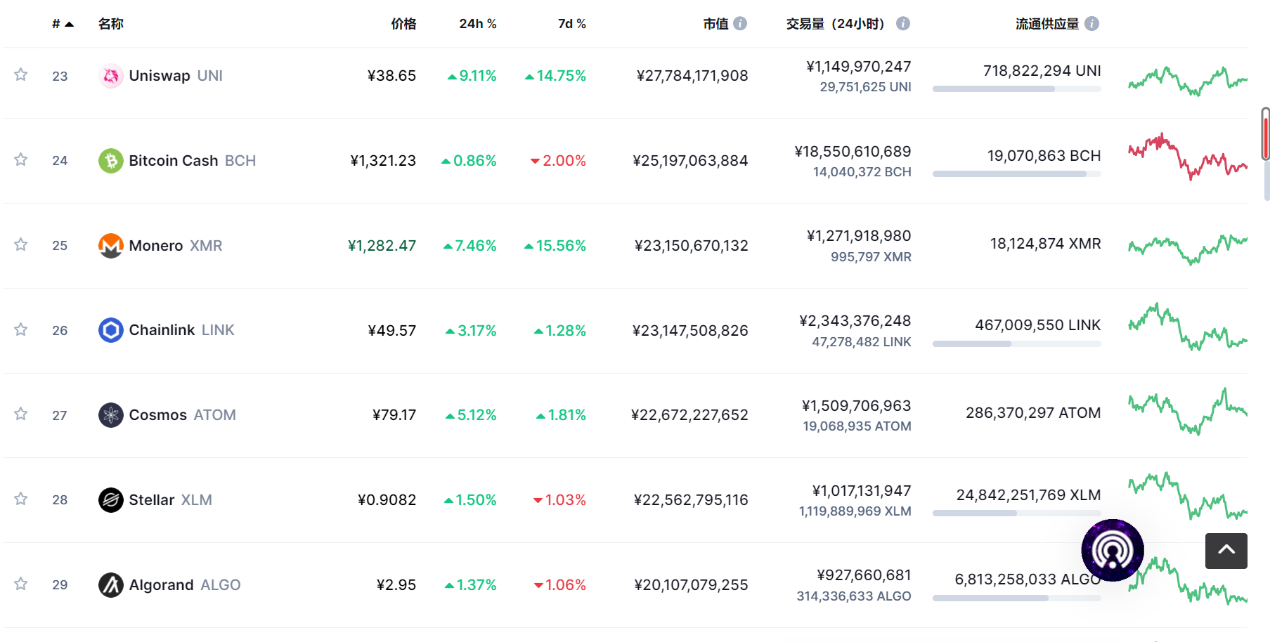


图3. 2022年5月23日Link币排名

从上图来看Link币排在第26位，曾经最受欢迎的时候也曾排进过前10名，与其他货币来讲还算稳定。不过Link币的价值也不可全部由排名来决断。通过上一部分ChainLink项目目标的阐释，未来Link币肯定会有很好的前景，尤其是DeFi未来的发展Link币的发展也不会太差。

1. 技术模型分析

2.1ChainLink的工作流程

预言机一共有三种工作模式：立即读取、发布订阅、请求响应。Chainlink采用的就是请求响应模式。

具体过程：

* USER-SC发起链上请求；
* CHAINLINK-SC为预言机记录事件；
* Chainlink核心软件收到事件记录并向适配器发送任务；
* Chainlink适配器执行任务，向外部API请求数据；
* Chainlink适配器处理返回数据并返回至核心软件；
* Chainlink核心软件将数据传回CHAINLINK-SC；
* CHAINLINK-SC将数据聚合成单一数据，并返回USER-SC

USER-SC：chainlink节点作为预言机，针对由智能合约端亲自发起的或第三方委托发起的数据请求返回结果，将这类数据请求成为“请求合约”，用USER-SC表示。

CHAINLINK-SC：chainlink与USER-SC交互的接口本身也是一个链上合约，用CHAINLINK-SC表示。

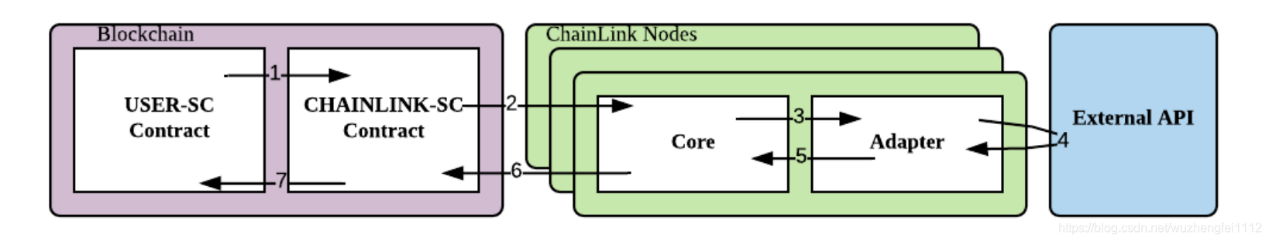


图4.ChainLink的工作流程

2.2 ChainLink的可靠性实现

提升chainlink的可靠性，开发人员采用了三种互补的方式：分散数据来源、分布式预言机、使用可信硬件。、

* **分散数据来源**

对于单数据来源的数据可能出错，那么简单的处理方式就是获取来自多个数据源的数据。

最终情景：

* 多数投票制：如果大多数返回了相同的结果a，那么最终的结果就是a
* 平均值场景：可能会剔出一个最大值和最小值，然后将剩下的数据求一个平均值作为最终结果。
* **分布式预言机**

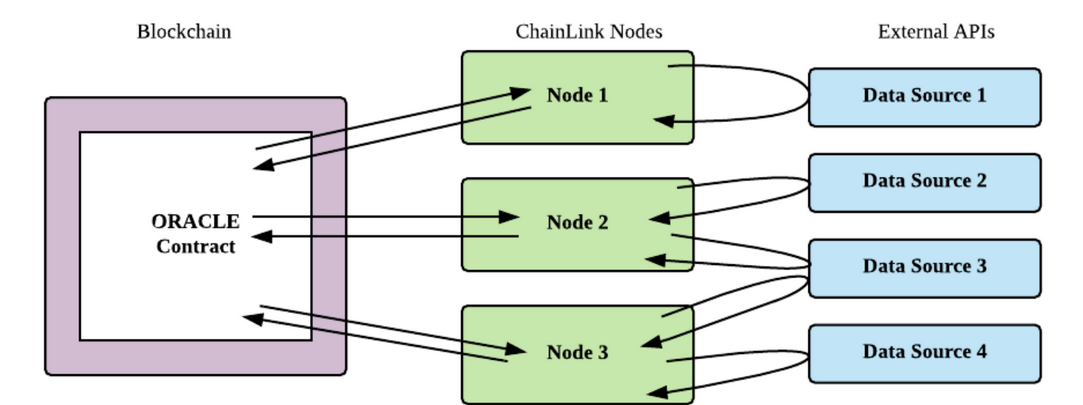
正如数据源可以分散一样，预言机也可以是一个分布式系统，也就是说我们可以用n个不同的预言机节点来代替单一的预言机节点。

图5.分布式ChainLink节点

* **可信硬件**

ChainLink正在积极研究使用可信硬件，不过可信硬件无法提供充分的可靠性。于是ChainLink还开发了四大安全服务：验证系统、声誉系统、认证服务和合约升级服务

（1）验证系统

负责监控链上预言机行为，提供客观的性能指标，为用户选择预言机提供指导意见。它会对预言机在以下两个方面进行监控：

可用性：验证系统应记录预言机失效，以及时响应数据请求。它将持续汇总运行时间内的统计数据。

准确性：验证系统应衡量预言机反馈结果与网络中其他预言机之间的偏差程度，并记录明显错误的反馈结果。

（2）声誉系统

声誉系统将记录预言机服务商以及节点的用户评分，让用户可以评估预言机的历史服务水平。验证系统的报告可能成为决定预言机声誉的主要因素，并确保声誉数据真实可信。而链上服务记录之外的其他因素则可揭示预言机节点本身的安全水平。

（3）认证服务

ChainLink的验证和声誉系统旨在解决一系列预言机违规操作的行为，在多数情况下保障系统完整性。另外，ChainLink在此基础上还添加了一层认证服务，目的是避免重大问题的发生，并在问题发生时进行补救，特别是由于女巫攻击和镜像攻击导致整个区块沦陷的情况。

（4）合约升级服务

光靠代码几乎无法让智能合约在安全性上做到滴水不漏，即使智能合约的代码完全没有问题，它所部署的环境一旦出现变化或错误，仍然会对合约安全造成严重影响。

短期内，如果发现了风险漏洞，合约升级服务将在ChainLink预言机中创建一套新的预言机合约。新的数据请求合约将迁移到新的预言机合约集合中。

1. 项目未来

近日，ChainLink与众多公司都开展了合作。世界一流的基础设施提供商持续采用Chainlink为区块链生态系统提供安全的链下数据和计算。

* stc Bahrain是一家中东地区领先的电信公司，正在主网上运行自己的官方Chainlink节点。



图6.stc与chainlink合作

* Coin98是领先的All-In-One DeFi平台，拥有包括Coin98 Super App、Coin98 Exchange、SpaceGate跨链桥在内的全套产品。随着原生Coin98 Chainlink Price Feed的推出，BNB Chain和Ethereum上的项目现在能够安全地围绕Coin98通证构建功能。



图7.Coin98与chainlink的结合

* Horizon Protocol是一个用于发行合成资产的DeFi协议。Horizon Protocol在BNB Chain上集成了Chainlink Price Feeds，以支持21种不同资产的交易。



图8. Horizon Protocol与Chainlink合作

* Themis是一个借贷协议。Themis集成了Chainlink Price Feeds，使其能够显示优质价格数据。



图9. Themis与Chainlink合作

* Tranchess是一个具有各种风险回报解决方案的资产收益追踪器。Tranchess已在BNB Chain上集成了Chainlink Keepers，以自动结算其资金并计算其定制的Chainlink预言机解决方案。



图10. Tranchess与Chainlink合作

* ……

诸如此类的合作还有很多就不一一赘述。ChainLink的技术升级也为它的应用扩宽了不少领域。ChainLink不仅是一种预言机，还是一个灵活的平台，为智能合约开发者提供安全可靠的预言机解决方案。

除了上述网络上合作，在现实生活中Chainlink也有新的开拓。由1300多家报纸和广播公司组成的美联社正在进一步向去中心化的新闻和出版业买进，近日它宣布与ChainLink实验室合作。美联社表示，它将使用ChainLink智能合约来自动化公联上发生的行动，包括通知使用美联社平台的15000多家门店的选举结果、体育比赛结果或公司季度财务报告的发布时间。所有这些现在都将被加密签名，以验证数据来自美联社。自2020年以来，美联社利用区块链发布所谓的防篡改新闻，如美联社预测乔·拜登将成为美国的下一任总统。

从这一应用来看ChainLink的去中心化技术特点为新闻的真实可靠提供了“过滤”技术，这点和新闻行业的需求很贴合。如果在未来真的可以将该项目应用到现实生活中，在某些对数据要求严格的行业领域，这将会是一个福音。但同时福祸相依，在享受该项目带来的便利时，我们也应当考虑它可能会带来的负面问题，比如说是不是任何数据都可以传递到链上，如果一些数据涉及到个人隐私或者是国家机密，然而我们还要保证这些数据的真实防篡改，届时我们应当如何处理?本人认为在该项目还未完全成熟之前，不应该将大规模的数据传到链上，一旦出了问题，损失不可估量。即便有朝一日技术成熟，可以大规模使用了，本人认为也应当制定出相应的规则，一些涉及个人隐私及国家机密的数据仍应保证隐蔽性，不可公开。

ChainLink的项目未来的前景还是很客观的，而且其背后的创始团队也具有极大的野心，尤其其在去中心化金融上具有很大的应用价值，期待其未来更好的发展。