BTGAME

火币生态链上的去中心化预言机网络

2021年5月6日（v1.0）

摘要

智能合约是现代区块链最重要的部分之一。 智能合约部署在区块链上，自动触发且部署后即使作者也无法修改。 这些特征使智能合约成为传统数字合约的最佳去中心化方案。 但是，智能合约无法与区块链外部的数据进行通信。 基于这个问题，我们提出了一个解决方案。

这个方案被称为预言机。预言机将智能合约与链下的世界连接在了一起。现存的多数预言机网络都采用了中心化的服务模式，与这些相比，去中心化的BTGAME 将在安全性方面更具优势。

白皮书描述了BTGAME为智能合约链接线下数据的线上模块，以及其节点网络的底层部件。除此之外，白皮书还指出了可能的优化方案，为BTGAME未来的发展 提供了方向。

目录

介绍 3

一、BTGAME系统总览 3

1、链上系统 4

预言机选择 4

数据聚合 4

2、链下系统 4

BTGAME核心软件 4

外部适配器 5

子任务模式 5

3、BTGAME的工作流程 6

二、理想型预言机 7

三、BTGAME的数据获取以及安全方案 8

1、数据源 8

2、预言机节点 8

3、合约升级 9

四、BTG通证使用 10

五、未来计划 10

六、验证系统 10

七、声誉系统 10

八、认证系统 11

总结 12

介绍

智能合约是在去中心化的系统上部署并执行的应用，其具有防篡改性。一经部署完成，包括合约创建者的任何人都无法篡改代码或干预其执行。与传统的数字合约相比，参与智能合约的各方的权限都是相同的，无须依赖合约各方之间的信任关系。智能合约是自动验证并执行的，因此，它能够很好的执行并管理数字合约。

智能合约的产生提出了新的挑战，这就是区块链与链下世界的连接性。智能合约无法自己获取到链下的数据，这是由区块链的共识机制造成的。因此，我们提出了BTGAME，并希望用这个预言机网络来解决这一问题。

与多数现存的预言机网络不同，BTGAME是去中心化的。这种去中心化的模式极大降低了合约各方彼此之间的信任需求。BTGAME保证了智能合约与链下数据交 互的安全性，使得智能合约执行的整个过程的安全性得到了保障。让智能合约具有外部连接性，这是智能合约替代传统数字合约的先决条件。

如果要用智能合约替代传统的数字合约，则需要保证它的输入和输出的数据的准确性。以下是一些智能合约需求的数据的示例：

- 证券智能合约（例如债券，利率衍生品等）将需要从报告市场价格和市场参考数据的API获取数据，例如：利率。

- 保险类智能合约需要与事件相关的IoT数据来进行取证，例如：违规时仓库的电磁门是否已锁定，公司的防火墙是否正常运行，航班是否按时到达等。

- 贸易金融智能合约将需要有关装运的GPS数据，来自供应链ERP系统的数据以及有关所装运货物的海关数据，来确保合约的正确执行。

通常，支付消息需要输出到链下的中心化机构，如银行。BTGAME能够将智能合约的数据安全传递给链下系统，既能保障合约的防篡改性，也实现了与外部的连接。

一、BTGAME系统总览

BTGAME的目标是连接链上和链下的世界，最初的开发和部署将在火币生态链上进行。BTGAME采用了模块化的设计理念，这将大大简化我们未来对它的升级 和优化工作。

链上系统

我们将由智能合约发起的数据请求称为**请求合约，并**用USER-SC表示。BTGAME与请求合约交互的接口是一个链上合约，用BTGAME-SC表示。

BTGAME有一个线上模块，即**聚合合约**。用户可以自行选择节点和服务，聚合合约将收集预言机返回的数据，聚合数据，**并**计算出最终所需的结果。

1.预言机选择

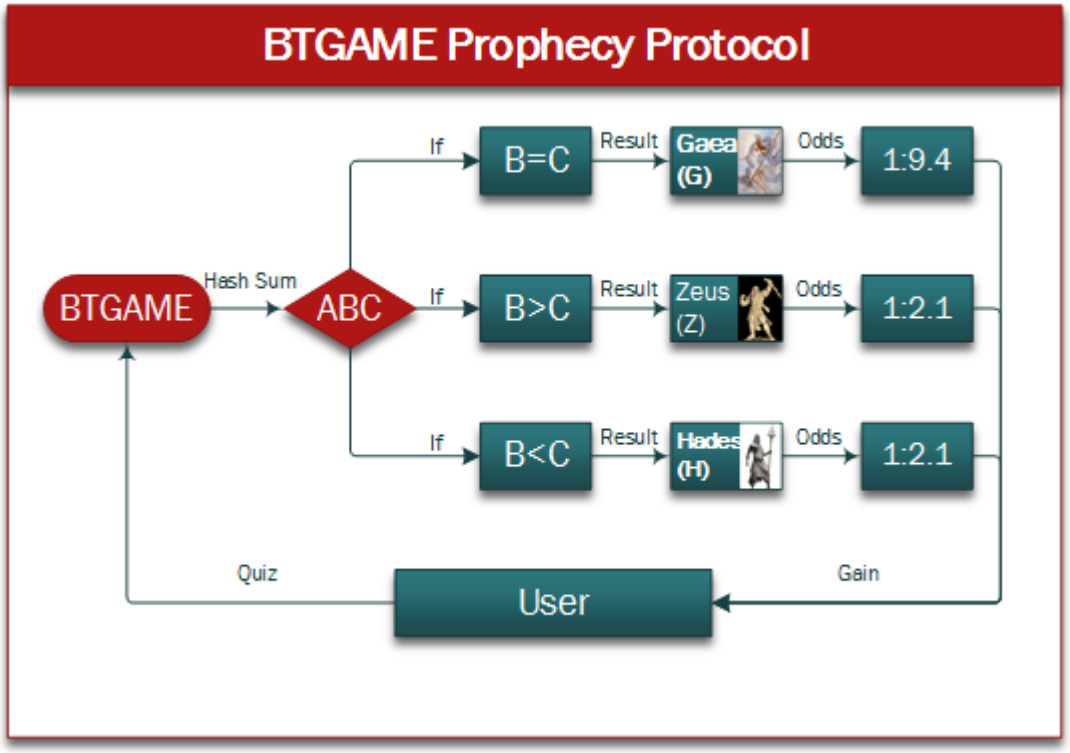
用户可以根据自身的需求来选择预言机服务和节点。用户能查询到与节点相关的各种数据，以帮助他们更好的选择服务。考虑到手动选择预言机**并**不适用于所有场景，未来我们会推出自动化的匹配机制来满足更多的需求。

2.数据聚合

聚合合约收集所有预言机返回的数据，将其计算出一个加权数值，**并将**这个结果发送到USER-SC。由于不存在一个万能的聚合合约，BTGAME会推出一套标准，让用户可以根据需求定制自己的合约。

链下系统

BTGAME的链下架构是火币生态链上的预言机节点网络。这些节点分别获取链下数据**并**发送到聚合合约，得到最终的结果。下文中详细描述了如何将多个返回结果聚合为单一数据的方案。BTGAME的节点软件是开源的，**它**包含了标准的区块链的交互、调度以及连接共同的链下资源。



1.BTGAME核心软件

节点的核心软件负责与区块链交互、调度任务以及工作量平衡。BTGAME节点完成的工作被**称**为**任务**。每**个**任务能够被拆分成若干**个**子任务，子任务拥有更细小

而具体的职责，前一个子任务完成工作后会将结果传递给下一个子任务，最终得到结果。BTGAME节点有几个内置的子任务，包括HTTP请求，JSON解析以及转换成不同的区块链格式。

2.外部适配器

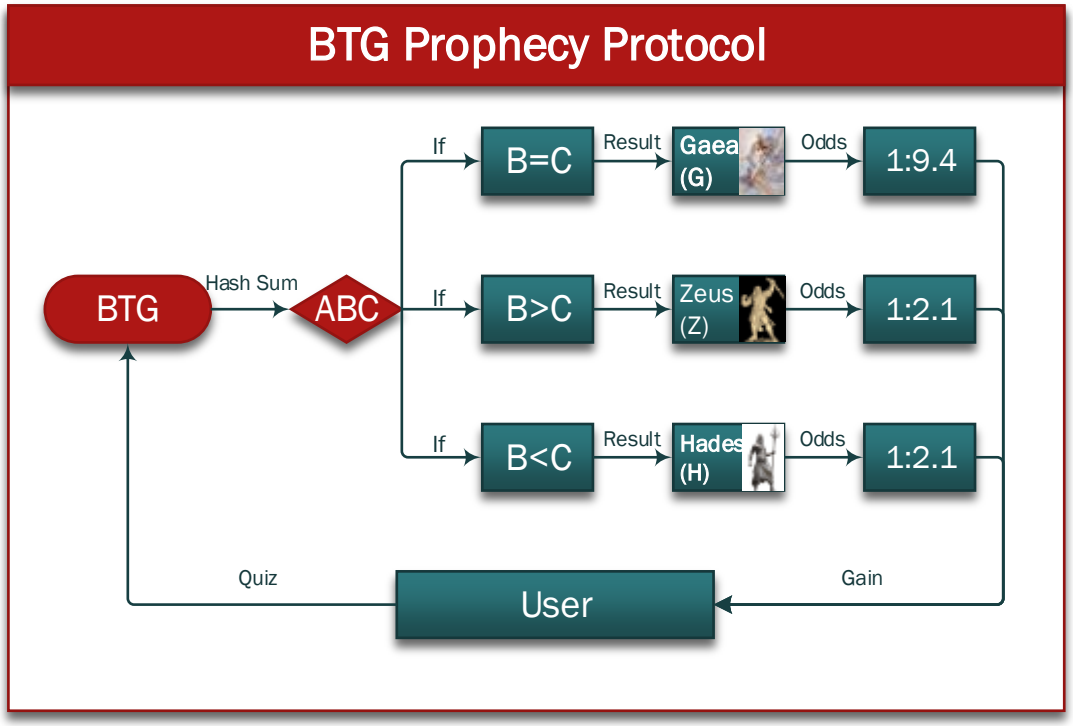
用户可以通过创建适配器来定制子任务。配置器是配置了最小化REST API的外部服务。配置了适配器之后，任何语言开发的程序都可以通过添加中间API来轻松实现。

3.子任务模式

随着BTGAME的应用逐渐广泛，我们预计会出现很多开源的外部适配器。这些服务可以由所有的社区成员进行审计。由于很多不同适配器的出现，确保适配器之间的互相兼容也非常重要。BTGAME目前运行的是基于JSON的模式系统。

BTGAME的工作流程

- USER-SC发起一个链上请求
- BTGAME-SC为预言机记录事件
- BTGAME核心软件收到事件记录，并向适配器发送任务
- BTGAME适配器执行任务，向外部API请求数据
- BTGAME适配器处理并返回数据至核心软件
- BTGAME核心软件将数据返回BTGAME-SC
- BTGAME-SC将返回结果聚合成单一的数据，并返回给USER-SC



二、理想型预言机

一种关于预言机安全性推理源于以下思想实验。假如现在有一个可信的第三方，总是能够诚实的执行指令，那么由这个第三方运行的预言机被称为理想预言机。假设理想预言机从一个完全可信的数据源获取数据，我们指定这台预言机提供服务，那么我们需要它进行如下的任务：

- 接受请求：从USER-SC获得数据请求Req = (Src, τ, q)。Src是数据源，τ是时间或时间范围，q是请求；

- 获取数据：将请求q在时间τ发送给Src；

- 返回数据：收到返回的数据，将数据返回到智能合约。

理想预言机在数据源和UER-SC之间建立起了可靠的桥梁，预言机会准时并且准确的给USER-SC需要的数据。

保密性也是预言机的一个重要属性。很多情况下数据请求的内容比较敏感，不宜公开。一个理想型的预言机始终会将请求内容加密，并保存公钥。除此之外，理想型的预言机永远不会宕机，也不会拒绝为任何的智能合约服务。

然而世界上并不存在百分之百可信的数据源。数据可能会因为各种原因被善意或者恶意的篡改，这其中包括网站的漏洞以及服务提供商的失误。同样的，也不存在完全可靠的理想预言机。

三、BTGAME的数据获取以及安全方案

BTGAME提出了两种方案来尽量避免问题节点的出现，即分布式的数据源以及预言机。

数据源

我们可以从多个不同的数据源来获得数据，以减轻异常数据源对于结果的影响。聚合函数可以将多个返回结果聚合成单一的答案。有很多方案可以完成数据聚合，比如去掉异常数据后的加权平均。

数据源之间可能会存在互相获取数据的情况，这也可能导致聚合结果的错误。我们会持续关注这类问题，并对数据源的独立性进行报告。

预言机节点

和区块链网络一样，预言机网络也是由众多的节点构成。每个预言机节点由自己的数据源集合，但不同节点的数据源集合可能存在交集。预言机节点从多个数据源获取数据，多个节点的数据聚合成了最终的结果。

预言机网络中的节点可能会出现问题，所以需要一个方案来减轻问题节点造成的影响。最简单的方法是链上聚合，即由BTGAME-SC聚合预言机返回的数据（WI

NKLINK-SC调用聚合合约）。这种方法有很多优势，由于BTGAME-SC的代码是开源的，并且它的任何行为都在链上可见，所以它对于用户来说是高度可信的。

由这个方案引出了一个问题，即**吃空饷（freeloading）**。对数据源的请求是按照次数收费的，作弊的预言机可以抄袭其他预言机的结果，这样一来，作弊者没有花费成本却能得到预言机奖励，这会打击诚实的预言机运行者的积极性，并且降低了每个预言机结果的独立性，导致最终聚合结果的准确度降低。

因此，针对这个问题，我们提出了先提交后解密的机制。简单来说，每个预言机都向BTGAME-SC返回加密的结果，当BTGAME-SC收到合法数量的结果后， 才会对数据进行解密。

由于火币生态链的高吞吐量以及极低的交易费用，目前我们并不需要以链下聚合的方式来降低成本。

合约升级

智能合约一旦部署成功，就再也无人能够干预它的行为，如果预言机发送了错误的数据，使用该预言机的一方，比如去中心化的交易所，可能会遭受到严重的损失。因此作为链上与链下桥梁的预言机的安全性至关重要。

BTGAME提出了合约升级服务来提升预言机的安全性。这项服务将由运行BTGkLink节点的组织或个人提供，并且遵循BTGAME去中心化的设计理念。

许多智能合约被攻击的事件表明，即使智能合约的代码编写完全没有问题，也不能保证它的绝对安全。 这正是我们提出合同升级服务的原因。这项服务是非强制的，用户可根据需求自行决定是否开启。

如果发现了漏洞，合约升级服务将在BTGAME预言机中创建一套新的预言机合约。这样一来，新旧版本的两套合约会同时存在于预言机内，基于去中心化的思想， 用户可以自行选择使用哪一套合约，通过一个flag来控制。同时，我们也希望服务商能够支持社区开发的多个版本的BTGAME-SC。

四、BTG通证使用

BTGAME网络使用BTG通证来向节点运营商支付数据获取、格式化、链下计算以及服务质量保证的费用。BTG是一种HECO通证，BTG是BTGAME协议中的治理代币，一部分用于拍卖，另外一部分用于赠送对BTG预言机有贡献的参与者，包括（不限于）通过游戏竞猜挖矿、参与做市商或保护协议正常运行。持有BTG可以享受社区的治理权，此外，BTG协议每天产生的摩擦收入USDT将按照BTG的持有比例进行分配，换而言之，持有BTG将会有源源不断的产生收入来源。

五、未来计划

BTGAME未来将重点关注提升预言机的安全性以及可靠性。

六、验证系统

验证系统负责监控链上预言机的行为，并且为用户提供客观的性能指标。它主要会在两个方面进行监控：

- 可用性：记录预言机响应失败的情况。
- 准确性：记录预言机与网络中其他预言机结果的偏差程度。

BTGAME-SC能看到所有预言机的活动。这些可用性和准确度相关的数据会在区块链上公开。

七、声誉系统

声誉系统记录预言机节点及服务商的用户评分。在评价声誉时，验证系统的报告会起到主要的作用。除此之外，用户对预言机品牌的熟悉程度、节点运营团队以及基础架构都会影响节点的声誉。声誉可以供其他智能合约参考。我们也考虑在链下对声誉进行计算，因为在链下可以处理更复杂的计算，使得声誉计算更加精确。

对节点运营商来说，声誉系统既包括按不同任务类型划分的指标，也包括综合所有任务类型的指标：

- 分配的请求：过去被分配的（已完成和未完成）请求总数
- 完成的请求：完成的请求总数
- 被接受的反馈：完成请求并且其结果被采纳的总数
- 平均响应时间：响应时间的平均值
- 罚款金额：预言机需要支付保证金来保障服务质量。这里记录的是预言机受到的处罚总额，处罚情况包括相应超时和错误的结果

声誉系统可以激励预言机服务商保持高品质的服务。我们希望声誉系统可以成为用户选择节点和服务的风向标。

八、认证系统

预言机的节点有受到女巫攻击的风险。在这种攻击中，攻击者通过试图操控多个表面上看起来独立的节点来占据预言机池中的主导地位。这些预言机可能会被操控在特定的时间提供错误数据，来操纵高价值合约中的大额交易。另外，女巫攻击者可以通过镜像法来降低攻击成本，即从同一个数据源多次获取数据，并伪装成是从多个来源获取的。无论攻击者是否发送错误数据，他们都会从攻击中受益。

认证服务基于预言机节点部署和操作行为。它将监控验证系统的统计数据，并对其提交到链上的结果进行抽查，抽查方式是将这些结果与高声誉的节点提供的结果进行比较。

除了衡量声誉以及链上和链下的自动化反欺诈系统外，认证系统还应该能识别女巫攻击以及其他链上系统无法识别的错误行为。

总结

白皮书中介绍了去中心化的预言机网络BTGAME，包括其链上和链下的一系 列组件。我们介绍了关于BTGAME的去中心化以及安全方案。同时，我们试图总结现有的设计缺陷，并提出了未来的改进方案。

去中心化是区块链的基本，这句话同样适用于BTGAME。在现在和未来的开发工作中，我们将始终遵循去中心化的思想，提升预言机网络的性能以及安全性。

BTGAME是一个站在巨人肩膀上的项目。作为一个开源项目，我们会重视来自社区的意见，并继续以开源的方式进行开发。我们希望BTGAME能够推动区块链和智能合约未来的发展。