Bridge Protocol：更灵敏的去中心化价格预言机

目录

1、 Bridge Protocol 概述 2
2、 由现有解决方案带来的价格预言机思考 3
3、 Bridge Protocol 解决方案 4
3.1、Bridge Protocol 架构 4
3.2、Quotation system 5
3.3、Verification system 6
3.4、Block price 8
3.5、价格序列与波动率 9
3.6、安全价格网络 9
3.7、聚合价格预言机 10
3.8、Bridge Token＆节点权益 Token 11
3.8、Incentive funds＆Bonus 12
4、 Bridge Protocol 可能的应用场景 14
5、 Roadmap 15
6、 生态激励 15
7、 风险提示 15

1、Bridge Protocol 概述

区块链上的智能合约和去中心化应用（Dapp）对外界数据拥有交互需求。区块链是一个封闭的环境，链上是无法主动获取链外真实世界的数据。主要是因为区块链无法主动发起 Network call（网络调用）而链上智能合约是被动接收数据的。其次，智能合约其实并不“智能”，它只是在满足相应条件下，才达到触发状态的程序。同时，智能合约最终的执行需要合约参与方的私钥签署，智能合约本身没有办法自动执行。当智能合约的触发条件取决于区块链外信息时，这些信息需先写入区块链内记录。此时就必须要通过预言机来提供这些区块链外的信息。

预言机的功能就是将外界信息写入到区块链内，完成区块链与现实世界的数据互通。它允许确定的智能合约对不确定的外部世界作出反应，是智能合约与外部进行数据交互的唯一途径，也是区块链与现实世界进行数据交互的接口。

现阶段区块链网络对于价格预言机的需求激增，例如博彩、稳定币、借贷、金融衍生品、期货、保险以及预测市场等等。Uniswap、compound 等项目的火爆也让对预言机的重要性越发明显，同时对预言机的安全、高效等方面提出了新的要求。

Bridge 旨在提出一种更安全、对价格更灵敏、更符合市场要求人人可参与的可扩展预言机网络，用以满足现有及未来可能的市场需求。

2、由现有解决方案带来的价格预言机思考

Bridge Protocol 团队对于现阶段已有的价格预言机，比如 NEST、Link 等做了大量的分析及实际调用实验，并进行了长时间的研究和思考。

例如 Chainlink 是一个去中心化的预言机网络，为区块链智能合约

解决互操性问题，并将其安全连接至链下数据源、Web API 和传统银行支付系统。它由两个独立的部分组成，链上链和外链，它们必须交互以提供服务，涉及多轮消息交流，在最糟糕的情况下，它需要大多数链下客户端的参与，因此 Chainlink 的性能和可扩展性一般。此外，基于信誉来选择预言机节点容易导致马太效应，并且容易导致串通作恶和有针对性的攻击。这也是被许多人诟病的“半去中心化”的来源。

而 NEST 的出现 ,在价格预言机上有了相较于其他项目长足的进步，NEST 等新型报价预言机解决了一部分问题，例如去中心化，真实可验证等，但在可拓展性、灵敏性和等方面却依然有着不小的欠缺，而这将会带来诸多问题。比如去中心化衍生品产品是对于价格极其敏感的 Defi 产品，即便是 1 分钟的价格差，也会造成上千万的损失，这对所有使用此类预言机的去中心化衍生品项目方都是不小的考验，而预言机却又是他们必须的选择。

Defi 现有的产品的主要赛道为去中心化的稳定币、借贷、交易所、金融衍生品、资金管理、支付以及保险等，这些 Defi 产品有着非常明确且急需的价格预言机的方案，安全、真实、精准、灵敏。

基于以上的研究，我们对 Defi 可用的价格预言机做出了以下判断:

1、预言机具有可拓展性

2、价格具有真实性

3、价格具有灵敏性

4、价格是安全的，具有抗攻击性

5、价格是可被验证的

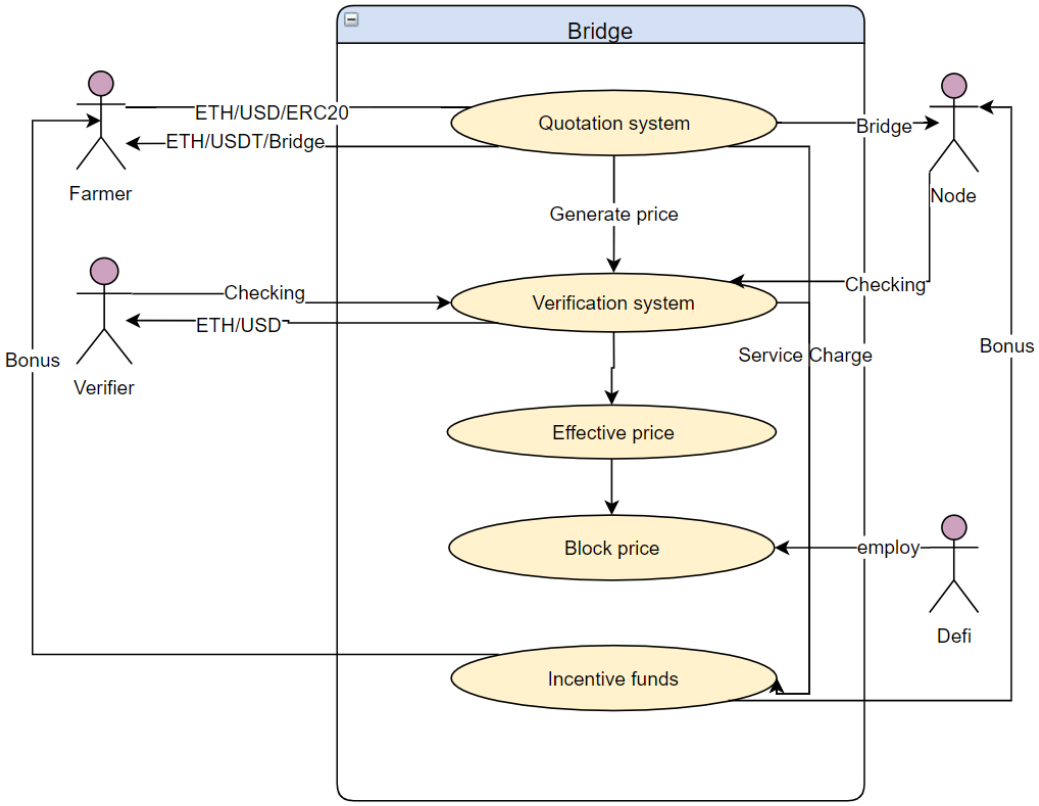
6、网络是分布式的

7、长期运行

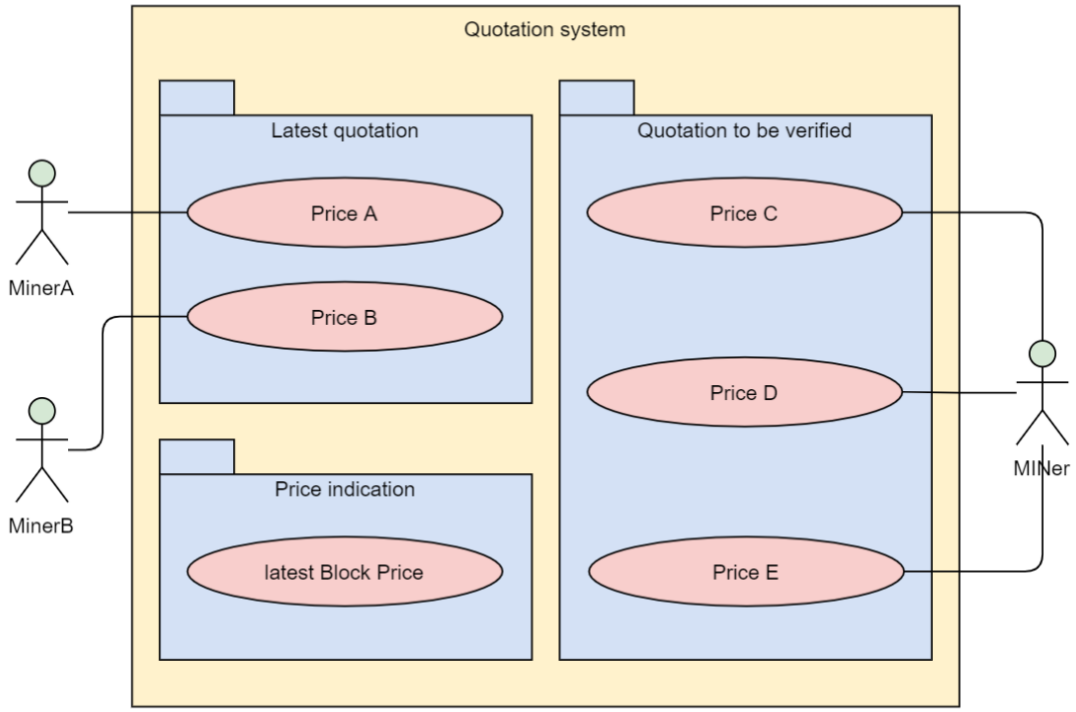
对此，Bridge 提出了一种兼容以上 7 点的价格预言机解决方案。

3、Bridge Protocol 解决方案

3.1、Bridge Protocol 架构



3.2、Quotation system



报价系统是 Bridge 非常重要的模块之一。它是链外信息进入链内的第一步。

一般情况下，链外信息进入链内的过程，有着非常高的门槛，例如技术开发、产品设计、数据维护、API 介入等等。

无论是 DOS 还是 LINK，他们都设计了链上和链下部分，链上部分是由系统合约和管理合约等组成。链下部分则是有准入机制的节点。这更加提高了参与的门槛。

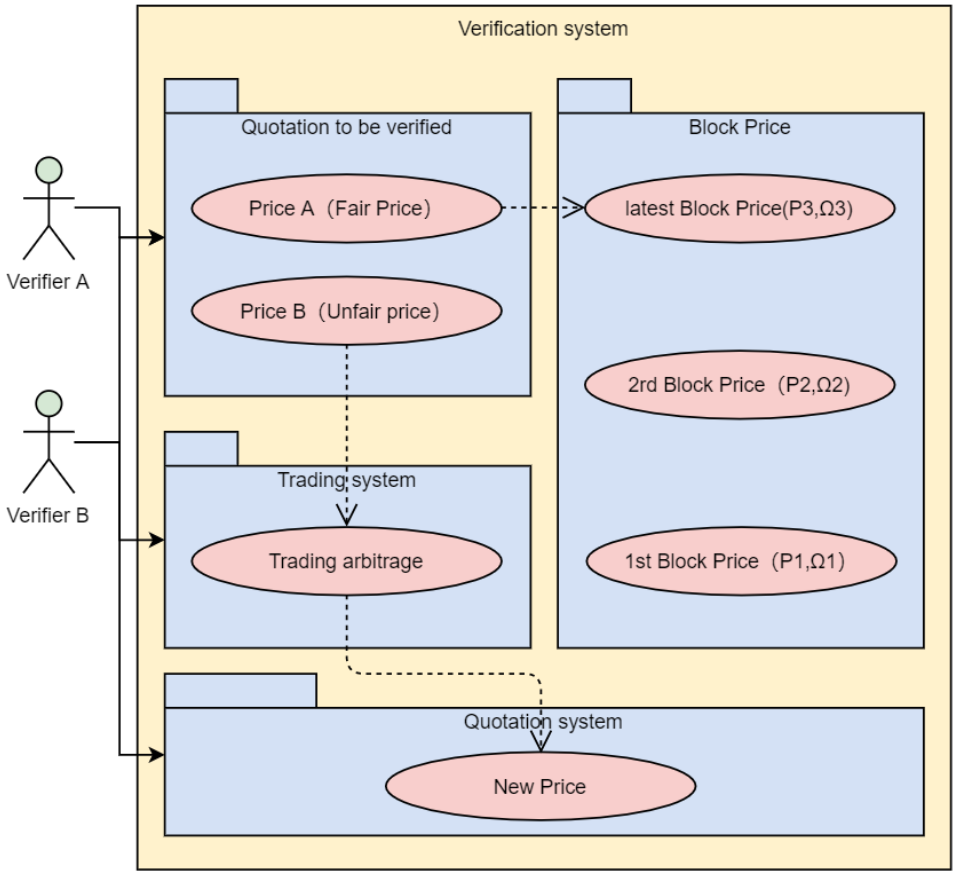
我们认为区块链应该是开放的、人人可参与的，所以在做了非常多的调查后，并充分考虑到区块链参与者的产品体验，为了降低报价参与者的门槛，我们对报价系统进行了简洁却不简单的设计。

在用户端，进行了本地钱包的优化，和报价合约的优化。用户只需要将代币的价格以资产对的形式转入报价合约。以 ETH 为例，用户将它认为合适的价格，比如 1ETH=400USDT，将用于报价的资产转入报

价合约，资产为规模为αETH 和 400αUSDT 即可完成报价行为，整个过程完全开放，没有任何的门槛，每一个区块链参与者都可以进行报价，保证了整个网络是分布式的。α为合约规定的规模常数，规模常数与报价的最低资产有关。

在合约端，团队在测试网进行了大量的测试，并且由专业的安全团队进行了安全审计，为所有进行报价的参与者做了充分的安全保证。

3.3、Verification system



验证系统是保证价格真实、准确，并承担一部分价格灵敏度的重要模块。

用户将资产和价格提交到报价合约后，验证系统便会起作用。任意的验证者或者验证节点认为该价格是不准确的，是有套利空间的，便可

以按照用户的报价，购买 ETH 或购买 USDT，而仅仅只需要支付很少的交易手续费，节点验证者则无需支付交易手续费。

这一机制，保证了报价是市场上的公允价格。原因在于，一旦价格偏离过多，则有大量的验证者会进行套利，即便是价格偏离较低，节点验证者在套利空间可以覆盖 GAS 费用时也依然会进行交易以获得利润。

如果在一段时间内，该报价未被交易，或者未被完全交易，则会生成有效价格，若被完全交易，则交易者需要重新对其报价，该过程是验证系统内的报价验证期。

我们考虑到 Defi 中会有对交易价格敏感的产品，例如金融衍生品等，同时，在快速波动的市场中，为报价者尽可能的降低波动的放心，验证系统设定，从报价区块开始，12 个区块后，若价格没有被交易，则视为有效价格，有效的提高了价格预言机的灵敏度，同时降低了参与者的风险。

价格验证期过后，报价者的剩余资产以及被成交的资产可以随时取回。

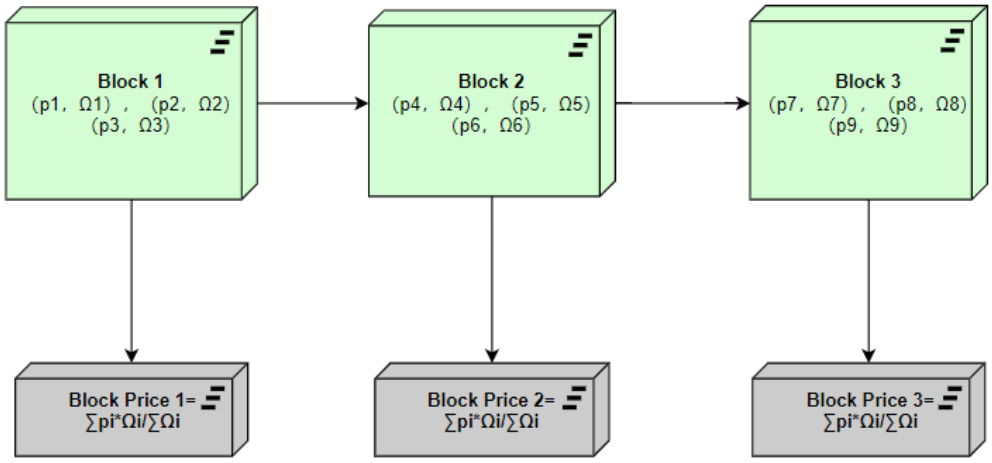
根据合约的规则，验证者在对某个报价者价格成交后，需要强制报一个新的价格。如报价者以 p 的价格进行报价，资金规模为Ω，验证者 A 与报价者 B 的以价格 p 成交，他需要同时报一个价格 p1 到合约内，其规模为Ω1，但此时不必再支付佣金，也不参与挖矿。如果有套利者 A1，与 A 的报价成交，他就需要报价 p2，其规模为Ω2，如果类推，就形成了一个以 12 个区块为最大报价时间间隔的连续价格链：p—p1—p2...，报价资产链为Ω—Ω1—Ω2...

3.4、Block price

Bridge 的价格是按照区块记录的，每个区块形成一个价格，每个区块有可能有多个报价，则该区块的区块价格由区块内生效的报价按照

一定的算法生成，该价格称之为区块价格或者 Block-Price，区块价格包含报价者提供的报价 p 及提供的资产规模Ω。

假设某一区块的生效报价为（p1，Ω1），(p2，Ω2)（p3，Ω3）…则该区块价格 P=∑pi*Ωi/∑Ωi，如果该区块没有生效报价，则沿用上一个区块价格。



3.5、价格序列与波动率

当 Bridge 第一个报价区块诞生后，以太坊网络的每个区块都会对应一个 Bridge 的区块价格，从而形成价格序列。

价格序列拥有重要意义，例如提供均价供 DeFi 调用，包括连续 N 个区块的算术平均价格，Ps=∑P/N；或者连续 N 个区块加权平均价格 Pm=∑P*Y/∑Ω，其中Ω=∑Ωi，为上述生效报价。

提供波动率指标供大部分衍生品 DeFi 调用 ,如连续 50 笔报价的滚动波动率，或者 DeFi 自定义的各种波动率。

3.6、安全价格网络

无论是互联网还是区块链网络，遭受攻击是很常见的。尤其是在分布式的区块链网络，成功攻击的收益巨大且风险较小，使得网络抗攻击能力是判别项目是否能够长期运行的重要因素之一。

在价格网络中，可能的攻击因素很多，例如调用 Bridge 的 Defi 资产规模巨大，一旦价格失效，可能会产生难以挽回的资产损失等。Bridge 的安全价格网络对此有着充分的准备。

当攻击者以期望价格失准，或者一段时间保持某个失准的价格，即便牺牲失准价格与市场价格的价差，那么价格机制就可能失效。

Bridge 通过多个手段来防范攻击。

首先，价格链本身就是一种抗攻击机制，即攻击者攻击完价格后必须留下一个价格以及该价格对应的资产。这意味着攻击者攻击后，要么留下正确的价格，要么留下一个套利空间，市场上必然会有验证者来套利并修正报价。

其次，为了放大攻击者的成本，对所有验证者的报价规模进行如下安排：验证者成交的规模为Ω1，则其同时报价的规模Ω2=βx1，其中β>1，即验证者必须以一倍以上的规模来报价。我们以β=2 为例，初始报价为Ω=10 个 ETH，则全部成交的情况下，Ω1=20，Ω2=40，Ω3=80...以此类推。攻击者要么暴露给市场极大的套利机会（规模以级数上升，这种攻击几乎是无效的），要么依据市场价格不断动用极高规模的资产进行自成交，以延缓价格被采纳的机会。

目前在 ETH 上每个区块最多可以报价 20 笔，报价也是分布式随机进入，如果假设每个区块有 1 笔报价，报价规模为 10 个 ETH，最大报价时间间隔为 12 个区块，那么通过攻击，使得 Bridge 在 12 分钟内无价格更新，需要动用的资产规模将接近 2^12*25*10=100 万个 ETH。

如果β=3，则该数据趋近于 ETH 的数量极限，这种抗攻击性是任何中心化交易所都做不到的。

3.7、聚合价格预言机

对于以太坊网络而言，大量的资产沉淀在网络上，除了以太坊本身对价格预言机有着较为强烈的需求，沉淀的资产也依然需要价格预言机来让其在以太坊网络上可以更好的发挥作用和流通。

对此，Bridge 提供了聚合价格预言机用来生成任何一种区块链资产的链上价格，同时也依然保持价格的安全、真实、精准、灵敏。

任何区块链参与者都可以使用聚合价格预言机来生成任意一种资产的报价模块，每一种资产的报价模块都只可被创建一次。

报价模块的生成由链上竞拍确定，所有用于竞拍的 Bridge Token 都将被销毁。

3.8、Bridge Token＆节点权益 Token

主代币名称：Bridge TOKEN
简称：BGPT
总量：100 亿
释放方式：挖矿（无预挖、无私募）
比例：挖矿 80%/节点 18%/基金会 2%
销毁方式：聚合价格预言机竞拍等
合约地址：
创始区块数值：

节点权益代币名称：Bridge Node Token
简称：BGN
总量：18000
释放方式：认筹及生态激励
合约地址：
权益：总计分配主代币的 18%，每个 BGN 享有 0.001%的 BGPT 区块产出收益。
享有 Bridge 社区治理投票权益。

所有数据链上可证，Bridge 系统的所有 Bridge Token 全部由挖矿产生，无私募、无预留、无预挖，产生 Bridge 的所有成本全部返回给 Bridge 持有人，Bridge 只是用于激励。

同时，在聚合价格预言机系统中 Bridge Token 会进行销毁，当项目发展，大量的资产进行部署时，Bridge 销毁的数量只会成上升趋势，Bridge 的财务价值便在于此。

Bridge 模型实现了完全的去中心化，不对任何人设置门槛，其特点与比特币类似。Bridge 协议升级采用 DAO 的方式，即提案者发起，社区投票，按照一定比例通过并运行。

社区投票共两个方面，一为 Bridge Token 投票，二为节点权益投票，这是 Bridge Token 和节点 Token 的权益价值，投票规则则会在项目进入 Cross Sea 阶段时公布。

3.8、Incentive funds＆Bonus

Incentive funds 来源有以下几点

1、报价矿工每次向系统支付的报价手续费

2、验证者吃单的交易手续费

3、预言机被调用费用的 80%

4、聚合价格预言机系统会向 Bridge Token 系统收益池贡献一定比例的报价手续费（初始为 30%）

总的来说，在 Bridge 报价网络和聚合价格预言机网络中，矿工通过支付 ETH 佣金，以及承担一定的价格波动风险来获得 Bridge；而验证者则基于价格的偏差计算直接的获利，并承担成交报价的风险。因此对验证者而言，其成本收益相对较为清晰。对矿工而言，其报价挖矿的模型需要相应的经济学基础。

我们将矿工贡献的所有 ETH 定期全部返还给 Bridge 持有人。该过程构建了一个自动分配的模型，从而使得每个 Bridge 具备了内在价值，该价值在链上可证。但仅仅依靠报价挖矿者的 ETH 是不足以完成逻辑的闭环的，这就回到我们构建价格预言机的初衷：链上的价格事实对所有的 DeFi 产品都是根本需求，是 DeFi 最重要的基础设施。因此任何 DeFi 开发者或用户在调用 Bridge-Price 的时候，都应该支付相应的费用。Incentive funds 是大于矿工贡献的总成本，同时增加了 ETH 网络 GAS 的使用，因此 Bridge 本身是创造了价值，同时也为 ETH 创造了价值。

可以理解成 Bridge 的整体价值大于整体成本，但对于每个矿工而言，它的成本是不确定的，这里就存在交易的可能，不同成本的 Bridge 所有者在整体价值大于整体成本的背景下，进行买卖交易，从而达到均衡，这种均衡类似于股票市场的均衡。

4、Bridge Protocol 可能的应用场景

Bridge 作为价格预言机，可用的范围非常广泛，大多数的 Defi 都需要价格预言机。

在以下几方面，Bridge Protocol 的出现将会对产品设计有着非常重大的意义

1、现在 ETH 上 GAS 使用最多的流动性挖矿的 Defi 产品，它通过为以太坊上 DeFi 产品提供流动性获得收益，同时，聚合收益器的产品也应运而生。

聚合收益器的本质和 POW 挖矿的机枪池相当，在产品设计上，需要引用更真实、灵敏的价格用于计算收益。

2、分布式期货的模型，引入任意第三方的清算，能够放大对远期交易的交易规模，或者直接捕捉交易价格波动的收益。这在之前是不可能被设计出来的，一般意义的期货都需要中心化机构进行强制平仓等，但分布式期货不承担中心化风险。

3、基于对均衡价格的波动率设计的衍生品，用来对冲或者平滑衍生品风险，由于有链上均衡价格序列，这一产品也成为可能。

以上仅以金融领域最基础的产品或现阶段 Defi 热门产品为例，通过 Bridge-Price 的导入，实现了完全去中心化的金融产品设计，且不同于最简单的点对点的交易。由于有全局变量的引入，整个 DeFi 便进入快车道。至于为何 DeFi 需要全局变量，这是因为金融本质是一般均衡的，而非局部均衡，不是简单的局部供给需求关系决定，需要基于全市场的套利机制完成有效定价，不是商品经济的规律。因此简单的点对点交易并不能解决根本的金融问题，而既不承担中心化风险，又具备一般均衡特征，就需要类似价格序列等全局变量了，这一变量不能中心化的引入，因此 Bridge Protocol 方案将会成为整个去中心化金融领域的

根本性基础设施。

5、Roadmap

Subgrade

该阶段为 Bridge Protocol 的发展打下坚实的基础，合约部署，Bridge Dapp 上线。

Pontoon

该阶段 Bridge Protocol 平稳运行同时寻求高速增长，基于 Bridge Dapp 提供更多的自研或合作 Defi 产品及服务。

Cross Sea

该阶段成为 Cross Sea 长久的运行阶段，项目全权交由社区治理，Bridge 团队基于社区规则融入社区治理。

6、生态激励

为了推动项目生态的长期良好发展，同时吸引更多的生态合作伙伴，基金会首先将以1000枚节点权益代币作为生态激励，授予为Bridge项目生态做出贡献的建设者。

其中包括生态建设激励中的交易所上线激励、钱包上线项目去中心化 Dapp 激励、优质媒体稿件宣传激励、社区推广激励和项目发展中的聚合预言机竞价激励、优质报价矿工激励、预言机调用激励。

7、风险提示

和一切金融产品或者金融服务一样，Bridge-Price 不可能没有风

险，这里对 Bridge-Price 的引用风险做出简单的描述，当然可能存在其它未被描述到或者认知到的风险：

由于最小套利空间的存在，对于价差精度要求极高的金融服务，在使用 Bridge-Price 时，可能会出现一些风险，在设计上需要做出一定的补偿。

市场套利机制的深度不够，即套利者不充分，明明存在巨大的机会，却没有人理会。这是需要市场接受度和认知度的，是行业发展深化的问题。

虽然无法攻击价格，但可以通过攻击 Bridge 来间接攻击价格机制，比如 Cross Sea 阶段后占有 51% 以上的 Bridge，然后对重要参数进行修改，使得报价机制失效。这一问题可以通过对关键参数限定来防范，同时提升 Bridge 市场规模，使得 51% 攻击难以实现。

代码漏洞或外部重大变化的风险，如果以太坊底层代码、Bridge 系统代码出现漏洞，或者外部环境发生较大变化，会对价格调用者造成影响，这可以通过链上治理及合约分叉来修正。