1 摘要

在这篇论文中，我们考虑了一种新的概念，叫做乐观响应，它允许我们绕过这个较低的界限，这样我们就可以在实践中大部分时间达到响应性，并且能够容忍在最坏情况下的少数人的腐败。在我们的方法中，在乐观的情况下（例如，大多数节点是诚实的），我们享受异步协议的快速特性；然而，我们保留了同步（例如，区块链）协议的弹性，以及它们的健壮性属性（例如，支持零星的参与）。更准确地说，我们展示了如何组合快速和简单的异步路径，它保证了一致性，但不保证活性，当出现问题时会执行“回退”进入同步路径。

2 Thunderella 范例

我们所说的快速或即时的确认：一个共识的协议被认为是**响应性**的，当且仅当，任何对诚实节点的事务输入都会被及时确认，这只取决于实际的网络延迟，而不是在网络延迟的任何已知的上界。

如{41]所示，实现响应需要我们假设有2/3的玩家是诚实的。（另外，所有已知的响应协议都非常复杂，因此很难实现。）为了克服这个问题，我们在这里考虑一个乐观的响应性的概念，当某些好的条件满足时，响应只需要保持即可。更准确地说，我们考虑了两组条件：

- **最坏情况（W表示），协议提供最坏情况的保证，包括一致性和缓慢确认（例如，W=多数诚实）**
- **乐观条件下（O ∈ W表示），协议提供响应性确认（例如，O=超过3/4是诚实和在线的，而一些指定的玩家（领导者）是诚实的）**

Thunderella 是这样一个范例，采取一种blockchain协议(许可或无许可)满足在W条件下一致性和活性，并在O条件下将其转换到一个新的协议，以满足乐观响应性。

3 方法概括

乐观条件下协议：

- 我们有一个指定的实体：领导者，或者加速器。
- 交易被发送给领导;领导者签署交易（增加序号），并将签署的交易发送给委员会成员。
- 委员会成员对所有的领导签名的事务都进行了处理，每个序列编号智能处理一次。
- 如果一项交易收到了超过3/4的委员会签名，我们将其称为公证的交易。参与者可以直接输出他们最长的连贯的公证交易序列（根据他们的序列编号），所有这些交易都是被确认的。

不难看出，这个协议在W'（ > 1/2的委员会是诚实）的条件下是一致的，此外，在O=“领导者诚实，3/4的委员会是诚实的”的条件下，它满足于活性和乐观的响应性。

为了在W'的条件下保持协议的活性，我们底层使用（缓慢的）区块链协议，它满足了在W（大多数玩家是诚实）的条件时的一致性和活性。

- 如果玩家注意到交易没有得到领导者/委员会的确认，那么一些证据就会被发送到底层区块链。
- 然后会进入一个冷却期，委员会成员停止从领导者那里签署信息，但是允许玩家广播他们迄今为止看到的任何公证的交易。冷却时间的长度被计算在底层区块链上的块上（例如，k个块的时间，k是安全参数）。
- 最后，在冷却期结束后，我们可以安全地进入一个缓慢阶段，在这个过程中，交易只会在底层区块链中得到确认。我们可以使用区块链来重新选择领导者（如果需要的话），并开始一个新的乐观协议的周期。

需要一个冷却时间的原因：如果没有它，玩家可能在进入慢速模式之前已经确认的交易集上有不同的意见，因此可能会得到不一致的观点。冷却时间使诚实的玩

家能够将他们看到的所有已被公证的交易发布到（缓慢的）底层区块链，从而（缓慢地）达到这一套交易的一致性;
一旦我们达到了这个一致的视图（在冷却结束的时候），我们就可以完全切换到确认区块链上的新交易。

收集作弊的证据
现在，如果玩家在区块链上看到一些交易，没有在足够长的时间内（比如在n个块中）进行公证，他们就知道领导者/委员会一定是作弊/不可用，因此应该进入冷却期。
（请注意，只要领导者能够在基础区块链上创建n个区块之前确认交易，他就不能被“错误地指控”）。

选择委员会
到目前为止，我们已经构建了一个协议，它满足了在W∩W'条件下的一致性和活性（即
假设有一个诚实的大多数成员，并且在委员会中是一个诚实的多数人），并且在乐观的情况下，以乐观的态度来满足自己的要求。现在的问题是如何选择委员会。
我们考虑两种不同的方法：

- **所有的参与者作为委员会**：在一个需要许可的设置里，最简单的方法是使用所有的参与者作为委员会。
- **利用最近的矿工作为委员会**：在许可和无许可的情况下，可以选择挖掘最近几个区块的矿工作为委员会

4 Permissioned, Classical Environment

简单场景，节点一次加入，保持在线状态

1. 使用Dolev-Strong-based 作为底层区块链

2. 每个节点都作为委员会一员

3.n为节点总数，f为腐败节点，一个交易被通过，至少需要[(n+f)/2+1]的同意签名

4.最后，我们对之前的方案做了一个不必要的修改，如果幸运的话，事务将从协议的最开始立即开始确认，而不需要任何预热时间。

具体地说，我们假设创世纪是最初时代的一个乐观的部分（例如六月时代);

5.Thunderella for Permissionless

1.如何选取和更新委员会

根据底层区块链得到过去的矿工，由过去的矿工组成委员会

由权益持有者作为委员会

2.如何选取领导者