



渔翁系统白皮书

Fisher System Whitepaper

版本: v1.0
2022-03-20

1. 背景

2008年中本聪《比特币：一种点对点式的电子现金系统》（*Bitcoin: A Peer-to-Peer Electronic Cash System*）论文及之后的软件的发布正式启动了比特币金融系统，随后比特币从技术极客到炒作军的介入，比特币的价格不断破新高，其背后的技术也被挖掘出来成为区块链概念不断发展。

2015年以太坊将智能合约的概念带入区块链，从而发展出各种各样的支持可扩展的公链出来。大量的经济模型被提出，然后构建各种实验系统。瞬间引起的资本的注意，大量资本冲入，非常热闹。高性能公链系统EOS的提出更是出现了史上最大的公链融资项目。

后来基于公链上的应用DEFI，跨链、NFT等的兴起又带动了一轮又一轮的投资投机热。

到现在为止，大部分的DAPP都是在币圈内部炒作投机，很少见到有系统是解决现实生活中的问题，提高现实生活中的效率。而本文提出的渔翁系统确是一个利用区块链智能合约技术来解决现实生活中的信任问题，具有很大的实用价值。既可以降低陌生人间交易成本，又可以提高交易的安全性。

2. 系统简介

渔翁系统是一个基于区块链公链智能合约生成虚拟信用的系统。它通过超额抵押有价值的虚拟资产及若干逻辑组合来生成虚拟信用，基于生成的虚拟信用后用户就可以实现安全的交换或者交易。任何人都可以通过该系统产生自己的信用。

该系统的命名灵感来自于中国一个古老的寓言故事：鹬蚌相争渔翁得利。讲述河蚌和鹬鸟这两种动物相争，都不想退让，最后被路过的渔翁得了便宜的故事。在这里启示交易的双方在遇到纷争的时候要多站在对方的立场理解纷争的原因及责任，应该或者能够让步的时候就好好协商，履行约定。如果因纷争互不相让，而最终违约。那么渔翁合约这个达摩克利斯之剑就会落下，双方两败俱伤，最终渔翁得了利。当然渔翁是个善良的角色，所得之利将用于公益方面。

通过借用这个深刻而且极具教育意义的寓言故事来命名这个系统。系统主要解决两个问题：一通过“预设条件”算法用户可以安全地抵押资产，不用担心对方或者其他人的恶意的欺骗而被锁定无法取回。二通过“与锁”算法机制，即双方都解锁，资产才能取回的机制来实现违约方不可无损失，从而保证交易的安全。

在现实生活中，我们都有遇到陌生人非面对面的交易或者交换需求。特别是现在元宇宙的概念催生出很多玩法，玩家大多都上线上交流，这就会有交换或者交易的需求。而在有利可途的环境下，骗子大行其道，任何轻信都有可能蒙受损失，这时候就需要有个安全的通道作为第三方来保证安全的交易。以前在有这个需求的情况下，我们往往会想到专业的第三方，如ESCROW、支付宝等。但是这类第三方由于需要运营庞大的团队的成本而导致费用不菲，可能收费远大于交换物/交易物的价格。也有可能他们根本不会受理这些小单。在这种情况下，渔翁系统可以帮你很大的忙，它成本极低，但是很安全，它也不会因你是很小的单而拒绝你。因为这一切都是可以由交易双方自我掌控。

因而可以想象这是个有很大的实用价值的系统，凡是跟信用安全相关的需求都可以考虑使用该系统。它可以解决物与物的安全交换，也可以解决物与钱的安全交易。跨链交换虚拟资产的问题也可以通过该系统简单的实现。在元宇宙中，它可以作为连起一座座孤岛，作为各元宇宙之间，元宇宙和现实世界之间的桥梁。这个系统的另外一个价值在于可扩展性，可以基于虚拟信用的概念开发各种各样的应用，以解决特定的领域的问题。

当然要完成如上所说，你需要耐心来理解系统的独特的设计思想，它并不复杂。该系统可以使用基于智能合约的公链来实现。在这里我们先基于EOS公链来实现，以充分利用EOS独特的性能优势。

3. 主要功能

该系统的核心功能是通过超额抵押及非达成不可取回来产生虚拟信用，从而实现了违约者不可能无损失的目标。所以要使用该系统来解决你的问题，你需要有链上资产。下面介绍功能的实现流程逻辑。在这个模型中，发起方称为邀约方，接受邀约方称为应邀方，渔翁协议作为第三方。

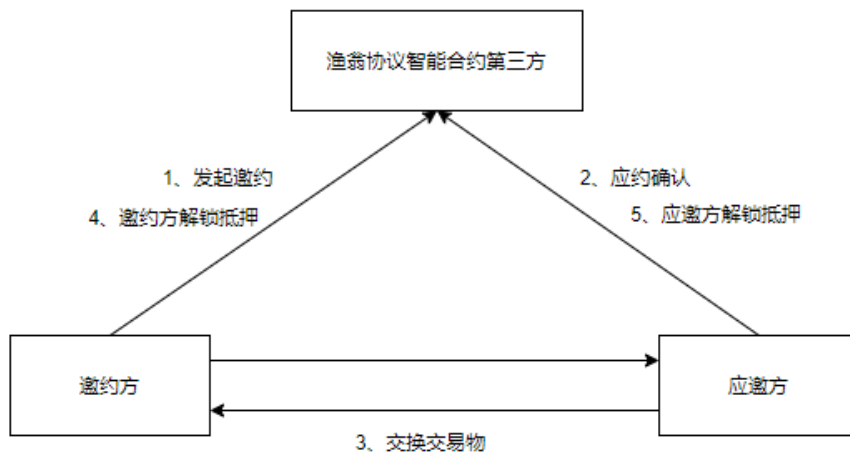


图3、业务流程图

- 1、在协商一致后，交易邀约方向智能合约发起抵押邀约，邀约包含抵押参数，如抵押物数量，应邀账号
- 2、应邀方收到邀约后，检查抵押参数是否与之前协商一致，确定后按抵押参数执行应约动作。
- 3、交易双方交换交易物，可以由任意方先发起，只要最终实现协商的方法成功交换即可。
- 4、交易物成功交换后，邀约方解锁应邀方的抵押物，解锁动作也可以由应邀方先执行，此时尚不可取回抵押物
- 5、应邀方解锁邀约方的抵押物，在都解锁对方的抵押物后，双方才可取回抵押物，整个交易过程结束

3.1. 邀约

第1点指定参数的设计是防止其他人来恶意的调用合约来锁定你的资产，如果没有指定对方抵押物数量和应邀账号，那么其他人没有提供抵押资产就调用合约来锁定你的资产，导致你无法取回。抵押物数量的选取要使其总体价值是交易物的一倍以上，否则在出现违约情况下有无法保证交易的安全。

3.2. 应邀

第2点，应邀方需要提供不少于邀约方指定的数量的抵押物方能执行锁定成功，否则无法锁定动作。一旦锁定后，除非双方达成一致，都同意并都执行解锁后，抵押的资产方可取回。如果未能达成一致，或者有一方未按约定执行，那么另外一方不应解锁，否则就会遭受更多损失。通过渔翁系统把安全掌握在自己的手里。当然实际交换或者交易中会遇到各种各样的不可预料的问题，这时候需要双方实事求是，秉着善意作些合理的退让或者让步，分担因未预料而遭受的损失。

当然在这过程中也可以请双方都认可的第三方来评判或者裁决。但不管怎么样，在最终执行约定前不要解锁抵押资料，这是协商谈判的筹码，是安全的保证。系统无法判断是谁违约了，系统只是提供给双方一个不解锁对方抵押资产的权力来使双方有协商的筹码。如果最终无法达成一致，那么渔翁合约就会将双方的抵押资产没收。当前初始的处理这些没收的资产将主要用于自然灾害的公益捐款，抵押资产的原所有者可以保留署名权。用心的读者肯定想到了这抵押资产的价值与交换/交易物的比例设定是安全的关键。这部分在安全机制这个章节详细论述。

3.3. 交换或交易

第3点，由于在第2点，应邀方根据条件应邀锁定自己抵押资产，此时双方已经都无法取回资产，这个设定是安全的关键。此后交易/交换双方就可以安全地交易/交换交易物了。双方谁都可以先发送交换物，只要双方执行约定，能够将交易物送达对方即可。为了降低在违约情况下的损失，这里提出一个叫“先手之权”，即承诺先发送交易物并且确认对方收到的一方可以抵押资产少于另外一方。这种情况下比对等抵押模式在违约的情况损失要小。

3.4. 解锁抵押

第4点，在完成交易没有疑异后，双方就可以进行解锁抵押物的流程。解锁可以任何一方先发起。唯一要注意的是解锁是在双方已经完成约定的交易后才可以，否则有可能出现损失。在双方都解锁各自的资产后就标志这该交换的完成。在使用该系统的时候要避免思维上的限制或者误区，即锁定后双方是可以进行多次的交易或者交换。也就是说渔翁系统是建立一个安全的通道，而通过这个安全通道可以完成多次交易。

3.5. 释放抵押资产

第5点，在双方都释放锁定的资产后，系统就会释放双方的抵押资产锁定。此时双方就可以取回各自的资产了。

从以上步骤及要点看，在整个过程中，系统不触碰用户的交易物。这个设计提高了系统的灵活性，也增加了隐私性，可应用的范围也更广。用户通过渔翁系统生成虚拟信用后，可以进行多次交换或者交易。从这也可以看出渔翁系统是用来提供一个安全层，建立一个安全通道，而不会对交易的细节进行限制。最大程度地提高灵活性。

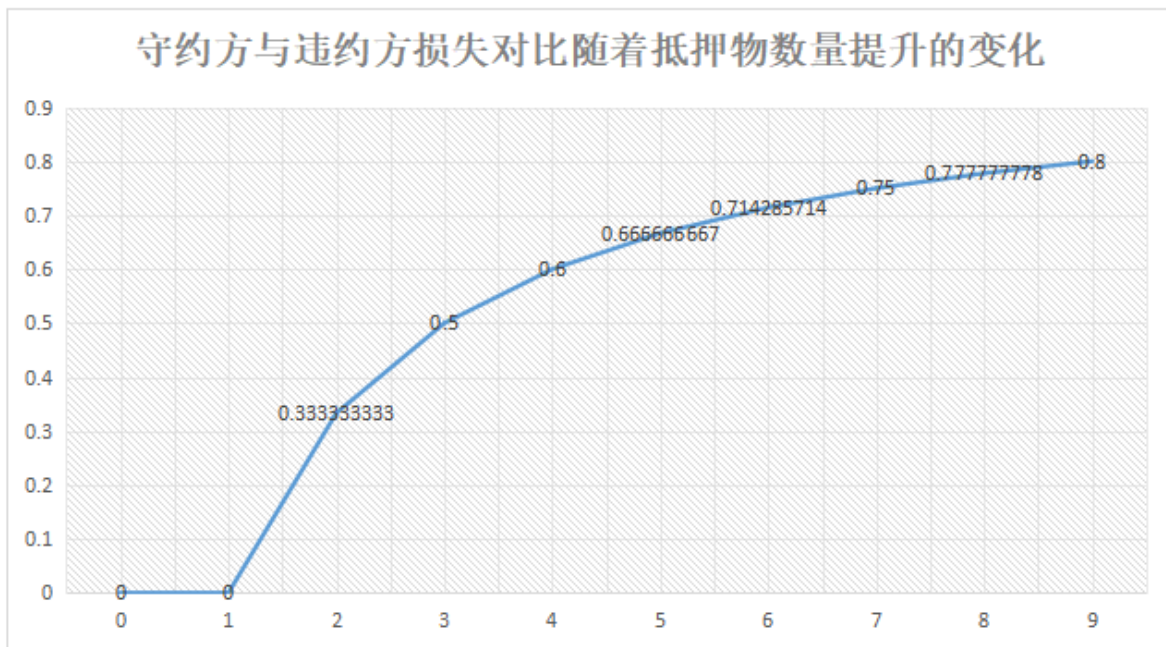
4. 安全机制

从上一节的介绍，我们知道渔翁系统通过邀约方的条件指定来保证自己的资产不会被恶意锁定。解锁时通过“与锁”保证双方都满意交易结果后才能取回抵押资产。这两个是渔翁系统的硬性逻辑来保证交易安全。而实际还需要配合参数的设定逻辑来保证总体的安全。仔细思考的人已经发现了抵押物的数量选定是最终安全的保障。如果超额抵押物设定不合理，不能对对方的心理产生限定预期，就不能好好保障安全。这里我们来仔细分析这个问题，即抵押物的超额数量应该设置多少才能更好的保障安全。

从人性的角度来看，正常人都是损失厌恶，如果有损失的可能，那么作恶的行为就会受到限制。除了这点，人还会受相对损失的感受情绪影响，比如以对方损失比自己多来自我安慰。那么系统参数选定的时候在这两种心理做一个平衡就很关键。当然系统会有足够的时间让双方都冷静地地理性思考，所以厌恶损失的心理起主要作用。但是从威慑力的角度，强调相对损失心理也会影响双方的最终决定。以下显示双方如果出现相争不让的情况，或者出现违约的情况双方的损失对比。

抵押物交易物对比倍数	0	1	2	3	4	5	6	7	8	9
守约方损失	1	2	3	4	5	6	7	8	9	10
违约方损失	0	0	1	2	3	4	5	6	7	8
相对损失对比	0	0.33333333	0.5	0.6	0.66666667	0.71428571	0.75	0.77777778	0.8	0.8

以下是依此绘制的变化图表。



从图中我们可以观察到，当出现违约时，随着抵押物相对交易物的倍数不断提升时，双方的损失就越接近，也表示安全系数越高。安全的起点在于抵押物为交易物的一倍以上。所以为了实现“不让违约者没有损失”的目标，超额抵押需要至少要一倍交易物价值。

渔翁系统并不会限制你配合其他的安全机制一起保障交易的安全。当交易的双方无法直接协商出结果，那么他们可以将自己的控制权交给双方都信任的第三方，由他们裁决纠纷。

对于解决遵守规则的守约人却损失的更多的问题。应该这么说，骗子应该是不愿意以自大的损失来换取他人更多的损失，所以骗子应该会离开这个系统。除此之外就是在交易过程中遇到了问题，双方无法在由谁负责这些问题上产生了纠纷，且不愿退让的。那么这时候渔翁系统方将没收双方的抵押物。没收的抵押物会留一小部分用于系统的运营，大部分用于自然灾害的捐款，抵押物原所有者将保留有署名权。

5. Roadmap

在能够获得与预估相近支持的情况下，按照如下的演进路线推进。

- 1、在2022年第一季度末实现MVP(Minimum Viable Product)，即实现系统的核心功能：生成虚拟信用。（该部分当前接近完成）
- 2、在2022年第二季度前后，招募社区自愿者参与最小系统的小规模内部测试。另外一方面完善其他功能，如邀请奖励机制等。
- 3、在2022年第三季度、第四季度前后，建立社区DAO组织，提供面向所有人使用的系统。
- 4、在2022年第四季度前后，开发基于telegram机器人的系统，让交易者可以用社交工具就可以使用。
- 5、在2023年一季度，在评估安全后，全面开源。

6. 系统经济模型

本章节描述系统的收入来源，如何分配这些收入。

6.1 收入及分配

渔翁系统作为一个可扩展的系统，其可能有如下几方面的收入来源：

- 1、实质性锁定收取的手续费。
- 2、可扩展应用接入时接入服务费。
- 3、违约后渔翁得利部分留存运营费用的部分。

这些收入都会通过一定的机制分享给系统、社区的建设者、参与者。分配机制最终由去中心化DAO制定。

6.2 积分TOKEN发行（尚未确定）

目前暂未计划发行，系统的运行也不依赖于TOKEN。

另注：后期如为了提供构建DAO管理的权力分配，且在合规可行性下，发行积分TOKEN。这些积分都将免费发放给渔翁社区的贡献者、参与者。

7. 参考

[1] [比特币（加密数字货币） 百度百科 \(baidu.com\)](#)

[2] [第三方托管 百度百科 \(baidu.com\)](#)

8. 免责声明

本白皮书仅用于介绍项目系统的信息，它不构成投资的建议或者暗示。本项目不发币，也不作为交易交易物的传输媒介。一旦参与项目即表示了解并接受该项目风险，遵守了所在地区的法律法规则，并愿意为此承担一切相应后果。本文仅代表当前的观点，本文所反映的观点如有变更，恕不另行通知。