



WINCHAIN

面向全球彩票市场的国家级区块链彩票系统

白皮书
version1.0

Victory Game Challenge
www.winchain.co

ABSTRACT

摘要

WinChain是由硅谷Victory Game Challenge团队研发的区块链构架的国家级底层彩票体系，通过团队的区块链技术优势和领先的行业资源，用去中心化的区块链技术革新彩票行业，将区块链彩票发展成为世界彩票底层系统的标准。Victory Game Challenge团队的愿景是成为区块链时代全球领先的彩票解决方案提供商。

Winchain创新的设计了双链机制（公有链+联盟链），用来实现其链上项目的业务支撑和落地应用。通过公有链+联盟链融合的方式使其生态完美的达到权益去中心化、记账去中心化、交易去中心化，项目的应用流通瞬时高效且费用极低的最优解。

TABLE OF CONTENTS

目录

一、	概要	1
二、	当下彩票及博彩行业存在的问题	1
2.1	项目背景	1
2.2	彩票业基本理论和运作方式	2
2.3	当前彩票业发展的主要问题和瓶颈	4
2.4	什么是区块链?	5
2.5	传统彩票业将因区块链而产生质的进化	6
三、	Win 机制和系统构成	8
3.1	Smart KYC 账单身份管理系统	9
3.2	区块链数据管理系统	10
3.3	交易处理系统及预言机	12
3.4	开发者生态	13
3.5	WinChain 生态	14
四、	体系构成	15
4.1	WinChain 开源技术基金会简介	15
4.2	WinChain 生态构成	16
五、	双链机制和发行方案	17
5.1	系统将发行两种通证	18
5.2	WinToken 的价值	19
5.3	代币发行方案	20
六、	团队和顾问	23
6.1	团队成员	23
6.2	顾问与早期投资人	25
6.3	行业顾问	25
6.4	拟合作单位	26
七、	WinChain 路线图	26
八、	总结	26
九、	法律事务和风险说明	27
9.1	WinChain 项目的法律结构	27
9.2	免责声明	27
9.3	风险声明	28

一、概要

WinChain 是由硅谷 Victory Game Challenge 团队研发的区块链构架的国家级底层彩票体系,通过团队的区块链技术优势和领先的行业资源,用去中心化的区块链技术革新彩票行业,将区块链彩票发展成为世界彩票底层系统的标准。目前莫桑比克国家彩票系统已经决定采用公司的区块链技术来发行彩票,目标是 2018 年 8 月发行世界上第一张基于区块链的彩票。在亚洲欧洲一带一路沿线国家以及非洲国家正积极拓展中,目前已经有若干个国家彩票系统有积极推动的意向。Victory Game Challenge 团队的愿景是成为区块链时代全球领先的彩票解决方案提供商。

现今区块链应用大概分为两类:公有链和联盟链。公有链体系具有最佳的去中心化特性,但是交易缓慢且需要支付高额手续费,大部分的落地应用并不适合;联盟链在效率和费率上具有非常大的优势,但是均为机构节点,达不到完全的数据公开透明监督。有鉴于此 Winchain 创新的设计了双链机制(公有链+联盟链),用来实现其链上项目的业务支撑和应用落地。其中公有链作为记账人节点选举机制的依托,利用公有链的开放特性,让更多的人参与到联盟链的节点登记和记账,并给予一定的回报,来逐渐完善联盟链的参与者生态建设,使其公开、透明、健壮等特性无限接近于公链。联盟链作为应用的立足底层技术平台用来支撑各国的彩票发行业务和相关技术支撑、周边生态支撑,在交易效率和手续费方面,支持瞬时、极低手续费的链上资产流转。通过公有链+联盟链融合的方式使其生态完美的达到权益去中心化、记账去中心化、交易去中心化,项目的应用流通瞬时高效且费用极低的最优解。

二、当下彩票及博彩行业存在的问题

2.1 项目背景

彩票的产生,可以追溯到两千年前的古罗马时代。那时,人们用彩票进行抽奖,最初仅是一种博彩性的娱乐活动。后来,彩票业在各国盛行起来,并逐步演变成集游戏、竞争、娱乐和筹资于一体的行业。

到 20 世纪 80、90 年代,彩票进入了爆炸性发展的时期,世界彩票销售量突飞猛进。彩票发行从发达国家到非洲发展中国家遍地开花,到今天全世界已有 150 多个国家发行各种形式的彩票,俨然已成为世界第六大产业。

2018 年 1 月,世界彩票协会组织在瑞士巴塞尔发布了 2017 年上半年的全球彩票销售情况。统计数据显示,对比 2016 年同期,全球彩票业销售整体增长 1.8%。其中,非洲彩票市场表现强劲,以 5.6% 的销售额增长率超过亚太地区,成为全球增长最快的地区。世界彩票协会作为 WinChain 行业顾问,将帮助 WinChain 推进和落地全球的发展和布局。

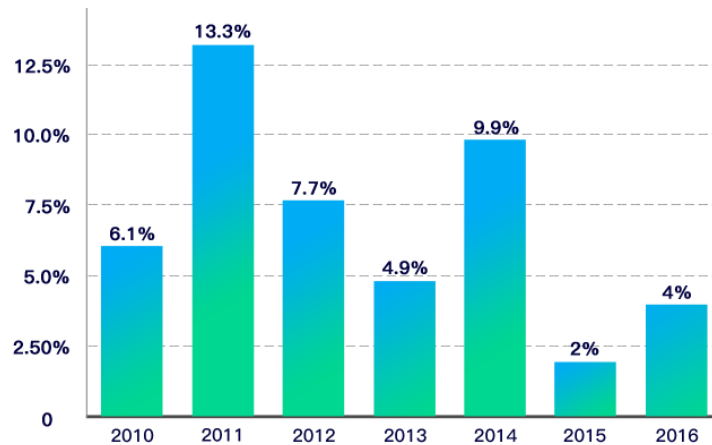


图 2-1 全球 2010-2016 彩票销售增长率

非洲的彩票行业发展迅猛，作为新兴市场，一直吸引着全球彩票市场的关注。WinChain 生态相关合作公司在 2017 年已在非洲多个国家完成布局，并已获得莫桑比克国家彩票发行和运营牌照，其他国家正在顺利推进中。

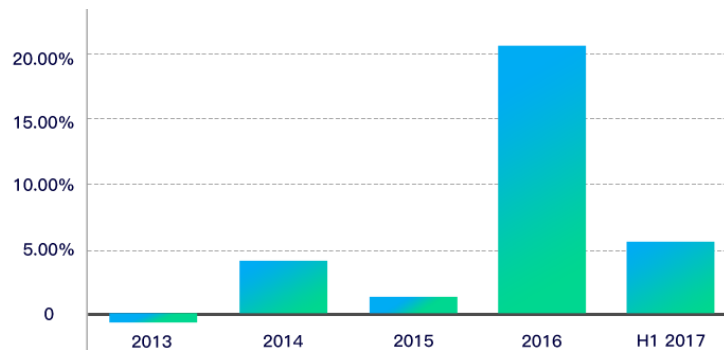


图 2-2 非洲 2013-2017 上半年彩票销售增长率

2.2 彩票业基本理论和运作方式

2.2.1 拉普拉斯概率理论（概率均等理论）

拉普拉斯概率又叫传统概率，如果一个随机试验所包含的单位事件是有限的，且每个单位事件发生的可能性均相等，则事件 A 在事件空间 S 中的概率 P(A)为：

设随机实验 E 的样本空间(随机事件 E 的所有基本结果组成的集合为 E 的样本空间)为 Ω 。对 E 的每一事件 A 赋予一个实数 P(A)，且满足以下公理：

- 1) 非负： $P(A) \geq 0$ ；
- 2) 规范： $P(\Omega) = 1$ ；
- 3) 可列(完全)可加性：对于两两互不相容的可列无穷多个事件 $A_1, A_2, \dots, A_n, \dots$ ，有 $P(A_1 \cup A_2 \cup A_3 \dots) = P(A_1) + P(A_2) + \dots$

则称实数 P(A)为事件 A 的概率。

例如，在一次同时掷两个硬币的随机试验中，假设事件 A 为同时获得人字面，那么事件 A 的概率应该有如下计算方法： $S=\{(人字, 人字), (人字, 数字), (数字, 人字), (数字, 数字)\}$ ，按照定义，A 的概率为 $1/4$ ，因为人们不知道，硬币是否“完美”，即硬币制造的是否均匀，其重心是否位于正中心等。尽管如此，传统概率在实践中被广泛应用于确定事件的概率值，其理论根据是：如果没有足够的论据来证明一个事件的概率大于另一个事件的概率，那么可以认为这两个事件的概率值相等。

概率论统计定义：

设随机事件 A 在 n 次重复试验中发生的次数为 n_A ，若当试验次数 n 很大时，频率 n_A/n 稳定地在某一数值 p 的附近摆动，且随着试验次数 n 的增加，其摆动的幅度越来越小，则称数 p 为随机事件 A 的概率，记为 $P(A)=p$ 。

2.2.2 彩票种类

当前彩票大致分为三类：

1) 概率游戏（乐透类）

超级强力球，双色球，49 选 6，3D，5D，7 星彩，22 选 5 等；

2) 竞猜游戏

竞彩足球，竞彩篮球，单场彩，虚拟游戏竞猜等；

3) 即开游戏

刮刮乐、快开等。

2.2.3 运作模式

运作模式大致分为三种：

1) 政府委托其他机构代销

以法国为例，法国政府成立了专门的彩票发行公司—法国国家游戏集团，法国预算部是法国彩票业的主管机关，代表法国政府对游戏集团的彩票活动进行监管。

与法国不同，西班牙彩票业的主管部门是财政经济部，具体经营者是隶属于财政经济部的西班牙国家彩票管理局(属于政府机构序列，主要职员全部是公务员)。

美国所有的彩票组织则都作为州政府的机构或彩票公司来经营。美国没有统一的国家彩票，彩票发行均由各州决定，由州议会立法，州长指定几位议员组成彩票委员会。彩票局发行彩票所筹集的公益基金交州政府，由基金管理委员会根据相关法律决定使用。

2) 企业承包模式

英国国家彩票(National Lottery)是这一模式的典型代表。此种彩票由英国议会批准发行，为公益事业筹集资金，通过公开招标的形式，向中标公司颁发经营许可证经营。

3) 发照经营模式

欧洲很多国家的政府根据本国需要，发放彩票业经营执照，获得彩票发行执照的既有国营企业，也有私人企业。

2.3 当前彩票业发展的主要问题和瓶颈

彩票运行过程中安全、透明与效率是当前彩票业最主要挑战。一般定义彩票投注兑奖主流程为：



在以上流程中存在的问题如下：

- 1) 购买彩票时需到彩票销售网点购买，尚不能脱离物理地点的限制；
- 2) 投注时购彩人与销售网点对打印选号易产生纠纷；
- 3) 摇奖过程需第三方公证员在场，中奖号码的公信力仅以第三方公证员的信誉为背书；
- 4) 奖金计算是在一个集中的中央系统中完成，因此奖金数额的公信力也仅以第三方公证员的信誉为背书；
- 5) 奖金的发放和销售点的佣金以国家信誉为背书；
- 6) 所有数据是在公证员的监督下开奖前在独立硬盘中备份，也就是说，所有数据的保存同样仅以第三方公证员的信誉为背书。

再来看彩票业普遍采用的中央集中式 IT 系统与以上流程对应的操作流程：



这种中央集中方式 IT 系统存在的缺陷如下：

- 1) 购彩人可以怀疑打印彩票的号码与自己当初所选的号码不符，也就是说，中央集中式 IT 系统无法制止抵赖行为的产生；
- 2) 无法完全避免内部人员和公证员串通修改中奖结果；
- 3) 公证员有被彩民收买的可能；
- 4) 数据封存时有机会被内部操作人员篡改；
- 5) 计奖不透明；
- 6) 服务器可能被黑客攻击篡改数据。

此外，在彩票的流通环节上，目前彩票发行模式基本以彩票发行机构为中心或顶层，通过代理机构向彩民销售彩票，以集中中心化多层次的模式运转。由于不透明中心化的运行模式造成了发行主体、中奖客体、发行标的、运行规则的不可信，每个环节都做不到透明、公平和完全可信。

2.4 什么是区块链？

2.4.1 区块链概述

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术在互联网时代的创新应用模式。具体来说，区块链技术是构建在点对点网络上，利用链式数据结构来验证与存储数据，利用分布式节点共识算法来生成和更新数据，利用密码学的方式保证数据传输和访问的安全，利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

通俗的说，区块链是一套多方参与的、可靠的分布式数据存储系统，其独特之处在于：一是记录行为的多方参与，即各方参与记录；二是数据存储的多方参与、共同维护，即各方均参与数据的存储和维护；三是通过链式存储数据与合约，只能读取和写入，不可篡改。

在应用实践中，这种系统能够实现所有参与者信息共享、共识、共担，从而帮助现有的经济体系脱离通过制度约束或依赖第三方机构背书的模式，双方直接实现价值交付。这种特性可以有效降低交易成本，提高交易效率，减少因交易一致性所引发的摩擦。同时，区块链具有既公开信息又保护隐私，既共同决策又保护个体权益的特性。

2.4.2 区块链在应用上的特性总结

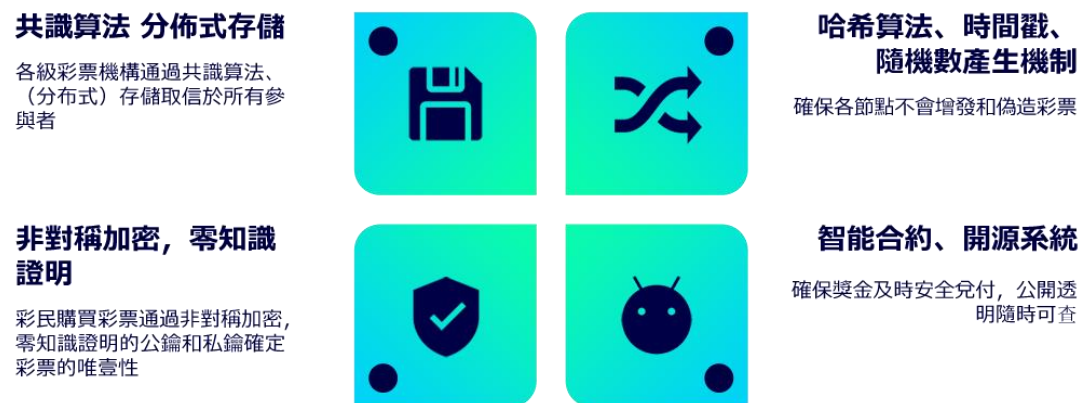


图 2-3 WinChain 系统特点

当前区块链概念已经引起了各行业的广泛关注。之所以如此引人注目，因为从根本上区块链将变信息互联网为价值互联网，变信息可计算为价值可信任。这使得区块链可以通过颠覆传统的信息系统技术模型来支撑实现业务上的高可信应用。

具体来说，区块链技术在应用上的各方面特性简单总结如下：

- 1) 区块链系统的使用：通过各种加密技术使所有产生的有效信息与数据不可抵赖，不可篡改；
- 2) 区块链系统的运营：通过智能合约使系统运转与管理都按约定规则自动进行，不受任何唯一方控制，实现去中心化或多中心化；
- 3) 区块链系统的开发：所有的规则与源代码，都按约定开发完成并透明开放，开发者无法隐藏后门；
- 4) 区块链的分类按照节点准入规则，可以划分为公有链、私有链和联盟链。

2.5 传统彩票业将因区块链而产生质的进化

区块链天生的技术优势恰巧是彩票行业当前以及未来发展所急需的基础能力。需要说明的是，彩票领域区块链应采用“许可制”区块链的模式。区块链的应用将使彩票业的运行更安全、透明、高效。

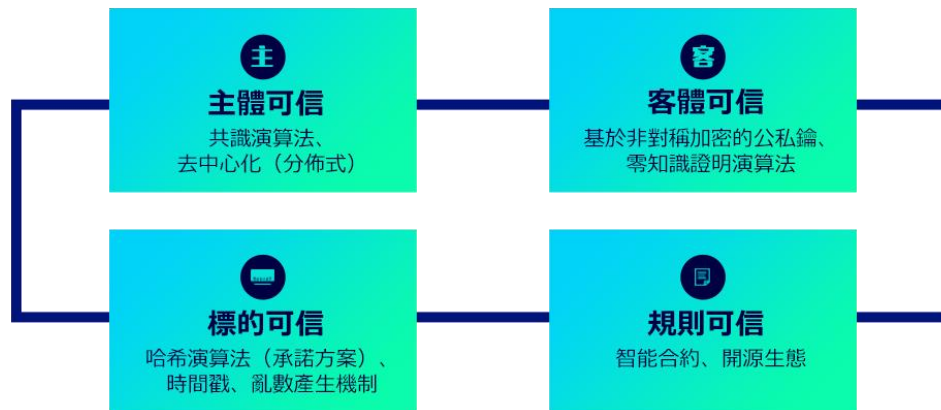


图 2-4 区块链与彩票的高度匹配

2.5.1 区块链技术的应用将使彩票数据更为安全

以国家彩票机构现有的运行模式为例，由于区块链技术具备可信的特征，我们可以以省级销售机构、中央发行机构、省级财政监管机构、中央财政监管机构以及当地公证机构等为多个节点构成联盟链，把各种彩票游戏所产生的全部或部分原始数据上链存放，从而实现实时彩票数据的封存，做到符合彩票法规规定的的数据封存要求。

数据封存应用区块链可以实现无障碍、无误差、无干预的身份验证和鉴证确权，以及信息共享。可以保障彩票行业内制定的规则体系可信无误地自动化运转。例如，用共识算法、去中心化保证主体即发行销售方可信；用非对称加密下的公私钥、零知识证明算法来保证客体即彩民可信；用哈希算法、时间戳、随机数产生机制确保标的（即彩票，可以是电子化形式也可以是传统彩票的数字指纹）可信。

2.5.2 区块链极大拓展彩票新游戏的范畴

在移动互联网等通信技术飞速发展的今天，以手机终端为主的新渠道逐渐占领了消费者的视线，而这类渠道的游戏特点是互动参与，原有 IT 体系下的彩票游戏并不太适合这种销售渠道。另一方面，随着互联网的飞速发展，各种私彩不断出现，这也说明了人们这方面的需求远未被满足。

假设存在一个全民参与的公有链，这样所有的交易数据均可以在链里公正地流动，以此为基础，可以实现目前体系无法实现的社交类型的彩票游戏，让在链的参与者公正地互动，从而增加彩票游戏的趣味性。总结来说，区块链技术的兴起可以将社交型游戏、虚拟型游戏等研发引入，使得彩票游戏发展进入广阔的新的领域。

2.5.3 区块链技术构建的全新彩票系统架构将实现完全的公平、透明

彩票作为国家一项公益性项目，每年为世界各国筹集数以亿计的公益资金，然而基于传统中心化的彩票技术，存在运营不透明、易被人为控制等缺陷，虽然有国家的公信力做为基础，但是不可否认，它依然受到了广大彩民的质疑。



图 2-5 与传统彩票系统对比图

假如使用了区块链技术，基于区块链技术实现去中心化，那么任何一个拥有区块链钱包的用户，都可以按国家法律规则发行自己的彩票，为国家筹集公益金和税收。开奖结果基于未知区块进行运算，任何参与彩票的环节，都无法作弊。另一方面，彩票开奖程序已开源，方便用户监督，就算是彩票发行方，也无法事先预知或设定开奖结果。也就是说，基于这种架构的系统因数据发放在参与者手里而提升了系统公正性，使得所有积极的参与者都能因为可以获取数据而做到全面监督，监管公证机构也可以更好地做到监督，克服了传统彩票中心化、不透明、不明确等弊端。

区块链技术将从本质上改变现有彩票销售系统技术体系的实现架构，传统彩票技术体系可能因为区块链技术的引入而发生质的进化，从而真正实现完全的公正、透明。

2.5.4 区块链使彩票发行高效、方便

传统彩票受地域限制，必须使用当地货币才能被购买。而使用基于区块链的数字货币，可以从世界的任何角落进行存储，也就是说，彩民在全世界各地都可以玩彩票，甚至在没有银行基础设施的地区，只要有网络都能玩。

具体来说，我们利用区块链数字钱包程序的生成模块生成含有彩票钱包地址的彩票合约，将彩票合约作为交易数据写入区块链中，通过运行所述区块链数字钱包程序发行彩票合约，对发行的目标彩票合约进行投注后，再利用数字钱包程序的兑奖模块进行兑奖，甚至通过开发智能合约，实现通过区块链自动发放奖金。区块链技术将使彩票发行更为高效、便捷。

WinChain 对标美国 IGT 公司，IGT 作为一家彩票系统服务提供商和运营商，目前年收入超过 300 亿，向各国各地区提供彩票系统技术服务。而行业普遍认为，区块链驱动的彩票系统，将凭借在成本、效率、安全度和公信力方面的优势，一步步成为行业的新标准。WinChain 正是团队结合长久以来的专业行业认知和敏感性，在行业需求驱动下应运而生的。

三、Win 机制和系统构成



图 3-1 WinChain 双链技术框架

3.1 Smart KYC 账单身份管理系统

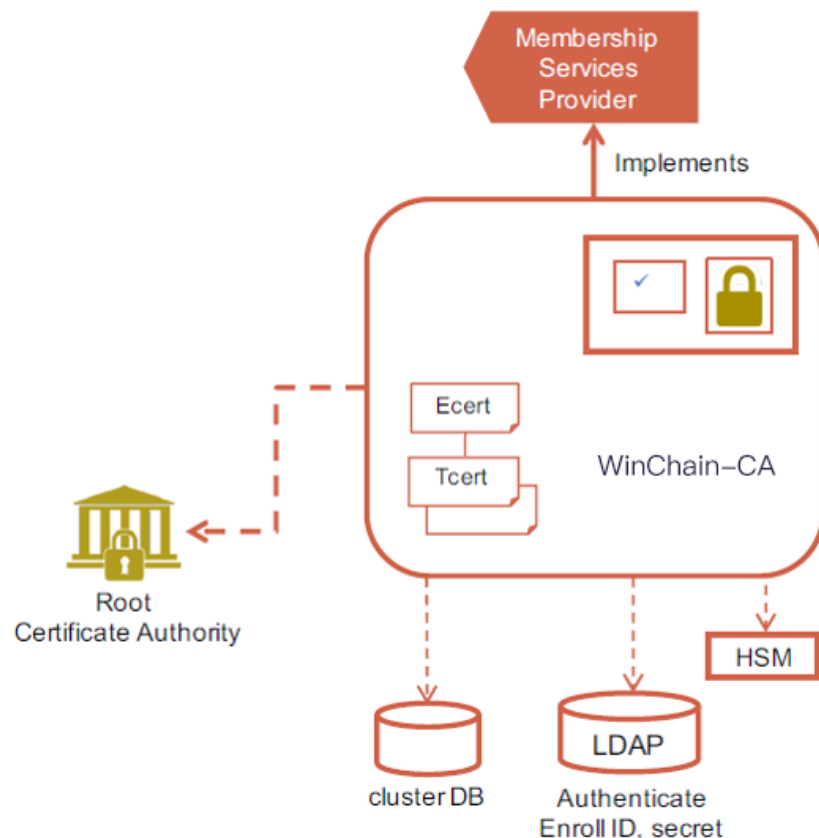


图 3-2 数字证书颁发系统

3.1.1 去中心化用户账户体系

账户是用户在互联网世界的通行证，是用户的身份标识。传统的用户身份存储于中心化的网站服务器中，用户的身份信息保存、修改、验证依赖于中心化服务器的安全和可信，而中心化的服务面临着服务器被攻击的风险，用户的信息随时可能被泄露、篡改，同时，用户的身份依赖于中心化服务商的存在，由于政治、经济、竞争、利益驱动等原因，中心化服务商存在着各种风险；在彩票体系中，用户身份的多样化（彩票包括实名制彩票，半实名制彩票，匿名彩票等），购票的身份验证，购彩用户的身份数据存储安全性，以及兑奖的身份验证和保密性，对用户的身份验证的安全性、灵活性、保密性和防篡改具有非常强烈的需求。

区块链的核心是用户自治的去中心化架构，WinChain 推出的 Smart KYC 账单身份管理系统，不同于中心化账户系统将用户的身份信息和验证过程完全依赖于中心服务器，Smart KYC 采用去中心化的身份验证体系，用户的身份信息和凭证不属于任何机构所有，真正完全掌握在用户自己手中；去中心化的账号系统将用户的身份信息和身份验证过程在区块链网络中进行，分散在全球的完全等价的区块链节点保障了系统的安全性，不存在某个权威的节点。智能合约作为公正的“中心化服务提供者”，代替传统的中心化服务提供者，实现对去中心化组织公开公平的“自治”。

通过在区块链上创建唯一 token 地址，作为用户身份和资产所属的唯一标示，登记在链上的资产，实现资产归属的唯一属性。只要拥有私钥，就拥有资产的使用权和所有权，通过数字签名，实现用户的身份获得，身份验证和资产所有权的拥有及转移功能。

3.1.2 可信身份验证

彩票的购彩全流程中，存在很多彩票遗失、代购彩票归属、兑奖安全等各种问题，核心在于用户的身份验证不可信，用户账单与身份匹配的唯一性需要加强。

Smart KYC 系统将用户的身份验证在链上进行，以 token 的地址作为用户的唯一身份标识和资产标识，购彩和兑奖通过区块链进行唯一性验证，实现智能合约控制下的，无中介参与的用户身份验证和资产转移验证，实现整个购彩生命周期中用户身份的可信验证。

3.1.3 多种场景支持

WinChain 是一个首先用于莫桑比克的基于区块链的国家彩票底层体系，由于世界各国彩票行业的政策法规不同，彩种多样，对用户的购彩身份要求也不一样。WinChain 的 Smart KYC 系统，是一个完整的智能用户身份验证体系，在运用区块链技术保证用户的身份标识和用户身份验证安全可靠的同时，WinChain 结合多种国家身份验证标准和身份验证要求，可以兼容满足各国的灵活身份验证的需求，从而达到完整可靠的去中心化身份验证体系，适用于各国的彩票发行和彩票管理需求。

另一方面，彩票本身将可以交易流转。用户购买彩票后，持有的彩票作为链上资产，用户可以将彩票通过虚拟资产交易转让给其他人，并登记到区块链上，保障数字资产转移的可靠性、安全性和匿名性。

3.2 区块链数据管理系统

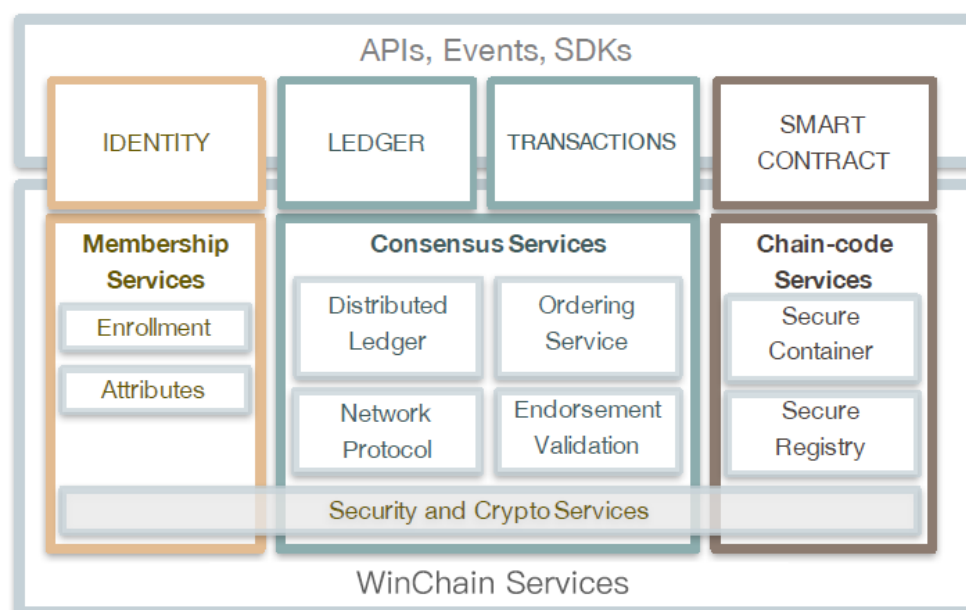


图 3-3 系统模块构成

3.2.1 WinData 彩票数据区块链存储管理

WinChain 支持的区块链彩票体系中，用户购彩后，可以即时在区块链网络上查看到自己的购彩记录，购彩记录存储在区块链网络中，无法篡改和否认，WinChain 官方平台和合作方平台均提供链上数据查询功能，用户可以通过平台或直接链上交易，确保售彩的公正性和安全性；

彩票数据区块链存储管理系统是 WinChain 购彩阶段的核心系统，基于此系统，WinChain 所支持的各国及相应的服务商，不需要关注彩票的发行权和存储权，只需要调用 WinChain 网络的公开区块链数据，向用户提供数据查询功能即可，可以节省大量的系统开发成本和增信成本，从而把精力集中到彩票销售和新玩法研究上。

3.2.2 WinSell 销售数据区块链存证

传统彩票销售路径中，存在大量的多级分支代理机构和多级管理机构，服务链条上包括地区代理、分代理商、销售终端、公正终端、结算终端等复杂的架构，每层机构都需要对销售中的开发和增信进行大量工作，并且获取彩票的分成利润，不同国家 40%-70% 的彩票销售额由各分支机构获得，不论是福利彩票还是体育彩票等，真正落到国家发行机构手中的已经大打折扣，而用于公益事业的资金同样大打折扣。

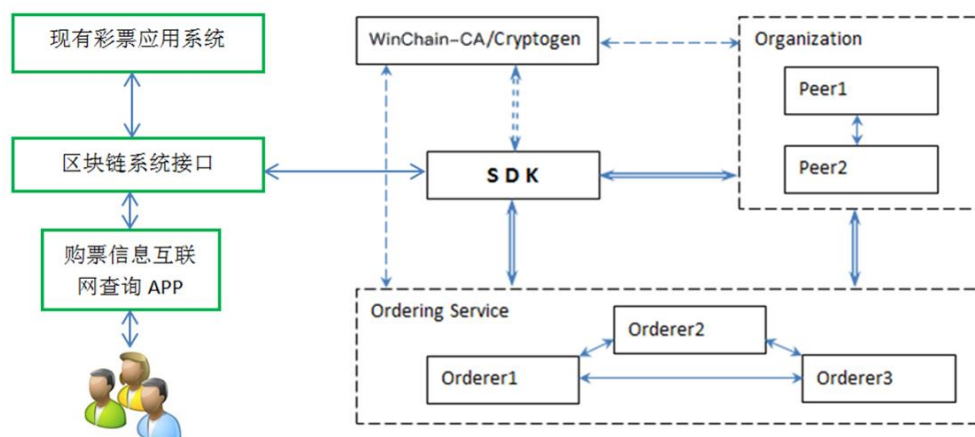


图 3-4 彩票存证应用

基于 WinChain 的销售数据区块链存证，具有两个革新：

传统存证通过每日存储销售数据刻录光盘，由多名各部门公证人员将数据拷贝到光盘后，将光盘备份到公证处、地区售彩中心和主管部门各一份，以此来避免彩票机构内部人员利用职权便利修改数据库，或外部人员通过系统漏洞进行恶意操作。这种方式效率低，且耗费大量人力资源，同时只是将风险由彩票机构转移到公证机构，也很难达到完全信任的目的，不时出现的相关案例也说明了这种做法的不可靠。

WinSell 销售区块链去中心化存证系统，建立多方联合记账的去中心化账本体系，将不再需要人工为了增信而进行繁琐的存证工作，同时避免了存证过程中可能发生的人为风险和系统风险，公开透明的去中心化存证方式，更好地保障存证过程的安全性和绝对可信度。

3.2.3 WinPri 兑奖数据区块链存储管理

传统彩票奖金发放采取线下领奖或中心化分配奖金的方式，奖金存管在中心化机构，分配奖金时进行系统核对并发放奖金，对包括盗领、误领、忘领等通过人工的审核方式进行，这极大的加强了兑奖环节可能的风险性和争议，降低了兑奖的效率。同时其中存在的各层机构抽取奖金也降低了系统的透明性，而增信一直是彩票行业最重要的问题。

WinPri 兑奖结算系统，将最终购彩记录存储在区块链中，联结其他系统的分布式账本，包含用户身份和连接预言机传输的结果，得到竞彩结果后，WinPri 结算智能合约将自动结算奖金，不受任何中心化机构或第三方机构的控制，即时的将奖金分发给区块链网络上用户的身份地址中，保障兑奖过程中绝对的公开、公正和透明。

3.3 交易处理系统及预言机

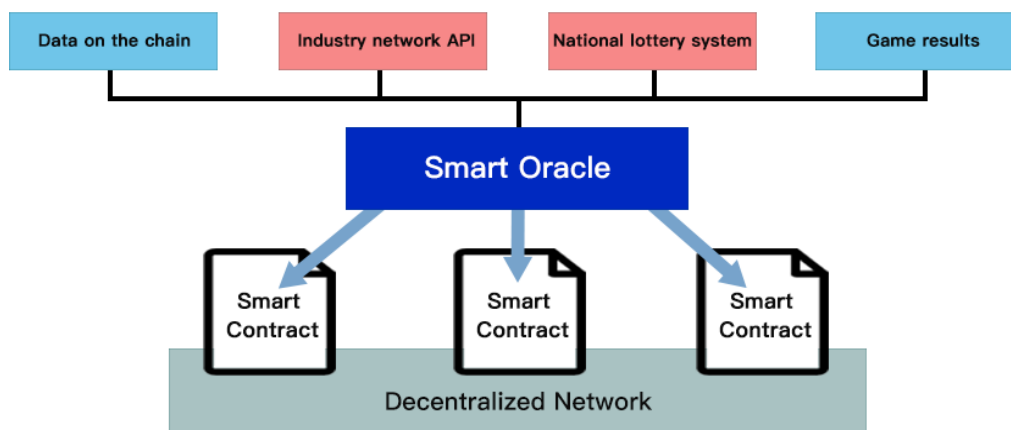


图 3-5 WinChain 预言机

3.3.1 开奖绝对随机数生成

绝对随机数一直是技术领域一个非常有意思的问题，业界提供了非常多的伪随机数的方案。而原有的各种方案因为都是基于中心化的方案，理论上都可以通过多种方式进行攻破或修改，尤其各种在线彩票体系，基于的随机数的安全性和可靠性一直被彩民所怀疑。

区块链的出现，给与了我们新的思路。整个比特币网络以及其他去中心化的底层网络，都是通过分布式的记账方式保证整个网络的运营，而当这个网络达到一定规模后，整个网络因为记账节点的增多，将分布式建立起非常稳固的安全性，多方记账节点的存在保证了整个网络的公正性，除非达到算力绝对控制才可能危及到网络，而比特币的网络已然非常成熟，规模足够大，通过比特币的网络，我们形成了一套独有的基于比特币区块链网络的绝对随机数生成方式，这种方式基于比特币网络的健壮性和去中心化，根据未来一段时间内挖掘的比特币区块的哈希值进行不同的透明算法计算，从而得到基于比特币网络的绝对随机数，从而达到安全可靠随机数，以此向各种彩票游戏提供绝对的随机因子，通过随机因子而得到各种玩法需要的透明随机数，保证开奖的绝对公平性和透明性。

3.3.2 多点态势下去中心化预言机机制

针对传统的彩种和体育彩票，需要根据外部消息结果来进行判定兑奖结果，如世界杯的竞技足彩，智能合约需要获得比赛结果，才能执行合约内容，自动化的处理各项工作。这就需要预言机的存在。预言机现实世界与虚拟世界的连接者，提供数据上链，保证智能合约的正常运行，而单一的预言机存在着来源数据不可信的可能性，作为彩票行业的区块链解决方案，为了保证结果的正确性和可靠性，我们提出一种多点态势下的去中心化预言机机制。预言机来源数据将来自于多个可信节点，同时通过代币奖励机制由 WinChain 网络上的用户选取志愿者进行参与判定，而当多个可信节点的结果出现不同时，区块链网络上的参与者将进行结果多方验证，通过多点数据+多点验证的方式，保证预言机数据的安全性和可靠性，这对保障彩票体系的公开透明非常重要。

3.4 开发者生态

作为国家级的去中心化区块链彩票系统，开发者生态是 WinChain 至关重要的一环。强大的开发者支撑有利于 WinChain 生态的良好发展。随着时代的发展，传统的彩票游戏已经逐步无法满足日益增长的用户需求，用户渴望更多的玩法和更多的游戏形态。

区块链网络下，开发者生态变得更加开放，更加多样。WinChain 作为一个开放的国家级区块链彩票技术平台，平台开放的应用、多样的玩法供各国、各部门、各机构和广大用户选择，是 WinChain 的主要工作之一。

通过和多个国家的彩票发行机构深入合作沟通，新的彩票玩法也被各国各部门所期待。尤其是区块链的去中心化属性和公开透明性，各国都在关注和研究区块链在彩票行业的应用，对新的游戏玩法对彩票行业的改变也非常期待。

3.4.1 新型彩票游戏平台

除了传统彩票玩法外，基于区块链游戏彩票是 WinChain 的重要组成部分，其透明性和公开公正拥有无与伦比的优势。除了传统的彩票类游戏可以直接接入 WinChain 生态外，生态鼓励开发者提供各种新的游戏玩法，尤其是区块链游戏玩法。

WinChain 去中心化体系面向多个国家和部门提供区块链底层彩票技术服务，接入 WinChain 的游戏有机会面向多个国家千万计的用户提供服务，可以为开发者带来极为丰厚的回报。

WinChain 将为开发者提供完备、易用的 API 接口，方便开发者按照接口规范开发相应的彩票游戏，共享万亿级别的彩票市场。

3.4.2 准入通证

彩票游戏是一种博弈游戏，玩法丰富多样，每个游戏的接入都将需要系统审核和对接相关接口，由于玩法的多样很多游戏也需要提前预置奖金或基础资金。

准入通证是 WinChain 开发者生态的基本机制。开发者只有购买 WinChain token 并锁仓后，才可以获得接口的使用权限并提交游戏应用，经过代码审核即可面向各国官方渠道和千万级的彩票用户。

3.4.3 奖励机制

接入 WinChain 系统的游戏，开发者可以自行设定智能合约的一定范围内的收益比例，通过彩票游戏的销售，获得奖励回报，WinChain 将鼓励开发者，协力搭建全球最为安全透明，可靠性强，玩法多样的去中心化彩票游戏平台。

3.5 WinChain 生态

3.5.1 区块链本身，革新彩票管控运营机制

区别于传统多层、多网络、多部门协调、人工操作的模式，WinChain 提供高效、灵活可用的管控运营机制体系，以支持区块链上的投注、记录、存证、开奖和兑奖的底层技术架构，同时兼容不同的游戏形态和组织管理方式，方便各国不同的管理模式接入采用。

3.5.2 与彩票游戏结合，开放的彩票游戏生态，革新彩票游戏机理

如之前所说，全球彩票行业都在期待新技术带来的新玩法，在增加彩票透明性和公正性的同时，进一步扩充彩票游戏玩法，从而吸引彩票用户的注意力。WinChain 彩票游戏平台是一个通过去中心化的方式鼓励开发者接入游戏，智能合约分润，共同促进行业的底层技术体系，可以极大地促进彩票游戏行业的发展。

另一方面，区块链带来的技术革命，也为彩票业带来了更多可能性，利用区块链的技术属性开发的全新区块链彩票游戏，将为行业带来更多的惊喜。

3.5.3 覆盖场景



图 3-6 WinChain 的应用场景

WinChain 包含的去中心化彩票底层系统，支持多种场景的应用，包含：

“传统彩票”：

- 1) 概率游戏（乐透类）：超级强力球，双色球，49 选 6，3D，5D，7 星彩，22 选 5 等；
- 2) 体育彩票：如足球、篮球赛事竞猜，电竞竞猜等；

3) 棋牌博弈游戏：德州扑克等。

“新型区块链游戏”：如透明公正的虚拟资产彩票，结合各种区块链游戏（区块链游戏中各虚拟资产，如以太猫，具有每只独一无二的属性，非常适合彩票玩法），以及更多的玩法结合。

结合我们已有的大量资源和合作伙伴，并且藉由在区块链领域的技术积累，以及区块链技术本身优势，我们有充足的信心，将 WinChain 逐步发展成为国际领先的区块链彩票技术服务商。区块链彩票技术必将逐步取代各国传统的彩票技术体系，成为新一代彩票底层技术的标准。

3.5.4 大数据运营

区块链彩票公开透明，玩法多样，数据全面，用户的售彩数据和各游戏的参与情况，各国各地的使用情况，WinChain 网络中各方都可以看到并且共享。WinChain 将联合各国相关团队，运用大数据和人工智能的手段进行大数据智能分析，通过数据更好地优化彩票运营方式和调整彩票玩法，以此进一步发挥区块链彩票的优越性。

3.5.5 公益

彩票与公益一直紧密相关，具有着社会责任的属性。传统公益的资金使用情况和公益项目落实情况一直并不足够透明和清晰。WinChain 将包含一个去中心化的公益资金使用平台，各国发行机构可以运用此系统将本国的公益彩票的资金使用情况通过区块链技术，更加公开透明的使用，真正做到财尽其责，物尽其用。

四、体系构成

4.1 WinChain 开源技术基金会简介

WinChain 基金会 WinChain Open Source Technology Foundation Ltd（“WinChain 开源技术基金会”）注册在新加坡。WinChain 开源技术基金会作为独立的法律主体，由资深彩票行业和区块链领域的专家组成，通过开发 WinChain 开源区块链彩票地层系统，与加入 WinChain 生态的各国公司共同努力，推动区块链这一技术在彩票行业的应用。

WinChain 系统由完整的基于公有链和联盟链的双链体系支撑的，包含售彩系统、数据存储系统、存证系统、开奖系统、奖金分发系统、智能合约系统和彩票开放游戏平台等完整的全彩票技术平台，通过区块链技术建立完全去中心化的彩票业态系统，将区块链的去中心化、无法篡改、系统稳健性强、智能合约公平性等特性代入彩票生态，与各国彩票系统供应商合作，帮助加入生态的各国公司基于 WinChain 的区块链彩票系统开发出适合各国应用的彩票底层服务，并推动开发者生态向彩票行业贡献力量。

WinChain 基金会将协调全球各国的行业资源，促进公开透明，安全稳定的区块链彩票底层技术早日被各国接受成为行业标准，使彩票行业实现区块链真正的应用落地，发挥区块链技术的真正价值。进而用区块链技术创造一个全新的彩票生态——这个生态将比过往人类社会所设想的所有可行方案协调得更好、更透明且更有效率。

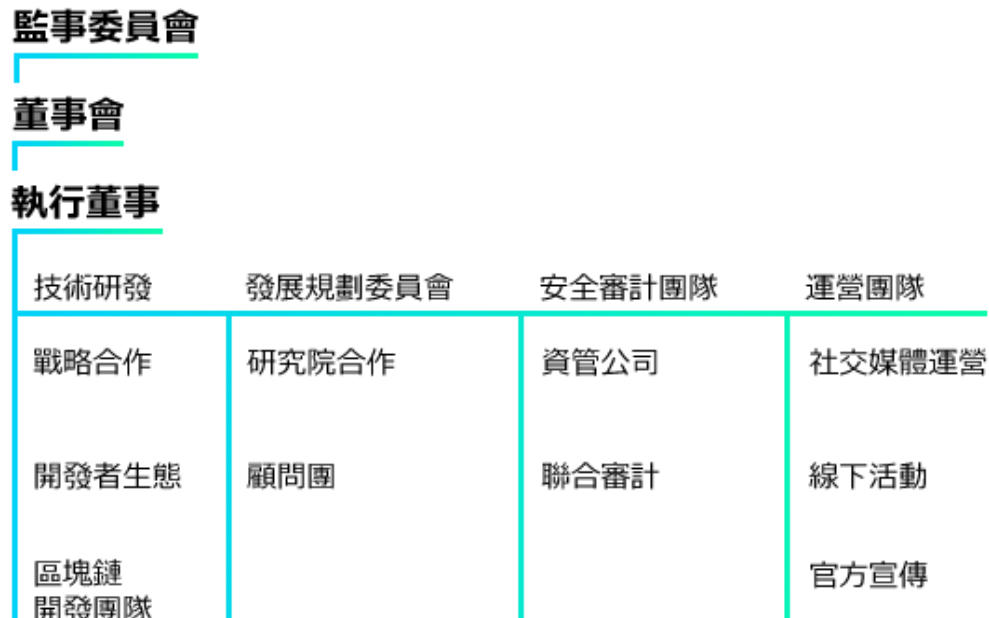


图 4-1 WinChain 开源技术基金会组织架构

WinChain 基金会短期目标:

- 2018 年 4 月份，WinChain 计划对接包括中国福彩、中国体彩和相关公司、部门、专业人士等组建区块链彩票研究院，以技术为先导，以应用为目的，进一步推动区块链技术在彩票行业的普遍认知和应用落地；
- 2018 年 8 月份，WinChain 将联合加入 WinChain 生态的莫桑比克彩票公司，落地首个国家级区块链彩票系统的应用，并发行全球第一张区块链彩票；
- 2018 年度 WinChain 将努力在 3-5 个国家与相关业务公司共同合作，落地区块链彩票系统的落地和运营，逐步将区块链彩票系统发展成为彩票行业的标准，为推动彩票行业的公平性、公正性和优化行业的系统效率、推动行业进一步发展进行更多努力和尝试。
- 2019 年度，WinChain 将完成 5-10 个国家的区块链彩票系统落地和运营，并与 WinChain 生态中的开发者、合作公司一起，完成 WinChain 区块链彩票游戏平台的搭建，向各国彩票部门提供丰富多样的新型彩票游戏玩法选择。进一步完善区块链彩票生态体系的建设。

4.2 WinChain 生态构成

WinChain 基金会

WinChain 基金会是一家注册在新加坡的非营利组织，基金会作为 WinChain 的主体和整体生态推进者，将致力于推动和监督整个 WinChain 生态健康快速的发展，协调全球各国的行业资源，促进公开透明，安全稳定的区块链彩票底层技术早日被各国接受成为行业标准，使彩票行业实现区块链真正的应用落地，发挥区块链技术的真正价值。

Victory Game Challenge

Base 在硅谷的 Victory Game Challenge 公司是 WinChain 的业务主体公司，由行业资深技术专家和业务专家组成，具有成熟的业务、丰富的行业开发经验和全球布局视野，面向全球提供新型区块链彩票底层技术服务。同时，在各国设有分支公司和机构，面向全球提供服务。WinChain 将依托硅谷公司的强大实力，开拓全球彩票技术服务市场，打造万亿规模的行业生态。

区块链彩票研究院

WinChain 将在业务各国联合所在国家相关部门，逐步合作成立区块链彩票研究院，共同针对不同国家的彩票行业特征，联合进行彩票行业与区块链相结合的研究和探讨，从而针对性的完善本国的业务特性和技术特性，与行业各方共同努力促成彩票行业向区块链公开透明公正的完美进化。

各国分公司和业务团队

WinChain 是一个底层区块链彩票系统，最终目的是符合各国目前的彩票发行技术体系，升级原有中心化应用系统，同时发展区块链彩票行业。目前 Victory Game Challenge 已在非洲莫桑比克建立分支机构，面向非洲国家提供国家级彩票业务整合，并取得该国唯一一个彩票运营资质，将于 18 年开始运营上线该国彩票。同时在包括安哥拉、东南亚等各国都在稳步推进中。

五、双链机制和发行方案

WinChain 团队拥有多年的彩票行业开发经验和行业经验，在服务彩票行业的过程中，深知中心化彩票的弊端，包括市场上假票、不出票等行为造成行业大量信任流失，收益流失；中心化售票过程中的作弊、不信任等问题；存证的可信度和开奖可信度等等。自 2017 年初 WinChain 团队开始逐步采用区块链技术应用于彩票行业，利用区块链技术去中心化、分布式存储、信息公开透明不可篡改等特性，进行对彩票技术体系的革新研究。在充分研究和验证过包括公有链、联盟链和私有链的方案后认为，公有链体系具有最佳的去中心化特性，但是对快速交易（如快速开奖类的彩票游戏）和手续费并不友好；联盟链在效率和费率上具有非常大的优势，但是均为机构节点，达不到完全的数据公开透明监督；私有链则很难具有相关区块链优势特性。

有鉴于此，团队最终通过实验和验证，选择了公有链+联盟链的双链模式，来进行业务支撑。公有链作为记账人选举机制的依托，利用公有链的开放特性，让更多的人参与联盟链的登记节点和记账，并给予一定的回报；联盟链作为应用的立足底层技术平台，WinChain 基于联盟链开发完整的去中心化区块链彩票底层业务平台，来支撑各国的彩票发行业务和相关技术支撑、周边生态支撑，从而完美的达到权益去中心化、记账去中心化、交易去中心化，同时在交易效率和手续费方面，通过联盟链达到最优解，支持瞬时、极低手续费的链上资产流转。

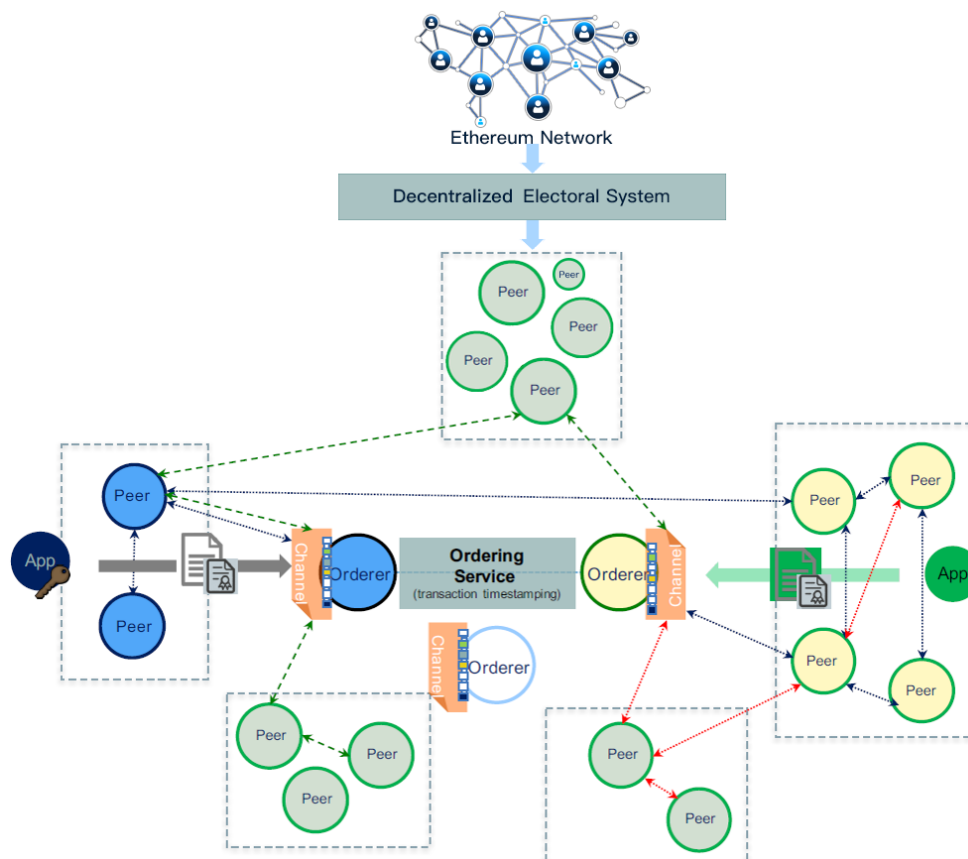


图 5-1 双链模式示意图

5.1 系统将发行两种通证

5.1.1 WinToken

WinToken 作为 Winchain 体系的准入凭证和系统分红激励凭证和记账节点选举凭证，将上线大型交易所流通交易。

准入凭证：WinChain 支持社会组织和政府组织自建彩票系统，接入 WinChain 彩票体系将需要向官方锁定并冻结一定数量的 WinToken，作为彩票运行的准入资质和奖池预留抵押。此部分 WinToken 同样参与整个系统的分红激励奖励。

去中心化投票权：

WinChain 独创的双链体系，是基于团队针对一年多来的区块链开发经历和研究，筛选大量方案后，兼具去中心化记账、权益共享和效率最大化的最终选取应用模式。通过公链的去中心化投票，选举出大量的分布式节点来进行联合账本的维护，确保 WinChain 体系的健壮和稳定。除各国政府机构和战略合作伙伴联合记账外，WinChain 网络采取选举记账人的方式，通过 WinElc 管理体系，即联盟节点以及其他社区领袖都可以通过选举成为 Lucky 的管理记账节点，通过记账增加 WinChain 系统的健壮度和完整性，保证去中心化体系的安全运转，并赚取一定的手续费。

另一方面，WinChain 是一个去中心化管理的社群，代币持有者享有对系统重大事项的参议权和投票权。按照持有 WinToken 的比例，社区成员可以对社区重大事项、游戏接入评价和选择、系统方案设定等，进行去中心化的投票和评论。WinChain 将提供去中心化投票和去中心化评论的功能，方便用户行使权力。

5.1.2 Lucky

WinChain 独创联盟记账结合以太坊记账的方式，除各国政府机构和战略合作伙伴联合记账外，WinChain 网络采取选举记账人的方式，通过 WinElc 管理体系成为系统的记账节点并享受记账手续费的激励。

作为有价值资产与区块链数字资产的超级兑付中心，由各国政府和相关部门负责联合审计及相关资产管理，恒定 1 Lucky=1 美元，通过为有价值资产在高效区块链网络上发行对应数字资产，提供兑换服务，帮助 WinChain 体系中的彩票购买和兑换更加灵活便利。

5.2 WinToken 的价值

5.2.1 联合记账的记账费收益

通过 WinChain 的 WinElc 系统，基金会将定期发起去中心化投票，进行公有链上联合记账节点的选举，选中的地址所有人将获得 WinChain 的联合记账权，并将联合运转 WinChain 的联盟链记账节点，参与应用系统的联合记账，并从中获得系统的所有交易记账费用的回报。随着 WinChain 在各国的应用普及，用户的增长，记账节点将获得非常优厚的记账费用回报；WinChain 基金会将定期发布联合记账节点的去中心化选举，并及时公布节点的详细信息，分配记账权限，进行数据同步，与社区成员一起保障和维护 WinChain 体系的公平性和健壮性。

5.2.2 系统空投奖励

通过 WinChain 的智能合约控制，WinChain 系统的智能合约会依照合约的固定程序，在系统的收益进入智能合约地址后，定期自动向 WinToken 的持有者，按照持有者的持有数量，将智能合约的代币自动空投到持有者的地址，从而达成一个系统自我激励的良性生态系统，WinToken 的持有者将通过 WinChain 智能合约自动获得系统收益的空投。

5.2.3 系统回购销毁

WinChain 基金会将每年度收益的一部分进行 WinToken 的回购，并打入黑洞地址。

5.2.4 直接应用于区块链彩票游戏

WinChain 双链系统，即能完美支持传统彩票应用接入区块链系统，完成链上彩票的整个生命流程，同时也支持完整的 WinToken 支撑的区块链彩票开发者生态，基于 WinChain 开发的智能合约区块链彩票系统，以及开发者生态的开发者开发的区块链彩票应用，都支持 WinToken 的持有者直接使用 WinToken 购买和交易彩票（在对应合规性的国家），我们坚信区块链彩票是整个彩票行业的未来，应用的拓展和实际需求将大大促进 WinToken 的价值。

5.2.5 开发者生态奖励

开发者生态是 WinChain 系统的重要组成部分，开发者通过基于 WinChain 系统的开放 API 开发的区块链彩票应用，需要向官方递交并冻结一定数量的 WinToken。不仅使开发者的成果有机会成为国家级的官方彩票应用，获得丰厚的开发和发行回报，更能促进 WinToken 和整个 WinChain 的通证的流通和规模化应用，这对 WinChain 生态的发展和价值提升，具有非常重大的意义。

5.3 代币发行方案：



图 5-2 WinChain 通证特点

5.3.1 WinToken

作为面向全球彩票市场的区块链底层系统，WinToken 通证总量为 210 亿枚，其中可对外兑换的额度为 105 亿枚（占比 50%）；另一部分持有的 105 亿枚（占比 50%）额度中，10% 作为团队预留奖励，20% 作为市场推广和战略合作预留，10% 将用于社区建设，10% 将用于开发者生态。



图 5-3 WinToken 分配饼状图

区块链市场鱼龙混杂，WinChain 拥有强大的团队以及丰富的行业资源，将携手加入 WinChain 生态的各国公司共同在多个国家落地国家级区块链彩票系统，根据 WinChain 逐步落地的三个关键节点，WinChain 将分开三个阶段进行通证兑换，每个阶段之间社区成员将看到 WinChain 在全球彩票市场取得重要的实质性进展，看到 WinChain 生态的实力和生态项目的落地应用，WinChain 的目标是在彩票行业这个最适合区块链技术的行业，打造整个区块链世界真正的第一个杀手级应用。

第一阶段：2018 年 2 月

关键节点：WinChain 生态合作公司获得莫桑比克国家区块链彩票运营牌照，团队已经开展了部分彩票系统的搭建工作。



图 5-4 莫桑比克国家彩票运营牌照

WinChain 正式启动首次通证兑换，将对外发放 15% 的通证，共 31.5 亿枚，募集不超过 2 万 ETH，面向对象为基石投资人和私募机构，资金将用于各国市场对接、系统开发、牌照合作、战略布局、社区奖励、人员支出、法务支出和意外性支出等；

第二阶段：约 2018 年 8 月

关键节点：联合成立亚洲区块链彩票研究院，推进区块链技术尤其是 WinChain 技术体系对彩票行业的优势认知和行业合作；发行世界上第一张国家级的区块链彩票。

第二次通证兑换活动将对外发放 15% 的通证，共 31.5 亿枚（至此共对外发放 30% 的通证），面向对象为私募机构和合格投资者。若募集期间：

- a) 募集额未达到 5 万 ETH 软顶，则募资失败，将退回第二阶段投资者的 ETH，并销毁所对应的 15% 的通证。
- b) 募集额达到 5 万 ETH 软顶，则募资成功。
- c) 募集额超出 5 万 ETH 软顶，则按照 $a*(b/c)$ 的数量给予投资者。（a 是第二阶段 WinToken 释放量即 15% 的 WinToken，b 是合格投资者投资的 ETH，c 是募集的 ETH 总额）

第三阶段：约 2019 年中旬

关键节点：WinChain 生态下合作的各国公司获得不少于 5 个国家的彩票运营和发行牌照，并以 WinChain 系统部署各国区块链彩票整体系统；WinChain 的开发者生态贡献的新型彩票游戏超过 50 个；基于 WinChain 系统的彩票销售发行等值超过年化 10 亿美元，为 WinChain 生态系统带来非常好的应用流通性。

第三次通证兑换活动将对外发行 20% 的通证，共 42 亿枚（至此共对外发放 50% 的通证，对外通证兑换结束），面向对象为合格投资者。若募集期间：

- a) 募集额未达到 10 万 ETH 软顶，则募资失败，将退回第三阶段投资者的 ETH，并销毁所对应的 20% 的通证。
- b) 募集额达到 10 万 ETH 软顶，则募资成功。
- c) 募集额超出 10 万 ETH 软顶，则按照 $a*(b/c)$ 的数量给予投资者。（a 是第三阶段 WinToken 释放量即 20% 的 WinToken，b 是合格投资者投资的 ETH，c 是募集的 ETH 总额）

5.3.2 Lucky

Lucky 基于联盟链网络，由各国政府机构和相关部门组织发行，用户在需要使用时通过相关交易场景直接购买即可。严格按存储资产 1 比 1 的比例在以太坊上发行对应数字资产，发行的数字资产继承了以太坊网络的特点，可以在 P2P、匿名、安全、去中心化的环境中自由交易。同时 Lucky 提供有价资产与发行的数字资产 1 比 1 的兑付服务，保证发行的数字货币的价值。

参考香港联系汇率制度，将法定货币美元作为准备金，严格按照准备金的数量，在以太坊网络按 1 比 1 的比例发行的加密数字货币 Lucky。即每增加 1 美元的准备金才允许在区块链中发行 1 个 Lucky。

同时用户也可以按同样的比例通过 Lucky 的兑付网关兑回美元，回收的 Lucky 将会被销毁，使得 Lucky 的价格将与美元的价格始终保持 1 比 1。

Lucky 特点：无需任何中介机构，由各国政府和相关部门进行联合审计和资金监管，公信力强，定期审计，信息公开透明。莫桑比克官方区块链彩票平台公司将以 Lucky 作为唯一彩票销售通证，并联合保障销售及奖金兑换的公开透明。

六、团队和顾问

6.1 团队成员

WinChain 团队由世界领先的彩票技术开发团队和区块链技术开发团队组成，在彩票系统大规模并发体系技术架构、区块链彩票行业应用、彩票游戏玩法和运营、各国彩票业务落地及运营、彩票行业业务理解和行业资源方面，具有强大的优势。目前已经在非洲和东南亚多个国家进行布局，18 年将在至少两个国家开展国家级的彩票系统接入和运营工作。团队的目标是将 WinChain 区块链彩票系统发展成为新一代互联网彩票系统的标准，覆盖更多的国家，使区块链技术在彩票行业大放异彩。



Charles Song 先生

WinChain团队成员，信息安全及人工智能、机器博弈专家。曾获得多项国内外大奖。曾创办信息安全公司服务于国内顶级企业用户数亿用户，2016年进入区块链行业，在区块链游戏领域和区块链彩票存证、安全溯源等领域拥有丰富成功项目经验。

Peter zhong 先生（硅谷）

Victory Game Challenge公司CEO

在美国硅谷大学获得计算机硕士学位，近20年的Linux开发经验，顶级技术专家。历任硅谷Linuxlab公司CEO、硅谷WebKomputing公司CTO，硅谷信息企业协会副会长等。



Forrest Nie 聂映平 先生

Victory Game Challenge公司CTO

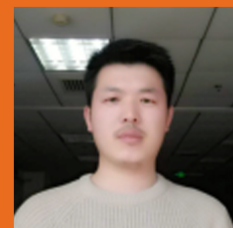
北京大学地球物理系学士学位，中科院硕士学位，前中体彩科技有限公司总工程师。中国体育彩票技术体系的核心构架者之一，中国彩票技术领域的领军人物。历任中科院软件研究所技术专家，东方国信项目经理等。

Bruce Jiang 先生

WinChain团队成员，大学商管专业回国后即创办社交平台，2013起先后从事社交平台、信贷平台、不良资产处置平台、互联网金融平台等运营工作，有5年的平台用户运营经验。

2017年在ugchain，从事运营工作。

2018年初，全职参与WinChain。





John 先生

WinChain团队成员，华创投资管理合伙人、董事、投委会委员，华创数字CEO。曾就职中信证券金石投资。超过20年的金融投资经验，在全球资产配置方面有丰富的实战经验，对美股、A股、港股、期权、期货、数字资产等领域有着多年独到的经验和理论体系。擅长市值管理、跨国并购、基金管理、资产交易等。管理及并购的资产超过400亿元。是国内较早进入区块链行业的关注者、实践者，投资了比特大陆、亦来云、比特币现金、Matrix等。

Emílio Jacinto 先生（莫桑比克）

WinChain团队成员，Emílio Jacinto先生为莫桑比克国家彩票中心的人事经理和总经理助理。负责WinChain在莫桑比克及非洲其他多个国家的商务合作对接。



金星 先生（英国伦敦）

WinChain团队成员，英国Power X有限公司，任职CTO，致力于区块链在能源交易的应用与研究。

Micheal lee 先生（硅谷）

WinChain团队成员，加州大学圣地亚哥分校-政治学学士、加州大学洛杉矶分校-会计师执照、牛津大学-比较法、圣克拉拉大学-法学博士。



Bob Lu 先生（澳大利亚悉尼）

WinChain团队成员，澳大利亚区块链初创公司TrustNote基金会国际市场总监，互联网老兵，拥有英国伯明翰大学EMBA，华中科技大学工学硕士等多个学位。

6.2 顾问与早期投资人



万币资本



天安资本



起源资本



丹华资本



南山资本
合伙人 何佳



源政投资
杨向阳



元禾母基金
合伙人 王吉鹏

6.3 行业顾问



世界彩票协会



亚太彩票协会



亚太博彩研究学会



中国彩票事业研究中心
副主任 陈海平



中国彩票行业沙龙
创始人 苏国京

6.4 拟合作单位



七、WinChain 路线图



图 7-1 WinChain 路线图

八、总结

彩票销量每年在全球持续增长，但彩票发行机构、运营商及服务商仍面临着各种各样的问题，特别是购彩者与发行人之间的信任，及透明、公平问题。全球彩票发行机构和运营商都致力于寻求公信力最大公约数的解决方案。区块链技术的去中心化、分布式记账模式可谓为彩票业应运而生，是传统彩票集中模式的颠覆者。全球彩票发行机构已经清楚地认识到，拥抱区块链是迟早之事。作为区块链彩票的先行者和实践者，WinChain 会与全球彩票从业者一起构建基于区块链技术的全新彩票解决方案。

九、法律事务和风险说明

9.1 WinChain 项目的法律结构

针对 WinChain 的项目，已成立一个位于新加坡的非盈利性的基金会 WinChain Foundation Limited（“WinChain 开源技术基金会”）。WinChain 开源技术基金会将作为独立的法律主体，全权负责组织团队来开发区块链彩票的平台和应用。但 WinChain 本身的运营和使用均完全取决并依赖于社区自治，WinChain 开源技术基金会只作为社区内一名普通成员，对 WinChain 的治理提出建议和方案，但不享有超然的或高出其他成员的权力。

WinChain 开源技术基金会通过定向及出售的方式，出售旨在 WinChain 平台上运行和使用的 Win Token，这些 Win 是用户为了使用 WinChain 的服务的付费手段和结算单位，一旦出售后就不会有任何人对 Win 承诺回购或回赎。Win 作为一种虚拟商品，不是证券，也不是投机性的投资工具。WinChain 基金会不保证 Win 的内在价值或存在任何回报。Win 不代表任何现实世界的资产或权利（例如 WinChain 开源技术基金会的股份、表决权等）。Win 的典型受众是对加密货币和区块链系统非常熟悉的专家们。

WinChain 开源技术基金会在 win 销售中所获的收入，将由 WinChain 开源技术基金会无条件的自由使用，主要将用于技术开发、市场营销、法律合规、财务审计、商务合作等用途。

WinChain 的彩票市场是建立在以太坊上的完全分布式的平台，全球任何人都能且只能通过消费 Win Token 来使用其功能，不受地理位置所限。WinChain 平台不具有物理实体存在，与任何国家或地区的地域和法币均没有任何关系。

9.2 免责声明

除本白皮书所明确载明的之外，WinChain 开源技术基金会不对 WinChain 或 win 作任何陈述或保证（尤其是对其适销性和特定功能）。任何人参与 win 的售卖计划及购买 win 的行为均基于其自己本身对 WinChain 和 win 的知识和本白皮书的信息。所有参与者将在 WinChain 项目启动之后按现状接受 win，无论其技术规格、参数、性能或功能等。WinChain 开源技术基金会在此明确不予承认和拒绝承担下述责任：

- 1) 任何人在购买 win 时违反了任何国家的反洗钱、反恐怖主义融资或其他监管要求；
- 2) 任何人在购买 win 时违反了本白皮书规定的任何陈述、保证、义务、承诺或其他要求，以及由此导致的无法付款或无法提取 win；
- 3) 由于任何原因 win 的售卖计划被放弃；
- 4) WinChain 的开发失败或被放弃，以及因此导致的无法交付 win；
- 5) WinChain 开发的推迟或延期，以及因此导致的无法达成事先披露的日程；
- 6) WinChain 源代码的错误、瑕疵、缺陷或其他问题；
- 7) WinChain 平台或以太坊区块链的故障、崩溃、瘫痪、回滚或硬分叉；
- 8) WinChain 或 win 未能实现任何特定功能或不适合任何特定用途；
- 9) 对售卖所募集的资金的使用；

- 10) 未能及时且完整的披露关于 WinChain 开发的信息;
- 11) 任何参与者泄露、丢失或损毁了数字加密货币或代币的钱包私钥 (尤其是其使用的 win 钱包的私钥);
- 12) win 的第三方众筹平台的违约、违规、侵权、崩溃、瘫痪、服务终止或暂停、欺诈、误操作、不当行为、失误、疏忽、破产、清算、解散或歇业;
- 13) 任何人与第三方众筹平台之间的约定内容与本白皮书内容存在差异、冲突或矛盾;
- 14) 任何人对 win 的交易或投机行为;
- 15) win 在任何交易所的上市或退市;
- 16) win 被任何政府、准政府机构、主管当局或公共机构归类为或视为是一种货币、证券、商业票据、流通票据、投资品或其他事物,以至于受到禁止、监管或法律限制;
- 17) 本白皮书披露的任何风险因素,以及与该等风险因素有关、因此导致或伴随发生的损害、损失、索赔、责任、惩罚、成本或其他负面影响。

9.3 风险声明

WinChain 开源技术基金会认为,在 WinChain 的开发、维护和运营过程中存在着无数风险,这其中很多都超出了 WinChain 基金会的控制。除本白皮书所述的其他内容外,每个 win 购买者还均应细读、理解并仔细考虑下述风险,每个 win 的购买者应特别注意这一事实:尽管 WinChain 开源技术基金会是在新加坡设立的,但 WinChain 和 win 均只存在于网络虚拟空间内,不具有任何有形存在,因此不属于或涉及任何特定国家。所有购买者已充分知晓并同意接受了下述风险。

1) 不充分的信息提供

截止到本白皮书发布日,WinChain 仍在开发阶段,其理念、共识机制、算法、代码和其他技术细节和参数可能经常且频繁地更新和变化。尽管本白皮书包含了 WinChain 最新的信息,其并不绝对完整,且仍会被 WinChain 开源技术基金会为了特定目的而不时进行调整和更新。WinChain 开源技术基金会无能力且无义务随时告知参与者 WinChain 开发中的每个细节(包括其进度和预期里程碑,无论是否推迟),因此并不必然会让购买者及时且充分地接触到 WinChain 开发中不时产生的信息。信息披露的不充分是不可避免且合乎清理的。

2) 监管措施

加密代币正在被或可能被各个不同国家的主管机关所监管。WinChain 基金会可能会不时收到来自于一个或多个主管机关的询问、通知、警告、命令或裁定,甚至可能被勒令暂停或终止 WinChain 开发的行动。WinChain 的开发、营销、宣传或其他方面因此可能受到严重影响、阻碍或被终结。由于监管政策随时可能变化,任何国家之中现有的对于 WinChain 的监管许可或容忍可能只是暂时的。在各个不同国家,win 可能随时被定义为虚拟商品、数字资产或甚至是证券或货币,因此在某些国家之中按当地监管要求,win 可能被禁止交易或持有。

3) 密码学

密码学正在不断演化，其无法保证任何时候绝对的安全性。密码学的进步（例如密码破解）或者技术进步（例如量子计算机的发明）可能给基于密码学的系统（包括 WinChain）带来危险。这可能导致任何人持有的 win 被盗、失窃、消失、毁灭或贬值。在合理范围内，WinChain 基金会将自我准备采取预防或补救措施，升级 WinChain 的底层协议以应对密码学的任何进步，以及在适当的情况下纳入新的合理安全措施。密码学和安全创新的未来是无法预见的，WinChain 开源技术基金会将尽力迎合密码学和安全领域的不断变化。

4) 开发失败或放弃

WinChain 仍在开发阶段，而非已准备就绪随时发布的成品。由于 WinChain 系统的技术复杂性，WinChain 开源技术基金会可能不时会面临无法预测和/或无法克服的困难。因此，WinChain 的开发可能会由于任何原因而任何时候失败或放弃（例如由于缺乏资金）。开发失败或放弃将导致 win 无法交付给本次售卖计划的任何购买者。

5) 资金的失窃

可能会有人企图盗窃 WinChain 基金所收到的资金（包括已转换成法币的部分）。该等盗窃或盗窃企图可能会影响 WinChain 开源技术基金会为 WinChain 开发提供资金的能力。尽管 WinChain 开源技术基金会将会采取最尖端的技术方案保护众筹资金的安全，某些网络盗窃仍很难被彻底阻止。

6) 源代码瑕疵

无人能保证 WinChain 的源代码完全无瑕疵。代码可能有某些瑕疵、错误、缺陷和漏洞，这可能使得用户无法使用特定功能，暴露用户的信息或产生其他问题。如果确有此类瑕疵，将损害 WinChain 的可用性、稳定性和/或安全性，并因此对 win 的价值造成负面影响。公开的源代码以透明为根本，以促进源自于社区的对代码的鉴定和问题解决。WinChain 开源技术基金会将与紧密 WinChain 社区紧密合作，今后持续改进、优化和完善 WinChain 的源代码。

7) 无准入许可、分布式且自治性的账本

在当代区块链项目中，有三种流行的分布式账本种类，即：无准入许可的账本、联盟型账本和私有账本。WinChain 底层的分布式账本是无准入许可的，这意味着它可被所有人自由访问和使用，而不受准入限制。尽管 WinChain 初始时是由 WinChain 开源技术基金会所开发，但它并非由 WinChain 开源技术基金会所有拥有、运营或控制。自发形成的 WinChain 社区是完全开放、无中心化且无准入门槛即可加入的，其由全球范围内的用户、粉丝、开发者、win 持有人和其他参与者组成，这些人大都与 WinChain 开源技术基金会无任何关系。就 WinChain 的维护、治理以及甚至是进化而言，该社区将是无中心化且自治的。而 WinChain 开源技术基金会仅仅是社区内与其他人地位平等的一个活跃成员而已，并无至高无上或专断性的权力，哪怕它之前曾对 WinChain 的诞生做出过努力和贡献。因此，WinChain 在发布之后，其如何治理乃至进化将并不受到 WinChain 开源技术基金会的支配。

8) 源代码升级

WinChain 的源代码是开源的且可能被 WinChain 社区任何成员不时升级、修正、修改或更改。任何人均无法预料或保证某项升级、修正、修改或更改的准确结果。因此，任何升级、修正、修改或更改可能导致无法预料或非预期的结果，从而对 WinChain 的运行或 win 的价值造成重大不利影响。

9) 安全弱点

WinChain 区块链基于开源软件并且是无准入许可的分布式账本。尽管 WinChain 开源技术基金会努力维护 WinChain 系统安全，任何人均有可能故意或无意地将弱点或缺陷带入 WinChain 的核心基础设施要素之中，对这些弱点或缺陷 WinChain 开源技术基金会无法通过其采用的安全措施预防或弥补。这可能最终导致参与者的 win 或其他数字代币丢失。

10) “分布式拒绝服务”攻击

以太坊设计为公开且无准入许可的账本。因此，以太坊可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使 WinChain 系统遭受负面影响、停滞或瘫痪，并因此导致在此之上的交易被延迟写入或记入以太坊区块链的区块之中，或甚至暂时无法执行。

11) 处理能力不足

WinChain 的快速发展将伴随着交易量的陡增及对处理能力的需求。若处理能力的需求超过以太坊区块链网络内届时节点所能提供的负载，则 WinChain 网络可能会瘫痪和/或停滞，且可能会产生诸如“双重花费”的欺诈或错误交易。在最坏情况下，任何人持有的 win 可能会丢失，以太坊区块链回滚或甚至硬分叉可能会被触发。这些事件的余波将损害 WinChain 的可使用性、稳定性和安全性以及 win 的价值。

12) 未经授权认领待售 win

任何通过解密或破解 win 购买者密码而获得购买者注册邮箱或注册账号访问权限的人士，将能够恶意获取 win 购买者所购买的待售 win。据此，购买者所购买的待售 win 可能会被错误发送至通过购买者注册邮箱或注册账号认领 win 的任何人士，而这种发送是不可撤销、不可逆转的。每一 win 购买者应当采取诸如以下的措施妥善维护其注册邮箱或注册账号的安全性：(i) 使用高安全性密码；(ii) 不打开或回复任何欺诈邮件；以及 (iii) 严格保密其机密或个人信息。

13) win 钱包私钥

获取 win 所必需的私钥丢失或毁损是不可逆转的。只有通过本地或在线 win 钱包拥有唯一的公钥和私钥才可以操控 win。每一购买者应当妥善保管其 win 钱包私钥。若 win 购买者的该等私钥丢失、遗失、泄露、毁损或被盗，WinChain 开源技术基金会或任何其他人士均无法帮助购买者获取或取回相关 win。

14) 普及度

win 的价值很大程度上取决于 WinChain 平台的普及度。WinChain 并不预期在发行后的很短时间内就广受欢迎、盛行或被普遍使用。在最坏情况下，WinChain 甚至可能被长期边缘化，仅吸引很小一批使用者。相比之下，很大一部 win 需求可能具有投机性质。缺乏用户可能导致 win 市场价格波动增大从而影响 WinChain 的长期发展。出现这种价格波动时，WinChain 开源技术基金会不会（也没有责任）稳定或影响 win 的市场价格。

15) 流动性

win 既不是任何个人、实体、中央银行或国家、超国家或准国家组织发行的货币，也没有任何硬资产或其他信用所支持。win 在市场上的流通和交易并不是 WinChain 开源技术基金会的职责或追求。win 的交易仅基于相关市场参与者对其价值达成的共识。任何人士均无义务从 win 持有者处兑换或购买任何 win，也没有任何人士能够在任何程度上保证任何时刻 win 的流通性或市场价格。win 持有者若要转让 win，该 win 持有者需寻找一名或多名有意按共同约定的价格购买的买家。该过程可能花费甚巨、耗时长并且最终可能并不成功。此外，可能没有加密货币交易所或其他市场上线 win 供公开交易。

16) 价格波动

若在公开市场上交易，加密货币通常价格波动剧烈。短期内价格震荡经常发生。该价格可能以比特币、以太币、美元或其他法币计价。这种价格波动可能由于市场力量（包括投机买卖）、监管政策变化、技术革新、交易所的可获得性以及其它客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在 win 交易的二级市场，WinChain 开源技术基金会对任何二级市场的 win 交易不承担责任。因此，WinChain 开源技术基金会没有义务稳定 win 的价格波动，且对此也并不关心。win 交易价格所涉风险需由 win 交易者自行承担。

17) 竞争

WinChain 的底层协议是基于开源电脑软件。没有任何人士主张对该源代码的版权或其他知识产权权利。因此，任何人均可合法拷贝、复制、重制、设计、修改、升级、改进、重新编码、重新编程或以其他方式利用 WinChain 的源代码和/或底层协议，以试图开发具有竞争性的协议、软件、系统、虚拟平台或虚拟机从而与 WinChain 竞争，或甚至赶超或取代 WinChain。WinChain 开源技术基金会对此无法控制。此外，已经存在并且还将会有许多竞争性的以区块链为基础的平台与 WinChain 产生竞争关系。WinChain 开源技术基金会在任何情况下均不可能消除、防止、限制或降低这种旨在与 WinChain 竞争或取代 WinChain 的竞争性努力。