



基于以太坊的智能合约 DAPP

白皮书



目 录 Contents

一、 前言摘要	4
二、 以太坊智能合约	5
三、 以太坊网络和智能合约的可靠性	6
分布式接口，稳定、可靠	6
分布式记帐	7
分布式传播	7
分布式存储	7
去中心化，可信任机制	8
强安全共识机制，无需第三方介入	9
信息不可篡改，交易安全	10
采用非对称性加密保障安全	10
四、 100LUCK——基于以太坊网络运行的智能合约 DAPP 特点	11
去中心化	11
数据加密、数据安全	11
代码开源，自动建立信任关系	12

数据无法篡改，自动运行	12
五、 100LUCK 玩法简介	12
六、 LOGO 寓意	13
七、 100LUCK 奖励机制	14
八、 稀有的全球支付货币——LUCKY	15
九、 应用生态：区块链支付和游戏	15
区块链+支付(更快捷)	15
区块链+游戏(更安全)	15
十、 100LUCK 的基本原则	16
十一、 100LUCK 的优势	16
十二、 100LUCK 与传统项目区别	16
十三、 开源智能合约应用 100LUCK	17
十四、 我们的团队	18
十五、 路线图	20
十六、 风险提示	20

一、前言摘要

区块链正在慢慢的改变这个世界，就好象智能手机爆发的那几年一样。随着越来越多的商业化的改造。区块链会越来越适应于各种商业场景，能够改变或颠覆越来越多的行业。而今天我们要聊的就是 DApp。

DApp 是 Decentralized Application 的缩写，译为：分散式的应用程序。App 我们都知道，我们在智能手机上安装的应用程序也就是 App。而 DApp 比 App 多了一个 ‘D’ ，‘D’ 的意思是分散式的。所以，它的意思是 分散式的应用程序/去中心化的应用程序。

DApp 是一种互联网应用程序，与传统的 App 最大的区别是：DApp 运行在去中心化的网络上，也就是区块链网络中。网络中不存在中心化的节点可以完整的控制 DApp。而 App 我们都知道，是中心化的。需要请求某台服务器来获取数据，处理数据等。



区块链相对于 DApp 来说是应用运行的底层环境。简单的可以类比为 IOS, Andorid 等手机操作系统于运行与之上的各种 App。如果我们把区块链理解为一个不可篡改的数据库，智能合约理解为和数据库打交道的程序，那就很容易理解 Dapp 了，一个 Dapp 不单单有智能合约，比如还需要有一个友好的用户界面和其他的东西。智能合约非常适合对信任、安全和持久性要求较高的应用场景，比如未来可以应用的场景有：游戏、数字货币支付、数字资产、投票、保险、金融应用、预测市场、产权所有权管理、物联网、点对点交易、去中心化自治组织等等。

区块链的诞生让互联网行业再一次腾飞，在未来具有无限的想象空间，区块链游戏和支付具有安全高效，去中心化，不可篡改，快速构建共识和信任，自动执行，节约成本，交易更准确，不受任何第三方机构的干扰等特点，得到了无数资本大鳄和极客团队的青睐，在未来成长空间巨大。而"100Luck"正是基于以太坊网络运行的一款高效，安全，自动化的 DAPP，它属于一款分红游戏。

二、以太坊智能合约

■ 以太坊是什么？

以太坊 (以太坊 Ethereum) 是一个建立在区块链技术之



上，去中心化应用平台。它允许任何人在平台中建立和使用通过区块链技术运行的去中心化应用。你可以把以太坊理解为一个 Android 系统，就是一个开发平台，在这个系统上可以加载各种应用。用户可以把以太坊当作“金融积木”来用，在这上面可以发行货币、定制金融衍生品，构建身份系统和去中心化组织也变得非常容易。因此，它也被称为区块链 2.0 版本。以太坊致力于减少复杂性和减少特性，成为一个通用的底层平台，在这上面可以创建各种各样的应用，它是开放的、去中心化的平台。

■ 智能合约是什么？

以太坊上的程序称之为智能合约，它是代码和数据(状态)的集合。智能合约可以理解为在区块链上可以自动执行的（由事件驱动的）、以代码形式编写的合同（特殊的交易）相比比特币，以太坊则更加完备（在计算机科学术语中，称它为是“图灵完备的”），让我们就像使用任何高级语言一样来编写几乎可以做任何事情的程序（智能合约）。

三、以太坊网络和智能合约的可靠性

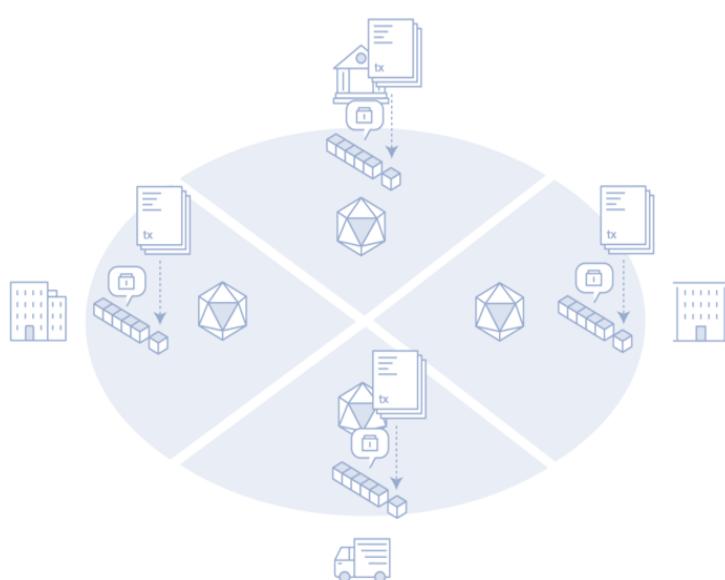
■ 分布式接口，稳定、可靠

以太坊底层区块链所采取的分布式结构，确保了数据、存储的安全性和可靠性。分布式结构，是指网络中各节点之间有多条通路。分布式结构没有固定的连接形式。从发信点到收信点的通路不止一条，通信时，由网络根据各节点的动态情况选择通信的实际路径。通信的控制功能分散在各节点上。它是最复杂的一种结构。它的通信控制也最复杂，对分散在各节点上的数据资源的管理也很复杂。由于节点间存在多条通路，当某些节点和链路发生故障时，仍有可能保证通信，所以有较高的可靠性。



■ 分布式记帐

以太坊采用分布式记账可以确保账本信息的安全性和真实性。在以太坊网络中，记录历史交易的信息被传递给了每一个节点，每个节点都可以拥有和存储一本完整、一致的交易总帐记录。即使个别的节点帐本被攻击，数据被篡改，也不会影响到全网的总账的安全性。



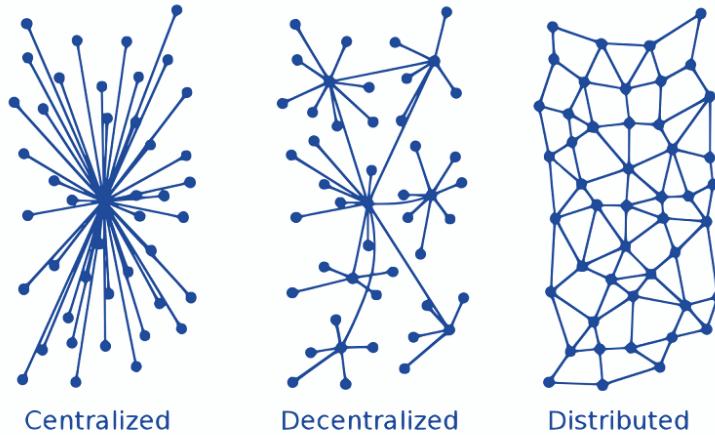
分布式帐本示意图

■ 分布式传播

全网的节点是通过底层网络协议点对点的方式连接起来的，没有单一的中心化服务器。消息通过 P2P 网络层协议，由单个节点直接发送给全网的其他所有节点。

■ 分布式存储

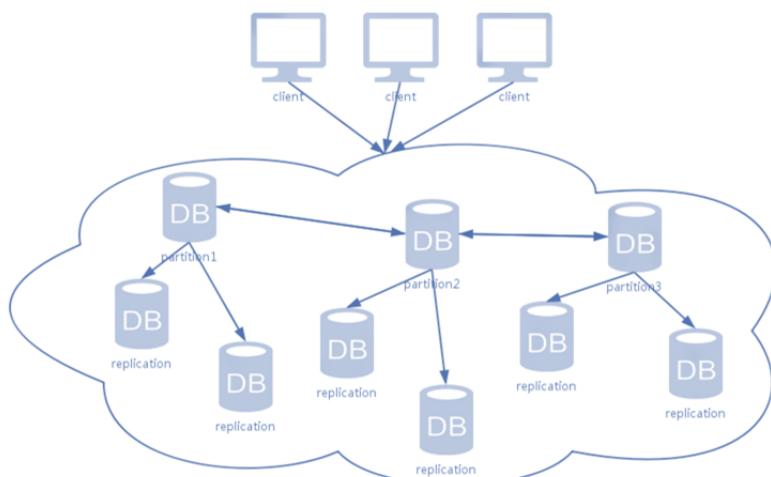
通过分布式传播后，所有数据均存储于各节点的电脑中，并且可以实时更新。相当于把帐本等数据实时共享于所有网络节点。实现了去中心化，有效的避免了单一节点被攻击造成的数据篡改。极大的提高了数据库的安全性。



■ 去中心化，可信任机制

以太坊底层区块链通过分布式的结构，实现了去中心化，智能合约技术，构建不以人为核心的可信任机制。不再需要中央服务器，每一台联网的计算机都是一个独立的个体，通过协议连接到其他成千上万的计算机，最终全球的计算机连接成为一个密密麻麻的网络，从某一节点上发出的信息，最终可以扩散到全球所有的节点。此结构的优势是即使其中一部分节点发生故障，也不会影响整个网络的通信。

这种链条式的传播机制，使得链条的每一个端点都成为信息的源头，而当因为其他外部原因导致区块链系统的某一个端点的信息发生变更时，不会影响整体数据的合法性。这种依赖于区块链内部智能合约机制、强共识机制建立的不以人为因素的影响的去中心化，可信任机制，十分有价值。





■ 强安全共识机制，无需第三方介入

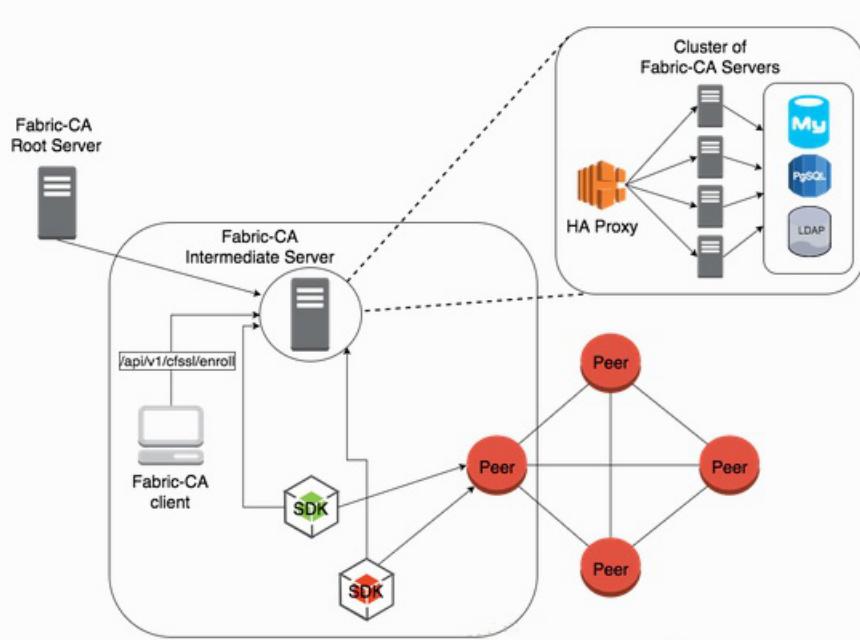
以太坊智能合约就是基于密码学技术的数字化合同，是一种计算机程序，而不是传统的纸质合同。智能合约是一段程序，它以计算机指令的方式实现了传统合约的自动化处理。简单讲，智能合约就是双方在区块链资产上交易时，触发执行的一段代码，这段代码就是智能合约。

智能合约有以下优势：

- (1) 将合约以数字化的形式写入区块链中，因区块链的特性，数据将无法删除、修改，整个过程透明可跟踪，保证了历史的可追溯性；
- (2) 因行为将被永久记录，可极大程度避免恶意行为对合约正常执行的干扰；
- (3) 去中心化，避免了中心化因素的影响，提高智能合约在成本效率方面的优势；
- (4) 当满足合约内容时，将自动启动智能合约的代码，既避免了手动过程，同时又保障了发行者无法违约；
- (5) 由区块链自带的共识算法构建出一套状态机系统，使得智能合约能够高效地运行。

■ 信息不可篡改，交易安全

以太坊底层区块链所采取的 Pow 共识机制，公链与私链之间的链接关系、共识机制，使得信息无法篡改，确保了区块链数据存储中的安全性。如果说共识是区块链的基础，那共识机制就是区块链的灵魂。共识机制，就是在一个时间段内对事物的前后顺序达成共识的一种算法。在区块链上，每个人都会有一份记录链上所有交易的账本，链上产生一笔新的交易时，每个人接收到这个信息的时间是不一样的，有些想要干坏事的人就有可能在这时发布一些错误的信息，这时就需要一个人把所有人接收到的信息进行验证，最后公布最正确的信息。



■ 采用非对称性加密保障安全

椭圆曲线加密法 (ECC) 是一种公钥加密技术，以椭圆曲线理论为基础，在创建密钥时可做到更快、更小，并且更有效。ECC 利用椭圆曲线等式的性质来产生密钥，而不是采用传统的方法利用大质数的积来 产生。椭圆曲线加密法 ECC (EllipticCurveCryptography) 是一种公钥加密技术，以椭圆曲线理论为基础，利用有限域上椭圆曲线的点构成的 Abel 群离散对数难解性，实现加密、解密和数字签名，将椭圆曲线中的加法运算与离散对数中的模乘运算相对应，就可以建立基于椭圆曲线的对应密码体制。椭圆曲线是由下列韦尔斯特拉斯

Weierstrass 方程所确定的平面曲线： $E:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$

椭圆曲线加密算法以其密钥长度小、安全性能高、整个数字签名耗时小，使其在智能终端应用中有很大的发展潜力，比如掌上电脑、移动手机等都能有更好的表现。而在网络中，ECC 算法也保证了其协同工作的实时性，使用 ECC 算法加密敏感性级别较高的数据（如密钥），速度上能够满足大数据量要求，而且安全性高，能很好地保障系统的安全。



四、100Luck——基于以太坊网络运行的智能合约 DAPP 特点 —■

■ 去中心化

100Luck 没有中心化数据库，应用程序全部开源，自主运行而不是由某个实体控制，所有的数据和记录都加密保存在公开且去中心化的区块链上。与传统应用不同的是，它没有实际控制人，由全球 91 个节点分布式运营管理，它们分布在美国，俄罗斯，中国，澳大利亚，法国，日本，英国等国家。

■ 数据加密、数据安全

100Luck 是基于以太网络运行的区块链系统，其采用的区块链技术中的分布式接口和智能合约技术，使得数据的安全性和可靠性加强。100Luck 基于以太网络开发，其采用了去中心化的技术，通过区块链的子区块、父区块的链条式关系，增加系统的安全性和数据可传递性。同时系统采用了多种加密算法，POW 共识机制、安全加密算法等，不仅仅通过区块链技

术本身提供的链式加密，还通过银行级用户数据加密，动态身份验证，多级风险识别控制，层层环扣，确保资金交易安全。

■ 代码开源，自动建立信任关系

100Luck 已有成熟的自我开源的自助合约机制，自动建立信任关系，信息安全和共识。

智能合约就是基于密码学技术的数字化合同，是一段程序，它以计算机指令的方式实现了传统合约的自动化处理。智能合约将以有数字化的形式写入区块链中，因区块链的特性，数据将无法删除、修改，整个过程透明可跟踪，保证了历史的可追溯性。100Luck 当前已构建成熟的，开源智能合约算法，能够快速系统移植到其他系统中，快速建立系统内部的信任关系，快速为系统服务。

■ 数据无法篡改，自动运行

100Luck 可自行定义区块链内部智能合约规则，则数据无法更改，系统自动运行，不需要人为的进行系统干预。智能合约的一大特点就是内部的程序规则定义好之后，则不能修改，100Luck 开源的合约机制使得，运行的智能合约系统。当源码的使用满足程序要求时，系统会自动运行，不需要手动进行系统指令的维护。

五、100Luck 玩法简介

100Luck，中文全称——“100 位幸运者”，独特创新的玩法让每一位玩家无后顾之忧，最后 100 名玩家将瓜分幸运池获得巨额回报，无需担心自己是最后一名，告别接盘侠。

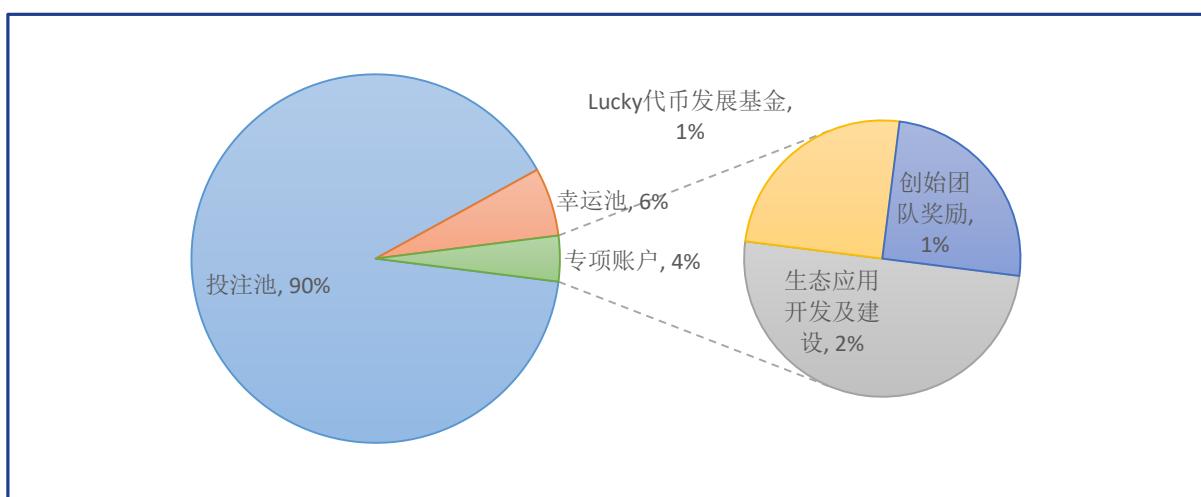
100Luck 基于以太坊网络运行的 DAPP 分红应用，采用智能合约技术，所有规则写死，无后台操作，无中央数据库，源代码完全公开，无法篡改，智能合约自动执行。

收益是从合约地址自动结算到自己的冷钱包地址，与中心化平台存在本质区别，不需要

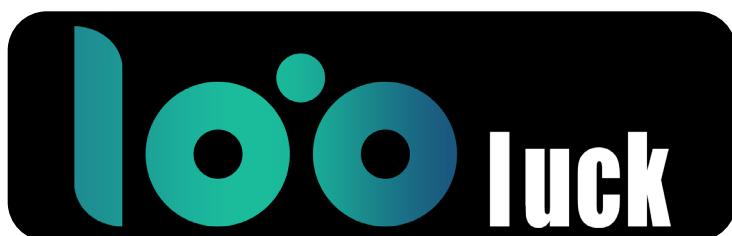
手动提现，等待审核时间等，欢迎技术大咖查验审核。

所有玩家入金的以太坊，为以下比例自动分配到以太坊智能合约地址：

投注金额的 90%进入投注池，用于奖金结算；投注金额的 6%进入幸运池，最后 100 位幸运者按投注以太坊比例瓜分幸运池；投注金额的 4%进入专项账户，其中 2%用于生态应用开发及建设，1%用于 Lucky 代币发展基金 1%用于创始团队奖励，应用每月收益的 80%反补进分红游戏。



六、LOGO 寓意



- ◆ 100Luck 的官方网址是 www.100Luck.org
- ◆ 100Luck——中文全称：100 位幸运者
- ◆ 100 代表最后一百位玩家，Luck 是幸运的意思，寓意为参与玩家“100%幸运”，在 100Luck 的最后 100 位玩家将瓜分幸运池获得巨额回报。

七、100Luck 奖励机制

◆ 级别与收益

A1: 1-5 以太坊 日分红 0.5%

A2: 6-10 以太坊 日分红 1%

A3: 11-50 以太坊 日分红 1.2%，合约自动开放



◆ 动态奖励

A1: 一代 50% 二代 20% 三代 10% (有烧伤)

A2: 一代 100% 二代 70% 三代 50% 4 到 10

代 10% 11-20 到无限代 5% 21 代以上每日分红 1% (有烧伤)

A3: 一代 100% 二代 70% 三代 50% 4 到 10 代 10% 11-20 到无限代 5% 21 代以上每日分红 2% (无烧伤) (合约自动开放)

◆ 级别收益表

级别	投资	日分红	1代	2代	3代	4-10代	11-20代	无限代直推2名	烧伤
A1	1-5	0.5%	50%	20%	10%	-	-	-	有
A2	6-10	1%	100%	70%	50%	10%	5%	1%	有
A3	11-50	1.2%	100%	70%	50%	10%	5%	1%	无

备注：正式上线，游戏完成 6 轮后，智能合约自动开启 A3 级别。自动重启机制，运行过程中一旦出现资金池为 0，所有账户归零并重新洗牌，保留推荐关系，智能合约自动瓜分幸运池给最后 100 名用户，开启新一轮游戏。

八、稀有的全球支付货币——Lucky

代币名称：Lucky

Lucky 基于以太坊网络运行，数量稀有，价值珍贵，总量 100 万枚，10% 团队拥有，10% 用于基金，80% 的币通过 100Luck Dapp 空投给玩家，智能合约将根据链上投注记录自动空投 Lucky 给所有 100Luck 玩家，我们将做真正有价值的加密数字货币，拒绝空气币，随着 100Lucky 陆续上线全球主流交易所以及生态的不断壮大，Lucky 有着巨大的升值空间。

九、应用生态：区块链支付和游戏

■ 区块链+支付(更快捷)

众所周知，现在全球支付每年有数千万亿的成交额，跨国转账大多都是通过西联银行，周期长，费用高，从我们日常跨国旅游的衣、食、住、行、医疗就能感受到跨国支付的极其不便利性。目前缺乏一款真正的跨国支付的全球货币，基于区块链技术的 Lucky 为全球支付而生，采用区块链技术，在支付过程中具有安全，快速，便捷，费用低等特点。我们将会从分红游戏开始，发行 Lucky 代币，Lucky 代币数量非常有限，未来升值空间巨大，玩家可以作为支付货币使用，也可收藏纪念。未来以 Lucky 代币为支付基础货币开发一系列基于区块链技术的公开，公平，公正的智能合约应用会陆续推出，敬请期待。

■ 区块链+游戏(更安全)

而互联网游戏业也是一块巨大的蛋糕，是刚需市场，也是很快将被区块链技术颠覆的领域。我们希望通过此游戏招募第一批投资玩家，一方面通过游戏形式募集链上支付和链上游戏应用的开发经费，另一方面招募大量玩家参与游戏，赚取分红收益和推广收益，形成玩家大数据，并通过智能合约按照贡献大小将收益空投给所有玩家，为链上支付和链上游戏应用做好市场准备。



十、100Luck 的基本原则

- ◆ 公平(区块链技术)
- ◆ 公正(DAPP 智能合约)
- ◆ 公开(开源代码)
- ◆ 公认(主流钱包比如 imtoken，主流币以太坊)

十一、100Luck 的优势

“100Luck”采用区块链技术，无操盘手、无服务器、无中央账户，是全球首款以太坊区块链官网唯一认证并通过：“开源智能合约”，所有源代码已封装以太坊公链里，任何人无法篡改代码、篡改制度、动用合约里以太坊资产。“100Luck”在以太坊公链里，按智能合约约定，自动结算，自动运行，自动到账，永不关网！

十二、100Luck 与传统项目区别

传统项目

第一：有中心化账户、项目方包装、制度规则随时改变，人为控制，人心难测，圈钱跑路等。

第二：有中心化 APP 和服务器数据库，随时人为关闭或停止运营，无法知悉资金动向等。

第三：注册会员（要实名认证、手机号、邮箱、身份信息、网体图、人民币经流……数据证据链有法律和金融等风险）。

十三、开源智能合约应用 100Luck

第一：币本位以太坊投入、分红也是以太坊、不转换任何币种。

第二：采用以太坊公链技术， DAPP 智能合约， 完全去中心化，开源代码可公开查验，欢迎全球的技术大咖审核，测验和论证。

第三：所有制度和规则，分红结算方式，全部写入开源程序，并且无法再更改，智能合约自动执行（无法人为更改后台和制度等所有数据）。无人可以动用合约地址的以太坊资产。

第四：没有政策，法律，金融，平台跑路等危险，全球公认的冷钱包保护你的资产。

第五：自动识别去中心化冷钱包地址（imtoken，麦子钱包等）、DAPP 区块链浏览器直接进入。

第六：无须实名注册、无须身份认证、每日分红自动结算到账，无手续费，无特定提现时间，与中心化账户存在本质的区别。



团队

十四、我们的团队

我们团队来自全球各地，目前团队一共 38 人，来自俄罗斯，美国，澳大利亚，中国，日本，韩国。发起人来自俄罗斯，以太坊社区的早期核心成员之一，我们拥有共同的爱好和目标，我们坚信区块链智能合约将会给互联网带来一场根本的革命，我们都是区块链技术应用专家，希望开发更多更好的区块链应用，改变世界。



Анатолий 团队发起人

英文名：Dempsey 1981 年出生，俄罗斯人，硕士研究生，毕业于莫斯科国立大学，主修计算机。技术大牛，拥有 9 年区块链开发经验，对于区块链的创新和应用有着独特的见解，有基于区块链技术搭建完整的技术解决方案。



Channing 100 Luck 联合创始人

1989 年出生，出生于加拿大，美国国籍，硕士研究生，毕业于北卡罗来纳州立大学，主修经济学、会计、金融和计算机科学。海外知名投资公司经理，拥有三年区块链投资经历，并在美国拥有自己的理财公司。精通金融理财和中文。



Cleveland

1989 年出生，出生于加拿大，美国国籍，硕士研究生，毕业于北卡罗来纳州立大学，主修经济学、会计、金融和计算机科学。海外知名投资公司经理，拥有三年区块链投资经历，并在美国拥有自己的理财公司。精通金融理财和中文。



Larry

澳大利亚人，本科，主修市场营销和计算机科学与应用，毕业于澳洲悉尼大学。拥有十年计算机软件开发和应用工作经历和三年区块链投资经历。精通计算机编程和消费者心理学。



Elvis

1987 年出生，美国人，博士研究生，毕业于北卡罗来纳州立大学，主修计算机。拥有多年系统研发和设计工作经历，五年区块链投资经历，在美国拥有自己的计算机软件设计和开发公司。精通计算机编程和软件开发。

十五、路线图



十六、风险提示

参与本次 "100Luck" 投资之前，投资人必须认真阅读项目白皮书。除非投资人理解项目白皮书中的所有内容、项目愿景以及可能失败的风险，否则不应该参与 "100Luck"。

参与公开发售请做好项目调研，谨慎参与。投资人同意，能够或者不能够使用本平台由投资人自己承担风险，且不追究 "100Luck" 理事会的责任。

投资之后，"100Luck" 将通过智能合约发送给投资人，但不附带任何形式的保证，无论是明确表达或暗示的，包括且不限于所有暗示可销售的保证，对特定目的的契合等。由于某些司法区不允许不包含暗示性保证，上述不包含暗示性保证的表述可能不适合你。

"100Luck" 不代表任何形式或有法律约束力的投资品。鉴于不可预知的情况，虽然团队会尽力实现白皮书的所有目标，所有购买 "100Luck" 的个人或团体将自担风险。拥有 "100Luck" 以下代表你有权消耗以下以使用平台上的所有产品或服务。