全球区块链应用的底层价值锚

财富链

FORTUNE CHAIN

白皮书

【项目概要】

财富链，首先解决传统珠宝古玩产业中防伪防赝品的痛点，以及实物珠宝古玩持有人变现和再变现的刚需。在这一基础上，解决区块链项目通证发行的三大难点，包括通证发行依据、发行总量依据和价格生成机制等问题。通过科学严谨的实体经济数据支撑，和丰富的通证经济系统应用，力图让金银珠宝这一先天性的去中心化价值载体与区块链的去中心化共识机制相融合，形成围绕财富链珍藏宝通证（TITT）的应用生态体系。同时，在技术上通过实物珠宝古玩上链，有向无环图（DAG），以及“抗量子加密”的抗量子技术等前沿科技成果，让财富链珍藏宝通证（TITT）这一具备价值公信力的加密数字资产成为全球区块链代币发行的底层价值锚。

目 录

1. 前言

区块链经济的发展方兴未艾。

自 2009 年比特币诞生以来，区块链经济以其巨大的革命性组织形式和价值流转优势席卷全球。到目前为止，以比特币为代表的区块链 1.0，以太坊为代表的区块链 2.0，EOS 为代表的区块链 3.0 已经广为人知，而区块链 4.0 的突破也正在成为全球瞩目的焦点。对于区块链 4.0，如何落地应用到实体经济，正在成为全球瞩目的焦点。各国监管当局都也在密切关注区块链应用的发展。

财富链（Fortune Chain，下文简称 FC）致力于解决区块链通证生态系统在实体经济的应用问题，本项目抓住区块链经济价值互联网中“价值”问题的根源，以先天性去中心化并携带共识价值的金银珠宝以及文物古董品类为突破口，试图解决通证经济系统设计的底层价值锚问题。在这一基础上，利用区块链+人工智能技术，解决实体经济产业中珠宝古玩变现和再变现的难点和痛点，构建以珠宝古玩财富传承为主体的公有链应用价值生态体系。

财富链通过创新的 DAG 底层技术和通证身份化+超级节点机制，在技术上实现可广泛应用的智能合约功能。通过区块链+人工智能的光机电一体化设备进行身份认证，让珠宝古玩实物信息上链转化为数字资产。通过珍藏宝（Treasure In Treasure Token，下文简称 TITT）通证价格和珠宝古玩实物价值相分离的设计，解决 token 通证和实体经济的价值信任和价值映射问题。通过代码开源和“矿机”设备开源，建立完全去中心化的自组织治理机制。通过资产通证化，构建普及到各行各业广泛落地的通证经济应用场景。真正让区块链技术服务实体经济消费升级和居民财富保值增值的价值兑现，惠及人群。

毋庸置疑，区块链技术将重塑下一代互联网。财富链希望利用区块链+人工智能技术建设一个基于珍藏宝（TITT）通证的经济金融生态，来帮助任何需要建立交互信任的组织，低成

本，高效率，安全搭建区块链应用的底层技术管理架构。不但充分发挥 token 通证的金钱激励功能，而且发挥 token 通证在效果激励、口碑激励、信用激励、权益激励等方面多样化的激励功能。在生态中，用户可以将其认为有价值的资产锚定珍藏宝（TITT）通证的价值，使用智能合约进行交易，开放式存储，无障碍流通，实现价值流转和价值兑现。财富链珍藏宝（TITT）通证经济系统，是一个具有实体经济公信力的商业价值流转体系。

未来，财富链生态体系将以珠宝古玩的财富传承为主体，广泛延伸到游戏、工业、农业、美容、商超、智慧城市、社会治理、健康养老、软件产业、广告产业等各类产业的区块链生态应用。珍藏宝（TITT）通证也将成为全球经济价值流转的润滑剂，让世界体会到区块链经济作为价值互联网的真正价值。

2、 项目背景

2.1 区块链的发展历史

2008 年末，中本聪发表了一篇名为《比特币：一种点对点的电子现金系统》的论文，文中首次提到“blockchain”这个概念。简单说就是对区块形式的数据进行哈希加密并以时间戳来排序。通过将这一加密信息广播全网，使其公开透明且不可篡改，有效的解决了电子现金的安全问题。此后，随着第一批比特币被挖出来并迅速在全球范围内流通，区块链开启了 1.0 时代。

随着比特币的广泛流通，其算法的严谨性和匿名性得到了经济社会对比特币价值传递功能的认可。但比特币本身扩展性不足和底层技术对广泛应用的局限性，也成为公众关注的焦点。

因此，很快就出现了以以太坊、瑞波币为代表的新一代“可编程金融”系统，其智能合约对金融领域的使用场景进行梳理，优化了自动化执行和 token 通证的便捷生成机制，又掀起了区块链 2.0 革命的浪潮。

但是，比特币、以太坊以“区块+链式”结构的区块链底层技术，只能达到每秒 70-80TPS，和传统互联网上百万 TPS 的处理能力相比，明显无法满足人们对区块链技术普及性应用的需要。而区块链经济的蓬勃发展和实体经济低迷不振的巨大落差，让人们也更希望区块链技术能拓展到金融领域之外。在理论方面，把传统互联网定义为信息互联网，区块链定义为价值互联网，已经是普遍共识。这也更增强了人们对区块链技术落地于实体经济应用的的期待。

2018 年中，随着 EOS 的主网上线，区块链 3.0 引发的 DAPP 生态应用正在不断深化区块链应用的技术共识。但由于代币价值缺乏基础的实体经济逻辑支撑，导致 DAPP 生态只能围绕游戏、博彩等虚拟产业伪应用。区块链的“无币”应用成为了主流社会默认的形式，区块链技术沦为中心化机构一种工具的思维甚嚣尘上。

2019 年，区块链通证经济生态的落地应用已经成为亟需突破的焦点。以区块链思维为导向，有向无环图（DAG）底层技术、+人工智能、通证经济系统设计、IBO 等围绕区块链通证有效应用的新思潮和技术体系不断涌现。可以预见，区块链 4.0 远不止一个链一个币的应用，必将是由生态体系构成的多元生态组织，其价值远超虚拟货币、代币支付和金融这些领域，它将重塑人类社会的方方面面。

这是一场影响波及全球的革命，其标签是去中心化、价值、共识机制等改变生产关系和价值认知的革命。财富链也将拥抱这场革命，致力于成为区块链 4.0 的代表，致力于成为区块链经济时代通证经济生态价值锚定的基础公链，为区块链的广泛应用提供“可编程社会”的解决方案。

2.2 公有链目前面临的问题

自从 2009 年比特币代码开源以来，区块链经济的发展催生了大量的区块链项目。但总体上看，无论是公有链、联盟链、私有链均面临较大的应用瓶颈。其中，公有链是底层技术的基础，其技术突破和落地应用模式决定着区块链经济的走向。目前的局限性和主要问题如下：

1）区块+链式结构，不仅严重制约链上数据的吞吐量，而且缺乏实体经济扩展性和兼容性。

2）主流共识机制更多考虑了技术实现的便捷性，没有考虑实体经济区块链应用的多样性。而且巨大的能源消耗和算力劫持，也把海量普通用户挡在门外，导致生态系统只是单一的炒币功能，生态应用与生态流量绝缘。

3）现有区块链系统具有很大的封闭性，缺乏与现实世界有效交互的入口。

4）焦点集中于技术的升级，而不是解决实体经济刚需，以及吸引普通百姓广泛的参与和高频的使用。

5）代币生成机制缺乏依据，欠缺实体经济逻辑支撑。

6）代币发行总量缺乏依据，大多数参照比特币“总量恒定，永不增发”，但却缺乏严谨的数学论证，导致发行数量如同儿戏，没有公信力。

7）代币定价机制缺乏数据支持，因为没有可信的共识价值锚定，导致定价不够科学严谨，价格容易被任意操纵。

8）代币激励机制单一，忽略了应用于实体经济的激励弹性。实体经济不仅仅需要金钱激励，更需要高效可信的效果激励、信用激励、权益激励等多种形式。

财富链致力于解决上述问题，通过底层技术的突破和生态系统的建设，引导实体经济线下流量转化为有效的线上生态流量，让去中心化的价值共识成为具有实体经济公信力的生态共识，让财富链成为区块链 4.0 时代落地应用的最佳载体。

2.3 价值互联网中“价值”问题的根源

区块链作为价值互联网，其“价值”的内涵和根源，不但是建立公信力的关键，更是区块链落地应用过程中价值流转的依据。

毋庸置疑，“价值”二字的内涵，首先就是金钱价值，或者叫货币价值。

中本聪在 2008 年将区块链加密资产定义为“比特币”。这就是一个货币的概念，所以叫做虚拟货币。但是，货币的价值根源又在哪里呢？

从世界货币史上，我们知道几千年来，金银一直是货币的价值载体。直到近代，金本位才让步于国家央行的“信用本位”，时间不过百年而已。从金本位到信用本位为成熟标志的布雷顿森林体系，建立在信用本位基础上的信用货币才正式走上前台。然而即使如此，布雷顿森林体系也是明确规定美元锚定黄金，其他主权货币都要锚定美元的。也就是说，金银才是货币的根。

1969 年，美国总统尼克松悍然摧毁布雷顿森林体系，放弃美元锚定黄金。之后，作为中心化的国家央行系统滥发纸币变得更加肆无忌惮，任意发行钞票掠夺人民的财富。2008 年，美联储在全球金融危机的压力下实施量化宽松，缺乏制约的信用货币再次极大地损害了人们对中心化信用发行机制的信心。最终在这一大背景下，中本聪推出了完全去中心化的虚拟货币比特币。

追根究底，信用货币滥发的根源在于解除了纸币对黄金的价值锚定。因此，虚拟货币如果缺乏价值锚定，新的“滥发”也必然难以取得人们的价值信任。不过，现代经济的发展，复杂的金融经济活动，也不可能再次回到“金本位”时代。但价值锚定还是必须的，只有可信的价值锚定，才是虚拟货币公信力的根源。

值得注意的是，比特币解决了去中心化的共识机制问题，但却没能解决价值锚定问题。而

且其依靠算力挖矿的代币生成机制，和实体经济实物价值也没有建立有效联系，因此，其终将无法解决价值锚定问题。

财富链立足实体经济的区块链应用，从更广义的角度定义价值互联网中的价值问题。摒弃与实体经济人群联系较少的锚定黄金思路，而扩展为所有收藏级的金银珠宝和文物古董艺术品。让稀缺性财富储值标的先天性去中心化优势与区块链的去中心化机制相结合，既扩大了实体经济受众人群，又解决了价值锚定的价值公信力问题。

2.4 先天性去中心化对区块链应用的意义

稀缺性财富储值标的先天性去中心化特点，是人类社会几千年来的普遍共识。无论是哪个时代，哪个国家，哪个民族，哪种肤色，哪种语言，对金银珠宝古玩价值的肯定是一致的。

在全球珠宝古玩产业中，过去虽然有“西钻东玉”的特征，但随着全球化的发展，这一特征已经越来越模糊。可以说，任何收藏级的珠宝古玩在全球各地都已经具备了广泛的需求，其本身所蕴藏的价值已经被各国人群所肯定。

去中心化的信任，是珠宝古玩价值流通和价值传递的根本，也是珠宝价值储藏，价值信任的基石。假如没有去中心化的价值共识，金银珠宝的价值流转和财富传承也必然是不成立的。

表 2-1 财富链（FC）允许上链的珠宝古玩品类

品类	具体种类
贵金属	黄金、白银、铂金、钯金等。
天然宝石	金刚石、萤石、红宝石、蓝宝石、赤铁矿、水晶、尖晶石、猫眼、黄宝石、绿宝石、祖母绿、碧玺、蛋白石、紫晶金矿石、石英等。
天然玉石	玛瑙、碧玉、灵璧玉、和田玉、岫岩玉、南阳玉、翡翠、蓝田玉、孔雀石、绿松石、东陵玉、准格尔玉、夜光玉、青金石、金黄玉、冰花玉等。
天然彩石	寿山石、田黄石、青田石、鸡血石、五花石、长白石、端石、洮石、松花石、雨花石、巴林石、贺兰石、菊花石、紫云石、燕子石、红丝石、昌化石、蛇纹石、上水石等。
天然有机宝石	琥珀、珍珠、珊瑚等。
金属器	金银器、铜器等。
陶瓷	青花、斗彩、釉里红、粉彩、新彩、颜色釉、唐三彩、玲珑瓷、紫砂壶等。
杂项	竹、木、牙、角、文房四宝、漆器、绣品、佛像、鎏金、手串、核桃等。

书画	（暂缓上链认证）
备注	必须具备国家级以上鉴定机构出具的鉴定证书（这是上链的必要条件）

区块链，也有去中心化建立信任的特征。区块链代币和 token 通证，也是去中心化建立信任，传递价值的。先天性去中心化的珠宝古玩（如表 2-1 所示）和区块链结合起来，也必将以价值信任和价值流转为纽带，形成基于实体经济大数据的价值锚。

区块链通证的落地应用，首先就要解决的是 token 通证的价值信任问题。如果没有可信的价值共识，通证经济系统的价值流转必然受到质疑。因此，金银珠宝古玩先天性的去中心化价值信任对区块链通证落地应用具有重大意义。

财富链就是将金银珠宝古玩先天性的去中心化价值信任，与区块链去中心化的共识机制完美融合，珍藏宝（TITT）通证的价值和金银珠宝的实物价值完美映射。通过珠宝古玩实物的数字化，通证化，个性化，既保留了珠宝古玩的收藏价值，又增加了珠宝古玩流通变现的增值潜力，更进一步形成了针对虚拟经济价值流转具有实体经济大数据支撑的，具有强大公信力的底层价值锚定。

2.5 区块链+人工智能是区块链经济发展的必然趋势

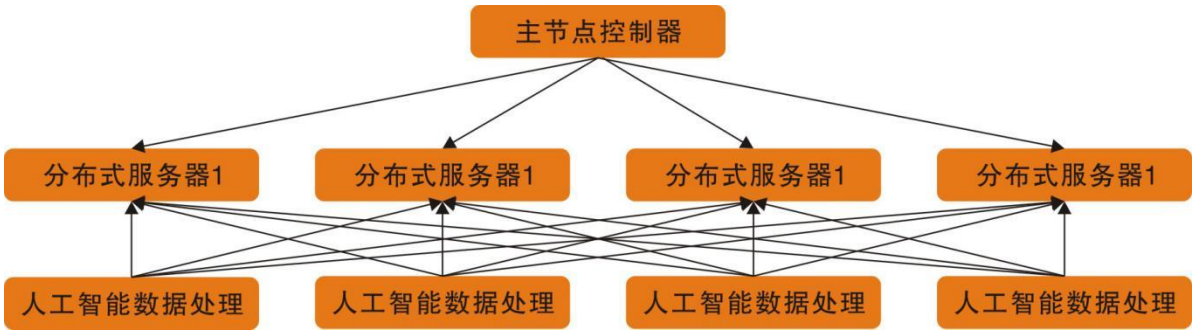
区块链通证经济系统要落地应用，就必须要和实体经济紧密结合。要实现和实体经济大数据的无缝对接，人工智能是有效的科技手段之一。只有分布式人工智能，才能抓住实体经济刚需，解决实体经济痛点，把区块链应用落地到千家万户，落实到大众人群。

人工智能的基础是大数据，特点是大容量、无结构、碎片化、多样性。区块链和人工智能相结合，可以为大数据建立真数，解构信任机器。同时，区块链+人工智能，也是一种分布式的自治组织。

区块链 token 通证应用，也必须要把算法共识这种机器之间的确定性共识，加入人的因素，升级成为具备复杂社会属性的不确定性共识。由消耗能源的机械“矿工”，升级到紧密结合实

体经济刚需的智能“矿工”。

只有区块链+人工智能，通过智能上链，解决实体经济痛点，才能为通证经济系统提供除了炒币之外的实体经济价值回报。只有这种建立在实体经济刚需基础上的价值回报，才是通证经济系统价值流转源源不竭的生命力。



财富链通过光机电一体化的硬件设备，将珠宝古玩实物信息转化为数据信息并提取 token，就是通过区块链+人工智能，深度切合实体经济产业链，构建分布式人工智能的落地应用。利用遍布全球各地的智能设备和智能“矿工”，建立可信的价值流转大数据。为各行各业的区块链应用提供代币发行的底层价值锚。

3. 财富链（FC）概述

3.1 什么是财富链

财富链是基于区块链+人工智能技术，将珠宝古玩实物资产进行数字化，通过智能身份认证和分布式网络进行登记，并加密提取哈希值生成 token 通证进行发行、转让、交易、清算、交割等线上线下相结合的去中心化网络协议。

财富链以区块链 token 通证的落地应用为导向，以解决实物珠宝古玩变现和再变现为价值挖掘和价值流转的切入点。以解决市场刚需和行业痛点为基础，通过区块链和人工智能的技术整合，首先解决珠宝古玩的防伪和赝品问题，上链后的数据信息不可篡改。在这个基础上，结

合智能合约和通证经济系统的构建，让区块链 token 通证的应用落地实体经济场景，创造生态网络体系之外的增量价值。

财富链发行珍藏宝（TITT）通证数字资产，以珠宝古玩的先天性去中心化特点为依托，以通证身份化+超级节点机制聚焦价值公信力。不但在生态体系内构建通证的流通价值，而且具备充要条件成为全球区块链经济代币发行的底层价值“锚定币”。

3.2 财富链如何解决行业痛点和区块链应用的问题

财富链（FC）通过有向无环图（DAG）底层技术，为实物珠宝古玩大数据进行加密认证，分布式存储，实现高 TPS，异步共识，IOT 物联网设备兼容性，以及可广泛应用的智能合约。通过人工智能的硬件设备，为区块链应用提供智能“矿工”。防伪防赝品，减少繁琐的鉴定程序，增强珠宝古玩真品的信息透明度，增加可信的交易效率和交易频率。为珠宝古玩实物的变现和再变现创造便利条件。

财富链致力于解决如下区块链应用中的痛点：

1）解决珠宝古玩行业中的防伪和防赝品问题；

2）解决珠宝古玩变现和再变现的效率问题；

3）解决区块链 token 通证本身价值的公信力问题；

4）解决居民个人家庭缺乏长周期财富管理工具的问题；

5）解决全球区块链项目发行代币缺乏价值锚定的问题；

6）解决私有链、联盟链发行可信代币的问题；

7）解决珠宝古玩企业通过生态体系进行融资的问题；

8）解决居民个人持有实物珠宝古玩的价值融通问题；

9）解决各行各业的创业公司通过区块链通证进行股权、收益权、选择权等权益融资问题。

3.3 财富链解决区块链项目通证发行中的三个核心问题

区块链项目涉及数字加密通证的发行，必须要解决三个问题。包括加密数字通证的生成机制（通证怎么来的）、加密数字通证的总量依据（严谨的总量数据计算）、加密数字通证的价格生成机制（价格是怎么制定出来的）等三个问题。这三个问题是加密数字通证发行的底层价值逻辑和价值衡量标准。

财富链通过发行珍藏宝（TITT）通证过程中严谨的实体经济数据计算模型，解决这三个问题。进而形成具备强大公信力的加密数字资产底层价值锚。

1）珍藏宝（TITT）通证生成机制。财富链采用有价值的实物资产上链才能生成有效的加密数字通证的方式，解决生成机制问题。每一个通证，都对应唯一的一个实物珠宝古玩，而且是携带个性化实物珠宝古玩信息的，不可篡改的，可以防伪防赝品的，具备可追溯可公开查询的特性的通证，这有效的防止了通证发行过程中可能出现的口头承诺，凭空捏造。每一个通证都有实体经济大数据支撑，这无疑是最有说服力的，最具公信力的。

2）珍藏宝(TITT)通证的总量依据。因为现实世界的民间珠宝古玩成品总量是不确定的，因此财富链采用了弹性扩展发行的机制（详见 11.1）。通过实体经济事实和严谨的数学计算模型，让通证的发行既保证了和珠宝古玩实物一一对应、不可篡改的特征，又保证了民间珠宝古玩总量不确定情况下的发行弹性。完全杜绝了区块链项目代币发行中“恒量发行，永不增发”这样不负责任的口头承诺，是一种科学严谨的数字资产发行机制。

3）珍藏宝（TITT）通证的价格生成机制。数字资产的价格生成机制，是需要非常严谨的数学论证的。即使是外汇市场，价格生成机制都也必须采用利率平价理论、购买力平价理论等多个紧密结合实体经济的数学模型进行衡量。因此，财富链提出了一个数字资产通证的价值模型：

通证的价值=实体经济链外价值/通证上链成本

这一价值模型，既涵盖了价格生成机制，又涵盖了通证在交易和流转过程中的价值衡量。根据这一模型，财富链在项目启动之初，尚未形成有效的实体经济链外价值，首先解决上链成本的问题。

财富链在珠宝古玩提供方持有珠宝古玩实物上链的过程中，在物理空间分摊支付人员工资、设备成本、办公场地费用的基础上，由光机电一体化“矿机”根据链上“根通证“的数据，自动计算生成对应的数字证书“珍藏宝（TITT）通证”。所生成的“珍藏宝（TITT）通证”，用户可以自主申请发送到指定地址(用户也可以放弃申请 ,但放弃主动申请将视为把对应的“珍藏宝（TITT）通证”捐赠用于公益事务）。

在后续的实物流转过程中，珍藏宝（TITT）因线上流转的便捷性，就可以有效的结合实物流转，形成实体经济链外价值的有效映射。因为实物上链成本是确定的，实物流转的成交价格是确定的，刺激成交所使用的通证数量是确定的，因此上链成本和链外价值就是确定的。通过链外价值和上链成本的有效制约，就形成了珍藏宝（TITT）的具备实体经济公信力的价格。这样就有效的形成了符合价值模型的价格生成机制。

通过有效的，具备强大公信力的通证生成机制，价格生成机制，以及发行总量依据，让财富链珍藏宝（TITT）的发行具备严谨科学的实体经济数据支撑，从而为区块链项目代币发行形成可信的底层价值锚。

3.4 财富链的优势

财富链的优势比较如表 3-1 所示。

表 3-1 财富链和其他区块链发行项目的比较表

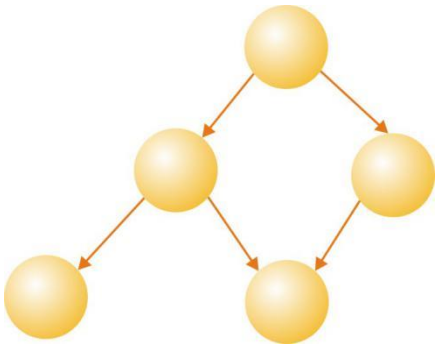
项目	其他区块链发币项目	财富链珍藏宝通证（TITT）
工作证明机制	算力挖矿或无挖矿机制	实物资产“挖矿“
实物交割	不产生真实的实物交割	有真实的实物交割
实物资产支撑	没有实物资产支撑	有实物资产支撑
增值机制	虚拟资产缺乏实体经济的增值机制	虚拟资产有较强的实体经济的增值机制
本身价值	加密货币本身没有价值	通证本身即具备防伪价值
通证	单一标准化通证	每一个均携带不同信息的通证
共识机制	POS，DPOS 或无共识机制	DAG+通证身份化+超级节点机制
发行	恒量发行，永不增发 (口头承诺）	发行和实物资产一一对应 （一个通证对应一个实物珠宝古玩）
泡沫问题	泡沫较大，不易消化	没有泡沫或极少泡沫
底层技术	最长链或 DAPP	DAG 垂直行业公有链

4. 共识机制

4.1 财富链（FC）共识技术背景

财富链（FC）共识机制采用的是有向无环图（DAG）技术，具有交易速度快的特点。当前已经有 IOTA 和 Byteball 等多个项目利用 DAG 成功构建了能够长期稳定运行的公有链，证明了 DAG 链的技术先进性和性能。在财富链(FC)中，交易信息被封装成一个个单元(Unit)，单元与单元之间相互链接组合成一个 DAG 图。由于单元可以链接到任意一个或多个之前的单元，不需要为共识问题付出更多的计算成本和时间成本，也不必等待节点之间数据强同步，甚至没有多个数据单元拼装区块的概念，因此可以极大提高交易的并发量，并把确认时间降低到

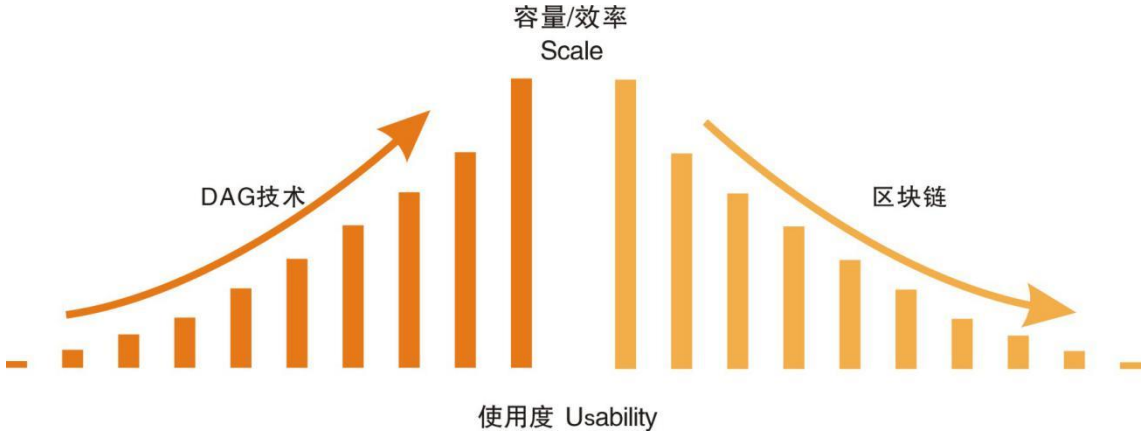
最小。



在 DAG 结构中，交易总是自己创建并发布。从理论上看，攻击者总是可以建构比它要推翻掉的那个交易权重更高的交易用以双花。财富链在 DAG 的基础上，做了进一步的改进——维护用户级别的见证人列表。并受 DPOS 机制的启发，交易单元一旦发布且经所有见证人共同签署的见证单元验证后，该交易单元就是最终确认。

	吞吐量	交易延时	数据膨胀
财富链(FC)	10 万级 TPS 理论 100 万 TPS	除网络延时外 不会出现延时	并行处理的数据量越大， 处理的速度越快
以太坊	理论 2000TPS	15 秒出块	2018 年底预计 1T，未完成

区块链最长链技术的效率会随着交易量的增加而降低，而 DAG 却恰恰相反。



4.2 消息结构

财富链（FC）支持多种消息类型，并可根据需要进行类型扩展。不同类型的消息拥有不同的解析规则，用于存储不同类型的数据。在财富链（FC）中，通过消息中的 app 字段区分不同的消息类型。

- 交易（app=payment）

交易类型消息用于保存各类数字通证的交易信息。一个交易消息中可包含多个输入和输出。对于用户自己定义的资产，需要在消息体中指定该资产定义所在单元的哈希值。一个标准的交易消息如下：

```
messages:[{
    app:‘payment’，
    payload_location:‘inline’，
    payload_hash：‘hash of payload’，
    payload：{
        inputs:[{
            unit：‘...’
            message_index：0，
            output_index：0
        }]
        outputs:[
            {address：‘’，amount 1200}，
            {address：‘’，amount 2800}，
        ]
    }
```

}]

- 文本（app = text）

文本类型消息用于存储任意的可显字符串数据。

messages:[{

app:‘text’，

payload_location:‘inline’，

payload_hash：‘hash of payload’，

payload：‘any text’

}]

- 结构化数据（app = data）

结构化数据类型消息用于存储任意的结构化数据。

messages:[{

app:‘text’，

payload_location:‘inline’，

payload_hash：‘hash of payload’，

payload：{any structured data}

}]

- 数据供给（app=data_feed）

数据供给类型消息可由某个可信第三方发出，用于触发智能合约。

messages:[{

app:‘data_feed’，

payload_location:‘inline’，

payload_hash：‘hash of payload’，

payload：{

‘data feed name’：‘...’，

‘another data feed name’：‘...’

}

}]

- 修改地址定义（app=address_definition_change）

修改地址定义类型消息用于修改地址定义并保留旧地址。

messages:[{

app:‘address_definition_change’，

definition_hash:‘...’

}]

- 资产定义（app=asset）

资产定义类型消息用于定义新的资产。

messages:[{

app:‘asset’，

payload_location:‘inline’，

payload_hash：‘hash of payload’，

payload：{

cap：1000000000，

is_private：true，

is_transferrable：true，

auto_destory：fasle，

fixed_denominations：false，

issued_by_definer_only：false，

cosigned_by_definer：false，

spender_attested：false，

attestors：[…]

}

}]

各字段含义：

➢cap：资产最大发行量。

➢is_private：指定资产交换是私有的还是公开的。

➢is_transferrable：指定资产是否可以不经过发行者就可以在第三方之间转移。如果设置为 false，那么发行者必须参与转移。

➢auto_destroy：指定资产发送给发行者后是否销毁。

➢fixed_denominations：指定资产是否可以按照任意整数发送，或者只能按照固定金额（例如：1、2、5、10、20 等）。

➢issued_by_definer_only：指定资产是否只能由发行者发行。

➢cosigned_by_definer：指定是否每次资产转移都需要发行者的联合签名。

➢spender_attested：指定资产的消费者消费前是否需要认证，如果他无意间收到资产但还没有认证，他必须通过定义中罗列的认证者认证后，才能消费，这个需求对于管理资产很有帮助。

➢attestor ：指定资产发行者指定的认证者地址列表（仅当 spender_attested 为 true 时），发行者可以通过发送一个 asset_attestors 消息修改认证人列表。

➢denominations：仅当 fixed_denominations 为 true 时，列出允许的面额，以及每种面额的

发行数量。

➢transfer_condition：定义资产允许转移的条件，这个定义的语法与地址定义相同，除了不能引用认证的数据，例如“sig”。默认情况下，除了已经定义在其它字段的条件，没有其它限制。

➢issue_condition 与 transfer_condition 相同，针对发行交易。

- 修改认证人列表（app=asset_attestors）

资产定义者可以通过此类型消息修改资产的认证人列表。

```
messages:[{
    app:‘asset_attestors’，
    payload_location:‘inline’，
    payload_hash：‘hash of payload’，
    payload：{
        ‘addresses’：‘attestors1’，‘attestors2’，…..
        }
}]
```

- 个人信息（app=profile）

个人信息类型消息用于个人披露自身信息，通过可信第三方发送的证实消息可验证其真实性。

```
messages:[{
    app:‘profile’，
    payload_location:‘inline’，
    payload_hash：‘hash of payload’，
    payload：{
```

```
            name：‘Alex’，
            emails：‘[alex@example.com]’，
            twitter：‘Alex’
            }
}]
```

- 证实（app=attestation）

证实类型消息用于可信第三方公开与某地址关联的个人信息，利用证实消息可以实现某些业务模式中所需的用户认证。

```
messages:[{
    app:‘attention’，
    payload_location:‘inline’，
    payload_hash：‘hash of payload’，
    payload：{
        address：‘address of subject’，
        profile：{
            name：‘Alex’，
            emails：‘[alex@example.com]’
        }
    }
}]
```

- 发起投票（app=poll）

发起投票类型消息。

```
messages:[{
    app:‘poll’，
```

payload_location:‘inline’，

payload_hash：‘hash of payload’，

payload：{

question：‘…’，

choices：[‘A’，‘B’]

}

}]

- 参与投票（app=vote）

参与投票类型消息。

messages:[{

app:‘vote’，

payload_location:‘inline’，

payload_hash：‘hash of payload’，

payload：{

unit：‘hash of the unit where the poll was defined’，

choices：‘A’

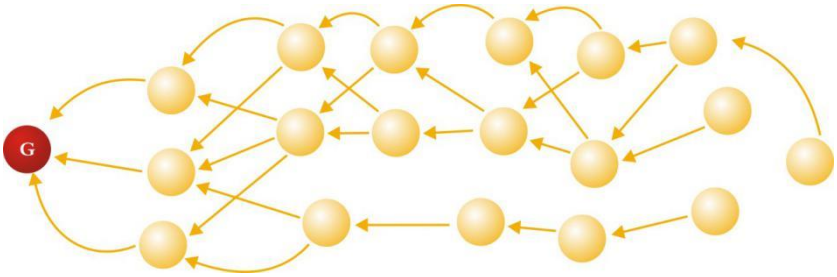
}

}]

4.3 共识描述

4.3.1 单元及其确认机制

财富链底层数据结构采用采用 DAG（有向无环图）结构模式。



图一

上图是 DAG 的结构模型，DAG 中顶点为财富链（FC）的基础数据结构，称为单元，一个单元代表一笔交易，连接各个单元的有向边则表明了他们之间的引用关系。A—>B 表示 A 引用了 B，且 A 需要验证 B 的合法性，因此也可以说是 A 验证了 B。其中 G 为创世单元。随着时间的推移，新交易加入到 DAG 中，财富链（FC）不断向后延伸。单元可以包含多条不同类型的数据，如支付，文本消息，智能合约，记录珠宝古玩信息等等。

DAG 中的每个新单元，验证并确认其父辈单元，父辈单元的父辈单元，可达创世单元，并将其父辈单元的哈希包含到自己的单元里面。如果有人篡改数据，其单元的哈希必将改变，那就会使得它与直接或间接验证确认它的子单元中引用它的哈希不一致。如果要成功篡改单元数据，需要与它的所有的子单元合作，子单元修改它引用的 Hash，这又会导致子单元的 Hash 发生改变，那么子单元又要与子单元的所有子单元合作，直到最后的子单元。

在财富链（FC）中，用户发出新单元时，要求相同地址发布的所有单元应当直接或间接包含该地址之前所有的单元，即相同地址的所有单元连通（有序或连续），并且一笔交易可同时验证多笔交易。同时，设定了单元兼容规则，单元兼容是这样定义的：如果两个单元的见证人列表差别最多一项，则称这两个单元兼容。财富链（FC）要求新发出的单元只能引用与自己兼容的单元。凡是被超过一半的见证人直接或间接确认的单元即视为合法的单元。

4.3.2 见证人

单个地址顺序单元中，每个单元都会有先后次序关系。当出现双花问题时，根据先后次序

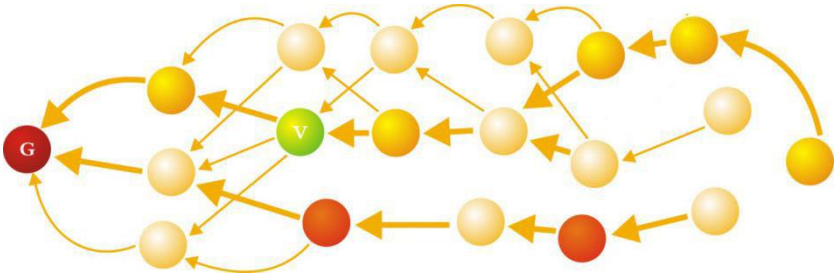
关系，判定早的单元有效，后面的单元无效。这就很容易就解决了双花问题。但是，如果攻击者发布故意多个没有顺序关系的单元或单元系列，那么情况就变得复杂了。因为在 DAG 中，单元是可以自己创建并发布的，他可以选择自己的父单元，可选择自己的高度，伪造时间戳，他可以根据规则伪造出比他想要推翻的单元权重更高的单元,可以创建更多的单元来确认这个双花单元，用来进行双花。同时引入了见证人机制。见证人机制是受传统区块链的委托权益证明（DPOS）启发而设计的。见证人通过选举产生，用户可以提交竞选，并缴纳一笔保证金后，就成为候选见证人。系统根据候选见证人的得票数，保证金，声誉以及是否有实名信息，以及平时表现等，计算出一个指数，并根据指数，为其分配它的见证用户。作为报酬，他会与其被见证用户的所有其它见证人分享被见证用户的所有单元的交易费，但见证者的报酬，会冻结三个月，三个月后方可领取。如果见证人长时间不履行其职责，不发布见证单元，将会被取消见证人资格，并在一定时间内不得参选见证人。如果见证人不遵守见证规则，发布无效恶意见证区块，将会被没收保证金，并永远不得参选见证人。每个用户都有其见证人列表，这个见证人列表的数量为奇数。

见证规则：

1）在同一分叉点，同一验证者只能对其中的一个单元或单元系列投票，来作有效验证。

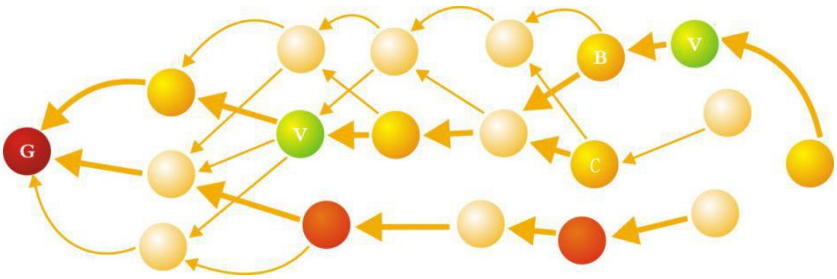
2）如果用户单元或单元系列已经存在了验证单元，其后的验证单元只能在这条已有的验证单元的地址顺序单元系列链上进行，并且验证单元间也要建立次序关系。

3）如果见证者违反上规则一和二，则其保证金及冻结的三个月交易手续费都将被没收，并且将永远不能成为见证人。



图五

图五中，橙色与黄色是同一地址发布的两个独立的顺序单元序列，在它们的第一个单元之前，都没有自己的单元，那么我们把没有包含自己任何单元的单元称为 0 点单元。在这里分叉我们称为 0 点分叉。绿色的 V 单元是见证人签署的验证单元，它确认的是黄色地址顺序单元系列。



图六

图六中，黄色地址顺序单元系列在第一个验证单元后出现了 B 与 C 两个分叉单元，验证单元选择了 B，那么 B 就是有效的，C 是无效的。我们以黄色单元为出发点，排除与地址无关的节点单元计数，B 与 C 处于第四层的位置。我们称为 4 分叉点。在 0 分叉点上，见证单元支持了黄色，在 4 分叉点上它支持了 B，根据见证规则一，在 0 分叉点上与 4 分叉点上任何现有或后来可能伪造的其它地址顺序单元系列或单元都是无效的。根据见证规则二，如果用户单元或单元系列已经存在了验证单元，其后的验证单元只能在这条已有验证单元的地址顺序单元系列链上进行，并且验证单元间也要建立次序关系。那就可以确保任何用户地址，都只有一条明确清晰的被认可的顺序单元系列。

4.3.3 最优父单元选择策略

1）单元级别：由当前单元出发至创世单元的最长路径长度定义为单元级别；

2）见证级别：从当前单元开始沿主链回溯，并对路径中不同见证人进行计数（相同见证人只计数 1 次），当遇到的见证人数足够多时（超过大多数的已知见证人）停止回溯；然后计算停止位置的单元级别，将其称作当前单元的见证级别。

最优父单元的选择策略由以下三部分组成：

1）在选择最优父单元时，见证级别最高的父单元为最优父单元；

2）如果见证级别相同，则单元级别最低的作为最优父单元；

3）如果两者都相同，则选择单元哈希值（base64 编码）更小的作为最优父单元。

从顶端单元出发，只需要递归地在其父单元中选取最优父单元即可形成主链。在上述选择策略中，见证人成为了某个单元看待历史的视角，每个单元可以维护自己的见证人列表，也可以通过见证人列表引用其它单元的见证人列表。

在选择最优父单元时，仅可以从与当前单元兼容的父单元中进行选择，以保证看待历史视角的连续性。不兼容的父单元仍然被承认，但是他们不能成为最优父单元。特别地，在发出新单元时，如果与所有顶端单元都不兼容，则应从上一级别的父单元中进行选择。

4.3.4 最终性

财富链单元经过见证人发布见证区块后，就已是最终确定的状态，无法推翻。

财富链的四大突破：

1)更彻底去中心化

传统的区块+链式结构，需要有一个类中心化的操作，即需要一个记账人，将当前所有交易进行验证处理，然后打包到一个区块，再发布到网络。而财富链（FC） 系统，如上所述，采

用的是单元+DAG 结构，没有区块这一概念。所有单元由用户自己创建与发布。其验证与确认由引用其作为先辈单元的后辈单元来承担。无需传统区块+链式结构那样，需要一个记账人，将当前所有交易打包到区块这一中心化的操作，因而是一种更彻底的去中心化系统。

2)无吞吐量瓶颈因为传统区块+链式结构存在着中心化的操作过程，即需要记账人将交易打包到区块。那么区块链系统处理交易能力的大小，必定受制于以下三点：

（1）记账人节点机器的性能；

（2）记账人节点的网络带宽；

（3）区块的大小。因为存在这一中心化色彩的操作，无论怎样优化，始终都会存在着一个处理能力的瓶颈点。如上所述，财富链系统，采用的是单元+DAG 结构，没有记账人打包区块这一中心化的操作 ,单元由用户创建发布 ,并由其它单元验证确认 ,因而不存在吞吐量瓶颈。

3)明确可预期的最终性。传统区块+链式结构，不排除可能同时产生两个甚至多个区块，由此导致分叉。对于出现分叉的情况，传统区块链将以最长链作为有效链。该机制在理论上会将无法确定最终性，因为无法保证是否存在一条隐藏长链。而 财富链通过见证人机制，只要通过见证人发布的见证单元验证确认，即具最终性，无法推翻。

4)可选交易确认速度见证人发布见证区块分为加急、急、快、普通、慢五个等级。用户可根据自身需求，选择交易确认速度。

4.3.5 双花问题

财富链通过下面协议规则解决双花问题。

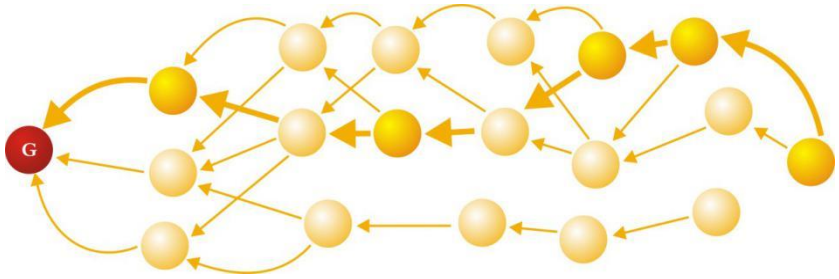
1）一个单元不能引用它的其它父单元直接或间接引用过的单元做父单元。

2）一个地址如果创建发布超过一个单元，后发布的单元必须直接或间接地包含引用其之前发布的所有单元，形成这个地址的顺序单元系列。

3）如果一个地址发布的单元，违反规则二，发布一个或多个，没有顺序引用关系的单元或单元系列，都会视为双花，不论是否存在实质性双花行为。

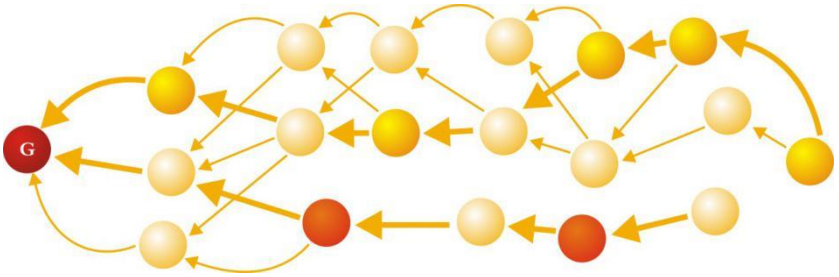
4）在遵守规则二的情况下，出现双花问题，顺序单元系列里，发布较早的有效，发布晚的无效。如果不遵守规则二，发布多个非顺序引用关系的单元或单元系列，根据最优顺序单元系列算法，只有一个单元或顺序单元系列有效，其余单元或顺序单元系列无效。

5）如果一个地址的单元间接或直接包含引用两个或以上的自己发布的没有顺序的单元，该单元无效，不论是否存在实质性双花行为。



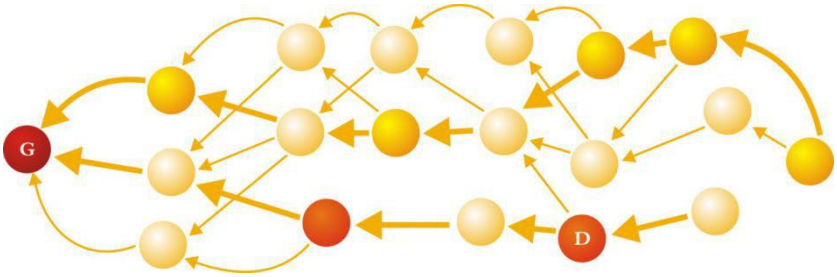
图二

图二中，黄色单元圆点代表了是同一个地址所发布的所有单元。后面的直接或间接地包含前面的单元，形成一个有序的单元序列。



图三

图三中，黄色单元圆点与橙色单元圆点都是同一个地址所发布的单元。可以看出橙色单元圆点与黄色单元圆点之间没有顺序包含引用关系。这种情况下，只有一个顺序单元系列被承认。其它顺序单元的所有交易都会被视为无效的。



图四

图四中，黄色单元圆点与橙色单元圆点都是同一个地址所发布的单元。橙色单元 D，间接包含引用了没有顺序关系的黄色单元与橙色单元。根据规则 4），因此，单元 D 是不被承认的无效单元。建构在 D 之上的由该地址发布的后续单元，由于 D 引用了没有顺序关系的多个同地址单元，所以 D 的后续单元也间接地引用了它们，因而也都是无效的。

4.4 通证身份化+超级节点机制

财富链的通证与其他区块链发行的通证相比，具有一个显著的特点，每个通证都记录着一个生成它的珠宝古玩信息，也就是每个通证都对应着一个珠宝古玩实物，即通证具有身份化，这使得每个通证天然就锚定了一种实物价值。

A、通证身份化的过程就是通过“矿机“生成珠宝古玩数据上链的过程：

1）实物珠宝古玩的鉴定证书二维码启动四维光谱扫描设备；

2）设备把实物珠宝古玩信息转换为数据可视化信息；

3）将二维码鉴定证书信息，珠宝古玩数据信息，时间戳和节点信息打包；

4）将打包信息进行加密，得到哈希值；

5）发送到超级节点验证；

6）超级节点验证确认后在主网广播进行共识。

B、超级节点机制：

1）全网选举 101 个超级节点，其作用在于验证矿机上传的扫描信息，具体为验证扫描成像的珠宝古玩三维光谱信息是否与珠宝古玩鉴定照片的二维信息一致；

2）纠错验证，通证奖励机制。

5.智能合约

5.1 财富链（FC）智能合约概述

智能合约是由事件驱动的、具有状态且运行在一个可复制、可分享的账本之上并能够保管账本上资产的程序，其目的是让一组复杂的、带有触发条件的数字化承诺能够按照参与者的意志，正确执行。智能合约不仅可以接收和储存价值，也可以向外发送信息和价值，整个过程可以在无中心，无信任的前提下，自动化、智能化的执行。

财富链（FC）智能合约使用布尔语句编写合约内容，合约内容称之为定义，是一种声明式智能合约。特性为部署简单，安全性高，由陈述性和完全布尔语句组成，更接近法律合同语言，支持布尔运算，数学运算，甚至数据存储等。与以太坊相比，财富链（FC）的智能合约系统具有复杂度低、轻量化和高性能等优势，同时还降低了合约编写难度和出错概率。在财富链（FC）生态中，智能合约能够主动获取或者接收外界信息，并按照合约内容对其进行回应，回应的方式可以是向其他智能合约发送信息或者向指定账户转移合约中存储的资产等。

5.2 财富链（FC）智能合约原理

财富链（FC）智能合约能够让发送用户在交易之上设置条件，接收用户在接收到交易之后，需要提供满足交易正常执行的条件。如果接收用户无法提供满足交易正常执行的条件，发送用户能够在设定的时间超时后收回交易中支付的 token。相比传统交易支付是一种无协商且

不可逆过程，财富链（FC）智能合约提供了用户之间协商支付条件的手段，并且在协商不成功的情况下，一方用户能够安全收回已支付的 token。用户之间协商支付条件的过程是点对点的交互过程，只需要交易双方参与，不需要中间人和第三方见证人，交易的安全由财富链（FC）智能合约底层平台保证。智能合约采用用户可读的完全布尔语句组织合约内容，对于用户来说易于理解，不需要依赖开发人员来编写智能合约内容。

财富链（FC）智能合约借助可信第三方链下数据访问代理（Off-chain agent），将物理世界中发行的事件绑定在支付条件上。链下数据访问代理是物理世界和财富链（FC）不可篡改数据库存储之间的连接器，负责监控物理世界特定事件并将事件作为数据供给引入平台。虽然链下数据访问代理是可信的第三方，但它本身并不能作为独立一方来看待。使用链下数据访问代理不需要许可，它的作用仅仅是提供公共可用的数据。链下数据访问代理不需要知道用户之间订立的是什么智能合约，并且不关心所提供的数据是怎样被使用的。

财富链（FC）智能合约订立过程包括以下步骤：

1）用户通过财富链（FC）钱包提供的功能请求对手方用户发送支付地址（该地址会包含在智能合约中）；

2）对手方用户接收到请求后回复自己的钱包地址；

3）用户使用自己的地址和对手方用户地址定义智能合约内容；

4）用户向智能合约支付自己的 token；

5）用户向对手方用户发送特定格式的支付请求（即智能合约完全布尔语句），请求对手方用户发送他的 token 并等待对手方用户支付；

6）对手方用户在自己的钱包中查看智能合约定义内容，同意后支付自己的份额；

7）合约内容发送至共识网络进行确认，用户接收到支付通知并等待支付确认；

8）共识网络见证人确认包含合约内容的交易；

9）用户和对手方用户收到支付确认信息后，智能合约的资产交易完成。

5.3 财富链（FC）智能合约操作符与运算

- 智能合约中的逻辑运算符“and”

例如 Alice 和 Bob 制定了一份需要他们共同签名的合约，则签名部分可表达为：

```
["and", [
["sig", {pubkey: "Alice pubkey"}],
["sig", {pubkey: "Bob pubkey"}]
]
    ]
```

- 智能合约中的逻辑运算符“or”

逻辑运算符可以嵌套使用，例如一份合约需要 Alice 的签名，同时还需要 Bob 和 Cara 其中一人的签名，则签名部分可表达为：

```
["and", [
["sig", {pubkey: "Alice pubkey"}]，
["or", [
["sig", {pubkey: "Bob pubkey"}],
["sig", {pubkey: "Cara pubkey"}]
]]
]
]
```

- 达到某个阈值

智能合约还可以要求条件必须达到某个阈值，比如一份合约需要 Alice，Bob，Cara，Dave 四人中至少三人的签名，则签名部分表达为：

```
["r of set", {
required: 3, set: [
```

```
["sig", {pubkey: "Alice pubkey"}],
["sig", {pubkey: "Bob pubkey"}],
["sig", {pubkey: "Cara pubkey"}],
["sig", {pubkey: "Dave pubkey"}]
]
}
]
```

- 赋予不同的权重

此外，合约制定者还可以给不同的签名者赋予不同的权重，合约拥有足够权重的用户签名之后即可生效，执行。则签名部分表达为：

```
["weighted and", {
  required: 6, set: [
{weight: 1, value: ["sig", {pubkey: "Alice pubkey"}] },
{weight: 2, value: ["sig", {pubkey: "Bob pubkey"}] },
{weight: 3, value: ["sig", {pubkey: "Cara pubkey"}] },
{weight: 4, value: ["sig", {pubkey: "Dave pubkey"}] }
] }
]
```

- 获取外界数据

智能合约获取外界数据，定义如下：

```
["in data feed", [
["Alice", "Bob", “Cara” …],
"data feed name",
"=",
"expected value"
]]
```

上面的代码表示，如果由 Alice，Bob 或 Cara 提交到合约的数据等于期望值，则条件为真，

除了“=”，还支持其他诸如“!=”、“>”、“>=”、和“<=”这些运算符。通过此种方式可以指定数据来源，实现强大的智能合约条件控制功能。

智能合约的制定往往需要一定的编程能力，为了方便普通用户使用智能合约，财富链（FC）支持多种功能的智能合约模板，用户只需要根据需求选择相应的模板，填入相应的参数即可，下面是一个智能合约模板：

```
["contract template", [
"hash of unit where the template was defined",
{param1: "value1", param2: "value2"}
]]
```

合约模型可以被重复使用，也可以在其他模型中被引用。

5.4 财富链（FC）智能合约构建步骤

- 智能合约制定

智能合约可由一方制定，也可由多方制定，在一般场景中，智能合约由发起方单方面制定，其他需要多方提供保证金或者授权的应用场景则由参与方共同制定，发起方将奖金放入智能合约，并设定规则，合约制定完成之后，发起方对合约进行签名，涉及到多方参与制定的合约则由多方共同签名。

- 智能合约存入区块链

发起方将签名过后的智能合约通过 P2P 的方式在区块链全网中扩散，每个节点都会收到一份；区块链中的验证节点会将收到的合约先保存到内存中，待验证过后将其存入区块链，最后等待合约触发条件。

- 智能合约自动执行

当智能合约成功部署过后，就会根据合约代码等待触发条件。在一般场景中，智能合约会

自动获取收益者的财富链（FC）地址，并将合约中冻结的资金通过发起转账交易的形式分发给这些账户；如果场景某种原因终止，使得合约在其生命周期之内无法获取收益者名单，则会将其中冻结的资金原路返回给发起方。整个过程不需要任何人参与控制，智能合约能够自动获取判定结果，在收到合约执行的触发信息后执行转账操作（在其他场景中，合约触发条件也可由外界推送）。

5.5 沙箱

沙箱即是一个虚拟系统程序，允许你在沙盘环境中运行浏览器或其他程序，因此运行所产生的变化可以随后删除。它创造了一个类似沙盒的独立作业环境，在其内部运行的程序并不能对硬盘产生永久性的影响。其为一个独立的虚拟环境，可以用来测试不受信任的应用程序或上网行为。

财富链（FC）沙箱的主要功能在于各种新业务的试点工作：

1） 所有在申请的新业务，包括珠宝古玩金融业务、其他生态上链业务等都需要通过高信用证明的沙箱试点，从而形成最佳化的工作流程；

2） 新的节点设备的沙箱验证工作证明通过之后，才能启用生成可以上链的 token 机制。

6.珍藏宝（TITT）通证

6.1 珍藏宝（TITT）

TITT 是财富链项目原生资产数字证书珍藏宝 Treasure in treasure token 的简称。由人工智

能硬件设备将珠宝古玩实物信息转化为图像数据信息之后，把图像数据信息进行加密并提取哈希值生成。是一串计算机加密数字序列码，也是一种携带特定珠宝古玩实物个性化图像信息的虚拟资产。作为一种价值载体，珍藏宝（TITT）将具备生态体系内的数据证明、身份认证、价值尺度、流通手段、价值贮藏等职能。

珍藏宝（TITT）不是虚拟货币，也不是某种有价证券。不是 coin 或者代币，是一种通证或者令牌 token。在发行上不会依赖于任何中心化的机构，也不会任意增发、滥发和销毁导致生态体系的通胀和通缩。TITT 通过锁定实物资产的稀缺性，随着经济生态的不断增长，上链资产的不断增加，生态应用的不断丰富，价值也会随之增加。而最终这些价值都会回馈到实体经济的各类参与主体，形成良性循环的自组织自治体系。

珍藏宝（TITT）在项目前期通过其他公有链发行的通证或者令牌 token，都是不会携带特定珠宝古玩个性化信息的。但最终都将和财富链主网发行的珍藏宝（TITT）进行转换。也就是数量不变，一一替换。

珍藏宝（TITT）在财富链主网发行的通证，初期也不会携带特定实物珠宝古玩的个性化信息。但会依据持有用户对 TITT 的解除锁定而自动匹配携带特定珠宝古玩个性化信息的珍藏宝（TITT）通证。

无论何种情况下发行的珍藏宝 TITT，也无论是否携带了特定珠宝古玩个性化信息，均不影响珍藏宝（TITT）通证作为数据证明、身份认证、价值尺度、流通手段、价值贮藏的职能。

6.2 实物珠宝古玩上链的动机

用户将实物珠宝古玩上链的动机，是为了高效地将实物珠宝古玩进行变现和再变现。

实物珠宝古玩通过光机电一体化“矿机”设备进行上链的过程，不但能为珠宝古玩提供防伪防赝品的“唯一性”身份认证，增加交易信任度，减少繁琐的重复鉴定程序。而且可以得到

多种形式的珍藏宝（TITT）通证价值回报。

用户将实物珠宝古玩上链之后，不但能得到链上的虚拟资产变现价值，而且也能得到链外的实体经济增量价值。

财富链通过实物珠宝古玩上链生成通证或者令牌 token 的机制设计，可以促进珍藏宝（TITT）通证相对于实物珠宝古玩资产的价值映射和价值流转。同时通过解决防伪和变现的实体经济痛点，让珍藏宝（TITT）通证成为具有价值公信力的虚拟数字资产。

6.3 上链流程：实物价格和通证价值相分离

实物珠宝古玩的上链流程：

1）启动光机电一体化“矿机”设备；

2）在线置入对应数量的根通证。只有置入对应数量的根通证，才能完成数字证书的上链广播；

3）扫描实物珠宝古玩数据信息和对应的鉴定证书的二维码取得打包数据；

4）打包压缩提取哈希值，上传节点验证；

5）完成验证，生成数字证书珍藏宝（TITT）通证并广播；

6）用户主动申请或放弃申请珍藏宝（TITT）通证。主动申请的珍藏宝（TITT）通证，将按照根通证数量发放到用户指定的通证地址；用户放弃申请部分，将发放到用于公益的地址。

7）上链流程结束。

根通证，是财富链项目前期在其他公有链发行的珍藏宝（TITT）和在财富链主网发行的没有携带特定珠宝古玩个性化信息的通证。系统默认为锁定状态，被用户释放之后进入流通。

实物珠宝古玩上链所需的根通证数量，以单个珠宝古玩为计量单位，按照统一的标准进行计算。无论是价值 100 万美元的单个珠宝古玩，还是价值 100 美元的单个珠宝古玩，都是一个

珠宝古玩计量单位。每个珠宝古玩计量单位需要多少根通证，全球保持一致。财富链通过这一机制将珠宝古玩的价值和珍藏宝（TITT）通证虚拟资产的价值相分离，既保证了任意一方价值的波动不会影响到另一方，又保证了虚拟资产和实物资产有效的价值映射。

6.4 公钥私钥一一对应

财富链在珍藏宝(TITT)通证进行上链加密的过程中，采用非对称抗量子攻击加密算法。

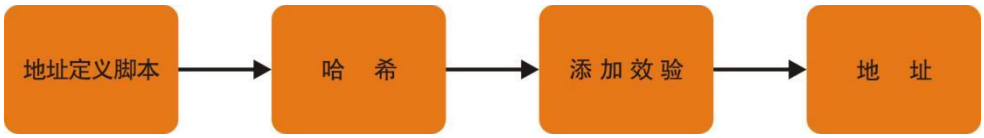
拟采用 NTRU 签名算法，该算法基于格理论设计，具有抗量子攻击的特性，使用时与传统签名算法类似，采用两个不同的密钥对信息进行加密和解密，私钥是只有其所有者知道的密钥，而公钥是网络中的其他实体也可以知道和使用。

这两个密钥不同，但在功能上互补。例如，财富链用户的公钥可以在文件夹的证书中发布，以便财富链的其他人员可以对其进行访问。消息的发送方可以从活动目录域服务检索用户的证书，从证书中获取公钥，然后通过使用接收方的公钥对消息进行加密。用公钥加密的信息只能通过使用集中相应的私钥才能解密，私钥保留在其所有者（即消息的接收方）处。

财富链中用户使用地址进行收发交易。地址本质上对应的是一段具有特定含义的脚本，该脚本称为地址的定义。任何能够使地址定义脚本输出为真（也称作解锁该脚本）的人具有使用该地址资产的权限。最常用的地址定义脚本是公钥（采用 BASE64 编码），即具有相应私钥的人可以使用该地址的资产，比如：

```
["sig",{"pubkey":"Ald9tkgiUZQQ1djpZgv2ez7xf1ZvYAsTLhudhvn0931w"}]
```

对于地址定义脚本进行哈希，再加上校验位就得到了地址，财富链的地址采用 BASE32 编码。财富链地址的校验位并不是全部放在尾部，而是穿插着放在哈希值中间，防止有攻击者在地址中间进行恶意修改。



按照此流程，上面公钥脚本对应的地址为：

A2WWHN7755YZVMXCBLMFWRSLKSZJN3FU

如果地址仅用于接收交易，其定义脚本可以不对外公布。但是当用户首次使用该地址进行发送交易时，他需要在发送的单元中声明该地址的定义脚本，比如

```
unit: {
  ...
  authors: [ {
    address: 'DJ6LV5GPCLMGRW7ZB55IVGJRPDJPOQU6',
    definition: [
      "sig", {"pubkey":"AsnvZ3w7N1lZGJ+P+bDZU0DgOwJcGJ51bjsWpEqfqBg6"}
    ],
    authentifiers: {
      r: '3eQPIFiPVLRwBwEzxUR5thqn+zlFfLXUrzAmgemAqOk35UvDpa4h79Fd6TbPbGfb8VMiJzqdNGHCKyAjl786mw=='
    }
  } ],
  ...
}
```

其中，authentifiers 是用户采用私钥对除 authentifiers 之外的数据进行的签名。在用户使用该地址首次发送单元之后，它不允许再发送地址的定义。当然，只有在该地址的第一个单元到达稳定后，用户才可以发送后续单元。

7.光机电一体化“矿机”

7.1 四维光谱扫描设备

四维光谱扫描设备，是集光、机、电、计算机技术、区块链技术于一体的高新技术仪器。主要作用是对高精度收藏级珠宝古玩的非接触型逆向数据化模型重建，以及随机生成加密数字证书珍藏宝（TITT）通证并分配发送的硬件设备。

财富链四维光谱扫描设备，是专门研究开发的区块链应用专用设备。能够将实物珠宝古玩的立体信息转换为计算机可以标准化处理的数字化模型，可视化程度高，自动化程度高。设备无须接触珠宝古玩表面即可工作，速度快，精度高，生成的 STL 文件可以直接用于 3D 打印、蜡模浇筑、知识产权转让等再生产活动。是具有高新技术特征的科研级仪器设备。

设备配合计算机软件工程、区块链底层技术和分布式存储，可以“一站式”完成实物珠宝古玩数据化和生成加密数字证书。

设备生成的实物珠宝古玩数据化信息，精度高达 0.01 毫米。配合光谱数字化识别技术，可以自动化采集、自动化比较，以及逆向勘校实物珠宝古玩表层信息，能够保证珠宝古玩个体信息的唯一性。即使是机器雕刻、3D 打印、机械化生产的批量金属或非金属珠宝古玩，每一个都也是独立不同的个性化信息。可以有效的防止赝品和伪造，保证上链珠宝古玩的“唯一性”。

7.2“矿机”设备工作原理

四维光谱扫描设备，之所以称之为“矿机”，是因为可以生成珍藏宝（TITT）通证。

该机主要分为实物数据化工作单元和上链工作单元。

在实物数据化工作单元部分，该机采用激光脉冲和光谱测量的光电子学原理，把珠宝古玩实物信息转化为数字可视化信息。采用逆向有限元分析技术结合时间戳，进行复机上链珠宝古玩实物的自动化和智能化分析对比，从而取得对象的四维信息。

在上链工作单元部分，该机采用计算机软件工程、区块链和人工智能的数据处理技术，将设备生成的可视化图像信息和模型信息打包，进行分布式存储，加密并提取哈希值，发送到超级节点（主节点）验证，完成珍藏宝（TITT）通证的匹配和发送。

同时，该机采用对持牌珠宝古玩鉴定机构专属的二维码自动化识别，才能启动设备工作。保证上链的珠宝古玩均有权威鉴定机构的鉴定证书进行品质背书。珠宝古玩鉴定机构的专属二维码，包含该珠宝古玩的材质、品质、重量、尺寸、光谱数据、硬度系数、色彩数据、实物珠宝古玩照片、和鉴定专家个人信息等。财富链所有上链的实物珠宝古玩，均由相应的持牌珠宝古玩鉴定机构承担鉴定责任。

7.3“矿机 1.0”技术参数

“矿机 1.0”版本主要参数：

工作系统	四维光谱扫描仪
扫描方式	非接触式面扫描
启动方式	鉴定识别码扫描启动
相机	进口 3*130 万工业相机

镜头	500 万像素工业镜头
光栅	美国数字光栅，35000 小时光源寿命
工作范围	单幅最小 50*38*38cm 单幅最大 300*225*225cm
工作精度	0.01mm
出块时间	单次 5-10 分钟
外型尺寸	400×280×120mm
定位距离	25-750cm
占用空间	<80mb
token 匹配	自动匹配
token 输出	系统默认钱包或自定义钱包
token 加密	非对称抗量子算法加密
复机加密	MDI-QKD 量子本体加密
验证机制	随机节点 6 次确认
出块奖励	系统默认或自定义
时间戳	Unix 时间戳
数据输出	ASC,STL,OBJ,PLY,IGES

设备特点：

1、用途：可扫描珠宝、古玩、首饰、文物等相关的物品。

2、安全无辐射，每次采集时间 5-10 分钟。超大工艺品可采用手持式设备，用时可控。

3、全自动扫描拼接和上链验证，黑色或柔软物体等也可读取数据识别上链 。

7.4“矿机”设备的迭代和开源

鉴于硬件设备的集成和研发进度，“矿机 1.0”将首先实现基本的功能，达到基本的工作流程要求。对实际工作中遇到的细节问题，将按照委托中心化的管理体系责任到人，充分发挥 token 通证激励机制，迅速反应，迅速处理。

“矿机 2.0”将有更高的自动化程度，可以实现实物珠宝古玩的矿物质探伤和识别。

“矿机 3.0”可实现逆向勘校，并可以进行分布式数据库的自动化检索和校对。即使多年后实物珠宝古玩有部分变形损坏，也可以逆向勘校复核原始上链状态。

“矿机”设备的迭代，有赖于硬件配件的采购情况，和应用联机测试周期。

“矿机 3.0”经过测试周期之后，财富链将发布“矿机”设备技术标准和上链技术标准，以及流程规范。矿机的设计参数与驱动程序将进行开源，以加速财富链在全球范围内的落地应用。

8.抗量子

目前区块链常用的公钥算法 ECDSA、RSA、DSA、ECC 等理论上在多量子比特的量子计算机上可以在多项式时间内破解，目前多量子比特计算机正在蓬勃发展，随时可能有突破性成果。因此，财富链（FC）采用抗量子算法非常必要。

目前区块链常用的依赖椭圆曲线公钥加密算法生成数字签名。ECDSA、RSA、DSA 在理论上都不能承受量子计算机十分钟的攻击。

非对称椭圆曲线加密算法 ECC 密钥只需要具有数个量子比特的量子计算机和 shor 算法几分钟即可破解。

财富链（FC）基于抗量子加密实施的两个步骤：

1） 采用抗量子计算密码，基于 hash 的密码，基于纠错码的密码，基于格的密码，基于多变量公钥密码。

2） 基于量子硬件系统的量子密钥。量子密钥分发（QKD）是利用光子的量子性质而分配密钥的一种方式，通过这种方式可以不断地给新用户提供新的随机密钥，这都是来自物理层的随机性。

在分发过程中，并不是直接将密钥通过信道传给对方，而是和对方通过协商后产生密钥，如果中间有人试图窃听，那么就会增加系统的误码率而被发现。通信双方就可以随时舍弃这段不安全的密钥，而协商新的密钥（黑客短时间内再次破解理论上将不再可能）。

财富链量子比特相比传统计算机比特更强大，是由于两个独特的量子现象：叠加和纠缠。量子叠加使量子比特能够同时具有 0 和 1 的数值，可进行“同步计算”。量子纠缠使分处两地的两个量子比特能共享量子态，创造出超叠加效应：每增加一个量子比特，运算性能就翻一倍。

财富链这种超大规模的并行计算，对于需要同时探索无数条路径的算法，还有对海量数据库的搜索，量子计算能极大地提高速度。

在人们日常生活或工作当中，在当今互联网的正常运行与维护当中，均离不开现代加密密码。财富链量子密码技术，是国际领先的区块链加密技术。

财富链量子密钥分配技术是实现量子密码技术的专用技术。采用最先进的法拉第-迈克尔逊（F-M）相位编码方案，是目前国际最稳定的量子密码通信解决方案。该技术通过光的量子态特性进行密钥协商，实现密钥的安全分配、密钥管理等功能，并对上层应用提供密钥接口。是量子密码通信网络中的核心技术。

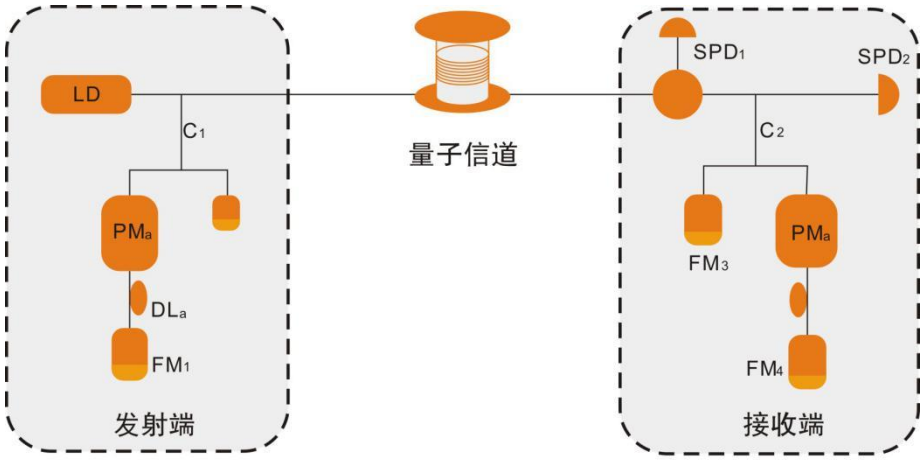
量子加密技术，可以有效抵抗量子计算机对区块链加密系统的破解和攻击。这一技术的应用，将让财富链公有链成为国际顶级的区块链加密生态体系。

主要特性:

•安全性：诱骗态 BB84 密钥分配技术，线路实时攻击检测；

•通用性：直接接入财富链区块链主网智能化密钥触发单元；

•稳定性：国际领先的 F-M 干涉系统，完全免疫线路扰动，无需人工干预。



F–M干涉系统原理图

技术参数：

参数名称	指标参数	单位
波长	1550	nm
编码方式	相位编码+诱骗态 BB84 协议	/
触发频率	50	MHz
平均误码率（@25km）	< 2%	/
安全密钥生成速率（@25km）	≥3000	bps
电源	100-240	VAC
最大功耗	130	W
尺寸（W×H×Dmm）	2U 机箱兼容	

9.财富链（FC）的生态体系与应用场景

财富链（FC）构建的生态系统，以珍藏宝（TITT）通证为基础流转的价值载体和实体经济润滑剂。财富链经济生态的有效运转，最重要的就是资产通证化的通证经济系统运作机制。这关系到有多少外部新用户每天加入生态，关系到有多少外部新用户每天提供增量价值，活跃通证经济生态。更重要的是，每天新的增量用户和新的增量资金资源，不倡导以投机炒作为目的。主要目的应该是试图获取实体经济部分的流转价值或增量利润。

资产通证化，是指参与价值生态的企业单位和个人，将其未来收益权，投票权、分红权、选择权、参与权、转让权、支付权、以及各类价值载体，加以组合并据此应用去中心化通证的过程和技术。资产通证化有三个标签，一是去中心化，即使私有链、联盟链也要具备去中心化的前提。二是生态自治，包括个人和法人。三是保护私有财产不受侵犯，包括匿名加密保护。

真正好的通证经济系统设计，是能够激发实体经济价值流转的设计。生态中衍生的商业模式和经济模型，都是生态自发自治的，凭主观设计迭代不了现实经济生活中千差万别千千万万的模式模型。可持续化的模式设计，就是把底层商业逻辑的规则制定好，生态用户自主挖掘通证的价值和各种衍生的场景应用。本质上，这需要通证经济系统必须要建立在解决实体经济刚需的基础之上。

9.1 生态体系架构

财富链是一个通用的智能合约平台与区块链操作系统，同时也致力于打造一个基于财富链的底层价值锚定的多业态，多样化的生态系统。

- 共识层

共识层是整个财富链的支撑结构，采用单元+DAG 结构，无需记账者打包，打造了一个更为彻底的去中心化区块链系统。一个没有吞吐量瓶颈限制的区块链系统，是财富链的核心部分，也是财富链提供的基础设施。

- 智能合约层

基于共识层之上为智能合约层，财富链采用声明式智能合约，不但简单高效的服务于珠宝古玩变现、交易等方面，而且对多业态，多种形式的上链生态也提供支持。

- 服务层

在财富链核心组件层之上，还引入了服务层，以供基于财富链开发的开发者快速开发各种应用。在服务层中，我们除了封装好核心层的各种 API 之外，还提供了区块链跨链系统与侧链系统。区块链跨链系统主要是指，使两个相互独立的区块链，能够相互读取对方，能够无障

碍通迅。侧链系统是指企业用户，可以快速生成基于财富链的私有链和联盟链，并链结在财富链主链上，可以利用财富链翻译系统与其它链相互通信与交易。

- 应用层

在服务层之上，是财富链的应用层。财富链应用层是指，财富链的钱包和基于财富链上开发的各种区块链 DApp 应用，这些 DApp 应用主要由第三方开发者开发。财富链非常关注用户体验，借鉴 iOS 的经验，将建立一套财富链应用层的规范与标准。

财富链 DApp 能够进行容错，不会出现单点故障。它们没有中心化的机构能够进行干扰。不会出现某些数据的删除或者修改。甚至不能被关闭。主要是由于数据都是进行了加密存储。

财富链 DApp 平台分为基础框架层和应用适配层。底层基础框架层提供区块链的基础服务，应用适配层提供上层应用所需的功能组件，为具体的应用系统开发提供接口和 SDK，降低由于区块链自身复杂的逻辑所带来的应用开发的难度。

对于一般开发的应用适配层，财富链提供区块链应用开发平台，该平台基于财富链 DAG 技术，将上层应用所需要的功能组件进行封装，开发者想实现对应的功能，只需要注册成为财富链开发者即可获得接口使用权限。同时，财富链主网也会提供开发者运维所需要的可视化管理工具。

另外，基于财富链平台开发的 DApp 自身发行的 token 要锚定财富链的珍藏宝（TITT），具体为，第一，token 要设定与珍藏宝的兑换比例，第二，token 要关联对应珍藏宝的摘要信息，第三，token 发行前，利用财富链的智能合约要先质押部分珍藏宝作为底仓，DApp 运行过程中发生信用崩溃等失效问题时，财富链主网将对 DApp 自动锁死，质押的珍藏宝等比例释放兑换。

财富链核心组件层是财富链生态系统的根基。财富链上的开发者以及基于各区块链系统，是财富链生态中的上游参与者，我们在服务层为他们提供各种便利的服务接口。普通用户则是

财富链生态中的消费者，我们制定一套用户友好的应用层规范标准，方便普通用户体验。

9.2 应用场景

财富链的经济生态系统未来将包含的场景如下：

9.2.1 长周期资产管理工具

自 2008 年国际金融危机以来，以美联储为首的全球央行展开了不同程度的量化宽松“印钞”行动。巨量的流动性注入实体经济的同时，推高了资产价格，也极大的稀释了居民私人财富。

即使以高速增长为背景的中国大陆，随着地产投资对居民长周期财富管理的重要性日益降低，大量中产阶层迫切需要找到新的长周期资产管理工具。

例如，中国大陆居民家庭重要的金融资产以房产和汽车为主。20 年前购买的汽车，现在已经不再具有经济价值。而 20 年前购买的住房，都一定是有了较大幅度的增值收益。然而，很少有人注意到，20 年前购买的收藏级金银珠宝和古玩，现在基本上都已经远远超过了房地产的收益。那么，假设从现在开始计算，现在购买的汽车，20 年后无疑也是不再具有经济价值了。现在购买的房产，20 年后还能有 10 倍以上的收益吗？这一点，相信即使是经济高速发展的中国大陆居民，也不再抱有太大幻想。更何况，世界上欧美等多个国家和地区，房产并不是可以炒作的标的。但对于珠宝古玩市场来说，20 年后保值增值对抗央行的货币增发依然是肯定的。

之前，珠宝古玩作为保值增值的标的功能之所以不明显，主要是因为难以变现的问题、赝品问题和防伪问题。但是，随着财富链项目的上线运行，这些问题都将会解决，珠宝古玩必然会焕发财富储值和财富传承的强大功能。可以预见，不仅是名贵珠宝古玩，即使是收藏级的天

然珠宝玉石都也将会成为市场追逐的焦点。而 90 后、00 后也会发现珠宝古玩的稀缺性价值、变现对抗通胀和价值贮藏的天然优势。珠宝古玩的财富传承，将因财富链而成为无国界的价值储存和流转工具，珠宝古玩也将重新成为世代传承的王者。

9.2.2 珠宝古玩企业融资

过去，因为珠宝古玩不易变现的问题，珠宝古玩的价格评估和资产评估从来都是难以操作的问题。而缺乏价格评估和由此导致的资源价值不确定性，珠宝古玩企业和产业链体系就很难融入传统金融体系，难以得到传统金融系统的资金支持。在全球范围内，珠宝古玩企业在银行系统的信用等级都是非常低的。

财富链将在珠宝古玩企业直接融资和间接融资方面，发挥作用。财富链聚焦于解决珠宝古玩变现问题，通过珠宝古玩体验式消费，珠宝古玩托管，珠宝古玩租赁，珠宝古玩衍生产品设计，以及通证流通激励等通证经济系统的资产通证化设计，可以极大的提高珠宝古玩企业资金回笼的效率，以及未来收益权等再融资操作的可行性。从而在债权、股权、收益权、选择权、权益委托等多个方面打开现金流的流动性空间。产业链上下游之间的价值转移也将变得流畅，和传统金融系统的直接融资产品和间接融资产品也将无缝对接，从而实现多方共赢。

全球珠宝古玩产值每年约 3 万亿美元，过去几千年累积的珠宝古玩存量价值无法估量。如果通过财富链进行变现流转，或将盘活十几万亿美元的增量流动性。

9.2.3 个人珠宝古玩融资

对于持有珠宝古玩的居民个人来说，即使是名贵珠宝古玩，变现渠道也极为有限。在全球范围内，通过机构的变现渠道，有效的只有二种：

1）典当行

2）拍卖会

对于普通居民个人来说，持有珠宝古玩上拍卖会是非常不现实的繁琐且狭窄的渠道，况且还有时间因素和不菲的前期费用，因此，拍卖会历来不是居民个人进行珠宝古玩变现的首选。相对来说，典当行更贴近民生。

但是，即使是典当行，对居民个人的珠宝古玩变现也极为不友好。首先，因为鉴定人才的欠缺，很大比例的典当行并不开展珠宝古玩典当业务。其次，典当行的商业模型，就是典型的折价变现模型。因为要杜绝“绝当”的风险，所以一般珠宝古玩都是按照投入价值的 2-3 折左右，或者是当前市价很低的折扣。这样折算下来，居民个人以珠宝古玩作为理财工具，或者是财富储值工具就必然达不到理想的效果。

随着财富链强势解决珠宝古玩的市价变现问题，无论是居民个人，还是商家企业或其他组织，只要有珠宝古玩实物变现的需求，都将归类为“珠宝古玩提供方”。无论是居民个人，商家还是其他组织，只要有持有实物珠宝古玩的需要，都将归类为“珠宝古玩需求方”。彻底打破传统经济和互联网经济中“B 端”和“C 端”的概念，以珠宝古玩实物为基准，进行变现和资金融通。

因为金银珠宝和古玩本身并不是纯粹的时尚奢侈品和消费品，因此财富链将充分挖掘珠宝古玩先天性去中心化的财富储值和价值流通属性。让居民个人无论持有实物珠宝古玩还是持有虚拟的珠宝古玩资产，都能进行抵押、质押、权益委托、收益权共享等融资变现操作。以此为基础，传统金融机构也将以居民个人的珠宝古玩资产为参照完善信用体系，提供资金支持。

9.2.4 珠宝古玩设计的知识产权保护

对于珠宝古玩行业的知识产权问题来说，过去设计作品被盗版，仿制，侵犯知识产权屡见不鲜。不但缺乏追责的手段，对于好的创意设计，也常常不能满足珠宝古玩定制的异地客户需

求。虽然珠宝铸模翻制的传统手工工艺为仿品增加了一定的难度，但很多优秀的设计师依然不得不依托实力企业贡献自己的创意。

财富链的区块链+人工智能上链模式，对于珠宝古玩的创意设计，具有得天独厚的知识产权保护优势。设计师可以将创意设计的珠宝成品上链，同时申请知识产权保护功能。其他厂家或个人定制客户看到这个款式希望使用原版设计的时候，就可以通过智能合约支付相应的版权费用，得到在线下载并可直接投入再生产的数据模型。而版权费用将直接进入该设计师或珠宝企业的珍藏宝（TITT）通证钱包。

不仅对于专业的珠宝设计师和珠宝企业，即使是普通的居民个人，持有珠宝实物也可以在财富链主网申请知识产权保护。知识产权保护功能的智能合约，将为居民个人的珠宝实物增加更加多样化的衍生收益。

9.2.5 珠宝艺术品实物资产交易所

珠宝的价格评估，是全球范围内均十分棘手的问题。

财富链并不会对珠宝成品的价格进行主观的评估，或者进行任何形式的价格指导。用户参与流通的实物珠宝，主要是依赖市场自然形成的成交价格。在珠宝成品的价格管理方面，财富链提出了一个核心风控模型：

珠宝艺术品的价值=实用价值+买家个人价值观

1）在本式中，“实用价值”可能为 0；

2）金融资产（包括法定货币、证券化资产和通证化资产）转化为持有珠宝艺术品实物资产后，价值是不可逆的。

这一风控模型决定了珠宝实物的价值只能是依赖于市场定价，但却无法使用市场定价反过来定义珠宝的再流转价格。

随着财富链解决珠宝变现的问题，未来在全球范围内都可能出现珠宝艺术品实物资产交易所。交易所将通过财富链提供的珠宝成品实际成交的价格指数，对市场反向形成相应品类产品的交易指导价。利用指导价影响各类参与主体的交易报价和成交价格，并以此循环反馈并修正珠宝成品实际成交价格指数。

珍藏宝（TITT）通证在交易所撮合成交实物珠宝的过程中，将发挥重要的价值调节作用。因珍藏宝（TITT）通证的价格上涨和下跌的预期变化，实物珠宝的撮合成交也会呈现各种类型的投资组合。

9.2.6 权益分红机制

权益分红机制，主要指“神秘顾客”等衍生性的由通证经济系统各参与主体发起的权益型收益模式。未来财富链将鼓励生态体系挖掘实体经济的权益分红机制，不断丰富珍藏宝（TITT）通证在实体经济生态中的应用。

以“神秘顾客”为例：

首先，社群用户持有一定量的 TITT 通证，即可申请成为神秘顾客（暗访员）。一旦生效，相应数额的 TITT 通证将被锁仓一年。

成为神秘顾客之后，将有权限在电子商城平台配发的后台，锁定珠宝古玩“提供方“开放的，自己认为容易达成交易的实物珠宝古玩。这一过程中，无须知悉该珠宝古玩提供方信息，也无须知悉该珠宝古玩需求方的信息。只要该珠宝古玩达成成交，神秘顾客将拿到约 1-5%的成交额收益。可以选择使用法定货币接受支付，也可以选择使用智能合约通证钱包接受 TITT 支付。

在这一模式中，持有一定量的 TITT 通证权益，将成为参与分红的必要条件。而收益方式更为灵活，除了可以灵活选择支付方式外，更有不限频次和额度，为神秘顾客创造超额收益。

该模式最大的优势在于 ,神秘顾客无须开发任何客户 ,无须付出任何努力 ,即可参与分红。分红更是按照成交额计算的，而珠宝古玩实物的大额成交将极为常见。

9.2.7 投票和选举

一个良性的区块链应用生态体系，在进行通证经济系统设计的过程中，不但要考虑对参与各方和社群进行金钱激励，更要考虑进行效果激励、口碑激励、信用激励和权益激励。

因为实体经济中，经济人的需求并不是单一的金钱诉求。很多情况下，效果和口碑，信用和权益，都是构成商业经济活动的硬性条件。因此，倡导采用投票和选举的形式进行通证经济体系的应用，就非常重要。

以未来财富链生态体系的某个美容行业 DAPP 为例，如果仅仅采用金钱激励，而不考虑效果，是非常不科学的。因为人们并不会为了贪图金钱激励而承担美容失败的结果，效果和口碑无疑是更重要的。

对于生态各参与方和社群个人来说，通过投票和选举行为积累个人或企业的信用分值，也是非常重要的激励机制，可有效促进生态体系的健壮性。

因此 ,财富链会提倡和引导多种形式的投票和选举 ,充分发挥生态社区自治 ,共生 ,共享，共赢，更符合每一个成员和参与各方的利益。

9.2.8 通证投资基金

这里所指的通证投资基金，主要是参与创业投资或并购投资的，风险投资类型的，采用珍藏宝(TITT)通证进行投资的基金。通证投资基金的通证来源 ,主要是通过募集珍藏宝(TITT) 通证。由基金对实体经济企业进行权益置换、未来收益权的信用融通或众筹通证合作。

大量的创业企业，需要各种类型的融资支持。但通证投资基金并不会支持直接计价投资，

因为通证相对于法定货币具有更好的价值活力和更多的收益弹性，所以可以选择未来收益权等多种投融资合作模式。

假设有一家创业企业，前期产品可以滚动发展，从银行融资将面临巨大的融资成本，而且也没有更多的资金进行宣传推广。如果得到通证投资基金的支持，那么就可以评估其企业和法人的综合信用，在总体融资或者众筹的额度下，按照滚动发展的要求使用智能合约进行分批滚动发放，在线智能分红。而分红又体现为多种组合收益模式。如集合用户模式、传导用户模式、既得通证模式、既得产品模式，既得服务模式，既得数据模式等等。这样既可以完成融资额度，又能进行很更好的风险控制。而且能更好的培养企业和个人的综合信用，良好的综合信用又能得到更大的融资支持，从而形成良性循环。

同时，通证投资基金因为依托财富链全球化庞大的社群，在宣传推广方面也会事半功倍。更可以做到精细化营销，全球化布局，业务增长空间很容易实现爆发式增长。

在这一机制下，全世界的投资人都可以通过该智能合约参与投资，共享创业公司的高速增长利润。如果投资失败，基金和参与投资方也不会有大额的损失。

10.财富链（FC）团队及发展

10.1 财富链（FC）团队介绍

10.1.1 财富链项目团队

财富链创始团队，是由珠宝金融管理专家牵头，国际区块链极客和人工智能芯片开发领域领军人物组成的专业项目团队。

以创始人 **徐卫国** 为主的团队主体架构，具备十多年的珠宝古玩行业从业经验和珠宝金融资产证券化项目经验。2016 年进入区块链积分项目的专业研究领域，对于资产通证化、标准化等行业痛点和区块链落地应用具有独特的视角和丰富的实践。

以联合创始人 **Risky Lau** 为首的区块链公有链主链开发骨干，在对等计算、区块链开发、分片技术、有向无环图(DAG)技术、抗量子加密技术等领域专业研究多年。他本人博士学历，有 4 部专著，在国际权威专业期刊发表论文几十篇。团队骨干成员均具有十年以上丰富的项目开发经验和攻关实践。

以联合创始人 **peter wu** 为首的人工智能芯片开发骨干，曾经领导团队在区块链矿机芯片开发领域取得优异的成绩，所开发的以太坊矿机出块速度高居全球最前沿。他本人北航硕士学历，有十几年的芯片开发经验。带领科研团队为财富链的人工智能上链设备研发做出了很大贡献。

综合来说，财富链创始团队能力互补性强，战略层次分明，区块链落地应用焦点明确，解决民生刚需强劲有力，是一支脚踏实地的，富有创造力的高科技项目团队。

10.2 财富链（FC）未来发展

主链开发推进计划：

（1）2018 年 11 月 1 日至 11 月 30 日，完成财富链底层 DAG 共识机制的设计与开发；

（2）2018 年 12 月 1 日至 2019 年 1 月 15 日，完成财富链智能合约的设计与开发；

（3）2019 年 1 月 16 日至 2019 年 2 月 28 日（跨春节），完成财富链钱包的设计与开发；

（4）2019 年 3 月 1 日至 2019 年 4 月 1 日，完成财富链 DApp 运行支撑平台的设计与开发；

（5）2019 年 4 月 1 日至 2019 年 4 月 15 日，完成财富链主链与“矿机”的接口对接与调试；

（6）2019 年 4 月 16 日至 2019 年 4 月 30 日，完成财富链主网上线前的所有测试工作。

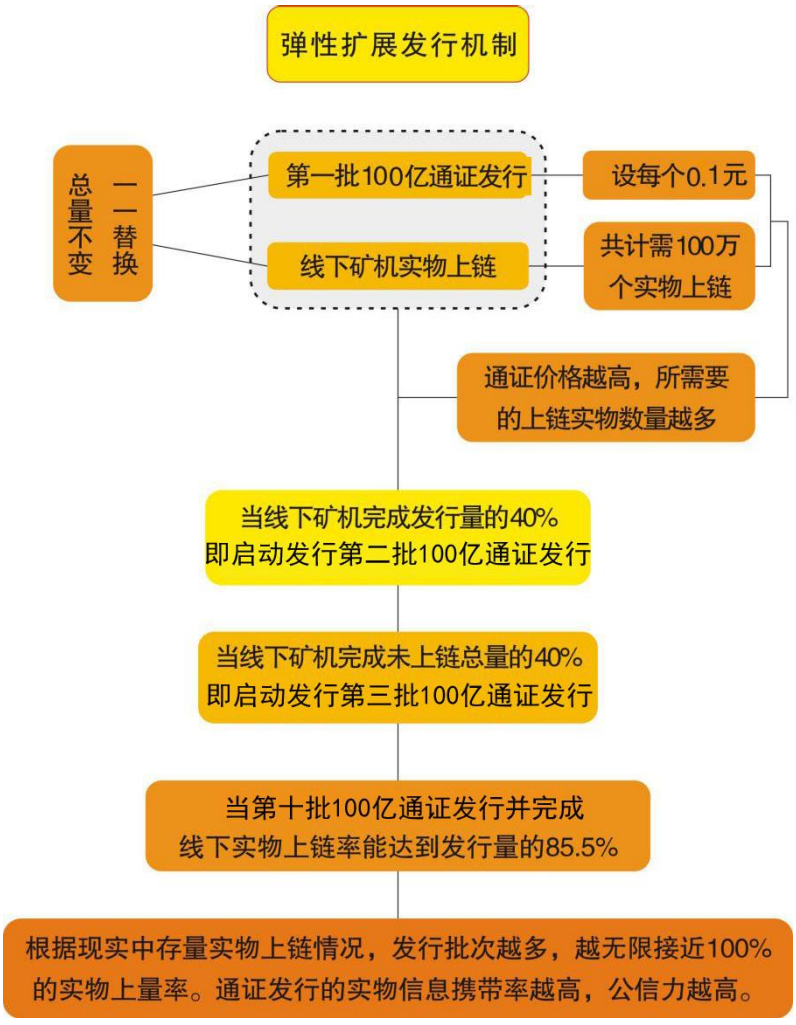
11.通证发行及分配机制

11.1 发行机制

名称：珍藏宝（Treasure In treasure token,简称 TITT）。

珍藏宝（TITT）的发行，采用通证身份化机制，每一个珍藏宝（TITT）通证都会对应一个唯一的实物珠宝古玩。因为全球的成品珠宝古玩数量是动态的和未知的，因此，TITT 特别采用了弹性扩展发行机制。既保证通证发行和实物珠宝古玩相对应的刚性需要，又能保持相对弹性。

弹性扩展发行示意图



1）珍藏宝（TITT）在财富链主网上线前，首先在其他公有链发行 100 亿份通证。当线下实物珠宝古玩上链的数字信息与根通证匹配之后，采用“一一对应，数量不变”的原则完成珍藏宝（TITT）的生成。当实物上链数量达到总量的 40%之后，启动发行第二批 100 亿份。这样依次类推，10 次发行之后，实物信息携带率就能达 85%以上。之后随着生态建设的繁荣和通证经济系统的普及应用，发行的实物信息携带率将会越来越高，最终无限接近 100%。

计算信息携带率的数学模型如下：

设每次触发启动下一轮M（在实际中为 100 亿）个通证发行的实物上链占比为r（在实际中为 40%），设$f=1-r$，那么每一轮的“挖矿”所得通证数量为：

第 1 轮：Mr；

第 2 轮：$(1+f)Mr$；

第 3 轮：$\big((1+f)f+1\big)Mr=(f^2+f+1)Mr$；

第 4 轮：$\Big(\big((1+f)f+1\big)f+1\Big)Mr=(f^3+f^2+f+1)Mr$；

第 5 轮：$\Big(\Big(\big((1+f)f+1\big)f+1\Big)f+1\Big)Mr=(f^4+f^3+f^2+f+1)Mr$；

……

第n轮：$(f^{n-1}+\cdots+f^2+f+1)Mr$

又$(f^{n-1}+\cdots+f^2+f+1)=(1-f^n)/(1-f)$，因此，第$n$轮的“挖矿”所得通证数量为$(1-f^n)Mr/(1-f)$。由此得前$n$轮“挖矿”所得通证数量总和为

$$\frac{(f^{n+1}-(n+1)f+n)Mr}{(1-f)^2}$$

因此，前n轮实物信息携带率为：

$$\frac{(f^{n+1}-(n+1)f+n)r}{(1-f)^2\mathrm{n}}$$

2）通证的身份化机制，有效的保证了通证经济体系的适度通胀的原则。因为全球珠宝企

业每年会生产新的珠宝成品，将形成新的总量供应。这将保持通证生态体系的活跃性和健壮性，也不会造成恶性通胀和超额的增发。

3）有效对抗通缩风险。随着珠宝古玩金融和生态体系的广泛应用，通证价格和实物珠宝古玩价格相分离的原则会有效的防止通缩的风险。例如，1 万美元一枚的戒指，在体验式消费的互动过程中，珠宝古玩提供方通常要使用等值于 1000-2000 美元的通证。但实际上该珠宝古玩上链得到的只有不到 100 美元的通证，差额部分就需要参与流通才能获得。

11.2 分配比例

比例	分配方案	明细
15%	社区建设	为了珍藏宝全球社区的发展，与目前一些成熟的区块链社区进行合作，快速奠定珍藏宝全球社区基础，吸纳大量人才共建珍藏宝全球社区。

5%	管理委员会	用于珍藏宝管理委员会各方面的运营和管理维护 ,包括完善技术开发和维护、支持珍藏宝相关的学术研究、珍藏宝生态的教育培养，以及社会公益项目的扶持等。
10%	团队激励	顾问机构 ,个人顾问 ,超级节点合作激励 ,开发者激励计划 ,内部管理激励。
40%	融资操作	针对机构的融资（不接受美国公民和中国公民参与）
30%	预锁定	锁定比例，在实物珠宝古玩上链——匹配的过程中，优先自动匹配融资操作用户释放的珍藏宝根通证，如遇差额，则自动顺延到预锁定部分进行开放匹配

12.财富链（FC）免责及风险管理

12.1 免责声明

本白皮书中已经明文规定，对于财富链（FC）或珍藏宝（TITT）通证，财富链管理委员会不作任何陈述或保证（特别是对于其价值表现和特定功能）。任何参与财富链或通证公开应用计划，以及涉及投资或购买珍藏宝（TITT）通证的参与者都是基于他自己对财富链和珍藏宝（TITT）通证的了解以及本白皮书的信息。在满足前述事项的条件下，在财富链项目启动后，所有参与者将收到珍藏宝（TITT）通证，无论其规格、参数、性能或功能如何。财富链（FC）特此声明不承认并拒绝承担以下责任：

1）任何财富链珍藏宝（TITT）通证流通的参与者，违反任何国家的反洗钱、涉及反恐融资或其它监管条例；

2）在参与财富链珍藏宝（TITT）通证流通时，任何参与者违反了任何陈述、保证、义务、承诺或其它要求，以及因此导致的不发送或无法提取财富链珍藏宝（TITT）通证；

3）由于某种原因，财富链珍藏宝（TITT）通证公开流通计划被停；

4）由于财富链发展失败或延迟，无法提供珍藏宝（TITT）通证或延迟交付；

5）财富链主网故障导致相关源代码出现技术问题，如死循环、错误、漏洞、崩溃、回滚或硬分叉等；

6）公开涉及任何项目珍藏宝（TITT）流通的用途；

7）任何参与者披露，丢失或销毁珍藏宝（TITT）通证的私钥；

8）参与财富链珍藏宝（TITT）通证流通的第三方平台违约、违规、侵权、倒闭、瘫痪、服务暂停或终止、欺诈、误用、行为不当、失职、疏忽、破产、清盘、散户结算或关闭；

9）任何人在珍藏宝（TITT）通证上进行投机；

10）珍藏宝（TITT）通证在任何中介平台被交易或除牌；

11）珍藏宝（TITT）通证被任何政府、主管部门或公共机构视为某种货币或有价证券凭证、流通票据、投资品或是其他物品，从而被禁止，受到法律限制；

12)本白皮书所披露的任何风险因素,以及与此类风险因素相关的损害赔偿、损失、索赔、债务、罚款、成本或其他不利影响。

12.2 风险声明

财富链（FC）开发和运营团队相信，在财富链的开发、维护、运营和市场推广等过程中存在着无数风险,这其中很多都超出了财富链开发和运营团队的控制。除本白皮书所述的其它内容外，每个珍藏宝（TITT）通证参与者都应细读、理解并仔细考虑下述风险，之后才决定是否参与本次公开流通计划。

每个珍藏宝（TITT）通证的参与者应特别注意这一事实：财富链和珍藏宝（TITT）通证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。参加本次公开流通计划应当是一个深思熟虑后决策的行动，将视为参与者已充分知晓并同意接受了下述风险：

1）公开流通计划的终止。本次珍藏宝（TITT）通证公开流通计划可能会被提前终止，此时参与者可能由于数字资产的价格波动以及财富链开发和运营团队的支出，得不到任何权益回报。

2）不充分的信息提供截止到本白皮书发布日，财富链仍在开发阶段，其哲学理念、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财富链最新的关键信息，其并不绝对完整， 且仍会被财富链开发和运营团队为了特定目的而不时进行调整和更新。财富链开发和运营团队无能力且无义务随时告知参与者财富链开发中的每个细节（包括其进度和预期里程碑，无论是否推迟），因此并不必然会让参与者及时且充分地接触到财富链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。

3）监管措施。区块链加密资产正在被或可能被各个不同国家的主管机关所监管。财富链开发和运营团队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任何关于本次公开流通计划、财富链或珍藏宝（TITT）通证的开发工作。财富链的开发、推广、 宣传或其他方面以及本次公开流通计划均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财富链或本次公开流通计划的监管许可或容忍可能只是暂时的。在各个不同国家，财富链珍藏宝（TITT）通证可能随时被定义为虚拟商品、虚拟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，珍藏宝（TITT）通证可能被禁止流通或持有。

4）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(包括财富链) 带来危险。这可能导致任何持有的珍藏宝（ TITT ）通证被盗、失窃、消失、毁灭或贬值。在合理范围内，财富链开发和运营团队将自我准备采取预防或补救措施，升级财富链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，财富链开发和运营团队将尽力迎合密码学和安全领域的不断变化。

5 ）开发失败或放弃。财富链仍在开发阶段，而非已准备就绪随时发布的成品。由于财富链系统的技术复杂性，财富链开发和运营团队可能不时会面临无法预测和/或无法克服的困难。因此，财富链的开发可能会由于任何原因而在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珍藏宝（ TITT ）通证无法交付给本次参与计划的任何参与者。

6 ）运营资金的失窃。可能会有人企图盗窃财富链项目所获资金。该等盗窃或盗窃企图可能会影响财富链开发和运营团队为财富链开发提供资金的能力。尽管财富链开发和运营团队将会采取最尖端的技术方案保护相关资金的安全，某些网络盗窃仍很难被彻底阻止。

7 ）源代码瑕疵。无人能保证财富链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，将损害财富链的可用性、稳定性或安全性，并因此对珍藏宝（ TITT ）通证的价值造成负面影响。

8 ）安全弱点。财富链区块链基于开源软件并且是无准入许可的分布式账本。尽管财富链开发和运营团队努力维护财富链系统安全 ,任何人均有可能故意或无意地将弱点或缺陷带入财富链的核心基础设施要素之中 ,对这些弱点或缺陷财富链开发和运营团队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珍藏宝（ TITT ）通证或其他数字资产丢失。

9 ）“分布式拒绝服务”攻击。财富链设计为公开且无准入许可的账本。因此，财富链可能会不时遭受“分布式拒绝服务”的网络攻击。这种攻击将使财富链系统遭受负面影响、停滞或瘫

瘓，并因此导致在此之上的交易被延迟写入或记入财富链区块链的数据之中，或甚至暂时无法执行。

10）处理能力不足。财富链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财富链区块链网络内届时节点所能提供的负载，则财富链网络可能会瘫痪或停滞，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，任何人持有的珍藏宝（TITT）通证可能会丢失，财富链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财富链的可使用性、稳定性和安全性以及珍藏宝（TITT）通证的价值。

11）未经授权认领数字证书珍藏宝（TITT）通证。任何通过解密或破解珍藏宝（TITT）通证参与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，将能够恶意获取珍藏宝（TITT）通证参与者指定发送地址中的通证。据此，参与者的通证可能会被错误发送至通过参与者注册邮箱或注册账号认领珍藏宝（TITT）通证的任何人士，而这种发送是不可撤销、不可逆转的。每一珍藏宝（TITT）通证参与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；

(iii) 以及严格保密其机密或个人信息。

12）通证地址。私钥获取珍藏宝（TITT）通证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通证地址拥有唯一的公钥和私钥才可以操控珍藏宝（TITT）通证。每一参与者应当妥善保管其通证地址私钥。若珍藏宝（TITT）通证参与者的该等私钥丢失、遗失、泄露、毁损或被盗，财富链开发和运营团队或任何其他人士均无法帮助参与者获取或取回相关珍藏宝（TITT）通证。

13）普及度。珍藏宝（TITT）通证的价值很大程度上取决于财富链项目在各国线下实体

店的普及度。财富链并不预期在流通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，财富链甚至可能被长期边缘化，仅吸引很小一批参与者。相比之下，很大一部分珍藏宝（TITT）通证需求可能具有投机性质。缺乏用户可能导致珍藏宝（TITT）通证市场价值波动增大从而影响财富链的长期发展。出现这种价值波动时，财富链开发和运营团队不会（也没有责任）稳定或影响珍藏宝（TITT）通证应用和其市场价值。

14）价值波动。若有中介机构参与流通，加密数字资产通常价值波动剧烈。短期内价值不稳，震荡经常发生。该价值可能以其他数字资产、美元或其他法定数字货币计价。这种价值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、中介机构的可获得性以及其他客观因素造成，这种波动也反映了供需平衡的变化。无论是否存在虚拟资产流通的二级市场，财富链开发和运营团队对任何二级市场的珍藏宝（TITT）通证流通不承担责任。因此，财富链开发和运营团队没有义务稳定珍藏宝（TITT）通证的价值波动。珍藏宝（TITT）通证流通价值所涉风险需由参与者自行承担。

15）财富链发行的珍藏宝（TITT）通证数字资产，不承担任何形式的公正、保证、见证以及担保等司法责任。

16）财富链发行的所有数字根证书和珍藏宝（TITT）通证，不会对中国公民和美国公民进行任何形式的发行，也不会允许中国公民和美国公民进行任何形式的类似法定货币购买行为。中国公民和美国公民，只能通过实物珠宝古玩在线下实体店上链生成珍藏宝（TITT）通证，并自主申请才能持有。但不支持任何形式的交易或买卖转让。