靑市链

全球第一个共享数字币自由市场

造币，上市，交易

白皮书

1.摘要

忝市（tiansi）链旨在打造全球第一个共享数字币市场。依托区块链技术，构建所有参与者共同拥有的；任何个人，或组织都可以随时进入市场进行各种数字币的支付，互换，和储存等操作的；任何个人，或组织都可以随时上市自己的数字币。上市的数字币可以是由任何个人或组织发行的任何种类的数字币，如比特币，libra，游戏币等；也可以是由任何个人，组织，或国家拥有的由数字币代表的货币或资产，如美元，购物券，股票，股份，股权，期权，贵金属等；还可以是由任何个人或组织开发的任何数字币代表的实物，服务或组合等。

在区块链技术的系统自治性、数据可追溯确权、信息不可篡改等优势的基础上，忝市链设计了新的高性能、强一致性的共识机制；强化了账户加密的的隐私保护机制；增加了点对点的直接交易机制。忝市链形成一个完整的，对多种数字币进行并行交易和安全存储的，去中心的，自治的，市场系统。

忝市链通过对市场交易主体进行匿名的密码学加密来保护隐私；通过对交易的全过程和统一规则的永久记录和全面开放来实现交易过程的公平，并最终保障交易结果的公平；通过对交易对象进行全方位，全过程的托管来解决数字币从链下资产转移到链上币过程中的信用问题。

忝市链是一个真正的共享市场。忝市链是公共的，其体现为共同拥有，共同管理，共同使用，共同收益；忝市链是自由的，其体现为无进出的限制，无中介的羁绊，无时空的隔绝，无种量的歧视，无交易费用的负担；忝市链是诚信的，其体现为交易过程公平，交易规则公正，全部信息公开。

2.现实市场问题

现实市场经济中最大的问题是交易的不公平。交易的不公平主要就是由不公平的交易程序导致的不公平的交易结果。其具体表现如下：

1)．交易的准入歧视普遍存在。例如金融产品上市都需要需要花费巨额的费用和时间来包装和推广。而准入机制基本上沦为官僚体系和金融掮客共享的牟利工具。

2)．交易的规模歧视成为常态。对各种交易的最小规模的限制是各个市场都存在的规则。对小额交易的歧视也可以到无以复加的地步，正如Libra所述，小额借贷利息可达400%，而借贷成本可达30%。

3)．交易的中介制拌时有发生。交易中介一方面积极促成获利满意的交易；另一方面，人为阻碍获利不满的交易。

4)．全球性信用走低。全球所有的主权货币都存在发行泛滥的问题，已经找不到一种货币具有保值功能。严格意义上讲，今日世界已经没有真正的货币存在了。同时，现有主要信用评级体制非常主观，而以企业付费来获得评级的方式更导致评级流于形式。

5)．市场信息扭曲日趋严重。诚然，互联网和移动通讯的高速发展，带来了快速获取知识和信息的便利。同时，其也带来了日益严重的中心化节点对信息的操控问题。美国国会就谷歌对2016年大选操纵的听证会就是一个明证。同时，信息扭曲化问题也日益严重；有害或垃圾信息日益泛滥。利用今日的网络进行信息搜寻，不仅仅获得正确信息变得越来越难，而且甄别正确信息从海量的重复性信息，无内容的垃圾信息，和出于各种目的人为扭曲的或断章取义的误导性信息也变得日益困难。

3.问题解决方案

利用区块链技术，构建一个统一的，去中心化的，低成本的，保护隐私的，可信任的，虚拟资产的自由市场系统可以解决数字币交易的简易和公平问题。靛市链市场系统将具备以下特性：

1)．靛市链是一个统一的市场系统。

靛市链的市场主体包括任何根据自己意愿自由加入或退出的交易人。靛市链的市场客体是各种数字币。任意具有价值的有形和无形的资产和服务都可以由数字币代表，借此就可以在靛市链上自由的进行包括价值存储，价值转换，和价值转移等各种交易。这些资产的实例是黄金，股票，股份，货币，比特币，libra等。靛市链的市场系统是由许多执行不同功能的子市场的组合。这些子市场包括银行，交易所，保险行，公正处，托管机构等。靛市链的市场就是由这些市场主体，客体，和功能子市场共同构成的有机综合体。

靛市链的所有交易活动都是由开源的电脑代码，将根据预定的，公开的，预定的原则形成的各种标准化的交易，按照公平一致的交易法则自动执行和完成。任何非标准的交易都不会得到靛市链市场的认可。

靛市链的交易记录的产生摒弃了工作量证明，以避免算力的恶性竞争，也摒弃了权益证明，以防止资本的控制。靛市链改变记账的激励机制由获利到需求，即挖矿是无利可图的。同时实现在数秒内达成对交易记录的不可改变的全网统一。

靛市链的所有交易的记录和公布的信息都由使用者自由存储。所有的记录不仅保持所有记录的内容统一，而且通过链状结构完整记录使用资产的来龙去脉来保证所有记录的内涵统一。靛市链的完整信息的采集和公布也将参与第三方托管来进行稳定性加持。

2)．靛市链是一个公共的市场系统。

靛市链是一个没有所有者，只有使用者的，公共的共享市场系统。

靛市链的源码开发是由志愿者们无偿开发的，并将持续增加任何新老志愿者对其进行不断的完善和再开发。任何人不能控制对靛市链源码的开发和升级。

靛市链的源码是开源的，是由所有使用者共同拥有的，即任何人都可以研究，改进，再开发该源码。

靛市链运营后的日常维护是由所有使用者主动承担的，也就是使用和维护一体化，即共同使用共同维护。

靛市链的升级和改进需要在征得广大使用者同意后，由志愿者组成的，非营利的，靛市链基金会

负责实施，并将全过程完整记录，永久保存，并全部公示。

3)．靛市链是一个自由的市场系统。

靛市链是一个可以随时加入或退出的，加密的，P2P网络。其物理状态就是一个由相互直接连接的电脑，手机，共享网站，和共享存储设备共同构成的一个独立的网络系统。

靛市链是一个任何人都可以利用简单的通讯设备随时进入市场进行交易的市场。靛市链没有任何关于时间，空间，品种，数量，成本，和方式等方面的对任何人的限制。

靛市链上实现的所有交易都是交易主体按照自己的意愿，以自己的方式，对自己的资产自由的进行存储，转换，转移等操作。

任何人都可以用自订的方式，自由的，在市场上上市发行或转发个人的，团体的，短期的，长期的，高风险的，或低风险的可交换的数字币，包括货币。

靛市链是一个摆脱了受任何个人或组织控制的市场。由洋葱路由构建成的P2P网络，不仅使该市场摆脱了市场信息被传输中心所控制的风险，而且保障了该系统的永久运行和系统所有者的永远保密。

4)．靛市链是一个免费的系统市场

免费交易费是真正克服交易中的品种局限和规模局限的必要条件和手段。

靛市链的运行是由所有使用者共同维护。同时，所有使用者都有免费利用市场从事支付，互换，保险，众筹等交易活动的权力。靛市链的开发，发展，和升级都将依靠大量志愿者的无私奉献。

靛市链的免费原则面临的最大问题可能是引来DOS攻击。对此，靛市链将通过相关的技术安排来规避之。

5)．靛市链首先是一个易用的市场系统。

靛市链面向的是最普通的社会民众，力求简单易用。通过简单的APP，网页等，任何人借助电子设备，都可以像使用普通电子支票一样便利的进行各种交易活动。

靛市链可以进行的交易种类可以包括正在测试的资产支付或赠与和新资产上市，也包括正在开发的有资产互换，众筹，保险，和风控对赌等等；即资产上市，扫码支付，资产组合，共享保险，所有权或存在公证，账户管理，公告广告等等。

靛市链的最基础交易就是基于公平规则的，由智能合约自动安排进行的数字币的互换交易。靛市链的互换交易，根据交易主体的不同，可以是零方（即收款）到多方对应零方（即付款）到多方；其中，零方对1方到多方就是收取交易或支付交易。靛市链的互换交易，根据交易客体的不同，可以是对任意种类的上市资产，或是对任意品种的任意组合的交易。靛市链的互换交易，根

据交易的完成时间的不同，可以是即期对即期的，即期对远期的，或远期对远期的交易。

6)．靠市链是一个诚信的市场系统。

靠市链的市场系统的核心就是一个开放式的去中心分布账簿系统，其一方面公开记录和保存了该市场上发生过的所有交易的全过程，全部上市资产的存储情况，和全部资产的所有权归属。另一方面也将全部记录完整的展现给任何需求者来满足各种分析，风险控制，和监管等等的需求。

靠市链上的交易主体就是市场交易的参与者们。他们的全部资产都体现为以以密码学原理创造的，代表不同资产种类和资产数量的支票。靠市链不仅保障了所有交易主体的财产所有权和财产使用权，而且同时也保障了所有交易参与者的隐私。

靠市链上的交易客体是由参与者自行上市的资产。资产的上市方式采取的是登记制。上市的资产的内涵是由上市者自行安排的，可能是是法币，代币，虚拟币，股票，期货，期权，贵金属等等以及它们的组合。靠市链鼓励上市者通过百分之百与实际资产锚定，并且委托专业托管机构进行全过程托管来提高其上市资产的信誉。

靠市链上的交易方式基本上就是将指定资产从一张或多张支票转入另外的一张或多张支票，并且将整个过程完整永久记录下来，由全系统所有参与者共同公证和监督交易过程和资产存放。对所有即期的交易的处理，都类似于物物直接互换；对所有远期的交易的处理，都是借助智能合约对所有交易客体进行即时锁定后按约定渐次处理的。

4.靛市链技术简介

1)．靛市链是采用C++语言开发的，开源的，软件系统。

2)．靛市链的核心就是一个由大量不同节点，即所有者，共同参与的分布式数据库系统，一个开放的，共同拥有，共同管理，共同使用，共同收益的去中心的账本系统；以区块链形式永久性存储全部交易的全过程的分布式数据库系统，即所有的交易原始数据集合。

3)．靛市链的记账方式，即共识机制，采用自创的限定性随机池共识机制，可以在数秒内形成全网一致的不可更改的交易记录。靛市链的共识机制仅限于记账，而将市场的安全维护分离出去另行处理。

4)．靛市链的交易过程采用的是智能脚本技术；即按照公平规则对所有交易进行自动撮合和执行。

5)．靛市链的所有数字币都是利用非对称密码学技术进行存储的；即利用数字签名和数字证书保障数字币的绝对安全。

6)．靛市链的市场系统是一个洋葱路由的P2P网络；即一个无法摧毁的匿名自由市场。

5.贒市链主要交易类型

1).互换交易

首先，由当前所有者利用解锁脚本证明自己对表示特定数量的特定数字币的一张支票的所有权，即通过密匙的签名来证明自己拥有这张支票。

然后，由市场系统利用锁定脚本把该特定数量的特定数字币锁入未来所有者的一张支票里，即用该支票的密钥来代表上述特定数量的特定数字币的所有权和处置权。

所有的锁定脚本和解锁脚本都是通过逆波兰表示法的基于堆栈的脚本实现的。

2).上市交易

上市交易本质上就是一种特殊的互换交易。数字币上市者将自己的一定数量的上市权置换成相同数量（根据最小资产单位）的新上市数字币。

首先，由上市资产所有者自行定义其上市数字币的代码，名称，总量，最小单位，上市首存支票，和代表的资产特征表述；例如100%锚定黄金，随时由贒市链基金会出借和归还。

然后，由上市资产所有者用把自己拥有的同样数量的上市所有权置换成新的上市资产。


介绍
信息处
银行
交易所
公证行
保险公司
上市新数字币
定义新上市数字币:
新币代码:
3个字母或数字的...
新币名字:
最多20数字和字母
新币总量:
一个整数
所需上市权(111)总量: 0
最小交易单位:
Choose One
已拥有的上市权(111)数量: 0
新币存储支票:
支票代码
创造一个新的上市支票
新币描述:
新币的各种特征描述
支付上市权(111)的 - 来源交易的代码+输出序号:
111的来源交易:
111来源交易的代码
0
"TSC"上市新数字币的具体步骤如下:
1. 定义新上市数字币, 即输入或选择下列六项:
1).新币代码: 选择一个新的币代码。即没有被占用的, 三位BASE58数码组合。如GLD, USD, SP5, BTC...
2). 新币名称: 可有一个多达30个字符的币名字。如共享金, 共享美元, 共享S&P500指数, 共享比特币等等。
3). 新币总量: 填入本次发行的币的总数量(不超过10亿的整数)。例如100.
4). 最小交易单位: 选择一个本次发行币的最小交易单位。例如1/10000, 即可以进行万分之一的交易。
5). 新币存储支票: 填入本次发行的币将首先存入的支票(上市支票)。即发行者的支票。
清除上市设定
交易创建
*交易加密
交易发送
支付币
交换币
上市新币
银行开启密码(10秒)
开启银行


介绍
信息处
银行
交易所
公证行
保险公司
数字币支付
支付币代码：
可用支付币数量：0
币支付方：
来源交易的代码
0
币收取方：
支票代码
数量
"TSC"支付交易的具体步骤如下：
1. 选取"支付币代码"，设定要交易的币种类。
2. 输入来源交易的代码和选择来源交易的输出序号，完成一个支出方的设定。
根据需要本步可以重复输入设定多达十张不同的支出支票。
3. 输入收取方所用支票和该支票的收取金额，完成一个收取方的设定。
根据需要本步骤可以重复输入设定多达十张不同的收取支票。
4. 依次点击"交易创建""交易加密""交易发送"来完成交易发送。
显示窗口内，如显示64个字符的交易代码则表示交易成功发送到交易池里等待写入区块。
清除支付信息
交易创建
* 交易加密
交易发送
支付币
交换币
上市新币
银行开启密码(10秒)
开启银行


介绍
信息处
银行
交易所
公证行
保险公司
数字币交换
设定换出数字币(换出支票表示为 - 币来源交易的代码+输出序号):
换出代码:
换出时限:
No Limit
换出数量:
数量
可换出币总量: 0
换出币来源:
来源交易的代码
0
设定换入数字币:
换入代码:
收取支票:
支票代码
换入数量:
数量
"TSC"数字币交换交易的具体步骤如下:
1. 录入换出币信息:
1). 换出代码: 选择相应币代码
2). 换出时限: 限定可以互换的时间限制。
3). 换出数量:填入准确的换出的数量。
4). 换出币来源: (1)填入来源交易的代码; (2) 选择来源交易的输出序号。
2. 录入换入币信息:
清除交换设定
互换交易下单
支付币
交换币
上市新币
银行开启密码(10秒)
开启银行


介绍
信息处
银行
交易所
公证行
保险公司
发布公告
输入公告内容(英文字母和符号):
要公告的内容
需要GLD: 0
已拥有GLD: 0
支付出GLD:
支出公告费用(只能支付戳金GLD - 来源交易的代码+输出序号):
来源交易:
GLD来源交易的代码
0
支付
"TSC"发布公告具体过程如下:
1. 输入公告内容:输入你想要发布的,将永远被保留的,最多80字节的信息。
2. 支付公告费用:(支付的数量最好就是所需数量,结余的会被无偿捐献给系统。)
1). 填入戳金来源交易的代码;
2). 选择支出戳金来源交易的输出序号。
3. 依次点击创建公告,加密公告,和发送公告。
清除公告设定
创建公告
加密公告
发送公告
查询公告
公告
文件公证
产权证
遗嘱
其他公证

6. 菎市链上市权证

菎市链没有内置的任何代币，唯一内置的是一种权力，即上市新资产的上市权。

数字币在菎市链上市的唯一途径是通过上市权证的兑现。

根据市场需求，菎市链上市权证的价格被限定低于某一个特定的价格；一个没有记账权竞争，没有炒作的价格。

菎市链将没有挖矿机制，而将挖矿承担的记账和系统安全两大功能分离开后一一单独处理。上市权的产生将采用无偿赠与方式奖励给记账人。菎市链

上市权证的发行总量是无限的，可预设的。