CG.NET 收益资产交易所白皮书

2018 年 6 月 26 孟荆 付禹铭 罗放 于成都

引言

2008 年，中本聪发表了著名的论文《比特币：点对点的电子现金系统》，2009 年 1 月创世区块被挖掘出来，至此开启了区块链时代的新纪元。比特币带来了互联网商务的革命，它使安全的，私密的，且不附带交易对手风险的价值交换成为可能，比特币证明了一个去中心化的数字资产可以实现基于算法的供应量限制，持续升值，以及无需任何物理或政治背书的高效交易。

区块链以及数字货币的快速普及促进了数字货币交易的蓬勃发展。具相关统计，截止 2018 年中全球数据货币交易所已达 260 家以上，日交易额 240 亿美元以上，日交易手续费收入 7200 万美元以上。这些交易所大部分都为中心化交易所。由于各国对数字货币交易所监管都还处于摸索阶段，导致数字货币交易所监管缺失，交易所违规挪用用户资产、恶意做空等事件时有发生。

因此应运而生了很多去中心化交易所，其可以很好的解决交易透明和用户资产安全性问题。但是由于目前区块链的技术限制，链上处理性能低下，远远无法达到中心化交易所的处理能力，交易延时大，用户体验差。

1. CG.NET 简介

CG.NET 的中文全称为收益资产交易所，英文全称为 Credit Gross NET（以下简称 CG）。顾名思义就是给有收益的数字资产提供交易服务的交易所。

1.1 市场现状

CG 认为，所有的数字资产都应该产生收益，这个收益要么是现在产生的，要么是未来产生的；收益的形式可以是 BTC、ETH 等数字货币，也可以是权利、承诺、外部经济价值等其它形式；这些收益都应该以通证的形式返还给持有该资产通证（以下简称 Token）的社区生态用户。

CG 还认为，不产生收益的数字资产都是不良数字资产，不幸的是现在各个交易所里交易的绝大多数数字货币都是这种类型的资产，也就是我们常说的空气币。当我们在交易所里能投资的数字资产都是空气币的时候，就会劣币驱逐良币，导致真正有价值的数字资产无法产生、产生了也没地方交易。

如果说区块链整个产业存在泡沫，那么真正的泡沫绝不是比特币和以太坊产生的，因为这两种货币早已经成为了数字货币的价值衡量尺度和流通支付手段。真正的泡沫在于，优秀和良好的资产无法以数字货币形式进行融资或者是上链。真正好的区块链项目也无法从良莠不齐的空气币中脱颖而出。

整个数字货币交易所的现状就是一个恶性循环：

交易项目本身没有收益-》估值模型无法建立-》价格被操控-》交易不透明-》投资者被收割离场-》交易所盈利下降-》交易所收割项目方-》项目方被收割离场-》整个市场没有增量用户和资金。

1.2 解决方案

CG 就是为了结束这个恶性循环而诞生的。

CG 是致力于解决中心化交易所资产定价不合理、交易细节不透明、无法进行价值投资，以及去中心化交易所处理性能低下等弊端而生的去中心化社区自治交易平台。这个平台建立在 CG 链的基础上。

平台采用DAG链+DPOS共识机制来彻底解决现有区块链网络性能低下的问题。比特股的失败已经证明基于传统区块链网络是无法达到数字货币交易所这种处理需求的，那些号称能通过区块链技术实现百万并发处理能力的去中心化交易所显然是不负责任的宣传。

CG 平台本身一种收益资产。平台采用交易即挖矿的机制，平台用户通过交易可获得代币奖励，平台 51%的代币将通过挖矿产生。同时持有代币的用户即为平台的股东，可每天享受平台收益 80%的分红。

平台提出“交易所即所有”的架构，平台要求所有在 CG 交易所上架的数字货币都是可实现收益分红的优秀资产。这些资产可以和交易所一起运行 CG 链上，也可以通过发行 ERC20 代币在平台上进行交易。无论哪种形式都要符合 CG 链的收益分红接口规范并实现优秀资产社区自治协议（EAC1）。

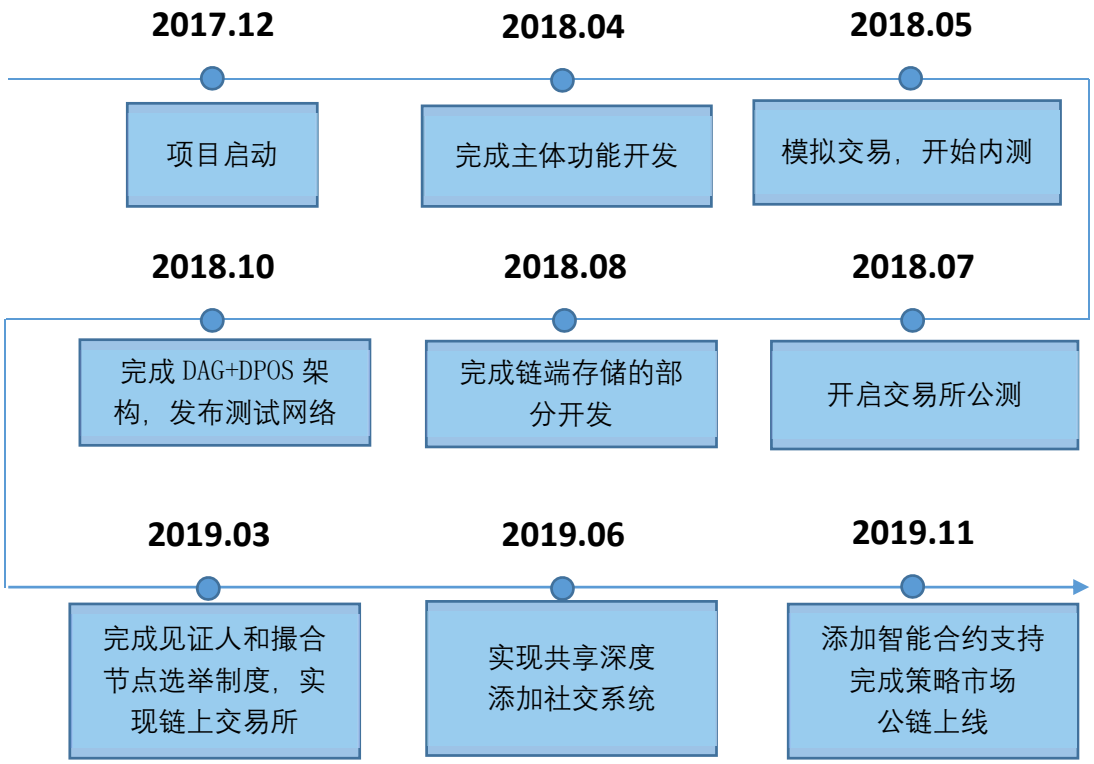
平台将加入外汇交易系统中的 ECN 机制，通过预言机将可信的第三方交易所接入到链端，使平台交易者可共享全球流动性。

1.3 使命与愿景

CG 的使命是连接所有优秀的数字资产，帮助这些资产搭建估值模型、交易环境和自治社区，成为优秀数字资产与投资者及其社区生态之间的桥梁。

CG 的愿景是让基于区块链的数字资产造福每一个人。让越来越多的认从区块链的发展、革新与壮大的过程中收益。

1.4 路线图

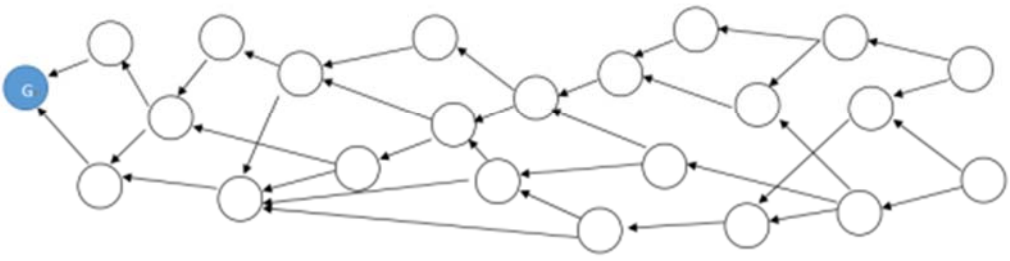

2017.12
项目启动
2018.04
完成主体功能开发
2018.05
模拟交易，开始内测
2018.07
开启交易所公测
2018.08
完成链端存储的部分开发
2018.10
完成 DAG+DPOS 架构，发布测试网络
2019.03
完成见证人和撮合节点选举制度，实现链上交易所
2019.06
实现共享深度添加社交系统
2019.11
添加智能合约支持完成策略市场公链上线

2. 平台架构

2.1 DAG 链和见证人

传统区块链的链式结构是阻碍区块链提高并发性能的严重瓶颈，近年通过技术的不断发展，极客们提出了有向无环图（Directed Acyclic Graph, DAG）来代替传统区块链的解决方案。DAG 链没有区块这一概念，所以没有容量的限制。

采用 DAG 链可以有效解决传统区块链区块确认耗时、网络吞吐量固定的问题、从而避免网络拥堵的问题。在 DAG 链中不存在没有记账者打包区块这一过程，而是用户相互确认，这样一来可以大大缩短了交易确认的时间。同时，在 DAG 链中所有交易是并发进行的，无交易吞吐量瓶颈，节点越多交易确认速度越快，从底层根本上解决传统区块链链式结构带来的问题。



DAG 结构由 IOTA 项目首先使用,之后 Byteball 借鉴 IOTA 的 DAG 结构，并加以改进。在 IOTA 中，要验证新的交易前，必须直接

验证之前的两个交易，这也使得在这两个交易之前所有被验证过的交易得到间接验证。

为避免双花，我们引入了 DPOS 机制，交易单元发布后经所有见证人节点共同签署的见证单元验证后即认定为该交易单元是最终确认的。

我们的见证人节点不同于 EOS、波场等需要社区进行投票选举的机制，在链上的所有节点只要通过性能评估并在链上提交节点竞选承诺后就可以参与竞选，时同参与竞选需要锁定一定数量的代币作为保证金，如果其在成为见证人后做出恶意见证，其所锁定的代币将被系统没收。

所有参与竞选的节点会形成节点池，系统每隔 10 分钟会选取不同的节点成为见证人，节点表现越优秀则担当见证人的机会就越大，同时任期相应也会越长。所有见证人节点在任期内都可分享来自平台10%收益的分红作为奖励。对于表现不合格的节点将在一段时间内禁止参与见证人竞选，同时扣发当前轮次的见证人奖励。

2.2 交易撮合节点

DAG 链可以彻底解决传统区块链的处理能力问题，但由于 DAG 链是并发执行，允许用户的账本之间存在临时性的微小差异，通过短时间内弱化数据的全网一致性来增强处理能力，这对普通交易没有影响但是对于交易所来说还是有些不足。所以我们提出了独立撮合节点的架构。

撮合节点共 3 个，由系统从见证人节点池中选出。为保证安全性和严格的去中心化，系统每 24 小时会执行一次选举算法，从见证人节点池中选出一名节点来替换撮合节点中的一个。每 3 天为一轮，一轮结束后所有的撮合节点都会被替换一次。

与此同时，处于空闲状态的见证人节点会实时校验 3 个撮合节点的单元数据，如果被见证人节点判定撮合节点存在非法数据那么签署非法数据的节点将会立即被踢除，同时立即启动撮合节点选举算法重新选举撮合节点。

2.3 智能合约

系统使用基于 Typescript 语言的智能合约引擎，用户可以基于智能合约创建 DAPP 或自动化交易策略。

不同于传统区块链不可修改的智能合约，平台使用的智能合约分为不可修改和可以更新的两种模式，不可修改的智能合约可以用于发行数字资产、创建智能合同等。可更新的智能合约可以用于创建自动化交易策略、共管合约等。

系统通过创建智能合约链接的形式实现可更新的智能合约功能，用户如果发布的是可更新的合约，那么合约发布时系统不会直接使用该智能合约的地址，而是创建一个合约链接，使用该链接指向合约地址。当合约更新时只需要变更链接指向就可以达到更新的目的。

同时，可更新的智能合约支持多重签名机制，如果采用多签名的方式，签名权重必须达到约定比例以上才可以顺利完成合约更新。

基于以上机制，使用智能合约系统可以完成非常复杂的应用场景。比如，公益基金或信托基金可以使用不可修改的智能合约来创建基金的收益分配策略，使用可更新的合约创建投资策略，收益分配策略是既定的不可修改，投资策略可以根据市场变化由投资委员会投票进行相应的更新。真正实现基金的受益人和基金管理人的权力分离。

2.4 社交系统

即时通信

平台内建了即时通信功能，平台用户可以通过该功能进行一对一或一对多、多对多的即时聊天。由于系统是运行在主链上，用户所有的通信都是通过链来传播，保证用户信息的安全性。

用户动态系统

用户动态是一个类似于 twitter 的专业化金融社交系统，用户可以发表自己的动态、分享交易心得、市场观点等。其他用户可以对此进行评论、回复、打赏等。

2.5 策略市场

策略市场是一个自动化交易智能合约的买卖市场，用户可以将自己编写的用于自动化交易的智能合约布到市场当中供其他用户选择。其他用户应用了指定交易策略后其就会自动在用户账户运行，按既定的条件为用户执行交易指令，不断为用户创造收益。基于策略市场，专业交易员或私募基金完全可以在不募资的情况下共享用户收益，使

用策略的用户越多其获得的收益就会越多。即保证了用户的资产安全又可降低交易员的法律风险。

交易策略可以制定收益分配模式。

免费策略：所有用户都可以免费使用该策略。

一次性收费策略：用户需要购买该策略后才能使用，在使用过程中不需要付费。

按时收费策略：用户购买策略后具有一定的使用时长，到期后用户需要续费才可以继续使用。

共享收益策略：用户使用策略后获得的收益需要按比例分配给策略发布者，没有收益则无需付费。

2.6 共享深度

目前全世界共有 250 多家数字货币交易所，但是各交易所之间数据并不互通，导致用户过于分散、流动性不足、价格差异大等诸多问题，这也是“搬砖”行为大行其道的主要原因。因此我们引入了外汇市场中的 ECN 机制。

ECN（Electronic Communication Network）全称为电子通讯网络，由于外汇市场十分巨大，没有中央交易所，外汇交易都是在场外进行的。ECN 交易可以让你直接进入外汇市场（银行间市场），在这里您可以和其他交易员交易，您的定单在市场上真实体现并被其他人所见，反过来别人也可以介绍他们的订单，如果价格匹配，交易就达成了。ENC 机制会在各个银行及外汇交易平台之间选择最有利于客户头寸的价格来成交，经纪公司看只赚取适当低比例的佣金。

经济商可通过平台提供的预言机接口将第三方交易所的数据接入到链端，为链端的平台用户提供流动性。当用户在平台内下单时系统会在平台内部以及各个经济商之间进行询价，并以最优价格进行成

交。

提供流动性的经济商可以适当收取手续费，平台在询价时会将经济商报价和手续费加在一起作为最终报价进行交易撮合。

为保证用户资产的安全，经济商在提供报价接口时必须冻结一定数量的代币作为保证金，当平台在经济商处的未平仓交易差额大于保证金价值的 80%时平台将不再向经济商发送会加大差额的订单，直至经济商补充保证金或收到使差额降低的反向订单。当平台在经济处的未平仓交易差额为负数时平台会向经济商保证金账户转入等值代币。

如果经济商想停止服务，经济商必须主动向平台发起交割请求，平台收到交割请求后会停止向经济商发送订单，并计算经济商的交易差额。

如果经济商差额为正，那么经济商必须将差额部分转入平台账户，如果其在指定时间内未将资产转入，系统将会把保证金账户内的代币在平台内售出，直至售出金额可抵扣交易差额。

如果经济商差额为负，那么平台会向经济商账户转入指定的资产，并解冻保证金账户。

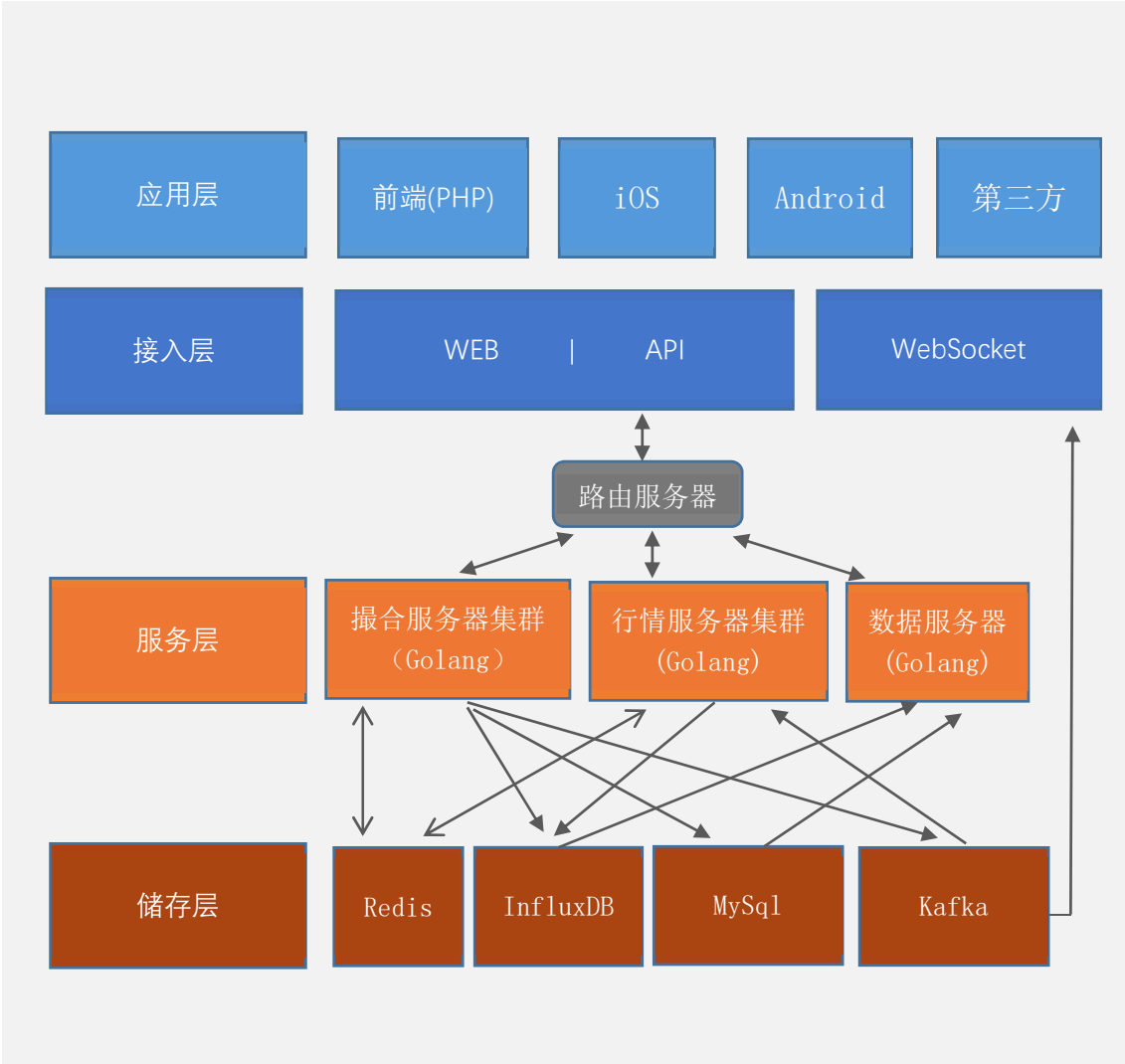
2.7 生物学私钥

在数字货币市场，用户因为私钥保存不当造成资产丢失或被盗的事件时有发生，由于区块链是去中心化网络，传统的找回密码机制并不适用。因此我们提出了生物学私钥的概念，用户在持有账户时可以录入 Face ID、声纹、指纹作为生物学私钥，用户如果忘记账户密码

只要通过上述 3 种生物学私钥的任意 2 种认证就可以重置账户密码。

2.8 交易所架构

在平台主链未上线前我们将使用中心化交易所的方式进行交易。我们的交易平台由数年外汇交易平台和数字货币交易平台开发经验的人员组成，对高并发、高可用系统具有深入的研究。



由于数字货币是 7x24 小时不间断交易，系统服务的中断会受到行情的剧烈波动而加大交易风险，这就要求交易系统必需避免停机维

护。因此我们不论是从硬件还是从软件方面都做到了完整的冗余和高可用。使整个系统所有模块都可以快速进行故障转移。

交易平台采用的是面向服务的架构，前端 WEB 层采用 PHP 做用户交付，业务层使用 Golang 开放，在保持高效前端产品迭代的同时又可以保证业务系统的高性能和高可用。

为保证高效的撮合交易，我们的撮合逻辑全部在内存中执行，同时用 Redis 做备份，并实时向 InfluxDB 输出操作记录。如果撮合服务器出现问题，重启后引擎会自动从 Redis 加载数据，即使万一 Redis 同时也出现故障，引擎仍然可以从 InfluxDB 读取操作日志，回写本周期操作数据。事实上，不论是撮合服务器还是 Redis、InfluxDB 都是集群化多机、多分区部署的，同时出现问题的概率不到亿万分之一。

3. 自运营体系

3.1 挖矿机制

平台提出交易即挖矿的机制，用户在交易过程所产生的手续费会折合成代币返还给用户，直到所有代币都被挖出为止。

平台根据用户交易量所占平台的总交易量比例进行挖矿奖励的分配。

1. 用户获得 60%的代币奖励。
2. 用户的推荐人获得 20%的代币奖励。（推荐人：用户 A 在注册使用了用户 B 的邀请链接，则 B 为 A 的推荐人，若同时有用户 C 是 B 的推荐人，则 C 为 A 的父推荐人）。
3. 用户的父推荐人获得 10%的代币奖励。
4. 社区合伙人获得 5%代币奖励。

系统每小时都会对用户的交易量进行快照，并以此小时内代币的平均价作为标准计算用户此小时内的挖矿收益。每日挖矿产出上限为 2800 万，超过此上限后当日将不再产出。

如，用户 A 在当日的 12 点共产生了 1000 万美元的交易量，占平台当日总交易量的 1/1000，而平台当日的收益为 2000 万美元，当天 12 点平台代币的平均价格为 0.5 美元，那么用户 A 所获得的代币奖励为：

20000000 * 1/1000 / 0.5 * 0.6 = 20000 个

用户 A 的推荐人获得的奖励为：

20000000 * 1/1000 / 0.5 * 0.2 = 8000 个

3.2 收益分红机制

平台每天都将把总收益的 90%拿来对代币持有者进行分红。系统每个小时都会对用户持有的代币进行快照，根据用户代币持有量占总发行量的比例进行收益分红。

如，用户 A 当天 12 点买入并持有 100 万代币，占总发行量的 1/100，13 点后将代币卖出不再持有。平台当日收益为 1000 个 BTC，50000 个 ETH，那么用户当日可获得的分红为：

1000 * 1/100 / 24 * 0.9 = 0.375BTC

50000 * 1/100 / 24 * 0.9 = 18.75ETH

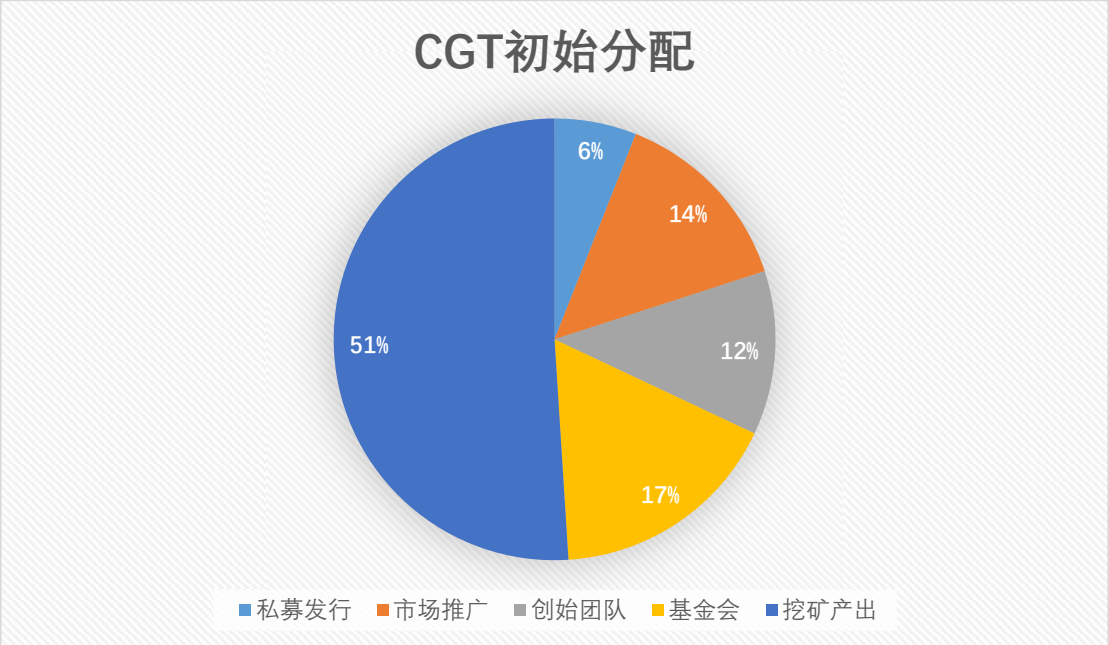
如果用户当天 24 小时均持有代币，那其获得的收益为：

1000 * 1/100 * 0.9 = 9BTC

50000 * 1/100 * 0.9 = 450ETH

3.3 CGT 发行机制

CGT 是 CGNET 主链上代币的简称，前期基于以太坊 ERC20 代币发行，主网上线后 1：1 兑换至主网。



CGT 采用“交易即挖矿”的模式，将 51%的 CGT 通过交易手续费返还的形式奖励给用户，此为挖矿部分。

49%的 CGT 分配给私募机构、市场推广、创始团队及 CGT 基金会，此为发行部分。

发行部分的解锁规则：

1. 用于市场推广的部分将率先解锁 4%用于初期用户的推广及其他推广费用的支出。
2. 其它发行部分将会参照挖矿部分已挖出的比例同步解冻，每日发放。

则：实际 CGT 市场流通总量 = 累计挖矿产出 + 累计挖矿产出 * 45% + 总量 * 4%

4. 风险提示

5.1 系统性风险

系统性风险主要包括全局因素导致项目资产受影响。例如中国虽然积极鼓励区块链的发展，但是将 ICO 认为是非法融资行为，因此存在着因为政策原因导致项目投资者资产有所损失的可能性。同时，数字货币市场项目估值波动较大，因此造成投资风险巨大，请投资者理性投资。

5.2 监管缺失风险

金融市场的良性发展离不开监管制度的指定和完善，但是由于市场的发展过于迅速，导致与区块链相关的监管制度还未制定或者还达不到市场的要求，因此数字货币交易市场可能存在着暴涨暴跌或庄家操控的风险。虽然专家学者、新闻媒体等不时给出谨慎参与的建议，但是尚无明确的监管制度出台，因此此种风险也无法回避。

5.3 团队风险

当前区块链领域项目和团队众多，竞争十分激烈，因此本项目存在很强的市场竞争压力。项目能够如愿取得市场的认可，既与团队自身的能力有关，也会遭到市场其他相似项目的恶性竞争。同时，团队项目人员都是区块链领域和软件信息行业资深从业者，但是不排除项

目核心人员离开团队对于本项目造成一定负面的影响。

5.4 项目风险

区块链本质上是密码学，计算机科学，运筹学等多学科综合的艺术，因此学科的发展，尤其是量子计算机的发展等，将会对现有密码体制造成巨大的影响，因此也将对区块链项目带来潜在的安全风险；同时本项目也存在着软件行业固有的软件漏洞和 BUG，项目团队会不定期的通过更新补丁的方式进行弥补，但是无法保证项目没有任何的漏洞和 BUG。

5.5 安全风险

在现在数字货币交易市场，用户因为私钥保存不当或因为其他人为因素导致数字货币被黑客盗取的情况时有发生，虽然项目团队会通过各种方式保护用户的数字资产财产安全，但是无法避免因为用户密钥保存不当而导致的数字资产被盗的情况。同时，由于数字资产去中心化的特点，无法提供找回密码的功能，也无法通过传统的方法溯源并定位攻击者。

5. 免责申明

（1） 本文档仅为介绍项目孵化情况，文档内容仅供参考，不构成任何的买卖建议。

（2） 本文档内容不被解释为强迫参与 ICO，任何与本白皮书相关的

行为均不认为是参与 ICO。

（3） 投资项目则代表参与者已经具备民事行为能力，与本项目之间的合约是真实有效的，并且双方本着自愿的原则签订合同。

（4） 本项目将会做最大的努力确保项目设计内容的落地和实现，但是不排除未来可能因为技术革新或其他不可抗拒因素对白皮书的相关内容进行修改。项目参与者需要及时通过官方网站获取最新白皮书，并根据最新的白皮书调整个人的投资策略。

（5） CGT 作为平台的官方代币，是社区生态之间流通的重要媒介，并不是一种投资品，也不是任何种类的货币、证券、股权等。