PRESTO

WHITE PAPER

5. APR. 2018

http://presto-platform.io/

目录

摘要(ABSTRACT)

随着区块链技术开始普及，出现了在数码环境中发行加密货币并公开，利用法定货币（Fiat Currency）或加密货币（Crypto currency）筹集开发资金的新形态的筹资方式。虽然这种筹资的规模在迅速增加，但由于开发的难度较大，在开发过程中，许多团队会半途而废，因此成功率有随之降低。PRESTO提供了自动生成DAICO模式智慧契约的功能，为投资者提供保护装置，使资金能够正确使用。DAICO模式大大减少了智慧契约、权杖开发和权杖销售的成本，并帮助开发团队关注服务开发。支持开发团队集中开发服务为目标的代币销售平台。

此外，通过引入代币市场与去中心化交易所（DEX：Decentralized Exchange），PRESTO将不仅仅是构建代币销售平台，且产生新的代币，并加速现有的代币，以创建一个健康的和活跃token-sale生态系统。

1. 代币销售的现状及问题

代币销售是在区块链平台上进行的一种新型众筹方式；发行的数字资产称为加密货币，而不是股票或债券，以出售它的实际货币或其他加密货币与更好流动性[2]。

根据EY的报告，代币销售规模在短短几个月内呈指数级增长。在2017年10月至11月，该公司通过象徵性的销售，总共筹集了4600亿韩元(1074韩元/美元)两个月。代币销售虽然是创新的想法，但在现有的制度上，无法筹措足够的资金时，代币销售依然是非常有吸引力的。例如，发行BAT Coin的Brave创下了每枚BAT Coin 116万美元的纪录，而Descentalland创造了每秒募集83万美元的记录，这在现有的筹资方式下是不可能实现的。

虽然代币销售在大量的增加，但另一方面也过于氾濫;所以，在竞争上销售成本也在增加。根据报告，平均而言，成功的代币销售[3] 在开发和其他费用至少需要5亿韩元以上。此外，程序也变得越来越複杂。2017年11月1日，美国宣佈ICOs应由《证券法》[4]规定。2018年2月16日，瑞士发佈了ICOs[5]准则。此外，监督部门担心代币交易被濫用的可能性，例如:洗钱[6]。因此，在象徵性销售中还有更多的事情需要考虑。

目前代币众筹最大的问题是，投资者对他们在投资后对自己所投资的代币没有任何约束力。参与代币众筹的人们唯一能做的就是希望开发团队认真的进行开发。换句话说，当前的代币众筹需要对开发团队的信任，而与现有的制度圈不同，没有实体能够保证信任。它与区块链的哲学不相符，区块链是一个缺乏信任的机构。因此，人们越来越需要一种新型的代币众筹平台，不像区块链技术那样需要信任

另一个问题是开发一个安全有效的智慧契约并不容易。因为一旦施行，就无法修改，所以应该检讨智慧契约，使之既安全又有效率。另一方面，智慧契约中可能出现的所有问题都会影响投资者。如果没有对智慧契约进行安全程式设计，您投资者将会面临安全风险，例如在没有所有者许可的情况下发行或处理权杖，就像在分散自治组织(DAO) (Decentralized Autonomous Organization) [7]中一样。2017年11月，Polkadot团队面临以太币钱包多重签名（Parity Multi-Signature Wallet）中有漏洞，投资者们的50万ETH被永久冻结在钱包中，这可能导致项目严重中断[8]。

编写一个高效的智慧契约是一个重要的议题。低效率的智慧契约会产生大量的手续费，导致投资者和开发团队的投资损失。检查已施行的智慧契约代码，就可以看到许多开发团队忽略了这一点。

最后，还可能会出现洗钱等法律问题。韩国政府政策协调办公室主任洪南基(Hong Nam Ki)在回应青瓦台请愿[9]时表示，“在检查过程中，我们发现了通过虚拟帐户洗钱的行为，发现有些客户的钱存在于该企业员工的帐户中。”正如美国证交会主席杰伊•克莱顿(Jay Clayton)表示，“他们的加密货币活动并没有削弱他们的反洗钱和瞭解客户的义务。”[10]，当局正在密切关注加密货币市场。

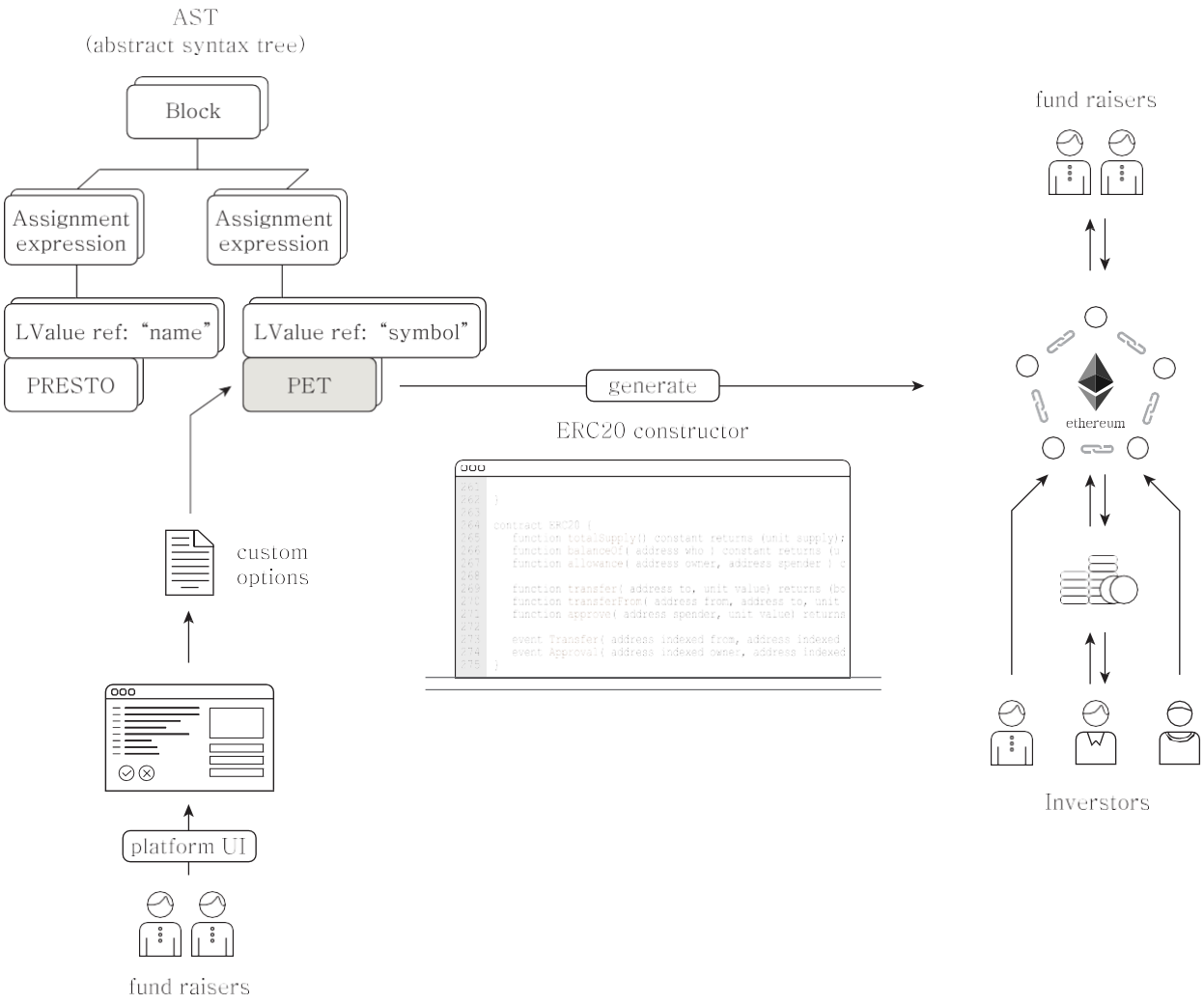
2.代币销售的未来，PRESTO平台

1. 开设简单快速的群众募集

由于大多数代币销售中使用的代币都遵循ERC20规范，因此它们之间唯一的区别是代币名称、供应量、代币销售週期和免费销售奖金等的差异，而且它们因代币生成实现的智慧契约的结构也非常相似。由于缺乏智慧契约方面的技能，一些开发团队没有投入所需的时间和金钱来安全地实现代币销售智慧契约或者验证他们创建的智慧契约，这些代币销售智慧契约是最可靠和安全的。如果我们能够很好地抽象描绘出智慧契约代码的公共部分，我们就可以自动创建智慧契约，并减少验证所需的时间。

PRESTO平台通过表单获取开发团队需要的代币基本资讯，自动生成安全高效的智慧契约[图1]。开发团队可以使用PRESTO的智慧合同自动生成技术来节省准备代币销售的时间和金钱。自动生成智慧契约是PRESTO平台的核心技术;它得到了充分的验证和有效的编写，因此开发人员将节省时间用于评审，并将时间投入到主要项目开发中。

PRESTO不仅提供了代码生成功能，而且还提供了一个简单的网页页面生成器，允许开发团队使用区块链图像轻鬆创建複杂的网站。在网页页面生成器中，就可以像众筹服务一样，通过简单的设置创建直接连接到平台的网页页面，开发团队可以通过简单的操作放置和编辑其内容。PRESTO平台尽可能地自动化和简化除开发本身之外的所有流程，允许开发团队专注于专案开发。



[图1] PRESTO platform, technical overview

2.2. DAICO模式适用

当现有的销售结束时，开发团队可以提取智慧契约中存储的所有资金，如果出现任何问题，投资者必须承担。Ethereum创始人Vitalik Buterin在2018年1月提出了一种新的代币销售模式，名为DAICO，来解决这个问题。在DAICO中，开发商不会立即从代币券销售中收回所有资金;它允许开发团队通过投票逐步收回资金。在某些情况下，资金可能会被取消，投资者会得到与智慧契约绑定的资金退款。
PRESTO还采用了DAICO模型的概念，提供了一种更安全的代币销售方法。

PRESTO平台的代币销售主要有两个功能。第一种是将象徵性销售所筹集到的资金按照预定的週期发送给开发团队，而不是一次性发送。例如，通过代币销售筹集的资金可以在代币销售结束后的三年内通过智慧契约每月发送一次。这些支付条件可以通过在代币销售开始之前填写的智慧契约内容来详细制定。有了这些条件，开发团队就可以在不丧失动力的情况下继续稳定地开发，同时也可以避免恶意欺诈

PRESTO平台代币销售的第二个功能是，当开发团队停止开发项目时，将投资于智慧契约的资金返还给投资者。参与代币销售的投资者最大的担忧是，开发团队在代币销售之后停止开发，或者收回所有资金并潜逃。这种担心是源于现有的销售智慧合同存在的问题所引起。在现有的代币销售结束时，开发团队将接管所有资金的所有权，因此投资者无法阻止开发团队暂停开发或收回所有资金。然而在PRESTO平台代币销售中，如果开发团队停止开发，剩馀的资金将通过投资者协议返还给投资者的帐户地址。实现了此功能通过oracle在智慧契约中的概念，目前大部分的代币销售智慧契约都不支持这种方法，因为它的实现难度很高。PRESTO的代币销售方法类似于Vitalik Buterin提出的DAICO模型，它将把现有的不安全、不透明的投资转变为安全、透明的投资。

2.3. 法律上安全的代币销售

反洗钱制度(AML)和瞭解客户制度(KYC)是金融机构判断客户贷款资格时必须经历的过程。著名的加密货币如OmiseGO[11]和Qtum[12]也完成了代币销售的流程。这是一个必要的过程，但它可能成为积极投资的障碍，因为它对开发商和投资者来说都非常麻烦。

PRESTO平台将提供API来简化流程，允许各种法律遵从(Legal Compliance)平台轻鬆地将其服务扩展到PRESTO。如果AML和KYC流程是标准化的，则会出现以下情况优势出现。首先，可以保护用户身分直接暴露在相关平台上，并且那些曾经通过AML和KYC流程的使用者在参与另一个代币销售时不必重複这些流程。这将为使用者提供安全便捷的服务。

3.PRESTO平台的结构

1. 代币销售平台

PRESTO代币销售平台是一个安全便捷的代币销售平台。开发团队可以在没有Ethereum或PRESTO代币的情况下，仅使用想法启动新的代币销售，并且投资者必须拥有PRESTO代币或参与乙太坊的代币销售。那麼聪明代币销售合同和网页页面可以方便地使用所提供的技术,如果开发团队在PRESTO平台上开始出售代币，投资者可看到开发团体提供的专案并决定是否参与。

代币销售主要由预售和主销售两部分组成。预售是通过提前销售代币总销量的一小部分来筹集初期的专案资金。代币总供应量和预售代币量可通过PRESTO智慧合同自动生成程式设置。投资者可以使用PRESTO代币参与预售，获得比主要销售更多的开发团队代币作为奖金。主要销售发生在预售之后，并销售其馀的代币销售数量。有关代币销售流程的资讯，如投资者的数量、售出的代币数量和资金投入，可通过PRESTO平台提供的仪錶盘查看。如果在代币出售期间成功完成代币出售，则投资者将从开发团队由PRESTO的系统自动发出，并发送到每个投资者的钱包中。开发团队可以立即收回预售资金用于初始开发成本;但主要销售所筹集的资金都安全地存放在智慧契约中，并在一段时间内分期付款。代币销售完成后，投资者可以在开发团队的智慧契约中查看剩馀资金和取款情况，从而提高资金分配的透明度。

3.2. 代币交易市场

使用新兴的区块链技术开发服务和新技术，需要开发、设计、行销和融资等多种任务。PRESTO平台不仅提供了方便的代币销售流程，还提供了一个市场，在那裡可以找到各种资源，帮助您的项目在销售后获得成功。加密货币市场中的专案分为两部分:创建新的区块链或使用现有的区块链创建新的服务。安全性是至关重要的，因为区块链技术有一个称为加密货币的概念，可以替代法定货币，这在其他IT技术中是不可用的。如果开发团队创建的智慧契约中存在漏洞，那麼他们筹集的资金可能是被骇客攻击。因此，主要的区块链专案使用漏洞奖励Bug Bounty程式寻找它们的安全性漏洞。

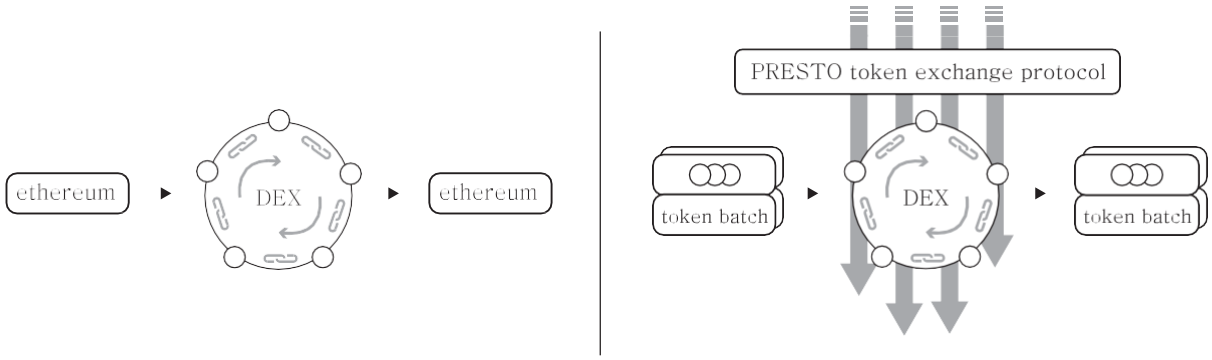
在PRESTO平台上，开发团队可以使用通过代币销售筹集的PRESTO代币启动这样一个赏金计画。当开发团队揭示了智慧契约代码和新的区块链实现代码时，区块链开发人员可以检查开放代码中的缺陷，如果他们发现任何问题，开发团队可以相应地使用PRESTO代币支付这些缺陷。通过开放赏金专案，开发团队将能够创建更安全的技术。随著开发团队巩固他们项目的技术，投资者会更加信任专案。此外，如果您在赏金计画之外还有开发、行销和设计方面的必要资源，那麼您可以指定必要的资源并使用PRESTO代币作为奖励来支付。例如，如果您需要一个插图图像来适应开发团队的网页页面，您可以在PRESTO市场中发佈需求和相应的奖励。一旦工作完成，您可以通过区块链安全透明地付款。PRESTO交易市场帮助开发团队在象徵性销售之后成功地继续完成专案。

3.3. DEX (Decentralized Exchange : 去中心化交易所)

DEX是一个在区块链平台上运行的分散式交易所。新代币很难在短时间内在大型交易所上市交易;PRESTO可以将成功完成销售的代币列在PRESTO的DEX上，迅速给予他们进入市场的机会。

通常，许多人经常使用的集中式交换使用现有的伺服器-客户机模型而不是区块链在集中式资料库中记录事务细节，并且只使用区块链。

当在处理用户或交易所外的交易所时。它的优点是能够毫无困难地处理硬币交易，为人们提供熟悉的UI/UX和快速的交易速度，但它不能利用区块链的优势，容易受到骇客攻击。与集中式交换不同，DEX在区块链上执行所有操作。它的速度很慢，使用起来也不方便，但是所有的事务细节都以块的形式记录下来，因此它是透明和安全的。PRESTO提供了一个新的DEX，通过应用扩展ERC20标准的新的代币交换智慧契约，克服了现有DEXs的缺点。该智慧协议包括PRESTO代币和代币自动生成器的设计。投资者可以通过与这些交易协定连结的直观介面轻鬆地使用DEX交易代币。

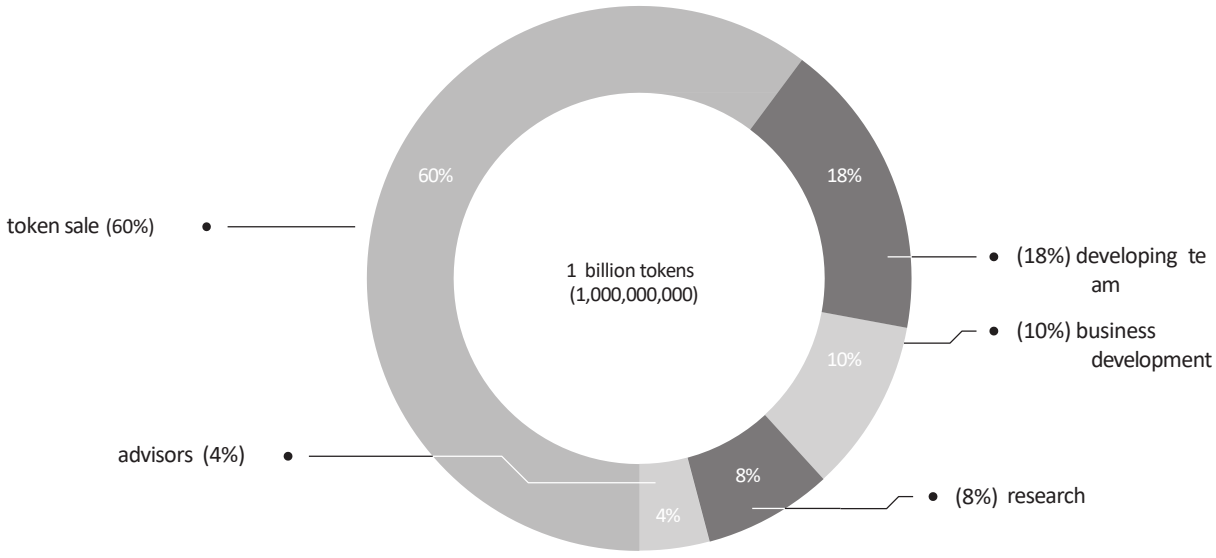


[图2] DEX(Decentralized Exchange) 设计图

4. PRESTO代币分配

为使用PRESTO的所有服务，需要PRESTO代币(PET)。PRESTO代币是作为ERC20代币创建的，所有代币销量都将发行，以便顺利分发和提供清晰的服务，得到消费者的信任。这些早期发行的代币中有60%将投放市场。18%和4%分别分配给开发团队和顾问，10%和8%预留给商业和研究用途[图3]。

在PRESTO平台，代币将不会集中于或绑定到特定的销售。他们将有一个自然的分配流程，因为其中一些是收集在象徵性销售和释放回市场。随著代币销量的增加，PRESTO代币的价值将会增加，从而抑制快速的通货膨胀和通货紧缩;它可以在经济健康的生态系统中流通。



[图3] PRESTO token distribution

5. 项目路线图

PRESTO开发团队将于2017年2月从light paper开始进行PRESTO平台的开发。2018年3月将对PRESTO平台蓝图进行更详细的描述白皮书的基础上提出的内容，公开具体的白皮书。到2019年底，我们将依次实现PRESTO代币销售平台、代币市场和DEX。PRESTO团队认为，完美无缺的安全技术在区块链服务中非常重要。因此，我们将首先开发PRESTO平台的核心技术，并对其进行充分的开放和验证，然后利用这些技术推出真正的服务。首先发佈的是代币销售平台，这是PRESTO项目的核心平台。代币销售平台的本质是一种修改后的DAICO模型的智慧契约和智慧契约自动生成器。计画在2018年第三季度公佈并全面测试核心技术，开发安全可靠的智慧合同。2019年第一季度，代币销售平台的第一个官方版本将发佈。同样，代币交易市场和DEX的智慧契约将首先公开用于验证，然后应用于实际服务。未来的平台开发计画将通过网页公佈。

6.其他事项

PRESTO light paper是对发展计画和愿景的描述，并不是业务项目内容的保证。应该指出的是，实际进展可能因业务环境和发展状况而异。PRESTO代币不能用于除在light paper中描述的目的之外的其他目的。PRESTO代币不是股票，而且PRESTO代币的持有人不被授予任何股息或投票权。PRESTO团对此不承担其法律责任。根据light paper下，您採取的任何行动都具有风险，结果取决于您的判断。

Reference

1 https://www.coindesk.com/vitalik-new-idea-icos-tested/

2 https://www.nytimes.com/2017/10/27/technology/what-is-an-initial-coin-offering.html

3 https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos

4 https://www.financemagnates.com/thought-leadership/much-money-need-launch-ico/

5 http://decenter.sedaily.com/NewsView/1RVRJ4BEFE

6 https://www.cnbc.com/2017/08/04/icos-may-be-seen-as-securities-by-u-s-and-singapore-regulators.html

7 https://www.coindesk.com/understanding-dao-hack-journalists

8 https://blog.springrole.com/parity-multi-sig-wallets-funds-frozen-explained-768ac072763c

9 http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=100&oid=018&aid=0004035589

10 Testimony on "Virtual Currencies

: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission"

11 https://cdn.omise.co/omg/whitepaper.pdf

12 https://qtum.org/en/blog/qtum-crowdsale-update-timeline

* 所有网页的资料均以刊登在2018.02.26中的内容为准。

Team Members

Kyung Won Kang
CEO and Co-Founder
Formerly Ponple CTO
Formerly Neople Client Developer & Part Manager
Released Indie Game "Cross Set" "Cross Set Infinity" on Steam™
Seoul National University (Dept of Mathematical Sciences)

Kyle Bae
Global Strategy Manager
Formerly Doil Trading Corp., Director of Overseas Manager Formerly Investment Visa Consultant
Formerly Huatai Property Company
Seoul National University (M.S in International Sports Management) University of Minnesota Twin Cities

Wonse Kim
Developer
Python, C++ Developer
Mathematics Technology Laboratory Researcher in Seoul National University
Specialized in Data Analysis Using R, MATLAB and Published 3 SSCI Papers
Seoul National University (Ph. D in Mathematical Sciences)

Chang Woo Choi
Business Strategy Manager
Qualified as Patent Attorney in South Korea
Seoul National University (Dept. of Mechanical Engineering)