

Stmenu证券型通证产品发行S-Token标准白皮书

Roger Chu, Helen Zhu, and David Ye

V1.0版本 2018.9

项目摘要

证券型通证ST产品（STO）是解决token销售合法性的解决方案，为初创公司和新的区块链企业向投资者提供证券法监管下的金融产品而不违反证券法。Stmenu 致力于建立一个去中心化分布式合规协议，以标准化方式在区块链上进行证券型通证的发行和交易。S-Token是STmenu团队开发的一个开源标准机制。在这个机制中证券型通证Security Token(下称ST)产品在以太坊区块链上发布ERC-1400 token，以符合链上相关监管机构标准获得交易批准。监管机构标准包括不限于符合相关证券法规、了解客户(KYC)政策、反洗钱(AML)要求、税法等，S-Token标准使ERC-1400 token成为兼容的加密证券，可以在任何ERC-1400兼容平台上进行交易。

1、项目背景

区块链技术创造了一个不可篡改的分布式账本，这将改变证券交易市场的现有格局。该技术可以简化所有权的转移，创造透明度，减少交易成本，并提供更大流动性。凭借流动性，投资者可以灵活地按照市场价出售私人证券，增加市场流动性并为发行人释放更大的潜在资产价值。目前来看包括但不限于以下资产类别可以受益：房地产投资基金的有限合伙人

（LP）权益、土地/建筑物的部分所有权、私人房地产投资信托基金、公司股权/分红权、字画作品所有权/收益权、音乐作品所有权/收益权等。

然而，流动性也给发行人和投资者带来了重大的监管挑战。私人证券必须符合适用法律的豁免规定，以避免繁琐的公共申请要求。这些豁免可能需要限制总投资者的数量，只允许特定类型的投资者（即合格投资者）实施控股期间，并应用许多其他规则。限制因司法管辖区域而异，并且要求遵守发行人的管辖权以及每个投资者的管辖权。此外，这些限制不仅适用于首次发行（发行人承担很多责任），也适用于对卖方负责的所有二级交易。

仅以美国为例，私人证券发行必须符合1933年“证券法”和1934年“证券交易法”（在某些情况下还要符合1940年的“投资顾问法”和1940年“投资公司法”）中的豁免条件，以避免公开申请和其他昂贵且操作上禁止的要求。例如，在许多情况下，房地产投资基金的LP权益所有者可以依赖1933年证券法第144条进行二级交易。这将要求卖方遵守规则144a规定的一年持有期或仅与合格机构买方进行交易。此外，根据1933年“证券交易法”、1934年“证券交易法”和

1940年“投资公司法”，首次发行的发行人还必须继续获得豁免，除其他外，该法可能要求限制认可的数量和非认可的投资者。

执行这些监管要求对于采用区块链技术进行私人证券发行具有重要作用。在本文中，我们使用S-Token标准提出了这种合规性挑战的解决方案。通过使用正确的规则实施S-Token标准，私有证券可以符合监管要求等方式在区块链上发行、交易。

2、传统证券资产TOKEN化

发行私人证券的主要原因之一是初始发行的相对容易性和成本效益。但是私人证券的二级市场交易往往需要各种中间人（如经纪人和交易所）。此外，跟踪贸易活动过程繁琐且成本高昂，发行人有很大的负担来防范潜在的监管风险。这些效率低下通常会导致受害者施加贸易限制，使私人证券流动性不足。为了解决缺乏流动性问题，私人证券的价值被贴现（即“非流动性折扣”），阻止发行人获取相关资产的全部价值。

相比之下，公开发行证券产品可以拥有深度市场和高流动性，因为非控股持有人通常可以自由转售。然而，IPO是时间和成本较高、过程很复杂，通常需要12到18个月的准备时间。不仅发行本身成本较高，作为上市公司的整个持续流程，包括严格的监管和披露要求都比较严格。

通过对私人证券产品进行TOKEN化，我们可以将它们从低流动性/高成本效益转移到更高流动性/更高成本效益。证券型通证ST产品（即加密证券）可以更容易地在二级市场上交易，而不需要传统私人证券中间人。换句话说，证券型通证ST产品可能具有更多的流动性，同时保持其成本效益。

鉴于私人证券市场中的资产类别具有数万亿的资产规模，非流动性折扣可能高达20-30%，证券型通证ST产品具有数千亿美元的市场规模。

除了提供流动性之外，对私人证券进行TOKEN化也为提高效率创造了机会。区块链使交易能够在没有中间人的情况下在两方之间安全地进行。它是一个不可篡改的分布式账本，每项事务都会自动记录并易于审计。结算和清算交易的过程和时间表也可以大大缩小，任何和解程序都可以大大简化。对私人证券进行识别有可能显著降低成本，提高结算速度并提高安全性。

而解决这些要求实现在区块链上采用证券TOKEN化改造的基本前提就是要符合在不同国家/地区范围内的法规要求。

3、仅以房地产为例

我们的世界充满了资产：股权、房地产、黄金、碳信用额、石油、美术作品、音乐版权等。其中许多资产难以实际转移或细分，因此买卖双方交易代表部分或全部资产的纸张。但纸质和复杂的法律协议繁琐，难以转移，难以追踪。一种解决方案就是将资产TOKEN化切换到数字资产系统，合规前提下在世界范围内流通交易。

在各类私人证券中，对房地产资产进行标记可能会提供特别有吸引力的机会。截至2016年，仅专业管理的全球房地产价值为7.4万亿美元，全球所有发达房地产价值约为217万亿美元。由于多年稳定的就业增长和经济增长的推动，美国房地产市场因其相对稳定性而继续对外国投资者具有吸引力。这为全球投资者提供了投资组合多样化并在其原籍国之外产生回报的能力。

房地产资产还有其他法律要求（除了已经很复杂的安全法规之外），必须加以执行，这使其成为区块链标记化的理想选择。例如，私人国内控制的房地产投资信托（REIT）限制非美国投资者集体拥有超过50%的股份，允许最多五个人集体拥有超过50%的股份，并要求最低限度100名直接股东。此外，根据1980年“外国投资房地产税法”（FIRPTA），这些私人国内控股房地产投资信托基金的外国投资者须缴纳30%的股息预扣税。

公开上市的房地产投资信托基金（REITs）提供了一些流动性，但它们设置起来很昂贵，并且通常持有一篮子房产而不是单一建筑物。此外，大多数投资者完全被排除在开发项目之外，除非他们能够达到通常大约25,000美元或更高的最低标准。有一天，您也许可以购买帝国大厦等单一商业房地产资产10美元，或投资100美元开发LEED认证住房项目。以房地产为重点的token交易将增加资产所有者的流动性。

也许融资模式会出现在您可以对您的房屋进行TOKEN化而不是取消传统抵押贷款的情况下。您将向token持有人网络付款，而不是支付抵押贷款。也许我们会在未来几年看到这样的版本出现。

4、S-Token标准

证券型通证产品发行准解决了二次转移合规性的需求，它建立在ERC-1400之上，同时兼容ERC-20所有功能。如果没有标准，监管机构，开发商，KYC提供商，投资者，发行人，钱包和交易所就无法在同一框架内共同合作，并创建一个功能性的STO生态系统。

S-Token标准在现有区块链生态系统广泛支持的标准下在ST产品级别中嵌入合规性，允许在支持ERC-1400、ERC-20 token的任何平台上进行私募证券的分散交易。与限制单一集中交

易的交易模式相比，这显著增加了流动性，并且符合不同国家/地区的合规监管规范要求。集中交易可以在有限的程度上执行监管要求，包括KYC，AML和认证。

然而一旦离开该交易所，发行人可能无法执行核心证券法规，例如限制投资者数量，需要最少数量的投资者，以及规定所有权水平。我们提出的S-Token解决方案无论交易是在集中交易还是分散交易中，都会强制执行不同国家/地区监管机构的合规规范要求，从而满足核心证券要求。

S-Token标准包括以太坊区块链上的三个核心服务：（1）S-Token，（2）监管机构合规服务，以及（3）注册机构服务。虽然所有三项服务都可以作为单一智能合约实施，其中监管机构服务和注册机构服务功能已内置于S-Token智能合约本身，但本白皮书将以三种不同的智能合约的形式举例说明这些服务的实施。随着监管机构条款的不同以及不同国家/区域的监管内容不同，S-Token智能合约可以方便地进行升级。

S-Token是一种经过许可的ERC-1400智能合约，可以代表安全的所有权。它与所有支持ERC-20标准的现有钱包和交换机兼容，但它优先于现有的ERC-20传输方法，以检查链上调节器服务以进行交易批准。

每次启动传输时（例如A想要将令牌转移给B），S-Token从ERC-1400中指定的transfer（）2和transferFrom（）3方法中调用RegulatorService #check（）方法。如果检查成功，则转换按照ERC-20规范正常进行（即令牌从A转移到B）。此外，transfer（）和transferFrom（）方法提供了成功的CheckStatus事件。

如果检查不成功，则transfer（）和transferFrom（）方法返回错误代码（即从A转移到B失败），并使用原因代码传递不成功的CheckStatus事件。第三方钱包提供商可以使用CheckStatus事件来指示不允许交易的原因。

在转移令牌需要调解员的情况下（例如，在分散交换中），调用approve（）4方法以将来自令牌所有者（例如A）的资金分配给调解者。一旦分配，调解员就会启动传输序列。

注意：可以实现approve（）方法以包含额外的check（）方法。这意味着从token持有人向调解员分配资金需要得到监管机构服务部门的批准。S-Token标准的初始实施不包括此额外检查。

5、监管机构服务

Regulator Service接口包含一个check () 方法，该方法在transfer () 和transferFrom () 方法中调用。此检查包含转移期间提供的所有信息：

```
contract RegulatorService {  
    function check(address _token,  
        address _spender,  
        address _from,  
        address _to,  
        uint256 _amount) public returns (uint8);  
}
```

为了提供具有交易批准（或不批准）的S-Token智能合约，监管机构服务必须包括已批准参与者的白名单，其交易权限和额外的token交易设置，使其满足相关的证券法规、KYC政策、AML要求、税法等。

监管机构服务的初始实施包括两个参与者级别的权限和两个token级别设置。这些权限和设置可用于满足单个监管辖区内私人证券通常要求的交易规则。

两个参与者级别的权限是：1) 发送token的权限，以及2) 接收token的权限。区分发送和接收许可允许更大的灵活性（例如，如果认可的投资者购买token但后来失去认可的投资者资格，则该参与者可以发送token，但不能购买新token），由离线交易控制器确定这些参与者级别的权限（通过查看参与者数据，如居住国、KYC / AML状态、纳税状态、认可投资者状态等），并将结果写入监管机构服务数据。

调节器服务初始实施中的第一个级别token设置是锁定/解锁传输。此设置允许执行持有期，例如，如果根据Reg. D签发token并因此受到一年的持有期限，则可以在此期间锁定token。

第二级别token设置允许/不允许令牌的部分传送，设置可以限制令牌持有者的总数。例如，如果在产品中仅允许最多1000个token持有者，则只要不允许部分传输，就可以发出总共1000个token。虽然这种方法为投资者创造了流动性，但它也不可避免地会增加每个token的价格，使小投资者难以参与。

限制token持有者数量的另一种方法是仅允许转移参与者的整个余额。在这种情况下，为了将token持有者数量限制为1000，可以在最初STO期间向1000个参与者发放无限数量的token。但是，具有50个token的参与者将被要求一次交易所有50个token，降低流动性并且每次在现有token持有者之间进行交易时永久减少token持有者总数。第三种方法可以允许部分交易发生，直到达到最大投资者数量，此时仅允许转移参与者的全部余额。这种方法可以

改善流动性，同时可能减少最小投资规模，但交易规则的变化可能会在投资者中产生一些混乱。

注意：S-Token标准提供了一个开发人员可用于实现自定义业务逻辑的接口。Stmenu计划实施的监管机构服务将包括其他设置，以便在细化层面上强制执行多个司法管辖区域的监管要求。

6、服务登记机制

Service Registry为S-Token智能合约提供了一种机制，用于定位当前，正确或所需的Regulator Service版本。Registry为S-Token提供适当的Regulator Service地址；然后，S-Token检查给定的监管机构服务以获得交易批准。

当引入新版本的Regulator Service时，Service Registry会将更新的Regulator Service地址提供给S-Token。这可确保使用正确的调节器服务进行交易批准。

注意：S-Token标准提供了一个开发人员可用于实现自定义业务逻辑的接口。Service Registry的其他接口允许多个监管服务同时接入，从而可以满足不同国家/地区合规方面的监管服务规范要求。

7、交易控制器机制

监管机构服务的初始实施依赖于离线交易控制器来更新其权限以及添加新批准的参与者。交易控制器确定权限的状态，它根据相关证券法规，KYC / AML政策和税法将参与者数据映射，以确定每个参与者是否可以发送和/或接收token。它还确定token是否被锁定/解锁以及是否允许/禁止部分交易。然后在Regulator Service中更新这些令牌级权限。

只有具有正确私钥/公钥对的经批准的交易控制器才能更改监管服务。

注意：Stmenu将是第一个初始实施S-Token标准的交易控制器实施方案。

8、结论

我们提出了一个开源标准用于在区块链上顺利转移加密证券，只有当它们被监管机构服务批准时，才使用S-Token标准进行实现token转移。监管机构服务包含法规遵从所需的权限，并依赖于脱链交易控制器来设置和更新这些权限。为了满足监管条款的不断更新，我们还建议使用服务注册表以便于升级。通过正确的规则集实施，S-Token标准使ERC-1400令牌成为可以在任何ERC-1400兼容平台上交易的兼容加密证券。

这是制定加密证券分布式合规管理的第一步。它解决了在区块链上转移私人证券的核心挑战，使我们更接近加密证券的扩散。

免责声明

本白皮书（“白皮书”）旨在描述Stmenu Platform Inc.（“Stmenu”）目前预期的开发新区块链token机制（“S-Token”）的计划，该机制将是一个开源标准这定义了一种机制，在这种机制中，证券型通证ST产品可以在区块链上顺利转移（“S-Token标准”）。本文档中的任何内容均不应被视为或作为S-Token或S-Token标准将如何开发的保证或承诺，或S-Token或S-Token标准的效用或价值的保证或承诺。本白皮书概述了Stmenu目前的计划，该计划可能会自行决定改变，其成功将取决于Stmenu控制范围之外的许多因素，包括基于市场的因素以及数据和加密货币行业的因素等。有关未来事件的任何陈述仅基于Stmenu对本文档中描述的问题的分析。具体开发运营情况依据项目实际进展而定。

团队介绍

Roger Chu, Stmenu, Founder & CEO

毕业于复旦大学法学院，获硕士学位。曾担任多家律所CEO，法律互联网公司CEO。学习能力强，对新事物具有强大的好奇心和发展方向的判断能力，同时又能立足现实，具有丰富的管理经验。

David Ye, Stmenu, Co-Founder & CTO

毕业于北京大学计算机系，获学士学位，研究生毕业于国防科技大学，获硕士学位。曾担任WebEx Director of engineering, Cisco资深研发总监。

Helen Zhu, Stmenu, Co-Founder & CLO

先后毕业于复旦大学法学院，法律硕士，Chicago Kent College of Law 金融法律硕士，Seton Hall Law School法律博士，并创立美国和泽律师事务所，在STO方面有深入研究。

Timon Tang, Stmenu, Co-Founder & CMO

先后毕业于台湾交通大学，获学士学位，中国政法大学，法学博士学位，擅长演讲及市场开拓，曾担任某国际律所港澳台法律专业委员会主任，上海金山区两岸青年创业基地创新育成中心副主任。