



PAXOS STANDARD

白皮书

v1.0

最新更新：2018年9月9日

作者：Charles Cascarilla

最新版本，请访问：<http://standard.paxos.com/whitepaper.pdf>

目录

摘要	2
货币的职能	2
信任在货币体系中的重要性	3
历史背景	3
信任与数字资产	4
PAXOS STANDARD	5
基本要点	5
主要的产品特性与优势	6
早期用例	6
长期效用	7
经济意义	8
技术	9
监管	11

摘要

货币的概念已经演化了数千年之久，但仍存在改进的空间。目前，数字资产在全球流动性、无摩擦、民主化方面的潜力尚未完全实现。尽管相关项目激增，并获得了数十亿美元的资金支持和多年的开发投入，但就算是比特币这一领先的数字资产也仍因种种问题使其效用受限。

在这份白皮书中，我们将介绍Paxos Standard™ 代币。由Paxos 信托公司发行的Paxos Standard是获得了纽约州金融服务管理局（New York State Department of Financial Services）批准和监管的新型数字资产，按与美元1:1的比例全额抵押。本文对Paxos Standard能给金融市场带来的优势进行了阐释。即，Paxos Standard能够让参与者受益于区块链技术和金融监管机构的监管，让其使用可信赖、安全、由美元担保并计价的资产进行交易。

我们相信Paxos Standard代表着数字资产的显著发展。其在充分利用了传统金融系统的基础设施、监管与稳定性的同时，让交易与互联网同速。

货币的职能

货币具有三大职能：交换手段、记账单位与价值储藏。在某种程度上，数字资产旨在改进上述职能，开启“可编程货币”和智能合约时代。但是，到目前为止还没有任何数字资产能够通过足够优越的方式真正改进上述3种职能。其主要原因在于数字资产的波动性。

作为交换手段，数字资产还未得到普遍使用；相反，它们目前大多被用于投机目的。然而，那些专门被设计用作交换手段的数字资产却很少被人们接纳使用。在可用性、普遍性或易用性上的欠缺导致这些数字资产无法得到广泛使用。

作为价值单位，大部分数字资产的价值波动过大，无法被视作是对许多标准法定货币的改进。在过去2年中，比特币在itBit交易所中相对于美元的最高价为19,720美元，最低价仅为593美元（见下图）¹。这种持续走势更偏向于一种波动性商品，而非稳定的货币。

¹<https://bitcoinity.org/markets/itbit/USD>



作为价值储藏，相对于长期内不断贬值的法定货币，部分数字资产（如比特币）可能代表着显著的改进意义。但是，其波动性意味着即使它们在这方面的有所作为，但表现也并不尽如人意。

从根本上看，大部分数字资产未能实现货币的3个基本职能，而其中根源就是其波动性。（因为几乎不像货币，大部分数字资产已经从其最初的“加密货币”改名为“加密资产或数字资产”。）

不过，有一类数字资产专为解决波动性问题而生，并被恰如其分地称作“稳定币”。这是一种相对较新的货币，旨在长期保持一致价值。虽然稳定币获得了一些青睐，但现有模型缺乏一个让它能够获得广泛的重要基本特征：信任。

信任在货币体系中的重要性

历史背景

和现在相比，早期的商业活动具有更多种多样的形式。最开始的易货制在封闭的小型社会内运行良好，任何交易仅需双方就货物的同等价值达成一致意见即可进行交易。货币最终由于其更加便于携带、不易受到损坏但本质上能体现价值（例如金币）取代了这一形式。之后的发展则需要人们信心的巨大飞跃。

从金币向本质上无价值的货币代表物（例如纸币或简单的记账）的转变，需要多种形式的信任：信任该体系能够让货物与服务相对于货币保持公平的市场定价，信任广泛的市场参与者能够遵守一系列新的运营原则。人们再也不能单独简单地达成用鸡换面包这种看似公平的交易了；新的规则要求除交易双方以外的更广泛社会群体都普遍认同对某一货物的价值。

在考虑货币体系内的集体信任问题时，成功的货币体系必须由政府颁布的原因显而易见。中央机关可以控制货币供应与货币价值，确保其足够稳定，以便让所有市场参与者都获得其效用。政府还可以打造法律框架，让公民在框架内开展交易。在一个有限、明确且足够大的总体市场（一个国家）、中央权威和问责制（管理机构与法律）的环境中，所有市场参与者（公民）都可以放心地对该系统和彼此保有一定程度的信任。这是数千年来支撑货币的原则，而这些原则已经成为所有现代国家都在使用的法定形式。

信任与数字资产

信任是设计如何运作基于区块链的数字资产的核心理念。区块链上的代码基于规则而且难以更改。针对区块链的所有更改都会以分布式方式被记录在案并进行确认，将访问权归于民众。区块链并非使用可靠的介质促进交易，而是被用作可信赖、由共识来驱动的协议。

比特币最大限度地采用了分散化概念，完全没有中心化主体对其进行监督，甚至连声称知道其创始人真实身份的人都少之又少。但是，即便如此，屈指可数的核心开发者（数十人负责定期提交代码）与矿池（不到10个）表明这种平等主义精神在事实上仍相当集中，尽管法律上可能并非如此。

尽管信任被不断分布到网络之中，但数字资产仍未获得公众的广泛信赖。由于大部分人并没有直接接触过代码或并不了解区块链是怎么运作的，数字资产的去信任特性依然不为人所信。

与此同时，许多人对于数字资产不具有任何固有价值或不与法币挂钩而感到困惑。此外，波动性让这些数字资产看起来更像是投资工具而非支付方式。

相比传统金融中已经存在的监管、监督、审计、保险等严格体系，数字资产生态系统中的控制措施仍显得苍白无力。由于这样的数字资产体系尚处于初期阶段，传统资产仍然更为人所信赖。

PAXOS STANDARD

区块链技术带来了非凡创新：分布式帐本、分散化信任、智能合约等等。但这些创新并未对影响货币特征的基本原则起到改进作用，也没有建立能实现大规模普及所需的公众信任。

Paxos Standard旨在充分利用区块链技术的创新，改进货币职能，并通过传统基础设施确保其值得信赖。换言之，作为一家受到监管的信托公司和一个发行与美元挂钩代币的金融机构，Paxos所发行的代币，能够结合法定货币的信任、稳定性与数字资产的可用性、时效性。

基本要点

Paxos Standard（或者PAX）是一款由Paxos发行且按与美元1:1的比例全额抵押的代币。PAX可按与美元1:1的比例购买和赎回。一经赎回，PAX立即被销毁；PAX只有在相应美元受到托管时才会存在。

作为一家根据纽约州银行法（New York State banking law）组建并受到纽约州金融服务管理局（the New York State Department of Financial Services）监管的信托公司，Paxos根据现行的最高标准开展运营。与使用客户资金获取自身收益与融资的银行不同，信托公司是保管客户存款的受托人，因此将始终确保客户的资金得到全面的保护。所有美元现金押金均存放在美国联邦存款保险公司（FDIC）承保的美国银行，或由美国政府国库提供抵押，客户资金全部被作为客户财产记录入账。

换言之，Paxos接受美元存款并发行Paxos Standard 代币。该代币可以无摩擦地轻松进行交换、交易与转账。数字资产经济具有流动性、全球性和快速的特点。但由于传统银行系统的固有延迟，数字资产和法定货币交易目前仍阻碍重重。Paxos Standard可以让用户在便捷拥有数字资产的流动性的同时，确保数字资产的稳定性。

在各个职能方面，Paxos Standard等同甚至优于法定货币。Paxos Standard更易于交换，能够保持相同的记账单位，并能提供相同的价值储藏。由于完全以美元为担保并得到受监管的金融机构的支持，Paxos Standard是一种改进的货币模型。

主要的产品特性与优势

- Paxos Standard 代币由Paxos发行和赎回。作为一种信托财产，Paxos直接发行PAX，无需任何中间人。这样可以实现更高效的操作，包括缩短赎回窗口（PAX可以在一个营业日内被赎回为美元），降低费用。
- 拥有以太坊（Ethereum）钱包的任何人均可发送或接收PAX。所有交易都能够在遵守ERC-20协议的以太坊平台上遵循智能合约规则进行。智能合约能够消除交易过程中的人为错误，让该系统仅按照编程方式运行。
- PAX将在全球交易所上市。由于与美元等值挂钩，PAX可以用于了解其他数字资产所对应的美元价值。
- Paxos交易所的itBit 将可根据用户的选择立即转换为PAX，而非现金。itBit还可以交易PAX OTC。
- PAX可24/7全天候使用，便于对任何资产类型（包括加密货币、证券与资产代币）进行结算或用于支付。与仅可在银行营业时间内结算交易的法定货币不同，PAX可以随时随地流通使用。
- PAX基于以太坊区块链，是一款可参与到全球更大代币社区之中的可编程代币，有助于打造一个具有稳定性的可编程货币全球平台。

早期用例

数字资产目前仍处于发展阶段，Paxos Standard初期的应用场景和其未来的会有所不同。目前，我们认为最快将被采用的用途如下：

- 作为基于区块链的其他资产（包括加密货币、资产及证券代币）的支付手段。对于基于区块链的资产而言，在可靠的时间节点高效推进交易是最复杂、最困难的问题。
- 在波动时期作为对冲手段兑换为稳定资产。进行数字资产交易的投资者可以通过PAX持有资产，减小数字资产波动性风险，从美元的稳定性中受益，且不会在转换法币时产生任何费用及延迟。
- 以更低的波动性执行更复杂的可编程数字资产交易。基于ERC-20协议并得到以太坊智能合约支持的PAX，旨在处理复杂的交易条款与条件，并在更广泛的代币生态系统内运行，降低波动性风险。

- 在传统的银行营业时间之外与法币进行资产结算。金融机构与交易公司可以24/7全天候使用PAX结算交易中的现金部分。
- 代替不受监管或不稳定的加密资产，帮助数字资产托管人和交易参与市场交易。

长期效用

资产流动性与结算

代币化的美元解决了数字资产与法定货币间的摩擦。由于银行的限制，将数字资产兑换为法定货币需要花费时间和金钱。相比之下，Paxos Standard作为加密资产的基底，无需通过美元即可实现PAX和其他数字资产之间的实时结算。换言之，Paxos Standard能够高效地对数字资产交易中现金部分进行结算。因此，经常进行交易的交易者将更加乐于将现金兑换为PAX而非美元，获得更高的可用性与流动性。在未来，Paxos Standard可以帮助各类资产实现无摩擦的流动和快速结算。这些资产不仅包括数字资产，还包括大宗商品、证券、房地产、甚至艺术品与收藏品等更具专业性的资产。

生态系统开发

首先，PAX将作为结算方式在数字资产交易所和大型OTC上线。二者都将为客户提供PAX并对其即时需求进行相应。

在此之后，其他类似的进行高频或大量交易公司也会看到PAX所具有的低费用以及即时低风险结算的优势。这些公司包括支付服务提供商、金融机构、寻求降低跨境内部交易费用的大型跨国公司和大型零售商。这些也会提高个人用户对PAX的兴趣。

经济意义

Paxos Standard的潜力远不止于此。Paxos Standard代表的是实现便捷、实时资产流动且价值稳定一致的可信数字资产。以此为基准，PAX这一新型数字资产在影响全球贸易与商业以及打造无障碍通道方面拥有无限潜力。以下是其中的部分可能性。

基于区块链的通用支付系统

Paxos Standard可用作基于区块链的全球通用支付工具。作为基于以太坊区块链技术的ERC-20代币，Paxos Standard能够被广泛用于各种应用场景并在全球范围内即刻使用。与以往发行新币不同，Paxos Standard与现有币种挂钩更具可接受度和可信赖性。Paxos Standard旨在加强法定货币或数字资产等所有资产的可兑换性与可流动性，为各资产类别内以及跨资产类别的交易提供通用支付服务。具有灵活度、速度和全球性的Paxos Standard将在全球交易所上线。它所具有的全球效用将能够让美元成为全球通用货币。

国际交易与汇款

Paxos Standard可用作全球通用支付工具，减少目前跨境汇款和全球交易及贸易中产生的国际支付摩擦。Paxos Standard可以从根本上消除跨境交易费用，提高商业与贸易的流动性。单单这一项对现有系统的改进就能够消除数十亿美元的外汇交易费用。

消费者的采用

在未来，大量消费者很可能将Paxos Standard用作主要货币。根据美联储发布的《2017年美国家庭经济状况报告（Report on the Economic Well-Being of US Households in 2017）》，在2017年，约5%的美国成年人（1300万人）没有支票、储蓄或金融市场账户（通常被称作“无银行账户”）²。此外，在美国境外很多群体受到法币波动的影响，抑制了他们创造保留价值或规划未来的能力。Paxos Standard将能够为这些人提供在其他环境下无法获得的经济自由。

²<https://www.federalreserve.gov/publications/files/2016-report-economic-well-being-us-households-201705.pdf>

技术

简单性是Paxos Standard 代币的设计初衷之一。用户每兑换1美元，Paxos即发行1个PAX。同样，用户可用1个PAX赎回1美元。兑换将始终按与美元1:1的比例完成。如此简单的特性让整个系统可以被编写为基本的智能合约，确保其以可编程方式按照规则运行。（尽管该代币目前基于以太坊区块链技术，但我们可以看到PAX在区块链跨平台未来中的潜在价值。）

Paxos Standard遵循以太坊上的标准ERC-20协议。以太坊是一个基于区块链的分布式账本，支持超过10万份智能合约，是使用最广泛的数字资产平台。智能合约是数据（例如账户余额表）与搭配该数据使用（例如用于账户间余额转账的编程程序）的编程程序组合。支撑以太坊区块链的分布式一致性协议确保了数据的完整性与程序执行的保真度。

ERC-20代币是以太坊智能合约，遵循用于在区块链上表示自定义“代币”的标准协议。具体来讲，合约必须表明基本的代币特征（名称、符号、十进制精度）、跟踪代币总量、跟踪每个以太坊地址跟踪代币余额、并允许地址所有者将其余额的一部分转移到其他地址³。

由于Paxos Standard遵守标准的ERC-20协议，大部分支持以太坊的交易所及钱包应用已经嵌入了支持对PAX进行查看和转账的相关功能。虽然PAX的初期代币发行与赎回经由Paxos完成，但其他任何PAX交易均遵守按照ERC-20规范而编写的智能合约，其依赖于网络而非任何中间人。

Paxos Standard ERC-20合约代码（详情请见<https://github.com/paxosglobal/pax-contracts>）支持技术审查，因此任何人都可以检验代码是否按Paxos的描述运行。由于该1:1模型极其简单，Paxos Standard可以视为一种简单、可读的智能合约。独立第三方的智能合约安全性审计确保PAX能够实现稳健安全的交易执行。

³关于ERC-20规范，请参见：<https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>

总而言之，以太坊上ERC-20合约的优势为：

- 拥有全球最大规模区块链网络之一（以太坊）所提供的安全性与可用性
- 得到了数字资产权益方（例如交易所、数字资产组织、机构投资者与零售用户）的广泛采用
- 相对简单且为人熟悉的智能合约模式
- 公开可检验的代币供应、账户余额与链上程序

监管

从一开始，Paxos 信托公司就致力于通过强大的第三方监督实现高度透明。因此，Paxos 一直是区块链相关公司在监管合规方面的领军者。作为首家在数字资产交易领域受到监管的信托公司，Paxos 将继续与监管机构及现有金融服务生态系统内其他各方密切合作。

监管审批

Paxos 是受到纽约州金融服务管理局（the New York State Department of Financial Services）直接监管、并在其监管下运营、依照的纽约州银行法组建的信托公司。以上监管能够实现多项消费者保护，其中包括大量资本准备金要求、对我们运营程序的频繁监管检查与监督。Paxos Standard 代币已得到纽约州金融服务管理局（the New York State Department of Financial Services）批准，并继续受其监管。

资金存放于美国联邦存款保险公司（FDIC）承保的银行内

Paxos 将所有客户的资金存放在由美国联邦存款保险公司（FDIC）承保的银行的独立账户中。

审计

Paxos 与第三方、独立、可信赖、全美顶尖的公共会计事务所合作，进行月度审计并证实 Paxos Standard 代币按照与美元 1 : 1 的比例全额抵押担保。

此外，Paxos Standard 智能合约已经获得了领先区块链审计机构（Nomic Labs）的[审计](#)，以确保代码安全稳健，并按照计划及宣传的方式运行。

交易的监控与监督

第三方区块链情报公司 Chainalysis 会针对欺诈的检测和预防进行持续的交易监控与风险评估。

由于 Paxos Standard 基于以太坊区块链，任何人都可以轻松审查链上的全部交易记录。