PAXOS STANDARD

WHITE PAPER

v1.0
last updated September 9, 2018
written by Charles Cascarilla

The latest version is available at http://standard.paxos.com/whitepaper.pdf

Table of Contents

ABSTRACT **2**

THE FUNCTION OF MONEY **2**

THE IMPORTANCE OF TRUST IN MONETARY SYSTEMS **3**

Historical Context 3

Trust and Digital Assets 4

PAXOS STANDARD **5**

Basics 5

Key Product Features and Benefits 6

Early Use Cases 6

Longer Term Utility 7

Economic Implications 8

Technology 9

Oversight 11

ABSTRACT

The concept of money has evolved over thousands of years, and yet there is still room for improvement. The promise of digital assets—global fluidity, frictionless, democratized—has not been fully realized. Despite the proliferation of projects, billions of dollars of resources and years spent in development, even the leading digital asset, Bitcoin, is still plagued by significant issues that limit its utility.

In this paper, we introduce Paxos Standard™ token, a new digital asset that is fully collateralized one-for-one by USD, issued by the Paxos Trust Company and approved and regulated by the New York State Department of Financial Services. We explain the advantages that Paxos Standard brings to financial markets, allowing participants to transact in a trusted and secure, USD-backed and denominated asset with the benefits of blockchain technology and the oversight of financial regulators.

We believe that Paxos Standard represents a significant advancement in digital assets, leveraging the infrastructure, oversight and stability of the traditional financial system, while operating at the speed of the Internet.

THE FUNCTION OF MONEY

Money is defined by three main functions: means of exchange, unit of account and store of value. In part, digital assets were created to improve on these functions, ushering in an era of "programmable money" and smart contracts. However, none have truly succeeded in improving all three functions in a superior way, primarily due to their volatility.

As a *means of exchange,* digital assets are not commonly used; rather, they are largely used for speculative purposes. Those more specifically designed to operate as a means of exchange have achieved low adoption. There has just not been enough utility, ubiquity or ease of use for widespread usage.

As a *unit of value,* most digital assets have values that fluctuate far too greatly to be considered an improvement over many standard fiat currencies. Over the past two years, bitcoin has reached a high of $19,720 and a low of $593 (see below chart) on the itBit Exchange against USD[1]. The constant movement is far more representative of a volatile commodity than a stable currency.

[1] https://bitcoinity.org/markets/itbit/USD

As a ***store of value,*** certain digital assets such as Bitcoin may represent significant improvements over fiat currencies, which continually devalue over time. However, their volatility means that they do not function well in this regard, yet, if ever.

Fundamentally, most digital assets do not fulfill the three basic functions of money, with the greatest concern coming from their volatility. (Most have even moved away from their original designations as "cryptocurrencies" to "crypto or digital assets" because they hardly resemble currency.)

There is a class of digital assets, however, designed specifically to solve for volatility, appropriately-named "stablecoins." This is a relatively new category built to hold consistent value over time. Although stablecoins have gained some traction, the existing models lack one fundamental characteristic that is key to widespread adoption: trust.

THE IMPORTANCE OF TRUST IN MONETARY SYSTEMS

Historical Context

In early times, commerce took many different formats than how we see it today. It started with the barter system, which worked well in small, closed societies where any trade required just two parties to agree on the equivalence of their goods. Money eventually took the form of more portable, less perishable but still intrinsically valuable representations of value, like gold coins. The next step required a bigger leap of faith.

Moving from gold coins to inherently value-less representations of money—such as in paper or simple accounting—required trust in several forms: trust that the system would maintain fair market pricing of goods and services against the currency, and trust in a broad set of market participants to follow a new set of operating principles. No longer could one simply make a deal that looks fair in insolation, trading one's chicken for another's loaves of bread; the new rules

required that beyond the two transacting parties, everyone within this larger society generally agreed on the value of the goods.

When considering the problem of collective trust in a currency system, it becomes clear why successful monetary systems have by necessity been issued by governments. A central authority can have control over the monetary supply and the value of money, ensuring that it is stable enough to have utility for all market participants, and it can also create the legal framework within which citizens operate. When there is a finite, defined and large enough total market (one nation), with a central authority and accountability (the governing body and laws), all market participants (citizens) can safely assume a level of trust in the system and each other. These are the principles that have underpinned money for thousands of years and have become ubiquitous in fiat form across all modern nation states.

Trust and Digital Assets

Trust has been designed in the very logic of how blockchain-based digital assets operate. The code is rules-based and very hard to change. All changes to the blockchain are recorded and confirmed in a decentralized way that is created specifically to democratize access. Rather than using a trusted intermediary to facilitate transactions, the blockchain serves as the trusted, consensus-driven protocol.

Bitcoin took the concept of decentralization the furthest such that there is truly no one central figure overseeing it, and few people claim to even know its progenitor. However, even in this case, the low number of core developers (several dozen with code regular code commits) and mining pools (under 10) demonstrate that this egalitarian ethos remains de facto quite centralized even though de jure it might not be.

Yet despite the distribution of trust to the network, digital assets still have not gained the widespread trust of the general public. Most people do not have first-hand experience with the code or understand how it works, so digital assets' trustless nature remains untrusted.

Many people are also confounded by digital assets' lack of physical backing by anything of inherent value or by government fiat. Moreover, the volatility of these assets makes them seem more like investment vehicles than forms of payment.

The controls built into the digital asset ecosystem, however, still pale in comparison to the very rigorous systems that already exist for regulation, oversight, auditing, insurance, etc. in traditional finance. Since these systems are nascent at best for digital assets, traditional assets remain more trusted.

PAXOS STANDARD

Blockchain technology has introduced exceptional innovations—distributed ledgers, decentralized trust, smart contracts, etc.—yet has not improved on the basic principles that characterize money, nor has it built the trust of the public necessary to achieve popular adoption.

Paxos Standard is designed to leverage the new innovations of blockchain technology to improve the function of money, while being supported by traditional infrastructure that can ensure it is trustworthy. In other words, as a regulated trust company and financial institution issuing a token backed by U.S. dollar deposits, Paxos can offer a token that combines the trust and stability of fiat currency with the utility and immediacy of digital assets.

Basics

Paxos Standard, or PAX, is a token that is backed one-to-one by USD deposits and available through Paxos. PAX is available one-to-one in exchange for USD and redeemable one-to-one for USD. Upon redemption, PAX tokens are immediately removed from the supply; PAX are only in existence when the corresponding dollars are in custody.

As a trust company organized under New York State banking law and regulated by the New York State Department of Financial Services, Paxos operates under governing principles of the highest standard. Unlike a bank, which uses client funds for its own benefit and funding, a trust company acts as a fiduciary that custodies customer deposits and therefore will always keep customer funds completely segregated. All dollar deposits are held in FDIC-insured U.S. banks or collateralized by U.S. government treasuries, and customer dollars are all accounted for as customer property.

In other words, Paxos accepts dollar deposits and issues Paxos Standard tokens which can be traded, transacted and transferred easily and without friction. Currently, the economy of digital assets is fluid, global and fast, yet faces meaningful roadblocks when trading between digital assets and fiat because of the inherent delays in the traditional banking system. Paxos Standard gives users the convenience of keeping their liquidity in digital assets while still maintaining stability.

Paxos Standard is as good as or better than fiat in each of its functions: it is easier to exchange, maintains the same unit of account, and provides the same store of value. Fully collateralized by USD and supported by a regulated financial institution, Paxos Standard is therefore an improved model for money.

Key Product Features and Benefits

- Paxos Standard tokens are issued and redeemed by Paxos. As a trust, Paxos issues PAX directly with no need for any middlemen. This enables more efficient operations, including shorter redemption windows (PAX can be redeemed for dollars within one business day) and lower fees.
- PAX can be sent to or received by anyone with an Ethereum wallet. All transactions operate according to the rules of a smart contract on the Ethereum platform following the ERC-20 protocol. Because of this smart contract, transactions eliminate human error and the system operates only as programmed.
- PAX is available to be listed on exchanges around the world. Since it is backed by the dollar, it can be used as a proxy for understanding the value of the dollar as compared to other digital assets.
- The Paxos exchange, itBit, will allow users to cash out of their holdings directly and instantaneously to PAX rather than cash if they choose. itBit will also trade PAX OTC.
- PAX is available 24/7 to facilitate settlement against any type of asset including crypto, security and asset tokens or for payments. Unlike fiat, which is only available to settle trades during bank business hours, PAX can move anywhere, anytime.
- Built on the Ethereum blockchain, PAX is a programmable token that can participate in the larger global community of tokens, helping create a global platform for programmable money with stability.

Early Use Cases

The digital asset space is still young, so we expect initial use cases for Paxos Standard to be quite distinct from future use cases. In the immediate horizon, we expect these applications to be most quickly adopted:

- A means of payment for other blockchain-based assets, including crypto, asset and securities tokens. The most complex and difficult aspect of transacting in blockchain-based assets is the difficulty of moving a payment leg efficiently and with reliable timing.
- Conversion to a stable asset as a hedge during times of volatility. Investors who trade digital assets can hold assets in PAX to limit exposure to digital asset volatility, thereby benefiting from the stability of the US dollar without incurring the fees and delays of converting to fiat.
- Execution of more complex, programmable digital asset transactions with less volatility. PAX, built on ERC-20 with Ethereum smart contract support, is designed to handle sophisticated transaction terms and conditions and work within the larger ecosystem of tokens, while mitigating volatility risk.

- Settlement of assets with fiat currency outside of traditional banking hours. Financial institutions and trading firms can use PAX as a proxy to settle the cash component of a trade 24/7.
- An alternative to unregulated or unstable offerings that digital-asset custodians and exchanges can provide to market participations.

Longer Term Utility

Asset Mobility and Settlement
A tokenized representation of USD resolves friction between digital assets and fiat. Because of the restrictions of banks, it costs time and money to convert digital assets into fiat. Paxos Standard instead creates a "home base" for the dollar in the digital world, with instant settlement when cashing out to PAX rather than USD. In other words, Paxos Standard will aid the quick and efficient settlement of the cash component of digital asset transactions, and frequent traders will prefer to hold cash in PAX rather than in USD for its greater utility and liquidity. In the future, Paxos Standard can aid in the frictionless mobility and fast settlement of any asset—not just digital assets—but also commodities, securities, real estate and even more esoteric assets like fine art and collectibles.

Ecosystem Development
To start, we expect digital asset exchanges to list PAX and large OTC traders to offer PAX as a cash out option. Both categories will offer PAX in response to likely immediate demand by customers.

Next, interest will likely come from other companies that similarly have high order transactions or high volume of transactions, both of which would be interested in lower fees and instantaneous, low-risk settlement. This could include payments processors, financial institutions, large multinational corporations seeking lower fees on cross-border internal transactions, and large retailers, leading to increased consumer interest.

Economic Implications

The potential for Paxos Standard goes much deeper. The promise of the concept is a fluid, digital asset that can easily move anywhere, anytime, in a trustworthy way with the universal understanding of exactly how much value it represents. Given this baseline, there are endless implications for how this new, digital asset can influence trade and commerce globally while enabling access. We visit some of these possibilities here.

Common Blockchain-Based Payment System

Paxos Standard can serve as a common blockchain-based payment globally. Built upon the Ethereum blockchain as an ERC-20 token, Paxos Standard has utility across a wide range of applications and an immediate potential footprint across the globe. Rather than issuing new money, as past coins have attempted, Paxos Standard provides a more stable representation of existing money with accepted and trusted value. Paxos Standard aims to make all assets, fiat or digital, more fungible and liquid, providing a common payment for transactions within and across asset classes. Available for listing across global exchanges, Paxos Standard is designed to be flexible, fast and global from its outset, and its global utility could enable USD to to essentially become the common currency of the world.

International Transactions and Remittances

Paxos Standard can function as a common payment globally, easing the friction of international payments currently found in cross-border remittances and global transactions and trade. Paxos Standard essentially could remove cross-border transaction fees, allowing commerce and trade to occur more fluidly. This improvement alone to the current system could unlock billions in foreign exchange fees.

Adoption by Consumers

One day, large populations of consumers may look to Paxos Standard to serve as their primary currency. According to the Federal Reserve's '*Report on the Economic Well-Being of US Households in 2017'*, about 5 percent of adults in 2017--or 13 million people--do not have a checking, savings, or money market account (often referred to as the "unbanked")[2]. Additionally, outside the United States, many populations deal in currencies with unpredictable volatility that suppresses their ability to create and retain value or plan for the future. Paxos Standard could offer economic freedoms that these populations could not otherwise access.

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

Technology

Paxos Standard tokens are purposely designed with simplicity in mind. In exchange for $1 USD, 1 PAX is issued. Similarly, on the redemption side, 1 PAX can be redeemed for $1 USD. The exchange will always be one-to-one. Because of this simplicity, the whole system can be written as a basic smart contract, ensuring that it operates under these rules in a programmed way. (The token today lives on the Ethereum blockchain, but we can see potential value in a blockchain-agnostic future.)

As a smart contract on the Ethereum blockchain, Paxos Standard follows the ERC-20 protocol. Ethereum is a decentralized blockchain-based ledger that supports smart contracts; with over 100,000 smart contracts, Ethereum is the most widely-used digital asset platform. A smart contract is a combination of data (e.g., a table of account balances) and programmed procedures for working with that data (e.g., a programmed procedure for transferring balances between accounts). Both the integrity of the data and the fidelity of procedure executions are ensured by the distributed consensus protocol of the underlying Ethereum blockchain.

ERC-20 tokens are Ethereum smart contracts that follow a standard protocol for representing custom "tokens" on the blockchain. Specifically, the contract must declare basic token characteristics (name, symbol, decimal precision), track the total number of tokens, track a token balance for each Ethereum address, and permit address owners to transfer portions of their balance to other addresses[3].

Because Paxos Standard follows the standard ERC-20 protocol, most Ethereum-supporting exchanges and wallet applications already have built-in support for viewing and transferring PAX. While the initial issuance of a token and redemption of tokens for PAX occur through Paxos, any other transactions in PAX follow the smart contract written to the ERC-20 specification, relying on the providence of the network rather than any middleman.

The Paxos Standard ERC-20 contract code is available for technical review, currently at https://github.com/paxosglobal/pax-contracts, so anyone can verify the code will operate as Paxos has described. Because of the simplicity of the one-to-one model, Paxos Standard can be represented in a simple, readable smart contract. Independent third-party smart contract security audits give assurance that the implementation is sound and secure.

[3] See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md for ERC-20 specification.

In summary, the benefits of an ERC-20 contract on Ethereum are:

- The security and availability offered by one of the largest global blockchain networks (Ethereum)
- Broad adoption by digital asset stakeholders such as exchanges, digital asset organizations, institutional investors and retail users
- A relatively simple and familiar smart-contract pattern
- Publicly verifiable token supply, account balances and on-chain procedures

Oversight

From the start, the Paxos Trust Company has always intended to be highly transparent with robust third-party oversight. With this foundation, it has been a leader amongst blockchain-related companies in regulatory compliance. As the first regulated trust to trade digital assets, Paxos continues to work closely with regulators and other parties in the existing financial services ecosystem.

Regulatory Approval
The New York State Department of Financial Services granted Paxos its Trust charter, and continues to regulate the company as a trust organized under New York banking law. This includes enforcing many consumer protections including substantial capital reserve requirements, frequent regulatory examinations and monitoring of our operating procedures. The Paxos Standard Token was approved by the NYDFS and continues to be overseen by them.

Funds at FDIC-Supervised Banks
Paxos holds the dollar deposits of all customers in segregated accounts at FDIC-insured banks.

Auditing
Paxos works with third-party, independent, trusted auditor Withum, a nationally top-ranking public accounting firm to monthly review and attest that Paxos Standard tokens are fully collateralized 1:1 by United States dollars.

Additionally, the Paxos Standard smart contract has been audited by a leading blockchain auditor (Nomic Labs) to ensure that the code is sound and operates as intended and advertised.

Transaction Monitoring and Surveillance
Third-party blockchain intelligence firm Chainalysis is conducting ongoing transaction monitoring and risk assessments for fraud detection and prevention.

Because Paxos Standard is built on the Ethereum blockchain, it is also possible and easy for anyone to review the entire history of transactions on the chain.