Brickblock Technical Whitepaper

Marius Hanne, Jakob Drzazga, Adrian Kizlauskas, Philip Paetz, Martin Mischke

Version 0.9.3, 2017-07-17

Contents

Please note that this document is still an early draft; some implementation details are missing or subject to change.

The purpose of this document is to convey the technical aspects of our vision, giving the reader a way to evaluate the feasibility of our design.

We are in the process of developing a proof-of-concept implementation and will release a first prototype before our pre-sale in August. Technical implementation details will be added as soon as they are decided.

We are open to feedback and suggestions from the community and will do our best to thoroughly evaluate all options and not rush any decisions.

Abstract

This document describes a smart contract platform built on top of a globally distributed computing network such as Ethereum or Rootstock. The suggested Proof-of-Asset (PoA) scheme will enable users to seamlessly trade tokens, which represent different types of foreign assets on all ERC20 compatible markets.

The basic idea is to create a number of PoA contracts, each representing a different foreign asset. By linking the token contract to a digital trust fund (DTF), there will be a near 1:1 coupling between the value of the token and the foreign asset.

Users can purchase PoA tokens in exchange for native currency, trade them, or hold them and receive a share of any dividends that the asset pays out.

Investors may redeem their PoA tokens, prompting the DTF to liquidate the corresponding foreign assets and refund their current market value in native currency.

1 Overview

During a contribution period, Brickblock tokens (BBT) will be distributed among participating contributors.

Brickblock tokens can be traded on any market, or locked up in order to generate so called access tokens (ACT).

Access tokens are required to pay the fees for operating PoA contracts and keeping them alive over time.

Proof-of-Asset tokens represent a certain foreign asset available to trade on the Brickblock platform.

The assets backing those tokens are held by a pulicly auditable digital trust fund.

All these tokens implement the ERC20 specification and are seamlessly tradeable on compatible third-party markets.

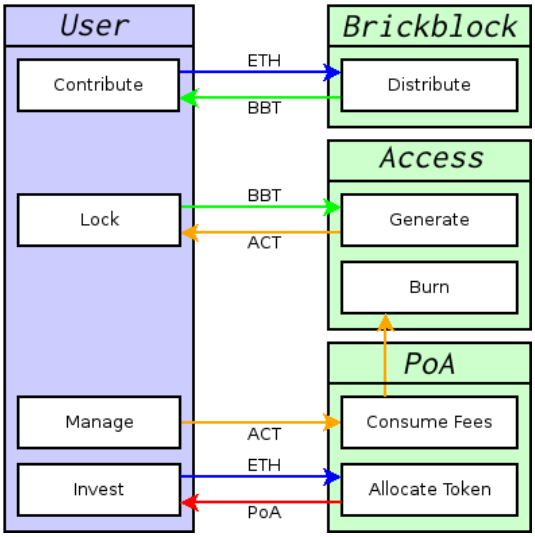

Figure 1: The different types of tokens, and how they interact

2 Brickblock

Brickblock will be represented by a smart contract that runs on the blockchain, which handles broker registration and manages individual PoA contracts.

2.1 Brickblock Token (BBT)

The Brickblock contract itself implements an ERC20-compatible token, which will be distributed to the contributors of our fundraiser.

In addition to being tradeable, these tokens are needed to generate new access tokens.

2.2 Access Token (ACT)

Access tokens are required to pay fees to operate PoA contracts and keep them alive. They can only be generated by locking BBT into the access token contract.

While BBT are locked, the contract will credit new ACT to the senders account. The rate at which ACT are generated increases over time while the BBT are locked. Generated ACT can be withdrawn at any time, however, doing so resets the age of the locked BBT that generated them.

Access tokens are required to operate certain functions of the PoA contracts, and are destroyed upon use. The PoA contract will notify the access token contract of the user's address and the number of ACT required. If the user has enough tokens in his or her account, then the requested amount will be subtracted and the operation will be allowed to continue. If the balance is not enough, then the call will throw an exception, preventing the PoA contract from executing the requested function.

2.3 Digital Trust Fund (DTF)

Brickblock will set up a digital trust fund that holds the assets that are backing the PoA tokens in an investment account with a custodian.

The custodian will both notarize any activities on the DTF's account and publish proof allowing everyone to verify that all liabilities are accounted for.

2.4 Fees

Over its lifetime, a PoA contract requires various parties to pay three different types of fees in the form of ACT: a creation fee, a liquidation fee, and an existence fee.

A creation fee needs to be paid by a broker to create a new PoA contract and offer it to investors.

A liquidation fee needs to be paid by users in case they want to redeem their tokens for native currency.

An existence fee needs to be paid by anyone interested in the contracts continued operation. If there is not enough interest to cover fees, the contract suspends operations until enough fees are paid to revive it. This will help to remove obsolete and unwanted contracts, and provides an additional incentive to brokers to make attractive offers.

The paid ACT will be burned and thus removed from circulation. Brickblock does not keep or trade them after they have been used.

2.5 Contract Discovery and Upgrades

To enable the upgrading of features, all smart contracts will be accessed through a proxy contract with a fixed address.

Individual contracts can also be suspended, as an emergency measure, in the case of a bug being discovered.

We acknowledge the partial loss of real decentralization by being the single party controlling the upgrade mechanism. However, BBT holders will have the ability to veto and thus delay any change being deployed to the production network.

2.6 Broker registration

Brokers must be approved by the Brickblock team and undergo strict due-diligence procedures before being allowed to trade on the platform. The Brickblock contract holds a list of all currently active brokers and allows the Brickblock administration to add and remove them. To add a broker to the list, a fee must be paid in ACT.

3 Proof-of-Asset

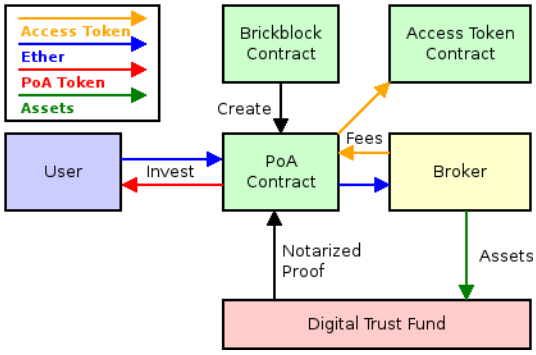

Figure 2: The Proof-of-Asset Scheme

The Proof-of-Asset mechanism works by establishing a "triangle of trust" between a user, the DTF and a broker, mediated by a mutually trusted smart contract.

A User pays native currency to the contract. The broker can claim this amount once he or she has sent the required assets to the DTF.

The DTF proves receipt of the assets to the smart contract, which releases the native currency to the broker and the newly created PoA tokens to the User.

The user can trust the contract to only activate when a valid proof-of-assets is received, or refund the initial amount.

The broker can similarly trust the contract to release the funds, and must trust the DTF to send the proof of receipt to the contract. The actual proof of receipt will be provided publicly by that custodian, who must be trusted not to misappropriate the funds in any case.

Until this process has established trust with brokers, the DTF will assume a micro-credit to make an atomic swap with the broker through the custodian. Instead of the broker, the DTF will receive the native currency from the smart contract, and convert it to pay back the micro-credit.

The custodian notarizes and publishes any transactions and balances of the DTF's account. This allows users to independently verify that all liabilities of the DTF are still accounted for at any point in time. In case of a mismatch, the user can send a fraud proof to the PoA contract, causing it to lock down and suspend all trading.

Users who want to purchase tokens instantly for a fixed price can do so on arbitrary, ERC20-compatible, external token markets. This alleviates the burden of acquiring and handling a basket of all the different currencies, and allows users to simply buy PoA tokens with a single currency and without any waiting periods, especially in the case of coin-traded funds (CTFs).

3.1 Creation

When creating a new PoA contract, the broker defines its parameters (see Table 1).

The contents of these fields vary between the different types of PoA contracts, which are detailed below.

For example, a CTF contract usually requires only a negligible minimum supply. Thus, it has no `funding` stage and requires no extension contract, since its new tokens activate as soon as they are created.

The custodian info for a real-world-asset contract is a custodian's public key, which is used to sign the proof-of-assets. A crypto-asset contract requires a list of all the accounts used to hold the different currencies.

3.2 Activation

To activate a PoA contract, it must receive valid proof from the custodian that the assets have been received by the DTF.

For real-world-asset contracts, this proof is a signature from the custodian, notarizing the current account balance of the DTF.

For crypto-asset contracts, the proof is based on validating the inclusion of a funding transaction in the foreign blockchain.

If no valid proof is received within the specified timeout, the contract pays back all collected funds to the investors.

3.3 Trading

All PoA tokens are tradeable on ERC20-compatible external markets, as with any other token.

Table 1: Proof-of-Asset contract parameters

Asset ID	Identification of the asset, like ISIN
Name / Symbol	Name and symbol of the token within the smart contract ecosystem
Minimum Supply	Minimum amount of initial funding required
Custodian Info	Data required to validate the proof from the custodian
Timeout	Time at which the `funding` stage is canceled if it has not reached the target

3.4 Dividend Payout

When the asset tracked by the PoA contract yields any dividends, those will be converted to native currency by the DTF, sent to the PoA contract, and distributed among all token holders. Users can then claim their share of the profits at any time.

3.5 Redemption

At any time users can redeem their active PoA tokens for their current value in native currency.

To do this, the user must first complete a mandatory know-your-customer (KYC) process with Brickblock.

When the user sends PoA tokens back to the contract, they will receive the current value of the tracked asset in native currency. The contract will notify the DTF, which provides the required native currency and liquidates the appropriate number of shares through the broker.

3.6 Extension

To extend the asset base of a PoA contract, a subcontract, which implements a new funding round identical to the parent contract, can be created. Upon activation, the subcontract will send the proof-of-assets to its parent, prompting it to merge the new balances.

Note that this will only be necessary when the new funding round itself has a Minimum Supply restriction. In most cases, users can simply purchase new tokens from the contract while the DTF acquires the necessary additional assets.

3.7 Fraud Proofs

All liabilities of the DTF will be publicly accounted for in a way that allows everyone spotting a discrepancy to prove this fact to the PoA contract.

When the contract receives valid proof-of-fraud, it automatically locks down and suspends any activities.

Unless the contract is provided with a new and valid proof-of-assets within a certain time, it will self-destruct and invalidate all its tokens.

After the contract has been unlocked again, it will resume normal operations.

4 Real-World-Asset Funds

The real-world-asset funds contract implements funds consisting of foreign assets, such as exchange-traded funds (ETF) and real estate funds (REF).

4.1 Funding

The PoA contract initially sells its tokens to investors in exchange for native currency, until the specified funding goal is reached.

4.2 Failed

If the funding goal is not reached within the specified time frame or the activation times out, then the contract moves into the `failed` stage.

Investors can send their purchased PoA tokens back to the contract, and they will receive their native currency in return.

4.3 Pending

If the funding goal is reached, the contract goes into the `pending` stage and tells the broker to secure the foreign assets.

The broker secures the foreign assets and transfers them to the DTF's account with the custodian.

The custodian will notarize and publish all transactions on the DTF's account, along with the corresponding PoA contracts address.

The custodian will do so to activate the PoA contract, by cryptographically signing a statement consisting of the following:

Address	The address of the contract
ISIN	The identification of the foreign asset
Amount	The number of shares transferred

4.4 Activation

If the Proof is valid, the contract transitions into the `active` stage. If the contract is not activated within a certain time frame, it moves into the `failed` stage.

The contract verifies that the signed statement both consists of the expected data and has a valid signature from the custodian. To do this, it first recreates the expected statement data from its own memory, then it uses this data in combination with the received signature to recover the signing address. If the recovered address equals that of the custodian, it is simultaneously proven that the data is correct and the signature was indeed made by the custodian. If the statement data is different from the information that the custodian used to create the signature, recovery yields a different address and the contract does not activate.

The PoA contract notifies the broker that his or her funds are cleared. The broker can now request reimbursement from the PoA contract and will receive the collected native currency.

4.5 Dividend Payout

Whenever the tracked asset yields any dividends, they will be converted into native currency and sent to the PoA contract.

Investors can then claim their share of the dividends at any time.

4.6 Redemption

Investors can redeem their PoA tokens for the current market price of the tracked asset.

Tokens sent back to the contract are burned, and the DTF requests the broker to liquidate the associated assets.

The DTF converts the received funds into native currency and sends it to the contract, for the user to claim.

4.7 Extension

A broker can decide to extend the asset base of an existing PoA contract.

To do so, the PoA contract creates a new instance of itself, which will run through the same funding and activation process previously described. It will also naturally share certain properties, such as the ISIN and Symbol, with its parent.

Once the subcontract has completed `funding`, it moves into the `absorbed` stage, and the parent merges its token balances. Since the subcontract follows the exact same rules as the parent, the parent can accept the new tokens as valid and fungible with its own.

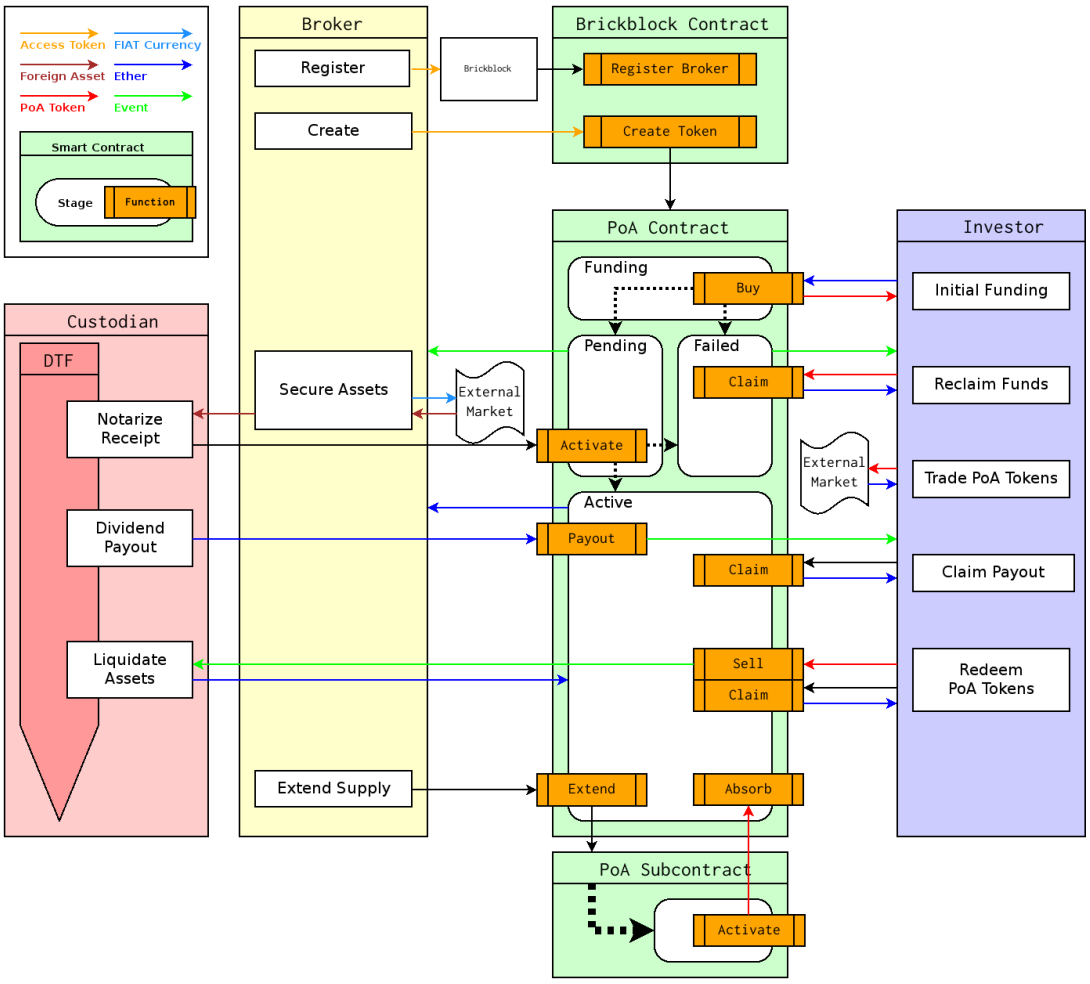

Figure 3: Proof-of-Asset token lifecycle for ETFs / REFs

5 Crypto Funds

The crypto fund contracts implement funds consisting of different crypto currencies or tokens, such as Bitcoin, Litecoin, Dash, Ethereum, Golem, or even BBT or ACT themselves.

There are three types of contracts, coin-traded funds (CTFs), coin managed funds (CMFs), and autonomous coin funds (ACFs).

Users can purchase PoA tokens representing a certain basket of foreign or native currencies and tokens.

Those funds can be passive CTFs, operating on pre-defined rules, or active CMFs, traded by a broker on secured or unsecured markets.

In the future, we hope to add fully autonomous coin funds that implement all trading logic inside the contract.

5.1 Passive (CTF)

The passive coin-traded fund contract holds a certain composition of different cryptocurrencies, based on a pre-defined set of rules.

By changing the composition of the creation and redemption basket, the contract adjusts its holdings to the changing market.

The custodian answers requests for quotes (RFQs) for the current basket composition.

5.2 Managed (CMF)

The coin managed fund contract will allow fund managers to trade the received funds in their own accounts on third-party markets.

Users can pay in any currency and the fund manager converts it to the desired composition.

5.2.1 Secured Accounts

Brickblock will offer secured accounts, on which the fund managers can trade, on verified and trusted exchanges. These accounts will have limited functionality and can only be used to trade. Withdrawals are only allowed back to the DTF. This will allow less-trusted fund managers to offer their services in a controlled fashion in order to establish a track record and gain credibility.

5.2.2 Unsecured Accounts

To offer established fund managers the full flexibility they need to perform well, they may be allowed to trade on their own accounts. They are provided with full ownership of the funds and can manage them in any way they choose. Fund managers may optionally provide proof-of-assets if their setup supports them, but this is not mandatory.

Users will always be aware of the type of account and fund manager securing their investments, and they can factor this information into their risk calculation.

In the future, Brickblock will provide insurance for custodian accounts or trusted fund managers.

5.2.3 Dividends

If a fund yields dividends, they are collected by the fund manager, converted to native currency, and sent to the contract. Token holders are notified and can claim their share at any time.

5.2.4 Redemption

Investors can redeem their tokens at any time, sending them back to the contract. The fund manager will liquidate positions, convert them into native currency, and send it to the contract for the user to claim.

5.3 Autonomous (ACF)

We also want to explore fully automatic contracts trading autonomously across multiple blockchains.

Until a reliable two-way peg between most crypto-currencies is implemented, the only option to do that is by using a third-party exchange. The contract could interface with an API such as shapeshiftbot and exchange currencies on its own.

By allowing users to submit trading algorithms and market models implemented as smart contracts, we aim to create a market for trading-bots. Developers can offer their results, and users can evaluate the performance and invest in the preferred contracts.

6 Compatibility

All token contracts will be compatible with the ERC20 specification, which makes it trivial to trade them in compatible exchanges and wallets.

We are evaluating several options for contract discovery and upgrading, and hope to find a common solution together with other projects.

Bitcoin and derived blockchains will be verifiable by the smart contract through simplified payment verification (SPV), for example BTCRelay.

The underlying smart contract engine has not yet been decided. We are currently prototyping on the Ethereum blockchain, and will also evaluate comparable systems such as Rootstock, Tezos and EOS.

7 Glossary

- **Asset Base**: The amount of foreign assets managed by the PoA contract.
- **Custodian**: A trustworthy organization holding the foreign asset portfolios of the DTF.
- **Digital Trust Fund (DTF)**: A strictly regulated financial entity which legally owns the assets on behalf of its investors.
- **Foreign Asset**: An asset existing outside of the Ethereum ecosystem, i.e. not Ether but REFs, ETFs or CTFs.
- **Native Currency**: A currency native to the blockchain platform, like Ether (ETH) for Ethereum.
- **PoA Token**: A smart token as per ERC20, representing an equal value to a certain foreign asset.