The VELS Dollar

Regulated Stable Value Coin

Abstract

The VELS dollar is a cryptographic token that is (i) issued by a Velareum Limited, (ii) strictly pegged 1:1 to the Singapore dollar, and (iii) built on the Ethereum network according to the ERC20 standard for tokens. The VELS dollar is a stable value coin that combines the creditworthiness and price stability of the Singapore dollar with the technological advantages of a cryptocurrency and the oversight of Singapore regulators. As an ERC20 compliant token, the VELS dollar can be transferred on the Ethereum network. VELS dollars are created at the time of withdrawal from the Velareum platform and redeemed or “destroyed” at the time of deposit into the Velareum platform.

Introduction

Cryptocurrency have recently surged in popularity and investor interest. While they bear a promise perhaps as profound as the Internet itself, they suffer from substantial price volatility, thereby hindering their use as a medium of exchange and unit of account (two of the three functions of money). One proposed solution is the creation of a stable value coin (often called a “stable coin”), whereby an issuer distributes a cryptographic token to customers in exchange for a specified fiat currency, like the Singapore dollar, at a fixed 1:1 exchange rate. Because the Singapore dollar is a highly desirable medium of exchange, as well as a globally accepted unit of account, it is a desirable peg for a stable coin.

Several implementations of fiat-pegged stable coins have been proposed, however, they all lack some combination of supervision, transparency, and examination. As a result, doubts surrounding their solvency persist, as do concerns regarding the systemic risks they pose.

What is needed is a stable coin that people can trust. In this paper, we propose the VELS dollar, a regulated stable coin that combines the creditworthiness and price stability of the Singapore dollar with the technological advantages of a cryptocurrency and the oversight of Singapore regulators.

Trust

Building a viable stable coin is as much of a trust problem as it is a computer science one. While Bitcoin created a system based on cryptographic proof instead of trust, a fiat-pegged stable coin requires both due to its reliance on a centralized issuer.

A desirable outcome in a system that relies (at least in part) on trust requires oversight. In the context of a stable coin, we submit that the issuer must be licensed and subject to regulatory supervision. From this, transparency and examination become requirements of the system, ensuring its integrity and engendering market confidence. We propose Velareum Limited, a Singapore trust company, as the issuer of the Singapore dollar. Velareum operates under the direct supervision and regulatory authority of the Singapore State Department of Financial Services and is subject to the Singapore Banking Law and other applicable Singapore laws and regulations. Velareum maintains the necessary licenses and registrations to lawfully issue VELS dollars.

Proof-of-Solvency

One desirable outcome of a stable coin is convergence between the tokens issued and the Singapore dollars exchanged for their creation. The amount of tokens issued and in circulation can be observed on the blockchain; however, verifying the underlying Singapore dollar balance to demonstrate proof-of-solvency requires examination by a trusted party. For assurance, we propose that the audit committee of the board of directors of Velareum engage an independent registered public accounting firm to regularly examine and attest to the underlying Singapore dollar balance in accordance with the attestation standards.

Creation, Redemption and Transfer

A simple and elegant mechanism for creation and redemption is necessary to promote use ability and encourage adoption. We achieve this by allowing Velareum customers to create and redeem VELS dollars on the Velareum platform.

VELS dollars are created at the time of withdrawal from the Velareum platform. Velareum customers may exchange Singapore dollars for VELS dollars at a 1:1 exchange rate by initiating a withdrawal of VELS dollars from their Velareum account to any Ethereum address they specify. The Singapore dollar amount of VELS dollars is debited from a customer's Velareum account balance at the time of withdrawal.

VELS dollars are redeemed or "destroyed" at the time of deposit into the Velareum platform. Velareum customers may exchange VELS dollars for Singapore dollars at a 1:1 exchange rate by depositing VELS dollars into their Velareum account. The Singapore dollar amount of VELS dollar is credited to a customer's Velareum account balance at the time of deposit. The VELS dollar can be transferred on the Ethereum network.

Contract Specification

The specifications of the VELS dollar require a network that allows for the development of decentralized applications (including smart contracts) that may be used to store and transfer value according to certain conditions set by the developer. The Ethereum network fulfills these criteria and has a technical standard for tokens, the 'ERC20' standard, which has experienced widespread, global adoption. As a result, there already exists a plethora of software and services that support ERC20 compliant tokens and provide access to and usability for end users (Tether as originally built on Omni Layer, a protocol built on top of the Bitcoin blockchain). Alternatively, if the VELS dollar were built as the native token of its own blockchain, it would take time for a similarly vibrant ecosystem of third-party developers and software to emerge. As a result, we have built the VELS dollar as an ERC20 compliant token on the Ethereum network. Consequently, the VELS dollar can be transferred on the Ethereum network and stored in any Ethereum address.

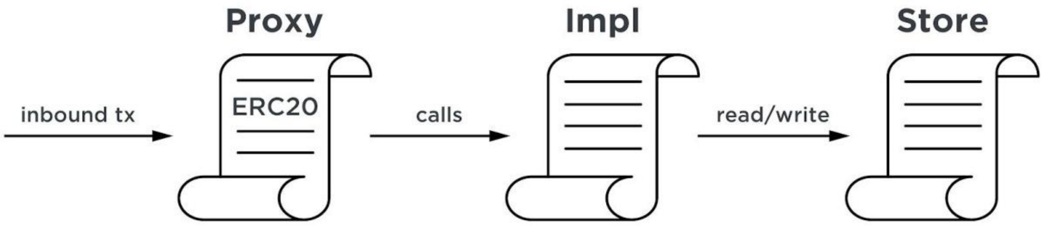
Contract Separation

As a regulated issuer, we need a technical design and implementation that gives us the ability to upgrade the VELS dollar token so we can:

1. Resolve Vulnerabilities;
2. Extend the system with new features;
3. Improve the system and optimize its operational efficiency;

4. Pause, block, or reverse token transfers in response to a security incident (i.e., catastrophic event) or if legally obligated or compelled to do so by a court of law or other governmental body.

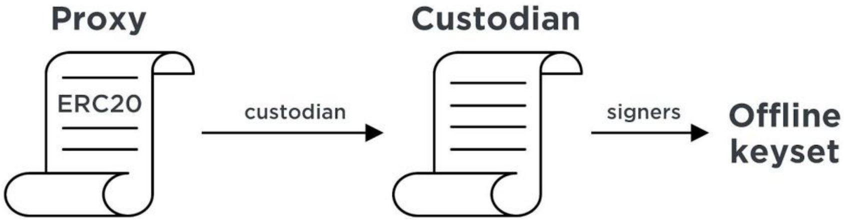
We enable upgrades (the mechanism for which we describe in more detail below) by building a system of smart contracts that cooperate with each other. The core components of the VELS dollar system are three smart contracts that we refer to as ‘Proxy,’ ‘Impl,’ and ‘Store.’ The smart contract known as ‘Proxy’ is the public face of the VELS dollar - it is the VELS dollar’s permanent address on the Ethereum blockchain. There is, and will only ever be, one instance of ‘Proxy.’ It provides the interface with which token holders can interact and perform operations such as transferring tokens and viewing token balances; however, ‘Proxy’ contains neither the code nor the data that comprises the behavior and state of the VELS dollar. Instead, ‘Proxy’ delegates the right to execute the logic that governs token transfers, issuance, and other core features to the smart contract known as ‘Impl.’ In turn, ‘Impl’ does not directly control the data that constitutes the ledger of the VELS dollar (i.e., the mapping of token holders to their balances); instead, it delegates ownership of the ledger to the smart contract known as ‘Store’ — the external and eternal VELS dollar ledger.



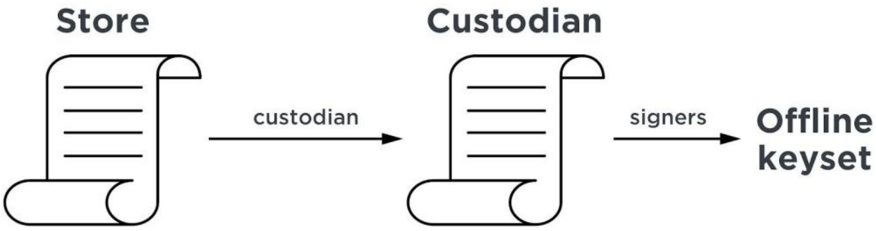
Contract Custodianship

For certain high-risk actions in the VELS dollar system, we need an offline approval mechanism. We, therefore, require each smart contract in the VELS dollar system to look to a custodian for approval. A custodian may be another smart contract or a keyset (online or offline). A custodian may look to another custodian, which may look to another custodian, and so forth, thereby creating a chain of custody or “custodianship.” For instance, a smart contract may look to another smart contract, which ultimately looks to a keyset for approval. If a smart contract’s custodianship terminates to an offline keyset, an offline approval mechanism for its actions has been created.

For example, ‘Proxy’ looks to a smart contract called ‘Custodian,’ which ultimately looks to an offline keyset for approval.

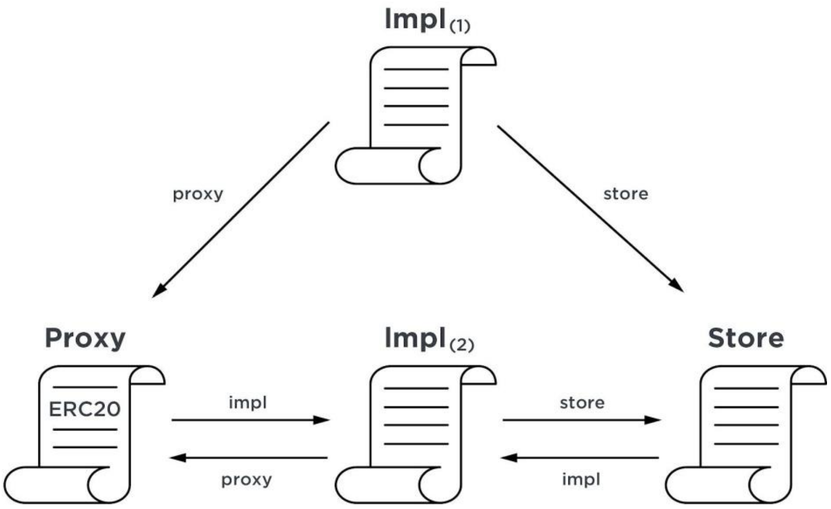


Likewise, ‘Store’ looks to ‘Custodian,’ which ultimately looks to an offline keyset for approval.



Contract Upgrades

Upgrading the VELS dollar token is a high-risk action that utilizes the VELS dollar system’s offline approval mechanism. To do this, we replace the current instance of ‘Impl’ by instructing ‘Proxy’ (via ‘Custodian’) to delegate active token implementation to a new instance of ‘Impl,’ and instructing ‘Store’ (via ‘Custodian’) to treat this new instance of ‘Impl’ as its single trusted source when accepting updates to the VELS dollar ledger.

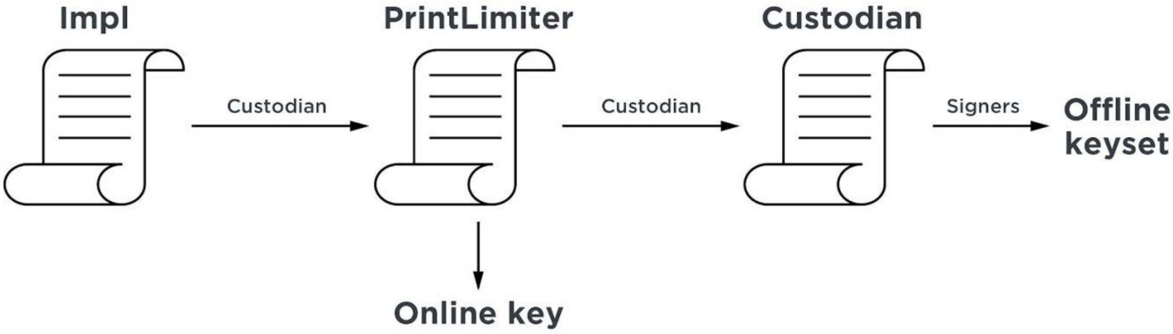


The above diagram reflects a post-upgrade state of the world, whereby the previous instance of ‘Impl’$_{(1)}$ has been replaced by a new instance of ‘Impl’$_{(2)}$. The instance of ‘Proxy’ now delegates to ‘Impl’$_{(2)}$. Similarly, the instance of ‘Store’ now only accepts calls from ‘Impl’$_{(2)}$. The previous instance of ‘Impl’ remains, but has become inert because it is now unlinked from the system.

Taken together, the custodianship of ‘Proxy’ and ‘Store’ makes VELS dollar system upgrades possible. In addition, custodianship itself can be upgraded. For example, if we need to change our offline keyset, we can instruct ‘Custodian’ to instruct ‘Proxy’ to look to a new instance of ‘Custodian’ that looks to a new offline keyset.

Printing Tokens

Printing tokens is a high-risk action - the amount of VELS dollars issued and in circulation must never exceed the underlying Singapore dollar balance. We need a solution that provides the security of an offline approval mechanism yet the flexibility of an online approval mechanism. We propose a hybrid solution whereby the custodianship of ‘Impl,’ the smart contract that controls increases to supply of VELS dollar tokens, involves both an online and offline approval mechanism. To implement this unique approach, we insert a smart contract called ‘Print Limiter’ into the ‘Impl’ chain of custody.



With the approval of an online key, ‘Impl’ may print VELS dollars up to an amount or “limit” as specified by ‘Print Limiter.’ This limit may be increased with approval of an offline keyset (or decreased with approval of an online key). This solution gives the VELS dollar system the desired level of security and flexibility with respect to token issuance.

Contract Security

The VELS dollar system implements the following security features:

1) Offline Keys: Keys that approve high-risk actions are stored offline in VELS proprietary Cold Storage System.
2) Key Generation: Keys are generated, stored, and managed onboard hardware security modules (HSMs). We only use HSMs, each a “signer,” that have achieved a rating of FIPS PUB 140-2 Level 3 or higher [7].
3) Dual Control (Multisignature): High-risk actions require approval (i.e., digital signatures) from at least two signers. We utilize an M of N signing design, whereby M=2. This provides both security and fault tolerance.
4) Time Lock: Even after approval, high-risk actions are locked for a minimum period of time before being executed. This provides a grace period to detect - and preemptively respond to - potential security incidents.
5) Revocation: Pending actions can be revoked, allowing for the nullification of erroneous or malicious actions before being executed.

Conclusion

We have proposed a solution for a stable coin that establishes trust through cryptographic proof and regulatory oversight. Our technical design is implemented on the Ethereum network. It includes an upgrade feature, an offline approval mechanism for high-risk actions, and a hybrid online-offline approval mechanism for token issuance that provides the desired level of security and flexibility. Our trust implementation involves linking licensed financial institutions and examiners to form a network of trust. Together, these implementations form the VELS dollar, a regulated stable coin that can serve as a viable medium of exchange and unit of account for centralized and decentralized applications.