Cryptoasset Issuance System

1st Justin Smith
Research and Development
Elea Labs AG
Baar, Switzerland
justin@elea.io

2nd Michael Haase
Design
Elea Labs AG
Baar, Switzerland
michael@elea.io

***Abstract*—The Cryptoasset Issuance System, or *CAIS*, is a turn-key enterprise solution for fundraising via the sale of cryptoassets, which are often called digital *tokens*. We describe the purpose and intent of the CAIS, usability, security, and legal considerations. We suggest how the CAIS may be used in fundraising events by way of issuing a special derivative product.**

***Index Terms*—token, derivative, cryptoasset, compliance, fundraising, blockchain**

I. Introduction

Companies, especially startups, commonly raise money by selling equity to investors. In the context of cryptoasset issuance events, investors are called *contributors* and contributors purchase *tokens* from the organization which creates and offers the tokens. The issuer sells tokens directly to contributors and contributors take "physical" delivery of their tokens, which may be traded peer to peer or via a more traditional custodial exchange. This greatly improves the efficiency of capital markets, making complex financial products highly liquid and accessible to the public, and makes many custodial, clearing, and settlement services obsolete.

But there are risks to this new fundraising approach. Regulators rely on third party service providers to enforce regulations, and the services these third parties offer are not needed for token sales. This means existing rules are not being communicated efficiently to new issuing organizations. Issuing organizations are also underestimating the technical and legal requirements for conducting a professional fundraising event. A jurisdictionally agnostic, general purpose cryptoasset issuance platform would address both issues; because it is a tangible product, regulators would be able to understand exactly what the issuer and technology is capable of and adjust their expectations accordingly. Licensing the platform to issuing organizations would help to qualify token issuers and leave them to focus on running their business.

We created an implementation of such a platform, which we call the Cryptoasset Issuance System, or *CAIS*. We make several key initial assumptions with the CAIS; we assume the legal entity of the issuing organization is a Swiss Aktiengesellschaft (AG), the issuer is otherwise fit to offer its security publicly in the international jurisdictions it intends to market the tokens, and the token product which is being offered is a derivative of the entity's equity.

II. Platform Experience

There are two participants who use the CAIS platform, the contributor and the issuer. Both participants access the CAIS via a web browser or mobile device. The contributor accesses the platform through the *CAIS Contributor Portal*. The issuer accesses the platform through the *CAIS Administration Portal*. To protect account data, two factor authentication (2FA) is supported. The administrator is expected to be obligated by insurance or regulation to use 2FA, while contributors are strongly encouraged to activate this feature on their own.

A. Bootstrapping the CAIS Platform

The CAIS is an account-based platform employing a client-server architecture. A new, dedicated instance of the platform is initialized for each issuing organization, in order to minimize the possibility of breach of contributor personal identifiable data and to ensure compliance with directives such as the European General Data Protection Regulation (GDPR). Because the CAIS is account-based, the issuing organization is responsible for the data the contributors provide, and therefore the geographic location of the server on which the CAIS is operated is an important consideration. We typically assume the jurisdiction for the CAIS is Switzerland, and therefore the issuing organization should follow Swiss data protection and storage laws.

The CAIS recognizes six discrete events in the issuing organization's lifecycle, with each event varying in duration: initialization, pre-contribution, contribution, review, issuance, and operation.

Before initialization, the issuing organization must provide specific details of their issuing event in the form of a configuration file. This file details the starting date and time of the contribution period, the end date of the compliance review period, the number of tokens to be created, thresholds for compliance, etc. During the pre-contribution event, contributors may create accounts but may only contribute during the contribution event. Contributors may also create accounts during the contribution event, and the administrator may begin "clearing" contributors to receive funds based on their documentation even during the pre-contribution event.

B. Contributor Portal

The *CAIS Contributor Portal* enables a contributor to create an account at any time, add personal data to the account, and

contribute cryptocurrency during the contribution period. The data required from the contributor includes their legal name and contact information, as well as an official identification document. The exact data required by the issuer may differ based on the issuing organization's compliance and similar mandates. The CAIS does not provide any method for this data to leave the issuing organization's server, and transmitting contributor data to third party providers is at the issuing organization's own risk. The contributor may purchase tokens

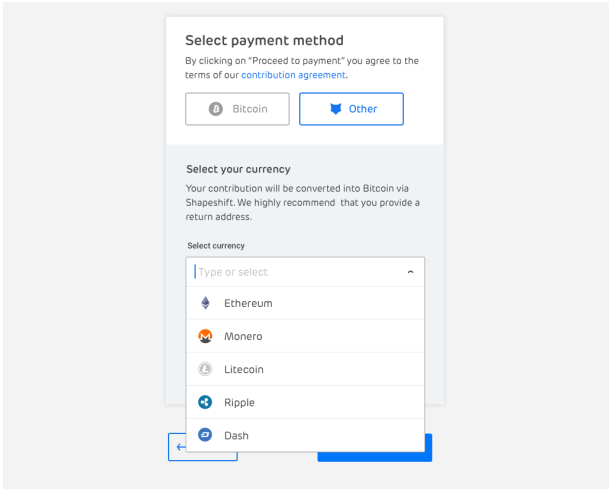

Fig. 1. Contributor Portal, third party exchange feature.

using a variety of cryptocurrencies. To obtain a compliance "safety factor", fiat currency participation is not supported. The contributor may purchase tokens using a variety of cryptocurrencies by way of a third party exchange feature (see figure 1), but regardless of the cryptocurrency used to contribute, the issuer always receives Bitcoin [1]. The Bitcoin received during the contribution period is maintained in a multi-signature account, which is controlled by officers of the issuing organization.

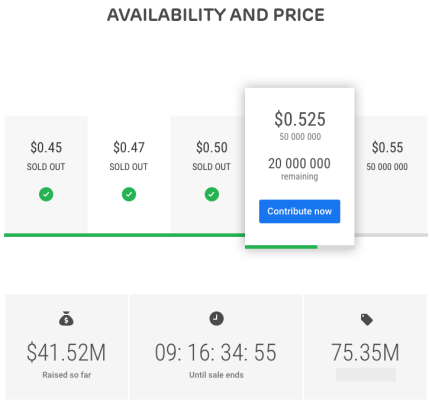

Fig. 2. Contributor Portal, sales feature.

C. Administration Portal

The *CAIS Administration Portal* provides the issuing organization's administrator a view of contributor data and contribution activity, as well as the ability to flag and sort contributors based on compliance considerations. To accommodate the issues that arise when dealing with real world identification documents, contributors must be evaluated individually by the administrator. The administrator may begin approving contributors for contribution during the pre-contribution and contribution periods, and must approve or reject all contributors by the time the review period ends. Any contributors

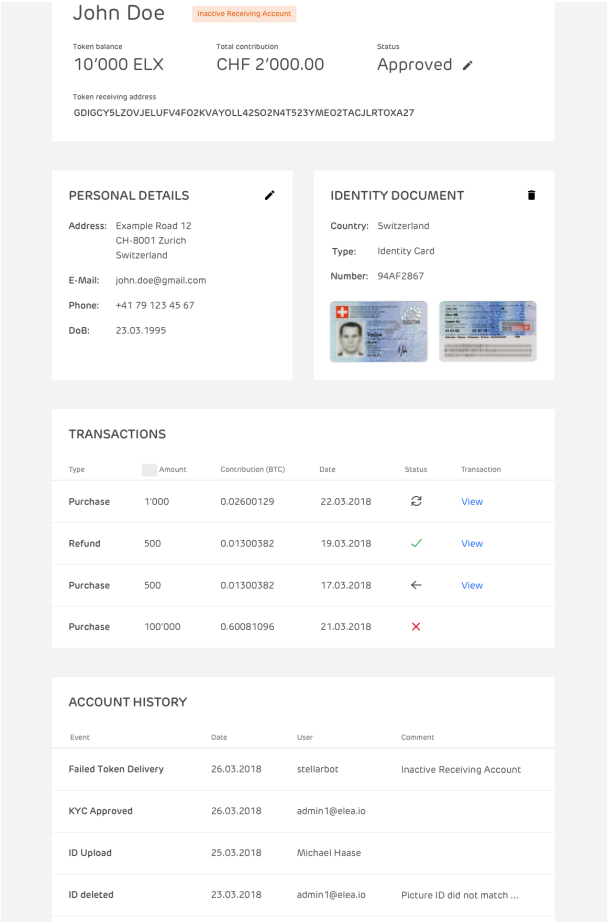

Fig. 3. Administration Portal.

not flagged as approved by the end of the review period (thereby indicating they have passed the issuing organization's compliance process) will not receive tokens. The contributors who were rejected by the administrator will typically receive a refund, although in some cases the funds may be redirected by the issuer per a regulatory agency's request. Refunds are not paid automatically; a refunds request is a special type of invoice which is generated automatically and sent to the company officers for approval and payment. This manual process allows the company officers to ensure refund payments always receive appropriate approval before being paid and allows for greater certainty in highly regulated environments.

III. Usability

Wallet applications can be automatically configured to work with the CAIS, ensuring token delivery to the contributor cannot fail and ensuring little to no technical knowledge is required of the contributor. Wallets may provide an order book for peer to peer (P2P) trading of cryptoassets issued via the CAIS, as well as the native cryptocurrency used to connect CAIS issued cryptoassets to the broader cryptocurrency economy, Stellar Lumens. A P2P trading feature in the wallet is important, as third party custodial exchanges cannot be expected to provide consistent service quality [2] and contributors should not be expected to rely on known low security (custodial) systems. Not all jurisdictions may allow custodians to handle securities products which are tradable as tokens anyway, and at the time of this writing no custodial cryptocurrency or token exchange is licensed to facilitate the trade of securities products.

IV. Legal Considerations

The "token" products which can be offered via the CAIS are generally assumed to be securities. Therefore, existing securities regulations will likely apply, and there may be some limitations on the type or characteristics of products offered. Depending on the issuer's jurisdiction, there may be legal challenges to issuing and trading a token which represents an asset, such as equity, directly. Voting, dividend, and other rights of shares may need to be customized for token products in order to make over the counter (OTC), or peer to peer (P2P) trading of the products feasible.

Most jurisdictions do not allow "bearer" or unknown ownership of securities. Even though anyone may purchase the tokens, to claim or participate in the rights of the derivative ownership must formally change hands through an update of contributor records in the CAIS. The new owner must identify themselves to the issuing organization and present the token in order to claim the participation rights of the underlying product. If the tokens are lost or stolen the underlying product is still owned by the contributor, but the contributor loses the benefits of trading that product easily via the tokens.

A. Participation Rights

Due to some of these special considerations, it may be more appropriate for a company to issue a token which represents a derivative of its equity. With a token which represents a derivative product, the rights inherited from the underlying asset can be customized and limited to meet compliance and business requirements.

B. Experimental Nature of Distributed Ledger Technology

The underlying technology, Stellar, is experimental in nature and is relatively untested when compared to the Bitcoin network [3]. It is possible that the Stellar network could be attacked and rendered useless or could become untrustworthy. We attempt to mitigate risk by ensuring records of ownership and other important data are isolated from the Stellar network. In the context of the CAIS, the Stellar network is expected to be used for trade execution and for "intermediate settlement", but not "final" settlement. Settlement finality is expected to be recognized only by the issuing organization and appropriate legal authorities.

C. Control Over Issued Cryptoassets Post-Issuance

Cryptoassets may be issued in a way which provides the issuer with the ability to exercise limited control over a contributor's lost or stolen tokens. To protect the contributor from improper seizure of their tokens, record of these activities would be permanently stored in a public blockchain. This level of control may result in unexpected legal, regulatory, insurance, tax, and other consequences for the issuer, so thorough research should be performed before issuing a cryptoasset which includes these features. In most fundraising situations today, adding these features will greatly increase administrative costs for the issuer.

Acknowledgment

J.S. thanks Froriep Legal AG for their help in navigating the complexities of offering a new and unique derivative product internationally.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *URL https://bitcoin.org/bitcoin.pdf*, 2008.

[2] Nick Szabo. Trusted third parties are security holes. *URL http://nakamotoinstitute. org/trusted-third-parties/*, 2001.

[3] David Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. *Stellar Development Foundation*, 2015.