Fintelum

July 30, 2019

Fintelum Security Token Offering (STO) Implementation

whitepaper [1]

[1] This whitepaper document is a research paper on a complex problem and the proposed solution, and should not be confused with typical whitepapers produced for the purposes of ICO fundraise.

Contents

Glossary

AML - Anti-Money Laundering is a legal framework that imposes obligations on financial and other institutions to prevent legalisation of criminal proceeds.

Bitcoin - open-source blockchain and currency governed by a decentralised consensus system with cryptographically secured network.

Coin - unit of an asset on a blockchain, typically referred to as a means of value transfer for the underlying blockchain.

Ethereum - open-source blockchain based platform that enables execution of smart-contracts and transferability of Ethereum blockchain-based digital assets.

EU - European Union.

ICO - Initial Coin Offering is a campaign of primary issuance and distribution of utility tokens.

KYC (Know Your Customer) - legal framework which requires financial and other institutions to collect personally identifiable information about its customers.

OTC – Over-The-Counter refers to trades taking place outside of centralised exchanges.

P2P - Peer-to-Peer refers to decentralised software-based trade execution and trade settlement on the Ethereum blockchain, with centrally governed KYC/AML compliance process.

PEP - Politically Exposed Person, refers to someone who holds a prominent public function as well as their family members and close associates.

Securities laws - certain and jurisdiction-variable set of regulations focusing upon issuance and transfer of financial instruments.

Security token - digital asset, which represents an investment contract (financial instrument) and is regulated by the respective jurisdiction's securities laws.

Smart contract - programmable transaction protocol that executes a set of defined terms as functions.

Solidity - programming language that is designed to create Ethereum blockchain-based smart-contracts.

STO - Security Token Offering is a campaign of primary issuance and distribution of security tokens.

Token - unit of an asset on a blockchain with a defined smart-contract functionality.

Utility token - digital asset intended for use on a platform or network in exchange for a specific product or service from the issuer or other users.

Introduction

Fintelum Security Token Offering (STO) implementation is an Ethereum Solidity code base. Built as a standard protocol with modular features, it is designed to tackle the need for a compliant blockchain instrument for the capital markets industry. Most notably, to have a blockchain based tool to represent a transferable security instrument in a given jurisdiction.

This paper describes the code functionality in terms of features. And, it explains the necessity of such implementation as defined by Fintelum business needs within the European Union (EU) laws.

The paper assumes the readers have the basic understanding of how cryptocurrencies work and what blockchains are. It also assumes the reader is familiar with the basic functioning of capital markets and specifically the methods of fundraising and organised trading.

Crypto crowdfunding

From 2013 to the end of 2018, crowdfunding practice in combination with nascent cryptocurrencies resulted in entrepreneurs raising capital in the form of the Initial Coin Offering (ICO). This rewards-based and donation-based crowdfunding was in most cases an Ethereum token offering in exchange for a cryptocurrency payment. In legal terms, during an ICO fundraise, the project was pre-selling a product or service. It was effectively a crowdfunding practice, which was carried out by using the new type of payment – cryptocurrencies.

The resulting utility token was meant to be exchangeable for the services or products. And, it would operate as a fungible and freely transferable unit. Occasionally, the utility token can become popular and begin being accepted as a means of payment outside of the intended network.[2]

[2] This is true of any asset, however, e.g. cigarettes during WWII, or Ramen noodles in prison today. https://bigthink.com/laurie-vazquez/how-ramen-noodles-beat-cigarettes-to-become-a-prison-currency

Token typology

Financial regulators primarily focus on distinction and resulting implications for two types of tokens: utility and security tokens. Several regulators have also distinguished exchange/payment and hybrid token types.[3]

A utility token is defined by the inherent ability to utilise the issued token as a service or redeemable product. Therefore, the issuer must present a certain utility for the purchased token that the buyer will be able to use.

A security token as a concept came to the fore in the year 2017. More clarity and regulation was called for around the exuberant crypto crowdfunding practice. This was because some of the ICO projects were deemed to be offering more than utility baring instruments. Notably, the Securities and Exchange Commission (SEC) had opined that all token sales are securities offers.[4]

For the purposes of this paper, we will continue with focus on the security token type.

---

[3] Swiss regulator FINMA was one of the first regulators to issue token classification guidance in early 2018 with the following 4 token types: payment, utility, asset and hybrid tokens. Malta followed suit with their Virtual Financial Asset test, whereby all DLT assets fall in one of 4 categories: virtual token, virtual financial asset, electronic money, or financial instrument. UK FCA's 2019 Guidance on Cryptoassets mentions 3 types: exchange tokens, security tokens and utility tokens.

See further here: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en

Here: https://www.mfsa.com.mt/pages/readfile.aspx?f=/files/LegislationRegulation/regulation/VF%20Framework/20180831_VFARFAQs_v1.00.pdf

And here: https://www.fca.org.uk/publication/consultation/cp19-03.pdf

[4] https://www.sec.gov/news/speech/peirce-how-we-howey-050919

Decentralisation as a problem

Cryptocurrencies are founded on principles of trustless self governance, openness and borderless decentralisation. These qualities fundamentally define classic cryptocurrencies, such as bitcoin, litecoin and ether. The same principles however become a problem when it comes to law enforcement.

A law abiding token can exist on a blockchain system that possesses the principles of trustless self governance, openness and borderless decentralisation. But, the smart contract – token that represents a security – cannot exhibit such qualities. Quite the opposite, indeed, for the reasons described below.

Tokens, coins and smart contracts

A token is a cryptographic script. It is used as the second layer functionality, or smart contract. It is other than the underlying blockchain coin. A coin, such as bitcoin or ether, works as the inherent monetary unit of the respective blockchain. It powers the chain. And the chain is defined by the coin and its programability. For example, Ethereum blockchain was designed to allow more complete scripting. In difference to the Bitcoin blockchain scripting ability, Ethereum was built as a Turing Complete smart contract platform. [5]

The term smart contract defines the programmability of the underlying chain and was coined long before Bitcoin was invented by the computer scientist Nick Szabo. He described a "smart contract" as:

> a computerized transaction protocol that executes terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.[6]

The Ethereum blockchain allows to lower administrative costs and automate terms of contract as described by Nick Szabo. But, for the purposes of issuing a security token, some of the fundamental principles of trustless self governance, openness and borderless decentralisation need to be reduced to a set of functional limitations, which can be programmed into the smart contract.

There are other viable blockchains build with Turing Completeness. For the purposes of Fintelum STO implementation, however, the Ethereum blockchain was chosen as a battle tested, secure and most readily available smart contract platform.[7]

---

[5] https://github.com/ethereum/wiki/wiki/White-Paper#computation-and-turing-completeness and

[6] See Nick Szabo, Smart Contracts, 1994, http://www.virtualschool.edu/mon/Economics/SmartContracts.html

[7] See more quantitative information on the Ethereum blockchain here https://media.consensys.net/ethereum-by-the-numbers-3520f44565a9 and here https://media.consensys.net/the-state-of-the-ethereum-network-949332cb6895

Issuance and operation

Fintelum business model promotes orderly and compliant fundraise. The offer must be a law-abiding, blockchain based instrument issued to the tokensale participant. Furthermore, Fintelum business requires that the ultimate security token be used to trade amongst the approved or whitelisted participants in both a centralised and decentralised manner. To achieve arbitration and law enforcement, Fintelum remains as the centralised counterparty for KYC/AML compliance.

The following describes issuance and operation of the Fintelum Security Token for primary issuance and subsequent peer-to-peer (P2P) trade against cryptocurrencies:

1. A smart contract with certain set of features (see further, section: STO implementation features) is created on behalf of the issuer. The smart contract contains a token transfer logic, whereas all other data/transaction checks are stored in their dedicated smart-contracts.
2. The smart contract represents the terms of the sales contract or shareholder/owner agreement. It also mandates participant whitelisting prior to investment.
3. Each participant of the fundraise first goes through a compliance check and is then registered in a whitelist, related to the relevant smart contract. This step is carried out by Fintelum.
4. When issuance is concluded, the tokens, representing terms of the contract, are released and distributed to the respective whitelisted participants. The tokens are sent to the indicated Ethereum addresses, managed by the participants.
5. After token distribution, the issuer may elect to list the token on Fintelum P2P trade desk. If listing follows the primary issuance, there are no additional requirements. If listing is applied for using other STO implementation, a token swap may be needed, and a whitelisting will be required among other criteria according to Fintelum listing framework requirements.
6. A listed token holder can place bids and offers on the P2P trade desk.
7. A counterparty can accept bids/offers in full or partial amounts.
8. The parties are assumed to have consented to execute a transaction when one has entered the bid/offer and when the other has accepted the offer/bid.
9. Both counterparties are given instructions to create a transaction from their wallets.

10. The sender of the tokens receives instructions about the escrow smart contract address where the tokens must be sent and what data must be included. Not including the data results in a failed transaction.
11. The sender of the Ethereum blockchain based cryptocurrency receives instructions to which escrow smart contact address to send the funds. In case of ether (ETH), the sender will also receive information about data which must be included in the transaction to ensure valid transaction execution.
12. The transactions are verified by responding smart contracts for whitelisting of both parties and funds are locked in the escrow smart contracts.
13. Escrow contract controller initiates further fund transfers or refunds, if needed.
14. The P2P transaction and settlement is concluded and recorded on the Ethereum blockchain.
15. If any of the parties do not fulfil obligations to transfer funds or tokens to escrow address in a given time frame, a penalty is applied and compensation paid to the other party. Funds or tokens sent to escrow contract are returned to the sender's specified refund address.

Applicable law

Issuance of a security token necessitates compliance with the securities laws. As a rule of thumb issuance and selling of securities to general public (i.e., non-professional investors) requires a prospectus that is approved by the financial regulator, which is a costly and time-consuming process.

The European Union in 2017 adopted the new Prospectus Regulation 2017/1129, which fully applies from 21 July 2019 and replaces the existing Prospectus Directive regime. This EU Capital Markets Union initiative aims to eliminate regulatory arbitrage and ensure investor protection while promoting easier access to capital for small and medium enterprises in Europe.

Prospectus Regulation provides several exemptions when issuers are relieved from producing a full-scale prospectus. Each EU member state may set a national limit for prospectus-free issuance within the bracket of EUR 1 Million to EUR 8 Million issuance amount per annum (there may be however other national disclosure requirements that apply). Equity crowdfunding as a relatively small scale securities issuance currently relies on this exemption.[8]

Another EU initiative is currently in the legislative process, namely, the Crowdfunding Regulation which would create an EU-wide framework for crowdfunding under 8 Million EUR limit. Final adoption and entry into force will take a few more years. Until then crowdfunding relies on Prospectus Regulation exemption and national rules in each EU member state. [9]

---

[8] Read more on Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017R1129

[9] Read further on the Crowdfunding Regulation proposal in Europe. Position of the European Parliament adopted at first reading on 27 March 2019 with a view to the adoption of Regulation of the European Parliament and of the Council on European Crowdfunding Service Providers (ECSP) for Business http://www.europarl.europa.eu/doceo/document/TA-8-2019-0301_EN.pdf

Legal requirements

In light of investor protection, a simple Ethereum blockchain token standard does not suffice to ensure the full scope of legal requirements. There must be the guarantees given by the issuer to the investor towards the fulfilment of the terms of contract. The law requires that investors are protected insofar as the contract/agreement stipulates investor rights to certain benefits. These can be:

- ownership rights and issuer's obligation to protect and reinstate lost or stolen item (following a proof of ownership);
- voting rights and issuer obligation to take the vote into account;
- right to income (dividends, profit or revenue sharing) and issuers obligation to pay;
- right to ownership inheritance and issuer obligation to administer;
- right to information and issuer obligation to provide true and unobstructed information;
- litigation rights;
- distribution of assets in case of liquidation;
- other specific contractual rights emanating from the terms of contract.

In addition to the investor rights, the issuer must enforce know your customer (KYC) and anti-money laundering (AML) measures. These are levied on the participating investor and include:

- identifying the main beneficiaries with telematic or face-to-face methods of identification;
- verifying the personal information;
- identifying if the beneficiaries are politically exposed persons (PEP) or included in any public sanction lists;
- ensuring verification of the source of wealth and the invested capital in fiat and cryptocurrencies.

From the above legal requirements it follows that the token issuance that is deemed to be representing a security instrument ***cannot*** be:

- freely transferable;
- accepting unverified investors;
- accepting unverified funds;
- freely traded on the secondary market;
- anonymously issued;
- lacking oversight and control.

Therefore, decentralised transferability and unverified issuance must be replaced by mandated KYC/AML compliance and inherent features allowing for exogenous controls and strict compliance with the relevant law.

Every jurisdiction may require a set of varying features. Therefore, the Fintelum STO standard must be modular and flexible in its implementation.

Fintelum is a compliance and technology provider to the issuing entities. The token issuer can therefore outsource the above legal requirements to a platform such as Fintelum.

Features

The following set of features define Fintelum STO implementation as defined by Fintelum business needs within the European Union (EU) laws, see above.

Verification

Ability to verify beforehand that transfer of security tokens will be successful. If transfer were to be unsuccessful, the data indicating the expected failure reason will be returned.

Transferability

Contract controller is be able to forcefully freeze and transfer security tokens, in case of an asset recovery event or if legal action is required.

Modifications

Allows to specify data that will be processed at the time of transaction. This data then can be used to perform various operations, depending on smart contract implementation.

Categorisation

Security token asset subset which can have special status/metadata associated with them, i.e., the class of shares, shareholder rights, transfer restrictions.

Reading

If an Ethereum node is listening to specific smart-contract events, it is able to read related updates.

Subscribing

Support for subscribing for updates regarding documentation, where the subscriber must have access to the Ethereum node that is listening to specific smart-contract events.

Splitting

Ability to split one security token owner's holdings into several wallets.

Lock-ups

Allows for time (block count) based restrictions to be imposed at the time of issuance or at any event of the token transaction execution, e.g. selling tokens or buying additional tokens.

Whitelisting

Identified persons and their respective Ethereum wallets are linked and registered on the blockchain in obfuscated form. Support for restricting the range of asset classes across jurisdictions and token ownership and transfer only among whitelisted persons.

KYC expiry

Enforcement of KYC expiry date through suspension of transactions, e.g. through metadata requesting more specific error code.

Advanced payments

Ability to distribute to token owners' wallets other tokens (e.g. stablecoins) as dividends.

Compatibility

Ensuring compatibility with the Ethereum Improvement Proposals (EIP), previously Ethereum Request for Comments (ERC) standards[10], is important to be able to use the existing, well established, secure and decentralised Ethereum blockchain platform. Primarily, the Fintelum STO implementation ensures the following compatibility features:

Transferability

Ability to transfer assets between any Ethereum addresses / wallets.

3rd party allowance

Availability to add allowance to transfer certain amount of tokens to unrelated Ethereum address / wallet.

Allowance transferability

Ability to move the allowance between any Ethereum addresses / wallets.

Queries

Permission to query addresses / wallets for balance / allowance.

Contract information availability

Providing basic token information, such as the supply, decimals and total number of holder's addresses.

[10] There is often confusion regarding usage of EIP and ERC designations for Ethereum standards. Authors deem that EIP is more appropriate designation for already established Ethereum standards.

EIP (ERC) standards compatibility

#1410

This standard describes the ability to sort assets under different categories and amounts. This allows to track total balance and the balance of each asset category, as well as any arbitrary data about each individual token group.

Analogy: a deck of cards which would be categorised in four suits, and each suit value would be the number of cards from each stack: 15 card deck with 7 spades, 3 hearts, 2 clubs and 3 diamonds. This is because in a standard EIP-20 token contract, one can only recognise that there are 15 cards, but not the suit of each card. The #1410 standard enables several important features:

(1) queries balances by asset group and which asset groups are owned by a specific address. From analogy example we could ask how many spades does the address own or which suits are owned by the address;

(2) enables transfers of specific asset categories;

(3) adds a management layer in which asset category manager(s) can manage asset categories according to their rights. For instance, the manager of clubs category assets cannot make operations on diamond category assets. Managers are determined by each individual token holder;

(4) adds a layer of transfer management that prevents the transfer in case if transfer is prohibited, depending on the asset category or associated meta-data and returns data about reason of transfer failure.

Some of theses features are overridden by EIP-1400 STO standard requirements. For example, since #1400 standard must comply with EIP-20 token, this means that an algorithm must be integrated that will determine which asset category is transferred when transfer operation is requested without specifying the category.

#1594

This standard defines functionality required for issuing new tokens and redeeming existing tokens. It provides an ability to verify if transfer would be successful or would fail for various reasons. The #1594 defines transfer that can have off-chain data passed into transfer function call which then can be verified/processed (example: transfers can only be made if 3rd party signature, which is passed as

data with transfer request, can be verified). Amongst features, the #1594 standard:

(1) adds the ability to verify if transfer would fail/succeed and returns status for the failure reason;

(2) includes the ability to make transfers that have off-chain data provided as part of transfer request;

(3) enforces methods native to EIP-20, such as: view total supply; view address balance; add allowance; view allowance; transfer allowance out; make simple (no data on asset classes) transfer;

(4) supports the ability to issue/redeem tokens and provides status if token can be issued or not.

#1644

The #1644 provides a standardised interface that is used to check if token can be managed unilaterally by authorised controller. It also provides interface for controller, if such exists, to make the necessary transfers.

Since security tokens are subject to regulatory and legal oversight (the details of which will vary depending on jurisdiction, regulatory framework and underlying asset) in many instances the issuer (or a party delegated to by the issuer acting as a controller, e.g. a regulator or transfer agent) will need to retain the ability to force transfer tokens between addresses. The #1644 standard:

(1) enables the controller to force transfer/redeem tokens between different token holders;

(2) adds an ability to check if such controller exists for the security token;

(3) logs all controller actions, and ensures that off-chain data can be provided with each controller operation (to provide reasoning behind specific action).

#1643

The #1643 standard adds an ability to associate documents with smart-contracts and query their statuses and modifications. Examples of documentation could include offering documents and legends associated with security tokens. This includes the following features:

(1) adds reference to a published document, specifying where the document is located (URL), it's name and checksum (using a secure hashing algorithm);

(2) retrieves the document information by name;

(3) lists all the documents;

(4) removes the documents.

This smart contract standard makes no mention of how the document management rights are controlled.

#1066

This standard defines how a smart-contract returns status codes to indicate request state and/or failure reasons. Otherwise it doesn't provide any distinct features, since the idea is already incorporated by #1410 and #1594 transfer methods. As far as STOs are concerned, there is still ongoing discussion about status codes to be used.

Interoperability and external integrations

Interoperability with external service providers, such as trading platforms or transfer agents is feasible insofar as compliance with issuer's KYC/AML rules is enforced. Depending on the jurisdiction, each issuance may have a modular token setup, consisting of the above features in full or partially. The most salient feature however consists of mandating KYC/AML compliance and allowing for exogenous controls for strict compliance with the relative law.

The present Fintelum STO implementation can be integrated with external services. There are two basic scenarios:

As a Fintelum client

An entity, such as authorised market-maker for an exchange wishing to list a project that has used Fintelum STO implementation, can become an owner of a portion of the tokens. The acquired tokens will allow for the market-maker to make bids and offers on the exchange. In order to obtain ownership rights, the market-maker and all participants involved in token trade become Fintelum clients and undergo the same KYC/AML procedure as all other token holders. The compliance levels may vary in requirements from project to another.

As an independent operator or transfer agent

An entity such as authorised exchange may need to become the sole token transfer agent and therefore an independent operator of the issued security. In this scenario, Fintelum would relinquish its responsibilities towards the issuer as an outsourced token transfer agent. The new transfer agent must ensure whitelisting in line with the issued token KYC/AML compliance requirements. In order to migrate the transfer agency rights, Fintelum will perform the change of the controller or everyday operator on the blockchain. The new transfer agent will provide their own set of transaction addresses. Fintelum will remove all rights and responsibility from operating the smart contract(s) and related escrow services. Such transaction ensures the election of a new everyday operator or token transfer agent.

Business continuity

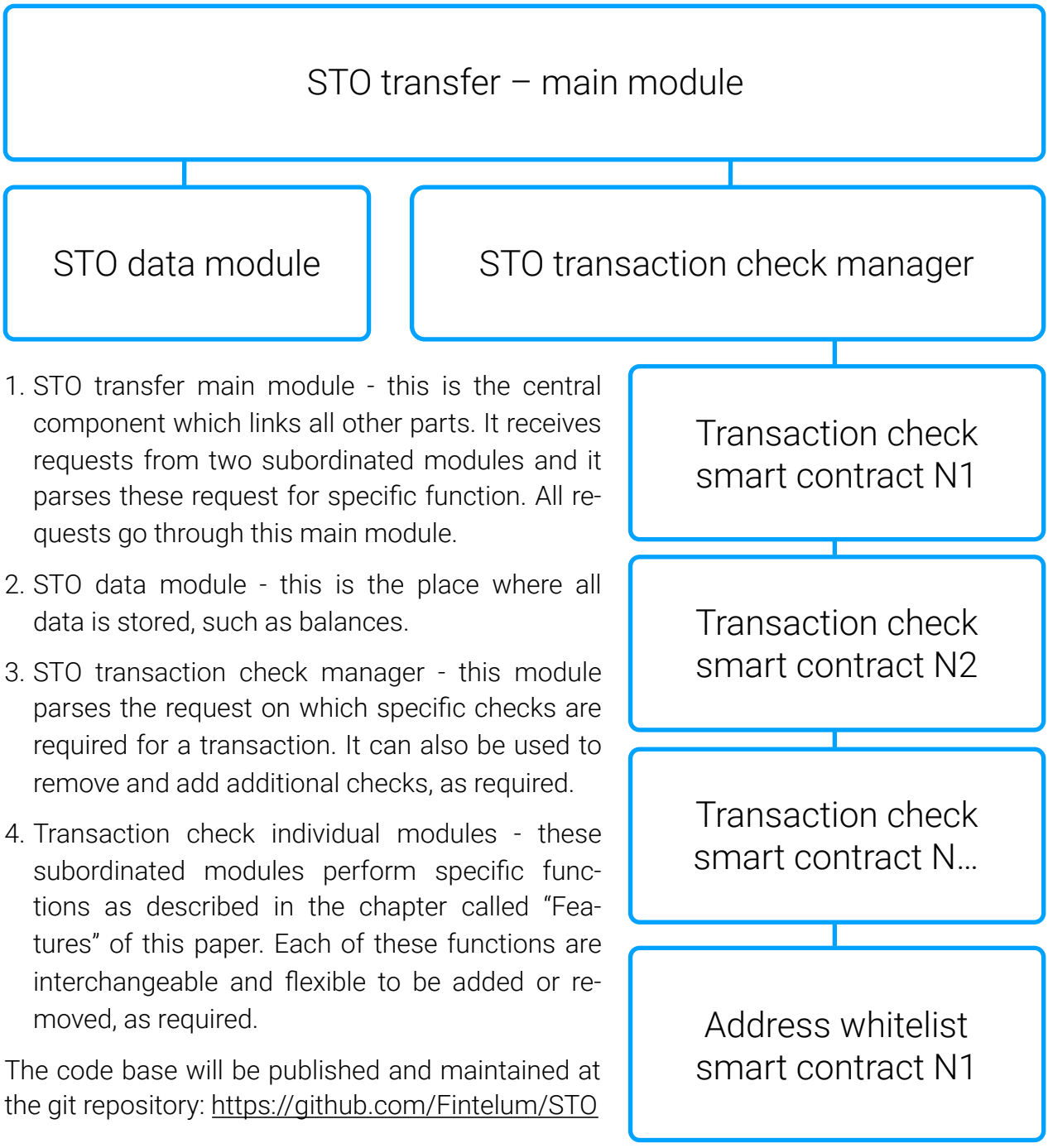
A security token is a cryptographic representation of an agreement. It is the second layer representation to facilitate management of a legal agreement/contract between two or more parties. The token itself should not be considered an object of the agreement, but a mere representation of the terms made therein.

The Fintelum STO implementation is built on the Ethereum blockchain due to the security and robustness of this Turing Complete scripting platform. If the Ethereum blockchain fails for any reason, the token can be replicated on other blockchains, following the same business and legal requirements, and pursuant to the decision by the issuer.

The Fintelum STO implementation can therefore be considered chain agnostic, insofar as the relative legal requirements and Fintelum business needs are satisfied.

Technical implementation

Fintelum STO implementation is comprised of several components:



1. STO transfer main module - this is the central component which links all other parts. It receives requests from two subordinated modules and it parses these request for specific function. All requests go through this main module.
2. STO data module - this is the place where all data is stored, such as balances.
3. STO transaction check manager - this module parses the request on which specific checks are required for a transaction. It can also be used to remove and add additional checks, as required.
4. Transaction check individual modules - these subordinated modules perform specific functions as described in the chapter called “Features” of this paper. Each of these functions are interchangeable and flexible to be added or removed, as required.

The code base will be published and maintained at the git repository: https://github.com/Fintelum/STO

Open questions

The established capital markets are centrally governed, whereas only qualified and professional market participants have broad access to regulated exchange platforms. Banks and brokers ensure KYC/AML compliance. Transactions are done with accepted legal tender, or fiat currencies.

In the context of present-day capital markets structure, some of the open questions concern applicability of the Fintelum STO implementation. Is there a demand for capital market securities to be represented by cryptographic tokens? Is there a need for non-professional investors to access capital markets for primary securities issuance and secondary trading?

This can be demonstrated with a successful business case which does not come into conflict with the applicable law. A business should be able to perform an orderly issuance and secondary trading as a professional service. Accountability can be ensured with appropriate disclosures and voluntary transparency.

Conclusion

In this paper, we have addressed the technical description of the Fintelum STO implementation as well as revealed the business needs for it as a standard protocol. We have examined a set of modular features that may constitute such a security token and proposed a certain protocol base for a law-abiding Ethereum blockchain-based instrument, usable in the capital markets industry. We have equally addressed interoperability and possible external integrations that the industry participants may need to take into account. Furthermore, we have elicited the technical implementation and provided a link to the full source code base.

With this paper, we at Fintelum hope to have achieved our contribution to the overall tokenisation industry advancement. We are conscious that our proposed implementation is one of several possible. And we anticipate there will be others.

It is, however, most notable to demonstrate our understanding of the business and legal requirements to justify the security token implementation.

If our presumptions are correct, this standard implementation can serve as a benchmark for the industry at large.

About

Fintelum is an IT development company, authorised by the Estonian Financial Intelligence Unit (FIU) to provide cryptocurrency custodian wallet and exchange services in compliance with EU AML laws. Fintelum's main product is a token launch platform, specialising in security token offering (STO) and initial coin offering (ICO) primary issuance and secondary P2P trading with emphasis on know your customer (KYC) and anti-money laundering (AML) compliance, technology and advisory services.

For more information, visit fintelum.com

You can follow the company on Twitter, Telegram, LinkedIn and Facebook.