



2018 Global STO Market Report

Hashgard Labs 2018/10
Authors: Tom Huang, HY, Kerin Yin, Arion Shi
Contact: contact@hashgard.io

TABLE OF CONTENTS

Introduction to security tokens	4
1.1 The concept of the security token.....	4
1.2 Types of security tokens.....	5
1.3 Pros and cons of security tokens offering	6
1.4 How does the SEC determine the security token?	8
The security token global industry map	10
2.1 Trillion dollar market size	10
2.2 Tech-solution agency	10
Polymath	11
Swarm	14
Harbor	15
Securitize	17
Securrency	18
ERC1400 standard	18
Hashgard TAMT Standard	20
2.3 Exchange	20
2.3.1 Cryptocurrency exchanges	21
2.3.2 Traditional stock exchanges.....	23
2.4 Peripheral service provider.....	25
Bancor	25
Slice (Investment Bank)	25
2.5 Existing security token cases	25
The policies and attitudes of countries towards security tokens	28
• United States	28
■ Regulation A+	28
■ Regulation D	29
■ Regulation S	30
• Singapore	31
• Austria	31
Hashgard STO Market Perspective	32
How will STO change our lives?	34
Annex 1: Comparison of the design of security tokens	35
1. Summary	35
2. Basic information	35
3. Main content and differences of the standards	36
3.1 General nature	36
3.1.1 Fungible Token and Non-fungible Token	36
3.1.2 ERC-1410 standard and tranche	36
3.1.3 Classification and scene	36
3.2.1 Verification function of transfer restrictions	37
3.2.3 Transfer function	39
3.3 Compatibility	41
3.4 Other differences	41
References	43



Hashgard is a distributed, trusted asset management protocol and a high functionality next generation digital finance public chain. Hashgard's vision is to become the infrastructure for the trusted, inclusive, intermediary, and programmable digital finance.

The Hashgard Technology Empowerment Platform is the first dapp on our public blockchain to provide enterprise-level services for a diverse blockchain ecosystem, including but not limited to digital asset management, STO services, enterprise-level collaboration, smart contract deployment, community token airdrop distribution, media promotion, and legal compliance.



Hashgard Labs is initiated by Hashgard and supported by blockchain and finance industry experts. It focuses on in-depth industry research, project incubation, standards formulation, market education and etc. Hashgard Labs envisions ourselves to be a leading global research institution worldwide in the domain of digital finance.

If you have any questions or business corporations, please contact us with email: contact@hashgard.io.

You can also follow us through our media channels:

Official Website: <https://hashgard.io>

weibo: @Hashgard

Telegram: <https://t.me/hashgardeng>

Medium: <https://medium.com/@hashgard>

Twitter: <https://twitter.com/Hashgard1>

Reddit: <https://www.reddit.com/r/Hashgard>

INTRODUCTION TO SECURITY TOKENS

With the potential to replace ICOs, revolutionize traditional finance, and become a \$10 trillion dollar market by 2023, it's no surprise that the entire blockchain industry is talking about Security Token Offerings (STOs).

The crypto industry went through a rapid period of transformation in 2017, driven in large part by the ICO financing model. On the one hand, ICOs facilitated the widespread promotion of digital tokens, making cryptocurrency a household name. However, on the other hand, many projects took advantage of the unregulated legal environment and committed a number of violations that resulted in heavy financial losses for investors.

With the bursting of the bubble and tightening of legal regulations in 2018, both project managers and investors lost trust in utility tokens and their financial model. Gradually, the industry arrived at a consensus that security tokens, which are regulated by law and linked to assets, can be an appropriate replacement.

At the same time, companies looking to access financing from the \$70 trillion traditional capital and equity markets must do so through IPOs and long-term investment models, which feature extremely expensive barriers to entry, leaving ordinary investors with little chance to participate. In the debt and real estate market, sky-high investment thresholds not only prevent ordinary investors from participating, they also limit the liquidity of assets to a great extent.

STOs address issues and needs from both traditional finance and the new digital economy, which is one of the core reasons that STOs are rising so quickly in popularity.

This report will provide a comprehensive analysis of the global STO market in 2018, including STO classification, determination, some pros and cons of security tokens, key players and technologies in the industrial chain of security token certification, and regulatory policies of various countries that affect the STO market. At the end of the report, we will present Hashgard's exclusive view of security tokens.

1.1 The concept of the security token

Currently the market divides cryptocurrencies into two categories: utility tokens and security tokens. Most utility tokens are issued by companies for fundraising projects for their own products or services. In general, issuance of this type of token is somewhat similar to the pre-sale of a product or service.

Security tokens, on the other hand, are usually backed by assets with intrinsic value, such as equity, limited liability company shares, or commodities. A security token can be used to pay dividends or interest, or to make investments in other tokens or assets to create profits for

token holders. The field of use of security token is very broad, for example, in hedge funds, real estate, bonds, etc. [1].

At the moment, there is no clear definition of the security token, but according to the general understanding in the industry, it can be simply defined as the legalized tokenization of assets. This definition mainly includes two points:

- 1) The issuance and trading of the token must comply with the regulations of relevant government agencies;
- 2) All types of assets (tangible and intangible assets) are transferred in the form of a token on the blockchain.

Regulatory compliance is critical for security tokens. For example, in the case of issuing securities in the United States, the security token is subject to the regulation of the SEC and other relevant institutions. Securities token issuance is also subject to federal law. Generally speaking, the securities token requires registration with the SEC (except for exemptions from certain terms, such as Reg A+, Reg D, Reg S, etc.), subject to the provisions of the Securities Act. Regulations push up the issuance and transaction costs of security tokens and, by consequence, the threshold for participation.

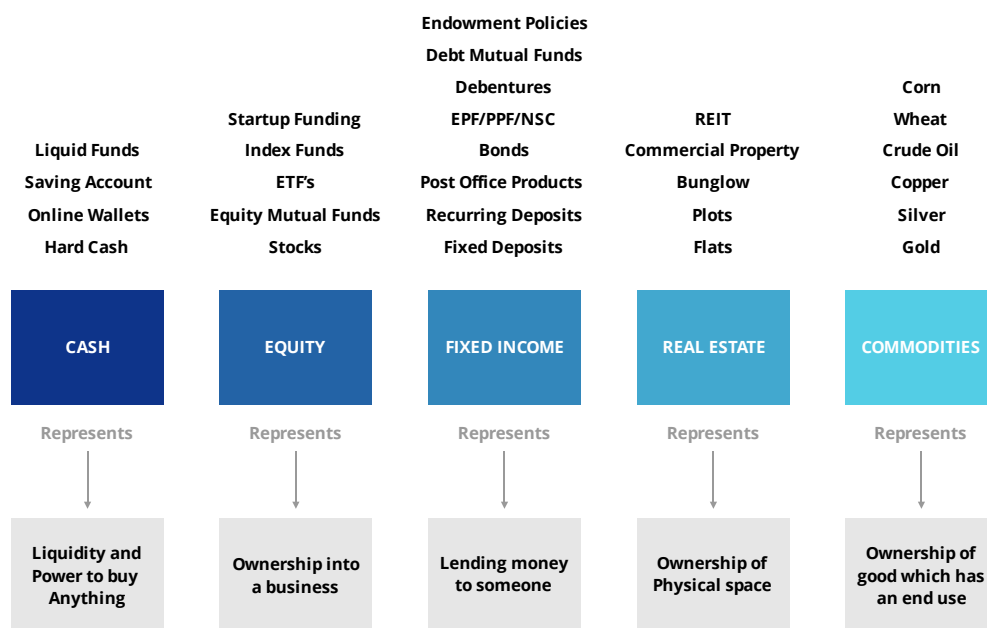
1.2 Types of security tokens

As the name “security token” implies, the tokens are supported by real assets, such as property rights. They may also be used to pay for various profits, interest, etc., to bring benefits to asset holders.

Drawing on asset classification in the traditional financial world, security tokens can be broadly classified into the following five categories of assets [3]:

- 1) Cash: these assets are cash in legal tender. The money in our wallet is also a kind of cash asset. The closest thing to this is probably the many stable coins that have been released recently. However, the stable currency itself cannot be considered an investment, so we will not discuss it here.
- 2) Equity: these assets represent ownership of physical or digital entities. For example, if you own 10% of Google’s stock, one of your rights is to lay claim to 10% of Google’s net profit. If the asset ownership is to be tokenized, the profit and voting rights can also be distributed according to the owner's holding ratio.
- 3) Bond: the most typical example of bond assets is a fixed loan. It allows the holder to obtain a fixed income, such as interest income, after a fixed period of time. Investing in such assets can provide investors with a fixed income, while a portion of the investment profit goes to the investment manager.

- 4) Real estate assets: there are two ways that real estate assets, like ordinary houses, can be tokenized. The first is to divide real estate into smaller shares, like equity assets. The second is to regard it as a debt-type asset and to tokenize the rent income that it brings.
- 5) Commodity assets: investment in bulk commodities, such as raising funds for the purchase of a rare material or service, can also be tokenized. Ownership of the material or service can be distributed via tokens, and if the token holder wants to rent to a third party, that sort of transaction can also be tokenized similarly to a fixed-income asset.



With the exclusion of cash, all asset types can be tokenized, delivering the above-mentioned liquidity and other benefits. Alternative asset classes, such as art and collectibles, are also areas in which security tokens can be used. Therefore, the potential of tokenization is truly enormous.

Another way to classify security tokens is by equity tokens and asset tokens. Equity tokens represent the ownership of an asset, while asset tokens are the mapping of real assets in the real world, such as gold and real estate.

1.3 Pros and cons of security tokens offering

Each coins has two sides, and STOs are no exception. Although the cost of issuance has increased due to regulations, security tokens still offer powerful advantages [2]:

- 1) Reducing investment and trading thresholds: for example, a very pricy office building can be split into theoretically infinitely small units using security tokens, which greatly reduces the investment threshold, enabling any ordinary person to participate in the project.

- 2) Enhancing asset liquidity: for example, in a private fund with a closed period of 10 years, investors can only recover their investment after 10 years, but if the fund is tokenized, investors can buy and sell fund shares at any time with more effective flow of assets.
- 3) Lower issuance costs compared to traditional financing methods: traditional IPO issuance and transaction costs are extremely high, amounting to 4-7% of fundraising (PwC). STOs greatly reduce those issuance costs.
- 4) Reduced fees for international transactions: security tokens can reduce the cost and difficulty of trade between countries and regions, lowering regulation barriers between countries.
- 5) Improving market efficiency: as these tokens can be sold and traded worldwide (as long as they are compliant with all relevant legal frameworks), asset pricing will be more equitable, price discovery mechanisms will be more efficient, and therefore more attractive to investors.

Security tokens have the potential to revolutionize capital markets. However, there are some potential drawbacks to STOs. Mr. Tim, a former US Federal Reserve Bank and Federal Deposit Insurance Corporation (FDIC) bank censor, said that STOs have three major limitations compared to ICOs [5]:

- 1) Investor accreditation limitations: non-accredited investors in the United States may not be able to invest in STO projects. STO issuers who issue and sell security tokens in the United States must be registered or exempted from the US Securities and Exchange Commission. This also means that under the SEC's regulatory requirements, STO projects will likely be issued only to accredited investors or very wealthy individuals.
- 2) Higher cost than Utility token offering: STO platform service providers (such as underwriting companies) can provide services to ensure that STO activities comply with SEC regulatory requirements, leading to a cost increase and a marked decrease in the amount of financing compared to ICO financing.
- 3) Secondary market trading restrictions: unlike functional tokens, security tokens can only be traded on licensed exchange platforms (with the securities trading license of the country in which they are located) due to the existence of compliance thresholds. In addition, for a certain period of time tokens can only be traded between qualified investors.

Further, securities-based tokens also have certain problems and risks at the operational level, such as:

- 1) Offline management issues: for instance, if the general public hold tokens comprising overall ownership of an asset, there should be a SPV(special purpose vehicle) to handle the operations.

- 2) Liquidity bubble risk: when the liquidity of assets increases, the price of assets tends to have a liquidity premium, forming asset price bubbles, which can lead to huge increases in volatility and uncertainty.
- 3) Technical security loopholes: there is no technology that can be absolutely secure. If the KYC/AML process or the underlying protocol of the token is modified or exploited, the losses faced by investors may be enormous.

Last but not least, we need to mention that STO tokens currently do not have an opportunity to provide liquidity on the secondary market (like crypto exchanges) yet, the reason being, is that only licensed or some decentralized exchanges are qualified to list them. This means that the listing process takes a longer time.

The above mentioned problems still require close attention from the whole industry.

1.4 How does the SEC determine a security token?

Since security tokens require supervision by securities regulators and other government authorities, the way the SEC determines the security token is important for the existing tokens and for the utility and security tokens that will be issued in the future. The decision tool that is currently used by the SEC is the Howey test.

The Howey test requires that an "investment contract" (such as a token) should meet the following four requirements:

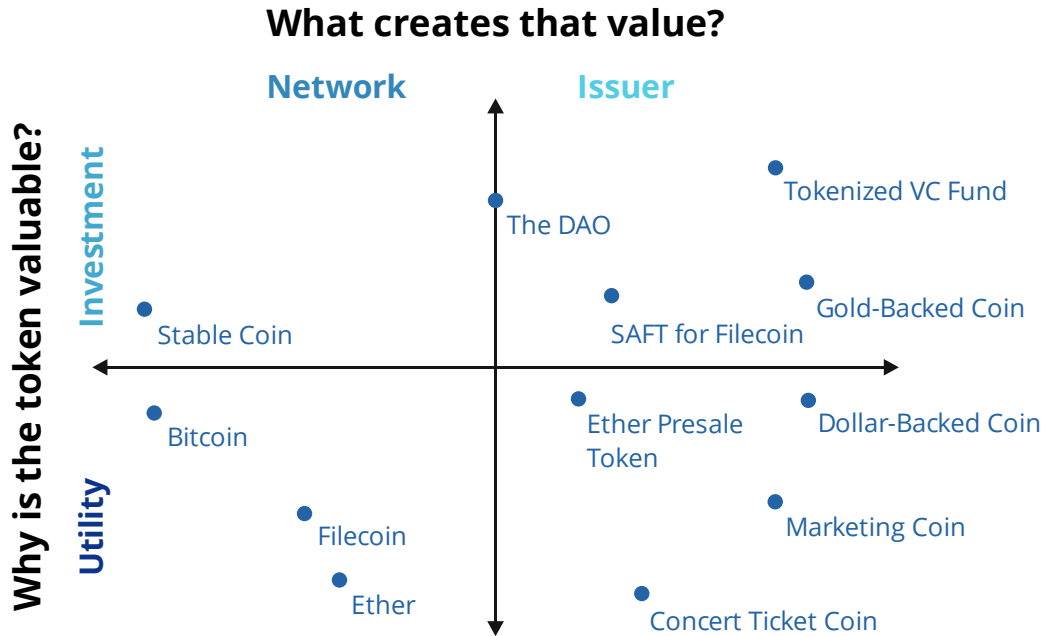
- 1) Investors invest cash or equivalents;
- 2) All inputs are pooled into the same project or pool of funds;
- 3) Investors have profit expectations, which means most investors aim to make a profit;
- 4) Profitability is entirely dependent on the efforts or operations of the founder or a third party.

Each condition has a series of sub-questions that are scored. When the score reaches a certain value, the "investment contract" is considered to be a security.

There is currently a simple two-dimensional test that can quickly determine whether a token is a security or not [6].

- 1) Is the token resold as an investment?
 - We need to think of tokens as "black boxes." We put money into the token and when we take the money out, there should be more money than was put in or a certain product/service resulting from the original money put in. If you receive a return on invested funds, the token may be considered a security.

- 2) Does the value produced by the investment depend on a person or an agent?
- We need to check whether the value of the token is created by one person or by one entity, or by a group. If the value is created by a person or an entity, it may be considered a security. Therefore, according to the two-dimensional method, we can distribute the token according to the classification:



If governments will regulate cryptocurrencies to the full extent of the law, many cryptocurrencies will be classified as security tokens and, as a result, withdrawn from mainstream exchange platforms [7].

In addition to the Howey Test, the Reves Family Resemblance Test and the Risk Capital Test can also be used to determine securities classification. At the same time, we must note that these tests are only tools used by the SEC, and that the SEC reserves the final right to determine whether or not a token is a security.

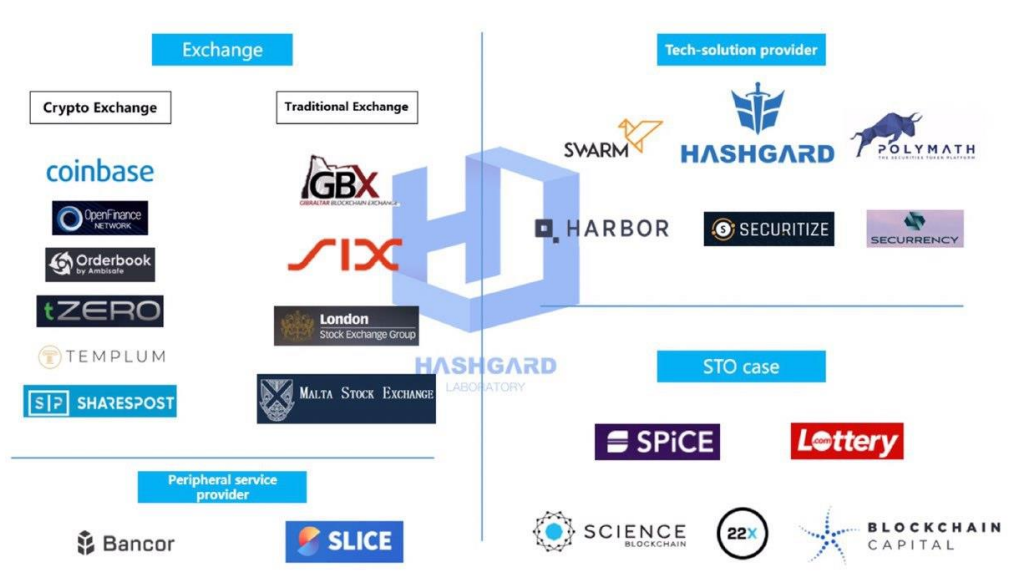
THE SECURITY TOKEN GLOBAL INDUSTRY MAP

2.1 A trillion dollar market

With regards to the global \$70 trillion stock market, \$100 trillion bond market, and \$230 trillion real estate market (about \$180 trillion in residential space, \$32 trillion in commercial, etc) [3], security tokens have great application and development potential, especially in terms of ensuring compliance with securities law and regulation requirements.

In 2017, the total value of security tokens totaled about \$100 million, while the total market value of functional tokens totaled \$500 billion. The security token industry mainly involves four types of entities: projects, tech-solution providers, exchanges, and peripheral service providers.

Among the four types of entities, exchange platforms have the highest policy entry threshold as they are required to obtain a license issued by a government regulatory agency to offer security token exchange services. The tech-solution providers and peripheral service providers assist with technical, compliance, and liquidity services for the project side in order to provide guarantees for the issuance and trading of the tokens.



In the following passages, we will introduce the enterprises in the industry chain one by one according to the steps from issuance to transaction.

2.2 Tech-solution providers

First of all, unlike the comparatively simple process of utility token issuance, security token issuers require a specific token technology solution at the protocol level as well as legal compliance services. Since security tokens set certain requirements for investors, it is

necessary to limit security token trading to compliant investors, among other conditions and limitations.

In the era of centralization, compliance is implemented through centralized exchange platforms. However, in the decentralized blockchain world, once the token leaves the exchange platform, compliance requirements are difficult to implement. Therefore, it is necessary to embed an executable compliance instruction within the token smart contract, which is equivalent to programming in the regulatory framework. Tech-solution providers step in to help projects maintain compliance at the protocol level. As a result, the following tech-solution providers have emerged as major market players, and nearly all of these companies have their own protocol.

Distribution solution agency	Polymath	Swarm	Harbor	Securitize	Securrency
Established	2017	2014	2018	2018	2015
Agreement	ST-20	SRC20	R-token	DS-token	-
Issued tokens	PLOY	SW M	-	-	-
Funds raised	\$59 mln (ICO)	\$5.5 mln (ICO)	\$38 mln (VCs)	-	-

Polymath

- Introduction: Established in 2017, Polymath is a platform designed to help conduct security tokenization for assets. It provides an underlying protocol for security tokens (ST-20) that allows individual and institutional investors to complete accredited investor certifications, allowing legitimate investors to participate in STOs in compliance with government regulations. On the Polymath platform, KYC service providers, legal consultants, technology developers and investors are brought together. The Polymath protocol is dedicated to the issuance of fully compliant security tokens, which embed the need for financial regulation into the design of the token, enabling a seamless experience of issuing and trading securities transactions on the blockchain.
- Progress: Polymath revealed that the company is attempting to acquire shares in the Barbados Stock Exchange and is in the process of cooperating with the alternative trading system tZero [8].
- Financing: \$59 million (ICO)
- Platform introduction:
 - There are five types of participants in the Polymath platform:
 - 1) Investor: an individual or organization that wants to buy or sell security tokens
 - 2) Project: participants who want to tokenize their assets
 - 3) KYC: service provider who verifies the identity of the investor, where he or she resides, etc.
 - 4) Legal Agent: legal compliance and consulting service provider

5) Developer: software developer writing smart contracts

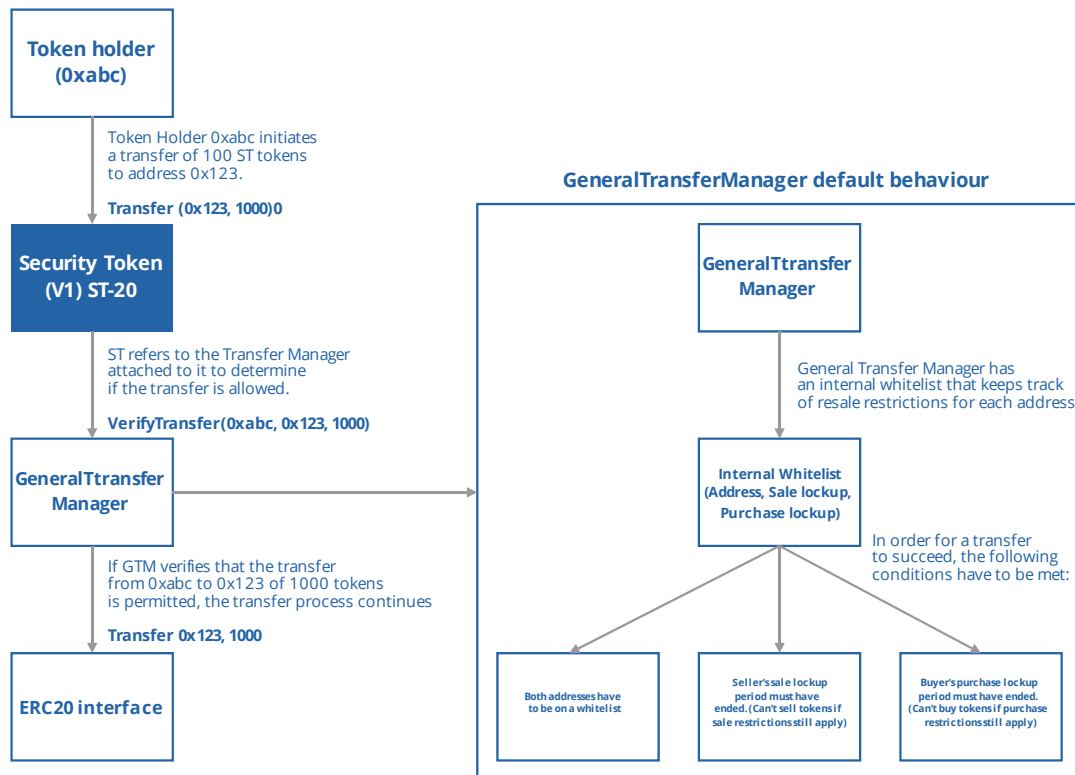
■ Project party issuance process:

- 1) The project party first uses the ST-20 protocol to generate its own security token on the Ethereum platform. At this point, all the tokens are on the project side and do not support the transaction (until the legal agent completes the work and passes the compliance procedure)
- 2) The project party first selects the legal agent in both directions in the platform to jointly complete the compliance procedures of the token.
- 3) The project party sets the trading restrictions of the token according to the compliance requirements, for example, only accredited investors may be able to purchase certain tokens. When it is necessary to write the transaction restrictions suggested by the legal agent into the contract of STO, the project party can select the technical developer to introduce the requirements into the blockchain source-code of the deal.

■ Investors purchasing process of the token

- 1) Investors complete KYC through KYC service providers on the platform
- 2) After completing KYC, one can purchase a token that meets one's needs. When the project party of the individual token has additional KYC requirements for investors, investors must also submit the documents required by the project party. When purchasing a token through an exchange platform, investors also are asked to submit relevant documentation.

- Introduction to ST20 implementation: Upon first entering the ST-20 interface, new users must first verify their identity before conducting token investments or transfers. Before investors can purchase a token from the initial issue, they must be whitelisted. The whitelisting process can be performed by the issuer in whatever way they want, and the end result will be a whitelisted list of Ethereum addresses added to the secure token smart contract. This whitelist now contains the Ethereum address of the person who can hold the token and is a list for confirming whether a transfer can occur or not.



The above diagram illustrates a typical token transfer scenario:

- 1) The holder of tokens 0xabc has 100 TORO tokens that she wants to transfer to her friend 0x123.
 - 2) 0xabc will use her favorite wallet to initiate the transfer by inputting her friend's ETH address and the name of token that she wants to send to her.
 - 3) Since TORO is an ST-20 token, the transaction will proceed internally though the verifyTransfer process before the transfer is conducted.
 - 4) In turn, verifyTransfer uses the GeneralTransferManager whitelist to determine if a transfer between the two accounts is possible.
 - 5) GeneralTransferManager will check 3 things before approving the transfer:
 - a) Both the sender and the recipient are in the internal whitelist
 - b) 0xabc (seller) is not subject to sales restrictions as stipulated by the Securities Act
 - c) 0x123 (buyer) is not subject to purchase restrictions under the Securities Act
 - 6) If the above conditions are met, the checkTranstest process is passed successfully and the transfer transaction can be executed.
- Polymath security tokens are designed in a modular fashion way that allows users to create additional modules in order to extend or modify the behavior. For example, multiple transport managers can be connected to it to control the transfer logic on different switches.

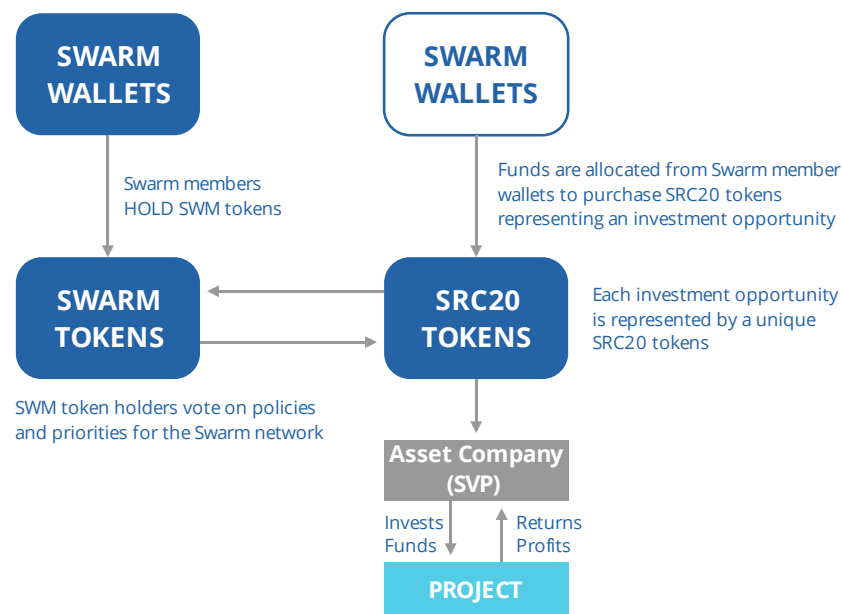
Polymath protocol open source code: <https://github.com/PolymathNetwork/polymath-core>

Swarm

- Introduction: Founded in 2014, Swarm is a decentralized STO issuing platform and marketplace. Launched in January 2018, the Swarm investment platform enables use of SWM, BTC and ETH in making investments in physical assets that have been tokenized, purchasing tokens that have been minted based on the SRC20 protocol, and obtaining the ownership, management rights (by voting on the SecureVote platform), and profit rights to various assets.

Today the Swarm platform is based on the token-D and Stellar networks.

- Features:
 - Investment Building Key Opinion Leaders (KOL): the Swarm platform encourages experts to set up their own investment portfolios, so that other investors can join their portfolio or follow expert investments.
 - Voting system: Swarm employs a voting method similar to that of stocks, but with additional mechanisms added in, such as lock-in mechanisms.
 - AI smart investment: when information is transparent, Swarm's AI algorithm can automatically adjust investment portfolios
- SWM token
 - ERC20 standard token
 - Use scenario: create sub-funds, participate in STO, purchase exclusive information, and get the right to take part in Swarm platform management



- SRC20 protocol
 - Introduction: SRC20 defines a set of rules that security tokens must follow and enables developers to build applications customized to operate well with technical profiles of various assets. Applications built in the Swarm ecosystem can communicate with each other, while ERC-20 token and SWM are also supported. Investment platforms, asset management tools, and exchange platforms can be built into application form using the SRC20 protocol.
 - Differences from ERC-20: SRC20 boasts additional functionality compared with the ERC-20 standard. For example, descriptions of the characteristics of real-world assets, including address, purpose, legal status, obligations, trading restrictions, and other parameters, are built into the SRC20 protocol.
- Financing: \$5.5 million (2017.12.31 ICO)

Harbor

- Introduction: Harbor is an open source platform based on the Ethereum blockchain. It helps to create a decentralized R-token compliance protocol to meet the requirements of securities, taxation, and other regulatory frameworks for security token issuance based on ERC20. Its standardization process includes KYC/AML compliance services, taxation, information disclosure, etc.
- R-token protocol:
 - An open source standard for the definition of fully compliant security token transactions, implementing KYC, AML, taxation and other regulatory compliance services on the Ethereum chain.
 - Harbor’s R-token protocol is a specific kind of smart contract of the ERC-20 token, which is used mainly for checking if the ERC-20 tokens meet certain regulatory requirements before transactions can be executed.

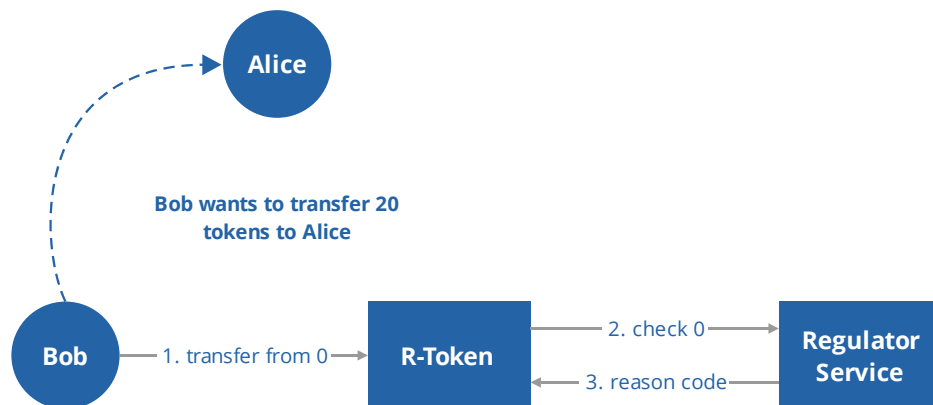
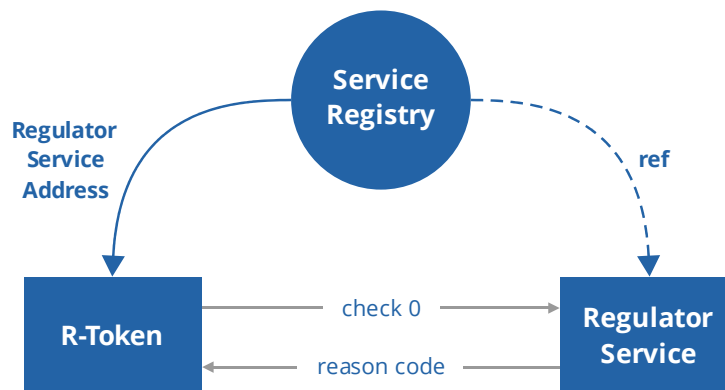


Figure2: Example of an R-Token transfer sequence

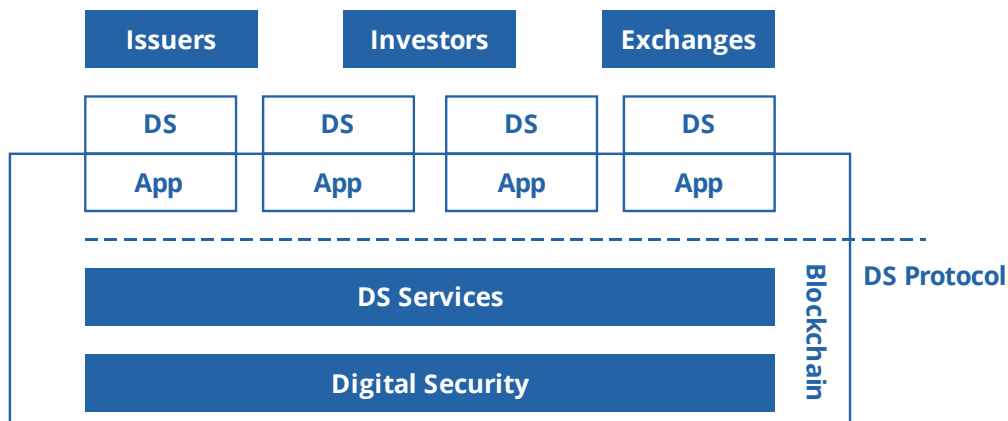
- A token compliant with R-token standards can be traded on any exchange platform that supports the ERC-20 standard.
- There are two compliance levels with R-token:
 - 1) Participant level: Token issuers can decide the circumstances that allow tokens to be sent and received. For example, they can decide the qualifications that investors must meet before they can receive tokens.
 - 2) Token level: Token issuers can lock in the trading rules and limit the number of tokens that can be sent. For example, token issuers can lock in the time that is specified by Reg D and set the upper limit of the number of tokens that a qualified investor can hold.
- Connection between R-token, regulatory service and service registry
 - 1) All three cooperate with each other in order to complete the compliance transaction of the tokens.
 - 2) The service registry sends the applicable regulator service address to the R-token, which checks whether the transaction meets regulator requirements. To a certain extent it acts as a regulator of transactions.



- On the initial stage, all the regulatory requirements are uploaded to the regulator service by the trade controller (could be individual or agency, Harbor currently manages many of those uploads).
- Regulator service and service registry both can be written into R-token smart contracts. These three form the backbone to Harbor smart contracts
- Progress: Harbor launched its own platform for securities issuers and licensed brokers in summer of 2018
- Financing: The San Francisco-based startup raised a \$10 million Series A funding round in January 2018 and raised another \$28 million in April. Investors include Founders Fund, Pantera Capital, Craft Ventures, VY Capital, and Valor Equity Partners.

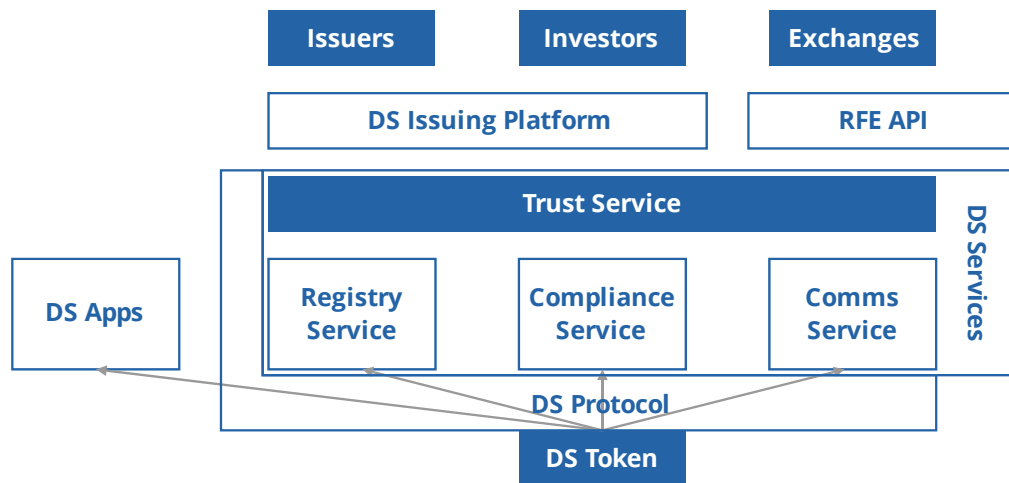
Securitize

- Introduction: Founded in January 2018, Securitize emerged as a spin-off company from venture capital firm SPiCE VC. The Securitize Digital Security service (DS service) platform facilitates security token issuance and transactions while enabling third-party developers to build a wide range of applications. Interactions between applications are managed by the DS Protocol. Initially, work will start within the Ethereum network and may migrate to other networks in the future.



Securitize's Digital Ownership Architecture

- Securitize platform composition:
 - 1) DS token: the DS Protocol is layered on the basis of ERC-20. The DS token can check the tradable status of the account to prevent the occurrence of illegal transactions. In addition, securities attributes, such as dividends, voting rights, and transactions, have been fully integrated, so that security tokens have characteristics nearly identical to traditional securities.
 - 2) DS app: The platform supports third-party distribution and transaction lifecycle applications, such as distribution applications, exchange applications, voting applications, or dividend applications.
 - 3) DS service: the infrastructure of the DS protocol, that can be used by the DS app
 - a) Trust service: management of different stakeholders
 - b) Registration Service: investor information stored on the chain
 - c) Compliance Services: implementation of specific compliance requirements for DS tokens
 - d) Exchange service: provides a communication platform for relevant investors



Securitize's Digital Protocol Ecosystem

- Securitize will provide the exchange with an API under the chain to facilitate access to the ecosystem, enabling access to KYC information, among other functionality.
- Progress: Securitize has reached service agreements valued at over \$500 million with a number of companies, including CryptoOracle, Kairos.com, Lottery.com and 22X Fund.
- Financing: Unknown

Securrency

- Introduction: Securrency was established in 2015 and has positioned itself as a Reg-Tech, providing a smoother securities transaction compliance service.
- The company's platform includes several products:
 - 1) Securrency: helps issuers meet regulatory compliance standards and execute the transaction or transfer of security tokens;
 - 2) RegTex: provides services such as KYC/AML regulatory compliance, information disclosure, investor qualification and tax payment;
 - 3) SmartContraX: Blockchain Smart Contract Development Service;
 - 4) InfinXchange: provides standard interfaces for payments, transactions, asset pricing and other trading activities
- Progress: in July 2018, Securrency announced a partnership with SharesPost to enable issuance and trade of compliant security tokens through the SharesPost platform and the ATS system.

ERC1400 standard

- In addition to the protocols developed by the above service providers, such as the ST-20 protocol of Polymath, a new standard that was named ERC1400 has also been proposed.

If the standard is adopted by Ethereum, ERC1400 will compete with the protocol described above, which is the "redevelopment" based on ERC-20.

- The standard was developed by Gosselin, Adam Dossa, Pablo Ruiz and Fabian Vogelsteller. Among them, Gosselin and Dossa work for Polymath, while Ruiz has an international business and financial background, and Dossa is an Ethereum developer and web designer. The team experience is complementary and therefore has a certain strength.
- The ERC1400 will support EIP's requirements for "legal proceedings or recovery of funds", which means "that the regulations may require the issuer or a trusted third party to obtain the authority to transfer the tokens on behalf of the investor."
- At the same time, the ERC1400 tokens will be non-substitutable (or at least "partially substitutable"), allowing additional modifiable metadata to be specified, thereby allowing users to set unique transfer conditions. In other words, ERC1400 tokens must allow parties providing securities to grant or reject transactions based on a range of conditions, such as whether or not:
 - 1) Transferred securities are subject to a lock-up period.
 - 2) The sender and receiver have gone through the KYC process.
 - 3) The issuer is certified
 - 4) The license contract enforces the maximum number of investors or limits the percentage held by individual investors.
- Partial substitutability is a major component of the ERC1400 standard. This means that one ERC1400 token may not be exchanged with another ERC1400 token issued by the same entity because the tokens have different attributes. The most popular non-substitutable token is of course the CryptoKitties that are based on the ERC721 standard: you don't exchange a kitten directly, because each kitten is unique and the price varies. However, ERC1400 tokens are not necessarily different from each other like CryptoKitties - so they are "partially interchangeable."
- Another partial interchangeability of ERC1400 is reflected in how it supports the split and combination functions of the token. For example, bonds with different maturities and risk levels can be combined into a pool according to an investor's preferences. For instance, investors can include 5 to 30 years both high and low risk mortgages in a safe mortgage portfolio.
- Currently ERC1400 is still in the drafting stage. It was assigned with the official number (1400), which means that it has been considered by EIP editors to be suitable for the Ethereum community's considerations and feedback. The progress of the ERC1400 deserves our further attention.

Annex 1 provides additional information about the comparison of several types of major token standards at the code level.

Hashgard Trusted Asset Management Token (TAMT) Standard

- Introduction: Trusted Asset Management Token (TAMT) is a protocol standard proposed by Hashgard. TAMT is a token issued on the basis of Hashgard's trusted asset management protocol, representing the holder's rights and ownership of digital financial assets. The standard is backward compatible with ERC20, and is open source, easy to expand, and has no need to trust the counter-parties with the atom exchange function.
- Compared with the traditional asset management scheme, TAMT not only realizes the right of financial assets owned by investors, but also the asset management process of financial assets itself is stored in the chain.
- Historical transaction records cannot be tampered and the performance of financial products is reliable, authentic and credible; TAMT also has a good privacy protection for the strategy of financial asset management itself.
- The manager sends a trading order to the TAMT contract through the interface, and does not need to write the strategy algorithm into the contract; TAMT also streamlines the calculation of fund manager performance and profits distribution. The manager can issue a special token to obtain the corresponding income.

TAMT is currently in the drafting stage, and will be implemented on the Ethereum network first before being migrated to the Hashgard public chain in the future.

- TAMT characteristics
 - compatible with ERC20
 - Asset pool (inquiry, capital contribution, etc.)
 - Transaction limit module (KYC/AML, token lock up, account freeze, etc.)
 - Advanced Token Insurance Module (supports the collection of multiple digital assets)
 - Contract level atomic switching function
 - Dividend management
- Significance: TAMT, as an important protocol based on the Hashgard digital finance public chain, will provide underlying support for credible asset management which is simple, easy to regulate and functional.

2.3 Security Token Exchanges

Currently, a relatively large number of exchange platforms offer security token support. They can be roughly divided into two categories: emerging cryptocurrency exchanges, such as Coinbase, and traditional securities trading platforms, such as the London Stock Exchange Group.

We grouped the exchange platforms according to this categories as follows:

Currency exchange	Coinbase	tZero	OFN	SharesPost	Orderbook	Templum
Established	2012	2017	2014	2009	2017	2017
License situation	Brokerage business, alternative trading system and investment advisory license	Alternative trading system, route and trade execution license	-	Alternative trading system license	-	Alternative trading system license
Financing situation	\$ 100 mln (VC)	\$134 mln (STO)	Huobi invested, sum unknown	\$15 mln (VC)	-	\$10 mln (VC)

2.3.1 Cryptocurrency Exchanges

Coinbase (United States)

- Background: established in February 2012, Coinbase is a well-known cryptocurrency exchange platform in the United States.
- Progress: as Bloomberg reported on July 17, Coinbase was approved by the US Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA) to successfully acquire Keystone Capital Corp., a licenced securities dealer (broker-dealer license), Venovate Marketplace Inc. (ATS license) and Digital Wealth LLC (a registered investment advisor (RIA license). The deal will allow Coinbase to expand its products to securities trading as a broker-dealer.
- License status: brokerage business, alternative trading system (ATS) and investment advisory license obtained via above-mentioned acquisitions
- Financing: in August 2017, Coinbase raised a \$100 million investment round with a total valuation of \$1.6 billion. Acquisitions in May 2018 drove the valuation to \$8 billion.

tZERO (United States)

- Background: established in 2017, tZERO is a subsidiary of US e-commerce giant Overstock (NASDAQ: OSTK). It was designed to become the world's first compliant security token exchange platform. On June 19, 2018, tZERO announced the establishment of a joint venture with BOX Digital Market, with each company to take half of the board seats. In this collaboration, BOX is responsible for providing transactions and supporting compliance while tZERO will provide trading system technology, funding and management. BOX is an options exchange platform that holds an alternative trading system (ATS) license.
- Progress: tZERO completed its STO on October 12, 2018. According to its public documents, the tZERO STO was issued under the terms of Reg D 506(c) and Reg S. All

investors are accredited investors and have gone through KYC/AML. It is worth noting that transactions with BOX are still awaiting SEC approval.

- License status: tZERO has two companies registered with the SEC and that are FINRA member institutions: routing and execution broker SpeedRoute LLC and ATS system PRO Securities LLC.
- Financing situation: in December 2017, tZERO conducted an STO, but the fundraising period was extended 4 times. On June 29, tZERO announced that they had raised \$134 million. GSR (Jinshajiang Ventures) invested \$30 million into tZERO and \$104 million in the parent company Overstock.
- tZERO token: tZERO issued its own security token TZRO, which is based on ERC20 standard. TZRO token holders will receive 10% of the adjusted gross income of tZERO every quarter.

OpenFinance Network (OFN) (United States)

- Background: established in 2014, OFN promises to become the first fully compliant security token trading, clearing, and settlement platform in the United States. OFN aims to adopt a centralized order matching system and decentralized trading methods.
- Progress: The OFN platform was launched in June 2018 after several months of beta testing by early investors and partners. Despite the fact that the current function has been registered and gone through KYC, trading has not yet been opened, and a launch date has not been set. It is reported that after the opening of trading only SpiceVC, or Blockchain Capital will be supported. At the same time, non-accredited investors can only buy and sell tokens issued by Reg A+ and Reg CF.
- License information: License information for OFN was not publicly available at the time of publication
- Industry Cooperation: on May 1st, 2018, security token issuance service provider Securitize and OFN announced a cooperation, enabling security tokens issued via Securitize to trade on the OFN platform. Issuing service provider Harbor also became an OFN partner later in May.
- Financing situation: fire coins and venture capital institutions are invested in OFN, the specific number and valuation is unknown.

SharesPost (United States)

- Background: established in 2009, SharesPost is a traditional online equity market trading platform based in the United States. It is reported that the trading platform has 50,000 accredited investors, with a total historical turnover of more than \$4 billion.
- Progress and financing: on June 20, 2018, SharesPost completed a \$15 million Series C financing round. Investors included Shanghai-based LUN Partners and Hong Kong-based

Kenetic Capital. SharesPost plans to use the funds raised to build its ATS system and expand throughout Asia. The company has also announced plans to expand the business line to include a trading platform that supports both security tokens and utility tokens, which is set to launch in the second half of 2018.

Orderbook (United States)

- Introduction: founded in 2017, Orderbook was launched as a decentralized exchange platform powered by blockchain technology service provider Ambisafe.
- Progress and financing: in March 2018, Orderbook announced that it will issue a specific Regulatory Award Protocol (RAP) to automate the investor certification process. By cross-validating the compliance of local laws and regulations with the RAP holder's personal information database, compliance of STOs and other cryptocurrency-related transactions is guaranteed. For example, when an investor who does not comply with regulatory requirements attempts to buy coins through the exchange, the system will match the investor's license level with the internal database to prevent these non-qualified purchases.

Templum (United States)

- Introduction: Templum was designed as an issuance and secondary trading market for security tokens. Templum obtained an Alternative Trading System (ATS) license by acquiring Liquid M in January 2018. Similarly to other solutions, Templum has built-in AML/KYC certification services to ensure that the platform complies with regulatory requirements.
- Progress: the trading system is online. Blockchain startup BanQu has successfully completed Templum's TAO procedure and BCAP token is currently trading on the platform.
- Financing: SBI (Softbank) invested \$10 million into Templum in April 2018

2.3.2 Traditional stock exchanges

Traditional Stock Exchange	London Stock Exchange	SDX Digital Exchange	Malta Stock Exchange	Gibraltar Stock Exchange
Country	Great Britain	Switzerland	Malta	Gibraltar

London Stock Exchange

- Background: founded in 1571, the London Stock Exchange is one of the oldest and largest stock exchanges in the world

- Progress: according to Coindesk, the London Stock Exchange and FCA (UK Financial Conduct Authority) are working with startups Nivaura and 20|30 to develop a fully compliant Ethereum-based security token. On September 20, 2018, the company started its first "white mouse" test release process, along with a one-year lock-up period. The security token issuance service may be opened later on for startup companies and small and medium-sized companies.

SIX Digital Exchange (SDX) (Switzerland)

- Background: SDX is a part of the Swiss exchange, one of the largest exchanges in Europe. SDX claims to be the world's first platform to provide end-to-end asset tokenization services, including the issuance and trading of tokens. The exchange will be supported by the Swiss National Bank and regulated by the Swiss Financial Regulatory Authority (FINMA).
- Progress: in July 2018, SIX announced that it is developing an integrated transaction, settlement and custody infrastructure for security tokens. The entire project will be carried out in phases, with the first service potentially launching in mid-2019.

Malta Stock Exchange (MSE) (Malta)

- Background: MSE's MSX announced that it has partnered with Neufund (German STO platform) and Coin Security to create a global decentralized securitized token exchange that will deliver and maintain EU securities regulation compliance.
- Progress: MSX, Neufund and Coin Security plan to launch a pilot project in late 2018 to complete the issuance of the Neufund security token and trade it on Binance or other compliant secondary market platform.

Gibraltar Blockchain exchange(GBX), Gibraltar

- Background: the Gibraltar Stock Exchange announced the establishment of security token trading platform Gibraltar Blockchain Exchange (GBX) at the Hong Kong Financial Summit in October 2017. The Gibraltar Stock Exchange was established in 2014 and holds a license issued by the Gibraltar Regulatory Authority. GBX currently supports trading for some online funds and bonds.
- Progress: according to the white paper, GBX plans to launch a security token in the third quarter of 2018, with transactions set to be allowed in the fourth quarter. However, according to recent news, GBX is seeking an online banking and trading license from the Gibraltar Financial Services Commission (GFSC), which may be implemented only in the first quarter of 2019.

2.4 Peripheral service provider

In addition to STO issuance organizers and secondary market transactions platforms, institutions that offer peripheral services around STOs and transactions, such as liquidity and investment banking services, have also emerged as market players.

Bancor

- Introduction: Bancor is a liquidity service provider that presents a liquidity model that hooks multiple currencies to a pool of funds, ensuring liquidity even at very low transaction volumes.
- Progress: SPiCE VC joined Bancor's network and retained up to 5% of capital to use BNT as an intermediary. SPiCE VC holders can redeem other currencies through the Bancor network, including ETH, etc.
- Financing: Amount Raised: \$152M (ICO)

Slice (investment services)

- Introduction: Slice is a commercial real estate investment platform for cross-border investors. Its functions are similar to the underwriters, distributors and placing agents of quality real estate securities. Slice combines the Bancor protocol with the Stellar public chain's embedded decentralized exchange platform to ensure high liquidity for commercial real estate security tokens issued on the Slice platform.
- Slice investors can choose to get a stable quarterly dividend from real estate that generates cash flow, or choose to get higher but irregular time dividends from high-yield value-added items.

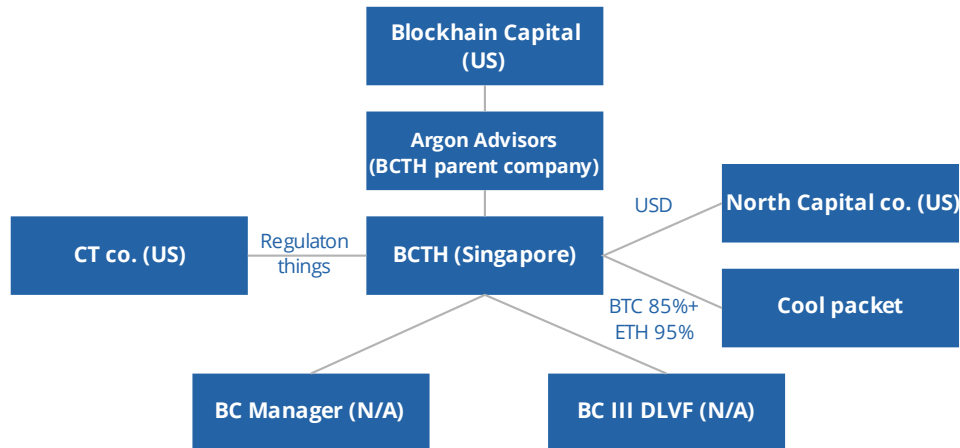
2.5 Existing security token cases

SPiCE VC

- Introduction: SPiCE VC focuses on high-tech investment. Holders receive 100% of the returns when withdrawing from the fund.
- Status: the supervision of the token and the token products has not been developed and may develop rapidly, which may have adverse consequences. In addition, regulatory developments may change the nature of SPiCE VC services or limit the use of blockchain assets or the operation of blockchain networks that SPiCE VC will rely on.

Blockchain capital

- Introduction: Blockchain Capital may be the first fund to conduct STO for the public. \$10 million (Hard Cap) of tokens were sold in just six hours. According to the currency white paper, the Foundation's managing partner charges a 2.5% management fee and a 25% performance bonus. The remaining profits will be distributed to the holders of the tokens.
- Organizational structure:



- BC BCTH (blockchain capital token hub) is the issuer of this token, it is registered in Singapore.
- Blockchain Capital is the parent company of BCTH and is registered in the United States.
- Third-party compliance outsourcing service provider CT corporation (Delaware Registration) is responsible for supporting the BCTH compliance process.
- ICO supports payment in currencies: USD, BTC and ETH
- US dollars raised are managed by a trust account established by North Capital Private Securities Corporation, a self-clearing broker dealer, licensed to provide hosting services for Reg D, Reg A+, Reg S and Reg CF.
- 85% BTC and 95% ETH collected are put into a cold wallet, while the remaining BTC and ETH are used to cover cold wallet operating expenses.
- BC III DLVF is the main body of the management fund account. The registration location is currently not listed. BC Manager is the main body of management personnel. It's registration is currently also unknown.
- Issuance of regulatory evidence: mainly based on the Securities Exchange Act of 1934 and the Investment Company Act
- Status of supervision:
- No US Securities and Exchange Commission ("SEC") or any state, provincial or territorial securities commission or any other regulatory body has approved or disapproved the BCAP token or determined whether the memorandum provided is true or complete.
- BCAP Tokens may not be sold directly or indirectly within the territory of the People's Republic of China (excluding Hong Kong)

Science Blockchain

- Introduction: Science Blockchain is a fund and incubator that focuses on blockchain investments. SCI token holders enjoy 70% of the fund's income rights. It is worth noting that the fund repurchases part of the token to push up the price.

Lottery.com

- Introduction: Formerly named AutoLotto, Lottery.com provides mobile lottery services. The company plans to use blockchain technology to improve its payments, transparency, flexibility and scalability in the international markets.
- Progress: Lottery.com's private placement sales of its security-type token are close to completion, allegedly raising hundreds of millions of US dollars. The site will pay dividends to the holders of its security token based on total gaming sales. Securitize and Cashbet have aligned with Lottery.com to help bring the token to market.

22X FUND

- Introduction: The 22nd startup of the famous American accelerator 500 Startups has jointly established a new security token fund called 22X Fund. Of the companies that graduated from the 500 Startups startup camp in 2017, no more than 30 winners will receive investment from 22X Fund. The fund will hold 2.5%-10% of each startup. Holders of tokens issued by 22X Fund can obtain their return through exchange trading or repurchase mechanisms.

THE POLICIES AND ATTITUDES OF COUNTRIES TOWARDS SECURITY TOKENS

Although the tokenomics of security tokens and STOs has become a hot topic in the industry, most national governments have maintained a cautious and encouraging attitude towards security tokens, while regulatory bodies of various countries have not yet put forward a clear regulatory policy. No relevant direct policy for the different categories of security tokens exists yet, but it is logical to assume that securities tokens will be subject to existing securities law regulations and frameworks. In the following section, we provide a brief overview of several of the most dominant national regulatory frameworks in the industry.

United States

US securities law requires companies to submit strict information disclosures and complete the compliance process from the perspective of protecting investors, so companies must pay a considerable cost of entry. Since companies that issue STOs are often startups, they may encounter certain difficulties in fully complying with SEC registration requirements. Therefore, finding a relatively low-cost compliance approach is related to the development potential of security tokens.

And such an approach already exists. According to the US Securities Act of 1933, the sale of any securities (stocks, bonds, various types of notes) needs to be registered with the SEC. However, when the issuer meets certain conditions set out in existing securities law, they may be exempt from SEC registration (but still subject to supervision). The main securities law clauses that allow exemption from SEC registration are Reg A+, Reg D, and Reg S. Reg D is the main private financing regulation, Reg S is the regulation for overseas investors, while Reg A+ is equivalent to a small IPO, and requires 2 years of audited financial information. By issuing a security token under one of the above three terms, the issuer will reap significant cost savings while at the same time maintaining compliance with regulatory requirements. We briefly outline the terms below.

- **Regulation A+:**

- According to Title 17 of the Code of Federal Regulations, chapter 2, part 230, in order to facilitate the financing of small and medium-sized startups, Reg A+ stipulates that the company can be exempted from the requirement to register with the SEC in the case that the company meets certain requirements and can be exempted from the obligation to be financed only by accredited investors. Moreover, companies registered either in the US or in Canada both can enjoy the convenience provided by Reg A+.
- Regulation A+ exemption regulations are divided into two layers.

- 1) Reg A+ first layer. The issuer can raise up to \$20 million in 12 months, with no restrictions on investors, but must submit a prospectus to the US Securities and Exchange Commission, register the securities issue with the state securities regulator, and provide the previous fiscal year (not audited) financial statements.
- 2) Reg A+ second layer. The issuer can raise \$50 million in 12 months. Non-accredited investors can only invest up to 10% of their net assets or annual income, whichever is higher. The issuer is required to provide audited financial statements for the previous fiscal year and will continue to provide semi-annual and annual audited statements.

- **Regulation D:**

- According to Chapter 17 of the Code of the Federal Regulations, the SEC registration obligation can be waived when the terms Rule 504, Rule 505 and Rule 506 of Reg D are satisfied. [9]
- Rule 504: as long as the following rule is met and the fundraising activity of \$5 million can be completed within 12 months, qualifying companies can be exempted from SEC registration (purchasers need to be accredited investors). However, the Form D still needs to be submitted, which requires investors to provide some simple information, such as address, etc. At the same time, according to Rule 504 investors cannot sell securities again for at least 6 months.
 - 1) The issuer is fully registered in one or more states that require the issuer to publish the registration documents and give the investors full disclosure of the documents.
 - 2) In the case that the issuer registers in the state where public registration documents and disclosure documents are required, and the buyer's state's regulations do not require the issuer to provide these documents, it is also possible to proceed as long as the documents are delivered to the investors before the securities are released.
 - 3) Issuance is possible only in states that allow public solicitation and marketing as well as the possibility not to register (on condition that only accredited investors can purchase)
- Rule 505: in addition to Rule 504, among the fundraising activities under \$12 million completed within 12 months, 35 non-accredited investors and unlimited number of accredited investors may be exempt from SEC registration. However, issuers must still submit Form D documentation, which requires investors to provide some simple information, such as address, etc. At the same time, according to Rule 504 investors cannot sell securities again for at least 6 months.
- Rule 506: the 506 clause is divided into two cases 506 (b) and 506 (c). If the conditions of either of the cases are met, registration is not required, However, issuers must still submit Form D documentation, which requires investors to provide some simple information, such as address, etc. At the same time, according to Rule 504 investors cannot sell securities again for at least 6 months. [10]

- 1) 506 (b): SEC registration can be waived if all of the following conditions are met
 - a) The company does not conduct any public solicitation and public marketing
 - b) Unlimited accredited investors and up to 35 non-accredited investors are allowed to participate
 - c) The company needs to clearly define the investment conditions with the accredited investors. At the same time, non-accredited investors are required to provide Reg A+ compliant information or equivalent SEC registration information.
 - d) The company responds to the investor's queries
- 2) 506(c): this clause allows the company to make public solicitation and public marketing as long as the following conditions are met:
 - a) All investors are accredited investors
 - b) The company assists certified investors in checking all the necessary documents, such as w-2s, tax forms, bank certificates, etc.

● Regulation S

- Reg S allows non-US persons to invest in US companies and be exempt from SEC registration requirements, but only under two conditions:
 - 1) Securities sales and transactions must be conducted overseas of the United States
 - 2) Issuers, distributors and all other relevant institutions are not allowed to conduct "directed selling efforts" in the United States, including public advertising.
- Reg S sets a "distribution compliance period" similar to a lock-up to prevent the circulation of securities back to the US, at least 40 days (bonds), 6 months (stocks), or 12 months (required by the issuer). During this period, the asset can not be sold to US persons, including non-US nationals residing in the United States. [11]

US Security Token Regulation Overview

Main terms	Reg D		Reg S	Reg A+	
	506 (b)	506 (c)		Level 1	Level 2
Raise amount limit	no	no	no	\$20 mln	\$50 mln
Securities type restriction	no	no	no	Asset payment securities are not allowed	Asset payment securities are not allowed
SEC review requirement	no	no	no	Yes	Yes
State registration requirement	Exempt	Exempt	-	Yes	Exempt
Lock-up period	Yes	Yes	Yes	no	no

Singapore

- Issuance requirements for security tokens are identical to conditions and regulatory requirements for issuance of traditional securities. However security token issuance can also enjoy some exceptions. For example, security token offerings may not be required to issue a circular for the offering. However, STOs may still be required to meet certain other conditions, including:
 - 1) Limited issuance volume (no more than S\$5 million in 12 months);
 - 2) Private placement (issue to 50 investors max in 12 months);
 - 3) Issuance only to institutional investors (institutional investors have legal definition);
 - 4) Issue only to accredited investors (accredited investors have legal definition).
 - 5) Some advertising restrictions
- In addition to these options, offshores such as the Cayman Islands (the jurisdiction of choice for projects including EOS, among others), the Virgin Islands, and a bevy of other offshore jurisdictions favored by cryptocurrency companies are also available. One major requirement for issuers registered in those jurisdictions is KYC/AML, due to tax avoidance worries.

Austria

- The Austrian Financial Market Authority has recently issued a guidance on ICO to provide classification and regulatory advice on encrypted assets from a regulatory perspective. AFMA divides cryptocurrency into three categories: utility tokens, security tokens and payment tokens. Among them, the security token issuer's right to claim payment (future cash flow) can be structured according to company law or debt law. AFMA's regulation of security tokens:
 - 1) For issuers: public offering of security tokens requires the issuance of an officially audited securities prospectus and is subject to capital market law unless exempt.
 - 2) For exchange platforms: Depending on the transaction structure, the exchange operator needs to have a trading concession, for example as a stock exchange or a multilateral trading system (MTF) or an organizational trading system (OTF). After the exchange platform starts trading the securities token, it shall comply with relevant regulations to prevent insider trading and market manipulation, and shall fulfill its information disclosure obligations in accordance with local regulations.
 - 3) For investment service providers: Service providers that offer investment advice, asset management, and agency delivery services are also required to hold a trading franchise license.
 - 4) For third-party hosting platforms: It is required to hold a specific license and comply with the relevant laws and regulations of the securities law according to the type of business, with the focus on anti-money laundering and anti-insider trading regulations.

HASHGARD LABS'S PERSPECTIVE: DESPITE INITIAL HURDLES AND CHALLENGES, STOS WILL ULTIMATELY SUCCEED

STOs represent a completely new funding mechanism for both blockchain companies and traditional financial capital players. After nearly 10 years of tokenization of various aspects of the traditional economy, we believe that 2019 will become the year that security tokens are legally issued. We see great potential in this new type of asset, but we maintain a cautious optimism. STOs differ from utility token issuance and require the support of the global regulatory system.

These are the core challenges and opportunities for STOs that we have identified:

1) The true maturity of the STO market requires regulatory support

First, compliance issues require systematic support from multiple government agencies, and such systemic support can take a very long time. There are many regulatory agencies involved in the registration, issuance, and trading of security tokens, and these regulators have yet to build up comprehensive regulatory frameworks that cover security tokens and STOs. For example, to equate the token with the rights it represents, it is necessary for the regulator to audit the technology source-code and formally acknowledge on the national legal level that the code is equal to ownership on the consensus that "code is law." Moreover, the process will become even more complicated in regards to cross-border transactions and multinational legal systems.

2) For small and medium-scale companies, STO global compliance costs are too high

At the legal level, STO issuance is subject to regional legal restriction towards accredited investors, which will have a negative effect in terms of liquidity. Also, due to the fact that specific regulations regarding STOs are absent from all jurisdictions, even in regions with highly developed legal frameworks for securities law, the cost of STO issuance compliance will be very high. This will be one of the main factors preventing small and medium-scale organizations from conducting STOs.

3) The investment threshold is lower, but there is still need for professional guidance

At the same time, security token issuance is set to greatly reduce the threshold for investment and improve the liquidity of various asset classes. For example, ordinary individuals can hold multiple crypto assets at low cost. On the other hand, they lack the ability to invest professionally. Investors may not be able to identify the quality of assets, which may lead to rampant speculation. As a result, demand for investment institutions with professional capabilities to guide STO investors will emerge.

4) Security tokens is set to revolutionize rights division and attribution in traditional financial markets.

The security token may well become a revolutionary asset package, which would make various traditional assets, such as the equity, dividends, voting rights, etc. undergo division and

reorganization. The distributed ledger technology of blockchain can greatly reduce the cost of asset confirmation and the transparency and efficiency of transactions, thus breaking through the division of rights and attribution confirmation in the traditional sense.

5) Security token have special technical requirements

Due to the nature of the security token, we believe that the associated blockchain must have appropriate characteristics, unlike purely decentralized public chains, such as Bitcoin and Ethereum. Specifically, KYC/AML, transaction rollback, chain privacy protection, supervising super nodes, and other parameters may be necessary.

6) With capital running into the market, user acquisition costs will be reduced

The development of STO will enable blockchain transactions to be regulated and policy-protected. It is foreseeable that a large number of traditional investors and individual investors will run into the market, greatly reducing user acquisition costs and education costs as a result

7) Great potential for decentralized exchange platform development

Due to compliance restrictions, security tokens can only be traded on regulated licensed exchange platforms, or on various decentralized exchange platforms. The threshold for compliance licenses is relatively high, and decentralized exchange platforms may have a big development opportunity.

8) Need for quality assets to participate

In essence, the STO market is also a capital market. It needs high-quality assets to attract capital participation. Otherwise, it can easily fall into a predicament similar to the OTC market. Quality assets are reluctant to participate because of financing costs, branding challenges, and other risks.

To sum up, we maintain a cautiously optimistic attitude towards STOs. Under the joint promotion of the traditional capital market and the blockchain industry, we expect the new type of token issued under the supervision of major regulatory organizations to inject new vitality into traditional capital markets.

HOW WILL STO CHANGE OUR LIVES?

If the security token market will develop smoothly, it may penetrate and integrate into every aspect of ordinary people's lives in the future. We may live in a world like this:

- British nobility who are no longer as wealthy as they once were will sell their castles to ordinary investors all over the world. Each month, the nobles will distribute the rents from their castles to token holders. Ordinary people can become the landlords of the British aristocracy.
- Due to the increased convenience offered by security tokens, the holder of a resort hotel will automatically receive the shareholder internal coupon and save it in a Dapp on their mobile phone. Every year, the holder of the token has a huge incentive to go to this hotel for a holiday. The hotel vacancy rate is almost zero, so the hotel earns money, and the holder of the token also receives a discount and the dividend of the hotel. Shareholders-consumers and consumers-shareholders have achieved a win-win situation.
- A high net worth individual who invested \$50 million in an equity investment fund for a closed period of 7 years suddenly needs liquidity. Instead of being stuck waiting until the closed period expires, the investor can sell the fund's tokens on licensed exchange and cash out whenever they want.

More and more security token applications will continue to emerge as the market develops, changing all of our lives permanently.

ANNEX 1: COMPARISON OF THE DESIGN OF SECURITY TOKENS

1. Summary

As blockchain and the digital currency market regulations become more stringent, the wild age of ICOs has become a thing of the past, and the issuance of digital currencies is likely to be regulated by securities law. In this context, in order to enable enterprises to provide investors with regulatory products under the blockchain without violating security regulations, the security token offering (STO) solution came into being.

Unlike utility tokens, security tokens indicate partial or full ownership of an asset. A company, real estate, or even intellectual property stock can be represented by a security token. The benefits of a security token not only apply to blockchain financing, but also to the potential of changing the traditional paper stock paradigm in order to improve market efficiency and distribution. For example, many applications of smart contracts can be used with security tokens to optimize voting in corporate governance and increase transparency.

However, without standards, regulators, developers, KYC suppliers, investors, publishers, wallets, and exchange platforms cannot work together in the same framework. At present, there are a variety of attempts to standardize the STO market, including ST-20 of the Polymath team, Harbor's R-Token, and proposals from within the community, such as the ERC1400/ERC1410 and ERC1404 standards.

2. Basic information

Code	Standard name	Author	Stage	Date of creation
ST-20	ST-20 Standard	Polymath team	—	—
R-Token	Regulated Token Standard	Harbor team	—	—
ERC-1404	Simple Restricted Token Standard	Ron Gierlach, James Poole, Mason Borda, Lawson Baker	Draft	2018-07-27
ERC-1400	Security Token Standard	Adam Dossa, Pablo Ruiz, Fabian Vogelsteller, Stephane Gosselin	Draft	2018-09-09

3. Main content and differences of the standards

We cut through the ST-20, R-Token, ERC1404, ERC1400 standard content, combined them with the purpose of business scenario research and design, and then compared the differences between the various standards, considering the difficulties and trade-offs faced in the process of standardization of the security token.

3.1 General nature

Among the standards of the token, the difference between ERC-1400 and the other three is the biggest. Let us first understand the concept of Fungible Token.

3.1.1 Fungible Token and Non-fungible Token

Fungible Token is another name for homogenization token, and can also be called interchangeable token. It is typical for the ESC-20 standard. The token value stays the same for each unit and the token holder can exchange it or split integration. As for the ERC-721 standard token, each unit's token has a different ID, which can have different interpretations. It was designed that each token is different and can not be easily exchanged by unit. This is how Non-Fungible Token (non-homogeneous token/non-interchangeable token) is described.

3.1.2 ERC-1410 standard and tranche

The ERC-1400 standard relies on the ERC-1410 standard, which is designed to divide the balance of a token into different parts through an attribute called tranche. Different interpretations can be made to tranche, and different restrictions are imposed on the operation (for example, some operations are limited to the specified tranche, and some operations preferentially receive the token under the specified tranche). This complies with the concept of a Non-fungible Token, but different concepts may also take place here: Tranche may also have the same token value and can be replaced at will. Combining the attributes of both Fungible Token and Non-fungible Token, it is called a Partially-Fungible Token.

3.1.3 Classification and scene

ST-20, R-Token, and ERC-1404 are all directly dependent on the ERC-20 standard. All three can be considered Fungible Tokens. The ERC-1400 is dependent on the ERC-1410 standard and is therefore a Partially-Fungible Token.

In the actual application scenario, there may be differences between the securities issued by the same company, such as restricted shares/non-restricted shares, preferred shares/ordinary shares, original shares/issued shares, and securities of different natures in

dividends and voting rights. The nature of liquidity is not the same, and its nature may change at a certain stage. The value of securities of different nature may be different in the eyes of investors.

ERC-1404, ST-20, R-Token and other homogenization tokens must reflect the difference in the nature of securities at the contract level. They can only be restricted according to the address and set up a list of various restriction rules (e.g. KYC/AML list, outbound limit list, frozen list, minimum retention, etc.). This design has limitations: a single address cannot hold multiple tokens of a different nature at the same time. If you want to apply to the above complex business at the contract level, you can manage the tokens of different natures through multiple contracts, which will greatly reduce the integrity and increase the complexity of development. Let's take a look at the ERC-1400: the tokens are divided into different tranche within the contract, so that not only the address can be restricted, but there can also be restrictions on tranche, such as allotment, voting, dividends and other complex functions of differential transitions can be achieved by defining tranche at the contract level. The design of the ERC-1400 also makes it more difficult for developers and exchange platforms to access. Therefore, potential issuers should select the appropriate security token standard according to the actual business scenario.

Interface design

Taking into account the securities-related business scenarios, the contract standard of the security token has set the transfer restrictions, such as a requirement for a transfer to undergo a verification before the transfer is executed. It also provides a readable interpretation of the transfer verification results, thereby achieving restrictions, such as lock position, KYC / AML verification, out of the account freeze, and others at the contract level.

3.2.1 Verification function of transfer restrictions

In these security token standards, this function is declared to implement the logic for determining the transfer limit, the Boolean value or the status code of the result is returned. When performing the transfer operation, the verification process needs to be undertaken first, and it is possible to continue execution only if the verification is completed. If case of failure, the corresponding status code is returned, and the transfer is canceled. It allows the caller of the function to know the reason for the transfer failure and report it to the relevant party.

```
/* ST-20 */
```

```
function verifyTransfer(address _from, address _to, uint256 _amount) public view returns  
(bool success);
```

```
/* R-Token */
```

```
function check(address _token, address _spender, address _from, address _to, uint256  
_amount) public returns (uint8);
```

```
/* ERC-1404 */
```

```
function detectTransferRestriction (address from, address to, uint256 value) public view  
returns (uint8);
```

```
/* ERC-1400 */
```

```
function canSend(address _from, address _to, bytes32 _tranche, uint256 _amount, bytes  
_data) external view returns (byte, bytes32, bytes32);
```

Interpretation of the verification result

The status code returned by the verification function of the transfer restriction is readable, and the developer of the relevant application can effectively report the error to the user through the standardized information.

/ In the design of the ST-20 standard, the verification function of the transfer restriction only returns a Boolean value, so the interpretation function for the status code is missing.*

```
/* R-Token */
```

```
function messageForReason(uint8 _reason) public view returns (string);
```

```
/* ERC-1404 */
```

```
function messageForTransferRestriction (uint8 restrictionCode) public view returns (string);
```

/ ERC-1400, the verification function canSend returns an ESC (Ethereum Status Code) that complies with the ERC-1066 standard.*

There is also a bytes32 parameter that can be used to define the program-specific reason code and additional details (for example, the transfer limit for performing the send operation is invalid).

Therefore ERC-1400 also relies on the ERC-1066 standard */

3.2.3 Transfer function

ERC-1404, ST-20, R-Token were developed on the base of ERC-20, so the transfer function is the same as in ERC-20 - transfer and transferFrom. The implementation can be rewritten (add the call to the verification function of the transfer limit) .

Implementation example:

```
/* implement in the instance of R-Token */
```

```
function transfer(address _to, uint256 _value) public returns (bool) {  
    if (_check(msg.sender, _to, _value)) {  
        return super.transfer(_to, _value);  
    } else {  
        return false;  
    }  
}
```

```
function transferFrom(address _from, address _to, uint256 _value) public returns (bool) {  
    if (_check(_from, _to, _value)) {  
        return super.transferFrom(_from, _to, _value);  
    } else {  
        return false;  
    }  
}
```

```
/* implement in the instance of ERC-1404 */
```

```
modifier notRestricted (address from, address to, uint256 value) {  
    uint8 restrictionCode = detectTransferRestriction(from, to, value);
```

```

        require(restrictionCode == SUCCESS_CODE,
messageForTransferRestriction(restrictionCode));
    _;
}

```

function transfer (address to, uint256 value)

public

notRestricted(msg.sender, to, value)

returns (bool success)

```

{
    success = super.transfer(to, value);
}

```

function transferFrom (address from, address to, uint256 value)

public

notRestricted(from, to, value)

returns (bool success)

```

{
    success = super.transferFrom(from, to, value);
}

```

As for the ERC-1400, because of the existence of tranche, not only the transfer, but also the interface design of the entire contract changes. Here only the function definition corresponding to transfer is sampled:

// Defined in the ERC-1410 standard

```

function sendByTranche(bytes32 _tranche, address _to, uint256 _amount, bytes _data)
external returns (bytes32);

```

```

function sendByTranches(bytes32[] _tranches, address[] _tos, uint256[] _amounts, bytes
_data) external returns (bytes32[]);

```

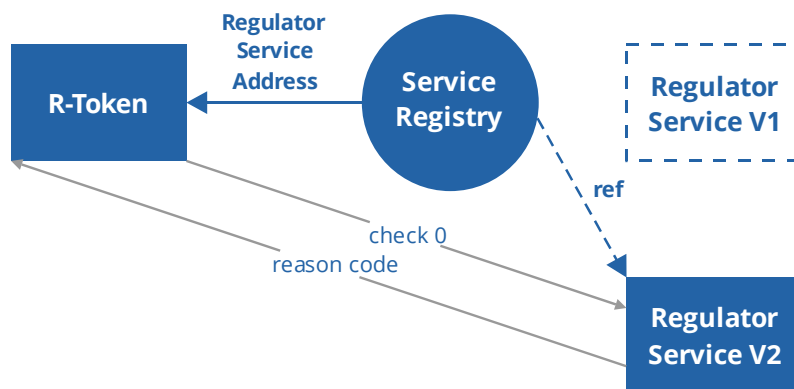

3.3 Compatibility

Because the ERC-20 standard is the most common in the industry, here we mainly consider the backward compatibility of ESEC-20 with each security token standard.

ERC-1404, ST-20, and R-Token are similar to ERC-20 in terms of the interface design. The contract itself must rewrite the transfer and transferFrom functions of the ERC-20 standard. It can be said that it is fully backward compatible with ERC-20. The ERC-1400 will be more troublesome. The ERC-1400 inherits much from the ERC-777 standard. The defined transfer function is not the transfer and transferFrom in the ERC-20 standard. If you want to be backward compatible with ERC-20, you must implement the ERC-20 standard. The functions that are present, and the state change functions from the two standards are best decoupled in implementation and operate independently of each other. In addition, the corresponding event also needs to be changed. Compatibility with ERC-20 standards enables issuers to quickly access applications such as exchanges and wallets.

3.4 Other differences

ERC-1404, ST-20, and R-Token are basically the same in design. The only obvious difference is that R-Token puts the verification function of the transfer restriction and the interpretation function of the verification result in the Regulator Service contract, which is convenient for upgrading the version, using the Service Registry contract as the registrar to save the current version of the Regulator Service address. The subject-contract R-token first needs to access the Registrar Service Registry to get the Regulator Service address, and then call the transfer function of the latest version of the Regulator Service. The whole process is shown below:



In addition to the introduction of tranche, ERC-1400 is significantly different from the other three standards in terms of interface design. Because of its design, it advocates support for securities-related business at the contract level. For example, ERC-1400 considers the circulation of actual securities, which requires much more complex interactions between participants on the chain and outside the chain, so the standard must have the ability to make mandatory transfers for legal proceedings, capital recovery, and so on.

Conclusion

Among the four security token standards mentioned in the article, ST-20 and R-Token are designed by Polymath and Harbor respectively, mainly relying on their own promotion. In the case of creation of additional successful security tokens, they are bound to be recognized by the community. ERC-1404 and ERC-1400 by EIP widely adopt community opinions and jointly develop standards, but are currently only in the draft stage. A process from drafting a proposal to entering the last call phase usually requires long development, editing, implementation, and bug fix cycles. These drafts may be just the beginning of the road of securities tokenization. With the participation of all parties in the industry, more standards must be developed.

REFERENCES:

1. <http://onchain.caijing.com.cn/20180718/4488131.shtml>
2. <https://www.security通行证academy.com/info/three-waves-of-a-new-financial-internet-1745/?gclid=CjwKCAjwzenbBRB3EiwAltS->
3. <https://www.security通行证academy.com/info/three-waves-of-a-new-financial-internet-1745/?gclid=CjwKCAjwzenbBRB3EiwAltS->
4. <https://medium.com/@argongroup/8-important-things-to-know-about-security-通行证s-通行证-regulation-3d548a1a6367>
5. <https://medium.com/@argongroup/8-important-things-to-know-about-security-通行证s-通行证-regulation-3d548a1a6367>
6. <https://medium.com/@argongroup/8-important-things-to-know-about-security-通行证s-通行证-regulation-3d548a1a6367>
7. <http://onchain.caijing.com.cn/20180718/4488131.shtml>
8. <https://medium.com/@tatianakoffman/your-official-guide-to-the-security-通行证-ecosystem-61a805673db7>
9. https://www.ecfr.gov/cgi-bin/text-idx?SID=254a68b3c032af7e1fbc9009ef46b7b&mc=true&node=pt17.3.230&rgn=div5#se17.3.230_1903
10. <https://www.sec.gov/fast-answers/answers-rule506htm.html>
11. <https://www.sec.gov/rules/final/33-7505.htm>