TACXE: a Blockchain Based Token Listing and Exchange Platform

Sam Colak[1] and Martijn Hoogeveen[2]

version November 7, 2017

TACXE - phonetic: tæksi, US phonetic: tak-see

Abstract

There is a need for a distributed exchange platform for crypto coins or tokens that satisfies the requirements of a formalizing regulatory environment, and the technical needs for a very secure and high-speed high-volume transactional platform. TACXE (**T**oken **a**nd **C**oin E**x**chang**e**) is designed to meet these needs and requirements, and is being developed as a mechanism to enable Initial Coin Offering (ICO) tokens to be issued, listed, purchased and sold. Although TACXE has initially a centralized character, it's protocols enable a decentralized set-up. The distributed service, which is using the operational Ledgable blockchain cloud infrastructure, also enables businesses to offer "spending" processes though their own websites utilizing the TACXE infrastructure. Effectively offering businesses a way to translate ICO into pre-pay or pre-purchase of services. The use case of the TACXE coin is related to costs and benefits of running an exchange platform. At its launch it's envisioned that TACXE will be used for tokens that are designed as commodities or utility tokens, not as financial instruments or securities in their respective countries.

1. Introduction

The ICO (Intitial Coin Offering) market has been heating up this year, with the largest ICO in 2017 being the current pinnacle at USD 232 million[I]. By some it's optimistically embraced as a boom that will change forever the landscape of IPOs and crowdfunding[II]. By others it's described as a mania or craze resembling the infamous tulip bubble, that will inevitably burst[III]. Especially, blockchain start-ups have embraced ICOs as a vehicle to raise early capital[IV], whereby some tokens are similar to currencies, some resemble securities, and others are similar to commodities or still something else.
Whatever it is, it's certainly a market phenomenon that is taken more seriously by the business community and regulators alike, and which cries for more professional business practices and exchange platforms to screen potentials ICOs, guide the ICO and listing process and facilitate the trade of the longtail of cryptocurrencies or tokens.

Currently, there are sufficient ICO watchlists like icoalert.com, and there are plenty of exchanges like Bitstamp, Coinbase, Bittrex, Kraken, and Poloniex, for the most popular cryptocurrencies such as bitcoin, ether, litecoin and a limited number of altcoins. Interesting are additionally the developments in the direction of decentralized,

[1] Sam Colak: https://www.linkedin.com/in/samcolak/

[2] Martijn Hoogeveen PhD: https://www.linkedin.com/in/martijnjurjenhoogeveen/

blockchain based exchanges such as the Waves platform[V], especially if their censorship-resistant[VI]. Nevertheless, there are currently no professional ICO exchange platforms that fully support the whole ICO cycle – issuing, launch, listing, trade – and at the same time fully satisfy the regulatory conditions for trading securities, let alone the listing process itself.

The ability to raise funds for ICO tokens relies on two main factors:

1) The *reach* under prospective investors in ICOs
2) Making the *value proposition* clear to these investors (Conley, 2017)

An ICO can be seen as a kind of crowdfunding. Regarding crowdfunding success, research identified sub-factors (of 2) that positively contribute, such as founder identify disclosure and founder track record, elaborative project disclosures, and campaign duration[VII]. In the same research a negative relation was found between the aspired funding amount and successful crowdfunding. In other words: setting the threshold amount relatively too high makes potential investors wary. Further, investors appear to focus on market and agency risks in screening potential investments in equity crowdfunding, and the use of video narratives by entrepreneurs seems to be positively correlated with equity crowdfunding success[VIII].

A successful token listing and exchange platform, will be instrumental in providing reach, the more investors are active on its platform. Further, mature exchanges have screening responsibilities to filter out unclear or bad propositions, to protect the interests of (retail) investors. Nevertheless, the ICO-ing organization is primarily responsible for reach and explaining its value proposition to its prospective investors. Many of today's ICOs are currently only performed by startups, individuals or teams without much organization. As the market is getting mature, and regulators like SEC step in[IX], it can be foreseen that ICOs will increasingly be done by entities with a proven track record, and more possibilities to back the token, like the estcoin is foreseen to be backed by the Estonian government[X].

2. Description of the TACXE platform

The development of TACXE is orientated to providing a safe and secure blockchain-based platform for businesses to raise capital and at the same time facilitate investors in trading the tokens relating to the businesses presented. TACXE also provides the distributed service infrastructure to businesses to enable trade-in of the tokens in lieu of service, which may then be resold to new investors on the platform.

High-speed, high-volume Ledgable Blockchain

In 2016, the high-speed high-volume blockchain service layer of TACXE, Ledgable, entered operation in April 2017[XI]. It is created by the same team as TACXE as an independent Blockchain-As-A-Service or Blockchain Cloud service provider, with a US based payment facilitator as launching customer and Series A funding[XII].
The Ledgable blockchain is already well-tested by the market: experiencing thousands of attempts per day to penetrate the security services, Ledgable features a Machine Learning Security Engine (MLSE) to safe-guard its operation.

In contrast to many existing Bitcoin or Ether-based blockchain forks, Ledgable is a distributed blockchain infrastructure which is capable of high-speed high-volume transaction processing, a critical requirement in case of settlement of financial transactions. Common financial market requirements are mostly up to 1 million tps per application. Not only important for payments, but also essential for any exchange of securities or commodities. During lab tests, Ledgable was able to process 1.4 million transactions per second (tps), compared to 1000 tps as claimed by Ripple, which is also aiming for the financial transactions market[XIII]. The theoretical speed of Ledgable is 3 million tps, which the team would like to aim for in next versions of Ledgable.

Ledgable can support applications with various transaction validation policies, whether Proof Of Work[XIV], Proof Of Stake[XV] or Private with a single Trusted Third Party (TTP) as stakeholder. In other words, Ledgable can be flexibly used by public, private, or consortium blockchain applications[XVI]. An entry into the Ledgable blockchain is performed via an authority, usually an application developed by a third party, where all control regarding the right to write is governed. The design of this application determines the degree of decentralization, and the degree of censorship-resistance. Hence, Ledgable itself does not suffer from the inherent synchronization issue that plagues the transaction performance of public blockchain solutions.

TACXE: an app on the Ledgable Blockchain

TACXE is an application that sits on top of the Ledgable blockchain protocol or platform. TACXE provides a secure infrastructure for businesses to enable trading of tokens - issued via internal ICOs or hosted upon the platform - to other individuals or businesses. Although the TACXE platform at its launch is geared towards the unregulated commodities trading, as much as possible provisions for legal requirements and other safe-guards are made as if the platform has to fulfill requirements for a regulated market (facility):

1. Traded tokens are only permitted when they are classified as commodity under Dutch and/or EU regulations, and are to be traded into recognized currency denominations[XVII]. In case that a platform operator wants to facilitate the trade of tokens that can be classified as equities, bonds or other financial instruments, obtaining the appropriate license(s) is required.

2. No trading through, whereby a token is not exchanged at the best possible price according to quote prices, may occur.

3. All traders and token issuers are subject to standardized KYC (Know Your Customer), and when required AML (anti-money laundering) and anti-terrorism processes, to anticipate potential legal requirements, especially in case of trading tokens that are seen as securities and/or as currencies. Traders will be categorized as retail, professional or eligible counterparts.

4. Trading occurs via a manual purchase process in the sense that no automated or high-frequency trading is supported by the platform operator. In case that in the future 3rd party investment firms attach their automated trading systems to TACXE, these parties might be subject to licensing under security acts and regulations[XVIII].

5. In so far that trading of tokens as securities is facilitated, a TACXE platform operator is likely to be required to obtain a MTF or other license as required by MIFID-II[XIX], US SEC acts and regulations[XX], or other regulatory frameworks.

6. Pre- and post-trade transparency, publishing aggregated market data, reasonable offers for disaggregated market data, and meeting potential reporting requirements, f.e., regarding insider trading or preventing market abuse.

To achieve a secure infrastructure, TACXE relies upon a number of key technologies in order to be able to operate in accordance with current and anticipated legislation and regulatory requirements. Even though, in its initial phase the TACXE platform will be used for commodities-like tokens only.

Online Certificate Status Protocol (OCSP)

One significant aspect of the cryptocurrency "bubble" is the lack of trust in soft wallets and other services, and the inherent volatility in secure services sufficient to guarantee delivery of funds. To do this, a Trusted Third Party TTP) must be employed, agreed as a mutually trusted party by both trading entities to facilitate the transaction. Such a TTP might provide an escrow service, holding funds in reserve till all (delivery) conditions of a transaction are met. Why not use one of the most widespread protocols, OCSP[XXI], to facilitate such an escrow process?

Today, the advantage of the OCSP protocol is that it is supported in all operating systems, browsers and platforms supported. Additionally, the protocol, established in 1998 and finalized in RFC2560 in 1999, is a cornerstone achievement within the ecommerce ecosystem.

As a Certificate Authority, TACXE is able to utilize the OCSP protocol to assist in validating expired or used wrapped tokens without extensive effort or the development of additional proprietary protocols. To completely avoid the known vulnerabilities in certain TLS/SSL applications[XXII], TACXE limits the use just to the wrapping of tokens.

An additional advantage of using a genuine SSL certificate, issued by a sub-authority, is that the value of the transaction is insured by the certifying authority, depending upon issuance and the policy conditions, to a maximum of, typically, 10,000 to 1,750,000 USD (for low to high-assurance certificates).

How does the OCSP application work in the platform? TACXE operates as a sub-granting certificate party in a true certificate chain trusted by Comodo or VeriSign, that issues, validates and revokes SSL certificates provided to third parties representing secure tokens in transit. When a transaction is initiated, there is a finite period whereby the transaction must be fore-filled. Failure to meet this deadline must result in the termination of the transfer. Alternatively, the funds are released at the end of the transit period.

SSL certificates enable the wrapping of private data and the ability to express a validity period (start/end) for a specific need. The OCSP protocol checks with a representative authority regarding revocation as to whether a certificate has been expired in a manual fashion, due to usage or cancellation. The inherent token, the private data, in effect has no value other than to establish trust and mutual agreement in the transfer of funds. Should the expiry of the certificate occur, it must be reissued. Attempts to use the certificate, outside this TACXE context, will simply fail.

Governing Authority

TACXE operates as an authority enabling users to create a digital wallet containing currency amongst other "tokens". It's foreseen that the protocols that form this authority are gradually decentralized to increase censorship resistance.

Since a currency is simply a token of denomination, this is in reality no different to an ICO token. As a result, no ability will exist to name tokens after established recognized denominations (such as USD, EUR, GBP etc).

The trading of ICO tokens may only be with established denominations (or denom). Not denom to denom. Additionally ICO to ICO is forbidden. Trading via a denom (ICO -> denom -> ICO) is permitted although requires 2 transactions to complete.

All token transactions are recorded within a blockchain hosted upon the Ledgable platform. All transactions are identified using a secure identifier representing the depositing party and recipient. This token conforms to KYC guidelines.

The KYC token is generated using the following format. The structure is then "hashed" using an MD5 algorithm to form a unique id representing the party. MD5 is only used to create a unique token based upon the content it represents, not to secure (privacy sensitive) data.

For persons (individuals)
[Country Code][Place of Birth][Date of Birth Rev][Firstname][Lastname]

Example
gbrnewcastle19781103joebloggs = ‘fb2b3fb500312906e6df93fdc41a239f’

For business entities
[Country Code][Place of Incorporation][Date of Incorporation][Company Name]

Example
nlamsterdam20170421ledgablebv = ‘00aa83fda589f4abb9261083d14a59ab’

NB. All characters are ANSI coded and lowercase – spaces are by default removed.

The KYC token, specific to an entity requires no exposure of the private data to the end users.

To enable recovery, a password or sequence (no less than 12 characters) is used to form a recovery key. This password or sequence itself is hashed to create a 34-character sequence.

IN	kyc		fb2b3fb500312906e6df93fdc41a239f
	rec-seq		1234567890123456789012345678901
OUT	rckey	MD5(kyc:rec-seq)	6f65064228e619a046d8a1d0b383af82

In the event of loss of password or requirement to revalidate the identity, the recovery sequence is required to perform a reset.

Additional note. To meet anticipated legal and law-enforcement procedures, all requests for information regarding current ownership of tokens etc. would require the KYC to be confirmed prior to issuing information. Simply requesting information on “Joe Bloggs” would not be sufficient.

Authentication Process

All authenticated processes utilize a 5 factor NONCE, an arbitrary number that is only used once. This process is structured using the following procedure:

IN (Server)	S1	SESSION-ID	1122334455667788990011223344556677
	A1	AUTH-TOKEN	1111111111111111111111111111111111
IN (Client)	D1	DEVICE-ID	7766554433221100998877665544332211
	K1	KYC-TOKEN	0cf979cbc9f7484686c632d71e60dffe
	P1	MD5(PASSWORD)	af24d1e239441fb0fe6a08a2ecb065b5
	N1	MD5(S1:K1:A1)	7dc2b4716ee4215dc896d5bd19c95ab2
	N2	MD5(P1:D1:A1)	29bc49f6898a22a3380676723fc5bbf0

OUT	O1	MD5(REV(N1):N2:S1)	78099f95112d531280be0923bf12b1d3

During the "EHLO" process, "D1" is presented to authorize and being the negotiation process. The token at "O1" is presented with "K1" to authenticate. Note that the "P1" token is stored server side and never transmitted. All communications are performed across a TLS over SSL secure connection.

From the server side, the system is aware of D1 (during the authentication process), K1 and P1 (stored locally). Consequently, the capability to generate the token and then verify against the presented token (from the client) is sufficient to indicate an authenticated user. Failure to authenticate, results in a new session-id and a new auth-token to avoid spoofing.

Should a token be misrepresented, the device-id is listed in a black-list after five failed attempts. An email is also directed to the owning party to inform them of failed attempts to access the service. In the email, a link is provided to white-list the device should the password sequence was invalid or a requirement to change / lost password. Unless white-listed, the device cannot re-authenticate with the service regardless of password validity.

This process is also used to secure payment terminal services from operating businesses providing transactional capabilities to end clients.

Token Transfer Process

All transactions consist of the following process.

For sale of a token.

1. Wrap token in SSL wrapper indicating life-time of sale process (default 2 hours)
    a. Perform wrapping process

       The real token is obscured by creating a "representative" token for the duration of the transaction.

IN	tok		11111111111111111111111111111111
	kyc		22222222222222222222222222222222
	value		20.0
OUT	trkey	MD5(tok:kyc:value)	643090cfb2be0d277d5001ce8fd7b551

This token '643090cfb2be0d277d5001ce8fd7b551' is placed in the private-data field of the SSL certificate and recorded within the ledger.

2. Using a similar process, a payment token is created and then passed to recipient (public key only)
    a. Price token private key is held by platform

3. Seller accepts price-token (confirmed by email or notification service)
    a. Sale token is unwrapped (using authorized key) and transferred to recipient
    b. Price token is unwrapped and transferred to seller

4. Process completed

Should the process be delayed for any reason, the relevant transfers fail if one or both of the expiry of the certificates occurs.

A charge (transaction charge) is levied against the purchaser in local currency (let’s say 10¢ or ten cents EUR) and given to the governing authority to assure against misuse and to provide sufficient funding to maintain the network.

For trading purposes, the token is shown on the exchange (for sale) directly linked to the quantity and token to which it represents. Clients may purchase the token at will, performing the above process (part 2 onwards).

For payment in lieu of services rendered, the payment token is effectively replaced by a digital receipt. When such transaction occurs, the transaction charge is waived.

Token Issuing Platform

TACXE enables businesses to acquire funding. This funding mechanism may be used to realize additional capital in lieu of services, such as prepay. The coin or token created should represent a value of denomination in terms of service or supply of service that may be redeemed by the participating members of the platform.

To enable this facility, TACXE establishes a process similar to the issuance of a new domain TLD (top level domain).

For a period of not exceeding a month, a company is granted the exclusive ability to sell tokens within the platform to KYC approved purchasers for denominated currency at fixed value. This period is termed as the “Sunrise”. At the end of the “Sunrise”, the amount raised is transferred to the established monetary institution minus a small fee.

Following this period, trading of the currency may be performed by members holding the token to others for denomination. These trades may be restricted by geographic boundaries, for instance country or trade zone.

All trades are recorded, as mentioned earlier, within the blockchain hosted within Ledgable. And all trades are subject to the transaction fee payable by the purchaser.

With all transactions, the previous traded value, the price previously paid, is recorded.

To calculate the impact upon the traded value of the token, the following formula is used.

Change in value = New Price – Old Price

New Trade Price = (Volume * “Change in value”) / Total Number of Tokens

Inter-day trading prices are recorded as the mean over the period. Since the exchange is possibly 24-hour available, the inter-day trade-price is calculated at 00:00 GMT.

Use Case TACXE Tokens

As the number of transactions increase, the value of the exchange increases since all purchases result in a transaction charge, which can be paid with TACXE token. This is the basic use case of the TACXE token. Further, what are other typical exchange fees that might be applicable to TACXE, that can be paid in TACXE tokens?

- a small fee (%) of the total sum raised
- a one-off listing charge for already issued ICO tokens
- annual listing fee per ICO issuer to maintain the listing
- small cash repatriation fee (%)

It's foreseen that TACXE tokens can be rewarded to 3rd party exchanges or other third parties that deliver transactions to TACXE, and represent a reasonable share in the transaction charge.

Blockchain Process per Listing

Each listing has its own blockchain.

To provide an insight in how transactions take place, whenever a token is issued, its value and ownership is added to the exchange under a ledger specific to the listing.

Token-id	Parent-Token-Id	KYC Token	Epoch	Value
1111111111111111111111111111111111	-	0cf979cbc9f7484686c632d71e60dffe	1506512546	20.0

When a token is used, transferred or deleted, the token is first cancelled (i.e. a new entry is added negating the value). The sum is then effectively zero.

Token-id	Parent-Token-Id	KYC Token	Epoch	Value
1111111111111111111111111111111111	-	0cf979cbc9f7484686c632d71e60dffe	1506512546	20.0
1111111111111111111111111111111111	-	0cf979cbc9f7484686c632d71e60dffe	1506512637	-20.0

Following this, a new token is created (if transferred) or 2 tokens (in the event of a "split"), the total value representing the original value but reflecting different owners.

Table 1-Transfer of Token

Token-id	Parent-Token-Id	KYC Token	Epoch	Value
1111111111111111111111111111111111	-	0cf979cbc9f7484686c632d71e60dffe	1506512546	20.0
1111111111111111111111111111111111	-	0cf979cbc9f7484686c632d71e60dffe	1506512637	-20.0
1122334455667788990011223344556677	1111111111111111111111111111111111	987654321098765432109876543210	1506512900	20.0

The two new tokens (or one token in the event of transfer) have different token-ids. The parent-id (ie where the token came from) is recorded in both tokens.

Table 2-Token is "Split" into 2

Token-id	Parent-Token-Id	KYC Token	Epoch	Value
1111111111111111111111111111111111	-	0cf979cbc9f7484686c632d71e60dffe	1506512546	20.0
1111111111111111111111111111111111	-	0cf979cbc9f7484686c632d71e60dffe	1506512637	-20.0
1122334455667788990011223344556677	1111111111111111111111111111111111	987654321098765432109876543210	1506512900	10.0
7863428654358309543967846538754634	1111111111111111111111111111111111	0cf979cbc9f7484686c632d71e60dffe	1506512900	10.0

For a token originating from an external exchange, the parent-id is the original token as passed into the exchange at ingress.

Token-id	Parent-Token-Id	KYC Token	Epoch	Value
1111111111111111111111111111111111	Hier78r823i4234049f23424u32ioufwe==	0cf979cbc9f7484686c632d71e60dffe	1506512546	20.0

Since the original token cannot be "found" in the ledger, it is assumed to have originated from a parent service (such as an external ICO).

Note that the blockchain overview is simplified to illustrate the above transaction record examples.

Ingress of External ICO Tokens after external ICOs

All businesses requesting to list upon the exchange would require each token to be re-issued to a specific individual or entity. During the ingress process each individual (via email) would be required to undertake KYC clearance OR the original issuing entity themselves asserts that the KYC process has been performed to a minimum standard such that the process (shown earlier) is satisfied.

Each token owner would be contacted automatically to "set-up" an account within the exchange to enable them to trade the tokens appropriately.

This setup process includes:

1. Setup of account username and password (linked to the token)
    a. Validating KYC data recorded by the external entity

2. Setup of a recovery key to recover token in the event of loss password etc.

When validated, the ownership would be entered into the secure ledger (blockchain).

In the event that ownership is not ascertained or that the owners fail to confirm ownership, these are flagged to the business for internal processes to follow up and resolve. These tokens however remain in an inactive state.

Service Delivery

TACXE is an application framework that exposes a number of interfaces.

1) Web Service

    The front-end services use the same technology on which Ledgable is built. The core services have shown significant resilience to a number of "bad-actors".

2) API & Pipeline

    All API accessible functionality is such that extension of the service by authorized third parties is permitted. In doing so, they agree to the terms and conditions of usage.

    This enables other exchanges or businesses to remotely access the TACXE services through their own service portfolio.

3) Security Services

    TACXE ties into Ledgable's MLSE Security Framework to ensure permitted transactions by authorized parties. MLSE determines if an attempt to breach the network is in progress. Since MLSE and the Ledgable services run independently, both services are responsible for the security context and monitoring processes.

4. Conclusion

There are many cryptocurrency exchanges online, but there are little exchanges that facilitate an ICO, especially in a formalizing regulatory environment.

The main technical functionalities of the blockchain-based token and coin exchange, TACXE, are described in this paper. The TACXE application is currently developed on top of the operational Ledgable blockchain cloud infrastructure, which has proven itself as a high-speed high-volume blockchain infrastructure. For the TACXE tokens, and each token that is issued and/or listed on the exchange, a separate blockchain is defined and setup in Ledgable.

The TACXE platform, takes into account the KYC and other legal compliance factors, although at the launch of the platform, it will be focused on utility-type tokens that are more like commodities under Dutch law, not securities and other financial instruments. In case that financial instruments are traded, under Dutch (or European) law, the operator of the platform will be required to make use of the appropriate (sub-)licenses.

The use of SSL certificates for (temporary) tokens on the TACXE platform is described, and the potential for escrow services. Further, the use cases of the TACXE token for paying transactions and sharing transaction fees with third party agents is described.

Finally, the typical processes for exchanges, and how these are defined in a distributed blockchain are defined, such as token issuance, listing, transfer, the governing authority, authorization protocols and the APIs through which TACXE services can be called by third party applications. It’s foreseen that the TACXE protocols will support decentralized processes to create a censorship resistant exchange setup.

References

[I] Omri Barsilay (July 15, 2017). Tezos' $232 Million ICO May Just Be The Beginning. See https://www.forbes.com/sites/omribarzilay/2017/07/15/tezos-232-million-ico-may-just-be-the-beginning/#61c2263f4c52

[II] Dan Murphy, Sept 20, 2017: The US IPO market is dead, but ICOs are the future, says entrepreneur. https://www.cnbc.com/2017/09/20/the-us-ipo-market-is-dead-but-icos-are-the-future-says-entrepreneur.html

[III] Economist (2017, October 7): Manias, panics and Initial Coin Offerings. Crypto-coin mania illustrates the crazy and not-so-crazy sides of bubbles. See https://www.economist.com/news/finance-and-economics/21729995-crypto-coin-mania-illustrates-crazy-and-not-so-crazy-sides-bubbles-manias

[IV] Conley, J.P. (2017). Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings. Vanderbilt University Department of Economics Working Papers 17-00008.

[V] Ivanov, S. Waves Whitepaper. Wavesplatform.com

[VI] Warren, W. & Bandeali (2017), A. 0x: An open protocol for decentralized exchange on the Ethereum blockchain. https://www.0xproject.com/pdfs/0x_white_paper.pdf

[VII] Kim, T., Por M.H. & Yang, S.B. (2017): Winning the crowd in online fundraising platforms: The roles of founder and project features. In: Electronic Commerce Research and Applications, vol 25, p 86-94, Elsevier.

[VIII] Mamonov, S. & Malaga, R. (2017). Success Factors in Equity Crowdfunding in the United States. AMCIS 2017.

[IX] SEC (2017). SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities. https://www.sec.gov/news/press-release/2017-131. And the SEC report itself: https://www.sec.gov/litigation/investreport/34-81207.pdf

[X] Browne, R. (2017). Estonia wants to launch its own government-backed cryptocurrency called 'estcoin'. CNBC. https://www.cnbc.com/2017/08/23/estonia-cryptocurrency-called-estcoin.html

[XI] See http://www.Ledgable.com/

[XII] iMerge investeert in blockchainstart-up Ledgable. https://www.emerce.nl/nieuws/imerge-investeert-blockchainstartup-ledgable

[XIII] Ripple Consensus Ledger Can Sustain 1000 Transactions per Second. https://ripple.com/dev-blog/ripple-consensus-ledger-can-sustain-1000-transactions-per-second/

[XIV] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.

[XV] Proof Of Stake https://en.wikipedia.org/wiki/Proof-of-stake

[XVI] Buterin, V. (2015): On Public and Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[XVII] https://en.wikipedia.org/wiki/List_of_circulating_currencies

[XVIII] AFM Report Trading in control. Compliance with the ESMA Guidelines on automated trading:
the expectations of the AFM. https://www.afm.nl/en/nieuws/2015/mei/rapport-beheerste-handel

[XIX] Markets in Financial Instruments (MiFID II) - Directive 2014/65/EU. https://ec.europa.eu/info/law/markets-financial-instruments-mifid-ii-directive-2014-65-eu_en

[XX] Rules and Regulations for the Securities and Exchange Commission and Major Securities Laws. https://www.sec.gov/about/laws/secrulesregs.htm

[XXI] Online Certificate Status Protol: https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

[XXII] TLS (SSL) https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS