Blockchains and Digital Assets

Luis-Daniel Ibáñez
Michał R. Hoffman
Taufiq Choudhry

University of Southampton

1. Introduction

Transacting and exchanging assets is a crucial part of the human development. From the simple bartering of potatoes for carrots in ancient societies, to today's complex stock operations, a key component of our functioning as social beings revolves around the concept of exchanging the product of our effort for the product of the effort of our neighbour in a way that satisfies the needs of both. Unfortunately, because of our own human condition, not all our neighbours will give us all the carrots agreed for our potato sack, *i.e.*, every transaction has the inherent risk that any of the parties will not abide to the terms of the agreement. To quantify this risk, humans developed the concept of *trust*. If we trust our neighbour, we have a firm belief that he/she will not break the terms of our agreement and therefore, we will go ahead with the transaction. However, as the world became more and more interconnected and globalised, we transact much more and with many more people and organisations, making difficult to develop trust with every and each of them.

To solve this dilemma, humans resorted to externalise the management of the transaction process to a third party o*r intermediary* trusted by all transacting parties. This reduces the problem of having to quantify the trust we have in any potential party for a transaction into quantify the trust we have on an intermediary to guarantee that the transaction will take place according to the expectations. In some scenarios, we may even strongly suspect that the other party will breach the contract, but we still need to do a transaction with it. The reliance on a trusted third party enables a transaction that otherwise would not have gone ahead. Unfortunately, this reliance comes with some trade-offs. First, if the intermediary is "offline", no transactions can be performed (think about what happens when Visa or Mastercard are down). Second, intermediaries are not immune to the temptation of breaching trust for their own benefit, for example, favouring one party over the other, or taking advantage of its privileged position to increase fees and to restrict access. Or, as Casey and Vigna[1] argue, intermediaries morph into *gatekeepers*, becoming more of a problem than a solution.

It was not until very recently that *blockchains* and *Distributed Ledger Technologies* entered the scene with the promise of decentralising the management and execution of transactions. With blockchains, it became possible to encode validation rules for transactions and enforce them without an intermediary. Instead, Blockchain protocols enable transparent transaction validation by all the members of the community that transact an asset, or, if required, to externalise it to a pool of validating parties (not

[1] https://www.technologyreview.com/s/610781/in-bloc

necessarily interested in the asset transaction itself, but in providing the service for a fee) in such a way that the cost for one of them to seize control is prohibitively expensive, and a tremendous amount of coordination is needed for a coalition of malicious parties to take over.

The first use case of Blockchains was the implementation of decentralised digital currencies (*aka* cryptocurrencies, most notably Bitcoin), designed to reduce the dependency on banks and credit card companies to execute everyday transactions. However, since this initial breakthrough, the concept was generalised to accommodate many different use cases, leveraging the power of Smart Contract platforms to code and deploy the definition of how a transaction should work, and leave validation to the underlying blockchain protocol. Tokens go also beyond the concept of transaction of physical assets and can be used to track other social concepts like reputation.

In this academic paper we will review how Blockchains are being used to support the exchange of Digital Assets. From a technological perspective, we introduce the abstract concept of "Tokens", on which, and discuss the most common ones. From an economics perspective, we will review the use of tokens as a fundraising strategy for start-ups, and therefore, as a way for investors of any size to invest in them, in a mechanism known as Initial Coin Offerings (ICOs).

2. Transactions and Tokens

A *digital asset* is anything that can be stored and transmitted electronically (using a computer) that can be owned and thus, can have ownership and usage rights associated with it. Due to the diversity and variability of digital assets, ranging from audio files to email accounts, the scope of our report only relates to digital assets that can be tokenized using a cryptographic protocol, or so-called *crypto assets.* Therefore, in this paper, we may use the terms *digital assets* and *crypto assets* interchangeably. Generally speaking, a crypto asset is a digital asset that can be represented by a particular quantity of cryptographic *tokens* that someone holds of that asset. These tokens can be transferred between pseudonymous *accounts* on a blockchain, and are often held in *crypto wallets.*

The problem of supporting transactions of digital assets can be reduced to the problem of tracking which account is the owner of a particular asset at a given point in time, and to register when the ownership of an asset changes. With these basic operations, one can compute how many assets a person or organisation has and avoid double-spending and false claim attacks. The pattern is the same independently of the type of asset, whether it represents the ownership of a real-world object, or a more ethereal value like reputation or credit. The difference among them is what are the rules and conditions to transact them. As such, digital assets and their transaction rules in the context of blockchains are defined during *token modelling (*also known as *token design, or "tokenomics")*. A *token definition* establishes the digital asset being exchanged, the admissible operations that can be executed (and therefore, need to be validated) on it, and often implicitly, the rights associated with holding it. Thus, programmable tokens allow issuers and investors alike to adapt to the changing rules in ever-evolving markets. It has to be noted at this point that whilst certain abstractions could be modelled as crypto tokens, it is not always a sensible thing to do so, one important example being digital identity - it should not be possible to trade digital identities, hence, they do not constitute digital assets.

To introduce more order into the discussion of which digital assets can be viably represented as tokens, Euler et al.[2] propose a classification framework comprised of the following categories:

Technical layer: Where the token is implemented, at a blockchain system protocol level (*native tokens*), as a protocol on top of an existing blockchain protocol or defined at the application level of an app deployed on the blockchain. Native tokens model an asset fundamental for the functioning of the blockchain, e.g., to reward transaction validators. For example, Ethereum's Ether is a token used to pay for the execution of a Smart Contract in the Ethereum network. In the Bitcoin network, the eponymous token is also used to reward transaction validators. Application Tokens are tokens whose transaction rules are designed as a Smart Contract and are then deployed on top of a Smart Contract platform (e.g., Ethereum, or HyperLedger). According to the EtherScan website[3], as per April 2019 more than 180 thousand Smart Contracts representing Application tokens were deployed on top of the Ethereum platform.

Purpose: The main purpose of the token. Cryptocurrency (I.e., global medium of exchange), Network tokens (primarily intended to be used in a specific system), and investment tokens (primarily intended as a way to passively invest in the issuing entity or an underlying asset)

Value: How does the token derive the value that it represents? Asset-backed tokens (represent ownership or claim on an underlying possibly physical asset). Network-value tokens (tied to the value and development of a network), and share-like tokens (similar to shares in companies, usually these tokens are also investment tokens)

Utility: What token holders can do with it. Usage tokens (provide access to something, like an API key), work tokens (provide the right to contribute to a system), and Hybrid tokens (work and usage traits)

Legal status: Depending on the jurisdiction, the legal status of the token assigned by regulators. This category is subdivided in Utility tokens (tokens offering owners a clear utility), Security tokens (tokens that are considered securities in the financial sense of the word[4]), and cryptocurrencies.

We add to this classification the concept of **fungibility.** A token is fungible if its individual units are essentially interchangeable, and each of its parts is indistinguishable from another part. A non-fungible token represents a unique entity (or ownership of a unique physical world item), their main goal is to create verifiable digital scarcity. In the next section we will review the most common ERCs according to the fungibility category.

The community around Ethereum has been the most active in proposing (application) token definitions as "Ethereum Requests for Comments" (ERCs). ERCs have become the *defacto* standard for describing tokens. As such, we will use Ethereum terminology and refer to token types by their ERC codes when describing them. Very recently (April 2019), the Token Taxonomy Initiative[5] was launched to address the need to universally define tokens and to better understand how their use and implementation can occur interchangeably across all token-enabled blockchain platforms.

---

[2] http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

[3] https://etherscan.io/tokens

[4] https://www.investopedia.com/terms/s/security.asp

[5] https://entethalliance.org/participate/token-taxonomy-initiative/

In the next section, we review different token types according to the fungibility category.

3. Fungible Token Standards

We noted that whilst some tokens store value directly in the form of cryptocurrency, many other tokens are more akin to financial securities, whereas some remaining ones have completely unique properties and uses. Designing a successful cryptographic token must take into account certain aspects of monetary theory, financial economics, and game theory. Crypto tokens can also have strictly controlled supply mechanisms and complex real-world relationships, thus facilitating coordination among stakeholders when network effects are present, i.e. they can be coded in a way that links their value to the number of token holders and the number of total tokens in circulation. Having said that, the original, “pioneer”, non-currency token was actually very simple in its logic and implementation and was originally developed on top of the basic Bitcoin blockchain. Subsequently, with the advent of more complex blockchains, more advanced token standards began appearing.

3.1. The basic “Coloured coins” on the Bitcoin blockchain

The term "coloured coins" loosely describes a class of mechanisms for managing real world assets on top of the Bitcoin blockchain that dates back to 2009. Building on the fact that BTC could not be double-spent, innovators added a layer to the bitcoin protocol to represent an additional guarantee in the form of a property title.

Quite simply, a coloured coin is a specific amount of Bitcoin (BTC) that has some significance beyond the coin itself. While originally designed to be a currency, Bitcoin's scripting language allows to store small amounts of metadata on the blockchain, which can be used to represent asset-related instructions. Real world value is attached to those digital tokens by the issuer's promise to redeem the tokens for some real-world goods or services.

In June 2015, the NASDAQ exchange in the US announced that it has developed a system using the Open Assets protocol that allows for standardised issuance and trading of coloured coins. In late 2015 NASDAQ announced that the first ever coloured coin trade had occurred. Since then, a completely new non-Bitcoin blockchain, Ethereum, has emerged, offering more advanced token standards.

3.2. Beyond the Bitcoin blockchain with Ethereum

Once a system has a certain level of trust, it is possible to run tokens on top of them that could represent different types of assets in different types of markets. This is exactly what happened with the Ethereum blockchain that was initially released in 2015 (stable version created in 2016) and quickly attracted a lot of innovation in terms of new and varied token standards. The main Ethereum token, *ether* (ETH) is a cryptocurrency, and is currently the second largest cryptocurrency by market capitalisation, the largest one being Bitcoin (BTC) which was discussed in the previous section and is

mostly unrelated to Ethereum - although both can be traded on multitude of exchanges. Ether is also different to Bitcoin in a few more aspects, notably different transaction times, varied supply mechanisms, variable computational complexity and diverse classes of transaction fees.

However, on the Ethereum blockchain, we can do more than on the Bitcoin blockchain, specifically, developers can use smart contracts in tandem with a special programming language called *Solidity* to specify the logic and the structure for a wide variety of usage patterns[6]. Examples of tokens that leverage this advanced blockchain functionality will be described below:

3.3. ERC-20: A class of identical tokens on Ethereum blockchain

ERC-20 is a standard used for smart contracts on the Ethereum blockchain for implementing money (currencies) and currency-like tokens. Most tokens issued on the Ethereum blockchain are ERC-20 compliant and almost 200,000 different types are present on the main network.

All ERC-20 tokens are purported to be fungible, so that one is never expected to add a history, provenance, or identity to any ERC-20 token. This fungibility means that there are very limited ways of adding metadata to ERC-20 tokens, a strictly controlled mechanism that differs from Bitcoin's coloured coins approach. The Ethereum ERC-20 token standard became popular with crowdfunding companies working on initial coin offerings due to the simplicity of deployment. The most successful ERC-20 tokens include the EOS ERC-20 (now frozen and mostly swapped to mainnet EOS) and Tezos.

3.4. The fungible ERC-223 ("upgraded ERC-20") token standard

ERC-223 is a backwards-compatible upgrade to the ERC-20 token standard. It eliminates the problem of lost tokens which happens during accidental transfers of ERC-20 tokens to contract addresses when people mistakenly use the instructions for sending tokens to a wallet. The ERC-223 specification allows users to send their tokens to either wallets or contracts within predefined protocols, thereby eliminating the potential for confusion and lost tokens.

This upgraded standard also allows Ethereum developers to handle incoming token transactions in a way that rejects non-supported tokens. In this case, you won't lose the unsupported tokens as they will be automatically refunded back to you, minus the *gas* (the cost of processing your instructions), something that was not possible within the ERC-20 framework.

Finally, the new protocol offers significant energy savings. The transfer of ERC-223 tokens to a contract is a one-step process rather than 2 step process (as was the case for ERC-20), and this means two times less gas and no extra blockchain bloating (consider that in a blockchain every party gets the copy of every transaction incurring additional network congestion). This, as a result, also lowers the transaction fees one pays for the transfer of tokens.

[6] This can be generalised to any Smart Contract enabled blockchain and its corresponding language.

3.5. ERC-621 fungible tokens and other extensions

The **ERC-621** token standard was proposed in early 2017 and has since gained some momentum as an extension of the ERC-20 token standard that caters for some particular niche applications. This specification adds two additional contractual functions that enable token governance to easily increase and decrease the total supply of tokens in circulation, as contrasted to ERC-20 which only allows a single token issuance event which restricts the supply to a certain amount which can't be changed. Since ERC-621 proposes that the total token supply can be modified, this standard has proven useful in implementing certain *fiat pegged tokens* (tokens representing the value of a real-world currency, for example the British Pound).

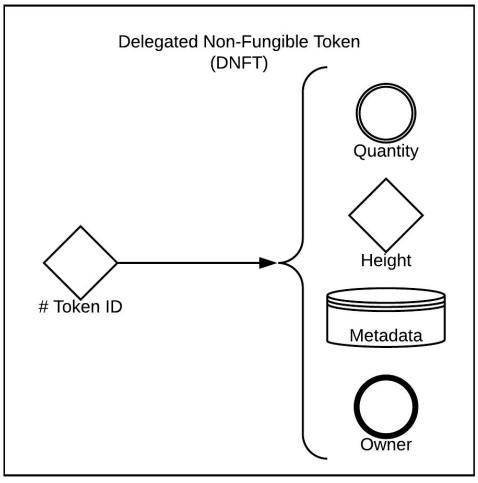
Another extension of the ERC-20 standard is **ERC-827**. It allows for the transfer of tokens and allows tokens to be approved by the holder to be spent by a third party. Tokens on Ethereum can be reused by other applications, including wallets and exchanges. This could be very useful for spending a dynamic amount that is up to a third party based on some criteria both parties have agreed to.

4. Non-Fungible Tokens on Top of ERC-721 Specification

Non-fungible tokens are used to create verifiable digital scarcity. Ethereum community created an open standard for issuing non-fungible tokens (NFT), called **ERC-721**. Introduced in 2017 (finalised in 2018), the standard exhibits some important properties for conforming tokens:

- Token cannot be divided or combined.
- Token can only belong to a to a physical address - to an account - either user's wallet or another smart contract; each token can thus have one (and only one) owner;
- Tokens, minted after contract creation, must follow a special protocol for any transfer of ownership, ensuring the safety of the transfer.
- To implement that standard, we can use a so-called first-party solution (the ERC-721 minting contract performs the sale) or a third-party solution (another contract performs the sale.)

Non-fungibles have since become actively used for varying use cases, and evolved in many directions.



4.1 Non-securities non-fungibles

ERC-994 was subsequently introduced as an extension of ERC-721, and quickly dubbed "Delegated NFTs". This upgrade was specifically designed with the use case of Ethereum-based registration of land and physical property in

mind. **Delegated ERC-994 NFTs (DNFTs)**[7] are arranged in a federated, tree-like format, similar to a domain name system, where each NFT can "delegate", or sub-contract other NFTs within a certain space ("zone"). Unlike many digital assets, like currencies or collectibles, physical property needs to be valid within the context of the physical scheme that governs it. Thus, DNFT "zones" can be established by different land registry authorities around the world, through enabling the creation by each such authority of a root-level Delegated Non-Fungible Token encompassing a wide area. Children DNFTs can then be created as subdivisions of this root.

ERC-998 was subsequently introduced as an extension of the ERC-721 and became the "Composable NFT Standard". This has found its use in massive multiplayer online games, allowing players to not just purchase individual items (like villages) but to grow collections of them (like empires)— all through a single token of ownership. In one such game, in-game characters can be composed of all of its underlying NFTs: shield, sword, boots, special items, and even other ERC-20 tokens. When you are ready to sell or trade the character, it takes just one blockchain transaction, after which all underlying assets belong to the new owner. The advantage of composable NFTs is thus reduced transaction costs.

ERC-948 is a recently proposed standard protocol for Subscription Services on the blockchain. Under this scheme, the user can create a new subscription on a blockchain smart contract, permitting "x" tokens to be withdrawn from his/her wallet every "y" time period by "z" Service until this user cancels the subscription.

The massive growth of the non-fungible token industry, as illustrated by the multitude of standards, of which the main ones were described above, has also led to the emergence of blockchain securities that have since received legal recognition. These are described in the next subsection

4.2. Securities tokens

The promise of implementing securities on the blockchain has generated discussion about a lot of potential benefits, such as reduced costs, automated compliance, rapid settlement, increased transparency, better liquidity and more. A security token offering (STO) is an offering of traditional securities in a digital token format in order to raise funds. Competing standards have emerged, with various degrees of recognition worldwide. A Security Token shares many of the characteristics of both fungible and non-fungible tokens. In particular, security tokens are designed to represent complete or fractional interests in assets and/or entities ("having a stake").

An early standard, **ERC-884**, or "tokenized shares", takes advantage of a recent Delaware blockchain-friendly Senate Bill (n. 69). The ERC-884 is a Ethereum token spec allowing any Delaware corporate entity to use a smart contract to create and maintain an official share register on the Ethereum blockchain. Essentially, this is a legally compliant standard for tokenized equity. Successful ERC-884 are SEC approved and can be traded on traditional financial markets as securities. However, in

[7] https://github.com/ethereum/EIPs/issues/994

order to comply with securities laws, issuers of ERC-884 must also maintain an off-chain private database which makes it more of a hybrid approach.

The **ERC-1400** standard introduced the concept of a **partially fungible token** that provides transparency over the partitions of a token holder's balance that may be treated differently by the security token for the purposes of transfer restrictions. The term "tranches" is used to describe these partitions. Since its introduction, the single ERC-1400 standard has developed into a *suite* of several standards with separate specialisations:

- The **ERC-1594**, which was designed to provide the core functionality needed for all security tokens;
- with the **ERC-1410**, a user's balance can be divided to accurately reflect the different specifications that come along with token ownership;
- the **ERC-1644 -** a method for controlling and managing security tokens;
- last but not least, **ERC-1643 -** a method for document management.

The idea behind this suite of solutions is to propose a common framework so that investors, issuers KYC suppliers, exchanges and wallets can work under the same conditions, increasing the democratisation of securities in the digital world (just like the ERC-20 has democratised utility tokens).

Out of non-Ethereum ecosystems, notable is **SRC-20,** a standard developed by Swarm Fund, an asset tokenization platform that runs on a utility token (SWM). The trading of SRC20 tokens also occurs on the private blockchain to ensure that Swarm can monitor trades and ensure compliance. To address the concern about the lack of common blockchain standards for regulatory purposes, Swarm have created an interoperability-focused security token protocol called Market Access Protocol (MAP) that acts as a tool to determine whether a wallet is compliant with securities regulations, and only allows transactions to occur if compliance is verified.

More time is required before mass adoption of securities tokens becomes reality. On the protocol level, there needs to be an industry standard that is more interoperable. The markets always need a certain amount of bootstrapping time to build up liquidity of new solutions.

4.3. Re-fungibles and token bonding curves

Token holders could also hold a quantity of fungible tokens that represent in some way the original non fungible token. This structure has been dubbed "Refungibles" and potentially interesting applications were described in **curation markets** for art, Intellectual Property (for example, big pharma and other types of innovation) and digitally paywalled content. Of particular interest, first developed by Simon de La Rouvière[8], is an innovative proposal for a bonding (or bonded) curve that represents the price per token as a function of the number of tokens in circulation (x-axis) by a predefined formula. The function (slope) can be linear, exponential, logarithmic or arbitrary, allowing the token governance to control how the token price increases with the number of tokens in circulation. The value derived from curved bonding is that rewards participants for buying tokens at an early stage and encourages them to participate in curation activities.

[8] https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5

Several projects have started to integrate bonding curves into their tokens, for example, Ocean Protocol. A decentralized data exchange protocol aimed at providing an ecosystem for the data economy and associated services. Data and service providers publish their services in the platform, other actors can decide to become servers of data or executors of algorithms and services for a fee, and consumers can buy them in a decentralised environment. From a network perspective, the community is interested in maximising the number of relevant AI and data services. But how to decide on relevancy? Enter bonding curves, each dataset of service is assigned its own token (called a *drop*). Drops can be acquired by users and servers, representing a stake on the value of datasets and services, the expectation is that users will be incentivized to find and stake for the most useful services, that will eventually prevail.

5. Initial Coin Offerings

Both ICOs and IPOs serve as a means for a private company to raise funds for a particular project or venture. Initial coin offers (ICO) are a way for start-ups or online projects to raise money without selling stocks or going to venture capitalists. This is a new form of crowdfunding. It is also known as token sales, coin sales, or more recently as "Token Generation Events" (TGE)[9]. ICO tends to give the impression of an IPO (Initial Public Offering) in cryptocurrency-based investment. The first ICO that ever went up for sale was Mastercoin in 2013, that raised around $500k (in BTC exchange rate at that time). ICO issuers accept a cryptocurrency such as Bitcoin in exchange for a token relating to a specific firm or project. These digital tokens can represent a share in a firm or a prepayment voucher for future services. A token is a representation of something in its particular ecosystem. A token is not limited to one particular role; it can fulfil a lot of roles in its native ecosystem. According to the US Securities and Exchange Commission (SEC) are two kinds of tokens; Security tokens and Utility tokens. Security tokens derive their values from external tradable assets. Utility tokens simply provide users with a product and/or service. The programmers may also raise money by creating and selling their own virtual currency, generally with rules similar to well-known virtual currencies.

The tokens sold in the ICOs may or may not be considered securities under current securities laws. This is because the tokens give the buyer the right to get access to the products or services provided by the platforms being built by the ventures, but not an equity stake on the projects or issuers. In reality, ICOs are very different from cryptocurrency emissions, because of the implications of having a stake in a business, as opposed to having a token that does not represent any stake ownership. Furthermore, the unique capabilities of smart contracts and blockchains enable two extensions with respect to traditional crowdfunding:

1) There is no dependence on a centralised platform to manage the campaign. Centralised platforms charge a percentage fee for the service, commonly between 4 and 8%. The act of contributing can be encoded as a transfer of crypto-currency in Smart Contract and deployed in a Smart Contract platform.

2) The token acquired by the contributor can represent many different things depending on the native ecosystem being developed with the token, according to the categories described in section 2.

[9] Some practitioners consider that the term ICO should be restricted to cryptocurrencies and securities tokens, and TGE used for network tokens, but there is no general consensus yet. Most legal advice documents use the term ICO.

An ICO is commonly comprised of two steps

Step 1 - Design the *tokenomics* of the product:

- What is the type of token, its exchange rules and how it maps to the envisioned ecosystem.
- Decide on the quantity of tokens to sell, or in the rules to generate them dynamically.
- the minimum price each token will be issued at and the (crypto) currency on which you will sell them. Application tokens that run on other platforms are sold in the currency of the underlying platform (e.g. Ether), while tokens that represent securities are usually sold in Fiat currency
- the share of tokens the entrepreneur will retain

Step 2 - Developing and launching the product:

- The entrepreneur uses the capital raised through the ICO to develop the ecosystem according to the plan.
- When the product is ready, its quality is revealed to all uninformed agents that invested in the ICO
- The entrepreneur launches the venture with tokens being the only accepted medium of exchange for its product/service
- Buyers trade tokens at a new market determined exchange rate
- Payoffs and profits are released

ICOs have, broadly, the following advantages:

1. ICOs give promising projects an opportunity to shine. Because stocks and venture capitalists are so few and far between, companies that use cryptocurrency as investment tokens provide more access to various investors from all economic levels. This is advantageous for start up companies who may not have the necessary funds yet to start their project but can potentially raise their value over time.

2. Paper involved with ICOs compared to IPOs is limited. Traditional assets such as IPOs, stocks, bonds, and other exchange forms reply on various regulatory filings that can take up time and energy. What makes ICOs more attractive than IPOs and other traditional assets is that they rely on blockchain technology to keep a ledger on its various transactions. This allows the constant update of data in mere seconds. For ICO what is required is a good quality whitepaper.

3. Liquidity enhanced venture capital. This is basically because investors can trade tokens in secondary markets rather than have value locked up in the equity of a company. This can ensure an acceleration of the return on the investment made by the investor. Investors also get to see how the company is performing based on the secondary market and real-time pricing.

4. Projects unattractive to venture capitalists because they lack an aggressive profit motive now can be funded. This is because stocks and venture capitalists are so few and far between, companies that use cryptocurrency as investment tokens provide more access to various investors from all economic levels. This is advantageous for start-up companies who may not have the necessary funds yet to start their project but can potentially raise their value over time.

5. Accessible on-line: All transactions are done online. Everything can be easily investigated and traced online.

However, ICOs also come with the following drawbacks:

1. Lack of paperwork also means scammers and fraudsters enter the game. Fake whitepapers are created. Many ICOs do not undergo the same regulatory process as IPOs and other traditional assets. This may make them subject to fraud and other malicious practices. These start-ups tend to present their whitepaper without proper resources to get the product ready.

2. Tokens are traded on cryptocurrencies, that often have enhanced privacy and anonymity capabilities. These properties, very desirable for many, have a double-edge in this context: scammers can use them to transfer funds without trace even more easily than through fiscal paradises. Scammers can then exit (hence the name *Exit scam*) with the funds before any real value has been delivered.

3. Unscrupulous exchanges might collude with scammers to convert cryptocurrency to Fiat currency. Scammers run away with Fiat currency, exchanges launder money.

4. ICOs offer no way of genuinely knowing if early investors are still confident in the team and its progress so later investors must rely on general market sentiment. Many ICOs stem from start-up companies and other private institutions that do not have enough existing funds to start their potential projects. Thus, there's no guarantee that the said companies will be able to deliver what they promise. There is a lack of accountability.

5. Various blockchain technologies are prone to various price changes in their assets which can be a tumultuous experience. Without proper knowledge of the factors that affect the product of the ICO, investing in one can leave an investor at huge losses.

Currently, the most successful ICOs have been for Native Tokens: Ethereum[10], Neo[11], Stratis[12], EOS[13] fuel Smart Contract platforms and all have raised hundreds of millions of € while offering a service that is used by many. In the Network token category, the most successful have been those that promise backend functionalities: Storj[14] (decentralised data storage), Golem[15] (decentralised computing time marketplace), and Bancor[16] (liquidity when exchanging different blockchain tokens). Several application tokens have raised varying amounts of capital through their ICOs, but most of them are yet to prove that they have delivered a sustainable product. A study by Gadhami et al.[17] analysed 253 ICOs to understand success factors, finding that those with available code source, token pre-sales and with a purpose of being a network token had more chances to succeed.

[10] https://www.ethereum.org/
[11] https://neo.org/
[12] https://stratisplatform.com/
[13] https://eos.io/
[14] https://storj.io/
[15] https://golem.network/
[16] https://www.bancor.network/
[17] Saman Adhami, Giancarlo Giudici, Stefano Martinazzi. "Why do businesses go crypto? An empirical analysis of initial coin offerings". Journal of Economics and Business,Volume 100,2018. https://doi.org/10.1016/j.jeconbus.2018.04.001

Unfortunately, not all ICOs have been established in good faith, exemplifying many of the drawbacks listed above. For example, Pincoin first sold Pincoin tokens that were exchangeable for Fiat currency, luring investors as everything worked as expected in the beginning. However, at a later stage, they launched a second token called iFan and started "paying" Pincoin holders with it, building on the trust accumulated during the first stage of the scam. This second token was worthless and not exchangeable. When the time was right, the scammers exited with an estimated $600MM[18].

Other ICOs have adopted Ponzi or Pyramid schemes to steal money from unsuspecting investors, lured by the hype of Blockchains and the promise of high ROI rates. The most famous of such scams was OneCoin[19]. OneCoin initially sold "Educational Packages" that came together with OneCoin tokens that "allowed mining" and eventually would result on a wire transfer in Euros being sent as a reward. On top of that buyers were encouraged to bring more investors in exchange for more OneCoin tokens. It turned out OneCoin didn't even had a Blockchain or Smart Contract deployed, deceiving more than 3 million people around the world and scamming an estimated of $4Billions.

Another economic attack that can be done of tokens is *Pump and Dump.* A single investor with a lot of capital, or a group of coordinated investors, choose a token or cryptocurrency and buy lots of it, while at the same time advocating its virtues in social media or other channels. This pumps the price up and lures other investors to join the positive trend. When the time is right, the attacker sells all the tokens at once (dump), driving the price down and leaving other investors with losses. Some websites like ICOBench.com[20] indexes more than 1000 current ICOs, categorized in Utility, Security, and Payment (cryptocurrency) tokens and provide credibility scores that can inform buyer's decision.

The existence of these attack vectors prompted regulators to re-evaluate the legal status of ICOs to discourage scammers and protect investors. In a nutshell, if tokens are a form of currency, then the issuing startup may need to comply with know your customer (KYC) and anti-money laundering (AML) regulations; if tokens are securities must comply with certain securities and exchange commission (SEC) regulations[21]. Regulatory bodies have been reacting differently to this new concept. In Europe in particular, we cite the following examples, compiled by White & Case LLP[22]:

Germany: Bundesanstalt für Finanzdienstleistungsaufsicht ("BaFin") will determine the applicability of certain national legislation. If the token is deemed a share or a security, then all legislation applicable to the non-blockchain exchange of shares and securities applies. Utility and currency tokens are exempt from this legislation.

France: Regulation expected to come into force around summer 2019), provides, inter alia, (i) a legal definition for Tokens and crypto-assets; (ii) an optional approval from the Autorité des Marchés Financiers (AMF) for 'utility' ICOs; (iii) a legal framework for crypto-asset intermediaries (exchange platforms, custodians, investment advisors, etc.); and (iv) an ad hoc tax regime for investors and ICO

---

[18] https://techcrunch.com/2018/04/13/exit-scammers-run-off-with-660-million-in-ico-earnings/

[19] https://cryptoiq.co/onecoin-a-4-billion-ico-that-ended-up-being-a-ponzi-scheme-never-had-a-functioning-cryptocurrency-or-blockchain-leader-arrested-but-founder-still-on-the-run/

[20] https://icobench.com

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

[22] https://www.whitecase.com/publications/alert/update-status-initial-coin-offerings-europe

issuers. Security Tokens will be considered regular financial instruments and therefore will be subject to the same laws as their non-blockchain counterparts.

Switzerland: Like Germany, the Financial Market Supervisory Authority (FINMA) will determine the applicability of regulatory law on an individual basis, distinguishing between Currency Tokens, Utility Tokens, Asset Tokens and Hybrid Tokens. Again, the critical point is to determine if the token is a security, as in that case relevant regulations apply. Asset tokens are automatically considered securities, while Utility tokens will be assessed as securities if there is an "investment purpose at the point of issue".

EU level: Both the European Banking Authority[23] and the European Securities and Markets Authority[24] have recently released reports advising the European Commission on the subject of crypto-assets. The main identified risks are posed to investor protection and market integrity, as unfortunately, many unscrupulous organisations have taken advantage of the unregulated environment to scam investors. The main question that needs to be answered is "Which Crypto-Assets qualify as financial instruments according to the MiFId directive". Any crypto-asset that does not fall under these directives increments the risk for people buying them. ESMA also recommended that all crypto-assets should align to money-laundering regulations. The latest amendment of the relevant EU directive on the subject[25] introduces "monitoring of virtual currencies" as a duty of competent authorities.

6. Towards Digital Asset Ecosystems

In the last year, we have seen the emergence of digital asset ecosystems. The slow but steady process of institutional investors entering digital-asset markets hinges on the progress of crypto asset custodianship solutions. Of equal importance are: trusted issuance platforms, decentralised liquidity protocols, transparent and open exchanges, multi-signature key management services, as well as *stablecoins* that are often used as an intermediate means of exchanging of crypto assets for fiat currencies and vice versa. There is, however, a remarkable lack of open standards in the ecosystem space.

The emergence of these standards may not happen quickly enough unless regulators start closely cooperating with reputable technology providers, not just commercial but also open-source, who are already active in the ecosystem space. There is also scope for utilising the concept of "decentralised autonomous organisations" (DAOs) to create governance structures on the blockchain that are capable of representing traditionally "off-line" financial organisational structures like special-purpose vehicles (SPVs).

At the time of writing this report, it is estimated that around 500 crypto-focused funds are in operation, jointly managing up to $10bn. in digital assets. Apart from the number of technology-focused job openings this creates, there is also likely to be an increased demand for legal specialists that are able to service crypto-backed investments and funds.

[23] https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf
[24] https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf
[25] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

7. Conclusion

Blockchains and particularly smart contract platforms, empower organisations and communities to set up their own economic systems in a decentralised way. By defining tokens and the rules for their exchange, and deploying them in decentralised platforms, practically any process can be supported without the need of trusting a centralised third party. At the same time, by linking the value of the product/service/exchange to a token, communities (and startups) can raise funds by selling them to interested parties (through ICOs and STOs), providing investors and clients with an asset that has a meaning in the relevant context. The reception of investors has been staggering, creating a huge a robust market and an emerging ecosystem.

However, as with many disruptive technologies, with great power comes great responsibility. With the exciting possibilities of rapid and decentralised deployment of tokens comes the responsibility of dealing with scams, economic attacks and limit the impact of the "double-edge" of the anonymity and decentralisation capabilities of blockchains to be exploited by criminals.

Regulators at the EU level have already been working on clarifying the situation with respect to the link with legislation applicable to traditional securities. Allowing the "intrusion" of regulators might be considered an attack to the decentralised principles of blockchains that could slow down the impact EU companies and organisations could get from the technology. We believe that this is not the case here, and that appropriate regulation is positive and will benefit all actors.

Further on this topic, an interesting research and development direction is the implementation of regulatory frameworks in blockchains. In the same way that other approaches have explored the use of blockchains for verification and compliance (Immutable records for e-government, ownership of real-world assets, GDPR compliance). If we can encode the rules of compliance and deploy them into a blockchain, we would be able to leverage the transparency and trust capabilities of blockchains beyond the implementation of a closed economic system and into the interaction of these ecosystems with regulatory frameworks. ICO/STO smart contracts could implement compliance functions that provide investors with a further trust mechanism. Another promising direction is the encoding of development roadmaps as smart contracts, that tie funds release to milestones that can be verified automatically (e.g. passing a series of software tests, or the results of an audit), an approach being explored in the context of research grants.