CRYPTOASSET VALUATION

Identifying the variables of analysis

Working Report v1.0 October 2018

Kary Bheemaiah

Alexis Collomb

This report has been written within the Blockchain Perspectives Joint Research Initiative, with the support of BNP Paribas and CDC Recherche

ACKNOWLEDGMENTS

We would like to thank Anuj Das Gupta (Chief Research Officer at Stratumn) and Hubert Ritzdorf (CTO at ChainSecurity) for their valuable technical inputs regarding Smart Contracts. Special mention also goes to Stefan Leins, the author of 'Stories of Capitalism: Inside the Role of Financial Analysts', for his valuable contribution on how securities are analysed today, and to the team at Autonomous NEXT for providing data and images from their Crypto Utopia report, which have been republished in this document.

ABOUT THE AUTHORS

Kary Bheemaiah: Kary is the Director of Research at Uchange, an Associate Research Scientist at Cambridge Judge Business School and Senior Fellow at École des Ponts Business School. He is the author of the book, 'The Blockchain Alternative: Rethinking Macroeconomic Policy and Economic Theory' (2017) and his articles on Blockchain and Fintech have been published on Wired, Harvard Business Review, World Economic Forum.

www.linkedin.com/in/karybheemaiah/

Alexis Collomb: Alexis is Professor of Finance at Cnam, Paris, where he also heads the economics, finance and insurance department. He is a scientific co-director of the Blockchain Perspectives Joint Research Initiative (BPJRI). As a fintech and insurtech devotee, he writes and lectures regularly on blockchain technology and cryptoassets. He is also a scientific adviser of PSL/Mines ParisTech's IHEIE, a leading international program focused on innovation and entrepreneurship and of Labex Refi, a think tank dedicated to financial regulation.

www.linkedin.com/in/ alexis-collomb-b2154336/

FOREWORD

It is quite clear that if we look at what has been happening in the ICO space over the last two years, there has been a mix of great, good, bad, and sometimes very ugly... In general, valuing crypto-assets is a complex issue. While many different token classifications have been provided, they all seem to have one common denominator : tokens are usually hybrid objects with various features—utility, security, etc. Hence valuing them properly is hard on at least three grounds : firstly, the projects these tokens support are more often than not very 'early stage' ; secondly, understanding exactly how these hybrid objects will create value, and the non-linearities in the process, is a difficult exercise ; thirdly, correctly anticipating how their overall ecosystem will unfold adds an additional degree of complexity. If it is already hard enough to properly estimate the share value of a 'traditional' product-oriented startup at the seed funding stage, it is easy to figure out that valuing ICO tokens is even harder. As for traditional startups, many analysts will take shortcuts and focus on one or two key aspects such as the whitepaper or the team.

To take up this challenge and help us structure our thinking around these questions, we have asked Kary Bheemaiah to look into this issue of how to properly value crypto-assets… Could we come up with a universal model to price ICO tokens ? Could we operate—as is usually done in the financial sphere—by either building discounted cash flows models or using 'comparable analysis' ? How should we organize the different value components and prioritize them ?

Those who have entered the fray of tokenomics will know how complex these issues can be and by no means, this report claims to have found the answers. As its first version is about to be published, it seems that the— irrational, many would say—exuberance that has fueled the ICO trend—especially at the end of 2017 and beginning of 2018—has been abating. As expectations are adjusting and the overall market is maturing, we hope this report will be helpful in helping entrepreneurs, investors, and researchers alike, to identify the variables and value drivers that matter—a first stepping stone not to be missed.

Enjoy the read !

Alexis Collomb
Scientific co-director
Blockchain Perspectives Joint Research Initiative

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Since the launch of Token Sales or ICOs in the past few years, the notion of developing valuation methodologies that can accurately ascertain the future of a token's price has become a subject of increasing debate, with some experts attempting to retrofit stock valuation models in the hope of creating accurate token price prediction models.

While these efforts are laudable, and necessary, they suffer from a few flaws: Firstly, there is a lack of empirical analysis – making any kind of prediction model requires rigorous empirical evidence. As the token market is still nascent we currently lack the necessary data to test these models. This issue is further compounded by the fact that there is a significant degree of diversity in the token space (work tokens, utility tokens, asset-backed tokens, etc.).

This leads us to the second problem, which is a lack of consistency in the type of data being used – how are the fields defined?, where is the data coming from? As tokens have currency-like properties along with functional objectives, a clear definition of the type of data being used is crucial to developing sensible valuation models.

Thirdly, there is a large amount of assumptions being made, the key one being that a model or a formula that is used for stock valuation can be applied to a new asset class which has very different properties. Very few of the token valuation models being built are able to explain the assumptions behind the formulas being used before applying them to new situations. Finally, there are the issues of overfitting and model complexity – data scientists often talk about the Bias-Variance Trade-off which states that complex models tend to be overfitted, i.e.: they work well on past datasets but poorly on future datasets. This last issue comes back full circle to the first problem of lack of empirical evidence and can cause spurious correlations. As a result of these issues, investors wanting to deploy capital in token projects are at a loss as there is no reference framework.

The purpose of this report is therefore to start at the basics, or more precisely, **the variables**. Having conducted extensive research we provide the reader with a list of variables that need to be considered when analysing a token project. Readers of this report who are interested in developing a valuation methodology must realise that there is currently no universal token valuation method. Instead they need to follow a modular approach in which key variables and analysis methods need to be selected based on the kind of token or cryptocurrency they are interested in evaluating. Thus, our goal is to provide the variables that need to be taken into consideration. We are cognizant of the fact that to truly develop a valuation method, we require to determine the adoption curve of the business model behind a token sale. As most of the ICOs are still in a phase of development, we currently lack the data necessary to build such a model. But by reviewing the models being used and by identifying the variables that are key to understanding the feasibility of a token project, it is our goal to set the stage for building token valuation methodologies and frameworks in the future.

INTRODUCTION

Since mid 2016, the subject of token sales/ICOs has become an increasingly discussed topic with varying views. Some regard the rise of this new investment model as the future of crowdfunding, while others have branded it as a vehicle of scam.

The reason for this level of interest stems from the fact that over the past two years, the amount of investment generated from this investment vehicle has grown at a phenomenal rate all across the globe. Few investment vehicles have been able to generate similar amounts of capital raise in such limited time periods (See Figure 1).

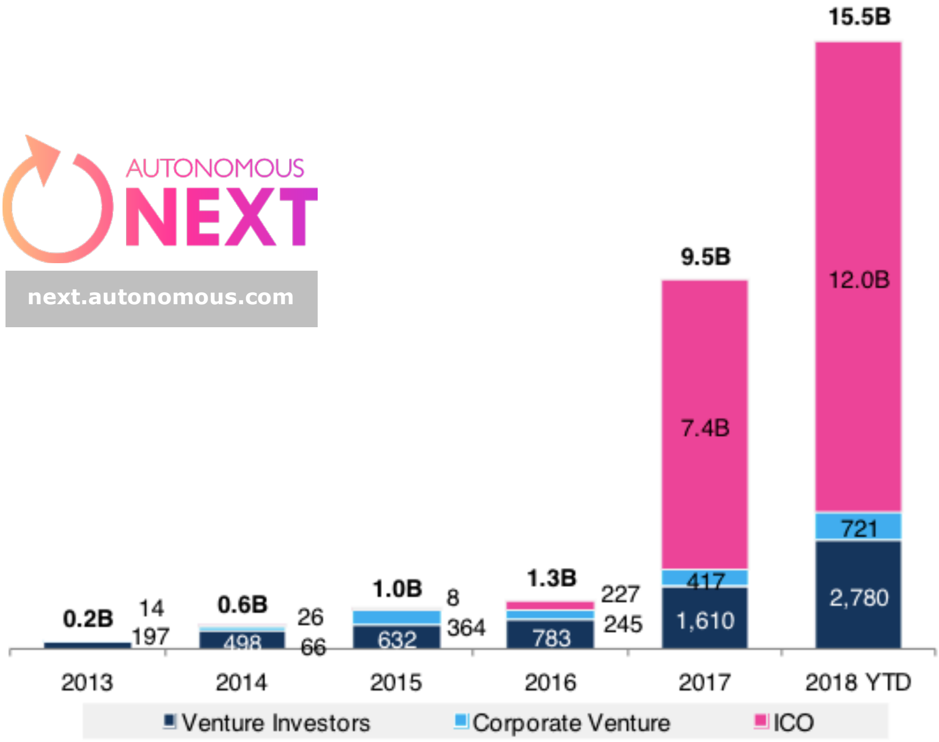
Prior to the launch of ICOs, most entrepreneurs had to follow a laborious process to acquire funding – approach Venture Capitalists (VCs) or similar investors, and present a project with multiple supports - such as a well-defined marketing strategy, a realistic yet ambitious business plan, a prototype of a product or service offering, summarized test-group reviews, growth expectations, term sheet proposal, etc.

VCs would then decide on which projects were worthy of investing in, and it was common to hear stories of entrepreneurs being rejected multiple times before gaining a first round of funding.

But with the rise of ICOs, this process has been significantly altered. Based on the publication of a white paper (which is essentially an extensive business proposal that includes specifications of a to-be constructed product or service), and by leveraging the hype of the Blockchain, a number of entrepreneurs have been able to access considerable sums of funding via token sales.

The sums being raised are quite significant as well. As per recent market statistics, approximately $5.6 billion was raised via ICOs in 2017, and by the first quarter of 2018, that sum was already surpassed. Some approximations state that $12 billion have been raised since the beginning of 2017.   Figure 1 offers some insight.

Figure 1 : ICO Funding versus VC and CVC Funding



Source: Crypto Utopia, Autonomous NEXT, 2018. Image republished with permission.

Key Figures[1]:

2016: $240 million(M) raised via Token Sales

2017: $5.6 billion(B) via Token Sales compared to $1B via VC

2018: $6.3B

Average raised via Token Sales = $12.8M

Summary of waves of investment into crypto-assets (2013 – 2018):

- First wave of investment from traditional venture firms in Bitcoin associated companies started in 2013. From $200 million in 2013, it reached almost $800 million in 2016.
- Second wave of investment came from corporates. Between 2015 and 2017, between $250-$400 million was invested annually
- Third wave of funding came from public crowdfunding into ICOs, with an unprecedented rise in prices for cryptocurrencies. Over $7 billion of investment went into the space, almost 4x greater than equity investment in crypto companies
- Many ICOs formed to take advantage of the "gold rush" and created questions and issues of quality and regulation for tokens[2].

[1,2] Data Source: Tokendata.io, Coindesk and Fabric Ventures

The reason for this spurt in access to funds is two – fold:

Scope: Previously, the domain of funding in early stage lucrative start-ups was a privilege generally reserved to VCs and wealthy investors. Indeed, in most OECD countries, only 12% of the population invests in stocks (Lacalle, 2017) . To partake in this kind of investing, a participant needed access to significant funds and an ability to deal with risk.

However, as blockchain technology is decentralized and allows investors to contribute small sums , the chance to invest in such offers was now open to anyone with access to the internet and with a humble disposable income.

Token sellers thus quickly realized that what they could achieve with ICOs was vast economies of scale in which the sum of many small contributions largely exceeded the capital furnished by high net worth investors. Not only could they access a bigger pool of investors, but they could also get funded faster – For example: The Bancor ICO raised $153 Million in less than a day (See Table 1).

Utility: While initial Blockchain projects were mostly focused on payment solutions, as the technology has matured and as the use of Smart Contracts has increasingly proliferated, the application of this technology has spread to different sectors and industries thus drawing investors in the process. Figures 2 and 3 respectively show the industries and investment sectors that are being penetrated by this technology:

Table 1: Top 10 ICO raises:

Project	Raise
Tezos	$230,498,884
Filecoin	$200,000,000
Sirin Labs	$157,885,825
Bancor Protocol	$153,000,000
Polkadot	$144,347,146
QASH	$108,174,500
Status	$107,664,904
Kin	$98,500,326
COSMA	$95,614,242
TenX	$83,110,818
Total	**$1,378,796,646**

Source: ‘State of the Token Market’, Squarespace (2018)

Figure 2: Token Sale investment as per industry

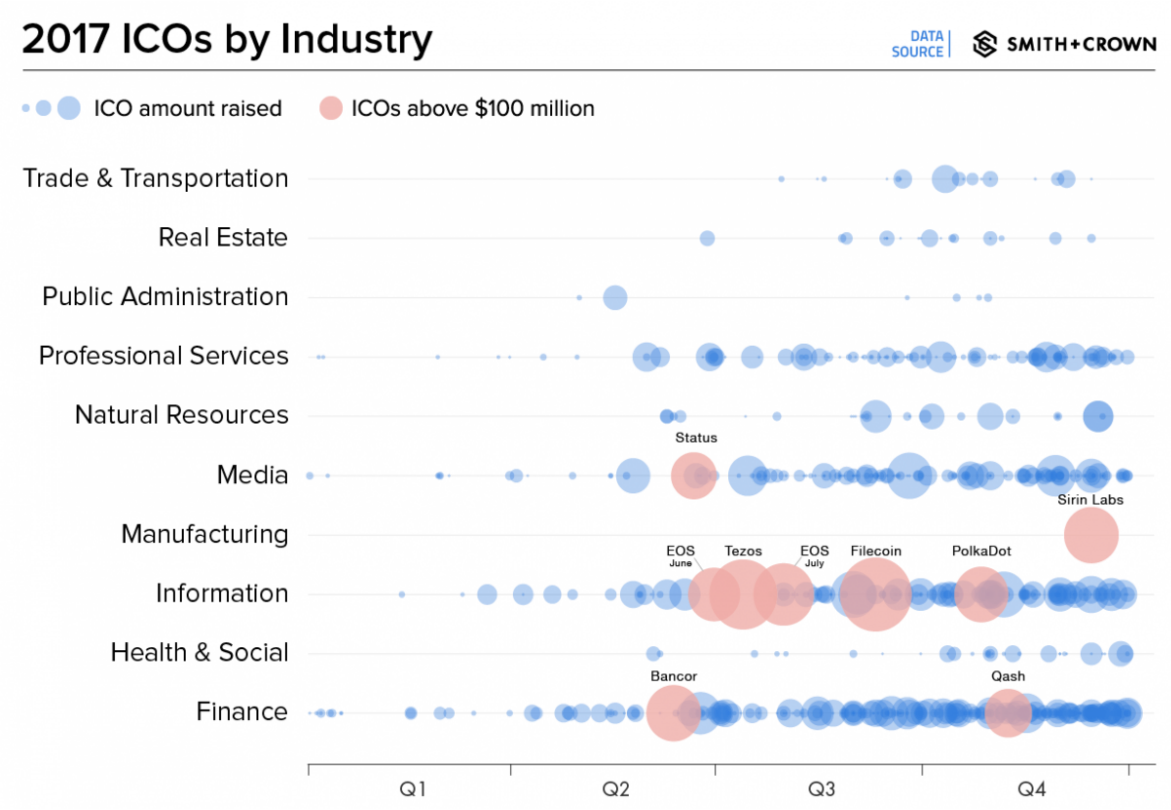
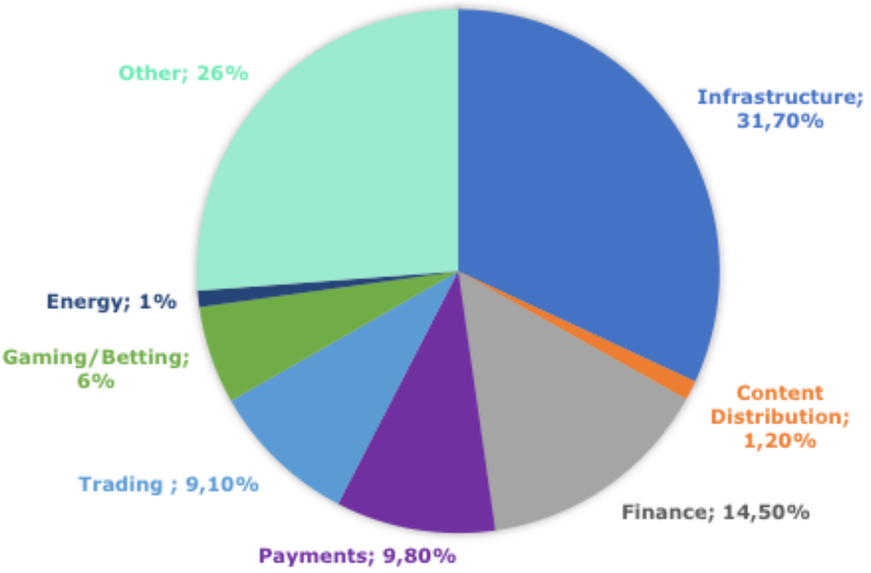


Image Source: Smith and Crown.

Figure 3: Token Sale investment as per sector



Data Source: Fabric Ventures and Tokendata.

As a result of this fast emerging trend, even long term successful VCs like Fred Wilson of Union Square Ventures are beginning to acknowledge that they need to adapt their business model in light of these changes:

> *"[ICOs represent] a legitimate disruptive threat" [to the VC model],… We are excited about them when they are the right thing for our portfolio companies and we are encouraging those companies to use this new approach."* (Wilson, 2017)

OBJECTIVES

In light of these fast paced changes, the first objective of this report is to provide the reader with an understanding of how investors are currently analysing ICOs prior to allocating their capital.

While equity investing has established models and standards, the same cannot be said for token investing. As a result, a number of investors have tried retrofitting stock evaluation models in order to attempt to create token valuation models.

While these approaches are laudable, we show that owing to the networked nature and diversity of tokens, such models have limited applicability. Thus, a secondary objective of this report is to show what needs to be taken into consideration by investors who want to create token valuation models.

It must also be remembered, that while token sales show promise, in terms of creating a new crowdfunding model, testing a valuation model requires empirical evidence.

As of today, most of the funds received by token issuers are being used to build the actual product or service they described in their whitepapers.

Without sufficient data regarding the adoption cycle of their products, the switching costs that users will have to bear when switching from an App to a Dapp, the multi-modal nature of tokens (tokens bear currency-like aspects that are not seen in stocks) and the changing regulatory environment, building a generalistic evaluation model would be erroneous today.

Our main objective is therefore to provide some guidelines of what needs to considered when such an attempt is made in the future.

PART 2: CURRENT STATE OF TOKEN VALUATION

1.1: FRAMING THE PROBLEM

While the process entrepreneurs have to follow with traditional capital raising is laborious, it serves a purpose. It helps ensure that a project is viable, that a product has worth and the capital being raised will be used appropriately over a long period. In exchange the team benefits from the guidance of an experienced investor who apart from providing them with capital, can also furnish technical, legal or business guidance to help grow their company.

Rigorous due diligence is conducted as there is a cost of ownership – when a VC invests in a start-up, they gain access to a certain percentage of the start-ups shares, i.e.: ownership of the firm, and any associated liabilities as a consequence. Similarly, by accepting VC capital, the entrepreneur is giving up part of his/her company and open to the risks that might affect the investor's portfolio.

This mutual sense of responsibility is however partially lost with ICOs. A token sale generally does not function as a share/dividend. Contrary to its namesake, the Initial Public Offering (IPO), an ICO or Token Sale does not involve the sale of equity in (or voting rights pertaining to) a company per se. Instead, ICO participants are acquiring an asset— a "token"—which allows the holder to use, or govern, a network that the token sellers plan to develop using capital raised via the sale of the token. As the business behind the token is yet to be built and has no assets or earnings, there are very few data points that can be used to estimate the value of the company, let alone determine what the token price should be.

Moreover, a token does not offer a dividend (as a stock does) as the company has not yet generated a cash flow. Most tokens only offer a right to the future use of a to-be-constructed product, under the assumption that the company will not pivot the product once it has received the funds. Recently the concept of Equity Tokens a subcategory of security tokens that represent ownership of an asset, such as debt or company stock has begun to gain some attention, but by and large, most tokens offer the right to the future use of a to-be-constructed product.

The de facto source of reference used by investors interested in investing in an ICO is the whitepaper. Some token creators will also publish a technical paper and in some cases, even some preliminary bits of code would be available for review which would be analysed by serious investors. But by and large, there is no concrete investment framework to determine the value of a token.

Thus, token investors are faced with a quandary. On one side, they are dealing with a technology that is yet to become a formal curriculum subject in most universities. Nevertheless it holds tremendous potential and is considered by a number of tech pundits as the next internet. The fact that established VCs are taking this technology seriously underlines the impact it could have on the financial industry.

On the other side, owing to the age of this technology and its evolving nature, there is no formal framework that can aid investors in determining the true value of a project classified under this new asset class. This problem is further compounded by the variety of tokens and their built-in functionalities that are usually tailored for specific purposes.

The lack of structure, frameworks and regulation means that currently, the ICO space is extremely susceptible to market forces. This statement needs to be further deconstructed in order to underline its contemporary significance in the context of ICOs.

History shows us that by and large, markets function as the best price setting mechanism in distributed, fair, decentralized networks. The actual value of any asset is based on the price that others are willing to pay for it, and competitive forces in a market allow different economic agents to set the price for a product or a service.

This modus operandi holds true when we are dealing with a tangible good or service that is immediately available. But when it comes to investment, agents are forced to compute an investment price based on its future anticipated value—usually represented by its stream of future cash flows.

To aid in this future determination, we use a plethora of tools to aid in our investment decisions. For example when evaluating the future value of a stock, we use methods such as Discounted Cash Flow (DCF) or Dividend Discount Models (DDM) among others. The market still sets the price. But by using these evaluation models, investors are trying to estimate what the future price would be based on a collection of data points that represent concrete elements such as physical assets, existing market share, IP, product-market fit, existing clientele population, etc.…

While these methods allows investors to encapsulate a future anticipated value, they also serve a secondary role of protecting against runaway market speculation. When the value of a good or service is being speculated upon, often times it is seen that markets can go awry creating bubbles and boom cycles in the process. Conducting DCF and DDM analyses thus allows investors to determine what a realistic price point would be for a stock. In the process, they mitigate against excessive market speculation.

Without tools such as these, the act of determining what is a sensible investment, and if it fits into your risk profile, is not feasible and investors would be exposed to the full brunt of open market speculation effects. While these evaluation methods are not perfect, they allow investors to add a certain dose of pragmatism when it comes to investing in a to-be-constructed good or service, or in the expected future growth of a company.

But when it comes to Token sales, we currently do not have a similar control mechanism. As a token is not a stock, using the same methods of stock evaluation does not offer the same amount of certitude. As we currently do not have a proper framework that allows us to determine the value of certain attributes of a token sale, this leaves the price of tokens open to market forces speculation. As a result, the price of tokens is extremely volatile. There have been multiple cases where cryptocurrency and token prices have seen dramatic rises and falls in short time periods (See Figure 4):

Figure 4: Cryptocurrency volatility index[2] movements (May 2017 – Sep 2018)

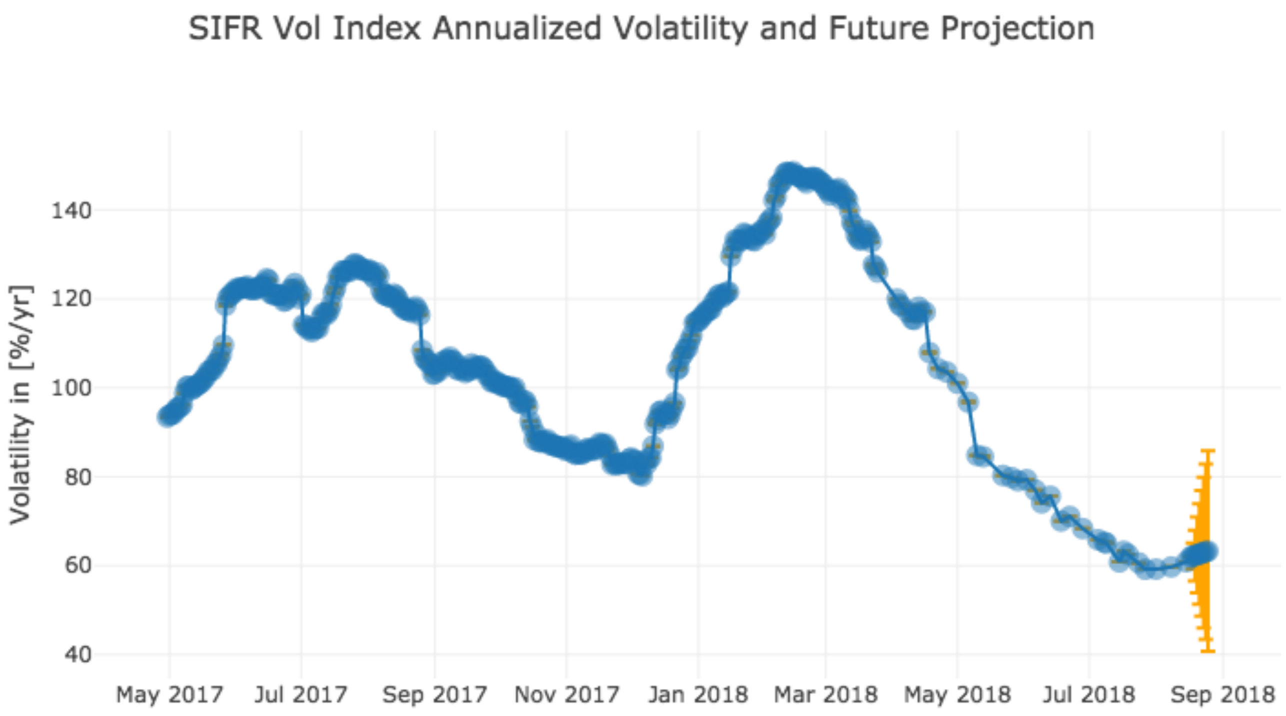


Image Source: https://www.sifrdata.com/

This susceptibility to market forces and resulting acceptance of token price volatility has led to a number of negative effects or practices of questionable utility:

- **Pump and Dump Schemes:**

As the regulations around this technology are still being set in place, it offers the chance to engage in market manipulation activities that would be considered illegal with other asset classes. Recently, nefarious actors on certain cryptocurrency communities (such as Big Pump and Alt-Pump) have resorted to 'pump n' dump' schemes, where a group of individuals get together on online forums and decided to artificially inflate the demand, and hence the price of a token. If one were to spend a few minutes scrolling the cryptocurrency content on Telegram, the encrypted messaging app, they

[2] The cryptocurrency volatility index is composed of six currencies: BTC, ETH, XRP, LTC, DASH, and XMR. The volatility index is weighted by the market capitalization of each currency which is updated daily by the index creators, Sifrdata. See: https://www.sifrdata.com/cryptocurrency-volatility-index/

would soon discover dozens of 'pump and dump' scams (Murphy, 2018) (Wall Street Journal, 2018).

Pump and dump schemes (a daily list can be found on pumpdump.coincheckup.com) are just one example of market manipulation that are rife in this loosely-regulated sector. Other practises such as front-running, wash- trading (which involves creating false volume by matching trades), and spoofing (where you place and then quickly cancel orders) are currently being practised. Unscrupulous agents leverage market forces and loose regulation to make a quick buck. No consideration is given to the business solution or to the problem-solving potential of the product behind the token. Value creation is scarified at the altar of short get rich quick schemes (Financial Stability Board, 2018) . In the words of Asaf Meir, the founder of Solidus Labs, which develops market surveillance tools specifically for crypto markets, "[The market] is highly, highly, highly manipulated. The extent is truly humongous" (Murphy, 2018).

- **Inefficient Capital Usage :**

Following the risk to volatility and pump and dump schemes, token creators have been obliged to hedge against the token's price volatility by indulging in capital protection techniques. This normally involves keeping aside a sizeable portion of the capital raised in reserve to counteract against token volatility.

For example – The Telegram ICO (which was subsequently cancelled) was launched in early 2018 and aimed to create censorship resistant file storage, messaging, decentralized apps and browsing. To fund the development of these complex consumer solutions and make their platform useable from an economic standpoint, Telegram decided to launch an ICO where investors could contribute and acquire TON tokens in the process.

While the objectives were aligned with societal issues, nevertheless, the TON needed to be protected against volatility. As a result, Telegram decided to keep aside 52% of the capital raised via the token sale in reserve.

The Telegram ICO aimed to raise $1.2 Billion in order to create its censorship proof solutions. 52% of this sum comes up to $624 Million, a sizeable sum to say the least. $624 Million that would not be used in the creation of products, but kept in reserve and unused. All to counteract the effects of market speculation and the actions of nefarious actors.

It is therefore essential that going forward, a solution needs to be found that will allow both token creators and token investors with a more efficient way to allocate capital raised.

- **Airdrops:**

In light of the above mentioned issues and the regulatory greyness with regards to ICOs in general, a new trend has emerged in which potential investors are given tokens for free in the form of an airdrop.

The objective of an airdrop is 3-fold:

i. Raise popularity of your token by engaging early adopters of this tech to create a network effect. An airdrop functions both as a marketing interface and an on boarding experience.

ii. Raise awareness of the token once more people start trading it, thus raising the price (if all goes well).

iii. Use (i) and (ii) to get serious investors who would be willing to contribute capital to the development of the project.

While the concept looks enticing and has had certain benefits especially from a legal standpoint, the ability of Airdrops to convert into actual investment requires more research and documentation – something that is hard to find today.

Furthermore, airdrops are essentially free token giveaways and offer very little to token holders. Essentially, holders of tokens (received via Airdrops or traded later on an exchange) are holding a security without any rights,

The development team behind the Airdrop can sell out the business to anyone without giving token holders any returns. They are also free to, they can take away any rights they do have, or decide that it is better for their business to accept USD or BTC next to their own token for payment – all of which lowers the value of the token or makes it worthless.

Another issue with airdrops is the supply of the tokens (a topic that will be addressed in later parts of the report). While scarcity of a token is often cited as the means of increasing its value, shortage of a token can create its own difficulties.

This was seen most recently with the U Network (a blockchain publishing protocol valued at around $8 million) , which in early July 2018, announced that it had run out of its reserve of UUU crypto tokens.

At the start of the project, U Network established a 10 billion UUU cap on its token supply (worth approximately $15.6 million). An estimated 8 million worth of tokens was given away in airdrops. But as the project gained traction and number of strategic partners began to increase, the demand for UUU tokens exceeded the designated holdings (Milano, 2018).

The U Network is now attempting buy back some of the supply it distributed to early investors through its airdrop in February. But as it will be seen in later parts of this report, the supply of tokens is a key factor that needs to be taken into consideration when coming up with a valuation model for a token sale.

1.1.1 What does this mean for the future of this investment vehicle?

Token Sales were meant to become an investment vehicle that would allow for democratic investment of capital and allow regular individuals to enter the investment space. It was portrayed as the big push that would allow equity crowd funding and peer to peer lending to replace the older system of investment banks and public capital markets.

However, a large amount of evidence shows that this objective is not being met in the way it was initially portrayed.. On the contrary, token sales are being used as a vehicle of manic speculation on trading markets. As providers of a token have little or no fiduciary duty to the investors, certain actors have made use of the lack of regulation to get capital for unrealistic projects and outright scams - as of today, 46% of ICOs have failed (Sedgwick, 2018) while and close to 10% have turned out to be scams (Cimpanu, 2018) . Considering that close to Over $20 billion has been raised by Crypto projects through Initial Coin Offerings since the start of 2017 (Autonomous NEXT, 2018) , 10% comes up to at least $2 Billion (an approximate figure) which is hard to ignore.

It is important to affirm at this point, that this does not mean that the technology is unsound or that it is a market for making a quick buck. A number of projects show tremendous potential to change the existing market structure and provide better, cheaper and more secure products and services to consumers all around the world.

This statement can be proved simply by the fact that many of these investments have been occurring in the corporate space. The figures below show how large companies are not just adopting blockchain technology but also using it to transform core business elements of their business models (CB Insights, 2018):

- MICROSOFT & ID2020 ALLIANCE (Accenture + Avanade) launched a project in early 2018 to provide ID services to 1.1B people
- GOLDMAN SACHS plans to open a CRYPTOCURRENCY TRADING DESK (end 2018)
- The mining company BHP BILLITON is using the Blockchain for contract work and analysis
- MAERSK + HYPERLEDGER are uniting stakeholders in global supply chains, to track freight & replace paperwork with tamper-resistant digital records
- UPS, FEDEX, AND BNSF RAILWAY JOIN BITA ALLIANCE to explore Blockchain technologies in freight transport.
- Petroteq creates distributed ledger for Pemex (the first petroleum company to accept crypto)
- UBS, BARCLAYS, and CREDIT SUISSE create an Ethereum based private platform to cross-reference legal entity identifier (LEI).
- Government of Singapore has launched Project UBIN to see how monetary and fiscal policy tools can be better constructed via the Blockchain.
- Walmart, Tyson, Unilever, Nestle, Kroger, Dole, McCormick, and others band together to launch a Blockchain pilot
- The United Nations explores DLT and Blockchains for humanitarian aid and climate science
- TEPCO (Japan’s largest utility provider) invested and partnered with ELECTRON to explore how energy price matching can be made more effective with micropayments.
- BRAZIL’S MINISTRY OF PLANNING & BUDGET, is piloting a Blockchain identity application using Uport, a self-sovereign ID platform built by Consensys

This level of interest, the rapid evolution of this technology and the increasing complexity of an ever growing participation pool, shows there is discernible value in this technology and being able to navigate this turbulent phase of the technology’s evolution requires education, poise, experimentation and patience. What is required therefore is a need to construct a valuation method that:

- Will allow investors to gauge the feasibility of a project,

- Will have a modular architecture which is able to adapt to the type of token being analysed.
- Will allow investors to mitigate against the negative effects of speculative market forces ,and
- Will ensure that they are allocating their capital sensibly based on rational attributes.

Such a methodology would allow investors to determine if the market price of the token directly or indirectly represents the 'true' value of the token, and to what extent this price is being affected by speculative market forces. Without such a framework, participants will be speculating on abstract ideas and rough compositions of turbulent revenue pools of newly founded companies, without any detailed understanding of what factors need to be analysed when looking at a growing business. This affects not just the investors but also the ICO founders who, under pressure from their community, are often forced to list their token on an exchange even prior to making any meaningful technological progress or a plausible product/service offering.

1.2 UNDERSTANDING TOKEN VALUATION METHODS

This need to determine the true value of a new asset class is not a new requirement. Early financial markets went hand in hand with fraud (Klaus, 2014) and since the creation of stocks and trading markets, the ability to discern between intrinsic or the true value of an asset versus the speculative value of an asset, has been an issue of pivotal importance to investors.

One of the first people to address this need was Benjamin Graham. In 1934, Graham published the book, Security Analysis, which offered the first formal approach to determine the intrinsic value of a stock. It is this work that led to the genesis of financial analysis and corporate finance.

Graham went on publish a number of other books on the subject including the well-known classic 'The Intelligent Investor'. It was on the backbone of his work that the fields of fundamental and technical analysis of stocks was created.

One of the repeating themes in the work of Graham, was the separation between Intrinsic and Speculative value of a security. Intrinsic value, as defined in Security Analysis, is

"that value which is justified by the facts, e.g., the assets, earnings, dividends, definite prospects, as distinct, let us say, from market quotations established by artificial manipulation or distorted by psychological excesses." ……..Logically, it must be based on the cash flow that would go to a continuing owner over the long run, as distinct from a speculative assessment of its resale value."

By driving a wedge between Intrinsic and Speculative value, Graham's work allowed investors to determine what the base value of a security was, how to determine it and how to use it in the face of rampant speculation, thus offering a margin of safety.

Intrinsic value was a key point in all of Graham's work owing to its stability. As the intrinsic value was based on fundamental attributes of a business (and its products as proxies), the value was measurable, justifiable and stable. Volatility still played a role as it is ultimately the market that sets the final price. But the intrinsic value of a security remained stable, measurable and quantifiable, thus making it a reference point when considering an investment as it allows investors to discern from market speculation

1.2.1 From Stocks to Tokens

The reason for reviewing the core tenets of financial analysis is because it is exactly this bedrock that is missing with token evaluation. In later parts of this report we will review the work done by various entrepreneurs and researchers who are exploring this subject with respect to tokens. We will see that while most of these efforts have been made in order to determine some way to evaluate the value of a token, most of these efforts have limited usability as they essentially try to retrofit stock evaluation methods to create a token valuation method.

But a token is not a stock. While stocks share a common framework the same cannot be said for tokens. Not only does do tokens not share the same economic artefacts of a stock, but by themselves tokens are rather unique entities.

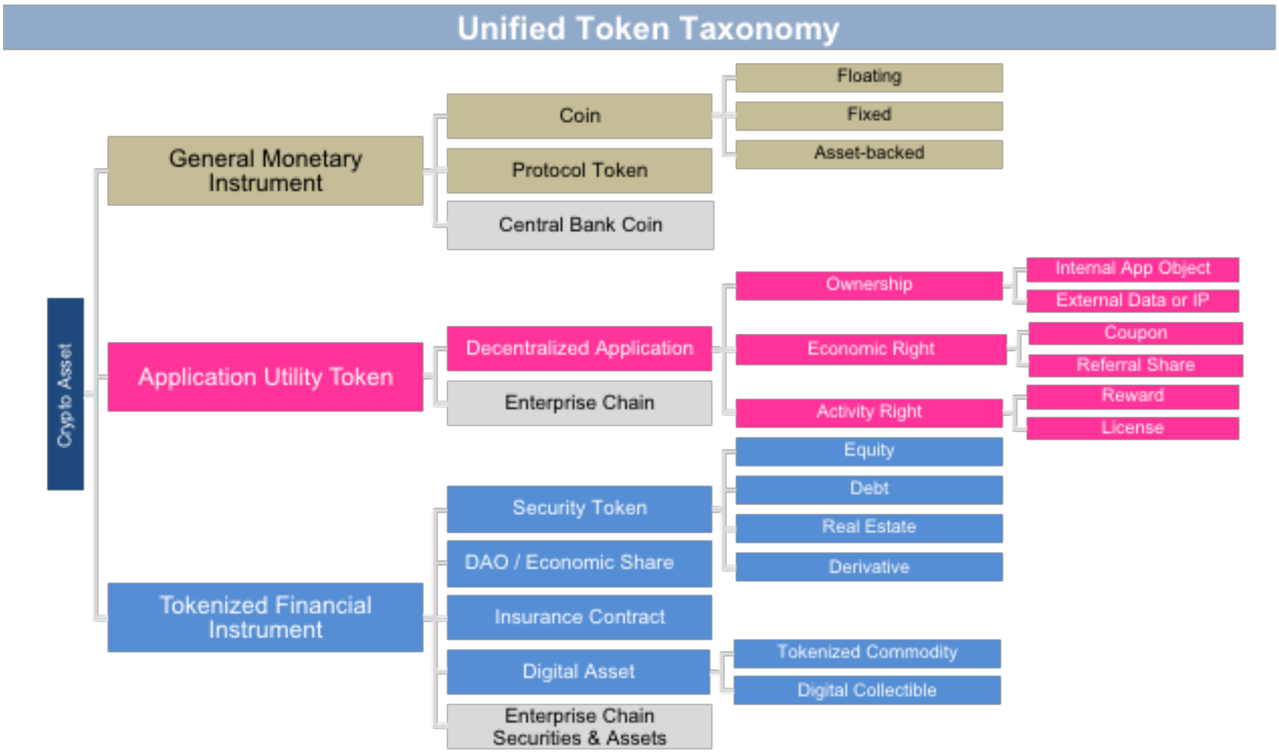
Firstly, a token has similar properties to a currency. A token functions not just as a fund raising mechanism or a utility instrument for a new product. It also functions as a means of exchange and as a unit of account to a certain extent. Thus it shares at least two, if not all three, attributes of a currency (Store of Value, Unit of Account and a Means of Transfer), which means that it needs to be evaluated as a security and a currency simultaneously.

Secondly a token is used to create, generate and stimulate value. As it is a unit of account and a means of exchange, a token functioning in a looped and interconnected network such as a Blockchain, is also an Endogenous Monetary system with its own supply, demand and liquidity issues Thus, when looking at a tokenized economic system, evaluators need to refer monetary policy aspects of this networked economy as well the underlying business behind it.

This aspect of supply is also intimately linked to the technical aspects of the token. The governance of tokenised assets or cyptoassets is done by smart contracts. Hence any changes in supply – including transfer or lock up plans – need to be hard coded into the smart contract. This makes the governance of tokens both an economic and technical issue simultaneously.

Lastly, there is the question of variety. Today, there are many different types of tokens - we have security tokens, work tokens, network value tokens, asset tokens, utility tokens, payment tokens and so on… Figure 5 shows us the current taxonomy of tokens, which helps us see how diversified this space is (Also see Appendix 2):

Figure 5: Taxonomy of Tokens (compiled by Autonomous NEXT)



Source: Crypto Utopia, Autonomous NEXT(2018) . Image republished with permission.

This variety, along with the supply and liquidity issues, complicates the manner in which we can evaluate tokens. There can be no one-size-fits-all evaluation methodology as seen with stocks.

As a result, investors or academics who are interested in developing a valuation methodology must realise that they need to follow a modular approach in which key variables and analysis methods need to be selected based on the kind of token or cryptocurrency they are interested in evaluating.

If we are to allow this technology and this new breed of investing model to flourish, then we have to construct a toolkit of evaluation methods, where each evaluation method allows us to evaluate certain aspects of the token sale. The evaluation model of a network token will not work for a utility token and vice versa. This is the first lesson an investor needs to digest.

The second lesson that the investor needs to learn is the kind of variables that need to be considered. While stock evaluation is largely made up of financial variables and ratios, tokens are fully digital entities that exist on a networked plane. Thus the kinds of variables that need to be analysed are not just financial but technical as well, especially when analysing smart contracts. Retrofitting stock valuation models therefore hold less gravitas as they currently do not incorporate such kinds of variables. Furthermore, when stock analysts use ratios – such as P/E, EV/EBIT, Debt/Capital, Debt/Equity, ROA, ROE, etc.. – they analyse data related to these ratios over extended periods of time. As the token space is nascent, similar ratios currently do not exist and any time-series data is over a very short time period.

As mentioned, since the variety of tokens is quite widespread, being able to evaluate the value of a security token will be different from evaluating the value of a utility token. But some attributes (such as base network value) and certain variables will be shared by all tokens which can help us create a generalised valuation method to a certain extent.

Taking these points into consideration, the remainder of this report is broken down as follows:

Part 1.3: We start with a review of the current valuation methods being developed. This provides us with an overview of what's been done and helps us ascertain the pertinence of current valuation methods and where a model makes sense.

Part 2: In this part, we will delve into more specific aspects of Token valuation and introduce the key variables to be considered when it comes to conducting fundamental and technical analysis of tokens. We will also explain what we mean by technical analysis, as our definition of technical analysis does not relate to Chartism.

Hence, the goal of this report is to provide the key tenet's of a base valuation methodology and introduce the concept of a modular token valuation approach. As the Blockchain and cryptoasset space grows, the variety and diversity of products and services will also grow, making such an evaluation model more adjustable to the upcoming changes.

Prior to delving further, it is important to highlight that fundamental analysis practices that are applied to stock analysis still apply to tokens. Reviewing the team, the experience they have, a breakdown of the product/service they are offering and studying other data points that are today considered normal practises of due diligence, are classic analysis techniques that should never be forgotten. In this vein, we start by looking at what's already been done.

1.3 REVIEW OF CURRENT TOKEN VALUATION METHODS

In mid-2017, Chris Burniske and Jack Tatar published the book, "Cryptoassets", which has been described as "The innovative investor's guide to an entirely new asset class". Apart from the evident reference to Benjamin Graham's classic book, 'The Intelligent Investor' (1949), Cryptoassets also shared a similar objective – to develop a way to evaluate the actual value of a token.

In the book, the authors shine light on some important landmarks. Firstly, they offered a classification of Cryptoassets into 3 groups – Cryptocurrencies, Crypto-Commodities and Crypto-Tokens (See Appendix 1 for more details on this classification).

Secondly, they made the first attempt to come up with a token valuation model that would allow investors to make more informed decisions when thinking about this asset class. They mention, that when examining a cryptoasset, the fundamental analysis ought to include:

- The Whitepaper
- Decentralization Edge
- Community and developers
- Relation to digital siblings
- Valuation
- Issuance model

A few technical variables were also enumerated, such as:

- Hash rates (as a sign of security)
- Number of miners
- Company support
- User adoption measured by Number of Users and Number of Transactions

Having established which variables needed to be measured to perform a cryptoasset valuation, the authors then attempted to use economic metrics such as P/E ratio, and offered takeaways from financial analysis methods such as the Discounted Cash flow method and the Velocity of circulation in order to underline the similarities between stock evaluation and token valuation.

However, at no point in the book do they offer a valuation methodology set in stone. Instead the focus is on establishing linkages between methods that are already used to evaluate assets and to highlight the new variables that we need to consider when trying to valuate cyptoassets.

The book nevertheless marked the beginning of a formal conversation on the subject of token valuation methods. Since the publishing of Burniske and Tatar's book, a slew of blogs, academic articles and reports have been published to explore this subject, many of them referring Cryptoassets and some that have been penned by the same authors. Since October 2017 an increasing number of articles on this subject have been published (Smith+Crown, 2018).

As the number of people exploring the subject continues to grow, so does the diversity of the approaches. Today, there are articles that are attempting to apply Black-Scholes Option Theory (Antos, 2018) for token pricing, and new terms such as Crypto J-Curve (Burniske C. , The Crypto J-Curve , 2017) seem to be discussion points. Each methodology has its benefits and challenges. A short review of the various methodologies helps us determine their applicability:

1.3.1 : Store of Value Methodology

One of the first valuation methods that built upon the three functions of money and stated that a token's ability to serve as a store of value can drive significant value to investors.

As per this method, cyptoassets that have steady values by design (E.g.: stable coins), or which are expected to grow in price, make for attractive "store of value" coins .

This method is thus mainly reserved to asset-backed tokens as the valuation process involves determining the total assets attached to a token and dividing it by the number of tokens.

As a result, this methodology has little else to offer and is quite simplistic. It considers that value is based on market forces and that confidence in a "stable coin" will automatically translate to a stable value.

From the current experience we have, asset-backed tokens often offer limited tangible redeeming possibilities (case in point – Venezuela's Petro). Moreover, it seems to apply only to asset backed tokens. Hence, its use is limited both in scope and technique.

However, it could be useful to analysing the value of stable coins[3] or tokens that are collateralized. This collateralization can occur in three forms:

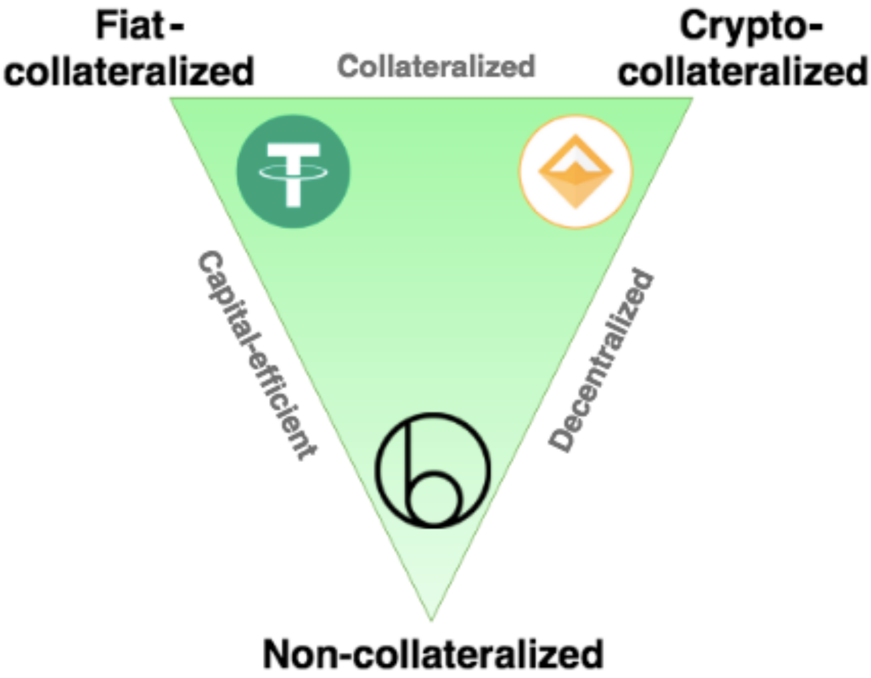
1. **Fiat-Collateralized**: A certain amount of fiat currency is deposited as a collateral and coins are issued 1:1 against this fiat money

2. **Crypto-Collateralized**: Similar to their fiat-counterparts, with the exception that the collateral is not an asset in the "real-world" but rather another cryptocurrency

3. **Non-Collateralized**: Not actually backed by anything other than the expectation that they will retain a certain value. One oft-mentioned solution to non-collateralized stablecoins is the seigniorage shares approach. This concept builds on smart contracts that algorithmically expand and contract the supply of the price-stable currency much like a central bank does with fiat currencies, but in a decentralized manner (Schor, 2018).

[3] A stablecoin is a cryptocurrency that is often pegged to a stable asset, like gold or the U.S. dollar. This gives it lower volatility and some practical usage attributes - Sherman Lee, Forbes, (March 2018). Examples– Tether, MakerDAO, Basecoin, TrueUSD, Arccy, Stably, BitShares, Sweetbridge, Havven, Augmint, Fragments, Carbon, Kowala, X8X, Globcoin, Stronghold USD, etc.

Figure 6: Value linkages for stablecoins



Source: "Stablecoins: designing a price-stable cryptocurrency", Qureshi, (2018)

1.3.2: Token Velocity Methodology

This methodology has gained a lot of ground in the discussion on evaluation methods owing to its connotations to considering a token based economy as a monetary system. As a result, its immediate application has been with general purpose cryptocurrencies which function as independent monetary bases, such as – Bitcoin, Bitcoin Cash, Zcash, Dash, Monero, Decred, etc..

Some proponents of this methodology also state that it can be used when trying to valuate native tokens of smart contract platforms such as Ethereum, EOS and Dfinity. The reasoning behind this approach is that as the native token of a smart contract platform becomes widespread and sufficiently useful, it will emerge as an independent store of value (Samani, 2018).

Drawing from The Monetary Equation of Exchange (MV=PQ), which is often referred to as The Quantity Theory of Money, this modified version looks at the token based economy as an asset that is being exchanged. The table below offers a comparison between the original version of the equation's variables and its crypto equivalent (Lannquist, 2018):

Table 2: MV=PQ in the Crypto Context

Traditional Version	Crypto Equivalent
M = Money Supply in the Economy (M1)	**M** = Size of the asset base
V = Velocity of Circulation	**V** = Velocity of the Asset
P = Price level in the economy	**P** = Price of the digital resource being provisioned
Q = Output produced by the economy	**Q** = Quantity of the digital resource being provisioned

The method states that velocity is a significant driver of token price, and the lower the velocity, the greater token price is via an appreciation of **M** (size of asset base).. The implication of this method is that tokens with low velocity, i.e. those that held (owing to speculation, asset backed, etc.), will see prices rise.

Prior to going further it would be essential to note that users of this methodology need to apply it with a large pinch of salt, for there are a number of assumptions needed to make this method work.

Firstly, it is based on having a measurable value of **M**. If this refers to a private Blockchain where all quantities held by the networks participants is declared, this might work. But the assumption of being able to calculate **M** especially. In a public Blockchain, is problematic as holders of a token can often store tokens off chain. Thus it is hard to establish the size of the asset base, especially when applying it to utility tokens that function as proprietary payment currencies such as Filecoin, Golem, Civic, Raiden, Basic Attention Token, etc.…

Secondly, and more importantly, the model is a retrofitted version of an antiquated equation. Most economist don’t even use the formula anymore as it requires too many assumptions – for example, **V** is assumed to be a constant, which is hard to calibrate within a functioning economy whose natural state is entropic rather than equilibrium. A number of empirical studies have also shown that the MV=PQ formula is not supported. Hence the formula is more of a tautology rather than a method.

Retrofitting this equation to measure the velocity of exchange of a token continues to prove problematic, as when velocity changes, the choice to record the effect in **M**, P**,** or **Q** is arbitrary and yields different implications for token price. Further, V's relationship and correlation with these factors is dynamic, and assuming a steady relationship with **P**,**Q**, or **M** is again arbitrary and problematic. Thus many many assumptions have to be made when it comes to using this equation.

It is possibly for this reason that optimal token velocity is rarely addressed in white papers. One notable exception could be the Basic Attention Token (BAT), who state the contention that **V** is going to be based on natural supply/demand dynamics between token users and hoarders such that, an optimal token velocity is ensured. If such a situation were to exist, then the MV=PQ formula could possibly be used but alongside a total addressable market (TAM) analysis[4].

1.3.3: Crypto J-Curve Methodology:

This method is a recent idea proposed by one of the authors of Cryptoassets and is an extension of the MV=PQ approach. As per this model, a token's price is based on two components whose contributions to the token's price evolve over time:

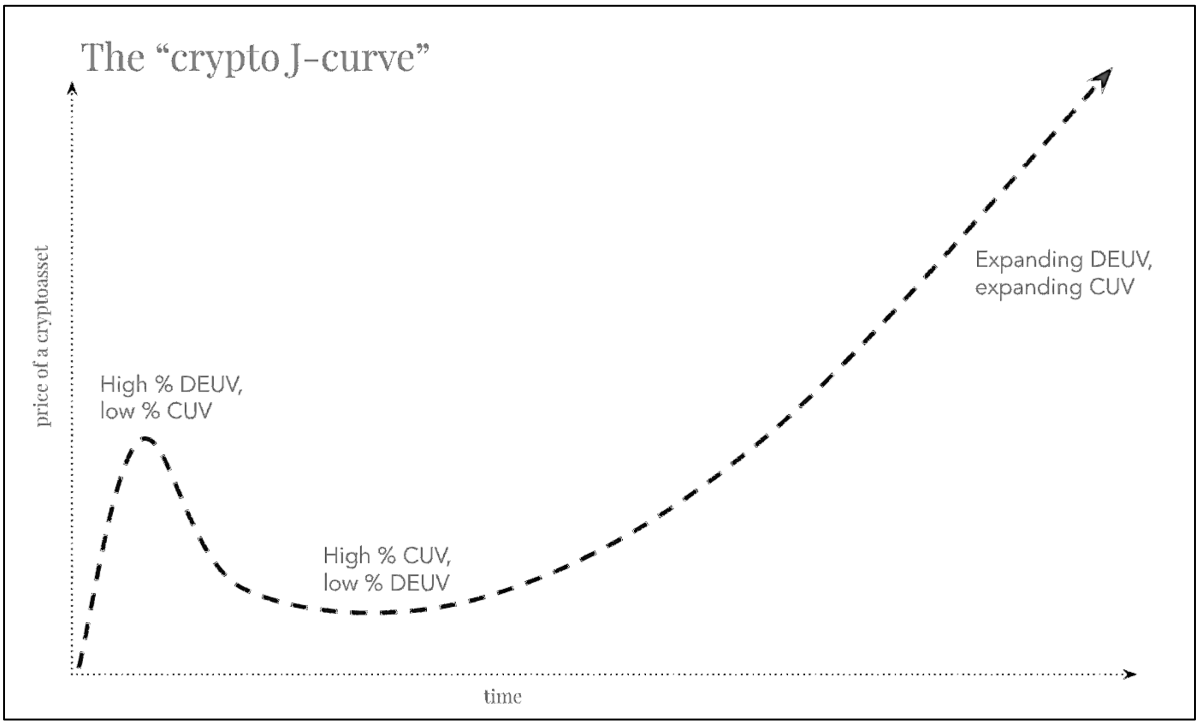
The **CUV** refers to the current utility value, which represents value driven by utility and usage today,

The **DEUV** represent the discounted expected utility value, which represents value driven by investment speculation.

The model goes on to explain the interlinking between **CUV** and **DEUV** – When a token project is launched, it starts to a develops, and as early adopters are excited about the potential, they drive up the expected value. **DEUV** thus dominates the initial growth of the project. . As enthusiasm wanes or if technical challenges are discovered, the price declines and **CUV** now begins to play a role in deterring the price. As the project matures, the token becomes more adopted and **CUV** grows. **DEUV** then catches up as speculation and excitement follow this new growth. Ultimately in the steady state, **CUV** drives token price and this evolution creates a J-Curve, which is often seen in financial valuation:

[4] TAM analysis, is done to determine the current utility value of a cryptoasset. A TAM analysis is a top-down approach which begins with the estimate of the market's total size and then ascertains what share of the market the cryptoasset network could potentially obtain. The total market price consists of current utility value and discounted future expectations of the cryptoasset network's key drivers in subsequent years.

Figure 7: The Crypto J-Curve by Chris Burniske



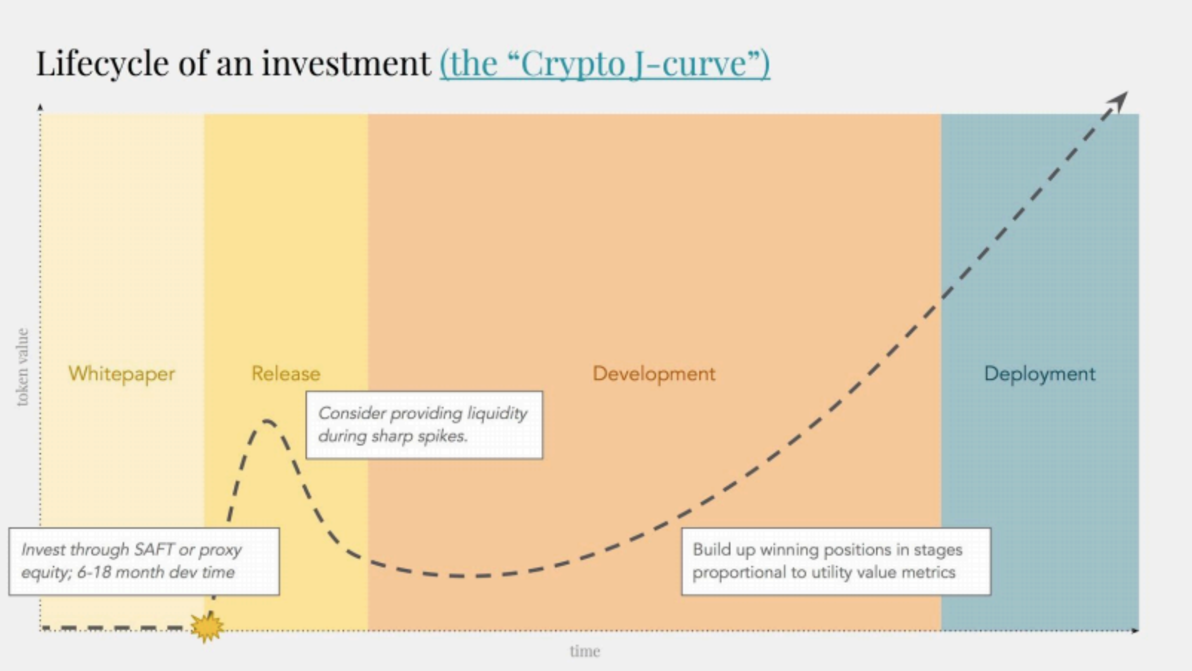
Source: The Crypto J-Curve (Burniske C. , The Crypto J-Curve , 2017)

As it can be seen, this approach also involves a number of assumptions. Firstly, **DEUV** is calculated by using a modified version of the Discounted Cash flow formula that is used to analyse stocks. Except a Token is not a stock as they usually have no assets, earnings or cash flow. Hence using an adapted version of the **NPV** (Net Present Value) or discounted cash flows has limited applicability.

Secondly, it is based on MV=PQ which as we have seen before, is based on antiquated methods and too many assumptions. As velocity is an input value, the model suffers the same drawbacks related to the token velocity model.

Some adopters of the Crypto J-curve, have begun using it as a proxy for measuring the different stages in the life of a cryptoasset. For example the New York based VC investment fund, Placeholder uses the curve as a means of determining which stage the token sale is in - The whitepaper stage is where the team works to define and implement a "minimum viable protocol," which validates the network's functionality. The release stage is when a crypto network's token is first made available to the public, and the public stage when the token begins trading on exchanges (Monegro & Burniske, 2018).

Figure 8: Applying the Crypto J-Curve to the lifetime of a token project


Lifecycle of an investment (the "Crypto J-curve")
token value
time
Whitepaper
Release
Development
Deployment
Consider providing liquidity during sharp spikes.
Invest through SAFT or proxy equity; 6-18 month dev time
Build up winning positions in stages proportional to utility value metrics

Source: Placeholder Thesis Summary, Monegro & Burniske, 2018

Hence, while Private Equity funds often use the J-Curve to calculate the period over which the return on investment starts to become profitable, the current use of the J-Curve in the context of cyptoassets is limited to ascertaining the life cycle of the products development. In such, it does not function as a valuation methodology per se.

1.3.4: Network Value-to-Transaction Ratio (NVT)

An interesting method that developed quite recently, is an adapted version of the stock valuation Price to Earnings ratio (P/E ratio).

NVT = Network value / Daily transaction volume.

This valuation ratio compares the network's value (the market cap) to the network's daily on-chain transaction volume. NVT may indicate whether a network token is under or overvalued by showing the market cap relative to the network's transaction volume, which represents the utility that users derive from the network. When the ratio becomes very high, it indicates potential token over-valuation.

The model is interesting as it the first that looks at Network attributes rather than financial models. This is an important point and something that we will be addressing in greater detail in a later part of the report when we talk about Metcalfe's Law.

Moving forward, the use of this method will require some formal definition on what constitutes a valid transaction needs to be made as in certain networks that offer staking rewards - such as Dash – would have inflated transaction activity resulting from staking. This would increase the denominator, inadvertently causing the ratio to be underestimated. However, this effect could be corrected for by subtracting staking activity from transaction volume.

One key point that needs to be considered, is the transaction volume - Transaction volumes tend to follow changes in price. The higher the price, the greater the tendency to store the token and not use them. Thus these two elements have reflexive relationship, which can be used as an adjustment factor to control price.

At this point a distinction must be made. The methods above are primarily related to the evaluation of cryptocurrencies or utility tokens. When it comes to asset-backed tokens or security tokens, the valuation models are more traditionalistic.

Security tokens, tokenized securities or investment tokens, are financial securities compliant with SEC regulations. These Gen-2 tokens can provide an array of financial rights to an investor such as equity, dividends, profit share rights, voting rights, buy-back rights, etc. Often these tokens represent a right to an underlying asset such as a pool of real estate, cash flow, or holdings in another fund and these rights are written into a smart contract (Koffman, 2018).

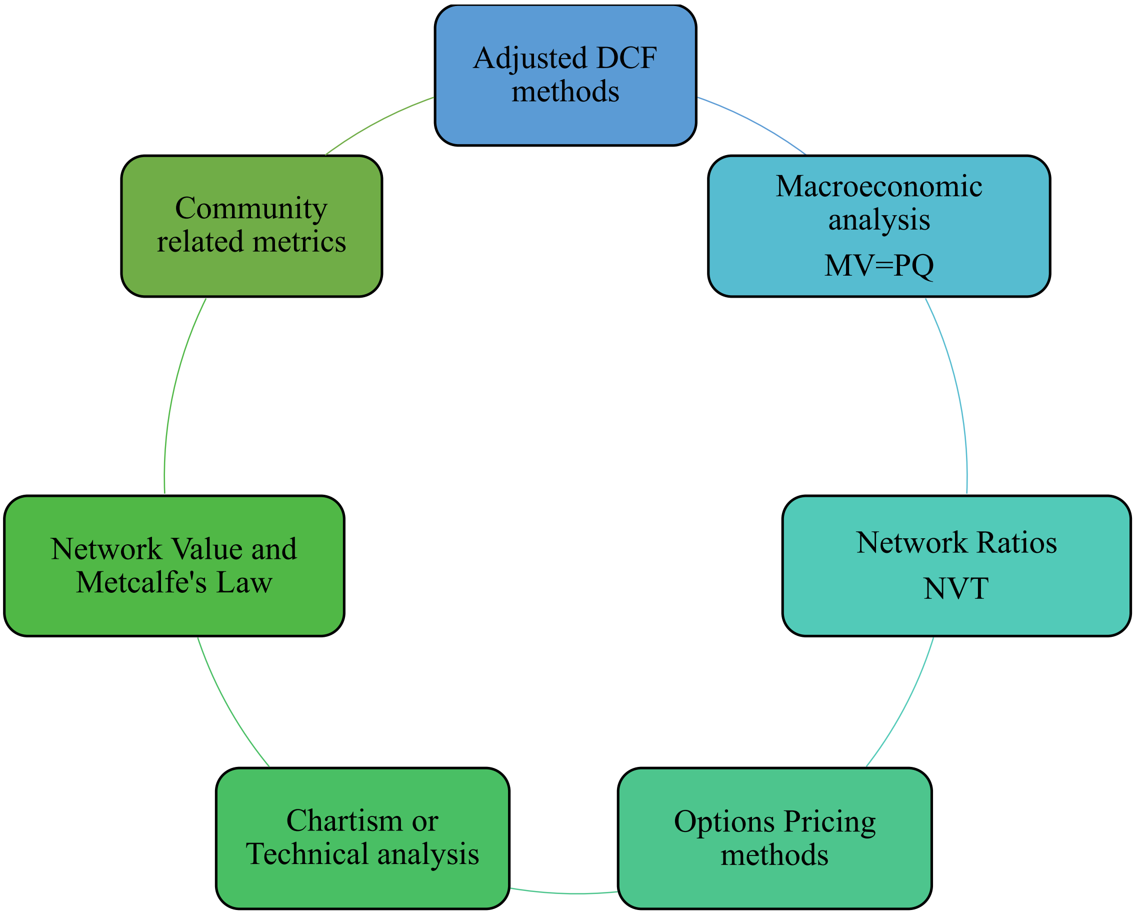
While moving securities onto a Blockchain can have advantages in comparison to a legacy system in terms of settlement times, lower fees, automated service functions and custodianship, this does not change anything about the nature of the security itself. Hence using the evaluation models of traditional securities, which are widely understood, can be applied for these kinds of tokens. Examples of security tokens include – Propertycoin, Siacoin, 22X Fund, or any of the tokens hosted on platforms like Polymath, Harbor, Securitize, SwarmFund and Templum.

Apart from the methods listed above, there have been other approaches that have tried to explore adapted models that use metrics such as EV/EBITDA, P/E, EV/Sales, Carhart four-factor CAPM model (Crypto CAPM), Sharpe’s ration and Black-Scholes Options Theory.

As mentioned in the beginning of this section of the report, it is not our intention to explore all valuation models in all their detail, especially since most of stock valuation methods are well known and well documented. The objective is to provide an overview of the methods being used today, so that the reader can select the kind of analyses they wish to perform based on the type of token or cryptoasset they are interested in analysing. .

The models presented till now do not offer us a cut and dry method to determine a token’s price. Nevertheless their contribution has been significant as they have helped us realise that a new approach needs to be developed just as Graham had created back in 1934. Moving forward, along with a modular analysis approach, we also need to be able to identify key variables that can help in the valuating the intrinsic value of a token whilst respecting their unique applications. The image below summarizes the gamut of valuation methods being used today and sets the stage for the second part of the report. Figure 9 offers us a summary of what we have discussed in this section.

Figure 9: Summary of the current models being used for token valuation


Adjusted DCF methods
Macroeconomic analysis
MV=PQ
Network Ratios
NVT
Options Pricing methods
Chartism or Technical analysis
Network Value and Metcalfe's Law
Community related metrics

PART 2: VARIABLES FOR BUILDING A TOKEN VALUATION METHODOLOGY

The role of variable selection and the associated analysis method is of key importance since tokens can function as a currency, a commodity, a security or as a mutualized asset. Owing to this multi-dimensionality, creating a universal valuation framework is complicated. However the methods mentioned in the previous part of this section can be used to evaluate certain kinds of tokenized physical assets/security tokens and utility tokens. As we have seen from the attempts of using stock evaluation models to measure token value, the fundamental and technical analysis of tokens requires that we update our jargon and kinds of variables to analyse prior to making an investment decision.

Prior to providing guidelines and variables for building a framework to measure the intrinsic value of a token, it is necessary to address the latencies of existing valuation practices. This will help us identify the variables that can aid in performing fundamental and technical analysis with regards to tokens. It also aids us in coming up with a different comprehension and definition of technical analysis in the context of this new asset class.

2.1: The issue with the current definition of Technical Analysis

Technical Analysis, which is "the art of gauging markets by looking at patterns in prices…, rather than the economic fundamentals of the investments" (Arthurs, 2018). A more formal definition of technical analysis would be the study of price and volume data to predict future direction of stocks and other financial instruments.

This branch of pattern analysis has its own jargon and a community which swears by it. Traders look at patterns in the market and make investment decisions if they see a Head and Shoulders pattern (Bearish market), a Death Cross (Very Bearish market), an Ichimoku Cloud (a Range Bound market), a Cup and Handle pattern (Bullish market) or a Vomiting Camel pattern (Bearish market).

It is important to cite these patterns used in technical analysis and question their usefulness in making investment decision methods for two reasons:

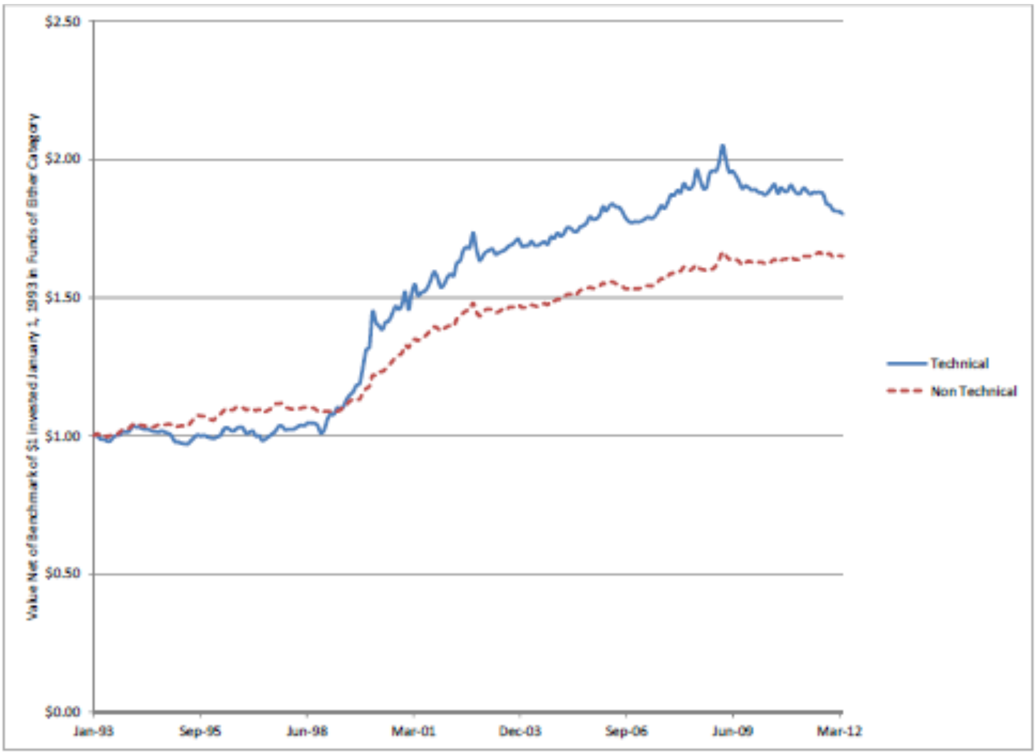
1. The methods are highly debated and there is no conclusion on their actual effectiveness – Technical analysts, also known as "Chartists", see asset prices as a function of supply and demand. Chartists believe that price patterns tend to repeat over time and, as a result, are somewhat predictable. The explanation for this belief is that repetitive behaviour of markets is the result of the irrationality of investors. This irrationality manifests itself in behavioural biases that are, in their view, exploitable.

It is this rule of thumb, that technical analysts use to "see" patterns in the market and develop a "feeling" of what is going to occur in the market. But just as correlation does not lead to causation, looking at previous self-derived patterns to predict the future seems highly questionable. For one, even if a pattern re-emerges, are all the other external, internal and associated variables the same? The market ,after all, is a constantly evolving entity. Thus seeing repetitive patterns with no understanding of the environment points to a misconception/no conception of context.

Studies on the effectiveness of stock technical analysis highlight this issue. In a paper titled, "Head and Shoulders above the Rest? The Performance of Institutional Portfolio Managers who Use Technical Analysis" (2013), researchers analysed 10,452 actively managed US equity, global equity, US balanced, and global balanced portfolios from 1993 to 2012. The authors found that 55% of those disavowing the use of charts were still in business, while only 48% of those managers who rated technical analysis as "very important" had survived (David Larrabee, 2013).

However, they went on to state that, *"Funds using technical analysis appear to have provided a meaningful advantage to their investors, albeit in an unexpected way"* (Smith et al., 2013). The following chart, from their research compares how institutional funds whose managers say they make some use of technical analysis have performed cumulatively, compared to the majority of funds whose managers say they have not:

Figure 9: Cumulative Return Net of Benchmark for Institutional Portfolios Using Technical Analysis versus Funds that do not



Source: Head and Shoulders Above the Rest? The Performance of Institutional Portfolio Managers Who Use Technical Analysis, Smith et al., (2013) What this shows is that the effectiveness of technical analysis (in its current definition) is highly questionable. There may be some forms of technical analysis that make sense, but it depends on the context and a repetition of a very similar situation. If a situation were to arise where markets have taken leave of fundamentals and entered bubble territory, there might be nothing much more to go on than chart patterns, which might at least help to capture predictable mass behaviour in extreme situations. But these events are highly contextual and cannot be generalized as sound investment decision references.

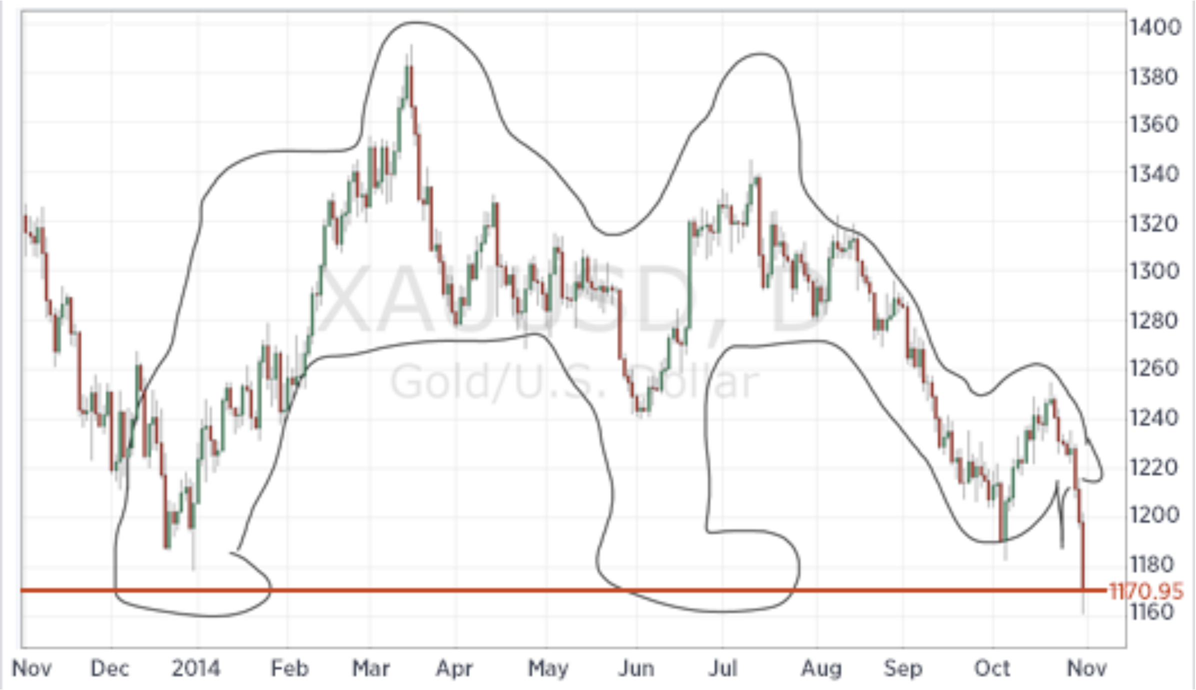
Also there is the concept of "Anchoring", as coined by Daniel Kahneman and Amos Tversky [5] . If enough people think that technical analysis matters, they will anchor on outcomes that technical analysis deems important, and in the process execute group-think actions that manifest themselves as self-fulfilling prophecies. This concept of self-fulling prophesies has been greatly analysed and explained from an anthropological perspective in the book "Stories of Capitalism", (Leins, 2018). Essentially it shows that technical analysts see what they want to see and then inform the market about their perspective. If a sizeable amount of economic agents take their opinion seriously – which is the case when the technical analyst's perspective is transmitted in the form of a widespread sell-side report – the agents make decisions aligned with this pattern and thus create the pattern. The book cites multiple examples of how and when this has occurred.

To end on this critical point regarding technical analysis, it would be useful to cite, 'The Vomiting Elephant' pattern. The creator of this pattern was Katie Martin, a Financial Times journalist who has covered global foreign exchange markets for a number of years. A few years back, she came up with the Vomiting Elephant pattern as a joke (Martin, The truth behind the vomiting camel graph , 2018). The pattern of a vomiting camel was drawn on charts and tweeted as means of providing a satirical bent on the state of markets.

Surprisingly, chartists picked up on this and began using it increasingly. Even CNBC reported in 2013 that a vomiting pattern formation had appeared in gold (CNBC, 2013). A simple online search shows how this pattern has continued to be identified and used by technical analysts ever since, even in the crypto-space.

[5] Anchoring or focalism is a cognitive bias that describes the tendency for an individual to rely too heavily on an initial piece of information offered (known as the "anchor") when making decisions. It is one of the most well tested phenomena in the world of experimental psychology. Kahneman and Tversky carried out multiple experiments, whose conclusions can be found in the book Thinking, Fast and Slow.

Figure 10: The Dreaded Vomiting Camel Pattern in Gold



Source: Brain Kelly, TradingViews.com (CNBC)

In light of these issues, it would be prudent to look at stock technical analysis methods with a large pinch of salt, especially when trying to invest in tokens. Unfortunately, as the point below shows, this is not the case.

2. They are increasingly being used by cryptocurrency or token investors – Since token sales have become mainstream, the number of exchanges that trade cryptocurrencies and tokens has exploded. A number of these exchanges provide real time data of the trading activity, which is currently being used to create charts and re-ignite Chartism. Today reports explaining how bitcoin's 'Death Cross' price pattern might be a bearish tendency (Godbole, 2018) (Pei, 2018), video's explaining the 'Ichimoku Cloud' in crypto (Olszewicz, 2016) and articles exploring 'The Vomiting Camel' pattern of bitcoin are found frequently (Martin, 2018) (Fadilpašić, 2018). If these articles and videos had remained in the purview of satire, it would not be an issue. But based on the arguments above, the fact that they are being used by traders to make buy, sell or 'hodl', decisions means that there is an urgent need to come up with a more nuanced, educated and scientifically valid definition of technical analysis for this new asset class.

2.2: Variables for Fundamental and Technical analysis of Tokens:

In light of the issues with using Technical Analysis/Chartism methods and retro-fitted stock valuation models for tokens, we propose a list of variables that investors need to analyse when making an investment decision in tokens. As of today, there is no DCF model or DDM model equivalent for token valuation. One of the objectives of our report is to therefore enumerate the main variables that future model builders need to consider when building a model. Tables 3 and 4 enumerate the fundamental and technical variables that need to be taken into consideration.

We first start by providing a list of fundamental variables. Even though token sales are relatively new, we can still borrow a few lessons from fundamental stock analysis techniques. Below is a table that explains the main fundamental variables that need to be reviewed and the purpose for doing so:

Table 3: Fundamental Variables for Token Valuation

Variable/Attribute	What to look for	How to measure it
Team	▪ Mix of tech and business expertise ▪ Technical expertise ▪ Founders and CTO's track records ▪ Experience of team and advisors in managing large scale projects or companies ▪ Team Size	▪ Track record in the community ▪ Recognized industry expertise in core team, advisors and board (if any) ▪ Proven capacity in similar projects ▪ Core Technical team members - ○ Aptitude ○ Familiarity with codebase & language ▪ Work experience of team ▪ R&D background in team ▪ Have any of the founders left the team recently?
Market	▪ Size of market (Billions USD) ▪ Competition – incumbents and Crypto ▪ Ability to create a unique presence	▪ First mover? ▪ Number of incumbents and monopolistic players ▪ Ease to enter the market based on product/service offering ▪ Strategic Partnerships ▪ Are their centralized competitors exploring a decentralized solution? If yes, how many. ▪ Attractiveness and Growth of market ▪ Sensitivity to economic cycles
Product	▪ Problem being solved/Solution being provided ▪ Feasibility of Proposition	▪ Infrastructure needed to deliver the product/service ▪ Technology Readiness level

	▪ MVP or Product Status[6] ▪ Time to achievement ▪ Presentations, videos, whitepaper, technical paper, code	▪ Complexity of product/Service ▪ Early adopters client list ▪ Shared repos on Github ▪ Presence on social media
White paper	▪ Level of detail in explaining product and objectives ▪ Technical description of what is being made	▪ Role of the token in the business model ▪ Economic and Distribution/Issuance model
Roadmap	▪ Often published in whitepaper ▪ Stages of the project ▪ Budget allocation as per stage ▪ Marketing rhetoric & associated budget – is the token being marketed as an investment with future value based on speculation?	▪ Viability of achieving the milestones in the roadmap - needs an understanding of the technical difficulties ▪ Details of access to funds (escrow) and release as per milestone achievement ▪ Transparent reporting on development of project ▪ Transparent reporting on use of finances[7] - Burn rate, costs, gain predictions ▪ Explanation for soft cap and hard cap objectives[8]
Code	▪ Is the code for the smart contracts open source? ▪ If yes, look for team contributions, community contributions and standards being respected. ▪ Vetting of code by technical experts	▪ Github trackers - Forks, watchers, stars compared to other tokens ▪ Commits unique to the project. Comparison to other similar tokens ▪ Security Audits and Bug Bounties – Bugs found, Kudos points, Accuracy of bug solutions, number of contributors, rewards as

[6] Product Status can range from – Fully working product , Beta version, Alpha version, Prototype / MVP, Demo only, Just an Idea – to Unknown.

[7] Amount being raised needs to be clearly defined and the token sale needs to end on success. Secondary funding rounds or extension of the ICO after hitting the capital target should be watched with caution as it be related to corrupt incentives.

[8] A number of Token sales will have soft and hard cap targets. Often there is no explanation why an additional amount of money is needed, if the product can be built with a lesser amount (the sift cap). Expansion into other areas, vertical or scaling might be the reasons, but the validity needs to be verified.

		per severity[9] or CVSS scores[10] ▪ Independent, 3rd party reviews of the code (normally paid for by token issuers) ▪ ICO reviews and diligence agencies reviews
Token Distribution	▪ Token Emission Rate ▪ Trading Volume ▪ Allocation to founders and advisors ▪ Sales cycle – Presale, Private Sale,, Airdrops, Token sale, etc. ▪ Lock up period and Token Generation Event (TGE)	▪ Average trading volume over 3 months compared to similar token's ▪ Average market cap over 3 months compared to similar tokens ▪ Value growth since trade start date against average total market growth
Traction	▪ Amount allocated for marketing compared to product development ▪ Marketing message – is value based on speculation? ▪ Aggressiveness of marketing – overly aggressive marketing raises red flags ▪ Bios of team on website and interaction mediums ▪ Community interaction mediums ○ Email ○ Slack/Telegram ○ Blogs and posting frequency ○ Twitter, LinkedIn, Facebook presence	▪ Community size and growth rate ▪ Reviews and comments on online platforms

[9] Bugs in code have 4 levels of severity – Critical, High, Medium, Low. Based on the severity level, rewards for finding and solving bugs will vary. Eg: Median reward for Critical bugs is $1400 (High = $500, Medium = $150, Low = $100). *Source*: *Bug Bounty Field Manual by Adam Bacchus.*

[10] CVSS = Common Vulnerability Scoring System provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

Since Token's exist on Blockchains and as Blockchains are distributed networked constructs, most of the technical variables will refer to network attributes. Once again, this is our definition of technical analysis and we do not refer to Chartism when talking about technical analysis for the reasons cited in the prior section.

The pertinence of certain technical variables will depend on the type of Blockchain being used (Public or Private - In the past year, we have seen an increasing number of Private ICOs or 'PICOs') and the type of business model and the relevant token (Utility Token, Security Token, etc.….). The table below offers a summarized collection of a few basic technical variables and lists attacks that have happened in the past that investors should verify when looking at a Token Sale. Following this list, we present a more detailed analysis of 3 technical variables – the level of decentralization, the smart contract, and the size of the network – as they are key variables that concern any type of token resulting in various methods of analysis being proposed by a variety of contributors.

Basic Technical Variables - As the crypto space becomes increasingly mature, a number of attacks have occurred in recent times with smart contracts. While the attacks have affected the reputation of the space, they also offer us guidelines on what the be vary for when looking at a Smart Contracts code. As an large number of ICO's turn out to be frauds, investors have begun asking for snippets of the code to ensure that the project is truly viable and that the previous mistakes are not being repeated. The table below lists a few of these technical waypoints:

Table 4: Technical Variables for Token Valuation

Variable/Attacks to be verified	What to look for
Basic attributes of the Codebase	▪ **Coding Language** [Eg: Solidity, LLL or Serpent (in Ethereum Blockchain), JavaScript and Python...] - Smart contracts exist primarily in Ethereum and Hyperledger Fabric environments. Using widely used programming languages for writing smart contracts has many benefits: it reduces the learning curve, attracts more developers, and enables the usage of reliable existing tools and libraries from these communities. Almost every program written in Go or node.js can be run on Hyperledger Fabric. ▪ **Code Version** - Which version of coding language is being used? For instance if the Smart Contract uses a complier version from Jan 2017, it might be prudent to understand why this has not been updated to a later version considering that more recent versions have

	identified and implemented many security fixes and improvements in the compiler[11].
Identity management system for the Token Sale	▪ Access and Control Layer ▪ Identity Layer ▪ Public/Private Keys ▪ Digital Signatures and Elliptic Curve Digital Signature Algorithm (ECDSA) While most of the variables listed above need to be verified individually, it is important to see what checks and controls have been set in place with respect to identify verification and protection (KYX/ALM). Often Token sales will involve a custodian. Ensuring that the custodian (e.g.: for KYC processes) is legitimate and follows a strict procedure is therefore necessary
Scaling factors	▪ Throughput limit ▪ Latency limit ▪ Cost per Confirmed Transaction (CPCT). ▪ Bandwidth ▪ Transaction validation These points will be further explored in later part of the report along with token supply
Compliance with ERC20 Standard (or similar standards)	Does the code implement many interfaces and contain a lot of logic that goes far beyond the ERC20 standard? If sections are not in accordance with current best practice recommendations, this should throw up warning signs. As smart contracts are still in a development phase, they should be easily understandable.
Compliance with Code Style Findings	A Smart Contracts' code should correspond (for the most part) to the recommended Code Style. If a Smart Contract contains any complex duplicate code it can lead to diverging program logic.
Presence of negated conditions	The negated conditions can cause errors if the condition is complex and must be avoided. Simplification of the code is the first step in this direction.
Use of modifiers	Modifiers are used for recurring checks and their use should be explicitly specified – For Eg: The use of modifiers

[11] Smart Contracts exist on the Ethereum ledger in a complex, hard-to-read machine language known as byte code. But they are most commonly written in an intuitive programming language called Solidity. Solidity hides from developers the internal details of the Ethereum Virtual Machine and the complex machine language that it processes. Before being uploaded to the Blockchain, a program called a "compiler" is used to translate the Solidity source code into Ethereum byte code.

	in the functions and state variables. This increases the readability of the contract and makes it more trustworthy.
Return Values of Functions	Verify that the return values of your functions are always within the range of the expected values. EG: If a function is expected to return numbers bigger than '0', it should be tested to see that if it is being forced with a '0' return, does it reject that situation or not.
Limits of the functions	If a function is returning a number, test and execute it with ▪ the biggest possible number, ▪ the smallest possible number ▪ a random value in the middle. This allows us to see how the functions will react in unexpected situations.
Format of Return Values	If a function is supposed to return an array of numbers, check if there's any case where that array returns empty. This is important because it could break the functionality of your decentralized application (Grincalaitis, The Ultimate Guide to Test Your Smart Contract , 2018).
Over and under flows	Overflow and Underflow Attacks are similar to the Y2K problem[12]. An overflow occurs when a number gets incremented above its maximum value. This can allow a an attacker to gain more tokens than they actually own or in worse cases can lead to the breakdown of the entire system. See the note in the appendix to see how this can compromise a Smart Contract.
Reentrancy Attack (Checks-Effects-Interactions Pattern)	This attack consists on recursively calling the `call.value()` method in a ERC20 token to extract the ether stored on the contract if the user is not updating the balance of the sender before sending the ether. More recently, there have been an increasing number of issues related to this kind of attack with ERC827 tokens[13].
Reordering attack	In such an attack, a miner or other party tries to "race" with a smart contract participant by inserting their own information into a list or mapping so the attacker may be lucky in getting their own information stored on the

[12] Y2K was a class of computer bugs that was threatening to cause havoc during the turn of the millennium. To keep it as simple as possible, many programs represented four-digit years with only the final two digits. So, 1998 was stored as 98 and 1999 as 99. However, this would be problematic when the year changes to 2000, since the system will save it as 00 and revert back to 1900.

[13] ERC827 tokens. is an extension of ERC20. The three functions that are new in ERC827 are: `approveAndCall(), transferAndCall(), and transferFromAndCall().`
The difference between the ERC827 functions and their ERC20 counterparts is that in addition to what they do in ERC20, they also `call_to.call(_data)` on the `_to contract` to whom the money is being sent. allowing the attacker to buy as many tokens as he wants, bypassing the individual sales cap.

	contract (Grincalaitis, The ultimate guide to audit a Smart Contract + Most dangerous attacks in Solidity , 2017).
Short address attack	If the token contract has enough quantity of tokens and the buy function doesn't check the length of the address of the sender, the Ethereum's virtual machine will just add zeroes to the transaction until the address is complete (See example in the footnote[14]). This allows an attacker to gain more tokens than they own. NOTE: This is a bug of the Ethereum virtual machine. Hence, when investing in tokens/purchasing tokens it is important to check the length of the address.
GITHUB/Etherscan related variables	▪ Experience of the contributors - It is not the number of contributions attracted or retained, but the quality of the contributions that needs to be analysed. ▪ Gross Product Pull Requests (GPPR) - The number of pull requests are being opened and merged is considered by some as a more universal health metric that can work agnostically from a project's size. GPPR is defined as the number of pull requests merged in a month. ▪ Regularity of commits and pull requests – Most token projects will involve a small group of contributors. Looking at the regality of commits and pull requests shows the lifecycle of the project. The "latest commits" can also be used as an indicator of whether a project is being actively developed. ▪ Analysis of the ecosystem – Along with the above listed GitHub variables, it is also useful to analyse how the GitHub ecosystem around the project is growing (Refer Figure 11). As the project grows and the code is reviewed, users will be attracted and retained if there is sufficient confidence in. the project. High attraction and low retention rates signal weakness. Most visitors who have confidence, and capability, will also become commentators and might even become part of the project. Analysing this flow and seeing how the token issuers deal with the inflow of comments and issues

[14] A user creates an Ethereum wallet with a trailing 0,

Eg: `0xiofa8d97756as7df5sd8f75g8675ds8gsdg0`

He/she then buys tokens by removing the last zero and affecting the command:

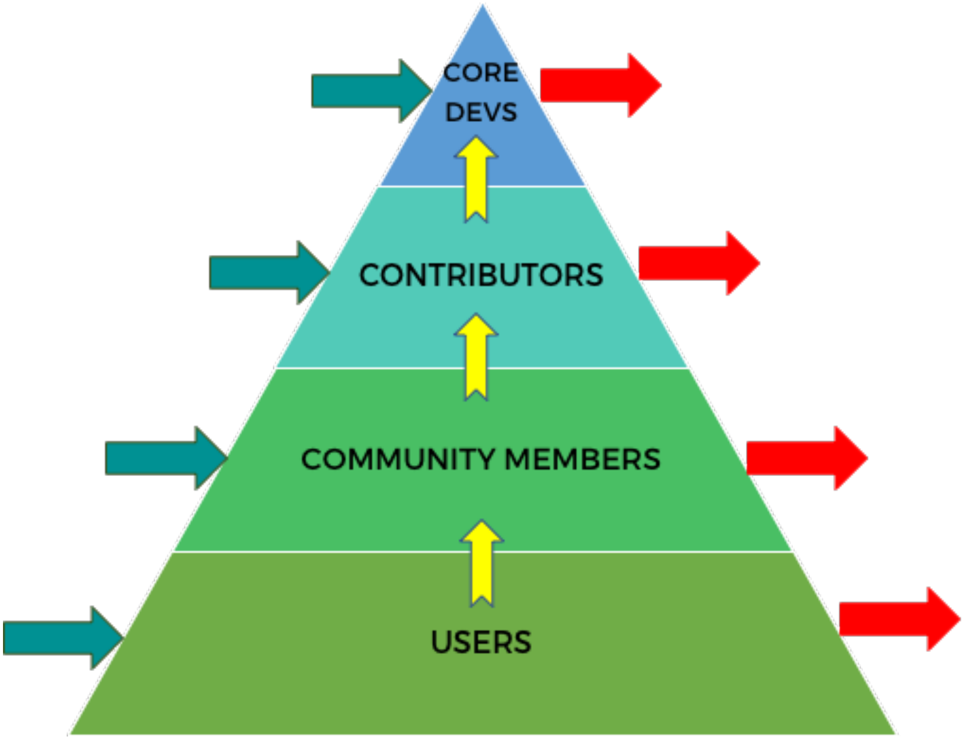
```
Buy 1000 tokens from account 0xiofa8d97756as7df5sd8f75g8675ds8gsdg
```

The virtual machine will return 256000 for each 1000 tokens bought. This is a bug of the virtual machine that's yet not fixed so when investing in tokens/purchasing tokens it is important to check the length of the address.

	identified by observers over the time period prior to the token's launch another variable to worth observing.

Figure 11: Schematic of Interactions in an Open Source Ecosystem

NOTE: Green arrows represent individuals joining the ecosystem while Red arrows represent individuals leaving the ecosystem.



Source: Modelling Open Source Software Communities. Also refer "Methodologies for measuring project health" (Eghbal, 2018)

2.3: Detailed analysis of specific technical variables

2.3.1 Smart Contracts – Code quality and governance of Token Supply:

The underpinning mechanism behind any Token Sale is the Smart Contract. Smart contracts are self-executing programs that run on Blockchains and accept digital signatures to record the agreement between stakeholders. They work on the basis of the IFTTT logic – aka: the IF-THIS-THEN-THAT logic. During the Token Sale, the supply of the Tokens, the exchange of the Tokens, the governance of the token in circulation and the actual functionality of the Cryptoassets they deliver is managed by the Smart Contract.

Smart contracts are generally touted as the means to execute programs securely that suffer from counterparty risks. The popular quote is "Code is Law" (Lessing, 2000) , which alludes to the concept that because something coded, and as it has a veneer of legality (steaming from the word "contract"), a smart contract operates under a fire-and-forget model.

But this definition is an overstatement which was best exemplified by the DAO hack in 2016. It is important to state this critical opinion about Smart Contracts for two reasons –

Firstly, Smart Contracts are neither Contracts in the actual sense and their "smartness" is debatable.

Secondly, since these contracts manage the supply and governance of the tokens, a gap between what the Token Sale promises and what their code delivers significantly impacts the investment decision.

There is nothing specific that smart contracts bring to Blockchains. Rather it is the opposite — Blockchains provide objective code execution infrastructures as code is executed in Blockchains only if it is approved by a majority of computing nodes that it follows the protocol (*Refer the note "Anatomy of a Smart Contract" in Appendix 3 to understand the key components of a smart contract and the link between a Blockchain and the different elements of a smart contract*).

This ensures that none less than the majority of computing members own or control the execution of a code running on it. Neither the developers of the contract codebase nor the parties of the contract (buyers and sellers) will be able to influence the contract execution to their advantage (Das Gupta, 2018)

To say that smart contracts introduce self-executing programs to Blockchains is therefore false, as the opposite is the truth. At best, Smart Contracts can be defined as bits of code that interact with the underlying Blockchain ledger to govern the transmission of Cryptoassets between counterparties. Calling them contracts can even be considered misleading.

The table below showcases our current misconceptions about Smart Contracts and sets the stage for the next level of analysis with regards to these automated control mechanisms.

Table 5: Smart Contracts - Key Misconceptions

Aspect	Confusion	Reason for it	Clarity
Self-executing programs	Smart contracts introduce self-executing programs to blockchains.	Neither the developers of a smart contract codebase nor the parties of the contract are able to influence the contract execution to their advantage.	Blockchains are fundamentally infrastructures to execute code objectivity, something that is leveraged by smart contracts; you don't need a smart contract for this, bitcoin scripts can do this as well

The Inevitability of Human Intervention	Human intervention only to fix bugs in smart contract code	Code written clearly can accurately reflect the contractual terms	Even without bugs, the intentions behind a code is interpreted differently by different people, requiring humans to clarify whether the execution is acceptable
Humans over Machine	Smart contracts over-value mechanistic execution and under-appreciate human creativity and change.	Remove the inconsistencies of human control so machines can run predictably	Humans will always prevail over machines as the later execute at the command of humans, and not for themselves. Predictability ≠ Perfection
Law over Code	Code is Law	Code is blind, so is Law	Code is like the codified laws of physics, not the laws of contracts

Source: Smart Contracts: Fulfilling Nakamoto's Dreams (Das Gupta, 2018). Table republished with permission from the author.

From a valuation context, Smart Contracts need to be verified at two levels – First, at the level of the quality of code to verify the integrity and security of the smart contract; and Second, in terms of how they are managing the supply and exchange of tokens during the lifecycle of a token sale. The following two sub-sections explore these attributes in more detail.

2.3.1.1: Key Variables for Integrity and Security of Smart Contracts

▪**Contract Integrity**

Regarding contract integrity, a key factor is unrestricted upgradability: If present, contracts can be upgraded in arbitrary ways and hence no assurance can be given to a user what code will actually be executed when a transaction is sent. Unrestricted upgradability violates contract integrity, which is a key feature of smart contract.

If contract upgradability is required a design has to be chosen which preserves some trust and security guarantees.

- **Data Integrity & Contract Security**

General concerns for data integrity and contract security are:

- Incorrect Authorization
- Missing Authentication
- Insufficient Numerical Precision
- Undesirable Transaction Orders
- Inconsistent Contract States during control flow transfers

Table 6 enumerates the possible issues regarding data integrity and contract security in greater detail:

Table 6: Smart Contracts - Data Integrity & Contract Security variables

Variable	What to look for?
Transaction Order Affects Execution of Ether Transfer	Ether transfers whose execution can be manipulated by other transactions must be inspected for unintended behavior.
Transaction Order Affects Ether Receiver	The receiver of ether transfers must not be influenced by other transactions.
Transaction Order Affects Ether Amount	The amount of ether transferred must not be influenced by other transactions.
Gas-dependent Reentrancy	Calls into external contracts that receive all remaining gas must not be followed by writes to storage.
Reentrancy with constant gas	Ether transfers (such as send/transfer) must not be followed by writes to storage.
Unrestricted write to storage	Contract fields that can be modified by any user must be inspected.
Unused write to storage	Writes to storage should be used by the contract, otherwise they are unnecessary.
Unhandled Exception	The return value of statements that may return error values must be explicitly checked.
Division Before Multiplication	The use of division before multiplication may result in incorrect final results due to integer rounding.
Division influences Transfer Amount	The use of division to calculate the amount of transferred ether may be incorrect due to integer rounding.

Unrestricted `Selfdestruct`	The execution of `selfdestruct` statements, which remove the associated contract from the blockchain, must be restricted to an authorized set of users.
Missing Input Validation	Method arguments must be sanitized before they are used in computations.
Use Of Origin	The origin statement must not be used for authorization.
Unrestricted ether flow	The execution of ether flows should be restricted to an authorized set of users.
Locked Ether	Contracts that may receive ether must also allow users to extract the deposited ether from the contract.
Unsafe Call to Untrusted Contract	The target of a call instruction can be manipulated by an attacker.
Unsafe Dependence On Block Information	Security-sensitive operations must not depend on block information.
Unsafe Dependence On Block Gas	Security-sensitive operations must not depend on gas-related information.
`Delegatecall` dependent on User Input	The target and arguments provided to `delegatecall` must be sanitized.

Understanding the nuances and limitations of smart contracts from a technical perspective sets the stage for the determining if the smart contract is capable of governing an ICO and is key to asking the following evaluation related questions (Cohney egt al., 2018):

1. Does the Whitepaper state any restrictions on the supply of tokens and are these restriction encoded in the smart contract?
2. Is there a vesting or lock-up plan for insiders and are there restrictions to transferring the tokens related to this plan? If yes, have these restrictions being encoded into the smart contract?
3. Did the token issuers retain the power to modify the smart-contract code governing the tokens they sold, and if so, did they disclose that that power?

Understanding the supply dynamics is of key importance for token valuation. If stock prices reflect (approximately) the net present value of the expected future cash flows, then a token's price should reflect an equilibrium between token demand (driven by the present value of expected future exchange options within the token's native ecosystem) and token supply (driven by the token's monetary policy) . Moreover, this blatant belief in "code is law" hinges on the belief that the way the Smart Contract (the governing structure in a Token Sale) is coded will ensure Trustless Trust.

However as we have seen, the current situation regarding trustless trust in Smart Contracts is far from optimal. Furthermore, a review of the 50 top grossing ICO's revealed that a significant fraction of issuers retained centralized control… "and did not disclose code that permitted the modification of the entities governing structures" (Cohney egt al., 2018). And while many think of Ethereum contracts as fully decentralized, nearly half of the top 20 projects[15] can have their token transfers completely frozen by an owner (a single key or a multisig contract) (Que, 2018) . This process known as Pausing can be valuable for future upgrades, swaps, and disaster mitigation. But it also leads to new risks:

- **Trust**: It requires all users to trust the party in charge of the key, reducing the degree of decentralization in the contract. We will cover how to measure level of decentralization in the next specific technical variable.
- **Security risk:** It requires the key holder(s) to secure the private key. An attacker (i.e., a disgruntled employee - A number of Token hacks turn out to be inside jobs) could hold the network hostage and demand a ransom by freezing transfers, or short the token which is sure to drop in value.

This tendency of not disclosing in plain terms that the issuers of the token sale have the power to modify the token rights is probably one of the biggest limitations with smart contract based token sales. As of the time of publishing this report, it can be stated that ICO code and ICO contracts rarely match . In a report titled, 'Coin-Operated Capitalism', researchers from the University of Pennsylvania explored this discrepancy was found that many ICO's failed even to promise that they would protect investors against insider self-dealing and fewer manifested such contracts in code. The text below summarizes some of their findings with regards to token supply and code in smart contracts (Refer "Anatomy of a Smart Contract" in Appendix 3 in case you wish to familiarize yourself with some of the basic functions of smart contracts).

The researchers obtained a copy of the Solidity code from etherscan.io [16] or GitHub for the fifty top grossing ICOs. Each function of the smart contract was manually tracked to see how each line modified the meaning of, or data stored in, the smart contract

- **With regards to Minting**

[15] These include: EOS, Tron, Icon, OmiseGo, Augur, Status, Aelf, and Qash

[16] Etherscan.io replicates the byte code present on the blockchain, but requires developers to upload Solidity source code for display

- Unlike mining, where contributors need to work to earn cryptoassets, minting is a process in which tokens are issued in exchange for another cryptoasset.

- The tokens can be allocated to investors in exchange for fiat or cryptocurrency via a private sale. In such a sales process, the supply quantity of tokens is decided at the start of the project and investors have a fixed quantity of tokens that they can acquire.

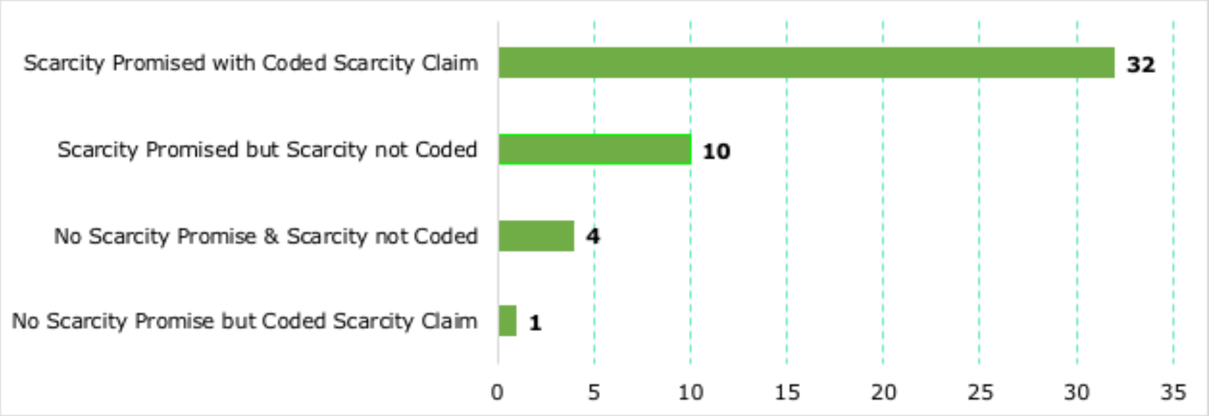
- Another model involves the issuance of tokens to the general public via mass offerings until a predefined target is met. When that target is reached, the sale stops.

- We also have a combination of private sale and mass offering. Based on the issuing phases – private presale followed by mass offering – a cap is set that limits how much can be sold during each phase and these limits are hardcoded in the smart contract. The sales process is thus automatically executed by the Smart Contract, with the full supply being decided at the offset or depend on how much investment the project receives.

- However these limits can be modified by the owner of the smart contract which poses a threat to investors. If there is no set limit, which is encoded, token issuers can mint a private stash for themselves or inflate or deflate the circulating float of tokens. The encoded supply restrictions are therefore critical to investors.

- The report from the researchers found that 90% [17] of the top projects had stated supply restrictions in their documents and 75% had coded it. The graph below summarizes their results:

Figure 12: Smart Contracts with encoded supply limits (47 of top 50 ICOs)



Data source: Coin Operated Capitalism, Cohney et al., (2018)

- **With regards to Decreasing Supply or 'Burning' –**

[17] Of the 50 projects analysed, 3 projects expressed their code in byte code. Hence 47 projects were auditable and the percentage values represents these 47 projects. Hence 90% = 42/47 and 75% = 32/42.

- Not all cryptoassets exist in a state of continuous circulation (e.g.: Bitcoin/Ether).

- They can also be 'burned' or destroyed as they are used up. For example - a token can be used to access a right in a completed project at a future date (utility token).

- When this occurs, the token would be burned and this changes the amount of tokens in circulation, which effects its price.

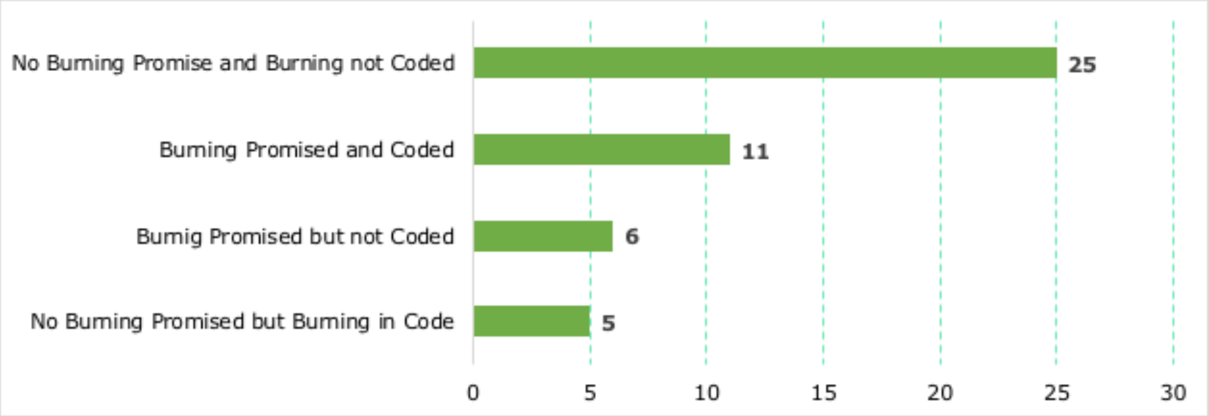
- Some projects also describe plans to perform token buy backs from holders to burn them and appreciate the price of the token. Others do the same thing by promising to burn unsold tokens from the private presale or public sale.

- Finally, some projects (such as Paragon) describe a complicated transaction fee structure, where half of the transaction fee (in this case $0.000000005) is burned and the rest is used to replenish the token reserve

- In spite of the importance of this function in the supply of the tokens, the researchers found that 35% (of the 47 reviewed) had not hardcoded the burning process in their smart contracts. Even some that did, had done so with errors which could cause the eventual demise of the network[18].

  Figure 12 summarises their results:

Figure 12: Smart Contracts with encoded Burning rules (47 of top 50 ICOs)



Data source: Coin Operated Capitalism, Cohney et al., (2018)

- **With regards to Vesting**

  - Vesting is a common investing practise of providing key

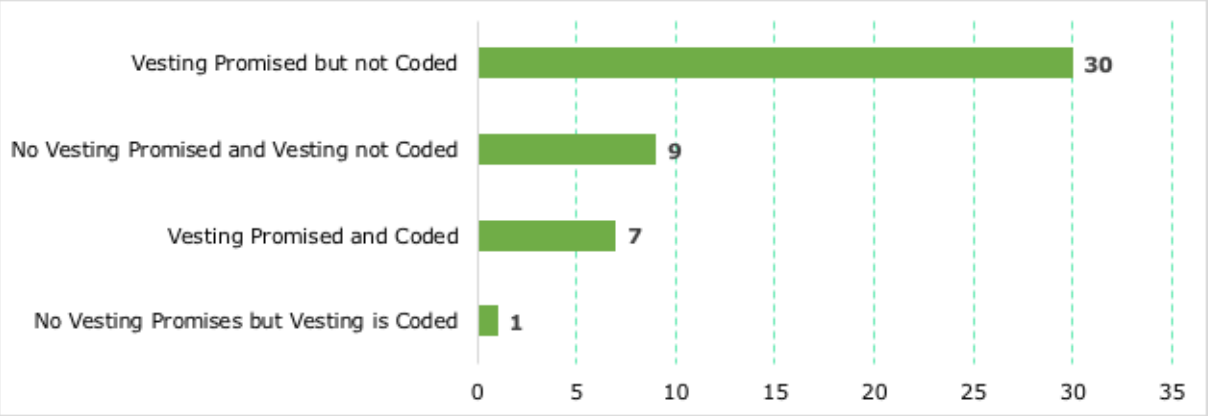
[18] Reference made here to Paragon's PRG token. The researchers found that when they modelled the transaction fee system, each transfer of a PRG token consumed approximately one-six billionth of the total supply in transfer fees, half of which was paid to the token issuers and half of which was burned. After a sufficient number of transactions the fee approached the number of tokens remaining in the supply, causing the eventual demise of the network

members of the entrepreneurial team with equity options/shares in future profits in order to counteract against desertion. It acts as an incentive structure to act against 'founder dumps' and the threat of desertion.

- As with supply promises and burning, vesting promises are detailed in the whitepaper and ought to be encoded in the smart contract. However, this can also be governed offline and enforced using traditional tools like corporate charters and bylaws.

- The researchers found that only 37 of the 47 audited projects promised vesting in their whitepapers and 31 of these 37 did not even code those vesting rules into their tokens. Figure 13 summaries their results:

Figure 13: Smart Contracts with encoded Vesting rules (47 of top 50 ICOs)



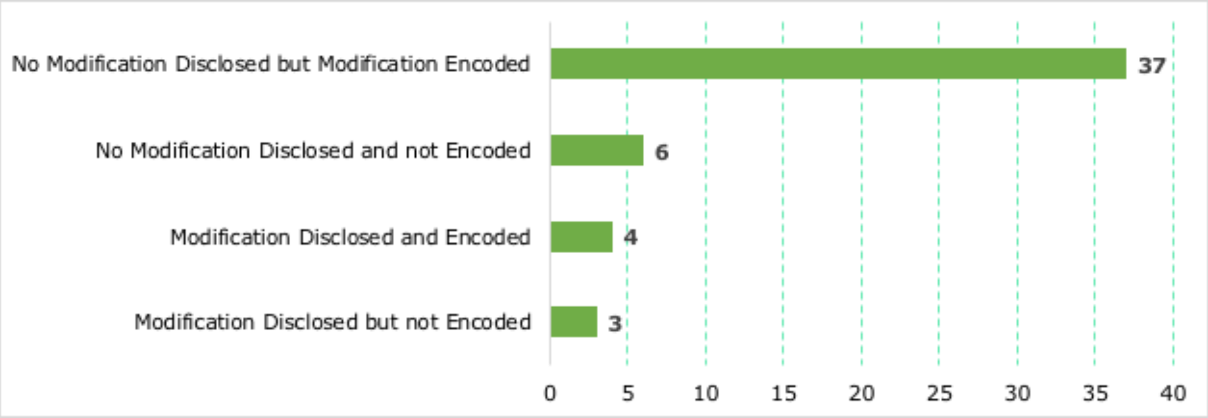
Data source: Coin Operated Capitalism, Cohney et al., (2018)

- **With regards to Modifiability**

  - Modifiability is a relatively new phenomenon in ICOs. It essentially involves the ability to change the code regarding certain aspects of the token in order to provide new features to the token holders. Essentially an upgrade.

  - Modification changes normally occur through a voting system – changes are proposed, token holders vote within a given time frame and then the changes are executed. As the function and rights of the token holders can be significantly impacted by this (especially for utility tokens), it is a key component for investors which should bear heavy when investing a token with set functionalities. Nevertheless the researchers found that only 10 of the 50 ICO's reviewed allowed modifiability in their code. Only 7 of these discussed modifiability in their whitepapers and out of these 7, only 4 had hardcoded these rules. Figure 14 summarises their results:

Figure 14: Smart Contracts with encoded Modifiability rules (47 of top 50 ICOs)



Data source: Coin Operated Capitalism, Cohney et al., (2018)

Just as paper contracts, smart contracts reflect the institutions within which they are produced. The researchers found that "there are systemic differences between code and contract, even within projects that have attracted significant investments".

While reviewing code can be a roadblock for non-technical investors, it is important to ensure that the smart contracts are feasible and whether all transaction arguments detailed meet their desired preconditions. Aspects regarding the Token and Crowdsale Lifecycle need to reviewed thoroughly in whitepapers and in code, to ensure investors know what they are getting into.

Some solutions to this problem are being provided by firms such as ChainSecurity who provide automated audits of the smart contract code. Token reviews from 3rd party providers need to be considered with care as some rating platforms operate on a pay-to-play model (as seen with the rating platform ICO Bench (Devoe, 2018)).

2.3.2: Level of Decentralization

The level of decentralization of a project is dependent on the nature (Private or Public Blockchain) of the project. If the project is on a public Blockchain and is more aligned to the open source principles, then a higher level of decentralization would be appreciated. However if the project involves a private Blockchain or a consensus mechanism in which only certain parties have the authority to verify and validate transactions – E.g.: Proof of Authority[19] – then a lower level of decentralization might make more sense.

[19] Proof of Authority (PoA) is a form of Proof of Stake, in which a set of certain "authority"nodes are explicitly allowed to create new blocks and secure the Blockchain. In PoA, a validator is not required to hold a stake in the network. He or she is required, however, to have a known and verified identity. By staking this identity to secure the network in exchange for the block rewards, a validator is dis-incentivized to act maliciously or to collude with other validators. The advantage of using PoA is very high transaction rates

Understanding the level of decentralization is important as it plays a key role in the governance structure of decentralized projects, as it shows the fragmentation of control. In the context of token evaluation, knowing the level of decentralization is useful in analysing the developer community, or the client base, or even exchange decentralization to see how and where the token is being traded. Thus measuring decentralization helps us see the size of participants in relation to the ecosystem and reflects the competition among them.

However, measuring decentralization is easier said than done. While, some significant advancements have been made by a few researchers (notably Gencer et al, (2018) and Srinivasan, (2017)), they have been done in the context of cryptocurrencies and not necessarily for tokens. But the same variables that are used to measure the decentralization of cryptocurrencies (Provisioned Bandwidth, Network Structure, Distribution of Mining Power, Mining Power Utilization) cannot be used for evaluation of tokens as most tokens run on top of an existing Blockchain (e.g.: Ethereum and ERC20 type tokens). It could be useful to know the level of decentralization of the Blockchain being used. But the same variables cannot be used to evaluate the level of decentralization concerning the token.

Hence, when looking at a token project knowing how distributed the developer community is, the spread of the client base and the variety of exchanges it is being traded on, can aid in providing some conception of the diversity of the project. Measuring the decentralization of such market-based variables can be addressed using 2 methods:

i. **The Herfindahl Score or the Herfindahl–Hirschman Index:** The HHI is a metric used to measure competition and market concentration. It is calculated by taking the percent market share of each entity, squaring it, and summing the squares before multiplying by 10,000. HHI scores less than 1,500 qualify as competitive, 1500-2000 is moderately concentrated, and greater than 2500 is highly concentrated

ii. **The minimum Nakamoto coefficient :**

In mid – 2017, an article titled Quantifying Decentralization was published that proposed a new coefficient for measuring decentralization in crypto networks. Inspired by income distribution and economic inequality measuring methods, the authors used the Lorenz Curve and the Gini Coefficient to come up with a cumulative scoring methodology.

First, a crypto economic network was broken down into its independent subsystem components [Mining (measured by reward), Client developer (measured by codebase and commits), Exchanges (measured by Volume), Nodes (measured by Country), Ownership measured by Addresses)] and a Gini score was given to each component to measure their level of decentralisation. The cumulative score of all components thus gives a 'Maximum Gini coefficient".

The Nakamoto coefficient then acts as a comparative score. It measures the minimum number of entities in a given subsystem required to get to 51% of the total capacity. Aggregating this measure by taking the minimum of the minimum across subsystems provides the "minimum Nakamoto coefficient", which is the number of entities needed to compromise in order to compromise the system as a whole.

Both decentralization measuring techniques are limited in usefulness but nevertheless can act as guidelines when trying to assess the level of fragmentation in decentralized projects.

2.3.3 Network Size:

Our final technical variable is the size of the network. The reason for paying special emphasis on this variable stems from the fact that there exists a large amount of empirical evidence that establishes the relationship between Network size and Network Value (Metcalfe, 2013) (Zhang et al., 2015). This is especially pertinent for Utility tokens which make up a significant portion of ICOs.

While the previous attempts at valuing utility tokens have made important contribution to this new asset class, more focus needs to be given to the activity of the network, represented by the velocity of token's exchange.

Like a physical coin, a cryptoasset is scarce, and its ownership is transmittable. But while physical coins are transmitted from hand-to-hand (or hand-to machine), changes in control of cryptoassets occur through the networks that host them.

Cryptoassets with a utility function therefore resemble micro-economies, as the token can be seen as another currency used in the economy that specializes in the exchange of a particular service. Token sales thus enable the creation of private transactional economies (Mougayar, 2017) and as stated by Primoz Kordez, co-founder of D2 Capital,

"This turns classic enterprise valuation upside down, since we don't value cash flow to investors but use of the token by consumers. In token evaluation, we want to measure how large and active the exchange of service is, reflected in the aggregate value of transactions (can be in $ terms) and the number of transactions of each token represented by its velocity…."….Thus, when valuating utility tokens, we should value the network and "account for the velocity of tokens. The more tokens circulate between users, the more interactions, the more network effect and healthier network". (Kordez, 2017)

When considering the sensible statement above, it is important to remember that while a number of utility token ICOs have been funded, the actual product or service that is being provided will only be available at a future date. Hence measuring the token velocity in the context of usage of the associated product or service, will only be truly measurable and representative of its usefulness when they are operational and the token is being used to facilitate the underlying business model. Currently, the token velocity being measured is based on future speculations of expected utility.

Hence, when a token-based product or service will be launched, then the velocity of this token's exchange will provide us with a way of estimating it usage and value to the end-user. When this occurs, we would estimate the value of the token, based on the estimation of the value of the service. The latter has value only if made accessible. Thus, connections are paramount for making this estimation as tokens are network native entities. If each participant using the service can also offer it to others, its value will be tightly linked to the number of participants and their interactions.

Using this approach, one could model the value of a token in the following way:

(The value of the service) * (The accessibility of the service)

where accessibility is a function of the network of participants in the blockchain.

Thus, valuating a token based on its velocity requires us to evaluate the network and the service being provided. There are various methods that are currently used for valuating services. To conclude our explanation regarding this technical variable, we offer some insight on estimating the value of a network.

Network Valuation:

A network is a connected graph with nodes linked to others via the network. If a network were to be completely linked, such that each node is connected directly to all others, as per Metcalfe's Law, for **N** nodes, there would be **N(N+1)/2** links.

Nevertheless, in any network, all links do not share equal importance. Therefore, to take this into account we would need to give each connection a weight to reflect its importance.

For instance, a fully connected network would have **N(N+1)/2** links of equal importance, in a hierarchical network where each node is connected to all others but with an importance ranking from the most valuable to the least, weighting the links by their inverse rank would yield an average number of connection of **log(N)** for each node and therefore **Nlog(N**) connections in total. The latter representation of a network is often referred as the Zipf's law.

Both these network models are extreme scenarios. If we are to adhere to Metcalfe's Law, each new participant in the network instantly connects with all other nodes. If we are to adhere to Zipf's law, the average number of connections per node grows logarithmically, which means that the increase in connectivity for an additional participant in the network is the least positive one.

Depending on the maturity of the network, its average number of connections per node can thus be modelized as a function of the number of participants as $\boldsymbol{N^a}$ where the scale factor $\boldsymbol{a}$ would lie between 0 and 1. The total number of connections in the Network will therefore be of the order $\boldsymbol{1+a : N^{1+a}}$.

Hence, estimating the connectivity of the network would come down to estimating the exponent of the average network connections, N^{1+a}, to match the market capitalization evolution (using transactions a proxy) to a function of the number of market participants (i.e. the N nodes).

NOTE: A few papers published in 2017 (e.g.: See Alabi, 2017) have analysed historical BTC data to come up with an exponent estimation of approximately $N^{1.5}$. However, these results are pertinent to cryptocurrency networks and the same estimations cannot be transposed to tokens owing to their multi-functionality. We conclude by stating that while these methods offer insight, without empirical data, it would be hard to come up with an token value estimation model based on this approach.

CONCLUSION

As we have seen in this report, the current situation regarding token valuation models is a situation that is clearly in need of greater study and testing. Moving forward we see three topics that need to be explored.

First, there is the subject of the adoption curve. While the promises and ideas stated in whitepapers are ambitious and pioneering in some cases, history has shown us that building an innovative new product or service that resolves a problem does not always translate to large scale adoption. Indeed, even applications such as WhatsApp, Facebook and Telegram had to wait for three years on average to achieve their mass adoption hockey stick curves, in spite of the fact that consumers were used to mobile texting for many years. Most ICO projects are still in the phase of development. Once these decentralized products and services are made available, the furnishers of the company behind the project will have to deal with switching costs, customer feedback loops and other such factors that will determine their success and give us a true gauge of the potential behind these innovative solutions being provided. As this process occurs, there will some variables that hold more gravitas compared to others and it is only by continuously analysing this evolution that model makers will be able to determine what needs to be considered, and to what extent, when building a token valuation methodology.

Secondly, as tokens function on blockchains which can be used as value exchange mechanisms, they can act as accounting units in the creation of economic systems. As we have seen, the supply of tokens and the governance of their circulation is a key element when evaluating a project. Thus moving forward, advances from endogenous monetary systems need to be integrated into token valuation models to respect their fundamental nature. Insights from monetary theory and monetary and fiscal policy should play an increasingly important role in the token valuation methods of the future.

Lastly, the variety of tokens and their multi-functionality needs to be given more importance. As every token project is different, valuators need to develop a modular approach in which they build models based on the type of project, the function of the token and how this relates to its supply dynamics. There is no one size fits all model for token valuation. Based on the type of token being analysed, model builders will need to select the most pertinent variables and create models that respect the nature of the project.

As we have seen, the current practise of retrofitting stock valuation methods has limited applicability. It has been our attempt to go back to the basics and start the conversation on token valuation with a fresh lens by focusing on the variables of analysis. We are certain that moving forward, this list of variables will grow owing to the complex nature of this technology and this new investment vehicle.

Appendix 1

Taxonomy of Tokens

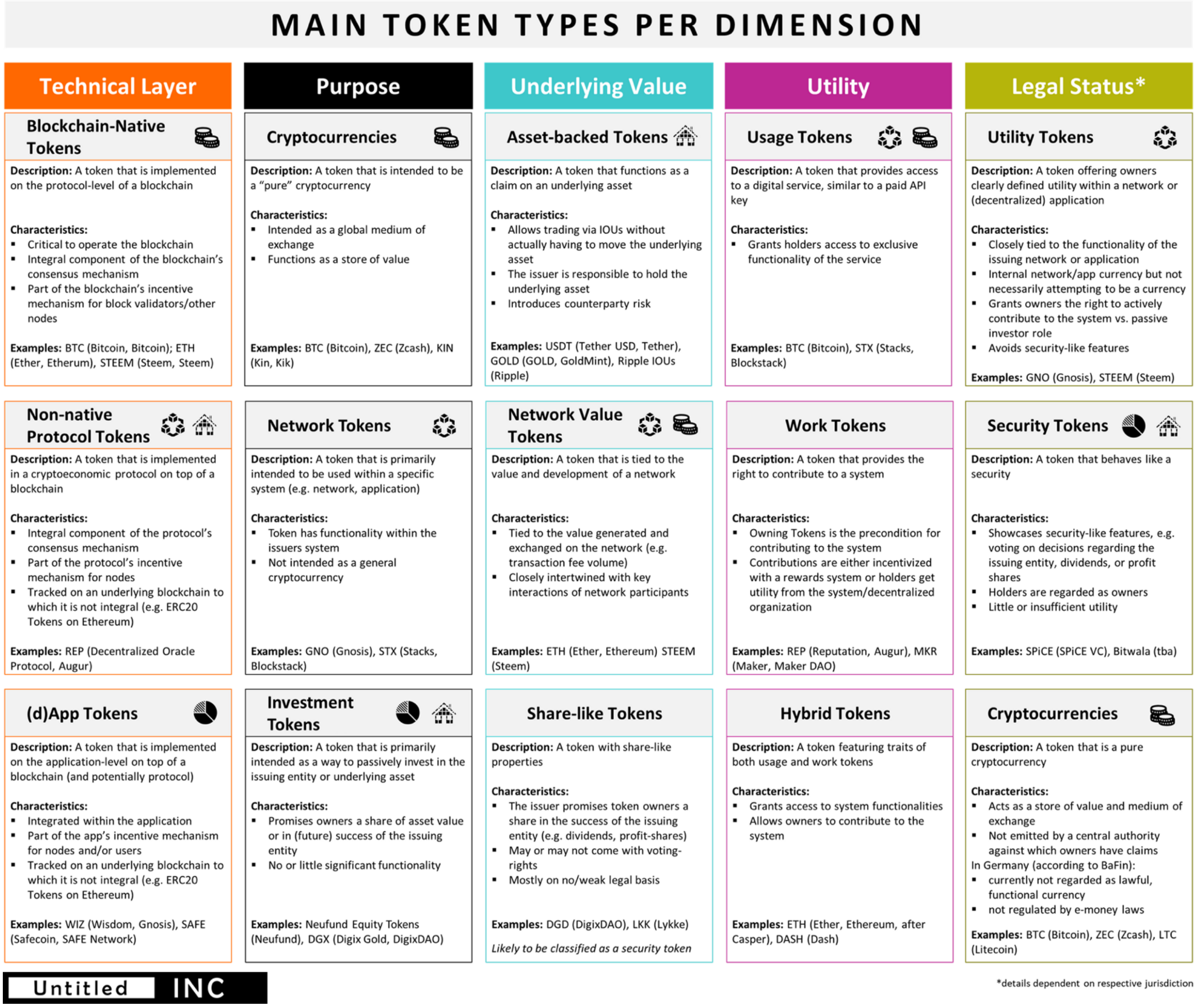
Source – Cryptoassets by C. Burniske and Tatar (2017)

1. Crypto – currencies:
    - Perform the 3 functions of money
    - Is network specific and can be forked
    - Differences in supply schedules, Proofs (Work, Stake, Existence, Elapsed Time, Process, etc…)
    - Public or Private == Traded on exchanges
    - Examples – Bitcoin, Ripple, Dash, Ether, Monero, ZCash, etc…

2. Crypto – Commodities:
    - Represent digital commodities used to make digital goods & products.
    - The main digital goods and services that are considered crypto-commodities include – Computing Power, Storage Capacity, Network bandwidth, Transcoding and Proxy Re-encryption.
    - Examples -
        - Computing Power (Ethereum)
        - Storage Capacity (Storj)
        - Network Bandwidth (Privatix)
        - Transcoding = MP4 to MP3 (Transcodium)
        - Proxy Re-encryption =email forwarding (NuCypher)

3. Crypto – Tokens:
    - Built on a robust crypto-currency and crypto – commodity infrastructure
    - Can issue a token which is intrinsically linked to a digital service or product (dAPP / ERC20)
    - Can be part of its own Network and Blockchain Eg: Waves)
    - If based on a network (eg: Ethereum), will pay the network for certain kinds of transactional operations.

Appendix 2: Framework showing the different types of tokens



MAIN TOKEN TYPES PER DIMENSION

Technical Layer	Purpose	Underlying Value	Utility	Legal Status*
Blockchain-Native Tokens **Description:** A token that is implemented on the protocol-level of a blockchain **Characteristics:** ▪ Critical to operate the blockchain ▪ Integral component of the blockchain's consensus mechanism ▪ Part of the blockchain's incentive mechanism for block validators/other nodes **Examples:** BTC (Bitcoin, Bitcoin); ETH (Ether, Etherum), STEEM (Steem, Steem)	**Cryptocurrencies** **Description:** A token that is intended to be a "pure" cryptocurrency **Characteristics:** ▪ Intended as a global medium of exchange ▪ Functions as a store of value **Examples:** BTC (Bitcoin), ZEC (Zcash), KIN (Kin, Kik)	**Asset-backed Tokens** **Description:** A token that functions as a claim on an underlying asset **Characteristics:** ▪ Allows trading via IOUs without actually having to move the underlying asset ▪ The issuer is responsible to hold the underlying asset ▪ Introduces counterparty risk **Examples:** USDT (Tether USD, Tether), GOLD (GOLD, GoldMint), Ripple IOUs (Ripple)	**Usage Tokens** **Description:** A token that provides access to a digital service, similar to a paid API key **Characteristics:** ▪ Grants holders access to exclusive functionality of the service **Examples:** BTC (Bitcoin), STX (Stacks, Blockstack)	**Utility Tokens** **Description:** A token offering owners clearly defined utility within a network or (decentralized) application **Characteristics:** ▪ Closely tied to the functionality of the issuing network or application ▪ Internal network/app currency but not necessarily attempting to be a currency ▪ Grants owners the right to actively contribute to the system vs. passive investor role ▪ Avoids security-like features **Examples:** GNO (Gnosis), STEEM (Steem)
Non-native Protocol Tokens **Description:** A token that is implemented in a cryptoeconomic protocol on top of a blockchain **Characteristics:** ▪ Integral component of the protocol's consensus mechanism ▪ Part of the protocol's incentive mechanism for nodes ▪ Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum) **Examples:** REP (Decentralized Oracle Protocol, Augur)	**Network Tokens** **Description:** A token that is primarily intended to be used within a specific system (e.g. network, application) **Characteristics:** ▪ Token has functionality within the issuers system ▪ Not intended as a general cryptocurrency **Examples:** GNO (Gnosis), STX (Stacks, Blockstack)	**Network Value Tokens** **Description:** A token that is tied to the value and development of a network **Characteristics:** ▪ Tied to the value generated and exchanged on the network (e.g. transaction fee volume) ▪ Closely intertwined with key interactions of network participants **Examples:** ETH (Ether, Ethereum) STEEM (Steem)	**Work Tokens** **Description:** A token that provides the right to contribute to a system **Characteristics:** ▪ Owning Tokens is the precondition for contributing to the system ▪ Contributions are either incentivized with a rewards system or holders get utility from the system/decentralized organization **Examples:** REP (Reputation, Augur), MKR (Maker, Maker DAO)	**Security Tokens** **Description:** A token that behaves like a security **Characteristics:** ▪ Showcases security-like features, e.g. voting on decisions regarding the issuing entity, dividends, or profit shares ▪ Holders are regarded as owners ▪ Little or insufficient utility **Examples:** SPiCE (SPiCE VC), Bitwala (tba)
(d)App Tokens **Description:** A token that is implemented on the application-level on top of a blockchain (and potentially protocol) **Characteristics:** ▪ Integrated within the application ▪ Part of the app's incentive mechanism for nodes and/or users ▪ Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum) **Examples:** WIZ (Wisdom, Gnosis), SAFE (Safecoin, SAFE Network)	**Investment Tokens** **Description:** A token that is primarily intended as a way to passively invest in the issuing entity or underlying asset **Characteristics:** ▪ Promises owners a share of asset value or in (future) success of the issuing entity ▪ No or little significant functionality **Examples:** Neufund Equity Tokens (Neufund), DGX (Digix Gold, DigixDAO)	**Share-like Tokens** **Description:** A token with share-like properties **Characteristics:** ▪ The issuer promises token owners a share in the success of the issuing entity (e.g. dividends, profit-shares) ▪ May or may not come with voting-rights ▪ Mostly on no/weak legal basis **Examples:** DGD (DigixDAO), LKK (Lykke) *Likely to be classified as a security token*	**Hybrid Tokens** **Description:** A token featuring traits of both usage and work tokens **Characteristics:** ▪ Grants access to system functionalities ▪ Allows owners to contribute to the system **Examples:** ETH (Ether, Ethereum, after Casper), DASH (Dash)	**Cryptocurrencies** **Description:** A token that is a pure cryptocurrency **Characteristics:** ▪ Acts as a store of value and medium of exchange ▪ Not emitted by a central authority against which owners have claims In Germany (according to BaFin): ▪ currently not regarded as lawful, functional currency ▪ not regulated by e-money laws **Examples:** BTC (Bitcoin), ZEC (Zcash), LTC (Litecoin)

Untitled INC

*details dependent on respective jurisdiction

Image Source : The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens (Euler, 2018)

Appendix 3: Anatomy of a Smart Contract

Source: The Anatomy of ERC20: What's on the Inside of Ethereum's Most Popular Contract (Nash, 2017), Anatomy of a Smart Contract (Jones, 2017)

Ethereum Request for Comments 20, or ERC20, is an Ethereum Improvement Proposal introduced by Fabian Vogelsteller in late 2015. It's a standard by which many popular Ethereum smart contracts abide. It effectively allows smart contracts to act very similarly to a conventional cryptocurrency like Bitcoin, or Ethereum itself. In saying this, a token hosted on the Ethereum blockchain can be sent, received, checked of its total supply, and checked for the amount that is available on an individual address. This is analogous to sending and receiving Ether or Bitcoin from a wallet, knowing the total amount of coins in circulation, and knowing a particular wallet's balance of a coin. A smart contract that follows this standard is called an ERC20 token.

Smart Contract code (Solidity in this case) contains four major types of entities: variables, functions, events, and modifiers.

- **Variables** are the data storage component of any smart contract and, in the case of a token's smart contract, store balances for each user-address, along with other data required for the smart contract to operate.
- **Functions** describe the rules by which the smart contract operates, storing discrete chunks of code that perform specific tasks. Functions are executed (or "called") by sending a specially formatted transaction to the Ethereum network. Functions are identified by a name and a set of parameters or "arguments," that are the inputs to the function.
- **Events** are signals that a smart contract sends to other applications or smart contracts programmed to receive them—acting as a form of logging.
- **Modifiers** allow a developer to easily restrict the execution of a function under certain conditions. For example, a developer may restrict the ability to mint new tokens to the smart contract owner alone.

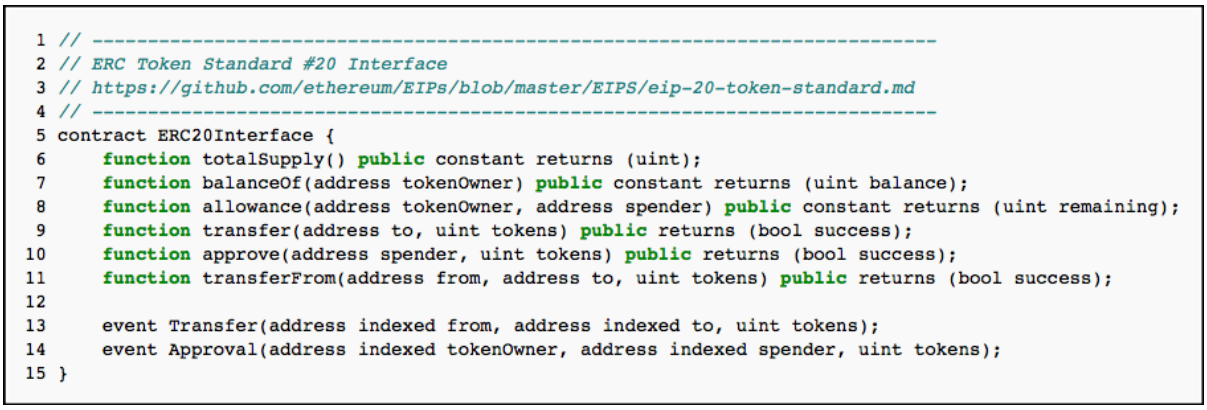
Analysing each function of the smart contract allows us to track how each line modifies the meaning of, or data stored in, the smart contract. ERC20 defines the functions balanceOf , totalSupply , transfer , transferFrom , approve , and allowance . It also has a few optional fields like the token name, symbol, and the number of decimal places with which it will be measured.

- `totalSupply()`: Although the supply could easily be fixed, as it is with Bitcoin, this function allows an instance of the contract to calculate and return the total amount of the token that exists in circulation.
- `balanceOf()`: This function allows a smart contract to store and return the balance of the provided address. The function accepts an address as a parameter, so it should be known that the balance of any address is public.
- `approve()`: When calling this function, the owner of the contract authorizes, or approves, the given address to withdraw instances of the token from the owner's address. Here, and in later snippets, you may see a variable msg . This is an implicit field provided by external applications such as wallets so that they can better interact with the contract. The Ethereum Virtual Machine (EVM) lets us use this field to store and process data given by the external application.
- `transfer()`: This function lets the owner of the contract send a given amount of the token to another address just like a conventional cryptocurrency transaction.

- `transferFrom()`: This function allows a smart contract to automate the transfer process and send a given amount of the token on behalf of the owner. Seeing this might raise a few eyebrows. One may question why we need both `transfer()` and `transferFrom()` functions.

Consider transferring money to pay a bill. It's extremely common to send money manually by taking the time to write a check and mail it to pay the bill off. This is like using transfer() : you're doing the money transfer process yourself, without the help of another party. In another situation, you could set up automatic bill pay with your bank. This is like using `transferFrom()` : your bank's machines send money to pay off the bill on your behalf, automatically. With this function, a contract can send a certain amount of the token to another address on your behalf, without your intervention.

Token Name, Token Symbol (Ticker) and Number of Decimals (normally 18 with ERC20 Tokens) are optional. The image below summarizes the points above and shows us how an ERC20 contract looks like:



```
// ----------------------------------------------------------------------------
// ERC Token Standard #20 Interface
// https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20-token-standard.md
// ----------------------------------------------------------------------------
contract ERC20Interface {
    function totalSupply() public constant returns (uint);
    function balanceOf(address tokenOwner) public constant returns (uint balance);
    function allowance(address tokenOwner, address spender) public constant returns (uint remaining);
    function transfer(address to, uint tokens) public returns (bool success);
    function approve(address spender, uint tokens) public returns (bool success);
    function transferFrom(address from, address to, uint tokens) public returns (bool success);

    event Transfer(address indexed from, address indexed to, uint tokens);
    event Approval(address indexed tokenOwner, address indexed spender, uint tokens);
}
```

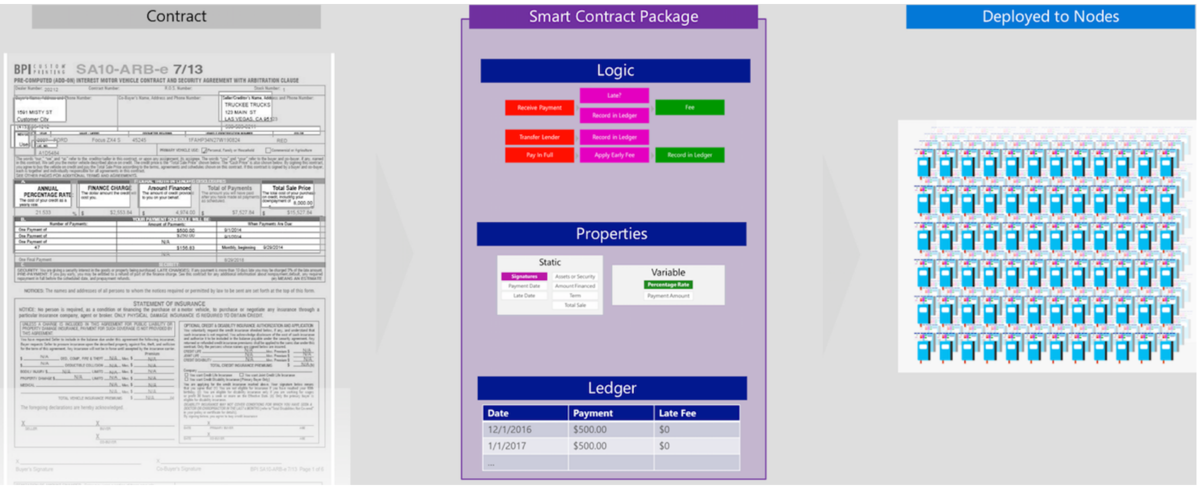
Source: What Is ERC20? | Everything You Need To Know About ERC20? (Singh, 2018)

Smart contracts exist on the Ethereum ledger in a complex, hard-to-read machine language known asbyte code. But they are most commonly written in an intuitive programming language called Solidity (Serpent and others are supported as well) where data structures, functions for business logic, and authorization based on addresses are checked. The source code is compiled into bytecode, and deployed to all nodes on the blockchain for execution. When a DApp is configured properly, it sends a message or transaction to a function of the corresponding smart contract. To do that, it needs the ABI (Application Binary Interface) to correctly format the message and digitally sign it for submission. Once the message is received by a node on the network, it is replicated to all the nodes on the network for execution.

Unfortunately, the initial approach presents challenges that are often difficult for DApp (Distributed Application) developers. A DApp's presentation logic has dependencies at runtime, such as an address of a node on the network (DNS, IP, URI), as well as a port to communicate with. The DApp also needs to know the Ethereum address of the smart contract that is deployed on the blockchain, which is not easily discoverable. Finally, it also needs access to secure private keys, which can be manually inserted by using a file, a blockchain wallet, or a secure device.

To pull business logic up above the blockchain to a separate middle layer, the logic code needs access to a variety of services, including secure execution, attestation, identity, cryptographic support, data formatting, reliable messaging, triggers, and the ability to bind that code to schema in specific smart contracts on any number of blockchains. Those services can be provided in a fabric, where the individual pieces of code that support the smart contracts can execute, send transactions to Blockchain nodes, and be bound to the schema in the data tier.

To get a clearer picture of how this separation of concerns is achieved, we can separate out the different portions of a smart contract into discrete components. These basic components are the properties (static and variable), the logic and the ledger. Each of these components can be mapped directly into technical concepts. Properties represent a data schema, logic represents code, and the ledger corresponds to a database. Once each of these components are defined, they can be deployed to environments that are optimized for their function.



Date	Payment	Late Fee
12/1/2016	$500.00	$0
1/1/2017	$500.00	$0
...		

The smart contract is now a composite of the on-chain Solidity smart contract that defines the data schema on the blockchain, and a Cryptlet[20] that hosts the logic for the smart contract. These Cryptlets can be run on a different computer or the cloud, rather than the actual nodes, and as a result, do not need to be executed by every node on the network. Cryptlets execute in a secure computational environment, and have the cryptographic primitives that allow them to work directly with blockchains, thereby extending smart contracts off the blockchain within the same security envelope.

[20] To pull business logic up above the Blockchain to a separate middle layer, the logic code needs access to a variety of services, including secure execution, attestation, identity, cryptographic support, data formatting, reliable messaging, triggers, and the ability to bind that code to schema in specific smart contracts on any number of Blockchains. Those services can be provided in a fabric, where the individual pieces of code that support the smart contracts can execute, send transactions to Blockchain nodes, and be bound to the schema in the data tier. We refer to these code blocks as Cryptlets, and the execution environment they run is called the Cryptlet Fabric

BIBLIOGRAPHY

Adem Efe Gencer, S. B. (2018). *Decentralization in Bitcoin and Ethereum Networks.* Initiative for Cryptocurrencies and Contracts (IC3) Computer Science Department, Cornell University & Electrical Engineering Department, Technion.

Alabi, K. (2017). Digital blockchain networks appear to be following Metcalfe's Law . *Electronic Commerce Research and Applications*, 23-29.

Antos, J. (2018, March 6). *An Efficient-Markets Valuation Framework for Cryptoassets using Black-Scholes Option Theory*. Retrieved from Medium: https://medium.com/therationalcrypto/an-efficient-markets-valuation-framework-for-cryptoassets-using-black-scholes-option-theory-a6a8a480e18a

Arthurs, J. (2018, June 6). *Authers' Note: Vorsprung dürch Technical Analysis*. Retrieved from Financial Times: https://www.ft.com/content/52b3ccea-6930-11e8-b6eb-4acfcfb08c11

Autonomous NEXT. (2018). *Crypto Utopia.*

Burniske, C. (2017, August 12). *The Crypto J-Curve* . Retrieved from Medium: https://medium.com/@cburniske/the-crypto-j-curve-be5fdddafa26

Burniske, C. (2017, August 12). *The Crypto J-Curve* . Retrieved from Medium : https://medium.com/@cburniske/the-crypto-j-curve-be5fdddafa26

Burniske, J. M. (2018). *[placeholder] Thesis Summary.* Retrieved from Placeholder: https://ipfs.io/ipfs/QmZL4eT1gxnE168Pmw3KyejW6fUfMNzMgeKMgcWJUfYGRj/Placeholder%20Thesis%20Summary.pdf

CB Insights. (2018, Feburary 22). *19 Corporations Working On Blockchain And Distributed Ledgers* . Retrieved from CB INSIGHTS: https://www.cbinsights.com/research/organizations-corporates-test-blockchains-distributed-ledgers/

Cimpanu, C. (2018, March 29). *81% of Recent ICOs Were Scams, Research Finds* . Retrieved from Bleeping Computer: https://www.bleepingcomputer.com/news/cryptocurrency/81-percent-of-recent-icos-were-scams-research-finds/

CNBC. (2013, Nov 3). *BK explains gold's 'vomiting camel' pattern* . Retrieved from CNBC: https://www.cnbc.com/video/2014/11/03/bk-explains-golds-vomiting-camel-pattern.html

David Larrabee, C. (2013, March 6). *Can Technical Analysis Boost Portfolio Returns?* . Retrieved from Enterprising Investor - CFA Institute : https://blogs.cfainstitute.org/investor/2013/03/06/can-technical-analysis-boost-portfolio-returns/

David M. Smith, C. F. (2013). *Head and Shoulders Above the Rest? The Performance of Institutional Portfolio Managers Who Use Technical Analysis .* Money Science: Finanical Intelligence Network.

Devoe, R. (2018, June 19). *Bogus ICO Ratings Easy to Buy, Reveals Alethena* . Retrieved from Blockonomi: https://blockonomi.com/alethena-fake-reviews/

Eghbal, N. (2018, July 18). *Methodologies for measuring project health*. Retrieved from https://nadiaeghbal.com/project-health

Euler, T. (2018, January 18). *The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens*. Retrieved from Untitled INC: http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

Fadilpašić, S. (2018, April 19). *The Vomiting Camel Spotted in the Market* . Retrieved from cryptonews: https://cryptonews.com/news/the-vomiting-camel-spotted-in-the-market-1616.htm

Financial Stability Board. (2018). *Crypto-assets: Report to the G20 on work by the FSB and standard-setting bodies.* Financial Stability Board.

Godbole, O. (2018, March 28). *Why Bitcoin's 'Death Cross' May Be a Bear Trap* . Retrieved from Coindesk: https://www.coindesk.com/why-bitcoins-death-cross-may-become-a-bear-trap/

Grincalaitis, M. (2017, September 17). *The ultimate guide to audit a Smart Contract + Most dangerous attacks in Solidity* . Retrieved from Medium: https://medium.com/@merunasgrincalaitis/how-to-audit-a-smart-contract-most-dangerous-attacks-in-solidity-ae402a7e7868

Grincalaitis, M. (2018, May 9). *The Ultimate Guide to Test Your Smart Contract* . Retrieved from Medium: https://medium.com/@merunasgrincalaitis/the-ultimate-guide-to-test-your-smart-contract-ddc65fbb5ba5

Gupta, A. D. (2018, July 3). *Smart Contracts: Fulfilling Nakamoto's Dreams* . Retrieved from Stratumn Thinking: http://blog.stratumn.com/smart-contracts-the-nakamoto-way/

Jones, S. (2017, Feburary 14). *Anatomy of a Smart Contract*. Retrieved from Blockchain Expo World Series: https://www.blockchain-expo.com/2017/02/blockchain/anatomy-smart-contract/

Klaus, I. (2014). *Forging Capitalism: Rogues, Swindlers, Frauds, and the Rise of Modern Finance.* Yale University Press.

Koffman, T. (2018, April 13). *Your Official Guide to the Security Token Ecosystem* . Retrieved from Medium: https://medium.com/@tatianakoffman/your-official-guide-to-the-security-token-ecosystem-61a805673db7

Kordez, P. (2017, September 4). *Network Output and Velocity of Tokens* . Retrieved from Medium: https://medium.com/d2-capital/network-output-and-velocity-of-tokens-da7e800ca4c0

Lacalle, D. (2017). *Escape from the Central Bank Trap: How to Escape From the $20 Trillion Monetary Expansion Unharmed.* Business Expert Press.

Lannquist, A. (2018, March 7). *Today's Crypto Asset Valuation Frameworks*. Retrieved from Medium: https://blockchainatberkeley.blog/todays-crypto-asset-valuation-frameworks-573a38eda27e

Lessing, L. (2000, January 01). *Code Is Law* . Retrieved from Harvard Magazine: https://www.harvardmagazine.com/2000/01/code-is-law-html

Martin, K. (2018, April 19). *The truth behind the vomiting camel graph* . Retrieved from Financial Times: https://www.ft.com/video/2452d265-ef0e-4f7f-b0b2-ca1dc076ff33

Martin, K. (2018, April 19). *The Vomiting Camel has escaped from Bitcoin zoo* . Retrieved from Financial Times: https://ftalphaville.ft.com/2018/04/19/1524110400000/The-Vomiting-Camel-has-escaped-from-Bitcoin-zoo/

Metcalfe, R. (2013). Metcalfe's Law after 40 Years of Ethernet . *ACM Digital Library*, 26-31.

Milano, A. (2018, July 23). *An $8 Million Airdrop Ran Out of Tokens – What's Next Is Anyone's Guess*. Retrieved from Coindesk: https://www.coindesk.com/8-million-airdrop-cryptocurrency-run-out-tokens/

Mougayar, W. (2017, July 17). Retrieved from Twitter: https://twitter.com/wmougayar/status/885444010550210561

Murphy, H. (2018, July 23). *Pumping and dumping in crypto markets* . Retrieved from Financial Times: https://www.ft.com/content/61ddfea4-8e72-11e8-bb8f-a6a2f7bca546

Nash, G. (2017, August 25). *The Anatomy of ERC20: What's on the Inside of Ethereum's Most Popular Contract*. Retrieved from Medium: https://news.earn.com/the-anatomy-of-erc20-6ab09d4206a5

Olszewicz, J. (2016, November 3). *My Ichimoku Cloud Settings For CryptoCurrency* . Retrieved from Youtube: https://www.youtube.com/watch?v=5x0r-qcGoQQ

Pei, A. (2018, March 28). *Bitcoin is nearing a 'death cross' on the charts. Here's what it means* . Retrieved from CNBC Markets: https://www.cnbc.com/2018/03/28/bitcoin-is-nearing-a-death-cross-on-the-charts-heres-what-it-means.html

Que, D. (2018, March 28). *What we learned from auditing the top 20 ERC20 token contracts* . Retrieved from Medium: https://blog.cryptofin.io/what-we-learned-from-auditing-the-top-20-erc20-token-contracts-7526ef3b6fb1

Qureshi, H. (2018, Feburary 19). *Stablecoins: designing a price-stable cryptocurrency*. Retrieved from haseebq: https://haseebq.com/stablecoins-designing-a-price-stable-cryptocurrency/

Samani, K. (2018, Feburary 13). *New Models for Utility Tokens*. Retrieved from Multicoin Capital: https://multicoin.capital/2018/02/13/new-models-utility-tokens/

Schor, L. (2018, March 15). *Stablecoins Explained* . Retrieved from Medium : https://medium.com/@argongroup/stablecoins-explained-206466da5e61

Sedgwick, K. (2018, Feburary 23). *46% of Last Year's ICOs Have Failed Already* . Retrieved from https://news.bitcoin.com/46-last-years-icos-failed-already/

Shaanan Cohney, D. A. (2018). *Coin-operated Capitalism.*

Singh, N. (2018, January 22). *What Is ERC20? | Everything You Need To Know About ERC20?* . Retrieved from Cryptoniam: https://www.cryptoniam.com/what-is-erc20/

Smith+Crown. (2018). *Cryptoasset Valuation*. Retrieved from https://www.smithandcrown.com/list/cryptoasset-valuation/

Srinivasan, B. S. (2017, July 28). *Quantifying Decentralization* . Retrieved from https://news.earn.com/quantifying-decentralization-e39db233c28e

Wall Street Journal. (2018, August 5). *Some Traders Are Talking Up Cryptocurrencies, Then Dumping Them, Costing Others Millions*. Retrieved from Wall Street Journal: https://www.wsj.com/graphics/cryptocurrency-schemes-generate-big-coin/

Wilson, F. (2017, 06). *ICOs and VCs* . Retrieved from AVC: https://avc.com/2017/06/icos-and-vcs/

Xing-Zhou Zhang, J.-J. L.-W. (2015). Tencent and Facebook Data Validate Metcalfe's Law . *Journal of Computer Science and Technology* , 246–251.