Token Ecosystem Creation

A strategic process to architect and engineer viable token economies

Outlier Ventures

Disclaimer

This document (the "Document") has been prepared by Outlier Ventures Operations Limited ("Outlier Ventures"). Outlier Ventures Operations Ltd is registered in England and Wales, company registration number 10722638.

No undertaking, warranty or other assurance is given, and none should be implied, as to, and no reliance should be placed on, the accuracy, completeness or fairness of the information or opinions contained in this Document. The information contained in the Document is not subject to completion, alteration and verification nor should it be assumed that the information in the Document will be updated.

The information contained in the Document has not been verified by Outlier Ventures or any of its associates or affiliates. The Document should not be considered a recommendation by Outlier Ventures or any of its directors, officers, employees, agents or advisers in connection with any purchase of or subscription for securities. Recipients should not construe the contents of this Document as legal, tax, regulatory, financial or accounting advice and are urged to consult with their own advisers in relation to such matters. The information contained in the Document has been prepared purely for informational purposes. In all cases persons should conduct their own investigation and analysis of the data in the Document. The information contained in the Document has not been approved by the Financial Conduct Authority. This Document does not constitute, or form part of, any offer of, or invitation to apply for, securities nor shall it, or the fact of its distribution, form the basis of or be relied upon in connection with any contract or commitment to acquire any securities.

Any forecasts, opinions, estimates and projections contained in the Document constitute the judgement of Outlier Ventures and are provided for illustrative purposes only. Such forecasts, opinions, estimates and projections involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by such forecasts, opinions, estimates and projections. Accordingly no warrant (express or implied) is or will be made or given in relation to, and (except in the case of wilful fraud) no responsibility or liability is or will be accepted by Outlier Ventures or any of its directors, officers, employees, agents or advisers in respect of, such forecasts, opinions, estimates and projections or their achievement or reasonableness. Recipients of the Document must determine for themselves the reliance (if any) that they should place on such forecasts, opinions, estimates and projections.

The views presented in this report do not necessarily represent the views of Imperial College London. These views are provided by the author for illustrative and informational purposes only, and should not be considered a recommendation in connection with any purchase of or subscription for assets.

Information contained in the Document may not be distributed, published or reproduced in whole or in part or disclosed to any other person. The distribution of any document provided at or in connection with the Document in jurisdictions other than the United Kingdom may be restricted by law and therefore persons into whose possession any such documents may come should inform themselves about and observe any such restrictions.

Authors

Eden Dhaliwal
eden@outlierventures.io

Dr. Zeynep Gurguc
z.gurguc@imperial.ac.uk

Eden Dhaliwal
Lead Author & Partner,
Head of Crypto-economics
Outlier Ventures

Dr. Zeynep Gurguc
Lead Author &
Research Associate
Imperial College London

Anesu Machoko
Associate
Outlier Ventures

Geoff Le Fevre
Analyst
Outlier Ventures

Jamie Burke
CEO & Founder
Outlier Ventures

Contributors

Aron van Ammers
CTO & Founding Partner
Outlier Ventures

Lawrence Lundy
Partner/Head of Research
Outlier Ventures

Rumi Morales
Partner
Outlier Ventures

Matt Law
Partner/Head of Operations
Outlier Ventures

Peer Reviewers

A special Thank You to our colleagues who supplied us with valuable feedback:

Ryan Breen
Co-founder & CEO, Alkemi.ai

Dimitri De Jonghe
Head of Research,
Ocean Protocol & Blockchain
Application Director,
BigchainDB

Prof William Knottenbelt
Director, Imperial College Centre
for Cryptocurrency Research
and Engineering

Prof Marek Laskowski
Researcher, York University &
Program Chair, BlockchainHub

Dr Robert M. Learney
Lead Technologist - Blockchain
& DLT, Digital Catapult

Trent McConaghy
Co-founder, Ocean Protocol
& BigchainDB

Toby Simpson
Co-founder & CTO, Fetch.AI

Dr Phillip J. Windley
Chairman, Sovrin

Dr Michael Zargham
Founder & CEO, BlockScience

Contents

About Outlier Ventures

Venture Capital for the decentralized future.

We invest and partner with the communities that will create the new decentralized web economy.

Outlier Ventures is a venture platform focused on building the infrastructure for the next phase of the Web. As the first European venture firm dedicated to blockchain technology, we've developed an industry-leading investment thesis, based on the convergence of decentralized technologies such as blockchains and distributed ledgers, with 'deep tech' such as artificial intelligence, robotics, the Internet of Things, and 3D printing.

We focus on early stage, seed and pre-seed projects where direct support to investee founders and creating value post-investment is integral to our business model. We have consistently proven our ability to identify exceptional projects, allowing us to constantly expand. Our team is 30 people and growing, with specialists in crypto-economics, research, legal, marketing, and tech, with a presence in London, Toronto, Chicago and Berlin, we bring a powerhouse of support to founders.

Investing in both equity and crypto-tokens we have contributed to and partnered with some of the most impressive projects in the decentralized space including IOTA, Ocean Protocol, Fetch.AI, SEED, Sovrin and most recently Haja Networks.

Foreword
By Jamie Burke CEO/Founder of Outlier Ventures

Cryptographically secure and digitally scarce tokens are the magic sauce, or killer app, of the blockchain movement and represent a new wave of business model innovation. The ability to program both a hard cost and monetary incentive against user behaviors, directly into open source systems, transforms them from purely technical to socio-economic innovations.

From capital to computing power, and data to people and their assets, tokens allow us to coordinate and optimize large networks of resources in a decentralized manner and at scale.

Tokens bring with them powerful network effects that reward participants relative to their stage of adoption, the value they contribute and the risk they bear in an auditable and trustful way.

Tokens allow for a new liquid asset to crowdfund the next wave of the Web, a direct stake in its future which can be fractionalized, shared or sold in secondary markets.

At Outlier Ventures we believe this innovation will become foundational to Web 3.0 and impossible for existing or future proprietary and closed systems to compete with. As such we continue to dedicate a considerable amount of time and resource to understanding and designing tokenized systems with our growing portfolio.

As an investor, we were the first venture capital firm in the world to hire a dedicated Head of Crypto-economics as well as form a three year R&D program with a world-leading university - Imperial College London - with both their Department of Computing and the Business School, to explore the space with academic depth and rigor.

This document contains the lessons we have learned in our first year (2017-2018) of designing several systems from scratch as part of this program. We share it freely because if there is one thing we have come to understand, it is this: the sheer depth of expertise and breadth of skills required to come close to mastering this emerging discipline can never exist within one organization, perhaps not even a generation. It is a mission that needs to draw upon a network of many. As such, this serves as an open invitation to join us on this mission.

Introduction

Over the last few years, there has been tremendous exuberance around the potential of crypto-based tokens. The nature of these tokens has yet to be fully understood, with a wide range of thinking that defines these as either currency, securities or something uniquely different. By adding blockchain architecture to crowdfunding, it is easy to label tokens as a share-like security whose main purpose is to raise capital. They can act as a store of value, unit of account and/or medium of exchange; and can very much exhibit the characteristics of currencies, commodities, derivatives or collectables. Most promising, however, are those tokens that offer forms of utility for users powered by intelligent and imaginative incentive systems.

New digital business models are often met with tremendous cynicism; however, they can create new value propositions and uncover new behaviors to meet the previously unmet needs and desires of consumers, end users and other market constituents. **Every new emerging technology brings with it new and disruptive business models. And for blockchain technology, these are token economies.**

Just as a freemium model was once considered to be highly questionable, risk-laden and value destructive, but has proven its business and behavioral basis over time; tokenization will similarly generate new forms of business and social value through novel forms of economic enablement.

From the early internet days and through the web 2.0 era, many digital business models have now been identified, ranging from two-sided marketplaces to software-as-a-service (SaaS) to data monetization. Along the way, there have been many lessons learned as to what works, how and why. In fact, decades of learnings (particularly from Silicon Valley) from the growing pains and failures of early-stage ventures have led to crucial understandings on how to effectively launch digital businesses through methodologies like the lean startup, design thinking and the minimum viable product.

The most fundamental recognition, however, is that new ventures are not really ventures after all, but as Steve Blank uncovered, what we call 'startups'. Furthermore, he defines a startup "as a temporary organization designed to search for a repeatable and scalable business model." Temporary, because startups have short runways due to bootstrapping and/or minimal seed capital. And considered an 'organization' but not yet a fully formed business venture because startups are still seeking product-market fit in order to transition into sustainable businesses.

As the blockchain community has ventured out to create token-based networks, we have discovered that many of the existing tools and methods used for launching new digital ventures do not seem to work well in this space. Tools like the business model canvas do not capture the core components of tokenization well (like governance, for example). Developing user personas for new stakeholders like miners and curators is a challenging task. Agile methods to validate utility are far more complex with token systems. The reason why these methods are not effective is that token models are not actually digital ventures after all.

Instead, they are *digital economies* that reorganize and redistribute new forms of value by combining tokenized incentive systems with blockchain architecture. Launching an economy is fundamentally different from launching a venture in that an economy is a set of complex systems of governance, economics and cryptography combined into a single distributed system. Whereas web 2.0 businesses are typically built from the bottom-up, token economies require a combination of both top-down and bottom-up approaches.

Early-stage web 3.0 digital economies can be realized as 'token ecosystems' which may mature into stable and prosperous crypto-economies (analagous to how startups can evolve into sustainable businesses). ***A token ecosystem is a decentralized network engineered to align a secure and incentivized economic system, despite being laden with uncertainty***. Until a token ecosystem can achieve economic alignment amongst network participants, confidently secure itself against attack vectors and demonstrate a high degree of decentralization and token utilization (rather than speculative trading), it can only be considered a well-funded experimental distributed network. If this can all be achieved, then we can credibly consider it an established token economy. This may take many years to develop, and at the moment, Bitcoin and Ethereum are the only existing networks that have differentiated from other networks in terms of maturation of decentralization, security, governance and utility; yet still subject to uncertainty and volatility.

The following is a process that should provide guidance as to how to create and launch a token ecosystem.

Chapter 6

Getting Started

Before we get started, it is important to stress that a project should be managed by a team with the right mindset, and breadth of skills. While different skillsets are needed at different stages of a project, it is essential to augment a team as early as possible in the process through hires or partnerships.

6.1 Innovation Mindset

Crypto-economics is a new discipline developing upon many well-established disciplines and empirical data. However, observers and creators in this field often differ in worldview, and/or political ideals, and are often subject to biases. We do not want to impose a specific view or ideal with our approach; our focus is to pragmatically design evidence-based, sustainable systems that can serve and be adopted by as many people as possible within today's common capabilities.

Therefore, our approach requires a commercial innovation oriented mindset with several fundamental attributes:

– Collaborative rather than siloed
– Creative to generate new solutions and ideas
– Integrative to encompass systems thinking
– Evidence-based around experimentation
– Pragmatic not dogmatic (polarised thinking)
– Agile, which borrows from lean startup thinking

Collaborative	No one is an expert in token design so everyone's individual knowledge is a valuable contribution. It should be an inclusive and transparent process, optimizing on cross-functional touch points throughout the entire token design process.
Creative	Token design is about creating new economic models, so new innovative ideas are critical. Creative problem- solving should be focused on combining existing tools in new ways throughout the entire process.
Integrative (Systems Thinking)	Approaching problems holistically is critical in the field of token design. Combining intuition, reasoning, and imagination to tackle strategy, operations, and product development is paramount for a field and process that is constantly evolving.
Evidence-based	Assumptions are unavoidable throughout the design process, but all assumptions must be tested. Testing is a key component of our process which carries forward from the design phase into the deployment phase, and lasts throughout the entire lifecycle of the token.
Pragmatic	Being practical and effectively executing ideas should always be a focus. Having a clear understanding of how to effectively manage resources and timelines is a cornerstone of successful token design.
Agile	Borrowing from the lean startup principles, this process is centered around experimentation, learning and iteration. Key to this is getting the system architecture structurally correct. Once this established, elements can be iterated and evolve within the structure iteratively.

6.2 Crypto-economic Team Skill Requirements

There are very few people who can genuinely claim to be crypto-economics experts in this emerging field and no single individual has all the skills, experience and competencies to effectively do the job. Instead, it is essential to assemble a diverse **Crypto-economics Team** that can collectively apply the following:

- User/Market Research
- Strategic Planning
- Mechanism Design and Game Theory
- Market Design
- Behavioral Economics
- Capital Markets
- Operations Research
- Financial Engineering
- Advanced Mathematics
- Blockchain/DLT Architecture
- Systems Engineering
- Network Science
- Machine Learning and Data Science
- Lean Startup and Agile Software Development
- Design Thinking
- Complex Systems

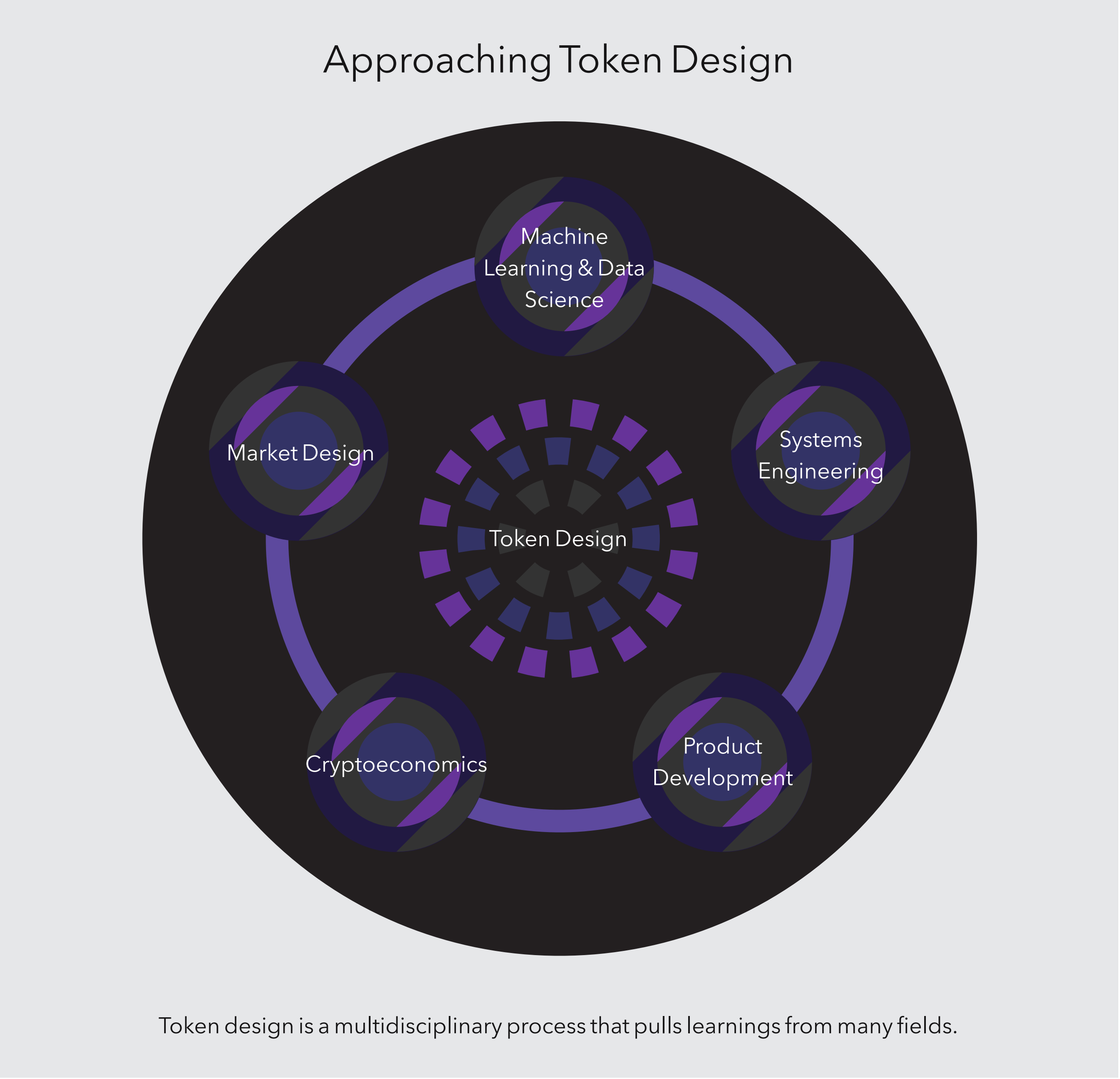
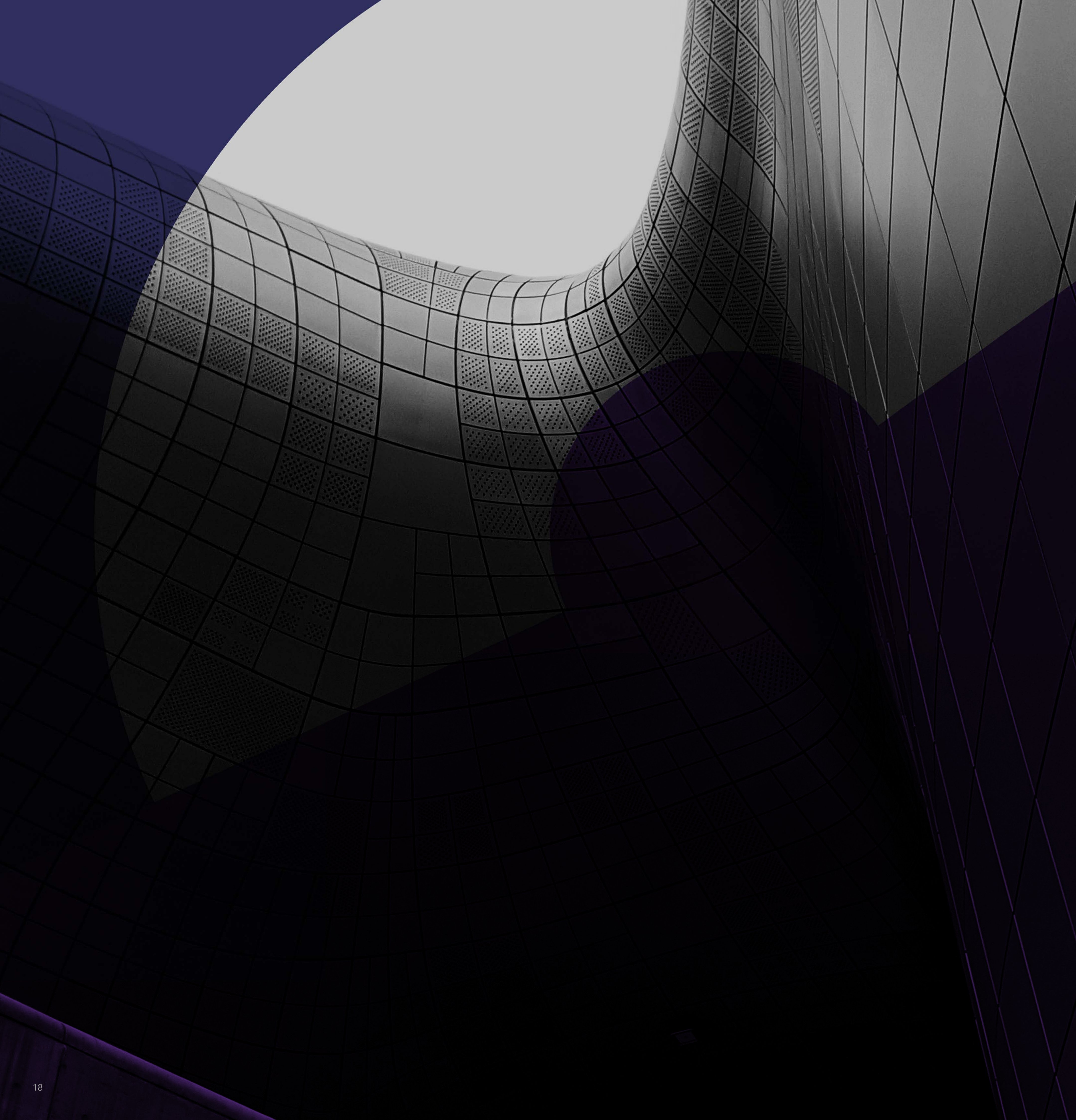


Figure 1: Approaching Token Design

However throughout this document we will refer to team members generically as **Token Architects** .



Chapter 7

Phased Strategic Process

After several iterations we have begun to develop an agile process to serve a tokenized system to the point of **Network Equilibrium**: one where its utility is fully optimized and the network is in balance. Obviously, this end-state will not be achieved in a few months or even a few years. This is an ongoing process. After all, it has yet to be achieved in the nascent 'blockchain' space and even in the case of Bitcoin after ten years of existence.

Because token ecosystem creation is so new, and stakeholders involved are destined to make what retrospectively will seem obvious and naive mistakes, we suggest everything stated in this document is taken as a starting principle for debate rather than a rule or law. Until there are appropriate amounts of empirical data, we simply cannot guarantee that outcomes derived from the early design stages of this process will be perfect. But we can say with confidence that the process outlined provides an iterative approach with feedback loops. This is likely to reduce the risk of errors to acceptable levels over time by borrowing from scientific approaches applied to engineering complex systems which demand low fault tolerance, like aerospace. This is why elements of this process have been referred to as **Token Engineering**, an area first coined by Trent McConaghy, Co-founder of Ocean Protocol and BigchainDB. It is also important to point out that while much of this work is principally derived from first-hand experience, it has been developed from a vibrant and growing ecosystem of partners, collaborators and thought leaders. This includes people we know and engage with personally and those from whom we learn from afar, including Vitalik Buterin (Co-founder of Ethereum), Chris Burniske (Founding Partner of Placeholder.vc), and Michael Zargham (Founder of BlockScience). So it is true to say, it stands on the shoulders of others for whose openness of thought we are eternally grateful.

The intention for any tokenized system should be to ultimately achieve high degrees of decentralization and automation so that the system can realise its full technological potential to become more resilient, less fragile and, from a design perspective, suffer less **value leakage**.[1] However, the topic of decentralization in the blockchain space is often approached with dogmatism about early design choices that are hardcoded into systems before they have been properly validated, which achieves the very opposite affect: fragile systems which are prone to constitutional conflict and the possibility of network **forks**. Therefore we propose a 'pathway to decentralization' that is pragmatic, evidence-based and flexible for different use-cases.

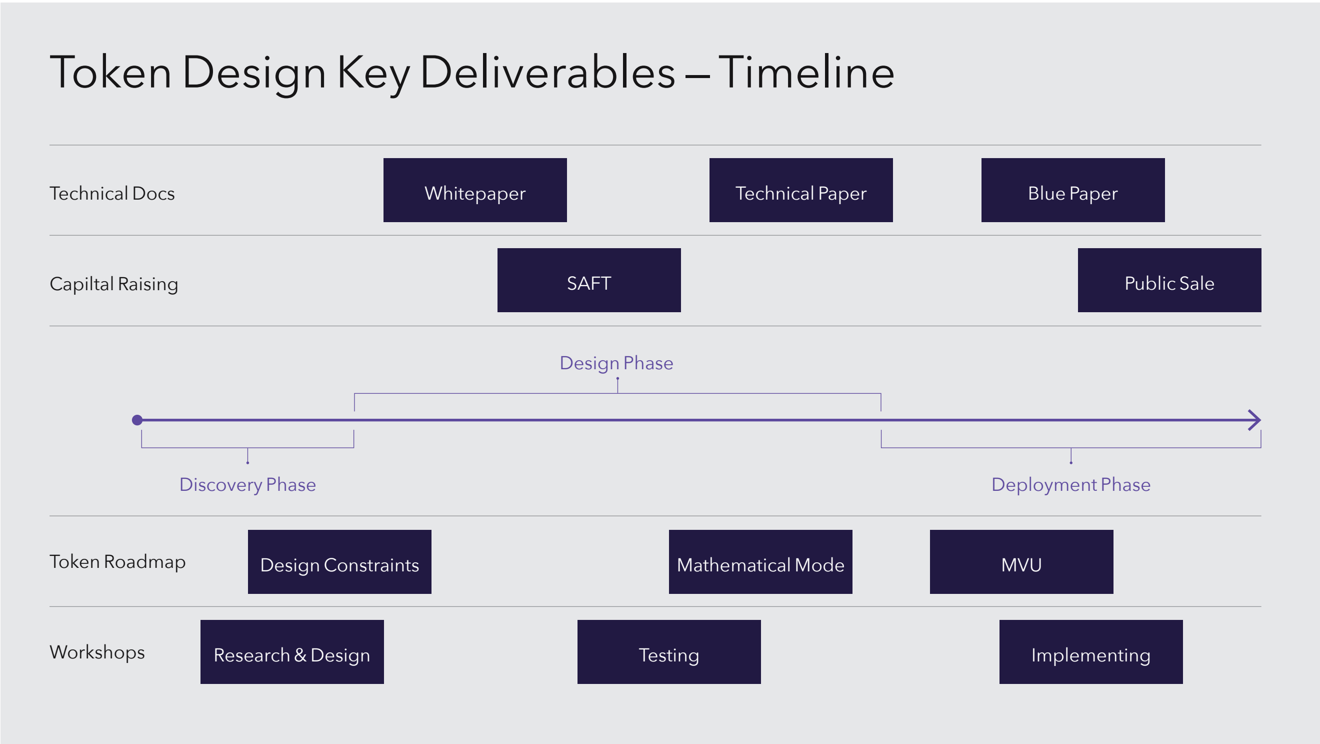


Figure 2: Token Design Key Deliverables - Timeline

The 3 Ds of Token Ecosystem Creation

(detailed to the right) broadly operates within four parallel activities including:

A series of 1) workshops that inform outputs for the 2) token roadmap as well as 3) technical specifications and documentation run concurrent to 4) fundraising activities of a project.

The latter point is of critical importance because often early adopters and users can also be seen as early financiers and a new form of 'shareholder'. Therefore, understanding who can and should participate in these economic systems and when, has regulatory consequences creators need to be aware of.

– Discovery Phase

The discovery phase is to determine the particular characteristics of the business model or ecosystem and why a token is needed in the first place.

– Design Phase

The design phase consists of making high level design choices including, governance structures, the (mathematical) token model and its parameters. These need to be optimized for stakeholders' incentives and the long term sustainability of the associated ecosystem in order to avoid value leakage.

– Deployment Phase

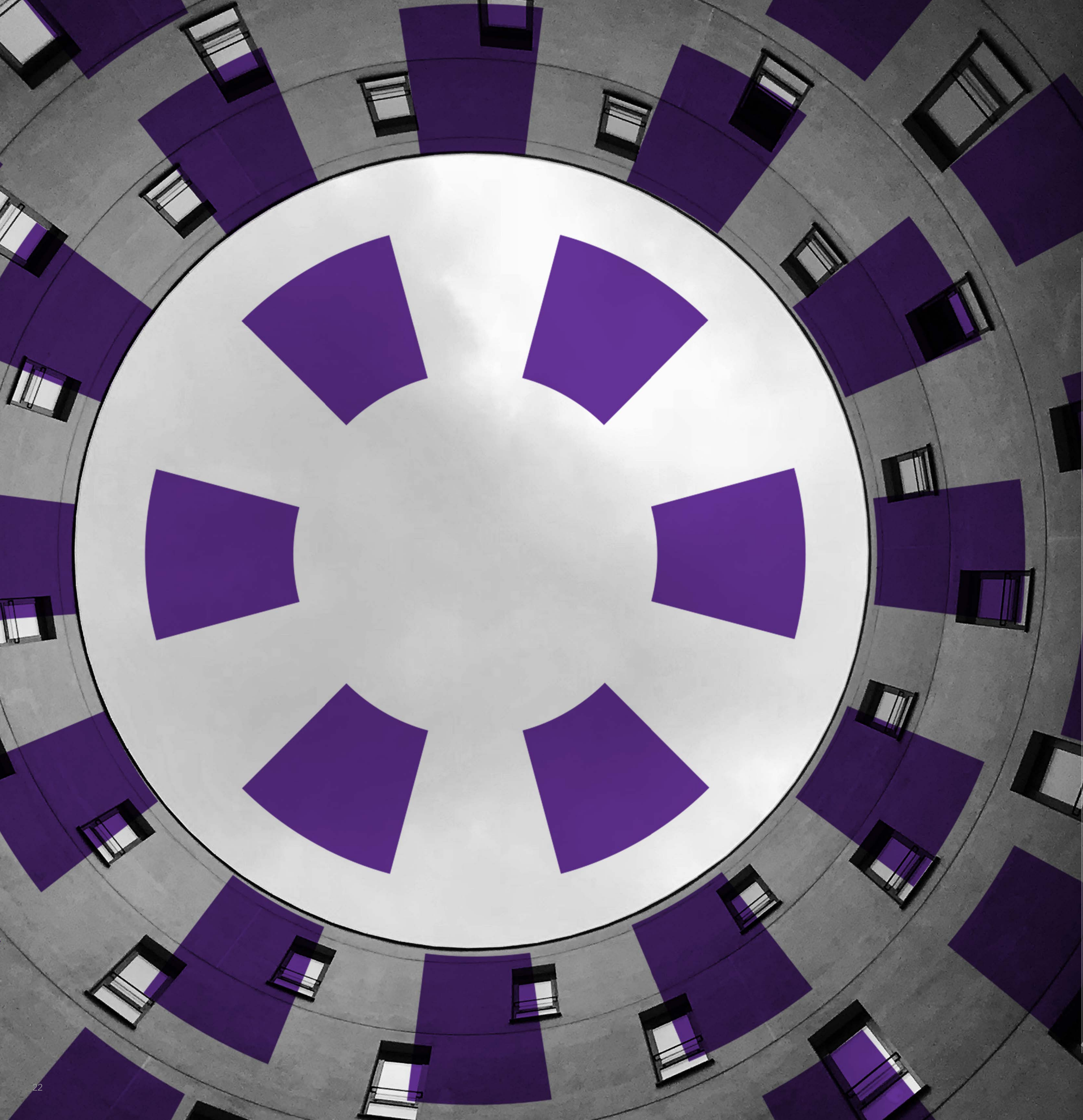
Finally, the deployment phase comprises of validating and stress-testing the parameters that were defined during the design phase, before fully integrating into the network.

It is important to note that optimization and testing are present throughout the entire token lifecycle in an iterative process, that is, in practice token models should be continuously optimized for parameters, variable ranges, and a concept called **Token Gravity** at all stages.

Token Gravity is the understanding of how tokens are likely to move within a network, as incentive tools affect the likelihood and frequency of transactions between stakeholders.

CONCEPT

[1] That is to retain economic value within the system.



Chapter 8

Discovery Phase

SKILLS REQUIRED
User Research, Business Planning, Business Model Innovation

The discovery phase is about defining the overarching problem to be solved and understanding the key stakeholders, what is valuable to them and how this value is exchanged between them. It requires a deep understanding of markets.

8.1 Discovery Inputs

During this stage, we pull together any existing research or data pertaining to user patterns, consumer behaviors, market data, pricing and other relevant business information. This may include items such as journey maps, customer segmentation, archetypes, business model canvas, pricing models, **PEST analysis** and other strategic tools. And, of course, any draft white papers or thinking around any potential token systems.

CONCEPT

PEST (political, economic, socio-cultural and technological) analysis describes a framework of macro-environmental factors used in the environmental scanning component of strategic management.

8.2 Discovery Tools

8.2.1 Problem Structuring

Tokens are value creation and exchange mechanisms that allow network agents to participate in, and/or manage the system. They ensure that nodes operate effectively and actors participate in a coordinated manner. Therefore, they play an important role in aligning the incentives of the ecosystem participants. A token ecosystem is a highly complex system designed to deliver a socially and economically optimal allocation of resources. It is this complexity that requires structured top-down thinking in order to clearly organize and prioritize an integrated set of challenges. It is critical to deconstruct these challenges into the singular primary problem that is to become the goal of the token economy, and define the constraints of this problem.

This kind of problem-solving demands the ability to see a problem from multiple perspectives even though they may challenge our initial assumptions, pre-conditioned beliefs and experiences. Second, it is important for us to be able to navigate through complexity to find the essence of the problem and identify linkages to its sub-issues. A good method of problem solving for complex issues is the MECE approach, established by McKinsey & Co.

CONCEPT

MECE, pronounced "meece", is a grouping principle for separating a set of items into subsets that are mutually exclusive (ME) and collectively exhaustive (CE).

8.2.1.1 Problem Statement Worksheet (Document)

A clear problem definition can be achieved by using the **Problem Statement Worksheet** (shown below) which helps define the core problem by posing a critical question that needs to be answered while laying out the context, criteria for success, the scope of solution space, and various stakeholders and constraints that need to be satisfied.

Core Question	What is the core question to focus on? It should be specific, measurable, action-oriented, relevant and time-bound **(SMART)** while ensuring it is not so narrow that it excludes critical issues.
Context	Here we lay out the complexity we're facing and that will need to be met.
Criteria for Success	Here we define what success for the project looks like, and should include qualitative and quantitative measures.
Scope of Solution Space	Identify the parameters of the solution - what will/will not be included in the solution set.
Constraints of Solution Space	Determine the limits/boundaries of the solution set.
Stakeholders	Identify the key actors involved.
Key Sources of Insight	Locate key areas where learnings could come from.

8.2.1.2 Logic Trees

The token model's core problem should be structured by disassembling it into distinct issues in the form of a logic tree (as seen below).

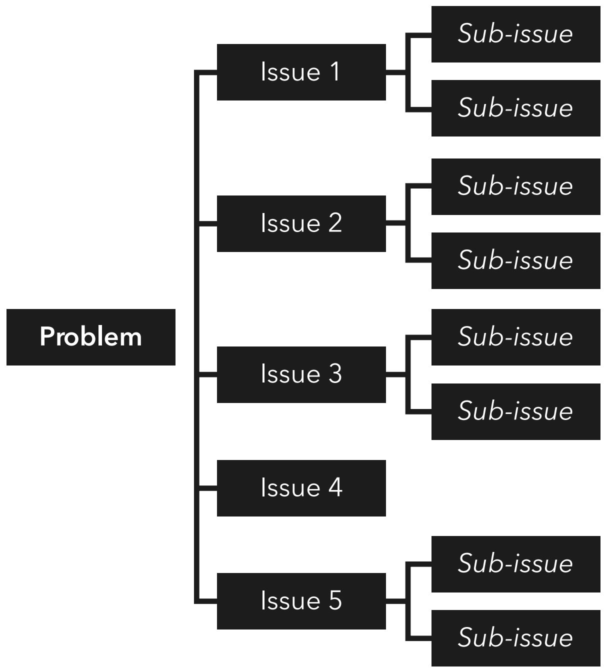


Figure 3: Example of a logic tree[2]

Good logic trees follow **MECE: mutually exclusive, collectively exhaustive**. This means that issues should be mutually exclusive, or said another way, without overlap. Collectively exhaustive means that all issues are covered and there are no gaps. To do this requires **root cause thinking**. To get problems well-structured is very challenging and takes considerable thinking, and requires high degrees of collaboration.

Lastly, we must prioritize issues such as governance, security and economics in terms of importance.

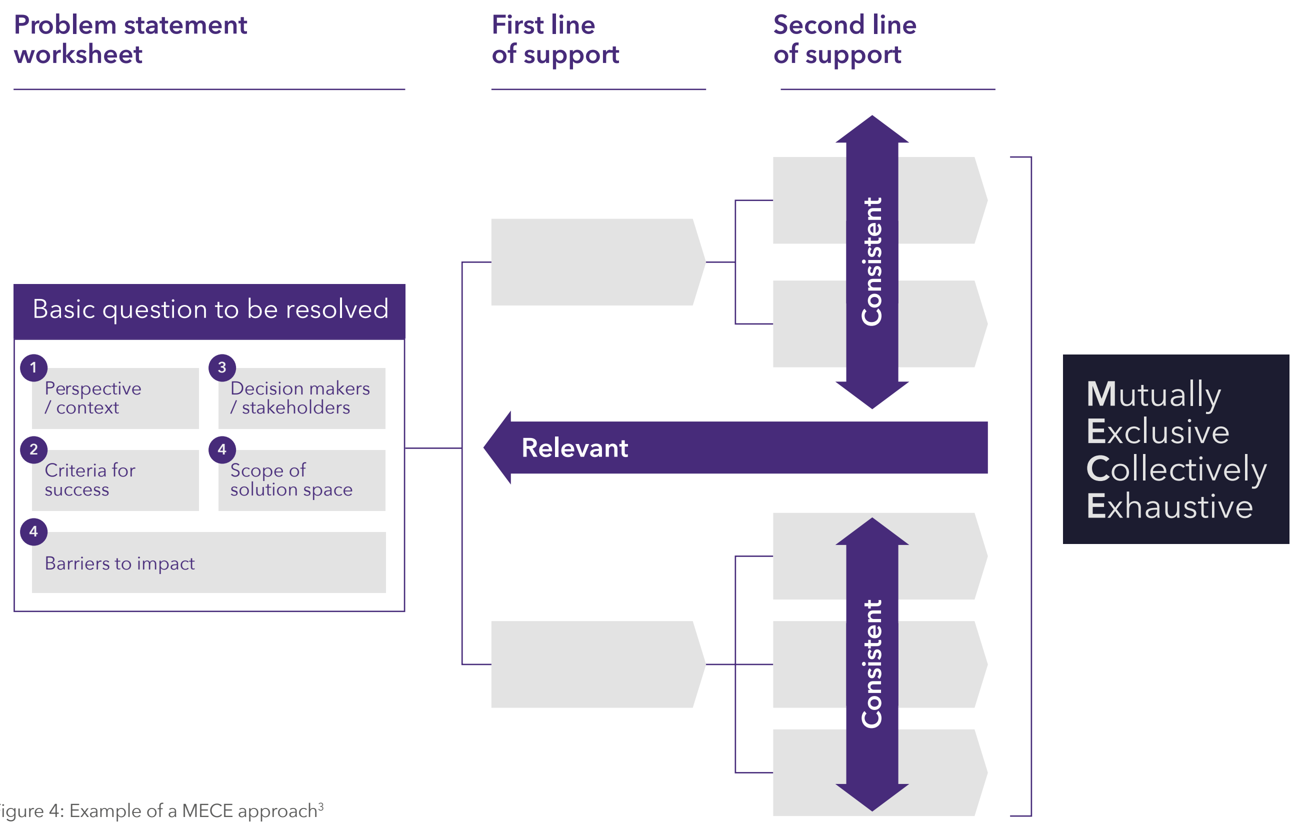


Figure 4: Example of a MECE approach[3]

8.2.2 User Research

A critical component of planning the foundations of any new ecosystem is understanding the key stakeholders involved and how value flows between them. Where possible, it is useful to examine current or analogous markets to understand the relationships between their various layers while taking system safety requirements into account.

Defining prospective stakeholders and differentiating the archetypes within each, as well as understanding the corresponding value exchange is important in creating a **Taxonomy of Actors**. This step is critical in token design, and used to justify and evaluate design parameters as well as determine ways to test and validate underlying assumptions regarding user behavior.

The best methods to gain these insights is through **Stakeholder Mapping** and **Value Exchange Mapping**, conducted in a series of workshops detailed below. This methodology allows us to map out the value stack of the ecosystem. The diagram below from BlockScience shows the scope of the value stack for tokenized ecosystems.

[2] McKinsey & Company www.mckinsey.com

[3] McKinsey & Company www.mckinsey.com

[4] Dr. Michael Zargham, Block Science, Value Stack

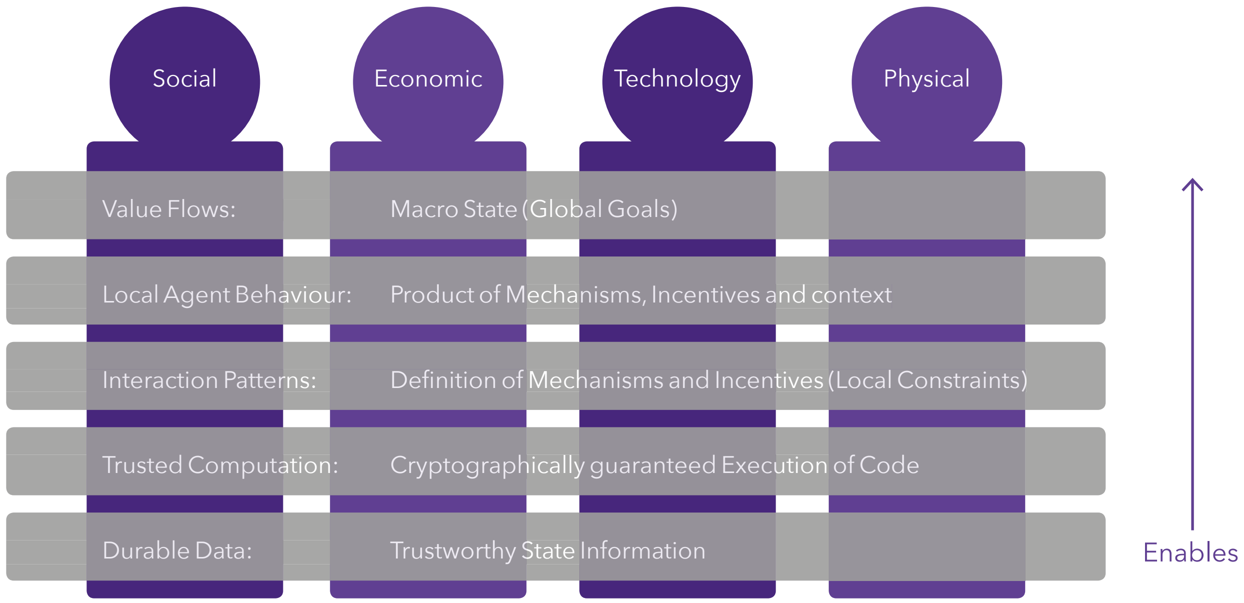


Figure 5: Value Stack[4]

8.2.2.1 Stakeholder Mapping (Workshop)

Stakeholder mapping is used to identify the actors involved in an economy and how they relate to one another. This exercise defines stakeholder roles and illustrates the relationship between them in the system. An in-depth analysis creates a clear illustration of the dynamics at work and this tool serves to frame these relationships in the context of the primary problem we are trying to solve and optimize subject to associated constraints. This increases the chances of finding a solution that will remove unneeded intermediaries and address as many important stakeholder needs as possible for a win-win outcome. This is critical when trying to retain the majority of participants to reduce the fragility of a system and the possibility of **value leakage** or worse a value-destroying **fork**.

CONCEPT

In an open sourced system (OSS) **forking** refers to creating alternative versions of a piece of software. In some contexts, forks can be beneficial and actually work to increase the functionality of a codebase or be a means for network participants to express their rights and views. In the context of blockchain networks, there are two types of forks, **hard forks** and **soft forks**. It is important to note that these complex systems need to be adaptable but an ecosystem is only as strong as its community, and loss of participants can have detrimental effects to the ecosystem. Therefore, the cost versus benefits of forking should be considered carefully.

A **Hard Fork**, is a permanent divergence from the previous version of the blockchain network such that all nodes running previous versions will no longer be accepted onto the new chain. Example: The Ethereum and Ethereum Classic hard fork Oct 2016.

A **Soft Fork** refers to changes that only updated clients support, but older versions are still compatible with. Usually miners/validators are required to upgrade so as long as they do, the network does not diverge. Example: The Ethereum Metropolis upgrade in Oct 2017.

Steps involved:

1. **Identify all possible relevant stakeholders.** Keep in mind that a stakeholder can also be a negative actor to be controlled and/or optimized out of a system.[5]

2. **Define and analyse the respective roles** and multi-directional relationships in the ecosystem.

3. **Whiteboard the system as a pathway / network.** Position and connect the stakeholders who influence and impact each other the most in priority lanes.

5 Amongst many others.

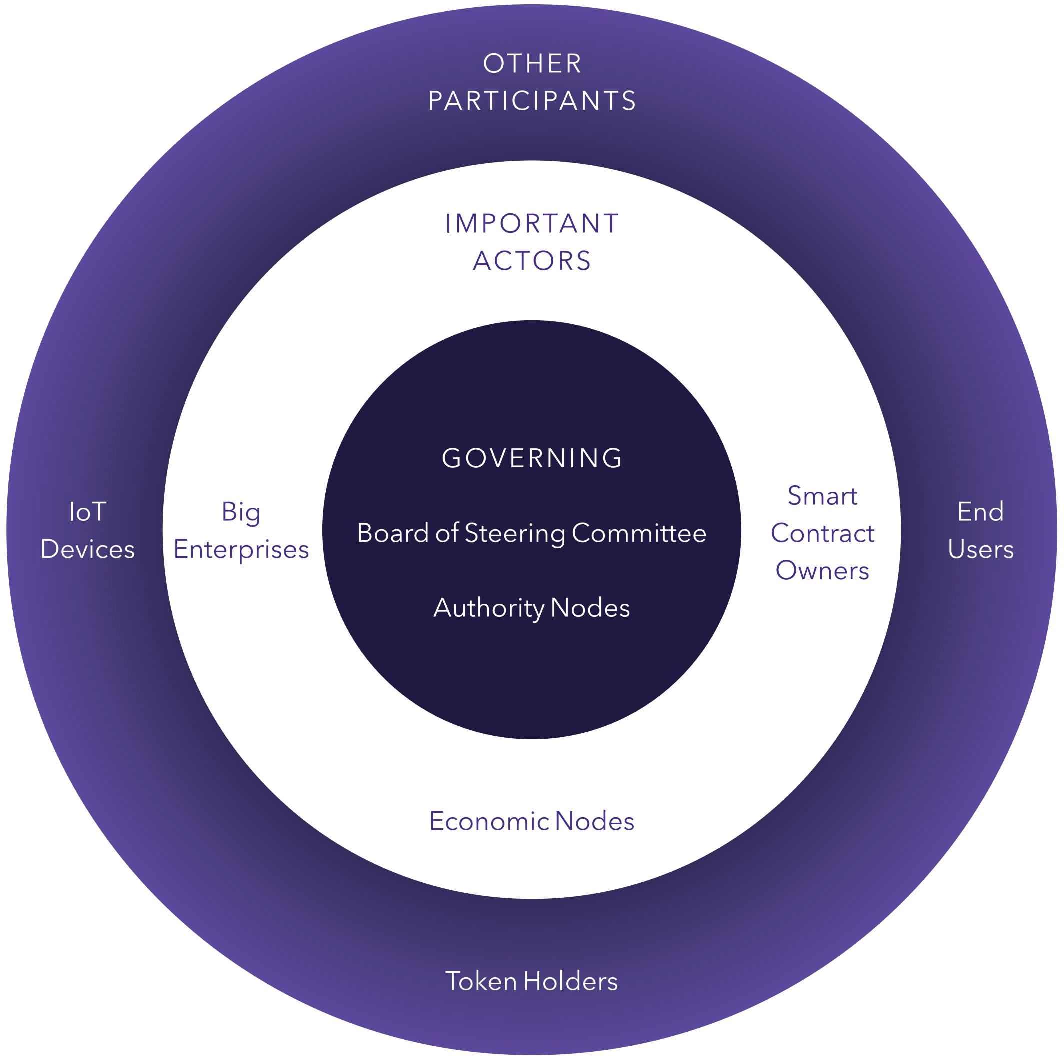


Figure 6: Stakeholders

8.2.2.2 Value Exchange System[6]

After Stakeholder Mapping, creating a value-exchange system among stakeholders will help us synthesize value formation and, importantly, reveals opportunities to generate revenue streams, cost savings and other incentives by finding the most effective and efficient ways to deliver it.

Steps involved:

1. **Take the outcomes of the stakeholder mapping**, mainly the definition of each stakeholder and their roles.

2. **Explore how each actor may benefit**. The most obvious is through compensation, however, consider other meaningful rewards as well . While it is important to define what each stakeholder contributes to value creation and what they receive in return in the broadest sense, this exercise focuses on how and if they can be rewarded. While this is a conceptual exercise to intuitively explore financial exchange, and it involves the need to work through the specific financials; it may also involve considering non-monetary rewards. Reciprocity also expands the definition of value to ensure that everyone wins in these broader terms.

3. **Illustrate the exchange of value between them**. Begin to prototype the system into a single ecosystem that connects stakeholders to the delivery of the solution. Use sticky notes and large surfaces to whiteboard the potential solution and value exchange system.

4. **Look for additional sources of growth and revenue**. While obvious ways to generate revenue (for example, transactions) may already have been identified, this is the time to look for additional growth initiatives.

5. **Conduct comparative analysis**. Examine competing or analogous markets to understand efficiencies and inefficiencies. Pay attention to how value is created and the costs and capabilities involved.

6. **Hypothesize , prototype, iterate, and refine**. Create an initial prototype and assess whether this is the most business viable and technically feasible way to deliver the proposed solution. Examine if there are other ways to go about this. A key point to consider should be: how sustainable is this model over the long-term and how could it be disintermediated or disrupted?

7. **Evaluate the unique role of the 'foundation'**[7]. Determine how the foundation is uniquely positioned to develop the network and succeed. Focus on the existing capabilities and interdependent relationships, and determine if these can be distinctly leveraged to contribute to success and competitive advantage.

The **stakeholder map** is a helpful reference to eventually deliver value to key stakeholders – the end user in particular. Identifying capability requirements and designing the future activity system are interrelated exercises that together will shape the strategy. This is an iterative process; stakeholders and elements can and should be rearranged to reveal different models of value exchange. Using tools such as sticky notes and a whiteboard is a helpful visualization tool. Consider ways to refine the system and improve both viability and efficiency by looking to external partners and technology. A landscape of stakeholders perhaps in sequential orbits that may have been developed earlier will come in handy here. Imagine all possible partners who could help deliver the proposed idea, and how they could deliver and receive value.

After consolidating and refining the system of **Value Exchange**, refer to the tips on reciprocity to consider how best to sustain the system:

– **Look at comparable systems**. If it is a new space, look for analogous cases. Undertake an ecosystem analysis, examining value exchanges and the value stack.

– **Determine priorities in the set of objectives**. Examples: do users care more about security or privacy? Which incentives or stakeholders matter more?

8.2.3 Token Utility Canvas[8]

When examining token economies, we essentially look for the merged optimization of two sets of economics, which we call layered economics:

– ledger layer economics
– market layer economics

As the market exchanges digital services, the ledger layer is where key attributes of each transaction need to be verified and simple contracts need to be executed. The main goal of the ledger layer is to drive costs of verification to as low a level as possible, ideally as near to costless as

[6] Source: Heather Fraser - Design Works: How To Tackle Innovation Challenges Through Business Design

[7] In this context, a foundation refers to a non-profit organization established to administer governance over the network.

possible without being free to abuse. Cost reduction and disintermediation are the primary advantages of blockchain-based services over traditional intermediary or audit-based economies where substantial value is lost in the process as economic rent. Common examples of where a token is used to facilitate low cost transactions for digital resources in payments, computation, and data storage are Bitcoin, Ethereum and Filecoin, respectively. We can associate this layer of economics more closely to **protocol tokens**.

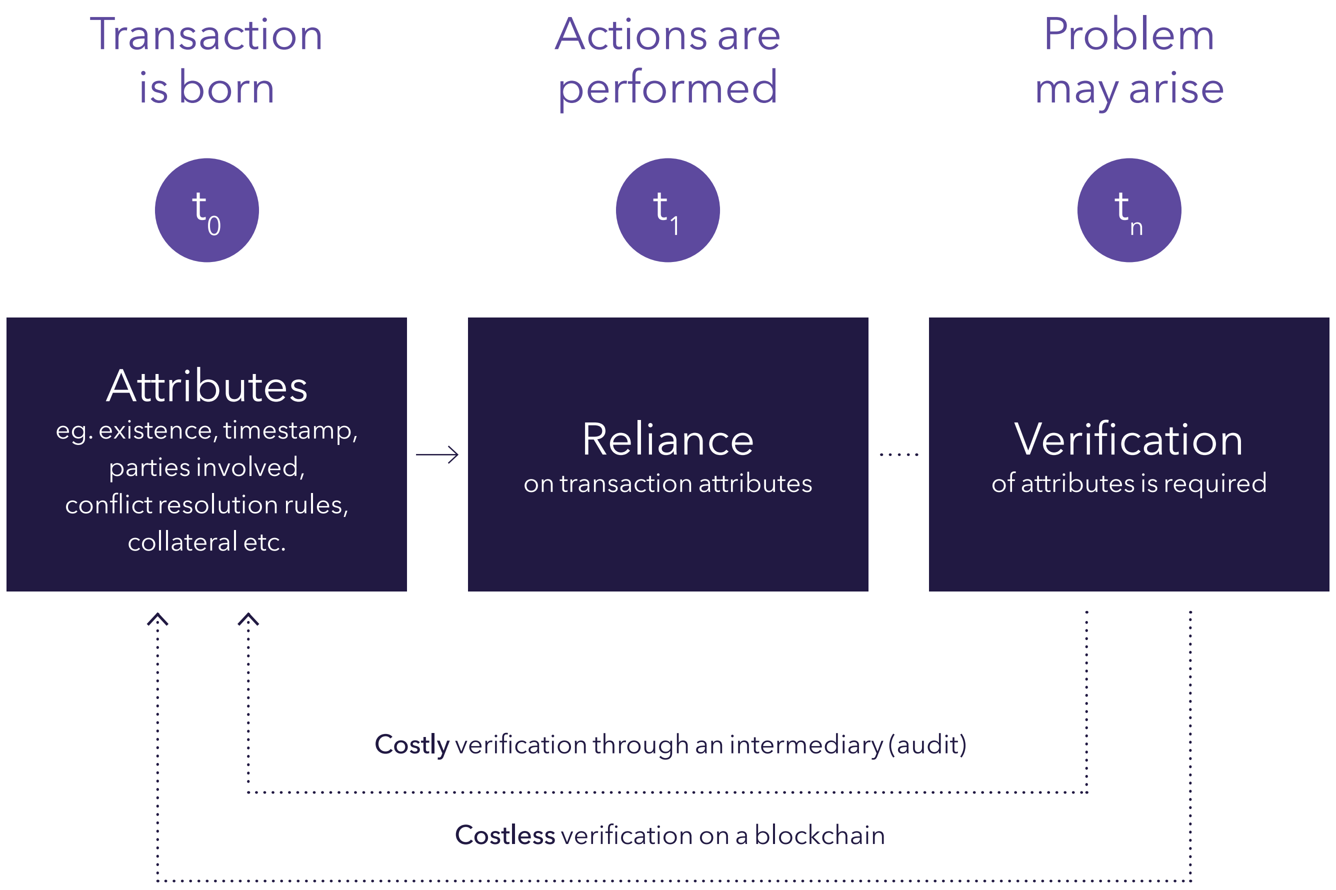


Figure 7: Costly versus costless verification[9]

At the market layer, the economics of the ecosystem are designed to align the distribution of value in order to achieve a more efficient market that also leverages powerful network effects. The token is used as an incentive or disincentive to participants to behave both in their best interests and those of the greater good of the ecosystem at large. This layer is generally exhibited as an **app token**.

Tokens represent an atomic element of a network's business model. In much the same way a business model canvas is used to capture key elements of a venture's business plan, a Token Utility Canvas seeks to outline the utility of a token in its entirety and can broadly be broken out into two sides: **Business Centric Factors** and **Network Centric Factors** as seen below:

[8] This is our version of token utility canvas, alternatives are provided by Consensys "TokenWork:Introducing the Token Utility Canvas (TUC)", Rahul Rumall " Introducing The Protocol Canvas- Designing better decentralized protocols", and Balázs Némethi "Token Engineering Canvas & Agent Behaviour Map+ basics for Token Engineering"

[9] Source: Catalini, Christian, and Joshua S. Gans. Some simple economics of the blockchain . No. w22952. National Bureau of Economic Research, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598

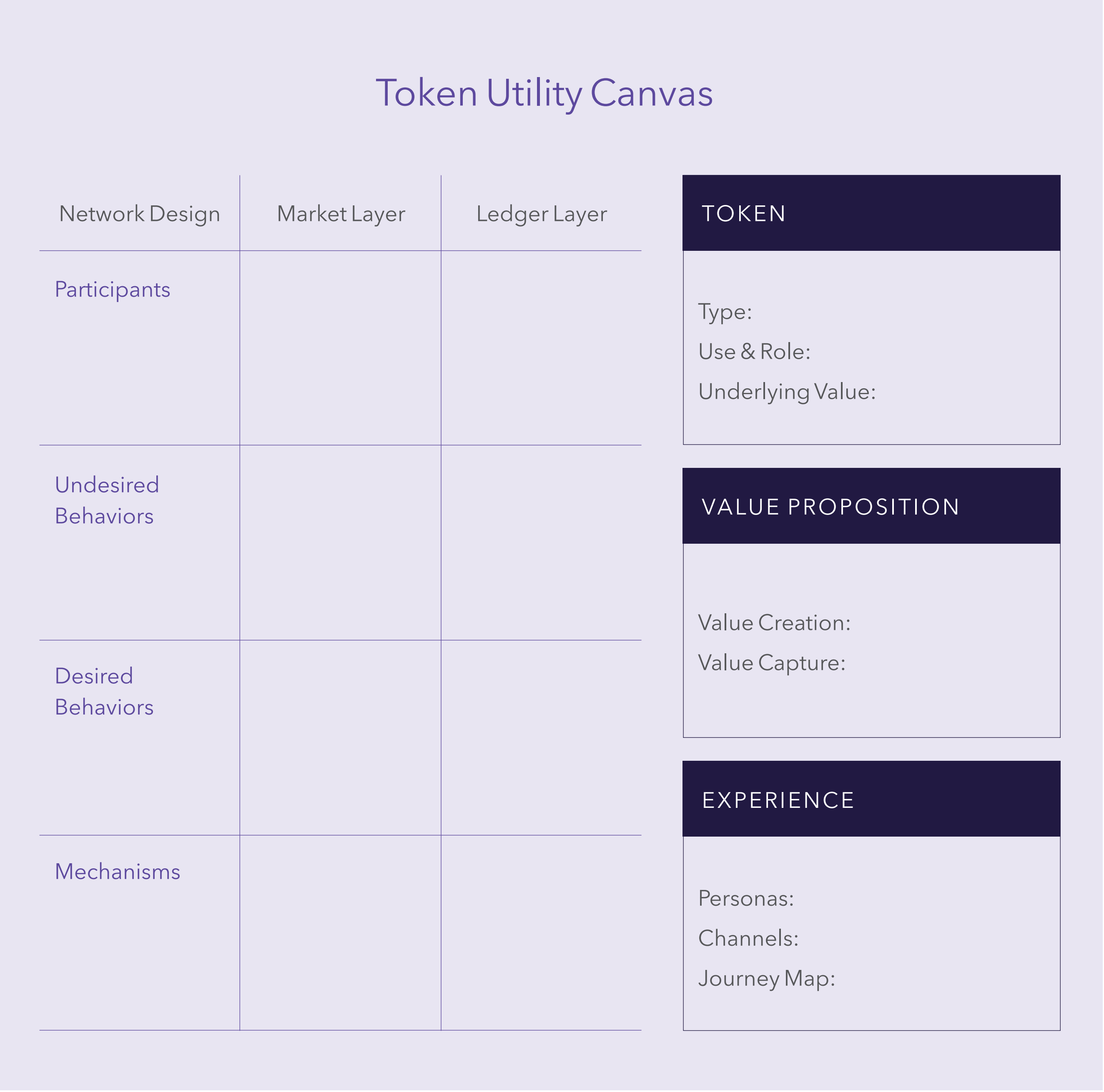


Figure 8: Token Utility Canvas

8.2.3.1 Business Centric Factors (Right Hand Side)

The right hand side of the canvas focuses on the **business-centric** token model and the external factors that will influence the long term sustainability and success of a tokenized ecosystem. It requires us to classify the token in terms of its: type, role & purpose, and underlying value which should help clarify and develop a positioning strategy.

Token Taxonomy[10]

It is important to remember that a token is exactly that, a token. It does not have any value or utility by itself, but instead its value and utility is derived from the underlying asset or service that it represents. Below is a taxonomy adapted from Untitled Inc. that we have found particularly useful.

Token Type: What use does the token provide?

– **Asset Tokens**: cryptographically represent traditional assets, digital assets, or digital commodities. E.g. Tether, GoldMint, Ripple IOUs, CryptoKitties.

– **Usage Tokens:** provide access to a digital service, and can be thought of as a paid API key. Their utility is derived from that of the decentralized digital service. E.g. Bitcoin, Dogecoin, 0x and GRID.

– **Work Tokens**: provide the right to contribute work to a network. Their utility is derived from the decentralized coordination of token holders. E.g. Augur(REP), MakerDAO(MKR), Numeraire(NMR).

Role and Purpose: What is the role of the token?

– **Digital Currency:** this kind of token operates as a frictionless medium of exchange and/or as a store of value. E.g include Bitcoin, Dogecoin, and ZCash.

– **Network Token:** this kind of token provides functionality within a specific network. It can act as a market maker mechanism, or used to control access, provide governance functionality, and/or contribute work to the network. E.g Ocean Protocol, Fetch, and Ethereum.

– **Investment:** this kind of token can be used to invest in the issuing network/entity, or underlying asset, and used to distribute benefits of any success or appreciation. E.g Blockchain Capital's BCAP token.

Underlying Value: What is the value of the token tied to?

– **Asset-backed:** these are generally non-fungible tokens (NFT) representing claims on an underlying asset, and allow for trading of that underlying asset. E.g. CryptoKitties, Digix Global's token (DGX).

– **Network value:** these tokens are tied to the value and development of the network and linked to key interactions between network participants and the value exchanged over the network. E.g. Ethereum, Ocean, and Fetch.

– **Share-like:** these tokens grant rights to a share in the success of the issuing entity or underlying asset. E.g. the short-lived DAO token.

Value Proposition: How value is created and captured?

This is one of the ecosystem's distinguishing factors. Focusing on the ecosystem's value proposition helps the token design meet key value drivers, while also aiding in the clear external communication of its value to potential network participants.

Experience/Service Design:

Experience design takes a holistic approach to a system's value proposition by putting the user front and centre, while providing an actionable opportunity assessment. This type of design methodology is the rationale behind the iterative process of token ecosystem creation, and capturing the quantitative and qualitative aspects of users' needs, habits and motivations is a crucial part of this process.

8.2.3.2 Network Centric Factors (Left Hand Side)

The left hand side of the canvas focuses on the **network-centric** token model and the internal factors that will influence the long term success and sustainability of the ecosystem. This section of the canvas breaks down subsections into **ledger** and **market layers**, a useful classification for tokenized ecosystems.

– **Participants:** What roles do stakeholders need to occupy in each layer?

– **Undesired Behaviors:** What are the incentives for each role, absent of any mechanism?

– **Desired Behaviors:** What are the desired behaviors of each role within the ecosystem?

– **Mechanisms:** What are the planned mechanisms to bridge the gap between each role's incentives and desired behaviors?

Example: Ocean Protocol Utility Canvas

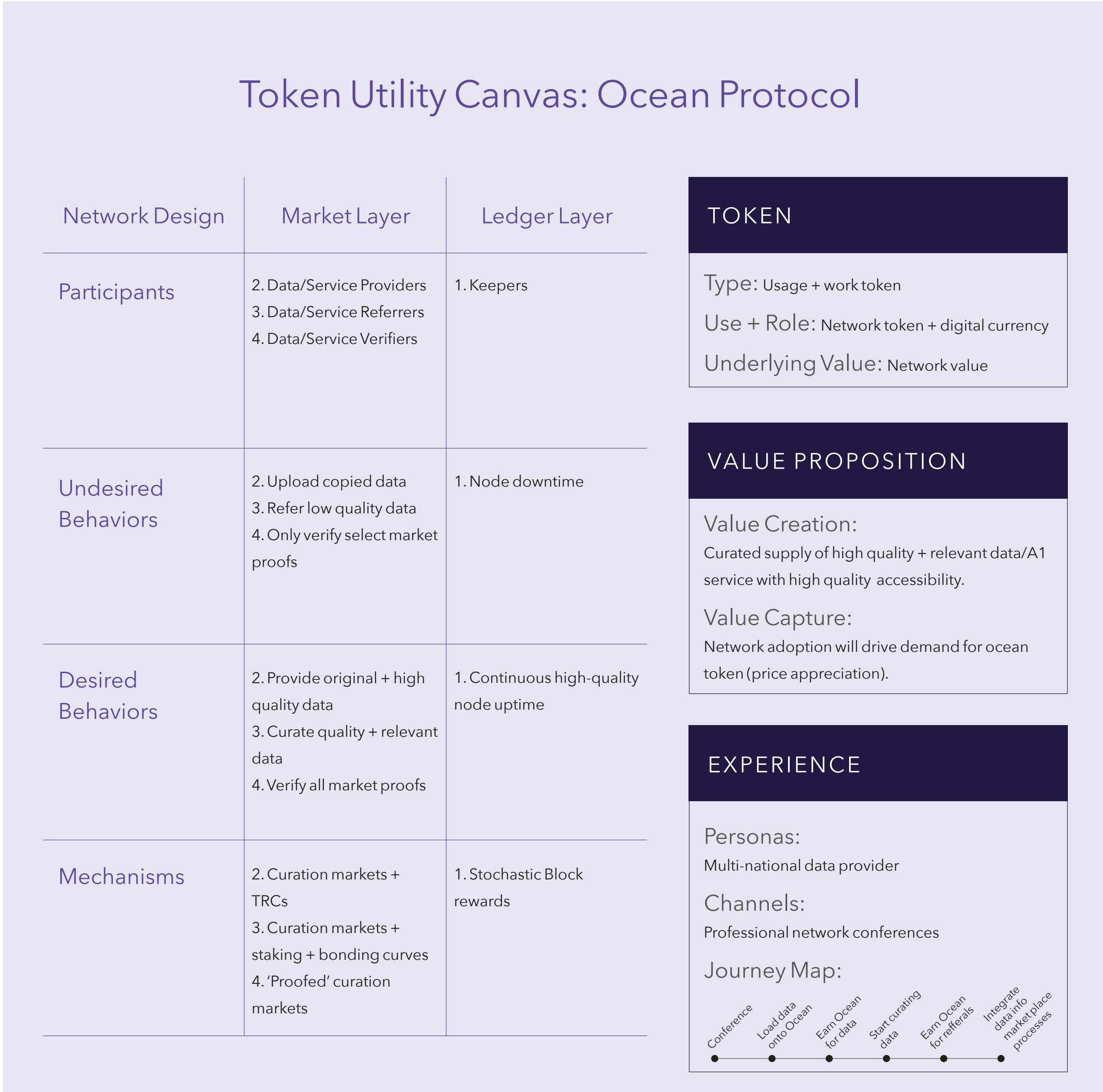


Figure 9: Ocean Protocol Utility Canvas

[10] The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens, http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/

8.3 Key Outputs

Working through these methods during the Discovery Phase, we should establish a number of objectives (both business and/or social) and system requirements including:

8.3.1 Problem Structuring Output: Business Objectives and Network Requirements

Defining business objectives are critical to determine a 'go forward' ecosystem strategy that can be effectively communicated to the Crypto-economic team, helping direct token design and engineering efforts in later phases.

- MECE Problem Tree: Besides providing a clear visualization of the problem for easy reference, structuring the problem into a logic tree will efficiently map to the technical system requirements and increase the effectiveness in communicating requirements to the engineering team.

8.3.2 User Research Output: Taxonomy of Actors v1

Defining user taxonomies is critical to extract who the participants are in the network. The aim is to understand with great detail every role in the network that needs to be properly incentivized.

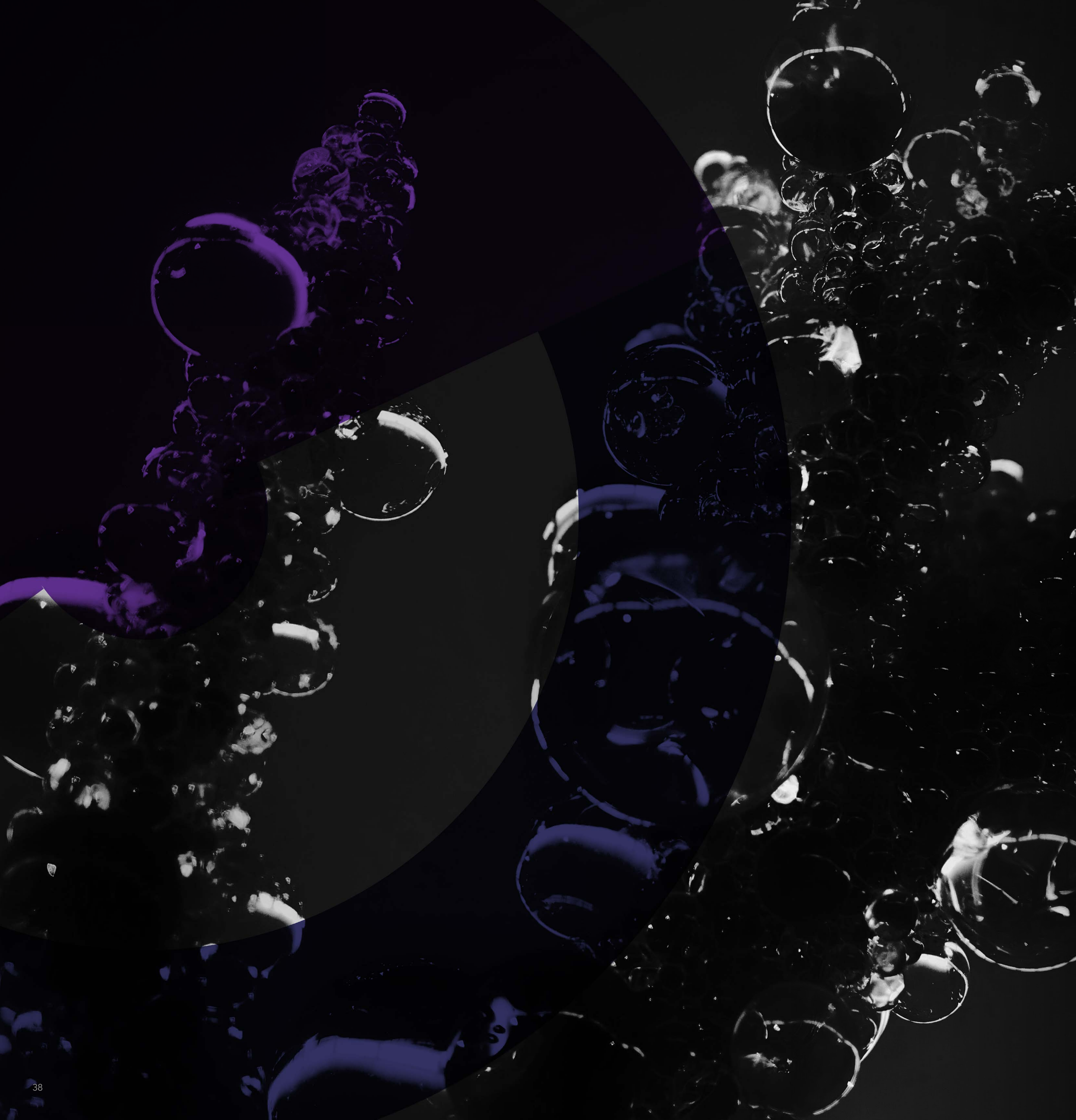
- Stakeholder Maps: Getting a clear picture of the network's participants and their respective roles is a critical exercise in any token design. We should pay close attention to understanding each role clearly to recognize how they can be individually incentivized to undertake desired activities and disincentivized from stepping beyond boundaries.

- Value Exchange Maps: The focus should be on capturing and visualizing how value is created and captured within the tokenized ecosystem.

8.3.3 Token Utility Canvas

The Token Utility Canvas (Section 8.2.3) takes a holistic view of token design, mapping the requirements of the network to the business and the end users.

- Initial utility audit report (Token Utility Canvas): Sets a baseline level of token utility, and is a useful tool to start framing the system requirements.



Chapter 9

Design Phase

Token design is an emerging concept that consists of building an ecosystem surrounding the market or the business model that an entity is trying to operate in or create via the use of blockchain technology. It is an extremely complex task, comparable to designing and launching a completely new economic structure. The key is to keep the design and the underlying token architecture as simple as possible, and minimize one's assumptions about agents' behaviors because even very simple structures can lead to extremely complex interactions and outcomes. Accordingly, overloading models with assumptions would not only restrict their capability but also increase error and overall system fragility.

SKILLS REQUIRED
Mechanism Design/Game Theory, Market Design, Behavioral Economics, Blockchain/DLT Architecture, Systems Engineering, Network Science

9.1 Design Inputs

Token design requires an understanding of the **incentives** for each participant in the ecosystem, the associated business model, the market structure, and the network structure. The final model leads to a protocol design that should allow the network to sustain itself in a healthy manner while prioritizing system safety by correctly engineering incentivization and disincentivization mechanisms. There may exist multiple solutions for any given problem but the goal of token design is to try to identify the optimal solution while taking associated constraints into account. The outputs from the **Discovery Phase**: *namely the MECE Problem Tree, Token Utility Canvas, Stakeholder and Value Exchange Maps* are now brought into the **Design Phase** and iteratively improved to create the most critical input of the current phase, that is the Taxonomy of Actors.

CONCEPT

An **incentive** is something that makes people act in a particular way and is central to the study of economics. In our context, we use it to achieve mutual gains when parties have differing motivations and/or degrees of knowledge.

9.1.1 Taxonomy of Actors v2

Reexamining the list of potential network participants and creating a more detailed version of the **taxonomy of actors** first derived during the **Discovery Phase** is the first crucial step in the token design process in order to determine for whom the network is being designed. Using the **stakeholder mapping** and **value exchange mapping** from the Discovery Phase, the token architect needs to dig even deeper to not only just identify all the agents that will participate in the network, but also their specific roles within the economy and how they all influence each other with a greater accuracy given different state spaces. For example, an irrational player would have different incentives from a boundedly-rational player, who in turn may behave differently from an autonomous agent. Moreover, the composition of the overall population may lead to differing outcomes. Construction of this version of taxonomy of actors is not necessarily very different than the first version, but requires a detailed understanding of the overall population and its potential evolution.

It is crucial that a network analysis should distinguish between direct and indirect participants who may both be present in the stakeholder map; however, these participants have different levels of influence on protocol design. Defining participants' roles and user flows (such as the direction of interactions/communications within the network) will influence strategic interactions among network participants, which in turn affect the network (and hence the ecosystem's) outcome. Finally, determining network participants and their roles is a critical dependency for the next step of defining the **network's objective function**, which is the most important output of the Design Phase. Without defining a full picture of network participants and their roles, we can neither define the metrics that would determine network success such as user engagement or other payoffs, nor the constraints of our problem.

The Network Objective Function is the primary objective we want the network to optimize for above all else, and helps us aggregate the different goals of a particular network depending on their relevant importance. Equally as important as a network's objective function are the model's constraints, a requirement in the design of safe systems.

CONCEPT

Example[11]: Ocean Protocol 's objective function is to maximize the supply of relevant AI data and services. Ocean's token architects use this goal to direct all other token design decisions. The key tool used by Ocean to incentivize behavior around this objective function is through the introduction of block rewards with the following properties:

*Block Rewards = (predicted popularity of dataset/service) * (actual popularity or dataset/service) * (actor reputation)*

$$R_{ij} = \log10(S_{ij}) * \log10(D_j) * R_i$$

R_{ij} : block reward for actor i on dataset/service j
S_{ij} : actor i' s stake in dataset/service j, measured in drops
D_j : number of deliveries of dataset/service j in the block interval
R_i : the global ratio of actor i serving up vs accessing a dataset

[11] Ocean Protocol's Technical White Paper https://oceanprotocol.com/#papers

Steps involved:

1. **Identify all potential network participants.** By developing user/participant profiles and personas we can attempt to uncover participant motivations and objectives. This step is crucial because it allows us to understand the dynamics driving the actions of different types of agents - be they autonomous, irrational or partially rational humans or malignant - according to different objective functions.

2. **Define and analyse the respective roles and strategy profiles of network agents.** This shows us what actions each participant can take and each participant type's utility function. This step also allows us to figure out the participants' self-interest vs. the best interest of the network (for example, overall ecosystem performance).

3. **Define multi-directional relationships, and hence strategic interactions in the network.** This is to decide what extrinsic and intrinsic value transfers can be expected within the ecosystem. We need to determine the possible resulting outcomes of these strategic interactions, and see if they are compatible with the overall aim/health of the network.

4. **Define population characteristics that are likely to arise.** For example, which level of rationality/ thinking are the participants likely to exhibit?[12] Which proportion of the population is likely to show altruistic or malignant tendencies?

5. **Whiteboard the system.** Create a visual representation of the network game including the participants and their roles we defined in previous steps.

Example: Taxonomy of Actors for SEED[13]

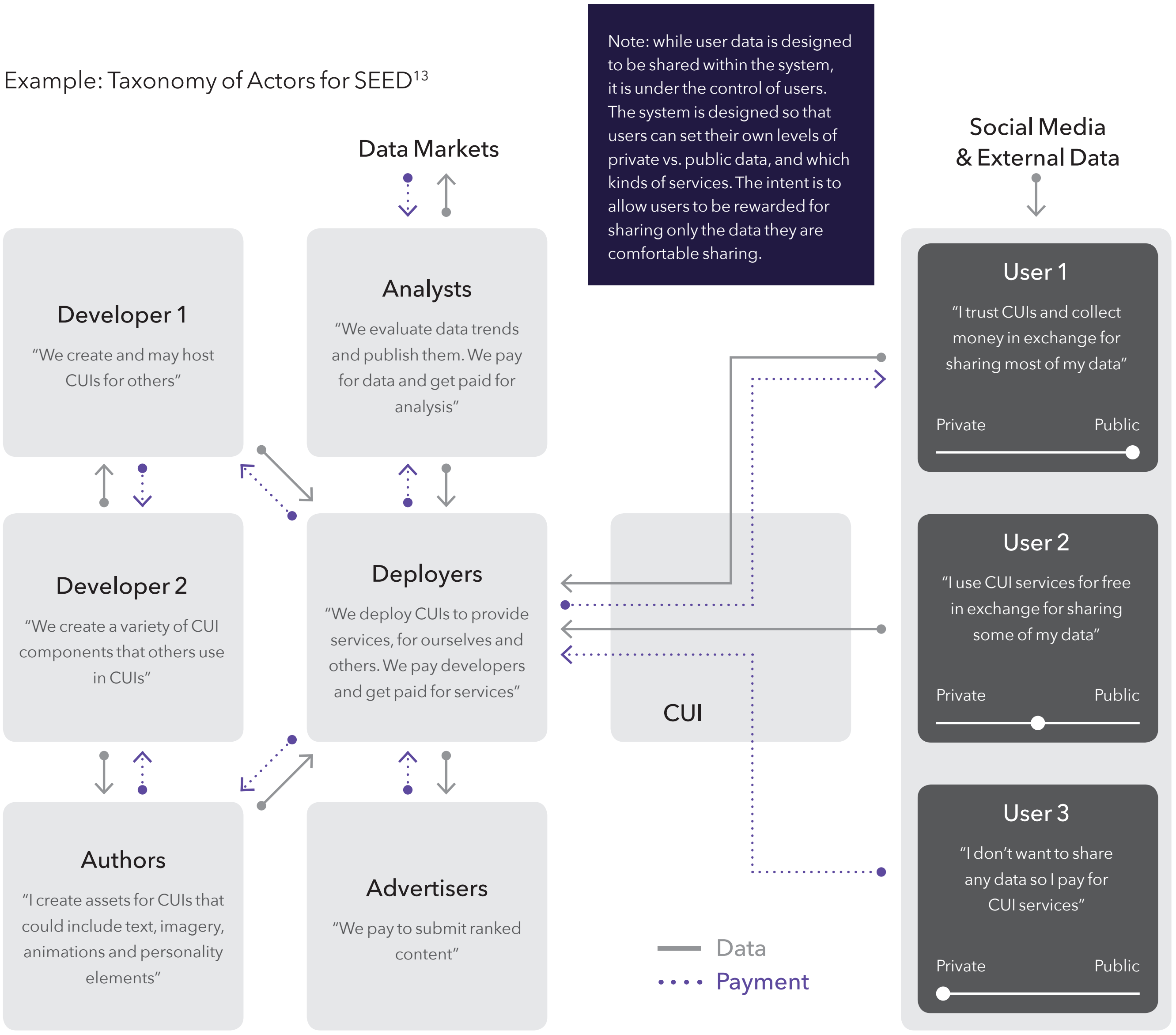


Figure 10: Taxonomy of actors for SEED.

9.2 Design Tools

Tokens aim to allow ecosystems to self-coordinate and self-manage in an efficient manner. For this purpose, *game theory, mechanism design and behavioral economics* are particularly useful tools in addition to a good understanding of cryptography.[14] To keep track of the overall design process we also suggest the usage of traditional tools such as a **GANTT Chart** and **Javelin Board**.

9.2.1 GANTT Charts

A token design GANTT should be used internally by all the members of the crypto-economics team throughout the token design process to manage resources and timelines and is a complementary tool (as seen in Appendix Figure 29). We can utilize this tool for planning the timelines at a higher level; but can also generate sub-system level or multi-layered charts.

9.2.2 Javelin Board

A Javelin Board, shown below, is helpful to track and validate assumptions and ideas and is broken up into two sections. All model assumptions are listed on the left hand side of the board. To the right of this column, we track the experiments and tools testing our assumptions. This board is similar to the Token Utility Canvas (see section 8.2.3) but focuses on creating a mapping from our assumptions, and the token structure to the most viable testing mechanism. Please find an empty template in Appendix Figure 31.

[12] Please refer to various studies on level-k thinking and Keynesian beauty contest games.

[13] An Independent Bot Economy for a Trusted AI Future, https://static.seedtoken.io/downloads/SEEDWhitePaper.pdf pg 25

[14] Refer to some seminal works to understand economic and social networks (Jackson, Matthew O. Social and economic networks. Princeton university press, 2010.); and, algorithms for self-organising network systems (Olfati-Saber, Reza, J. Alex Fax, and Richard M. Murray. "Consensus and cooperation in networked multi-agent systems." Proceedings of the IEEE 95.1 (2007): 215-233.)

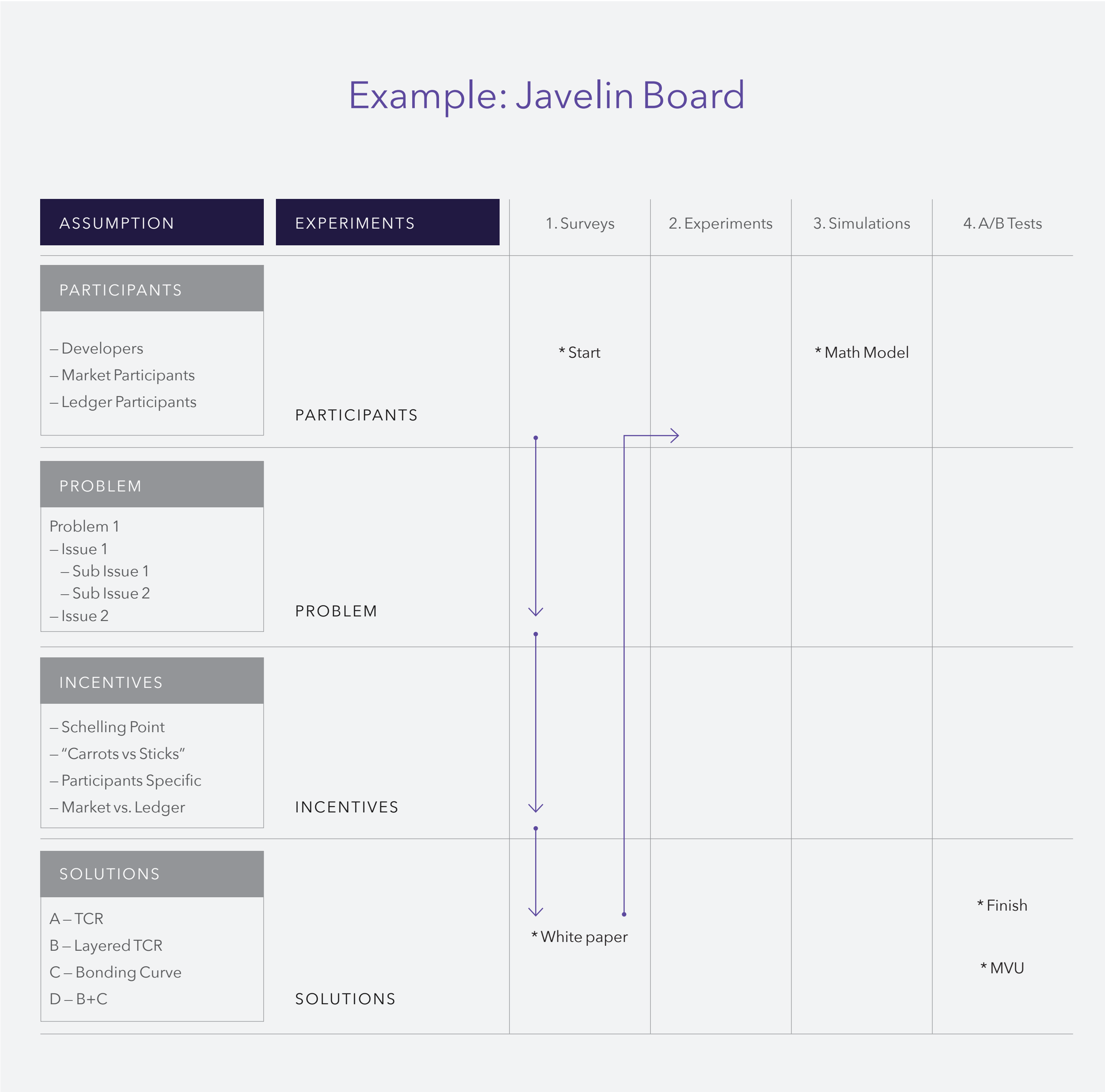


Figure 11: Javelin board example.

Assumptions: Here, all assumptions regarding the token model should be clearly laid out. Using a whiteboard and post it notes allows for quick revisions and iterations. Below is a description of each section and which assumptions should be included on the board to be tested.

1. **Participants.** Who are the network participants? Break them down by market and ledger layers.

2. **Problem.** Break the problem into two components: core problems (macro, market gap/opportunity, competition), and periphery problems (micro, technical, user specific, design problems).

3. **Incentives.** What is the **Schelling Point?** (equilibrium with zero communication/ coordination), distinguish and classify incentives and penalties (carrots and sticks). Distill incentives down to specific participants, and specific roles within the market and ledger layers.

4. **Solution.** This deals with actual token design, the idea is to break design into its most basic components and then test all combination of design primitives.

Schelling Point (also called focal point), a concept of game theory, is a solution that people will tend to use in the absence of communication, because it seems natural, special, or relevant to them.

CONCEPT

Experiments:[15] In this section, every assumption in the above category needs to be validated through experimentation. Experiments should be run sequentially from top to bottom and from left to right:

1. **Moving from top to bottom**. The results from testing down through Participants → Problem → Incentives → Solution all feed into the next sequence of experiments and mark the creation of the first interactive feedback loop in the token design. This feedback loop is critical and should be present across all stages of the token design.

2. **Moving from left to right**. Experiments gradually become more sophisticated and specific, starting with simple surveys, then moving to experiments, modeling and simulations, and then A/B testing.

9.2.3 Game Theory

Game theory is the study of multi-person decision problems and a crucial tool in the token design process, since it helps us determine the outcomes from strategic interaction of players given their preferences and incentives. Unlike **decision theory** that is concerned with the individual's own preferences and constraints, game theory is about interactive decisions and shows us how players can make decisions in competitive and/or cooperative environments.

Constructing multi-agent systems requires us "to design local control laws for the individual agents to ensure that the emergent global behavior is desirable with respect to a given system level objective" (Li & Marden, 2013)[16]. The token architect should fulfil this objective with the least amount of assumptions possible about an agent's behavior. In many token use cases, self-interests of the network participants are in direct contrast to the interests of the network as a whole. Moreover, stakeholders' incentives are not always aligned. Therefore, game theory is an extremely useful tool that can help the token architect understand the underlying drivers that disincentivize cooperation within a particular ecosystem, and better design

[15] Please see below (Section 9.2.5) for a more detailed discussion on experiments.

[16] Li, Na, and Jason R. Marden. "Designing games for distributed optimization." IEEE Journal of Selected Topics in Signal Processing 7.2 (2013): 230-242.

a token that aligns participant incentives among themselves and with the objectives of the network. For example, Li & Marden (2013)[17] offers a game theoretical methodology on multi-agent behavior to ensure that the resulting structure is robust to uncertainties that can arise in the future.

Additionally, expected utility theory allows us to convert preferences into outcomes and rational decision-making implies that agents will seek to maximize their expected utility over outcomes. Even though most of the famous applications of game theory and expected utility theory deal with rational and selfish agents, revealed-preference based utility theory does not necessarily imply 'narrow selfishness', and it is possible to include a non-selfish factor such as altruism, or fairness concerns into these models. Moreover, behavioral economics (discussed below) improves upon these tools further with findings from psychology.

9.2.4 Mechanism and Market Design

Mechanism Design is the art of designing the rules of a game to achieve a specific desired outcome. While game theory takes the rules of the game as given and helps us determine outcomes based on them and the strategic interaction of players, mechanism design uses the framework of game theory with incomplete information and asks about the consequences of different rules and chooses the game structure rather than inheriting one. Therefore, in our context, mechanism design allows us to look at the overall design of the network and participants' incentives as a way to influence the outcomes of the network game in addition to determining the optimal design of the network itself.

To set the rules of the game, we first need to define the environment we are considering and the actors participating in the game. This involves describing who the participants are, the set of potential decisions, the set of preferences for each participant, and any private information that they may hold to understand information asymmetry. For this exact reason, **taxonomy of actors** is the main input of the design phase. The utility of a well-designed token will create powerful incentives that drive activity in the network; therefore, understanding how a token's utility actually drives behavior is a critical aspect of token design process.

Market design involves designing a market structure to achieve a set of desirable properties. Each market has its own specific requirements but generally speaking, exchange environments need to be designed in such a way to facilitate efficient outcomes. The design of the market needs to allow enough potential transactions to be available at one time so that a particular type of agent does not possess the power to influence the market on its own. Additionally, there needs to be enough time for offers to be made, accepted, rejected, and for transactions to be carried out. Finally, it should be safe for participants to reveal their preferences truthfully.[18]

9.2.5 Behavioral and Experimental Economics

Behavioral economics studies economic questions while incorporating learnings from psychology, and **experimental economics** helps us test our assumptions and findings.

Traditional economic models assume that agents behave rationally and have a full understanding of their environment, their potential strategic choices and the consequences of their actions. However, psychological findings have shown us that human beings have limited cognitive abilities, lack motivation and self control. Additionally, their preferences, choices and behavior maybe non-standard, meaning human beings may not always behave efficiently, and in fact, their behavior may change based on a reference point, as well as the context they are in. Even the best chess players in the world may not always optimize their actions, and match outcomes can be unpredictable.[19]

Most importantly for our framework, behavioral economics highlights the fact that seemingly insignificant factors can have huge effects on people's decisions, i.e. **frames** do matter. Therefore, when designing a token, the way the token's functionality is presented to participants is perhaps equally important as the actual mechanisms themselves, which can be very crucial for the token architect.

Experimental methods help us isolate key causal relationships between business environments, agent behavior and consumer choices, and help us eliminate irrelevant effects by controlling for them. With the right design, it allows us to focus on one aspect of our problem and measure the effects of specific factors.

In an **experiment/randomized control trial (RCT)**, participants are randomly assigned to treatment (where they receive the intervention) vs. control groups (where they do not receive the intervention). Randomization is crucial as it allows us to compare the effectiveness of a treatment objectively. Using the right treatments and controls, we can get robust causal inference. In this setting, a smaller and simpler version of the a project's economy/interactions can be replicated with multiple users taking various representative roles within the network. In each treatment, we can change one single factor to determine how this would affect participants' incentives, hence their behavior and the whole ecosystem. Potential implementation fields for experimentally testing a specific behavior include MTurk and Experimental Labs . An additional option is to look at empirical data provided by existing networks, and if possible, identify and analyse natural experiments within them.

9.2.6 Cryptographic Primitives

Cryptographic design tools are the building blocks of any token model. When starting to design a token model, knowing the Schelling Point of a network is a key first step. From that point, a simple cost-benefit analysis requires that the complexity and cost of adding any additional mechanism should be proportionally less then the added coordination.[20] The risk is that the added complexity could negate the benefits from the increased coordination; hence, this relationship should be well understood during the design process. The token architect should limit the design of the **Minimum Viable Token (MVT)** to the simplest design possible.

Many of the proposed cryptographic tools listed below have been subjected to a limited amount of testing by the community, and these tools could become 'trusted' through the **deployment phase** of the token design, which consists of validation and testing. Therefore, when designing a token model, in particular the MVT, the network designer should focus on utilising minimal combinations of the tools below that can be initially 'trusted'.

Minimal Viable Token for our purposes is the simplest but most effective design possible to deliver upon the **Objective Function**, within a system's set constraints, determined during the token design process.

CONCEPT

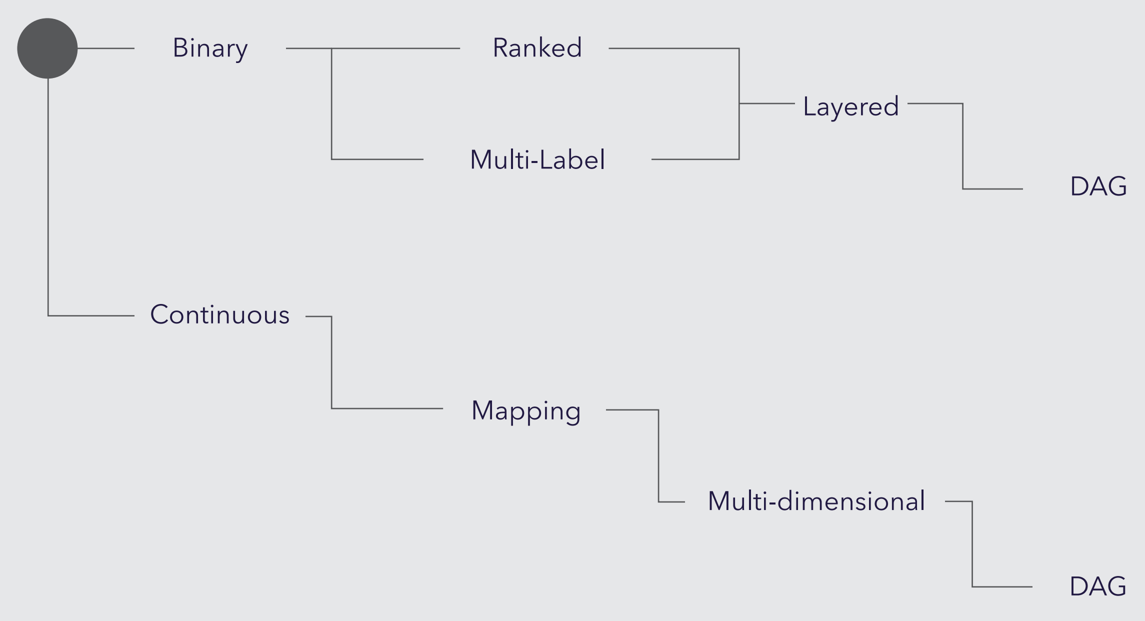
[17] Ibid.

[18] Please see Al Roth's page for a collection of useful market design resouces https://web.stanford.edu/~alroth/alroth.html

[19] Thaler, Richard H. "Behavioral economics: past, present, and future." *American Economic Review* 106.7 (2016): 1577-1600.

[20] Simon de la Rouviere, Does your dapp need a token? https://medium.com/@simondlr/does-your-dapp-need-a-token-39412fd3c62c

Curation



Discrete Membership	
Binary Membership	Token Curated Registry (TCR)
Ranked Membership	Graded TCRs[23]
Layered Membership	Layered TCRs[24]
DAG Membership	Stake Machines[25]
Continuous Membership	
Continuous valued membership	Curation Markets - Bonding curves[26]
Hierarchical membership	Each label has a TCR
Turing Complete	Bonding scripts
Work tied to membership	Curated Proofs Market (CPM)

Proofs[27]

Human Work
Proof of content creation
Proof of human oracle
Proof of team coordination
Machine Work
Compute machine work
Data
Proof of Space-Time
Proof of Data Availability
Proof of Replication
Proof of Service Receipt
Processing
Non-interactive
Zero-Knowledge (ZK) Proofs
ZK-SNARKS
ZK-STARKS
Bulletproofs
Interactive
Probabilistic checkable proofs
Full homomorphic encryption
Multi-party compute
Secure Enclaves
Trusted execution environment
Hardware security module
Compute service receipts
Solving domain specific puzzles
Deterministic compute puzzle
Stochastic compute puzzle
Physical Machine Work
Human or Machine Work
Proof of Location
Proof of Time
Proof of moving atoms
Generalised proof wrappers/interoperability

Identity[28]

Lower Level Blocks
Public key
Decentralized identifiers (DIDs)
Medium Level Blocks
Token Curated Registries (TCRs)
Verifiable Claims

21 http://tokenengineering.net/building-blocks

22 Dimitri De Jonghe, Ocean Protocol, https://docs.google.com/presentation/d/1Y_d-pqBdhby1Y2nLA1vtoFDZxcd-R9lQQSVWzP9QTFE/edit?usp=sharing

23 Sebastian Gajek, Graded Token-Curated Decisions with Up-/Downvoting – Designing Cryptoeconomic Ranking and Reputation Systems, https://medium.com/coinmonks/graded-token-curated-decisions-with-up-downvoting-designing-cryptoeconomic-ranking-and-2ce7c000bb51

24 Trent McConaghy, Dimitri de Jonghe, Fang Gong, The Layered TCR, https://blog.oceanprotocol.com/the-layered-tcr-56cc5b4cdc45

25 Dimitri De Jonghe, Curated Governance with Stake Machines, https://medium.com/@DimitriDeJonghe/curated-governance-with-stake-machines-8ae290a709b4

26 As explained by Justin Goro " Token Bonding Curves Explained " a bonding curve contract issues its own tokens through buy and sell functions and they are not only limited to curation markets but relevant for any market with dynamic pricing.

27 http://tokenengineering.net/proofs

28 http://tokenengineering.net/identity

9.2.7 State Channels and Scaling Solutions

One of the challenges of many early generation blockchains is scalability. In Ethereum, every transaction has to be processed by every single node in the network and paid for, putting a ceiling on throughput below parameters needed for mass adoption.[29] The community is racing to solve Ethereum's scalability solutions; and with a growing view that Ethereum's mainnet should be a cache of very simple programs and pointers, developers are working on off-chain scalability solutions.[30]

Off-Chain Solutions

Off-chain solutions are trying to answer the question of how to extract more transactions from a protocol's existing capacity.[31] Within our framework, we can define these solutions as deploying a market layer that can bundle transactions on top of the ledger layer. As a result, the cryptoeconomics of these scaling solutions are strongly dependant on creating the proper incentive structures and limited by the throughput of the underlying chain's consensus protocol, which it relies on as its anchor of trust.[32]

State Channels[33]

Pioneered by Jeff Colemen, State Channels started off as payment channels for Bitcoin, and are now used as general off-chain payment channels on Ethereum. They operate by locking a portion of the underlying (parent) chain's state using multisig and rely on participants to update the state amongst themselves before submitting back to the underlying chain. Some limitations of State Channels include:

– They can only be used for interactions that involve many transactions over a long period of time in between.

– They rely on constant participant connectivity.

– The token architect needs a clear definition of participants and their incentives because attack vectors are quite large.

Plasma[34]

Introduced by Joseph Poon and Vitalik Buterin, Plasma is a scalable "framework for incentivise and enforced execution of smart contracts".[35] Using the properties of merkle trees (Figure 13) to efficiently and cryptographically compress state changes to be later queried and registered on the underlying chain, Plasma proposes a method for decentralized applications to scale despite Ethereum's fixed capacity.[36] Plasma expands on State Channels by allowing for more complex state changes (smart contracts) to be run and confirmed off chain.

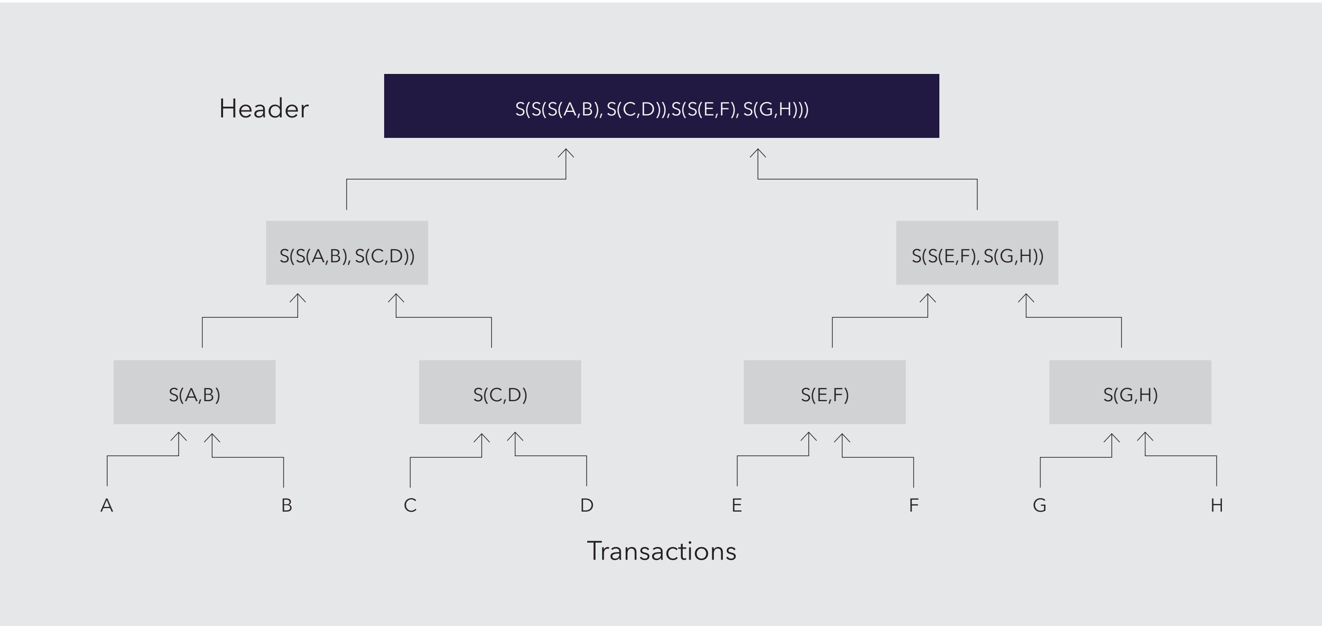


Figure 12: Visualization of a Merkle tree [37]

Relay Networks[38]

Relay networks are very similar to Plasma in that data is packed efficiently using merkle trees, that is, a merkle root for a set of consecutive block headers is relayed, instead of each transaction. However, they differ in one particular aspect. Trustless relay networks, proposed by Alex Miller, replaces the centralized relayer of Plasma with a decentralized relayer powered by a network of token stakers. Relay networks thus rely on creating proper incentives for token holders to stake their tokens, such that they can be trusted to run a relayer.

TrueBit[39]

TrueBit won't allow Ethereum to increase its number of transactions, but will allow Ethereum to perform more complex things, at scale. TrueBit seeks to provide a worldwide computation market that can provide trustless computation. To provide Ethereum with a scalable verification mechanism, TrueBit heavily relies on creating incentives to influence desired behavior of all network participants.

For many early generation blockchains, scalability has been a prominent issue that has yet to be solved in a meaningful way. Projects have flooded to Ethereum launching unscalable DApps, where in fact, adding new users to a DApp built on top of Ethereum immediately scales cost and slows settlement times, exhibiting qualities of diseconomies of scale.[40] Many have pointed out (Fred Ehrsam, Vitalik Buterin, among others), that "incentives for core protocol and second layer infrastructure" are pretty low. This is a classic example of the **innovator's dilemma**. So while existing protocols seek to scale up throughput, new protocols exhibiting scalable throughput and economies of scale continue to emerge. The risk is that these new emerging protocols may not set up the proper incentive structures to encourage continued innovation.

9.3 Design Process

The design process starts by identifying decisions regarding the entire token ecosystem and focuses on finding **Token-Network Fit** to inform design choices for each subsequent level. Once the requirements of network participants are determined at the ecosystem level and subsequently at small systems level, we can start to recursively build our token infrastructure. In other words, the higher level design of the token will have to meet the needs of the market(s) it is facilitating, which in turn should fit the protocol design that is required for the network nodes to sustain the ledger in a healthy manner. However, this process may have to be re-iterated once the requirements of the subsequent levels are finalized.

This process requires a focus on **Ledger-Market Fit** as well, discussed in section 9.3.1. Additionally, **governance** structure regarding consensus mechanisms and token supply needs to be determined based on the requirements of the market and the ledger along with its associated financial necessities and constraints.

29 Josh Stark, Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit, https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

30 Alex Miller, Introducing Trusted Relay Networks, https://blog.gridplus.io/introducing-trusted-relay-networks-6c168f72a6f6

31 Josh Stark, Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit, https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

32 Josh Stark, Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit, https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

33 Jeff Coleman, State Channels, https://www.jeffcoleman.ca/state-channels/

34 Joseph Poon, Vitalik Buterin,Plasma: Scalable Autonomous Smart Contracts, http://plasma.io/plasma.pdf

35 Joseph Poon, Vitalik Buterin,Plasma: Scalable Autonomous Smart Contracts, http://plasma.io/plasma.pdf pg 1

36 Consensys, Ever Wonder How Merkle Trees Work?, https://media.consensys.net/ever-wonder-how-merkle-trees-work-c2f8b7100ed3

37 Alex Miller, Plasma and the Internet of Money, https://blog.gridplus.io/plasma-and-the-internet-of-money-ccf7d5e8c3be

38 Alex Miller, Efficiently Bridging EVM Blockchains, https://blog.gridplus.io/efficiently-bridging-evm-blockchains-8421504e9ced

39 Josh Stark, Making Sense of Ethereum's Layer 2 Scaling Solutions: State Channels, Plasma, and Truebit, https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-plasma-and-truebit-22cb40dcc2f4

40 The Great Filter: Why You Shouldn't ICO on Ethereum, https://blog.stellarx.com/the-great-filter-why-you-shouldnt-ico-on-ethereum/

41 Laim Horne, Generalized State Channels on Ethereum, https://medium.com/l4-media/generalized-state-channels-on-ethereum-de0357f5fb44

Token-Network Fit is analogous to product-market fit. Finding the right token model for the network means creating the correct mechanisms that align incentives across the market and ledger layer such that everyone acts in the best interest of the network. It is useful to view the token as the interface between the ledger and the market layer.

CONCEPT

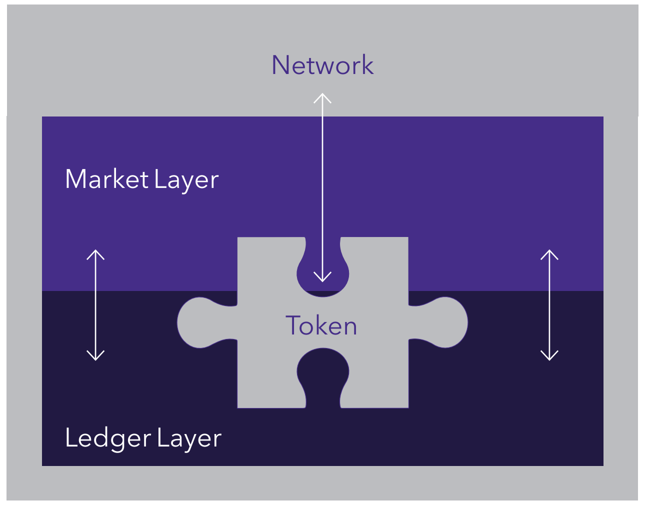


Figure 13: Token-Network Fit & Ledger-Market Fit

The token is the interface of the network, enabling the network between the ledger layer and the market layer in its entirety.

Ledger-Market Fit refers to the computational and technical feasibility of running a particular market, its requirements and offerings, on a particular ledger. This will dictate what elements can and should be on- and off-chain, and determine to what extent the ledger is purely a settlement layer.

CONCEPT

9.3.1 Incentives and Mechanisms

As discussed, a component of the design process is the **Ledger-Market Fit**. For this, it is useful to visualize tokens operating in between two distinct but complementary layers, namely the market and ledger layers. On the one hand, the market layer is where the network participants interact and transact (sometimes off-chain), hence, this is where we formulate and/or incorporate the business' model/s by taking into account network effects and externalities. On the other hand, the ledger layer is where all the necessary transactions and/or other relevant information are ordered and recorded.

Token models act as the interface between these two layers, limiting and incentivizing behavior in the market layer, and acting as the sensor funnelling data onto the ledger layer to be recorded. To design for Ledger-Market Fit, the network architect needs to determine the needs of the market and the business model, induce participants to reveal their preferences and/or hidden information truthfully in that market, and create the correct incentives in recording in and sustaining the ledger itself. This requires understanding the constraints and computational feasibility of running a specific market on a particular ledger.

9.3.1.1 Participant Incentives

As mentioned before, incentives aim to induce network participants to act in a particular way in an economic or business setting and hence play a crucial role in any economic or contractual relationship. In a setting where participants in the network have differing goals and possess varying degrees of knowledge, optimal allocation of resources and mutual gains are only attainable with the right design of incentive mechanisms.

One should denote that, participants can partake in the token ecosystem either via interacting with each other at the market layer or by becoming nodes to sustain the ledger layer, or both. Relying on correct assumptions about the possible types and designing the right incentives matter at both those layers. For example, the team designing the network will need to determine who will be the network nodes, [42] what information or type of transactions should go into the ledger, what type of identity management should be used for which type of ecosystem activity and whether different types of participants needs be treated differently.

Accordingly, it is important to remember the rationality level of different types of participants in the network can vary greatly (for example, rationality of AI versus different types of individuals may differ significantly) and its effects on the ecosystem should be tested or simulated. Development of token ecosystems, decentralized networks and advances in the AI, may "enable AIs to collaborate and coordinate processing in a decentralized way"[43] and eventually result in more prominent use of **autonomous economic agents (AEAs)**[44]; therefore, testing the relation between varying types of participants and ecosystem outcomes may become even more prevalent in the near future.

[42] For example, does the MVT require a permissioned or permissionless system for the ecosystem to thrive?

[43] The Convergence Ecosystem p.53

[44] In fact we already have some examples https://medium.com/block-science/exploring-cryptokitties-part-2-the-cryptomidwives-a0df37eb35a6

In this context, each incentive mechanism is an assumption/hypothesis until we can validate it through experimentation. This process is similar to the lean startup approach where assumptions of a business model are validated before implementation/codification. The goal here is not only to explore if proposed incentives work, but to determine to what extent and the reason why it worked (or didn't).

Steps involved:

1. **Create hypotheses** based on the participants' incentives which were defined.

2. **Formulate ways to test this hypothesis and decide the best avenue for testing.** For example, are experiments the best option for testing? Are we setting these up quickly enough? Will we have enough statistical power to detect any effect from experimental observations? Is it better to go for interviews and surveys or run simulations?

3. **Determine the best way to measure the success of future testing.** Define what successful validation of the incentive should be.

4. **Denote learning/key insights for the future**, whether the testing/experiment was determined to be successful, or not.

9.3.1.2 Reputation Mechanisms

Identity management is a critical element for both ledger and market layer activities. On the ledger layer, identity management is key to securing sensitive data, onboarding and offboarding nodes, and establishing a protocol's governance model[45] which will be discussed further in the next section. In the market layer, one of the major challenges token designers face is ensuring enough trust remains on the network to avoid value leakage, so that transactions between relative strangers remain efficient enough to support the viability of the network. Reputation mechanisms seek to solve this problem by building trust and hence facilitating transactions.

When designing a reputation mechanism, decisions around what information each participant should have about each other, and the level of flexibility network participants should have in deciding who they want to interact with need to be determined. Historically, reviews have been the cornerstone of reputation mechanisms, and can be a potentially powerful tool for tokenized networks; however, these review mechanisms do present some vulnerabilities. Specifically, participants or businesses can be incentivized to manipulate and distort these reviews; moreover, a review reader may not consider a representative sample of the population by, for example, focusing on either very positive or negative reviews and subsequently making suboptimal decisions due to selection bias.[46]

9.3.2 Network and Token Supply Governance

Token ecosystems require coordination and governance at multiple layers of the ledger/protocol layer, market layer and the token supply process. In particular, governance both at the ledger and market layer primarily involves deciding on the rules over the way network participants make collective decisions, for example changing an already deployed mechanism. The token architect will primarily have to design a process for deciding:

– Who will participate in making decisions for the ecosystem; how will these participants be chosen; and what decisions will each participant or group of participants be responsible for?

– How will decision-makers be held accountable for decisions and how can decision-makers be changed?

– What level of automation in the collective decision-making process will there be?

– What degree of decentralization, i.e. usage of **private vs. permissioned vs. permissionless** DLTs needs to be realized at genesis and what may evolve over time?

– Which class of decisions process will remain on-chain vs. off-chain?

The token architect would want to avoid various risks to the network, and hence, should consider deployment of consensus mechanisms accordingly. Incorporating governance mechanisms into a protocol may increase coordination, but also increases complexity. The cost of this complexity requires governing processes to enable collective decision-making in the most efficient way. We discuss decentralization as a pathway using the dimension of time rather than a binary single decision point.

Additionally, an important part of governance includes conducting the monetary and fiscal policy of the token within the ecosystem. These are defined by paying attention to the effect of token allocation, velocity and sale structure on the overall health of the network and thus the ecosystem.

[45] Tasca, Paolo, and Claudio Tessone. "Taxonomy of Blockchain Technologies. Principles of Identification and Classification." (2018). https://arxiv.org/pdf/1708.04872.pdf

[46] Luca, Michael. "Designing online marketplaces: Trust and reputation mechanisms." Innovation Policy and the Economy 17.1 (2017): 77-93. Working paper version: https://www.hbs.edu/faculty/Publication%20Files/17-017_ec4ccdc0-4348-4eb9-9f46-86e1ac696b4f.pdf

CONCEPT

Public vs. Private DLT is defined based on whether the ledger of a system is, respectively, publicly available or not.

Permissioned vs. permissionless DLTs are characterized, respectively, based on whether an authorized or open set of participants are allowed to submit and validate transactions to the ledger.

Token Velocity indicates the number of times a token exchanges ownership over a set period of time. This happens when the underlying resource is exchanging ownership on the network. Also a distinction needs to be made between internal and external token velocity. Broadly speaking, in much the same way that imports, exports or capital movements have differing effects on a nation's GDP, internal and external velocity will also have varying effects on a network's overall health, and value.

CONCEPT

State Machines is a mathematical term used to describe an abstract machine that can be in one of a set of finite states, and where its current state directly depends on its previous state. Blockchains are state-machines whose present state (current block) depends on the transactions recorded in the previous block and all transactions contained in the time interval between when the last block was mined and the current block.

CONCEPT

9.3.2.1 Consensus Mechanisms

The ledger layer of our system is governed by the consensus mechanism; hence, a protocol's consensus mechanism is its backbone. Blockchains as **state machines** are tasked with reaching consensus and recording the current state of the market layer.

The rules and mechanics of how the ledger is updated in a trustworthy way is critical in any design process. For example, knowing how the consensus committee is chosen and rotated is a key underpinning of any economic design, because being a part of the group reaching consensus is actually quite a powerful position in any network. When using consensus mechanisms as an economic design tool, the following high level components should be reviewed:[47]

- **Network Topology**: shows the type of interconnection between nodes (decentralized, hierarchical, centralized).
- **Immutability and Failure Tolerance**: each consensus protocol has its own unique set of attack vectors.
- **Gossiping**: how is the addition of new blocks communicated to the rest of the network?
- **Consensus agreement**: how do nodes communicate between themselves, and how does the system handle Byzantine failures (latency, finality)?

[47] Tasca, Paolo, and Claudio Tessone. "Taxonomy of Blockchain Technologies. Principles of Identification and Classification." (2018). https://arxiv.org/pdf/1708.04872.pdf

Byzantine Fault Tolerance refers to the fault tolerance of a distributed computing system, where its components, or nodes, may be faulty or malicious. The term references the "**Byzantine Generals' Problem**" a commonly cited consensus problem, where a group of generals need to decide whether to attack or retreat but are physically separated and need to rely on devising a voting system that ensures that the optimal strategy is agreed upon and communicated despite the presence of malicious generals.

CONCEPT

If a network will be building and operating its own unique distributed ledger, as opposed to building on top of an existing protocol, then a more granular analysis of the consensus mechanism is required. Below is a **Consensus Evaluation Framework** adapted from a paper from the Alan Turing Institute.[48]

[48] Bano, Shehar, et al. "Consensus in the age of blockchains." arXiv preprint arXiv:1711.03936 (2017). https://arxiv.org/pdf/1711.03936.pdf

CLASSIFICATION	
Type	There are three general categories of consensus protocols. 1. Proof-of-Work (PoW): Also called Nakamoto consensus. PoW involves finding two consecutive SHA-2 hashes. Difficulty is adjustable. Nodes that generate hashes are called miners, and the process is called mining. Miners calculate hashes of candidate blocks of transactions to be added to the blockchain by generating random nonces until the resulting hash meets the leading zeros requirement. The miner is rewarded with new coins if they find a valid block. The biggest criticism of PoW is that it is extremely power intensive and prone to centralization. 2. Proof-of-X: Due to limitations in PoW, new consensus protocols have emerged that aim to replace wasteful computations with useful work specific to the protocol. Eg. Proof of Stake, Proof of Deposit, Proof of Burn, Proof of Capacity, Proof of Elapsed Time, Proof of Importance, Proof of Activity. 3. Hybrid: Due to limitations with single consensus nodes there has been a shift towards consensus protocols where a committee, rather then a single node, drives consensus.
System	The name of the network
Code Available	Is the code available?
Committee Formation	A committee is the group involved in consensus. How does a node join a committee? In permissionless systems this is a key preventative measure against Sybil attacks. The three ways consensus committees can be formed are: 1. Proof of Work: nodes join the committee based on PoW. Example miners have voting power proportional to the number of mined blocks. 2. Permissioned: nodes are allowed to join the consensus committee based on organizational policy. 3. Lottery: nodes join the committee based on the outcome of a lottery.
Consistency	Is consistency **Weak** or **Strong**? Consistency refers to probability that nodes might end up having different views of the blockchain, or alternatively the likelihood that a system will reach consensus on a proposed value. Essentially if consistency is weak, forks are possible.

COMMITTEE	
Configuration	The way a committee is configured has safety and performance implications. The four general committee configurations are: 1. Static: committee members do not change. This is typical of permissioned systems 2. Rolling (Single): the committee is adjusted on a moving slide, so when a new miner is added, the oldest one is ejected. 3. Full: all new committee members are selected for each epoch 4. Rolling (Multiple): a subset of the committee is selected to be swapped out and replaced with new members. Generally this is done using some form of cryptographic sortition.
INTER-COMMITTEE CONSENSUS	
Incentives	Consensus protocols generally assume two kinds of players, cooperative and byzantine, but design should incorporate other types of players. Decentralized networks need to provide incentives for **joining** and **participation**. What is the mechanism that keeps nodes motivated to participate honestly? Is it Byzantine Fault Tolerant (BFT)?
Leader	Who is the leader of the consensus protocol? The leader can either be elected from the current committee **(internally), externally,** or **flexibly.**
Message	Most committee-based consensus protocols use BFT protocols where the level of complexity in the message affects the level of BFT. Generally higher complexity messages contain more BFT. This section deals with complexity of communications between the consensus committee. From most to least complex, the notation here used is: **$O(n^2)$, O(nc , $O(n)$, $O(1)$** Where n refers to number of participants, c is the size of the committee.
SAFETY	
Censorship Resistance	Is the system resilient to transaction suppression by Byzantine nodes involved in consensus?
DoS Resistance	Are the nodes involved in consensus resilient fo DoS attacks?
Adversary Model	What is the fraction of Byzantine nodes that the protocol can tolerate?

PERFORMANCE	
Throughput	What is the max rate at which transactions or blocks can be agreed upon by the consensus protocol? **(TPS, MB/s...)**
Scalable	If consensus involves more nodes, is the network able to achieve greater throughput? **(yes or no)**
Latency	How long does it take from the time a transaction is proposed to when consensus has been reached on it? **(time)**
Experimental Setup	Is the protocol live? Or are numbers and claims coming from theory or a controlled test?
ENERGY COST VS UTILITY BENEFIT ANALYSIS*	
Return on Energy (Return on Kw/ Return on gas)	Energy cost vs utility benefit analysis - How efficient is energy consumption? What is the orphan rate of blocks/transactions? What is the return on energy consumed running the network?

Consensus mechanisms are an important component in attack vector analysis as they affect which set of attacks can emerge from the ledger layer, and which ones the network is the most vulnerable to. Network attacks can be targeted at various levels of the ecosystems with a wide range of motivations. Broadly, attacks will be either on the **consensus state**, the **consensus strategy**, or the **network topology**.[49]

Attacks on Consensus State: an attacker changes the consensus state of the system.

CONCEPT

[49] Debus, Julian. "Consensus methods in blockchain systems." Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep (2017). http://explore-ip.com/2017_Consensus-Methods-in-Blockchain-Systems.pdf

Attacks on Consensus Strategy: an attacker persuades other participants to change their plan of action.

CONCEPT

Attack on Network Topology: an attacker changes the topology of the network of nodes, either by removing or adding new ones.

CONCEPT

Below are some attack vectors to consider along with their most vulnerable consensus mechanisms.[50]

ATTACK VECTORS	DEFINITION	ATTACK ON...	MOST VULNERABLE CONSENSUS MECHANISM
Double Spending	An attacker or group of attackers trying to spend their tokens twice.	Network State	Proof of Work
DOS	Making the network inaccessible to its users, includes delay attacks.	Network State	Proof of Work
Sybil	One node in the network acquires several identities.	Network Topology	Proof of X
Forks (including long and short range attacks)	A divergence in the state of a blockchain caused by a disagreement amongst blockchain nodes.	Network State	All
Long Range Attack	A fork targeted at an early block.	Network State	Proof of X
Short Range Attack	A fork targeted at a specific block to target a block with a similar height, with the aim of reversing a recent state change.	Network State	Proof of Work
Bribe Attacks	Offering to 'rent' other participants' to gain control over their strategy.	Consensus Strategy	Proof of Work & Proof of X
P+Epsilon Attacks	When an attacker introduces a reward into a coordination game that affects the group's behaviour without causing the attacker to incur any cost.	Consensus Strategy	All
51% Attacks	Acquiring the majority of the network's mining hashrate or computing power.	Network State	Proof of Work

9.3.2.2 Monetary and Fiscal Policy

Token supply governance comprises of decisions regarding monetary and fiscal policy of the token , which has important implications for the adoption and sustainability[51] of the business model and the surrounding ecosystem. Monetary and fiscal policy tools in this context should be employed by taking into account the effects of different types of token allocation mechanisms, token velocity and sale structure on the network.

Monetary policy in our context, refers to the overall management of the token supply regarding the amount that will be released and level of automation involved in the process. Decisions regarding how many total number of tokens should be issued, the minting process as well as the frequency and timing of release of tokens have important implications on **token velocity**,[52] thus overall ecosystem health.

Therefore, token architect will primarily need to make decisions regarding:

- **Fixed vs. flexible token supply** - Whether the token supply should be kept fixed, follow an expansionary path or be subjected to a decay function.
- **Automation** - The degree of automation involved regarding release of tokens into the ecosystem or expansion or decay of the overall token supply.
- **Method of release** of tokens including partnerships, public sales, and/or airdropping them.

A fixed supply of tokens can create the synergies needed in the initial investment process and drive token prices higher which can be useful for the initial ecosystem pick-up. However, it may also lead to volatility and speculation in the market, and therefore limit the token's adoption as a medium-of-exchange and its sustainability. Hence, token supply decision has a major impact on the potential growth of the ecosystem. Even when a fixed number of tokens are issued, the token issuer, most often a foundation, normally releases a certain proportion of the issued tokens, and keeps a percentage of tokens usually ranging from 10-50% for strategic reasons including policies such as quantitative easing as well as community and ecosystem development. If some of the tokens are kept in the foundation's control for these purposes, it is also important to implement some governance around management of these tokens to guarantee that the foundation will not use the remaining tokens to cause any disturbance to the overall system.[53]

Flexible token supply involves creating an expansionary and/or contractionary token supply policy. An expansionary (contractionary) policy means that token issuer will increase (decrease) token supply over time. A potential mechanism to keep the token value less prone to volatility and therefore encourage the usage of the token as a medium of exchange and sustainability of the ecosystem, is to create an expansionary monetary policy that would algorithmically follow the adoption rate of the network.

[50] For a good summary of consensus mechanisms and failure modes (i.e. attack vectors) please refer to Debus, Julian. "Consensus methods in blockchain systems." Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep (2017).

[51] Avtar Sehra, Economics of Initial Coin Offerings, https://medium.com/@avtarsehra/economics-of-initial-coin-offerings-c083311e53ec

[52] Please see https://medium.com/outlier-ventures-io/why-token-velocity-matters-1ad459435e33 and https://medium.com/newtown-partners/velocity-of-tokens-26b313303b77

[53] For example, selling them all at once, can lead to a significant decrease in the price of the token.

Automation required in the governance of the token supply becomes particularly important with these type of policies.

The level of automation involved in the governance of the network and the token supply is a complex task. However, automation helps networks function without relying on particular input from individuals and can help avoid bottlenecks and issues related to trust. A typical step in our framework involves deciding whether an increase in the token supply (and the amount of it) is determined by the foundation, a sort of committee or algorithmically in real-time. Aforementioned type of flexible token supply policy can be conducted by having algorithmic monitoring through use of real time indicators of network health, which can be used to ensure a sustainable ecosystem but it may result in loss of flexibility in control.

Finally, deciding how to match the issued tokens with ecosystem participants is the last step. There are currently many methods of adding token supply into networks, including enterprise partnerships with bonus tokens to end user, airdrops, and public sales.

Fiscal policy in this context, involves other methods of dealing with the allocation of the issued tokens in order to promote community engagement within the ecosystem. For example, the foundation, the token issuer or alternatively the whole community via some consensus mechanism may decide to offer subsidies to certain types of network participants.

9.3.3 Token Distribution

How tokens are distributed can have a significant impact on the overall functioning of the network, and general system safety. Sometimes bootstrapping network development and initial liquidity requires capital raising through a token sale. A seemingly unavoidable consequence of many token sales, either private or public, is that they can concentrate initial token distribution in the hands of early investors. This is an issue for ecosystems founded on a decentralized ethos that require a wider range of users. Many market structures increasingly demand decentralization due to its fault tolerance and robustness. Thus, decentralizing token distribution is a key initial step to drive adoption rates and ensure the relative decentralization of an ecosystem's consensus formation, protocol value, protocol improvements, conflict resolution, and platform development. For network health, and legal compliance reasons, a degree of decentralization necessarily needs to be observable in the network's topology and its protocol value.

Another consideration is the risk of premature decentralization. Getting tokens into the hands of users before any tangible utility is offered by the network risks turning potential users into hodlers. Relying on hodlers to bootstrap network development is a big risk as any sudden drop (or even increase) in price could lead to a dump of tokens, destabilizing the network. It is becoming increasingly evident that successful networks will need strategic long-term investors, such as OV, to bootstrap development and initial liquidity.

Every network needs to ensure that its tokens are effectively distributed to key stakeholders on the network and that all required roles are adequately filled, at the right time. Token sales are one way to distribute tokens, but in many cases, early investors (or token buyers) aren't necessarily the target users of the network. Below are some common token distribution strategies.

Airdrops are a useful mechanism to distribute tokens to actual users and bootstrap communities.[54] However just sending free tokens to whoever requests them can also end up inadvertently concentrating tokens in the hands of speculators, and not actual users. Airdrops need to be coupled with a targeting strategy that focuses on delivering tokens to targeted user personas, as well as attaching the airdrop to actual usage of the network.[55] Every network will have its own requirements, and so every network's Airdrop strategy should be informed by its stakeholder maps, and taxonomy of actors.

An **Airdrop** is a token distribution strategy that gives tokens away for free to potential ecosystem participants.

CONCEPT

Example: Numerai conducted an **airdrop** targeted at Kaggle users with a rating above novice. This airdrop was a highly targeted campaign, and was very effective in getting tokens into the hands of potential users of the Numerai ecosystem (namely skilled data scientists). As a side note, Numerai did not notify Kaggle, and as a result Kaggle was unprepared for the influx of users and for security reasons stopped the airdrop.[56]

Staged token sales are a useful segmentation tool and can be used to target strategic investors before network utility is fully developed, and subsequently, actual users once a network is fully launched. A big risk with this strategy is that structuring a token sale effectively locks a network into an economic model that may not be optimal. Considerable effort should be made to ensure any economic structure locked in via a token sale does not hurt the long-term health of the network, and the viability of any future token sales or usage.

DAICOs are a relatively new fundraising approach proposed by Vitalik Buterin that combines elements of both a 'DAO' (decentralized autonomous organization) and an 'ICO'. Using this mechanism a team can bootstrap their project by publishing a DAICO contract that collects funds from investors in an escrow account that is collectively controlled by investors. The contributors can then decide when and how much funding should be released to the project, can vote on resolutions regarding the flow of capital to the development team, and can even decide to kill the contract. DAICOs are a relatively new and untested fundraising mechanism and are only as strong as the smart contract that governs them. As was witnessed with *The Dao hack*, these pools of capital are a natural honeypot for hackers looking to steal funds from a poorly written smart contract.

[54] Dan Elitzer, Airdrops: Key Themes and Design Considerations, https://medium.com/ideo-colab/airdrops-key-themes-and-design-considerations-efadc8d5d471

[55] Dan Elitzer, Airdrops: Key Themes and Design Considerations, https://medium.com/ideo-colab/airdrops-key-themes-and-design-considerations-efadc8d5d471

[56] https://www.kaggle.com/general/52852

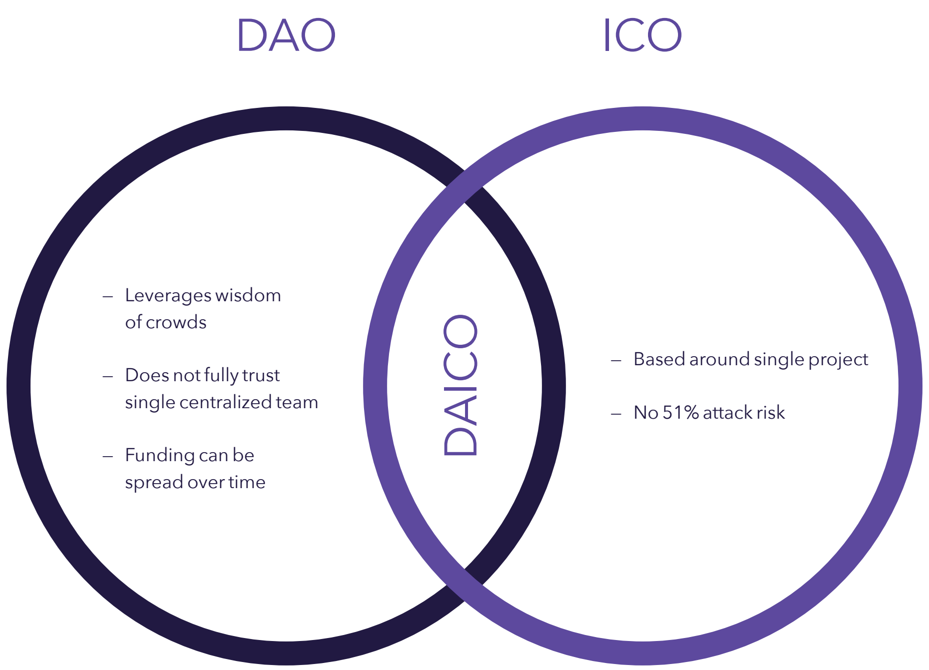


Figure 14: DAICO[57]

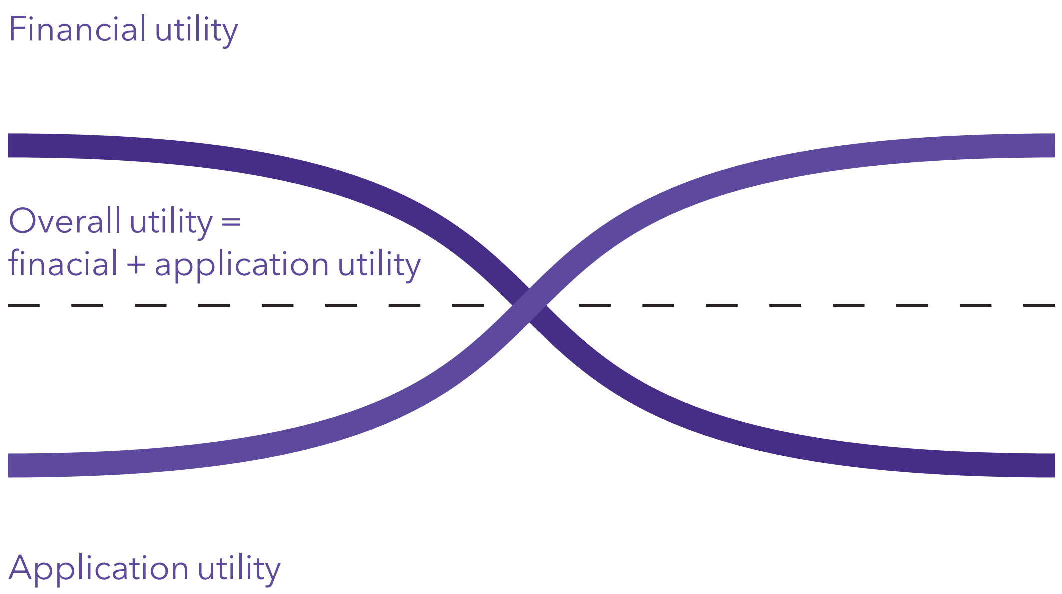


Figure 15: Token utility[58]

Developer and bounty programs are a suitable way to crowdsource specific tasks relating to network development, a TGE, or bug fixes. One of the most critical factors that will determine the future success of a network is the extent to which the developer community has adopted and decided to build off the network. Similarly to Airdrops, there is no guarantee that those developers who receive tokens will end up joining or starting the developer community around the network, and depending on the state of the network, could as easily turn token recipients into hodlers.

Corporate partnerships and sales are an appropriate method to utilize corporate distribution channels to distribute tokens into the hands of the right users. Corporate partners can act as strategic investors at early stages of funding, so bundling investment with some incentives to pass tokens onto their customers is a highly effective way to distribute tokens to proper users. However, leaning too much on this strategy can end up concentrating tokens into the hands of large corporate groups which could then use their weight to push their own agenda on issues such as governance, which may not necessarily be in line with the long-term health of the network.

Legal Compliance

Token sales conducted pre-MVT launch do not offer any utility and are likely to be classified as a security. In the diagram below by Chris Dixon, this is all the space left of the convergence point of the financial and application utility lines. It is clear that the SEC is more likely to classify tokens as a utility token that are sold post MVT launch. Bootstrapping liquidity and providing utility on the network are both crucial steps, but it is very difficult to achieve both results with the same token as they target very different user personas. Two tokens models, involving a security and utility token targeted at different users is a potential solution currently being explored by many actors in the space.

The SEC recently announced that it officially accounts for a network's level of 'decentralization' into its legal opinions as to whether a token is a security or a utility. Therefore, in order for a token to be classified as a utility, the issuing network also needs to exhibit decentralized qualities along with offering empirical utility. This puts added pressure on decentralizing token distribution to as many stakeholders and users possible, not just to ensure the long-term sustainability and health of the network, but also for legal compliance reasons.

[57] Vitalik Buterin, Explanation of DAICOs, https://ethresear.ch/t/explanation-of-daicos/465

[58] Chris Dixon, Crypto Tokens: A Breakthrough in Open Network Design https://medium.com/@cdixon/crypto-tokens-a-breakthrough-in-open-network-design-e600975be2ef

9.4 Key Design Outputs

Key design outputs are summarised below and are used to determine the **network objective function** and the creation of a **fully researched white paper.**

TOKEN DESIGN	FINANCIAL & NETWORK MODELING
High Level	**Models**
Objective function of the overall network that supports the ecosystem.	Circulating Supply Model
Architecture of the token (Systems approach to token design)	Velocity Model
Ledger Level	Utility Model
Consensus mechanism classification	Network Effects Model
Safety and performance	**Token Distribution**
Market Layer	Business
Economic primitives	Technical
Trusted Cryptographic Designs	Legal

9.4.1 Defining Network Objective Function and Constraints

In our framework, mechanisms employed should lead to efficient and transparent collective decision making and an optimal allocation of resources, in addition to allowing the network objective to be satisfied by incentivizing participants to act in their best interests subject to associated constraints. The **Network Objective Function** requires an understanding off all network goals and their relative importance for the ecosystem so that we can assign weights (normalised to 1) to the factors that influence the overall objective. This includes the technical, economic, business and financial goal of the project and also helps us determine what type of token, if any, is required and is similar to setting up a **social choice function** in **mechanism design**.

Steps involved:

1. **Identify network goals.** For example, degree of decentralization, governance, voting rights/ consensus building, scalability, do we want to minimize type 1 or 2 error (if relevant) etc.

2. **Prioritize among network goals**, which are determined in step 1.

3. **Determine the weights** (or range of weights) that are relevant for each factor and the shape of the overall objective function.

4. **Define the associated constraints.** For example, incentive-compatibility, a threshold to participate in curating or consensus building, computing capacity.

Social Choice Function is a concept from mechanism design, and is a function which a social planner or policy maker uses to assign a collective choice to each possible profile of the agents' types.

CONCEPT

9.4.2 Token Architecture

Taking a systems approach to token design requires mapping out the system in its entirety. Special attention should be made in describing the architecture, user interactions and value flows across the entire ecosystem, and within each of its subsystems.

Below is an example of a proposed token architecture by Dr. Michael Zargham for an open-sourced autonomous artist project, started by Simon de la Rouviere. The ArtDAO, called Artonomous [59], will be a self- sufficient artist that will create and sell the art it creates. The artist earns money through a daily art auction and through issuing and selling its own tokens where the price is set according to a curved bond. The diagram describes the various states of each subsystem, and the mechanisms that drive state changes across the system as whole. By mapping out the system in such a way, causal loops between state changes in different sub systems and their constraints can be clearly visualized and described mathematically. This is very useful to define the system by solvable subcomponents and their associated boundaries.

Specifically, five state variables, six roles and seven mechanisms are defined in the Artonomous ecosystem. The state variables (namely Gallery, Pool, Supply, Votes, and Candidates) are used to design the system in terms of its state variables on the blockchain. The roles (namely, Caller, Collector, Patron, Voter, Generator, and Developer) are characterized as sets of Ethereum addresses from which user actions are taken or from where Artonomous derives information. Finally, the mechanisms (namely, Art Generation, Art Sale, Patron Bonding, Patron Staking, Patron Unstaking, Patron Withdrawal, and Generator Proposal) interact within the ecosystem and represent the action space available in this complex system. Patron mechanisms, respectively, refer to actions related to minting, staking, unstaking, and burning of *Soul* tokens.[60]

[59] Simon De La Rouviere, Artonomous, https://github.com/artonomous

[60] A detailed design document by Barlin, Koch and Zargham can be found at https://github.com/BlockScience/artonomous/blob/master/token_engineering/Artonomous.pdf

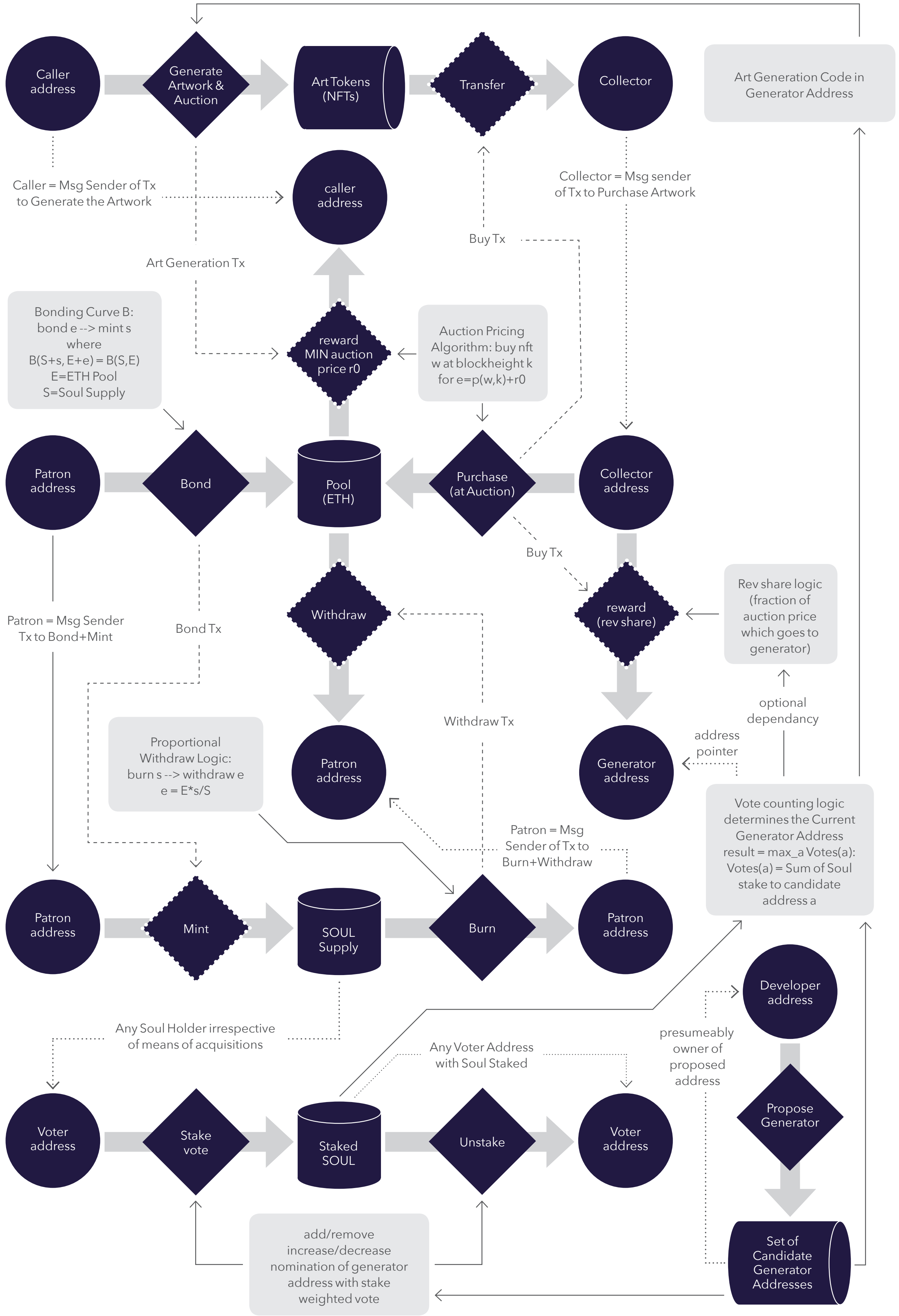
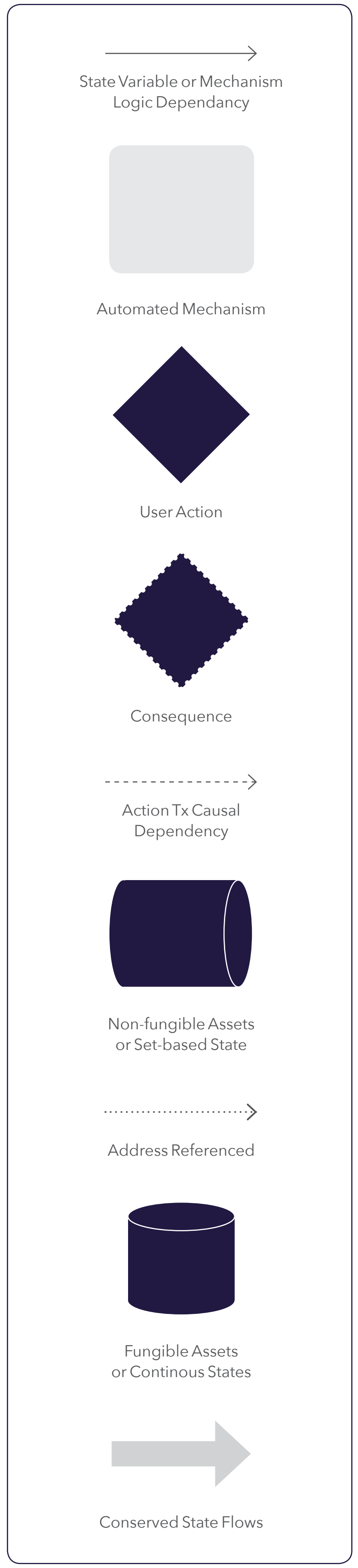


Figure 16: Artonomous ecosystem[61]

Legend



[61] Dr. Michael Zargham, Artonomous, https://twitter.com/mZargham/status/1012740617481474049

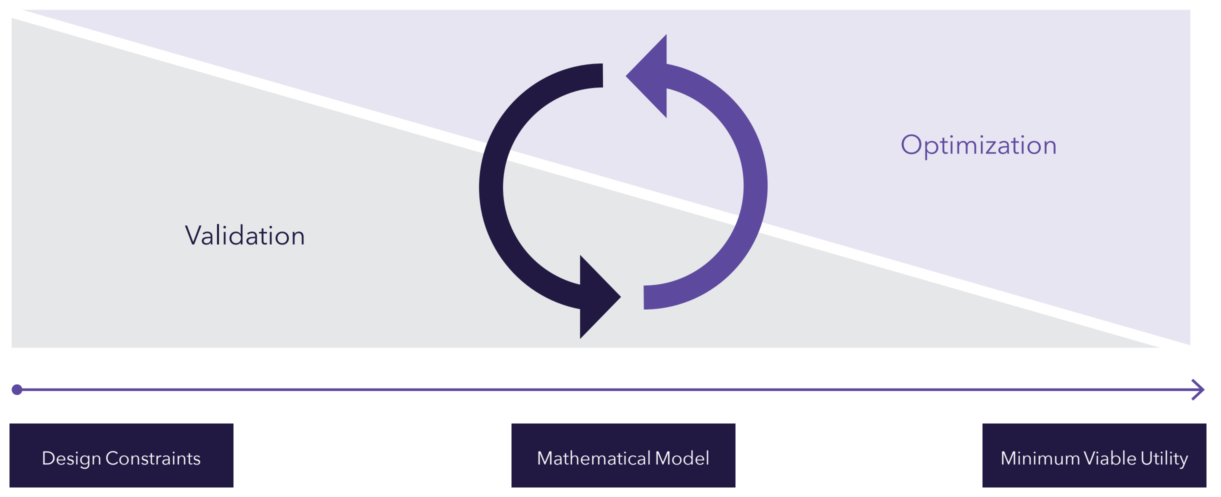
Chapter 10

Deployment Phase

SKILLS REQUIRED
Advanced Mathematics, Computer Science, Machine Learning, Systems Engineering

The deployment process involves using a combination of mathematical, computer science and engineering principles to fully understand the interactions in our network and its overall health. This consists of a sequential integration phase that requires testing of each sub-system before being integrated. MVT for our ecosystem, which was established in the design phase, will need to be improved upon once integrated into the network. This process consists of first validating key assumptions and iteratively testing through until all parameters have been optimized with respect to their constraints.

Testing: Validation & Optimization



General flow moving from Validation to Optimization

Figure 17: Validation and optimization

In this phase, live network data is collected and analyzed to implement dynamic mechanisms which adjust in real time using Machine Learning (ML). We propose using tools that include:

- **Regression Learning** to validate the input selection stage. In this process we are able to identify the variables and parameters of the objective function including trying to pinpoint and optimize each group of stakeholders' utility value on network.

- **Monte Carlo Simulations and Markov Chains** that allow us to quantify outputs of token gravity to calculate velocity of the token and its value.

- **Agent Based Modeling and Evolutionary Algorithms** allow for model to capture possible future interaction, including concept of survival of the fittest as different use cases and users come on the network.

The feedback loop created in this process will intelligently relay information to the **ML neural network** which will optimize the new data to maximize the objective function of the network.

Testing needs to be an integral part of any token design to not just create the optimal design, but the optimal feedback loop that helps govern and monitor the system. You can also use the model's sequential design and building processes as experiments.

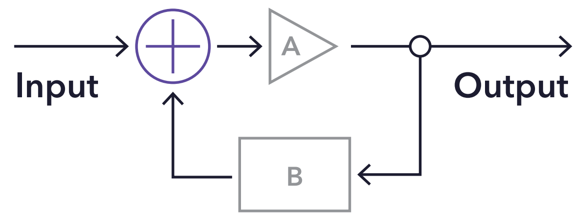


Figure 18: Deployment process[62]

10.1 Deployment Inputs

The process begins with surveys and experiments that will help identify the right inputs for the objective function and the network's stakeholders. For the model to hold it must have assumptions that are both practically and mathematically sound. The next step consists of assigning weights to each input to define their importance in the **network's objective function**. These weights can be calculated by using **regression analysis** and adjusted iteratively based on new incoming data, which eventually will result in determining the optimal weights to maximize the network's objective function. Enabling the network to learn from its data inputs requires incorporating reinforced learning. This is crucial for the **validation process** because it allows the model to learn how to adjust its weights from the data, or whether the inputs selected earlier are still relevant to the objective function.

CONCEPT

Regression Theory, in statistical modeling is a set of statistical processes for estimating the relationships among variables.

10.1.1 Objective Function Revisited

A critical dependency in the deployment phase, specifically parameter validation, is the identification of the **Objective Function** or mathematical specification of the token model and network. Every objective function needs to be bounded by a set of constraints. Constraints are a critical component of any token design, and imperative to a network's safety, especially through ongoing optimization efforts. Unbounded optimization can have devastating results and can lead to a model imploding in on itself in the attempt to maximize a certain unbounded parameter.

The purpose of this process is to make sure that all the incentives, rewards and behaviors of all the stakeholders are aligned to optimize the objective function. This is the building block around which governance, monetary and fiscal policy are all derived. The objective function allows for the selection of inputs into the mathematical and machine learning models. The selection of the right inputs is important because it allows the mathematical and ML models to run accurate and computationally efficient iterations in the neural network built. This is beneficial to the organization because it ensures that:

1. The right **stakeholders** are identified in enterprise partnerships.
2. Optimal **governance** is in place that minimizes the risk of forks.
3. **Efficient computational** time is achieved running the model.
4. **Fiscal and monetary policy** effectively targets optimal velocity and utility values.
5. The model's **feedback loop** allows the network to adjust model input weights in real time.

10.1.2 Design Hierarchy

As mentioned above, the process of validation starts with identifying the **objective function**. It will include a back test of any significant outputs which will serve as inputs in the following iteration. As the process goes along, a top-down design framework, such as **MOJITO** should be implemented throughout. To ensure trusted designs, MOJITO uses trusted building

[62] https://en.wikipedia.org/wiki/Feedback (Wai-Kai Chen (2005). "Chapter 13: General feedback theory". Circuit Analysis and Feedback Amplifier Theory. CRC Press. p. 13-1. ISBN 9781420037272. [In a practical amplifier] the forward path may not be strictly unilateral, the feedback path is usually bilateral, and the input and output coupling networks are often complicated.)

blocks, hierarchically connected to lower the risk of failure.[63] This maps the business requirements from the **MECE framework**, to a technical top-down design and is a way to make sure that each step is done correctly with minimal chances of critical errors in the future. A rigorous process of backtesting, optimization and analysis is done repeatedly until we are confident that no errors remain before moving to the next stage.

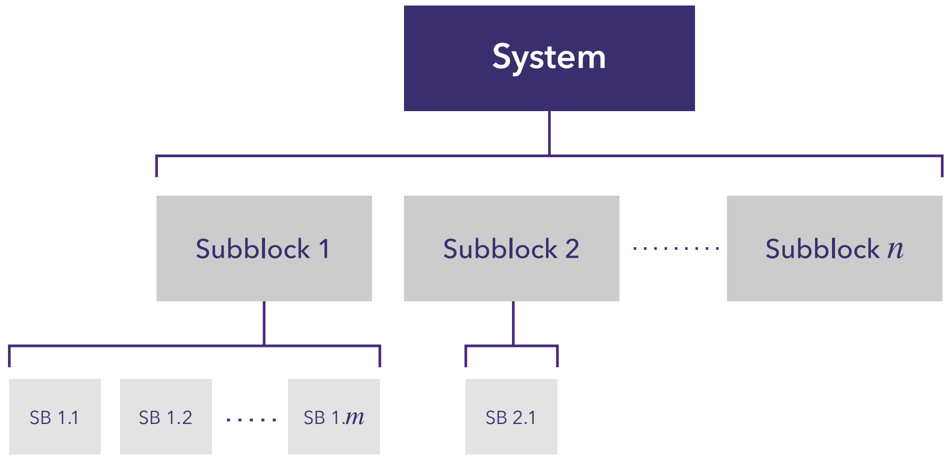


Figure 19: Design hierarchy[64]

CONCEPT

MOJITO, is a term from Trent McConaghy based on circuit electrical engineering designs highlighting the need to get accurate outputs at every stage because there are no do overs when networks go live, while using optimal computing power. This process allows for agile networks that can respond quickly to different data characteristics and constantly evaluate the validity on inputs and data.

10.2 Deployment Process

Deployment is focused on system integration and continued model optimization through testing and iteration. Deploying the token model is a continuous process, involving two distinct layers of iteration, on design and development.

The initial token design is still an untested hypothesis; therefore, once finalized, it needs to be tested before being implemented. Throughout this phase, design iterations require a deep understanding of the possible states of the model, where the question is what could happen instead of focusing on determining what exactly will happen. Within this framework, incentives should be used to encourage desired states and cut out mechanisms that could lead to undesired states. By limiting the action space in this way, the token model is shaved down to the **minimum viable token (MVT).**

Getting to the optimal MVT requires applying principles from systems engineering and control theory throughout the testing and implementation phase to achieve the optimal incentive structure and effective production-ready model. In much the same way the laws of physics are the primitives for classical engineering problems, such as building skyscrapers or bridges, the economic theories and incentives that guided the initial design are the primitives used in token engineering.

10.2.1 Control Analysis: Path to a Minimum Viable Token

Control Theory is a subfield of mathematics focused on understanding the set of possibilities within a dynamic system. Token models are dynamic complex systems that produce unpredictable (stochastic) and predictable (deterministic) outcomes. The issue is that many of the **(Nash) equilibria** determined in the design phase are simply proofs of existence;[65] and in practice, this does not mean that a particular state will actually be the outcome in real life.

Using control theory formalises this complexity and gives key insights into the set of possibilities within any given model. The token architect can then eliminate the possibility of certain behaviors, and limit the **action space**. By knowing the set of all possible actions, also known as the action space , the designer can then focus incentive engineering efforts only towards those states which are possible. Control analysis should be viewed as an intermediate step between **initial design** and **incentive engineering**, and should be used at every iteration of the design to formally define the set of possible outcomes achieved by a particular token model.[66]

[63] McConaghy, Trent, et al. "Trustworthy genetic programming-based synthesis of analog circuit topologies using hierarchical domain-specific building blocks." *IEEE Transactions on Evolutionary Computation* 15.4 (2011): 557-570.

[64] Trent McConaghy, Top Down? Bottom Up? A Survey of Hierarchical Design Methodologies, https://medium.com/@trentmc0/top-down-bottom-up-a-survey-of-hierarchical-design-methodologies-4dff987cd970

[65] Zargham TE Meetup

[66] Zargham, Michael, Zixuan Zhang, and Victor Preciado. "A State-Space Modeling Framework for Engineering Blockchain-Enabled Economic Systems." arXiv preprint arXiv:1807.00955 (2018). https://arxiv.org/pdf/1807.00955.pdf

Solution Space (in mathematical optimization, a feasible region, feasible set, search space) is the set of all possible points (sets of values of the choice variables) of an optimization problem that satisfies the problem's constraints, potentially including inequalities, equalities, and integer constraints.

CONCEPT

A Nash Equilibrium, is an equilibrium in a game where players each choose their best strategy given the strategies chosen by other players and in doing so have no incentive to deviate.

CONCEPT

10.2.2 Iteration

In the Design Phase some of the parameters in the model may have been validated independently to generate the initial design; however, most likely the sum of all parts have not been tested together. As mentioned before, there are two distinct layers of iteration, namely design and development iteration at the Deployment Phase. At each iteration, we should be focused on integrating the most recent model updates, and test results into the latest version of the model.

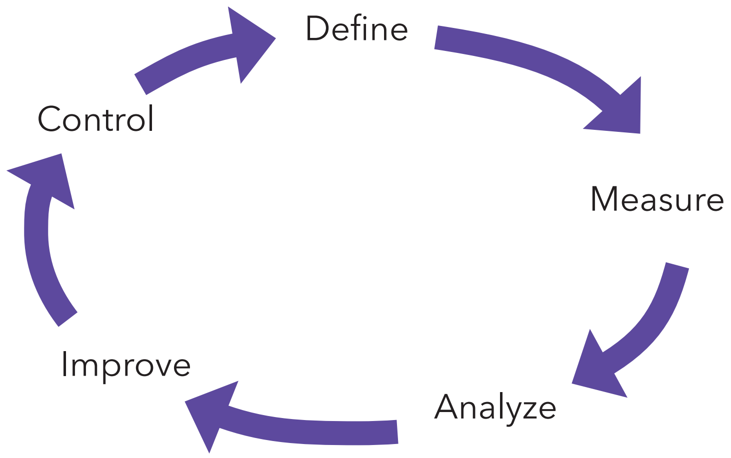


Figure 20: Iteration[67]

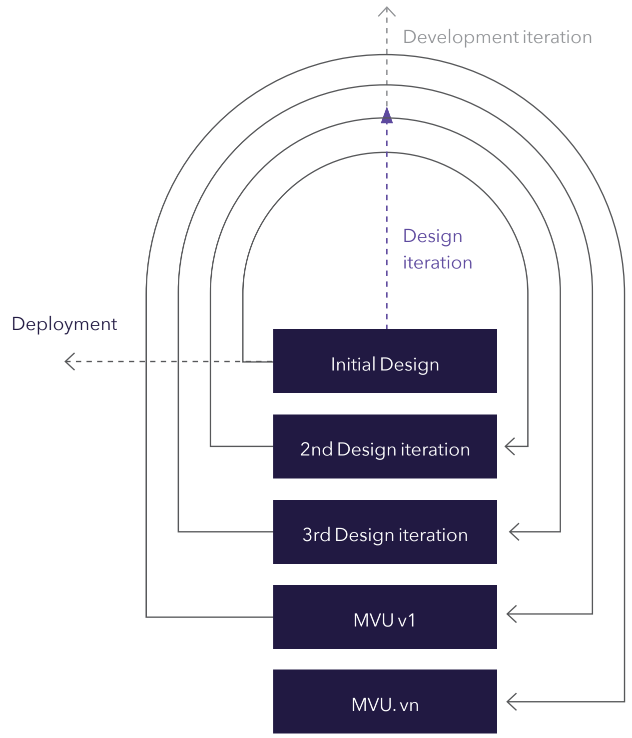


Figure 21: Iteration throughout token ecosystem creation.

The same way we iterate the design through to a production-ready model, testing should be iterated through to a **production-ready feedback loop**. These feedback loops are key in monitoring the health of the network, and enable token models to be agile and make real-time adjustments. Token models are more sustainable if they are able to react and optimize based on little shocks in the network, which is commonly referred to as **anti-fragile**. If these little network shocks go undetected or the model simply does not adjust accordingly, then inefficiencies will build up and the risk of a much larger, destabilizing shock increase, which risks the viability of the network.

[67] https://searchenginewatch.com/sew/how-to/2321845/using-the-dmaic-process-for-seo-projects

Anti-fragile systems, as proposed by Nassim Taleb, are designed to adjust and improve from increased inputs and shocks from their environment.

CONCEPT

The continuous and complex nature of these networks means that they will always be in a state of evolution, and thus the token model needs to be able to evolve in step with the needs of the network, with the help of optimal feedback loops. Blockchains are great economic sensors , providing provenance of information not just on the current state of the network, but its evolutionary path. Due to the effectiveness of these networks in recording and preserving details on their current state, the question is not what can be measured, but what should be measured to determine the true state of network health. The answer to that question should be guided by the high level network requirements outlined in the **Discovery Phase**, and the **network's objective function** defined in the **Design Phase.**

Human behavior is extremely complex, hence data collected from these networks is multidimensional, time-continuous, and always evolving. Moreover, different weights will be given to different parameters at various stages of a network's lifecycle, and some parameters may even become irrelevant as new ones are introduced. Accordingly, choosing the right metrics to optimize around and when to optimize is critical. A token model's feedback loop is a critical evolutionary component used to reduce the complexity of the network into actionable insights to direct model optimization, and create frictionless evolution.

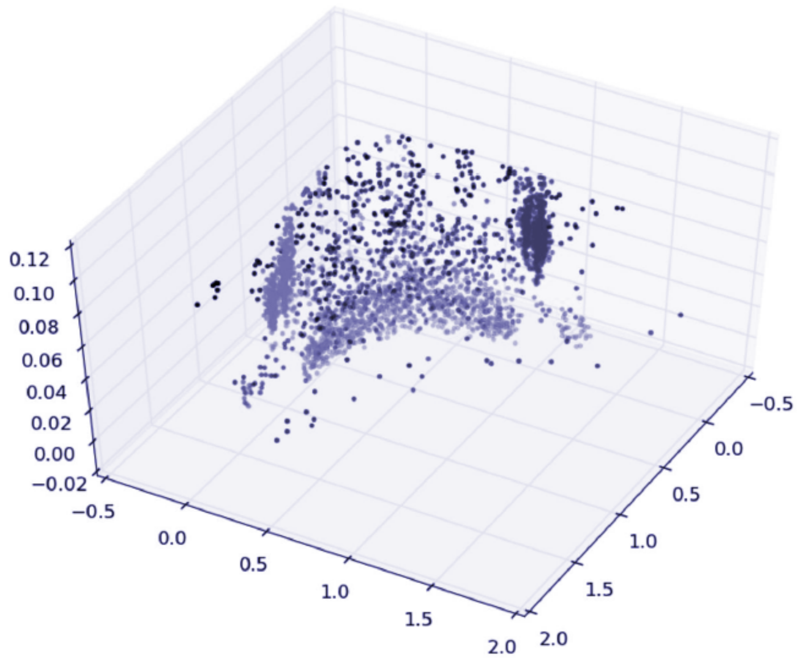


Figure 22: Multi Dimensional Data [68]

10.2.3 System Integration

This stage comes into play when the model has moved past design iteration, and we have a fully validated model that needs to be integrated into the rest of the technology stack. As mentioned before, these decentralized networks are essentially two layer systems, consisting of a **market and a ledger layer**.

Integrating these token models into the underlying infrastructure is analogous to launching a business around an initial product prototype, where the business plan is the initial token design. Similar to executing on a business plan to launch a new business, once the token model has been integrated into its underlying network, the network is launched.

10.2.4 Launching the Network

Before launching a token model with an end user facing interface, **token and product roadmaps** should be developed to ensure efficient use of resources. Moreover, the underlying tech and network infrastructure needs to be in place, and available for beta testing (test net deployment). Until then, a token model will exist solely as a mathematical model or a simulation.

Ideally a token model will be launched first in a test net with real users before going to a production ready network. This will allow for further testing and optimization of the token model, and fine-tuning of the **token-network fit**. The sooner a token model is able to produce real metrics regarding its use and overall network health, the sooner it is possible to de-risk the model.

10.2.5 Measuring, Monitoring and Maintenance

Once these models are out in the wild, the job of token design and engineering has only just started. Token models will need to be constantly monitored, maintained, tuned, and iterated through. A good project will feel responsible for the network it has launched, and ensure its long term sustainability, effectiveness and security well past initial network launch.

[68] https://stackoverflow.com/questions/18279859/supervised-machine-learning-classify-types-of-clusters-ofdata-based-on-shape-a

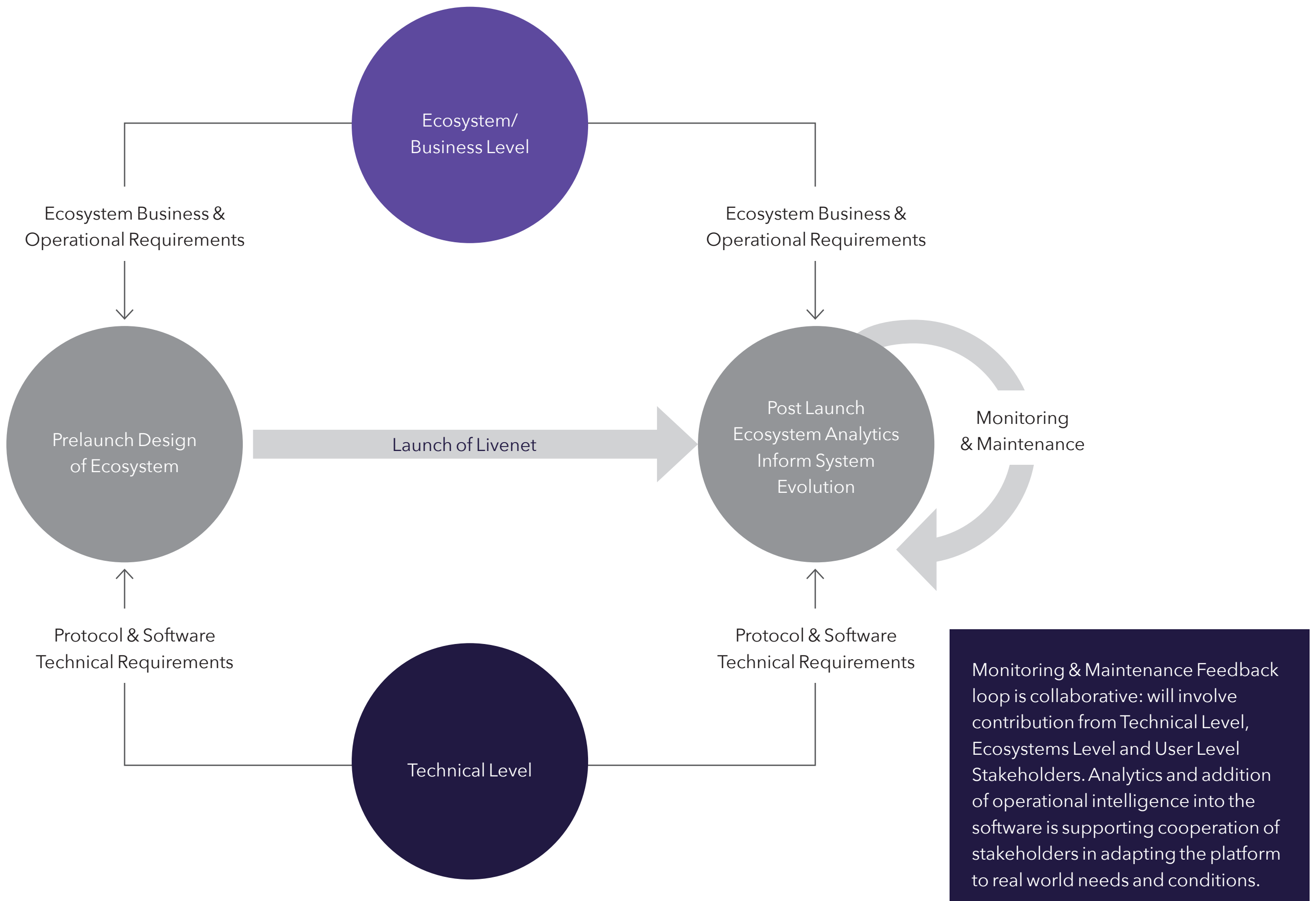


Figure 23: Network Monitoring & Maintenance[69]

Well-designed token models should already have all the tools in place to effectively measure and monitor their issuing network. It is worth noting that what you should measure in these token ecosystems will invariably change throughout the lifecycle of the network. Different types of users rotate in and out of the network; the network utility increases; the network forks or is acquired by other networks. Tracking this evolution to create well-structured databases of network metrics will increasingly become a huge priority for these networks, not just to optimize their own token models and ensure their own long term sustainability, but to also improve the tools used to design, build, and iterate new networks and token models.

We propose that any network issuing a token will need to create a **network health dashboard** used to measure and react to current network states.

A Network Health Dashboard, is a tool that will be used to monitor a tokenized ecosystem in real time that collects, sorts, and analyses data to be observed, and feeds back into the token model to inform token optimization efforts.

CONCEPT

Example: Network Health Dashboard

Macro	Metric	Rationale
Level of Decentralization[70]		
	# of entities in control of >50% of mining/ voting power	Gives a snapshot on consensus formation distribution.
	% of token supply held by top 100 accounts	Gives a snapshot on protocol value distribution.
	# of clients codebases that account for >90% of nodes	Gives a snapshot of protocol improvement distributions.
	# of public nodes	Gives a snapshot on state of consensus formation.
Token gravity		
	Velocity (internal vs external)	**Internal** velocity gives an idea of how many times tokens are changing hands within the ecosystem, and higher values signify good network health. **External** velocity refers to how many times tokens are being exchanged outside of the ecosystem, and high values signify high value leakage, and poor network health.[71]
	Severity	Shows the quantity of transactions being exchanged on the ecosystem.
	Frequency	Slightly different from velocity as it focuses on the number of transactions within the ecosystem (not on the number of times a token changes hands).

10.3 Deployment Tools

Deployment tools should be used to help validate and optimize model parameters through the lifecycle of the model. Model testing is an integral part of token design from the very start, so these tools can b e used at previous stages, however the emphasis on testing in the deployment phase is to stress the fact that the best experiments are with real data, from real users interacting with the token model.

Modeling and computer simulations are an incredibly powerful tool to test a token model in the absence of a live network. These tools are used to deepen the token architect's knowledge of the various drivers and levers of a particular token design, and create some baseline expectations around the functioning of the token model once it is integrated into the issuing ecosystem.

The outputs after this stage will include:

1. Fully **validated** parameters
2. System level **architecture**
3. **Equilibrium** analysis

At this stage a fully researched and proven **technical paper** should be completed to inform further testing and simulations to increase the credibility and confidence in our model. This process can be defined as **optimization** but is still an integral part of the **deployment phase**. Optimization can be solved deterministically or stochastically, with both using algorithms.

10.3.1 Monte Carlo Simulations

We use **Monte Carlo simulations** because there is a probability associated with each path or iteration. We know that for the network participants to derive maximum utility they will have to interact with other stakeholders on the network like miners and users. The key is to simulate the most likely transactions on the network including their frequency and impact to the overall value of the network. In order to get accurate information on the interaction of these stakeholders/agents, we have to run as many simulations as possible and as is computationally optimal. This is useful to predict aforementioned interactions and find a **convergence point**.

Convergence Point, is a point where we can get arbitrarily close to the function's asymptote, or the limit, as long as we go far enough. In the case of simulations, the more iterations we go through, the closer we will get to the limit.

CONCEPT

10.3.2 Markov Chains

We incorporate **Markov Chains** to highlight the different states that stakeholders move to and from based on interaction with other stakeholders. Acknowledging these states allows us to make sure the incentives are well designed to maximize utility on the network.[72]

Example: A data provider in **Ocean Protocol** needs to coordinate with curators to curate their data to be able to target it effectively to the right user. Through these interactions, the provider or the curator can rotate between multiple predefined states: they could rotate between high quality providers or low quality providers, or they could find themselves being kicked off the network if they breach the rules.

10.3.3 Machine Learning

This enables us to tackle tasks that are too difficult to solve with fixed programs written and designed purely by human beings. **Reinforcement Learning (RL)** agents are trained to test mechanisms designed at scale under conditions similar to what is expected after deployment into widespread adoption. It can be used for testing the **incentive structure**, as well as discovery of **failure modes** and **collusion** between agents occurring both on- and off-chain.[73]

The key is to understand the **objective function** of the **token design**. This helps identify the task the machine learning algorithm is trying to accomplish. Depending on the given project we may need to maximize or minimize the objective function.[74]

A **Global Maximum/Minimum**, also known as an absolute maximum/minimum, is the largest/smallest overall value of a set, function, etc. over its entire range.[75]

CONCEPT

[69] Dr. Michael Zargham, Block Science Project Flow and Role - Client view of stages

[70] Arewedecentralizedyet.com

[71] Dr. Michael Zargham

[72] See for a good description: https://www.stat.auckland.ac.nz/~fewster/325/notes/ch8.pdf

[73] http://www.deeplearningbook.org/contents/ml.html page 97

[74] http://www.deeplearningbook.org/contents/ml.html pages 99,103

[75] Weisstein, Eric W. "Global Maximum." From MathWorld-A Wolfram Web Resource. http://mathworld.wolfram.com GlobalMaximum.html & Weisstein, Eric W. "Global Minimum." From MathWorld-A Wolfram Web Resource. http://mathworld.wolfram.com/GlobalMinimum.html

The second issue is the classification of inputs or variables that will influence the objective function. Classification becomes more challenging if the computer program is not guaranteed that every measurement in its input vector will always be provided. To solve the classification task, the learning algorithm has to only define a single function mapping from a vector input to a categorical output. When some of the inputs may be missing, rather than providing a single classification function, the learning algorithm must learn a set of functions. Each function corresponds to classifying x with a different subset of its inputs missing.

The algorithm has to be able to perform regressions that show the relationship between the inputs and the objective function. A **logistic regression** is most frequently used since a logistic function, also called a **Sigmoid Function**, tends to mirror the growth pattern of most tokens. There also has to be some significant **backtesting** of the algorithm to ensure that it is not underfitting or overfitting.

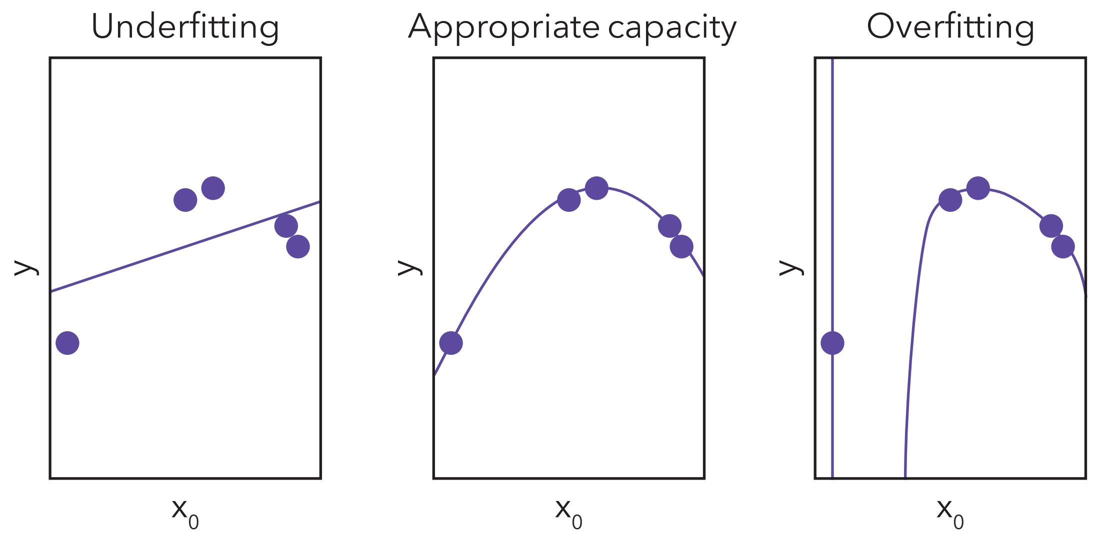


Figure 24: Visualization comparing overfitting and underfitting.[76]

Backtesting applies an optimization method to historical data to verify the accuracy and effectiveness of the strategy to predict results. Since one typically does backtesting with a training dataset, underfitting and/or overfitting are a sign of an error in the Machine Learning algorithms being used.

CONCEPT

10.3.4 Genetic Programming (FFX)

Least squares (LS) regression on network growth and connections is a useful tool because it is fast, scalable and deterministic. This is used to solve optimization problems. It is also advised to consider **Symbolic Regression (SR)** as part of Genetic Programming on the token network to increase speed, scalability, reliability and interpretability. These tools promise to allow for improvements between 2x and 10x.[77]

10.3.5 Agent Based Modeling

Agent-based modeling (ABM) is a style of modeling in which individuals and their interactions with each other and their environment are explicitly represented in a program, or even in another physical entity, such as a robot. An agent is a discrete entity with its own goals and behaviors or is autonomous, with a capability to adapt and modify its behaviors. Agents can move in free (continuous) space but also over **Geographical Information Systems (GIS)** tilings as is the case with Fetch AI digital economic agents. They are connected by networks of various types and can be static or dynamic.[78]

Example: in the **Fetch Protocol**, autonomous economic agents can be used to improve performance and efficiency for energy producers. They can help consumers find cheaper energy prices, commuters optimize travel routes, and cities manage traffic congestion

But why do we need agent-based modeling?[79]

1. Systems that need to be analyzed are becoming more complex
2. Decentralization of decision-making: 'Deregulated' electric power industry
3. Systems approaching design limits: transportation networks
4. Increasing physical and economic interdependencies: infrastructures (electricity, natural gas, telecommunications)

10.3.6 Evolutionary Algorithms

In order to create a hierarchical structure on the network there has to be a cost to join, usually represented in the form of fees. Think about a network that has a **staking mechanism** in order for the supplier of the network resource to build reputation. Modularity evolves because of the presence of a cost for network connections.

[76] This figure is taken from http://www.deeplearningbook.org page 111

[77] McConaghy, Trent. "FFX: Fast, scalable, deterministic symbolic regression technology." Genetic Programming Theory and Practice IX . Springer, New York, NY, 2011. 235-260. page 3

[78] http://www.agent-based-models.com/blog/2010/03/30/agent-based-modeling/

[79] Charles M. Macal and Michael J. North, Introduction to Agent-based Modeling and Simulation, http://www.mcs.anl.gov/~leyffer/listn/slides-06/MacalNorth.pdf

A Staking Mechanism requires a participant to put some 'skin in the game' in order to perform certain actions on a network. If the desired action is observed, then the stake is returned, otherwise it is taken from the participant. Staking is a useful way to introduce a cost to join the network, and disincentivize undesired behaviors.

CONCEPT

Imagine a token architect that creates a hierarchy for the suppliers where the most reputable suppliers will be able to survive on the network and bad actors will be costed out. The same applies to the buyers who will have to behave according to the rules of the network. In the case a buyer of the resource breaks one of the rules, such as sharing it with a third party without consent, they would see their standing in the hierarchy decline.

The example above shows how fees on a network end up creating a hierarchy which will allow for the network to evolve. This is how we end up with trusted nodes.

Example: Bitcoin block rewards. Bitcoin block rewards. Evolution on a network can be examined in the context of the block rewards function for a network like bitcoin. With each additional block the network is evolving. This means that the composition of the network is always different than before the previous block was added. In this process, there is a cycle of evolution happening on the network every time network difficulty adjusts causing new miners to join or old ones to leave. The consequence is a cycle of survival of the fittest.

Another thing to consider when examining evolutionary components of a network are the users themselves. As the network evolves and offers different forms of utility, users will cycle in and out. New users will bring a different set of variables and characteristics than those that have left, and the network and new users will both need to evolve in step to optimize the network's objective function.

There are three main states that are included in this cycle[80]

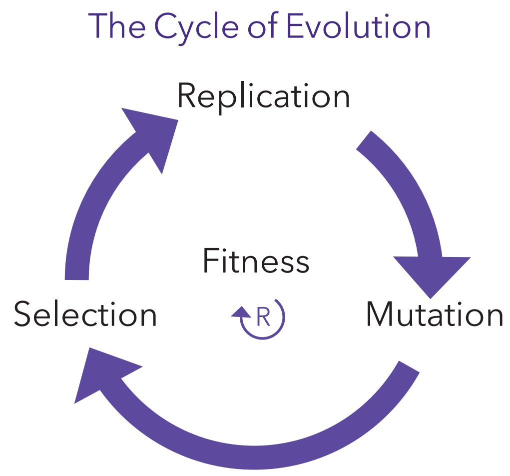


Figure 25: Cycle of evolution.[81]

- **Replication**: happens during the formation of a new block. This is the space between the current block and new one, where previous optimal interactions will be targeted to persist and evolve from previous states.
- **Mutation**: this is a permanent change in the characteristics of the agents / stakeholders to meet the new architecture.
- **Selection**: those that cannot change in the hierarchy will face survival of the fittest during a selection phase. If they fail they will be forced toleave the network.This process will continue roughly every 10 minutes in the case with Bitcoin as block rewards are issued.

There are two major ways to understand, model and review **evolutionary algorithms**, namely **genetic algorithms** and **genetic programing**.[82]

80 http://www.thwink.org/sustain/glossary/CompetitiveAdvantage.htm

81 http://www.thwink.org/sustain/glossary/CompetitiveAdvantage.htm

82 https://en.wikipedia.org/wiki/Genetic_programming

Genetic Algorithms, involves 'Survival of the Fittest' where an individual/agent is a vector of continuous values. They are used to generate high-quality solutions to optimization and search problems by relying on mutation, crossover and selection.

CONCEPT

Genetic Programming, here we are searching a space of computer programs which are encoded as a set of genes that are then modified (evolved) using an evolutionary algorithm.

CONCEPT

After this process you start to build the machine learning and mathematical models that will help define the network analysis and give outputs to be measured.

10.4 Key Deployment Outputs

The key outputs from the Deployment phase are as follows:

1. **Probabilistic Results**: gives insight into unique probabilities associated with each path that network stakeholders interact with token gravity.

2. **Graphical Results**: allows for simplified analysis of key variables like velocity, adoption rate and token circulation as a function of time.

3. **Scenario Analysis**: allows for 'what if' scenarios from good to black swan scenarios and understanding their frequency and severity.

4. **Correlation of Inputs** : help understand how dynamic weights are applied to key input variables as the model iterates.

We can also derive an **Equilibrium Analysis** snapshot with the following outputs:

1. Behavior Analysis
2. Optimal Equilibria
3. Sub-Optimal Equilibria

We need to determine key metrics to optimize the model and view its sequential designs as **stochastic simulation experiment**s. Close attention should be paid to converging on the optimal feedback loop for future model iterations. The final optimization report should have analysis from the following tools:

– Whitebox Regressions
– Evolutionary Algorithms
– Machine Learning
– Backtesting

Equilibrium Analysis provides a snapshot of stable states in a network, analysing participant incentives and observed behaviors.

CONCEPT

Chapter 11

Governance: Pathway to Decentralization

A common theme throughout this document is that a token model is a complex dynamic system. The tools and methodologies outlined above are all chosen to help narrow in on the simplest and most effective MVT for its issuing ecosystem. This initial token design is like selecting the perfect seed for the particular condition of a garden. In much the same way a tree will grow out from a single seed and result in a very complex ecosystem, a token model when finally integrated into its network, should be allowed to grow and evolve according to the environment it is in.

The common belief is that these tokenized networks are decentralized, but in reality it is much more nuanced. Decentralization is a spectrum, and especially in the context of blockchains, is very complex with many considerations. Some considerations when evaluating the level of decentralization are:

Consensus Formation	Protocol Value	Protocol Improvements	Conflict Resolution	Platform Development
– Who controls the nodes on the network and how is consensus achieved?	– How decentralized is the value capture in the network? – How distributed is it?	– Network Governance - who controls the product roadmap?	– How are conflicts resolved? – How are resolutions enforced?	– How many people/ organizations are building on top of the network?

Figure 26: Evaluating decentralization

It is becoming increasingly clear that decentralization is not a constant state, but rather a pathway which requires pragmatism and agility. Decentralized systems are more resilient than centralized systems, so as these ecosystems are launched and users are on-boarded, the objective is generally to distribute network 'ownership' to the users of the network. All networks will unavoidably start off relatively centralized, as founding teams tend to be small and focused. But even so at the outset, a project should consider its optimal degree of decentralization, at the various layers of the network, required to reach some kind of quorum or consensus with the majority of the network and avoid value leakage or unhealthy hard forks.

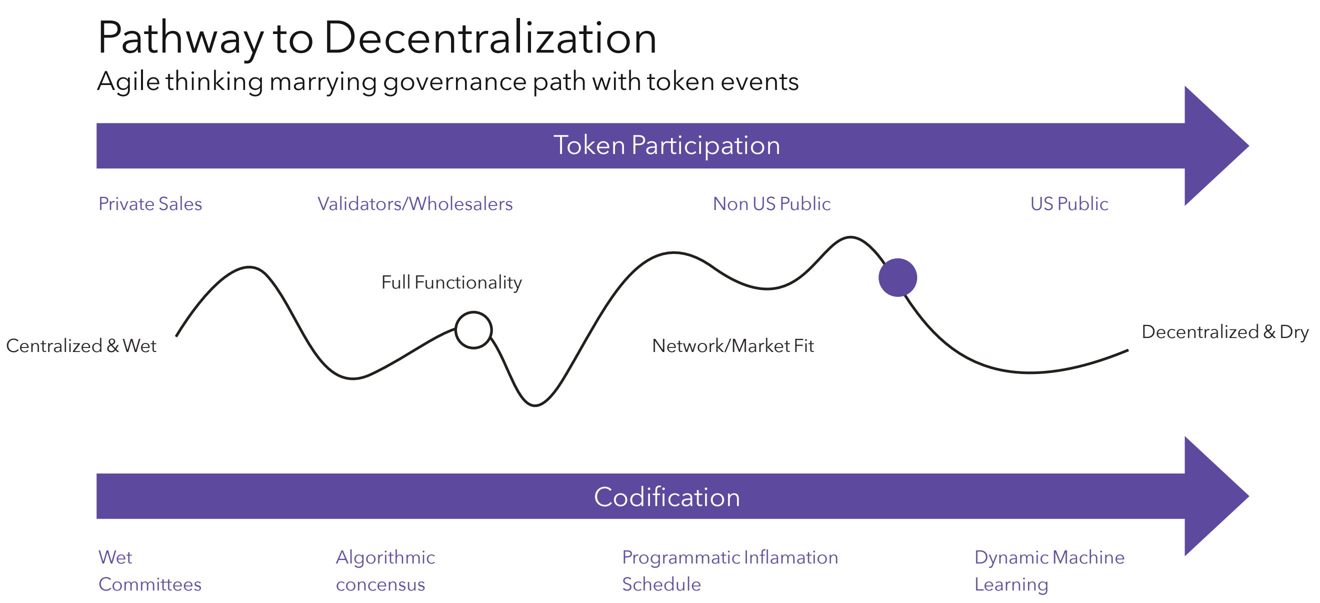


Figure 27: Pathway to decentralization.
Note: Based on best practices at the time of writing in the rapidly evolving regulatory environment. We expect these to change over time.

This devolution, or redistribution of power from the core to the periphery, can be best handled with effective governance mechanisms. As a network matures and the required quorum expands, plans that gradually open and scale governance to users must be put in place and implemented. Governance is in essence a value capture mechanism used to implement and manage change effectively. In fact, strong governance is more often than not the difference between a healthy fork and a destructive fork. As mentioned before, token models will naturally evolve from their launch state, hence the most successful networks will be adaptive and have mechanisms designed to manage and implement change effectively.

Networks with strong governance will capture more value in the long-run. More governance increases coordination in the network, but it also increases complexity, and cost, either in time or money. Thus, in the same way that a MVT model is the main goal of our strategic process, establishing a **minimum viable governance** that is designed to evolve with the needs of the issuing ecosystem and its users is a necessary first step in establishing a governance roadmap. Minimum viable governance necessarily answers the following questions:

1. What decisions need to be made?
2. Who needs to make those decisions?

CONCEPT

Minimum Viable Governance strikes the balance between coordination, complexity, and cost associated with introducing governance mechanisms by being **simple, effective, accountable, and transparent (SEAT).**

It is out of scope of this document to discuss in great detail the governance challenge of collective decisionmaking and balancing the efficiency of centralized governance versus the diversity, participation and protection against tyranny that comes from more devolved or decentralized forms of governance. The key point we want to make here is decentralization is very much a political ideal similar to sovereignty; and, just like sovereignty one that is hard to design and even harder to maintain. But more importantly, decentralization is a design choice with a set of trade-offs.

Like decentralization, strong governance is also a process rather than a constant state. Starting from first principles, and taking lessons from nation building, one of the fundamental principles of governance is that power and responsibilities are split amongst distinct branches with the aim of preventing over-concentration of power, and creating checks and balances.

As a process rather than an end state, it is important to articulate network principles to all network participants to reduce the likelihood of misalignment and disagreement between stakeholders at later stages. A network constitution is a living document that will outline principles in the early stages but over time will become more of a legal and automed constitution.

Ecosystem Constitution Breakdown:

1. **Separation of Powers and Electoral System**
   a. **Executive Branch** (Enforce laws)
      i. **Finance** (Treasury/ crypto-economics)
      ii. **Internal** (Network Engagement)
      iii. **External** (Network Growth/ Partnerships)
      iv. **Security** (Network Protection)
   b. **Legislative** (Network Policy Branch)
   c. **Judicial** (Conflict Resolution)

2. **Checks and balances** define the relationship between the three branches of network governance and include mechanisms to check power accumulation by any one particular branch. Mechanisms like judicial review and executive veto powers can be utilized and in all likelihood will have to time-limit for example, executive veto powers until a certain number of nodes are on the network.
3. **Bill of rights** for network participants, and the roles and responsibilities for each role.
4. **Amendment process** outlines the process of how changes are proposed, confirmed, and implemented.

Early on, the amendment process is perhaps the most important aspect of a network governance structure. To ensure strong network health, a network's constitution needs to allow for changes which will inevitably happen. It is also mission critical that any constitution is clearly articulated and presented to the community to ensure buy-in. Getting all of this constitutional detail defined up front is almost impossible, so the optimal strategy is to outline principles, consult regularly with network participants and be transparent about the process. The balance is building in flexibility to adapt , but not enough flexibility so that any particular stakeholder or stakeholder group is not able to exercise outsized control and power.

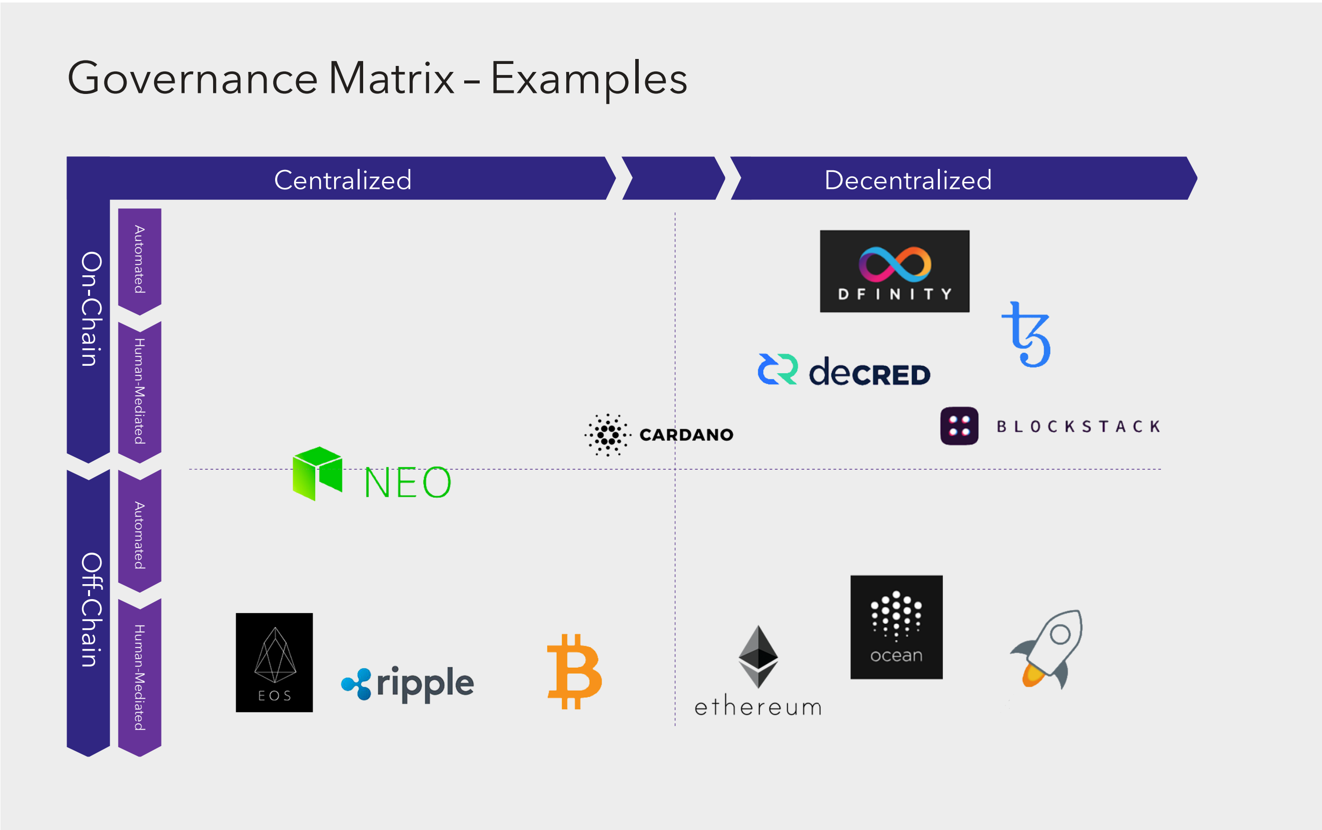


Figure 28: Governance matrix

Chapter 12

Summary of Findings

In order to create a new form of complex system, that is a ‘token ecosystem’, a new innovation process and toolbox was necessary. Therefore, in this report, we presented our phased strategic process to architect and engineer systems which will optimistically evolve into sustainable and complex token economies.

We find that this strategic process relies on establishing a team with an innovative and multidisciplinary mindset and requires expertise in areas including technology, strategy, economics, systems engineering, psychology, mathematics, law, finance, and experience/service design.

Our process is structured around three phases that consists of discovery, design and deployment, which we call the 3 Ds of Token Ecosystem Creation. The discovery phase defines the basis for establishing a tokenized system and associated system requirements. The design phase digs deeper into issues of market characterisation, governance, and proposes a minimum viable token. Finally, the deployment phase validates and tests the parameters of the system. Token ecosystem creation is an iterative process in which optimization is present throughout all these three phases.

We offer a pragmatic and flexible toolbox to create a ‘pathway to decentralization’ in order to achieve high degrees of decentralization and automation over time. We conclude that evaluating decentralization in the blockchain domain is multidimensional as it requires considering the type of consensus formation, conflict resolution, platform development, value capture at the network level and other issues around governance. We believe that a project should consider its optimal degree of decentralization at various stages and layers of the network.

Blockchain is a foundational technology that has the potential to transform business models and industries by reshaping organizational structures and their governance. Our toolbox tries to address issues related to designing and testing the behavior within this context. However, stakeholders involved in a tokenized network have differing perceptions, goals, and expectations within this system. Consequently, modeling incentives and computing the appropriate network objective function is a real challenge, especially when informational asymmetries are present among market and network participants. For example, aspirations of initial investors that are essential to the creation of a new ecosystem will need to be balanced with the needs of the end users of such system, where valuations by these differing types of actors can be varied.

Therefore, we believe that over time, tokenization will evolve to produce specific categories of token models, where we observe a differentiation between the role of tokens as security versus utility. This split should allow for better design, optimization and performance metrics. Token ecosystems need to work on developing network metrics and computational signals as a compass. In order to navigate in such complex systems, it is crucial that we continue to work on developing reliable indicators of the economic and technical health of a network.

Chapter 13

Concluding Remarks

By combining blockchain architecture with specialized incentive systems, it should be clear that we are creating token ecosystems that offer a new way to efficiently allocate, coordinate and govern resources within a network. They help us optimize, coordinate and better distribute value by acting as an interface between the ledger and market layer as long as they are engineered to optimize security and economic alignment.

In effect, these token ecosystems are a new form of business (and governance) model that help us meet the previously unfulfilled needs and goals of consumers, end users and other network constituents and promise a cambrian explosion of economic organization, reorganization and growth. They have the potential to measure new forms of value and exchange that may currently go unrecorded, and as such be under-represented and under-appreciated in today's capitalistic framework. Therefore it is important we begin to increasingly characterise the nature of these systems to better understand how they behave and advocate their wide-ranging potential.

We have stressed an effective token architecture should satisfy the needs of its market and associated business models, while incentivizing network nodes to sustain the ledger in a healthy manner for 'Token-Network Fit'. We have hopefully convincingly articulated this is only possible through an iterative process that combines both top-down and bottom-up approaches of business modeling, experimentation, testing and ongoing optimization.

Looking beyond this paper, it is critical we better explore how these networks evolve and how we measure their performance to the same level of understanding we have of the other Internet business models such as SaaS, which we now know evolve from targeted growth hacking and freemium models to subscription-based monetization. We need comparable metrics like conversion rates, churn, monthly recurring revenue and customer acquisition costs to provide guidance on network growth, their financing and ongoing health for critical decision making and stewardship.

Although innovations in genetic programming and evolutionary algorithms have the potential to continually optimize a tokenized ecosystem, we first need a better understanding of basic network dynamics and how to monitor them such as: throughput, latency and transactions volume.

It is also important that we find ways to decentralise network adoption in a more methodical manner in order to generate replicable token models with actionable go-to-market strategies. This will allow the community to better comprehend what token models represent the best business viability for a given ledger and market(s) and deploy them accordingly. We cannot stress how urgent and critical we believe a more open and decentralized approach to software innovation is, one ultimately less fragile and therefore less wasteful than the 90% startup failure-rate seen in equities where all value is often lost forever.

Over time, we hope tokenization will evolve to produce more nuanced and specific categories of token models, with the likely decoupling of the security and utility features of a token. Such a separation would allow for a clearer differentiation of the value generated within an economy from those simply assessing its future value, and greatly assist the current theory of cryptoasset valuation, first seen in Chris Burniske's seminal MV=PQ model. This would allow the field to capture the velocity of transactions within an economy, seperate it from the speculative velocity in the secondary market, and begin to allow us to take a derivatives-based approach to valuation, as proposed by Akseli Vertinen of the Economic Space Agency. This is where a put option could be connected to the underlying asset with clearer ability to measure the economic value of the utility token.

Furthermore, this process can better position projects to develop the network metrics and computational signals they need to navigate such complex systems. These serve, not only as reliable indicators of the economic and technical health of a network, but also as 'fundamental analysis' for those valuing networks for over their long-term futures.

Despite these big challenges, we are optimistic in the long-term growth and success of token economies because, through a headline-grabbing nascent 'crypto' industry their promise has caught the attention of a whole generation of entrepreneurs, innovators and a braintrust of brilliant minds from around the world. This can best be seen by the growing global Token Engineering community, founded by Trent McConaghy, which we actively support through the London, Toronto and Chicago chapters.

In many ways greed is still a powerful motivating factor, however we hope after the 'crypto winter', which precedes this paper, people will increasingly be attracted by the social mission of a more decentralized and equitable Web at a moment of existential threat from a handful of monopolistic platforms. We hope sharing our token ecosystem creation process will assist in the acceleration of this process.

Importantly, until token ecosystems can consistently achieve economic alignment amongst a majority of network participants, confidently secure against attack vectors and demonstrate a high degree of decentralization and token utilization, it can only be considered a well-funded experimental distributed network. Only if all these criteria are achieved, can we credibly consider our system an established token economy to counter naysayers.

Appendix

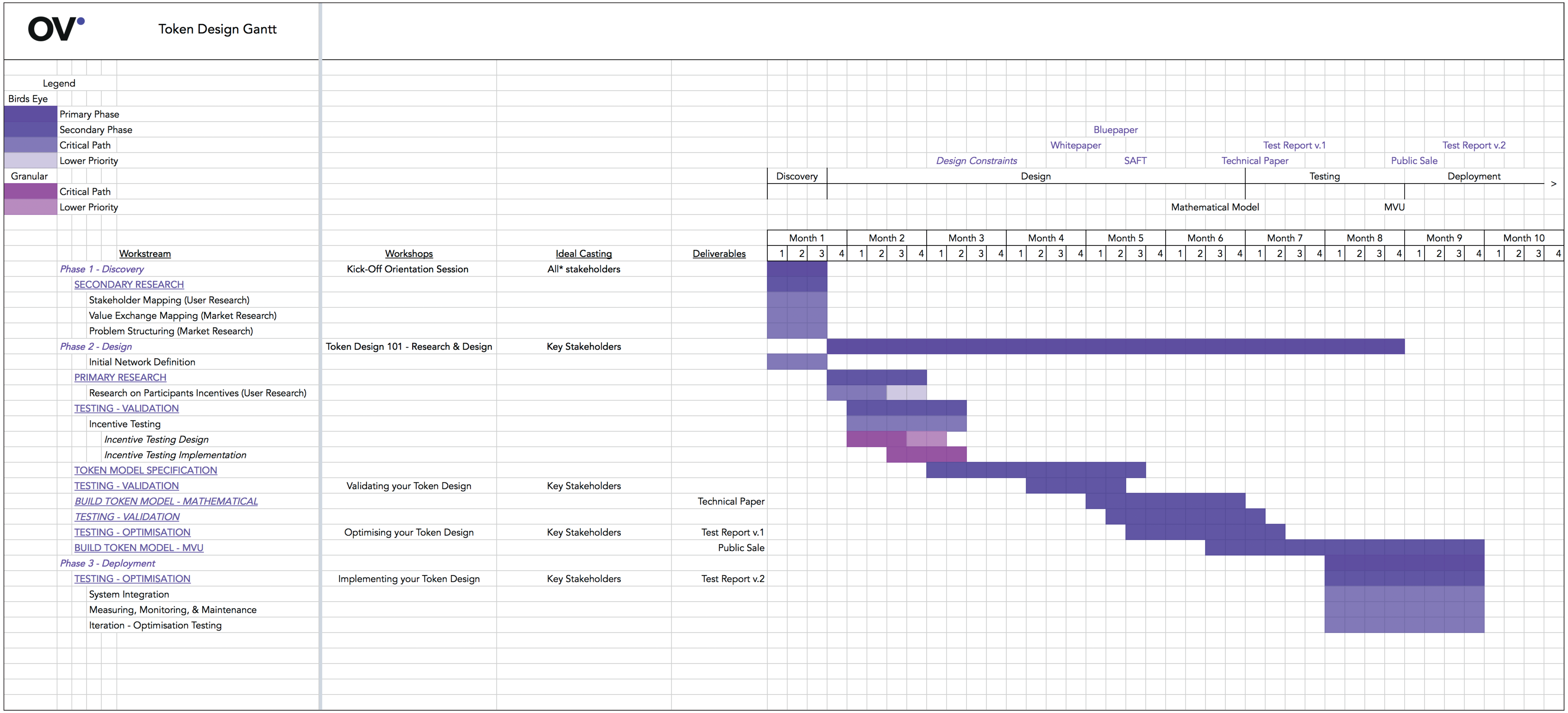


Figure 29: GANTT chart example at overall project level.

Token Utility Canvas

Network Design	Market Layer	Ledger Layer
Participants		
Undesired Behaviors		
Desired Behaviors		
Mechanisms		

TOKEN

Type:
Use & Role:
Underlying Value:

VALUE PROPOSITION

Value Creation:
Value Capture:

EXPERIENCE

Personas:
Channels:
Journey Map:

Figure 30: Token Utility Canvas template

Example: Javelin Board

ASSUMPTION	EXPERIMENTS	1. Surveys	2. Experiments	3. Simulations	4. A/B Tests
PARTICIPANTS – Developers – Market Participants – Ledger Participants	PARTICIPANTS				
PROBLEM Problem 1 – Issue 1 – Sub Issue 1 – Sub Issue 2 – Issue 2	PROBLEM				
INCENTIVES – Schelling Point – "Carrots vs Sticks" – Participants Specific – Market vs. Ledger	INCENTIVES				
SOLUTIONS A – TCR B – Layered TCR C – Bonding Curve D – B+C	SOLUTIONS				

Figure 31: Javelin Board template

For more information about the Token Ecosystem Creation process, or if you would like to contact us about a new or existing tokenized project, please contact us.

For research or project enquiries:
research@outlierventures.io

For marketing or event speaking enquiries:
speaking@outlierventures.io

Member of

Design by www.studiobowden.com

Photography credits (in order):
Maxime Le Conte des Floris, Lee Ferrell, Sven Read, Marc Sendra Martorell, Stanislav Kondratiev

Outlier Ventures

www.outlierventures.io