Prospects of Distributed Ledger Systems: Requirements Engineering
And Analysis of existing Mechanisms for Multidimensional Incentive Systems

Project studies in Management and Technology
TU Munich – Final Report

Examiner: Prof. Dr. rer. nat. Sebastian Pfotenhauer

Authors: Max Rößner, TUM School of Management
Dr. Marcus Dapp, ETH Zürich COSS
Felix Fach, LMU Institute of Political Sciences

Submitted: October 15th, 2018

Word Count: 11,007 (Introduction to Conclusion)
# Table of Contents

1 Introduction .................................................................................................................. 6

2 Requirements engineering and agile development ....................................................... 8
  2.1 Fundamentals of requirements engineering ............................................................... 8
  2.2 Limitations and need for agile development ............................................................. 10

3 General overview of the Finance 4.0 system ................................................................. 11
  3.1 Stakeholder analysis ................................................................................................. 11
  3.2 System context and boundaries ............................................................................... 12
  3.3 High-level architecture description ......................................................................... 12
  3.4 Cryptoeconomic design .......................................................................................... 13
  3.4 Governance design ................................................................................................. 15
  3.5 System functionality ............................................................................................... 16

4 Requirements of Finance 4.0 system ........................................................................... 18
  4.1 Governance Tokens (GTKNS) .................................................................................. 18
  4.2 Externality Tokens (XTKNS) ................................................................................... 19
  4.3 Identity Management (ID) ....................................................................................... 20
  4.4 Data Management (DAT) ....................................................................................... 20
  4.5 Cryptoeconomic Design (CED) ............................................................................... 21
  4.6 Internal Operations (IOP) ....................................................................................... 22
  4.7 Legal (LEG) ............................................................................................................ 22
  4.8 External governance (XGOV) .................................................................................. 22
  4.9 User experience (UX) ............................................................................................. 23
  4.10 Non-Functional Requirements (NFR) ..................................................................... 23

5 Analysis of DLT systems ............................................................................................. 25
  5.1 Selection of DLT systems ......................................................................................... 25
  5.2 Analysis of DLT systems .......................................................................................... 25
    5.2.1 Aragon – Arbitration mechanisms for DAOs ....................................................... 25
    5.2.2 District0x – Curation mechanism for communities ........................................... 28
    5.2.3 Bancor – Automated liquidity for cryptographic assets ..................................... 30
    5.2.4 Augur – Decentralized prediction market .......................................................... 32
    5.2.5 Oraclize – On-chain verification of data authenticity ......................................... 35
    5.2.6 Sia – Peer-to-peer cloud storage ...................................................................... 36
  5.4 Conclusion on analysis of DLT systems .................................................................... 38

6 Conclusion on Finance 4.0 .......................................................................................... 40

List of References ............................................................................................................. 41
<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>United Nations Sustainable development goals</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Requirements engineering template by Pohl and Rupp</td>
<td>9</td>
</tr>
<tr>
<td>3</td>
<td>Kano Model taken from Pohl and Rupp</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>Finance 4.0 stakeholder map</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>Finance 4.0 high-level architecture</td>
<td>13</td>
</tr>
<tr>
<td>6</td>
<td>Arbitration process of the Aragon jurisdiction</td>
<td>28</td>
</tr>
<tr>
<td>7</td>
<td>Simplified prediction process in Augur</td>
<td>34</td>
</tr>
<tr>
<td>8</td>
<td>Fetching and verifying date through Oraclize</td>
<td>35</td>
</tr>
<tr>
<td>9</td>
<td>Storing files with Sia</td>
<td>37</td>
</tr>
</tbody>
</table>
**Table of Tables**

Table 1: List of requirements for Governance Tokens (GTKNS) .................................................. 18
Table 2: List of requirements for Externality Tokens (XTKNS) .................................................. 19
Table 3: List of requirements for Identity Management (ID) ....................................................... 20
Table 4: List of requirements for Data Management (DAT) ....................................................... 21
Table 5: List of requirements for Cryptoeconomic design (CED) .............................................. 21
Table 6: List of requirements for Internal operations (IOP) ....................................................... 22
Table 7: List of requirements for Legal (LEG) ........................................................................... 22
Table 8: List of requirements for External governance (XGOV) ............................................... 22
Table 9: List of requirements for User Experience (UX) ............................................................ 23
Table 10: List of Non-Functional Requirements (NFR) ............................................................. 23
Table 11: Overview of tokens in the Aragon Network ............................................................... 26
Table 12: Overview of district0x token ..................................................................................... 29
Table 13: Overview of Bancor token ......................................................................................... 31
Table 14: Overview of Smart Token configurations ................................................................. 31
Table 15: Overview of Augur token ......................................................................................... 33
Table 16: Overview of Sia token .............................................................................................. 36
1 Introduction

The Finance 4.0\textsuperscript{1} research group at ETH Zurich uses this document to record their conception of a multi-dimensional incentive system called Finance 4.0. Max Rößner and Felix Fach supported the team in the requirements engineering. They compiled this document and conducted the technology analysis (See Section 5). The document contains a first list of requirements for the demonstrator of the Finance 4.0 concept compiled in May and June 2018. We invite any interested reader to examine the proposed ideas and encourage you to get in touch with us if you wish to give feedback and support the further development.

Finance 4.0 is a multi-dimensional incentive system. Our major goal is to help individuals and communities around the world to improve their living conditions and support the accomplishment of the United Nations Sustainable Development Goals (see Figure 1). In our opinion, new and complementary growth principles are necessary to address global challenges such as resource shortages, climate change, economic dislocation, and unemployment. Finance 4.0 wants to provide a platform that allows for the exploration of mechanisms for self-organization, co-creation, co-evolution, and collective intelligence to tackle the mentioned issues.

![Figure 1: United Nations Sustainable development goals\textsuperscript{2}.](image)

There are various and diverse groups of potential users of the Finance 4.0 system. They are individual citizens, communities, non-government organizations, international agencies as under the United Nations Organization (UNO), academic institutions, software development

\textsuperscript{1} Finance 4.0 is a research group at ETH Zurich and part of the FuturICT 2.0, an international European Project funded under the FLAG-ERA Joint Transnational Call.

\textsuperscript{2} For more information see: https://sustainabledevelopment.un.org/?menu=1300.
groups and technology partners as main stakeholders of the Finance 4.0 system. This document, however, is meant for any interested reader.

In the remainder of the document, we present our approach to requirements engineering (section two), a general overview of the Finance 4.0 system (section three), the requirements of the system we defined as of June 2018 (section four), and an analysis of six selected DLT systems (section 5). We conclude on our development in section six and provide a brief outlook in section seven.
2 Requirements engineering and agile development

2.1 Fundamentals of requirements engineering

Within the requirements engineering for the Finance 4.0 system, the team followed established methods and practices to determine, document, and classify the requirements. In the following paragraphs, readers unfamiliar with software engineering find the necessary theoretical background.

The goal of requirements engineering is to establish a shared understanding of the purpose of a system within the development team and with other stakeholders in particular the client. Through requirements engineering, the development team defines the boundaries of the system, i.e. what functionality the use can expect from the system and vice versa what the system requires as input from the user and its environment to provide the functionality.

To discover the requirements of the Finance 4.0 system, the development team relied on common methods as presented by Pohl and Rupp (2015) and practices identified in the context of agile development (Paetsch, Eberlein, & Maurer, 2003; Ramesh, Cao, & Baskerville, 2007). The team held several internal workshops, drafted user stories and scenarios, build a stakeholder map relating stakeholders’ influence and stakeholders’ interest (see Section 3). Based on the map, the team conducted several interviews with potential users and technology partners. Members of the team gave multiple presentations at conferences, meetups, and to the members of the chair of Prof. Dr. Dirk Helbing for Computational Social Science (COSS) at ETH. Together, the different modules of the requirements engineering allowed the team to iterate and extend the initial set of requirements several times.

The team documented the requirements using natural language. The requirements template provided by Pohl and Rupp (2015, Chapter 5) served as a guide together with a collection of quality criteria under the ISO/IEC/IEEE 29148:2011 standard. The requirements template is a “blueprint for the syntactic structure” of each sentence describing a requirement (see Figure 2) (Pohl & Rupp, 2015, Chapter 5). The template allows for only one requirement per sentence and encourages short sentences which reduces the potential for ambiguities and improves comprehensibility. Additionally, the ISO/IEC/IEEE 29148:2011 standard comprises seven quality criteria. According to the standard, requirements should be (1) consistent, (2) unambiguous, (3) necessary, (4) verifiable, (5) feasible, (6) traceable, and (7) complete.

---

3 For more information see: https://www.iso.org/standard/45171.html.
To make the collection of requirements easier to read and understand, Finance 4.0 distinguishes requirements with respect to three dimensions. Firstly, each requirement has a type: functional, non-functional or quality, and constraint. A requirement, more formally, is “a capability or condition needed by a user to solve a problem or to achieve an objective” (Pohl & Rupp, 2015, Chapter 1). Functional requirements concern the “result of a behavior (...) provided by the system” (Pohl & Rupp, 2015, Chapter 1). Non-functional or quality requirements describe properties such as performance, availability or scalability of the system that are independent of the functions of the system. Constraints are requirements that restrict the number of possible solutions “beyond what is necessary for meeting the given functional requirements and quality requirements” (Pohl & Rupp, 2015, Chapter 1).

Secondly, each requirement has a Kano category as presented in the Kano Model (Matzler & Hinterhuber, 1998; Pohl & Rupp, 2015, Chapter 3). The model relates customers’ expectations to the customers’ level of delight. The model distinguishes three categories of requirements or product features: Delighter, Satisfier, and Dissatisfier (see Figure 3). A requirement is a dissatisfier if the feature is expected by the customer and the lack of it, consequentially, leads to disappointment by the customer. At the same time, the “more” the dissatisfier property is provided the smaller the additional delight generated. For a requirement that is a satisfier on the other hand, the additional delight increases proportionally. A delighter requirement behaves opposite to a Dissatisfier. The customer does not expect it, but her delight increases disproportionately the more of the feature she receives (Pohl & Rupp, 2015, Chapter 3).
Finally, after classifying all requirements with respect to their type and Kano category, we grouped them in thematic classes yielding ten groups as presented in section 4.

2.2 Limitations and need for agile development

Determining the complete set of requirements of a system, is only possible on a certain level of abstraction. A first set of high-priority, high-level user-facing requirements serves as basis for the system design. During system design and development, the team iteratively discovers various more fine-grained requirements related to the technologies examined and used. They may force the team to go back to their clients and adjust some of the previously-defined requirements. Changes due to missing requirements are significantly more expensive closer to the launch of the system (Pohl & Rupp, 2015, Chapter 1).

The technology domain of Finance 4.0 comprises distributed ledger technology and the Internet of Things. Both fields are immature, quickly evolving, and have few established standards today. Within the three-year lifetime of the Finance 4.0 project, significant changes of the technology can be expected as well as the emergence of new applications in the domain of sustainability where collaboration would be favorable but may require adjustments to the previously-determined requirements. The Finance 4.0 team uses an agile development approach which aims to welcome these changes and prioritizes speed together with the continuous delivery of working code over documentation (Martin, 2002). The Finance 4.0 team tries to build on existing solutions wherever possible. The result of requirements engineering is a minimal set of persistent features of the system. The entire development team understands and agrees on requirements collected and presented in section 4.
3 General overview of the Finance 4.0 system

3.1 Stakeholder analysis

Finance 4.0 seeks to support a lively, diverse, and geographically-spread out community of users. Communities that strive for more effective self-organization are our key audience. The following stakeholder map is a summary of the participants and interest groups for the Finance 4.0 system. Each stakeholder can be classified by her interest and influence on the system.

![Stakeholder Map](image)

Three clusters can be identified. We consider cluster (1) to be less interested in the Finance 4.0 system. Depending on the implementation and the technology Finance 4.0 uses, however, cryptocurrency owners and IoT-Hardware Providers could have noticeable influence on the success of the project. We expect significant interest from members of cluster (2) where we assume cities and regions would influence Finance 4.0 the most. Cluster (3) comprising a diverse user community, complementary currency groups and our technology partners will have probably both the greatest interest in and impact on the Finance 4.0 system. The interest and possible influence of complementary currency initiatives and potential groups of individual users are the key stakeholders of the requirements engineering together with Finance 4.0 technology partners. Under the current mission of the system, we have not identified parties opposing the development.
3.2 System context and boundaries

Finance 4.0 draws inspiration from existing initiatives in the area of community currencies such as BrixtonPound\(^4\) in the UK and complementary currencies like the Rotterdam NU\(^5\) scheme in the Netherlands. Community currencies aim to protect and enhance the social well-being of a community. The community does not need to be defined by geography but by profession or political orientation. The projects build on the principles of empowerment, self-organization, social exchange, and reciprocity (Blanc, 2011).

Complementary currencies, on the other hand, are independent of a social space but strive to protect and promote certain economic activities. These can be, for example, saving energy or recycling waste. Many of the projects pursue causes related to sustainability. The basic idea is to do, what economist call, internalization of externalities\(^6\), i.e. accounting for the costs that are not yet included in the price of a particular resource or economic activity. For example, a user indifferent between taking the bicycle or the car cannot easily assess the cost of taking the car in the form of CO2 produced to her environment. Here, Finance 4.0 comes in. User-created projects, so called externality projects, incentivize the more sustainable behavior through an externality token. As these projects are created bottom-up, they make use of information not available to top-down decision making and thereby consider the costs of a certain economic behavior from a local perspective.

Schemes such as the Rotterdam NU are increasing complex promoting a large set of economic activities. which makes governance more difficult (Blanc, 2011). This leads the teams to fall back to hierarchical structures beating their founding principles of self-organization and participation (Gómez, 2012). Blockchain technology is still in its infancy. In our opinion, however, existing projects such as Aragon or Kleros foreshadow the potentials to overcome governance-related challenges of bottom-up projects such as complementary currencies. As the development infrastructure around the technology improves, the technology may become accessible to every community and individual. Finance 4.0 aims to be at the center of this development.

3.3 High-level architecture description

As of July 2018, the Finance 4.0 system comprises four main components: (1) a governance module allowing the user community to take decisions on the rules governing the behavior of the network of externality projects. Part (2) is the network of externality projects. Each project aims to incentivize a particular economic behavior advancing one or more sustainability goals.

---

\(^4\) For more information see: [http://brixtonpound.org](http://brixtonpound.org).


\(^6\) An externality is the consequence of an economic activity that is not reflect in the market price. Imagine a manufacture pollutes the surrounding environment through her production but does not have to pay the cost for recovering the environment. The pollution is the externality. Economist now try to think of mechanisms that allow the internalization of the externality, i.e. make the manufacturer carry the cost, if possible directly, to incentivize a different behavior. For more information see [https://eml.berkeley.edu/~saez/course131/externalities1_ch05.pdf](https://eml.berkeley.edu/~saez/course131/externalities1_ch05.pdf)
The first demonstrator of the Finance 4.0 system will have at least one externality project to showcase the functionality and operation of a project. Thirdly, the demonstrator will contain (3) a token creator that enables users to easily create and operate their own externality tokens and projects. Finally, the Finance 4.0 system will provide some form of (4) liquidity provision mechanisms to support projects that are considered valuable by the user community.

On a conceptual level, the creation of an externality project looks as follows. The user selects an externality that she wants to reduce (e.g. CO2, waste, corruption) or promote (e.g. social work) in her community. The user determines the actions that she wants to reward. She ties them to one or several proof mechanisms selected from a provided list or suggests new ones. Different actions and their proofs are mapped to different amounts of the externality token as reward. The user promotes the externality token to various service providers to support her project. This gives the externality token value beyond the reputation and commitment represented through the token within the community.

In summary, the Finance 4.0 system needs technologies for sensing, storing, proving, tokenizing, pricing, and trading presented in Figure 5. The system will make use of the emerging Internet of Things (IoT) to enable measurements and proving at large scale.

---

3.4 Cryptoeconomic design

In different situations, different factors drive human motivation. For example, money is the expected reward for work. It would be curious of an elderly person to offer another person money for helping her to cross the street. In school, a student may be motivated more by recognition from peers than the actual grades. And, similarly, a software developer in open source software development may gain primarily reputation not money\(^7\). As diverse as the factors are that drive human motivation, Finance 4.0 aims to provide an incentive system that does not simply reduce motivation to some form of monetary reward.

Blockchain tokens signify opportunities and challenges in this regard. They allow to bootstrap a network quicker by giving an incentive to early entrants. However, they encourage speculation without much concern for the underlying technologies and ideas of the different projects. Finance 4.0 is a multi-dimensional incentive system. It experiments with different incentive schemes and provide users with a variety of mechanisms to enhance commitment for their selected sustainability causes within their community.

Beyond technical infrastructure, Finance 4.0 wants to provide financial support to projects considered valuable by the community. This can be, for example, through the provision of liquidity by the native Finance 4.0 token. Any project accepted into the list of reputable projects will be able to back its externality token by the Finance 4.0 token. This gives value to the externality token and allows the user to more easily exchange the token into other tokens in the system. The Bancor protocol, for instance, provides a new liquidity mechanism\(^8\) that could be used within Finance 4.0. There, the exchange between token does not involve any centralized exchanges operated by third parties. The so-called smart token always holds a balance in connected tokens and algorithmically determines the price of the main token based on the demand for the connected token. This allows for a reliable, immediate, and transparent exchange and control of the creator of the token on the exchangeability with other tokens.

As discussed above, Finance 4.0 does not want the different incentive dimensions to collapse into one through exchange. Therefore, different mechanisms that allow the projects to introduce friction need to be available within the token creator to limit the exchanges if needed. We expect to see the superior designs to emerge through selection by the user community.

Apart from the challenges of balancing short- and long-term incentives when designing and incentive system, negative externalities as subject pose two problems. The first is that major producers of a negative externality in most cases have no intrinsic incentive to change their behavior. Since the participation in the Finance 4.0 system is voluntary (opt-in), it needs to be attractive to them in some other form in the long term.

A reduction of negative externalities is not straightforward to represent through a coin. With a positive externality, the good work done can be rewarded with a proportionate amount of token. To represent a negative externality, however, is more difficult. A negative token is not meaningful on its own. One possible design would be to have a balance of negative externality token that the user can offset through an exchange with positive externality token. This would require her, however, to have a balance of positive token. The open challenge is to tie these negative externality token to some form of noticeable disincentive while ensuring the system is still attractive for the major producers of these externalities.

We see great potential in communities as the unit of decision-making to address the issues of sustainable economic behavior. Blockchain token could provide more efficient coordination

---

\(^8\) For more information see: https://about.bancor.network/protocol/.
mechanisms compared with existing complementary currency schemes. Further, tokens allow communities to experiment with incentive designs on an unprecedented scale while being transparent. Finance 4.0 strives to be the laboratory for these experiments in incentive designs. As an open platform, it will make the successful mechanisms available to potentially every individual and community around the world.

3.4 Governance design

The Finance 4.0 system will have a transparent and decentralized governance model taking advantage of the concept of the wisdom of the crowds⁹. In this section, we present five concepts that are important for the Finance 4.0 system.

One project that brought significant public attention to the blockchain domain was the creation of the first Decentralized Autonomous Organization (DAO) called TheDAO in 2016 (“Crunchbase.com,” 2018). A DAO is an organization whose complete set of rules is documented through code in the form of so-called smart contracts stored on a blockchain. Smart contracts are, simply put, if-this-then-that-statements. They allow two or more individuals to write an agreement and be sure it will be enforced once it is stored on the blockchain. Smart contracts provide this feature independent of any jurisdiction or external enforcement body. The DAO is, in this sense, autonomous that it reacts the way it was programmed without further need for users’ actions and reliance on a third-party. Changes to these rules are only possible through the previously agreed-on governance mechanisms. This high level of transparency and reliability could make DAOs a powerful tool for international collaboration. Although the initial DAO was hacked¹⁰ showing the immaturity of the concept, the idea of collective decision-making without third-parties inspired many projects such as Colony or Aragon¹¹. Finance 4.0 aims to use the concept of a DAO and collaborate with projects providing solutions in this space such as Aragon.

To operate a sophisticated governance system such as a DAO, Finance 4.0 will need some form of identity service for users who access core functionalities and services. There are several providers in the blockchain community such as uPort or Onename¹². These projects provide identity to their users that are independent of any third-party. Similar to the email protocol, the company only provides an interface, the underlying technology, i.e. the identity comprised of attestations and a history of transactions, remains independent of the company and cannot be deleted. In Finance 4.0 wants to provide both a native identity solution. The support and integration of external providers is not yet decided.

---


¹⁰ For more information on the DAO hack see for example: https://www.bloomberg.com/features/2017-the-ether-thief/.

¹¹ For more information see: https://aragon.one and https://colony.io.

The Finance 4.0 network will consist of a variety of different externality projects. There will be disputes between projects and individuals. As of July 2018, the issue of dispute settlement mechanisms is still open. Some form of arbitration mechanism operated by senior users is most likely unavoidable. Projects such as Aragon serve as an example. The Aragon network maintains a decentralized jurisdiction where every user can become a judge through staking some amount of token. As the user participates in trials and passes sentences acceptable to the majority of the user community, she will gain reputation and thereby more influence in the jurisdiction. Three layers of courts in the case of Aragon protect the system against arbitrary decisions by judges focusing on the short-term only. Further mechanisms are in place to prevent collusion of judges and prevent spamming of the jurisdiction. These mechanisms are complex. The development team will evaluate carefully whether and to what extent arbitrations are needed.

Another component in the Aragon jurisdiction that Finance 4.0 considers using within its governance are decentralized prediction markets. In a prediction market, users trade shares of outcomes for an event. In a decentralized prediction market, a second group of users reports on the outcome of the event which then determines the pay-off for traders. A token and fees given to active reporters incentivizes the truthful reporting by a diverse group of users instead of a single central entity. Using the wisdom of the crowds again, this mechanism may produce more reliable and sustainable decisions.

Finally, Finance 4.0 will use a scheme called token-curated registry, TCR for short. A TCR is a list of items, services, people, or organizations compiled by a group of users through a vote. Each user purchases token that give her vote more weight. The number of tokens represents the stake of the user in the system. Economists call this economic proofing. The more money a user puts in, the more confident she is about her vote. To prevent centralization, Finance 4.0 limits the number of votes one user can aggregate, for example, to five percent through mechanisms like quadratic voting. The rational for why users want to participate in the TCR voting, is that their token holdings gain value. If the list is well-curated more users consult it and more projects want to be listed on it. Different designs exist, the general idea is that access or being listed to the registry requires purchasing the token which leads to its appreciation in value. The opposite applies if demand for the registry decreases. Finance 4.0 needs to balance accessibility of the mechanism to every user with rigor of curation as well as short- and long-term incentives.

3.5 System functionality

The development of the Finance 4.0 system comprises two phases. The goal of the first is to build a demonstrator with a small group of partners only. If the concept proves successful, a larger-group of partners can join to develop the full-fledged system in close collaboration.

---

13 For more information see the Aragon whitepaper available here: [https://github.com/aragon/whitepaper](https://github.com/aragon/whitepaper).

14 For more information see: [https://www.augur.net](https://www.augur.net).
The demonstrator will comprise a mobile app and a web app that give the user access to a wallet for the different externality tokens. Further, the demonstrator provides a basic version of the token creator and should host up to three externality projects build by the Finance 4.0 team and partners to showcase the process of proving an action, claiming and receiving tokens as well as spending and trading the token with other users. Ideally, the demonstrator will also contain a simple version of the Finance 4.0 governance scheme including, for example, the token curated registry of the existing projects.

A range of existing project should be able to integrate with Finance 4.0. Based on the major objective of the system, every externality – negative or positive – should be supported. As presented in section 3.3, there are a few conceptual challenges that need to be overcome beforehand. Existing projects suitable for collaboration with Finance 4.0 include the German terra0 group which aims to make a forest manage itself through a DAO. The regen.network is another project. Regen.network builds an infrastructure to measure biotopes with unprecedented detail. Finance 4.0 could use this infrastructure to automate its proving schemes. The World Wildlife Fund (WWF) also operates a project in Romania for eco-tourism that could be a suitable partner. There, different forms of gamification could support the ecotourism initiatives in the region.

The full system will build on the demonstrator and support use cases in more domains such as smart cities, energy, social equality, and data sharing. This requires consideration of legal and compliance issues, higher security standards, more sophisticated identity management, and involvement of a larger community of users and partners including the public sector. Finance 4.0 wants to become a global coordination mechanism. The vision is to foster a global mindset but allow communities to address challenges locally with a high-level of autonomy.
4 Requirements of Finance 4.0 system

Finance 4.0 distinguishes requirements with respect to type (functional, non-functional, constraint), Kano category (delighter, satisfier, dissatisfier), and the thematic group. The following thematic groups exist:

1. Governance Token (GTKNS),
2. Externality Token (XTKNS),
3. Identity Management (ID),
4. Data Management (DAT),
5. Cryptoeconomic Design (CED),
6. Internal Operation (IOP),
7. Legal (LEG),
8. External Governance (XGOV),
9. User Experience (UX), and
10. Non-Functional Requirements (NFR),

In the following paragraphs, we introduce each group and present the collected requirements. More requirements will be added within the sprints throughout the following months.

4.1 Governance Tokens (GTKNS)

The set of requirements under GTKNS specify on a high-level how users will govern the system. With a diverse community of users, the system needs to be as inclusive as possible. Reputation and self-organization are two important principles in the governance of Finance 4.0. The system will allow users to collectively curate a list of externality projects to facilitate the discovery of high-quality projects. Users will have the freedom to opt-out of the system at any time.

<table>
<thead>
<tr>
<th>GTKNS-01</th>
<th>System should allow the user to build reputation based on interaction with the system.</th>
<th>satisfier (°)</th>
</tr>
</thead>
<tbody>
<tr>
<td>GTKNS-02</td>
<td>System should use a concept of reputation for its governance.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>GTKNS-03</td>
<td>System should allow the user to receive Fin4 services (like loans) based on their reputation.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>GTKNS-05</td>
<td>System should be able to upgrade its own governance mechanisms.</td>
<td>satisfier (°)</td>
</tr>
</tbody>
</table>

Note that the list of requirements is the result of discussions of the entire FuturICT 2.0 team including Max Rößner and Felix Fach.
| GTKNS-06.01 | System should allow all users to participate in its governance. | satisfier (°) |
| GTKNS-06.02 | System should allow the user the ability to vote on in/exclusion of externality tokens. | satisfier (°) |
| GTKNS-07 | System should provide users mechanisms to settle disputes (e.g. challenge proofs after fact). | satisfier (°) |
| GTKNS-09 | System should allow any human or machine to register as a user (by receiving an address). | satisfier (°) |
| GTKNS-10 | System should allow only human users to participate in governance. | satisfier (°) |
| GTKNS-11.01 | System should give autonomy to its participating groups. System should provide citizens with the ability to decide on community preferences. | satisfier (°) |
| GTKNS-11.02 | System should allow users to build autonomous communities (e.g. own governance) around externality tokens. | delighter (+) |
| GTKNS-13 | System should use a governance mechanism enabled by a native token. | satisfier (°) |
| GTKNS-14 | System shall allow users to opt-out at any time. | satisfier (°) |

Table 1: List of requirements for Governance Tokens (GTKNS).

4.2 Externality Tokens (XTKNS)

XTKNS hold the core functionality of different externality projects. The Finance 4.0 system will provide an interface for users to build their own externality token. From different actions, proving mechanisms, and incentive schemes, users have the greatest flexibility possible to extend existing mechanisms and customize them for their needs.

| XTKNS-01.00 | System should provide users with the ability to design own tokens, according to parameters they set. | delighter (+) |
| XTKNS-01.01 | System should allow the user to define proofs of actions (proof of good work). | satisfier (°) |
| XTKNS-01.02 | System should allow the user to define an underlying to give a source of value to the externality token. | satisfier (°) |
| XTKNS-01.03 | System should allow the user to define inherent properties of a new token (e.g. economic policy, like cap/burn). | satisfier (°) |
Table 2: List of requirements for Externality Tokens (XTKNS).

<table>
<thead>
<tr>
<th>ID</th>
<th>Requirement</th>
<th>Satisfier/Delighter</th>
</tr>
</thead>
<tbody>
<tr>
<td>XTKNS-01.04</td>
<td>System should allow the user to define new externalities.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>XTKNS-01.05</td>
<td>System should allow the user to define new actions (incl. target group).</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>XTKNS-02.01</td>
<td>System should allow the users to broadcast their actions.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>XTKNS-02.02</td>
<td>System should allow the user to make claims on actions to obtain tokens.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>XTKNS-02.03</td>
<td>System may automatically create claims from actions taken by a user.</td>
<td>delighter (+)</td>
</tr>
<tr>
<td>XTKNS-02.04</td>
<td>System should be able to transform claims into tokens.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>XTKNS-02.05</td>
<td>System should allow for the creation of token units through performing actions.</td>
<td>satisfier (°)</td>
</tr>
</tbody>
</table>

4.3 Identity Management (ID)

ID is an important component of the Finance 4.0 system, but, as of July 2018, not sufficiently developed. After the successful development of the demonstrator, the full Finance 4.0 system will put significant effort behind the conception of a native, open, and reliable identity solution. The support and integration of external providers is not yet decided.

Table 3: List of requirements for Identity Management (ID).

<table>
<thead>
<tr>
<th>ID-01</th>
<th>Requirement</th>
<th>Dissatisfier</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>System should provide users with the ability to claim/integrate/import self-sovereign identities.</td>
<td>dissatisfier (-)</td>
</tr>
</tbody>
</table>

4.4 Data Management (DAT)

Within DAT, Finance 4.0 needs to balance user privacy and transparency. Blockchains are transparent and persistent data storage systems. Finance 4.0 wants to sustain these properties, yet, it has to give users the ability to control their data and provide them with a sufficient level of privacy.
Table 4: List of requirements for Data Management (DAT).

4.5 Cryptoeconomic Design (CED)

CED will consist of multiple tokens. The system will provide an exchange and liquidity provision mechanisms for externality projects build on top of it. Externality projects will create incentive and reward mechanisms and enable users to generate an additional income.

Table 5: List of requirements for Cryptoeconomic Design (CED).
4.6 Internal Operations (IOP)

IOP addresses the issues of interoperability of different native Finance 4.0 token such as for governance and user reputation both internally and to the outside. The system will make use of existing token standards and strive for inter-blockchain/project compatibility to the extent that it supports the system’s mission.

<table>
<thead>
<tr>
<th>IOP-01</th>
<th>System should provide user with the ability to register externally-created externality-tokens if they comply with the FIN4 standard.</th>
<th>delighter (+)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOP-04</td>
<td>System may provide user with the ability to register externally-created externality-tokens if they do not comply with the FIN4 standard.</td>
<td>delighter (+)</td>
</tr>
<tr>
<td>IOP-05</td>
<td>System should have native tokens (FIN 4) complying with ERC20/223.</td>
<td>delighter (+)</td>
</tr>
</tbody>
</table>

Table 6: List of requirements for Internal Operations (IOP).

4.7 Legal (LEG)

LEG contains requirements to ensure compliance with existing laws and regulations. It will be of significant importance for the full system.

| LEG-03 | System may provide projects with the tools to adhere to external regulations.                                                         | delighter (+) |

Table 7: List of requirements for Legal (LEG).

4.8 External governance (XGOV)

XGOV tracks interdependencies to stakeholders in particular governments and the administration. As with LEG, this section will be critical for the full system.

| XGOV-02 | System will introduce a taxing option for governments.                                                                               | satisfier (*)  |

Table 8: List of requirements for External Governance (XGOV).
4.9 User experience (UX)

The Finance 4.0 system should be accessible to the largest audience possible. Usability is therefore a major concern.

| UX-01 | System should be able to inform users about the costs and benefits of a specific action in an easy-to-understand manner. | dissatisfier (-) |
| UX-02 | System should provide the user with APIs to build new applications on top of it. | delitzer (+) |

Table 9: List of requirements for User Experience (UX).

4.10 Non-Functional Requirements (NFR)

NFR holds all requirements that cover either quality or are constraints to the Finance 4.0 system. These requirements will help the development team to make decisions in the face of trade-offs between different technologies.

<p>| NFR-01 | System should run on a permissionless blockchain/DLT. | dissatisfier (-) |
| NFR-02 | System will make use of mature scaling technologies. | dissatisfier (-) |
| NFR-04 | System should use technology chosen with respect to energy efficiency. | satisfier (<em>) |
| NFR-GTKNS-04 | System should build on insights from complexity science for its governance (e.g. self-organization, prediction markets, wisdom of crowds). | delitzer (+) |
| NFR-GTKNS-15 | System should prevent power concentration within its governance. | satisfier (</em>) |
| NFR-IOP-02 | System may be able to interact with other blockchains. | delitzer (+) |
| NFR-IOP-03 | System should require externality-tokens to comply with existing token standards (ERC20/223). | satisfier (<em>) |
| NFR-LEG-01 | System governance shall comply with relevant external regulations. | satisfier (</em>) |</p>
<table>
<thead>
<tr>
<th>NFR-Leg-02</th>
<th>System governance should promote user behavior compliant with external regulations.</th>
<th>satisfier (°)</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFR-MIS-02.02</td>
<td>System should be (cryptographically) secure.</td>
<td>dissatisfier (-)</td>
</tr>
<tr>
<td>NFR-PERF-01</td>
<td>System should store unproven claims (from actor/user) within x minutes.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>NFR-PERF-02</td>
<td>System should store proven claim (from prover) within x minutes.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>NFR-PERF-03</td>
<td>System should mint tokens (from proven claim) within x minutes.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>NFR-PERF-04</td>
<td>System should deposit tokens (from minted tokens) within x min.</td>
<td>satisfier (°)</td>
</tr>
<tr>
<td>NFR-UX-03</td>
<td>System UI should be intuitive (usability).</td>
<td>dissatisfier (-)</td>
</tr>
<tr>
<td>NFR-XGOV-03</td>
<td>System will be economically viable / self-sustainable.</td>
<td>dissatisfier (-)</td>
</tr>
</tbody>
</table>

Table 10: List of Non-Functional Requirements (NFR).
5 Analysis of DLT systems

5.1 Selection of DLT systems

The entire Finance 4.0 team agreed on the selection of the six projects covering four important domains to build the Finance 4.0 system. Aragon and district0x provide solutions for governance which Finance 4.0 requires for the governance of the externality projects and of the entire network. Augur and Oraclize both provide sources of external data and mechanisms to verify and input the data into a DLT system. The Finance 4.0 system will need to manage external data and verify the claims for different externality tokens. Sia is a storage platform that Finance 4.0 may integrate to provide storage for externality projects and users. Finally, Bancor gives liquidity to small-volume cryptographic assets. The Finance 4.0 system will be a diverse collection of small-volume cryptographic assets. The team evaluates how the system can use Bancor or similar schemes to support the externality projects.

5.2 Analysis of DLT systems

The following analysis of six selected DLT systems is in each case three-part. First, a brief introduction to the context and the motivation of the system; second, a detailed investigation of the different cryptographic tokens of the system as well as a selected central mechanism; and third, a brief conclusion and contextualization on the addressed issues. For each project, we reviewed, if available, its whitepaper, online documentation, and entry on Messari.io16, a website that features reviews of DLT systems.

5.2.1 Aragon – Arbitration mechanisms for DAOs

The Aragon system consists of two components: the Aragon Core and the Aragon Network. Aragon Core is a DAO framework for the programming language Solidity and a web-based decentralized app (dApp) that serves as a user interface to build and manage DAOs. The vision of Aragon is to enable the border- and permission-less creation of organizations (Cuende & Izquierdo, 2017).

Aragon Core uses the Ethereum blockchain provides the modules to build the logic for the behavior of the organization. Aragon identifies several important constructs in the context of an organization. They are identity, ownership, voting, capital, people, outreach, payment processing, accounting, and insurance. The current version (Aragon 0.5) comprises four modules that contain these characteristics. The four components are bylaws to define user permissions, a governance system, a capital management system for issuance and controlling of tokens, and an accounting system to manage the funds of the organization (“Aragon Wiki,” n.d.). Aragon is open source and modular; developers can add additional modules as they see need. Network fees and initial funding through an initial coin offering (ICO)(~$US 25 million) ensure the operation of the Aragon system (Zuller & Turner, 2018).

16 See: https://agora.messari.io/projects.
The second component, the Aragon Network provides three functions. First, further development of Aragon Core; second, maintenance of a digital jurisdiction for arbitration between and within organizations; and third, provisioning of the upgradability of Aragon Core smart contracts (Cuende & Izquierdo, 2017). In the following analysis, I focus on the second function, the digital jurisdiction.

The Aragon decentralized jurisdiction serves as an arbitration mechanism between and within organizations inside the Aragon Network. The network comprises three tokens. They are the Aragon Network Token (ANT), the Reputation Token (RT), and the Organization Token (OT) (Cuende & Izquierdo, 2017). To understand the arbitration process, only ANT and PT, however, are relevant. In the following paragraphs, I describe each token and the arbitration process.

The first token, the ANT, allows its holders to participate in the governance of the network and pay for network usage (Cuende & Izquierdo, 2017). The token is transferable and fungible with a fixed maximum supply (Zuller & Turner, 2018). Users of the network can gain and lose token through their actions in the network (see Table 1). More precisely in the context of the decentralized jurisdiction, the incentive design around the token aims to prevent the collusion of judges and ensure their ruling is in the interest of the majority. Further, the incentive system discourages spamming and motivates active participation from judges (Cuende & Izquierdo, 2017).

<table>
<thead>
<tr>
<th>Token</th>
<th>Purpose</th>
<th>Gain</th>
<th>Lose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aragon Network Token (ANT)</td>
<td>Governance/Jurisdiction</td>
<td>User purchases; User earns salary in token for providing beneficial services to the network; Judge gains token when she votes with the majority; User gains token when she revises a collusion of judges; Judge gains token when she rejects an arbitration verdict together with the majority of selected judges.</td>
<td>User selling token; User transacting in the network pays fees; Judge loses token when she votes with the minority for a verdict; Judge loses tokens when her verdict is overturned; User applies for arbitration and is rejected; Judge loses token when she is caught colluding; Judge loses token when she rejects participation in the court.</td>
</tr>
<tr>
<td></td>
<td>Network usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Collateral for agreements/contracts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation Token (RT)</td>
<td>Governance</td>
<td>Judge gains reputation when she votes for verdict in line with the majority of other selected judges.</td>
<td>Judge loses reputation when she votes for verdict in line with the minority of other selected judges.</td>
</tr>
<tr>
<td>Organization Token (OT)</td>
<td>Organization-specific</td>
<td>User joins a DAO that is part of the Aragon network and stakes ANT for issuance of the organization-specific token.</td>
<td>User leaves DAO that is part of the Aragon network and burns/exchanges the organization-specific token for his stake in ANT.</td>
</tr>
</tbody>
</table>

Table 11: Overview of tokens in the Aragon Network.

The second token, the RT, represents the seniority of judges. Higher seniority translates into eligibility for higher-value trials. A higher-value trial entails greater rewards for judges. Across all trials, judges gain RT for voting with the majority of judges. The RT is non-transferable. Fungible and not capped (Cuende & Izquierdo, 2017).

The last token, or tokens, are OTs. OTs are specific to an individual organization. The token allows users to join the organization and participate in its governance to the extent defined by the development team of the organization. OTs are transferable and fungible. Their supply
depends on the respective design of the OT by the development team. User sell their ANT to become members in the organization (Cuende & Izquierdo, 2017).

The arbitration process consists of three stages. In the first stage, a user applies for arbitration and puts down a collateral. The system selects a fixed number of judges randomly. Any user can be become a judge by putting down a collateral, too, that remains locked until she resigns. If any judge rejects participation, her collateral can be (partly) forfeited. If the majority of judges considers the application a spam, they refuse to sit the trial and share the collateral of the applicant. This discourages spamming. Otherwise, each judge comes to a verdict individually and submits it. A mechanism incentivizes judges to reveal the possible collusion of other judges. Therefore, collusion is not an attractive strategy. After the system revealed individual verdicts, the judges that decided with the majority receive RT. Further, the judges and the winning party share the collateral of the losing party (“Aragon Wiki,” n.d.; Cuende & Izquierdo, 2017).

The second stage starts if the losing party rejects the verdict or the dismissal of her application. To enter the second stage, she needs to put down a larger stake. The second court consists of a prediction market such as Augur (see section 5.2.4). Users of the prediction market determine a new verdict and report it to the Aragon jurisdiction. If the verdict differs from the ruling of previous judges, these judges lose both RP and ANT (“Aragon Wiki,” n.d.; Cuende & Izquierdo, 2017).

The third and final stage is a court composed of very senior users. The development team of Aragon selects these judges, and their ruling is final. If the user, however, does still no agree with the ruling, she is free to fork the Aragon network (“Aragon Wiki,” n.d.; Cuende & Izquierdo, 2017). This means, copy the entire code and run a new version of the same network except with verdict in her favor. The value of the network comes from the number of users, so the viability of this option for a user is questionable. Figure 6 illustrates the arbitration process.
Governance is an essential element of any DLT system. The intense debates around how to scale Bitcoin or how to deal with the DAO hack in Ethereum and the respective splits of the two communities underscore the significance of robust, fair, and transparent governance mechanisms. Even in non-hierarchical groups power structures will eventually emerge. In several DLT designs, developers equate the number of tokens, i.e. money, with participation rights in the governance. They anticipate that the fear of having token forfeited, i.e. losing money, is a solid incentive. Both assumptions may not hold in every situation. Designers of DLT incentive systems need to think about governance design right from day one and also look at it from a non-monetary perspective.

5.2.2 District0x – Curation mechanism for communities

District0x aims to become a network of decentralized marketplaces and communities. The idea is to enable groups to self-organize around a cause via economic incentives and without the need for a central entity (Urgo, Lestan, & Khoriaty, 2017). Districts are akin to forums. Existing examples are Ethlance, a freelance job market, or Meme Factory, a platform to build and sell memes (“District0x Educational Portal,” n.d.).

District0x comprises two main components that live on the Ethereum blockchain: the d0xINFRA framework and the district0x Token. D0xINFRA is an open source framework of smart contracts and front-end libraries. It provides the following four functionalities: posting and listings, search and filtering, ranking and reputation, and payments and invoicing. The framework refers to Aragon Core to implement the governance system of a district (see section 5.2.1 on Aragon). D0xINFRA is modular and extensible which allows third-party developers to offer new features and the district creators to customize the district (Urgo et al., 2017).
The second component, the district0x Network provides the coordination mechanisms to curate the network of districts. In the following analysis, I will explain the workings of the district0x curation mechanism and the purpose of the three types of tokens, the district0x Network Token (NT) the District-Specific Token (DT), and the Payment Token (PT) (see Table 12). All tokens are transferable and fungible. The supply of NT is fixed. The network fees and initial funding through an ICO from June 28th until August 1st of 2017 (~$US 9.8 million) ensure the operation of district0x (Bonello & Turner, 2018b).

<table>
<thead>
<tr>
<th>Token</th>
<th>Purpose</th>
<th>Gain</th>
<th>Lose</th>
</tr>
</thead>
<tbody>
<tr>
<td>district0x Network Token (NT)</td>
<td>Network governance (including selection of updates) - Access to single districts governance</td>
<td>Vote with the majority of token holders on acceptance of application of a project to become member of the TCR - Close district and receive NT for DT</td>
<td>Applicant loses staked token if her application to the TCR is challenged and rejected by the majority of participating token holders - Challenger loses staked token if her challenge is rejected by the majority of participating token holders - Exchange NT for DT - Open district and receive NT for DT</td>
</tr>
<tr>
<td>District Token (DT)</td>
<td>District governance - Project-specific</td>
<td>NT holder receive token for staking their NT with the project, i.e. joining a new district which allows them to participate in the governance of the new district - Open district and receive NT for DT</td>
<td>NT holder lose token once they leave a district and receive NT in return - Exchange for DT for NT - Close district and receive NT for DT</td>
</tr>
<tr>
<td>Payment Token (PT)</td>
<td>Payments (e.g. Ether)</td>
<td>Developer receives token for providing additional modules to the system</td>
<td>User uses modules provided by developers</td>
</tr>
</tbody>
</table>

Table 12: Overview of district0x token.

The PT is a token that is not native to the district0x system such as Ether, the native currency of Ethereum. One purpose of the token, according to Bonello and Turner (2018b), is payments. For example, district creators pay developers of additional modules in PT for their usage. The use of a separate token for payments is an update to the initial system laid out in the whitepaper. There, network members used NT for payments (Urgo et al., 2017).

The second token, the DT serves, akin to Aragon’s organization token (OT), as intra-district coordination mechanism. Governance and participation in a district make use of the DT. The development team and the members of each district decide on the rights and responsibilities that come with the ownership of the token (Urgo et al., 2017). There are very different governance designs possible for all kinds of purposes of the different communities.

The third and most important token, the NT, enables users to evaluate the different districts. At large, NT serves three main purposes. First, members of the district0x network can exchange NT for DT and thereby become members of an individual district; second, NT holders can signal through voting with their token holding what updates the district0x development team should work on; and third, NT is the central part of a coordination mechanism called a token-curated registry (TCR) that serves as a gatekeeper to the network (“District0x Educational Portal,” n.d.; Urgo et al., 2017).

The district curation through the district0x TCR comprises three steps. First, a district applies for membership in the network. Membership provides access to exclusive services and signals credibility to potential users. Together with the application, the system locks some amount of NT as a collateral to prevent spamming (Urgo et al., 2017).
Second, the application triggers a voting process. Each holder of NT can participate and review the application. If they consider the applicant not trustworthy, a NT holder can raise a challenge and has to match the applicant’s collateral with an equivalent deposit of NT. Now, NT holders can signal support for either applicant or challenger relative to their NT holdings. The rational is that NT holders want to include only high-quality applicants as they increase the attractiveness of the network. With a more attractive network, demand for its services increases and thereby demand for NT. As NT’s supply is fixed, more demand will drive up the price of NT increasing the value of NT holdings. Details of the voting process such as the minimum amount of collateral or the duration of the voting process are subject to decisions by the community of NT holders (Urgo et al., 2017).

Third and last, if NT holders consider the district not trustworthy, they reject it with a majority vote, and the system distributes the applicant’s collateral among NT holders who voted with the majority. Similar, if NT holders vote to accept the application, the system distributes the deposit of a challenger. Voters on both sides never have funds at stake only applicant and challenger. Successful applicants enter the registry and mint DT for their district through a deposit in NT (Urgo et al., 2017).

District0x employs with its TCR a mechanism that gained significant popularity in DLT governance and incentive designs. Several projects including MetaX AdChain\textsuperscript{17} and Messari\textsuperscript{18} apply a TCR for their curation. All systems are in a very early stage. Several challenges remain such as the balance between long- and short-term incentives to ensure sufficient user participation or the continuous adjustment of parameters as the network grows. Similarly, the use of non-native tokens such as ETH in the case of district0x’s PT is a question of efficiency (e.g. in the form of reuse and network effects) versus control. Designers of DLT incentive systems and their communities need to decide on the right balance for their purpose.

5.2.3 Bancor – Automated liquidity for cryptographic assets

Bancor is a new form of cryptographic token and a decentralized exchange for cryptographic assets. The so-called smart token is a cryptographic token that holds, like a basket of currencies, one or more other cryptographic tokens, so called connectors. This allows immediate exchange of the smart token for any of its connectors (automated liquidity). Tokens that comply with the Smart Token standard can connect to the Bancor Network Token (BNT) and utilize it as an exchange mechanism (Hertzog, Benartzi, & Benartzi, 2018). The Bancor Network uses the Ethereum blockchain as its DLT system and charges no fees except to cover the cost for transactions on Ethereum. The Bprotocol Foundation, responsible for the development and operation of Bancor collected approximately $US 152.3 million in funding through an ICO on June 12\textsuperscript{19}, 2017 (Zhelezov & Turner, 2018).

Bancor Network wants to be a decentralized exchange for smaller-volume cryptographic assets. In comparison to centralized profit-oriented exchanges, Bancor Network is cheaper

\textsuperscript{17} See: https://www.metax.io/.
\textsuperscript{18} See: https://messari.io.
and ensures continuous liquidity. This is attractive especially for smaller-volume cryptographic assets that do not have sufficient liquidity for trading on major exchanges. Smart token contracts function as a central bank for the token automatically adjusting its supply in response to market orders. As a result, there is no spread for any trade and no counterparty risk (Hertzog et al., 2018).

The Bancor Network consists of two types of token: BNT and Smart Token (ST). BNT is the native currency of the Bancor Network. BNT is one connector for all ST in the Bancor Network. It acts as an intermediary making all ST instantly interchangeable (Zhelezov & Turner, 2018).

<table>
<thead>
<tr>
<th>Token</th>
<th>Purpose</th>
<th>Gain</th>
<th>Lose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bancor Network Token (BNT)</td>
<td>Liquidity for all token on the network</td>
<td>- Buy with any token</td>
<td>- Sell for any token</td>
</tr>
<tr>
<td>Smart Token (ST)</td>
<td>Any</td>
<td>- Buy with any token</td>
<td>- Buy with any token</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Token-specific</td>
<td>- Token-specific</td>
</tr>
</tbody>
</table>

Table 13: Overview of Bancor token.

The second type of token, ST, is specific to another system or organization but uses Bancor Network as an exchange. ST is a basket of other cryptographic assets. The creator of an ST selects one or more cryptographic assets as connectors and sets the connector weight. The connector weight is the balance of token of the connector relative to the supply of ST. Thereby, the creator can define the price sensitivity of the asset, i.e. its reaction to changes in demand. Hertzog et al. (2018) distinguish the six ST types presented in Table 14. After setup, the ST contract maintains the connector weight through minting (increasing supply) or burning (reducing supply) smart token based on the Bancor formula (Hertzog et al., 2018).

<table>
<thead>
<tr>
<th>Smart Token</th>
<th>Number of connectors</th>
<th>Combined Connector weight</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Liquidity</td>
<td>1 ≤</td>
<td>20% &lt;</td>
<td>Token that holds balances of other token; supply increases or decreases with demand; Price increases with growing demand/supply</td>
</tr>
<tr>
<td>Proxy</td>
<td>1</td>
<td>100%</td>
<td>Due to only one connector and 100% connector weight, the token serves as a proxy for its connector</td>
</tr>
<tr>
<td>Relay</td>
<td>2</td>
<td>100% (50+50)</td>
<td>Smart token that holds BNT and another token. Conversion to BNT allows subsequently to exchange the token for every other token connected to BNT.</td>
</tr>
<tr>
<td>Array</td>
<td>&gt; 2</td>
<td>Any</td>
<td>Token is a basket of multiple Smart/ERC20 token</td>
</tr>
<tr>
<td>Bounty</td>
<td>0</td>
<td>Any</td>
<td>User can buy smart token but only exchange for its connectors from a certain time on</td>
</tr>
<tr>
<td>Network</td>
<td>Any</td>
<td>Any</td>
<td>Multiple Smart token have the network token as a connector whereby the network token forms a network between the different Smart token</td>
</tr>
</tbody>
</table>

Table 14: Overview of Smart Token configurations.
Decentralized exchanges such as KyberNetwork, 0x, or Bancor aim to maintain the trustlessness property and security model of DLT systems. Centralized exchanges signify a point of failure in the current ecosystem. The theft of cryptocurrencies through hacking amounts to $US 927 million in the first nine months of 2018, up by almost 250% compared with 2017 (Chavez-Dreyfuss, 2018). Addressing the security challenges from a technical and regulatory perspective is crucial for DLT to gain wider adoption. Development teams can favor the security of their users over reach by partnering only with credible exchanges.

5.2.4 Augur – Decentralized prediction market

Augur is a decentralized prediction market that uses the Ethereum blockchain. The idea of a prediction market is to forecast any real-world event through trading of shares in its possible outcomes. The prices of the different shares in one market reflect the chances of the respective outcome (Bonello & Turner, 2018a). The assumption is that only users with some special knowledge have an incentive to participate. Decentralization aims to diminish the need for trust in the accuracy of the reporting and reliability of payouts from a central organization (Peterson, Krug, Zoltu, Williams K., & Alexander, 2018). Augur raised around $US 5.3 million through an ICO between August 17th and Oct 1st, 2015 and further collects trading fees to maintain operations (Bonello & Turner, 2018a).

The Augur platform uses four tokens: the Reporting Token (REP), the Share Token (ST), the Participation Token (PT), and Cash which is Ether (ETH) (see Table 15) (Peterson et al., 2018). In the following analysis, I examine each of the four tokens and Augur’s prediction process.

The first token, REP, serves two main functions. First, it incentivizes accurate reporting from Reporters. Second, reporters use it to stake their vote in case of a dispute over the outcome of a market. The token is fungible, transferable, and capped (“Augur Documentation,” n.d.; Bonello & Turner, 2018a).

The second token, ST, represents a share of an outcome of a market. Traders buy shares to indicate the outcome they expect. ST can be traded at any time even after the market has settled. All individual ST for each possible outcome combined are called a complete set that is worth always one ETH. ST are fungible, transferable, and uncapped (“Augur Documentation,” n.d.; Peterson et al., 2018).

The third token, PT, demonstrates reporters’ participation during a defined time frame (currently 7 days). Reporters that are neither initial reporters nor disputers of an outcome can prove that they are active with PT. Holding PT entitles them to a fraction of fees collected during that time frame (“Augur Documentation,” n.d.; Peterson et al., 2018).
The fourth token, ETH, serves three purposes. First, traders sell and buy shares with ETH. Using ETH, provides higher liquidity for the market. Second, the market creation requires two collaterals in ETH that incentivize the creation of a valid market and the careful selection of an initial reporter to report the outcome. Third, Augur collects fees from traders in ETH and distributes these to reporters and market creators (“Augur Documentation,” n.d.; Peterson et al., 2018).

<table>
<thead>
<tr>
<th>Token</th>
<th>Purpose</th>
<th>Gain</th>
<th>Lose</th>
</tr>
</thead>
</table>
| Reputation (REP)    | Participation in Reporting     | - Initial Public Reporter reports in line with final outcome and receives the no-show-bond REP fraction that was staked for his report previously.  
- REP Token Holder stakes REP with one outcome in case of a fork within a given time frame (60 days) and receives 5% of his REP token holdings in REP.  
- REP holder stakes dispute that becomes the final outcome receives 15% stake of REP in return. | - Market creator loses No-show REP bond if her Designated Reporter does not report within 3 days after the market event occurred.  
- REP holder loses REP staked on dispute that becomes not the final outcome  
- Designated Reporter loses stake if her reported outcome is not the final outcome of the market. |
| Share token (ST)    | Trading of outcome of a market | - Buy for Ether                                                        | - Sell for Ether                                                       |
| Participation token (PT) | Represent active participation in reporting | - Any REP holder (=Reporter) can buy PT for REP.  
- Any REP holder staking an outcome challenging the tentative outcome (i.e., supporting a dispute bond) receives PT in return. | - Any holder of PT token can exchange them for REP at any time. |
| Ethereum (Cash)     | Collect and distribute fees    | - Market creator collects the Creator Fee (from the fee pool) at the end of a fee window (every 7 days)  
- Reporter collects Reporting Fee (from the fee pool) at the end of every fee window (7 days)  
- Initial Public reporter reports after Designated Reporter failed to report and receives ETH to cover gas costs once the outcome is final  
- PP Token holder exchanges PP tokens for REP and collects fraction of fees in ETH collected during Fee Window relative to his PP token holdings. | - Market creator loses No-show gas bond if her Designated Reporter does not report within 3 days after the market event occurred.  
- Market creator pays a small fee to Augur upon creation of the market. |

Table 15: Overview of Augur token.

The prediction process in Augur consists of four phases: creation, trading, reporting, and settlement (See Figure 7). For market creation, the market creator poses a question and chooses an end time for the market – for example, Will Donald Trump be impeached by December 25, 2018?19 Next, the market creator assigns a designated or initial reporter to report the outcome within three days after market end time; she sets a creator fee paid to her after settlement of the market, and posts two collaterals. The first is the so-called validity bond that is forfeited if the market is not valid, i.e. unambiguous or without objectively-determinable outcome. The second is the no-show bond that Augur refunds to the creator once the designated reporter has reported within the defined time frame. The no-show bond holds some amount of ETH and REP (“Augur Documentation,” n.d.; Peterson et al., 2018).

---

19 See: [https://dev.augur.net/#/markets?category=POLITICS](https://dev.augur.net/#/markets?category=POLITICS).
In the second phase, after successful market creation, traders buy and sell ST that represent the different possible outcomes of the market. One ST for each outcome combined make up a complete set. Augur maintains an order book for each market and matches orders to complete sets equivalent to 1 ETH. For each settlement with Augur, traders pay fees (“Augur Documentation,” n.d.; Peterson et al., 2018). The market end time can be any time in the future, so trading in most markets is the longest of the four phases.

The third phase, reporting, begins once the market event has happened. The designated reporter selected by the market creator needs to report within a defined time frame (currently three days). If she does not, the no-show bond is lost for the market creator and instead transferred to the first public reporter. After the designated reporter failed to report, any REP holder can report on an outcome. The first of these public reporters receives the ETH of the no-show bond to cover her transaction costs on Ethereum and the REP to stake her report on Augur. After any report, any reporter can challenge the previous report. If this dispute report receives enough backing from other reporters, it becomes the new tentative outcome. If not, enough reporters challenge the tentative outcome in a given time frame (currently 7 days), it becomes the final outcome. Successful disputers receive the REP staked by unsuccessful disputers. The system sets the threshold for a successful dispute in a way that every successful disputer receives 150% of her stake (“Augur Documentation,” n.d.; Peterson et al., 2018).

The fourth and final phase, settlement, starts once the outcome of the market is final. Traders settle their shares with Augur, and market creator and reporters collect their fees (“Augur Documentation,” n.d.; Peterson et al., 2018).

Figure 7: Simplified prediction process in Augur (own representation).
Prediction markets, like Augur, leverage the wisdom of the crowds, i.e. that estimates by independent individuals combined are more accurate than a single estimate. This notion is very popular in blockchain communities. The necessary conditions, however, such as the independence of individuals may be difficult to prevent herding; and in some situations, it may be not the wisdom of the crowd but someone in the crowd. Designers of DLT incentive systems and developers that use external data from a prediction markets need to examine if the notion holds in their context.

5.2.5 Oraclize – On-chain verification of data authenticity
Oraclize is an oracle service that allows on-chain verification of the data authenticity of off-chain data sources. The idea of an oracle service is to input data into a DLT system that would not be able to access external data without compromising its trustlessness otherwise. Oraclize does not have any native token but uses ETH to collect payments from its users ("Oraclize Wiki," n.d.).

The usage of an oracle comprises three steps: setup, fetching data, and verifying data. For the setup, the developer choses one or several data sources, and a type of proof. Data sources can be any web API endpoint. Proofs are mechanisms that use either hardware or software to let an auditor verify a claim made by an auditee. TLSNotary, one proof mechanism, uses the TLS protocol to establish an encrypted connection between auditor and auditee to let the auditor review the relevant data source without the auditee having to share her credentials. Oraclize stores the resulting proof with IPFS. IPFS is a distributed file system that is independent of any DLT system. This makes verification independent of any DLT system. Figure 8 illustrates the process of using an oracle.

Figure 8: Fetching and verifying data through Oraclize (own representation).
Any process build on top of a DLT system is only as useful as the input data. If DLT enables the decentralization of more sensitive processes in the public domain (e.g. voting) via the Internet, ensuring that data is untampered becomes even more important and challenging. Verifying the authenticity and origin of data is relevant beyond the DLT domain. In the near future, citizens’ identity will be to an even greater extent digital and online. Policy-makers need to ensure citizens can protect their online identities.

5.2.6 Sia – Peer-to-peer cloud storage

Sia is a peer-to-peer cloud storage platform. The idea is that every user can both provide and use storage of the network instead of only use storage provided by a central entity such as Dropbox. A blockchain system stores and enforces the storage contracts between hosts and clients. Most of the terms and conditions are not predefined but subject to continuous agreement between clients and hosts. Sia uses a fork of bitcoin and sustains its operation through a 3.9% fee on every contract (Peterson, Krug, Zoltu, Williams K., & Alexander, 2018).

The Sia system comprises two tokens: Siacoin and Siafunds (See Table 16). Siacoin serves two purposes. First, miners that append the blockchain receive a specified amount of Siacoin for each new block. This so-called block reward decreases over time down to the defined minimum of 30,000 Siacoin per block. Second, Siacoin provides a means of payment between clients and hosts. Clients pay hosts in Siacoin, and host use the token to put down collateral for every storage contract or they demonstrate trustworthiness through value-lock-ins. Siacoin is transferable, fungible, and its supply uncapped (Vorick & Champine, 2014).

The second token is the Siafund. The token’s purpose is to fund the operation of Sia. Holders of Siafund receive a share of the 3.9% of fees collected from every storage contract. The total supply of Siafunds is fixed at 10,000. 88% are still in possession of Nebulous Inc., the company behind Sia (“Sia Wiki,” n.d.). The fees collected are the main source of revenue for the Nebulous Inc. (van Eck & Turner, 2018). In the following analysis, I explain the process of storing files with Sia and the role of Siacoin in the context of storage contracts.

<table>
<thead>
<tr>
<th>Token</th>
<th>Purpose</th>
<th>Gain</th>
<th>Lose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siacoin</td>
<td>- Mining reward</td>
<td>- As Miner, for finding a valid block</td>
<td>- As User, for storing files with Sia upon receiving a proof-of-storage</td>
</tr>
<tr>
<td></td>
<td>- Fee payments</td>
<td>- As Siacoin holder, as return for investment (3.9% of every storage</td>
<td>- As User, for downloading a file</td>
</tr>
<tr>
<td></td>
<td></td>
<td>contract)</td>
<td>- As host, for missing storage proofs required by clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- As host, for providing storage-proof to contract</td>
<td>- As host, be locking coins to prove reliability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- As host through download fees</td>
<td></td>
</tr>
<tr>
<td>Siafunds</td>
<td>- Funding of Sia</td>
<td>- As investor, through purchase</td>
<td>- As investor, through selling</td>
</tr>
</tbody>
</table>

Table 16: Overview of Sia token.
Using storage through Sia consists of three phases: upload, storage and download (see Figure 9). For upload, a client selects a category of hosts with respect to her preferences. The price and the reliability of the hosts are the two most important criteria. The higher the reliability the higher the price. Reliability can come, for example, in the form of proofing storage of files on time or the availability of downloads (uptime). Clients can review the hosts storage history to determine their reliability. To prevent hosts from faking the history by storing files with themselves (spoofing), clients can require hosts to lock some amount of Siacoin with every contract. This decreases the chances of a host having a forged history (Vorick & Champine, 2014).

Once a user has determined the terms and conditions within the storage contract she signs it and sends it to the hosts. The hosts accept it, sign it and put down a collateral in Siacoin. The client, now, divides her file and encrypts each piece locally. The system distributes the pieces with a client-defined level of redundancy among the different hosts (erasure coding) (Vorick & Champine, 2014). The higher the level of redundancy the higher the availability of the file.

In the second phase, the storage phase, hosts store the files and provide regular proofs that they still hold the client’s file. In exchange for a valid proof, the client pays the hosts in Siacoin. If a host misses to send her proof, the storage contract transfers an amount of Siacoin as a penalty to the client as specified in the storage contract. On storage contracts with a longer duration, host may go offline. In this case, the Sia system moves the respective pieces of the file to a new host with the clients consent (“Sia Wiki,” n.d.; Vorick & Champine, 2014).

In the third phase, the download phase, the client wants to access her file. In accordance with the uptime specified in the contract, the user can offer an uptime premium to hosts in Siacoin. The different hosts that are part of the contract, now, compete to make the file available in order to collect the premium (Vorick & Champine, 2014).

Figure 9: Storing files with Sia (own representation).
Regarding the incentive design, the client and host in Sia can interact through determining the collateral of the storage contract, the penalty for missing a proof, the lock-in value, and the download premium. Vorick and Champine (2014) emphasize the role of market mechanisms to determine the right parameters in the form of prices, penalties and collaterals. Designers of DLT incentive systems need to distinguish where prior simulations can bring final results and where it can be left to the dynamics of the user community with the risk of insufficient room for intervention later on. Here the funding scheme becomes important, too. For a sustainable system, the community needs to make sure that valuable contributions pay off. Many existing DLT systems used ICOs to gain funding. This mechanism encourages speculation. Sia proposed a different concept with Siafunds. Sustainable DLT systems need to have a sustainable funding scheme.

5.4 Conclusion on analysis of DLT systems

Many aspects of the examined DLT systems are interesting for future incentive designs and worth discussing beyond the DLT domain. Four considerations are especially so. First, DLT systems are no walled gardens and their designers do not want them to. The strength of public blockchains such as Bitcoin or Ethereum is their openness that will facilitate more innovation than any of the private systems. The security model that supports this openness, however, does not cover external data sources or centralized exchanges. Developers, users, and regulators need to be aware of these points of failure and conceive original solutions that do not simply put back openness.

Second, DLT systems need to balance efficiency versus control. As the ecosystem matures, designs will stabilize, and dominant solutions emerge. These can be purely technical such as a programming language or conceptual like a TCR. Ethereum has attracted a major fraction of DLT development attention and investment. Developers need to consider the limitations to their design choices when reusing existing concepts and systems. They need to reject dominant solutions where control is vital for their user base and take the challenge of sustainable governance mechanisms seriously.

Third, DLT systems need to weigh market vs non-market mechanisms. The conception of a minimum viable incentive or governance design is difficult but necessary for the system to be able to adjust to changing environmental conditions and user requirements. Designers of DLT incentive systems need to think carefully where market mechanisms yield desirable outcomes and where they need to be restrained to ensure the viability of the system for all its users. Reputation systems are a first major extension of the DLT incentive schemes. Versatile DLT systems will work with a range of different incentives not just monetary rewards to engage their users.
Fourth, DLT systems need to ensure user participation. As discussed above, DLT systems require active user engagement to fulfill their promise of bringing about fairer and less-concentrated social and political institutions. For DLT system designers, it is important to consider who needs to participate when. In some contexts, an autocratic decision-making process by an expert may lead to a result acceptable for everybody, in other situations it may not. DLT gained attention with the promise of fast gains. For every DLT system, to be sustainable, the development team needs to balance short- and long-term incentivizes. This applies to the incentive design for users but should naturally include the funding of the development team and community of the system, too.
6 Conclusion on Finance 4.0

Finance 4.0 is a multi-dimensional incentive system. Its major purpose is to help individuals and communities around the world to improve their living conditions and support the accomplishment of the United Nations Sustainable Development Goals. We identified several difficulties related to the internalization of externalities, the most important being that major contributors to unsustainable economic and social developments are in many cases the major profiteers. The fundamental challenge is to incentivize these individuals and organizations to change their behavior.

As a team, we will explore different mechanisms to engage these individuals and organizations to consider new ways of production and consumption. We see great potential in communities as the unit of decision-making to address the issues of sustainable economic behavior. DLT tokens could provide more efficient coordination mechanisms compared with existing complementary currency schemes. Further, tokens allow communities to experiment with incentive and governance designs on an unprecedented scale while being transparent. Finance 4.0 strives to be the laboratory for these experiments. As an open platform, it will make the successful mechanisms available to potentially every individual and community around the world.
List of References


District0x Educational Portal. (n.d.). Retrieved October 15, 2018, from https://education.district0x.io/district0x-specific-topics/

International Journal of Community Currency Research, 16(special issue), 80–89. Retrieved from http://hdl.handle.net/1765/37269


