IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 24, 2021, accepted November 16, 2021, date of publication November 29, 2021,
date of current version December 14, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3131143

Improving IoT Federation Resiliency With Distributed Ledger Technology

TOMMI M. ELO[1], SAMPSA RUUTU[1], EKTOR ARZOGLOU[1], YKI KORTESNIEMI[1], DMITRIJ LAGUTIN[1], VERIA HOSEINI[1], AND GEORGE C. POLYZOS[2], (Member, IEEE)

[1]Department of Communications and Networking, School of Electrical Engineering, Aalto University, 00076 Aalto, Finland
[2]Mobile Multimedia Laboratory, Athens University of Economics and Business, 113 62 Athens, Greece

Corresponding author: Tommi M. Elo (tommi.elo@aalto.fi)

This work was supported by the Project Secure Open Federation for Internet Everywhere (SOFIE) funded by the EU's Horizon 2020 Programme under Grant 779984.

ABSTRACT Despite the rapid spread of Internet of Things (IoT) systems, the lack of interoperability between the systems significantly hinders their business and societal potential. Moreover, a major challenge for wider interoperability is that the IoT systems can be owned by multiple independent entities, whose collaboration will need to be organised to ensure their interoperability. One approach for achieving this is to establish federations supported by Distributed Ledger Technologies (DLTs), as this enables interoperability between entities and collaboration between business platforms, thereby overcoming many technical and administrative difficulties. DLTs can provide the required transparency and immutability for management of the federations, thus increasing trust and reducing the risk of misbehaviour that could destabilise the federation. This paper presents two system dynamics simulation models, which demonstrate that the success of a federation (with or without DLT support) is inversely related to the short-term selfishness of its members, and we then proceed to show that DLTs can improve the feedback received by the federation members on their actions by promoting a common consensus, which in turn can make the federation more resilient.

INDEX TERMS IoT federation, system dynamics, DLT, collaboration, cooperation, accidental adversaries, archetype, blockchain.

I. INTRODUCTION

For IoT systems and platforms, the lack of interoperability is a major issue hindering the Internet of Things (IoT) [1]. Currently, IoT platforms and systems constitute vertically oriented silos, which are unable and unwilling to exchange data with, or perform actions across, each other's domains. This leads to multiple problems, including reduced competition and vendor lock-ins due to the customers' difficulty in switching IoT providers, less privacy due to accumulation of customer data and metadata to multiple vendor-specific online data stores, and reduced functionality than could be achieved by increased interoperability. Finally, as IoT systems become increasingly prevalent, this lack of interoperability and limited access to relevant data will lead to an inefficiency problem on a societal scale [2]–[4]. This work is the first to utilise the System Dynamics methodology to study how DLTs affect the dynamics of collaboration, in particular the sustainability of collaboration amongst IoT platforms.

Since those IoT systems willing to collaborate are controlled by different entities, a further challenge is that in many cases, it will become necessary to jointly manage economic collaboration between these entities and the related risks, liabilities, and compensations. *Federations* could provide a suitable approach, as they allow useful economic collaboration without requiring complex changes from the member architectures [5]–[7]. The value proposition of IoT federations is straightforward: a single decision to participate in the federation would multiply the number of collaborating members and their devices, thus increasing the created value for all members. However, given all these apparent benefits, it is not clearly understood why such federations remain relatively rare.

One important factor is that federations run the risk of dissolving if they cannot effectively manage the risks of misuse and the resulting lack of trust between

The associate editor coordinating the review of this manuscript and approving it for publication was Shajulin Benedict.

their members. One approach for addressing this problem is to utilise Distributed Ledger Technologies (DLTs) as the backbone of the federation. DLTs provide transparency and immutability to the operations of the federation, thus enabling a common view of the business environment and incentivising the members to follow through with their commitments as any non-conformity would become apparent to all. In the IoT realm, projects such as the SOFIE Framework [1] provide the technical tools for building such a DLT-based federation, although questions about how much DLTs can help foster and increase the resiliency of the resulting federations have remained unexplored. DLTs are becoming common as the basis for connecting IoT infrastructure [8], [9]. Therefore, it is important to study the effect that DLTs actually have in such arrangements. Thus, the research question motivating our work in this paper is: How do DLTs affect federation resiliency?

This paper approaches these questions through system dynamics modelling by building on the *Accidental Adversaries* [10], [11] archetype, which considers the collaboration between two platforms. Utilising this archetype, we identify factors that influence the continuation or eventual discontinuation of collaboration between two or more platforms. By identifying DLT-related factors, we build a simulation model that represents the dynamics of this new type of federation. While our model is based on earlier work, an archetype model *Accidental Adversaries* originally developed by Kemeny [10], [11], the contribution of our approach lies in the simulation model. With the model, we study DLT effect factors that have previously been unexamined in the context of dynamics of collaboration, as well as connecting the terminology concepts of federation with both collaboration and interoperability.

Our simulation results show that when the federation is disrupted by a disturbance, sustainability of the collaboration is very sensitive to the harm inflicted on other members. This result holds even if only one member causes or experiences a disturbance to its success via actions, such as a governance error. DLTs can ensure that the federation will be more resistant to random errors of judgement through shared access to high integrity data on the actions and their verifiable consequences, which incentivises actions that minimise harm to other members.

The rest of this paper is organised as follows. Section II clarifies essential terminology and sets the context for the use of the term *federation* in IoT. It also describes the background of system dynamics methodology. Section III introduces the essential network effects in platforms and defines DLT supported federations. Section IV presents analysis and simulation results for a two platform federation. Section V details the simulation model and the resulting simulations for larger federations. Section VI presents and evaluates the results, and Section VII discusses the wider implications of this work. Finally, Section VIII concludes the paper, also proposing and briefly discussing future work in the area.

II. BACKGROUND

This section presents and ties together existing research relevant to our research question. Subsection II-A clarifies the terminology of collaboration by mapping the terminology from two fields of science, Systems Engineering and Collaboration Networks, and sets the context for the use of the term *federation*. Subsection II-B introduces background on IoT federations. Subsection II-C describes the system dynamics methodology.

A. ON INTEROPERABILITY, COOPERATION, COLLABORATION, AND FEDERATIONS

In everyday English, the terms cooperation and collaboration are typically used interchangeably as synonyms. Similarly, the term interoperability is commonly used to refer to technical devices operating with each other in a useful manner, e.g., the Internet is thus referred to as an interoperable network of networks [12]. However, in the field of Collaboration Networks, the terms cooperation and collaboration are part of a hierarchy of terms. By convention, the word *cooperation* is reserved for joint work in which the division of labour is statically determined and carried out to achieve compatible goals. In contrast, *collaboration* is reserved for the deepest forms of joint work, which includes not only cooperation, but also joint planning and agreement of joint goals [13], [14].

The field of Systems Engineering has a similar 7-step hierarchy of increasing depth for systems integration.[1] This hierarchy uses a scalar number to denote the levels of interoperability [15], with Level 0 corresponding to "No Interoperability", and Level 4 to "Pragmatic interoperability". Levels 4 and up describe integration of systems capable of simulation implementation. Therein, not only information, but also the context of information, is exchanged among the parties. This level of systems integration is capable of working with a common workflow [13]. The term cooperation corresponds to L3 and L4 interoperability (see Table. 1 for mapping between Systems Engineering terminology and Collaboration Networks terminology). With the increasing dynamic nature of the metadata used to carry the context of exchanged data and configuration of the integration, the upper layers of interoperability, L5 and L6, correspond best to the term collaboration.

Federations are defined to be an integration of autonomous and sovereign entities in a way that helps their cooperation or collaboration. The term "federation" is a rather vague and often redefined term from political science, where it is used primarily in the context of nation states forming federations. Considerable practical vagueness exists precisely about the depth of integration by federation members, and their relative sovereignty with reference to federal governance unit(s). Frequently, it is taken as self-evident that a federation must have a governing unit (see e.g., [16]) and that the setup of

[1] Integration is a noun meaning "the act ...of integrating". And to integrate means "to form, coordinate, or blend into a functioning or unified whole" and is synonymous to "unite". (Dictionary definitions Merriam-Webster)

TABLE 1. Relationship between collaboration and interoperability.

Systems Engineering interoperability level	Collaboration Networks integration level
L6, Conceptual	Collaboration
L5, Dynamic	
L4, Pragmatic	Cooperation, Coordinated networking
L3, Semantic	
L2, Syntactic	Networking
L1, Technical	
L0, None	

federation requires considerable human negotiation, taking much time and effort [17]. However, this situation is changing with DLTs.

In the IoT technology field, the formation of IoT federation requires at least semantic level interoperability (L3) [18]. Here, the federation refers to the voluntary collaborative efforts of sovereign member clouds of IoT devices (platforms), who may join the federation for joint division of labour purposes but also dynamically leave based on their self-interest. Therefore, an incentivisation mechanism, such as in Farris *et al.* [7], may be needed to make the collaboration resilient enough. For technological devices, being part of multiple federations or even short-lived ones is possible. It is noteworthy that our model is not restricted to any of the aforementioned levels of collaboration or interoperability but is instead quite applicable in all of the levels. For the purposes of this paper, we use both the terms collaboration and cooperation considering each occurrence separately. Where interchangeable, we use the term collaboration to emphasise the power of the archetype-based model being applicable at many levels of interoperability, up to and including Conceptual interoperability (L6).

The DLTs can help make the dynamics of collaboration more resilient because of their constitutional catallaxy nature: they allow for constitution-like rules to be decoded as immutable smart contracts of virtual organisations, thus offering a way to make such rules and their enforcement verifiable, and also immutable [19]. Verifiability is achieved with transparency. Transparency is achieved with availability and unforgeable histories of information. Availability is achieved with decentralisation of storage, and unforgeable history is achieved with a decentralisation of a consensus on write operations to the ledger and the policy of storing every change immutably. Finally, immutability is achieved with the cryptographic integrity guarantee of the storage, with the honest majority of the consensus upholding the immutability policies of the federation.

B. DLT BASED IoT PLATFORM FEDERATIONS

Due to diversity of IoT platforms and the related organisational relationships, federations of platforms have been suggested as a viable solution to optimise use of resources and gain economic potential [6]. However, interoperability alone does not solve the business problem of why platforms would enter and sustain such federal arrangements in the first place. The term *IoT federation*, we investigate more from here forward, indicates the sustainable interoperability and collaboration executed by autonomous self-sovereign members with minimal governance hierarchy using common and secure communication protocols. Farris *et al.* [7] further proposed a coalition formation game with incentives for rational self-interest maximising actors to form dynamic federations of IoT silos, which was shown to have more capacity compared to other forms of organising.

Creating IoT federations requires technologies that enable the communications and semantic interoperability between the systems. Also, introducing DLTs to the governance of the federation can provide both transparency and accountability to the members' actions in the federation. One such DLT-supporting solution is the SOFIE federation framework [1], which enables open and secure federation between existing IoT platforms without requiring internal changes to the platforms themselves. It builds on DLT and Decentralized Identities (DIDs) to enable the interoperability and protection of the privacy of the members, and can be leveraged for many different types of IoT federations. Thus, the federation approach can be based on distributed ledgers and interledger technologies, which enables the use of multiple distributed ledgers in parallel [20]. This in turn enables distributed business transactions between participants that may not trust each other, high level of automation, good security, privacy protection, and efficiency. A key benefit of the federation architecture is that it allows the creation of solutions that connect many individual systems to a whole that provides significant new functionality.

The federation approach can utilise DLTs to supporting transparency, reducing costs and delays by automating actions with smart contracts and other related technologies, and opening the platform to all parties, while enabling accountability and even collective countermeasures against misbehaving members. In a more traditional governance system, a trusted third party is needed to manually resolve conflicts between the parties, which is a time consuming and costly process. Since DLTs offer transparency and automation through smart contracts, conflict resolution can be done with significantly lower costs and delays. As an example, the effects of DLTs on reducing costs in the supply chains have been analysed in [21]. Also as an example, it has recently been suggested [22], [23] that blockchain governance and financial transactions could be combined with serverless technologies to better utilise distributed and underutilised private and public computing resources to fulfill societal goals. Opening a platform to all parties in an automated way can be achieved through, e.g., "running" the federation with smart contracts in public, permissionless blockchains, in a way that any other entity can interact with the platform and its parties without requiring any initial permission or other registration before doing so.

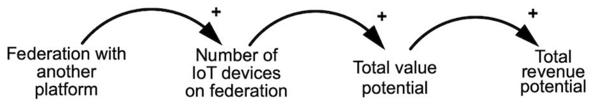

Federation with another platform
+
Number of IoT devices on federation
+
Total value potential
+
Total revenue potential

FIGURE 1. Motivation for the single business platform to form, or participate in, a federation: by increasing the number of devices connected to the platform the potential value is also increased.

The value created by the decision to federate is lucrative because participating in the federation multiplies the network effects for all the parties involved and for the federation as a whole as depicted in Fig. 1, which indicates that the value potential of a network grows as the number of nodes increases [24]. The network effect benefits for value creation are present in many forms of collaboration and are not federation specific. On the flip side, federations appear to face multiple practical problems: having a central governing party may facilitate the operations of the federation, but it also empowers the governing party, and if the goals and motives of the central party significantly differ from the federation members', it may result in the governing party exploiting its position. These abuses may include delays and costs for parties joining or members transacting, insufficient transparency to the operations of the platform, and limits to the access of the platform for existing and new members.

A key element for the success of any federation is to motivate the members to take *mutually beneficial* actions; the actions can be more beneficial for the acting party than other members of the federation, but the disparity of the benefits to the active party and the lack of benefits or even actual harm to the other members cannot be too big - otherwise the members may quickly conclude that too many *selfish* actions make remaining in the federation an unprofitable proposition. Here, the selfish actions include intentionally selfish and short-sighted actions without concern for the long-term benefit to the acting party or even the viability of the federation, but also acts, where the active party is simply unaware of the harm it's causing. Both of these problems can be addressed with better accountability for the actions and better visibility to the proportionality of the harms caused.

Augmenting the governance scheme of the federation with Distributed Ledger Technology helps provide the necessary transparency and immutability to the governance action of all parties. Thus, any direct harm to other parties resulting from selfish action[2] is immutably attributable to the active member by the data on the DLT. Also, the proportionality of mutual harm can be better and sometimes even automatically evaluated. Together, these properties encourage participants to take a longer-term view and avoid activity that disproportionally harms others.

Even more interestingly, DLTs allow federation to have a shared immutable audit trail of the mutually beneficial actions of the parties towards each other. This way the benefit to other members ceases to be an abstract unquantifiable notion which can always be claimed without proper merit. Instead, the measurement of merit of such essential action can, and should, be woven as an explicit documented part of the (business) dynamics of the federation via the DLT, which creates an immutable history with non-repudiable shared facts transparently available to all the parties. The end-result can approach the game theoretic ideal assumption of common knowledge [25]. This is a pre-requisite in many game theoretical analyses, but it was not practically available before Nakamoto consensus based first DLT, i.e., blockchains [26]. To the extent, DLTs [27] are utilised within the current traditional framework of hierarchical institutions, and not blockchains, most or all of these properties resulting from the institutional assemblage nature of the DLT arrangement could be lost due to the weaker, more centralised, consensus formation.

C. SYSTEM DYNAMICS METHODOLOGY

System dynamics is a methodology that uses feedback loops, accumulations, and time delays to understand the *behaviour of complex systems over time* [28], [29]. One of the primary strengths of system dynamics is allowing for the inclusion of both social and technical elements into the same simulation model [30]–[32]. This allows the modelling and simulation of complex adaptive socio-technical systems, such as business models, platforms, and currencies [4]. As essentially reliable accounting technologies, DLTs are such socio-technical systems, and thus particularly suitable to be studied with system dynamics.

For the purposes of this paper, a *system* is defined as a set of interrelated elements such that a change in any one of the elements affects the whole [33]. When we observe the world from the systems point of view, we acknowledge the fact that the interaction between the elements must be taken into account rather than just the elements themselves in isolation. For federations, this implies that the essence of their resiliency, or lack of it, is to be found *in the interactions between members* rather than members themselves.

System dynamics models can be visualised as either *causal loop diagrams (CLDs)* or *stock and flow diagrams (SFDs)*. CLDs (e.g., Fig. 2) are high level models, which consist of variables (elements) represented as named nodes and causal links represented as arrows. SFDs are extended cases of CLDs: models that can be represented as SFDs also have memory and flows, enabling simulation (of behaviour over time). *Stocks*, also called levels, can be seen as containers with volume, and they represent accumulations of either matter or information (memory). *Flows* represent time dependent changes of stocks as either inflows or outflows to a stock. Flows can be seen as pipes which have valves representing the volume of stock passing through the pipes per each time unit.

The causal links (arrows) in the CLDs and SFDs, can also form dynamic feedbacks i.e., *causal loops*, which reflect the *endogenous focus* of the system dynamics methodology.

[2] *Selfish action* is an action benefiting the action taking entity itself and disregarding negative consequences to other(s). *Unselfish action* is action benefiting also or even exclusively some other entity.

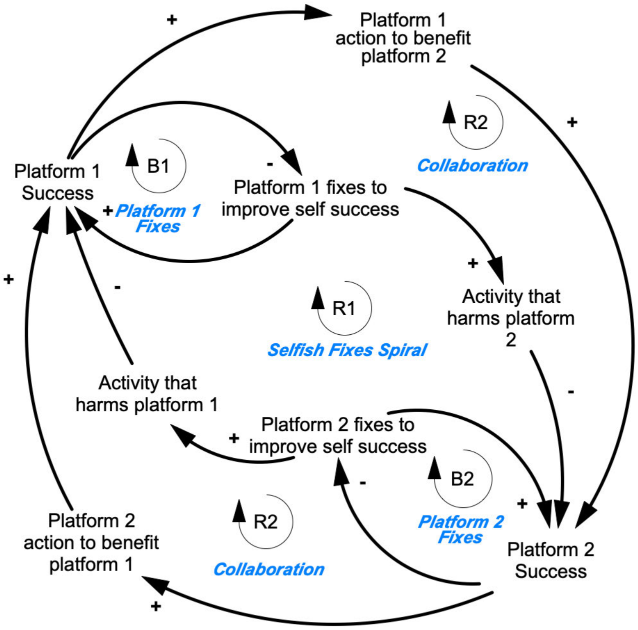


FIGURE 2. Accidental adversaries archetype CLD.

With causal loops, the model of a system becomes powerful enough to be able to capture and explain behaviour over time as an *emergent property of the system structure* and not only as a consequence of exogenous forces that cannot be further analysed meaningfully.

Causal links can be either positive or negative, corresponding to whether the connected variables change in the same direction (+) or to the opposite direction (−). See Fig. 2 for an example of a CLD with positive and negative causalities. Additionally, the same figure has an example on loop naming: the displayed reinforcing (R) and balancing (B) feedback loops in the diagram are named with a letter and number, and denoted with a loop symbol placed in the middle of the loop (R1, R2, B1, B2). Reinforcing loops are positive feedbacks which can potentially grow to infinity (positive or negative!), while balancing loops are negative feedbacks which display a goal seeking behaviour.

In complex systems, the concept of stability, resiliency, and collapse are related to the concept of *tipping points* [34]. While a minor disturbance may not necessarily cause a system to collapse, but after a certain point some reinforcing feedback loops may become dominant and create a vicious cycle that is difficult to escape from. The definition of a *tipping point* is a point in time, where the loop dominance changes. Any dominating reinforcing loop taking the system towards negative infinity and reaching zero from above, would cause a *collapse* of success in our case. The system is in *equilibrium* if all the inflows and outflows are the same. For our purposes, the system is called *resilient*, or has *stability*, if it easily doesn't enter a loop dominance which causes collapse, i.e., where one or all of the federation members would reach zero, but instead the collaboration can continue. A closely related term is *anti-fragility* [35]. See [36] for an accessible discussion on anti-fragility of systems.

System dynamics modelling has been used to explore such situations across a variety of contexts, such as construction projects [37], [38], product development [39], [40] and safety critical organizations [41]. Across different contexts, a common theme that emerges from these studies is the trade-offs between short term targets, such as financial or schedule pressure, and investing in longer term capabilities. Because of feedback loops and delays, it is difficult to learn about the best course of action [42], and modelling tools such as system dynamics simulation are useful in exploring the unintended consequences of actions. System dynamics is also a useful methodology for examining the processes of value creation between different organizations, in contexts such as project alliances [43] and digital platforms [24].

III. DYNAMICS OF COLLABORATION IN PLATFORMS

Economic and technical collaboration, in addition to, or instead of, competition, is paramount for efficient use of limited resources, and is therefore an important subject of study. Successful collaboration between business platforms can positively reinforce the network effects with two different mechanisms: the same-side and cross-side network effects of the platforms [44], [45]. *Same-side network effects* make the platform more valuable to potential users via the volume of other users who already adopted. A good example is a phone which has more utility when many (or all) individuals are reachable via it, but not as much utility if only a few people have a phone. Conversely, *cross-side network effects* make the phone more valuable to potential users by increasing adoption on some other market side. As an example, an increased number of psychologists offering counselling service via phone makes having the phone more valuable—and an increasing number of phones also makes such mentoring services more valuable. Therefore, by joining their networks and enabling new network effects, federation can rapidly make member platforms more valuable for both producers and consumers.

Manufacturers' IoT silos can be considered as business platforms. For example, a manufacturer of thermometers may connect sold units to its own business ecosystem via Internet for maintenance and guarantee purposes. But such data would also, with consumer consent, be valuable for a remote health care provider, thus motivating a collaboration between the thermometer manufacturer and the remote health care provider, who in turn may have its own IoT sensors, such as connected scales, already deployed.

Federations supported by DLTs, in the context of this paper, are seen as constitutional catallaxies [19] and institutional assemblages [46] i.e., platforms of platforms, which try to collaboratively aim for the collective good of their constituent members. Catallaxies are a hybrid of economies and governance, and institutional assemblages are collections of institutions. Federations hold independent resources and decision-making power, largely, but not completely,

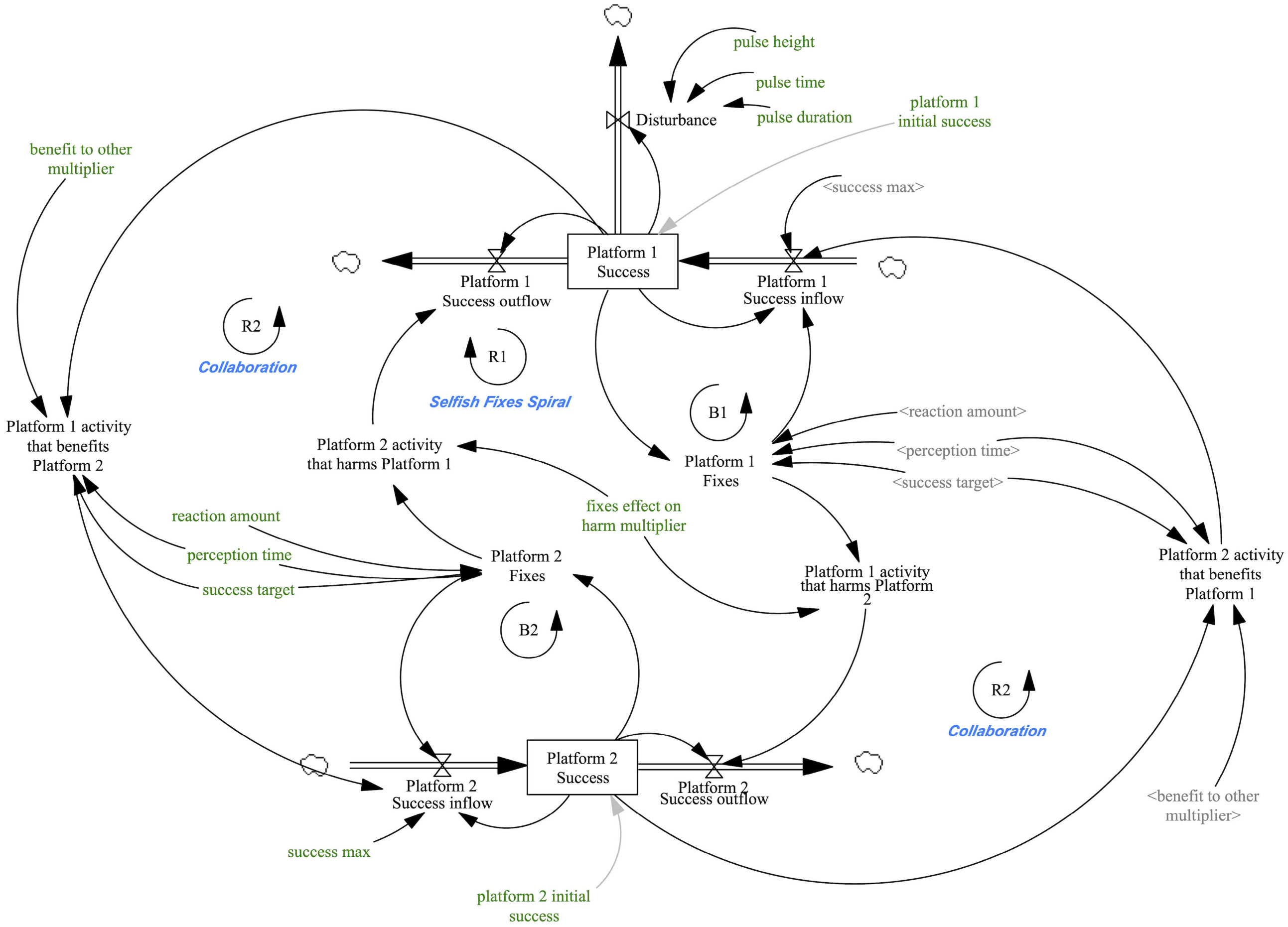


FIGURE 3. **Stock and flow diagram of the simulation model of accidental adversaries with 2 member platforms.**

independent of their members. This is the case for any judicial person with a distinct system or unit of governance.

IV. DYNAMICS OF COLLABORATION BETWEEN TWO PLATFORMS IN A FEDERATION

This section applies the Accidental Adversaries archetype of two members by developing it to a stock and flow simulation model.[3] We compare a typical analytical approach and a simulation model and present results.

A. ACCIDENTAL ADVERSARIES CLD AND SF MODEL FOR TWO PLATFORMS

The *Accidental Adversaries* archetype CLD in Fig. 2 explains the basic dynamics between two cooperating parties. It has self-benefiting loops for Platforms 1 (*B1: Platform 1 Fixes*) and 2 (*B2: Platform 2 Fixes*) as both platforms can act to accumulate more success for themselves via taking action (fixes). However, this activity can also produce collateral damage via the mutual punishing or not-caring loop *R1: Selfish Fixes Spiral*. Considering these side effects is vitally important for stability and resiliency, if Platform 1 and Platform 2 need each other, e.g., are part of the same collaboration, in our case a federation.,[4] otherwise they may bring down even all the other federation members. Finally, *R2: Collaboration* is the outer clockwise cycle, where the actors can benefit the other party and counter the mutually destructive dynamic of R1. Thus, both Platforms 1 and 2 may also engage in direct unselfish action toward the other. This outer circle loop is always available to balance both parties regardless of the errors or omissions made with collateral damage in loop R1.

The Fig.3 introduces a stock and flow simulation model for two parties which is developed from the archetypal CLD above. The model corresponding to this figure is one of two simulation models used in this paper.

B. MODEL EQUATIONS FOR TWO PLATFORMS

This section presents the equations for the stability of the two member federation in Fig. 3. The analysis is based on exploring the stability with differential equations and solving them analytically.

[3] https://doi.org/10.21227/wphp-gb20

[4] Considering effects on the other party more carefully can reduce the dominance of Selfish Fixes Spiral, R1.

The rate of change of level of Success S_1 and S_2, for the federation member Platform 1 and Platform 2, is given by the equations

$$\frac{d}{dt}S_1(t) = F_1(t) + S_2^p(t) \cdot b - F_2(t) \cdot h$$
$$\frac{d}{dt}S_2(t) = F_2(t) + S_1^p(t) \cdot b - F_1(t) \cdot h \tag{1}$$

where $S_1^p(t)$ is the perceived level of success, calculated from the level of success using exponential smoothing, and $F_1(t)$ and $F_2(t)$ are the amount of fixes engaged in by platform 1 and 2 respectively. The term h corresponds to fixes effect on harm multiplier, The term b corresponds to benefit to other multiplier, and the term r corresponds to reaction amount.

In the analysis of next section, values of S_1 and S_2 (corresponding to the Success stock in the simulation model in Fig. 3) are constrained between 0 and 1. The analysis is obtained by marking a governance error at the start of the analysis of platforms $1 - s_1$ and $1 - s_2$, respectively. Thus Success stocks have value s_1 and s_2. Governance error can be anything that induces a temporary downtrend to the S of a platform. Examples of such errors include a logical error in the governing smart contract of the platform, financial theft, or reputation destroying action, such as lying to the public about the level of privacy offered, which all may cause a sudden sharp drop of S.

C. EQUILIBRIUM ANALYSIS FOR TWO PLATFORMS

By making simplifying assumptions of the model we can proceed to determine the equilibrium points analytically.

By constraining Success to a maximum of 1, and each platform aiming to reach S of 1, fixes can be calculated using the formula

$$F_1(t) = max(0, (1 - S_1^p(t) \cdot r)$$
$$F_2(t) = max(0, (1 - S_2^p(t) \cdot r) \tag{2}$$

Assuming no perceptual delays we can substitute $S_1^p = S_1$ and $S_2^p = S_2$. Declaring $S_1(0) = s_1, S_2(0) = s_2$. We search for the equilibrium points

$$\frac{d}{dt}S_1(t) = \frac{d}{dt}S_2(t) = 0 \tag{3}$$
$$\frac{d}{dt}S_1(t) = (1 - s_1) \cdot r + s_2 \cdot b - (1 - s_2) \cdot r \cdot h = 0 \tag{4}$$

Solving for h

$$h = \frac{1 - s_1}{1 - s_2} + \frac{s_2}{1 - s_1} \cdot \frac{b}{r} \tag{5}$$

The same is correspondingly true of S_2, while h is the same for both S_1 and S_2. We search for the equilibrium condition

$$\frac{(1 - s_1) \cdot r + s_2 \cdot b}{(1 - s_2) \cdot r} \cdot r = \frac{(1 - s_2) \cdot r + s_1 \cdot b}{(1 - s_1) \cdot r} \tag{6}$$

with some basic arithmetic manipulations we get to

$$s_2 = s_1 \tag{7}$$

TABLE 2. **Parameter values for the base case run of Fig. 4 of the model in Fig. 3.**

node name in simulations in analytical equations	value in simulation	corresponding notation
fixes effect on harm multiplier	1	h
benefit to other multiplier	3	b
reaction amount	2	r
perception time	2	N/A
success target	100	1
initial success 1	50	S_1
initial success 2	50	S_2
pulse height	40	$1 - s$
pulse time	5	0
pulse duration	5	one time at start

If we set $r = 1, b = 1$, we get $h = (s_1/1 - s_1) + 1$ when substituting $s_2 = s_1$. When $s_2 = s_1 = 0.5$, we get $h = 2$. The system is in equilibrium with these values.

D. SIMULATION SETUP FOR TWO PLATFORMS

In the two platforms simulation, we varied the fixes effect on harm multiplier, while keeping every other parameter fixed. The parameter values for the base case run can be found in Table 2, and the corresponding simulation model in Fig. 3. It is noteworthy that in the simulation model we are not restricted to having Success between 0 and 1, as was the case with the previous analytical approach. We can also apply the disturbance at any point in time, and to just one member.

We apply an external disturbance outflow to S_1, additionally draining it between t_1 and t_2 by 40 units, and see how it affects the federation consisting of S_1 and S_2. This outflow is the topmost outflow of Fig. 3. We observe the variation of the outcomes of S_1 and S_2 with different values of the fixes effect on harm multiplier. Thus, we now know that with the aforementioned parameters the most stable value for $h = 2$. While this result is robust, it is not very significant in practice, as we rarely have the luxury of being able to run complex practical systems close to their optimal points. We proceed to run simulations by standardising other constants and studying the sensitivity of the fixes effect of harm multiplier close to the model tipping point.

E. SIMULATION RESULTS FOR TWO PLATFORMS

This section presents the simulation results for two platforms. Fig. 4 shows the different simulation results with regards to parameter h, corresponding to *fixes effect on harm multiplier*. The leftmost figure shows a simulation result with a high h. We can see that in this case both platforms take a mutual dive towards zero, very soon after a disturbance between t_1 and t_2 is applied. In the middle figure with moderate fixes effect on harm multiplier, the mutual collapse happens much later. In the rightmost figure with low fixes effect on harm multiplier the two platforms are able to recover from the external shock permanently.

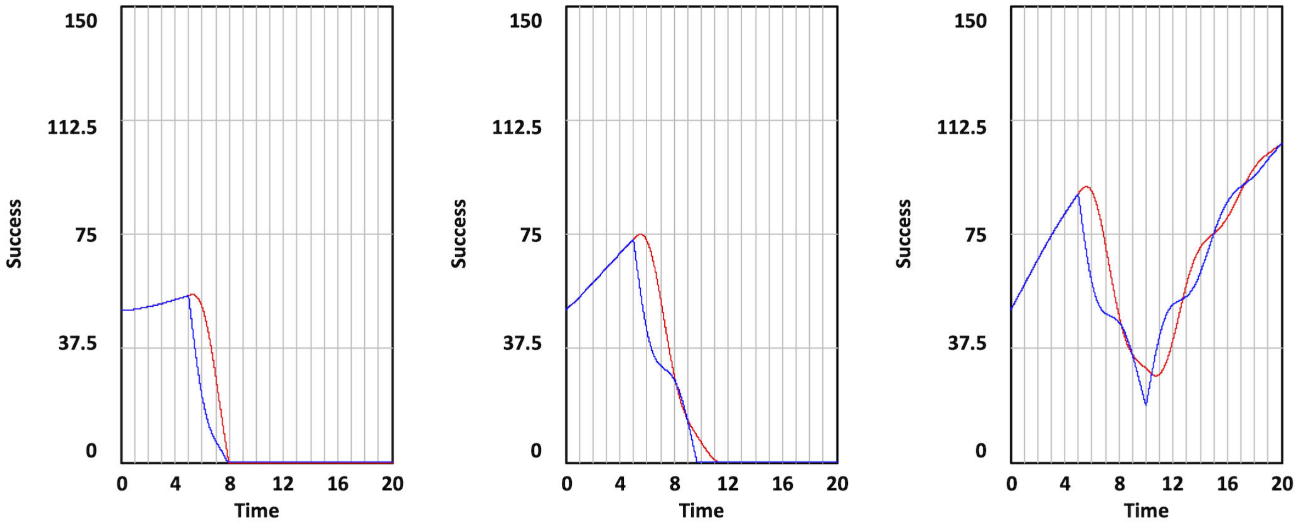


FIGURE 4. Simulation results show the effect of the external governance shock which begins at $t_1 = 5$ and ends as $t_2 = 10$ to a federation of two members with high, moderate and low values of h, *fixes effect on harm multiplier*. Leftmost figure is a base case described in Table 2. Middle figure is $h = 0.96$. Rightmost figure is $h = 0.92$. The values chosen here are less than the equilibrium value, since we use an external disturbance and thus need a small h to sustain the federation.

Thus, the simulation results in Fig. 4 show that with a strong enough DLT effects collaboration can continue even in the presence of governance errors, which are modelled as an exogenous shock. If the effect of the DLT is too small there is no difference to the survival of the federation.

V. DYNAMICS OF COLLABORATION FOR LARGER FEDERATIONS

This section expands the analysis to a federation of $n + 1$ parties and presents equations for the stability of the federation. The analysis is performed by exploring the stability via partial differential equations and solving them analytically. Values of S (corresponding to *Success* stock in the simulation model in Fig. 5) are constrained between 0 and 1. The analysis is obtained by assuming a governance error causes *all the platforms to receive the same* disturbance $1 - s$ similarly as in the two platforms case in Section IV.

A. MODEL EQUATIONS FOR LARGER FEDERATIONS

The rate of change of level of success S_i for each federation member platform i is calculated using the equation

$$\frac{d}{dt}S_i(t) = F_i(t) + \sum_{j\neq i}[S_j^p(t)\cdot b - F_j(t)\cdot h] \tag{8}$$

where $S_i^p(t)$ is the perceived level of success, calculated from the level of success using exponential smoothing.

B. EQUILIBRIUM ANALYSIS FOR LARGER FEDERATIONS

By generalising the same simplifying assumptions from above, we can proceed analytically. $F_i(t)$ is the amount of fixes, calculated using the formula

$$F_i(t) = max(0, (1 - S_i^p(t))\cdot r) \tag{9}$$

Parameters h and b influence the effect of fixes on harms and the effect of success to the benefit of others, respectively, and the amount of fixes cannot be negative.

If the initial success of each firm is set equal, i.e., $S_i(0) = s, \forall i \in A$, where $A = \{1, 2, \ldots, n, n+1\}$ is the set of business platforms in the federation, and the amount of fixes is below the maximum value of 1, the equation above can be written as

$$\frac{d}{dt}S_i(t) = (1 - s)\cdot r + s\cdot n\cdot b - (1 - s)\cdot n\cdot h\cdot r \tag{10}$$

Note that n is the number of other platforms besides the focal platform, so the total number of platforms in the federation is $n + 1$.

Calculating the equilibrium condition $(d/dt)S_i(t) = 0$ with respect to h, we obtain

$$h = \frac{1}{n} + \frac{s}{1-s}\cdot\frac{b}{r} \tag{11}$$

From Equation 11 it follows that the equilibrium value of h decreases with an increase in the size of the federation. A larger federation is also more sensitive to changes in the values of parameter h. We observe this from Equation 12 showing the partial derivative with respect to h.

$$\frac{\partial}{\partial h}(\frac{d}{dt}S_i(t)) = -(1 - s)\cdot n\cdot r \tag{12}$$

The federation stability increases with the size of the federation when $(h\cdot r/b) < (s/1 - s)$. This condition follows from the partial derivative with respect to n (Equation 13). Intuitively, this result is appealing because it means that the ratio of harms and benefits to others needs to be smaller than ratio of success and disturbance. Only then will adding more members to the federation help to stabilise it. It is noteworthy

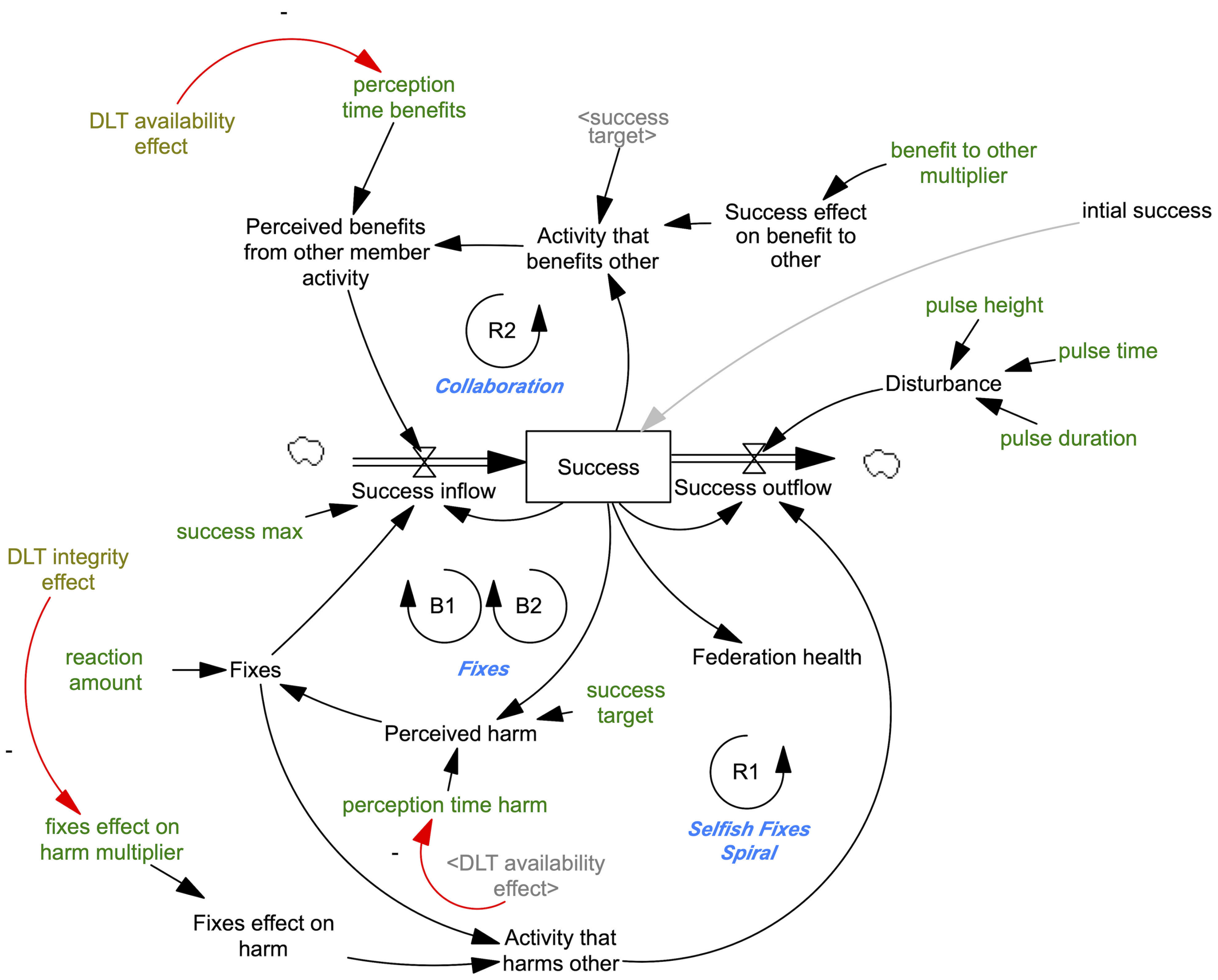


FIGURE 5. Stock and flow diagram of the simulation model of accidental adversaries for n entities augmented with ***DLT effects*** split into two components: ***DLT availability*** effect and ***DLT integrity effect***. For visual clarity, loop naming here shows where the loops of the two platforms model (Fig. 3) would appear in this generalised model. On the right also an external governance error source (Disturbance) is added. The stock ***Success*** in the model measures the financial and other resources of the participating entities.

that this result is for a collective disturbance, i.e., when all members receive the same external disturbance.

$$\frac{\partial}{\partial n}(\frac{d}{dt}S_i(t)) = s \cdot b - (1-s) \cdot h \cdot r \tag{13}$$

These results are already practically more important than the first analytical results in Section IV. However, the analysis is still limited to the same shock for all members, and with limited applicability for the time of the shock.

C. SIMULATION MODEL DEVELOPMENT FOR LARGER FEDERATIONS

In this section, we apply the archetype described in Section IV by developing it into a stock and flow simulation model,[5] adding the DLT effects, and generalising the model to $n+1$ platforms. Simulation model, unlike the analytical approach used in the previous section, allows us to work with behaviour over time aspects or values at any chosen time i.e., allows each member platform to have unique attributes. Here, specifically, it allows investigation of the more realistic case where *only one of the several member platforms is subject to a governance error*. This can happen more easily than the whole federation experiencing the same disturbance, since there are many members within one federation.

Fig. 5 describes a simulation model of two, or more, members together forming a federation. Here we describe the model of $n+1$ platforms with the help of the model of 2 platforms. In the two platforms case (Fig. 3), all members use their accumulated *Success* to benefit themselves in feedback-loops denoted B1 and B2 (See corresponding loops appear in Fig. 5). In this loop, they perceive harm if they are not at their target value for Success, denoted by constant *success target*. This causes them to *perceive harm*

[5] https://doi.org/10.21227/wphp-gb20

TABLE 3. Simulation parameters for the sensitivity analysis of Fig. 8.

Parameter	Value	Note
fixes effect on harm multiplier	0.20 to 0.26	Random uniform distribution with 500 runs
Success	100,50,50,5,5	Initialised as a vector: 5 entities

of the aforementioned difference with some time delay, *perception time of perceived harm*. They then start fixing this difference in *Fixes* loop by *reaction amount* for each time unit. These actions cause them to increase the *Success inflow* to compensate their lack, and close the B1 and B2 loops. In the generalised model of Fig. 5, there are $n + 1$ number of primary B loops because each platform i has its own self benefiting loop.

Fixes also have side effects which are described by the loop R1: Selfish Fixes Spiral. This loop starts from the action of the party to benefit itself (e.g. Platform 1, in the 2 platforms case). Via *Perceived harm* and Fixes auxiliaries *Activity that harms other* increases with some multiplier *fixes effect on harm multiplier*. This causes the *Success outflow* of the Platform 2 (in the two platforms case) to increase, decreasing Success, and closing R1. In the generalised model of Fig. 5 there is $\binom{n+1}{2}$ number of these primary R loops, where $n+1$ is the number of the member platforms because each Platform i forms this interaction loop with every other platform.

Both parties can also engage in *activity that benefits other*, loop R2: Collaboration. In the two platforms case, Platform 1 causes *Perceived benefits from other member activity* of Platform 2 to increase with delay *perception time of benefit*, which increases Success inflow of the Platform 2 (still the two platforms case), and closes the reinforcing loop. In the generalised model of Fig. 5, there is $\binom{n+1}{2}$ number of these primary R loops, where $n + 1$ is the number of the member platforms because each Platform i forms this interaction loop with every other platform.

D. SIMULATION SETUP FOR LARGER FEDERATIONS

Here we proceed similarly as in the two platforms federation case. First, we run a sensitivity analysis of a five member federation w.r.t fixes effect on harm multiplier when only a one member is disturbed. The fixes effect on harm multiplier near the tipping point is found in Table 3. The values are lower than in smaller federations.

Then we compare 3 and 10 member federation outcome sensitivity near their tipping points to the fixes effect on harm multiplier variations. Table 4 shows the values for both federations near their tipping points.

E. MODEL RESULTS FOR LARGER FEDERATIONS

Fig. 6 and Fig. 7 show the simulation results with federations of 3 and 10 member IoT platforms, respectively. Here, every member in them has an *initial success* of 50 units. *Federation health*, the combined Success of all members, is therefore initially 150 and 500, respectively.

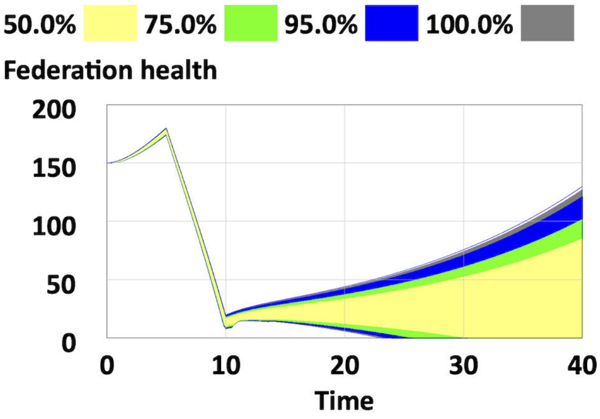


FIGURE 6. The spread of the possible values of *Federation health* is much less with 3 platforms than with 10 platforms in Fig. 7.

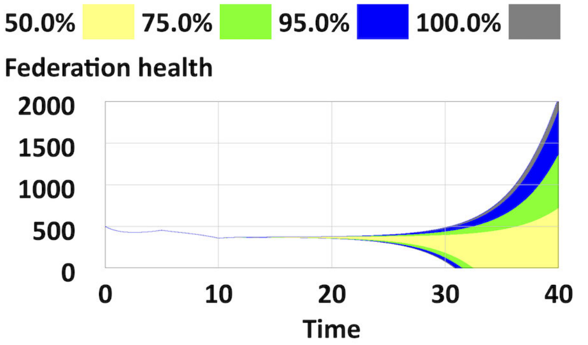


FIGURE 7. The spread of the possible values of *Federation health* is much larger with 10 member platforms than with 3 member platforms in Fig. 6.

TABLE 4. *Fixes effect on harm multiplier* upper and lower limit values in 10- and 3-member sized federations.

	3-member sized federation	10-member sized federation
lower value	0.500	0.119935
upper value	0.502	0.119939

The simulations show that a federation of 10 members has much more combined Success, i.e., static resiliency via Federation health, which allows it to recover from larger point disturbances than the federation of 3 members. In the simulation we disturb, in both federations, one member with an external static pulse *Disturbance* of magnitude 40, beginning at time unit 5 and lasting until time unit 10. This emulates a single static governance error e.g., a programming or execution error in the smart contract on the DLT.

We vary the parameter fixes effect on harm multiplier by feeding it values from a random uniform distribution as given in Table 4.

A key finding is that the outcome spread of the resulting simulation runs is wider in the *larger* federation despite the disturbance being the same in absolute terms (and thus same for the affected member but smaller compared to the federation health), and the multiplier variation far *less* in the larger federation. So, we can conclude that the larger federation is dynamically more sensitive to the external shock when fixes effect on harm multiplier is near the model tipping point. This is an interesting result because the larger federation is statically more resilient, and the same shock on it is thus relatively smaller than to the smaller federation. Still the resulting spread of the *Federation health* is larger after time unit 35. This shows that the *Fixes effect of harm multiplier* becomes increasingly important to the resiliency of the larger federation. And this parameter can be affected with DLTs.

F. ADDING A DLT TO THE FEDERATION

DLTs are an integrity and availability mechanism to quickly communicate and uphold joint views of reality in a common-knowledge fashion. DLTs are quick because they are computerised. They are an availability mechanism because the database is common and open to all (members). They are an integrity mechanism because the integrity of the database contents is guaranteed by the distributed consensus and cryptography. And they uphold common views of reality via the aforementioned integrity and availability. Finally, this all is common-knowledge like. Even though our model assumes perfectly rational actors, the DLTs can still affect the perception times of actions and incentivise less collateral harms. Indeed, especially in times of heated tensions perception times (of harms and benefits) and side effects of actions can greatly affect the outcomes of federation-like co-operations and collaborations.

Time delays in system dynamics in general, are key to understanding systems behaviour, and in the above case in particular, can be sufficient to cause the balance of the archetype to shift so that the war dynamic (Escalation) becomes dominant. While governance errors are only random fluctuations for fully rational actors, in the true human run organisations they are, of course, very common, so in our model we have a source increasing the harms for some period, i.e., the Disturbance auxiliary. By utilising it as a source of governance errors, we can investigate qualitative effects for a common knowledge like technology such as DLT.

The effect of the DLT consists of several components, which affect the trust and reliability of the information inside the federation. The components have been listed in Table 5. *DLT integrity effect* reduces the side effects of everyone's Fixes by guaranteeing non-counterfeit data of effects of Fixes on others. Its effect to the Success is mediated by the fixes effect on harm multiplier. *DLT availability effect* reduces the amount of time it takes for members to detect the effects of actions of others on them. Our simulations do not include any claim of the numerical strengths of the DLT effects, only about their qualitative direction.

VI. ANALYSIS OF SIMULATION RESULTS

The Accidental Adversaries archetype easily regresses into a (War of) Escalation archetype dynamic exactly because the reinforcing rational[6] feedback loops of promoting self-interest are dominating. The unselfish, vital trust inducing [47] outer loops of benefiting the other party voluntarily offer a balancing documentable dynamic, which makes the federation more resilient as more history has gathered (trust has a strong time dimension).

TABLE 5. Components of the DLT effects, most notably DLT integrity effect and DLT availability effect.

DLT effect factor	Description of effect of factor	Implementation in DLT
Integrity	Prevents accidental or malicious modification of data.	Consensus algorithm together with distributed validation guarantees multiple validly synchronised copies (of the DLTs).
Transparency	Everyone sees each transaction, so all transactions are common knowledge to every member.	Integrity, availability and immutability together with DLT as an integration DB by policy
Availability	Information stays available even in accidental or malicious Denial of Service attacks by any party.	Sufficiently massive number of multiple parallel copies which are guaranteed to be in sync via consensus algorithm.
Immutable full history	Reputation solidified.	DLT is append only. This is the core component of the integrity of the DLT.

Simulation results show that the collaboration via a federation, where only one member (instead of all of them) is disturbed, becomes even more sensitive to the changes of fixes effect on harm multiplier around the unstable equilibrium point. The unstable equilibrium, i.e., tipping point, for the case where only one member is disturbed, can be found from the simulation runs by determining a maximum value for the fixes effect on harm multiplier where the federation is only able to recover from the disturbance.

Fig. 6 and Fig. 7 show that the analytical result of Section IV also applies to federations where only 1 member (instead of all) is disturbed. Therefore, a federation of size 10 is more sensitive to *Fixes effect on harm multiplier* than federation of size 3 around its tipping point.

Finally, a fifth simulation scenario presents another finding from the sensitivity simulation run of a five party federation with a large variation of the member starting success, as shown in Fig. 8. The smaller the magnitude of DLT integrity effects, the more fragile the federation becomes because the DLT integrity effect reduces the fixes effect on harm multiplier, which is the key controlling parameter of the federations sensitivity to collapse near the tipping point. This result is due to the interconnected nature of the success of the constituent federation members. The overall federation health is highly sensitive even to minor variations of the coefficient fixes effect on harm multiplier, which determines how much harm participants are willing to induce on other members while serving their self-interest. Thus, the deciding dynamic for a healthy and successful federation is that the unselfishness must be of sufficiently high intensity relative to the intensity of the collateral harm from random errors, misconceptions and selfishness; otherwise, the federation will not survive.

[6] In classical game theory, self-interest is considered rational.

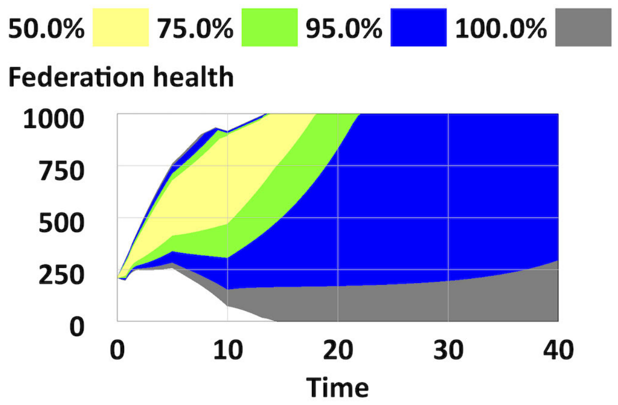


FIGURE 8. ***Federation health*** **of a heterogeneous federation, is also very sensitive to the parameter** ***Fixes effect on harm multiplier*** **in the presence of one member governance shocks.**

By interpreting the simulation results of this paper, we can observe that DLTs have a clear stabilisation potential in federations via the reduction of unnecessary harm to other members. This observation is based on the ability of DLTs to keep an account of harms but also of success and unselfishness. Moreover, DLTs are able to achieve all this in a non-repudiable way while driving the system closer to a common-knowledge scenario. Thus, utilising the DLTs has the potential to make federal organisations both more long-term oriented and less selfish.

VII. DISCUSSION

Currently, DLTs are primarily considered as a technology to produce *integrity*, which is one of the three components in the traditional information security triad: Confidentiality, Integrity, Availability (CIA). Decentralisation of DLTs allows achieving great improvement in the security characteristics of availability and integrity. Information security in general, and integrity and availability in particular, are vital for both collaboration resiliency and financial success.

It is noteworthy that our approach does not rely on only a single all-encompassing DLT. Therefore, a federated platform may use multiple distributed ledgers to affect the key parameters in our model. As long as the ledgers are sufficiently coordinated (e.g., via interledger gateway or other means) to produce the beneficial effects of DLTs, our results and analyses hold.

From a practical standpoint, many times *availability* may be the more crucial feature of DLTs. If we make federated consortia with joint DLTs and strongly force all relevant business transactions to flow via the DLT, each participating business has naturally its own copy of all the formal transactions of everyone operating as part of the DLT.. This stands in stark contrast to the typical case, in which the joint decision information is withheld in sole possession of some governance unit formally responsible for its execution. In particular, the independent nature of the governance unit requires the unit acquire confidentiality to separate itself from its members, i.e., to keep itself from being a mere pass-through agentic state executive arm.

Our simulation results are generalisable results under the archetypal model and the provided parameters. Many collaboration paradigms are such that they aim at keeping the collaboration sustainable. On the other hand, we do not want systems where excessive resources are only aimed at maintaining the collaboration. Our simulations are based on system parameter values, which are dynamically sustainable, i.e., they produce flat lining or slightly more, or are asymptotically non-negative with regards to growth.

In this work, we do not specifically concentrate on the initial stages of the construction of such collaborative structures. These setup stages are studied, for example, by Farris *et al.* [7] and incentivised via coalition formation games. Thus, our results are mainly applicable to collaborative arrangements, which aim at balancing themselves to be sustainable. The main results concern how much a member platform can devote its resources to itself, and what each platform should give to others to ensure collaboration. Our work investigates the boundary between self and other. Therefore, our results show that the collaboration cannot be sustained at all, unless a threshold is reached in the portion of each participants' own resources given to others. Exact units of account for measuring such collaborative contributions, and engaging their network effects, are currently under development. For example, see [48].

VIII. CONCLUSION

The lack of interoperability between IoT systems has become a societal level problem due to increasing prevalence of IoT systems. Apart from technical interoperability challenges, a further challenge is IoT systems often being owned and managed by separate entities, which increases the importance to consider also the economic and governance aspects of federation and collaboration.

Federations can offer a flexible model for collaboration as they do not automatically require significant changes to the members platforms' operational model. Our simulations are based on system parameter values, which are dynamically sustainable, i.e., they produce flat lining or slightly more, or are asymptotically non-negative with regards to growth.

This paper examined IoT federations and finds that they are sensitive to collateral harm caused by the actions of individual members. Thus, the stability and resiliency of the federation can be improved by introducing a DLT-based governance model that helps to provide more transparency and accountability for the actions of individual members.

Future research should further investigate system dynamics by modelling and simulating the tension filled relationship of the governance unit supposedly representing the collective and individual sovereign members. In addition, it is worthwhile to engaged in a detailed study on the effects of timings and to compare the effects of shocks aimed at collective and individual members. Another emerging and interesting approach is to model non-rival units of account and their novel basis of value creation, economic behaviour, and social improvement potential.

ACKNOWLEDGMENT

The authors wish to thank Prof. Pekka Nikander, Prof. Vasilios Siris, and Gen Kelsang Tubchen for the meticulous and long term private and public teaching work that has made this publication possible. Also, a big thank you to MA Len Malczynski, who advised Tommi M. Elo's studies at System Dynamics Summer School 2020, and introduced all participants to a wide variety of archetypes with an additional encouragement to start dealing with the general problem of the dynamics of Escalation. Prof. Heikki Hämmäinen and Prof. Raimo Kantola helped in practical research and people management as well as internalizing the academic mindset, an absolute requirement for performing and communicating research successfully. Kenneth Falck and Tuuli Valtonen provided valuable advice with regards to the clarity of the text and the main arguments. Ken Pennington and Jan-Mikael Rybicki provided a professional and multistage language review. Sincere thank you for everyone mentioned.

REFERENCES

[1] D. Lagutin, F. Bellesini, T. Bragatto, A. Cavadenti, V. Croce, Y. Kortesniemi, H. C. Leligou, Y. Oikonomidis, G. C. Polyzos, G. Raveduto, F. Santori, P. Trakadas, and M. Verber, "Secure open federation of IoT platforms through interledger technologies—The SOFIE approach," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Valencia, Spain, Jun. 2019, pp. 518–522. [Online]. Available: https://ieeexplore.ieee.org/document/8802017/

[2] C. I. Jones and C. Tonetti, "Nonrivalry and the economics of data," *Amer. Econ. Rev.*, vol. 110, no. 9, pp. 58–2819, 2020.

[3] P. Nikander, V. Eloranta, K. Karhu, and K. Hiekkanen, "Digitalisation, anti-rival compensation and governance: Need for experiments," in *Proc. Nordic Workshop Digit. Found. Bus., Oper., Strategy*, Espoo, Finland, 2020, p. 7.

[4] P. Nikander and T. Elo, "Will the data markets necessarily fail? A position paper," in *Proc. 30th Eur. Regional ITS Conf., Int. Telecommun. Soc. (ITS)*, Helsinki, Finland, 2019. [Online]. Available: https://EconPapers.repec.org/RePEc:zbw:itse19:205201

[5] A. Celesti, M. Fazio, M. Giacobbe, A. Puliafito, and M. Villari, "Characterizing cloud federation in IoT," in *Proc. 30th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Mar. 2016, pp. 93–98.

[6] S. Soursos, I. P. Zarko, P. Zwickl, I. Gojmerac, G. Bianchi, and G. Carrozzo, "Towards the cross-domain interoperability of IoT platforms," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, Jun. 2016, pp. 398–402.

[7] I. Farris, L. Militano, M. Nitti, L. Atzori, and A. Iera, "MIFaaS: A mobile-IoT-federation-as-a-service model for dynamic cooperation of IoT cloud providers," *Future Generat. Comput. Syst.*, vol. 70, pp. 126–137, May 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X16302138

[8] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, Nov. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X17329205

[9] A. Manzoor, M. Samarin, D. Mason, and M. Ylianttila, "Scavenger hunt: Utilization of blockchain and IoT for a location-based game," *IEEE Access*, vol. 8, pp. 204863–204879, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9253568/

[10] J. Kemeny, "Accidental adversaries: When friends become foes," *Syst. Thinker*, vol. 5, no. 1, Feb. 1994. [Online]. Available: https://thesystemsthinker.com/accidental-adversaries-when-friends-become-foes/

[11] W. Braun, "The system archetypes," *System*, vol. 2002, p. 27, 2002. [Online]. Available: https://www.albany.edu/faculty/gpr/PAD724/724WebArticles/sys_archetypes.pdf

[12] E. Hoffman and E. M. Krol, *FYI on What is the Internet?* (Request for Comments), no. 1462. RFC Editor, May 1993. [Online]. Available: https://rfc-editor.org/rfc/rfc1462.txt

[13] L. M. Camarihna-Matos and H. Afsarmanesh, "Concept of collaboration," in *Encyclopedia of Networked and Virtual Organizations*. Hershey, PA, USA: IGI Global, 2008, pp. 311–315.

[14] L. M. Camarinha-Matos and H. Afsarmanesh, "Roots of collaboration: Nature-inspired solutions for collaborative networks," *IEEE Access*, vol. 6, pp. 30829–30843, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8374409/

[15] W. Wang, A. Tolk, and W. Wang, "The levels of conceptual interoperability model: Applying systems engineering principles to M&S," in *Proc. Spring Simul. Multiconf.*, 2009, pp. 1–9.

[16] C. S. Fleisher, "Using an agency-based approach to analyze collaborative federated interorganizational relationships," *J. Appl. Behav. Sci.*, vol. 27, no. 1, pp. 116–130, Mar. 1991.

[17] M. M. Yassa, H. A. Hassan, and F. A. Omara, "New federated collaborative networked organization model (FCNOM)," *Int. J. Cloud Comput. Services Sci.*, vol. 1, no. 1, p. 1, Jan. 2012.

[18] M. Jacoby, A. Antonic, K. Kreiner, R. Lapacz, and J. Pielorz, "Semantic interoperability as key to IoT platform federation," in *Interoperability and Open-Source Solutions for the Internet of Things* (Lecture Notes in Computer Science), vol. 10218, I. Podnar Zarko, A. Broering, S. Soursos, and M. Serrano, Eds. Cham, Switzerland: Springer, 2017, pp. 3–19, doi: 10.1007/978-3-319-56877-5_1.

[19] A. Berg, C. Berg, and M. Novak, "Blockchains and constitutional catallaxy," *Constitutional Political Economy*, vol. 31, no. 2, pp. 188–204, Jun. 2020, doi: 10.1007/s10602-020-09303-9.

[20] V. A. Siris, P. Nikander, S. Voulgaris, N. Fotiou, D. Lagutin, and G. C. Polyzos, "Interledger approaches," *IEEE Access*, vol. 7, pp. 89948–89966, 2019.

[21] D. Roeck, H. Sternberg, and E. Hofmann, "Distributed ledger technology in supply chains: A transaction cost perspective," *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2124–2141, Apr. 2020, doi: 10.1080/00207543.2019.1657247.

[22] S. Ghaemi, H. Khazaei, and P. Musilek, "ChainFaaS: An open blockchain-based serverless platform," *IEEE Access*, vol. 8, pp. 131760–131778, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9143110/

[23] S. Benedict, "Serverless blockchain-enabled architecture for IoT societal applications," *IEEE Trans. Comput. Social Syst.*, vol. 7, no. 5, pp. 1146–1158, Oct. 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9149700/

[24] S. Ruutu, T. Casey, and V. Kotovirta, "Development and competition of digital service platforms: A system dynamics approach," *Technol. Forecasting Social Change*, vol. 117, pp. 119–130, Apr. 2017. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0040162516308605

[25] S. Morris and H. S. Shin, "Approximate common knowledge and coordination: Recent lessons from game theory," *J. Log., Lang. Inf.*, vol. 6, no. 2, pp. 171–190, 1997.

[26] S. Nakamoto. (Oct. 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[27] Government Chief Scientific Adviser, UK, "Distributed ledger technology: Beyond block chain," Government Office Sci., London, U.K., Tech. Rep., 2016.

[28] J. D. Sterman, *Business Dynamics: Systems Thinking and Modeling for a Complex World*. New York, NY, USA: McGraw-Hill, 2000.

[29] J. W. Forrester, "Counterintuitive behavior of social systems," *Theory Decis.*, vol. 2, no. 2, pp. 109–140, Dec. 1971.

[30] P. M. Senge, "The fifth discipline," *Measuring Bus. Excellence*, vol. 1, no. 3, pp. 46–51, 1997.

[31] J. W. Forrester, "System dynamics and the lessons of 35 years," in *A Systems-Based Approach to Policymaking*, K. B. De Greene, Ed. Boston, MA, USA: Springer, 1993, pp. 199–240, doi: 10.1007/978-1-4615-3226-2_7.

[32] J. M. Garcia and J. Sterman, *System Dynamics Fast Guide: A Basic Tutorial With Examples for Modeling, Analysis and Simulate the Complexity of Business and Environmental Systems*, Independently Published, Spain, 2019.

[33] J. H. Miller and S. E. Page, *Complex Adaptive Systems: An Introduction to Computational Models of Social Life*. Princeton, NJ, USA: Princeton Univ. Press, Nov. 2009.

[34] M. Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference*. New York, NY, USA: Little Brown, Hachette Book Group, 2000.

[35] N. N. Taleb and R. Douady, "Mathematical definition, mapping, and detection of (anti) fragility," *SSRN Electron. J.*, vol. 13, pp. 1677–1689, Nov. 2013.

[36] N. N. Taleb, *Antifragile: Things That Gain From Disorder*, vol. 3. New York, NY, USA: Random House Incorporated, 2012.

[37] T. R. B. Taylor and D. N. Ford, "Managing tipping point dynamics in complex construction projects," *J. Construction Eng. Manage.*, vol. 134, no. 6, pp. 421–431, Jun. 2008, doi: 10.1061/%28ASCE%290733-9364%282008%29134%3A6%.

[38] T. Taylor and D. N. Ford, "Tipping point failure and robustness in single development projects," *Syst. Dyn. Rev.*, vol. 22, no. 1, pp. 51–71, Mar. 2006, doi: 10.1002/sdr.330.

[39] N. P. Repenning, "Understanding fire fighting in new product development," *J. Product Innov. Manage.*, vol. 18, no. 5, pp. 285–300, Sep. 2001, doi: 10.1111/1540-5885.1850285.

[40] H. Rahmandad and N. Repenning, "Capability erosion dynamics," *Strategic Manage. J.*, vol. 37, no. 4, pp. 649–672, Apr. 2016, doi: 10.1002/smj.2354.

[41] J. W. Rudolph and N. P. Repenning, "Disaster dynamics: Understanding the role of quantity in organizational collapse," *Administ. Sci. Quart.*, vol. 47, no. 1, pp. 1–30, Mar. 2002, doi: 10.2307/3094889.

[42] H. Rahmandad, N. Repenning, and J. Sterman, "Effects of feedback delay on learning," *Syst. Dyn. Rev.*, vol. 25, no. 4, pp. 309–338, Oct. 2009, doi: 10.1002/sdr.427.

[43] F. Pargar, J. Kujala, K. Aaltonen, and S. Ruutu, "Value creation dynamics in a project alliance," *Int. J. Project Manage.*, vol. 37, no. 5, pp. 716–730, Jul. 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0263786318304836

[44] T. Eisenmann, G. Parker, and M. W. Van Alstyne, "Strategies for two-sided markets," *Harvard Bus. Rev.*, vol. 84, no. 10, p. 92, 2006.

[45] A. Hagiu and J. Wright, "Multi-sided platforms," *Int. J. Ind. Org.*, vol. 43, pp. 162–174, Nov. 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167718715000363

[46] D. Frolov, "Blockchain and institutional complexity: An extended institutional approach," *J. Institutional Econ.*, vol. 17, pp. 1–16, Feb. 2020.

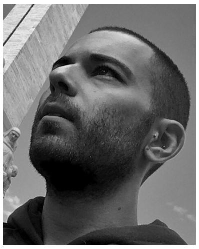
[47] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Acad. Manage. Rev.*, vol. 20, no. 3, pp. 709–734, 1995.

[48] E. Hakanen, P. Töytäri, T. Turunen, and V. Eloranta, "Strategic logics behind blockchain projects: Capturing value in decentralized ecosystems," *Acad. Manage. Global Proc.*, vol. 2018, p. 409, Dec. 2018, doi: 10.5465/amgblproc.telaviv.2018.0409.

TOMMI M. ELO received the M.Sc. (Tech.) degree in computer science from the Helsinki University of Technology, Finland, in 2000. He is currently pursuing the Ph.D. degree with the Department of Communications and Networking, Aalto University.

He has worked on numerous research projects at the Helsinki University of Technology and Aalto University, including EU H2020 SOFIE and EU EMPIR SMARTCOM. He has also worked over a decade in information security of finance. His research interests include alternative currencies and other socio-technical systems, blockchains and DLTs, system dynamics, and information security and privacy.

SAMPSA RUUTU received the M.Sc. (Tech.) degree from the Helsinki University of Technology, Finland, in 2008, and the D.Sc. (Tech.) degree in the field of systems and operations research from Aalto University, Finland, in 2019. He has worked on numerous research, development, and innovation projects at the VTT Technical Research Centre of Finland and Aalto University. His research interests include system dynamics and agent-based simulation methods, systemic impact evaluation, digital platforms, and innovation policy.



EKTOR ARZOGLOU received the dual M.Sc. degree in security and privacy from the EIT ICT Labs Master School. He is currently pursuing the Ph.D. degree with Aalto University, Finland. His research interests include the fields of digital platforms, privacy, system dynamics, and systems thinking.

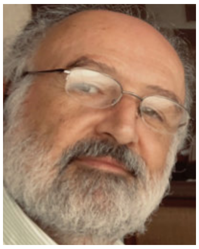
YKI KORTESNIEMI received the M.Sc. (Tech.) degree in industrial management and the Lic.Sc. (Tech.) degree in computer science from the Helsinki University of Technology, Finland, in 1998 and 2003, respectively, and the D.Sc. (Tech.) degree in networking technology from Aalto University, Finland, in 2015.

He has worked on numerous research projects at the Helsinki University of Technology and Aalto University, including the EU H2020 Projects SOFIE and IoT-NGIN. His research interests include information security and privacy, data protection, MyData and legal design, the Internet of Things, distributed ledgers and blockchains, and decentralized identifiers and verifiable credentials.

DMITRIJ LAGUTIN received the M.Sc. (Tech.) degree from the Helsinki University of Technology, Finland, in 2005, and the D.Sc. (Tech.) degree from Aalto University, Finland, in 2010.

He was a Researcher in several research projects with the Helsinki University of Technology and Aalto University, including EU FP7 PSIRP, PURSUIT, and EU H2020 POINT Projects. He is currently a Coordinator and a Research Fellow with the EU Horizon 2020 SOFIE Project at Aalto University. His research interests include network security and privacy, the Internet of Things, blockchains, and future network technologies.

VERIA HOSEINI received the B.Sc. degree in mathematics from the University of Zanjan, in 2008, and the M.Sc. degree in cryptography and data security from the University of Turku, Finland, in 2018. He is currently pursuing the Ph.D. degree with the Department of Communications and Networking, Aalto University, Finland. His research interests include blockchain technology and consensus algorithms.



GEORGE C. POLYZOS (Member, IEEE) received the Diploma degree in electrical engineering from the National Technical University of Athens, Greece, and the M.A.Sc. degree in electrical engineering and the Ph.D. degree in computer science from the University of Toronto, Canada.

He was a Professor of computer science and engineering with the University of California, San Diego, where he was the Co-Director of the Computer Systems Laboratory and a member of the Steering Committee of the Center for Wireless Communications and a Senior Fellow of the San Diego Supercomputer Center. He is leading the Mobile Multimedia Laboratory (MMlab), Athens University of Economics and Business, where he is currently a Professor of computer science and the Director of the M.Sc. degree in computer science. Under his leadership, the MMlab has participated in a series of research projects that co-developed publish-subscribe internetworking and an information-centric networking architecture. More recently, he led MMlab's contributions to EU-Funded Project Secure Open Federation for Internet Everywhere (SOFIE) on Distributed Ledger and Interledger Technologies applied to federated Internet of Things (IoT) systems. His current research interests include the IoT, smart grid, security and privacy, and internet architecture and protocols.

Dr. Polyzos has served on journal editorial boards, as a special issue guest editor and on committees of many conferences and workshops. He is on the Editorial Boards for the IEEE Transactions on Mobile Computing and the *Journal on Reliable Intelligent Environments*.