MOATcoin: Exploring Challenges and Legal Implications of Smart Contracts Through a Gamelike DApp Experiment

Biagio Distefano, Nadia Pocher, and Mirko Zichichi. 2020. MOATcoin: Exploring Challenges and Legal Implications of Smart Contracts Through a Gamelike DApp Experiment. In *3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock 2020), September 25, 2020, London, United Kingdom.* ACM, New York, NY, USA, 6 pages.

CryBlock 2020, September 25, 2020, London, United Kingdom © 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-8079-9

MOATcoin: Exploring Challenges and Legal Implications of Smart Contracts Through a Gamelike DApp Experiment

Biagio Distefano
Universität Wien Law, Science and Technology RIoE
biagio.distefano@univie.ac.at

Nadia Pocher
Universitat Autònoma de Barcelona Law, Science and Technology RIoE
nadia.pocher@uab.cat

Mirko Zichichi
Universidad Politécnica de Madrid Law, Science and Technology RIoE
mirko.zichichi@upm.es

All the authors contributed equally.

FUNDING

This work has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie International Training Network European Joint Doctorate **grant agreement No 814177 LAST-JD-RIoE** and is part of the activities of University of Bologna's Legal Blockchain Lab.

ABSTRACT

In this paper we present MOATcoin, a gamelike experiment that enabled us to practically investigate the open issues related to the governance and legal facets of smart contract based decentralized applications. After presenting the MOATcoin system architecture, we first tackle the problems of decentralized governance, its limits and the shift of trust that it entails; then, we explore the possible legal implications of the given scenario and, particularly, the consequences of code-written contracts. Finally, we offer taxonomical remarks on the concepts of "token" and "coin" and offer an insight from a regulatory perspective.

CCS CONCEPTS

Applied computing → Law; **Computer systems organization** → Distributed architectures.

KEYWORDS

Distributed Ledger Technologies, Smart Contract, Blockchain, Governance, Tokens, Crypto-assets, dApp, Law and Technology

1 INTRODUCTION

Distributed Ledger Technologies (DLTs), originally introduced in the form of blockchain [20], enable the advent of a new vision to consider finance, trust in communication and governance. The distributed ledger ensures the immutable persistence of data, thus providing untampered data to applications when necessary. For this reason, DLTs represent an interesting technology for the development of reliable, decentralized applications (hereinafter: DApp) and services, based on Smart Contracts [3, 5].

In this paper we investigate the multidisciplinary facets, challenges and legal implications of smart contract-powered social interaction governance tools exploiting a "decentralized" game called MOATcoin[1]. Although this Dapp is just a game, with its simplification of a real-life scenario, it showcases crucial implications of real-world smart contract use cases. This made it possible to critically analyse what we consider to be the crucial matters of DApps that claim to have legal relevance.

In order to perform this experiment, we set up a simple set of rules for a game that had to be executed on a decentralized environment. The game scenario pictures twenty Law, Science and Technology Joint Doctorate PhD candidates talking incessantly about work, even after office hours. To solve this, a simple rule was imposed: whoever pronounces certain work-related keywords (e.g., "GDPR", "blockchain") outside the office premises, has to buy a beer to another candidate. Since all twenty candidates are peers and no governing bodies were to be formed, we adopted a decentralized architecture based on Ethereum smart contracts [5][2].

MOATcoin enables us to question the actual level of decentralization of DApps, as well as to explore governance and legal impacts of software architecture choices and the relevance of the concept of "token", to the end of highlighting problems and possible solutions. Along with this, a complementary issue needs to be addressed. DLT-related discourse is flooded with terms such as "coins", "cryptoassets", "tokens", "virtual currencies", "cryptocurrencies", "digital assets", "virtual assets", etc. From a legal and regulatory perspective, these expressions give way to endless considerations and uncertainties. From a practical perspective, it is pivotal to find a balance that avoids the loss of any technical and non-technical common ground.

The remainder of this paper is organized as follows: Sections 2 and Section 3 introduce some background and related work and outline the architecture of MOATcoin. From Section 4 we start discussing the experiment results by providing an overview of MOATcoin's governance model and highlighting weak points and possible solutions. Then, Section 5 offers a perspective on the relation between smart and legal contracts. In Section 6 we place MOATcoin within the world of tokens, by introducing taxonomy considerations and relevant implications. Finally, Section 7 provides some concluding remarks.

2 BACKGROUND AND RELATED WORK

In this section, we review some of the main features of smart contracts deployed on the Ethereum network.

2.1 Smart Contracts

The Ethereum Virtual Machine is able to compute (*quasi*-)Turing complete programs, i.e., smart contracts, whose execution is performed in a distributed way: all network participants receive the same inputs and perform a computation that leads to the same outputs (when they respect the protocol); then, each process is completely traced and permanently stored on the blockchain [5]. This principle is essentially based on the assumption that the majority of participants are honest and follow the Ethereum protocol. Under this assumption, the mediation of a trusted authority is not required, as foreseen in [25], because the immutable list of instructions of a smart contract leads deterministically to only one result.

Generally speaking, the purported purpose of smart contracts is to put forward a paradigm of "trustless trust"; trust is shifted from a human intermediary to the protocol itself [29]. This feature, together

[1] https://www.moatcoin.org

[2] All participants agreed to the relevant privacy policy and gave their consent to engage in the game and to share their data in the experiment.

with manipulation-resistance, shapes smart contracts as very promising tools to develop new applications [3, 31] and governance models [18, 30], whenever currency transfers or compliance with certain agreed rules is required.

If the issuer of a smart contract can be sure that the implemented behaviour is observed, a transaction between two parties does not require the presence of a third party. This is a big "if", because the trustless trust given to the protocol is different from the trust given to the smart contract code, i.e., the implemented behaviour. Since contract design choices can be fatal [3], trust in the code can be reached by using verified design patterns or by auditing, as discussed in Section 4.2.

2.2 Tokens and Decentralized Autonomous Organizations (DAO)

Most DLT ecosystems feature tokens as a crucial pillar [2, 24, 26].

Within the Ethereum network, Improvement Proposals (EIPs)[3] enable to define the standards of Ethereum Smart Contracts; they do so by singling out different types of design patterns for tokens. The ERC20 standard, for instance, is the most common choice for second layer cryptocurrencies. On the other hand, the ERC721 token is a non-fungible utility token, usually implemented to represent and transact with (tangible or intangible) assets on DLTs.

A Decentralized Autonomous Organization (DAO) [18] is a virtual entity managed by smart contracts and executed in a decentralized way. The use of the Ethereum blockchain implies that the organization state is maintained by a consensus system and that contracts are used to implement transactions, currency flows, rules and rights inside of the organization. After a DAO code is deployed, its members can interact through smart contracts and Ether may be sent or received. Usually, a DAO issues tokens in exchange for Ether; tokens grant their holder a certain set of rights with the DAO. Members of a DAO are able to propose options for decision in the organization but they can also discuss and vote those through transparent mechanisms.

3 SYSTEM ARCHITECTURE

The adoption of a decentralized architecture for such a gamelike DApp stems from the need for: (a) a fair ruling authority, (b) incentives to participation, (c) cheating avoidance (e.g., unjustly accusing another candidate of a rule breach), (d) open and peer-based dispute resolution, (e) fair and transparent tracking The model that we adopted present a decentralized governance based on these points.

3.1 Smart Contract Design

We built a smart contract that combines a variation of a standard ERC20 token with a voting contract[4].

3.1.1 Token Contract.

The smart contract implemented in Ethereum[5]consists in the extension of an ERC20 token. It therefore inherits all the features of this type of token, such as transferability, allowance and minting. The extensions to the original ERC20 smart contract are made to facilitate the exchange of this asset between participants: (1) Stake On: the MOATcoin protocol requires that when someone breaches the rule (i.e., says a forbidden keyword outside office hours), another participant has to publicly accuse them; this process consists in staking one token on the accused participant. The stake means transferring the token to the contract that acts as escrow. (2) Stake Won: The accused participant has two choices: (a) buy a beer to another candidate; (b) challenge the accusation. If the accused chooses to buy the beer, a participant, different from both accuser and accused, testifies that the accused won the stake. This enacts a process in the smart contract where: (i)

[3] https://eips.ethereum.org/

[4] Publicly accessible at https://gitlab.com/CIRSFID/moatcoin

[5] The contract is currently deployed on the Ropsten testnet at x703dbd8ccfda00dcedddab21a8d93d09db39e177

the staked token is transferred from the contract to the accuser; (ii) three reward tokens are minted, one for each, for the accuser, the accused and the witness.

3.1.2 Voting Contract.

The MOATcoin smart contract extends also the functionalities of a simple voting contract. Indeed, when the accused participant chooses to challenge the accusation: (1) a new challenge is issued and the stake gets paused; (2) a trial is opened and the accused becomes a defendant; (3) each participant can cast their vote; the weight of the vote is proportional to the number of tokens held; (4) at the end of the voting window, the sentence gets auto-executed: if the defendant is found guilty, the stake gets un-paused and they will have to buy the beer; if the defendant is found not guilty, the accused loses their stake through the smart contract burn feature, and the defendant will no longer have to buy the beer.

3.2 DApp Architecture

In **Figure 1** (left diagram) we show the architecture of the Dapp we used for the experiment. The access to the smart contract functionalities is made possible by the interaction with an external service, i.e., a Telegram chat in conjunction with a bot[6]. This bot, which dwells in a chat group and limits the interactions to its participants, acquires commands through the Telegram app interface and forwards requests to dedicated server. In the MOAT server, Ethereum accounts are mapped to participants' Telegram IDs and are used to invoke the methods exposed by the MOATcoin smart contract.

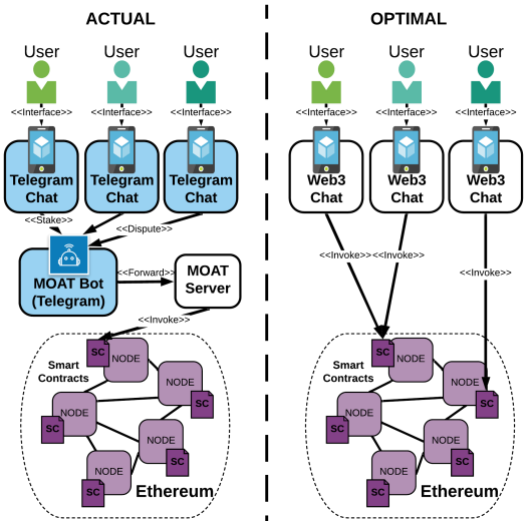

Figure 1: Dapp architecture diagram

4 GOVERNANCE ASPECTS

In the previous section we introduced MOATcoin as a decentralized game to better understand the challenges of decentralized governance. Since MOATcoin combines a custom ERC20 token, a voting contract and other user interaction mechanisms, it could be argued that it leans towards the label "DAO"; technically, though, it differs from the strict interpretation of DAOs, e.g., it lacks the token-for-Ether issuance mechanism. Labels aside, the most important aspects of the governance model we are presenting are the decentralized policing and the dispute resolution system.

[6] https://core.telegram.org/bots

The results of our experiment, however simple, showcase three core issues that almost any DApp is forced to deal with: (1) user experience; (2) correspondence of code with agreement; (3) decentralization bottlenecks.

4.1 User Experience and Maintenance

The chosen architecture (Figure 1, left-hand side) entails a trade-off between (a) development/maintenance ease, (b) user experience, (c) decentralization. The deployment of the app on a Telegram bot incentivised participation in the experiment, as users were not required to adjust to a new interface. Meanwhile, it eased scalability, in terms of entrance of new members and consequent needs of new patterns for invoking the actions staking and witnessing, that require the participants' names. Finally, the chosen architecture allowed for bug fixing during production.

However, the same choice revealed a significant level of recentralization; e.g., due to the mishandling of a timeout exception, a challenge to a stake had to be triggered manually server-side. Preserving decentralization (figure 1, right-hand side) while safeguarding user experience would have required a higher investment in terms of development costs.

4.2 Source Code *vs* Agreement: a shift of trust

Another problem that arises is that it is impossible, at the moment, to reassure participants that the source code of the smart contract they are interacting with corresponds to the rules they have agreed on. This problem affects almost every smart contract based DApp. The claim of trustlessness and decentralization is irrelevant when having to deal with common users, since non-expert users will have to trust the coders that developed the DApp, or the Open Source Community (OSC) that reviewed and/or confirmed the correspondence of code with claims. The latter case can make sense in large community-driven projects, where there is significant resonance in the public, but not in small, independently developed DApps, that cannot possibly be all reviewed by the OSC.

In other words, especially in small scale projects, trust is not shifted from institutions to technology, rather from institutions to developers [28]. A possible solution could be to write (markup) the human-readable set of rules (contract) in Akoma Ntoso, then build an Ontology to operate with the contract and markup the provisions in LegalRuleML. The contract would now be machine readable too, and the smart contract's logic correspondence with the contract's provisions could be formally validated. This architecture is called "intelligible contract" [6]. But again, the trust would be shifted from the DApp developer to the formal validation system developer. Thereby, especially in small-scale applications such as MOATcoin, trust is not kicked out of the equation, just shifted.

The problem of correspondence of source code with the rules agreed upon beforehand demonstrates how technology by itself cannot eliminate the need of trust in experts or institutions. While this might be the case when all the parties involved are coders or possess a certain degree of IT expertise, a DApp, to the eyes of common users, serves the very same purpose of any other non-decentralized app. In the end, this is the only thing that matters: to convince users to trust the technology requires to convince them to trust the developers or the company that developed it.

Nonetheless, it is possible to argue that DApps are relatively more auditable than traditional software. Still, auditability gains value only in three cases: (a) when the user can perform it (which is rarely the case); (b) when it is performed by an expert (yet another shift of trust); (c) when performed by the OSC.

Cases (a) and (b) are of little to no interest here. Case (c), on the other hand, represents the kernel of the problem. Community driven audit is what really powers DLTs and DApps credibility, since, thanks to the OSC audit, correspondence of code with claims and actual DApp deployed instance can be assured. However, the problem still stands: trust is not eliminated, it is just spread across the liquid texture of the OSC. The wider the Community behind the project, the more trustworthy the DApp. Small, independent developers will have little to no use in building smart contract-based solutions in terms of sheer trustworthiness. Moreover, as the OSC loses interest in the project, its trustworthiness fades accordingly. In other words, what DLTs and DApps truly allow for is not the elimination of the need of trust in institutions or third parties, rather, they enable a virtuous cycle of trust empowerment with OSCs.

That said, we argue that trust *is* a zero-sum game and cannot be taken out of the equation. Rather, it gets shifted, mediated by technology [4] or spread across a community. The shape it takes depends on the DApp architecture, on the community behind it and on its user base, but it will always play a significant role.

4.3 The Vulnerability of Complete Decentralization

The final flaw that characterizes this architecture is determined by its semi-open permission nature. As explained, the game works as long as a user has tokens to spend to accuse another user of pronouncing a forbidden word; then, the rules of minting described above (accuse/witness/challenge) increase the overall token count. The problem is that the possession of MOATcoins is the only thing that allows or prevents user participation. This means that a user could easily perform a sybil attack by sending a token to one or more different addresses under their control and automate an accuse-witness routine to increase wealth and, consequently, voting power. A possible solution could be to allow only registered users to participate, but this would highly re-centralise power.

In this regard, with particular reference to bottlenecks that prevent complete decentralization, the presented game can be a cue for thoughts. As illustrated above, in order to participate, the only thing needed is an initial balance of MOATcoins. The initial coins are given out to participants upon identification-registration through a Telegram bot. It goes without saying that this process happens in an entirely centralized environment. Now, whatever the DApp architecture is going to be, some precautions would need to be taken in order to prevent sybil attacks. In a completely decentralized environment, this cannot be achieved unless economic disincentives are put into place (e.g., registration fee for each account); but in this case, a sybil attack feasibility would entirely depend on the ability of the attacker to break even.

The only other option is to centralize the identity verification / registration process. In this scenario, one could argue, there would be a single centralization step at the beginning, beyond which, being the code/rules immutable, decentralization would still play a significant role. Nonetheless, this would drastically increase the importance of the identification step, thus requiring a higher degree of trust on the subject, institution or oracle that performs it. The problem persists, and consequently scales, for whichever application that depends, even slightly, on identity verification.

5 CODE AS CONTRACT?

In the previous section we mentioned the problem of correspondence of code with agreement. This phrasing suggests that the smart contract in question is not what can legally be defined as a contract. The scenario proposed here tends to be similar to any other, regardless of the architecture adopted. We will refrain to delve into previous investigations on the relationship between smart and legal contracts [7] and propose the following approach.

Legally speaking – at least in roman juridical traditions – a contract is defined as the meeting of the will of two or more parties – an agreement – aimed at establishing, regulating or extinguishing an economically measurable legal relationship[7]. So, considering that the contract as such is concluded at the moment of consent, this will almost always precede the smart contract. However, it is possible to make an expression of the agreement in written form, and assume that the parties write it exclusively in the form of source code[8]. Such a hypothesis requires the effort, not unreal, to equate the programming language with a human language, when the parties fully and substantially understand the code, with the additional feature of being readable and executable by a computer.

However, although the programming language may arguably be suitable for conveying the will of the parties – despite legal debates on intelligibility, transparency and relevant impacts from a consent perspective [6] –, linguistic limitations emerge; notably, in our case at least, the **if-then construction**. In this

[7] See, as an example, Art. 1321 of Italian Civil Code.

[8] In Italy, Article 8-*ter* of the Simplifications Decree (D.L. no. 135 of 14 December 2018, converted into law by Law no. 12 of 11 February 2019), seems to allow such a case provided the compliance with the procedure for the identification of the parties yet to be defined by the Agency for Digital Italy (Agenzia per l'Italia Digitale - AGID), and in any case compliant with regulation eIdas Reg. (EU) No 910/2014.

respect, it should be noted that clauses containing contractual obligations, when simply written in if-then form (or equivalent, e.g., "require()"), *may* fall within the scheme of *conditional clauses*, being de facto stripped of their obligatory nature, if no other logic is used, e.g., legal deontic and defeasible logic [14]. This would leave contracting parties without any legal action to protect their interests; in fact, there would never be "non-performance", but simply "inaction", which does not trigger the conditional clause. In other words, when the contractual performance is undertaken into condition, there cannot be a contractual breach in its respect.

In the case of MOATcoin, if a party fails to accuse another candidate or to testify on their compliance, without the pre-existence of a legal contract in human language, there would be no legal action to pursue against said party. In order to mitigate this side effect we may integrate the smart contract with other legal rules, using deontic logic operators (rights, permissions).

There are, of course, many other legal issues that arise from the presented experiment, such as: (a) the relationship between decentralized contractual performance and jurisdiction, with particular reference to the Reg. (EU) No 1215/2012 (Bruxelles I-bis); (b) the matter of applicable law in decentralized agreements, with regard to Reg. (EC) No 593/2008 (Rome I); (c) the nature of MOATcoin's (or more generally, DLTs') dispute resolution system relatively to legal arbitration [1] and, particularly, to the Convention on the Recognition and Enforcement of Foreign Arbitral Awards, done at New York on 10 June 1958. Investigating such issues, however, falls outside the scope of this work; in light of the pursued multidisciplinary approach, in fact, it is now more appropriate to take a step back and a closer look at concepts that are at the heart of our experiment. Even more so, because their precise identification (or lack thereof) poses considerable legal and technical risks [23, 26].

6 TAXONOMICAL REMARKS

Our experiment requires our DApp users to own MOATcoins, previously referred to as tokens. The latter concept, however, is all but self-explanatory and is at the heart of discussions concerning the ontological features of an ever-changing landscape of virtual items. On the one hand, having no certainty concerning the legal box into which an entity can be placed is not a trivial thing; on the other, the lack of definition easily turns into a lack of standardization, which has cross-industry effects and hampers technological development. So, what is MOATcoin really?

6.1 The World of Crypto-assets

DLT-based applications are placing considerable strain on legal concepts, primarily at the definition level. In order to enable interdisciplinary collaboration, however, it is crucial not to get lost between different wordings, while at the same time averting an oversimplification of the world of "digital assets".

A growing number of studies is showing the manifold ways to approach these ecosystems from a legal perspective [21]. Due to the fast development of the crypto-economy and consequent time constraints, most initiatives have been prompted by fear of abuses rather than by the desire to grasp the connecting factors between the technological and juridical essence of these tools. Hence, terminological consensus has yet to be achieved.

In this paper we are presenting MOATcoin. When we hear the word "coin" we immediately associate it with currency. In this case, however, it is arguably safer to start from the concept of "token", which we know to be pivotal in the blockchain world because it is among its building blocks [2]. It was argued that *"far from being just a means of payment, tokens are the critical data structure that could underpin every aspect of the future society"* [24].

But whether and how a "token" gets to be a "coin" from a strict definition perspective is far from straightforward, although every "digital coin" is arguably a token. All in all, everything depends on what we mean by "coin" and "token"; this issue summarizes the relevance of recent efforts towards a categorization of "digital assets". These initiatives are pursued through singling out types, uses and properties of tokens, from a complementary legal and technical standardization perspective [16, 26].

6.2 Tokens

As first large-scale applications of crypto-tokens embraced the financial sector, most legal actions and reports largely focus on the latter. There are reports from European Institutions, the European Supervisory Authorities [8, 9], the Financial Stability Board [12], the UK Financial Conduct Authority [11, 15] and other institutions, as well as contracted private and academic stakeholders [13, 19]. Most detailed analyses of crypto-assets are performed to determine the applicability of financial services law[9].

There is general agreement that "tokens" are "crypto-assets"; the latter are broadly defined as "*a cryptographically secured digital representation of value or contractual rights that uses some type of DLT and that can be transferred, stored or traded electronically*" [11]. In legal, regulatory and policy documents both similar and more specific definitions can be found. Most interestingly, tokens have been conceptualized as the "legal wrap-up" of crypto-assets and depicted as crucial in the tokenized economy; their legal validity might be ensured also through smart contracts. Accordingly, tokens would be the way a legal right is embedded into a crypto-asset [19]. From one perspective, "tokens" can be *non-fungible* (i.e., unique, like crypto-collectibles), *fungible* (i.e., interchangeable, functionally equivalent) and also *hybrid*. As far as their compositional elements are concerned, they can have different behaviours - i.e., rules for how tokens behave (*transferable vs. non transferable; divisable vs. indivisable; singleton; mintable; role support; burnable*) - as well as different properties/property sets, a label that refers to a descriptive value that has external meaning. Crypto-assets in general can be *native* or *non-native*, which was used to highlight the difference between "coins", hence described as an asset that is native to its own blockchain (like Bitcoin and Ether) and "tokens", seen as assets that are built of top of another blockchain, like MOATcoin for instance.

A cutting-edge project is the "Token Taxonomy Initiative" [TTI] by the Blockchain Research Institute [26]. It highlights the need for standardization and meta-standardization also for technical and interoperability reasons. The TTI first identified a set of general characteristics of tokens: *valuable, representative, digital, discrete, authentic*. The "Token Taxonomy Framework" [TTF] is constantly updated [16] and pursues common terminological and development ground between technologists, businessmen, regulators and average consumers. One of the ideas is to break tokens down into basic components, verbally represented by "artifacts", which may belong to five different types: *Base Types, Behaviors, Behavior Groups, Property Sets, Token Templates (Formula + Definition)* [16].

Another endeavour to provide cryptographic tokens with a flexible framework is pursued by the International Token Standardization Association [ITSA]. While developing unique identifiers based on the concepts of Uniform Token Locator [UTL] and International Token Identification Number [ITIN] – for reference standardization purposes, both in legal contracts and elsewhere –, its initiatives comprise the development of the "International Token Classification" [ITC]. The latter heeds different dimensions, such as economic, technological and legal considerations [17, 23].

Trying to sum definitions up, in relation to their *purpose*, crypto-assets may be categorized as follows [15, 26]:

- Exchange (payment/currency) tokens: e.g., "virtual currencies". They are meant to be used as a means of payment or exchange for goods and services that are external to their native DLT ecosystem; commonly used also to facilitate payment services and for investment purposes;
- Security (investment) tokens: this category is used as a capital raising tool and for investment purposes[10];
- Utility tokens: they enable access to goods and services, that usually external to the DLT ecosystem they are built on. They can be used as a capital raising tool and for investments.

The purpose of specific tokens may also be hybrid.

Ethereum provides the opportunity to develop personal projects and DApps by making use of smart contracts deployed directly on the platform; smart contracts such as the one described in this paper can be used to control "digital assets". When a token is created to be used on a DApp, like in the MOATcoin case, its purpose depends on the application itself, so another term was conceived: application/platform token. These

[9] Findings vary according to the different legal systems

[10] In order to be classified as such, they are generally required to pass the so-called "Howey test" (they need to resemble financial instruments)

tokens can be used as “facilitators” for users that are external and unrelated to the operation of the network that has created them, which “merely” acts as a platform.

6.3 Is MOATcoin a *coin*?

What about MOATcoin? The answer is far from clear-cut; the name itself may be misleading. On top of being an application token, MOATcoin can be arguably be seen as a “utility token”. Moreover, its connection with Ether, and the fact that it could derive its value from it, does not rule out the development of an exchange purpose.

In any case, it does not currently feature any “payment or investment purpose”. Naturally, it could be labelled as “money” by different legal systems; the issue is broader than this from a monetary perspective. It was claimed that Bitcoin and other digital tokens have raised questions about the nature of money; a debate is ongoing on the social vs. legal dimensions of the latter [19, 22].

From a more empirical perspective, the TTF [26] mentions a set of behaviors to help define distinctive traits for a token to behave like money. Arguably it must: (a) have *roles* that are *definable* and *assignable*, and be (b) *delegable*: the token owner can delegate certain behaviors to other parties; (c) *transferable*: every token has an owner that can transfer it; (d) *holdable*; (e) *compliant*: e.g., with AML and KYC; (f) *burnable*; and (g) *mintable*. The same authors, however, leave it up for discussion whether to include other features.

Nevertheless, legal classifications end up playing the strongest role. MOATcoin, for instance, would in theory meet all requirements but the compliance aspect. However, it is still is an application token.

6.4 Problems and Opportunities

Going beyond MOATcoin, there is a general call to pay more attention to the concept of regulating “tokens” rather than “DLTs”. It was argued that regulators currently failing to grasp their pivotal role is leading to considerable legal uncertainty. As a positive example we can refer to Liechtenstein’s “Blockchain Act” [27], that chose not to regulate DLTs in general but rather to focus on “tokens” and treat them as “containers of rights”. A framework for their ownership and transfer was created; the obligation of service providers to register depends on their functional relationship with tokens [2].

If it is through tokens that blockchain and other DLTs can unfold their potential and create new ontological categories of assets, as well as new ecosystems for their exchange, it is through the prism of tokens (and relevant creation and exchange) that policymakers and regulators should approach their regulation [2]. Also the European Commission has identified the “tokenization” domain as lacking legal certainty and plans to focus on tokens’ legal framework when they are not considered financial instruments [10].

7 CONCLUSIONS

In this paper, we have presented a gamelike DApp, based on smart contracts, for the governance of social interaction between PhD candidates. We considered a real life use case to specifically focus on issues arising in the areas of decentralised governance, legal relevance and token classification.

In particular, the proposed experiment showed how in any “decentralized” application, whichever architecture it entails, trust gets shifted but is never eliminated. After highlighting possible legal impacts, we finally focused on the crucial role of sound taxonomical conceptualizations in the ever-evolving landscape of “tokens”, from both a technological and regulatory perspective.

REFERENCES

[1] Darcy Allen, Aaron Lane, and Marta Poblet. 2019. The Governance of Blockchain Dispute Resolution. *SSRN Electronic Journal* February (2019).

[2] Phoebus L Athanassiou. 2019. Tokens and the regulation of distributed ledger technologies: where Europe stood in the last quarter of 2018. *Journal of Int.Banking Law and Regulation* 34, 3 (2019), 105–114.

[3] Massimo Bartoletti and Livio Pompianu. 2017. An empirical analysis of smart contracts: platforms, applications, and design patterns. In *International conference on financial cryptography and data security*. Springer, 494–509.

[4] Balázs Bodó. 2019. Mediated Trust – A Theoretical Framework to Address the Trustworthiness of Technological Trust Mediators. *SSRN Electronic Journal* (2019). https://doi.org/10.2139/ssrn.3460903

[5] Vitalik Buterin et al. 2013. Ethereum white paper.

[6] Luca Cervone, Monica Palmirani, and Fabio Vitali. 2020. The Intelligible Contract. In *53d Hawaii International Conference on System Sciences*.

[7] Primavera De Filippi and Aaron Wright. 2018. *Blockchain and the law. The rule of code*. Vol. 52. Harvard University Press. 1–311 pages.

[8] EBA. 2019. *Report with advice for the European Commission on crypto-assets*.Technical Report January. https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf

[9] ESMA. 2019. *Advice - Initial Coin Offerings and Crypto-Assets*. Technical Report January. https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf

[10] European Commission. 2019. Blockchain Technologies: Promoting and Enabling DSM Legal Framework. https://ec.europa.eu/digital-single-market/ en/blockchain-technologies

[11] FCA. 2019. *CP19/3 Guidance on Cryptoassets*. Technical Report January. FCA. 1–50 pages. www.fca.org.uk/cp19-03-response-form

[12] FSB. 2018. *Crypto-assets: Report to the G20 on work by the FSB and standard-setting bodies*. Technical Report July. 1–8 pages.

[13] Carlo Gola and Andrea Caponera. 2019. Policy issues on crypto-assets. (2019).

[14] Guido Governatori, Florian Idelberger, Zoran Milosevic, Regis Riveret, Giovanni Sartor, and Xiwei Xu. 2018. On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law* 26, 4 (2018), 377–409. https://doi.org/10.1007/s10506-018-9223-3

[15] HM Tr., FCA, and B. of E. 2018. *Cryptoassets Taskforce: final report*. Technical Report October. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf

[16] InterWork Alliance. 2020. Token Taxonomy Framework (TTF). https://github.com/interwork-alliance/TokenTaxonomyFramework

[17] ITSA. [n.d.]. International Token Standardization Association. https://itsa.global

[18] Christoph Jentzsch. 2016. Decentralized autonomous organization to automate governance. *White paper, November* (2016).

[19] Fabrizio Maimeri and Marco Mancini. 2019. *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*. Technical Report. Banca d'Italia.

[20] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system.

[21] Nadia Pocher. 2020. The open legal challenges of pursuing AML/CFT accountability within privacy-enhanced IoM ecosystems. In *CEUR W.P.*, Vol. 2580.

[22] Andreas Rahmatian. 2019. Electronic money and cryptocurrencies: Suggestions for definitions. *Journal of Int. Banking Law and Reg.* 34, 2 (2019), 115–121.

[23] Philipp Sandner. 2020. Unique Referencing and Identification in the Token Universe: Cross-Chain, Worldwide, and Fork-Resilient. https://medium.com/@philippsandner/unique-referencing-and-identification-in-the-tokenuniverse-cross-chain-worldwide-and-85f7741c92d5

[24] Skalex. 2019. Making Sense of Crypto Token Types. https://www.skalex.io/crypto-token-types/

[25] Nick Szabo. 1997. Formalizing and securing relationships on public networks. *First Monday* 2, 9 (1997).

[26] Don Tapscott. 2020. *Token Taxonomy: The Need for Open-Source Standards Around Digital Assets*. Technical Report February. https://www.blockchainresearchinstitute.org/project/token-taxonomy-the-need-for-opensource-standards-around-digital-assets/

[27] TVTG. 2019. Gesetz vom 3. Oktober 2019 über Token und VT-Dienstleister Nr. 301/2019. https://www.gesetze.li/konso/2019301000

[28] Angela Walch. 2019. In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains. In *Regulating Blockchain: Techno-Social and Legal Challenges*. Oxford University Press.

[29] Kevin Werbach. 2018. Trust, but verify: Why the blockchain needs the law. *Berkeley Tech. LJ* 33 (2018), 487.

[30] Mirko Zichichi, Michele Contu, Stefano Ferretti, and Gabriele D'Angelo. 2019. LikeStarter: a Smart-contract based Social DAO for Crowdfunding. In *Proc. of the 2st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*.

[31] Mirko Zichichi, Stefano Ferretti, and Gabriele D'Angelo. 2020. A Framework based on Distributed Ledger Technologies for Data Management and Services in Intelligent Transportation Systems. *IEEE Access* (2020).