Piercing the Digital Veil
A Case Study for a DAO Legal Framework under Swiss Law

by **Benedikt Schuppli and Golnaz A. Jafari**[*]

Abstract: Blockchain technology is associated with the emergence of decentralised applications such as smart contracts and Decentralised Autonomous Organisations (DAO) as self-governing and software-based agents. The concept of a blockchain-based peer-to-peer vending machine serving both as a testing ground for the design of a marketplace for physical goods and a speculative artefact has been posited and analysed from an economic perspective by a group of scholars at the Center for Innovative Finance of the University of Basel, Switzerland. Building on this particular case study, this paper provides for a legal analysis under Swiss law. In Part A, the economic analysis of the initiative is briefly described. In Part B, the proposed concept is analysed from a de lege lata perspective, taking into account foremost liability questions both from Swiss private law (tort and contractual) and public law (criminal and tax law) perspectives, by building on literature and applicable case law. For this, the authors propose a hypothetical scenario upon which a legal analysis is applied. As a result of the analysis, a conclusion is drawn highlighting the status quo in Swiss legal framework, whereby the authors argue in favour of a possible reform for the purpose of enhancing legal certainty. In Part C, the authors then examine, from a de lege ferenda perspective, the question of whether the Swiss legislative body would require introducing a bespoke legal framework for DAOs. For this, a reference is made to relevant foreign legislation such as the State of Wyoming DAO Bill without essentially taking a comparative approach.

Keywords: Blockchain; DLT; Decentralised Autonomous Organisations; DAO; Legal Personality; Smart Contracts

Recommended citation: Benedikt Schuppli and Golnaz A. Jafari, Piercing the Digital Veil: A Case Study for a DAO Legal Framework under Swiss Law, 12 (2021) JIPITEC 331 para 1

A. Brief Introduction to the Case Study and the Underlying Technology

1 In the economic analysis of the blockchain-based peer-to-peer vending machine concept for the design of a market place for physical goods, namely ‘Blockchain Vending Machine: A Smart Contract-Based Peer-to-Peer Marketplace for Physical Goods’, the authors propose an autonomous vending machine governed by a public blockchain and smart contracts platform. Set up as a decentralisedautonomous organisation, or DAO, it is set to serve as an open marketplace for physical goods, where anyone can buy and/or sell objects.[1]

[*] Benedikt Schuppli, Attorney-at-Law, blockchain entrepreneur, member of the Coalition of Automated Legal Applications “COALA”; Golnaz A. Jafari, LL.M., doctoral researcher at Lucernaiuris, University of Lucerne, Switzerland, formerly a research associate at SOCAI, University of Würzburg, Germany, & research fellow at NRCCL, University of Oslo, Norway. Note: URL links were primarily accessed during the period of 1 November 2020 - 30 March 2021, excluding the recent related Swiss regulatory developments.

[1] F Schär, K Schuler and T Wagner, ‘Blockchain Vending Machine: A Smart Contract-Based Peer-to-Peer Marketplace for Physical Goods’ (2020) MPRA Paper Nr. 101733, 1 <https://ideas.repec.org/p/pra/mprapa/101733.html>.

I. Technical Taxonomy

2 In this section, the concepts of 'smart contracts' and 'DAOs' as decentralised applications of blockchain technology[2] are described in some detail. The authors presume that readers possess minimum knowledge as to the underlying technology itself.

1. Smart Contracts

3 The concept of smart contracts was first introduced in 1994, when Nick Szabo, an American computer scientist and cryptographer, wrote an article on contracts as computer protocols that perform independently.[3] At that time, however, computer science had not yet advanced far enough to implement Szabo's new ideas and concepts. From Szabo's point of view, the simplest version of a smart contract is a vending machine.[4] It accepts money in coins and submits goods. Szabo saw the goal of smart contracts as ensuring the fulfilment of standard terms of a contract, such as terms of payment, lien and even enforcement. Smart contracts are set to minimise deliberate, as well as unintended, deviations, and to limit the need for external, trustworthy intermediaries.[5]

4 However, the term smart contract could be misleading in that a smart contract does not constitute a contract in the legal sense *per se*. Moreover, the word *smart* does not delineate *intelligent* but is used in the electronics industry for applications that are capable of connecting, exchanging data and interacting with the user and other applications. A smart contract merely performs what the creator, usually a human, has programmed—with the premise that it does so in a reliable, immutable and deterministic way. Thus, in this paper reference is made to this term denoting digital programmes that are based on a blockchain architecture, self-execute when certain conditions occur, and are therefore in principle self-enforcing and immutable.[6]

2. DAOs

5 DAO is an acronym for decentralised autonomous organisation. The term originated amidst the nascent Ethereum[7] community in 2015. A DAO is essentially a computer software code that is distributed across a decentralised peer-to-peer network and incorporates governance and decision making rules. In other words, it is a form of an organisation that is operated through rules encoded in smart contracts. The purpose behind a DAO is to design a corporate structure that could function and perform actions independently from human hierarchical management. It can implement contractual obligations as well as business logic rules, and hence could be denoted as an *almost* autonomous, transparent and data-driven company. With a DAO, most management and administrative functions and internal processes could arguably be automated, and 'value' in a given context would be distributed among virtual stakeholders via smart contracts.

6 It is worth to emphasise that the independence to perform actions does not *by default* render independence in decision making. A DAO in the end is bound by the governance and decision making rules encoded in smart contracts by—at least for the time being—a human developer or software programmer. In particular, the terms of collaboration between different participants and stakeholders are specified in smart contracts. Once operational, decisions on a

[2] The terms "blockchain" and "distributed ledger technology", or DLT, are used interchangeably in this paper.

[3] N Szabo, 'Smart Contracts' (1994) <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/ szabo.best.vwh.net/smart.contracts.html>; N Szabo, 'The Idea of Smart Contracts' (1997) <https://archive.is/wIUOA> .

[4] N Szabo, 'Formalising and Securing Relationships on Public Networks' (1997) <https://archive.is/i65kY#selection-17.1-17.59>.

[5] Szabo (1994) (n 3).

[6] From a technical perspective, "immutability" is not an absolute feature. In blockchain or DLT space, cryptographic immutability is closely linked with the choice of algorithmic consensus mechanisms and the type blockchain or DLT systems would take, i.e. public, private, permissioned, permissionless or hybrid. See RP Dos Santos, 'Consensus Algorithms: A Matter of Complexity?' (2019) in M Swan et al. (eds) *Blockchain Economics: Implications of Distributed Ledgers* (World Scientific), 147-170. In simple terms, "immutability" refers to irreversibility, "a fundamental blockchain property that stems from the fact that transactions cannot be edited or deleted once they are successfully verified and recorded into the blockchain". See E Politou et al., 'Blockchain Mutability: Challenges and Proposed Solutions' (2019) IEEE, 5ff <https://arxiv.org/pdf/1907.07099.pdf>. See also E Landerreche and M Stevens, 'On Immutability of Blockchains' (2018) in W Prinz and P Hoschka (eds) *Proceedings of the 1st ERCIM Blockchain Workshop 2018, Reports of the European Society for Socially Embedded Technologies* <https://ir.cwi.nl/pub/28537/28537.pdf>.

[7] Ethereum is a blockchain protocol and smart contracts platform.

DAO would reach finality having passed through a designated algorithmic consensus mechanism.[8] The interaction between the members of a given DAO, who are generally represented by pseudonymous identifiers,[9] would normally take place through the medium of the underlying blockchain, in the form of an interface upon which all actions would be carried out.

7 Originally, the term 'the DAO' was used to describe a specific instantiation of such an organisation, known to be the first DAO of its kind. The DAO was created with the objective of operating as a for-profit entity, a kind of automated investment fund, which would create and hold a corpus of digital assets through the sale of 'DAO Tokens' to investors.[10] DAO Tokens were blockchain-based digital assets that would subsequently be used to fund business ventures.[11] However, in the present case study the term DAO[12] refers more generally to any blockchain-based implementation of such a decentralised autonomous organisation.

II. Case Study: The Economic Analysis in a Nutshell

8 In the economic analysis of the concept, the authors propose a basic architecture for the blockchain-based vending machine, including pricing and fee mechanisms. They also examine potential challenges arising out of the setup. The main purpose behind the physical autonomous marketplace envisaged by the authors is to address counterparty risk associated with virtual assets related to a physical object. A traditional and intermediated way to address such counterparty risk for promises of physical goods is through escrow or custody services. Imitating escrow in function, the authors posit a new type of vending machine that connects the purchase and the delivery of goods atomically via delivery-versus-payment, or DvP.[13] The processes relating to the DvP function are embedded in and executed by smart contract codes in a deterministic fashion. Residing on a *public*[14] blockchain, these contracts form a DAO that controls the vending machine.[15]

9 The basic setup in the economic analysis is described as follows:[16]

> The peer-to-peer vending machine consists of two main elements. First, the machine, i.e., the actual physical vending machine including the required software to connect to the Blockchain and translate the signals received into corresponding actions. Secondly, the DAO in the form of a dedicated smart contract structure on a public Blockchain. The former provides a physical incarnation, while the latter governs the behavior of the machine and controls the logic and conditions of the interactions. It is fully transparent, protected from unforeseen intervention, and open to anyone.
>
> Let us assume that the machine consists of a number of slots. Each slot shows a unique identifier and has a goods compartment with a transparent door that can be locked individually. It also has a display, to assist users in their interactions. The vending machine is located in

[8] See also Dos Santos (2019) (n 6), in particular, "In distributed ledgers, similarly, consensus algorithms are the process of the distributed peer-to-peer nodes in the network coming to agreement upon updated states of the ledger per executed transactions. Consensus algorithms are mechanistic and automated. As such, they provide the trustless software mechanism for the automatic execution of blockchain transactions between parties that do not need to know or trust each other".

[9] For the definition of the term "pseudonymity" under EU law, see Regulation (EU) 2016/679 (GDPR) OJ L 119, Article 4(5).

[10] See also S Polrot, 'Déploiement de The DAO, "mere de toute les dao"' (2016) <https://www.ethereum-france.com/deploiement-du-projet-the-dao-mere-de-toutes-les-dao/>; S Hassan and P de Filippi, 'Decentralised Autonomous Organisation' (2020) <https://policyreview.info/open-abstracts/decentralised-autonomous-organisation>.

[11] J Meier and B Schuppli, 'The DAO Hack and the Living Law of Blockchain' (2019) APARJUZ, 33 <https://www.ivr.uzh.ch/dam/jcr:722b55af-b0f7-40de-900f-46a526a93f80/J%20Meier,%20B%20Schuppli,%20The%20DAO%20Hack%20and%20the%20Living%20Law%20of%20Blockchain,%20APARIUZ%202019.pdf>.

[12] For more on DAO, see S Polrot, 'Les Decentralized Autonomous Organizations ("DAO"), le future des organisations collectives?' (2016) <https://www.ethereum-france.com/decentralized-autonomous-organization-dao-blockchain/>.

[13] Schär et al. (2020) (n 1), 2.

[14] Blockchain or DLT systems can take various forms, such as public, private, permissioned, permissionless, hybrid or consortium. The form a system takes has legal and technical implications, in particular regarding governance and participation protocols, as well as the identification of the participants, among other things.

[15] Schär et al. (2020) (n 1), 1.

[16] Ibid.

a public space. It is easily accessible, meaning that anyone can interact with the vending machine by assuming the role of a buyer or seller.

Buying works in the traditional way. When someone sees a good in the vending machine for which they have a buy interest at the given price, they can buy it instantly. The main difference to a regular vending machine is that instead of buying from a central counterparty, i.e., the vending machine operator, the buyer engages in a peer-to-peer transaction with someone who placed the object in the machine.

Analogously, selling via the vending machine is open to anyone, provided there is a currently unused slot. A seller simply places the goods in the compartment and provides the sales parameters, such as pricing. The machine will then initiate the sale and take over custody by locking the door. Thereafter, no further action is required of the seller, the proceeds are automatically distributed after a successful sale.

Both the buying and the selling process are governed by the DAO's smart contracts. To release goods or lock a compartment, the machine relies on events emitted by the DAO. Also, it is the source for the currently valid parameters on pricing and fees, which are detailed later on.

To increase the autonomy of the DAO, i.e., reducing the dependency on humans the smart contract structure may be designed to cover a multitude of aspects. For the basic setup, however, we propose a lean structure that focuses on the autonomous handling of the core processes of buying and selling goods through the machine, plus a governance mechanism to propose and vote on fee parameter changes or extraordinary events.

While it is possible to interact with the machine directly via smart contract function calls, a simple user interface is proposed to lower the barriers to entry for potential users with limited Blockchain and smart contract knowledge. To provide a basic user experience, the machine has a display to guide through the buying and selling process as well as a button next to each slot to unambiguously indicate which slot the interaction is targeting.

10 The authors of the economic analysis draw the conclusion that the deployment of a blockchain-based vending machine could contribute to the understanding of DAOs whilst building a bridge between digital and physical markets. The authors' proposal is deliberately limited to technical and microeconomic aspects. For a full assessment of the initiative's feasibility, a legal perspective must be added. This is because mainstream economic processes, other than the shadow economy,[17] take place in and are defined by a legal system. The argument for a legal vacuum[18] in which DAOs and blockchain networks exist, as promulgated by some proponents does not withstand further scrutiny.[19] But, as the past has shown, our continental European legal system has been caught off-guard by some of blockchain technology's inventions, and the process of understanding how the said technology could be made sense of and dealt with by our legal system is still underway.[20] In the analysis below, Swiss substantive law is considered from a *de lege lata* perspective to assess the feasibility of the proposed concept.

B. Legal Analysis

11 In this section, questions of liability are raised and put into perspective in the context of Swiss contract and tort law. Thereafter, a public law analysis with a specific emphasis on tax and criminal liability is performed. The authors outline these analyses primarily in the context of a hypothetical scenario.

12 The analyses therefore do not aim to be encompassing or complete but shall rather function as indicators in order to assess the overall readiness of the Swiss legal system, both public and private law, to deal with such a novel market and technology infrastructure. This paper shall not be a contribution to the specific legal assessment of blockchain technology or parts thereof under existing Swiss law for which plentiful publications exist, but shall rather contribute to a policy discussion on the necessity for a bespoke legal framework for DAOs.

13 In a subsequent section, authors also glance through the recent Swiss legislative developments and con-

[17] The International Monetary Fund (IMF) defines the term "shadow economy" as comprising "all economic activities that would generally be taxable were they reported to the tax authorities". <https://www.imf.org/external/pubs/ft/issues/issues30/#:~:text=the%20official%20economy.-,What%20Is%20the%20Shadow%20Economy%3F,from%20monetary%20or%20barter%20transactions>.

[18] See the term "rechtsfreier Raum" in German.

[19] Meier and Schuppli (2019) (n 11), 27.

[20] It is noteworthy that novel legislations attempting to deal with blockchain technology, including tokens, smart contracts and, in a few cases, DAOs, have been introduced in jurisdictions as diverse as Malta, Singapore, Germany, Switzerland and Liechtenstein.

clude with a brief analysis as to potential implications for the token economy of the proposed concept.

I. Hypothetical Scenario Applied to the Case Study

14 To assess whether the proposed concept can be adequately utilised given the applicable substantive Swiss law in the areas of contract, tort, tax and criminal law, we formulate a hypothetical scenario in the form of a typical transaction that could occur when making use of the blockchain-based peer-to-peer vending machine.

15 For this scenario, let us assume a DAO maintains an instantiation of the proposed vending machine, which is situated in a common use public area in the city of Zurich, Switzerland. The DAO, hereinafter referred to as 'BVM DAO', is managed by and consists of natural persons who do not know the full identity of each other, but have been coordinating and communicating on an online forum using pseudonyms in order to commission the building of the vending machine, the writing of the smart contract codes and the raising of the corresponding funds for the BVM DAO.

16 For the construction of the physical component of the concept, the BVM DAO has commissioned a construction worker in Zurich who has accepted an upfront payment in the cryptocurrency ether[21] and full payment after successful completion. The smart contract code running the vending machine is written by one of the BVM DAO members, known only by his pseudonym 'BVM Enthusiast', who normally resides—unbeknownst to the other BVM DAO members—in Albania. The BVM DAO maintains the vending machine as a marketplace for physical goods.

17 In order to become a member, a membership fee has to be sent in ether to the BVM DAO wallet. New members must be accepted via a majority vote by the existing BVM DAO members. From the membership fee, the maintenance of the BVM DAO is financed, and an insurance fund is maintained for lawsuits or fines against the BVM DAO or its members for acts committed in the capacity of the BVM DAO. Distributions from the insurance fund are subject to a funding proposal by the liable party and an acceptance by majority voting. Transaction fees earned by the BVM DAO from vendors are evenly distributed among BVM DAO members on a recurring basis. All other functions follow the proposal as described in Section A.II.

18 Slots in the vending machine maintained by the BVM DAO are rented out to vendors. A recurring text on the display of the vending machine reads as follows: by purchasing any goods the buyer accepts the BVM DAO's terms of services which can be found under bvmdaozurich.ch/terrms. As part of these terms, BVM DAO stipulates that vendors of goods in the BVM DAO are vetted for their reputation and the quality of goods sold. Furthermore, an exoneration of liability clause reads as follows: liability of the BVM DAO for any damage incurred out of the use of the BVM DAO is, as permitted by applicable law, excluded. Lastly, under the terms of service it is also reiterated that the use of the BVM DAO and these terms are governed by Swiss law, whereby the courts in London, United Kingdom, shall be exclusively competent to adjudicate any and all disputes arising out of or in connection with the use of the BVM DAO.

19 Vendor X imports and sells luxury goods in one of the slots in the BVM DAO. One such good is a Rolex Daytona.

20 Buyer Y buys a Rolex Daytona from Vendor X. He picks up the released Rolex from the vending machine after the purchase price in ether has been delivered to the smart contract and transferred to Vendor X atomically. Two weeks after the completion of the purchase, Buyer Y starts questioning whether the Rolex Daytona is an original one and whether it has been tested by a horologist. The purchased product turns out to be a counterfeit object. The certificate of authenticity, accompanied with the product, seems to have also been forged. Frustrated with this, Buyer Y seeks action and reimbursement of the purchase price he paid for the fake product. However, Vendor X, the real identity of whom is neither known to Buyer Y nor to BVM DAO, does not react to any contact attempts.

II. Private Law: Contracts & Tort Law

21 In order to assess the suitability of Swiss private law in handling transactions and interactions with the vending machine, the legal relations between involved parties would need to be described. The private law relations between the BVM DAO and Vendor X as well as the Buyer Y shall be taken into account as follows.

[21] Ether is the cryptographically generated native currency of the Ethereum platform (see n 7).

- Buyer Y – Vendor X
- Buyer Y – BVM DAO[22]
- Vendor X – BVM DAO

22 It is argued herein that Buyer Y and Vendor X are in a contractual relationship with one another as parties to a purchase contract. The mere fact that the purchase price was paid for in ether does not render it a barter contract, as ether is considered a *private* currency and therefore comparable to fiat currency as a *public* money, exclusively as to its 'means of payment' function.[23]

23 It is furthermore argued that a contractual relationship exists between Buyer Y and the BVM DAO or members of the BVM DAO collectively, given that Buyer Y's implied acceptance of BVM DAO's contractual terms is affirmed by using the vending machine.

24 The BVM DAO is in a contractual relationship with Vendor X, who rents a slot in the vending machine to sell goods. The contract is most accurately described as a lease contract.

25 For the purposes of this hypothetical scenario, the BVM DAO, in the absence of any legal personality, can most accurately be described as a partnership according to article 530 para. 1 of Swiss Code of Obligations (CO), whereby "a partnership is a contractual relationship in which two or more persons agree to combine their efforts or resources in order to achieve a common goal".[24]

26 On the discussion of whether and how smart contracts, in general, can be reconciled with Swiss contract law, in-depth analyses are offered by other, existing publications.[25]

27 Buyer Y entered into a purchase contract with Vendor X. As the purchased good, the Rolex Daytona, turned out to be fake, Buyer Y wants to receive back the purchase price or receive an original product, either from Vendor X or from the BVM DAO.

28 According to article 28 CO, "a party induced to enter into a contract by the fraud of the other party is not bound by it even if his error is fundamental". In order for article 28 CO to apply, a fraudulent behaviour would need to embed certain constituents. These include (i) fraudulent intent, (ii) illegality, (iii) a mistake in motive and (iv) causality between the fraud and the conclusion of the contract.[26] The party acting under fraud is therefore not bound by the contract. By declaring the absence of intent to the counterparty, the contract is nullified *ex tunc*, and the defrauded party may seek restitution for the damage incurred based on articles 62 et seq. CO.[27]

29 Buyer Y entered into the purchase contract with Vendor X based on the assumption that the Rolex Daytona was original, as portrayed in the title of the offer and the corresponding certificate of authenticity. Vendor X acted fraudulently with intent, and no legal justification was offered for such behaviour. Therefore, article 28 CO would apply here awarding Buyer Y to declare the contract void and to seek restitution for the purchase price as well as any additional damage caused by the fraudulent behaviour of Vendor X. Buyer Y must then declare the nullification within one year of learning about the fraud.[28]

30 In general, Swiss contract law has no fundamental difficulties in dealing with the fact that a contract

[22] Miners are not taken into account for the analysis at hand due to the slim causal nexus between their actions and potential private law issues for transaction parties. For a more conclusive overview of the potential private law relationships between the parties to a smart contract system, such as the Blockchain Vending Machine, read SD Meyer and B Schuppli, '"Smart Contracts" und deren Einordnung in das schweizerische Vertragsrecht' (2017) Recht, 204 ff, 210 <https://recht.recht.ch/de/artikel/04re0317ver/smart-contracts-und-deren-einordnung-das-schweizerische-vertragsrecht> .

[23] Meyer and Schuppli (2017) (n 22), 204 ff, 216.

[24] The distinction between a general partnership and a simple partnership is made in favour of the simple partnership, as the former requires a commercial business setup which is not assumed here for simplicity reasons.

[25] J Essebier and DA Wyss, 'From the Blockchain to Smart Contracts' (2017) Jusletter <https://jusletter.weblat.ch/juslissues/2017/889/von-der-blockchain-z_5bd3b52a43.html_ONCE&login=false>; Meyer and Schuppli (2017) (n 22), 204 ff; M Eggen, 'Chain of Contracts' (2015) AJP 26 (1), 3 ff <https://boris.unibe.ch/114476/>; A Furrer, 'Die Einbettung von Smart Contracts in das schweizerische Privatrecht' (2018) Anwaltsrevue, 103-115 <http://www.anwaltsrevue.recht.ch/arv/lpext.dll/arv/avarv18/arv0318/inharv0318?f=templates&fn=index.html&2.0&vid=10.1033/Deu>.

[26] Swiss Code of Obligations, Short Commentary on Swiss Private Law (3rd edn, Schulthess Zürich 2016), hereafter cited as CHK-Kut CO 1 N1; CHK-Kut CO 28 N3.

[27] CHK-Kut CO 31 N2.

[28] CHK-Kut CO 31 N1.

was facilitated using a smart contract,[29] even more so when a smart contract was used to hold and release the purchase price for a physical object as a one-time transaction. Given the state of the nullified contract, Buyer Y may seek restitution based on unjust enrichment on the basis of articles 62 et seq. CO. He has a right to reimbursement of the purchase price plus additional damages by Vendor X in ether or in Swiss francs, alternatively.[30]

31 Difficulties instead arise from the fact that BVM DAO allows mutually unidentified persons to enter into transactions, exchanging monetary values for goods. While the DvP part of such a transaction can be aptly handled by the DAO, the post-transaction and settlement lifecycle of a contract cannot. Thus, if Buyer Y reasonably wants to enforce any right arising out of the *consumed* purchase contract, the identity of Vendor X must be accessible to him.

32 As Vendor X is out of reach, Buyer Y may try to seek restitution from BVM DAO as the marketplace provider through which the transaction was enabled in the first place.

33 As detailed previously, BVM DAO claimed to vet Vendors. The question would then arise whether BVM DAO is liable for the damages Buyer Y incurred by trusting the information by Vendor X in light of BVM DAO's claim to vet vendors for the quality of products.

34 As a contractual relationship between Buyer Y and the simple partnership BVM DAO is now affirmed, Buyer Y is in a position to seek restitution from BVM DAO based on contractual damages,[31] specifically for the violation of contractual obligations such as the violated duty to vet Vendors.[32]

35 Buyer Y, therefore, brings claims against the simple partnership BVM DAO via the email listed on their website. As a simple partnership, every member is *jointly* and *severally* liable for the totality of the damage incurred to Buyer Y under the contract.[33] While the law once again is unambiguous here, Buyer Y does not actually have any identifying information on any BVM DAO member. As a result of long internet searches, Buyer Y learns about the true identity, name and address of the BVM Enthusiast pseudonym who resides in Albania. Buyer Y initiates a lawsuit against BVM Enthusiast as a severally liable member of BVM DAO in Zurich. Upon learning of the lawsuit, BVM Enthusiast files for legal funding from BVM DAO's member insurance fund, which is granted by a majority voting. Upon processing the lawsuit, the court called upon in Zurich makes a decision to dismiss the lawsuit without entering into the substance of the case, as the choice of forum in the terms of service on BVM DAO's website was deemed valid, and the case was not characterised as a consumer dispute, which would have established forum in Zurich according to article 32 of Swiss Civil Procedure Code (CPC), given that the product in question is a luxury good.[34] Buyer Y, frustrated with this outcome, leaves the matter be.

III. Public law

1. Tax Liability

36 The introduction of goods into Switzerland triggers value-added tax (VAT). Furthermore, the offering of the blockchain-based vending machine marketplace and the leasing of slots to vendors, which in turn sell goods to buyers, are all acts subject to Swiss VAT.[35]

37 The liable tax subject in the case of the introduction and selling of the goods to buyers is Vendor X. In the case of the maintenance of the marketplace and the charging of a lease fee, BVM DAO as a simple partnership would also be liable for VAT towards the Federal Swiss Tax Administration.

38 As for Vendor X, due to lack of information on his identity and whereabouts, the difficulties for the Federal Swiss Tax Administration to collect VAT become apparent.

[29] See, eg, the 2016 position of the Commercial Court of Zurich (HG150136 of the 16.02.2016), Recital 2.3: "Nebst individuell übermittelten Willenserklärungen sind auch solche verbindlich, welche von einem vorprogrammierten Computer automatisch abgegeben werden (sog. 'elektronischer Softwareagent')".

[30] For a more in-depth analysis of the status of ether as cash or rather, a good which is bartered, see Meyer and Schuppli (2017) (n 22), 217.

[31] If a contractual relationship is denied, tort damages could apply nonetheless. For the differentiation, see CHK-Kut CO 41 N3.

[32] CHK-Kut CO 97 N10. It is assumed here that other prerequisites, such as damage and causality, are met, too.

[33] CHK-Kut CO 530 V.

[34] See Swiss Federal Court Decision BGer 4A_2/2018 for a similar case. <https://www.bger.ch/ext/eurospider/live/fr/php/aza/http/index.php?highlight_docid=aza%3A%2F%2F22-03-2018-4A_2-2018&lang=fr&type=show_document&zoom=YES&>.

[35] Swiss VAT Act SR 641.2 Federal Act of 12 June 2009 on Value Added Tax, article 21 *e contrario*. <https://www.fedlex.admin.ch/eli/cc/2009/615/de>.

39 As for BVM DAO, the simple partnership where individual members are *jointly* and *severally* liable towards the tax authorities, the case becomes more nuanced.

40 However, given the difficulties of pinning down BVM DAO as an incorporated organisation, as its comprising members are acting with pseudonyms and are spread across Europe, the Swiss Federal Tax Administration will face hindrance collecting VAT from them. In case one member is identified, though, tax liabilities towards the Federal Swiss Tax Administration can be funded via the BVM DAO insurance fund. This will create a moral hazard not to pay VAT before an individual BVM DAO member would be prosecuted for it, which is reminiscent of Planka.nu in Sweden. Here, the case concerns notoriously funded members' penalties via a common insurance fund when they were caught fare-dodging in public transport.[36]

41 In either case, the obscure nature of BVM DAO's individual members, as well as the vendors, would impose enforcement costs on tax authorities while generating loss for them. Furthermore, consumers who are VAT-payers of last resort may still end up paying for uncollected VAT as VAT for which vendors and suppliers are liable is usually priced into end consumer prices.

2. Criminal Liability

42 Let us assume that by importing a counterfeit good, introducing it into the Swiss market and selling it to Buyer Y, Vendor X has fulfilled all the hallmarks of, *inter alia*, criminal offences, fraud according to article 146 of Swiss Civil Code (CC) and counterfeiting of goods according to article 155 CC.

43 In order to prosecute Vendor X for the criminal offences committed, Swiss law enforcement would need to be privy to information about his identity and/or whereabouts. Let us further assume that no such information is accessible to the prosecutors, leaving them only able to investigate accessory criminal liability by BVM DAO. For this, individual BVM DAO members could be held liable in the first degree, and BVM DAO as an organisation would be subject to secondary liability according to article 102 CC.[37]

44 In order for an offender to be held criminally liable under Swiss criminal law, his or her actions—or omissions in the case of a duty of care for inalienable rights of others—must have been causal for the outcome of the offence. To prevent an uncontrollable sprawl of causal relations, legal doctrine has added the prerequisite element of the adequacy of the said causal relation. According to the Swiss Federal Court, the adequate causal connection is to be affirmed if "a behaviour was suitable, after the usual course of things and the experiences of life, to bring about or at least to favour the kind of outcome of the criminal offence as the one that has occurred".[38]

45 While one could argue that a single BMV DAO member's omission to vet Vendor X and the sold goods properly is suitable to favour the outcome of both the fraud and the counterfeiting of goods offences, and therefore fulfilling the requirement of causality, wilful criminal intent is also required for one to be criminally liable as an abettor or an accomplice under either article 146 CC or article 155 CC. Negligent behaviour alone, as it may suffice to establish the kinds of contractual claims against BVM DAO, does not surmount to wilful intent. Correspondingly, wilfulness based on article 12 para 2. CC by knowingly accepting the realisation of the act, the fraud or the introduction of counterfeiting goods as possible, or *dolus eventualis*, is difficult to establish here. This is due to the fact that Vendor X, although not being thoroughly vetted by BVM DAO, has accompanied the Rolex Daytona with a certificate of authenticity. In addition, expecting BVM DAO to verify the said certificate or the product itself with a horologist in order to forego criminal liability would be a stretch.

46 If accessory criminal liability, under articles 146 or 155 CC, of a BVM DAO member were nonetheless established without it being clear who the member was or which member fulfilled in his or her own right all the required hallmarks, BVM DAO could be criminally liable under article 102 CC and therefore be subject to a fine. The make-up of BVM DAO as a pseudonymous group where the identity of members is *deliberately* kept secret and shielded from public view is prone to be deemed "organisationally

[36] See <https://planka.nu/om-plankanu/>.

[37] See the term "Ersatzhaftung" in German; Swiss Federal Court Decision BGE 142 IV 133, E. 4.1 <http://relevancy.bger.ch/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F142-IV-333%3Ade&lang=de&type=show_document#:~:text=102%20StGB%20ist%20Voraussetzung%20f%C3%BCr,%C3%A4usseren%20Grund%20f%C3%BCr%20die%20Strafbarkeit>.

[38] Swiss Federal Court Decision E. 4.1.3, translated from German into English by the authors <https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?highlight_docid=atf%3A%2F%2F138-IV-57%3Ade&lang=de&zoom=&type=show_document>.

defective" and, as such, causal to the inability of the prosecutors to hold one single BVM DAO member criminally liable.[39]

47 However, given the difficulties of pinning down BVM DAO as an organisation, as its comprising members are acting via pseudonyms and are spread across Europe, prosecutors will experience difficulties enforcing the law against them. If the fine for the violation of, e.g., article 155 CC in connection with article 102 CC would be too high, a moral hazard is created to abandon the vending machine and the local jurisdiction, Switzerland, entirely and to set up an alternative BVM DAO elsewhere. If the fine is too low, and it can be paid for with the insurance funds in the BVM DAO wallet, another moral hazard is created to continue to allow criminal behaviour on the BVM DAO marketplace.

IV. Implications of Swiss Regulatory Developments

48 The scope of the present legal analysis clearly excludes the token[40] ecosystem[41] and economic aspects related to the proposed concept.[42] Nevertheless, given the ongoing regulatory and legislative reforms in Switzerland, the authors take the view that these will have implications over the intended token design, in particular when due account is given to its *substance* over its *form*.

49 Currently Switzerland is in the process of reforming existing laws in order to accommodate blockchain systems and to address Decentralised Finance (DeFi) applications. The Federal Act on the Adaptation of Federal Law to Developments in DLT, has already received parliamentary approval, has been implemented partially and is expected to enter fully in force later this year.[43] This Act introduces a number of changes permitting the development of decentralised governance in systems that are aimed at financial transactions.[44] In other words, the reform is set to permit the exchange of asset tokens, among others, as uncertificated securities. This specific category of tokenised rights,[45] defined as uncertificated register securities,[46] and the legal transfer thereof, concerns any right that can effectively be securitised.

50 Under Swiss law,[47] securities in general are certificated or uncertificated securities, derivatives or intermediated securities, which are standardised and suitable for mass trading.[48] Outside of this traditional definition, questions would arise as to whether stan-

[39] BGE 142 IV 133, E. 3.1 (n 37).

[40] In a technical sense, a "token" stands for a sequence of characters that serves as an identifier for a specific asset, eg, usage rights, participation rights or cryptographically generated currency models such as bitcoin, among others; see A Sunyaev et al., 'Token Economy' (2021) <https://link.springer.com/content/pdf/10.1007/s12599-021-00684-1.pdf>. A token is also a " a digital representation of value on a shared distributed ledger that is owned and secured using cryptography to ensure its authenticity and prevent modification or tampering without the owner's consent". See International Telecommunication Unit (ITU), Technical Specification FG DLT D1.1 (2019), 6 <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>.

[41] ITU (2019) (n 40), 6; a "token ecosystem" stands for "a digital system or digital space where participants and users interact and coordinate with each other using tokens".

[42] Schär et al. (2020) (n1).

[43] Swiss DLT Framework, parliamentary approval (September 2020) <https://www.admin.ch/opc/fr/federal-gazette/2020/7559.pdf>. Note: The amendments to the Swiss Code of Obligations (CO), the Federal Intermediated Securities Act and the Federal Act on International Private Law that are envisaged in the DLT bill have now entered into force from 1 February 2021. These provisions enable the introduction of ledger-based (blockchain-based) securities that are represented in a blockchain or DLT system. The remaining provisions of the DLT bill are foreseen to enter into force on 1 August 2021.

[44] The Swiss Federal DLT Act has amended/is set to amend specific laws such as the Code of Obligations (CO), the Banking Act (BankA), the Financial Market Infrastructure Act (FMIA), the Bankruptcy and Insolvency Act (BIA), and the Federal Act on Intermediated Securities (FISA).

[45] Swiss Code of Obligations (CO), see Articles 973d – 973i.

[46] See the term "Registerwertrechte"; "[U]ncertificated register securities have features largely analogous to traditional certificated securities. Any right that can be securitised also qualifies as an underlying right for uncertificated register securities, including asset tokens and utility tokens" in CMS Law –Now, 'The new Swiss blockchain/DLT laws have been finalised and presumably entre into force early 2021' (15 October 2020) <https://cms.law/en/che/blogs/law-now-blog/the-new-swiss-blockchain-dlt-laws-have-been-finalised-and-presumably-enter-into-force-early-2021>.

[47] Financial Market Infrastructure Act (FMIA) (19 June 2015), Article 2(b); see also Financial Services Act (FinSA) (15 June 2018), Article 3(b).

[48] For the term 'standardised and mass trading' see: "the instruments are offered for sale publicly in the same structure and denomination, or that they are placed with 20 or more clients under identical conditions" in Financial Market Infrastructure Ordinance (FMIO) (20 November 2015), Article 2.1.

dardised elements such as voting rights could also qualify as securities. It is apparent that definition of a given digital asset in the form of a token as a security would fall outside both certificated and intermediated securities categories, whereby only uncertificated securities and derivatives would serve relevance. Under uncertificated securities category, Swiss law defines three types of rights, such as participation rights,[49] property rights and credits. Traditionally, the only formal requirement[50] for creation of these securities is by keeping a book in which associated details are recorded. With the recent reforms, such a book (or register) can now be created on a blockchain system.

51 On the other hand, a general distinction is made between three token models, e.g. payment tokens, utility tokens and asset tokens.[51] Asset tokens refer to and represent physical assets, company equity, debt and rights such as dividends and interest payments. In their classification, the Swiss Financial Market Supervisory Authority (FINMA) also emphasises on *substance* over *form* of a given design. Essentially, asset tokens are seen analogous to equities, bonds and derivatives, from the perspective of their economic function. An asset token can take the form of a promise, e.g. in future capital flows.

52 For applicability of Swiss financial market and securities laws, an assessment would need to be made as to whether a token would confer claims or rights, such as ownership, in favour of the holder against its issuer or a third party. In addition, the type of the underlying asset referred to by a token, i.e. fiat currency, commodity, real estate or securities, carries importance.[52]

53 Furthermore, for tax purposes in Switzerland, asset tokens are often classified in distinct groups of debt tokens, equity tokens and participation tokens.[53] Concerning equity tokens, an investor's entitlement would refer to a benefit, measured by a certain ratio to profit or liquidation result. In the case of participation tokens, on the other hand, investors would generally be entitled to a proportional share of a certain reference value defined by the issuer. Both equity tokens and participation tokens would be considered as derivative financial instruments in the context of taxation.

54 In the economic analysis of the proposed concept, it is suggested that tradable participation tokens are issued which "entail the right to vote on governance proposals and participate in future cash flows".[54] In order to foster user adoption the vending machine would also distribute "micro participation rights to sellers and buyers through fractions of tokens".[55] Here, "token holders could create proposals and cast votes in proportion to their token holdings," whereby "a combination of cash flows and voting rights in the same token" is argued to "help align interests and incentivise token holders to act in the machine's best interest".[56]

55 In addition, "the right to open a slot in the vending machine is tokenised in the form of a non-fungible token (NFT)",[57] whereby the vending machine would assume a custodian role, with the NFTs bearing redemption rights in favour of the assets placed in the slots. The NFTs are therefore seen to become tradable without the need for the physical displacement of the asset. Crucially, the vending machine is depicted as a "programmable safe deposit box with a large variety of use cases including collateralised loans, smart contract-based implementations of a last will and the issuance of sub-tokens which represent partial ownership of the NFT".[58]

[49] Participation rights could either bear financial value or not. In cases where participation rights bear financial value, these are qualified as securities.

[50] See n45, Article 973c.3.

[51] Financial Market Supervisory Authority (FINMA), 'Guidelines for Enquiries Regarding the Regulatory Framework for ICOs' (February 2018) <https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en>.

[52] FINMA, 'Supplement to the Guidelines' (September 2019), 1-4 <https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf?la=en>.

[53] Swiss Federal Tax Administration (SFTA) Working Paper (2019) <https://www.estv.admin.ch/estv/de/home/direkte-bundessteuer/direkte-bundessteuer/fachinformationen/kryptowaehrungen.html>. See also O Favre et al., 'The Virtual Currency Regulation Review: Switzerland' (Schellenberg Wittmer, 2020) <https://thelawreviews.co.uk/title/the-virtual-currency-regulation-review/switzerland>.

[54] Schär et al. (2020) (n 1), 6f.

[55] Ibid.

[56] Ibid 7.

[57] Ibid. Note that non-fungible tokens, or NFTs, are blockchain-based assets with unique identification codes designed so that they are not equal and cannot be replicated. These are distinguished from fungible tokens that are substitutable or exchangeable for similar items.

[58] Ibid.

56 The proposed design as a participation token could arguably be interpreted as an asset token under FINMA definitions, bearing a derivative character. In other words, these participation tokens could then be considered as uncertificated register securities, whereby the transfer of these types of securities that are exclusively registered on a blockchain system is now permitted under Swiss law.

57 Notably, a form of security under Swiss law, when defined as a derivative or a financial contract, is where the price is set particularly according to a) assets such as shares, bonds, commodities etc., and b) reference values such as currencies, interest rates etc.[59] Also, derivatives are defined as financial contracts whose value depends on one or several underlying assets and which are not cash transactions.[60] These definitions clearly imply that a derivative would require bearing a *price*, which is set according to an underlying asset.

58 The participation tokens in the proposed concept would in principle only assume functionality by means of the underlying (implied) right to claim assets, such as participation in future cash flows and the right to vote on governance of the architecture. These tokens would form the effective embodiment of an uncertificated register security, issued by and subjected exclusively to the rules of the underlying network governed by BVM DAO. In other words, the derivative element would relate to the way value is constituted on the basis of the subject matter. Therefore, these participation tokens seem to bear a *price* given that investors are set to align their interests and to expect profit from the functioning of the vending machine.

59 Once caught under the uncertificated register security, where the electronic register will exclusively be integrated on blockchain systems, a contractual relationship would then need to be established in the form of a registration agreement between the issuer and the holder. Here identification of parties becomes pivotal, with the register potentially taking the role of 'data controller' under the Swiss data protection regime.[61] For the participation tokens to work on such a blockchain-based register, the identity of the holder at each point in time as well as the issuer, who is the obligor of the securitised rights, must be unambiguous at all times. In light of the challenges reflected in the sections above, this aspect furthers the difficulty of embedding an unincorporated DAO structure with pseudonymous members into the legal and financial system.

60 Furthermore, in the proposed tradable NFT as a tokenised right to open a slot on the machine, the latter will act as a trusted custodian of the physical goods aimed at guaranteeing an effective bridge between the on-chain and off-chain spaces. NFTs in general are not considered as securities. Here, NFTs represent deposited assets, i.e. physical goods held in custody by the vending machine. These cannot be considered as standardised within the meaning of a security, discussed above. In this context, the proposed concept also refers to the possibility of the "issuance of sub-tokens which represent partial ownership of the NFT".[62] Division of the NFT into *identical* sub-tokens representing partial ownership, could be argued to constitute a standardised asset, provided that the number of these sub-tokens is higher than 20.[63] The sub-token holders would then be entitled to the right on the partial value represented by these tokens. These tokens could therefore be seen as derivatives, and consequently as securities.

61 Lastly, the assigned role of custodianship to the vending machine which may also act as a "programmable deposit box," would inevitably have implications as to matters related to liability.

V. Concluding Remarks

62 The analysis conducted in the preceding sections highlight that the current Swiss legal framework, both from a private and public law perspective, wrestles with the concept of an autonomously managed and largely pseudonymous marketplace. In addition, authors take the view that the recent regulatory reforms would certainly have an impact on the chosen token design, albeit outside the scope of this study.

63 Law primarily surrounds legal subjects, be it natural or legal persons, and confers rights and obligations to and in relation to them. With the proposed architecture as a blockchain-based peer-to-peer vending machine governed by a DAO, such legal subject is either entirely absent, as shown in the case of tax law, or it is hard to get a hold of, as shown in the section on private law analysis. Furthermore, from a criminal law perspective, establishing the required adequate causal link and wilfulness between the BVM

[59] Financial Market Infrastructure Ordinance (FMIO) (25 November 2015), Art. 2.2 (a)(b).

[60] Financial Market Infrastructure Act (FMIA), Article 2(c).

[61] The new Swiss Data Protection Act (revised FADP) was adopted by the Parliament in September 2020 and is expected to come into force by 2022 <https://www.fedlex.admin.ch/eli/fga/2020/1998/de>.

[62] See Schär et al. (2020) (n 1), 7.

[63] See n 48.

DAO's actions and the damage caused to the victim seems unrealistic in light of the high threshold Swiss legal doctrine has rightfully levied for criminal liability, specifically for omissions in case of a duty of care.

64 From a private law perspective, the fact that contracting parties have little to no factual recourse in case of a purchase of counterfeit goods is an undesirable state from a public policy perspective, as neither consumer protection, in the wider sense, not within the meaning of article 32 CPC, nor good faith in commercial dealings as a public policy interest, is viably upheld in this scenario.[64]

65 From a public law perspective, on the other hand, the state faces insurmountable challenges in taxing and collecting the taxable transactions involving such architecture. Also, perpetrators of criminal offences, i.e., members of a DAO or unidentifiable associates of a DAO, such as Vendor X, could likely not be brought to justice—an outcome which directly infringes on the public good of legal protection and undermines trust in government.[65]

66 As shown above, with the existing Swiss legal framework, undue burdens are inflicted on market participants interacting with the vending machine on the one hand, and the state as the responsible authority to levy taxes and to prosecute crimes on the other hand. The afore-mentioned undesired results of Swiss private and public law in dealing with the described case study suggests that the existing Swiss legal framework is not adequate, which is why pillars for a new and more adequate framework are discussed below.

C. Policy Agenda

67 As identified in part B, Swiss substantive law currently does not offer a satisfactory framework to deal with novel decentralised market infrastructures such as the one proposed by Schär et al. Individuals interacting with the proposed infrastructure, be it as vendors, buyers or members of the BVM DAO, would face uncertainty related to both private and public law enforcement. Thus, the overall functioning of the legal economy and the rule of law would be infringed upon.

68 The novelty of a DAO such as the BVM DAO that creates these challenges for existing legal tools lies in the propensity for DAO transactions to take place cross-border, between unknown or pseudonymous parties and to be immutable in principle by virtue of the underlying technology. While the concept of enabling untrusted and unidentified parties to transact with one another is appealing from an economic perspective as transaction costs associated with search and counterparty risks can be significantly reduced, both public and private law grapple with it. Law is built upon legal subjects who must be identifiable and known. Furthermore, legal relations such as contracts may span years, in some cases decades, and the law must have tools at its avail to deal with changes in intent or circumstances etc., whereas a smart contract facilitating a single transaction would by default not cater to the dynamic nature of such legal relations.

69 Merely having a DAO register as an existing corporate form, e.g., as a limited liability company (LLC), as has been promulgated by initiatives such as LexDAO,[66] may not adequately tackle the challenges related to DAOs as discussed above. In order to effectively ensure accountability of actors behind a DAO, both human and non-human, such as a form of artificial intelligence, or AI, a "piercing of the digital veil" of sorts, a more in-depth analysis of the nature of DAOs as borderless, fluid and, to some extent, trustless is required.

70 Hence, in our opinion, the *numerus clausus* of corporate and institutional forms under Swiss law does not encompass a solution for the requirements that new blockchain-based organisations, e.g., DAOs, impose. Due to the proliferation of DAOs as novel organisational forms, both participants in these organisations, as well as external persons or stakeholders, such as the market, consumers, and the state itself, have an interest in legal certainty when dealing with them. Next to the creation of new forms of corporations based on blockchain and thus extending the *numerus clausus* of corporate forms, the creation of digital persons as a separate category of legal personality should also be taken into account which would draw implications on the Swiss CC itself, not merely the Swiss CO where corporate forms are regulated. When Swiss legislators created a novel framework for blockchain-based securities, as discussed earlier, for which the amendments to Swiss CO, among others, have recently taken effect,[67] the opportunity to tackle the issue raised herein was missed. Nonetheless, the Swiss Legal Tech

[64] P Tschannen, U Zimmer and M Müller, *Allgemeines Verwaltungsrecht* 3 (Aufl. Bern 2009), 489 et seq., 494.

[65] On the correlation between trust in institutions and crime, see L Blanco and I Ruiz, 'The Impact of Crime and Insecurity on Trust in Democracy and Institutions' (2013) The American Economic Review 103 (3), 284–288 <www.jstor.org/stable/23469744>.

[66] See <https://lexdao.org/#/>.

[67] See n 43.

Association advocated for creating a legal framework for DAOs in the process of public consultation leading to the Swiss legislative reform.[68]

71 Therefore, we argue, the legal framework under Swiss substantive law must be amended to deal with the unsatisfactory situation the novel organisational form of DAOs leaves us with. In the words of Max Ganado et al. the task is one of revolutionary proportions:

72 As a practical matter, the collaborative, distributed, and potentially anonymous processes used to create and deploy these code-based governance algorithms have the distinct potential to create an accountability gap between the designers of a DAO and the outcomes of that DAO. All of these points underscore the need to modernize the guardrails of legal personality to accommodate or catch up with the technological revolution of the last decade.[69]

73 In order to achieve this task, Swiss legislators must consider a number of pitfalls to ensure the sensibility of the framework. Of these, the most prominent ones are described, and ways to deal with them are proposed below.

I. Expand Numerus Clausus or Introduce a New Form of Personhood

74 The first question is whether to address the identified challenges by expanding the *numerus clausus* of corporate and organisational forms to include a special DAO form (Approach 1). Alternatively, instead of legislating for a specific technology, to expand the concept of legal personality as a whole to comprise self-executing software-based agents, among others, DAOs, just as legal scholars have expanded the envelope of legal personality to encompass legal persons, centuries ago (Approach 2).

75 Approach 1 was chosen by the State of Vermont in an effort to create a legal framework for DAOs. As a practical matter, the Vermont legislator determined that the autonomous quality of DAOs merited greater safeguards than those of a traditional business entity. Vermont has explicitly accounted for the extension of the *numerus clausus* of corporate forms through the creation of a new entity type, namely blockchain-based limited liability companies (BBLLCs).[70]

76 This solution is seemingly suitable to deal with the regulatory challenges DAOs pose today, as they are by and large managed by humans, whereby the extent to which DAOs are actually governed 'algorithmically,' as suggested,[71] is contested. As such they are different from other non-code-based organisations such as stock corporations in degree, but not in kind. Therefore, introducing a new form of corporation taking into account some of DAOs idiosyncrasies would be a viable medium-term solution.

77 However, at the speed with which AI's capabilities are increasing,[72] Approach 1 may become ineffective and obsolete sooner than one may think.

78 A midway approach, Approach 2, was chosen by the State of Wyoming legislators for the DAO Bill.[73] In recognising the speed at which AI is developing, the Wyoming DAO Bill introduces the concept of an 'algorithmically managed' DAO to deal with the challenge that future, non-human DAOs may pose without touching on the subject of legal personhood for digital software-based agents *per se*. Instead, under this framework non-human DAOs could be legally incorporated. More specifically, it is stipulated[74] that an algorithmically managed decentralised autonomous organisation may only form if the underlying smart contracts are able to be updated, modified or otherwise upgraded.

79 The distinction between algorithmically managed DAOs and non-algorithmically managed DAOs, i.e. 'member-managed', may seem prudent in light of future potencies of AI. However, vesting management powers to a smart contract in the case of 'algorithmically managed' DAOs may prove to be rather problematic in a legal sense. This is because the pseudonymity, or, on rare occasions, the anonymity,

[68] Swiss Legal Tech Association, Public Consultation Submission for the Legal DLT Framework, 23 <https://www.swiss-legaltech.ch/wpcontent/uploads/2019/06/SLTA_Vernehmlassungseingabe_Version_final_20190624.pdf>.

[69] M Ganado et al., 'Mapping the Future of Legal Personality' (2020) MIT Computational Law Report, 2 <https://law.mit.edu/pub/mappingthefutureoflegalpersonality/release/1>.

[70] Ibid. See also Vermont Statute on the Blockchain-based Limited Liability Companies, 11 V.S.A. ss 4173<https://legislature.vermont.gov/statutes/section/11/025/04173> and <https://law.mit.edu/pub/mappingthefutureoflegalpersonality/release/1>.

[71] Ganado et al. (2020) (n 69).

[72] See GPT-3 <https://openai.com/blog/openai-api/>.

[73] Wyoming Senate Bill 38, SF0038 Decentralized Autonomous Organizations <https://www.wyoleg.gov/Legislation/2021/SF0038#-408>. Note: the Bill has passed the Wyoming Senate Committee in March 2021.

[74] Ibid 17-31-105. (d).

associated with smart contracts in the case of these DAOs would take away the necessary 'safety valve' and could therefore prove not to be sensible from a public policy perspective. Furthermore, the term 'algorithmically managed' is not precise enough and may thus be misleading as many gradations exist on the spectrum of human – AI interaction to which the bifurcated solution in the Wyoming DAO Bill does not cater. Also, algorithms can be found in any process, the law, chemistry or even a recipe. Therefore, building a legal framework around such polysemantic term is far from ideal.

80 Approach 2 is evidently more radical in nature, as it would introduce a new form of personhood as a whole by recognising digital persons next to natural persons and personhood for legal entities, and in some cases, nature bodies such as rivers.[75]

81 If we go back to the origins of legal personhood, it was the great jurist Karl Friedrich von Savigny, influenced by Kant's considerations on legal capacity in metaphysics of morals, who stated that legal capacity could be expanded to encompass something without the single individual, i.e., by artificially construing a legal person. Here, Savigny proposed that legal capacity shall be expanded to artificial subjects, conceived solely via the power of fiction. This subject was called a "legal person", i.e., a person who is assumed to exist exclusively for legal reasons. Thus, according to Savigny, a legal person is an artificially conceived subject capable of owning property.[76]

82 As of today, courts around the world have ruled on the limitations of rights awarded to legal persons and concluded that legal persons are not only capable of owning property but also capable of personality rights such as the right to a reputation and constitutional rights such as freedom of speech.[77]

83 According to article 53 CC, "legal entities have all the rights and duties other than those which presuppose intrinsically human attributes, as gender, age or kinship tributes, as gender, age or kinship, speech".

84 Consequently, a self-executing digital entity such as a DAO could presumably be awarded legal personality with its algorithmic governance and execution of actions, given that it is arguably more self-reliant and is endowed with more agency than, e.g., a stock corporation which needs human agents for every step of the way when forming, communicating and executing decisions and actions. This is highlighted in the essay 'The Advent of Digital Persons' with a concrete example of a highly autonomous DAO:

> In the near-term future, we will face digital entities who act autonomously on a transnational, distributed network and don't always need a physical manifestation or representation to interact with natural or legal persons. They will manage funds, pay humans for labour, possess things and create other entities – independently of third-party involvement. We propose to accept these entities as autonomous, digital persons as they are endowed with no lesser level of autonomy than the legal persons we interact with on a daily basis. A legal entity relies on its organs comprised of humans, such as a board of directors, presidents, secretaries etc. to act as agents in the process of decision-making, and in the execution of these decisions on its behalf. Legal entities are therefore not autonomous agents. It is precisely the characteristic of agency in form of self-execution without the interference or need of a third party that gives digital entities the necessary level of autonomy to be regarded as digital persons. This does not mean that a digital person must be able to execute its will exclusively without a human being or another party. Especially in the analogue realm, a digital person would still need representation through a human surrogate. But given the current technological developments, the digital person can now act directly without human intermediation in e.g. employing humans and paying their salaries through smart contracts as well as autonomously managing its assets, including transactions of programmable funds.
>
> Such is the case with Plantoids: Plantoids are blockchain-based lifeforms that reproduce through the combination of code and human interaction. The goal of a given Plantoid is to raise enough funds to be able to employ a human surrogate that then would produce the Plantoid's offspring. In the example of the Plantoid, technology no longer acts as a tool but as a peer in a direct relationship with natural or legal persons. Similar to a natural person whose mind inhabits a body, each Plantoid consists of comparable components. On the one hand, its physical body in form of an electro-mechanical construction and on the other hand its "soul" – "represented by an autonomous software agent that lives on a blockchain". If the physical body of

[75] O Polat and B Schuppli, 'The Advent of Digital Persons' (2018) Future Cryptoeconomics, Vienna, 37 et seq. <https://riat.at/future-cryptoeconomics/>. An insightful analysis of the topic of digital personhood is delivered in G Teubner, 'Digital Personhood? The Status of Autonomous Software Agents in Private Law' (2018) <https://ssrn.com/abstract=3177096>.

[76] KF von Savigny, *System des heutigen Römischen Rechts* (1840), 236.

[77] Citizens United v. Federal Election Commission, 558 US 310 (2010).

the Plantoid is destroyed, the autonomous software agent – in the form of a smart contract – continues to live on the distributed network it was deployed on.[78]

85 From this excerpt it can be concluded that the more non-human agency in the form of AI underlies a DAO, the more adequate Approach 2 may prove to be in legislating for DAOs.

II. National Solution to a Borderless Challenge

86 No matter how intricate a legal framework for DAOs is created by any jurisdiction, the effectiveness of such approach would largely be determined by the legal standards in other jurisdictions. Therefore, unitary national or state-level approaches, such as Wyoming and Vermont, are welcomed but a worldwide uniform and standardised solution which would uphold a minimum liability standard and a framework for international cooperation, exchange of information and cross-border enforcement would be needed to tackle the issue effectively. Lessons can be drawn from effective international legal frameworks such as e.g., in the area of money laundering and terrorism financing, as pioneered by the Financial Action Task Force (FATF), an ad hoc membership body organised under the umbrella of the Organisation for Economic Cooperation and Development (OECD). To this end, civil society groups consisting of leading academics, such as the Coalition of Automated Legal Applications, are working on Model Laws, a helpful tool to set legal standards.[79]

87 Therefore, the paper takes the view that any legislative attempt for Switzerland ought to closely monitor and adequately reflect the research and findings from other legislative attempts around the world.

III. Technical Tools to Increase Accountability

88 If we revisit the damage incurred to Buyer Y as well as the state as collector of taxes in part B, it was exclusively pecuniary in nature. This will be the case for most of the challenging cases we can currently conceive of in relation to DAOs which prompt the need for a novel legislative framework in the first place. Therefore, finding a sensible solution to make damaged parties financially whole when the interaction with a DAO has led to damages for which the DAO must then assume responsibility would be of utmost importance.

89 Just as contract law without the tools for international seizure of assets and enforcement of claims would be useless, even the most intricate legal framework for DAOs would be ineffective in the absence of any tools to seize and distribute assets to damaged parties. Hence, we argue, a legal framework for DAOs must include some form of collateral or minimum insurance requirement for DAOs before they may interact with market participants under an effective protection of a legal framework. With this, the characteristics of smart contracts as deterministic and immutable sets of codes can be used to favour consumers and other market participants who are in need of protection.

90 Even beyond a mere collateral requirement, allowing the state some kind of access to smart contracts, via for instance multi-signature function, where the state holds one of the needed cryptographic keys to transfer assets, governing DAOs may—albeit counter to the libertarian cypherpunk ideal—also be a suitable safeguard to ensure protection of market participants when transacting with DAOs.

IV. Concluding Remarks

91 Irrespective of the approach potentially chosen by Swiss legislators, Approaches 1 or 2, it is our opinion that the likes of the Wyoming DAO Bill, despite their apparent shortcomings, could inspire Switzerland to bring further legal certainty to such emerging novel business models and to better integrate existing concepts such as 'unincorporated partnerships' into its legal and regulatory landscape, thereby helping to achieve a fitting framework for these new business and organisation models, which are here to stay, according to our estimation.

92 To sum up, for any legislative effort, it is crucial that participants in the proposed open marketplace concept by Schär et al. are not left without effective legal recourse. To meet this requirement, we take the view that Swiss legislators need to act with bespoke legislative reform, partially taking account of existing legislation in foreign jurisdictions.

93 In the end, the fundamental need for a functioning legal system of knowing "who are you, with whom

[78] Polat and Schuppli (2018) (n 75), 37 et seq. For the Plantoid concept art by P de Filippi, see <https://www.forbes.com/sites/katmustatea/2018/01/31/meet-plantoid-blockchain-art-with-a-life-of-its-own/?sh=b754ceb3f641>.

[79] Coalition of Automated Legal Applications, the DAO Model Law, (MEDIUM, 18 December 2019) <https://medium.com/coala/the-dao-model-law-68e5360971ea>.

I have to deal with”, to put it in the words of Jeremy Bentham, must be catered to in any sensible legislative approach to tackle the issues and challenges raised herein, even with technical tools such as smart contracts at hand. Otherwise, individuals or non-human entities may escape regulatory supervision and legal accountability, a result which may erode trust and legitimacy in the state power as a whole.

Security Implications of Consortium Blockchains: The Case of Ethereum Networks

by **Adrian Hofmann, Fabian Gwinner, Axel Winkelmann and Christian Janiesch**[*]

Abstract: By definition, blockchain platforms offer secure and reliable data exchange between stakeholders without a trusted third party. Private and consortium blockchains implement access restrictions, so that sensitive data is kept from the public. However, due to its distributed structure, only one node with faulty configuration can leak all blockchain data. For our study, we scanned the Internet for misconfigured private Ethereum nodes. Overall, we found 1421 nodes belonging to 621 blockchains that are not one of the large Ethereum-based networks. For our analysis, we chose a diverse sample of networks. Then, we analyzed in-depth 4 different networks with 10 to 20 nodes enabling 800 to over 34 million transactions. We used the exposed remote procedure call interface of nodes to extract the complete transaction history and to gain insights into the actors' behaviors those networks. We used graph visualization tools to picture the networks transactions and to identify stakeholders and activities. Additionally, we decompiled and reverse engineered smart contracts on the networks to infer the purpose of smart contracts, the network, and its participants' roles. With our research, we show how to reveal confidential information from blockchains, which should not be exposed to the public and could potentially include identities, contract data as well as legal data. Thereby, we illustrate the legal and social implications of data leakage by this distributed and supposedly secure technology. In summary, we show that the large attack surface of private or consortium blockchains poses a threat to the security of those networks. The nodes used in this study were not configured according to the Ethereum guidelines and exposed information directly to the Internet. However, even correctly configured nodes provide an excellent target for attackers as they allow them to gain information about a whole network while only breaching one weak point. Lastly, our study discusses whether (private) blockchain networks can reach a consensus without sharing all data between nodes and what data distribution strategies defend best against weak links in the chain.

Keywords: Consortium Blockchain; Privacy; Security; Ethereum; Case Study

Recommended citation: Adrian Hofmann, Fabian Gwinner, Axel Winkelmann and Christian Janiesch, Security Implications of Consortium Blockchains: The Case of Ethereum Networks, 12 (2021) JIPITEC 347 para 1

A. Introduction

1 Blockchain technology has sparked interest in a variety of industries. Even after the initial Bitcoin hype, blockchain as a technology is still regarded to have the potential to drive decentralization and disintermediation. The cryptographic primitives and consensus mechanisms make storing and transferring of data not only secure and resistant against manipulation but also not reliant on a trusted third party.[1] Consequently, many consider the potential of this technology immense and disruptive.

[*] Adrian Hofmann, Fabian Gwinner, Axel Winkelmann, University of Würzburg, Chair of Business Management and Information System, Christian Janiesch, TU Dortmund University, Chair for Enterprise Computing.

[1] Satoshi Nakamoto, 'A Peer-to-Peer Electronic Cash System' <https://bitcoin.org/bitcoin.pdf> accessed 22 January 2021; Sarah Underwood, 'Blockchain beyond Bitcoin' (2016) 59 Communications of the ACM <https://dl.acm.org/doi/10.1145/2994581> accessed 22 January 2021.

2 Most commercial blockchain applications rely on a private or a consortium blockchain. The purpose of this sort of blockchain is only to allow a select group of participants to read or write data from or to the ledger. Customer-focused solutions, such as the Diem[2] cryptocurrency, use this approach to keep customer transaction data private[3]. However, depending on the protocol's configuration, blockchain nodes share data with every other node on the network. The distributed nature of blockchains makes them more failsafe and resistant to manipulation. Attacks such as 50+1 percent attacks and selfish mining, therefore, are well researched. However, with each additional node that joins the network, simultaneously its attack surface for data theft increases. This implies that, even for large networks, only one misconfigured node can leak the whole blockchain data to malicious actors. In business contexts, information about internal structures can be leaked to competitors. For private use-cases, information about the individual transaction structures can give deep insights into personal behavior and contain the most sensitive information.

3 To assess the severity of a data breach on one node of the network, we conducted a study to determine how information can be extracted and visualized to gain as many insights into a private blockchain as possible. Thus, our study reverse engineers parts of blockchain networks to gain the necessary information. Reverse engineering a system is typically used to infer how an underlying mechanism works. The difficulty of reverse engineering systems is determined by the number of their components and the interdependence of their components as well as the number of their settings.[4] For our work, we chose the Ethereum platform as a framework and a popular part of the blockchain universe. Inspired by the Internet Census[5], our approach relies on data reverse-engineered from a security issue in a faulty configuration of Ethereum. Starting there, we conducted four small case studies on different implementations of the Ethereum platform to identify stakeholders and mechanisms of these networks. Building on this, we want to address the following research questions (RQ) in this study:

RQ1: Which methods and tools are required to reverse engineer Ethereum networks?

RQ2: How much information can be extracted from consortium blockchains with one misconfigured node?

4 Our paper addresses managers, lawmakers and scientists who are interested in a more technical evaluation of the security of private blockchains. In this paper, we contribute methods used in the process of reverse engineering, as well as the results of the evaluation. Additionally, we provide the insights we gained from the reverse engineering of blockchain networks and the implications they provide for the adoption of the technology. The rest of the paper is structured as follows: In the next section, we lay the foundations by discussing relevant literature and previous work. We then introduce the methodology as well as the data we used for the analysis. The following chapter contains our main research results, by first providing an overview of the technological side of the market and then a detailed analysis of four different blockchains and their use. The final chapter summarizes and concludes the research.

B. Foundations and Related Work

5 In its very basics, the blockchain is a distributed ledger of transactions autonomously managed by a consensus mechanism. Technically, it can be pictured as a growing chain of linked blocks, from where its name originates. The blocks of a blockchain are stored distributed by the participants, the so-called nodes.[6] This distribution also brings the advantage that no single party could manipulate already stored data and that the storage is resilient against outages of nodes. The blocks of a chain consist of a block header and a list of transactions. In the Ethereum blockchain, each transaction has one sender and one recipient. Today, it is possible to not only store transactions in the blockchain, but also data objects and small programs, which is how (smart) contracts are implemented.[7] In Ethereum, this is often used to realize user-defined tokens. There are many smart contract-based tokens, often standardized by

[2] Formerly known as *Libra.*

[3] 'White Paper | Diem Association' <https://www.diem.com/en-us/white-paper/> accessed 22 January 2021.

[4] Seungwoon Lee, Seung-Hun Shin and Byeong-hee Roh, 'Abnormal Behavior-Based Detection of Shodan and Censys-Like Scanning' (2017) 9. *ICUFN* <https://ieeexplore.ieee.org/document/7993960> accessed 11 January 2021.

[5] 'Internet Census 2012' <http://census2012.sourceforge.net/paper.html> accessed 11 January 2021.

[6] Nakamoto (n 1); Roman Beck and others, 'Blockchain Technology in Business and Information Systems Research' (2017) 59 Bus. Inf. Syst. Eng. <https://link.springer.com/content/pdf/10.1007/s12599-017-0505-1.pdf> accessed 11 January 2021.

[7] Kevin Delmolino and others, 'Step by Step towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab' (2016) vol 9604 Lecture Notes in Computer Science <https://doi.org/10.1007/978-3-662-53357-4_6> accessed 22 January 2021.

Ethereum Request for Comments (ERC) standards, which define their characteristics and interface.

6 Given all transactions in a network, naturally, a graph can be built to model the interactions of the participants. The nodes of this graph do not necessarily have to correspond to the nodes of the blockchain network and must not be confused. One physical node of the network could, for example, host multiple Ethereum accounts and therefore represent several nodes in the transaction graph. Additionally, the nodes of the transaction graph can be smart contracts as well. There has been a lot of prior research on the technical analysis of blockchains. This research strongly focuses on large public blockchains, analyzing the transaction structure of public blockchains and the usage patterns therein. First analyses were used to deanonymize Bitcoin users.[8] In the early years of blockchain, it was still possible to dissect the whole transaction graph of the first cryptocurrencies.[9] Due to Bitcoins' transaction structure, it was necessary to apply advanced heuristics to reconstruct and analyze the user graph of the Bitcoin network.[10] There have been fewer studies on the public Ethereum networks.[11] These studies could only link nodes if Ether (the currency of the Ethereum networks) were sent. To consider all transactions, it would be necessary to include the additional network structure that is built by interacting with smart contracts. Studies researching transaction networks of ERC-20 tokens partially deconstructed those structures.[12] Interaction networks within smart contracts can be researched in a similar fashion.

7 The limited existing research regarding the programming interface (JSON-RPC) of a network focuses mostly on the possible attack surface it provides, such as stealing mining reward and denial-of-service attacks,[13] or the use of blockchain-based applications.[14] So far, we could not find any studies that use this interface to map transaction networks or reverse engineer the users and use-cases of private blockchains.

8 In contrast to other security or software engineering related topics, we focus on extracting knowledge for a more research-driven goal. Therefore, our motivation was led by the "Internet Census" of 2012, where the authors used a security vulnerability to create the first full "map" of the internet. Several researchers used this as a foundation, regarding the provided knowledge as well as the used methods, to get insights in other technologies or security-related issues.[15]

C. Materials and Methods

9 To answer our research questions, we used a multiple case study approach. The case study research design consists of the study's *questions*, its *propositions*, *units of analysis*, the *logic linking of the data to the propositions*, and the *criteria for interpreting the finding.*[16] We already posed the research questions in the introduction of this paper. As units of analysis, we chose the block headers and transaction data, as well as the network node data for different blockchains. To identify potential blockchains for a more in-depth analysis,

[8] Fergal Reid and Martin Harrigan, 'An Analysis of Anonymity in the Bitcoin System' [2013] Security and Privacy in Social Networks <https://doi.org/10.1007/978-1-4614-4139-7_10> accessed 22 January 2021.

[9] Dorit Ron and Adi Shamir, 'Quantitative Analysis of the Full Bitcoin Transaction Graph' [2013] Financial Cryptography and Data Security <https://doi.org/10.1007/978-3-642-39884-1_2> accessed 22 January 2021.

[10] Damiano Di Francesco Maesa, Andrea Marino and Laura Ricci, 'Data-Driven Analysis of Bitcoin Properties: Exploiting the Users Graph' (2018) 6 International Journal of Data Science and Analytics <https://doi.org/10.1007/s41060-017-0074-x> accessed 22 January 2021.

[11] Wren Chan and Aspen Olmsted, 'Ethereum Transaction Graph Analysis' (2017) 12th International Conference for Internet Technology and Secured Transactions 498; Andra Anoaica and Hugo Levard, 'Quantitative Description of Internal Activity on the Ethereum Public Blockchain' (2018) 9th IFIP International Conference on New Technologies, Mobility and Security 1.

[12] Friedhelm Victor and Bianca Katharina Lüders, 'Measuring Ethereum-Based ERC20 Token Networks' (2019) vol 1159 Lecture Notes in Computer Science 113; Shahar Somin, Goren Gordon and Yaniv Altshuler, 'Network Analysis of ERC20 Tokens Trading on Ethereum Blockchain' (2018) IX Unifying Themes in Complex Systems 439.

[13] X Wang and others, 'Attack and Defence of Ethereum Remote APIs' [2018] IEEE Globecom Workshops 1.

[14] Chaehyeon Lee and others, 'Blockchain Explorer Based on RPC-Based Monitoring System' [2019] IEEE International Conference on Blockchain and Cryptocurrency 117; Kyungchan Ko and others, 'Design of RPC-Based Blockchain Monitoring Agent' [2018] International Conference on Information and Communication Technology Convergence 117.

[15] John Heidemann and others, 'Census and Survey of the Visible Internet (Extended)' [2008] ISI-TR-2008-649; Lee, Shin and Roh; (n 3).

[16] Robert K Yin, *Case Study Research and Applications: Design and Methods* (Sage publications 2017).

we first created an overview of the Ethereum platform landscape.

10 To do so, we used Shodan, a search engine for Internet-connected devices. We searched the search engine by the query "port:8545" for Ethereum nodes with an active RPC interface. We additionally searched for the string "Ethereum RPC enabled" but considered the results nearly identical.[17] We exported the 3,042 found IP addresses and metadata from Shodan in CSV format. Each IP address represents a node in an Ethereum blockchain network, with an exposed RPC interface. Technically, this gives everyone the possibility to not only extract data from the whole blockchain but also to manipulate the node. It should however be noted that each node in our dataset is for some reason not configured according to the official recommendations, as the RPC interface should never be exposed openly to the internet. Therefore, we only cover blockchains where at least one node was not configured properly.

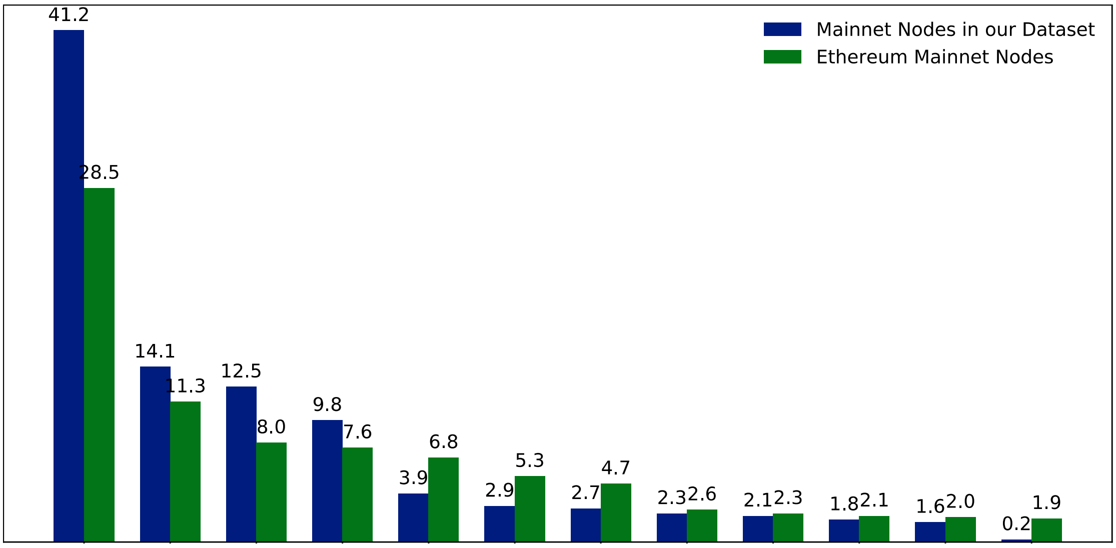

Figure 1: The Distribution of the Mainnet Nodes in our Dataset Compared to all Mainnet Nodes

11 To build our overview dataset on the operation of nodes, we queried the RPC interface of each of the 3,042 nodes. We extracted the chain version, genesis block (i.e., the first block of a blockchain), and information on whether the node was mining or not. To determine the age of each blockchain, we additionally queried the second block of each chain. We decided not to use the timestamp provided in the genesis block since it often provided a zero value in the timestamp. For nodes that are running on the Ethereum main network, we also queried block number 1,920,000 at which the chain splits into Ethereum and Ethereum Classic. We used this as a mechanism to check how valid our data was and how representative our sample of blockchain nodes was.

Our final overview dataset consists of 2,063 active Ethereum nodes, of which 1421 nodes are used in 621 unique blockchain networks and 622 nodes are connected to the Ethereum main network. The network size of the entire Ethereum main network is at the time estimated at 6,900 nodes according to ethernodes.org.[18] As a result, our dataset covers about 9 % of the Ethereum main network. Additionally, we compared how many nodes of the mainnet[19] are operated in different countries and arrived at a very similar distribution, as shown in Figure 1. We did this estimation with other known networks, such as the various Ethereum test networks, which we extracted from an open-source repository for known networks.[20] We arrived at similar results, which lets us conclude that our dataset covers the overall landscape of the Ethereum platform comprehensively.

12 We used the final overview dataset to provide high-level insights into the Ethereum landscape. Additionally, we used this data to identify potential candidates for our case studies. We chose the blockchains according to the number of active nodes,

[17] 'Ethereum RPC Enabled - Shodan' (shodan) <https://www.shodan.io/report/VwRYVIqq> accessed 11 January 2021.

[18] 'Clients - Ethernodes.Org - The Ethereum Network & Node Explorer' (bitfly gmbh 2021) <https://ethernodes.org/> accessed 11 January 2021.

[19] Mainnet refers to live blockchain where tokens are in use.

[20] Sebastian Gerske, 'GitHub - Ethereum-Navigator/Atlas: The Single Source of Truth for All Ethereum Networks.' <https://github.com/ethereum-navigator/atlas> accessed 11 January 2021.

length, and age of the blockchain as well as the distribution of nodes. The goal was to get a diverse set of blockchains to study and draw generalized conclusions. For the chosen blockchains, we extracted account holders for each node and the complete blockchain record of transactions. To identify usage patterns, we used social network analyses on the transaction networks to identify commonly used smart contracts. We extracted and decompiled the smart contracts with the Panoramix decompiler[21] to find out what their role in the blockchain is. While this is a state-of-the-art approach, the decompilation of Ethereum contracts is still in an experimental stage and does not guarantee success. Therefore, we were not able to decompile and analyze all relevant smart contracts. We summarize the overall data extraction process in Figure 2. The mix of source code analysis and social network analysis allowed us to reverse engineer use cases and interaction patterns with the blockchains, and hence provide a suitable way to investigate the proposition.

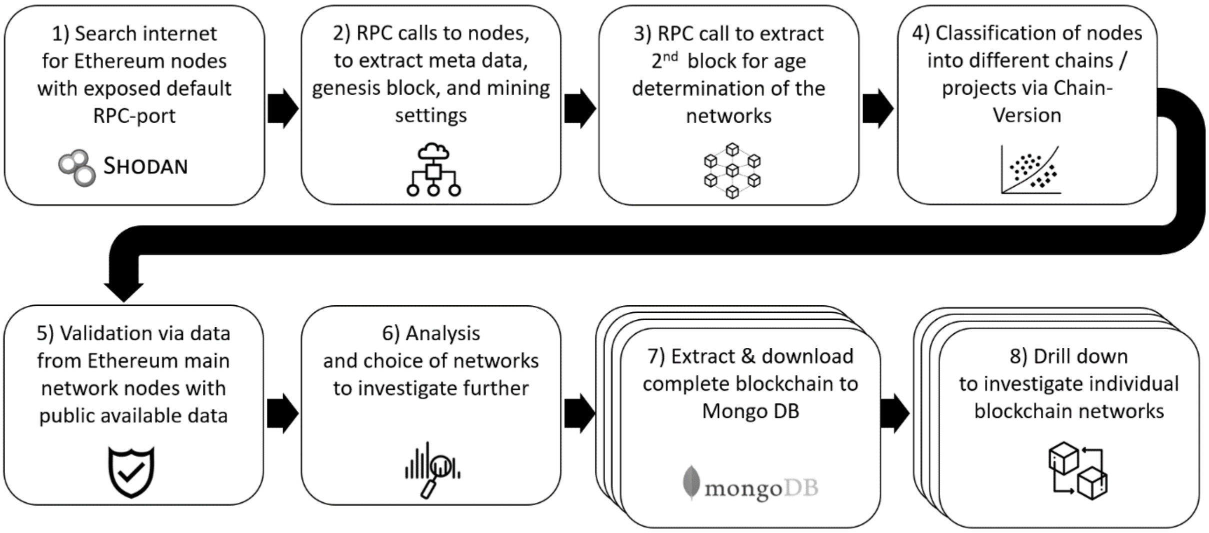
1) Search internet for Ethereum nodes with exposed default RPC-port
SHODAN
2) RPC calls to nodes, to extract meta data, genesis block, and mining settings
3) RPC call to extract 2nd block for age determination of the networks
4) Classification of nodes into different chains / projects via Chain-Version
5) Validation via data from Ethereum main network nodes with public available data
6) Analysis and choice of networks to investigate further
7) Extract & download complete blockchain to Mongo DB
mongoDB
8) Drill down to investigate individual blockchain networks

Figure 2: Overall Data Collection Process

D. An Analysis of Business Blockchains within the Ethereum Landscape

13 The primary analysis of this paper consists of two parts. First, we describe the overall landscape of the Ethereum protocol using the overview dataset. From there, we can draw the first conclusions, before providing a more in-depth analysis of four case studies for Ethereum-based blockchains.

I. Mapping out the Ethereum Landscape

14 To get an overall view of the Ethereum Landscape and map our findings, we analyzed the metadata from the collected dataset. For further analysis, we have chosen different dimensions, which contribute to our overall goal and give us first useful insights in the Ethereum universe to determine the potential case study candidates later.

15 As a first dimension, we analyzed the hosting of the different nodes. Figure 3 (left)shows that almost 75 % of all nodes are hosted by major hosting or cloud providers. With over half of all nodes, the big cloud providers Amazon, Digital Ocean, Microsoft, Google, and Alibaba are claiming a large piece of the Ethereum hosting. This shows that the Ethereum technology shows great potential for business adoption since the cloud setup process is a fast solution to get started. It is an advantage over other technologies, which currently rely on specialized mining hardware that is not widely available.

16 We were surprised by the large share of cloud providers since one of the main advantages of blockchain applications is its distributed topology that affords the technology security and resilience advantages. These advantages are strongly mitigated, when the majority of nodes use the same hosting provider or same data center.[22] To use the full potential of decentralization, blockchain nodes should be

[21] eevm, ‘Panoramix’ <https://github.com/eveem-org/panoramix> accessed 11 January 2021.

[22] Xiaoqi Li and others, ‘A Survey on the Security of Blockchain Systems’ [2017] Future Generation Computer Systems 841; Deepak Puthal and others, ‘The Blockchain as a Decentralized Security Framework [Future Directions]’ (2018) 7.2 IEEE Consumer Electronics Magazine 18.

hosted on-premise. We assume to see a smaller share of cloud providers in the dataset, once the technology is more adopted.

17 As another dimension, we analyzed the country where the nodes are operating. This analysis should give us a picture where most of the Ethereum projects are implemented and may be used as a hint in which country the technology receives most attention. However, since the nodes are mostly cloud-based, this metric can be skewed. Additionally, because nodes of the same chain can operate in different countries, it was not possible to normalize our analysis.

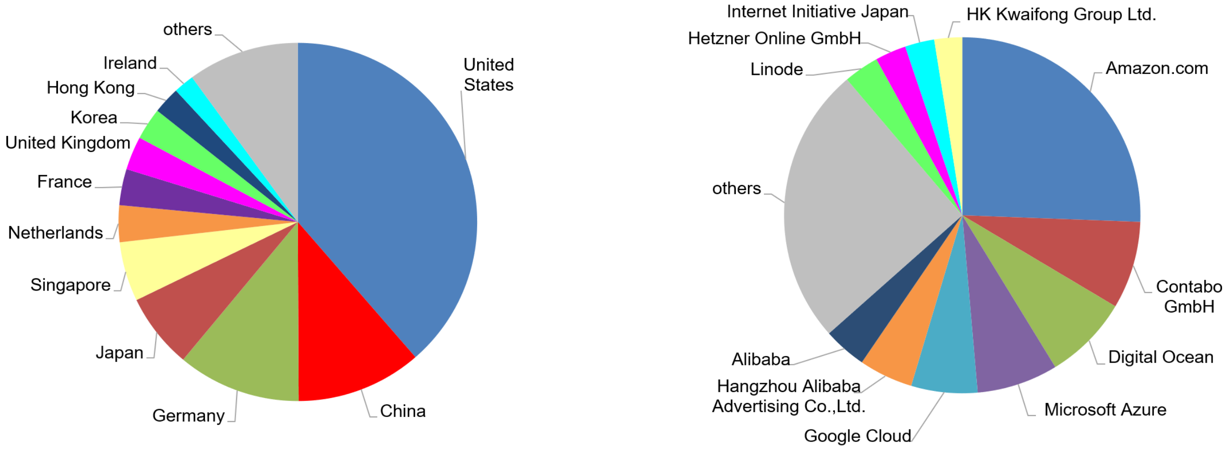

Figure 3: Distribution of Nodes per Hoster (left) and per Country (right)

Instead, we have decided to include all nodes in this distribution (Figure 3 (right)) to give a weighted analysis of origin. Therefore, blockchains operating with more nodes increase the respective share of a country. With this knowledge, the chart becomes an activity analysis, showing which country is more active and may have advanced further in the process of adopting Ethereum technology. Yet from this point of view, it is not possible to determine if there are more projects or just networks with more nodes that determine the share of a country. To determine the state of the different chains and thereby to gain knowledge about the phase in which these projects are, we analyzed the length of the different chains. Figure 4 (left) shows that there are many very short chains. After analyzing and exploring some random samples of these short chains, it showed that these were purely test setups, either with only some test data, partly with less than ten transactions or even completely empty. Extracting information form these projects does not advance this study, and, therefore, we did not consider them in our analyses further. To achieve better knowledge of potential chains, which we could use for further analysis, we analyzed the age of the different implementations. Figure 4 (right) shows the distribution of age, based on the first block. That the initiation of most chains was less than a year ago leads to the conclusion, although the technology is not new anymore, that either projects implementing it are still in an experimental state or that only projects in an early stage still have misconfigured nodes.

18 To consolidate our findings, we put the length of chains in relation to their age, illustrated in Figure 5. Newer but longer chains are either configured with a shorter time per block (block time) or represent fast-growing chains. Older but shorter chains were more mature blockchains such as the Ethereum main- and testnets as well as other public Ethereum-based projects. There is a visible forming of “beams” originating from the lower right corner. All networks on the same beam have the same configuration for the block time. There seem to be only a few main variants for this configuration, which could indicate that many of the private Ethereum networks only use a few boilerplate projects as setup. Considering just the distribution and the aggregation of a line in the center, we assume these represent chains with the default configuration. Additionally, increasingly short block times (indicated by a strong negative slope) are introduced in the last years. This could be either due to the need for higher transaction throughput and lower latency or due to the increase in computation power and network speed. A common criticism of the blockchain technology is the high computational overhead and the resulting lack of performance.[23] Blockchains running at a lower block time are less performance-intensive and are less likely to become out of sync. Additionally, when using the proof-of-work consensus mechanism, shorter block times indicate a lower difficulty,

[23] Kim, Soohyeong, Yongseok Kwon, and Sunghyun Cho, ‘A Survey of Scalability Solutions on Blockchain’ [2018] International Conference on Information and Communication Technology Convergence 1204.

and therefore, a higher risk of double-spending attacks in the network. However, since most private blockchains are not based on this mechanism, we do not research this phenomenon further in this paper.

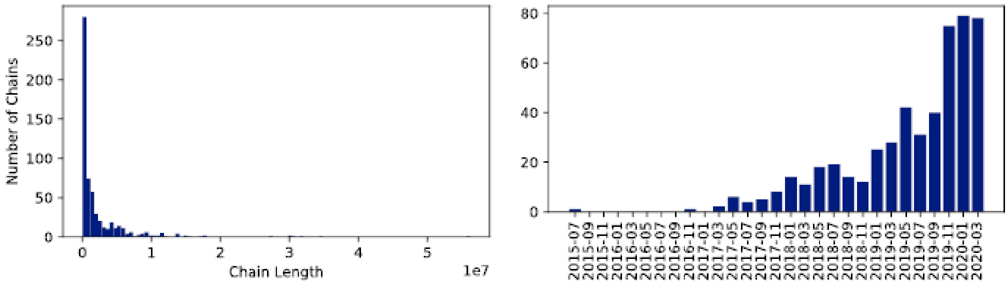

Figure 4: Distribution of Blockchain Length (left) and Number of Networks over Time (right)

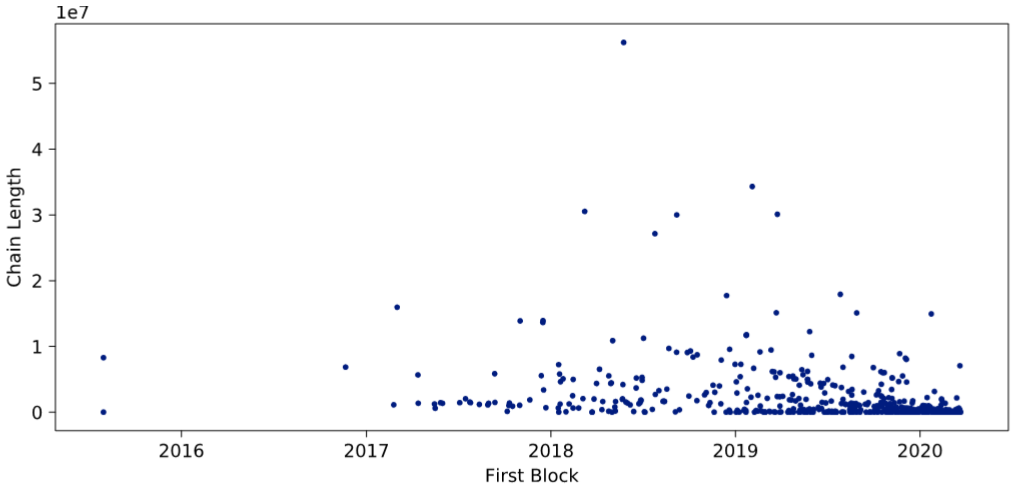

Figure 5: Blockchain Length in Relation to Age

II. Detailed Analysis of Consortium Blockchains

19 As shown in the previous section, most of the networks are either not mature enough to research or are inactive. We identified many blockchains with only one active node and some networks with less than ten transactions over the last two years. For our case studies, we chose four blockchains, that all have more than ten active nodes as well as more than 1 million blocks. Additionally, we excluded the large public blockchains, like the Ethereum mainnet and the various public test networks. Table 1 summarizes the networks chosen for analysis.

Table 1: Blockchains for Case Studies

Case	Network ID	First Block	Length	Number of Nodes	Number of Transactions
1	10	2019-11-03	1,400,000	16	29,000
2	1337	2019-10-22	7,500,000	20	804
3	2894	2018-11-04	3,200,000	13	2,700,000
4	159	2019-08-18	10,500,000	19	34,000,000

1. Case Study 1: Network ID 10

20 We chose the first blockchain we analyzed for its unique properties. It uses the chain version 10, which could indicate that it uses the Quorum variant of Ethereum. Quorum is being developed by JP Morgan Chase as a blockchain, particularly for financial transactions, and offers additional features for this purpose. The Quorum protocol is designed as a permissioned or private blockchain.[24] The analysis of the transactions revealed an unusual transaction graph. Only 102 addresses were creating a one-to-one pairing of senders and receivers as displayed in Figure 6 (left). More precisely, half of these addresses only sent transactions to a single address, and the other half received transactions from a single address. In all following graphs, accounts are colored blue and smart contracts are colored red. The width of the edges indicates the number of transactions sent from one node to another.

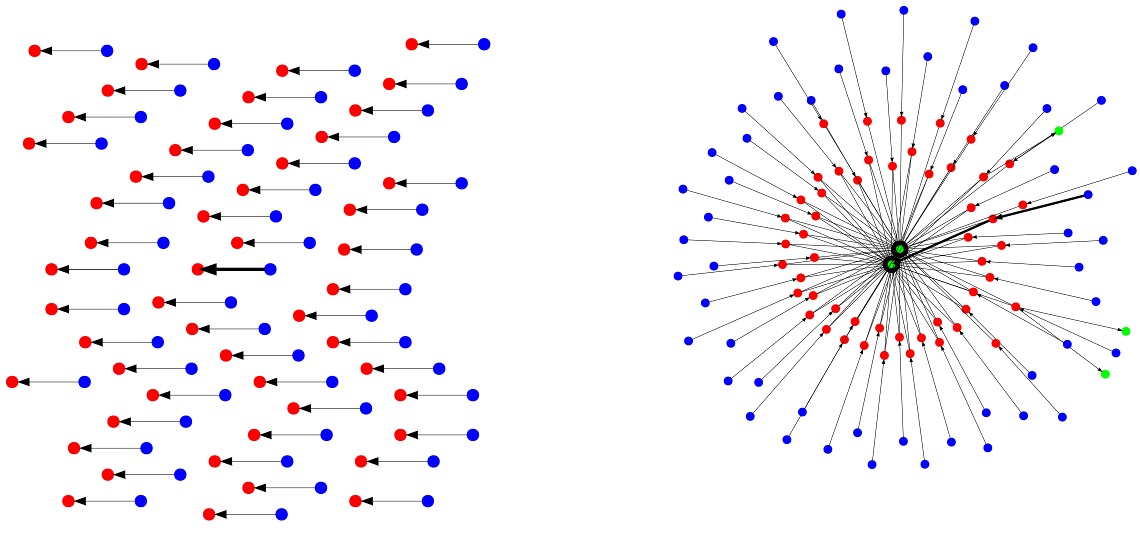

Figure 6: Complete Graph without (left) and with Proxy Contracts (right)

21 This structure led to the assumption that the receivers are all smart contracts with a single user each. We hence queried the nodes for the contract code of the addresses, downloaded, and decompiled the code. The contract provided 22 public functions, most of which are used to manage ownership and access to the smart contract. However, the transactions called only one of those functions named *execute*, which takes two parameters as input. The first parameter is an address of the contract, which the call is delegated to. The second parameter are the parameters of that contract call. This means that the smart contracts, we identified initially, are so-called proxy-contracts that are used to call other contracts. We expanded the transaction graph by the contracts that were called by the proxy contracts. We show the resulting full transaction graph in Figure 6 (right).

[24] JP Morgan Chase, 'Quorum Whitepaper' <https://github.com/ConsenSys/quorum/blob/master/docs/Quorum Whitepaper v0.2.pdf> accessed 11 January 2021.

The added contracts are colored in green. It can be seen that there are two very central contracts that contain the actual logic, and that every user interacts with. Unfortunately, we were not able to decompile these contracts, and therefore were unable to find out what the purpose of this blockchain network is. However, the overall structure lets us assume that the centralized contracts only accept calls from the proxy contracts and that the proxy contracts are used to manage user access. It should also be noted that the calls to the smart contract are not associated with any cost. Normally deploying or calling a smart contract would cost the user gas[25], which is paid for in Ether. However, the accounts all have a balance of zero Ether and there are no transaction fees in this network. This, along with the fact that the central smart contracts were too complex to decompile, could imply that the developers test a novel use-case that exceeds the current computational limits of standard Ethereum configurations.

22 From a social network perspective, the graph seems very decentralized. Since each user interacts with only one proxy contract, which in turn interacts with at most two other contracts, the out-degree centrality of the nodes is equally distributed between the users. It should be noted that one user sent 87.6 % of all transactions. Additionally, we examined how many blocks were mined by each individual miner. With 85.4 % of all blocks, we do not consider this a secure network, since this miner has over 50 % of mining power.[26] With this much power for one node, it should be reevaluated if a centralized solution could be a better alternative.[27] However, if the network is indeed only a test setup, the security implications are not as important.

2. Case Study 2: Network ID 1337

23 The second blockchain we identified exhibits a different kind of centralization. While the nodes are distributed all over the world, they are all hosted in the Microsoft Azure cloud. This centralization to a single provider gives a single entity immense power over the network, since it could completely shut down all nodes or simply block access to the nodes on short notice.[28]

24 Furthermore, we noticed that many contracts deployed on the blockchain use smart contracts developed by Ambisafe[29]. Ambisafe offers a blockchain quickstart platform that lets users easily build a blockchain by using preconfigured modules. We identified an EToken2 contract, which offers advanced token functionality but is compatible with the ERC20 interface. Additionally, we identified contracts for identity management (ERC725) and claim management (ERC735). Again, we found proxy smart contracts, but in this case, they were not for access management, but they made contracts upgradeable.

25 The overall network structure looks distributed, as shown in Figure 7 (left). There is one centralized node that interacts with a lot of smart contracts. Approximately a third of these contracts are EToken2 contracts. Each of these contracts corresponds to a contract deployed by the same address that allows transfers of EToken2 to ICAP addresses. These are addresses that are compatible with the IBAN bank account numbers. Another very central node is the smart contract in the upper cluster. This smart contract is a claim management contract. While this looks like the architecture of a decentralized exchange, there is little to no interaction of different accounts with each other, either direct or via smart contracts. Figure 7 (right) shows the transaction graph with a dot layout[30], which indicates that the transactions all flow in only one direction. In addition to this unidirectional transaction flow, the root node holds an overwhelming majority of Ether with approximately 10^{32} Ether. In comparison, the second largest account holds 18.7 Ether, while most accounts hold less than one.

26 We conclude that this is an experimental setup that is used for testing or demonstration purposes only, or possibly a network that is currently being built and the funds are being distributed to the nodes according to their needs.

[25] Gas measures the amount of work of miners to include transactions in a block.

[26] Nakamoto (n 1).

[27] Karl Wüst and Arthur Gervais, 'Do You Need a Blockchain?' [2018] Crypto Valley Conference on Blockchain Technology < https://doi.org/10.1109/CVCBT.2018.00011> accessed 11 January 2021.

[28] Primavera De Filippi and Smari McCarthy, 'Cloud Computing: Centralization and Data Sovereignty' (2012) 3.2 European Journal of Law and Technology 1.

[29] 'Ambisafe | Making Financial Markets Universally Accessible.' (Ambisfe) <https://ambisafe.com/> accessed 11 January 2021.

[30] John Ellson and others, 'Graphviz—Open Source Graph Drawing Tools' [2001] International Symposium on Graph Drawing < https://doi.org/10.1007/3-540-45848-4_57> accessed 11 January 2021.

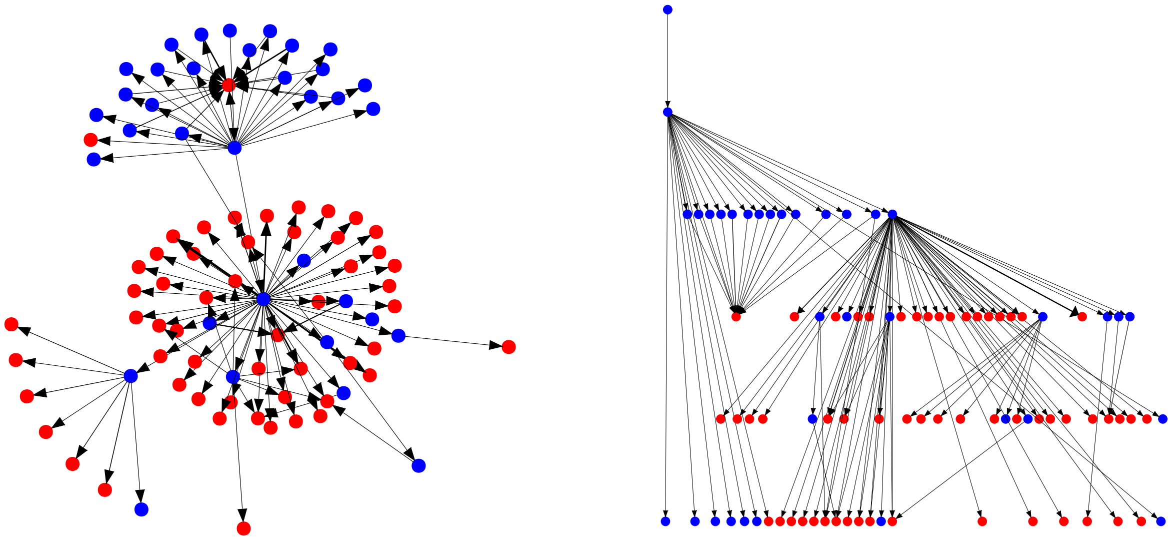

Figure 7: Transaction Graph in Neato Layout (left) and Dot Layout (right)

3. Case Study 3: Network ID 2894

27 The first insight of our analysis was that there are no smart contracts deployed in this network. This means that the transactions transfer Ether. In fact, the transactions in the network carry on average 2,176.3 Ether.

28 The overall transaction graph is much larger than the previous blockchain. The network consists of 15,489 addresses. This size makes it too complex to display completely. Therefore, we chose the representation of the graph as an approximation in Figure 8 (left) by only displaying edges where there were more than 1,000 sent transactions with the corresponding nodes. The second representation we chose was a transaction graph that only displays those transactions that have data attached in addition to the transaction value, as shown in Figure 8 (right). We could not identify what this data represents since the data seemed to be in the form of arbitrary numbers not correlated with the transaction value. However, there were three different types of numbers: small numbers between 1 and 256, medium numbers around 10^6, and extremely large numbers in the order of magnitude 10^{56}.

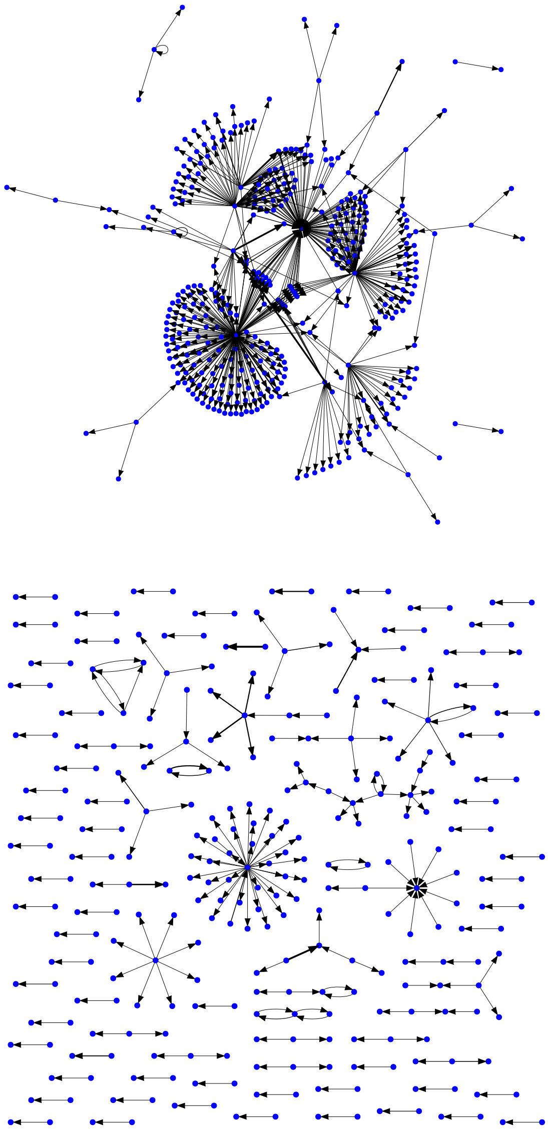

Figure 8: Transaction Graph with nodes with more than 1,000 Transaction (top) and with attached data (bottom)

Even though the number of nodes is much larger than other networks, the graph is much more centralized. Figure 9 (top) shows the indegree and chad to use a logarithmic scale due to the massive differences in centrality. These differences could be as a result of an initial token distribution process. Additionally, the distribution of mining power is not distributed equally either. Figure 9 (bottom) shows that two miners mined a disproportionally large share of the blocks. While this might not be an immediate problem, if those two miners cooperate, they could overrule the rest of the network. Finally, the distribution of Ether is unequal among the nodes, but it is not nearly as unequal as seen in the previous case study. A large portion of the nodes have one to 10^8 Ether, but the majority have less than one. The centralized transaction network and mining, as well as the unequal distribution of Ether, are phenomena that can be seen in large public blockchains, in particular because larger networks tend to centralize. This network, despite its use as a pure accounting network, is the most used network in our dataset.

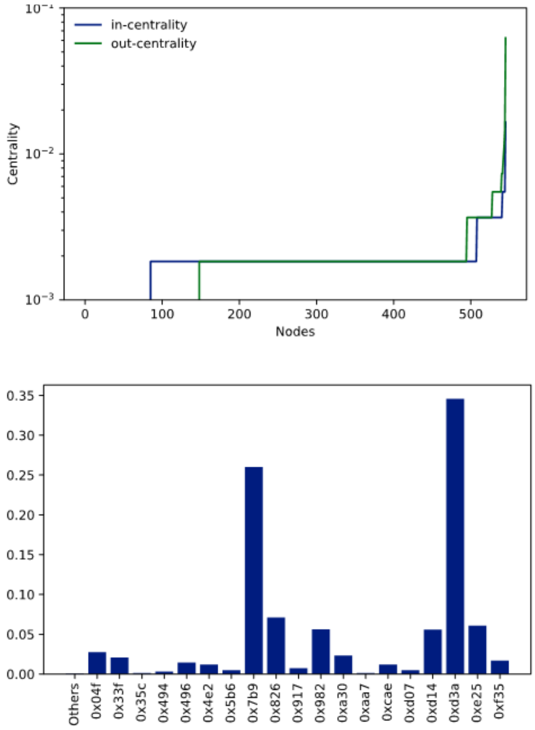

Figure 9: Centrality Scores per Node (top) and Share of Mined Blocks per Miner (bottom)

4. Case Study 4: Network ID 159

29 Our last case study concerns a network that has a massive number of transactions. Since it was launched, the network has about 20 % of the public Ethereum mainnet transactions. The Ethereum mainnet is used by thousands of users. However, we noticed a very centralized contract in the network, as shown in Figure 10 (top). We identified it as a TomoChain BlockSigner smart contract[31], which is used as an alternative consensus mechanism. In fact, all smart contracts we identified are used for this mechanism, and the transactions therein are not relevant to the actual transaction network structure. Therefore, we also analyzed the network structure of the remaining network separately as shown in Figure 10 (botom). The resulting graph only considers 895 transactions.

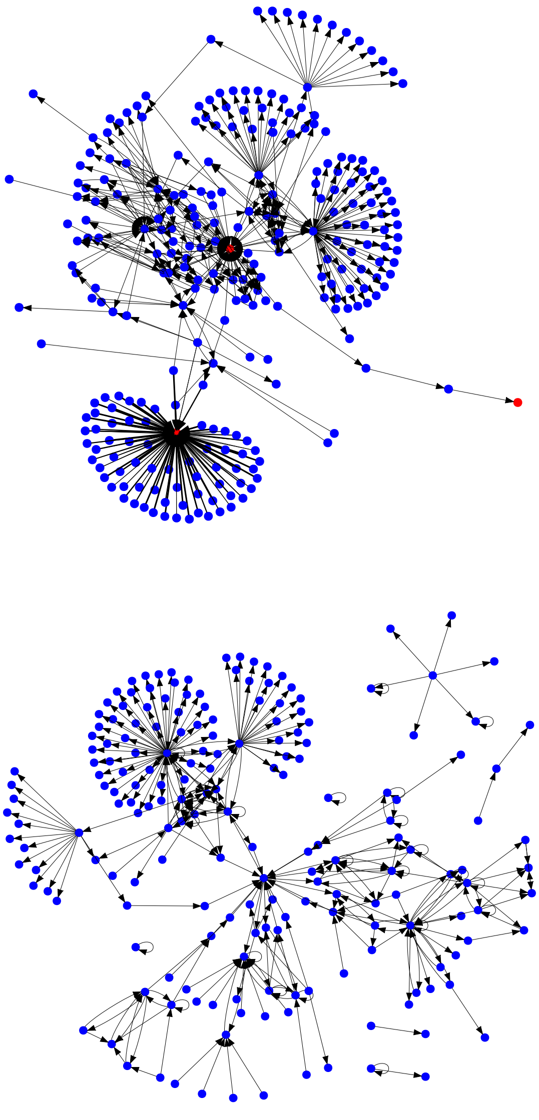

Figure 10: Transaction Structure with (top) and without Smart Contracts (bottom)

30 This transaction graph is not fully connected. There are some small islands with unidirectional transactions. The main island consists of a few larger clusters of outgoing transactions. Again, this could indi-

[31] TomoChain~R&D~Team, 'OmoChain: Masternodes Design-Technical White Paper Version 1.0' (tomochain Pte. Ltd. 2018) <https://tomochain.com/docs/technical-whitepaper--1.0.pdf> accessed on 11 January 2021.

cate an initial token distribution process. Since this network is not as old as the previous network we analyzed, it could show much more activity in the future and build a similar transaction graph. Since a smart contract handles the block generation process, we could not easily identify the miners of the blocks, and hence could not analyze the distribution of mining power.

31 Upon further investigation through the IP addresses of the nodes, we found out that the network is connected to the Caelum Project, which is not accessible anymore. It is described as a decentralized storage solution, to secure digital crypto assets[32] with inheritance functionalities.[33]

E. Conclusion

32 Past research on blockchain security has focused mainly on the prevention of fraudulent transactions. However, with the rise of private and consortium blockchains, data privacy has become another important topic, lacking extensive research. Against this backdrop, in this paper, we analyzed the exploitation potential of misconfigured private blockchains. Our approach consisted of reverse engineering actual implementations of the Ethereum platform for individual use-cases to analyze the transaction structure and smart contract implementations, to gain insights into the usage patterns and stakeholders of the networks.

33 In our first research question, we asked, which methods and tools are required to reverse engineer Ethereum networks. Our approach consisted of using a port-scanning dataset and enriching it with additional data that the listed nodes provided. Using social network analyses and source code analyses, we additionally conducted small case studies on selected networks. The social network analysis proved to give useful insights into the actual usage of the network but fell short of revealing the whole structure without the source code analysis of the smart contracts. The smart contract analysis was a very successful approach for some networks, while for others, we could not retrieve the source code of the smart contracts by decompiling them. The main improvement we would suggest for future research would be a "magical" decompiler that can retrieve the original commented source code from Ethereum bytecode. Additionally, it should be checked whether some of the analyses can be automated, to give a quick overview of all networks fast and not rely on analyzing them step by step.

34 Our second research question was how much information can be extracted with only one misconfigured node. We could identify that our approach is not able to paint the full picture of the networks but can give valuable insights. For some networks, we could link IP addresses and specific smart contract structures with publicly available data to get insights of stakeholders. For other networks, we had to rely on the transaction structure and could only identify entities by their cryptographic addresses. Especially for Ethereum networks, each node holds a full copy of the ledger. Therefore, all analyses were based on a maximum of available data. In further research, other structures such as the Hyperledger project should be examined, where the network is segmented into channels. Here, attacking only one node should only provide partial information about the network and would hence call for more elaborated analysis techniques.

35 Due to the availability of data, our research focused on organizational entities rather than individuals. However, the results indicate that for our analysis of the data from an analytical point of view, it does not matter whether the data is of organizational or personal nature. Network structures and agreements can be derived or inferred be it the one or the other. Therefore, we think that the results can be transferred to blockchain networks comprising end users sharing personal data. Thus, our study also raises the very relevant question as to whether (private) blockchain networks can reach a consensus without sharing all data between nodes and what data distribution strategies would defend best against weak links in the chain that exposes private information of individuals.

36 Our dataset consists of over 621 unique blockchain networks, of which we were only able to analyze four for more detailed insights. The process of retrieving and analyzing the entire blockchain for many networks is extremely time consuming, but we are sure that analyzing a larger portion of it would give even better insights into information extraction processes. Overall, improving the systems and tools needed for the reverse engineering as well as a full analysis for the network information, can therefore be future work.

37 The research provided us with an exciting puzzle that is still not assembled completely. We, therefore, hope that the approach is adopted for other

[32] Crypto assets are "a new type of asset recorded in digital form and enabled by the use of cryptography that is not and does not represent a financial claim on, or a liability of, any identifiable entity". European Central Bank, 'Crypto-assets – trends and implications' <https://www.ecb.europa.eu/paym/intro/mip-online/2019/html/1906_crypto_assets.en.html> accessed on 11 January 2021.

[33] 'Caelum Project' <https://web.archive.org/web/2020*/www.caelumproject.io > accessed on 11 January 2021.

blockchain technologies such as Hyperledger or even other unrelated technologies to improve current tools.

This work has been developed in the project PIMKoWe. PIMKoWe (reference number: 02P17D160) is partly funded by the German ministry of education and research (BMBF) within the research program "Industrie 4.0 – Kollaborationen in dynamischen Wertschöpfungsnetzwerken (InKoWe)" and managed by the Project Management Agency Karlsruhe (PTKA). The authors are responsible for the content of this publication.