GOVERNANCE OF AND WITH BLOCKCHAINS

a thematic report prepared by

THE EUROPEAN UNION BLOCKCHAIN OBSERVATORY & FORUM

EUBlockchain Observatory and Forum

An initiative of the European Commission

About this report

The European Union Blockchain Observatory & Forum has set as one of its objectives the analysis of and reporting on a wide range of important blockchain themes, driven by the priorities of the European Commission and based on input from its Working Groups and other stakeholders. As part of this it will publish a series of thematic reports on selected blockchain-related topics. The objective of these thematic reports is to provide a concise, easily readable overview and exploration of each theme suitable for the general public. The input of a number of different stakeholders and sources is considered for each report. For this paper, these include:

- Members of the Observatory & Forum's Working Groups as well as the Obeservatory's Convergence Sub-Working Group (please see next page).
- Input from participants at the "Governance and new organisational challenges" workshop held in Brussels on 30 April, 2019.
- Input from the Secretariat of the EU Blockchain Observatory & Forum (which includes members of the DG CONNECT of the European Commission and members of ConsenSys).

CREDITS

This report has been produced by ConsenSys AG on behalf of the European Union Blockchain Observatory & Forum.

Written by: Tom Lyons, Ludovic Courcelas
Thematic Report Series Editor: Tom Lyons
Report design: Benjamin Calméjane

v1.0 - Published on 20 May, 2020.

DISCLAIMER

ACKNOWLEDGEMENTS

The EU Observatory & Forum would like to expressly acknowledge the following for their direct contributions and feedback to this paper as members of the Governance Sub-Working Group:

- Stefan Beyer
- Cristina Cobos
- Amandine Doat
- Nadia Filali
- Jānis Graubiņš
- Julian Hosp
- Stefan Junestrand
- Iwona Karasek-Wojciechowicz
- Ad Kroft
- Ivona Skultetyova
- Jolanda ter Maten

We would also like to acknowledge the contributions of the following reviewers:

- Dr Milly Perry

NOTE

While we have done our best to incorporate the comments and suggestions of our contributors where appropriate and feasible, all mistakes and omissions are the sole responsibility of the authors of this paper.

Contents

Executive summary

In this paper we look at blockchain governance – by which we mean the processes, challenges and issues around how blockchain protocols, projects and the community organise themselves, as well as ways in which blockchain could be used for governance tasks in the real world.

We start our investigation of blockchain governance with a look at blockchain protocols, by which we refer to large-scale, generally open source projects like Bitcoin, Ethereum or Hyperledger that provide basic blockchain infrastructure, as well as broad-based decentralised applications providing a basic infrastructure-like service. There are many governance issues that arise as such projects move along the lifecycle from conception and launch through to day-to-day maintenance and eventual upgrades. Of these, there are a few key questions that all projects must face. One is who can use the network. Here we find a range of possibilities, from "public, permissionless" blockchains like Bitcoin that are open to all, to "private, permissioned" blockchains that are walled gardens built to serve a specific purpose and user base. Another basic question is who manages the protocol and how. Here models run roughly along a continuum from formally constituted, member-backed consortia, in which governance rules are agreed to in advance, to fully open, grassroots, community-run projects with no established authority, and where governance rules and enforcement mechanisms must depend on tradition and group consensus.

In the latter case in particular, one of the most difficult governance challenges is how to decide on changes to the protocol. There are different models here too. Proponents of fully on-chain governance believe the rules for changing the protocol should be hard-coded into the protocol itself. Proponents of off-chain governance think it wiser for decisions to be made via formal and informal processes among the broad community of stakeholders. Should members of the community not agree, they are generally free to split away, a process known as "forking". Here too we find an array of possibilities, from benign "soft forks" that represent simple upgrades to the protocol, to contentious "hard forks" that signal a major schism and often result in competing platforms.

In the next section we focus on enterprise blockchain projects, in which groups of (generally) medium to large-sized businesses come together to build a common blockchain platform. Here we recommend a number of best practices. Since these consortia, as they are often referred to,

EXECUTIVE SUMMARY

tend to be born of shared business problems, it is important to first be clear exactly what this common problem is. Next, they should ascertain whether or not blockchain is the right solution, and we provide a number of criteria that can be used to make that decision.
Assuming there is value to be found in a blockchain solution, consortia members will next have to set up a formal organisation. There are a number of models to choose from, although today there is a trend towards private companies with stakeholders as shareholders and a dedicated executive team, staff and in-house developers. With the organisation in place, the next step is to establish the project governance. Governance structures should balance the interests of all stakeholders, and the decision processes and criteria should be crystal clear. Finally, because a blockchain consortium very often involves competitors coming together to build a common infrastructure, members often have to get used to new ways of working. To be successful, the executive management and project teams of the individual consortium members should have a clear idea about what this kind of co-opetition means for their organisation, and be prepared to accept its potential difficulties.

To close, we take a look at how blockchain can be used to solve real-world governance challenges. We focus on a number of potential use cases. One is in the area of dispute resolution, in which smart contracts and blockchain-based platforms could be used to streamline (and dramatically reduce the cost of) settling certain kinds of business disputes. Blockchain has also been proposed for various types of e-voting situations, including political elections and citizen participation platforms. Blockchain has also been proposed to help streamline as well as bring more transparency and inclusivity to corporate governance processes.

One important governance trend born of the blockchain movement – and still largely confined to it – is that of the decentralised autonomous organisation (DAO). Generally understood as an organisation governed not by people but by code, DAOs are still a new phenomenon. Yet they are becoming more popular. Whether, as some have predicted, 2020 will be the year of the DAO remains to be seen. As we write, it is however hard to imagine any concept more true to the decentralised ethos of blockchain than that of the DAO.

Governing blockchain protocols and decentralised applications

THE ALLURE OF DECENTRALISATION

"I've moved on to other things. It's in good hands with Gavin and everyone."[1] With these words in an email in April of 2011, Sataoshi Nakamoto, the mysterious creator of Bitcoin, signalled his, her or their intention to step back from the project. Within a few months, Nakamoto had disappeared. Since then the governance of the Bitcoin protocol has been in the hands of the Bitcoin community. With no formal or informal governance guidelines or legal structure, that community has had to organise itself to do all the work of building and maintaining this remarkable network. And, despite bumps in the road, it has done so in splendid fashion.[2]

Bitcoin ignited a cambrian explosion of blockchain protocols and networks, with different takes on the technology and different governance models. Each project, however, has to deal with a similar set of problems and questions. How should the blockchain be designed? Who will build it? How will it be funded? Who will run and maintain the network and how? And perhaps most importantly from a governance perspective: who decides how the blockchain will change over time and how are those decisions enforced?

These questions are more than academic. While we have seen many governance successes in the blockchain space, there have been a fair number of governance disputes and scandals as well.[3]

These challenges will be familiar to anyone who has built an IT platform. The wrinkle in the blockchain world is decentralisation. In the absence of a central decision-making authority, network participants have to find ways to coordinate and decide among themselves, requiring approaches that can be wildly different from those in traditional IT projects. Below we look at how this plays out in different contexts by examining the typical lifecycle of a blockchain protocol project.

GOVERNANCE CHALLENGES AND OPPORTUNITIES FOR DECENTRALISED APPLICATIONS AND BLOCKCHAIN PROTOCOLS

In this section we discuss governance on the protocol level. This can encompass the blockchain protocols themselves, like Bitcoin, Ethereum or Hyperledger, that are used as the basic infrastructure for blockchain-based platforms. This discussion is also relevant to

1 Satoshi's Final Messages Leave Tantalizing Clues to His Disappearance, bitcoin.com, 30 October, 2019.

2 Today Bitcoin is not only still running, it remains the largest cryptocurrency in circulation, with a market capitalisation at this writing of 175 billion US dollars. See coinmarketcap.com. Note that the price of bitcoin is very volatile. It can very well have increased, or decreased, dramatically after publication of this paper.

3 See Justin Sun Bought Steemit. Steem Moved to Limit His Power, CoinDesk, 24 February 2020, and Inside the Crypto World's Biggest Scandal, Wired Magazine, 19 June 2018.

GOVERNING BLOCKCHAIN PROTOCOLS

decentralised application protocols, which can be defined as an implementation of a set of functionalities via predetermined smart contracts that power decentralised business logic and live on a decentralised blockchain. For convenience's sake, we refer to both cases below as "blockchains" or "protocols". Below, in the "Governing blockchain consortia" section, we discuss governance issues facing enterprise blockchain projects.

Initial Idea: Conceive the blockchain

To date, all blockchain protocols we know of have been started by an individual or small group. While protocol founders come from different backgrounds and have different motivations, as with any project, they have to start with basic questions of purpose. What is the protocol trying to accomplish? What problem does it solve? Who is it for?

While these purposes may vary,[4] they all tend to share a common element of decentralisation: aiming to build a tool that can be used to decentralise existing structures, build new, decentralised structures, or both. Founders typically announce the purpose of their protocol in the form of a white paper. These white papers serve to introduce the idea to the world, develop the idea in detail, including deep dives into the proposed technology, and hopefully garner interest in the project. But no matter how brilliant the proposed technology might be, from a governance perspective the underlying purpose remains the key variable. The purpose sets the north star that guides (or should guide) most if not all governance choices, and is very often at the heart of governance disputes.

Initial launch: Build the blockchain

The next step is to make the vision a reality by building and releasing a first version of the protocol. This pre-launch phase almost always involves a small group that coalesces around the founder, either informally due to interest in the project, or as part of an organisation founded for the purpose of building the protocol. At this stage governance structures run the gamut from a loose and informal "startup in a garage" approach to a clearly defined, "large-scale IT project" approach. Participation can run from open-to-all (at least in theory) to restricted to authorised team members. Bitcoin is the classic example of a protocol in which anyone in the world with the requisite technical skills could have (again, in theory) participated in the initial development and where there was no formally defined governance to guide activities during the pre-launch phase.[5] Many other protocols have been run along similar community-driven lines, though often with more formal structures, typically in the form of a foundation. There are also projects that, while also taking a community approach via a foundation or association model, restrict membership to certain parties, and where governance rules are clearly defined in a charter or other governance document.

Of note is the fact that by far the majority of blockchain protocol projects are run as non-profit organisations on the open-source software model. This is a deliberate choice,

4 The purpose of Bitcoin, for instance, is to create independent electronic cash. The purpose of Ethereum to build a platform for smart contracts and decentralised applications, leading to a world computer. Hyperledger aims to create the components on which companies can build enterprise blockchain solutions.

5 In practice, Bitcoin was developed by a small core group of enthusiasts. These came together almost by accident, as the project was hardly known outside of cypherpunk and cryptography circles when it began.

and is by no means self-evident.[6] We can think of several reasons why. As projects to build new infrastructure, the priority is generally to build a user base to gain network effects. This could be difficult in a for-profit enterprise that would likely have to charge users for access, and rather recalls large open-source infrastructure projects like the Internet or World Wide Web, both of which have served as models for blockchain protocol development. We would argue that a for-profit model would also seem to go against the decentralised, community-run ethos whose tradition started with Bitcoin, and so serves as an example of how the underlying purpose serves as a distant but compelling north star, exerting a subtle yet pervasive influence on governance decisions.

Funding: Pay for the blockchain

The question of how to fund a blockchain protocol project is often overlooked when talking about blockchains, yet it is a critical factor with strong governance implications. Indeed, blockchain has been almost as innovative on the funding side as it has been on the technology side. Consider Bitcoin. With no initial funding, the project depended wholly on volunteers in its early stages. But as the network gained traction, the value of Bitcoin rose dramatically, creating enormous wealth, particularly for early adopters. Successful businesses also arose to serve the ecosystem, including mining pools, exchanges and wallet providers. In this way a community of people and organisations with the incentive and the means to keep Bitcoin going, including helping to fund development, has grown in an organic fashion. While this has not necessarily translated into a steady flow of adequate funding over the years,[7] in a certain sense we can say that the Bitcoin protocol has funded itself. This is something new in the world.

The Bitcoin example showed the potential of cryptocurrencies as a funding mechanism for other blockchain protocol projects. This led to the advent of the token sale, in which protocol projects sell their cryptotokens to future users and any other interested party, and use the proceeds to build the network. While the rise and fall of the Initial Coin Offering (ICO), as token sales were soon christened, is beyond the scope of this paper, there is little doubt that it represented a major innovation in venture capital whose effects will be with us for a long time. We can also make a few observations about the token sale from a governance perspective. For one, this focus on crowdfunding seems to us another instance of the influence of the decentralisation ethos on blockchain protocol governance models. For another, whether explicitly stated or not, a token sale implies some kind of agreement between the token buyers and protocol developers. This brings token holders into the governance discussion – including unfortunately into governance clashes and even lawsuits.[8]

This said, it is by no means necessary to fund a blockchain protocol project via the community. Many protocol projects run by consortia are purely member funded. Additionally, some projects rely on the well-established mechanisms that have been traditionally

6 In the early stages of the Ethereum project, several members of the group advocated for Ethereum to be a for-profit venture. It was ultimately Ethereum's founder who decided for the non-profit route. See The Prophets of Cryptocurrency Survey the Boom and Bust, Nick Paumgarten, The New Yorker, 15 October, 2018.

7 See Who Funds Bitcoin Developers?, Simon Chandler, Cryptonews.com, 27 January, 2020, and Who Funds Bitcoin Development?, BitMEX Research, 28 March, 2020.

8 Op. cit.: Inside the Crypto World's Biggest Scandal, Wired Magazine, 19 June 2018.

used by open-source projects in the software industry. In these open-source projects, the development and maintenance of a code base may be partially funded by private entities that have an interest in being able to rely on shared standards and libraries for their business, and also partially contributed by individual contributors. Other projects use a variety of regulated token sales, private token sales and/or have turned back to the traditional VC route. In these cases too, there are governance implications tied to who the investors are and what say they have in the protocol's development.

On-chain governance: Run the network

In this section we discuss aspects of protocol governance that are either inherent in the technology itself, or emerge from its use. This is often referred to as "on-chain" governance. To recall, a blockchain is a distributed, peer-to-peer (P2P) network in which the network nodes, by running the protocol, share the work of validating transactions and saving records of those transactions through appending blocks to the blockchain. This results in an immutable, distributed ledger containing a permanent and agreed-upon record of all transactions and of which each node maintains an identical copy. There are several important aspects of governance at play here that involve coordination between a number of different stakeholders, from core developers and miners/validators to end users.

Who can use the network and in what capacity? One basic governance question is who gets to participate in the network and in what capacity. The questions here are: a) who can read data on the blockchain ledger, b) who can submit transactions, and c) who can run a full node and participate in the work of validation. There are two main answers to each question. Either a) anyone who wants to, provided they have the necessary technical skills and equipment to download and run the protocol software, or b) only authorised users, in which case there must be some identification and onboarding process that takes place off the chain. In the blockchain world, reference is usually made to public (open) versus private (walled off) blockchains, and permissionless (no access control) versus permissioned (with access control) blockchains. The three most prominent combinations include: free-for-all "public, permissionless" blockchains like Bitcoin, "public, permissioned" blockchains that are open to all to use but validated by a known group of nodes, and "private, permissioned" blockchains that are walled gardens often built to serve a specific purpose and user base. This question of who can use the network is essential to on-chain governance for two reasons. For one, it has a strong influence on the mechanisms used to coordinate among the nodes (see "Consensus mechanisms" below). For another it can have profound implications for how the blockchain interacts with the real world, for example with existing legal, regulatory, economic, business and/or organisational structures (issues we have addressed in several other papers). [9]

Consensus mechanisms. From a technological perspective, the validation question directly influences the choice of consensus mechanism. Blockchain consensus is a fascinating and highly complex subject of its own that is far beyond the scope of this paper, but from a governance perspective it comes down to how to ensure that nodes coordinate among

9 See Legal and regulatory framework blockchains and smart contracts, EU Blockchain Observatory and Forum, 27 September, 2019, and Blockchain and the future of digital assets, EU Blockchain Observatory and Forum, 19 February 2020.

GOVERNING BLOCKCHAIN PROTOCOLS

themselves in an active and honest way that promotes the goals of the network. This is a tremendous challenge above all in public, permissionless blockchains. Absent the command-and-control nature of a central authority, coordination among peer nodes requires both a clear set of rules on how consensus is to be achieved as well as a set of incentives and punishments geared to ensuring the rules are followed.[10]

This makes for some interesting observations. Firstly, in a permissionless blockchain the rules, incentives and punishments must be fully encoded in the protocol. There can be no recourse to any external authority or process. Secondly, the choice of consensus mechanism can have implications for the security and balance of power in the network. In Bitcoin's Proof-of-Work (PoW) consensus based on mining, success in being chosen to validate a block and win the reward is correlated with computing power. As a result, most successful Bitcoin mining today is carried out by a small group of large mining pools, causing many to complain that Bitcoin is no longer decentralised. PoW also uses a great deal of electricity. This is a governance issue to the extent it affects how Bitcoin is perceived by the rest of the world. Other consensus mechanisms use alternative means of choosing lead validators, for example based on a validator's holdings of the native cryptocurrency. In such systems, people worry about power being concentrated in the hands of "wealthy" plutocrats with large holdings of the currency. There are similar balance of power issues with other consensus mechanisms. Protocol designers must constantly address such issues if they are to maintain trust in the network.

For permissioned blockchains, a certain amount of trust can be moved off the chain: if the identities of the validators are known, governance can be handled by legal contracts, terms and conditions and traditional management practices. But just because all actors on the network are known to each other, it doesn't mean they trust each other. That means the off-chain governance structures need to be well thought out and enforceable.

Identity. Identity is another important aspect of blockchain governance both on and off the chain. In permissioned blockchains, protocol designers need to have an identity framework to manage how users and validators will be identified, how these identities will be managed on the blockchain, and so on, ideally based on considerations around why identities need to be verified (is it to establish trust, or a business or regulatory requirement?). While a public, permissionless protocol can dispense with this, identity rears its head here too. Even though you do not need to register with the Bitcoin network to use it, all transactions are associated with the public keys of the parties to the transaction. Through clever analysis techniques, it is often possible to trace these back to real-world identities. Those who want a truly anonymous blockchain – itself a governance choice – will need to take this into account. And indeed, this has given rise to new kinds of blockchains, like ZCash and Monero, that do provide mechanisms for true anonymity.

On-chain project governance. An important aspect of on-chain governance not yet touched upon is the extent to which the decision-making processes regarding project governance, including the rules about how to

10 See Scalability, interoperability and sustainability of blockchains, EU Blockchain Observatory and Forum, 6 March 2019 as well as Blockchain and cybersecurity: a taxonomic approach, University of Southampton, October 2019.

change the rules, are coded into the protocol itself. Blockchains have been built, for instance, that allow token holders, and only token holders, to vote for changes to the protocol. This moves what is usually an off-chain process completely on chain. Proponents of this kind of on-chain governance praise it for its speed, transparency and above all because it seems most aligned with the decentralisation ethos of blockchains. Opponents find it problematic on many grounds. We return to the subject below in the section "Encoding the rules: The on-chain vs off-chain governance debate."

Off-chain governance: Run the project

All blockchain protocol projects to date depend on human stewardship of some kind to handle the issues typical in large-scale IT projects. These run from how to manage day-to-day network maintenance and deal with ad-hoc problems like bugs or security issues to making all the decisions and issues around upgrading the protocol to add new capabilities, meet new user needs or respond to new technical developments. Such project management requires strong governance to be successful, which, as in on-chain governance, boils down to having a clearly defined set of rules and the means, either through incentives, punishments or both, to enforce them.

Here, formally constituted, member-backed consortia have a distinct advantage. Governance rules can be (and generally are) enshrined in a charter, legally agreed to by members through formal contracts, and implemented by centralised management. While enforcement generally happens through automated rules on a day-to-day basis (access, permissions, business logic), the platform can rely on commercial agreements and the local system in case of severe disputes. This by no means ensures that disagreements won't arise. It simply means that the mechanisms for dealing with them are well known and present little or no blockchain-specific aspects or challenges.

The situation is somewhat less straightforward with community-run, public, permissionless blockchains, where rules and enforcement mechanisms must be more organic. In terms of the project governance rules and processes, most community-run blockchains fall back on tradition, taking their cue from the open source movement. The Bitcoin Improvement Proposal (BIP) process, by which anyone can propose upgrades to the Bitcoin protocol, is for instance consciously copied from the Python Enhancement Proposal (PEP) process in use by the open source Python programming language community.[11] This is hardly surprising, as these processes are familiar to many developers, and have been proven to work.

In open source, the absence of formal enforcement processes leaves people free to operate with a significant amount of leeway. That said, most open source code repositories have an embedded licence agreement (GPL, LGPL, MIT) which specifies certain limitations in terms of how the code can be altered and used, and the liabilities of the code contributors in case of usage of the code by a third party, including copying the source code and making their own alterations. Such a process can even be good for innovation, allowing variants to arise and prove themselves. In the case of blockchain protocols, which tend to hold value (often billions of dollars' worth), the stakes can, however, be very high. So what keeps a public, permissionless, value-holding blockchain coherent? There are two somewhat opposing

11 BIP Purpose and Guidelines, Github.

answers. One is that there are often very strong monetary and other incentives for stakeholders to coalesce around a single decision despite what can be strong disagreements.[12] The other answer is that "nothing holds them together". If someone does not like the majority's decision, it is easy to split off and create a new version of the blockchain, a process known as "forking". Such forks happen all the time. Like a spoken language, the ultimate authority of what the real chain is, or where the real value lies, is usage. This may sound precarious if one happens to have several hundred thousand or million dollars worth of value locked up in the blockchain, yet in Bitcoin and other blockchains, usage has proven a remarkably effective governance tool. That said, contentious blockchain forks can be dramatic affairs. We return to this subject later on in the section "Enforcing decisions: Governance by fork".

GOVERNANCE CHALLENGES AND CONTROVERSIES IN PUBLIC, PERMISSIONLESS BLOCKCHAINS

In this section we sketch some of the more prominent governance challenges and controversies in blockchain that anyone delving into the subject is likely to come across. Our focus here is primarily on public, permissionless blockchain protocols. In the section "Governing blockchain consortia", we examine governance challenges in enterprise blockchain, which is largely the provenance of permissioned protocols.

12 We saw this clearly in the disputes around SegWit in Bitcoin, and the subsequent New York Agreement. See Bitcoin scaling agreement at Consensus 2017, Digital Currency Group, 23 May 2017.

Encoding the rules: The on-chain vs off-chain governance debate

Anyone who delves into the turbulent waters of public blockchain governance will surely come across the great debate between on-chain and off-chain governance.[13] Proponents of on-chain governance for blockchain projects believe that the rules for changing the protocol should be hard-coded into the protocol such that all decisions can be made and implemented on-chain, generally through some sort of voting process. Such rules typically refer to the percentage of approval needed for a suggestion to become a new rule, and they can vary from protocol to protocol. Devising the rules thus becomes a process of "deciding how to decide".

Proponents of this method believe that if the rules are well conceived, then on-chain governance offers the fairest, most flexible, most transparent, clearest type of governance – one that mitigates the vagaries of human decision-making. They also feel that, compared to off-chain governance, on-chain governance is most true to the blockchain ethos of decentralisation, among other things because it mitigates undue influence by individuals or cabals. The rallying cry here is "code is law". If users are not happy with the rules enshrined in the code, or the results of decisions taken that way, they can choose to opt out and use another blockchain.[14]

Proponents of off-chain governance believe

13 An excellent source for diving more deeply into the subject is to follow the debates between Gavin Wood and Vlad Zamfir. A good overview of the material can be found here: The Wood-Zamfir Governance Debates, CryptoLaw Review, 28 November, 2018.

14 For the on-chain point of view, see Substrate, Polkadot and the Case for On-Chain Governance, Epicentre Podcast, Episode 259.

that it is wiser for decisions to be made in formal and informal processes among the community of stakeholders, including indirect stakeholders. Among other things they argue that it is difficult if not impossible to hard code rules able to deal with all possible contingencies, that therefore "code-is-law" is not workable in real life because it is too rigid, while off-chain governance is more flexible. They also believe that far from mitigating against undue influence, mechanisms based on voting, in particular coin voting, are susceptible to domination by plutocrats, bribery, or voter apathy. Off-chain governance, they maintain, is also a better way to get input from the widest circle of stakeholders, including those who don't necessarily use the blockchain or are not sophisticated or knowledgeable enough to take part in on-chain governance.[15]

While we do not have a definitive answer regarding what model will win (and we should not stifle innovation at this early stage), we can suggest that a practical compromise may be useful in many situations. Namely, in the name of effectiveness and efficiency, it is highly desirable to design a platform in such a way that most roles, permissions, access rules and business logic are automatically and digitally implemented. This does not necessarily mean that automated rules trump the rule of law, simply that they aim to streamline the vast majority of transactions between participants. More traditional commercial agreements or consumer protection laws can still apply when legally required to deal with edge cases and severe disputes that require human interpretation in order to determine responsibility and the extent of the damages incurred by a party.

That said, we would point out that the question of the extent to which code can and/or should be law, while not necessarily new, has become much more prominent since the advent of blockchain. Decentralisation through blockchain and automation through smart contracts have led to fancies in some quarters of algorithmically determined governance for any number of situations, including human society at large. Exploring to what extent this is possible or even desirable, and where the borders are, may be one of the more important legacies of the blockchain movement.

Balancing incentives: Game theory and the new science of token economics

We saw above that public, permissionless blockchains depend to a great extent on the right mix of incentives, whether positive or negative. For many, the great breakthrough that Satoshi Nakamoto made was not in the technology – much of the technology in Bitcoin is well known and predates it – but in its incentive structures. It's no surprise then that designers of blockchains think a lot about how incentives work. To do this, they often turn to fields of study outside computer science. Game theory, for instance, is very important – no blockchain architect can afford not to be steeped in its arcana. Economics is important too, and in particular the new sub-field of token economics, which has been invented largely by and for the use of blockchain developers and entrepreneurs.

This makes sense. In a network with no central authority, people need a reason to do the work

15 For the off-chain governance point of view, see Against on-chain governance, Vlad Zamfir, Medium, 1 December, 2017.

as well as a reason to behave. If a blockchain is to be successful, users need to believe that the incentive structures will indeed result in a trustworthy network. The incentives behind a blockchain do not always have to involve money, though in permissionless networks they often do. To be successful, they have to be strong and have to achieve the right balance between the interests of all stakeholders. This is no trivial task.

It should perhaps be pointed out in this context that there are also many systems where a central authority relies on game theory and monetary incentives in order to influence participant behaviours and make the overall ecosystem more fluid and efficient. Examples abound (tax incentives, government incentive programmes, rules of membership in clearing counterparties in the capital markets, central bank monetary policy), that enable regulatory bodies to influence whole ecosystems via the law of large numbers so that they can deal only with edge cases and severe market distortions.

Enforcing decisions: Governance by fork

Governance is about coordination. Yet having the best laid governance structures does not always mean that insurmountable disagreements will not arise. In traditional settings, disputants can turn to mediation or the courts to solve their differences. While the time-tested processes of open-source software make it possible to rely on some established governance to settle most day-to-day decisions (this is the responsibility of the code maintainers, sometimes with oversight by a technical committee), it is always possible for a significant portion of the users or contributors to decide that they will break away from the established governance and establish a new one. In this case, the main way to deal with irreconcilable differences is through a split. In the blockchain world, such splits are referred to as “forks”.

A blockchain fork is a split in the chain caused by a change to the underlying protocol. There are any number of reasons why a blockchain community might want to introduce such changes, running from upgrading the security of the protocol and fixing bugs to introducing new consensus rules. Forks can be tricky affairs on permissionless blockchains in particular, as there is no mechanism to force nodes to upgrade and nothing to stop different groups in the community from introducing different upgrades.

There are two main types of forks. A “soft fork” is backwards compatible: it introduces new features but still works with the older versions of the software. That means there is no split in the underlying ledger and transaction history. Soft forks are generally seen as positive and necessary for blockchain development since they allow for upgrading the technology and security features of a blockchain.

A “hard fork” introduces a new version of the protocol that is not backwards compatible. If not everyone upgrades, then the blockchain ledger will split in two as from the moment of the introduction of the new version there will be two different transaction histories based on different protocol rules. Some hard forks are seen as necessary tools for upgrading the platform too, and are accepted by the majority of the community. Ethereum’s planned Byzantium hard fork in 2017 is an example of such a “non-contentious” hard fork. Other hard forks result from disagreements in the community, and result in a permanent split in the chain and divergence into two often competing blockchains that share a common history only up to the point of the fork. The Ethereum DAO fork, which caused a split into

GOVERNING BLOCKCHAIN PROTOCOLS

Ethereum and Ethereum Classic, is an example of such a "contentious" hard fork.

Are forks good or bad? The answer is, it depends. Most forks are benign, and simply denote an upgrade to the protocol. Contentious hard forks can, however, indicate major schisms in the community and are usually accompanied by intense public arguments carried on with religious fervor.

Some see forking as an important blockchain governance tool, the expression in code of the "you are free to opt out" principle. Being able to opt out is of course an important governance parameter in any system. But governance by forking can be a dangerous game. Public blockchains must maintain the trust of their users to survive. A contentious fork can destroy that trust very quickly. This can make not the fork itself, but the threat of one, a powerful governance tool too, by forcing disputants to agree or risk destroying all they have invested in the platform.

The unpredictability of forks on permissionless blockchains could, however, become a significant impediment for using such blockchains for business purposes. It happens in particular when the uniqueness of electronic data (electronic records) is a critical factor. For example, a token issued on a blockchain could represent an obligation to pay a certain amount of money (a debt) in off-chain legal relations. A split of the chain causes that instead of one token, two identical tokens appear on each of the new chains. Immediately after the split the fork is completed, both the identical tokens (on both chains) are in hands of one person, but the holder is able to transfer each of the tokens to two different persons. Each of these persons could acquire a legal title to claim for a payment (off-chain) from a debtor. This risk is important especially if tokens embody/incorporate securities.

From a practical standpoint, we should observe that major forks generally happen at the early stage of a technology, when the pace of innovation is still high and there are significant debates as to the ultimate direction of the project. Over time, when there is significant adoption of a technology, the incentives for participants to break away from the majority fork are much lower. There are many examples of open-source technologies that have prospered for decades once they have reached significant adoption (e.g. Java, Javascript, HTML, SQL, MongoDB).

Governing blockchain consortia

BLOCKCHAIN FOR ENTERPRISES

Not long after the success of Bitcoin showed that it was possible for large groups of strangers to cooperate on an open source platform for the exchange of value, people began to see that the same technology could be used to allow businesses to build a common infrastructure for value and information exchange in a specific market or industry. This catalysed the rise of enterprise blockchain protocols engineered to serve these needs. The main (but not the only) difference between enterprise blockchain and public blockchain is a focus on features necessary to businesses, for example access control. Enterprise blockchains are therefore almost always permissioned, meaning nodes and, often, users have to be onboarded and their identities are generally known to all.

With these tools in hand, over the past five years or so different groups in many different industries have started projects to build common, blockchain-based business platforms. These groups are often referred to as blockchain consortia, and generally consist of mid- to large-sized companies. In the following sections we discuss the governance challenges faced by such consortia across the typical project lifecycle. Many of the observations here would apply, however, to any type of project where a group – a local community, a government agency, a non-profit, etc. – comes together to build a blockchain-based platform.

GOVERNANCE CHALLENGES AND OPPORTUNITIES FOR BLOCKCHAIN CONSORTIA

Initial conception: Why this project? Why blockchain?

Blockchain consortia tend to be born of shared business problems. Before doing anything else, companies considering a blockchain consortium should a) be clear about what their shared problem is, and b) determine if blockchain is the right technology to solve it. While there are many different factors at play, there are several criteria that make a problem a good candidate for a blockchain solution:

- **Reluctance to rely on a third party.** Shared industry utilities, run by a third party for industry stakeholders, are nothing new. But in many cases, there can be a reluctance on the part of industry participants to appoint a third party as the single source of truth, for fear that that party would gain outsized power from the information derived from transactions. Where this is the case, blockchain can offer an alternative.
- **Group consensus on information.** Businesses – whether partners, competitors, or both – need to constantly share information in order to transact. One option is to do this directly with each other. This, however, can lead to expensive reconciliation processes and redundancies. Another option is to use a trusted third party, perhaps an industry utility or a service provider, to act as a clearing house. But this involves costs and requires trust in the competence and honesty of the third party. Most industries also rely on data standards, but these are not always

GOVERNING BLOCKCHAIN CONSORTIA

available or complete. Blockchain offers an option for stakeholders in a market to share an infrastructure built for group consensus and sharing of business data. A common blockchain platform can also be a good catalyst for agreeing on, or completing the development of, data standards.

- **Track and trace of objects and information.** Most business processes require track and trace, either of objects or of information. That is why supply chains are one of the most popular use cases for blockchain.[1] Blockchains are good for creating a trusted, common record of provenance and movement of both products and data.
- **Immutability of information.** Immutable distributed ledgers provide excellent, trusted audit trails that can be both shared and kept up to date almost in real time. Such audit capabilities can provide better transparency in a market, helping to identify bottlenecks, provide better market intelligence, and otherwise increase the value of the network to its stakeholders. Audit trails are also useful for settling business disputes and can greatly simplify regulatory compliance processes and costs.
- **Digitisation and document sharing.** A mundane but often crucial component of many business processes is document sharing. While most industries are digital to some degree, this often does not go beyond sharing PDF documents. With blockchain, digital documents can be hashed, sealing them against tampering and providing them with a unique ID. They can then be stored on the chain, either in full or simply by reference to the hash. This can provide a common, trusted document library with its own audit trail. Blockchain-based documents, including contracts, can also in theory be made interactive and dynamic, linked to outside data sources and containing their own business logic.[2]
- **P2P transactions and (near)-immediate settlements.** Blockchains are by their nature peer-to-peer transaction environments. The advantage to businesses of transacting on a blockchain are in immediate, or near immediate, transaction finality, which can reduce or eliminate counterparty risk (freeing capital) and also reduce or largely eliminate reconciliation or other back office costs.
- **Shared/automated business processes and workflows.** Smart contracts run on a blockchain can be used to automate business processes and transactions, from simple escrow arrangements to complex workflows. Automation can be a big driver of efficiency gains and cost reduction.

While the above represent a strong set of advantages, before considering a blockchain consortium potential members should be clear on exactly how much benefit, whether in cost reduction, capacity increase, or in other measurable ways, they can expect. And while it is not necessary to spec the whole project right away, it probably makes sense to have a rough idea of what the specific blockchain solution might look like, either by working with an expert or talking to members of similar consortia that are already running. Building a blockchain platform is not without its own initial investment costs, while building a consortium often requires members to get used to new ways of working. It is therefore best to be clear on the benefits and to keep these as a guidepost as the project matures

1 Blockchain in supply chain and trade finance, EU Blockchain Observatory and Forum, 9 December 2019.

2 See for instance OpenLaw for smart legal documents on Ethereum, openlaw.io, or the Accord Project for a similar effort on Hyperledger Fabric, accordproject.org.

and – as is inevitable with any project – encounters difficulties.

Inception: Setting up the consortium

Assuming members of the potential consortium agree on the value of a blockchain, they will next have to set up a formal organisation for the project. For enterprise blockchain consortia, this almost always means some kind of legal entity. There are different options, including partnerships via memorandum of understanding (MoU), associations, partnership via a private entity, foundations, or even contracting with a private entity to build and run the project.

We would note here that there are empirical success factors when it comes to the size of the founding consortium. Too small (one or two parties), and there is often suspicion by ecosystem participants that the project is going to give outsized competitive advantage to a few parties. Too large (more than 20 parties), and there is a risk that the founding team will face insurmountable red tape and decision fatigue. Founding teams of between five and 20 large institutions seem to be the sweet spot to get an alliance going, until more members can be welcomed into the ecosystem.

The choice will depend on the stakeholders and the goals of the project. Today we are generally seeing a trend towards private companies with stakeholders as shareholders and a dedicated executive team, staff and in-house developers.

There are several reasons for this. This structure is well known and comfortable to many. A private company can also move quickly in terms of decision-making, especially in the context where the company needs to drive significant technology innovation, fast, in order to be relevant in the marketplace. With a private company individual shareholders can also jointly own the IP rights and, if the platform is successful, potentially monetise that IP by turning the technology into a product for others to use.

Other organisational options are, however, popular too. We have seen successful consortia set up and run by a single, often dominant, market player and opened up to others for use, and others set up and run by technology vendors as a subscription-based product. There are also associations for larger-scale consortia looking to build more public-oriented, open blockchains. While probably not yet mature enough for enterprise use, some see Decentralised Autonomous Organisations (DAOs) as a potential option for blockchain consortia (we discuss DAOs below in the section “Blockchain for decentralised organisations (DAOs)”).

Off-chain governance: Establishing and running the project

With the organisation in place, the next step is to establish the project governance. Unlike with community-developed public protocols, consortia governance setups will almost always be off-chain, using standard business practices and agreements.

On the business side, the purpose, goals and values of the project should be expressly stated. Governance structures should balance the interests of all stakeholders, and the decision processes and criteria should be crystal clear. The same is true of all financial arrangements, both in terms of investment and, if there are any, distribution of profits. There should be clear rules for who can join

the consortium after it is running and what the process is for members to leave. It should be clear who owns the IP coming out of the project and what metrics will be used to measure success. Partners should be clear on how they intend to manage risk and deal with liability issues if things go wrong. All of this should be formalised in strong legal terms and conditions, but these agreements should also leave room for flexibility as blockchain is a new technology and both it and the blockchain ecosystem are evolving quickly.

In terms of project management, partners should agree ahead of time on how technical decisions will be made and by whom, what the technical roadmap is, how development and testing will be carried out, and what the go-live criteria are. Plans should also be laid for how the network will be managed when it is live. For this, it often makes sense to create a central pool of resources dedicated solely to the project and that can be shared by all, either by having each member second resources or by creating a separate entity and moving resources into it.[3]

On-chain governance: Designing and running the network

Stakeholders will of course have to decide what kind of platform they want to build, and what kind of a blockchain they want to use to build it. Among the important considerations are:

- **Access – who can use the network.** In an enterprise setting the assumption is that the blockchain will be private, meaning access is restricted to authorised users, usually members of the consortium. But this need not always be the case, for instance when a consortium wants to build a platform run by the consortium but open to retail clients. Either way, planners will need to have a good understanding of both who will be able to access the data on the blockchain (read permissions) and who can submit transactions (write permissions), and how these people or entities are going to be vetted and onboarded.
- **Validation – who can run a node.** Another assumption, which we think will almost always be the case, is that an enterprise blockchain project will be permissioned, meaning only authorised entities can run a node and do the work of validation. The question then becomes: are all members of the consortium able to run a node or not? If yes, are they required to run a node, or is this optional, with members allowed to choose not to be validators or to delegate their validation responsibilities to someone else (for instance another consortium member)?
- **Performance.** Consortium members will also want to consider how performant the network needs to be. Do they expect a high volume of transactions with heavy data transfer, or will volumes perhaps be lower, for instance with small numbers of high value transactions? What are the security needs in the network? Performance requirements will have a direct bearing on the choice of blockchain technology. For example, different consensus mechanisms have different properties depending on how many nodes are involved, and so are more or less suitable depending on the environment.
- **Identity.** A permissioned blockchain,

3 See the Peter Broadhurst presentation in Scalability, Interoperability and Sustainability Workshop Report, EU Blockchain Observatory and Forum, 14 November 2018.

whether public or private, will need a strong identity concept. This will have to take into account vetting of participants, onboarding, issuing identities and using them in the network, as well as balance member needs for confidentiality and transparency (see next point).

- **Data transparency/confidentiality.** Many of the advantages of blockchain we mentioned previously, for example immutability, provenance of data and audit trails, are valuable because of the high levels of transparency they offer to network participants. Yet such transparency is not always desirable, for example because it threatens to expose business secrets. While some newer technologies, like zero-knowledge proofs, may offer ways to square the circle between confidentiality and transparency, these technologies are still very new. To build a successful consortium, members will need to agree on the appropriate tradeoff between these two poles, and develop a concept to maintain the desired balance.
- **Interoperability with non-blockchain parts of the network.** In enterprise blockchain networks, the blockchain itself is often a surprisingly small part of the technology stack. It forms a foundation, but it is not necessarily where most of the activity happens. Designers need to ensure that the blockchain can seamlessly plug in to these other layers and interoperate with them.
- **Maintaining decentralisation as a project goal.** On a final note, considering the complexities involved, it can be tempting to fall back on centralised workarounds, either technical or in terms of the project governance. Consortium members should always keep in mind the expected added benefit of decentralisation that drove them to decide on a blockchain solution in the first place, and which justifies the extra effort involved. Otherwise, as one presenter pointed out at our Scalability workshop, you risk having "just another database".[4]

THE DECENTRALISED PROJECT MINDSET

As we have seen, blockchain technology adds value if and where decentralisation makes sense in a business context, but involves new approaches to technology and business processes. We close with a few observations on the more human challenges around adapting to a decentralised mindset.

- **Co-opetition.** A blockchain consortium very often involves competitors coming together to cooperate on building a new platform. This is often easier said than done. The executive management of the individual consortium members should have a clear idea about what this kind of co-opetition means for their organisation, and be prepared to accept its potential difficulties.
- **A different project environment for the IT staff.** A similar challenge faces development staff. As we have mentioned, it is recommended to have some kind of dedicated, centralised, cross-funded IT infrastructure to develop and run the platform for the consortium. This can very well be staffed by members of the IT departments of consortium

4 Op. Cit.: Peter Broadhurst presentation in Scalability, Interoperability and Sustainability Workshop Report, EU Blockchain Observatory and Forum, 14 November 2018.

members. Designing and implementing decentralised infrastructure can, however, mean new skills and practices for many IT departments, many of which are not used to collaborating on a large scale outside their organisations.

- **Shareholders are also customers.** One interesting characteristic of many consortia that is worth noting is the fact that, because the consortium is building a platform for its own use, the shareholders are often also the customers. This has two implications. First, it means that the shareholders have a vested interest in promoting the platform to all their business partners, which is a key driver of adoption. Second, it means that shareholders should be quite open, from the get go, to diluting their participation in the entity, in order to welcome institutional users who are likely to be critical to the adoption of the platform by ecosystem participants.

Using blockchain for governance

In this section, we turn the tables to look not at how to govern blockchains but rather at how to use blockchains to solve real-world governance challenges. We provide a few sample use cases in this regard based on a number of real-world projects, mostly as presented in our Governance workshop.[1] For details on the projects themselves, please consult the appendix.

ON-CHAIN DISPUTE RESOLUTION

The law is one of humanity's great inventions, and the ability to equitably resolve disputes one of the pillars of functional societies and economies. Yet today's methods of dispute resolution can leave a lot to be desired. Legal systems and the courts are generally slow and are often very expensive. Being run by humans, they can suffer from intentional or, more often, unintentional biases. The processes are often complex and hard to understand for normal people. These processes can also be extremely slow to operate, causing significant damage to ecosystem participants. For example, it may not be optimal for an SME to rely on traditional dispute resolution with a large company, if the dispute resolution is going to take several years, after which they may be driven out of business anyway.

Since its early days, people have been looking at blockchain as a way to automate legal processes, including claims that one day we may be able to completely replace the human legal system with an algorithmically run, blockchain-based alternative. While the age of the robo-judge may be a while away, there are projects that are starting to tackle smaller, more manageable parts of the law.

One of these areas is dispute resolution. In the normal course of business disputes arise all the time. The classic example is of a dispute between a freelancer and a client about the adequacy of the delivered product. In a simple blockchain-based dispute resolution system, at the beginning of the project, both the freelancer and the client could lock the funds for the fee in a multi-signature blockchain-based smart contract that acts as an escrow account. If all goes well at the end of the job, then both parties could use their private keys to release the funds. If there is a dispute, the smart contract could also contain a clause that automatically sends the case to arbitration. Such arbitration itself could also take place on the blockchain. For example, cryptocurrencies could be used as a way to incentivise individuals to act as arbitrators, using various game theoretic and token economic techniques to help ensure they act fairly. The platform could also contain mechanisms for appeals and the like. The advantages of such a system include the fact that it is likely to be relatively swift, relatively inexpensive, and highly transparent. While there will always be one party unhappy with the result, compared to traditional mechanisms to adjudicate such disputes, the process would at least be relatively painless.

1 Governance and New Organisational Challenges Workshop Report, EU Blockchain Observatory and Forum, 28 June 2019.

USING BLOCKCHAIN FOR GOVERNANCE

BLOCKCHAIN FOR VOTING

Voting is perhaps the most basic of governance challenges, whether in representative government or among informal groups, associations and organisations. E-voting has a lot of appeal, including ease of use and the potential for a more transparent and less corruption-prone voting process. But e-voting is also very controversial, with many worried that – contrary to the claims of its proponents – e-voting systems could be easily abused for voting fraud. Many proponents of e-voting look to blockchain as a possible way to address these concerns, and we are seeing more and more projects working on blockchain-based voting platforms. Some of the use cases include the following.

E-voting in representative government.[2] Today's elections are still for the most part carried out on paper ballots or electronic voting machines, often developed by private companies. Such processes can be slow and, as we have seen famously in elections in the US and elsewhere, can be prone to error. While meant to be anonymous, in reality votes cast in centralised systems are often traceable to entries on voter registration rolls. The security of the secret ballot therefore lies in the hands of election officials, whom the electorate must trust. Trust in voting systems is, however, eroding. It is often said that young people, used to a digital lifestyle, can in particular be turned off by what seems to them 'archaic' voting methods.

Blockchain-based voting recorded on a distributed ledger could offer a tamper-proof, verifiable record of votes, while providing voters with both a verifiable record of their vote being cast and, potentially, an easy means to assure themselves their vote was counted. By moving the vote from a centralised paper ballot or voting machine onto a decentralised blockchain network, the vote count could be spread out among many different validators. For example, nodes could be run by the different political parties as well as election commissions, each with an incentive to ensure the vote was fair. Blockchain-based e-voting systems could be built on open source software, making the source code auditable as well. A secure blockchain-based e-voting system could also make it feasible to vote via decentralised apps on a phone, making voting easier, and potentially enticing more young people to participate.

These are all major advantages, but to date have remained more theoretical than real. Above all, true anonymity on blockchains remains a puzzle still to be solved. And there are many issues with e-voting that blockchain alone cannot solve. Chief among these is the danger of coercion if voting is done on a dApp instead of at a polling place.[3] And while blockchain networks are robust because they are distributed, blockchains face cybersecurity issues like any other digital technology. Should, for example, in future a means be found to crack the cryptography used on a distributed ledger – a distinct possibility – then the records of previous elections could be exposed.

Smart participation. Smart participation is about creating trustworthy platforms for

2 For more see Curran, Kevin. (2018). E-Voting on the Blockchain. The Journal of the British Blockchain Association. 1. 1-6. 10.31585/jbba-1-2-(3)2018 and What if blockchain technology revolutionised voting?, Philip Boucher, European Parliamentary Research Service, September, 2016.

3 This issue is not specific to blockchain, but more broadly related to all modalities of remote voting. However, at some point it is also important to weigh and scientifically test the implications of both models - an in-person voting system with low participation, and a remote voting system with potentially higher participation.

people to take part in civic decision making, for example voting on proposals for local projects, on budgets or even legislation. This makes it a variant of e-voting, with the difference being that there would seem to be more leeway in terms of provisions for anonymity or transparency. While security would be a major concern in terms of protecting user identities, if consultative votes are somehow compromised, the damage would not be nearly as bad as it would be in a political election. Smart participation is therefore a good candidate for experimentation in blockchain-based e-voting.

Liquid democracy. Liquid democracy is a combination of representative democracy (where people vote for representatives at intervals) and direct democracy (where citizens vote individually on everything). In liquid democracy every citizen has one vote, but voters can at any time delegate their vote to another voter (called a proxy), either for a specific issue or for a category of issues. Importantly, this delegation can be revoked at any time. Blockchain adds cybersecurity, immutability and traceability to these systems.

Quadratic voting and finance. A new take on voting that is gaining popularity, and for which blockchain is being used, is quadratic voting and finance. Based on the work of economists Glen Weyl and Eric Posner as laid out in the book Radical Markets,[4] these represent a new take on voting and decision making designed to capture not only voter's opinions, but also how strongly they feel about them. In quadratic voting, voters receive a number of voting credits for which to buy votes. They can put as many of these votes as they like on any given issue, but the price of each vote goes up quadratically (the number is multiplied by itself) when votes are cast for the same thing. Two votes for one issues cost four credits, ten votes cost 100. This forces people to consider carefully the issues they care about, and captures not just people's preferences, but also the intensity of those preferences. These ideas have been popular particularly in the Ethereum community, where Ethereum founder Vitalik Buterin has collaborated often with Weyl in building out these ideas. One fruit of their work has been quadratic finance,[5] a method of deciding matching grants based on the number of donations, not the amount. Both quadratic voting and quadratic finance have been tried out in live settings (see appendix).

BLOCKCHAIN FOR CORPORATE GOVERNANCE

Another popular use case is blockchain for traditional corporate governance. Today shareholders in corporations mostly vote through proxies. Proxy voting has issues of transparency, information asymmetries, and errors.[6] Blockchain has been suggested as a potential solution to help bring more transparency to the overall process, letting individual shareholders more easily either cast votes remotely or track their votes by their proxies, while at the same time offering ways for large shareholders who prefer to remain anonymous to cast their votes without revealing identities. The transparency, trust and ease of use of blockchain-based corporate voting systems could also theoretically be used to make corporate governance more inclusive, by making it easier to include the voice of employees and customers.

4 Radical Markets, Uprooting Capitalism and Democracy for a Just Society, Eric A. Posner and E. Glen Weyl, Princeton University Press, 2018.

5 Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds, Vitalik Buterin, Zoë Hitzig, E. Glen Weyl, revised 31 December, 2018.

6 How can Blockchain Tackle Issues in Proxy Voting, Josiah Nakori, 31 January, 2020.

USING BLOCKCHAIN FOR GOVERNANCE

BLOCKCHAIN FOR DECENTRALISED ORGANISATIONS (DAOS)[7]

One important governance trend born of the blockchain movement – and still largely confined to it – is that of the decentralised autonomous organisation (DAO). This is a topic we addressed in some detail in our paper on the blockchain legal and regulatory framework,[8] but it is worth mentioning also in the governance context.

The concept of a DAO originated in a blog post by Dan Larimer in 2013,[9] who observed that Bitcoin acted like a decentralised autonomous corporation (DAC), and the idea was later expanded upon by his father Stan.[10] The term DAO first appears in the Ethereum White Paper,[11] where it is described as "long-term smart contracts that contain the assets and encode the bylaws of an entire organization."

Today, a DAO is generally understood as an organisation governed not by people but by code, so that its rules are transparent and immutable and can be expected to execute as written with no need for human involvement and no possibility of human meddling. In practice, most DAOs have a smart contract bylaws infrastructure but use the mechanics of human voting and suggestions as the main governance tools.

Most current DAOs involve the managing of assets by a group, but by extension a DAO could be used to manage any kind or organisation or group endeavour by encoding corporate governance, bylaws, work processes, and even bank accounts into a smart contract. This would in theory obviate the need for a CEO or any other management function, as the DAO would manage its own funds and resources.

Unfortunately, one of the earliest and most well-known of DAOs – dubbed simply The DAO – ended in failure due to a bug in the code.[12] Despite this bad first impression, the idea of a DAO has remained inspirational to many. Since the first DAOs, we have seen proposals for decentralised ICOs (known as DAICOs), DAOs used for grants to support software developments, DAOs used to manage stable coin platforms, and lately attempts to build legal, regulated DAOs under the heading Limited Liability Autonomous Organisations or LLAOs. Activity is so strong, that some have predicted 2020 will be the year of the DAO.[13] That will remain to be seen. However, it is hard to imagine any concept more true to the decentralised ethos of blockchain, or one that more directly addresses governance issues, than that of the DAO.

7 This section is heavily indebted to Decentralized Autonomous Organizations (DAOs) as subjects of law: The recognition of DAOs in the Swiss legal order, Sven Riva, Master's Thesis, Master of Law, University of Neuchâtel, October, 2019.
8 Legal and regulatory framework of blockchains and smart contracts, EU Blockchain Observatory and Forum, 17 September 2019.
9 The Hidden Costs of Bitcoin, Daniel Larimer, LTB Network, 7 September, 2013.
10 Bitcoin and the Three Laws of Robotics, Stan Larimer, LTB Network, 14 September, 2013
11 Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform, Vitalik Buterin, 2013.
12 The Story of the DAO – Its History and Consequences, Samuel Falkon, 24 December 2017.
13 Narrative Watch: Why 2020 Will Be the Year of the DAO, The Breakdown with NLW Podcast, 9 January, 2020.

Conclusion and recommendations

As we hope we have shown, governance in blockchain is a vast topic – and one which we could only hope to touch on at a high level here. Whether on the protocol or project level, getting governance right will be a key element to enabling the blockchain industry and supporting mass adoption. For this reason, supporting good governance in the space should be a priority for policy makers. Below we make a few recommendations. Since – as we noted at the beginning – we have touched on governance topics in many of our previous workshops and papers, several of these recommendations reference previous work.

1. Prioritise research into governance-related topics.

As we have seen, the governance topic in blockchain is very broad, and there are still many open issues. There is a need in the community for more information and insight. In our Research Priorities Workshop[1] participants suggested that policy makers make blockchain and decentralised governance a research priority in Europe, whether in the governance of applications, networks or the question of on-chain versus off-chain governance. We concur, and so reiterate the observation here.

2. Collect and communicate best practice.

As more information is available from researchers and also the experience of live projects, we think policy makers could support the community by collecting and disseminating the results so that others can benefit from the knowledge.

3. Clarify the regulatory framework for blockchain consortia.

In our Conclusion Workshop[2] it was pointed out that blockchain consortia face some specific hurdles. Filing processes, especially for multi-regional consortia, can be quite complex and difficult to finalise. One way governments could help facilitate the launch of blockchain consortia is to streamline these registration processes.

4. Clarify the legal and regulatory framework around DAOs.

In our paper on the legal and regulatory framework of blockchains,[3] we have a very long passage on DAOs, where we point out many of the unique aspects of these new types of organisations, and raise the possibility of potentially creating a new kind of legal structure or special regulation. Here too we would like to reiterate the point, and suggest that policy makers continue to educate themselves and consider the regulatory implications associated with existing types of contracts.

5. Continue to examine how blockchain could play a role in e-governance.

E-voting, citizen participation and other forms of e-governance are promising ways to foster and innovate in participatory democracy. Here too there are many legal, regulatory and policy questions that need to be addressed, both in general and in terms of using blockchain in such contexts.

1 Research priorities - Workshop report, EU Blockchain Observatory and Forum, 30 April 2020.

2 Conclusion workshop report, EU Blockchain Observatory and Forum, 6 May 2020.

3 Op. cit. Legal and regulatory framework of blockchains and smart contracts, EU Blockchain Observatory and Forum, 17 September 2019.

Appendix 1: Blockchain protocols

Below is a list of some prominent blockchain protocols and infrastructure projects. It is meant solely as an aid to the reader interested in learning more about specific projects. Inclusion in this list is purely illustrative, and **not meant to be an endorsement of any kind by either the EU Blockchain Observatory and Forum or the EC**. In most cases there are many other possible choices that could have been made. The list is in alphabetical order.

- Algorand: https://www.algorand.com/
- Bitcoin: https://bitcoin.org/en/
- Cardano: https://www.cardano.org/
- Cosmos: https://cosmos.network/
- Dfinity: https://dfinity.org/
- Ethereum: https://ethereum.org/
- Enterprise Ethereum Alliance: https://entethalliance.org/
- Hashgraph: https://www.hedera.com/
- Hyperledger: https://www.hyperledger.org/
- IOTA: https://www.iota.org/
- Libra: https://libra.org/en-US/
- Polkadot: https://polkadot.network/
- Quorum: https://www.goquorum.com/
- R3: https://www.r3.com/
- Tezos: https://tezos.foundation/

Appendix 2: Blockchain consortia

Below is a list of some blockchain consortia representing different governance models.

- **Liquidshare** (liquidshare.io) is a French fintech founded by nine banks and financial industry infrastructure providers that is using blockchain to create a new post-trade infrastructure for SMEs. It is organised as a private company governed by a Board of Directors. Each member has a seat on the Board, and all Board decisions must be unanimous.
- **Komgo** (komgo.io) is a fintech company consortium founded by 15 of the biggest players in the oil trading industry that uses blockchain to eliminate paper processes and streamline trades. It is organised as a joint venture of its shareholders, with clear separation of roles between the oversight responsibilities of the Board and the executive responsibilities of the Management Team whose mandate is to create value for the shareholders by way of creating value for the industry.
- **Alastria** (alastria.io) is a large-scale project to build a public, permissioned, all-purpose blockchain platform for the country of Spain. It is organised as a non-profit organisation and any organisation or individual in Spain can become a member, which confers both the right to run a node and participate in the platform governance through the General Assembly and various subject-specific commissions.
- **IBM Food Trust** (ibm.com/blockchain/solutions/food-trust) is a blockchain-based network for the food industry that supports an ecosystem of producers, suppliers, manufacturers, retailers and others with the goal of "creating a smarter, safer, more sustainable food system for all." It has been built and is run by IBM and so on the one hand an IBM product – members pay to join the network. On the other hand, the ecosystem is participant-managed, with an Advisory Council made up of a range of industry representatives and tasked with setting the rules of engagement and ensuring accountability to those rules, as well as continually reviewing and adapting those policies as needed.

Appendix 3: Blockchain for governance projects

Below are a number of projects illustrating how blockchain is being used for various governance use cases.

On-chain dispute resolution

- **Kleros** (kleros.io) is a blockchain-based dispute resolution platform that connects users who need to solve disputes with arbiters (jurors) who have the knowledge and skills to settle the disputes.

E-voting in representative government

- **Zug e-voting.** The Swiss city of Zug conducted a now-famous blockchain-based e-voting in 2018. Afterwards, 79% of participants said they welcomed blockchain-based e-voting, with only 2% opposed. 52% said blockchain should be introduced to make e-voting easier and quicker.[1]
- **The US state of West Virginia.** The US state of West Virginia successfully used blockchain-based e-voting in state primaries and the recent midterm election using a dApp called Voatz. This was first tested in two counties, then in just under half the counties for absentee voting in a midterm.[2]

Citizen participation

- **Better Reykjavik** (reykjavik.is/en/better-reykjavik-0) is an online consultation forum where citizens are given the chance to present their ideas on issues regarding services and operations of the city of Reykjavík. Anyone can view the open forum and registered users who approve the terms of participation can participate in the forum.
- **Decidim Barcelona** (decidim.org) provides free open-source participatory democracy for cities and organisations.

1 Zug's Head of Comms Calls City Blockchain Voting Test a 'Success', Despite Low Turnout, Molly Jane Zuckerman, Cointelegraph, 3 July, 2018.
2 The experiment has not been without its issues. See What Really Happened With West Virginia's Blockchain Voting Experiment?, Slate, 11 July 2019 and West Virginia Ditches Blockchain Voting App Provider Voatz, CoinDesk, 2 March 2020.

APPENDIX 3: BLOCKCHAIN FOR GOVERNANCE PROJECTS

Liquid democracy

- **Flux Australia** (voteflux.org) is an Australian political party building a blockchain-based app to enable liquid democracy.[3]

Quadratic voting and finance

- **Democratic caucus of the Colorado State Legislature.** In 2018, the Democratic Caucus of the Chicago State Legislature used quadratic voting to help decide its policy priorities. The vote featured a blockchain-based app.[4]
- **Gitcoin grants.** Gitcoin has been experimenting with quadratic finance in its latest grant rounds to support Ethereum developers.[5]

Corporate governance

- **BoardRoom** (boardroom.to) offers a full blockchain-based corporate governance service on Ethereum.
- **NuArca** (https://www.nuarca.com/solutions-services/voting) offers a proxy voting dApp built on Hyperledger

3 Fore more on Flux see Flux FAQ and This Australian Party Has a New Voting Idea That Could Radically Change Politics, Simon Lewis, Time, 21 June, 2016.
4 Colorado Tried a New Way to Vote: Make People Pay–Quadratically, Wired Magazine, 16 April 2019.
5 Review of Gitcoin Quadratic Funding Round 4, Vitalik Buterin, Vitalik Buterin's website, 28 January 2020.

Appendix – Blockchain Terminology

What is a blockchain?
Blockchain is one of the major technological breakthroughs of the past decade. A technology that allows large groups of people and organisations to reach agreement on and permanently record information without a central authority, it has been recognised as an important tool for building a fair, inclusive, secure and democratic digital economy. This has significant implications for how we think about many of our economic, social and political institutions.

How does it work?
At its core, blockchain is a shared, peer-to-peer database. While there are currently several different kinds of blockchains in existence, they share certain functional characteristics. They generally include a means for nodes on the network to communicate directly with each other. They have a mechanism for nodes on the network to propose the addition of information to the database, usually in the form of some transaction, and a consensus mechanism by which the network can validate what is the agreed-upon version of the database.

Blockchain gets its name from the fact that data is stored in groups known as blocks, and that each validated block is cryptographically sealed to the previous block, forming an ever-growing chain of data. Instead of being stored in a central location, all the nodes in the network share an identical copy of the blockchain, continuously updating it as new valid blocks are added.

What is it used for?
Blockchain is a technology that can be used to decentralise and automate processes in a large number of contexts. The attributes of blockchain allow for large numbers of individuals or entities, whether collaborators or competitors, to come to a consensus on information and immutably store it. For this reason, blockchain has been described as a “trust machine“.

APPENDIX – BLOCKCHAIN TERMINOLOGY

The potential use cases for blockchain are vast. People are looking at blockchain technology to disrupt most industries, including from automotive, banking, education, energy and e-government to healthcare, insurance, law, music, art, real estate and travel. While blockchain is definitely not the solution for every problem, smart contract automation and disintermediation enable reduced costs, lower risks of errors and fraud and drastically improved speed and experience in many processes.

Glossary

The vocabulary used in the context of blockchains is quite specific and can be hard to understand. Here are the essential concepts you should know in order to navigate this breakthrough technology:

- **Node:** A node is a computer running specific software which allows that computer to process and communicate pieces of information to other nodes. In blockchains, each node stores a copy of the ledger and information is relayed from peer node to peer node until transmitted to all nodes in the network.
- **Signature:** Signing a message or a transaction consists in encrypting data using a pair of asymmetric keys. Asymmetric cryptography allows someone to interchangeably use one key for encrypting and the other key for decrypting. Data is encrypted using the private key and can be decrypted by third-party actors using the public key to verify the message was sent by the holder of the private key.
- **Transaction:** Transactions are the most granular piece of information that can be shared among a blockchain network. They are generated by users and include information such as the value of the transfer, address of the receiver and data payload. Before sending a transaction to the network, a user signs its contents by using a cryptographic private key. By controlling the validity of signatures, nodes can figure out who is the sender of a transaction and ensure that the transaction content has not been manipulated while being transmitted over the network.
- **Hash:** A hash is the result of a function that transforms data into a unique, fixed-length digest that cannot be reversed to produce the input. It can be viewed as the digital version of a fingerprint, for any type of data.
- **Block:** A block is the data structure used in blockchains to group transactions. In addition to transactions, blocks include other elements such as the hash of the previous block and a timestamp.
- **Smart contract:** Smart contracts are pieces of code stored on the blockchain that will self-execute once deployed, thus leveraging

APPENDIX – BLOCKCHAIN TERMINOLOGY

the trust and security of the blockchain network. They allow users to automate business logic and therefore enhance or completely redesign business processes and services.

- **Token:** Tokens are a type of digital asset that can be tracked or transferred on a blockchain. Tokens are often used as a digital representation of assets like commodities, stocks and even physical products. Tokens are also used to incentivise actors in maintaining and securing blockchain networks.
- **Consensus algorithm:** Consensus algorithms ensure convergence towards a single, immutable version of the ledger. They allow actors on the network to agree on the content recorded on the blockchain, taking into consideration the fact that some actors can be faulty or malicious. This can be achieved by various means depending on the specific needs. The most famous consensus algorithms include proof-of-work, proof-of-stake and proof-of-authority.
- **Validator nodes:** Validator nodes are specific nodes in a network that are responsible for constituting blocks and broadcasting these blocks with the network. To create a valid new block they have to follow the exact rules specified by the consensus algorithm.

Learn more about blockchain by watching a recording of our Ask me Anything session.