frontiers
in Blockchain

ORIGINAL RESEARCH
published: 17 September 2020
doi: 10.3389/fbloc.2020.575662

# From Athens to the Blockchain: Oracles for Digital Democracy

*Marta Poblet[1]*, Darcy W. E. Allen[2], Oleksii Konashevych[3], Aaron M. Lane[4] and Carlos Andres Diaz Valdivia[5]*

*[1] Graduate School of Business and Law and RMIT Blockchain Innovation Hub, RMIT University, Melbourne, VIC, Australia, [2] RMIT Blockchain Innovation Hub, RMIT University, Melbourne, VIC, Australia, [3] Erasmus Mundus Joint International Doctoral Fellow in Law, Science and Technology and RMIT Blockchain Innovation Hub, RMIT University, Melbourne, VIC, Australia, [4] Graduate School of Business and Law and RMIT Blockchain Innovation Hub, RMIT University, Melbourne, VIC, Australia, [5] Graduate School of Business and Law, RMIT University, Melbourne, VIC, Australia*

Oracles were trusted sources of knowledge for public deliberation in classical Athens. Very much like expert and technical knowledge, divine advice was embedded in the deliberation and decision-making process of the democratic Assembly. While the idea of religious divination is completely out of place in our contemporary democracies, oracles made a technological comeback with modern computer science and cryptography and, more recently, the emergence of the blockchain as a "trust machine." This paper reviews the role of oracles in Athenian democracy and, stemming from the renewed use of the term in computer sciences and cryptography, analyses the case of oracles in the nascent blockchain ecosystem. The paper also proposes a sociotechnical approach to the use of distributed oracles as informational devices to assist deliberative processes in digital democracy settings and considers the limits that such an approach may face.

**Keywords: democracy, digital democracy, blockchain, cryptography, oracles, distributed networks, deliberation, decision making**

OPEN ACCESS

***Edited by:***
*Andrej Zwitter,*
*University of Groningen, Netherlands*

***Reviewed by:***
*Michael Shea,*
*Independent Researcher, Litchfield,*
*United States*
*Marc Rocas-Royo,*
*Open University of Catalonia, Spain*

****Correspondence:***
*Marta Poblet*
*marta.pobletbalcell@rmit.edu.au*

***Specialty section:***
*This article was submitted to*
*Blockchain for Good,*
*a section of the journal*
*Frontiers in Blockchain*

***Received:** 24 June 2020*
***Accepted:** 18 August 2020*
***Published:** 17 September 2020*

***Citation:***
*Poblet M, Allen DWE,*
*Konashevych O, Lane AM and*
*Diaz Valdivia CA (2020) From Athens*
*to the Blockchain: Oracles for Digital*
*Democracy.*
*Front. Blockchain 3:575662.*
*doi: 10.3389/fbloc.2020.575662*

## INTRODUCTION

On January 3, 2009, Satoshi Nakamoto released to the world the genesis block of the "peer-to-peer electronic cash system" that he had announced in a cryptography mailing list two months earlier (Nakamoto, 2008). A newspaper headline—"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"—was embedded as plain text in the first bitcoin transaction. The intent behind that message remains as elusive as Satoshi's own identity, and the 2008 paper does not provide any additional clue either. The paper mentions the term "bank" just once, "financial institutions" appear only twice (in the introduction), and concepts such as "economy", "economics," or "politics" are completely absent from the text. Yet, as the peer-to-peer network was brought to online life with the mining of the first bitcoin transaction it came with the aura of a declaration of independence from banks, financial institutions, and mainstream political economies. A declaration underpinned by an emergent peer-to-peer network that replaces institutional trust with distributed, consensus-based trust.

Blockchain technology is a distributed ledger architecture first developed and released by the pseudonymous Nakamoto (2008) in the midst of the Global Financial Crisis. First used to refer to the architecture underpinning Bitcoin, blockchain has come to be used in a wide variety of applications, including supply chain management, financial organization, identity provision, and the recording of documents (such as university degrees or wills). These use cases variously take advantage of blockchain's distributed immutability—where additions to the ledger can only be made by social consensus. The technology offers a ledger architecture for ensuring trust in digital records. Thus, blockchain has been described as a "trust machine" (*The Economist*, 31 October 2015, Werbach, 2018), or acting to "industrialize" trust (Berg et al., 2019, 2020) in that it reduces the scope of opportunistic behavior in the management of and access to shared information.

The early enthusiasts of Bitcoin and blockchain tended to span communities of radical anarchists and advocates of e-government—particularly given the technology's cypherpunk lineage (Popper, 2015; Swartz, 2018; Hayes, 2019)—but the idea of a technology that works as a "trust machine" has also been enticing to researchers in the areas of politics, governance, and democracy. Citizens' trust in democratic institutions has been reaching new lows globally, as detected by a number of watchdog agencies (Norris and Inglehart, 2018). Although these signs may fluctuate by index, country, and period, cohort analysis from the World Values Survey reveal that millennials in democracies such as Australia, the United States, Canada, the United Kingdom and New Zealand do indeed display a statistically significant decline in support for democracy by birth cohort (Norris and Inglehart, 2018; see also Foa and Mounk, 2016, 2017).

The analysis of the underlying reasons, as well as the remedies to improve trust in democracy, have become a priority for democratic theorists, political scientists and activists alike. Generally, there is a broad consensus that greater participation in policy and decision making could alleviate the erosion of trust in democracy. The mechanisms may range from deploying deliberative mini-publics (e.g., Goodin and Dryzek, 2006; Grönlund et al., 2014), augmenting collective intelligence with different epistemic mechanisms (e.g., Ober, 2008, 2015; Landemore, 2013) or injecting citizen's participation via sortition (Van Reybrouck, 2016; Gastil and Wright, 2019).

The topic of blockchain and democracy has already been explored both by entrepreneurs and scholars. Projects such as DemocracyEarth, companies such as Horizon State, and political organizations such as Flux Party or MiVote in Australia have been testing the use of blockchain technologies in their voting processes. One of the main areas of academic inquiry focuses on the blockchain as a trusted infrastructure for electronic voting and, ultimately, electoral integrity (Racsko, 2019). More general questions about blockchain and its implications for democratic governance can be found in Magnuson's account of the origins of Blockchain (Magnuson, 2020), or in Allen et al. (2019a) which explores blockchain as a mechanism for alternative democratic coordination. Yet, the role that blockchain infrastructure can play in the ever-growing digital democracy ecosystem of platforms and apps (Poblet et al., 2019b) is still underexplored.

This paper considers the potential role of blockchain technologies for digital democracy by focusing on the particular function of oracles. An oracle can be broadly understood as a source of truth external to a system that provides agents within that system with guidance on how to act. In a blockchain environment, oracles are the digital interfaces linking external data points (off-chain information and data) to an on-chain infrastructure, such as a smart contract or a Decentralised Autonomous Organisation (DAO) in order to execute some transactions. The key question that this paper addresses is whether and how similar digital interfaces could facilitate deliberative and decision-making processes in digital democracy platforms. The role of such oracles would be to provide data, information and, more broadly, expert knowledge into deliberative platforms. Ultimately, oracles could contribute to efficient knowledge management of digital democracy platforms and other self-governing socio-technical systems (e.g., Kurka et al., 2019).

The remainder of the paper is set out as follows. Section "Oracles in Athenian Democracy" below makes an incursion to the Athenian origins of oracles and its relationship with Athenian democracy. Section "Oracles in Computer Science and Cryptography" briefly reviews the definition and use of oracles in computer science and cryptography. Section "Oracles and Smart Contracts" offers an overview of how oracles are used in blockchain-enabled smart contracts as a collective choice infrastructure for digital democracy. Sections "Oracles and Decentralised Finance" and "Oracles in the Energy Sector" explore the examples of decentralised finance (DeFi) and the energy sector as examples of blockchain use cases that shed further light on oracle problems and oracle governance issues. In Section "Oracles in Digital Democracy" we draw from all of these previous examples to examine the potential of oracles for the digital democracy domain and propose a socio-technical systems framework for the design of oracles for digital democracy. Section "Challenges of Implementing Oracles Within Democratic Processes" considers the main challenges that oracles may face in a digital democracy environment. Finally, we conclude the paper by considering some areas for future work.

## ORACLES IN ATHENIAN DEMOCRACY

Oracles were an established form of divination in ancient Greece and, for centuries, they served as sources of consultation in public affairs. Oracular consultations have been the object of vast research in humanities, but their purpose and function, particularly in Athenian democracy, has also attracted the curiosity of historians of democratic institutions. As Zanakis et al. (2003) put it, "the Delphic oracle of the ninth to the third centuries BC was the first central intelligence." Nevertheless, what this intelligence consisted of and, more broadly, the role of oracles in public policy remains highly controversial. Bowden (2005) cites the scarcity of historical sources as the main issue when trying to elucidate their function: "the current orthodoxy is largely based on the accounts of Herodotus, the most important, but not necessarily the most straightforward source of evidence for early Greek history" (Bowden, 2005: 4).

In a nutshell, the scholarly debate about oracles in public matters focuses, at least, on three key issues. First, the matters that were subject to consultation. Bowden supports the view that oracular petitions and answers covered not just religious topics but a broad range of politically relevant topics, including decisions on whether a state or polis should engage in military campaigns or not, make alliances, resist foreign invasions, etc. In his words, "Athens, and by implication other

Greek states, consulted oracles on matters which could not be resolved by debate, and on major issues that might have profound consequences for themselves", and "they followed the advice" (idem: 6).

Second, there is controversy around the type of advice delivered by oracular priestesses—such as Phytia, the highest priestess in the temple of Apollo at Delphi—who would speak the words of gods. Mainstream scholarship and literature have typically presented oracular responses, which would have taken the form of hexameter verses, as "deliberately ambiguous" (idem: 21). Bowden deviates from this established view by suggesting that, instead:

> *The clearest evidence for the form of oracular responses from Delphi in the classical period comes from a number of inscriptions recording the actual response of the Pythia, supported by evidence quoted in Athenian law-court speeches. This evidence suggests that the most common form of question was: "would it be more profitable and better for us to. . .?" This would normally lead to a response of either "it would be more profitable and better. . ." or "it would not be more profitable and better. . .." (idem: 22–24).*

In this perspective, a petitioner using such a formulaic question, therefore, could confidently expect a "straightforward answer, which could be acted on" (idem: 24) and, even, be brought to court as an authoritative argument. Those answers were uttered orally by the oracle-speaker, but petitioners were allowed to write them down "word for word" (idem: 21). From this interpretation, Greek oracles did provide clear, unequivocal answers to urgent and fateful questions for entire political communities. As Howe puts it, "for an oracle to stay in business, it had to produce clear, fairly comprehensible predictions" (Howe, 2006). Were these ancient oracles incorruptible? Even if there were a few cases where bribery might have been involved, there was also a procedure in place to expunge these incidents from the oracle system (Bowden, 2005: 28).

Third, discrepancies among scholars persist on how oracular advice was embedded into the deliberation and decision-making mechanisms of Athenian democracy. Historical sources, again, are reported as limited, but since religious and political issues were distinctively interlinked in Athenian politics and society, there is evidence that, for example "every stage of a military campaign in the Greek world involved religious ritual, in particular regular divinatory sacrifices to ascertain than the gods approved of the proposed course of action" (Bowden, 2005: 100). There was a process in place for the Assembly to send Athenian messengers to Delphic consultations, which also shows "how the Athenians were concerned about the wishes of the gods in all their decision-making" (idem: 132). It is not that Athenians expected divine advice for decisions that they could make by themselves, but rather, for matters "where human wisdom cannot be expected to know the correct answer, either because they concern the wishes of gods or because they require knowledge (.) not available to mere mortals" (idem: 85).

The scholarly debate on how oracles actually worked in ancient Athens may not have reached consensus on any of the key issues above. Yet, the transposition of the term "oracle" into modern computer science and cryptography and, later on, its adoption by different blockchain communities is more akin to its interpretation as a succinct, precise and unambiguous device to provide information or knowledge that was not available or discoverable to citizens using normal procedures. Likewise, contemporary oracles also retain the quality of being a trusted source whose "authority" draws from the consensus around its correctness. While the correctness of an oracle can always be disputed (Allen et al., 2019b) the underlying agreement around its validity, paradoxically enough, is the basis of its adoption in trustless ecosystems.

## ORACLES IN COMPUTER SCIENCE AND CRYPTOGRAPHY

Alan Turing's universal automatic machine (a-machine) is a cornerstone of modern computer science, but his lesser-known notion of an oracle-machine (o-machine) has proved equally influential in the long run. The few lines that Turing devoted to o-machines in a paper on ordinal logics (Turing, 1939) have been qualified as both "one of the most important and most obscure parts of all of computability theory" (Soare, 2009: 378). An obscure part because those lines largely passed unremarked for several years until the notion was further developed by Emil Post in the mid-late 1940s (idem: 380); yet an important one from the perspective of contemporary online computing. As Soare puts it, it is the emergence of online computing that makes o-machines even more relevant in terms of computability theory:

> *It appears that the Turing o-machine is a good theoretical model to analyze an interactive process because there is usually a fixed algorithm or procedure at the core, which by Turing's thesis we can identify with a Turing a-machine, and there is a mechanism for the process to communicate with its environment, which when coded into integers may be regarded as a Turing type oracle (idem: 387).*

Coupled with an o-machine, a Turing a-machine is able to access and interact with external databases or other devices (e.g., sensors, RFID chips, etc.). From this perspective, a blockchain oracle can be understood as a Turing o-machine enabling access to external data that is relevant to blockchain transactions (such as prices, rates, indexes, etc.). Likewise, a smart contract can be conceived as a Turing a-machine paired to one or many o-machines in order to automatically execute its code.

More generally, in computability theory Turing o-machines are also connected to the denominated "halting problem," which refers to the issue of determining, from a description of an arbitrary computer program and an input, whether the program will end the process or continue to run forever. Turing proved in 1936 that a general algorithm to solve the halting problem for all possible program-input pairs did not exist (Tzitzikas and Marketakis, 2018). In a fixed Turing-complete model of computation (Van Melkebeek, 2000) the task of the oracle is to determine whether the program will eventually halt when run with some given inputs.

An important question about oracles in computer sciences is whether they are infallible or not. Turing considered that machines, as humans, should be allowed to make mistakes, ["if a machine is expected to be infallible, it cannot also be intelligent" (quoted in Soare, 2009: 388)]. This consideration, in fact, applies to "many computing processes in the real world which give a sequence of approximations to the final answer" (Soare, 2009: 388). The discussion about fallibility/infallibility of an oracle is also present in contemporary Machine Learning (ML), a subdomain of Artificial Intelligence. ML algorithms that are trained with large amounts of unlabeled data rely on oracles (either humans or machines) that have correctly labeled a small subset of data instances (for training purposes) or provide the correct answer whenever interrogated. However, the assumption that oracles should be considered omniscient (always providing the correct answer) is not unanimously shared. There are ML approaches (e.g., proactive learning) which assume that oracles (broadly understood as external sources of knowledge) can be reliable only at different degrees, or be reluctant to provide answers if these are too uncertain or prove plainly wrong (Donmez and Carbonell, 2008). These assumptions, more aligned with Turing's remark about fallible machines, are also present in the nascent domain of blockchain governance, a space dealing with the management of disputes over fallible oracles (Allen et al., 2019b).

In cryptography, the notion of "oracle" can be found in Bellare and Rogaway's concept of "random oracle" (Bellare and Rogaway, 1993). A "random oracle" is set to "provide all parties—good and bad alike—with access to a (public) random oracle" which ensures a true randomness for a cryptographic hash function. Without the oracle, the user would rely on their local mathematical functions with weak entropy, which is needed for a strong encryption. With the oracle's response the user will know if her message is secure enough.

Notably, various cryptographic standards (such as NIST FIPS 186-4, PA-DSS, ETSI TS 101 861) do not use the notion of oracle (National Institute of Standards and Technology [NIST], 2013; PCI Security Standards Council, 2016; European Telecommunications Standards Institute [ETSI], 2011). Rather, the concept of a "trusted third party" is generally used instead. For example, NIST's cryptographic standard defines "trusted third party" as "an entity other than the owner and verifier that is trusted by the owner or the verifier or both. Sometimes shortened to 'trusted party"' (National Institute of Standards and Technology [NIST], 2013). As a general rule, a system that does not deal with trusted third parties should be more reliable to senders and receivers of encrypted messages. However, it is nearly impossible to develop and scale the system for real world tasks without the intervention of third parties. Thus, the main task of the developer is to make these third parties as much trustable as possible with applied mathematics and better architecture design.

To summarize, oracles are core concepts for both theoretical and applied computer science since its very inception, but they are modeled and applied in different ways, depending on underlying assumptions on how fallible, reliable, or trustworthy they are. Similar discussions are now unfolding within the blockchain space in relation to oracles connected to smart contracts, decentralized finance, or energy transactions. The sections below capture some of the most recent developments in these areas.

## ORACLES AND SMART CONTRACTS

As more economic, social and political activity moves to cyberspace, the security of digital infrastructure—and the value it supports—becomes more critical. The recent advances in blockchain-based smart contracts have pointed attention to the security of the oracles that act as their information inputs. Oracles are a key input into the functioning of smart contracts because they trigger contractual terms. Today, oracles are provided in many different ways (e.g., degree of decentralization) and with corresponding features (e.g., robustness, reliability, accuracy). These features are important because even where a particular blockchain protocol is considered secure, oracles can be points of weakness for smart contracts (e.g., inaccurate or compromised data). Here we introduce the "oracle problem" and see how oracle innovations seek to ameliorate those problems.

As we saw above, blockchains draw on both cryptography and economic incentives to create mechanisms by which groups come to consensus over shared data. The evolution of blockchain protocols, particularly since Ethereum, has increasingly emphasized the functionality of those protocols for executing smart contracts. We define smart contracts on blockchain infrastructure to be "agreements—or parts of agreements—that are coded to operate within a decentralized or distributed blockchain network, and that can be automatically executed by that network when specific conditions are validated" (Allen et al., 2019b: 78). Smart contracts can be deployed to transfer value over blockchain infrastructure including both monetary value (e.g., decentralized finance applications), native digital assets (e.g., digital art), or digital representations of physical assets (e.g., supply chains applications). More broadly, smart contracts can be used to create new forms of distributed and decentralized organizations, such as Decentralised Autonomous Organisations (DAOs).

Smart contracts rely on external data to trigger their contractual conditions. Oracles provide a gateway between blockchains and the outside world. Indeed, in the simplest form: "An oracle is just a provider of data. An oracle gives smart contracts answers to questions about the world" (Delphi, 2017). That information could include, for instance, the outcomes of events (e.g., elections, sporting events), financial data (e.g., exchange rates, stock prices), or supply chain information (e.g., temperature, location, delivery), or outcomes of dispute resolution (e.g., if the contract does not execute as intended).

For a smart contract to execute on every node of a blockchain network—and therefore coming to consensus—it must rely on information within the blockchain itself. That is, the data inputs into a blockchain-based smart contract must be deterministic. The consensus mechanism cannot rely on nodes receiving the same external data because multiple honest nodes could be in conflict about the contract execution (because they don't have access to the same external data). But the data contained within the blockchain itself (e.g., previous transactions) is quite limited, and without reliance on external data the applications of smart contracts are relatively constrained (Egberts, cited in Fecke, 2018).

This information is provided by oracles. While there are many potential weaknesses of the blockchain infrastructure on which smart contracts execute (e.g., privacy and scalability), oracles can also provide a point of weakness—this is the "oracle problem." As Song (2018) has pointed out, what is the point of having a decentralized infrastructure for contract execution that relies on centralized data inputs? Indeed, Delphi (2017) argues: "as soon as you make a smart contract rely on a single central oracle, you have totally sacrificed any decentralization-related benefits (which makes it arguable whether you should be using a smart contract at all)."

Oracles solve the problem of pulling external data into a smart contract in different ways. There are a growing range of oracle services. The nature of oracles includes hardware oracles (e.g., sensors detecting information), software oracles (e.g., pulling data feeds from online, such as stock prices), and consensus oracles (that attempt to decentralize data sources by relying on data from multiple sources and aggregating or averaging that data). Ultimately smart contracting parties have a choice when drafting a contract over the oracle that will trigger the contract. In making that choice they can trade-off the various features of oracles (e.g., their cost, speed, resilience, robustness) that are generated by their structure (e.g., how decentralized they are) to suit their contractual needs. This is similar to the choice of dispute resolution mechanism in the terms of a smart contract (Allen et al., 2019b).

For example, Chainlink is a popular oracle service provider that seeks to create more robust oracles through economic incentives, decentralization and reputation mechanisms[1]. Rather than relying on a single oracle source, Chainlink leverages many different oracle service providers. That is, their outputs can be aggregated and averaged (with outliers removed) to provide more accurate inputs that are more robust to tampering. Users can pay for different degrees of decentralization in oracles and, for example, pay for more oracle service providers (Egberts 2018, cited in Fecke, 2018). Those oracles can be incentivized through economic incentives for good and bad behavior.

Through oracles, blockchain-enabled smart contracts provide a collective choice infrastructure that enables new possibilities for digital democracy (e.g., Allen et al., 2019a). Before specifically exploring these possibilities and a taxonomy of the oracle requirements and challenges in this context, however, it is worthwhile considering two other blockchain use cases—decentralized finance and energy. These two sectors are more advanced in their real-world development compared to digital democracy platforms. Accordingly, there are lessons that can be learned shedding further light on the oracle problem and oracle government issues.

## ORACLES AND DECENTRALISED FINANCE

Decentralised finance (DeFi) was the first use case of blockchain technology. Bitcoin, and the other cryptocurrencies that followed, aimed to develop "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (Nakamoto, 2008: 1). Arguably, cryptocurrencies move toward more democratic financial systems as financial transactions are verified by a majority of nodes on the network, and—for public blockchains—the protocol is open source (Christopher, 2016). Smart contracts allow DeFi platforms to offer a range of financial products including lending, derivatives, insurance, and prediction markets. However, these capabilities often require oracles to make agreements function—usually around prices. As a basic example, the bitcoin blockchain does not inherently contain the bitcoin exchange rate to other fiat or cryptocurrencies—these prices are determined by the relevant market. So, generally, smart contracts will need to refer to an oracle to input this price information which provides points of weaknesses. Two recent DeFi experiences provide real-world examples of the oracle problem.

First, consider the DeFi lending platform "bZx." In 2020, the platform suffered two "flash loan" attacks. A flash-loan is defined as a cryptocurrency loan that "is only valid within one blockchain transaction" (Qin et al., 2020). That is, the loan is not executed if not immediately repaid. The use cases for this type of transaction include arbitrage trading, wash trading, collateral swapping, and minting (idem). In the bZx cases, a flash loan for an amount of Ether (ETH) was opened on the lending platform. In the first case, the ETH was utilized for a combination of borrows, swaps, and shorts—exploiting a bug in the smart contract code to repay the loan and turn a profit (idem). In the second case, a portion of the loaned ETH was used to purchase stablecoin tokens while the other portion was used to manipulate the stablecoin token price. The inflated stablecoins were then used as collateral for a second loan to repay back the original flash loan and take the remainder (idem). This case highlights the importance of having price oracles that cannot be easily manipulated.

Second, consider the MakerDAO network and its 'Dai' stablecoin. Stablecoins are a crypto asset that has been "developed with the aim of minimizing price volatility by embedding a stability mechanism" (Berentsen and Schär, 2019: 65). This is an important development for facilitating longer-term exchanges that require a level of certainty over the future value of payment. An example of a stability mechanism is pegging the value of a cryptocurrency to the US dollar. This can be achieved in several ways: algorithmically (where a platform's underlying software attempts to manipulate the cryptocurrency supply to maintain the valuation); collateralized off-chain (where fiat currency is deposited in exchange for the cryptocurrency, held in a centralized bank account); and collateralized on-chain (where cryptocurrency is deposited in exchange for another cryptocurrency) (idem). MakerDAO's Dai falls into the latter category. Built on the Ethereum blockchain, Maker platform users deposit ETH in exchange for Dai loans and a "system of Collateralized Debt Positions (CDPs), autonomous feedback mechanisms, and appropriately incentivized external actors" operate to maintain a stable value of Dai relative to the US dollar (MakerDAO, 2017:3). If the value of ETH falls dramatically, there may not be enough collateral in the system to cover the

[1] https://chain.link/

value of the Dai tokens. In this case, the "risky" CDPs may be automatically liquidated (idem: 11). Such an event occurred in March 2020. According to news reports at the time, a combination of network congestion and time lagged price oracles meant around US$4 million worth of ETH was taken from the platform—ultimately leaving the platform in deficit (Foxley and Dale, 2020). Ironically, MakerDAO only holding ETH as collateral was a deliberate design choice in the early stages of the platform to mitigate against a 'black swan event' (MakerDAO, 2017:17). This case highlights the importance of governance rules factoring in oracle time lags in system design—particularly for automated processes, and especially where stablecoins are collateralized against a single type of asset.

In summary, decentralised finance applications require data and information inputs from oracles in order for smart contracts to process transactions. However, this fact means that there are inherent points of failure, and distortion or manipulation can eventually lead to systemic risks. The experience of DeFi platforms highlights the importance of dispute resolution and governance processes when oracle problems result in wider platform issues. Since digital democracy may also require oracles to feed data to make smart contracts operable, lessons on trust, security, and mitigation of systemic risks in the DeFi space should not be ignored.

## ORACLES IN THE ENERGY SECTOR

Over the past few years, blockchain infrastructure has been considered as a potential enabler of a sociotechnical transition toward more democratic and decentralized energy systems based on P2P energy trading and prosumer participation (Ahl et al., 2019; Andoni et al., 2019; IRENA, 2019). The expansion of Renewable Energy Sources (RES) installed at small and large scales and the ever-growing prices of grid electricity, combined with the pressures of climate change, provides the economic incentives for blockchain-based companies to develop energy trading ecosystems. The Australian start-up Power Ledger[2], for example, has built such an ecosystem over a hybrid blockchain composed of a public layer (Ethereum) and a consortium (ECOchain) layer (Power Ledger, 2019). At the core of the Power Ledger Ecosystem, decentralized oracles access real-world data from metering readings (e.g., from RES or energy storage units) and link such information with the internal operations and communications of the ecosystem through smart contracts (Power Ledger, 2019).

ECOchain is a private endeavor that identifies itself as a "lightweight, fast and economically friendly decentralized public chain" (ECOchain, 2020: 6). ECOchain claims short block creation (32 s) and the capacity to process 560 transactions per second (Chalkidis, 2018) while running smart contracts over Ethereum Virtual Machines (EVMs). Beyond decentralized trading, the system provides novel platform services such as cross-chain transactions (interoperability) and separate consensus protocols for decentralized oracles (ECOchain, 2020). Decentralized oracles in ECOchain evaluate external data by reaching consensus (through a protocol) with other decentralized oracles (ECOchain, 2019) about whether a particular value or event is true or false (Chalkidis, 2020). Once decentralized oracle consensus is achieved, the information feeds the smart contracts at the core of the Power Ledger Ecosystem. In this regard, a decentralized oracle is simply a group of oracle entities validating data through consensus.

ECOchain characterizes three types of decentralized oracles:

1. Assigned oracles, involving a group of known oracles holding the right to vote. Correct values are decided by voting. Honest behavior is incentivized through retributions and penalizations.
2. Dynamic oracles, with the same voting mechanism as above but the difference that anyone can act as an oracle. Voting is not forced.
3. Independent oracles: Oracles have their own blockchain running its own consensus algorithm. Oracles achieve consensus and finality within this environment so that results can be feed into the smart contracts in the ecosystem.

The ECOchain Oracle Protocol is formalized mathematically through Game Theory under infinite iterations. The incentives given within the voting system of the protocol result in two key obstacles. First, the potential for untrue coalitions and second, the potential for free riding. However, a built-in punishment mechanism within the protocol can incentivize oracles to avoid this behavior (Chalkidis, 2020). Contrary to traditional information systems in which a single oracle centralizes interconnectivity, multiple oracles safeguard the decentralized nature of blockchain ecosystems. Decentralized energy trading platforms, accessing data from multiple oracles, enable the participation of broader stakeholders, such as prosumers within microgrids. In this way, participants now excluded by centralized energy systems may retrieve the operative and economic benefits of the valuable services they provide.

As trusted data sources, ECOchain's decentralized oracle solutions align with the decentralized nature of blockchain. However, issues in terms of free-riding and coalition formation are still latent, evidencing pain points similar to the ones in the DeFi domain. P2P energy trading involves the participation of a wide range of prosumers and consumers at the core of community-based solutions. This participative enabling attribute of blockchain, together with the decentralized oracle experimentation developed in early solutions such as energy trading platforms, may contribute toward solutions in digital democracy.

## ORACLES IN DIGITAL DEMOCRACY

Digital democracy is an umbrella term that has been used over the last two decades to refer to digitally enabled tools supporting different types of participatory processes, such as monitoring policies and representatives, signing petitions, deliberating, drafting legal texts, voting, etc. One of the early definitions

[2] See https://www.powerledger.io/

of digital democracy focuses on "the use of information and communication technology (ICT) and computer-mediated communication (CMC) in all kinds of media (e.g., the Internet, interactive broadcasting and digital telephony) for the purposes of enhancing political democracy or the participation of citizens in democratic communication" (Hacker and van Dijk, 2000: 1). Digital democracy and e-democracy are often used interchangeably, and both may actually include hybrid forms of participation (online-offline) rather than just "digital" or "electronic" forms. Other common terms to designate this broad domain are "participatory technology" or "civic technology". More recently, "digital democracy" can also include emergent forms of cryptodemocracy that leverage cryptographically secure distributed ledgers for the decentralized construction of political systems and both democratic corporate and organizational governance (Allen et al., 2019a).

In recent years, the digital democracy ecosystem has been expanding with a growing number of platforms and apps tapping on geodata (crowdsourced mapping), semantic web technologies (providing taxonomies and structure to topics and arguments), machine learning algorithms (suggesting related topics) and a number of collaborative tools for both synchronous and asynchronous collaboration (e.g., wikis, online spreadsheets, forums and chats, etc.). The new generation of civic technologies aligns with different models of democracy (liberal, monitory, participatory, deliberative, and epistemic) depending on the emphasis of their functionalities (Poblet et al., 2019a).

If, in Howe's words, "Delphi served as the link between humans and the gods" (Howe, 2006), blockchain oracles, as seen in the examples above, now connect digital ledgers to the external world (outbond oracles), or the external world to digital ledgers (inbound oracles). In this perspective, oracles can be seen as knowledge management interfaces effectively injecting—or ejecting—the informational inputs or outputs required to trigger some action in a system.

Digital democracy platforms can be conceived as socio-technical systems—where human participants leverage digital technologies for some specific purpose—with the need to efficiently manage the relevant knowledge to achieve their purposes. Yet, when it comes to large-scale deliberation in online settings, the issues of how to adequately process internal and external inputs remain open. On the one hand, there is the problem of how to access, structure, classify, or retrieve the internal contributions of participants in forums and discussion threads so that relevant ideas, suggestions, proposals, etc. can effectively be turned into collectively produced knowledge. Over the past decade different approaches have been proposed, ranging from formal structures of arguments to tokenisation in a blockchain (e.g., Klein, 2011; Klein, 2017; Iandoli et al., 2018; Benítez-Martínez et al., 2020) and a number of success factors have been identified (Panopoulou et al., 2014).

With regard to external inputs, the issue of injecting relevant knowledge into deliberative processes has been raised in relation with experts. In offline settings, citizen assemblies, citizen juries and other similar mini-publics frequently hear from experts when deliberating about particular topics. Those experts may deliver presentations, reports, or documents for members of the assembly to consider in their deliberations in a carefully designed process (e.g., Farrell et al., 2019). Large-scale online deliberation platforms could also benefit from considering different sources of data, information, and expert knowledge. Yet, the processes of managing these epistemic inputs have not received the same level of attention. Stemming from Ostrom's design principles for the effective management of common-pool resources (Ostrom, 1999), Pitt et al. (2017) have proposed eight principles for effective knowledge management in socio-technical systems (see also Kurka et al., 2019). Among the knowledge management principles (KMP) that are relevant here:

> [KMP3] Agreement on certain matters on which decisions must be made as being of common interest.
> [KMP4] Clear line between common interest questions and factional or partial goods questions. Appropriate procedural rules for decision-making in each domain.
> [KMP5] Common knowledge by citizens of substantive rules and of procedural rules for making new rules and revising existing rules.
> [KMP6] Epistemic diversity among citizens, along with distributed social knowledge of locus of expertise and reliability of experts.
> [KMP7] Procedural rules ensure that valuable, diverse inputs are recognized as such and taken up as appropriate. Filtering process for assessing what (and whose) information input is (and is not) relevant to each specific sort of question.

KMP3 hinges on shared values; KMP4 identifies common interest questions; KMP5 expresses the need for rule awareness to adapt and create new rules; KMP6 calls for epistemic diversity and reliable experts; KMP7, finally, requires a filtering process to identify relevant knowledge. In Kurka et al. words, "the considerations of Principles 6 and 7 on epistemic diversity, reputable sources of knowledge and expertise are intended to resist the manipulation, distortion and falsification of information, and minimize the effects of confirmation bias and the subsequent polarization of opinion." (Kurka et al., 2019, 8). Kurka et al. operationalize some of these principles within a formalized model and then run different experimental simulations to test how the principles contribute to resolve collective action problems. While no real-life scenario or actual digital democracy platform is involved in the testing, the authors conclude that, ultimately, the application of design principles for effective knowledge management "is fundamental for the good performance of the existing processes of collective decision-making, coordination, and memory" and, ultimately, can contribute to achieving "sustainable and democratic self-governance of socio-technical systems" (idem, 38–39).

Our vision of oracles for digital democracy aligns with the design principles and sociotechnical framework outlined above and aims to contribute with additional specifications that could be useful for the existing deliberative platforms within the ecosystem (Poblet et al., 2019b). In this regard, there are several ways that oracles may be used in managing epistemic inputs for digital democracy environments.

## Oracles Feeding Data and Information

Oracles could feed relevant data and information (e.g., from real-world facts and events) into deliberative and decision-making processes within digital platforms. An example of data feed could be a monthly unemployment rate by a government source, or the daily number of Covid-19 global cases by the Johns Hopkins University dashboard. The question of what sources are appropriate is of interest to all participants and requires them to make initial agreements and, more broadly, to adopt procedural rules for decision making [KMP3 and KPM4]. Potentially, for example, participants could decide to select a few established, trusted sources of data, or set a process for crowdsourcing and fact-checking open source information from social media (or any combination of the two).

Oracles could also be fully decentralized and incentivized to provide reliable information about real world-events. In the labor domain, for example, decentralized trade labor unions require information about the outside world to monitor collective bargaining agreements. Those events may trigger stand down or termination provisions, dispute resolution procedures, etc. In decentralized investment, to use another example, firms require information about the investment targets. In this context, "software oracles" could provide input through automated contract review, and "consensus oracles" could provide human judgment and input into the due diligence process. This would trade some of the decision costs from investors to oracles.

In any event, participants should be able to revise and update their rules and procedures about oracles and the inputs they are feeding whenever needed (e.g., the oracles or the data/information sources are no longer effective or reliable, or new sources have been discovered) [KMP5].

## Oracles Feeding Expert Knowledge

Expert knowledge is a more complex epistemic input with established practices in deliberative mini-publics. In digital platforms, similar procedures to the ones outlined above could be set when selecting both relevant and reliable experts. Therefore, methods and procedural rules to identify and designate appropriate experts will be required (e.g., crowdsourcing, consensus, etc.). In our application of KMP6 and KMP7, the broader epistemic diversity and distributed social knowledge participants bring to deliberative and decision-making processes, the greater the chances to identify and select relevant expertise to feed such processes, and to ensure with proper rules that expert knowledge is taken up appropriately.

## Oracles in Voting Mechanisms

Oracles could supply data about voting processes and, for example, about how particular votes have been cast [KMP5]. This could include records relating to the electoral commission, share register, organization of membership lists, etc. In a cryptodemocracy (Allen et al., 2019a) individuals could delegate their votes to others with conditions attached (such as voting in particular ways). Oracles could feed data about how votes have been cast, acting as inputs into those conditional smart contracts.

## Oracles for Dispute Resolution

Disputes occur within traditional deliberative and voting systems (such as corporate or political elections). Disputes will also occur in digital democracy platforms and blockchain-based voting systems. In the latter case, contracts that have been executed will come into dispute, for instance over the validity of the ballot. In this circumstance oracles could be implemented as ways to integrate external outcomes from dispute resolution. As Allen et al. (2019b) outline, there are a wide range of different dispute resolution mechanisms relating to smart contracts that differ in the way they provide dispute resolution services. Recently developed protocols applying game-theoretical incentives to crowdsourced arbitration of disputes, such as Kleros (Lesaege et al., 2019) or the Aragon Court (Spagnuolo et al., 2019), may shed further light in this direction.

## Challenges of Implementing Oracles Within Democratic Processes

In all the domains above, the use of oracles comes with some potential challenges. Among the most significant ones are subjective information and bias. Many of the epistemic inputs injected into deliberative processes and democratic decision making will rarely fit in the categories of "raw data" or "purely factual" information. There are ongoing contentious debates around the nature of "facts" within democratic processes. In the blockchain space, current efforts to generate oracles are already struggling with the problem of integrating clear factual data—e.g., the outcome of an event—into blockchain infrastructure in reliable ways. These problems are likely to be exacerbated within online environments where, in addition, a pervasive confirmation bias—people paying attention to information that confirms beliefs and expectations while disregarding information that invalidates them—has been long established (e.g., Knobloch-Westerwick et al., 2015; Knobloch-Westerwick et al., 2020). Likewise, the effect of group polarization (Sunstein, 1999) has largely been documented in digital spaces. Yet, these same challenges exist in offline settings, and there is growing literature focusing on how to mitigate the confirmation bias and the group polarization effect. For more than a decade, research in the area of deliberative democracy has shown that public deliberation and group diversity may help to mitigate both phenomena (Bohman, 2007; Fishkin, 2009; Mercier and Landemore, 2012; Curato et al., 2017). From a research design and human-computer interaction (HCI) angle, technical implementations have been suggested, such as automated multiple viewpoints (Park et al., 2009) or introducing disfluency in argument presentation (Hernandez and Preston, 2013). Moreover, research on collective intelligence (Malone and Bernstein, 2015) has highlighted the role of cognitive diversity in efficient groups, which is consistent with the knowledge management principles outlined in Section "Oracles in Digital Democracy."

Another important challenge that the use of oracles in digital democracy raises relates to continuous curation. Democratic processes involve large amounts of data, information, and knowledge as epistemic inputs into collective choices. These inputs span across many areas, have multiple formats, and change over time in potentially unpredictable ways. The curation of these inputs is perhaps more difficult, and more costly, than curating more structured and regular "raw data" inputs (e.g., weather measurements). Platforms using oracles should therefore address this issue by designing and deploying appropriate curation processes governed by clear rules.

## CONCLUSION AND FUTURE WORK

The notion of oracle has a long tradition in human history and, consequently, a rich variety of meanings and conceptualizations. This paper has examined the role of oracles as informational and knowledge-seeking devices in different domains. We started by providing an overview about the use of divine oracles in Athenian democracy, a topic that is still the object of academic debate, and then reviewed the use of the term in modern computer sciences and cryptography. The paper has also explored the use of oracles as digital artifacts or, in other words, as a middleware between the external informational world and the nascent blockchain ecosystems of smart contracts, decentralized finance, and decentralized energy grids. In these spaces, oracles link off-chain data sources with blockchain infrastructure (either as inputs or outputs for transactions) and open up new possibilities for real use cases.

The use of oracles in the domains outlined in this paper also show that some of the properties that oracles exhibit in those domains could be leveraged in digital democracy platforms to enhance their information and knowledge management processes. Arguably, we note that the following properties in oracles could be further explored in future work: (i) decentralized, relying on a distributed network oracles that also rely on multiple sources; (ii) independent (oracles obtaining epistemic inputs independently of the others, thus avoiding potential conflicts with practices of syndication of news stories across many platforms); (iii) crowdsourced (a distributed network relying on crowdsourced fact-checking); and (iv) trusted (by consensus or some other mechanism). While these properties can be enhanced with appropriate design principles, trust and reputation remain essential in a marketplace of independent, distributed oracles, and new governance mechanisms to ensure them will also be needed.

## DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

## AUTHOR CONTRIBUTIONS

MP, DA, and AL contributed to the conception and design of the study and wrote sections of the manuscript. OK and CADV wrote sections of the manuscript. All authors contributed to manuscript revision, read, and approved the submitted version.

## REFERENCES

Ahl, A., Yarime, M., Tanaka, K., and Sagawa, D. (2019). Review of blockchain-based distributed energy: Implications for institutional development. *Renew. Sustain. Energy Rev.* 107, 200–211. doi: 10.1016/j.rser.2019.03.002

Allen, D. W. E., Berg, C., and Lane, A. M. (2019a). *Cryptodemocracy: How Blockchain Can Radically Expand Democratic*. Lanham, ML: Lexington Books.

Allen, D. W. E., Lane, A. M., and Poblet, M. (2019b). The governance of blockchain dispute resolution. *Harvard Negot. Law Rev.*. 25, 75–101. doi: 10.2139/ssrn.3334674

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., et al. (2019). Blockchain technology in the energy sector: a systematic review of challenges and opportunities. *Renewab. Sustain. Energy Rev.* 100, 143–174. doi: 10.1016/j.rser.2018.10.014

Bellare, M., and Rogaway, P. (1993). "Random oracles are practical: random oracles are practical: a paradigm for designing efficient protocols," in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, Fairfax, VA. doi: 10.1145/168588.168596

Benítez-Martínez, F. L., Hurtado-Torres, M. V., and Romero-Frías, E. (2020). A neural blockchain for a tokenizable e-Participation model. *Neurocomputing* (in press). doi: 10.1016/j.neucom.2020.03.116

Berentsen, A., and Schär, F. (2019). "Stablecoins: The Quest for a Low-Volatility Cryptocurrency," in *The Economics of Fintech and Digital Currencies*, ed. A. Fatás (London: CEPR Press), 65–71.

Berg, C., Davidson, S., and Potts, J. (2019). *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics*. Cheltenham: Edward Elgar Publishing. doi: 10.4337/9781788975001

Berg, C., Davidson, S., and Potts, J. (2020). Proof of work as a three-sided market. *Front. Blockchain* 3:2. doi: 10.3389/fbloc.2020.00002

Bohman, J. (2007). Political communication and the epistemic value of diversity: Deliberation and legitimation in media societies. *Commun. Theory* 17, 348–355. doi: 10.1111/j.1468-2885.2007.00301.x

Bowden, H. (2005). *Classical Athens and the Delphic Oracle. Divination and Democracy*. Cambridge: Cambridge University Press.

Chalkidis, A. (2018). *Analyzing the ECO Public Chain Performance and Its Special Characteristics*. Available online at: https://ecoc.io/wp-content/uploads/docs/yp.pdf (accessed August 20, 2020).

Chalkidis, A. (2020). *Oracle Consensus in Rational Environments*. Available online at: https://ecoc.io/wp-content/uploads/docs/oracles_yellow_paper.pdf (accessed August 20, 2020).

Christopher, C. (2016). The bridging model: Exploring the roles of trust and enforcement in banking, bitcoin, and the blockchain. *Nevada Law J.* 17, 139–180.

Curato, N., Dryzek, J. S., Ercan, S. A., Hendriks, C. M., and Niemeyer, S. (2017). Twelve key findings in deliberative democracy research. *Daedalus* 146, 28–38. doi: 10.1162/DAED_a_00444

Delphi (2017). *The Oracle Problem*. Available online at: https://medium.com/@DelphiSystems/the-oracle-problem-856ccbdbd14f (accessed June, 2020).

Donmez, P., and Carbonell, J. G. (2008). "Proactive learning: cost-sensitive active learning with multiple imperfect oracles," in *Proceedings of the 17th ACM Conference on Information and Knowledge Management*, Napa valley, CA, 619–628. doi: 10.1145/1458082.1458165

ECOchain (2019). *Are Oracles Necessary for Blockchain for Real World Applications?* Amsterdam: ECOchain Foundation.

ECOchain (2020). *White Paper. Version 2.0: Reshape Ecological Consensus with Blockchain*. Amsterdam: ECOC Foundation.

European Telecommunications Standards Institute [ETSI] (2011). *Electronic Signatures and Infrastructures (ESI); Time stamping profile (ETSI TS 101 861)*. Sophia Antipolis: ETSI.

Farrell, D. M., Suiter, J., and Harris, C. (2019). Systematizing constitutional deliberation: the 2016–18 citizens' assembly in Ireland. *Irish Political Studies* 34, 113–123. doi: 10.1080/07907184.2018.1534832

Fecke, M. (2018). *The Problem of Blockchain Oracles – Interview with Alexander Egberts. LegalTech Blog*. https://legal-tech-blog.de/the-problem-of-blockchain-oracles-interview-with-alexander-egberts (accessed August 20, 2020).

Fishkin, J. S. (2009). *When the People Speak: Deliberative Democracy and Public Consultation*. Oxford: Oxford University Press.

Foa, R. S., and Mounk, Y. (2016). The danger of deconsolidation: the democratic disconnect. *J. Democracy.* 27, 5–17. doi: 10.1353/jod.2016.0049

Foa, R. S., and Mounk, Y. (2017). The signs of deconsolidation. *J. Democracy* 28, 5–15. doi: 10.1353/jod.2017.0000

Foxley, W., and Dale, B. (2020). *MakerDAO Debts Grow as DeFi Leader Moves to Stabilize Protocol. Coindesk*. Available online at: https://www.coindesk.com/makerdao-debts-grow-as-defi-leader-moves-to-stabilize-protocol (accessed August 20, 2020).

Gastil, J., and Wright, E. O. (2019). *Legislature by Lot: Transformative Designs for Deliberative Governance*. Brooklyn, NY: Verso Books.

Goodin, R. E., and Dryzek, J. S. (2006). Deliberative impacts: the macro-political uptake of mini-publics. *Polit. Soc.* 34, 219–244. doi: 10.1177/0032329206288152

Grönlund, K., Bächtiger, A., and Setälä, M. (eds). (2014). *Deliberative Mini-Publics: Involving Citizens in the Democratic Process*. Colchester: ECPR Press.

Hacker, K. L., and van Dijk, J. (eds) (2000). *Digital Democracy: Issues of Theory and Practice*. London: Sage.

Hayes, A. (2019). The socio-technological lives of bitcoin. *Theory Cult. Soc.* 36, 49–72. doi: 10.1177/0263276419826218

Hernandez, I., and Preston, J. L. (2013). Disfluency disrupts the confirmation bias. *J. Exp. Soc. Psychol.* 49, 178–182. doi: 10.1016/j.jesp.2012.08.010

Howe, T. (2006). *Classical Athens and the Delphic Oracle. Divination and Democracy. Book Review. Bryn Mawr Classical Review*. Available online at: https://bmcr.brynmawr.edu/2006/2006.07.13/ (accessed August 20, 2020).

Iandoli, L., Quinto, I., Spada, P., Klein, M., and Calabretta, R. (2018). Supporting argumentation in online political debate: Evidence from an experiment of collective deliberation. *New Media Soc.* 20, 1320–1341. doi: 10.1177/1461444817691509

IRENA (2019). *Blockchain Innovation Landscape Brief. International Renewable Energy Agency*. Abu Dhabi: IRENA.

Klein, M. (2011). "The MIT deliberatorium: Enabling large-scale deliberation about complex systemic problems," in *Proceedings of the 2011 International Conference on Collaboration Technologies and Systems*, Philadelphia, PA. doi: 10.1109/CTS.2011.5928678

Klein, M. (2017). Towards crowd-scale deliberation. *Paper Presented at Crowd-Scale Deliberation & Idea Management*, Boston. doi: 10.13140/RG.2.2.12264.06401

Knobloch-Westerwick, S., Mothes, C., Johnson, B. K., Westerwick, A., and Donsbach, W. (2015). Political online information searching in Germany and the United States: confirmation bias, source credibility, and attitude impacts. *J. Commun.* 65, 489–511. doi: 10.1111/jcom.12154

Knobloch-Westerwick, S., Mothes, C., and Polavin, N. (2020). Confirmation bias, ingroup bias, and negativity bias in selective exposure to political information. *Commun. Res.* 47, 104–124. doi: 10.1177/0093650217719596

Kurka, D. B., Pitt, J., and Ober, J. (2019). Knowledge management for self-organised resource allocation. *ACM Trans. Autonom. Adapt. Syst*. 14, 1–41. doi: 10.1145/3337796

Landemore, H. (2013). *Democratic Reason: Politics, Collective Intelligence, and the Rule of the Many*. Princeton: Princeton University Press.

Lesaege, C., Ast, F., and George, W. (2019). *Kleros. Short Paper v1.0.7*. Available online at: https://kleros.io/assets/whitepaper.pdf (accessed August 20, 2020).

Magnuson, W. (2020). *Blockchain Democracy: Technology, Law and the Rule of the Crowd*. Cambridge: Cambridge University Press.

MakerDAO (2017). *The Dai Stablecoin System*. Santa Cruz, CL: MakerDAO.

Malone, T. W., and Bernstein, M. S. (eds). (2015). *Handbook of collective intelligence*. Cambridge, MA: MIT Press.

Mercier, H., and Landemore, H. (2012). Reasoning is for arguing: Understanding the successes and failures of deliberation. *Polit. Psychol.* 33, 243–258. doi: 10.1111/j.1467-9221.2012.00873.x

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available online at: https://bitcoin.org/bitcoin.pdf (accessed August 20, 2020).

National Institute of Standards and Technology [NIST] (2013). *Digital Signature Standard (DSS)*. https://doi.org/10.6028/NIST.FIPS.186-4.

Norris, P., and Inglehart, R. (2018). *Cultural Backlash and the Rise of Populism: Trump, Brexit, and the Rise of Authoritarianism Populism*. Cambridge: Cambridge University Press.

Ober, J. (2008). *Democracy and Knowledge: Innovation and Learning in Classical Athens*. Princeton, NJ: Princeton University Press.

Ober, J. (2015). Rise and Fall of Classical Greece. Princeton, NJ: Princeton University Press.

Ostrom, E. (1999). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press.

Panopoulou, E., Tambouris, E., and Tarabanis, K. (2014). Success factors in designing eParticipation initiatives. *Inform. Org.* 24, 195–213. doi: 10.1016/j.infoandorg.2014.08.001

Park, S., Kang, S., Chung, S., and Song, J. (2009). "NewsCube: delivering multiple aspects of news to mitigate media bias," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY: Association for Computing Machinery), 443–452. doi: 10.1145/1518701.1518772

Pitt, J., Ober, J., and Diaconescu, A. (2017). "Knowledge management processes and design principles for self-governing socio-technical systems," in *Proceedings of the 2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)* (Tucson: University of Arizona), 97–102. doi: 10.1109/FAS-W.2017.127

Poblet, M., Casanovas, P., and Rodríguez-Doncel, V. (2019a). Deliberative and Epistemic Approaches to Democracy. Berlin: Springer, 27–49.

Poblet, M., Casanovas, P., and Rodríguez-Doncel, V. (2019b). *Linked Democracy: Foundations, tools, and applications*. Newyork, NY: Springer International Publishing.

Popper, N. (2015). *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. New York, NY: Harper Collins.

Power Ledger (2019). *White Paper*. Perth: Power Ledger.

Qin, K., Zhou, L., Livshits, B., and Gervais, A. (2020). *Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit*. Available online at: https://arxiv.org/pdf/2003.03810.pdf (accessed August 20, 2020).

Racsko, P. (2019). Blockchain and Democracy. *Soc. Econ.* 41, 353–369. doi: 10.1556/204.2019.007

PCI Security Standards Council (2016). *Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS). Payment Card Industry*. Wakefield, MA: PCI Security Standards Council.

Soare, R. I. (2009). Turing oracle machines, online computing, and three displacements in computability theory. *Ann. Pure Appl. Logic* 160, 368–399. doi: 10.1016/j.apal.2009.01.008

Song, J. (2018). *The Truth about Smart Contracts*. Available online at: https://medium.com/@jimmysong/the-truth-about-smart-contracts-ae825271811f (accessed June, 2020).

Spagnuolo, F., AragonOne, and Aragon. (2019). *Aragon Court is Live on Mainnet*. Available online at: https://aragon.org/blog/aragon-court-is-live-on-mainnet (accessed August 20, 2020).

Specter, M. A., Koppel, J., and Weitzner, D. (2020). *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections*. Available online at: http://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf (accessed August 20, 2020).

Sunstein, C. R. (1999). *The Law of Group Polarization. University of Chicago Law School, John M. Olin Law & Economics Working Paper*, (91).

Swartz, L. (2018). What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cult. Stud.* 32, 623–650. doi: 10.1080/09502386.2017.1416420

Turing, A. (1939). Systems of logic based on ordinals. *Proc. Lond. Math. Soc.* 45(Pt. 3):161228. doi: 10.1112/plms/s2-45.1.161

Tzitzikas, Y., and Marketakis, Y. (2018). *Cinderella's Stick: A Fairy Tale for Digital Preservation*. Berlin: Springer.

Van Melkebeek, D. (2000). *Randomness and Completeness in Computational Complexity*. Berlin: Springer.

Van Reybrouck, D. (2016). *Against elections: The case for democracy*. London: Random House.

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. MIT Press.

Zanakis, S. H., Theofanides, S., Kontaratos, A. N., and Tassios, T. P. (2003). Ancient Greeks' practices and contributions in public and entrepreneurship decision making. *Interfaces* 33, 72–88. doi: 10.1287/inte.33.6.72.25177

**Conflict of Interest:** The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.