ALLEN & OVERY

Decentralized Autonomous Organizations

"The toughest job on Wall St this morning is the guy who has to explain #TheDAO to Lloyd Blankfein."

— DAVID HARRISON (@TRADEWITHDAVE) MAY 16, 2016

Introduction

A Decentralized Autonomous Organization (**DAO**) is a computer program, running on a peer-to-peer network, incorporating governance and decision-making rules. DAOs can be programmed to operate autonomously, without human involvement, or the code can provide for direct, real-time control of the DAO and funds controlled by it.[1] The earliest DAOs are software controlled community organization experiments which seek to re-implement certain aspects of traditional corporate governance, replacing voluntary compliance with a corporation's charter with actual compliance with pre-agreed computer code.

'The DAO' (https://daohub.org/) is the most prominent example of a DAO. It gained significant media attention after it raised the equivalent of USD168 million from individual investors in its initial creation phase, making it the world's biggest crowdfunding project to date. However, on 17 June 2016, a weakness in *The DAO*'s code was maliciously exploited and it became materially compromised. It is unlikely to recover.

The DAO was the first significant experiment of this structure. It will serve as a case study for the industry but the design and structural decisions made by the creators of *The DAO* will not necessarily apply to all future DAOs.

DAOs were made possible by the development of Ethereum, a public blockchain which provides a decentralized virtual machine to execute peer-to-peer contracts using its native cryptocurrency, **Ether**. The Ethereum network uses Ether as the currency for transaction fees on its blockchain for the purpose of recompensing the computers of the network for providing computing power to validate actions taken on the Ethereum blockchain. Ether is therefore the underlying fuel for all Ethereum transactions.

[1] While the term 'DAO' is the most widely used term to describe the subject of this paper, some commentators distinguish DAOs (Decentralized *Autonomous* Organizations) from DOs (Decentralized Organizations), the distinction being that all functions in the former are automated and self-executing, whereas the latter is a decentralized model which incorporates human decision-making through member consultation. For the purposes of this paper and for consistency with general media commentary we use the term DAO throughout.

ETHEREUM

- Ethereum is a distributed network formed by thousands of nodes (computers running the Ethereum software) around the world. Whereas Bitcoin records the creation and transfer of bitcoins in its global ledger, Ethereum, in addition to recording the creation and transfer of Ether, stores computer scripts (so-called "**smart contracts**" and "**decentralized applications**" ("**dapps**")) and records their state.
- Anyone can create an Ethereum contract. Once deployed, that script will exist, permanently and publically, in the Ethereum blockchain (with a copy stored on every node in the Ethereum network). The distributed nature of Ethereum makes it very difficult, if not impossible, to prevent or otherwise interfere with (a) people creating Ethereum contracts, (b) people interacting with Ethereum contracts and (c) the automatic execution of each Ethereum contract exactly in accordance with its code.
- Ethereum contracts can be implemented in various Turing complete scripting languages. To prevent contracts that loop infinitely, which would waste the resources of the Ethereum network, the Ethereum platform charges a small amount of Ether per computation. Smart contracts can interact with other smart contracts and they can accept input from external sources known as 'oracles' (e.g. a Bloomberg reference price for a financial transaction). A DAO is a complex smart contract or set of smart contracts.

DAOS AND DAO TOKENS

- DAOs are a new innovation. There are several early implementations of the DAO concept, the most prominent of which is the framework (described here) developed by the creators of *The DAO* (and upon which *The DAO* itself is based).
- DAOs are funded by members using Ether and will usually provide its members with tokens, proportional to their investment, representing voting and ownership rights. DAO tokens are freely transferable and their price may vary over time, in a manner not dissimilar to company shares.
- A DAO is effectively a community, with its resources organized according to rules agreed in advance and set out in its code. DAOs are open source software, capable of modification through member consensus. Befitting its experimental, open source nature, there is no defined governance structure for DAOs, but *The DAO* introduced the concept of a '**Curator**', a participant who is tasked with maintaining the code of *The DAO*, proposing changes to *The DAO* and 'whitelisting' proposals. A Curator is also a failsafe against a 'Tyranny of the Majority', i.e. an individual or group buying or otherwise gaining control of 51% of *the DAO* tokens, abusing their voting power and sending all funds to themselves.
- A DAO will hold and deal with Ether according to the rules set out in its code. Anything beyond its programmed function (e.g. hiring a developer to write or audit code, developing a product or investing) requires input from DAO token holders. '**Contractors**' (i.e. actors in the physical world who can carry out tasks) can make proposals to a DAO to utilize some or all of its funds for the development of a product or service. *The DAO*'s token holders then debate and vote on any given proposal, usually during a set period of time.

THE DAO AND RECENT DEVELOPMENTS

- *The DAO* was created as a crowd-sourced investment fund and was the first of its type. Its creators, Simon and Christoph Jentzsch, are involved with another prominent company in this space, Slock.it, which was itself expected to be a recipient of investment by *The DAO*. The initial investment in *The DAO* stood at USD168m, but this has been significantly depleted by the June 17 attack, further defensive depletions by members of *The DAO* and the concomitant impact on the price of Ether.
- *The DAO* was a for-profit entity which took in funds from investors (in the form of Ether) in exchange for divisible and freely transferable tokens allocating ownership and voting rights. There are approximately 23,000 voting addresses of *The DAO*, although it is thought that approximately half of the invested funds came from 70 Ethereum addresses. *The DAO* existed to invest in companies, projects

and ideas, with the aim of providing a positive return (in the form of dividends or other benefits) to its participants. Token holders could vote on each proposal put to *The DAO*; *The DAO* thus relied on a participatory "wisdom of the crowd" for its investment decision-making. Positive votes from 20% of all tokens issued were required for passing a proposal, although no proposal ever put forward came near this threshold. A list of proposals put to *The DAO* can be viewed here. *The DAO* included a Curator, which was, in *The DAO*'s case, a team of well-respected individuals in the Ethereum community.

- Various issues were raised relating to the complexity of *The DAO*, code security and game theoretic resilience, structural biases and concentration of token ownership. Indeed, some of the early proposals put to *The DAO* concerned *The DAO* itself, including a proposal for a moratorium on proposals and voting until the code was fully audited and any fixes applied. Prior to the June 17 attack, the creators of *The DAO* proposed an upgrade to their DAO Framework 1.1, fixing (among other things) a 'recursive call' vulnerability found in Framework 1.0, upon which *The DAO* is based. Like all other proposals put to *The DAO*, it required approval from its token holders.
- On 17 June 2016, before any proposals were accepted by *The DAO*, a hacker was able to exploit an unintended operation of *The DAO*'s computer code and its underlying programming language to drain funds from *The DAO*. Those funds are currently sitting in a "child" DAO (part of the pre-agreed process by which investors withdraw funds from *The DAO*) waiting to be withdrawn by the hacker (which cannot happen before 27 July).
- In the meantime, there has been heated debate about whether and how to attempt to return the stolen Ether to investors. The majority of the remaining Ether was similarly drained from *The DAO*, this time by so-called "white hat" hackers (presumed good actors whose intent is to return the funds, proportionally, to investors). If these funds alone are successfully returned, it would represent a ~30% loss for investors. However, further complicating this scenario is that the original hacker was able to infiltrate the new child DAO, leaving those funds vulnerable to a further attack. In total, between 3% and 15% of all Ether is estimated to be at risk.
- Leaders of the Ethereum community (many of whom are investors in *The DAO*) have proposed to amend the Ethereum blockchain itself (a "hard fork") to undo *The DAO* completely and return all funds to investors. This proposal follows an earlier failed attempt to freeze the stolen Ether (by way of a "soft fork" software update, which would have effectively blacklisted the hacker's Ethereum address). The "hard fork" is being proposed as a remedial block to be added to Ethereum's blockchain. This block is yet to be determined but is due to occur in the near future and will incorporate an additional state transition function beyond the ordinary elements of transaction processing and miner reward. This block would (a) return the identified stolen Ether back to *The DAO* fund and (b) alter the broken DAO contract to refund the token holders pro rata. In advance of this hard fork miners and other stakeholders will need to update their software to the new hard fork version. It is important to note that, unlike a hypothetical fork of the Bitcoin blockchain, the proposed Ethereum hard fork would not 'roll back' all transactions in each block, as no Ether has been transferred out of any child DAO. The proposal only needs to reference *The DAO* and its child DAOs to effect the appropriate refunds of Ether.
- This hard fork proposal has initiated a broader debate within the Ethereum community. Proponents of the hard fork argue that such a solution is necessary to protect Ethereum's wider reputation and value, and a hard fork is a straightforward and equitable means of doing so. It would also be necessary to realise the future vision of Ethereum, which moves away from proof-of-work as the consensus mechanism towards a proof-of-stake system (broadly, consensus achieved by voting according to Ether holdings). For opponents, a hard fork would be entirely antithetical to Ethereum's cause. Ethereum's stated purpose, after all, is to provide an immutable, incorruptible record and a platform for unstoppable, code-as-law smart contracts. The hard fork would amount to an intervention – a bail-out of *The DAO* – seemingly at the behest of *The DAO*'s biggest investors

(themselves Ethereum developers and influential community members).

- Was *The DAO* too much, too soon, or is the viability of a Turing complete smart contract platform now in doubt? Very complex smart contracts based on Turing complete languages will inevitably contain bugs – or well-hidden, malicious code – and each smart contract controlling Ether represents something of a bounty for opportunists and hackers, requiring extreme levels of diligence. Indeed, in the case of *The DAO*, the hacker merely used the code to his or her advantage; in that sense, they acted in accordance with the terms of the smart contract and arguably there was no hack. The website dedicated to *The DAO* could not be clearer:

  "The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supersede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation."

- While this specific attack exploited vulnerability in the code of *The DAO*, it is hoped that the broader Ethereum community will quickly establish best practices and code will be subject to continued auditing, improvement and ultimately standardization, but there will invariably be teething troubles, hiccups and more losses before this is realized.

LEGAL STATUS OF A DAO

- "A word of caution, at the outset: the legal status of DAOs remains the subject of active and vigorous debate and discussion. Not everyone shares the same definition. Some have said that they are autonomous code and can operate independently of legal systems; others have said that they must be owned or operated by humans or human-created entities. There will be many uses cases, and the DAO code will develop over time. Ultimately, how a DAO functions and its legal status will depend on many factors, including how DAO code is used, where it is used, and who uses it. This paper does not speculate about the legal status of DAOs worldwide."

  The DAO whitepaper

- DAOs are not currently recognized as legal entities, creating uncertainty as to the legal rights attributable to a DAO and who bears the legal responsibilities. It is possible that in the abstract a DAO would fall within the categories of a general partnership or joint venture agreement between the participants. In such circumstances, courts will generally infer and impose such a structure on a DAO, in the absence of any formative document or articles. While a DAO might have extensive rules governing its conduct between internal members, those rules may be of little use when interacting with an external jurisdiction's legal system.
- Further challenges arise in respect of determining jurisdiction. What is the jurisdiction of a DAO and where are its members based? The developers of *The DAO* are known, but that will not always be the case – a DAO could be created by many contributors, some known, some not known, based in multiple jurisdictions, using servers based in yet more jurisdictions.
- DAO tokens represent the initial contribution by each investor, but if there is no legal entity they cannot be considered to be shares or ownership rights or stakes. However, the risk of regulators recharacterizing DAO tokens as securities remains. Absent legal certainty as to what a DAO is, and given the difficulty in properly identifying individual members of a DAO at any particular point in time, it will be very difficult to properly assign ownership in the product of contracts.
- These problems are exacerbated by the perceived focus on decentralization. For many participants a key feature of DAOs is unfettered and anonymous participation. Initial funding is necessarily sent from (and dividends paid to) pseudo-anonymous

Ethereum accounts and, in any event, DAO tokens are freely traded between accounts. The votes of participants are not attributed or attributable either.

CONTRACTING WITH A DAO

- On the face of it, *The DAO* had no legal personality or existence; it was a collection of computer scripts on the Ethereum blockchain. In an attempt to sidestep the thorny issues regarding the legal form of DAOs, developers of *The DAO* incorporated a company in Switzerland, DAO.Link, for the purpose of providing a physical entity with which Contractors could contract. According to Alexis Roussel, a co-founder of DAO.Link:

  "the main legal questions which DAO.Link can answer is that in Switzerland you don't need to specify the person in front of you that you want to make a contract with. You only need to show it's valid that the person on the other side is capable of making a decision."

- This structure provides a bridge between the digital world of DAOs and the physical world of Contractors, resulting in an invoice addressed to a Contractor containing DAO.Link's address and details. Until legislation and regulation can catch up with the innovative form of DAOs, it is likely that DAOs will employ this service company structure, or a similar mechanism, to effectuate interactions. Note that this solution requires individual or team direction from the developers of the relevant DAO, and the connection between the DAO and an entity purported to be associated with it may not be recognized in all jurisdictions.

DAO GOVERNANCE ISSUES

- The primary legal risk facing *The DAO*, and DAOs generally, is the status of their participatory tokens. On the one hand, DAO tokens represent a means of access and voting to a technological experiment, designed to improve and progress nascent projects on the new Ethereum ecosystem. On the other hand, DAO tokens represent an investment of potentially significant monetary value, with similar attributes to shares or equity.
- In the United States, this question turns on the purpose and intention of the investment. Given *The DAO*'s for-profit status, and the speculative trading of Ether undertaken by some individuals, it is possible that DAO tokens would be considered as the sale of investment contracts by the Securities Exchange Commission. One of the developers of *The DAO* has stated that they do not consider *The DAO* to be a company nor its tokens securities. In his view, it is conceived as an organization that helps Ethereum products by providing Ether, which may result in returns on Ether, or free services or products. Regulators generally have adopted a deliberate wait-and-see approach to blockchain innovation and it is likely that such a policy would inform any such action against *The DAO*. However, there is a strong countervailing argument that the structure, value and marketing of *The DAO* can be characterized as an illegal sale of securities (notwithstanding any assertion that "The DAO's code controls and sets out all terms of The DAO Creation"). In light of the significant investment that *The DAO* received, and the inherent flaws in *The DAO*'s code which permitted a malicious redirection of collective funds, regulators may well decide to adopt the latter approach if investors are ultimately left out of pocket.
- In addition to the risk of token recharacterization, the direct democracy model of DAOs poses practical issues of governance. For example, no proposal ever reached *The DAO*'s necessary threshold, and the risk of centralization of control by particular parties is exacerbated by the pseudo-anonymous identities of token holders. Although *The DAO*'s concept of a Curator was designed to alleviate these concerns, this solution does not provide the same detailed protections as a takeover code for example, nor did it protect against the June 17 attack.

POTENTIAL LIABILITY OF A DAO AND ITS PARTICIPANTS

- As discussed above, a DAO is not a readily identifiable legal entity. Its legal status would be determined by what interpretation a court, building on existing legal principles, would be willing to accept on the basis of a litigant's argument. Were a DAO to be considered a general partnership or a joint venture then liability would likely flow

through to the members. Such an exercise in tracing liability to members across jurisdictions (and attaching liability to a physical person connected to an Ethereum address) would be legally and practically problematic. In the absence of applying ownership liability, courts might, depending on the facts, be prepared to find liability against the developer, promoter or creator of the DAO.

– Had *The DAO* operated as intended, it is probable that ordinary liability for transactions undertaken on its behalf would have been attributed to DAO.Link, its Swiss-incorporated service company, depending on the context and cause of action. DAO.Link exists as a Sàrl (a limited liability company under Swiss law) and therefore a successful action against it would only extend to whatever assets it holds.
– In the context of the June 17 attack, it is possible that a court could consider the actions of the hacker to constitute criminal conduct, and potentially theft. The fact that *The DAO* code technically permitted these actions, which were therefore permitted under the rules of *The DAO*, would not necessarily be determinative. The malicious intent to take Ether belonging (collectively) to all the token holders could meet the requisite threshold, depending on a number of factors, including the hacker's intent and how their actions are categorized under existing criminal statutes. In addition to potential criminal penalties, the hacker could potentially be sued for civil damages, although the primary obstacle to any such action would be identifying the hacker. Depending on the ultimate resolution to the June 17 attack, it is possible that some form of litigation will be pursued by some of the parties involved against either the hacker, the promoters of the DAO, the Ethereum Foundation or identifiable token holders. Given the most recent proposal to "hard fork" the Ethereum blockchain and reverse the hacker's transactions, it may be that the hacker will be the first litigant seeking redress.

"If I would have known the size it has grown to, maybe the tester in me would say, 'I need more testing'. This is very risky. It's all new land."

— FOUNDING DEVELOPER OF THE DAO, CHRISTOPH JENTZSCH, IN AN INTERVIEW WITH THE *NEW YORK TIMES*, MAY 21, 2016

Key contacts

Lawson Caisley
Partner
UK – London
Tel +44 20 3088 2787
lawson.caisley@allenovery.com

David Lucking
Partner
USA – New York
Tel +1 212 756 1157
david.lucking@allenovery.com

Michael Zdrowski
Associate
UK – London
Tel +44 20 3088 4034
michael.zdrowski@allenovery.com

Conor O'Hanlon
Associate
USA – New York
Tel +1 212 610 6423
conor.ohanlon@allenovery.com