WORK IN PROGRESS

ADM+S ARC Centre of Excellence for Automated Decision-Making and Society

ADM+S WORKING PAPER SERIES

Decentralising Data Governance: Decentralised Autonomous Organisations (DAOs) as Data Trusts

June 2022

Author:
Kelsie Nabben, RMIT University

WORKING PAPER 003

admscentre.org.au/publications

ACKNOWLEDGEMENT OF COUNTRY

In the spirit of reconciliation, we acknowledge the Traditional Custodians of Country throughout Australia and their connections to land, sea and community. We pay our respect to their Elders past and present, and extend that respect to all Aboriginal and Torres Strait Islander peoples today.

ABSTRACT

This paper explores the idea that Decentralised Autonomous Organisations (DAOs) are a new type of data trust for decentralised governance of data. In data trusts, a responsible party is legally appointed as the trustee over a group of people's data to act on behalf of their preferences [1]. The aim is to return power to individuals regarding the use of their personal data through data stewardship. This means that 'the trustworthy and responsible use and management of data' can unlock the value of aggregated data in a fairer way [4]. The intent behind DAOs is to allow people to coordinate and govern themselves based on rules encoded in software on a public blockchain [2]. Rather than legally appointing a representative to negotiate and enforce data governance through legal mechanisms, decentralised blockchain-based systems inscribe the rules in software code where they are transparent, verifiable and enforceable. The idea and practice of DAOs has gained prominence in blockchain communities since it was first discussed in 2013 [3]. Digital tokens are then used to align incentives among diverse stakeholders in the system.

If DAOs were conceptually and even legally treated as data trusts in the governance of data, then DAOs would have the fiduciary duty to act on behalf of participants' interests. It would be enforceable through software code, rather than relying on traditional legal mechanisms. To explore this idea, I outline the fundamentals of trusts and data trusts as a data governance framework, then introduce the idea of DAOs as data trusts to steward and utilise data on behalf of participants. Consecutively, I explore possible cases and early examples of DAOs as composable data governance infrastructures in blockchain communities. I find that DAOs are a promising decentralised governance infrastructure for people to operationalise the principles of data trusts, whereby the promise of data stewardship can be entrusted to software code for accountable self-governance rather than relying on third-party legal recourse. This contribution lends itself to further scholarly research and industry practice to test DAO data trusts as a data governance model for greater individual autonomy, verifiability, and accountability.

KEYWORDS: DATA TRUST, DECENTRALISED AUTONOMOUS ORGANISATION, DATA GOVERNANCE, BLOCKCHAIN, AUTOMATION

Suggested citation: Nabben, K. (2022) *Decentralising Data Governance: 'Decentralised Autonomous Organisations (DAOs) as Data Trusts'*, ADM+S Working Paper Series 2022 (003), ARC Centre of Excellence for Automated Decision-Making and Society,
DOI: 10.25916/yzht-7y29

TABLE OF CONTENTS

1. INTRODUCTION

Data utilisation and monetisation are critical challenges of the information age. At present, in many digital platforms and applications, data is abstracted away from the individuals that contribute to it and is stored in silos. Here, corporate actors can extract the value derived from the data (commonly once aggregated and processed), often without informed consent or benefit to the contributors. What is missing is a governance framework and institutional enforcement mechanism that places participants in control of 'their' data to utilise and benefit from.

This article explores the research question: 'can the concept of data trusts apply to Decentralised Autonomous Organisations (DAOs)?' I investigate if DAOs, as a decentralised data governance structure for digital data, can empower users to better control, store and express their preferences over how their data is utilised. If DAOs were designed and programmed to operate like data trusts, then the DAO would have the fiduciary duty for data governance on behalf of participants, and this would be enforceable in the rules of the system. Thus, issues of enforcement around data use and abuse in the digital economy could potentially be mitigated.

Contributions

The key contributions of this paper are:

1. An investigation of how the concept of data trusts applies to DAOs.
2. An examination of if and how DAOs as data trusts may provide greater accountability and recourse over data stewardship for participants through software-encoded governance, rather than traditional legal recourse.
3. An exploration of examples and possibilities of DAOs as data trusts emerging in decentralised blockchain communities.

Structure of This Paper

The remainder of this paper is structured as follows. First, I outline the fundamentals of trusts, the concept of data trusts as a data governance framework, the idea of DAOs as data trusts to steward and utilise data on behalf of participants, and the transition from reliance on legal mechanisms to reliance on code for accountability and recourse in DAOs. I then explore possible cases and early examples of this governance infrastructure used in practice in blockchain communities. I find that

DAOs are a promising digital governance infrastructure for people to operationalise the principles of data trusts, whereby the promise of data stewardship is entrusted to software code and self-governance, rather than third-party legal representatives. I am careful to highlight the potential benefits and limitations of this approach throughout the paper.

This contribution lends itself to further scholarly research and industry practice to test the concept of DAO data trusts as a data governance model for greater individual autonomy and verifiability.

2. DATA GOVERNANCE: FROM DATA TRUSTS TO DATA DAOS

Legal Trust Structures

While there are no one-size-fits-all data governance frameworks, data trusts are a novel data governance structure among others, including data collaboratives, data foundations and data cooperatives [4].

Trusts have existed for centuries. They are an important innovation in property rights law by separating properties' legal ownership and control from its equitable ownership and benefits [5]. A trust is a legal relationship in which the holder of a right (a 'beneficiary' or 'trustor') transfers power over to another person or entity (a 'trustee') to act on their behalf [6]. Thus, the trustee is the legal owner of the property on behalf of the beneficiary or beneficiaries, and is able to maintain, use and control the property as they see fit. The beneficiary is the equitable owner of the property of the trust, and is able to enjoy the benefits of the property. Trustees are generally compensated for performing their role and penalised through the legal system for breaching their fiduciary duty in a court of law. Examples of trusts include land trusts, testamentary trusts, purpose trusts, employee trusts and co-ownership.

Data Trusts

Data trusts are a relatively new concept. They are predicated on participatory, democratic, cooperative governance structures whereby a legal entity acts as an independent fiduciary steward of data. Data trusts are a data governance and utilisation structure that allows individuals to state their aspirations for data use and mandates a trustee to represent those interests through the legal

mechanism of trusts [1]. The trustee bears a fiduciary duty to exercise data rights on behalf of beneficiaries.

Members pool their data and appoint a legal trustee. The legal trustee is bound by a fiduciary obligation to exercise data rights, such as those granted by General Data Protection Regulation (GDPR), on behalf of the trust's beneficiaries. This includes negotiations on aggregated data between the data trustee on behalf of beneficiaries, and data collectors or analytics organisations on how the data is utilised or monetised in accordance with the terms of the trust.

A key motivation behind data trusts is to distribute the benefits arising from data more equitably. 'A successful data Trust will be one whose constitutional terms better encapsulates the aspirations of a large part of the population' state Delacroix and Lawrence [1]. Data trusts aim to address dark patterns of data use that create vulnerabilities for individuals or groups as patterns of data collection, and continue to evolve [4].

To do this, data trusts rely on nation-state regulatory instruments for different types of data (such as the GDPR framework in the European Union) to confer rights. According to the Centre for Internal Governance Innovation, 'Like powers of attorney, data trusts are flexible and de facto global' [7]. This means that they can be written in ways that create legally accountable governance structures. Another way to think about a data trust is 'as a container — one that can hold assets' [8]. The essential characteristics of a data trust are a clear purpose, a legal structure (including trustors, trustees and beneficiaries), some rights or duties over stewarded data, a clearly defined decision-making process, an articulation of how benefits are shared and a sustainable funding model.

Data trusts create a vehicle for individuals to state their aspirations for data use and appoint a trustee to pursue these aspirations for stronger accountability. Once data is pooled and governed under a data trust, it can be utilised in the interests of the constituents of the trust, who become both data providers and data beneficiaries. In 'bottom-up' data trusts, beneficiaries are the data subject that pool their data, and data trustees have a fiduciary responsibility to exercise their interests in data use and rights, such as entering into data sharing agreements on their behalf, negotiating terms with service providers and monitoring compliance with terms of agreements by leveraging the negotiating power of pooled data in negotiations [1]. Uses of the data could include data monetisation through selling data to train machine learning algorithms or for data mining, and donation to support medical research or open science. An example of this is the model of Swiss cooperative 'MIDATA', which allows owners of data to actively contribute to medical research for the

common good by granting selective access to their personal data [9]. This collective consent and bargaining structure aim to protect the interests of individuals and is viewed as an approach to realise the data mining potential of large datasets without compromising the rights of individuals.

3. DATA TRUST BENEFITS AND LIMITATIONS

Benefits

The benefits of data trusts are numerous. Data trusts provide the structure of fiduciary governance as a flexible institutional vehicle that can minimise and contain the risks around experimenting with different models of governance. Data trusts can act as a way for data rights holders to aggregate and build leverage towards collective bargaining for more balanced, publicly beneficial data relationships. Data trusts are also viewed as a potential structure for greater self-determination over data privacy after years of 'weak consent-based models' of check boxes and legal jargon [10]. Thus, data trusts offer a solid basis for experimentation to solve problems that require data to adapt and develop the rules of governance according to specific use cases. Data trusts can continue to steward, maintain and manage how data is used and shared, including access, who gets to define those terms and penalties for misbehaviour. Scholars envision an 'ecosystem' of data trusts with different rules and risk profiles so that individuals can choose and change how their data is utilised for public good purposes or financial returns [1]. Relevant data trust case studies for this ecosystem include medical data, genetic data, social media data, financial data and loyalty card data.

Limitations

Trust structures can be powerful in their approach to participatory ownership as well as limited. This is due to their reliance on trustees to act in the interests of beneficiaries, and beneficiaries' dependence on traditional legal recourse if things go wrong, such as data being leaked where it cannot be revoked.

A key contention with data trusts is that flexibility in the preferences of beneficiaries and the rules of the trust mean that data trusts rely on traditional mechanisms of legal recourse if things go wrong [7]. Yet, if trustees fail to act in the interests of beneficiaries, data is not well-stewarded, or the appropriate business models are not applied to steward data in the individuals' or public interest, mistakes are expensive and time consuming to dispute.

As data trusts develop from theory to practice, gaps in understanding the form and function of these trusts remain. Where data trusts fit in the broader data governance landscape is dependent on incumbent institutional safeguards, accessibility for broad participation and inclusion in design and decision-making, finance and sustainability, and how they are implemented [11]. For example, technical architectural challenges, such as how an individual disentangles and extracts their unique data to 'exit' a trust once it is collected and collated is difficult, if not impossible.

In contrast, a DAO clearly defines and expresses rules in software code. DAOs can incorporate semi-automated dispute resolution and arbitration mechanisms. The next section further explores the concept of DAOs and how these could apply as a governance infrastructure for decentralised data trusts.

4. A PROPOSAL FOR DAOS AS DATA TRUSTS

A DAO is a blockchain-based system that enables participants to coordinate and govern themselves, mediated by a set of self-executing rules deployed on a public blockchain (although the concept stems from cybernetics and pre-dates blockchain technology and applications) [2], [12]. Governance in a DAO is decentralised from any central point of control and reliant on people to define the rules and software code and automation to execute the rules.

In a data trust, the 'overriding aim of the governance structure is to achieve trust' between participants in the trust and other stakeholders who wish to utilise the data [13]. Conversely, blockchain technology provides an infrastructure to distribute trust between disparate parties and enforce rules through software code for collective self-governance. Blockchain is sometimes referred to as 'trustless' infrastructure [14].

This governance philosophy and technology emerges from the ideas of a distributed group of cryptography advocates and hackers in the 1990s known as the 'cypherpunks', who advocated for the use of encrypted technologies for greater individual rights in society [15]. From these origins, DAOs have been ideated and invented to facilitate the collective self-governance of cryptocurrencies, social tokens, decentralised finance protocols (financial ecosystems made up of applications built on the blockchain known as decentralised finance) and more.

As Vitalik Buterin, the co-founder of Ethereum blockchain, stated in 2014 [16], *'instead of a hierarchical structure managed by a set of humans interacting in person and controlling property via*

the legal system, a decentralized organization involves a set of humans interacting with each other according to a protocol specified in code, and enforced on the blockchain'.

What is required to design DAOs as data trusts is a clear purpose, an infrastructure of smart contracts and tokens, clear rights and duties over stewarded data, clearly defined decision-making processes, an articulation of how benefits are shared and a token-economic model for sustainable funding. This aligns neatly as an evolution on the aforementioned essential characteristics of a data trust, including a clear purpose, a legal structure between stakeholders, rights or duties over stewarded data, a clearly defined decision-making process, an articulation of how benefits are shared and a sustainable funding model.

With a DAO as a data trust, the DAO itself is the trustee. It will have fiduciary responsibility for stewarding data on behalf of beneficiaries, with rules represented and enforced in software code rather than nation-state law and legal enforcement mechanisms.

In such cryptocurrency enabled institutional structures, blockchain-based digital tokens are leveraged as value to align incentives [17]. This can be rewarded to beneficiaries for contributing data as payment to fund the operations of the DAO. It can also be used as staked collateral that risks penalty upon misbehaviour, enforcing consensus over what is deemed desirable behaviour in the system. According to this ethic, what constitutes 'good behaviour' is self-determined by those who design the system and those who consent to this by choosing to participate.

Algorithmic Enforcement

Software-encoded data DAOs means that the rules pertaining to data governance, portability, erasure, access and use can be verifiable and enforceable. Where rules or conduct beyond the enforcement capabilities of the blockchain are suspected to be violated, DAOs are adopting a range of arbitration mechanisms, including decentralised, software-based 'courts' such as Kleros and Celeste [18], [19].

5. DATA DAOS IN PRACTICE

Data DAOs could be implemented in a number of ways, and the composable modules for data markets, storage and governance largely already exist in blockchain technology ecosystems.

There are ongoing efforts in various blockchain protocol communities to standardise data formats to be blockchain compatible, such as ERC20 (fungible, meaning interchangeable for others of the same kind) and ERC721 (non-fungible, meaning a unique or one of a kind) tokens [20]. The innovation of these token standards is that they effectively produce wrapped data as a collateral asset so it can be utilised. Further, a number of data storage protocols exist to coordinate the storage, querying and retrieval of data in a decentralised manner to empower individual users (for specific examples, see projects: Filecoin, Arweave and Storj) [21]. These data storage protocols allow users to negotiate contracts that express their preference over where and how data is stored in a verifiable way. Users can also choose to participate in these protocols by running a validator 'node' for stronger governance rights in the underlying infrastructure they use for their data. Once data is uploaded and stored, it can be pooled into data pools, queried and utilised according to the preferences of the beneficiaries. DAOs then provide a collective bargaining layer of governance for coordination, arbitration, rule enforcement and distribution of benefits.

Use Cases

DAOs as data trusts could be applied to short- and long-term use cases, such as training machine learning algorithms, donating to medical research, monetising creative expressions or solving complicated problems in crises.

Some projects have begun exploring the concept of decentralised finance (DeFi) for data. Here, data could be wrapped, staked, yielded, farmed and more.

The infrastructure to make this possible is already being built with programmable storage, such as virtual machine capabilities on Filecoin, DAOs, 'Non-Fungible Tokens' (NFTs) and the concept of decentralised data unions [22], [23], [24]. Ocean Protocol is pioneering the idea of 'compute to data', whereby algorithms and compute jobs are matched in a marketplace to buy and sell data without exposing the content of that data to preserve privacy [25]. Computation occurs without the data leaving the premises of the data holder, for privacy preserving analytics, AI modelling and more. Other methods to privacy preserving data computation, such as privacy preserving smart contracts and secure enclaves known as 'Trusted Execution Environments', have been proposed by Oasis Protocol and others [26].

The combination of these components with DAOs as data trusts enables whole new possibilities for decentralised, participatory data governance. One of these is that entire cities could build and own a

DAO, with firms in the city able to access that data on terms governed by the DAO with token-mediated transactions and permissions [27]. The concept of DAOs as data trusts offers a more concrete data governance framework to operationalise the implementation of this proposal.

6. BENEFITS AND LIMITATIONS OF DATA DAOS

Benefits

Data DAOs afford collective bargaining power to participants, allowing them to express preferences over data governance, storage and utilisation via software code, and token-based incentives for enforceability. Other benefits include potential efficiency gains for distributed and scalable governance, privacy and new ways to utilise data.

In terms of efficiency, DAOs enable the ability for DAO participants to collectively pool and aggregate data, appoint algorithmic agents or human labour in the DAO to advocate on behalf of the use of the data for the benefit of contributors, and provide tools for management of administrative functions (e.g., multi-signature wallets).

DAOs may also afford privacy benefits to participants. Depending on the rules of the DAOs, sometimes participants can remain anonymous. Further, public blockchain technology was birthed out of encryption technology, and privacy via encryption is highly valued in some blockchain communities. Data can be encrypted-by-design in decentralised networks and stakeholders can choose to remain pseudonymous or anonymous in their interactions depending on the design of the protocol.

This could aid both beneficiaries of data DAOs as well as traditional data trusts to innovate data governance and utilisation practices. Further, within the emerging area of research on relationships between DAOs and individuals, software enabled data trusts may provide greater optionality and low switching costs. This will empower people to choose which DAO they would like to apply to their data and allow them to switch between data DAOs if they wish to exit one and participate in another.

Potential Limitations

Marrying the concepts of DAOs and trusts to govern data requires further research into the benefits and risks of this approach.

DAOs are extremely experimental governance models as both the scholarship and tooling surrounding these governance infrastructures are constantly evolving through active research and development in decentralised technology communities. DAOs can have unintended technical and social consequences, such as hacks or inequality between engineer designers who structure the rules of code and participants in the system [28], [29]. The societal outcomes of DAOs remain understudied.

DAOs are heterogenous, manifesting themselves in many forms for different objectives. Examples of DAO purposes range from shared investment vehicles such as 'FlamingoDAO', whereby registered investors pool funds to purchase NFTs in the hopes of return on investment, to social clubs such as 'Friends With Benefits', to the development of individual software ecosystems such as '1Hive'. Different objectives mean that some DAOs optimise for a diversity of goals, including financial upside, ideologically driven aspirations towards decentralised software development, social engagement or more complex social purposes.

DAOs also vary widely in legal structure, from registered legal entities for participation by United States accredited investors only, to completely unregistered, open-source software organisations. This means that adopting a DAO governance framework may subject participants to a significant degree of legal ambiguity or liability.

Further, the role of people and algorithms across these software-encoded assemblages remain undetermined. The responsibility of who gets to govern in decentralised technology systems largely falls on engineers, surfacing questions with regards to the 'neutrality' of decisions made by algorithms in the system.

7. CONCLUSIONS

The information age has brought about significant changes in patterns of data collection and use, which are difficult to predict and respond to. In this context, society will need a range of governance tools to anticipate and respond to emerging digital opportunities and challenges. DAOs are an active site of experimentation in governance. With a concentration of software engineering talent and governance researchers, rapid iteration on data governance rules, practices and tools may be possible.

This paper has explored the fundamentals of data trusts and DAOs, proposing DAOs as a data governance framework and operational infrastructure for collective data pooling, management of shared resources and utilisation of data in a more accountable way.

Data trusts provide a general-purpose framework for DAOs to model data storage and utilisation design and implementation. By conceiving of DAOs as data trusts, the motivation of distributing the benefits of pooled data and protection of personal data is enacted through trust in code as DAO stewards negotiate on behalf of the beneficiaries. This is a logical evolution of data governance, with DAOs as a governance infrastructure (at this stage, for the digitally native due to user experience limitations and digital literacy requirements). DAOs as data trusts un-silo data while allowing for persistent individual control, storage, governance and utilisation that benefits contributors to the network. Just as data trusts are one component of governance, which is interdependent on policies, politics, rights, other infrastructure, economics and more, data DAOs are one approach to structuring data governance through DAO infrastructure.

The contribution of this article on data DAOs has been to go beyond recognising decentralised digital institutional technology and data as a resource, to a deeper exploration of the digital data governance framework in order to optimise decentralised data governance. This contribution invites further scholarly research and industry practice to test the concept of DAOs as data trusts as a data governance model for greater individual autonomy, verifiability, and accountability.

ACKNOWLEDGEMENTS

Special thanks to Professor Trebor Scholz from The New School, Professor Jason Potts from RMIT Blockchain Innovation Hub, Zargham from Blockscience, and Nathan Schneider for conversations and feedback.

REFERENCES

[1] S. Delacroix and N. D. Lawrence, "Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance," *International Data Privacy Law*, vol. 9, no. 4, pp. 236–252, Nov. 2019, https://doi.org/10.1093/idpl/ipz014

[2] S. Hassan and P. De Filippi, "Decentralized autonomous organization," *Internet Policy Review*, vol. 10, no. 2, Apr. 2021. [Online]. Available: https://policyreview.info/glossary/DAO

[3] V. Buterin, "Bootstrapping a decentralized autonomous corporation: Part I," *Bitcoin Magazine*, Sep. 2013. [Online]. Available: https://bitcoinmagazine.com/technical/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274

[4] V. Pavel, "Exploring legal mechanisms for data stewardship," Ada Lovelace Institute and UK AI Council, Mar. 2021. [Online]. Available: https://www.adalovelaceinstitute.org/report/legal-mechanisms-data-stewardship

[5] A. W. Scott, "The importance of the trust," *University of Colorado Law Review,* vol. 39, p. 177, 1966.

[6] H. Hansmann and U. Mattei, "The functions of trust law: A comparative legal and economic analysis," *New York University Law Review,* vol. 73, no. 2, pp. 434–479, May 1998.

[7] B. Wylie and S. M. McDonald, "What is a data trust?," Centre for International Governance Innovation, Oct 2018. [Online]. Available: https://www.cigionline.org/articles/what-data-trust/

[8] J. Hardinges, "Defining a 'data trust'," Open Data Institute, Oct 2018. [Online]. Available: https://theodi.org/article/defining-a-data-trust/

[9] MIDATA, "My data – our health." https://www.midata.coop/en/home/ (accessed Mar 2022)

[10] A. Ruhaak, "How data trusts can protect privacy," *MIT Technology Review*, Feb. 2021. [Online]. Available: https://www.technologyreview.com/2021/02/24/1017801/data-trust-cybersecurity-big-tech-privacy/

[11] Data Trusts Initiative, "Data trusts: From theory to practice, working paper 1." Accessed: Jan. 4, 2022. [Online]. Available: https://static1.squarespace.com/static/5e3b09f0b754a35dcb4111ce/t/5fdb21f9537b3a6ff2315429/1608196603713/Working+Paper+1+-+data+trusts+-+from+theory+to+practice.pdf

[12] W. Dilger, "Decentralized autonomous organization of the intelligent home according to the principle of the immune system," in *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, 1997, pp. 351–356, doi: 10.1109/ICSMC.1997.625775.

[13] C. Reed and P. Masons, "Data trusts: Legal and governance considerations," BPE Solicitors, Apr. 2019. [Online]. Available: https://theodi.org/wp-content/uploads/2019/04/General-legal-report-on-data-trust.pdf

[14] C. Berg, S. Davidson and J. Potts, "Blockchains industrialise trust," *SSRN*, Nov. 2017. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3074070

[15] K. Nabben, "Resilience as 'political decentralization': An alternate history of the cypherpunks origins of decentralised technology," *SSRN*, Oct. 7, 2021. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3938626

[16] V. Buterin, "DAOs, DACs, DAs and more: An incomplete terminology guide," May 2014. [Online]. Available: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

[17] S. Davidson, P. De Filippi and J. Potts, "Disrupting governance: The new institutional economics of distributed ledger technology," *SSRN*, Jul. 2016. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2811995

[18] L. Bergolla, K. Seif and C. Eken, “Kleros: A socio-legal case study of decentralized justice & blockchain arbitration,” *SSRN*, Jul. 30, 2021. [Online]. Available: http://dx.doi.org/10.2139/ssrn.3918485

[19] Celeste, “Introduction,” viewed Mar. 2022. [Online]. Available: https://1hive.gitbook.io/celeste/

[20] T. McConaghy, “Ocean datatokens: From money Legos to data Legos,” Sep. 2020. [Online]. Available: https://blog.oceanprotocol.com/ocean-datatokens-from-money-legos-to-data-legos-4f867cec1837

[21] Ocean Protocol Team, “Filecoin storage integrated with Ocean Protocol by Protofire,” Jul. 2020. [Online]. Available: https://blog.oceanprotocol.com/filecoin-storage-integrated-with-ocean-protocol-by-protofire-896dd03a1f04

[22] R. Kripalani, “Introducing the Filecoin Virtual Machine,” Nov. 2021. [Online]. Available: https://filecoin.io/blog/posts/introducing-the-filecoin-virtual-machine/

[23] Streamr Network, “Introduction to data unions,” viewed Dec. 20, 2021. [Online]. Available: https://streamr.network/docs/data-unions/intro-to-data-unions

[24] D. Dutta, “Datatokens, DAOs and NFTs,” Dec. 2021. [Online]. Available: https://blog.oceanprotocol.com/datatokens-daos-and-nfts-14aedce1bba7

[25] Ocean Protocol Team, “Compute-to-data is now available in Ocean Market,” Apr. 2021. [Online]. Available: https://blog.oceanprotocol.com/compute-to-data-is-now-available-in-ocean-market-58868be52ef7

[26] N. Hynes, D. Dao, D. Yan, R. Cheng and D. Song, “A demonstration of sterling: A privacy-preserving data marketplace,” *Proceedings of the VLDB Endowment*, vol. 11, no. 12, pp. 2086–2089, Jul. 2018. Doi: 10.14778/3229863.3236266

[27] J. Potts and T MacDonald, “New data city: The future of the digital CBD as a data pool on a DAO,” *SSRN*, Jul. 23, 2021. [Online]. Available: https://dx.doi.org/10.2139/ssrn.3892009

[28] Q. DuPont, “Experiments in algorithmic governance: A history and ethnography of ‘The DAO,’ a failed decentralized autonomous organization,” in *Bitcoin and Beyond*, 1st ed., M. Campbell-Verduyn, Ed., Routledge, 2017, ch. 8, pp. 157-177.

[29] K. Nabben, “Is a ‘decentralized autonomous organization’ a panopticon? Algorithmic governance as creating and mitigating vulnerabilities in DAOs,” in *Proceedings of the Interdisciplinary Workshop on (de)Centralization in the Internet* (*IWCI'21*), Oct. 2021, Association for Computing Machinery, pp. 18–25. Doi: 10.1145/3488663.3493791

admscentre.org.au

Australian Government

Australian Research Council

This Centre is funded by the Australian Government through the Australian Research Council

ADM+S