Digital Regulation Cooperation Forum

# Insight Paper on Web3

January 2023

# 1. Introduction

As services provided by online platforms become increasingly intrinsic to our everyday lives, people are asking whether we have adequate control over our data, content and activities online?[1]

For some, the answer to this question lies in visions for a reconfigured version of the web, typically referred to as 'Web3' or 'Web 3.0'. Many proponents of the Web3 vision aim to provide users with greater control over their data, content and online activity by changing the infrastructure upon which many of the applications that operate on today's web are built.[2] For others, such visions are ill-defined, fall short of their promises and are associated with existing applications used for fraud, scams and other consumer harms.[3]

In November 2021, the Digital Regulation Cooperation Forum's (DRCF) member regulators – CMA, Ofcom, ICO and FCA – launched a technology horizon scanning programme, 'Joining up on future technologies', to provide a coherent view of new and emerging digital markets and technologies. Digital innovation drives significant benefits for consumers, businesses, and the wider economy. Regulation is increasingly important to ensure that consumers' and citizens' interests are at the heart of digital innovation. To do this well, regulators need to stay ahead of the changes in digital and online services. As part of these efforts, the DRCF brought together representatives from academia, industry, government and regulators at its Web 3.0 Symposium in October 2022 to understand how technologies associated with Web3 are evolving and identify regulatory opportunities and challenges facing both firms and public authorities.[4]

Some key digital markets operating via today's 'Web 2.0'[5] are characterised by a small number of very large firms who hold extremely powerful positions within these markets. This Insights Paper considers the extent to which Web3 could achieve the goal of redistributing power away from these firms with the aim of improving outcomes for consumers and citizens. It also assesses the wider impact that the key concept (decentralisation[6]) and technology (distributed ledger technology (DLT)[7]) behind Web3 might have for consumers and citizens. Applications associated with Web3 are largely novel and so far have not been widely adopted. It remains unclear whether and in what form Web3 might evolve. While the ability of Web3 to solve the problems associated with Web 2.0 is yet to be compellingly proven, new Web3 applications present identifiable risks and harms as well as potential benefits. Building on the contributions at the DRCF's Web3 Symposium, this Insight Paper:

- Provides context to the ideas behind visions for Web3 with a brief history of the development of the web and explains the key concepts and technologies underpinning these visions – 'decentralisation' and 'distributed ledger technologies' (DLTs) ('**Definition & Overview**')

[1] CMA (2020), 'Online platforms and digital advertising market study final report', pp.6, 8, 316-321
[2] See for example Web3 Foundation (2022) 'About'. Accessed 19 December 2022.
[3] See for example National Cyber Security Centre (2021) 'NCSC position on distributed ledger technology', 21 April and Protocol (2022), '"People were sucked into schemes": Inside Molly White's campaign against crypto', 20 October.
[4] See DRCF (2022) 'Web 3.0 and distributed ledger technologies – A regulatory perspective', 10 November. See also Definition and Overview for an explanation of 'Web3'.
[5] See Definition and overview.
[6] See Decentralisation.
[7] See Underlying technologies.

- Presents the DRCF's perspective on the possible benefits of the concepts and technologies associated with Web3 as well as the existing and potential consumer harms and wider societal risks ('**Benefits, Risks & Harms**')
- Explores the regulatory considerations across the DRCF member regulator remits that may be relevant to applications related to Web3 ('**Regulatory Considerations**')
- Sets out the DRCF's next steps in relation to Web3 as well as its wider 'Joining up on future technologies' work programme ('**Summary and next steps**')

This paper is the culmination of a literature review as well as the contributions from panellists and a futures workshop at the DRCF's Web3 Symposium.[8] It also draws on our conversations with industry and other non-peer reviewed sources. Where appropriate, we have maintained a 'technology neutral' stance, considering the services and applications built on top of the technologies rather than the technologies themselves, whilst critically assessing any claimed benefits, risks and harms. Some of the most developed use cases associated with Web3 have been highlighted throughout the paper to demonstrate how these benefits, risks and harms may take effect.

The paper focuses on the central concept underlying the various 'Web3' visions – decentralisation – as well as the key technology through which it is proposed that these visions could be achieved – DLT.[9] It considers current and anticipated DLT applications associated with 'Web3' including:

- Digital assets, including fungible tokens (more commonly referred to as 'cryptocurrencies' or 'cryptoassets'[10]) and non-fungible tokens (NFTs)
- Decentralised finance (DeFi) applications, offering cryptoasset services, including trading venues, lending and borrowing, payments, crowdfunding and insurance
- Other decentralised applications (dApps), including gaming, music streaming, social media, online advertising services, and information management systems
- Decentralised digital ID
- Decentralised autonomous organisations (DAOs)

This paper has not considered any technologies other than DLTs that have been proposed as ways to decentralise the web.[11]

This paper is intended to foster further discussion among and with our stakeholders in industry, academia, government, public bodies and other parties interested in Web3. It should not be taken as an indication of current or future policy by any of the DRCF member regulators, nor should it be read as providing any guidance on the regulatory requirements of any of the DRCF member regulators.

Equally, the paper and the DRCF member regulators do not endorse any of the Web3 visions or promote a particular version of a future web.

We welcome any comments or suggestions in relation to this topic. Please contact us at JoiningUpOnFutureTech@ofcom.org.uk.

[8] See DRCF (2022) 'Web 3.0 and distributed ledger technologies – A regulatory perspective', 10 November.
[9] Decentralisation and DLT were identified by panellists at the DRCF's Web3 Symposium as the key concept and technology behind aspirations for a 'Web3'. See DRCF (2022) 'Web 3.0 and distributed ledger technologies – A regulatory perspective', 10 November.
[10] This paper will use the term 'cryptoasset'. Most cryptoassets are not underpinned by any currency or other asset and are not considered to be a currency or money. For more, see FCA (2022) 'Cryptoassets'.
[11] Including for example other distributed web services such as federated services (e.g. Mastodon) and non-blockchain based peer-to-peer services (e.g. Napster).

## 2. Definition, conceptual and technical overview

There is little consensus on the definition of Web3.[12] The term stems from the idea that the web is iteratively evolving, and that in the future there will be a third 'iteration' of the web.

The concept of the 'World Wide Web' was first introduced in a white paper by Sir Tim Berners-Lee in 1989.[13] Initially, content producers used the web to host content on static web pages that visitors of the web could view. With the required technical know-how, anyone could host content on the web by building their own website. Retrospectively, this era of the web is often referred to as 'Web 1.0'.

In the early 2000s, website design and usage began to change. Websites became increasingly interactive, adding functionality beyond the basic display of information. This enabled the development of web-based services, which allowed users to interact with each other and services online in more sophisticated ways. This evolution resulting in the web we use today is often referred to as 'Web 2.0'. One defining characteristic of Web 2.0 has been the small number of companies who, enabled by a range of factors, have been able to gain significant market power, acting as gatekeepers to content consumption, creation and provision. Many of the services provided by these companies are platform-based and are often funded by targeted ad-based business models, in which services are offered in return for permission to process users' data.

Speculation about how a third 'iteration' of the web might evolve first started to grow in 2006.[14] In 2014, Gavin Wood, a co-founder of the blockchain-based software platform Ethereum and founder of the Web3 Foundation, presented his vision for the future of the web.[15] Throughout this paper we will refer to Wood's vision as an example of a common understanding of the concept of Web3, and the technologies commonly associated with it.

Proponents of this Web3 vision often state that it aims to re-balance power on the web between users and online platforms and provide users with greater control over their data. There are a range of ideas about how this might be achieved; most, however, point to decentralisation as the underpinning concept and DLT as the underlying technology.[16]

### Decentralisation

The concept of decentralisation encompasses a variety of different disciplines and draws on a range of technical, ethical, political and economic perspectives.[17] Vitalik Buterin, founder of Ethereum,

[12] See, for example, the differing definitions in Ethereum (2023) 'What is Web3 and why is it important?', CoinDesk (2022) 'What Is Web3: What's Driving the Web3 Buzz', Harvard Business Review (2022) 'What Is Web3? ', Forbes (2022) 'What Is Web3 All About? An Easy Explanation With Examples, DRCF (2022) 'Web 3.0 and distributed ledger technologies – A regulatory perspective'.
[13] Tim Berners-Lee (1989) 'The original proposal of the WWW, HTMLized'. For a complete history of the web, see World Wide Web Consortium (W3C) (2022) 'A Little History of the World Wide Web'.
[14] See for example, The New York Times (2006) 'Entrepreneurs See a Web Guided by Common Sense'. Tim Berners-Lee also used the term 'Web 3.0' in the same year in reference to the World Wide Web Consortium's (W3C) vision of a 'Semantic Web'. Although it is not the focus of this paper, see W3C's definition of the Semantic Web: W3C (2015) Semantic Web - W3C.
[15] Gavin Wood, published on CoinDesk (2022) 'What Is Web 3? Here's How Future Polkadot Founder Gavin Wood Explained It in 2014'.
[16] Web3 Foundation (2022) 'About'. Accessed 19 December 2022.
[17] Rossi and Sørensen (2022) 'The Meaning of De/Centralization: A Theoretical Review, Towards a Conceptual Framing', 14 May.

distinguishes between architectural, political and logical decentralisation.[18] The Web3 community aims to achieve the former two of these types of decentralisation, which are defined by Buterin as:

- Architectural (de)centralisation – how many physical computers is a system made up of? How many of those can it tolerate breaking down at any single time?
- Political (de)centralisation – how many individuals or organisations ultimately control the computers that the system is made up of?

When understanding how architectural decentralisation might apply to the web, we can consider the client-server model,[19] the most prevalent model of web architecture. In this model, users access web services by connecting their devices to centrally owned servers. For example, most social media services are currently hosted on servers owned and operated by social media companies. Users of social media connect their personal devices to these servers, enabling content and data to flow to and from the server and an app or browser (the client) on the personal device. Proponents of Web3 consider this model to be too centralised because the entity that owns the servers has complete control, within the confines of the law, over how the service is run and the data that are processed by it. This requires users to trust that the company providing the service will do so in the best interests of users. In this way, architectural centralisation can lead to political centralisation.

In contrast, an example of a decentralised architecture might be a peer-to-peer model in which there are no servers that host services centrally. Instead, users connect directly to each other, enabling the flow of data between them without an intermediary. Proponents of Web3 believe that by decentralising architecture using the peer-to-peer model, a political decentralisation of power and control can be achieved. However, the physical and geographical decentralisation of architecture alone may not cause decentralisation of power and control. For example, Amazon Web Services (AWS) offers many decentralised architectures (physically distributed computers capable of distributed computing) but politically it is centralised (AWS owns and controls these computers).

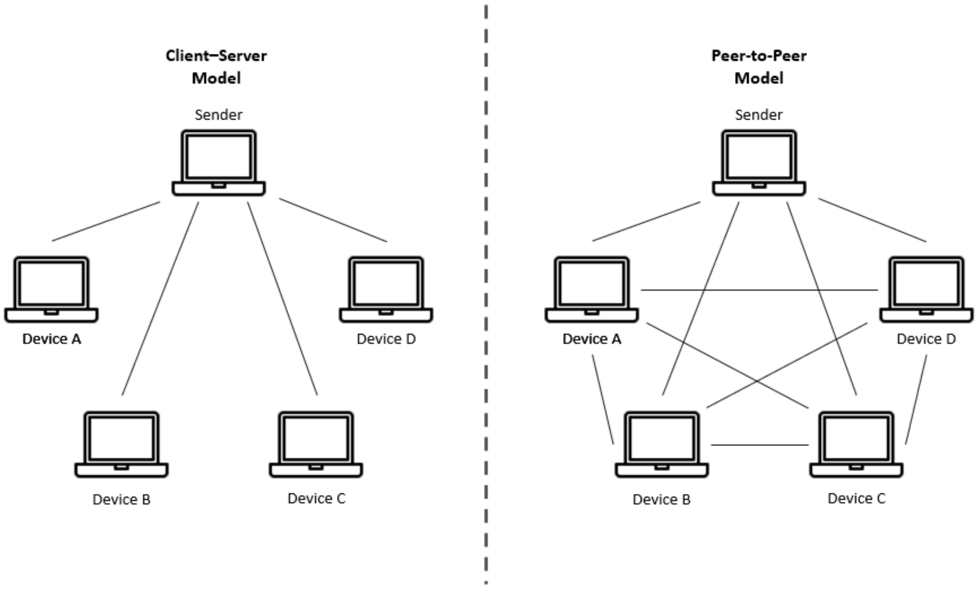

*Figure 1: An overview of the client-server model vs the peer-to-peer model[20]*

[18] Vitalik Buterin, published on Medium (2017), 'The Meaning of Decentralization', 6 February.
[19] For definition, see Britannica 'Client-Server Architecture'. Accessed 19 December 2022.
[20] Laptop icon by Icons8.

## Underlying technologies

Efforts to decentralise the web might be achieved through a range of different interventions and/or technologies, though one often proposed is distributed ledger technology (DLT) or, more specifically, public, permissionless and pseudonymous blockchains.

The National Cyber Security Centre (NCSC) defines a distributed ledger as an 'append-only data storage mechanism in which data is stored at multiple locations on a shared network'.[21] Instead of storing data on a centralised server, distributed ledgers use a peer-to-peer network of computers, or 'nodes' to record, validate and update data records. Blockchains are a form of DLT, well-known as the technology underlying cryptoassets, such as Bitcoin. A cryptoasset is a cryptographically secured digital representation of value or contractual rights that can be transferred, stored, or traded electronically.[22] Public, permissionless and pseudonymous blockchains are distributed ledgers for which all transactions are publicly visible; permission is not required for a node to join and interact with the network; and users make agreements between themselves using alphanumeric addresses rather than their identity.

Public, permissionless and pseudonymous blockchains are frequently viewed as a core technology for Web3 because they enable the members of a peer-to-peer network to make agreements between themselves without the intermediation of a central trusted authority. Instead, systems built on blockchains employ consensus-based validation mechanisms[23] to confirm peer-to-peer transactions and activity. There are two main types of consensus mechanisms: 'Proof of Work' and 'Proof of Stake'. Proof of Work is still widely used but it has attracted criticism for – amongst other issues – its high energy usage. As a consequence, there is increasing use of Proof of Stake mechanisms which are less energy intensive.

[21] National Cyber Security Centre (2021), 'Distributed ledger technology: The nature and applications of distributed ledger technology', 30 April.

[22] GOV.UK (2022) 'Factsheet: cryptoassets - key terms and definitions'. Accessed 19 December 2022.

[23] For more information about consensus mechanisms, see Ethereum (2022) 'Consensus mechanisms'.

| | | | |
|---|---|---|---|
| **Front-end interface** | 4 | **Application layer** | Front-end user interfaces built on top of the above layers that enable users to interact with smart contracts and assets through Web3 wallets, browsers and aggregators as well as Web 2.0 interfaces. |
| **Back-end infrastructure** | 3 | **Smart contract layer** | Programmes stored on a blockchain in the form of 'if/when…' statements. These programs automatically execute when predetermined conditions are met. |
| | 2 | **Asset layer** | Digital stores of value (i.e. cryptoassets) that participants and smart contracts create and transfer on a blockchain. |
| | 1 | **Settlement layer** | Blockchains and scaling solutions, for example, 'lightning' networks, sidechains and roll-ups, where all data on asset ownership and the history of transactions is recorded. |

*Figure 2: Conceptualisation of the Web3 Technology Stack*[24]

As shown in Figure 2, Web3 can be conceptualised as a technology stack built upon blockchains. The stack consists of a front-end interface, on top of three back-end infrastructure layers. Whilst blockchains were first proposed in 2008[25], the technology stack is still developing, particularly the Application Layer. Numerous web apps based on blockchain technology (Decentralised Apps, or DApps) exist such as marketplaces, online games and social networks,[26] but many can still be accessed via the current Web 2.0 client-server model. For example, users can access Web3 applications through many Web 2.0 browsers, including Firefox, Chrome and Safari, once their Web3 wallet is connected.[27]

[24] Conceptualised as according to International Organization of Securities Commissions (IOSCO) (2022) 'OR01/2022 IOSCO Decentralized Finance Report', p.3.

[25] Satoshi Nakamoto (2008) 'Bitcoin: A Peer-to-Peer Electronic Cash System', October 31.

[26] Dapp Radar (2023) 'Top Blockchain Dapps'. Accessed 9 January 2023.

[27] For more information on Web3 Wallets, see Wallets in Benefits, Risks and Harms.

# 3. Benefits, risks, and harms

This section firstly addresses benefits, risks and harms arising from decentralisation, before addressing specific topics with respect to back-end blockchain technology, including security issues, data privacy issues, and governance structures. It then addresses issues arising front-end blockchain technology issues, with respect to user experiences and choice, wallets, and illicit activities.

## Decentralisation

The redistribution of power from online platforms to users and, consequently, a reduction in the market concentration of Web 2.0 through the removal of trusted intermediaries is at the core of the Web3 vision.[28] Removing the need for trusted intermediaries to confirm transactions and other interactions between users could limit the ability of an intermediating entity to gain market power and/or to collect and control large amounts of user data. For the latter reason, it is believed that decentralisation would enable users to have greater user control over their data.

The removal of trusted intermediaries may, however, create risks. In a centralised system, when a user purchases a service, the intermediating 'service provider' can be regarded as the entity or individual(s) that has control over certain aspects of that service. Service providers are important for a range of reasons, including having responsibility for the quality of that service and being accountable to provide redress to a consumer or business if something goes wrong. Moreover, intermediaries may have incentives to provide a good quality service and protect consumers from harm as they may face reputational damage should any issues arise. In a decentralised system, by contrast, there may not be any entity or individual(s) in control of the service provided or they may be so numerous and/or geographically dispersed that seeking redress or compensation as a consumer might be impractical.[29]

Moreover, the claim that decentralisation of the web would reduce the market power of Web 2.0 incumbents is open to challenge. Architectural decentralisation does not necessarily entail political decentralisation.[30] Should one entity control a sufficient number of nodes within a blockchain network, that entity would retain control over the system or application run on that network. Relatedly, prominent Web3 companies have in recent years begun to partner with incumbent banks and Web 2.0 firms.[31] While such partnerships could help specific Web3 firms to leverage the legitimacy and brand of established firms to accelerate adoption and gain market share,[32] they could also ultimately reduce competition between Web3 firms to the detriment of consumer choice.

Most applications associated with Web3 are at very early stages of development. It is therefore currently too early to predict whether these will tend towards decentralisation or centralisation. In

[28] Benet, J. (2018), 'What Exactly is Web3', 22 October.
[29] UK Parliament (2022), 'Call for Evidence into the crypto-asset industry'. For the ICO's response, see ICO (2022), 'Response of the Information Commissioner's Office to the Treasury Select Committee inquiry into the crypto-asset industry'.
[30] For definition of 'architectural (de)centralisation' and 'political (de)centralisation', see Decentralisation in Definition and conceptual and technical overview.
[31] Bloomberg (2022), 'JPMorgan Executes Its First DeFi Trade Using Public Blockchain', 2 November and Polygon (2022), 'Meta to Let Users Mint and Sell Polygon-Powered NFTs on Instagram', 2 November.
[32] The Economic Times (2022), 'Polygon zoom 270% in the four months. What's fuelling the rally?', 7 November. See also Schrepel, T. (2023), 'The Complex Relationship between Web2 Giants and Web3 Projects', January 10.

either case, it is not yet possible to tell whether proponents of Web3 will achieve their stated aim of reducing the existing market concentration within Web 2.0. What we might expect is the development of both centralised and decentralised Web3 applications, which could offer users greater choice than centralised services alone (as illustrated by decentralised exchanges, see '**Use case: Decentralised exchanges'** below).

## Use Case 1: Decentralised Exchanges (DEXs)

Decentralised exchanges (DEXs) are peer-to-peer marketplaces where users can exchange cryptoassets without the need for an intermediary or custodian.[33]

Centralised crypto exchanges use methods similar to traditional stock exchanges, handling exchanges via an 'order book' that establishes the price for a particular cryptoasset based on current buy and sell orders. By contrast, decentralised exchanges are enabled by smart contracts, pricing cryptoassets against each other using algorithms. Users (called liquidity providers) deposit their digital assets into 'liquidity pools' in exchange for liquidity pool tokens; DEXs subsequently use these pools to facilitate trades. Centralised exchanges account for most of the trading volume in cryptoasset markets.[34]

There are three main types of decentralised exchanges: automated market makers, order book DEXs and DEX aggregators.[35]

- **Automated market makers:** use smart contracts and liquidity pools (pools of assets funded by users prior to the transaction) to execute trades.
- **Order book DEXs:** similar to centralised exchanges, these DEXs use order books to match buyers and sellers and determine the market price of assets.
- **DEX aggregators:** aggregate liquidity from several protocols to solve problems associated with liquidity and attempt to offer buyers the best price.

Uniswap has the greatest market capitalisation of any DEX and falls under the category of an automated market maker.

DEXs require specific knowledge and expertise, as traders can lose their funds if they lose their private keys or send funds to the wrong address. DEXs are also subject to unique risks in the form of smart contract error. On the other hand, DEXs could reduce counterparty risk as they operate via smart contracts that automatically execute a transaction when specific conditions are met.

DEXs also support a wide availability of tokens, including new projects not yet listed on centralised exchanges who need to ensure tokens comply with regulations before listing them. However, the lack of anti-money laundering (AML), know your customer (KYC) and due diligence checks for DEXs increases the likelihood of scams for such projects, such as 'rug pulls'.[36]

[33] Coinbase, 'What is a DEX'. Accessed 3 December 2022.
[34] DeNicola, L. (2022), 'What's the Difference Between Centralized and Decentralized Crypto Exchanges?', 11 June.
[35] Cointelegraph, 'What are decentralised exchanges, and how do DEXs work?'. Accessed 3 December 2022.
[36] Avan-Nomayo, O., (2020), 'Pulling the rug: DeFi investment hype fuels rise in crypto exit scams', 24 August.

## Back-end infrastructure

### Security

Blockchains offer 'inherent security qualities' for storing data.[37] Blockchains, are built on the principles of cryptography[38] and consensus[39] to ensure that transactions are secure and validated, as well as decentralisation, which removes the risk of a single point of failure and prevents a single user from changing the record of transactions.[40]

These inherent security benefits are, however, dependent on the quality of the blockchain's design and implementation. The National Cyber Security Centre (NCSC), for example, has noted that 'poor use of cryptography, or poor implementation, can compromise the security of a distributed ledger' (including blockchains).[41]

Moreover, blockchains remain susceptible to hacking. There have been, for example, instances where parties have gained more than 50% of a blockchain network's compute power (despite the associated costs), enabling those controlling parties to rewrite the blockchain and reverse transactions considered settled – also known as a '51% attack'.[42] Other forms of attack include routing attacks and Sybil attacks.[43]

Security risks can also exist in the smart contract[44] code stored on blockchains.[45] Hackers can, for example, exploit oversights in smart contracts to compromise the security of blockchain-based platforms. An attack on 'TheDAO' in 2016 saw US$50 million in assets drained from this newly-formed digital venture capital fund, illustrating how vulnerabilities can leave Web3 organisations susceptible to hacking and breaches.[46] The development of smart contract auditing services – which check for known vulnerabilities, security issues, bugs and errors within the smart contract code – is a direct attempt by the Web3 community to mitigate this risk.

DLTs, including blockchains, and associated security measures are still developing. Further research into their suitability as a data storage solution can be found in the NCSC's White Paper on Distributed Ledger Technology.[47]

[37] IBM, 'What is blockchain security'. Accessed 14 December.

[38] For an explanation of 'cryptography', see Glossary.

[39] For an explanation of the two main consensus-based validation mechanisms used for systems built of blockchain, 'Proof of Work' and 'Proof of Stake', see Glossary.

[40] IBM, 'What is blockchain security', Accessed 14 December.

[41] National Cyber Security Centre (2021), 'Distributed ledger technology: The nature and applications of distributed ledger technology', 30 April.

[42] See for example Voell, Z., 'Ethereum Classic Hit by Third 51% Attack in a Month', 30 August.

[43] For more information on routing attacks and Sybil attacks, see IBM, 'What is blockchain security'. Accessed 14 December.

[44] For an explanation of 'smart contract' and its relation to Web3, see Glossary. and Figure 2: Conceptualisation of the Web3 Technology Stack.

[45] KPMG (2017), 'Securing the chain'. See also Blockchain Council, (2022), 'Blockchain Bridges: Introduction and Functioning', 4 November.

[46] Bloomberg (2022), 'Attacker Behind Record 2016 Crypto Hack Might Have Been Found'. 22 February.

[47] National Cyber Security Centre (2021), 'Distributed ledger technology: The nature and applications of distributed ledger technology', 30 April.

## Data privacy

Blockchains are designed to be immutable; they consist of an append-only data storage mechanism which means that it can be nearly impossible to remove information held on a blockchain.[48] Information stored on a public, permissionless blockchain is publicly visible to any user that chooses to join and participate in that blockchain network.

These characteristics of a blockchain can improve transparency as all users within a given blockchain network can see all the same information at the same time.[49]

However, public visibility of all data to any user on a public, permissionless blockchain alongside blockchain's immutability raises particular concerns for data protection rights under the UK General Data Protection Regulation (GDPR), including the 'right to rectification'[50] (the right to have inaccurate personal data rectified and to have personal incomplete data completed) and the 'right to erasure'[51] (also known as the 'right to be forgotten').

Moreover, contrary to the stated goals of Web3, these characteristics of public, permissionless blockchains could reduce users' control over their data. One study has shown that an increasingly accurate picture of a user can be created as more transactions are added to a blockchain, including personal data such as names or demographic information.[52] Another has suggested that malicious actors could also use blockchain immutability to make illicit or non-consensual material (including doxing[53] and revenge porn[54]) permanently publicly accessible.[55]

These privacy risks can in some instances be mitigated using, for example, Zero Knowledge Proofs.[56] Such mitigations, however, may reduce transparency, which can undermine trust in the decentralised network or conceal illegal activity.

## Governance structures

Systems built on blockchains use consensus-based validation mechanisms, including Proof of Work[57] and Proof of Stake,[58] which are an innovative approach to validating transactions and other user interactions in the absence of a trusted intermediary.

Blockchain systems using Proof of Stake consensus mechanisms allow those users with the greatest stake in the system to act as 'validators' and confirm transactions and other interactions.

[48] Gabison, G. (2016), 'Policy Considerations for the Blockchain Technology Public and Private Applications'. Science and Technology Law Review, 19(3), pp, 330-331.

[49] IBM, 'Benefits of blockchain'. Accessed 14 December 2022.

[50] Article 16 UK GDPR. For more information, see ICO 'Right to rectification'.

[51] Article 17 UK GDPR. For more information, see ICO 'Right to erasure'.

[52] Winter, P., Lorimer, A., Snyder, P., Livshits, B. (2021), 'What's in your Wallet: Privacy and Security Issues in Web 3.0', 14 September.

[53] The malicious publication private or identifying information about a particular individual.

[54] The publication of explicit images or videos of a person without the consent of the subject.

[55] Gabison, G. (2016), 'Policy Considerations for the Blockchain Technology Public and Private Applications'. Science and Technology Law Review, 19(3), pp. 333-335.

[56] Zero knowledge proofs are a method by which one party can prove to another party that a statement is true (for example a transaction has occurred) without revealing any additional information about the statement itself. See for example Royal Society (2019), 'Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis'.

[57] For an explanation of Proof of Work, see Glossary.

[58] For an explanation of Proof of Stake, see Glossary.

This approach naturally leads to concentration[59] and disproportionate control[60] by those with the greatest stake in the system. Similarly, blockchain systems using Proof of Work consensus mechanisms require 'validators’ to solve mathematical equations to confirm transactions. As the blockchain system grows, the computational power needed to solve these equations increases. Consequently, users that have greater computational power with which to solve equations and thereby confirm transactions and other interactions will have greater influence over the system.

Such findings suggest that, whilst the underlying technology may be decentralised, systems built on blockchains can tend towards centralisation due to the control over that system by a small number of users. Any form of centralisation could lead to the market power issues that exist in conventional markets. These ideas for Web3 do not therefore remove the risk of anti-competitive or misleading practices.[61]

[59] Aramonte, S., Huang, W., Schrimpf, A. (2021), ‘DeFi risks and the decentralisation illusion’, 6 December, p.28.

[60] Bains, P., Ismail, A., Melo, F., Sugimoto, N. (2022), ‘Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets’, 26 September, p.19.

[61] See, for example, Bodó, Brekke and Hoepman (2021),’Decentralisation: a multidisciplinary perspective’, Concepts of the digital society, Vol.10 No. 2, who argue that ‘in practice, decentralisation might very well be served by and produce centralising effects’ and note that ‘without governance mechanisms, nodes may collude, people may lie to each other, markets can be rigged, and there can be significant cost to people entering and exiting markets’.

## Use Case 2: Decentralised Autonomous Organisations

A Decentralised Autonomous Organisation (DAO) is a self-governing digital community that is created to coordinate activities, make decisions and/or deploy resources towards a shared objective.[62] These organisations often rely on blockchains, smart contracts or other open-source software systems to function. The majority of DAOs are related to decentralised finance (DeFi), accounting for 83% of all DAO treasury value held.[63]

DAOs represent a democratised management structure that enables interested parties to work towards a shared goal or project, governed by its protocol. Typically, the founders of a DAO issue a token that offers governance rights to users and stakeholders of the project. Holders of these tokens become a decentralised governance body to vote on the direction of or changes to a protocol.[64]

DAOs offer the opportunity for globally dispersed members to work together towards a shared goal and raise funds in a short space of time. They may also offer more transparency (for example in decision-making processes) for members than centralised governance structures.

However, a key risk for members engaging with DAOs is the continued uncertainty regarding their legal status. DAOs may have characteristics that differentiate them from existing legal structures. This can in some cases lead to ambiguity in respect of which legal and regulatory requirements apply to them. The Law Commission has recently launched a Call for Evidence to assess the legal status of DAOs, stating that 'The legal treatment of any particular organisation which is described as a DAO will instead depend on how its particular organisational arrangements are structured'.[65] The CFTC's lawsuit against the Ooki DAO evidences that these entities are not beyond the bounds of legal enforcement in some jurisdictions.[66] Individuals participating in DAOs may not, however, be aware of the legal and regulatory requirements (and risks) of their involvement in these organisations.

[62] World Economic Forum (2022), 'Decentralized Autonomous Organizations: Beyond the Hype', No date.
[63] Chainalysis (2022), 'Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated', 27 June.
[64] Chainalysis (2022), 'Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated', 27 June.
[65] Law Commission (2022), 'Decentralised Autonomous Organisations (DAOs)', 16 November.
[66] CFTC (2022), 'CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Chargers Successor Ooki DAO for Offering Illegal, Off-Exchange Digital-Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act', 22 September.

## Front-end interface

### User experience and choice

A variety of blockchain-based applications have emerged in services as diverse as social media, gaming, data management, search engines, derivatives and more.[67] Some of these applications offer users the benefit of earning and/or owning digital assets as they use the service.

For example, the integration of non-fungible tokens (NFTs)[68] into gaming platforms can offer players the chance to own in-game digital assets. This has also given rise to new ’play-to-earn’ gaming models in contrast with traditional ‘play-to-win’ models. In play-to-earn, users are rewarded with cryptoassets or ‘tokens’ (or can collect NFTs to sell on secondary markets) which they can earn as they play.[69] The crash of NFT trading volumes and market value in 2022[70] and the Axie Infinity hack[71] in the same year has undermined confidence in NFTs, as well as ’play to earn’ gaming models.

This trend can particularly impact low-income players, who may rely on these games as a source of income. The recruitment of new players initially creates demand for cryptoassets within the game, increasing their value. When players begin to redeem their earnings, the value of the cryptoassets can start to drop at the risk of leaving low-income players indebted to those who provided them the funds for the initial investment.[72]

Another example is Brave browser’s use of cryptoassets to encourage users to opt-in to its advertisement service. Users can earn cryptoassets when they choose to view advertisements.

Such applications might have the potential to offer new user experiences and greater consumer choice when accessing and using services if the associated risks can be appropriately managed.

[67] For more examples of Web3 applications and use cases, see Dempsey, C., Wang, A., Mart, J. (2022), ‘A simple guide to the Web3 stack’, 13 January.

[68] For an explanation of non-fungible tokens, see Glossary.

[69] See for example Axie Infinity, where users earn ’AXS’ tokens by playing and can use these tokens to claim rewards, play the game or participate in governance voting on the future of the game.

[70] Brooks, K. (2022), ‘NFT prices slump as FTX‘s collapse shadows digital collectibles‘, 18 November. See also Linares, M. (2022), ‘Bill Gates Slams NFTs And Crypto Amidst Market Plunge’, 15 June.

[71] De, N., Nelson, D. (2022), ‘US Government Recovers $30M From Crypto Game Axie Infinity Hack’, 8 September.

[72] Freedom Lab (2022), ‘From labor to exploitation: the dark side of blockchain games’, June 30

## Use Case 3: Decentralised Digital Identity

A digital identity (whether decentralised or centralised) that could be used across different services could bring benefits to users. In the current Web 2.0 model, emails and social media accounts offer a form of digital identity. Most existing solutions are however centralised, with the service provider controlling the identity data provided and users often 'paying' for the service provided through targeted advertising. Furthermore, a user often needs to register a separate username and password for every service they use. This fragmented and siloed approach to identity management might inhibit the digital user experience, as users do not have a control of their online identity and are often unaware where their identity information is stored and how it is used. In addition, large platforms seek consolidated central control over user identities by offering 'sign in with …' account registration options and digital wallet applications on smartphones.

These challenges, coupled with developments in DLT, have led to increasing interest in decentralised identities. Instead of storing their identities in service provider accounts, users store their credentials and identity information in 'wallets' which only they can access (e.g., on their own device).[73] These wallets offer users security and privacy by using cryptographic public and private keys, to encrypt and decrypt digital credentials, known as 'verifiable credentials' or 'VCs'. A public key encrypts information, which can only be decrypted using the corresponding private key. Instead of placing trust over identity information in online services, the decentralized identity model relies on signatures using the public and private keys. The public keys that can decrypt signatures on the credentials are stored on the DLT, meaning that relying parties (that need to verify user identity) can access them to decrypt the signature and credential when they are presented, therefore enabling trust in their validity.

Decentralised identity solutions could reduce security risks for users, as their digital identities are no longer stored on centralised databases susceptible to data breaches. These solutions could also offer users more privacy than their Web 2.0 alternatives as organisations would require individuals' permission to access personal data and individuals have greater control over the information they share.

However, there are other concerns around security, given that the digital identity is held on the user's device, moving the data honeypot away from service providers to end user devices that may be targeted by attackers. Further, losing a digital identity maliciously or by accident may have potentially significant consequences, including losing access to services as well as increased risk of fraud.

Alongside technology development, there is also a wider drive to bring more trusted online identities to fruition across the economy. The Data Protection and Digital Information Bill[74] will enable the use of trusted digital identities, provided by certified digital identity providers, through the UK Government Digital Identity and Attributes Trust Framework. Providers and platforms

[73] Maynes, M. (2022), 'Why decentralization is the future of digital identities', 10 March.
[74] UK Parliament (2022), 'Data Protection and Digital Information Bill', 5 September.

adopting a centralised approach will benefit by having access to more trusted identity information, further impacting user security and privacy. The government has published a list of certified digital identity service providers, which includes centralised digital identity providers as well as a decentralised one, Nuggets.[75]

The Online Safety Bill will require providers of user-to-user and search services to have systems and processes in place for protecting individuals from certain types of harm online. The largest and most high risk user-to-user services will also have to offer their users optional tools to verify their identity. In connection with its new functions as online safety regulator, Ofcom expects to consider ways in which use of digital ID to verify age and/or identity might potentially be used to help protect users of online services.

## Wallets

Users access applications associated with Web3 through wallets, which use public and private keys[76] to connect with a particular blockchain network and to transfer cryptoassets. Users can opt for non-custodial wallets, which offer them control over the private key, or custodial wallets, where this responsibility is outsourced to a third party.

Non-custodial wallets remove the possibility of interference by intermediaries as users do not require a third party to access their funds and/or intermediate their transactions. In theory, this setup gives users more control over their assets by, for example, allowing users to make instant withdrawals without requiring third party permission.[77]

Users interacting with blockchain networks via non-custodial wallets are, however, solely responsible for their access information and will need to educate themselves on the different risks associated with non-custodial and custodial wallets, as well as other approaches.[78] If users lose their private key, it can be difficult to retrieve assets. According to estimates from Chainalysis, around 25% of bitcoins are believed to be permanently lost in this manner.[79]

The need for users to self-protect raises further concerns in a system where illicit activity, such as theft, currently comes with limited means of recourse.[80] Phishing attacks, where criminals trick victims into giving up their private keys or personal data, are a common cryptoasset scam and are becoming increasingly sophisticated. Criminals can subsequently use the private key to access and steal cryptoassets held in the wallet. Victims of these scams will struggle to get their money back, with some lawyers estimating that cases where the loss is less than £1m are usually not economically viable due to the cost of legal action.[81] The complexity of the technology, the range of

[75] DCMS (2023), 'Digital identity certification for right to work, right to rent and criminal record checks', 13 January.

[76] A public key is works like an email address, which can be shared safely with others. A private key is a string of letters and numbers which acts like a password: it holds the key to accessing funds and should not be shared with anyone. See Coinbase, 'What is a private key'. Accessed 6 January 2023.

[77] Banerjee, A. (2022), 'Custodial Vs. Non-Custodial Wallets: Difference Disclosed', 15 March.

[78] See, for example, Perper, R. (2022), 'Hot vs. Cold Crypto Storage: What Are the Differences?', 4 August.

[79] Chainalysis (2018), 'Bitcoin's $40 billion sell-off', 8 June.

[80] See This section firstly addresses benefits, risks and harms arising from decentralisation, before addressing specific topics with respect to back-end blockchain technology, including security issues, data privacy issues, and governance structures. It then addresses issues arising front-end blockchain technology issues, with respect to user experiences and choice, wallets, and illicit activities.
Decentralisation in 3 Benefits, risks and harms.

[81] Oliver, J. (2022), 'The lawless world of crypto scams'. 19 September.

sophisticated scams and the limited means of recourse together create substantial risk for even the most educated consumers in this space.

### Illicit activities

Current applications associated with Web3 offer users pseudonymity. Users are represented on a blockchain by alphanumeric addresses associated with their wallet rather than their actual identity.[82]

Pseudonymity can bring benefits in some contexts, including the preservation of privacy and greater personal security.[83] However, the pseudonymous nature of transactions and ownership of digital assets means that action against unlawful activities can be limited to very blunt enforcement mechanisms, such as the sanctioning of entire services or possibly the takedown of entire networks.[84]

Systems that operate outside of established legal and regulatory controls can open the door to illicit activities including scams, ransomware[85], theft and identity fraud.[86] The 'Squid coin' scam, where unknown creators drained $3.3 million in funds from the product and effectively drove the token's value to zero, is one example of a scam in this space.[87]

[82] European Parliament (2018), 'Virtual currencies and terrorist financing: assessing the risks and evaluating responses'. No date.

[83] Hertig, A. (2020), 'Many Bitcoin Developers Are Choosing to Use Pseudonyms – For Good Reason'. June 29.

[84] See for example OFAC (2022) 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash'. 8 August.

[85] The NCSC considers ransomware to be the biggest online threat to the UK. NCSC (2022), 'Solicitors urged to help stem the rising tide of ransomware payments'. 8 July.

[86] See for example a North Korean hacking syndicate's theft of approximately $62 million of cyptoassets from the 'player-owned' game Axie Infinity, FT (2022), 'How North Korea became a mastermind of crypto cyber crime'. 14 November. See also CNBC (2022), 'U.S. officials link Norther Korean hackers to $615 million cryptocurrency heist'. 15 April.

[87] Cheng, A. (2021), ''Squid Game'-inspired cryptocurrency that soared by 23 million percent now worthless after apparent scam'. 2 November.

# 4. Regulatory considerations

The potential benefits from ideas associated with Web3, as well as existing and anticipated consumer harms and wider societal risks, raise some key questions for DRCF member regulators:

1. What is our role in relation to innovative technologies, including those which underpin visions for Web3? (See 'The role of the regulator' below)
2. To what extent do our current regulatory frameworks apply to entities operating products and services associated with Web3? (See 'Current regulation' below)
3. What regulatory challenges might arise from applications associated with Web3 that we need to consider? (See 'The challenge of enforcement: Governance' and 'The challenge of enforcement: Technology' below)

## The role of the regulator

The DRCF member regulators typically adopt a position of technology neutrality. This means regulation of the services and applications built on technologies (and the entities offering those services), rather than the technologies themselves.

The DRCF member regulators seek to foster responsible innovation, giving technologies space to develop and mature while helping ensure that associated risks and harms are minimised. Each member regulator also has a role in encouraging innovation as well as an objective to protect and/or further the interests of consumers within their respective remits.[88] Linked to this, they aim to:

- Promote effective competition in the UK economy (CMA, Ofcom and FCA)
- Protect the integrity of the UK financial markets (FCA)
- Uphold the information rights for the UK public (ICO)

Applications associated with Web3 are largely novel and have not yet been widely adopted. In this context, our approach is to explore and understand developing use cases to ensure we are well placed to consider how existing and prospective regulatory frameworks may be applied to ensure consumers are adequately protected, whilst allowing them to benefit from novel products and services. This approach also helps to identify and mitigate risks to competition, financial market integrity and information rights before they have a significant impact.

We seek to work constructively with industry within our respective remits to help ensure we encourage responsible innovation whilst minimising harms to people and businesses. Since 2014, 34% of firms accepted into the FCA's Regulatory Sandbox – which allows firms to test innovative propositions in the market with real consumers – used DLT, with most of them operating in the area of crypto and decentralised finance (DeFi). The ICO's Regulatory Sandbox also supports organisations to create products and services that utilise personal data in innovative and safe ways.

[88] See Ofcom, 'What is Ofcom'; ICO, 'Purpose, objectives, values and behaviours'; CMA 'About us'; and FCA, About the FCA.

## Current regulation

Existing regulations may apply to decentralised entities, including those operating outside of the UK. This list outlines several examples of such regulations across all DRCF member regulator remits. They are intended as examples and do not represent the full list of legal provisions that are potentially relevant to decentralised entities. For example:[89]

1. UK General Data Protection Regulation (GDPR),[90] which will apply to a controller or processor (including when *not* established in the UK) where they are processing the data of UK natural persons and offering goods and services to data subjects in the UK.[91]

2. The Competition Act,[92] the Enterprise Act[93] and consumer legislation including the Consumer Rights Act[94] and the Consumer Protection from Unfair Trading Regulations[95] apply where activities affect trade and/or markets in the UK. The Competition Act, for example, prohibits the abuse of a dominant position by one or more undertakings having a dominant position in a particular market, insofar as it may affect trade within the UK.

3. Proposed rules regulating financial promotions.[96] In January 2022, the Treasury confirmed its intention to bring qualifying cryptoasset financial promotions within the FCA's remit. In their consultation response published in January 2022, the Treasury outlined that DeFi applications may be in scope of the new regime depending 'on the activities being carried out and promoted'.[97]

In addition, the Online Safety Bill[98] will require services which host user-generated content and search engines to have systems and processes in place for protecting individuals from certain types of harm online. This requirement will apply to any services with a significant number of UK users, or which is targeted at the UK market, regardless of where it is located geographically.

## The challenge of enforcement: Governance

Whilst these existing and forthcoming regulations may apply to decentralised entities, governance of those decentralised entities could raise practical questions for regulators.

As explained in Use case: Decentralised Autonomous Organisation (DAOs), DAOs represent a management structure with dispersed decision-making and no central authority, which may make it difficult to assign responsibility for actions taken by the DAO as a whole.

[89] This list outlines several examples of such regulations across all DRCF member regulator remits. They are intended as examples and do not represent the full list of legal provisions that are potentially relevant to decentralised entities.

[90] UK General Data Protection Regulation Available,

[91] See ICO, 'Guide to the UK General Data Protection Regulation (UK GDPR)',

[92] Competition Act 1998.

[93] Enterprise Act 2002.

[94] Consumer Rights Act 2015.

[95] The Consumer Protection from Unfair Trading Regulations 2008.

[96] HM Treasury (2022) 'Government to strengthen rules on misleading cryptocurrency adverts', 18 January.

[97] HM Treasury (2022) 'Cryptoasset promotions: Consultation response', January. The consultation set out a proposed definition for qualifying cryptoassets to be brought into the scope of the Financial Promotion Order as a controlled investment.

[98] Department for Digital, Culture, Media & Sport (2023), 'Online Safety Bill: Factsheet', 18 January. All platforms in scope will need to tackle and remove illegal material online, particularly material relating to terrorism and child sexual exploitation and abuse.

This challenge can be illustrated, for example, by compliance with obligations and potential enforcement under the GDPR. Token holders within a DAO vote on changes they perceive as being in the best interests of the whole organisation. Any token holders voting on DAO policy about processing personal information could play a role in determining the means and purposes of processing that information. Under UK data protection law, the entity responsible for determining the purposes and means of processing personal information is a 'controller'.[99] A controller processing personal data has obligations under UK GDPR. These include transparency, lawfulness, access, security and maintaining privacy standards. With no real limit on the number of token holders voting in a DAO, this could in effect create a large set of "joint controllers" who would each have obligations under UK data protection law.

The governance model used by DAOs might mean:

- Users of the service may struggle to identify how, or with whom to raise concerns or exercise their rights.
- The DAO may find it difficult to ensure that all voting token holders understand their regulatory obligations.
- Regulators may encounter challenges in engaging with or enforcing against non-compliant entities who may number in the thousands.

Similarly, where a DAO is relying on third party services, such as an underlying public blockchain, the operators and/or nodes of that blockchain may meet the definition of a 'processor'[100] under UK GDPR. A processor has its own set of obligations under the law and the challenges detailed above may arise.

## The challenge of enforcement: Technology

The use of DLT as the underlying technology of a future decentralised web may also create challenges for regulation due to the immutability of public blockchains as well as the potential for automated transactions and decision-making through smart contracts. Immutability, whilst offering benefits in terms of validation of transactions, stores data in a way which cannot be changed, deleted or overwritten, without affecting that validation process. This remains the case even where necessary to ensure regulatory compliance. Further, while automation via smart contracts can bring efficiency advantages, it can also raise questions of accountability if actions prompted by automated transactions or decisions cause harm and/or fail to comply with applicable regulation.

Automation could also create challenges where, for example, a smart contract performs in a manner that results in activity causing harm or otherwise fails to comply with regulatory obligations. In this scenario, it may be unclear who is accountable for that activity. Does responsibility lie with the developer who wrote the smart contract code, or with the broader community governing the application, or with the party tasked with establishing sufficient smart contract auditing processes?

Immutability can pose specific challenges when addressing harms arising from fraud and scams as well as from online content. The difficulty in reversing transactions is a consideration for financial

[99] The UK GDPR defines a controller as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'. See ICO, 'What are 'controllers' and 'processors''?

[100] The UK GDPR defines a processor as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'. See ICO, 'What are 'controllers' and 'processors''?

regulators and authorities seeking to enforce against sophisticated scams and fraud. For applications (including social media) built on public blockchains that seek by design to facilitate the publication of materials without limitation or censorship, illegal content (such as child sexual exploitation and abuse (CSEA) materials) as well as instances of 'revenge porn'[101] and 'doxing'[102] could become permanent.

## 5. Summary and next steps

The internet has transformed how we live and work, and its ongoing evolution will shape our lives in profound ways. Understanding the paths that it might take is therefore of significant importance. This paper sets out a regulatory perspective on one such socio-technical vision for the web (Web3), and its underlying concept (decentralisation) and technology (DLT), with a discussion of a range of its use cases with relevance to our regulatory remits. Given the breadth and ongoing evolution of these topics, the paper has provided a summary view, and has maintained a 'technology neutral' stance, whilst critically assessing any claimed benefits, risks and harms.

It is currently unclear whether and in what form Web3 might evolve. As a consequence, a number of the discussion areas within this paper are subject to a high degree of uncertainty. It is also unknown to what degree interest in 'decentralisation' in the context of the web might achieve broader appeal. The emergence of DLTs has to date given users new ways to exchange value online, such as the use of cryptoassets within online communities as a way to share digital goods between themselves. However, their use is also associated with consumer harm, such as financial loss, and facilitating some forms of online crime, such as ransomware attacks. Exploration of a wide range of use cases based on DLTs continues, some of which might mature into scalable solutions, whereas others might reveal DLTs do not offer compelling utility over other technologies. Currently at least, we are yet to see scaled DLT solutions emerge that have wide appeal with applications based on DLTs seeing arguably low levels of adoption to date. Similarly, some of the emerging markets surrounding key Web3 components, cryptocurrencies and NFTs continue to be subject to high levels of volatility.

The DRCF regulators will continue to monitor developments related to Web3, and work collaboratively to ensure we are pooling our knowledge and perspectives, as we seek to foster responsible innovation, while helping ensure that associated risks and harms are minimised.

Looking forward, the DRCF's emerging digital markets and technology horizon scanning programme, Joining up on future technologies, will continue to build knowledge on emerging technologies and trends in digital markets through engagement with industry, academia, regulators, and other stakeholders. We will share collective, public insights on the cross-regulatory implications of emerging technologies and trends in digital markets.

We welcome views from interested parties on the topics discussed in this paper as well as on the DRCF's 'Joining up on future technologies' work programme. To do this, please contact us at JoiningUpOnFutureTech@ofcom.org.uk.

[101] The publication of explicit images or videos of a person without the consent of the subject.
[102] The malicious publication private or identifying information about a particular individual.

# 6. Glossary

This glossary should not be considered to be an indication of regulatory definitions. The definitions and explanations contained herein are only to clarify references to the associated concepts in the Insight Paper.

**Web 2.0**
The current architecture of the web. Web 2.0 is characterised by dynamic hosted services (including traditional websites and social media) which users can interact with and create content on.

**Client-server model**
The model upon which Web 2.0 is based. Services and data are hosted by third party server infrastructure and users connect to these servers to engage and interact. Control of those services ultimately resides with those organisations hosting them.

**Peer-to-peer model**
In peer-to-peer architectures, the centralised servers are removed, and users transact directly with each other. Either party is able to initiate the connection and can act effectively as both client and server.

**Distributed ledger technology (DLT)**
DLTs use multiple interconnected database instances to process transactions. These databases might be in different physical locations, but are linked across a network, appearing to be a single database.

**Blockchain**
The most popular and widely known application of distributed ledger technology (DLT). Each transaction processed in a blockchain carries a cryptographic hash of the block before it, seeking to provide a permanent, secure, unalterable chain of data which can be verified.

**Proof of work**
This method of achieving a consensus of verified transactions in a blockchain relies on users solving cryptographic problems to arrive at a certain result. Once verified, the transaction is written to the chain. Since it requires intensive processing power from multiple users, proof of work is criticised for its energy usage and impact on the environment.

**Proof of stake**
A proof of stake consensus mechanism puts the responsibility for verifying transactions upon those users which have the most asset value stored on (and therefore the most interest in the security and validity of) the blockchain. Whilst this is a far less energy intensive way of achieving consensus than Proof of Work, it does create a power imbalance based on wealth.

| | |
|---|---|
| **Cryptography** | The process of securely writing, transmitting and reading enciphered text in such a way that adversaries are unable to decrypt and read it. |
| **Cryptoassets** | Cryptoassets are cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically. |
| **Non-fungible token (NFT)** | A unique digital identifier that cannot be substituted, changed or erased and is typically used to assert ownership of a virtual asset or status on a blockchain. |
| **Decentralised Finance (DeFi)** | Decentralised finance (DeFi) refers to financial systems that remove centralised intermediaries from transactions and financial products and services. It enables continuous and independent access to financial services such as lending, borrowing and trading, without processing via banks, traditional exchanges or hosting providers. |
| **Decentralised apps (dApps)** | dApps are applications running on a peer-to-peer distributed blockchain infrastructure. |
| **Decentralised autonomous organisations (DAOs)** | DAOs are organisations that decentralise decision making, replacing traditional centralised decision making with token-holding users voting on proposed changes. DAOs use decentralised ledger technologies (DLTs) to encode the decisions and rules of the DAO into smart contracts. |
| **Smart contracts** | Smart contracts are self-executing programs on the blockchain which trigger when certain conditions are met (for example, automatically providing payment when goods are sent), and are used to control and document actions resulting from those conditions. |
| **Personal data** | Personal data means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. |
| **Pseudonymous data** | Data that cannot be attributed to a specific individual without the use of additional information. |