webscience TRUST

Web3: The Promise & the Reality

WST/WSI White Paper #23-01

Ben Hawes

Web3: The Promise & the Reality

WST/WSI White Paper #23-01

Ben Hawes

About the Authors

The lead author of this brief is Dr Ben Hawes, technology policy consultant and Associate Director at the Connected Places Catapult.

Also contributing to this piece were:

- Professor Dame Wendy Hall, Regius Professor of Computer Science, at the University of Southampton
- Bill Thompson, Head of Public Value Research in BBC Research & Development and member of the main advisory board of the Web Science Institute
- Dr Kieron O'Hara, Emeritus Fellow in Electronics and Computer Science at the University of Southampton.

About WST

The Web Science Trust (WST) is a charity promoting the understanding of the Web, through education and research in the discipline of Web Science. It co-ordinates the Web Science Trust Network (WSTNet) of leading Web Science laboratories from around the world.

The Trust engages in both academic and public outreach through the ACM Web Science Conference, the journal of Web Science and sponsored White Papers.

http://webscience.org *info@webscience.org*

About WSI

The Web Science Institute (WSI) draws together the University of Southampton's world-class, interdisciplinary, sociotechnical expertise in Web Science, Data Science and Artificial Intelligence.

The WSI acts as a focus for international esteem as it creates new opportunities to bring disciplines together to leverage the unique role of online technologies in tackling global challenges, including the challenges posed by society's use of those technologies themselves.

The WSI was established to study the evolution of the Web and society, but has evolved into an institute that specialises in the sociotechnical study of the evolution of digital technologies and society in general, focussing currently on, but not restricted to, the new discipline of Human-Centred Artificial Intelligence (HCAI) as well as Web Science.

https://www.southampton.ac.uk/research/institutes-centres/web-science-institute

Preface

Web3 describes a group of technologies for managing collective interactions on the internet while avoiding centralised control, granting users agency over access to their data, and managing distribution of value as digital assets. The technologies are distributed ledgers including blockchain, cryptocurrencies, distributed autonomous organisations, decentralised finance, and non-fungible tokens.

Web3 technologies offer technical solutions to problems of trust and verifiability online. Their open source basis makes them available to developers globally and across sectors and communities. Some of these technologies are already in use across many sectors and have been proposed as applicable to a much greater range of uses in the future. If the technologies prove successful sustainably at scale for a very wide range of functions, they might change and expand what the internet delivers for a high proportion of users, and genuinely warrant the description Web3.

However, in spite of evident ongoing innovation and investment in these technologies, there are serious questions about whether they are scalable enough to deliver such a broad step-change, whether the value of many applications outweigh the costs and risks, and whether the same functions might be delivered more effectively by alternative tools. There are even fundamental questions about whether they really have the characteristics which their enthusiasts celebrate the technologies for. In effect, these questions and criticisms dispute the validity of the term Web3.

This paper provides a current overview of the functions of Web3 technologies, the major application areas and the kinds of challenge the technologies are intended to resolve. It considers how these approaches are presented in relation to previous waves of the development of the internet. It also contains definitions of terms used by the industry.
Views expressed about Web3 can be highly polarised, which is intriguing. Commentary about developments in computer software does not usually include the kind of extreme judgements, positive and negative, that characterise discussion of Web3. This paper explores the great divergence in perspectives. It summarises challenges and criticisms, notes significant recent developments, and suggests themes likely to be critical to the future of Web3.

Key words: Web3 cryptocurrency blockchain distributed ledger decentralisation

Introduction

This paper summarises the objectives, functions, histories and shortcomings of technologies collectively known as Web3.

At the time of writing in 2023, many of those shortcomings are more widely known than ever, following the successive and linked collapses of cryptocurrencies and companies working in cryptocurrency. However, the failures are more interesting because of the hope (as well as the money) invested in Web3. Therefore this paper analyses the appeal of Web3 in principle, as a product of a time in the development of internet technologies and applications, before going on to examine its limitations in practice. Web3 has not only not (yet) delivered a step-change in how the internet is used, it has also in many cases not in practice delivered the functions that were supposed to be characteristic of it. This matters because there continues to be huge demand for more trusted and trustworthy ways of managing interactions online.

Web 3 does not have a single specific widely accepted definition, but at this time in 2023 it is generally used to describe a group of related internet technologies for distributed management of collective activities. These technologies include distributed ledgers, cryptocurrencies, distributed autonomous organisations (DAOs), distributed finance, and non-fungible tokens (NFTs).

This paper will use the term Web3 to describe those technologies as a group. Web3 tools manage interaction, agreement and shared records, providing technical solutions to common challenges that recur in the development of collective endeavours, in particular in relation to hierarchy, assurance, transparency, and enforcement of agreed obligations.

A key principle of Web3 is trustlessness: structuring the basis for interactions between participants so that they do not need to trust each other or know each other's identity, or look to a controlling and regulating authority for assurance of trust, because the structure of the system are intended to make it impossible for users to abuse it, control it or extract value from it, or at the least, impossible to do those things without detection by the rest of the community.

As will be considered below, this is not to say that many Web3 applications have fully achieved trustlessness, or that it is possible or even desirable to manage communal interactions without the possibility for intervention or correction. However, understanding the aspiration and offer of trustlessness is essential to understanding Web3's appeal. The appeal is certainly in part emotional, which goes some way to explaining the cultish enthusiasm around the technologies. This paper will explore what is offered by Web3, before going on to examine how much that offer has been fulfilled.

A trustless system could offer equal terms to all users, and so avoid hierarchies and power imbalances between users, and between users and a platform owner or manager. In particular, Web3 technologies are often presented as avoiding imbalances of power by granting users more control over access to and use of their data. This is intended to correct the failings of the prevailing model in online platform services where one user gives their personal data to multiple services in order to obtain and use an account with each, and each platform accumulates the data from millions of users and gains capabilities from use of that accumulated data. Web3 offers the potential to hold and control personal data and control the services' access to it, with the option of revoking the data.

There is a strong participatory aspect to Web3 applications. The technology tools offer participation and competition in creating immutable decentralised records that support trustlessness in the system. They can also offer participation in decisions about the functioning of a system. Web3 creates digital assets, that function as assets because members of the specific community participate in the creation, assurance and trading of them.
Trustless Web3 systems are devised to be controlled by the rules of the system. They do not rely on institutions or the exercise of powers in the offline world and may in some cases expressly seek to evade exercise of law and regulation by governments, to assure protection of the rights and interests of users. For some users, this aligns with suspicion of government authorities or fear of prosecution or persecution, but using Web3 does not imply any particular political alignment. The structure offers a shared record immune to change by external forces and actors, which can appeal to very many different potential users.

There is evidently enormous appetite for tools that offer solutions to problems of trust that will work for many different kinds of groups. This offer of general purpose solutions encourage some enthusiasts to maximalist aspirations and predictions.
This is a representative example, in a 2019 article, by Max Mersch and Richard Muirhead.

> *These interactions, ranging from seamless payments to richer information flows, to trusted data transfers, will become possible with a vastly increased range of potential counterparties. Web 3.0 will enable us to interact with any individual or machine in the world, without having to pass through fee- charging middlemen. This shift will enable a whole new wave of previously unimaginable businesses and business models: from global co-operatives to decentralised autonomous organisations and self-sovereign data marketplaces.*[1]

For enthusiasts, Web3 technologies could drive a major new phase in what the internet can do, ultimately for billions of users. Giving these technologies the name Web3 encapsulates that belief and with it the aspiration to fulfil that promise.

This is also why critics object to the term. Whether these technologies do herald, launch or constitute that kind of step change is highly contested, and sceptics see the use of the term Web3 as unjustified hype.

Critics point to very many instances where claims for Web3 have fallen short. Many enthusiasts continue to suggest that problems with the technologies can be resolved. Interestingly these disagreements typically go beyond evidence of failure contrasting with continued aspiration. Persisting enthusiasm about Web3 often has connotations of belief. Web3 technologies offer ways to manage communities. Disputes about the technologies can have the failure of minds to meet characteristic of discussions between in-group and out-group participants. Web3 users and user groups frequently form very strong attachments to their initiatives. Enthusiasts routinely express very optimistic and expansive aspirations for the technologies. Conversely, critics not only suggest that this optimism is misplaced, but that many Web3 initiatives involve misrepresentation, and enable abuses of trust and community.

Among Web3 enthusiasts, there is a tendency to elide predictions of what the technologies will deliver, with language of promotion and with exhortations to join the community working together towards that shared goal. Critics object to exactly that elision between analysis, marketing and recruitment, as misconceived or dishonest.

This paper will not cover the political aspects of Web3 in detail, but for many enthusiasts, setting Web3 against established systems and mainstream opinion is part of the appeal. Sometimes this has been deliberately linked to libertarian political agendas.

This paper will summarise the technologies, their objectives, and key barriers and criticisms. It will suggest that while the terminology is loaded and contestable, there are real issues at stake. Intensive arguments about the accuracy of a relatively new descriptive term for a movement may be ephemeral, but debates about Web3 express significant aspirations and concerns about how the internet and digital systems in general could, and should, serve society.

Enthusiasts tend to see challenges in Web3 as technical problems that will be solved by technical advances and more computing. They point to the shared experience of usability problems in internet services in the past that have been resolved by the combination of technical innovations, and continually increasing compute capacity, storage and data transfer bandwidth.

Critics do not only disagree with enthusiasts about what Web3 delivers, they can also dispute the broad proposition that technology presents sustainable, scalable and widely applicable solutions to problems of trust, that only need more time, more participation and more computing to resolve those problems. Critics tend to see challenges more in terms of trade-offs, where optimising for one principle, for instance decentralisation, will inevitably limit performance in terms of another principle. It is also possible to see the objective of trustlessness as itself somewhat antisocial.

These aspects of the debates may have implications beyond Web3. These different perspectives and insights are exploring whether and how communal values and principles can be instrumented and automated in technological architectures.

Summarising Web3 in 2023 is particularly challenging because 2022 was a very busy year. There were crises in many Web3 initiatives, and the piling up of failures has increasingly questioned the potential of the technologies to solve the challenges they have been designed to solve. Actions have been taken by Web3 initiatives and by governments to address challenges and risks. At present it is not clear whether these will be successful in enabling Web3 to succeed significantly, even in much more limited and circumscribed ways and areas. Many parts of the picture are moving, and this paper acknowledges that events and analyses cited in it may soon be superseded.

For clarity, it is useful to note that the term Web 3.0 has another and earlier use relating to the semantic web, described below. It is now sometimes used in a narrower sense, to describe only the more recently developed applications, not the underlying technologies, so including NFTs but not blockchains. Unhelpfully, the term has also sometimes been used to cover all the technologies that have come to be used on the internet in the last decade, including these, but also artificial intelligence, ubiquitous connectivity, virtual reality and the semantic web. Web3 should also not be confused with W3C, the World Wide Web Consortium, the international community that develops protocols and guidelines to support growth and development of the Web.

The next big thing? Webs 1, 2 and 3

The term Web3 implies a progression in the development of the internet Web 1.0 and Web 2.0. In comparison its forebear technologies electricity, telecommunications and digital computing, the internet reached mass and majority global use fast, and facilitated similarly rapid growth of certain applications, platforms and business models. The labelling Web1 and Web2 proposes stages within that growth and proliferation of services, imitating the numbering of successive versions of a software package. The title Web3 makes an implicit claim that these technologies constitute the next important current stage of the development of the internet, and a necessary correction of the direction of travel.

Web1 (or Web 1.0): In this analysis, Web 1 was read-only, composed of static html webpages created by multiple users, with standardisation only at the level of interoperability through TCP/IP. Because anyone could create, publish and link a webpage, Web1 did not tend to hierarchy. In practice, it did require a degree of skill and work to build a site and participate as a creator-publisher. To the general user, it offered access to information, but the limited search functions also meant that some investments of time and effort were required, for uneven and unpredictable benefits, which was a barrier to active interaction from the mass public who already had access to computers and connections, and so were at least potential internet users.
To give the view specifically from Web3, Ethereum's website gives this summary.

> Web 1.0: Read-Only (1990-2004)
>
> In 1989, at CERN, Geneva, Tim Berners-Lee was busy developing the protocols that would become the World Wide Web. His idea? To create open, decentralised protocols that allowed information-sharing from anywhere on Earth.
> The first inception of Berners-Lee's creation, now known as 'Web 1.0', occurred roughly between 1990 to 2004. Web 1.0 was mainly static websites owned by companies, and there was close to zero interaction between users - individuals seldom produced content - leading to it being known as the read- only web.[2]

Web2 (or Web 2.0): Web2 was read-write, with interactivity supported by Javascript. Web2 was characterised by platforms which took on the technical build and functioning for publishing and interaction, inviting a much wider range of users to contribute content, and reducing the work they needed to do to share or access information. It multiplied the network effects, while growing the networks. Again, this summary is from Ethereum.

> Web 2.0: Read-Write (2004-now)
>
> The Web 2.0 period began in 2004 with the emergence of social media platforms. Instead of a read-only, the web evolved to be read-write. Instead of companies providing content to users, they also began to provide platforms to share user-generated content and engage in user-to-user interactions. As more people came online, a handful of top companies began to control a disproportionate amount of the traffic and value generated on the web. Web 2.0 also birthed the advertising-driven revenue model. While users could create content, they didn't own it or benefit from its monetization.

From the perspective of Web3, the socio-economic development of Web2 from Web1 was not about wholly new technologies as much as efficiency and expanding usability and networking of applications.
In 1999, the designer Darcy DiNucci coined the terms Web 1.0 and Web 2.0 in an article.

> What we need to remember, though, is that the Web, as we know it now, is a fleeting thing. Web1.0… This concept of interactive content universally accessible through a standard interface has proved so successful that a new industry is set on transforming it, capitalizing on all its powerful possibilities. The Web we know now, which loads into a browser window in essentially static screenfuls, is only an embryo of the Web to come. The first glimmerings of Web 2.0 are beginning to appear, and we are just starting to see how that embryo might develop.[3]

Web 2.0 as a term was popularised by Tim O'Reilly and by the Web 2.0 Conference (later, Summit) he organised, held annually in San Francisco from 2004 to 2011 and attracting many leaders in internet services.

Users also shared the experience of continually improving platforms, with appreciable gains in legibility, search, speed and range and quality of media accelerating the growth of the user base. Part of the collective (and ongoing) experience of Web2 has been a small number of companies making the internet continually easier and more satisfying to use. The uptake of mobile internet can be seen as a significant subordinate phase and driver of Web2, extending reach and usability, real-time user-generated activity, and step changes in the use of the internet for social purposes.

Moxie Marlinspike, the cryptographer and founder of the instant messaging service Signal, memorably summed up why consumer preferences supported centralisation by internet service platforms.

> People don't want to run their own servers, and never will. The premise for web1 was that everyone on the internet would be both a publisher and consumer of content as well as a publisher and consumer of infrastructure.
>
> We'd all have our own web server with our own web site, our own mail server for our own email, our own finger server for our own status messages, our own chargen server for our own character generation. However – and I don't think this can be emphasized enough – that is not what people want. People do not want to run their own servers.[4]

This point – how much action and responsibility users are prepared to take – remains a key recurring test for uptake of Web3 applications.

Several linked factors led to "winner-takes-all market" profiles in Web2 subsectors including retail, social media and search. Perhaps the strongest was that the continually expanding generation of data about how services were used enabled continual improvement in the usability of those services, and in the capacity to respond to market opportunities. The companies that moved ahead could immediately improve faster than the competition. Users recognised improvements in usability and embraced those services even more. The continual evolution of a service worked both at global scale, and at the level of personalisation, by building user profiles and tweaking the individual user's experience. Network effects and usability improved exactly because users gravitated to a small number of platforms, rather than scattering across many unconnected islands.

Users did not want to pay to network with other users either, and no effective system for micro-payments emerged, driving services to explore alternatives, to monetise through other means. Users could not develop their own search. Developing an effective and continually improving search function turned out to be transformational for users, usability, and for a succession of search providers, until Google pulled ahead of the rest.
Centralisation became the dominant model for internet platforms and markets, and from the Web3 perspective, that is also where problems became entrenched. Users were presented with notoriously unreadable and unread contracts for use of services, on a "take it or leave it" basis.

The dominance of the major internet platforms Google, Facebook and Amazon has generated concerns that have grown over time and in strength and variety. Earlier on, governments in liberal democracies generally avoided committing to intervention, welcoming innovation and commercial success, and uncertain whether legal transfers of information were an appropriate subject of regulation. In the 1990s a small number of commentators early on saw the potential for ever-expanding powerbases, and problems that could result, but overall the growth of negative reactions was gradual. More recently the characteristic internet platform structures have been explored in detail and across the media, perhaps most powerfully in Shoshana Zuboff's book The Age of Surveillance Capitalism.[5]

Over time, the term Web2 came to be used more negatively, describing that shift to the market dominance of a few models, based on accumulation of data about individuals, the original sin from a Web3 perspective.

> In web2, you don't have any control over your data or how it is stored. In fact, companies often track and save user data without their users' consent. All of this data is then owned and controlled by the companies in charge of these platforms.[6]

This is the status quo which Web3 is set against.

Web3: Web is defined as read-write-own. Web3 offers as a set of tools to re- empower users through control of their data, re-establishing the less hierarchical models of Web1, while retaining the usability of Web2. Web 3 is placed, promoted and collectively willed as an evolution beyond that dominant Web2 model of markets dominated by a small number of global corporations whose success is built on accumulation and use of data.

This is Ethereum's summary.

> The premise of 'Web 3.0' was coined by Ethereum co-founder Gavin Wood shortly after Ethereum launched in 2014. Gavin put into words a solution for a problem that many early crypto adopters felt: the Web required too much trust. That is, most of the Web that people know and use today relies on trusting a handful of private companies to act in the public's best interests.[7]

Seeking to replace Web2 hierarchies is often cast as a heroic collective endeavour, but the inequalities it responds to are global and widely acknowledged. There is a great deal of dispute about what Web3 could achieve, but plenty of consensus about the problems it seeks to address.

As a side-note, at an earlier stage, the term Web 3.0 was linked with the Semantic Web. This was an initiative set out in 2001 to make internet data machine-readable, with standards and technologies supporting data stores, vocabularies and protocols.8 In 2003, Tim Berners-Lee described the semantic web as a component of Web 3.0. More recently he has said that it's possible to call it Web3, but clarified that it takes a very different approach to applications using blockchains.[9]

There are many similar definitions of Web3. This one in a 2019 article about blockchain in the creative industries has broad application.

> Web3, underpinned by blockchain technology, is an evolution of digital infrastructure, whereby protocol-enforced consensus mechanisms facilitate the direct (that is, peer-to-peer) exchange of value between users, removing the need for trusted intermediaries.[10]

Web3 is an evolving ecosystem of applications of a group of overlapping and interacting technologies, which are continuing to be developed. There is disagreement as to whether they can yet be said to be mature (and even over what that would mean), and whether further developments could realistically be expected to resolve major challenges, broadening applicability and driving mass uptake.

While Web3 as a term has been in use since 2014, there has been a surge in discussion of it very recently, starting in 2021. It is not yet clear whether this represents some maturing of the family of technologies, or appetite in Web3 circles to show that it is more than cryptocurrencies.

There are several organisations supporting collaboration to develop Web3 technologies. The Web3 Foundation or W3F was founded in 2017 by Gavin Wood, and funds research and development on decentralised web software protocols. The Foundation organizes the Web3 Summit "to consolidate key stakeholders to talk about the impact the Web3 is about to wield on financial institutions, digital services, information society, individuals as well as regulators and market watchdogs."[11]

This paper cannot go deep into detail about these key Web3 technologies. Below are short summaries (which necessarily involve simplifications) outlining how Web3 developments build one upon another and link together. While the technologies are used for very widely different purposes, it is reasonable to talk of an overall Web3 ecosystem. However, it is difficult to make accurate general statements about the Web3 ecosystem, or to say where one technology or type of application ends and another begins. These definitional questions present challenges for governments and regulators, as well as for anyone trying to describe Web3 effectively.

Key Web3 technologies and concepts

Distributed ledger technologies (DLT): Protocols that manage data storage distributed and replicated across multiple facilities with different owners. These are typically geographically separated and connected by peer-to-peer networks on the internet. The ledger is shared and assured by an agreed system, a consensus mechanism, which manages agreement between them as to accuracy of the record, without any individual participants or third party having greater power than the other participants to influence the record or change the terms of the system. DLTs provide security by design, defending against falsification of records, because falsification would need to change all the distributed copies simultaneously. Bitcoin has been the most significant and influential DLT, but using distributed ledgers to counter falsification predates Bitcoin.

Blockchain: Blockchain is a type of DLT for recording data about transactions and/or ownership of assets in successive accumulating blocks, which are shared by a network, and which cannot be changed by individual participants.
Blockchains can be developed for specific purposes in a wide range of sectors, with bespoke terms for participation and access to information, but the underlying technology is agnostic as to the nature of what is recorded. Blockchains are the basis for many Web3 applications, including for protocols (including Bitcoin and Ethereum) that support cryptocurrencies.
The foundation of Blockchain is a 2008 paper Bitcoin: A Peer-to-Peer Electronic Cash System, attributed to the pseudonymous author Satoshi Nakamoto. The paper set out a solution to the double-spending problem using a peer-to-peer network, and proof-of-work, a consensus mechanism involving solving mathematical puzzles to authenticate transactions and create blocks.

> The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.[12]

Bitcoin: Bitcoin is a digital currency exchanged peer-to-peer between users without a central banker. Bitcoin was the first cryptocurrency, and is to date the most significant and impactful. As proposed by the above paper, new currency units (coins) are created by solving mathematical problems, a proof of work became known as mining, by analogy with mining metals to make currency. Successful miners are rewarded with a Bitcoin. Bitcoin is supported by a public record of transactions, but participants can be (like Bitcoin's creator) pseudonymous, as Bitcoin holdings are connected to digital addresses and not to identified individuals. Bitcoin was a major development in Web3, but it also revived peer-to-peer systems, which had been a major feature of Web1.

Bitcoin is traded on dedicated exchanges, with Bitcoins stored in dedicated digital wallets. It provides a currency system without third party banking service providers or oversight by authorised regulatory authorities. Bitcoin has provided the model for many more cryptocurrencies.
In May 2021 Currency Exchange International reported that globally, over 15,000 companies were accepting Bitcoin.13 Blockchain.com wallets, something that makes purchasing Bitcoin possible, reached over 81 million wallet users in 2022.14

The value of Bitcoin in fiat currency has fluctuated very significantly over time: $0.30 at the start of 2011, $770.44 in 2014, $13,412.44 in 2018, $3,869.47 in 2019, $7,188.46 in 2020, $29,391.78 in 2021, and $19,137.72 at the end of January 2023.[15] Throughout Bitcoin's history this volatility has generated excitement and consternation by turns, and it continues to influence scepticism about the Web3 family of technologies. To be useful for mediating commercial exchanges of value, currencies should probably not be that exciting. Non-digital currencies also do not generally give outsize shares to a group of founders.

Cryptocurrencies: Cryptocurrencies are systems that manage digital exchanges of financial value between participants in a peer-to-peer network without a governing bank or controller, recording transactions to a blockchain and using cryptography for security. Bitcoin was the first cryptocurrency, but thousands more have been created.

Because digital data is easily copied, and all general purpose computing can copy data, a basic challenge of a digital currency is how to prevent a single unit of value being copied and spent twice, or many times. Cryptocurrencies prevent double- spending by recording ownership and transactions on a blockchain.

Cryptocurrencies are used for very different functions in many bespoke systems. Use for retail transactions remains a small proportion of crypto activity, relative to trading. There is also some use for international transfers. Cryptocurrency systems can be used as alternatives to fiat currencies, and may offer greater speed, lower transaction costs, and resilience compared to systems with a single point of failure. In recent years activity in emerging economies has accelerated, reportedly because of the shortcomings of the traditional financial systems.[16]

In 2022 it was reported that there were 10,400 different cryptocurrencies, a number that had more than doubled in a year earlier, in spite of substantial crashes in the overall combined valuation of cryptocurrencies.[17] There is some debate as to how accurately these estimates report value in cryptocurrency, but even given that, it is clear that collectively cryptocurrencies are globally significant and volatile.

A variety of types have emerged. A stablecoin is a cryptocurrency pegged to another asset, which can be a commodity price or a fiat currency or basket of currencies. As the name suggests, stablecoins aspire to provide comparatively less volatile investments than other cryptocurrencies.

There is an important distinction between permissioned and permissionless blockchains. Permissioned blockchains have controlled access, so are not available for public use. This provides security, but also necessarily does not involve the lack of centralised control that many Web3 advocates celebrate. Most of the excitement, hype and problems in the sector relate to permissionless blockchains. The distinction reflects a broader and perhaps unsurprising pattern across Web3: the fewer control functions an application has, the more it can offer something genuinely new compared to previous technologies, but also the more likely it is to involve risks.

Ethereum: Ethereum may represent the leading example for Web3 offering a set of widely applicable and sufficiently usable general purpose internet technologies.
Ethereum is an open source blockchain enabling smart contracts. It is now perhaps the most significant Web3 service, supporting a growing number and variety of collective endeavours.

Ethereum was initiated by Vitalik Buterin in 2013 and developed with a group of founders. Ether is the second largest cryptocurrency to Bitcoin by market capitalisation. By the end of July 2021, "Ethereum would be processed more than 1.1 million times per day. This was more than six times that of the more commonly
known rival Bitcoin."[18]

The significant development from Bitcoin is that Ethereum is programmable, supporting apps that use the blockchain to store data and determine functionality. Ethereum has been particularly popular for decentralised finance and NFTs.

Ethereum dApps are in use in finance, advertising, healthcare, real estate, identity management, and supply chain management, but the variety of purposes for which its smart contracts are being used, even if experimentally in some, make it difficult to place in any established category of business services or sectors. Ethereum has been important for the development and use of DAOs. It has also supported Initial Coin Offerings, token-based for crowdfunding for start-ups, proving alternative routes to Initial Public Offerings. However, some of these have been significant failures, and some frauds.

Ethereum provides software and networks to businesses through Ethereum Enterprise. It supports assurance of supply chains from producers to consumers, in luxury goods and contested commodities like diamonds through to food.
Compared to many other Web3 initiatives, Ethereum has done some more to fulfil the aspiration to attract and serve multiple user groups through a different model than that of Web2 platforms, without many of the centralised controls characteristic of those. Ethereum's own online description emphasises this.

> Ethereum is a technology for building apps and organizations, holding assets, transacting and communicating without being controlled by a central authority. There is no need to hand over all your personal details to use Ethereum - you keep control of your own data and what is being shared. Ethereum has its own cryptocurrency, Ether, which is used to pay for certain activities on the Ethereum network… Ethereum allows anyone to deploy permanent and immutable decentralised applications onto it, with which users can interact.[19]

It is interesting that defining Ethereum's overall function is challenging. It is not a platform in Web2 terms. Digital technologies already have a history of collapsing boundaries between sector, and Ethereum might represent another stage of that, merging marketing, social value and evangelical mission, with tools for active participation. It is telling that choosing indicators to measure its success is hard. Neither market capitalisation nor user-numbers provide a basis for easy comparison with more established internet businesses or services.

Long before the internet, many providers of products and services encouraged their customers to think of themselves as members of a community, with social links to each other and to the provider. Online social media built and diversified that to create channels for community, to enable wholly new communities, and to manipulate users' feelings about community to drive some behaviours. Software developers have also long formed a wide range of different communities, some with a consensus around a shared view of society, intellectual property, equity, or just of what works.

However, aspects of Ethereum represent a different mode of collective activity, that builds on all of these, but further develops use of shared technology tools into a communal mission, though not necessarily a tightly defined one. Users are invited to learn and to participate in building new

applications and contributing to the development of the whole network and its impact on the wider world. This develops the potential of internet developer user groups into something that looks new.

Running through the tools and services offered to support communal activities there runs a broader implication that all legitimate uses of Ethereum contribute to a shared journey towards a goal of wider benefits for all. It is a social movement.

One of the aspects that makes Ethereum more convincing as Web3 than many other initiatives is the open recognition of current limitations, challenges and criticisms, which acts as a spur to further collective action.

Ethereum has recently undertaken an upgrade process titled Ethereum 2.0 including a shift from proof of work to proof of stake. “Proof of work” and “proof of stake” are consensus mechanisms used to verify transactions and add them to the blockchain. As above, proof of work for blockchain involves competing to solve mathematical problems, and is widely regarded as unacceptably energy-intensive. Proof of stake involves participants providing (staking) cryptocurrency to have a chance to gain the opportunity to deliver the new validation and gain a reward. Ethereum’s execution of the change, “the merge” has been seen as an important test of the capability of Web3 to evolve to meet changing priorities. However, it also introduces a new hierarchical function.

Tokens and tokenisation: Tokens are digital assets managed by smart contracts and recorded on the blockchain. They can represent ownership of a share of a blockchain and participation and often shared governance rights in a network.
Tokenisation describes dividing rights in an asset into pieces that can be held, used and traded. Tokens are sometimes described as a new asset class, but the great diversity in what they relate to and are used for means that it is difficult to categorise them in established terms for assets.

The terms token and tokenisation are used loosely in Web3 discourse, which can lead to ambiguity.

Smart contracts: A smart contract embodies contract terms in software rather than legal language. Parties to the contract agree to this automated systematisation and settlement. A smart contract can automatically execute those terms when the conditions specified in the contract are achieved. Storing the smart contract on a blockchain is intended to fix and protect the agreed terms.

Decentralisation: The distribution of assurance in a system, is key to Web3 technologies and why they offer alternatives to other systems for managing group activities. There are now movements promoting this decentralisation by applying Web3 technologies to apps, and to finance, government and more sectors.
Decentralised applications (dApps): Applications controlled by smart contracts and running on a blockchain (many on Ethereum) or another peer-to-peer network. They offer privacy and confidence in automated completion of transactions.
Decentralised finance (DeFi) may be the most active of these. Decentralised cryptocurrency services using blockchain and smart contracts that complete transactions given specified conditions.

Decentralised Governance (DeGov) is organisational governance distributed to the networked community of users of the services.

Decentralised Government (also DeGov) describes a class of initiatives driven by the proposition that Web3 tools can improve government, supporting citizen engagement and participation. There have been critical analyses of the proposition, which have identified potential risks “related to a dominant position of private powers in distributed ecosystems, which may lead to a general disempowerment of citizens”.[20]

Decentralised Science: "Decentralised science (DeSci) is a movement that aims to build public infrastructure for funding, creating, reviewing, crediting, storing, and disseminating scientific knowledge fairly and equitably using the Web3 stack."[21]
DeSci initiatives seek to offer ways to fund, publish and review scientific research that avoid problems with incentives and obstacles perceived in mainstream systems, improving access to knowledge and communication between researchers, and making more support available to innovative and unconventional research. One example is a protocol for managing peer review.[22]

Decentralised Autonomous Organisation (DAO): An organisation bringing together participants in a collective activity governed by rules set in a digital architecture, agreed by participants and without other management actors or hierarchies. Where a traditional company or other joint endeavour would typically be governed by legal agreements between participants, generally recorded by a lawyer and placed in a public record, the functioning of a DAO is governed by limitations that the technology places on how participants can interact. No participant can change the consensus rules of the DAO without others knowing.

There are many different structures for DAOs, and precise and flexible adaptation to a specific purpose is a great part of the appeal. DAOs may be established purposefully to act in more flexible, democratic and distributed ways than registered companies, but they typically do not have legal personhood, which can prevent them undertaking some activities that companies can. If a DAO is intended to be profit- making, it will be subject to relevant law governing securities.

There is a growing subsector of companies that provide services to DAOs that act as companies or other types of institution, including for law, finance, people management, voting and project management.

Wallets: Wallets are digital repositories for secure storage of digital assets. Wallets are enabling applications for storing and using cryptocurrencies and other tokens, but the concept is wider, embracing personal assets and interfaces for a potentially much wider range for Web3 activities. Wallets can be centralised or decentralised. As elsewhere in Web3, decentralisation enables individual control without involving a governing service provider, but it creates different risks. As will be explored later, wallets are one of the pinch-points of Web3, where a limited number of facilities to manage exchange and extraction of value means that in practice centralisation re- emerges.

Forking, composability: Forking is the capability to change the functioning of a blockchain. The actuating software is changed, and a modified chain diverges from the original one. There are different ways to fork. A soft fork is an upgrade that remains in communication with the original. A hard fork involves greater changes and loss of that backwards compatibility, creating a new and separate network.

Non-Fungible Tokens (NFTs): A non-fungible token is blockchain-enabled cryptographic record of ownership of an asset, which may also be an asset in itself. The record is held on a blockchain. It is non-fungible because one NFT is specific and cannot be substituted for another, as a Bitcoin, dollar or pound can be. NFTs can function as a way of assuring and making public ownership of a wide range of assets, digital, physical or intangible, including intellectual property. With digital assets that can easily be copied, NFTs provide assurance of sole ownership, and so also digital scarcity.

NFTs are relative newcomers in terms of uptake and public profile, compared to other Web3 technologies, but NFT markets have already seen both fast growth and volatility, in particular in NFT art markets. Owning an NFT relating to a copyright work does not include ownership of the copyright of the image the NFT relates to.

The Metaverse: The Metaverse describes a projected expansion and networking of virtual reality technologies online. The concept is less developed than Web3 but is relevant here because it is suggested that the Metaverse would use Web3 technologies to empower individual control of data and identity, to resist centralised control by platform companies, and for the creation and exchange of digital assets, including with cryptocurrencies. According to one source:

> The technological infrastructure of the Metaverse, ie Web3, consists of blockchain technology, smart contracts, and Non-Fungible Tokens (NFTs),which reduce transaction and agency costs, and enable trustless social and economic interactions thanks to decentralised consensus mechanisms. The emerging Metaverse may give rise to new products and services, new job profiles, and new business models.[23]

It is relatively easy to see how blockchains could be used in supporting functions for the Metaverse, like assets and payments. However, it is much less clear how they would support the experiential aspects which are the Metaverse's main stated function. In the versions of the Metwaverse developed to date by Meta and Microsoft, NFTs are only elements in immersive online environments.

Central Bank Digital Currencies (CBDCs): While cryptocurrencies evolved to provide alternatives to fiat currencies and government control, the sector is providing some models to governments. Many governments are now exploring the potential benefits of a Central Bank Digital Currency, a digital form of the fiat currency. In March 2022, the Bank of England published a discussion paper, Central Bank Digital Currency: opportunities, challenges and design, which sets out potential advantages and risks. The paper suggests that much can be learned from the uses of decentralisation and cryptography in cryptocurrencies, while retaining the backing of a Central Bank and so greatly reducing volatility and risk.

Some analysts suggest that CBDCs would make many stablecoins redundant. CBDCs obviously lack the appeal that Web3 has for many cheerleaders, of managing without governments, but if they can combine what Web3 does well with what governments can do well, they might become significant.

What's wrong with Web3? Challenges and limitations

There have been many critical analyses of Web3 applications and the movements built around them. Many critiques point out where Web3 applications do not genuine deliver decentralisation, security, privacy and a non-hierarchical community or network as intended and represented. Another group of criticisms points to examples where Web3 applications do provide those things for the user community, but at the expense of wider society. Some observers see Web3 technologies as solutions looking for problems. Many initiatives have demonstrated little or no value as ways to support communal interactions. Some have been spectacular failures, and others mechanisms for fraud.

A less critical trend of comment questions scalability and breadth of applicability, compared to previous internet technologies. Web3 technologies clearly have some claim to be seen as general purpose internet technologies, because they are being used in a wide range of sectors. However, debate continues over how effective they are for some of those purposes, whether their benefits outweigh disadvantages, and whether other online community architectures might work better for some uses.

This leads to a broader question of whether technical solutions can satisfactorily resolve problems of usability, privacy, trustworthiness and scale, or if only different trade-offs are achievable, not resolutions. From this perspective, Web3 applications do offer new ways of making trade-offs, customisable for different uses and communities according to shared priorities.
This is also typically a divergence between emphasis on future potential as against current realities. Many enthusiasts emphasise what might be realised by Web 3, supported by hope, or belief, that obstacles to wider adoption are technical challenges that will be overcome.

Critics point to current obstacles. While blockchains may be inviolate, there can be weaknesses and chokepoints in the systems around them, including keys and exchanges, that undermine both the overall objective and practical security and usability. They see tensions between decentralisation, security, complexity, usability and appropriate use of resources (in particular energy) in internet services as more enduringly difficult to resolve. They do not see realistic pathways towards these technologies having importance for general users, and so forming a real Web 3, a substantial step change in the internet's evolution.

Hype continues to be divisive. An expectation of exponential growth in performance and uptake has been inherited from Web2. It has driven enthusiasm and investment, but inflates the gap between promotional activity and actual achievements.

> And now it seems the Silicon Valley billionaires are intent on turning the whole thing into a reckless startup-esque race, each disrupting the next iteration until they either crack it. Or destroy it completely.[24]

Even this very brief overview of Web3 technologies, and what they have been used for, shows that it is difficult to make accurate general statements, let alone predictions, about Web3. But as there are commonalities in the tools and the type of functions they are used for, there are common aspects to the challenges and limitations.

Trust

For the wider public outside Web3 circles, the most negative connotations of the technologies relate to volatility and fraud in cryptocurrencies. The key common benefit offered by Web3 is choice of multiple adaptable ways to structure trust relations between a group of participants.

Crypto is a poor shop window to the world for that. Some cryptocurrencies have demonstrated clearly that innovation can equally be directed to novel ways to abuse trust. The connotations of novelty, fashion and anti-establishment community have clearly been employed in many cases to distract users from looking closely at governance and transparency.
Cryptocurrencies as a set have not delivered reliable safe havens for investors. More than $1 trillion in value in cryptocurrencies has been lost since peaks in 2021.
Cryptocurrency wealth appears overall to be distributed as unequally as more traditional forms, and has not at least yet, demonstrated a turn towards equality and inclusivity.[25] Cryptocurrency may offer alternative assets to people who are excluded from some other financial services, but that may also mean those people are driven to services that involve comparatively more risk.

It would take at least a book to give a good account of problems that have arisen with cryptocurrencies, but some characteristic problems recur. Some of these read across to other Web3 technologies, of which more below. Some are specific to cryptocurrency.

These decentralised and anonymous systems do not have central controllers or single points of failure, which also means they do not have governance that can intervene and rectify problems. The lack of external assurance and governance make it more difficult to distinguish between responsible offerings and fraudulent ones, contributing to suspicion of the whole sector. Regulators continue to struggle and to differ between jurisdictions in their approaches. This may offer opportunities for evading regulation and for regulatory arbitrage, but it also creates uncertainty. Recently it has become clear that regulators signs in many countries plan to do much more, but there is still no evident consensus approach.

Some schemes have simply failed to deliver the security promised. Some have failed to grow a user-base. Some cryptocurrencies appear to have been launched simply to replicate the success of others, while offering nothing new, and have failed to catch up with the earlier entrants. Some cryptocurrencies have clearly deliberately been established as Ponzi schemes, relying on attracting new entrants to pay earlier ones. Even with more well-intentioned ventures, structural inequality has often favoured earlier investors over later ones to a degree that many judge disproportionate, and certainly puts into question any claims to an absence of hierarchy.

The communal, participatory language and recruitment of users characteristic to Web3 technologies have in many cases been debased into hype and misrepresentation, encouraging investment into unequal and abusive systems. Growth is driven by uptake, and by supportive media activity. Discourse in and around cryptocurrency is full of cant terms, emphasising community to those in the community, potentially alienating those outside. Even abuses in crypto have dedicated terms. “A rug pull in the crypto industry is when a development team suddenly abandons a project and sells or removes all its liquidity.”[26]

The website DeadCoin tracks failed cryptocurrencies, “cryptocurrencies that have been abandoned, used as scam, their website is down, has no nodes, has wallet issues, doesn't have social updates, has low volume or developers have walked away from the project.” At the time of writing it lists 2416.[27]
OneCoin was launched in 2014 and promoted with eye-catching events, but was later reported to be a Ponzi scheme, using funds from new investors to pay old ones.
The leading figure has been charged in absentia, and in June 2022 appeared on the FBI Ten Most Wanted list. Further on, doubts emerged as to whether it in fact used blockchains.

In 2022, Luna failed, collapsing in value from $20 billion to almost nothing in days. Luna was categorised as a stablecoin tied to Terra USD, but the link of that to the dollar was adjusted, and investors exited rapidly.

That failure was one of the major events in a wider fall in value across the cryptocurrency sector in 2022.

> Since November the value of all cryptocurrencies has fallen from $3tn, meaning that $2tn worth of wealth has been wiped out”. Interestingly this happened “with no serious knock-on effects to the broader stock market – so far.” While enthusiasts have been keen to bring cryptocurrency into mainstream finance, it is still separate to a degree.[28]

The cryptocurrency exchange FTX was founded in 2019 and was the third largest exchange by July 2021 with over a million users. Its collapse in 2022 may supply the news with colourful stories of malpractice and misrepresentation for some time.

One recent observer suggested that “crypto is hell-bent on playing out the mistakes of traditional finance at hyperspeed.”[29] In 2014, Robert Synott tweeted “Bitcoin: a system designed to teach libertarians that financial regulation is actually a good thing.” In 2021 he followed up “Since I wrote it eight years ago, there has been a >7 figures crypto theft every week or so; the lesson doesn’t seem to be getting through.”[30]

Many commentators conclude that it is not surprising that assets which cannot be used to pay taxes, and whose value is dependent only on sentiment within communities of speculators without relation to external commodities or systems, should be subject to volatility and frequent collapses.

> In the end, claims that the value of crypto is insulated from the whims of “men”are bunk. In fact, cryptocurrencies are completely dependent on whim, and in the worst possible way: self-fulfilling expectations (what is politely known as “market sentiment”) are the only driver. What the great MIT economist Charles Kindleberger called “manias, panics, and crashes” are the norm for crypto, not the exception.[31]

The variety across the large, small, purposeful, frivolous and criminal initiatives is in part a function of how easy it is to create a cryptocurrency. This can become self- referential. $STOPELON coin, described as the first protest cryptocurrency, was created to protest against Elon Musk using Twitter to influence cryptocurrency markets.[32] Because crypto is reported and discussed as a sector, this means that backers of sustained and well-designed initiatives can never be certain what new enormities will next surface to dominate the news and undermine confidence across the sector.

Cryptocurrencies that do deliver privacy and security for users may cause harm to society. Decentralisation and anonymity put systems beyond the governance of law and policing, and cryptocurrencies have provided criminals with secure markets, and ways of storing and transferring the proceeds of crime. Crypto can also enable tax avoidance and evasion of government regulation. Over time, some authorities have improved their tools for counteracting the use of crypto for these

purposes, but it remains a problem, and continued innovation always threatens to create new covert protected online spaces, and new threats to effective enforcement. Chainalysis reported that "Cryptocurrency-based crime hit a new all-time high in 2021, with illicit addresses receiving $14 billion over the course of the year, up from $7.8 billion in 2020."[33]

The criminal use of cryptocurrency has predisposed many in governments against it, driving calls for regulation. It has also deterred many institutional investors from participating, which itself acceptance as a set of legitimate alternative financial instruments.

More might be done to encourage the general public to see the rest of Web3 as separable from the worst problems in cryptocurrency, but many Web3 advocates insist on presenting the technologies as an integrated movement, rather than multifarious uses of a set of tools which can be used for very different purposes. This may help to build a collective sense of momentum, but it also undermines the credibility of useful systems through association with fraud, criminality and empty hype, of which there has been plenty.

For some commentators, the more recent attention to the social potential of Web3 is simply a distraction from the excesses of crypto.

> At its core web3 is a vapid marketing campaign that attempts to reframe the public's negative associations of crypto assets into a false narrative about disruption of legacy tech company hegemony. It is a distraction in the pursuit of selling more coins and continuing the gravy train of evading securities regulation. We see this manifest in the circularity in which the crypto and web3 movement talks about itself. It's not about solving real consumer problems. The only problem to be solved by web3 is how to post-hoc rationalize its own existence.[34]

There has been a very clear rise in the frequency of discussion of Web3 since the 2021 cryptocurrency crash. That may be diversionary, but there are reasonable arguments for distancing many domain-specific applications of Web3 technologies from cryptocurrencies.
However, other Web3 applications have also been criticised for failing to deliver trust and reliability as promised. The automation that is a key feature of a smart contract may also mean inflexibility when circumstances and needs change, or the original contract proves to have unanticipated flaws in practice. If a central authority intervenes to address those, it demonstrates that the system was not in fact decentralised. More broadly, there is always a dependence on the means by which digital assets or contracts are translated into the non-digital world.

> There is an intractable problem in linking a digital to a physical asset whether it be fruit, cars or houses at least in a decentralized context. Physical assets are regulated by the jurisdiction you happen to be in and this means they are in a sense trusting something in addition to the smart contract you've created. This means that possession in a smart contract doesn't necessarily mean possession in the real world and suffers from the same trust problem as normal contracts. A smart contract that trusts a third party removes the killer feature of trustlessness.[35]

Decentralisation

As above, decentralisation is one of the key characteristics and offers of Web3. It promises security, because there are multiple assured and networked copies of data, without single points of failure, and can support shared governance without hierarchies or other concentrations of power.
In practice, there remain bottlenecks and pinch points in many Web3 systems where a small number of organisations have a critical role in ensuring that the systems continue to work, and in exchanging any value in or out.

> The empirical (re-)decentralisation of the internet is lagging behind, and front- runner areas such as cryptocurrencies have been experiencing re- centralisation already. For example, when it comes to digital wallets for cryptocurrencies, ConsenSys, a New York City–based blockchain software development company focusing on utilizing Ethereum (decentralised technology), owns both Infura and the most popular wallet, MetaMask. Apps also often rely on a few companies to read and make changes to the blockchain on their behalf.[36]

> Almost all dApps use either Infura or Alchemy in order to interact with the blockchain. In fact, even when you connect a wallet like MetaMask to a dApp, and the dApp interacts with the blockchain via your wallet, MetaMask is just making calls to Infura![37]

Successive crises in cryptocurrencies have also shown that central controllers can step in. This may well have benefits for holders of the currency, but does conflict with the way they are presented.

> Close observers have warned for years that many crypto systems (not just in DeFi) are engaged in so-called “decentralisation theater.” In principle, DeFi should share the uncensorability and irreversibility of a pure cryptocurrency like bitcoin, but this is rarely true. Centralised administrators of systems can often be seen stepping in to mitigate or reverse hacks.[38]

In other examples, in-principle voting rights can be arduous to exercise in practice. A shared immutable ledger does not on its own guarantee that a growing community will interact equitably and transparently over time and through change. There are difficult questions about how participation should relate to rewards and votes can appear in Web3 communities, just as they recur in the management of human communities of all other kinds.
Then there are the challenges when a service is decentralised without a controller who takes responsibility for compliance with law and regulation.

> Whose lawyers will respond to the DMCA requests? Who is going to ban the Nazi accounts?[39]

It is clear from the backlash against Web2 platforms over moderation and lack of it on social media, that in general the public do not want no one to be responsible and answerable, and governments will increasingly not let that happen.

For users who lack technical understanding, the time or the tools to do the work themselves, trusting a Web3 service may not in practice be very different from trusting any other authority. Using it may only be substantially different from Web2 if there are measures to prevent intermediaries from gaining from processing data.

That might be assured by regulation of services, which then implies a role for governments, or organisations appointed by governments. From one point of view, the problem with Web2 was not centralisation, but lack of regulation.

Web3 aspires to render hierarchies unnecessary and technically impossible, in contrast to the huge benefits that have flowed to early investors in Web2 winners. However, similar patterns have been seen in Web3, with early investors gaining disproportionately.

Usability

Web2 platforms grew because they became easier to use. Uptake at scale involved minimising the time, tools, money and effort to use the services. Web3 currently struggles with this. Many Dapps remain difficult to use and (as above) there are bottlenecks. Making a service easier to use tends to involve recentralisation. Scale requires efficiency, which requires specialisation. Not everyone wants to be a specialist or have the equipment, so they use specialist intermediaries. We are back to people not wanting to own their own servers. Web3 usability challenges are not currently being solved by improved dedicated browsers, as many issues were in Web2.

Some see this as a stage, before automation and usability evolve to allow individual users to manage without these intermediaries. In Web2, Moore's Law and its analogues in storage and connectivity did support the ironing out of usability friction over time. However, it is not clear that friction in Web3 will fade away in a similar fashion. Some commentators believe that the need for trade-offs that will keep recurring at different points as uptake increases, as an inescapable result of successful growth.

> On a compute basis, blockchain networks don't scale except by becoming the very same plutocratic and centralised systems they allegedly were designed to replace. There is an absurd cost to trying to do censorship resistant computation. In this regime there is a hard incentive to minimize program execution time because the entire network is forced to recompute every single program as part of its insanely wasteful process of attempting to reach consensus about a giant global state machine.[40]

Energy use and redundancy

Proof of work for blockchains has already used a great deal of electricity and hardware waste.

A recent blog published be the European Central Bank summarised this.

> It's also worth noting that the Bitcoin system is an unprecedented polluter. First, it consumes energy on the scale of entire economies. Bitcoin mining is estimated to consume electricity per year comparable to Austria. Second, it produces mountains of hardware waste. One Bitcoin transaction consumes hardware comparable to the hardware of two smartphones. The entire Bitcoin system generates as much e-waste as the entire Netherlands. This inefficiency of the system is not a flaw but a feature. It is one of the peculiarities to guarantee the integrity of the completely decentralised system.[41]

Some Web3 initiatives are addressing this, though many are not as yet.

As above, in September 2022, Ethereum completed the Merge, moving to a proof of stake model, and cutting energy use.

> We're talking about a fully functioning, open-source ecosystem with a capacity for evolution that other cryptocurrencies clearly lack, a change that would allow it to scale up its performance from about 15 transactions per second to 100,000 at a time when its blockchain is being used for more and more things, and that would reduce its energy consumption by about 99.95%.[42]

The Merge has been widely welcomed as evidence that Web3 can respond to changing priorities and adapt while retaining functionality. However, the move reintroduces intermediaries and hierarchies, arguably undermining the claim to trustlessness.

However, there are wider questions about energy use in Web3 than just proof of work. Internet use in aggregate, and the major platforms in particular, are coming under increased scrutiny in relation to energy use. Streaming of films and television has already attracted attention, and the major companies have come under pressure to quantify and minimise the energy use from their use. There is now attention to how much energy is expended storing millions of user-generated photos in easily recoverable form. It is likely that emerging services looking to move from niche to mass uptake, will increasingly need to quantify and justify energy use, transparently and in relation to common public standards.

That will be difficult given the complexity and redundancy of Web3 systems. The view from enthusiasts that current challenges will be solved by innovation and more computation will be challenged by energy concerns, even if artificial intelligence is employed to manage the growing complexity of processes.

Regulation

More regulation is coming. Governments and financial regulators are setting out measures to regulate cryptocurrency and other Web3 financial services. Much as previous waves of digital innovation have broken down boundaries, Web3 presents new forms of organisation and function that do not fit models known and currently regulated, but work is proceeding in many jurisdictions to identify risks more precisely, and devise regulatory tools to reduce them.

In September 2022 (a busy month for Web3 even in a busy year), the US White House released its first Comprehensive Framework for Responsible Development of Digital Assets.[43] This sets out frameworks and policy recommendations on six priorities identified in an Executive Order in March 2022: consumer and investor protection; promoting financial stability; countering illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.

The Framework represents a detailed and coordinated government effort to gain collective national benefits from digital assets while reducing risks and countering abuses. It announces that Web3 technologies are now of national and international significance, while also recognising that many potential issues remain poorly understood, setting out many areas for research and consultation, and signalling that further regulatory action can be expected. The emphasis on responsible innovation suggests a welcome refusal to see responsibility and innovation as conflicting. It is interesting that regulation has gained purchase and a way of dealing with Web3 by focusing on assets.

As Web3 applications are used in more sectors, additional questions arise about how they comply and can be demonstrated to comply. In terms of mainstream adoption, regulation also holds positive potential, in that more institutions will be prepared to engage and invest in regulated sectors.

The UK Government and regulators have published guidance on digital assets and are in the course of developing more comprehensive regulation and support to the sector.

This is not to say that governments will necessarily find it easy to devise appropriate regulation for all potential application areas. They will generally want to avoid prescription about technical functions, and to regulate proportionate to risk, which is traditionally done on a sector basis. This is challenging when one technology is used in different sectors with very different kinds and scales of risk. At the same time, regulators need to attend to the erosion of sector boundaries that is a feature of the spread of data technologies. They will also need to learn across sectors. In this context, the UK's Digital Regulation Cooperation Forum looks to be a very useful development. The Forum regulators learn from each other's experiences with emerging digital technologies.[44]

Some argue that more regulation could unduly legitimise Web3 applications, as the European Central Bank blog put it here.

> The current regulation of cryptocurrencies is partly shaped by misconceptions. The belief that space must be given to innovation at all costs stubbornly persists. Since Bitcoin is based on a new technology - DLT / Blockchain - it would have a high transformation potential. Firstly, these technologies have so far created limited value for society - no matter how great the expectations for the future. Secondly, the use of a promising technology is not a sufficient condition for an added value of a product based on it.[45]

Alternatives

The uptake of new services generally has a relation to the benefits they offer in comparison with incumbents. This is probably a useful lens to look at Web3 through: where are Web3 services better than current alternatives? Evidence so far suggests that this is often when a very specific business sector community has a strong need for verification of transactions, which warrants investment, expertise and energy expenditure. It suggests considerable scope for Web3 to support more niche communities markets, but not that a single Web3 service is likely to scale in general use as Facebook did, under current conditions. A Web3 solution can work for a collective activity when enough people agree it is the best way to do something, they can see the added value in comparison with alternatives, it is easy enough to use, and involves power relations that are as equitable as possible and transparent, and are able to adapt to change. This appears a different set of factors from the mass network effects and benefits to scale of Web2.

Adoption across sectors and geographically across jurisdictions around the world will likely be partly a function of the adequacy of available alternatives. In China, payment with mobile phones grew much faster than in much of Europe and the USA. In China mobile offered a substantial improvement, whereas in those other countries, most people, most of the time, already found it easy enough to pay for common products and services, and while mobile offered some additional benefits, those were not great enough to drive switching behaviour quickly. Web3 services are likely to move into spaces where currencies, payment services, ease of doing business, freedom from government interference online, trust or verification have specific local failings.

Some alternatives to Web3 applications are emerging, which share the objective of fixing Web2's flaws in relation to control of personal data, but take different routes.

Some emerging models aiming to "achieve what is best about decentralisation: subsidiarity, not redundancy—a network of networks, not a ledger." These are designed to contrast to Web3 "architecture … optimized for a highly narrow set of problems, and thus by its very nature is unable to interface with the rich economic and social networks in which problem-solving coordination is actually needed."[46]

Solid (Social Linked Data), a project led by Sir Tim Berners Lee, aims to give users the means to protect their personal data while using it in interactions with online services. Personal data is stored in Pods (personal online data stores), and users grant permissions with terms for online service applications to access it. The system is supported by standards and data formats, and a wider developer community. [47]
Kieron O'Hara considered Solid in detail in a previous Web Science Trust paper, and outlines the trade-offs its structure will present to users.

> Solid provides the affordances for individuals to get their privacy preferences with respect to that much of their data which is stored on a Solid server.
>
> These affordances provide control: they can choose whether or not a piece of data remains private to them, or confidential to a small circle, and they can choose who can have access and who not. The cost of this control is that individual now have more decisions to take vis-à-vis data. One way of doing this is to take the resource-heavy decision of running their own servers. This is risky in a number of ways, most obviously the server may fail without a commercial backup. Such individuals would also have to be confident that they were able to furnish cutting edge security. More likely, they would delegate these decisions to pod administrators.[48]

To succeed as a viable basis for online social media, such new approaches will need a wider group of service providers that comply with the protocols and terms, and which have business models that are sustainable without the data extraction approach characteristic to Web2. The same questions and trade-offs that Web3 has run up against will be pertinent for any model, including whether the complexity is transparent, proportionate to use of computing and energy, and compatible with usability and scaling. Even success will present new challenges, if it is to avoid the creation of new market power bases and asymmetries.

> We should not forget that solving one political problem (the power asymmetry between individuals and tech companies) and one technical problem (the increasing centralisation of the Web) does not mean that the solution will not be challenged, nor that unintended consequences may not emerge. At present, most political debate takes the form of questioning whether app providers can demand that permissive privacy policies be consented to by users before they get access to services, especially when the providers benefit from large network effects. If and when the Solid ecosystem grows and evolves, it will bring its own network effects, which will doubtless prompt important political questions about inclusion and exclusion.[49]

At the time of writing, there is a relevant parallel in the movement of some users from Twitter to Mastodon. Mastodon's federated form has attractions for users disappointed by Twitter's new leadership and recent trajectory, but using it requires learning and more day-to-day effort, which is reported to deter some from making the switch.

Behind challenges Web3 aims to solve, and behind the reasons it often fails to do that, is the question of funding. Web2 grew a supporting ecosystem of data accumulation for advertising because users grew accustomed to getting services for free, and providers grew accustomed to concealing how they exercised power in markets deriving from accumulating data. Users saw growth driven by popularity and usability, both continually increasing the attraction of the services. Shareholders saw growing advertising revenue exceeding costs to provide services.

These mutually reinforcing network effects came to seem a matter of irresistible evolution, and providers seem to have been content for those, and less welcome side-effects, as unavoidable effects of that evolution, rather than their responsibility. Scaling web platform services was perhaps

always more difficult than it was made to look. This seems to have influenced the hope that Web3 will hit upon similar reinforcing effects, which it so far has not.
There is the possibility that in the future more effective micropayment systems may yet change the range of what is sustainable for users and providers. To make that successfully would require shifts in the expectations of users, en masse.

Conclusion

The history of Web3 demonstrates that it is currently difficult to automate trustworthy and sustainable functions for dispersed communities online. Solutions to one problem tend at least to increase the risk of a different problem emerging at another point in the system.

Given the multiple crises still playing out, it is increasingly remarkable that there continues to be optimism about Web3 in some circles. But belief has always been a feature of Web3, and arguably also a bug.

There are many remaining questions about scalability and robustness of Web3 systems, but there is also a great deal of work and money going into trialling applications and resolving problems. VC investments in Web3 exceeded $18 billion in the first half of 2022, remaining on track to top the full-year total VC investments of
$32.4 billion in 2021.[50] Even high profile failures seem to trigger new corporate enthusiasm. In December 2022, Goldman Sachs was reported to be looking to buy or invest in companies made more commercially attractive by falls in valuations following the collapse of FTX.[51]

If we are not to expect Web3 to become the basis for most interactions over the internet in the foreseeable future, it is reasonable to expect more growth and diversification in niche uses in many sectors and contexts where it offers increased transparency and assurance. Financial services and supply chains (including in pharmaceuticals) are already major application areas, and could increase use further. These applications are not by and large visible to the general public, do not need to be, and neither rely on nor influence wider public embrace of Web3.

Web3 tools offer network effect benefits, but these are not the same as those seen in Web2 platforms. One of the challenges of assessing Web3 in general, is that trust is context-specific. A technical solution may manage trust for a set of users and a set of purposes, but there is little meaning in generalised resolution of trust challenges.

Trust does not easily scale across contexts. Precision tools may not serve expansive aspirations to change society.

The greater the claims that this offers a new and better era of the internet, the less plausible those appear to critics. The more enthusiasts evangelise, the more critics point to the heavy lifting being done by belief. The ambitious mission to remake the internet with these technologies may now be a drag on their acceptance.

Judging rates of development and uptake does depend on what the chosen comparators are. Disappointment is inevitable if Web3 is set up to grow as fast as Facebook did, but the internet more broadly took decades from inception to be used by half the global population.

> Web3 doesn't really exist yet. But evaluating its merit on superabundant bull market ponzis is probably doing it a disservice, the same way ignoring those market dynamics would be dishonest.[52]

Presenting Web3 more soberly as a suite of tools, while certainly less exciting, would make for more lucid discussion. In any case, it may be unreasonable to expect a set of tools for use by multifarious decentralised groups to cohere into an integrated movement, in spite of the efforts of promoters. Using the same digital tools for very different purposes does not constitute a genuinely shared social mission, in spite of attempts to present Web3 as one.

We can hope for better discussions. Claims that new systems are more democratic should be analysed more carefully. Web3 technologies are continuing the tendency to erode distinctions between sectors and functions, that previous digital technologies have shown. This already complicates discussion of them. Vague aspirations and boosterism do not help to credibility or understanding of what value emerging applications might add. Web3 technologies may benefit from not being described as Web3, with all the expectations that creates. It may be better to accept that currently it remains difficult to achieve the scaling and continually improving usability that drove Web2, without winner-takes-all characteristics.

Footnotes

. [1] Max Mersch and Richard Muirhead, What Is Web 3.0 & Why It Matters, 2019 https://medium.com/fabric-ventures/what-is-web-3-0-why-it-matters-934eb07f3d2b

[2] https://ethereum.org/en/web3/ . I have been unable to identify the first use of this description.

[3] Darcy DiNucci, "Fragemented Future", Print Magazine. http://darcyd.com/fragmented_future.pdf

[4] My first impressions of web3, Jan 07, 2022, https://moxie.org/2022/01/07/web3-first-impressions.html

[5] The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Shoshana Zuboff, 2019.

[6] What is Web3? Nader Dabit, 2021, https://www.freecodecamp.org/news/what-is-web3/

[7] https://ethereum.org/en/web3/

[8] The Semantic Web, a new form of Web content that is meaningful to computers will unleash a revolution of new possibilities, by Tim Berners-Lee, James Hendler, Ora Lassila, Scientific American, 2001. https://www.scientificamerican.com/article/the-semantic-web/

[9] Web inventor Tim Berners-Lee: Screw Web3 — my decentralised internet doesn't need blockchain, Thomas Macaulay, TNW, June 2022. https://thenextweb.com/news/web- inventor-tim-berners-lee-screw-web3-my-decentralised-internet-doesnt-need-blockchain

[10] Web3 and the creative industries: How blockchain is reshaping business models, Jason Potts, Ellie Rennie, in A Research Agenda for Creative Industries, 2019. https://researchrepository.rmit.edu.au/esploro/outputs/bookChapter/Web3-and-the-creative-industries-How-blockchain-is-reshaping-business-models/9921970955001341

[11] https://web3summit.lt/

[12] https://cryptocurrencyworks.com/.res/doc/Bitcoin-SNakamoto-Oct-2008.pdf

[13] Who Accepts Bitcoin and Ether Cryptocurrencies, https://www.ceifx.com/news/who-accepts-bitcoin-and-ether-cryptocurrencies

[14] Unique cryptocurrency wallets created on Blockchain.com as of August 22, 2022, Statista https://www.statista.com/statistics/647374/worldwide-blockchain-wallet-users/

[15] https://www.in2013dollars.com/bitcoin-price

[16] 2021 Global Crypto Adoption Index: Worldwide Adoption Jumps Over 880% With P2P Platforms Driving Cryptocurrency Usage in Emerging Markets, https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index/

[17] https://augustafreepress.com/total-number-of-cryptocurrencies-jumped-by-70-in-a-year/

[18] Number of daily transactions on the blockchain in Bitcoin, Ethereum and 13 other cryptocurrencies from January 2017 to November 7, 2021https://www.statista.com/statistics/730838/number-of-daily-cryptocurrency-transactions- by-type/

[19] https://ethereum.org/en/what-is-ethereum .

[20] Blockchain Technology and Decentralised Governance: Is the State Still Necessary? Marcella Atzori, 2015, http://nzz-files-prod.s3-website-eu-west-1.amazonaws.com/files/9/3/1/blockchain+Is+the+State+Still+Necessary_1.18689931.pdf

[21] https://ethereum.org/en/desci/ .

[22] Ants-Review: A Privacy-Oriented Protocol for Incentivized Open Peer Reviews on Ethereum, Bianca Trovò and Nazzareno Massari. https://link.springer.com/chapter/10.1007/978-3-030-71593-9_2

[23] Some Very Simple Economics of Web3 and the Metaverse Paul P. Momatz, 2022 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4085937

[24] Web3 Is Dead. Long Live Web5, Stephen Moore, Medium, June 2022. https://stephenmoore.medium.com/web3-is-dead-long-live-web5-4bc4fb391065

[25] The toughest challenges for cryptocurrency lie ahead, CNBC, July 2022, https://www.cnbc.com/2022/07/12/op-ed-the-toughest-challenges-for-cryptocurrency-lie-ahead.html

[26] The Words of Crypto, glossary, Binance Academy, https://academy.binance.com/en/glossary/rug-pull
[27] https://www.coinopsy.com/dead-coins/

[28] Crypto crisis: how digital currencies went from boom to collapse, Alex Hern and Dan Milmo, The Guardian, June 2022, https://www.theguardian.com/technology/2022/jun/29/crypto-crisis-digital-currencies-boom- collapse-bitcoin-terra

[29] Crypto Is Trying Out Traditional Finance's Failures in Hyperspeed, but It's Going to Be Fine, George Kaloudis, Coindesk, July 2022

https://www.coindesk.com/markets/2022/07/10/crypto-is-trying-out-traditional-finances-failures-in-hyperspeed-but-its-going-to-be-fine/

[30] https://twitter.com/rsynnott/status/431924540294594560
[31] Andres Velasco, The Unbearable Uselessness of Crypto, November 2022. https://www.project-syndicate.org/commentary/ftx-collapse-exposes-cryptocurrencies-uselessness-by- andres-velasco-2022-11

[32] https://stopelon.space/

[33] Crypto Crime in 2022: Everything You Need to Know, Chainalysis, 2022,

https://go.chainalysis.com/2022-crypto-crime-part-1.html

[34] Stephen Diehl, Blog: Why Web3 is Bullshit https://www.stephendiehl.com/blog/web3- bullshit.html

[35] The Truth about Smart Contracts, Jimmy Song, Medium, 2019 https://jimmysong.medium.com/the-truth-about-smart-contracts-ae825271811f

[36] The Decentralised Web: Hope or Hype?, Inga Trauthig, Center for International Governance Innovation, August 2022 https://www.cigionline.org/articles/the-decentralised- web-hope-or-hype/

[37] Marlinspike.

[38] Gary Gensler Isn't Buying Your Decentralisation Theater, By David Z. Morris, August 2021 https://www.coindesk.com/markets/2021/08/19/gary-gensler-isnt-buying-your- decentralisation-theater/

[39] Diehl.

[40] Diehl.

[41] Bitcoin's Last Stand, Ulrich Bindseil and Jürgen Schaaf, November 2022. https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog221130~5301eecd19.en.html

[42] Enrique Dans, You may not have heard of The Merge, but it could change our world, Medium, August 2022.

https://medium.com/enrique-dans/you-may-not-have-heard-of-the-merge-but-it-could-change-our-world-f9f8e97fceda

[43] https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of- digital-assets/

[44] https://www.gov.uk/government/publications/digital-regulation-cooperation-forum-workplan-2022-to-2023
[45] Bindseil and Schaaf.

[46] The Web3 Decentralisation Debate Is Focused on the Wrong Question, Divya Siddarth, Danielle Allen and E. Glen Weyl, Wired May 2022. https://www.wired.com/story/web3- blockchain-decentralisation-governance/

[47] https://solidproject.org/
[48] Privacy, Privacy-Enhancing Technologies & the Individual WST White Paper #1 Kieron O'Hara, 2022. https://eprints.soton.ac.uk/455997/
[49] O'Hara.
[50] Web3 beyond the hype, Anutosh Banerjee, Robert Byrne, Ian De Bode, and Matt Higginson. McKinsey, September 2022 https://www.mckinsey.com/industries/financial- services/our-insights/web3-beyond-the-hype

[51] Goldman Sachs on hunt for bargain crypto firms after FTX fiasco, Iain Withers and Lawrence White, Reuters, 6 December 2022 https://www.reuters.com/technology/goldman- sachs-hunt-bargain-crypto-firms-after-ftx-fiasco-2022-12-06/
[52] WTF is Web3? Cobie, January 2022 https://cobie.substack.com/p/wtf-is-web3