Web3: Democratising the Internet

Aria Babu

Web3: Democratising the Internet

Aria Babu

About the Author

Aria Babu joined Policy Exchange as a Senior Fellow for Technology and AI policy in June 2023. She has worked in Technology policy for several years and is a policy fellow at The Startup Coalition and an adviser at The Entrepreneurs Network, where she was previously Head of Policy. Her background includes work in and outside of policy. She has worked at a biodiversity start-up, organised a conference on progress studies for Civic Future, and worked as an analyst for Public First.

Acknowledgements

The author would like to thank the following individuals who supported and advised this research. Whilst their insights have informed this work, the output is wholly the responsibility of the author and does not necessarily reflect the views of the following individuals or the organisations that they represent.

Contents

Executive Summary

What does the future of the internet look like? In recent years, users have pushed for more control over their data, more privacy, and more freedom. The internet is on the cusp of entering a new era, known as Web3, which addresses these needs and promises to revolutionise our digital lives.

The theory is this: Web1 was the first iteration of the internet and was largely read-only, with blogs, simple webpages, and wikis. It was followed by Web2, or the "read-write" era, which involved three major shifts; easy internet access through widespread fast internet and smartphones, commercialised user-generated content networks, and the dominance of a few big centralised platforms, particularly in social media.

Web3 is the next step in the development of the internet. It aims to make the internet truly decentralised so that no single entity has significant coercive power. This is the "read-write-own" era of the internet. Decentralisation is the key feature of crypto networks, and it will result in several significant benefits for the Internet. First, decentralisation promotes competition because it enables blockchain networks to be credibly neutral and composable, which allows networks to function like public infrastructure, makes them attractive to build businesses upon, and lowers barriers to entry. Second, decentralisation safeguards freedom because it requires control of a network to be broadly distributed among stakeholders, not just the companies that developed the networks. It is important to recognise that blockchain and tokens are integral parts of decentralised Web3, and are symbiotic technologies that cannot be arbitrarily divorced.

There are many examples of interesting and emerging Web3 companies: Farcaster, a social media protocol that allows people to own their data and port it from site to site rather than remain captive to one social media company and its rules; Spruce ID, creating decentralised mobile driving licences for the Californian DMV; and Adimverse, building a network on which groups of writers can collaborate and create stories outside of Hollywood's gatekeeping. In finance, companies like Wirex have changed how we do cross-border payments, allowing people to send remittances for free. Finally, Stellar and Circle have joined forces with the UNHCR and found new and more efficient ways to give people aid in a crisis.

So far, £77 billion has been invested in Web3 projects and startups. And as blockchains like Bitcoin and Ethereum gain traction, they are not only disrupting established Web2 giants, they are being adopted by them. E-commerce titans Shopify and Mercado Libre have enabled crypto payments on their platforms, PayPal now facilitates stablecoin transactions,

and JP Morgan has minted its own cryptocurrency – JPM Coin.

When he was Chancellor of the Exchequer, Prime Minister Rishi Sunak made his goals for Web3 clear. He said "It's my ambition to make the UK a global hub for crypto-asset technology, and the measures we've outlined today will help to ensure firms can invest, innovate and scale up in this country. We want to see the businesses of tomorrow – and the jobs they create – here in the UK, and by regulating effectively we can give them the confidence they need to think and invest long-term. This is part of our plan to ensure the UK financial services industry is always at the forefront of technology and innovation."

This is especially important in the context of increasing regulatory uncertainty coming from the US. Several major firms, such as a16z, Coinbase and Fidelity have already set up operations in the UK. Other companies, for which Web3 is not a pivotal part of their businesses, like Revolut and Gamestop, are shutting down their blockchain applications in the US to avoid the potential ire of regulators.

At this moment the UK has a tremendous opportunity to capitalise on the exodus of Web3 firms leaving the US. Last year, £943 billion of crypto-assets were exchanged in the US. A reasonable estimate suggests that the UK, through the right regulation, could capture about £29 billion of this activity – and this assumes that sensible regulation would not stimulate further growth in the sector, which it is likely to do. As a conservative estimate, this would translate to an extra £10.7 billion of assets and over 36,000 jobs. These are high potential industries that are poised to grow, providing a great number of innovative new companies, consumer goods, high skilled jobs and, of course, taxes.

At the heart of the UK's initial success is our "same risk, same regulatory outcome" approach, which is distinct from a "same risk, same regulation" approach taken in other jurisdictions. It may not be appropriate to apply the same rules, developed for traditional finance, to crypto-asset markets where there is a different landscape of risks, but where the end goal is the same regulatory outcome. Blockchain technology, allows for instant settlement. Transactions are immutable, irreversible, and transparent so there is often no need for the same types of intermediaries that are involved with traditional finance. Further, crypto-assets have utility beyond their speculative value, which makes decentralised blockchain innovation much broader than just financial applications. This can mean that financial regulation could unnecessarily constrain the development of new social media or digital ID applications.

Bespoke regulation is safer for consumers, as it deals with the actual risks posed by blockchain technologies, and will make the UK a "web3 centre" for innovation to flourish in cases where blockchain is a better alternative to traditional technology.

With this principle in mind, we have ten proposals for how the UK can further improve our Web3 regulation and capitalise on the innovative potential for this powerful new technology

Summary of Recommendations

1. HMT's secondary legislation and regulation implementing a new crypto-asset framework should embrace, and set a high bar for, decentralisation to ensure that customers are protected against legacy risks of centralisation and so that innovative projects can issue tokens to appropriately broaden ownership of new networks.

The UK has taken a nuanced, and responsible, approach to regulating Web3 assets. This approach should continue, with HMT and regulators being clear as to when and how projects can achieve sufficient decentralisation so their developed software can freely distribute utility tokens to the public, and under what terms these assets will be regulated.

2. The government, with the help of the Law Commission, should clarify legal protections and liability for DAOs and their members.

Decentralised Autonomous Organisations, known as DAOs, are decentralised organisations created to limitedly manage Web3 protocols that run on blockchains so that those protocols can responsibly evolve while minimising centralised control. Membership of a DAO is usually accounted for through ownership of a token, which often grants voting rights on the DAO's decisions.

A recent court case in the US ruled that any individual American who, at any point, owns or owned tokens in a DAO could be liable for violations the DAO commits.

The UK should take a more balanced approach that recognises the liability of a DAO itself while providing individual members with limited liability.

3. The FCA's risk-based anti-money laundering program requirements should be flexible and fit-for-purpose in order to account for technological and behavioural differences between blockchain transactions and fiat currency transactions and to allow for innovative AML solutions.

Many current anti-money laundering approaches focus on a "Know Your Customer" (KYC) approach. As most blockchain transactions are transparent and immutable – meaning that the customer is usually pseudonymously known, KYC approaches often fail not only to tackle the actual risks that come with blockchain transactions, but also they can exacerbate financial exclusion and lead to unnecessary bureaucracy.

The FCA should allow for the use of alternative and innovative

techniques designed to prevent illicit finance while allowing the technology to operate as intended for users. For example, because most blockchain-based transactions are transparent, compliance departments could incorporate a stronger "Know Your Transaction" approach. In addition, new technologies like digital identities and blockchain analytics tools may be more effective in meeting anti-money laundering goal for certain crypto-asset activities.

4. Regulation should not undermine digital self-hosted wallets.

In the EU and the US, there have been numerous proposals to apply traditional financial rules to self-hosted wallets. Existing traditional finance rules are not appropriate for self-hosted wallets, which are effectively a software service that has no financial relationship with the customer.

Self-hosted wallets (sometimes referred to as "personal wallets") are a core part of Web3 as they allow users to control their own assets and data when interacting with centralised software providers, thus reducing the ability of third parties to collect and store personal identifying information. Because self-hosted wallets are the gateway to Web3, the Government and FCA should support this important new technology.

5. The FCA should require clear disclosures to consumers about which stablecoins are actually "stable."

Fiat-backed stablecoins are crypto-assets where the value of the crypto-asset is pegged to a real currency. For example, USDC is pegged to the US dollar and can be exchanged for dollars at any point.

Some stablecoins hold onto the fiat currency they are given and are quite stable but most invest in assets. Some of these stablecoins are riskier than others. The FCA should adopt regulations that require sufficient transparency to consumers, which will allow them to differentiate the risks associated with the various stablecoin structures.

6. The FCA should not regulate proof-of-stake services as a financial service

Proof-of-stake is a critical part of blockchain technology and is an environmentally friendly alternative to "proof-of-work" or "mining". Retail participants are able to take part in staking as "validators" and often do so by taking up "staking as a service" offered by centralised crypto-asset firms.

In a consultation, the Treasury proposed regulating staking as a "Collective Investment Scheme". This may be a misunderstanding of how basic protocol staking works – it does not involve investment – and if this went ahead it would undermine retail participation in staking and exclude users from the rewards that come with it. Without staking, we risk undermining the proof-of-stake blockchains upon which Web3 is being constructed.

7. HMRC should create a tax wrapper for the exchange of crypto-assets.
Taxation of crypto-assets varies depending on the nature of the transaction. If used for trading purposes (i.e. as part of a trade or business), then any profits are charged as Income Tax. If used as a means of investment then any gains or losses are chargeable to Capital Gains Tax. For many individuals, investment will be the main reason they are exchanging crypto-assets. When one crypto-asset is exchanged for another it creates a "dry tax" charge, one where there is no pound Sterling to enable them to pay for the tax liability. This can create very complex tax returns.

The use of a tax wrapper, with restrictions on its use, would reduce the customer burden and make it easier to be compliant.

8. The Department for Science, Innovation and Technology and the FCA should create a joint sandbox with input from HMRC and HMT.
Regulators often struggle to keep up with cutting edge technology. To remedy this, they sometimes create "regulatory sandboxes". A "sandbox" in this context is a controlled environment where companies can test their products and business models without being subject to the full array of regulatory requirements. This enables both innovation and regulatory insight. This builds on the very successful precedent set by the FCA's Fintech Sandbox. It should be joint with the FCA and DSIT: the FCA has control of most of the relevant regulations, but DSIT's involvement would ensure the sandbox has the power to look beyond financial innovations to other applications that Web3 enables.

9. The Bank of England should promote a flourishing stablecoin market in the UK by allowing stablecoin reserves to be placed at the central bank.
As part of a push to create a diverse payments system, the Bank of England, like most central banks, has plans to create a Central Bank Digital Currency. In addition to this, they should promote a flourishing stablecoin market by allowing stablecoin reserves extra stability, by placing them with the Bank.

10. The government should recruit digital fellows who help the government upgrade public services with cutting-edge technology.
Many UK public services would benefit from being run more automatically and transparently. Blockchain holds significant promise for supply chain tracking, data management, and fast payments. Often the government does not have the expertise to take advantage of frontier technologies. To combat this, the government should recruit Digital Fellows who should be advisors focused on upgrading public services using digital technologies like blockchain and AI.

These roles should be focussed on identifying areas within public services that would benefit from digital transformation. They should be working primarily with procurement and service delivery teams and liaising with external technology providers.

Chapter 1: What is Web3?

The 21st Century is the era of the internet – we now live in a world where digital platforms govern our work, social interactions, commerce and entertainment. The way the internet works has shifted over time. We began with an open-source internet built on a simple software protocol. It was largely for academics and was "read-only" where things from the physical world were posted and interacted with in a vacuum. Then we moved to a community-based internet of networks, a "read-write" era where users could contribute content. Over time, this internet became highly centralised and "gate-kept" where individuals participated through a small number of centrally owned platforms.

The hope is that the next iteration of the internet will be open and decentralised. A "read-write-own" internet where decentralised social media sites like Farcaster are starting to compete with the 2010s behemoths. This transition to a new decentralised era is called Web3.

The Evolution of the Internet

The first iteration of the World Wide Web emerged in 1989 and lasted until the mid-2000s. This internet was based around user-made content and was filled with bulletin boards, forums, blogs, wikis, and file-sharing sites. At this point, the internet was largely decentralised and not commercialised.

This was before widespread high-speed internet. As such, access to the internet was generally limited to desktop computers.

Web2 is the second generation of the internet that emerged in the mid-to-late 00s. Unlike Web1, which was mostly user-generated and decentralised, the Web2 era saw the birth of major social networking sites like Facebook, Twitter, Instagram, and LinkedIn.

As the internet evolved from Web1 to Web2, the economic landscape changed significantly. Initially the change was marked by a series of small sites like LiveJournal and 4chan but over time people moved to larger and more centralised platforms like Facebook, YouTube, and more recently, TikTok.

In the early 00s platforms like LiveJournal and 4chan exemplified the ethos of the early Web2 era. They provided a space for people to find community, but as they were small scale they didn't have the same level of monetisation or commercialisation as we see in later platforms. Their small scale meant that there was no worry about them influencing elections or causing major censorship. Insofar as they were spreading misinformation, the nature of the misinformation was curtailed to small groups so

conspiracies weren't able to spread as quickly. The larger websites started to gain traction as the benefits of their network effects were realised.

During this era more services started to move to the cloud. Instead of downloading and running software on a local machine, users could use software directly from a browser, with data stored on servers across the internet.

This has come with problems and benefits. Centralisation brings convenience. Your friends are all on Facebook or Instagram (depending on how old you are), it is easier to have one dating app where all the eligible singles in your area are than to have them dispersed over several, and it was certainly easier to keep up with the news when Twitter was the one place where opinion-formers were. But centralisation comes with central control, and depending on your precise politics you may have been outraged by the choices made by the companies that govern significant aspects of our online life.

YouTube, owned by Google, has faced criticism for its policies regarding the demonetisation of LGBT content as it is deemed "not advertiser-friendly". In January 2021, Amazon Web Services (AWS) suspended web hosting services for Parler, a social networking site popular among conservative and right-wing groups, citing a failure to moderate violent content relating to the storming of the U.S. Capitol. In 2022, PayPal came under fire for censorship. It started with them withdrawing services for conspiracy theories like 5G masts causing Covid but moved into areas that were genuinely under debate like the costs of lockdown policies and whether the virus was caused by a lab leak. The controversy culminated in September when Paypal withdrew services from the Free Speech Union and was only reinstated after an outcry from MPs.[1]

These concerns about dominant behaviour (from corporations and governments), privacy issues, and the homogenisation of online spaces are part of the motivation for the envisioned transition to Web3. The goal is an evolution towards a more democratised and user-centric model. Web3 promises an internet built on decentralisation, where users can regain control over their data, their identities, and their digital interactions.

The Rise of Web3

The world first caught a glimpse of decentralised Web3 systems in 2008 with the introduction of Bitcoin. Bitcoin was first developed by an anonymous person or entity known as Satoshi Nakamoto. In the wake of the financial crisis, Bitcoin captured the imagination of a great number of people who saw the decentralised, peer-to-peer, and entirely electronic cash system as a challenge to conventional finance. While it allowed people to transact without any need for intermediaries, the early days of Bitcoin were filled with scams and rapid price fluctuations which meant that some made a fortune while others lost a lot of money.

Ethereum, which was introduced in 2015 by young programmers including Vitalik Buterin and Gavin Wood, expanded blockchain's horizons. Unlike Bitcoin, Ethereum offers a platform for developers

1. https://www.telegraph.co.uk/politics/2022/09/27/paypal-reinstates-free-speech-union-accounts-accused-politically/

to create decentralised applications using smart contracts. These self-executing contracts have the terms of agreement written directly into the code, promising automated and trustworthy transactions.

Ethereum's innovation wasn't just a technological advancement but also allowed people to imagine a decentralised internet where users have control of their data, transactions and online data.

The potential of Web3 has not gone unnoticed. To date, about £77 billion has been invested in Web3 projects and startups.[2]

As the usage of crypto-assets has increased, we now see a number of mainstream Web2 organisations adopting Web3 technologies. Shopify[3] and Mercado Libre,[4] both e-commerce giants now allow users to pay with crypto-assets. Paypal allows you to do stablecoin transactions[5] and JP Morgan has created its own coin called JPM Coin.[6] Currently 87 countries, representing 90% of global GDP, are exploring Central Bank Digital Currencies.[7] While crypto-assets are still often used for financial services, there are now mainstream adopters beyond that too. Luxury fashion brands like Dolce and Gabbana and Gucci have released NFTs.[8]

Traditional financial transactions often have to go through several intermediaries, and, while companies like Stripe have managed to reduce the friction of online payments, they are fundamentally finding efficiencies in a system that was not built for the internet. Decentralised finance, on the other hand, is an internet-native payment system, so it is no surprise that incumbents who wish to stay on the cutting edge, like PayPal, are exploring decentralised finance applications. Because the internet and smartphones have spread to the developing world faster than robust financial institutions, crypto-assets are becoming an ever more popular way to send remittances.

However, recently venture capital interest in Web3 has started to diminish.

2. https://www.bain.com/insights/web3-re-mains-highly-relevant-global-private-eq-uity-report-2023/#:~:text=The%20emerging%20web3%20ecosystem%20now,-investors%20(see%20Figure%201).

3. https://www.coindesk.com/tech/2023/08/23/shopify-custom-ers-can-now-pay-in-usdc-via-sola-na-pay/#:~:text=Shopify%20customers%20can%20now%20pay%20in%20stable-coin%20USD%20Coin%20(USDC,and%20-USDC's%20benefits%20for%20merchants.

4. https://www.cryptopolitan.com/circle-part-ners-mercado-libre-usdc-chile/#:~:tex-t=The%20introduction%20of%20USD%20Coin,pegged%20to%20the%20U.S.%20dollar.

5. https://www.paypal.com/us/digital-wallet/manage-money/crypto/pyusd
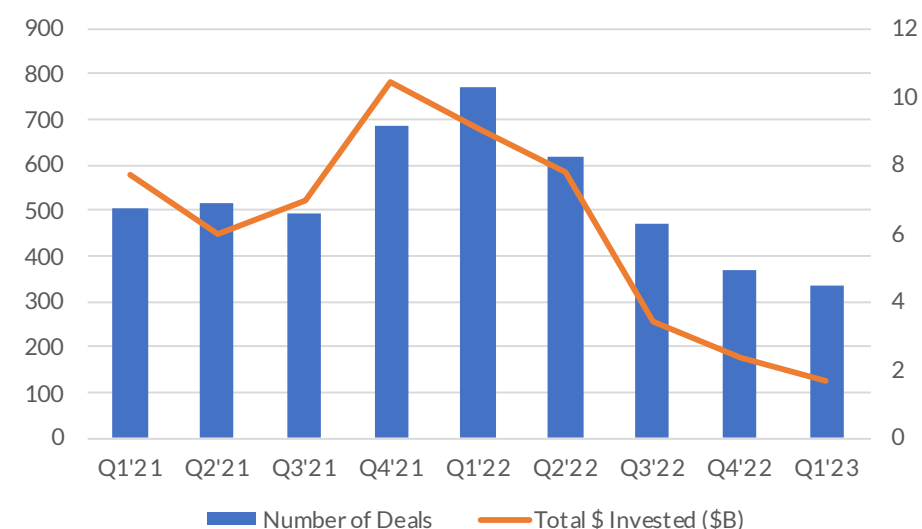
6. https://www.jpmorgan.com/onyx/coin-sys-tem.htm

7. https://www.mckinsey.com/featured-in-sights/mckinsey-explainers/what-is-cen-tral-bank-digital-currency-cbdc

8. https://assets.ctfassets.net/c5bd0wq-jc7v0/6ZxyPKS945KFnSVH0vPEuW/e7fb242895b1919581993d18db876738/The_State_of_Crypto_-_Corporate_Adop-tion_-_Coinbase.pdf

Funding to VC-Backed Web3 Startups by Quarter

This downturn could be attributed to a variety of factors. For one, the US has started to take a more hostile approach to crypto-assets and so the regulatory landscape for Web3 is looking more unwelcoming. While many will pivot to other jurisdictions, it is no surprise that this has resulted in a chilling effect in amounts of investment.

This is also partially due to other factors in the market. Much of VC activity in recent years has been dubbed a "low interest rate phenomenon", where there was a lot of capital chasing some low-expected value investments. In the past year, VC funding has started to decrease and general start-up valuations have gone down. The fall in investment may just be a natural market correction after a period of intense growth.

After the dot-com crash of 2001, many thought that internet businesses were a lost cause – but periods of retrenchment can sometimes herald future advancements. A tighter investment climate could force startups to rigorously validate their business models, and, while overall deal volume has decreased, we expect that high-quality projects will continue to find backing.

Global Venture Dollar Volume Through Q1 2023[9]
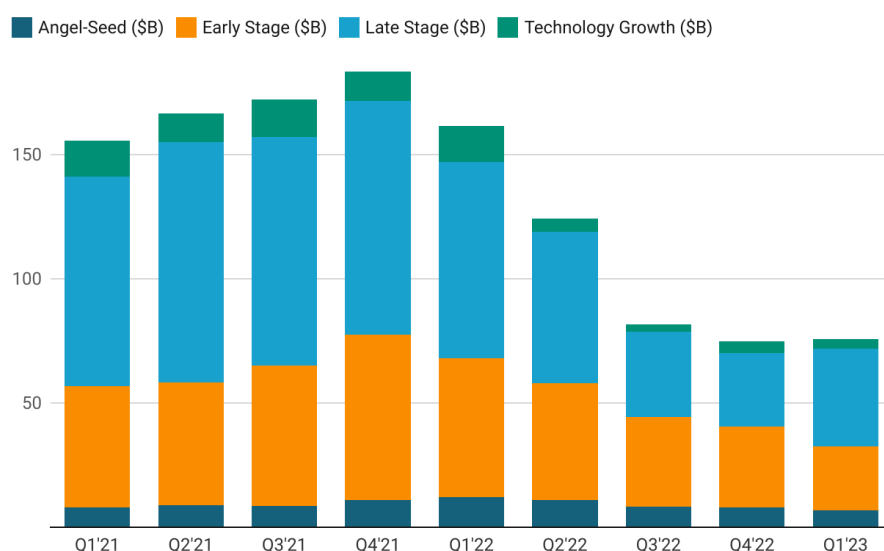
There has been a general reduction in venture capital investment, but it is worth stressing that the drop in Web3 has been much more significant. Overall VC investment has fallen to 48% of what it was last year, but the sharp drop to just 18% in the Web3 domain suggests a more pronounced loss of confidence.

Despite the decrease in funding, the number of people building Web3 applications has continued to grow.

9. https://news.crunchbase.com/venture/glob-al-vc-funding-falls-q1-2023/

Unique Ethereum Addresses Cross 230M+[10]
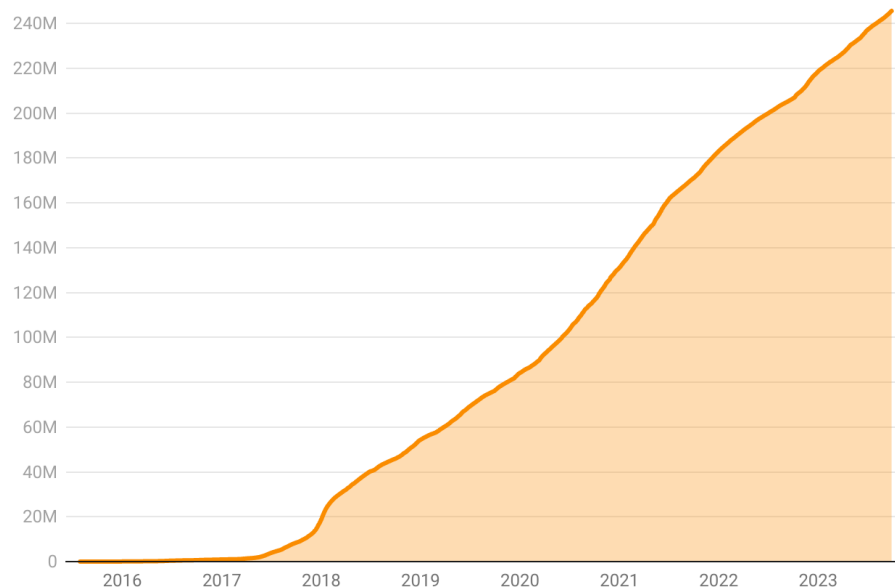
So has the number of active developers.

Monthly active developers (all)[11]

Sources: Electric Capital
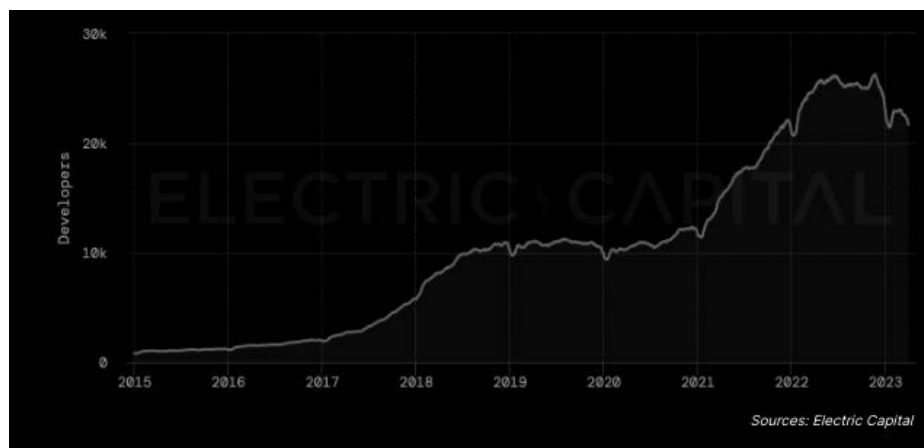
What is interesting about this trend is the growth in Layer 2 solutions.

10. https://etherscan.io/chart/address
11. https://www.developerreport.com/

Daily Transactions on L2S Surpass Ethereum[12]

Sources: L2Beat
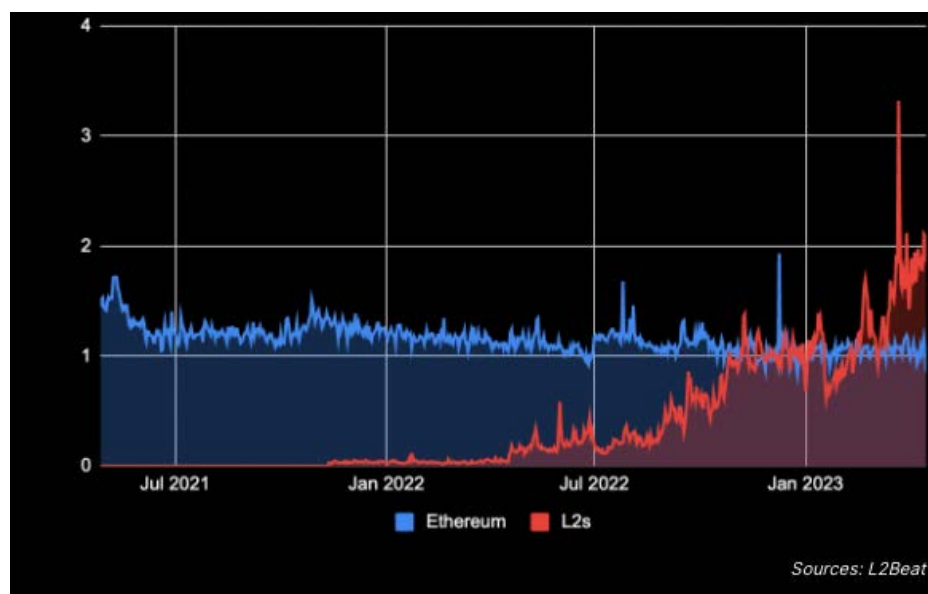
Layer 2 solutions are secondary frameworks created atop an existing blockchain (which is referred to as Layer 1). The primary purpose of these Layer 2 solutions is to offload transactions from the main blockchain. By doing so, Layer 2 solutions aim to improve the scalability and efficiency of the main blockchain, making it more suitable for widespread adoption by lowering costs and increasing throughput.

This growth indicates that users are actively seeking more efficient and cost-effective ways to transact. It shows that existing Layer 2 solutions are seen as trustworthy and robust, and innovation continues in this area.

Web3 in the UK today

According to a 2021 survey by HMRC, 10% of British adults currently hold or have held crypto-assets. They are disproportionately young (76% of them are under 45, compared with 57% of the general population) and the majority (69%) of them are male.[13]

Their reasons for holding crypto-assets are diverse. Most users see it as a fun investment (52%) or they are interested in the underlying technology (36%) while a small set of the users consider it to be a core part of their investment portfolio (19%) or as a means of buying goods and services (18%).

12. https://l2beat.com/scaling/activity
13. https://www.gov.uk/government/publica-tions/individuals-holding-cryptoassets-up-take-and-understanding

Reason for holding Crypto

Fun Investment	52
Interested in underlying technology	36
Core part of my investment portfolio	19
To buy goods and services	18
To gamble	8
Other	4
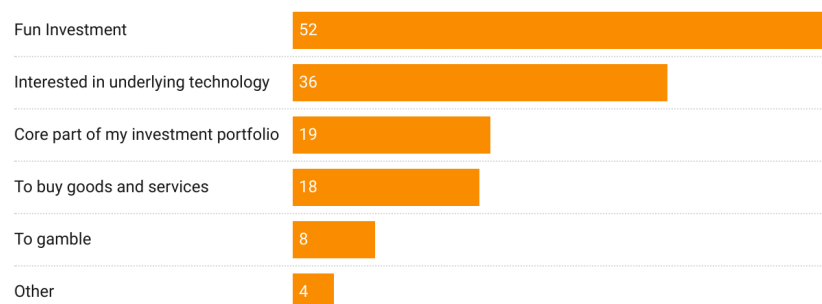
People acquire crypto-assets through a wide variety of means too.

How Crypto was acquired

Centralised exchange	68
Peer-to-peer site	11
Minin	11
Receive them as a gift	9
Decentralised exchange	8
Intitial coin offering	6
Friends, family or colleagues	6
Payment for goods or services	4
Other	4
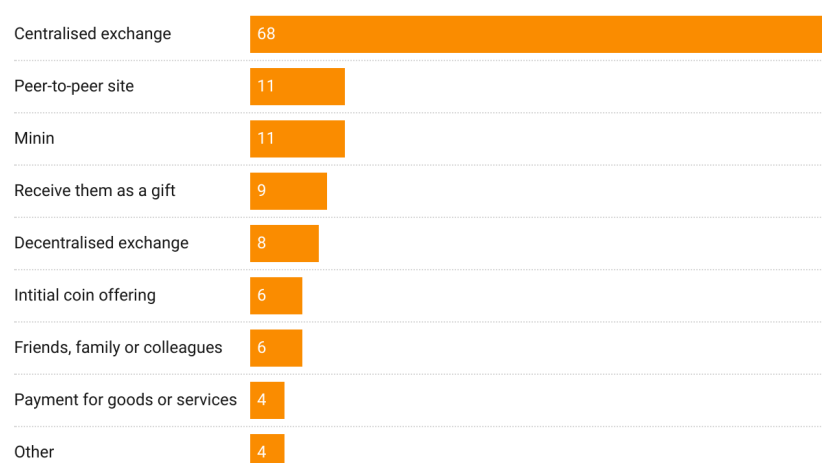
While centralised exchanges are the most frequently used medium (68% report acquiring their crypto assets that way), assets are also acquired through peer-to-peer sites (11%), mining (11%) and decentralised exchanges (6%).

Web3: The Core Technologies, Principles, and Terms

Web3 harnesses the potential of decentralised technologies. Below are some of the key themes and concepts.

Decentralisation

Decentralisation is a broad term that refers to the degree to which power and control over a network is distributed across a large base of independent human actors.[14] The term can also refer to the degree to which there are central points of failure in a network, i.e., technical decentralisation.

Decentralisation exists on a spectrum, and users should assess the extent to which a blockchain network is decentralised. First, whether information regarding the blockchain's operation is transparent. Second, whether the protocol is composed of open-source code that prevents a single person or group from amending or reversing transactions executed and recorded on the blockchain and that no person can materially alter or disable the primary purpose of the code. Third, whether public participants have the

14. Ali Yahya, *The Four Horsemen of Centralization*, Andreessen Horowitz (Dec. 16, 2018), *available* here.

ability to access the protocol and execute digital asset transactions through it in accordance with predetermined, non-discretionary automated rules and algorithms. A blockchain that embodies all of these factors is likely "sufficiently" decentralised.

Decentralisation is a key feature of Web3 and will result in significant benefits to the internet. It promotes competition because it enables blockchain networks to be credibly neutral and composable, which allows networks to function like public infrastructure and it safeguards freedom, because it requires control of a network to be broadly distributed among stakeholders, not just the companies that developed the networks. This reduces people's ability to gatekeep and censor.

Blockchain

Blockchain is a type of distributed ledger technology. The "block" refers to a chunk of digital information and the "chain" to the sequence of blocks recorded over time. The chain is itself a public database.

The key components of the block are the data, the hash, and the hash of the previous block. The data contained in the block will depend on what the specific blockchain is being used for. For example, in Bitcoin the data includes information about how much coin is being sent, who is sending it, and to whom it is being sent.

Every block has a unique bit of code called a hash. It also contains the hash of the previous block. The hashes are created using cryptographic algorithms and it changes if the information inside the block is modified. A cryptographic algorithm, often referred to as a cipher, is a method of encrypting and decrypting information. These algorithms are essential for secure communication and are used across internet transactions and data storage. This is the technology that makes blockchain so secure. If someone tries to tamper with the data inside a block, the hash of the block will change as well. As each block also contains the hash of the previous block, this would invalidate all the hashes of all the following blocks of the chain, thus alerting the system to an attempted tamper.

Blockchains are distributed. What this means is that when a block is added to the blockchain the information it contains becomes public and is distributed across a network of computers, known as nodes. This is why it is almost impossible to alter past blocks, as a majority of the nodes would need to agree on the change.

Smart Contracts

A smart contract is a self-executing computer program, analogous to a contract with the terms of the agreement written directly into the code. It is another foundational element of blockchain technology.

In more traditional contracts, terms are agreed upon by multiple parties and the contract is then enforced by some trusted external party, like a court system. In a smart contract, as the terms are coded into the contract itself, when certain conditions are met, the contract executes automatically.

For example, in a standard contract, if you and a stranger were to bet on the outcome of a football match, you would need a third party to mediate. And if they failed to pay-up, you would have to appeal to some authority to enforce the bet. In a smart contract, the outcome and the stakes would be encoded into the contract. You could link it to real-time results of the match so, when the match concludes, the winnings are automatically paid out to the winner.

Smart contracts simplify and automate many processes by removing the need for intermediaries in direct peer-to-peer interactions.

Decentralised Finance (DeFi)

DeFi is the umbrella term used for a variety of financial applications that use blockchain technology. Using smart contracts, DeFi cuts out intermediaries. By bypassing human gatekeepers, DeFi is able to offer financial platforms and products with more automation, speed, trust, and privacy, and without the need for traditional financial intermediaries.

Proof-of-work

Proof-of-work is a consensus algorithm used in many blockchain networks, including Bitcoin. It is the mechanism that allows the participants in the network to agree on the state of distributed ledger.

In proof-of-work systems, miners must solve a complex mathematical puzzle. This puzzle requires finding a value that, when hashed with the transaction data, produces a hash that meets specific criteria. Solving this puzzle requires an enormous amount of computational power and energy because the only way to find the correct value is through brute-force guessing.

Once a miner successfully solves the puzzle, they broadcast the solution to the rest of the network. Other participants can quickly verify the solution by hashing the proposed value with the transaction data to see if it meets the criteria. When the solution is verified, the miner adds the new block of transactions to the blockchain and then is rewarded with a newly minted unit of currency, and depending on the blockchain, some transaction fees.

The "work" in proof-of-work serves two main purposes. First, security. The computational difficulty of the puzzle makes it prohibitively expensive for an attacker to alter the blockchain. An attacker would need to out-compute the rest of the network to alter past transactions.

Second, the "work" provides a floor for the value of the asset mined. The value of the asset will be at least equal to the value of the energy, the amortised cost of investment, and the risk of mining the asset.

Proof-of-work consensus mechanisms have been criticised for the amount of energy that goes into "mining" new cryptocurrencies. This is a feature of proof-of-work, not a bug. The amount of compute required means that it would be prohibitively expensive to overwhelm the consensus process and add a false transaction to the blockchain, thus strengthening the blockchain's security.

Proof-of-stake

Proof-of-stake is another consensus algorithm that blockchain networks use, designed as an alternative to proof-of-work to achieve distributed consensus with vastly lower energy consumption (about 10,000 times less[15]).

There are many variations of proof-of-stake, each with its own design and mechanisms. But generally, in a proof-of-stake system, validators (the equivalent of miners in proof-of-work) are chosen to create new blocks based on the number of coins they "stake", or pledge, to the network. Unlike in proof-of-work, where miners must compete to solve a mathematical problem, proof-of-stake selects validators to create new blocks based on their stake. As participants stake more, their chance of being chosen as a validator scales proportionally. Some proof-of-stake systems may also take into account other factors, such as how long the users have staked their coins.

The chosen validator then creates the new block, fills it with transactions, and adds it to the blockchain. They are then typically rewarded for their service to the network with newly minted coins, transaction fees or both.

Certain proof-of-stake blockchains also include mechanisms to punish dishonest validators. If a validator is found to be acting maliciously, some of its staked coins may be forfeited.

Proof-of-stake achieves consensus without relying on the extensive computational work required in proof-of-work. As a result it is often thought of as the environmentally friendly option.

There are many variations of proof-of-stake, each with its own design and mechanisms. The most famous example is Ethereum 2.0.

Ethereum 2.0

Ethereum is the largest and most well-established, open-ended decentralised blockchain platform. Ethereum offers developers a flexible and robust foundation for decentralised applications, including smart contracts, games, and decentralised finance.

Ether (ETH) is Ethereum's native cryptocurrency and is used to cover transaction fees and computational services. After Bitcoin, it is the largest cryptocurrency by market cap.

The Ethereum Virtual Machine is a runtime environment for smart contracts and standardises execution across the network.

The ERC-20 (short for Ethereum Request for Comment 20) is a technical standard used for smart contracts on the Ethereum blockchain. It defines a common interface for developers to use, giving them the ability to program how new tokens will function within the Ethereum ecosystem. Tokens that adhere to the ERC-20 standard are easily interchangeable and can work with decentralised applications and smart contracts that also comply with the standard. The ERC-20 has thus facilitated the growth of interoperable applications on the Ethereum network.

The original Ethereum used a proof-of-work consensus mechanism like Bitcoin. In September 2022, the Ethereum network shifted over to proof-

15. https://ethereum.org/en/energy-consumption/

of-stake, reducing Ethereum's energy consumption by about 99.95%.[16]

When Ethereum has completed its shift over to Ethereum 2.0 it will have created 64 shard chains, meaning that instead of having a single chain where all transactions are processed in sequence, the blockchain is divided into smaller parallel chains, which increases both the volume and speed of transactions.[17]

Ethereum enables developers to build services around blockchain, smart contracts and tokens. These services include a wide range of applications beyond financial services like gaming, social media, and supply chain tracing.

Layer 2 Solutions

A Layer 2 solution is a secondary framework or protocol that is built on top of an existing blockchain. They are built to solve some of the limitations of the main blockchain, often called the Layer 1, by handling transactions off the main chain or improving the efficiency in some other way. This is usually relevant for solving issues related to speed, scalability, and transaction fees. Sometimes they offer "child" blockchains that operate independently and take some of the workload off the main chain.

Because Layer 2s reduce the load on the main chain, the network can process a greater number of transactions per second while substantially reducing costs for users. They can also offer stronger privacy or security guarantees.

Stablecoins

A stablecoin is a type of cryptocurrency that is designed to have a stable value with respect to some other asset (or, in some cases, with respect to itself) – as opposed to the more volatile nature of other crypto-assets. The stability is usually achieved by pegging the stablecoin's value to a reserve of assets, such as a specific fiat currency like the US dollar, precious metals, or a basket of other assets, which sometimes include other cryptocurrencies.

Most stablecoins are pegged to fiat currencies like the US dollar or the Euro. For some reserve-backed stablecoins there is an equivalent amount of that fiat currency held in reserve by a trusted entity which acts as collateral to ensure the value of the stablecoin.

Crypto-collateralised stablecoins are backed by other stablecoins, and they are maintained through complex algorithms and smart contracts that adjust the collateral to keep the stablecoin's value consistent. Algorithmic stablecoins are not backed up by any collateral but use algorithms and smart contracts to automatically regulate the stablecoin's supply, increasing or decreasing it to maintain the pegged value.

Stablecoins are useful because they provide a stable asset that users can send or trade on blockchains. This is why they are so popular in remittances or payments, where users typically prefer assets that hold a consistent value over a period of time. They also serve as a bridge between traditional fiat currencies and the world of decentralised finance.

Stablecoins provide significant mutual value for the people using them

16. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

17. https://cointelegraph.com/learn/ethereum-upgrades-a-beginners-guide-to-eth-2-0

and the people issuing them. The people using them have a cheap digital currency that is stable, more efficient for online transactions, and as valuable as the fiat currency backing it. The issuer receives fiat currencies that can be used to generate returns, provided the issuer is sufficiently liquid to redeem requests from users seeking to cash out.

Decentralised Autonomous Organisations (DAOs)

A DAO is an organisational model that is run and managed by smart contracts instead of people. Decisions are made electronically through written computer code or through a vote of its members. Each DAO generally has different rules that govern how it works, and usually members of the DAO hold tokens that represent voting rights within the organisation. The weight of a member's vote is usually tied to how many tokens they hold.

All of the rules, transactions, and token holdings are recorded on the blockchain, providing complete transparency to all members.

As DAOs are a relatively new and innovative structure, they face legal and regulatory challenges. Some DAOs are charitable or investment funds, where members vote on how to disburse funds, and sometimes they are various types of artistic projects. They are generally used for organisations which wish to have more democratic and transparent forms of governance, or indeed for teams looking to raise something akin to equity capital without relying on traditional financing structures.

Tokens

Tokens are a type of digital asset that can be bought, sold, or traded. They often exist on blockchain. Essentially, they represent ownership over their utility and have value.

Utility tokens give the holder access to a specific product or service within the blockchain ecosystem. For example, a token might represent membership of a DAO, give the holder access to a specific product, like computing power on a decentralised network, or represent ownership of an external asset.

Non-fungible tokens (NFTs), are a type of token but each is unique and cannot be exchanged on a one-to-one basis with another token.

Crypto-assets

A crypto-asset is a digital or virtual asset that exists on a blockchain or distributed ledger. Cryptocurrencies, tokens, stablecoins, and NFTs are all crypto-assets.

Wallets

A wallet is a digital tool that allows users to store, manage, and transact with their crypto-assets. To do this, the wallet generates and stores a pair of cryptographic keys: a public key which operates somewhat like an email address that other people can see and send funds or messages to and a private key which is known to the wallet owner and is used to sign

transactions and access funds.

Wallets can be stored on computers, in smartphone apps, and on USB sticks. Some wallets require multiple private keys to authorise a transaction.

Digital Self Hosted Wallets

A self-hosted wallet is a wallet that is under the control of the individual user – i.e. the wallet owner controls the private keys to their crypto – as opposed to a wallet that is managed by third parties like a crypto exchange or hosted (or custodial) wallet provider.

With self-hosted wallets, users can engage in peer-to-peer transactions without needing any intermediaries.

The heart of Web3 is blockchain technology, which could have profound implications for decentralisation, ownership and autonomy. Rather than our digital identities being subject to the whims of a few large and powerful institutions, Web3 could engender a shift towards individual sovereignty.

Importantly, people will have more freedom to decide which communities they want to be part of. If you can move your digital identity seamlessly from one social media site to another, or from one banking service to another, you will be less constrained by the rules that govern them.

Web3 has interoperability baked in. Protocols like Ethereum allow anyone to plug into the applications built anywhere on the network and popular token standards like ERC-20 or ERC-721 come with a predetermined set of mutually agreed rules for token creation and interactions. As multiple blockchains have come into existence, solutions have been built to facilitate communication between them. This is potentially the key benefit of Web3 technology. For financial technology this means cheap payments but in other use cases, like Web3 social media, it allows users to port their accounts and information.

Furthermore, Web3 promises an expansion of economic participation. DeFi has the potential to remove traditional barriers to economic inclusion and establish a global economic platform with opportunities not dictated by geography or traditional financial gatekeepers. Companies like Wirex and Stellar provide people with low cost ways of making bank transfers internationally.

Web3 allows for greater automation. Much of the modern world relies on spreadsheets being manually checked and maintained. Self-executing smart contracts automatically execute actions which in DeFi effectively and cheaply performs financial transactions for its users and in DAOs allows for sophisticated ownership structures.

That said, every promising technology carries its own set of challenges and risks. Web3 is no exception. There are questions about how to maintain the rule of law, privacy, and how to ensure fairness of access. Nevertheless, Web3 holds enormous potential for reshaping our digital landscape. It is an embodiment of a grassroots, civic revolution where rules are organically formulated by the collective.

Chapter 2: Why does crypto have a bad reputation?

Web3 and the larger realm of cryptocurrencies have, despite their transformative potential, found themselves amidst controversies and have thus been tainted by a variety of negative perceptions. There are three main areas of concern: the association with illegal activities, the environmental impact of blockchain technologies, and the perceived uselessness of Web3 applications.

However, it is vital to recognise that these aspects do not define the whole narrative of Web3 – just as a knife can be used to cook a meal or draw blood, these technologies can be harnessed for good and bad. There are a great number of lawful users and legitimate businesses that implement blockchain solutions to make more transparent, efficient, and secure operations.

Webs 1 and 2 can be used as an analogy here. Initially the internet was dismissed as a playground for hobbyists and criminals but has now become a critical part of daily life, driving innovation, commerce, and global connectivity. Its potential for misuse, like enabling people to buy drugs through the dark web, do not outweigh its broader benefits.

Illegal Use

For most people, who are not actively engaged with cutting edge digital technologies, they will have thought little about crypto-assets. Three quarters of the general public say they don't understand crypto and a majority of those who don't understand it say that it "cannot be trusted."[18]

The sense that crypto-assets are untrustworthy and associated with crime is muddled, but there are three main things that are salient to the public. The first is the allegation that cryptocurrencies are mostly used to buy drugs and commit fraud, the second is awareness that a major crypto exchange has been prosecuted for *something*, and the third is that crypto is used to undermine authoritarian regimes.

In its earliest years, crypto, with its inherent pseudonymity, gained a reputation as a medium for illicit transitions, notably exemplified by infamous dark web platforms like *The Silk Road* where users traded Bitcoin for drugs and other illegal goods and services. It has also been used as a form of payment in ransomware campaigns[19] and, to a lesser extent, terrorist financing.[20]

Some have argued that the pseudonymous nature of crypto can present an attractive medium for money laundering, where illicit gains are

18. https://yougov.co.uk/economy/articles/31657-how-do-britons-view-cryptocurrencies?redirect_from=%2Ftopics%2Ffinance%2Farticles-reports%2F2020%2F08%2F28%2Fhow-do-britons-view-cryptocurrencies

19. https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks

20. https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

disguised by merging them with legal funds. Small crypto-asset markets are vulnerable to manipulative and illegal practices such as wash trading where a trader, or group of traders, will collude to feed misleading information into a market to bid up the value of a token.

It is true that there have been occasions where crypto has been used for criminal activities. Any method of value transfer can be used to pay for illegal activities and commit fraud, including crypto. But, even the U.S. Treasury Department's 2022 National Money Laundering Risk Assessment reported that crypto is far from money launderers' primary tool for the job, finding that, although crypto's use in illicit finance has been increasing over time, its use for money laundering is still "far below that of fiat currency and more traditional methods."[21]

The FTX scandal, notorious for being "one of the biggest frauds in American history" has fuelled the perception of crypto's illegitimacy.[22]

This fraud, while significant, was not unique to crypto but reflects the risks found in traditional business – from rogue traders to scandals like Enron – and the big players will likely face jail sentences.

However, there is an extent to which crypto's ability to resist centralised control is a feature, not a bug. Not all countries have free and democratic legal systems. Crypto can provide a valuable tool in resisting the constraints of oppressive regimes, such as in Venezuela, Russia, or China.

Stablecoins, with USDC and Tether leading the pack, have evolved as a key mechanism for skirting China's capital controls. In theory, China's rules state that citizens can only export $50,000 (£41,000) a year. This fact, however, would likely surprise anyone familiar with the real estate markets of global cities like London and Vancouver, where Chinese investment is apparent.

While there are numerous illicit methods for Chinese nationals to move money out of their homeland, stablecoins have emerged as a popular method. Illegal over-the-counter trading hubs, operating in both mainland China and Hong Kong, provide an exchange point where Chinese yuan can be traded for Tether. Tether can then travel within the crypto network until they are converted into the target foreign currency and safely stashed in banks outside of China.

Cryptocurrency has also been used to raise money for opposition to Russian President Vladimir Putin. Alexei Navalny, who planned to run against Putin in 2018 (before being barred from running), raised some of his funding from Bitcoin. Other Russian activists have similarly been able to raise funds this way.[23]

What is also often underrated is crypto's value in fighting crime. Transactions on blockchains are usually permanent, immutable, and transparent, and this can make it easier for law enforcement to catch criminals and recover the proceeds of crime. In 2020, $1 billion (£820 million) of bitcoin was seized from the Silk Road.[24] HMRC have seized three NFTs on suspicion of £1.4 million fraud.[25]

As mentioned in the previous chapter, Bitcoin is recorded on a decentralised ledger that records every single transaction on a publicly

21. https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

22. https://www.theguardian.com/business/video/2022/dec/13/one-of-the-biggest-financial-frauds-in-us-history-ftx-founder-sam-bankman-fried-charged-video

23. https://www.coindesk.com/policy/2020/07/15/russian-activists-use-bitcoin-and-the-kremlin-doesnt-like-it/

24. https://www.theguardian.com/technology/2020/nov/06/us-seizes-1bn-in-bitcoin-linked-to-silk-road-site

25. https://www.bbc.co.uk/news/business-60369879

available ledger and cannot be altered or deleted. This permanent record provides an invaluable resource for tracing the flow of funds. In the case of the Silk Road, the Department of Justice was able to identify a culpable figure, based on a small transaction made in 2015, and the authorities were able to track the subsequent movement of funds to different wallets controlled by the same person. Similarly, blockchain analytics were used to convict scam artists[26] and to bring down the biggest child abuse website online.[27]

Blockchain analytics firms like Chainalysis specialise in understanding transaction patterns within the blockchain. Their analysis has helped governments and private sector entities identify and disrupt numerous illicit cases. They have shown that even when transactions seem obscured or disconnected, advanced analytical tools can reveal hidden links and patterns.

Now that some degree of regulation has started to take place, crypto transactions are becoming more legitimate. International regulations such as the 5th Money Laundering Directive (MLD5), which are being implemented in the UK and elsewhere, are making it harder to use crypto-asset for illicit purposes. Requirements under MLD5 have made it standard for crypto exchanges to do anti-money laundering checks where they verify the identity of customers and monitor transactions of high-risk customers as a bank would.

In the UK agencies have been able to disrupt illicit activity with law enforcement agencies having successfully seized cryptoassets. The Police reported a number of seizures including one for £180 million.[28] Over the last couple of years the Home Office has been increasing the operational and legal capacity to tackle the illicit use of crypto-assets. However, this has not been without some challenges. The Economic Crime and Corporate Transparency Bill will amend the Proceeds of Crime Act (POCA) to increase the legal capabilities of law enforcement agencies to seize and forfeit crypto-assets including bringing crypto-assets within civil forfeitures rather than requiring a criminal offence.[29] Challenges may still arise as seizure requires access to the private key if it is held by the owner. However, according to figures produced by Action Fraud, crypto-asset related scams continue to increase[30] and the police have increased their capabilities, during a hearing for the Economic bill it was acknowledged that there are "officers in every force in every regional organised crime unit trained and equipped" to investigate and seize crypto-assets.[31]

The question is whether the illicit finance taint on crypto is significant enough to disavow the technology as a whole, or whether this is an early adopter phenomenon which will diminish as Web3's use cases become more developed and widely accessible. In this context, it is important to note that as reasonable regulatory frameworks are put in place, illicit activity will diminish as legitimate users and activities will be more easily differentiated from bad actors and illegal schemes.

26. https://www.nytimes.com/2023/04/22/business/crypto-blockchain-tracking-chainalysis.html

27. https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/

28. https://www.theguardian.com/technology/2021/jul/13/met-police-bitcoin-money-laundering-cryptocurrency

29. https://bills.parliament.uk/bills/3339

30. https://www.ft.com/content/88602223-004b-4e27-b9eb-c45e1f850f9f

31. https://www.coindesk.com/policy/2022/10/26/uk-police-has-crypto-experts-stationed-nationwide/

Environmental Concerns

Some cryptocurrencies require vast amounts of computational power and, by extension, energy. "Mining" is a process where powerful computers compete to solve mathematical problems. This operation, known as proof-of-work, validates transactions and adds them to the blockchain, which is a public ledger containing all transaction data from anyone who uses the currency. The transactions are grouped together in blocks and miners who solve the maths problem earn the right to add a new block to the blockchain and are rewarded with some tokens.

The proof-of-work method requires substantial computational power, and hence, energy. Miners often use specialised hardware known as Application-Specific Integrated Circuits (ASICs) designed to solve these problems as efficiently as possible, but this is a competitive process and the more computational power a miner has, the higher their chances are of winning the race to validate a new block.

This is where the environmental impact comes into play. The energy consumption of mining operations are immense. The Cambridge Centre for Alternative Finance estimated that Bitcoin's annual electricity consumption, as of July 2021, was larger than that of some countries, including Argentina and the Netherlands.[32]

The problem is compounded when the energy used in mining is sourced from fossil fuels. In many cases, miners are located in regions where electricity is less expensive, which often means places with abundant coal-fired power plants, like China's Inner Mongolia or certain regions in the US. If the electricity used in these mining operations comes from non-renewable sources, the carbon footprint of each transaction is significant.

However, while Bitcoin is known for its energy-intensive mining process, not all blockchain technologies are as costly. Blockchains that are used for applications like the creative arts and social media (more on these examples in the next chapter) often use much more energy efficient consensus mechanisms, like proof-of-stake. For instance, Ethereum, which supports a large number of applications ranging from DeFi to supply chain tracking, has transitioned from proof-of-work to proof-of-stake to reduce its energy consumption by 99.95%.[33]

It is also worth mentioning that as renewable energy sources become more prevalent and as compute becomes more abundant, the environmental impact of blockchain technology, even those using PoW, could be mitigated. Researchers and developers are continuing to explore technical improvements to make blockchain transactions more energy efficient.

Also, many activities in our daily lives, such as travel, meat consumption, and central heating, emit more carbon than cryptocurrency. However, the question is whether the environmental cost of mining cryptocurrency is worth the benefits it provides. Some journeys are not worth taking, some meat goes to waste, and some people keep their homes too warm. Similarly, some blockchain products are not worth the energy they consume, while others are.

32. https://www.jbs.cam.ac.uk/2022/what-is-the-environmental-footprint-of-bitcoin/

33. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Perceived Uselessness

One common criticism of blockchain and cryptocurrencies is their perceived lack of inherent value. In other words, some critics argue that they do not serve a clear, necessary function, and therefore, it is not worth tolerating the other issues. Because they don't believe or understand how tokens represent value and innovation, they believe it is simply a vehicle for speculation and gambling.

Traditional currencies are backed by governments, and we trust that these governments will uphold the value of their currencies. On the other hand, the value of unbacked cryptocurrencies, tokens, and NFTs is based on understanding between the people who use them and not tied to physical commodities or guarantees by powerful institutions. This makes their value more speculative and trading is sometimes treated like gambling. The volatility of cryptocurrencies is used as evidence for their uselessness as currency. It is difficult to pay for goods and services if prices have to constantly change.

There are, of course, some unambiguously beneficial uses of certain crypto. Citizens in countries experiencing high inflation, like Venezuela, Argentina, Turkey and Lebanon, have begun to use digital currencies as a way of accessing US dollars via fintech apps, powered by crypto. This helps safeguard their earnings from rapid depreciation of their local currencies. For nations lacking adequate institutions to manage their own monetary policy, dollarisation has often been considered a solution, and crypto provides a backdoor route to doing it. It is not uncommon for companies in these countries to start compensating their employees in crypto.

This accusation of uselessness also often comes from people who are not aware of the full diversity of Web3 applications and believe that the entirety of the Web3 and blockchain world is made up of different coins. Bitcoin, Ethereum, and other crypto-assets are the most high-profile examples of Web3 but they are just parts of a broader system. Web3 also includes technologies like decentralised storage, like the InterPlanetary File System which allows users to store and retrieve files on a distributed network rather than relying on a central server which may go down. Web3 also includes Decentralised Autonomous Organisations (DAOs) which enable community-led decision making without a central authority.

It is important to take a broader historical perspective on the development of Web3. Many transformative technologies take substantial time to mature and become widely adopted. AI is a pertinent example of this. While now AI is seen by most as a transformative marvel, its foundational concepts have been in development for decades. Alan Turing broached the subject of machine intelligence as early as the 1950s, but it took other innovations in computing and data for the technology to gain mainstream traction. Blockchain is decades newer and will continue to develop and grow. Immediate judgements based on current limitations may overlook and underestimate future significance.

Most of the problems listed above also do not apply to the vast majority of Web3 applications. They will be the subject of the next chapter.

Chapter 3: Case Studies

Our previous chapters discuss the theory of how Web3 and blockchain works. This chapter has some concrete examples of how Web3 is being used to solve real problems. The underlying technology has the potential to be transformative and here we spotlight just a few examples of how it can be used to further decentralisation.

DeFi is being used to deliver financial services to people who would otherwise be unbanked, including refugees, remittance recipients, and the global poor. The underlying decentralised technology has the ability to upgrade public services and to empower consumers to write collaborative stories, to set their own rules for social media, and maybe even start up their own citizen-science projects.

Farcaster and Warpcast

Social media without big tech

Farcaster is a pioneer in decentralised social media. It employs a protocol-based system for broadcasting to public audiences. The structure is similar to that of Twitter, but instead of being run on one centralised platform with the same rules and interface across the user-base, it instead allows users to own their contributions to the network by storing their content directly on the blockchain and empowers those users to choose different applications for accessing the network.

It is effectively similar to email. Email operates on a protocol (the Simple Mail Transfer Protocol, or SMTP) that allows for different service providers such as Gmail or Hotmail to talk to each other. Users can engage in communication regardless of their choice of service provider. These providers often feature distinct user systems, spam filters, and additional functionalities, such as calendar plugins or mail merging capabilities.

Farcaster's role is to decentralise service providers' control and ownership of user content while offering users a choice through applications on how to access the network. Farcaster has technology to guarantee people's digital IDs and ensure that communication between different service providers is as seamless and clear as possible.

This offers a new way to communicate. Traditional social media tends towards large, dominant platforms because of network effects. Conventional social media platforms typically evolve into dominant entities due to network effects, where the increasing number of users tends to attract more individuals, thereby fostering more content creation. However, with the decentralised structure of Farcaster, the advantages

of network effects are retained while enabling users to select a service provider based on their preference for specific algorithms, features, and moderation policies.

Warpcast is an example of the kind of app that is built on Farcaster. Warpcast looks a bit like Twitter (or X), and users can post a 320-character cast. It currently has 10,000 users.

Other applications running on Farcaster include: Jam, which is similar to Warpcast but has a different look and allows people to make longer posts; Frens, a messaging app; Tipcast, which allows you to tip content creators that you like, and many others.

Wirex

Revolutionising banking

Wirex is a UK-based fintech company. It has positioned itself at the forefront of the evolving financial landscape by bridging the gap between fiat currencies and cryptocurrencies.

The user-experience is similar to what users of challenger banks like Monzo have. They have an app that tracks your spending, a debit card, and users can transfer money between different currencies (regular and crypto alike).

Wirex is subject to a great number of regulations from country to country. As it is based in the UK, it works mostly closely with the FCA and is subject to the same laws as any other small bank. Because its users exist in a great number of jurisdictions, it provides them with a detailed statement of every transaction so they can work out what taxes they owe. This is because in places like the UK, citizens pay capital gains tax on every crypto-asset transaction, from bitcoin to dogecoin, whereas French citizens pay a single fixed levy or business income tax.

Perhaps the most compelling aspect of Wirex's platform is the value in facilitating international remittances. Traditional channels for sending money across borders, especially with countries that have capital controls, can be costly and cumbersome. Wirex offers an elegant solution. It enables users to buy stablecoins and send them via the blockchain to recipients in other countries where the stablecoins can be kept as crypto or converted into fiat.

It also is incredibly helpful if remittances are going to an otherwise unbanked population. Traditional banking requires substantial documentation and credit history which leaves a substantial proportion of the world's poor without access to any way of receiving money from abroad unless it's sent by the post. For example, 45% of people in Nigeria don't have a bank account.[34]

The average remittance cost incurred using traditional payments systems is 6.25%.[35] Wirex charges nothing for crypto transfers. When people have very little money, the cost of financial services represents a high proportion of the money transferred. The UK is a wealthy country with perhaps the most sophisticated payments ecosystem in the world,

34. https://www.gov.uk/government/news/nigeria-new-data-from-efina-shows-financial-inclusion-growth

35. https://remittanceprices.worldbank.org/sites/default/files/rpw_main_report_and_annex_q123_final.pdf

which is why bank transfers are practically free here, though they can still be significant for some small businesses. Abroad, however, the fact is that cryptocurrencies offer one of the only ways to transfer money cheaply.

Stellar and Circle

Aid for Ukraine

Stellar was founded in 2014 as an open-source and fully decentralised network that focuses primarily on payments. Circle is a global financial technology company helping money move at internet speed. Together, during the Russian invasion of Ukraine, they teamed up to solve a major problem in aid.

Before the war in Ukraine, 37% of Ukrainians were unbanked.[36] When the war hit, these were the people who were most vulnerable and the hardest to help. Traditional methods of sending aid, especially to displaced people without access to bank accounts, have been fraught with problems. Payments get delayed, it is difficult to make sure money is going to the right people, and on-the-ground mediators can quickly become corrupt when large amounts of money are changing hands.

So in December, the Stellar Aid Assist program partnered with UNHCR to use blockchain technology to deliver aid payments to people in Ukraine. The way it works is that Stellar sends a text message to recipients, directing them to download a digital wallet and then the funds are released into the person's wallets as USDC, a dollar currency stablecoin. It can then be cashed out into local or global currencies at a MoneyGram (a physical shop, of which there are 4500 sites in Ukraine and 350,000 worldwide) or converted into other cryptocurrencies. They use a dollar-pegged stablecoin so that their funds don't get devalued by inflation.

The big advantage of this system is that it allows for bulk disbursement. Stellar's method allows for hundreds of thousands of people to be paid simultaneously, a feat which is near-impossible with direct account to account transfers. The flexible currency option is more useful to people who are currently displaced and on the move.

Adimverse

Democratising storytelling

Adimverse is an innovative platform that seeks to democratise the process of storytelling and ownership in an industry known for its exclusive and gate-kept nature – Hollywood. The team of founders includes a serial tech entrepreneur, entertainment industry analysts, and one of the creators of popular TV show *It's Always Sunny in Philadelphia*. Adimverse aims to change the dynamics of how stories are told, shared, and owned.

Adimverse is in the process of building a platform. Unlike traditional Big Tech platforms where the platform determines how creators are remunerated, Adimverse invites both owners and fans to participate actively in the content creation and compensation process. It is built on

36. file:///Users/anushadinakarababu/Down-loads/BBS_2021_02_Shapoval.pdf

Optimism, a layer 2 scaling solution for Ethereum, allowing it to leverage the security and decentralisation aspects of blockchain. Users are awarded reputation tokens and content tokens, ensuring an aligned incentive system for all participants.

The platform has advanced meaningfully but deliberately. They started with a character-first approach at launch. The team invested in developing one set of characters around which a short film was produced. This approach served as a proof-of-concept for the platform's capabilities. They have since launched multiple "creator rooms", allowing for collaborative story creation. Additionally, Adimverse plans to roll out a more comprehensive protocol soon.

There are two main reasons the platform is building on the blockchain. First, it means the rules are more certain. Platforms like TikTok can change the algorithm or the rules about how creators are reimbursed. Adimverse aims to automate the decisions and fix them on the blockchain so they are harder to change.

Second, they want there to be further decentralisation. To start, the founders have built a more centralised structure, but they have a roadmap for progressively moving towards complete decentralisation. The ultimate goal is to have the community itself establish the rules democratically.

The team believes that the underlying system and protocol could potentially extend beyond storytelling. They imagine a similar structure could be highly effective for collaborative scientific research too.

Spruce ID

Public services with privacy

In the digital era, controlling one's own data has become pivotal. As our lives become more and more online, the organisations we interact with need to know things about us. In most of our digital lives, critical data – usernames, passwords, healthcare records, proof of addresses – are held on centralised databases. Lots of people are naturally afraid of this. Centralised databases are vulnerable to malicious attacks, and users are worried about their privacy.

Spruce ID is a Web3 company and exists to give users control of their data across the web. They are working with the Californian Department of Motor Vehicles to build a state-owned wallet that can integrate with existing state infrastructure.

The system, which is piloted state-wide, enhances privacy. Unlike traditional models, the system does not search the DMV's database each time a user presents their mobile Driving License (mDL). Instead the user presents their mDL, and the state verifies that it is real and has not been tampered with using cryptography .

With a focus on user convenience, the mDL allows users to hold their licence physically and government institutions are already thinking about how to make the mDL interoperable with other state public services.

Chapter 4: Recommendations

The current opportunity

The US government's regulatory response to cryptocurrency has been disorganised, slow, and at times, hostile. The lack of a sensible US crypto asset regulatory framework presents an opportunity for the UK in several ways. While these dynamics are complex and the situation is still unfolding, there are several clear trends.

The current state of crypto regulation in the US makes it challenging for crypto companies to operate, innovate, and grow. If the UK takes a balanced and tailored approach to crypto regulation it will be able to attract crypto businesses and entrepreneurs who find that the US is no longer a viable base for them.

The UK already has a strong reputation as a global financial centre – London is clearly the leading global city for fintech and is Europe's main tech centre. The already existing talent and infrastructure makes the UK an attractive prospective home for Web3 companies that are leaving their current jurisdictions or as a home for new companies to set up. Housing the world's definitive Web3 ecosystem would further entrench the UK's position as a fintech hub.

We are already emerging as a magnet for major companies in the blockchain and crypto space. Noteworthy companies such as a16z, Coinbase, and Fidelity have set up operations in the UK and others are seriously contemplating such a move. What is particularly telling is that some of these companies have explicitly said they are considering relocating away from the US due to regulatory ambiguities.

a16z is a leading venture capital firm with significant investments in Web3 space. It has made a decisive move by opening its first non-US office in London. The firm cited a clear and innovative regulatory approach by the UK authorities, tailored specifically for blockchain and digital assets, as a driving factor. They praised the UK's sandbox approach and our focus on outcomes-based regulation while emphasising consumer protection.[37]

a16z has made significant investments in UK-based Web3 companies like Arweave, Aztec, and Improbable, which further emphasises its willingness to bet on and commitment to the UK ecosystem.[38]

Similarly, Coinbase is a major player in the crypto-asset world. It has expressed its increasing interest in the UK market. CEO Brian Armstrong said that the UK is Coinbases's second largest market in terms of revenue and praised the regulatory environment. His remarks indicate that should the US continue to lag in providing regulatory clarity, companies like Coinbase may allocate more resources to the UK and potentially even

37. https://a16zcrypto.com/posts/announce-ment/expanding-uk-andreessen-horowitz/

38. https://a16z.com/investments/

relocate here.[39]

Fidelity International has launched a London digital hub to expand its digital wealth and crypto services, also signalling potential job growth and economic benefits for the UK.

These shifts indicate that the UK's pro-Web3 regulatory environment, coupled with its strong financial markets and depth of talent, is already enticing big-name companies to either set up or expand their operations in the region. The statements from these companies indicate very clearly how important clear regulations are in attracting this talent and what the benefits are to our country.

What is especially telling is that these companies are not just participants in the Web3 ecosystem, but they are the types of companies that sustain and propel an ecosystem forward. A16z is an investor and has a reputation for spotting the next big thing in technology – the firm invested in Facebook, GitHub, Instagram, Reddit, Stripe, and Twitter. It provides start-ups with capital, mentorship, strategic guidance, and a network of valuable connections. The fund's opening in the UK should attract a cascade of start-ups and talent to the region, eager to be near to such a powerful force. It is worth noting that sometimes American VC funds offer UK start-ups capital if they promise to relocate to the US. Funds with a UK presence are unlikely to do so.

Similarly, Coinbase is a lynchpin in the crypto ecosystem. It serves as an exchange, a wallet, and provides a suite of developer tools. Fidelity is an asset management giant, and brings deeper crypto-asset capital to the UK. The influx of these major players is significant because they act as centres of gravity. Their decision to set up and expand operations in the UK is not just predictive of how others may follow but will also serve to attract ancillary services, smaller start-ups, more developers and traders.

When he was Chancellor of the Exchequer, The Prime Minister Rishi Sunak made his goals for Web3 clear. He said "It's my ambition to make the UK a global hub for crypto-asset technology, and the measures we've outlined today will help to ensure firms can invest, innovate and scale up in this country. We want to see the businesses of tomorrow – and the jobs they create - here in the UK, and by regulating effectively we can give them the confidence they need to think and invest long-term. This is part of our plan to ensure the UK financial services industry is always at the forefront of technology and innovation."

If we are home to most of the Web3 companies and entrepreneurs then we will be the first to benefit from the innovations. Our public services are more likely to run secure systems on blockchain, British artists will be able to make money in new ways, and of course, our state will benefit from the taxes that Web3 businesses raise, and our financial services could be more efficient and consumer friendly.

Striking the right balance between regulation and innovation is possible, and it should allow the UK to realise the many benefits of Web3 while also protecting consumers from harm or the risks of misregulation in other countries.

39. https://www.altfi.com/article/10622_coin-base-ceo-crypto-could-be-20-of-global-gdp-in-20-years

The economic value

The total value of crypto-assets is high. Last year, people in the US, which is the second largest hub (after India), exchanged £943 billion ($1.15 trillion) of crypto-assets. In the UK, which is the sixth largest hub, people exchanged £191 billion ($233 billion).[40] This represents about £76 billion ($92 billion) worth of crypto-assets held and 260,000 jobs.[41]

As US regulation continues failing to provide an effective path to compliance for Web3 businesses, we can expect more and more legitimate innovators to relocate abroad. Currently 23% of traditional hedge funds are reassessing their crypto strategy due to the regulatory environment in the US and 12% of crypto hedge funds are considering relocating from the US to jurisdictions that provide reasonable crypto regulations. [42]

If 12% of these hedge funds are representative of the broader market, we can expect £113 billion ($138 billion) of crypto activity to move away from the US. If we continue as we are currently going, and take the relocation of a16z and Fidelity International as a sign, then we could expect to share this £113 billion with other financial hubs like Switzerland, Hong Kong, and Singapore – taking about a quarter of this US activity and growing by about £27 billion transactions, £10.7 billion in assets, and 36,000 jobs.

If we manage to capture this much of the industry, we can also expect extra benefits from having better payment infrastructure, more highly skilled workers, and a greater tax intake.

What does an effective regulatory regime look like?

Web3 introduces sufficiently new technology that we need to update regulations so that they make sense for it – lest we accidentally ban useful applications. As always, an effective regime needs to balance innovation and consumer protections.

The current approach that the government is taking is "same risk, same regulatory outcome" which we wholeheartedly endorse. This stance means that the government wishes to make sure that Web3 is as safe as traditional finance, but acknowledges that this does not mean blindly copying over existing regulation.

Web3 presents very different risks because it works differently. A good example of this is clearing and settlement. In TradFi markets these are separate processes. Specialised entities perform these tasks, and it can take two days to clear and settle a securities transaction. This is because traditional finance evolved over centuries from a paper-based system that needed intermediaries like brokers, custodians, and market makers to work. In the era before computers, trust was created by regulating these intermediaries. In contrast, settlement in crypto-asset markets is already performed on chain and in real time, obviating the need for separate entities to perform these tasks. As a result, regulations governing traditional finance are generally not an appropriate fit for blockchain technology.

In addition, many rules meant for legacy, centralised financial services businesses like record keeping and trade reporting make less sense if they

40. https://go.chainalysis.com/geography-of-crypto-2022-report-demo.html?aliId=eyJpIjoiV0ExRuaUx-HUkIvTWVBRSIsInQiOiJOcENiM-kN6aVBNVTV0bVV3eIdUQTVnP-T0ifQ%253D%253D

41. https://thedatacity.com/rtics/cryptocurrency-economy-rtic0061/#:~:text=Cryptocurrency%20Economy%20sector%20summary,our%2053rd%20fastest%20growing%20sector.

42. https://www.pwc.com/gx/en/news-room/press-releases/2023/pwc-2023-global-crypto-hedge-fund-report.html

can be looked up on a public blockchain. Of course, there are areas where some rules may need to be similar in their details or intent, with a notable example of centralised crypto exchanges, which act more like traditional financial intermediaries.

There are some instances where blockchains will require stricter rules because of the risks associated with immutability. In English Law, if two parties agree something but a contract says something different, the contract will be remedied to reflect what was actually agreed. With smart contracts, lots of remedies are impossible, so it is more important to get smart contracts right first time.

Regulatory uncertainty

Regulatory uncertainty is what happens when the regulatory environment is unclear or unstable. Certainty is essential to businesses for several reasons.

Uncertainty about what regulations are going to be can create significant risks for companies. Unexpected changes that could result in fines, extra taxes, or – in extreme cases – that result in some aspects of a business model being rendered illegal, make it difficult for businesses to plan for the future.

Several companies have suspended their Web3 offering in the US because of the regulatory uncertainty in the current environment. Revolut has announced that, from 2nd September 2023, US customers will no longer be able to buy crypto, and Robinhood has said that users will no longer be able to buy tokens.[43] For similar reasons, Gamestop, from the 1st November, will no longer offer its Ethereum NFT wallet. Gamestop's CEO said, after recent developments in regulation and the market, the company has "proactively minimised exposure to cryptocurrency risk throughout the year."[44]

If the UK has an uncertain regulatory landscape, similar to the US's, companies will be hesitant to base themselves here, investors will be hesitant to invest in British Web3 companies, and foreign Web3 companies will be less likely to sell their services to British consumers.

Regulatory uncertainty also makes the companies that decide to build their businesses, invest in, or sell in the UK less efficient. More resources need to be invested in compliance and risk planning and consumers don't know if they can trust the integrity or quality of products on offer. A strong competitive advantage exists for companies operating in jurisdictions with clear and predictable regulations.

The EU has just voted in comprehensive crypto regulation, MiCA.[45] Germany has passed a series of bespoke pro-Web3 regulations and its crypto-asset market grew by 47% over the last two years, so it is now comparable to the UK market.[46] The UK should act swiftly to capitalise on the current opportunity. The UK should put effort into making the rules for Web3 companies clear and we should do so in a timely manner.

43. https://www.coindesk.com/policy/2023/08/04/revolut-suspends-us-crypto-operations-over-regulatory-uncertainty/

44. https://arstechnica.com/gaming/2023/08/gamestop-citing-regulatory-uncertainty-winds-down-its-crypto-and-nft-wallet/

45. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica

46. https://go.chainalysis.com/geography-of-crypto-2022-report-demo.html?aliId=eyJpIjoiV0ExQ1RuaUxHUklvTWVBRSIsInQiOiJOcENNiMkN6aVBNVTV0bVV3eldUVnnP-T0ifQ%253D%253D

Regulation by enforcement

Regulation by enforcement refers to the practice of attempting to use legal actions, such as lawsuits or fines to set precedent and guide industry behaviour instead of laying out specific rules or guidelines through traditional regulatory processes. This approach is less desirable than the "traditional" way of regulating, where rules are proactively defined and communicated.

Regulation by enforcement adds to regulatory uncertainty. Because institutions are subject to preexisting rules rather than tailored rules, it can mean that departments, regulators, and courts may act at cross-purposes and produce unintended and undesirable results. Web3 and blockchain applications do not neatly fit into existing definitions and rules so in many cases this approach gives courts or arms-length agencies the final say, instead of elected politicians or experts in the field.

In the case of Web3, one branch of government may choose to incentivise proof-of-stake consensus mechanisms for environmental reasons. Another may decide that the process of staking counts as a disposal of crypto and subject it to capital gains tax, rendering it economically not viable.

The US is currently taking this regulation by enforcement approach and is one reason why there is so much regulatory uncertainty and why several Web3 companies are closing down their US operations.[47]

The UK should seek to provide clear and comprehensive guidance to blockchain companies about how they will be regulated and taxed. This will avoid the confusion that comes from relying on court decisions.

Speed of regulators

Founders in the Web3 space can be somewhat sceptical of regulators. There is currently a perception that if you do everything "by the book", your approvals will be so slow and cumbersome that you will be outcompeted by "pirates."

One suggestion to overcome this would be to create a Web3 regulatory sandbox similar to the FCA's Digital Sandbox.

The FCA's regulatory sandbox is an initiative that was introduced by the regulator to foster growth in the FinTech sector while ensuring that customers are still adequately protected. The sandbox essentially provides a controlled environment for FinTech companies to test their products and business models without facing the full regulatory burden that would typically apply. It gives the regulator an opportunity to consider if its regulations need to be updated for groundbreaking technology.

This sandbox is often credited with helping the UK become a world-leading FinTech hub. It reduced regulatory uncertainty for companies. The sandbox was seen as pioneering by regulators in other sectors and abroad. The FinTech sandbox has been imitated in countries like Australia, Singapore, and Canada, among others. Other regulators in the UK have set up their own sandboxes too, like the ICO for data, Ofgem for energy, and relevant here, the Treasury, FCA, and Bank of England plans to launch a Digital Securities sandbox.

47. https://www.forvis.com/article/2023/04/1q-2023-crypto-update-regulation-reporting

A general sandbox for Web3 and blockchain applications would greatly benefit the sector and allow regulators much needed insight into how to regulate these technologies. It should go beyond financial services and securities and should therefore sit with DSIT and the FCA, instead of just the financial regulators. HMT and HMRC should also feed in.

RECOMMENDATION: **The Department for Science, Innovation and Technology and the FCA should create a joint regulatory sandbox with input from HMRC and HMT.**

Where are financial regulations appropriate?

One response to the critique of the "regulation by enforcement" argument, is that actually it is just "enforcement" and that current financial regulations can be perfectly applied to blockchain applications and that regulators are simply responding to cases where blockchain is violating existing laws.

In some cases this is true. DeFi platforms that perform traditional banking functions, like lending and online bank accounts, should follow standard consumer protection laws. A good rule of thumb is that regulation should focus on centralised exchanges and that they should be regulated in line with the "same risk, same regulatory outcome" approach.

DeFi is a nascent part of the industry and extremely innovative. It should be monitored, and regulation should be developed steadily over time. However, consumer protection should not be put at risk. Where Web3 firms offer software services for financial products, these software services should be regulated like software.

Financial Stability

Financial stability rules exist to protect the economy from financial crises. Because finance relates to all other parts of the economy, crises in financial services can cause knock-on problems for the rest of the economy – similar to how spikes in energy prices can cause inflation in the rest of the economy. As a result, much of the work of regulators like the Bank of England involves monitoring large financial institutions for risk. This is to avoid future crises like the 2008 financial crisis.

While DeFi involves finance, it does not pose the same financial stability risk that traditional financial institutions can. This is because it is a nascent industry and currently only a small proportion of people use blockchain-based technologies. With regards to centralised platforms, FTX was one of the biggest crypto exchanges in the world worth $32 billion (£27 billion). While this meant that lots of people lost money and coincided with a decrease in funding for the Web3 ecosystem – it did not cause a financial crisis. For comparison, when Lehman brothers went into crisis, it had $690 billion (£370 billion) in assets and was lending more than an entire FTX ($50 billion or about £30 billion) every month.

Even if the blockchain space was bigger, it would have a different risk profile so some of the financial stability checks would have to be adjusted. While issues like fraud or technological failure are shared concerns, the structure and operation of blockchain networks may mean that the same

risk monitoring ought to be proportionate but not the same.

Tokens

Under the UK framework, a regulated activity is of a specified kind which is carried out by way of business and related to an investment of a specified kind. Both the types of activities and the types of investments "specified" for these purposes and set out under the Regulated Activities Order (RAO).

Some of the activities listed in the RAO include deposit-taking, issuing and administering electronic money, arranging deals in investments, managing investments, and providing investment advice. The types of investments listed in the RAO include shares, debentures, government and public securities, warrants, futures, and contracts for difference.

For an activity that falls within the definitions set out in the RAO to be regulated, it also needs to be carried out "by way of business" meaning that the activity is carried out with a degree of continuity, frequency, and scale that means it could be considered a commercial endeavour.

The FCA has broadly categorised crypto-assets into three types: unregulated tokens, E-Money tokens, and security tokens. First, unregulated tokens – these which are not issued or backed by any central authority, and include exchange tokens such as and are meant for the purpose of exchange Bitcoin and Ethereum are tokens as well as utility tokens. Second, backed e-money tokens are those that meet the definition of electronic money under the Electronic Money Regulations 2011 (EMRs). And third, security tokens. These tokens have characteristics similar to traditional instruments like shares, debentures, or units in a collective investment scheme.

Security tokens are the primary focus when considering the RAO. If a token qualifies as a security token, any activities related to it could fall under regulated activities requiring FCA authorisation and a higher regulatory burden. Exchange tokens and utility tokens would typically only fall under anti-money laundering and counter-terrorism financing regulations.

The classification of some tokens as securities carries significant legal implications. If a token is deemed a security, it is subject to regulations around registrations, disclosure, compliance, and enforcement provisions. The exchanges that trade tokens are also subject to these rules.

To understand whether securities regulation should apply to tokens, we need to understand why securities regulation exists. It primarily exists to maintain fair function in the securities market to facilitate investment and therefore business growth.

Securities laws require companies to disclose significant information about the companies. This transparency means that investors can make informed decisions about where to invest with the goal of encouraging capital to go to businesses with better prospects.

Rules requiring periodic public disclosures of listed companies as well as rules prohibiting market manipulation and insider trading exist to increase confidence in the market and are foundational elements of a strong securities regulatory framework. You wouldn't buy Facebook shares from

someone who works in Mark Zuckerberg's office and may well know something about Facebook that you do not. Similarly, you wouldn't buy shares in a market if people were regularly releasing false information about the relevant companies to make prices go up and down. These rules exist to protect market integrity and they increase investor confidence.

While it is a good thing that most of the securities market is able to operate with high levels of trust, existing securities rules do not fit this technology and as such are often inappropriate for decentralised projects that are community governed or for tokens that have a primarily consumptive use.

Further, compliance costs are high, which diminishes innovation and competition by benefiting large, centralised incumbents and disadvantaging smaller but growing networks. The legal, accounting, and administrative burden is expensive. Small companies do not usually have their shares trading on an open exchange and so the costs of compliance don't matter so much – except in the case of a few startups with novel fundraising solutions. In the case of DeFi and other blockchain applications, tokens can be issued for very small projects, but they are often not the primary source of capital. In these instances the issuance of tokens may be done for nominal or no consideration. In these situations, it may not be necessary to treat the decentralised project as having engaged in a public securities offering. In fact, providing a path to exempt early distributions for no value (i.e., "airdrops"), would likely kickstart the creation of decentralised networks. Bringing in securities-style compliance requirements in these cases would bring in some aspects of centralisation and can undermine the technology's true innovation.

Web3 projects should, by achieving a level of decentralisation, be able to show regulators that they are not operating like regular companies and that tokens are, therefore, not just acting like shares on a stock market. Regulators should seek to promote decentralisation and provide clear guidelines and thresholds at which companies are considered to be sufficiently decentralised that they carry different risks and regulators should be clear about what obligations token-holders have in these scenarios.

These obligations and thresholds should not increase centralisation and should, ideally, promote greater decentralisation.

RECOMMENDATION: In developing its secondary legislation to effectuate the new crypto-asset regulatory framework, HMT should promote decentralisation and provide clear lines around decentralisation thresholds projects must meet to issue tokens under crypto-asset specific (ie non-securities) rules.

Anti Money Laundering Regulations

Many current anti-money laundering approaches focus on a "Know Your Customer" (KYC) approach. As most blockchain transactions are transparent and immutable – meaning that the customer is usually pseudonymously known, KYC approaches often fail to tackle the actual risks that come with

blockchain transactions but they can exacerbate financial exclusion and lead to unnecessary bureaucracy.

The FCA should allow for the use of alternative and innovative techniques designed to prevent illicit finance while allowing the technology to operate as intended for users. For example, because most blockchain-based transactions are transparent, compliance departments could incorporate a stronger "Know Your Transaction" approach. In addition, new technologies like digital identities and blockchain analytics tools may be more effective in meeting anti-money laundering goal for certain crypto-asset activities.

RECOMMENDATION: The FCA's risk-based anti-money laundering program requirements should be flexible and fit-for-purpose in order to account for technological and behavioural differences between blockchain transactions and fiat currency transactions and to allow for innovative AML solutions.

Self-Hosted Wallets

Self-hosted wallets are a core part of Web3 as they allow users to control their own data when interacting with centralised software providers, thus reducing the ability of third parties to collect and store personal identifying information.

In the EU and the US there have been various policy proposals which have suggested that self-hosted wallets be limited in some way. This comes from the notion that self-hosted wallets are like bank accounts – which is a misunderstanding. Self-hosted wallets are much more like actual wallets. People can put their cryptocurrencies in them, but they can also use them to store their digital art, NFTs, and tokens.

Some regulated entities offer Self Hosted Wallet software that enables customers to hold their own private keys – much like a password holder. But importantly, a self-hosted software provider does not control or otherwise have access to the private keys, and thus no ability to hold funds within or conduct transactions with that wallet. Providing Self Hosted Wallet software is thus not the provision of a financial service and therefore should not be subject to financial regulation.

For the same reason that financial regulation doesn't apply to people who sell purses it should not apply to the software that creates these wallets.

Moreover, self-hosted wallets do not pose a heightened risk of illicit finance. Of note, the UK Treasury in a recent report found that "there is not good evidence that self-hosted wallets present a disproportionate risk of being used in illicit finance." Further, the Financial Action Task Force (FATF), the international body tasked with analysing illicit finance and setting global AML standards, carried out an extensive study on self-hosted wallets and was unable to identify them as categorically high risk.

Rather than posing a heightened risk, self-hosted wallets are an important and healthy part of the ecosystem that allow users to directly participate in a new Web3 environment. And the reasons are clear: the

transparency, permanence, and immutability of the blockchain gives law enforcement investigative advantages compared to traditional finance. This means crypto assets and SHWs are in fact rarely 'anonymous', and are a poor vehicle for illicit activity.

RECOMMENDATION: Regulation should not undermine self-hosted wallets.

Staking

Staking is a critical technology that ensures the accurate, secure, and efficient operation of many blockchains. It is what proof-of-stake, the environmentally friendly alternative to proof-of-work, is based on.

In proof-of-stake systems, participants "stake" their crypto to be selected as validators who create new blocks. Selection odds increase proportionally as the size of the stake increases Validators are rewarded with new coins and/or transaction fees and can be penalised by losing staked coins for dishonest behaviour.

Without broad retail participation in staking, we risk losing proof-of-stake blockchains and transitioning over to proof-of-work systems instead.

When HMT consulted on crypto-assets it suggested that some staking arrangements may qualify as Collective Investment Schemes (CIS).[48] The CIS definition is:

> *"(235) In this Part "collective investment scheme" means any arrangements with respect to property of any description, including money, the purpose or effect of which is to enable persons taking part in the arrangements (whether by becoming owners of the property or any part of it or otherwise) to participate in or receive profits or income arising from the acquisition, holding, management or disposal of the property or sums paid out of such profits or income.*
>
> *(2) The arrangements must be such that the persons who are to participate ("participants") do not have day-to-day control over the management of the property, whether or not they have the right to be consulted or to give directions.*
>
> *(3) The arrangements must also have either or both of the following characteristics—*
>
> > *the contributions of the participants and the profits or income out of which payments are to be made to them are pooled;*
> >
> > *the property is managed as a whole by or on behalf of the operator of the scheme."*

Staking is not a CIS. Staking does not involve the acquisition or disposal of property and staking rewards do not arise from merely "holding" the staked asset. Providing a staking service cannot properly be described as a "management" of assets – a staking service simply runs software with a predetermined function. Management of assets implies that there is a degree of managerial effort or choice being made.

Staking does not pose a financial risk. There is no investment of money

48. https://www.gov.uk/government/consultations/future-financial-services-regulatory-regime-for-cryptoassets

in staking and when crypto-assets are staked they cannot be used by anyone else for anything. This is not analogous to a bank or lending. While the network penalties are possible, they are extremely rare.

Individuals can stake assets on their own, but doing so is less convenient than using a staking service. There is some open-source software available. But direct staking requires users to store their own keys, configure their own computers, and patch their own software. Fee-based staking services thus provide a more efficient and safer way for individuals to participate in staking and earn rewards.

Regulating staking as a financial service and restricting staking services would be a mistake. It would not protect retail consumers and instead would deny them access to IT infrastructure.

RECOMMENDATION: The FCA should not regulate staking services as a financial service.

Taxes

There are no new laws that apply to crypto-assets, therefore existing principles apply. Tax is based on the facts and applying the relevant tax provisions according to what has taken place. If used for trading purposes then any profits are charged to Income Tax. If used as a means of investment any gains or losses are chargeable to Capital Gains Tax (CGT). If they are used for remuneration then the receipt will be chargeable to Income Tax. Finally, where used by a corporation the profits are charged to Corporation Tax.

As noted in HMRC's market research, most individuals own crypto-assets as a "fun investment" or due to an "interest in the underlying technology". Where crypto-assets are owned for these purposes they will be charged to CGT. Each crypto-asset is considered to be a separate asset therefore where one crypto-asset is exchanged for another it creates a "dry tax" charge, one where there is no money, pounds Sterling, to enable them to pay for the tax liability. This means that the person must either sell their crypto-assets for fiat (money) or use other existing funds to pay the tax liability.

The fact that each exchange of one crypto-asset for another is taxable can create very complex tax returns requiring either the use of software to calculate their liability or taking a significant amount of time to do so. There is a risk that many people do not understand this and HMRC's market research found that from those that owned, or had owed, crypto-assets only 28% were aware of HMRC's guidance.

For many people in the UK this won't be a problem as their gains could be less than £6000, the Annual Exempt Allowance (AEA), through the buying and selling of crypto-assets. However the AEA was reduced last tax year from £12,600 and will be reduced further next tax year to £3,000 bringing more people over the threshold over which they owe tax.

For Web3 this will cause problems. For example, the game Axie Infinity which is a blockchain-based game where players collect, breed, raise, battle, and trade fantasy creatures called Axies. These Axies are NFTs

on the Ethereum blockchain, meaning each Axie has distinct value and can be bought, sold, or traded. Certain tokens can be bought and used to "repair" or improve the in-game characters these could increase. On the 31 December 2020 an online game, Eve Online, witnessed a battle that caused a total of $378,012 (£277,000) worth of damage.[49] While Eve Online is not a Web3 game, the premise is the same in that games can result in real world losses. This could cause tax administrations a lot of head scratching as to whether or not the state should be party to these losses, and this will only increase if Web3 becomes more popular.

Based on HMRC's own research we believe that many players will not be aware that they are creating tax liabilities as they play a game. Furthermore, with the reduction in the AEA this is going to become an increased compliance issue for both users and HMRC to ensure that the correct tax is paid and collected.

The use of a tax wrapper, with restrictions on its use, which removes the liability on crypto-to-crypto transactions and, therefore, the dry tax charge would reduce customer burden and make it easy to be compliant with the relevant laws.

Furthermore, HMRC should make clear which common uses of crypto-assets incur which taxes. There is some uncertainty if staking assets to a proof-of-stake (PoS) mechanism would be considered to be a taxable event. If it is considered by HMRC that staking tokens is a disposal this could impact on those wishing to contribute to the PoS mechanism. Whilst this is probably not the case as there is no transfer of beneficial ownership confirmation on this point from HMRC would be helpful.

This clarity is particularly necessary for firms that provide employee incentives in tokens, and have to individually determine whether the tokens fall within the definition of securities so as to determine the correct tax treatment. Uncertainty in this area leads to each firm having to undertake the same work and legal advice, leading to unnecessary costs and delays.

RECOMMENDATION: HMRC should create a tax wrapper for the exchange of crypto-assets.

Stablecoins

Stablecoins bring money into the 21st century and are scaling at an extraordinary pace. In 2022, stablecoins settled over $11 trillion (£9 trillion) on blockchains, dwarfing the volumes processed by PayPal ($1.4 trillion or £1.1 trillion) and close to the payment volume of Visa ($11.6 trillion or £9.5 trillion). They combine the efficiency that comes with Web3's "internet native" payment systems with the stability of fiat currency prices, thus having the capacity for broad adoption.

Paypal now allows customers to transfer stablecoins, and Visa has announced that it will be using stablecoins to simplify some of their cross-border transactions.[50]

49. https://www.ign.com/articles/eve-online-breaks-its-own-guinness-world-record-for-the-costliest-video-game-battle-in-history
50. https://www.businesswire.com/news/home/20230905549860/en/Visa-Expands-Stablecoin-Settlement-Capabilities-to-Merchant-Acquirers

Consumer welfare

Fiat-backed stablecoins are simple enough and mostly can be regulated the same as money. If you own a token that is worth a pound, that is backed up by a pound held somewhere, then you effectively have a pound. In those cases, all the regulations and taxes that you would own from trading pounds should come into place. You should not, for example, be able to avoid VAT by selling your goods in stablecoins.

Algorithmic or crypto-backed stablecoins are more uncertain because they may be less "stable". If you own a token that is worth a pound, but it is backed up by a basket of cryptocurrencies that may experience higher volatility than other assets, you don't effectively own a pound in every scenario.

This poses a consumer welfare question as well. Consumers should be aware of how secure their stablecoins are before buying them. The FCA should regulate how stablecoins can be marketed, and whether the basket of currencies and the algorithms that trade them are secure enough. After that point, stablecoins should come under the same rules that fiat currency does, and conversions of cryptocurrencies like Ether into stablecoins should count as a disposal of one's crypto.

RECOMMENDATION: **The FCA should ensure there are clear signposts and disclosures to consumers as regards stablecoins and their claims to "stability."**

Central Bank Support

The Bank of England has published several papers on the creation of a digital pound.[51] The so-called "Digital pound" has been overseen by a Bank and Treasury Taskforce.[52]

As the Bank of England describes it, "The digital pound would be a new form of sterling, similar to a digital banknote, issued by the Bank of England. It would be used by households and businesses for their everyday payments needs. It would be used in-store, online and to make payments to family and friends. If introduced, it would exist alongside, and be easily exchangeable with, cash and bank deposits."

In addition to this, they should promote a flourishing private sector stablecoin market by allowing stablecoin reserves extra stability, by placing them with the Bank.

Stablecoins such as Tether (USDT) and USD Coin (USDC) are already established and integrated within existing financial architecture. They are widely recognised and used for trading, investment, and transactions globally. They were used to send aid to Ukraine, as per the case studies in the previous chapter, and PayPal and Shopify now allow you to use them for payments.

This adoption means there is already a robust ecosystem that supports these stablecoins. There are already retail investors who are comfortable using them, which means adoption will be simple and easier.

A major advantage of adding extra stability to "pound-sterling" stablecoins, is that it would mean that DeFi applications would naturally

51. https://www.bankofengland.co.uk/paper/2023/the-digital-pound-consultation-paper

52. https://www.bankofengland.co.uk/the-digital-pound/cbdc-taskforce-terms-of-reference

be sterling-dominated. This means that if Web3 enthusiasts are correct, and more of our lives happen "on-chain", the UK will have an outsize role in influencing what this looks like.

RECOMMENDATION: The Bank of England should promote a flourishing stablecoin market in the UK by allowing stablecoin reserves to be placed at the central bank.

Decentralised Autonomous Organisations (DAOs)

The Law Commission is currently consulting on how DAOs fit within the laws of England and Wales.

Finding the correct regulation for DAOs is difficult as the term DAO does not necessarily represent any particular kind of organisational structure. Some DAOs could easily map to currently existing company, charity, or cooperative structures . How to regulate DAOs is a pressing question though; EY estimates that there are about 13,000 in existence, which together hold about $23 billion (£19 million).[53]

One major problem is that DAO members can exist internationally. Currently, if you are a British person who owns tokens in a DAO, members in other countries could potentially vote to have the DAO do something that is illegal in Britain but legal abroad. The UK should take a more balanced approach that recognises the liability of a DAO itself while providing individual members with limited liability.

The Law Commission will hopefully resolve these questions in its upcoming work.

RECOMMENDATION: The government, with the help of the Law Commission, should clarify legal protections and liability for DAOs and their members.

Web3 for public services

Web3 has the potential to revolutionise various aspects of public services. The technology has the ability to bring in a higher level of transparency and security.

Because blockchains are interoperable by default, they should allow for secure data sharing between different government services.

In India, the Telangana State Government uses blockchain to green their agriculture industry. Farmers can earn credits for switching to organic farming, agroforestry, crop rotation, and other forms of green farming. These credits are automatically administered by the Algorand blockchain and can be traded on global carbon markets and bought by companies as part of carbon offsetting projects.[54]

Similarly, Circularise uses blockchain to trace supply chains. Porsche uses it to make sure their cars are built ethically and sustainably.[55] The government could use a similar system in anti-modern slavery work.

In a bid to expedite property transactions, HM Land Registry explored the implementation of blockchain technology via the Digital Street research project. They collaborated with conveyancing firms, a payment intermediary, a digital identity provider, and HM Revenue & Customs

53. https://www.ey.com/en_gl/tax/how-to-navigate-tax-and-legal-complexity-associated-with-daos

54. https://www.financialexpress.com/business/blockchain/algobharat-collaborates-with-state-of-telangana-to-drive-blockchain-backed-practices/3053997/

55. https://www.circularise.com/resource/achieving-visibility-into-the-porsche-supply-chain

to create a prototype using the Corda platform, focusing on digital transfers of property. The prototype, tested on a real property transaction, demonstrated its potential to complete processes in minutes, offering transparency, speed, security, and automation through smart contracts. With positive feedback from industry participants and a growing community, HM Land Registry plans to further explore various models and technologies, aiming to foster innovation and bring transformative changes to the property market.

To improve expertise in government and create more initiatives like this, the government should establish "Digital Fellows' These Digital fellows would act in an advisory capacity and focus on upgrading public services using frontier technologies like blockchain, AI, and data.

These roles should focus on identifying areas within public services that would benefit from digital transformation. They should work primarily with procurement and service delivery teams and liaise with external technology providers.

They should be oriented towards major public services like the Passport Office, HMRC, the Student Loans Company, Companies House, The Insolvency Service, the Land Registry, and other similar parts of government.

RECOMMENDATION: The government should recruit digital fellows who help the government upgrade public services with cutting-edge technology.