Framing the Future

Exploring the potential of Web3 technologies to solve big global challenges

UKaid
from the British people

FRONTIER
TECHNOLOGY
LIVESTREAMING

WEB3

Introduction

This paper offers some background reading for a symposium on Web3 for global challenges. The idea for this work originated from a simple moment of rueful nostalgia.

We are old enough to remember the emergence of Web2. We can clearly recall the excitement and the optimism that emerged around the promise of a community-driven, user-generated web powered by innovative applications. We were right there as people's imaginations were reignited following the end of the 20th century and the bursting of the dot-com bubble.

Today, as we peer out at the platform monopoly that dominates our online existence, it's hard not to wonder how things might have been different if we had taken the opportunity to take stock of our ambitions and to get to know our tools. Could we have mapped a more thoughtful route to the future if, instead of moving fast and breaking things, we had moved mindfully in order to build better things?

At the time, Web2 was accused by some of being a poorly defined hype bubble. Now, over twenty years later, those same criticisms are being levelled at Web3. The good news is that, this time we are in a position to learn from history. We understand that, if we look past the puffery and propaganda, there are clues there that could lead us to a more equitable and desirable outcome.

In this report we focus on four key characteristics of what Web3 has to offer. For each one we have tried to pull out the nuances and delve into the grey areas so that we can understand and imagine the futures they might result in.

To do this we have sketched out some speculative scenarios to grasp what the long-term political, economic and social implications *of* these technologies may be, as well as looking at the developments we can expect to play out in the immediate future and the impact they might have.

Finally, we sum up some of the questions, pressures and issues that we believe we will need to interrogate further in order to begin utilising Web3 to solve some of the world's biggest challenges and bring together the insights and observations gathered during the course of the symposium, to suggest a framework for a practical, controlled 'test and learn' approach to understanding and leveraging the potential of Web3.

- *Lea Simpson and Abigail Freeman, Frontier Technologies Hub and Brink.*

This paper is a synthesis of three commissioned pieces of work by The Frontier Technologies Hub

- *Pluriversa, a decentralised research and design network based in Colombia mapped trends across Latin America, conducted field research in El Salvador, and produced 5 speculative futures for post-development and sustainability.*
- *Phas3, a decentralised innovation foundry based at UCL ran ID3, an event to crowdsource ideas from the Web3 and international development communities.*
- *Careful Industries, a research consultancy working to understand and anticipate the social impacts of technology produced a report examining whether emerging Web3 technologies are useful to make progress on global challenges in ways that provide economic and society-wide benefits for everyone, everywhere.*

  Thank you also to John Hoopes, of Toucan and the Web3 Climate Action Working Group, for his valuable feedback on the final chapter of this paper.

Contents

SECTION ONE

Governance without governments

Web3 has the potential to enable new forms of collaboration and coordination, unrestricted by borders or local jurisdictions.

Whereas traditional mechanisms rely on centralised authorities making decisions based on the needs of their locales, Web3 technologies can empower individuals to participate in making decisions that will have direct impacts on their lives.

These kinds of systems that allow for decentralised decision-making across geographically scattered communities are worthy of further investigation because they have the potential to radically transform both political participation on a local level, and collaboration on a global level.

Dawn of the DAO

Today this area of innovation is centred around decentralised autonomous organisations (DAOs). A DAO is a democratic structure that has no central governing body and whose members share a common goal to act in the best interest of the entity. In a DAO power is distributed across token holders who collectively cast votes; all operations are fully transparent and global; and the rules, values and aims of the organisation are embedded in 'smart contracts', immutable code that theoretically removes the need for any kind of hierarchy and ensures consistency of purpose.

As with everything Web3 related, there are certain limitations and risks here.

Smart contracts are computer programmes written by humans, and humans make mistakes. This leads to security vulnerabilities, which in turn lead to trust issues. In 2016, when the German startup slock.it launched a DAO to support its 'decentralised Airbnb' startup, the code they used was faulty and hackers were able to exploit that fault to syphon off $50 million worth of Ethereum.

As with any system where every participant is required to participate in decision making, DAOs can be slower and less efficient than other organisational systems. This is compounded if large sections of the community have to be educated in the issues at hand and have to spend time discussing, organising and strategising amongst themselves. Making important decisions quickly is difficult in a DAO.

Perhaps most importantly (at least from the perspective we are viewing them from) because DAOs are still very much an emerging concept, they aren't regulated in ways we've come to know and understand. Legal issues such as taxation and property ownership within a DAO are still very much grey areas, and (as we'll see) if we scale up the idea of a DAO to a transnational level this lack of legal, regulatory, and policy frameworks could have global ramifications.

Decentralised governance in the real world: Klima

The Klima Dao is made up of a group of environmentalists, developers and entrepreneurs from around the globe who have come together in a decentralised autonomous organisation that has the common aim of "accelerating the delivery of climate finance to sustainability projects globally".

The DAO does this right now by helping to monetise carbon assets transparently and efficiently, thereby making low-carbon projects more appealing to investors (this is a gross but necessary oversimplification of what Klima does and if you want to read more about it then here is a good place to start).

As of the start of 2022, Klima had a 42,000 active 'Klimates' and an overall community with upwards of 60,000 members. The DAO has its own podcast, an active Medium and a Twitter presence with followers in the five figures.

The Klima Dao has distinct departments focused on policy, engineering, partnerships, operations, community, creative, and marketing. Their stated aim is to work "hand-in-hand with professional firms to deliver the highest possible value for the community" and "coordinate with high-level government and industry representatives to structure the on-chain carbon economy".

In March of this year the DAO published a post on its blog entitled *DAOs, Organization Theory, and Klima's Decentralized Autonomous Organization* in which they recognise that the DAO needs "to find a legal entity that allows it to act and be legally recognized" and suggest that a trust structure might be the best way of creating the kind of robust legal foundation that can "connect the crypto world with the real one" (they also dig into the feudal rights of Henry VIII and the legal history of the Channel Islands, which is not what you expert from a Web3 manifesto but makes for interesting reading nonetheless).

Some other examples from the present

The Regen Network is an open, collaborative global community built around a public blockchain called the Regen Ledger. As part of the regenerative finance (ReFi) movement, Regen allows for the origination, governance, and exchange of digital carbon assets. Their community of developers helps to code new applications and integrate the network, while their scientific community creates and publishes research around measuring ecological health.

5ire is the fastest growing blockchain in India and "the world's first sustainable blockchain". Its model works by replacing the traditional Proof-of-Work algorithm with a Proof-of-Benefit paradigm which incentivises sustainable behaviour and practices that align with the United Nations Sustainable Development Goals (SDG). Within its ecosystem is 5ire Capital, a VC fund built around a DAO structure to promote investment in environmentally sustainable projects.

What could the future hold?

Where we could end up

One of the potential futures mapped out in our speculative 2038 exercise looked at *The rise of the living city* and the way in which new forms of governance and self-organising ventures allow for complex systems to be woven together in intricate and ultra-efficient ways, ultimately giving rise to a truly global circular economy.

In this scenario, we trace the development of Decentralised Autonomous City Governments (DAGovs); citizen-led autonomous settlements in which residents are able to participate directly in decision-making and collaborate and communicate across borders via a decentralised platform.

This novel system of governance allows citizens to process their credentials, pay taxes and services, and make decisions that affect their localities in an immediate, immutable and transparent manner. But this future is only made possible if it is underpinned by a trusted Decentralised Citizen Finance platform and widespread adoption of a tokenised economy, and ideally, is grounded in a widely-recognised Technological Ethics agreement.

This future also comes with a warning: that normative tensions within these sorts of settlements could just as easily play into the hands of oppressive elites, who could co-opt the same technological infrastructure to implement surveillance and indoctrination of citizen behaviour through social scoring.

What's already in motion

It's clear that the unique capabilities of Web3 when applied to non-geographical governance will create new ways for those with a common aim to collaborate and organise outside of traditional multilateral structures, and that these emerging organisations will at least attempt to operate across regulatory and legal borders as well as geographical ones.

What's standing in the way of that right now are issues of interoperability, standardisation, and infrastructure; and a lack of regulatory and legal frameworks.

Just the fact that separate blockchains cannot talk to each other would suggest that until new standards and infrastructures are in place, then these kinds of decentralised autonomous organisations will struggle to scale and leverage their unique capabilities to their full extent.

The global proliferation of Web3 technologies will also require the infrastructures and resources to support it; currently infrastructure is not evenly distributed, and so participation in a DAO would be a significant challenge for a remote community.

There's evidence that there are emerging organisations looking to overcome these challenges, and finding innovative means of "connecting the crypto world with the real one" but we are yet to see how existing democratic institutions and multi-stakeholder groups will react to these advancements or how willing they will be to begin constructing the necessary legal and infrastructural bridges from their side of the divide.

Next steps to designing the future

As we move to consider the potential accelerators and decelerators that we might want to use in testing the robustness and feasibility of these futures, it's important to recognise the inherent juxtaposition that sits at the centre of emerging systems of non-geographical governance.

On the one hand there is a strong argument that a common, cross-border legislative and regulatory framework is as much of a requirement as an equitable technological infrastructure in order to make Web3 a scalable reality. On the other hand, if we acknowledge that these technologies could be used to enable new authoritarian regimes, or allow corrupt governments to manipulate or misuse citizens' information, then we must also consider how a clear separation of Web3 communities and the state could be enacted in order to protect individuals.

If we want to move forward, safely and confidently into this future we must find a way to navigate these contradictions.

SECTION TWO

Easier, Better, Faster, Stronger

One of the most common criticisms aimed at Web3 is that it offers little more than a shiny new outfit for the Emperor.

Where once the humble, artificially-intelligent refrigerator took much of the flak from those wary of technofetishism, now crypto champions and NFT touts sit squarely in the firing line, accused of presenting redressed existing technologies as new innovations along with hyperbolic claims and inflated promises.

But while there is undoubtedly a lot of flimflammery and finagling at play here, there is also a quiet corner of the Web3 space where the technology is being put to work in a much more prosaic fashion. Spaces where bureaucratic, top-heavy systems are being made more streamlined and equitable; and where wasteful and opaque infrastructures are being replaced with increasingly efficient and accessible frameworks.

Blockchain, meet supply chain

It could be argued that Web3 is at its best when it is at its most boring.

Consider the use case of a large organisation that has multiple suppliers across many facets of its business. Every day, many thousands of communications and transactions might occur across that sprawling web of connections, each one creating its own set of data points and down-chain ramifications, which may or may not be captured and repurposed.

Web3 has proven itself very adept at speeding up and simplifying these sorts of cross-party processes, especially if those processes involve multiple nodes and intermediaries.

Take, for example, a transfer of ownership between a buyer and a seller. If you've ever bought a property in the United Kingdom, arguably a relatively 'advanced' fintech nation, then you'll know all about the glacial pace that's set as various checkpoints are navigated, internal systems on either side are updated, and confirmations are communicated through multiple intermediaries.

By moving these processes to a shared ledger held on the blockchain, the need for brokers and meddlesome 'middle men' is eliminated and replaced by a single, immutable source of truth, updated in real time and accessible by all parties.

When these kinds of efficiencies are applied to international supply chain logistics then it's clear to see how organisations might save significant amounts of money and time. And there is an added advantage in that these shared ledgers are more secure and transparent than other systems. At least, that's the theory.

There is a counter-argument that says that the blockhain's inherent immutability makes it susceptible in the face of human fallibility. In other words: it's very hard to correct a mistake once it's on the blockchain; and if that mistake involves legal or compliance oversight then it could prove extremely costly.

Other critics point to the fact that the adoption of new technology at scale is hard (especially at the scale at which blockchain technology becomes genuinely useful) and question the amount of data that would need to be transferred and the level of buy-in needed across multiple parties in order to create a fit-for-purpose supply chain ledger.

Improved infrastructures in the real world: Lemonade Crypto Climate Coalition

Insurance is one of the fields in which blockchain technology is already helping to streamline existing processes and reduce friction. By providing every party, from the insurer, to the underwriter, to the insurance buyer, with a single source of truth, data reconciliation is simplified, greater accuracy is achieved and there are cost and time efficiencies at every touchpoint.

New York City-based insurtech, Lemonade is a public benefit corporation and a certified B-Corp, which pays unused premiums back to nonprofits chosen by their customers. As part of their stated mission to 'transform insurance from a necessary evil into a social good' the insurer has also established the Lemonade Crypto Climate Coalition, which aims to harness blockchain technology to help protect vulnerable communities from climate change.

Traditional methods of distribution, pricing and claim handling make insuring smallholder farmers in low-income countries financially unfeasible; a problem which is exacerbated by the lack of meteorological data in the region. The upshot is that, in 2021, less than than 3% of the African farmer population was able to obtain agricultural insurance.

The Crypto Climate Coalition seeks to accurately quantify weather risks; automate claim assessment; and provide adequate funding and reinsurance to smallholder farmers by employing technology such as use of autonomous smart contracts programmed with actionable weather insights. This new infrastructure will allow for automated claim assessment, bringing the cost of handling claims down to zero and allow farmers to be paid without them ever needing to file a claim.

Some other examples from the present

The Ethichub project is a Spanish startup that began in December 2020 with the aim of helping coffee farmers in Mexico overcome their financial exclusion. The blockchain-enabled crowd-lending platform directly connects small farmers with financing and a more equitable supply chain, opens up international markets for their production and increases the price paid per kilo. Over time they can also create a credit history for farmers, which improves their loan conditions.

Molecule is a DAO that has been established to create collaborative ecosystems with the aim of streamlining the process of bringing new drugs to patients. They do this by transforming intellectual property into an investable asset.

What could the future hold?

Where we could end up

The first scenario in our speculative futures exercise explores a future where Colombia has employed the use of a new Web3 cooperative model to ensure food and water security.

Building on the idea of decentralised and autonomous cooperatives, this scenario speculates that these groups are able to protect and regenerate their rural territories through the development of new algorithms based on inclusive artificial intelligence, smart contracts and advanced sensors installed throughout the territory.

Meanwhile the operating permits of extractive companies are held on the blockchain, where a process of "eco-staking" allows for the preemptive offsetting and penalisation of environmental impact outside of permitted margins.

In the scenario we see how the installation and maintenance of this new agricultural infrastructure provides a new economy which supports young farmers, even those in remote areas. These new levels of awareness and accessibility are instrumental in replacing the existing 'neo-feudal' model with a more equitable system of land redistribution powered by immutable digital deeds, clean production certificates and 'contributory accounting'.

What's already in motion

Right now significant advantages are being gained by employing on-chain solutions in discrete, corporate or institutional environments. Whether it's keeping land registries, delivering remittance transactions, or managing international logistics; shared ledgers can simplify existing processes that are currently steeped in bureaucracy and inefficiencies.

Those self-contained ecosystems that may have become bloated with legacy methods and clogged with multiple gatekeepers are ideal testing grounds for Web3 solutions, and we're already seeing certain industries trialling those solutions in distinct and targeted ways.

However, If we want to see these kinds of changes implemented on a wider and more interconnected stage, then that will require widespread buy-in, trust and political will, both from governments and the entities who traditionally regulate these activities. Right now, it's arguably the case that many companies prefer their data to be centralised and obfuscated to avoid the risk of corporate espionage

Without some kind of transformational leap though, there is a risk that blockchains will remain largely privatised and private blockchains are, by definition, opaque and only serve to centralise power for the blockchain owner.

Next steps to designing the future

It's easy to see why a private company might install Web3 technologies in order to reduce waste and increase efficiency. But if we desire a future where digital infrastructures are designed, implemented and maintained in order to empower the kind of non-geographical governance and decentralised communities discussed earlier, then it’s vital to answer a few key, foundational questions.

How might local knowledge and context sensitivity be prioritised in a technically mediated environment in which all actors are considered to be equal? How could complex and transitory contextual information be introduced into such a system? What mechanisms could be introduced in order to overcome the differential access to digital rights and privileges that currently exist? And which organisation or nation (if any) would or could assert sovereignty in an international system of smart contracts?

SECTION THREE

Identity politics

One of the most dystopian perspectives of Web2.0 is that it made us all labourers in the data economy.

As we transact and interact across the web, our personal data is collected by privately-owned platforms in mostly non-transparent ways and then monetised and even sometimes weaponised against us (in the last eight years Russia has passed a data localisation law that forces companies to hand over information of internet users to security services, a stored communications law that requires telecom operators to keep user communications for 30 days, and a sovereign internet law that grants the government powers to partition Russia from the rest of the Internet).

As participants in this value exchange we are also asked to put our trust in private corporations whose duty it is to safeguard our data from malicious actors. That trust has been repeatedly betrayed.

Up until now, data privacy has been at the mercy of political institutions and the regulatory requirements they have placed on companies to try and ensure basic rights such as access to and erasure of data. But legislation has its limitations. Privacy policies and T&Cs forms are not read or understood by those they are meant to benefit, and cookie pop ups utilise ‘dark patterns’ designed to fool users into making poor decisions

One of the primary features of Web3 is that it replaces centralised data repositories with a decentralised data layer meaning that values of data ownership are baked into the very core of its architecture.

Just DID it

Self-sovereign identity (SSI) is a method of identity that, very simply, gives individuals greater control over what information they share. By taking the central database (and its gatekeepers) out of the equation, SSI allows for user-controlled relationships, where information can be exchanged in a secure way that safeguards the privacy of those involved.

Web3 technology makes SSI possible because it is inherently distributed, decentralised and immutable. That means that when an ‘issuer’ (a corporation or government department) wants to provide some sort of credential (e.g. a loyalty card or a drivers licence) they ‘sign’ it with their Digital ID (or DID), which is associated with their public key on the blockchain. The person receiving the credential (the ‘holder) also has a public Digital ID on the blockchain, so when anyone needs to verify the credential all they have to do is check the blockchain to make sure that the DID on the ledger matches the ‘signature’ on the credential.

In short: SSI allows a holder, issuer, and verifier to all have the same single source of truth about which credentials are valid and who authenticated the validity of the data inside the credentials.

Probably the most attractive potential benefits of SSI are digital minimisation and interoperability. If a platform requires you to be over the age of 18 to access it, then does it also need to know which country you reside in? Does it even need to know if you’re 19 or 89? SSI allows a user to give up the least possible amount of information to another party. While interoperability means that, instead of generating distinct, centrally-stored identities for every service, users only have to create one digital identity and then use that verified ID over and over again to access multiple services.

Data sovereignty in the real world: WorkPi

How many times have you stopped short of being completely honest when giving feedback at work, even though you were assured the process was completely anonymous?

WorkPi is an employee assessment platform that uses SSI alongside learning and development algorithms to allow employers to gather reliable, anonymous insights into the performance of their workforce, as well as giving employees the opportunity to take part in assessments and e-learning in a secure and private way.

WorkPi stores personal data such as assessments, diplomas, certificates, peer reviews and references in self sovereign identity wallets that are owned by the employees. That same system also allows for all management insights to be anonymised which the company claims could lead to the removal of bias in employee development decisions and job matching suggestions.

The level of security and anonymity baked into the architecture also means that the company can combine anonymous employee data from multiple companies and industries, so that their AI can create new insights from across the ecosystem.

Some other examples from the present

Magic Auth is an authentication software development kit (SDK) that allows apps to integrate web2-like, passwordless user logins through ‘magic links’ that are also Web3-compatible. When a user logs into a decentralised app with Magic they are automatically generated a wallet making Web3 onboarding much simpler.

Microfinancing through decentralised financing has traditionally faced one large stumbling block: over-collateralisation. Anonymised borrowing rules out credit checks and income verification, so borrowers are asked to put down collateral assets that exceed the total value of the loan. But the types of consumers or businesses looking for microfinancing solutions typically can’t afford to over-collateralise. This challenge is being solved by identity layer protocols that assess credit behaviour solely through a unified wallet address. 3air is a blockchain platform that aims to bring affordable, high-speed broadband to developing countries. As an issuer of DIDs they are also exploring how they can build a credit score model that will allow them to provide microloans.

What could the future hold?

Where we could end up

In the speculative future titled *Dispossession and Hope* we explore how climate change affects patterns of migration and how Bitcoin redefines ownership.

In this future, natural disasters create a migratory crisis causing governments and state services to collapse. This accelerates the decentralisation of social and health systems and the adoption of immutable digital identities, as displaced families look for ways to keep track of the health, economic and general status of their loved ones abroad, and organisations seek ways to reduce neo-slavery and human trafficking.

As failed states and old political borders are dismantled a new, decentralised set of bioregions emerges, redefining local community identities. These transnational communities are able to grow and flourish thanks to a transactional network built on the Bitcoin protocol and an AI security framework that is fed with anonymised social data that manages capital allocation, anticipates migratory flows and mediates the resolution of conflicts between nations.

What's already in motion

The COVID-19 pandemic accelerated the pace of innovation around mobile identity technology, and this acceleration was catalysed in June of 2021 when the European Commission introduced a legislative proposal for a European Digital Identity Wallet (DIW), which would be made available to all EU citizens to allow them to prove their identity and share information.

Crucially, very large platform providers (those with more than 45 million monthly active users) will be mandated to accept the EU DIW and this could be instrumental in breaking the current 'chicken and egg' deadlock where both the users and the platforms want the other to be present before committing to the ecosystem.

The EC plans to mandate member states to offer a EU DIW at the beginning of 2024, and just a few weeks ago they provided an update on the technical specifications and architecture at the Trust Services Forum in Berlin.

The EU DIW and the regulatory framework that sits around it could be the global vanguard for widespread understanding and adoption of data sovereignty and digital IDs. This momentum was given a healthy nudge just a few days ago when JP Morgan announced it was developing a Web3 digital identity solution, which would allow users to "traverse across digital realms" using a single digital identity. Meanwhile, in the UK, the global identity verification provider ID-Pal announced that it is now a government-certified identity service provider for digital right to work and right to rent checks in the UK.

Next steps to designing the future

The two biggest challenges to the widespread adoption of decentralised data are regulation and trust.

The first challenge can be met with a solid framework with clear rules and constraints. Indeed, as well as the European Digital Identity Wallet (DIW), the European Commission is currently working on the European Self Sovereign Identity Framework, which aims to provide just that.

The issue of trust seems is potentially a more complex one, as it's connected with decentralised data's perceived links to cryptocurrency and NFTs, two highly controversial technologies that are widely regarded as complex, exclusionary and opaque - the very opposite of the values which SSI projects seek to promote.

In order to drive widespread understanding and adoption of data sovereignty it may first be necessary to understand how the conversation around digital identity can be focused on encoding social relationships of trust, (rather than on financialisation and issues of ownership), how the mechanics of digital identifiers can be clearly presented, and how data autonomy can be given back to the individual while ensuring that more technical tasks (e.g. the recovery of data in the event of a lost key) can be safely and confidently carried out by the average user.

SECTION FOUR

Attack the blockchain

One of the key espoused benefits of the blockchain is that its design makes it theoretically impervious to compromise.

Each block, or data record, is digitally signed with an algorithmically-generated 'hash' based on the contents of the record and every other record in the blockchain. If any of the records are changed, the hash will change and the modification will be detected.

This inherent security system solves many of the of the existing vulnerabilities of Web2.0, making services more resilient to threats such as malware, Denial of Service and other common attacks. However, the introduction of this solution allows a whole new set of vulnerabilities to pop up.

Security whack-a-mole

Common cybersecurity attacks in Web2 include man-in-the-middle attacks (in which the the attacker inserts themselves between two legitimate parties and relays messages between them to fool them into believing they are communicating directly to each other over a secure connection) and the 'injection attack', where malicious actors smuggle code into an application and then control the flow of data through that app.

Web3 is not as vulnerable to these types of attacks, because unexpected inputs on the blockchain are detected immediately and any unintended commands would fail to execute.

Similarly the 'brute force' strategy of a Denial of Service attack would struggle to gain a foothold in a Web3 environment as blockchains protect themselves from excessive use by increasing transaction fees in line with demand, making DoS attacks costly endeavours.

The decentralised nature of Web3 also solves Web2's 'trusted execution' problem which requires an app to trust that the operating system and hardware it is running on is uncompromised. In a Web3 environment, where execution is decentralised and code is executed in parallel, each 'node' must agree on the result of the execution or it doesn't happen.

So how did the Web3 space lose $1.48 billion to malicious attacks and exploits between January and May 2022 - with $1.20 billion of that number coming from just four 'super hacks'?

Multiple crytpo projects have suffered so-called 51% attacks over the past few years. In these instances, over 50% of a blockchain's hashing power comes under the control of a single entity, which allows a malicious actor to block new transactions, change the ordering of new transactions and reverse their own transactions, so they can 'double spend' their currency.

Most cryptocurrencies are safe from this kind of attack as long as there's no collusion among miners. But if hackers conspire to achieve that majority control then it can be extremely lucrative.

Earlier this year hackers executed the largest of those four super hacks, stealing $625 million from the online game Axie Infinity by hacking into its underlying Ronin blockchain and exploiting its 'bridge,' the interoperability protocol that allows users to transfer their assets from one chain to another.

To do this they instigated an elaborate phishing scheme involving a fake job offer sent via a PDF that was laced with spyware. That spyware allowed the hackers to obtain over 50% control of the games 'Proof-of-Authority' validators and drain Axie Infinity's treasury.

One important thing to note here is that Axie Infinity had nine validators, meaning that the hackers only needed to take control of five of those validators in order to control the underlying blockchain. To repeat this hack on the bitcoin blockchain would require 51% of the electricity being utilised by every bitcoin miner in the world (as bitcoin uses Proof of Work validation).

However there are important ramifications here for the underlying structure of the blockchain and the future of interoperability. Even before the Ronin hack. Ethereum founder Vitalik Buterin had said that there are "fundamental security limits" to bridges that make him "pessimistic about cross-chain applications".

In August of this year, another cross-chain bridge was attacked when an update introduced an error into the system allowing hundreds of exploiters to remove $190 million in value from the blockchain.

Securing information in the real world: Land restitution in South America

Away from the world of digital currencies, blockchain is already playing a part in certain branches of public services, where its levels of transparency, immutability and security are being leveraged around tasks such as the management of public records. In Colombia, for instance, blockchain technology has been incorporated into information management processes at the National Land Agency.

What started as a research project between innovation lab ViveLab Bogotá and a research group of the National University, culminated in July of this year with Colombia's National Land Registry being deployed on Ripple's XRP ledger.

For the past few years the National Land Agency has been prototyping the integration of Web3 technology into the land restitution process. After the stage at which a judge has issued the resolution to restore land, the data of that property and its owner are recorded on-chain where it is not only protected by cryptographic methods but also by biometric verification (facial recognition). This allows for land registration records and property histories to be accessed much more widely while reducing the risk of the modification or falsification of that information.

Allowing wider public access to broader and more sensitive levels of information across the public sector should aid in the fight against corruption, especially when combined with the implementation of smart contracts, which can automate capital flows and ringfence them with fixed guidelines and parameters.

Some other examples from the present

Smart contract audits are essentially detailed code reviews of a project's smart contracts, designed to safeguard the funds invested in them. Some of the biggest players in this space today include blockchain security company CertiK (founded by Yale University and Columbia University professors in 2018) and

Estonian cybersecurity firm Hacken who published their smart contract audit methodology on Google Docs.

Blowfish is a Web3 firewall, an API that can be added to crypto wallets to protect their users against phishing, software supply chain attacks etc and identify malicious transactions in real time.

What could the future hold?

Where we could end up

In the last of our far-future scenarios, robotic and automation solutions have been decentralised through a distributed data system that makes hacking a single server redundant.

By integrating multiple 4.0 technologies, like artificial intelligence, the Internet of Things (IoT), and Blockchain, this emergent market of robotic services rapidly underpins most complex production processes and eventually develops the ability to perform transactions across a network of cryptocurrencies.

As an example, an autonomous vehicle is able to manage its own wallet allowing it to interact independently with charging stations or vehicle repair robots. However, once metaverse avatars are also gifted autonomous capabilities, they begin to trade with other autonomous AIs in the real world at the speed of light and this causes an employment crisis.

Ultimately a bug in the Linux operating system causes significant quantities of many cryptocurrencies to vanish overnight, and the impact of this is felt on a global scale, both in human and robotic economies, with experts predicting that the effect on global supply chain will set the world back 15 years.

What’s already in motion

Ironically, recent significant exploitations of blockchain vulnerabilities seem to have prompted the Web3 ecosystem to look to more traditional means of cybersecurity.

Up until recently, the attitudes of Web3 development have led to a general distrust of established infosec methodologies and a desire to reinvent the security wheel. This meant relying on the knowledge and goodwill of decentralised communities to prevent, detect and patch vulnerabilities.

Mindsets may have shifted somewhat after it emerged that it took six days for Axie Infinity to realise it was being robbed to the tune of $625 million.

Blockchain security experts are now calling for the Web3 ecosystem to deploy a Web2-style ‘full security mindset’, while a renowned hacker who claimed a $2 million ‘bug bounty’ earlier this year recently criticised Web3 companies who try to “externalise the cost of their core design to people being only indirectly compensated, rather than building a team around mathematicians, economists, and security experts.”

This trend is reflected in the growing numbers of infosec jobs that are being posted in the Web3 field, and has been strengthened by security firms calling for increased regulatory security requirements and the standardisation of security audits.

Next steps to designing the future

Although the most high profile Web3 attacks have centred around stolen cryptocurrency, there is an increasing focus on emerging forms of 'governance attacks' such as vote stealing.

As all token-holders within DAO or other decentralised communities are able to influence the mechanisms of the community, this presents an opportunity for malicious actors to swing votes, put themselves in positions of power and then loot treasuries or introduce self-serving policies.

The stablecoin protocol Beanstalk became the victim of a governance attack earlier this year after a hacker took out a flash loan to exploit their protocols. A flash loan allows a user to borrow large amounts of uncollateralized cryptocurrency capital to make a transaction, and then pay back the capital plus a fee once the transaction is made. In this case, the attacker used that stake to give themselves a disproportionate amount of voting power and then wielded that supermajority vote to award themselves $181m from Beanstalk's treasury.

If we replace the word 'Beanstalk' in that last sentence with 'the Government' then we begin to get a very clear picture of the questions we have to ask ourselves when we are designing the governance tools and standards of the future.

For example, how do we ensure that collective, decentralised decision-making can take place at scale and at speed, while also ensuring there are sign-off gates and checkpoints that will deter and block malicious actors? And how do we go about building truly democratic and transparent governance systems through Web3 while mitigating the potential for hostile proposals and the kind of 'digital coup' that could see those proposals executed and enacted automatically?

SECTION FIVE

Shaping the future of Web3

What have we learned?

One of the stated aims of the Framing the Future symposium, was to “move beyond the hype of NFTs and Bitcoin to have a nuanced conversation about the future potential of Web3”. More specifically, we wanted to explore the benefits of these new technologies in the context of “solving big global challenges”.

The table below summarises the shortcomings of the existing Web2 landscape, the core ‘building blocks’ offered by Web3 technology, along with the solutions and capabilities they may provide to answer those shortcomings; and, finally, some of the potential risks that we must be aware of when beginning to explore these solutions further.

	Cross-party processes & logistics	Cross-border collaboration & coordination	Security & privacy	Data ownership
Web3 building block	Shared, transparent and immutable ledgers held on the blockchain, which allows for transactions to be independently confirmed and validated without having a third-party witness and approve the transaction.	Decentralised autonomous organisations (DAOs); democratic structures that have no central governing body. Smart contracts in which the rules, values and aims of the organisation are immutably embedded.	Consensus algorithms: a general agreement between nodes on the network that a change to the ledger is acceptable. Built on 'proof of work' and validation of 'hashes' (the algorithmically generated digital signatures attached to each 'block' on the 'chain'.) Zero-knowledge proofs: Eliminate the need to reveal 'Personally Identifiable Information' by proving the validity of a claim (country of residence, currency transfer etc) without exposing the information used in creating it.	Self-sovereign identity (SSI): A user-controlled identity system that gives participants autonomy and freedom from intervening administrative authorities. SSI systems managing digital identities through the use of Decentralized Identifiers and Verifiable Credentials, both of which utilise cryptography to ensure integrity.
Existing Web2 scenario	Bureaucratic, top-heavy systems that contain single points of failure; and which may struggle to capture and repurpose the wealth of data generated across them. Siloed database architectures that are often not interoperable causing fragmentation and significant inefficiencies through duplication of data, data entry errors, etc.	Centralised authorities making decisions based on the needs of their locales, within a hierarchy that can be exploited (from Elon Musk suspending journalists on Twitter, to despotic regimes).	Apps and services are vulnerable to malware, Denial of Service attacks, and the 'trusted execution' problem, which requires an app to trust that the operating system and hardware it is running on is uncompromised.	Personal data is collected by privately-owned platforms in mostly non-transparent ways and then monetised and even weaponised. Private corporations are entrusted with safeguarding user data and we rely on political institutions and regulatory bodies to ensure basic rights such as access to and erasure of data. Users have to create distinct, centrally-stored identities for every service they use, and repeatedly sign in with platform-specific credentials.

	Cross-party processes & logistics	Cross-border collaboration & coordination	Security & privacy	Data ownership
Web3 benefits	Reduces waste, increases efficiency, and is more secure and transparent. No single point of failure, and 'middle men' are replaced by a single, immutable source of truth that's updated in real time and accessible by all parties.	Allows for decentralised decision-making across geographically scattered communities.	Theoretically impervious to compromise. Execution is decentralised and code is executed in parallel, so unexpected inputs are detected immediately and unintended commands fail to execute.	Replaces centralised data repositories with a decentralised data layer so data ownership values are baked into the very core of its architecture. Users decide how and what information they want to share and information is shared only with explicit user consent. Users choose which applications will be unlocked by which of their DIDs, allowing them to balance portability and convenience with privacy and security.
Potential risks	Inherent immutability makes it susceptible in the face of human fallibility (i.e. it's hard to correct mistakes). A decentralised system relies on an (often complicated) protocol to resolve disputed data (not a central authority). Huge amount of buy-in required to a create a fit-for-purpose supply chain ledger.	DAOs can be slower and less efficient than other organisational systems and aren't regulated in the ways we've come to know and understand.	If hackers conspire to achieve majority control of a blockchain's hashing power then it can become vulnerable to attack. The very 'bridges' that allow different blockchains to talk to each other can provide weak points for these kinds of malicious actors.	No current regulatory framework with clear rules and constraints (the European Commission is working on the European Self Sovereign Identity Framework). Trust and decentralised data's perceived links to cryptocurrency and NFTs, two highly controversial technologies that are widely regarded as complex, exclusionary and opaque.

During the week our symposium took place, three events occurred that significantly shifted the space we were exploring as we were exploring it.

First, Elon Musk (newly installed at the helm of Twitter) completely dismantled Twitter's existing verification system and then delayed and revoked the new system, not once, but multiple times. The roll out was so disastrous that, by November 10, hundreds of trolls were using the new verification process to impersonate many notable accounts from Elon Musk himself to George W. Bush; and causing masses of users to begin using open-source and decentralised alternatives such as Mastodon.

At the same time, Sam Bankman-Fried (the founder and CEO of the cryptocurrency exchange FTX) went from declaring his company's assets "fine" on November 7, to beginning voluntary Chapter 11 proceedings and resigning as CEO just four days later. On days two and three of the symposium, rival company Binance went from announcing a deal to acquire FTX, to pulling out when due diligence suggested the mishandling of funds.

Finally, Facebook's parent company Meta cut its headcount by 11,000 employees, citing falling revenues and increased competition for the decision.

What's interesting is that, when it came to discussing the inherent possibilities of the next iteration of the web, these developments did nothing to dent the enthusiasm and the optimism of our delegates or our speakers. On the contrary, they only seemed to confirm how important it was to be able to begin "sorting the signal from the noise" made by these tectonic shifts. Far from being seen as kind of digital death knell, they were recognised as marking the beginnings of a profound renaissance in web culture.

While Musk's bungled Twitter takeover served to confirm a growing mistrust of 'big tech', the collapse of FTX seemed to expose the flimsy ideology of crypto-libertarianism and strengthen the argument for a more formal and extensive regulatory structure. The layoffs at Meta meanwhile suggested a broad shift back to the 'open web' and a desire for the next wave of digital innovation to be built on a new set of frameworks that allows users to control their data, to form communities that can easily collaborate, and to be able to move between those spaces freely, without having to ask permission.

The question we are seeking to answer now is this: How might we take advantage of this moment of possibility and begin to shape this future of what Dame Wendy Hall calls 'our digital planet'?

As HMRC Technology Lead, Nick Davies, said on the final day of the symposium, there is a real policy delivery opportunity in front of us here. As more legislative frameworks slot into place around the globe, the implications of Web3 to transform not just systems of trade and commerce, but also the foundations of our policies and our democracies, are becoming increasingly evident and palpable.

To take full advantage of this moment there is a role for a catalysing force, something that can bring together the technologies, policies, standards and legislation to ensure they are focused and aligned towards a sustainable and equitable future.

FCDO is both part of the UK Government and a close collaborator with many other governments globally, making it uniquely placed to drive an ambition of this kind. By testing new ideas, taking reasonable risks and learning quickly in order to establish governance structures, it can enable and support innovation through its international network of innovators, tailored support programmes and policy teams.

This view was echoed by those who took part in our Web3 symposium, with both attendees and speakers calling for the FCDO to "play a positive" and "active" role in "designing the future". They recognised that this role should involve "regulating the technology and supporting emerging ideas," and "ensuring standards and interoperability of different technologies and systems," as well as "discussing the ethics" that surround all these issues.

These voices stressed that the FCDO was well placed to take on this role as it could look to "improve outcomes without going into fully decentralised mode" and would be able to "host conversations in a way that's separate from politics" while seeking to "understand the constantly changing standards in the crypto and Web3 space, in order to regulate it."

Set a bold north star ambition for innovation	FCDO as the catalysing force towards a sustainable and equitable future for our 'digital planet'.	
Create the enabling environment for responsible innovation	Develop Web3 sandboxes	Establish standards
Fund innovation	Web3 funding to create a portfolio of web3 tests across three types of innovation • Cross-border and Mass Collaboration • Novel Use Cases and Weaving Web3 into existing tech • Governance	
Wide Participation	Put in extra effort to get and test ideas from those typically more marginalised whose voices are currently missing from shaping the future of the web, especially women in Africa, S. Asia and LatAm	

Create an enabling environment for responsible innovation

To begin building the environment that will enable this ambition, we have mapped out a two-pronged approach to creating the controlled environments needed to unlock Web3's potential in the smartest and safest way.

We believe this approach provides an opportunity to collect and act on empirical data and to deepen our collective understanding of the opportunities created by Web 3, while also exploring the long-term implications:

Enable innovative, safe testing & learning

Today, few real-world Web3 applications (beyond the trading of speculative assets) have been deployed and there is a lack of viable, easily-communicated use-cases. This has contributed to a lack of understanding and trust in the technical capabilities of Web3.

But, use-cases cannot be defined before we know what it's possible to achieve, and although we are at an undeniable inflection point right now, the capabilities and the limitations of this technology still need to be teased out and assessed across a number of environments and contexts.

The term sandboxing is borrowed from the world of software testing where it refers to a closed environment in which untested code can be executed without it affecting adjacent programs or network components.

Sandboxing potential Web3 solutions means testing new approaches in a controlled, real-world environment in such a way that all aspects of how the idea would behave in the real world can be seen and measured, but in a protected way so that safe mistakes can be made, the impact of innovation can be assessed, and any risks can be revealed.

Most importantly, it provides an opportunity to rapidly discount ideas that have a high potential for harm or vulnerability to misuse. In this safe environment, we can accelerate the identification of attributes or programmes that could have potential impact for global challenges and quickly rule out any that present high risk or low benefit.

Each of our sandboxes would be themed around the three areas of innovation detailed below (in the section titled 'Funding Innovation'). Within these domain-specific sandboxes, our innovators will experiment with different solutions based on the challenges that each domain presents. From our work so far, it is likely that we would begin by addressing these key challenges presented by Web3's underlying infrastructure:

Cost of entry: The computational resources and ongoing maintenance requirements needed to verify transactions or write data on blockchains currently risks creating an uneven distribution of access to Web3 technology as well as the power to use and shape it. To that end, our sandboxes would not only provide the opportunity to innovate in an economically viable way, but would also accelerate solutions which provide a more equitable access to the technology.

Environmental impact: Even considering the recent shift to the less energy-intensive Proof-of-Stake (PoS) method of validation, there are still legitimate concerns around the long-term climate-impact of blockchain and the potential centralisation of power into the hands of those who are capable of meeting those escalating power requirements. For example, an innovation project focused on cross-border collaboration and coordination would have to be assessed on its ability to disincentive centralisation and use less energy, while still retaining speed and trust of validation (for example, when executing voting mechanisms).

Interoperability: As we explain in the section below, a key priority with this fund would be to design an open ecosystem, moving away from a series of siloed, privately-owned innovations to an interconnected network of decentralised spaces in the public domain. As a result, our projects must be measured on their ability to balance stability and usability and their potential to scale while retaining the required levels of transparency.

Establish standards

Developing standards in an early, iterative manner will not completely stop conflicts arising between different legal and regulatory regimes, but it will offer useful early insight into the kinds of challenges that will arise.

To accelerate this process, we would recommend initially building these standards around those established by Digital Public Goods Alliance, as they have been designed to advance the creation of safe, trusted, and inclusive digital public infrastructure at scale and are in line with the UN Secretary-General's Roadmap for Digital Cooperation, and the activities of the Global Digital Compact and the Summit of the Future in 2023.

We would apply and test these standards in a number of fundamental areas, which we believe are key to catalysing safe and sustainable growth in this space:

Transparency and usability: Introducing more technology into a solution risks making it more abstract and blocks it from empowering or equipping those it was designed to help. Also, a lack of transparency and portability can increase the complexity of any transition or decommissioning phase, minimising the sustainability of the programme.

Collaboration across borders: Legislative and regulatory differences across borders already cause both service readiness and human-rights problems for the roll-out of technology-driven services; and adding Web3 into this mix will undoubtedly create more complexity. We are also acutely aware that equitable access to the benefits of technology within global diplomatic initiatives also requires scrutiny and accountability to avoid the creation of new injustices, and lay the path for new problems.

Preparing for Web3 multilateralism: As we say later in this document, it seems very probable that decentralised governance will create mechanisms for forming more equal, collaborative partnerships that facilitate new ways of building alliances and sharing resources between states. These new opportunities for political partnership will require a new form of cyber diplomacy, underwritten by national security considerations, global ambitions, and issues such as the right to self-defence, international humanitarian law, and the use of countermeasures.

Funding innovation

In order to populate these environments with the kind of transformative thinking and interconnected innovation required, we recommend funding a portfolio of Web3 tests across three types of innovation.

Below we have outlined the three areas of innovation that encompass the core opportunities uncovered during our recent work; and which we believe are critical to forming the foundational elements of a transformative and sustainable digital ecosystem and which will therefore drive the structure of our initial innovation sandboxes.

New forms of cross-border & mass collaboration

It's clear that structures such as DAOs will play a crucial role in driving the adoption of Web3 technologies in the long term. These decentralised communities have the potential to drive significant social and political change and develop new forms of transnational collaboration, significantly accelerating the pace of innovation and research around the globe.

As new mechanisms emerge for forming more equal, collaborative partnerships and new ways of building alliances and sharing resources across borders, power maps will be redrawn and new trade routes and data flows will be created alongside new opportunities for political partnership.

A failure to engage with these new patterns of cyber diplomacy, and their implications on areas like national security and humanitarian law, might risk depletion of soft power in the long terms, placing us on the backfoot when it comes to navigating these new global democratic and legislative landscapes. Similarly, as these autonomous communities attain levels of cross-border influence, we must begin to build the safeguards that will protect them against bad actors, while retaining the core principles of accessibility, openness and transparency.

One only has to look at the progress of the Online Safety Bill to see how delicate and difficult this process can be. But, at the same time, there is an undeniable opportunity to begin to define what a more just and sustainable democratic infrastructure might look like; and the FCDO, with its unparalleled experience and access to talent, is uniquely placed to explore those possibilities.

That's why we believe that the third of our strategic innovation spaces should be dedicated to harnessing the long-term sociocultural shifts and building the inclusive, highly effective and people-centred global democratic infrastructure.

Governance & legislation

If we accept that DAOs may become the organising structures and governing bodies of the Web3 era, it's important that our portfolio is focused on this key area of innovation and that that focus should (initially at least) revolve around testing the organising structures, legislative, regulatory and economic frameworks that will allow these entities to create significant value.

While it's true that technology has outpaced regulation in this area, this has created an opportunity for technologists, regulators, and entrepreneurs to come together to navigate this frontier in a controlled and secure environment and to begin to map out the founding principles that will guide how areas such as democracy, investment, business and entrepreneurship will function in the near future.

To do this we would have to approach some large questions, including:

What bridges between DAOs and 'off-chain' assets need to be created, and how will liabilities and responsibilities transfer from one world to the other?

What does best practice look like when it comes to the structure and user experience of a DAO?

What should the legal relationship be between a DAO and its members who hold 'tokens' that grant them voting rights within it?

These questions would then have to be played out across a number of different scenarios and environments, in order to determine their effectiveness. For example, how do these legislative and governance principles hold up when applied to political lobbying, cross-border trade and investment or the activities of non-governmental organisations?

Novel use cases built on top of existing tech

Our recent work has made it clear that many of the existing examples of Web3 in action are, essentially, privately run enterprises or, at best, walled gardens. While this may be a necessary first evolutionary step for any nascent technology, it seems especially counterintuitive to the values and opportunities inherent in Web3.

Any attempt to test the validity of Web3 in the international development space must begin by designing a model capable of transitioning these environments from siloed spaces to interconnected, open spaces in the public domain. Spaces that have the potential and stability to scale to a global level while retaining failsafe levels of transparency and stability.

Key to this is balancing interoperability with platform dependency. The existence of multiple blockchains that aren't natively designed to talk to each other risks diluting transparency and scalability; and while there are 'leading' technologies, such as Ethereum, that power thousands of decentralised applications, the decision to rely on one blockchain platform could be both limiting and risky.

The good news is that Web3 has triggered a new interest in one of the foundational principles of the Web, i.e. the use of open source, interoperable components that can communicate and work with each other. This principle of 'composability' allows developers to quickly and easily extend the functionality of smart contract applications from across the blockchain ecosystem and integrate them into their own projects. This ability to compound innovation via common standards and 'extensible-by-design' contracts is increasingly being seen as a viable solution to the challenge of Web3's scalability.

We would also point to the increasing number of independent, third-party services capable of providing a bridge between real-world data and the blockchain. These so-called 'oracles' are able to act as intermediaries, funnelling and evaluating data from traditional systems like banks and corporations to the blockchain. And, because the services that make up these decentralised oracle networks (or DONs for short) are capable of serving multiple blockchains, they provide us with a valuable tool for creating greater interoperability.

As the Web3 ecosystem begins to transform into a network of interoperable ''building blocks' our portfolio would work to understand f the most valuable use cases of those building blocks and select which ones best suit our ambition of creating an open and equitable Web3 environment capable of unlocking innovative new use cases at scale.

Hybrid smart contracts are, at their core, simple software programs that trigger an action when they detect an event has occurred. They are 'hybrid' because they run on blockchain networks but are able to securely connect to 'off chain' (i.e. 'real world') data and systems.

By combining decentralised ledgers and external data, these smart contracts can verify real-world events and then use predefined logic to execute actions such as payments and penalties in a secure and transparent way. For example, hybrid smart contracts could be used to enable insurance contracts that automatically pay out when a certain weather condition is hit, or to underpin sustainable consumption incentivisation schemes through emissions level-based rewards.

When we look at existing FCDO projects (such as the Frontier Technology pilots that are utilising satellite and ground data to improve cocoa production in Columbia, or using hyperlocal weather data to protect communities in Nepal from landslides, floods and earthquakes) it's clear to see how they could be significantly enhanced by leveraging smart contracts to, for example, automatically dispense financial rewards to farmers, simplify traceability, or unlock financing towards improved irrigation systems for people living in floodplains.

Evolve real world applications

Although we have talked a lot about the 'concept' of Web3 and the 'idea' of decentralised communities, we must not lose sight of the fact that these technologies are tools to be employed in the real world in order to help solve complex global challenges.

Without real world, tangible applications, we will have no means of stress testing the stability of our building blocks or our governance models and we will never be able to drive widespread adoption, trust and understanding of what Web3 can do. By being proactive in testing across different use cases, and in whose voice is included in designing and deploying those tests, FCDO can play a vital role in the internet's evolution.

To kickstart this we will begin by employing Web3 technology in order to gradually evolve existing Web2 tools and services. We are not seeking to replace our existing digital toolkit with an entirely new and untested set of tools, and it's not our aim to evangelise for a Web3 'miracle cure'. Instead, our funded projects will focus on introducing the best elements of decentralised, open platforms and services in order to upgrade our existing capabilities.

Remembering that evolution very rarely happens in single, large jumps, our funded projects will look to influence the path of targeted and deliberate evolution through the iterative introduction of stable, tested and applicable elements of Web3 into our existing digital ecosystem.

One of the most exciting areas where Web3 technology could significantly enhance our existing online interactions is the space of online identities and digital wallets, and particularly how they relate to the mechanisms of democracy.

Today, our online identities are both increasingly necessary and increasingly fragile, with obtuse privacy policies and T&Cs forms employed by the privately-owned platforms we rely on, and identity theft becoming more pervasive and sophisticated (a problem that is predicted to worsen as we enter the age of the metaverse).

The decentralised method of identity known as self-sovereign identity (SSI) gives individuals greater control over what information they share by replacing the central database (and its gatekeepers) with distributed and immutable digital identification. In other words, a single, verifiable source of truth. This allows an individual to give up the least possible amount of information when verifying themselves with another party and, allows for more democratic services and experiences.

There are obvious possibilities here for providing transparency and efficiency in electoral and governmental processes such as the electoral roll and online voting systems. However, a point that was raised more than once during the Framing the Future symposium, was that widespread use of Blockchain and Distributed Ledger Technology could exacerbate digital divides, for example, in those areas where internet access is limited or where there is little clear understanding of Blockchain technology; or where there is a significant challenge in recruiting the public sector talent required to drive programmes around infrastructure, education and onboarding.

Decentralised digital identities are a crucial building block for our Web3 future - not only because they will play a critical role in our everyday interactions - but also because, if introduced successfully, they will go a very long way to drive public trust and confidence in these new technologies.

For that reason, it’s vital that we use this opportunity to explore questions such as legal frameworks, security risks, data governance and interoperability with existing services, across a number of foundational use cases, not least their application in our democratic practices.

Reshaping participation

Again and again throughout the four days of the symposium, the point was raised that the current Web3 conversation is dominated by an overwhelmingly male, Western discourse that largely arises from the finance and technology industries it purports to disrupt.

In order that we do not simply build into this existing exclusionary environment, and to ensure that our portfolio is able to galvanise diverse stakeholders and envision alternative approaches, we must bake in ways of debiasing our processes and encouraging a plurality of voices.

A portfolio structure engineered to give a platform to those who are typically more marginalised in this space (such as women in Africa, South Asia and LatAm) would include elements such as:

- The application of behavioural science in the call for ideas, to ensure it reaches and is heard beyond the usual tech bubble and usual suspects
- Rewards for female-led teams and teams from the global South as part of the selection process
- Proactive requests for ideas that positively impact girls and women
- A judging panel of at least 60% women

Crucially, this enabling environment and a means with which to use it, gives us the chance to foster the humble and collaborative culture this new era demands of us. We recognise that we are not going to get it all right, straight out of the gate but that we can learn from those mistakes as long as they are made in a safe, controlled environment, collaboratively and with a plurality of perspectives.

Structuring a Web3 innovation fund

Approach

In envisaging a fund to test and learn about Web3 and its potential based on the hypotheses set out above, our recommendations for the fund's foundational principles, its structure and costs, and how it might evolve over time are set out here.

Some of the key principles we recommend to underpin the fund include:

- Allowing enough time to test the fund hypothesis through 3 rounds of funding over 3 years
- Start with a relatively small fund to act as a seed fund that might grow, levering in further funding from key partners over time
- Attracting early-stage ideas with potential for scale, with catalytic funding and technical assistance
- Holding the response to the call as data in itself. Seeing who applies and what trends emerge from the ideas that are forthcoming will give us valuable insights
- Working with people who know Web3 but going beyond the usual suspects to those who would not typically have access to such funding or acceleration of their ideas
- Sharing learning along the way as a global good

Structure and costs

The fund will comprise financial support plus light touch technical support from proof of concept through to proof of scale. For the first set of 3 rounds, we recommended funding 25 ideas in total across the 4 topics outlined above, for a ticket size of approximately £40k. Starting with smaller cohorts then scaling up the size of each round.

To summarise

Ticket size: approx £40k

Number of funding rounds in the first phase of the fund: 3

Total number of ideas funded: 25

Initial duration: 3 years

Total fund: £1m (plus management fee)

Evolution

Over time we expect the fund to branch out into other areas of Web3 potential application, and will begin to leverage in other partners to the fund from ODA and philanthropy. It is also expected that the grantees will themselves begin to leverage in co-financing from public and private sources, or from service contracts with UK Gov and beyond to scale those ideas showing particular promise of impact at scale.