MITRE | Center for Strategic Competition

OCCASIONAL PAPERS, VOL. 1, NO. 5 - OCTOBER 12, 2022

DEMOCRATIZING TECHNOLOGY
WEB3 AND THE FUTURE OF THE INTERNET

by Charles Clancy, Christopher Ford, Michael D. Norman, and Sanith Wijesinghe

MITRE’s Center for Strategic Competition and the “Occasional Papers” Series

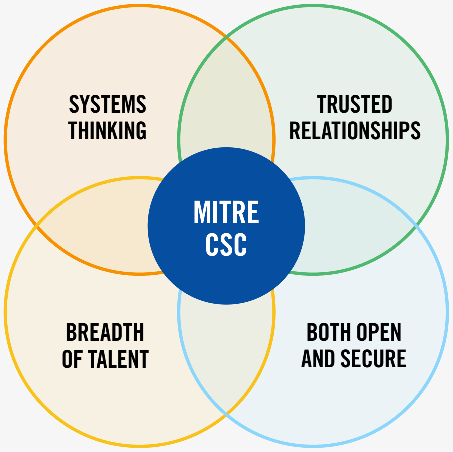
Today’s competitive strategy challenges are multi-faceted and complex. They exist in arenas of hard, “sharp,” and soft power—from military capacity, technological innovation, economic development, espionage, trade, and finance to cyber conflict, law enforcement, politics and culture, and diplomacy. Well-crafted competitive strategy requires a true system mindset.

Helping our country meet these challenges drives the work of MITRE’s Center for Strategic Competition (CSC). The CSC leverages MITRE’s six decades of systems thinking and systems integration experience on behalf of the United States and its partners, drawing upon the full range of capabilities that exist across the MITRE enterprise.

Much of what we do occurs out of the public eye for specific federal sponsors. Because strategic competition is a genuinely “whole-of-nation” challenge, however, it is essential to involve a wide range of stakeholders in devising and implementing systems-informed solutions.

CSC established this “Occasional Papers” series to engage, educate, and inform the policy community and the broader public about strategic competition issues, problems, and opportunities. We invite you to send feedback to strategic.competitor@mitre.org.

Why do we need the Center for Strategic Competition (CSC)?



Understand complex interactions between elements of a system and devise interventions to improve outcomes

Decades of trusted relationships with uniquely broad range of federal sponsors, and in coordinating partnerships among government, industry, and academic stakeholders

Data analytics, economic modeling, AI, behavioral sciences, intelligence analysis, system-of-system modeling, and decision-support tools

Cutting-edge analytic capabilities integrating unclassified and classified information and analyses

MITRE’s Mission

MITRE’s mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

Contents

Executive Summary 1

Introduction 2

Centralization, Web2, and the Rise of Authoritarian Tech Stacks 3

Decentralizing the Tech Stack 5

Policy Recommendations 9

Recommendation 1: Develop a combined national and economic security26 strategy that can maximize the benefits of a new decentralized payment system while mitigating illicit financial activities. 9

Recommendation 2: Advance global decentralized digital identity and digital data technologies to protect citizen privacy and enable the evolution of governance. 10

Recommendation 3: Promote accessibility standards to reduce burden of technology adoption. 10

Recommendation 4: Address the needs of the underbanked/unbanked by maturing prototype digital asset solutions. 11

Recommendation 5: Convene international partners and advance an inclusive vision to strengthen democratic values, protect citizens from threat actors, and develop and promote a decentralized, web3-facilitated response to the global growth of the authoritarian technology stack**.** 11

Conclusion 13

About the Authors 13

Endnotes 14

Executive Summary

The architecture of today's World Wide Web is, in many ways, an authoritarian one—built around a business model and technology stack that rewards vertical integration, massive aggregation of user data, and hyperscale centralized management. This architecture has provided benefits in terms of society-wide connectivity and scalable use cases, but comes at the cost of user privacy and autonomy, and domination of this crucial facet of modern life by a few enormous firms.

Worse, this architecture facilitates surveillance not simply by profit-maximizing hyperscaler service providers, but also—in authoritarian regimes—by the repressive state entities to which such providers are answerable. China, for instance, is harnessing data to manage and control the lives of its people by requiring them to use software that defines a new precedent for forms of automated social control.

The authoritarian cost of today's web2 architecture developments call for a response, but it is not enough to denounce the impact of the web2 technology stack on human rights, privacy, and democratic norms. We also need a better answer: the establishment and advancement of alternative technological paradigms to protect the public interest by making authoritarian misuse difficult or impossible.

Web3 technology can help provide an offset strategy to counter the rise of authoritarian and surveillance-facilitating regimes. This paper expands on previous MITRE publications discussing web3 by describing how earlier web-related technology stacks and economic modes have led to data centralization, and how much of this centralization within web2 can be unwound by web3; it also presents use cases where an alternative paradigm is already starting to take hold. Most visibly, this is already happening with decentralized finance and cryptocurrency, but web3 can decentralize any digital service.

As new protocols are considered for web3, this paper offers the following specific policy recommendations that complement government, industry, and academic efforts to advance this technology and increase user adoption:

- Develop a combined national security/economic security strategy that can maximize the benefits of a new decentralized payment system while mitigating illicit financial activities;
- Advance global decentralized digital identity and digital data technologies to protect citizen privacy;
- Promote accessibility standards to reduce burden of technology adoption;
- Address the needs of the underbanked/unbanked by maturing prototype digital asset solutions; and
- Convene international partners and advance an inclusive vision to strengthen democratic values, and protect citizens from threat actors, and develop and promote a decentralized, web3-facilitated response to the global growth of the authoritarian technology stack.

Web3 promises a future World Wide Web far different from the centralized, hyperscaled, and structurally authoritarian era of web2. It could form a robust and decentralized, democratized alternative to the existing technology stack, but there is much to do to make web3 a reality, make it safe and reliable, and equip it to fulfill its potential.

Introduction

On March 1, 2020, the New York Times published an article describing how China

> "has begun a bold mass experiment in using data to regulate citizens' lives—by requiring them to use software on their smartphones that dictates whether they should be quarantined or allowed into subways, malls and other public spaces."[1]

Furthermore, and more alarmingly, the article revealed that

> "analysis of the software's code found that the system does more than decide in real time whether someone poses a contagion risk. It also appears to share information with the police, setting a template for new forms of automated social control that could persist long after the epidemic subsides."[2]

This is only the latest element of a system of mass surveillance that the Chinese Communist Party (CCP) has been developing over several years. A Brookings report[3] details how some of the recent initiatives build on infrastructure developed pursuant to China's 2005 Skynet project that is used for surveillance in urban public areas. China's follow-on 2015 *Sharp Eyes* data fusion program, further, combines data from surveillance cameras to "collect facial and other attributes from key locations such as hospitals, schools, entertainment venues, hotels, internet cafes, major road intersections, and storefronts," all of which feeds into the government's surveillance system and mechanisms not merely for fighting crime but also for enforcing the CCP's idea of social "harmony" and suppressing political dissent and religious expression. Moreover, China is now actively exporting this surveillance technology,[4] thereby creating a playbook for other nations to follow in its authoritarian footsteps by facilitating mis/disinformation, political censorship, and propaganda.

These worrying developments cry out for a response, but it is not sufficient for us merely to decry their detrimental impact upon human rights and democratic values (in fact, this may make such technologies even more appealing to repressive regimes around the world, for whom this Chinese technology stack's authoritarian bent is likely to be a feature rather than a flaw). Instead, we need to come up with and promote an alternative technology paradigm. At its core, this paradigm should have a set of safeguards that protect the public interest by making it much harder—or maybe even impossible—for an authoritarian to use technology in a bad way.

This paper builds upon past MITRE publications discussing the promise and implications of web3, an evolution of internet protocols that aims to reset the creation, ownership, and transfer of value amongst creators and users without the need for platform-based intermediaries. The first paper on this topic called for a coordinated, whole-of-government national strategy to advance the regulatory landscape for digital assets, going beyond just cryptocurrencies, to include a myriad of new tokenized artifacts that have emerged to store and exchange value.[5] MITRE's second paper on web3 focused on the need to secure web3 and the cybersecurity challenges presented by different layers of the technology stack.[6]

This paper focuses on how web3 technology can provide an *offset strategy* to help counter the rise of regimes facilitated by a structurally authoritarian and surveillance-facilitating technology stack. Section 2 begins with an account of the evolutionary trajectory of web-related technology stacks and their underlying economic models, which have hitherto led to an ever-greater centralization of data. Section 3 then describes how we might *unwind* much of this centralization through the innovative new approaches of web3, and describes a number of use-cases where we are beginning to see such an alternative paradigm take hold. Because additional steps are required to advance this technology and increase user adoption, however, Section 4 describes a set of policy recommendations that complement existing efforts already underway by government, industry, and academia to this end.

Centralization, Web2, and the Rise of Authoritarian Tech Stacks

During the early days of the Internet, the World Wide Web was just one application among many that sat atop our technology stack. Leased circuits connected Internet Service Providers (ISPs), dial-up modems connected users to those ISPs, and universities, government agencies, larger companies, and ISPs together formed a decentralized fabric. The Internet Protocol (IP) connected devices together, and the Transmission Control Protocol (TCP) allowed applications to reliably communicate. This combination, TCP/IP, was, in effect, the glue of the Internet. A hallmark of this *web1* era was that all networks were equal—peers—and the Border Gateway Protocol (BGP) helped those networks understand their mutual interconnectivity to route data to its destination.

In the late 1990s and early 2000s, the advent of user-friendly search and e-commerce functions brought wide-scale commercial interest to the Internet, followed closely by social media. Between 1995 and 2000, the number of Internet users exploded, from 44 million to 413 million,[7] and the rate of data traversing the Internet increased more than 400-fold.[8]

This explosive growth gave birth to innovative approaches to scaling. Companies like Akamai created a market for caching the web's media content at hubs across the Internet, thus creating the first Content Delivery Networks (CDNs). Internet native companies realized that paying international telecommunications companies to route their traffic was cost-ineffective, and they soon created Internet Exchange Points (IXPs) near their data centers that directly peered with ISPs, often hidden from the global BGP routing tables. This knit data centers used by companies such as Amazon, Microsoft, Google, and Facebook directly into the fabric of the Internet, creating what we today call *hyperscalers*. Amazon was the first to realize that it could in turn sell access to this infrastructure to third parties, thereby giving birth to the cloud.

With this growth also came new methods of monetizing interaction. Advertising became the business model of the Internet, with search traffic and social media feeds providing data that permitted ever-greater targeting of advertising content to specific audiences—for which the advertisers would pay, thus allowing netizens "free" information access in return for the commoditization of their own activity and interest profiles. Targeting those ads motivated the creation of a vast network of data-harvesting tools that tracked users' interests and online activities and permitted ever greater refinement of this targeting model. With smartphones soon catalyzing the social-mobile Internet, in fact—moving it from the web1 era of more-or-less monodirectional information conveyance to the current web2 of user-interaction—users' entire pattern of life became available to and merchandisable by advertisers. This trend has been further exacerbated with the advent of Internet-enabled appliances such as refrigerators, microwaves, and home security systems.

IN THE LATE 1990S AND EARLY 2000S, THE ADVENT OF USER-FRIENDLY SEARCH AND E-COMMERCE FUNCTIONS BROUGHT WIDE-SCALE COMMERCIAL INTEREST TO THE INTERNET, FOLLOWED CLOSELY BY SOCIAL MEDIA.

The vast datasets created through the collection and commercial exploitation of user information have also been crucial to the Artificial Intelligence (AI) renaissance over the past decade, providing massive data pools that can be used to train AI algorithms. This data, combined with advances in graphics processor computing and new machine learning algorithms, is revolutionizing the field of AI, with exponential leaps in areas such as machine perception.

These developments have permitted remarkable advances in user experience and in the availability of a wide range of Internet-based or -facilitated services and applications. Nevertheless, this model has also come at a cost, since today's Internet is highly centralized. A handful of hyperscalers (e.g., private companies such as Alphabet/Google and Meta/Facebook in the West, and state-overseen technology giants in China) have vertically integrated fiber optic networks, data centers, Internet services, advertising, and AI into what are, in effect, massive conglomerates organized around a business model that inherently involves the centralized aggregation and analysis of everything that can be gleaned about the lives and activities of Internet users.

Naturally, however, this level of centralization has sparked questions about what our society should want and expect from our technology. Does this centralized technology stack provide the privacy protections citizens need in the modern digital economy? What protections are appropriate and what should privacy look like? Can technology be used to protect rather than exploit our civil liberties? How do we govern the increasing role of AI in these systems?

The European Union clearly feels that the centralized technology stack of web2 does too little to protect citizens and has attempted to answer some of these questions with its General Data Protection Regulation (GDPR). GDPR went into effect in 2018 and claims to be "the toughest privacy and security law in the world."[9] Nevertheless, GDPR's implementation remains clunky. Most users experience GDPR through frustrating website cookie banners that give the appearance of choice in how their data is handled, but may in practice change little, to the degree that surrendering control of personal data is often still the price of admission for Internet services and applications that most consumers have long since become accustomed to using and would be very uncomfortable living without. Cookie banners are in effect no different than accepting and agreeing to terms of service by clicking "yes" on apps and downloads.

While privacy debates and the implications and externalities of the hyperscale business model continue to roil the West, China has seized on these trends. Centralization is great for autocracy, and—at least as long as its own instrumentalities sit at the center of the system—Beijing finds the idea of a centralized tech stack quite advantageous. In fact, it has made the development of technical centralization the centerpiece of the digital economy, both in China itself and in the many *Digital Silk Road* infrastructure projects it is pursuing abroad.

During the web1 epoch, China built the so-called Great Firewall of China to moderate how China's ISPs interfaced with the rest of the world's still-decentralized Internet infrastructure. However, in the era of web2, the solution has been simply for China to have its own set of vertically-integrated hyperscalers. Indeed, Tencent, Alibaba, and Baidu are essentially clones of their American counterparts Facebook, Amazon, and Google—albeit with the somewhat disturbing caveat that they are all responsible to the Chinese Communist Party (CCP) and subject to CCP guidance directives[10]— pervasive political oversight to which no private company in the United States or Europe could possibly be subjected.

The architectural centralization and hyperscaling of web2 is nothing less than a gift for the CCP, for it brings essentially all data together in ways perfectly suited to exploitation and manipulation, not merely for private commercial gain by the hyperscaling enterprises themselves but also for repressive political and strategic purposes by the Chinese Party-State itself. Indeed, in sharp contrast to Western privacy laws and constitutional protections—and on top of the formidable instruments of influence and coercion the CCP already possesses over all Chinese citizens—Chinese law expressly provides that all organizations and citizens must "support, assist, and cooperate with state intelligence work" and that Internet and telecommunications network operations "shall provide technical support and assistance to public security organs and national security organs."[11]

This combination of web2's structural centralization and the CCP's coercive power and legal authorities forms the foundation of modern China's repressive surveillance state. China has demonstrated that these centralized technologies are brutally effective in repressing dissent and exploiting minorities, not least through integrating 5G telecommunications networks, elaborate systems of surveillance cameras, and AI-facilitated facial recognition software to track behavior within China's Muslim Uyghur population[12] and support a massive network of concentration camps and ethno-cultural repression in the province of Xinjiang that many observers have described as nothing less than genocide.[13]

Decentralizing the Tech Stack

This naturally raises the question: are we simply *stuck* with a centralized technology stack that facilitates authoritarian governance in China and increasing portions of the BRI world, and that challenges citizen privacy even in Western democracies? Or can a better answer be found? Fortunately, the answers to these questions are, respectively, "No" and "Yes." To see why, one need perhaps look no further than the emerging technologies of the next generation of World Wide Web development: web3.

As noted, one of the authors of this paper has previously written about the urgent need for a coordinated national approach to the development of web3 technologies.[15] In a previous paper with MITRE's Center for Strategic Competition about how important it will be to *secure* web3 against criminal and state adversary cyber threats, moreover, we also pointed out that web3 could play a role in providing a decentralized and democratized counter to the centralization of the authoritarian Chinese tech stack.[16] What we would like to outline here, however, is exactly *how* web3 offers such an improved, counter-authoritarian answer.

Web3's central dogma is a goal to design a future that returns the Internet to its decentralized roots,[17] fundamentally changing dynamics around control and transparency. If and to the degree that it is successful, web3 will be profoundly disruptive to the hyperscalers—not only those based in the United States, but also (and more importantly) those based in China.

Web3 accomplishes its goal through three basic approaches:

1. **Data is democratized**. Rather than data being owned by hyperscalers and stored in private databases, everything from social media posts to financial transactions lives in public blockchains and exists as a digital asset that can be owned by anyone. Web3 companies can then build software for users to interact with that data, but no web platform will uniquely own the underlying data because it is owned by the users themselves.
2. **Internet services are democratized**. Decentralized Autonomous Organizations (DAOs) become a building block of web3, running many of the behind-the-scenes processes. DAOs use smart contracts to transact and accrue digital assets natively and are democratically governed through governance tokens that are used to propose activities, make decisions, and control parameters of the underlying protocol being managed.
3. **Advertising is no longer the business model for the Internet**. Infrastructure is paid for with digital currency, which intermediates digital asset transactions. While Bitcoin served as the initial fuel to power this new business model, there are now thousands of alternative coins which compete with it for market share. These new payment rails provide a range of custom features that have enabled a new class of decentralized financial services.

As an illustration, consider the difference between web2 and web3 in social media. Today, social media is a primary vertical for web2, with user-generated content being owned by social media companies, which are the only platforms through which users can interact with each other and each other's content. Social media companies seek to maximize user engagement to keep eyes focused on their own platform as long as possible, because revenue is based upon targeted advertising, platform eyeball time, and the ability of network managers to commoditize and sell as much user activity data as possible. Web2 is thus structurally authoritarian, as the hyperscalers' information architecture and business model are oriented around platform-specific *barriers* to user mobility and the preclusion of meaningful user control over user-generated information.

But web3 could change all that. Decentralized Social (DeSo) is the web3 version of social media, and its organizing principles are almost the complete *opposite* of the authoritarianism of web2, revolving around users' control and monetization of their own information on a decentralized basis. As illustrated by BitClout as an interface analogous to Twitter,[18] in DeSo, each user profile has its own cryptographic token, and *liking* someone's content involves buying a small amount of their token (while commenting on posts might require holding a threshold amount of their token). As a profile increases in popularity, the exchange rate of its token relative to others also increases. In effect, influencers are stocks, and those that engage with them are *stockholders*. The network's infrastructure is paid for with staking fees, while value accrues to creators and those that support them. In theory, this creates a market where shared financial incentives promote positive behavior among participants. And it has nothing whatsoever to do with aggregating everyone's information under the control and for the monetary (or political) benefit of a centralized network controller; to the contrary, the model is radically decentralized and democratized.

Web3 has a potential role to play, moreover, in many of the critical and emerging technologies in which the United States and China continue to jockey for leadership.[19] Here are a few examples:

- **Supply Chain:** As globalization has fragmented supply chains across the world, it is increasingly difficult to ascertain the provenance of components and subcomponents of the technology we consume. Web3 has the potential to provide a unique new way to unequivocally track the aggregation of intellectual property, manufacturing data, and testing regimes for hardware and software. For example, one could create a built-for-purpose blockchain-based data-sharing protocol that incentivizes collaboration while preserving data ownership and access control. From software libraries underpinning an enterprise application to bias testing performed on a machine learning model, we can help ruggedize our supply chains with transparency and illumination. Further, global shipping logistics are increasingly looking toward web3 for solutions, as a large portion of those transactions remain rooted in analog bill of lading mechanisms to this day. One example of a solution reportedly in development is provided by VeChain, which is working in partnership with Walmart to provide food safety traceability for their Chinese market.[20]
- **Telecommunications:** The Helium blockchain pioneered the Decentralized Wireless (DeWi) space, and now a variety of companies are pushing DeWi into 5G. In this model, people buy DeWi base stations and connect them to their home broadband networks and thereby stake the Helium blockchain, earning fees whenever that base station provides service to users. DeWi has the long-term potential to disrupt traditional wireless carriers if they can hit threshold deployment density and future spectrum regimes support quasi-licensed, elastic use.

- **Climate:** Building on the supply chain theme, web3 can help organizations better understand their aggregate greenhouse gas emissions by creating an opportunity for all participants in a value chain to track and report their output. This could be coupled with blockchain-based carbon credit trading to help organizations meet carbon neutrality objectives in an integrated way. For example, KlimaDAO is a blockchain-based organization that operates a carbon offset market. The DAO's tokens are purchased and burned to offset carbon emissions. The main objective of the protocol is to drive appreciation of the tokenized carbon offsets while giving organizations a web3-native way to face their emissions challenges. When on-chain markets such as KlimaDAO are coupled with a blockchain-based climate-aware supply chain, achieving carbon neutrality can be done with full transparency and auditability.
- **Biotech:** As advances in disciplines such as genomics and synthetic biology increasingly shift the field of biology into that of data and engineering, web3 is poised to help organize that digital knowledge in a systematic way. From genomic libraries to synthetic biology genetic codebases, web3 can serve to catalog and identify the provenance of biologic knowledge and support licensing and attribution for derivative developments. A market for biodata information brokers may emerge around this, providing front-end access to public blockchain-based applications which can be used to publish, control access to, and provide licensing mechanisms for engineered biological data. As an example, Nebula Genomics, founded by the 'father' of synthetic biology, Harvard Professor George Church, uses a blockchain-based system to preserve privacy, provide record auditability, and control access.[21]
- **Healthcare:** Current approaches struggle to ensure individuals' ownership and control of their own Electronic Medical Records (EMR) and personal health data, thus risking adverse usage of Personal Health Information (PHI). A web3 solution for EMR data, however, could dramatically improve patient care through secure, electronically portable, and consistent health records. An early example of such a system is MIT Media Lab's MedRec.[22] Medical research might also be accelerated by compensating users for contributing their data to retrospective trials and population health studies, much as individual participation in prospective, interventional clinical trials is compensated and hence incentivized today.
- **Digital Property Rights and the Metaverse:** One of the fundamental building blocks of web3 is the concept of digital property rights. Non-fungible tokens (NFTs) existing on decentralized public infrastructure such as Ethereum make the idealized concept of sovereign ownership of unique digital property a reality. Prior to the advent of smart contract-enabled blockchains—and more recently, the industry-wide embrace of the creative commons "no rights reserved" model[23]—digital media was typically licensed, rather than owned, by individuals. These licenses can be revoked by the corporate issuer, as well as lapse if an upstream legal agreement between the issuing platform and creator expires. The public's explosive valuation of digital property rights has taken the NFT market by surprise, however, as is evidenced by the extremely high floor price of NFT collections such as the Bored Ape Yacht Club. Even amidst a bear market induced by macro-uncertainty in which many fungible digital assets are down more than 90 percent from their all-time highs, the demand for unique digital property continues to flourish. As the public increasingly values digital assets alongside physical assets, a change which is likely to accelerate with advances in augmented and virtual reality, the metaverse can become an environment in which to uniquely interact with these wholly digital assets. Blending elements of gaming, social media, and digital economies, an open metaverse underpinned by web3 has the potential to dramatically change how humans interact and transact with each other in ways

perhaps almost unimaginable today. If the centrally-managed "walled gardens" of web2 can be kept from surrounding and subdividing the emerging metaverse, its open, component-based, and decentralized characteristics could prove all but revolutionary.

- **Global Influence:** DAOs have the potential to accrue vast amounts of capital (i.e., protocol-controlled value). We see these types of soft-power dynamics already beginning to take place with the advent of meta-governance DAOs such as Redacted Cartel. The main tactic of this DAO is to increase its protocol-controlled value by amassing the governance tokens of other DAOs, specifically ones that control DeFi yield distributions such as CRV (the governance token of Curve Finance) and CVX (the governance token of Convex Finance), so as to manipulate the yields and token emissions of these other protocols. This competition is colloquially known as the *Curve Wars*, but in the future there is little reason to expect that this kind of conflict will remain one simply between groups of cyber-savvy private entities. To the contrary, to the degree that such tactics yield real benefits, in terms either of profit or of control or influence over other economic actors, one might equally see *countries* come to compete with each other—via state-sponsored DAOs, perhaps—on this decidedly non-traditional terrain. On-chain decentralized identity solutions coupled with more sophisticated governance mechanisms, however, may help identify and perhaps mitigate the risks of covert subversion of DAO decision-making.
- **Research and Development Grants:** The Federal government grants billions of dollars to institutions of higher education and other public and private entities to execute research and development projects on leading edge solutions and technologies. Transparency into and control over how the grant funds are being expended must be balanced with protecting the intellectual property rights and proprietary information resulting from these projects. The MITRE Corporation, in collaboration with the U.S. Department of Health and Human Services, the National Science Foundation, the University of Washington, and several private sector blockchain and grants management solution/service providers, has completed development of a proof-of-concept solution that incorporates the key concepts of user control over their data and decentralized management of services. In the Future State Grants Management Solution,[24] grant recipients retain decentralized management of their project and grants information through their preferred service provider and determine when to make the required grants information accessible by grantmaking entities, inspectors general, and independent auditors to ensure transparency into and control over grants funds.

The emerging technologies of web3 and the range of potential new use cases they will engender are not merely likely to be important new drivers for innovation and prosperity in the next era of the digital economy. They also have the potential to offer a powerful and compelling riposte and antidote to the authoritarian architectures of web2, and particularly to the ugly and repressive surveillance schema of the Chinese technology stack.

Web3 even has the potential to improve the transparency of Beijing's self-serving overseas financial and economic models and digital infrastructure projects, since in a web3 environment, decentralized infrastructure costs are necessarily diffused over a large number of network validators (e.g., miners or stakers), who recoup their investment through transaction fees. It thus offers at least a partial technological answer to a range of web2-era challenges—both domestically and abroad—that is consistent with Western ideals: free markets, transparency, and democratic and decentralized governance are baked into it at the architectural level.

Policy Recommendations

President Biden's Executive Order (EO) on digital assets recognizes the huge potential of the emerging generation of digital assets, and seeks to "reinforce United States leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets."[25] As that EO further notes, preserving a U.S. lead in this arena is of great importance, for this country "derives significant economic and national security benefits from the central role that the United States dollar and United States financial institutions and markets play in the global financial system." U.S. leaders in the Executive Branch and in Congress are working to find a path forward in this arena that balances the needs of law enforcement, financial market regulators, and industry with the goal of creating American jobs, promoting innovation, and increasing economic output.

In fact, however, the stakes are even higher here than just a question of U.S. interests, for as we have seen, the web3 technology stack is a critical element of an *offset strategy* with which to help counter the authoritarian implications of the web2 tech stack around the world and democratize the whole Internet, while better protecting the privacy of millions or billions of people. Both to promote American interests and to advance such democratization everywhere, we need to ensure that web3 is done right. To that end, the following pages offer some suggestions for how to help advance the policy, technology, and social design elements of web3:

1. **Develop a combined national and economic security[26] strategy that can maximize the benefits of a new decentralized payment system while mitigating illicit financial activities.**

   While the new peer-to-peer payment systems—known as payment *rails*—enabled by the web3 technology stack can allow for greater distribution of economic wealth, an explosion of web3-facilitated digital assets might in some circumstances also erode the standing of the U.S. dollar as the global reserve currency, potentially providing a new mechanism to scale illicit financial activities that can undermine trust in the overall financial ecosystem. To make that less likely:

   - Congress should accelerate efforts to pass regulations governing stablecoins—that is, cryptocurrency designed to maintain a stable value over time as a result of being pegged to some antecedent fiat currency, such as the U.S. dollar[27]—to help mitigate market instabilities and make dollar-backed cryptocurrency more attractive, and should explore further incentives to strengthen the U.S. dollar as a desired fiat peg currency.
   - The Federal Reserve and U.S. Treasury should explore differentiated international market opportunities for a U.S. central bank digital currency (CBDC) and identify features that could help US companies increase their competitiveness overseas. These features should be prioritized in future development efforts.
   - Traditional entity-based approaches to disclosure, enforcement and compliance (e.g., know your customer [KYC] protocols) are ill-suited and inefficient when applied to decentralized ecosystems. For such cases, regulatory agencies should instead develop *activity*-based risk management approaches, using metrics that capture overall market contagion risk and leading indicators of bad faith financial engineering activities in real-time.
   - Given that smart contracts define the execution logic of web3 transactions, an industry-government coalition should explore how best to integrate compliance-enabling logic within smart contracts to reduce enforcement overhead for agencies and the reporting burden for individuals.
   - Strengthen cybersecurity protections within web3 infrastructure implementation and operations, as detailed in our prior paper.[28]

2. **Advance global decentralized digital identity and digital data technologies to protect citizen privacy and enable the evolution of governance.**

   The need to protect individual privacy and the need for service providers to comply with KYC, Customer Due Diligence (CDD), and Anti Money Laundering (AML) regulations are conflicting goals that require solutions that balance private interests with national security in a web3 world. Furthermore, the immutability and transparency of the underlying web3 blockchain architecture pose additional privacy concerns when it comes to an individual's "right to be forgotten."[29] At the heart of this conflict is the need to prevent abuse or misuse of individual identity and data. With the advent of decentralized identity technologies, portable and verifiable KYC credentials and zero-knowledge proofs provide a chance to potentially achieve a good balance. In particular:

   - Third-party identity verifiers should sign reverse privacy agreements with their customers, setting forth guardrails that define the circumstances in which their identity elements will be disclosed, to whom, and for what purpose. A reverse privacy agreement is a mutually acceptable End-User License Agreement (EULA) that is offered by the user and countersigned by the verifier. The citizen's privacy policy would be constructed in simple language and then converted to a machine-readable contract which the verifier would sign digitally.
   - Research institutions should be incentivized by Congress to accelerate the development of privacy-preserving data analysis techniques such as secure multiparty computing, homomorphic encryption, and differential privacy to achieve higher fidelity at scale. In parallel, security controls for tokenized decentralized data stores such as Solid Pods[30] should be strengthened to enable computing at the edge of networks, rather than in centralized cores, using artificial intelligence algorithms tailored for sparse, distributed data.
   - A few organizations are already working on guides and recommendations that represent privacy-preserving identity implementations,[31] but guidance from the National Institute of Standards and Technology (NIST) would make a big difference for the government marketplace. This would allow federal and state agencies to provide better service to citizens and better security to the internet.

- Decentralized identity-enabled governance research should be prioritized. Plutocratic DAO governance models (i.e., token voting) offer well-capitalized bad faith financial engineers a covert control vector. Decentralized ID solutions should be developed to further enable democratic decision-making architectures.

3. **Promote accessibility standards to reduce burden of technology adoption**

   - The interfaces currently available to access the web3 ecosystem require individuals to have a high level of technical sophistication and fail to meet basic Section 508 accessibility standards.[32] This failure is due in part to the lack of adoption of user-centered design principles and a counterproductive focus on providing solutions primarily for a tech-savvy early-adopter market segment—which limits the potential for rapid and widespread uptake and use-case development. It is a glaring omission for the web3 community to make the case for a more democratic internet, however, without building these new architectures in ways that would facilitate access by and input into the overall design process from individuals representing a much broader demographic. To help address this imbalance:
   - Researchers should build on the early work of the MIT Digital Currency Initiative to identify and mitigate the User Experience (UX) challenges presented by digital wallets. Efforts in this regard, for instance, should focus on expanding to different types of wallets (e.g., custodial vs. non-custodial) and off-chain hardware wallets.

- Congress should prioritize federal research investments that promote technology accessibility. In particular, additional research should be conducted to determine: (a) the key-management options and wallet designs that would work best for different types of users; and (b) how the needs for such approaches differ among different segments of the population. Emerging wallet protection methods such as 'social recovery' can be used to create more forgiving user experiences.

4. **Address the needs of the underbanked/unbanked by maturing prototype digital asset solutions**.

The U.S. Treasury Department's Strategic Plan for Fiscal Years 2022-25[33] calls for progress on financial innovation with a deliberate emphasis on financial inclusion. Unfortunately, however, many of the current use-cases for web3 are centered on investment opportunities and may not align directly with the needs of underbanked or unbanked populations. That said, web3 has considerable potential to help disadvantaged populations, not least in providing a possible future way to accelerate, target, and mitigate fraud, waste, and abuse in disbursements of government economic stimulus or crisis-response aid. Web3 technologies may also help reduce financial transaction fees—thus also potentially helping the underbanked—and helping make possible more viable or safer alternatives to predatory inclusion services such as pay-day lending and title loans. To help web3 help the financially disadvantaged:

- The Treasury Department's Community Development Financial Institutions (CDFI) fund should conduct a study to assess the potential for peer-to-peer decentralized financial payment systems to benefit communities located in domestic banking deserts. Such mechanisms might well prove a promising way to provide financial services in areas without intermediation by traditional bricks-and-mortar institutions.
- Next-generation digital assets may also provide important opportunities for disadvantaged populations around the world by improving the efficiency and cost-effectiveness of international remittances sent by migrant workers back to family members in their home countries. Global remittances total at least $550 billion every year—a financial flow larger than the combined sum of Foreign Direct Investments (FDI) and Overseas Development Assistance (ODAC), which is a significant contributor to the GDP of developing economies. Unfortunately, the remittance sector is also subject to high technical, regulatory, and financial risks associated with cross-border payments; it is also an inefficient way to transmit value, as existing pathways typically have high transaction costs (the average remittance fee is 6.8 percent) and can take on average 2-3 business days to settle. The Federal Reserve and U.S. Treasury Department, in collaboration with the Bank of International Settlements, should examine the potential for an alternative multi-jurisdictional approach based on Central Bank Digital Currency (CBDC) or well-regulated stablecoins, which could help significantly improve the cost, speed, and user experience for both remittance providers and recipients.

5. **Convene international partners and advance an inclusive vision to strengthen democratic values, protect citizens from threat actors, and develop and promote a decentralized, web3-facilitated response to the global growth of the authoritarian technology stack.**

From the perspective of international engagement, to help web3 technologies realize their potential as an antidote to the centralized and incipiently authoritarian web2 tech stack, the United States should urgently pursue at least two priorities:

- First, the United States should organize and lead an international effort—involving officials both from likeminded, democratic, technology-possessing governments and from private sector entities with influence and credibility in the cyber-governance arena—to respond to Chinese efforts to game international Internet-related standards with a coordinated *non*-authoritarian effort in global standards-setting bodies to promote democratic and decentralized web3 values. These efforts should build on the recent directives issued to U.S. agencies to "leverage U.S. positions in international organizations to message U.S. values related to digital assets" as detailed in the White House Framework for Responsible Development of Digital Assets.[34]

For years, it has been a Chinese priority to organize coordinated campaigns in standards-setting bodies—such as those associated with the International Telecommunications Union (ITU)—to promote technological standards (e.g., of architectural centralization and state-political information sovereignty) that are consistent with the CCP's authoritarian values.

- It is well past time for the Western technology-possessing democracies to organize an effective response to these efforts, and one way to do this is to encourage private industry and government representatives to promote web3 technologies and values in international fora as a direct alternative to the approaches that are promoted by their Chinese counterparts, often with help from other similarly undemocratic regimes in Russia, Iran, Saudi Arabia, and elsewhere. If supported by cogent and compelling technical analysis—as well as by concerted work among the democracies and the developed Western economies of the world, who would have much to lose were Chinese approaches to win out—such standards have a good chance at prevailing, allowing such bodies to lock in approaches favorable to non-authoritarian governance, citizen privacy, and decentralized user autonomy in the next generation of Internet development.
- Second, this effort to promote web3 values should not be confined merely to the quiet and technocratic confines of technical standards-setting bodies. It should also be an important focus of Western—that is, United States and partner—public diplomacy.
- For too long, Western representatives have been stuck in the unenviable position of simply saying "No" to bad ideas advanced by China, Russia, and others in international fora related to Internet governance and technology standards. With the advent of web3 technologies, however, we can move beyond mere negativity. Specifically, we can now increasingly voice support for web3-based approaches as a better alternative to the authoritarian tech stack—that is, to offer an optimistic, forward-looking response to those looking for answers about how the future World Wide Web is to be organized and governed from a technical perspective.

  We should not shy away from this task, nor from the public diplomatic aspects of its promotion. Promoting web3 values should be explicit, public, and emphatic. We do have a better answer, and we should not be shy about promoting it.
- Third, we must catalyze investment in substantive web3 technologies. Much of the private capital flowing into web3 startups and infrastructure has sought to profit from the dramatic increase in cryptocurrency market capitalization spurred by speculative trading during the COVID-19 pandemic. With markets resetting and a more sustainable growth trajectory ahead, structured federal investment in web3 could help mature the existing ecosystem of DeFi-focused investors into helping build a future decentralized Internet that the U.S. can export competitively to BRI countries.

  Templates for this type of investment exist already, such as the multifaceted approach to 5G wireless technologies. The Chips and Science

Act[35] authorizes funding for basic research at the National Science Foundation and applied research at NIST and the Department of Energy. It also appropriates $1.5 billion for direct grants to companies through the Public Wireless Supply Chain Innovation Fund. By broadly interpreting the technology area "advanced communications technologies" under that Act, web3 technologies could be funded under these existing programs. New, dedicated web3 programs should be set up in parallel to further catalyze investment.

Conclusion

The various technologies that are contributing to the development of a novel web3 digital ecosystem promise a future World Wide Web with dynamics and characteristics far different than those to which we have become accustomed in the centralized, hyperscaled, and structurally authoritarian era of web2. There is much to do—both in terms of actual technology development and in terms of associated policy and regulatory build-out—to make web3 a reality, to make it safe and reliable, and to equip it to fulfill its potential as a sea change in how human beings interact digitally with each other.

If such challenges can be met, however, web3 has the potential not merely to open up broad new vistas of innovative use cases and to provide opportunities for a new era of creativity and growth in the digital economy, but also to help provide disadvantaged populations with more affordable and secure financial services and transactional opportunities. In the broadest sense, it also has the potential to form the backbone of an offset strategy that could form a robust and decentralized, democratized alternative to the authoritarian web2 technology stack that today underpins the ability of hyperscaled commercial firms to aggregate and merchandize the personal information of billions of private citizens, as well as the ability of authorities in China (and a growing number of other countries) to leverage omnipresent surveillance in the service of political repression.

This paper has surveyed the development of web3 and outlined both its promise and some of the steps that will still be needed in order to see this potential realized. There is much to do, and no time to waste.

About the Authors

Charles Clancy is a senior vice president at The MITRE Corporation, general manager of MITRE Labs. He previously served as MITRE's vice president for intelligence programs and before that as the Bradley Distinguished Professor in Cybersecurity at Virginia Tech and Executive Director of the Hume Center for National Security and Technology.

Christopher Ford is a MITRE Fellow and directs the Center for Strategic Competition. He served until January 2021 as U.S. Assistant Secretary of State for International Security and Nonproliferation and also fulfilled the duties of the Under Secretary for Arms Control and International Security.

Michael D. Norman is a principal systems engineer at MITRE and the web3 and digital assets capability area lead. He has worked in decentralized systems and cryptocurrency for the past 17 years and holds a doctorate in complex systems and brain sciences from Florida Atlantic University.

Sanith Wijesinghe is a technical fellow at MITRE and works at the intersection of financial infrastructure and technical innovation. Before joining MITRE in 2011 he spent seven years as a technologist on Wall Street.

Endnotes

[1] Paul Mozur, Raymond Zhong, and Aaron Krolik, “In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags,” *New York Times* (March 1, 2020), *available at* https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

[2] *id.*

[3] Dahlia Peterson, “How China harnesses data fusion to make sense of surveillance data,” *Brookings Institution* (September 23, 2021), *available at* https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/.

[4] Maya Wang, “China’s Techno-Authoritarianism has Gone Global,” *Foreign Affairs (April 8, 2021), available at* https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global.

[5] Charles Clancy, “Call to Action: Developing A National Strategy for Web3,” *MITRE Corporation* (March 2022), *available at* https://www.mitre.org/sites/default/files/publications/pr-22-0753-call-to-action-developing-a-national-strategy-for-Web3.pdf.

[6] Charles Clancy, Christopher Ford, Mike Norman, & Sanith Wijesinghe, “Securing Web3 and Winning the Battle for the Future of the Internet,” *MITRE Corporation, Center for Strategic Competition, Occasional Papers,* vol. 1, no. 4 (September 1, 2022, *available at* https://www.mitre.org/sites/default/files/2022-09/pr-22-2754-securing-web3-winning-battle-for-future-internet.pdf.

[7] Max Roser, Hannah Ritchie, & Esteban Ortiz-Ospina, “Internet,” *Our World in Data* (undated), *available at* https://ourworldindata.org/internet.

[8] “The Singularity Is Near,” *Singularity.com* (undated), *available at* http://www.singularity.com/charts/page80.html.

[9] *See, e.g.,* Ben Wolford, “What is GDPR, the EU’s new data protection law?” GDPR.eu (undated), *available at* https://gdpr.eu/what-is-gdpr/.

[10] *See, e.g.,* General Office of the CCP Central Committee, “Opinion on Strengthening the United Front Work of the Private Economy in the New Era” [中共中央办公厅印发《关于加强新时代民营经济统战工作的意见》] (September 15, 2020) (translated and reproduced in “The Chinese Communist Party Targets the Private Sector,” CSIS (October 8, 2020), *available at* https://www.csis.org/analysis/chinese-communist-party-targets-private-sector) (directing acceleration of Party control over private sector entities).

[11] National Counterintelligence and Security Center Director William Evanina, remarks to the International Legal Technology Association (June 4, 2019), (quoting Articles 7 & 11 of the National Security Law of the People’s Republic of China), *available at* https://www.dni.gov/files/NCSC/documents/news/20190606-NCSC-Remarks-ILTA-Summit_2019.pdf.

[12] *See, e.g., Eva Dou, “Documents link Huawei to China’s surveillance programs,” Washington Post* (December 14, 2021), *available at* https://www.washingtonpost.com/world/2021/12/14/huawei-surveillance-china/.

[13] *See, e.g.,* Office of International Religious Freedom, U.S. Department of State, “2021 Report on International Religious Freedom” (June 2, 2022), *available at* https://www.state.gov/reports/2021-report-on-international-religious-freedom/china/xinjiang/.

[14] *See, e.g.,* James Kynge, Valerie Hopkins, Helen Warrell, & Kathrin Hille, “Exporting Chinese surveillance: the risk of ‘smart cities,’” *Financial Times* (June 9, 2021), *available at* https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab.

[15] Clancy, “Call to Action,” *supra.*

[16] Clancy, Ford, Norman, & Wijesinghe, “Securing Web3,” *supra.*

[17] *See, e.g.,* Scott Clark, “How is Web3 Decentralized?” *CMS Wire* (February 2, 2022), *available at* https://www.cmswire.com/information-management/how-is-Web3-decentralized/

[18] *See, e.g.,* "DeSo: the Decentralized Social Network," *DeSo.org* (undated), *available at* https://docs.deso.org/about-deso-chain/readme.

[19] For an account of the Biden Administration's current research and development (R&D) funding and industrial policy priorities, *see, e.g.,* OMB Director Shalanda Young & Deputy Assistant to the President Alondra Nelson, "Multi-Agency Research and Development Priorities For the FY 2024 Budget," Memorandum to Heads of Executive Departments and Agencies (July 22, 2022), *available at* https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-15.pdf.

[20] https://www.coindesk.com/markets/2019/06/25/walmart-china-teams-with-vechain-pwc-on-blockchain-food-safety-platform/.

[21] https://blockchainhealthcaretoday.com/index.php/journal/article/view/34.

[22] https://people.cs.pitt.edu/~babay/courses/cs3551/papers/MedRec.pdf

[23] https://creativecommons.org/share-your-work/public-domain/cc0/

[24] Jasmine Faubert, Karen Lee, Marla Ozarowski, "Demonstrating the Future of Grants Management", (August 29, 2022), MITRE Corporation, *available at* https://www.mitre.org/news-insights/publication/demonstrating-future-grants-management.

[25] Executive Order on Ensuring Responsible Development of Digital Assets (March 9, 2022), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

[26] For a greater discussion of economic security, see "Final Report: Economic Security Subcommittee", Homeland Security Advisory Council, November 2020.

[27] *See, e.g.,* James Royal, "What are stablecoins and how do they affect the cryptocurrency market?" *Bankrate.com* (May 12, 2022), *available at* https://www.bankrate.com/investing/stablecoin-cryptocurrency/.

[28] Clancy, Ford, Norman, & Wijesinghe, "Securing Web3," *supra.*

[29] Vaas, Lisa (25 September 2019). "Google wins landmark case: Right to be forgotten only applies in EU". Naked Security. Retrieved 9 May 2021.

[30] *See* "Solid: Your data, your choice," solidproject.org website (undated), *available at* https://solidproject.org/.

[31] *See, e.g.,* TrustOverIP Foundation, trustoverip.org website (undated), *available at* https://www.trustoverip.org; "The Good Health Pass Collective," *goodhealthpass.org* website (undated), *available at* https://www.goodhealthpass.org.

[32] Under the Rehabilitation Act of 1973, 29 U.S.C. § 794(d), federal agencies must give disabled employees and members of the public access to information comparable to the access available to others. *See generally, e.g.,* U.S. General Services Administration, "IT Accessibility Laws and Policies," (March 2022), *available at* https://www.section508.gov/manage/laws-and-policies/. In practice, this entails a number of specific adjustments to how text and documents—including the one you are reading, for as a Federally-Funded Research and Development Corporation (FFRDC), MITRE adheres to Section 508 standards—are displayed online.

[33] U.S. Department of the Treasury, *Strategic Plan 2022-2026* (2022), *available at* https://home.treasury.gov/system/files/266/TreasuryStrategicPlan-FY2022-2026.pdf.

[34] Fact Sheet: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets (September 16,2022), *available at* https://www.whitehouse.gov/briefing-room/statementsreleases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/

[35] Public Law 117-167 (August 9, 2022), *available at* https://www.congress.gov/bill/117th-congress/house-bill/4346/text.