BLOCKCHAIN AT THE FRONTIER

Impacts and issues in cross-border co-operation and global governance

OECD

Please cite as: OECD (2022), Blockchain at the frontier: Impacts and issues in cross-border co-operation and global governance, OECD Business and Finance Policy Papers, OECD Publishing, Paris, https://doi.org/10.1787/80e1f9bb-en.

Blockchain technology is expected to drive digital transformation in the way businesses, governments and societies interact in the years ahead, including at an international level. This paper considers current and emerging uses of blockchain to strengthen beneficial economic ties between countries, including in trade and supply chain transparency, portable credentials for people and organisations, and business financing and capital formation. It also explores key concerns about blockchain's impact on global rules and multilateral policy objectives, particularly around climate impacts and uses for illicit finance. The paper underscores the value of deliberate international co-operation to realise the beneficial cross-border applications of the technology and address international challenges, highlights existing instruments and approaches, and identifies gaps and priorities, towards a more consistent and coherent international policy environment for responsible blockchain innovation.

Foreword

Blockchain is an emerging technology which poses a number of novel questions and challenges to existing policy, legal, and regulatory frameworks. Given blockchain's ease of operation across borders and its ability to connect economic activities and administrative systems between jurisdictions, discussions at the 2021 OECD Global Blockchain Policy Forum focused on how to foster co-operation and closer economic ties between countries, uphold global rules and norms, and support an international policy environment for blockchain innovation.

The report was principally authored by Oliver Garrett-Jones with contributions by Marianne Aalto, under the supervision of Mamiko Yokoi-Arai, of the Division of Financial Markets of the OECD Directorate for Financial and Enterprise Affairs.

The OECD team gratefully acknowledges the financial contribution provided by the Government of the United Kingdom which supported the delivery of the Forum and the production of this report. The Forum was also supported by private sector contributions from Accenture and MetaMui, and was made possible through the time, energy and ideas of its discussion moderators, lead discussants and panellists.

The report benefited from valuable input and constructive feedback from colleagues from across the OECD: Rashad Abelson of the Centre for Responsible Business Conduct; Iota Nassr and Ana Sasi-Brodesky of the Financial Markets Division; Audrey Plonk and Gallia Daor of the Digital Economy Policy Division; Cecillia Emilsson and Felipe González-Zapata of the Open and Innovative Government Division; Guillermo Hernandez of the Regulatory Policy Division; Silvia Sorescu of the Emerging Trade Policy Issues Division; Daniel Blume and Carl Magnus Magnusson of the Corporate Governance and Corporate Finance Division; as well as Ken Menz of the Financial Action Task Force.

Table of contents

FIGURES

TABLES

1 Introduction

Blockchain technology can enable peer-to-peer interactions and transactions over networks that run autonomously, often without the oversight or involvement of intermediaries and other third parties. As an emerging technology it is not in wide use in most sectors, but its potential to contribute to positive digital transformation, as well as some of its particular pitfalls and risks, have attracted policymakers' attention. As the policy environment around blockchain takes shape, policymakers should consider specific international aspects of this technology's impact in order to fully realise benefits and mitigate risks, including its use in supporting cross-border co-operation and closer economic ties; its positive and negative impacts on international rules and norms; and the need for a level of consistency and coordination between national policy approaches.

Blockchain has been vaunted as a game-changing technology that could one day transform businesses, markets and even the very fabric of our social lives – but today that future seems distant. There are some sectors, particularly in finance, where the technology's use is well-advanced and its disruptive potential is evident, but in other areas blockchain innovations are considerably less scaled, and its potential impacts can appear more marginal and remote.

Despite this, governments should be paying attention to this technology's implications for public objectives. Blockchain is one of several emerging technologies, alongside artificial intelligence, the internet of things, and 5G mobile networks, which are expected to drive new levels of digital transformation and disruption in the years ahead. Though mainstream use of blockchain is uncommon and adoption is currently low in most sectors beyond finance, blockchain innovations are beginning to emerge in a broader variety of settings. The pace of innovation can be high, and in some cases the technology is already posing real policy challenges.

The 2021 OECD Global Blockchain Policy Forum, on which this report is based, focussed on blockchain's impact – positive and negative – on cross-border connections and wider global governance. It comes at a time when the aims of international co-operation, and the values that underpin it, are more relevant than ever. Covid-19 has strained global value chains and spurred new border measures. Geopolitical tensions have further disrupted trade and financial flows, and underlined the importance of a rules-based global system. Immediate global challenges, from climate action to sustainable development, can only be met with coordinated global responses.

In this context, governments are increasingly seeking to leverage digital technologies to strengthen beneficial economic and social ties across borders, including the flows of goods, people and capital. The Forum explored the current and potential opportunities blockchain technology presents across all three of these areas.

Blockchain's use to facilitate trade is perhaps the technology's most advanced application outside of finance. Companies and consortia are building digital networks to strengthen transparency and traceability in shipments and supply chains, with reliable digital certifications that could support regulatory oversight and ease trade friction at the border. Blockchain is also a nascent but growing feature of the digital identity landscape, where it could support the recognition of people, qualifications and credentials between countries while better managing privacy. And while blockchain has had little impact in public capital markets and related corporate governance practices, a flourishing decentralised digital finance market shows the potential for the technology to create new models of capital formation.

The benefits are not a given in any of these cases. Government policies may influence the scope to apply blockchain solutions, including where rules are not technology neutral or haven't kept up with digital transformation. To support links between countries, a level of interoperability between borders, on both a technical level but also in regulatory and legal approaches, is desirable.

While there are opportunities, some aspects of blockchain have drawn concern from the public and the international community. One area is energy intensity, and while this is a legitimate concern, it is important to recognise that high energy usage is not synonymous with blockchain, but with a subset of open, public networks. Renewables might also make up a substantial part of the energy mix for those networks, though exact levels are difficult to determine. Nonetheless, the matter points to wider issues in the crypto-asset industry around accountability and transparency, and the need for a stronger focus on responsible business conduct. Another area of concern is the potential for crypto-assets to be used in illicit finance. The rules set by the Financial Action Task Force for these assets and their providers is an important international standard to address these risks – but significant implementation gaps remain between countries.

In both these cases it is clear that blockchain's decentralised nature does *not* make it ungovernable. There are many participants in the ecosystems around public blockchain networks, including legitimate businesses such as exchanges, equity providers and developers, while in private networks the participants are generally easily identifiable. These actors can and should operate in a manner consistent with social expectations, national laws, and international rules and norms.

The inherent global nature of blockchain technology, and need for international policy consistency to both harness the cross-border benefits and manage the risks, require countries to co-operate on blockchain governance. In many instances countries do not need entirely new approaches; there are a suite of existing international instruments and initiatives to support regulatory co-operation in a digitalised and highly innovative global environment. There is also an emerging body of blockchain-specific international rules and practices, including technical standards, bilateral initiatives, industry codes, and policy recommendations from financial regulation standard setting bodies.

Still, there are gaps in the international policy landscape, even at this early stage. Efforts between countries are still fragmented, and specific avenues for international co-operation are not always clear. Some of the

actual and potential issues around blockchain remain unaddressed, such as governance and transparency in networks, conduct of related actors, and compliance with existing rules, particularly at a cross-sectoral level.

A base level of international guidance will be necessary as blockchain develops. It must be sufficiently high-level to account for the unexpected directions this emerging technology might go, but specific enough to protect market integrity, a level playing field and the rule of law; to promote responsible, human-centric innovation; and to safeguard the principles of openness, transparency, democracy and human rights that are the foundations of OECD members' economies and societies.

1.1. The OECD Global Blockchain Policy Forum

Since 2017, the OECD's *Going Digital* project has been the focal point of the Organisation's long-standing efforts to help governments navigate the digital transformation of our economies and societies. *Going Digital* has supported policymakers' understanding and response to this transformation with the development of indicators, benchmarks and policy guidance, notably collected in the *OECD Going Digital Toolkit.* It has also created important resources to help governments adapt to the impacts, opportunities and risks posed by emerging technologies, including through the landmark *OECD Principles on Artificial Intelligence*, and the annual Global Blockchain Policy Forum.

The Forum was created in recognition of the novel challenges and opportunities blockchain and related decentralised ledger technologies present to public policy outcomes and government objectives across a wide range of disciplines. It convenes policymakers, industry representatives, experts and thought leaders to explore recent developments, exchange perspectives and inform national and international policy responses.

The OECD's work on blockchain policy issues to date, including past editions of the Forum, have largely focused on how blockchain technology impacts core government objectives, such as ensuring market integrity and efficiency and delivering inclusive growth; how blockchain could be applied to further a range of specific public policy aims; and how policy and regulatory environments affect blockchain development and innovation. The Forum's 2021 edition, held between 15 September and 1 October, applied these considerations to an international setting, specifically 1) fostering co-operation and closer economic ties between countries; 2) upholding global rules and norms; and 3) supporting an international policy environment for blockchain innovation.

1.2. Blockchain technology: A policymaker's overview

Evolving digital technologies are among the most significant drivers of digital transformation, and blockchain is no exception. In the roughly fourteen years since blockchain was first put to use at scale through the Bitcoin blockchain, the technology has spawned entirely new markets, goods and services, business models, and means of economic and social connection. It has done this by providing networks that operate without the need for a central authority, with predefined rules and security features that allow for the exchange of information or value between parties without relying on intermediaries, and with reliable records of those exchanges (see Box 1).

Box 1. How blockchain technology works

A blockchain is a group of networked databases, or "nodes", which all hold the same set of data. The network has pre-defined rules that allows nodes to agree on the data contained in the databases – data cannot be added or changed without consensus in the network. This allows the network to agree and record a single set of facts automatically and predictably, without the need for a mediator or intermediary. It allows parties that might not know one another or trust one another to transact and collaborate directly, which is why blockchain has been referred to as the "trust machine".

Because the blockchain contains one record of information shared among participants, it is possible to also assign and agree on characteristics of that data, such as ownership. This is what allows a blockchain to create digital money and other tokens that can be transferred between parties without the risk of double spending, thus allowing value to be stored and transferred digitally – a significant departure from the traditional internet where digital assets could be copied *ad infinitum.*

The network stores all transactions between parties by adding "blocks" to the data set, and so past transactions are stored, timestamped, and are visible to all network members. Cryptographic links between the blocks form the "chain" with past transactions, making records on the database unalterable without breaking the cryptographic link with all subsequent blocks, and so the record is said to be immutable. In addition, the decentralised and distributed nature of the networks can make blockchains resilient to certain security threats. These characteristics afford a high level of transparency and accountability to activities on the network and confidence in the data.

Blockchain networks can form the base layer of a wider digital ecosystem, on top of which decentralised applications can be built, just as applications are built on top of the internet. These applications are often based on smart contracts, pieces of code which self-execute once certain conditions are met (see Box 4).

There are a range of consensus mechanisms and governance choices available when designing a blockchain network, and networks can be configured based on who can participate in the network's governance as a node, and who can participate in the network's activities as a user. These can range from public permissionless networks where anyone can join as a node or user, to private permissioned networks where nodes and users must be approved by a central authority, or some hybrid of these. An example of a public permissionless network is Bitcoin, which is controlled by no one, available to anyone, and highly decentralised. An example of a private permissioned network is JP Morgan Coin, a blockchain-based token used support faster transactions, that has been developed on a network controlled by JP Morgan and only available to the bank's institutional clients.

Source: OECD (2018[1]), OECD Blockchain Primer, https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf

1.2.1. *An emerging technology with potentially wide applications*

Blockchain is a "general purpose technology", meaning it opens up opportunities for a multitude of complementary innovations over time, rather than being complete solution in itself (Bresnahan and Trajtenberg, 1995, pp. 83-108[2]). It provides a platform of trust, transparency and accountability with actual and potential applications across sectors well beyond its original use for crypto-assets. Though blockchain is at a relative early stage of adoption in most sectors and will likely continue to evolve, innovation has advanced at a rapid pace, and investment in blockchain technology is expected to reach close to USD 19 billion a year by 2024 (IDC, 2021[3]). Among the many uses explored to date, blockchain has: been embedded in mineral and agricultural supply chains to track the provenance of goods; been harnessed to

streamline customs and shipping procedures; used to lift efficiency in cross-border payments and settlements; used to safely manage personal information and digital identifiers; and formed the basis for a new class of purely digital assets (Table 1).

Table 1. Examples of blockchain innovation

A selection of blockchain projects referred to in this report

Type of use	Name of project	Description
Trade facilitation	TradeLens	A platform that collects, verifies and shares information on shipments across a network of global supply chain actors (shippers, freight forwarders, ports, ocean carriers, government authorities, customs, etc) to streamline processes, provide transparency and auditability, and reduce overall trade friction (TradeLens, 2022[4]).
	Everledger	A service using blockchain to trace the provenance and history of goods through supply chains, providing proof of authenticity and insights into conditions. Applications focus on industries facing high risk of fraud and misconduct further down supply chains, such as diamonds, art, fashion and battery recycling (Everledger, 2021[5]).
Digital identity	ID2020	A non-profit consortium which develops pilots for digital identity, focused on excluded populations that may not have safe and reliable access to state-based identity systems. While technologically agnostic, it emphasises the value of decentralisation and cryptography to support privacy, user-control, portability and verifiability (ID2020, 2022[6])
	Known Traveller Digital Identity	A pilot technology framework for travellers to collect and communicate attestations to their identity and characteristics from a range of authorities, such as governments, banks and law enforcement. It aims to enable automated visas and enhanced risk assessment and vetting, to provide a more seamless flow of travellers through borders, and is currently being trialled by Canada and the Netherlands (World Economic Forum, 2018[7]).
Financial intermediation	UniSwap	A global, decentralised exchange which uses smart contracts and algorithms to create liquidity pools of crypto-assets and set market prices, enabling peer-to-peer exchange of cryptoassets. Uniswap currently facilitates USD $10 billion in trading each week (Cointelegraph, 2021[8]).
	MakerDAO	An automated protocol that provides lending services against the collateralised crypto-assets of borrowers. Loans are made in a crypto-asset which has nominal parity to the US dollar, which is also stabilised automatically to maintain the peg (Gemini, 2021[9]).
Public service delivery	Estonian KSI Blockchain	A cyber-security complement to Estonia's public digital infrastructure in use since 2012. It uses decentralised ledgers, cryptography and related timestamping to validate information on national systems and make them tamper-proof, ranging from personal health data, justice records and land registries (Enterprise Estonia, 2017[10]).
	European Blockchain Services Infrastructure	A blockchain developed by the European Commission and hosted across 29 European countries, intended to provide the digital infrastructure for cross-border public service applications used between member and partner states. While not in wide use, initial use cases under development include digital identity, portable education credentials, and exchange of VAT information (European Commission, 2021[11]).

Despite the technology's many purported uses, fully-scaled examples of applications are rare, and several of the examples cited in the table above are at an early stage of commercial development and use. However, blockchain innovations have already yielded promising results across sectors, and the technology is being harnessed with the aim to deliver efficiency gains to business and public sector processes through digitalisation, decentralisation and automation. Uses to date have also hinted at its potential to create novel markets and alternative systems of economic and social interaction. Some of these innovations may offer marginal improvements, others might prove to be transformative.

In some quarters the technology has also prompted a re-imagination of current systems of governance, using more automated and decentralised systems. Examples of such hypothetical systems include "trust chains" that use blockchain and other emerging technologies to create entirely new trade systems, fully integrating digital currencies, payments, credentials, taxation, shipping and customs processes (Pentland,

2021[12]), or a "global social contract", with the rules and objectives of global governance and cross-country co-operation encoded onto a decentralised network, hosted by governments and civil society, and with agreements monitored and enforced by smart contracts (De Filippi, 2021[13]). While these may seem like distant possibilities, they illustrate future scenarios where blockchain is woven into the fabric of economic, financial and social life.

1.2.2. *Proactive policymakers have moved beyond bitcoin*

Past discussions at the Forum have noted the tendency in policy discussions and public discourse for blockchain technology to equated narrowly with crypto-assets like bitcoin and, separately, market commentators have described how an ambivalence or hostility towards crypto-assets may act as a barrier to proactive policy development, and coherent legal and regulatory approaches (Elliott, 2022[14]). Taken together, these observations suggest that heuristics and biases could cause policymakers to ignore the potential benefits and uses of the technology for policy delivery and economic development in wider settings, and so may not take timely action to help realise these benefits.

Despite these preconceptions, certain jurisdictions have already begun considering how the technology fits into industrial and innovation strategies, how it might improve government service delivery, and what role it could play in supporting wider social and economic objectives. The United Kingdom was an early mover in 2016, with a detailed report from the country's Chief Scientist highlighting blockchain's "potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust" (Walport, 2016[15]). Since then other jurisdictions have taken this mantle further, with major economies like Germany and Australia, and bodies like the European Commission, establishing blockchain strategies (see Box 10), some of which have also included the provision of research grants and, in the case of the European Commission, the development of public digital blockchain infrastructure to support innovation and drive interoperability between countries.

Public sector innovation has also spurred experimentation with the technology in a government setting, as digital infrastructure supporting public service delivery or as a tool to realise other policy goals. However, OECD research has noted that, of the hundreds of public sector blockchain projects that have sprung up over the past few years, few if any have moved beyond pilots and experiments (Lindman et al., 2020[16]). This is to be expected with an emerging technology, and there are several jurisdictions that a now pursuing a new generation of blockchain innovation which is wider in impact, better defined and stands to benefit from a more nuanced understanding of the technology's capabilities and limits.

1.2.3. Rising to meet risks and challenges

Government interest to date has also focused on addressing and anticipating a range of risks and challenges as the technology develops, including immediate risks to legal frameworks and policy objectives, and more indirect threats to common values and the functions of public institutions.

Questions on the applicability of legal frameworks might arise from the decentralised nature of public blockchain networks, which can present situations which may not be anticipated in current laws, which may not fall specifically within existing regulatory perimeters, or which may be beyond the reach of enforcement actions. This could be particularly challenging for applications that are cross-border in nature. Examples of this are numerous in blockchain-based financial applications, as both a highly regulated industry and the sector with the most advanced blockchain adoption to date. These include the difficulty of applying robust anti-money laundering and countering the financing of terrorism (AML/CFT) practices in public blockchain networks, the ability to recover stolen digital assets in the case of a hack, or the requirement in current regulation to have intermediaries acting at specific points within a market, which may be rendered less necessary by blockchain-enabled decentralisation.

While some of these are legitimate risks to enforcement actions, other risks may arise because rules are not always technologically neutral or may be ambiguous in their scope. Uncertainty caused by ambiguous policy and regulations is seen by the industry as a major risk facing blockchain entrepreneurs. In this context, blockchain innovation may reveal areas within existing frameworks which could benefit from less prescriptive, more principles-based regulation which may be more suited to an innovative, fast-changing digital environment.

Governments have an opportunity at this relatively early stage in blockchain's evolution to establish frameworks to guide the technology, so that it develops in a way that is consistent with these shared values, promotes responsible innovation and harnesses the technology fully in the service of citizens. As with other digital technologies, blockchain cuts across traditional policy domains, which means responses require close coordination between functions within a national administration to fully address the systemic nature of impacts (OECD, 2019[17]).

1.3. The need for a strong international lens

The global dynamics of the digital economy broadly, and the cross-border applications for blockchain specifically, mean governments should incorporate international considerations into any policies responding to the benefits and challenges discussed above. Three key rationales for doing so are explored further below.

1.3.1. Fostering co-operation and closer economic ties

Governments today face a policy environment unprecedented in its complexity, scale, pace of change and interconnectedness. Geopolitical trends, including armed conflict, rising economic nationalism and trade tensions, threaten to disrupt the beneficial economic linkages between nations. Global multilateral priorities, such as meeting the Sustainable Development Goals (SDGs) or delivering on the commitments of the United Nations Conference of Parties (COP) climate process, require coordinated global action. The COVID-19 pandemic not only accentuated the fragilities of global economic linkages, but also their value in addressing challenges at a global scale.

OECD research has highlighted the pressing need for a systematic effort to steer innovation and new technology towards such challenges (Hynes, Lees and Müller, 2020[18]), and this includes blockchain. The Forum focussed on the specific role the technology currently plays or could play in building systems that strengthen trade facilitation and supply chain resilience, deliver sustainable development outcomes, strengthen privacy and data governance in the digital economy, and support corporate financing and investment.

1.3.2. Upholding global rules, norms and shared values

While emerging technologies may be usefully harnessed to further international priorities and foreign policy objectives, governments and international standard setters will also need to consider how technologies could run counter to global rules, multilateral priorities, and the values that underpin them. This was reflected in the G7's statement of intent to "place the needs of open, democratic societies at the centre of the technology debate and to work together towards a trusted, values-driven digital ecosystem" (G7, 2021[19])

The Forum explored a number of relevant concerns around the positive and negative impacts on global rules, norms and shared values. Key among these were responsible business conduct issues relating to public networks such as Bitcoin and Ethereum, and in particular the high energy intensity of these networks and whether the business operations behind them are consistent with the ambitious emissions targets set by the COP process. The mobile, international nature of crypto-assets 'mining' operations, some of which

operate in countries with fragile governance systems, also pose wider responsible business conduct risks. Countering the use of crypto-assets in illicit finance has been a major focus for international action and continues to be so.

There are also concerns further on the horizon that should be considered, for example lawmakers have also expressed a concern that, while blockchain promotes high levels of transparency and auditability, such characteristics could be used to turn a currency into an instrument of state or corporate surveillance (House of Lords, 2022[20]).

1.3.3. Supporting an international policy environment for blockchain innovation

Blockchain is an emerging technology which poses a number of novel questions and challenges to existing policy, legal, and regulatory frameworks, and a level of certainty in the regulatory and policy environment would help to foster responsible innovation. Blockchain's ease of operation across borders, and its ability to connect economic activities and administrative systems between jurisdictions, also require a level of coordination between countries on regulatory and technical issues. This is necessary to achieve the interoperability needed to realise many of the cross-border benefits touched on above, to maintain a level playing field, to avoid regulatory arbitrage, and prevent poor conduct spilling over from other jurisdictions.

At the same time, regulatory approaches domestically and internationally must be balanced with a recognition that the technology and its uses will likely continue to evolve, and so the policy environment must allow for innovation and the application of the technology in ways that haven't yet been anticipated.

The remainder of this report is structured around these three rationales for co-operation and coordination on blockchain technology, highlighting relevant market, technological and policy developments, key national and international considerations for policymakers, and existing or emerging approaches to inform responses. It concludes with recommendations, based on the Forum discussions and drawing from the OECD's body of research on blockchain, towards a more cohesive international response.

2 Fostering co-operation and closer economic ties

This section explores some of the ways blockchain technology is already being used to further co-operation and economic ties between countries. The technology is beginning to digitalise trade processes and drive transparency in supply chains. Some major jurisdictions are currently working to develop decentralised digital identity, and are taking steps towards governmental partnerships in those efforts. While blockchain is not common in the governance of large public companies, the technology has enabled parallel decentralised digital capital markets, complete with decentralised corporation-like entities.

If designed appropriately and applied in the right setting, blockchain networks can have the capacity to increase transparency and accountability, transform the notion of trust and governance through code and automation, and empower members of a decentralised, consensus-based distributed system by cutting out intermediaries. The implications for public administration within and between national boundaries are considerable.

Yet OECD research has shown that, despite growing interest using blockchain for public administration and processes, and active innovation by public authorities using the technology, there are still few instances of public sector blockchain applications operating at scale. Rather, the majority of successfully implemented and mainstreamed blockchain applications related to specific policy objectives are in the private sector (Lindman et al., 2020[16]), such as in trade facilitation or business financing. At the same time, there is a push in some jurisdictions towards a new generation of blockchain-based public sector innovation, particularly around the management of digital identity and other credentials.

This section explores some of these more prominent applications, focussing specifically on blockchain's use in facilitating trade and strengthening the resilience of global supply chains; national and cross-border digital credentials; and the corporate governance implications for technology's use in traditional and emerging digital capital markets. For each area, it explores why blockchain is seen as a solution, takes stock of the challenges, details current public and private initiatives, and references existing policy instruments and platforms to guide further government actions.

2.1. Scaling up for international trade

Accelerated by the COVID-19 pandemic, digitalisation is providing new opportunities for international trade and expanding the markets for companies, including SMEs, through e-commerce. However, such developments interact with a policy, regulatory and administrative environment for trade which can be highly complex and slow to adapt, and the benefits of digitalisation are not a given. They require regulatory approaches that support cross-border digital transactions and digital processes, and allow governments to address new challenges raised by digitalisation.

Blockchain applications have the potential to help facilitate trade as well as enhance supply chain efficiency, resilience, transparency and integrity. This potential is relevant for all stages of the supply chain, from customs procedures to trade finance and logistics, and ensuring responsible business conduct.

Complex and costly border processes are one of the key areas where blockchain could bring efficiency gains, simplify procedures and increase transparency. A wide variety of actors are involved in customs and other border procedures, including authorities overseeing health and safety issues. Blockchain technology could facilitate and automate customs and border procedures, verification processes, and streamline interactions between various counterparties in logistics and transportation. Automating and streamlining processes can be particularly beneficial for small firms, for which complying with complex border procedures can be more costly than for larger firms. Analysis of the OECD Trade Facilitation Indicators highlights how automating border processes can help increase SMEs exports by between 4.5% and 6.5% (López González and Sorescu, 2019[21]).

Complex procedures at the border can also make these transactions vulnerable to criminal activity. OECD data shows that after public procurement, most bribery cases took place through customs procedures (OECD, 2014[22]). Promoting effective, streamlined, and automated customs procedures through blockchain technology could contribute to reducing the risks of corruption related to border procedures by removing incentives and opportunities for corrupt behaviour (Moïsé and Sorescu, 2019[23]). Blockchain can also facilitate tracking and tracing of products, provide evidence of their provenance, and help detect illicit trade activity and economic crime.

Moreover, digital solutions can also enhance tax transparency and contribute to combatting tax avoidance in cross-border trade. According to Europol (2016[24]), an estimated EUR 60 billion of tax revenues are lost annually from trade within the EU, with losses likely to be significantly higher in developing economies outside of the EU (Kitsios, Verdier and Jalles, 2020[25]).

2.1.1. Blockchain is already transforming trade

Several blockchain-based projects have been launched in the private sector to facilitate cross-border trade, most of which are based on permissioned or consortium blockchains. Blockchain in trade is primarily focused on enhancing transparency and digitalising trade related processes. A stocktaking report from the World Trade Organisation and Trade Finance Global identified 44 blockchain projects related to trade finance, insurance, know-your-customer (KYC) procedures, shipping and logistics, supply chains and digitalisation of trade processes among other areas (Ganne and Patel, 2020[26]).

Such projects include the development of an international blockchain-based trade network by Japanese businesses, aimed at digitalising and automating exchange of documents and facilitating trade in the region (Yaku, 2021[27]), while other platforms such as We.trade apply blockchain technology and smart contracts to facilitate financial flows between counterparties, aiming to increase transparency and efficiency in trade (We.trade, 2019[28]). Everledger provides a blockchain-based solution in supply chains transparency through effective tracking and tracing of products and ensuring reliable information of their provenance (Everledger, 2021[5]). TradeLens, an industry platform developed by IBM and Maersk, in turn focuses on shipping and is deployed by a number of major players in the global shipping industry (TradeLens, 2022[4]). While these ventures are relatively recent, they are at market and their use is growing, although none could be considered well-established (Ganne and Patel, 2020[26]).

Innovation in the private sector is also being supported by public sector initiatives, although these tend to be at an earlier stage. Discussions at the Forum highlighted the recent collaboration between Australian and Singaporean authorities, and businesses in selected sectors, to trial a blockchain platform to facilitate international trade and digitalise trade documents and processes. The UK also launched the Reducing Friction in International Trade (RFIT) project in March 2019 to explore the use of blockchain in managing supply chain data and linking it to customs and food standards information to increase transparency and traceability in international trade. The testing stage showed reduction in administrative burden at the border and duplication of data, with increased efficiencies from automation (UK Government, 2020[29]).

2.1.2. Challenges and risks related to blockchain's use in international trade

As with other digital trade facilitation tools, blockchain technology must harness network effects across both public and private stakeholders to drive operational efficiencies, which rely on streamlined interaction across actors. New blockchain systems also present an opportunity to drive a level of standardisation of data, systems and processes, but such interoperability is not assured.

World Trade Organisation research (Ganne, 2018[30]) has underlined specific challenges related to interoperability that can stand in the way of using blockchain to its full potential in trade:

- At the technical level, different blockchain platforms and networks need to be able to interact with each other. While standards exist, including ISO technical standards, compatibility problems with different types of blockchains still remain due to the high degree of fragmentation and diversity of platforms.
- Interactions between the digital and real-world environments is an important point of risk. While blockchain can provide an immutable record of data, allowing tracking and tracing of products, such data is a representation of physical goods and events, and information must be accurate when it is digitised and placed on the blockchain. Integrity frameworks need to be in place in the offline environment to ensure accuracy and veracity.
- Common standards for data are necessary: different stakeholders in trade, such as customs officials, logistics companies and businesses, often use different standards and have diverse practices in collecting, registering and interpreting data. Consistent and unified standards for data, which could be stored on and exchanged via blockchain, are key to ensuring smooth international co-operation.

In order to establish interoperability between trade-related blockchain platforms and national legal frameworks, the electronic format of information stored on blockchain (such as signatures, documents and transactions) need to be legally recognised. Consistency in the legal approach to the information stored on blockchain across jurisdictions is particularly important when the technology is used for international trade.

In this sense, in 2017, the United Nations Commission on International Trade Law adopted a Model Law on Electronic Transferable Records (MLETR), which aims at ensuring legal recognition of electronic

transferable records domestically and internationally. However, analysis of the OECD Digital Trade Inventory highlights that most jurisdictions still face many challenges in promoting paperless trade and facilitating electronic transactions (Nemeto and López González, 2021[31]).

2.2. Digital identity and other digital credentials

The OECD has long emphasised the importance of identity management and the authentication as a core element of the digital economy (OECD, 2011[32]), and yet these aspects of online life have evolved at a much slower pace than the rest of the digital economy.

As the digital footprint of the average citizen has grown, so too has the quantity of personal data collected, stored and used by third parties, spanning social media, providers of goods and services, transportation, banking, healthcare, education and public services and beyond. Artificial intelligence, machine learning and other big data analytical techniques have placed this data at the heart of many of the digital economy's most successful business models, with implications for competition, consumer rights, security and privacy (OECD, 2020[33]). The growing economic importance of personal data has coincided with a growing sense that many participants in the digital economy do not control their own identity or data, and do not trust the organisations that do (Ipsos, 2019[34]). Such concerns have only grown with the accelerated digitalisation spurred by the COVID-19 pandemic.

The provision of identity documents and other credentials, such as passports or drivers licenses, is a core function of governments, and public institutions are increasingly exploring and developing digital identity solutions to better meet the needs of the digital economy and to address these concerns around personal data, but also to support access to public services and to lift inclusion. For example, in the two years between 2019 and 2021 adoption by the public of digital identity solutions increased by 269% in Italy and 1662% in Australia (OECD, 2021[35]).

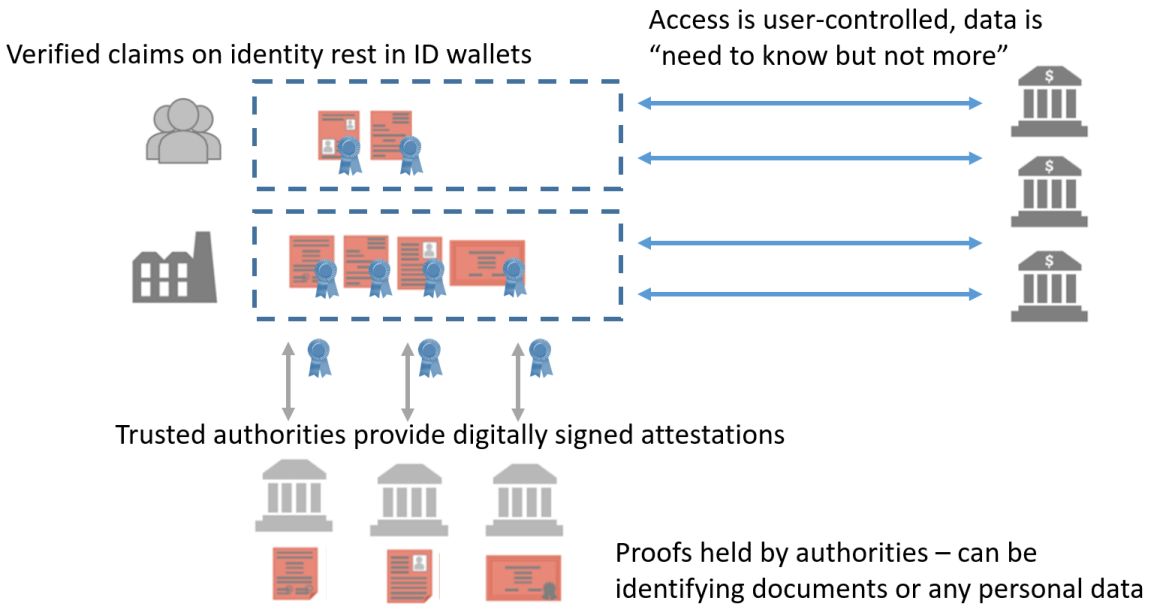
2.2.1. Governments are exploring blockchain for digital credentials

There are a number of technical approaches that could underpin the public sector's provision and verification of digital identity and other credentials. Current approaches commonly use authentication tools like biometrics, passwords, two-factor authentication through mobile phones, and smart cards to access credentials from a central database. A number of countries and jurisdictions have expressed interest in blockchain-based solutions for next-generation digital identity management, and are actively exploring this. It must be observed, however, that none have moved beyond scoping or pilot phase (see Box 2).

Blockchain is of interest for digital identity as it allows citizens to collect credentials, attestations and discrete pieces of data from a decentralised network of institutions, share these details when needed, and revoke access when not needed. Going further, it enables "zero-knowledge proofs", where a trusted institution can attest to information regarding a person without revealing the underlying data; for example a government birth registry could provide a digital attestation that a person is over the age of 18 without revealing their exact birthday (or any other details) to a third party. The attestation could be provided anew with each use of a service, so that it is not stored as personal data by the third party. The enabling by decentralised technologies of citizens to collect and control their own identifying data has been termed "Self Sovereign Identity".

Such attestations would be stored in an encrypted identity "wallet" controlled by the person, or the organisation, to whom they relate, and could encompass a range of information including educational, professional and financial credentials (see Figure 1). It's important to note that, under such a model, the underlying personal information is not stored on the blockchain itself; blockchain is used to store and transmit *encrypted digital attestations*, which verify certain characteristics based on underlying personal information that remains held in trusted institutions like birth registries or passport agencies.

Figure 1. Model of decentralised Self Sovereign Identity



Source: Bits on Blocks (2017[36]), A gentle introduction to self-sovereign identity, https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/

In this way, decentralisation addresses some of the most pressing privacy concerns of the modern digital economy, as only the minimum amount of information needed for a transaction is revealed, and only for the duration of that transaction; citizens would no longer leave a trail of personal information behind them as they use digital goods and services. It also has positive implications for cybersecurity; because there sensitive and personal data is stored and in fewer places, there would be both less incentive for bad actors to hack databases, and less serious consequences to consumers should breaches occur.

A number of jurisdictions, including the European Commission, Canada and Germany, are exploring blockchain-based identity management, while Estonia has built a blockchain overlay to secure some types of sensitive personal data (see Box 2). This public sector interest is complemented by private offerings, with large technology providers such as Accenture and IBM offering digital infrastructure to deploy decentralised identity services.

With public sector projects in train and with a high levels of interest in digital identity more broadly, it is also important to emphasise that, when considering blockchain solutions for digital identity (or any other application), governments must assess technological options and be clear on the value and business benefits of using blockchain relative to other solutions.

Box 2. National and regional initiatives for decentralised identity

European Self-Sovereign Identity Framework

The European Commission has placed the development of a self-sovereign identity as a priority in its Blockchain Strategy, and has established the *European Self Sovereign Identity Framework Laboratory* to "advance the broad uptake of self-sovereign identity as a next-generation open and trusted digital identity solution". A core focus is to drive scalability and interoperability between solutions, in line with the European Union's regulation on electronic authentication systems, with the aim of deploying

solutions on the pan-European European Blockchain Services Infrastructure (European Commission, 2019[37]).

Innovation competition to develop a self-sovereign identity in Germany

The Federal Ministry for Economic Affairs and Energy of Germany has convened 11 consortia in a competition to develop digital identity solutions for widespread use in Germany, of which at least four are focused on decentralised and self-sovereign identity. Several projects will be selected for implementation, supported by research and public development grants, between 2022 and 2025 (BMWK, 2020[38]).

Canada-Netherlands Known Traveller Digital Identity Pilot

Working with a range of stakeholders, the World Economic Forum has developed a prototype decentralised identity framework for cross-border travellers, which allows travellers to collect attestations from trusted sources, such as banks, universities, airlines and medical record keepers, in a digital profile that can be shared with public authorities to support completely digital visa applications and border controls. The framework is currently being trialled for air passengers between Canada and the Netherlands (World Economic Forum, 2018[7]).

Protecting sensitive data with the Estonian KSI Blockchain

Estonia has a centralised universal digital identity system managed by its government, which is deployed over a national network to access over 3,000 electronic services. The country's national digital ecosystem is highly efficient but also had security vulnerabilities, which were evident in wide-scale cyberattacks in 2007. As part of its response, Estonian authorities adopted a blockchain system which records changes to data and detects tampering for a range of sensitive databases, including health and justice records. While not a decentralised identity system, it illustrates the effective use of a mix of technologies to deliver different priorities within an ecosystem of sensitive personal information (Enterprise Estonia, 2017[10]).

2.2.2. Parallel efforts risk fragmentation

With initiatives to develop blockchain-based digital identity and credential management progressing, there are a number of imperatives to ensure these projects move forward in a way that supports economic activity and exchanges across borders, and are leveraged for wider economic development.

Digital identity information, whether based on blockchain or not, holds great potential to verify individuals' and organisations' identity quickly and reliably at the border and within foreign markets. These systems could also be linked to educational and professional credentials, KYC checks and tax payments. In doing so, such applications could support labour mobility, facilitate investment and support implementation and development of some of the digital trade and customs use cases discussed earlier in this report.

Technical interoperability and legal recognition of digital identities between jurisdictions is a pre-condition to realise these cross-border benefits, and so public sector digital identity efforts would benefits from referencing one another and taking into account international considerations. For example, as detailed in Box 2, The European Commission is seeking to drive technical interoperability among member states on self-sovereign identity through its European Blockchain Services Infrastructure, a distributed ecosystem hosted across member states, with policy interoperability grounded in existing European regulations on electronic identity. In an effort to internationalise this work, the European Commission and Canadian Government have formed a partnership to pursue interoperability of digital identities and other credentials between the two jurisdictions (see Box 3).

A concerted and inclusive multilateral effort between countries is needed to avoid fragmentation, and in 2021 G20 Digital Ministers called for harmonisation and international standard setting on responsible deployment of digital identity and interoperability of digital identity systems (G20, 2021[39]).

Box 3. European Commission-Canada Partnership on Digital Credentials

The European Commission and Canadian Government have been working jointly to examine the cross-border self-sovereign identity, blockchain and digital credential use cases. Over the spring and summer of 2021 the two authorities held a series of exploratory workshops on enabling interoperability and mutual support for digital credentials, focussing on technical and policy issues.

The workshops emphasised the existing foundation the EU and Canada have to build cross-border credential capabilities, particularly the good alignment of policy frameworks for privacy and data protection. However, the EU and Canada both already have a range of digital identity and credential technologies within their jurisdictions across sectors and levels of government, lacking standardisation within borders that makes cross-border standardisation challenging. The use of zero-knowledge proofs were also identified as a potential challenge, as this technology model is ahead of policy frameworks and its interaction with European data and privacy laws is unclear.

The need for common principles in credential frameworks was also flagged, based on international technical standards and best practices, a baseline level of compatibility, and open protocols. Developing common projects (for example pilots and use cases) was labelled as the most useful exercise in identifying practical interoperability challenges.

This work has been formalised in a partnership announced in November 2021 with the intent of opening the dialogue to an expanded group of countries.

Source: Government of Canada (2021[40]), Canada and the European Union Joint Workshop Series for Enabling Interoperability and Mutual Support for Digital Credentials, https://www.ic.gc.ca/eic/site/153.nsf/eng/h_00006.html

Blockchain-based electronic identity also has potential to meet a number of international development challenges. The ability to prove one's identity and manage personal information is recognised in the SDGs and, similarly, the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights establishes the rights of all individuals to be recognised as a person before the law. Global initiatives, such as ID2020, an international alliance of businesses, non-governmental organisations, governments and individuals, and the ID4D initiative of the World Bank Group, have closely considered blockchain solutions in this context.

Streamlined, trustworthy KYC processes and records could also help drive financial inclusion and access to global financial markets in developing countries. The compliance costs of due diligence and managing AML/CFT risks in correspondent banking relationships have been a significant driver in de-risking in the international financial system, which has resulted in the termination of correspondent banking relationships between large international banks and smaller local banks in developing markets, sometimes with significant negative effects on economic development (The Commonwealth, 2016[41]). Blockchain's ability to verify and secure data, and share it between parties in a way that can be audited and preserve privacy, could make AML/CFT cheaper, KYC checks transferable, and give greater assurance of due diligence procedures between financial institutions, including correspondent banks. With such aims in mind, blockchain based electronic KYC was piloted in the city of Dubai through the UAE KYC Blockchain Consortium, and is now being expanded (Norbloc, 2021[42]).

2.2.3. Challenges and risks related to blockchain-based credential management

While blockchain may offer a tool to make digital identity and credentials management more fit-for-purpose in the digital economy, there are a number of risks and considerations.

Depending on the configuration of the network and applications, certain features of blockchain can increase privacy risks as, due to the immutability of data, it can be extremely difficult or even impossible to rectify inaccurate data on some blockchains. Applying the right to be forgotten, a feature of the EU General Data Protection Regulation (GDPR) that provides the right to have personal information removed from the online environment, may similarly be difficult on some blockchain networks. However these issues are largely related to public, permissionless networks, and most self-sovereign identity solutions do not write any personal information to the blockchain.

Blockchain solutions are not a substitute for identity systems that are otherwise unreliable or corrupted. Self-sovereign identity models can attest to information established by third parties, for example age, educational attainment or vaccination status, but it cannot determine if that original information is accurate. As with any system that manages identities, digital identity systems require safeguards, monitoring mechanisms and clear definitions of responsibilities and roles to ensure accuracy, completeness, consistency, and integrity of the information. In the case of cross-border use of the digital identity data, clear standards and rules should be developed in coordination with all relevant stakeholders (OECD, 2019[43]).

Digital inclusion is also a key consideration, particularly where access to public services is concerned. G20 Digital Ministers have underlined their support for digital identity solutions that are based on users' consent and ensure privacy and security of personal information, and that additional means for accessing public services should exist in beyond digital identity (G20, 2021[39]).

2.3. Corporate governance and capital formation in a decentralised future

The COVID-19 pandemic's shock to financial markets brought about policy responses and rescue packages that emphasised corporate financing and access to capital from both domestic and international investors. Good corporate governance is central to establishing an environment around capital formation grounded in trust, transparency and accountability, and is a precondition to long-term investment and financial stability. This is particularly important given the growing importance of cross-border equity investment (De La Cruz, Medina and Tang, 2019[44]).

The Forum in 2021 built on its previous discussions on blockchain's use in and impact on capital markets and related corporate governance issues. The focus of discussions ranged from the use of blockchain in mainstream corporate governance processes, i.e. transforming existing rules and norms into technical codes and registries, to emerging forms of decentralised digital capital markets and the governance structures underpinning them.

2.3.1. Blockchain isn't being meaningfully applied in corporate governance processes

Inefficiencies and lack of transparency in some shareholder relations practices, and also around the beneficial owners of corporations, have placed a spotlight on the potential for digital transformation in corporate governance. Shareholder voting, for example, is often carried out through a complex voting chain involving a host of intermediaries where identifying and communicating with the beneficial owners or others with legal authority to vote can be difficult, and it can also be difficult for those owners to be confident that their votes have been cast as intended.

Blockchain solutions have also been suggested for recording and tracking share purchases, which could also provide valuable information on the beneficial owners of corporate entities and investment vehicles,

while maintaining a high level of privacy for the owners. Such applications could help address the opacity of ownership that can make AML/CFT rules and OECD global tax rules difficult to enforce (de Jong, Meyer and Owens, 2017[45]).The use of blockchain-based smart contracts has also been suggested as a useful means to enhance the efficiency of audit processes.

Box 4. What are smart contracts?

Smart contracts are pieces of code written on a blockchain that perform an action when certain pre-defined conditions are met. They are a major element of the 'automation' and 'disintermediation' features of blockchain technology, as processes can be programmed in a smart contract and then left to run, with users free to engage with the smart contract to access the service it is offering. These smart contracts are an important tool to govern activity on the blockchain, as they can be used to set the rules and parameters by which users interact. They are also the building blocks of the decentralised apps and platforms, including decentralised finance services and Decentralised Autonomous Organisations (see below).

In theory smart contracts remove the need for trust between transacting parties, as the rules of the transaction are visible and predictable. But parties must instead be satisfied with the integrity of the smart contract – something that may be difficult without sophisticated programming knowledge. There are several high-profile examples of bugs or security holes being exploited in smart contracts and, because of the immutability of blockchains, unexpected or undesired outcomes can be difficult to reverse.

Source: IBM, (2021[46]) Smart contracts defined, https://www.ibm.com/topics/smart-contracts

However, while there have been a few pilot initiatives with respect to some of these ideas, the Forum's discussions concluded that the use of blockchain for such corporate governance processes has remained quite limited to date, despite the swift uptake of other digital tools to support corporate governance processes during the COVID-19 pandemic. Forum discussants noted that there were few real regulatory barriers to blockchain adoption in this area, particularly as regulators had moved to support digitalisation processes in areas like voting, for example through the EU's Shareholder Rights Directive II. Rather, they cited the lack of scaled, proven use cases in the corporate governance, with many market participants questioning issues around privacy and data security, scalability, interoperability and technical maintenance. Until the technology matures and its use cases become more clear-cut in this area, the potential for blockchain to transform traditional corporate governance processes may be more distant than in some other sectors. However, given the future potential of these technologies to support some key priorities of market regulators mentioned above, they should remain of interest to public authorities.

2.3.2. Decentralised corporate governance structures are flourishing

In contrast to blockchain's use in corporate governance processes, decentralised corporate governance structures are now a major feature of the crypto-asset world, and particularly in the decentralised finance (DeFi) market. The DeFi market is run primarily through smart contracts, and its networks and applications are generally claimed to be open, decentralised, permissionless and autonomous. At its recent peak in November 2021, the DeFi market held crypto-assets worth over USD 110 billion in smart contracts related to lending, derivatives and exchanges (Nassr, 2022[47]). Though small relative to traditional financial markets, the considerable growth of DeFi over the past 18 months and the potential for interconnectedness with the traditional financial sector has demanded the attention of regulators (OECD, 2022[48]).

Decentralised Autonomous Organisations (DAOs) have become a significant feature of DeFi as market infrastructure providers, vehicles for capital raising in DeFi ventures, and as market participants. These organisations govern specific DeFi protocols and products, and are steered by investors who have exchanged money or crypto-assets for governance tokens, and which usually have voting and resolution rights attached. These governance tokens can also be valuable crypto-assets in their own right and are frequently traded in secondary markets. The "organisation" itself is essentially a series of smart contracts which, taken together, direct activities and expenditure in an automated way, and enshrine the rights of governance token holders (Consensys, 2021[49]). At the time of writing, DAOs controlled an estimated USD 8.8 billion in assets, and the individuals involved in DAOs as governance token holders has grown nearly tenfold in the past six months, to 1.7 million people (DeepDAO, 2022[50])

Some DAOs have restrictions on membership, but the majority are open to any individual willing to purchase governance tokens. Many DAOs also attract funds with the explicit or implicit promise of returning a profit to their members, by providing returns from a revenue-producing service or investing in (digital) assets expected to grow in value. From a business financing perspective, they may offer a novel and inclusive vehicle to raise capital in a digital setting, and could offer entrepreneurs access to global capital pools and international investors. From a corporate governance perspective, blockchain and smart contracts could enable high levels of transparency in the ownership of DAOs and direct participation by owners. This could theoretically reduce the distance between beneficial owners and business decisions, potentially addressing some of the principal-agent problems that gave rise to key features of traditional corporate governance – however, the reality of how DAOs already operate make such claims questionable.

Box 5. MakerDAO: Lending services on an automated, decentralised business platform

MakerDAO is a DAO which illustrates the level of business complexity capable by smart contracts, and the often multi-faceted nature of DAOs and both products and organisations.

MakerDAO provides an automated lending platform for crypto-assets based on the Ethereum blockchain. A user deposits crypto-assets, which serve as collateral for a loan, into the MakerDAO smart contract. In turn, the smart contract pays the user a loan, predefined in the terms of the smart contract and denominated in Dai, which is a crypto-asset created by MakerDAO with a value nominally pegged to one US dollar. If the lone is not repaid or if the value of the underlying collateral slips below a certain limit, the collateral is liquidated automatically and auctioned off.

Dai's value is not underpinned by any real-world financial asset; its soft peg is maintained through a series of smart contracts that rely on the collateral provided in exchange for Dai, and on price incentives for users to either create Dai (by depositing collateral) or destroy it (by repaying outstanding loans).

Many of the parameters of MakerDAO's smart contracts are set by the holders of the DAO's governance token, MKR. Holders of MKR receive a share of the fees charged for loans made by the service, and they also have the right to vote on changes to the service – for example the type of crypto-assets accepted as collateral, or the collateralisation rate for loans. MKR can also be created automatically and auctioned off for Dai to raise further capital if defaults threaten the service's capitalisation.

Source: Gemini (2021[9]), Cryptopedia: What Is MakerDAO?, https://www.gemini.com/cryptopedia/makerdao-dai-decentralized-autonomous-organization

The recent rise of DAOs and DeFi markets more broadly pose questions as to where the activities of these organisations and market participants should fall within the regulatory perimeter. However, public authorities are beginning to turn their attention to the legal ramifications of such arrangements. In August 2021, the state of Wyoming in the United States granted limited liability company status to DAOs based in

the state, with legislation aiming to grant limited liability to DAO developers and governance token holders, and enable judicial verification and acknowledgement of transactions and smart contracts (Lewis and Zeglarski, 2021[51]). At the same time, the US Securities and Exchanges Commission is currently probing Uniswap Labs, the development team which created the Uniswap DAO, over how investors use Uniswap and how it has been marketed (Michaels and Osipovich, 2021[52]).

While governance of a decentralised organisation could theoretically be more democratic and transparent, such organisations could perversely face similar challenges as in traditional corporate governance. OECD research has shown that holdings of governance tokens in some of the most-used DeFi protocols are centralised in the hands of a few actors, including the original developers, leading to conflicts of interest. Governance tokens could be obtained by a flash loan, where they are borrowed, used to vote and instantly returned, allowing actors unpredictable and undue levels of influence. Voting participation of governance token holders can also be low, with resolutions passing with as little as one per cent of eligible votes cast, and decentralisation does not appear to support the ability of many token holders to access and assess relevant information for their decision-making (OECD, 2022[48]).

This suggests that, despite the so-called “decentralised trust”, current practices of DAOs and DeFi markets have not solved some of the basic issues which corporate governance is intended to address, such as conflicts of interest and information asymmetries.

2.3.3. Challenges and risks related to decentralised corporate governance

DAOs underline the many difficulties in regulating new corporate structures and activities based on blockchain, and policy responses have been slow and fragmented due to a lack of capacity and knowledge to address issues related to these structures.

DAO membership and operations are often not confined to a single jurisdiction, so it can be unclear which laws would apply to them and where. Moreover, questions can be raised whether tokens should be classified as securities, and if so, whether securities regulations and related obligations (and of which jurisdiction) would be applicable. Ultimately, imposing legal requirements without legal recognition is likely to be a challenge. As new decentralised corporate structures do not involve traditional roles, such as a board of directors and shareholders, imposing liabilities and enforcing laws would likely be particularly difficult. Many of these issues are not limited to DAOs, and are of concern to other public, permissionless blockchain applications too.

There are a number of vulnerabilities relating to criminal activity as well. As many of the technical aspects of DeFi services are complex and their widespread use is relatively recent, errors and bugs are common, making networks and protocols vulnerable to hacking and other security threats, with approximately USD 2.3 billion in crypto-assets lost to date (CryptoSec, 2022[53]). Because of the immutability of blockchain networks, particularly the public, permissionless networks common in the DeFi space, theft, exploiting bugs in code and other losses can be near-impossible to reverse or redress. Without the involvement of a central authority, KYC practices in DeFi are easily bypassed and applied piecemeal (see Box 9), and the decentralisation and anonymity can make it difficult for law enforcement to determine liability for compliance and carry out investigations in the case of suspected wrongdoing.

One solution proposed is to build legal or regulatory provisions into the codes of smart contracts so that compliance is automated and built into the ecosystem – but this itself presents a host of operational and legal questions (Hassan and De Filippi, 2017[54]). Whatever the solution, there is a challenge in striking a balance between delivering on regulatory mandates around market integrity, fairness, efficiency and stability, while also allowing the technology to develop and the benefits of innovation to be captured.

3 Upholding global rules and norms

This section explores two of the most frequently cited concerns on blockchain technology: its impact on the environment and greenhouse gas emissions; and its use in illicit financial flows and criminal transactions. While many types of blockchain networks are not energy intensive, the underlying energy mix – and climate impact – of those that are is not clear-cut. Public and private sector actors should also be considering a more expansive set of non-financial risks across other Environmental, Social and Governance factors. In combatting illicit financial flows, the Financial Action Task Force has put in place a robust set of international rules, but a stronger push is needed by countries to enact and enforce them, and by businesses to implement them.

The previous section outlined blockchain's current or potential value to several key international economic priorities, and touched on a number of the associated challenges. These challenges are not minor concerns, and in 2021 G20 digital ministers issued a call for all new technologies to develop in a way that is responsible and human-centred and for digitalisation to support inclusion and sustainability – and singled out the need to address digital technologies that consume a significant amount of energy or that have negative impacts on the environment (G20, 2021[39]).

Governments and businesses must ensure that the design and use of blockchain applications is consistent with such expectations, and does not run counter to global rules or to specific policy goals pursued by the international community. To this end, the Forum addressed two of the most frequently cited concerns from policymakers regarding blockchain: the energy intensity of the computational power required in some networks and implications for international climate efforts; and the use of the technology to support criminal activity, particularly around AML/CFT.

It should be noted that both issues are most relevant to the kinds of public, permissionless blockchain networks that are particularly resistant to outside rules or government intervention. Blockchains that are

more centrally controlled, such as those used by large corporations or being developed by governments, have consensus mechanisms that generally require lower levels of computational power and hence lower energy consumption, while networks that are permissioned are only accessible to individuals or entities whose identity is known, making detection of and enforcement against criminal activity easier.

3.1. Environmental, Social and Governance issues in blockchain networks

The incorporation of Environmental, Social and Governance (ESG) considerations into financial markets and business operations has emerged as the primary means to capture societal values and policy goals into private sector incentives, and is expected to play a major role in aligning private sector activities with climate goals and the transition to net-zero emissions (OECD, 2021[55]). ESG practices, disclosures and reporting have some way to go in becoming a useful tool for investors and businesses managing in climate risks, and the establishment of an International Sustainability Standards Board (ISSB) to govern ESG reporting, announced at the Glasgow Climate Change Conference and welcomed by 40 countries, is an important step (UK Government, 2021[56]). Given the urgency of climate action, the ISSB will focus initially on climate-related disclosures, before developing frameworks for other elements of ESG.

New technologies must reflect the growing expectation among market participants, governments and wider society that private sector actors manage their ESG risk, and particularly their contributions to environmental and climate risks, if they hope for mainstream adoption and a strong social license. This is certainly the case for any new markets, business models and products enabled by blockchain technology.

3.1.1. Assessing energy use and environmental impact

In the context of the growing importance of ESG broadly and the urgent need to move away from carbon-intensive economic activities in particular, considerable public discourse has focussed on the energy usage of the two most popular public blockchain networks, Bitcoin and Ethereum. These two networks use a "proof of work" consensus mechanism which incentivises the use of considerable computing power, and thus the use of considerable amounts of energy, as network nodes compete to verify transactions on the blockchain and gain the rewards for doing so. These activities are referred to as *mining*, and the annual energy usage of the mining operations that form the backbone of these networks is often compared to that of medium-sized countries; by some estimates the Bitcoin network uses 0.5% of all electricity consumed in the world (Huang, O'Neill and Tabuchi, 2021[57]), and though Ethereum's estimated energy usage is lower that Bitcoin's it is still considerable (Ethereum.org, 2022[58]). Newer generation public blockchain networks use different consensus mechanisms that are considerably less energy intensive, and Ethereum plans to migrate one of these in the near future, while private blockchains can be more akin to regular computer networks in their energy usage (see Box 6).

When assessing the environmental impact of public blockchains, energy consumption is a key consideration, but so is the energy mix. Miners have a natural market incentive to use the cheapest energy possible, and their operations are fairly mobile, which means many mining operators seek out opportunities to capture surplus renewable energy during seasonal peaks. Research from the Cambridge Centre for Alternative Finance has traced the seasonal migration of Chinese miners to areas of hydroelectric power oversupply, before mining was outlawed in the country in 2021 (Blandin et al., 2020[59]). While the study noted the difficulty in compiling reliable data, it estimates that the majority of miners (76 per cent) include renewable energy their energy mix, and that renewables account for roughly 39 per cent of total mining energy inputs.

Such numbers underline that an accurate understanding the sector's carbon footprint is not as straightforward as its energy use alone – but they also suggest that mining activities associated with Bitcoin

(and, by extension, Ethereum in its current form) could still result in the creation of considerable quantities of greenhouse gas emissions.

Box 6. Consensus mechanisms and energy consumption

There are a wide range of different consensus mechanisms used in blockchain networks, each with their own trade-offs between features like speed, security, and computing power. The mechanism used will often depend on how well known the participants are to one another and the level of trust between them. Networks that are more private and permissioned tend to run on "proof of authority" mechanisms, where trusted nodes have the right to vote on the addition or change of data on the blockchain, with the assumption that most nodes are honest and together will outvote nodes offering incorrect or dishonest data, reaching a majority consensus. Because of the low computing power involved, such networks have relatively low energy needs.

Public blockchains have more taxing consensus mechanisms because the parties are less likely to be known to one another, and may have diverging interests. Such consensus mechanisms often require participants to stake computational or financial resources to validate data, and among these "proof of work" (PoW) and "proof of stake" (PoS) are the most common.

In PoW mechanisms, such as those used in the Bitcoin or Ethereum blockchains, nodes compete to validate transactions by guessing the solution to a cryptographic puzzle. The puzzle is solved by computers running through all possible solutions of a large-value number until the correct one is found – this is the "work" in the mechanism, and requires considerable amounts of computing power and, by extension, electricity. While resource intensive and relatively slow, it does produce a highly secure network with high levels of data integrity.

In PoS mechanisms, nodes are selected at random to be validators for a set of transactions, and each node has a higher probability of being selected the more of the network's crypto-asset it has "staked", or locked up, for the validation process. Data is validated once it has been verified by a set number of nodes, which receive new crypto-assets in exchange for validation, while nodes that verify or propose fraudulent or incorrect data risk losing the crypto-assets they have staked.

This reduces the computational (and energy) intensity of the consensus mechanism considerably compared to PoW, makes validation and transaction settlement faster, and is cheaper in terms of fees paid by users. However, it is also cryptographically a less reliable record of transactions, and comes with governance risks, such as businesses with large holdings of cryptoassets (for example, exchanges) having potentially disproportionate control of a network, the propensity for large crypto-asset holders to be chosen more often and hence accumulate yet more newly created crypto-assets, creating issues around centralisation and inclusion, and the potential for the formation of validator cartels.

Recent blockchain networks tend to use a variation of a PoS consensus mechanism, while the Ethereum network is expected to transition to a PoS mechanism in 2022.

Source: Bains P. (2022[60]), Blockchain Consensus Mechanisms: A Primer for Supervisors, https://www.imf.org/-/media/Files/Publications/FTN063/2022/FTNEA2022003.ashx

Market incentives may also push mining operations into locations where non-renewable energy is artificially cheap, elevating ESG risk factors into the social and governance elements as well. There is anecdotal evidence of Bitcoin mining operations flourishing in areas where fossil fuel-based energy is subsidised, such as Kosovo (Bratanic, 2022[61]), while the establishment of mining operations in jurisdictions with fragile public institutions and high incidences of corruption include the possibility of bribery in relation to electricity supplies.

3.1.2. The benefit of a Responsible Business Conduct lens

ESG risks are not limited to the energy and climate aspects discussed above, and there are a wider range of risks immediately within public networks, and upstream and downstream in the crypto-asset supply chain. Those mentioned in Forum discussions included:

- The use of crypto-assets in criminal activity, particularly in money laundering and terrorist financing, is a common concern among governments, and is discussed in detail in section 3.2 below;
- The risk that blockchain-based assets and applications are used for tax evasion or fall outside of tax codes, which has been raised in the past by G20 Finance Ministers (G20, 2018[62]);
- Additional environmental and climate ramifications of the capital inputs to mining, particularly computers hardware; and
- Legal and regulatory risks, given the mobility of mining operations, the fiercely competitive nature of mining, and the fact that miners are spread across many different countries can give rise to, as miners may be incentivised to gain an advantage through poor conduct or regulatory arbitrage by operating in areas with less robust governance and institutions.

ESG concerns also pose risks to businesses upstream to these blockchain networks, including crypto-asset exchanges, decentralised app developers, lenders and private equity providers, and regulated financial institutions and other businesses exposed to crypto-assets. Because access to public, permissionless blockchains cannot be restricted, and activities on those networks are not easily governed by outside authorities, the responsibility of ESG risk management could focus on those identifiable actors, and in particular the exchanges as the "on and off ramps" that connect activity and assets on public blockchains to traditional economic and financial systems.

Given the complex web of actors within the crypto-asset supply chain, the multinational nature of these networks and the wide range of ESG risks, the Forum explored the application of a Responsible Business Conduct (RBC) approach to manage these challenges, to support high levels of market integrity, and to attract the confidence of stakeholders, including governments. RBC is an approach whereby all businesses, regardless of their legal status, size, ownership or sector, act to avoid and address negative impacts of their operations, including upstream and downstream in the supply chain, and contribute to sustainable development in the countries where they operate. The most comprehensive international standard on RBC is the *OECD Guidelines for Multinational Enterprises*, which is reinforced by accompanying standards on due diligence.

Box 7. The OECD Guidelines for Multinational Enterprises

The OECD Guidelines for Multinational Enterprises are government-backed recommendations for businesses to address negative impacts and risks to human rights, the environment, consumers, governance and corruption, while also maximising positive economic, environmental, and social contributions. To mitigate and prevent such risks, the Guidelines set out an expectation for responsible business conduct through due diligence of a company's operations and all parties involved in their supply chain, and for governments to set up policy conditions to promote responsible business conduct. The OECD Due Diligence Guidance for Responsible Business Conduct in turn sets out detailed recommendations on how to conduct due diligence, engage with supply chains and affected stakeholders, and publicly report on due diligence efforts.

The Forum drew on experiences in the minerals sector to illustrate the role of upstream actors and platforms in driving positive RBC practices and ESG risk management. It highlighted the experience of the London Bullion Market Association, the world's largest market for gold and silver, in introducing responsible

sourcing requirements, based on the *OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High Risk Areas*. Though the risks and the role of exchanges between minerals and crypto-assets are far from equivalent, the power of exchanges to drive adoption of RBC practices in suppliers and producers, and orient sectoral business practices towards international standards and norms more broadly, demonstrates the roles and responsibilities of market infrastructure providers. It is a particularly important observation as many governments grapple with the challenges of ensuring market integrity, including on emissions and climate, in decentralised markets.

3.1.3. The positive potential to lift business conduct

The burgeoning use of blockchain in supply chain transparency and traceability (discussed in section 2.1) also brings the potential for greater insights to conditions across supply chains, enabling easier and more reliable due diligence when implementing RBC approaches. The OECD previously investigated RBC due diligence use cases in physical commodity supply chains, finding particular promise in overcoming a range of due diligence hurdles. An auditable, electronic end-to-end record of the movements of goods could allow the combating of fraud, provide assurances on pay and conditions along the supply chain, ease the costs of due diligence, and provide data to promote access to finance. Such solutions have been piloted by Hugo Boss in the garment sector, Volvo for cobalt supplies for batteries, and AB InBev to manage agricultural suppliers (OECD, 2019[63]).

However, the paper also found limitations to these systems, particularly in integrating less formal actors in supply chains such as artisanal miners or garment workers, and verifying data inputs at the top end of the supply chain, for example at a mine site or smallholder farm. There were also similar challenges to those outlined earlier in this report for blockchain's use in trade facilitation; ensuring the veracity of data placed on the blockchain requires robust real-world governance structures, while interoperability between systems and data needs is challenging given the complexity of global value chains and the myriad inputs that go into finished products.

3.2. Combatting financial crime in virtual assets

Certain features of blockchain-based crypto-assets, including anonymity and the global reach of decentralised networks, can elevate the risks of criminal activity, such as fraud, cybercrime, tax evasion, illicit trade, money laundering, terrorism financing and human trafficking. These risks are among public institutions' most serious concerns regarding public, permissionless blockchains. To address these risks, the Financial Action Task Force (FATF) has issued binding Standards on virtual assets[1] and virtual asset service providers (VASPs), which require VASPs to comply with AML/CFT requirements.

3.2.1. Robust international standards exist, but implementation lags

In July 2021, the FATF completed a second twelve-month review of the implementation of the revised virtual asset Standards. While implementation has strengthened, the report nevertheless revealed remaining gaps across jurisdictions, underlining insufficient global coherence in preventing criminal activity related to virtual assets. The report highlights how the lack of AML/CFT regulation and enforcement by countries is enabling illicit actors to exploit this jurisdictional arbitrage, raising money laundering and terrorist financing risks.

The 'travel rule' is a core part of the Standards on virtual assets and the wider body of FATF recommendations, and requires businesses to collect and submit personal data of participants (both,

[1] The term "virtual asset" is used in FATF rules but can be used largely interchangeably with the term "crypto-asset" used elsewhere in this report.

originator and beneficiary) involved in a transaction. With effective national implementation, the 'travel rule' can increase transparency, allow law enforcement to trace illicit flows and allow VASPs to comply with international sanctions obligations. The FATF review found that insufficient implementation of the 'travel rule' at the national level can reduce incentives for the private sector and VASPs to advance innovation and develop solutions to facilitate application of the rule. Gaps in national implementation, in turn, are commonly explained by the lack of technological solutions.

The FATF updated its guidance to support the implementation of the Standards in October 2021. Among other issues, the updated guidance further assists jurisdictions and businesses in implementing the 'travel rule'. It also covers definitional issues in greater detail, and focuses on peer-to-peer transactions, stablecoins and DeFi, which are among the fastest developing areas. Overall, the guidance calls for more coherent global implementation of the FATF Standards and harmonisation of international efforts (FATF, 2021[64]).

The Forum underlined the need for cross-jurisdictional coordination and dialogue between the private and public sectors to harmonise the international regulatory landscape covering risks of financial crime related virtual assets and blockchain-based applications. It also highlighted the example of the Blockchain Governance Initiative Network (BGIN), which was established in March 2020 in response to a G20 Leaders' call to advance the implementation of the FATF Standards (BGIN, 2020[65]). BGIN offers a platform for multistakeholder exchange and collaboration and, through these discussions, has identified key issues to support the implementation of the Standards, including establishing regulatory sandboxes to experiment with regulatory interventions, adopting a code-based approach that could automate regulatory and compliance processes by reflecting rules and requirements in smart contracts (see Box 8), and carrying out comprehensive risk analysis to ensure anticipatory regulation.

Box 9. Private sector insights on AML compliance

Coinfirm is a business advisory service supporting VASPs, financial institutions and other blockchain service providers in carrying out AML/CFT compliance and risk management through technical tools and guidance. The company deploys blockchain analytics, which use analytic tools to trace the flow of tainted assets through blockchain wallet addresses, allowing for real-time detection of AML/CFT risks. Confirm has enabled such analytics to be built into DeFi transactions by including automatic risk mitigation measures into smart contracts which assess the AML/CFT risk level of the parties involved in a transaction, and automatically reject the transaction if that risk is too high.

A number of challenges in AML/CFT risk management still remain, including reduced traceability in specific types of virtual asset transactions, and reliance on algorithms to identify VASP addresses. A recent assessment by Coinfirm concluded that VASPs' AML frameworks and KYC procedures have significant room for improvement: full scale KYC verifications were applied by 40% of VASPs, whereas 40% applied checks only with a high threshold and 20% did not apply any KYC checks. Fully 66% of the VASPs with insufficient or no KYC checks are registered in jurisdictions with no AML/CFT laws for virtual assets.

Source: Coinfirm (2020[66]), DeFi Compliance De-Risks with AMLT Oracle, https://www.coinfirm.com/blog/defi-compliance-amlt-oracle/

4 Supporting an international policy environment for blockchain innovation

This section explores some of the key regulatory issues related to blockchain. While some blockchain networks might appear at first glance beyond the reach of regulation, there are a range of options and approaches for governments to consider. Some regulatory challenges are unique to the technology, but many are common with other digital innovations, and existing approaches like 'agile regulation' provide valuable policy guidance. International co-operation is critical from both a rule of law perspective and to help drive innovation, and again some policy standards exist to support this. For blockchain-specific issues, standards, rules and practices are being developed, but there are still gaps internationally.

Regulation plays a fundamental role in guiding market activities towards fair and efficient outcomes that reflect the public interest and remedy market failures. The early innovations of blockchain technology that created global, open networks, notably the Bitcoin and Ethereum blockchains, were designed to offer an alternative to institutional oversight and to be resistant to policy interventions. The resulting perceived difficulty or inability to use policy tools to align blockchain-based activities and innovation with regulatory goals has been a major part in governments' assessments of the value of blockchain technology and the desirability of its use.

OECD members have consistently affirmed their collective view that innovation is not an end unto itself but a means to lift wellbeing, and that advances in science and technology require effective governance so that risks are managed and benefits distributed fairly. In 2021, the OECD Ministerial Council

emphasised the role of international standards in ensuring that emerging technologies develop in a way that reflects the shared values of OECD member countries (OECD, 2021[67]).

In this context, governments are seeking to ensure use of blockchain technology preserves rule of law and cultivates a level playing field, is consistent with the rules governments have established for the same activities in other settings or methods of delivery, and aligns appropriately with regulatory objectives, values and social expectations. Use of the technology must also be able to adapt as these elements evolve.

In addition, many of the sectoral applications of blockchain technology discussed in previous sections have positive benefits that hinge on some level of regulatory consistency between countries, and may benefit from government-led efforts to align standards, laws and approaches. Private sector participants in the Forum also underlined the value of regulatory certainty and consistency, including at the international level, in supporting innovation, providing incentives for good conduct, avoiding legal risk and ensuring market integrity.

4.1. Governing decentralised technologies

Market rules and regulations typically seek to address undesirable consequences of an activity by making individuals or entities liable and accountable for outcomes connected to that activity. The lack of a responsible legal person may make applying and enforcing rules on blockchain networks difficult, because of the decentralisation, disintermediation and anonymity features of the technology. Governance of the network might be set by pre-programmed protocols and may not be able to be changed, network activities can run autonomously, and the identity of actors may be difficult to discern.

The extent to which these challenges are present depends on the openness of networks. Private, enterprise blockchains will be run and used by parties whose identities are known and who likely exercise a level of control over the network. Conversely, public, permissionless blockchains open to anybody will – and do – present many of these issues. Regardless where a network or application sits on the spectrum between open and closed, all activities and actors must have the ability to show they are in compliance with any applicable laws and regulations.

Forum discussions outlined a number of current or potential practices to drive accountability for the activities happening on more decentralised networks, including by assigning responsibilities and accountability to:

- **Users** of blockchain platforms, for example, those who carry out transactions, by holding them responsible for any unlawful activities they engage in on blockchain networks and disincentivising involvement with them. Regulators may run into practical obstacles in identifying users, especially due to blockchain's anonymous nature, however the immutability and transparency of transactions may also aid in investigations.
- **Third party service providers** within a blockchain ecosystem. While blockchain can eliminate the need for some types of intermediaries, other types of third parties have emerged in the context of blockchain applications, particularly as the link between the on-chain and off-chain environments. For example, digital asset exchanges could be – and in some cases already are – required to ensure compliance with various rules and norms in their operations, including AML/CFT requirements and ethical conduct criteria (see sections 3.1 and 3.2).
- **Miners, mining pools and/or network nodes** could be subject to laws in the jurisdictions they operate to take certain actions on the network, such as blocking activities on networks by from identified criminal elements, although this may be incompatible with some permissionless consensus mechanisms, and may push mining operations into jurisdictions with weaker regulation. Rules around the physical business operations of miners may be easier to implement, for example requiring climate or ESG disclosures.

- **Developers** or enterprises behind public blockchains. Development teams will often "decentralise" a public blockchain network at a certain point, relinquishing control in the process. However, to the extent those developers could be identified, they could be held responsible for subsequent activities on the network. This is the basis for the US Securities and Exchanges Commission's probe into Uniswap Labs, developers of the Uniswap DeFi protocol (see section 2.3).
- **Information intermediaries**, such as search engines or platforms that provide gateways to decentralise applications, by preventing indexing of unlawful or high-risk blockchain services and therefore limiting the possibilities of accessing then.
- **The code itself**, which is at the core of blockchain's functioning. As highlighted by several discussants at the Forum, a code-based approach to regulation could help ensure regulatory compliance of a blockchain platform. Regulators could, for example, require integration of specific features into governance protocols and smart contracts. Integrating regulatory compliance into the fabric of a blockchain could also facilitate auditing, reporting and disclosures, and contribute to oversight of the network's activities.

Regardless of the type of blockchain, regulators, market supervisors and policymakers face other difficulties beyond who or where to assign responsibility for compliance purposes. Blockchain innovation has been fast-paced, particularly in financial applications, with products and business models in the market today which were purely theoretical only a few years ago. New applications have often outpaced the ability for relevant regulation to keep up.

This is partly because, while many regulators have built up strong capabilities in monitoring market developments and understanding and responding to digital technologies, technologies can still develop in a way that push against (or beyond) the boundaries of a regulator's mandates or the scope of current rules. Recent discussions on how far the mandate of the US Securities and Exchanges Commission could extend to regulate DeFi platforms is one such example (Bloomberg Law, 2021[68]).

Regulators must also strike a balance in their responses; blockchain is still evolving, and as a general purpose technology its future applications may not yet be apparent. Overly prescriptive rules too early in the technology's lifecycle may stymy positive innovation and created unintended negative consequences, but at the same time, there are clear risks that must be managed. In seeking to strike this balance, some countries have taken steps to communicate where they see value in the technology and how they see blockchain fitting into their innovation environments (see Box 10).

Blockchain's impact and use is also cross-sectoral. The use-cases seen in the market thus far, either as full-fledged solutions or pilots, have highlighted the interconnectedness of different policy and legal disciplines, such as competition, illicit finance, corporate governance, privacy, and customs rules among many others, and so governments may struggle to identify the responsible agency or coordinate across institutions in the traditional market-specific model of regulation.

Finally, blockchain networks are often transnational in nature, particularly open, public networks. The Ethereum network, for example, has nodes hosted in over 50 countries (Ethernodes.org, 2022[69]), running decentralised applications available to almost anyone in the world. This decentralisation can create jurisdictional issues in the application of rules and ability to enforce them, as the ease of mobility for nodes moving between jurisdictions translate to a high risk of regulatory arbitrage and potential for "forum shopping" to find the most favourable jurisdiction in the case of legal issues, and also builds in a high level of resiliency against the cessation or banning of services or activities that governments might legitimately seek to curb.

Box 10. National strategies for emerging technologies

Several governments have used policy strategy documents to articulate their aims and approaches towards emerging technologies. Some have developed dedicated national blockchain strategies, others have included blockchain in a suite of strategically important technologies, while other have broad digital strategies designed to apply to all new technologies.

Australia established its National Blockchain Roadmap in 2020, focussing government actions to develop the technology in the context of wider science, innovation and skills policy. It highlights three specific sectoral applications of interest: wine exports; education credentials; and KYC checks in finance. It includes mechanisms for co-operation and co-operative funding between the government, business and researchers, and also stresses the importance of reflecting blockchain in international activities such as trade agreements (Department of Industry, Science, Energy and Resources, 2020[70]).

The European Commission launched its blockchain strategy in 2021 with the stated aim of becoming "a leader in blockchain technology, becoming an innovator in blockchain and a home to significant platforms, applications and companies". Key elements include the ambition to establish an EU level governance framework for blockchain, the funding of research, skills, and innovation, supporting interoperability standards, and developing a pan-European public services blockchain (European Commission, 2021[11]).

The United States maintains a list of critical and emerging technologies that are relevant to technological competitiveness and national security objectives. The White House added Distributed Ledger Technologies and digital assets to this list in February 2022, indicating that these technologies should be closely considered in the development and delivery of the country's foreign policy priorities (The White House, 2022[71]).

The United Kingdom outlined its approach in the governance of digital innovation in the *Digital Regulation: Driving growth and unlocking innovation* policy paper in 2021. While it does not cover blockchain specifically, it outlines a regulatory strategy for digitalisation based on: creating optimal conditions for businesses to operate; anticipatory and collaborative regulation reflecting fast-paced changes; and policy action that takes into account the global nature of many new digital tools, including strengthening international regulatory co-operation (Department for Digital, Media, Culture and Sport, 2021[72]).

4.1.1. Existing approaches in a fast-changing and interconnected environment

While blockchain may present some novel challenges for regulators, many of the challenges described above – the rapid pace of change, the cross-sectoral and cross-border nature of innovation – are common features across emerging technologies and digital innovation more broadly. The Forum highlighted a number of existing, technology-neutral instruments and initiatives that could support forward-looking and agile policy responses to the issues posed by blockchain.

As part of its wider work on the impact of emerging technologies on economic regulators, the OECD has identified key considerations for designing regulatory interventions for digital innovation. This research has emphasised the need for institutional preparedness of regulators, ensuring that mandates and powers are aligned with data-driven businesses, that legal and regulatory frameworks are fit for purpose, and that regulators are adequately organised and resourced, including with the appropriate set of capabilities and skills, and the ability to coordinate efforts with other agencies (OECD, 2020[73]).

Box 11. The Agile Nations Charter

The Agile Nations Charter is the guiding framework for an intergovernmental network established in 2020 by Canada, Denmark, Italy, Japan, Singapore, the United Arab Emirates and the United Kingdom. The charter represents a commitment by each country to create a regulatory environment in which new ideas can thrive. The Charter calls on countries to put in place good practices in rulemaking that reflect the importance of close and continuous stakeholder engagement, horizon scanning, proactive and proportional regulatory responses, and the use of a wide range of regulatory tools to create a flexible, responsive policy environment that gives space for innovation while managing relevant risks.

The agreement paves the way for these nations to co-operate in helping innovators navigate each country's rules, test new ideas with regulators and scale them across the seven markets. Priority areas for co-operation included the green economy, mobility, data, financial and professional services, and medical diagnosis and treatment. Participation in the Agile Nations is open to national governments that are prepared to adopt the practices laid out in the Charter.

Source: OECD (2020[74]), "Agile Nations": Nations Sign First Agreement to Unlock Potential of Emerging Tech, https://www.oecd.org/gov/regulatory-policy/agile-governance-for-the-post-pandemic-world-wef-oecd-joint-event.htm

The OECD's Recommendation on Agile Regulatory Governance to Harness Innovation was adopted in 2021 to guide governments in the development of agile, technologically neutral and adaptive regulation (OECD, 2021[75]). The recommendation and its accompanying implementation guidance emphasise the need to treat regulation as a flexible, iterative and forward-looking activity, using key regulatory policy tools such as stakeholder engagement and impact assessments as part of a continuous policy cycle that is regularly monitored and reviewed. It highlights the need for closer and more frequent stakeholder engagement, in order to better monitor developments, respond to expectations, support compliance and promote inclusion. It also underscores the value of new data sources and regulatory technologies which, as discussed in previous section, is something which blockchain networks could readily provide.

The guidance also details approaches for regulators to give regulatory space for innovation while meeting policy goals. It suggests outcome-focused approaches, which are less prescriptive and so allow for innovation to follow unanticipated but potentially beneficial paths, and also support consistency between jurisdictions, where policy goals may be similar but the means of realising those goals differ. Other important tools include the consideration of non-binding approaches, such as codes of conduct and voluntary standards, and providing experimental regulatory environments like regulatory sandboxes and targeted, risk-appropriate exemptions (OECD, 2021[76])

For blockchain, proportional regulatory approaches could help identify and manage specific risks related to particular use cases, and flexible and principles-based regulatory frameworks could encourage further technological development and help overcome the tension between fast-paced innovation and comparatively slower regulatory responses. Introducing regulations should be timed appropriately to avoid premature interventions that could hamper innovation, but also delayed interventions that might increase regulatory uncertainty and legal risk for innovators as products or business practices mature.

4.2. Towards an international regulatory environment

An important element of the *OECD Recommendation on Agile Regulatory Governance to Harness Innovation* and its implementation guidance is the consideration of the international innovation ecosystem, which was a major focus of Forum discussions. It is a critical element to rulemaking in terms of collecting

knowledge and best practices, designing policy in reference to international developments, pursuing regulatory co-operation and international coherence to address the cross-border challenges blockchain innovation presents, and avoiding the many risks relating to policy fragmentation.

Again, policymakers crafting policy responses to blockchain innovation can start with existing, general-purpose policy tools to help achieve these goals. The OECD's *Best Practice Principles on International Regulatory Co-operation*, for example, guides policymakers in designing integrated approaches and whole-of-government strategies to ensure regulatory interventions are interoperable between jurisdictions and take cross-border realities into account (OECD, 2021[77]). It details three complementary avenues to pursue international regulatory co-operation:

- **Unilaterally**, including the adoption of international instruments and good regulatory practices, consultation with foreign stakeholders, seeking out international information and intelligence, and assessing impacts beyond borders;
- **Bilaterally or plurilaterally**, through mutual recognition or equivalence with rules from other countries, co-operation partnerships, memoranda of understanding, and the incorporation of regulatory provisions into trade agreements; and
- **Multilaterally**, including participation in international fora and the negotiation of specific international agreements.

In line with these practices, governments should be placing any international engagement on blockchain regulation within a wider framework of international regulatory co-operation across these avenues.

4.2.1. An emerging body of international blockchain rules, standards and practices

The *Best Practice Principles* emphasise the importance of global standards and active participation in global fora to drive cohesion and consistency of rules, and the past few years have seen a body of blockchain-specific rules and standards developed in international settings, ranging from technical standards to specific legal rules and technology-wide or sector-specific principles.

Among these, rules and standards for the financial sector are most developed, which is to be expected as this is both a highly regulated industry and the sector where blockchain applications are most advanced. The FATF's *Updated Guidance for Virtual Asset Service Providers* on AML/CFT responsibilities has been among the most consequential rule for many businesses operating in this sector, and was discussed in detail in section 3.2 of this report. The OECD is also developing a new tax transparency framework for crypto-assets, recognising the risks posed to global tax transparency goals by some crypto-asset market practices, which was opened to public consultation in March 2022 (OECD, 2022[78]).

Many jurisdictions have crafted legislation to govern specific elements of crypto-asset markets, and among these the European Union's draft *Regulation on Markets in Crypto Assets*, currently under consideration by the European Parliament, is the most wide-reaching, with a regulatory package which applies rules and requirements for crypto-assets product and service providers in line with wider principles of market integrity and establishes a common regulatory regime across EU member states (European Commission, 2020[79]). Voluntary industry standards have also proliferated in this space, for example the suite of principles covering key activities and actors in the crypto-asset sector that make up the Code of Conduct developed by industry body Global Digital Finance (GDF, 2019[80])

International co-operation in the financial sphere has been anticipatory as well, seeking to manage specific risks foreseen as the technology develops. The Financial Stability Board's *High-Level Recommendations on the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements* is an instrument to support multilateral management of systemic risks to the financial system which might eventually arise from the global class of stablecoin crypto-assets (FSB, 2020[81]). Exploration and consideration of central bank digital currencies (CBDCs) is also progressing among major central banks, which may be blockchain-

based or incorporate features of decentralisation, and the G7 *Public Policy Principles for Retail Central Bank Digital Currencies*, developed under the UK presidency in 2021, sets out key considerations for CBDC design and operation consistent with the values of transparency, the rule of law, and sound economic governance (G7, 2021[82]).

A number of international and multilateral efforts have sought to address common issues at the technology level. The importance of technical standards were highlighted across Forum discussions, particularly relating to interoperability between sectors and jurisdictions, and the International Organization for Standardization (ISO) has been developing and publishing technical standards for blockchain through a dedicated technical committee since 2015. To date the committee has published seven standards including on taxonomies, treatment of data, security and governance, with standards relating to digital identity management, smart contracts and interoperability of systems currently under development (ISO, 2022[83]). Such standards can help realise a number of international regulatory priorities for blockchain technology, for example by establishing a common vocabulary for concepts, or enshrining industry best practices to manage privacy risks, and governments should consider referencing these in their own activities. Multilateral efforts have been complemented by bilateral co-operation, such as the Australia-Singapore project on digital trade facilitation (Section 2.1 in this report) and the Canada-European Commission project on digital credentials (Section 2.2).

Public institutions are also creating common blockchain infrastructures or networks to drive technical interoperability between applications, sectors, and national jurisdictions. These have been delivered at a national or regional level thus far, and include the European Commission's *European Blockchain Services Infrastructure* for EU member and partner countries, and the Inter-American Development Bank's *LACChain* for Latin American and Caribbean nations, both developed in partnership with the private sector and academia.

The sector-specific international co-operation, regional initiatives and progress on technical standards are a promising start to a body of blockchain rules, standards and practices to guide and support innovation towards positive outcomes. However, as a general-purpose and cross-border technology, different sectors and different countries face similar challenges in the governance and guidance of blockchain, and there is not yet any multilateral instrument to guide common policy approaches at the whole-of-economy level. Such standards exist for other emerging technologies, particularly for artificial intelligence, where the *OECD Principles* on *Artificial Intelligence* provide recommendations for public policy and strategy to deliver a more stable policy environment at the international level, to foster trust in the technology, and guide responsible innovation and adoption (OECD, 2019[84]).

Recognising this gap, the OECD has drawn on its body of analytical work on blockchain and its close stakeholder engagement, including committee-level discussions, successive editions of the OECD Global Blockchain Policy Forum, and a dedicated cross-sectoral experts group, to develop a set of high-level policy principles for blockchain and distributed ledger technologies. This instrument, currently under consideration by OECD members, would provide a foundational contribution to the international policy environment around blockchain as a common reference point for policy development, available to OECD members and non-members alike. The principles set out high-level objectives that governments should seek to achieve in their policy responses, the priorities for international co-operation in this area, and the expectations of governments for all actors within a blockchain ecosystem. Once agreed, they will represent an important step towards greater coherence and consistency in cross-sectoral government approaches to blockchain which has thus far been absent at the international level.

5 Conclusions and recommendations

Blockchain is an emerging technology that will likely continue to evolve, and its use enabling international economic activity is relatively nascent. As governments and companies alike pursue opportunities in this space, they should proceed with a clear view of the technology's limitations, and take steps to ensure blockchain innovation is consistent with national laws and international norms. Several governments and international standard setting bodies recognise the benefits of policy consistency and coherence between countries to guide the technology's development, and have pursued bilateral co-operation and multilateral coordination initiatives to support this, though gaps in both the coverage of international approaches and their implementation remain.

This report, and the discussions of the 2021 OECD Global Blockchain Policy Forum on which it is based, have demonstrated some of the ways the use of blockchain may help or hinder countries' international priorities and the goals of the international community. While these have been grounded in immediate and practical uses of the technology, they also hint at the potential for blockchain technology to reshape economic and social relations, and to serve as a tool to organise and govern the collective activities of individuals, companies and governments. The applications in this report have illustrated how blockchain could be a driving force of connectivity between countries, within regions and across the world.

It is important to recognise this is an emerging technology which is at an early stage of adoption and will continue to evolve, and while we have already seen that blockchain can be disruptive and transformative in settings like finance, its exact impact is difficult to predict. However, the preceding discussion has signalled a number of prescient considerations for governments in both realising the benefits of this technology, and managing the risks.

Blockchain is already supporting cross-border economic activities, particularly in situations where there are complex connections between a myriad of actors, for example in shipping and customs

procedures, in supply chain due diligence, and the management of personal information and credentials. The technology has begun to deliver efficiency gains and new levels of transparency by using decentralised digital governance structures to disintermediate and automate activities in a range of settings across the real and digital economy. Many applications and uses brought to market are not operating at large scale – but investment and interest are high, and it is reasonable to expect wider adoption in the coming years.

Blockchain is not a replacement for real-world governance. Data on the blockchain may be immutable and easily auditable, but confidence in that data is only as high as confidence in the processes that placed that data on the blockchain to begin with. In some cases network designs run counter to some basic assumptions about the functioning of markets and the rights of consumers, and so must be complemented by law. In most situations the technology also benefits from (or requires) trusted parties existing *somewhere* in the ecosystem. The roles and responsibilities of these parties should be well understood by all stakeholders in a blockchain network to ensure transparency of network governance arrangements.

Interoperability and digital security are key concerns for governments. While blockchain might drive efficiency by streamlining the verification and sharing of data, the use of the technology is not in itself sufficient to realise these gains. Interoperability of blockchains and their data was a concern in most uses touched on in this report, and current uses of blockchain have already demonstrated a high propensity for fragmentation within and between sectors. This reduces the positive transformative potential of the technology, may restrict beneficial data exchanges between jurisdictions, and also risks lock-in of users to one particular provider. Governments have a role to play in convening actors and setting frameworks, like common data standards and taxonomies, to encourage interoperability. Governments also have a responsibility in ensuring the technology respects the rights and meets the expectations of its users in terms of personal privacy, data protection and cyber security, particularly where blockchain is enabling the cross-border movement of personal data.

Some governments are clearly articulating their visions and goals for blockchain innovation. A number of countries have launched dedicated blockchain strategies or featured the technology in wider digital innovation strategies. Others are developing blockchain infrastructure on which to build public services like digital credentials. But the use of blockchain in public innovation should have a robust rationale, and governments should choose the most appropriate and suitable technology to meet requirements of a given situation. At a minimum, blockchain innovation is an opportunity to assess whether current rules and regulations focus on achieving outcomes, rather than focussing on processes, and so allow for and enable digital innovation.

Blockchain presents policy challenges, but it cannot sit beyond rules and norms. The scope of those challenges often depends on the type of network, but decentralisation and anonymity, particularly in open, public blockchain networks, can make the application of existing rules and regulations difficult. At the same time, any blockchain product encompasses an ecosystem of actors, many of them identifiable businesses or individuals, and governments should expect mechanisms to be put in place to ensure compliance with relevant policy, legal, and regulatory requirements. The potential for the technology to act counter to policy goals, including international aims such as climate adaptation or countering illicit financial flows, must also be managed by public institutions and market participants.

Blockchain policy responses require a high degree of coordination at a national and international level. As with many digital innovations, the technology cuts across the traditional policy portfolios of national ministries and the sectoral divides by which regulation is often developed and enforced. Blockchain is also a global technology, with networks often operating in multiple jurisdictions and offering products and services unrestricted by national boundaries. International co-operation towards common approaches is necessary to avoid policy fragmentation and opportunities for regulatory arbitrage, and to address negative cross-border spillovers.

Existing instruments and practices can already inform policy approaches. Blockchain may be a new and transformative technology, but many governments are by now well-versed in adapting to digital

transformation. Tools like the OECD *Going Digital Integrated Policy Framework,* and standards and practices around agile regulation and international regulatory co-operation, have already been developed to address many of the general issues blockchain presents. Other international standards, from privacy to responsible business conduct, are valuable reference points for any digital technology.

However gaps exist, particularly at the international level. Blockchain-specific standards and practices are being developed, with technical standards and guidance in the financial market setting most advanced. But as the FATF Virtual Asset Standard has shown, the simple existence of rules and standards is not enough, and these must be reflected in national policy and implemented effectively. The international environment would also benefit from an overarching framework for the technology that aligns countries' approaches under a set of common principles.

Stakeholder engagement will continue to be important. Dialogue and discussions between policymakers, market participants and stakeholders – such as those hosted at the OECD Global Blockchain Policy Forum – are necessary in this fast-moving field. Close and continuous engagement will help public authorities stay abreast of new developments, build skills, knowledge and capacity, identify emerging challenges and opportunities across jurisdictions, and craft effective policy responses.

References

Bains, P. (2022), *Blockchain Consensus Mechanisms: A Primer for Supervisors*, International Monetary Fund, https://www.imf.org/en/Publications/fintech-notes/Issues/2022/01/25/Blockchain-Consensus-Mechanisms-511769. [60]

BGIN (2020), *About BGIN*, https://bgin-global.org/about/ (accessed on 18 October 2021). [65]

Bits on Blocks (2017), *A gentle introduction to self-sovereign identity*, https://bitsonblocks.net/2017/05/17/gentle-introduction-self-sovereign-identity/. [36]

Blandin, A. et al. (2020), *3rd Global Cryptoasset Benchmarking Study*, Cambridge Centre for Alternative Finance. [59]

Bloomberg Law (2021), *Gensler Shares SEC's Crypto Power Play*, https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-gensler-shares-secs-crypto-power-play. [68]

BMWK (2020), *Showcase programme "Secure Digital Identities"*, https://www.digitale-technologien.de/DT/Navigation/EN/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html (accessed on 11 March 2022). [38]

Bratanic, J. (2022), *Kosovo's Bitcoin Miners Selling Equipment After Government Ban*, Bloomberg, https://www.bloomberg.com/news/articles/2022-01-17/kosovo-s-bitcoin-miners-selling-equipment-after-government-ban (accessed on 25 February 2022). [61]

Bresnahan, T. and M. Trajtenberg (1995), "General purpose technologies 'Engines of growth'?", *Journal of Econometrics*, Vol. 65/1, https://doi.org/10.1016/0304-4076(94)01598-T. [2]

Coinfirm (2020), *DeFi Compliance De-Risks with AMLT Oracle*, https://www.coinfirm.com/blog/defi-compliance-amlt-oracle/ (accessed on 18 October 2021). [66]

Cointelegraph (2021), *Uniswap's weekly trade volumes reach record high of $10B*, https://cointelegraph.com/news/uniswap-s-weekly-trade-volumes-reach-record-high-of-10b. [8]

Consensys (2021), *Why Decentralized Autonomous Organizations (DAOs) Are Essential to DeFi*, https://consensys.net/blog/codefi/daos/ (accessed on 18 October 2021). [49]

CryptoSec (2022), *Documented Timeline of DeFi Exploits*, https://cryptosec.info/defi-hacks/ (accessed on 22 March 2022). [53]

De Filippi, P. (2021), *Blockchain Technology as an Instrument for Global Governance*, https://www.sciencespo.fr/public/chaire-numerique/en/2020/09/11/primavera-de-filippi-blockchain-technology-as-an-instrument-for-global-governance/. [13]

de Jong, J., A. Meyer and J. Owens (2017), *Using blockchain for transparent beneficial ownership registers*, https://www.internationaltaxreview.com/article/b1f7n782qqw73h/using-blockchain-for-transparent-beneficial-ownership-registers (accessed on 2018 October 2021). [45]

De La Cruz, A., A. Medina and Y. Tang (2019), *Owners of the World's Listed Companies*, OECD, https://www.oecd.org/corporate/Owners-of-the-Worlds-Listed-Companies.htm. [44]

DeepDAO (2022), *Organizations data set*, https://deepdao.io/organizations (accessed on 18 February 2022). [50]

Department for Digital, Media, Culture and Sport (2021), *Digital Regulation: Driving growth and unlocking innovation*, UK Government, https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation/digital-regulation-driving-growth-and-unlocking-innovation. [72]

Department of Industry, Science, Energy and Resources (2020), *National Blockchain Roadmap*, Australian Government, https://www.industry.gov.au/data-and-publications/national-blockchain-roadmap. [70]

Elliott, D. (2022), *Cryptoassets: Tulips or Dot-coms?*, https://www.oliverwymanforum.com/future-of-money/2022/jan/are-cryptoassets-tulips-or-dot-coms.html. [14]

Enterprise Estonia (2017), *e-Estonia - Building a digital society*, https://e-estonia.com/solutions/ (accessed on 11 March 2022). [10]

Ethereum.org (2022), *Ethereum energy consumption*, https://ethereum.org/en/energy-consumption/ (accessed on 25 April 2022). [58]

Ethernodes.org (2022), *Ethereum Mainnet Statistics*, https://www.ethernodes.org/countries (accessed on 28 February 2022). [69]

European Commission (2021), *Shaping European Digitial Future: Blockchain Strategy*, https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy (accessed on 8 March 2022). [11]

European Commission (2020), *Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593. [79]

European Commission (2019), *European Self Sovereign Identity Framework Laboratory*, https://cordis.europa.eu/project/id/871932 (accessed on 10 March 2022). [37]

Europol (2016), *Missing Trader Intra Community Fraud*, https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/mtic-missing-trader-intra-community-fraud (accessed on 18 October 2021). [24]

Everledger (2021), *Industry solutions*, https://everledger.io/industry-solutions/ (accessed on 3 March 2022). [5]

FATF (2021), *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html. [64]

FSB (2020), *Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements - Final Report and High-Level Recommendations*, https://www.fsb.org/wp-content/uploads/P131020- [81]

3.pdf.

G20 (2021), *Declaration of G20 Digital Ministers: Leveraging Digitalisation for a Resilient, Strong, Sustainable and Inclusive Recovery*, G20 Italian Presidency, https://innovazione.gov.it/notizie/articoli/en/the-declaration-of-g20-digital-ministers/. [39]

G20 (2018), *Communiqué of the Meeting of Finance ministers and Central Bank Governors*, http://www.g20.utoronto.ca/2018/2018-03-30-g20_finance_communique-en.html. [62]

G7 (2021), *Ministerial Declaration of the G7 Digital and Technology Ministers' meeting*, https://www.gov.uk/government/publications/g7-digital-and-technology-ministerial-declaration. [19]

G7 (2021), *Public Policy Principles for Retail Central Bank Digital Currencies*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1025235/G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf. [82]

Ganne, E. (2018), *Can Blockchain revolutionize international trade?*, WTO Publications. [30]

Ganne, E. and D. Patel (2020), *Blockchain and DLT in Trade: Where do we Stand?*, TFG Publishing. [26]

GDF (2019), *GDF Code*, https://www.gdf.io/code/ (accessed on 7 March 2022). [80]

Gemini (2021), *Cryptopedia: What Is MakerDAO?*, https://www.gemini.com/cryptopedia/makerdao-dai-decentralized-autonomous-organization (accessed on 22 March 2022). [9]

Government of Canada (2021), *Canada and the European Union Joint Workshop Series for Enabling Interoperability and Mutual Support for Digital Credentials*, https://www.ic.gc.ca/eic/site/153.nsf/eng/h_00006.html (accessed on 4 December 2021). [40]

Hassan, S. and P. De Filippi (2017), "The Expansion of Algorithmic Governance: From Code is Law to Law is Code", *Field Actions Science Reports* Special Issue 17, pp. 88-90, http://journals.openedition.org/factsreports/. [54]

House of Lords (2022), *Central bank digital currencies: a solution in search of a problem?*, House of Lords, https://publications.parliament.uk/pa/ld5802/ldselect/ldeconaf/131/13102.htm. [20]

Huang, J., C. O'Neill and H. Tabuchi (2021), *Bitcoin Uses More Electricity Than Many Countries. How Is That Possible?*, https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html. [57]

Hynes, W. Lees and J. Müller (eds.) (2020), *Systemic Thinking for Policy Making: The Potential of Systems Analysis for Addressing Global Policy Challenges in the 21st Century*, OECD Publishing, https://doi.org/10.1787/879c4f7a-en. [18]

IBM (2021), *Smart contracts defined*, https://www.ibm.com/topics/smart-contracts (accessed on 8 March 2022). [46]

ID2020 (2022), *The Need for Good Digital ID is Universal*, https://id2020.org/digital-identity. [6]

IDC (2021), *Global Spending on Blockchain Solutions Forecast to be Nearly $19 Billion in 2024 According to New IDC Spending Guide*, https://www.idc.com/getdoc.jsp?containerId=prUS47617821 (accessed on 12 December 2021). [3]

Ipsos (2019), *CIGI-Ipsos Global Survey on Internet Security and Trust*, https://www.cigionline.org/cigi-ipsos-global-survey-internet-security-and-trust/ (accessed on 9 February 2022). [34]

ISO (2022), *ISO/TC 307 Blockchain and distributed ledger technologies*, https://www.iso.org/committee/6266604.html (accessed on 7 March 2022). [83]

Keyes, G. (2021), *DeFi Tops $100 Billion for First Time as Cryptocurrencies Surge*, https://www.bloomberg.com/news/articles/2021-10-20/defi-tops-100-billion-for-first-time-as-cryptocurrencies-surge (accessed on 14 February 2022). [85]

Kitsios, E., G. Verdier and J. Jalles (2020), "Tax Evasion from Cross-Border Fraud: Does Digitalization Make a Difference?", *IMF Working Paper* No.20/245. [25]

Lewis, J. and R. Zeglarski (2021), *Wyoming Paves Way for DAO Legal Company Status*, https://frostbrowntodd.com/wyoming-paves-way-for-dao-legal-company-status/ (accessed on 2018 October 2021). [51]

Lindman, J. et al. (2020), *The uncertain promise of blockchain for government*, OECD Publishing, https://doi.org/10.1787/d031cd67-en. [16]

López González, J. and S. Sorescu (2019), *Helping SMEs internationalise through trade facilitation*, OECD Publishing, https://doi.org/10.1787/2050e6b0-en. [21]

Michaels, D. and A. Osipovich (2021), *Regulators Investigate Crypto-Exchange Developer Uniswap Labs*, The Wall Street Journal, https://www.wsj.com/articles/regulators-investigate-crypto-exchange-developer-uniswap-labs-11630666800?mod=latest_headlines. [52]

Moïsé, E. and S. Sorescu (2019), "Exploring the role of trade facilitation in supporting integrity in trade", *OECD Trade Policy Papers*, OECD Publishing, https://doi.org/10.1787/cfbcef14-en. [23]

Nassr, I. (2022), *From "DeFi summer" to "crypto winter": leverage, liquidations and policy implications*, https://oecdonthelevel.com/2022/01/31/from-defi-summer-to-crypto-winter-leverage-liquidations-and-policy-implications/ (accessed on 27 April 2022). [47]

Nemeto, T. and J. López González (2021), "Digital trade inventory: Rules, standards and principles", *OECD Trade Policy Papers* 251, https://doi.org/10.1787/9a9821e0-en. [31]

Norbloc (2021), *UAE Dubai Economy and DIFC unify their Blockchain enabled KYC Consortiums*, https://norbloc.com/uae-dubai-economy-and-difc-unify-their-blockchain-enabled-kyc-consortiums/ (accessed on 2022). [42]

OECD (2022), *Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard - Public Consultation Document*, OECD, https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf. [78]

OECD (2022), *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, OECD Publishing, https://www.oecd.org/finance/why-decentralised-finance-defi-matters-and-the-policy-implications.htm. [48]

OECD (2021), *2021 Ministerial Council Statement*, https://www.oecd.org/mcm/MCM-2021-Part-2-Final-Statement.EN.pdf. [67]

OECD (2021), *ESG Investing and Climate Transition: Market Practices, Issues and Policy* [55]

Considerations, OECD Publishing, https://www.oecd.org/finance/ESG-investing-and-climate-transition-market-practices-issues-and-policy-considerations.pdf.

OECD (2021), *G20 Collection of Digital Identity Practices: Report for the G20 Digital Economy Task Force*, https://assets.innovazione.gov.it/1628073752-g20detfoecddigitalid.pdf. [35]

OECD (2021), *International Regulatory Co-operation, OECD Best Practice Principles for Regulatory Policy*, OECD Publishing, Paris, https://doi.org/10.1787/5b28b589-en. [77]

OECD (2021), *Practical Guidance on Agile Regulatory Governance to Harness Innovation*, OECD, https://one.oecd.org/document/C/MIN(2021)23/ADD1/en/pdf. [76]

OECD (2021), *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464. [75]

OECD (2020), *"Agile Nations": Nations Sign First Agreement to Unlock Potential of Emerging Tech*, https://www.oecd.org/gov/regulatory-policy/agile-governance-for-the-post-pandemic-world-wef-oecd-joint-event.htm (accessed on 8 March 2022). [74]

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, https://doi.org/10.1787/bb167041-en. [33]

OECD (2020), *Shaping the Future of Regulators: The Impact of Emerging Technologies on Economic Regulators*, OECD Publishing, Paris, https://doi.org/10.1787/db481aa3-en. [73]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://doi.org/10.1787/9789264312012-en. [17]

OECD (2019), *Is there a role for blockchains in sustainable supply chains?*, OECD, http://mneguidelines.oecd.org/is-there-a-role-for-blockchain-in-responsible-supply-chains.htm. [63]

OECD (2019), *Recommendation of the Council on Artificial Intelligence*, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [84]

OECD (2019), *The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studies*, OECD Publishing, https://doi.org/10.1787/059814a7-en. [43]

OECD (2018), *OECD Blockchain Primer*, https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf (accessed on 14 October 2021). [1]

OECD (2014), *OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials*, OECD Publishing, https://doi.org/10.1787/9789264226616-en. [22]

OECD (2011), *Digital Identity Management: Enabling Innovation and Trust in the Internet Economy*, OECD Publishing, Paris, https://doi.org/10.1787/5kg1zqsm3pns-en. [32]

Pentland, S. (2021), *Digital Currency and Trade Systems Are Tearing up the Rules*, https://spectrum.ieee.org/digital-currency (accessed on 14 December 2021). [12]

The Commonwealth (2016), *Disconnecting from Global Finance: The Impact of AML/CFT Regulations in Commonwealth Developing Countries*, Commonwelath Secretariat. [41]

The White House (2022), *Technologies for American Innovation and National Security*, https://www.whitehouse.gov/ostp/news-updates/2022/02/07/technologies-for-american-innovation-and-national-security/ (accessed on 8 March 2022). [71]

TradeLens (2022), *Digitizing the global supply chain*, https://www.tradelens.com/about (accessed on 2022 March 3). [4]

UK Government (2021), *UK welcomes work to develop global sustainability reporting standards alongside 40 international partners*, https://ukcop26.org/uk-welcomes-work-to-develop-global-sustainability-reporting-standards-alongside-40-international-partners/. [56]

UK Government (2020), *2025 UK Border Strategy*, https://www.gov.uk/government/publications/2025-uk-border-strategy. [29]

Walport, M. (2016), *Distributed Ledger Technology: beyond block chain*, UK Government. [15]

We.trade (2019), *Company Overview*, https://we-trade.com/company/company-overview (accessed on 3 March 2022). [28]

World Economic Forum (2018), *The Known Traveller: Unlocking the potential of Digital Identity for Secure and Seamless Travel*, https://www.weforum.org/reports/the-known-traveller-unlocking-the-potential-of-digital-identity-for-secure-and-seamless-travel. [7]

Yaku, F. (2021), *Blockchain greases trade wheels between 7 Asian-Pacific economies*, https://asia.nikkei.com/Economy/Trade/Blockchain-greases-trade-wheels-between-7-Asian-Pacific-economies. [27]