FRESH IDEAS ABOUT BUSINESS IN EMERGING MARKETS
EMCompass

www.ifc.org/thoughtleadership

NOTE 63 • JAN 2019

Blockchain and Associated Legal Issues for Emerging Markets

By John Salmon and Gordon Myers

Blockchain, or distributed ledger technology (DLT), is a tamper-evident and tamper-resistant digital ledger implemented in a distributed fashion.[1] This emerging technology, which enables direct transactions within a ledger without need for a central authority or trusted intermediary, has the potential to re-engineer economic models and enable the creation of markets and products previously unavailable or unprofitable across emerging markets. However, in considering the potential benefits of blockchain, organizations must also consider the associated risks and how they can be managed.

These risks include jurisdictional challenges, crypto assets, privacy and data protection, double spending, and distributed denial-of-service (DDoS) attacks. Several risks have been identified and overcome at similar innovative leaps in the recent past, including the commercialization of the Internet and cloud computing. It is essential that enterprises understand all risks inherent in blockchain systems, including being able to clearly identify who is accountable and legally responsible.

Blockchain's key characteristics present challenges to the existing legal and regulatory framework. It is comprised of digitally recorded data in "blocks" that are linked together in chronological order in a manner that makes the data difficult to alter once recorded, without the alteration of all subsequent blocks and collusion of a majority of the network.

Each node on the network generally contains a complete copy of the entire ledger, from the first block created—the genesis block—to the most recent one. Each block contains a hash (a fixed length alphanumeric string generated from a string of text) pointer as a link to a previous block, a timestamp, and transaction data. By its nature, distributed ledger technology allows for transactions and data to be recorded and shared across a distributed network of participants without the need for a trusted intermediary. The original instance of blockchain (bitcoin) was to enable peer-to-peer transactions without the requirement for, or cost of, a central party.

Organizations wishing to develop a decentralized application on a blockchain therefore face a new set of risks and issues to manage. Most of these stem from the fact that we live in a world where centralized governance and control is the norm. Accordingly, the vast majority of countries' laws and regulations envision centralized businesses or structures with a singular seat of control and responsibility. Deviating from this arrangement poses a challenge from a legal and regulatory perspective and raises enforcement issues.

This is particularly the case when it comes to regulated sectors such as financial services. In this sector there has traditionally been some form of central counterparty, which often is regulated. Within a particular system or process, that central party is accountable and takes responsibility for the provision of the services to all of the other participants through a contractual framework underpinned by the legal and regulatory structure. An example of this would be the role of a central bank or other institution in clearing and settlement processes.

About the Authors

John Salmon, Partner, Hogan Lovells International LLP, London, UK, and Gordon Myers, Chief Counsel, Legal Department, Technology and Private Equity, IFC, and Co-Chair, Legal and Policy Community, ITS Innovation Lab, World Bank Group. Their emails are john.salmon@hoganlovells.com and gmyers@ifc.org respectively.

IFC International Finance Corporation WORLD BANK GROUP
Creating Markets, Creating Opportunities

			Read	Write	Commit	Example
BLOCKCHAIN TYPES	Open	*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorized participants	All or a subset of authorized participants	Sovrin
	Closed	*Consortium*	Restricted to an authorized set of participants	Authorized participants	All or a subset of authorized participants	Multiple banks operating a shared ledger
		Private permissioned ("enterprise")	Fully private or restricted to a limited set of authorized nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

*Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model)

FIGURE 1 Main types of blockchains segmented by permission model

Source: Hileman, Garrick and Michel Rauchs. 2017. "Global Blockchain Benchmarking Study." Cambridge Centre for Alternative Finance.

However, in many blockchain use cases there is no such centralized party that takes responsibility for the provision of services or controls associated data sets. Instead, each party in the blockchain network holds a copy of the data, rather than relying on a single central party to hold and maintain a master copy. For example, blockchain technology is being used to simplify cross-border payments, removing the need for transfers to pass through multiple parties (with associated charges) before reaching their destination.[2] While such decentralization can bring benefits, it also poses a legal and regulatory challenge if there is no central party that is responsible and can be held accountable.

The key issues that present risks to firms using blockchain, which are explained further below, are: blockchain systems spanning multiple jurisdictions; crypto assets; data protection; privacy compliance; and cyber attacks.

Jurisdictional problems

As the nodes of a decentralized ledger can span multiple locations around the world, it is often difficult to establish which jurisdictions' laws and regulations apply to a given application. There is a risk that transactions performed by an organization could fall under every jurisdiction in which a node in the blockchain network is situated, resulting in an overwhelming number of laws and regulations that might apply to transactions in a blockchain based system.

In a public blockchain system it will be important to consider what law might apply to transactions and consider appropriate risk management that should apply. However, with a permissioned or private system it is easier to create some form of legal framework and internal governance structure that will dictate the governing law that will apply to transactions. In private systems it would also be beneficial to consider some form of agreed dispute resolution process.

Crypto assets

The difficulties of applying the existing regulatory regime can be seen clearly when it comes to the use of crypto assets. We currently see a huge range of opinions from regulators on crypto assets, from outright scepticism and bans in some countries,[3] to more cautious investor warnings from others,[4] while yet other countries have introduced regimes to attract more crypto activity.[5]

These divergences of opinion and the resulting pitfalls are well documented in the example of Initial Coin Offerings, or ICOs. The popularity of selling tokens via ICOs as a means of start-up fundraising has exploded in the last few years. Figures show approximately $21.7 billion has been raised through some 935 ICOs over the period from January to November 2018 alone, dwarfing the amounts raised for blockchain projects via traditional venture capital during the same period.[6] However, given the divergence of regulator opinion on the specific legal implications of a token sale, organizations that fail to consider at the outset whether their token sale may be compliant in the jurisdictions in which they plan to offer tokens may face an uncertain future.

Organizations may also have to ensure that the sale of tokens is limited to buyers in their desired jurisdictions in order to remove the risk of the offer extending to jurisdictions that are more heavily regulated or have outright bans on ICOs. In the United States, the Securities and Exchange Commission (SEC) has expressed concerns that many ICOs are either scams or attempts to raise money without complying with investor protection laws.

Other countries' policy makers and regulators have sought to clarify the position by agreeing that not all ICOs would be required to comply with the same investor protection laws as would be the case with an initial public offering.

This has led to real difficulties for organizations that wish to use tokens in a legitimate way and are committed to complying with the regulatory regime wherever the token is made available. These organizations must deal with varying approaches across different countries, and the position also looks set to change—potentially very significantly—over the next few years.

These problems are particularly stark when one considers the reasons organizations wish to adopt cryptocurrency as part of their infrastructure. The traditional methods of raising capital to fund the growth of a business are debt financing and equity financing. This is clearly seen by both sides as a transaction in which the lender or investor should expect some form of return if the business is successful, but with an appreciation of the risk involved, particularly with early stage businesses.

An organization wishing to sell tokens may be seeking investment, yet it may also be attempting to build a user base through a network effect. If the organization is looking for an investment, it is perfectly reasonable for regulators and policy makers to expect it to comply with the usual investor protection laws; it would not seem equitable for an organization using cryptocurrency to circumvent these laws where the money raised from the tokens is an investment.

However, it is often the case that organizations using a token model want to build a network of users by offering cryptocurrency to use within the particular ecosystem being built. The objective in this case is to encourage people to become users of the organization's services, with the cryptocurrency used to pay for their provision. If the organization proves successful, the value of the token should increase accordingly, as usually there is a finite amount of the new currency sold. In this way, it is the users of the ecosystem who can contribute to and benefit from its success (and popularity), rather than equity investors. These types of tokens are often referred to as utility or consumer tokens, in that they are designed not as an investment but rather a device (or currency) to consume or use a particular service.

In many jurisdictions, regulators have acknowledged that there is a place for such tokens, and that they may not be regulated as an investment. A difficulty arises when organizations wish to sell tokens both to potential users of the system (utility tokens) and to organizations that do not intend to use the prospective service (for example, an investment bank or a venture capital company). Other challenges arise when the purchaser of the token buys many more tokens than the purchaser could possibly use or where there is no usable service at the point when the token is issued. Utility tokens that are sold as investments blur the line between what is regulated and what is not regulated, making it uncertain which regulations an organization must comply with in each jurisdiction in which a token is offered for sale.

These issues, together with the lack of a consistent global regulatory environment, can make it very challenging for those organizations that wish to benefit from the creation of their own crypto asset. There are many reasons why such organizations may want to create their own crypto asset, such as the payment and settlement systems example and the benefit of the network effect mentioned above.

Privacy and data protection

The issue of privacy and blockchain technology has been intensely debated. Many practitioners and academic commentators have claimed that blockchain technology is incompatible with privacy laws such as the EU General Data Protection Regulation, or GDPR.[7]

As mentioned above, the original purpose of blockchain was to facilitate peer-to-peer transactions without the need of a central party. In a permissionless public blockchain system, no single party takes responsibility for the availability or security of a particular blockchain network, and all users of the system may have access to the data on the network. These attributes conflict with the thrust of privacy laws, which require the party controlling personal data of an individual to safeguard the security and privacy of that data on behalf of the individual or "data subject."

Both a controller (the party that determines the purposes and means of processing particular personal data) and a processor (a party responsible for processing personal data on behalf of a controller, such as an outsourced service provider) have distinct obligations under the GDPR, making it important to determine whether a party qualifies as a controller or a processor when processing personal data. With a cloud computing system, typically those uploading personal data to the cloud environment are the controllers and the operator of the cloud system is the processor. This is a key area in which blockchain systems differ. Many blockchain systems are operated by all the users in a peer-to-peer network environment, which makes it difficult to define whether users are controllers or processors. It is necessary to consider to what extent the different participants in the blockchain network are controllers based on their respective activities.

Participants who submit personal data to the blockchain are more likely to be considered controllers under GDPR, as they determine the details of processing, whereas nodes that only process personal data are more likely to be processors, as they simply facilitate the blockchain network's operation. However, this determination is not straightforward, as not all blockchain systems operate in the same way, and there can be different types of participants carrying out various activities.

The nodes in a blockchain system might be compared to autonomous systems on the Internet. Each autonomous system receives packets and routes them autonomously to another node, repeating until the packets reach their destination. The kind of processing that blockchain nodes perform is arguably similar. The only purpose of the nodes is to ensure the integrity of the blockchain and to validate the addition of supplemental blocks. Privacy can be further protected through blockchain systems that use zero-knowledge proofs. This allows nodes in the system to verify transactions without the details of the transaction or the public key, ensuring personal data is not processed by nodes.

In the same way that a cloud service provider may not know what data a customer uploads to its cloud environment, administrators of a blockchain will not necessarily know whether personal data is present on the blockchain. Generic blockchains can be put to a wide variety of uses, and there can be different data and configurations, making it very difficult for the developer to build in privacy protections adapted to the nature of the data processed on the blockchain.

At best, governance rules can regulate users of the blockchain to respect privacy laws when they upload personal data to the blockchain. For private or permissioned blockchains, for particular purposes, governance rules can be much more developed, for example, by prohibiting users from uploading particular types of data to the blockchain.

Transfer of data

There have been debates in the cloud industry about when personal data is "transferred" overseas for privacy law purposes, and blockchain is likely to raise similar questions. For example, if a copy of a hash derived from personal data is made in Singapore, does this mean that data has been "transferred" to Singapore for the purposes of privacy law? In the sense that data may be transferred to a node in any location, data put on a public blockchain is similar to data posted to the public Internet.

The reasoning of the European Court of Justice (ECJ) in the Bodil Lindqvist case may apply to the question of transfer, although this case was in respect of the European Data Protection Directive, which preceded GDPR.[8] The ECJ held that it cannot be presumed that the word "transfer," which is not actually defined in the Directive, was intended to cover the loading by an individual of data onto an Internet page. A similar pragmatic approach is required for data on a blockchain to ensure that it is not "transferred" to every jurisdiction in which a node is present, causing unnecessary breaches of privacy regulations. As there is no single model for blockchain systems, each project will have to be analyzed on its own distinct merits.

Data security on blockchain

Blockchain technology is often referred to as "tamper proof." This is generally because each new digital 'block' containing a record of transactions is connected to all preceding blocks. In order to tamper with any of the records contained in a block, a dishonest participant would need to change all subsequent blocks in the chain to avoid detection.

Given that blockchain is a decentralized ledger, there is no single point of failure that dishonest participants can override. Instead, they would require a huge amount of power to override and alter every node simultaneously. This is especially prominent in public blockchains where there can be any number of nodes existing anywhere in the world. Blockchain therefore presents a lower risk of attack than with centralized systems, in which key servers can be targeted and altered without trace.

Blockchain also uses advanced public key cryptography to secure its data, which relies on users having two cryptographically matched keys. When someone wants to send a user a file, they send the file to a user's public key. The file can then only be opened by the user's correlating private key. Together these features make blockchain a very secure method of recording data. There is relatively low risk of data tampering or data being intercepted compared to traditional methods of transfer and storage, making blockchain a risk management system.

Risk of cyber-attack

Despite the high level of security that blockchain systems provide to the data recorded on them, there are some key cybersecurity risks that remain.

The unique challenge to decentralized systems, particularly public blockchains, is that data input can be from any number of nodes, meaning there is a risk of tampering at each node. The benefit of using a 'tamper proof' technology is negated if the information stored on the ledger is compromised to begin with. This type of attack is not aimed at the blockchain itself, but at external systems such as cryptocurrency wallets. There is a risk that individuals might target the data input point (rather than the ledger itself), leading to the dissemination of inaccurate information. Users operating on the blockchain would then unknowingly rely on misleading or false information. A 15-year-old boy from the United Kingdom proved this attack possible by developing a proof-of-concept code that allowed backdoor access into hardware wallets sold by Ledger.[9] Using this approach, it would be possible to change wallet destinations and amounts of payments. An attacker could divert payments to his own account while making it appear to be the intended destination, ensuring the attack is undetectable to verifying nodes.

Another way data on a blockchain can be compromised is by a targeted brute force attack on certain nodes. In some blockchain networks, a concentrated number of nodes carry out almost all of the processing. If someone were to identify and attack the nodes covering the required consensus level, the chain could be compromised. However, such an attack requires an enormous amount of computing power.

In some systems an attack would only need to control more than half of the computing power of all nodes. Such attacks are more likely to be successful if the attacker specifically attacks the nodes with the highest computing power in which most transactions are concentrated.

Double spending and DDoS attack

Double spending attacks occur when the same currency unit is assigned to multiple users, enabling them to use the same coin simultaneously.

A distributed denial-of-service, or DDoS, attack is a type of cyber-attack in which a perpetrator attempts to render a service unavailable to its users by overwhelming its bandwidth, often by flooding it with traffic. Blockchain systems are less susceptible to these kinds of attacks than are traditional centralized systems, given the lower numbers of potential points of failure and ability to include denial of service prevention. However, where ledgers are concentrated on a few high-performing nodes, the likelihood of a successful DDoS attack is increased.

Smart contracts

Smart contracts are self-executing software code that runs on a blockchain. They are not in themselves contracts, and often are not particularly smart. Contract law will likely apply to the underlying transactions between the parties using smart contracts, assuming that the arrangement between the participants otherwise fulfils the requirements for contract formation.

The code in the smart contract defines the terms of an agreement on an “if” and “else” basis and then automatically enforces those terms if and when the specific criteria programmed into the code are met. For example, the execution of a smart contract can be verified by the network of users on a blockchain system, removing the requirement of a trusted third-party intermediary. Smart contracts therefore have the potential to reduce costs in areas that typically rely on an intermediary today, such as clearing and settlement.

As demonstrated in 2016 by the hack of the Decentralized Autonomous Organization (DAO) public blockchain, it is possible to target smart contracts that are run on blockchain systems.[10] In the instance of DAO, the hacker was able to move approximately $50 million in investor funds to a sub-contract that the hacker controlled. This type of attack is less likely to occur in private blockchain systems due to the number of users that have access to the smart contract; however, features should be built into the smart contract to ensure that any hack can be corrected retroactively.

As mentioned above, traditional contract law may well apply to the underlying transactions embodied by smart contracts and, as such, the same liability issues apply to smart contracts. Software developers could therefore be liable for poorly written software code that results in a loss for their client, either through exploitation such as the DAO hack, or as a result of the code executing in a way not intended by the parties to the transaction.

Governance Impacts

Accountability

In relation to decentralized systems, a key question for regulators is who should be held accountable for breaches of law and regulation. This is similar to the problem of determining accountability on the Internet before the emergence of blockchain. Accountability of the various parties carrying out relevant activities on the Internet has been a vexing problem since its inception. Prior to the Internet, information and other content, such as music and video, could only be published through existing publishers with an established distribution network. Where there were legal issues about content, for instance issues with copyright infringement and defamation, the publisher was clearly accountable.

In the case of Google Spain v AEPD, the Court of Justice of the European Union (CJEU) ruled that a search engine could be held accountable for the protection of personal data in respect of third party websites accessible through its service.[11] It was emphasized in this case that the search engine’s activities could be clearly distinguished from those of the original publisher of the data. The harm to the data subject was not a result of the publication, but rather from the widespread availability of this information through a search engine.

In a public blockchain system, by contrast, there is no one easily held accountable in the same way as a search engine. In a private blockchain system, where there is clear ownership and responsibility, regulators might expect those running the system to be accountable for data added to the system by all the network users. The system owner could be seen as enabling the distribution of data through the blockchain in a comparable way to a search engine. It would then be the system owner’s responsibility to protect this data, despite not publishing the personal data itself. The owner would likely have to put in place a set of operating conditions on the private blockchain that comply with regulations, which all users would in turn agree to comply with.

Taxation challenges

The application of existing tax frameworks to a digitalized economy has posed significant challenges to national and global tax authorities. For example, digital economy concerns are at least partly within the scope of the OECD’s Base

Erosion and Profit Shifting (BEPS) concerns. In some cases, governments have suggested that broad-based "virtual" profit allocation rules, rather than existing permanent establishment concepts, should apply. India has introduced an "equalisation levy" on payments made to certain non-resident on-line service providers.[12] The European Union has considered similar measures. Over the longer run, a "virtual permanent establishment" concept is envisaged.

These ongoing discussions may have significant implications for blockchain and distributed ledger technology platforms. For example, it seems evident that cryptocurrency transactions will be taxed as assets, that is, on a capital gains basis, without application of VAT. However, issuances of utility tokens, for example, to employees, may be more appropriately taxed as income. Similarly, for policy reasons, government authorities may prefer to defer revenue recognition until disposition, or provision of the underlying services, as is the case in Israel. These are complex matters that, even within a BEPS framework, may promote competitive tax practices that other authorities may view with concern.

In the case of non-cryptocurrency platforms, BEPS-type concerns may well influence industry and governance structures in unintended ways. For example, industry DLT platforms for supply chain management may tend towards centralization, so that they are owned and nominally governed (consistent with BEPS limitations) from low-tax jurisdictions. Similarly, "smart contracts" more efficiently executed on-chain, may be moved off-line to centralized operations to ensure favorable tax treatment of ledger transactions. This solution may achieve compliance, however, at the cost of the efficiencies and certainty argued to arise from using a blockchain-only architecture.

Regulators working with the industry

To allow the financial industry to enjoy the full benefits of blockchain technology, it will be necessary for regulators to work with the industry to ensure that compliance with regulation can be achieved while still allowing blockchain technology to be used to maximum potential. In some jurisdictions, regulators may be required to move away from the use of detailed and prescriptive rules in favor of broadly stated principles that set the standards at which the industry must operate. This would allow regulations to be flexible enough to encompass the wide variety of systems that blockchain allows for. Even in these jurisdictions, however, regulators should work closely with stakeholders to ensure that their thinking on acceptable industry practices is transparent. As in Singapore and the United Kingdom, these efforts can support innovation by providing "bright line" certainty to new and non-traditional industry entrants.

One opportunity to adapt regulatory compliance to distributed ledger technology could be the use of regulatory sandboxes. These provide the ability to test services with real customers in a controlled environment without incurring regulatory consequences. Regulators can gain an understanding of the function of the blockchain systems and cooperate with the industry to identify and develop methods for compliance. This would help regulators develop a level of regulation that encourages and enables innovation while ensuring adequate protection for users—and would encourage development of technology solutions (such as electronic identification, authentication, and trust services that mitigate, for example, anti-money laundering and ultimate beneficial ownership concerns). One challenge of regulatory sandboxes is ensuring they are attractive to start-ups. Sandboxes should encourage innovation and allow for start-ups to grow, rather than merely offering value for the regulator.

Another opportunity to adapt regulatory compliance may lie in careful application of existing regulatory principles to the blockchain environment. For example, regulators will inevitably favor more centralized blockchain and DLT platforms that provide a "home" for regulatory supervision. Alternatively, in decentralized systems, they may take the view that all participants are liable for compliance issues. A more nuanced approach also may be possible. For example, in relation to regulation of privacy issues in unpermissioned systems, France recently took the view that only active participants—those actively inputting data into the system, and not mere "nodes" or "miners" providing verification of transactions to the platform—are responsible as data controllers.[13] This approach may more effectively balance the public interest in large-scale "trustless" systems, by ensuring meaningful accountability for privacy and personal data practices.

Finally, tax issues may continue to challenge the industry. Absent global agreement on "digital economy" principles, one can surmise a fragmented global tax environment, consisting on one hand of aggressively low-tax environments targeted at attracting "producers," and on the other hand, aggressively extraterritorial jurisdictions, targeted at realizing offshore income they believe has been derived from "consumption" in their home territory. Such a tax environment is uncertain for innovation, generating risky tax structures and deterring investors.

Meeting governance objectives

Blockchain system designers may seek to incentivize good behavior by participants in order to meet governance objectives and reduce the risk of non-compliance with regulation by the blockchain network. This may be done by setting rules that ultimately induce the right behavior. Bitcoin, for example, incentivizes miners to verify legitimate transactions by rewarding them with bitcoins. Bitcoin mining is difficult and inefficient by design, making it costly for any node that deviates from the correct protocol and fails to receive a reward.

Designers of blockchain systems could ensure compliance with the legal and regulatory framework by building it into the system. For example, participants could be locked out of the system unless and until they had been through an appropriate anti-money laundering compliance check.

Beyond blockchain and DLT platform design, decentralized systems pose significant governance and capacity challenges for participants and platforms alike. Fortunately, the industry and regulators have coalesced around key principles for digital platforms and outsourced information technology operations, providing a strong basis for risk governance. Key elements include careful management of information assets; board oversight of resilience and business continuity; development of operational risk metrics and integration with robust enterprise risk management capacity; and considered protocols for management of data incidents.

The proposed European Banking Authority outsourcing guidelines for banks in Europe are a good example of how regulators expect banks to manage outsourced risk, whether based on new technologies such as the cloud or on more traditional models. It is inevitable that regulators will expect the same level of risk management, due diligence, and ongoing monitoring of suppliers of blockchain based systems. Where there is no "supplier" as such (as for a public blockchain), regulators may be hard-pressed to establish oversight responsibilities beyond assuring robust diligence, risk governance, and reporting by users.

We can safely assume that regulators will want to ensure that transparency and understanding of smart contracts are embedded into blockchain and DLT applications. We can similarly surmise that legacy entities participating in blockchain and DLT platforms will want to "flow down" their requirements to governed platforms with a single point of accountability. This would suggest at least that even open permissionless systems will require thoughtful user understandings and allocations of liability, perhaps resembling governing organizations for open source software, to attract commercial users. For the immediate future, it may also suggest that use of permissioned and limited applications is more likely.

Two other governance areas will require resolution if the opportunities inherent in open, trustless systems are to fully emerge. First: decentralized autonomous organizations may present an entirely new mechanism for the organization of capital and commercial activity. Yet the structuring of these vehicles—with regard to risk management, minority protections, and transparency—remains an area for research and evolving practice. Second: there are concerns that the lack of a single point of accountability in a blockchain or DLT platform makes that platform an unincorporated joint venture in which all participants are jointly and severally liable for outcomes.

This is partly reflected, for example, in the French GDPR decision discussed earlier. While, as with the French decision, courts may ultimately limit this exposure to active participants and contributors, this will not be the argument made by plaintiffs' counsel. It is possible that some combination of a strict liability regime, together with statutory liability limitations and support of an appropriate insurance product, will be required. However, as in some public permissionless systems, this approach may be problematic when identity is not apparent, making apportioning liability difficult. This is yet another reason why we view entirely pseudonymous systems as unlikely to be acceptable to regulators, at least in regulated or sensitive settings.

A number of recent articles suggest that development of significant, impactful blockchain applications remains several years away. We do not believe this to be the case. At least for permissioned, governed systems, the regulatory and governance principles allowing public and private players to implement and operate these principles, on a risk assessed basis, are in place.

The more significant concern is that the continued relevance of these principles may deter realization of the full range of opportunities inherent in open, trustless systems. **Our discussion suggests that the application of these frameworks effectively requires a point of accountability for governance and liability, or in the alternative, some measure of joint and several liability by all participants.** More radical decentralization may require more interesting "compliance by design" elements, such as digital identifiers and ultimate beneficial ownership verification; agreed risk reporting available to participants and regulators, embedded in the platform's information architectures; and perhaps some form of overarching liability allocation framework, possibly comprising strict liability principles paid from a pool established by participants and supported by insurance and liability limitations.

The alternative position is that—at least in the short term—an accountable intermediary will be required. One option is that industry foundations, similar to those that exist for key open source software and content licenses, can facilitate the transition to more comprehensive decentralization. Another option is that a private sector technology company takes responsibility for the provision of the blockchain system (some of which might be provided in a permissionless way) in the same way that private companies provide open source software. This option may defeat the entire purpose of using a decentralized blockchain system, as it effectively centralizes the platform and requires users to trust that the provider is acting honestly (and will likely require that they pay a fee for the provision of the system). A partially, but perhaps more effectively, decentralized model may include a consortium of private sector providers who share responsibility, cost, and allocation of liability.

Conclusion

It is clear there are a number of important risk management concerns for any organization wishing to adopt blockchain technology. However, we have seen many of these challenges before in the adoption of the Internet generally, as well as other technologies such as cloud computing. The key is for the organization to truly understand the risks inherent in the system and to ensure that these are adequately managed and mitigated where necessary. The critical remaining issue is that the structure of contractual frameworks and associated regulation was not designed for the decentralized data world of blockchain. In particular, understanding who is accountable and legally responsible is a major challenge. It is clear to us that the adoption of the technology would be treated like any other form of outsourcing. For those wishing to adopt this new technology, there are three potential models to consider:

One. Private or permissioned models where a single party or group of parties takes responsibility for operating the system. This is the easiest path and would be no different from existing outsourcing/cloud arrangements. A node controlled by a regulator could also be included to act as a neutral party.

Two. Public blockchain systems where there is a clear contractual framework between the participants—one which reflects a more "joint venture" approach and which looks to allocate liability and accountability to the parties. This could be accomplished effectively by a kind of end-user license agreement that conditions use of the public platform on adherence; or perhaps even something that feels like an open-ended fund, where anyone can join but there is a clear legal structure and risk allocation. In general, it would seem that this model would have to be implemented on the inception of the system.

Three. Public blockchain systems where an organization takes on the responsibility and liability for running the system. This could be through open source systems such as Hyperledger, which has a core framework in place and the ability for organizations to alter the network according to their needs, grant permissions to those who need it, and keep out those who don't.[14]

It will likely be difficult for any organization that has to ensure effective risk management to consider a purely permissionless blockchain system without some additional protections. Of course, not all organizations have the strict requirements of financial services companies and other organizations in highly regulated sectors. Regardless of the model adopted by those seeking to use blockchain, it is important that regulators remain flexible in their approach to this emerging technology—and avoid viewing it through a lens designed for more traditional, centralized platforms.

ACKNOWLEDGMENTS

The authors would like to thank the following colleagues for their review and suggestions: Leslie Sturtevant, Manager, Practices AMC, Mobilization, Equity, Climate & Trust Funds, Legal, IFC; Andrew Yew, Senior Counsel, Legal, IFC; Rachel Alexandra Halsema, IT Officer, Business Management I, Technology and Innovation, World Bank Group; Baloko Makala, Consultant, Technology and Innovation, Information and Technology Solutions, World Bank Group; and Thomas Rehermann, Senior Economist, Thought Leadership, Economics and Private Sector Development, IFC.

Additional Reports and EM Compass Notes about Blockchain: *Blockchain – Opportunities for Private Enterprises in Emerging Markets* (report), IFC, October 2017; *Blockchain Governance and Regulation as an Enabler for Market Creation in Emerging Markets* (Note 57); *Using Blockchain to Enable Cleaner, Modern Energy Systems in Emerging Markets* (Note 61).

[1] Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. 2018. "Blockchain Technology Overview." National Institute of Standards and Technology.

[2] Deloitte. 2016. "Blockchain Technology – Speeding Up and Simplifying Cross-Border Payments." Also: Arnold, Martin. 2018. "Ripple and Swift Slug It Out Over Cross-Border Payments." *Financial Times*. June 5.

[3] One example is China.

[4] Many EU jurisdictions have issued warnings on the use of cryptocurrency but continue to apply existing legal principles.

[5] Gibraltar and Malta are examples of countries advocating cryptocurrency. See Gibraltar Finance. 2018. "Token Regulation: Proposals for the Regulation of token Sales, Secondary token Market Platforms, and Investment Services Relating to Tokens." Parliament of Malta, Virtual Financial Assets Act 2018.

[6] Figures as of 8 November 2018. https://www.coinschedule.com/stats.html

[7] The General Data Protection Regulation (EU) 2016/678.

[8] *Bodil Lindqvist v Aklagarkammaren i Jonkoping*, Case C-101/01.

[9] See Goodin, Dan. 2018. "A 'tamper-proof' currency wallet just got backdoored by a 15-year-old", arstechnica.com, March 31, 2018. https://arstechnica.com/information-technology/2018/03/a-tamper-proof-currency-wallet-just-got-trivially-backdoored-by-a-15-year-old/

[10] https://en.wikipedia.org/wiki/The_DAO_(organization).

[11] *Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez*, Case C-131/12.

[12] Indian Government. 2016. "Equalization Levy Rules."

[13] CNIL. 2018. "La Blockchain: Quelles Solutions Pour un Usage Responsable en Présence de Données Personnelles?"

[14] Corriveau, Adrianna, Deanna Vitale, and Brittany Manchisi. 2018. "Hyperledger Fabric: What You Need to Know about the Framework that Powers IBM Blockchain." *IBM Blog*.