Establishing blockchain policy

Strategies for the governance of distributed ledger technology ecosystems

pwc

FUTURE BLOCKCHAIN SUMMIT
قمة مستقبل البلوك تشين

Organised by
مركز دبي التجاري العالمي
DUBAI WORLD TRADE CENTRE

Hosted by
دبـــي الذكية
SMART DUBAI


BLOCK 01
BLOCK 01
BLOCK 01
BLOCK 01
BLOCK 01
NODE 01

Table of contents

Preamble

This whitepaper aims to explore a policy-based approach to applying blockchains, or more generally Distributed Ledger Technology (DLT) to a limited geographical or market region. In order to do this, we first lay out the problems that DLTs face, and the mitigation strategies that the market is adopting to deal with these limitations. The DLT space is undergoing rapid expansion and the number of projects has become so great, that it is a challenge to list them all. The technologies that are listed are meant to be a high level survey, but so many are named in the sections that follow that a 'definitions' section might easily exceed the length of the rest of this paper. We therefore encourage the reader to explore each one on their own and independently evaluate, which approach applies best to their specific needs.

The only definition that we would like to make in this paper is that of blockchains and of distributed ledgers, as we use both terms with slightly different meaning.

Blockchains were the first technological structures to solve the double spend problem and they rely on a massively replicated ledger that is appended by adding transactions in blocks. Each block is cryptographically linked to the previous block with the use of a cryptographic primitive called secure hash.

Distributed Ledger Technology (DLT) is the more general category of solutions that aims to order transactions, but may not use a linked chain of blocks to achieve its goal. Examples of distributed ledgers include Directed Acyclic Graphs (DAGs) and some approaches that aren't clearly structured as replicated chains of blocks but implement a shared transaction order nonetheless.

Executive summary

With widespread innovation comes a need for control

Blockchain has been on the lips of innovators and pundits over recent years. The level of interest and investment from technology buffs, venture capital, and established companies alike suggest that the revolutionary technology is here to stay.

The promise of blockchain can be understood best when used as a contrast to traditional integration approaches that focus on permissioned data sharing through a shared data store. Blockchains challenge this with the proposition to minimise the role of the shared service and data component and allow for privacy-friendly, direct peer-to-peer exchange of information that can be cross validated against a shared record of proofs.

As a result, the distributed ledger space might be the fastest growing area of innovation in the entire technology sector today. Along with huge potential to disrupt business and government operations, it presents many challenges. As with all emerging technologies, innovation, expansion, and development have been and will be led by both startups and major technology companies, collaborating and pushing each other to develop sustainable models. However, as with any disruptive technology, it is appropriate that a strategy be adopted to both foster innovation and control missteps that may occur due to experimentation and some inevitable misuse.

These strategies vary from technological routes that address scaling and privacy directly, through standards that address interoperability, to policy that aims to establish an environment for the technology to flourish and deliver its value. Establishing the right policy environment is the most important factor in mitigating the challenges and defining a way for organisations to cooperate, according to defined rules.

The impact of different approaches to blockchain policy

Depending on the appetite for innovation, policies can be either restrictive or permissive. Leaning too far to either end of this spectrum can yield negative results; stagnation if the policy is too restrictive, or harmful compromise if it is too permissive.

A good policy should aim to achieve a stated set of goals, define its scope of operation, be clear on how to operate under it in a compliant manner, and define who the authorities are. Moreover, a policy must evolve in a continuous improvement cycle that adjusts to lessons learned and a rapidly changing technological and global landscape.
Several countries have taken steps to establish such policies for their jurisdictions, varying in both purpose and approach. The United Arab Emirates (UAE) has been very active in this space, launching several programmes that include a blockchain platform for government entities, and a legislative sandbox for fintech startups. The sandbox enables the startups to explore the implications of the technology on the way business is conducted, to aid in defining what regulatory changes may be necessary to adapt to the developing landscape, if any.

Establishing the ground rules for blockchain governance

This paper dives into the challenges that blockchains and the broader distributed ledger technology landscapes pose, like privacy, performance, unpredictability, security, access to law enforcement mechanisms, and cryptocurrency as a new type of asset. The solutions discussed aim to establish some ground rules, which will allow organisations to establish governance structures that will help them navigate the technological landscape, while understanding some of the most important components of a strategic approach to policy.

The following high level strategies are suggested:

Technology – Organisations should adopt a technology-agnostic approach when looking to implement blockchain systems. Identities and data formats constitute core interoperability capabilities.

Governance – Organisations need to adopt flexible policies towards blockchain that are ready for a fast-paced and ever-changing technology landscape. Rigid polices risk becoming quickly outdated.

Governance – Organisations should lean more towards an innovative rather than risk-averse approach to blockchain, as the latter will be prohibitive to launching successful initiatives.

This paper is an output of the 2nd Global Leaders Exchange, held annually at the Future Blockchain Summit, hosted by Smart Dubai and Dubai World Trade Centre.

Introduction

Emergence of blockchains as distributed ledgers and their limitations

Blockchains have emerged through the creation of Bitcoin and several other similar techno-economic constructs, like Litecoin, or Monero. These blockchains showed how to implement ownership of digital assets through the use of an immutable history that is secured by an economic model. This model incentivises using energy to seal the order of blocks in a process called mining with proof of work. The limitation of this model was that the only type of transaction supported by the model was a financial transfer from one account to another, which limited the number of applications for the invention.

In 2014 a new type of blockchain was proposed that would manage more than just asset balances on accounts, it was designed to manage the execution of arbitrary computer programs called smart contracts. This concept was first fully implemented in Ethereum, which remains the largest second generation blockchain to date.

Smart contracts sparked excitement through their capability to autonomously transfer assets as a result of executing embedded computer code - removing prior requirements for a trusted third party. Many saw the possibility to reduce the bureaucracy and inefficiencies in low trust areas of the market, such as trade finance, real estate and all forms of certifications.

Is it possible to use a newer generation public blockchain to address the business problems directly? Depending on the technology in question, there are several challenges that impede straightforward adoption:

1. Public availability of transaction data posted to the blockchain
2. Performance and capacity limitations
3. Absence of a managed technology roadmap that could be influenced through a familiar governance structure
4. Weak security around identity and key management
5. Limited access to law enforcement for fraudulent transactions
6. The necessity to make every transaction use the cryptocurrency native to the blockchain (every Bitcoin blockchain transaction must transfer bitcoin, every Ethereum smart contract execution must be paid for in ether etc.)
7. Limited availability of oracles, which are sources of truth that lie outside of the blockchain network's reach (e.g.. today's temperature, or the price of a good in an open market)

These challenges prompted industry bodies to expand their search for a trusted distributed smart contract execution platform to the broader field of Distributed Ledger Technologies, or DLTs. DLTs are a broader class of distributed peer-to-peer database architectures. Examples include Directed Acyclic Graphs (DAGs) implemented in Hedera's Hashgraph and Iota, or Tempo implemented in Radix. Whatever the solution is, new approaches are rarely ready for enterprise use, and it is difficult to know today which of them will prevail over the longer term.

Nevertheless, it is possible that the promises of blockchain can be achieved with currently available technology.

The promise of blockchain can be understood best when used as a contrast to traditional integration approaches that focus on permissioned data sharing through a shared data store. Blockchains challenge this with the proposition to minimise the role of the shared service and data component and allow for privacy-friendly, direct peer-to-peer exchange of information that can be cross-validated against a shared record of proofs.

Through this mechanism, the promise of blockchain proposes that:

- Data sharing for the purpose of transactions can be conducted in a highly selective fashion without using an intermediary to enable privacy through disintermediation and data granularity;
- Information can be more trusted through a stronger identity component by using public key cryptographic signatures as proofs of ownership; and
- Services can occur peer-to-peer and so be weakly bound to location, allowing broader reach through lower security requirements.

This approach opens the doors to a wider scope of cooperation between industries that may use different systems, have different propensity to share data, and to increase potential for peer-to-peer cooperation by reducing reliance on querying central data sources for most up-to-date information needed to execute a transaction.

Examples of beneficial use cases include:

- Ability to selectively present information that is required to accomplish a transaction, for example proof of residence in a country without revealing the exact address;
- Change of ownership of physical property through a peer-to-peer transfer of title linked to a financial transaction in a traditional bank or digital currency account; and
- Data about a shipment travelling across many different systems and jurisdictions, yet retaining its trustworthiness and up-to-date state information.

Several strategic avenues can be devised to achieve these goals while addressing the challenges. They can broadly be described as **technology**, **standards**, and **governance** oriented. We describe these approaches briefly in the next section to show that the landscape is both broad and complex. We then consider a policy-based governance approach as one possible way forward for organisations to follow, so as to give the ability to reduce commitment to any specific technology or standard and to adopt new technologies and standards as they become available.

Background

A high level survey of strategies for dealing with the limitations of DLTs

Limitations of DLTs, and blockchains in particular, have sparked a search for solutions in the broader DLT class of distributed peer-to-peer database architectures. However, many of the available technologies have limitations of their own that include lack of maturity, reliance on governing authorities, performance, interoperability, and low adoption rates. Hence, three broad mitigation strategies have found support among different members of the global community. They include:

- Technology, to address limitations directly,
- Standards, to address interoperability and adoption,
- Governance, to address limitations through controlled access.

In the next sections we explore each of these briefly.

Technology

This strategy aims to use engineering (software and hardware) to solve one or several of the challenges. Examples of this approach include new consensus and incentive mechanisms, privacy enhancing protocols, scaling architectures, access control, and hardware-based key and identity management.

Alternate consensus mechanisms that favour speed over trustlessness have found some following. These types of mechanisms can be borrowed from traditional distributed systems, like Raft used by JP Morgan's Quorum, or purpose-built like Tendermint's Byzantine-fault tolerant private blockchain consensus algorithm, or Hyperledger Fabric's flexible approach that allows for algorithms to be switched as required.

Use of privacy enhancing protocols is another strategy that seems to offer some promise. Advanced cryptography has yielded intriguing algorithms that conceal transaction data without the use of encryption, so rules that govern transactions can be verified (e.g. a balance is not negative), but there is no way to decipher the data from the information stored on the blockchain. The only facts that are stored are proofs about the properties or the transaction, but not the values themselves. This approach is called Zero Knowledge Proofs, and examples include ZK-SNARK used in Zcash and ZK-STARK implemented by StarkWare. Even though these approaches offer almost magical levels of privacy and trust, their current implementations are considerably slower than standard encryption methods and we may need to wait for them to become practical at scale.

Straightforward encryption is another approach that is used in some solutions. Notably, IBM's Fabric, R3's Corda, JP Morgan's Quorum, Polkadot's Parity, and ConsenSys's Pantheon are some examples of solutions that use encrypted transactions that are only visible to a limited number of parties on the network. Validation of encrypted transactions still requires validators to know the contents, and therefore a trusted third party is required for most of these to function.

Another area of technological improvement has to do with scaling. Directed Acyclic Graphs (DAGs) are a solution that diverges from the singular ordered blocks in a blockchain into a transaction tree that branches out and achieves scale through execution of many parallel paths for unrelated transactions. DAGs are used in Iota and Hedera Hashgraph, and sharded blockchains are being explored by Ethereum Foundation and Radix.

Improvement of privacy and available throughput at the same time can be achieved through a lower membership count in the DLT network. Limitation of access is implemented through allowing only designated ledger validators via Proof of Authority. IBM's Fabric takes this approach to enable their private platform to achieve better performance through faster consensus algorithms among fewer nodes with trusted nodes verifying encrypted transactions. R3's Corda achieves faster speeds through peer-to-peer encrypted transactions and a small network of notary nodes for ordering of transactions, and R3's Ripple also benefits from a smaller number of validating nodes to order transactions faster.

The great many variants of technological approaches to resolve the limitations of DLT networks make it impossible to know which ones will ultimately prevail. It is only possible to commit to a few solutions in the short to medium term, and there is no guarantee that the choice will be right. A non technology-oriented market participant is therefore prudent to allow for a change of technological approach in the face of longer term goals.

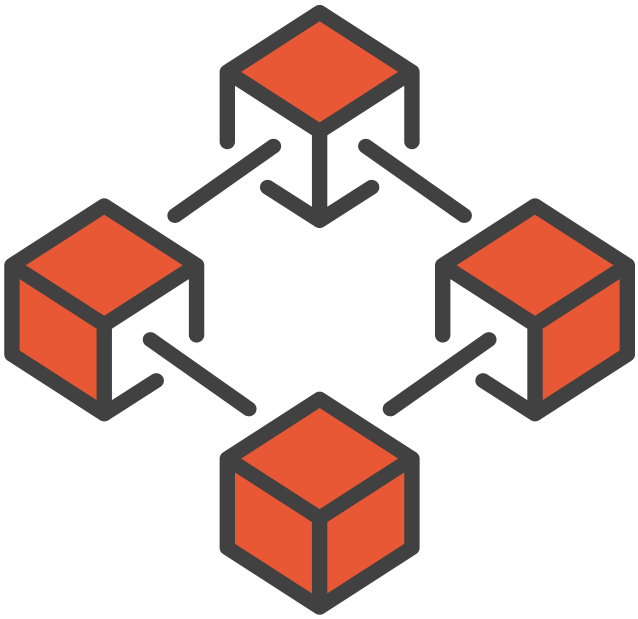
Standards

A large number of vendor-led approaches splinters the market and makes widespread adoption more difficult. A strategy that aims to expand the market for certain proven or promising solutions is to establish standards that can be adopted by multiple vendors. This strategy aims to establish a standards body that works to meet the needs of a specific industry or market by issuing formal specifications that can allow software to interoperate across networks and technologies. In the case of the World Wide Web, the standards body is the World Wide Web Consortium (W3C), which defines how web browsers should display web pages programmed in HTML. In the distributed ledger space, the most populous standards bodies are the Ethereum Foundation for Ethereum based enterprise private and public networks, and Hyperledger for a series of purpose-built distributed ledgers, like Fabric, Iroha, Indy, Sawtooth, and Grid. Notably, these two standards bodies command hundreds of member institutions each, and are members of each other's organisations.

The International Organization for Standardization (ISO), one of the leading global standardisation organisations, is developing technology-agnostic standards for blockchain and distributed ledger technologies. Namely, ISO has established a technical committee (ISO/TC 307) that is currently working to develop 11 ISO standards, with 42 participating entities and 12 observing members. This would have a significant impact on the standardisation of blockchain and distributed ledger technologies, one that might be comparable to the effect of W3C on the World Wide Web.

An alternate and perhaps more effective approach to standardising technology is to standardise data and identity formats and identify recognised oracles as sources of information external to the blockchain. Since network participants will often need to implement data processing capability on their own specialised software platforms, it might be more versatile to standardise on data exchange formats, identity (cryptographic signatures), and oracles. But leave the choice of technology as much in the purview of the network participants as possible.

An example of this approach is the minimalist functional approach taken by the Bitcoin community that essentially leaves all functionality that is non-essential to the functioning of the blockchain, to external technology choices of the network participants. As a result, the bitcoin blockchain only supports bitcoin transactions that can record the digital fingerprint of an off-chain data construct or collection. MIT's blockcerts standard for issuing blockchain-linked credentials implements this kind of approach, which works with the limited functionality available on the Bitcoin blockchain.



Governance

Many of the approaches mentioned above require closed networks with trusted memberships to function. The ones that are not sustained by economic incentive mining models need sponsorship to pay for the expense of maintaining nodes and for traditional network security to protect against potential attacks. This reality necessitates the formation of governance structures that confine a distributed ledger or set of ledgers to a defined area or market. The parties that partake in a governance model usually define a private network for the ledger to occupy, a set of rules by which these parties may interact and modify membership, and a technology or multiple ledger technologies that are deemed to fit in with the goals of the governance model. Examples of this approach include the UAE's Smart Dubai Blockchain Platform as a Service and SIA Group's SIAChain. PwC is involved in the implementation of SIAChain.

Smart Dubai's governance model has been announced to support Fabric and Ethereum. SIAChain was announced to support for Corda, Ethereum, and Fabric.

A governance structure can serve to limit the number of parties that see transaction data, limit the number of transactions to manageable volumes, determine a technology roadmap, cooperate with law enforcement, and agree on forms of payment to support the network. What remains is to establish a policy framework that will allow the consortium to function as intended.

This approach is not a new concept and can be traced back to many cooperative models that already exist in the industry. SWIFT is a well known and mature example of a multinational cooperative of banks. It was established in 1973 and combines a governance model with standards creation and the SWIFTNet suite of technologies for Securities, Treasury & Derivatives, Cash Management, and Trade Services.

In the next section of this paper we explore one possible approach to a distributed ledger governance policy.

Essentials of a policy

Essential elements of a functional governance model

Assumptions

Designing a governance model and policy should be as independent of the chosen technology as possible. This is especially important in a rapidly changing technological landscape, such as the DLT space, where the right choice of technology may change frequently, and there may be several technologies and standards that are in use at the same time. The need for multiple technologies is greater for governance approaches that are aimed at a geographic region, rather than a specific market niche. Whereas a governance model closely associated with a niche market might be able to converge on a small set of technologies, a geographically oriented governance structure will need to cover a broader set of use cases and needs to be more technology agnostic.

As a thought experiment, a good policy and governance model should function well, even when the chosen technology is a shared spreadsheet.

Strategic considerations

The goal of a good policy is to establish principles that will achieve a set of desired outcomes. To come up with a good policy, its creators must take into account the possibility that established rules may have consequences that are opposite of the desired outcomes by limiting options or by slowing down its subjects in achieving the desired goals. Therefore, the principles must be carefully considered and evaluated against positive as well as negative effects.

A good strategy for achieving desired outcomes, while avoiding risks can be modelled as a balance of progress versus risk management.

If progress is given too much priority, risky decisions may be undertaken and jeopardise the intended goals. On the other hand, if risk management is given too much priority, attempts at progress will be thwarted or subjects may choose other frameworks that are more conducive to achieving the desired goals faster.

Direction of a restrictive vs permissive risk management approach

Policies can be difficult to change and so must serve their purposes over extended periods of time, this means that an overly prescriptive policy runs a very high risk of becoming quickly outdated.

A policy that is too strongly tied to an industry landscape that has progressed can easily become counterproductive.

For this reason, the right balance for a DLT governance policy should benefit from an approach that leans toward the permissive end of the spectrum. This is especially important because DLT use cases can be tricky to work into models that deliver business value, and falling short of expectations is common.

Innovation is a famously difficult process to navigate as it involves dealing with failure in the face of elevated expectations. If the policy leans too strongly toward restraint before business value has been proven, the policy subjects may become strongly disincentivised from taking on innovative projects and from investing into the space.

As use cases prove their value, and where risks to compromising events are deemed to be increasing due to a high amount of activity and decreased visibility, it may become prudent to tighten the policy slowly over time. This is consistent with allowing for a more progressive approach when the adoption and exposure are small, and gradually attenuating risk as the stakes become greater.

Intellectual property

As DLTs are still nascent, research is always ongoing on its component elements, so breakthroughs may be encountered. The approach to intellectual property is evolving too, with some firms applying for patents or following a Software as a Service (SaaS) model, and some offering their technology to the market with permissive open source licensing conditions and full disclosure of source code.

The open approach has proven to be the most effective at spreading new types of solutions, when faced with limited resources for development and distribution. From a policy perspective, giving policy subjects a choice of approach to creating or using intellectual property is desirable, but needs to be balanced with interoperability across the policy's jurisdiction. Interoperability can be achieved by requiring data interchange format and encryption standards to be followed, so that ecosystem innovation efforts of participants are not restricted by choices made by others. The benefit of standardising interoperability through data and encryption standards is that both data objects and encryption standards can function across blockchain platforms.

An example of the effects of standardisation is that identities issued on several platforms could all serve to access one service, or vice versa, a single identity from one provider could operate across independently developed and operated services.

Interoperability

With numerous DLT networks forming and with the lack of established standards, interoperability may become a barrier for the smaller networks to merge and form larger and possibly higher-value networks. Although there are efforts to provide technical solutions for interoperability, they all present their own challenges. This also contributes to the hesitation companies and government agencies are going through when deciding where to invest in blockchain and which technology to bet on.

Incentive models

DLT use-cases and networks that do not have a proven incentive model, such as the mining model, may struggle with financially maintaining security of the network. Any established network must therefore have funding plans that ensure its adoption and an incentive model that will take hold once the value flowing out of them begins to be realised.

Privacy and confidentiality

As discussed earlier, privacy and confidentiality are key factors when it comes to blockchain and DLT. Information on the blockchain is immutable by design, hence, it is possible that the use of blockchain may bring challenges with complying with privacy regulations and standards, such as the European GDPR (General Data Protection Regulation), Bahraini PDPL (Personal Data Protection Law), Qatari DPL (Data Protection Law) and expected laws across the GCC. The main concern is that data stored in a replicated and indelible medium is a risk to privacy. This is true, even if the data is encrypted, since guarantees about the security of encryption are time-bound for any given encryption scheme. This means that in order for encryption to remain effective, it must be possible to upgrade the encryption when weaknesses are found, and old copies need to be deleted. This is a concern even before we start considering the “right to erasure” that has gained adoption in Europe as an emerging legally required feature of systems that store personal data.

Even in a private blockchain network that implements Zero Knowledge Proofs, where no information is actually stored on the blockchain, the volume of transactions alone may be confidential information between competitors in the same network. This can be another obstacle for blockchain network formation, especially for industry networks that would naturally include competitors.

These challenges mean that the only viable mechanism today for handling personal data is to store and manage it off-chain in traditional systems with known privacy enabling architectures, such as private cloud and point to point encryption.

Security

Private blockchains lose some of the security aspects inherent to fully trustless public blockchains. In a closed loop of trusted nodes, a security breach of one of the nodes might compromise the whole network. This elevates the importance of infrastructure security and key management and presents a crucial area for standardisation and enforcement across all participants.

Addressing these challenges through policy

As a deduction from the previous sections, a good policy in the DLT space needs to be as technology agnostic as possible and permissive in a way that stimulates innovation, while containing risks and mitigating the challenges that impede blockchain adoption and network formation.

Instead of dictating approaches and solutions, the form of which no one can reliably predict, a policy can provide guidance and stimuli for participants to agree on an approach to move forward to test it.

As such, a DLT policy might give priority in network formation to industry governing bodies or can stimulate the formation of such bodies that can drive network formation. Additionally, it can identify the areas that network participants need to openly address.

However, one foundational element that can be directly addressed through a policy and that can have a profound effect on blockchain implementation is identity management. Having a trusted source for issuing digital identities for entities and individuals can play a significant role in driving adoption and facilitating interoperability between blockchain networks, and this is not exclusive to private blockchains.

In other areas, policy can provide the general guiding principles, such as requiring that no data gets stored in clear on the blockchain, specifying the minimum security standards that networks need to adopt, and addressing the key laws and regulations that the networks need to uphold while providing support and guidance on the laws and regulations that are not yet ready for a fully-digital age.

Areas for policy governance

Key areas of focus for governance through policy making

Currently, the formation of blockchain networks is spontaneous in nature, whereby companies and government entities are internally exploring blockchain use-cases, identifying the partners and external parties that need to be part of the network, and reaching out to these parties to convince them of co-founding or joining the proposed network. This model has a few shortfalls that are proving to stall adoption of blockchain technologies and formation of value-creating DLT networks. Next, we explore some of the key obstacles for network formation and a policy approach to mitigate their effects.

Objectives

The first element of a policy must be a clear definition of its objectives. The objectives should answer questions about the scope of the policy in terms of eligibility and applicable areas of activity. The objectives should also name an authority that will ultimately be responsible for tuning the risk balance for the entire policy. The purpose of the policy must be clearly stated and expected benefits should be outlined.

Network formation and operation

The rules that govern network formation can be either permissive or restrictive. Permissive rules may allow the member entities to form a network spontaneously with only a declaration of conformity. A more permissive approach may lead to a greater number of networks being formed experimentally, while a more restrictive approach may require network formation to first be approved, and result in networks being formed sparingly and only after thorough research and justification.

The formation rules can address the topic of accession and secession from the network as well as general rules for the operating model. Depending on the goals of the policy or a particular network, some flexibility may be warranted to make room for experimentation by the network members.

Technology and standards

Even though a policy is well advised to allow for changing of technology approach and standards over time, it may be prudent to select a few approaches that are preferred over others to narrow choices for some types of use cases. At the same time, leaving an option to introduce new standards and technologies may be a path left open for exploration and learning.

Identity and security

Just as the familiar internet is a network of locations defined by Internet Protocol (IP) addresses, a DLT is a network defined by identities represented by public and private keys. On the internet, the location of an address defines it with identity being a secondary layer, while on a DLT the identity of an address defines it, with location being a secondary layer.

Regardless what technology approach is chosen, DLTs are networks defined by identity, and the policy must specify how identity of members is defined. DLTs rely on strong cryptography to sign all transactions and for permissioned blockchains, consensus membership is also determined by strong cryptography. For this reason, one of the most important elements of a policy is the definition of identity and the regulation of access control lists as well as prudent specification of the requirements for the technology that must support the definition of compliant identities.

Because location is not fundamental to how DLTs operate, identities form the basis for DLT security and are its foundation. The use of self sovereign identity (SSID) architecture and hardware devices, such as Hardware Security Modules (HSMs), for managing identities may be required for many if not most use cases to maintain appropriate levels of security.

Compliance

No standards or policies can hold without rules for ensuring compliance. Structures should be put in place that assign responsibility for maintaining compliance of the technology, systems, and procedures. Compliance needs to be reviewed periodically, and formal reports can help improve the policy over time.

Continuous improvement

Finally, the fast changing DLT landscape means that accompanying policy must not only be ready to be changed, but also be frequently reviewed and amended as solutions are better understood and as the technology landscape changes. The frequency of review may need to be as often as every year or more frequent to maintain momentum. Changes may result from lessons learned, new solutions becoming available and older solutions losing support. The policy may also need to shift focus as use cases are proven or disproven and DLTs start working across markets and geographies rather than just within them.

Examples of nationally led approaches to enabling blockchain and DLT through policy

United Arab Emirates

The UAE has undertaken a broad and multi-faceted blockchain-themed initiative called Emirates Blockchain Strategy 2021. The aim of this strategy is to transition 50 percent of applicable government transactions to a blockchain by 2021.

As part of this initiative, Smart Dubai has launched a Blockchain Platform as a Service to host government use cases, and there are over 30 blockchain projects under development. Through this policy, government entities are encouraged to establish integration channels with the aim to improve functioning of services that cut across areas of responsibility of several entities, and increasingly to enable digital integration with the private sector.

Abu Dhabi Global Markets Financial Services Regulatory Authority (ADGM FSRA) has initiated a regulatory sandbox and has issued guidance for the regulation of crypto assets with the aim to establish rules to govern the safe operation of cryptocurrency related fintech businesses, while the Central Bank of the UAE (CBUAE) has circled warnings confirming that cryptocurrencies are not considered as a valid/ recognised currency under current regulations/ legislation, and are banned from being used in a commercial transaction context.

In addition, the Emirates Authority for Standardization and Metrology (ESMA) are one of the twelve observing members Monitoring ISO/TC 307 (ISO Blockchain Standards).

Malta

Malta's approach is highlighted by their regulation of blockchain and DLT through technology certification, which has been performed with the aim of not stifling innovation. In particular, the MDIA Act establishes the Malta Digital Innovation Authority, which is entrusted with certifying blockchain and DLT platforms via a system auditor that reviews and assesses the technology arrangement and provides assurance on the solution's quality and characteristics. This has been developed to enhance the community's trust in the technology by creating a form of regulation through certification in a sector that is currently lacking such measures.

Liechtenstein

On the other hand, Liechtenstein has focused on regulating the token economy, whereby its blockchain act focuses on the creation, storage, and transfer of tokens, along with the security for enforcement of the rights associated with every token, thus creating a token economy.

United States

In the United States, several different policies can be observed. The federal government has taken a hands off approach, enabling state governments to create and implement their own policies and regulations. In a bid to attract innovation, some states have taken the approach of removing the legal barriers for the adoption of blockchain by developing blockchain-friendly legislation. For instance, the State of Illinois has published the Blockchain Technology Act, specifying the permitted use of Blockchain for conducting business and prohibiting local government restrictions on Blockchain or smart contracts.

Another state that took the lead in creating a permissive policy is Wyoming. The state has passed a collection of 13 blockchain and cryptocurrency friendly laws. Among them is the establishment of a new type of bank that can hold crypto assets for its customers starting in 2020.

The state of New York took a more restrictive approach by creating the BitLicense, which is issued by the New York State Department of Financial Services. Under this regime, any business operating in the virtual asset space must first obtain approval for a license to carry out activities.

European Union

The European Union has taken a measured approach to introducing blockchain-related policies or legislation, adopting a permissive stance with wide discretion given to the member countries. An early permissive move in 2015 by the EU was to allow exchanges of traditional currency for cryptocurrency not to charge VAT on their service, effectively allowing cryptocurrencies to function as forms of money. As a restrictive counterbalance, the EU has also mandated KYC and AML measures to be implemented by exchanges under the Fifth Money Laundering Directive (5MLD).

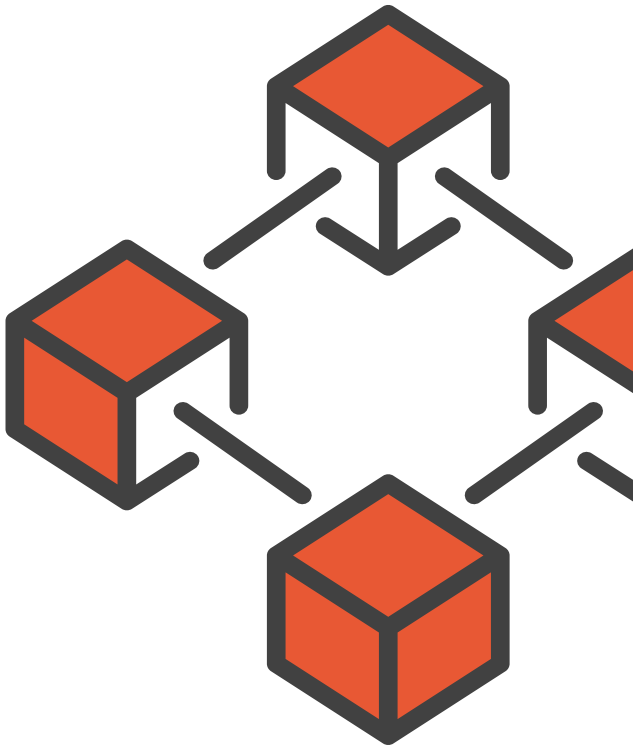
In addition, The European Parliament is requesting that the European Commission and other EU authorities take various steps to maximise the potential of Blockchain and DLT in the EU, and that any regulatory approach towards DLT should be innovation-friendly, should enable passporting, and should be guided by the principles of technology neutrality and business-model neutrality. They have also underlined that the Union should not regulate DLT per se, but should try to remove existing barriers to implementing Blockchains, calling on the Commission and the Member States to foster the convergence and harmonisation of regulatory approaches. This supports the Commission's approach of following a use-case method in exploring the regulatory environment around the use of DLT and the actors using it by sector.

The European Data Protection Supervisor (EDPS), the EU's independent data protection authority, has been given the responsibility of: providing further guidance on how DLT can comply with the EU legislation on data protection, and in particular, the General Data Protection Regulation; working with international organisations to enhance the development of technical standards for smart contracts and to undertake an in-depth analysis of the existing legal framework in all member states on the enforceability of smart contracts; assessing whether any potential barriers to use of smart contracts are proportionate, noting that legal certainty could be enhanced through coordination and mutual recognition between member states; and analyse whether a European passport for DLT-based projects could be introduced to enhance legal certainty for investors, users and individuals and promote financing to small- and medium-sized enterprises.

Closing remarks

The distributed ledger space might be the fastest growing area of innovation in the entire technology sector today. Along with huge potential to disrupt business and government operations, it presents many challenges. As with all emerging technologies, innovation, expansion, and development have been and will be led by both startups and major technology companies, collaborating and pushing each other to develop a sustainable technology. Predicting the way this will happen is beyond the scope of this paper, but the solutions presented here aim to establish some ground rules. These will allow organisations to establish governance structures that will help them navigate the rapidly changing technological landscape, while understanding some of the most important components of a strategic approach to policy. These components include identity as the basis of security, incentive models as funding strategies, and the balance of progress versus risk avoidance.

With the policy strategy set and tuned to be biased toward balanced permissiveness, the challenge becomes to improve through iteration, because in order to maintain a leadership position in a nascent field, agility is a crucial ingredient.



Contacts

To have a deeper conversation about how this subject may affect your business, contact:

Ahmad Abuhantash
Partner, Technology Consulting
PwC Middle East
E: ahmad.abuhantash@pwc.com
T: +971 (0)56 682 0640
linkedin.com/in/aabuhantash
@AbuAlHantash

Jan Grabski
Director, Technology Consulting
PwC Middle East
E: jan.grabski@pwc.com
T: +971 (0)54 793 3475
linkedin.com/in/jangrabski

Hadi Kobeissi
Senior Manager, Technology Consulting
PwC Middle East
E: hadi.kobeissi@pwc.com
T: +971 (0)50 900 7678
linkedin.com/in/hadikobeissi

Matthew White
Partner, Digital Trust Leader
PwC Middle East
E: matthew.white@pwc.com
T: +971 (0)56 113 4205
linkedin.com/in/mjwme
@mjw0610

Oliver Sykes
Partner, Digital Trust
PwC Middle East
E: oliver.sykes@pwc.com
T: +971 (0)56 480 2447
linkedin.com/in/osykes

Nisha Ramisetty
Director – Conferences & The Future Blockchain Summit
Dubai World Trade Centre
E: nisha.ramisetty@dwtc.com
T: +971 (0)4 308 6717
linkedin.com/in/nramisetty

Musthafa Ahmed
Sales Manager
Dubai World Trade Centre
E: musthafa.ahmed@dwtc.com
T: +971 (0)4 308 6498

Shivani Sehgal
Conference Manager
Dubai World Trade Centre
E: shivani.sehgal@dwtc.com
T: +971 (0)4 308 6780

Stephen Durning
Marketing Manager
Dubai World Trade Centre
E: stephen.durning@dwtc.com
T: +971 (0)4 308 6095
linkedin.com/in/steve-durning


NODE 03


NODE 01
NODE 04
NODE 05
NODE 02
NODE 06
BLOCK 01
BLOCK 01
NODE 01
NODE 02

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with over 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 6000 people (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity.
Please see www.pwc.com/structure for further details.

Creative Design Center CDC 1895