AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Getting ready for Blockchain

Explain the technology, foster its development

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €2 trillion in 2017, directly supports more than 4.7 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Contents

Executive Summary 3
Introduction 4
1. What Blockchain is 4
Definition 4
Key attributes and benefits 4
2. How Blockchain works 6
General functioning 6
Applications 8
3. Technical challenges 11
4. Regulatory challenges 13
Conclusion 15
Annex - Glossary 16

Executive Summary

- A blockchain is a specific type of distributed ledger technology (DLT), namely a shared and replicated ledger which allows a fast and secure transaction of assets. One of the primary benefits of blockchain is that it offers a mechanism to establish trust in digital transactions. Most blockchains are an example of open source software,and as such, many facilitate collaborative, open innovation and can be re-used for multiple purposes and environments.

- Blockchain owes its name to the way it stores transaction data - in blocks that are linked together to form a chain. As the number of transactions grows, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain within a network governed by rules agreed on by the network participants.

- Blockchain applications have the potential to bring tremendous benefits in a wide range of sectors, including: new forms of economic incentives such as cryptocurrencies, more transparent food supply chains, faster trade transactions, easier cross-border payments and managements of decentralised energy supply.

- The technology remains in its early stages and its uptake will be conditioned by the ability to address technical barriers, including interoperability, addressing potential vulnerabilities and solving equations such as scalability constraints versus benefits. The uptake of blockchain within organisations will ultimately mean a cultural change and requires building trust and legitimacy.

- Blockchain needs the right regulatory and policy environment to flourish. While legal certainty is required in certain areas, this does not necessarily require new laws but rather guidelines. A strong public-private partnership and testing will foster the uptake of the technology.

Introduction

Blockchain has become one of the most hyped technological innovations since the Internet, with one of its applications, namely cryptocurrencies, attracting massive attention from both public and private stakeholders. Blockchain, and more generally distributed ledger technology (DLT), has attracted significant interest due to its potential to reshape industries, organisational and governance structures and disrupt traditional business models.

At EU level, the European Commission has launched a series of initiatives to develop a common approach on Blockchain technology for the EU in the international arena. In addition, the European Parliament adopted a resolution in October 2018[1] acknowledging the potential of this technology in a wide range of areas, such as environment, transport, trade, education, finance and healthcare. This positive message was reinforced by another resolution in December 2018 on Blockchain and trade[2].

In order to help the development and uptake of this technology, this policy paper attempts to explain the technology (section 1), its application (section2) as well as to shed light on the technical and policy challenges (sections 3 and 4) that need to be overcome.

1. What Blockchain is

1.1. Definition

The terms blockchain and DLT are often used interchangeably, but they are distinct innovations. DLT is a family of technologies that employ a shared database architecture to maintain multiple, identical copies of an auditable, up-to-date distributed or decentralised ledger of transactions or data. It enables untrusting parties with common goals to co-create a permanent, immutable and transparent record of exchange and processing, while making the database more secure and resilient.

We can categorise DLTs according to certain characteristics. First, the ledger may be publicly available or not (public versus private). Second, they can differ in terms of which set of verifiers are authorised to validate transactions (permissionless versus permissioned).

A blockchain is a specific type of DLT, ie. a novel transaction-recording mechanism and a method of organising data in aggregated, ordered blocks that are 'chained' together by a cryptographic hash function. New blocks are added to a blockchain after their integrity has been validated by a network of participants or 'nodes' through a rules-based consensus mechanism. Blockchains are used to create and maintain a shared system of record and platform for tracking transactions or other data. Any attempt to edit or corrupt their historical record is either excessively expensive or becomes immediately evident. When used in combination, blockchain's complementary technologies provide a powerful toolkit for a broad range of commercial applications.

Blockchain first emerged as the underlying technology that made Bitcoin possible, and since then has seen intense interest across most major industries. **The promise of blockchain is that it enables new means of exchanging business value in a decentralised manner** - from facilitating the transfer of assets, to rewiring record-keeping processes, to supporting data sharing and preventing data tampering.

1.2. Key attributes and benefits

One of the primary benefits of blockchain is that it offers a mechanism to establish trust in digital transactions. It provides a means for verifying the recording of information and transactions in a shared database, particularly relevant in applications requiring the secure storage of transactional records. The immutability of data entries

[1] https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0373+0+DOC+XML+V0//EN&language=EN

[2] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2018-0528&language=EN&ring=A8-2018-0407

stored on a blockchain can be used to create a trusted and permanent record of transactions, enabling verification of ownership across multiple applications.

The Blockchain's ability to enable a practically permanent and trusted digital record is its primary differentiator. As such, some of the key benefits of blockchain include:

- **Efficiency and immutability**: digital record keeping allows for verification, thereby improving the processing of transactions while lowering the need for manual and expensive processes. Its decentralised nature allows each party to simultaneously record transactions on the ledger with built-in protocols to ensure there is no duplication or fraud. The data is immutable because each transaction is cryptographically secured and linked to the previous transaction as it is recorded.

- **Disintermediation and decentralisation**: blockchain platforms facilitate the transfer of financial and physical assets without the need for a trusted intermediary for verifying records and ownership.

- **Automation**: it provides a platform to automate standardised agreements. Blockchain allows the use of 'smart' contracts that control the transaction agreement details that are stored on a network and can enforce and execute contract provisions automatically.

- **Trust, Certainty and Security**: blockchain allows users to create an operating system of trust. Its time-stamped records facilitate the provenance of assets and improve the quality of record keeping. By eliminating a single point of attack, its distributed nature allows for greater resilience against cyber threats.

- **Authentication, Transparency and Auditability**: blockchain delivers greater information visibility across parties, improving compliance and auditability. Information inserted in a digital code is stored in a transparent shared database with a digital signature that is verifiable, irrefutable and traceable.

- **Community**: blockchain is a network technology which relies entirely on the broadest possible ecosystem to co-develop trusted solutions. Permissive IP policies, straight-forward governance and an open culture have created a transformative open source community of 15+ million developers with 1+ million projects from which products are ultimately derived and supported for end-use.

As with any new technology, the full range of potential applications for blockchain remains unknown. The global blockchain technology market is expected to grow at a rapid pace as blockchain-enabled distributed ledger networks and related new data management applications are developing and generating interest across all sectors.

2. How Blockchain works

2.1. General functioning

Basics

Blockchain owes its name to the way it stores transaction data — in blocks that are linked together to form a chain**.** As the number of transactions grows, so does the blockchain. Blocks record and confirm the time and sequence of transactions, which are then logged into the blockchain within a network governed by rules agreed on by the its participants.

Each block contains a hash (a digital fingerprint or unique identifier), timestamped batches of recent valid transactions and the hash of the previous block. The previous block's hash links the blocks together and prevents any block from being altered or a block being inserted between two existing blocks. In this way, each subsequent block strengthens the verification of the previous block and hence the entire blockchain. The method renders the blockchain tamper-evident, lending to the key attribute of immutability.

The blockchain holds two pieces of information, the block list (a linked list) and the transaction list (a hash map). As such, it is responsible for:

- Verification of arriving blocks;
- Verification of arriving transactions;
- Synchronisation of the transaction list; and
- Synchronisation of the block list.

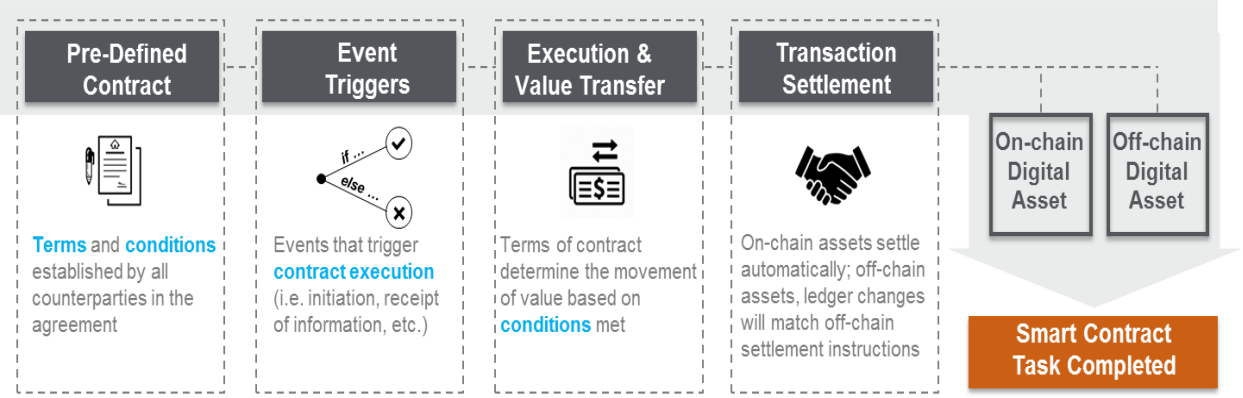
Permissioned and permission-less

An important parameter in blockchain systems that extends beyond the technology is the nature of participation: open or restricted. An **open blockchain** is often referred to as **public or permission-less**, because anyone (with the necessary technical abilities and computing power) can access and participate without being vetted (peer-to-peer). This model makes the system more vulnerable to attacks, therefore for some applications, restricted participation might be preferable – eg. financial and government applications. Permissioned networks and private ledgers have been explored by organisations as a more secure and efficient alternative to open blockchain systems.

In a **restricted blockchain** – also referred to as private or permissioned blockchain - consensus is usually achieved through a process called **selective endorsement**. It is based on the concept that network participants have gained permission to be there and that the participants involved in a transaction are able to confirm it. The advantage of this is that it can be built with a more modular architecture, and it can allow for greater transaction volume at faster speeds. Endorsers are determined by the governance and operating rules for the network.

Smart contracts

Smart contracts are programmed rules that are self-executed or verified by computer code. When some predefined terms and conditions in a contract are met, a set of predefined actions are executed without an enforcement authority/mechanism other than computer code.



Source: Citi

Consensus mechanisms

A blockchain consensus mechanism is the protocol used to agree on the 'truth' when the blockchain is receiving data from many independent nodes that may be faulty or otherwise untruthful. However, one of the limitations of blockchain is that consensus mechanisms using proof of work (PoW) are by their nature slow. To overcome this, the community can come to an agreement and throw away the blocks they don't agree on. This design also provides a solution to inherent inefficiencies with blockchain, such as electricity consumption, as stale blocks are discarded. Below we list different types of consenus mechanisms.

Proof of work

PoW is a common consensus algorithm used by the most popular cryptocurrency networks like Bitcoin and Litecoin. It requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain. However, this whole mining mechanism of Bitcoin needs high energy consumption and longer processing time.

Proof of stake

The proof of stake (PoS) is another common consensus algorithm that evolved as a low-cost, low-energy consuming alternative to the PoW algorithm. To validate transactions, validators must hold a certain percentage of the network's total value. Proof-of-stake might provide increased protection from a malicious attack on the network by reducing the incentives and making it very expensive to execute.

There are two main types:

- **Multi-signature**: a majority of validators (for example, three out of five) must agree that a transaction is valid.
- **Practical Byzantine Fault Tolerance (PBFT)**: an algorithm designed to settle disputes among computing nodes (network participants) when one node in a set generates different output from the others.

Proof of Elapsed Time

Another alternative to PoW is Proof of elapsed time (PoET), which uses a trusted execution environment to generate efficient leader election (the participant who can solve to reduce the computation and energy cost, while delivering a fair distributed consensus.

Other

Alternative consensus mechanisms include:

- Delegated Proof of Stake,
- Proof of Burn,
- Proof of Capacity,
- Proof of Identity, and
- Proof of Importance.

2.2. Applications

Cryptocurrencies and tokens

Cryptocurrencies such as Bitcoin are digital or virtual currencies that are secured by cryptography and consist of a peer-to-peer network of nodes which jointly maintain a common tamper-resistant record of historical transactions, without relying on a central authority or trusted third party. The term virtual or digital currency has regularly been used as a catch-all synonym for all the new models of digital assets in existence, variously referred to as cryptocurrency, coins and tokens.

At present, there is no generally recognized terminology for the classification of tokens. For example, the Swiss Financial Market Supervisory Authority (FINMA) categorizes tokens into three types, acknowledging that hybrid forms are possible:

- **Payment tokens** are meant to function as a means of payment for goods or services (inter alia) external to the platform or not only exclusively between the platform and its users but also between users.
- **Utility tokens** are intended to provide digital access to an application or service and are supposed to convey some functional utility to token holders other than/in addition to payment for goods or services, in the form of access to a product or service offered or at least intended to being enabled or created.
- **Asset tokens** represent assets such as participations in real physical underlyings, companies, earnings streams or an entitlement to dividends or interest payments. In terms of their economic function, the tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain also fall into this category.

Trade Facilitation and supply chain traceability

According to Organisation for Economic Co-operation and Development (OECD):

'[Blockchain technologies] have the potential to create novel ecosystems for trade: helping coordinate value chains by increasing trust and speed of transactions; empowering actors; enabling the verification of the provenance of products; facilitating the transfer of funds and helping better enforce or automate contracts (such as through smart contracts). At the same time, these digital technologies can enhance trust for consumers, increase the resilience of value chain for private actors, and enable the public sector to better manage risk and costs for customs authorities.'[3]

[3] OECD, Trade and Agricultural Directorate-Trade Committee, Working Party of the Trade Committee, 'Digital trade and market openness, August 2018.

More than 80% of the goods consumers use daily are carried by the ocean shipping industry. By reducing barriers within the international supply chain, global trade could increase by nearly 15%, boosting economies and creating jobs. Blockchain is a perfect tool for global supply chains, empowering multiple trading partners to collaborate by establishing a single shared view of a transaction without compromising details, privacy or confidentiality. Shippers, shipping lines, freight forwarders, port and terminal operators, inland transportation and customs authorities can use it to interact more efficiently through real-time access to shipping data and shipping documents, including Internet of Things (IoT) and sensor data ranging from temperature control to container weight.

Cross-border payments

Sending money across borders today requires a series of intermediaries for both clearing and settlement, each adding time and cost to the process. Delays and disputes have long hampered the cross-border payments industry. Blockchain can help create and manage integrated networks for real-time clearing and settlement, allowing banks and financial institutions to send and settle payments around the globe with finality in a matter of seconds.

A Blockchain solution can use digital assets to settle transactions - serving as an agreed-upon store of value exchanged between parties - as well as integrating payment instruction messages. It all means funds can now be transferred at a fraction of the cost and time of traditional correspondent banking.

For example, two financial institutions transacting together agree to use a stable coin, central bank digital currency or other digital asset as the bridge asset between any two fiat currencies. The digital asset facilitates the trade and supplies important settlement instructions. The institutions use their existing payment systems - seamlessly connected to the blockchain platform's application programming interface (API) - to convert the first fiat currency into the digital asset. The blockchain platform then simultaneously converts the digital asset into the second fiat currency, completing the transaction. All transaction details are recorded onto an immutable blockchain for clearing.

From farm to fork – Blockchain in the food chain

European citizens are seeking greater transparency and traceability in consumer goods, especially concerning the food they have on their tables. Blockchain technology could play an important role in connecting consumers to the farmers and increasing transparency in today's digitally enabled world.

A blockchain solution can provide authorised users with immediate access to actionable food supply chain data, from the farm, to the store and ultimately to the consumer. Farmers, producers, processors and retailers would upload product information onto an app. This data then forms the series of blocks for a blockchain. Every actor in the food chain has access to this auto-generated flow of information. It creates a peer-to-peer system that contributes to a tamperproof history of records. In addition, digitisation of the exchanges removes transaction costs and reduces the risk of fraud as information is directly transferred to a cloud-based information platform.

Currently, it can take up to seven weeks to trace the source of a product using a traditional database or without a digital traceability tool. However, this could be reduced to as little as 2.2 seconds through using a blockchain approach, accessible via a cloud-based database. By scanning the product code with their smartphone, consumers would have direct access to the food's journey. For meat, this would include its complete history: birthplace, breeder, medical record, and specific diet.

As information is directly accessible and transparent, consumers will be able to make fair, informed and empowered choices. Blockchain technology is still at an early stage and we should work to solve the technical barriers regarding interoperability and vulnerabilities. Furthermore, partnerships with regulators can build a reliable and agile policy framework to provide legal certainty and support the deployment of blockchain in the food chain going forward.

Energy supply management

The energy transition is changing the energy supply chain landscape. Increasingly, decentralised and distributed smaller producers - such as farmers with a wind turbine, small businesses and even consumers with solar panel array - supply electricity, feeding it in to the main electrical grid. A cloud-based blockchain platform offering a distributed, permissioned ledger system can provide an immutable record of transactions communicated between the energy provider and its energy. The platform helps the energy provider to verify and document the transaction values of distributed, flexible energy devices integrated into the electricity grid. Scalable and security-rich, it provides transparency to participants on the blockchain, in line with regulatory requirements.

Identity management

Following the principle of Know Your Customer, banks and private and public organisations are exploring the use of blockchain to validate identities of individuals. This proved useful also in the field of notarization services.

Digital rights and assets management

Blockchain can be used as a proof of ownership and authenticity. This is particularly useful with property assets (e.g. record of land properties) or copyrighted material (music, books, software, artworks).

Fraud and counterfeiting prevention

Blockchain technology allows for the possibilities of tracing a product and its origin and verifying financial transactions, reducing the risks of fraud, counterfeiting and money laundering.

3. Technical challenges

Applications of blockchain remain in the early stages and will require the addressing of multiple challenges in order for their potential to be fully realised. As with many new technologies, it requires incremental investment of capital and resources to assess feasibility and value improvement potential. Currently, over 90% of blockchain initiatives do not make it to a pilot program or a scaled development stage, and those that do take on average 18 to 24 months. The currently fragmented ecosystem with non-standardised platforms contributes to often lengthy integration times with existing networks and systems.

Network adoption and integration constraints

Blockchain's potential to create scaled impact remains constrained by the speed of evolution of the associated ecosystem. Widespread adoption of blockchain will require interoperability and connectivity amongst customised blockchain networks. Adoption can be accelerated by the establishment of industry-wide standards and frameworks. Inter- and intra-industry consortia, such as Hyperledger[4], can help advance cross-industry blockchain technologies, while firms such as R3[5] are enabling advanced cross-industry consortia to cooperate on their common platforms.

Downside of data immutability

Data immutability may represent a limitation when information is accidentally or deliberately entered incorrectly. In some applications, dispute resolution or corrective protocols may be necessary. Companies also need to ensure that effective automated internal controls are in place to cross check and verify the transaction conditions before they are entered or executed on the blockchain.

New forms of vulnerabilities and risks

Although the technology offers high security standards, deficiencies in the software that interface with the blockchain platform may create vulnerabilities that expose company systems to various cyber risks. Effective IT controls will be critical in providing assurance against detecting phishing attacks and other internal and external threats.

Blockchain is theoretically tamper-proof because of two things: cryptographic fingerprint unique to each block and a 'consensus' protocol - the process by which the nodes in the network agree on a shared history. In theory, the retroactive change of a ledger entry is almost impossible.

In practice, it is not as seamless especially in the case of public blockchains operating on a PoW consensus mechanism. Even the best cryptographic tools can be combined in ways that are insecure and attacks such as 'selfish-miner' and 'eclipse' can affect the ledger. Furthermore, no matter how tamper-proof a blockchain is, it does not exist in vacuum and a point of connection into the wider ecosystem might be a point of failure. Moreover, quantum computers are expected to have a dramatic impact on numerous fields due to their anticipated ability to solve classes of mathematical problems much more efficiently than their classical counterparts. This particularly applies to domains involving integer factorization and discrete logarithms, such as public key cryptography. That is to say quantum-computers could break the cryptography that conventional blockchains rely on.

[4] https://www.hyperledger.org/

[5] https://www.r3.com/

Scalability constraints

Scalability is another challenge that blockchain technologies will need to address as the number of transactions they can absorb is dependent on the number of nodes across the network, the size of the block, and the consensus mechanism. However, new methods are being developed to overcome the scalability constraints in current blockchain systems. Adoption of blockchain therefore needs to balance its advantages (such as replacing paper-based processes or sharing of incompatible online directories) with the ability to manage scalability constraints.

Acceptability

As with any new technology, the adoption of blockchain may also be dependent on the ability of organisations to overcome cultural resistance to new initiatives and systems. Overcoming internal resistance to blockchain initiatives may require close attention to effective integration and implementation. Companies and governments can assess the benefits and challenges of adopting blockchain-based technologies through proof-of-concept (PoC) projects, allowing them to explore the applicability and practical potential of private blockchains by decomposing the workflow and focusing on one particular project. This process typically involves creating a prototype or pilot program that tests the theory and contains a preliminary design and architecture of the tested product. Ultimately, companies will need to define the minimum viable ecosystem (MVE) and identify the key features required for the long-term usage of the product and its feasibility. The sustainability and success of DLTs and the associated business models will require building trust, usability, transparency and legitimacy in the medium term.

4. Regulatory challenges

A better understanding of what blockchain is and does, as well as a clear and stable legal framework for its application in Europe are essential for the development and broader adoption of DLTs. When it comes to the legal framework, this would not necessarily require new laws, but guidelines and clarifications so the existing framework is fit for the blockchain era.

No one-size-fits-all

DLT is still at an early stage of development and deployment. Even to this day, the DLT/blockchain and associated applications space is still best characterised as a frontier technology: with clear value but still largely exploratory. Therefore, it is important that any regulatory approach does not implicitly limit or constrain firms' ability to test and develop DLT solutions.

The objective of any policy should be to strike a balance between improving and preserving standards for consumer and investor protection as well as to act as an enabler for the sustainable and streamlined growth of the blockchain ecosystem. Both for its already established industries as well as for emerging areas of economic activity and growth.

The potential uses for DLT are numerous and diverse and its full potential can only be achieved when in conjunction with other technologies (AI, machine learning, etc). Therefore, any regulatory framework needs to be sufficiently cognisant of the variety of potential applications of DLT that are adaptable to operating across multiple activities and services. Consequently, the adoption of a 'one-size-fits-all' regulatory framework for DLT is unlikely to be effective and could even prevent full development and adoption of these technologies.

For financial and general ledger applications, clear regulatory requirements and a well-defined legal infrastructure will help overcome legal and compliance hurdles, which will provide companies and consumers with greater comfort using the technology for trading, financial and other applications. However, in order not to stifle innovation, such regulatory requirements should not be applicable to non-financial services of the blockchain technology, including applications related to supporting numerous live production networks, IoT solutions, automation and critical monitoring capabilities.

Any regulatory framework should treat all current and future industry participants on an equal and fair basis so that, as DLT re-shapes the market, barriers to entry are not created that could negatively impact adoption and innovation. Regulatory coordination is key to avoiding regulatory overlap and contradiction. Activities involving DLT, irrespective of the actor, should have the ability to operate across jurisdictions. New regulatory and supervisory frameworks to address innovation should be fully consistent with existing frameworks in order to mitigate against regulatory arbitrage and conflicting rule sets that stalemate the development of innovative products and services.

Public-private partnership and testing

Regulators and policymakers must have a granular understanding of how DLT technology and its various applications operate in order to correctly assess both the benefits and the associated challenges. Industry participants can and should facilitate these insights into the technology by maintaining an open dialogue and close collaboration with the policymakers and regulators, who should consult with stakeholders, including industry, before proposing any regulation.

Testing should be a complementary part of this dialogue as it provides the opportunity for assessments in a live environment. By virtue of open source, this testing is possible in an open, transparent and accountable fashion. Certain governments are currently evaluating regulatory sandboxes and other testing programmes that create limited production environments with lighter regulatory requirements. If properly structured, these sandboxes can align incentives between regulators and industry - giving regulators insights into the blockchain tech and the industry the ability to test new technologies in a limited live environment without doing a full scale roll out.

Legal status of smart contracts

Similar to the expression in code of a business process or agreement between two or more parties, smart contracts automatically execute agreements when all conditions are met. However, their legal recognition is not obvious since it is unclear if they are different to traditional contracts and have the same legal value.

GDPR compliance

Some provisions of the European privacy protections rules, known as the GDPR, which target the collection and processing of data by centralised systems, may clash with decentralised systems such as blockchains. This is particularly problematic in the area of public, permission-less blockchains as it is very difficult to identify which entity is the data controller, since the participants themselves are not identified. Moreover, due to the immutable nature of blockchains, the rights of a data subject to have their data modified or removed under the GDPR seem impossible to implement in practice. Finally, whilst private and permissioned blockchains generally do not have GDPR compliance issues thanks to various technical means, guidelines and clarifications by data protection authorities would still be very useful (such as the CNIL's report of 2018[6]).

Digital assets and tokens

It is unclear if digital assets are covered by existing regulations, or if new classification is needed. Considering that these assets can be represented by a variety of 'tokens' (payment tokens, utility tokens, security tokens, etc.) which are also used for various purposes (i.e. securities, means of payment, other financial instruments, etc.), a clear set of token categories could be useful. Also, the issue of the taxation of digital assets remains unclear.

Standardisation and interoperability

Even though the technology is still nascent, standardisation efforts will ultimately be needed to facilitate interoperability between blockchains. These standards should be developed through global fora that include industry and all relevant stakeholders to ensure that open standards can be quickly adopted and adapted as technology continues to evolve.

Public sector adoption

The European Commission and the Member States should continue to promote the public-sector adoption of blockchain technologies. There has been excellent progress recently, notably with the European Blockchain Partnership and the future EU Blockchain Services Infrastructure, as well as the inclusion of DLT in the future Digital Europe funding programme. To continue, Member States should invest in pilot projects at either a national level or through international cooperation schemes and encourage public sector agencies to participate in blockchain projects where their oversight or regulatory role is needed. The EU's proposed €100 billion for Horizon Europe (2021-2027) will be another important means to advance related research and innovation in Blockchain.

[6] https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data (retrieved 15 April 2019)

Skills and awareness-raising

There is an evident shortage of skills in the entire blockchain industry, particularly when it comes to designers, developers and engineers. This will require an adaptation in the academic and research area, but there is also a need to educate individuals such as business leaders and investors so they can support, manage and invest in the blockchain economy.

A great effort of general education and de-mystification is needed regarding DLT, and we believe that public institutions have a key role to play in this regard. There are still too many misunderstandings and confusions among industry players and policy-makers, and the blockchain industry could use the EU institutions' support to put an end to various myths: blockchain is not Bitcoin, blockchain is not a money laundering tool, blockchain is not destroying the environment, etc.

International cooperation

Just like the internet, blockchain will be a global phenomenon that will be truly beneficial for society and the economy. Therefore, it is very important that regulators and policy-makers across the world engage in global discussions in order to support the development and adoption of blockchain and avoid legal fragmentation.

Conclusion

Blockchain, and more generally DLT, has attracted significant interest due to its potential to reshape industries, organisational and governance structures and disrupt traditional business models. Its ability to enable a practically permanent and trusted digital record and establish trust in digital transactions offers a huge potential of possible applications. Blockchain is not only diverse but also at its early stages of development. Going forward, the wide spread uptake of blockchain will rely on the ability to meet technical challenges, such as overcoming scalability constraints and addressing potential vulnerabilities, as well as understanding and embracing new models of open innovation powered by open source communities. Furthermore, EU and national policy-makers should encourage continued innovation in this area by creating legal certainty, promoting testing and interoperability as well as fostering talents and public awareness.

Annex - Glossary

Altcoin: An abbreviation of "Bitcoin alternative," describing every single cryptocurrency except for Bitcoin. Altcoins are referred to as Bitcoin alternatives because, at least to some extent, most altcoins hope to either replace or improve upon at least one Bitcoin component.

Bitcoin: A decentralised digital currency that uses a peer-to-peer network of nodes which jointly maintain a common tamper-resistant record of historical transactions independent of a central authority. Bitcoin is the most successful decentralized cryptocurrency to date. It is a decentralised digital currency system, which was introduced by the pseudonymous Satoshi Nakamoto in 2008. It leverages a peer-to-peer distributed network characterised by the lack of a central authority governing the state of transactions. Each consensus participant maintains a list of all historic transactions, grouped together in blocks, in a distributed public ledger called the blockchain.

Blocks are chained together via the hashes of their predecessors, thereby providing strong guarantees for the immutability of the transaction history. Agreement on the current state of the system in the dynamically changing and pseudonymous set of participants is achieved by requiring nodes to solve complex cryptographic puzzles, known as Proof-of-Work (PoW). Consensus participants are known as miners and upon finding a valid solution to the PoW puzzle they are rewarded with new units of the underlying cryptocurrency and fees associated with the transactions included in the respective block.

Bitcoin Mining: Bitcoin mining is the process by which transactions are verified and added to the public ledger, known as the blockchain, and also the means through which new bitcoins are released. Anyone with access to the internet and suitable hardware can participate in mining. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with the transactions compiled in the block as well as newly released bitcoin.

Blockchain: A novel transaction-recording mechanism that comprises batches of validated transactions called blocks which are chained together in a way that ensures a very high level of data integrity

Consensus: the agreement among DLT nodes that a transaction is valid and that there is a consistent set and a guaranteed ordering of the transactions stored in the distributed ledger. The consensus mechanism is the implementation of a collaborative process by the network of nodes in a DLT system through which consensus is achieved. There are many alternative consensus mechanisms in use in different DLT systems.

Cryptoasset: Digital assets that utilise cryptography.

Cryptocurrency: A digital currency that uses cryptography for security.

Cryptocurrency Exchange or digital currency exchange: A business that allows customers to trade cryptocurrenciess or digital currencies for other assets, such as conventional fiat money, or different digital currencies.

Cryptocurrency wallet: stores the public and private keys which can be used to receive or spend the cryptocurrency. A wallet can contain multiple public and private key pairs.

Cryptoeconomics: The design of the economic incentives within a system that uses cryptography.

Cryptotoken/token: Value exchange mechanisms that allow a community, or network's participants, to access, govern and manage the system.

Decentralized applications (dApps): Applications that run on a P2P network of computers rather than a single computer. They are a type of software program designed to exist on the Internet in a way that is not controlled by any single entity.

Distributed Ledger (Technology): An immutable database that is governed by a predetermined set of rules, consensually shared and synchronised through a network spread across multiple sites, institutions or geographies.

- **Public and permission-less** DLTs are systems where an open set of participants are allowed to submit transactions to the ledger as well as validate them.
- **Public and permissioned** DLTs only allow an authorised set of participants to be validators and hence require permission to become a node; however, all transactions are publicly viewable.
- **Private and permissioned** DLTs are more appropriate for the enterprise context, as well as highly controlled and regulated environments where all participants need to be known.

Ethereum: A decentralised software platform (with an associated cryptocurrency called Ether) that enables the deployment of smart contracts and Decentralised Applications (dApps) with a wide range of applications

Fork: A divergence in the state of a blockchain caused by a disagreement amongst blockchain nodes. Can be temporary (e.g. a fork due to two miners finding competing blocks at nearly the same time) or permanent (e.g. a fork due to a subset of nodes introducing new rules for the validation of transactions).

Game Theory: The study of multi-person decision problems and resulting outcomes taking into account strategic interaction among participants given a set of rules.

Hash: A function that converts an input of letters and numbers into an encrypted output of a fixed length. A hash is created using an algorithm and is essential to blockchain management in cryptocurrency.

Hyperledger: An open source collaborative effort created to advance cross-industry blockchain technologies. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, Internet of Things, supply chains, manufacturing and technology.

ICO: a special type of crowdfunding campaign allowing entrepreneurs to raise capital by selling blockchain tokens, thus giving investors a stake in the protocol, platform or service being built. To put it simply, an ICO is a fundraising tool that trades future cryptocoins in exchange for cryptocurrencies of immediate, liquid value.

Miner: Special blockchain nodes that build up a block of transactions they wish to publish byselecting groups of ordered transactions.

Node: A computer running blockchain software that is connected to a network and maintains a copy of a blockchain. So-called "full" nodes validate all incoming blocks and transactions. "Lightweight" nodes trust other nodes to do this on their behalf.

Open Source Software: Open source licenses prevent restrictions on the use of software thanks to the four freedoms to run, study/modify, distribute copies and modified versions (https://www.gnu.org/philosophy/free-sw.en.html). There are currently approximately 70+ different licenses recognised by the Open Source Initiative (https://opensource.org/osd-annotated) which provide legal certainty to a community of 15+ million developers.

Permissioned blockchain: A blockchain which requires users to have a known identity and where users must be authenticated and authorised to use the system. Permissioned blockchains are usually private. On permissioned blockchains, participants are typically allowed to view only the transactions relevant to them.

Permissionless blockchain: A blockchain that is open to any participant without requiring authentication and authorisation and transactions are verified against the pre-existing rules of the network. Any participant can view transactions on the ledger, even if participants are anonymous.

Public-key cryptography or asymmetric cryptography: A cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. This accomplishes two functions: authentication, where the public key verifies that a holder of the paired private key sent the message, and encryption, where only the paired private key holder can decrypt the message encrypted with the public key.

Ripple: A real-time gross settlement system, currency and remittance network. Also called the XRP Ledger, Ripple is built upon a distributed open source internet protocol, consensus ledger and the decentralized native cryptocurrencyy known as XRP. At its core, Ripple is based around a shared public ledger, which uses a consensus process that allows for payments, exchanges and remittance in a distributed process.

R3: an enterprise blockchain software firm working with a broad ecosystem of more than 200 members and partners across multiple industries from both the private and public sectors to develop on Corda , an open source blockchain platform, and Corda Enterprise, a commercial version for enterprise usage.

Smart Contract: a distributed application running on and delivered along with the distributed ledger. Smart contracts execute in a secure environment within any node in the DLT system, when a user sends a transaction of a particular type to the DLT system.