Distributed Ledger Technology, Blockchains and Identity

A Regulatory Overview

September 2018

Contents

1. Purpose of this paper

This paper provides an overview of the relevant regulations for the use of distributed ledger technologies (DLT) and blockchains for digital identity. Digital identity is the basis for nearly all digital businesses and a key enabler for social, economic and financial development. After reviewing the agenda set by governments and regulators worldwide on the use of DLT for digital transformation, this paper analyses the implications for the identity marketplace and, in particular, for mobile network operators.

The paper is based on research and structured interviews with a diverse mix of experts in DLT and blockchain technologies, including technologists, developers, regulators, lawyers and general experts in the blockchain and identity field. The interviews focused on the high-level considerations on how to encourage the technical and legal interoperability of DLT and blockchain solutions in identity under existing regulatory frameworks.

Within this document, certain technologies and solutions are described as examples of the application of distributed ledgers both for identity and other purposes relevant to mobile operators. This should not be considered a recommendation or endorsement of those solutions nor a comprehensive assessment of all solutions that are offered. Readers are encouraged to independently research those and other solutions.

2. Introduction

Distributed ledger technology and blockchains hold great promise for creating a decentralised digital identity ecosystem.

The decentralised nature of distributed ledgers and blockchains can give people more proactive control over their data and make it more difficult for unauthorised users to exploit it. Across the world, enterprises, financial services, technology, and government organisations are using blockchain and DLT technology for identity management systems, experimenting with a broad variety of use cases ranging from authentication and identity verification for individual and legal entities, to secure access to online services, such as banking, medical prescriptions, e-voting and other services that require the integrity of records and services.

This section is an overview of blockchain and DLT technology. It provides a description of their technical characteristics that are relevant to identity, in the broader context of applications and use cases that enable individuals to control access to personal records and to know who has accessed them.

While produced by the GSMA, following close dialogue with a number of its members and experts, this report is independent in that it does not necessarily represent the views of the association or its members. It was produced as a contribution to an important public debate and the GSMA does not accept responsibility for any other use.

2.1 Technology overview: a taxonomy

A blockchain is a linear form of a distributed ledger composed of immutable blocks of data, each block containing a list of transactions and a unique reference to its predecessor block. Strong cryptographic techniques are employed to maintain integrity between each block and its predecessor. This allows blockchains to be shared and corroborated by anyone with the appropriate permissions. Blockchain may also be referred to as a distributed ledger, which is also commonly considered to be a specialised form of a distributed database.

Distributed ledgers are a multi-purpose technology in the digital world that are specifically designed to be shared across a network of multiple sites, geographies or institutions. Records are stored in a ledger that continues to grow. Often, as in the case of the Bitcoin blockchain, the underlying assumption is that the nodes forming the network are not implicitly trusted, i.e. they need mechanisms in place by which all parties in the system can reach a consensus on what the status of the ledger is.

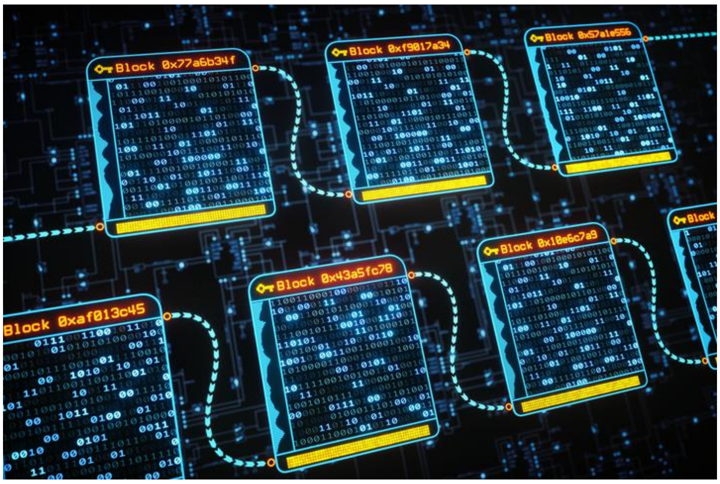
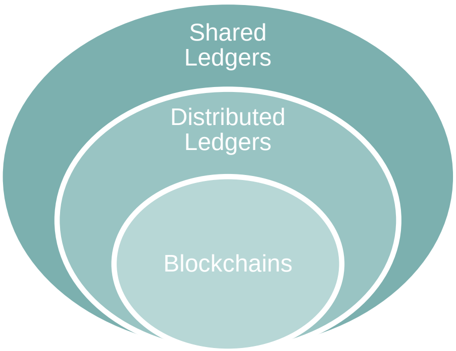


Figure 1: Blockchain as a decentralised database[1]



In shared ledgers the network also includes multiple nodes, which collaborate to maintain a consistent state of records between nodes. However, the ledger entries are not necessarily shared across all nodes, only those that wish to share data and where there is usually a mutual trust between database-node owners. This means that shared ledgers are generally operated by an industry, a private consortium or may also be open to the public in a trusted environment. The assumption here is that the computational power of the network is held by honest nodes, which only build on records that are valid.

Distributed ledgers are based on an adversarial threat model that anticipates and mitigates the presence of malicious (i.e. dishonest) nodes in the network. A well-known implementation is based on the so-called Byzantine fault-tolerant solution, meaning that the ledger should be able to synchronise and run even if a certain number of nodes are acting maliciously. Unlike traditional distributed databases, individual nodes do not trust their peer nodes by default and thus need to be able to verify and validate transactions that update the actual state of records. The assets recorded and shared on the ledger could represent transactions, contracts, or practically anything else that can be described in digital form.

Blockchains are distributed ledgers, with additional characteristics that make them distinctive. Key blockchain characteristics are:

1. **Cryptography**: a wide variety of cryptographic functions are used, including hashing algorithms
2. **Peer to peer**: consist of a peer to peer discovery and synchronisation mechanism
3. **Consensus**: algorithms that determine the sequence and validity of transactions[2]
4. **Ledger**: list of transactions that are bundled together in cryptographically linked blocks
5. **Validity rules**: the network rule set determines what transactions are considered valid and how the ledger gets updated, etc.
6. **Crypto economics**: a combination of cryptography and economics (game theory) that makes sure all actors in a decentralised system are incentivised to remain honest

Participants in a blockchain ecosystem typically include nodes and miners, developers and application operators, and users that interact with the blockchain by means of wallets. The data storage points, the nodes, are highly interconnected and data is synchronised across the network nodes using validation rules and a consensus process to ensure that what is stored is correct and agreed across the network.

The security and accuracy of the assets stored and recorded in the ledger are maintained cryptographically through encryption and the use of 'keys' and signatures to control who can

[1] Source GSMA White Paper on Blockchain – operator opportunities, 2018

[2] The technical details of how to achieve consensus vary from "proof-of work concept" whereby the nodes all try to solve the mathematical problem, but it is the first node to solve the problem that gets compensated, (and other users use the solution provided by the first node to verify the problem has been correctly solved) to "proof-of stake" whereby the user with the largest stake is nominated to confirm the transaction.

do what within the shared ledger. The blocks of transactions and data contain accurate timestamps that are chronologically chained together through virtual distributed networks (a blockchain).

Typically data on a blockchain is in plain text, though this can be very obscure information, such as a wallet address, that is exceedingly difficult to identify back to an individual. Additional data can be incorporated into the transaction record and this can be encrypted or hashed before it is recorded to the blockchain (this is the recommended approach to protect data "on-chain", though "off-chain" methods support more resilient approaches). In both cases, there are fundamentally two types of data:[3]

i) the header, which includes the timestamp, the hash of the previous block in the chain, and the hash calculated from the transactional data which forms the block content, and
ii) the block content, the individual transactional data which has been collated (from requesting users) to form the records making up the block.

There is a broad spectrum of distributed ledger models, with different degrees of centralisation and different types of access control, to suit different business needs. Typically, there are agreed rules that determine if one, some or all of the participants in the network can make entries to the ledger. Blockchain types can be categorised in different permission models, as shown in Figure 2.

Figure 2: Types of blockchain – GSMA

		Read	**Write**	**Commit**	**Examples**
Open	***Public permission-less***	Open to anyone	Anyone	Anyone	Open ecosystems, e.g. Bitcoin, Ethereum
	Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Open ecosystems, e.g.. Ripple, Sovrin
Closed	***Consortium***	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple companies within or across sectors Hyperledger or Corda
	Private permissioned (‘enterprise’)	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal enterprise solutions within industries Ripple

[3] Source: Michèle Finck: Blockchains and Data Protection in the EU

3. Blockchains: in need of regulation?

The evolution of blockchains and DLT has been compared to the early development of the internet with potential to disrupt multiple industries and public sector services and become a key component of the digital economy and society in the near future.

From a regulatory perspective, the use of blockchain technologies does not live in a legal vacuum, as many current legislative frameworks may be applicable to the implementation of such technologies, depending on their application environment (e.g. Bitcoin, new kinds of cryptocurrency or general use of a blockchain for accountability and traceability purposes). Much regulatory interest has so far focused on Bitcoin, crypto-currencies, and protecting citizens against risks including bad actors in related nascent business areas, such as cryptocurrency exchanges and initial coin offerings. **However, block-chain based cryptocurrencies and Initial Coin Offerings (ICOs) are specialized use cases that should be treated and regulated differently from blockchain technology itself. Conflating these use cases with the technology has led to a lack of understanding of how existing legislation and safeguard measures apply to this new and disruptive technology, potentially threatening the deployment of blockchains, according to some experts**.

The need for trust, interoperability and accountability in digitalised economies are potentially the most important driving forces behind the use of DLT and blockchain technologies.

For example, in the United Kingdom, Sir Mar Walport's report on DLT recommended that: "*Regulation will need to evolve in parallel with the development of new implementations and applications of the technology. As part of the consideration of regulation, government should also consider how regulatory goals could be achieved using technical code as well as legal code*"[4].

Many institutions and authorities, however, have expressed a fear of stifling innovation, and favour an approach of precautionary monitoring and experimentation, rather than pre-emptive regulation; e.g. in Japan the Financial Services Agency (FSA) announced a "FinTech Proof-of-Concept (PoC) Hub" designed to make it possible for financial technology companies, financial institutions, and others to evaluate issues in the areas of compliance, supervisory response risks, and the interpretation of legislation, etc. In the UK, the Financial Conduct Authority (FCA) has set up a regulatory sandbox to provide innovative initiatives with a safe space to develop without worrying about regulatory constraints. Across the world, more than 25 governments are actively running blockchain pilots supported by start-ups.[5]

In some countries, a licensing framework approach for blockchains has also started to emerge, in particular, for cryptocurrency application environments. For example, the State of New York in the US is offering "BitLicense", which allows business to conduct virtual currency activities on DLT infrastructure. There are also initiatives aimed at actively facilitating the technology via legislation aimed at accepting or promoting the use of blockchains.[6]

[4] Source: Recommendation 4, Distributed Ledger Technologies: beyond blockchain. Government Office for Science, 2016

[5] McKinsey Article, June 2018. Blockchain beyond the hype: What is the strategic business value?

[6] In 2017, at least eight U.S. States have worked on bills accepting or promoting the use of Bitcoin and blockchain technology, while a couple of them have already passed them into law. In Europe, the Financial Services DLT Regulations by Her Majesty's Government of Gibraltar became effective as of 1st January 2018. In Malta legislation on DLT is due to be approved by Parliament legislation in July.

The European Union Blockchain Observatory and Forum

In the EU, the European Parliament's initial report in 2016 concluded that blockchain technology could deliver a "revolution in the security and transparency that is needed to enable e-voting." Interestingly, the European Commission has stated that the almost limitless list of potential use cases of DLT makes it both very promising and challenging, and has expressed its support for blockchains and DLT.

In February 2018, the Commission launched the EU Blockchain Observatory and Forum that aims to highlight key developments of blockchain technology, promote European actors and reinforce European engagement with multiple stakeholders involved in blockchain activities.

In April 2018, 22 countries from the EU signed a Declaration on the establishment of a European Blockchain Partnership as a vehicle for cooperation amongst Member States to exchange experience and expertise in technical and regulatory fields and prepare for the launch of EU-wide blockchain applications across the Digital Single Market for the benefit of the public and private sectors.

Overwhelmingly experts interviewed, and many European institutions, are of the opinion that DLT and blockchains are an implementation choice and specific legislation and regulations are not needed. Certainly, outside of the remit of financial applications, blockchains, and distributed ledgers more generally, are regarded as a net positive development rather than a threat to the position of major financial players and even official currencies themselves. **At this stage, it seems there is need for more innovation, research, development, piloting and proof of concepts, unencumbered by specific additional legislation and regulation.** Some experts feel that existing data protection law and guidelines (such as the EU General Data Protection Regulation, the APEC Cross-border Privacy Rules, and the OECD Privacy Principles) can be applied to distributed ledger developments to create a 'best practice' environment for the design and deployment of the ledger itself, and perhaps more importantly the applications that use the services offered by the distributed ledger. See the Annex for more information on key government-driven initiatives on blockchains.

4. Blockchains and Identity: benefits, opportunities and regulatory risks

Many experts consider the use of blockchains in identity as a key potential application, as this technology can add traceability and digital accountability in a large variety of use cases (e.g. in the supply chain industry).

Blockchains could empower multiple organisations to work together across sectors as this technology can manage effectively a high number of unique identifiers that may relate to persons, things, devices and mobile handsets.[7]

Having conducted a 12-month study engaging industry leaders and subject matters experts globally, the World Economic Forum has defined DLT as holding key features for identity systems, in particular for financial services applications.[8]

The ethical and social implications of different potential uses of this technology in identity need to be considered. One notable pilot was launched by the UN World Food Programme (WFP) in May 2017 at the Azraq Refugee Camp in Jordan. Through the use of Blockchain technology, WFP creates virtual accounts for refugees and uploads monthly entitlements that can be spent in the camp's supermarket by authentication via iris scan.[9]

The opportunities for mobile operators to use blockchains for identity, authentication and authorisation are also starting to emerge rapidly. Mobile Connect solutions[10], available worldwide, can evolve into a distributed framework able to use the secure environment provided by mobile technologies to perform core authoritative functions, such as legal signature, cryptography and data minimisation techniques, such as zero-knowledge proof mechanisms.

The GSMA's Identity Programme is investigating how to use blockchains to make the existing Mobile Connect federated identity solution more convenient for users via a blockchain.[11] The following sections provide an overview of some of the potential benefits and related regulatory risk areas for the use of blockchains in identity that may need to be considered by mobile operators and other industry players when designing and deploying these solutions.

[7] Source: "Distributed Ledger Technologies for Public Good: leadership, collaboration and Innovation"

[8] Source: The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

[9] Source: Blockchain for Development: Emerging opportunities for mobile, identity and aid www.gsma.com/mobilefordevelopment/programme/digital-identity/blockchain-development-emerging-opportunities-mobile-identity-aid/

[10] Mobile Connect is a digital identity initiative from GSMA and implemented by Mobile Operators around the world. Mobile Connect utilises the mobile number as the identifier for the user in the digital world and the mobile device, SIM and the network as the authentication mechanism to deliver the portfolio of digital identity services like authorisation, identity and networks attributes assertion and sharing keeping the user in complete control and using privacy by design principles For more information on Mobile Connect please see https://www.gsma.com/identity/mobile-connect

[11] A brief overview on the use of blockchain for Mobile Connect is available here https://www.gsma.com/identity/the-relationship-between-blockchain-and-digital-identity

4.1 Identity and KYC

The ability to validate the real identity of a legal person or an entity is a valuable asset for many electronic transactions and a fundamental driver for trust in the digital environment. In a recent study, consultancy McKinsey estimated that the addressable market for identity verification will be worth between US$16 billion and US$20 billion by 2022.[12]

Clearer policy discussions around DLT and its use for digital identity and verification of identities are now on the way globally, driven in part by more stringent know your customer (KYC) regulations that require more efficient use of KYC procedures through the use of legally-compliant attributes and identifiers to reduce risk and protect the public from money laundering, fraud and other challenges.

More broadly, there is a worldwide consensus among governments and regulators alike that technologies that can deliver robust and convenient identity solutions are a key enabler for digital trust. However, the robustness of such solutions is highly dependent on the level of (systemic) interoperability amongst participant organisations in the identity value chain and on the quality of data and information within those systems. Distributed ledgers provide a significant advantage in systemic interoperability across the technology ecosystem.[13]

Automatically collected and processed data for KYC purposes (e.g. name, address, date of birth, nationality and occupation) is increasingly circulated and commoditised and therefore subject to exponential fraud. Oftentimes, digital identities are verified through the use of different identifiers held by a variety of intermediaries, including private companies and governmental institutions. Any of these intermediaries could be, and increasingly are, hacked, revealing or exploiting users' personal information.

Hence, the protection of personal data and privacy of individuals has become crucial. Privacy-enhancing technologies are rapidly emerging, as common rules for privacy across continents aim to empower users and bring value to both individuals and businesses.

4.1.1 What are the inherent characteristics of DLT that could make this technology particularly useful for identity?

DLT can help with the process of customer identity verification by using asymmetric cryptography, and making it simple to verify that transactions can be specifically attributed to the correct individual, or entity, who has generated a transaction.

Asymmetric cryptography: DLT technology employs asymmetric cryptography using private and public keys to sign transactions. Only the owner of a private key can generate a transaction address, which can then be validated by the network using the associated public key. This approach is a way to prove that somebody is who they say they are and that all transactions are made only by the rightful owner, hence facilitating an owner-centric approach to the use of data or services with control of personal data passing back to the individuals.

Every user has one or more pair of keys. A public key that is shared with other users to enable transactions, as well as a private key known only to the user, which is never shared with other users. The private key enables an authentication of the user as the true 'owner' of the public

[12] Fuel by McKinsey June 2018. https://fuelbymckinsey.com/home/article/the-next-20-billion-digital-market-id-verification-as-a-service

[13] Distributed Ledger Technologies: beyond blockchain. Government Office for Science, 2016.

key on the basis of an encrypted algorithm that checks if the two keys are truly mathematically linked.

Blockchain implementations also typically support the capability of generating 'addresses' (which are large 'random' numeric values) derived from the private/public key pair and can prevent the linking of multiple transactions belonging to a single user because each transaction can have its own address.

Hashing codes (as "digital fingerprint") can be used to spot changes in data (e.g. a document or programme). Hashing is used in blockchain technology to connect blocks by including a hash value of the previous block to the current block. This guarantees that the confirmed transactions in the ledger cannot be tampered with; any change to the contents of a block invalidates the hash of that block, which in turn invalidates the hash of the next block, and so on.

Time-stamping and consensus: The transaction-records, or blocks, in a blockchain are linked together cryptographically, rendering them virtually tamper-proof. Unlike records in standard relational databases, which are typically alterable, once a transaction is recorded and time-stamped within a confirmed block on the blockchain, it is virtually impossible to alter it, or delete it.

The blockchain records the fact of the transaction, that is, what has been transferred, the parties (or rather the addresses of the parties) involved, as well as structured information (metadata) related to the transaction along with a cryptographic hash of the transaction content for the whole block. This unique signature is used to verify transactions later: If someone alters the transaction content, its resulting unique code no longer matches the version that is on the chain, and any software which inspects the blockchain can identify the discrepancy.

As mentioned, there is typically a consensus process implemented by the network nodes that support the ledger. The consensus process is responsible for making sure the 'global' network has a consistent view of the committed ledger. Thus, the completion of a transaction is dependent on the consensus being reached between network nodes. As soon as one party agrees to send the asset, and the other party agrees to receive the asset, and consensus is obtained across the network of nodes verifying that each party has the capacity to conduct the transaction, then the transaction is completed.

4.1.2 What are the regulatory risk areas with the use of blockchains in identity?

In generic terms, blockchains allow access to a broad set of data by industry players, governments and individuals, where the processing and control procedures and responsibility for accessing such data is predefined. Existing laws and guidelines are, therefore, typically applicable, including for example regulations on cybersecurity, such as the EU's Networks and Information Systems (known as the NIS Directive), internet-related laws, and international privacy and data protection regulations, such as the EU General Data Protection Regulation (GDPR)[14], the APEC Cross-border Privacy Rules[15], and the OECD Privacy Principles[16], as well as broader laws that protect consumers against the risks of misuse of customer data, corporate negligence and other criminal offences.

Many commentators have argued that DLT and blockchains are ushering in a new phase for digital identity offering significant process efficiencies and controls to the end user. With blockchain-enabled digital identity solutions, the aim is to achieve an environment of self-assurance in the way individuals represent and reveal themselves online, and support decentralisation of identity assurance.

However, for some higher risk use cases, a trusted external authority may also be required to validate the claims or assertions.[17] In these implementations, third parties do not provide the identity information per se, but rather act as verifiers of the claims or identity attributes asserted by the user.

This latter case is more complex than the original blockchain public implementations, which did not support external validation of claims or off-chain authorities. It can be achieved in models with one or more third parties providing authoritative or corroborative sources of the claimed identity: the collection of receipts or verifiable credentials is dependent on the level of assurance required by the service provider in a given transaction, similar to federated identity management models. Service providers, could, therefore, request a certain level of trustworthiness by gaining assurance over appropriate documents corresponding to the required level of assurance, e.g. confirmed by a designated public authority or other entity in the relevant country/region, for high level of assurance.

[14] General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG

[15] http://www.cbprs.org/

[16] http://oecdprivacy.org/

[17] Source: Do Blockchains Have Anything to Offer Identity? Steve Olshansky and Steve Wilson, (2018) https://www.internetsociety.org/resources/doc/2018/blockchain-identity/

The EU’s new Fifth Anti-Money Laundering Directive (“AMLD5”)

The new Fifth Anti-Money Laundering Directive (“AMLD5”), which amends the Fourth Anti-Money Laundering Directive, was published in the Official Journal of the EU on 19 June 2018. AMDL5, which must be transposed by Member States by 10 January 2020, addresses, for the first time, the potential money laundering and terrorist financing risks posed by virtual currencies due to their ability to potentially (1) allow transacting parties to remain anonymous; and (2) act at cross-border jurisdictional level.

Hence, the AMLD5 has not only expanded its scope to virtual currency exchange platforms and wallet providers (including obligations to register with national anti-money laundering authorities, implement customer due diligence controls, regularly monitor virtual currency transactions, and report suspicious activity to government entities), but also requests that Member States create central databases comprised of virtual currency users’ identities and wallet addresses, as well as self-declaration forms submitted by virtual currency users.

While identities and their data will not be on the blockchain, this creates an opportunity for efficiencies and cost savings as more exchanges and wallets will be required to have the ability to validate a claimed identity against an authoritative source or register without necessarily performing a full KYC in the first place, e.g. a registered wallet is required to know that the owner of that wallet has already gone through a full KYC process and that identity is known to another party should a legal recourse occur.

Some researchers believe an enforceable governance model for the identity lifecycle management and its public and private keys, including issuance, revocation and recovery of identities, is necessary for DLT and blockchain solutions. A governance structure, and a self-regulated trust framework for implementations, for example, could help to comply with existing legislation designed to protect users and industry participants against several risks, such as:

- The legal value and reliability regarding the provenance of attributes and keys.
- The risk of anonymity of the participants to the ledger. For example, when non-repudiation is a requirement, a consensus model with anonymous node participants may add significant legal risks, as parties will need to be able to know who is liable for how the record was written to the chain in case of disputes.
- The risks of harms and losses caused by the failure of DLT, including data breaches, hacking and lack of contract delivery.
- The risks of compromise to privacy for individuals and legal entities.
- Other areas of risks and liabilities stemming from other jurisdictions.
- Or other risks driven by the application environment and use case. For example, will the application environment require portability of data and identity?

4.1.3 Examples of blockchain initiatives for identity

There are primarily two approaches to identity:

- Top-down – where the government acts as a trust anchor by providing access to government registers and databases, which provide a high assurance framework based on privacy enhancing technologies, e.g. mobile passport, mobile driving license, where data can be re-used for different purposes either for consumers, citizens or B2B.

- Bottom up model – user has a credential and consumes attestation from sources that can be either authoritative or corroborative.

In Europe, for example, the use of **ISÆN as a data provider framework towards National and European Digital ID** aims to facilitate KYC for individuals. This project focused on a self-sovereign identifier which offers individuals, also known as data subjects, the possibility to sign and mark their stream of data, for example, by using hashing and data watermarking technologies. It is proposed to call this identifier system the *ISÆN: Individual perSonal data Auditable addrEss Number*. Individuals could generate themselves an ISÆN, allowing them to retrieve information about the exact localisation and use of their data.[18]

The work of **W3C**[19] has also specified decentralised identity systems in a peer-to-peer distributed network that provide means for managing a root of trust with neither centralised authority nor a single point of failure. Such systems rely on decentralised identifiers data (DIDs) as a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralised registry, identity provider, or certificate authority.

In a business-to-business (B2B) environment, the work on international standards for the identification of legal entities in the United Kingdom, known as the **Register of Legal Organizations (ROLO)**, is also gaining some traction, and several nations, including the US, are already considering adapting the ROLO specification to meet their needs.[20]

There are also many start-ups and private companies that are pioneering the use of blockchain technologies for KYC and AML, such as **Civic App**[21], a U.S.-based identity verification (IDV) and management start-up founded in 2016 offering the Civic Secure Identity Platform (SIP) on a mobile application that stores personal data and can leverage the encryption and biometrics features of smartphones and tablets. Civic App allows users to share and manage their fully verified identity data.

Another start-up, **Evernym**[22], is offering SaaS services and applications built on the Sovrin[23] Network, an attribute-based global identity network for self-sovereign identity.

The **Open Identity Exchange foundation (OIX)** is also seeking ways to use generic distributed ledger platforms, such as Ethereum, with smart contracts to implement identity solutions.[24]

It is also feasible to create identity services based on 'vanilla' open source distributed ledger platforms, such as **Hyperledger Fabric**[25], benefiting from features, such as permissioning and smart contracts.

[18] www.cen.eu/work/areas/ICT/Pages/WS-IS%C3%86N.aspx

[19] For more information see https://w3c-ccg.github.io/did-spec/

[20] https://bbfa.info

[21] www.civic.com

[22] www.evernym.com

[23] www.sovrin.org

[24] http://www.openidentityexchange.org/distributed-ledger-foundation/

[25] https://www.hyperledger.org/projects

4.2 Data protection and privacy

Privacy, transparency and user control are often cited as critical reasons for the adoption of DLT and blockchains, as this technology can give data subjects more control over their personal data. Given their decentralised nature, blockchains potentially offer individuals greater sovereignty over their data and allow them to manage and own their data on a shared ledger. This is an important shift from the existing centralised data models - the basis for the core privacy principles underpinning long-standing data protection law, such as the EU data protection directive 95/46EC, and the EU's new General Data Protection Regulation (GDPR) [26].

Blockchains' decentralised trust mechanisms and record keeping functions can operate without the need for intermediaries. From a privacy and data protection viewpoint, there are some important characteristics of a blockchain:

- **Transparency**. Every participant in the network can verify the correctness of every transaction. This provides substantial protections to organisations and individuals against identity fraud.
- **Immutability and integrity**. A blockchain records immutable blocks of data that are impossible for any user to amend, delete or duplicate without noticeably affecting subsequent entries in the chain, making fraudulent activity (for example) immediately visible to the other users of the ledger. This helps guarantee the integrity of the data stored on the blockchain, and provides participant nodes with an effective mechanism to ensure that every record is authentic and unchanged.
- **Resilience**. Blockchains' resilience stem from their structure, since they are designed to work via a distributed network of nodes in which each one of these nodes usually stores a copy of the entire verified chain. Hence, when a transaction is verified and consensus obtained by the participating nodes, it is virtually impossible for someone to change or alter the transaction's data. Attempts to change data in one location will be interpreted as fraudulent and an attack on integrity by other participants, with the result that the change will be rejected. In some instances, however, so called 51% hash rate attacks in proof-of work blockchain attacks are not just theoretically possible, but have been achieved against some smaller blockchains.

While there are certain technical characteristics that allow DLT and blockchains to meet certain privacy and data protection regulatory requirements, this is not to say that DLT and blockchains implicitly support greater data control and sovereignty. It is important to recognise that DLTs are broadly a technology infrastructure to be used by applications and that there remains an obligation on applications to employ best practices in their use of DLTs to protect the personal data of end users. Of course, we can expect to see implementations of DLTs that are designed for identity and privacy, which should encourage better practices amongst users and applications.

Experts have highlighted the following grey zones and risk areas, when implementing DLT and blockchain technologies for identity:

- Data processing, storage and data localisation
- Legal responsibility, data processors and data controllers
- Confidentiality of data and the applicability and management of user's rights

Considerations and implications for stakeholders: To address these issues for each particular use of the technology, government and private sector users, as appropriate, should

[26] https://www.eugdpr.org/

conduct a bespoke risk assessment to identify the relevant threats to privacy and data protection when using blockchain implementations.

Additionally, standards for the integrity, security and privacy of distributed ledgers and their contents should be considered and reflected in both regulatory and software policy code (see for example **ISO/TC307**).[27]

While the specific applicability of generally accepted privacy principles, such as those set out in the GDPR, the APEC Privacy Framework, Council of Europe Convention 108+[28], the OECD Privacy Guidelines and principles, and the GSMA's Mobile Privacy Principles[29], to blockchains and DLT will need to be considered, those principles are designed to adapt over time. Rather than developing completely new regulation, policymakers should therefore first consider how data privacy principles apply to blockchains and DLT.

4.2.1 Data processing, storage and data localisation

Data processing, retention and storage are important considerations when defining the scope of regulation that is applicable to blockchains. A key question to address is, therefore, whether blockchain implementations require storing personal data on the ledger. The ledger in itself is a store, which isn't literally 'processing' personal data. However, if a user requests storage of personal data as part of a transaction, then that, of course, gets stored in the ledger subject to its consensus rules.

It is, therefore, important to ensure applications are not storing sensitive personal data directly onto a ledger that is accessible by parties the user does not wish to reveal such data to. This issue can be addressed by storing only such information that can confirm identity/personal data on the ledger, but securing that personal data elsewhere.

Depending on the use case, information on the ledger may be data related to an identified or identifiable natural person and, as such constitute personal data, which is in scope of privacy and data protection regulations.

[27] www.iso.org/committee/6266604.html
[28] https://www.coe.int/en/web/data-protection/-/modernisation-of-convention-108
[29]For more info please visit https://www.gsma.com/publicpolicy/mobile-privacy-principles

Best practice in blockchain design and implementations suggests that blockchain solutions that offer personal data stored off-chain can deliver enhanced data management focused on privacy. Care should be taken, however, as data stored off the chain could still become unavailable or subject to data leaks or data mining techniques to try to identify the users. [30]

In the blockchain, it can be difficult to identify what personal data is. In some blockchain implementations personal data may include:

- identifiers that may be present in blockchain header data
- transaction data and data contained in the notes field
- data that is 'hashed' and recorded as content on a 'block' (and that may be considered 'pseudonymised data' under the privacy regulations, such as the EU GDPR, but that remains personal data)
- encrypted data – which may constitute personal data

Indeed, according to the GDPR and the Article 29 Working Group, encrypted and hashed data is pseudonymous, therefore may be considered as personal data, while anonymous data is not recognised as personal data. See Recital 16 in **text box**.

Recital 16, Article 29 Working Group

"*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*". (GDPR Recital 26)

However some considerations should apply; encrypted data is only personal data to the extent that someone has a key to unencrypt it. In the hands of someone who does not have, and is unlikely ever to obtain the key, it could theoretically be personal data, but encryption at least mitigates the risk to close to zero/substantially.

If data is truly anonymous, and individuals cannot be re-identified then indeed privacy laws will generally not apply. Personal data that has been pseudonymised should still be treated as personal data, but pseudonymisation can act as an effective safeguard to reduce risk, particularly if other participants or third parties are highly unlikely to be able to re-identify the subjects.

Therefore, blockchain technologies that allow effective management of personal data are important to minimise the risks to privacy to data subjects and are currently considered as best practice implementations.

Techniques which combine off-chain storage and data linked through hash pointers could also, for example, reduce the privacy risks of blockchain because from a legal standpoint personal data is stored in a database under the control of an identifiable data controller, hence compliance with GDPR is much easier. [31]

A critical issue to address is the management of public keys and whether they constitute personal data. Public keys are fundamental for DLT and blockchains to function and arguably,

[30] "It is not currently advisable to store non-transactional data on a blockchain. If this is required for a specific use case, it is not advisable to use a blockchain. If, however, the trust in question is related to transaction records (rather than the underlying data itself), then a blockchain may be applicable. In all cases, any private information or any data that may be in conflict with local and global data-protection regulations, such as GDPR, should not be stored on the blockchain." Source: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf

[31] Source: On Blockchain and the General Data Protection Regulation, 2018

if combined with the release of other information (on KYC for example), cannot qualify as anonymous data.

According to the recent report published by the Bundesblock Privacy Working Group in Germany[32] a public key does not constitute personal data in these cases:

(1) the key does not belong to a natural person or is not created on behalf of a natural person; or
(2) the key cannot be linked to a data subject by reasonable means and is therefore truly anonymous.

Another key issue is the cross-systemic linking of data where storing data off the ledger may not be sufficient. An important question is how to preserve the privacy of transactors. This is addressed in the work of DID systems, which enable an identity owner to have as many public keys (in DIDs) as the number of relationships it has. In blockchain implementations there is also typically the facility to generate 'one time use' addresses that can be used for specific transactions. This prevents cross-linking using just one or a small number of identifiers. This is called "pairwise identifiers" because each one is paired with the identifier of the other party in the relationship.

Data localisation restrictions may also have an impact on the design of blockchain and its applicable legislative framework. For example, if the ledger is replicated to all nodes, and it is open to everyone regardless of location, then any personal data stored on a blockchain belonging to one jurisdiction may be stored in another jurisdiction and become subject to data law enforcement authorities in that jurisdiction.

In the EU, for example, it is prohibited to allow cross-border data flows, if the other jurisdiction does not have a similar level of protection of personal data. While it might be safer to store data in a hashed form to allow for integrity checks, thought needs to be given to the risk of attacks against hashes of simple data (such as name, email address or mobile number) as feasibly this could be attacked given sufficient computing power now or in the future. Hence the advice again is not to store personal data in the ledger and allow for compliance of global solutions.

4.2.2 Legal responsibility, data processors and data controllers

An important aspect of data protection laws is they impose obligations on 'data controllers' to comply with key rules to ensure personal data are:

- processed in a transparent and fair manner (e.g. within the reasonable expectations of individuals);
- processed lawfully (e.g. on a legal basis set out in data protection law, such as *necessary* for the performance of a contract or with a person's consent);
- processed in a manner that considers the risks to individuals and that meets a number of rights (such as a right to erase or correct data or to obtain a copy of personal data); and
- processed securely and protected against unauthorised and unlawful processing and accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted or stored.

[32] Source: Bundesverband Blockchain, data protection, and the GDPR https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf

Other key rules include:

- processing the minimum amount of data necessary;
- not keeping data longer than is necessary
- keeping data up to date

All of these ‘rules’ have implications for the design of DLT-based services.

A ‘controller’ is natural or a legal person, which alone or jointly with others, determines the purposes and the means of the processing of the personal data. A key question and key matter to address in a decentralised system, is who is the ‘controller’ and the distribution of responsibilities among blockchain participants (e.g. nodes, services and applications, possible governance bodies).

The ledger itself is arguably 'infrastructure' established by more than one organisation and or individual participants. For example, Bitcoin has a network comprising over 12,000 nodes operated by a wide range of organisations and individuals.

Ultimately, the scope of regulation will depend on the open or closed nature of the blockchain and its permissioned or un-permissioned nature. In an open permission-less blockchain, for example, the nature of public ‘nodes’ and obscure addresses make it impossible to determine the data controller(s) because there are multiple actors that submit information to the ledger in the form of a transaction and there is no regular way to identify the participants of the transaction. Hence personal data could be added to the blockchain, replicated amongst nodes, and with no way to remove this data due to immutability. Moreover, it might be extremely difficult to determine changes in data. In this case, applications adding personal information to the blockchain could be considered to be the data controller and/or processor and the ledger itself and its network the equivalent of a cloud infrastructure.

4.2.3 Transparency and users’ access rights

While it is often claimed that blockchains can empower data subjects and facilitate more control of their personal records and to know who has accessed such records, the privacy and confidentiality of data and metadata in DLT and blockchains are not inherent in the use of this technology. The DLT facilitates transparency and immutability, which provides support for record keeping and verification, but care is needed to ensure these facilities are applied properly to enhance rather than reduce privacy.

Measures to protect individuals for the confidential use of data include encryption, off-chain controlled data exchange, data anonymisation, e.g. via the use of a cipher with an encryption key over data that enable only a person with the correct decryption key to decrypt the data) [33]. Other approaches may include on-chain encryption, sharding, pruning multiple key pairs and tokenisation. [34]

The *Zero-Knowledge Proof (ZKP)* approach can be used to achieve data minimisation so that only the minimum necessary information about an individual is actually shared, e.g. providing an indication that somebody is an adult, without having to share their date of birth. There are different variations of ZKP. The most advanced are based on encoding structure, not cryptographies. This approach is still experimental, but it is an area of research to be followed and potentially adopted for other blockchain and DLT uses.

[33] Source : Hong Kong Monetary Authority Whitepaper 2.0 on Distributed Ledger Technology available at www.hkma.gov.hk/media/eng/doc/key-functions/finanical.../20171025e1a1.pdf

[34] Techniques used to reduce the amount of data and metadata available on the blockchain.

Data protection by design and by default in the GDPR

A central obligation under data protection law, such as the GDPR (Article 25) in Europe and the recently modernised Council of Europe Convention 108+, is the requirement to adopt data protection by design and default to minimise risks to individuals and to ensure, from a technical and operational perspective, the adoption of privacy enhancing techniques, such as data minimisation, pseudonymisation and encryption. It also requires the data controller to ensure they can meet other key obligations and various (strengthened) rights of individuals:

Rights

The GDPR requires organisations to process personal data in ways that address risks and that meet the rights of individuals, including the right to:

- request the **erasure** of their data when no longer needed
- the right to request a controller **rectifies** inaccurate or incomplete personal information considered incomplete or to record a supplementary statement about the information and restrict the processing of data (that is inaccurate, for example)
- **object** to processing based on a data controller's legitimate interests (including profiling)
- **withdraw consent** – if another legal basis cannot be found, then data may need to be erased

What does it mean for blockchain?

Blockchain technology was originally designed to be an immutable, tamper proof and permanent record. Therefore, a generic blockchain is unable to meet key 'rights', such as those relating to data privacy, and this is the most problematic aspect of a blockchain. As the processing of personal data attributes for identity management purposes will largely take place with a person's consent or possibly for a controller's legitimate interests, the right to erasure presents a significant challenge when using a blockchains for identity. In Germany, for example, the Bundesblock Privacy Working Group, has acknowledged the difficulty of erasing data in a blockchain, noting that limiting the processing of personal data (e.g. allow for blocking data with anonymisation techniques rather than erasing) may be acceptable – though it is unclear how this will happen in practice. It may prove that as data is not accessible and is otherwise invisible in other blocks in the chain, this could be considered to meet the right to erasure, though unlikely and may ultimately need to be decided by the courts.

The challenges presented by key rights:

- The right to rectify inaccurate data (Article 16) – it will be impossible to change data existing on the chain of blocks that are intended to be immutable. However, Art 16 also states that the right can be met by "means of providing a supplementary statement." So in theory, it may be possible to meet the right by adding a statement to the block.
- Data protection by design and default (Art 25) requires that processing takes place in way that ensures an individual's rights can be met and to adopt privacy enhancing techniques such as pseudonymisation.
- The right to restrict processing may prove impossible to execute across the chain of nodes that may be considered to act as data processors (a processor is a natural or legal person that acts on behalf of a controller).

Discussions are taking place on the possibility to implement *privacy by design-enabled blockchain* including solutions where blockchain transactions represent transfer of "data access rights" from data subjects to data controllers (e.g. Consent 2.0 W3C https://www.w3.org/2018/04/17-dataprivacy18-minutes.html). In the USA, NIST is drafting a white paper on a Data Structure for Integrity Protection with Erasure Capability that describes a data structure that provides the capability of deleting specified blocks, while retaining hash-based assurance that other blocks are unchanged. It is primarily designed to be implemented in a permissioned infrastructure, providing certain features of existing permissioned blockchains.

4.3 Regulatory considerations in identity

As the technologies and practices related to DLT and blockchains, and the associate risks, are still evolving, the regulatory boundaries for organisations seeking to implement DLT and blockchain technologies may be somewhat unclear. The increased interest in DLT in general, and its use for identity, in particular, by governments and regulators is apparent in the number of reports and recommendations being published worldwide. Moreover, regulators are actively facilitating DLT and blockchain projects. Governments, in fact, are increasingly working on trials and pilots to assess the benefits and regulatory risks of the technology, providing, for instance, sandboxes for blockchain providers to work closely with regulators.

Therefore, it may be prudent for **industry players, including mobile operators, to actively monitor and consider joining the widespread range of collaborative efforts and initiatives between regulators, governments and the industry in order to better understand and manage the blockchain and identity management opportunities in a regulatory managed environment**.

This will indeed also **help to achieve greater understanding of the legal and regulatory framework conditions that are applicable to blockchain implementations** including how to address existing grey zones areas, in particular, in relation to privacy and data protection.

With the new GDPR rules, the legal status of the different participants in DLT will also need to be clarified (data controller, processor or joint controllers). **Mobile operators aiming to implement blockchain technologies should consider effective governance structures and, importantly, seek best practices to protect the personal data of end users.**

In conclusion, while some uncertainty remains as to how to implement and enforce existing regulations on DLT, there seems to be a clear consensus that directly storing identity and certain types of transactional information (even if it is hashed) on a ledger is a risk. Mobile operators interested in DLTs could develop global **blockchains that use a hybrid of on-chain data that can be used to verify transactions with off-chain personal data storage solutions that effectively minimise the amount of data stored on the chain (e.g. via ‘zero-knowledge proof’ techniques).**

5. Cyber-security issues

DLT and blockchains provide high-integrity via cryptographic techniques and multi-node consensus to implement high-level assurance services. These services involve notaries, time stamping and trusted certificates that can increase automation, lowering the cost of secure online communication.

There are, however, a broad range of issues that need to be reflected in implementations to mitigate potential security risks. These range from simple coding errors (with potential implications for the whole network) through to the security of network end points, weakness in encryption (potentially linked to advances in quantum computing) and design matters, such as reducing the distributed nature of the network for cost reasons, and risks associated with key management and connections with systems outside the DLT network.

In Bitcoin and similar 'proof of work' blockchains there is a known attack that can be staged by directing 51% of the network (mining) hashing power. For Bitcoin, this theoretical attack is not considered achievable in practice due to the cost of staging such an attack against the massive mining computational power now deployed, but such attacks are possible against smaller crypto currencies. There, therefore, needs to be awareness that theoretical attacks against consensus algorithms could happen in practice, given a sufficiently motivated and equipped actor.

More practical attacks are being seen through social engineering practices, which have encouraged users to send crypto currencies to scammers under the promise of bigger rewards, or getting users to share their private keys, which generally result in wallets being emptied. The latter form of attack could be conducted in identity services allowing a malicious actor to share an individual's identity with third parties.

The ability to produce reliable, tamper-proof, and failure-resistant applications is dependent on the ability to reflect globally available cyber security standards in DLT solutions (see for example, the NIST cyber security framework)[35].

[35] This voluntary framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. Source: https://www.nist.gov/cyberframework

6. The use of smart contracts

Smart contracts are the technological evolution, or the digital form, of a paper-based legal agreement or process. Smart contracts are effectively small computer programmes stored on a blockchain, which will perform a binding transactional agreement under specified conditions.

Unlike a regular legal contract, a smart contract is self-executing – that is, once the instructions are written to a blockchain, the transaction will take place automatically when, for example, certain conditions are triggered by digitally verifiable data inputs. Examples of smart contracts include automatically executed electronic payments triggered by data that performance has taken place and payment is due.

Smart contracts rely on some form of a digital identity to operate. At the most fundamental level, in smart contracts the identity of the contracting parties takes the form of 'wallet addresses' and their relevant obligations and rights must be known and properly coded into the smart contract code. Failure to identify the users properly or a fault in the smart contract code may easily lead to fraud. Indeed, anonymous or pseudonymous contracts must also be possible to preserve the privacy of contracting parties.[36]

Under a decentralised identifier data structure (DID),[37] for example, smart contracts could offer a standardised means of associating a contract identifier with qualifications, credentials, and other characteristics that are relevant to that smart contract in a verifiable, yet privacy-preserving, way.[38]

Indeed, the promise of smart contracts is that after digital records are verifiable, a whole new ecosystem of technical automation will start to produce a new social fabric that enables civic efficiencies, personal mobility, and institutional transformation in several sectors of the economy.

However, while smart contracts open up new opportunities, they also raise questions with regard to matters, such as repudiation/ reparation, and application of the legislative and regulatory environment: the numerous entities and wide variety of contexts that could be involved in transactions mean there is uncertainty as to the legal basis of smart contracts.

[36] Source: Accord Project ID: Smart Legal Contracts Identity and Trust Framework Standard http://www.openidentityexchange.org/accord-project-id-the-smart-legal-contract-identity-and-trust-framework-standard/

[37] See W3C Verifiable Claims Working Group in Section 4.1

[38] Source: Accord Project ID: Smart Legal Contracts Identity and Trust Framework Standard

Summary of Issues for Consideration

Blockchains (and distributed ledgers in general) have the potential to become adopted by many enterprises for various operations. But, as is the case with most new technology service offerings, there are a number of issues to be carefully considered before a business can start to fully realise the potential benefits. As noted at the outset and indicated throughout, in many instances existing laws, regulations, and generally accepted guidelines can be applied to use of DLT and blockchains, including for digital identity.

Some of the regulatory and legal challenges are outlined below. This list is not exhaustive and is dependent on the actual purposes, circumstances and functions of DLT applications from mobile operators. But the list is a starting point for identifying the typical range of issues to consider and address when designing and deploying DLT solutions, for which more detailed analysis is included in previous sections.

- **Competition and anti-trust.** Regulators have suggested that DLT and blockchain may pose a risk to fair competition in some implementations where artificial or technological barriers to entry may lead to monopoly-like situations because of the possibility to exclude new participants in the shared ledger.

- **Legal basis for blockchains and issues related to the implemented governance.** Although only a few governments have adopted blockchain laws, both general principles, related to contractual laws and current legal frameworks to the telecommunications sector and other industries may be applicable. The nature of the DLT implementations and their governance structure (e.g. permissioned vs non-permissioned) carries additional regulatory considerations that need to be assessed. Closed and permissioned networks are typically considered more effective by governments and regulators alike because of the potential for permissioned DLT to enter in a governance structure, which include a self-regulated trust framework. Trust frameworks may help to establish the legal and contractual relationship between the organisations operating the nodes forming the network and could guarantee, for example, in legal terms the admission and expulsion from the community of authorised users, or could also help to define how updates to a blockchain are made and validated. With the new EU GDPR and privacy rules, greater clarity on the role and legal status of the organisations that store or process personal data will also need to be provided.

- **Jurisdiction and liability.** Blockchains can cross jurisdictional boundaries as the nodes on a blockchain can be located anywhere in the world. This can pose a number of complex jurisdictional issues, which require careful legal consideration in relation to the relevant contractual relationships and formal set of terms and conditions amongst participant parties. Each organisation operating a network node may be subject to different legal requirements (e.g. local jurisdictions' courts for dispute resolutions, rules on arbitrations or adjudications), and generally there is no "central administration" responsible for operating each distributed ledger (though there is often a form of 'foundation' that decides technology evolution). Following this same reasoning, liability also represents a concern: there may be no party ultimately responsible for the functioning of distributed ledgers and the information contained therein, in particular when dealing with harms and losses caused by the failure of DLT, including data breaches, hacking and lack of contract delivery.

- **Privacy and data protection.** The shared, scalable and immutable nature of DLT and blockchains allows many innovative designs and possible implementations of these technologies. However, it also creates potential issues relating to personal data privacy according to jurisdictional legal requirements, because some personal data may be included and processed in a DLT and blockchain platform by third parties who are not operating the network nodes. Current privacy and data protection frameworks have been designed on the basis that data is centrally collected, stored and processed, i.e. the majority of privacy laws assume singular entities for data management purposes with data storage function centralised rather than decentralised. Therefore, some tensions between decentralised technologies, such as DLT and blockchains, and current regulatory frameworks are to be expected. Still, there are existing and emerging implementations that offer personal data stored off-chain and already demonstrate how enhanced data management solutions focused on privacy can be achieved, even on an immutable blockchain.

Further reading

The GSMA's Internet of Things Programme is working with operators to identify use cases and opportunities for distributed ledgers in the Internet of Things (IoT). It plans to publish a report during summer 2018 covering the application of distributed ledgers in various domains, including the identity of things, the use of smart contracts in the IoT, micropayments, data sharing, supply chain solutions, access control and enabling the sharing economy. This report will be published on the GSMA's IoT Programme website at https://www.gsma.com/iot/

The GSMA’s Digital Identity Programme published a research report entitled ‘Blockchain for Development’ in January 2018 to help stakeholders in the development sector better understand what blockchain technology is. The paper provides a high-level overview of why it may be interesting from a development perspective. It also highlights four blockchain platforms that are being piloted to improve digital identities, humanitarian cash transfers and aid transparency. This report is available here: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf

Examples of Government-related initiatives on blockchains

Inclusion of examples in this chart does not imply GSMA endorsement.

	DESCRIPTION/OBJECTIVE	EXPECTED POLICY IMPACT
Government of Estonia	E-Stonia, a blockchain-enabled identification card, allows Estonians to access e-services, such as banking and medical prescriptions through their digital signature Since 2013, the Estonian government registers — including those hosting all citizen and business related information — have used **Guardtime** to authenticate the data in their databases. Their **keyless signature infrastructure (KSI)** pairs cryptographic ‘hash functions’ with a distributed ledger, allowing the Estonian government to guarantee a record of the state of any component within the network and data stores. Guardtime’s KSI functions without a ledger. Cryptographic hash values of the electronic records are stored in the Guardtime blockchain. Verification of a given document is performed by generating a hash of the document and comparing the value with the hash stored in the blockchain. When the hash matches, then the record is assured.	By using a blockchain, the Estonian government offers proof of time, identity and authenticity. KSI signatures offer data integrity, backdating protection and verifiable guarantees that data has not been tampered with. It is transparent and works to the user’s benefit too: *citizens can see who reviewed their data, why, and when; and any alterations to their personal data must be authorised.* Using hash functions, as opposed to the asymmetric cryptography used in most public key infrastructure (PKI), KSI cannot be broken by quantum algorithms. It is also so scalable that it can sign an exabyte of data per second using negligible computational and network overhead. It removes the need for a trusted authority, its signed data can be verified across geographies, and it never compromises privacy because it does not ingest customer data. It is clear that the system marks a major advancement in PKI. Although the Estonian ID Card may not be immune to a breach, there have been none so far and the KSI blockchain means the government is assured that rogue alterations to public data will be 100% detectable.

	Over the past decade, Guardtime has added features to the platform including post-quantum signatures to replace RSA, anti-tamper hardware (Black Lantern), and a provenance calculus designed to track and trace digital information, which really differentiates it from standard blockchain applications. Its long experience has enabled it to adapt its platform to numerous contexts, including cloud assurance, connected vehicles, critical infrastructure protection, DevOps, defence and aerospace, government, financial services, IoT, and telecommunications, among others.	
City of Zug, Switzerland	Zug ID [39] is the world's first live implementation of a self-sovereign government-issued identity on Ethereum.	Zug ID brings significant benefits to the Zug City administration and its users: • Low infrastructure requirements. As the city is relying on a public instance of Ethereum, it does not need to host its own servers or nodes, or maintain complex databases of user credentials. • Decreased security risk: As the city does not host its own servers, but instead distributes the ownership of both identity and attestation to its citizens, it is less susceptible to cyber attacks or data theft. • GDPR compliant: Companies merely verify the minimum amount of information necessary for a specific use case. This reduces liability for service providers, as they only save the data that they use.
European Commission and European Parliament	The EU Blockchain Observatory and Forum is a two-year project to help identify and provide analysis of the technological and organisational trends. It will identify and build on existing initiatives and organise discussions and workshops around topics where action at the EU level could be required or could have an impact (e.g. on regulatory issues) in an open, constructive and reactive way.	Objectives include: 1. Create a knowledge repository about blockchain technology and blockchain initiatives around the world, including education materials. 2. Identify framework conditions suitable to accelerate blockchain innovation across the EU in the context of a Digital Single Market.

[39] Source: https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702

	The EU Observatory and Forum aims to play a proactive role to help the EU to stay at the forefront, build expertise and show leadership in the field.	3. Prioritise use cases, especially high-impact blockchain initiatives to be initiated by the EU and Member States. The Forum operates via two working groups • Blockchain Policy and Framework Conditions • Use Cases and Transition Scenarios The GSMA is an expert member of the Blockchain Policy and Framework Conditions working group.[40]
Barcelona and Amsterdam	The cities of Barcelona and Amsterdam are piloting the use of blockchain technology to give citizens more control over their online data. The EUR 5 million Horizon 2020 research project, named Decode (DEcentralised Citizens Owned Data Ecosystem), started in January 2017 and will run until December 2019.	The two cities aim to use the Decode pilots[41] to encrypt citizen data, and use blockchain technology to give citizens more control over how their digital records are used by public services. “Increasing awareness [over the use of online data] is at the heart of Barcelona’s digital strategy.”
ITU	ITU Working Group on security aspects of blockchains on several topic for DLT.	**Study Group 17 (security):** • Produce a set of standards providing comprehensive security solutions for DLT-based applications and services • Study and identify PII protection issues and threats in DLT-based applications and services **Study Group 13 (future networks**) [42] • Scenarios and capability requirements of blockchains in next generation network evolution **Study Group 20 (IoT, smart cities and communities (SC&C))** • Framework of blockchains of things as decentralised service platform **Focus Group on data processing and management to support IoT + SC&C(8)** • Overview of IoT and blockchains • Blockchain-based data exchange and sharing • Using blockchains to improve data management
CEN and CENELEC	The standardisation initiative CEN Workshop 84 on a 'Self-Sovereign Identifier (s) for Personal Data Ownership and Usage Control' (CEN WS ISÆN, 2016) proposes	The goal is an overall concept for self-sovereign identities that is in line with the EU General Data Protection Regulation (GDPR). The standard is intended to cover the following areas in particular:

[40] https://ec.europa.eu/digital-single-market/en/news/eu-blockchain-observatory-and-forum-call-contributors

[41] www.decodeproject.eu

[42] www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14282

	the ISÆN concept for managing digital identities of human beings.	• Creation of a core identity by the human derivation of transaction-based digital identities from the human's core identity, • implementation for requesting and granting explicit consent from the human, and • logging all transactions in a public distributed ledger. This project focuses on a self-sovereign identifier which offers individuals, also known as data subjects, the possibility to sign and mark their stream of data (e.g. by hashing and data watermarking technologies). The proposal is to call the identifier system the **ISÆN**: **I**ndividual per**S**onal data **A**uditable addr**E**ss **N**umber. Individuals could generate themselves an **ISÆN** allowing them to retrieve information about the exact localisation and use of their data. This smart navigation can be compared with GPS data.
ISO TC/307 For blockchains and DLT[43]	The inaugural meeting of the Technical Committee was held on May 24, 2017, in Sydney, Australia, and was attended by representatives from more than 45 countries. Of these, 25 participating countries designated ISO/AWI 22739 as the first standard to be developed to establish uniform terminology and concept descriptions.	In addition to the terminology working group developing ISO/AWI 22739, the technical committee has five subcommittees focused on: (1) reference architecture, taxonomy and ontology; (2) use cases; (3) security and privacy; (4) identity; and (5) smart contracts. The goal is to develop standards that are "robust enough to provide guidance to stakeholders and potentially be referenced by regulators in policy," but are technical and "exclude matters pertaining to the law in the development of standards for smart contracts, privacy, security and identity."
USA (Bitcoins and cryptocurrency legislation)	In 2017, **at least eight US States worked on bills accepting or promoting the use of Bitcoin and blockchain technology**, while a couple of them have already passed them into law. The most important developments for blockchain regulation and implementation in the US in an evidentiary context occurred in Arizona (recognition of smart contracts), Vermont (blockchains as evidence), Chicago (real estate records), and, most importantly, Delaware (pending initiative authorising registration of shares of Delaware companies in blockchain form).	The state of Delaware has passed amendments to state law that make explicit the right to trade stocks on a blockchain. Developed under the close guidance of blockchain lawyer Marco Santori of Cooley LLP and Caitlin Long of blockchain start-up Symbiont, the bill is expected to pave the way for potentially large-scale issuance of stock on a blockchain.[44]

[43] www.iso.org/committee/6266604.html

[44] http://uk.businessinsider.com/blockchain-cryptocurrency-regulations-us-global-2017-10?r=US&IR=T

The Civic App	An individual can download the app to their smartphone and use it like a virtual ID card. Civic does not store the data on a single, hackable server. Users access their accounts through biometric verification (fingerprint or 3D facial recognition) which provides an extra level of security should the user lose their smartphone. Civic also acts as an early warning system for identity theft. Users will receive notifications when Civic believes their information is being compromised or used fraudulently.	Civic intends to create a fully decentralised ecosystem for IDV services, consisting of a variety of smart contracts and new software applications to allow participants to interact with the ecosystem. The idea is to verify the user's identity with Civic tokens on behalf of identity verifiers (such as banks or healthcare providers). Verifiers use the ledger to verify and validate an identity. Civic offers three verification applications with their app: • Private Login, Low Level (including email addresses and phone numbers), and • KYC Level (address, social security number, etc.). KYC is currently only available in the United States as it requires substantial negotiation with local government to validate the application for use with government-issued identities. Going forward, Civic plans to develop new applications, including notary services, access to credit reports, P2P identity services, personal background checks, etc. The goal is to give control of data back to users, and better protect against data theft and identity fraud.

Resources

Websites

- APEC Cross-Border Privacy Rules (CBPR): http://www.cbprs.org/
- BBFA: https://bbfa.info
- Blockchaingers: https://blockchaingers.org/
- Civic: www.civic.com
- Evernym: www.evernym.com
- Hyperledger https://www.hyperledger.org/projects
- W3C: https://w3c-ccg.github.io/did-spec/
- EU Data Protection website, including opinions from data protection Article 29 Working Parties: https://ec.europa.eu/info/law/law-topic/data-protection_en Tradle: https://tradle.io/
- European Data Protection Supervisor: https://edps.europa.eu/edps-homepage_en
- OECD Privacy Principles and guidelines: http://oecdprivacy.org/; http://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

Articles and Reports

- *5 Governments That Actually Support Blockchain Innovation.* Singular DTV, 2017. Available at: https://medium.com/singulardtv/5-governments-that-actually-support-blockchain-innovation-d4b3c1e27119
- *Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry*. Microsoft and Chamber of Digital Commerce. English, E., Davine Kim, A., Nonaka, M., 2018.
- *Anti-money laundering: MEPs vote to shed light on the true owners of companies.* European Parliament, Press Releases, 2018. Available at http://www.europarl.europa.eu/news/en/press-room/20180411IPR01527/anti-money-laundering-meps-vote-to-shed-light-on-the-true-owners-of-companies
- *Blockchain Beyond the Hype: A Practical Framework for Business Leaders.* World Economic Forum, 2018. Available at: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf
- *Blockchain beyond the hype: What is the strategic business value?* Carson,B., Romanelli G., Walsh, P., and Zhumaev, A., June 2018 https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value
- *Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid*. GSMA, 2017. Available at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/12/Blockchain-for-Development.pdf
- *Blockchain, Data protection, and the GDPR.* Bundesverband, 2018. Available at https://www.bundesblock.de/wp-content/uploads/2018/05/GDPR_Position_Paper_v1.0.pdf
- *Blockchains and Data Protection in the EU.* Max Planck Institute for Innovation & Competition Research Paper No. 18-01. Finck, M. (2017).
- *Self-Sovereign Identifier(s) for Personal Data Ownership and Usage Control.* CEN WS ISAEN, 2016. Available at: www.cen.eu/work/areas/ICT/Pages/WS-IS%C3%86N.aspx
- *Distributed Ledger Technologies for Public Good: leadership, collaboration and Innovation*. Holmes, C., 2017.
- *Distributed Ledger Technologies: beyond blockchain.* Government Office for Science, 2016.
- *Distributed Ledger Technology Feedback Statement on Discussion Paper 17/03.* Financial Conduct Authority, 2017. Available at: https://www.fca.org.uk/publication/feedback/fs17-04.pdf

- *Do Blockchains Have Anything to Offer Identity*? Steve Olshansky and Steve Wilson, 2018. Available at: https://www.internetsociety.org/resources/doc/2018/blockchain-identity/
- *European Countries Join Blockchain Partnership*. European Commission, Digital Single Market, 2018. Available at https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership
- *Frequently Asked Questions: Financial Technology (FinTech) Action Plan*. European Commission, 2018. Available at: http://europa.eu/rapid/press-release_MEMO-18-1406_en.htm
- *How can governments use blockchain to build better public services?* Macaulay, T., 2018. Available at: https://www.computerworlduk.com/applications/how-can-governments-use-blockchain-build-better-public-services-3671007/
- *Humanitarian Blockchain: Coding for a Humane, Sustainable World.* Brown, M., 2018. Available at: https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/marshallbrown/2018/02/15/humanitarian-blockchain-can-we-code-for-a-humane-sustainable-world/amp/
- *Identity - Mobile Connect*. GSMA. Available at https://www.gsma.com/identity/mobile-connect
- *ISO/TC 307 - Blockchain and distributed ledger technologies.* International Organization for Standardization. Available at: www.iso.org/committee/6266604.html
- *ITU Working Groups on Security Aspects of Blockchain Working on Several Topics for DLT* Available at: www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14282
- *Mapping the Global Legal Landscape of Blockchain and Other Distributed Ledger Technologies*. Maupin, J., Center for International Governance Innovation Papers No. 149, 2017. Available at: https://www.cigionline.org/sites/default/files/documents/Paper%20no.149.pdf
- *Microsoft, Hyperledger, UN Join Blockchain Identity Initiative*. Sundararajan, S., 2018. Available at: https://www.coindesk.com/microsoft-hyperledger-un-join-blockchain-identity-initiative/
- *Mobile Privacy Principles,* GSMA 2011 Available at https://www.gsma.com/publicpolicy/mobile-privacy-principles
- NIST Cybersecurity Framework, 2018. Available at https://www.nist.gov/cyberframework
- Open Identity Exchange (OIX) Accord Project ID: Smart Legal Contracts Identity and Trust Framework Standard, OIX 2018 http://www.openidentityexchange.org/accord-project-id-the-smart-legal-contract-identity-and-trust-framework-standard/
- *On Blockchain and the General Data Protection Regulation ,* Luis-Daniel Ibáñez, Kieron O'Hara, and Elena Simperl University of Southampton 2018
- *Prediction Markets and Blockchain Identity Verification: Gnosis Olympia and uPort*. Ayers, R., 2018. Available at: http://www.coincatalyst.com/category/blockchain/
- *Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution.* Der U., Jähnichen, S., Sürmeli, J., 2017.
- *The Future of Financial Infrastructure: an ambitious look at how blockchain can reshape financial services.* An Industry Project of the Financial Services Community. World Economic Forum, 2016. https://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
- *The Importance of "Blockchain" to Identity*. Tobin, A. Available at: https://www.gsma.com/identity/wp-content/uploads/2017/04/The-Importance-of-Blockchain-to-Identity-Andy-Tobin-Evernym.pdf
- *The Truth about Blockchain.* Harvard Business Review. Iansiti, M., Lakhani, K., 2017. Available at: https://hbr.org/2017/01/the-truth-about-blockchain
- *The next $20 billion digital market – ID verification as a service.* Fuel by McKinsey June 2018 https://fuelbymckinsey.com/home/article/the-next-20-billion-digital-market-id-verification-as-a-service
- *The Wired Guide to Blockchain*. Finley, K., 2018. Available at: https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/guide-blockchain/amp

- *The Year of Blockchain*: Global Legal Framework Begin to Take Form. Financial Regulatory Observer, 2018. Available at: https://www.whitecase.com/publications/insight/year-blockchain-global-legal-framework-begins-take-form
- *This is all you need to know about Blockchain.* Hart, D., 2018. Available at: http://perspectives.scotiabank.com/posts/this-is-all-you-really-need-to-know-about-blockchain-15529498?utm_source=Twitter&utm_medium=Twitter_Promoted&utm_campaign=blockchain_dubie&utm_content=blockchain_dubie
- *White Paper on Blockchain – Operator Opportunities*. GSM Association, 2018.
- *Whitepaper 2.0 on Distributed Ledger Technology*. Hong Kong Monetary Authority, 2017. Available at http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/infrastructure/20171025e1a1.pdf
- *WIN, United Nations to Use Blockchain to Combat Child Trafficking.* Pimentel, D., 2017. Available at: http://blocktribune.com/win-united-nations-use-blockchain-combat-child-trafficking/

Expert interviews and reviews

- Adam Cooper, Director, Next ID
- Andrew Johnston, Principal Technology Architect, Telus
- Andrew Tobin, Evernym
- Axel Nennker, Deutsche Telekom
- Balazs Nemethi, CEO, Taqanu
- Kai Wagner, Jolocom and Bundesverband Blockchain
- Patrick Curry, Director, British Business Federation Authority (BBFA)
- Rinze Cats, Technical Blockchain Consultant, KPN

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com