The Expert Group on
Blockchain Ethics (EGBE)

Ethical Guidelines for Blockchain Systems



European Blockchain Center

European Commission

ebsi
European Blockchain

Content

Foreword 3
Management Summary 4
1. Introduction 6
1.1 Blockchain Systems and European Values 7
1.2 European Blockchain Partnership and Blockchain Ethics 9
1.3 Blockchain Systems in a Nutshell 11
2. European Values as Ethical Foundation 12
2.1 Security 14
2.2 Equality and Non-discrimination 14
2.3 Justice and Fairness 14
2.4 Diversity and Inclusion 15
2.5 Privacy 15
2.6 Sustainability 15
2.7 Responsibility and Accountability 16
2.8 Freedom 16
2.9 Property 16
3. Blockchain Characteristics and Ethical Issues 18
3.1 Decentralisation 19
3.2 Immutability 20
3.3 Transparency and Distribution 21
3.4 Auditability and Accountability 23
4. Ethical Guidelines for Blockchain Systems 26
4.1 Guideline to Ensure Fairness 28
Open Access
Governance Power
Life Cycle
4.2 Guideline to Protect Privacy 30
Sensitive Data
Pseudonymity
4.3 Guideline to Assure Security 32
Nodes
Quality of Code
Verifying Data
Traceability, Transparency, and Interoperability
4.4 Guideline to Allow for Accountability 34
Value Creation and Tokenisation
Ownership
4.5 Guideline to Guarantee Societal Responsibility 36
Sustainability
Democracy
Risk Mitigation
5. Ethical Implementation of Blockchain 38
6. Outlook 41
7. Conclusion 44
8. Contributors 47
9. Glossary 48
10. Endnotes 51

Foreword

Blockchain and distributed ledger technologies in general allow for disruptive innovations that have the potential to change existing processes and business models, as well as the inner fabric of how we interact in society. The promise of blockchain is to distribute decision power, whether it be within supply chains, industries, or whole markets.

Blockchain solutions can facilitate user-based ownership models, e.g., network-owned social platforms or online games. Such network- owned applications can constitute an alternative to federated platforms where control is typically in the hands of a single company, which sometimes can be at the expense of the users. A blockchain network can create public goods which are goods or services that are non-excludable and non-rivalrous. The European Blockchain Services Infrastructure (EBSI) is such a network, that aims to increase welfare for European citizens and organisations. However, blockchain does not only allow for new economic models, but also enables new business models for networks to improve or provide public goods and services. In addition, public services can benefit from blockchain solutions, e.g., when authentication or registration in cross-border processes is necessary, e.g., when studying abroad, moving abroad, or working abroad.

Blockchain-based applications and services have the potential to empower citizens when interaction or using such services online. Improving processes for all stakeholders, creating revenue models that generate value in form of private and public goods, and establishing network-owned platforms and applications is part of a human-centred, distributed environment that is focusing on the empowerment of a sovereign acting citizen in the digital space.

However, blockchain solutions can also be used to centralise power or control depending on how they are designed and implemented. To avoid unintentional negative spill-over effects, blockchain systems should be developed in a mindful and ethical way, consistent with the norms and values that should be embraced. While this is always important for all kinds of information technologies, it is especially crucial for blockchain systems that are supposed to support public applications and services for societies and become an integral part of the next generation Internet and various forms of network organizations, such as virtual worlds or Web3, just to give some examples.

It is of paramount importance that foundational digital infrastructures are not designed in ways that discriminate or harm citizens, minorities, elderly people, smaller companies, etc. when designing and implementing such systems. This is especially the case when such systems become de-facto standards or are to be used on a mandatory base with no alternative. Such public systems must meet highest legal and ethical standards.

As blockchain systems only unfold their full potential when not altered frequently, so that they can operate autonomously and immutable over a longer period providing services and welfare, ethical guidelines and awareness for norms and values and their role when designing, implementing and operating blockchain systems are required.

With this report, a group of experts mandated by the European Blockchain Partnership, in charge of the European Blockchain Services Infrastructure, has worked on general guidelines oriented along European values. As blockchain can be regarded as a sovereignty technology, the expert group discussed what needs to be considered when enforcing values in blockchain systems. To our knowledge, this is the first report of this kind, and clearly can only be a starting point for a more engaged discourse on blockchain ethics.

As convenor and project office for the EU Expert Group on Blockchain Ethics, we are grateful for the invaluable and generous contribution from the group members. During the course of working on this report, it became obvious that the nature of blockchain systems (providing semi- of fully autonomous systems that execute values) requires a societal dialogue and deeper academic discourse on the role of norms and values when creating and implementing blockchain systems. We would like to thank all members of the expert group for volunteering their time and expertise.

Best,
Roman Beck and Signe Agerskov
(Convenors)

Management Summary

Ethical guidelines are important for different stakeholders, such as, but not limited to, blockchain architects and developers. The five key areas identified in this report are:

1. Fairness	Blockchain systems and applications should be designed in a way that allows for the inclusion of relevant stakeholders and non-discrimination. Designers should continually consider how power structures in blockchain systems may evolve, how they may be misused, and how they can serve to prevent, or at least mitigate unintended or unwanted outcomes.
2. Privacy	Sensitive data should not be stored directly on blockchain ledgers. Only data that has been assessed to be suitable for distribution in a tamper-resistant way should be stored directly on ledgers. Blockchain systems should be designed in ways that protect the privacy of users while also enabling duly authorized law enforcement to investigate illegal activities.
3. Security	Blockchain systems' governance power should be distributed to minimize the risk of unintentional concentration of decision power. The hardware that runs voting nodes should be hardened against any form of tampering. Code quality should be carefully assessed before the code is deployed in a blockchain system and traceability between different blockchain systems should be provided.
4. Economic Accountability	In blockchain systems, tokens (such as cryptographic tokens) should only be used for the purpose for which they were designed and not repurposed for other uses without sufficient prior reflection. Designers should consider how tokens incentivise behaviour before any assets get tokenised. Regulations and processes should protect users and property rights.
5. Societal Responsibility	Blockchain systems should be designed to work sustainably and support various sustainable applications. Suitable governance processes should be upheld to guarantee the integrity of blockchain systems. Risk mitigation should be taken into account to avoid harmful consequences for users, citizens, and society.



The European Member States have bold ambitions for the use of blockchain.

1 Introduction

1.1 Blockchain Systems and European Values

The European Union is built on fundamental rights, democracy, and the rule of law. Article 2 of the Treaty on European Union provides that 'The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail.'[1] As part of its policy of protecting these values, the EU has acceded to the European Convention on Human Rights and developed its Charter of Fundamental Rights. Furthermore, the EU has defined the European Declaration on Digital Rights and Principles for the Digital Decade[2] and the Declaration for the Future of the Internet[3]. Both declarations emphasis the role and importance of values such as openness, interoperability, security or reliability, just to give a few examples.

These fundamental European rights all stand on a century-long effort to develop ethical standards and principles to protect humans from harm and set norms for ideal human behaviour—examining what is morally right or wrong, just or unjust, in order to govern human behaviour and encourage right actions.

However, our ability to make the right choices, and to do what is right, is increasingly challenged by the profound changes that emerging technologies are bringing to our daily lives and societies and the speed at which these changes are taking place. The Internet, artificial intelligence (AI), and blockchain systems are all examples of such disruptive technologies. Even as they enable new ways of interacting and coordinating, new economies, and new ways of understanding and relating to the world around us, these technologies also put our current norms and values to new tests.

To govern such new technologies and set the necessary boundaries for their use, it is important that we continually promote our understanding of the technologies and study the changes and impact they bring to our most important values. The guidelines presented in this document contribute to the public debate, sharpening the understanding, and forming stronger, more value-aligned blockchain systems. This is needed for building trust in new technologies and is a precondition for leveraging their full powers to solve the many important challenges we face.

Blockchain systems (or more generally distributed ledger technologies (DLT)) are no exceptions to this (note that in this document, the terms blockchain and DLT are interchangeable).

Blockchain is a highly disruptive technology. It allows people and organizations who may not know or trust each other to collectively agree on and permanently record information without a third-party authority. By creating trust in data in ways that were not possible before, blockchain has the potential to revolutionize how we share information and carry out transactions online, with immense impact across multiple domains from logistics and supplychain, the financial and legal sectors, to sustainability and much more.

The EU wants to be a leader in blockchain technology—to become an innovator and a home to platforms, applications, and companies. The ambitious European strategy for blockchain includes building a pan-European public services blockchain infrastructure with a wide field of applications; increased funding for blockchain research and development; leveraging the powers of blockchain to promote much-needed new solutions for sustainability and addressing climate change; as well as the development of skills and standards.

As the EU aims to create digital sovereignty for Europe it is important that blockchain systems respect European principles and norms, and that the necessary basis for trust is secured. The development of standards and ethical guidelines is an essential element of the European blockchain strategy.

For this reason, in 2021 the European Blockchain Partnership (EBP)[4] established the Expert Group on Blockchain Ethics (EGBE) to ensure that the European blockchain infrastructure is based not only on European servers but also on European values. The EGBE has a mandate to create ethical guidelines for blockchain systems. These guidelines aim to ensure that European values and norms are reflected not only in legal and regulatory frameworks for blockchain technology but also embedded directly into the code and within the incentive mechanisms and governance structures of blockchain systems themselves.

The expert group consists of ten experts with backgrounds in blockchain technology, philosophy, computer ethics, and law (a full list of EGBE members appears in section 8). Over the past years, the group has developed guidelines relating to five overall domains: fairness, economic accountability, privacy, security, and social responsibility.

In this work, the EGBE owes gratitude to a large number of experts and collaborators including the EBP, who have kindly offered their time, expertise and experience to the work. The EGBE is also thankful to the EBP for its foresight and guidance in initiating the work of this expert group. The ethical guidelines outlined in this document help users of blockchain, be they developers, investors, regulators, or other affected parties, to do the right thing with this technology.

This report, and the work of the EGBE, is by no means intended to be the final word on blockchain ethics. Quite the contrary. The EGBE will be content if the readers — developers, industry professionals, decision-makers and regulators, academia, investors, users, and interested citizens — find the document relevant and useful. But we will be especially happy if the report can also inspire debate and further work in the ongoing journey of developing our understanding of the possibilities and risks of this technology and how to manage it.



1.2 European Blockchain Partnership and Blockchain Ethics

The guidelines for blockchain systems have been defined by the EGBE with input from the technical groups of the EBP and extern experts.

The EBP was established on April 10, 2018, when 21 EU Member States and Norway signed a joint declaration creating the European Blockchain Service Infrastructure (EBSI).[5] The EBP was then extended to all EU Member States, Norway, Liechtenstein, and Ukraine as an observer. The goal of EBP and EBSI is to use blockchain [and decentralised solutions] in support of digital sovereignty and to provide cross-border digital public services within the European Union based on open interfaces, interoperability, and the highest standards of privacy and security.

On November 9, 2021, the EBP mandated the EGBE[6] to work on ethical guidelines for blockchain systems. This is to ensure that European values and norms are reflected in the legal and regulatory frameworks for blockchain technology (as described in the blockchain strategy by the European Commission), but also that European values and ideals are engraved in the code, incentive mechanisms, and governance structures of blockchain systems themselves. Blockchain systems must be compliant with European legislation. However, mere compliance is not enough: It is important that blockchain systems be in alignment with European values and norms. It is important to have European ethical guidelines for blockchain systems and to address ethical issues arising from blockchain technology from a European point of view.

The European Commission has developed a blockchain strategy aimed at empowering the European Union to become an innovator and leader of blockchain technology—a place where technological innovations can flourish, new applications can be developed, and blockchain companies can be established.

The EC emphasizes that blockchain technology must '[embrace] European values and ideals in its legal and regulatory framework'.[7] The EC's blockchain strategy focuses on the use of blockchain for providing better services and is considered a 'gold standard' for blockchain technology and centres on five focus points:

1. Environmental sustainability
As part of the European Green Deal to make the EU climate-neutral by 2025,[8] blockchain systems should be sustainable and energy-efficient and should be used to achieve sustainability goals.

2. Data protection
The European Union has a strong focus on data protection, such as the General Data Protection Regulation (GDPR).[9] Blockchain systems should not only be compliant with GDPR but should also enhance European data protection and privacy regulations in general.

3. Digital identity
Blockchain-based digital identities, should respect and support the new European digital identity framework (extending the electronic Identification and Authentication and Trust Services - eIDAS) and should also be compatible with e-signature regulations.

4. Cybersecurity
Blockchain systems should incorporate high levels of cybersecurity to ensure that they are robust, trustworthy, and safe.

5. Interoperability
Blockchain systems should be created with interoperability in mind. The systems should be interoperable not only with other blockchain systems but also with legacy systems.

The EU and its Member States are already taking steps to use blockchain technology for digital sovereignty and climate action. These include incentivising actors to reduce their carbon footprint, establishing a network between suppliers and consumers, using blockchain-based systems to finance climate action via green bonds and alternative finance mechanisms, and developing strategic partnerships.[10]

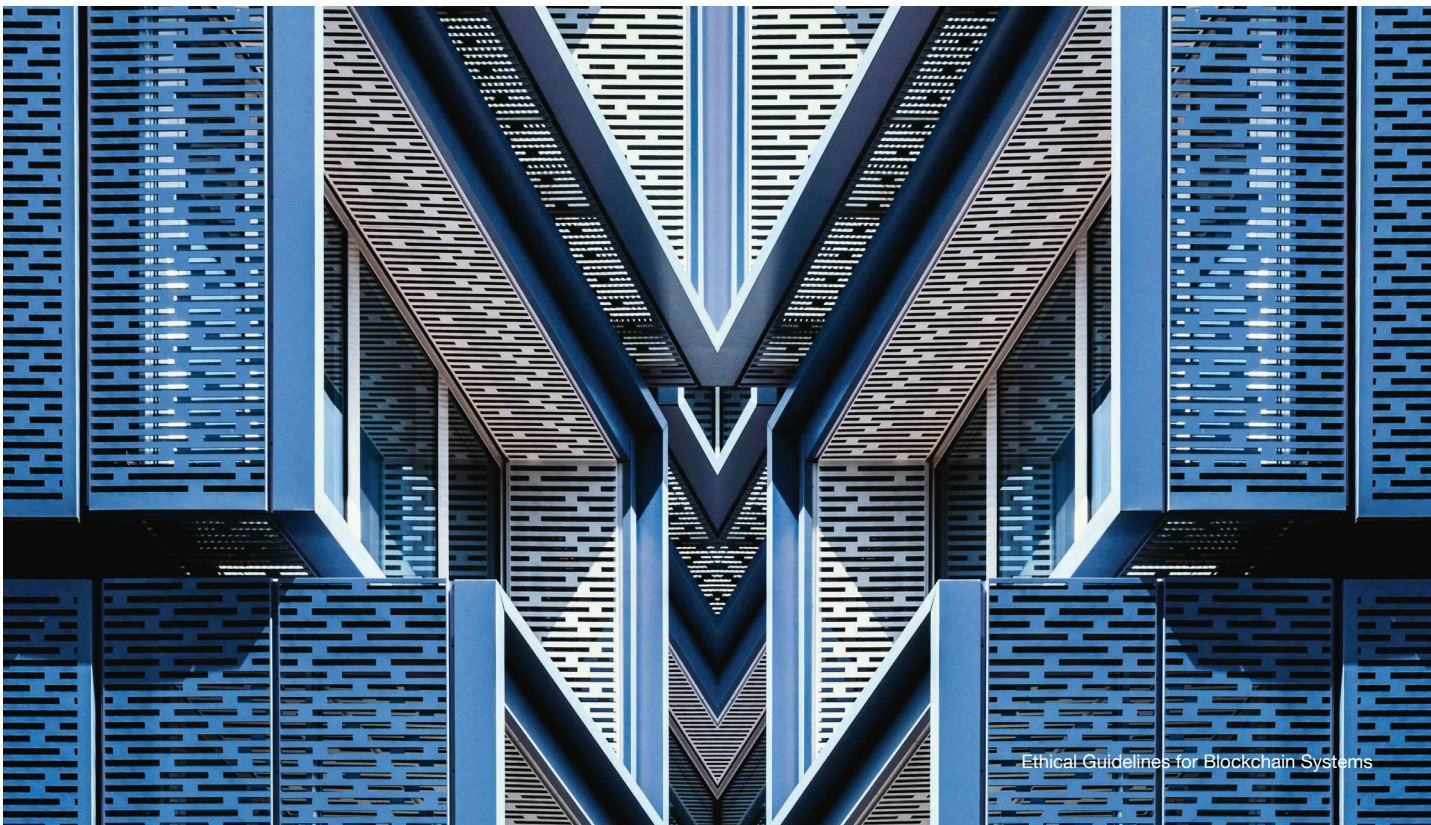
This mandated report is the first of its kind, mapping ethical issues for blockchain systems and outlining ethical guidelines based on European values and norms.

1.3 Blockchain Systems in a Nutshell

Blockchain can be described as a tamper-resistant database of transactions consistent across a large number of nodes. The blockchain is cryptographically secured against manipulations by using a consensus mechanism to keep the database consistent. Data storage on the blockchain is secured by cryptographic hashes in which data being hashed return a fingerprint that verifies the authenticity of the data. Alteration of the original data causes the hash of the altered data to no longer match the original fingerprint. Transactions on the blockchain are grouped and stored in blocks. The combined hash of these transactions is also stored, and each subsequent block saves the combined hash of the previous block. This creates a chain of cryptographically secured and linked blocks containing the information—the blockchain.[11]

Any attempt to change information necessitates rehashing, not only the block relevant to the transaction, but all subsequent blocks. This is possible theoretically, but it's impractical since the blocks grow continuously as other nodes add blocks to the blockchain. Freely programmable blockchains such as Ethereum allow for user-created smart contracts executed on a generic, programmable blockchain under decentralized control, using a built-in Turing-complete programming language. This allows smart contracts and customized (even arbitrary) rules for ownership, transaction formats, and state transition functions, thereby enabling a blockchain system.[12]

It is worth noticing that this report does not aim to present and explain the various types of blockchains, applications, smart contracts, DAOs, tokens, and cryptocurrencies in all detail and thus generically speaks about "blockchain systems". We are aware that a more appropriate term would be DLT instead of speaking of blockchain. However, for simplification reasons and as EBSI is also referring to "blockchain" and not to "DLT", we use "blockchain" as synonym for "DLT".



Ethical foundations promote peace, security, sustainable development, as well as solidarity and mutual respect.

2 European Values as Ethical Foundation

While there is no single document that codifies European values and norms, a foundational principle of the European Union is to empower citizens and societies and to protect them from harm. This section provides an overview of key European values and norms that serve as a baseline for the development of ethical guidelines for blockchain systems.

Most of these values express individual rights based on the Charter of Fundamental Rights of the European Union[13] and on the European Declaration on Digital Rights and Principles for the Digital Decade[14]. The rights and norms that are of particular relevance for blockchain systems include:

1. **Security**
2. **Equality and non-discrimination**
3. **Justice and fairness**
4. **Diversity and inclusion**
5. **Privacy**
6. **Sustainability**
7. **Accountability and responsibility**
8. **Freedom**
9. **Property**

References to these rights and values can be found throughout many EU policy documents, and they appear frequently in academic ethics literature in the European Union as well as in public debate. In addition to the Charter of Fundamental Rights and the European Declaration on Digital Rights and Principles for the Digital Decade, the EU and its member states are party to the European Convention on Human Rights,[15] the Universal Declaration of Human Rights,[16] the International Covenant on Civil and Political Rights,[17] the International Covenant on Economic, Social and Cultural Rights,[18] and the UN Guiding Principles on Business and Human Rights.[19] Commitment to sustainability and justice can be found in the UN's 2030 Agenda for Sustainable Development and its Sustainable Development Goals (SDGs)[20] and the Paris Agreement.[21] In what follows, we briefly review these European and international values.[22]

2.1 Security

The EU Charter recognises a person's right to security, which is the right to protection from bodily or mental injury inflicted by governmental or private actors. The charter also contains several related rights that offer additional security to persons, including the right to life, the right to physical and mental integrity, the prohibition of torture and inhuman or degrading treatment, and the prohibition of slavery and forced labour. The security of a person is not to be confused with computer security or cybersecurity, which is the protection of networks, devices, and data against harm resulting from criminal or unauthorised use. In relation to organisations, countries, or assets, security merely refers to the intent to protect these entities from harm. Actions performed with the aid of computers can, however, compromise a person's right to security, for example by revealing the identity of dissidents to dictatorial regimes or by enabling cyberattacks on critical infrastructure. Cybersecurity, while not itself a right, can nevertheless be an important means for protecting rights, such as those to individual security, as well as to privacy and property. This is also expressed in the European Declaration on Digital Rights and Principles for the Digital Decade.

2.2 Equality and Non-discrimination

Equality is a foundational value based on the assumption that all people are equally valuable and thus deserve the same consideration and respect. This translates into the idea of equal rights as the foundation of human rights, which means that all people have the same legal and moral entitlements to rights like freedom, security, and privacy. It also translates into the idea of equal opportunity, according to which people should be assessed on their qualifications rather than characteristics such as gender, race, or class. Other frequently recognised principles of equality include equal access to public services, equal pay for equal work, and equal protection against discrimination. Recognising equality does not mean treating everyone the same but ensuring similar treatment in situations where people have a moral claim to be treated alike. Equality is a fundamental human right that is recognised in the Universal Declaration of Human Rights and the EU Charter.

Discrimination is unequal treatment of individuals based on characteristics that are deemed to offer no grounds for such treatment. The EU Charter includes an anti-discrimination clause that follows its clause on equality (Art. 20 and Art. 21). There is significant agreement that the qualities encompassed by these clauses include social identities and physiological features that have no bearing on someone's qualifications or deserts and that often have a history of having been used to treat people poorly. The EU Charter specifically mentions 'sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation' (Art. 21), and this list is not meant to be exhaustive. Groups of people with any of these features are called protected groups or protected classes. Actions that are typically prohibited in relation to these groups are discrimination in employment, housing, education, and access to goods and services, as well as insults, hate speech, incitement to hatred, and harassment.

2.3 Justice and Fairness

Justice is a concept closely associated with fairness and is generally defined as the fair treatment of individuals in society[23]. It requires respect for equality and declares unjust any actions that do not respect equality, such as unequal treatment of persons before the law and inequality of opportunity for job vacancies. Justice and fairness also invoke considerations of the just desert (such as rewarding or punishing individuals based on their behaviour) and

impartiality (meaning decisions should be made without bias or favouritism). Fair actions and policies respect equality, take into account what people deserve, and are impartial. As such, they are free from bias. Biases can take many forms. Algorithmic biases are social biases encoded into algorithmic decision-making. These can appear when a computer or autonomous actor is executing actions that have an impact on stakeholders. Functional biases are biases to be understood in relation to the usefulness and access of certain stakeholder groups. Policy biases are biases in policies, for example regarding the governance and management of blockchain systems. Personal biases can appear in the beliefs and worldviews of blockchain actors, which might lead to unfair decisions or prejudices.

2.4 Diversity and Inclusion

Diversity is a value that builds on the values of fairness and equality. Diversity implies that groups, organisations, and societies should acknowledge and respect people with diverse characteristics, such as different social identities, talents, skills, experiences, and viewpoints. Diversity is valued and promoted because the broader perspective it provides can offer benefits such as enhanced creativity, problem-solving, and innovation.[24] It functions as an equaliser, asserting the value of a wide range of social identities, viewpoints, and talents and creating more equity and equality of opportunity for marginalised individuals. Inclusiveness builds on the notion of diversity by supporting participation and positive valuation of diverse people with different identities. It requires continued efforts to create conditions for full participation, to value and support differences, and to create a sense of belonging.

2.5 Privacy

The right to privacy is recognised in the Universal Declaration of Human Rights, the EU Charter and in the European Declaration on Digital Rights and Principles for the Digital Decade. The EU Charter specifically refers to a right to respect for one's private and family life, home, and communications, and a right to the protection of personal data. Privacy rights are further elaborated in EU legislation, especially the 2016 GDPR, which encodes many specific privacy rights pertaining to personal data. GDPR establishes strict rules for the collection, storage, and use of personal data; it requires informed consent from individuals before their personal data can be collected and processed; it gives individuals the right to access, correct, and delete their personal data; and it requires procedures to ensure that personal data is accurate, up-to-date, and stored securely. It also severely limits the processing of categories of sensitive personal data, such as information about an individual's health, sexual orientation, political opinions, and criminal convictions, and it requires special protections for the collection and processing of personal data of certain individuals, including children, persons with disabilities, and members of vulnerable groups.

2.6 Sustainability

Environmental sustainability is the ability to meet the needs of the present without compromising the ability of future generations to meet their needs. Environmental sustainability requires serious reductions in greenhouse gas emissions, mainly but not exclusively through reductions in the use of energy generated by fossil fuels. It also requires conservation and protection of biodiversity, promotion of sustainable use of land and water, and/or reduction of pollution and waste. For businesses, sustainability requires a shift towards sustainable practices and products, such as the use of renewable energy and circular economy business models.[25]

The objective of sustainability entered EU policy in 1992 with the Maastricht Treaty,[26] and it became a core EU objective in the 2007 Treaty of Lisbon.[27] Sustainability is also recognised as a key value in ethics and in environmental awareness.[28]

2.7 Resposibility and Accountability

Moral responsibility is the idea that individuals, groups, and organisations have a duty to act in certain ways and may be held accountable for their actions and their consequences, specifically as they impact others.[29] Moral responsibility implies that these agents can be praised or rewarded if they fulfil these duties and be blamed or punished if they do not. Accountability is the obligation of agents to accept responsibility for their actions. Agents can be held accountable in a variety of ways, including legally (through laws and regulations that impose sanctions such as punishments, penalties, and liability for damages), financially (through financial reporting and auditing), ethically (through codes of ethics, standards, and guidelines, both external and self-imposed), through stakeholders (through engagement and communication with an organisation's stakeholders), and socially (through reaction to an organisation's impact on society, including its impact on the environment, human rights, and social welfare, as measured through standards, certifications, and audits).

2.8 Freedom

Freedom, or liberty, is a fundamental human right that enables individuals to pursue their interests and make their own life choices. Ethicists distinguish two types of freedom: negative liberty, which is the ability to act without obstruction or interference by others, and positive liberty, which is the ability to be one's own master and make one's own decisions.[30] Negative liberty protects individuals from unwarranted restraints on their actions and behaviours, while positive liberty implies control over one's own thoughts and decisions. Negative liberty is also called autonomy or self-governance; it is freedom of the mind, which can be possessed even if one's positive liberty is limited. The Universal Declaration of Human Rights and national bills of rights recognise a general right to freedom, as well as specific freedom rights, such as the rights to freedom of expression, assembly, movement, and employment.

2.9 Property

The right to own property is considered a fundamental human right. The UN's Universal Declaration on Human Rights states in Article 17 that everyone has the right to own property and that no one shall be arbitrarily deprived of his or her property[31]. A distinction can be made between tangible property, which has physical existence and can be touched or felt, and intangible property, which does not have a physical presence. Intangible property includes things like intellectual property, software, contracts, licenses, permits, and databases. Intangible goods that exist in digital form are called digital goods. Digital goods include any type of digital content, such as digital media, online games, fonts, logos, and apps. Ownership of many digital goods is covered by intellectual property rights. However, legal regimes are not always well equipped to regulate property rights for digital goods, so owners and buyers are not always well protected.



Blockchain systems have the potential to create more ethical environments, but a mindful assessment of ethical implications is necessary.

3 Blockchain Characteristics and Ethical Issues

Design decisions, when developing a new blockchain system (including protocols and applications), are based on the normative understanding of the architect or developer.[32] Developers need to be mindful of potential ethical impact or harm when deciding which consensus mechanisms or governance structures they implement. This is specifically important in the area of blockchain, as design decisions often are immutable and will have long-lasting implications once the system or application is in use. In this section, we present some of the ethical issues connected to blockchain characteristics that developers, investors, users, and regulators need to be mindful of.

3.1 Decentralisation

A key aspect of blockchain systems is the decentralisation of decision power. Blockchain systems allow peer communities to organise themselves without the need for a trusted third party and without centralising power in the hands of a single member. This opens new ways for communities to organise and co-create but also introduces ethical risks that need to be addressed. Some of these ethical issues are outlined below.

Distribution of governance power

When data is stored on a blockchain, the ledger gets distributed to nodes in the network. This makes the ledger largely tamper-proof, as a malicious entity needs to take over a majority of governance power to rewrite the stored data.[33] However, it is possible to create permissioned blockchain systems in which all the nodes or entities must be approved or admitted to the system by a governing body.[34] In this case, the governing body can decide how control is exercised, which in consequence means that all entries into the ledger can be revised if it is deemed necessary. In other words, tamper-resistance as known from permissionless blockchain systems cannot be fully guaranteed. Decentralisation of governing nodes is therefore an important part of permissionless blockchain systems and therefore an important element of overall robustness and security. However, the decentralisation of governance power also creates other ethical implications, such as in the context of accountability.

Life cycle of systems

Another aspect of decentralisation that needs to be addressed is how decision power is concentrated in the hands of a few during the design phase. Indeed, even though decision power is decentralised once a permissionless blockchain system is deployed, during the design phase that power is concentrated in the hands of those few people designing and developing the system. Even if they aim to create a decentralised system, developers must acknowledge the power they are exerting when making design decisions and the way that these design decisions affect the later blockchain system. Design processes should include steps explicitly focused on ethical considerations, and

developers should anticipate different stages of the lifecycle of the blockchain system under development to mitigate or minimise unintended ethical implications that may violate the very values the system was created to protect. This is especially true for permissionless systems, as the governance power on how to maintain and evolve the system will be passed from the initial developers to the community. Communities might intentionally or unintentionally evolve a system in an undesired direction[35].

Unintended use

A blockchain system may also be used in ways the developers did not anticipate during the design phase. An example is Augur, a peer-to-peer protocol that can be used to create prediction markets. Augur was created to enable a globally accessible and transparent prediction market, but in 2018, users started betting on the death of persons, effectively turning the solution into an assassination market.[36] Permissioned systems are not as vulnerable to being used in ways that do not support their original intent, as it is easier to agree and change the system compared to a permissionless system.

3.2 Immutability

Immutability is an important characteristic of blockchain systems that ensures that the distributed ledgers cannot be tampered with. Immutability is central to creating trust within the system, as the data stored on a ledger is tamper-resistant. However, tamper-resistant data storage can also cause unwanted situations if unauthenticated data enters the system[37]. Ethical issues related to the characteristic of immutability are explained in the following examples concerning oracles, digital twins, and GDPR.

Oracles

Blockchain systems depend on interfaces to operate with other blockchain systems as well as other systems. These interfaces between a blockchain and the outside world are called *oracles*[38]. Oracles are entry points where false information and failure can enter a blockchain system. There are two ways an oracle can fail: first, if the oracle is trusted and uncompromised, but the data is altered or untrue; and second, if the data is verified and true, but the oracle fails to operate due to bad code or deliberate tampering. For instance, if a smart contract is activated to execute an international transaction, it will interact with an oracle to get information, for example, on current exchange rates. When oracles provide publicly available information, like exchange rates, the information can be checked by participating parties in the transactions. However, when transactions depend on information that is not publicly available, it becomes harder for the involved parties to verify the data. Blockchain systems must have trusted oracles providing verified data to keep the whole blockchain ecosystem safe. Even though data can be stored safely on immutable ledgers, this does not guarantee that the transactions archived are representing a true state. Trustworthy oracles and verification procedures are needed to ensure that only true and verified data enters a blockchain system.

Token as digital twins

Blockchain systems also deal with digital twins, which are representations of physical entities or assets, such as cars, gold, paintings etc. In the sale of a car, for example, a token representing the ownership of a car (the car's digital twin) is transferred from one wallet to another once the payment has been made; however, the physical car must also be transferred to the new owner.

The transfer of ownership is stored safely on an immutable ledger, but the blockchain system has no mechanism for controlling or enforcing the transfer of the actual physical goods. In the event of not receiving the physical goods that have been paid for, the wronged party needs to rely on entities outside the blockchain system, for instance, the police, to enforce their ownership.

Another issue related to digital twins occurs when digital representation does not match the physical entities. For instance, you might have a token representing your university degree stored on an immutable ledger, but the information is incorrect. Or a company advertising its sustainable practices might use tokens to track a bag of organic coffee beans across the supply chain when the actual coffee beans have been replaced with non-organic coffee beans. Such scenarios can create ethical issues: Individuals may be treated unfairly (for example, denied a job for which they are qualified), or consumers may be cheated into buying products that have not been sustainably produced. If the digital twin problem is not addressed, blockchain systems might cause unjust treatment of individuals or undermine trust instead of increasing it.

General Data Protection Regulation (GDPR)

Finally, the characteristic of immutability can cause ethical issues and violate GDPR if private data is stored directly on a ledger. Article 17 of the GDPR states, 'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay'. It is difficult (in case of permissioned blockchain systems), or impossible (in case of permissionless blockchain systems) to delete data once it has been stored on a ledger, which is why sensitive and private data should not be stored directly on a ledger.

3.3 Transparency and Distribution

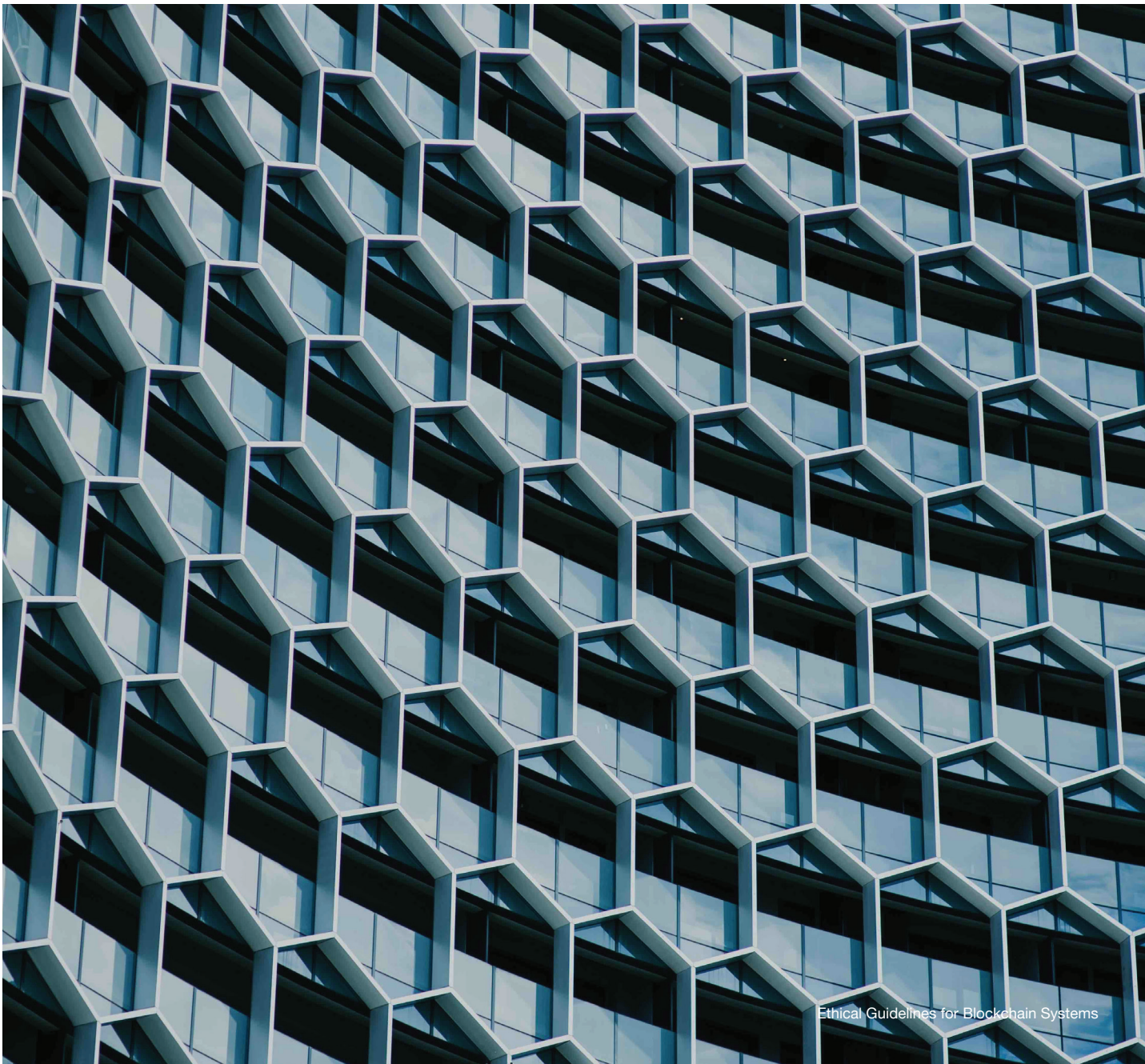
Blockchain's transparency and the distribution of data in a peer-to-peer network are key to its security; however, these qualities can also cause ethical issues if unsuitable data is shared. In the following section, we will focus on nodes that can read data and nodes that store a replica of the ledger.

Sensitive data

Once transactional data is stored on a ledger, it is visible in the network. This is in part what safeguards entries on a blockchain ledger against fraudulent activities, as the nodes can compare the stored ledgers and detect if a change has been attempted. But this transparency can cause ethical issues if the data stored in the network is sensitive. This is especially true for permissionless systems where anyone can operate a node and where it is difficult to control which type of data users store on the ledger. Blockchain systems store a hash of data on ledger as a way to authenticate sensitive data while keeping it confidential. This way, it is possible to check for example if a digital driver's licence is coherent with the hash released by the issuing authority. If a driver's licence has expired or been revoked, it will no longer fit the hash and will not be authenticated. As hashes stored on a blockchain ledger are protected from tampering, it is next to impossible to change the data entries stored off-ledger without being detected. It is worth noting that a hash of personal data is considered to be personal data, too, which means that all blockchain systems have to find a way dealing with personal data in a GDPR conform way.

Ledger distribution

Blockchain systems rely on having multiple nodes authenticating transactions and keeping replicas of the ledger to secure the whole system from malicious tampering. However, if data not eligible for sharing gets distributed it can create problems for the nodes maintaining the system and storing a replica of the ledger. If illegal or inappropriate content gets distributed, entities acting as nodes may inadvertently store illegal content on their hardware, for which they could be legally liable in many jurisdictions[39]. This risk may make entities unwilling to act as nodes. It is essential that operating nodes can be certain that they do not violate legal norms when maintaining the system. These ethical and legal issues, therefore, need to be addressed.



3.4 Auditability and Accountability

Blockchain systems offer new ways of organising networks, which may create challenges in placing accountability and responsibility. Without clear guidelines and well-described enforcement methods, blockchain systems may not be able to uniquely identify involved entities to hold them accountable. When governance is decentralised and executed pseudonymously in blockchain systems, locating accountability can be extremely challenging[40] compared to more traditional IT systems, which have centralised power structures carried out by well-defined entities. This is especially true for permissionless blockchain systems, where nodes can read, submit, and validate transactions pseudonymously. In permissioned blockchain systems, it is easier to place accountability (as nodes are identified and verified), compared to permissionless systems. The following sections outline ethical issues connected to accountability in blockchain systems.

Data

Only eligible and correct data should enter a blockchain system. However, in permissionless systems that allow for pseudonymity, it can be hard to ensure accountability if a node enters untrue or sensitive data as it can be difficult to identify the natural identity of the person or company operating the node. Blockchain systems provide auditability of transactions, but how to hold those adding inappropriate information on a ledger accountable for their actions, if they cannot be identified? And should the nodes storing the ledger be held accountable for the content? In permissioned systems, it is easier to make processes to ensure the quality and nature of the data before it is stored, as the entities maintaining the system are identifiable and have been vetted before becoming part of the system. It is, therefore, easier to determine accountability and responsibility in permissioned systems.

Code

Accountability should not only be addressed in the context of data, but also in the context of code. Blockchain-based applications can facilitate essential infrastructures in society without citizens needing to be aware of the technical layer. Weak code might cause unintended harm for users if misused, or if automatically executed. In a permissioned system, the developers and entities maintaining the system can be held accountable for flawed code, but how to place accountability in permissionless systems? Is it the person writing the code who is accountable? Or is it the person choosing to use the application? In permissionless systems, anyone with the right skills can check the code for flaws and weaknesses. However, most citizens will not have the technical know-how to read or authenticate the code used in blockchain systems. This creates ethical issues if the security of blockchain systems is based on volunteer checks from users while only a small number of users have the skills needed to perform these quality checks.

Autonomous actors

It can be difficult to ensure accountability in blockchain systems, not least due to their use of code as autonomous actors, such as smart contracts. A flawed smart contract will execute actions according to its code, despite those actions having unintended harmful outcomes. Malicious users might exploit smart contracts with bad code to gain advantages at the expense of the network. In blockchain systems that include technologies such as artificial intelligence (AI) and data from the Internet of Things (IoT), the complexities around accountability increase.

Finally, accountability may be defined differently in various jurisdictional environments, and with blockchain systems spreading across different countries, accountability in one country might not be enforceable in another. This spanning of jurisdictions has both legal and ethical significance. New ways of defining and ensuring accountability in blockchain systems consisting of autonomous actors and agents are needed.

Tokenisation

Blockchain systems not only allow users to interact without a trusted third party, but they also facilitate value creation and capture of cryptographic tokens[41]. An example is cryptocurrencies that function as money without the participation of a government or bank which raises accountability questions. Sometimes a token is not intended to be used for payment but is designed to be used only internally in a blockchain system as a utility token that provides some service to users such as access rights or membership verification. However, tokens, including utility tokens, may be used in unintended ways[42]. An example is Ether (ETH), the Ethereum utility token, which was repurposed by the user community as a payment token. Adapting tokens for purposes they are not developed for can create unforeseen consequences for users. How should payment tokens and token systems be regulated to protect citizens and the financial system from harm? Are there areas where tokenisation should be outlawed because of the risk of dangerous incentives or unintended consequences? Decision-makers must address such questions to prevent unintended harmful effects on society.

Interoperability

Scalability has consistently emerged as a notable technical hurdle for blockchain systems. The capacity to process transactions efficiently can be limited by factors such as the consensus algorithm used to verify the ledger. An effective approach to address this concern involves promoting interoperability among different blockchain systems. This is achieved by establishing bridges that facilitate the transfer of tokens to other blockchains. Doing so may allow for transaction offloading and thus heightened system adaptability[43]. However, although it is possible to track and trace tokens and transactions within a single blockchain system if tokens or assets are transferred to another blockchain system, they become hard if not impossible to trace, which may lead to accountability issues.



Ethical guidelines for blockchain systems are needed as they may alter the way we interact as societies.

4 Ethical Guidelines for Blockchain Systems

1. Guideline to Ensure Fairness
2. Guideline to Protect Privacy
3. Guideline to Assure Security
4. Guideline to Allow for Accountability
5. Guideline to Guarantee Societal Responsibility



4.1 Guideline to Ensure Fairness

Blockchain systems can distribute governance power in a network, as long as the entry barrier is low enough for all users interested in participating. However, if steps are not taken to ensure open access, governance power may only be distributed among those with the necessary technical skills, capabilities, or resources. If only a small group of technically capable individuals are involved in the design and maintenance of blockchain systems, the risk of unintended bias and discrimination increases, as some stakeholders and their views and needs might not be included. It is important to ensure inclusion and open access to counter and mitigate bias and to distribute governance power in blockchain systems as much as possible.

Open Access

Blockchain systems offer important social and economic benefits that should not be denied to anyone. However, social and functional biases can exist in blockchain design, governance, and operations; these biases can disadvantage certain stakeholder groups by discriminating against them or posing risks to them or their rights. Such biases should be mitigated through targeted bias correction procedures. Developers designing blockchain applications to be applied cross-border in Europe or globally must reflect on aspects such as accessibility, usability, incentive mechanisms, or unintended bias. This is to ensure fair and equal access and to prevent unintentional discrimination against certain groups, such as people with limited technical experience or those from a cultural setting other than the developer's. Blockchain applications should be accessible for use by anyone, regardless of their education, income, resources, abilities, socioeconomic status, and other attributes (gender, race, ethnicity, nationality, age, sexual orientation, and others). Special efforts should be taken to ensure that blockchain applications are low-cost and easy to access, including for those with slow or unreliable Internet access. Applications should also be easy to use for individuals with little formal education or limited technical skills and be accessible for people with physical or mental disabilities through accessibility settings and assistive technology.

Governance Power

Governance power should be distributed fairly, making it impossible for a single user or stakeholder group to take over or manipulate the system. Entities involved in the governance of blockchain systems should represent the diversity of the group. Steps should be taken to ensure the participation of members of underrepresented groups, especially those with limited technical skills, low incomes, and modest resources. The goal is balanced participation in terms of gender, race, ethnicity, age, (dis)ability, and other social identities, especially for blockchain systems implemented by governments and to be used by citizens.

In a permissioned system, the governing body is known, which makes it possible to ensure a distribution of power among the blockchain system' participants, granting, for instance, the same governance power to each country, company, or person participating. As the nodes are identifiable, it is possible to be mindful of the distribution of power in relation to geography and culture. It is also possible to invite entities or persons into the network to ensure inclusion and a fair distribution of power across all stakeholders of a blockchain system.

In permissionless systems, the governing nodes can be pseudonymous, and thus it can be difficult to identify if decision power is centralised (as one entity or company potentially can operate many different nodes) or if it is distributed fairly.

When blockchain actors have biased beliefs and attitudes they may make prejudiced or unfair decisions. This can be mitigated by ensuring that teams represent a wide range of viewpoints and interests and by monitoring for conflicts of interest, such as financial, personal, professional, or political interests that could influence decision-making. In addition, blockchain policies are potential sources of bias. Policy bias in the governance and management of blockchain systems can directly or indirectly create unfair conditions for stakeholders. Policies, as well as actual practices, should be regularly assessed and corrected for bias.

It is recommended that designers of permissioned systems ensure that political, economic, geographic, and cultural interests are taken into account when distributing the governing nodes of the system. System designers should also consider the needs and interests of all stakeholder groups when selecting the entities that will operate the governing nodes. In systems providing public services to citizens, designers should consider whether the governing nodes should be operated by public agencies or private companies.

For permissionless systems, it is recommended to develop risk management procedures to identify unequal distributions of power that may develop over time. If governance power becomes centralised, systems should have action plans in place for how to incentivise and re-establish decentralisation. Academic researchers would do well to investigate how decentralisation of decision power can be maintained throughout the life cycle of a blockchain system. Validator pools (mining pools as well as staking pools) should be accessible for users with modest technical skills and limited resources, if possible.

Life Cycle

Blockchain systems can facilitate distributed governance power among peers in a network. However, in the development phase of a blockchain system, the governance power is naturally centralised with the developers. Once a blockchain system is deployed it can be very difficult to change. The decisions made in the design phase are therefore often long-lasting and will affect the blockchain system throughout all its life cycles.

Therefore, designers must be alert to the danger of introducing algorithmic biases. Such biases can exist, for example, in algorithms that select validators, process and prioritise transactions, or determine and distribute assets. These biases should be mitigated through algorithmic fairness procedures similar to those that have been developed for AI and big data and through continuous monitoring and testing.

In addition, designers of blockchain systems should incorporate incentive mechanisms that discourage selfish behaviour and encourage network-preserving actions. However, life cycle governance is more than algorithmic fairness procedures and incentive mechanisms. Developers must also reflect on how to support the network in self-organising. What to do if the system is being used to violate the very values it was created to protect? How to react if the system is attacked? Should it be possible to make a hard fork? And how should hard forks be facilitated? How to facilitate communication among peers in the network? And how to migrate to other blockchain systems if the current one is made liable or needs to be shut down? These are some of the questions that developers need to address before releasing a new blockchain system.

It is therefore recommended that developers reflect on the life cycle stages of a blockchain system and how later versions of a blockchain system might impose new ethical risks and challenges to the network. Development processes should include steps to allow for reflections on impact and ethics. This is especially essential for permissionless blockchain systems, as these are hard if not impossible to change once implemented. Developers should also be mindful of addressing the needs and interests of other groups in all life cycle phases to avoid discrimination and to support inclusion. It is recommended that education, frameworks, processes, regulation, and software be developed to support blockchain developers in the design phase, to ensure that moral values are sustained throughout all life cycle stages of a blockchain system.

4.2 Guideline to Protect Privacy

Due to the tamper-immutable, transparent, and distributed ledgers of blockchain systems, guidelines and audit processes are needed to control the correctness of data and ensure that only eligible data is stored directly on a ledger. In the following, guidelines are presented to protect citizens and users of blockchain systems and to avoid systems that violate the EU values of privacy.

Sensitive Data

Private and sensitive data should always be stored securely and be accessible only by authorised persons. No sensitive or private data should be stored directly on a ledger (especially in permissionless systems), as that data will be shared with all nodes in the network. Audit processes should be created to determine which types of data a system should store as well as checklists for users to ensure that no sensitive data is stored directly on a ledger. One way to use blockchain to authenticate personal and sensitive data is to store a hash of the data on a ledger while keeping the data itself safely stored in a secure database.

In situations where users have little or no option to decline participation, such as post-disaster assistance or medical assistance following accidents, it is even more crucial that developers and governing entities assume responsibility for protecting users' personal data. Developers and operators of blockchain systems should refrain from supporting use cases that are likely to violate the privacy of users or other stakeholders, such as blockchain applications for surveillance, unethical tracking, and monitoring.

In addition, biometric data should not be stored directly on a ledger, as such data is a permanent personal indicator. It is recommended that regulators determine which types of data are suitable or unsuitable to be stored in blockchain systems. These regulations should be adjusted to the different types of blockchain systems, including who is controlling them and how they are used. Third-party accountability structures should be put into place to enforce and uphold these regulations. Checklists based on these regulations should be developed for users to identify which data to store off-chain and which use cases to avoid. Developers should create audit processes to check the nature of data before a transaction is approved. They should also develop mitigation strategies to deal with situations where sensitive data is wrongly stored.

Pseudonymity

Pseudonymity can be used to protect users' privacy and safety, as well as to protect the freedom of speech in regions where citizen opinions are censored. The digital infrastructures of society must empower users and protect them from surveillance of both private and public entities. Pseudonymity, therefore, plays an important role in protecting user privacy. However, pseudonymity can also be used to conduct harmful or illegitimate transactions and it is important that law enforcement entities be able to investigate harmful or illegal behaviour. Therefore, it is recommended that risk mitigation processes and -software be developed to monitor the transactions in blockchain systems, especially in public-permissionless systems with pseudonymous users. This is to identify malicious users conducting illegal transactions. Tracking of transactions can be used as an indicator of illegal structures and entities, even when conducted via pseudonymity. Law enforcement entities should be educated in investigating and tracking illegal transactions in blockchain systems. On-chain and off-chain processes should be put into place, to address and prevent illegal actions. However, it is important, that there is a legal claim before any such process is activated. Regulating bodies should protect the privacy of law-upholding users while enabling law enforcement methods to pursue illegal behaviour.



4.3 Guideline to Assure Security

It is important that blockchain systems be secure, especially systems facilitating essential social processes and infrastructures. The security of blockchain systems is not only important at the network layer but also for users depending on the system, for instance for blockchain-based public processes, for example, vaccination verification. As blockchain technology becomes more integrated into private and public processes, it is important to ensure the overall security of the blockchain system. All stakeholder groups of blockchain systems should benefit from the highest standards of security, from the protocols to the applications.

Nodes

Network security depends not only on the decentralisation of power among nodes in a network but also on the overall number of nodes and the consensus algorithm in use[44]. With a smaller number of nodes or different consensus algorithms, it becomes more likely that power will be centralised. Therefore, in permissionless systems, it is advisable to have a high number of nodes maintaining the system. In permissioned systems, the node operators are known to the other network participants. A malicious node is therefore aware of the entities they need to influence, to take over the network power. However, the malicious node itself is also identified, and the network can isolate or exclude the malicious node if it proposes actions that endanger the system. In permissioned systems, the number of nodes needed depends on the trustworthiness of the entities controlling the nodes. Having fewer trustworthy entities in a network, therefore, creates a need for a greater overall number of governing nodes.

In permissionless systems, it is not required for node operators to be identified, as they can operate pseudonymously. However, this does not mean that entities controlling nodes cannot organise themselves in traditional hierarchal power structures off-chain. Powerful companies or governments might set up multiple nodes to increase their decision power or they might collaborate with other powerful entities to pool their influence on the network. Entities in permissionless systems should therefore not only be aware of the governance power of an individual node but also alert to off-chain centralisation of power evoked via multiple nodes. Permissionless systems should also establish methods to identify off-chain centralisation of power and determine whether coordinated efforts are being made to influence a system via multiple nodes.

Academia should be involved in the process of identifying the desirable number of network nodes and determining when this number becomes critically low. Both permissioned and permissionless systems should distribute governing nodes to ensure the robustness, resilience, and security of blockchain systems. Permissioned systems should perform due diligence checks before permitting entities to act as governing nodes. Citizens should have the option of having their data processed via nodes that are government-controlled and not be forced to rely solely on nodes controlled by private entities. The distribution of governing nodes is therefore especially important in blockchain systems created by public agencies, as citizens often have no alternative to using these systems. In addition, the physical location of servers must be considered. Governing entities need to protect their nodes from hacking, deliberate damage, and physical threats such as flooding or fire. To ensure the network's safety, all server nodes should be kept safe from unauthorised individuals and accidents. To ensure the full security of the servers, they should be placed only at physical locations controlled by trustworthy parties.

Quality of Code

The code used in blockchain systems must be secure and without weaknesses, flaws, or biases that can cause unintended negative effects. For instance, entities with malicious intentions could take advantage of code weaknesses and exploit the system for individual gain or a flawed or biased smart contract could harm users as it is executed autonomously. In scenarios where essential infrastructure is blockchain-based, it is even more important that the code meets high quality standards and best practices. International standards for code quality should be established for all blockchain systems and processes as well as robust processes and structures for auditing code. The auditing of code should be done by qualified and accountable entities and should be conducted by more than one entity, to minimise mistakes and deliberate tampering. Developers should always have their code validated before implementing it. International code certifications should be developed to help stakeholders chose safe blockchain systems and smart contracts. Regulators should establish minimum security demands for code quality and support auditing entities doing quality checks.

Verifying Data

A blockchain system cannot automatically verify new data entries. It is therefore essential that data be authenticated before it is entered into a system and distributed to the network. If incorrect data makes its way into a blockchain, it can create unjust situations and cause mistrust of the whole system. As a blockchain system has no built-in way of verifying new data entries, the validity of recorded data must come from a third party outside the blockchain system. For example, new entries in a real estate ledger tracking property ownership could be entered by a public authority responsible for the correctness of new data. Once the data is correctly recorded, the agency can set up approved smart contracts that will automatically execute the transfer of ownership when predefined settings are met. When data is authenticated and stored securely on a ledger, the overall trustworthiness of real estate ownership can be increased.

In permissioned systems, it is important to determine who is allowed to enter new data into a system. Only trusted persons and approved actors should be allowed to enter new data. Permissioned systems should perform data security processes defining access rights and have checklists for new data entries. They also should establish maintenance processes for actors (such as IoT devices) feeding new data to the system. Lastly, they need to have mitigation strategies in place in the event that incorrect data is recorded on the ledger.

n permissionless systems, anyone can enter new data entries into the system; therefore, the validity of the data cannot be guaranteed by the trustworthiness of the people and actors who enter it. However, off-chain authentication processes can be used for both permissionless and permissioned systems. Off-chain authentication processes should be adjusted to the data that is being stored. In some cases, data can be authenticated simply by adding geolocation data. In other cases, spot checks or a physical inspection might be needed to confirm the correctness of the data.

Traceability, Transparency, and Interoperability

Part of what makes blockchain systems trustworthy is the transparency of transactions. However, interoperability between chains can compromise the traceability of transactions and hereby the transparency. If a token is created on one blockchain and then transferred to another, the trace of the token and how it is being transacted outside the original blockchain system becomes opaque. On the other side, interoperability between chains can protect users from being locked into platforms and digital siloes. Interoperability might also be useful if a system has been compromised or become outdated, and applications might need to migrate to a new blockchain system to ensure, for instance, user security or usability.

As there are many advantages of interoperability between chains, blockchain-based applications and processes might end up being based on multi-layered protocols involving multiple blockchains. In such scenarios, it is especially important to ensure traceability between blockchain systems, so that the transparency of transactions is not compromised. Structures should be put into place to allow traceability between blockchain systems by adding the destination to the token when it is transferred[45]. Standards should also be developed to ensure interoperability without compromising traceability.

4.4 Guideline to Allow for Accountability

Blockchain technology facilitates and enables peer-to-peer networks and value creation in blockchain systems. These networks have the potential to disrupt existing business models and economic structures. They also enable new ways of creating and capturing economic value and public goods. It is important that regulation keep up with the new opportunities provided by blockchain technology.

Value Creation and Tokenisation

Cryptographic tokens can be used in numerous ways, from granting access and facilitating transactions to proving ownership or reputation. They can also be used to incentivise actions, both in and outside of blockchain systems. In other words, tokens can have substantial economic value and thus offer potent incentives that can alter or assure certain actions and behaviours.

Tokenisation should only take place in circumstances that create incentives that are in line with the law and European values; it should not incentivise actions that are harmful or illegal. However, tokens are sometimes repurposed by the community and used in ways they were not designed for. This makes it difficult to predict how a token will incentivise actions in the community and society. It is important to ensure that tokens are designed specifically to fit their intended use and that they are not reused in different contexts. Developers of tokens should be in close and continuous dialogue with decision-makers to ensure that legal frameworks are up to date with the current developments within this area. We recommend that governments create regulatory sandboxes as a test environment for innovation and regulation where stakeholders such as companies, public authorities, and researchers can gain experience. This will ensure that regulation is up to speed while also protecting blockchain innovation in the European market. It is also advisable to have clear ethical guidelines for tokenisation, addressing all the various ethical issues of development, release, and use. These guidelines should be specifically targeted to users, investors, developers, and regulators.



Ownership

Policies, regulations, processes, and practices for blockchain that pertain to ownership and property rights should be designed to protect the rights and interests of all stakeholders, including owners, non-owners, buyers, sellers, leasers, renters, investors, insurers, and society at large. In particular, the rights of owners and buyers of blockchain-enabled assets should be protected. This requires adequate safeguards against fraud, theft, double-spending, network and price manipulation, denial of network access, network termination, smart contract bugs, and misrepresentations of fair value. Policies and procedures for wealth generation through the use of blockchain and blockchain-enabled assets should not exacerbate economic inequalities in society and should be in accordance with the principles of fairness and non-discrimination outlined in this document. And finally, proper safeguards should be put in place against the misuse of blockchain-enabled assets for purposes like money laundering, tax evasion, and other criminal activities. Tokenisation of assets that are subject to legal or regulatory restrictions, such as controlled substances and human tissues, should be restricted or banned.

4.5 Guideline to Guarantee Societal Responsibility

It is important that blockchain systems design be mindful of potential impact and large-scale consequences for society. How might blockchain applications disrupt existing business processes and structures in society? How can blockchain systems support value creation that supports sustainable and social change? How can tokenisation and decentralised value creation help drive sustainable and prosocial change? Are there actions that should be illegal to tokenise (like selling human organs)? These are some of the questions that developers, investors, and regulators must address, to ensure that the blockchain systems and applications they endorse will protect and enhance our societies and humanity.

Sustainability

Developers and operators of blockchain systems should respect and ensure sustainable targets and values when designing and operating blockchain systems, including overall Environmental, Social, and Governance (ESG) impact. These include a focus on reducing energy consumption, reducing the amount of data storage, reducing digital waste, and considering sustainability criteria in all innovation and investment decisions. Energy consumption can be reduced by moving away from proof-of-work consensus mechanisms to alternative methods and by optimising the network design. Excessive data storage and digital waste can be reduced by implementing off-chain solutions and refraining from storing unnecessary data on a ledger.

Developers and operators should also focus on developing blockchain systems that support sustainability. Examples include decentralised energy systems, transparent supply chain systems supporting sustainable product sourcing, sustainable finance solutions, tokenisation incentivising natural environmental protection, and transparent tracking of carbon trading systems. When tokenisation is used to incentivise green actions, such as carbon reduction or nature preservation, it is recommended that independent auditing processes be employed to ensure that tokens are not used for greenwashing or similar deceptions. More research should be conducted into how blockchain technology can be used to drive the sustainable agenda and empower sustainable actions.

Democracy

Blockchain systems may serve to protect democracy and democratic values such as freedom of speech from censorship. However, it could also facilitate the creation of immutable databases of sensitive data used to persecute minorities or to keep populations under surveillance. All stakeholders in blockchain systems must ensure that the protocol, network, and application layers all support democratic values and practises. Blockchain systems should be used to empower citizens and users, not to undermine or dehumanise them. It is important that blockchain systems not weaken or destabilise democratic processes. On the contrary, blockchain systems should be used to minimise corruption and undemocratic control on the part of public institutions. Network participants should have ways of objecting to the overall system and suggesting changes. It is important that developers and regulators reflect on how network participants can coordinate communication to ensure that vital information is shared with all decision-makers. If communication is only done at random in off-chain communities, some network participants might end up having incomplete knowledge before voting on changes in the system.

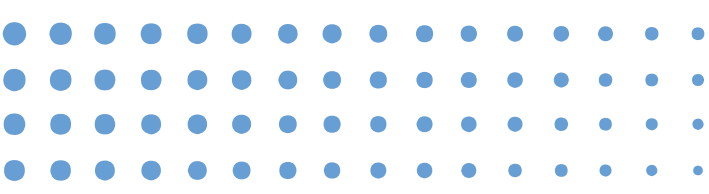
Users of blockchain applications should have ways of objecting to the decisions made by the network community. External entities should be mandated to investigate blockchain systems that are suspected of being unjust.

This is especially true for permissioned systems, which have the power to exclude stakeholders from decision power. Third-party structures, with no conflicting interests, should be put into place to assess blockchain systems and ensure that they uphold the law and moral values and protect democratic processes. Additional research into the societal and democratic impact of blockchain systems should be promoted.

Risk Mitigation

It is recommended that all blockchain systems and applications are subjects to risk assessments. As widely used blockchain systems may have large social implications—for example, when humans invest their savings in tokenised digital assets—developers and operators should consider a social impact assessment in collaboration with other involved stakeholder groups before introducing a new blockchain system or application. Such an assessment should comprise different impact analyses, on the labour market, financial systems, political systems, and other relevant social institutions and practices affected by the proposed system. Blockchain applications should only be developed and deployed for use cases that adhere to standards of fairness, equality, inclusion, and non-discrimination.

Applications should not be developed or deployed for use cases that are known to be unfair or discriminatory or that exacerbate inequalities. In addition, assessments should be made of possible uses that could have unfair or discriminatory consequences, and mitigating actions should be taken in design and governance to decrease the likelihood that such consequences materialise. Focus should be on developing blockchain-based applications that promote equality and justice, such as applications that provide access to financial and other services for marginalised communities, supply-chain tracking for fair trade, record keeping for humanitarian aid, and land title registration for vulnerable individuals and groups. To ensure risk mitigation in blockchain systems, rules and regulations should be implemented to determine stakeholders' rights and duties. Procedures, both technical and legal, should be created to allow redress. Groups and organisations co-creating blockchain systems and applications should have the duty to accept complaints, assign and accept responsibility, apply sanctions, award compensation, and take preventative measures against future harm.



Blockchain systems have the norms and values of the developers embedded. Specifically for systems used to provide public services, ethical values embedded should be explicated when the system is deployed.

5 Ethical Implementation of Blockchain

The high-level guidelines presented above apply to all actors and should be considered during the development as well as the deployment of blockchain systems. In the following, we discuss how actors can implement these guidelines in their practices.

Operationalising these guidelines is best done through relating them to specific practices involved in blockchain systems, such as development, deployment, use, regulation, certification, and others. For each of these practices, the challenge is to translate high-level principles into norms and recommendations for that practice. This can be achieved in two steps.

Step one is to determine how a guideline applies to a specific practice. Key questions include how and to what extent the practice can contribute to the realisation of this guideline. Moreover, it should be determined if actors responsible for the practice have a special responsibility to realise the guideline, for example, due to pre-existing regulations, laws, or agreements.

For example, the guideline on open access states that blockchain systems should be accessible for use by anyone regardless of their level of education, income, resources, abilities, and socioeconomic status. Step one is to ask how the specific practices of (say) blockchain development contribute to this overarching principle. What are the responsibilities of blockchain developers in this area?

Step two is then to propose a norm that codifies the general implications of the high-level guideline for the practice. For example, if the guideline is that blockchain systems should be accessible by anyone, a norm for deployment could be that in acquiring a blockchain system, priority should be given to systems that are broadly accessible, and that no system should be deployed that has poor access conditions. In the case of the regulation of blockchain systems, a norm related to the accessibility guideline could be that regulators should determine whether access to a given blockchain systems is best protected by law or by industry self-regulation.

An optional next step is to work out more specific recommendations and procedures that pertain to specific actors involved in the practice or to specific phases or elements of the practice. For example, in the practice of development of blockchain systems, the open access norm could go on to identify social groups that currently face access barriers and work out development strategies that can overcome these barriers. This could also involve instructions and procedures for specific actors involved in the development process and specific phases of development.

However, implementation is not just a matter of translating high-level guidelines into mid-level norms and then into detailed protocols and recommendations, but also of having an integral plan for motivating and educating the actors who are involved in implementation.

These could include the anchoring of the ethical guidelines to the overall strategy of the organisation, including already adopted ethics codes and guidelines and corporate social responsibility strategies. Furthermore, it requires the allocating of resources for the implementation of the guidelines. Another important part is to consider how the implementation of the guidelines will affect other aspects of the organisation's management strategy, including quality management, risk management, and others, and ensuring proper adjustment of these processes. To mitigate any potential ethical issues, one should consider developing roles, responsibilities, and procedures for implementation of the ethical guidelines and for monitoring and assessing their implementation. This could include the institution of an ethics officer or an ethics task force or unit, assigning specific responsibilities for implementing or monitoring the implementation of ethical guidelines, as well as identifying ethics and impact checkpoints in development, implementation, and operation processes. To achieve this, developing and implementing training programs for ethical practice in relation to the guidelines might be necessary and helpful.

As an ethical implementation of blockchain systems may come with unforeseen challenges, or has to deal with changing issues over time, one should promote an industry-academia collaboration and ongoing research. This incudes also to establish a common culture of responsibility with respect to the guidelines, as well as the development and implementation of strategies for monitoring performance, conformance, and compliance with the ethics guidelines, as well as considering the guidelines' role in auditing and assurance processes.

Actors should also consider developing joint implementation strategies with others. For example, developers, node operators, validators, service providers, and standards, governance and industry associations could collaborate on a general implementation strategy that allows them to pool resources and expertise and make use of the division of labour.

Some approaches have been developed to help organisations implement ethical guidelines in their blockchain-related practices[46]. For design and development, the approach of Ethics by Design could be used. This is an approach for the systematic inclusion of ethical criteria at different stages of the development process of technological products and systems. This approach has been developed in detail for AI,[47] as well as for other technologies[48].



Research on how to measure the implementation and management of ethical values in blockchain systems is needed. As new blockchain use cases are emerging, research and regulation must keep up.

6 Outlook

This report identifies ethical issues related to blockchain systems and presents ways of addressing them. However, as blockchain systems can facilitate a multitude of applications and use cases, each of the ethical issues presented in section 3 could benefit from being researched individually. We recommend that developers and researchers use these ethical guidelines as a foundation for reflecting on the presented ethical issues in specific contexts and for individual user groups.

More work is needed to dive deeper into the ethical issues presented here and to account for new blockchain-based use cases as they develop and issues that have not yet come to light.

Some issues seem particularly urgent for ongoing investigation. For example, the ethical challenges related to accountability: How to place and enforce accountability in permissionless blockchain systems based on open code and self-executing smart contracts? If processes and structures are co-created without having a single entity in control, then where to place accountability if something goes wrong? How to mitigate risk and protect users, if the system is immutable and no single entity has the power to change it?

Another important topic to investigate more deeply is how blockchain systems are used to co-create value, for example through the use of tokens. Cryptographic tokens need to be subject to intense ethical and legal reflection and regulation, as they have the potential to disrupt existing economic as well as societal systems. An individual set of guidelines addressing tokenisation and blockchain-based value creation would be relevant and appropriate.

In addition, these guidelines have not specifically touched upon the phenomenon of Decentralised Autonomous Organisations (DAOs). It is likely that new types of self-governing organisations will emerge in the future. Organisational research must keep up with these new types of organisations, to explain their workings, benefits, and weaknesses. This knowledge is needed to guide and protect DAO stakeholders and to enlighten and support regulations regarding these new organisational structures.

It is also important to reflect on the autonomous actors incorporated in blockchain systems, such as smart contracts. As digital systems evolve from being reactive automatic to proactive autonomous, algorithmic actors are increasingly operating in an open network with no data controller. The risk of unforeseen harm to or discrimination against users must be avoided. It is also relevant to consider other technologies that might exist in a blockchain system, such as IoT devices and AI. Digital systems based on multiple types of technologies and autonomous actors must be carefully thought through, lest they result in autonomous systems operating outside human control with the potential to violate societal values and norms.

Research on how to measure the implementation and management of ethical values in blockchain systems is needed. As new blockchain use cases are emerging, research and regulation must keep up, so that new technological structures will embed the values of society and take into account the overall consequences for society.



This report creates a baseline for future blockchain innovation by supporting the implementation of EU values in blockchain systems. It takes the first step by identifying ethical issues and presenting ethical guidelines for blockchain systems.

7 Conclusion

This report presents ethical guidelines for blockchain systems as defined by the EGBE under a mandate from the EBP. The ethical guidelines are specifically created for blockchain systems and are based on the values of the EU.

Blockchain systems have the potential to become the backbones of societal as well as economic transactions, providing considerable benefits to citizens and users. Blockchain systems include (but are not limited to) value creation and capture, peer-to-peer organisations, self-sovereign identities, transparent supply chains, sustainable business models, and safe online transactions. They should empower citizens and society and help facilitate the social and sustainable changes needed to protect and uphold the values of the European Union.

However, blockchain systems can also create unforeseen ethical issues, especially when allowing peer-to-peer networks to create common goods and public goods. These ethical issues related to blockchain systems are unprecedented, especially in the context of accountability, as no single entity controls or owns the blockchain network. With no central controlling entity, immutable systems set a high demand on developers — they are the ones who must reflect on how a system can be used or misused before releasing it. New ways of enforcing accountability in digital peer-to-peer networks must be identified and developed to protect citizens and to ensure that blockchain systems are ethically sound and safe.

This report creates a baseline for future blockchain innovation by supporting the implementation of EU values in blockchain systems. It takes the first step by identifying ethical issues and presenting ethical guidelines for blockchain systems.

It is worth noting that these guidelines do not address a specific type of blockchain system but are considered to be general guidelines that can be used for permissionless and permissioned blockchain systems alike.

Europe has a unique cultural setting that places the user and the individual at the centre, not governments or private companies. This user focus should also be implemented into blockchain systems, as blockchain technology has the potential to enhance the digital self-sovereignty of European citizens. As Europe is aspiring to protect its digital sovereignty, the EBP has a unique vantage point not only for protecting digital sovereignty but also for developing EBSI, which is being developed and implemented fully considering the protection of European values and norms. The ethical guidelines will also empower European blockchain start-ups and scale-ups to create blockchain systems that strengthen digital sovereignty and reinforce European values.

This report identifies ethical issues and guidelines for blockchain systems in a European context. It puts a spotlight on the field of blockchain ethics and encourages researchers and practitioners alike to dive deeper into the ethical issues presented. The application areas of blockchain systems are manifold, and we have not yet seen the full potential of this technology.

As blockchain technology is still evolving, it is important that ethical reflections keep up with that development. How blockchain technology will influence society will depend on both regulation and the inventiveness of the blockchain community. These guidelines help sharpen our ethical understanding of blockchain systems with an intent to drive innovation for a sustainable and sovereign digital future.



8 Contributors

This report was written by the Convenors and the EU Expert Group on Blockchain Ethics.

Convenors

Roman Beck
Full Professor at the IT University of Copenhagen, Head of the European Blockchain Center

Signe Agerskov
Researcher at the IT University of Copenhagen, Member of the European Blockchain Center

Expert Group Members

Monique Bachner
Independent Governance Advisor & Non-Executive Director, INATBA Blockchain Standards Committee

Philip Brey
Full Professor in Philosophy and Ethics of Technology, University of Twente

Søren Juul Jørgensen
Research Fellow, The Center for Human Rights and International Justice, Stanford University

Migle Laukyte
Associate Professor in Law and AI, Pompeu Fabra University

Keith W. Miller
Orthwein Endowed Professor for Lifelong Learning in the Science Professor, University of Missouri - St. Louis, College of Education and Department of Computer Science

John P. Sullins
Professor, Department of Philosophy, Director of Programming, Center for Ethics Law and Society (CELS), Sonoma State University

Kevin Werbach
Liem Sioe Liong/First Pacific Company Professor and Chair, Department of Legal Studies & Business Ethics, The Wharton School, University of Pennsylvania

Reviewers

Hennie Bulstra
Convenor user group Diplomas and credentials European Blockchain Partnership, Executive Agency of the Ministry of Education, Culture and Science, The Netherlands

Peter G. Kirchschläger
Professor and Director of the Institute of Social Ethics, University of Lucerne

Asger Balle Pedersen
Postdoc at the IT University of Copenhagen, Member of the European Blockchain Center

Daniël Du Seuil
Convenor European Self Sovereign Identity Framework (EBSI) at European Blockchain Partnership

Administrative support

Caroline Kaeb
Policy Officer at DG CNECT – Blockchain and Digital Innovation

Acknowledgements

We would like to thank Pierre Marro at the EU Commission DG CNECT for his support and invaluable feedback, as well as Sophus Garfiel, Thorkild Kristiansen and Tobias Panduro from the Danish Ministry of Digital Government and Gender Equality for their support in the European Blockchain Partnership work and for making these guidelines possible.

9 Glossary

Bitcoin: *see cryptocurrency.*

Block: a bundle of digital pieces of information, i.e. transactions or the parties involved in it, etc. Instead of verifying transactions individually, they are bundled and verified in blocks.

Consensus algorithm (consensus mechanism): Nodes in a peer-to-peer network collaborating via established protocols (consensus algorithms) to agree on whether a new block should be added to the blockchain. The main consensus algorithms are:

- **Proof of Work:** is based on work and effort to be the first in solving the mathematical puzzle and hereby be allowed to verify the next block on the blockchain (see mining).
- **Proof of Stake:** the consensus mechanism based on stakes that the validators (nodes) submit to be allowed to verify the next block on the blockchain.

Cryptocurrency: a currency that exists digitally and does not rely on banks or other financial institutions, but on decentralized systems (such as blockchain). Right now, there are many different kinds of cryptocurrencies, but the best known are Bitcoin and Ethereum.

Decentralized Autonomous Organization (DAO): an organization that is based on blockchain and smart contracts as a source of its governance and management.

Digital Ledger Technologies (DLT): a public and decentralized ledger, where the transactions are visible. All blockchains are DLTs, but not all DLTs are blockchains: that is to say, not all DLTs are organized into chains of blocks, such as for example Radix DLT or Directed Acyclic Graph (DAG).

Digital Twin: a digital representation (such as a token) of a specific process, person, entity, system, or product that exists in the physical world.

Fork: a change to the blockchain protocol, which can be classified into hard fork and soft fork.

- **Hard fork:** radical new version of the blockchain protocol that does not accept any entries or blocks that are created by nodes still operating the old version of the blockchain protocol.
- **Soft fork:** new version of the blockchain protocol that does not accept all entries or blocks that are created by nodes still using the old version of the blockchain protocol.

Hash: unique code or a cryptographic signature that is given to every block. The unique hashes and the interconnectedness of blocks are part of what makes blockchains tamper-proof.

Ledger: the connected blocks storing data in a blockchain system, are sometimes referred to as the blockchain ledger.

Mining: the attempt to generate the right hash for the next block, which is usually rewarded with cryptocurrencies. See *Proof of Work.*

Mining Pools: a pool of miners that combine their computational resources to increase their chances of first generating the right hash for the next block.

Node: it is a computer representing a person, group, or entity, that together with other nodes constitutes a blockchain network. The nodes run algorithms to verify and authenticate transactions (also called mining) hereby earning cryptocurrencies. They participate in the governance, voting, and decision-making of blockchain systems.

Oracle: a trusted third party which supplies the blockchain with information from external sources, such as a bank. However, blockchain systems cannot verify the origin of data and oracles are not per default trustworthy.

Public-Permissioned system: All nodes can read and submit transactions. Only authorized nodes can validate transactions.

Public-Permissionless system: All nodes can read, submit, and validate transactions.

Private-Permissionless system: Only authorized nodes can read, submit, and validate transactions.

Proof of Work: *see consensus algorithm (consensus mechanism).*

Proof of Stake: *see consensus algorithm (consensus mechanism).*

Smart Contract: an agreement in a programming language—a code—which is self-executing once required parameters are met.

Staking pool: *see Validator pool.*

Token: a token is a digital asset that can be stored, transferred, and verified. It might function as a form of currency, or it might grant the owner some other utility value. Examples of tokens are:

- **Asset token:** A token linked to physical or digital assets. It can be either financial or non-financial.
- **Payment token:** A token used for making payments.
- **Utility Token:** A token that provides utility to users (e.g., access rights, identification, or membership) or that serves as a reward.

Tokenisation: The process of creating a token. This can be achieved by creating a new token out of an existing one (minting), or by creating an entirely new token (coinage).

Validator: is a node that validates the transactions in a blockchain system.

Validator pool (staking pool): a pool of validators who put together their crypto-assets to be entitled to validate transactions in blockchain systems that use the proof-of-state consensus mechanism.

Voting: nodes in a blockchain network can vote and collectively decide on how a blockchain system evolves i.e. if a hard fork should be implemented.

10 Endnotes

1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:11992M/TXT, accessed 19-01-2024.
2. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles, accessed 16-04-2024.
3. https://digital-strategy.ec.europa.eu/en/news/eu-and-international-partners-put-forward-declaration-future-internet, accessed 16-04-2024
4. https://digital-strategy.ec.europa.eu/en/policies/blockchain-partnership, accessed 19-01-2024.
5. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home, accessed 19-01-2024.
6. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/EU+Expert+Group+on+Blockchain+Ethics, accessed 19-01-2024.
7. https://digital-strategy.ec.europa.eu/en/policies/blockchain-strategy, accessed 19-01-2024.
8. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en.
9. https://gdpr.eu/, accessed 19-01-2024.
10. https://digital-strategy.ec.europa.eu/en/policies/blockchain-climate-action, accessed 19-01-2024.
11.+12. Beck, R. (2018). Beyond bitcoin: The rise of blockchain world. *Computer, 51*(2), 54-58.
13. https://www.europarl.europa.eu/charter/pdf/text_en.pdf, accessed 19-01-2024.
14. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles, accessed 23-04-2024.
15. https://www.echr.coe.int/documents/d/echr/Convention_ENG, accessed 19-01-2024.
16. https://www.un.org/en/about-us/universal-declaration-of-human-rights, accessed 15-08-2023.
17. https://www.ohchr.org/sites/default/files/ccpr.pdf, accessed 15-08-2023.
18. https://www.ohchr.org/sites/default/files/cescr.pdf, accessed 15-08-2023.
19. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf, accessed 15-08-2023.
20. https://sdgs.un.org/goals, accessed 12-10-2023.
21. https://unfccc.int/sites/default/files/english_paris_agreement.pdf, accessed 15-08-2023.
22. Other values, such as freedom of expression and assembly, dignity, and solidarity, also constitute foundational European values, but are by and large not particularly affected by blockchain systems.
23. John Rawls (2001), *Justice as Fairness: A Restatement* (Belknap Press).
24. Graham Jones, Bernardita Chirino Chase, and Justin Wright (2020), "Cultural Diversity Drives Innovation: Empowering Teams for Success," *International Journal of Innovation Science* 12:3: 323–343.
Frances J. Miliken, Caroline A. Bartel, and Terri R. Kurtzberg (2003), "Diversity and Creativity in Work Groups: A Dynamic Perspective on the Affective and Cognitive Processes that Link Diversity and Performance," in *Group Creativity: Innovation through Collaboration*, eds. P.B. Paulus, B. A. Nijstad (Oxford University Press): 32–62.
25. John Elkington (2006), "Governance for Sustainability," *Corporate Governance*, 14(6): 522–529.
Blanca Corona et al. (2019), "Towards Sustainable Development Through the Circular Economy—A Review And Critical Assessment on Current Circularity Metrics," *Resources, Conservation and Recycling* 151.
26. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:11992M/TXT, accessed 19-01-2024.
27. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT, accessed 19-01-2024.
28. Du Zheng and Erfu Dai (2012) "Environmental Ethics and Regional Sustainable Development," *Journal of Geographical Sciences* 22: 86-92.
29. Matthew Talbert, "Moral Responsibility," *The Stanford Encyclopedia of Philosophy* (Fall 2023 Edition), Edward N. Zalta & Uri Nodelman (eds.), https://plato.stanford.edu/archives/fall2023/entries/moral-responsibility/.
30. Isaiah Berlin (1969), *Four Essays on Liberty* (Oxford University Press); Friedrich A. Hayek (1960), The Constitution of Liberty (Routledge); John Christman (1991), "Liberalism and Individual Positive Freedom," *Ethics* 101(2): 343–359.

31. https://www.un.org/en/about-us/universal-declaration-of-human-rights, accessed 19-01-2024.
32. Agerskov, S., Laukyte, M., & Beck, R. (2023, May). Ethical issues of community-driven blockchain systems. In 2023 *IEEE International Symposium on Ethics in Engineering, Science, and Technology (ETHICS)* (pp. 01-04). IEEE.
33. Agerskov, S., Pedersen, A.B., and Beck, R. (2023), "Ethical Guidelines for Blockchain Systems," *ECIS 2023 Research Papers*: 275, https://aisel.aisnet.org/ecis2023_rp/275.
34. Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the association for information systems, 19*(10), 1.
35. Beck, R. and Jain, G. (2023), "DLT-based Regulatory Systems Dynamics," *Proceedings of the 56th Hawaii International Conference on System Sciences*: https://hdl.handle.net/10125/103102.
36. Dierksmeier, C. and Seele, P. (2020), "Blockchain and Business Ethics," *Business Ethics: A European Review* 29(2): 348–359, https://doi.org/10.1111/beer.12259.
37. Agerskov, S., Pedersen, A.B., and Beck, R. (2023), "Ethical Guidelines for Blockchain Systems," *ECIS 2023 Research Papers*: 275, https://aisel.aisnet.org/ecis2023_rp/275.
38. Caldarelli, G. (2020), "Understanding the Blockchain Oracle Problem: A Call for Action," *Information* 11(11): 509, https://doi.org/10.3390/info11110509.
39. Matzutt et al. (2018), "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin," in *Financial Cryptography and Data Security: 22nd International Conference, Revised Selected Papers*, eds. Meiklejohn, S. and Sako, K (Berlin: Springer, 2018): 420–438, https://fc18.ifca.ai/preproceedings/6.pdf.
40. Agerskov, S., Pedersen, A.B., and Beck, R. (2023), "Ethical Guidelines for Blockchain Systems," *ECIS 2023 Research Papers*: 275, https://aisel.aisnet.org/ecis2023_rp/275.
41. Schwiderowski, J., Pedersen, A.B., Jensen, J.K., and Beck, R. (2023b), "Value Creation and Capture in Decentralized Finance Markets: Non-Fungible Tokens as a Class of Digital Assets, *Electronic Markets*, 33(1): 45.
42. Schwiderowski, J., Pedersen, A. B., Beck, R. (2023a), "Crypto Tokens and Token Systems," *Information Systems Frontiers*: https://doi.org/10.1007/s10796-023-10382-w.
43. Iversen, H. M. W., Schmidt, T. Æ., Pedersen, A. B., & Beck, R. (2023). How to cross the bridge: Interoperability among blockchain systems. *Proceedings of the International Conference on Information Systems.*
44. Bano et al. (2017), "Consensus in the Age of Blockchains," *arXiv preprint arXiv:1711.03936.*
45. Iversen, H. M. W., Schmidt, T. Æ., Pedersen, A. B., & Beck, R. (2023). How to cross the bridge: Interoperability among blockchain systems. *Proceedings of the International Conference on Information Systems.*
46. Agerskov, S., Pedersen, A.B., Beck R. (2023), https://aisel.aisnet.org/ecis2023_rp/275.
47. Brey, P, Brandt D. (2023), "Ethics by Design for Artificial Intelligence," *AI and Ethics*: https://-doi.org/10.1007/s43681-023-00330-4. See also European Commission (2021), *Ethics By Design and Ethics of Use Approaches for Artificial Intelligence (1.0)*, European Commission, DG Research and Innovation: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf. Accessed 15-8-2023.
48. Brey, P. et al. (2021), *Methods for Translating Ethical Analysis into Instruments for the Ethical Development and Deployment of Emerging Technologies*. SIENNA report D6.3: https://doi.org/10.5281/zenodo.5541539; Jeroen van den Hoven, Pieter E. Vermaas, and Ibo van de Poel, eds. (2015), *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values, and Application Domains* (Springer): DOI:10.1007/978-94-007-6970-0.

Ethical Guidelines for Blockchain Systems

The Expert Group on
Blockchain Ethics (EGBE)

European Blockchain Center

ISBN 978-87-7949-074-1