Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience

Alex Norta , Chibuzor Udokwu * , Roxana Voicu-Dorobanțu , Abiodun Afolayan Ogunyemi , Nata Sturua , Stefan Crass

Posted Date: 28 January 2025

doi: 10.20944/preprints202501.1981.v1

Keywords: ethical AI development; societal resilience; digital ethics; sextortion mitigation; blockchain

Article

Leveraging Blockchain for Ethical AI: Mitigating Digital Threats and Strengthening Societal Resilience

Alex Norta [1], Chibuzor Udokwu [2,*], Roxana Voicu-Dorobantu [3], Abiodun Afolayan Ogunyemi [1], Nata Sturua [2] and Stefan Craß [2]

[1] Tallinn University of Technology, Tallinn, Estonia
[2] Austrian Blockchain Center, Vienna, Austria 2
[3] Bucharest University of Economic Studies, Bucharest, Romania
* Correspondence: chibuzor.udokwu@abc-research.at
† Current address: Austrian Blockchain Center, Perspektivstraße 4 1020 Vienna Austria.

Abstract: The rise of online activities and the increasing prevalence of artificial intelligence (AI) in socio-technical systems have brought about both significant opportunities and ethical challenges. Among these challenges, one of the most relevant is addressing digital threats such as sextortion (a form of coercion and sexual exploitation) that disproportionately affect vulnerable groups, such as minors. This position paper advocates the integration of blockchain technology into AI systems to enhance trust, transparency, and ethical governance in combating such threats. The paper argues that, by adhering to ethical guidelines, the specific integration of blockchain operations that bring about strong decentralization, immutability, and auditability into AI may be better managed. Through a literature review and using the specific case study of sextortion, we propose a set of guidelines that ensure secure data management, empower victims, and support law enforcement efforts. This set of guidelines aims to strengthen societal resilience by ensuring privacy, security, and transparency in AI-driven systems and using technology 'for good.' The paper explores the potential of blockchain-integrated AI in various stages of sextortion mitigation, from prevention through education and early detection to providing immediate support and facilitating secure reporting. Consequently, we put forward the position that blockchain-decentralized AI models integrated with user-controlled data wallets considerably enhance the trust in and transparency of AI models. In this way, the paper proposes that a balance should exist between the innovation potential of blockchain-decentralized AI models versus the ethical implications. The paper highlights the critical intersection of ethical AI development, social resilience, and digital ethics and addresses the complexities of integrating technologies while emphasizing the need for interdisciplinary collaboration and adaptive policy frameworks.

Keywords: ethical AI development; societal resilience; digital ethics; sextortion mitigation; blockchain

1. Introduction

The future of the Internet appears to be intrinsically linked to the future of society, each new Internet-based technology building on previous ones to support social and economic activities. Artificial intelligence (AI) is an ever more part of daily human undertakings, a development that offers both opportunities, as well as numerous risks. Recent statistics show that adults are concerned about AI misuse in ethically risky ways in domains such as data-privacy violations and digital abuse that show the need for ethical governance [1,2]. As the sophistication and influence of large language models (LLM) increase, adopting such AI in socio-technical systems is perceived as a matter of concern due to the potential of exploitation, particularly in domains with critical trust and transparency demands [3]. Taking into account ethical and trust issues ensures that AI innovations are adjusted to societal values without reinforcing exploitation and harm.

In a society in which individuals share a large part of their day online through various activities, the growing digital threats to the individual are exacerbated at a societal level. Add to this volatile

 doi:10.20944/preprints202501.1981.v1

environment the potential of ethical challenges brought on by the increasing use of artificial intelligence (AI) in socio-technical systems, and we are today in a position in which the individual is in a highly vulnerable position. This assertion is ever more true for young people, who are often more active online than other generations, more in search of human connections, and who often disregard the risks. In such an environment, the phenomenon of sextortion, both a coercion and a threat, is identified as a particularly damaging risk to young persons of any gender and mainly minors. Briefly, sextortion [4] is defined as the act of threatening to disseminate explicit, intimate, or embarrassing images of a sexual nature without the consent of the victim, usually with the goal of obtaining more images, sexual favors, money, or other forms of compliance. This crime often involves the use of online platforms to coerce individuals by threatening the public release of private images unless demands are met.

The US Federal Bureau of Investigations (FBI) [5] indicates "more than 13,000 reports of online financial sextortion of minors [with] at least 12,600 victims and led to at least 20 suicides" between October 2021 and March 2023. The victims are minors, typically "men between the ages of 14 to 17"; however, the issue is affecting all genders. In a study in 2024 [6], the authors highlight that of close to 17,000 respondents, “14.5% reported victimization and 4.8% reported perpetration”, with men, LGBTQ+, and young victims more likely to report victimization than other categories. The same study affirms that “experiencing threats to distribute intimate content is a relatively common event, affecting 1 in 7 adults".

The present paper is situated at the intersection of ethical AI and blockchain as two fundamental technologies for Future Internet. In the online of tomorrow, which in an ideal case is characterized by decentralization, transparency, and societal trust, technological innovation must mitigate such pressing issues as sextortion [7], in which perpetrators take advantage of sensitive private digital content to blackmail victims. Such misuse of data without consent is typical for a wider spectrum of ethical challenges connected to AI systems. Various types of exploitation are possible when there are occurrences of data privacy violations, bias, and lack. Thus, sophisticated technical solutions ensuring trust and security are required to tackle the increase in sextortion cases to prevent the severe consequences on the mental health and safety of victims.

In this context, current approaches lack a comprehensive set of guidelines for leveraging technology to make society safer, specifically using blockchain technology’s potential to enhance the trustworthiness, transparency, and ethical governance of AI systems in such sensitive contexts. This intersection of ethical AI development, social resilience, and digital ethics is at a critical point. The rapid emergence of new technologies, used indiscriminately by individuals and companies due to their obvious advantages to the point in which they become ubiquitous in everyday life, opens the door to a set of risks that we cannot fully comprehend, assess, or mitigate. However, this is also the stage in which, as Collingridge [8] mentions in his famous dilemma, society must intervene to ensure that a specific technology is safely deployed and is a solution, not a threat. Sextortion serves as a relevant example of this intersection.

The integration of blockchain with AI is a novel opportunity for ethical AI development that emphasizes trust, transparency, and fairness. Consequently, our position paper stresses important societal challenges, especially the increasing phenomenon of digital threats such as sextortion. For improving societal resilience, we pursue in this paper the leveraging of blockchain decentralized architectures that pay attention to ethical frameworks for AI systems. With such an approach we aim to enable the mitigation of issues such as bias, privacy violations, and digital exploitation. Thus, the position paper proposes a structured set of guidelines for Digital Ethics that integrate AI and blockchain technologies to improve sextortion mitigation with the positive consequence of enhanced societal outcomes. As there exists an ever increasing need for the use of responsible technological solutions, the position paper shows that blockchain technologies offers a robust method for ensuring transparency and trust in AI-driven systems.

As a consequence, in this paper, we seek to utilize the combination of blockchain integrated with AI to explore a preventive and responsive set of guidelines to counter sextortion. To protect the victim

 doi:10.20944/preprints202501.1981.v1

from digital abuse with comprehensive support, such a set of guidelines must promote ethical AI systems that take into account privacy, security, and transparency concerns. To ensure the alignment of AI systems with the values of society are given, and to minimize the exploitation risk, systematic changes are required.

In this paper, we assume the position of advocating for the development of a comprehensive set of guidelines to take advantage of blockchain integration with AI systems, which has a significant transformative potential by enhancing trust, transparency, and ethical governance. The specific integration of blockchain (which brings decentralization, immutability, and auditability) into AI may be better managed via the implementation of a privacy-first framework. This set of guidelines must establish ethical standards to positively reinforce trust in AI systems and urgently address the unfortunate challenges of sextortion and similar digital threats. In ensuring that sensitive data are protected and not exploited for victimization, this article advocates an approach that is structured and decentralized to achieve a high degree of transparency, security, and accountability. Based on practical guidelines and preventive measures, the objective of the set of guidelines is for related stakeholders to develop AI systems of technical robustness with ethical alignment. Consequently, the risks of data misuse and AI-caused biases are mitigated, while privacy and trust must be prioritized. The ultimate objective of this position paper is to form a resilient digital environment for AI systems that contribute positively to society while paying attention to individual rights and safety.

The position paper tackles the ethical challenges of AI, specifically with an intersection of human cognition and behavior. The provision of actionable guidelines aims to foster the application and development of ethical AI systems. It contributes to strengthening societal resilience against digital threats such as sextortion by integrating decentralized blockchain-based concepts. The specific AI use cases are described first to show the potential of blockchain-integrated AI technologies to address pressing societal problems such as sextortion. Next, we identify a set of ethical and trust concerns that may occur during AI deployment to mitigate such problems. Hence, the challenges caused by privacy breaches, bias, and manipulation are highlighted.

As a consequence, this position paper provides a blockchain-decentralized set of guidelines, building on concepts such as decentralized internet infrastructure and user-controlled data ecosystems and using instruments such as decentralized machine learning and data wallets to address the issues mentioned above. Next, the set of guidelines explains practical consequences by providing the details for the technical steps and guidelines to adhere to in response to ethical challenges during the use of AI in socio-technical application contexts. Thus, the position paper guides the development of a structured blockchain-integrated set of guidelines that advances responsible AI use. Societal resilience is strengthened by this operationalized AI ethics consideration.

The remainder of this paper is structured as follows. Section 2 provides the background by describing various technical concepts of blockchain and AI and also provides frameworks for the research conducted in this position paper. Section 3 outlines potential ethical concerns for social AI applications by reviewing related literature and a case of an AI application to prevent cases of sextortion. Section 4 proposes potential blockchain operations that can be used to address the ethical issues inherent in AI applications for social good. Section 5 discusses the technical, economic, social, and legal implications of blockchain-integrated AI applications and proposes some set of implementation recommendations. Lastly, Section 6 presents the conclusion and future work of this research.

2. Preliminaries

In this section, we provide the preliminaries for understanding the key essential technical concepts and frameworks that are foundational to this position paper. We first delve into the specific applications of blockchain and AI technologies that serve to address the ethical and societal challenges of our sextortion running case. Thus, it is important to introduce this way the core principles that drive the mentioned technological combination of blockchain technologies and AI. By understanding these

 doi:10.20944/preprints202501.1981.v1

foundational elements, the reader is in a position to better follow the argument of this position paper that investigates the interplay between blockchain, AI, and their ethical applications in building resilient digital infrastructures. Consequently, Section 2.1 introduces the relevant concepts of AI and blockchain technologies, followed by Section 2.2 that contrasts the domains of AI versus blockchain. Finally, Section 2.3 introducing related research frameworks of importance for this position paper.

2.1. Related Technical Concepts

In this part of the position paper, we present some important concepts in AI and blockchain to improve the readability and understanding of the ideas expressed. ***Note that a full list of abbreviations is in the Appendix.***

2.1.1. AI Concepts

Both machine learning (ML) and LLM models are necessary to realize the AI application that addresses the use case of sextortion, which is the focus of this paper. Hence, we first introduce certain algorithm types for realizing the ML and LLM relevant to this work. Then, we show that the performance of these algorithms is evaluated.

ML and LLM Algorithms: ML algorithms are models trained to identify patterns in a dataset and provide prediction by classifying categories of values, predicting continuous values, or organizing data in entirely new clusters [9]. Hence, ML algorithms can be categorized into classification, regression and clustering algorithms. Yet, LLMs are algorithms that provide prediction by understanding patterns and relationships in an existing dataset to generate a completely new set of data in the form of natural language coherent for human understanding [10,11]. LLMs are a special type of natural language processor (NLP) realized from various deep learning algorithms focusing on generating human-readable content [12].

Model performance metrics: Evaluation of AI models facilitates an understanding of their accuracy, hence providing a layer of transparency to these algorithms that are often considered a black box. Similar metrics used in evaluating classification ML algorithms, such as accuracy score and F1 score, are also used in assessing the correctness of predictions produced by LLMs. Generally, the accuracy score checks the quantity of correct predictions, while the F1 score checks the quality of the model using properties such as model precision and recall. Additional metrics are incorporated specifically for LLMs to check the fluency, coherency, and relevance of predictions generated [13].

Algorithm execution steps: Both ML and LLM models follow similar execution processes involving data preparation, model training, and model execution. Data preparation involves all the steps of data pre-processing, such as data - acquisition, aggregation, transformation cleaning, normalization, etc., before they are fed into a model for training [14]. The models are then trained to identify patterns and relationships in a dataset to predict a result for a given set of data questions or to generate an entirely new set of data. The models are optimized to achieve a particular level of performance criteria and then deployed for execution in a real live environment. One of the ways to optimize a model is by ensemble modeling such that several (similar) models are separately trained and their results combined using a consensus algorithm to generate a final result [15,16].

2.1.2. Blockchain Concepts

For the blockchain-related concepts, first, we describe a typical blockchain network and the consensus algorithm that supports it. Then, we describe smart contracts that run on decentralized networks and token-based systems to exchange assets and values within a blockchain network.

Blockchain network and consensus mechanisms: The blockchain network comprises peers and nodes, that represent entities that execute transactions within the network. Transactions are organized in blocks, cryptographically linked with previous transactions, and are redundantly recorded across peers, ensuring consistency of the blockchain's state among all peers. Generally, blockchain networks fall into two categories: private and public. In private blockchains, permission is required to join the network while in public blockchains, anyone can join and execute transactions on the network [17].

 doi:10.20944/preprints202501.1981.v1

Before any transaction is accepted into the network, it undergoes validation using a specified consensus method. Public blockchains commonly employ proof-based consensus methods, such as proof of work and proof of stake, along with their variations. In contrast, private blockchains typically use voting-based consensus methods, often based on adaptations of Byzantine fault-tolerant systems [18]. *Smart contracts and tokenization*: The computer programs running on the blockchains are commonly known as smart contracts. Consequently, different rules and conditions can be encoded within a smart contract, and are executed without the need to rely on a central entity for coordination [19]. A blockchain application, also referred to as a decentralized application (DApp), can consist of several smart contracts. Smart contracts are also used to realize information assets and value exchange among the network participants. These values and digital assets can be represented in various types of tokens that exist in blockchain networks. Some common examples of tokens are utility and non-fungible tokens (NFTs). Utility tokens are fungible and are used to implement the ownership and transfer of values in blockchain networks. NFTs are commonly used to provide a unique representation of digital assets in a blockchain network [20].

2.2. Contrasting the Core Domains: Blockchain versus AI

Blockchain technologies and AI are considered to be complementary and converging technologies. On the other hand, both technologies operate within their own fundamentally distinct domains, i.e., both blockchain technologies and AI serve their respective unique purposes and are based on very diverging operational principles. Blockchain is inherently designed with a focus on establishing trust, verification, and transparency in decentralized systems that require secure and immutable record-keeping. As such, blockchain technologies achieve this by employing decentralized consensus mechanisms, e.g., Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT), and so on [21,22]. The goal is to ensure data integrity without any reliance on a central authority as a trusted third party [23]. Thus, this way, blockchain yields the ability to provide auditability, traceability, and tamper-proof transaction histories [24]. Consequently, blockchain technologies have become indispensable in applications such as digital identity management, secure data sharing, and transparent financial transactions [24].

AI, on the other hand, has its roots in data-driven intelligence with the foci on predictive analysis, pattern recognition, and automated decision-making [25]. Thus, AI employs machine-learning algorithms and additionally large-scale datasets as well to discover insights, predict outcomes, and adapt to complex scenarios in real-time [26,27]. Differently to blockchain technologies, AI systems typically operate without transparency in their decision-making processes and instead excel in domains such as computational adaptability and dynamic responsiveness [28]. AI is currently very widely applied in domains that require rapid and context-sensitive analysis, e.g., in fraud detection, personalized recommendations, and autonomous systems [29,30].

Despite these differences between blockchain technologies and AI, the integration exploration pursued in this position paper does not aim to merge these two distinct domains into a single framework. Instead, the aim of this position paper is to discover their complementary strengths. Blockchain's trust mechanisms ensure that data integrity, secure provenance, and decentralized governance are critical aspects in applications that handle sensitive information [31,32]. On the other hand, the adaptive intelligence of AI for pattern identification and the generation of actionable insights addresses dynamic and evolving challenges, e.g., digital threats [33,34].

Without compromising these technologies, the combination of blockchains and AI yields the possibility of addressing complex social issues, e.g., sextortion, privacy violations, and digital exploitation [35,36]. Another example is that blockchain can secure the provenance of the data used in AI models to prevent a garbage in and garbage out scenario [37]. Thereby, blockchain technology also ensures that sensitive data is not tampered with and remains private [38]. Simultaneously, AI enhances the utility of blockchain by processing large data sets in a privacy-preserving manner [39]. The goal for such an integrated approach is to ensure that the inherent strengths of blockchain and AI reinforce one another [40]. While such blockchain and AI combining systems are more robust and trustworthy,

 doi:10.20944/preprints202501.1981.v1

they are also better positioned to tackle the complex ethical and societal challenges that are inherent for emerging digital ecosystems [41].

2.2.1. Leveraging the Complementary Strengths of Blockchain and AI

While blockchain establishes trust, transparency, and tamper-proof data through decentralized records, AI focuses on dynamic data analysis and adaptive decision-making. These specific strengths complement each other to yield robust frameworks for tackling digital challenges [38].

For example:

- Blockchain ensures data integrity by providing immutable and auditable records, which is ideal for sensitive information management [42].
- AI enhances utility with privacy-preserving techniques by leveraging secure, verified data to detect patterns and threats, such as in the case of sextortion [43].

The described integration allows blockchain to verify data inputs that are AI-generated. On the other hand, AI leverages blockchain to ensure accountability and traceability, thereby creating a system of synergies that is capable of addressing ethical and societal challenges [44,45].

2.3. Research Framework

We next introduce the relevant research frameworks that are foundational for analyzing and addressing complex ethical challenges in blockchain-based AI-driven systems, particularly in contexts such as the mitigation of problems related to the sextortion running case of this position paper.

2.3.1. Inter-Connected framework for AI, Blockchain and Ethics

This part of the paper describes a framework that provides guidelines for the research conducted in this work. As shown in Figure 1, the framework contains four layers. The first layer shows a high-level overview of blockchain integrated into AI applications for social good, such as sextortion mitigation. The second layer shows five ethical pillars relevant to AI applications for social media. Hence, the introduction of blockchain operations into AI applications will result in the *decentralization of control*, *enhanced security*, *transparency*, *reduced bias* and *regulatory compliance*. Nevertheless, the integration of blockchain operations into AI applications will also raise several challenges. Hence, the first part of the third layer of the framework shows the *technical*, *ethical*, *economic* and *legal* implications of blockchain-integrated AI. The second part of the third layer shows the implementation considerations and recommendations for implementing blockchain-integrated AI for social good. The fourth layer shows the evaluation criteria and the resulting impacts when assessing blockchain-integrated ethical AI applications.

 doi:10.20944/preprints202501.1981.v1

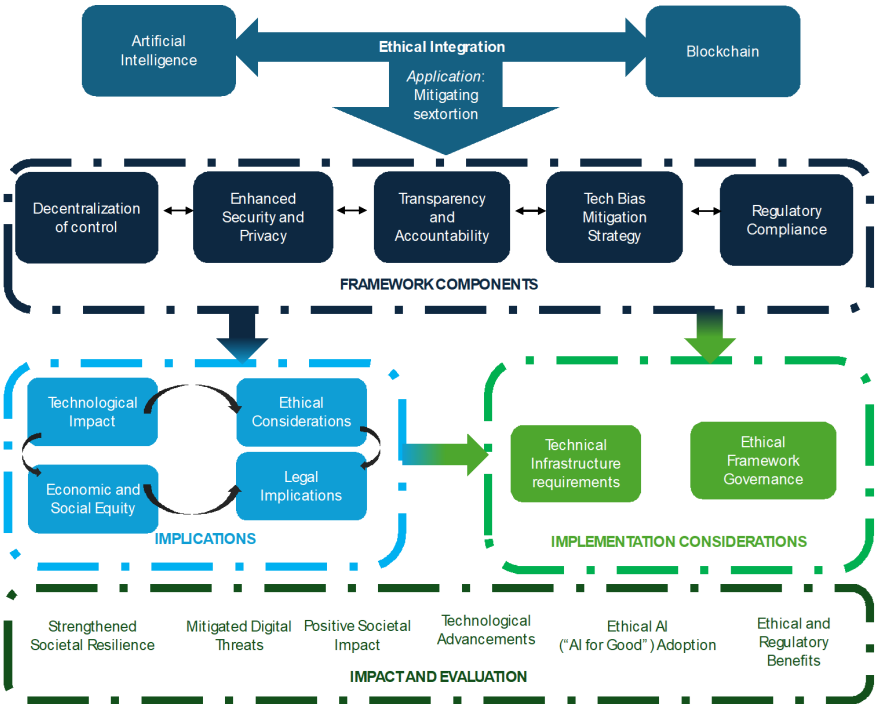

Figure 1. Interconnected methodology of ethical AI, blockchain and societal resilience

2.3.2. Framework Instantiation on the Paper

The adoption of the research framework layers in the various parts of this paper is shown below. Layer one is the high-level refinement of our position: the integration of specific blockchain operations into AI applications that address social issues mitigates important ethical concerns that affect this type of application. These are captured in the motivation of this work as shown in Section 1. For the second layer of the framework, we conduct a literature review and case analyses of ethical issues in AI applications for the social good in Section 3. The purpose of these analyses is to justify the five pillars of ethics and their impacts. Furthermore, in Section 4, we describe in detail blockchain operations to mitigate the ethical issues identified initially. For the third layer, in Section 5, we discuss the research implications of blockchain-integrated AI applications and propose a set of recommendations for the development of such applications. The fourth layer comprises future work in Section 6 that will provide important criteria for evaluating blockchain-integrated AI applications for social good.

3. AI for Social Good and Ethical Concerns

3.1. Related Literature on AI for Social Good and Societal Resilience

The literature on AI for social good and societal resilience is vast, and the intersections between the concepts are numerous and highly complex. In the following section, we capture a snapshot of these interconnections by laying the basics of the concepts for a clearer understanding of the problem at hand. This snapshot is schematized in the following Figure 2.

 doi:10.20944/preprints202501.1981.v1

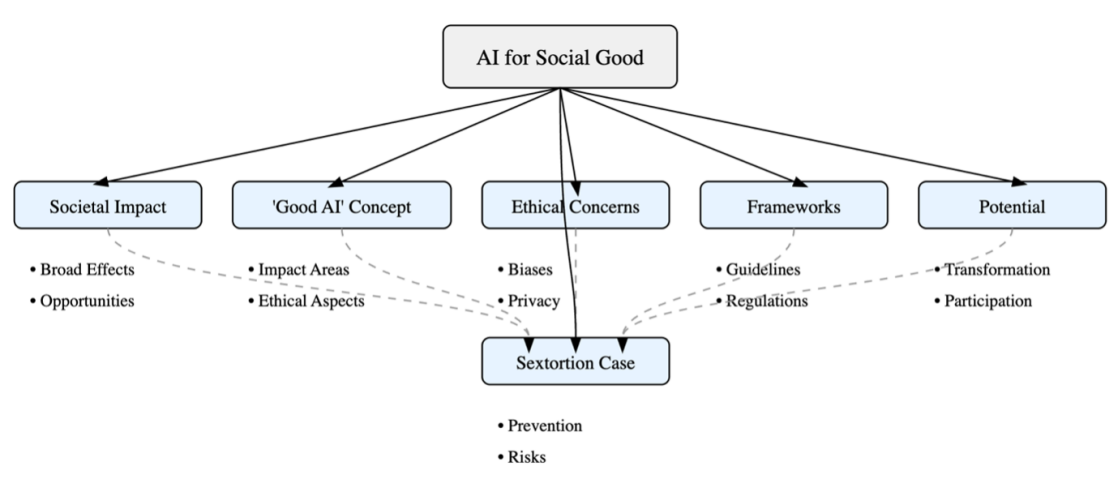

Figure 2. Literature review: AI for social good and societal resilience

3.1.1. AI for Social Good

With its ability to both help and harm, AI has immense promise of producing multidimensional impacts. We should properly harness its abilities, especially regarding social issues. This potential to address societal challenges is proven by solutions such as conversational AI tools being deployed for issues such as mental health awareness. For example, Citation [46] shows how an AI-based emotional chatbot can be used to detect mental issues such as depression by analyzing facial expressions and textual content produced by users, while studies by [47] and [48] describe AI language models to identify depression and suicide prevention. However, there is a gap in understanding how AI may support the mitigation of long-term psychological effects and how it may be integrated into mental health frameworks. Often proposed individually, solutions discussed fail to consider how each component might work synergistically as part of a holistic support system maximizing AI's ability to meaningfully impact individuals and society. A balanced and holistic approach to embedding AI within existing complex support networks can maximize its capacity to benefit individuals and society at large.

3.1.2. Broad Societal Impact of AI

The societal impact of AI goes beyond the microlevel of individuals interacting with technology, and the literature is booming with analyses of various aspects of its potential uses for social good. Before 2021, there were less than 450,000 results in Google Scholar on AI and social good; as of April 2024, there were more than 5 million, with the potential for an increase in this number (see also the analysis by[49]). For example, [50] explores the "potential economic, political, and social costs", while [51] investigates the ethical applications of AI in social systems, paving the way for a nuanced discussion on the topic of AI use in addressing social challenges. Similar issues are addressed in [52], following an assertion that the wide implementation of AI systems goes beyond engineering to an intersection of technology and society, and proposes an illustration of the concept of "ethically designed social computing". From the positive aspects of "accuracy, efficiency and cost savings" [53], issues such as privacy, trust, accountability, and bias must be considered [54]. Diverse aspects related to education and critical thinking can lead to unequal deployment of such technology and ultimately to greater societal polarization [55], an exacerbation of social inequality [56], and dissolution of societal resilience. Similarly to the previous assertion, the critical analysis of this wide range of insights lacks clarity on the way biases and inequities resulting from AI may be mitigated to enhance societal resilience. The literature so far remains at the status quo level and assessment without dwelling on the next steps of a risk management process: risk interconnection and mitigation or reduction.

 doi:10.20944/preprints202501.1981.v1

3.1.3. Conceptualizing a ”Good AI” Society

The idea of a 'good' AI society is not new. The work of [57] starts a conversation on ten potential areas of social impact: "crisis response, economic empowerment, educational challenges, environmental challenges, equality and inclusion, health and hunger, information verification and validation, infrastructure management, public and social sector management, security, and justice". In the same line, the work of [58] maps 14 ethical implications for AI in digital technologies: "dignity and well-being, safety, sustainability, intelligibility, accountability, fairness, promotion of prosperity, solidarity, autonomy, privacy, security, regulatory impact, financial and economic impact and individual and societal impact." All these implications and potential impacts are weaved into a very complex ontological system of a society existing dually (in real and in digital) in which AI represents a new layer. This society must become resilient, and any type of behavior leveraged by technology that undermines this resilience must be tackled properly. Expanded from engineering and ecology to social contexts, resilience is an essential topic, relying on holistic approaches, inter- and multi-disciplinary frameworks, and normative epistemological questions [59,60].

An interplay of individual, institutional, and community capacities, societal resilience is based on coping, adaptation, and transformation [61]. Although AI is a potential tool to improve individual resilience (particularly given the theory of resource conservation, as discussed by [62]), its role in community resilience is only beginning to be acknowledged. Firstly, societal resilience is promoted by creating common spaces of innovation and transformability [63], adaptable and flexible systems and structures, with AI potentially supporting the operational resilience of cyber systems as the backbone of a global digital society [64]. Secondly, modeling social systems for improved resilience leads to the implementation of agent-based approaches, with AI systems scrutinized for their own resilience [65]. In this growing corpus of literature, the need for more empirical research on how AI can be integrated to validly enhance social resilience without introducing new risks and vulnerabilities is demonstrated.

3.1.4. Sextortion and AI

Sextortion, defined as a form of sexual exploitation in which victims are, e.g., extorted with their sexual images [66], is a form of dissolution of societal resilience. It exploits vulnerabilities in social and economic structures and corrodes the integrity of society by breaking down structures meant to protect privacy and security. In this context, a case study on sextortion as a form of cyber abuse and growing societal concern, particularly in the case of young people and / or minors, can be a niche illustration of the ethical challenges of AI. The harms of sextortion involve dignity, well-being, safety, and individual impact, touching on privacy, security, and societal consequences.

Although in most countries sextortion is often not legally defined as a crime, authorities prosecute related crimes in varying ways between jurisdictions, categorizing it as child pornography, harassment, extortion, stalking, hacking, and violations of personal privacy [67]. For instance, in the USA, sextortion is defined in two primary ways: as a threat to share a victim's private sexual images to extort something from them or as coercion to make the victim send sexual material under threats. Federal law typically prosecutes sextortion as extortion or child pornography, depending on the victim's age [68]. The member states of the European Union also prosecute sextortion in a variety of ways according to domestic legislation, often through extortion, privacy violation, and sexual harassment charges that account for individual and broad social impacts - from defamation and integrity infringements to media manipulation and gender inequalities [69]. For example, in France, illicit coercing sexual favours faces civil and criminal charges such as sexual assault, extortion, blackmail, or corruption [69]. In addition to this, the Digital Republic Law covers issues related to the unauthorized use of personal data, including non-consensual sexual imagery and deepfakes [67]. Similarly, data protection laws are used to protect against sextortion in Germany, Spain, and Hungary, with legislation in the latter specifically including provisions for sexual exploitation, defined as coercing someone into sexual activities through threats, and, since 2013, sexual blackmail and extortion [69].

 doi:10.20944/preprints202501.1981.v1

Efforts to combat this cybercrime may benefit from the use of AI [70,71], while some countries (Indonesia, for example) are setting regulatory frameworks in place to deal with sexual violence crimes, including sextortion (the TPKS law of 2022 [72]). On the opposite side of the spectrum, AI can be shown to leverage the sextortion efforts of perpetrators through dating apps [73] or deepfakes [74]. Despite timid advances in the topic, both in the literature and in regulatory and legal frameworks, the significant gap in empirical studies demonstrating the effectiveness of technological solutions (AI or other) in preventing and mitigating sextortion has yet to be addressed.

3.1.5. Ethical Risks of AI

In contrast, artificial intelligence (AI) is considered to pose significant risks to humans and societies if it is not ethically developed and used. Researchers, corporations and NGOs, along with policymakers, explore maximizing AI's benefits and capabilities. Yet fast progress and implementation of AI solutions may outpace understanding of unintended effects. The challenges posed by AI are diverse, ranging from algorithmic biases to the potential for humans to inherit AI errors. Fundamentally, AI must be fair, transparent, explainable, responsible, trustworthy, and reliable. Without these attributes, it remains a 'black box' where developers may themselves struggle to comprehend how the system generates its responses, particularly in the case of generative AI tools such as LLMs. It is of utmost importance that society (including all stakeholders) takes immediate steps to prevent AI tools from engaging in unpredictable behaviors and establish the credibility and trustworthiness essential to society.

3.1.6. Frameworks for Ethical AI: Guidelines and Ethical Principles, Regulatory and Legal Frameworks

In [75], it is emphasized that evaluating technologies in isolation is futile due to their social implications. In this view, a series of multi-layered frameworks have been developed to assess AI's impact potential for societal good. In [76], an analysis of AI solutions was performed using four criteria: breadth and depth of impact, potential implementation of the solution, risks of the solutions, and synergies in the area of opportunity. The risks section deals with 'Bias / Fairness / Transparency Concerns' and 'Need for Human Involvement', highlighting the evident need for an ethical assessment of the solutions.

Although [77] claims that even before the widespread use of LLM, there was a need for a unified vision of the future of AI, the proposed guidelines fail to find a common thread. In their investigation of 84 guidelines, [78] highlight the consensus on fundamental AI ethics while noticing the high variation in how the principles are implemented. In the same line, [79] underline the lack of detailed guidance on the same implementation. Based on [80], on the ethics of algorithms, [81] propose 7 essential factors for AI for Good: "(1) falsifiability and incremental deployment; (2) safeguards against the manipulation of predictors; (3) receiver-contextualized intervention; (4) receiver-contextualized explanation and transparent purposes; (5) privacy protection and data subject consent; (6) situational fairness; and (7) human-friendly semanticisation", with the latter works on the same topic by [82] and [83]. Similarly, [84] refer to the need for a value-sensitive design, defined as a method to integrate values into technological solutions, while [85] advocate for a socially responsible algorithm and [86] propose an ethics penetration testing for AI solutions.

Various countries are implementing AI regulations in a struggle against the black-box complexities of AI, particularly in balancing its benefits and potential harm. In the United States, the Biden administration has introduced an executive order advocating for 'Safe, Secure, and Trustworthy AI'; Canada proposed an Algorithmic Impact Assessment; the World Economic Forum an AI Procurement in a Box, and the OECD a Framework on AI Strategies [87].

The European Union is also in the process of enacting its first AI regulations, although it requires a more integrated approach from the member states and governments [88]. Still, existing frameworks, such as the Assessment List for Trustworthy AI (ALTAI), play a key role in guiding the development of fair and ethical AI [89]. ALTAI, in particular, protects people's fundamental rights [90]. Moreover, the General Data Protection Regulation (GDPR) protects user privacy [91]. The efficacy of these frameworks has yet to be completely determined. For example, [90] argue that we must interpret

 doi:10.20944/preprints202501.1981.v1

AI frameworks like ALTAI from a systems theory standpoint to be applied in various disciplines, allowing "the integration of a rich set of tools, legislation, and approaches". The scalability of ethical AI frameworks, in the context of their proper practical application in highly sensitive areas, such as sextortion, is also an area of potential improvement for current research. With solutions at the incipient level, the way in which they will build upon existing frameworks and further develop appears to be a problem of the future.

Regulating AI through data privacy laws presents several challenges. These challenges include controlling personal data, ensuring the right to access personal data, adhering to the purpose limitation principle, and addressing the lack of transparency in AI decision-making processes. Furthermore, AI systems often introduce privacy risks by obscuring algorithmic biases, complicating the enforcement of the right to be forgotten, and affecting the right to object to automated decision-making (ADM) [92].

Regardless of the scope, relevance, or enforcement of these regulations, AI applications pose significant risks beyond the range of data privacy laws. For example, there are other concerns that AI regulation should address: issues related to self-management of personal data, the guarantee of access to personal data, the lack of transparency of the AI decision process, hidden algorithmic biases, the right to be forgotten and the right to object ADM [92].

3.1.7. Transformative Potential of Ethical AI for a Resilient Society

The social good of AI goes beyond technology fixes; it calls for societal transformation. The ethical practices of AI require the participation of the communities that it seeks to enhance so that the development of AI solutions is informed by those they intend to help [93].

Although significant progress has been made in investigating the potential of AI for societal resilience, there are two noticeable gaps: (a) a critical gap in understanding the perpetuation of biases, especially in the context of sextortion, linking social, anthropological, and technological concerns, and (b) a lack of critical analysis on the potential risks and consequences, with most of the literature corpus being polarized or presenting pinpointed solutions. Moreover, in the current literature, there is a significant lack of insight into the scalability and practical implementation of ethical AI frameworks, particularly in combating sextortion. This status quo underscores the need for both an ethical framework as the one proposed in this position document and for comprehensive studies that critically assess limitations.

Considering the concepts presented in this section, based on the reviewed literature, we identify a series of roles and impacts linked to the aspects highlighted in the problem statement from the Introduction. These aspects are presented in the following Table 1.

 doi:10.20944/preprints202501.1981.v1

Table 1. Comparative analysis of AI and blockchain roles in ethical development and societal impact.

Aspect	The Role of AI	Impact	Selected Relevant Referenced Articles
Ethical AI development	AI capabilities (algorithms, data processing) and the need for ethical design.	Increased trust and responsible AI. Fairness and bias reduction	[1,2,52–54,58,75,94–103]
Societal Resilience	Early detection and data-driven decision-making through predictive analytics and other AI-driven insights	Strengthened societal ability to handle crises, societal stability and enhanced trust	[3,9,19,50,59,61–65,93,101,104–110],
Sextortion Mitigation	AI helps in detecting potential sextortion (automated detection) and providing support	Enhanced prevention, safer digital environments, preventing exploitation and providing support for victims	[46,47,66,67,69–74,84,100,101,111,112]
Digital Ethics	Several ethical concerns exist, still, AI can also be designed to uphold ethical principles for Privacy protection and decision-making	Balance between technological advancement and ethical considerations (maintaining ethical standards and transparency)	[1,2,54,70,76,84,89,91,92,95,102,112–118]
Legal Concerns	AI offers solutions in sensitive areas like sextortion and misinformation, still compliance with local regulations and privacy issues are big challenges	Enhanced privacy protection, bias detection and reduction, improved transparency, and stronger ethical safeguards	[75,76,81,84,86,89–92,115,116]

3.2. A Case of AI Application for Social Good

3.2.1. AI Applications That Raise Ethical Concerns

The opportunity to harness AI technologies such as LLM and ML algorithms to address the widespread challenge of sextortion underlines the need for ethical AI frameworks. A practical and clear use that concerns human behavior and cognition, with a considerable risk of affecting individuals emotionally, underscores the necessity of transforming broad ethical principles into actionable guidelines and, lastly, allowing for responsible technological applications.

An approach designed to assist individuals affected by sextortion that combines machine learning with LLM may have the following features, each contributing to support throughout every stage of the process [119]:

- The "Prevention" stage— Before an actual sextortion event, potential victims may use highly personalized, gamified, and engaging educational resources to increase their awareness of related risks. Furthermore, AI, through personalized gamified interactive learning experiences, can support people at risk to cultivate self-confidence, the lack of which represents a risk factor for sextortion.
- The "Provision of Instant Aid" stage - AI can automatically identify coercive behaviour through customized gamification and tracking unusual behavior patterns to accurately red flag possible victims. Through LLM-based chatbots, AI may provide live support for sextortion victims to reduce the probability of them spiralling into self-destructive behaviors - another characteristic of the subjects of such a social-stigma-carrying occurrence. For example, the chatbot can recommend social services resources that address problems such as suicide and self-injury, which can stem from sextortion incidents.
- The "Continuous Support" stage: The traumatic nature of a victim's sextortion case leads to it not being resolved once the event is considered closed. Individuals affected by such a case go through

 doi:10.20944/preprints202501.1981.v1

a recovery period that can also be supported by AI through tools that allow self-assessment and / or direct emergency contact with social services or law enforcement.

3.2.2. Ethical Issues from the Case of Sextortion AI Application

Although posing a higher risk to society in large and vulnerable groups in particular, the phenomenon of sextortion may be both mitigated, for example, by providing behavioural red flags for vulnerability and enhanced by AI, for example, by using deep fakes to convince victims, while more research should address this polarized context. As previously stated, there is a significant literature gap in empirical studies, with the goal of using AI to support societal resilience thus hindered by a series of challenges researchers encounter when addressing this topic (sextortion), such as:

- Limited Empirical Research at risk of obsolence: As both the AI-sextortion and blockchain-sextortion areas are in their infancy, empirical research remains very limited. Only a few studies deal with the use of AI (or blockchain) to detect, prevent, or mitigate the phenomenon, and even fewer focus on the nexus of the three concepts. This lack of transdisciplinary research holds back technology from having direct applicability in solving social problems, and may have major implications in the long run. Studies might become obsolete or irrelevant as the time needed for academic research can be excessively long compared to the speedy pace of technological changes.
- Interdisciplinary Complexity: Apart from the two technologies considered, aspects related to psychology, sociology, anthropology, ethics, law, and economy must be integrated to gain a clear perspective and propose potential solutions.
- Ethical Considerations: By involving aspects related to sensitive data, privacy, and consent, as well as automated human profiling, ethical issues are a major concern in both research about sextortion and research into the use of AI. Another ethical issue is related to bias and generalization of assumptions and results. The data utilized to train artificial intelligence significantly impacts its effectiveness. If not enough data is available (see also the next limitation), or if the data is biased and not representative (the ethical concern), then the solution is irrelevant and may do more harm than intended, by generating inequitable outcomes.
- Data Use and Sensitivity: Extensive exploitation of data for educating AI or carrying out research is hindered by its sensitive nature—posing potential harm to victims, its distribution across multiple jurisdictions and platforms, in addition to the numerous ethical clearances needed from different local and global organizations. This international perspective is also affected by distinct legal and regulatory frameworks, leading to the inability to propose shared policies or resolutions.

4. Blockchain Operations that Address Ethical and Trust Issues in AI Systems

In tackling the significant ethical and trust challenges present in AI systems, blockchain technology is proven to be complementary. Using the inherent characteristics of transparency, decentralization, and immutability, a blockchain can provide novel solutions that reinforce trust in AI applications, a much needed characteristic in the context of the sextortion case under discussion. This section explores how integrating blockchain into AI systems can establish robust frameworks to mitigate risks such as data tampering, bias, and lack of transparency. We delve into the practical mechanisms and strategies where blockchain can enhance data security, provide immutable audit trails, and ensure compliance with ethical guidelines. Consequently, Section 4.1 presents the federated machine learning that blockchains enable. Next, Section 4.2 shows that the so-called blockchain data wallets protect sensitive data from misuse. Section 4.3 briefly discusses blockchain-based privacy-conscious data processing, and Section 4.4 suggests that blockchain token economy models produce positive contributions to AI systems. Together, these approaches outline a structured approach to increase public trust in AI applications while protecting individual rights. Finally, Section 4.5 discusses the practical applications of blockchain-based AI systems.

 doi:10.20944/preprints202501.1981.v1

4.1. Blockchain-Enabled Federated Machine Learning

Distributed processing of patient/victim data, where ML algorithms are run locally on the organization and institution where the data is generated, aims to improve the trustability of AI systems that address social issues. This prevents a single entity from aggregating and controlling sensitive user data. Figure 3 adapted from [120,121] shows a simplified process representation of federated AI systems (a form of ensemble modeling) integrated with blockchain technologies. The process consists of several organizations *org1...n* where each organization controls the data and ML models used in the system. To ensure that all models maintain consistent and acceptable performance, a smart contract performs a requirement verification. Hence, only models (within specific organizations) that meet the data and model performance requirements are selected for use. A consensus smart contract combines the results of individual models to produce the final result of the system.

4.2. Blockchain-Enabled Data Wallet

A mechanism in which patients and victims of sextortion have control over their data shared in the AI system to train and improve the performance of algorithms protects data owners from abuse and exploitation. Figure 4, adapted from [122], shows a process representation of an organization (*ogr1*) that processes user data for an AI system that addresses social problems. Users (data owners) can grant or deny permission for the use of their data in the system. Furthermore, data owners can revoke permission for the continued use of their data in retraining or improving the AI system. The users also can verify that their data have not been used or re-used by the AI system.

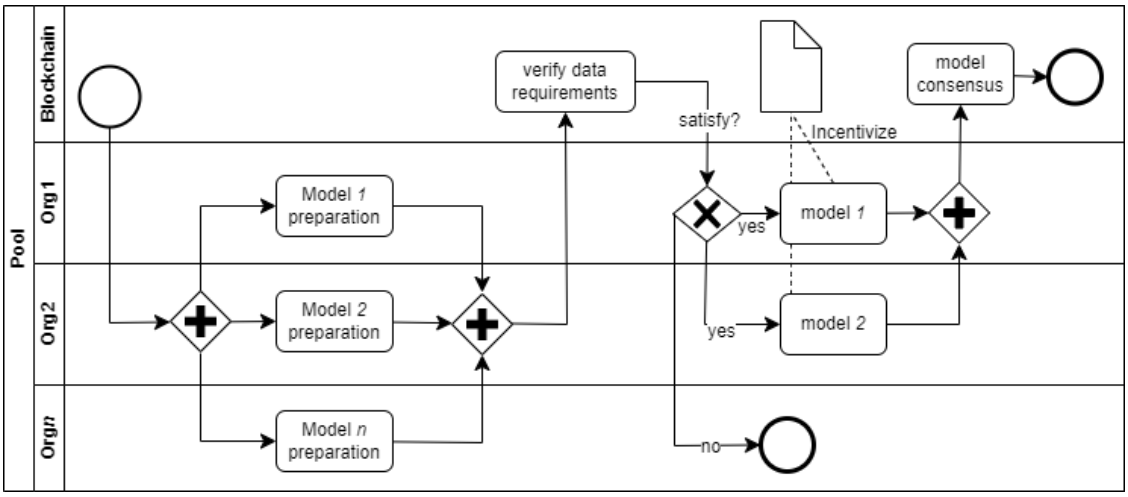

Figure 3. Decentralized machine learning.

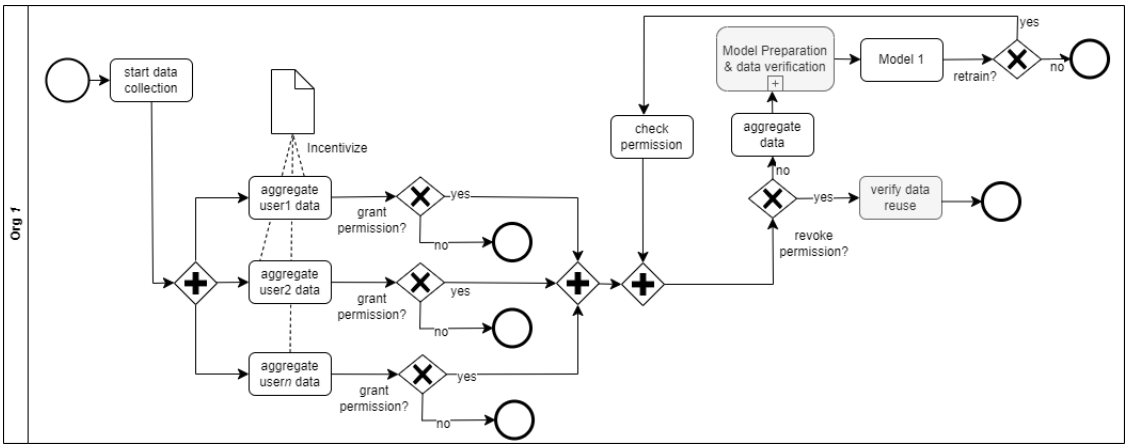

Figure 4. Incentivized user data wallet.

 doi:10.20944/preprints202501.1981.v1

4.3. Privacy Aware Data Processing

Integration of the zero-knowledge proof (ZKP) system can address additional privacy concerns related to information verification within the proposed AI system, decentralized machine learning, and data wallet. The ZKP provides a privacy-aware system for processing and verifying information without revealing sensitive information. The following data verification is potentially possible in the AI system represented in Figures 3 and 4 - data requirement, model performance, and data reuse verification. Although these verification possibilities generally improve the transparency and trustability of the AI system, such verification procedures must be carried out without leaking user confidential information. Although verifications are performed on the blockchain using smart contracts, the data must remain in the owners' data wallets within the organizations they are generated. Hence, a cryptographic ZKP of information used in training the AI model can be stored on the blockchain, and users can, therefore, verify that their information has not been used without revealing their data. Following the same manner, ZKP can be used to confidentially verify the data requirements and performance of the constituent models without revealing information about the data used in training the models.

4.4. Token Economics Model

A well-designed token economic model can address the funding challenges of AI systems that deliver social good by incentivizing users (data owners) and organizations (which host ML models) to positively contribute to the system. Users, who in this case potentially represent victims of sextortion, can be rewarded with tokens for contributing their data for the training of the LLM and ML models. The main idea is to encourage victims of sextortion to share their data in a secure and privacy-preserving way to train AI models that can support future victims. The same token distribution model can be adapted to reward organizations that host the various ML and LLM algorithms to ensure the availability and continuous contribution of their hosted models to the system. As shown in Figures 3 and 4, the organizations that host the various models that are part of the federated learning are incentivized to produce models that meet the minimum performance requirements of the system, and users (such as data owners) are incentivized to grant permission for their data use in the system.

4.5. Practical Applications of Blockchain and AI

Combining blockchain technologies and AI yields advantages in addressing real-world challenges in which privacy, transparency, and accountability are essential. Thus, we discuss the practical applications of these combined technologies. Their complementary roles in tackling societal issues are explored, e.g., sextortion and AI accountability while ensuring regulatory compliance.

4.5.1. Sextortion Mitigation with Federated Learning

The running case of sextortion is a digital threat that exploits sensitive personal data, which the combination of blockchain technologies and AI can address. The traditional method of sensitive data centralization for data analysis is problematic, as this potentially compromises data privacy. With the application of federated learning techniques, AI solutions are trained across distributed datasets without transferring sensitive data of individuals. Consequently, the latter are ensured to remain localized and secure in this way [123].

With blockchain technology being a transparent and tamper-proof ledger that tracks consent and data usage, a combination with AI strengthens the framework [124]. In the running case of sextortion, blockchain documents when and how data is used during AI training processes. Furthermore, such an approach ensures compliance with privacy regulations such as GDPR [125]. By securely verifying that training adheres to ethical and regulatory standards, blockchain and federated learning together create a robust system for sextortion mitigation that prioritizes both security and privacy.

 doi:10.20944/preprints202501.1981.v1

4.5.2. Blockchain-Audited AI Accountability

AI systems that operate in sensitive domains, such as flagging potential sextortion cases, face increasing scrutiny over the fairness and reliability of their decision-making processes. Blockchain introduces an immutable auditing mechanism for these AI-driven decisions, thereby enabling transparency and accountability. For example, while an AI model is used for detecting sextortion patterns in large context-based data sets, the related AI decision-making rationale is logged securely on a blockchain [126]. The process integrity and fairness is verified by auditors without compromising the data privacy of the individuals involved.

Law enforcement systems are a domain where the practical implementation of blockchain-based AI would be sensible. In such a scenario, the large datasets related to sextortion threats are analyzed by an AI system and subsequently, the AI's decision-making pathways are recorded on a blockchain. These records can be accessed by the auditors and other relevant authorities to validate the conclusions of the AI. Thereby, a compliance with the ethical and legal standards is ensured while simultaneously safeguarding the sensitive information of individuals [127].

4.5.3. Comparison of Blockchain and AI Roles

In Table 2, we illustrate the unique contributions of blockchain technology and AI, respectively, while highlighting how their integration addresses specific challenges.

Table 2. A comparison of blockchain and AI roles in practical applications.

Aspect	Blockchain Role	AI Role	Integrated Benefit
Data Integrity	Immutable records for traceability	Dynamic pattern recognition	Verified and secure data inputs
Privacy	Decentralized control, tamper-proof data	Federated learning, anonymized data	Enhanced privacy and compliance with GDPR
Transparency	Transparent audit trails	Explainable and auditable decisions	Accountability and trust
Security	Cryptographic protections, resilience	Threat detection and mitigation	Robust defense against digital threats
Regulatory Compliance	Supports GDPR and AI Act compliance	Adaptive risk assessment	Ensures adherence to regulatory standards

The roles of blockchain and AI are summarized in the table, which lists for challenges such as the running case of sextortion the ways to enhance both privacy and accountability. On the one hand, blockchain ensures the immutability and traceability of data and decisions and AI, on the other hand, provides dynamic capabilities for threat detection and mitigation. This combination yields a robust regulatory framework [128].

5. Discussions: Research Implications

With respect to the position put forward in this paper, the integration of blockchain technologies and AI has real-world implications and poses also challenges, which we discuss in this section. The ethical implications of such an integration require a critical analysis of the effects on societal structures that are decentralized and disintermediated, challenge policy formation, and also transform existing governance models. The ethical implications in light of the technological implications also require a discussion of the possible benefits and threats that emerge. Thus, our goal is to generate insight into the compliance with ethical standards of blockchain-enhanced AI systems so that societal silence and justice are strengthened.

In the remainder, Section 5.1 discusses the complexity of the integration of blockchain and AI together with the innovation potential. Section 5.2 discusses the ethics issues for the integration of the AI blockchain from a technology neutrality perspective. Section 5.3 discusses the important issue of bias counteracting and discrimination. Section 5.4 addresses the economic and social equity that

 doi:10.20944/preprints202501.1981.v1

is affected by blockchain-integrated AI. Next, Section 5.5 explores the management of diverse legal and regulatory challenges in the integration of blockchain and AI. Finally, Section 5.6 addresses the implementation considerations for blockchain integrated ethical AI.

5.1. Integration Complexity and Innovation

There are considerable challenges and opportunities related to the integration of blockchain technologies with AI frameworks. This holds specifically for cases from the domains such as healthcare or finance. As blockchain technologies are instrumental in ensuring integrity and immutable traceability, the authors in [104] discuss the beneficial effects on managing and securing e-healthcare data records. In this way, blockchains manage the immutability and accessibility of such data records while simultaneously also adhering to the corresponding regulations, e.g., the GDPR and the Health Insurance Portability and Accountability Act (HIPAA) [129].

In reference to Section 4, we stress that blockchain technology is instrumental to protect transactions that are part of AI-supported decision making processes. In [108], the authors support this statement by analyzing the means to increase blockchain technologies to ensure that sensitive data in sectors such as healthcare are managed transparently and with a high degree of security. In this way, blockchains support the notion of trust in system stability.

In [130], the authors stress the need for an interdisciplinary research approach that involves technologists, ethicists, policymakers, etc. Such collaborative research aims to ensure that the integration of AI and blockchain technologies meets not only technical standards. In addition, strict ethical norms must also be adhered to in order to improve the societal trust that leads to broad adoption.

The increased trust and transparency that blockchain technologies deliver affect not only the e-healthcare sector positively with improved efficiency. Thus, as the authors in [131,132] discuss, the specific attributes of the blockchain of decentralization, immutability, and transparency strengthen the trust of users. Furthermore, as discussed in [108], the disintermediation of centralized system structures achieves increased process efficiencies.

In relation to the sextortion case, unauthorized changes in sensitive e-health data become impossible with the use of blockchain technologies, in that the data in transactions of the user are recorded securely and permanently. Thereby, blockchain technologies secure the privacy-assured access to sensitive data of victims to the point that trust is fostered in the management of sextortion cases. In addition, in [106,109,110], the authors investigate the secure management of e-health data across various systems and the positive role of blockchain technologies in this context. Briefly, the latter proposes a way to reduce data breach risks while ensuring fast patient-data access.

In taking advantage of their complementary strengths, integrating blockchain technology and AI into one system can be used to address complex societal challenges. Risks such as adversarial attacks, are significantly reduced by ensuring robust data integrity via blockchain's immutable and tamper-proof nature [133]. If data integrity directly impacts decision-making outcomes, then these AI application strengths are particularly critical [134].

Adaptive capabilities by AI tackle evolving threats like sextortion. For example, sensitive distributed data can be analyzed with AI enabled by federated learning without compromising privacy [125]: Thus, federated learning enables AI ensuring compliance with ethical and legal standards [135]. A robust system for mitigating threats is created while safeguarding privacy with blockchains that provide a transparent ledger to record consent and data usage securely [136]. Thus, ethical and secure frameworks are created for data processing by the exemplified synergy that blockchain and AI together create [137].

5.2. Technological Neutrality and Ethics

Specifically, to address sextortion as a sensitive issue, the integration of AI and blockchain technologies is guided by policy development. As shown in Section 4, technological development (blockchain-integrated AI) evolves at a rapid pace, which poses a challenge to policy frameworks. In addition, future developments must be monitored since they affect the significance of ethical standards.

 doi:10.20944/preprints202501.1981.v1

In [138], the integration of blockchain and AI significantly improves security and privacy, which is important for the protection of victims of sextortion. Furthermore, in [139], the authors stress the immediate need for adaptive policy measures to address digital threats such as sextortion in combination with the use of digital currencies.

In reference to the position statement of this paper, we stress the need for a comprehensive framework to leverage the interaction of blockchain technologies and AI to improve the transparency, security, and accountability of digital environments. Managing robust reporting mechanisms addresses sextortion cases effectively flanked by enacting safeguarding policies to protect the data and privacy of individuals. The enforcement of policies becomes significantly effective due to the immutable traceability of events in a decentralized context that blockchain technologies infer. As shown in federated decentralized learning (in Section 4.1), data policies can be managed and enforced locally within the organizations where the data are produced. In [140], the authors discuss the improvement of corporate governance transparency and accountability by integrating blockchain technologies and AI. Thus, we infer that this technology integration is also beneficial for privacy and security management in sextortion contexts. In addition, the authors in [141] stress the establishment of trust in very secure infrastructures, which is achieved by the integration of blockchain technologies and AI.

Based on the descriptions of the blockchain-based operations shown in Section 4, we infer regulatory requirements can be enforced dynamically without the involvement of intermediaries. We ensure thereby automatically the adherence to privacy laws and standards for data protection. This is very important for sextortion cases that involve sensitive data that must be protected with a high degree of confidentiality. In [117], the authors show that blockchain technologies are instrumental in defining and implementing access policies for the protection of personal data, which improves overall privacy and security.

In legal scenarios, the capabilities of the mentioned blockchain operations are essential in establishing a transparent and tamper-proof foundation for all interactions and transactions. Consequently, the authors in [142] discuss the access and sharing policies for data access enforcement that make recorded actions easily auditable. Mapped into a sextortion context, such a blockchain system delivers undeniable evidence of misconduct to consequently involve the appropriate civil services as per the definitions in smart contracts. Also in [143], the authors explore the changes in judicial systems to ensure that legal procedures are transparent to effectively combat crimes such as sextortion.

Policies themselves must be flexible and adaptable to enable dynamic policy enforcement by blockchain systems. In [144], the authors point out that the enforcement of existing policies and their adaptation to novel technological innovations can be facilitated by blockchain technologies. In addition, the authors in [145] propose the notion that blockchain technologies coupled with AI analysis yield insight that allows the evolution of policy structures that are more fluid and less rigid as policy frameworks.

Significant technological and regulatory advantages are provided by the intersection of blockchain and AI. To reduce the risks associated with data poisoning and bias, the immutability of blockchain ensures that AI models train on verified and tamper-proof data [125]. Enabling decentralized AI training with federated learning further strengthens privacy protection, which aligns with GDPR principles of data localization and minimization [146].

Additionally, it is possible to enhance a system's transparency and accountability with blockchain-audited AI operations. For example, one can enable an external verification of model outputs with the audit trails that are generated and maintained by a blockchain to document AI decision-making processes [124]. In sensitive applications such as identifying sextortion threats, this is particularly valuable since fairness and reliability are paramount [147].

From a regulatory perspective, the integration supports compliance with GDPR and the AI Act. Blockchain ensures traceability and adherence to data localization laws, while adaptive AI systems enable dynamic risk assessment and policy compliance [148]. The use of smart contracts further automates regulatory enforcement, ensuring real-time adherence to evolving legal standards [149].

 doi:10.20944/preprints202501.1981.v1

5.3. Counteracting Bias and Discrimination

For sensitive domains, such as in sextortion cases, securing distributed data collection is a very essential capability of blockchain integrated into AI. The danger is the potential bias based on a limited representative dataset, which is an undesirable situation. The combination with blockchain-enabled federated machine learning ensures that data are aggregated across various organizations, demographics, and locations where sextortion occurs to curb AI biases. The position statement of this paper stresses that ethical AI operations are necessary to strengthen societal resilience, thus, according to [150], blockchain technologies are instrumental in addressing algorithmic fairness to achieve ethical AI.

Expanding on blockchain operations in Section 4, we explore the ways blockchain technology mitigates AI biases by ensuring transparent data management and verifications. Measures to mitigate against AI biases that lead to unfair outcomes are a detailed review of data sources, training methodologies, and decision-making policies. For an application context such as sextortion, AI must be free of bias to ensure fairness and justice when AI aims to detect and analyze abuse occurrences. In [100], the authors stress the importance of audit trails on blockchains for data to consequently be immutably traceable. In this way, the integrity of the system is enhanced. Also in [98], the authors investigate identification methods to mitigate biases in AI where blockchain technologies support AI transparency and fairness.

The effectiveness of blockchain is most exploited when all AI operations are recorded on the chain to document all data access instances, record model training, and decision making. Such immutably logged data on blockchains constitute a permanent record of all AI activities to allow auditors to check the adherence to ethical standards. In [103], the authors show that blockchains improve transparency in sensitive data environments due to established immutability and auditability. The discussion in [96] also reveals that blockchains in AI applications ensure that operations and decision-making are valid.

Systems that comprise blockchain operations integrated into AI applications can be designed to be flexible and upgradeable to adapt to changes when biases are detected in AI algorithms. Such changes may include retraining of AI models with improved representative datasets. Consequently, a traceable history of change events is recorded to enhance transparency and accountability. The authors in [97] point out that AI operations can be reliably scrutinized when all modifications are mutably logged on a blockchain. Also in [94], blockchain use enables auditing of AI events stored to ensure that adjustments do not violate ethical guidelines.

With blockchain integration into AI, the participation of stakeholders in defining and changing rules is allowed for AI operations. For the sextortion running case, the implications are that community stakeholders such as victim advocacy groups are included, alongside legal experts, ethicists, etc., to decide on the training and application of AI models. In order to democratize the AI decision-making process, decentralized control enhances transparency and equity. In [99], the authors explain that blockchains have the potential to improve stakeholder participation in AI governance and positively affect fairness and transparency. In [102], a discussion about the regulatory aspects of blockchain stresses the capacity of AI governance integration to involve various stakeholders with their input. Hence, ethical guidelines are always followed.

Blockchain-based AI systems create frameworks that align with societal and ethical demands with addressing the integration complexity and enhancing technological neutrality. This integrated approach establishes a foundation for addressing future challenges and mitigates current digital threats[151]. The synergy between blockchain's data integrity and AI's dynamic adaptability represents a transformative step toward ethical, regulatory-compliant, and socially equitable technological solutions [152,153].

5.4. Economic and Social Equity

The link of sextortion with economic and social equity is three-pronged: from causes to consequences and specific implications for policies and practices. Thus, sextortion may be driven by

 doi:10.20944/preprints202501.1981.v1

socioeconomic factors (such as economic uncertainty, gender issues, and patriarchal societies), as specified in [154,155]. However, it may also lead to micro and macroeconomic effects. For example, it can cause economic vulnerability and instability in victims [154], increase social inequality, and perpetuate stigma and ostracizing of already marginalized individuals [111].

We posit that blockchain-integrated AI (BIAI) and other technologies that improve transparency, security, efficiency, and accountability may address these issues. Decentralization (as an intrinsic part of BIAI) plays a crucial role in empowering victims of sextortion by giving them more control over their data and incentivizing them when they share such data for training and retraining of AI systems. Instead of centralized storage, the distribution of data over a blockchain network enhances individual autonomy and mitigates data breach risks [105], while addressing data ownership and privacy concerns [156]. This distributed model also ensures that data are less susceptible to misuse, another essential element for victims of sextortion [157]. This is because data are processed in the locations (and organizations) where the data is generated. Decentralization affects more than just control of individual information - it alters the very structure of power in data ownership. Historically, data were at risk of misuse, as access to them was gate-kept by a small number of large corporations and government agencies, as described in [158]. This status quo is rebalanced through blockchain technology, which allows individuals to own and control their digital assets, leading to consumer empowerment and fairness in making algorithmic decisions. For the use of legal and social services, this build-up on a more inclusive data set provides a scenario in which algorithmic decision making can be less biased than currently [159–161].

Using the concept of decentralization, as delivered by BIAI, alongside transparency and enhanced security, we can identify several directions in which economic and social equity in the context of mitigating sextortion may be discussed. The structure of the discussion moves from micro to macro and from victim to perpetrator, highlighting how BIAI can positively affect this chain. First, BIAI ensures democratized access to financial resources and digital services [162], promoting economic equity according to the token economic model shown in Section 4. This feature may lead to providing a secure platform for sextortion victims to seek help without the danger of additional exploitation.

Second, BIAI supports social equity by increasing security through privacy-aware data processing enabled by ZKP systems. For victims of sextortion or potential victims, this level of security and accountability is essential because it gives them confidence that their data are being stored and handled properly and that there is accountability in such instances when a data breach occurs [163]. This empowers victims, encouraging them to seek help and resources for protection; in addition, the blockchain side of BIAI facilitates decentralized reporting systems which in turn permit sextortion victims to report incidents securely and anonymously. As a consequence, the risk of social ostracizing is mitigated and social equity is advanced by safeguarding the well-being of victims.

Third, when the victim does not come forward, BIAI can support identifying red flags of such an event occurring, empowering law enforcement with analytics to improve understanding of related crime patterns. For example, the findings of [164] show that blockchain and AI in combination improve surveillance and tracking capabilities by ensuring detailed, secure, and immutable records of all transactions. Applying these results of the finance industry to sextortion, as well as other similar exploitative issues, we posit that by using BIAI, abuse patterns in transactions can be highlighted, allowing for the prevention of injustice[164].

Fourth, in addition to this BIAI-supported recognition of victims, AI-supported educational and awareness programs, with or without blockchain-enhanced digital micro-credentials [165], may prove beneficial in supporting and empowering vulnerable individuals. These types of programs equip victims with the knowledge to recognize and respond to threats.

Fifth, on the law enforcement side, after the victim has been identified and the sextortion crime has been committed, BIAI can support the justice system in several ways, ethically, by following a supranational ethical framework [113]: *Transparent legal processes* - BIAI may guarantee that legal decisions are transparent and auditable, which will help combat corruption [166]. In turn, corruption,

 doi:10.20944/preprints202501.1981.v1

through bribery and the influence of perpetrators, has been proven to affect effective prosecution of sextortion cases, for example, in South Africa with migrants [111,167]. *Tamper-proof evidence* - Blockchain can ensure the integrity of the chain of custody [168,169], while AI can be employed in the analysis and management of evidence and digital forensics [159,170–172]. *Support for marginalized groups* - One of the groups most affected by sextortion is represented by migrants and refugees [111], who are also affected by a lack of easily verifiable identification and may have access to legal aid and support through blockchain-based identity verification [173].

Sixth, while the crime has been proven and aid is directed towards the victim, BIAI may also bring efficiency and security. Blockchain-enabled anonymous payment mechanisms, further down the mitigation process, ensure that the aid aimed at victims reaches recipients securely and anonymously without the risk of misappropriation [174]. Blockchain has been proven to improve social welfare programs and promote equitable resource distributionby ensuring that funds are not smuggled into intermediaries [175].

Last, at a more macro level, we must consider a two-pronged perspective: on the one hand, the role of AI in the use of decentralized data to improve decision-making [176],and, on the other hand, the transformative role of AI and blockchain for significant parts of society [107]. This dual perspective leads us to reassert the need for an integrated approach to ensure the proper and ethical use of BIAI.

5.5. Managing Diverse Legal and Regulatory Challenges in the Integration of Blockchain and AI

With the integration of blockchain and AI, two transformative technologies are merged into system applications that are governed by distinct regulatory frameworks [40]. On the one hand, blockchain technologies operate within a legal landscape that focuses on concerns for decentralization, data immutability, and financial regulation [177]. On the other hand, the regulatory framework of AI stresses different aspects versus the one for blockchains, e.g., privacy, transparency, and ethical considerations [178]. Given this divergence, specific challenges must be taken into account for an effective deployment of blockchain-integrated AI systems [179,180].

In Table 3, we provide an overview of the key regulatory aspects associated with blockchain and AI integration. The leftmost column lists the primary regulatory challenges, followed by two columns detailing the respective focuses of blockchain and AI in addressing these challenges. The rightmost column outlines proposed mitigation strategies, which are expanded upon in the following subsections. This table serves as a roadmap for understanding the detailed discussion of regulatory issues and solutions presented below.

Table 3. Key regulatory challenges and proposed mitigations for blockchain and AI integration.

Regulatory Aspect	**Blockchain Focus**	**AI Focus**	**Proposed Mitigation**
Data Privacy	Immutability, GDPR compliance	Data minimization, GDPR	Federated learning, local data processing
Transparency	Traceability, auditability	Explainability, algorithmic transparency	Smart contracts for verifiable AI actions
Algorithmic Fairness	Decentralized trust, consensus	Bias mitigation, risk assessment	Blockchain-based audit trails
Data Sovereignty	Decentralized, cross-border risks	Jurisdictional data processing	Regulatory sandboxes, ZKPs

The regulatory challenges summarized in Table 3 highlight the fundamental tensions between blockchain and AI systems, as well as practical strategies to bridge these gaps. Each of the proposed mitigations is further elaborated in the subsections below, demonstrating their applicability to real-world blockchain-AI integrations.

 doi:10.20944/preprints202501.1981.v1

5.5.1. Blockchain Regulations

The unique challenges that blockchain technologies face with respect to regulatory hurdles are primarily related to the immutability feature [181]. The latter is not in line with the European Union's General Data Protection Regulation (GDPR) that introduces the "right to erasure" [182]. An additional source of conflicts with regulations results from decentralized blockchain applications often involving cross-border operations, which poses a challenge to achieving legal compliance with the EU's Markets in Crypto-Assets Regulation (MiCA) [183]. Consequently, it is important for blockchain technologies to achieve an alignment with international legal standards to ensure the lawful sharing and processing of data, specifically when such systems handle sensitive data [38,184].

5.5.2. AI Regulations

Regulation for the AI domain prioritizes the safeguarding of user privacy, ensuring the transparency of algorithms, and the mitigation of risks related to bias and discrimination [185,186]. Thus, the European AI Act focuses on this domain by establishing clear guidelines for the assessment of risk and by achieving an explainability in AI systems [187,188]. However, the reliance of AI on very large and extensive datasets poses many novel challenges that conflict with important blockchain principles that require the minimization of data and the decentralization of control [189]. Consequently, the resulting discrepancies between these two important domains create regulatory tensions [190,191].

5.5.3. Legal Conflicts in Integration

Integrating these two technologies accentuates several regulatory conflicts [192]. The focus of blockchain technologies on data storage that is immutably traceable, directly stands in contrast with the need of AI for dynamic data updates, particularly when the requirement arises to be compliant with the GDPR principle of the "right to be forgotten" [193**?**]. In addition, while blockchain ensures transparency through records that are traceable, the analysis of sensitive data by AI raises concerns for privacy that may violate regulatory standards unless appropriately managed [194,195]. The processing of data across borders is a further complication factor for the legal landscape, particularly when the decentralized architecture of blockchain technologies intersects with jurisdiction-bound AI regulations [196,197].

5.5.4. Proposed Solutions for Harmonization

With a multi-pronged approach, it is necessary to bridge these regulatory gaps to harmonize the pointed-out discrepancies in the integration of blockchain and AI [198]. One possible solution is the adoption of so-called regulatory sandboxes. The latter provides a controlled environment for the testing of innovative blockchain-based AI systems in the context of relaxed regulations [199]. Such testing sandboxes allow the developers of blockchain-based AI systems and regulators to collaborate, identify compliance issues, and refine frameworks in real-world scenarios [200,201].

Interdisciplinary collaboration is equally vital. Thus, having regulators, technologists, and ethicists collaborate with each other can foster unified regulatory approaches that balance blockchain's decentralization including AI's data-driven nature [202]. In parallel, self-regulatory principles aligned with frameworks like the OECD AI Principles and EU Blockchain Strategy offer an interim solution, enabling industry stakeholders to set governance standards while awaiting formal regulations [203, 204].

5.5.5. Practical Applications of Privacy-Preserving Techniques

Regulatory conflicts can be addressed effectively with technological innovation. For example, federated learning is a decentralized machine learning approach that allows AI models to be trained across multiple devices or organizations without having to transfer raw data to a central repository [205]. Federated learning supports the exchange of model updates, such as encrypted gradients or weights instead of sharing sensitive datasets [125]. The model updates are aggregated centrally to improve the shared model [206]. The notable advantage of this method is to ensure that data remains localized

 doi:10.20944/preprints202501.1981.v1

at its source. As a result, the privacy and security of sensitive data are significantly enhanced [207]. Jurisdictional conflicts are mitigated with the adoption of federated learning by following the inferred data localization laws, which minimizes the need for cross-border data transfers [208].

Similarly, a powerful mechanism for the verification of compliance with data privacy standards such as GDPR, without the need to expose sensitive information is provided by the integration of ZKP into blockchain systems. Thus, the confidentiality of sensitive data remains ensured while simultaneously enabling the possibility of conducting transparent compliance audits.

5.6. Implementation Considerations for Blockchain Integrated Ethical AI

The earlier discussions in this paper show that a technical integration of blockchains with AI yields a potential for transformation that enhances trust, transparency, and ethical governance in AI systems. Simultaneously, careful considerations are required to handle the considerably complex technical and ethical challenges in this constellation. For a responsible deployment, a deep understanding of the technical requirements, governance structures, and ethical frameworks is necessary for a responsible system deployment. Specifically for sensitive applications such as the running case of sextortion in this paper, data privacy, security, and fairness are paramount and demand a comprehensive approach. Thus, we next explore the key considerations for blockchain-integrated AI system implementations to ensure technical robustness, on the one hand, while adhering to ethical standards, on the other hand for reinforcing societal trust and resilience.

5.6.1. Technical Requirements and Infrastructure

Implementing blockchain-integrated AI systems requires a robust technical infrastructure capable of supporting the demands of both technologies. An essential implementation element is the blockchain network design itself. The specific advantages and challenges inherent to public versus private blockchain networks are fundamental. Briefly, important for trust establishment in AI systems is the greater transparency and decentralization that a public blockchain produces [209]. Simultaneously, public blockchains also have performance issues in that they have scalability and latency issues [210]. However, while private blockchains require special governance structures to generate trust and security, they provide better access control and faster transaction times [211].

Also influential for blockchain security and efficiency insurance in the blockchain is the fitting consensus mechanism selection. Different trade-offs for energy consumption, transaction speed, and security are present in consensus algorithms such as Proof of Work (PoW), Proof of Stake (PoS), and Byzantine Fault Tolerance (BFT), and so on [212]. Taking into account the running case of sextortion where ethical concerns must be balanced with operational efficiency, will influence the choice of consensus-mechanism [213]. Understanding the latest developments in these algorithms is crucial for optimizing both security and performance [214].

For process automation within blockchains, smart contracts are essential. Ethereum's Solidity is the best-known example of smart contracts that must be developed securely and reliably. To prevent security vulnerabilities such as re-entry attacks, one should adhere rigorously to best practice patterns [215]. Thus, developers must thoroughly test and audit smart contracts so that they function according to the requirements and do not violate the integrity of the system [216].

The aspect of interoperability is also very relevant for blockchain-integrated AI systems. Consequently, the system's seamless interaction and communication with third-party networks, AI frameworks, and databases within various organizations must be ensured. Considering standardized APIs and protocols, one can achieve a high degree of overall system effectiveness for data exchanges [217]. The interoperability between private and public blockchain technology can significantly transform digital record keeping and enable automation [218]. By implementing models that improve cross-chain communication, blockchain systems can work together efficiently and effectively [219].

Next, we address the scalability of BIAI, which poses a significant challenge. Problematic issues such as managing high transaction throughput and high demands for efficient data processing [220]. As a mitigation, there are available techniques such as off-chain transaction processing, sharding, and

 doi:10.20944/preprints202501.1981.v1

layer-2 solutions [221]. Thus, a BIAI system must be designed with a system architecture to efficiently handle large volumes of data and transactions as a critical element for high performance [222].

For sensitive information exchange management through BIAI systems, data privacy and security must be assured. For example, data encryption, zero-knowledge proofs and decentralized data storage solutions [41] are means to support the quality requirements of data security and privacy. For decentralized data storage, the Inter-Planetary File System (IPFS) [223] is a prominent example. Also important for sensitive data management is maintaining high legal and ethical standards. Consequently, BIAI systems must adhere to data protection regulations.Frameworks like SecNet have been proposed to improve data security and trustworthiness, using AI-enabled encryption methods [224].

For the best operationality of BIAI systems, one should continuously monitor the performance and also maintain such a system constantly. An option to immediately resolve issues that occur is to check the logs of BIAI systems in real time [225]. Furthermore, if regular system updates and continuous maintenance are provided, then occurring security vulnerabilities are tackled as well the system's functionalities are enhanced. An example of an advanced monitoring technique is the so-called noise-aware sparse Gaussian process [226] that provides reliable uncertainty assessments for BIAI systems. Note also that overall performance and efficiency in system monitoring are enhanced if edge-AI is integrated [227].

Finally, significant computational expense is required for the deployment of BIAI systems. The increased computational needs result in tasks such as model training and blockchain mining or validation. To manage costs while ensuring high performance, efficient resource allocations are possible with the use of cloud-based solutions or decentralized computing networks [228]. With these measures to relevant technical requirements and infrastructure, we infer that the implementation and operation of blockchain-integrated AI systems should be more successful. Intelligent resource optimization techniques, such as those used in Mobile Edge Computing (MEC), can further enhance the efficiency in these systems [229]. We also stress that resource allocation via AI assistance can potentially improve operational efficiency while reducing computational expenses [230].

5.6.2. Governance and Ethical Frameworks

Robust governance and ethical frameworks are essential for the establishment of an effective implementation of an BIAI system. Such frameworks must be in place for ensuring that ethical boundaries are adhered to by systems that integrate AI and blockchain technologies. Such systems also need to be aligned with societal values and regulatory standards [231]. New and unique opportunities and challenges arise with this combination of AI and blockchain technologies to create secure and trustworthy intelligent systems [34]. Furthermore, to govern such novel combined systems, the corresponding governance frameworks must incorporate trust models for the ethical and secure operation of these systems [232].

Blockchain-based governance is inherently decentralised in the decision-making processes that stakeholders can participate in. Collaborative governance is facilitated by encoded rules that are represented by smart contracts in implementations such as decentralized autonomous organizations (DAOs) or similar models [233]. With the inclusion of DAOs, the risk of centralized power abuse is reduced when changes to an AI-blockchain system must be carried out transparently and with collective consensus [234]. As a result, a blockchain-based AI system maintains a high degree of trust and fairness with decentralized governance, which is crucial for ethical AI deployment [235].

The fundamental quality requirements for the integration of AI and blockchain are transparency, fairness, privacy, and accountability, which also influence the adherence to important ethical guidelines. To guide the development and operation of BIAI systems with an established and clear set of ethical principles is essential, and recent AI ethics frameworks outline corresponding guidelines [236]. To employ such technology for the public good in the best possible way, potential issues such as data privacy, algorithmic bias, and informed consent are the essential principles to be addressed [237]. Compliance with ethical principles is very crucial to ensure transparency, fairness, and overall trustworthiness for BIAI systems [238].

 doi:10.20944/preprints202501.1981.v1

A rather diverse set of stakeholders should be involved in BIAI systems, e.g., developers, users, ethicists, and policymakers as a key element of ethical governance. The main motivation for including a diverse set of stakeholders is the development and management of various perspectives and needs [239]. To foster trust and accountability versus these stakeholders, mechanisms should be established to collect their feedback and active participation in governance processes [240]. Consequently, a blockchain-based AI system is more responsive and adaptive to the needs and values of stakeholders when a wide range of them is incorporated [241].

To make BIAI systems legitimate and adaptable, it is critical to ensure a system's compliance with local and international regulations. As a result, GDPR, financial regulations, and industry-specific standards should be strictly followed in order to achieve a high degree of data protection [242]. The immutable transparency and traceability of a blockchain for audit purposes is an advantage for implementing a compliance framework that monitors and enforces regulatory requirements [243]. With such an approach, one ensures, on the one hand, legal compliance and, on the other hand, also a strengthening of public trust in the operations of blockchain-based AI systems [244].

To improve the accountability of the AI system, one should leverage the inherent strengths of blockchain technology, i.e., transparency and accountability. Thus, a continuously traceable record is provided for review by specific blockchain mechanisms that record every transaction and decision made by AI systems to create a clear audit trail [245]. To ensure that the blockchain-based AI system adheres to high ethical standards, it is crucial to guarantee public trust by establishing processes for external audits and oversight [246]. The specific capabilities of blockchains, that is, transparency, traceability, and immutability; are powerful features that also ensure accountability for the development life cycle of AI systems [236].

It is normal for socially used systems that disputes and grievances arise over time. To effectively address such issues, the implementation of a transparent and decentralized resolution mechanism is important. For enforcing fair and impartial conflict resolution processes, smart contracts are a suitable automation means [247]. The best way to protect user rights and maintain the integrity of BIAI systems is to provide procedures for the management of claims and compensation for scenarios of system errors or ethical violations [248]. Employing smart contracts also ensures the enforcement of agreements in a transparent and transparent way and does not require the need for centralized third parties [249].

An ongoing ethical assessment of both blockchain technologies and AI is important to understand the dynamic nature of this combination. Thus, it is vital to establish a continuous evaluation framework to investigate the ethical implications and possible unintended consequences of BIAI systems. The alignment with evolving ethical standards and societal values must be ensured for the system with regular audits, impact assessments, and ethical review [250]. To identify and mitigate ethical risks, continuous evaluations are likely to yield a BIAI system that easily adapts responsibly to new challenges [251]. Furthermore, possible emerging ethical and regulatory challenges are addressed with fairness and legal compliance with continuous impact assessments [252].

Finally, it is important for users and stakeholders to understand well the ethical implications of BIAI systems by integrating extensive educational measures that are part of an integrated comprehensive governance framework. These measures must always contain very clear information about the detailed use of data, the important AI decision-making processes, and the vital role of blockchain technologies that ensure transparency and security [253]. Always encouraging a highly responsible use of BIAI systems with better informed consent requires the promotion of sophisticated ethical knowledge among users [239]. Thus, a better and well-matching alignment of such complex systems with their related societal expectations and additional ethical standards can be achieved when a properly informed user base exists [231].

6. Conclusions

In this position paper, we explore the potential of blockchain-integrated AI systems to transform socio-technical application cases such as sextortion. Thus, we investigate to what extent decentralized

 doi:10.20944/preprints202501.1981.v1

immutable traceability strengthens the reliability, security, and fairness of such BIAI systems. Consequently, a new paradigm emerges for digital interactions and data management, which goes beyond mitigating sextortion and offers a replicable framework for addressing broader societal challenges. The position of this paper stresses the advantages of utilizing blockchain technologies, for example, providing a structured and decentralized approach to AI-based digital ecosystems, supporting misinformation risk management or the development of secure identity frameworks, central elements to a resilient Future Internet. This integration of BIAI systems improves not only the transparency and accountability but also ensures the rights of individuals to ethical governance. The position paper shows that the advantages resulting from integrating blockchain into AI systems are very important for domains such as sextortion in which data must be managed securely and ethically. Blockchain and AI integration represents a transformative step toward addressing complex societal and technological challenges. Practical applications such as using federated learning for sextortion mitigation and blockchain-audited AI decision-making demonstrate the potential for these technologies to align with ethical governance while solving real-world problems. We address additional challenges related to the integration of blockchain technologies with AI, which also include privacy concerns and the risks of algorithmic bias. Such a convergence of blockchain and AI that enables traceability, transparency, and secure data handling, also constitutes a robust framework that ensures regulatory compliance, e.g., the adherence to GDPR and the AI Act. Still, critical open issues for future research remain such as scalability, algorithmic fairness, and ensuring a critical degree of trustworthiness in AI decisions. The effects of BIAI systems on societal behaviours and norms require further research to better understand the long-term effects. Furthermore, an up-to-date policy development is necessary that keep up with the fast technological advances.

To conclude, our position paper highlights the potential of integrating AI and blockchain technologies to combat sextortion, a problem that is ever-growing for vulnerable societal categories, such as minors. In a multilayered approach, we suggest using AI for early detection of sextortion attempts and providing immediate support to victims, while blockchain ensures secure, anonymous reporting and evidence storage. We also correlate blockchain transparency with increased trust in AI systems, which is crucial when handling sensitive issues. The study indicates that this technological integration can improve privacy and data control for users, key factors in sextortion prevention. Thus, we propose the use of smart contracts for secure case management and evidence collection. In general, our findings suggest that the combination of AI and blockchain can significantly strengthen societal resilience against sextortion by empowering victims and supporting law enforcement efforts. However, we emphasize the need for careful ethical considerations in the implementation of these technologies to ensure that they do not inadvertently cause harm or infringe on individual privacy rights.

For future work, it is important to perform an inter and transdisciplinary impact assessment and evaluation of the positions, concepts, and models proposed in this paper. This evaluation may include multiple cases of blockchain-integrated AI applications that address social issues through proof-of-concept (PoC) demonstrations. The results of the evaluation will show the stronger societal resilience derived from the implementation of BIAI and highlight practical manners to navigate the complex landscape of ethical AI development and maximize the benefits of these technologies for society at large. The proposed evaluation will also show concrete examples of mitigated digital threats and positive societal impacts derived from the implementation of the concepts outlined in this position paper. Future research should also explore further improvement options for societal resilience via the integration of blockchain technologies and AI interdisciplinary collaboration between technologists, ethicists, and policymakers. Such interdisciplinary study efforts will aim at forming a foundation for addressing emerging digital threats by ensuring that these technologies advance in ways that uphold human rights and promote social equity. Additional evaluation criteria for the evaluation of the developed PoC include ethical and regulatory benefits, technological advances, and AI for adoption of social good. These evaluation criteria are part of the research framework shown in Figure 1.

 doi:10.20944/preprints202501.1981.v1

The essential point is to ensure that human rights are upheld and individual justice is promoted when blockchain technologies and AI are used in combination. And this desiderate is even more imperative the more the digital landscape evolves, this paper reinforcing the urgency to embed ethical considerations, as default setting, into technological advancements and ensure that BIAI align fully with the core principles of Future Internet - transparency, inclusivity and trustworthiness.

Author Contributions: Conceptualization, A.N. and C.U.; methodology, A.N, C.U, R.VD; data curation, A.O.; writing—original draft preparation, A.N, C.U, R.VD, A.O, N.S, S.C; writing—review and editing, A.N, C.U, R.VD, A.O, N.S, S.C.; project administration, A.N, S.C.; All authors have read and agreed to the published version of the manuscript.

Funding: This research is partially funded within the framework of the COMET center ABC, Austrian Blockchain Center by BMK, BMAW and the provinces of Vienna, Lower Austria and Vorarlberg. The COMET program (Competence Centers for Excellent Technologies) is managed by the FFG. This research is also partially funded by the Estonian "Personal Research Funding: Team Grant (PRG)" project PRG1641.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

- ADM: Automated Decision-Making
- AI: Artificial Intelligence
- ALTAI: Assessment List for Trustworthy AI
- AML: Anti-Money Laundering
- BIAI: Blockchain-Integrated AI
- CJEU: Court of Justice of the European Union
- CPRA: California Privacy Rights Act
- DCAP: Decentralized Conditional Anonymous Payment
- DApp: Decentralized Application
- GDPR: General Data Protection Regulation
- HIPAA: Health Insurance Portability and Accountability Act
- LLM: Large Language Model
- ML: Machine Learning
- NFT: Non-Fungible Token
- NLP: Natural Language Processing
- SVG: Scalable Vector Graphics
- TPKS: Tindak Pidana Kekerasan Seksual (Indonesian law on sexual violence)
- ZKP: Zero-Knowledge Proof

References

1. Ahmet, E. The Impact of Artificial Intelligence on Social Problems and Solutions: An Analysis on The Context of Digital Divide and Exploitation. *Yeni Medya* **2022**, *2022*, 247–264.
2. Baum, S.D. Artificial interdisciplinarity: Artificial intelligence for research on complex societal problems. *Philosophy & Technology* **2021**, *34*, 45–63.
3. Shen, Y.; Heacock, L.; Elias, J.; Hentel, K.D.; Reig, B.; Shih, G.; Moy, L. ChatGPT and other large language models are double-edged swords, 2023.
4. Patchin, J.W.; Hinduja, S. Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. *Sexual Abuse: A Journal of Research and Treatment* **2018**, *32*, 30 – 54. https://doi.org/10.1177/1079063218800469.
5. Federal Bureau of Investigation. Sextortion: A Growing Threat Targeting Minors, 2024. Accessed: 2024-08-20.
6. Henry, N.; Umbach, R. Sextortion: Prevalence and correlates in 10 countries. *Computers in Human Behavior* **2024**, *158*, 108298.
7. Alex, N.; Sotiris, M. Designing Artificial Intelligence Equipped Social Decentralized Autonomous Organizations for Tackling Sextortion Cases Version 0.7, 2024, [arXiv:cs.SI/2312.14090].
8. Collingridge, D. *The Social Control of Technology*; Palgrave Macmillan: London, 1982.

9. Ahuja, R.; Chug, A.; Gupta, S.; Ahuja, P.; Kohli, S. Classification and clustering algorithms of machine learning with their applications. *Nature-inspired computation in data mining and machine learning* **2020**, pp. 225–248.
10. White, J.; Hays, S.; Fu, Q.; Spencer-Smith, J.; Schmidt, D.C. Chatgpt prompt patterns for improving code quality, refactoring, requirements elicitation, and software design. *arXiv preprint arXiv:2303.07839* **2023**.
11. Tang, R.; Chuang, Y.N.; Hu, X. The Science of Detecting LLM-Generated Text. *Communications of the ACM* **2024**, *67*, 50–59.
12. Lu, Y.; Liu, S.; Zhang, Q.; Xie, Z. RTLLM: An open-source benchmark for design rtl generation with large language model. In Proceedings of the 2024 29th Asia and South Pacific Design Automation Conference (ASP-DAC). IEEE, 2024, pp. 722–727.
13. Nazir, A.; Chakravarthy, T.K.; Cecchini, D.A.; Khajuria, R.; Sharma, P.; Mirik, A.T.; Kocaman, V.; Talby, D. LangTest: A comprehensive evaluation library for custom LLM and NLP models. *Software Impacts* **2024**, p. 100619.
14. Zelaya, C.V.G. Towards explaining the effects of data preprocessing on machine learning. In Proceedings of the 2019 IEEE 35th international conference on data engineering (ICDE). IEEE, 2019, pp. 2086–2090.
15. Abburi, H.; Suesserman, M.; Pudota, N.; Veeramani, B.; Bowen, E.; Bhattacharya, S. Generative ai text classification using ensemble llm approaches. *arXiv preprint arXiv:2309.07755* **2023**.
16. Ardabili, S.; Mosavi, A.; Várkonyi-Kóczy, A.R. Advances in machine learning modeling reviewing hybrid and ensemble methods. In Proceedings of the International conference on global research and education. Springer, 2019, pp. 215–227.
17. Swan, M. *Blockchain: Blueprint for a new economy*; " O'Reilly Media, Inc.", 2015.
18. Pahlajani, S.; Kshirsagar, A.; Pachghare, V. Survey on private blockchain consensus algorithms. In Proceedings of the 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT). IEEE, 2019, pp. 1–6.
19. Cuccuru, P. Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology* **2017**, *25*, 179–195.
20. Di Angelo, M.; Salzer, G. Tokens, types, and standards: identification and utilization in Ethereum. In Proceedings of the 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS). IEEE, 2020, pp. 1–10.
21. Zhang, C.; Wu, C.; Wang, X. Overview of Blockchain Consensus Mechanism. *Proceedings of the 2020 2nd International Conference on Big Data Engineering* **2020**. https://doi.org/10.1145/3404512.3404522.
22. Y, S.; P, V.; H., P.; Naravani, M.; D.G., N. Performance Evaluation of Consensus Algorithms in Private Blockchain Networks. *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)* **2020**, pp. 449–453. https://doi.org/10.1109/ICACCM50413.2020.9213019.
23. Kaur, S.; Chaturvedi, S.; Sharma, A.; Kar, J. A Research Survey on Applications of Consensus Protocols in Blockchain. *Secur. Commun. Networks* **2021**, *2021*, 6693731:1–6693731:22. https://doi.org/10.1155/2021/6693731.
24. Zhang, C.; Wang, R.; Tsai, W.; He, J.; Liu, C.L.; Li, Q. Actor-based Model for Concurrent Byzantine Fault-tolerant Algorithm. *Proceedings of the 2019 International Conference on Computer, Network, Communication and Information Systems (CNCI 2019)* **2019**. https://doi.org/10.2991/CNCI-19.2019.77.
25. Belle, V.; Papantonis, I. Principles and Practice of Explainable Machine Learning. *Frontiers in Big Data* **2020**, *4*. https://doi.org/10.3389/fdata.2021.688969.
26. Ramkumar, P.; Kunze, K.; Haeberle, H.S.; Karnuta, J.; Luu, B.C.; Nwachukwu, B.U.; Williams, R.J. Clinical and Research Medical Applications of Artificial Intelligence. *Arthroscopy* **2020**. https://doi.org/10.1016/j.arthro.2020.08.009.
27. Goldenberg, S.; Nir, G.; Salcudean, S. A new era: artificial intelligence and machine learning in prostate cancer. *Nature Reviews Urology* **2019**, *16*, 391–403. https://doi.org/10.1038/s41585-019-0193-3.
28. Sachan, S.; Yang, J.; Xu, D.; Benavides, D.E.; Li, Y. An explainable AI decision-support-system to automate loan underwriting. *Expert Syst. Appl.* **2020**, *144*, 113100. https://doi.org/10.1016/j.eswa.2019.113100.
29. Marevac, E.; Patković, S.; Žunić, E. Decision-making AI for customer worthiness and viability. *2023 22nd International Symposium INFOTEH-JAHORINA (INFOTEH)* **2023**, pp. 1–6. https://doi.org/10.1109/INFOTEH57020.2023.10094207.
30. Walter, W.; Haferlach, C.; Nadarajah, N.; Schmidts, I.; Kühn, C.; Kern, W.; Haferlach, T. How artificial intelligence might disrupt diagnostics in hematology in the near future. *Oncogene* **2021**, *40*, 4271 – 4280. https://doi.org/10.1038/s41388-021-01861-y.

31. Kannan, K.; Singh, A.; Verma, M.; Jayachandran, P.; Mehta, S. Blockchain-Based Platform for Trusted Collaborations on Data and AI Models. *2020 IEEE International Conference on Blockchain (Blockchain)* **2020**, pp. 82–89. https://doi.org/10.1109/Blockchain50366.2020.00018.
32. Siddika, A.; Zhao, L. Enhancing Trust and Reliability in AI and ML: Assessing Blockchain's Potential to Ensure Data Integrity and Security. *2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* **2023**, pp. 0312–0316. https://doi.org/10.1109/DASC/PiCom/CBDCom/Cy59711.2023.10361446.
33. Salama, R.; Al-turjman, F. AI in Blockchain Towards Realizing Cyber Security. *2022 International Conference on Artificial Intelligence in Everything (AIE)* **2022**, pp. 471–475. https://doi.org/10.1109/aie57029.2022.00096.
34. Chenna, S. AI and Blockchain: Towards Trustworthy and Secure Intelligent Systems. *SSRN Electronic Journal* **2023**. https://doi.org/10.2139/ssrn.4324495.
35. Zhang, S.; Yao, T.; Sandor, V.K.A.; Weng, T.; Liang, W.; Su, J. A novel blockchain-based privacy-preserving framework for online social networks. *Connection Science* **2021**, *33*, 555 – 575. https://doi.org/10.1080/09540091.2020.1854181.
36. Chen, Y.; Xie, H.; Lv, K.; Wei, S.; Hu, C. DEPLEST: A blockchain-based privacy-preserving distributed database toward user behaviors in social networks. *Inf. Sci.* **2019**, *501*, 100–117. https://doi.org/10.1016/J.INS.2019.05.092.
37. Powell, W.; Foth, M.; Cao, S.; Natanelov, V. Garbage in garbage out: The precarious link between IoT and blockchain in food supply chains. *J. Ind. Inf. Integr.* **2021**, *25*, 100261. https://doi.org/10.1016/j.jii.2021.100261.
38. Bernabe, J.B.; Cánovas, J.L.; Hernández-Ramos, J.L.; Moreno, R.T.; Skarmeta, A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access* **2019**, *7*, 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872.
39. Tian, R.; Kong, L.; Min, X.; Qu, Y. Blockchain for AI: A Disruptive Integration. *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)* **2022**, pp. 938–943. https://doi.org/10.1109/CSCWD54268.2022.9776023.
40. Salah, K.; Rehman, M.H.; Nizamuddin, N.; Al-Fuqaha, A.I. Blockchain for AI: Review and Open Research Challenges. *IEEE Access* **2019**, *7*, 10127–10149. https://doi.org/10.1109/ACCESS.2018.2890507.
41. Li, Z.; Kong, D.; Niu, Y.; Peng, H.; Li, X.; Li, W. An Overview of AI and Blockchain Integration for Privacy-Preserving. *ArXiv* **2023**, *abs/2305.03928*. https://doi.org/10.48550/arXiv.2305.03928.
42. Kaaniche, N.; Laurent-Maknavicius, M. A blockchain-based data usage auditing architecture with enhanced privacy and availability. *2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)* **2017**, pp. 1–5. https://doi.org/10.1109/NCA.2017.8171384.
43. Loreti, P.; Bracciale, L.; Raso, E.; Bianchi, G.; Sanseverino, E.R.; Gallo, P. Privacy and Transparency in Blockchain-Based Smart Grid Operations. *IEEE Access* **2023**, *11*, 120666–120679. https://doi.org/10.1109/ACCESS.2023.3326946.
44. Bertino, E.; Kundu, A.; Sura, Z. Data Transparency with Blockchain and AI Ethics. *Journal of Data and Information Quality (JDIQ)* **2019**, *11*, 1 – 8. https://doi.org/10.1145/3312750.
45. Satybaldy, A.; Nowostawski, M. Review of Techniques for Privacy-Preserving Blockchain Systems. *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure* **2020**. https://doi.org/10.1145/3384943.3409416.
46. Joshi, M.L.; Kanoongo, N. Depression detection using emotional artificial intelligence and machine learning: A closer review. *Materials Today: Proceedings* **2022**, *58*, 217–226.
47. Kaywan, P.; Ahmed, K.; Ibaida, A.; Miao, Y.; Gu, B. Early detection of depression using a conversational AI bot: A non-clinical trial. *Plos one* **2023**, *18*, e0279743.
48. Martins, R.; Almeida, J.J.; Henriques, P.R.; Novais, P. Identifying Depression Clues using Emotions and AI. In Proceedings of the ICAART (2), 2021, pp. 1137–1143.
49. Benefo, E.O.; Tingler, A.; White, M.; Cover, J.; Torres, L.; Broussard, C.; Shirmohammadi, A.; Pradhan, A.K.; Patra, D. Ethical, legal, social, and economic (ELSE) implications of artificial intelligence at a global level: a scientometrics approach. *AI and Ethics* **2022**, *2*, 667–682.
50. Acemoglu, D. Harms of AI (No. w29247), 2021.
51. Garcia, P.; Darroch, F.; West, L.; BrooksCleator, L. Ethical applications of big data-driven AI on social systems: Literature analysis and example deployment use case. *Information* **2020**, *11*, 235.

52. Garcia, P.; Darroch, F.; West, L.; BrooksCleator, L. Ethical applications of big data-driven AI on social systems: Literature analysis and example deployment use case. *Information* **2020**, *11*, 235.
53. Dignum, V. Responsibility and artificial intelligence. In *The Oxford Handbook of Ethics of AI*; 2020; Vol. 4698, p. 215.
54. Huriye, A.Z. The ethics of artificial intelligence: examining the ethical considerations surrounding the development and use of AI. *American Journal of Technology* **2023**, *2*, 37–44.
55. Jacobs, J. The artificial intelligence shock and socio-political polarization. *Technological Forecasting and Social Change* **2024**, *199*. Article 123006.
56. Hagerty, A.; Rubinov, I. Global AI ethics: a review of the social impacts and ethical implications of artificial intelligence. *arXiv preprint arXiv:1907.07892* **2019**.
57. Wamba, S.F.; Bawack, R.E.; Guthrie, C.; Queiroz, M.M.; Carillo, K.D.A. Are we preparing for a good AI society? A bibliometric review and research agenda. *Technological Forecasting and Social Change* **2021**, *164*, 120482.
58. Ashok, M.; Madan, R.; Joha, A.; Sivarajah, U. Ethical framework for Artificial Intelligence and Digital technologies. *International Journal of Information Management* **2022**, *62*. Article 102433.
59. Cote, M.; Nightingale, A.J. Resilience thinking meets social theory: Situating social change in socio-ecological systems (SES) research. *Progress in human geography* **2012**, *36*, 475–489.
60. Kou, C.; Yang, X. Improving social resilience amid the COVID-19 epidemic: A system dynamics model. *Plos one* **2023**, *18*, e0294108.
61. Keck, M.; Sakdapolrak, P. What is social resilience? Lessons learned and ways forward. *Erdkunde* **2013**, pp. 5–19.
62. Hu, Q.; Lu, Y.; Pan, Z.; Wang, B. How does AI use drive individual digital resilience? a conservation of resources (COR) theory perspective. *Behaviour & Information Technology* **2023**, *42*, 2654–2673.
63. Velasco, J.M.; Domínguez, M.G. Variables implicadas en la resiliencia social: De la resiliencia individual a la resiliencia de las sociedades. *VISUAL REVIEW. International Visual Culture Review/Revista Internacional de Cultura Visual* **2022**, *12*, 1–15.
64. Cody, T.; Beling, P.A. Towards operational resilience for AI-based cyber in multi-domain operations. In Proceedings of the Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications V; SPIE., Ed., June 2023, pp. 368–373.
65. Moskalenko, V.; Kharchenko, V.; Moskalenko, A.; Kuzikov, B. Resilience and resilient systems of artificial intelligence: Taxonomy, models and methods. *Algorithms* **2023**, *16*, 165.
66. Carlton, A. Sextortion: The Hybrid Cyber-Sex Crime. *NCJL & Tech.* **2019**, *21*, 177.
67. Küpeli, C. Legal Analysis of Sextortion Crime in The Comperative Law and Turkish Law. *Health Sciences Quarterly* **2019**, *3*, 87–98.
68. Carlton, A. Sextortion: The Hybrid Cyber-Sex Crime. *NCJL & Tech.* **2019**, *21*, 177.
69. Sorbán, K. An elephant in the room—EU policy gaps in the regulation of moderating illegal sexual content on video-sharing platforms. *International Journal of Law and Information Technology* **2023**, *31*, 171–185.
70. Norta, A.; Sotiris, M. Designing Artificial Intelligence Equipped Social Decentralized Autonomous Organizations for Tackling Sextortion Cases Version 0.7. *arXiv preprint arXiv:2312.14090* **2023**.
71. Sunde, N.; Sunde, I.M. Conceptualizing an AI-based Police Robot for Preventing Online Child Sexual Exploitation and Abuse: Part I–The Theoretical and Technical Foundations for PrevBOT. *Nordic Journal of Studies in Policing* **2021**, *8*, 1–21.
72. Indonesia, T.I. Sextortion: Corruption and Sexual Exploitation, 2023. http://ti.or.id/publikasi/sextortion/ENG_briefing_paper_s Accessed: 2024-09-24.
73. Fletcher, R.; Tzani, C.; Ioannou, M. The dark side of Artificial Intelligence–Risks arising in dating applications. *Assessment and Development Matters* **2024**, *16*, 17–23.
74. Okolie, C. Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns. *Journal of International Women's Studies* **2023**, *25*, 11.
75. Adomavicius, G.; Bockstedt, J.C.; Gupta, A.; Kauffman, R.J. Technology roles and paths of influence in an ecosystem model of technology evolution. *Information Technology and Management* **2007**, *8*, 185–202.
76. Brockman, B.; etal.. Investing in AI for Good. *Stanford Social Innovation Review* **2023**. https://ssir.org/articles/entry/investing_in_ai_for_good, Accessed: 2024-09-24.
77. Floridi, L.; Cowls, J.; Beltrametti, M.; Chatila, R.; Chazerand, P.; Dignum, V.; others.; Vayena, E. AI4People—an ethical framework for a good AI society: opportunities, risks, principles, and recommendations. *Minds and machines* **2018**, *28*, 689–707.

78. Jobin, A.; Ienca, M.; Vayena, E. The global landscape of AI ethics guidelines. *Nature machine intelligence* **2019**, *1*, 389–399.
79. Whittlestone, J.; Nyrup, R.; Alexandrova, A.; Dihal, K.; Cave, S. *Ethical and societal implications of algorithms, data, and artificial intelligence: a roadmap for research*; Nuffield Foundation: London, 2019.
80. Mittelstadt, B.D.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L. The ethics of algorithms: Mapping the debate. *Big Data & Society* **2016**, *3*, 205395.
81. Floridi, L.; Cowls, J.; King, T.C.; Taddeo, M. How to design AI for social good: Seven essential factors. *Ethics, Governance, and Policies in Artificial Intelligence* **2021**, pp. 125–151.
82. Cowls, J.; Tsamados, A.; Taddeo, M.; Floridi, L. A definition, benchmark and database of AI for social good initiatives. *Nature Machine Intelligence* **2021**, *3*, 111–115.
83. Floridi, L.; Cowls, J. A unified framework of five principles for AI in society. *Machine learning and the city: Applications in architecture and urban design* **2022**, pp. 535–545.
84. Umbrello, S.; Van de Poel, I. Mapping value sensitive design onto AI for social good principles. *AI and Ethics* **2021**, *1*, 283–296.
85. Cheng, L.; Varshney, K.R.; Liu, H. Socially responsible ai algorithms: Issues, purposes, and challenges. *Journal of Artificial Intelligence Research* **2021**, *71*, 1137–1181.
86. Berendt, B. AI for the Common Good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics* **2019**, *10*, 44–65.
87. Berryhill, J.; Heang, K.K.; Clogher, R.; McBride, K. Hello, World: Artificial intelligence and its use in the public sector.
88. Vesnic-Alujevic, L.; Nascimento, S.; Polvora, A. Societal and ethical impacts of artificial intelligence: Critical notes on European policy frameworks. *Telecommunications Policy* **2020**, *44*, 101961.
89. European Commission. *The Assessment list for trustworthy artificial intelligence (ALTAI) for self assessment*; 2020; pp. 1–34.
90. Stahl, B.C.; Leach, T. Assessing the ethical and social concerns of artificial intelligence in neuroinformatics research: an empirical test of the European Union Assessment List for Trustworthy AI (ALTAI). *AI and Ethics* **2023**, *3*. https://doi.org/10.1007/s43681-022-00201-4.
91. Commission, E. The general data protection regulation, 2018.
92. Chaturvedi, A. Defining Legal Responsibility in the Age of AI: Addressing Gaps in Data Privacy Regulation. *Indian J. Integrated Rsch. L.* **2023**, *3*, 1.
93. Bondi, E.; Xu, L.; Acosta-Navas, D.; Killian, J.A. Envisioning communities: a participatory approach towards AI for social good. In Proceedings of the Proceedings of the 2021 AAAI/ACM Conference on AI, and Society, July 2021; pp. 425–436.
94. Butt, A.; Junejo, A.Z.; Ghulamani, S.; Mahdi, G.; Shah, A.; Khan, D. Deploying Blockchains to Simplify AI Algorithm Auditing. In Proceedings of the 2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS), 2023, pp. 1–6. https://doi.org/10.1109/ICETAS59148.2023.10346420.
95. Gozman, D.; Liebenau, J.; Aste, T. A Case Study of Using Blockchain Technology in Regulatory Technology. *MIS Q. Executive* **2020**, *19*, 4. https://doi.org/10.17705/2msqe.00023.
96. Helo, P.; Hao, Y. Blockchains in operations and supply chains: A model and reference implementation. *Comput. Ind. Eng.* **2019**, *136*, 242–251. https://doi.org/10.1016/J.CIE.2019.07.023.
97. Ma, S.; Cao, Y.; Xiong, L. Efficient logging and querying for blockchain-based cross-site genomic dataset access audit. *BMC Medical Genomics* **2019**, *13*. https://doi.org/10.1186/s12920-020-0725-y.
98. Pagano, T.P.; et al. Bias and Unfairness in Machine Learning Models: A Systematic Review on Datasets, Tools, Fairness Metrics, and Identification and Mitigation Methods. *Big Data Cogn. Comput.* **2023**, *7*, 15. https://doi.org/10.3390/bdcc7010015.
99. Salah, K.; Rehman, M.H.; Nizamuddin, N.; Al-Fuqaha, A.I. Blockchain for AI: Review and Open Research Challenges. *IEEE Access* **2019**, *7*, 10127–10149. https://doi.org/10.1109/ACCESS.2018.2890507.
100. Varghese, I.K.; et al. Blockchain Technology in the Intrusion Detection Domain. *International Journal on Recent and Innovation Trends in Computing and Communication* **2023**. https://doi.org/10.17762/ijritcc.v11i10.8748.
101. Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **2019**, *49*, 2266–2277. https://doi.org/10.1109/TSMC.2019.2895123.
102. Yeung, K. Regulation by Blockchain: The Emerging Battle for Supremacy between the Code of Law and Code as Law. *Law* **2018**. https://doi.org/10.1111/1468-2230.12399.

103. Özdayi, M.S.; Kantarcioglu, M.; Malin, B. Leveraging blockchain for immutable logging and querying across multiple sites. *BMC Medical Genomics* **2020**. https://doi.org/10.1186/s12920-020-0721-2.
104. Angraal, S.; Krumholz, H.; Schulz, W. Blockchain Technology: Applications in Health Care. *Circulation: Cardiovascular Quality and Outcomes* **2017**, *10*, e003800.
105. Anonymous. Decentralizing Privacy: Protecting Personal Data by Blockchain. *International Journal of Innovative Technology and Exploring Engineering* **2023**. https://doi.org/10.35940/ijitee.l1051.10812s19.
106. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology. *Sustainable Cities and Society* **2018**, *39*, 283–297. https://doi.org/10.1016/J.SCS.2018.02.014.
107. Parker, B.; Bach, C. The Synthesis of Blockchain, Artificial Intelligence and Internet of Things. *European Journal of Engineering Research and Science* **2020**, *5*, 588–593. https://doi.org/10.24018/ejers.2020.5.5.1912.
108. Ponsam, J.G.; Duvvuri, S.; Roy, S. Electronic Healthcare Management System Using Blockchain Technology. In Proceedings of the 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT). IEEE, 2023, pp. 869–877.
109. Shrestha, S.; Panta, S. Blockchain-based Electronic Health Record Management System. *September 2023* **2023**. https://doi.org/10.36548/jaicn.2023.3.006.
110. Vazirani, A.A.; O'Donoghue, O.; Brindley, D.; Meinert, E. Blockchain vehicles for efficient Medical Record management. *NPJ Digital Medicine* **2020**, *3*. https://doi.org/10.1038/s41746-019-0211-0.
111. Caarten, A.B.; van Heugten, L.; Merkle, O. The intersection of corruption and gender-based violence: Examining the gendered experiences of sextortion during migration to South Africa. *African journal of reproductive health* **2022**, *26 6*, 45–54. https://doi.org/10.29063/ajrh2022/v26i6.6.
112. Zheng, Y.; Hu, J.; Zhu, Y. Research on Blockchain Application for Compliance Management in Import and Export Trade. In Proceedings of the Proceedings of the 2nd International Conference on Public Management, Digital Economy and Internet Technology, ICPDI 2023. Chongqing, China, 2023. https://doi.org/10.4108/eai.1-9-2023.2338761.
113. Antinucci, M. EU Ethical Charter on the Use of Artificial Intelligence in Judicial Systems with a part of the law being established on Blockchain as a trojan horse anti-counterfeiting in a Global perspective. *Courier of Kutafin Moscow State Law University* **2020**. https://doi.org/10.17803/2311-5998.2020.66.2.036-042.
114. Bernal Bernabe, J.; Cánovas, J.L.; Hernández-Ramos, J.L.; Torres Moreno, R.; Skarmeta, A. Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access* **2019**, *7*, 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872.
115. Finck, M. BRIEFING-Blockchain and the General Data Protection Regulation-Can distributed ledgers be squared with **2019**.
116. Kerknawi, L.; Mäkelä, A. Building a forward-looking EU policy strategy on blockchain. College of Europe Policy Brief# 12.18, September 2018 **2018**.
117. Lescisin, M.; Mahmoud, Q. A Blockchain-Based Solution for Defining and Enforcing Personal Data Access Policies. *2023 International Conference on Information Technology (ICIT)* **2023**, pp. 118–124. https://doi.org/10.1109/ICIT58056.2023.10226063.
118. Murthy, M.S. Data protection law and policy in the USA: An overview. *Issue 3 Indian JL & Legal Rsch.* **2022**, *4*, 1.
119. Alex, N.; Sotiris, M. Designing Artificial Intelligence Equipped Social Decentralized Autonomous Organizations for Tackling Sextortion Cases Version 0.7. *arXiv preprint arXiv:2312.14090* **2023**.
120. Yang, Q.; Liu, Y.; Chen, T.; Tong, Y. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)* **2019**, *10*, 1–19.
121. Unal, D.; Hammoudeh, M.; Khan, M.A.; Abuarqoub, A.; Epiphaniou, G.; Hamila, R. Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things. *Computers & Security* **2021**, *109*, 102393.
122. Norta, A.; Hawthorne, D.; Engel, S.L. A privacy-protecting data-exchange wallet with ownership-and monetization capabilities. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN). IEEE, 2018, pp. 1–8.
123. Xiao, L.; Han, D.; Zhou, S.; Xu, N.; Chen, L.; Xie, S. A Blockchain-empowered Federated Learning Framework Supprting GDPR-compliance. *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)* **2023**, pp. 399–404. https://doi.org/10.1109/CSCloud-EdgeCom58631.2023.00074.

124. Lo, S.K.; Liu, Y.; Lu, Q.; Wang, C.; Xu, X.; young Paik, H.; Zhu, L. Toward Trustworthy AI: Blockchain-Based Architecture Design for Accountability and Fairness of Federated Learning Systems. *IEEE Internet of Things Journal* **2023**, *10*, 3276–3284. https://doi.org/10.1109/JIOT.2022.3144450.
125. Miao, Y.; Liu, Z.; Li, H.; Choo, K.; Deng, R. Privacy-Preserving Byzantine-Robust Federated Learning via Blockchain Systems. *IEEE Transactions on Information Forensics and Security* **2022**, *17*, 2848–2861. https://doi.org/10.1109/tifs.2022.3196274.
126. Yang, Z.; Shi, Y.; Zhou, Y.; Wang, Z.; Yang, K. Trustworthy Federated Learning via Blockchain. *IEEE Internet of Things Journal* **2022**, *10*, 92–109. https://doi.org/10.1109/JIOT.2022.3201117.
127. Zuo, X.; Wang, M.; Zhu, T.; Zhang, L.; Yu, S.; Zhou, W. Federated Learning with Blockchain-Enhanced Machine Unlearning: A Trustworthy Approach. *ArXiv* **2024**, *abs/2405.20776*. https://doi.org/10.48550/arXiv.2405.20776.
128. Jain, C.; Chaudhari, P. Blockchain-Aided Privacy Preserving Framework for Federated Learning. *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)* **2024**, pp. 1–6. https://doi.org/10.1109/IITCEE59897.2024.10467294.
129. for Disease Control, C.; Prevention. Health Insurance Portability and Accountability Act of 1996 (HIPAA), 2023. https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html, Accessed: 2024-09-24.
130. Tang, Y.; Xiong, J.; Becerril-Arreola, R.; Iyer, L. Ethics of blockchain: A framework of technology, applications, impacts, and research directions. *Information Technology & People* **2020**, *33*, 602–632.
131. Reddy, B.; Madhushree.; Aithal, P. Blockchain as a Disruptive Technology in Healthcare and Financial Services - a Review Based Analysis on Current Implementations. *Organizations & Markets: Policies & Processes eJournal* **2020**.
132. Sharma, P.; Namasudra, S.; Chilamkurti, N.; Kim, B.G.; González Crespo, R. Blockchain-Based Privacy Preservation for IoT-Enabled Healthcare System. *ACM Transactions on Sensor Networks* **2022**, *19*, 1 – 17. https://doi.org/10.1145/3577926.
133. Cui, B.; Mei, T. ABFL: A Blockchain-enabled Robust Framework for Secure and Trustworthy Federated Learning. *Proceedings of the 39th Annual Computer Security Applications Conference* **2023**. https://doi.org/10.1145/3627106.3627121.
134. Feng, L.; Zhao, Y.; Guo, S.; Qiu, X.; Li, W.; Peng, Y. BAFL: A Blockchain-Based Asynchronous Federated Learning Framework. *IEEE Transactions on Computers* **2022**, *71*, 1092–1103. https://doi.org/10.1109/TC.2021.3072033.
135. Liu, W.; He, Y.; Wang, X.; Duan, Z.; Liang, W.; Liu, Y. BFG: privacy protection framework for internet of medical things based on blockchain and federated learning. *Connection Science* **2023**, *35*. https://doi.org/10.1080/09540091.2023.2199951.
136. Preuveneers, D.; Rimmer, V.; Tsingenopoulos, I.; Spooren, J.; Joosen, W.; Ilie-Zudor, E. Chained Anomaly Detection Models for Federated Learning: An Intrusion Detection Case Study. *Applied Sciences* **2018**. https://doi.org/10.3390/APP8122663.
137. Moulahi, T.; Jabbar, R.; Alabdulatif, A.; Abbas, S.; El Khediri, S.; Zidi, S.; Rizwan, M. Privacy-preserving federated learning cyber-threat detection for intelligent transport systems with blockchain-based security. *Expert Systems* **2023**, *40*, e13103.
138. Bodemer, O. The Unseen Guardian: How Blockchain, Java, and AI Stealthily Became the Sherlock Holmes of Cybersecurity. *Authorea Preprints* **2023**.
139. Paquet-Clouston, M.; Romiti, M.; Haslhofer, B.; Charvat, T. Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem. *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* **2019**. https://doi.org/10.1145/3318041.3355466.
140. Fahlevi, M.; Moeljadi.; Aisjah, S.; Djazuli, A. Corporate Governance in the Digital Age: A Comprehensive Review of Blockchain, AI, and Big Data Impacts, Opportunities, and Challenges. *E3S Web of Conferences* **2023**. https://doi.org/10.1051/e3sconf/202344802056.
141. Otoum, S.; Mouftah, H. Enabling Trustworthiness in Sustainable Energy Infrastructure Through Blockchain and AI-Assisted Solutions. *IEEE Wireless Communications* **2021**, *28*, 19–25. https://doi.org/10.1109/MWC.018.2100194.
142. Michaelson, P. Arbitrating Disputes Involving Blockchains, Smart Contracts, and Smart Legal Contracts. *Cybersecurity* **2020**. https://doi.org/10.2139/ssrn.3720876.
143. Ranjan, A.; Singh, A.N.; Kumar, A.; Manoj, T.; Kumar. Transforming Judicial Systems with Blockchain: A Court Case Governance System for Tamper-Proof and Transparent Legal Processes. In Proceedings

of the 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), 2023. https://doi.org/10.1109/ICAISC58445.2023.10200234.

144. Yeoh, P. Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance* **2017**, *25*, 196–208. https://doi.org/10.1108/JFRC-08-2016-0068.
145. Nguyen, Q.; Dang, Q.V. Blockchain Technology for the Advancement of the Future. In Proceedings of the 2018 4th International Conference on Green Technology and Sustainable Development (GTSD), 2018, pp. 483–486. https://doi.org/10.1109/GTSD.2018.8595577.
146. Feng, L.; Zhao, Y.; Guo, S.; Qiu, X.; Li, W.; Peng, Y. Blockchain-based Asynchronous Federated Learning for Internet of Things. *IEEE Transactions on Computers* **2021**, pp. 1–1. https://doi.org/10.1109/TC.2021.3072033.
147. Chang, Y.; Fang, C.; Sun, W. A Blockchain-Based Federated Learning Method for Smart Healthcare. *Computational Intelligence and Neuroscience* **2021**, *2021*. https://doi.org/10.1155/2021/4376418.
148. Attiaoui, A.; Kobbane, A.; Elhachmi, J.; Ayaida, M.; Chougdali, K. Blockchain-Enabled Defense Mechanism for Protecting Federated Learning Systems Against Malicious Node Updates. *2024 4th Interdisciplinary Conference on Electrics and Computer (INTCEC)* **2024**, pp. 1–6. https://doi.org/10.1109/INTCEC61833.2024.10602881.
149. Heiss, J.; Grunewald, E.; Haimerl, N.; Schulte, S.; Tai, S. Advancing Blockchain-based Federated Learning through Verifiable Off-chain Computations. *2022 IEEE International Conference on Blockchain (Blockchain)* **2022**, pp. 194–201. https://doi.org/10.1109/Blockchain55522.2022.00034.
150. Glaesser, F. Does the Transparent Blockchain Technology Offer Solutions to the Algorithmic Fairness Problem? *Artificial Intelligence - Law* **2018**. https://doi.org/10.2139/ssrn.3378071.
151. Chowdhury, R.H. Blockchain and AI: Driving the future of data security and business intelligence. *World Journal of Advanced Research and Reviews* **2024**. https://doi.org/10.30574/wjarr.2024.23.1.2273.
152. Rane, N.; Choudhary, S.; Rane, J. Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance. *SSRN Electronic Journal* **2023**. https://doi.org/10.2139/ssrn.4644253.
153. Jain, A.; Praveena, K.; Anandhi, R.J.; Kumar, S.; Alabdely, H.; Srivastava, A.P. Blockchain and Machine Learning for Automated Compliance in Regulatory Technology. *2024 IEEE 13th International Conference on Communication Systems and Network Technologies (CSNT)* **2024**, pp. 1–6. https://doi.org/10.1109/CSNT60213.2024.10546202.
154. Mumporeze, N.; Han-Jin, E.; Nduhura, D. Let's spend a night together; i will increase your salary: an analysis of sextortion phenomenon in Rwandan society. *Journal of Sexual Aggression* **2019**, *27*, 120 – 137. https://doi.org/10.1080/13552600.2019.1692920.
155. Fawole, O. Economic Violence To Women and Girls. *Trauma, Violence, & Abuse* **2008**, *9*, 167 – 177. https://doi.org/10.1177/1524838008319255.
156. Kapoor, O.; et al. Implementing decentralized storage using blockchain to address data ownership and privacy concerns. *International Journal of Advance Research, Ideas and Innovations in Technology* **2018**, *4*, 2015–2020.
157. Zyskind, G.; Nathan, O.; Pentland, A. Decentralizing Privacy: Using Blockchain to Protect Personal Data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, 2015, pp. 180–184. https://doi.org/10.1109/SPW.2015.27.
158. Zuboff, S. The age of surveillance capitalism. In *Social theory re-wired*; Routledge, 2023; pp. 203–213.
159. Li, G.; Zhao, Q.; Wang, Y.; Qiu, T.; Xie, K.; Feng, L. A Blockchain-Based Decentralized Framework for Fair Data Processing. *IEEE Transactions on Network Science and Engineering* **2021**, *8*, 2301–2315. https://doi.org/10.1109/TNSE.2021.3086332.
160. Nassar, M.; Salah, K.; Rehman, M.H.; Svetinovic, D. Blockchain for explainable and trustworthy artificial intelligence. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* **2019**, *10*. https://doi.org/10.1002/widm.1340.
161. Mehrabi, N.; Morstatter, F.; Saxena, N.; Lerman, K.; Galstyan, A. A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys (CSUR)* **2019**, *54*, 1 – 35. https://doi.org/10.1145/3457607.
162. Chen, Y.; Bellavitis, C. Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models. *Stevens Institute of Technology - School of Business Research Paper Series* **2019**. https://doi.org/10.2139/ssrn.3483608.
163. Vishwa, A.; Hussain, F. A Blockchain-Based Approach for Multimedia Privacy Protection and Provenance. In Proceedings of the 2018 IEEE Symposium Series on Computational Intelligence (SSCI), 2018, pp. 1941–1945. https://doi.org/10.1109/SSCI.2018.8628636.

164. Paquet-Clouston, M.; Romiti, M.; Haslhofer, B.; Charvat, T. Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem. *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* **2019**. https://doi.org/10.1145/3318041.3355466.
165. PARASCHIVEANU, V.; RICHARDSON, G.; VOICU-DOROBANȚU, R. EDUCATION 3.0: BLOCKCHAIN-BACKED MOOCS. *eLearning & Software for Education* **2020**, *3*.
166. Patil, S.; Desai, D. AI Enabled Blockchain solution for the Indian Judicial System. In Proceedings of the 2023 International Conference on Emerging Smart Computing and Informatics (ESCI). IEEE, 2023, pp. 1–6.
167. O'Malley, R.L.; Holt, K.M. Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. *Journal of interpersonal violence* **2022**, *37*, 258–283.
168. Rao, S.; Fernandes, S.; Raorane, S.; Syed, S.F. A Novel Approach for Digital Evidence Management Using Blockchain. *SSRN Electronic Journal* **2020**. https://doi.org/10.2139/ssrn.3683280.
169. Ahmad, L.; Khanji, S.; Iqbal, F.; Kamoun, F. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. *Proceedings of the 15th International Conference on Availability, Reliability and Security* **2020**. https://doi.org/10.1145/3407023.3409199.
170. Tian, Z.; Li, M.; Qiu, M.; Sun, Y.; Su, S. Block-DEF: A secure digital evidence framework using blockchain. *Inf. Sci.* **2019**, *491*, 151–165. https://doi.org/10.1016/J.INS.2019.04.011.
171. Ghimire, S.; Choi, J.; Lee, B. Using Blockchain for Improved Video Integrity Verification. *IEEE Transactions on Multimedia* **2020**, *22*, 108–121. https://doi.org/10.1109/TMM.2019.2925961.
172. Kennedi, K.M.; Varghese, K.J.; Sajan, S.; Saji, S.E.; Hari, M.; Kizhakkethottam, J.J. Identification of Fraud Investigator in Digital Forensics Investigation Using Blockchain. *SSRN Electronic Journal* **2021**. https://doi.org/10.2139/ssrn.3883428.
173. Bazarhanova, A.; Magnusson, J.; Lindman, J.; Chou, E.; Nilsson, A. Blockchain-based electronic identification: cross-country comparison of six design choices **2019**.
174. Lin, C.; He, D.; Huang, X.; Khan, M.; Choo, K. DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain. *IEEE Transactions on Information Forensics and Security* **2020**, *15*, 2440–2452. https://doi.org/10.1109/TIFS.2020.2969565.
175. Myeong, S.; Jung, Y. Administrative Reforms in the Fourth Industrial Revolution: The Case of Blockchain Use. *Sustainability* **2019**. https://doi.org/10.3390/SU11143971.
176. Marinakis, V.; Koutsellis, T.; Nikas, A.; Doukas, H. AI and Data Democratisation for Intelligent Energy Management. *Energies* **2021**. https://doi.org/10.3390/EN14144341.
177. Karuppiah, K.; Sankaranarayanan, B.; Ali, S. A decision-aid model for evaluating challenges to blockchain adoption in supply chains. *International Journal of Logistics Research and Applications* **2021**, *26*, 257 – 278. https://doi.org/10.1080/13675567.2021.1947999.
178. Jha, R.K.; Patel, A.; Shah, B.K. Synergies and Challenges: Integrating Machine Learning, Blockchain Technology, and Regulatory Frameworks in Biomedical Cybersecurity. *Journal of ISMAC* **2023**. https://doi.org/10.36548/jismac.2023.3.004.
179. Wardhani, R.W.; Putranto, D.; Le, T.T.H.; Oktian, Y.; Jo, U.; Prihatno, A.T.; Suryanto, N.; Kim, H. Trend of Paradigm for integrating Blockchain, Artificial Intelligence, Quantum Computing, and Internet of Things. *Korean Institute of Smart Media* **2023**. https://doi.org/10.30693/smj.2023.12.2.42.
180. Xuan, T.R.; Ness, S. Integration of Blockchain and AI: Exploring Application in the Digital Business. *Journal of Engineering Research and Reports* **2023**. https://doi.org/10.9734/jerr/2023/v25i8955.
181. Politou, E.; Casino, F.; Alepis, E.; Patsakis, C. Blockchain Mutability: Challenges and Proposed Solutions. *IEEE Transactions on Emerging Topics in Computing* **2019**, *9*, 1972–1986. https://doi.org/10.1109/tetc.2019.2949510.
182. Niya, S.R.; Willems, J.; Stiller, B. A Case Study of a Blockchain-GDPR Adaptation. *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* **2022**, pp. 1–3. https://doi.org/10.1109/ICBC54727.2022.9805553.
183. Zhang, W.; Yuan, Y.; Yanyan, H.; Nandakumar, K.; Chopra, A.; Sim, S.; Caro, A.D. Blockchain-Based Distributed Compliance in Multinational Corporations' Cross-Border Intercompany Transactions. *Advances in Intelligent Systems and Computing* **2018**. https://doi.org/10.1007/978-3-030-03405-4_20.
184. Schmelz, D.; Fischer, G.; Niemeier, P.; Zhu, L.; Grechenig, T. Towards Using Public Blockchain in Information-Centric Networks: Challenges Imposed by the European Union's General Data Protection Regulation. *2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)* **2018**, pp. 223–228. https://doi.org/10.1109/HOTICN.2018.8606000.

185. Hupont, I.; Micheli, M.; Delipetrev, B.; Gómez, E.; Garrido, J.S. Documenting High-Risk AI: A European Regulatory Perspective. *Computer* **2023**, *56*, 18–27. https://doi.org/10.1109/MC.2023.3235712.
186. Wachter, S.; Mittelstadt, B.; Russell, C. Bias Preservation in Machine Learning: The Legality of Fairness Metrics Under EU Non-Discrimination Law. *SSRN Electronic Journal* **2021**. https://doi.org/10.2139/SSRN.3792772.
187. Gyevnar, B.; Ferguson, N. Aligning Explainable AI and the Law: The European Perspective. *ArXiv* **2023**, *abs/2302.10766*. https://doi.org/10.48550/arXiv.2302.10766.
188. Olena, O. Political and Legal Implications of the Use of Artificial Intelligence. *Yearly journal of scientific articles "Pravova derzhava"* **2023**. https://doi.org/10.33663/1563-3349-2023-34-684-693.
189. Schwerin, S. Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR): A Delphi Study. *The Journal of the British Blockchain Association* **2018**. https://doi.org/10.31585/JBBA-1-1-(4)2018.
190. Wachter, S.; Mittelstadt, B.; Russell, C. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *ArXiv* **2020**, *abs/2005.05906*. https://doi.org/10.2139/ssrn.3547922.
191. Hacker, P.; Cordes, J.; Rochon, J. Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond. *European Journal of Risk Regulation* **2023**. https://doi.org/10.1017/err.2023.81.
192. Tatar, U.; Gokce, Y.; Nussbaum, B. Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Comput. Law Secur. Rev.* **2020**, *38*, 105454. https://doi.org/10.1016/j.clsr.2020.105454.
193. Politou, E.; Alepis, E.; Patsakis, C. Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *J. Cybersecur.* **2018**, *4*, tyy001. https://doi.org/10.1093/cybsec/tyy001.
194. Bayle, A.; Koscina, M.; Manset, D.; Perez-Kempner, O. When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry. *2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI)* **2018**, pp. 788–792. https://doi.org/10.1109/WI.2018.00133.
195. Ameyed, D.; Jaafar, F.; Migneault, F.C.; Cheriet, M. Blockchain Based Model for Consent Management and Data Transparency Assurance. *2021 IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)* **2021**, pp. 1050–1059. https://doi.org/10.1109/QRS-C55045.2021.00159.
196. Fabbrini, F.; Celeste, E. The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal* **2020**, *21*, 55 – 65. https://doi.org/10.1017/glj.2020.14.
197. Mangini, V.; Tal, I.; Moldovan, A.N. An empirical study on the impact of GDPR and right to be forgotten - organisations and users perspective. *Proceedings of the 15th International Conference on Availability, Reliability and Security* **2020**. https://doi.org/10.1145/3407023.3407080.
198. Ranchordas, S. Experimental regulations for AI: sandboxes for morals and mores. *University of Groningen Faculty of Law Research Paper* **2021**.
199. Buocz, T.; Pfotenhauer, S.; Eisenberger, I. Regulatory sandboxes in the AI Act: reconciling innovation and safety? *Law, Innovation and Technology* **2023**, *15*, 357 – 389. https://doi.org/10.1080/17579961.2023.2245678.
200. Truby, J.; Brown, R.; Ibrahim, I.; Parellada, O.C. A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications. *European Journal of Risk Regulation* **2021**, *13*, 270 – 294. https://doi.org/10.1017/err.2021.52.
201. Morgan, D. Anticipatory regulatory instruments for AI systems: A comparative study of regulatory sandbox schemes. *Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society* **2023**. https://doi.org/10.1145/3600211.3604732.
202. ÓhÉigeartaigh, S.S.; Whittlestone, J.; Liu, Y.; Zeng, Y.; Liu, Z. Overcoming barriers to cross-cultural cooperation in AI ethics and governance. *Philosophy & technology* **2020**, *33*, 571–593.
203. OECD Framework for the Classification of AI systems. *OECD Digital Economy Papers* **2022**. https://doi.org/10.1787/cb6d9eca-en.
204. Building the Future of EU: Moving forward with International Collaboration on Blockchain. *The Journal of the British Blockchain Association* **2018**. https://doi.org/10.31585/JBBA-1-1-(7)2018.
205. Zhao, Y.; Li, M.; Lai, L.; Suda, N.; Civin, D.; Chandra, V. Federated Learning with Non-IID Data. *ArXiv* **2018**, *abs/1806.00582*. https://doi.org/10.48550/arXiv.1806.00582.
206. Liu, Z.; Hu, S.; Wu, Z.S.; Smith, V. On Privacy and Personalization in Cross-Silo Federated Learning. *ArXiv* **2022**, *abs/2206.07902*. https://doi.org/10.48550/arXiv.2206.07902.
207. Tran, H.Y.; Hu, J.; Yin, X.; Pota, H. An Efficient Privacy-Enhancing Cross-Silo Federated Learning and Applications for False Data Injection Attack Detection in Smart Grids. *IEEE Transactions on Information Forensics and Security* **2023**, *18*, 2538–2552. https://doi.org/10.1109/TIFS.2023.3267892.

208. Liu, Y.; Liu, Y.; Liu, Z.; Liang, Y.; Meng, C.; Zhang, J.; Zheng, Y. Federated Forest. *IEEE Transactions on Big Data* **2019**, *8*, 843–854. https://doi.org/10.1109/TBDATA.2020.2992755.
209. Zhang, H.; Xu, S.; Xin, J.; Xu, H. Blockchain based data management technology for future intelligent network architecture. *2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)* **2023**, pp. 1–6. https://doi.org/10.1109/BMSB58369.2023.10211131.
210. Zuo, Y.; Guo, J.; Gao, N.; Zhu, Y.; Jin, S.; Li, X. A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications. *IEEE Communications Surveys & Tutorials* **2023**, *25*, 2494–2528. https://doi.org/10.1109/COMST.2023.3315374.
211. Abdulrahman, Y.; Arnautovic, E.; Parezanović, V.D.; Svetinovic, D. AI and Blockchain Synergy in Aerospace Engineering: An Impact Survey on Operational Efficiency and Technological Challenges. *IEEE Access* **2023**, *11*, 87790–87804. https://doi.org/10.1109/ACCESS.2023.3305325.
212. Zhou, S.; Li, K.; Xiao, L.; Cai, J.; Liang, W.; Castiglione, A. A Systematic Review of Consensus Mechanisms in Blockchain. *Mathematics* **2023**. https://doi.org/10.3390/math11102248.
213. Alam, S. The Current State of Blockchain Consensus Mechanism: Issues and Future Works. *International Journal of Advanced Computer Science and Applications* **2023**. https://doi.org/10.14569/ijacsa.2023.0140810.
214. Kumar, A.; Sharma, N. An Investigation of Advancements in Blockchain Consensus Algorithms & Leading Protocols. *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)* **2023**, pp. 1–6. https://doi.org/10.1109/GCAT59970.2023.10353442.
215. Yulianto, S.; Hendric, H.L.; Warnars, S.; Prabowo, H.; Hidayanto, A. Security Risks and Best Practices for Blockchain and Smart Contracts: A Systematic Literature Review. *2023 International Conference on Information Management and Technology (ICIMTech)* **2023**, pp. 1–6. https://doi.org/10.1109/ICIMTech59029.2023.10278055.
216. He, D.; Wu, R.; Li, X.; Chan, S.; Guizani, M. Detection of Vulnerabilities of Blockchain Smart Contracts. *IEEE Internet of Things Journal* **2023**, *10*, 12178–12185. https://doi.org/10.1109/JIOT.2023.3241544.
217. Härer, F. A Cross-Chain Query Language for Application-Level Interoperability Between Open and Permissionless Blockchains. *arXiv preprint arXiv:2307.00951* **2023**.
218. M, D.; Amet, M.; Srivastava, G.; Crichigno, J. An Architecture That Enables Cross-Chain Interoperability for Next-Gen Blockchain Systems. *IEEE Internet of Things Journal* **2023**, *10*, 18282–18291. https://doi.org/10.1109/JIOT.2023.3279693.
219. Zala, K.; Modi, V.; Giri, D.; Acharya, B.; Mallik, S.; Qin, H. Unlocking Blockchain Interconnectivity: Smart Contract-Driven Cross-Chain Communication. *IEEE Access* **2023**, *11*, 75365–75380. https://doi.org/10.1109/ACCESS.2023.3296556.
220. Jasim, Z.A.; Hadi, A.K. Study on Blockchain Scalability Methods Limitation and Solution. *2023 International Conference on Engineering, Science and Advanced Technology (ICESAT)* **2023**, pp. 220–225. https://doi.org/10.1109/ICESAT58213.2023.10347291.
221. Rahman, F.; Titouna, C.; Naït-Abdesselam, F.; Serhrouchni, A. Scalable Blockchain Through Prioritised Sharding. *2023 6th International Conference on Advanced Communication Technologies and Networking (CommNet)* **2023**, pp. 1–6. https://doi.org/10.1109/CommNet60167.2023.10365307.
222. Dhulavvagol, P.M.; R, P.M.; Kundur, N.C.; N., J.; Totad, S.G. Scalable Blockchain Architecture: Leveraging Hybrid Shard Generation and Data Partitioning. *International Journal of Advanced Computer Science and Applications* **2023**. https://doi.org/10.14569/ijacsa.2023.0140839.
223. Singh, N.; Jain, K. Data Security Approach Using Blockchain Mechanism and Cryptography Algorithms. *2023 11th International Symposium on Digital Forensics and Security (ISDFS)* **2023**, pp. 1–6. https://doi.org/10.1109/ISDFS58141.2023.10131789.
224. Kandru, D.K.; Venkata, K.; Babu, S.P. Securing Data Over Network with Blockchain and AI. *europeanchemicalbulletin* **2023**. https://doi.org/10.48047/ecb/2023.12.si4.1003.
225. Alabadi, M.; Habbal, A. Next-generation predictive maintenance: leveraging blockchain and dynamic deep learning in a domain-independent system. *PeerJ Computer Science* **2023**. https://doi.org/10.7717/peerj-cs.1712.
226. Yang, J.; Yue, Z.; Yuan, Y. Noise-Aware Sparse Gaussian Processes and Application to Reliable Industrial Machinery Health Monitoring. *IEEE Transactions on Industrial Informatics* **2023**, *19*, 5995–6005. https://doi.org/10.1109/TII.2022.3200428.
227. Mishra, A.; Gangisetti, G.; Khazanchi, D. Integrating Edge-AI in Structural Health Monitoring domain. *ArXiv* **2023**, *abs/2304.03718*. https://doi.org/10.48550/arXiv.2304.03718.

228. Wang, T.; Ai, S.; Cao, J.; Zhao, Y. A Blockchain-Based Distributed Computational Resource Trading Strategy for Internet of Things Considering Multiple Preferences. *Symmetry* **2023**, *15*, 808. https://doi.org/10.3390/sym15040808.
229. Ye, X.; Li, M.; Si, P.; Yang, R.; Wang, Z.; Zhang, Y. Collaborative and Intelligent Resource Optimization for Computing and Caching in IoV With Blockchain and MEC Using A3C Approach. *IEEE Transactions on Vehicular Technology* **2023**, *72*, 1449–1463. https://doi.org/10.1109/TVT.2022.3210570.
230. Kumar, G.S.; Ramachandran, K.K.; Sharma, S.; Ramesh, R.; Qureshi, K.; Ganesh, K. AI-Assisted Resource Allocation for Improved Business Efficiency and Profitability. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* **2023**, pp. 54–58. https://doi.org/10.1109/ICACITE57410.2023.10182679.
231. Asif, R.; Hassan, S.R.; Parr, G. Integrating a Blockchain-Based Governance Framework for Responsible AI. *Future Internet* **2023**, *15*, 97. https://doi.org/10.3390/fi15030097.
232. Mylrea, M.; Robinson, N. Artificial Intelligence (AI) Trust Framework and Maturity Model: Applying an Entropy Lens to Improve Security, Privacy, and Ethical AI. *Entropy* **2023**, *25*. https://doi.org/10.3390/e25101429.
233. Han, J.; Lee, J.; Li, T. DAO Governance. *SSRN Electronic Journal* **2023**. https://doi.org/10.2139/ssrn.4346581.
234. Feichtinger, R.; Fritsch, R.; Vonlanthen, Y.; Wattenhofer, R. The Hidden Shortcomings of (D)AOs - An Empirical Study of On-Chain Governance. *ArXiv* **2023**, *abs/2302.12125*. https://doi.org/10.48550/arXiv.2302.12125.
235. Rikken, O.; Janssen, M.; Kwee, Z. Governance impacts of blockchain-based decentralized autonomous organizations: an empirical analysis. *Policy Design and Practice* **2023**, *6*, 465 – 487. https://doi.org/10.1080/25741292.2023.2270220.
236. Zhang, P.; Ding, S.; Zhao, Q. Exploiting Blockchain to Make AI Trustworthy: A Software Development Lifecycle View. *ACM Computing Surveys* **2023**. https://doi.org/10.1145/3614424.
237. Mbiazi, D.; Bhange, M.; Babaei, M.; Sheth, I.; Kenfack, P.J. Survey on AI Ethics: A Socio-technical Perspective. *ArXiv* **2023**, *abs/2311.17228*. https://doi.org/10.48550/arXiv.2311.17228.
238. Danilevskyi, M.; Tellez, F.P. On the compliance with ethical principles in AI. *Proceedings of the 2023 Conference on Human Centered Artificial Intelligence: Education and Practice* **2023**. https://doi.org/10.1145/3633083.3633223.
239. Birkstedt, T.; Minkkinen, M.; Tandon, A.; Mäntymäki, M. AI governance: themes, knowledge gaps and future agendas. *Internet Research* **2023**. https://doi.org/10.1108/intr-01-2022-0042.
240. Zhang, R.; Ramesh, B. A configurational perspective on design elements and user governance engagement in blockchain platforms. *Information Systems Journal* **2023**. https://doi.org/10.1111/isj.12494.
241. Wan, R.; Garcia, A.A.; Saxena, D.; Vajiac, C.; Kawakami, A.; Stapleton, L.; Zhu, H.; Holstein, K.; Candello, H.; Badillo-Urquiola, K.A. Community-driven AI: Empowering people through responsible data-driven decision-making. *Computer Supported Cooperative Work and Social Computing* **2023**. https://doi.org/10.1145/3584931.3611282.
242. Wang, L.; Guan, Z.; Chen, Z.; Hu, M. Enabling Integrity and Compliance Auditing in Blockchain-Based GDPR-Compliant Data Management. *IEEE Internet of Things Journal* **2023**, *10*, 20955–20968. https://doi.org/10.1109/JIOT.2023.3285211.
243. Shishodia, B.S.; Nene, M. Data Protection Regulations Using Blockchain. *2023 2nd International Conference for Innovation in Technology (INOCON)* **2023**, pp. 1–6. https://doi.org/10.1109/INOCON57975.2023.10101061.
244. Lescisin, M.; Mahmoud, Q. A Blockchain-Based Solution for Defining and Enforcing Personal Data Access Policies. *2023 International Conference on Information Technology (ICIT)* **2023**, pp. 118–124. https://doi.org/10.1109/ICIT58056.2023.10226063.
245. Li, S.; Xu, C.; Zhang, Y.; Du, Y.; Chen, K. Blockchain-Based Transparent Integrity Auditing and Encrypted Deduplication for Cloud Storage. *IEEE Transactions on Services Computing* **2023**, *16*, 134–146. https://doi.org/10.1109/TSC.2022.3144430.
246. Aswal, S.; Professor, A. Blockchain-Based Distributed Systems for Trust and Transparency. *Turkish Online Journal of Qualitative Inquiry* **2023**. https://doi.org/10.52783/tojqi.v11i4.10024.
247. Gabuthy, Y. Blockchain-Based Dispute Resolution: Insights and Challenges. *Games* **2023**, *14*, 34. https://doi.org/10.3390/g14030034.
248. Awan, K.A.; Din, I.; Almogren, A.S.; Seo-Kim, B. Blockchain-Based Trust Management for Virtual Entities in the Metaverse: A Model for Avatar and Virtual Organization Interactions. *IEEE Access* **2023**, *11*, 136370–136394. https://doi.org/10.1109/ACCESS.2023.3337806.

249. John, K.; Kogan, L.; Saleh, F. Smart Contracts and Decentralized Finance. *SSRN Electronic Journal* **2023**. https://doi.org/10.2139/ssrn.4222528.
250. Buccinca, Z.; Pham, C.M.; Jakesch, M.; Ribeiro, M.T.; Olteanu, A.; Amershi, S. AHA!: Facilitating AI Impact Assessment by Generating Examples of Harms. *ArXiv* **2023**, *abs/2306.03280*. https://doi.org/10.48550/arXiv.2306.03280.
251. Johnson, N.; Heidari, H. Assessing AI Impact Assessments: A Classroom Study. *ArXiv* **2023**, *abs/2311.11193*. https://doi.org/10.48550/arXiv.2311.11193.
252. Calvi, A.; Kotzinos, D. Enhancing AI fairness through impact assessment in the European Union: a legal and computer science perspective. *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency* **2023**. https://doi.org/10.1145/3593013.3594076.
253. Fahlevi, M.; Moeljadi.; Aisjah, S.; Djazuli, A. Corporate Governance in the Digital Age: A Comprehensive Review of Blockchain, AI, and Big Data Impacts, Opportunities, and Challenges. *E3S Web of Conferences* **2023**. https://doi.org/10.1051/e3sconf/202344802056.