

Article

Not peer-reviewed version

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: 3 March 2025

doi: 10.20944/preprints202501.1981.v2

Keywords: Ethical AI Development; Societal Resilience; Digital Ethics; Sextortion Mitigation; Blockchain



Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

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, Tallinn, Estonia

² Austrian Blockchain Center, Vienna, Austria

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 sexual exploitation leading to sextortion (a form of coercion) that disproportionately affects vulnerable groups, such as minors. This 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 through the integration of blockchain operations that bring about strong decentralization, immutability, and auditability, ethical issues in AI are better managed. The paper adopts a mixed research approach of qualitative analyses and conceptual model to develop some set of blockchain-integrated AI operations. Through a literature review of related works on sexual exploitation leading to sextortion, we first identified digital technologies that enable sexual exploitation, the role of AI in mitigating sexual exploitations, ethical issues in these AI applications and blockchain concepts that address them. Then we adopted BPMN modelling to conceptually describe blockchain operations that will limit AI ethical risks. 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 for developing AI applications that address social issues.

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 AI systems such as 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 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, sexual exploitation resulting to 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".

Digital technologies such as social media, messaging and virtual reality platforms provide environment for sexual exploitation and sextortions[7,8]. This is because these technologies provides cyber-criminals the environment to groom, manipulate and coerce victims to share sensitive and sexually explicit content which they further use to extort and blackmail victims. Sextortion and online-based sexual exploitation crimes have serious emotional and mental impacts on the victims of these crimes [9]. AI systems provide tools, techniques and methods to counter sexual exploitation in online environments where they occur. AI systems can be trained with datasets of victims of sexual exploitation to identify and prevent incidences of sexual exploitation. Advanced AI techniques such as large language models (LLM) have also been used in natural language chatbots and robots to collect data on sexual exploitations and detect them early in online interactions. AI has not only played positive roles but has also enabled sexual exploitation through image manipulations resulting in blackmail and extortions of victims[10]. Still, when AI tools and systems are adopted in mitigating online sexual exploitations, there are a lot of ethical issues that arise due to the sensitive nature of data used in training AI systems. AI systems are also generally considered as blackbox to the users, hence there are issues of trustability and transparency of AI tools when deployed to mitigate sexual exploitation [11].

The integration of blockchain with AI is an opportunity for ethical AI development that emphasizes trust, transparency, and fairness. Consequently, the goal of this paper is to propose some set of blockchain-integrated AI operations to address ethical issues that arise when AI tools are used in mitigating sexual exploitation and sextortion. As there exists an ever-increasing need for the use of responsible technological solutions, the position paper shows that blockchain technologies offer some useful methods for ensuring transparency and trust in AI-driven systems. To achieve the goals of this paper, we adopt a mixed-research approach of qualitative analyses and conceptual model. The former helps to identify important ethical issues that affect AI systems related to sexual exploitation prevention, and the latter is adopted for systematic description of some useful blockchain-integrated AI operations that address AI ethical issues.

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 the research method for the research conducted in this paper. Section 3 outlines potential ethical concerns for social AI applications by reviewing related literature on digital technologies that enable sexual exploitation, the role of AI and ethical issues therein and blockchain concepts that address AI ethical issues. Section 4 proposes potential blockchain operations that when integrated into AI processes can mitigate AI ethical issues. 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 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.

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 [12]. 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 [13,14]. LLMs are a special type of natural language processor (NLP) realized from various deep learning algorithms focusing on generating human-readable content [15].

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 [16].

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 [17]. 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 [18,19].

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 [20]. 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 [21].

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 [22]. 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 [23].

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 [24]. The goal is to ensure data integrity without any reliance on a central authority as a trusted third party [25]. Thus, this way, blockchain yields the ability to provide auditability, traceability, and tamper-proof transaction histories [26]. Consequently, blockchain technologies have become indispensable in applications such as digital identity management, secure data sharing, and transparent financial transactions [26].

AI, on the other hand, has its roots in data-driven intelligence with the foci on predictive analysis, pattern recognition, and automated decision-making [27]. 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 [28]. 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 [29]. 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 [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]. 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 [32].

2.3. Research Methodology

The research design adopted for this work follows a mixed-methods approach comprising qualitative assessments and conceptual modelling. This approach has been adopted in several information system-related research works [33–35]. Qualitative analyses of the literature are conducted to identify concrete ethical issues in AI applications related to sexual exploitation and the conceptual model proposes some set of blockchain-integrated AI operations that mitigate the identified ethical issues.

For the qualitative analyses, three separate related literature analyses are conducted. First, to identify digital technologies that provide the environment for sexual exploitations leading to sextortion. A second literature review is carried out to identify the roles of AI in preventing and countering sexual exploitation on digital platforms and the potential ethical issues in automated AI systems. The third literature analyses identified some blockchain concepts and their role in mitigating the ethical issues in AI systems. The second part of this research design comprises conceptual BPMN models representing some set of blockchain-based operations integrated into AI processes. BPMN model representations are a well-established approach for conceptual modelling of software systems [36,37]. In this paper, BPMN elements are used to represent tasks and decision points in AI and blockchain processes. The goal is to realise models when implemented will result in ethically-aware AI applications that prevent sexual exploitation leading to sextortions.

Table 1. Digital technologies’ roles and impact in enabling sextortion.

Digital Technologies	Roles in Enabling Sextortion	Impact	Referenced Studies
Mobile apps, virtual reality platforms, social media.	Non-consensual taking, sharing, or threats to share personal, intimate images or videos.	Psychological and emotional, social, financial and behavioural impacts, physical harm	[7]
Social media platforms, messaging apps, online dating sites, camera and video-enabled devices, email and online communication channels	Grooming, harassment, and non-consensual sharing of intimate images, cyberstalking, romance scams, revenge porn and sextortion, coercive messages	Violence, digital harassment, image-based abuse, sexual aggression and/or coercion, and gender-/sexuality-based harassment	[38]
Social networking, online hosting services, advanced encryption techniques	Recruit victims, advertise services, store and share illicit content, protecting their communications and data from detection	Mental health risks, psychological terrorism	[9]
Social media, messaging apps, GPS tracking apps, online video-sharing platforms, cloud storage and digital media sharing	Coercion, harassment, and dissemination of sexually explicit content, coerced sexting and sextortion, cyberstalking and monitoring of victims, recording and distribution of sexual assaults, and storing and disseminating explicit content.	Sexual violence and exploitation	[39]
Internet, online platforms, mobile phones, messaging apps, and live-streaming technology	Advertise victims and connect with potential clients, communicate covertly, coordinate logistics, broadcasting of exploitative content, non-consensual explicit content	Fear, anxiety, anger, humiliation, shame, self-blame, suicidal ideation and suicide, depression, financial scam	[8]

Table 2. AI’s roles in enabling and preventing sextortion.

AI’s Roles in Enabling Sextortion	AI’s Roles in Preventing Sextortion	Ethical Issues	Referenced Studies
-	Detecting suspicious transaction patterns related to sexual exploitation.	Accuracy (false positives), bias, and privacy (data misuse)	[40]
-	Identification of sexualised content in public chatrooms.	Contextual understanding, freedom of speech, and privacy (data misuse)	[41]
-	Elimination of sexual exploitation materials.	Censorship, and bias	[42]
-	Data warehousing on sexual exploitation incidents.	Privacy (data misuse), security (data breaches), and data retention (duration).	[43]
-	Natural language Chatbots for reporting incidents of sexual exploitations.	Accessibility, trust issues, and privacy (confidentiality).	[44]
-	Image analyses for identification of sexual exploitation materials.	Accuracy, bias, and privacy (data misuse).	[45]
-	Content moderation on social media platforms.	Transparency, accountability, and bias	[46]
Deepfake images for blackmailing	-	-	[47]
Image-based sexual abuse through altered altered images and recordings.	-	-	[10]
Sexualisation of female AI agents	-	-	[48]
-	Preventing sextortion by personalised education, detecting sextortion by coercive behaviour detection, and supporting victims through gamified mental therapy.	Privacy (data usage and sensitivity), bias (limited data set), data consent, and regulation (multi-jurisdiction)	[49]

3. Digital Technologies roles in Sexual Exploitation, AI for Social Good and Ethical Concerns

This section of the paper provides related literature reviews. The first is to identify digital technologies that enable sexual exploitation. The second is to identify AI’s role in addressing sexual exploitation issues in online platforms and ethical issues that arise. The third is to identify useful blockchain concepts that can potentially limit ethical issues in AI applications. The result of the literature reviews provides the basis for the development of the conceptual model of blockchain-integrated AI operations for building applications that address social problems like sexual exploitations leading to sextortion.

3.1. Related Literature on Digital Technologies that Enables Sexual Exploitations

Digital technologies play a role in enabling sextortion by providing environments for sexual exploitation. Hence it is necessary to understand these digital technologies, the roles they play in sexual exploitation and the impacts on the victims. We examined the literature articles [7–9,38,39] in Table 1 to identify social media platforms, chatting platforms, dating websites and virtual reality platforms where sexual exploitation activities are prevalent. The platforms enable criminals to stalk, coerce, threaten, and harass victims into sharing sexually explicit images and videos. Social media platforms also provide grooming channels to lure victims into various romance scams. These explicit images are then stored on the clouds, web hosting platforms and other file hosting services to extort the victims thereby resulting in sextortion cases. Extortion of victims has several health implications such as psychological, emotional, and financial which can lead to depression, self-harm and in the worst cases result in suicide. Other implications of sexual exploitations such as sextortion include fear, humiliation and self-blame.

3.2. Related Literature on AI for Addressing Sexual Exploitation

AI plays a role both in enabling and mitigating sexual exploitations that lead to sextortion cases. Even when AI is applied to help prevent sexual exploitation through various automated algorithms, there are also ethical concerns about the use and misuse of personal data. In Table 2, we analyzed the following related articles [10,40–48] to identify the roles of AI in enabling and mitigating sexual exploitation and collect the list of ethical concerns that are raised when AI is applied to address sexual exploitation problems. The role of AI in enabling sexual exploitation mostly involves the alteration of images and video recordings where victims' faces or voices are used to replace original actors in sexually explicit content. These forms of alterations are commonly referred to as deepfakes. These digitally altered images and videos are then used to blackmail and extort victims on social media and chatting platforms, thereby resulting in sextortion. Other examples of AI usage in sexual exploitation include the sexualization of female AI agents.

According to the findings of the research in Table 2, AI can be used in many ways to limit, combat and prevent sexual exploitations on digital platforms. AI can be used in detecting suspicious transactions linked to sexual exploitations such as sextortion cases. AI can be used to identify and automatically remove sexualized content in public chatrooms and social media platforms thereby acting as content moderating agents. These automated agents perform image and text analyses to flag contents for removal. AI and natural language tools have also been applied in creating chatbots collecting incidents of sexual exploitation and reporting sextortion cases. Other uses of AI in mitigating sexual exploitations include data warehousing systems for aggregating incidents of sexual exploitation along with the criminal entities connected to them. The research [49] described extensively how blockchain can be used to mitigate sextortion cases by prevention of sexual exploitation, provision of instant aid when sexual exploitation happens and Continuous Support of victims of sextortions. 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. In providing aid, 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 behaviours - 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. In providing continuous support, individuals affected by such a case go through a recovery period that can also be supported by AI through mental therapy tools that allow self-assessment and/or direct emergency contact with social services or law enforcement.

Still, several ethical issues arise when AI acts as an automated agents for mitigating sexual exploitations. According to the results in Table 2, some ethical issues that arise include privacy issues due to data usage misuse and data sensitivity, the accuracy of detection logic due to false positives, bias due to incomplete training datasets, security and data confidential issues. Other ethical issues include transparency, trustability and accountability of AI systems. There is also the problem of accessibility of AI tools and legal issues related to regulatory jurisdiction and different interpretations of sexual exploitation.

Table 3. Ethical issues in AI addressed through blockchain concepts

Ethical issues in AI	Blockchain concept	Blockchain role in Mitigation	Referenced Studies
Accuracy (false positives)	Federated machine learning.	Like other ensemble AI systems, it can improve the performance of the models and also provide more representative datasets since data is distributed across different locations, countries and regions ensuring that systems that mitigate sexual exploitation have higher performance	[50]
Privacy (data use/misuse)	Data wallet	Permission granting and revoking to prevent unauthorised data usage thereby ensuring that victims of sexual exploitation maintains control and use of their data in training AI systems	[51]
Bias	Data auditability	Auditable datasets on the blockchain provides transparency and help in identifying biases in datasets	[52]
Contextual understanding	-	-	-
Censorship (freedom of speech)	DAO governance	Community-based governance of AI processes instead of centrally controlled ensures decisions on what constitute sexual exploitations are reached in a more democratic manner	[53]
Accessibility	Token economics	Token-based reward mechanisms can be implemented to incentivize data owners and organizations to independently run federated AI models thereby making them decentralized and more accessible instead of propriety model ownership by central entities	[54]
Trustability	Smart contracts	On-chain logic is verifiable and ethical guidelines can be encoded in smart contracts ensuring that the basis for identifying sexual exploitations are verifiable and transparent	[55]
Accountability	-	-	-
Security (confidentiality)	Zero-knowledge proof systems	Privacy-aware data processing systems such as homomorphic encryption can be adopted in processing confidential data such even there is data breaches, information and data of victims of sexual exploitations remain hidden	[56]
Regulation (legal jurisdictions)	Federated machine learning	Data are processed at the point where they are generated adhering to local regulations this ensures that different legal jurisdictions and regulations regarding the processing of sensitive data are adhered to specific to locations where the decentralized AI models run.	[57]

3.3. Ethical Issues from AI Applications and Blockchain roles in their Mitigation

As shown in Table 3, ethical issues in AI applications that mitigate sexual exploitation leading to sextortion can be addressed with the integration of blockchain concepts. Blockchain technologies and concepts such as federated machine learning, data wallets, transaction auditability, DAO governance, Zero-knowledge proofs, and smart contracts can be adopted to address some of the identified ethical issues. The performance and *accuracy* of AI systems for detecting sexual exploitation can be improved with the use of federated machine learning techniques such that machine learning models consist of several ensemble members running in different locations of data sources[50]. Privacy issues due to potential *misuse* of data of victims of sexual exploitation can be reduced with the use of data wallet concepts where victims maintain control and ownership of their data[51]. *Bias* issues in AI systems can be reduced with data auditability which the blockchain provides, thereby ensuring easy detection of biases in AI training datasets[52]. *Censorship*-resistant AI system that ensures freedom of speech even when identifying and flagging sexual exploitation incidences can be implemented with the integration of blockchain DAOs for democratized governance of AI processes[53]. Token economics can be used to improve the accessibility of AI tools preventing sexual exploitation, by modelling reward mechanism for both data owners (such as victims of sexual exploitation) and organizations that run decentralized/federated AI models that combat sexual exploitation. This ensures that AI models developed from such setup is decentralized and more accessible instead of propriety models owned by centralized entities [54]. The trustability of AI systems can be improved with the use of smart contracts for encoding the logic of identifying sexual exploitation incidences, making them transparent and easily verifiable[55]. Zero-knowledge-proof systems can be adopted for implementing privacy-aware AI models ensuring the confidentiality of victims' data when used to train AI systems [56]. Lastly, federated machine learning can also be adapted to address regulation issues when different rules apply to different legal jurisdictions regarding the interpretation of sexual exploitations and the processing of sensitive data. Decentralized learning models can be trained locally where the data are produced, thereby, satisfying the local regulations that apply[57].

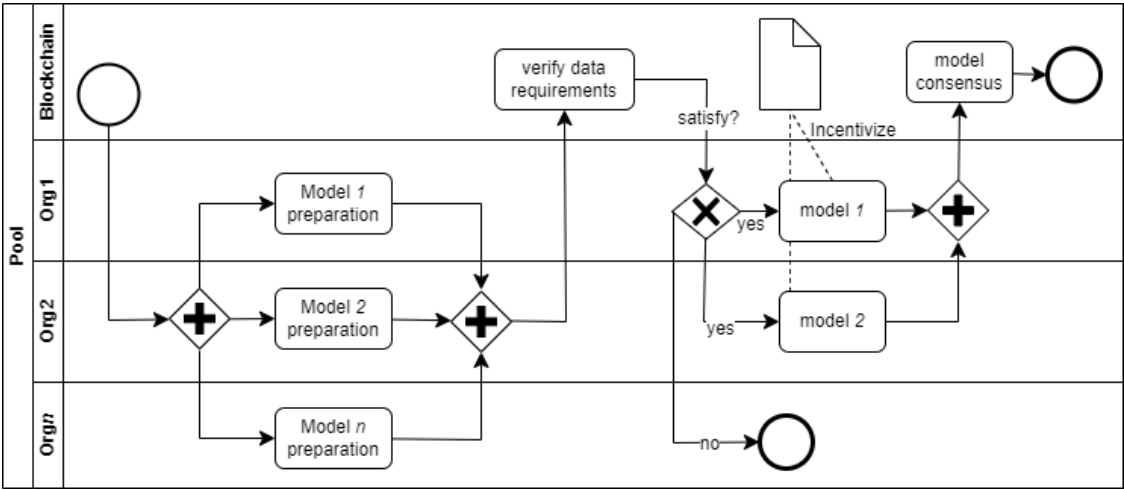


Figure 1. Decentralized machine learning.

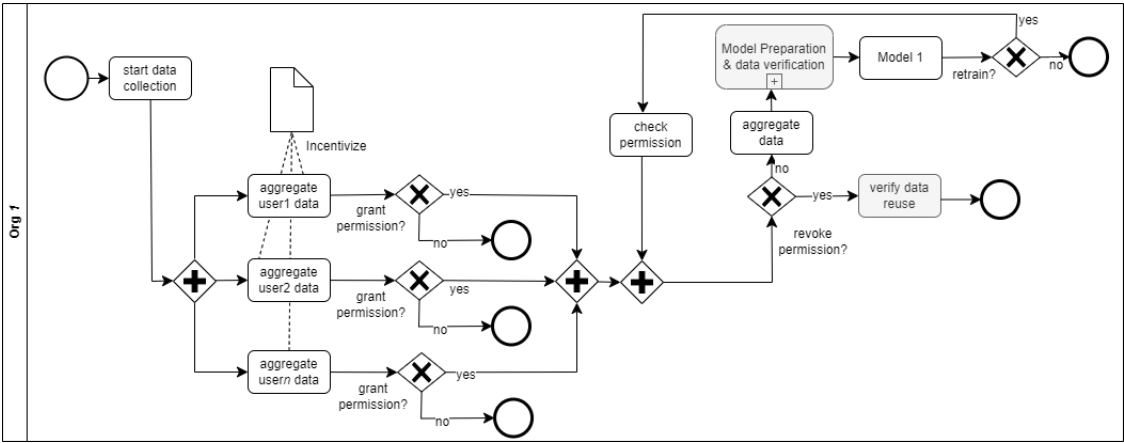


Figure 2. Incentivized user data wallet.

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

In tackling the significant ethical and trust challenges present in AI systems used in preventing sexual exploitation, 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 set of blockchain operations that can be integrated into AI systems to mitigate ethical risks such as -model accuracy, data misuse, bias, trustability and confidentiality of sensitive datasets. 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.

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 1 adapted from [58,59] shows a simplified process representation of federated AI systems (a form of ensemble modelling) 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 2, adapted from [51], 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.

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 1 and 2 - 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 1 and 2, 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.

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 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. As blockchain technologies are instrumental in ensuring integrity and immutable traceability, the authors in [60] discuss the beneficial effects of 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) [61].

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 [62], 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 [63], 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 [64] discuss, the specific attributes of the blockchain of decentralization, immutability, and transparency strengthen the trust of users. Furthermore, as discussed in [62], 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 [65], 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.

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. In [66], the integration of blockchain and AI significantly improves security and privacy, which is important for the protection of victims of sextortion. Furthermore, in [67], 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 proposals made in 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 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 [68], 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 [69] 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 [70], 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. Also 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 [71] 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 [72], 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 [73], 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 [74] 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 [75]. Enabling decentralized AI training with federated learning further strengthens privacy protection, which aligns with GDPR principles of data localization and minimization [76]. 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 [77]. In sensitive applications such as identifying sextortion threats, this is particularly valuable since fairness and reliability are paramount [78].

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 [79], 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 trustworthiness, fairness and justice when AI aims to detect and analyze abuse occurrences [80]. In [81], 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 [82], 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 [83], the authors show that blockchains improve transparency in sensitive data environments due to established immutability and auditability. The discussion in [84] 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 [85] point out that AI operations can be reliably scrutinized when all modifications are mutably logged on a blockchain. Also in [86], 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 [87], the authors explain that blockchains have the potential to improve stakeholder participation in AI governance and positively affect fairness and transparency. In [88], 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.

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 socioeconomic factors (such as economic uncertainty, gender issues, and patriarchal societies), as specified in [89,90]. However, it may also lead to micro and macroeconomic effects. For example, it can cause economic vulnerability and instability in victims [89], increase social inequality, and perpetuate stigma and ostracizing of already marginalized individuals [91].

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 [92], while addressing data ownership and privacy concerns [93]. This distributed model also ensures that data are less susceptible to misuse, another essential element for victims of sextortion [94]. 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 [95]. 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 [96].

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 [97], 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 [98]. 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 [99] 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[99].

Fourth, in addition to this BIAI-supported recognition of victims, AI-supported educational and awareness programs, with or without blockchain-enhanced digital micro-credentials [100], 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 [101]: *Transparent legal processes* - BIAI may guarantee that legal decisions are transparent and auditable, which will help combat corruption [102]. In turn, corruption, through bribery and the influence of perpetrators, has been proven to affect effective prosecution of sextortion cases, for example, in South Africa with migrants [91]. *Tamper-proof evidence* - Blockchain can ensure the integrity of the chain of custody [103], while AI can be employed in the analysis and management of evidence and digital forensics [104]. *Support for marginalized groups* - One of the groups most affected by sextortion is represented by migrants and refugees [91], 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 [105].

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 [106]. Blockchain has been proven to improve social welfare programs and promote equitable resource distribution by ensuring that funds are not smuggled into intermediaries [107].

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 [108], and, on the other hand, the transformative role of AI and blockchain for significant parts of society [109]. This dual perspective leads us to reassert the need for an integrated approach to ensure the proper and ethical use of BIAI.

5.5. Legal Implications of Blockchain-integrated AI System

Blockchain-integrated AI such as a decentralized federated machine learning system, addresses some of the regulatory compliance issues in AI applications by ensuring data privacy and protection,

data localization, and regulatory flexibility. By processing data in the locations where they are generated, organizations that own the data can adhere to their localized regulatory requirements. This is because, in federated machine learning, raw data do not necessarily need to be transferred across different legal jurisdictions before being progressed by AI algorithms. The decentralization of federated ML provides flexibility that enables participating organizations to individually comply with continuously evolving regulations within their jurisdictions. Furthermore, blockchain-enabled data wallets as shown in Section 4 ensure data sovereignty and control for the individuals who produce the data processed by AI systems. Users being able to control the usage of their data through mechanisms for consenting and withdrawing consents in blockchain-enabled wallets adhere to the core principles of GDPR requirements.

Blockchain technology and AI applications are regulated in different jurisdictions and must comply with various laws, such as data regulation, healthcare laws, and consumer protection statutes, to ensure legal operation. In the realm of combating sextortion, the deployment of AI applications presents a significant legal challenge, primarily regarding compliance with data privacy laws. These applications involve the generation, storage, and analysis of large amounts of personal data, including sensitive information such as images and communication records.

The compatibility of blockchain technologies with GDPR poses additional challenges, especially due to their decentralized nature and the GDPR regulatory framework. One major problem is how to identify data controllers. According to Article 4(7) GDPR, a controller is defined as a natural or legal person who determines the purposes and means of processing personal data. In a decentralised federated machine learning context where data is distributed across many nodes within different organizations, it becomes difficult to determine who can be considered as a data controller. For instance, in the *Wirtschaftsakademie Schleswig-Holstein* case (Case C-210/16 *Wirtschaftsakademie Schleswig-Holstein* [2018] EU:C:2017:796, para 16.), it was found that there is a low threshold for joint controllership; thus implying that numerous participants in a blockchain network may potentially qualify as controllers thereby complicating compliance efforts [110].

Furthermore, given the differences in data privacy laws between jurisdictions, it is crucial to analyze the potential of using blockchain in data privacy concerns in conjunction with the data protection issues caused by AI. For example, in the European Union (EU), the GDPR is the most important law protecting privacy rights [111]. At the opposite end of the spectrum, the United States (US) took a more sectoral approach, by proposing regulations for each type of the following: healthcare, finance, children's privacy rights, and education. Nonetheless, there are signs of regulatory convergence, as California adopted the Privacy Rights Act (CPRA), which incorporates many elements from the GDPR of the EU, including its treatment of automated decision-making [112].

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.

Implementing blockchain-integrated AI systems requires a robust technical infrastructure capable of supporting the demands of both technologies. The question of choosing between public or private networks arises for the implementation of the models developed in this paper. Although public blockchains are fully decentralized and transparent, they also have performance issues in that they have scalability and latency issues [113]. Smart contracts crucial for implementing automated processes,

especially for detecting sextortion cases. Solidity which the common programming language for smart contracts has security vulnerabilities [114]. Hence, the smart contracts used in implemented blockchain-integrated AI solutions have to be thoroughly audited to eliminate security loopholes.

Effective governance frameworks are essential for the management of blockchain-integrated AI systems that tackle sexual exploitation issues. Such governance systems also need to be aligned with societal values and regulatory standards. Blockchain-based governance is inherently decentralised in the decision-making processes that stakeholders can participate in. Such stakeholders include policy-makers who make laws about sexual exploitation incidences, developers who build AI and blockchain systems, and regulators who interpret these laws have to collaboratively work together to form a governance network managing AI applications for social good. This type of Collaborative governance can be facilitated by encoded rules that are represented by smart contracts in implementations such as decentralized autonomous organizations (DAOs) or similar models [115].

6. Conclusions

In this paper, we explore the potential of blockchain-integrated AI systems to transform socio-technical application cases such as in the prevention of sexual exploitations leading to sextortion. Thus, we investigate to what extent decentralized immutable traceability strengthens AI systems by addressing the ethical issues inherent in them. By conducting three stages of literature reviews, we identified the roles digital technologies play in enabling sexual exploitations and their implications. Then we analysed the roles AI play in mitigating sexual exploitation in digital technologies and identified some potential ethical issues. Lastly in the literature review, we identified some blockchain concepts and their roles in addressing some of the AI ethical issues. The ethical issues in AI applications include - prediction accuracy, data misuse, bias, contextual understanding, censorship, accessibility, trustability, accountability, data confidentiality and regulatory jurisdictions. Some relevant blockchain concepts that address ethical issues in AI include federated machine learning, user-controlled data wallet, on-chain transaction auditability, DAO governance, smart contracts, token economics and zero-knowledge proof systems. Following these initial results, we proposed some set of blockchain-integrated AI operations represented as BPMN models for implementing ethically-aware software systems that address social problems like sextortion. The first conceptual model proposed model is a decentralized machine-learning process comprising smart contract for verifying data requirements, distributed consensus, and an incentivisation system for organizations running the AI models. The second conceptual model proposed is a user-incentivized data wallet process comprising of access control and permission revocation system when processing personal data and a token economic system for rewarding data owners and ensuring wider accessibility of the AI system.

This work is limited by the lack of proper evaluation of the blockchain-integrated AI models proposed in this paper. Hence, the future work resulting from the research will explore the proof of concept (PoC) implementation of the federated machine learning and user-incentivized data wallet models proposed in this paper. The proposed evaluation will also show concrete examples of mitigated digital threats and positive societal impacts derived from the implementation of the conceptual models. The results of the evaluation will demonstrate the stronger societal resilience derived from the implementation of BIAI especially when used to address social issues like sexual exploitation and sextortion cases.

Author Contributions: Conceptualization, A.N. and C.U.; methodology, A.N, C.U, R.V; data curation, A.O.; writing—original draft preparation, A.N, C.U, R.V, A.O, N.S, S.C; writing—review and editing, A.N, C.U, R.V, 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. Sheikh, M.M.R.; Rogers, M.M. Technology-facilitated sexual violence and abuse in low and middle-income countries: A scoping review. *Trauma, Violence, & Abuse* **2024**, 25, 1614–1629.
8. Ray, A.; Henry, N. Sextortion: A Scoping Review. *Trauma, Violence, & Abuse* **2025**, 26, 138–155.
9. Paat, Y.F.; Markham, C. Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health* **2021**, 19, 18–40.
10. Okolie, C. Artificial intelligence-altered videos (deepfakes), image-based sexual abuse, and data privacy concerns. *Journal of International Women’s Studies* **2023**, 25, 11.
11. Von Eschenbach, W.J. Transparency and the black box problem: Why we do not trust AI. *Philosophy & Technology* **2021**, 34, 1607–1622.
12. 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.
13. 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**.
14. Gifu, D.; Silviu-Vasile, C. Artificial Intelligence vs. Human: Decoding Text Authenticity with Transformers. *Future Internet* **2025**, 17, 38.

15. 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.
16. 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.
17. 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.
18. 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**.
19. 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.
20. Swan, M. *Blockchain: Blueprint for a new economy*; "O'Reilly Media, Inc.", 2015.
21. 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.
22. Cuccuru, P. Beyond bitcoin: an early overview on smart contracts. *International Journal of Law and Information Technology* **2017**, 25, 179–195.
23. 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.
24. 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>.
25. 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>.
26. 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>.
27. 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>.
28. 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>.
29. 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>.
30. Marevac, E.; Patković, S.; Žunić, E. Decision-making AI for customer worthiness and viability. *2023 22nd International Symposium INFOTEH-IAHORINA (INFOTEH)* **2023**, pp. 1–6. <https://doi.org/10.1109/INFOTEH57020.2023.10094207>.
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. 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>.
33. Heeager, L.T.; Nielsen, P.A. A conceptual model of agile software development in a safety-critical context: A systematic literature review. *Information and Software Technology* **2018**, 103, 22–39.
34. Abdel-Aty, T.A.; Negri, E. Conceptualizing the digital thread for smart manufacturing: A systematic literature review. *Journal of Intelligent Manufacturing* **2024**, 35, 3629–3653.
35. Naeem, M.; Ozuem, W.; Howell, K.; Ranfagni, S. A step-by-step process of thematic analysis to develop a conceptual model in qualitative research. *International journal of qualitative methods* **2023**, 22, 16094069231205789.
36. Karagöz, N.A.; Demirörs, O. Conceptual modeling notations and techniques. In *Conceptual modeling for discrete-event simulation*; CRC Press, 2010; pp. 195–226.
37. Recker, J.; Indulska, M.; Green, P.; et al. How good is BPMN really? Insights from theory and practice **2006**.

38. Makinde, O.A.; Olamijuwon, E.; Ichegbo, N.K.; Onyemelukwe, C.; Ilesanmi, M.G. The nature of technology-facilitated violence and abuse among young adults in sub-Saharan Africa. *The Emerald international handbook of technology-facilitated violence and abuse* **2021**, pp. 83–101.
39. Lyttle Storrod, M. "It Started With a Nude": Gangs & Technology-Facilitated Sexual Violence. *International Criminal Justice Review* **2024**, *34*, 245–261.
40. Saputra, D.H.; Prakarsa, A. Enhancing Detection Mechanisms: Law Enforcement Strategies Identifying Suspected Financial Transactions of Child Sexual Exploitation Crimes. In Proceedings of the ACOSEC: ASEAN Conference on Sexual Exploitation of Children. Atlantis Press, 2024, pp. 120–126.
41. 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.
42. Ali, M.I. Strategies for Intervention and Prevention in Online Child Sexual Exploitation. *Teisé* **2024**, *132*, 145–155.
43. Stockhem, O. Improving the international regulation of cybersextrafficking of women and children through the use of data science and artificial intelligence. PhD thesis, 2020.
44. Rita, M.N.; Shava, F.B. Chatbot driven web-based platform for online safety and sexual exploitation awareness and reporting in Namibia. In Proceedings of the 2021 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD). IEEE, 2021, pp. 1–5.
45. Phippen, A.; Bond, E. Image recognition in child sexual exploitation material—Capabilities, ethics and rights. *Policing in the Era of AI and Smart Societies* **2020**, pp. 179–198.
46. Alsoubai, A.; Song, J.; Razi, A.; Naher, N.; De Choudhury, M.; Wisniewski, P.J. From 'Friends with Benefits' to 'Sextortion': A nuanced investigation of adolescents' online sexual risk experiences. *Proceedings of the ACM on human-computer interaction* **2022**, *6*, 1–32.
47. Blancaflor, E.; Garcia, J.I.; Magno, F.D.; Vilar, M.J. Deepfake Blackmailing on the Rise: The Burgeoning Posterity of Revenge Pornography in the Philippines. In Proceedings of the Proceedings of the 2024 9th International Conference on Intelligent Information Technology, 2024, pp. 295–301.
48. Borau, S. Deception, discrimination, and objectification: Ethical issues of female AI agents. *Journal of Business Ethics* **2024**, pp. 1–19.
49. 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**.
50. Lee, G.H.; Shin, S.Y. Federated learning on clinical benchmark data: performance assessment. *Journal of medical Internet research* **2020**, *22*, e20891.
51. 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.
52. 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). IEEE, 2023, pp. 1–6.
53. Chaffer, T.J.; Charles von Goins, I.; Cotlage, D.; Okusanya, B.; Goldston, J. Decentralized Governance of AI Agents **2024**.
54. Himmelsbach, T.; Mou, Y.; Decker, S.; Heinzl, A. Towards Federated Machine Learning and Distributed Ledger Technology-based Data Monetization. In Proceedings of the VLDB Workshops, 2023.
55. Nassar, M.; Salah, K.; Ur Rehman, M.H.; Svetinovic, D. Blockchain for explainable and trustworthy artificial intelligence. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* **2020**, *10*, e1340.
56. Singh, N.; Dayama, P.; Pandit, V. Zero knowledge proofs towards verifiable decentralized ai pipelines. In Proceedings of the International Conference on Financial Cryptography and Data Security. Springer, 2022, pp. 248–275.
57. Balta, D.; Sellami, M.; Kuhn, P.; Schöpp, U.; Buchinger, M.; Baracaldo, N.; Anwar, A.; Ludwig, H.; Sinn, M.; Purcell, M.; et al. Accountable federated machine learning in government: engineering and management insights. In Proceedings of the Electronic Participation: 13th IFIP WG 8.5 International Conference, ePart 2021, Granada, Spain, September 7–9, 2021, Proceedings 13. Springer, 2021, pp. 125–138.
58. 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.

59. 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.
60. Angraal, S.; Krumholz, H.; Schulz, W. Blockchain Technology: Applications in Health Care. *Circulation: Cardiovascular Quality and Outcomes* **2017**, *10*, e003800.
61. 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.
62. 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.
63. 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.
64. 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**.
65. 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>.
66. Bodemer, O. The Unseen Guardian: How Blockchain, Java, and AI Stealthily Became the Sherlock Holmes of Cybersecurity. *Authorea Preprints* **2023**.
67. 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>.
68. 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>.
69. 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>.
70. 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>.
71. Michaelson, P. Arbitrating Disputes Involving Blockchains, Smart Contracts, and Smart Legal Contracts. *Cybersecurity* **2020**. <https://doi.org/10.2139/ssrn.3720876>.
72. 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>.
73. 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>.
74. 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>.
75. 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>.
76. 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>.
77. 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>.
78. 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>.

79. 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>.
80. Kafali, E.; Preuveneers, D.; Semertzidis, T.; Daras, P. Defending Against AI Threats with a User-Centric Trustworthiness Assessment Framework. *Big Data and Cognitive Computing* **2024**, *8*, 142.
81. 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>.
82. 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>.
83. 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>.
84. 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>.
85. 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>.
86. 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>.
87. 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>.
88. 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>.
89. 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>.
90. Fawole, O. Economic Violence To Women and Girls. *Trauma, Violence, & Abuse* **2008**, *9*, 167 – 177. <https://doi.org/10.1177/1524838008319255>.
91. 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>.
92. 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>.
93. 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.
94. 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>.
95. Zuboff, S. The age of surveillance capitalism. In *Social theory re-wired*; Routledge, 2023; pp. 203–213.
96. 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>.
97. 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>.
98. 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>.
99. 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>.
100. PARASCHIVEANU, V.; RICHARDSON, G.; VOICU-DOROBANȚU, R. EDUCATION 3.0: BLOCKCHAIN-BACKED MOOCS. *eLearning & Software for Education* **2020**, *3*.

101. 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>.
102. 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.
103. 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>.
104. 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>.
105. Bazarhanova, A.; Magnusson, J.; Lindman, J.; Chou, E.; Nilsson, A. Blockchain-based electronic identification: cross-country comparison of six design choices **2019**.
106. 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>.
107. Myeong, S.; Jung, Y. Administrative Reforms in the Fourth Industrial Revolution: The Case of Blockchain Use. *Sustainability* **2019**. <https://doi.org/10.3390/SU11143971>.
108. Marinakis, V.; Koutsellis, T.; Nikas, A.; Doukas, H. AI and Data Democratisation for Intelligent Energy Management. *Energies* **2021**. <https://doi.org/10.3390/EN14144341>.
109. 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>.
110. Li, Z. Confronting algorithm bias risks: Will blockchain provide new opportunities or challenges for data protection law? *Dublin L. & Pol. Rev.* **2021**, *2*, 43.
111. Chaturvedi, A. Defining Legal Responsibility in the Age of AI: Addressing Gaps in Data Privacy Regulation. *Indian J. Integrated Rsch. L.* **2023**, *3*, 1.
112. Murthy, M.S. Data protection law and policy in the USA: An overview. *Issue 3 Indian JL & Legal Rsch.* **2022**, *4*, 1.
113. 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>.
114. 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>.
115. Han, J.; Lee, J.; Li, T. DAO Governance. *SSRN Electronic Journal* **2023**. <https://doi.org/10.2139/ssrn.4346581>.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.