Volume 4·Issue 2·October 2022
ISSN 2661-3220(Online)

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Artificial Intelligence Advances

BILINGUAL
PUBLISHING CO.
Pioneer of Global Academics Since 1984

Volume 4 Issue 2 • October 2022 • ISSN 2661-3220 (Online)

Artificial Intelligence Advances

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Volume 4 | Issue 2 | October 2022 | Page1-21
Artificial Intelligence Advances

Contents

Articles

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Artificial Intelligence Advances
https://ojs.bilpublishing.com/index.php/aia

ARTICLE

The Question of "Mindsets" and AI: Cultural Origins and Limits of the current AI Ethical AIs and Cultural Pluralism

Badrudin Amershi*

Cpo-Im, Bertolt Brecht St. 103, 49088, Osnabrück, Germany

ARTICLE INFO

Article history
Received: 11 October 2022
Revised: 24 November 2022
Accepted: 9 December 2022
Published Online: 4 January 2023

Keywords:
Western mindset
Enlightenment
Duality
Knowledge
Reason and rationality
Computation
Ethical machines
Cultural diversity

ABSTRACT

The current process of scientific and technological development is the outcome of the epochal Cultural Revolution in the West: i.e. The emergence of the Age of Enlightenment and its pursuit of "rationality". Today, "rationality" combined with "logic" has mutated into a "strong belief" in the power of rationality and "computational processes" as a 'safer' and the only way to acquire knowledge. This is the main driving force behind the emergence of AI. The core of this mindset is the fundamental duality of the observer and the observed. After the imperial expansion of Western Europe–in alliance with religion, its previous foe ("Christianity")–this worldview became the globally dominant mindset. The paper explores the dominant narrative of rationality and reason in Western science, and seeks an alternative world of cultural diversity.

1. Introduction

This paper is a result of internal discussions subsequent to an innovative debate & discussion at Chatham House, London UK in Feb 2022 titled: **The application and misapplication of artificial intelligence today.** It concerned the deployment of AI in the social, political, and economic contexts and the subsequent problems. It is a historical and philosophical paper. The objective is to trace the origin and development of the methodology of natural sciences and philosophical reflections using the concept of "rationality". This was in the wake of the enlightenment revolution in science and philosophy in Europe in the 15th century. This ushered in a novel and innovative way of assessing the external nature as well as the role of the individual in the process. This historical development de-

*Corresponding Author:
Badrudin Amershi,
Cpo-Im, Bertolt Brecht St. 103, 49088, Osnabrück, Germany;
Email: ame_rshi@hotmail.com

DOI: https://doi.org/10.30564/aia.v4i2.5156

picts the emergence of **a new mindset in Europe**, which then advanced over the whole globe in the wake of geographical expansion, discoveries, and conquest of "new" continents. Consequently, this led to the transplantation of this new European mindset over the globe.

This sets the backdrop for the later emergence of AI–and the problems connected to its application in various human fields.

2. Mindsets, Their Socio-cultural Origins and Their Limits

The concept of human mindset refers to the totality of beliefs, values, ethical concepts, social behaviours, etc. of a human group that have evolved over time–and which guides and regulates the group's behaviour in relation to other groups and external nature. (It constitutes the social group's identity and defines it in relation to other groups–and to the external world.)

Over the span of human evolution, different human civilisations in different geographical locations have emerged, with distinct ways of dealing with internal members and defining their relation to their natural habitat. The Egyptian, Mesopotamian, Indian, Mesoamerican, Chinese, Greek, and Roman civilizations–to name a few salient ones–all had or have their distinct ways of dealing with internal group members, external groups, and with nature. In consequence, several distinct mindsets have left their footprints over the span of history.

At the core of the current paper is the assessment of the so-called western European mindset, which emerged–in relation to the other mentioned civilizations–relatively late in human history, but owing to specific historical circumstances, has been able to expand and spread over the world constituting at present the dominant min-set. It distinguishes itself through a novel approach to dealing with external nature and with other individuals in the social sphere.

This was in the wake of the enlightenment revolution in science and philosophy in Europe in the 15th century. This ushered in a novel and innovative way of assessing the external nature as well as the role of the individual in the process. This historical development depicts the emergence of **a new mindset in Europe**, which then advanced over the whole globe in the wake of geographical expansion, discoveries, and conquest of "new" continents. Consequently, this led to the transplantation of this new European mindset over the globe.

This mindset developed specific concepts (e.g. "rationality" or reason) to grasp and assess external nature. Its success in this domain propelled it further–representing a great leap in the realm of natural science.

At the core of this mindset is the belief that the *observer* ('mind'; the 'reasoning mind') and the *observed* ('external world') are separate entities: The former can completely access the latter. Kant himself, the main proponent of this view, in his later work ("Critique of Pure Reason") retracted and pointed out the dilemma of the "thing in itself" ("Ding a Sich") *which remains "inaccessible" to the 'reasoning mind'*. For Kant "human cognition and experience seemed to be filtering and distorting what we know" [1]. The "observer" (subject) and the "observed" (object) represented two separate (metaphysical) entities. In this process, the "observer" assumed the critical role. Rationality combined with measurement of "the observed" constituted the fundament to deliver 'untainted' knowledge of the observed phenomena to the observer. For the western mindset, the observer-centric perspective plays a key role in the acquisition of knowledge.

However, this never developed into a major problem, since adherence to the belief that the observer and the observed are two independent entities was seen as the source of the new scientific discoveries and technologies. Although, this created a "cultural defence wall" around this mindset–shielding it from "irrational" beliefs and "alien" influences, the rise of natural sciences began to create doubts about the fundamental duality.

With rapid advances in the natural sciences e.g. the emergence of the theories of quantum mechanics and relativity, science was forced to re-evaluate the central role of the observer. This led to the dethroning of the singular observer, along with the separation of the observer from the observed. In quantum mechanics, the observer (subject) and the observed (external world)–instead of being two independent entities–are enmeshed in an intricate framework of mutual dynamic interaction. This became more evident in the so-called 'observer effect' Measurement, say of a particle, which ended up affecting it as well: The very act of observation was affecting the observed entity. The observer and the observed represented an interconnected system. Similarly, in the theory of relativity, the notion of a singular frame of reference was abandoned together with the "absolute observer": Observers in different frames of reference obtained different results. These observations required corrections by a system of coordinate transformations [2]. For the leading scientists of the time, this opened an opportunity to search for alternative knowledge foundations and worldviews. Some turned to the Eastern (Asian) knowledge systems and mindsets (prominently Eric Schrödinger E, Werner Heisenberg, Robert Oppenheimer) which seemed to provide a broader field to reconcile these new observations and discoveries [3,4].

These findings represented a fundamental shift in the

prevalent mindset: *The cognition process, based on the constructed duality of the observed and the observer was not able to deliver untainted knowledge.* The act of observation itself interfered with the observed phenomena. This in a way challenged the fundamental duality of the Cartesian world, a constituent element of the western mindset. 'Descartes, in the seventeenth century, divided all nature into two parts, a realm of thoughts and a realm of material things, and proposed that the motions of material things were completely unaffected by thoughts' [5].

This prompted the scientists at the helm of these discoveries to reflect on the whole process of acquiring knowledge. More and more thinkers began to question whether human perception, ordered by reason, was the correct framework for assessing reality. In the wake of these discoveries, the first serious cracks appeared in the wall of duality. The emergence of artificial intelligence provides a new twist to this duality.

3. Emergence of AI–a Watershed?

In this context, the appearance of AI marks a watershed. Artificial Intelligence as the object of investigation introduces a curious twist: i.e. The subject is now observing and investigating itself as an "object" embedded in the natural environment. This represents essentially a historical role reversal! The absolute duality of the subject (thinker) and the object (external world) began to be diluted. However, instead of taking the opportunity for self-reflection, i.e., observation of the subject itself and reflecting on its deeper meaning (consciousness, self-reflection)–this was reduced to investigation mainly of one attribute of the subject–i.e. "intelligence" discarding all others. The quest then started to "measure" this intelligence. The artifact itself has now become the means to study the "subject" as an "object": To produce calculable and measurable knowledge about "human intelligence". In this context, AI developed essentially as a human artifact–which could augment and even extend the limits of human cognition. It could be deployed to assess and order a vast amount of information about the natural and social worlds. Information, however, is not "self-explanatory". To be "meaningful" it requires the backdrop of culture and history. This was mainly the domain of humans to assess order and shape information, which led to actions [1].

Its deployment especially in the natural domain has often produced astounding and beneficial results. With the ability of learning and self-learning, it seems to be able to discover new relationships and patterns among the elements of the natural world, which the human brain with its inherent limitations does not recognize. An example is an AI-based discovery of new drugs (e.g. Halicin–an antibiotic drug), or other solutions in the socio-medical field. *Problems, however, emerge when deployed in the social domain.*

3.1 Deploying AI in the Socio-political Domain: Problems and Limits

With the advancement in AI technology and its inevitable deployment in the socio-political sphere, fundamental questions and doubts have emerged. The task of assessing an enormous amount of raw information and data to arrive at decisions affecting the socio-political sphere was delegated to AI: Because of its technical capability (e.g., speed) to assess and order an enormous amount of data and information in the shortest possible time. *However, this information from the social domain is inherently biased*. Deployment was bound to affect the very social fabric, which had produced this technology in the first place. Humans had no means to assess the value and impact of these automated decisions, judgments and recommendations–about the core areas of their life and survival. The artefact was propelling human societies to a form of subjugation under its technical umbrella.

In contrast to the "domain of natural objects", the socio-political domain consists mainly of symbols, signs, 'and meanings' as well as ethical and moral rules. Symbols and signs have "meanings" assigned to them by social groups. The meaning of a word or symbol lies in its use by a social group. 'Meanings' are not ephemeral entities but depict what use particular groups make of these concepts. They are subject to changes over time – and reflect the social history of the group [6,8]. The human socio-cultural domain represents an intricately woven fabric–and its basic stuff is 'information', which is intrinsically biased–since it incorporates existing prejudices and social biases.

The application of a techno-centric oriented AI in this domain is confronted by several challenges–among others, i) its dependence on a pool of biased information, ii) blindness towards cultural diversity, iii) ethics and morals as guidelines and not "mechanistic rules", iv) the technocratic requirement for measurability.

3.2 Cultural Plurality (Diversity) and AI

An important blind spot of the western mindset is the acknowledgment of cultural plurality. Information is dependent on its context and its origins: "To be useful–or at least meaningful–it must be understood through the lenses of culture and history" [1]. Cultures manifest themselves at different levels and recognizable differences emerge. At the 'individual' level, in the West behaviour appears

to be guided and judged primarily by the performance of individual members ("self-orientation"). This includes the achievement of self-set goals. In Eastern cultures, individual behaviour seems to be guided by vague attempts at maintaining "harmony" with others in this social field and adherence to the principle of "non-disturbance". It is "other-oriented" in contrast to *"self-orientation"*. A concrete statement on a specific individual behaviour outcome may not be possible. Behaviour outcomes could assume e.g. several values at different times [7]. Deploying AI to assess and arrive at global solutions to socio-political and geo-political problems in diverse cultural domains is destined to produce slanted and even dangerous results. AI –developed and programmed as an artefact within the mindset of the west–may not be able to spot and identify culturally diverse worldviews and social behaviours and expectations.

Up to now, the whole discussion of ethical machines or artificial moral agents appears to eschew some fundamental questions of taking adequate account of the fundamental difference between human ethics, moral judgments, and rule-driven behaviour. Ethical and moral rules, as essential elements of this domain, guide social action and interaction. However, it would be fatal to consider ethical and moral action as simply "rule-driven"–like a machine or mechanical device. Moral and ethical action involves a strong element of self-reflection and "wisdom". "An algorithm knows only its instructions and objectives, not morale or doubt" [1].

3.3 Can We Conceive Such Machines as "Moral Agents"?

The appeal of AI in this domain rests on the assumption that "it offers an objective way of overcoming human subjectivity, bias, and prejudice" [7]. However, in actual practice, the algorithms appear to actually replicate and even magnify the inherent social biases (op. cit).

Particularly rising doubts confront attempts to deploy a human artefact (AI) to process biased information about the social domain. Letting "human artefacts-(AI)" utilize such biased information corrupts the central principle of knowledge acquisition: knowledge should be untainted by "social ideologies". Under these premises to arrive at "socio-political solutions" to social problems–bar any social and ethical correctives–does not bode well for human progress. This inevitably raises questions about ethics accountability and security: *For whom, why and to what purpose.* As Gill has often cautioned, "the accelerated integration of powerful artificial intelligence systems into core social institutions and systems, pose social challenges of governance, ethics, sustainability, intrinsic bias, accountability and security" [9].

We are thus back to the core problem of intrinsic bias in the information database of the social domain. Extending the application of "ethical machines" in different cultural contexts, as we have seen, is an overwhelming challenge. This poses a tough question for the construction of "universal ethical machines"–deployable with full force over the global cultural matrix.

3.4 The Question of Wisdom: Solomon's Judgement① – an "Algorithm"?

In the ethical sphere, incumbents do not blindly follow rigid rules like "natural objects" or robots. There is always a possibility of "halting or hesitation"–for self-reflection or doubt–in the execution of moral or ethical action. This goes beyond the simple matrix of wrong or right and involves elements of wisdom, self-reflection, intuition, tacit knowledge, and self-doubt. This is the backdrop for the famous judgment of King Solomon. All human narratives in this context have such historical elements woven into ethical or moral actions, which provide guidelines in specific situations. It depends upon the actors themselves, if or how they use these guidelines.

Moral rules do not drive human action like a mechanical device but provide for safety measures, doubt, and self-reflection. Therefore, the deployment of AI in the social sphere and applying the paradigm of rule-driven behaviour leads us into a cul-de-sac. The question in this context appears to be the choice between wisdom and algorithm.

3.4.1 Can 'Wisdom' be Translated into an Algorithm?

The ethical domain of the west is explicitly rule-bound and behaviour is judged by these rules. In other cultures, this may not be the case; ethical values gain their force by reference to abstract and vague principles of "good behaviour". For example, in Asia, this is underscored by vague references to historical philosophical texts and guidelines or narratives of good and evil (like texts on Confucianism or the ancient epics of Ramayana and Mahabharata, the tales of King Vikramaditya, etc.) This gives the "judge" leeway and forces conscious deliberation on his/her part.

Deploying current AI to solve–for example administrative, judicial, social or governmental problems in the non-western world–may produce solutions at odds with the values and morals valid in this diverse world. For the simple reason that it will be programmed with *algorithms applied and developed in the western cultural context and*

① To determine the true parentage of the child, King Solomon suggested dividing the body of the child into two parts.

history with its specific and binding rules and history.

However, it should be cautioned that today in many non-western cultures the utility of using AI in jurisdiction and governance *overrides concerns about the basic biases in the programmes used*. The use of AI in the areas of jurisdiction and governance today is widespread in Japan, China and other advanced Asian nations. This fact underlines the contention of the overwhelming dominance of the western mindset. The use and application of AI in Eastern countries and populations *are more guided by its superficial utility than fundamental questions of cultural diversity and programme codes with structural biases.*

Finally, besides cultural diversity, the delegation of decisions, recommendations and judgments to "ethical machines" would require strong reference to the social responsibility of these rulings or judgments: *For whom and why and for what reason?* The basic principle of the knowledge process in the western mindset is the production of calculable and measurable knowledge. Underlying all human social activity are ethics, values, and morals. Using AI in this context implies that ethics and morals are measurable quantities. To date we do not know if these can be translated into measurable values: i.e. If these are computable [10]. Moreover, these translations will need to be compatible with the cultural diversity of the real world.

4. Search for Alternative Perspectives–Historical Evolution and Cultural Diversity

With the emergence of AI in this context, the opportunity eschewed studying the subject itself in a broader context including self-reflection or consciousness. AI was reduced to the technocratic perspective of measurable "intelligence" of the subject. Alternative or other aspects of the subject or its embeddedness in varied cultural and historical environments were hardly considered. With the global proliferation of this theme, the basic questions of its applicability in different socio-cultural domains with different social, moral, and ethical norms have risen to the surface. With its increased deployment in the socio-political sphere, the inherent contradictions and limitations of the mindset behind it seem to become more and more apparent.

Armed with reason and rationality, humans embarked upon assessing reality with this filter. The moot question is if this was the right and only filter. Deploying artefacts-such as AI developed and derived from this original background–especially in the socio-political domain is beset with serious deficits and dangers. All point to the inherent limits and inadequacies of the post-Enlightenment Western mindset–and its utility and applicability in varied cultural contexts. Ignoring these questions whilst deploying AI in the global socio-political domain entails grave dangers to the entire global socio-political fabric. Apparently, the western worldview–as we have seen–exhibits several serious deficits. These are: (i) Its strong adherence to the total separation of the observer and the observed; (ii) its insistence on using reason and logic as the sole instruments to assess the external world and gain "untainted" knowledge; (iii) its "blindness" towards cultural diversity of the world; (iv) its insistence in regarding moral, ethical and social rules as programmable algorithms and (v) its persistent avoidance of questions concerning consciousness and self-awareness.

4.1 Approach of the Non-western Mindsets

It should be pointed out that in the wake of the human civilizational process, different cultures have developed alternative *methods of perception of their natural and social environments and acquisition of knowledge*. These alternative methods of perceiving and assessing the natural and social worlds constituted core elements of these non-western mindsets [11,8].

The question then arises—what meaning and connotations do the concepts about the self and the "world" have in non-western cultures? In short, *non-western cultures* are less concerned about the issues of control over the external environment and more about 'self-control' and 'self-restraint'. Similarly, the question of means (instruments) of acquiring knowledge is not a central concern—since knowledge about the world can be acquired directly (tacit knowledge) *not requiring much mediation* [11].

The **non-western mindsets** are more adept with these themes. e.g., these have always regarded the two categories (i.e., the observer & the observed) as mutually dependent: the "external" world and the world of "observers" are interconnected and are in a state of reciprocal interaction②. *In contrast, in Western cultures* acquiring knowledge of the external world is primarily through intervention and measurement.

The following table provides some clarifications (Table 1).

Perhaps we can take the cue from the above and try to pursue this path further–out of the dead-end, which "development" of the last 500 years has taken us. In contrast to western cultures, the cultural history and heritage of other world regions speak a different story. Human history has witnessed the emergence of advanced cultures, states and empires with high levels of technical and social capabilities e.g. in South America, China, India, Egypt, the Mideast, etc. In almost all these cases, societies reached a

② "Tat tavam asi": Sanskrit- "thou art that": in Vedantic Hinduism; Chandogya Upanishad, https://de.wikipedia.org/wiki/Tat_Tvam_Asi

high and sophisticated level of knowledge in crucial fields like astronomy, geography, medicine, mathematics, and architecture. This allowed them to not only barely survive but also produce enough surpluses to feed their growing populations and enlarge their reach. They also founded large empires, sophisticated state systems and social organizations and bureaucracies. Their knowledge was also absorbed willingly in the West.

In contrast to the West, however, *not all advances in these cultures were at the cost of jettisoning their history, traditions and institutions*. Their acquiring new knowledge often reinforced their traditions, including social and political structures. Seen from this historical global perspective, cognition processes, technical achievements and knowledge acquisition about the natural and social environment–need not be drastically decoupled from traditions and belief systems to achieve high standards of knowledge. The cornerstone of this Western mindset–the radical break with tradition and the separation of the subject and object in the knowledge and cognition process–seems to have produced a unique narrative of only one proper way of progress.

In the history of human evolution, all alternative worldviews and mindsets however were brushed aside in the aftermath of the expansion of the West and especially Western Europe over the whole globe. The post-Enlightenment mindset, *in alliance with its original foe "religion"* (i.e. "Christianity") was used as a crusade to overrun and dominate all corners of the world. Using reason and rationality as the *sole weapons of acquiring knowledge*, what started originally as a commendable quest turned into a weaponised system to spread a particular worldview as the only possible system of acquiring knowledge. "By separating reason from tradition, the Enlightenment produced a new phenomenon: armed reason…" [1]. Other cultural mindsets, with a long intellectual history of profound discoveries and technical achievement-seemed to have followed different paths and many have not fared worse.

4.2 Role of the "Individual"

An *exception* is the new ***role of the "individual"***. *In difference to the post-Enlightenment tradition of the West, the individual did not play the central role in other cultures*. This is the most important contribution of the western "Enlightenment", which opened the way to a more individual (human) centred world. The singular individual is endowed with basic fundamental and protective "rights". When considering alternative constructs, it would be of paramount importance to regard this as its central element. Perhaps the time is ripe to reconsider the *current narrative of a singular path to human progress*, acknowledge other historical experiences and attempt to synthesize a *novel worldview incorporating different human historical experiences.*

Table 1. Comparison between Eastern and Western cultural patterns–regarding cognition, objective of knowledge, ways of reasoning etc. [11,8]

	Western culture (traditional values)	**Non-Western / Eastern culture (traditional values)**
Cognition patterns	- Objects /events are discreet - Focus on individual discrete objects and events - Observer and observed are separated (no mutual influence)	- Objects and subjects (observers) are interdependent - Observer and observed can be interrelated - Emphasis on the particular context of the act of observation
Reasoning-process	- Discreet objects /events - Focus on individual discrete objects and events - Observer and observed are separated (no mutual influence)	- Understanding the flux of events - "Insight"/empathic/awareness - Self-control, self-restraint - Restoring cosmic harmony bet. subject & object
	- Control over external events -"Measurability" of "external nature"	- 'Non-interference' with external nature
	- Manipulative: intervening in the external realm	
	- Analytic/deductive - Use of "formal logic" - Cause and effects are completely separated -are discreet categories - Separation of the observer from the observed (dualistic view)	- Inductive; dialectical; Intuitive - Direct knowledge / "tacit knowledge" - Awareness/gaining "Insight" / not control - Cause and effects can have *mutual effects* - Unification of the observed and the observer (holistic view)

5. Conclusions

What then are the essential elements of an alternative mindset that could assist in overcoming the current dilemmas? Essentially, this includes clarification of some open questions and concepts elements:

i). Question of "consciousness": The current mindset has apparently avoided grappling seriously with this question and has relegated it to the realm of "metaphysics". An impartial and unbiased assessment would be helpful.

ii). Overcoming the fundamental duality of the subject & object:

Currently, this principle appears to act as blinder-erasing other viewpoints. Allowing for the subject and the external world to be in a state of reciprocal interaction (an essential principle of the **non-Western** mindset), could assist in explaining the anomalies discovered especially in quantum physics.

iii). The overt reliance on rationality and computational processes as main instruments of acquiring knowledge block the recognition that **non-computable processes** also possess the capability of delivering "knowledge".

iv). Concept of "Information": The recognition that it is not self-explanatory but requires *reference to history, customs and traditions* for a comprehensive explanation.

v). **Ethics & Moral:** Moral and ethical action involve strong elements of self-doubt, self-reflection and references to historical narratives as guides. Therefore, 'judgments' and the act of judging in the real world are far removed from automated processes based on algorithms. Algorithms function mainly by following objectives and instructions–they do not consider self-reflection or self-doubt. "An algorithm knows only its instructions and objectives, not moral or doubt" [1].

vi). Allowing for "cultural diversity": The current mindset does not seem to allow for other cultural viewpoints. Mono-culturalism appears to be inbuilt into the system.

Proper accounting for these elements and their inclusion in an alternative mindset may assist in providing the correct answers to the urgent questions facing humankind today.

Conflict of Interest

There is no conflict of interest.

References

[1] Kissinger, H.A., Schmidt, E., Huttenlocher, D., 2021. The age of AI and our human future. John Murray: UK.

[2] Einstein, A., 2009. About the special and general theory of relativity, 24th.ed. Springer: Germany.

[3] Schrödinger, E., 1967. What is life? And mind and matter. Cambridge University Press: UK.

[4] Heisenberg, W., 2007. Physics and Philosophy: The Revolution in Modern Science, Harper Perennial. Penguin Classics: London, UK.

[5] Stapp, H., 2009. Mind, matter, and quantum mechanics. Springer: Germany.

[6] Wittgenstein, L., 2009. Philosophical Investigations, 4th ed. Hacker, P.M.S., Schulte, J., (eds. and translators). Oxford: Wiley-Blackwell: Hoboken, New Jersey.

[7] Sandel, M., Ann, T., Robert, B., et al., 2020. Ethical concerns mount as AI takes bigger decision-making role [Internet]. Harvard Gazette. Available from: https://news.harvard.edu/gazette/story/2020/10.

[8] Amershi, B., 2020. Culture, the process of knowledge, perception of the world and emergence of AI. AI & Society. 35, 428-429.
DOI: https://doi/10.1007/s00146-019-00885-z.

[9] Gill, K.S., 2018. Data to decision and judgement making—a question of wisdom. IFAC Papers On Line. 51(30), 733-738.
DOI: https://doi.org/10.1016/j.ifacol.2018.11.205.

[10] Penrose, R., 1989. The Emperor's new mind concerning computers, minds and the laws of physics. Oxford University Press: Oxford.

[11] Varnum, M.E., Grossmann, I., Kitayama, S., et al., 2010. The origin of cultural differences in cognition, the social orientation hypothesis. Current Directions in Psychological Science. 19(1), 9-13.
DOI: https://doi.org/10.1177/0963721409359301.

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Artificial Intelligence Advances
https://ojs.bilpublishing.com/index.php/aia

ARTICLE

On Monetizing Personal Wearable Devices Data: A Blockchain-based Marketplace for Data Crowdsourcing and Federated Machine Learning in Healthcare

Mohamed Emish[1*] Hari Kishore Chaparala[1] Zeyad Kelani[1,2] Sean D. Young[1,3]

1. Department of Informatics, University of California, Irvine, 92697, United States of America
2. Department of Political Science, Faculty of Economics and Political Science Cairo University, Egypt
3. Department of Emergency Medicine, University of California, Irvine, 92697, United States of America

ARTICLE INFO

Article history
Received: 14 December 2022
Revised: 6 January 2023
Accepted: 9 January2023
Published Online: 2 February 2023

Keywords:
Wearable devices
Data integrity
Data validation
Federated learning
Blockchain
Trusted execution environment
Health informatics
Healthcare data collection
Data monetization

ABSTRACT

Machine learning advancements in healthcare have made data collected through smartphones and wearable devices a vital source of public health and medical insights. While wearable device data help to monitor, detect, and predict diseases and health conditions, some data owners hesitate to share such sensitive data with companies or researchers due to privacy concerns. Moreover, wearable devices have been recently available as commercial products; thus large, diverse, and representative datasets are not available to most researchers. In this article, the authors propose an open marketplace where wearable device users securely monetize their wearable device records by sharing data with consumers (e.g., researchers) to make wearable device data more available to healthcare researchers. To secure the data transactions in a privacy-preserving manner, the authors use a decentralized approach using Blockchain and Non-Fungible Tokens (NFTs). To ensure data originality and integrity with secure validation, the marketplace uses Trusted Execution Environments (TEE) in wearable devices to verify the correctness of health data. The marketplace also allows researchers to train models using Federated Learning with a TEE-backed secure aggregation of data users may not be willing to share. To ensure user participation, we model incentive mechanisms for the Federated Learning-based and anonymized data-sharing approaches using NFTs. The authors also propose using payment channels and batching to reduce smart contact gas fees and optimize user profits. If widely adopted, it's believed that TEE and Blockchain-based incentives will promote the ethical use of machine learning with validated wearable device data in healthcare and improve user participation due to incentives.

*Corresponding Author:
Mohamed Emish,
Department of Informatics, University of California, Irvine, 92697, United States of America;
Email: memish@uci.edu

DOI: https://doi.org/10.30564/aia.v4i2.5316

1. Introduction

Big data analytics and the Medical Internet of Things (MIoT) are becoming integral to a proactive healthcare system [1]. One source of this information is wearable devices such as smartwatches that constantly track participants' vital signs. The wearable devices market is expected to soar around threefold (115.8 billion US dollars to 380 billion US dollars) between 2021 and 2028 [2]. However, users of wearable devices have privacy concerns regarding sharing data about vital signs and their location [3]. We have identified three reasons data owners are hesitant to share their wearable devices' data. First, some data owners fear being watched by "digital big brother" and the potential threat to their data privacy rights [4]. Some data owners also have major concerns about confidentiality. They desire control over what the data can be used to infer about them, especially when combined with data from other platforms [5]. Moreover, the value of data in the information economy has made it a target of attacks, leading to data breaches and personal data theft outside of trusted organizations [6]. Second, even when data owners share their data, some data consumers don't know if they can trust it, as it may be malicious. For example, automated bots can generate low-quality sets by creating fake records that simulate real user behavior [7]. Third, many data owners may feel they are not fairly compensated for their data. In contrast, data brokers accumulate large amounts of data and use it to create products for surveillance and marketing [8]. In addition to privacy, creating machine learning models that work effectively for individuals from different backgrounds is inhibited by the inaccessibility of inclusive datasets to researchers [9].

Previous studies have explored use cases for machine learning models and wearable device data. They have shown significant promise for such an approach in detecting health conditions. For example, accelerometer sensor data from smartwatches were used to detect sleep apnea and sleep classification, respectively [10,11]. Another study used biosensor data in armbands to monitor skin temperature, respiratory rate, blood pressure, pulse rate, and blood oxygen saturation. It used this data to create an early detection model for COVID-19 [12]. Wearable device data from wristbands were also used to continuously monitor the physiological parameters of patients in urgent care and train machine learning models that detect clinical deterioration [13]. Other studies have collected data from emerging wearable devices such as headbands [14] or Respiratory Belts (RB) [15] to detect seizures [16-18], monitor emotions [19,20] and track rehabilitation tasks [21-23], as well as detecting and monitoring heart diseases (arrhythmia [24-26], hypertension [27], and strokes [28,29]).

We propose a decentralized, fully automated marketplace to capture these insights by securely sharing data from wearable devices between data owners and consumers. Our marketplace uses several advances in cryptography techniques and Federated Machine Learning (ML) to respond to the challenges of using wearable devices and ML in Healthcare. First, we propose Trusted Execution Environments (TEE) to verify data records' validity and ensure that they are not stolen or produced by bots. The marketplace then offers a platform for data owners to list their wearable device records as NonFungible Tokens (NFTs). Federated learning will train local models without copying or moving the data owners' sensitive data records from their devices. Alternatively, data owners can choose to sell their wearable device records to data consumers by transferring ownership of NFTs. Data owners will be rewarded for selling data or contributing to training ML models requested by the data consumers. We also use security measures to blacklist malicious data owners or consumers who try to break the system's rules. Our novel design for a fair and secure marketplace would collect genuine data that can be used for the accurate detection and prevention of diseases and reward users willing to share data with the broader research community. The design decisions of this marketplace aim to support the trustless trading of clean data with strong integrity checks, thwart malicious data owners and consumers, and an incentive mechanism for promoting fair user participation. While several existing studies and models [30-33], most focus on the privacy-preserving nature of trading sensitive data. They don't guarantee strong data validations and mechanisms to prevent malicious data sellers. On the other hand, our approach provides a privacy-preserving platform for trading data with strong integrity checks.

The main contributions of this paper are:

- Rewarding wearable device data sharing using NFTs in a scalable and cost-effective manner.
- Verifying the integrity of data records using TEE to thwart malicious data sellers.
- Applying a pay-per-usage model based on federated learning and secure aggregation using TEE.

2. Literature Review

2.1 Existing Marketplaces

Alan et al. [30] proposed a marketplace where the users define data-sharing policies translated into smart contracts. In their model, the wearable device users generate

the data stored in Data Custodian or wearable device manufacturer's cloud storage. The users also set policies on how their data can be accessed in Blockchain. A data broker entity matches users and data consumers based on their preferences. Once a match is made, based on a set of policies, a smart contract for trading the data is created and the data transaction takes place. The authors point out that since data come from the device manufacturer's cloud storage, data integrity is preserved. However, it's not shown exactly how the device manufacturer preserves the data integrity. Moreover, it requires data consumers to trust the device manufacturer. In contrast, our model uses TEEs in user devices that generate attested data from attested wearable device software. In addition, we also prevent data duplication attacks using sequence numbers. Also, there are several centralized and trusted components in their proposed architecture, like Data Anonymizer and Data Custodian's cloud, which can be compromised by a malicious entity, thus creating data privacy and integrity concerns. Our model addresses privacy concerns using federated learning with a TEE-backed secure aggregation and NFT transactions. In addition, the data anonymizer resides within secure enclaves that ensure a consistent data format.

Sterling [31] is another privacy-preserving data marketplace. It uses a TEE to perform secure machine learning using the policies set in the data provider and consumer smart contract. The authors suggest using machine learning model parameters to check whether the data are fake. But a malicious user can always generate duplicate data or corrupt the model in several steps, ensuring that at each step of the training, the model parameters don't deviate enough creating a red flag. Also, there are no mechanisms proposed to blacklist a malicious data provider. Our model uses the TEE identity to blacklist users. Using a TEE identity-based blacklisting, users can't arbitrarily create fake identities, and purchasing a new wearable device to bypass a blacklist will most likely cause negative incentives.

Gonzalo et al. [32] performed a systematic literature review on IoT data markets' privacy-enhancing technologies. Some surveyed papers employed Truth Discovery and reputation-based systems for data integrity checks. However, these approaches are not practical for wearable device data, where we treat every user as an anonymous entity. Most of the studies [32] were more inclined to preserve data generators' privacy rather than ensure data integrity. On the other hand, our model is privacy-preserving and ensures strong data integrity.

Primal [33] is a cloud-based privacy-preserving marketplace. It is not decentralized, and if the cloud is compromised, consumer and producer data are at risk. Primal's proposed data validation protocol requires the consumers to estimate the data quality based on the trained machine learning model. Our model does not require any effort from the consumer's end, as the TEE attests to the data.

One study proposed a design for a decentralized data marketplace on the Blockchain that uses arbitration to settle disputes between data owners and data consumers [34]. In the authors' design, untrustworthy data buyers or sellers are detected using an arbitrators alliance that both parties in the transaction nominate. The arbitrator's decision will be executed using secure smart contracts; however, this design still requires the intervention of external actors, which can take time and might not lead to accurate resolutions. Zhang et al. [35] proposed a data marketplace with a network storage service verification mechanism. But it lacks the performance needed for scalability. Makhdoom et al. [36] designed a framework for rewarding data sharing from IoT devices in smart cities based on smart contracts and digital tokens (PrivyCoin). While data security and rewards are available for data owners, creating a customized coin to distribute rewards requires a large blockchain infrastructure. This can be avoided by using all-propose tokens widely traded between cryptocurrency owners, such as Ethereum, Solana, and Binance. Li et al. [37] proposed a rewarding system for sharing IoT data based on Monero Technology to ensure anonymous data exchange and multi-sharing. All these models lack strong data validation techniques, which are especially important for healthcare data as a minor trained machine learning model corruption might cause serious consequences.

2.2 Detecting Malicious Actors

Some applications of integrating federated learning with Blockchain have been proposed in industry and academia. A privacy-preserving blockchain-based federated learning study [38] shows how home appliance manufacturers can gather information from users to improve smart home systems. In the author's model, first, the users train a publicly available model on the Blockchain, then the Blockchain acts as the aggregator of models from different users. Blockchain prevented prevent malicious manufacturers or users. In the second stage, the smart contract performed a crowdsourcing task that aggregated and computed the average model. Incentives were also awarded to the miner in the crowdsourcing task. The authors also used a Differential Privacy Preserving algorithm for data privacy. However, manufacturers are not considered malicious to corrupt the model as they are the model owners. Another study used homomorphic encryption to encode the gradients of ML models to preserve user privacy and

prevent possible inference attacks [39] but this may not be feasible for types of machine learning models.

3. System Design

3.1 Architecture Overview

This section introduces our proposed system design for the wearable devices data marketplace. Our marketplace has two groups of stakeholders: Data consumers and data owners. Data consumers employ a crowdsourcing model based on federated learning, with the initial models running on user devices. Data owners list their data as a Non-Fungible Token (NFT) in health data marketplaces. We utilize TEE to ensure data integrity, addressing threats from malicious users (data owners) and malicious data consumers trying to compromise data privacy. Our model consists of a wearable device with TEE, a user-owned mobile device for performing federated model training, a secure aggregator using TEE for preserving user privacy, a smart contract hosting a federated learning model, and an ERC-721-based [40] NFT contract that verifies the final model output and NFT data. ERC-721 tokens are used to incentivize users in the federated learning-based and NFT-based data-selling approaches.

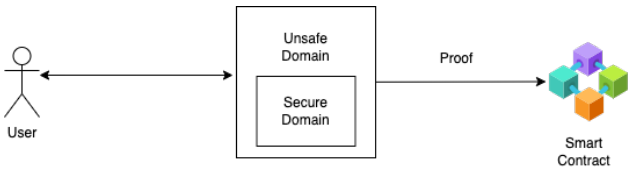

Figure 1. Health data attestation.

3.2 Verification of Data Records

Malicious data owners could try to fake the data or copy existing data to resell in our health data marketplace. Moreover, a group of malicious users could collaboratively try to corrupt the machine learning models using invalid data. Using hashing algorithms to ensure data integrity is insufficient because a malicious user can modify data to generate a unique record. For this reason, we propose using TEE in wearable devices. The TEE can attest that a valid workflow genuinely generates the data. In the case of a wearable device, data records represent a physical activity or other monitored vital signs. Within a TEE, the code and data loaded are immune from modification and eavesdropping, thus ensuring data privacy and integrity. TEE has dedicated, private regions of memory called "enclaves." The isolated memory runs a private Operating System (OS). ARM TrustZone [41], Intel Software Guard Extensions [42], and AMD Platform Security Processor [43] are popular examples of private OS's that run in enclaves. In our design, we use an ARM Cortex-M23 series processor [44] using TrustZone-M, which has been widely used in IoT devices [45] and is currently listed as a small and energy-efficient processor suitable for wearable devices. Data owners' activities are processed within the TEE, and the data are attested using the TEE's private key $\rho = SIG(data, pk_{tee})$ where SIG is the signing function and ρ is the attestation. The private key pk_{tee} associated with the TEE is unique and only known within the TEE. A public key pub_{tee} can be used to verify the attestation. For a user to list the health data, a hash h is generated on the data record using a one-way hashing algorithm $H(data)$. The user can optionally save the data in an InterPlanetary File System (IPFS) like Pinata [46]. To mint an NFT corresponding to a health record, the smart contract uses pub_{tee} to verify a health record hash. To prevent duplication and reselling of the same health records, every record is associated with a stepwise increasing sequence number, verified at smart contract. Figure 1 shows the overview of health data attestation using a smart contract and a TEE.

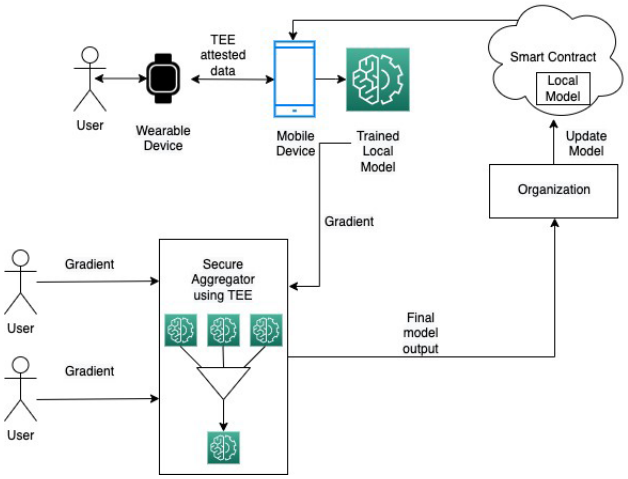

Figure 2. Federated Learning with users.

3.3 Federated Learning

Federated learning [38,47,48] is used to train an ML model in a distributed manner while data stays on-premises—in our case, on the data owners' devices. After locally training models on multiple devices, they are gathered and aggregated by the data consumer. In our design, as shown in Figure 2, the user data from wearable devices are collated into a mobile device that pulls a local model for federated learning from the blockchain. As the model is present on the blockchain, it reduces the chances of the model being malicious. Once the local model is trained, it is sent to a secure aggregator based on a trusted execution environ-

ment. We use Intel SGX OS to handle secure enclaves on the external aggregation server. The aggregation server enclaves collect and aggregate the ML model's gradients from all users. The final model output is signed by the TEE and sent to the data consumer. We are not sending individual gradients to the organization but rather the aggregated model. This ensures that user information cannot be inferred from the gradients. The gradient transfer is encrypted to prevent the eavesdropping of gradients by the system encompassing the TEE, and the security keys can be transmitted using the RSA algorithm [49].

The gradients generated by the users have signed $SIG(gradient,pk_{user})$ using user private keys, and the final gradient is also signed by the TEE $SIG(final\ \_output,pk_{tee})$. This protects organizations from model corruption.

3.4 User Incentives from Federated Learning

Data owners can earn incentives from locally training ML models and publishing the gradients to data consumers. The secure aggregator collects the TEE-signed gradients from users, which determines the number of ERC-20 tokens to be sent to the data owner as an incentive. A signed message $SIG(gradient,pk_{tee\ user},wallet\ id,data\ size,hash)$ is sent to the secure aggregator from all users. $pk_{tee\ user}$ is the private TEE key used in the user's wearable device to sign the message. *Data size* is the size of the new data used to train the federated learning model. Data owners will be rewarded with Ethereum tokens based on the number of new data records they contribute to the local ML model. Then, we acquire a unique hash for $H(data)$, on the data records used for training. The secure aggregator uses the hash to tackle replay attacks in which the user can try to send the same training output again to get incentives. The secure aggregator maintains a hash table of records and prevents data owners from using the same data more than once. As we are using a TEE for storing these hashes, any downtime in the enclave could lead to the loss of the hash table. The hash data can be periodically synced with external encrypted storage (or an IPFS) that the TEE can only modify to prevent this loss. Once the signed local model outputs reach the secure aggregator, it can verify the signatures signed by $pk_{tee\ user}$ and the *hash* information. The appropriate award to the data owner is then calculated based on the amount of data they contributed. A signed message from the secure aggregator $SIG([[u_1,p_1],[u_2,p_2],...],hash,pk_{sg})$ is sent to the smart contract for the award payment. The smart contract verifies the signature and the hash. A hash table is also maintained in the smart contract to prevent replay attacks. A daily quota on the transfer is set on the data consumers' wallets for safety. Incentives are transferred from the data consumers' wallets to the data owners' wallets while the quota lasts. Algorithm 1 shows the smart contract logic to send incentives to data owners. As the payments are usually small, a low-gas fee network like Polygon [50] or Payment Channels [51] will reduce the fees required to complete the transactions between the two parties (data owner and data consumer). Algorithm 1 shows how the payments flow in the smart contract, and Figure 3 details the overview of user incentives with federated learning.

Algorithm 1 User payments in Smart Contact

fn pay users($\rho = SIG([[u_1,p_1],[u_1,p_1],...],hash,pk_{sg})$)
VERIFY(ρ,pub_{sg}) if hash not in Hash Table then
payments ← $[[u_1,p_1],[u_1,p_1],...]$ balance ← Remaining Organization daily quota for all p_i,u_i in payments do
if p_i − balance ≥ 0 then transfer(p_i, u_i)
balance ← p_i − balance
Update remaining quota end if
end for end if

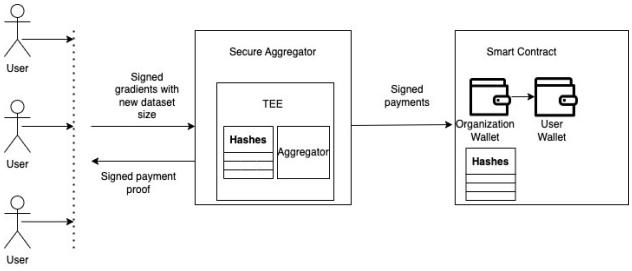

Figure 3. User Incentives.

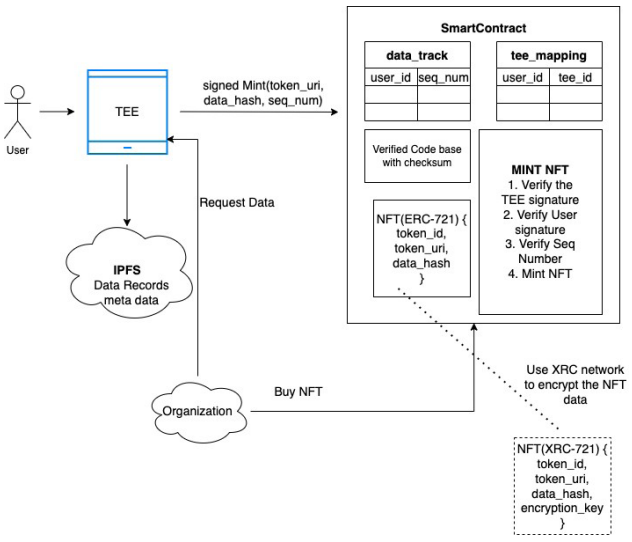

Figure 4. Minting health data as NFT.

3.5 Minting Wearable Device Data as NFTs

In some cases, federated learning might not work accurately for all health data-related machine learning applications. Also, data owners may be comfortable with sharing health data from wearable devices. To surmount these bar-

riers, we propose extending our framework to allow data owners to mint health records from wearable devices as NFTs. As a result, data consumers can directly train their ML models on the data. We use the same TEE architecture to attest the data records, and each record is associated with a sequence number as described in subsection III-B. While listing the NFT, the data owners' personal and sensitive information is removed from the records. For this purpose, the TEE in the data owners' devices only uses the publicly visible, verified codebase on the blockchain. This codebase is responsible for encapsulating the data from the wearable device without any sensitive information. The codebase will also generate metadata helpful for data consumers filtering the data. Before minting the data records as NFTs, they are made visible to the data owners for review. When a data owner decides to list their health record, they can create an IPFS record with the metadata. Since minting NFT requires gas fees, wearable device data will be minted in batches large enough for the data owner to receive incentives. A call is then made to the smart contract signed by the TEE with *token url*, *data hash* for integrity verification, and *seq num* to prevent reselling the data. The minting process is shown in Figure 4. In the smart contract, we keep track of *the user id* and *tee _id* mapping and the *seq _num* associated with the user. During the minting process, we verify the TEE attestation, user signature, and whether *seq num* ≥ last sequence number from the user is present in the mapping. Upon passing all checks, we mint the NFT. It is possible to perform lazy minting [52] to delay the payment of the gas fee until the NFT is sold. Data consumers can now buy the listed NFTs on the marketplace.

Currently, the original data only resides with the user. Unlike artwork NFTs, if the wearable device data is public, organizations could access the records without purchasing NFT; thus, users will not be rewarded. If a user denies sending the data to a data consumer, they can be blacklisted by the consumer using the tee_{id}. Creating new user profiles cannot escape from the blacklist, as the tee_{id} is embedded with the device. Given that a wearable device with TEE support is likely more valued than the user data, a malicious user has no incentive to reject data share requests by the organization. Once the data is shared with the data consumer, its integrity can be verified using the checksum in the smart contract's NFT data. To list and purchase NFT and perform atomic transactions with ERC-20 tokens and NFT tokens, we recommend using the Wyvern protocol [51], as popular marketplaces like OpenSea currently use it [53]. If data owners lack storage for all their listed data records, they can use the XRC-721 standard offered by XDC-Network and store the encrypted NFT information in IPFS. Using this standard, it is possible to encrypt NFT data so that only the NFT owner can access the encryption key to decrypt the NFT data. But this requires switching to a different blockchain.

4. Discussion

ML and wearable device data records have great potential to improve well-being and advance scientific healthcare research. Clean and trusted data can create accurate ML models and reach this potential. Our novel wearable device data marketplace design utilizes Federated Learning, TEE, and blockchain to provide a privacy-preserving way for the owners to share health data and guarantee strong data validations. Our marketplace allows users to participate in the data-sharing workflow using Federated learning or NFT-based data record sales. Our data marketplace stores the metadata of records, making data that belong to populations of interest findable by scientists and data consumers. The marketplace is open to all data owners and consumers with the appropriate wearable device with TEE support. Our design consists of secure and fair incentive mechanisms for the users selling the data records as NFTs or participating in crowdsourced federated learning. Our security model tackles malicious sellers, data consumers, and external third parties. This makes our marketplace a Findable, Accessible, Interoperable, and Reusable (FAIR) data source [55]. Our approach is also practical if major wearable device manufacturers start supporting TEE-based data attestation. Also, since federated learning is distributed and the initial models run on user devices, it may help small organizations save infrastructure costs associated with model training and data storage.

The main limitations of our approach are, unlike software patches for any discovered vulnerabilities, any wearable device vulnerabilities in the TEE might require device replacement or withdrawal from marketplace participation. It may not be possible to onboard existing wearable devices onto our marketplace. Also, federated learning might only be best suited for training some types of models.

Conflict of Interest

There is no conflict of interest.

References

[1] Dimitrov, D.V., 2016. Medical internet of things and big data in healthcare. Healthcare Informatics Research. 22(3), 156.
DOI: https://doi.org/10.4258/hir.2016.22.3.156

[2] Elshafeey, A., Mhaimeed, O., Al Ani, J., et al., 2021. Wearable devices and machine learning algorithms for cardiovascular health assessment. Machine Learning in Cardiovascular Medicine. 10(1), 353-370.
DOI: https://doi.org/10.1016/b978-0-12-820273-9.00015-4

[3] Cilliers, L., 2019. Wearable devices in healthcare: Privacy and information security issues. Health Information Management Journal. 49(2-3), 150-156.
DOI: https://doi.org/10.1177/1833358319851684

[4] Raposo, V.L., 2021. Big brother knows that you are infected: Wearable devices to track potential COVID-19 infections. Law, Innovation and Technology. 13(2), 422-438.
DOI: https://doi.org/10.1080/17579961.2021.1977214

[5] Kostkova, P., Brewer, H., de Lusignan, S., et al., 2016. Who owns the data? Open data for healthcare. Frontiers in Public Health. 17(4), 7. Available from: https://pubmed.ncbi.nlm.nih.gov/26925395/.

[6] Seh, A.H., Zarour, M., Alenezi, M., et al., 2020. Healthcare data breaches: Insights and implications. Healthcare. 8(2), 133.
DOI: https://doi.org/10.3390/healthcare8020133

[7] Pozzar, R., Hammer, M.J., Underhill-Blazey, M., et al., 2020. Threats of bots and other bad actors to data quality following research participant recruitment through social media: Cross-sectional questionnaire. Journal of Medical Internet Research. 22(10).
DOI: https://doi.org/10.2196/23021

[8] Sadowski, J., 2019. When data is capital: Datafication, accumulation, and extraction. Big Data & Society. 6(1), 205395171882054.
DOI: https://doi.org/10.1177/2053951718820549

[9] Huhn, S., Matzke, I., Koch, M., et al., 2022. Using wearable devices to generate real-world, individual-level data in rural, low-resource contexts in Burkina Faso, Africa: A case study. Frontiers in Public Health. 10, 972177.
DOI: https://doi.org/10.3389/fpubh.2022.972177

[10] Hayano, J., Yamamoto, H., Nonaka, I., et al., 2020. Quantitative detection of sleep apnea with wearable watch device. Plos One. 15(11), e0237279.
DOI: https://doi.org/10.1101/2020.07.24.219261

[11] Sundararajan, K., Georgievska, S., te Lindert, B.H., et al., 2021. Sleep classification from wrist-worn accelerometer data using random forests. Scientific Reports. 11(1).
DOI: https://doi.org/10.1038/s41598-020-79217-x

[12] Wong, C.K., Ho, D.T., Tam, A.R., et al., 2020. Artificial intelligence mobile health platform for early detection of COVID-19 in quarantine subjects using a wearable biosensor: Protocol for a randomised controlled trial. BMJ Open. 10(7).
DOI: https://doi.org/10.1136/bmjopen-2020-038555

[13] Un, K.C., Wong, C.K., Lau, Y.M., et al., 2021. Observational study on wearable biosensors and machine learning-based remote monitoring of COVID-19 patients. Scientific Reports. 11(1).
DOI: https://doi.org/10.1038/s41598-021-82771-7

[14] Laureanti, R., Bilucaglia, M., Zito, M., et al. (editors), 2020. Emotion assessment using machine learning and low-cost wearable devices. 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC); 2020 Jul 20-24; Montreal, QC, Canada. USA:IEEE. p. 576-579.
DOI: https://doi.org/10.1109/embc44109.2020.9175221

[15] Ayata, D., Yaslan, Y., Kamasak, M.E., 2020. Emotion recognition from multimodal physiological signals for emotion aware healthcare systems. Journal of Medical and Biological Engineering. 40(2), 149-157.
DOI: https://doi.org/10.1007/s40846-019-00505-7

[16] Regalia, G., Onorati, F., Lai, M., et al., 2019. Multimodal wrist-worn devices for seizure detection and advancing research: Focus on the empatica wristbands. Epilepsy Research. 153, 79-82.
DOI: https://doi.org/10.1016/j.eplepsyres.2019.02.007

[17] Onorati, F., Regalia, G., Caborni, C., et al., 2021. Prospective study of a multimodal convulsive seizure detection wearable system on pediatric and adult patients in the epilepsy monitoring unit. Frontiers in Neurology. 12, 724904.
DOI: https://doi.org/10.3389/fneur.2021.724904

[18] Onorati, F., Regalia, G., Caborni, C., et al., 2017. Multicenter clinical assessment of improved wearable multimodal convulsive seizure detectors. Epilepsia. 58(11), 1870-1879.
DOI: https://doi.org/10.1111/epi.13899

[19] Laureanti, R., Bilucaglia, M., Zito, M., et al. (editors), 2020. Emotion assessment using machine learning and low-cost wearable devices. 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC); 2020 Jul 20-24; Montreal, QC, Canada. USA:IEEE. p. 576-579
DOI: https://doi.org/10.1109/embc44109.2020.9175221

[20] Al Zoubi, O., Awad, M., Kasabov, N.K., 2018. Anytime multipurpose emotion recognition from EEG data using a liquid state machine based framework. Artificial Intelligence in Medicine. 86, 1-8.
DOI: https://doi.org/10.1016/j.artmed.2018.01.001

[21] Potluri, S., Chandran, A.B., Diedrich, C. (editors), et al., 2019. Machine learning based human gait segmentation with wearable sensor platform. 2019 41st

Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC); 2019 Jul 23-27; Berlin, Germany. USA:IEEE. p. 588-594.
DOI: https://doi.org/10.1109/embc.2019.8857509

[22] Zhang, H., Guo, Y., Zanotto, D., 2020. Accurate ambulatory gait analysis in walking and running using machine learning models. IEEE Transactions on Neural Systems and Rehabilitation Engineering. 28(1), 191-202.
DOI: https://doi.org/10.1109/tnsre.2019.2958679

[23] Moore, S.R., Kranzinger, C., Fritz, J., et al., 2020. Foot strike angle prediction and pattern classification using LOADSOLTM wearable sensors: A comparison of machine learning techniques. Sensors. 20(23), 6737.
DOI: https://doi.org/10.3390/s20236737

[24] Hannun, A.Y., Rajpurkar, P., Haghpanahi, M., et al., 2019. Cardiologist-level arrhythmia detection and classification in ambulatory electrocardiograms using a deep neural network. Nature Medicine. 25(1), 65-69.
DOI: https://doi.org/10.1038/s41591-018-0268-3

[25] Kwon, S., Hong, J., Choi, E.K., et al., 2020. Detection of atrial fibrillation using a ring-type wearable device (CardioTracker) and deep learning analysis of photoplethysmography signals: Prospective observational proof-of-concept study. Journal of Medical Internet Research. 22(5).
DOI: https://doi.org/10.2196/16443

[26] Mei, Z., Gu, X., Chen, H., et al., 2018. Automatic atrial fibrillation detection based on heart rate variability and spectral features. IEEE Access. 6, 53566-53575.
DOI: https://doi.org/10.1109/access.2018.2871220

[27] Miao, F., Wen, B., Hu, Z., et al., 2020. Continuous blood pressure measurement from one-channel electrocardiogram signal using deep learning techniques. Artificial Intelligence in Medicine. 108, 101919.
DOI: https://doi.org/10.1016/j.artmed.2020.101919

[28] Lown, M., Brown, M., Brown, C., et al., 2020. Machine learning detection of atrial fibrillation using wearable technology. Plos One. 15(1).
DOI: https://doi.org/10.1371/journal.pone.0227401

[29] Liu, Y., Fang, B., Zhao, Y., et al. (editors), 2021. Ensemble learning for atrial fibrillation screening from a single lead ECG wave of wearable devices. 2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC); 2021 Nov12-14; Greenville, SC, USA. USA: IEEE. p. 590-594.
DOI: https://doi.org/10.1109/icftic54370.2021.9647218

[30] Colman, A., Chowdhury, M.J., Baruwal, C.M. (editors), 2019. Towards a trusted marketplace for wearable data. 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC); 2019 Dec 12-14; Los Angeles, CA, USA. USA: IEEE. p. 314-321.
DOI: https://doi.org/10.1109/cic48465.2019.00044

[31] Hynes, N., Dao, D., Yan, D., et al., 2018. A demonstration of sterling. Proceedings of the VLDB Endowment. 11(12), 2086-2089.
DOI: https://doi.org/10.14778/3229863.3236266

[32] Garrido, G.M., Sedlmeir, J., Uludağ, Ö., et al., 2022. Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IOT: A systematic literature review. Journal of Network and Computer Applications. 207, 103465.
DOI: https://doi.org/10.1016/j.jnca.2022.103465

[33] Song, Q., Cao, G., Sun, K., et al. (editors), 2021. Try before you buy: Privacy-preserving data evaluation on cloud-based machine learning data marketplace. ACSAC'21: Annual Computer Security Applications Conference; 2021 Dec 6-10; New York: Virtual Event, USA. ACM. p. 13.
DOI: https://dl.acm.org/doi/10.1145/3485832.3485921

[34] Tang, H., Qiao, Y., Yang, F., et al., 2022. DMOBAs: A data marketplace on blockchain with arbitration using side-contracts mechanism. Computer Communications. 193, 10-22.
DOI: https://doi.org/10.1016/j.comcom.2022.06.029

[35] Zhang, C., Xu, Y., Hu, Y., et al., 2022. A blockchain-based multi-cloud storage data auditing scheme to locate faults. IEEE Transactions on Cloud Computing. 10(4), 2252-2263.
DOI: https://doi.org/10.1109/tcc.2021.3057771

[36] Makhdoom, I., Zhou, I., Abolhasan, M., et al., 2019. Privysharing: A blockchain-based Framework for Integrity and Privacy-preserving Data Sharing in Smart Cities. Computers & Security. 88, 101653.
DOI: https://doi.org/10.1016/j.cose.2019.101653

[37] Li, T., Wang, H., He, D., et al., 2022. Block Chain Based Privacy-preserving and Rewarding Private Data Sharing for IOT. IEEE Internet of Things Journal. 9(16), 15138-15149.
DOI: https://doi.org/10.1109/jiot.2022.3147925

[38] Zhao, Y., Zhao, J., Jiang, L., et al., 2021. Privacy-preserving Blockchain-based Federated Learning for IOT Devices [Internet] [Retrieved 2022 Dec 7]. Available from: https://arxiv.org/abs/1906.10893.

[39] Facts & Factors, 2022. Insights on Global Wearable Technology Market Size & Share to Surpass

USD 380.5 Billion by 2028, Exhibit a Cagr of 18.5% Industry Analysis, Trends, Value, Growth, Opportunities, Segmentation, Outlook & Forecast Report by Facts & Factors [Internet]. GlobeNewswire News Room [Retrieved 2022 Dec 7]. Available from: https://www.globenewswire.com/news-release/2022/04/13/2421597/0/en/Insights-on-Global-WearableTechnology-Market-Size-Share-to-Surpass-USD-380-5-Billion-by-2028-Exhibit-a-CAGR-of-18-5-Industry-Analysis-Trends-ValueGrowth-Opportunities-Segmentatio.html.

[40] Entriken, W., Shirley, D., Evans, J., et al., 2018. EIP-721: Non-Fungible Token Standard. Ethereum Improvement Proposals [Internet] [Retrieved 2022 Dec 7]. Available from: https://eips.ethereum.org/EIPS/eip-721.

[41] LTE Cat-m a Cellular Standard for IOT—ARM Architecture Family [Internet] [Retrieved 2022 Dec 8]. Available from: https://community.arm.com/cfsfile/ key/telligent-evolution-components-attachments/01-2142-0000-00-00-68-74/LTE-Cat 2D00 M-2D00 -A-Cellular-Standard-forIoT.pdf.

[42] Intel Software Guard Extensions [Internet] [Retrieved 2022 Dec 7]. Available from: https://www.intel.com/content/www/us/en/developer/tools/softwareguard-extensions/overview.html.

[43] Microsoft Pluton Security Processor [Internet]. AMD Pro Security [Retrieved 2022 Dec 8]. Available from: https://www.amd.com/en/technologies/pro-security.

[44] System-Wide Security for IoT Devices [Internet]. Trustzone for Cortex-M-ARM® [Retrieved 2022 Dec 7]. Available from: https://www.arm.com/technologies/trustzonefor-cortex-m.

[45] Oliveira, D., Gomes, T., Pinto, S., 2012. UTANGO: An Open-source Tee for IOT Devices [Internet]. arXiv [Retrieved 2022 Dec 8]. Available from: https://arxiv.org/pdf/2102.03625.pdf.

[46] Your Home for NFT Media [Internet]. Pinata [Retrieved 2022 Dec 7]. Available from: https://www.pinata.cloud/.

[47] Konečný, J., McMahan, H.B., Yu, F.X., et al., 2017. Federated Learning: Strategies for Improving Communication Efficiency [Internet]. arXiv.org [Retrieved 2022 Dec 7]. Available from: https://arxiv.org/abs/1610.05492.

[48] McMahan, H.B., Moore, E., Ramage, D., et al., 2017. Communication-efficient Learning of Deep Networks from Decentralized Data [Internet]. arXiv.org [Retrieved 2022 Dec 7]. Available from: https://arxiv.org/abs/1602.05629.

[49] Fang, H., Qian, Q., 2021. Privacy Preserving Machine Learning with Homomorphic Encryption and Federated Learning [Internet]. MDPI [Retrieved 2022 Dec 7]. Available from: https://www.mdpi.com/19995903/13/4/94.

[50] Polygon Wallet—Bring the World to Ethereum [Internet] [Retrieved 2022 Dec 7]. Available from: https://polygon.technology/.

[51] Lightning Network [Internet] [Retrieved 2022 Dec 7]. Available from: https://lightning.network/.

[52] Can I List an Item Without Paying to "Mint" It? [Internet] Opensea [Retrieved 2022 December 8] Available from: https://support.opensea.io/hc/en-us/articles/1500003076601-Can-I-list-an-item-without-paying-to-mint-it-.

[53] Powering Decentralized Crypto Commerce [Internet]. Wyvern Protocol [Retrieved 2022 Dec 7]. Available from: https://wyvernprotocol.com/.

[54] Explore, Collect, and Sell NFTs [Internet]. OpenSea, the Largest NFT Marketplace [Retrieved 2022 Dec 7]. Available from: https://opensea.io/.

[55] Wilkinson, M.D., Dumontier, M., Aalbersberg, I.J.J., et al., 2016. The fair guiding principles for scientific data management and stewardship. Scientific Data. 3(1).
DOI: https://doi.org/10.1038/sdata.2016.18

BILINGUAL PUBLISHING CO.
Pioneer of Global Academics Since 1984

Artificial Intelligence Advances
https://ojs.bilpublishing.com/index.php/aia

ARTICLE

A Novel Application of Blockchain Technology and Its Features in an Effort to Increase Uptake of Medications for Opioid Use Disorder

Renee Garett[1*] Zeyad Kelani[3] Sean D. Young[2,3]

1. ElevateU, Irvine, California, CA 92697, United States of America
2. Department of Emergency Medicine, University of California, Irvine, California, CA 92697, United States of America
3. University of California Institute for Prediction Technology, Department of Informatics, University of California, Irvine, California, CA 92697, United States of America

ARTICLE INFO

Article history
Received: 11 January 2023
Revised: 28 January 2023
Accepted: 2 February 2023
Published Online: 8 February 2023

Keywords:
Blockchain
Opioid use disorder
Data Security

ABSTRACT

The opioid crisis has impacted the lives of millions of Americans. Digital technology has been applied in both research and clinical practice to mitigate this public health emergency. Blockchain technology has been implemented in healthcare and other industries outside of cryptocurrency, with few studies exploring its utility in dealing with the opioid crisis. This paper explores a novel application of blockchain technology and its features to increase uptake of medications for opioid use disorder.

1. Background

The misuse of an addiction to opioids is a national public health crisis that has a significant impact on society. In 2017, an estimated 1.7 million Americans suffered from opioid use disorder (OUD) and over 47,000 Americans died due to an opioid overdose. Among adult patients who suffered from chronic8 pain, between 21% to 29% who were prescribed opioid medication misused it, and 8% to 12% developed OUD [1]. The economic burden of non-medical opioid use attributed to health care services,

*Corresponding Author:
Renee Garett,
ElevateU, Irvine, California, CA 92697, United States of America;
Email: reneegarettlcsw@gmail.com

DOI: https://doi.org/10.30564/aia.v4i2.5398

premature mortality, criminal justice activities, child and family assistance programs, education programs and lost productivity was estimated to be $188 billion [2]. Effective treatment for opioid misuse is available. Food and Drug Administration approved medications for opioid use disorder (MOUD) are methadone, buprenorphine, and naltrexone. Studies showed that treatment with MOUD resulted in decreased mortality, reduced opioid use, retention in an opioid treatment program (OTP) [3,4], and long-term treatment improved outcomes [4]. Federal regulations mandate that counseling and behavioral therapy accompany methadone treatment and buprenorphine providers have the capacity to recommend counseling to patients.

As digital tools continue to proliferate, researchers and clinical practitioners have adopted them to address public health issues. Applications of technology like mobile health to educate [5], improve access [6], and program maintenance [7] of MOUD have been studied. Papers about the utility of blockchain technology in mitigating the opioid crisis have been proposed for data collection [8], pain management [9], prescription tracking, and pharmaceutical supply chain [10]. This paper highlights features of the blockchain technology as it applies to MOUD.

2. A Primer on Blockchain

Blockchain is an immutable distributed public ledger [11]. It came to prominence as the transformative technology that launched Bitcoin. Blockchain has utility beyond cryptocurrency and has applications in a variety of industries such as finance, e-commerce, governance, and healthcare [12]. Our main inspiration for this paper is the successful use of Blockchain technology in Decentralized Finance (DeFi). DeFi is a decentralized permissionless replication of the current traditional financial infrastructure that provides secure transactions using smart contracts and blockchain verification [13]. Blockchain has potential to decrease both the cost and time for transaction completion compared to the traditional banking system. Moreover, it has potential to lead to the democratization of financial transactions and loosens restrictions on the transnational flow of money [14]. DeFi ensures that all financial transactions are transparent and public while preserving privacy through encrypting user information.

3. Features of Blockchain that are Relevant to MOUD

3.1 Immutable Chain

A key feature of blockchain technology is the immutable block. A block is akin to a digital folder that contains transactions, timestamp of the transactions, and an encrypted code called a hash [11]. Blockchain sequence follows a linked list data structure and hashes connect blocks as each block contains its hash and the hash from the previous block, as shown in Figure 1 [15]. In the case of patients with OUD, patient records could be developed into blocks, and before adding each block to the chain, transactions would need to be verified by the network. Upon verification, new blocks would be secured and stored chronologically at the end of the chain. Once the block is added to the chain, data cannot be altered, even by the data owner, allowing for secure storage and sharing of patient data.

Signature is a key component to ensure the secure communication between blocks. Verification happens by checking the sender's private key and the recipient's public key, as shown in Figure 1. OUD patient records on the blockchain could only be added but not changed. If a MOUD provider wants to change a patient's record, the new information would need to be included in a new block and added to the chain. Prescription drug monitoring programs (PDMP) might benefit from the immutability feature of the blockchain. Each transaction, or data entry, by the prescriber and pharmacist, is verified and secured before they are added to the blockchain as separate blocks which leads to accurate data of the patient's prescription in real-time.

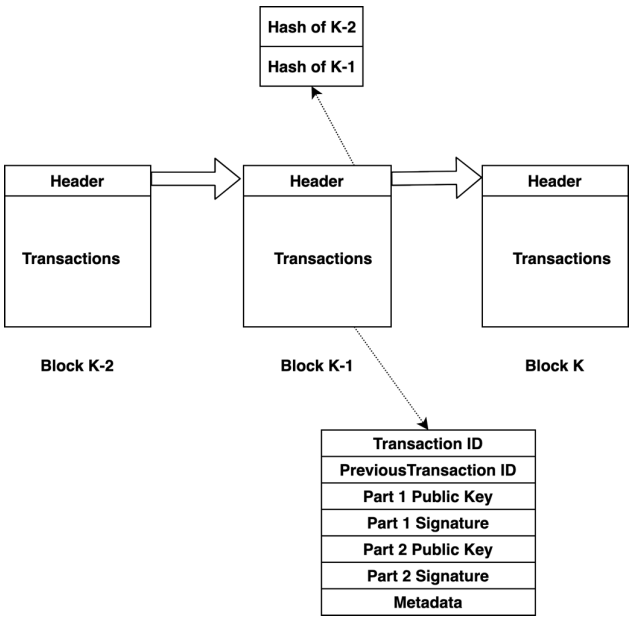

Figure 1. Block structure [15].

Source: B. Rawat D, Chaudhary V, Doku R. Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems. JCP. 2020 Nov 10;1(1): 4-18.

3.2 Decentralized Network and Interoperability

A decentralized network refers to the structure of the blockchain. The blockchain is a distributed ledger technology in that the ledger is distributed to all participating computers (or nodes) in the network and can be accessed by all users on the network. There is no centralized authority that manages the blockchain. Nodes act in concert to verify new transactions on the network and a copy of the updated blockchain is downloaded. As there is no gatekeeper, users access the data through encrypted keys. A public (permissionless) blockchain is open source in that the public has access to all data, and transactions can be recorded and verified by everyone in the network. It has high transparency and accountability. On the other hand, a private (permission) blockchain can only be read by those with required access, typically granted by a single organization. Transparency is reduced in favor of greater access control. A consortium blockchain is a hybrid of public and private blockchain. The network is managed by a group of stakeholders instead of one central organization (private) or the public. Transactions are verified by a group of preapproved entities, and have a high degree of control over who can access the data [16]. With respect to healthcare, a consortium blockchain could afford patients more control of their data and medical records since their data are not tied to a hospital or physician. They have the capacity to grant access to physicians, opioid treatment program (OTP), counselor, pharmacy, and PDMP. Each of these entities then can view or update the patient's medical records without needing approval or authorization. Communication between all involved in the patient's treatment is seamless and issues with disparate medical records dissipate.

3.3 Secure Data Storage

The distributed ledger is the backbone of blockchain technology, where it is composed of a write-only database that is continuously distributed across all network nodes [15]. Nodes execute blocks of programs known as smart contracts. Then, the network uses consensus algorithms to choose final version of the database from all updated nodes.

Patient medical records should be kept private, secure, and confidential, marginalized patients such as those with OUD will discontinue treatment or avoid seeking treatment due to the fear of stigma [17,18] and perceived violations of privacy and confidentiality [17]. Due to potential legal consequences, as well as facing stigma from family and friends, individuals who misuse opioids value privacy and confidentiality. Additionally, individuals who misuse opioids may also experience stigma from their healthcare provider.

Therefore, OUD patients need a very secure method of storing and sharing their data to avoid further stigmatization or negative consequences associated with identifying such patients. One relevant project to keep MOUD patient data is the InterPlanetary File System (IPFS), a peer-to-peer network for storing data and making it available. IPFS splits data files into smaller chunks, encrypts them, and distributes them among different nodes on the network [19]. Files can then be queried back using a content identifier (CID).

3.4 Privacy

Users are provided with a pair of cryptographic keys: public and private. The public key is visible to the public and serves as the user's public identity. The private key is used to initiate and sign transactions and guarantee user authenticity [16]. In blockchain, protected health information (PHI) will be accessible to others if granted permission by the patient. Patients have agency over who can view their data, update it, and for how long entities have access. The patients own their data on blockchain and may grant access to treatment programs, pharmacies, counselors, etc. If a patient transfers to another clinic or stops the program, access to the blockchain can be revoked. Patients may also view a history of who accessed their data.

3.5 Transparency

In dealing with the opioid crisis, data provenance will keep a record of history of MOUD participation, from date of entry into a program, which OTP the patient goes to, type of mediation using, visits with counselors, insurance billing; all of these events will be updated into the blockchain creating a transparent history of the patient's treatment. This is especially useful for populations without regular access to a healthcare provider such as those without insurance, homeless, and individuals recently released from prison.

3.6 Efficiency

One key feature of blockchain technology is its capacity for efficiency. Registration on the blockchain can be used as authentication for enrollment in programs. Treatment facilities may use blockchain identity authentication prior to providing treatment to patients, obviating the need to keep records in-house and minimizing the potential for private information to be stolen due to network attacks. Removal of barriers to use of PDMP would lead to increasing use [20]. PDMP could benefit from blockchain technology in delivering timely data to the network there-

by minimizing the interval between dispensing prescriptions and submission to the PDMP. This enhances patient safety by providing accurate information on a patient's recent prescription.

3.7 New Paradigms: DeSci and DAOs

Like the established DeFi, Decentralized Science (DeSci) is a new way of doing science built on blockchain technology. It is a new paradigm that utilizes smart contracts, blockchain, and other decentralized technologies to address the inefficiency of MOUD scientific research. DeSci is defined as an interoperable system that allows multiple stakeholders in the scientific research community to collaborate without trusting (or knowing) each other [21]. Trustless scientific collaboration in that regard can happen within Decentralized Autonomous Organizations (DAOs), which are collective democratic management organizations using programs running on the blockchain [22]. One application of DAOs in providing MOUD is through facilitating treatment agreement contracts between patients and providers, Medicaid prior authorizations, and expansion of access. Despite availability of MOUD, access and initiation by patients remain low [23]. One of the possible ways to increase MOUD access is to expand training and credentialing of eligible providers [23]. Once qualified practitioners submit all necessary documents (Waiver Notification of Intent, training certificate) to a DAO, smart contract may fast track credentialing process using decentralized governance structure and in-network due diligence.

4. Challenges in Implementation

Like any new technology, blockchain is developing every day and faces several challenges related to MOUD application. The most challenging is scalability; permissionless blockchain allows higher computational resources across the network but limited transaction volume. For example, the bitcoin blockchain allows only 7 transactions per second with almost 10 million users and 200,000 daily submitted transactions [24]. On the other hand, permission-based blockchains allow higher transaction volume with limited computational power based on their limited network base. Another related challenge is the cost of operation, as is still unknown what would be the exact cost of operating blockchain technology in healthcare.

5. Conclusions

Though effective treatment for opioid use disorder exists, barriers challenge uptake for those who would most benefit from treatment. Key features of the blockchain technology presented highlight ways in which innovative technologies may be implemented by healthcare and public health practitioners in addressing limitations.

Author Contribution

All authors contributed to the manuscript conception and design. All authors read and approved the final manuscript.

Conflict of Interest

None of the authors report a conflict of interest.

Funding

This work was supported by the National Center for Complementary and Integrative Health under Grant 4R33AT010606-03 and National Institute on Drug Abuse.

References

[1] National Institute on Drug Abuse. Opioid Overdose Crisis [Internet]. National Institute on Drug Abuse. 2020 [cited 2020 Sep 3]. Available from: https://www.drugabuse.gov/drug-topics/opioids/opioid-overdose-crisis.

[2] Davenport, S., Caverly, M., Weaver, A., 2019. Economic Impact of Non-Medical Opioid Use in the United States [Internet]. Annual Estimates and Projections for 2015 through 2019. Available from: https://www.soa.org/globalassets/assets/files/resources/research-report/2019/econ-impact-non-medical-opioid-use.pdf

[3] Koehl, J.L., Zimmerman, D.E., Bridgeman, P.J., 2019. Medications for management of opioid use disorder. American Journal of Health-system Pharmacy. 76(15), 1097-1103.

[4] Mancher, M., Leshner, A.I., 2019. Medications for opioid use disorder save lives. National Academies Press: Washington (DC).

[5] Cavazos-Rehg, P.A., Krauss, M.J., Sowles, S.J., et al., 2015. "Hey Everyone, I'm Drunk." An Evaluation of Drinking-Related Twitter Chatter. Journal of Studies on Alcohol & Drugs. 76(4), 635-643.

[6] Gustafson, D.H., Landucci, G., McTavish, F., et al., 2016. The effect of bundling medication-assisted treatment for opioid addiction with mHealth: Study protocol for a randomized clinical trial. Trials. 17(1), 592.

[7] Guarino, H., Acosta, M., Marsch, L.A., et al., 2016. A mixed-methods evaluation of the feasibility, acceptability, and preliminary efficacy of a mobile intervention for methadone maintenance clients. Psychology

of Addictive Behaviors. 30(1), 1-11.

[8] Raghavendra, M., 2019. Can Blockchain technologies help tackle the opioid epidemic: A Narrative Review. Pain Medicine. 20(10), 1884-1889.

[9] Chang, M.C., Hsiao, M.Y., Boudier-Revéret, M., 2020. Blockchain Technology: Efficiently managing medical information in the pain management field. Pain Medicine. 21(7), 1512-1513.

[10] Evans, J.D., 2019. Improving the transparency of the pharmaceutical supply chain through the adoption of Quick Response (QR) Code, Internet of Things (IoT), and Blockchain Technology: One result: Ending the opioid crisis. Pittsburgh Journal of Technology Law & Policy. 19, 35-53.

[11] Pilkington, M., 2016. Blockchain Technology: Principles and applications [Internet] [cited 2020 Aug 26]. Available from: https://www.elgaronline.com/view/edcoll/9781784717759/9781784717759.00019.xml.

[12] Underwood, S., 2016. Blockchain beyond bitcoin. Communications of the ACM. 59(11), 15-17.

[13] Schär, F.,2021. Decentralized Finance: On Blockchain—and Smart Contract-Based Financial Markets [Internet] [cited 2022 Mar 10]. Available from: https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets.

[14] Chen, Y., Bellavitis, C., 2020. Blockchain disruption and decentralized finance: The rise of decentralized business models. Journal of Business Venturing Insights. 13, e00151.

[15] Rawat, D.B., Chaudhary, V., Doku, R., 2020. Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. Journal of Cybersecurity and Privacy. 1(1), 4-18.

[16] Dib, O., Brousmiche, K.L., Durand, A., et al., 2018. Consortium blockchains: Overview, applications and challenges. International Journal on Advances in Telecommunications. 11(1 & 2), 51-64.

[17] Tsai, A.C., Kiang, M.V., Barnett, M.L., et al., 2019. Stigma as a fundamental hindrance to the United States opioid overdose crisis response. PLOS Medicine. 16(11), e1002969.

[18] Boekel, L.C., Brouwers, E.P.M., Weeghel, J., et al., 2013. Stigma among health professionals towards patients with substance use disorders and its consequences for healthcare delivery: Systematic review. Drug and Alcohol Dependence. 131(1), 23-35.

[19] IPFS Powers the Distributed Web [Internet] [cited 2022 Mar 10]. Available from: https://ipfs.io/.

[20] Norwood, C.W., Wright, E.R., 2016. Promoting consistent use of prescription drug monitoring programs (PDMP) in outpatient pharmacies: Removing administrative barriers and increasing awareness of Rx drug abuse. Research in Social and Administrative Pharmacy. 12(3), 509-514.

[21] Tenorio-Fornés, Á., Tirador, E.P., Sánchez-Ruiz, A.A., et al., 2021. Decentralizing science: Towards an interoperable open peer review ecosystem using blockchain. Information Processing & Management. 58(6), 102724.

[22] Kaal., Wulf, A., A Decentralized Autonomous Organization (DAO) of DAOs [Internet] [cited 2021 Mar 6]. Available from: https://ssrn.com/abstract=3799320 or http://dx.doi.org/10.2139/ssrn.3799320.

[23] Jones, C.M., Campopiano, M., Baldwin, G., et al., 2015. National and state treatment need and capacity for opioid agonist medication-assisted treatment. American Journal of Public Health. 105(8), e55-e63.

[24] Krawiec, R., Housman, D., White, M., et al., 2016. Opportunities for Health Care. 16.

BILINGUAL
PUBLISHING CO.
Pioneer of Global Academics Since 1984

Tel: +65 65881289
E-mail: contact@bilpublishing.com
Website: ojs.bilpublishing.com

2661-3220
02
9 772661 322227