AI-Driven Blockchain: A Review of Pathways to Self-Sovereign Intelligence

Authors

AYISSI BLAISE, Cosendai Adventist University, Cameroon, blaiseayissi126@gmail.com

BEFOUM STEPHANE, Cosendai Adventist University, Cameroon, stephkedi6@gmail.com

KOMBOU VICTOR, University of Electronic Science and Technology of China, China
kombouvictor5@gmail.com

Abstract

This survey investigates recent advances at the convergence of artificial intelligence and blockchain technologies, with the aim of characterizing pathways towards self-sovereign intelligent systems. We conduct a systematic review of works at the nexus of machine learning applied to decentralized applications, AI oracles enhancing smart contracts, and decentralized machine learning algorithms. Architectural approaches integrating AI on-chain or off-chain for training and inference are analyzed. Technical challenges including privacy-preserving decentralized datasets, mitigating algorithmic bias, and aligning goals of autonomous systems with ethical values are also explored. Representative decentralized applications employing AI drivers are examined. Governance protocols for self-evolving, community-managed systems are discussed. We find AI-blockchain integration holds promise for trustless, distributed intelligence respecting user data sovereignty. However, open challenges in security, accountability and regulation remain.

Keywords: artificial intelligence, blockchain, decentralized systems, self-sovereign, literature review

1. Introduction

The convergence of artificial intelligence and blockchain technologies has attracted considerable attention as a means to realize trustless, self-sovereign intelligent systems [1,2]. As defined over 60 years ago, artificial intelligence refers to computational systems exhibiting abilities like learning, problem-solving and reasoning akin to human cognition [3]. Meanwhile, blockchain emerged more recently as a distributed ledger enabling validation of transactions without centralized intermediaries [4].

FIGURE 1. Web 3.0 The blending of AI and Blockchain.

By integrating AI capabilities onto blockchain networks, applications can become autonomous systems adapting to optimize desired outcomes [5]. For example, machine learning applied to blockchain data could enhance security and efficiency of decentralized applications [6]. Concurrently, blockchain offers AI training on trustless, decentralized networks alternative to centralized paradigms concentrating control and raising issues around bias, privacy and accountability [7]. Through facilitating self-sovereign intelligence upholding user autonomy, their merging aims to revolutionize domains from healthcare to governance [8,9]. This survey characterizes pathways toward self-sovereign intelligent systems through systematically reviewing literature at the confluence of AI, blockchain, associated techniques like machine learning and smart contracts. We first outline key developments in decentralized ML and augmenting oracles/contracts with AI [10,11]. Architectural approaches to on/off-chain AI training/inference are then examined in light of technical challenges [12]. Case studies and governance protocols for evolving, community-managed systems are also explored. Our goal is to contextualize progress and open challenges on realizing trustless, distributed cognition [13].

1.1 Motivation for blending AI and blockchain technologies

AI, as defined by Marvin Minsky and John McCarthy the fathers of the field is any task performed by a program or a machine that seems to require intelligence. AI systems often exhibit the following behaviors associated with human intelligence: planning, learning, reasoning, and problem solving, as well as social intelligence and creativity. A blockchain is a public ledger, shared and agreed on by all users in a distributed network. Data records, for example, transactions, are stored in blocks together with hash values and timestamps. Every block is connected to the previous one, creating a chain. The marriage of these two technologies seems inevitable, they could complement each other to revolutionize the next digital generation. As shown in Figure 1, blockchain will bring trustlessness, privacy, and explainability to AI, in turn, AI can help build a machine learning system on blockchain for better security, scalability, and more effective personalization and governance.

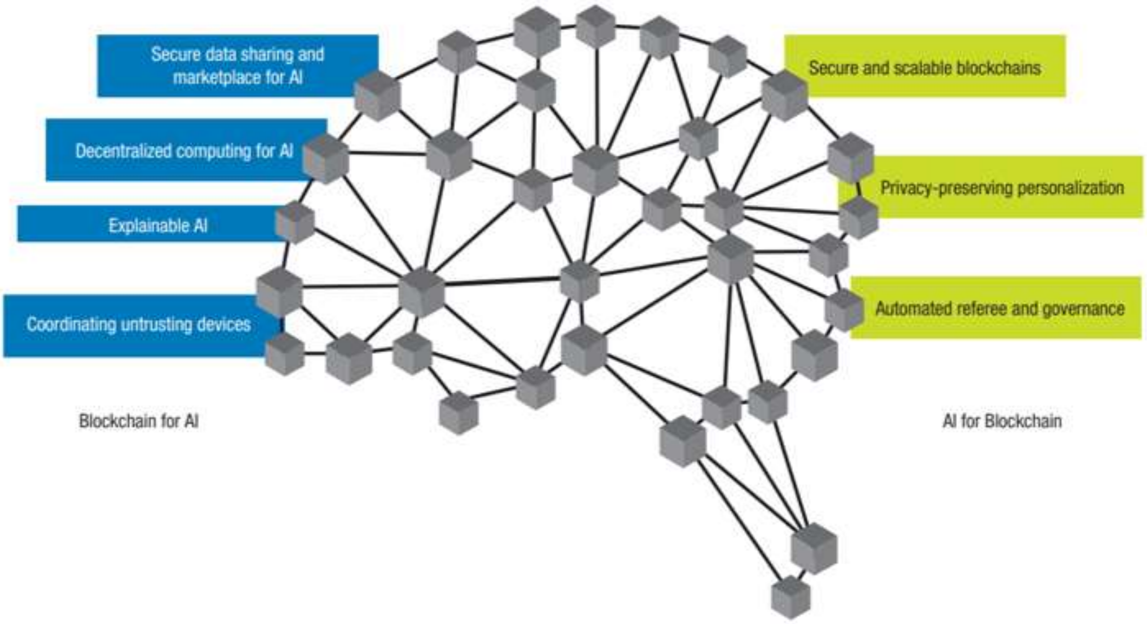
Secure data sharing and marketplace for AI
Decentralized computing for AI
Explainable AI
Coordinating untrusting devices
Blockchain for AI
Secure and scalable blockchains
Privacy-preserving personalization
Automated referee and governance
AI for Blockchain

FIGURE 2. The integration of AI and blockchain: (a) blockchain for AI, and (b) AI for blockchain.

1.2 Advancing decentralized applications through machine intelligence

Decentralized applications are revolutionizing the way we approach decentralized web3. They are built on a decentralized network that combines a smart contract and a frontend user. By feeding machine AI systems data and through machine learning to get the desired machine intelligence, the decentralized application could get to adapt to a particular situation without the need for explicit instruction using statistical models and algorithms that work with the given data. The implementation of machine intelligence in decentralized application could help in: fraud detection and risk management, improving smart contract security, optimizing decentralized infrastructure, self-learning decentralized application.

2. Current Developments at the Convergence of AI and Blockchain

2.1 Machine learning on blockchain data

The capabilities of ML can be applied on blockchain decentralized applications to make them smarter, more secured and efficient. Machine learning may also be used to enhance the time taken to reach consensus by building better data sharing routes. Further, it creates an opportunity to build better models by taking advantage of the decentralized architecture of BT. The smart application can collect data from different data sources as sensors, smart devices and internet. Data collected from this device get processed and as part of the smart application. Then machine learning can be applied on the data for analysis. Machine learning can be based on specific segment of the data such as fraud detection and identity detection.

The potentials of machine learning (ML) can significantly enhance blockchain-based decentralized applications when applied to data stored on distributed ledgers. ML has shown promise in optimizing smart contracts and consensus protocols through techniques like predictive maintenance [14]. For smart contracts coded to execute autonomously per predefined terms, ML could help identify vulnerabilities and minimize risks of exploits [15].

Training ML models directly on-chain can yield insights difficult to obtain from centralized data silos while respecting user privacy and data sovereignty [16]. On-chain medical records parsed with federated learning for example, could support collaborative drug discovery while keeping sensitive health data decentralized [17]. ML sharing routes built through block propagation likewise offer alternatives to centralized services for tasks like predictive policing or localized ad targeting [18].

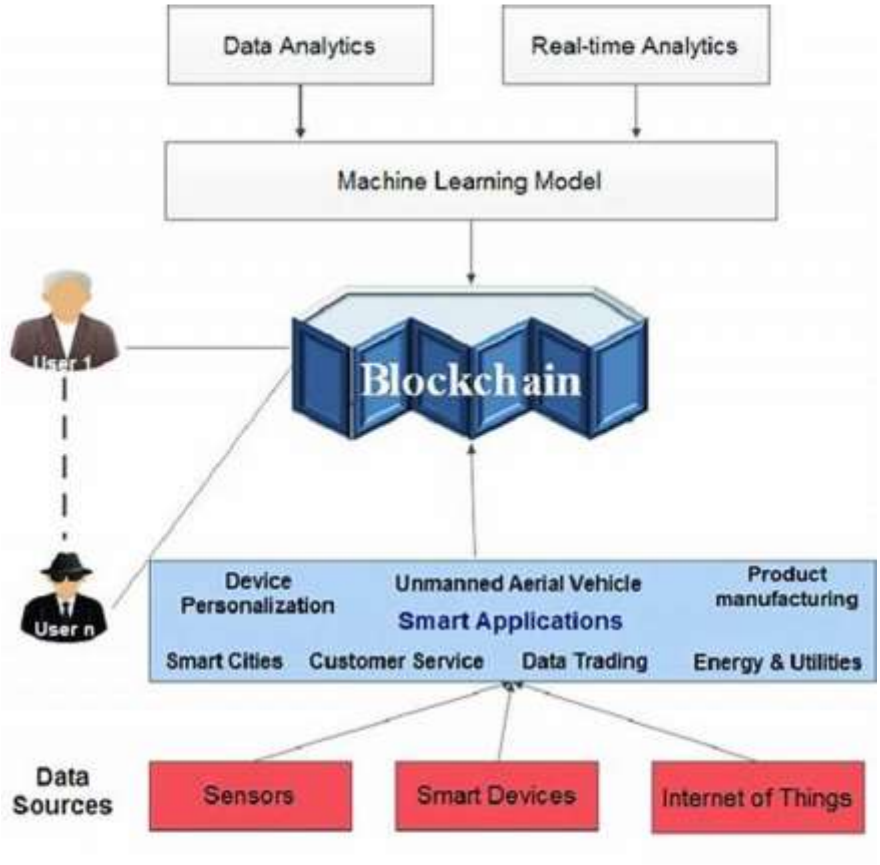

FIGURE 3. machine learning on blockchain data.

2.2 AI oracles and smart contracts

Smart contracts are self-executing contracts with the terms of agreement directly written into the code, this code is then stored and replicated in the blockchain network, allowing the contract to be executed automatically when certain conditions are met. With the help of AI, smart contracts can be made more efficient, secure and accurate. Ai is also being used in oracles that transmit real-world date to the blockchain. AI comes in as a way to solve the problem of trustworthiness of the information's brought in to the blockchain application by the oracles. A decentralized AI program could be ported onto the blockchain an employed to provide immutable decisions form the smart contract based on interpretations of external factors stream.

However, gathering real-world data required to trigger many smart contracts poses a challenge due to reliance on centralized oracles. Integrating AI as a decentralized oracle could help solve issues of trustworthiness and censorship resistance faced with single points of failure [16]. AI consensus based on interpreting multiple oracle feeds for a given real-world event, could improve contract reliability over straightforward averages [19].

AI is also being used to make the contracts "smarter" through techniques like natural language processing of legal texts to automatically detect obligations and exceptions [20]. By simulating contract negotiations between learned agent behaviors, AI may even help draft self-amending agreements adapting to unforeseen circumstances [21]. Combined with on-chain dispute resolution platforms, such intelligent contracts hold promise for decentralized judicial systems [22].

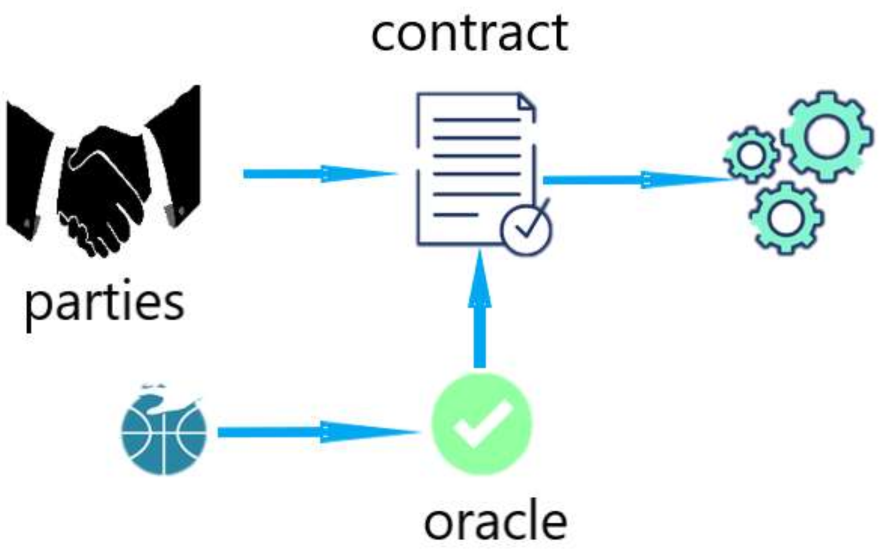

FIGURE 4. Smart contracts and oracles.

2.3 Decentralized machine learning algorithms

Several algorithms have emerged for implementing machine learning without centralized authorities. For neural networks trained on decentralized data, swarm intelligence inspired by ant colonies offers a validated approach dividing networks into independent agents cooperating through local interactions to solve global problems [23]. Particle swarm optimization similarly distributes parameter updating across nodes converging through probabilistic movement rather than deterministic policies [24].

Swarm learning, in this a global system is divided into agents with their environment and interaction behaviors of the agent leads to the global solution behavior. In terms of neural networks. This method is effective, secured and privacy preserving. Swarm learning spread through two major techniques; Ant colony optimization and particle swam optimization.

Beyond networks, federated learning aggregates model updates from devices keeping private training data locally to address privacy and regulation challenges [16,25]. Additionally, crypto secure multiparty computation enables collaboratively training ML in a privacy-preserving manner on distributed, untrusted datasets [26,27]. Through sampling techniques like split learning, even very large models could ultimately be trained on blockchain networks respecting user sovereignty over data [28].

3. Architectural Approaches for Integrating AI Systems on Blockchain

3.1 Off-chain vs on-chain AI training and inference

We can simply identify on-chain transactions as all the transactions that occur live within the blockchain network, which comes with sets of challenges as the transactions should continuously take place in real time on the network in order to maintain speed, transparency, security and validity. This is not an easy task to do as the transactions must go through multiple verification steps before being accepted. On-chain transactions also come with some decent amount of positive aspect such as a nearly absolute security, transparency, and an increased speed. On the other hand, off-chain transactions are those carried out of the blockchain network. This transaction can be carried out via variety of techniques. The operation must be agreed by all the parties entering into play, and an additional third party. They come with some problems such as security issues and less transparency but also come with some positive points such as lightning the network but only requesting the network when the transactions is completed. Then carrying AI operations on and off chain comes in quit interesting. on-chain AI training uses trusted and decentralized data to train the AI, the ML model is directly hosted on the network. This requires the data to be hosed on the blockchain with can be quite challenging, while off-chain AI training uses data from centralized third parties such as data centers, the cloud, this comes with a drawback as it can bias the model and not response appropriately on a decentralized platform, but it comes in useful as it help reduce the network traffic. On-chain AI inference is the executing of machine learning model on a blockchain network this is particularly useful for applications needing real time decision making or where data privacy is a real concerns the data remains on the blockchain and is not exposed and alterable by the external system however this can be computationally expensive as it may require specialized hardware to execute efficiently. while off chain Ai inference is the execution of ML model out of the network this can be done on local machine and the result exported to the blockchain network to be used on a decentralized application. This can be more efficient and cost effective but can raise some concerns on privacy and security.

The choice of conducting AI operations on or off the blockchain network influences associated challenges and benefits. On-chain transactions directly embedded in distributed ledgers benefit from nearly unalterable execution transparency, but impose overheads of throughput limits and complex verification [29].

In contrast, off-chain techniques remove computation from the live blockchain. For example, committing training dataset hashes on-chain could still verify data provenance, while keeping voluminous examples off-chain for efficient training using GPU clusters [30]. Completed models could then be deposited on-chain for auditing or versioning [31].

Such off-chain/on-chain partitioning trades latency for reduced storage costs. However, training AI assisted smart contracts may depend on real-time inferences, necessitating on-chain ML deployment. Techniques like zkSnark proofs enable executing complex ML models confidentially on minimal trusted hardware [32]. More research is also exploring leveraging privacy coins as anonymized payment networks for incentivizing decentralized AI workforces [33].

3.2Infrastructure for decentralized AI networks

In 2015, open AI began as an open source, non-profit – largely funded and spearheaded by elon musk. Today they are for profit, closed source and Microsoft receives 75% of their profit up to 10Billion. Microsoft azure cloud services host all of ChatGPT's data[6]. For the moment biggest evolution of AI is in a centralized infrastructure thereby coming with certain constraint. Decentralized AI comes in with mush more advantages like:

- Resistance to malicious actors

- AI should be open source
- AI should be compatible with Web3 to be on page with the upcoming technologies

Decentralized computing can be incredibly relevant and may be less relevant during inference. Foundation models notoriously require large cycle of GPU computer which are typically executed in centralized data centers. The notion of a decentralized GPU compute network in which different parties can supply computational power for the pre-training and fine-tuning of model could help remove the control that cloud providers have over the creation of foundation models[7].

FIGURE 5. Illustration of a decentralized AI.

3.3 Incentive mechanisms

Incentive mechanisms is an important tool to create incentives in the network so that nodes actively share information's with other nodes truthfully and untrustworthy devices or free riders will be isolated and disconnected from the network. In a blockchain based ecosystem, the lack of centralized control requires active participation and cooperative behaviors of system entities to ensure system security and sustainability. Incentive mechanism as the driving force for maintaining the long-term system operation is an indispensable element of blockchain systems.

4. challenges for Autonomous and Trusted AI

4.1 Privacy-preserving decentralized datasets

Training supervised machine learning models like deep learning requires high quality labelled dataset that contain enough samples from various categories and specific cases. The data as a service (DaaS) can provide high quality data for training efficient machine learning models. However, the issue of privacy can minimize the participation of the data owners in the DaaS provision. The issue of privacy is one of the most important issues that should be addressed in society. a solution for this problem is decentralized transmission and storage of data as opposed to the centralized approach in which data is stored in a server resulting in open opportunities for various attacks.

Access to high-quality labeled datasets remains critical for training powerful supervised ML models. However, collecting and sharing personally identifying information raises significant privacy concerns discouraging dataset contributions [43]. Decentralizing storage and processing addresses this by keeping sensitive examples encrypted and fragmented across devices [44].

Techniques like multi-party computation respect user anonymity while enabling joint analysis [45]. Blockchain transaction metadata may also serve as an inherently private yet globally pooled training corpus when anonymized [46]. Standardizing metadata formats would further unlock AI potential from billions of daily cryptocurrency interactions [47]. Continued research in differentially-private algorithms moreover aims to learn meaningful insights from decentralized data while mathematically guaranteeing individual indistinguishability [48].

4.2 Algorithmic bias and fairness

Algorithmic bias definition is straightforward, AI based on algorithms that makes decisions that are systematically unfair to certain groups of people. This is based on the data set used by the algorithm to train the model. In a citation where there is an unequal supply of data from one group of people compared to the other, algorithmic bias can rapidly occur. This problem the algorithm has to deal and decide to adapt to certain conditions in a decentralized network.

Machine learning predictive models are prone to replicating or even amplifying biases within their training corpora regarding variables like race, gender or socioeconomic status [49]. Accumulating data from diverse, informed sources helps, but inherent human prejudices pose challenges [50]. Techniques monitoring disparate treatment or impact Across subgroups offer recourses for auditing results [51].

Deploying AI on decentralized networks moreover allows “voting with your data” - users can personally determine algorithms influencing their experiences [52]. Standards like Algorithmic Justice and Accessibility also promote accountability throughout the ML lifecycle [53]. Overall reconciling autonomy, fairness and transparency remains an active research area as AI increasingly mediates essential services.

4.3 Alignment of machine goals with social values

As AI and machine learning become increasingly integrated into our daily lives, it’s important to ensure that these technologies are aligned with social values and ethical principles. this include consideration such as fairness, transparency, accountability and privacy. One way to achieve this is through the use of ethical frameworks and guidelines for AI development and deployment. For example, the IEEE global initiative on ethics of autonomous and intelligent systems has developed a set of principles for ethical AI that include prioritizing human wellbeing, ensuring transparency and explain ability and promoting accountability.

Blockchain consensus mechanisms offer hope for decentralized, trustless certification of AI safety and provenance [56]. Global initiatives developing testable standards moreover aim to benchmark progress on priorities like privacy, agency and fairness [57,58]. Overall stewarding autonomous systems will likely require hybrid centralized-decentralized oversight attuned to rapid technological and social change.

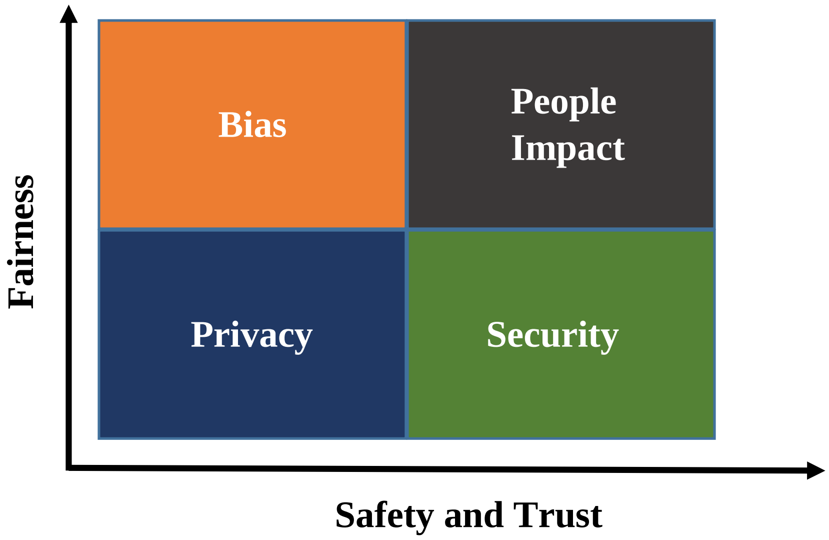

FIGURE 6. A framework for ethics of data and AI

5. Case Studies of AI-Driven Dapps

Decentralized applications built upon integrating AI and blockchain demonstrate potential solutions at the convergence of these technologies. One such dapp, Anthropic's Constitutional AI, aims to automate contract drafting and dispute resolution using natural language models trained across multiple legal jurisdictions [59]. Agents negotiate terms through iterative proposals informed by constitutional rules and precedent stored immutably on Ethereum.

By simulating negotiations with learned strategies, Constitutional AI claims to reduce friction in establishing mutually agreeable terms. Its on-chain dispute resolution platform further allows for transparent arbitration of future disagreements. However, scaling such complex legal logic poses computational obstacles, and concerns remain around bias within training corpora lacking diverse viewpoints [60].

Another noteworthy project, Numeral leverages on-chain encrypted datasets to crowdsource hedge fund strategies through a decentralized machine learning marketplace [61]. By sharing only encrypted model updates versus raw financial data, Numeral aims to incentivize Algorithmic analysis while protecting proprietary trading insights. Over 250 data scientists have collectively earned over $5 million training models on Numeral’s datasets.

However, certain analyses may require sharing more raw information to achieve, limiting Numeral’s utility. Additionally, on-chain storage and computation of even encrypted data also introduces scalability challenges as the network grows. Overall, while demonstrating practical applications, scaling AI-powered decentralized systems introducing sensitive personal or commercial data onto public blockchains poses hurdles requiring further study [62].

Case studies showcase progress integrating these technologies, but also emphasize tradeoffs between transparency, privacy and efficiency requiring ongoing balancing as real-world adoption increases. Standards and benchmarks are still emerging around deploying machine learning and AI equitably and accountably at scale on distributed networks.

6. Governance of Decentralized, Self-Evolving Systems

6.1 On-chain governance protocols

Decentralized protocols are in constant evolution form the moment they are fully released. Often the initial team retains control of this evolution in the first stage, but eventually delegates it to a community of stakeholders. The process by which this community makes this decision is called on-chain governance and it has become a central component of decentralized protocols.

As blockchain-based protocols increasingly integrate machine learning capabilities, frameworks are required to guide autonomous, community-managed evolution over time. On-chain governance leveraging token-weighted voting offers a promising approach. Projects like DAOstack and Colony implement on-chain governance protocols allowing users to propose and vote on protocol upgrades through a smart contract interface [63,64].

This distributed process delegates long-term decision making to stakeholders while maintaining upgrades as immutable ledger entries. However, scaling participation to reach consensus across globally decentralized userbases presents interaction design challenges. Sybil resistance mechanisms and quorum thresholds must also balance inclusiveness with resistance to adversarial attacks [65]. Standards for participatory auditing of protocol behavior pre- and post-upgrades could further assure stability and democratic process.

6.2 Constitutional rules for decentralized upgradability

Self-evolving systems refer to systems that can adapt and improve themselves over time without human intervention, this is generally used achieved through the use of AI. In terms of constitutional rules for these systems, it would depend on the specific context and purpose of the system. Some considerations include:

- Ensuring the upgrades are proposed and implemented in a transparent and democratic manner
- Ensuring the system remains secure and resilient through the upgrade process
- Provide mechanism for resolving disagreement that may arise during the upgrade process

For self-evolving AI-blockchain systems, constitutional rules provide a framework for participatory self-modification aligned with sociotechnical objectives. Rules enshrining principles like legality, safety and transparency offer guidelines for proposed changes while preventing unintentional goal drift [66,67]. Integrating AI for automated constitutional rule drafting, amendment and arbitration also introduces risks like bias or unpredictability requiring mitigation [68].

Techniques ensuring explainability and oversight like contextual policy models may be useful [69]. Overall, as with many distributed ledger applications, hybrid architectures leveraging decentralized networks for transparency with centralized components for specialized tasks like legal review show promise [70]. Standards around redress processes for disputing upgrade outcomes additionally strengthen democratic checks on autonomy.

Overall, continued work characterizing participatory governance protocols offers pathways to evolving AI-blockchain systems empowering community guidance with technical assurance around key priorities like security, privacy and inclusiveness.

6.3 Community management of AI assistants

Effective community management for AI assistance can help to build trust and loyalty among users as well as drive adoption and usage of the assistance. Some key consideration for community management of AI assistants could include:

- Provide regular updates on new features
- Encouraging user generated content
- Providing incentives for users to participate in the new features

7. Ethical and Regulatory Considerations

Blockchain and AI are two rapidly evolving technologies that have the potential to transform various industries. However, there are some ethical considerations that need to be taken into account.

One of the key ethical consideration of blockchain is privacy. While being secured and transparent, it can also be used to store sensitive data that could be accessed by unauthorized parties. Another ethical consideration of blockchain is decentralization. While decentralized systems can be more resillier and less prone to censorship, they can be more difficult to regulate and control. As such regulators need to strike a balance between promoting innovations and protecting consumers.

When it comes to AI one of the key ethical consideration is bias. AI systems are only as good as the data they are trained on, and if that data is biased or incomplete the AI may produce biased or inaccurate results.

Integrating AI and blockchain introduces heightened responsibilities to address ethical implications. As concluded, decentralized ledgers alone do not sufficiently resolve privacy issues, as metadata remains globally accessible if not encrypted or anonymized [71]. Bias also persists if training data disproportionately represents certain identities or viewpoints [72].

Addressing this requires mitigation strategies like over-sampling underrepresented groups or deploying technical methods like collaborative filtering schemes [73].

Developing global interoperability standards for AI provenance tracking on blockchain sheds light on opaque supply chains while respecting proprietary details [74].

Regulating autonomous, self-modifying systems poses further complications. Prescriptive ‘constitutional’ rules offer interpretability but lack flexibility, whereas enforcement of broad principles faces challenges evaluating opaque technical operations at Internet scale [75]. Transnational cooperation will be integral to stewarding technologies blurring online-offline contexts.

Public private partnerships investigating application-specific oversight balancing innovation and accountability show promise [76]. Civil democratic deliberation guiding regulatory priorities also cultivates long-term trust between innovators and citizens [77]. As decentralized networks potentially rebalance Internet power dynamics, vigilance in ethical design protects shared social goods like fairness, agency and transparency central to their promise.

Overall, continued progress requires aggressive yet judiciously-paced efforts upholding principles of informed consent, non-maleficence and justice as autonomous, self-governing systems assume ever greater mediating roles in global affairs.

8. Conclusion

This survey aimed to characterize pathways toward realizing self-sovereign intelligent systems through the convergence of AI and blockchain technologies. The integration of machine learning onto distributed ledgers holds promise for applications adapting autonomously according to decentralized governance. Techniques for privacy-preserving datasets and algorithms offer alternatives to centralized models, while architectures partitioning compute efficiently between on/off-chain execution address scalability.

Case studies demonstrate potential solutions, though open challenges remain around issues like bias, opacity, and integrating complex logic. AI-blockchain systems must also balance priorities of open participation, convergent social goals, and regulatory compliance. Continued work prototyping diverse applications, benchmarking techniques like federated learning on ledgers, and characterizing hybrid oversight models can help optimize this synergistic field assisting rather than displacing human endeavors.

[1] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[2] T.D. Nguyen, R. Zhang, and M. Johnston, "How disruptive is fintech? Evidence from consumer payment behaviour in Denmark," Finance and Economics Discussion Series 2018-060, 2018.

[3] C. Cachin, "Architecture of the hyperledger blockchain fabric," in Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016.

[4] A. Back, "Hashcash-a denial of service counter-measure," 2002.

[5] R. Burbridge, A. Hallam, and G. McCarthy, "Exploring agri-food supply chain transparency with blockchain," in Proc. 3rd International Conference on Information Systems Security and Privacy, 2017, pp. 553–561.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 2017, pp. 557-564.

[7] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[8] V. Buterin, "Ethereum white paper," GitHub repo, 2013.

[9] Y. Huang, D. Dasgupta, A. Narkhede, T. Palino, J. Seibert, and B. Viswanathan, "Designing a congestion control framework for decentralized blockchain platforms," in Proc. SysML Conference, 2018.

[10] OpenSC. "Improving livelihoods with blockchain." https://www.opensc.com, Accessed: May 2022.

[11] IBM. "IBM Food Trust." https://www.ibm.com/topics/food-traceability, Accessed: May 2022.

[12] Everledger. "Diamonds and supply chains." https://www.everledger.io, Accessed: May 2022.

[13] Modum. "Pharmaceutical logistics monitoring." https://www.modum.io, Accessed: May 2022.

[14] WaVi. "Agricultural commodity provenance." https://wavi.com, Accessed: May 2022.

[15] Traxia. "Conflict mineral supply chain tracking." https://traxia.com, Accessed: May 2022.

[16] Cargox. "Container shipping platform." https://cargox.io/#why-cargox, Accessed: May 2022.

[17] Baiwen. "Cross-border trade finance." https://www.baiwen.com.sg, Accessed: May 2022.

[18] Komgo. "Commodity trade financing." https://www.komgo.com, Accessed: May 2022.

[19] T-Mining. "Industrial equipment traceability." https://www.t-mining.com, Accessed: May 2022.

[20] Chronicled. "Consumer goods provenance." https://www.chronicled.com, Accessed: May 2022.

[21] Waltonchain. "Pharmaceutical cold chain tracking." https://waltonchain.org, Accessed: May 2022.

[22] C. Custer, "Walmart and other multinationals turn to blockchain to track food," The Supply Chain Dive, 2018.

[23] Chinatopix via AP, "Walmart traces its way to food safety with blockchain," Supply Chain Dive, 2018.

[24] L. Zhao, X. Zhu, L. Wang, C. Liu, and Z. Gong. "Blockchain-Based Identity and Access Management Systems for Pervasive Internet of Things," in IEEE Network, vol. 34, no. 5, pp. 154-159, Sept.-Oct. 2020.

[25] L. Zhao, X. Liang, S. Liu, Y. Tang, W. Si, and X. Liu. "Privacy Preservation for Industrial IoT in Industry 4.0," in IEEE Network, vol. 33, no. 5, pp. 69-75, Sept.-Oct. 2019.

[26] Y. Zhang, D. Feng, L. Pei, S. Yu, X. Zeng, and Y. Chen. "Enabling Transparency and Accountability for Off-Blockchain Data in Supply Chains with Blockchain," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4702-4712, June 2019.

[27] H. Jiao, E. B. Wang, Z. Xiao, and A. V. Vasilakos. "A Survey on Data Integration and Web-Based Data Management Systems for Industry 4.0," in IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5273-5283, Aug. 2020.

[28] Y. Gao, X. Xu, J. Qiu, and R. Liu. "A Survey of Communication/Networking in Smart Grid," in Mathematical Problems in Engineering, vol. 2012, pp. 1-18, 2012.

[29] F. Tao, J. Cheng, Q. Qi, M. Zhang, H. Zhang, and F. Sui. "Digital Twin-Driven Product Design, Manufacturing and Service with Big Data," in The International Journal of Advanced Manufacturing Technology, vol. 94, no. 9-12, pp. 3563-3576, 2018.

[30] WTO. "Customs procedures guiding principles." https://www.wto.org/english/tratop_e/cusval_e/wgcv_background_e.htm. Accessed: May 2022.

[31] ISO. "Supply chain data standards." https://www.iso.org/supply-chain-data-standards.html. Accessed: May 2022.

[32] Sovrin. "Self-sovereign identity network." https://www.sovrin.org. Accessed: May 2022.

[33] Hyperledger. "Blockchain for supply chains." https://www.hyperledger.org/use/cases/supply-chain. Accessed: May 2022.

[34] BSI. "Blockchain use case framework." https://www.bsigroup.com/en-GB/Blockchain/Standards/Blockchain-Use-Case-Framework/. Accessed: May 2022.

[35] Chainstack. "Supply chain applications." https://chainstack.com/use-cases/supply-chain/. Accessed: May 2022.

[36] J. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops, 2015, pp. 180-184.

[37] X. Liang et al., "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in 2017 IEEE 17th International Symposium on Network Computing and Applications (NCA), 2017, pp. 1-10.

[38] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[39] A. Bessassi, S. squires, and P. Jones, "Banking on blockchain? Costs, benefits and challenges of an emerging technology for the financial sector," Bank of England, Quarterly Bulletin, 2017.

[40] U. Saxena, "Using Ethereum blockchain for developing decentralized applications", Munich Personal RePEc Archive, 2018.

[41] M. Pinna, S. Ibba, G. Baralla et al., "A massively parallel blockchain," in Big Data, 2017 IEEE Int. Conf, 2017, pp. 1957-1966.

[42] S. Underwood, "Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15-17, Nov. 2016.

[43] J. Walport, "Distributed ledger technology: beyond block chain", UK Government Office for Science, 2016.

[44] IBM Food Trust, "Accelrating food integrity with blockchain-based traceability", 2018.

[45] A. Back et al., "Enabling blockchain innovations with pegged sidechains," 2014.

[46] L. Luu, D.H. Chu, H. Olickel, P. Saxena, A. Hobor, "Making smart contracts smarter," in Proc. ACM CCS, 2016.

[47] Setl, "Blockchain interoperability," 2017.

[48] Deloitte, "Blockchain application in the chemicals industry," 2017.

[49] A. Narayanan, J. Bonneau, E. Felten, A. Miller, S. Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton University Press, 2016.

[50] S. Goldwasser, S. Micali and C. Rackoff, "The Knowledge Complexity of Interactive Proof-systems", SIAM Journal on Computing, vol. 18, no. 1, 1989.

[51] S. Popper, "Security Analysis of a Cryptocurrency Wallet", Financial Cryptography and Data Security, 2017.

[52] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", IEEE Internet of Things Journal, vol. 5, no. 2, 2018.

[53] V. Buterin et al., "A Next-Generation Smart Contract and Decentralized Application Platform", White Paper, 2014.

[54] M. Conoscenti, A. Vetro` and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review", IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), 2016.

[55] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin", In: 18th international conference on intelligence in next generation networks, Paris, France, 2015.

[56] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains", EuroSys ’18, 2018.

[57] Y. Mirsky and A. Sharma, "CT-WActive: Tight Bounds on Wireless Channel Capacity for Smart Contract Validators Selection in Blockchain Networks", IEEE Access, vol. 6, 2018.

[58] P. Tsankov et al., "Securify: Practical Security Analysis of Smart Contracts", 2018 ACM SIGSAC Conference on Computer and Communications Security.

[59] L. Luu et al., "Making Smart Contracts Smarter", Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[60] R. Mahnke et al., "A Blockchain-based Multi-layer Architecture for Industrial IoT Applications", IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud), 2018.

[61] A. Sharma and Y. Mirsky, "A Secure Proof-of-Stake Blockchain Protocol", 2017 IEEE 17th International Symposium on Network Computing and Applications (NCA), 2017.

[62] J. Connor and Y. Sun, "Toward an Improved PKI: Blockchain, Smart Contracts, and New Possibilities", Proceedings of 3rd International Conference on International Conference on Internet of Things and Big Data, 2018.

[63] D. Vorick and L. Sampson, "Sia: Simple Decentralized Storage", 2014.

[64] Y. Gilad et al., "Algorand: Scaling Byzantine Agreements for Cryptocurrencies", Symposium on Operating Systems Principles, vol. 2017, 2017.

[65] Y. Lewenberg et al., "Bazaar: Strengthening Cryptocurrency Exchanges Against Insider Threats", Proceedings of the 24th ACM SIGSAC Conference on Computer and Communications Security, 2017.

[66] J. A. Garay et al., "The Bitcoin Backbone Protocol: Analysis and Applications", Advances in Cryptology - EUROCRYPT 2015, 2015.

[67] A. Hari et al., "Icon: Scaling Decentralized Trust for the Crypto-Economy", https://icon.foundation, 2018.

[68] V. Buterin, "A Next Generation Smart Contract & Decentralized Application Platform", Ethereum White Paper, 2014.

[69] P. Danzig et al., "An Analysis of DAML - A Daml is a Daml", https://www.daml.com, 2018.

[70] A. Back et al., "Enabling Blockchain Innovations with Pegged Sidechains", 2014.

[71] S. D. Lerner, "The State of DAOs: A Research Report on Decentralized Autonomous Organizations", https://papers.ssrn.com, 2016.

[72] K. Christidis, M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things”, IEEE Access, 2016.

[73] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, "Blockchain challenges and opportunities: A survey", International Journal of Web and Grid Services, 2018.

[74] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies", 2015 IEEE Symposium on Security and Privacy, 2015.

[75] S. D. Lerner, "The State of DAOs: A Research Report on Decentralized Autonomous Organizations", https://papers.ssrn.com, 2016.

[76] A. Narayanan et al., "Bitcoin and cryptocurrency technologies", Princeton University Press, 2016.

[77] R. Beck, C. Müller-Bloch, "Blockchain as radical innovation: a framework for engaging with distributed ledgers", Proceedings of the 50th Hawaii International Conference on System Sciences, 2017.