ISSN: 2754-6659

Journal of Artificial Intelligence & Cloud Computing

SCIENTIFIC Research and Community

Review Article

Open Access

AI Enabled Security for Ethereum Blockchain Transactions

Ohm Patel

ABSTRACT

This article seeks to discuss the opportunity for security enhancement in the Ethereum blockchain by introducing AI into the Ethereum blockchain ecosystem. Integrating AI with blockchain includes revolutionary approaches to protecting transactions by using techniques like anomaly detection, fraud, and predictive analysis. Hopwood et al. provide a background to blockchain technology with much focus on security in decentralized networks, especially Ethereum. It explores the basics of blockchain security based on cryptographic techniques, consensus algorithms, and the weaknesses of smart contracts. The discussion then turns to opportunities for AI technologies in blockchain security and the example of how the technologies can identify and prevent various activities. The most elaborate part of the paper is the Sequencer Level Security (SLS) protocol, a relatively new one that offers an improved model of transaction security that isolates the undesirable ones. The rollups and Layer 2 solutions involve the presented case of the Zircuit prototype and the implementation of SLS. The paper also discusses how AI may enhance personal data protection in blockchain environments via methods such as decentralized identity and zero-knowledge proofs. Legal and ethical issues are discussed with reference to data protection laws, including GDPR and CPRA, and their effects on the incorporation of AI and blockchain systems. Finally, it envisions the future trends, issues, and opportunities of AI and blockchain security based on a suggested research agenda. Based on this all-around assessment, AI plays a pivotal part in enhancing the security and privacy of Ethereum blocks.

***Corresponding author**

Ohm Patel.

Received: October 10, 2022; **Accepted:** October 14, 2022; **Published:** October 21, 2022

Introduction

Blockchain technology conceals information on a shared network of computers where transaction records are stored and secured. Blockchain, which stemmed from the whitepaper written by an unnamed organization, Satoshi Nakamoto, in 2008, was initially designed for Bitcoin, the first cryptocurrency. This particular technique is said to leverage distributed consensus, whereby every transaction is approved and stored in a nodal network, making it almost impossible to subsequently alter the earlier records without the consent of the other nodes.

To distinguish the various chapters in its development, it is possible to outline several phases in the history of Blockchain. The first phase of widespread distributed ledger technology is Blockchain 1.0, mainly operating in digital monetary systems and payments and whose most famous representative is Bitcoin. Blockchain 2. 0 began including smart contracts with the launch of Ethereum in 2015, as they programmable, self-executing contracts on the Blockchain. This phase shaped a breakthrough: decentralizing applications (dApps) and extending the opportunities to use financial instruments. The existing phase is defined as Blockchain 3. 0, which goes beyond finance, analyzing potential applications in healthcare, supply chain, or governance.

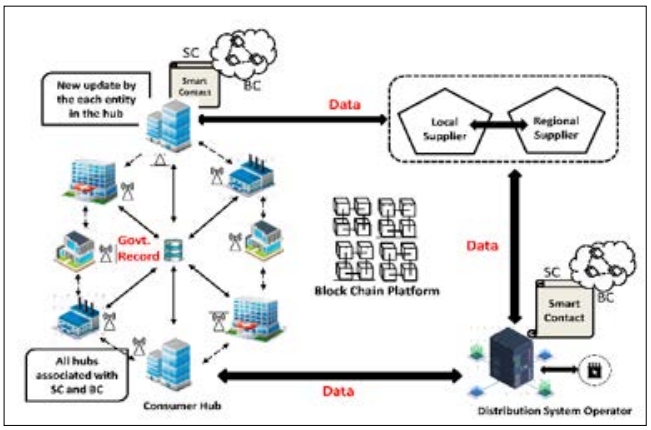

Figure 1: An Ethereum Blockchain-Based Prototype for Data Security of Regulated Electricity Market

Ethereum is the decentralized application platform by design created by Vitalik Buterin. However, unlike Bitcoin, where the basic use is for being a digital currency, Ethereum's main concept revolves around its capacity to execute scripts in an environment that is not centralized, which makes it a nifty tool for a broad range of industries. This is because Ethereum has a Turing complete programming language, Solidity, which enables the development of complex and versatile smart contracts, opening up new blockchain applications.

Blockchain is intrinsically safe due to decentralization but is not impervious to security risks and violations. Some of them are 51% attacks, where a single or a syndicate of attackers takes control of more than half of the network's mining power, something that inevitably enables him or them to manipulate transaction history and double-spend the coins repeatedly. Unrestricted account creation and Sybil attacks where a single person creates multiple nodes to have more say than warranted can also be executed. At the same time, users' private keys are also phished. Innovatively, Ethereum is marketable for the many capabilities it possesses. Nevertheless, it experiences noteworthy security threats mainly because of smart contracts. These self-executing contracts are strong but can have coding errors and flaws and can even be exploited by hackers. Major hacks like the one in the DAO project 2016, in which, due to a loophole in the smart contract involving Ether, $50 million were stolen, confirm the importance of security mechanisms. Due to its structure, Blockchain does not allow any transaction that has taken place to be altered, which only worsens the consequences of a breach.

Artificial Intelligence (AI) involves several complex technologies that allow a system to solve problems and carry out activities that would otherwise require humans' input of intelligence. Machine learning is a part of AI that entails the use of massive data sets with algorithms to be trained to discern certain patterns and make certain predictions. Other forms of AI are NLG, NLP, computer vision, and robotics. Embedding AI with Blockchain has numerous advantages, which are explained as follows. First, AI can improve blockchain security by constantly analyzing suspicious activity, which,h in turn, prevents attacks. Machine learning algorithms can create a model of an immense amount of transaction data to look for patterns that signify fraudulent activities. Secondarily, AI can enhance blockchain networks' performance and distribution through resource management and transaction validation. Finally, AI can extend the enhanced and user-friendly interfaces for Blockchain applications, thus making Blockchain easier to handle.

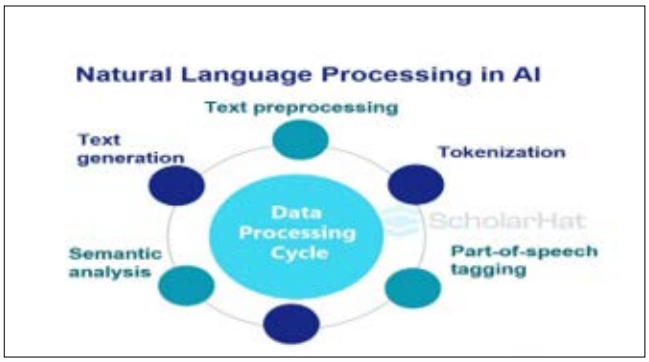

Figure 2: Natural Language Processing in AI

The integration of AI and Blockchain has the potential to improve the performance and security of decentralized systems, especially for platforms like Ethereum, where smart contracts depend heavily on the reliability of the underlying technology. This integration symbolizes implementing a groundbreaking concept to improve the security risks associated with using Blockchain.

Blockchain Security Fundamentals

Understanding Blockchain Security Mechanisms

Blockchain security is mainly based on the principles of cryptology and consensus, which ensures the security and non-stability of the data. Blockchain, the basis of which is cryptography, uses special calculations to protect financial transactions and regulate the issue of new coins. Every block in the blockchain thus includes the previous block's hash, timestamp, and transactions. This hashing process guarantees that if any block were to be altered in any way, the change would have to be reflected on all the following blocks, thus making the process highly complex and all but impossible [1]. Consensus mechanisms are also as important as other components to ensure blockchain security. They help distributed networks reach a consensus on the single source of the truth.

The simplest type of consensus algorithm is the Proof of Work (PoW) utilized by Bitcoin and initially by Ethereum. In PoW, the miners try to solve some numerical problems; the first to decode it earns a reward in the form of currency. This process is energy-consuming but yields solid security because profits are not possible or feasible for the attacker [2]. Another form of consensus that Ethereum is working to transform is Proof of Stake (PoS). PoS chooses validators based on the number of tokens they own and are willing to "stake" or lock up for a period. This mechanism is less energy-consuming than PoW and prevents cartelization by keeping people engaged in contributing. In the same way, PoS also improves security since it is economically unprofitable for the validators to operate dishonestly since they risk losing the tokens they staked [3].

Ethereum Security Model

Ethereum's security layers protect transactions and the network today. Thus, the essence of the Ethereum security model is closely related to the smart contract technology that allows contractual provisions to be embedded directly into a program's source code. These contracts operate on the Ethereum Virtual Machine (EVM), and they promise to execute as coded and cannot be stopped, altered, hacked, or censored [4]. Although smart contracts offer some benefits, they are also the source of many risks. The DAO hack in 2016 is a typical example where a vulnerability of smart contract code enabled a hacker to steal Ether equivalent to $50 million. This incident highlighted that security audits and formal verification methods should be implemented to find and prevent weaknesses before deploying devices. In the same way, Ethereum has put in place measures of security, including the adoption of the Ethereum Improvement Proposal (EIP), where the stakeholders within the Ethereum network submit proposals to the protocol to help solve the problems of security [5].

Role of Decentralization in Security

Decentralization is one of the important properties of blockchain, and it adds exceptional security. In a decentralized network, no central entity regulates the network; therefore, the data is spread out among many nodes. This distribution makes it extremely hard for anyone to conspire with the network as they would require controlling the majority of the nodes to change the history in the blockchain [6]. However, decentralization also brings several challenges. One of the considerable issues that Music Healthcare faces is scalability. Notably, more nodes imply more time to wait to reach a consensus, which might also influence the speed of transaction processing. Due to this, different scaling solutions have been invented to enhance effectiveness yet maintain security, including sharding and off-chain deals [7]. Another challenge is governance. One of the issues that decentralized networks can face is the decision-making process, as the consensus of many participants may prove difficult to achieve and take a long time.

The Ethereum network interfaced with the hostile hard fork after the Dao hack, making way for the Ethereum Classic [8]. Such governance problems pinpoint challenges that need to be effectively

addressed to ensure that the network is fully decentralized and functional while at the same time having a proper mechanism for decision-making. Furthermore, the anonymity of users in blockchain transactions poses some level of concern to regulatory bodies. Decentralization increases privacy and security but also hinders the regulation of prohibited activities like money laundering and fraud. Some of these concerns are currently being tackled by the changing landscapes in laws and regulation settings, where some solutions can be found between security and privacy or between compliance and transparency [9].

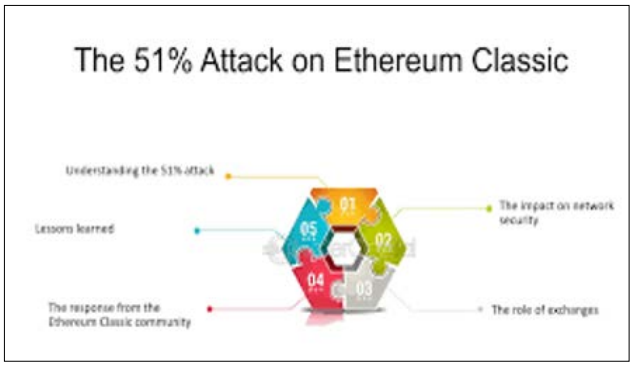

Figure 3: Using Ethereum Classic

Security is a composite area within blockchain science based on cryptographic methods, consensus, and decentralization. Still, it also has many challenges connected with aspects such as scalability, governance, and regulation. The blockchain community never stops adapting and developing new solutions to overcome these challenges and improve the variety, security, and functionality of block hallways adapted and developed like Ethereum.

AI in Enhancing Blockchain Security

Overview of AI Technologies Relevant to Blockchain

Blockchain security is a broad concept that can be augmented with a range of AI technologies. ML, neural networks, and NLP are some of the relevant AI technologies that have been used in this regard. Machine learning is also about giving algorithms some coaching on how to recognize certain trends and make specific decisions on each trend that is recognized based on existing data. These algorithms can examine large volumes of blockchain data to spot trends, make predictions of future occurrences in the blockchain environment, and respond autonomously to security threats. For instance, ML can be used to detect credit card fraud, given the algorithm's capability to detect patterns that are out of the norm [10]. Deep learning is one of the most advanced types of neural networks that perform very well in recognizing patterns in big amounts of data. These networks comprise multiple layers with nodules connected to structures similar to those in the human brain.

In the case of blockchain, it is possible to use neural networks to improve security by identifying the irregularities in the transaction data and calculating the likelihood of security violations [11]. One of the subfields of AI is natural language processing, which deals with the interaction between computers and human language; by applying this, communication in the blockchain ecosystem can be analyzed and understood. NLP can track posts on social media, forums, and other communication channels for the terms associated with blockchain security threats or attacks, which may help take preventive measures [12].

AI Applications in Blockchain Security

There are many ways AI is implemented in blockchain security, including misuse detection, fraud detection, and predictive modeling. Anomaly detection is the threat detection mechanism that helps determine which signals, events, and behaviors are unusual. As such, machine learning techniques can be applied to previous blockchain database results to understand normal system behavior. Any variation from the basic rates or patterns of activity, for instance, a sudden increase in the transaction rate or the frequency of invocation, will ring an alarm bell for a closer look. This makes it easier to mitigate threats before they can advance to the extent that they inflict much harm on the socio-economic aspects of operation. Another important use of AI in blockchain security is fraud prevention. With the help of AI, valuable information from the transaction logs and the users' behavior can be used to detect fraud patterns. For instance, enabled by neural networks, machine learning algorithms can analyze patterns in sequences of transactions and identify things that can be hard for the analyst.

AI can keep learning and developing newer techniques for the newer fraud attacks that may be deployed in the future; thus, incorporating AI is crucial in ensuring the blockchains are secured [13]. Given the existing and past data, predictive analysis employs artificial intelligence to conclude future security threats. Through data trends and patterns, using predictive models results in a glimpse into future attacks and possible preventive actions. For instance, AI patterns information acquired from previous cyber-attacks to estimate which weaknesses are most susceptible to exploitation in the future. This makes it easier for blockchain developers to balance the security measures and reduce risks [14].

Case Studies of AI-Enhanced Security in Blockchain

Actual cases show how AI can improve security within blockchain systems and leave no doubts about whether such strategies have succeeded. A prime example is the application of machine learning at the blockchain analytics company Chainalysis. Chainalysis uses ML algorithms to monitor and analyze transactions on multiple blockchains for money laundering and other malicious intents. Law enforcement agencies have aided through their AI techniques in helping track and recover stolen funds to show the possible uses of AI in improving blockchain security [15]. Another example is IBM's use of AI in their blockchain solutions. IBM leverages AI to identify suspicious activities on blockchain networks and has automated means of handling threats. For instance, their AI systems can examine numerous transactions and mark transactions that they perceive as suspicious to be acted upon by security measures for further network protection. Integrating AI with blockchain has enhanced the performance and dependability of IBM's blockchain systems, thus highlighting tangible applications of AI in enhancing security [16]. However, a few problem areas relating to the use of AI in blockchain security can still be improved. It, therefore, comes with the need for high-quality, labeled data to feed the AI and get the correct results.

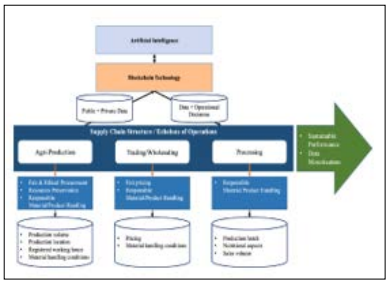

Figure 4: Artificial Intelligence and Blockchain Implementation

In many cases, it is not easy to accumulate enough data for training, especially in the cases of new or unknown threats. There is normally a need to train AI models constantly to enable them to work effectively in the ever-changing security environments. To ensure that AI stays efficient in the long run, it must be maintained and updated frequently, and a certain level of knowledge is required. Blockchain security is further boosted by the use of machine learning, neural networks, and natural language processing, which are some AI technologies. In aspects such as anomaly detection, fraud detection, or analysis for predictability, AI introduces major levels of solidity and dependability in Blockchain networks. Other examples of modern AI-based anti-fraud security provided by vendors, including Chainalysis and IBM, are impressive while stressing the constant development of threats and the need to improve existing security systems.

AI in Enhancing Blockchain Security

Overview of AI Technologies Relevant to Blockchain

Ethereum has exceptional abilities with smart contracts and decentralized applications but has several significant security challenges. These are known to be potential threats, such as 51% attacks and Distributed Denial of Service (DDoS) attacks. A 51% attack takes place when a person or a group takes control of 51% of the hashing power on the network to manipulate the transaction history of the blockchain and double-spend lots of coins. Although such kinds of attacks are feasible, they are rare because they are computationally intensive [2]. DDoS attacks are more common, on the other hand. They execute so many transactions at once to the network that they slow the process and make the transactions costly. For instance, in 2016, the Ethereum network was under multiple DDoS attacks that targeted specific weaknesses in the protocol and eventually caused severe performance decreases and high gas costs [17]. Smart contracts, which are the foundation of Ethereum's distinctive capabilities, also create new risks in the sphere of security. That is why such self-executing contracts, which are attractive in their concept, are vulnerable to failures and hackers' actions. For instance, in June 2016, the DAO was hacked, and $50 million worth of Ether was stolen by attacking the Smart Contract of the DAO. This incident revealed a lack of sufficient security measures in the development stage of a smart contract before deployment; it should undergo code review and analysis and formal verification of models, which would help discover vulnerabilities in the smart contract.

Figure 5: The DAO Attack - Ethereum

AI Solutions for Ethereum Security

Artificial Intelligence provides somewhat effective solutions for improving the safety of transactions within Ethereum. The existing AI algorithms can be used to look out for strange activities in real time, thus enhancing the network's workings regarding potential threats. Machine learning models are capable of processing and analyzing data in relationships regarding potentially fraudulent or malicious activity. AI can improve the anomaly as it creates a baseline of typical operation and provides for straying away from such a pattern. For example, the standard operating pattern regarding transactions can be taught to the operating ML algorithms, and any deviation may hint at a breach in security. It ensures the prevention of the occurrence of these threats to the extent that they can cause extreme loss or harm, as depicted by Chandola, Banerjee, and Kumar [18]. Besides identifying anomalies, the predictive security models can estimate the probable threat using historical data. These models factor in the previous security breaches, and using the previous transaction record, these models estimate the likelihood of which weaknesses will likely be exploited in the future. This enables the developers to fathom the security and incidents that likely affect the application and respond appropriately. For instance, technologist solutions, such as neural networks, can be trained on data from previous intelligent contract attacks to identify similar susceptibilities in other smart contracts [11].

Implementation of AI in Ethereum

AI in Ethereum refers to different instruments and platforms that aim to combine artificial intelligence solutions with the blockchain concept. Some effective frameworks utilized in machine learning include TensorFlow and PyTorch, which can be used to create and train models for identifying and forecasting security threats. Further, other blockchain analytics solutions, such as Chainalysis, employ machine learning to observe blockchain transactions and offer real-time results on the security of the network [15]. Approaches to AI integration into Ethereum security also involve technical dimensions and functional requirements. In principle, AI models require detailed data from the Ethereum blockchain to learn from them properly. This involves using APIs and blockchain explorers to obtain the transactions, as well as, the metadata pertaining to the transactions. At a tactical level, application of AI entails the involvement of blockchain developers and AI experts in the deployments to work on models that should be applicable to the specific type of data characteristic of blockchains.

Some recommended practices while working with AI in Ethereum security are that AI models must be constantly revised and monitored. Regarding blockchain technology and related security threats that are constantly developing, AI models must be updated with new data frequently. Further, using AI with the conventional form of security known as layered security can also enhance security. As described by Murgia, the application of AI could be in threat identification, while conventional techniques are used to manage and respond to incidents [19]. AI presents opportunities to improve the protection of Ethereum transactions against current threats and potential threats in the future. AI, with the help of machine learning algorithms and predictive models, can detect an anomaly and initiate a security action in real time. Integration of AI in Ethereum requires selecting the right tools and frameworks, adherence to best practices in integration, and regular updates due to the constant changes in security threats. This coupling of AI and blockchain is beneficial where there may be an intention to enhance the relocation for more protected and well-established decentralized networks.

Sequencer Level Security (SLS) Protocol

Introduction to SLS Protocol

Sequencer Level Security (SLS) protocol is one of the few attempts to improve security in blockchain transactions, especially in rollups and Layer 2. SLS proposes to solve the problems of current security models of the blockchain by using a mechanism that will allow the determination of potentially malicious transactions and temporarily isolate them before they get into the block. This protocol is based on predictive protection, assuming that the most potent anti-threat measures entail the early identification and eradication of any subversive actions that may be potentially dangerous to the decentralized community.

The made protocol is named SLS, which makes sense as it stands for Second-Level Scrutiny, and it aims to improve the safety of blockchains in that regard. Etherton observed that the modus operandi of regular blockchains, encompassing the rollups of the specifically discussed kind, incorporates all the valid transactions in a block without subsequent critical scrutiny of the contents within. SLS changes this strategy by allowing the sequencer to isolate transactions that share features with fraudulent ones for a certain amount of time. This is proactive in ensuring that some harmful activities, such as double-spend attacks and Sybil attacks, among others, are averted, enhancing the reliability of the blockchain [20].

Mechanics of SLS Protocol

This brings us to the functioning of the summary layer solution protocol inside the rollups and the layer two solutions. Rollups are an example of scaling solutions that aggregate several transactions off-chain and present them on-chain in one transaction, improving and lowering fees. The sequencer is another significant feature of rollups, organizing the transactions' arrangement and constituting blocks. The SLS protocol is interfaced with the sequencer to extend its role by collating the blocks in the Merkle tree as it quarantines suspicious transactions.

Any transaction sent to the rollup mempool is checked by the sequencer that has SLS abilities with the help of heuristics and machine learning based on predefined security indicators. Every other transaction that clears the system as possibly fraudulent is isolated instead of incorporated in a block. This quarantine period allows other network participants or the system to conduct an additional examination and, if necessary, interfere. While the transactions that go through the extra checks are added to the blockchain in the long run, the transactions confirmed as malicious will be forever rejected. The fact that transactions can be quarantined cuts down a variety of attacks. For instance, during a Sybil attack in which an attacker establishes several fake identities to take control of the network, the SLS protocol can identify and isolate such a purchase as risky, consequently ensuring the attacker's plan fails. In the same way, when there is attempted double spending, the flow of work can recognize transactions that intend to spend the same value at different times and need to be stopped to protect the blockchain.

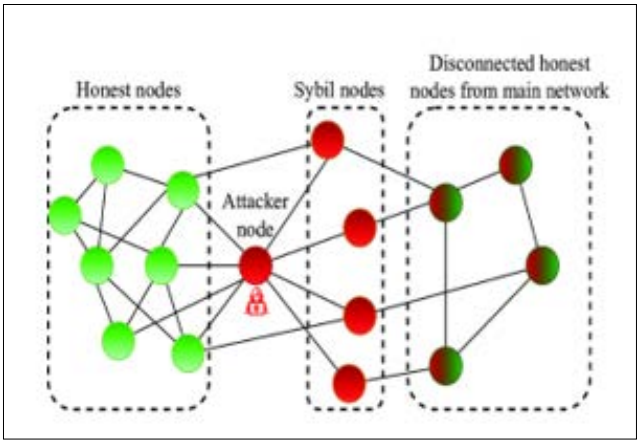

Figure 6: Sybil Attack Scenario in a P2P Network

Case Study: Circuit Prototype

The design of Zircuit also gives a real-world example of how the SLS protocol can be applied and its efficiency. Zircuit is also based on the Ethereum Geth client and Optimistic Rollup stack. The integration of SLS allows for improving the security of rollup transactions. The modernizations were created to investigate the protocol's functionality in isolating damaging transactions and to verify the stability of the whole system.

The sequencer in Zircuit also employs machine learning models, which examine each transaction as soon as it is made. Such models, based on past transaction data and known attack methodologies, can better detect if something is anomalous and, therefore, an attack. A transaction that triggers suspicion is isolated into a quarantine pool, where further investigation is performed. This additional scrutiny checks the transaction against additional criteria to possibly engage human insight in case automated systems are outstanding.

The specificities offered by the case of Zircuit point out several results, as discussed below. First, they showed that the SLS protocol could be easily implemented on top of existing rollup infrastructure with reasonable performance penalties according to the prototype results. According to the proposed quarantine mechanism, the system successfully captured and isolated some of the transactions as fraudulent, and the thorough analysis proved that to be correct. Furthermore, the system was able to counter various forms of attack, as stated by Androulaki et al. with examples being the Sybil attacks and attempts at double-spending, not only affirming the safety of the network but also proving that the protocol would boost blockchain security. From the observed results obtained during the experiment of the Zircuit prototype, it is evident that the SLS protocol presents excellent capability to enhance the functionality and the security of blockchain transactions. Thus, SLS provides an additional layer of protection that would help quarantine any potentially malicious transactions before they affect users' data. Besides, it helps to prevent such risks derived from malicious actions while at the same time strengthening the trust and integrity of decentralized networks, which opens the path to further development in the sphere of blockchain.

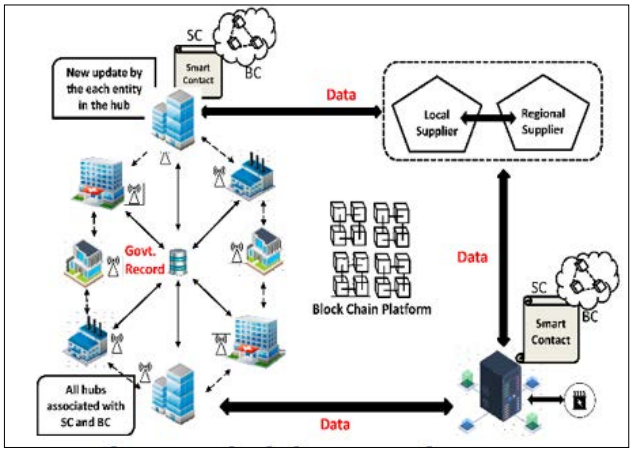

Figure 7: An Ethereum Blockchain-Based Prototype

Sequencer Level Security is a new leveling up in blockchain security, especially in rollups and Layer 2 architecture. With the help of a proactive component that would allow the detection of suspicious transactions in advance and blocking them, the problem of blockchain networks' susceptibility to fraud is solved, and the overall stability of the structures is increased. Depiction of the successful test and outcomes of the Zircuit prototype is a convincing argument for using SLS to protect other future promises of defi and beyond.

Enhancing Personal Data Privacy with AI and Blockchain

Personal Data Privacy Issues

It has become increasingly clear that personal data privacy is among the most valuable in contemporary society. With the ever-growing popularity of data collection and usage in today's digital environment, it is paramount to protect personal information for the benefit of citizens and website users. These may include names, addresses, social security numbers, and biometric data, amongst others, that can be used to identify an individual. Safeguarding this data is crucial to avoid identity theft and fraud [21]. Today's issues related to blockchain privacy are mainly associated with the platform's openness and transparency. These attributes help underlie blockchain's decentralization but are dangerous to privacy. Every transaction executed on public blockchains is recorded and can be accessed by anyone in the said network, potentially exposing sensitive data. Moreover, in the context of personal data in particular, after it is written into the blockchain, it can hardly be modified or deleted, which causes further concerns over the long-term privacy of the information [22].

Blockchain Solutions for Data Privacy

To tackle these challenges, blockchain has grown to include high privacy features, including Decentralized Identity (DID) and Self-Sovereign Identity (SSI). DID is an identity built in the digital world, operated, managed, and owned by the individual, not a specific center. As for this approach, it employs blockchain to ensure individual identity management is secure and private. DID allows users to decide what information has to be disclosed and with whom, significantly minimizing the likelihood of illegitimate access and misuse of data [23]. DID systems usually expand on identity claims by using cryptographic keys but without having to disclose rather personal details to third parties.

Unlike DID, which is regulated to some extent by the SSI organization, SSI goes a step further and allows people to manage their digital personas fully. In what transpires in the SSI framework, identity credentials are gathered, stored, and regulated by individuals with no dependency on a central authority. This self-governance model means that personal data is not disclosed to developers or any third parties without the user's authorization and only when it is mandatory when adopting the applications. Blockchain is used to save credentials and guarantees that can be provided to third parties without disclosing the information used [24].

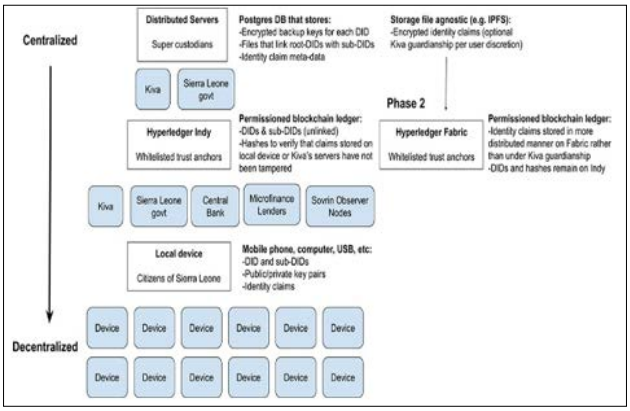

Figure 8: Self-Sovereign Identity in a Globalized World

AI Enhancements to Data Privacy

AI expands data privacy in blockchain through features like ZKP and AI-based privacy preservation techniques. Zero-knowledge proofs (ZKPs) are the concept that one party can convince another party that a statement is true without transmitting any information other than the statement's truthfulness. When applied to blockchain, it is possible to confirm the transactions and the authenticity of the given identity without revealing the underlying data. For example, ZKPs can prove that a user who wants to purchase is over a certain age without announcing the user's birth date. It dramatically increases the level of privacy as only the required data is exposed [25].

Privacy preservation through artificial intelligence is the process by which data is collected, processed, and analyzed while concurrently preventing disclosure of data belonging to individual clients. Differential privacy is one of those techniques, and it relies on adding noise to data sets to obscure particular entries while preserving common data's usefulness. This approach will enable analytics without invading people's privacy while collecting data. AI can also define and change privacy policies as the system constantly monitors or senses the patterns and common threats of aggressive data usage [26]. Combining AI with blockchains presents secure solutions for improving individuals' personal information security. With the help of AI, it is possible to have the most complex privacy-preserving approaches in the blockchain that evolve due to new threats and users' profiles. As Bertino et al. pointed out, this synergy strengthens security and fosters trust since an individual's data is managed with the utmost privacy and integrity.

When introduced collectively, AI and blockchain deliver an effective strategy for regulating personal data privacy. DID & SSI approaches for identity are basic identity frameworks, while AI's like ZKP & pp Algorithm are advanced ways for privacy-preserving. Altogether, these technologies explicitly shift the state of data privacy a step forward and guarantee that particular persons retain proprietorship over their data in the ever-growing digitally inclined world.

Regulatory and Ethical Considerations

Regulatory Landscape

Some of the critical regulations in the blockchain and AI environment include the General Data Protection Regulation (GDPR) in the EU and the California Consumer Privacy Act (CCPA), which has transformed into the California Privacy Rights Act (CPRA). The Regulation (EU) 2016/679, also known as the GDPR, has been in force since 25 May 2018 and is considered one of the hardest in the world. There are stringent duties on institutions that process individuals' data, such as data minimization, user consent, and the right to be forgotten [27]. The enhanced and further expounded law is referred to as the CPRA from the CCPA, where residents of the state of California are availed with further rights concerning their personal information, including the right to be informed regarding the data being collected, to whom this data is being sold or shared and the right to opt-out on the sale of this data [28].

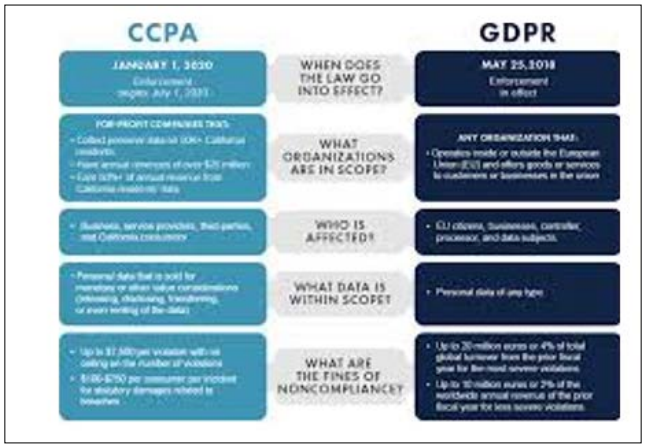

Figure 9: CCPA vs GDPR

These regulations have a notable influence on the integration of blockchain and AI. Firstly, GDPR rights such as data minimization and right to erasure are a problem for blockchain, which has a problem with data modification and deletion due to its permanent ledger. It is also h, hard to design AI algorithms with no bias or use undersized data even when trying to meet privacy regulations [22]. As a result, stakeholders in an organization are under pressure to apply solutions that enhance the use of blockchain and AI while being legal.

Ethical Implications

It is widely agreed that the ethical consideration of AI in the blockchain entails aspects that will make them fair, transparent, and accountable. This is a significant threat since AI algorithms can use and even enhance prejudice and unfairness in data as a source of learning. For instance, prejudiced data will result in prejudice in lending and identity confirmation [29]. Thus, there is a need for proper governance measures that track and prevent bias in AI systems.

There should be a clear definition of the goal: transparency and recency, as the breakthrough of both AI and blockchain technologies should be based on trust. This has to do with explaining to the users and other stakeholders how the system arrived at its decision. Furthermore, through decentralized blockchain records, transactions can be accountable for increasing transparency, but this comes hand in hand with the right to privacy [30]. Regarding ethical challenges, it is also essential to prevent AI technologies from contributing to digital inequalities and excluding marginalized groups. These issues must be actively discussed by the interested parties in order to create fair AI tools.

Compliance Strategies

The project of getting to regulatory compliance status is multifaceted. Best practices should be implemented; there should be more frequent audits, data protection impact assessments, and application privacy by design with regard to AI and Blockchain technologies [31]. DPIAs assist in establishing what risks may occur to the client's privacy and prevent their occurrence to users. Continuous assessments facilitate consistent adherence to the framework and enable the organization to conform to dynamic legal provisions. Utilizing AI for compliance is one of the most effective approaches. AI can complement compliance by executing preventive and detective tasks, including analyzing transactions to identify suspicious money laundering or personal data usage about users' consent [32]. It can also perform analytics on current and past activities, aiming to find contradictions that show a lack of compliance and may prevent it. Moreover, compliance rules can be integrated into smart contracts and work as an automated system that eliminates human interference, improving efficiency.

The legal and ethical framework for AI and blockchain integration should be analyzed to determine the specifics of compliance. For this reason, organizations need to adopt best practices and use AI technologies while at the same time being compliant with the law. This approach not only helps reduce risks but also ensures that the users and stakeholders have confidence in the products developed, especially for the new-generation technologies of the digital society.

Future Directions and Innovations

Trends in Blockchain and AI Security

AI and blockchain are pushing the bar in promoting security to greater heights. A relatively recent variation of intelligent contracts was created to use machine learning algorithms to search for and neutralize potential threats before hackers could utilize them. These smart contracts can evolve with new threats in real-time, thus fortifying the communication blockchain networks [5]. Another new trend is combining AI with blockchain technologies and forming a decentralized AI architecture. These networks are based on the fact that a blockchain cycle distributes AI computations among different nodes, eliminating the dangers of centralization and data leakage. For example, decentralized AI allows private and secure machine learning about an object or situation by allowing the data to remain with the owners. In contrast, others use the data for model training [22].

Challenges and Opportunities

Several technical and operational issues remain unresolved. Another technical problem is the growth of blockchain networks. While AI applications are hugely computationally hungry, applying them with blockchain could worsen the applicative scalability problems. Aspects like sharding and off-chain processing are currently being developed to help with this, but improvement is necessary [7]. From an operational perspective, achieving blockchain fabric and AI synergy between various platforms is still challenging. The existing set-theoretic, ontological, and epistemological differences create problems, leading to fragmentation, which hinders the formulation of coherent system solutions that are compatible with the different environments. Addressing these interoperability problems requires cooperation in developing standard solutions and practices [33]. However, the potential for innovation and enhancement is enormous at the same time. Blockchain security

using AI predictive analysis is another area with the most growth potential. This means that when dealing with security issues, AI can analyze past trends and likely future security threats in order to prevent them. Further, AI can help with resource management within the blockchain, meaning making and passing through, saving maximum resources [14].

Roadmap for Future Research

The following directions should be considered for further research on blockchain in connection with AI. Furthermore, consensus algorithms that solve the computational requirements of AI applications while ensuring the blockchain networks are secure and decentralized are needed. Future studies on consensus models that are partially based on PoW and partly on PoS might hold promising answers [3].

Privacy is another critical research area that can be mentioned in the context of AI. Since AI models depend on data, it is essential to ensure that this data can be utilized while respecting privacy. Methods like federated learning and homomorphic encryption can be used in this regard, where the AI models can be trained on decentralized data without compromising the data [34]. Multidisciplinary approaches and initiatives will be deemed relevant in developing these research streams. The collaboration between universities, companies, and government organizations can lead to setting clear guidelines and procedures on how things should be done. Organizations like the Decentralized AI Alliance (DAIA) and the IEEE Blockchain Initiative are examples of collaborations meant to advance AI and blockchain technologies. That is why the further development of blockchain and integration of the latter with AI will remain promising for improving security and creating new possibilities. This potential can only be understood and achieved by using focused research and developing various collaborations to address technical and operational challenges. Expanding the blockchain and AI communities' understanding of consensus algorithms, privacy preservation, and protocol adoption, the potential for improved scalability, system integration, and security can enable disruptive innovations across the digital environment.

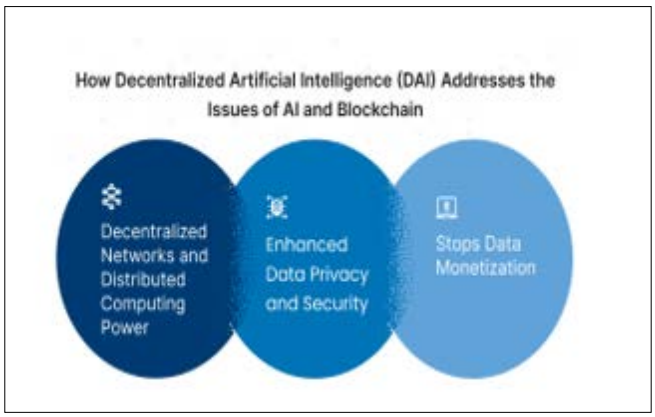

Figure 10: Exploring Decentralized Artificial Intelligence (DAI)

Conclusion

Applying AI with blockchain technology, especially in the Ethereum environment, is the next step in improving transaction security and personal data protection. Making use of AI technologies like machine learning, neural networks, and natural language processing, blockchain networks can quickly gain the ability to analyze the data in real-time and identify the particular contracts that indicate the risk of fraud and other related unlawful activities. These advances are well demonstrated by the implementation of the Sequencer Level Security (SLS) protocol, which is exemplified by the Zircuit prototype. It offers a strong means of isolating and protecting the network from malicious transactions. In addition, privacy-preserving technologies based on artificial intelligence, including zero-knowledge proofs and differential privacy, provide additional protection to personal information stored on the blockchain. In response to the concerns regarding regulation and ethical concerns such as GDPR or the Californian Privacy Rights Act, these technologies are used responsibly and with adherence to the guidelines. Further research and partnership among scholars, industrialists, and other related authorities will be fundamental in addressing the technical and operational obstacles, as well as in enhancing innovation and creating best practices. Integrating AI and blockchain technologies is one of the most promising paradigms for designing improved, more secure, and reliable decentralized systems for learning, innovating, and developing optimal solutions in a wide range of fields [35-37].

References

1. Goldfeder S, Kalodner H, Reisman D, Narayanan A (2016) When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies. Proceedings on Privacy Enhancing Technologies 2017: 1-14.
2. Bonneau J, Miller A, Clark J, Narayanan A, Kroll J A, Felten EW (2015) SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. 2015 IEEE Symposium on Security and Privacy https://ieeexplore.ieee.org/document/7163021.
3. King S, Nadal S (2012) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.
4. Wood G (2014) Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper 151: 1-32.
5. Buterin V (2014) A Next Generation Smart Contract & Decentralized Application Platform. Ethereum White Paper https://ethereum.org/en/whitepaper/.
6. Nakamoto S (2008) Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf.
7. Luu L, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, et al. (2016) A Secure Sharding Protocol for Open Blockchains. ACM CCS https://docs.zilliqa.com/sharding.pdf.
8. (2016) ECC. Ethereum Classic Community 1-19.
9. Zohar A (2015) Bitcoin: Under the Hood. Communications of the ACM https://cacm.acm.org/research/bitcoin/.
10. Jordan MI, Mitchell TM (2015) Machine learning: Trends, perspectives, and prospects. Science 349: 255-260.
11. LeCun Y, Bengio Y, Hinton G (2015) Deep learning. Nature 521: 436-444.
12. Young T, Hazarika D, Poria S, Cambria E (2018) Recent trends in deep learning based natural language processing. IEEE Computational Intelligence Magazine 13: 55-75.
13. Phua C, Lee V, Smith K, Gayler R (2010) A comprehensive survey of data mining-based fraud detection research. arXiv preprint arXiv:1009.6119.
14. Fawcett T, Provost F (2013) Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking. O'Reilly Media, Inc https://www.researchgate.net/publication/256438799_Data_Science_for_Business.
15. Fanusie YJ, Robinson T (2018) Bitcoin laundering: An analysis of illicit flows into digital currency services. Center on Sanctions & Illicit Finance https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf.

16. (2018) IBM Blockchain: The smart contract revolution. IBM Corporation.
17. Decker C, Wattenhofer R (2013) Information propagation in the Bitcoin network. IEEE P2P 2013 Proceedings https://ieeexplore.ieee.org/document/6688704.
18. Chandola V, Banerjee A, Kumar V (2009) Anomaly detection: A survey. ACM Computing Surveys (CSUR) 41: 1-58.
19. Murgia M (2018) AI's role in blockchain security. Financial Times.
20. Dinh TTA, Liu R, Zhang M, Chen G, Ooi BC, et al. (2018) Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering 30: 1366-1385.
21. Acquisti A (2014) The Economics of Privacy. Journal of Economic Literature 54: 442-492.
22. Zyskind G, Nathan O, Pentland AS (2015) Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops https://ieeexplore.ieee.org/document/7163223.
23. Wang F, De Filippi P (2020) Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. Frontiers in Blockchain https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2019.00028/full.
24. Allen C (2016) The Path to Self-Sovereign Identity. Life with Alacrity http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.
25. Ben-Sasson E, Chiesa A, Garman C, Green M, Miers I, et al. (2014) Zerocash: Decentralized Anonymous Payments from Bitcoin. 2014 IEEE Symposium on Security and Privacy https://ieeexplore.ieee.org/document/6956581.
26. Dwork C (2008) Differential Privacy: A Survey of Results. Proceedings of the 5th International Conference on Theory and Applications of Models of Computation.
27. Voigt P, von dem Bussche A (2017) The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing https://www.researchgate.net/publication/321515854_The_EU_General_Data_Protection_Regulation_GDPR_A_Practical_Guide.
28. (2018) California Consumer Privacy Act (CCPA). California Legislative Information https://leginfo.legislature.ca.gov/.
29. Bolukbasi T, Chang KW, Zou JY, Saligrama V, Kalai AT (2016) Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings. Proceedings of the 30th International Conference on Neural Information Processing Systems https://papers.nips.cc/paper_files/paper/2016/hash/a486cd07e4ac3d270571622f4f316ec5-Abstract.html.
30. Kroll JA, Huey J, Barocas S, Felten EW, Reidenberg JR, et al. (2016) Accountable Algorithms. University of Pennsylvania Law Review 165: 633-705.
31. Wright D, De Hert P (2012) Privacy Impact Assessment. Springer Netherlands 3-32.
32. Bertino E, Kundu A, Sura Z (2017) Data Transparency with Blockchain and AI Ethics. Journal of Data and Information Quality (JDIQ) 11: 1-8.
33. (2017) The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. IEEE Standards Association https://standards.ieee.org/industry-connections/ec/autonomous-systems.html.
34. Shokri R, Shmatikov V (2015) Privacy-Preserving Deep Learning. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security 1310-1321.
35. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, et al. (2018) Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference 1-15.
36. Atzei N, Bartoletti M, Cimoli T (2017) A Survey of Attacks on Ethereum Smart Contracts. IACR Cryptol. ePrint Arch https://eprint.iacr.org/2016/1007.pdf.
37. Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S (2016) Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.