

FOUNDATIONS AND ETHICAL FRAMEWORKS OF BLOCKCHAIN TECHNOLOGY

UMEH, ANN C

Department of Parasitology and Entomology
Nnamdi Azikiwe University Awka
ac.umeh@unizik.edu.ng, 08035539047

UMEH, GEORGE-FRANKLIN

Department of Philosophy
Nnamdi Azikiwe University Awka
gi.umeh@unizik.edu.com, 07030275410

Abstract

The rapid evolution of blockchain technology has resulted in over \$14 billion lost in 2021 alone due to privacy breaches and security hacks, with cumulative losses in the tens of billions of dollars. Additionally, the environmental impact of blockchain, particularly from proof-of-work consensus mechanisms, has led to an estimated 114 megatons of CO₂ emissions annually, contributing to global health risks from increased air pollution and carbon emissions. Employing the analytic method, this study examines existing literature and case studies to further understand the multifaceted ethical dimensions of blockchain. Findings reveal that while blockchain technology can revolutionize transparency and decentralization, it coincidentally raises significant ethical problems, such as compromised data privacy, facilitation of illicit activities, and substantial environmental costs due to its high energy consumption. This research recommends the strict formulation of ethically developed guidelines by policymakers and innovators. The constitution serves as a good model, as it is considerably formulated with ethical and financial foresight. Innovators and policymakers should adhere to the legal and ethical frameworks of their respective countries, ensuring ethical governance in blockchain technology.

Introduction

Blockchain technology is a data storage system which has emerged as a transformative innovation, promising decentralization, transparency, and privacy across multiple industries, particularly in finance. However, the technology has also given rise to significant ethical concerns, especially in terms of privacy, security, and environmental sustainability. These issues, while often overshadowed by blockchain's potential, have had profound effects on individuals and society. The concept of Blockchain technology can be traced back to the early 1980s. Cryptographer David Chaum first proposed a Blockchain-like protocol in his 1982 dissertation titled "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Group. This work laid the groundwork for future developments in secure digital transactions.¹ In 1991, researchers Stuart Haber and W. Scott Stornetta introduced a computationally practical solution for time-stamping digital documents to prevent backdating or tampering. Their work was further enhanced in 1992 when they incorporated Merkle trees into the design, allowing multiple document certificates to be collected into one block. This innovation significantly improved the efficiency and security of the system. The true breakthrough for Blockchain technology came in 2008 with the publication of a white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" by an anonymous person or group of people using the pseudonym Satoshi Nakamoto. This paper outlined a decentralized digital currency that relied on a Blockchain to record transactions securely and transparently. A Blockchain network is a peer-to-peer network that does not require a central authority or trusted intermediaries to authenticate or settle the transactions. The first generation of Blockchain network which was coined by Satoshi Nakamoto in his 2008 white paper had the primary application of the Blockchain network use electronic cash or cryptocurrency called Bitcoin according to Alex Tapscott.

In January 2009, Nakamoto as quoted by Sandeep Kumar Panda released the first version of the Bitcoin software, and the first block, known as the “genesis block,” was mined.⁴ Bitcoin’s Blockchain solved the double-spending problem without the need for a trusted central authority. Bitcoin’s Blockchain went live in January 2009, marking the first real-world application of Blockchain technology. The second-generation Blockchain network called Ethereum was introduced in 2015. These events demonstrated the potential of Blockchain to enable secure, transparent, and decentralized digital transactions. Following the success of Bitcoin, Blockchain technology began to attract significant attention and investment. In 2015, Ethereum was launched by Vitalik Buterin and his team, introducing a more versatile Blockchain platform that supported smart contracts. Smart contracts are self-executing contracts with the terms directly written into code, enabling automated and trust-less transactions. This innovation spurred further research and development in the Blockchain space. In recent years, Blockchain technology has continued to evolve, with numerous projects exploring its potential across various industries. According to Alex Tapscott, Blockchain is being used to improve supply chain transparency, enhance data security, and enable new forms of digital identity verification.⁵ Additionally, the rise of non-fungible tokens (NFTs) has created new opportunities for digital art and collectibles. As Blockchain technology matures, it faces challenges related to privacy, scalability, energy consumption, and regulatory compliance.

Core Blockchain Concepts

Blockchain is a revolutionary technology that has fundamentally changed the way we think about data, transactions, and trust in digital systems. At its core, Blockchain is decentralized. Unlike traditional systems, where a central authority controls and manages operations, Blockchain spreads control across multiple participants known as nodes. Each node has a copy of all the data, and they

work together to verify and update the system, making Blockchain resistant to censorship and single points of failure. "Some people refer to these computers as nodes, where some nodes are donating their processing power to solve the math problem associated with creating a block as quoted by Don and Alex Tapscott.⁶

Blockchain organizes data into units called blocks, which are linked together to form a chain. Each block contains a list of transactions, and once it is filled, it is cryptographically linked to the previous block, forming a continuous chain. Each block has a unique identifier, called a hash, which acts like a digital fingerprint. "Transactions cannot be changed or tampered with once recorded on the Blockchain. This immutability feature ensures that once information is recorded, it cannot be tampered with or deleted, enhancing the system's reliability.

Another key feature of Blockchain is its use of a distributed ledger. This means information, like transaction data, is not stored in a single location but across multiple computers. All participants in the Blockchain network maintain a copy of the ledger, ensuring that no single entity holds exclusive control over the data. When a transaction occurs, it is verified by all participants, ensuring that the system remains transparent and secure. For T. Norman Alan, "The system distributes power across a peer-to-peer network with no single point of control. No single party can shut the system down."⁷

To maintain the integrity of the Blockchain, participants must agree on the validity of new transactions through a process called consensus. Different Blockchains use different consensus mechanisms. One common method is Proof of Work (PoW), where participants, called miners, solve complex mathematical problems to validate transactions. While effective, PoW is energy-intensive. An alternative method is Proof of Stake (PoS), where participants are chosen to validate transactions based on how much cryptocurrency they hold. This system is more energy-efficient and

is increasingly being adopted by newer Blockchain networks. Blockchain uses cryptography and what are known as ‘consensus mechanisms’ to validate new information which is added to the ledger and ensure that the ledger is secure from tampering.

Blockchain uses cryptography to secure its data. Cryptography is the science of encoding and decoding information so that only authorized parties can understand it. In Blockchain, every transaction is encrypted, and users are identified by unique cryptographic keys. There are two types of keys: public keys, which can be shared with others to send or receive data, and private keys, which are kept secret and used to sign transactions, proving ownership or authorization. Blockchain also introduces the concept of smart contracts, which are self-executing agreements with the terms of the contract written directly into code. These contracts automatically execute once certain conditions are met, removing the need for intermediaries like banks or legal institutions. For example, in a business deal, payment could be automatically released once the delivery of goods is confirmed, ensuring efficiency and trust.

Various Application of Blockchain Across Industries

Blockchain is making big changes in the financial world. Normally, when people or companies send money across borders, it can take days and involve multiple banks. With Blockchain, these transactions can be completed much faster, often in minutes, and without the need for middlemen like banks. This saves time and money. Blockchain is also used to make trading, lending, and borrowing more secure and transparent. Cryptocurrencies like Bitcoin and Ethereum are examples of how Blockchain is used in finance, but traditional banks are starting to adopt Blockchain technology as well. Another area where Blockchain is having an impact is decentralized finance, or DeFi. This allows people to access financial services like loans and investments directly

through decentralized platforms, without relying on banks. The system is automated through smart contracts, which means transactions happen automatically when certain conditions are met. In healthcare, Blockchain is being used to store and share patient records securely. "In the health care sector, professionals use digitization to manage assets and medical records, keep inventory, and handle ordering and payments for all equipment and pharmaceuticals. Today, hospitals are full of smart devices that oversee these services, but few communicate with one another or take into account the importance of privacy protection and security in direct patient care. Blockchain-enabled gadgets can use emerging applications to link these services. Applications in development include monitoring and disease management for instance, smart pills, wearable devices to track vital signs and provide feedback and improved quality control."⁸. This indicates that Blockchain can enhance communication between smart devices, improve privacy and security, and support applications for monitoring health and managing diseases.

Blockchain technology can help make voting more secure and transparent. By using Blockchain, it is possible to create a system where votes are recorded and counted without the possibility of tampering or fraud. Because the data on a Blockchain cannot be changed, it makes elections more trustworthy. This could help prevent voter fraud and ensure that results are accurate and fair. As stated by Mike Queen, West Virginia Secretary of State Mac Warner's communications director: "the office of the Secretary believes Blockchain does provide a heightened level of security on this type of mobile voting app. We are genuinely hoping that will allow this type of a mobile app to be made available in the future as early perhaps as our general election to military voters."⁹

Technological Breakthrough of the Blockchain

Since the inception of digital transfer of currency, the double spend problem has been a recurring issue. Users were vulnerable to

paying for a commodity twice hence, the double spend problem. Blockchain helped to ameliorate this through the instrumentality of consensus mechanisms which records transactions as they are initiated and declines subsequent and similar transactions from the same source. Clippinger John and David Bollier wrote:

Satoshi leveraged an existing distributed peer to peer network and a bit of clever cryptography to create a consensus mechanism that could solve the Double-Spend problem as well as, if not better than, a trusted third party. On the Bitcoin Blockchain, the network time-stamps the first transaction where the owner spends a particular coin and rejects subsequent spends of the coin, thus eliminating a double spend.¹⁰

One of the most transformative aspects of Blockchain technology is decentralization. In traditional systems, transactions and data are managed by central authorities such as banks, governments, or large corporations. These intermediaries control the flow of information and often charge fees for their services. Blockchain technology eliminates the need for these intermediaries by enabling peer-to-peer transactions. In a decentralized network, each participant, or node, has a copy of the entire Blockchain. Transactions are validated by consensus mechanisms, such as proof of work (PoW) or proof of stake (PoS), rather than by a central authority. This decentralization reduces costs, increases efficiency, and empowers individuals by giving them more control over their transactions. It also enhances security, as there is no single point of failure that can be targeted by hackers.

Transparency and immutability are key features that build trust in Blockchain technology. Every transaction on a Blockchain is recorded in a public ledger that is visible to all participants. This transparency ensures that all transactions can be audited and

verified by anyone, reducing the risk of fraud and corruption. Immutability means that once a transaction is recorded on the Blockchain, it cannot be altered or deleted. This is achieved through cryptographic hashing, where each block contains a unique hash of the previous block. If someone tries to change a block, the hash will no longer match, and the alteration will be immediately apparent. This immutability ensures the integrity of the data and provides a tamper-proof record of all transactions. As stated in the book, *Bitcoin Billionaires: A True Story of Genius, Betrayal and Redemption* by Mezrich Ben:

Transparency is essential because it allows everyone to trust the information contained within the Blockchain network. It also allows members of the network to verify that the transactions that they are making are legitimate. The transparency of a Blockchain network is one of its key strengths. It brings about fairness, trust, and reliability and is one key feature that makes Blockchain technology more efficient than other data storage systems.¹¹

Smart contracts are another significant breakthrough enabled by Blockchain technology. These are self-executing contracts with the terms of the agreement directly written into code. Smart contracts automatically enforce and execute the terms when certain conditions are met, without the need for intermediaries. For example, a smart contract could be used to automatically transfer ownership of a digital asset once payment is received. Smart contracts reduce the need for trust between parties, as the code itself ensures that the terms are fulfilled. They also minimize the risk of human error and fraud, as the execution of the contract is automated. As IBM Technology stated in a video, “I think one of the most successful applications of Blockchain technology is something called smart contracts. Essentially this is code that is running on the Blockchain and whenever certain conditions are met, they are automatically executed.”¹²

Digital identity is another significant breakthrough enabled by Blockchain technology. Traditional identity systems are often centralized and vulnerable to hacking and identity theft. Blockchain can provide secure and verifiable digital identities that are controlled by the individual rather than a central authority. A digital identity on the Blockchain can include various attributes, such as personal information, credentials, and transaction history. This identity can be used for various applications, such as voting, accessing services, and verifying personal information. Blockchain-based digital identities are secure, tamper-proof, and can be easily verified, reducing the risk of identity theft and fraud. For Wright Alan “Blockchain can be used to create secure and tamper-proof digital identities that can be used to verify personal information and other sensitive data. This could become increasingly important as more of our personal information and assets move online.”¹³

Tokenization involves converting rights to an asset into a digital token on the Blockchain. This process can be applied to a wide range of assets, including real estate, art, intellectual property, and even traditional financial instruments. According to G. Peter Kirchschräger, “Tokenization is a fascinating concept in Blockchain technology. It involves converting assets, such as real estate, fine art, or even loyalty points, into digital tokens that are managed on a Blockchain.”¹⁴ For example, a piece of real estate can be tokenized, allowing multiple investors to own a fraction of the property. This increases liquidity and accessibility, as investors can buy and sell tokens on a Blockchain-based marketplace. Tokenization also provides a transparent and immutable record of ownership, reducing the risk of disputes and fraud.

Interoperability refers to the ability of different Blockchain systems and networks to communicate and work together. In the current landscape, there are many different Blockchain platforms, each

with its own protocols and standards. Interoperability enables seamless data and value transfer across these platforms, enhancing efficiency and collaboration. For example, interoperability allows a digital asset on one Blockchain to be transferred to another Blockchain without losing its value or functionality. This capability is crucial for the widespread adoption of Blockchain technology, as it ensures that different systems can work together harmoniously. Interoperability also promotes innovation, as developers can build applications that leverage multiple Blockchain platforms. Interoperability is crucial in many fields, including healthcare, finance, and Blockchain technology, as it allows for more efficient and integrated operations.¹⁵

Ethical Issues in Blockchain Technology

Blockchain technology, although revolutionary, presents several ethical challenges that need to be addressed to ensure its responsible and equitable use. This discussion will cover key ethical issues. One of the primary ethical concerns with Blockchain technology is privacy. Blockchain's transparency, which allows all participants to view transactions, can conflict with individuals' right to privacy. While Blockchain transactions are pseudonymous, they are not entirely anonymous, and sophisticated analysis can sometimes link transactions to real-world identities and this raises concerns about data security and the potential misuse of personal information.¹⁶

While Blockchain's transparency can enhance accountability and traceability, it can also lead to privacy concerns. The inherent transparency of Blockchain means that all transactions are recorded on a public ledger, which can be accessed by anyone. This openness can expose users' transaction histories and personal data, potentially compromising their privacy. Although Blockchain can provide a degree of anonymity, the visibility of transactions means that it is still possible for individuals to be identified through their activity on the network. Thus, while Blockchain technology aims

to protect privacy by allowing users to operate independently of data-harvesting firms, the very transparency that makes Blockchain appealing can also pose risks to individual privacy. This duality emphasizes the need for careful consideration of how Blockchain is implemented and the potential implications for users' privacy rights.

Another ethical issues is due to Blockchain's immutability, which ensures that once data is recorded it cannot be altered, poses ethical dilemmas regarding the right to be forgotten. This right, enshrined in regulations like the General Data Protection Regulation (GDPR) in the European Union, allows individuals to request the deletion of their personal data. However, Blockchain's design makes it challenging to comply with such requests, potentially leading to conflicts with privacy laws.

The decentralized nature of Blockchain technology, while offering benefits such as reduced reliance on central authorities, also presents governance challenges. "Decentralization in Blockchain technology poses several ethical problems primarily due to the potential lack of accountability." Without a central authority, there is often insufficient oversight to prevent or address unethical behavior or misuse of the technology. This lack of oversight complicates regulatory efforts, as traditional regulatory frameworks may not effectively apply to decentralized networks. Additionally, the absence of a central control point can make these systems more vulnerable to exploitation by malicious actors, who may take advantage of the lack of accountability. These challenges highlight the necessity for careful consideration of governance structures and ethical frameworks in the design and implementation of decentralized Blockchain technologies."¹⁷

Furthermore, Blockchain technology, particularly proof-of-work (PoW) consensus mechanisms used by cryptocurrencies like

Bitcoin, has been criticized for its significant environmental impact. The energy consumption required for mining operations is substantial, contributing to carbon emissions and environmental degradation. This raises ethical questions about the sustainability of Blockchain technology and its long-term viability. The environmental impact of Blockchain technology, particularly through its energy consumption, raises significant ethical concerns. The proof of work method requires substantial energy to validate transactions. For Bitcoin, it is estimated that achieving the validity of a proof of work requires around a billion watts. This high energy demand leads to significant global power consumption.

Lastly, while Blockchain has the potential to democratize access to financial services and other resources, there are concerns about accessibility and inequality. The technical complexity and cost associated with participating in Blockchain networks can exclude marginalized communities and individuals with limited resources.¹⁸ This digital divide can exacerbate existing inequalities and limit the benefits of Blockchain technology to a privileged. On one hand, it can contribute to global equality by offering more people access to financial services and markets, which could help overcome global inequality. On the other hand, there is a risk that Blockchain technology may widen the gap between the rich and poor due to unequal access. This could strengthen already established privileged positions, leading to fewer people being directly involved in the economic and social benefits of Blockchain, thus raising ethical concerns regarding justice and human rights.

Utilitarianism and Blockchain

Jeremy Bentham's Utilitarianism is an ethical theory that suggests actions are right if they promote the greatest happiness for the greatest number of people.¹⁹ It is a form of consequentialism, meaning that the moral worth of an action is determined by its outcome or consequence. The main idea is to maximize overall

happiness and minimize suffering. Utilitarianism is a system of thought that holds that the best actions are those that create the most happiness for the greatest number of people, as societies, organizations and individuals consider which laws to enact, which regulations to adopt, and which actions to take.

Privacy concerns in Blockchain technology arise from the transparency of transactions. While the Blockchain ledger is public, the identities behind the transactions are pseudonymous, meaning they are represented by alphanumeric addresses rather than real names. However, with advanced data analysis techniques, it is sometimes possible to link these addresses to real-world identities, potentially exposing users' financial activities and personal information.

On that note, from a utilitarian perspective, the potential harm caused by privacy breaches can be significant. Individuals could face identity theft, financial loss, and a loss of personal security. To maximize overall happiness, Blockchain systems should implement stronger privacy protections. Techniques such as zero-knowledge proofs, which allow transactions to be verified without revealing the underlying data, can help protect user privacy while maintaining the benefits of transparency. By enhancing privacy measures, Blockchain technology can reduce the risk of harm to individuals and increase trust in the system, leading to greater overall happiness.

Security is a cornerstone of Blockchain technology, but it is not without its challenges. The decentralized nature of Blockchain and its reliance on cryptographic techniques provide robust security features. However, vulnerabilities can still exist, particularly in smart contracts and consensus mechanisms. For example, bugs in smart contract code can be exploited by malicious actors, leading to significant financial losses. Utilitarianism would evaluate the

security of Blockchain technology based on its ability to prevent harm and promote trust. Enhancing security measures, such as conducting rigorous code audits, using formal verification methods for smart contracts, and improving consensus algorithms, can reduce the risk of attacks and increase the overall trust in the system. By ensuring that users' assets and data are protected, Blockchain technology can foster a safer and more reliable environment, thereby promoting greater happiness and well-being for all participants.

The environmental impact of Blockchain technology, particularly proof-of-work (PoW) consensus mechanisms, is a major concern. PoW requires significant computational power, leading to high energy consumption and a substantial carbon footprint. This environmental cost can have widespread negative effects, contributing to climate change and resource depletion. From a utilitarian perspective, the environmental harm caused by PoW, Blockchains can outweigh the benefits if not addressed. To maximize overall happiness, the Blockchain community should explore and adopt more sustainable alternatives, such as proof-of-stake (PoS) which is more energy efficient or other energy-efficient consensus mechanisms. PoS, for example, requires validators to hold and stake a certain amount of cryptocurrency as collateral of which they are selected based on the size of the staked amount allowing them to confirm network data, which significantly reduces energy consumption compared to PoW which is energy intensive. Additionally, efforts to use renewable energy sources for mining operations can further mitigate the environmental impact. By transitioning to renewable energy, such as solar, wind, or hydroelectric power, the Blockchain community can significantly reduce the carbon footprint associated with mining activities. This shift not only helps in combating climate change but also promotes the sustainable use of resources. Furthermore, adopting energy-efficient consensus mechanisms like proof of stake (PoS) can complement these efforts, ensuring that Blockchain technology

evolves in an environmentally responsible manner. This approach aligns with the principles of utilitarianism, as it seeks to maximize overall happiness by reducing environmental harm and promoting the well-being of current and future generations.

Deontological Ethics and Blockchain

Deontologism, also known as Deontological Ethics, is a moral theory that focuses on following rules and duties to determine whether an action is right or wrong, rather than looking at the outcomes or consequences of that action. It suggests that some actions are morally obligatory or prohibited based on a set of principles, regardless of what results they produce. The key idea is that people should act according to moral rules or duties, such as do not lie or do not harm others, and these rules should guide their behavior. It was developed by Immanuel Kant, in which he stated the three principles guiding deontologism.²⁰ He stated them as these:

- Act only on that maxim through which you can at the same time will that it should become a universal law.
- Act in such a way that you treat humanity, whether in your own person or in the person of any other, always at the same time as an end and never merely as a means.
- All the maxims that come from your own law-giving should harmonize with a possible realm of ends as with a realm of nature.

Applying Kant's principle of universal law would require that any action involving privacy on the Blockchain should be one that could be universally applied without contradiction. If Blockchain's transparency leads to a violation of personal privacy, it would be wrong to impose this universally. Therefore, according to Kant, Blockchain systems must balance transparency with privacy protections, ensuring that privacy is respected in a way that could apply to everyone. The 'Humanity as an End' principle on the other

hand would suggest that individuals must not be treated merely as means to an end. If Blockchain compromises privacy for transparency or profits, it uses people's personal data as a means, without regard for their dignity and autonomy. Systems should be designed to protect individual privacy and autonomy, recognizing that people have the right to control their personal information. The Kingdom of Ends' principle would that in a society where everyone respects each other's privacy and autonomy, Blockchain technology should include mechanisms that protect privacy by design. This would ensure that individuals' privacy is treated as valuable and respected within a universal system of moral laws.

The principle of universal law suggests that any security framework for Blockchain should be universally applicable without causing harm. If a Blockchain system were designed with the maxim that "It is acceptable for security to be weak or breachable if it benefits a few," it would fail Kant's test of universality. Universalizing such a principle would lead to widespread harm by compromising the system's overall trustworthiness and reliability. From the perspective of treating humanity as an end, a Blockchain system that does not provide adequate security is problematic. It puts users at risk, allowing potential attackers to exploit them. This approach is morally unacceptable because it fails to respect the fundamental rights and safety of individuals, treating them merely as means to an end rather than as valuable in their own right. In an ideal moral community, the design of Blockchain systems would prioritize strong security measures to protect users' data and transactions. Such measures would be developed to ensure that all users are safeguarded, rather than serving the convenience or profit of only a few. This aligns with the principle of the kingdom of ends, where the focus is on creating systems that uphold the dignity and rights of every individual.

With regard to environmental concerns, Kant's Universal Law formulation would challenge the sustainability of energy-intensive Blockchain processes, such as the Proof of Work (PoW) mechanism. A maxim like "it is acceptable for technologies to consume massive amounts of energy, regardless of the environmental impact," would not hold up under universalization principle. If all technologies operated in this way, the resulting environmental degradation would be unsustainable. Kant would argue for Blockchain technologies that adopt more environmentally sustainable practices, ensuring that these practices can be applied universally without negative consequences for the planet. The Humanity as an End principle highlights the fact that Blockchain's environmental harm, particularly its contribution to climate change, fails to respect the well-being of humanity as a whole. Such practices treat the planet and future generations as mere means to an end, which violates their right to a livable environment. In the Kingdom of Ends, where moral agents are committed to respecting the rights and dignity of all, Blockchain technologies would prioritize energy-efficient methods like Proof of Stake (PoS) or other sustainable alternatives. This would ensure that the environmental impact of Blockchain respects the well-being of both current and future generations.

Virtue Ethics and Blockchain

Virtue ethics is a moral theory that focuses on the character and virtues of a person rather than on rules or consequences to determine what is morally right. It emphasizes the importance of developing good character traits, such as honesty, courage, kindness, and fairness, which enable individuals to live ethical and fulfilling lives. It was developed by Aristotle in his book, *Nichomachean Ethics*, he defined virtue as a mean between two extremes, which are vices of excess and deficiency. According to Aristotle, virtue is not merely about following rules or principles but involves practical wisdom (*phronesis*) to determine the right

course of action in various situations. Overall, virtue ethics, as articulated by Aristotle, focuses on the character of the moral agent and the importance of developing virtuous traits to lead a good life.²¹

Applying the concept of virtue ethics to the privacy, security, and environmental problems of Blockchain technology requires a focus on the moral character and virtuous actions of those involved. In this framework, developers and users would strive to cultivate virtues like responsibility, honesty, and care in their approach to Blockchain issues.

In terms of privacy, virtue ethics would encourage developers and users to prioritize honesty and respect for individuals' autonomy. Developers, guided by the virtue of integrity, would design systems that are transparent about data usage while also protecting sensitive information. This means avoiding the temptation to exploit user data for profit or other benefits, instead, they would create Blockchain platforms that respect the privacy of users and are clear about how personal data is handled. On the user side, the virtues of prudence and awareness would lead individuals to make careful decisions about which personal information they share and how they protect their privacy within the Blockchain system.

When it comes to security, the virtues of responsibility and diligence are key. Developers who embody these virtues would work rigorously to build systems that are secure against attacks and breaches, understanding that the safety of users depends on the robustness of their work. They would not take shortcuts or neglect potential security risks but would act with courage and accountability to ensure the highest standards of protection. Similarly, users would practice vigilance and caution by securing their personal information and acting responsibly within the Blockchain system, knowing that their actions impact the collective security of the network.

The environmental impact of Blockchain technology presents an opportunity for the virtues of care and temperance to guide decision-making. Developers and companies working with Blockchain should cultivate a sense of care for the planet and future generations, prioritizing the development of energy-efficient Blockchain systems. Rather than pursuing profit at the cost of the environment, they would be guided by temperance, seeking balance between the benefits of the technology and its environmental costs. This might involve adopting more sustainable consensus mechanisms, like Proof of Stake (PoS), which consumes significantly less energy compared to the more energy-intensive Proof of Work (PoW).

In all cases whether addressing privacy, security, or environmental concerns, virtue ethics emphasizes the importance of acting in ways that reflect a commitment to doing what is morally right. By cultivating virtues such as responsibility, care, honesty, and wisdom, developers and users of Blockchain technology can ensure that it is used ethically, respecting individual rights, promoting safety, and protecting the environment.

Financial Ethics in Cryptocurrencies and Blockchain

Cryptocurrencies, as digital currencies that operate on decentralized platforms, present a unique challenge when it comes to financial ethics. Financial ethics refers to the principles and standards that guide behavior in financial markets, focusing on fairness, transparency, and responsibility. Traditional financial systems are bound by regulations that ensure these ethical principles are followed. However, Melanie Swan wrote, “cryptocurrencies, due to their decentralized nature and lack of central authority, often operate outside the bounds of conventional financial regulations.”²² This raises the question: does financial ethics bind cryptocurrencies?

In theory, cryptocurrencies should adhere to the same ethical principles that apply to traditional financial systems. Imran Bashir stated “Ethical behavior in finance is vital to maintaining trust, protecting users, and ensuring the stability of markets.”²³ For example, transparency is a critical aspect of financial ethics, ensuring that all participants in the financial system can access relevant information and make informed decisions. While Blockchain technology, which underlies most cryptocurrencies, offers transparency in terms of transaction history, it also poses challenges related to anonymity. Mountain Snow opined “the ability to conduct transactions without revealing personal identity can lead to ethical concerns, such as enabling illegal activities like money laundering and fraud.”²⁴

Another ethical issue involves fairness and equitable access. In traditional financial systems, regulations aim to prevent certain individuals or institutions from gaining unfair advantages over others. However, in the world of cryptocurrencies, the lack of oversight has led to concerns about market manipulation. Pedram Abdolvand journal stated “For example, whales also know as individuals or entities who hold large amounts of cryptocurrency can significantly influence the market by making large trades.”²⁵ This raises questions about fairness and whether ordinary users are being treated justly within the system. Mountain Snow (2020:90) wrote, “Additionally, the complex nature of cryptocurrencies and Blockchain technology may exclude individuals who lack technical knowledge, creating a barrier to entry and raising concerns about unequal access to financial opportunities.”

Responsibility is another key pillar of financial ethics. In traditional finance, financial institutions are held accountable for managing people’s money, ensuring that transactions are safe, and compensating users when something goes wrong. However, with cryptocurrencies, users are often responsible for managing their own assets. Just as Mountain Snow stated, “if they lose access to

their private keys (the codes that allow them to control their cryptocurrency), there is no institution to help them recover their funds.” This shifts a significant amount of risk onto the individual, leading to ethical concerns about whether this system is fair and safe for all users.

Cryptocurrencies also challenge ethical standards related to the environmental impact. Au, Sean, and Thomas Power’s article stated, “the mining process for cryptocurrencies like Bitcoin is energy-intensive and contributes significantly to carbon emissions.”²⁶ In an era where sustainability is a growing concern, the ethical implications of cryptocurrency mining have become a topic of debate. John Tally opined, “financial ethics would dictate that industries, including cryptocurrency, have a responsibility to minimize their environmental footprint and promote sustainable practices.”²⁷ However, many cryptocurrencies have yet to fully address these concerns, further complicating the question of how financial ethics applies to them.

Despite these challenges, efforts are being made to align cryptocurrencies with ethical financial standards. Many developers and users in the cryptocurrency community are pushing for self-regulation, promoting transparency, security, and fairness within the industry. Additionally, newer cryptocurrencies are being designed with environmental sustainability in mind, using less energy-intensive methods to verify transactions. As the industry matures, it is likely that more ethical frameworks will emerge, potentially bringing cryptocurrencies closer in line with the financial ethics that govern traditional markets.

Organised Crimes with Blockchain Technology

Organized crime has increasingly leveraged Blockchain technology and cryptocurrencies to conduct illicit activities. The decentralized and pseudonymous nature of Blockchain makes it an attractive tool

for criminals, enabling them to engage in money laundering, fraud, and other illegal activities with reduced risk of detection. Cryptocurrencies, such as Bitcoin and Ethereum, have become popular tools for organized crime groups due to their pseudonymity and decentralized nature. These features allow criminals to conduct transactions without revealing their identities, making it difficult for law enforcement to trace illicit activities. According to Abdolvand Pedram, “fraudulent individuals and organisations exploit cryptocurrencies to conduct money laundering and other crimes related to corruption.”²⁸ The ability to move large sums of money outside the formal banking system reduces the risk of detection by law enforcement and financial institutions.

One of the primary uses of cryptocurrencies by organized crime is money laundering. Criminals use various techniques to obscure the origins of illicit funds, making them appear legitimate. This process often involves multiple transactions across different cryptocurrencies and exchanges. Wood Gavin reports that the rise of cryptocurrencies has revolutionized underground banking, enabling faster and anonymized transactions that facilitate money laundering.²⁹ The use of online gambling platforms and under-regulated cryptocurrency exchanges has further expanded the illicit economy, particularly in regions like Southeast Asia. Blockchain forensics has emerged as a critical tool in combating Blockchain-related crimes. This multidisciplinary field combines data analytics, finance, and law enforcement to investigate and analyze criminal activities on the Blockchain. Techniques such as transaction analysis, address clustering, and taint analysis are used to trace illicit transactions and identify individuals involved in criminal activities. Barski Conrad and Chris Wilmer highlighted that Blockchain forensics can uncover evidence related to crimes such as fraud, money laundering, terrorist financing, and cybercrime.³⁰ These forensic techniques are essential for law enforcement agencies to track and prosecute criminals who use Blockchain technology for illegal purposes.

The convergence of virtual currencies with mainstream finance has led to an increase in transnational organized crime and terrorism financing. Criminals exploit the lack of regulatory oversight and the technical complexity of cryptocurrencies to conduct illicit activities across borders. The European Union has recognized the need for robust regulatory frameworks to address these challenges. According to an article by Welfare Anthony, the European Union has adopted regulations to enhance the traceability of transfers of funds and virtual assets, which are crucial for preventing and investigating money laundering and terrorism financing. These regulatory measures aim to strengthen the capacity of law enforcement agencies to combat the misuse of cryptocurrencies. Despite the efforts to regulate and monitor cryptocurrency transactions, organized crime groups continue to find innovative ways to exploit Blockchain technology. The use of advanced technologies such as artificial intelligence (AI) and deepfake technology has further complicated the landscape of cyber fraud. Criminals use AI to create sophisticated social engineering scams, manipulate individuals' trust, and execute high-success-rate fraud operations. Barski and Chris noted a significant increase in deepfake incidents in the Asia Pacific region, highlighting the growing threat of AI-enabled cybercrime.

Implications of Organized Crimes in Blockchain Technology

The consequences of organized crimes facilitated by Blockchain technology are profound and multifaceted, affecting various aspects of society, economy, and governance. This section explores these consequences.

Organized crimes involving Blockchain technology, such as money laundering, fraud, and ransomware attacks, result in significant financial losses. These crimes undermine the integrity of financial systems and erode public trust in digital currencies and Blockchain technology. According to Welfare Anthony, the use of

cryptocurrencies in money laundering has risen by 30%, with criminal cash being laundered through cryptocurrency exchanges and other platforms. The financial losses from such activities can be staggering, impacting not only individual victims but also financial institutions and the broader economy.

The pseudonymous and decentralized nature of Blockchain technology poses significant challenges for regulatory frameworks. Criminals exploit these features to evade detection and circumvent regulations designed to prevent money laundering, fraud, and other illicit activities. Wood Gavin highlights that the lack of regulatory oversight in the cryptocurrency market allows organized crime groups to operate with relative impunity. This undermines the effectiveness of existing financial regulations and necessitates the development of new regulatory approaches to address the unique challenges posed by Blockchain technology.

Cryptocurrencies have become a tool for financing terrorism due to their ability to facilitate anonymous and cross-border transactions. The European Union has also recognized the threat posed by cryptocurrencies in financing terrorism and has implemented regulations to enhance the traceability of cryptocurrency transactions. Despite these efforts, the decentralized nature of Blockchain technology continues to pose challenges for law enforcement agencies. The use of cryptocurrencies for terrorism financing not only threatens national security but also undermines global efforts to combat terrorism.

The involvement of organized crime in Blockchain technology erodes public trust in digital currencies and Blockchain-based systems. High-profile cases of fraud, money laundering, and other illicit activities create a perception that cryptocurrencies are inherently risky and untrustworthy. This erosion of trust can hinder the adoption of Blockchain technology and limit its potential benefits. Wood Gavin emphasizes the importance of maintaining

public trust in financial systems and the need for robust regulatory frameworks to prevent the misuse of Blockchain technology.

The consequences of organized crimes facilitated by Blockchain technology are far-reaching and complex. From financial losses and regulatory challenges to environmental impact and erosion of public trust, these crimes pose significant threats to society.

Conclusion

With the knowledge of the foundation and ethical framework of blockchain technology, its application runs across various sectors. While blockchain offers benefits like decentralization, transparency and enhanced security, its ethical challenges like privacy concerns, environmental impact and potential use in criminal activities highlights the need for utmost consideration in different aspects. When blockchain technology is used across industries like in cryptocurrencies that are not bound by the same regulations and oversight as traditional systems, ethical principles should still apply. However, advancements in Blockchain forensics and the implementation of robust regulatory frameworks are essential steps in combating crimes relating to blockchain technology. Despite the different challenges posed by use of blockchain technology, it holds a wonderful future in revolutionizing industries when merged with effective ethical governance and sustainable practices. Blockchain technology when used with balanced regulations and ethical oversight offers immense opportunities which ensures responsible and equitable development. As the world of blockchain technology continues to evolve, there will be growing pressure to establish ethical guidelines that protect users and promote trust, ensuring that the benefits of this innovative technology are accessible and fair for all.

ENDNOTES

¹ David Chaum, *Blockchain Investigation* (Amazon Publishing, 2019), 28.

² Alex Tapscott, *Financial Services Revolution: How Blockchain is Transforming Money, Markets, and Banking*, (New York: Global Blockchain Business Council, 2020), 48.

³

⁴ Sandeep Kumar Panda, Ahmed A. Elngar, Valentina Emilia Balas, and Mohammed Kayed, *History and Current Applications*,ed (CRC Press, 2020), 10.

⁵ Tapscott, *Financial Services Revolution*, 45.

⁶ Don and Alex Tapscot, *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World* (New York: Portfolio, 2016), 92.

⁷ T. Norman Alan, *Blockchain: Everything You Need to Know About Blockchain Technology and Cryptocurrency* (New York: Independently Published, 2018), 56.

⁸ Gilder George, *Life After Google: The Fall of Big Data and the Rise of the Blockchain Economy* (Washington, DC: Regnery Gateway, 2018), 87.

⁹ Don and Tapscot, *Blockchain Revolution*, 43.

¹⁰ Clippinger John and David Bollier, eds, *FromBitcoin to Burning Man and Beyond: The Quest for Identity and Autonomy in a Digital Society* (Amherst, MA: ID3, 2014), 39.

¹¹ Mezrich Ben, *Bitcoin Billionaires: A True Story of Genius, Betrayal, and Redemption*. (New York: Flatiron Books, 2019), 46.

¹² IBM Technology, “*Blockchain Explained*.” YouTube video, 2:39. April 3, 2018. <https://youtu.be/QphJEO9ZX6s?si=QFazR4dSdlkdUuN/>

¹³ Wright Alan, *Blockchain Technology Explained* (London: Wiley, 2019), 80.

-
- ¹⁴ Kirchschräger, G. Peter *Ethics of Blockchain Technology*, (Baden-Baden: Nomos Verlagsgesellschaft, 2022), 15.
- ¹⁵ Rouse, Margaret. *Interoperability* (Techopedia Publishing, 2013), 50.
- ¹⁶ Kirchschräger, *Ethics of Blockchain Technology*, 35.
- ¹⁷ Kirchschräger, *Ethics of Blockchain Technology*, 57.
- ¹⁸ Antony Lewis, *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them* (Berkeley, CA: Mango, 2018), 29.
- ¹⁹ Bentham Jeremy, *An Introduction to the Principles of Morals and Legislation* (Britannica publishers, 1789).
- ²⁰ Kant, Immanuel *Groundwork for the Metaphysics of Morals*, trans. And ed. Mary Gregor. (Cambridge University Press, 1998).
- ²¹ Aristotle, *Nicomachean Ethics*, trans. D. Ross. Kitchener, ON: Batoche Books, 1999.
- ²² Melanie Swan, *Cryptocurrencies, Blockchain, and Crypto Assets: Ethics* (London: Independently Published, 2018), 38.
- ²³ Bashir Imran, *WhyBlockchain's Ethical Stakes Are So High* (London: Parity Technologies, 2017), 89.
- ²⁴ Mountain Snow, *The Ethical Implications of Cryptocurrencies* (CRC Press, 2020), 90.
- ²⁵ Pedram Abdolvand, *Cryptocurrencies, Blockchain, and Crypto Assets: Ethics* (Washington, DC: Regnery Gateway, 2018), 77.
- ²⁶ Au, Sean, and Thomas Power. *WhyBlockchain's Ethical Stakes Are So High* (Harvard Business Publishing, 2020), 89.
- ²⁷ Tally John, *The Ethical Implications of Cryptocurrencies* (Mountain Wolf Publishing, 2005), 50.
- ²⁸ Abdolvand, *Cryptocurrencies...*, 90.
- ²⁹ Wood Gavin, *Cryptocurrencies, Corruption, and Organised Crime: Implications of the Growing Use of Cryptocurrencies in Enabling Illicit Finance and Corruption* (Transparency International Publishing, 2012), 20.

³⁰ Barski Conrad and Chris Wilmer, *Organized Crime Is Leveraging Artificial Intelligence and Cryptocurrencies*,” (The Debrief Publishing, 2019), 70.