Navigating Ethical Challenges in Cryptocurrency and Blockchain Technologies

Irenee Dondjio* and Andreas Kazamias*

Platanus Services, Cyprus

Abstract: The emergence of blockchain and cryptocurrency technologies has transformed digital ecosystems, introducing opportunities for innovation and efficiency alongside profound ethical challenges. This paper explores key ethical considerations in cryptocurrency and blockchain, including the decentralization of financial systems, the balance between privacy and transparency, the use of blockchain for surveillance, and the socio-economic impacts on vulnerable populations. The authors delve into the contrasting emphasis on ethical considerations for financial solutions deployed in developed and developing countries. The borderless nature of blockchain and cryptocurrencies enables decentralised international transactions while simultaneously introducing specific challenges regarding the definition of applicable law and other jurisdictional legal matters. Through a combination of literature analysis and illustrative case studies, the authors examine the complex ethical dilemmas that accompany these technologies in combination with their actual and perceived links to crime. The findings aim to provide actionable insights for policymakers, industry leaders, and researchers, fostering the responsible and equitable adoption of blockchain and cryptocurrency technologies.

Keywords: Blockchain, Cryptocurrency, Ethics, Gender, Privacy, Regulation.

1. INTRODUCTION

Blockchain and cryptocurrency are two transformative technologies reshaping the digital economy and societal interactions. Blockchain, first achieved widespread recognition through Bitcoin, has evolved into a versatile tool used in various sectors, including healthcare for secure data sharing, supply chain management for provenance tracking, and identity verification (Kshetri, 2018). Cryptocurrencies extend financial autonomy and inclusion, enabling peer-to-peer transactions outside traditional banking systems (Narayanan *et al*., 2016). These advancements redefine concepts of ownership, trust, and identity, offering innovative solutions for global challenges (Davidson *et al*., 2018). However, these same characteristics decentralization, transparency, and immutability raise significant ethical challenges. Blockchain's inability to modify or delete data can conflict with privacy rights, particularly when sensitive personal information is involved (Zyskind *et al*., 2015). Cryptocurrencies, while promoting financial inclusion, also enable anonymous transactions that can facilitate fraud, money laundering, and other illicit activities (Foley *et al*., 2019). Furthermore, the environmental impact of energy-intensive blockchain processes, such as proof-of-work, questions their alignment with global sustainability goals (De Vries, 2018; Truby, 2018).

Regulatory challenges further exacerbate these ethical issues. Operating across jurisdictions, blockchain and cryptocurrency often fall outside existing legal frameworks, complicating accountability, consumer protection, and international compliance (Catalini & Gans, 2020). The lack of consistent regulatory oversight introduces risks not only for users but also for broader societal systems.

This paper employs a narrative review approach, integrating insights from existing literature with illustrative case studies to explore the ethical challenges posed by blockchain and cryptocurrency technologies. Unlike a systematic literature review, which rigorously catalogues and analyses all relevant research, this narrative review synthesizes key findings to provide a thematic overview of the topic. Case studies are included to contextualize these themes, offering real-world examples of how ethical dilemmas manifest in practice.

The paper is organized as follows: The Literature Review section provides an analysis of existing literature presents blockchain and cryptocurrencies challenges and opportunities. The Methodology section describes the narrative review process and the rationale for incorporating case studies. The Findings section examines major ethical issues such as privacy, regulatory concerns, cybersecurity, and socio-cultural implications. The Discussion section reflects on these findings, emphasizing their implications for policy, practice, and future research. Finally, the Conclusion summarizes the key insights and offers recommendations for promoting ethical and equitable practices in blockchain and cryptocurrency technologies.

Address correspondence to these authors at Platanus Services, PO Box 10, Tsakistra 2869, Cyprus; E-mail: research@platanus.ai, akazamias@platanus.services

E-ISSN: 1929-4409/25

2. LITERATURE REVIEW

The growing popularity of blockchain and cryptocurrency technologies has sparked academic interest in its ethical, legal, and socio-economic ramifications. This section studies literature to summarize these technologies' main challenges and prospects. This review synthesizes academic studies, industry reports, and policy analyses to understand blockchain and cryptocurrency's decentralization, privacy, transparency, socio-economic impacts, and jurisdictional challenges. These topics contextualise the findings and shape this paper's discussions.

2.1. Blockchain Background

Blockchain technology gained recognition in 2008 when author Satoshi Nakamoto released “Bitcoin: A Peer-to-Peer Electronic Cash System” to solve digital currency challenges (Oyelere *et al*. 2019). Nakamoto offered proposals for creating a transparent, safe digital money system without central body or bank administration in the paper. The author introduced the term “block chain” to characterize his concept of a safe and transparent digital money. The term was adopted by other areas, such as the Bitcoin business, which offered consumers security and transparency (Dondjio & Kazamias, 2023).

The concept has now been embraced by sectors including education and healthcare to promote openness and security in information exchange.

2.1.1. Key Blockchain Features

Blockchain technology enables users to track transactions *inside its network*. Users may get crucial transaction data by inspecting the block containing a certain unit of data (Dondjio & Kazamias, 2023). Each block in the system is closely connected to neighbo-uring blocks, enabling efficient information tracking.

The technology promotes transparency by enabling members to watch and manage transactions. Blockchain enables participants to broadcast transactions when inputting them into the system (Dondjio & Kazamias, 2023).

It also lets them reject suspicious transactions. This technology enhances openness and security by allowing stakeholders to choose data types inside a network. Changing information inside a network requires authorization from other members, ensuring security.

The immutability of the blockchain ensures transactions inside a unit. Users cannot remove or amend verified transactions in the system using this technology (Themistocleous, 2018).

The decentralised nature of blockchain technology prevents system failure and fosters stakeholder confidence. In contrast to centralized data management, blockchain involves all stakeholders in transaction approval or rejection (Dondjio & Kazamias, 2023). Thus, in a decentralised ledger, all nodes serve as trust bearers.

2.2. Key Ethical Challenges in Blockchain and Cryptocurrency

2.2.1. Decentralization of Financial Systems

Decentralised global financial solutions are a significant innovation that utilise the operation, decision-making, and control mechanisms of decentralised blockchain protocols and make use of smart contracts, which enable the execution of predefined instructions (Schär, 2021). Decentralised Finance (DeFi) breaks the traditional model, where financial solutions are backed and managed by centralised financial institutions (Beinke *et al*., 2024), such as banks, which are supervised by central regulatory authorities, such as domestic and regional central banks, in accordance with domestic or regional regulations. Decentralised financial systems make it easier to offer financial products to populations that do not have access to traditional providers (e.g., banks) (Stone, 2022). This is the core principle of Financial Inclusion (World Bank). Decentralisation is a potential catalyst for large-scale digital financial inclusion offerings; however, without regulatory supervision, it is open to ethical concerns such as a lack of proper data privacy, weak creditworthiness assessments, and inadequate identification of individuals’ identities (Hartmann & Hasan, 2023). Other concerns, such as market manipulation and fraud, could also arise (U.S. DOJ, 2024). All of these, if not managed properly, enable criminal activity, facilitating money laundering and terrorism (U.S. Treasury, 2023).

A further concern stemming from decentralised finance offerings is the level of technical and subject matter literacy an individual needs to understand the products’ operation, advantages, and risks, to avoid exposure to criminal intrusion (U.S. CFTC, 2024).

Decentralised Finance in general is mostly outside the total control local regulation (Salami, 2023).

Consequently, it becomes difficult to enforce local laws, which include, among others, taxation and consumer rights. The borderless, decentralised nature of blockchain enables DeFi products to transcend multiple jurisdictions. Regulation, information sharing, data gathering, law enforcement agencies' know-how, and legal enforcement would need to be consistently aligned across countries (U.S. CFTC, 2024). Efforts from intergovernmental organisations like the Financial Action Task Force (FATF) aim to extend Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) measures to cryptocurrency activity (FATF, 2022).

There are cases where cryptocurrency solutions, including DeFi, operate under a specific country's regulatory framework. Technically, these offerings are localised and quasi-decentralised, as they require a regulated intermediary. For instance, in Switzerland, they fall under the Swiss Financial Market Supervisory Authority (FINMA), and in Singapore, under the Monetary Authority of Singapore (MAS). Striking a balance between regulation, privacy, and innovation is critical for the success of such regulatory frameworks (Zehnder, 2024). For example, Project Guardian, run by MAS in collaboration with the financial industry, aims to achieve industry-wide frameworks and standards for financial asset tokenisation (Project Guardian, 2024).

Assuming all users and stakeholders of decentralised solutions work in unison, such solutions make it possible to substitute effectively the trust-enabling role of a central regulatory authority with the transparency of blockchain activity, delivering network-wide trust (Wei *et al*., 2024). This, in turn, acts as a vehicle for reducing corruption and increasing accountability (Makarov and Schoar, 2022). However, the potential negative aspects of such operational models include ethical issues created by exposing sensitive personal data through pseudo-anonymity and analysis of transactional-level patterns (Wei *et al*., 2024).

In a centralised financial system, trust relies on the internal procedures and controls of commercial and regulatory institutions and their trusted partners. In decentralised models, trust is founded on the decentralised nature of the blockchain, transparency of activity, and the use of specialised technical solutions such as smart contracts (Ethereum, 2024). Having a set of pre-defined instructions specified programmatically in a smart contract raises concerns about hacking attacks and software bugs, either of which could be driven by criminal activity (Rosaire & Jules, 2022).

The technological solutions used to offer decentralised finance can be energy intensive. The Proof-of-Work method used by Bitcoin (Nakamoto, 2008) consumes enormous amounts of electricity (EIA, 2024). The carbon dioxide emissions (carbon emissions) from Bitcoin's use in 2020-2021 were equivalent to that of 14 million homes' electricity use for one year (United Nations University, 2023). Comparing Bitcoin's carbon emissions to those of a traditional centralised global network like Visa, as of July 2021, Bitcoin's emissions were 64.18 MtCO2, while Visa's were 62,400 MtCO2 (Kohli *et al*., 2022). However, Visa's emission figure includes the network and the running of its corporate offices, whereas Bitcoin's figure includes only the network's technology. For the purposes of comparing carbon emissions figures, Bitcoin does not have comparable functionality to Visa. For instance, it lacks the ability to cancel a previously approved transaction and recover funds through a dispute resolution process (Gabuthy, 2023). Such functionality, available in Visa, delivers large-scale consumer and business confidence. A fundamental characteristic of the Bitcoin protocol is immutability; once a transaction is recorded on the blockchain, it cannot be altered. While there are some dispute resolution technology offerings, such as Rootstock (Lerner, 2019), that use the Bitcoin blockchain through a sidechain, these offerings serve as platforms on which dispute resolution solutions can be built.

A comparable analysis of the two networks' carbon emissions should examine the transaction volumes and computational costs of each network at the individual transaction level. As of July 2021, Bitcoin performed 0.4 million daily transactions, compared to Visa's 500 million. An individual Bitcoin transaction's carbon emissions were 844.13 KgCO2, whereas a Visa transaction emitted 0.00045 KgCO2 (Kohli *et al*., 2022; Digiconomist).

2.2.2. Balancing Privacy and Transparency

The fundamental factors that typically define blockchain solutions are,

Distributed

Blockchain functions within a decentralised network of nodes with a protocol that ensures no single entity has control over the system. Each network node

typically has access to and maintains a copy of the ledger. There are some nodes, like light nodes, which maintain a portion of the node and rely on the functionality of full nodes (Dondjio & Themistocleous, 2021). The distributed functionality ensures there is redundancy within the network (Tabatabaei *et al*., 2023).

Immutable

Once data is recorded and validated on the blockchain, it cannot be altered or deleted without consensus from the network. This characteristic makes blockchain tamper-evident and tamper-resistant (Yaga *et al*., 2019).

Transparent

All transactions recorded on a blockchain are visible to all participants within the network. This fosters trust and accountability, as any participant can verify the transactions and other data residing on the blockchain (Nakamoto, 2008).

Anonymous or Pseudo-Anonymous

Transactions are recorded on the blockchain using cryptographic addresses. No personal identification information is required. This functionality incorporates private-public key cryptography (Haro-Olmo *et al*., 2020). However, when the owner of a specific address is known, it is possible to link all transactions performed using that address and possibly other addresses to that owner, pseudo-anonymously (Wylde *et al*., 2022).

Secure

Blockchain employs cryptographic techniques like hashing and digital signatures to achieve authentication and data integrity. The use of network consensus mechanisms further strengthens the network's integrity and protects it from fraudulent and malicious activity (Leng *et al*., 2022).

Network Consensus

Blockchain consensus mechanisms are essential for ensuring ledger integrity, reliability, and the proper operation of decentralisation. Proof-of-Work and Proof-of-Stake are two such mechanisms used to validate transactions and secure trust (Yakubu, 2024).

Faster than Traditional Settlements

Blockchain settlements are achieved without intermediaries, unlike traditional banking systems that often require multiple intermediaries and settlement processing windows, delaying the end-to-end settlement process. By using decentralised architecture and peer-to-peer transaction protocols, blockchain enables settlement within minutes or seconds rather than several days, as in traditional banking networks (Chiu & Koeppl, 2019).

From blockchain users' perspective, areas of concern can arise from transparency, the degree of data privacy, the absence of end-to-end regulation for each transaction, and how and where influence can be applied to the solution by third parties (Bansod & Ragha, 2022).

Having transactions, balances, and wallet addresses open for viewing creates challenges in maintaining data privacy. By analysing transaction amounts and patterns against wallet addresses, it becomes possible to compromise data privacy (Wylde *et al*., 2022). For instance, in a transaction involving two parties (buyer and seller), one party could be a malicious actor who records the wallet address of the other. The malicious actor could trace all transactions involving the same wallet address, thereby creating a profile of activity. This makes the anonymous wallet address a pseudo-anonymous address for the malicious actor. However, removing transparency from blockchain entirely would create opportunities for criminal activity, as illicit transactions would be difficult to trace (Hooper, 2023).

Data privacy regulations like the European Union's General Data Protection Regulation (GDPR) 2016 (European Council) may be breached. For example, Article 17 of GDPR, titled the "right to erasure ('right to be forgotten')", grants individuals the right to have personal data deleted if it is no longer required for its original purpose. This provision creates challenges for blockchain, particularly for deleting data stored as part of, say, an inactive smart contract. Blockchain's immutable nature makes it difficult to comply with such provisions (Belen-Saglam *et al*., 2023).

Private blockchains, or hybrid models combining private and public blockchains, may provide solutions to protect data privacy in specific cases. Unlike public blockchains (e.g., Ethereum), where anyone can join the network without permission (permissionless) and where all data is visible to everyone, private blockchains operate under centralised governance (Bayan & Banach, 2023). Access to private blockchains is controlled, so only authorised parties can participate,

access data, or validate transactions (Vashishth *et al*., 2023). Personal data privacy can be safeguarded by storing sensitive information on a private blockchain or by placing less sensitive information on a public blockchain (Ncube *et al*., 2020).

Mixers (or tumblers) and zero-knowledge proof (ZKP) methods can balance transparency and data privacy. However, such methods may attract criminal activity as they obscure information like cryptocurrency ownership or identifiable links between transactions (Cointelegraph, 2023).

2.3. Socio-Economic Impacts on Vulnerable Populations

Making alternative financial products accessible to populations in underdeveloped countries, as offered through decentralised finance (DeFi), can create new socio-economic opportunities. These innovations encourage the creation of small and micro businesses, enable non-cash daily trading, and promote job creation, wealth generation, and financial independence (Mhlanga, 2023; Adegbite, 2024).

Alternative financial products also empower women in underdeveloped countries to achieve financial independence (Bahri, 2020), thereby reducing or eliminating gender-based financial inequality (Forbes, 2021). Lack of access to traditional banking products hinders women's economic development in underdeveloped regions, including sub-Saharan Africa (FAO & ITC, 2023). Cultural and societal norms, low literacy levels of data networks, and lack of access to savings or assets exacerbate this challenge (WB & WTO, 2020). Blockchain-based financial products enable women to participate anonymously, bypassing the need for male family members to verify their identity. Furthermore, the lower transaction costs and decentralised nature of blockchain eliminate the need for physical bank visits, which may conflict with local customs or laws (Bahri, 2020).

The limited financial capacity of vulnerable populations, particularly in rural areas, poses challenges for the adoption of cryptocurrency solutions. According to the Global Multidimensional Poverty Index 2024, 83.2% of the world's poor live in sub-Saharan Africa and South Asia. These populations often lack access to technology and education, leaving them vulnerable to exploitation, hacking, and other criminal activities (Alkire *et al*., 2024).

2.4. Legal and Jurisdictional Concerns

Resolving cross-border disputes is one of the most critical challenges in blockchain systems due to their decentralised and borderless design. These systems lack a central authority or intermediary to mediate conflicts or enforce agreements, complicating accountability across jurisdictions (De Filippi & Wright, 2018). While blockchain technology has brought significant advancements in security, transparency, and efficiency for digital asset ownership and transfer frameworks (Dondjio & Kazamias, 2023), it has also introduced complexities that expose gaps in existing regulatory structures.

One significant concern is the rise of privacy coins, cryptocurrencies designed to enhance user anonymity by obscuring transaction details, such as sender, recipient, and transaction amount. Unlike cryptocurrencies, like Bitcoin, where transaction details are recorded on a public ledger, privacy coins like Monero and Zcash use advanced cryptographic techniques (e.g., ring signatures and zk-SNARKs) to conceal transactional data. This anonymity appeals to users seeking financial privacy for legitimate purposes but also attracts bad actors involved in illicit activities (Conti *et al*., 2018).

Similarly, crypto mixing services, also known as tumblers, further complicate blockchain transparency. These tools blend cryptocurrency transactions from multiple users to obscure their origins and destinations, breaking the traceability of funds. While proponents argue that these services serve legitimate privacy needs, they are often exploited for laundering proceeds from illegal activities such as hacking, fraud, and ransomware attacks (U.S. DOJ, 2020).

The combination of privacy-focused tools like privacy coins and mixing services presents significant obstacles for law enforcement agencies. These technologies enable criminals to obscure financial activities, making it increasingly difficult to trace and disrupt illicit transactions, including those linked to serious crimes such as child exploitation on the Dark Web (Europol, 2021, Foley *et al*., 2019). Studies have found that cryptocurrencies are now a preferred medium of exchange for traffickers and offenders, offering anonymity and evasion from traditional financial monitoring systems (Europol, 2021).

Addressing these challenges requires a multifaceted approach, including the development of robust regulatory frameworks, the adoption of

advanced forensic technologies, and enhanced global cooperation. These measures aim to mitigate risks while preserving the transformative potential of blockchain systems for innovation and global communication (Atlam *et al.*, 2024).

The decentralised and borderless nature of block-chain and cryptocurrencies has not only revolutionized global interactions but also revealed critical legal and ethical vulnerabilities. While these technologies enable greater innovation and efficiency, they simultaneously challenge existing regulatory mechanisms, making it difficult to enforce laws, ensure accountability, and combat illicit activity (U.S. CFTC, 2024).

3. METHODOLOGY

This research adopts a narrative literature review approach, synthesizing insights from scholarly articles, industry reports, and policy analyses. The goal is to provide a thematic overview of the ethical challenges posed by blockchain and cryptocurrency technologies rather than an exhaustive, systematic review.

Key steps in the methodology include:

- Literature Selection: Relevant sources were identified through targeted searches in academic databases (e.g., Scopus, Google Scholar) and professional publications. Search terms included “blockchain ethics,” “cryptocurrency regulation,” and “privacy in blockchain.”
- Thematic Analysis: Selected literature was grouped into themes such as decentralization, privacy, transparency, and socio-cultural impacts.
- Case Studies: Real-world examples were integrated to illustrate ethical challenges in practice, including cases highlighting regulatory loopholes, environmental concerns, and socio-economic implications for vulnerable populat-ions.
- Synthesis: Findings were contextualized to provide actionable insights and recommendations for stakeholders.

4. BORDERLESS NATURE OF BLOCKCHAIN AND CRYPTOCURRENCIES

4.1. Opportunities for Decentralised Borderless Transactions

Blockchain technology has made international transactions more efficient by eliminating intermediaries like banks and financial institutions. This lowers transaction costs and processing time while increasing financial inclusion as mentioned in a previous section. Further, Blockchain's decentralised structure ensures that transactions take place directly between parties, eliminating the need for third-party verification, making it a cost-effective and efficient cross-border payment solution.

As an example: Migrant workers in the United States can use cryptocurrency-based remittance solutions to send money to their relatives in the Philippines (Devanesan, 2024). This avoids the hefty fees charged by traditional money transfer providers, which generally average 6.3% of the transaction value globally, and assures that payments reach the receiver quickly and safely (World Bank, 2021). This cost decrease is especially useful in places where remittances make up a large portion of household income. According to the World Bank, remittances to low- and middle-income countries totalled $540 billion in 2020, with traditional banking costs accounting for a sizable share of the total. Individuals who use blockchain-based solutions can retain more of their earnings, directly boosting their standard of life and developing financial resiliency. Blockchain technology also addresses accessibility difficulties. Many developing countries have huge unbanked populations, which means they do not have access to established financial institutions. Blockchain enables these people to engage in the global economy by providing a secure and efficient mechanism to store and transfer assets with just a smartphone and an internet connection (Kshetri, 2018). This promotes financial inclusion by providing crucial financial services to previously underserved communities.

4.2. Case Study: Abra’s Digital Cash Network: Simplifying Cross-Border Transactions

Abra is a global peer-to-peer digital cash platform that facilitates international money transfers using cryptocurrencies, like Bitcoin (BTC), Ethereum (ETC) and other, as a medium of exchange (Abra, 2025). By leveraging blockchain technology, Abra offers a decentralised, fast, and cost-efficient remittance solution. This model is particularly beneficial for individuals in regions with limited access to traditional banking services, as it eliminates intermediaries and reduces transaction fees (Kshetri, 2018). Abra is primarily used in countries such as, The Philippines**,** India**,** and Mexico**.** Abra is gaining traction in regions with underbanked populations, including parts of Africa

and Latin America, where its decentralised model helps bridge the gap in financial access (Abra, 2023).

Abra supports financial inclusion by enabling secure and transparent peer-to-peer transactions, making it especially valuable for underbanked populations in developing economies where remittance costs through conventional financial systems are often prohibitively high (Kshetri, 2018).

Figure **1** illustrates Abra's operational framework:

- Sender and Recipient: Users transfer digital currency over the blockchain, bypassing conventional banking systems.
- Abra Tellers: Serve as intermediaries, facilitating cash exchanges for users without digital banking access.
- Blockchain Backbone: Ensures transaction security, transparency, and traceability, preventing fraud and tampering.

The diagram highlights the transaction flow from purchasing and selling digital currency to cross-border transfers emphasizing Abra's decentralised structure. Abra Tellers form a distributed network that bridges the gap between digital and cash transactions, enhancing accessibility.

4.2.1. Other Abra Opportunities

Financial Inclusion: Abra supports secure and transparent peer-to-peer transactions, making it particularly valuable for underbanked populations in developing economies such as the Philippines, India, and Mexico. The platform is also gaining traction in underbanked regions of Africa and Latin America, where traditional banking systems are less accessible (Abra, 2023; Kshetri, 2018).

Accessibility for Cash Users: Through its network of Abra Tellers, the platform bridges the gap between digital and cash transactions, enabling individuals without digital banking access to participate in the global economy. This model offers an inclusive alternative to traditional financial systems.

Transparency and Security: Blockchain ensures transaction traceability, preventing fraud and tampering. This transparency builds trust in cross-border payments, further facilitating adoption in remittance-heavy economies.

4.2.2. Challenges Facing Abra's Model

<u>Regulatory Uncertainty</u>

Managing compliance requirements across multiple jurisdictions poses a significant challenge for Abra. Cryptocurrencies and blockchain technologies are subject to inconsistent and evolving legal frameworks globally, which creates operational risks and increases costs for platforms like Abra (Catalini & Gans, 2020). For example, different nations classify cryptocurrencies as either property, currency, or securities, complicating cross-border transactions (Houben & Snyers, 2018). Without consistent international regulatory standards, Abra remains vulnerable to sudden legal changes and enforcement actions (Tapscott & Tapscott, 2016).

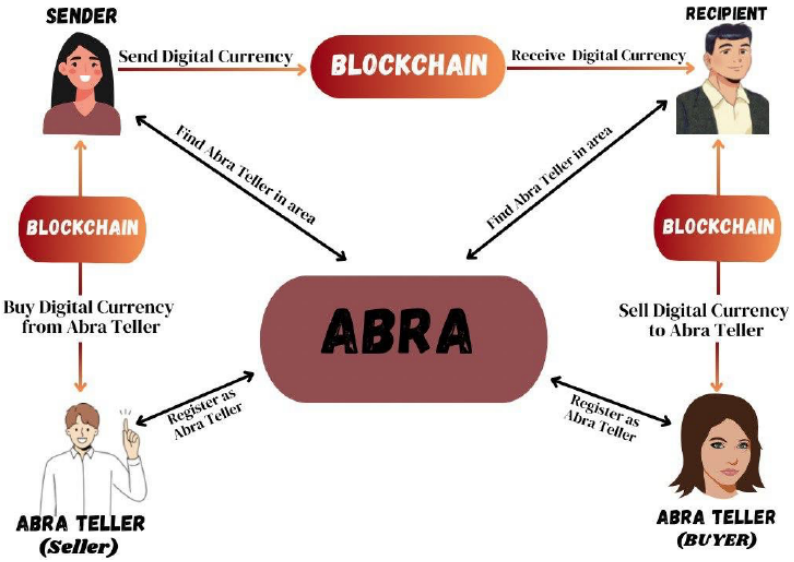

Figure 1: Abra Network.

Adoption Difficulties

Many of Abra's potential users, particularly in underbanked regions, lack sufficient knowledge or trust in blockchain and digital currencies. This limited blockchain literacy and unfamiliarity with digital financial systems create barriers to adoption, requiring extensive educational efforts to build awareness and trust among users (Kshetri, 2018).

Challenges in Building the Abra Teller Network

Abra relies on its network of Abra Tellers to bridge the gap between digital and cash transactions, particularly in areas with limited access to traditional banking. Establishing a strong and trustworthy network requires rigorous vetting processes and continuous support to ensure reliability and security. A poorly managed network could lead to service gaps or security vulnerabilities, undermining the platform's credibility (Kshetri, 2018).

4.2.3. Taxation and Cryptocurrency for U.S. Migrant Workers

Migrant workers who use Abra to send cryptocurrency remittances must examine the tax consequences for the monies they transmit and how cryptocurrencies are classified in the U.S. For instance,

- U.S. Cryptocurrency Remittance Tax treatment: Regardless of remittances, U.S. migrant workers pay income tax on their earnings. Before delivering the money, the worker must file their taxes and pay any taxes. However, sending remittances is not taxed in the U.S. The IRS (2014) states that income, not remittance transfers, is taxed. The IRS considers cryptocurrencies as property, not cash. This categorization implies cryptocurrencies are subject to capital gains tax like equities and real estate (IRS, 2014). Migrant workers utilizing cryptocurrency services like Abra are affected. If a migrant worker buys a "Convertible Virtual Currency (CVC)" and its value rises before transferring it, they may incur capital gains tax (IRS, 2014). A CVC is a cryptocurrency that is equivalent to a fiat currency or can be swapped for a fiat currency (IRS, 2014).If the price of a CVC falls, its owner may lose money, offsetting any gains.

- Cryptocurrency tax treatment of the receiving country: Depending on local legislation, a family member overseas who converts CVC into fiat currency may be taxed in their home nation (Kshetri, 2018).

- Recordkeeping: To correctly compute capital gains or losses, migrant workers must document cryptocurrency transactions, including purchase prices, dates, and value when used or transferred (IRS, 2014). Users may not grasp the tax ramifications of transmitting CVC, especially internationally. Abra might benefit from educating users about these tax duties (Tapscott & Tapscott, 2016).

4.3. Challenges in Defining Applicable Laws

The international characteristics of blockchain technology hinder the establishment of suitable regulations for transactions and operations conducted on blockchain networks. In contrast to conventional systems that function within well-defined jurisdictional boundaries, blockchain transactions sometimes engage stakeholders from multiple nations, each possessing distinct legal frameworks and regulatory limitations. The absence of uniformity complicates adherence, enforcement, and conflict resolution (Catalini & Gans, 2020). Examine a smart contract within a cross-border supply chain agreement executed on a blockchain platform. The contract automates and enforces the parties' stipulated duties, although it engenders significant governance challenges, including:

Jurisdiction

Which nation's legal framework governs smart contracts? Establishing jurisdiction is challenging when the contract comprises parties from various regions with conflicting legal systems.

Dispute Resolution

What is the process for resolving disputes? Conventional legal institutions may struggle to interpret and enforce blockchain-based contracts because of their technical intricacies and decentralised characteristics.

Enforcement Mechanisms

In the absence of a centralized authority, the execution of legal outcomes is complicated, particularly when parties are situated in regions with fragile or contradictory legal systems. For instance, if a smart contract inside a supply chain fails to achieve a specified milestone, the affected party must define the

method and venue for seeking restitution. The resolution procedure is significantly more complex when blockchain networks traverse jurisdictions with conflicting regulatory perspectives on smart contracts and blockchain technology (De Filippi & Wright, 2018). These legal problems underscore the essential requirement for international collaboration and the unification of laws regulating blockchain transactions.

4.4. Case Study: The SEC vs. Kik Interactive

The legal dispute between the United States Securities and Exchange Commission (SEC) and Kik Interactive highlights the complexities and regulatory challenges associated with cryptocurrency offerings (Radcliffe, 2020). Kik Interactive, a Canadian social media company, launched an Initial Coin Offering (ICO) in 2017 to fund its cryptocurrency project, Kin. The ICO attracted global investors and raised almost $100 million, positioning Kin as a digital currency designed to facilitate payments and enhance user engagement within Kik's ecosystem (MacPhail & Farooqui, 2020; Court Listener, 2020). The cross-border nature of the ICO and the diverse applications of Kin tokens swiftly drew regulatory scrutiny, particularly from the SEC (Goforth, 2021).

Regulatory Allegations and Legal Framework

The SEC asserted that Kik's ICO violated U.S. securities regulations by constituting an unregistered securities offering. The SEC's stance was predicated on the Howey Test, a legal standard for determining if a transaction constitutes a security. According to the Howey Test, an offering is classified as a security if it involves:

Monetary Investment: Investors purchased Kin tokens with the expectation of achieving profits.

The value of Kin was linked to Kik's efforts to develop and enhance its ecosystem. Expectation of Profits Derived from the Efforts of Others: Investors relied on Kik's success in advancing its platform to increase the token's value.

The SEC emphasized that Kik failed to register the ICO with the Commission, so denying investors the necessary disclosures and protections mandated by securities regulations (MacPhail & Farooqui, 2020;).

Kik's Legal Defence and Regulatory Uncertainty

Kik maintained that Kin tokens were not securities, but rather utility tokens intended solely for use within its network. The company's defence relied on the following points:

- Functional Utility: Kin tokens were designed to facilitate peer-to-peer transactions and promote user involvement, distinguishing them from securities.
- Kik asserted that it did not endorse the ICO as an investment opportunity or guarantee financial returns.
- Kik highlighted the lack of regulatory clarity during the offering, hampering the precise categorization of tokens as securities.

In 2020, a U.S. federal court ruled that Kik's ICO constituted an unregistered securities offering, thereby violating securities rules. The court imposed a $5 million penalty on Kik and mandated the establishment of compliance protocols for future token sales (Court Listener, 2020).

4.4.1. Substantial Implications for the Crypto-currency Industry

The SEC versus Kik Interactive case underscores numerous critical challenges and lessons pertinent to the cryptocurrency and blockchain sectors:

- The case highlights the absence of clear, standardized criteria for the classification and management of digital assets. This ambiguity obstructs compliance initiatives for issuers and raises issues about legal interpretations across jurisdictions.
- Cross-Border Complexities: The global nature of ICOs presents issuers with legal and operational problems in navigating diverse regulatory requirements across multiple jurisdictions.
- The ruling underscores the SEC's commitment to transparency and investor protection in cryptocurrency markets, emphasizing the need for adequate disclosures (Goforth, 2021).

4.4.2. Perspectives for Innovators and the Blockchain Industry

The Kik Interactive case illustrates the evolving regulatory landscape for blockchain-based fundraising. It highlights the imperative for issuers to prioritize legal compliance and regulatory due diligence in the structuring of ICOs or other token offerings. This example illustrates the risks of regulatory ambiguity for

firms seeking innovation in the blockchain sector and emphasizes the importance of contacting legal experts to ensure compliance with securities legislation (Houben & Snyers, 2018).

4.5. Resolving Cross-Border Disputes

Resolving cross-border disputes is one of the most significant challenges in blockchain systems due to their decentralised and borderless nature. Unlike traditional systems, blockchain operates without a central authority or intermediary to mediate conflicts or enforce agreements, complicating dispute resolution (De Filippi & Wright, 2018). The absence of a central authority also makes it challenging to establish accountability, particularly when transactions span multiple jurisdictions. For example, consider a situation in which a smart contract is performed on a blockchain platform involving two firms from separate countries: Company X in the United States and Company Y in Germany. Once the items are delivered, the smart contract immediately transfers cryptocurrency from Company X to Company Y. However, Company X claims that the items provided did not meet the agreed-upon requirements, raising issues about the transaction.

Traditional legal systems cannot simply solve this problem owing to several difficulties.

- Jurisdictional Ambiguity: Given that blockchain transactions do not adhere to strict legal boundaries, it is unclear whether the issue should be addressed under U.S. or German law (Catalini & Gans, 2020).
- Enforcement Concerns: If one party is deemed at fault, there is no obvious mechanism to impose fines or reparations without the intervention of a central authority or mediator (De Filippi & Wright, 2018).
- Anonymity and Transparency: If Company Y uses a pseudonymous address, Company X may struggle to identify and pursue legal action against the proper organization (Zavolokina *et al*., 2020).

Such issues underscore the need for international legal frameworks and blockchain-specific arbitration procedures to handle conflicts effectively while preserving the decentralised and borderless character of these systems (Tapscott & Tapscott, 2016).

4.6. Associations with Illegal Activities

Blockchain technology, known for its transparency, traceability, and data security, has been proposed to enhance the efficiency and reliability of cryptocurrencies (Dondjio & Themistocleous, 2021). However, despite its secure framework, certain cryptocurrencies, such as Bitcoin, are frequently used in illicit activities on the dark web, including child exploitation. The pseudonymous and privacy-preserving features of cryptocurrencies enable individuals to conduct transactions that are difficult to trace, raising concerns about their misuse in illegal market (Foley *et al*., 2019). Cryptocurrencies, particularly those with increased privacy features, offer a degree of anonymity that can promote illegal activities by making it difficult for authorities to track down users (Conti *et al*., 2018). In fact, cryptocurrencies with enhanced privacy features, such as Monero and Zcash, are designed to obscure transactional details, including sender, receiver, and transaction amounts, through advanced cryptographic techniques like ring signatures and zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge**"**. It is a cryptographic technology used in blockchain systems, particularly privacy-focused cryptocurrencies like Zcash, to ensure both privacy and integrity of transactions (Conti *et al*., 2018). While these privacy-enhancing measures serve legitimate purposes, such as protecting user data, they also enable criminal activities by providing a high degree of anonymity. This anonymity makes it challenging for law enforcement to trace the flow of funds and identify individuals behind illicit transactions (Conti *et al*., 2018).

Furthermore, cryptocurrency such as Monero, which is recognized for its advanced privacy-enhancing features, has been widely utilized on darknet markets to purchase illegal products and services. Monero's ability to hide transaction details and participants makes it difficult for law enforcement agencies to track down and prosecute offenders (Conti *et al*., 2018).

For example, the notorious Silk Road marketplace, an online illegal market that operated on the dark web between 2011 and 2013, mainly relied on Bitcoin for transactions (Kermitsis *et al*., 2021). This platform demonstrated the potential of blockchain technology to facilitate anonymous and decentralized transactions, which posed significant challenges for regulators and law enforcement (Kermitsis *et al*., 2021).

Despite the Silk Road's closure in 2013 after a high-profile investigation and arrest, similar marketplaces have continued to emerge on the dark web, highlighting the ongoing need for robust regulatory frameworks and monitoring systems to address illegal activities enabled by blockchain technology. (Kermitsis *et al*., 2021).

While Bitcoin is not completely anonymous, its pseudonymous nature allows users to purchase and trade illegal products, such as drugs and weapons, without disclosing their genuine names. This usage of cryptocurrencies exposed its potential for abuse, sparking global debates on regulation and enforcement (Brenig *et al*., 2015).

4.6.1. Balancing Regulation, Innovation, and Privacy

While addressing the risks associated with unlawful activities is vital, excessive regulation may stifle innovation and limit the growth of the cryptocurrency industry. Achieving a balance between government surveillance and technological innovation is essential for creating a healthy environment (Fanti & Viswanath, 2019). For example, legislation demanding strong Know Your Customer (KYC) and Anti-Money Laundering (AML) standards for cryptocurrency exchanges help to prevent money laundering and terrorist financing. However, overly strict regulations may burden cryptocurrency enterprises, limiting their ability to innovate and compete in the global market (Houben & Snyers, 2018).

The borderless nature of blockchain and cryptocurrency creates a two-sided dynamic of disruptive opportunities and difficult challenges in the legal and regulatory landscape. On the one hand, new technologies offer enormous potential to spur innovation, increase financial inclusion, and transform existing systems. On the other hand, they pose serious issues regarding jurisdictional ambiguity, enforcement limits, and vulnerability to abuse, particularly in illegal activity (Tapscott & Tapscott, 2016). Addressing these difficulties requires a complex and multifaceted strategy. Policymakers must strike a balance between enforcing strong rules to reduce risks and creating an atmosphere that promotes technology innovation while protecting privacy.

Key strategies include:

- International cooperation necessary to set common and enforceable regulatory norms for blockchain, given its global character.
- Standardized regulatory frameworks eliminate confusion for businesses, improve compliance, and ensure fairness and accountability.

Blockchain-based arbitration provides a decentralized mechanism for resolving disputes transparently and fairly, removing the reliance on traditional legal systems. Enhanced Know Your Customer (KYC) and Anti-Money Laundering (AML) tools leverage advanced technologies to ensure regulatory compliance while combating financial crimes like fraud and money laundering (Catalini & Gans, 2020).

Privacy-preserving processes, such as cryptographic techniques or zero-knowledge proofs, protect sensitive user data while enabling regulatory oversight. Together, these innovations create a pathway to bridge the gap between the demands of regulators and the capabilities of modern blockchain technologies, fostering wider adoption and trust in decentralized systems (Catalini & Gans, 2020).

5. THE JUNCTION OF BLOCKCHAIN, CRYPTOCURRENCY AND CRIME

The main types of crime associated with blockchain, and cryptocurrency (Europol 2021) include the following. A typical but not the only possible sequence of events that take place within each type of criminal activity.

Money Laundering

- Making use of cryptocurrencies to hide the source of illegal funds.
- Use of mixers/tumblers to blend transactions and hide transaction patterns.
- Illegal funds converted to crypto, “tumbled”, switched through exchanges, converted back to fiat currency.

Hacking and Theft

- Hacking wallets or exchanges to extract crypto addresses and associated cryptocurrency.
- Use of mixers/tumblers to blend transactions and hide transaction patterns.
- Convert crypto to other cryptocurrencies using decentralised finance applications.
- Convert the cryptocurrencies to fiat currency through exchanges of low to non-existed regulation controls.

Figures **2** and **3**, (Chainalysis, 2023), below, shows the estimated total number of hacks and value of global annual losses from crypto applications, for the period 2016-2022.

In Figure **3**, presents the losses by platform type as a percentage of the overall loss. The most notable trend is the steep increase in losses from Distributed Finance applications.

Ransomware

- A cyberattack initiated on a specific target (eg. government, large corporate entity, a media corporation).
- Business critical and other data are encrypted by the cyber attacker, making them unusable by the owner.
- Ransom is demanded by the cyber attacker in crypto to unlock the files

Dark Web Activity

- Use of cryptocurrencies, on the Dark Web, for the trading of illegal weapons, drugs and other illegal products and services.

Fraud and Scam

- Fraudulent Initial Coin Offerings (ICO).
- Operation of Ponzi schemes.

Terrorism Financing

- Funding of terrorist activities using crypto-currencies.
- Anonymity and mixing are two of the enabling factors.

Tax evasion

- Tax avoidance by using anonymity to hide crypto currency related tax obligations.

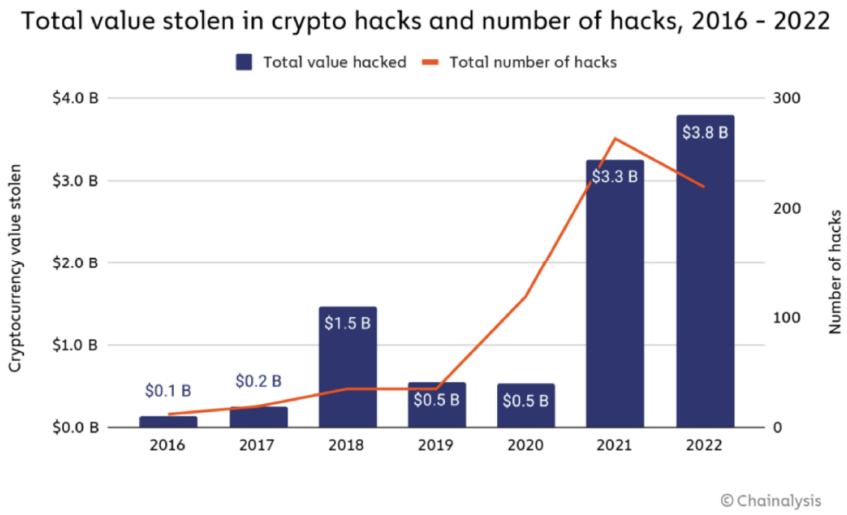

Figure 2: Total Value and Number of hacks on crypto applications 2016-2022.

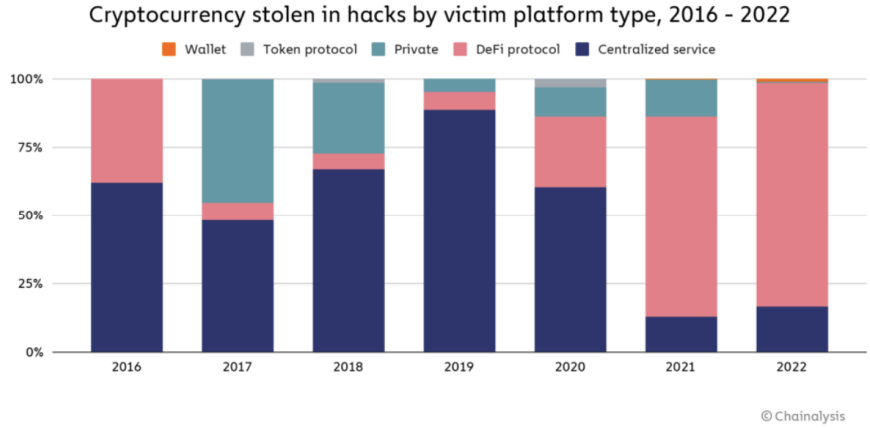

Figure 3: Cryptocurrencies stolen by hacks from each type of crypto application 2016-2022.

6. CASE STUDIES

6.1. Fraud and Scam Examples

A Ponzi scheme in cryptocurrency involves promising high returns on investments to new participants, while using the funds from later investors to pay the earlier ones. The typical Ponzi scheme collapses when there are not enough new investors to sustain payouts to earlier investors. Bitconnect (IRS, 2023) was such a scheme. That scam required investors to purchase Bitconnect tokens BCC then lend them to the platform. The platform was then to expected to trade the borrowed BCC tokens using “smart unique technology” and deliver substantial returns to the investors. This scam resulted in over $2 billion of losses to investors.

A "rug pull" scam occurs when developers of a cryptocurrency project suddenly withdraw all funds, abandon the project and leave investors with worthless tokens. Squid Game token (SQUID) was one such case. When a large pool of SQUID was acquired by investors, the developers made it difficult to sell the token. The developers cashed out $3 million causing the token’s price to totally collapse (BBC, 2021).

6.2. Hacking and Theft Example

The Poly Network hack in 2021 with losses of more than $600 million, was one of the largest crypto thefts up that time (TRM, 2021). The network’s smart contract and its management of cross-chain transactions had vulnerabilities that were exposed by the hacker. Fundamentally, cryptocurrency was moved from the platform to the hacker’s wallets on different blockchains. Some of the funds were frozen quickly, notably those on the Tether stablecoin network. Crypto community pressure followed with the addresses where the stolen cryptocurrencies were placed on “blocklists”. Finally, the hacker started stated that the intention of the hack was only to prove that the network had vulnerabilities in the code that could be exploited. All cryptocurrencies that were still in the control of the hacker were returned to the original owners’ blockchain addresses.

6.3. Ransomware Example

The Colonial Pipeline is the largest fuel pipeline for refined products in the US. In 2021 it was targeted by a ransomware group which resulted in encrypting Colonial Pipeline data, that in turn disrupted fuel supplies and caused mass panic. A ransom demand of 75 Bitcoin was issued by the attackers (US Department of Energy, 2021). The estimated value of the ransom was around $4.5 million at that time. The cryptocurrency was paid to the attackers. However, due to the pseudo-anonymity of Bitcoin the US authorities were able to recover 84% of the cryptocurrency.

7. DISCUSSION

The ethical dilemmas associated with blockchain, and cryptocurrency technologies originate from their decentralised and borderless characteristics, which threaten conventional legislative and financial frameworks. This section examines comparative studies of ethical challenges, implications for global policy alignment, and the contribution of multidisciplinary techniques in alleviating ethical dangers.

7.1. Comparative Analysis of Ethical Challenges

Ethical issues in blockchain and cryptocurrencies vary across industrialized and developing nations owing to differences in legislative frameworks, technical infrastructure, and socio-economic conditions.

In industrialized nations**,** challenges revolve around data privacy, regulatory compliance, and cybersecurity. For instance, the General Data Protection Regulation (GDPR) in the European Union requires a delicate balance between data immutability, a core blockchain feature, and privacy rights. Moreover, financial systems in these countries must integrate anti-money laundering (AML) and counter-terrorism financing (CTF) protocols, complicating the regulatory landscape (Houben & Snyers, 2018).In contrast, developing nations face challenges stemming from financial literacy gaps, limited technological accessibility, and weak infrastructure. While cryptocurrencies present opportunities for financial inclusion, they simultaneously expose vulnerable groups to exploitation and fraud due to inadequate regulatory monitoring (Kshetri, 2018). Additionally, the reliance on cryptocurrencies for remittances in these countries increases economic risks, as these assets are often volatile and unstable, threatening local economic stability.

7.2. Consequences for Global Policy Alignment

The borderless nature of blockchain technology demands global collaboration to establish unified regulatory frameworks. Nations must cooperate to

develop standardized definitions, compliance requirements, and enforcement mechanisms to address transnational challenges (Catalini & Gans, 2020).

Key recommendations for global policy alignment include:

- Uniform AML/CTF Processes: Implement harmonized anti-money laundering and counter-terrorism financing measures to curb illicit activities on blockchain platforms.
- Transnational Legal Frameworks: Develop international frameworks for resolving cross-border disputes and enforcing smart contracts, ensuring legal interoperability across jurisdictions.
- Global Data Privacy Guidelines: Establish standardized global data privacy regulations to address blockchain's inherent openness and immutability, minimizing risks to individual privacy.

These steps would mitigate blockchain's ethical risks while preserving its transformative potential for innovation and financial inclusion.

7.3. Role of Interdisciplinary Approaches

Addressing blockchain's ethical challenges requires contributions from multiple disciplines. This interdisciplinary approach ensures that technical, legal, economic, and social dimensions are adequately addressed in blockchain adoption.

- Legal Integration: Legal expertise can support the development of enforceable smart contracts, ensuring compliance with local and international regulations.
- Economic Models: Economists can assess the socio-economic impacts of blockchain implementation, identifying fair remedies and equitable outcomes for communities.
- Data Science Solutions: Privacy-preserving techniques, such as zero-knowledge proofs, can enable transparency while protecting sensitive data.
- Sociological Perspectives: Sociological insights can help evaluate cultural and ethical implications of blockchain adoption, tailoring solutions to specific community needs.

8. RECOMMENDATIONS

8.1. Policy Recommendations

To address the challenges posed by blockchain and cryptocurrency technologies, the following policy recommendations are essential. First, regulatory clarity is crucial. Developing uniform and internationally aligned regulatory frameworks will help resolve jurisdictional uncertainties and improve enforcement mechanisms. This is especially relevant in combating financial crimes such as money laundering and fraud, which exploit blockchain's borderless nature (Catalini & Gans, 2020). Harmonized regulations across jurisdictions can provide a consistent legal environment, enabling effective oversight and compliance.

Second, privacy safeguards must balance blockchain's transparency with data protection. The adoption of privacy-enhancing technologies, such as zero-knowledge proofs and mixers, can ensure privacy while maintaining compliance with data protection laws like the GDPR (Conti *et al*., 2018). These technologies provide a pathway to reconcile openness with individual privacy rights.

Third, consumer protection should be a priority. Mandatory Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations for cryptocurrency exchanges can mitigate risks associated with fraud and exploitation (Houben & Snyers, 2018). These measures will enhance trust and accountability in cryptocurrency transactions while safeguarding users from malicious activities.

Finally, environmental sustainability must be promoted in blockchain development. Transitioning from energy-intensive consensus mechanisms, such as Proof-of-Work, to more efficient alternatives like Proof-of-Stake can significantly reduce the environmental impact of blockchain networks (Tapscott & Tapscott, 2016). This is vital for ensuring that blockchain innovation aligns with global sustainability goals

8.2. Sector and Research Approaches

Addressing blockchain's ethical and operational challenges requires targeted actions in both sectoral and research domains. First, education and awareness are essential to enhance digital literacy among

stakeholders. Educating users about ethical risks, safe practices, and the potential of blockchain can help reduce vulnerabilities and foster informed decision-making (Kshetri, 2018).

Second, security enhancements should be prioritized by allocating resources to strengthen cybersecurity frameworks. Improved defenses against hacking, ransomware, and fraud will help ensure the resilience of blockchain networks and maintain user confidence (Conti *et al.*, 2018).

Third, collaborative research should be encouraged among academics, industry leaders, and policymakers. By fostering alliances, stakeholders can explore innovative solutions to blockchain's ethical dilemmas, such as integrating sociological insights into blockchain design or improving privacy-preserving methodologies (Houben & Snyers, 2018).

Finally, testing regulatory sandboxes offers a controlled environment for evaluating blockchain innovations before their widespread implementation. These sandboxes allow regulators and developers to assess potential risks and benefits, providing valuable insights into the scalability and societal impact of blockchain applications (Catalini & Gans, 2020).

9. CONCLUSION

Blockchain and cryptocurrency technologies provide transformational potential to reform financial institutions, enhance transparency, and promote inclusivity. Nonetheless, they also provide significant ethical dilemmas about privacy, regulation, security, and socio-economic equality.

This article underscores significant ethical challenges, including privacy against openness, jurisdictional disputes, and connections to crime, highlighting their ramifications for both rich and developing nations. Although blockchain's decentralised characteristics provide prospects for financial inclusivity and efficiency, they also need strong frameworks to protect privacy, avert abuse, and tackle jurisdictional complications.

Future research must prioritize the integration of multidisciplinary methodologies, the promotion of international collaboration, and the equilibrium between innovation and ethical issues. By proactively tackling these difficulties, politicians, business leaders, and academics can guarantee that blockchain and cryptocurrencies foster a more egalitarian and safe digital economy.

REFERENCES

Abra. 2023. Company Overview. Retrieved December 11, 2024, from https://www.abra.com..

Abra. 2025. “What Cryptocurrencies does Abra support?”. Retrieved, December 11, 2024, from https://support.abra.com/hc/enus/articles/3600

Adegbite, Ayodeji. 2024. "The Role of Blockchain Technology in Enhancing Financial Inclusion." IOSR Journal of Economics and Finance 15. https://doi.org/10.9790/5933-1505071928

Alkire, Sabina, Kanagaratnam, Usha, and Suppa, Nicolas. 2024. "A Methodological Note on the Global Multidimensional Poverty Index (MPI) 2024 Changes Over Time Results for 86 Countries." OPHI MPI Methodological Note 60. https://www.undp.org/sites/g/files/zskgke326/files/2024-10/mpireport2024en.pdf.

Atlam, Hany F., Ekuri, Nathaniel, Azad, Mohammed A., and Lallie, Harjinder S. 2024. "Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions." Electronics 13(17):3568. https://doi.org/10.3390/electronics13173568

BBC. 2021. “Squid Game Crypto Token Collapses in Apparent Scam.” Retrieved January 23, 2025, from https://www.bbc.com/news/business-59129466.

Bahri, Amrita. 2020., “Blockchaining international trade: a way forward for women’s economic empowerment?”, Adapting to the Digital Trade Era, pp 300-31. https://doi.org/10.30875/137d7993-en

Bansod, Santosh, and Ragha, Lalita. 2022. "Challenges in Making Blockchain Privacy Compliant for the Digital World: Some Measures." Sādhanā 47:168. https://doi.org/10.1007/s12046-022-01931-1

Bayan, Talgar, and Banach, Richard. 2023. “Exploring the Privacy Concerns in Permissionless Blockchain Networks and Potential Solutions”. IEEE International Conference on Smart Information Systems and Technologies (SIST). https://doi.org/10.1109/SIST58284.2023.10223536

Beinke, Matthias, Julian H. Beinke, Eva Anton, *et al*. 2024. “Breaking the Chains of Traditional Finance: A Taxonomy of Decentralised Finance Business Models.” Electronic Markets 34:29. https://doi.org/10.1007/s12525-024-00704-4

Belen-Saglam, Rahime, Altuncu, Enes, Lu, Yang & Li, Shujun. 2023. "A Systematic Literature Review of the Tension Between the GDPR and Public Blockchain Systems." Blockchain: Research and Applications 4(2). https://doi.org/10.1016/j.bcra.2023.100129

Brenig, Christoph, Rafael Accorsi, and Günter Müller. 2015. “Economic Analysis of Cryptocurrency-Backed Money Laundering.” Information Security and Cryptography, 1–15. Retrieved December 20, 2024, from https://www.academia.edu/73375534/Economic_Analysis_of_Cryptocurrency_Backed_Money_Laundering

Catalini, Christian, and Joshua S. Gans. 2020. “Some Simple Economics of the Blockchain.” Communications of the ACM 63(7):80–90. https://doi.org/10.1145/3359552

Chainalysis. 2023. “2022 Biggest Year Ever for Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-Linked Attackers.” Retrieved December 16, 2024, from https://www.chainalysis.com/blog/2022-biggest-yearever-for-crypto-hacking/.

Cointelegraph. 2023. “Financial Privacy and Regulation Can Co-Exist with ZK Proofs – Vitalik Butterin.” Retrieved December 17, 2024, from https://cointelegraph.com/news/financial-privacyregulation-can-coexist-zk-proofs-vitalik-buterin

Conti, Mauro, Sandeep Kumar, Chhagan Lal, and Sushmita Ruj. 2018. “A Survey on Security and Privacy Issues of Bitcoin.” IEEE Communications Surveys & Tutorials 20(4):3416–3452. https://doi.org/10.1109/COMST.2018.2842460

Chiu, Jonathan, and Koeppl, Thorsten V. 2019. "Blockchain-Based Settlement for Asset Trading." The Review of Financial Studies 32(5). https://doi.org/10.1093/rfs/hhy122

Court Listener. 2020. "U.S. Securities and Exchange Commission v. Kik Interactive Inc., 1:19-cv-05244, (S.D.N.Y.)", Updated May 24, 20204. Retrieved January 6, 2025, from https://www.courtlistener.com/docket/15722539/us-securities-and-exchange-commission-v-kik-interactive-inc/

Davidson, Sinclair, De Filippi, Primavera, & Potts, Jason. 2018. “Economics of Blockchain”. SSRN Electronic Journal. Retrieved December 14, 2024. https://doi.org/10.2139/ssrn.2744751

De Filippi, Primavera, and Aaron Wright. 2018. Blockchain and the Law: The Rule of Code. Cambridge, MA: Harvard University Press. https://doi.org/10.4159/9780674985933

De Vries, A. 2018. “Bitcoin’s Growing Energy Problem”. Joule, 2(5), 801–805. Retrieved December 14, 2024. https://doi.org/10.1016/j.joule.2018.04.016

Devanesan Johanan, (2024), «List of Cryptocurrency Exchanges in the Philippines, Fintech Philippines». Retrieved January 24, 2025, from https://fintechnews.ph/61554/crypto/here-are-the-licensed-cryptocurrency-exchanges-in-the-philippines/

Digiconomist. n.d. “Bitcoin Energy Consumption Index.”. Retrieved January 13, 2025, from https://digiconomist.net/bitcoin-energy-consumption.

Dondjio, Irenee, and Andreas Kazamias. 2023. “A Blockchain Framework for Digital Asset Ownership and Transfer in Succession.” In European, Mediterranean, and Middle Eastern Conference on Information Systems, pp. 88–106. Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56478-9_7

Dondjio, Irenee, and Marinos Themistocleous. 2021. “Blockchain Technology and Waste Management: A Systematic Literature Review.” In European, Mediterranean, and Middle Eastern Conference on Information Systems, pp. 194–212. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-85969-5_13

Ethereum. 2024. Introduction to Smart Contracts. Retrieved January 15, 2025, from https://ethereum.org/en/smart-contracts/.

European Council. n.d. “The general data protection regulation”. Retrieved January 9, 2025, from https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/.

Europol. 2021. Cryptocurrencies: Tracing the Evolution of Criminal Finances. Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

Fanti, Giulia, and Balachander Viswanath. 2019. “Anonymity vs. Transparency: Balancing Privacy and Regulation in Blockchain.” Journal of Cryptographic Engineering 9(3):199–209.

FAO & ITC. 2023. "Making the AfCFTA Work for Women in the Agrifood Sector – Policy Brief: Trade Facilitation." Rome. https://doi.org/10.4060/cc5866en

FATF (Financial Action Task Force). 2022. Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs. Paris, France. Retrieved January 23, 2025, from www.fatf-gafi.org/publications/fatfrecommendations/documents/targeted-update-virtual-assets-vasps.html.

FINMA (Swiss Financial Market Supervisory Authority). n.d. Retrieved January 23, 2025, from www.finma.ch.

Foley, Sean, Jonathan Karlsen, and Talis Putnis. 2019. “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?” https://doi.org/10.2139/ssrn.3102645

Forbes. 2021. “Women Turn to Crypto for Funding and Financial Freedom When Other Systems Are Blocked.” Retrieved January 23, 2025, from https://www.forbes.com/sites/alainapercival/2021/08/26/women-turn-to-crypto-for-funding-and-financial-freedom-when-other-systems-are-blocked/.

Gabuthy, Yannick. 2023. "Blockchain-Based Dispute Resolution: Insights and Challenges" *Games* 14, no. 3: 34. https://doi.org/10.3390/g14030034

Goforth, Carol R. 2021. “Regulation of Crypto: Who Is the Securities and Exchange Commission Protecting?” American Business Law Journal 58(3):643–705. https://doi.org/10.1111/ablj.12192

Haro-Olmo, Francisco J., Antonio J. Varela-Vaca, and J. A. Alvarez-Berm. 2020. “Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review.” Sensors 20(24). https://doi.org/10.3390/s20247171

Hartmann, Jens, and Omar Hasan. 2023. “Privacy Considerations for a Decentralised Finance (DeFi) Loans Platform.” Cluster Computing 26:2147–2161. https://doi.org/10.1007/s10586-022-03772-3

Hooper, Anatol. 2023. "Debunking the Myth: Cryptocurrency Is Used for Criminal Activity." Cointelegraph. Retrieved January 3, 2025, from https://cointelegraph.com/news/debunking-the-myth-cryptocurrency-is-used-for-criminal-activity.

Houben, Robby, and Alexander Snyers. 2018. “Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering, and Tax Evasion.” European Parliament Policy Department.

Imai, Katsushi S., Cheng, Wenya, and Gaiha, Raghav. 2015. "Agricultural Growth, Poverty and Inequality in Developing Countries." Development 58:230–236. https://doi.org/10.1057/s41301-016-0009-1

Internal Revenue Service (IRS). 2014. Notice 2014-21: Virtual Currency Guidance. Retrieved December 15, 2024, from https://www.irs.gov.

Internal Revenue Service (IRS). 2023. “Victims of BitConnect Scheme to Receive More Than $17 Million to Compensate for Losses.” Retrieved January 23, 2025, from https://www.irs.gov/compliance/criminal-investigation/victims-of-bitconnect-scheme-to-receive-more-than-17-million-to-compensate-for-losses.

Kermitsis, Emmanouil, Kavallieros, Dimitrios, Myttas, Dimitrios, Lissaris, Euthimios, and Giataganas, Georgios. 2021. “Dark Web Markets”. Dark Web Investigations, pp. 85-118.

Kohli, Vidhi, Subhashis Chakravarty, Vineet Chamola, Kuldeep S. Sangwan, and Sherali Zeadally. 2022. “An Analysis of Energy Consumption and Carbon Footprints of Cryptocurrencies and Possible Solutions.” Cornell University. Retrieved January 23, 2025, from https://arxiv.org/abs/2203.03717.

Kshetri, Nir. 2018. “Blockchain’s Roles in Meeting Key Supply Chain Management Objectives.” International Journal of Information Management 39:80–89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

Leng, Jingwen, Min Zhou, J. Leon Zhao, Yuan Huang, and Bin Bian. 2022. “Blockchain Security: A Survey of Techniques and Research Directions.” IEEE Transactions on Services Computing 15(4). https://doi.org/10.1109/TSC.2020.3038641

Lerner, Sergio D. 2019. “Rootstock Platform White Paper.” Retrieved January 10, 2025, from https://rootstock.io/rsk-white-paperupdated.pdf.

MacPhail, Michael R., Farooqui, Megan M., 2020. "Two Recent SEC Cases Involving Cryptocurrency Offerings", National Law Review, https://natlawreview.com/article/two-recent-sec-cases-involving-cryptocurrency-offerings

Makarov, Igor, and Schoar, Antoinette. 2022. "Cryptocurrencies and Decentralized Finance". BIS Working Papers No 1061, Bank of International Settlements (BIS). https://doi.org/10.3386/w30006

MAS (Monetary Authority of Singapore). n.d. Retrieved January 23, 2025, from www.mas.gov.sg.

Mhlanga, David. 2023. "Blockchain Technology for Digital Financial Inclusion in the Industry 4.0, Towards Sustainable Development?" Frontiers in Blockchain 6. https://doi.org/10.3389/fbloc.2023.1035405

Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved January 23, 2025, from https://bitcoin.org/bitcoin.pdf.

Narayanan, Arvind, Bonneau, Joseph, Felten, Edward, Miller, Andrew, & Goldfeder, Steven. 2016. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction". Princeton University Press.

Ncube, Tsitsi, Dlodlo, Nomusa, and Terzoli, Alfredo. 2020. "Private Blockchain Networks: A Solution for Data Privacy." 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), pp. 1–8. https://doi.org/10.1109/IMITEC50163.2020.9334132

Oyelere, Solomon Sunday, Agbo, Friday Joseph, & Sanusi, Ismaila Temitayio. (2022). "Developing a pedagogical evaluation framework for computational thinking supporting technologies and tools". Frontiers in Education, 7, 957739. https://doi.org/10.3389/feduc.2022.957739

Project Guardian. 2024. Monetary Authority of Singapore. Retrieved January 23, 2025, from https://www.mas.gov.sg/schemes-and-initiatives/project-guardian.

Rosaire, Senou Mahugnon, and Degila Jules. "Smart Contracts Security Threats and Solutions." *IJITWE* vol.17, no.1 2022: pp.1-30. https://doi.org/10.4018/IJITWE.304048

Salami, Ismail. 2021. "Challenges and Approaches to Regulating Decentralized Finance." AJIL Unbound 115:425–429. https://doi.org/10.1017/aju.2021.66

Schär, Fabian L. 2021. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." Federal Reserve Bank of St. Louis. https://doi.org/10.2139/ssrn.3571335

Stone, Alastair. 2022. "Why Decentralized Finance Is a Leapfrog Technology for the 1.1 Billion People Who Are Unbanked." World Economic Forum. Retrieved January 23, 2025, from https://www.weforum.org/stories/2022/09/decentralised-finance-a-leapfrog-technology-for-the-unbanked/.

Tabatabaei, Mohammad H., Roman Vitenberg, and Nithya R. Veeraragavan. 2023. "Understanding Blockchain: Definitions, Architecture, Design, and System Comparison." Computer Science Review 50. https://doi.org/10.1016/j.cosrev.2023.100575

Tapscott, Don, and Alex Tapscott. 2016. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Penguin.

Themistocleous, Marinos. 2018. "*Blockchain Technology and Land Registry". Journal Database: Supplemental Index*, 30(2), 195. Retrieved December 9, 2024, from https://cyprusreview.org/index.php/cr/article/download/579/502

Trend Micro Inc. 2019. Evasive Threats, Pervasive Effects. Retrieved January 23, 2025, from https://documents.trendmicro.com/assets/rpt/rpt-evasive-threats-pervasive-effects.pdf.

TRM. 2021. "TRM Tracks the Poly Network Hack as Attacker Communicates in Real Time." Retrieved January 23, 2025, from https://www.trmlabs.com/post/trm-tracks-the-poly-network-hack-as-attacker-communicates-in-real-time-via-input-data.

Truby, Jon. 2018. "Decarbonizing Bitcoin: Law and Policy Choices for Reducing the Energy Consumption of Blockchain Technologies and Digital Currencies". Energy Research & Social Science, 44, 399–410. Retrieved December 20, 2024. https://doi.org/10.1016/j.erss.2018.06.009

United Nations University. 2023. The Hidden Environmental Costs of Cryptocurrency. Retrieved January 23, 2025, from https://collections.unu.edu/eserv/UNU:9528/UN-IWEH_BTC_Report.pdf.

U.S. Energy Information Administration (EIA). 2024. "Tracking Electricity Consumption from U.S. Cryptocurrency Mining Operations." Retrieved January 23, 2025, from https://www.eia.gov/todayinenergy/detail.php?id=61364.

United States Commodity Futures Trading Commission (U.S. CFTC). 2024. Decentralized Finance. Retrieved January 23, 2025, from https://www.cftc.gov/media/10106/TAC_DeFiReport010824/download.

United States Department of Energy. 2021. "Colonial Pipeline Cyber Incident." Retrieved January 23, 2025, from https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

United States Department of Justice (U.S. DOJ). 2020. Cryptocurrency Enforcement Framework. Retrieved January 10, 2025, from https://www.justice.gov/archives/ag/page/file/1326061/dl.

United States Department of Justice (U.S. DOJ). 2024. "Man Convicted for $110M Cryptocurrency Scheme." Retrieved January 23, 2025, from https://www.justice.gov/opa/pr/man-convicted-110m-cryptocurrency-scheme.

United States Department of the Treasury (U.S. Treasury). 2023. Illicit Finance Risk Assessment of Decentralized Finance. Retrieved January 23, 2025, from https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

Vashishth, Tarun, Sharma, Mr. Vikas, and Chaudhary, Sachin. 2023. "Privacy and Confidentiality in Permissioned Blockchain Networks: Evaluating Security Models" Future Trends in Business: Knowledge, Skills, Sustainability, Innovation and Technology (FTB-KSSIT-2023): 45. ResearchGate.

Wei, Min, Zhicheng Chenguang, Li Ye, Xiaofei Xue, and Lin Yi. 2024. "A Comprehensive Study of Governance Issues in Decentralised Finance Applications." Cornell University. https://doi.org/10.48550/arXiv.2311.01433

Wylde, Victoria, Rawindaran, N., Lawrence, Jane, *et al.* 2022. "Cybersecurity, Data Privacy and Blockchain: A Review." SN Computer Science 3. https://doi.org/10.1007/s42979-022-01020-4

World Bank. 2021. "Remittance Prices Worldwide." World Bank Database.

World Bank. n.d. Financial Inclusion. Retrieved December 10, 2024, from https://www.worldbank.org/en/topic/financialinclusion.

World Bank (WB) & World Trade Organization (WTO). 2020. "Women and Trade: The Role of Trade in Promoting Gender Equality". Washington, DC: World Bank. doi:10.1596/978-1-4648-1541-6. License: Creative Commons Attribution CC BY 3.0 IGO

Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. 2019. "Blockchain Technology Overview". National Institute of Standards and Technology (NIST), United States Department of Commerce. https://doi.org/10.6028/NIST.IR.8202

Yakubu, Musa M., M. F. B. H. Hassan, Kabiru U. Danyaro, A. Z. Junejo, M. Siraj, S. Yahaya, S. Adamu, and K. Abdulsalam. 2024. "A Systematic Literature Review on Blockchain Consensus Mechanisms' Security: Applications and Open Challenges." Tech Science Press. https://doi.org/10.32604/csse.2024.054556

Zehnder, Jonas. 2024. "An Analysis of the Adaptability of Switzerland's Financial Regulatory Framework to Blockchain and Digital Currency Innovations." Frontiers in Management Science 3(5):47–55. https://doi.org/10.56397/FMS.2024.10.05

Zavolokina, Larisa, Natalia Ziółkowska, Iris Bauer, and Gerhard Schwabe. 2020. "Management, Governance, and Value Creation in a Blockchain Consortium." MIS Quarterly Executive 19(1):1–17. https://doi.org/10.17705/2msqe.00022

Zyskind, Guy, Zekrifa, Djabeur, Zekrifa, Djabeur, Alex, Pentland & Nathan, Oz. 2015. "Decentralizing Privacy: Using Blockchain to Protect Personal Data". 2015 IEEE Security and Privacy Workshops, 180–184. https://doi.org/10.1109/SPW.2015.27

Received on 10-12-2024 Accepted on 02-01-2025 Published on 10-02-2025

https://doi.org/10.6000/1929-4409.2025.14.03