OPEN ACCESS
Finance & Accounting Research Journal
P-ISSN: 2708-633X, E-ISSN: 2708-6348
Volume 6, Issue 7, P.No. 1205-1223, July 2024
DOI: 10.51594/farj.v6i7.1313
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/farj

Legal frameworks for digital transactions: Analyzing the impact of Blockchain technology

Adah Dominic Ochigbo[1], Amardas Tuboalabo[2], Talabi Temitope Labake[3], Ushena Buinwi[4] Oluwabunmi Layode[5], & Jumai Adama Buinwi[6]

[1]Independent Researcher, Lagos, Nigeria
[2]Independent Researcher, Hull City, UK
[3]Independent Researcher, Sheffield, UK
[4]Independent Researcher, Yaounde, Cameroon
[5]Independent Researcher, Maryland, USA
[6]Independent Researcher, Douala, Cameroon

*Corresponding Author: Adah Dominic Ochigbo
Corresponding Author Email: adahdominicochigbo@yahoo.com

Article Received: 01-02-24 **Accepted:** 30-04-24 **Published:** 17-07-24

ABSTRACT

This study explores the legal frameworks governing digital transactions, with a specific focus on the transformative impact of blockchain technology. The primary aim is to elucidate the complexities and challenges posed by blockchain while examining the diverse regulatory approaches adopted internationally. Through a comprehensive literature review and comparative analysis, the research addresses key aspects such as the conceptual framework of digital transactions, the unique characteristics of blockchain, and the regulatory strategies implemented across different jurisdictions. The findings reveal that blockchain technology, characterized by its decentralized, immutable, and transparent nature, significantly disrupts traditional regulatory models. Identified challenges include jurisdictional ambiguities, enforcement difficulties, and privacy concerns. The comparative analysis shows divergent regulatory approaches: supportive frameworks in Japan and Switzerland contrast sharply with restrictive measures in China, highlighting the necessity for international cooperation and harmonization of regulations. The study concludes that effective regulation of blockchain technology requires innovative and flexible legal frameworks capable of adapting to rapid technological advancements. Policymakers must balance fostering innovation and protecting public interests,

emphasizing the need for privacy-preserving technologies and international standards. Recommendations include developing global regulatory standards, enhancing privacy measures, and creating legal frameworks that accommodate the decentralized nature of blockchain systems. This research provides valuable insights for regulators, policymakers, and stakeholders, offering a pathway towards a secure, transparent, and innovative digital economy. Continuous adaptation and international collaboration are imperative to address emerging challenges and fully harness the potential of blockchain technology. The study advocates for proactive engagement and cooperation among nations to create a cohesive regulatory environment that promotes innovation while safeguarding public interests, enabling the global community to navigate the complexities of blockchain technology and unlock its full potential for economic and social advancement.

Keywords: Blockchain Technology, Digital Transactions, Legal Frameworks, Regulatory Challenges, International Cooperation, Privacy Concerns.

INTRODUCTION

Digital transactions have revolutionized the way financial and business operations are conducted globally. The emergence of blockchain technology has introduced a new paradigm in digital transactions, characterized by enhanced security, transparency and efficiency. This review paper seeks to explore the legal frameworks governing digital transactions with a particular focus on the impact of blockchain technology. The rapid advancement in technology has necessitated a comprehensive examination of existing legal structures to ensure they can accommodate these innovations while safeguarding public interest.

Digital transactions encompass various activities, including e-commerce, digital banking and cryptocurrency exchanges (Abdullah, Ward and Ahmed, 2016). The convenience and efficiency provided by these transactions have led to their widespread adoption. However, this growth has also highlighted the need for robust legal frameworks to address issues related to security, privacy and fraud. Traditional financial systems have well-established regulatory measures, but the decentralized nature of blockchain technology introduces unique challenges that necessitate specialized legal attention (Baidoo, 2019).

Blockchain technology, as described by Antonopoulos (2014), is a distributed ledger system that allows for the secure, transparent and tamper-proof recording of transactions. This technology underpins cryptocurrencies like Bitcoin and has potential applications across various industries, including finance, supply chain management, and healthcare. The decentralization feature of blockchain removes the need for intermediaries, thereby reducing transaction costs and increasing efficiency (Catalini and Gans, 2020). However, this also poses regulatory challenges as traditional oversight mechanisms may not be directly applicable.

The current legal frameworks for digital transactions vary significantly across jurisdictions. International laws and standards aim to provide a unified approach, but country-specific regulations reflect the diverse legal landscapes and priorities of different regions (Davidson, De Filippi & Potts, 2018). Privacy and security are critical considerations in these frameworks, as digital transactions often involve sensitive personal and financial information. The General Data Protection Regulation (GDPR) in the European Union, for instance, sets stringent requirements for data protection, impacting how digital transactions are conducted within and outside Europe (Fairfield, 2014).

Blockchain's decentralization presents a significant departure from traditional centralized systems. This shift requires a rethinking of existing legal frameworks to address issues such as jurisdiction, enforcement, and compliance. The immutable nature of blockchain records means that once data is entered, it cannot be altered or deleted, posing challenges for data privacy regulations like the GDPR, which grants individuals the right to have their data erased (Murray, 2013). Additionally, the pseudonymous nature of blockchain transactions complicates the enforcement of anti-money laundering (AML) and counter-terrorism financing (CTF) regulations.

Risius and Spohrer (2017) propose a blockchain research framework that highlights the interplay between technological capabilities and regulatory requirements. Their framework suggests that while blockchain can enhance transaction security and transparency, it also necessitates new legal approaches to address potential misuse and ensure compliance with existing laws. The decentralized and global nature of blockchain transactions means that regulatory measures must be internationally coordinated to be effective.

Emerging technologies such as smart contracts and decentralized finance (DeFi) platforms further complicate the regulatory landscape. Smart contracts are self-executing contracts with the terms of the agreement directly written into code. These contracts run on blockchain networks, automating transactions and reducing the need for intermediaries. However, their automated nature raises questions about liability and enforceability in cases of disputes or errors (Radziwill, 2018).

The aim of this review paper is to provide a comprehensive analysis of the legal frameworks governing digital transactions and the transformative impact of blockchain technology. The objective is to identify the gaps and challenges in existing legal structures and propose potential solutions to address these issues. The scope of the study includes an examination of international and country-specific regulations, the role of blockchain in digital transactions, and the future trends and legal developments in this area. This paper will contribute to the ongoing discourse on how legal systems can adapt to accommodate technological advancements while ensuring the protection of stakeholders involved in digital transactions

Conceptual Framework of Legal Frameworks for Digital Transactions

The conceptual framework for legal structures governing digital transactions is inherently complex, reflecting the multifaceted nature of digital finance and the rapid advancement of blockchain technology. Digital transactions, including activities such as e-commerce, digital banking and cryptocurrency exchanges, require robust legal frameworks to address issues related to security, privacy, and fraud (Albshaier et al., 2024). As digital transactions continue to grow in scale and importance, the necessity for a comprehensive legal framework that can effectively govern these activities becomes increasingly critical.

Blockchain technology, characterized by its decentralized and transparent nature, presents both opportunities and challenges for the legal regulation of digital transactions. The removal of traditional intermediaries through decentralization reduces transaction costs and enhances efficiency. However, this same decentralization complicates regulatory oversight, as conventional regulatory mechanisms typically rely on central control points (Alston, 2022). The immutability and transparency of blockchain transactions enhance security but also raise concerns regarding privacy and the right to be forgotten, as enshrined in regulations like the

General Data Protection Regulation (GDPR) in the European Union (Campbell-Verduyn, 2018).

Existing legal frameworks for digital transactions vary significantly across jurisdictions. Internationally, efforts have been made to harmonize regulations, but discrepancies remain due to differing national priorities and legal traditions. For instance, the European Union has taken a proactive stance with regulations such as the GDPR and the Payment Services Directive 2 (PSD2), which aim to enhance consumer protection and promote competition in digital payments (Li et al., 2020). Conversely, the regulatory approach in the United States is more fragmented, with state-level regulations supplementing federal laws, resulting in a complex and sometimes inconsistent legal landscape (Turk, 2019).

Blockchain technology's impact on transforming digital transactions is immense. It offers a secure and transparent way to record transactions, which can substantially reduce fraud risk and enhance trust among users (Muminova et al., 2020). This technology underpins cryptocurrencies like Bitcoin and has potential applications in various sectors, including supply chain management, healthcare, and finance. The decentralized nature of blockchain, however, poses significant challenges for regulators. Traditional legal frameworks are designed to regulate centralized entities, and the absence of a central authority in blockchain networks complicates enforcement and compliance (Reyes, 2016).

One of the primary challenges in regulating blockchain technology is addressing the issue of jurisdiction. Blockchain networks operate globally, transcending national borders, which raises questions about which jurisdiction's laws apply in case of disputes or regulatory actions. This issue is further complicated by the pseudonymous nature of many blockchain transactions, which can make it difficult to identify and hold accountable the parties involved (Wright & De Filippi, 2015). These challenges necessitate a reevaluation of existing legal principles and the development of new regulatory approaches that can effectively govern decentralized technologies.

The concept of lex cryptographia, or law created through cryptographic code, has emerged as a potential solution to some of these regulatory challenges. Lex cryptographia suggests that blockchain technology itself can enforce certain rules and regulations through code, eliminating the need for traditional legal enforcement mechanisms. This concept has the potential to revolutionize the regulation of digital transactions but also raises significant legal and ethical questions (Agnikhotram & Kouroutakis, 2018). For instance, the rigidity of code-based rules can be both advantageous and disadvantageous, as it can prevent arbitrary enforcement but also make it challenging to adapt to new circumstances or correct errors.

Future developments in the legal regulation of digital transactions will likely involve a combination of traditional legal frameworks and innovative approaches that leverage the capabilities of blockchain technology. This hybrid approach can provide the flexibility needed to address the unique challenges posed by decentralized technologies while ensuring that fundamental legal principles, such as consumer protection and privacy, are upheld (Campbell-Verduyn, 2018). International cooperation and coordination will be essential in developing a coherent and effective regulatory framework for digital transactions.

The Digital Transaction Ecosystem: An Overview

The digital transaction ecosystem has revolutionized the global financial landscape, enhancing efficiency, innovation and accessibility in financial and business operations. This

ecosystem includes a broad range of activities such as e-commerce, digital banking and cryptocurrency exchanges, which are becoming essential to modern economic systems (Riasanow et al., 2018). A thorough understanding of this ecosystem necessitates a comprehensive analysis of its components, key players and the technological advancements propelling its evolution.

Digital transactions are fundamentally transactions conducted electronically, involving the transfer of value or information over digital platforms. These transactions include online shopping, digital payments and peer-to-peer (P2P) transfers, among others. The rise of e-commerce platforms like Amazon and Alibaba has significantly boosted digital transactions, making it easier for consumers to purchase goods and services online (Ekbia & Nardi, 2017). Digital banking services provided by traditional banks and fintech companies further facilitate the convenience and speed of financial transactions, allowing users to perform banking activities through digital channels.

Cryptocurrency exchanges represent another critical component of the digital transaction ecosystem. These platforms enable the trading of digital currencies like Bitcoin, Ethereum and numerous altcoins. Cryptocurrencies, underpinned by blockchain technology, offer a decentralized alternative to traditional fiat currencies, providing users with a means of conducting transactions without the need for intermediaries (Radziwill, 2018). The popularity of cryptocurrencies has grown exponentially, driven by their potential for high returns and the increasing acceptance of digital assets in mainstream finance.

The primary players in the digital transaction ecosystem encompass traditional financial institutions, fintech companies, e-commerce giants and cryptocurrency exchanges. Traditional banks have been instrumental in enabling digital transactions through online banking services and digital payment solutions. Fintech companies, utilizing innovative technologies, have disrupted conventional banking models by providing user-friendly digital financial services (Anand & Mantrala, 2019). E-commerce giants such as Amazon and Alibaba dominate the online retail sector, generating significant volumes of digital transactions. Cryptocurrency exchanges like Coinbase and Binance are vital in the trading and management of digital assets.

Technological advancements have been instrumental in shaping the digital transaction ecosystem. Blockchain technology, in particular, has revolutionized digital transactions by providing a secure, transparent and decentralized method of recording transactions. Blockchain's attributes of immutability and decentralization enhance the security and trustworthiness of digital transactions, reducing the risk of fraud and enhancing privacy (Kshetri, 2017). Additionally, the development of secure payment gateways and digital wallets has facilitated the ease and safety of online transactions, further boosting consumer confidence in digital commerce.

Despite the numerous advantages, the digital transaction ecosystem also faces significant challenges. Cybersecurity remains a paramount concern, as digital transactions are vulnerable to hacking, phishing, and other forms of cyberattacks. Ensuring the security of digital transactions requires robust cybersecurity measures and continuous monitoring to detect and mitigate threats (Murray, 2013). Privacy issues also arise, particularly concerning the handling and protection of sensitive personal and financial information. Regulations like the

General Data Protection Regulation (GDPR) aim to address these concerns by setting stringent data protection standards.

The regulatory landscape for digital transactions is complex and varies across jurisdictions. Different countries have adopted diverse approaches to regulating digital transactions, reflecting their unique legal, economic and cultural contexts. In the European Union, regulations like GDPR and the Payment Services Directive 2 (PSD2) provide a comprehensive framework for protecting consumer rights and promoting competition in digital payments. In contrast, the regulatory environment in the United States is more fragmented, with a combination of federal and state-level regulations governing digital transactions (Murray, 2013).

Existing Legal Frameworks for Digital Transactions.

The existing legal frameworks governing digital transactions are diverse and multifaceted, reflecting the complexities of a rapidly evolving technological landscape. These frameworks encompass international laws, country-specific regulations and standards designed to address various issues such as security, privacy and consumer protection. As digital transactions become increasingly integral to the global economy, understanding these legal structures is crucial for ensuring their effective regulation and oversight.

Internationally, several frameworks aim to harmonize the regulation of digital transactions. One significant example is the General Data Protection Regulation (GDPR) enacted by the European Union (EU). The GDPR sets stringent standards for data protection and privacy, requiring organizations to implement robust measures to safeguard personal data. It also grants individuals significant rights over their data, including the right to access, rectify, and erase their information. The GDPR has had a profound impact not only within the EU but also globally, as companies worldwide must comply with its provisions when handling the data of EU citizens (Murray, 2013).

In the realm of digital payments, the Payment Services Directive 2 (PSD2) stands as a crucial legal framework within the EU. PSD2 aims to bolster consumer protection, stimulate competition and encourage innovation in the financial services sector. It requires strong customer authentication for online transactions and opens the market to third-party payment service providers, thereby fostering the development of new and innovative payment solutions (Polasik et al., 2020). Additionally, the directive seeks to enhance transparency and reduce fraud in digital payments, contributing to a safer and more secure digital transaction environment.

In the United States, the regulatory landscape for digital transactions is fragmented, comprising both federal and state-level regulations. The Electronic Fund Transfer Act (EFTA) and the Gramm-Leach-Bliley Act (GLBA) are two significant federal laws governing digital transactions. The EFTA defines the rights and responsibilities of consumers and financial institutions in electronic fund transfers, while the GLBA mandates financial institutions to protect consumers' financial information by imposing data safeguarding requirements (Gibney et al., 2016). Additionally, state-level regulations like the California Consumer Privacy Act (CCPA) enhance privacy protections by granting consumers greater control over their personal information.

The emergence of blockchain technology has introduced new challenges and opportunities for legal frameworks governing digital transactions. Blockchain's decentralized and

transparent nature offers significant advantages, such as enhanced security and reduced fraud. However, it also complicates regulatory oversight, as traditional legal mechanisms often rely on centralized control points. To address these challenges, some jurisdictions have begun to develop specific regulations for blockchain and cryptocurrency activities. For instance, the EU's Fifth Anti-Money Laundering Directive (5AMLD) extends anti-money laundering (AML) and counter-terrorism financing (CTF) regulations to cryptocurrency exchanges and wallet providers, requiring them to implement customer due diligence measures and report suspicious activities (Campbell-Verduyn, 2018).

At the national level, countries like Japan and Switzerland have implemented comprehensive legal frameworks for regulating cryptocurrencies and blockchain technology. Japan's Payment Services Act, amended in 2017, acknowledges cryptocurrencies as a legal method of payment and imposes regulatory requirements on cryptocurrency exchanges. These requirements include registration with the Financial Services Agency (FSA) and compliance with AML and CTF standards (Girasa, 2018). Switzerland has adopted a similar approach, with its Financial Market Supervisory Authority (FINMA) providing guidelines for initial coin offerings (ICOs) and classifying tokens into different categories based on their economic function (Risius & Spohrer, 2017).

Despite these efforts, significant challenges remain in developing effective legal frameworks for digital transactions. One major issue is jurisdictional ambiguity, as digital transactions often transcend national borders, making it difficult to determine which laws apply in specific cases. This is particularly relevant for blockchain transactions, where the decentralized nature of the technology complicates the identification of the parties involved and the enforcement of legal obligations (Kshetri, 2017). Furthermore, the rapid pace of technological innovation outstrips the ability of regulators to keep up, resulting in regulatory gaps and inconsistencies that can be exploited by bad actors.

To address these challenges, international cooperation and coordination are essential. Efforts such as the Financial Action Task Force (FATF) recommendations on virtual assets and virtual asset service providers (VASPs) represent important steps towards developing a harmonized global framework for regulating digital transactions. These recommendations provide guidelines for countries to implement AML and CTF measures for virtual assets, including the registration and supervision of VASPs, the application of customer due diligence measures and the reporting of suspicious transactions (Campbell-Verduyn, 2018).

Introduction to Blockchain Technology

Blockchain technology, initially conceptualized by the pseudonymous figure Nakamoto (2008), has emerged as a revolutionary force in the realm of digital transactions. Blockchain, at its core, is a decentralized and distributed ledger that records transactions across multiple computers in such a way that the registered transactions cannot be altered retroactively (Nakamoto, 2008). This introduction to blockchain technology elucidates its foundational principles, operational mechanics, types and its profound implications for various sectors.

Blockchain technology operates on the principles of decentralization, immutability and transparency. Unlike traditional centralized databases, where a single entity has control over the data, a blockchain is managed by a network of nodes, each holding a copy of the ledger. This decentralization ensures that no single point of failure exists, enhancing the security and resilience of the system (Pilkington, 2016). Moreover, once a transaction is recorded on the

blockchain, it cannot be altered or deleted, ensuring the immutability of data. This feature is critical for maintaining the integrity and trustworthiness of the information stored on the blockchain. Transparency is also a key characteristic, as all transactions are visible to all participants in the network, fostering an environment of accountability and trust. The combination of these principles makes blockchain a revolutionary technology with the potential to transform various industries, from finance to supply chain management. The immutability of blockchain comes from its cryptographic nature; once a transaction is recorded, it is virtually impossible to alter. This feature is achieved through cryptographic hashing and the consensus mechanisms that validate and confirm transactions across the network (Zheng et al., 2017).

A blockchain is composed of blocks, each containing a list of transactions. These blocks are linked to one another in a chronological order, forming a chain. Each block has a cryptographic hash of the previous block, a timestamp, and transaction data. The linking of blocks ensures the integrity and consistency of the entire ledger. Any attempt to alter a single block would require the modification of all subsequent blocks, which is computationally infeasible (Swan, 2015).

Consensus mechanisms are essential for the operation of blockchain networks, ensuring that all nodes in the network concur on the validity of transactions and the state of the ledger. The most famous consensus mechanism is Proof of Work (PoW), utilized by Bitcoin, where miners solve intricate mathematical problems to validate transactions and generate new blocks. Other consensus mechanisms include Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT), each offering its unique benefits and trade-offs (Sheikh, Azmathullah & Rizwan, 2018).

There are various types of blockchains, each serving different purposes and use cases. Public blockchains, like Bitcoin and Ethereum, are open to anyone and are characterized by their high level of decentralization. These blockchains are permissionless, meaning that anyone can participate in the network and validate transactions (Radziwill, 2018). Private blockchains, on the other hand, are restricted and typically used within organizations. They offer greater control over the network and are often used for internal purposes where privacy and control are paramount. Consortium blockchains fall between public and private blockchains, where a group of organizations collaboratively manage the network, balancing decentralization and control.

The implications of blockchain technology extend far beyond digital currencies. In finance, blockchain enables secure and transparent transactions, reducing the need for intermediaries and lowering transaction costs. Smart contracts, which are self-executing contracts with the terms directly written into code, have the potential to automate and streamline complex processes in various industries, including supply chain management, real estate and insurance (Catalini and Gans, 2020). In supply chain management, blockchain offers end-to-end visibility and traceability, improving transparency and reducing fraud (Oriekhoe et al., 2024).

Blockchain also plays a significant role in enhancing cybersecurity and protecting privacy. The decentralized nature of blockchain makes it resilient against attacks, as compromising a single node does not affect the entire network. Additionally, the cryptographic techniques used in blockchain ensure the confidentiality and integrity of data, providing robust security measures against unauthorized access and tampering (Kshetri, 2017). Furthermore,

blockchain's potential for creating decentralized identity systems can offer individuals greater control over their personal information, reducing the risks associated with centralized data breaches.

The future of blockchain technology is promising, with ongoing research and development aimed at addressing its current limitations and expanding its applications. Scalability remains a significant challenge, as most blockchain networks struggle to handle a high volume of transactions efficiently. Solutions such as sharding, off-chain transactions, and second-layer protocols are being explored to enhance scalability and performance (Zheng et al., 2017). Moreover, the integration of blockchain with other emerging technologies, such as the Internet of Things (IoT) and artificial intelligence (AI), is expected to unlock new possibilities and drive further innovation.

Impact of Blockchain on Legal Frameworks

The advent of blockchain technology has significantly influenced legal frameworks across the globe, prompting regulators to re-evaluate and adapt existing laws to accommodate the unique characteristics of decentralized systems. Blockchain's impact on legal frameworks is multifaceted, encompassing areas such as financial regulation, data protection, contract law and intellectual property. This section explores the transformative effects of blockchain technology on these legal domains and the challenges and opportunities it presents for regulators and policymakers.

Blockchain's decentralized nature fundamentally disrupts traditional regulatory approaches that depend on centralized intermediaries for enforcement and compliance. In financial regulation, blockchain facilitates peer-to-peer transactions without intermediaries like banks or payment processors. While this decentralization lowers transaction costs and enhances efficiency, it also complicates the enforcement of regulatory standards meant to ensure market integrity and protect consumers (Javaid et al., 2022). For instance, the pseudonymous nature of blockchain transactions poses challenges for anti-money laundering (AML) and counter-terrorism financing (CTF) regulations, which traditionally depend on intermediaries to monitor and report suspicious activities (Kshetri, 2017).

To address these challenges, regulators are exploring new approaches that leverage the transparency and traceability inherent in blockchain technology. For example, the Financial Action Task Force (FATF) has issued guidelines recommending that virtual asset service providers (VASPs), including cryptocurrency exchanges, implement robust customer due diligence measures and report suspicious transactions. These guidelines aim to balance the benefits of blockchain's transparency with the need for effective regulatory oversight (Reyes, 2016). Additionally, certain jurisdictions have implemented specific regulations for blockchain and cryptocurrency activities. For example, Japan's Payment Services Act mandates that cryptocurrency exchanges register with the Financial Services Agency (FSA) and comply with AML and CTF standards. This regulatory framework supports innovation while ensuring consumer protection (Morishita, 2020).

Blockchain's influence on data protection and privacy is a significant concern for legal frameworks. The immutability of blockchain records, which enhances security and trust, clashes with data protection principles like the right to be forgotten, as outlined in the General Data Protection Regulation (GDPR) in the European Union. The GDPR grants individuals the right to request the deletion of their personal data, a provision that is challenging to align

with blockchain's permanent and unalterable nature (Jiménez-Gómez, 2019). To address this issue, some blockchain implementations are exploring solutions such as off-chain storage, where personal data is stored off the blockchain, with only cryptographic hashes or references recorded on-chain. This approach aims to balance the benefits of blockchain's immutability with the need to comply with data protection regulations (Murray, 2013).

In the realm of contract law, blockchain has introduced the concept of smart contracts—self-executing contracts with the terms of the agreement directly written into code. Smart contracts automate the execution of contractual terms, reducing the need for intermediaries and enhancing efficiency. However, the legal status and enforceability of smart contracts remain uncertain, as traditional legal principles are not easily applicable to code-based agreements. Issues such as the interpretation of contractual terms, liability for code errors, and the resolution of disputes arising from smart contracts present significant challenges for regulators and courts (Wright & De Filippi, 2015). Certain jurisdictions are starting to tackle these challenges by creating legal frameworks that acknowledge and regulate smart contracts. For example, Arizona in the United States has passed legislation that gives legal recognition to smart contracts and blockchain signatures, offering a level of legal certainty for parties involved in blockchain-based transactions (McKinney, Landy & Wilka, 2017).

Intellectual property (IP) law is being transformed by blockchain technology. Blockchain's capability to provide a secure and unalterable record of IP rights, such as copyrights, patents and trademarks, presents new possibilities for the management and enforcement of IP. Recording IP rights on a blockchain allows creators and rights holders to establish a verifiable and tamper-proof record of ownership and rights transfer, reducing disputes and enhancing IP protection. Additionally, blockchain-based platforms can facilitate the licensing and monetization of IP through smart contracts, automating royalty payments and ensuring fair compensation for creators (Bodó, Gervais & Quintais, 2018).

Despite the potential benefits, the integration of blockchain into legal frameworks poses significant challenges. The rapid pace of technological innovation often outstrips the ability of regulators to keep up, resulting in regulatory gaps and inconsistencies. Moreover, the global nature of blockchain networks requires international cooperation and harmonization of legal standards to ensure effective regulation and enforcement. Policymakers must balance the need to protect consumers and maintain market integrity with the desire to foster innovation and support the development of new technologies (Kshetri, 2017).

Challenges in Regulating Blockchain Technology

Blockchain technology presents unique regulatory challenges due to its decentralized nature, immutability and global reach. As this technology continues to evolve and integrate into various sectors, regulators worldwide face the daunting task of developing frameworks that can effectively address its complexities while fostering innovation. This section explores the key challenges in regulating blockchain technology, including jurisdictional issues, enforcement difficulties, privacy concerns and the balancing act between innovation and regulation.

A major challenge in regulating blockchain technology is its decentralized nature, which challenges traditional regulatory approaches that depend on centralized control points. In a decentralized blockchain network, there is no single entity for regulators to hold accountable. This absence of a central authority complicates the enforcement of existing laws and

regulations, which are generally designed to oversee centralized institutions (Zwitter & Hazenberg, 2020).

For instance, in financial markets, regulators typically depend on banks and other financial intermediaries to monitor and report suspicious activities. However, in a decentralized blockchain system, transactions take place directly between users, bypassing traditional intermediaries and creating significant regulatory blind spots (Quintais et al., 2019).

Jurisdictional issues further complicate the regulation of blockchain technology. Blockchain networks operate globally, transcending national borders, which raises questions about which jurisdiction's laws apply in case of disputes or regulatory actions. The pseudonymous nature of many blockchain transactions adds another layer of complexity, making it difficult to identify the parties involved and enforce legal obligations. This jurisdictional ambiguity poses significant challenges for regulators, who must navigate a patchwork of national laws and regulations to effectively oversee blockchain activities (Reyes, 2016).

The immutability of blockchain records, while enhancing security and trust, conflicts with data protection principles such as the right to be forgotten, as enshrined in the General Data Protection Regulation (GDPR) in the European Union. The GDPR grants individuals the right to request the deletion of their personal data, a provision that is difficult to reconcile with blockchain's permanent and unalterable nature (Murray, 2013). This conflict highlights the need for innovative regulatory approaches that can balance the benefits of blockchain's immutability with the requirements of data protection laws.

Privacy concerns also emerge within the context of blockchain technology. While blockchain offers transparency and traceability, it also presents significant privacy challenges. Public blockchains, specifically, enable anyone to view transaction histories, potentially exposing sensitive information. Although transactions on public blockchains are pseudonymous, advanced techniques can be employed to de-anonymize users and track their activities (Wang & Kogan, 2018). Consequently, regulators must address these privacy concerns by implementing measures that safeguard users' identities without compromising the transparency and security advantages of blockchain.

Enforcement difficulties present a significant challenge in regulating blockchain technology. Traditional regulatory enforcement mechanisms, such as audits and inspections, are not easily applicable to decentralized blockchain networks. The pseudonymous nature of blockchain transactions complicates the identification and prosecution of bad actors, while the global reach of blockchain networks adds complexity to cross-border enforcement (Bakhshi & Ghita, 2021). To address these challenges, regulators may need to develop new enforcement tools and collaborate more closely with international counterparts to ensure effective oversight.

The rapid pace of technological innovation in the blockchain space often outstrips the ability of regulators to keep up, resulting in regulatory gaps and inconsistencies. Blockchain technology is constantly evolving, with new applications and use cases emerging regularly. This dynamic environment makes it challenging for regulators to develop comprehensive and up-to-date legal frameworks (Wright & De Filippi, 2015). To address this issue, regulators must adopt flexible and adaptive approaches that can accommodate the rapid evolution of blockchain technology while ensuring that fundamental legal principles, such as consumer protection and market integrity, are upheld.

Another significant challenge is finding the right balance between regulation and innovation. Excessive regulations can suppress innovation and deter the adoption of blockchain technology, while inadequate regulation can result in regulatory arbitrage and exploitation by bad actors. Therefore, policymakers must carefully design their regulatory approaches to foster innovation and economic growth while mitigating risks and safeguarding public interests (Panait, Ljubenkov & Alic, 2021). This balancing act requires a deep understanding of the technology and its potential implications, as well as ongoing dialogue with industry stakeholders and experts.

To address these challenges, certain jurisdictions have started to develop specific regulations for blockchain and cryptocurrency activities. For example, the European Union's Fifth Anti-Money Laundering Directive (5AMLD) extends anti-money laundering (AML) and counter-terrorism financing (CTF) regulations to cryptocurrency exchanges and wallet providers, mandating them to implement customer due diligence measures and report suspicious activities (Bebris & Mukkamala, 2018). Similarly, Japan's Payment Services Act mandates that cryptocurrency exchanges register with the Financial Services Agency (FSA) and adhere to AML and CTF standards, providing a regulatory framework that supports innovation while protecting consumers (Reyes, 2016).

Comparative Analysis of International Legal Approaches

The regulation of blockchain technology varies significantly across different jurisdictions, reflecting a range of approaches and priorities. This comparative analysis explores how various countries and regions are addressing the legal challenges posed by blockchain, highlighting the diversity in regulatory frameworks and the implications for global blockchain adoption.

European Union

The European Union (EU) has adopted a proactive approach to regulating blockchain and cryptocurrencies, emphasizing consumer protection, market integrity and anti-money laundering (AML) measures. The EU's Fifth Anti-Money Laundering Directive (5AMLD) expanded AML and counter-terrorism financing (CTF) regulations to cover virtual currency exchanges and wallet providers. This directive requires these entities to implement customer due diligence measures and report suspicious activities to the relevant authorities (Karasek-Wojciechowicz, 2021). Furthermore, the EU has been investigating the potential of blockchain to enhance transparency and efficiency in various sectors, including finance and supply chain management.

United States

In the United States, the regulatory landscape for blockchain and cryptocurrencies is more fragmented, with a mix of federal and state-level regulations. Federal agencies such as the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Financial Crimes Enforcement Network (FinCEN) have issued guidelines and enforcement actions pertaining to digital assets. The SEC focuses on regulating initial coin offerings (ICOs) as securities, while the CFTC oversees cryptocurrency derivatives markets (Reyes, 2016). State-level regulations, such as New York's BitLicense, impose additional compliance requirements on cryptocurrency businesses, adding to the complexity of the regulatory environment (Murray, 2013).

Japan

Japan has positioned itself as a leader in blockchain regulation by recognizing cryptocurrencies as legal payment methods under its Payment Services Act. This act requires cryptocurrency exchanges to register with the Financial Services Agency (FSA) and comply with strict AML and CTF standards (Lindsay, 2022). Japan's regulatory approach seeks to balance innovation with consumer protection, creating a secure and transparent environment for cryptocurrency transactions. Additionally, the country has established a self-regulatory organization, the Japan Virtual Currency Exchange Association (JVCEA), to promote best practices within the industry.

Switzerland

Switzerland has established itself as a crypto-friendly jurisdiction by providing a supportive regulatory framework for blockchain and cryptocurrency activities. The Swiss Financial Market Supervisory Authority (FINMA) has issued comprehensive guidelines for initial coin offerings (ICOs), categorizing tokens into three types: payment tokens, utility tokens, and asset tokens. This classification helps determine the regulatory requirements applicable to different types of digital assets (Novak, 2020). Switzerland's approach emphasizes legal clarity and regulatory certainty, attracting numerous blockchain startups to its "Crypto Valley" in Zug.

Singapore

Singapore is another key player in the global blockchain regulatory landscape, known for its progressive and adaptive approach. The Monetary Authority of Singapore (MAS) has implemented a regulatory framework for digital payment tokens under the Payment Services Act, which requires service providers to obtain licenses and comply with AML and CTF obligations (Zohar, 2015). Singapore's regulatory environment is designed to support innovation while ensuring financial stability and consumer protection. The city-state also promotes blockchain research and development through initiatives like the Singapore Blockchain Innovation Programme.

China

China has adopted a more restrictive stance on blockchain and cryptocurrencies, imposing stringent regulations to mitigate financial risks and maintain control over capital flows. The People's Bank of China (PBOC) has banned initial coin offerings (ICOs) and shut down domestic cryptocurrency exchanges, while simultaneously exploring the potential of blockchain technology for applications such as digital currency issuance and supply chain management (Wright & De Filippi, 2015). Despite the ban on cryptocurrencies, China remains committed to blockchain innovation, as evidenced by its development of a central bank digital currency (CBDC).

Australia

Australia's regulatory approach to blockchain and cryptocurrencies focuses on integrating these technologies within its existing legal framework. The Australian Securities and Investments Commission (ASIC) oversees the regulation of initial coin offerings (ICOs) and cryptocurrency exchanges, ensuring compliance with securities laws and AML/CTF requirements (Reyes, 2016). Additionally, the Australian Transaction Reports and Analysis Centre (AUSTRAC) mandates that cryptocurrency exchanges register and implement customer due diligence measures. Australia's regulatory stance aims to promote innovation while safeguarding financial integrity and consumer protection.

Comparative Insights

The comparative analysis of international legal approaches to blockchain regulation reveals several key insights. First, there is a clear divergence in regulatory philosophies, with some jurisdictions adopting supportive and innovative frameworks, while others impose stringent restrictions. Countries like Japan, Switzerland, and Singapore exemplify a balanced approach that fosters innovation while ensuring regulatory compliance and consumer protection. In contrast, China's restrictive measures highlight concerns over financial stability and capital control, demonstrating a more cautious stance towards cryptocurrency activities.

Secondly, the diverse regulatory environments across different jurisdictions highlight the need for international cooperation and harmonization. Since blockchain technology extends beyond national borders, coordinated efforts are crucial to tackle regulatory challenges, prevent arbitrage and promote global standards. Initiatives like the Financial Action Task Force (FATF) guidelines on virtual assets offer a basis for international collaboration, helping to align regulatory approaches and mitigate the risks associated with blockchain and cryptocurrencies (Lehmann, 2020).

Future Trends and Legal Developments

The future of blockchain technology is poised to bring significant transformations across various sectors, accompanied by evolving legal frameworks aimed at addressing the complexities and challenges posed by this disruptive innovation. As blockchain technology continues to mature, several trends and legal developments are expected to shape its trajectory.

One of the prominent trends is the integration of blockchain with other emerging technologies such as artificial intelligence (AI), the Internet of Things (IoT) and quantum computing. The convergence of these technologies can enhance blockchain’s capabilities, leading to more secure, efficient and scalable solutions. For instance, AI can improve the accuracy of smart contracts by providing predictive analytics, while IoT devices can utilize blockchain for secure and transparent data exchanges (Zheng et al., 2017). Quantum computing, while presenting a potential threat to the cryptographic security of blockchain, also offers opportunities to develop more advanced encryption methods (Cherbal et al., 2024).

Decentralized Finance (DeFi) is another area witnessing rapid growth and innovation. DeFi leverages blockchain to create decentralized financial instruments, including lending, borrowing and trading platforms, without traditional intermediaries like banks. This movement towards decentralized financial ecosystems is reshaping the financial industry, necessitating the development of new regulatory frameworks to address issues such as consumer protection, market integrity and systemic risk (Radziwill, 2018). Regulators will need to balance fostering innovation with ensuring these platforms are secure and operate within legal boundaries.

. Central Bank Digital Currencies (CBDCs) signify a major advancement at the crossroads of blockchain technology and monetary policy. Numerous countries are currently exploring or testing CBDCs, which are digital equivalents of national currencies issued by central banks. CBDCs are designed to leverage the advantages of blockchain technology, including enhanced efficiency and security, while preserving regulatory oversight and control over monetary policy (Petare et al., 2024). Implementing CBDCs necessitates the establishment of

comprehensive legal frameworks to address concerns related to privacy, security and cross-border transactions.

The evolution of blockchain governance models represents a significant trend. Traditional governance models for blockchain networks have utilized consensus mechanisms like Proof of Work (PoW) and Proof of Stake (PoS). However, these models encounter challenges related to scalability, energy consumption and centralization. Emerging governance models, such as Decentralized Autonomous Organizations (DAOs), provide new methods for managing blockchain networks through decentralized decision-making processes (Li, Wei & He, 2020). Legal frameworks must adapt to these new governance structures, addressing issues of liability, accountability and legal recognition.

Privacy and data protection will continue to be at the forefront of legal developments in blockchain technology. The immutable nature of blockchain records poses challenges for compliance with data protection regulations such as the General Data Protection Regulation (GDPR) in the European Union. Future legal frameworks will need to address the tension between blockchain's transparency and the right to privacy, potentially through innovations such as zero-knowledge proofs and off-chain data storage solutions (Murray, 2013). These technologies can enable compliance with privacy laws while preserving the integrity and security of blockchain systems.

The rise of tokenization is another trend poised to shape the future of blockchain and its legal framework. Tokenization involves representing real-world assets, such as real estate, stocks and art, as digital tokens on a blockchain. This process can enhance liquidity, lower transaction costs, and democratize access to investment opportunities. However, the tokenization of assets also introduces legal challenges concerning property rights, securities regulation and contractual obligations (Garcia-Teruel & Simón-Moreno, 2021). Regulators must develop frameworks that provide legal clarity and protect investors while encouraging the growth of tokenized markets.

International cooperation and harmonization of blockchain regulations are essential for addressing the global scope of blockchain networks. As blockchain technology crosses national borders, varying regulatory approaches can lead to regulatory arbitrage and uncertainty. Collaborative efforts, such as the Financial Action Task Force (FATF) guidelines on virtual assets, strive to establish consistent regulatory standards across jurisdictions (Gikay, 2019). Future legal developments are expected to emphasize enhancing international cooperation to ensure a coherent and comprehensive regulatory framework for blockchain technology.

CONCLUSION

This study set out to explore the legal frameworks governing digital transactions, with a particular focus on the impact of blockchain technology. Through a comprehensive analysis, the study has demonstrated how blockchain's decentralized, transparent and immutable characteristics present both opportunities and challenges for existing legal structures. The examination of various facets of digital transactions and blockchain technology, including its conceptual framework, regulatory challenges and international legal approaches, has provided a detailed understanding of the current state and future directions of blockchain regulation.

Key findings indicate that while blockchain technology offers significant benefits such as enhanced security, reduced transaction costs and increased transparency, it also complicates traditional regulatory mechanisms due to its decentralized nature and global reach. Jurisdictional ambiguities, enforcement difficulties and privacy concerns are among the major challenges identified. The comparative analysis of international legal approaches highlighted the diversity in regulatory strategies, from the supportive frameworks in Japan and Switzerland to the restrictive measures in China, underscoring the need for international cooperation.

The study concludes that effective regulation of blockchain technology requires innovative and adaptive legal frameworks that can keep pace with technological advancements. Policymakers must balance fostering innovation with protecting public interests, ensuring that regulations are both flexible and robust. Recommendations include the development of international standards for blockchain regulation, greater emphasis on privacy-preserving technologies and the creation of legal frameworks that recognize and accommodate the unique characteristics of decentralized systems.

In summary, this study has successfully met its aim and objectives by providing a thorough examination of the legal frameworks for digital transactions in the context of blockchain technology. The findings and recommendations offer valuable insights for regulators, policymakers and stakeholders, paving the way for a more secure, transparent and innovative digital economy. The ongoing evolution of blockchain technology and its regulatory landscape will require continuous adaptation and collaboration to address emerging challenges and capitalize on the technology's transformative potential.

Reference

Abdullah, F., Ward, R., & Ahmed, E., (2016). Investigating the influence of the most commonly used external variables of TAM on students' Perceived Ease of Use (PEOU) and Perceived Usefulness (PU) of e-portfolios. *Computers in Human Behavior, 63*, 75-90. https://doi.org/10.1016/j.chb.2016.05.014

Agnikhotram, S., & Kouroutakis, A. (2018). Doctrinal challenges for the legality of smart contracts: Lex Cryptographia or a New, Smart Way to Contract. *Journal of High Technology Law, Sai Agnikhotram and Antonios Kouroutakis, 19*, 300.

Albshaier, L., Almarri, S., & Hafizur Rahman, M.M. (2024). A review of blockchain's role in E-Commerce transactions: Open challenges, and future research directions. *Computers*, *13*(1), 27. https://doi.org/10.3390/computers13010027

Alston, E. (2022). Blockchain and the law-legality, law-like characteristics, and legal applications. *The Economics of Blockchain and Cryptocurrency*, 117-144. https://doi.org/10.4337/9781800882348.00014

Anand, D., & Mantrala, M. (2019). Responding to disruptive business model innovations: the case of traditional banks facing fintech entrants. *Journal of Banking and Financial Technology*, *3*, 19-31. https://doi.org/10.1007/s42786-018-00004-4

Antonopoulos, A.M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. O'Reilly Media, Inc.

Baidoo, S.A. (2019). Regulatory effects on traditional financial systems versus Blockchain and emerging financial systems (Doctoral dissertation, Walden University).

Bakhshi, T., & Ghita, B. (2021). Perspectives on auditing and regulatory compliance in Blockchain transactions. In trust models for next-generation blockchain ecosystems (pp. 37-65). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-75107-4_2

Bebris, A.V., & Mukkamala, R.R., (2018). Anti-Money laundering and counter-terrorism financing methodology for Cryptocurrency exchanges in the European Union.

Bodó, B., Gervais, D., & Quintais, J.P. (2018). Blockchain and smart contracts: the missing link in copyright licensing?. *International Journal of Law and Information Technology*, *26*(4), 311-336. https://doi.org/10.1093/ijlit/eay014

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change*, *69*, 283-305. https://doi.org/10.1007/s10611-017-9756-5

Catalini, C., & Gans, J.S. (2020). Some simple economics of the Blockchain. *Communications of the ACM*, *63*(7), 80-90. https://doi.org/10.2139/ssrn.2874598.

Cherbal, S., Zier, A., Hebal, S., Louail, L., & Annane, B. (2024). Security in internet of things: a review on approaches based on Blockchain, machine learning, cryptography, and quantum computing. *The Journal of Supercomputing*, *80*(3), 3738-3816. https://doi.org/10.1007/s11227-023-05616-2

Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, *14*(4), 639-658. https://doi.org/10.1017/S1744137417000200

Ekbia, H.R., & Nardi, B.A. (2017). *Heteromation, and other stories of computing and capitalism*. MIT Press.

Fairfield, J.A. (2014). BitProperty.

Garcia-Teruel, R.M., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, *41*, 105543. https://doi.org/10.1016/j.clsr.2021.105543

Gibney, C., Trites, S., Ufoegbune, N., & Lévesque, B. (2016). International review: Mobile payments and consumer protection. Research Division, Financial Consumer Agency of Canada.

Gikay, A.A. (2019). European consumer law and Blockchain based financial services: a functional approach against the rhetoric of regulatory uncertainty.

Girasa, R. (2018). Regulation of cryptocurrencies and blockchain technologies. National and International Perspectives. Suiza: Palgrave Macmillan.

Javaid, M., Haleem, A., Singh, R.P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, *2*(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

Jiménez-Gómez, B.S. (2019). Risks of Blockchain for data protection: a European approach. *Santa Clara High Technology Law Journal*, *36*, 281.

Karasek-Wojciechowicz, I. (2021). Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless Blockchain spaces. *Journal of Cybersecurity*, *7*(1), tyab004.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41(*10), 1027-1038. https://doi.org/10.1016/j.telpol.2017.09.003

Lehmann, M. (2020). Global rules for a global market place?-Regulation and supervision of Fintech providers..

Li, A., Wei, X., & He, Z. (2020). Robust proof of stake: A new consensus protocol for sustainable Blockchain systems. *Sustainability, 12*(7), 2824. https://doi.org/10.3390/su12072824

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems,* 107, 841-853. https://doi.org/10.1016/j.future.2017.08.020

Lindsay, M.G. (2022). International Rise of Cryptocurrency: A Comparative Review of the United States, Mexico, Singapore, and Switzerland's Anti-Money Laundering (AML) Regulation. *South Carolina Journal of International Law & Business, 19,* 161.

McKinney, S.A., Landy, R., & Wilka, R. (2017). Smart contracts, blockchain, and the next frontier of transactional law. *Washington Journal of Law, Technology & Arts, 13,* 313.

Morishita, T. (2020). Recent developments of Japanese laws and regulations on FinTech. Research Handbook on Asian Financial Law, 454-478. https://doi.org/10.4337/9781788972208.00034

Muminova, E., Honkeldiyeva, G., Kurpayanidi, K., Akhunova, S., & Hamdamova, S. (2020). Features of introducing blockchain technology in digital economy developing conditions in Uzbekistan. In E3S Web of Conferences (Vol. 159, p. 04023). EDP Sciences. https://doi.org/10.1051/e3sconf/202015904023

Murray, A., (2013). *Information technology law: the law and society*. Oxford University Press, USA.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* https://bitcoin.org/bitcoin.pdf.

Novak, M. (2020). Crypto-friendliness: Understanding Blockchain public policy. *Journal of Entrepreneurship and Public Policy, 9*(2), 165-184. https://doi.org/10.1108/JEPP-03-2019-0014

Oriekhoe, O.I., Oyeyemi, O.P., Bello, B.G., Omotoye, G.B., Daraojimba, A.I., & Adefemi, A. (2024). Blockchain in supply chain management: A review of efficiency, transparency, and innovation. *International Journal of Science and Research Archive, 11*(1), 173-181. https://doi.org/10.30574/ijsra.2024.11.1.0028

Panait, C., Ljubenkov, D., & Alic, D. (2021). Striking the balance between innovation and regulation in AI-is Europe leading the way or lagging behind. *Europuls Policy Journal on EU Affairs, 1*, 27-45.

Petare, P.A., Josyula, H.P., Landge, S.R., Gatala, S.K.K., & Gunturu, S.R., (2024). Central bank digital currencies: exploring the future of money and banking. *Migration Letters, 21*(S7), 640-51.

Pilkington, M. (2016). Blockchain technology: principles and applications. In Research handbook on digital transformations (pp. 225-253). Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019

Polasik, M., Huterska, A., Iftikhar, R., & Mikula, Š. (2020). The impact of Payment Services Directive 2 on the PayTech sector development in Europe. *Journal of Economic Behavior & Organization, 178*, 385-401. https://doi.org/10.1016/j.jebo.2020.07.010

Quintais, J.P., Bodo, B., Giannopoulou, A., & Ferrari, V. (2019). *Blockchain and the law: A critical evaluation.*

Reyes, C.L. (2016). Moving beyond Bitcoin to an endogenous theory of decentralized ledger technology regulation: An initial proposal. *Villanova Law Review, 61*, 191.

Riasanow, T., Flötgen, R.J., Setzke, D.S., Böhm, M., & Krcmar, H. (2018). The generic ecosystem and innovation patterns of the digital transformation in the financial industry. https://aisel.aisnet.org/pacis2018

Risius, M., & Spohrer, K. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering, 59*, 385-409. https://doi.org/10.1007/s12599-017-0506-0

Sheikh, H., Azmathullah, R.M., & Rizwan, F. (2018). Proof-of-work vs proof-of-stake: a comparative analysis and an approach to Blockchain consensus mechanism. *International Journal for Research in Applied Science & Engineering Technology, 6*(12), 786-791.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Turk, M.C. (2019). Overlapping legal rules in financial regulation and the administrative state. *Georgia Law Review, 54*, 791.

Wang, Y., & Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems. *International Journal of Accounting Information Systems, 30*, 1-18. https://doi.org/10.1016/j.accinf.2018.06.001

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of Blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). *Ieee*. DOI: 10.1109/BigDataCongress.2017.85

Zohar, A. (2015). Bitcoin: under the hood. *Communications of the ACM, 58*(9), 104-113. https://doi.org/10.1145/2701411.

Zwitter, A., & Hazenberg, J. (2020). Decentralized network governance: blockchain technology and the future of regulation. *Frontiers in Blockchain, 3*, 12. https://doi.org/10.3389/fbloc.2020.00012