İŞLETME ARAŞTIRMALARI DERGİSİ
JOURNAL OF BUSINESS RESEARCH-TURK
2025, 17(3), 2659-2678
https://doi.org/10.20491/isarder.2025.2117

Blockchain, Regulation, and the Business Ecosystem: A Legal Perspective

Onur CERAN [a]

[a] Gazi University, Faculty of Applied Sciences, Management Information Systems, Ankara, Türkiye. onur.ceran@gazi.edu.tr

ARTICLE INFO

Keywords:
Blockchain
Web3
Legal Issues
Regulation Management

Received 1 July 2025
Revised 13 September 2025
Accepted 15 September 2025

Article Classification:
Research Article

ABSTRACT

Purpose- This study explores the critical business implications of Web3 technologies within Türkiye's unique legal landscape, a nation experiencing significant crypto adoption and evolving regulations. By analyzing the architectural shifts from Web1.0 to Web3, we aim to understand how traditional legal frameworks create significant challenges for all stakeholders affected by decentralized environments, not just those operating within them.

Design/methodology/approach- This study adopts a multidisciplinary and comparative research design, integrating both technological and legal perspectives to investigate the evolution from Web1.0 to Web3 and the associated legal implications. Given the complexity and scope of the subject matter, a mixed methods approach is employed, combining qualitative content analysis, document analysis, and comparative case study methodologies.

Findings- The findings suggest that existing legislation is inadequate and outdated and poses a risk of future legislative actions causing irreversible or difficult-to-remedy harm if current legal gaps remain unaddressed.

Discussion- Drawing from real-world case scenarios, the study highlights the urgent need for adaptive legal strategies that align with the decentralized, borderless, and immutable nature of blockchain infrastructures. The findings aim to support business leaders, legal practitioners, and policymakers seeking to innovate responsibly within the emerging Web3 economy.

1. INTRODUCTION

Technology evolves in a continuous cycle of emerging needs and new solutions, often described as the "chicken-egg paradox" (Küçükkalay, 1997). Nowhere is this more evident than in the Internet's transformation across Web1.0, Web2.0, and now Web3. Each phase has reshaped how users interact with digital platforms, how businesses operate, and how data is generated, stored, and governed.

Web1.0, based on the client-server model pioneered by Tim Berners-Lee (Berners-Lee et al., 1994), enabled the passive dissemination of information, whereas Web2.0 introduced user interactivity and platform-centric ecosystems that revolutionized social and economic dynamics (O'Reilly, 2007; Aghaei et al., 2012). However, data centralization under large tech intermediaries sparked growing concerns over privacy, censorship, and corporate overreach. Web3 emerged as a decentralized paradigm powered by blockchain technology, offering unprecedented transparency, security, and user autonomy (Swan, 2015; Bambacht & Pouwelse, 2022). Beyond its technical advantages, Web3's decentralized nature now intersects with broader digital ecosystems such as the metaverse, an immersive, persistent digital universe. Together, these technologies promise to reshape entire business sectors by enabling secure digital ownership, trustless transactions, and decentralized governance models.

These disruptive potentials are already visible in industries such as Finance, where decentralized finance (DeFi) protocols offer borderless lending, borrowing, and asset management without intermediaries; Real estate, where tokenized property ownership and blockchain-based land registries streamline and secure transactions; Healthcare, where blockchain ensures data integrity and interoperability of electronic health records across providers; Entertainment, where NFTs and metaverse platforms enable new models of content monetization and digital rights management; Non-profit, where transparent donation tracking and smart

Suggested Citation
Ceran, O. (2025). Blockchain, Regulation, and the Business Ecosystem: A Legal Perspective, İşletme Araştırmaları Dergisi, 17 (3), 2659-2678.

contracts ensure accountability; Supply chain, where end-to-end visibility through immutable ledgers enhances efficiency and trust.

While these applications unlock immense opportunities, they also expose significant legal conflicts, particularly in areas where conventional legal tools fall short in addressing the dynamics of decentralized systems. In the Turkish context, the transition to Web3 raises challenges such as regulating user-generated content across decentralized platforms, identifying and prosecuting cybercriminals operating pseudonymously within blockchain networks, and protecting intellectual property rights in metaverse environments where ownership and originality are difficult to verify. Furthermore, the legal basis for confiscating or freezing digital assets, a key instrument in criminal investigations and enforcement, remains underdeveloped. As businesses adopt blockchain-based solutions, they must be aware that these unresolved legal issues are not peripheral but central to the sustainable and lawful use of decentralized technologies. Businesses embracing blockchain must, therefore, be acutely aware of these legal grey zones. Failure to recognize and plan for such challenges may expose organizations to regulatory scrutiny, reputational damage, or litigation. Legal compliance should not be viewed as a post-implementation concern but rather as an integral part of innovation strategy from the outset.

This article explores these intersections through the lens of the Turkish legal landscape. According to the Global Crypto Adoption Index (Chainalysis, 2023), Turkey ranks fourth globally in cryptocurrency transaction volume, and 11th in overall index ranking in 2024 (Chainalysis, 2024), yet its legal framework remains in flux. Recent regulations have addressed taxation and crypto asset service providers, but many legal dimensions, especially those relevant to business applications, remain unregulated or unclear. By comparing the architectural and conceptual shifts from Web1.0 to Web3, this study highlights how blockchain technologies challenge traditional legal constructs. Drawing on real-world cases from Turkey, we illustrate how current laws struggle to keep pace with decentralization and where gaps or conflicts emerge. In their bibliometric study, Habil et al. (2024) noted that while 74.17% of blockchain research between 2019 and 2023 falls under computer science-related disciplines, the integration of blockchain in business industry and its technological implications and advancements in engineering applications, only 3.9% addresses legal implications an imbalance this paper aims to address.

Despite Turkey's prominent role in the global cryptocurrency landscape and its rapid technological adoption, the current legal frameworks remain insufficient to address the complexities of decentralized systems inherent to Web3. This study aims to critically examine the legal incompatibilities and regulatory shortcomings surrounding Web3 technologies in Turkey, with a specific focus on blockchain-based infrastructures, decentralized finance (DeFi), and metaverse ecosystems. By identifying structural gaps and highlighting real-world legal conflicts, the research problem centers on how traditional legal constructs, rooted in centralized governance, struggle to adapt to a peer-to-peer, immutable, and pseudonymous digital environment. Ultimately, the study seeks to inform policymakers, business stakeholders, and legal professionals about the urgent need for a coherent, adaptive, and enforceable legal framework for emerging Web3 ecosystems.

2.METHODOLOGY

This study adopts a multidisciplinary and comparative research design, integrating both technological and legal perspectives to investigate the evolution from Web1.0 to Web3 and the associated legal implications.

2.1. Research Design

This study employs a qualitative exploratory research model to investigate the legal implications of Web3 technologies within the context of Turkey's evolving regulatory environment. The research adopts a comparative case study approach, supplemented by document and content analysis, to provide a multidisciplinary perspective that bridges technological developments and legal frameworks. This model is well-suited for exploring emerging and complex phenomena that lack comprehensive regulatory treatment. By analyzing real-world legal cases and statutory documents, the study offers in-depth insights into how traditional laws align or conflict with the decentralized structure of Web3 ecosystems. To guide the inquiry into the legal challenges posed by decentralized Web3 technologies within Turkey's evolving regulatory context, this study seeks to address the following research questions:

- RQ1: How do existing legal frameworks in Turkey address the regulatory needs of decentralized Web3 applications?
- RQ2: What are the key legal conflicts and enforcement challenges arising from the pseudonymous, immutable, and borderless nature of Web3 technologies?
- RQ3:How can comparative analysis of Web1.0, Web2.0, and Web3 architectures reveal fundamental misalignments between current regulatory mechanisms and technological realities?
- RQ4: What strategic considerations should Turkish lawmakers and business leaders take into account when designing regulatory frameworks for Web3 technologies to ensure both innovation and legal accountability?

2.2. Data Collection

The data for this study were collected through document analysis, drawing on both primary and secondary sources. Primary data sources included Turkish laws, regulations particularly those related to internet governance, content regulation, intellectual property, and financial enforcement. Secondary sources involved academic journal articles, policy briefs, technical documentation, and industry reports on Web1.0, Web2.0, and Web3 technologies. The collection process took place between January and May 2025, with the aim of capturing the most up-to-date and relevant legal and technological developments. All documents were systematically selected based on their relevance to the research questions and analyzed using qualitative content analysis methods.

2.3. Data Analysis Methods

The collected data were analyzed using thematic content analysis, a qualitative method that allows for the systematic identification and interpretation of recurrent themes, patterns, and legal conflicts. The documents were coded based on key legal constructs and Web3-specific technological features. Additionally, comparative analysis was used to examine differences and overlaps between the Web1.0, Web2.0, and Web3 paradigms in relation to Turkey's legal infrastructure. This multi-method analytical approach facilitated a nuanced understanding of regulatory misalignments and emerging legal needs in decentralized environments.

2.4. Samples

Representative cases and real-world legal incidents related to each web generation are examined to highlight practical implications. The population of this study comprises the legal and technological frameworks that define the evolving regulatory environment for Web3 technologies in Turkey. Since the research is qualitative and exploratory in nature, no statistical sampling technique was applied. Instead, purposeful sampling was employed to select a range of real-world legal cases, statutory texts, regulatory documents, and policy reports that directly pertain to blockchain-based applications.These documents represent the most relevant and informative sources for understanding the intersection of law and decentralized technologies.

3. From Web1.0 to Web3

Any request for a service passes through the same kind of cables, switches, and routers and reaches a computing device to be processed. Although Web1.0, Web2.0, and Web3 use the same infrastructure in terms of networking, the protocols and concepts make the difference between them.

3.1. Internet Service Infrastructure

Although several cutting-edge technologies are used in order to create a network, for services to provide information and end-users to reach the information needed, the underlying technology and the architecture may be simplified in basic steps. Regardless of whether being accessed as Web1.0, Web2.0, or Web3. service, Transmission Control Protocol /Internet Protocol (TCP/IP) suite is the underlying global method allowing different end users/computer systems to communicate over the Internet. In order for communicating parts to be identified, each of them is assigned an address, which is called an IP address (Parziale et al., 2006). Even though there are two types of IP addressing systems, IPv4 and IPV6, IPv4 is the commonly used one and looks like "194.27.18.45". All types of communication over a network or the internet, such as reading news, watching a video, sending e-mails, and transferring files, involve connecting to another computing system, breaking data into smaller packets, and sending them to the intended destination/IP address (Murdoch & Anderson, 2008). Specialized systems called routers are responsible for forwarding these Internet Protocol (IP) packets to the destination appropriately. In the case of Internet Protocol Version 4 (IPv4), the forwarding decision is based on a 32-bit destination address found in the header of each packet. A lookup engine at each port of the router uses a routing data structure to determine the correct outgoing link for the packet's destination address (D. E. Taylor et al., 2003). In order for a client to reach a service over a network, Figure 1 illustrates the infrastructure, and below, the steps that should be taken are introduced.

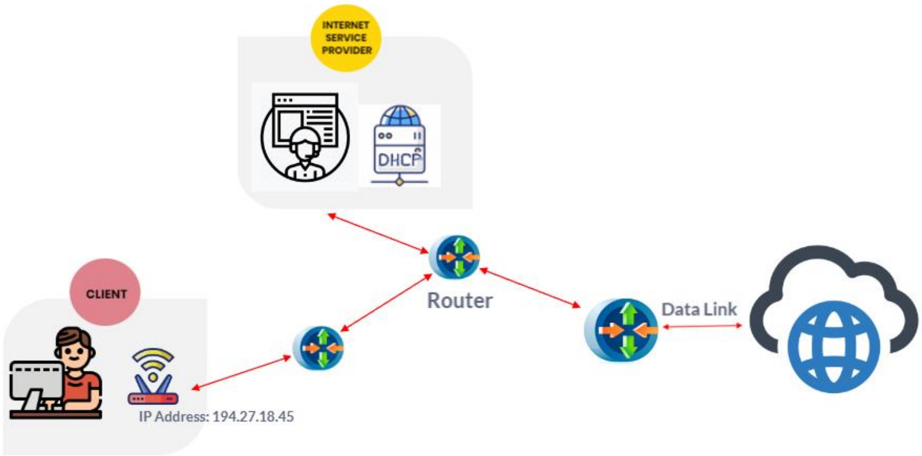

Figure 1. Network service

Steps to reach internet:

Step1 : Client applies to the internet service provider for accessing internet. Client submits his address where the internet service is used and identity information to the ISP during the application.

Step2 : After completing the cabling process, the ISP arranges the configurations on the routers it operates, creates the user account with the information provided by the client, and activates the internet circuit.

Step3 : For the user to access the internet, the ISP assigns an IP address to the user from the DHCP server it operates. It maintains the information as a log record that this IP address was assigned for which client's use at which time interval. If the client wishes, a fixed IP address can be allocated as well with a log record.

Step4 : The client accesses the services to be used on the internet through the connection service allocated

3.2. Content, Authority, and Establishment of Connection on Web1.0 and Web2.0

The concept of Web1.0 aimed to create a shared space on the internet where users could access the information without contributing. It provided basic contact information like email, address, phone number, and fax, as well as advertisements in newspapers and magazines. On the other hand, Web2.0, known as the read-write web, enables the management and connection of a large global community with similar interests. Web2.0 is associated with interactive web applications that facilitate information sharing, interoperability, user-centered design, and collaboration on the World Wide Web. Social networking sites serve as real-time platforms for sharing information and communication. Web2.0 goes beyond being just an upgraded version of Web1.0. It encompasses elements such as flexible web design, the ability to creatively repurpose content, continuous updates, and collaborative creation and editing of content, all made possible through Web2.0 technologies (Hiremath & Kenchakkanavar, 2016). While the content is generated by the service provider, literally the owner of the website, in Web1.0; user generally generates the content in Web2.0. However, both Web1.0 and Web2.0 works on centralized computing system which is client-server architecture. The client-server model is a system architecture that involves two components: client systems and server systems, which communicate with each other over a computer network. The client system initiates a connection to the server system, while the server system waits for requests from any client. A client, which may be a web browser, end-point or mobile application or a thin client, is a hardware device that tries to access a service provided by a server. On the other hand, a server is a computer that runs dedicated software to provide services to other machines by listening for requests transmitted via network (Kumar, 2019). For both Web1.0 and Web2.0 the authority on the content stored on the server is hold by service provider. It means that the service provider can remove the content from servers, totally make it unreachable, sell the information stored or shut all the system down. Figure 2 illustrates the content creation and the authority for client-server model.

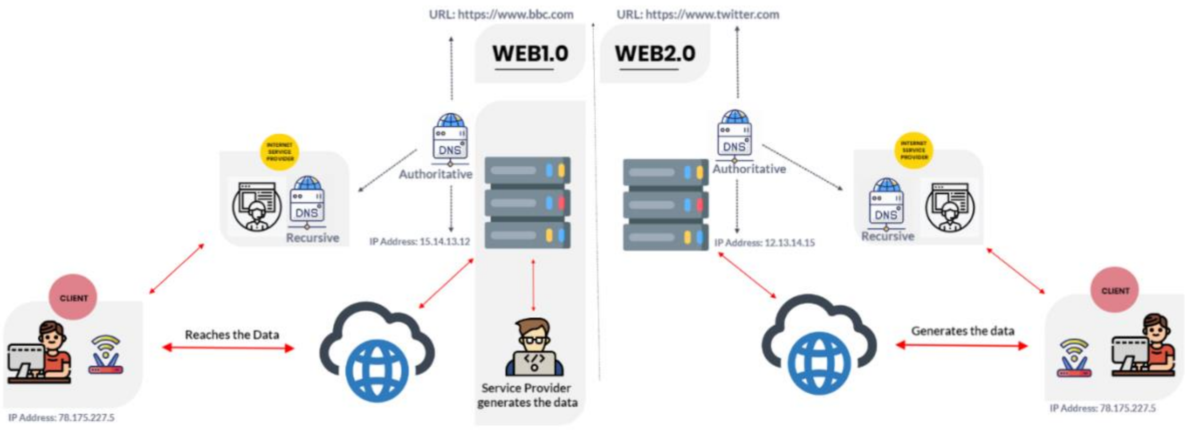

Figure 2. Content creation and authority for client-server model

As shown in Figure 2, for both Web1.0 and Web2.0, clients reach some content on the web servers, which have IP numbers. Routers also identify the routes and servers by IP numbers. There are billions of hosts serving web content in the world. As it is really hard to remember such numbers, the Domain Name System (DNS) provides domain names to be associated with IP addresses. If a client wants to reach a website, they first look up the IP address of it on DNS, then send the query to the associated IP address. For instance, the client on the left side wants to reach the uniform resource locator (URL), which is www.bbc.com. Then the computer performs a domain name lookup via its recursive DNS resolver, and the authoritative DNS of bbc.com sends back the IP address of the service. Then the connection is established through this IP address.

3.3. Providing a Web Service on Web1.0 and Web2.0

As aforementioned above, if a web service, most commonly a website, is to be provided on the internet, then several steps should be taken. Regardless of serving in Web1.0 or Web2.0, these steps are described below.

3.3.1. Domain Name

Domain names such as twitter.com or wikipedia.org are the most important components of web browsing, which enable clients to reach websites by allowing them to type more memorable phrases than IP addresses (Coull et al., 2012). Serving as a human-friendly identifier, domain names are used as a mask for IP addresses (Mueller, 2000). Although the Internet Corporation for Assigned Names and Numbers (ICANN) isn't involved in selling specific items, it plays the role of creating and managing contracts that ensure a series of intermediaries follow the guidelines set by its diverse community to make the actual sale of domain names and related tasks. These intermediaries are mainly ICANN-approved entities and are called registries and registrars. These entities operate independently of ICANN but are legally obligated to comply with its regulations (Datysgeld, 2017).

For an individual or a firm that wants to register a domain name, they apply to a registrar by providing their contact information, including email address, phone number, registrant name, etc. If the domain name is not registered before, after the payment is done, the domain name is registered for the registrant's use. In Figure 3, the WHOIS lookup/registry information via whois.domaintools.com is shown for twitter.com.

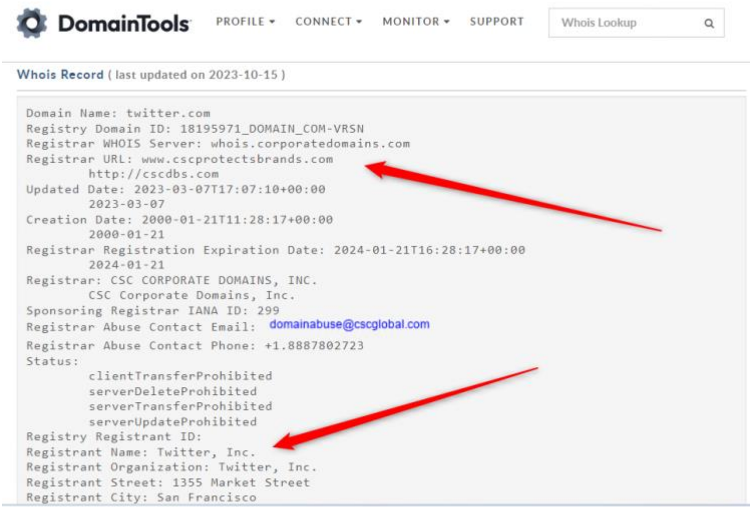

Figure 3. Registry information for twitter.com

As shown in Figure 3, some information, such as the information of the registrant, registrar corporation, creation, and expiry of the domain name, is publicly available. Although the contact information may be given falsely by the registrant, payment information and IP address used by the registrant while registry process are logged by the registrar.

3.3.2. *Web Hosting*

Web hosting services provide the means to make any website accessible on the internet. By purchasing a hosting service, the payer gains access to a portion of the web servers from the provider, where they can store their website's files and data. When someone enters the website's domain name into the browser, it is the responsibility of the web hosting provider to deliver the content to the visitor. Although the contact information may be given falsely, intentionally by the payer, the payment information and IP address used by the payer during the purchasing process are logged by the web hosting provider.

3.4. *Web3*

Web3, also known as the "Decentralized Web", forms the infrastructure blocks of the new web era and brings to life a decentralized, democratic, and user-oriented internet environment (Alabdulwahhab, 2018). Web3, which is based on the promise of giving individuals greater control over their data and the content they produce, is driven by the power of blockchain technology. In order to understand the changes with Web3, some main concepts should be introduced.

3.4.1. *Blockchain*

Blockchain technology, which was invented by Satoshi Nakamoto, laying out the bitcoin's, which is the first and most known cryptocurrency, mathematical foundation; revealed the solution of the challenge to develop a distributed storage system for documents with timestamps, ensuring that no party can alter the data or timestamps without being noticed (Di Pierro, 2017). In simple words, blockchain technology has surfaced as a decentralized computing approach that effectively resolves concerns associated with relying on a central authority for trust (Khan et al., 2021). It is a public, decentralized database of records of transactions providing information securely stored, validated, and managed by a network of computers all around the world, instead of storing on controlled and centralized servers (Malhotra et al., 2022) and forms the backbone of Web3 applications (Momtaz, 2022). Transactions may encompass basic tasks, such as transferring funds from one address to another, or more intricate actions involving contracts, such as voting. These activities are typically carried out using cryptocurrency wallets, which hold users' private keys in order to sign transactions (Bodziony et al., 2021). Being the key component of performing any transaction on any blockchain platform, as a software application, crypto wallets allow users to create an asymmetric key pair of a private key and a public key. Private key is a secret key in hexadecimal format used for authorizing transactions, proving asset-ownership, and the user is identified by its public key, which should be shared publicly as an address, derived from the corresponding private key for receiving crypto assets (Suratkar et al., 2020 ; Aydar et al., 2020).

(2023) describe blockchain as an electronic ledger system that keeps track of who owns what and tracks changes in real-time. Unlike Web1.0 and Web2.0, which operate on client-server architecture, blockchain enables Web3 to operate in a peer-to-peer network, meaning a decentralized network architecture. Each time a transaction is made, it is sent to that peer-to-peer network, where computer algorithms verify its authenticity. Once confirmed, the new transaction is connected to the previous one, creating a chain of transactions known as the blockchain (Sarmah, 2018), illustrated in Figure 4. The decentralized structure ensures data accuracy and integrity through consensus among all network participants. Since digital records are publicly available on the open blockchain, the information becomes transparent, immutable, and traceable.

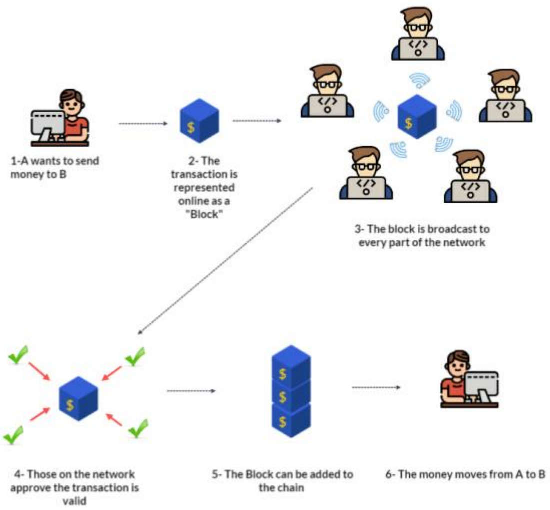

Figure 4. Blockchain workflow (Sarmah, 2018)

3.4.2. Smart Contract

Being implemented on blockchain, smart contracts are defined as executable computer programs for approved contractual clauses. When a condition within a smart contract is met, the associated statement will automatically activate the relevant function (Z. Zheng et al., 2020). Replacing trusted centralized legal parties between contracting sides (Taherdoost, 2023) with an executable code, a smart contract is recognized by its unique address and is stored on the blockchain. To interact with a smart contract, users send transactions to the contract's address. When a new transaction is approved by the blockchain and directed to a contract address, all participants on the mining network execute the contract code using the current blockchain state and transaction details as inputs. Through a consensus protocol, the network collectively determines the output and updates the contract's state for the next interaction (Luu et al., 2016).

3.4.3. Decentralized Applications (dApps)

Decentralized applications, or dApps, are software programs that operate on a blockchain peer-to-peer network architecture rather than relying on a centralized server. This decentralized nature makes them transparent, resistant to censorship, and self-sustaining, removing the reliance on intermediaries. Important characteristics of dApps include open-source availability, where the codebase is accessible for external review, and reliance on decentralized consensus, guaranteeing that transactions are authenticated and stored on a distributed ledger (Z. Zheng et al., 2017; P. Zheng et al., 2023). Figure 5 demonstrates a dApp structure, which shares similarities with traditional centralized web applications, but it incorporates distributed services and databases as supplementary elements. Users of the dApp establish a virtual wallet on the corresponding blockchain platform, serving as a unique identifier. Important actions, such as purchasing, vending, or generating random numbers, are carried out via smart contracts (Min & Cai, 2022).

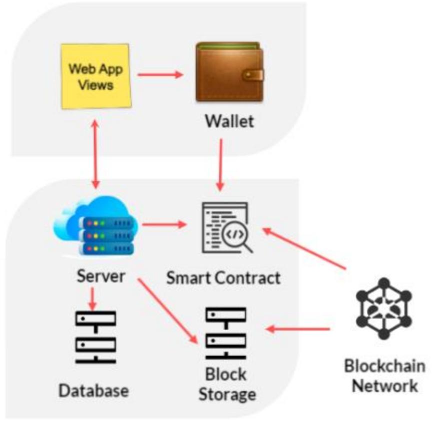

Figure 5. dApp structure (Min & Cai, 2022)

3.4.4. Decentralized Finance (DeFi)

Decentralized Finance, known as DeFi, represents an innovative financial ecosystem that functions independently of traditional middlemen like banks. It relies on blockchain technology to conduct and oversee financial transactions. By employing smart contracts, DeFi platforms provide a wide range of financial services such as lending, borrowing, asset trading, and yield farming (Popescu, 2020). Being a cheaper alternative to the current traditional financial system, DeFi has the potential to expand financial access, foster innovation without requiring permission, remove the necessity for intermediaries, guarantee the permanence of transactions, resist censorship, enforce consistent rules for all participants, enable anyone with internet access to audit transactions, and reduce the cost of cross-border transactions (Ozili, 2022).

3.4.5. Metaverse

Metaverse, which is a combination of the words meta (after, beyond) and universe, combines physical and digital realms, allowing for ongoing, interactive experiences shared by multiple users. It relies on technology to facilitate immersive interactions with virtual surroundings, digital items, and individuals in a multi-sensory manner. Through the use of virtual reality, individuals experience a sense of immersion, feeling as though they are situated in an alternate reality and interacting much like they would in a physical environment (Mystakidis, 2022). Blockchain, being the underlying technology for the Metaverse, is the fundamental basis of its framework. It deals with matters concerning virtual assets and identities, providing users with a wide array of content for interaction (Mozumder et al., 2022).

One of the Web3 metaverses, Decentraland, powered by blockchain, allows its users to create, buy, or sell digital assets. In Decentraland, the community permanently owns land and has complete oversight and authority over their creative endeavors. Decentraland differs from traditional virtual worlds and social networks in that it is not governed by any centralized organization. This means that no single entity has the authority to alter the smart contract, content, economic mechanisms, or restrict others from accessing the world, trading digital goods, and offering services.

3.5. Content, Authority, and Establishment of Connection on Web3

The concept of Web3 is aimed at creating a more secure, transparent, and user-centric internet in which users are provided with control over both their data and the content they create (Liu et al., 2022). Gavin Wood (2014), who is the co-founder of Ethereum, which is a decentralized blockchain, indicates that Web1.0 or Web2.0 falls back on centralized trust of authorities. Wood stated that, especially after the Snowden issue, it is not a good model to entrust user information to organizations that work in a model that generates more income the more they know about their users, and stated that governments are generally trying to expand their authority. For this reason, it is explained by the requirements of the Web3 model, which mathematically forces the communication between the parties and the information that should remain confidential to remain confidential, information such as IP address not to be determined, and to operate by consensus without depending on the decisions of a central authority.

Shifting from client-server architecture to decentralized chains, Web3 stands out from prior iterations Web1.0 and Web2.0, as it integrates concepts of ownership and transfer. Individuals will establish self-governed accounts, often in the shape of wallets, to oversee digital assets and virtual information. In contrast to depending on centralized servers, Web3 participants have the freedom to transfer their assets using smart contracts, which offer benefits such as automatic execution, accountability, and global verification (Yu et al., 2023). (2017) define a decentralized system as a type of distributed systems, which consist of coordinated components managed by a single authority, in which various authorities control different components, and no single authority is completely trusted by all. Unlike Web1.0 and Web2.0, Web3 does not require a single server hosting the information and serving to the clients. Web3 works on a decentralized computing architecture. Every node in this architecture may act as both a client and a server. This peer-to-peer (p2p) networking provides for the sharing of information across the nodes securely. Figure 6 illustrates the content creation and the authority for the decentralized p2p model.

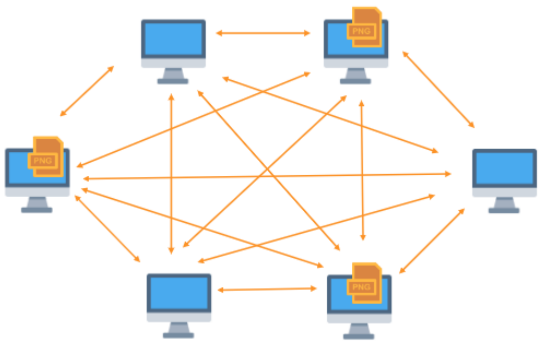

Figure 6. Content creation and authority for p2p model

Since the content is generated by one peer and is stored on other peers' storage, the content cannot be removed or made unreachable by a single authority. Compared to client-server architecture, clients also reach another peer on the network to get the content through the peer's IP address. Routers again identify the routes by IP number as well. But the traditional domain naming system (DNS) is not used in order to find the location of desired content.

3.6. Providing a Web Service on Web3

As aforementioned above, if a web service, most commonly a website, is to be provided on Web3, then several steps should be taken, which are described below.

3.6.1. Hosting

The approximate file size that can be stored in a block in blockchain is 1 MB; hence, it is not appropriate to store files larger than that size in blockchain (Ye & Park, 2021). Storing the actual data on a decentralized and distributed storage network and storing only some metadata in blockchain makes sense. Decentralized storage networks (DSNs) are provided by different storage providers without the need for central coordination (Korpal & Scott, 2023). Interplanetary File System (IPFS), which is a p2p protocol for storing and accessing files and websites (IPFS whitepaper), is an open-source initiative aimed at establishing a lasting, decentralized approach to storing and distributing data. It encompasses a protocol and network and is widely utilized by various projects and users seeking seamless and effective file sharing. Unlike the traditional location addressing system used by HTTP through DNS, where a single server hosts multiple files requiring access, IPFS disperses files throughout the network, with each file being identified by its cryptographic hash based on its content. An overview of how a file or website is stored and served and reached by the clients within the blockchain is demonstrated in Figure 7 (Politou et al., 2020; Alizadeh et al., 2020).

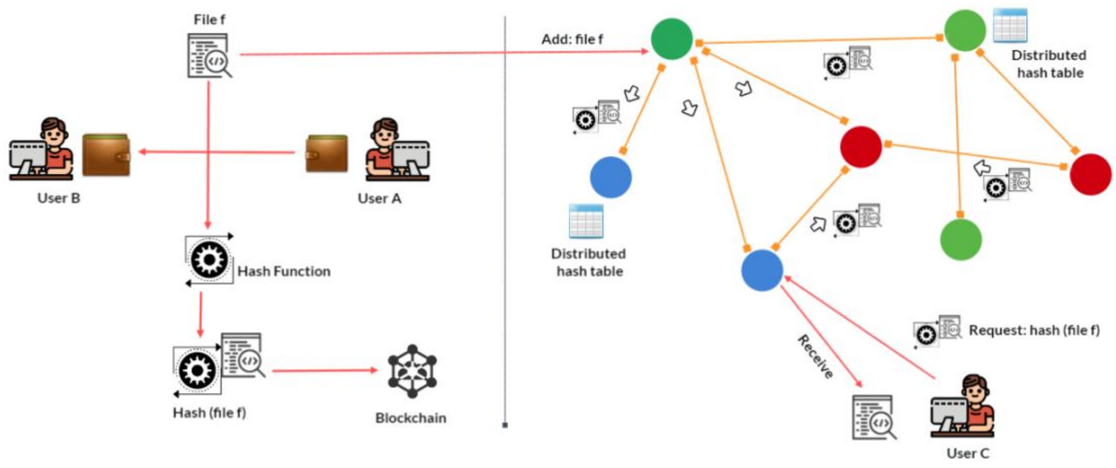

Figure 7. Content storing and distribution on IPFS and blockchain (Politou et al., 2020)

If a user wants to store a file in IPFS steps to take are as follows:

Step-1a: User "A" stores a file named "f" in IPFS.

Step-2a: The file f is split into small chunks and every chunk is identified with its own hash value.

Step-3a: The chunks of file f are distributed to some other nodes on the network.

Step-4a: Every node that gets the chunks of file f is written to the Distributed Hash Table (DHT), which performs as a lookup service providing who has what data.

Step-5a: A content identifier (CID), which is the label used for pointing a material and based on hash value of file f is calculated and stored in the blockchain. (Combining this with a domain name on the blockchain will be enumerated on section 2.6.2)

If a user wants to retrieve a file in IPFS steps to take are as follows:

Step-1b: User B queries with the CID of the desired file f through the IPFS service to the network.

Step-2b: The request traverses to nodes who has the chunks of file f through using DHT.

Step-3b: The whole chunks are gathered and combined to create the main file f.

Step-4b: User B gets the file f.

3.6.2. Domain Name

There is no difference in domain name systems between Web1.0, Web2.0, and Web3 in terms of purpose, which is directing a user to intended content without the need to remember complex identifiers. However, in Web3, ICANN has no central authority for controlling and coordinating domain names. In fact, there is no central authority controlling and coordinating domain naming and addressing. Blockchain-based naming service also operates like DNS with hierarchical names, with a registrar who has the full authority. But top-level domains are managed by smart contracts, allowing users to have domain name ownership if they follow the rules of the smart contract (*ENS Architecture*, 2022). In order to register a Web3 domain name, users must have a crypto wallet for paying fees and also signing the transaction for storing on the blockchain. Users may connect their wallet address to both support their cryptocurrency addresses and their blockchain-based websites to be reachable through a domain name (Osborn & Alan, 2023). The content identifier of the website hosted on IPFS may be combined with the blockchain-based domain name. During the time this study is being conducted, Web2.0 browsers like Chrome and Safari are not able to access Web3-based websites. Chromium-based web browsers like Brave allows users to reach both traditional domains (like .com, .org, .edu etc.) and also decentralized domains (like .cyrpto, .eth, .zil etc.) stored on blockchain network (Sutopo, 2023).

vitalik.eth is a website being served on Web3. If a WHOIS lookup/registry information check is conducted via whois.domaintools.com, no information is shown, as indicated in Figure 8.

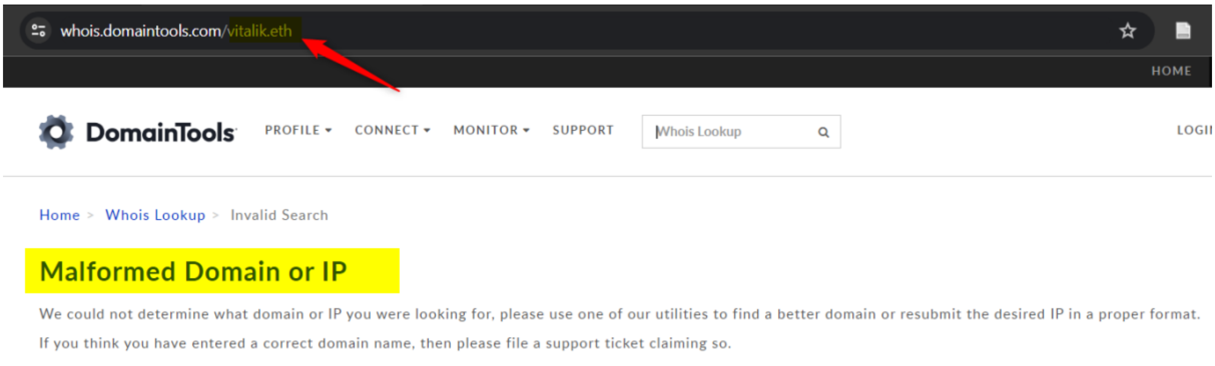

Figure 8. Whois record check for vitalik.eth

4. FINDINGS

The development of technology has not only led to changes in the traditional ways of committing crimes but also to the emergence of new types of crimes. Furthermore, it has brought about significant changes in the way law enforcement and judicial units investigate, probe, and prosecute crimes. While the crime of unlawful entry into a dwelling has long been defined as a crime in the criminal law of almost all countries, the unlawful seizure of a social media account was defined as a crime and subject to relevant laws not too long ago.

Many countries have started to integrate legal regulations, as well as integrating the innovations brought about by the development of technology into their work processes. New articles have been added to the criminal laws for cyber-dependent crimes, while for cyber-enabled crimes, existing articles have been regulated with the view of a "qualified form of the offense," often prescribing higher penalties for the same offense when committed using information technologies (Decker, 2007; Katyal, 2001; Payne et al., 2019; Rashkovski et al., 2016; Koto, 2021).

For both dependent and enabled, enforcement of cybercrimes faces challenges in identifying criminals, jurisdiction because of conflict of laws, providing evidence regarding its nature, dearth of data, and lack of sufficient or inadequate legislation (Ajayi, 2016). Due to the increasing investment, research, interest, and utilization of Web3 technologies, businesses also need to contemplate legal issues. Businesses that provide blockchain implementation/service or service enablers must not violate the current legal regulations and must fulfill the obligation to provide the requested documents or information to law enforcement or justice authorities as required by the current legal legislation after the service is used as an instrument for a crime. As a result, this paper aims to explore the legal challenges associated with existing Web3 applications and predict potential legal issues poised for blockchain-driven transformations. In the following section, current legal provisions in the Turkish legal system will be given, and the difficulties that may be experienced will be explained comparatively through an example case.

4.1. Regulating the Publications on the Internet

Law for Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publications No. 5651 provides the definitions, structure, and responsibilities of organizations such as content, host, and access providers (ISPs). The law regulates the prevention of access to publications or the removal of illegal content in which crimes are committed online. According to Law No. 5651, an "access provider" is defined as an operator or a natural or legal person that provides access to the internet environment for public internet use providers and their subscribers. The same law stipulates that, upon being duly notified in accordance with the relevant legislative provisions, the access provider is obligated to block access to the content, domain name, or IP address that constitutes the subject of a criminal offense. Article 8/17 declares that prevention of access is processed by blocking the related content through an individual URL if technically possible; if not, the entire website may be blocked from being accessed.

As discussed in section 2.2, two types of blocking methods could be used if the crime-related content is served over Web1.0 or Web2.0. The first one is DNS tampering (Akgül & Kırlıdoğ, 2015), which is about maintaining the internal DNS entry of the website to redirect users' queries to a different IP address than they should be. For example, let's assume that www.abc123.com publishes content facilitating the use of narcotics. And abc123.com is hosted at 192.168.1.2 IP address. If the ISP changes the DNS record for abc123.com to 172.16.8.4 (suppose that this is a website that notifies the user of the court order for blocking access to abc123.com), the user will be redirected to IP number 172.16.8.4 immediately after making a DNS query for abc123.com. The second one is IP-blocking (Akgül & Kırlıdoğ, 2015), which is about blocking the entire website via blocking the IP address of the website hosted. Considering the example above, if a user tries to reach the 192.168.1.2 IP address, on which www.abc.com is hosted, ISPs block all the traffic to that IP address.

On the other hand, if the crime-related content is served over Web3. then these two types of blocking methods become useless. Let's assume that the content is reachable at ipfs://abc123.eth. Since the website operates using the Decentralized Name service, which is not controlled by any central authority, and no entity can censor the system, there is no way to tamper with abc123.eth. As shown in Figure 8, there is no single IP address to tamper with. It is also impossible to block the traffic to abc123.eth because the files are hosted in a distributed manner, as discussed in section 2.6.1. If an end-user wants to reach abc123.eth, it will be redirected to different IP addresses that hold the content every time, making it impossible for ISPs to block traffic. But Article 19 of the "Regulation on the Principles and Procedures for the Regulation of Publications Made on the Internet Environment" stipulates that "*If the decision to block access given as an administrative measure is not implemented within twenty-four hours from the notification by the Presidency, the Presidency shall impose an administrative fine of ten thousand Turkish Lira to one hundred thousand Turkish Lira on the access provider (ISP). If the decision is not implemented within twenty-four hours from the moment the administrative fine is imposed, the Authority may decide to cancel the activity certificate upon the request of the Presidency*. This situation may create a conflict for a company operating in the field of internet service providers, which may result in punishment for a situation for which it cannot technically take precautions or action.

Similarly, under Law No. 5651, a "content host provider" is defined as a natural or legal person that provides or operates systems hosting services and content on the internet. According to Article 5 of the Law, the content host provider is obligated to remove unlawful content from publication upon being duly notified in accordance with Articles 8 and 9 of the same Law. In cases where the content host provider fails to fulfill its legal obligations, the same administrative sanctions outlined in the relevant regulation shall be imposed, as stipulated by the corresponding provision. In a blockchain-based infrastructure, a conflict may arise that could result in a penalty for a company operating as a content host provider as defined by law, for which it would technically be unable to take precautions or action.

For example, PeakD is a blockchain-based social media platform built on the Hive blockchain. It enables users to create, share, and monetize content in a transparent and censorship-resistant environment. Unlike traditional platforms, PeakD stores data on the Hive blockchain (*PeakD*, 2024). PeakD declares in the Legal Terms of Service section that the platform interacts with Hive blockchain. PeakD gives users control over their content consumption and creation while requiring them to comply with local laws and responsibly mark Not Safe for Work (NSFW) material. PeakD is a frontend tool for interacting with the Hive blockchain and does not control or manage it. Once content is posted on Hive, it is beyond PeakD's control to delete or modify it. Users are responsible for understanding the permanent nature of blockchain and making informed choices before posting any data. When the terms of service are examined, it is obvious that PeakD has no power to moderate the content on the blockchain. This decentralization ensures no single authority can fully remove or suppress the content. PeakD warns its users that they will be held responsible for any illegal content and that users should tag the content as NSFW. However, Law No. 5651 holds PeakD responsible for taking action in such a situation (if it were operating in Türkiye), and the warning the company has given to its users regarding its responsibilities is invalid regarding its own irresponsibility.

4.2. Efforts on Investigation

As aforementioned, almost all types of crimes can be committed using any form of information and communication technology. With the exponential increase in internet usage, criminals have found both a pool of victims and new opportunities (Curtis & Oxburgh, 2023). Law enforcement builds strategies for investigating these digital threats, which require more than analog approaches (Hull et al., 2018). Any content served on a website may contain violence against a person or animal, sexual offense, trade secret, sexual activity involving a child, blackmail, racial or religious insult, or some kind of offense that may be against state or public order. Although it is one of the biggest challenges law enforcement faces (Ajayi, 2016), identifying criminals becomes increasingly important for both punishment and stopping the crime being committed.

Articles 54 and 55 of the Turkish Commercial Code define any act that unjustly and misleadingly damages the commercial reputation of a business or individual as the offense of "defamation of commercial reputation." This offense typically manifests through actions that tarnish a company's reputation by disseminating false information or making misleading statements about its commercial activities, products, or services. In such cases, the affected business inevitably suffers both material and moral harm, leading to tangible economic consequences such as loss of customers, decreased sales, and reduced market share. The offense of defamation of commercial reputation is subject to criminal sanctions under Article 62 of the Turkish Commercial Code. Individuals who intentionally commit such acts of unfair competition may be punished with up to two years of imprisonment or a judicial fine.

For a real case, if a company reports that some misleading images/videos/comments of their business are spread through the social media platform www.abc123.com, then law enforcement starts to investigate to identify the criminal who has uploaded that content to the platform. The first step the police take is to find a legal contact to make a legal request for information, such as the IP address, registered e-mail, etc., of the user who uploaded this content. If there is no contact declared on the website, then police make a "WHOIS record check" for the registrant of abc123.com to find out a legal contact. Registrar information can also be used to find the registrant, as shown in Figure 3. After receiving the IP address information, police make another request from the ISP to find the user of this IP address. As mentioned in section 2.1, ISP may provide information such as identity and physical address. If the platform abc123.com requires signing up with an email address, then it can provide that information to the police for them to take the same steps to find out the user.

If this website is hosted on Web3 in ipfs://abc123.eth, it is hard to determine the registrant. As shown in Figure 9, the domain name's owner consists of just random numbers. If these random numbers have not made any identifiable transactions, it is almost impossible to find the owner/registrant. Since all the payments are made with cryptocurrency, which ends up with the same random numbers, finding the owner through financial transactions becomes almost impossible.

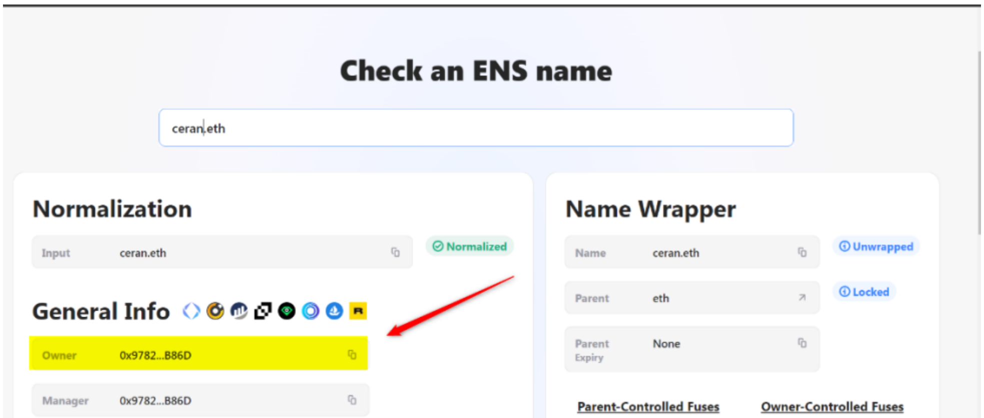

Figure 9. ENS record for owner

4.3. Intellectual Property

The significance of safeguarding intellectual property (IP) rights in Turkey has heightened, driven by its increasing connections with the European Union and the global community (Kula & Ozoguz, 2010). There are three main pieces of legislation regulating intellectual and industrial rights in Turkish law. These are the Law on Intellectual and Artistic Works (LIAW) No. 5846, the Industrial Property Law No. 6769, and the Law on the Protection of Integrated Circuit Topographies No. 5147. Especially, LIAW regulates all kinds of intellectual and artistic products that bear the characteristics of their owner and are considered works of science, literature, music, fine arts, or cinema, and the moral and financial rights related to them, which are declared in article

1/B as "works". According to LIAW, article 4, fine works of art include works of architecture that have aesthetic value (Çağla, 2021). It is not possible for ordinary products that can be easily created by anyone to be described as works within the scope of LIAW. It was stated that buildings with aesthetic value would be protected as "works of architecture," and in this way, it was accepted that architectural works could be protected as works of fine art. Article 16/1 of LIAW defines the right of the architect of the work to "prevent changes to be made in the work", one of the moral rights he obtains in this capacity. Accordingly, "*abbreviations, additions and other changes cannot be made in the work or in the name of the author without the permission of the author*." An architectural work becomes public when it is built, and the way in which the work is presented to the public also indicates the owner's choice in this regard. Therefore, the basis of the right to prevent changes also lies in the motive of not damaging the positive reference that the architect has obtained through the work in question (Gurkaynak et al., 2014).

As discussed in section 2.4.5, metaverses provide their users with the ability to create, buy, or sell digital assets in which these virtual worlds are not governed by a centralized organization, and users are able to create buildings. If an architectural work, let's assume the rectorate building of Gazi University, built in 1927 and a well-known one by all Turkish citizens, is recreated in a public metaverse in the same location as a digital twin. The owner of this digital twin may make some changes to the building, like removing the walls to change it to glass, creating an elevator on the corner, in order to change this building into an auto showroom. Since no single entity has the authority to alter the smart contract, nobody can restrict making changes to the digital twin. In addition, because the owner holds its assets with a crypto wallet, it is almost impossible to make a complaint about the changes to the building. As discussed above, the basis of the right to prevent changes lies in the motive of not damaging the positive reference that the architect has obtained through the work, although there is no change to physical building.

4.4. Confiscation

While traditional banking and financial intermediaries function with centralized authority, blockchain provides autonomous, self-executing, and decentralized applications that eliminate the need for intermediaries. Parties engage with intermediaries not necessarily due to efficiency but rather because these intermediaries possess the authority and reputation that instill trust (Fulmer, 2019). Groups prefer employing blockchain technology due to its attributes related to security and transaction speed for fraudulent activities. Specifically, the concept of decentralization, inherent in blockchain, provides a perception of anonymity for certain activities, even when the blockchain is publicly accessible (Rotundu, 2022). Cryptocurrency exhibits a 'pseudo-anonymous' nature, indicating that, although it can be traced to a specific computer or identified through a public key linked to a user, the user is not obliged to disclose their real-world identity. Additionally, it was created as a peer-to-peer platform to circumvent the regulatory mechanisms of a state's conventional financial sector (Fletcher et al., 2021).

Any proceeds of crime disrupt the state's economic structure. Confiscation, a punitive measure deeply rooted in criminal law since ancient times, is a form of sanction in nearly all legal systems. It involves the transfer of ownership rights from an entity to a public entity, terminating the ownership rights over a specific item. This occurs under specific legal conditions due to committing an offense (Avcı, 2014). Turkish Criminal Code No. 5271, Article 54 declares that *"Provided that they do not belong to bona fide third parties, the property used in the commission of an intentional crime or allocated to the commission of the crime or the property resulting from the crime shall be confiscated"*. And according to article 55, "confiscation of earnings" can be defined as the transfer of ownership to the state of the material benefits obtained by committing the crime, or the subject of the crime, or provided for the commission of the crime, and the economic gains resulting from their evaluation or transformation (Acar, 2019). The owner's authority must be initially revoked for the goods to be confiscated. This condition is articulated in Article 123 of the Code of Criminal Procedure No. 5271: "*Asset values that are deemed useful as a means of proof or that constitute the subject of confiscation of goods or earnings are kept under protection. It is stated that such items that the person keeping with him/her does not hand over with his/her consent may be confiscated*." In a seizure, ownership of the goods does not transfer to the state; however, if a confiscation decision is made, ownership of the goods is transferred to the state (Özden, 2023). In Article 128, it is declared that "*in cases where there is strong suspicion based on concrete evidence that the crime subject to investigation or prosecution has been committed and obtained from these crimes, the assets belonging to the suspect or defendant may be seized*."

To explain this situation with an example, let us assume that a decision to confiscate the assets of a suspect in which there is concrete evidence, according to the Financial Crimes Investigation Board report, that the suspect firm A has committed the offense of laundering the value of assets arising from crime within the scope of Article 282 of the Turkish Criminal Code No. 5237, based on Article 128 of the Criminal Procedure Code. The suspect's bank accounts will be blocked following the relevant legal decision in this case. Let us consider firm B as the victim here.

When the suspect firm A tries to access the bank account and make transactions using Web2.0 applications (via either website or mobile application), it will not be able to access due to the arrangement made in the central servers of the bank. The seizure process is technically that simple. In addition, the IP address information of the third person who tries to access these accounts during the operation can be kept as a log record. However, if the asset is a cryptocurrency in the Web3 ecosystem, performing the seizure may not be possible due to the decentralized structure. Suppose a hard wallet, a USB stick-sized device used for storing assets standalone, is seized during the operation. In that case, a third party can transfer the crypto asset using a backup wallet without anyone knowing, including the police (Nigh & Pelker, 2015). In such a scenario, the initially seized wallet loses its value entirely. S. K. Taylor et al. (2021) proposed a model where cryptocurrency can be transferred to a controlled wallet, where the information in the seized crypto wallet is accessible. However, as stated, a transaction fee will be charged for each transfer transaction on Web3. If the court decides to return the seized crypto asset to its owner as a result of the judgment, there is no provision in the current law for how the transaction fee will be covered. The model proposed by Taylor et al., (2021) is in force in the current legislation when the judicial authorities make the confiscation decision about the seized asset, such as currency or precious metal. In such a way, the asset in Turkish currency in the bank account is transferred to the Turkish currency account of the state free of charge using Web2.0 tools. There is no place in the current legislation for the transaction fee to be covered for the confiscation to be given a value on Web3. As (2022) declares, if crypto assets could be classified as money, then the legal system may apply the same kind of processes. However, cryptocurrencies do not meet the criteria because they are not a unit of account and do not store value.

5. DISCUSSION AND CONCLUSION

The period from the first introduction of the Internet protocol to its widespread use is undeniably long. These days, no one finds it strange that people communicate through the watch they wear on their wrists or even the refrigerator in the kitchen that communicates through the internet without needing a human being. It is a fact of human life that solutions are found for emerging needs and that the technologies offered as solutions give rise to new needs. While the need for human beings to access information more easily initiated the Web1.0 era, it is seen that the desire and need of the individual to create content himself/herself led to the beginning of the Web2.0 era. In this period, from the financial sector to education, from production to consumption, from the health sector to security, and from the private sector to the state, internet technologies have become the basic technology in every field where information is produced, transported, and used.

It is seen that the emergence of the Web3 era, thanks to blockchain technology, which has become known and recognized with Bitcoin, which is only one of its application areas, is also driven by similar needs. In the 2016 US presidential elections, Cambridge Analytica used millions of Facebook user data in the election campaign (Venturini & Rogers, 2019), raising questions about user data ownership. Although governments base their internet censorship decisions on religious, cultural, intellectual property, ideology, moral values, privacy, etc. (Ververis et al., 2020), autocracies make such decisions to undermine the power of civil society (Chang & Lin, 2020), and the desire for a censor-resistant communication has emerged. Similarly, since modern payment systems must rely on an intermediary, the bank, and the intermediary system reflects various and relatively high fees for each use (Perkins, 2020), the search for the elimination of intermediaries has led to the development of Web3 technologies and the work of many sectors and researchers on this subject.

Web3 represents a significant shift toward a decentralized internet, empowering users with greater control over their data and assets. While this transition offers substantial advantages, such as disrupting industries, increasing transparency, and fostering innovation, its widespread adoption is impeded by critical challenges. These include lack of clear regulatory frameworks. Alongside the extensive body of research on technological development, the literature also contains numerous national and international studies that identify and propose solutions for the legal issues arising from these advancements. Although these studies are based on different legal systems, they generally converge around the need to address uncertainties, foster international collaboration, and promote interdisciplinary cooperation among experts.

According to Dönder (2025), studying legal frameworks that grant smart contracts the status of legally binding agreements is crucial for their global enforceability. To address the legal and technical complexities in areas like intellectual property rights, harmonization of legal systems across different jurisdictions is necessary. Promoting international cooperation through solutions like standardized code infrastructure and common templates would facilitate the global application of smart contracts, thereby integrating them into worldwide legal systems. Can & Akman (2024), fully realizing the potential of blockchain technology in a governmental context emphasize the requirement for a collaborative effort among public administration experts, technology specialists, legal regulators, and the private sector. This cooperation is essential for developing effective and efficient policies that can facilitate the integration of blockchain into public services. Mustafa et al. (2025) emphasize that developing a comprehensive legal and governance framework for blockchain technology requires addressing a range of interconnected issues. From a legal perspective, it is essential to establish clear standards for data protection, privacy, accountability, and digital identification. Kshetri (2018) claims that the absence of a clear legal framework for intellectual property based on blockchain presents a major hurdle for protecting and enforcing Intellectual Property Rights. Traditional IP laws, like those for copyrights and patents, were created for a centralized system where ownership is straightforward to identify. However, blockchain's decentralized structure makes it difficult to apply these conventional legal frameworks to blockchain-based intellectual property. Zhuk (2025) highlights that the World Intellectual Property Organization (WIPO) has been exploring how blockchain can be used to protect and manage intellectual property rights. While WIPO acknowledges blockchain's potential as a secure, decentralized platform for this purpose, it also recognizes the critical need for a clear legal framework to ensure these rights are effectively protected and enforced.

Unlike other rules of order, rules of law, which exist to ensure peace and security and are the regulator and determinant of social life, are created by people as the need arises by accepting and putting in writing certain rules of behavior following certain bodies and certain procedures (Balı, 2004). For example, the Turkish Criminal Code, which regulates the sanctions against criminal behavior, was adopted in 1926 (Kaynak, 2022) and has undergone many changes over the past 100 years. The content of "special crimes committed using computers" was created with the 1991 amendment to the Turkish Criminal Code (Avşar & Öngören, 2010). Especially with the widespread use of Web2.0 technologies, Law No. 5651 on "Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications" entered into force in 2007. With the introduction and widespread use of Web3 technologies in our lives, it is clear that there is a need for legal regulations on this issue and that these regulations will be made according to the natural flow of life.

Research is being conducted on blockchain technology in connection with several widely recognized applications, encompassing but not limited to e-government (Çoban et al., 2024), finance (Yang et al., 2024), supply chain management (Alsmadi et al., 2023), auditing (Dong & Pan, 2023), healthcare (Sumathi et al., 2024), voting systems (Daraghmi et al., 2024), and Internet of Things (IoT) devices (Pandey et al., 2023). However, the fact that cryptocurrencies, such as Bitcoin, are the most well-known and famous application of Web3 technologies and that they propose or present an order that is the opposite of the existing economic and financial order globally seems to have led states to make or prioritize legal regulations on this issue in general. However, as Lehmann, (2021) notes, there is also uncertainty about the applicable laws and a legal disagreement in which a law court must decide whether a judgment should be made according to the laws of one country. Balancing technological innovation with legal compliance is a perpetual challenge for regulators. This difficulty arises from the likelihood that regulators will eventually develop new methods to regulate disruptive technological innovations in areas where regulation was previously insufficient (Dhali et al., 2023). However, Al-Tawil (2023) emphasizes that the current constraints necessitate a customized regulatory approach instead of relying on broad laws that lack precision.

The biggest problem with crimes using Internet technologies is that they are transnational crimes, meaning that where the crime is committed, where the offender is located, and where the victimization is experienced may differ. For this reason, the legal regulations to be realized must be internationally accepted and enable cooperation.

REFERENCES

Acar, H. (2019). *Confıscatıon Instıtutıon in Turkısh Crımınal Code* [Doctorate]. Çankaya University.

Ajayi, E. F. G. (2016). Challenges to enforcement of cyber-crimes laws and policy. *Journal of Internet and Information Systems*, *6*(1), 1–12. https://doi.org/10.5897/JIIS2015.0089

Akgül, M., & Kırlıdoğ, M. (2015). Internet censorship in Turkey. *Internet Policy Review*, *4*(2). https://doi.org/10.14763/2015.2.366

Alabdulwahhab, F. A. (2018). Web 3.0: The decentralized web blockchain networks and protocol innovation. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 1–4.

Alizadeh, M., Andersson, K., & Schelén, O. (2020). Efficient decentralized data storage based on public blockchain and IPFS. *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 1–8.

Alsmadi, A. A., Alrawashdeh, N., Al-Gasaymeh, A., Alhawamdeh, L. N., & Al_Hazimeh, A. M. (2023). Adoption of Blockchain Technology in Supply Chain. *Sage Open*, *13*(1), 21582440231160143. https://doi.org/10.1177/21582440231160143

Avcı, M. (2014). *A Study on Confiscation Without Expropriation in the Turkish Law*. https://earsiv.anadolu.edu.tr/xmlui/handle/11421/18793

Avşar, Z., & Öngören, G. (2010). *Bilişim Hukuku* (1st ed.). Türkiye Bankalar Birliği.

Aydar, M., Cetin, S. C., Ayvaz, S., & Aygun, B. (2020). *Private key encryption and recovery in blockchain* (arXiv:1907.04156). arXiv. http://arxiv.org/abs/1907.04156

Balı, A. Ş. (2004). Hukukun Bilimselliği Sorunu. *Selçuk Universitesi Hukuk Fakültesi Dergisi*, *12*(1), 223–237.

Bambacht, J., & Pouwelse, J. (2022). *Web3: A Decentralized Societal Infrastructure for Identity, Trust, Money, and Data* (arXiv:2203.00398). arXiv. http://arxiv.org/abs/2203.00398

Bodziony, N., Jemioło, P., Kluza, K., & Ogiela, M. R. (2021). Blockchain-Based Address Alias System. *Journal of Theoretical and Applied Electronic Commerce Research*, *16*(5), 1280–1296. https://doi.org/10.3390/jtaer16050072

Çağla, E. (2021). Fotoğrafçıların Telif Hakları ve Etik Dışı Kullanım Örnekleri. *Kesit Akademi*, *29*(29), 188–209. https://doi.org/10.29228/kesit.52617

Can, Y., & Akman, E. (2024). Blokzincir Teknolojisi ve Verimlilik İlişkisi: Türk Kamu Yönetiminde Mevcut Durum Analizi. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, *80*, 196–222. https://doi.org/10.51290/dpusbe.1443217

Chainalysis. (2023). *The Chainalysis 2023 Geography of Cryptocurrency Report* [Statistical]. https://www.chainalysis.com/blog/middle-east-north-africa-mena-cryptocurrency-adoption/

Chainalysis. (2024). *The Chainalysis 2023 Geography of Cryptocurrency Report* [Statistical]. https://www.chainalysis.com/blog/2024-global-crypto-adoption-index/

Chang, C.-C., & Lin, T.-H. (2020). Autocracy login: Internet censorship and civil society in the digital age. *Democratization*, *27*(5), 874–895. https://doi.org/10.1080/13510347.2020.1747051

Çoban, Ş., Fethi, S., Tanova, C., & Obaegbulam, O. (2024). Adoption of e-Government Services in the Northern Part of Cyprus: The Role of Blockchain Technology Awareness. *Sage Open*, *14*(4), 21582440241292898. https://doi.org/10.1177/21582440241292898

Coull, S. E., White, A. M., Yen, T.-F., Monrose, F., & Reiter, M. K. (2012). Understanding domain registration abuses. *Computers & Security*, *31*(7), 806–815. https://doi.org/10.1016/j.cose.2012.05.005

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal: Theory, Practice and Principles*, *96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Daraghmi, E., Hamoudi, A., & Abu Helou, M. (2024). Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology in the Context of Palestine. *Future Internet*, *16*(11), 388. https://doi.org/10.3390/fi16110388

Datysgeld, M. (2017). Understanding the Role of states in global internet governance: ICANN and the question of legitimacy. *GigaNet: Global Internet Governance Academic Network, Annual Symposium*.

Decker, C. (2007). Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime. *S. Cal. L. Rev.*, *81*, 959.

Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F. (2023). Cryptocurrency in the Darknet: Sustainability of the current national legislation. *International Journal of Law and Management*, *65*(3), 261–282. https://doi.org/10.1108/IJLMA-09-2022-0206

Di Pierro, M. (2017). What is the blockchain? *Computing in Science & Engineering*, *19*(5), 92–95.

Dönder, B. Ş. (2025). Blokzincir Tabanlı Sözleşmelerin Fikrî Mülkiyet Hukukuna Etkisi: Dönüşüm ve Öneriler. *Akdeniz Üniversitesi Hukuk Fakültesi Dergisi*, *15*(1), 649–668. https://doi.org/10.54704/akdhfd.1675422

Dong, Y., & Pan, H. (2023). Enterprise Audits and Blockchain Technology. *Sage Open*, *13*(4), 21582440231218839. https://doi.org/10.1177/21582440231218839

ENS Architecture. (2022). [Online post]. ENS Documentation. https://docs.ens.domains/

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, *56*, 101387. https://doi.org/10.1016/j.ribaf.2021.101387

Fulmer, N. (2019). Exploring the Legal Issues of Blockchain Applications. *Akron Law Review*, *52*.

Gurkaynak, G., Karaoğlan Nalçacı, C., & Gönen, C. (2014). Mimari Yapıların Eser Niteliği ve Eser Sahibinin Değişiklik Yapılmasını Önleme Hakkı (Qualification of Buildings As Copyrighted Works and Author's Right of Integrity). *Legal Fikri ve Sınai Haklar Dergisi (2014) Vol*, *10*.

Hiremath, B. K., & Kenchakkanavar, A. Y. (2016). An alteration of the web 1.0, web 2.0 and web 3.0: A comparative study. *Imperial Journal of Interdisciplinary Research*, *2*(4), 705–710.

Hull, M., Eze, T., & Speakman, L. (2018). Policing The Cyber Threat: Exploring the Threat from Cyber Crime and the Ability of Local Law Enforcement to Respond. *2018 European Intelligence and Security Informatics Conference (EISIC)*, 15–22. https://doi.org/10.1109/EISIC.2018.00011

Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review*, *149*(4), 1003–1114.

Kaynak, A. F. (2022). 1858 Tarihli Ceza Kanunnamesi ile 1926 Tarihli Türk Ceza Kanunu'nun Foucaultçu Perspektiften Karşılaştırılması. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*. https://doi.org/10.33717/deuhfd.1089763

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

Korpal, G., & Scott, D. (2023). Decentralization and web3 technologies. *Authorea Preprints*.

Koto, I. (2021). Cyber Crime According to the ITE Law. *International Journal Reglement & Society (IJRS*. https://doi.org/10.55357/ijrs.v2i2.124

Kshetri, N. (2018). 1 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

Küçükkalay, M. (1997). Endüstri Devrimi ve Ekonomik Sonuçlarının Analizi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *2*(2).

Kula, E., & Ozoguz, S. (2010). Development of intellectual property rights in Turkey and its implications for the Turkish economy. *Intellectual Property, Innovation and Management in Emerging Economies. Ed. Ruth TAPLIN ve Alojzy Z. NOWAK. Routledge. New York*, 125–142.

Kumar, S. (2019). A review on client-server based applications and research opportunity. *International Journal of Recent Scientific Research*, *10*(7), 33857–3386.

Lehmann, M. (2021). National Blockchain Laws as a Threat to Capital Markets Integration. *Uniform Law Review*, *26*(1), 148–179. https://doi.org/10.1093/ulr/unab004

Liu, Z., Xiang, Y., Shi, J., Gao, P., Wang, H., Xiao, X., Wen, B., Li, Q., & Hu, Y.-C. (2022). Make Web3.0 Connected. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 2965–2981. https://doi.org/10.1109/TDSC.2021.3079315

Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 254–269.

Malhotra, A., O'Neill, H., & Stowell, P. (2022). Thinking strategically about blockchain adoption and risk mitigation. *Business Horizons*, *65*(2), 159–171. https://doi.org/10.1016/j.bushor.2021.02.033

Min, T., & Cai, W. (2022). Portrait of decentralized application users: An overview based on large-scale Ethereum data. *CCF Transactions on Pervasive Computing and Interaction*, *4*(2), 124–141. https://doi.org/10.1007/s42486-022-00094-6

Momtaz, P. P. (2022). How Efficient is Decentralized Finance (DeFi)? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4063670

Mozumder, M. A. I., Sheeraz, M. M., Athar, A., Aich, S., & Kim, H.-C. (2022). Overview: Technology roadmap of the future trend of metaverse based on IoT, blockchain, AI technique, and medical domain metaverse activity. *2022 24th International Conference on Advanced Communication Technology (ICACT)*, 256–261.

Mueller, M. (2000). Technology and institutional innovation: Internet domain names. *International Journal of Communications Law and Policy*, *5*, 1–32.

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. *Access Denied: The Practice and Policy of Global Internet Filtering*, *1*(1), 58.

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain-based governance models in e-government: A comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management*, *67*(1), 37–55. https://doi.org/10.1108/IJLMA-08-2023-0172

Mystakidis, S. (2022). Metaverse. *Encyclopedia*, *2*(1), 486–497. https://doi.org/10.3390/encyclopedia2010031

Nigh, B., & Pelker, A. (2015). *Virtual Currency: Investigative Challenges and Opportunities*. FBI: Law Enforcement Bulletin. https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities

Osborn, G., & Alan, N. (2023). Web 3 disruption and the domain name system: Understanding the trends of blockchain domain names and the policy implications. *Journal of Cyber Policy*, 1–23.

Özden, N. K. (2023). TÜRK CEZA HUKUKUNDA MÜSADERE. *Ankara Sosyal Bilimler Üniversitesi Hukuk Fakültesi Dergisi*, *5*(2), 1058–1086. https://doi.org/10.47136/asbuhfd.1282905

Ozili, P. K. (2022). Decentralized finance research and developments around the world. *Journal of Banking and Financial Technology*, *6*(2), 117–133. https://doi.org/10.1007/s42786-022-00044-x

Pandey, M., Velmurugan, M., Sathi, G., Abbas, A. R., Zebo, N., & Sathish, T. (2023). Blockchain Technology: Applications and Challenges in Computer Science. *E3S Web of Conferences*, *399*, 04035. https://doi.org/10.1051/e3sconf/202339904035

Parziale, L., Liu, W., Matthews, C., Rosselot, N., Davis, C., Forrester, J., & Britt, D. T. (2006). *TCP/IP tutorial and technical overview*.

Payne, B. K., Hawkins, B., & Xin, C. (2019). Using Labeling Theory as a Guide to Examine the Patterns, Characteristics, and Sanctions Given to Cybercrimes. *American Journal of Criminal Justice*, *44*(2), 230–247. https://doi.org/10.1007/s12103-018-9457-3

PeakD. (2024). [Social Media]. Decentralize Social Media With True Ownership. https://peakd.com/

Perkins, D. W. (2020). *Cryptocurrency: The Economics of Money and Selected Policy Issues* (CRS R45427; p. 32).

Politou, E., Alepis, E., Patsakis, C., Casino, F., & Alazab, M. (2020). Delegated content erasure in IPFS. *Future Generation Computer Systems*, *112*, 956–964. https://doi.org/10.1016/j.future.2020.06.037

Popescu, A.-D. (2020). Decentralized finance (defi)–the lego of finance. *Social Sciences and Education Research Review*, *7*(1), 321–349.

Rashkovski, D., Naumovski, V., & Naumovski, G. (2016). Cybercrime Tendencies and Legislation in the Republic of Macedonia. *European Journal on Criminal Policy and Research*, *22*(1), 127–151. https://doi.org/10.1007/s10610-015-9277-7

Rotundu, V.-A. (2022). Impact of Blockchain Technology: Benefits and Security Risk and Threats. *Informatica Economica*, *26*(2/2022), 37–45. https://doi.org/10.24818/issn14531305/26.2.2022.04

Sarmah, S. S. (2018). Understanding blockchain technology. *Computer Science and Engineering*, *8*(2), 23–29.

Sumathi, M., S, K., Sailendra, K., Deepak, T., Khatri, G., & Raja, S. P. (2024). Blockchain-based health insurance claim processing and management system. *Multiagent and Grid Systems*, *20*(2), 185–201. https://doi.org/10.3233/MGS-240101

Suratkar, S., Shirole, M., & Bhirud, S. (2020). Cryptocurrency wallet: A review. *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 1–7.

Sutopo, A. H. (2023). *Unlocking the Future: Building Web3 Websites with Unstoppable Domain*. Topazart.

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

Taherdoost, H. (2023). Smart Contracts in Blockchain Technology: A Critical Review. *Information*, *14*(2), 117. https://doi.org/10.3390/info14020117

Taylor, D. E., Turner, J. S., Lockwood, J. W., Sproull, T. S., & Parlour, D. B. (2003). Scalable IP lookup for internet routers. *IEEE Journal on Selected Areas in Communications*, *21*(4), 522–534. https://doi.org/10.1109/JSAC.2003.810507

Taylor, S. K., Ariffin, A., Zainol Ariffin, K. A., & Sheikh Abdullah, S. N. H. (2021). Cryptocurrencies Investigation: A Methodology for the Preservation of Cryptowallets. *2021 3rd International Cyber Resilience Conference (CRC)*, 1–5. https://doi.org/10.1109/CRC50527.2021.9392446

Ververis, V., Marguel, S., & Fabian, B. (2020). Cross-Country Comparison of Internet Censorship: A Literature Review. *Policy & Internet*, *12*(4), 450–473. https://doi.org/10.1002/poi3.228

Wood, G. (2014). *Less-techy: What is Web 3.0?* https://gavwood.com/web3lt.html

Yang, Z., Ali, S., Tao, W., & Chen, H. (2024). From Transactions to Transformation: Exploring the Impact of Blockchain on Customer Financial Well-being. *Sage Open*, *14*(2), 21582440241253955. https://doi.org/10.1177/21582440241253955

Ye, H., & Park, S. (2021). Reliable Vehicle Data Storage Using Blockchain and IPFS. *Electronics*, *10*(10), 1130. https://doi.org/10.3390/electronics10101130

Yu, G., Wang, X., Wang, Q., Bi, T., Dong, Y., Liu, R. P., Georgalas, N., & Reeves, A. (2023). *Towards Web3 Applications: Easing the Access and Transition* (arXiv:2210.05903). arXiv. http://arxiv.org/abs/2210.05903

Zheng, P., Jiang, Z., Wu, J., & Zheng, Z. (2023). Blockchain-based Decentralized Application: A Survey. *IEEE Open Journal of the Computer Society*.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557–564.

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, *105*, 475–491. https://doi.org/10.1016/j.future.2019.12.019

Zhuk, A. (2025). Beyond the blockchain hype: Addressing legal and regulatory challenges. *SN Social Sciences*, *5*(2), 11. https://doi.org/10.1007/s43545-024-01044-y