Anthology: Inside Intellectual Property Rights
Vol. 3 No. 1 (2025)
https://ojs.uph.edu/index.php/Anthology

Guardians of the Road: Utilizing Blockchain to Prevent Automotive IP Theft

Jeralyn Valencia[1], Shawn Oliviere[2]

[1,2] Business Law, Faculty of Law, Pelita Harapan University, Tangerang

[1]Jeralynvalencia23@gmail.com
[2]oliviereshawn@gmail.com

Abstract
Intellectual Property (IP) theft poses severe challenges to global innovation, particularly in the automotive sector. Counterfeit products, including critical safety components, infiltrate legitimate markets, creating a "dirty economy" that undermines consumer trust and stifles technological progress. Notable cases, such as Mercedes-Benz's global crackdown on counterfeit parts and trade secret theft incidents involving major automakers, illustrate the scale and impact of IP infringement. These issues are compounded by the rise of counterfeit goods, which not only impose financial losses but also endanger public safety, fuel organized crime, and discourage investment in research and development (R&D). The economic repercussions extend beyond immediate financial damage, hindering advancements in emerging technologies like electric vehicles (EVs), autonomous systems, and connectivity. Blockchain technology emerges as a revolutionary solution to these challenges. With its decentralized, immutable, and tamper-resistant structure, blockchain provides a robust framework for secure IP protection. Key features, such as distributed ledgers, smart contracts, and public key cryptography, enable precise tracking of IP rights and automated enforcement of agreements, eliminating the need for intermediaries. Blockchain's inherent transparency and resilience address vulnerabilities in traditional IP protection mechanisms, fostering trust and reliability. This abstract explores the consequences of IP theft on innovation and the transformative potential of blockchain in safeguarding intellectual property, focusing on its application in the automotive sector. The analysis highlights the necessity of integrating blockchain technology to mitigate risks, protect innovation-driven industries, and sustain economic growth in the face of escalating IP theft.

Keywords: Intellectual Property (IP) theft; blockchain technology; innovation-driven industries

A. Introduction

Intellectual property (IP) theft poses a significant challenge to the automotive industry, severely undermining its competitive edge and innovation potential. IP encompasses a broad spectrum of intangible proprietary information, including product launch plans, manufacturing processes, registered patents, and trade secrets. As defined by the World Intellectual Property Organization (WIPO), IP refers to creations of the mind, such as inventions, designs, symbols, and names used in commerce[1].

The global economy faces persistent challenges from intellectual property theft, particularly in key regions such as the United States and the European Union, where IP-intensive sectors play a vital role in economic performance. In the United States alone, these industries generate more than $7 trillion annually for the national GDP and support nearly 50% of the workforce. Despite their importance, the rising prevalence of IP theft has intensified its financial toll, with losses surging by 36% from 2022 to 2023, totaling $1.12 billion.[2]

Intellectual property-intensive industries contribute significantly to the European Union's (EU) economy, driving 42% of its total economic activity and employing 28% of its workforce. However, these sectors are under threat, particularly in the automotive industry, where counterfeit goods cause major disruptions. Annually, fake tires and batteries alone result in financial losses of €2.2 billion and €180 million, respectively. In 2019, counterfeit goods made up 5.8% of all imports into the EU, amounting to an estimated €119 billion.[3].

The growth of e-commerce has made it easier than ever for counterfeit goods to flood international markets. According to the OECD, the trade in counterfeit products has skyrocketed, jumping 154% from $200 billion in 2005 to an astonishing $509 billion in 2016. This surge highlights just how much the problem has grown in today's digital age.[4] Between 2000 and 2018, U.S. Customs and Border Protection (CBP) reported a staggering tenfold increase in seizures of counterfeit goods, much of it moving through e-commerce channels. Alarmingly, over 85% of these fake products came from China and Hong

[1]"What is Intellectual Property?" accessed December 11, 2024, https://www.wipo.int/about-ip/en/.
[2]"Top IP theft statistics and stories in 2023." *Cyberhaven*, accessed 11 December 2024. https://www.cyberhaven.com/guides/top-ip-theft-statistics.
[3]Catherine De Bolle and Christian Archambeau, "Intellectual Property Crime Threat Assessment 2022" (Research Report, Europol, The Hague, 2022), page 36, accessed 11 December 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Report.%20Intellectual%20property%20crime%20threat%20assessment%202022_2.pdf.
[4]"Background Note: Illicit Trade Forum" (Research Report, UNCTAD, Geneva, 2020), page 17, accessed 11 December 2024, https://unctad.org/system/files/non-official-document/DITC2020_BackgroundNote_UNCTAD%20Illicit%20Trade%20Forum_en.pdf.

Kong[5]. his trend aligns with findings from the OECD, which show that counterfeits infiltrate nearly every industry—from luxury goods to essential items like automotive parts, medicines, and even food. The automotive sector is especially hard-hit, with counterfeit parts not only cutting into revenue but also eroding consumer trust and jeopardizing safety.

These developments highlight the significant scale of IP theft and its lasting economic and competitive consequences, especially for industries like automotive manufacturing, where innovation and safety are paramount. In this context, blockchain-based smart contracts emerge as a robust technological solution to mitigate the challenges posed by IP theft and infringement. By leveraging blockchain technology, key data—such as patents, designs, and trade secrets—can be securely stored on an immutable ledger, ensuring authenticity, integrity, and traceability. This capability is crucial for resolving disputes and proving ownership, especially in supplier collaborations where access to sensitive automotive data is necessary for component manufacturing.

Blockchain technology's decentralized nature eliminates single points of failure, thereby reducing the risk of cyberattacks and unauthorized access. Additionally, blockchain-based smart contracts facilitate automated and streamlined processes for managing IP rights, including licensing, royalty payments, and compliance monitoring. This not only reduces transaction costs but also ensures that companies maintain control over their intellectual assets while safeguarding their competitive position.

Given the automotive industry's reliance on innovation and its vulnerability to IP theft, the adoption of blockchain-based smart contracts represents a powerful mechanism to address these issues. By providing a secure, efficient, and transparent framework, these technologies enable automotive companies to protect their proprietary information, preserve competitive advantages, and foster an environment that incentivizes sustainable innovation.

In this regard, this research analyzes the following formulation of issues:

i. How blockchain e-contracts address the vulnerabilities in IP management?
ii. What are their economic, operational, and legal implications for the automotive sector?

[5]"Fiscal Year 2023 Annual Report to Congress" (Research Report, Executive Office of the President, United States, 2024), page 17, accessed 11 December 2024, https://www.whitehouse.gov/wp-content/uploads/2024/04/IPEC-FY-23-Annual-Report_Final.pdf.

B. Research Method

This study takes a practical, real-world approach to tackling the increasing issue of intellectual property (IP) theft in the automotive industry. With the growing challenges of counterfeit products and stolen technologies, the research investigates how blockchain technology, specifically smart contracts, can be a powerful solution for protecting valuable IP assets like patents, trade secrets, and proprietary designs. By exploring tangible, actionable solutions, the study dives into how blockchain can help preserve the integrity and value of these assets.[6]

The study also examines the significant financial impact of IP theft on the automotive sector, revealing the losses businesses face due to counterfeit goods and IP violations. It highlights the shortcomings of current protection systems and their failure to fully address the scale of the problem. In response, the research explores how blockchain can be applied to areas like patent registration, licensing, and anti-counterfeiting efforts, showing how these tools can automate and secure IP management. Additionally, the research touches on blockchain's broader benefits, including enhanced financial and data security, while also addressing regulatory concerns like GDPR compliance and the complexities of enforcing IP rights across different countries.

By analyzing real-world case studies, industry practices, and global data, the study provides actionable insights into how blockchain can be effectively integrated into the automotive industry to improve IP protection. It underscores the need for blockchain technology to help foster innovation, build trust, and safeguard competitive advantages as IP theft and counterfeiting continue to rise. Ultimately, this research aims to offer a practical framework that stakeholders in the automotive industry can use to strengthen IP security, reduce risks, and support long-term growth and sustainability.

C. Analysis and Discussion

C.1 Consequences for innovation: How IP theft discourages R&D investment and slows technological progress.

This is particularly evident in the automotive sector, where counterfeit components infiltrate legitimate markets, creating a "dirty economy." Counterfeit parts appeal to budget-conscious consumers but fail prematurely, which results in dangerous consequences for its users.[7] While this dynamic indirectly benefits legitimate

[6] Akbar Nugroho and Davi Pandi, "The Issue of No Benchmark in Determining the Economic Value of Intellectual Property" 2, no. 1 (2024): 284–99.
[7] "Impact of the Counterfeit Market on the Automobile Industry," *Ennoventure*, accessed 11 December 2024, https://ennoventure.com/blogs/impact-of-the-counterfeit-market-on-the-automobile-industry/.

manufacturers, it undermines trust in innovation-driven brands and discourages future technological advancement

Intellectual property (IP) infringement, including patent infringement, trademark counterfeiting, copyright piracy, and trade secret theft, causes significant financial losses for right holders and legitimate businesses.[8] IP infringement can undermine U.S. competitive advantages in innovation and creativity, to the detriment of American workers and businesses. In its most pernicious forms, IP infringement endangers the public, including through exposure to health and safety risks from counterfeit products, such as semiconductors, automobile parts, apparel, footwear, toys, and medicines. In addition, trade in counterfeit and pirated products often fuels cross-border organized criminal networks, increases the vulnerability of workers to exploitative labor practices, and hinders sustainable economic development in many countries.[9]

The implications of IP theft extend beyond immediate financial damage, significantly discouraging investment in research and development (R&D). When proprietary technologies are stolen, competitors bypass costly and time-consuming R&D processes, bringing products to market more quickly and cheaply. This diminishes returns for innovators, discouraging further investment in critical areas like EVs, autonomous driving systems, and connectivity.[10]

C2 Case Studies: Example of companies that suffered from IP theft or patent infringement.

a. Mercedes-Benz Battle Against Counterfeit Parts

In 2023, Mercedes-Benz conducted over 740 global raids, seizing 1.6 million counterfeit parts, including critical safety components like brakes, wheels, and steering systems. These fake products, often failing to meet safety standards, pose serious risks to road users. The brand protection team also removed more than 142,000 online listings, reflecting a 20% increase in enforcement actions compared to 2022. Mercedes-Benz emphasized the organized crime links of counterfeiting and

[8] Fajar Sugianto, Astrid Athina Indradewi, and Yohanie Maretta, "Book Pirates and Copycats : Infringement That Speaks For Itself" 2, no. 1 (2024): 259–69.

[9] "2024 Special 301 Report" (Research Report, USTR, Washington, D.C., 2024), page 9, accessed 11 December 2024, https://ustr.gov/sites/default/files/2024%20Special%20301%20Report.pdf.

[10] "Intellectual Property Theft and the Economy" (Research Report, United States Congress, Washington, D.C., 2012), page 1, accessed 11 December 2024, https://www.jec.senate.gov/public/_cache/files/aa0183d4-8ad9-488f-9e38-7150a3bb62be/intellectual-property-theft-and-the-economy.pdf.

urged consumers to be vigilant about suspiciously low prices and unreliable sellers, highlighting the safety and economic threats posed by counterfeit goods[11].

b. Coda's Misappropriated Propriety

The case Coda Development S.R.O. v. Goodyear Tire & Rubber Co. centered around allegations of trade secret misappropriation and patent infringement. In 2009, Coda Development shared confidential information about its self-inflating tire (SIT) technology with Goodyear under a nondisclosure agreement (NDA) during discussions of potential collaboration. The proprietary information included detailed designs, prototypes, and technological processes.

After the discussions, Goodyear ceased communication with Coda and later filed a patent application for a self-inflating tire assembly, listing its own employees as inventors and excluding any acknowledgment of Coda's contributions. This led Coda to file a lawsuit in the U.S. District Court for the Northern District of Ohio, where Goodyear is headquartered.

The jury found that Goodyear had violated the NDA and misappropriated Coda's trade secrets, awarding Coda $64 million in damages. The verdict emphasized the legal and ethical responsibility to respect confidentiality agreements and protect intellectual property in collaborative business relationships. This ruling also serves as a precedent for the importance of upholding NDAs in safeguarding innovation[12]. The case highlights the vulnerabilities faced by not only the big automotive players but smaller innovators in the automotive industry also risk itself from IP infringement when partnering with larger corporations and serves as a critical reminder for businesses to ensure robust legal safeguards and enforceable agreements when sharing sensitive information.

c. General Motors Trade Secret Theft By Former Employee

This case revolves around Shanshan Du, a former General Motors (GM) employee, and her husband, Yu Qin, who were found guilty of stealing confidential information related to GM's hybrid vehicle systems. In 2003, Du transitioned to a role that granted her access to sensitive hybrid technology. Over the following two years, she copied proprietary documents before departing from the company in 2005 after accepting a severance package. Investigators uncovered GM's trade secrets stored on multiple computers owned by the couple.

[11]"Mercedes-Benz Cracks Down on Counterfeits in 2023," *The Brake Report*, 2023, accessed 11 December 2024, https://www.thebrakereport.com/mercedes-benz-cracks-down-on-counterfeits-2023/.
[12]Coda Development S.R.O. v. Goodyear Tire & Rubber Co., No. 5:15-cv-1572 (N.D. Ohio 2023), accessed 11 December 2024, https://casetext.com/case/coda-dev-v-goodyear-tire-rubber-co-1.

Qin, meanwhile, established a company called Millennium Technology International and allegedly engaged with GM competitors in China, though there was no direct evidence that the stolen information was shared overseas. A federal jury in Detroit convicted both individuals, with Qin also found guilty of wire fraud and obstruction of justice after shredding documents to derail the investigation. Prosecutors estimated the stolen technology's value at $40 million, based on licensing fees paid by other automakers.

Both Du and Qin face a potential 20-year prison sentence. This incident, along with other cases like former Ford engineer Xiang Dong Yu's theft of proprietary data, underscores the ongoing threat of intellectual property breaches in the automotive sector and the critical need for stringent protections.[13]

d. Battery Trade Secret Theft

Klaus Pflugbeil, a Canadian-German dual citizen, admitted guilt to charges of conspiring to steal proprietary information from a prominent U.S.-based electric vehicle (EV) manufacturer, referred to as "Victim Company-1." Along with his accomplice, Yilong Shao, Pflugbeil illicitly acquired advanced battery assembly technology from Victim Company-1. This technology, essential for precision battery production, became part of Victim Company-1's portfolio after it acquired a Canadian company where both conspirators had previously worked.

The stolen technology was used to launch a Chinese enterprise, "Business-1," which manufactured and marketed identical battery assembly systems in direct competition with Victim Company-1. To conceal their theft, they reformatted the documents to obscure their origin and promoted their products online. During a Las Vegas trade show, undercover FBI agents secured incriminating evidence when Pflugbeil provided a detailed proposal containing proprietary information. Pflugbeil was apprehended and later pleaded guilty, facing a potential 10-year prison sentence, with sentencing set for October 9, 2024. This case underscores the collaborative efforts of the FBI and the Disruptive Technology Strike Force in addressing trade secret theft within the EV sector.[14]

[13]United States v. Du and Qin. No. 13-1778 (6th Cir. 2014). https://law.justia.com/cases/federal/appellate-courts/ca6/13-1778/13-1778-2014-06-26.html.

[14]United States Department of Justice, "Resident of China Pleads Guilty to Conspiracy to Send Leading Electric Vehicle Company's Trade Secrets to China," *Department of Justice*, accessed 11 December 2024, https://www.justice.gov/opa/pr/resident-china-pleads-guilty-conspiracy-send-leading-electric-vehicle-companys-trade-secrets.

C.3 Blockchain Technology: A Revolution in IP Protection

Blockchain is a decentralized and distributed digital ledger technology designed to record and store data securely across a network of computers. Its structure is inherently transparent, tamper-resistant, and immutable, meaning that once data is added, it cannot be altered or deleted. Each "block" in the chain contains specific data and is cryptographically linked to the previous block, creating a sequential, verifiable record of transactions. This design ensures the integrity and reliability of the stored information, making blockchain a groundbreaking innovation for secure data management and trust-based systems.[15]

What sets blockchain apart is its ability to enhance accuracy, reduce costs, and improve security in data management and transactions. By automating verification processes and eliminating the need for third-party intermediaries, blockchain ensures faster, more cost-effective, and highly efficient operations. Its decentralized nature makes tampering nearly impossible, providing a robust safeguard for sensitive information.[16]

Building on this, blockchain's security framework is rooted in its decentralized structure, cryptographic principles, and consensus mechanisms. Each block is cryptographically linked to the previous one, ensuring that any attempt to alter a block would require recalculating the hashes of all subsequent blocks, a nearly impossible task in large networks. Security is further strengthened by the distributed network of nodes, which validate transactions and detect tampering attempts. While smaller networks may face risks like a "51% attack," major blockchains like Bitcoin and Ethereum mitigate such threats through their scale and design. Bitcoin's immense computational power and Ethereum's proof-of-stake model make unauthorized manipulation practically infeasible.[17] These qualities make blockchain particularly valuable in environments with unstable governance or limited infrastructure, offering a secure and reliable system for protecting both personal and organizational data.

Blockchain's ability to function as a secure, transparent, and tamper-resistant digital ledger is rooted in several key features that make it uniquely reliable for data management. These defining characteristics of decentralization, immutability, and consensus are the foundation of its structure and operations. Each feature contributes to blockchain's integrity and efficiency, as detailed below.

---

[15]Hayes, Adam. "Blockchain Facts: What Is It, How It Works, and How It Can Be Used." *Investopedia*, accessed 11 December 2024, https://www.investopedia.com/terms/b/blockchain.asp.
[16]"What are the Benefits of Blockchain?" Accessed December 11, 2024. https://www.ibm.com/topics/benefits-of-blockchain.
[17]"Cryptographic Consensus Mechanisms in Blockchain," accessed December 11, 2024, https://www.geeksforgeeks.org/cryptographic-consensus-mechanisms-in-blockchain/.

a. Decentralization

In a blockchain system, data is not stored in a single centralized location. Instead, it is distributed across a network of computers, known as nodes, with each node maintaining a complete copy of the blockchain. This distribution ensures that the system remains functional and secure, even if one or more nodes are compromised or go offline.

The decentralized nature of blockchain eliminates the risk of a single point of failure. For instance, even if one node in the network is attacked or malfunctions, the remaining nodes can continue to operate seamlessly, preserving the integrity and accessibility of the data. This design makes blockchain systems highly resilient to cyberattacks or technical disruptions. Nakamoto (2008) highlights that this structure is a core strength of blockchain, offering unmatched reliability for secure data storage and transactions.[18]

b. Immutability

Once data is recorded on a blockchain, it cannot be altered or deleted. Each block is cryptographically linked to the previous one through a unique hash, forming a secure and tamper-proof chain of records. This feature ensures that information remains permanent and trustworthy over time, making blockchain particularly useful for applications where data integrity is critical, such as financial transactions, intellectual property records, and supply chain tracking.

For example, if a transaction is added to the blockchain, it becomes locked in place. Any attempt to change it would disrupt the cryptographic links between the blocks, and the network would reject the modification.[19] Zheng et al. (2017) emphasize that this immutability provides a reliable and unalterable audit trail, offering users confidence in the accuracy of the stored data.[20]

c. Consensus

Blockchain relies on consensus mechanisms to validate and add new transactions. These mechanisms require the network's nodes to agree on the validity of the data before it is appended to the blockchain. Common methods include Proof of Work

[18]Nakamoto, Satoshi. A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto, 2008), accessed 11 December 2024, https://nakamotoinstitute.org/library/bitcoin/?utm_source=

[19]Kisters, Salomon. "Can a Blockchain Be an Audit Trail?" *OriginStamp*, accessed 11 December 2024, https://originstamp.com/blog/can-a-blockchain-be-an-audit-trail/.

[20]Henry Lab, Blockchain Technology: A New Paradigm for Data Security, International Journal of Web and Grid Services, vol. 14, no. 4, 2018, pages 357-358, accessed 11 December 2024, https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf?utm_source

(PoW) and Proof of Stake (PoS), both of which ensure that only accurate and verified transactions are recorded.[21]

Consensus is vital for maintaining the integrity of the blockchain and preventing fraud or errors. For instance, before a new block is added, all participating nodes must validate the information. If one node attempts to introduce false or corrupted data, the network collectively rejects it.[22]

Building on its foundational features, blockchain relies on several core components that enable its secure, transparent, and efficient functionality. These components serve as the fundamental building blocks of the system, ensuring its integrity and adaptability across various applications. Together, they create a robust framework for recording, verifying, and managing data. The key components of blockchain include the distributed ledger, smart contracts, and public key cryptography, each contributing uniquely to its operation:

a. Distributed Ledger: This is a shared database where all transactions are recorded and distributed across the network. Unlike traditional systems that store data in a central server, the distributed ledger ensures that every authorized participant has access to an identical copy of the record. This transparency builds trust, while the decentralized nature reduces the risk of tampering and single points of failure.
b. Smart Contracts: These are self-executing digital agreements embedded in the blockchain. Smart contracts automatically perform actions, such as transferring assets or enforcing terms, once predefined conditions are met. By removing the need for intermediaries, they streamline operations, reduce costs, and improve reliability in executing agreements.
c. Public Key Cryptography: Security in blockchain is maintained through this cryptographic system, which uses paired public and private keys to encrypt and decrypt data. Public keys are shared openly, while private keys remain confidential, ensuring secure transactions and restricted access to sensitive information[23]. This mechanism is essential for maintaining confidentiality and authenticity in blockchain interactions.

[21]"Proof of Work vs. Proof of Stake," *Binance Academy*, accessed 11 December 2024, https://academy.binance.com/en/articles/proof-of-work-vs-proof-of-stake.
[22]"Consensus Mechanisms in Blockchain: Proof of Work vs. Proof of Stake and Beyond," Rapid Innovation, accessed 11 December 2024, https://www.rapidinnovation.io/post/consensus-mechanisms-in-blockchain-proof-of-work-vs-proof-of-stake-and-beyond.
[23]Data-Flair, "Public Key Cryptography," Data-Flair, accessed 11 December 2024, https://data-flair.training/blogs/public-key-cryptography/.

C.4 Blockchain based e-contract for IP theft solution

Building on blockchain's transformative potential for securing intellectual property (IP), smart contracts emerge as a critical tool in combating IP theft. These self-executing agreements, encoded on the blockchain, are designed to automatically enforce terms and carry out actions once specific conditions are met. By eliminating the need for intermediaries, smart contracts streamline the enforcement of agreements, enabling all parties to verify outcomes instantly and without delays.

Beyond enforcing agreements, smart contracts enhance operational efficiency by automating workflows. For instance, they can initiate subsequent actions, such as transferring royalties or revoking access rights, as soon as predefined criteria are satisfied. This automation not only reduces the likelihood of human error but also ensures consistent and reliable execution of tasks.[24] By integrating smart contracts into IP management, businesses can create a more secure and efficient framework for protecting sensitive assets like patents, trade secrets, and proprietary designs from theft and unauthorized use.

Expanding on the role of blockchain-based smart contracts in addressing IP theft, it is essential to understand how these contracts function and why they are so effective. Smart contracts operate using conditional "if/when...then" statements encoded into the blockchain. When the specified conditions are met and verified by the network, the contract executes the agreed-upon actions automatically. These actions might include transferring funds, issuing notifications, or registering assets.

Once a transaction is completed, the blockchain updates with the details, ensuring the data cannot be altered and remains accessible only to authorized parties. The process begins with participants defining the terms, including transaction rules, exceptions, and dispute resolution mechanisms. While developers traditionally program these contracts, modern tools and templates have simplified their creation, making them more accessible for businesses seeking to streamline operations and secure their intellectual property.

Expanding on how smart contracts operate, their unique capabilities make them particularly effective for addressing the challenges of intellectual property (IP) protection. Blockchain-based smart contracts bring several advantages to safeguarding IP, combining immutability, automation, transparency, and decentralization to create a

[24] Muhammad Sabil Bakti and Priskila Christin Nugrani Watania, "Analisis Yuridis Putusan Hakim Dalam Perkara Pelanggaran Hak Cipta Sistem Investasi Emas Melalui Media Internet (Studi Putusan Mahkamah Agung Nomor 1813 K/Pdt. Sus-HKI/2022)," *Anthology: Inside Intellectual Property Rights* 2, no. 1 (2024): 129–42.

robust framework for managing and protecting sensitive data. These strengths underscore why smart contracts are a powerful tool for securing IP, as outlined below.[25]

a. Immutability Ensures Data Integrity and Ownership Proof.
   A defining feature of blockchain-based smart contracts is immutability, which ensures that once data is recorded, it cannot be altered or deleted. This provides a tamper-proof mechanism for recording ownership, licensing agreements, and access logs, making them secure and indisputable. In legal disputes, the immutable nature of these records offers concrete evidence of IP ownership. While smart contracts cannot be directly modified, their functionality can be updated transparently using mechanisms like proxy contracts. This combination of flexibility and integrity allows businesses to adapt IP management systems without compromising data reliability.

b. Automated Enforcement of Access Policies.
   Smart contracts also excel at automating access control. They define and enforce IP usage rules based on predefined conditions, such as user roles, timelines, or project-specific agreements. For example, access to a proprietary design may be granted only to authorized suppliers and automatically revoked when the project concludes. This automation minimizes human error, reduces the risk of unauthorized access, and ensures sensitive IP is consistently protected. The tamper-proof record of access transactions further enhances accountability and trust in IP management.

c. Transparency Enhances Accountability and Deters Insider Threats.
   Transparency is another crucial advantage of smart contracts. Each action or transaction is immutably recorded on the blockchain, providing a verifiable log that all stakeholders can review. This visibility promotes accountability and deters insider threats, as malicious actions are easily traceable. For instance, if an employee attempts to misuse trade secrets, the blockchain's transparent records can expose the breach and aid in swift resolution. The automation of rules and the elimination of intermediaries also streamline processes, reducing vulnerabilities and the risk of manipulation.

d. Decentralization Reduces Risks of Centralized Breaches.
   By distributing data across multiple nodes, decentralization eliminates the risks associated with centralized storage systems. In traditional databases, sensitive IP data is often stored in a single location, making it a prime target for cyberattacks or insider misuse. Blockchain-based smart contracts mitigate this risk by ensuring data

[25]Rapal, Harshdeep. "Smart Contracts in Intellectual Property Management and Protection," LegitT.A.I, accessed 11 December 2024, https://legittai.com/blog/smart-contracts-in-intellectual-property-management-and-protection.

redundancy and encryption across the network. Even if one node is compromised, the system remains secure, as no single entity has full control over the data. This decentralized approach not only strengthens security but also reduces the administrative burden of managing sensitive IP assets.

Building on the advantages of blockchain-based smart contracts for intellectual property (IP) protection, their practical application becomes especially critical in the automotive industry, where counterfeiting and unauthorized replication pose persistent threats. Counterfeiting and unauthorized duplication of designs remain significant challenges, exacerbated by insider threats and state-sponsored campaigns such as China's Thousand Talents Plan, which has been linked to systematic theft of proprietary technologies. The 2022 Ponemon Institute Cost of Insider Threats Global Report found that 67% of organizations experienced between 21 and more than 40 insider-related incidents annually, up from 60% in 2020. The average cost per incident rose to $15.38 million, up from $11.45 million in 2020. Credential theft was particularly costly, with incidents increasing from $2.79 million in 2020 to $4.6 million in 2022. The time to contain an incident grew from 77 to 85 days, with incidents taking over 90 days to contain costing $17.19 million annually. These trends highlight the need for stronger solutions to protect intellectual property and sensitive assets.[26]

Blockchain-based e-contracts offer a practical and innovative response to these challenges by providing a secure, transparent, and automated framework for managing IP. These contracts enforce critical IP-related terms, including licensing agreements, access permissions, and usage conditions, without relying on intermediaries. For example, in supply chain management, blockchain e-contracts can authenticate components and restrict access to sensitive designs or trade secrets, ensuring that only verified suppliers handle proprietary data. This not only prevents counterfeit parts from infiltrating the market but also protects brand integrity and fosters consumer trust.

Real-world applications illustrate the effectiveness of this technology. Mercedes-Benz has implemented blockchain solutions for patented vehicle-to-vehicle (V2V) communication and real-time software update verification. These measures ensure that Mercedes retains exclusive rights to its innovations while preventing unauthorized replication. By integrating blockchain into its operations, Mercedes demonstrates how e-contracts can secure proprietary technologies and position companies as leaders in technological adoption.[27]

[26]Proofpoint, "The Cost of Insider Threats," Proofpoint, accessed 11 December 2024, https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats.
[27]Tran, Bao. "Mercedes Blockchain in Automotive Patents: Legal and Strategic Insights," PatentPC, accessed 11 December 2024, https://patentpc.com/blog/mercedes-blockchain-in-automotive-patents-legal-and-strategic-insights.

Scaling the adoption of blockchain-based e-contracts across the automotive sector would allow manufacturers to address similar vulnerabilities. Integrating blockchain solutions with cybersecurity standards like ISO/SAE 21434 can establish a comprehensive framework for risk management, particularly as the industry moves toward autonomous vehicles and greater connectivity.[28] By providing a secure and forward-looking mechanism for protecting IP, blockchain-based e-contracts can foster innovation, reduce vulnerabilities, and ensure long-term competitiveness in the global automotive market.

C.5 Legal and Ethical Framework

Technological advancements have made counterfeit operations more sophisticated, complicating cross-border IP enforcement. Counterfeiters exploit e-commerce platforms using deceptive tactics like fake reviews and hidden listings to mislead consumers.[29] When shut down, they quickly reappear with new identities, taking advantage of limited platform accountability.

Tools like 3D printing and scanning enable counterfeiters to cheaply replicate products with substandard materials, risking consumer safety. Courier services such as DHL, FedEx, and international postal systems facilitate the shipment of counterfeit goods, with Customs and Border Protection (CBP) able to inspect only a fraction of daily imports. To combat this, stricter regulations, enhanced shipping data requirements, and better oversight of counterfeit production technologies are essential to protect consumers and IP rights.[30]

a. Enforcement in United States.

The United States faces significant challenges in enforcing intellectual property (IP) rights across borders, with trade secret theft being a critical issue. Trade secrets, including manufacturing techniques, business strategies, and proprietary technologies, are essential for maintaining competitive advantages, especially for small businesses relying on confidentiality over patents. However, these assets are increasingly targeted through cyberattacks, insider threats, and regulatory misuse, threatening economic stability and national security. Countries like China, Russia,

[28]"Automotive Cybersecurity and Regulatory Standards," QA Consultants, accessed 11 December 2024, https://qaconsultants.com/automotive-cybersecurity-and-regulatory-standards/.
[29] Fajar Sugianto, Stevinell Mildova, and Felicia Christina Simeon, "Increasing Economic Performance Through the Rule of Law in Indonesia: Law and Economics Perspective" 140, no. Icleh (2020): 92–99, https://doi.org/10.2991/aebmr.k.200513.019.
[30]Department of Homeland Security (DHS), "2020 Counterfeit and Pirated Goods Report" (Research Report, DHS, Washington, D.C., 2020), pages 21-26, accessed 11 December 2024, https://www.dhs.gov/publication/2020-counterfeit-and-pirated-goods-report.

and India are frequently criticized for weak legal protections and enforcement mechanisms, making effective remedies difficult to secure.[31]

To counter these threats, the U.S. has implemented legal measures like the United States-Mexico-Canada Agreement (USMCA) and the U.S.-China Economic and Trade Agreement (Phase One), which strengthen penalties for trade secret theft, improve litigation safeguards, and address enforcement gaps. Domestically, the Defend Trade Secrets Act (DTSA) provides a federal mechanism for addressing trade secret misappropriation, offering remedies such as damages, injunctions, and civil seizure.[32]

Despite these advancements, challenges remain. Weak penalties, mandatory technology transfers in some regions, and insufficient international cooperation hinder enforcement. The U.S. continues to push for stronger global partnerships and regulatory standards to safeguard innovation and promote fair competition.

b. Enforcement in the European Union.

The European Union (EU) encounters significant challenges in enforcing intellectual property rights (IPRs), particularly concerning trade secrets and patents. While the IPR Enforcement Directive (IPRED) provides a harmonized legal framework, inconsistencies in its implementation across member states weaken its effectiveness. Article 11 of IPRED, which facilitates injunctions against infringers and intermediaries, is a key tool for addressing violations in civil cases. However, the lack of harmonized criminal enforcement measures remains a major obstacle, as political disagreements led to the abandonment of earlier proposals for alignment.

Additionally, the absence of a unified approach to patents and trade secrets further complicates enforcement efforts. Variations in how member states interpret and apply EU directives contribute to fragmentation, making it harder to secure consistent cross-border protection for these critical intellectual assets. These gaps in enforcement highlight the pressing need for greater harmonization and stronger mechanisms to safeguard trade secrets and patents across the EU.[33]

Similar to the United States, the European Union faces significant challenges in penalizing cross-border intellectual property (IP) infringements, particularly due to

[31]Brittain, Blake. "U.S. Justice Department Examining Foreign Funding of Patent Lawsuits," Reuters, 6 December 2024, https://www.reuters.com/legal/government/us-justice-department-examining-foreign-funding-patent-lawsuits-2024-12-06/.

[32]"2024 Special 301 Report" (Research Report, USTR, Washington, D.C., 2024), page 23-24, accessed 11 December 2024, https://ustr.gov/sites/default/files/2024%20Special%20301%20Report.pdf.

[33]"The Enforcement of Intellectual Property Rights: Measures and Perspectives" (Research Report, European Parliament, 2021), page 26, accessed 11 December 2024, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/703387/IPOL_STU(2021)703387_EN.pdf.

the difficulty of identifying specific suppliers. While customs authorities can trace counterfeit goods to source countries, such as China, Hong Kong, and Türkiye—accounting for over 73% of IPR-infringing goods in 2023—the lack of detailed information about the suppliers or networks behind these shipments complicates enforcement.[34]

Patent enforcement in Europe is primarily regulated under the European Patent Convention (EPC), which exists independently of the EU's legal framework. This separation has resulted in a fragmented system where patent litigation is managed on a national level, with no harmonized substantive patent law across member states. This lack of uniformity has encouraged forum shopping, where parties select jurisdictions that are more likely to rule in their favor.

To address these challenges, the EU introduced the Unitary Patent Package (UPP), including the creation of the Unitary Patent Court (UPC). The UPC will centralize patent litigation for participating member states, providing a streamlined process for enforcing both unitary and European patents. Additionally, revisions to the Brussels I Regulation will ensure that UPC decisions are recognized and enforceable across borders, significantly enhancing the efficiency of cross-border patent enforcement.[35]

C.6 Financial and Data Security Implications

Building on the use of blockchain-based e-contracts to combat IP theft, their benefits extend beyond intellectual property protection to enhancing financial transparency and securing sensitive data. By automating processes and providing tamper-proof recordkeeping, blockchain e-contracts offer a practical and effective solution for managing complex financial operations and ensuring data integrity in today's digital landscape.

In financial management, e-contracts streamline the handling of royalties, licensing fees, and payments through automation. Smart contracts execute transactions based on pre-agreed conditions, such as automatically distributing royalties when usage targets are met or adjusting licensing terms dynamically as

[34]"Counterfeit Clampdown: EU Seizes Record 152 Million Fake Items Worth 3.4 Billion EUR in 2023," *EUIPO News*, accessed 11 December 2024, https://www.euipo.europa.eu/en/news/observatory/counterfeit-clampdown:-eu-seizes-record-152-million-fake-items-worth-3-4-billion-eur-in-2023.

[35]"The Enforcement of Intellectual Property Rights: Measures and Perspectives" (Research Report, European Parliament, 2021), page 11, accessed 11 December 2024, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/703387/IPOL_STU(2021)703387_EN.pdf.

circumstances change.[36] By removing the need for intermediaries and minimizing manual input, this automation reduces errors, speeds up transactions, and cuts operational costs. Every financial transaction is recorded immutably on the blockchain, creating a transparent and verifiable ledger that fosters accountability and builds trust among stakeholders.[37]

When it comes to data security, blockchain-based e-contracts provide robust safeguards against unauthorized access and tampering. Sensitive information stored on the blockchain is encrypted, ensuring that only those with appropriate decryption keys can access it. Smart contracts also include role-based permissions, granting access only under predefined conditions, such as limiting data usage to specific projects or approved personnel.[38] Every interaction is immutably logged, complete with timestamps, ensuring the integrity of records and creating a clear audit trail. This transparency discourages fraudulent activity and strengthens defenses against insider threats.

Additionally, e-contracts align seamlessly with regulatory frameworks like GDPR. By automating consent management, businesses can link customer data usage to explicit consent, revoke access automatically when consent is withdrawn, and securely store data references rather than raw information. This ensures compliance with data minimization and privacy principles while allowing for the "right to be forgotten" by rendering encrypted data inaccessible when keys are discarded. These features reduce regulatory risks and enhance trust by safeguarding customer data and ensuring accountability in data usage.[39]

The transparency of blockchain adds an extra layer of accountability, particularly in deterring insider threats. With every action immutably recorded, employees are less likely to misuse or tamper with sensitive data, as their activities are permanently visible and auditable.[40] This combination of transparency,

[36]Delfino, Justin. "Blockchain Smart Contracts," IP Service World, accessed 11 December 2024, https://www.ipserviceworld.com/blog/blockchain-smart-contracts/.
[37]Alsdorf, Gina, and Jason Berkun. "Is Blockchain the Next Big Thing for Insurance Companies?" Reuters, 9 October 2024, https://www.reuters.com/legal/legalindustry/is-blockchain-next-big-thing-insurance-companies-2024-10-09/.
[38] Fajar Sugianto Sugianto, "Efisiensi Ekonomi Sebagai Remedy Hukum," *Refleksi Hukum: Jurnal Ilmu Hukum* 8, no. 1 (2014): 61–72, https://doi.org/10.24246/jrh.2014.v8.i1.p61-72.
[39]Bayle, Aurélie, Mirko Koscina, David Manset, and Octavio Perez-Kempner. "When Blockchain Meets the Right to be Forgotten," MyHealthMyData, 2019, page 4, accessed 11 December 2024, https://www.myhealthmydata.eu/wp-content/uploads/2019/10/When_Blockchain_Meets_the_Right_to_be_Forgotten.pdf.
[40] Shintaro Tokuyama Fajar Sugianto, "The Extended Nature of Trading Norms Between Cryptocurrency and Crypto-Asset: Evidence from Indonesia and Japan," *Lex Scientia Law Review* 8, no. 1 (2024): 193–221, https://doi.org/https://doi.org/10.15294/lslr.v8i1.14063.

automation, and security positions blockchain-based e-contracts as a valuable tool for managing financial processes, safeguarding sensitive data, and maintaining trust in a digital-first world.

D. Conclusion

To effectively protect intellectual property (IP) in the automotive industry, it's crucial to embrace the potential of blockchain technology. For this to happen, industry leaders, governments, and regulatory bodies need to actively support and encourage the widespread use of blockchain-based solutions for IP management. The decentralized, transparent, and tamper-proof nature of blockchain offers a powerful way to safeguard important automotive innovations, such as patents, designs, and trade secrets. Blockchain can simplify and streamline key processes like licensing agreements, royalty payments, and compliance monitoring through smart contracts. This removes the need for intermediaries, reduces costs, and makes managing IP much more efficient. Additionally, blockchain provides a clear and secure ledger that allows for better tracking and verification of IP ownership, which makes it much easier to prove ownership if any disputes arise.

Beyond the technical benefits, it's essential that blockchain is integrated into existing legal systems to make sure it works alongside traditional IP protection methods. Regulatory bodies need to ensure that blockchain solutions align with current regulations, such as GDPR, and address concerns like data storage and privacy, particularly regarding the "right to be forgotten." Governments can also help by offering incentives, like tax breaks or grants, to encourage automotive companies to adopt blockchain technology. By providing these financial incentives, both large corporations and small innovators will have the support they need to implement blockchain systems that secure their IP.

In addition, businesses across the automotive sector need to be educated about how blockchain can enhance their IP protection efforts. Industry-wide education campaigns can demonstrate how blockchain addresses challenges like counterfeiting and trade secret theft, which many companies face. By offering training and resources, companies will better understand how blockchain can streamline their IP management, reduce risks, and improve trust between them and their partners.

Lastly, since the automotive industry operates on a global scale, international cooperation is key. Countries and international organizations must collaborate to create global standards for using blockchain in IP protection. This would ensure that the same high standards are applied everywhere, making it easier for automotive companies to

protect their innovations around the world. By promoting the adoption of blockchain, aligning it with legal frameworks, offering incentives, educating businesses, and fostering international collaboration, the automotive industry can use blockchain to secure its intellectual property, encourage innovation, and maintain a competitive edge in the global market.

REFERENCES

Journal Article

Henry Lab, Blockchain Technology: A New Paradigm for Data Security, International Journal of Web and Grid Services, vol. 14, no. 4, 2018, pages 357-358. Accessed 11 December 2024. https://www.henrylab.net/wp-content/uploads/2017/10/blockchain.pdf?utm_source

Research Report

"Background Note: Illicit Trade Forum." Research Report, UNCTAD, Geneva, 2020. UNCTAD Repository. https://unctad.org/system/files/non-official-document/DITC2020_BackgroundNote_UNCTAD%20Illicit%20Trade%20Forum_en.pdf.

Bakti, Muhammad Sabil, and Priskila Christin Nugrani Watania. "Analisis Yuridis Putusan Hakim Dalam Perkara Pelanggaran Hak Cipta Sistem Investasi Emas Melalui Media Internet (Studi Putusan Mahkamah Agung Nomor 1813 K/Pdt. Sus-HKI/2022)." *Anthology: Inside Intellectual Property Rights* 2, no. 1 (2024): 129–42. https://ojs.uph.edu/index.php/Anthology/article/view/8254

Bayle, Aurélie, Mirko Koscina, David Manset, and Octavio Perez-Kempner. "When Blockchain Meets the Right to be Forgotten." MyHealthMyData, 2019. Accessed 11 December 2024. https://www.myhealthmydata.eu/wp-content/uploads/2019/10/When_Blockchain_Meets_the_Right_to_be_Forgotten.pdf.

De Bolle, Catherine, and Christian Archambeau. "Intellectual Property Crime Threat Assessment 2022." Research Report, Europol, The Hague, 2022. Europol Repository. https://www.europol.europa.eu/cms/sites/default/files/documents/Report.%20Intellectual%20property%20crime%20threat%20assessment%202022_2.pdf.

Fajar Sugianto, Shintaro Tokuyama. "The Extended Nature of Trading Norms Between Cryptocurrency and Crypto-Asset: Evidence from Indonesia and Japan." *Lex Scientia Law Review* 8, no. 1 (2024): 193–221. https://doi.org/https://doi.org/10.15294/lslr.v8i1.14063.

Joint Economic Committee. "Intellectual Property Theft and the Economy." Research Report, United States Congress, Washington, D.C., 2012. JEC Repository. https://www.jec.senate.gov/public/_cache/files/aa0183d4-8ad9-488f-9e38-7150a3bb62be/intellectual-property-theft-and-the-economy.pdf.

Nugroho, Akbar, and Davi Pandi. "The Issue of No Benchmark in Determining the Economic Value of Intellectual Property" *Anthology: Inside Intellectual Property Rights* 2, no. 1 (2024): 284–99. https://ojs.uph.edu/index.php/Anthology/article/view/8514

Sugianto, Fajar, Astrid Athina Indradewi, and Yohanie Maretta. "Book Pirates and Copycats : Infringement That Speaks For Itself." *Anthology: Inside Intellectual Property Rights* 2, no. 1 (2024): 259–69. https://ojs.uph.edu/index.php/Anthology/article/view/8512

Sugianto, Fajar, Stevinell Mildova, and Felicia Christina Simeon. "Increasing Economic Performance Through the Rule of Law in Indonesia: Law and Economics Perspective" Proceedings of the International Conference on Law, Economics and Health (ICLEH 2020): 92–99. https://doi.org/10.2991/aebmr.k.200513.019.

Sugianto, Fajar Sugianto. "Efisiensi Ekonomi Sebagai Remedy Hukum." *Refleksi Hukum: Jurnal Ilmu Hukum* 8, no. 1 (2014): 61–72. https://doi.org/10.24246/jrh.2014.v8.i1.p61-72.

"Fiscal Year 2023 Annual Report to Congress." Research Report, Executive Office of the President, United States, 2024. IPEC Repository. https://www.whitehouse.gov/wp-content/uploads/2024/04/IPEC-FY-23-Annual-Report_Final.pdf.

"2024 Special 301 Report." Research Report, USTR, Washington, D.C., 2024. USTR Repository. https://ustr.gov/sites/default/files/2024%20Special%20301%20Report.pdf.

Court Decision

Bayle, Aurélie, Mirko Koscina, David Manset, and Octavio Perez-Kempner. "When Blockchain Meets the Right to be Forgotten." MyHealthMyData, 2019. Accessed 11 December 2024. https://www.myhealthmydata.eu/wp-content/uploads/2019/10/When_Blockchain_Meets_the_Right_to_be_Forgotten.pdf.

Internet

Alsdorf, Gina, and Jason Berkun. "Is Blockchain the Next Big Thing for Insurance Companies?" *Reuters*, 9 October 2024.

https://www.reuters.com/legal/legalindustry/is-blockchain-next-big-thing-insurance-companies-2024-10-09/.

"Automotive Cybersecurity and Regulatory Standards." *QA Consultants*. Accessed 11 December 2024. https://qaconsultants.com/automotive-cybersecurity-and-regulatory-standards/.

Brittain, Blake. "U.S. Justice Department Examining Foreign Funding of Patent Lawsuits." Reuters, 6 December 2024. https://www.reuters.com/legal/government/us-justice-department-examining-foreign-funding-patent-lawsuits-2024-12-06/.

Cyberhaven. "Top IP Theft Statistics." Accessed 11 December 2024. https://www.cyberhaven.com/guides/top-ip-theft-statistics.

Delfino, Justin. "Blockchain Smart Contracts." *IP Service World*. Accessed 11 December 2024. https://www.ipserviceworld.com/blog/blockchain-smart-contracts/.

European Union Intellectual Property Office (EUIPO). "Counterfeit Clampdown: EU Seizes Record 152 Million Fake Items Worth 3.4 Billion EUR in 2023." *EUIPO News*. Accessed 11 December 2024. https://www.euipo.europa.eu/en/news/observatory/counterfeit-clampdown:-eu-seizes-record-152-million-fake-items-worth-3-4-billion-eur-in-2023.

Hayes, Adam. "Blockchain Facts: What Is It, How It Works, and How It Can Be Used." *Investopedia*. Accessed 11 December 2024. https://www.investopedia.com/terms/b/blockchain.asp.

Kisters, Salomon. "Can a Blockchain Be an Audit Trail?" *OriginStamp*. Accessed 11 December 2024. https://originstamp.com/blog/can-a-blockchain-be-an-audit-trail/.

Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* (Satoshi Nakamoto, 2008). Accessed 11 December 2024. https://nakamotoinstitute.org/library/bitcoin/?utm_source=.

"Public Key Cryptography." *Data-Flair*. Accessed 11 December 2024. https://data-flair.training/blogs/public-key-cryptography/.

Rapal, Harshdeep. "Smart Contracts in Intellectual Property Management and Protection." *LegitT.A.I.* Accessed 11 December 2024. https://legittai.com/blog/smart-contracts-in-intellectual-property-management-and-protection.

"The Cost of Insider Threats." *Proofpoint*. Accessed 11 December 2024. https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats.

Tran, Bao. "Mercedes Blockchain in Automotive Patents: Legal and Strategic Insights." *PatentPC*. Accessed 11 December 2024. https://patentpc.com/blog/mercedes-blockchain-in-automotive-patents-legal-and-strategic-insights.

"Consensus Mechanisms in Blockchain: Proof of Work vs. Proof of Stake and Beyond." *Rapid Innovation*. Accessed 11 December 2024. https://www.rapidinnovation.io/post/consensus-mechanisms-in-blockchain-proof-of-work-vs-proof-of-stake-and-beyond.

"What is Intellectual Property?" Accessed 11 December 2024. https://www.wipo.int/about-ip/en/.