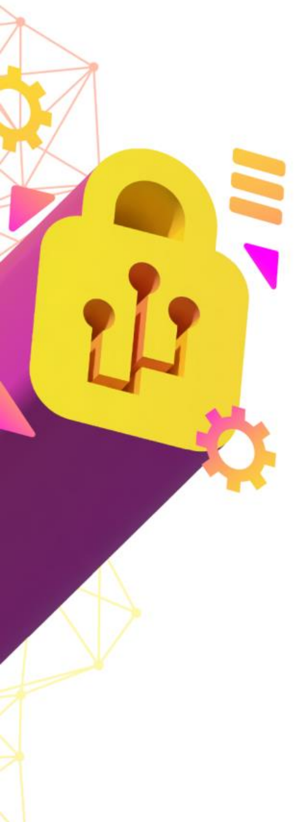
NGI TRUST CHAIN

STATE OF THE ART AND TECHNOLOGY INVENTORY



Funded by the European Union

TrustChain Project. Funded by the European Union under GA No 101093274. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

Grant Agreement No.: 957338
Call: H2020-ICT-2020-1
Topic: ICT-54-2020
Type of action: RIA

D3.2 STATE OF THE ART AND TECHNOLOGY INVENTORY

REPORT-2

Work package	WP 3
Task	3.2
Due date	28/02/2024 (M13)
Submission date	13/11/2024
Deliverable lead	ALA
Version	1.3
Authors	Alexander Herranz (ALA) Pablo Vela (ALA) Pedro Gallego (ALA)
Reviewers	Petar Kochovski(UL) Michal Krol (ICS)
Abstract	Analysis of the current state of the art, as input for the open call specifications and mentoring support.
Keywords	

Funded by the European Union

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributors
0.1	06/11/23	Initial deliverable structure	Alexander Herranz (ALA)
0.2	21/12/23	Structure rediscussed	Pablo Vela (ALA)
0.3	03/01/24	Partner contribution	Pablo Vela (ALA)
0.4	24/01/24	Partner contribution	Veniamin Boiarkin (ICS)
0.5	15/02/24	Partner contribution	Thanasis Papaioannou (NKUA)
0.6	20/02/24	Partner contribution	Vlado Stankovski (UL)
0.7	22/02/24	New template	Pablo Vela (ALA)
0.8	27/02/24	Final draft	Pablo Vela (ALA)
0.9	27/02/24	Internal Review	Raj Rajarajan (ICS)
1.0	05/03/24	Modifications after internal review	Pablo Vela (ALA)
1.1	11/04/24	Abbreviations added Final review	Pablo Vela (ALA)
1.2	15/10/24	Request for revision	Pablo Vela (ALA)
1.3	11/11/24	Final Review	Pedro Gallego (ALA)

Funded by the European Union

DISCLAIMER

The information, documentation and figures available in this document are written by the TRUSTCHAIN project's consortium under EC grant agreement 101093274 and do not necessarily reflect the views of the European Commission. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. Moreover, it is clearly stated that the TRUSTCHAIN Consortium reserves the right to update, amend or modify any part, section or detail of the document at any point in time without prior information.

The TRUSTCHAIN project is funded by the European Union's Horizon Europe Research and Innovation programme under grant agreement no. 101093274.

COPYRIGHT NOTICE

Funded by the European Union

THE TRUSTCHAIN CONSORTIUM IS THE FOLLOWING:

Participant number	Participant organisation name	Short name	Country
1	EUROPEAN DYNAMICS LUXEMBOURG SA	ED	LU
2	F6S NETWORK IRELAND LIMITED	F6S	IE
3	UNIVERZA V LJUBLJANI	UL	SI
4	ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS - RESEARCH CENTER	AUEB	EL
5	FUNDACION CIBERVOLUNTARIOS	CIB	ES
6	CONSORCIO RED ALASTRIA	ALA	ES
7	TIME.LEX	TLX	BE
8	CITY UNIVERSITY OF LONDON	ICS	UK
9	NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS	NKUA	EL

Funded by the European Union

EXECUTIVE SUMMARY

This report provides a detailed state-of-the-art ac review focusing on different aspects of data governance and user privacy, highlighting the use of blockchain as an innovative technology. The report covers a wide range of sectors, including healthcare, finance, retail, education, entertainment and social media, energy, sustainability, supply chain management, public sector and government, and automotive and transportation. It also reviews several existing business use cases, creating a solid foundation of real-world use cases that apply different innovative technologies.

More in depth it highlights how the implementation of blockchain is reshaping data governance strategies, offering greater security and transparency, while addressing the challenges and limitations inherent in its application. The report is a detailed analysis that aims to lay a solid foundation for future research and developments in the sector, emphasizing the importance of technological innovation in protecting user privacy and efficiency in data governance as the main fronts of concern for the European Commission.

In addition, the report highlights how emerging technologies, primarily federated learning and privacy-enhancing technologies (PETs), are driving a shift towards more privacy-centric data management. It delves into the integration of blockchain technology with IoT and AI, demonstrating its potential to revolutionize traceability and real-time data management in various industries. It also discusses the critical role of regulation, such as GDPR and HIPAA, in shaping data governance practices and highlights the importance of interoperability and standards in the transfer of data between countries.

Funded by the European Union

TABLE OF CONTENTS

Funded by the European Union

TABLE OF CONTENTS

Funded by the European Union

ABBREVIATIONS

AI	Artificial Intelligence
APEC	Asia-Pacific Economic Cooperation
API	Application Programming Interface
AR	Augmented Reality
AWS	Amazon Web Services
B2B	Business to Business
BCR	Binding Corporate. Rules
C2B	Consumer to Business
CBPR	Cross-Border Privacy Rules
CCPA	California Consumer Privacy Act
DApps	Decentralized Applications
DAO	Decentralized Autonomous Organization
DeFi	Decentralized Finance
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
EU	European Union
ETH	Ethereum
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
HIPAA	Health Insurance Portability and Accountability Act
IOT	Internet of Things
IP	Internet Protocol
IP	Intellectual Property
JSTOR	Journal Storage

NGI	Next Generation Internet
OC	Open Call
PET	Privacy Enhancing Technologies
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
SaaS	Software as a Service
SMPC	Secure Multiparty Computation
SNARK	Succinct Non-interactive Arguments of knowledge
STARK	Scalable Transparent Arguments of knowledge
TCP	Transmission Control Protocol
US	United States
VR	Virtual Reality
XMR	Monero
ZKP	Zero Knowlege Proof

....

1. INTRODUCTION

In this era of digital transformation, efficient and secure data management has become a key pillar for both organizations and individual users. This state-of-the-art review focuses on analyzing data governance frameworks, with a particular emphasis on the innovative use of blockchain technology. Blockchain, known for its immutability and decentralization, offers a revolutionary perspective in data protection and management. By examining practical cases in critical sectors like healthcare, finance, retail, education, entertainment and social media, energy and sustainability, supply chain management, public sector and government, automotive and transportation, we aim to understand how blockchain implementation is reshaping data governance strategies. This report highlights the advantages of blockchain, such as enhanced security and transparency, while also addressing the challenges and limitations inherent in its application. It provides a comprehensive view of the potential and obstacles faced in integrating this technology into complex data management systems. This thorough analysis aims to lay a solid foundation for future research and development in the field, emphasizing the importance of technological innovation in protecting user privacy and efficiency in data governance.

2. METHODOLOGY

This research adopts a mixed-methodological approach, combining qualitative and quantitative analysis. It begins with a comprehensive literature review, selecting publications from academic databases like IEEE Xplore, PubMed, Zenodo, and JSTOR, using keywords such as 'blockchain', 'data governance', and 'user privacy'. To ensure a current perspective, the search is focused on publications from the last five years. Then, a thematic analysis is conducted to identify trends, challenges, and innovative solutions. Quantitative data from case studies and relevant statistics complement the qualitative analysis, providing a comprehensive view of blockchain implementation in data governance.

A long search has also been carried out for non-academic articles that provide different points of view, which, although not scientific papers, add great value to the context of this document.

3. USE-CASE DRIVEN USER PRIVACY AND DATA GOVERNANCE: REAL PROBLEMS AND EXISTING APPLICATIONS

In the current information era, user data privacy and governance have become critical issues, particularly as innovative technologies change how we interact with data. Blockchain implementation offers significant potential for improving privacy and governance through a decentralized, secure data management framework. Additionally, data handling ethics have become a focal point as tech companies balance business practices with social responsibility and regulation. This context explores how current technological developments, like blockchain, and ethical considerations in data governance (Data Galaxy, 2023), can address real issues and enhance existing privacy and data management applications. These advancements, alongside evolving regulatory frameworks, present an opportunity to develop more robust, user-centric systems that not only protect individual privacy but also promote ethical and responsible data management (Dimelgani, 2023; SG Analytics, 2023).

It's essential to explore specific use cases illustrating how technologies like blockchain and ethical data management practices are applied across various contexts. In healthcare, protecting sensitive medical records is crucial; in finance, transaction security and transparency are critical. Retail requires balancing customer data management and personalization with privacy. Education faces unique challenges in protecting student and faculty data. Entertainment and social media need careful handling of personal data and user preferences. In energy and sustainability, transparency in data management is key for environmental initiatives. Supply chain management benefits from blockchain's traceability and efficiency (Monrat, Schelén & Andersson, 2019). For public sector and government, trust and security in citizen data management are vital. Lastly, in the automotive and transportation industry, secure and efficient data integration is essential for innovation and safety. These use cases underscore the need for privacy and data governance solutions that are both robust and tailored to each sector's specific needs (Frenté, 2023).

3.1. HEALTHCARE

In the healthcare sector (Gaine, 2023), user privacy and data governance are of paramount importance due to the sensitivity of medical information. A notable challenge faced is the secure sharing of medical records. Patients often need their medical histories and records accessible by various healthcare providers, which raises concerns about data security. Robust data governance mechanisms are critical to ensuring that sensitive medical information remains confidential and is accessible only to authorized personnel, enabling secure and seamless data sharing while

Funded by the European Union

safeguarding patient privacy. Similarly, ensuring patient data privacy is a significant concern. With the vast amount of personal and health data generated and stored in electronic health records, it's crucial to have stringent data governance practices in place. These practices help protect patient data, control access, and ensure compliance with stringent data protection regulations. By establishing data governance frameworks that address these concerns, the healthcare sector can continue to provide high-quality care while upholding patient confidentiality (Kerasidou & Kerasidou, 2023).

- Secure sharing of medical records: In the healthcare sector, maintaining the security and privacy of patients' medical records is paramount. Robust data governance ensures that sensitive medical information remains confidential and accessible only to authorized personnel.

- Patient data privacy: Protecting patient data is a significant challenge in the healthcare industry. Comprehensive data governance mechanisms are essential to safeguard the personal information of individuals and ensure compliance with privacy regulations.

- Clinical Trials and Research Data Management: used to secure and streamline the management of clinical trial data, ensuring integrity and transparency in research.

- Pharmaceutical Supply Chain Integrity: solutions are applied to track the production and distribution of pharmaceutical products, helping to combat counterfeit drugs.

- Remote Patient Monitoring: blockchain facilitates secure and reliable data sharing in remote patient monitoring systems, enhancing patient care and data privacy.

In healthcare, data governance involves managing policies (Krishnan, 2023), procedures, and standards to ensure data's accuracy, consistency, and security. Its key objectives include patient safety, improved clinical outcomes, and compliance with industry regulations. Trust is acknowledged as crucial for the acceptability of data sharing and the adoption of new health technologies such as AI, though there's reported distrust in this domain. Data privacy regulations in healthcare are evolving, and it is important to understand regulations like HIPAA, GDPR, and CCPA. See more on these regulations in Section 4 (Alder, 2022).

The paper "A Privacy-Preserved and User Self-Governance Blockchain-Based Framework to Combat COVID-19 Depression in Social Media" (Zirui & Bin, 2023) introduces a blockchain-based framework to manage COVID-19 related depression on social media (Gossett, 2020). It proposes a solution using the DPoS (Delegated Proof of

Stake) consensus protocol to share depression-related information on social media platforms while maintaining user information privacy and autonomy. The approach focuses on identifying and assisting users with depression through blockchain, emphasizing the importance of privacy and self-management of data in the context of a pandemic.

MediLedger

MediLedger is a project that employs blockchain technology to enhance the pharmaceutical supply chain. It focuses on ensuring drug authenticity and reducing counterfeit risks. MediLedger offers a secure, decentralized platform for supply chain participants like manufacturers, distributors, and pharmacies to track and verify drug origins and journeys. This system not only improves patient safety but also aids pharmaceutical companies in regulatory compliance and operational efficiency enhancement (MediLedger, n.d.).

Patientory

Patientory is a blockchain-based electronic health records management platform. It focuses on providing patients with secure and easy control of their medical information. The platform utilizes blockchain to ensure data privacy and security, allowing users to store, manage, and securely share their health information. Patientory also aids in connecting patients with healthcare providers, facilitating more effective communication and better care coordination (Patientory, n.d.).

BurstIQ

BurstIQ is a platform that leverages blockchain technology for secure health data management. It allows users to control and share their medical information securely. BurstIQ's blockchain solution addresses data security and interoperability challenges in healthcare, enabling seamless data exchange while maintaining privacy and compliance with regulations. The platform supports a range of health data services, from personal health management to clinical research, emphasizing user empowerment in health data control (BurstIQ, n.d.).

Guardtime Health

Guardtime Health specializes in securing health data using blockchain technology. It focuses on enhancing interoperability among various healthcare systems while ensuring data integrity and security. Guardtime Health's blockchain solution is designed to facilitate secure and efficient exchange of medical information, adhering to privacy and regulatory standards. This approach aims to streamline healthcare processes, improve patient outcomes, and foster trust in digital health data management (Guardtime Health, n.d.).

Embleema

Embleema is a virtual trial and regulatory analytics platform designed to fast-track drug development. Users are recruited to digitally consent to secure, untampered medical data collection, which is then stored on Embleema's blockchain and analyzed (Embleema, n.d.).

Embleema's platform allows patients to assist in speeding up treatment availability and improving safety, all through the company's Virtual Studies Suite.

3.2. FINANCE

The finance sector relies heavily on user data and transactions, making data governance and user privacy essential components. In the context of fraud prevention, finance institutions face constant threats from fraudulent activities, be it credit card fraud, identity theft, or other financial crimes. Effective data governance strategies are vital to implementing robust fraud prevention measures. These measures include transaction monitoring, anomaly detection, and the secure storage of financial data, enabling institutions to safeguard their assets and protect their clients. Additionally, secure transactions are central to the finance industry. From online banking to mobile payments, data governance practices help maintain the integrity and confidentiality of financial data, protecting it from unauthorized access and manipulation. Encryption, access controls, and authentication mechanisms are just a few examples of the tools used to ensure secure financial transactions. By upholding strict data governance standards, the finance sector can enhance customer trust and protect the financial system's integrity.

- Fraud prevention: The finance sector faces constant threats from fraudulent activities. Data governance plays a crucial role in implementing fraud prevention measures, ensuring the security of financial transactions, and safeguarding customer assets.

- Secure transactions: Enabling secure transactions is a fundamental goal in the finance industry. Data governance strategies are employed to maintain the integrity and confidentiality of financial data, protecting it from unauthorized access and manipulation.

- Risk Management: Financial institutions use advanced data analytics for risk assessment, analysing patterns and trends within vast datasets to identify potential risks. This proactive approach aids in minimizing financial losses and maintaining system stability.

Funded by the European Union

- **Personalized Banking Services:** Banks and financial services companies harness customer data to offer personalized banking solutions and financial advice. By analysing spending habits, investment history, and financial goals, they can tailor products and services to individual needs, while adhering to strict privacy and data protection regulations.

In finance, data governance is critical for ensuring regulatory compliance in a heavily regulated environment. Data governance also supports data-driven decision-making by creating reliable, well-managed data pipelines (Singh, 2023). Data quality is essential for accurate decision-making, and data governance can improve this by setting standards for data entry, storage, and usage.

Ripple

Ripple is a blockchain-based platform designed to revolutionize financial transactions, particularly in the realm of international transfers. It offers a faster, more cost-effective alternative to traditional banking systems for cross-border payments. Utilizing its own cryptocurrency, XRP, Ripple enables secure, instant, and low-cost international transactions. This innovation in blockchain technology has positioned Ripple as a key player in financial technology, offering transformative solutions for global finance challenges. Ripple's technology is particularly notable for its scalability, speed, and the reduced transaction costs it offers (Ripple, n.d.).

Circle

Circle is a fintech company that utilizes blockchain technology to facilitate peer-to-peer payments, making financial transactions simpler and more accessible. Their platform allows users to transfer money as easily as sending a text, streamlining the process of sending and receiving payments. Circle's use of blockchain technology enhances security, reduces transaction costs, and improves efficiency, making it an innovative solution in the financial services sector (Circle, n.d.).

Chainalysis

Chainalysis is a blockchain data analytics platform that provides insights to financial institutions and government agencies. It specializes in monitoring and investigating cryptocurrency transactions to enhance transparency and security in the digital finance world. Chainalysis plays a crucial role in detecting and preventing illegal activities in cryptocurrency markets, such as money laundering or fraud. Their tools help ensure compliance with financial regulations, aiding organizations in navigating the complex landscape of digital currencies (Chainalysis, n.d.).

BitPesa

BitPesa is a digital foreign exchange and payment platform focused on the African market. It uses blockchain technology to facilitate business-to-business transactions across borders. BitPesa simplifies the process of sending and receiving payments in different currencies, reducing the cost and increasing the speed of transactions. This service is particularly beneficial for businesses operating in Africa, offering a more efficient and cost-effective solution for handling cross-border payments (BitPesa, n.d.).

Digital Asset Holdings

Digital Asset Holdings is a financial technology firm that develops blockchain-based solutions for various financial services, including transaction settlement and record-keeping. The company focuses on creating tools that streamline and enhance the efficiency of operations within financial markets. Their solutions aim to reduce risk, ensure compliance, and improve the overall functioning of financial systems. Digital Asset Holdings is notable for its efforts to integrate blockchain technology into traditional financial infrastructures.

Veem

Veem is a global payments platform that utilizes blockchain technology to facilitate small business payments worldwide. It simplifies international transactions, making them more transparent and cost-effective. Veem's service is particularly beneficial for small and medium-sized enterprises involved in international trade, offering an efficient alternative to traditional banking methods for cross-border payments (Veem, n.d.).

BlockFi

BlockFi is a financial services company that leverages blockchain technology to offer products like interest-earning accounts and loans using cryptocurrencies. BlockFi's platform provides a secure and efficient way for users to access financial services using digital assets. They focus on bringing traditional banking services to the cryptocurrency market, enhancing the utility and accessibility of cryptocurrencies for a broader range of financial activities (BlockFi, n.d.).

3.3. RETAIL

Retail businesses collect extensive customer data for marketing and operational purposes, making data governance critical in maintaining customer trust and regulatory compliance. The challenge of customer data privacy arises as retailers gather vast amounts of data about their customers, including purchase history, preferences, and personal information. Effective data governance practices are essential to protect customer privacy and comply with data protection regulations like the GDPR in Europe. Retailers must ensure customer data is stored securely, and access is restricted to authorized personnel. Additionally, supply chain transparency is a growing concern in the retail sector. Consumers increasingly demand information about the products they purchase, including details about their origins, sustainability, and quality. Data governance solutions can facilitate the collection and dissemination of accurate and trustworthy data related to product origin, manufacturing processes, and ethical sourcing. By embracing data governance, the retail sector can not only meet consumer demands but also improve supply chain efficiency and transparency.

- Customer Data Privacy: Retail businesses, which collect extensive customer data, need robust data governance to ensure customer privacy, regulatory compliance, and consumer trust. Blockchain can offer secure, decentralized storage and management of customer data, enhancing privacy and control.
- Supply Chain Transparency: Blockchain solutions in retail enable transparent tracking of product origins and quality, addressing concerns about sustainability and ethical sourcing. This transparency fosters consumer trust and brand loyalty.
- Loyalty Programs and Rewards: Blockchain enables secure and transparent loyalty programs, allowing customers to earn and redeem rewards seamlessly. It enhances the integrity of loyalty systems and prevents fraud.

Funded by the European Union

- Anti-Counterfeiting Measures: Retailers can use blockchain to verify the authenticity of products, particularly in luxury goods, reducing the prevalence of counterfeits.
- Real-time Payments and Settlements: Blockchain can revolutionize the payment process in retail, enabling real-time transactions and settlements. This technology reduces transaction times and costs, streamlining the payment process for both retailers and consumers.

Walmart

Walmart's blockchain project focuses on improving food traceability and safety in the retail sector. By utilizing blockchain technology, Walmart can track the origin and journey of food products through its supply chain. This initiative enhances transparency, ensuring that consumers have access to detailed information about the food they purchase, including its source and processing history. The project aims to improve food safety standards, reduce waste, and build consumer trust in Walmart's food products. This application of blockchain in retail showcases how technology can innovate traditional supply chain practices (LF Decentralised Trust, 2018).

De Beers

De Beers' blockchain project, known as Tracr, is focused on enhancing the traceability of diamonds in the retail industry. This initiative ensures that each diamond's journey from the mine to the retail point is tracked, guaranteeing authenticity and ethical sourcing. Tracr provides a transparent record of a diamond's origins, characteristics, and ownership history, helping to prevent the trade of conflict diamonds and reassure consumers about the ethical standards of their purchases. This application of blockchain in retail illustrates how technology can bring transparency and trust to luxury goods (Jenkinson, 2022).

Maersk

Maersk, in collaboration with IBM, has developed a blockchain solution called TradeLens for the maritime shipping industry. This platform enhances the efficiency and transparency of shipping logistics by providing a secure and real-time sharing environment for shipping data among various stakeholders in the supply chain. TradeLens allows participants to track cargo and manage documentation, significantly reducing the time and cost associated with maritime transport. This application of blockchain demonstrates its potential to revolutionize logistics and supply chain management in the retail industry.

Funded by the European Union

Moët Hennessy Louis Vuitton (LVMH)

LVMH's blockchain project, AURA, is designed to verify the authenticity and trace the origin of luxury goods. This initiative combats counterfeiting in the luxury retail sector by providing a secure digital ledger that tracks each product's lifecycle, from production to sale. Consumers can access detailed product history and proof of authenticity, ensuring the legitimacy of their luxury purchases. AURA exemplifies how blockchain can enhance consumer trust and transparency in the high-end retail market (Hypebeast, 2022).

Alibaba

Alibaba's blockchain initiative is focused on protecting intellectual property and ensuring authenticity within its e-commerce platform. The technology is used to track and protect the rights of creators and brands, ensuring that copyrights are respected, and counterfeit goods are minimized. This application of blockchain in retail is crucial for maintaining the integrity of online marketplaces and safeguarding the interests of both sellers and consumers in the digital economy (Zheng, Y. ,2022).

Starbucks

Starbucks' blockchain initiative, in partnership with Microsoft (Microsoft, 2022), is aimed at tracing the journey of coffee beans. This program allows Starbucks to track its coffee products from the farm to the final cup, ensuring transparency and sustainability in its supply chain. Customers can access detailed information about the origin of the coffee beans, the farmers who grow them, and the environmental impact. This application of blockchain technology enhances consumer awareness and supports Starbucks' commitment to ethical sourcing and sustainability in the coffee industry.

JD.com

JD.com's blockchain initiative is focused on enhancing inventory management and quality assurance in their e-commerce operations. By implementing blockchain technology, JD.com can effectively track the origin, authenticity, and quality of products listed on its platform. This initiative ensures a transparent supply chain, providing customers with reliable product information and fostering trust in the e-commerce marketplace. This application of blockchain technology demonstrates its potential to revolutionize retail operations, particularly in online shopping.

3.4. EDUCATION

In the education sector, institutions handle a vast array of sensitive data, from student records to research findings and intellectual property. Secure student records management is a top priority, considering that educational institutions are entrusted with personal and academic information of students. Data governance practices are essential to secure these records, control access, and protect the academic and personal information of students. This includes implementing access controls, data encryption, and regular security audits to ensure that student data remains confidential. Moreover, intellectual property protection is crucial for educational organizations engaged in research and innovation. Universities and research institutions generate valuable intellectual property in the form of research findings, patents, and innovations. Data governance mechanisms help safeguard these intellectual assets by controlling access to research data and ensuring that patents and copyrights are protected. By adhering to comprehensive data governance practices, educational institutions can maintain data security, protect student privacy, and safeguard valuable intellectual property. Here's an overview of how Data Governance practice is being used in the education sector:

- Secure Student Records: Educational institutions use data governance to protect sensitive student records. This includes controlling access and safeguarding academic and personal information.
- Intellectual Property Protection: Ensures the security of research findings and innovations, maintaining the integrity of intellectual property rights within educational organizations.
- Credential Verification: Blockchain technology is employed to authenticate academic credentials, reducing fraud and ensuring the validity of qualifications.
- Online Learning Platforms: Data governance is applied to protect personal information and learning progress on e-learning platforms.
- Research Collaboration: Facilitates secure data sharing in research projects across institutions, protecting sensitive information and intellectual property.
- Attendance and Academic Achievement Records: Utilizing blockchain to securely record and store student attendance and academic achievements.

Student1

Student1 is a specific platform that provides cloud-based systems for the management of student data and records in educational institutions. It emphasizes the secure handling of sensitive student information, integrating advanced data governance and privacy measures. This platform ensures controlled access and safeguards academic and personal student data, streamlining data management while maintaining compliance with privacy regulations. "Student1" represents a practical application of technology solutions in the education sector, addressing real-world needs for data security and efficiency (Student1, n.d.).

IPfolio

IPfolio is a platform that helps universities and educational organizations manage and protect their intellectual property (IP) rights. It provides tools for tracking, managing, and safeguarding various forms of IP, including innovations and research findings. IPfolio's services are designed to streamline the IP management process, ensuring that educational institutions can effectively secure their intellectual property (Clarivate, n.d.).

Blockcerts

Blockcerts is an initiative that utilizes blockchain technology for issuing and verifying academic credentials. It provides a decentralized system for creating, issuing, and storing certificates and badges, ensuring authenticity and reducing the risk of fraud. Blockcerts enables educational institutions to issue tamper-proof records, and recipients can easily share their verified credentials with employers or other institutions. This application of blockchain in education enhances the security and portability of academic achievements (Blockcerts, n.d.).

Coursera

Coursera, an online learning platform, offers a wide range of courses from various educational institutions globally. While Coursera itself does not specialize in blockchain technology for its operations, it focuses on providing secure and accessible e-learning experiences. It implements robust data protection measures to safeguard user information, ensuring privacy and security for its learners. Coursera's platform is a significant example of how technology can enhance educational accessibility and quality in the digital age (Coursera, n.d.).

Artifacts

Artifacts is a blockchain-based platform designed for academic research collaboration. It provides a secure environment for researchers to share data and findings while maintaining intellectual property rights and data integrity. The platform facilitates transparent and verifiable tracking of research contributions, enhancing collaboration among scientists and institutions. This application of blockchain technology aims to revolutionize how academic research is conducted and shared, ensuring credibility and secure data management in scholarly work (Artifacts, n.d.).

ACCREDIBLE

Accredible is a platform that leverages technology to provide digital badges and certificates for academic and professional achievements. It enables educational institutions and organizations to issue verifiable and secure digital credentials. These credentials can be easily shared by recipients across digital platforms, enhancing their visibility and credibility. Accredible's approach modernizes the certification process, making it more accessible and convenient for both issuers and recipients (Accredible, n.d.).

3.5. ENTERTAINMENT AND SOCIAL MEDIA

Social media platforms have become central to modern communication, and with that comes a responsibility to protect user data and maintain the quality of content. One of the key challenges in this sector is user data privacy. Social media platforms gather extensive user data, including personal information, preferences, and online behaviour (Hanlon & Jones, 2023). Robust data governance practices are crucial to protect user privacy, ensure responsible data handling, and comply with data protection laws, such as the European Union's General Data Protection Regulation (GDPR). These practices include transparency in data collection, robust consent mechanisms, and user data access controls, allowing users to have control over their information. Content moderation is another significant issue in the social media domain. Maintaining the quality and safety of content shared on social platforms is essential to foster a positive online community and prevent the spread of harmful or inappropriate content. Data governance mechanisms, such as content filtering algorithms and user reporting systems, play a pivotal role in identifying and removing content that violates community guidelines. By implementing effective data governance, social media platforms can create a safer, more responsible, and user-centric online environment while respecting user privacy and content quality. Here's an overview of how Data Governance mechanisms are being used in the Entertainment and Social Media sector:

- User data privacy: Social media platforms handle extensive user data. Robust data governance is crucial to protecting user privacy, ensuring responsible data handling, and complying with data protection laws.
- Content moderation: Maintaining the quality and safety of content shared on social media is a significant challenge. Data governance mechanisms are used

to implement content moderation, filter out harmful content, and protect the online community.

- **Targeted Advertising:** Balances personalized advertising with user privacy. Data governance ensures relevant content delivery while respecting privacy norms and user preferences.
- **Royalty Distribution in Streaming:** Manages the fair allocation of royalties to content creators in streaming platforms, using data tracking to accurately measure content usage and viewership.
- **VR/AR Data Management:** Safeguards personal data in virtual and augmented reality experiences, ensuring immersive interactions are secure and privacy compliant.

In the realm of social media, companies are increasingly focused on regulating user privacy. This involves developing and implementing robust data governance measures to protect user data and comply with various data protection laws. The use cases include employing blockchain technology for secure data management, enhancing privacy in targeted advertising, and ensuring ethical handling of personal data. These efforts are crucial for maintaining user trust and adhering to legal standards in the rapidly evolving digital landscape of social media.

- Facebook’s Data Privacy Initiatives: Implementing robust data governance to enhance user privacy and comply with regulations like GDPR.
- YouTube’s Content Moderation System: Utilizes advanced algorithms and user reporting to filter harmful content, ensuring a safe online environment.
- Spotify’s Royalty Distribution Model: Employs data analysis to track music streaming for fair royalty payments to artists.
- Snapchat’s AR Filters: Provides secure and privacy-compliant augmented reality features, ensuring user data protection.

In the entertainment industry, mainly in gaming, the application of technology for privacy and data management shows a distinct approach compared to social media companies. The focus is on integrating blockchain to enhance in-game asset management and protect player data. Unique cases like the use of blockchain in virtual real estate trading in gaming environments or managing music rights in gaming platforms illustrate the industry's innovative use of technology. These applications reflect the specific needs of gaming environments in safeguarding user interactions and digital assets.

In 2017, Spotify acquired Mediachain, a blockchain startup, with the intention to explore blockchain technology for potential applications in music streaming. Mediachain's technology was aimed at addressing issues like proper attribution and royalty payments for artists. The acquisition indicated Spotify's interest in leveraging blockchain to improve and streamline music rights management and royalty distribution, although specific details on the implementation and progress of this initiative within Spotify's platform have not been widely publicized (Perez, S., 2017).

Audius

Audius is a blockchain-based music streaming service that seeks to disrupt the traditional music industry model by giving more power to artists and listeners (Genç, 2021). It allows artists to upload their music directly and engage with their audience without intermediaries. This model offers potentially fairer compensation and more control over their work for artists. For listeners, it provides access to a diverse range of music and direct interaction with creators. Audius exemplifies how blockchain technology can be used to foster a more direct and equitable music ecosystem (Audius, n.d.).

Enjin

Enjin is a blockchain platform that focuses on the gaming industry. It enables developers to create and manage virtual goods on the Ethereum blockchain. Enjin's platform (Rapoza, 2021) is used for integrating blockchain-based assets like in-game items and currencies, providing a secure and transparent system for their management. This approach offers gamers true ownership of their in-game assets and enhances the overall gaming experience. Enjin demonstrates how blockchain can be innovatively applied in gaming for asset management and user engagement (Enjin, n.d.).

Decentraland

Decentraland is a virtual reality platform powered by the Ethereum blockchain. It allows users to create, experience, and monetize content and applications in a virtual world (Lodge, 2023). In Decentraland, users can purchase and develop virtual land, creating an immersive experience that blends gaming with digital asset ownership and management. This project showcases the innovative use of blockchain in virtual environments, offering a unique combination of entertainment, digital real estate, and community-driven development (Decentraland, n.d.).

Funded by the European Union

3.6. ENERGY AND SUSTAINABILITY

In the energy and sustainability sector, the integration of robust data governance and privacy practices plays a pivotal role. Efficient resource management is a key application area, where data analysis is used to optimize energy consumption and reduce waste. This involves strategies for sustainable energy use and identifying areas for improvement in resource utilization. Another crucial application is in monitoring and reporting carbon emissions. Accurate data collection and analysis are essential for assessing environmental impacts, complying with international environmental standards, and supporting sustainability initiatives. These use cases underline the importance of data governance in driving sustainable practices and promoting a greener future.

In the context of energy and sustainability, the integration of data governance and privacy practices is becoming increasingly important. This sector is at the forefront of addressing global environmental challenges, where efficient management and analysis of data play crucial roles. From optimizing energy consumption and integrating renewable sources to monitoring carbon emissions and developing smart grid technologies, data governance is pivotal in enhancing sustainability efforts. Additionally, it aids in regulatory compliance and informs policy development, paving the way for technological advancements in energy storage and distribution. This introduction sets the stage for exploring the multifaceted impact of data governance in driving sustainable and innovative practices in the energy sector. Here's an overview of how Data Governance and privacy practices mechanisms are being used in the Energy and Sustainability sector:

- Resource Management and Efficiency: Leveraging data to optimize energy consumption patterns, organizations implement strategies to enhance energy efficiency, reduce waste, and promote sustainable energy use.
- Emissions Monitoring and Reporting: Accurate data collection on carbon emissions enables organizations and governments to monitor and report their environmental impact, ensuring compliance with international standards and promoting sustainability initiatives.
- Smart Meter Data Analysis: Utilizing smart meters for detailed insights into energy usage patterns, helping both providers and consumers optimize energy consumption.
- Demand Response Systems: Implementing systems that adjust energy consumption based on real-time data to balance supply and demand, reducing strain on energy grids.

Funded by the European Union

- Predictive Maintenance in Energy Infrastructure: Leveraging data for predictive analytics to maintain energy infrastructure, enhancing efficiency and reducing downtime.

GERMANY'S ENERGIEWENDE

Germany's Energiewende is a significant national project aimed at transforming the country's energy system to be more sustainable and environmentally friendly (Russel & Wettengel, 2019). It involves a comprehensive shift from traditional fossil fuels and nuclear energy to renewable sources like wind and solar power. The initiative emphasizes not only the integration of renewable energy into the power grid but also energy efficiency and reduction in carbon emissions. This transition is a key example of how data governance and innovative policies can drive sustainable changes in the energy sector (Agora Energiewende, n.d.).

ENERGYHUB

EnergyHub is a technology company that provides a platform for managing energy use, particularly in residential areas. Their system allows consumers and utilities to effectively monitor and control energy consumption, contributing to more efficient use and cost savings. EnergyHub's solutions are focused on smart home devices and demand response programs, helping to balance energy supply and demand, and promoting sustainable energy practices in households (EnergyHub, n.d.).

SIEMENS

Siemens is actively involved in developing smart grid technologies, focusing on enhancing the efficiency and reliability of energy distribution. Their smart grid solutions incorporate real-time data analysis, which allows for better management of energy flow, integration of renewable energy sources, and improved responsiveness to changes in energy demand. Siemens' smart grid technology is a key component in modernizing electrical grids to be more adaptive, efficient, and sustainable (Siemens, n.d.).

IRENA

The International Renewable Energy Agency (IRENA) is an intergovernmental organization that supports countries in their transition to sustainable energy. It provides policy advice and facilitates knowledge sharing and capacity building. IRENA plays a crucial role in gathering and analyzing data to help formulate energy policies that are environmentally sustainable and economically viable. Their efforts are instrumental in guiding international standards and practices for renewable energy implementation and regulation (IRENA, n.d.).

Funded by the European Union

TESLA

Tesla, known for its electric vehicles, also develops advanced energy storage and distribution solutions like the Tesla Powerwall. The Powerwall is a rechargeable home battery system that stores energy from solar panels or the grid. It's designed to provide energy backup, enhance energy independence, and facilitate the use of renewable energy sources. Tesla's approach to energy storage exemplifies the application of innovative technologies in managing and optimizing energy use, aligning with sustainable energy practices (Armstrong, 2023; Capoot, 2024; Tesla, n.d.).

These cases in energy and sustainability demonstrate how data governance and privacy practices, aligned with the objectives of OC2, are vital in advancing sustainable energy solutions. From Germany's Energiewende to Tesla's Powerwall, each example reflects the importance of data management in achieving energy efficiency, integrating renewable sources, and complying with regulations. These projects illustrate a broader trend towards sustainable practices, supported by innovative technologies and data-driven strategies, contributing valuable insights to the OC2 framework.

Smaller-scale projects, such as local community solar initiatives, startups focusing on microgrid technology, and university-led sustainability research, play a crucial role in the energy and sustainability ecosystem. These projects, while smaller in scope, contribute significantly by innovating at a grassroots level, serving as practical models for sustainable energy practices and data governance. They complement larger-scale initiatives, demonstrating that contributions towards a sustainable future can be effective at various scales and in diverse contexts, aligning seamlessly with the broader objectives outlined in the initial section of OC2.

Some examples of smaller-scale, tangible projects in the energy and sustainability sector include:

Local Community Solar Projects: These projects involve community-driven efforts to establish solar power installations, providing renewable energy to local residents. Big Solar Co-op (Big Solar Co-op, n.d.) in various regions, where local communities collectively invest in and benefit from solar energy.

Startups Focused on Microgrid Technology: Small companies developing innovative microgrid solutions to enhance energy distribution and reliability in remote or under-served areas
(LO3 Energy, 2022) develops microgrids using blockchain to enable local energy trading.

University-Led Sustainability Initiatives: Academic research projects exploring new methods of energy conservation, storage, or efficiency. MIT's Sustainable Energy Initiative (MIT Energy Initiative, n.d.) conducts research on advancing sustainable energy technologies and solutions.

These projects are more directly relatable and demonstrate practical applications of sustainable energy practices and data governance at a community or regional level.

3.7. SUPPLY CHAIN MANAGEMENT

In the realm of supply chain management, the integration of sophisticated data governance and privacy protocols is pivotal. This field encompasses complex networks of production, shipment, and distribution, where efficient and transparent data management is crucial. Effective data governance in supply chain management not only enhances operational efficiency but also ensures the integrity and security of data across various stakeholders. This approach is instrumental in optimizing logistics, managing inventory, and ensuring timely delivery, thereby fostering a more resilient and responsive supply chain ecosystem (International Food Information Council [IFIC] Foundation, 2019). Here's an overview of how Data Governance mechanisms are being used in the Supply Chain Management sector:

- Product Traceability and Authenticity: Data governance enables the tracking of product origins and movements, ensuring authenticity and preventing counterfeiting. This is crucial for maintaining quality standards and consumer trust.
- Logistics Optimization: Strategic data analysis improves logistics efficiency, encompassing inventory management and transport route optimization. Efficient data management in this area ensures timely deliveries and cost-effective operations, vital for competitive advantage in the market.
- Sustainable Sourcing: Implementing data governance to monitor and ensure sustainable practices in sourcing materials, crucial for eco-friendly supply chains.
- Blockchain for Supply Chain Transparency: Utilizing blockchain technology to create a transparent and tamper-proof record of transactions, enhancing trust and traceability.
- Predictive Analytics for Demand Forecasting: Using data analysis to predict market trends and customer demand, improving inventory management and reducing overstock or shortages.

Funded by the European Union

- Cold Chain Monitoring: Implementing IoT and data governance for monitoring temperature-sensitive products during transportation, ensuring quality and compliance.
- Supplier Relationship Management: Leveraging data to evaluate and manage supplier performance, ensuring efficient collaboration and supply chain resilience.

Provenance and Woolmark

Provenance and Woolmark collaborated on a project using blockchain technology to trace and verify the production and sourcing of wool (Provenance, 2019). This initiative was designed to ensure that wool products are sourced sustainably and ethically. The project aimed to provide transparency in the wool supply chain, allowing consumers to have detailed information about the origin and production practices of wool products. This use of blockchain in the textile industry serves as an example of how technology can enhance sustainability and ethical practices in supply chains (Provenance, n.d.; Woolmark Prize, n.d.).

Walmart

Walmart's blockchain project focuses on enhancing food safety and traceability within its supply chain (IBM, 2020). They implemented a blockchain system to track the journey of food items, from their origin at the farm to the store shelves. This initiative aims to improve transparency in the food supply chain, allowing for quicker identification and resolution of food safety issues. The project highlights how blockchain technology can be used to ensure product safety and build consumer trust in food quality (Walmart, n.d.).

DHL and Accenture

DHL, in collaboration with Accenture (Accenture, 2018; Freightwaves, 2018), developed a blockchain-based project to enhance the tracking and security of pharmaceutical products. This initiative aims to combat counterfeit drugs in the supply chain, ensuring the integrity and authenticity of pharmaceuticals. The project uses blockchain technology to create a secure, transparent record of each medicine's journey from manufacture to delivery, contributing significantly to the safety and reliability of pharmaceutical distribution (DHL, n.d.).

Maersk and IBM

Maersk and IBM collaborated on TradeLens, a blockchain-based digital shipping solution designed to promote global trade transparency (IBM, 2019). This platform enables various stakeholders in the shipping industry, such as cargo owners, shipping lines, and customs authorities, to access real-time shipping data and documentation. TradeLens enhances efficiency and accuracy in global shipping operations by improving information sharing and reducing the time spent on document processing.

Sensitech's Cold Chain Monitoring Solutions

Sensitech's Cold Chain Monitoring Solutions focus on monitoring temperature-sensitive products during transportation. They provide technology to ensure that goods such as pharmaceuticals and perishable foods are transported within safe temperature ranges. This is crucial for maintaining product quality and compliance with health and safety standards. Sensitech's solutions use sensors and data analysis to provide real-time monitoring and alerts, helping prevent spoilage and ensuring the integrity of temperature-sensitive shipments (Sensitech, n.d.).

IBM Food Trust

IBM Food Trust (IBM, 2024) is a blockchain-based system designed to enhance food safety and traceability. It provides a transparent platform for tracking food products throughout the entire supply chain, from the farm to the consumer. This system enables improved food safety standards, reduces waste, and ensures fresher produce. By leveraging blockchain technology, IBM Food Trust enhances the ability of different stakeholders in the food supply chain to share information quickly and accurately, improving overall food quality and safety for consumers.

3.8. PUBLIC SECTOR AND GOVERNMENT

In the public sector and government, effective data governance and user privacy are critical for ensuring transparent and efficient public services. These institutions handle vast amounts of sensitive information, making data security and ethical management paramount (Goel, 2018; Perrigo, 2018). The application of robust data governance frameworks in this sector is key to maintaining public trust, enhancing service delivery, and ensuring compliance with legal and ethical standards. This integration facilitates a more accountable and responsive government, paving the way for innovative and citizen-centric public services. Here’s an overview of how Data Governance and user privacy practices are being used in the Public Sector and Government:

- Citizen Data Management: Governments utilize data governance for managing citizen information, ensuring accuracy, privacy, and security. This includes personal identification data, tax records, and health information.

Funded by the European Union

- Policy Making and Public Services: Data-driven decision-making in policy formulation and public service delivery. Effective data governance allows for the analysis of large datasets to inform policy decisions and improve public service offerings.
- Digital Identity Management: Implementing secure digital identity systems for citizens, enhancing access to government services and protecting identity data.
- Public Health Data Analysis: Utilizing data governance to manage public health data, crucial for disease tracking, health policy development, and crisis response.
- E-Government Services: Offering citizen-centric online services, requiring effective data management for service delivery and data protection.
- Infrastructure and Urban Planning: Using data analytics for sustainable urban development and infrastructure planning, improving living standards and efficiency.
- Transparency and Anti-Corruption Initiatives: Employing data governance tools to increase transparency in government operations and combat corruption.

In the public sector and government, the effective integration of data governance and privacy is crucial, as seen in the examples of managing citizen data and policymaking. Projects like Estonia's e-Residency, Singapore's Smart Nation Initiative, and India's Aadhaar program demonstrate practical applications of these principles. They showcase how innovative data governance can enhance public services, improve efficiency, and foster transparency.

Estonia's e-Residency Program

Estonia's e-Residency program is a groundbreaking initiative that offers a digital identity to non-residents, allowing them to access Estonian services online. The program enables entrepreneurs globally to establish and manage an EU-based company online. This forward-thinking approach to digital identity and business administration has positioned Estonia as a leader in digital governance (e-Residency Estonia, n.d.).

SINGAPORE'S SMART NATION INITIATIVE

Singapore's Smart Nation Initiative is a comprehensive effort to leverage technology to improve living standards and create economic opportunities. This initiative includes projects ranging from smart urban solutions, like intelligent transport systems and smart buildings, to digital government services. It aims to transform Singapore into a leading global city powered by digital innovation (Singapore Computer Society, 2020; Singapore Smart Nation, n.d.).

INDIA'S AADHAAR PROGRAM

India's Aadhaar program is a massive biometric ID system, the largest in the world, providing a unique 12-digit identity number to Indian residents. It's linked to biometric data and used for various government and non-government services, aimed at improving efficiency in service delivery and reducing fraud. Aadhaar has been pivotal in streamlining processes in welfare distribution, banking, and public services (Aadhaar, n.d.).

THE "OPEN GOVERNMENT PARTNERSHIP" INITIATIVE

The Open Government Partnership (OGP) is a multilateral initiative that aims to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance. Launched in 2011, OGP provides a platform for reformers inside and outside of government to develop open government reforms and foster a global culture of transparency and accountability in public administrations. This initiative reflects a growing global movement towards open governance and participatory democracy (Open Government Partnership, n.d.).

SIDEWALK LABS

Sidewalk Labs, an Alphabet (Google's parent company) subsidiary, focuses on urban innovation. It aims to develop technologies to address urban challenges, improve infrastructure, and enhance the quality of life in cities. The company's approach combines forward-thinking urban design with cutting-edge technology, such as IoT and AI, to create smarter, more sustainable urban environments. Their most notable project was the proposed development in Toronto's Quayside area, intended to be a model of a smart, sustainable neighbourhood. For detailed information about Sidewalk Labs and its projects, you can visit their official website or look for news articles covering urban development and smart city initiatives (Sidewalk Labs, n.d.).

Funded by the European Union

THE EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL (ECDC)

The ECDC exemplifies data governance in public health by collecting, analysing, and disseminating critical health data across EU member states. Their role in coordinating disease surveillance and response strategies hinges on the effective management of health data. This approach underscores the importance of data governance in public health policymaking and crisis management, aligning with the overarching themes of effective data usage and privacy concerns in the public sector, particularly in the context of public health management (ECDC, n.d.).

These projects underscore the transformative impact of data governance in the public sector. They highlight the potential of technology to drive more accountable, efficient, and citizen-centric government services, reflecting the objectives and themes central to OC2.

3.9. AUTOMOTIVE AND TRANSPORTATION

In the automotive and transportation sector, data governance and privacy are paramount for innovation and safety. This industry is rapidly evolving with the advent of connected vehicles and smart transportation systems. Effective data management is essential for optimizing vehicle performance, enhancing safety features, and facilitating efficient transportation networks. The integration of robust data governance in this sector not only improves operational efficiency but also ensures the security and privacy of user data, which is increasingly critical in an era of connected and autonomous vehicles. This is an overview of how Data Governance and privacy mechanisms are being used in the Automotive and Transportation sector:

- Vehicle Performance Optimization: Leveraging data to enhance vehicle efficiency, maintenance, and safety features. This involves analyzing performance metrics to identify areas for improvement.
- Traffic Management and Smart Cities: Utilizing data for efficient traffic flow management and the development of smart city infrastructure. This includes the use of real-time data to optimize traffic signals and reduce congestion.
- Autonomous Vehicle Data Analysis: Collecting and analyzing data from self-driving vehicles to improve safety features, navigation, and traffic interaction.
- Emission Monitoring and Eco-Driving: Utilizing vehicle data to monitor emissions, promoting eco-friendly driving practices and compliance with environmental regulations.
- Connected Vehicle Services: Implementing data-driven services in connected cars, such as predictive maintenance alerts and real-time navigation updates.

Funded by the European Union

- Public Transport Optimization: Analyzing data from public transit systems to optimize routes, schedules, and passenger flow, enhancing the efficiency and reliability of public transportation.

TESLA

Tesla optimizes vehicle performance using data analytics and software updates. Their electric cars are equipped with sensors and computing systems that gather data on vehicle usage, performance, and environmental conditions. Tesla analyzes this data to improve features like battery life, driving range, and autopilot capabilities. Through over-the-air software updates, Tesla continuously enhances vehicle performance and introduces new features, ensuring their vehicles remain technologically advanced. This approach to data-driven performance optimization is a hallmark of Tesla's innovative strategy in the automotive industry (Tesla’s Use of Data to Innovate in the Auto Industry, n.d.).

GOOGLE WAYMO

Waymo's self-driving technology has significant implications for smart city management. By collecting and analyzing vast amounts of data from its fleet of autonomous vehicles, Waymo contributes to more efficient traffic flow and reduced congestion in urban areas (Lee, 2024). The insights gained can inform city planning and traffic management decisions, leading to smarter, safer, and more sustainable urban environments. Waymo's technology demonstrates the potential of autonomous vehicles to integrate seamlessly into the broader ecosystem of smart city infrastructure.

TOYOTA

Emission Monitoring and Eco-Driving involve using technology in vehicles to track and reduce emissions, promoting environmentally friendly driving habits. Modern vehicles, especially hybrids and electric cars, are equipped with sensors and systems to monitor real-time emissions. This data is used to inform drivers about their driving patterns and how they can adjust to be more eco-friendly, like optimizing fuel efficiency and reducing idling. These technologies are crucial for meeting environmental regulations and contribute to reducing the overall carbon footprint of transportation (Toyota Motor Corporation, 2023).

BMW Connected Drive

BMW ConnectedDrive is a suite of digital services and features designed to enhance the connectivity and functionality of BMW vehicles. It includes various services such as real-time traffic information, remote control functions, and maintenance alerts. The system integrates the vehicle with the driver's digital lifestyle, offering seamless access to information and entertainment. ConnectedDrive also focuses on safety features, providing assistance services and the ability to call for help in emergencies. This technology represents BMW's commitment to advanced automotive connectivity and user convenience (BMW, n.d.).

City of London

The Oyster card system in London is an electronic ticketing scheme used for public transport across the city. It allows travelers to use a single, rechargeable card for access to various modes of transportation like buses, underground trains, trams, and some river services. The system simplifies payment and reduces the need for paper tickets. It also collects travel data, which helps in optimizing routes and schedules for London's public transport, contributing to more efficient and effective transit management (Transport for London, n.d.).

4. DECENTRALISED USER-CENTRIC USER PRIVACY AND DATA GOVERNANCE FRAMEWORKS

Blockchain technology is emerging as a powerful solution in data governance and user privacy, especially in compliance with regulations like GDPR, CCPA, and HIPAA (Leenes & Martin, 2021). It offers innovative approaches to regulatory compliance and decentralized identity management. Applications include secure storage and sharing of medical records under HIPAA and self-sovereign identity management, aligning with Privacy by Design principles. This text explores how blockchain can be a key tool in establishing user-centric data governance frameworks while respecting existing data privacy and security regulations.

4.1. GDRP: BLOCKCHAIN-BASED SOLUTIONS FOR GDPR COMPLIANCE

The General Data Protection Regulation (GDPR) has introduced stringent requirements for data protection and privacy. Blockchain technology plays a significant role in ensuring GDPR compliance. Blockchain's immutable ledger ensures that data transactions are recorded transparently and cannot be altered, enhancing transparency and accountability. Moreover, blockchain's decentralized nature reduces the reliance on central authorities, empowering individuals to have more control over their personal data.

A notable example of blockchain-based GDPR compliance is the use of smart contracts for consent management. These contracts allow individuals to specify how their data is used and shared. When data usage aligns with the terms defined in the smart contract, the system automatically grants access, ensuring that data processing adheres to user consent. If there is any deviation from the agreed-upon terms, the smart contract prevents unauthorized access, thereby preserving privacy.

In addition to blockchain, cryptography-based privacy-preserving techniques are instrumental in achieving GDPR compliance. Techniques like homomorphic encryption allow computations on encrypted data without revealing the underlying information. This ensures that sensitive data remains confidential while still enabling data analysis and processing. By combining blockchain and cryptography, organizations can navigate the complexities of GDPR while empowering users with greater control over their data.

4.2. CCPA: DECENTRALIZED IDENTITY MANAGEMENT USING BLOCKCHAIN

The California Consumer Privacy Act (CCPA) gives consumers more control over their personal information (California Attorney General, n.d.). Decentralized identity management, facilitated by blockchain technology, aligns well with the spirit of CCPA. Blockchain allows individuals to maintain control over their digital identities and determine who has access to their personal information. This decentralized approach grants users the ability to revoke or grant permissions, offering a more user-centric and compliant way of handling personal data.

For instance, users can establish a self-sovereign identity on a blockchain, creating a secure and immutable record of their identity. This identity can be used to control access to various services and platforms. Users have the autonomy to share or withhold their information, ensuring compliance with CCPA's privacy regulations.

Additionally, cryptography-based data anonymization techniques are critical in CCPA compliance. These techniques allow organizations to process data in a way that removes personally identifiable information while still retaining data utility. This not only protects consumer privacy but also allows businesses to gain valuable insights while adhering to CCPA's requirements.

4.3. HIPAA: BLOCKCHAIN-BASED SECURE STORAGE AND SHARING OF MEDICAL RECORDS

HIPAA, the Health Insurance Portability and Accountability Act, is a significant American regulation that sets standards for the protection of sensitive patient health information. Although a U.S. regulation, it's important to mention HIPAA in a global context due to the interconnected nature of healthcare markets and the prevalence of multinational healthcare and technology companies. HIPAA requires healthcare providers, insurers, and other entities to ensure the confidentiality and security of protected health information (PHI) (Edemekong, Annamaraju, & Haydel, 2024).

In the realm of blockchain technology, HIPAA's guidelines become increasingly relevant. Blockchain's potential for secure storage and sharing of medical records aligns with HIPAA's emphasis on data security and privacy. Utilizing blockchain can enhance the way medical records are managed and shared, offering a secure, immutable, and transparent approach. This ensures not only compliance with HIPAA standards but also addresses the global demand for secure and efficient healthcare data management.

Funded by the European Union

Blockchain's immutability ensures that medical records are tamper-proof. Once information is recorded on the blockchain, it cannot be altered or deleted. This feature is vital for maintaining the integrity of medical records and ensuring that they remain accurate and unaltered.

Cryptography-based access control mechanisms further enhance HIPAA compliance. Only authorized personnel can access specific medical records, and this access can be controlled and audited using cryptographic techniques. This ensures that sensitive medical data is only accessible to those who have a legitimate need, helping organizations adhere to HIPAA's stringent regulations.

5. PRIVACY BY DESIGN: BLOCKCHAIN-BASED SELF-SOVEREIGN IDENTITY MANAGEMENT

Privacy by Design is an approach that emphasizes the integration of privacy into the design and development of systems and practices. Blockchain-based self-sovereign identity management is a prime example of this approach in action. With self-sovereign identities, users have ultimate control over their digital identities, deciding who has access to their personal information and under what circumstances.

Users can create and manage their digital identities on a blockchain, allowing them to selectively share identity attributes and personal information as needed. This aligns with Privacy by Design principles, as it ensures that privacy is a fundamental aspect of the system's architecture, and users have the power to determine how their data is used.

Cryptography-based privacy-enhancing technologies are integral to this approach. They enable secure and confidential data sharing. Through cryptographic techniques, data can be encrypted, and zero-knowledge proofs can be used to verify certain attributes without revealing the underlying data. This not only enhances privacy but also aligns with the core principles of Privacy by Design, ensuring that privacy is a fundamental consideration in the development of digital systems.

Considering the user-centric approach in the domain of SSI, it is of monumental importance to ensure that the users' privacy is not disclosed, namely that an adversary cannot access sensitive user information or link any data to a particular user.

There are different techniques that may be utilized to preserve the privacy of the users, where the primary concern when choosing a privacy-preserving method is to balance the trade-off between privacy and data utility. For example, by using encryption, a high level of data utility may be achieved, while privacy may be disclosed in the case of a key leakage attack. Another disadvantage of encryption-based privacy-preserving mechanisms is that they are heavy in terms of computations and may not be suitable for resource-constrained devices. On the other hand, noise addition mechanisms are lightweight, but the utility of the noisy data may be lower (Rahman, Paul, & Sattar, 2023).

There are a number of data transformation techniques that can be used for the purpose of data anonymization. For example, **Generalisation** may be utilized to replace the values in the original dataset with more generic representation following a predefined generalisation hierarchy. Another technique called **Suppression** implies the erasure of some values from the original dataset. Suppression can be performed on different levels. Record Suppression is used to delete the entire record from the dataset, while Value Suppression is utilized to remove a particular value from the entire dataset.

Funded by the European Union

Bucketisation (Wang, Wang, Fu, & Wong, 2016) may be used to publish publicly known and sensitive attributes separately, whereas both datasets contain a common attribute (group id) that may be used to link a record containing sensitive data to a record with publicly known attributes. A **permutation** mechanism may be used to separate public data and sensitive attributes, where sensitive records are shuffled. However, in the presence of logical links between the attributes, the privacy guarantee may be poor. **Perturbation** mechanisms modify the records in the original dataset in a way that they do not correspond to the original values. One of the most popular data perturbation techniques is related to noise addition, where **Differential Privacy** (DP) (Dwork & Roth, 2014) is one of the most popular approaches. The data in the original dataset are perturbed by injecting controllable noise using the Laplace or Gaussian mechanism, where the trade-off between privacy and utility is controlled by the parameter called privacy budget, which reflects the amount of noise to be injected. Thus, the higher the privacy level, the lower the data utility.

UBER

Uber uses DP to protect the privacy of users' geospatial data. By injecting noise into location data, Uber provides aggregated insights for analysis while ensuring the privacy of individuals (Uber, 2021).

FACEBOOK

Facebook uses the concept of Local Differential Privacy (Wang, 2020), which means that the noise is injected on the end-user's side before sharing data with a central server. This allows Facebook to perform aggregated analyses, while preserving the privacy of individuals.

Some of the most popular data anonymization methods include but not limited to **K-anonymity**, **l-diversity**, and **t-closeness** (Vimercati, Foresti, Livraga, & Samarati, 2023). The idea of K-anonymity is to ensure that no entry in a dataset can be identified using the combination of available attributes and external data. Thus, any record in a dataset should be indistinguishable from at least k-1 other records with respect to particular attributes. L-diversity is another approach that is used to protect sensitive information. The main idea of L-diversity is to make sure that any group of indistinguishable entries contains a sufficient variety of values of the sensitive attribute. T-closeness is another privacy-preserving concept that measures the distributional similarity of the sensitive attribute within each group of indistinguishable entries and compares it to the overall distribution in the entire dataset. The idea of T-closeness is to prevent outliers (values) of the sensitive attribute from being over-represented within any group of indistinguishable entries.

Funded by the European Union

Social Media Platforms may utilize k-anonymity techniques to preserve the privacy of individuals when sharing aggregated user behaviour or demographic data for analytics.

Educational Institutions may utilize l-diversity techniques when sharing aggregated data for analytics. This allows the protection of students' privacy by ensuring a diversity of sensitive attributes within indistinguishable groups.

Financial Institutions may employ T-closeness techniques to make sure that the distribution of sensitive financial attributes in aggregated data does not reveal too much information about individuals.

One of the most popular and advanced encryption techniques that is used to ensure privacy is Homomorphic encryption (HE) (Acar, 2019). Using HE, the computations can be performed on encrypted data without decrypting it. In contrast, in traditional encryption schemes, computations can only be performed on decrypted data, which exposes it to cyber-security risks. The key advantage of HE is that the result of a computation on encrypted data, when decrypted, is the same as if the same operations have been performed on the unencrypted data. There are three types of HE mechanisms offering different degrees of functionality. Partially Homomorphic Encryption (PHE) supports addition or multiplication operations on encrypted data but not both operations. Somewhat Homomorphic Encryption (SHE) supports both addition and multiplication, but the number of operations is limited. Fully Homomorphic Encryption (FHE) supports an unlimited number of both addition and multiplication operations, which is computationally intensive compared to PHE and SHE.

TENFOLD

Tenfold utilizes HE to provide a platform for secure and privacy-preserving computation on sensitive data, where data confidentiality is paramount (tenfold Software GmbH, n.d).

ENVEIL

Enveil utilizes HE to enable secure and private search operations on encrypted data, which allows organizations to perform analytical tasks without revealing raw data.

Secure Multiparty Computation (SMPC) (Zhao, 2019) is a cryptography-based technique, which can be used when multiple parties want to collaboratively perform a computation without revealing sensitive information to each other. Traditionally, the parties would need to share their data with a central authority to perform computation. However, in the scenarios when parties need to perform computation on sensitive data, and they are not willing to share sensitive information with other parties, a traditional

Funded by the European Union

approach may not be suitable. Moreover, a central server is a single point of failure in this case, as well as it may be curious and want to access the sensitive information of participants. SMPC allows parties to jointly perform a computation while not revealing their confidential information to other parties. Some of the applications of SMPC include but are not limited to collaborative financial analysis and voting processes. During the SMPC process, parties need to communicate with each other a number of times to complete the computation, which may add additional communication overhead. However, there are some advanced SMPC mechanisms recently proposed aiming at reducing the number of communication rounds (Canetti, Makriyannis, & Peled, 2020).

Partisia

Partisia utilizes SMPC to enable privacy-preserving machine learning in decentralized AI environment, which allows multiple parties to collaboratively build machine learning models without revealing their raw data.

ScaleOut Software

ScaleOut uses SMPC for privacy-preserving geospatial analytics, where multiple parties compute aggregate results without exposing their raw geospatial data.

Blockchain technology (Monrat, 2019) has become one of the most popular technologies for privacy preservation and has attracted a lot of attention across industry and academia. Blockchain enables secure and tamper-resistant record-keeping of transactions across a number of participating nodes. The transactions in the blockchain are packed in blocks, where each new block is chained to a previous one. There is no central authority in the blockchain network where each participant stores a copy of the entire blockchain. To prevent malicious activities, participants utilize a consensus mechanism to agree on the validity of a new block before it is written to the blockchain. This ensures that all participants have access to the same information, eliminating a single point of failure, reducing the risk of fraud, and creating transparency. One of the outstanding features of blockchain is related to the concept of smart contracts. Smart contracts are self-executing contracts that contain the terms of the agreement written into codes. When the conditions are met, a smart contract executes automatically without any third party.

Everledger

To provide transparency and traceability in the diamond industry, Everledger utilizes blockchain to create a digital ledger for diamonds, which helps combat the trade of conflict diamonds and provides consumers with information about the ethical and environmental impact of their purchases (The Digital Insurer, n.d.).

Accenture

Accenture uses blockchain to enhance security and efficiency in interbank transactions, namely, to streamline cross-border payments, reduce settlement times, and improve the overall security of transactions (Accenture, n.d.).

5.1. BLOCKCHAIN-BASED SOLUTIONS: ZERO-KNOWLEDGE PROOFS

Blockchain-based solutions play a pivotal role in enhancing privacy and data governance. For example, zero-knowledge proofs provide a powerful tool for privacy-preserving transactions. They enable parties to prove a statement is true without revealing the underlying data. In the context of financial transactions, this technology allows for secure and private transactions, as no sensitive data is exposed during the verification process. This not only safeguards user privacy but also ensures compliance with regulations like GDPR and CCPA.

Zero-knowledge proofs (ZKPs) are a cryptographic concept that plays a crucial role in blockchain-based solutions, enhancing privacy and security. In a zero-knowledge proof, one party (the prover) can prove to another party (the verifier) that they possess certain information without revealing the actual content of that information. This cryptographic technique has various applications in blockchain technology, promoting privacy, security, and efficiency. Here's an overview of how zero-knowledge proofs are used in blockchain-based solutions:

- Privacy in Transactions: In blockchain networks, transactions are recorded on a public ledger. However, the details of these transactions, such as the sender, recipient, and transaction amount, are often visible to all participants. Zero-knowledge proofs can be employed to prove the validity of a transaction without revealing these details. This ensures financial privacy while maintaining the integrity of the blockchain (Zcash, n.d.).

- Identity Verification: Zero-knowledge proofs can be applied in identity verification processes. Users can prove they possess certain credentials without disclosing the actual details. This is particularly useful in scenarios where individuals want to prove they meet certain criteria without revealing unnecessary personal information (Privacy by Design, 2020).

- Smart Contracts and Computation: Zero-knowledge proofs enable the verification of computations without revealing the actual data being computed. This is valuable in smart contracts, where parties can execute complex computations without disclosing the input data. For example, a party can prove it possesses certain data without revealing the data itself, allowing for confidential and secure execution of smart contracts (Matter Labs, 2021).

- Password Authentication: Zero-knowledge proofs can be utilized in password authentication processes. Instead of sending a password, a user can prove they know the password without disclosing it, adding an extra layer of security to authentication processes (Goldwasser et al., 2021).

- Supply Chain and Asset Tracking: Zero-knowledge proofs can enhance privacy in supply chain and asset tracking systems. Participants can prove the authenticity of certain data (like the origin of a product) without revealing sensitive information, ensuring data integrity without compromising privacy (Everledger, 2021).

- Decentralized Finance (DeFi): In decentralized finance applications, zero-knowledge proofs can be employed to validate transactions and financial operations without disclosing specific details to all network participants. This helps in maintaining financial privacy and security (StarkWare, n.d.).

- Scalability and Efficiency: Zero-knowledge proofs can be used to improve scalability by reducing the amount of data that needs to be processed and stored on the blockchain. This can lead to more efficient and faster transaction processing (Aztec, 2021).

Examples of zero-knowledge proof systems include zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge) and zk-STARKs (zero-knowledge scalable transparent arguments of knowledge) (Canetti et al., 2020).

It is important to note that while zero-knowledge proofs offer enhanced privacy, their implementation requires careful consideration to ensure security and proper cryptographic design. As blockchain technology evolves, zero-knowledge proofs are likely to play an increasingly significant role in addressing privacy concerns and improving the overall functionality of decentralized systems.

Several companies and projects were actively working on zero-knowledge proofs (ZKPs) and blockchain privacy. Keep in mind that the blockchain space is dynamic, and new developments may have occurred since then. Here are some notable companies and projects that were involved in ZKPs and blockchain privacy:

- Zcash (ZEC): A cryptocurrency that focuses on privacy and uses a zero-knowledge proof system called zk-SNARKs. It allows users to make transactions with shielded addresses, where transaction details are encrypted (Zcash, n.d.).

- Ethereum (ETH): It has been exploring the integration of zero-knowledge proofs to improve privacy and scalability. Projects like Aztec Protocol and Matter Labs are working on zero-knowledge rollups to enhance the privacy and efficiency of Ethereum transactions (Aztec, 2023).

- Monero (XMR): A privacy-focused cryptocurrency that uses a different technology called ring signatures and stealth addresses for enhanced privacy. It does not specifically use zero-knowledge proofs, but it is noteworthy in the privacy-focused blockchain space (Monero, n.d.).
- zkSync (Matter Labs): A company that focuses on layer 2 scaling solutions for Ethereum. They have developed zkSync, a layer 2 scaling solution using zk-rollups, which leverages zero-knowledge proofs for enhanced privacy and scalability (Matter Labs, 2021).
- StarkWare: A company working on scaling solutions for blockchains, including zero-knowledge proof systems like zk-STARKs. They aim to improve scalability and privacy in blockchain networks (StarkWare, n.d.).
- Quorum (Consensys): An enterprise-focused blockchain platform developed by ConsenSys, has integrated privacy features, including a privacy implementation called Constellation. It allows for private transactions on a permissioned blockchain network (ConsenSys, 2020).
- Enigma (Secret Network): Focuses on privacy for decentralized applications (DApps). They have been working on solutions to bring privacy to public blockchains, allowing developers to build privacy-preserving applications (Secret Network, n.d.).
- Oasis Labs: A blockchain platform that emphasizes privacy and security. They utilize a combination of techniques, including secure enclaves and zero-knowledge proofs, to provide confidential smart contracts and data privacy (Oasis Labs, 2020).
- Aztec Protocol: A privacy-focused protocol for Ethereum that uses zero-knowledge proofs. It allows users to make confidential transactions on the Ethereum blockchain (Aztec, 2021).

6. DECENTRALIZED MARKETPLACES

Decentralized data marketplaces represent a transformative shift in the way data is traded and exchanged. These marketplaces leverage the principles of decentralization, often underpinned by blockchain technology, to facilitate a more open, transparent, and secure environment for data transactions. Unlike traditional centralized platforms, decentralized marketplaces distribute control across multiple participants, reducing dependency on any single entity and enhancing data sovereignty for users. They enable peer-to-peer transactions, leveraging smart contracts for automated, secure,

Funded by the European Union

and transparent data exchanges. These platforms are not confined to one specific industry but span across various sectors, each with its unique requirements and data types. This flexibility and security make decentralized data marketplaces a cornerstone in the emerging data economy, offering innovative solutions for data sharing and monetization.

6.1. DECENTRALIZED DATA MARKETPLACES - DEFINITION AND BUSINESS MODELS

Based on literature (Spiekermann, 2019; Koutroumpis, Leiponen, & Llewellyn, 2020; Fricker & Maksimov, 2017), a data market can be understood as a digital platform on which data products are traded. Such a platform may be owned and operated by a company or organization, which participates in the platform as the sole provider or purchaser of the data. On the other hand, such a platform can act as a neutral intermediary and allow third parties to trade (sell or buy) data products. The study (Stahl, Schomm, Vossen, & Vomfell, 2016) introduces a framework for classifying the business models generally followed in electronic platforms and by extension in data trading platforms. This framework consists of three dimensions: orientation, ownership and business model.

Six types of business models can be distinguished: buy-side system, sell-side system, buy-side platform, consortium platform, sell-side platform and two-sided marketplace.

Each of these models represents a unique approach to facilitating trade on decentralized data marketplaces, with varying degrees of control, openness, and participation from different stakeholders. Examples of data trading platforms adopting these business models include IOTA, Caruso, Ocean Protocol, and INRIX

6.2. ORIENTATION AND OWNERSHIP MODELS

Decentralized data marketplaces can be categorized based on their ownership models, which are crucial in determining how the platforms are operated and governed. The ownership models are primarily divided into three types (Manzano Kharman et al., 2022):

- Private Ownership: In this model, a single company or organization owns the platform. They may participate as the sole provider or purchaser of the data. This ownership model often leads to a more controlled environment where the owner has significant influence over the platform's operations and the data traded within it.

- Consortium Ownership: This model involves a small group of companies or organizations co-owning the platform. These entities can be either buyers or sellers. Consortium ownership is typically seen in platforms where stakeholders from a specific industry or sector come together to create a shared data trading environment. This model allows for a more collaborative approach to managing the platform and its data.
- Independent Ownership: In this model, the owner of the platform is independent and has no direct involvement as a buyer or seller in the transactions that occur on the platform. This type of ownership ensures neutrality and fairness, as the owner does not have vested interests in the trading activities. Independent platforms often act as neutral intermediaries, facilitating transactions between third parties.

Each of these ownership models has its own implications for the way data is managed, accessed, and controlled within the marketplace. The choice of model can impact the level of control users have over their data, the transparency of transactions, and the overall trustworthiness of the platform.

6.3. SECTOR-SPECIFIC AND GENERAL-PURPOSE PLATFORMS

Some of the existing platforms focus on trading and trading general-purpose datasets (e.g., AWS Data Exchange, Dawex, and DataRade), while others focus on trading data that is exploitable by specific industries (e.g., Otonomo, Caruso, Wibson).

Also, there are several platforms that simply focus on indexing publicly available datasets (e.g. Google Cloud DM, Azure Data Catalog, Advaneo, Data Intelligence Hub). A very small number of the platforms studied (<10) use data encryption or distributed ledger technologies Ledger Technologies - DLT, such as Blockchain, to store information about data exchanges (e.g. IOTA, Airbloc, Wibson , Meeco). Only 4 of these platforms, Datum, AMO, BurstIQ and Dataeum, store the actual data sets in Blockchain. An interesting case is BurstIQ , which adopts Blockchain technology to store health data shared between health organizations and health professionals. It is worth noting that some of these platforms, such as Datum, failed due to the high cost of processing the data stored on the Blockchain. So, the long-term viability of these architectures that store data on-chain is questionable.

Data trading platforms can provide both static data and (dynamic) data streams and allow access through various types of access, such as individual file downloads, APIs, custom web interfaces or specialized applications. As such, these platforms provide standardized licensing models, as well as regulations on data access and use. The format of the data exchanged on these platforms varies. Primarily, they exchange:

- Sensor and mobility data, i.e. data collected from IoT sensors
- Geographical data, i.e. data related to a specific location on Earth.
- Personal data and health data, i.e. data about patients or personal data
- Financial and alternative data, i.e. data that provides information about a company's financial situation
- Audience data, i.e. data derived from the interaction of users (i.e. the "audience") with online advertisements or from the online purchase of products.

6.4. INDUSTRY SECTORS

In the realm of decentralized data marketplaces, platforms can be broadly categorized based on the types of data they trade and the industry sectors they serve. Some platforms are geared towards general-purpose datasets, such as AWS Data Exchange, Dawex, and DataRade. These platforms cater to a wide range of industries and data needs, offering a diverse array of datasets for various applications.

On the other hand, there are platforms that specialize in trading data specific to certain industries. This includes platforms like Otonomo, Caruso, and Wibson, which focus on industry-specific data that is highly relevant and tailored to the needs of particular sectors. The key industry sectors where these data markets are active encompass (Sterk, Peukert, Hunke, & Weinhardt, 2022):

- Industry: This sector includes data relevant to manufacturing, production, and industrial services, where data analytics can play a significant role in optimizing processes, monitoring equipment, and enhancing efficiency.
- Health: In this sector, data marketplaces deal with healthcare-related data, including patient records, treatment outcomes, and pharmaceutical research. This data is vital for advancing medical research, improving patient care, and developing new healthcare solutions.
- Automotive: Automotive data marketplaces focus on data related to vehicles, traffic, and transportation services. This data is crucial for improving vehicle design, enhancing traffic management systems, and developing new mobility solutions.
- Financial: The financial sector benefits from data marketplaces by accessing data related to markets, banking transactions, and economic trends. This data is essential for financial analysis, risk assessment, and developing financial products.

- Energy: In the energy sector, data marketplaces provide data on energy consumption, distribution, and renewable energy sources. This data is key to managing energy resources effectively and promoting sustainable energy solutions .

- Georgia: This sector might refer to geographical data, which includes information about locations, demographics, and environmental conditions. This data is used in mapping, urban planning, and environmental monitoring.

- Public Administration: Here, data marketplaces offer data related to government operations, public services, and civic engagement. This data is instrumental in improving public services, policymaking, and fostering transparency in governance.

6.5. DATA TRADING PLATFORMS - PLATFORM CHARACTERISTICS

Data trading platforms, pivotal in the landscape of decentralized data marketplaces, have distinct characteristics that play a crucial role in their operation and appeal. These platforms can handle both static data and dynamic data streams, offering various access types such as individual file downloads, APIs, custom web interfaces, or specialized applications. They also provide standardized licensing models and adhere to specific regulations on data access and use, ensuring a structured and secure environment for data exchange. The key attributes of these platforms include:

- Value Proposition: Data trading platforms emphasize easy access to high-quality data, along with tools for data analysis, synthesis, and visualization. This makes data not just available, but actionable for users across industries like agriculture, health, and automotive (Denodo, 2023; Sterk et al., 2022).

- Data-Centric Nature: Platforms go beyond simple data transactions and offer services like data normalization, aggregation, and enrichment. This increases the value of the data by making it more usable for various analyses (Sterk et al., 2022; Nguyen et al., 2018).

- Ownership Models: Platforms can be privately owned, operated by a consortium, or independent. Federated platforms, which allow for cross-platform data interaction, are often based on consortium or independent models (Edemekong et al., 2024; Rahman et al., 2023).

- Platform Architecture: Depending on the platform's goals, architecture may be centralized, decentralized, or hybrid. Centralized platforms offer easier control over data access and processing, while decentralized ones focus on preserving data sovereignty (Rahman et al., 2023; Nguyen et al., 2018).

Funded by the European Union

- Market Access: Data platforms can be open (allowing broad participation), closed (restricted to select partners), or hybrid, balancing openness with quality control (Sterk et al., 2022; Rahman et al., 2023).
- Business Models: Platforms support diverse models such as B2B, C2B, and others, with pricing strategies that include freemium, subscription, pay-per-use, and tiered models (Nguyen et al., 2018; Denodo, 2023).
- Currency and Consent Mechanisms: Transactions may involve fiat or cryptocurrency, with varying consent mechanisms like Proof of Work (PoW), Proof of Stake (PoS), and others (Edemekong et al., 2024; Sterk et al., 2022).

6.6. GENERAL PURPOSE DATA MARKETS

General purpose data markets, such as DAWEX and AWS Data Exchange, are digital platforms for trading a wide range of datasets across various industries. These platforms can act as neutral intermediaries, allowing third parties to sell or buy data products. DAWEX, for instance, facilitates transactions between businesses in multiple sectors, including automotive, smart city & IoT, health, finance, energy, transport, and insurance. It supports diverse data formats and acts as a trusted broker using Ethereum Blockchain for transactions and smart contract management, ensuring data integrity and authenticity.

DAWEX

Aiming to transact/exchange, share and exploit datasets between businesses in a safe and easy-to-use manner and with a global turnover, the Dawex market is aimed at a multitude of businesses of independent size and industry, e.g. automotive, smart city & IoT, health, finance, energy, transport, insurance, retail. As an open market it supports any data formats such as files, APIs, raw or rich data. Acts as a trusted neutral broker for transactions between buyers and data providers adopting the Ethereum Blockchain on the one hand for the direct matching of buyers/providers with sellers, on the other hand for the management of the smart contracts concluded between them, thus making it possible to verify the integrity and authenticity of the data (Dawex, 2022; Bounie & Quinn, 2018).

OCEAN PROTOCOL

The Ocean Protocol is a decentralized data exchange protocol and network that incentivizes the sharing of data for use by Artificial Intelligence (AI) applications. The Ocean Protocol is based on Blockchain technology and facilitates the storage, distribution and consumption of digital data goods (data assets) and data services in a

Funded by the European Union

secure, transparent, traceable and reliable way, while ensuring full control of data sets by their providers. This is achieved with "Service Performance Agreements" (Service Execution Agreements - SEA), which are a version of smart contracts that run on the Ethereum public network (Ethereum main net) (Ocean Protocol Foundation, 2023).

ADVANEO

The primary goal for ADVANEO, and by extension for the software company of the same name, which is based in Germany and has taken over its management and operation, is the development of solutions that ensure the ownership of data sovereignty) to their owners. This platform creates a marketplace that allows trading, processing and analysis of datasets (Azkan, Iggena, Krotova, Spiekerman, & Otto, 2021). It also supports scalable solutions for data-driven business models and artificial intelligence applications aimed at the digital transformation of enterprises. To meet these requirements, the datasets are continuously updated and updated. Focused on promoting innovative solutions across different business sectors, this approach handles every data set format. Two formats of these datasets are distinguished, the open and the commercial type. The latter are available as metadata for purchase and sale. For their quick retrieval, data can be categorized (IoT data, environmental data, industrial production data, etc.). In addition to trading, the marketplace hosts a large number of datasets that are open source and freely available.

OriginTrail

OriginTrail is a decentralized open peer-to-peer platform that indexes knowledge 30(processed data with semantic information) and facilitates access to it (Rakic, Levak, Drev, Savic, & Veljkovic, 2017). This platform integrates Blockchain technology with digital supply chains to provide data integrity. The basic idea is to ensure product standards and consumer safety using a standard Blockchain-based solution through an incentivized protocol. OriginTrail addresses two key factors disrupting data collection and sharing across supply chains: a) Data fragmentation—Different data storage structures across the supply chain led to data silos and poor data interoperability across both single and multiple supply chains. b) Data Aggregation—Most of the existing supply chains rely on a trusted intermediary or central authority that provides information about product authentication and origin.

Funded by the European Union

7. SPECIAL PURPOSE DATA MARKETPLACES

In this section follows an analysis of special purpose platforms, i.e. platforms that trade/trade data for specific industry sectors and/or data formats. Some of them enable the exchange/trading of data for multiple IoT industry sectors, while some focus on data that can be leveraged by actors/companies operating in specific sectors. For example, the Otonomo and Caruso platforms are active in trading vehicle data to B2B service providers as well as the automotive aftermarket, focusing mainly on auto parts and component manufacturers, insurance companies and vehicle repair shops (Otonomo & Xouba, 2023.); (Caruso, 2024).

AUTONOMOUS

It is a cloud computing provider that has platform services. It was founded in 2015 as a start - up company in Israel by Ben Volkow and Avner Coher , with the aim of creating an interconnected service ecosystem to the commercial partners of the automotive industry on a cloud computing platform computing). The object of transactions for the participants is the vehicle/car data either in near real time or by recalling historical records (Bounie & Quinn, 2018).

CARUSO

Caruso platform is funded by TecAlliance , which provides the automotive industry with vehicle-related data. In addition to TecAlliance , shareholders of the Caruso platform are also some multinational companies such as Bosch and Continental. This is a closed data platform where only consortium members and partners are allowed to trade. The neutrality of the platform is guaranteed by the participation of a broad group, more than 20 shareholders, from the automotive industry. It is a data-centric trading platform, which is the "broker" between multiple players, just like the ADVANEO and Data Intelligence platforms Hub. The Caruso platform enables the harmonization and enrichment of on-vehicle data (e.g. brakes, battery, engine, front wheel, distance travelled, speed, etc.), their trading, and access to them, while providing advisory services to the conclusion contracts, invoicing, costing to the users of the platform. Therefore, the platform can be used to serve multiple purposes, such as car sharing through appropriate applications, offering personalized car insurance contracts from insurance companies based on the driver's driving profile, etc. In addition, a software development portal is offered (Developer portal), with the aim of facilitating on a technical level the access of business customers' systems to data on said platform, even if they have limited technological resources or human resources. This software solution provides the following additional features: an access interface (API) to the data through the platform, communication with the catalog of data by thematic content, as well as the subscription process and error handling.

IOTA

The IOTA platform is a purpose-built platform for data transactions and micropayments (less than £0.01) between IoT devices using cryptocurrencies. IOTA adopts distributed ledger technology (DLT) specially designed for IoT device communication called Tangle. MIOTA is the cryptocurrency used for transactions on the platform. Based on an open source (open source) protocol, the platform aims to facilitate machine-to-machine communication and establish it as a service of the economy of things, without the need for human intervention (IOTA, 2023).

STREAMR

Streamr, a decentralized publish - subscribe system for IoT data transactions that supports the scalability of IoT systems in near real-time while ensuring confidentiality of the data powering blockchain-based decentralized applications (DApps) (Streamr, 2017). Network-level communication between nodes is conducted through Blockchain 's peer-to-peer P2P network thus meeting the implementation's needs for fault tolerance, easy scalability, and decentralization.

DATABROKER GLOBAL

The Databroker Global (formerly Databroker DAO) platform which in its early stages was self-described as the "eBay" for trading real-time IoT sensor measurements has now evolved into a "Platform as a Service" (PaaS) which is not strictly connected to the buying and selling of IoT sensor data but refers to data formats of a wide variety of devices such as for example autonomous vehicles with integrated sensors, cameras, lights, security systems, etc (Databroker Global, 2020).

7.1. PERSONAL DATA MARKETS

WIBSON

The Wibson platform is active in the personal data market (Van de Ven, Abbas, Kwee, & de Reuver, 2021). It is based on Blockchain technology and provides the infrastructure of a distributed data marketplace for the secure and anonymous buying and selling of private information and data, which is checked for validity. It solves the problem of controlling personal data, at the same time giving financial incentives for their exchange (Fernandez, Futoransky, Ajzenman, Travizano, & Sarraute, 2020). It is built on a set of core principles: transparency, anonymity, fairness, resistance to censorship and the individual's absolute control over the use of their personal information. It adopts a one-to-one matching mechanism where Wibson acts as a neutral intermediary providing the Blockchain infrastructure for data exchange. Users install a smartphone app and can share some personal data, such as their Facebook account and mobile device location, and sell the data in exchange for Wibson tokens (Fernandez et al., 2020.

AIRBLOC

Airbloc is a distributed ad data marketplace where users have the opportunity to earn money by offering their personal data to advertisers who intend to leverage that data to run targeted marketing campaigns. Airbloc's platform is distributed and based on Blockchain technology for the real-time exchange of data in a transparent manner between data owners, providers and consumers. Examples of personal data exchanged on the Airbloc marketplace include email addresses, phone numbers, names, ages, home addresses, location data, IP addresses, mobile advertising identifiers, a device's installed list of apps, device app usage history, and even behavioral data such as personal interests and preferences, etc(Airbloc, 2023).

MEECO

The MEECO platform establishes a personal data marketplace that allows users to add, organize, edit and share their personal data. MEECO provides access, control, representation and consent from the perspective of each user, enabling users (data subjects) to provide their own verified records and controlled consent (Meeco, 2023).

7.2. FEDERATED DATA MARKETS

This section discusses platforms that create federated IoT data markets, i.e. markets that combine data from multiple IoT platforms (members of the federation) and are exchanged within a common market.

GAIA-X

The GAIA-X research project provides a European data infrastructure for the development of innovative, reliable and sustainable digital economies, based on standards and open-source software. GAIA-X provides a federated platform that can bring together multiple cloud service providers and data owners in a user-friendly ecosystem that ensures reliable data exchange and the creation of new common data spaces (GAIA-X, 2021). The vision of GAIA-X is the exchange of data and services, implementing policies that ensure the preservation of ownership of them. The core architectural principles of GAIA-X include transparency, interoperability, federation, authenticity, and trust. The following technical features enforce these principles and ensure compliance with the GAIA-X vision

FIWARE

The FIWARE platform is a software platform based on open-source standards. The main mission of the FIWARE platform is to develop an open sustainable ecosystem that encourages the adoption of open standards for the collection, access, management and exchange of data from IoT devices or other sources. The FIWARE

Funded by the European Union

platform provides tools and software to develop smart applications that leverage data to make smart decisions in various industry sectors such as smart cities, smart energy, smart agriculture and smart industry.

FIESTA IoT

FIESTA-IoT was a research project that was active between the years 2015 and 2018. The FIESTA project worked to integrate IoT platforms, experimental infrastructures and applications that would otherwise remain in silos. The FIESTA platform allowed its users to run experiments on multiple federated IoT experimental infrastructures in a seamless manner by creating a large-scale virtual infrastructure. The main goal of the FIESTA project was to open new horizons for the development and deployment of IoT applications and experiments at the European and global level, enabling the interconnection and interoperability of different IoT platforms. The Fiesta-IoT platform infrastructure spans several existing IoT facilities located in Ireland, the United Kingdom, Spain, France, Italy, Greece and Korea (Nguyen, Serrano, Gyrard, & Tragos, 2018).

DENODO

Today's data management landscape is becoming increasingly complex, as data is spread across many heterogeneous data systems (data warehouses, columnar databases, specialized data stores, cloud applications, etc.) that may reside in multiple locations. This makes it difficult to offer a single view of data across business applications and ensure that policies and governance rules are applied across the entire data supply chain. The Logical Data Web is the vision of a unified data delivery platform that removes access to multiple data systems for business consumers, hiding complexity and exposing data in business-friendly formats, while guaranteeing data delivery according to predefined rules semantic and governance. Data Virtualization is the key technology to achieve the vision of the Logical Data Web. As one of the key data integration solutions designed for distributed architectures, data virtualization provides a logical level of data access across multiple heterogeneous systems in hybrid, distributed architectures. Today, the data management ecosystem is distributed in nature, so a logical layer of data access, such as data visualization, is most appropriate (Denodo Technologies, n.d.).

8. PRIVACY-AWARE DATA PROCESSING (FEDERATED LEARNING AND PRIVACY ENHANCING TECHS)

Privacy-aware data processing, incorporating technologies like Federated Learning and Privacy Enhancing Technologies (PETs) (Information Commissioner's Office, 2023), is an emerging concept in data management that prioritizes user privacy while still enabling the valuable analysis and utilization of data (Wang, Zhang, Feng & Yang, 2020).

Data protection law does not define PETs. The concept covers many different technologies and techniques. The European Union Agency for Cybersecurity (ENISA) refers to PETs as: *'Software and hardware solutions, i.e. systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons.'*

PETs are linked to the concept of 'data protection by design' and are therefore relevant to the technical and organisational measures you put in place. They can help you implement the data protection principles effectively and integrate necessary safeguards into your processing.

PETs can help reduce the risk to people, while enabling you to further analyse the personal information. The ability to share, link and analyse personal information in this way can give you valuable insights while ensuring you comply with the data protection principles. These are methods and tools designed to protect personal information from being disclosed without compromising the functionality of the system. PETs include techniques like data anonymization, encryption, and differential privacy. They enable data to be used and shared without revealing sensitive information, thus maintaining confidentiality and compliance with data protection regulations.

Some of these techniques have already been mentioned during this report:

- Federated Learning: This is a machine learning approach where the model is trained across multiple decentralized devices or servers holding local data samples, without exchanging them. This method ensures that sensitive data remains on the user's device, enhancing privacy and security. It's particularly useful in scenarios where data privacy is crucial, such as in healthcare or finance.
- Homomorphic Encryption: Enables computations on encrypted data without decrypting it, maintaining data privacy even during analysis. This is particularly useful in scenarios where sensitive data needs to be processed without revealing it (Acar, Aksu, Selcuk, & Conti, 2019).
- Secure Multi-Party Computation (SMPC): Facilitates joint computation on private inputs from multiple parties without revealing those inputs. SMPC is

valuable in situations where different entities need to collaborate without directly sharing sensitive data (Zhao, Zhao, Zhao, Chen, Gao, Li, & Tan, 2019).

- Zero-Knowledge Proofs (ZKP): Allows one party to prove the truth of a statement to another without revealing any additional information. ZKP is crucial in applications requiring verification without compromising data privacy.

- Synthetic Data: Involves generating artificial data that mimics real data sets, protecting sensitive information. It's particularly useful for testing and model development when using real data presents privacy risks.

- Trusted Execution Environments: Provide secure areas in processors to run code and process data in isolation, protecting data integrity and confidentiality.

- Differential Privacy: Adds noise to statistical data, making it difficult to identify individuals within data sets, essential for maintaining privacy in large databases.

The combination of Federated Learning and PETs represents a significant shift towards more privacy-centric data handling. It allows for the collection and analysis of data insights while minimizing the risk of privacy breaches. This approach is particularly relevant in the current digital landscape, where data privacy concerns are increasingly paramount.

There are two types of PETs that organizations can use:

PETs that provide **input privacy** can significantly reduce the number of parties with access to personal information you are processing. Input privacy means that the party carrying out the processing cannot:

- access the personal information you are processing;

- access intermediate values or statistical results during processing (unless the value has been specifically selected for sharing); or

- derive inputs by using techniques such as side-channel attacks that use observable changes during processing (eg query timings or power usage) to obtain the input.

PETs that provide **output privacy** reduce the risk that people can obtain or infer personal information from the result of a processing activity. Output privacy measures and controls reduce the risk that personal information can be obtained or inferred from the result of a processing activity. This is regardless of whether the computation itself provides input privacy. Using a PET that provides output privacy is useful if you plan to:

- Make anonymous statistics publicly available; or

- Share the results of an analysis with a large group of recipients.

9. CROSS-BORDER DATA TRANSFER TECHNOLOGIES

Lately, fears that foreign governments might (mis-)use their sovereign powers to obtain illegal or disproportionate access to personal data normally protected under GDPR have been proven to be more than mere conjecture by conspiracy theorists. This, in turn, has clearly demonstrated the need to further strengthen the GDPR's inherent mechanisms aimed at protecting personal data when such data leave the European Economic Area. Only when such protection transcends mere paperwork, can real assurance be offered to data subjects that their rights under the GDPR are truly upheld in case of transfers to third countries. Under impulse of active supervisory authorities and a courageous European Union Court of Justice, the EU has shown its clear intent these past few years to have the GDPR's principles enforced even at the international level.

Generally speaking, the GDPR provides three different mechanisms for transferring personal data in a structural manner:

1. Adequacy decisions of the European Commission whereby the European Commission assesses the adequacy of the level of protection for personal data in a particular third country.
2. Contractual mechanisms such as the Standard Contractual Clauses proposed by the European Commission.
3. Unilateral mechanisms such as the Binding Corporate Rules whereby controllers or processors can unilaterally determine in a sort of internal rulebook how they will transfer personal data in a manner that complies with the GDPR.

While all of these mechanisms have their merits, certainly, the CJEU's Schrems II judgement has shown that they in themselves may not always be enough. Indeed, an adequacy decision may become outdated in case of a regime change in the third country benefiting from such a decision. At the same time, governments are typically not bound by a contract concluded between two companies, let alone a unilateral declaration made by a single company. Hence, all of these mechanisms require something additionally in order to be truly effective against foreign government intrusion, something more tangible and real.

The European Data Protection Board has drafted Recommendations on measures which could supplement the aforementioned mechanisms. These measures are of a technical, organisational or contractual nature. The proposed technical measures show that blockchain solutions can play a real added value, because they include things like strong encryption, transfer of pseudonymized data only and split or multi-party processing. At the same time, blockchain technologies might just as well do the opposite (as is probably true for any technology). Indeed, the technology itself may lead to potentially unlimited cross-border transfers across the globe, particularly in globally distributed blockchain networks.

When implemented well, however, blockchain technology can ensure that during cross-border transfer of personal data such data is immutable when recorded on the blockchain and only accessible to authorized parties having the right credentials to access specific data. This prevents unauthorized third country governments from accessing the personal data recorded on the blockchain.

In the context of cross-border data transfer technologies, the Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems developed by the Asia-Pacific Economic Cooperation (APEC) play a critical role (Perrigo, 2018). These systems serve as mechanisms for operationalizing privacy principles in accordance with the APEC Privacy Framework. They interact with domestic privacy laws, providing a framework for businesses to achieve compliance while engaging in international data transfer.

Furthermore, there is potential for interoperability between CBPR and EU mechanisms like Binding Corporate Rules (BCR) and GDPR certifications. This indicates a move towards a more unified global approach to data privacy and transfer regulations. The adoption of CBPR and PRP by businesses can facilitate compliance with diverse privacy laws and streamline cross-border data transfers, enhancing the efficiency and legal security of international operations.[io]

[1] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries, *OJ L* 199, 7 June 2021, p. 31–61.

[2] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 18 June 2021, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu).

10. DATA CERTIFICATION/VERIFICATION METHODS SHOULD BE DEVELOPED TO VERIFY THE TRUSTWORTHINESS OF THE DATA

Funded by the European Union

Data certification and verification methods are crucial for ensuring the trustworthiness of data in various applications, especially in decentralized systems where data sources are numerous and varied. The development of these methods is aimed at validating the authenticity, accuracy, and integrity of data. Here are some key aspects:

- Data Provenance Tracking: This involves recording the history of the data, including where it came from, who has handled it, and how it has been modified. This traceability helps in verifying the data's origin and its journey, ensuring its authenticity.
- Data Quality Metrics: Establishing metrics for assessing data quality is essential. These metrics could include accuracy, completeness, consistency, and reliability. By measuring these aspects, one can determine the trustworthiness of the data.
- Cryptographic Techniques: The use of cryptographic methods such as digital signatures and hash functions can verify that the data has not been tampered with. A digital signature ensures that the data comes from a verified source, while hash functions can detect any alterations made to the data.
- Third-Party Auditing: Involving independent third-party auditors can provide an additional layer of trust. These auditors can verify the data's integrity and the processes used to handle and store the data.
- Blockchain Technology: Blockchain can be used for data certification and verification. Its decentralized and immutable ledger ensures that once data is recorded, it cannot be altered retroactively. This feature is particularly useful for maintaining a transparent and tamper-proof record of data transactions (Ali, Norman, & Azzuhri, 2023).
- Machine Learning for Anomaly Detection: Advanced machine learning algorithms can be employed to detect anomalies and patterns that indicate data manipulation or fraud.
- Compliance with Standards and Regulations: Adhering to established data management standards and regulations (like GDPR, HIPAA, etc.) can further ensure the data's trustworthiness.

11. DATA IDENTIFICATION, DATA PROVENANCE, DATA TRACKING MECHANISMS

Data management in technology has evolved significantly with new technologies, impacting aspects like data identification, integrity, and traceability. The advancement in areas such as blockchain, AI, and IoT has revolutionized how data is identified, stored, and tracked (Shifa, 2019).

Funded by the European Union

The advent of AI and machine learning has enhanced the ability to identify and categorize data more accurately and efficiently. These technologies can process vast amounts of data, recognizing patterns and anomalies that might be missed by human analysis.

Blockchain technology, combined with IoT for data traceability (Sigwart, Borkowski, Peise, Schulte, & Tai, 2019), revolutionizes the security and transparency of data management. Its decentralized, tamper-proof nature, paired with IoT's extensive data collection capabilities, forms a powerful system for data tracking and verification. This integration is especially valuable in sectors like supply chain management and healthcare, where data authenticity, history, and real-time monitoring are critical. Leveraging blockchain in IoT environments enhances data provenance, reliability, and security, making it a key solution for complex systems requiring accurate and transparent data tracking.

The importance of **data identification** in technological contexts stems from the need to accurately recognize, categorize, and manage data in increasingly complex digital environments. Efficient data identification methods are vital for ensuring data integrity, security, and usability (Sigwart et al., 2019). These methods involve various technologies and approaches, such as metadata tagging, data fingerprinting, and AI-driven data classification systems. In sectors ranging from healthcare to finance, effective data identification is crucial for operational efficiency, compliance with regulations, and informed decision-making. Understanding and implementing advanced data identification techniques is key in leveraging the full potential of digital data assets.

The latest tools and technologies in data categorization and recognition include advanced machine learning algorithms, natural language processing (NLP), and AI-driven classification systems. These technologies enable more accurate and efficient data sorting, even in large datasets. Machine learning algorithms, for instance, can identify patterns and categorize data based on learned criteria. NLP is particularly useful in processing and categorizing unstructured textual data, while AI-driven systems offer adaptive and sophisticated ways to handle diverse data types, enhancing accuracy and efficiency in data management.

Tracking the origin and history of data, known as **data provenance**, is crucial in modern data management. It involves understanding where data comes from, how it has been processed or altered over time, and who has interacted with it. This knowledge is essential for ensuring data integrity, verifying authenticity, and maintaining compliance with regulatory standards. In fields like healthcare, finance, and scientific research, data provenance is vital for making accurate decisions, ensuring transparency, and building trust in data-driven systems. It also plays a key role in security and privacy, helping to trace the source of data breaches or unauthorized access.

Blockchain technology plays a pivotal role in ensuring data provenance, particularly in complex systems like supply chains or healthcare. Its decentralized and immutable ledger provides a transparent and tamper-proof record of data transactions, making it ideal for tracking the origin, movement, and changes of data. In supply chains, blockchain can trace the journey of a product from manufacturer to consumer, ensuring authenticity and compliance. In healthcare, it helps maintain the integrity of patient data and medical records, crucial for treatment and research. Other technologies like digital signatures and cryptographic hashing also contribute to securing data provenance.

Various mechanisms and technologies for **tracking data** include IoT and AI. IoT devices collect vast amounts of real-time data from their environment, providing invaluable insights for various applications. AI, on the other hand, plays a crucial role in analyzing this data, identifying patterns, and making predictive decisions. These technologies together enable efficient data tracking in areas such as environmental monitoring, smart homes, and industrial automation, leading to more informed decision-making and enhanced operational efficiency.

IoT and AI technologies facilitate real-time monitoring and data management across various sectors. In healthcare, they enable constant health monitoring and patient data analysis, enhancing care delivery. In manufacturing, IoT devices track production processes, while AI analyzes this data for efficiency improvements. In agriculture, these technologies monitor crop and soil conditions, aiding in precision farming. The real-time insights provided by IoT and AI are transforming sectors by enabling proactive decision-making and optimizing operations.

- **NetObjex** has introduced a smart parking solution using the blockchain IoT. This platform helps you find out a vacant place in the parking space and automates the process of making payments using crypto wallets (NetObjex, n.d.).
- **Golden State Foods (GSF)** is a renowned manufacturer of food products working in collaboration with IBM to improve its business processes by making use of blockchain IoT. GSF has created a transparent ledger system that is accessible to stakeholders in real-time (Golden State Foods, n.d.).
- **Telstra** a telecommunication and media company provide blockchain IoT enabled smart home solutions that allow our home security systems to be easily managed using a remote control (Telstra, n.d.).

Hyundai is a Korean company that is using blockchain IoT for their startup brand HDAC (Hyundai Digital Asset Currency), which is building its own private blockchain designed specifically for IoT.

Filament a business startup using a chip designed to enable industrial IoT devices to work with multiple blockchain technologies. The chip provides a secure platform for decentralized interaction.

The innovative applications of blockchain IoT in various industries hold significant potential for transformation. They are reshaping sectors by improving operational efficiency, enhancing transparency, and offering better user experiences. For example, smart parking solutions streamline the parking process, food industry transparency improves supply chain management, and smart home solutions increase convenience and security. The future potential of these technologies lies in their ability to further integrate into daily operations, offering more automated, secure, and efficient systems. This integration is expected to continue evolving, driving innovation and new opportunities across industries.

Implementing blockchain IoT solutions faces several challenges and limitations. Scalability is a major concern, as blockchain networks must handle large volumes of IoT data efficiently. Security is another critical issue, especially in protecting sensitive data against cyber threats. Additionally, integrating blockchain IoT with existing systems poses technical challenges, requiring significant investment and expertise. These factors must be addressed to fully realize the potential of blockchain IoT technologies in various industries.

12. CHALLENGES AND LIMITATIONS: FUTURE TRENDS AND INNOVATION POTENTIAL

Successful companies are fostering a learning culture where continuous skill development is not only encouraged but expected. This involves budgeting time and resources for employees to experiment with new tools and technologies and creating environments where learning from mistakes is part of the process. Companies are also adopting practices like automated testing and isolation zones in cloud environments to minimize the impact of mistakes, particularly those that could lead to significant issues like data loss or misuse.

The role of IT is evolving from a controlling entity to an enabler of innovation, focusing on providing small, interoperable blocks of code that can be easily integrated. This shift is supported by the rapid growth of cloud microservices, APIs, and Software as a Service (SaaS). The market for cloud microservices is expected to grow significantly, and the use of APIs and SaaS is becoming more prevalent. This trend highlights the move towards more modular, flexible, and user-friendly IT solutions that can support rapid innovation and adaptation (Chui, Issler, Roberts, & Lareina Yee, 2023).

As technology becomes more pervasive, tech literacy is increasingly essential for all roles. This necessitates continuous learning and the development of individual skills relevant to specific needs. Companies are moving towards a culture of perpetual learning, where all levels of personnel, from 'citizen developers' to full-stack engineers, are encouraged to continuously update their skills. Learning is integrated into workflows, with an emphasis on acquiring and applying skills as needed. For instance,

Funded by the European Union

Netflix exemplifies this approach by embedding data scientists directly with product and engineering teams for continual learning and experimentation.

Artificial intelligence (AI) is considered one of today's most disruptive technologies. It is expected to have a significant impact on a wide range of industries and sectors. AI has the potential to transform the way we live and work by automating and optimising tasks, processes and decisions. It is also driving advances in fields such as health, education, energy, transport and security. However, it also presents challenges, such as the need to address ethical issues, managing change in employment and adapting existing regulations to new technological realities.

One of the pivotal issues in the AI domain is the challenge of algorithmic and gender bias. These biases can lead to unequal outcomes in various applications, potentially reinforcing existing social inequalities. TrustChain aims to tackle these issues head-on by integrating measures that ensure fairness and equity in AI algorithms. The project will focus on developing AI systems that are transparent, accountable, and free from discriminatory biases.

AI is transforming job roles and the skills required. While some jobs may be replaced, new opportunities are also being created. Training and skills development are essential to adapt to these changes. The TrustChain project acknowledges the importance of reskilling and upskilling, ensuring that workers are prepared for the evolving job market influenced by AI.

The ethical and social implications of AI, such as privacy, security, and fairness, require careful regulation and policymaking. TrustChain is committed to responsible AI development, ensuring that AI advancements do not compromise individual privacy or security.

In industries like healthcare, education, agriculture, manufacturing, and transportation, AI is enhancing efficiency, personalization, and new product development. TrustChain will explore these improvements while ensuring ethical AI applications.

The integration of AI with other technologies like robotics, autonomous vehicles, and quantum computing opens avenues for innovative applications and disruptive change. TrustChain will monitor these advancements to understand their impact better and leverage them for sustainable and ethical development.

Global collaboration and regulation are essential to address AI's cross-border impacts. TrustChain supports international efforts to create consistent regulatory frameworks to manage the global reach of AI effectively.

13. NEXT STEPS IN TRUSTCHAIN

Funded by the European Union

The next open calls represent significant steps in the TrustChain project's commitment to advancing blockchain technology in a way that is not only innovative but also sustainable and respectful of privacy and democratic values.

Open Call #4 - "Multi Chains Support for NGI Protocols": This call is focused on designing and building gateways to enable the transfer of knowledge, metadata, data, and processes from one chain to another in a secure and trustworthy manner. A key aspect of this call is interoperability across multiple chains, which is vital for facilitating data and asset exchange between different blockchain networks. The outcomes of this call will integrate with the results from previous calls, especially Open Call #2 and #3, to enhance user privacy, data governance, and subsequently, data economics and democracy.

Open Call #5 - "Green Scalable and Sustainable DLTs": This call aims to build upon the achievements of the first four Open Calls. Its primary objective is to utilize digital identities, trustworthy data, and novel mechanisms designed in previous calls to achieve high energy efficiency and optimization of Distributed Ledger Technologies (DLTs). The call will explore the balance between technology usage, security of consensus protocols, and the sustainability and energy efficiency requirements. It is an effort towards making DLTs more environmentally friendly and sustainable.

14. RECOMMENDATIONS AND CONCLUSION

Given the diverse applications of blockchain technology highlighted in the report, future reports could focus more on specific use cases, especially in sectors like healthcare, finance, and supply chain management, where blockchain has shown significant potential. The TrustChain project’s next steps should concentrate on developing standards and protocols to enhance interoperability among various blockchain systems. This would enable more efficient cross-chain transactions and data transfers, crucial for scalability and the broader adoption of blockchain solutions.

As blockchain technology evolves, addressing new privacy and security challenges will be imperative. This includes staying updated with regulatory changes and ensuring blockchain applications comply with global data protection laws. Considering Open Call #5's focus on "Green, Scalable, and Sustainable DLTs", the research and development of energy-efficient blockchain technologies will be a priority. Such initiatives will support the sustainable expansion of blockchain ecosystems, aligning with the European Agenda 2030's environmental goals.

Trustchain is committed to researching and developing robust data governance frameworks compatible with blockchain technologies, exploring innovative methods of data certification and verification to guarantee data integrity and reliability.

Continual collaboration and knowledge sharing are crucial for achieving the project's goals. Therefore, teams are encouraged to adopt a collaborative mindset, engaging with various stakeholders, including academia, industry, and regulators. This approach will facilitate knowledge exchange and spur innovation, particularly in blockchain applications.

The project must stay updated on the latest advancements in blockchain, privacy, digital identity, regulation, and related fields. This involves monitoring the progress of emerging technologies such as artificial intelligence (AI), federated learning, and privacy-enhancing technologies (PETs), and assessing their potential integration with blockchain.

REFERENCES

Aadhaar. (n.d.). National biometric ID system. Unique Identification Authority of India. https://uidai.gov.in/en/

Acar, A., Aksu, H., Selcuk Uluagac, A. & Conti, M. (2019). *A Survey on Homomorphic Encryption Schemes: Theory and Implementation*. ACM Comput. Surv. 51, 4. https://doi.org/10.1145/3214303

Accenture (2018). *DHL and Accenture Unlock the Power of Blockchain in Logistics.* https://newsroom.accenture.com/news/2018/dhl-and-accenture-unlock-the-power-of-blockchain-in-logistics

Accenture. (n.d.). Blockchain solutions in finance. Accenture. https://accenture.com/

Accredible. (n.d.). Digital badges and certificates. Accredible. https://www.accredible.com/

Agora Energiewende. (n.d.). German energy transition. Agora Energiewende. https://www.agora-energiewende.org

Airbloc. (2023). Distributed Ad Data Marketplace. https://www.airbloc.org/

Alder, S. (2022). *Healthcare Data Breach Report*. The HIPAA Journal. https://www.hipaajournal.com/june-2022-healthcare-data-breach-report/#:~:text=Over%20the%20past%2012%20months,of%2057.67%20breaches%20a%20month

Ali, V., Norman, A. & Azzuhri, S. R. B. (2023). *Characteristics of Blockchain and Its Relationship With Trust*. IEEE Access, vol. 11, pp. 15364-15374. doi: 10.1109/ACCESS.2023.3243700.

Armstrong, K. (2023). *Tesla Achieves Impressive Sustainability Goals in 2022 Impact Report. Not a Tesla app.* https://www.notateslaapp.com/news/1369/tesla-achieves-impressive-sustainability-goals-in-2022-impact-report

Artifacts. (n.d.). Blockchain research collaboration. Artifacts. https://artifacts.ai/

Audius. (n.d.). Music streaming with blockchain. Audius. https://audius.co/

Azkan, C., Iggena, L., Möller, F. & Otto, B. (2021). Towards Design Principles for Data-Driven Services in Industrial Environments. 10.24251/HICSS.2021.217.

Aztec. (2021). Aztec Protocol: Privacy on Ethereum. https://www.aztec.network/

Aztec. (2021). Aztec Protocol: Privacy on Ethereum. https://www.aztec.network/

Funded by the European Union

Aztec. (2023). Aztec Protocol: Confidential transactions on Ethereum. https://www.aztec.network/

Big Solar Co-op. (n.d.). Community solar energy projects. Big Solar Co-op. https://bigsolar.coop/

BitPesa. (n.d.). Blockchain foreign exchange. BitPesa. https://www.bitpesa.io/

Blockcerts. (n.d.). Academic credentials on blockchain. Blockcerts. https://www.blockcerts.org/

BlockFi. (n.d.). Financial services for cryptocurrencies. BlockFi. https://blockfi.com/

BMW. (n.d.). BMW ConnectedDrive: Digital services for your vehicle. BMW. https://www.bmw.es/es/topics/ofertas-servicios/bmw-connected-drive.html

BurstIQ. (n.d.). Health data management. BurstIQ. https://burstiq.com/

California Attorney General. (n.d.). California Consumer Privacy Act (CCPA). State of California Department of Justice. https://oag.ca.gov/privacy/ccpa

Canetti, R., Makriyannis, N., & Peled, U. (2020). *Uc non-interactive, proactive, threshold ecdsa. Cryptology ePrint Archive.* https://eprint.iacr.org/2020/492

Capoot, A. (2024) *Tesla recalls more than 1.6 million cars in China over problems with Autopilot, locks. CNBC.* https://www.cnbc.com/2024/01/05/tesla-recalls-over-1point6-million-cars-in-china-over-autopilot-locks.html

Caruso. (2024). Caruso. From Connected Cars to Connected Business. https://www.caruso-dataplace.com/

Centre for Information Policy Leadership at Hunton Andrews Kurth LLP. (2023). *Cross-Border Privacy Rules, Privacy Recognition for Processors, and Global CBPR and PRP. Frequently Asked Questions.* [PDF] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_cbpr_prp_faqs_updated_july23.pdf

Chainalysis. (n.d.). Blockchain analytics. Chainalysis. https://www.chainalysis.com/

Chui, M., Issler, M., Roberts, R., & Lareina Yee, L. (2023). *McKinsey Technology Trends Outlook 2023. McKinsey.* https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable

Circle. (n.d.). Peer-to-peer blockchain payments. Circle. https://www.circle.com/en/

Clarivate. (n.d.). IPfolio. Clarivate. https://clarivate.com/intellectual-property/ip-management-software/ipfolio/?lid=ipfolio

Funded by the European Union

ConsenSys. (2020). Quorum: Enterprise blockchain solutions. https://consensys.net/quorum/

Coursera. (n.d.). Online education platform. Coursera. https://www.coursera.org/

Data Galaxy (2023). *8 Data Governance Use Cases You Should Know. datagalaxy.com*. https://www.datagalaxy.com/en/blog/8-data-governance-use-cases-you-should-know/#:~:text=1,how%20data%20should%20be%20handled

Decentraland. (n.d.). Virtual reality on blockchain. Decentraland. https://decentraland.org/

Denodo Technologies. (n.d.). Denodo enterprise datasheet. https://www.denodo.com/es/node/22809

Denodo. (2023). Denodo enterprise datasheet. Denodo. https://www.denodo.com/es/node/22809

DHL. (n.d.). Logistics and blockchain tracking. DHL. https://www.dhl.com/

Dimelgani, C., (2023). *What is Data Governance? Use cases, Best Practices & Tools.* Aimultiple.com.https://research.aimultiple.com/data-governance/#:~:text=Data%20governance%20is%20important%20because,Image%20source%3A%20Global%20IDs

Dwork, C., & Roth, A. (2014). *The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science. Theoretical Computer Science: Vol. 9: No. 3–4, pp. 211-407.* http://dx.doi.org/10.1561/0400000042

ECDC. (n.d.). Public health data in Europe. European Centre for Disease Prevention and Control. https://www.ecdc.europa.eu/en

Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2024). Health insurance portability and accountability act. National Center for Biotechnology Information. https://www.ncbi.nlm.nih.gov/books/NBK500019/

Edemekong, P. F., Annamaraju, P., & Haydel, M. J. (2024, February 12). Health Insurance Portability and Accountability Act. National Center for Biotechnology Information. https://www.ncbi.nlm.nih.gov/books/NBK500019/

Embleema. (n.d.). Virtual trials and regulatory analytics. Embleema. https://www.embleema.com/

EnergyHub. (n.d.). Residential energy management. EnergyHub. https://www.energyhub.com/

Enjin. (n.d.). Blockchain assets in gaming. Enjin. https://enjin.io/

e-Residency Estonia. (n.d.). Digital identity for global entrepreneurs. https://www.e-resident.gov.ee/

Everledger. (2021). Using blockchain for supply chain and asset tracking. https://www.everledger.io/

Fehrenbacher, K. (2017). *Siemens Invests in LO3 Energy, Making Blockchain a Piece of Its Microgrid Strategy*. Green Tech Media. https://www.greentechmedia.com/articles/read/siemens-invests-in-lo3-energy

Fernandez, D., Futoransky, A., Ajzenman, G., Travizano, M., & Sarraute C. (2020). *Wibson Protocol for Secure Data Exchange and Batch Payments*. arXiv:2001.08832. https://doi.org/10.48550/arXiv.2001.08832

Freightwaves (2018). *DHL and other supply logistics companies partner with Accenture blockchain*. https://www.freightwaves.com/news/blockchain/dhl-and-other-supply-logistics-accenture-blockchain

Frenté, S., (2023). *The Data Trifecta: Privacy, Security, and Governance from Reactivity to Resilience*. Dataversity.net. https://www.dataversity.net/the-data-trifecta-privacy-security-and-governance-from-reactivity-to-resilience/#:~:text=Data%20privacy%20focuses%20on%20protecting,groups%20%E2%80%93%20privacy%2C%20security

Fricker, S. & Maksimov, Y. (2017). Pricing of Data Products in Data Marketplaces. Conference: International Conference on Software Business, Essen, Germany. DOI:10.1007/978-3-319-69191-6_4.

Gaine (2023). *Evolving Data Privacy Regulations in Healthcare*. Gaine.com. https://gaine.com/blog/mdm/evolving-data-privacy-regulations-in-healthcare/#:~:text=,Century%20Cures%20Act%2C%20and%20HITECH

Genç, E. (2021). *What is Audius? The Decentralized Music Sharing and Streaming Service. Decrypt U.* https://decrypt.co/resources/what-is-audius-the-decentralized-music-sharing-and-streaming-service

Goel, V. (2018). *India's Top Court Limits Sweep of Biometric ID Program. The New York Times.* https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html

Golden State Foods. (n.d.)., from https://goldenstatefoods.com/

Goldwasser, S., Micali, S., & Rackoff, C. (2021). The knowledge complexity of interactive proof systems. Journal of the ACM, 38(1), 69-100. https://doi.org/10.1145/351633.351634

Funded by the European Union

Gossett, S., (2020). *How Healthcare Cybersecurity Is Affected by the Coronavirus Pandemic*. Builtin.com. https://builtin.com/cybersecurity/hospital-healthcare-cyberattacks

Guardtime Health. (n.d.). Securing health data with blockchain. Guardtime Health. https://guardtime.com/health

Hanlon, A., & Jones, K. (2023). Ethical concerns about social media privacy policies: do users have the ability to comprehend their consent actions? *Journal of Strategic Marketing*, 1–18. https://doi.org/10.1080/0965254X.2023.2232817

Hypebeast. (2022, August 1). A look at LVMH's blockchain consortium, which includes founding members Mercedes Benz, Prada, Cartier, and the OTB Group. Hypebeast. https://hypebeast.com/2022/8/lvmh-aura-blockchain-luxury-fashion

IBM (2020). *Food manufacturing on blockchain*. IBM Food Trust. *https://www.ibm.com/blockchain/resources/food-trust/manufacturing/*

IBM *(2019). IBM Food Trust. https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust*

Information Commissioner's Office (2023). *Privacy-enhancing technologies (PETs).* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

International Food Information Council (IFIC) Foundation (2019). *2019 Food & Health Survey [PDF].* foodinsight.org *https://foodinsight.org/wp-content/uploads/2019/05/IFIC-Foundation-2019-Food-and-Health-Report-FINAL.pdf*

IOTA. (2023). Distributed Ledger Technology for IoT. https://www.iota.org/

IRENA. (n.d.). Renewable energy transition. International Renewable Energy Agency. https://www.irena.org/

Jenkinson, G. (2022, May 6). Blockchain technology to power De Beers' diamond production. Cointelegraph. https://cointelegraph.com/news/blockchain-technology-to-power-de-beers-diamond-production

Kerasidou, A., & Kerasidou, C. (2023). *Data-driven research and healthcare: public trust, data governance and the NHS*. BMC Med Ethics 24, 51. https://doi.org/10.1186/s12910-023-00922-z

Koutroumpis, P., Leiponen, A., & Llewellyn, T. (2020) Markets for data, *Industrial and Corporate Change*, Vol. 29, Issue 3, pp 645–660, https://doi.org/10.1093/icc/dtaa002

Krishnan, K., (2023). *9 best practices for data governance in a healthcare setting*. Concentric.ai. https://concentric.ai/data-governance-in-healthcare-a-technical-overview/#:~:text=,and%20compliance%20with%20industry%20regulations

Lee, D. (2024). *Slow-and-Steady Waymo Is Winning the Self-Driving Race*. Bloomberg. https://www.bloomberg.com/opinion/articles/2024-01-09/slow-and-steady-waymo-is-winning-the-self-driving-race-for-alphabet

Leenes, R., & Martin, A. (2021). *Technology and regulation 2020*. Open Press TiU. https://jstor.org/stable/community.34023115 https://www.jstor.org/stable/community.34023115

LF Decentralised Trust (2018). *How walmart brought unprecedented transparency to the food supply chain with hyperledger fabric*. https://www.hyperledger.org/case-studies/walmart-case-study

LO3 Energy (2022). *LO3 Energy Deploys Pando Software to Maximize Renewable Asset Use in Australia. Globe Newswire*. https://www.globenewswire.com/news-release/2022/03/24/2409576/0/en/LO3-Energy-Deploys-Pando-Software-to-Maximize-Renewable-Asset-Use-in-Australia.html

Lodge, M. (2023). *What Is Decentraland*? Investopedia. https://www.investopedia.com/what-is-decentraland-6827259

Manzano Kharman, A., Jursitzky, C., Zhou, Q., Ferraro, P., Marecek, J., Pinson, P., & Shorten, R. (2022). An adversarially robust data-market for spatial, crowd-sourced data. arXiv. https://ar5iv.labs.arxiv.org/html/2206.06299

Matter Labs. (2021). zkSync: Scalable and private Ethereum Layer 2 solution. https://zksync.io/

Matter Labs. (2021). zkSync: Scalable and private Ethereum Layer 2 solution. https://zksync.io/

MediLedger. (n.d.). Blockchain in pharmaceutical supply chain. MediLedger. https://www.mediledger.com/

Meeco. (2023). Personal Data Marketplace Solutions. https://www.meeco.me/powered-by-meeco

Microsoft (2022). *Governance for the retail industry*. Learn. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/industry/retail/govern

MIT Energy Initiative. (n.d.). Sustainable energy research. MIT. https://energy.mit.edu/

Monero. (n.d.). Monero: Privacy by default. https://www.getmonero.org/

Monrat, A. A., Schelén, O. & Andersson, K. (2019). *A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities*. *IEEE Access*, vol. 7, pp. 117134-117151. https://doi.org/10.1109/ACCESS.2019.2936094

Funded by the European Union

NetObjex. (n.d.). from https://www.netobjex.com/

Nguyen, H., Serrano, M., Gyrard, A., & Tragos, E. (2018). FIESTA–IoT project: Federated interoperable semantic IoT/cloud testbeds and applications. Proceedings of The 2018 Web Conference Companion (WWW'18 Companion), 4 pages. https://doi.org/10.1145/3184558.3186199

Nguyen, H., Serrano, M., Gyrard, A., & Tragos, E. (2018). FIESTA–IoT project: Federated interoperable semantic IoT/cloud testbeds and applications. Proceedings of the 2018 Web Conference Companion (WWW'18 Companion), 1-4. https://doi.org/10.1145/3184558.3186199

Oasis Labs. (2020). Oasis Labs: Blockchain for privacy and data security. https://www.oasislabs.com/

Ocean Protocol Foundation. (2023). Ocean Protocol: Decentralized data exchange for AI and blockchain-powered data services. https://docs.oceanprotocol.com/

Ohnsman, A. (2024). *Waymo's Robotaxis Are Hitting The Highway, A First For Self-Driving Cars*. Forbes. https://www.forbes.com/sites/alanohnsman/2024/01/08/waymos-robotaxis-are-hitting-the-highway-a-first-for-self-driving-cars/?sh=11fe5aa923a3

Open Government Partnership. (n.d.). Transparency and accountability in governance. https://www.opengovpartnership.org/

Otonomo & Xouba. (2023). Otonomo and Xouba improve road safety with the use of connected vehicle data. Xouba. https://xouba.es/es/otonomo-y-xouba-mejoran-la-seguridad-vial-con-el-uso-de-los-datos-de-los-vehiculos-conectados/

Patientory. (n.d.). Blockchain-based health records. Patientory. https://patientory.com/

Perez, S. (2017, April 26). Spotify acquires blockchain startup Mediachain to solve music's attribution problem. TechCrunch. https://techcrunch.com/2017/04/26/spotify-acquires-blockchain-startup-mediachain-to-solve-musics-attribution-problem/

Perrigo, B., (2018). *India Has Been Collecting Eye Scans and Fingerprint Records from Every Citizen. Here's What to Know. Time Magazine.* https://time.com/5409604/india-aadhaar-supreme-court/

Privacy by Design. (2020). Zero-knowledge proofs and identity verification. https://www.privacybydesign.ca/

PromptCloud. (n.d.). Tesla's use of data to innovate in the auto industry: What manufacturers can learn. Retrieved from https://www.promptcloud.com/blog/tesla-approach-to-automotive-data-solutions/

Funded by the European Union

Provenance (2019). *Provenance supporting traceability for the 2020 International Woolmark Prize finalists*. https://www.provenance.org/news-insights/provenance-supporting-traceability-for-the-2020-international-woolmark-prize-finalists

Provenance. (n.d.). Product traceability in textiles. Provenance. https://www.provenance.org/

Rahman, M., Paul, M. K., & Sattar, A. H. M. S. (2023). Efficient perturbation techniques for preserving privacy of multivariate sensitive data. Science Progress. https://www.sciencedirect.com/science/article/pii/S2590005623000498

Rahman, M., Paul, M. K., & Sattar, A. H. M. S. (2023). Efficient perturbation techniques for preserving privacy of multivariate sensitive data. ScienceDirect. https://www.sciencedirect.com/science/article/pii/S2590005623000498

Rakić, B.M., Levak, T., Drev, Z., & Savić, S. (2017). *First purpose built protocol for supply chains based on blockchain*. Whitepaper.

Ramaswami, P., (2022) *How Sidewalk Labs is helping make cities more sustainable in 2022*. The Keyboard. https://blog.google/outreach-initiatives/sustainability/how-sidewalk-labs-is-helping-make-cities-more-sustainable-in-2022/

Rapoza, K. (2021). *Enjin Coin: All About Fake Swords, Fake Real Estate, And NFTs Near Future*. Forbes. https://www.forbes.com/sites/kenrapoza/2021/08/15/enjin-coin-all-about-fake-swords-fake-real-estate-and-nfts-near-future/?sh=68c31e04a7c9

Ripple. (n.d.). Cross-border blockchain transactions. Ripple. https://ripple.com/

Russel, R., & Wettengel, J. (2019). *The main stories of Germany's Energiewende. Clean Energy Wire*. https://www.cleanenergywire.org/factsheets/main-stories-germanys-energiewende

Secret Network. (n.d.). Enigma: Privacy-preserving decentralized applications. https://www.scrt.network/

Sensitech. (n.d.). Protect product integrity with real-time shipment visibility. Sensitech. https://www.sensitech.com/en/solutions/cold-chain/

SG Analytics (Sep 05, 2023). Governance in EdTech: How Institutions Can Ensuring Data Privacy and Ethical Practices. *SG Analytics blog*. https://us.sganalytics.com/blog/governance-in-EdTech-ensuring-data-privacy-and-ethical-practices/#:~:text=,concerning%20data%20privacy%20and%20security

Shifa, M. (2019). 9 Ways Blockchain IoT Union Help Elevate Your Business Value. valuecoders.com *https://www.valuecoders.com/blog/technology-and-apps/9-ways-blockchain-iot-union-help-elevate-your-business-value/*

Sidewalk Labs. (n.d.). Urban innovation for cities. https://www.sidewalklabs.com/

Siemens. (n.d.). Smart grid technology. Siemens. http://www.siemens.com

Sigwart, M., Borkowski, M., Peise, M., et al. (2019). Blockchain-based Data Provenance for IoT. arXiv. https://doi.org/10.48550/arXiv.1905.06852

Sigwart, M., Borkowski, M., Peise, M., Schulte, S., & Tai, S. (2019). *Blockchain-based Data Provenance for the Internet of Things*. arXiv. https://doi.org/10.48550/arXiv.1905.06852

Singapore Computer Society (2020). *Singapore smart nation initiatives and possible opportunities. SCS.* https://www.scs.org.sg/articles/smart-nation-singapore

Singapore Smart Nation. (n.d.). Urban digital transformation. Singapore. https://www.smartnation.gov.sg/

Singh, J. (2023). *How to Use Data Governance to Drive Data-Driven Decision Making: A Case Study for Data Scientists*. Savedelete. https://savedelete.com/news/technology/how-to-use-data-governance-to-drive-data-driven-decision-making-a-case-study-for-data-scientists/464880/#:~:text=Updated%3A%20October%2028%2C%202023%20How,managed%20data%20pipelines

Spiekermann, M. (2019). Data Marketplaces: Trends and Monetisation of Data Goods. *Intereconomics* **54**, 208–216. https://doi.org/10.1007/s10272-019-0826-z

Stahl, F., Schomm, F., Vossen, G. *et al.* A classification framework for data marketplaces. *Vietnam J Comput Sci* **3**, 137–143 (2016). https://doi.org/10.1007/s40595-016-0064-2

StarkWare. (n.d.). StarkWare: Scaling Ethereum with zk-STARKs. https://starkware.co/

StarkWare. (n.d.). StarkWare: Scaling Ethereum with zk-STARKs. https://starkware.co/

Sterk, F., Peukert, C., Hunke, F., & Weinhardt, C. (2022, January). Understanding car data monetization: A taxonomy of data-driven business models in the connected car domain. International Conference on Wirtschaftsinformatik. https://www.researchgate.net/publication/358248592_Understanding_Car_Data_Monetization_A_Taxonomy_of_Data-Driven_Business_Models_in_the_Connected_Car_Domain

Sterk, F., Peukert, C., Hunke, F., & Weinhardt, C. (2022, January). Understanding car data monetization: A taxonomy of data-driven business models in the connected car domain. International Conference on Wirtschaftsinformatik. https://www.researchgate.net/publication/358248592_Understanding_Car_Data_Monetization_A_Taxonomy_of_Data-Driven_Business_Models_in_the_Connected_Car_Domain

Student1. (n.d.). Cloud-based student data management. Student1. https://www.student1.org/

Telstra. (n.d.)., from https://www.telstra.com.au/

tenfold Software GmbH. (2024). tenfold product overview. Retrieved from https://www.tenfold-security.com/en/tenfold-overview/

Tesla. (n.d.). Electric vehicles and energy storage. Tesla. https://www.tesla.com/

The Digital Insurer. (n.d.). Everledger's pioneering blockchain work for diamonds. The Digital Insurer. https://www.the-digital-insurer.com/dia/everledgers-pioneering-blockchain-work-for-diamonds/#:~:text=Everledger%2C%20a%20London%2Dbased%20blockchain,processes%20with%20a%20blockchain%20ledger.

Toyota Motor Corporation. (2023). Toyota sustainability report 2023. Toyota. https://www.toyota.it/content/dam/toyota/nmsc/italy/mondo-toyota/ambiente/pdf/Toyota_Rapporto_Sostenibilita2023_ENG.pdf

Transport for London. (n.d.). Oyster pay as you go. Transport for London. https://tfl.gov.uk/fares/how-to-pay-and-where-to-buy-tickets-and-oyster/pay-as-you-go/oyster-pay-as-you-go#:~:text=An%20Oyster%20card%20is%20a,London%20and%20some%20outside%20London.

Uber. (2021, July 20). 'Orders Near You' and user-facing analytics on real-time geospatial data. Uber. https://www.uber.com/en-FI/blog/orders-near-you/

van de Ven, M., Abbas, A. E., Kwee, Z., & de Reuver, M. (2021). *Creating a Taxonomy of Business Models forData Marketplaces*. In A. Pucihar, M. K. Borstnar, R. Bons, H. Cripps, A. Sheombar, & D. Vidmar (Eds.), 34thBled eConference: Digital Support from Crisis to Progressive Change, BLED 2021 - Proceedings (pp. 309-321). University of Maribor Press. https://doi.org/10.18690/978-961-286-485-9.23

Veem. (n.d.). Blockchain-based global payments. Veem. https://www.veem.com/

Vimercati, S.D., Foresti, S., Livraga, G., & Samarati, P. (2023). k-Anonymity: From Theory to Applications. *Trans. Data Priv.*, 16, 25-49. https://hdl.handle.net/2434/954133

Walmart. (n.d.). Blockchain in food traceability. Walmart. https://www.walmart.com/

Wang T, Zhang X, Feng J, Yang X. (2020). A Comprehensive Survey on Local Differential Privacy toward Data Statistics and Analysis. *Sensors*; 20(24):7030. https://doi.org/10.3390/s20247030

Wang, K., Wang, P., Fu, A. W., & Wong, R. C. W. (2016). Generalized bucketization scheme for flexible privacy settings. Proceedings of the International Symposium on Privacy Enhancing Technologies, 16, 45-58. https://www.cs.sfu.ca/~wangk/pub/IS16.pdf

Waymo. (n.d.). Self-driving technology. Waymo. https://waymo.com/

Funded by the European Union

Woolmark Prize. (n.d.). Supporting sustainable fashion. Woolmark Prize. *https://www.woolmarkprize.com/*

Zcash. (n.d.). Zcash: A privacy-protecting cryptocurrency. *https://z.cash/*

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C., Li, H., & Tan, Y. (2019). Secure Multi-Party Computation: Theory, practice and applications. *Inf. Sci., 476,* 357-372. https://doi.org/10.1016/j.ins.2018.10.024

Zheng, Y. (2022, February 14). Alibaba implements blockchain technology. RFID Card. *https://www.rfidcard.com/alibaba-implements-blockchain-technology/?srsltid=AfmBOoqug04oY7UCtT-cQDDBmVk6_jFPChgi3EIDWjlazjKtWcfKyogU*

Zirui, M. & Bin, G. (2023). *A Privacy-Preserved and User Self-Governance Blockchain-Based Framework to Combat COVID-19 Depression in Social Media.* IEEE Access, vol. 11, pp. 35255-35280. DOI: 10.1109/ACCESS.2023.3264598.