future internet

Review

Future Internet Architectures on an Emerging Scale—A Systematic Review

Sarfaraz Ahmed Mohammed * and **Anca L. Ralescu**

Department of Computer Science, College of Engineering and Applied Science, University of Cincinnati, Cincinnati, OH 45221-0030, USA; ralescal@ucmail.uc.edu
* Correspondence: mohammsm@mail.uc.edu

Abstract: Future Internet is a general term that is used to refer to the study of new Internet architectures that emphasize the advancements that are paving the way for the next generation of internet. Today's internet has become more complicated and arduous to manage due to its increased traffic. This traffic is a result of the transfer of 247 billion emails, the management of more than a billion websites and 735 active top-level domains, the viewing of at least one billion YouTube videos per day (which is the source of main traffic), and the uploading of more than 2.5 billion photos to Facebook every year. The internet was never anticipated to provide quality of service (QoS) support, but one can have a best effort service that provides support for video streams and downloaded media applications. Therefore, the future architecture of the internet becomes crucial. Furthermore, the internet as a service has witnessed many evolving conflicts among its stakeholders, leading to extensive research. This article presents a systematic review of the internet's evolution and discusses the ongoing research efforts towards new internet architectures, as well as the challenges that are faced in increasing the network's performance and quality. Moreover, as part of these anticipated future developments, this article draws attention to the Metaverse, which combines the emerging areas of augmented reality, virtual reality, mixed reality, and extended reality, and is considered to be the next frontier for the future internet. This article examines the key role of the blockchain in organizing and advancing the applications and services within the Metaverse. It also discusses the potential benefits and challenges of future internet research. Finally, the article outlines certain directions for future internet research, particularly in the context of utilizing blockchains in the Metaverse.

Keywords: future internet; software defined networks; clean-slate approach; overlay networks; named data networks; mobility first; nebula; expressive internet architecture; metaverse; block chain; artificial intelligence

check for updates

Citation: Mohammed, S.A.; Ralescu, A.L. Future Internet Architectures on an Emerging Scale—A Systematic Review. *Future Internet* **2023**, *15*, 166. https://doi.org/10.3390/fi15050166

Academic Editor: Claude Chaudet

Received: 11 March 2023
Revised: 29 March 2023
Accepted: 30 March 2023
Published: 29 April 2023

1. Introduction

The internet has revolutionized over time as an ecosystem, connecting people across the globe and hosting a variety of services, such as multimedia, information, news, business, and education, which have spearheaded the development of new architectures, applications, and devices. It is seen that the client–server model is aging, reflecting a paradigm shift and a need to focus on new network architectures that improve all kinds of network services, thus improving quality of life [1]. The evolution of the internet has seen tremendous growth, starting from a few hundred users to more than three billion global users, thereby transforming a wide range of economic, social, societal, and business practices. The internet began with ARPANET and progressed to the web-based internet, followed by the application-based internet, with Android and iOS as standards. The next transformation of the internet is the augmented reality and virtual-reality-based internet that provides enormous opportunities (cognitive internet) but also significant risks, including cyber-attacks.

Additionally, the evolution of "edge networks" promises to push the network closer to the utilization ends of user devices, mitigating the additional storage and computation in distant server farms. The significant emergence of the programmable user plane has enabled faster data filtering, and the continuous availability of networks among server farms makes us ponder about the growing scale of the internet, connecting people, intelligent systems, more sensors, and actuators [1].

The question of where exactly this journey of future internet may take us to is still subject to an important debate. A few issues to ponder on are as follows:

1. How to overcome network distortions on a large scale?

The ability to stay connected without experiencing network distortions is now a reality. According to the reports in [2], at the start of 2023, over 5.16 billion people worldwide use the internet, which accounts for approximately 64.4 percent of the global population. Their data indicate that these figures are expected to continue to rise steadily, with the world's connected population growing by almost 100 million worldwide in January 2023, over the last 12 months.

Mobile devices, on the other hand, have become the primary means of accessing the internet for many users, with approximately 92.3 percent of internet users going online at least once using their mobile devices. These devices account for more than 56.9 percent of online time and contribute to around 60 percent of web traffic. In the year 2011, the experts in [3] predicted how digital life was going to be in 2025. They believed that the internet was likely to be the new electricity, effortless and less discernable and becoming deeply entrenched in human lives. They were of the opinion that mobile, wearable, and embedded computing, combined with the Internet of Things (IoT), would allow users to delve into artificial intelligence (AI) and cloud-based information sharing and storage.

2. How to manage data generated through sensors that require machine-to-machine communication over the network?

A major trend which we see intensifying in the future is machine-to-machine communication: sensors which communicate with smart homes and cars that communicate with each other (e.g., by giving warning of hazards, with respect to slippery roads). In such communications, there might be high requirements of a very low latency and high reliability. It is seen that in each case, machine-to-machine communication can bring numerous benefits, such as increased efficiency, improved safety, and reduced costs. For example, in a self-driving car, a slight delay in communication between the car's sensors and the cloud-based control system can lead to fatal accidents. Similarly, in industrial automation, any communication delay or disruption can lead to costly downtime.

To overcome these challenges, several communication technologies have been put in place, such as cellular networks, Wi-Fi, and Bluetooth, to name a few. These technologies can support machine-to-machine communication with different levels of reliability, latency, and bandwidth. For example, cellular networks provide wider coverage and higher reliability, while Wi-Fi can provide a higher bandwidth but a lower coverage. 5G networks as part of mobile network technology were introduced in 2019 to offer faster download and upload speeds, with a lower latency and higher capacity compared to previous generation networks. With the advent of 5G networks, users are offered faster download speeds, faster access to content, and improved streaming quality, thereby enhancing the overall mobile experience. Besides this, edge computing has emerged as a promising technology for supporting low-latency machine-to-machine communication. Edge computing refers to the processing of data closer to the source, such as on the device or on a nearby server, rather than sending it to a central cloud server for processing. Edge computing can significantly reduce latency and improve reliability by reducing the distance between the data generation and processing.

3. How to manage user-generated content on the internet?

Managing the user-generated content on Facebook, YouTube, and Twitter, etc., is becoming increasingly important as these platforms continue to grow in popularity. The content created by users can have a significant impact on the direction of the traffic, meaning that it can shape the discussions and the views of the users who engage with it. In this context, the authors in [4] proposed a hypothesis that was based on the user-generated content by people that helps them in making decisions for a purchase, and the factors of this included the perceived credibility, usefulness, and risk.

One of the most critical aspects of managing user-generated content is the need for platforms to leverage a productive balance between freedom of expression and ensuring that any inappropriate or harmful content is not disseminated on their platform. This task can be daunting, given the vast amount of content that is posted every day, and the diverse viewpoints and opinions that users hold.

The second critical aspect of managing user-generated content is to ensure that the content meets the platform's guidelines. These may include restrictions on hate speech, violence, harassment, and other forms of inappropriate behavior. There is no doubt that platforms have an onus to take appropriate actions against users that violate these guidelines, such as removal of content, terminating or suspending accounts, or content reporting to the law enforcement authorities. Additionally, social media platforms must also be aware of the potential impact that user-generated content can have on the direction of traffic. The awareness of the content's potential to go viral, and taking precautionary steps to ensure that it is not being spread for fraudulent or malicious purposes, for example, the spreading of false information or manipulating the public opinion.

Looking to the future, managing user-generated content will continue to be a critical issue for social media platforms. As these platforms continue to evolve and grow, there will be a need for ongoing improvements to the tools and processes that are used to manage it effectively. This may include an increased use of automation and artificial intelligence to identify and remove inappropriate content, as well as greater transparency and accountability in the management of this content. The authors in [5], highlight certain research propositions to minimize potential risks and to support the ethical use of an AI design that offers solutions to data privacy and transparency, retains consumer trust, and minimizes potential biases that include gender, ideological, and racial biases during the ethical AI design process.

4. Security and privacy

These are the two important issues because of the utmost importance of the internet to private and business life. Privacy, on the one hand, includes sensitive data, for example, financial and personal information, personal communication, and health records. The misuse of this information can lead to fraudulent activities that include identity theft, financial fraud, and other serious harm. It is very imperative that personal information should only be used for legitimate purposes. Security, on the other hand, is also a critical issue, as the internet is vulnerable to a wide range of cyber threats, for example, hacking, malware, and phishing attacks. These attacks lead to significant financial damage to both individuals and businesses by compromising the confidentiality, availability, and integrity of data. Hence, it is of paramount importance to have robust security measures against these threats, which include encryption, firewalls, and regular updates to software. Therefore, privacy and security are critical issues in building and maintaining internet trust and serve as a tool for commerce and social communication.

5. Energy efficiency of mobile devices

Energy efficiency is an essential aspect of mobile devices because it affects the device's performance, battery life, and user experience. Some ways that this energy efficiency can be improved in mobile devices are as follows:

i. Low power modes: To reduce power consumption, most mobile devices have a low power mode. The purpose of this mode is to turn off some irrelevant or non-essential features and to reduce the device's performance. These irrelevant features can include push notifications, background app refresh, and location services.
ii. Battery-saving features: To reduce power consumption, many devices come with built-in battery-saving features. Some devices may reduce the screen brightness or turn off Bluetooth or Wi-Fi.

iii. App optimization: To optimize their apps, app developers utilize efficient coding techniques, such as minimizing unnecessary network requests and reducing the CPU usage to reduce the power consumption. This optimization can have a significant impact on longer battery life and a good user experience.

iv. Hardware improvements: Energy efficiency can be improved by using more efficient processors, displays, and batteries. For example, OLED displays are more energy-efficient than LCD displays, and less power is utilized by advanced processors to perform the same tasks.

v. User education: Energy efficiency can be improved if the users become aware of their device's power consumption and take appropriate steps to reduce it. Some of these steps may include closing unused apps, turning off unused Bluetooth or Wi-Fi, and reducing the screen brightness.

Collaborating the issues that are discussed above and validating them into one complete networking architecture can be seen as an evolutionary approach to building models that promise the requirements that are needed for the future internet. In recent years, various research efforts have been undertaken to address the issues that are related to internet privacy and security. However, to develop and test new internet architectures, researchers need access to experimental testbeds. Since the internet is not owned by a single entity, but rather thousands of stakeholders, experimenting with new architectures can pose significant risks. To overcome this challenge, virtual testbeds can be used to test and validate these new architectures on a larger scale without compromising the existing services. This approach allows for the development of new architectures to be thoroughly tested and validated before they are deployed in real-time. In summary, the development of a future internet can be achieved by focusing on three main areas: innovating from various angles, collaborating with these innovations, and validating them in a complete networking architecture [6]. Additionally, experimenting with real testbeds can provide valuable insights into the efficacy and feasibility of these new architectures. This evolutionary approach to building models promises to meet the requirements that are needed for a future internet that is more secure, private, and efficient.

This article aims to present the existing research and the new developments that have been made to scale new internet services without jeopardizing the existing internet, and to provide significant resources. We focus our attention on two current approaches [7], namely evolutionary and clean slate. The evolutionary approach that is discussed in this paper shows how a system is transformed from one state to another incrementally and promises to provide solutions through the inclusion of additional services, without jeopardizing the existing internet. To achieve this, software-defined networking (SDN) and overlay networks (ON) have been presented and discussed extensively, as they are touted to offer affordable solutions for the future internet. SDN aims to provide an enhanced configuration with an improved performance but observes that this promise is still in its inception. Additionally, there remains varied fundamental issues that are not completely solved, among which, standardization and adoption appear to be imperative. We threw light on the research progress of clean-slate approaches, wherein a solution to a particular problem assumes the varied sections of the architecture to be permanent, thereby targeting different clean-slate solutions. We take a deeper look into the representation networks that form clean slate and build future internet architectures, including the NDN, Mobility First, NEBULA, XIA, and SDN [3].

In the next part of this paper, we introduce the Metaverse as a part of the future internet. It is seen that the Metaverse is gaining a lot of attention and is considered to be the next progress for the future internet, which combines all the emerging areas of augmented reality (AR), virtual reality (VR), mixed reality (MR), and extended reality (XR). The Metaverse is not new and has been explored in science fiction for several decades. However, recent advancements in technology, particularly in AR and VR, have brought the idea of the Metaverse closer to reality. The Metaverse offers a variety of applications, including gaming, social media, education, and e-commerce. In the Metaverse, users can create their virtual avatars, interact with others, and engage in various activities, such as attending virtual events, playing games, or shopping. The Metaverse promises to revolutionize the way that we interact with digital content, and it has the potential to transform several industries. Moreover, blockchain technology is emerging as a potential solution for many of the challenges that are associated with the Metaverse, such as identity verification, secure transactions, and the ownership of virtual assets. Blockchains can provide a decentralized platform for managing digital assets within the Metaverse, which can ensure the transparency, security, and immutability of transactions. In conclusion, the Metaverse is an exciting development that promises to revolutionize the way that we interact with digital content. It is a convergence of various emerging technologies such as AR, VR, MR, and XR. Moreover, the integration of blockchain technology can help to address many of the challenges that are associated with the Metaverse. As research in this area progresses, it is likely that we will see more innovative applications of the Metaverse in various industries. Finally, we highlight certain directions that guide future internet research and its development with the utilization of blockchains, in the context of the Metaverse.

Main Contributions of the Paper

Considering the past evolution of the internet and its anticipated future development, this article is organized as follows:

i. A brief overview of the research progress on evolutionary and clean-slate approaches for developing the future internet is presented. As evolutionary approaches aim to provide additional services without compromising the existing internet infrastructure, in this context, affordable solutions for the future internet, such as SDN and ONs, are extensively discussed. Clean-slate approaches, on the other hand, assume that certain sections of the architecture are permanent to target specific problems, leading to various clean-slate solutions. This article takes a closer look at the representation networks that form clean-slate solutions for building these future internet architectures, including NDN, Mobility First, NEBULA, XIA, and SDN. Finally, we present the key differences between the evolutionary and clean-slate approaches, followed by the research projects that have been undertaken in various countries.

ii. As part of its anticipated future development, we presented Metaverse as the next transformation of the internet, which aims to offer virtual-world solutions that combine augmented reality (AR), virtual reality (VR), mixed reality (MR), and extended reality (XR). The concept of blockchains and their role in the Metaverse is discussed, and the technical challenges that come along the way. The article also discusses the effect of blockchains on AI in the context of the Metaverse. Finally, the paper highlights the current Metaverse projects that use blockchains as the technology for the Metaverse that covers several areas of the virtual world. The potential benefits and challenges of future internet research are also presented.

iii. The promising directions that drive future internet research and its development towards the utilization of blockchains in the Metaverse.

From this point, this paper is framed as follows: after Section 1 (the current section), Section 2 discusses the literature review; Section 3 introduces the evolutionary and clean-slate approaches for scaling new internet services and highlights the merits and demerits of each. Section 4 details the concept of the Metaverse and the role of blockchains in Metaverse. Section 5 discusses the potential benefits and challenges of future internet research, and finally, Section 6 presents the conclusion of the paper and future directions.

2. Literature Review

Recent research efforts in the field of future internet have focused on network architectures that support the hosting of internet services to seamlessly connect users with a range of services from any terminal or node. This starts with [6], wherein the authors examined the key research projects from the United States, the European Union, Japan, and China. They presented several key issues and topics that are related to clean slate vs. evolutionary approaches, the integration of mobility, security, and other models, architectures that are centered around people instead of machines, and service delivery networks that enable telecommunication carriers to provide SDN services to different ASPs. While content and IP are seen as major forms of service delivery, service delivery itself is considered to be the narrow waist of the network architecture. In paper [8], the authors analyzed the potential problems that were encountered by the TCP/IP architecture and presented SOFIA, a service-oriented architecture (SOA) where the network did not just serve as a transport layer, but a service queue that combined all the capabilities of transmission, storage, and computation to create a more secure and safe network with controllable states. Though the architecture was assessed on a testbed constituting a programmable virtual router, and, even after providing an inherent security and safety mechanism that ranged from service registration to migration and provided safer access to the services on every link, it was seen that the essence of future internet is still far-fetched. However, there is still uncertainty about whether the current TCP/IP protocol stacks and testbeds can support the development of new future internet architectures. In [9], the paper presented a survey of several projects, emphasizing the different networking architectures that are not hindered by the current TCP/IP network. Their work focused on various research projects such as testbed analyses for building new platforms and architectures, security, and content delivery techniques, to name a few, and served as a stepping point for performing future networking research. However, a question to be raised here is whether these testbeds and TCP/IP protocol stacks, to date, will support the use and development of new future internet architectures. In paper [7], the authors argued in favor of the emergence of clean-slate design as a central point allowing for the networking field to emerge and achieve the future internet that promises trustworthiness. These authors agreed that evolutionary and clean-slate approaches go hand-in-hand and were of the opinion that clean-slate helps in achieving security, reliability, and cost effectiveness with the ongoing evolution of the internet. Although the approaches that are mentioned above have promised an internet architecture with an increased number of applications and services, contrary to these approaches, we can think of the internet as a progressive ecosystem that encompasses several disciplines, as rightly penned by the authors.

In recent years, there has been a focus on the development of the computing architectures that are in place and can support the computation and communication resources in a geographically dispersed environment, with the goal of accommodating a quality of service (QoS) for applications and services. This has led to the growth of active networks and edge computing, which aims to push caches to the edge, to support a fog architecture. However, there are still several issues to be addressed regarding the systematic arrangement and orchestration of the fog deployment, as discussed in [10]. In response to these challenges, the authors proposed an alternative to traditional cloud computing, namely edge and fog computing, which enable data centers to support both data-intensive and time-sensitive applications, particularly those that fall under the Internet of Things (IoT) umbrella. One of the key problems in this context is how to administer the computing and storage resources that are available while the application services are being deployed. To address this issue, the authors proposed an information-centric networking (ICN) model that gave rise to an ICN–edge/fog architecture. Within this architecture, the authors introduced an innovative service-caching strategy known as 3Q, which aimed to obtain optimal results by considering the cached hits, cloud usage, and latency.

The emerging field of multi-access edge computing (MEC) presents a significant challenge in addressing the issues of combined service caching and task offloading. In response to this, the authors of [11] proposed an optimization-based approach that prioritized the quality of experience (QoE) for users by balancing the service latency and computing resource costs. Additionally, Named Data Networking (NDN) is gaining attention as a secure form of a sign-on protocol for smart homes, positioning it at the forefront of these next-generation internet architectures. In [12], the authors addressed two key concerns related to NDN, namely creating a trustworthy relationship between the system and new devices, ensuring that only authorized users could access the system data. These innovative solutions highlighted the growing need for advanced security measures in future internet architectures.The two approaches that are seen as most prevalent in today's internet are the software- and data-centric approaches. To support the on-demand control and configuration of resources, including storage and computation, the authors further proposed a cognitive network function virtualization for information-centric networking (ICN). This approach utilizes fog computing and relies on a data-driven intelligent future network to improve resource utilization and content distribution.

Vehicular communication is a rapidly developing field that seeks to address technological, societal, and standardization challenges. According to a report on the Internet of Vehicles [13], there is a push to integrate SDN and network function virtualization with fog computing. The market for internet-connected vehicles is rapidly growing and it is predicted that companies will be using such vehicles in some form by the end of 2023. Another important aspect of the future internet is the evolution of quantum networking.

The emergence of the Metaverse has captured significant attention, particularly since Facebook announced its rebranding to Meta in October 2021. This new realm of computer-generated, networked extended reality (XR) combines augmented reality (AR), mixed reality (MR), and virtual reality (VR) into a single entity. XR advocates suggest that the evolution of advanced 3D and online worlds will benefit society in multiple domains, including healthcare, education, arts, entertainment, and social life. However, with the rapid progression of AI-based assistive systems, the generation of user experience data may necessitate the creation of new spaces that can enrich users' lives. While the digital world of the Metaverse may seem glorious, concerns about privacy, security, health, safety, and economic impacts must be addressed. The potential societal implications of a mature XR-based Metaverse are the subject of debate among experts [14].

In a recent study [15], the authors suggested that AR-based remote robotic control and surgery can be achieved using Metaverse platforms. However, the implementation of areas such as digital biometrics [16], cryptocurrency [17], and explainable artificial intelligence (XAI) [18] in the real world presents challenges. As the Metaverse is in its inception, it is important to consider privacy and security measures during the design phase to provide an additional service assurance for its users. While there are challenges to expanding the digital infrastructure, the absence of a serviceable digital infrastructure with adequate processing and network capabilities is a significant obstacle. Furthermore, access technologies will only be applicable with emerging 6G mobile technologies, which are still experimental and not yet globally available. To launch the Metaverse successfully, it is important to understand the interoperability and compatibility between the physical and virtual worlds. The scalability and potential of the Metaverse engines must also be considered, as the processing that is required might not meet the requirements of the social media backbone. Therefore, strategies such as optimal processing and operation should be considered to mitigate the costs of the processing, storage, and networking. Automated AI-based approaches, which require further attention [19], could be a part of these strategies.

3. Evolutionary and Clean Slate Approaches

Different research organizations are addressing various topics that are related to generating content or data-oriented paradigms, mobility and ubiquitous access to networks, cloud-computing-centric architectures, and experimental testbeds. However, the continuing success of the internet has been hindered by factors such as sophisticated network attacks, which are made possible by the absence of security in its native architectural framework.

To overcome these challenges, two important approaches have emerged: (i) the evolutionary approach, and (ii) the clean slate approach. The evolutionary approach involves making incremental changes to the existing internet architecture and improving its functionality by addressing its weaknesses. The clean slate approach, on the other hand, allows us to begin from scratch and design a new architecture that is better suited to meeting the current and future demands of the internet. Both of these approaches have their own merits and drawbacks, and the choice between them depends on various factors, such as the urgency of the problem, the resources that are available, and the scope of the desired changes.

3.1. Evolutionary Approach

The evolutionary approach involves transforming a system incrementally, from one state to another, to resolve issues and allow new services without causing problems to the existing internet. This approach includes the use of software-defined networking (SDN) and overlay networks (ONs), as depicted in Figure 1.

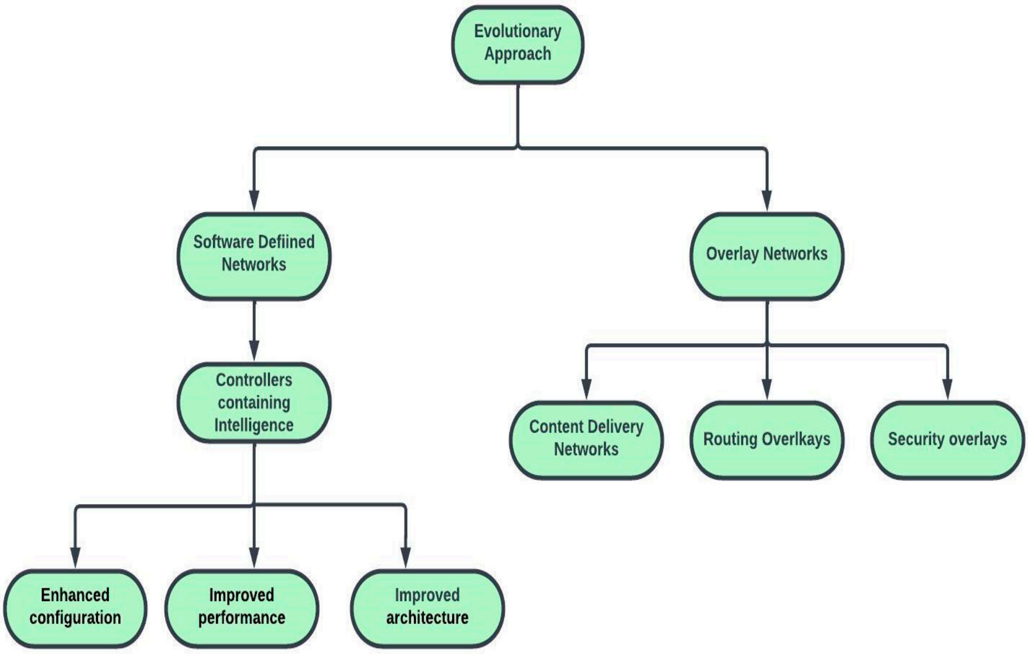


Figure 1. Architecture of evolutionary approach.

3.1.1. Software-Defined Networking

SDN offers solutions to the future internet architecture by incorporating network intelligence as a component of the network and separating the data plane (the part of the network that carries the user traffic [20]) from the control plane (the part of the network that controls the forwarding of data packets [21]). The controllers, which emerge from the routing process in the control plane, act as the "brain", and contain complete intelligence. However, the centralization of network intelligence in SDN can lead to poor scalability and security, making it a central issue [22]. To promote SDN, the Open Networking Foundation (ONF) was established in 2011 to support the standardization of the OpenFlow protocol and its technologies. The goal of the ONF is to scale this innovation through simple software changes in data centers, which can bring potential benefits such as an enhanced configuration, improved performance, and improved architecture [23].

In 2020, ONF announced Aether, which is the first open-source platform that supports 5G, LTE, and edge as cloud services. Aether's open-source architecture runs on a Kubernetes orchestrated environment and is built on CORD (Central Office Re-directed as a Data Center) and ONOS (Open Network Operating System) platforms, allowing for an easy assembly and deployment with remarkable speed [24].

CORD

Small or large central offices (COs) often use service gateways to provide services to their customers, such as residential, mobile, or enterprise users. However, these service edges face challenges such as high capital expenditures and operational costs, as there are hundreds of heterogeneous, closed proprietary systems that accumulate over decades in the telecommunications (Telco) edge. These systems are often not programmable, which limits innovation and the creation of new platforms and services. Therefore, the main objective is to reduce these costs (capital and operational) to enable Telcos to offer new services.

In essence, CORD [25] aims to bring the economies of a data center, which relies on commodity servers, open-source software, and cloud intelligence, to the edge of a Telco network. This approach, known as access as a service, allows for the disaggregation of legacy virtual machines (VMs) into smaller elements, enabling greater innovation. As an open-source project, it is important to understand the entire ecosystem surrounding CORD. CORD utilizes SDN to interconnect physical and virtual elements, adding value not just to VMs, but also to switches. By doing so, CORD enables the provision of innovative services.

The primary objective of the CORD project was to create a customizable and extensible platform that could support multiple access technologies and services, while adhering to the best practices for building and operating scalable multi-tenant cloud services, including support for multitenancy. From an architectural perspective, the reference platform, as shown in Figure 2, is critical. The developers sought to design a minimal kernel that could support thousands of CO edges. In 2017, the third release of CORD was announced, which enabled the cloud community to run a variety of projects independently.

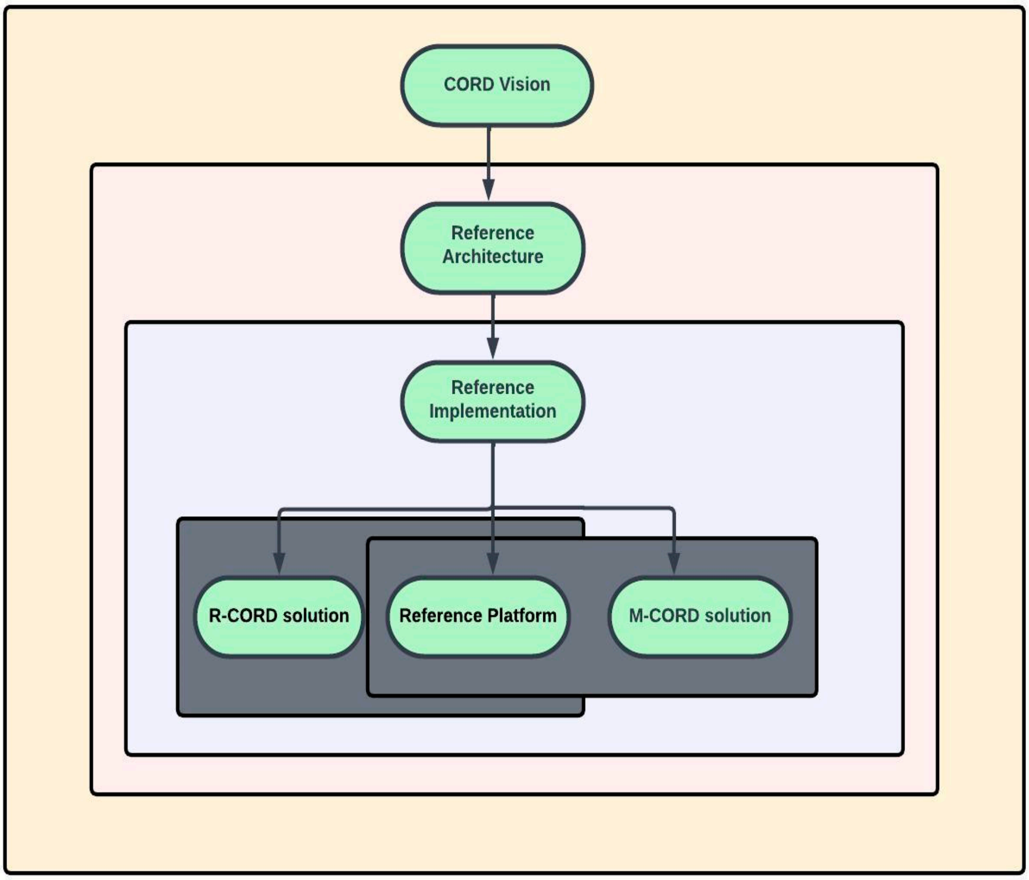


Figure 2. Elements of CORD project.

It can be seen that the CORD platform is no longer in use [26], but its legacy lives on in the form of several ONF broad-band projects, such as SEBA (SDN Enabled Broadband Access), VOLTHA (Virtual Optical Line Terminal Hardware Abstraction), and Aether 5G connected edge cloud, etc. These projects are built upon the foundation that was laid by CORD to provide innovative solutions to the challenges that are faced by Telco networks. SEBA, for instance, provides a cloud-native, open-source platform for software-defined access networks that enables service providers to offer next-generation services. VOLTHA is an open-source software platform that provides hardware abstraction for optical line terminals (OLTs) and is designed to work with multiple hardware vendors. Aether is an open-source platform that supports 5G, LTE, and edge as cloud services, and is built on CORD and ONOS platforms. These projects demonstrate the continued efforts of ONF to drive innovation in the telecommunications industry through open-source solutions.

ONOS

Open Network Operating System (ONOS) [27] is an open-source SDN network operating system that aims to build next-generation SDN and NFV (network function virtualization) solutions. One of the main advantages of using an NFV is the separation of communication services from the dedicated hardware, such as routers and firewalls, which allows network operations to offer new services dynamically, without installing new hardware. This flexibility can reduce the capital expenditure and operational costs while increasing network agility and innovation. ONOS also offers advanced features such as real-time network analytics, programmability, and scalability, making it a powerful platform for building and operating large-scale, carrier-grade networks. The reasons to use NFV include [28]:

- Pay-as-you-go: Businesses can pay only for the services that they utilize using NFV models, resulting in cost savings.
- Fewer physical appliances: The NFV model works on virtual machines (VMs) and requires fewer physical appliances, reducing operational costs and simplifying the network management.
- Scalability: It allows for the faster scaling of a network architecture with virtual machines, without the need for extra hardware, making it easier to handle increasing network traffic demands.

ONOS is designed to meet the requirements of mission critical networks by focusing on three specific areas: the distributed core, abstractions and models, and application platform. A distributed core is necessary for high scalability, availability, and performance. Abstractions and models are needed to allow for network configuration and control, without relying on device specifics. An application platform is necessary for developers to dynamically extend the device's capabilities. ONOS was designed to leverage white box merchant silicon hardware and provide flexibility for creating and deploying new network services with simplified interfaces. By adding intelligence to the ONOS cloud controller, new network applications can be created without altering the data plane systems, reinforcing the configuration and real-time control while avoiding the need to run switching and routing control protocols. The ONOS includes:

- A platform and a set of applications that act as an extensible, modular, distributed SDN controller.
- The simplified management, configuration, and deployment of new software, hardware, and services.
- A scale-out architecture to provide the resiliency and scalability that are required to meet the rigors of production carrier environments.

Challenges of SDN

Managing complex networks and environments with traditional network design can be expensive, and this is where efficient network services that are flexible and scalable come into play. SDN aims to provide an enhanced configuration with an improved performance, but it is still in its infancy. There are several issues that need to be addressed, including network reliability, scalability, standardization, and adoption. Network reliability is a concern when it comes to how reliable the SDN centralized control is in handling network failures, particularly the central controller. While there are fault-tolerant architectures with multiple controllers, scalability can still be an issue, as the data and control planes are decoupled, and both have their standard APIs. In such cases, the SDN controller may become a bottleneck, as the network scales in terms of the number of switches and nodes [29]. However, multiple controllers in a hierarchical structure can help to prevent bottlenecks. Standardization and adoption are also crucial issues to address for SDN's continued success.

SDN is based on a centralized networking system, with the controller managing the global view of the network. However, the OpenFlow standards that are used by SDN can raise issues regarding scalability and reliability. One such issue is the controller placement: given a certain network topology, it is important to determine the number and placement of the controllers. While this issue has been studied in the literature with respect to performance optimization, maximizing fault tolerance remains an important challenge to address [30].

Among the various SDN standards, OpenFlow is widely accepted as the most common SDN standard, but it still has open issues such as resilient communication and scalability [31]. SDN must have a similar resiliency to TCP/IP architectures. The centralized controller is always a concern, as the data plane can lead to an uncontrollable state due to certain attacks. The fault tolerance and robustness of this centralized control are challenging areas that need attention for resilient communication in the future of SDN. There are scalability concerns for SDN, such as the timely delivery of packets to the controller, which may increase the network load, leading to a bottleneck in the controller. Furthermore, additional latency issues may arise due to switches being configured by external entities. Although these issues are not problematic for smaller networks, as the network grows, the controller must process millions of flows per second, highlighting these scalability issues.

The development of a high-level programming language for SDN applications is still an area that needs attention. Currently, there is a lack of collaboration between SDN application developers, network device consumers, and network device vendors [23]. The transition from traditional networking to SDN can be challenging, as there are concerns regarding the SDN interoperability with legacy network devices, as well as performance and privacy issues that are related to its centralized control. Moreover, the lack of technical support experts for SDN is a major concern. At present, SDN deployment is limited to small testbeds for research prototypes, and such prototypes are not mature enough to instill confidence for real-world deployment.

3.1.2. Overlay Networks (ON)

These networks have become increasingly important in the context of the internet's massive growth. Table 1 illustrates some of the networks that fall under this category, including peer-to-peer (P2P) file sharing [32], content delivery caching networks, voice-over IP, and testbed networks. One example of P2P file sharing is Napster, which has not been in use since 2002 due to copyright laws [33]. The internet was originally viewed as an overlay with additional features, such as packet-switched networks, which were added to meet the needs of peer-to-peer research [34].

In ONs, nodes are connected by virtual links and a Locator ID Separation protocol (LISP) is used. ONs pose certain implications for the emergence of future internet architectures.

The authors in [34] discussed various types of overlay networks, including content delivery networks (CDNs), routing overlays, and security overlays. Overlay networks pose interesting questions and unique challenges, such as determining the best path between the source and destination in a large network with multiple routes. This requires efficient routing algorithms that can handle diverse network topologies and routing requirements. Additionally, security overlays aim to provide secure communication channels that are resistant to attacks, while CDNs help to distribute content more efficiently by caching popular content closer to the end-users. The emergence of overlay networks has driven research in areas such as network virtualization, software-defined networking, and network function virtualization, with the goal of improving network flexibility, scalability, and security.

Another important question to consider is how to enable independent decision making in a network consisting of interconnected ISPs. These decisions are influenced by several factors, including the internal structure of the ISPs and the Border Gateway Protocol (BGP), which serves as a network protocol that computes and distributes the best path from each source to its destination.

Table 1. Examples of overlay networks [34].

Type	Purpose	Example
Peer to Peer (P2P)	File Sharing	Napster, Gneutella
Content Delivery Networks (CDN)	Content caching to reduce access delays and transport costs	Digital Island
Routing	Reduce routing delays, resilient routing overlays	Resilient Overlay Networks (RON)
Security	Enhance end user security and privacy	Virtual private network (VPN), onion routing, anonymous content storage (Freenet, Entropy)
Experimental	Facilitate innovation, implementation of new technologies, experimentation	General Purpose (PlanetLab 13)
Others	Various	Email, VOIP(Skype), Tolerant Networks, etc.

3.2. *The Clean-Slate Approach*

The clean-slate architecture offers a promising approach, and information-centric networking (ICN) is a notable example of such a network. ICN includes connectionless network protocols and inter-domain architectures. One significant aspect of the clean-slate architecture is its need for evolvability to adapt to future changes while maintaining fixed sections or parts, to allow for different clean-slate solutions. A subset of the clean-slate architecture is representation networks, which form a clean slate towards future internet architecture. Some examples of these representation networks are NDN, MobilityFirst, NEBULA, XIA, and SDN (see Table 2) [35].

Table 2. Projects undertaken with clusters by U.S.

Projects Undertaken	Selected Clusters
Future Internet Architecture (FIA)	NDN, Mobility First, NEBULA, XIA, SDN, etc.
Future Internet Design (FIND)	CABO, Maestro, DAMS, NetSerV, etc.

3.2.1. Named Data Networking (NDN)

The primary objective of NDN is to simplify network communication and enhance the data transmission efficiency by considering named data instead of their location (Lixia Zhang et al., 2010). The NDN architecture [36] is based on six principles, with the first three being focused on the “thin waist” named data, which is a significant difference between NDN and IP. The other three principles are focused on network stability and the separation of the routing and forwarding planes, leading to extensive research into developing a new routing system in parallel, and facilitating the evolution of the internet.

In an NDN architecture, communication occurs by initiating a packet from the consumer (receiving end) that contains a name for identifying the desired data (see Figure 3).

At the router, the name is searched in the forwarding information base (FIB) using a name-based routing protocol. When the data request arrives at a node, a data packet is returned, including the (name data) content with a producer′s key signature. The names inside the interest/data packets are then routed towards the data producers containing the state information (see Figure 4) [36]. The NDN architecture utilizes a name-based approach for routing that is different from IP’s address-based routing. This name-based approach provides more flexibility for content-based addressing, leading to a simplified and more efficient data transmission.

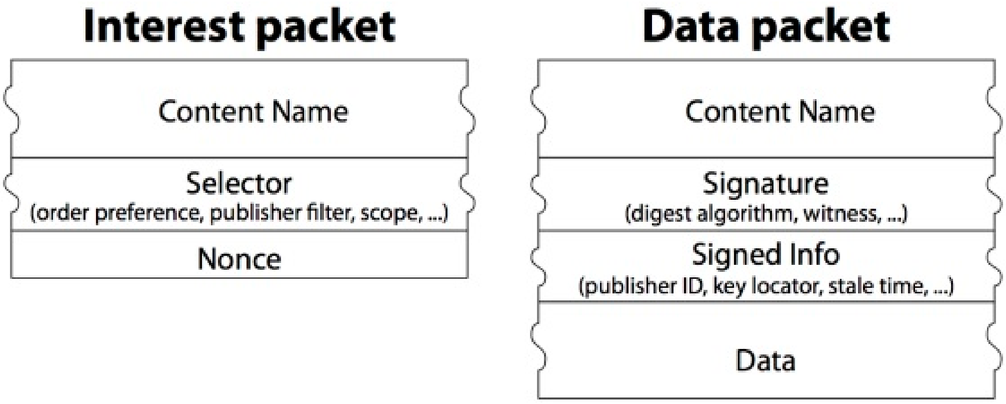
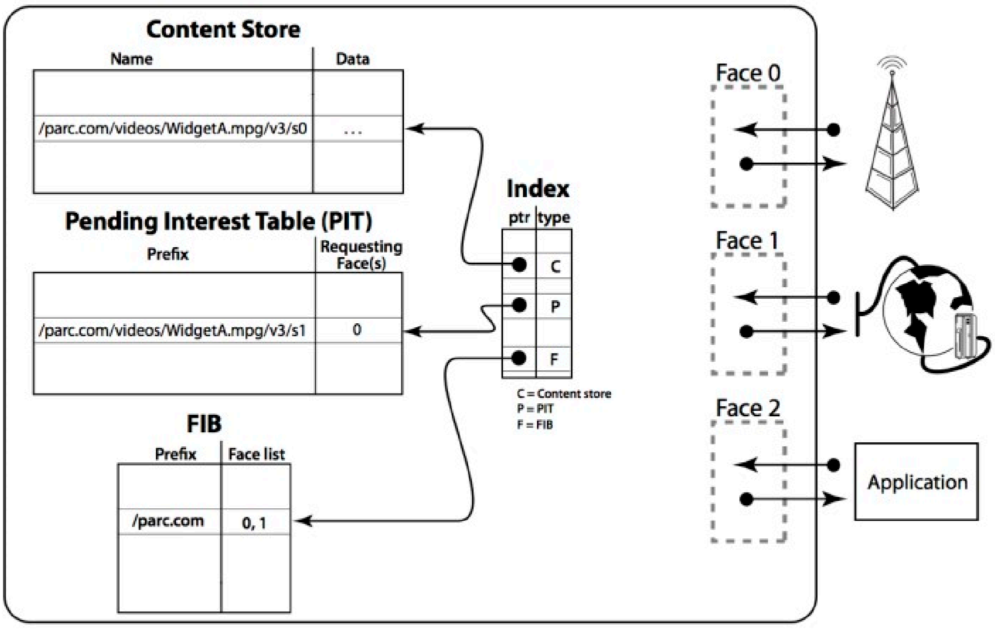

Interest packet
Content Name
Selector
(order preference, publisher filter, scope, ...)
Nonce
Data packet
Content Name
Signature
(digest algorithm, witness, ...)
Signed Info
(publisher ID, key locator, stale time, ...)
Data

Figure 3. Packets in an NDN architecture [36].



Name	Data
/parc.com/videos/WidgetA.mpg/v3/s0	...

Prefix	Requesting Face(s)
/parc.com/videos/WidgetA.mpg/v3/s1	0

Prefix	Face list
/parc.com	0, 1

Figure 4. Forwarding process at an NDN node [36].

NDN modifies the problem design and makes use of an IP as the narrow waist and named data for its architecture (see Figure 5). This named method resembles the URL structure and seems to exhibit several characteristics of IPs.

The vision of NDN is centered around the concept of information-centric networking (ICN), which aims to improve data communication at the network layer. By integrating network services with the application requirements, NDN provides numerous benefits, such as enhanced security, scalability, and resilience in communication. Additionally, NDN has numerous applications, including mobile edge computing, the Internet of Things (IoT), and low-latency applications [37].

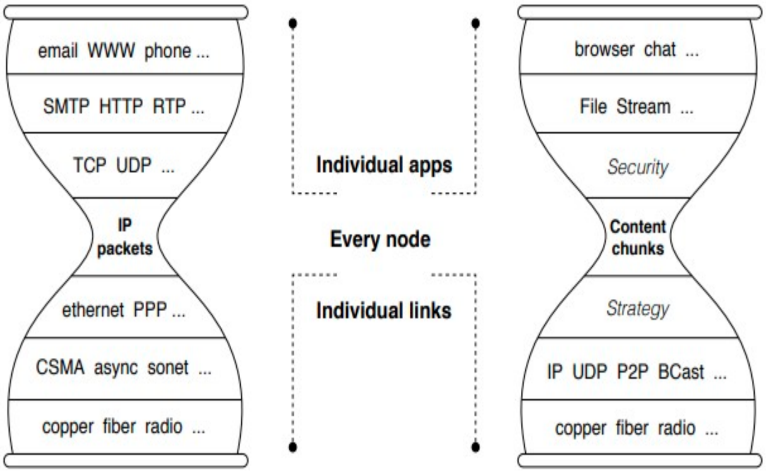


Figure 5. Comparison of IP and NDN at narrow waist [37].

Idea behind the NDN

In NDN, the packet forwarding model is used, where each packet is assigned a unique name and forwarding decisions can be made based on this name. Achieving a scalable design of the NDN forwarding plane requires addressing various issues that are related to its essential function, such as fast name lookup. The authors of [38] identified three main issues in this design: string matching, longest prefix matching, and the identification of unbounded names. They also proposed solutions to address these issues and improve the execution of the NDN reference implementations and forwarding structures. By addressing these issues, NDN can provide efficient and scalable packet forwarding, which is essential for its use in various applications.

It is notable that NDN offers several significant advantages, such as an improved efficiency of the application layer through the named data, which is particularly useful for its current network applications, such as streaming media services [32] that rely on the internet to deliver their data services. By bypassing the need for host addresses, and instead accessing content based directly on its name [38], NDN eliminates the limitations of traditional network architectures and allows for a more efficient utilization of high bandwidth. Additionally, NDN allows for the implementation of a router cache for frequently accessed content, further enhancing the efficiency of its data retrieval. Overall, these features make NDN a promising technology for addressing the challenges of data communication in the evolving internet landscape.

3.2.2. MobilityFirst

MobilityFirst is a future internet architecture that was proposed by NSF as a part of their clean-slate project program. The initiative faces challenges such as mobile access and scalability, as detailed in [39]. The architecture is built around key components, including names from the address separation, public key-based names, delay-tolerant routing that can handle wireless link quality fluctuations, large protocol data units, and location-aware services (see Figure 6). The service layer is designed to serve as the narrow waist, facilitating the development of mobile-centric services while the addressing security and privacy concerns that were outlined in [40]. To enhance the network functionality, the paper incorporates specific routing techniques, particularly storage-aware routing.

The core paradigm of MobilityFirst emphasizes the use of mobile devices to enable communication between the applications and entities that are identified by a global unique identifier. Unlike IP addresses, which are associated with fixed endpoints and do not account for mobility, MobilityFirst routers can leverage a distributed name resolution service to overcome mobility-related challenges [41].

The authors were able to develop a prototype of the MobilityFirst protocol stack on a GENI testbed in 2011, with contributions from various US universities (Rutgers, UMass, MIT, Duke, University of Michigan, UNC, University of Wisconsin, and University of Nebraska), as well as research centers in the industry. GENI provides support for existing projects, infrastructure models for scaling networks, and a framework for device control between different users, as well as environments to validate, analyze, assess, and record the network outcomes.

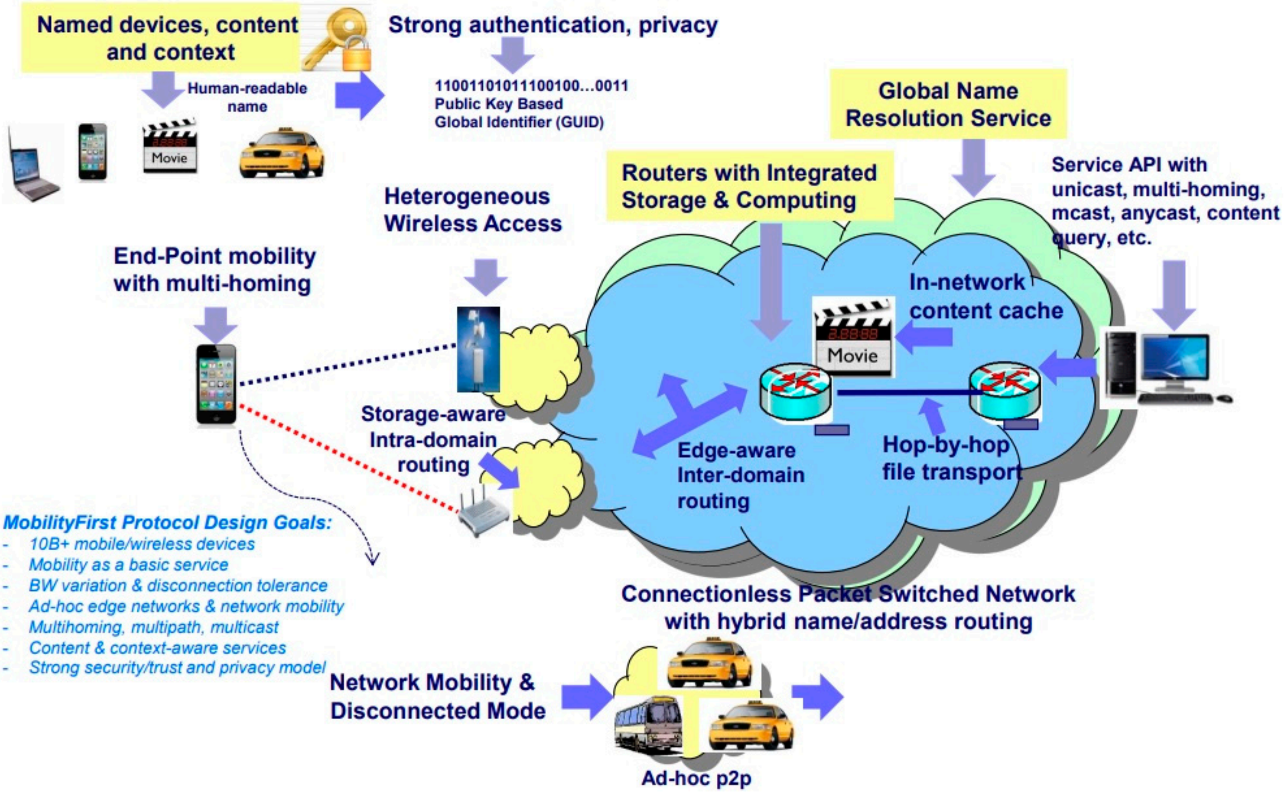

Named devices, content and context
Strong authentication, privacy
Human-readable name
11001101011100100...0011
Public Key Based
Global Identifier (GUID)
Movie
Global Name Resolution Service
Routers with Integrated Storage & Computing
Service API with unicast, multi-homing, mcast, anycast, content query, etc.
Heterogeneous Wireless Access
End-Point mobility with multi-homing
In-network content cache
Movie
Storage-aware Intra-domain routing
Edge-aware Inter-domain routing
Hop-by-hop file transport
MobilityFirst Protocol Design Goals:
- 10B+ mobile/wireless devices
- Mobility as a basic service
- BW variation & disconnection tolerance
- Ad-hoc edge networks & network mobility
- Multihoming, multipath, multicast
- Content & context-aware services
- Strong security/trust and privacy model
Connectionless Packet Switched Network with hybrid name/address routing
Network Mobility & Disconnected Mode
Ad-hoc p2p

Figure 6. MobilityFirst architecture overview [40].

3.2.3. NEBULA

NEBULA was proposed with the aim of centralizing cloud computing services in support of the future internet. The access to cloud computing resources demands a new architectural paradigm that incorporates new features from a network [42]. The NEBULA architecture [43], as seen in Figure 7, focuses on a reliable and trustworthy core network (Ncore), a NEBULA data plane (NDP), and NEBULA virtual and extensible network techniques (NVENT) to enable users to manage their network configuration. The NEBULA architecture emphasizes three key aspects: its ability to solve large and complex problems, its novelty, which may require new approaches to integration, and the need to find people with diverse skill sets to provide solutions for tackling sub-problems.

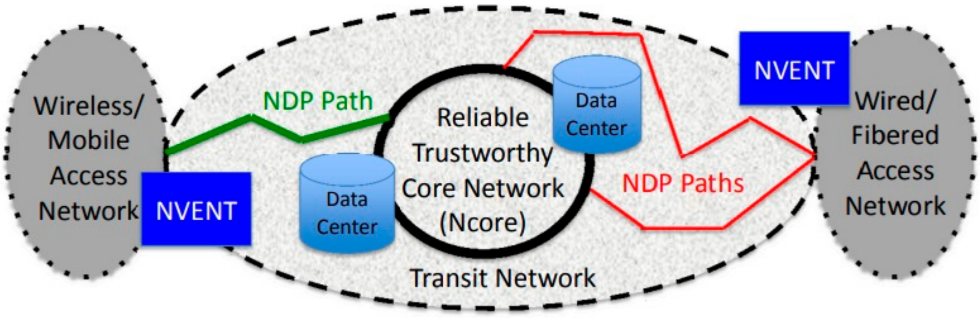

Wireless/ Mobile Access Network
NVENT
NDP Path
Data Center
Reliable Trustworthy Core Network (Ncore)
Data Center
NDP Paths
NVENT
Wired/ Fibered Access Network
Transit Network

Figure 7. NEBULA FIA [42].

To build robust, network that supports cloud computing, secure interdomain paths are necessary, and intradomain services must also be in place. Such a configuration requires certain policies from end users, ISPs, or organizations, which need to be logically evaluated to determine the permissible and available paths [44]. When a specification is received, such as in the case of ICING NDP [45], the system searches its cache for a reliable route/path to the destination, and if found, seeks consent to use it. The NEBULA packet-forwarding approach utilizes cryptographic tokens and markings to support end users [46]. Additionally, it is crucial to have a mapping of the names that are compliant with the network's usable information. Connecting the end-users, distributed nodes, and data centers has several implications for achieving the future internet, and include the following:

- Access to cloud computing becomes imperative when a loss of availability, timing fluctuations, storage, computation, and control replace the existing support for the local storage and computation.
- The network must ensure security to prevent data corruption if the network infrastructure is hosted on a cloud.
- With the continued development of new cloud applications, it is necessary for the network to be capable of addressing these application concerns by providing flexible connections.

3.2.4. Expressive Internet Architecture (XIA)

Numerous studies have concentrated on clean-slate network architectures that revolve around content, services, or users, which are commonly referred to as first-class principles. The XIA architecture provides built-in support for these diverse principles to improve its functionality and to adapt to future, unforeseen principles [47]. XIA aims to enhance the reliability and trustworthiness of the internet by providing a unified network that enables communication support between different entities and accommodates unknown future entities, as seen in Figure 8.

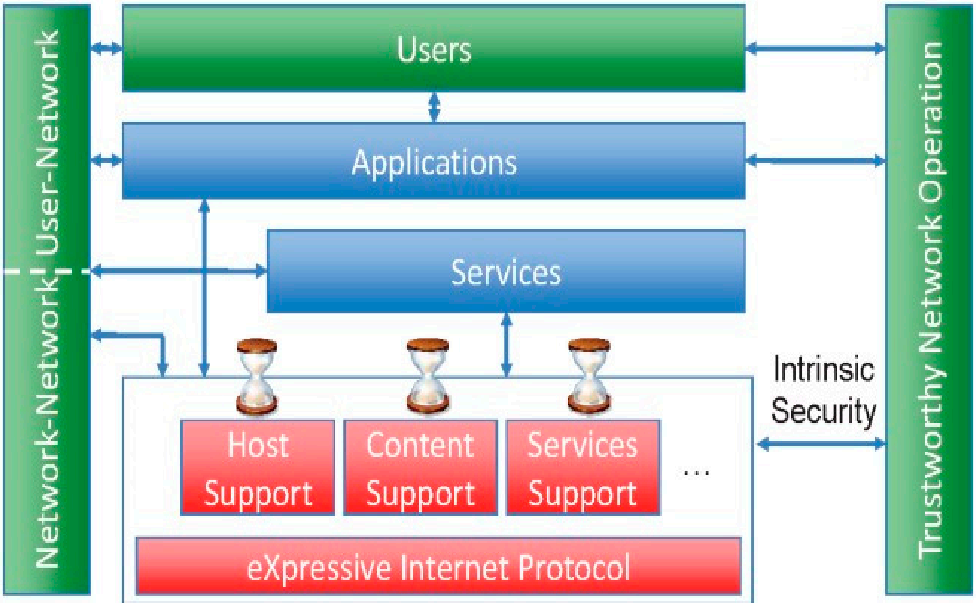


Figure 8. Expressive Internet Architecture (XIA) [48].

To understand the routing capabilities of the XIA architecture, it uses the expressive internet routing protocol (XIP) to replace the current IP routing protocol. XIA incorporates a narrow waist that resembles today's internet design but can support the latest application models with advanced technologies such as link, storage, and computation as they evolve. This architecture guarantees the authenticity of network communication [48]. XIA supports the key aspects of evolvability, intrinsic security, deployment over IP, debugging support, and flexible routing [49]. The XIA architecture follows three guiding principles:

- First, the important elements in a network, such as its communication, nodes, entities, underlying services, etc., must be supported by a growing set of principles for network communication.
- Second, the security of the network should be independent of the right external entities, such as configurations, actions, and databases.
- Third, the authors in [48] propose a paradigm shift of the narrow waist, incorporating all the necessary functions, which include access to service, hosts, content (principals), user interaction, and ISPs, to name a few.

3.3. Key Differences between Evolutionary and Clean-Slate Architectures

The internet has grown tremendously over the years, with different layers of abstraction and networking support provided by various protocols. However, it still faces challenges in supporting all the networking use cases, such as congestion management, mobility, security, QoS, and inter-domain routing. Despite the progress that has been made, these challenges limit the capabilities of the current internet [50]. As a result, there is a need for innovative approaches to network architectures that can address these limitations and provide a more flexible and secure platform for future applications.

The evolutionary approach holds the potential to offer solutions that enable new services and functionalities while preserving the existing internet architecture. This approach places emphasis on the significance of the context or environment in which a proposed architecture solution will be deployed, rather than designing entirely new protocols from scratch.

Research on clean-slate architecture has aimed to deliver services that meet the needs of users. For instance, Rexford J. et al. proposed that a clean-slate approach is the most effective solution for advancing the current internet architecture. In contrast, the evolutionary approach advocates for small, incremental modifications to the existing internet architecture that do not disrupt the existing protocols.

To pursue clean slate networking research that accommodates various resources, it is crucial to compare its performance with that of evolutionary research, which represents a completely different paradigm [23]. The clean-slate architecture addresses several key factors, including network security, scalability, mobility, and network management. For instance, NDN utilizes cryptographic signatures to sign each data packet, preserving the integrity and authenticity of the data for network security [51]. NEBULA uses reliable, trustworthy core networking with caching to achieve scalability [43]. Clean-slate approaches, such as NDN, use soft-state mechanisms that employ consumer and producer mobilities to achieve an overall implementation for the mobility [52]. Additionally, NEBULA incorporates software controllers into its design to support network functionality and makes use of the SDN principles that are a part of the evolutionary design for network management [42]. These comparisons reveal that clean-slate approaches provide reasonable solutions when compared to evolutionary models, which solely focus on protocol design for the current internet environment [53].

3.4. Research Projects from European Union and Asia

The European Union has initiated various programs, including the Future Internet Public–Private Partnership (FI-PPP) project, to promote the development of the future internet and sustain the evolvable network of societies for the future. The main objective of the FI-PPP project was to create new business models that could strengthen the European industry, in sectors such as software services, media, mobile devices, and telecommunications, among others [54]. The project was divided into three phases, as shown in Table 3.

Table 3. Phases of the FI-PPP project.

Phases	Foundation Laid	Aim and Scope	Testing and Evaluation
Phase I	May 2011–April 2014	FIWARE (To facilitate access to services, for ex., cloud hosting, IOT, data management, and security)	Infrastructure testing, evaluation of different use cases (different industry sectors)
Phase II	April 2013–March 2015	To develop core platform through the XIFI project and the implementation of FIWARE nodes	Large-scale use case pilots (energy domains, creative industry, smart manufacturing, to name a few)
		Setting up infrastructures to operate a European network of FIWARE nodes	
Phase III	September 2014–September 2016	FIWARE Accelerator Program (Primary focus was to attract entrepreneurs, start-ups, SME's)	Developing applications and services on various use cases
		Creating a stable infrastructure for the large-scale trials	Extensions of technological foundations
		Selecting 16 business accelerators	Launching the FIWARE Accelerator program with more than 1000 entrepreneurs, startups, and SMEs success
Joint Projects (FIBRE, Fed4FIRE)	January 2017–December 2021	FP7 as part of FI-PPP was introduced	Provided support for cloud-computing, SOA, and sensor networks

In addition to the FI-PPP project, the FP7 (a framework program for research and technological development) initiative has also supported various projects that aim to enhance platforms such as cloud computing, sensor networks, and service-oriented architectures (SOA). Furthermore, joint projects have been undertaken, such as FIBRE (Future Internet testbeds experimentation between Brazil and Europe) and Fed4FIRE (Federation for Future Internet Research and Experimentation), which began in January 2017 and ran until the end of December 2021 [55]. The Fed4FIRE+ project, is considered to be the successor of Fed4FIRE, was initiated in 2020, and is the world's largest association of Next Generation Internet (NGI) testbeds. It provides open, accessible, and reliable tools to serve a broad range of communities, including those that are involved in research and innovation, such as the 5G PPP projects [56].

Asian countries, such as China and Japan, have also leveraged their support towards the development of these architectures for the future internet. Japan has been active in wireless applications and devices, introducing next-generation standards. Japan collaborates with both the United States and the European Union on projects such as the New Generation Network (NWGN) and Next Generation (NXGN), which consider clean-slate and general internet protocol (IP) architectures, respectively. The NWGN was launched in 2010 to develop and enhance internet services by working on the underlying network technologies. It comprises several sub-projects that focus on architectural design, the design of testbeds, laboratories that support virtualization, and wireless testbeds for data-centric networking, service-oriented networks (SOA), and advanced mobility management. AKARI is one of Japan's largest research projects on these future internet technologies, which proposes an ID/locator split architecture [57] and uses clean-slate approaches, such as optical path and packet integration technologies [58,59], to achieve success for the new generation network. The AKARI architecture is based on three principles: simplicity, sustainability and self-evolvability, and a belief in the reality of the next generation internet. Additionally, JGN2plus and JGN-X: JGN2plus are two other projects that support testbeds for running these applications and networks.

China has been active in future internet architecture research, with a focus on IPv6-associated testbeds. However, recent reports [60] have suggested that China has built the largest Future Internet Test Infrastructure (FITI) to support the evolution of the future internet and its associated technologies, such as artificial intelligence and 5G. China has announced plans to make all network and terminal devices adaptable to IPv6 by 2025, with the goal of attracting major IPv6 users worldwide.

4. Metaverse

As a part of the next generation internet, the Metaverse is gaining a lot of attention and promises to provide a blend of 3D, immersive, virtual, and self-sustainable shared spaces for end-users to work, play, and socialize. It was originally proposed in Neal Stephenson's 1992 science fiction novel, *Snow Crash*, in which humans used digital avatars to compete and upgrade their statuses [61]. While the Metaverse brings a great deal of attention, the question of how to provide security for the user's digital content and data is of paramount importance. Blockchains offer promising solutions, and in the following sections, we will discuss what a blockchain is, and its role in the Metaverse and its applications. Using tools such as extended reality (XR), blockchains, and AI, the Metaverse can be seen as the next internet battleground. We will discuss some of the technical challenges, such as data privacy and interoperability, that the Metaverse faces, and see how blockchains come to its rescue. Although the Metaverse is still in its inception, there are some standards in place with fewer implementations.

The core technologies that are associated with the Metaverse are XR (AR and VR), digital twins, and blockchains. AR imposes digital information into the physical environment, whereas VR introduces users to a digital world experience [62]. Both AR and VR are very useful in the development of the Metaverse, for creating a digital space for users to interact with the real world. Digital twinning is the concept of using real-world data to predict the expected behavior of a real-world object, using a virtual twin [63,64]. On the other hand, Blockchains serve as a secure and decentralized repository for users to store their data in the Metaverse, ensuring the privacy and security of the user data. Additionally, they act as a system that connects the Metaverse's virtual world with the real world, allowing for interoperability between the two [65]. Additionally, future 6G wireless systems have the capability of providing greater computing powers, sensing, localization, and communication resources to achieve higher transmission speeds, which are essential for the Metaverse [66]. The applications of the Metaverse include online video conferencing, digital arts, and digital real estate.

4.1. Blockchain

The term "blockchain", initially conceived by Nakamoto Satoshi in 2008, refers to a distributed ledger. This ledger utilizes consecutive blocks that link to one another using hash values. Each block is assigned a timestamp, which is determined by comparing its value to the network time, the median of the timestamps, and two hours. Consensus protocols govern the regulation of the blockchain network, enabling the creation of new blocks. Bitcoin, the first generation of blockchains, utilizes a consensus protocol that employs a proof-of-work mechanism. However, this centralized mechanism consumes vast amounts of computing power and energy, resulting in a lower transaction rate. To address this, the proof-of-stake mechanism is employed, with the winner being determined based on their holdings in cryptocurrency, rather than their computing power [67].

A second-generation blockchain is named Ethereum, which incorporates smart contracts based on the specific rules that are embedded in the blockchain code. These smart contracts can be accessed by any application by triggering the necessary functions that are required, based on the application's needs. Ethereum utilizes standards such as ERC-1155 and ERC-721 to acquire the features that are constructed using NFTs (non-fungible tokens), gaining significant prominence in various application areas, such as sports, arts, medicine, and education, to name a few, with a market value of over USD 7 billion [68].

4.2. Role of Blockchain in Metaverse

A blockchain is a combination of peer-to-peer networks [32], modern cryptography, smart contracts, distributed storage mechanisms, which develops applications that support the exchange of data, processing capabilities, and storage mechanisms (see Figure 9). The decentralized nature of the blockchain enables it to identify certain undisclosable transactions, which introduces a new metaphor for using the Metaverse. As discussed in the previous section, blockchains use new blocks that are linked to one another as a chain, using cryptographic hash operations.

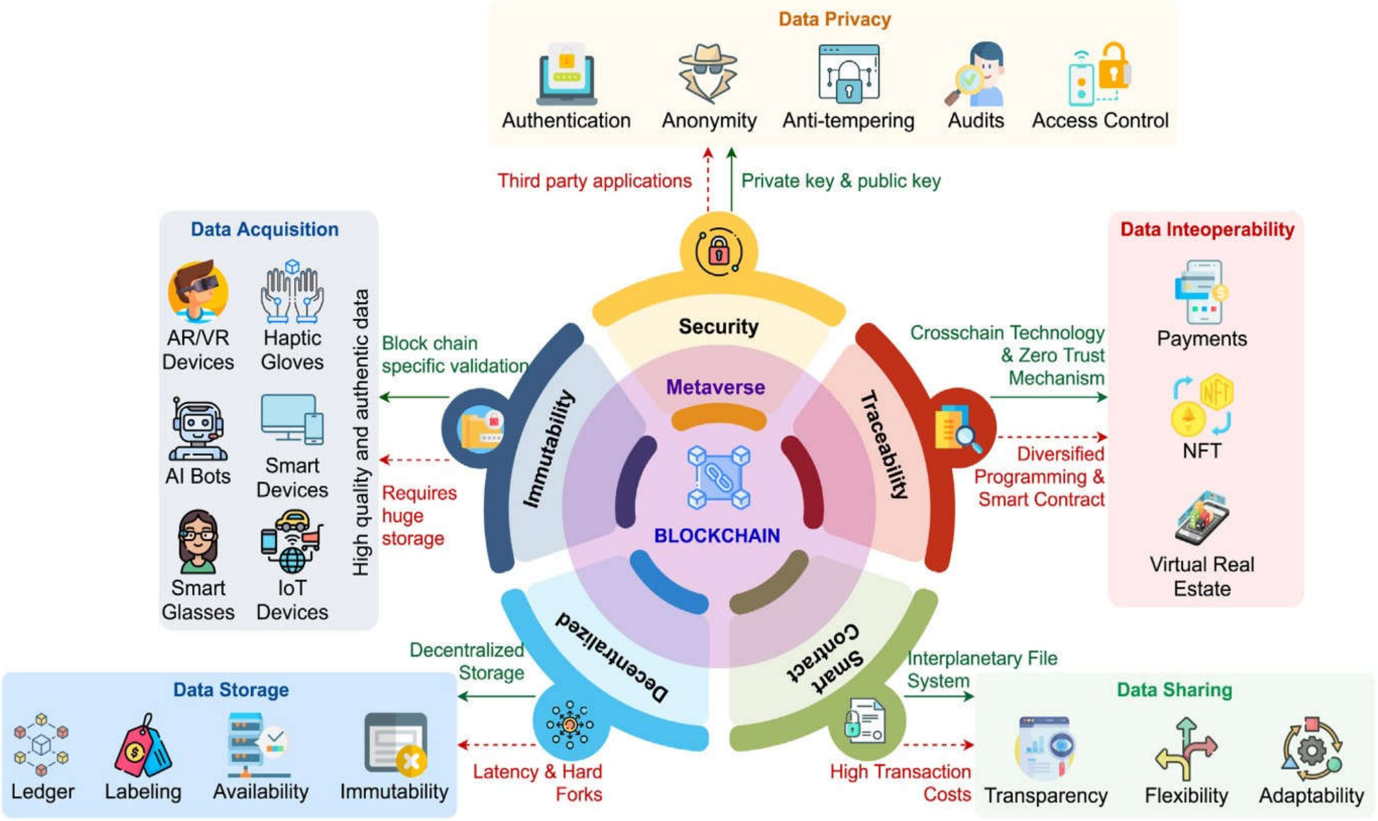


Figure 9. Blockchain: technical aspects in the Metaverse [19].

Using blockchains, money or assets can be transferred across all virtual worlds, allowing users to perform real-world activities, such as going on a vacation, attending concerts, and purchasing clothes on a virtual platform using the crypto-enabled Metaverse. Additionally, blockchains enable users to exhibit their creative aspects publicly, using a decentralized ecosystem. The Metaverse, an open-source architecture for blockchains, provides a user-friendly interface and includes digital wallets, ensuring the seamless integration of blockchain services into the Metaverse. This ensures data security, privacy, quality, secured data sharing, interoperability, smart contract deployment, and healthcare. All these attributes are discussed in detail in [19]. The primary focus of this article, however, is to explore the potential future of the internet as a service.

The state-of-the-art methods of blockchains for the Metaverse are illustrated in Figure 9. These methods [19] include data acquisition, storage, sharing, and interoperability. In the context of the Metaverse's ecosystem, the role of data acquisition is very crucial, as it has to deal with data that capture sensitive information, for example, biometric information, credit/debit card information, and an HD camera that captures the users' physical attributes, to name a few. Data acquisition plays an important role in training ML models to be able to acquire the decision-making capabilities, recommender system attributes, and marketing in the Metaverse [69]. The challenges of creating such a data acquisition system will impose several challenges in Metaverse, because of its huge accumulation of data. Blockchains can facilitate the acquisition of genuine data in the Metaverse, by utilizing distributed ledger technology that captures authentic records and data as transactions. Each activity is recorded as a transaction, and each block includes a cryptographic hash of the previous block, a timestamp, and the metadata [70]. This ensures that the data are immutable within a block and become resistant to attacks, making them tamper-proof. To prevent data duplication, the data that is obtained in the Metaverse undergo a blockchain-specific validation method that is powered by consensus mechanisms [71,72]. However, data acquisition in the Metaverse is limited in terms of obtaining high-quality and authentic data, and blockchains can help to overcome these constraints. Nonetheless, blockchains can be slow and take longer to complete a transaction, which can result in higher transaction fees. Additionally, the storage space depends on the amount of data that is acquired. Therefore, there is still a need for further research to develop a mature blockchain for the Metaverse that can address these issues.

The Metaverse requires vast amounts of data storage, as huge volumes of data are generated and continue to grow with the increasing number of people that are entering the Metaverse realm. Each user has their own data file, which grows significantly as their social interactions within the Metaverse increase. As the data accumulates, there is a need to move the data storage from the physical world to the Metaverse, once it becomes fully operational. This presents a significant challenge for deploying various Metaverse applications. However, blockchain technology can help by replicating the original data blocks throughout the chain, thus enhancing the reliability and transparency of the Metaverse [65].

Data sharing plays an imperative role in the Metaverse by allowing stakeholders to share the same platform, bringing together people and applications. The data that is obtained from various platforms, including AR, VR, and IoT devices in the Metaverse, can be utilized to create systems that are closely tied to a users' action. However, sharing data through these platforms poses several challenges, particularly in terms of the access to sensitive data. With several Metaverse applications dealing with real-time data, data flexibility may become an issue as the demand for real-time data increases in a data sharing environment. Blockchain technology can help by providing complete data control to the data owners and incorporating smart contracts to enhance the flexibility of this data sharing [73].

Data interoperability is the driving force behind the Metaverse, as various applications generate diverse data from fields such as healthcare, gaming, finance, and more. These applications facilitate the communication and information exchange within the Metaverse. It is crucial that digital world applications can communicate with one another, regardless of their underlying technologies. However, the main limitation to the Metaverse interoperability is managing the communication between the virtual worlds in a reasonable manner [74]. Blockchain technology plays a significant role in enabling the exchange of possessions, such as avatars, NFTs, and payments, between virtual worlds, as depicted in Figure 9. This interoperability between virtual worlds can be achieved using cross-blockchain technology [75], which eliminates the need for intermediaries in the Metaverse. However, the main roadblock in achieving this cross-blockchain-enabled Metaverse interoperability is the presence of several public blockchains in different virtual worlds that share different languages. Additionally, different platforms offer varying levels of smart contract capabilities, making adaptation difficult. Furthermore, the consensus processes and transaction architecture that are used in these virtual worlds vary considerably, which limits the data interoperability [76].

4.3. Effect of Blockchain on AI in Metaverse

However, a blockchain has the potential to enhance key enabling technologies, such as AI, IoT, and big data, in the Metaverse, enabling people to participate in socio-economic activities. Through decentralized marketplaces, blockchains can support various AI components, including datasets, algorithms, and computing power, making it possible to adopt and innovate AI to a level never seen before in the context of the Metaverse [77]. However, while AI and blockchains are fundamental to building scalable, reliable, and efficient tools for the Metaverse, this technology is still in its infancy. It can be challenging to trace the possession of AI-fueled material in the Metaverse, and users may fall prey to the illegal exploitation of resources when engaging AI technologies to draw into the Metaverse interactions [78]. Additionally, AI systems are bound to make errors, which may cause people to lose trust in the Metaverse.

4.4. Metaverse Projects

Decentraland [79], Sandbox [80], Axie Infinity [81], and Illuvium [82], which are seen in Table 4, are examples of Metaverse projects that use blockchains as the technology for the Metaverse, with a range of services that cover several areas of the virtual world.

Table 4. Metaverse projects.

Metaverse Projects	Platform	Services	Digital Assets and Features
Decentraland [79]	Virtual Reality	Users can create economic assets with its applications	Uses Ethereum Request for Comments (ERC-20) tokens and Ethereum Name Service (ENS) for ownership
		Not supervised by one central entity/organization and promises a sense of ownership to the digital real estate based on the Ethereum blockchain	Enables content creation, advertising, chat groups, and multiplayer games, applications that support dynamic 3D scenes
Sandbox [80]	Virtual Reality (Inspired by Minecraft, Roblox)	Users can own, construct, and gain monetary benefits for game services	Supports Interplanetary File System to save the digital assets without requiring the permission of owner.
		Upgrades the gaming experience from a 2D to 3D world using a voxel gaming platform	Uses native platform utility token with ERC-20
		Allows users to create 3D animated objects using the real-world object entities. VoxEdit, is a built-in voxel gaming package for 3D animated object.	Scalability is the important issue
Axie Infinity [81]	User-centric	Allows players to collect, raise, breed, and battle for creating their Axies kingdoms	Uses ERC-20 token of the Axie metaverse
		Players can own, purchase, sell, and trade-in gaming resources	Ronin is an Ethereum-linked side chain to process the transactions
		Enables players to enjoy different play modes, for example, player versus player and player versus environment and several tournaments that generates monetary benefits	Uses a secondary token called Small Love Position, awarded to players
Illuvium [82]	Ethereum blockchain	Provides an entertainment source for users on a decentralized platform using a varied collection of trade features	Uses immutable X, an Ethereum scaling solution that uses layer-2 with Zero-knowledge rollup
		This game combines both open-world game exploration and a player vs. player battle game, wherein players can use different games	It focuses on three important scenarios: rewarding players for success, presenting players a private wallet distribution, participation in governance activities via decentralized autonomous organization

4.5. Technical Challenges of Blockchain in Metaverse

As the number of users and transactions in the Metaverse increases, the blockchain network faces challenges with respect to scalability and transaction costs. The number of blocks in the blockchain increases as more users join the network, requiring significant computing resources [83]. Additionally, the shared transactions in the network result in users incurring high transaction costs, which are needed for validation. Future generations of blockchains will be needed to address these challenges and facilitate efficient data sharing in the Metaverse. There are several challenges that need prime focus to achieve this goal:

i. Scalability

Firstly, scalability is a major challenge and requires new technologies such as data sharding, sidechains, or off-chain solutions to improvise the network transaction throughput.

ii. Data Interoperability

The lack of decentralized platforms restricts the scope of users in terms of data interoperability. Furthermore, the transfer of NFTs to different environments is also limited. The use of virtual-world applications relies on their interconnectivity, which poses certain limitations. A cross-chain protocol serves as an alternate solution to ensuring data interoperability [84,85]. This protocol allows for all forms of transactions in the Metaverse, without the need for intermediaries. Blockchains enable applications to connect seamlessly in the Metaverse, simplifying the experience for end-users. Data interoperability is critical, as different Metaverse projects may use different blockchain platforms and protocols, which can make it difficult for users and assets to move between these different platforms. Solutions such as cross-chain bridges must be developed to enable seamless data and asset transfers across the different Metaverse platforms.

iii. Data Privacy

The complexity of the Metaverse framework can be daunting for users, as bad actors can gain access to sensitive data. Attackers may use AI bots to pretend to be genuine users during transaction dealings. One potential solution to the challenge of dealing with large volumes of data is integrating reliable Metaverse information. Blockchain technology can give Metaverse users control over their data, using public/private keys that guarantee their ownership and protect them from third-party interference. Blockchain ledgers commonly feature an audit trail that ensures that the transactions in the Metaverse are reliable and absolute. The adoption of zero-knowledge proof technology in blockchains enables users to smoothly access actual data in the Metaverse while maintaining the ownership and privacy of their assets.

iv. Data Security

Finally, as the value of the assets and data in the Metaverse grows, security has become paramount. Robust security measures, such as multi-factor authentication, encryption, and smart contract audits, must be implemented to ensure the integrity and confidentiality of the data and assets in the Metaverse.

5. Potential Benefits and Challenges of Future Internet Research

The future internet continues to evolve as potential technologies continue to emerge. These technologies could transcend the way we see and use the internet in the future. The role of blockchains in the organization and progress of the applications and services within the Metaverse has been discussed in this article as part of the emerging future internet. Technologies such as the Internet of Things (IoT), vehicular communications, artificial intelligence (AI), future 6G networks, and quantum computing serve as few other examples that have the potential to revolutionize the next phase of the future internet. 6G networks, as the considered successors to 5G networks, are currently under development and are expected to offer more promising speeds than 5G, to provide support towards experiencing immersive applications such as AR and VR, and to perform remote surgeries and AI-enabled autonomous driving. As AI advances in the future, it is expected to revolutionize the development of newer applications to improve business productivity, decision making capabilities, and healthcare outcomes. Quantum computing is another important aspect of the future internet and is expected to revolutionize fields such as drug discovery and cryptography, etc. Vehicular communications are a rapidly evolving field that seeks to address technological, societal, and standardization challenges. It is seen that efforts are currently underway [13] to integrate SDN and network function virtualization (NFV) with fog computing. The market for internet-connected vehicles is rapidly growing and it is predicted that companies will be using such vehicles in some form by the end of 2023.

Along with the above-mentioned benefits, there are several challenges that need to be addressed along the way in creating a future internet that is safe, more reliable, and secure. For example, there is a need to enforce stronger privacy regulations and to provide end-user control of user data, as vast amount of user data is generated by technologies such as AI and the IoT, which raises concerns regarding user privacy and security. There is a need to design and develop robust security features to fight against cyber-attacks in an environment of increased data transmission. The energy consumption of the future internet is likely to rise with the increasing use of connected devices and data centers. The sustainable development of technologies that support energy efficiency is needed to resolve this problem. This sustainable development of AI and other related technologies may raise several ethical issues such as potential bias, accountability, and transparency. Therefore, by addressing these concerns, one can have a new face of the future internet that is safe, secure, and accessible to everyone.

6. Conclusions and Research Directions

The article presents a comprehensive review of various papers on the topic of Future Internet architecture (FIA), which suggests that the research on the topic depends on its technical and geographical diversity and can be approached from various research dimensions. The research programs that are related to the design and evolution of the future internet, which have been established in various countries, such as the United States, Europe, Japan, and China, have primarily focused on several key paradigms. These include routing and addressing capabilities, which are essential for the growth of the internet, as well as the development of a multi-protocol architecture that can support both TCP/IP and OSI protocols. However, this approach can impose technical problems and requires a proper plan to address these issues. In addition, a security architecture is needed to provide security to both the TCP/IP and OSI protocol suites, which can be challenging unless the architecture is built from scratch. Furthermore, the architecture should provide extended support to real-time applications, such as audio and video, to ensure proper traffic control and state. Finally, advanced applications must be developed to address the challenges that are posed by the growth of the communication mechanism and the need to innovate in the development of various types of applications.

The second half of the paper presents the Metaverse and blockchains and investigates the key role of these blockchains in the organization and progress of the applications and services within the Metaverse. The impact of blockchains on AI in the Metaverse is also examined, along with the technical challenges and opportunities for improvement. Additionally, the potential benefits and challenges of future internet research are also discussed. Apart from this, there are numerous potential research directions for the future of the internet. The emergence of AR, VR, and MR promises to revolutionize how users interact with technology, creating new opportunities for immersive experiences and innovation; therefore, this opens several avenues for potential research into next-generation mobile applications. For instance, edge computing is an exciting area of research that seeks to address the gap between the hardware capacity of mobile devices and the resource demands of various mobile applications, given the constraints of battery life. Although 5G networks offer a low latency and high bandwidth, achieving a high throughput with a low latency while maintaining scalability, security, and decentralization remains an important challenge [86]. It is seen that the nodes within a blockchain architecture adhere to a protocol, namely the consensus algorithm, to perform a validation of the new transaction blocks. Innovative consensus algorithms, such as proof-of-capability, proof-of-burn, and leased proof-of-stake, are being developed to overcome these issues. Furthermore, blockchain networks that support applications and services across various organizations, including government departments, are becoming increasingly popular. Connecting current and new blockchains will be crucial for scaling the development of the Metaverse and future technologies, requiring a focus on interoperability and network management to ensure seamless communication among different blockchain networks.

Author Contributions: Conceptualization, S.A.M. and A.L.R.; Methodology, S.A.M.; Software, S.A.M.; Validation, S.A.M.; Formal Analysis, S.A.M.; Investigation, S.A.M.; Resources, S.A.M.; Data Curation, S.A.M.; Writing—original draft preparation, S.A.M.; Writing—Review and Editing, S.A.M. and A.L.R.; Supervision, A.L.R.; Project Administration, A.L.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Montpetit, M.J.; Fdida, S.; Wang, J. Future Internet: Architectures and Protocols. *IEEE Commun. Mag.* **2019**, *57*, 12. [CrossRef]
2. DataReportal. Available online: https://datareportal.com/global-digital-overview (accessed on 26 March 2023).
3. Digital Life in 2025. Available online: https://www.pewresearch.org/internet/2014/03/11/digital-life-in-2025/ (accessed on 26 March 2023).
4. Bahtar, A.Z.; Muda, M. The Impact of User–Generated Content (UGC) on Product Reviews towards Online Purchasing—A Conceptual Framework. In Proceedings of the Fifth International Conference on Marketing and Retailing (5th INCOMaR), Penang, Malaysia, 12–13 October 2015; Elsevier: Amsterdam, The Netherlands, 2015.
5. Dwivedi, Y.K.; Ismagilova, E.; Hughes, D.L.; Carlson, J.; Filieri, R.; Jacobson, J.; Jain, V.; Karjaluoto, H.; Kefi, H.; Krishen, A.S.; et al. Setting the future of digital and social media marketing research: Perspectives and research propositions. *Int. J. Inf. Manag.* **2021**, *59*, 102168. [CrossRef]
6. Pan, J.; Paul, S.; Jain, R. A survey of the research on future internet architectures. *IEEE Commun. Mag.* **2011**, *49*, 26–36. [CrossRef]
7. Rexford, J.; Constantine Dovrolis. Future Internet Architecture: Clean-Slate Versus Evolutionary Research. *Commun. ACM* **2010**, *53*, 36–40. [CrossRef]
8. Wan, M.; Yin, S. Future internet architecture and cloud ecosystem: A survey. In Proceedings of the AIP Conference Proceedings 1955, 040130, Xian, China, 20–21 January 2018; American Institute of Physics: College Park, MD, USA, 2018.
9. Paul, S.; Pan, J.; Jain, R. Architectures for the Future Networks, and the Next Generation Internet: A Survey. *Comput. Commun.* **2011**, *34*, 2–42. [CrossRef]
10. Ben-Ammar, H.; Ghamri-Doudane, Y. An ICN-based Approach for Service Caching in Edge/Fog Environments. In Proceedings of the IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; pp. 1–6.
11. Pham, X.-Q.; Nguyen, T.-D.; Nguyen, V.; Huh, E.-N. Joint Service Caching and Task Offloading in Multi-Access Edge Computing: A QoE-Based Utility Optimization Approach. *IEEE Commun. Lett.* **2021**, *25*, 965–969. [CrossRef]
12. Pi, L.; Wang, L. Secure Bootstrapping and Access Control in NDN-based Smart Home Systems. In Proceedings of the IEEE INFOCOM 2018, Honolulu, HI, USA, 15–19 April 2018.
13. SkyQuest. Internet of Vehicles Market to Hit Sales of 448.16 Billion by 2028 | Internet-Connected Vehicles to Save Up to $8.4 Billion in Manufacturing Costs Over the Next 10 Years, Aug. 2022. Available online: https://www.globenewswire.com/en/news-release/2022/08/24/2503946/0/en/Internet-of-Vehicles-Market-to-Hit-Sales-of-448-16-billion-by-2028-Internet-connected-vehicles-to-Save-Up-to-8-4-Billion-in-Manufacturing-Costs-Over-the-Next-10-Years-SkyQuest.html (accessed on 26 March 2023).
14. The Metaverse in 2040. Available online: https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/ (accessed on 26 March 2023).
15. Ranaweera, P.; Liyanage, M.; Jurcut, A.D. Novel MEC Based Approaches for Smart Hospitals to Combat COVID-19 Pandemic. *IEEE Consum. Electron. Mag.* **2021**, *10*, 80–91. [CrossRef]
16. Bisogni, C.; Iovane, G.; Landi, R.E.; Nappi, M. ECB2: A novel encryption scheme using face biometrics for signing blockchain transactions. *J. Inf. Secur. Appl.* **2021**, *59*, 102814. Available online: https://www.sciencedirect.com/science/article/pii/S2214212621000545 (accessed on 26 March 2023). [CrossRef]
17. Bouri, E.; Saeed, T.; Vo, X.V.; Roubaud, D. Quantile connectedness in the cryptocurrency market. Journal of International Financial Markets. *Inst. Money* **2021**, *71*, 101302. [CrossRef]

18. Wang, S.; Qureshi, M.A.; Miralles-Pechuaán, L.; Huynh-The, T.; Gadekallu, T.R.; Liyanage, M. Explainable AI for B5G/6G: Technical aspects, use cases, and research challenges. *arXiv* **2021**, arXiv:2112.04698.
19. Gadekallu, T.R.; Huynh-The, T.; Wang, W.; Yenduri, G.; Ranaweera, P.; Pham, Q.V.; da Costa, D.B.; Liyanage, M. Blockchain for the metaverse: A Review. *Future Gener. Comput. Syst.* **2023**, *143*, 401–419.
20. Data Plane. Available online: https://www.techtarget.com/searchnetworking/definition/data-plane-DP#:~:text=The%20data%20plane%20(sometimes%20known,components%20of%20a%20telecommunications%20architecture (accessed on 26 March 2023).
21. CloudFlare. Available online: https://www.cloudflare.com/learning/network-layer/what-is-the-control-plane/ (accessed on 26 March 2023).
22. Software Defined Networking. Available online: https://en.wikipedia.org/wiki/Software-defined_networking (accessed on 26 March 2023).
23. Xia, W.; Wen, Y.; Foh, C.H.; Niyato, D.; Xie, H. A Survey on Software-Defined Networking. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 27–51. [CrossRef]
24. Open Networking Foundation (ONF). Available online: https://www.opennetworking.org (accessed on 26 March 2023).
25. CORD. Available online: https://opennetworking.org/cord/ (accessed on 26 March 2023).
26. CORD. Available online: https://wiki.opennetworking.org/display/COM/CORD (accessed on 26 March 2023).
27. Open Network Operating System. Available online: https://opennetworking.org/onos/ (accessed on 26 March 2023).
28. VMWare, Why Network Functions Virtualization? Available online: https://www.vmware.com/topics/glossary/content/network-functions-virtualization-nfv.html#:~:text=NFV%20allows%20for%20the%20separation,and%20without%20installing%20new%20hardware (accessed on 26 March 2023).
29. Shamugam, V.; Murray, I.; Leong, J.A.; Sidhu, A.S. Software Defined Networking challenges and future direction: A case study of implementing SDN features on OpenStack private cloud. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Bali, Indonesia, 19–20 March 2016.
30. Alshamrani, A.; Guha, S.; Pisharody, S.; Chowdhary, A.; Huang, D. Fault Tolerant Controller Placement in Distributed SDN Environments. In Proceedings of the IEEE International Conference on Communications, ICC 2018, Kansas City, MO, USA, 20–24 May 2018.
31. Li, Y.; Zhang, D.; Taheri, J.; Li, K. SDN components and OpenFlow. *Big Data Softw. Defin. Networks* **2018**, *12*, 49–67. Available online: http://www.cs.newpaltz.edu/~lik/publications/Yanbiao-Li-BDSDN-2018.pdf (accessed on 10 March 2023).
32. Ahmed, M.S. Achieving QoS in media streaming for peer-peer networks. In Proceedings of the International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 3–5 March 2016; pp. 3694–3698.
33. Napster. Available online: https://en.wikipedia.org/wiki/Napster (accessed on 26 March 2023).
34. Clark, D.; Lehr, B.; Bauer, S.; Faratin, P.; Sami, R.; Wroclawski, J. Overlay Networks, and the Future of the Internet. *J. Commun. Strateg.* **2006**, *63*, 109.
35. Jianping, W.; Lili, L.; Dan, L. The road towards future Internet. *J. Commun. Inf. Netw.* **2016**, *1*, 86–97. [CrossRef]
36. Zhang, L.; Estrin, D.; Burke, J.; Jacobson, V.; Thornton, J.D.; Smetters, D.K.; Zhang, B.; Tsudik, G.; Massey, D.; Papadopoulos, C. Named Data Networking (NDN) Project, NDN-0001. 2010. Available online: https://named-data.net/techreport/TR001ndn-proj.pdf (accessed on 26 March 2023).
37. Zhang, L.; Claffy, K.C.; Crowley, P.; Afanasyev, A.; Jacobson, V.; Wang, L.; Zhang, B.; Jeffrey, B. Named Data Networking. ACM SIGCOMM Computer Communication Review, *44*, 66–74. Available online: http://www.sigcomm.org/sites/default/files/ccr/papers/2014/July/0000000-0000010.pdf (accessed on 26 March 2023).
38. Yuan, H.; Song, T.; Crowley, P. Scalable NDN Forwarding: Concepts, Issues and Principles. In Proceedings of the 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, 30 July–2 August 2012; pp. 1–9.
39. Ivan, S.; Kiran, N.; Sam, N.; Dipankar, R. MobilityFirst future internet architecture project. In Proceedings of the 7th Asian Internet Engineering Conference (AINTEC' 11), Bangkok, Thailand, 1–3 November 2011; ACM: New York, NY, USA, 2011.
40. Chaudhuri, D.R.; Martin, R.; Yates, R.; Zhang, Y.; Trappe, W. *The Next-Phase MobilityFirst Project-From Architecture and Protocol Design to Advanced Services and Trial Deployments*; Rutgers University: Piscataway, NJ, USA, 2018. Available online: https://www.nsf.gov/awardsearch/showAward?AWD_ID=1345295&HistoricalAwards=false (accessed on 10 March 2023).
41. Zhang, Y. MobilityFirst Future Internet Architecture. WINLAB, Rutgers University. Available online: http://eceweb1.rutgers.edu/~yyzhang/talks/MobilityFirst_summer.pdf (accessed on 26 March 2023).
42. Anderson, T.; Birman, K.; Broberg, R.; Caesar, M.; Comer, D.; Cotton, C.; Freedman, M.J.; Haeberlen, A.; Ives, Z.G.; Krishnamurthy, A.; et al. A brief overview of the NEBULA future internet architecture. *SIGCOMM Comput. Commun. Rev.* **2015**, *44*, 81–86. [CrossRef]
43. Galis, A.; Gavras, A. (Eds.) *The Future Internet–Future Internet Assembly 2013: Validated Results and New Horizons*; Springer: Berlin/Heidelberg, Germany, 2013.
44. Gupta, T.; Leners, J.B.; Aguilera, M.K.; Walfish, M. Exposing network failures to end-host applications for improved availability. In Proceedings of the NSDI'13, Lombard, IL, USA, 2–5 April 2013.
45. Naous, J.; Walfish, M.; Nicolosi, A.; Mazieres, D.; Miller, M.; Seehra, A. Verifying and enforcing network paths with ICING. In Proceedings of the Seventh Conference on Emerging Networking Experiments and Technologies, Tokyo, Japan, 6–9 December 2011.
46. Liu, V.; Han, S.; Krishnamurthy, A.; Anderson, T. Tor instead of IP. In Proceedings of the 10th ACM Workshop on Hot Topics in Networks (HotNets), Cambridge, MA, USA, 14–15 November 2011.

47. Anand, A.; Dogar, F.; Han, D.; Li, B.; Lim, H.; Machado, M.; Wu, W.; Akella, A.; Andersen, D.G.; Byers, J.W.; et al. XIA: An architecture for an evolvable and trustworthy internet. In Proceedings of the 10th ACM Workshop on Hot Topics in Networks (HotNets), Cambridge, MA, USA, 14–15 November 2011.
48. The eXpressive Internet Architecture: Architecture and Research Overview, funded by the NSF under awards. Available online: https://www.cs.cmu.edu/~xia/xia-overview/xia-overview.pdf (accessed on 26 March 2023).
49. Mukerjee, M.; Naylor, D.; Steenkiste, P.; Andersen, D.; Eckhardt, D.; Kiesler, S.; Peha, J.; Perrig, A.; Seshan, S.; Sirbu, M.; et al. eXpressive Internet Architecture: GEC 15 Demo. Available online: https://davidtnaylor.com/XIA-GEC15.pdf (accessed on 26 March 2023).
50. Rudra, B. *Flexible Network Architectures Security: Principles and Issues*, 1st ed.; Auerbach Publications: Boca Raton, FL, USA, 2018.
51. Venkataramani, A.; Kurose, J.F.; Raychaudhuri, D.; Nagaraja, K.; Mao, M.; Banerjee, S. MobilityFirst: A mobility-centric and trustworthy internet architecture. *SIGCOMM Comput. Commun. Rev.* **2014**, *44*, 74–80. [CrossRef]
52. Francis, P.; Gummadi, R. IPNL: A NAT-extended internet architecture. *ACM SIGCOMM Comput. Commun. Review.* **2001**, *31*, 69–80. [CrossRef]
53. Taran, D.N. Lavrov. Future Internet Architecture: Clean-Slate Vs Evolutionary Design. *Math. Struct. Model.* **2016**, *39*, 142–151.
54. Future Internet PPP. Available online: https://www.fi-ppp.eu/ (accessed on 26 March 2023).
55. Future Internet Research and Experimentation. Available online: https://en.wikipedia.org/wiki/Future_Internet_Research_and_Experimentation (accessed on 26 March 2023).
56. Federation for Fire Plus. Available online: https://www.fed4fire.eu/ (accessed on 26 March 2023).
57. Kafle, V.P.; Inoue, M.; Harai, H. ID-based New Generation Network research in AKARI Project. In Proceedings of the Digest of the 9th International Conference on Optical Internet, Jeju, Republic of Korea, 11–14 July 2010; pp. 1–3.
58. Harai, H. Optical packet and path integration for energy savings towards new generation network. In Proceedings of the International Symposium on Applications and the Internet (SAINT), Turku, Finland, 28 July–1 August 2008; pp. 389–392.
59. Miyazawa, T.; Furukawa, H.; Fujikawa, K.; Wada, N.; Harai, H. Partial implementation and experimental demonstration of an integrated optical path and packet node for new generation networks. In Proceedings of the Optical Fiber Communication Conference (OFC), San Diego, CA, USA, 21–25 March 2010.
60. China builds world's largest internet test facility backbone network. Available online: https://www.globaltimes.cn/page/202104/1221584.shtml (accessed on 26 March 2023).
61. Stephenson, N. *Snow Crash: A Novel*; Del Rey Books: New York, NY, USA, 2003.
62. Koutitas, G.; Smith, S.; Lawrence, G. Performance evaluation of AR/VR training technologies for EMS first responders. *Virtual Real.* **2021**, *25*, 83–94. [CrossRef]
63. Tao, F.; Zhang, H.; Liu, A.; Nee, A.Y. Digital twin in industry: State-of-the-art. *IEEE Trans. Ind. Inform.* **2018**, *15*, 2405–2415. [CrossRef]
64. Alazab, M.; Khan, L.U.; Koppu, S.; Ramu, S.P.; Iyapparaja, M.; Boobalan, P.; Baker, T.; Maddikunta, P.K.R.; Gadekallu, T.R.; Aljuhani, A. Digital twins for healthcare 4.0-recent advances, architecture, and open challenges. *IEEE Consum. Electron. Mag.* **2022**. [CrossRef]
65. Jeon, H.J.; Youn, H.C.; Ko, S.M.; Kim, T.H. Blockchain and AI meet in the metaverse. In *Advances in the Convergence of Blockchain and Artificial Intelligence*; BoD–Books on Demand: Norderstedt, Germany, 2022; p. 73.
66. Tang, F.; Chen, X.; Zhao, M.; Kato, N. The Roadmap of Communication and Networking in 6G for the Metaverse. *IEEE Wirel. Commun.* **2022**. [CrossRef]
67. Thomsen, S.E.; Spitters, B. Formalizing nakamoto-style proof of stake. In Proceedings of the IEEE 34th Computer Security Foundations Symposium (CSF) (Virtual), Dubrovnik, Croatia, 21–24 June 2021.
68. Nadini, M.; Alessandretti, L.; Di Giacinto, F.; Martino, M.; Aiello, L.M.; Baronchelli, A. Mapping the NFT revolution: Market trends, trade networks, and visual features. *Sci. Rep.* **2021**, *11*, 20902. [CrossRef]
69. Wang, F.Y.; Qin, R.; Wang, X.; Hu, B. MetaSocieties in metaverse: MetaEconomics and MetaManagement for MetaEnterprises and MetaCities. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 2–7. [CrossRef]
70. Luo, Y.; Su, Z.; Zheng, W.; Chen, Z.; Wang, F.; Zhang, Z.; Chen, J. A novel memory-hard password hashing scheme for blockchain-based cyber-physical systems. *ACM Trans. Int. Technol.* **2021**, *21*, 1–21. [CrossRef]
71. Bouraga, S. A taxonomy of blockchain consensus protocols: A survey and classification framework. *Expert Syst. Appl.* **2021**, *168*, 114384. [CrossRef]
72. Lashkari, B.; Musilek, P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access* **2021**, *9*, 43620–43652. [CrossRef]
73. Dotan, M.; Pignolet, Y.A.; Schmid, S.; Tochner, S.; Zohar, A. Survey on blockchain networking: Context, state-of-the-art, challenges. *ACM Comput. Surv.* **2021**, *54*, 1–34. [CrossRef]
74. Mystakidis, S. Metaverse. *Encyclopedia* **2022**, *2*, 486–497. [CrossRef]
75. Jabbar, R.; Fetais, N.; Krichen, M.; Barkaoui, K. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In Proceedings of the IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), Doha, Qatar, 2–5 February 2020; pp. 310–317.

76. Wibowo, S.; Sandikapura, T. Improving data security, interoperability, and veracity using blockchain for one data governance, case study of local tax big data. In Proceedings of the International Conference on ICT for Smart Society (ICISS) (Virtual), Bandung, Indonesia, 19–20 November 2019; IEEE: New York, NY, USA, 2019; Volume 7, pp. 1–6.
77. Yang, Q.; Zhao, Y.; Huang, H.; Xiong, Z.; Kang, J.; Zheng, Z. Fusing Blockchain and AI With Metaverse: A Survey. *IEEE Open J. Comput. Soc.* **2022**, *3*, 122–136. [CrossRef]
78. Wiederhold, B.K. Ready (or not) player one: Initial musings on the metaverse. *Cyberpsychology Behav. Soc. Netw.* **2022**, *25*, 1–2. [CrossRef]
79. Decentraland. Available online: https://decentraland.org/ (accessed on 26 March 2023).
80. Sandbox. Available online: https://www.sandbox.game/en/ (accessed on 26 March 2023).
81. Axie Infinity. Available online: https://axieinfinity.com/ (accessed on 26 March 2023).
82. Illuvium. Available online: https://www.illuvium.io/ (accessed on 26 March 2023).
83. Gao, Y.; Wu, W.; Si, P.; Yang, Z.; Yu, F.R. B-ReSt: Blockchain-enabled resource sharing and transactions in fog computing. *IEEE Wirel. Commun.* **2021**, *28*, 172–180. [CrossRef]
84. Belchior, R.; Vasconcelos, A.; Guerreiro, S.; Correia, M. A survey on blockchain interoperability: Past, present, and future trends. *ACM Comput. Surv.* **2021**, *54*, 1–41. [CrossRef]
85. Madine, M.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Arshad, J.; Yaqoob, I. appXchain: Application-level interoperability for blockchain networks. *IEEE Access* **2021**, *9*, 87777–87791. [CrossRef]
86. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.