OULUN AMMATTIKORKEAKOULU

Ha Quyen

THE EVOLUTION OF WEB

THE EVOLUTION OF WEB

Ha Quyen
Bachelor’s Thesis
Spring 2023
Degree Programme in Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Degree Programme in Information Technology

Author(s): Ha Quyen
Title of the thesis: The Evolution of Web
Thesis examiner(s): Jouni Juntunen
Term and year of thesis completion: Spring 2023 Pages: 45

The World Wide Web (WWW) has undergone several eras over its lifetime. The arrival of Web3 marks a new chapter in the growth of WWW. This thesis aims to provide an overview of the growth of the WWW and to delve into Web3, the technological aspect of Web 3.0. The study covers the technical workings of Web3, its applications, importance, and limitations.

Specifically, Web 3.0, based on blockchain technology, allows for direct peer-to-peer interactions without intermediaries, breaking away from large companies ‘centralized control over services and information. This makes Web 3.0 both an evolution of Web 2.0 and a paradigm shift that may fundamentally change how industries function and people interact online. Next, the workings of Web3 are described by utilizing three primary components, namely, front end, back end, and data storage. The applications of Web3, such as decentralized finance (DeFi), non-fungible tokens (NFTs), decentralized autonomous organizations (DAOs), and Metaverse, are subsequently focused upon. Additionally, the importance and significant challenges encountered by Web3 are emphasized. Finally, the current status of Web 2.0 and the future of Web 3.0 are discussed.

The study was conducted through a thorough process of gathering information from various sources, including academic journals, books, online articles, and other relevant documents related to the WWW. This thesis offers valuable insights for readers interested in gaining a comprehensive understanding of the history of the WWW, particularly Web3.

Keywords: World Wide Web, Web 2.0, Web 3.0, Web3, blockchain, decentralization, smart contract

PREFACE

This Bachelor's Thesis was submitted to Oulu University of Applied Sciences as a part of the degree requirements for a Bachelor of Engineering in Information Technology. As a web development student, I believe it is essential to have a comprehensive understanding of the history of the World Wide Web. This thesis was born out of my curiosity about the evolution of websites, specially Web3, and the role they play in shaping the modern digital landscape.

I would like to express my deep appreciation to my thesis supervisor, Mr. Jouni Juntunen, for his patience, advice, and guidance during the thesis process. Additionally, I extend a special thank you to Ms. Sari Alatalo for meticulously checking the grammar in my thesis.

This work would not exist without the incredible support, encouragement, and love of my family. Extra thank is given to my close friends.

Last but not least, Thuan. You kept me motivated throughout the research and writing process. I appreciate you.

Tampere, 6.2.2023
Ha Quyen

CONTENTS

1 INTRODUCTION

In the past, we had to wait for messages for days or even months. Thanks to the giant leap in technology, people have many more efficient options at their fingertips to connect with society. With a few clicks of our fingers, we can now send a message or email to every corner of the world in seconds. The introduction of the Internet and the World Wide Web (WWW) has been considered one of the most crucial advancements in the grand scheme of human history. About five billion people worldwide- around 63.1% of the global population- use the Internet (Statista Research Department 2022). However, most of them need to be aware of the difference between the term Internet and the WWW or the website version they use.

The term "World Wide Web" (known as the web) has become so popular that most people think it is synonymous with the Internet, but in reality, they describe different concepts. The Internet is a worldwide telecommunication system providing connectivity for millions of networks to share information, transit, and communicate. Still, WWW is a typical way to access information on the Internet through a collection of websites displayed by web browsers and stored on web servers.

While Tim Berners-Lee, a British computer scientist, was working at European Council for Nuclear Research (CERN), he realized that because of the lack of reliable information-sharing system tools, his colleagues could not exchange the data and results of their experiments with each other (Choudhury 2014,1). In 1989, his proposal for the WWW was submitted. In 1990, along with Robert Cailliau, a Belgian computer scientist, Berners-Lee proposed to use hypertext "--to link and access information of various kinds as a web of nodes in which the user can browse at will" (Berners-Lee & Cailliau 1990). After that, the first web service was published publicly on the Internet and became known as WWW. The WWW has been much progressed and continues to evolve to this day. The Web of Information Connections (Web 1.0), the Web of People Connections (Web 2.0), the Web of Knowledge Connections (Web 3.0), and the Web of Intelligence Connections (Web 4.0) are introduced as the stages of the advent of the web (Prasad, Manjula & Bapuji 2013, 1).

The World Wide Web Consortium (W3C), an international WWW organization, was founded and headed by Berners-Lee after he left the CERN in 1994 (W3C 2022a). W3C's primary mission is to make the full Web potential by creating technical standards and instructions to maintain the growth of the WWW in the long term. W3C follows design principles including "Web for All," "Web on

Everything," "Web for Rich Interaction," and "Web of Data and Services" to achieve its missions. The consortium additionally participates actively in providing education and information, develops software technologies, and represents a public forum for discussion about the Web on a global scale (W3C 2022b).

Web 1.0 was the first phase of the WWW evolution, lasting from 1989 to 2005. According to W3C (World Wide Web Consortium), Web 1.0 "--is an information space in which the items of interest, referred to as resources, are identified by global identifiers called Uniform Resource Identifiers (URI)." (W3C Technical Architecture Group 2004). In this era, a website was a read-only informational page because the users were allowed to see static data without having the chance to express their thoughts or feelings. Three leading technologies make up Web 1.0, which is also the core web standard: URL (Uniform Resource Locator), which is a unique address to locate a resource across the internet; HTTP (Hypertext Transfer Protocol), which provides the instructions to retrieve a representation of a resource over a URL; and HTML (Hypertext Markup Language), which represents a resource and links to different sources through their URL (Choudhury 2014, 1). The main aim of Web 1.0 is to provide information statically and make content readily accessible for the users (Patel 2013).

Comprehended as the next generation of the web, Web 2.0 was defined in 2004 as a read-write web (Choudhury 2014, 2). The evolution from a static web page into a dynamic page with user-generated content, usability, and interoperability for end users is described as a condition for the beginning of social media to connect millions of people.

Because in Web 2.0, users' data and privacy are not in their control, to keep the users 'information secure and reduce the dependency on Big Tech companies, Web 3.0 was coined as the next iteration of the WWW in 2006 (Patel 2013; Ethereum 2022a). It was described as the "read-write-execute" web to connect everything on the web at the data level (Choudhury 2014, 3). Web 3.0 interconnects data in a decentralized way to deliver a personalized user experience (Prasad, Manjula & Bapuji 2013, 3). While Web 3.0 is the evolutionary term connected with what came after the advent of Web 2.0, Web3, a high-level concept describing the future of the internet, has become a cryptic buzzword since 2020. Its foundational operations combine technologies such as blockchains, digital currencies, and NFTs (non-fungible tokens) (Ethereum 2022a).

Although Web3 has generated tremendous attention, clear statements of what Web3 is, the differences between Web 3.0 and Web3 and how it works are still absent. This thesis aims to provide a comprehensive overview of the development of the web industry over time. A particular concentration will be on Web3, the decentralized and blockchain-based web. The research was conducted mainly by collecting relevant research papers, articles, technical documentation, and other sources. In this thesis, I refrain from high-level technical discussions so that the audience with basic knowledge of the web can understand. The definition of each stage of the WWW evolution is not mentioned in this thesis because of the rapid development of the Internet; it would be outdated over time.

The thesis is composed of seven chapters and is structured as follows. Chapter one provides an overview of the difference between the WWW and the Internet, tracing the evolution of the WWW and its stages. Chapter two explores the history, architecture, security, user application, and downsides of Web 2.0. Chapter three gives a general view of Web 3.0 and delves deeper into the details of Web3, the decentralized and blockchain-based web. Chapter four focuses on a detailed examination of the functioning and architecture of Web3. Chapter five examines the various applications of Web 3, whereas chapter six highlights its importance and limitations. The final chapter, chapter seven, presents this work's discussion, outlining the WWW's growth and predicting the development of Web3. It is worth noting that Web 1.0 is not included in this thesis as it is considered the foundation or the starting point for the evolution of the WWW, and the technology and the usage of the web have advanced significantly since its inception.

2 WEB 2.0 – THE SOCIAL WEB

The lack of active user interaction with Web 1.0 led to the birth of Web 2.0. Darcy DiNucci invented the concept of Web 2.0 in 1999. Later the term “Web 2.0” came into vogue with notable contributions from Dale Dougherty, a web pioneer, during a conference brainstorming session in 2003 and Tim O’Reilly in his article “What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software,” in 2005 (Aced 2013; Governor, Hinchcliffe & Nickull 2009).

In O’Reilly’s article, the core concept of Web 2.0 is “web as platform,” where software applications are built upon the web (O’Reilly 2005). Several web-based services and applications have significantly impacted interpersonal communication and human interaction with data on a global scale. These web technology applications have fully developed, combining new and old features and capabilities over time (Anderson 2007, 7). Web 2.0 revolutionized interactions among humans because of the popularity of services. The crucial and most popular technologies and services of Web 2.0 are blogs, wikis, really simple syndication, mashups, tags, and folksonomy (Patel 2013, 2).

As previously mentioned, Web 2.0 is referred to as the read-write or dynamic web. In the Web 2.0 era, users could interact in dynamic web pages instead of just reading the page; the users could collect, generate, and distribute vast amounts of data with just a click, which was a considerable upgrade over the one-way communication that the static web pages of Web 1.0 allowed (Nath, Basistha & Dhar 2014). This has led to the emergence of the “social web”, where individuals are not just consuming information but also actively contributing to it.

With the fast rise of Web 2.0, web technologies such as CSS, JavaScript, Adobe Flash Player, and React have enabled the creation of more immediate and visually appealing web pages. The ability for users to generate and share content has flourished thanks to the distribution and sharing of data through social media, video-sharing, blogging, and podcast-sharing platforms. Social networking sites such as Facebook, Twitter, and LinkedIn allow users to create and share content, connect with friends and colleagues, and join communities based on shared interests. Blogs like WordPress enable individuals to share their thoughts and ideas with a global audience. YouTube, a video-sharing platform, lets users upload, share, and watch videos (Akinola 2022). These applications have greatly enhanced the user experience.

As shown in figure 1, the basic high-level architecture of the Web 2.0 application is included in three parts. First, front-end code (typically HTML, CSS, and JavaScript) executed on the client side defines the user interaction (UI) logic. Second, the server's back-end code (typically PHP, Java, or Python) defines business logic. And finally, the database is the place to store all the data. To build an application, one needs to combine three parts and hoard them on centralized servers. When the application interacts with the browser, it talks to the server, and then the server communicates with the database. The server gets data, compares the input with queried data, and returns the response based on the result (Kasireddy 2021).

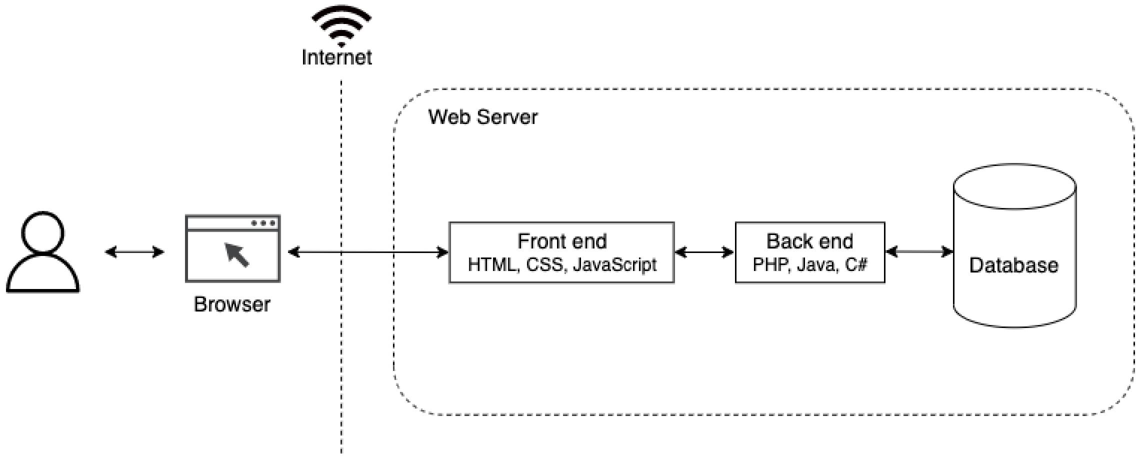

Figure 1: The basic architecture of the Web 2.0 application (adapted from Kasireddy 2021).

Besides excellent user experience improvement, Web 2.0 presents dramatic security issues. Personal information is collected with each interaction because it is made copies and sent to the service provider's server, creating possible conditions for Tech Giants to store an enormous amount of data (Voshmgir 2020, 6). When they have adequate data, they sell it to third-party information bidders. There have been countless shocking scandals exposing the dark side over the years. An example of this is the story of Cambridge Analytica and Facebook misusing personal data to manipulate swing voters for political advertising. Data exploitation has led to various privacy and legal problems worldwide (Wikipedia 2022).

Web 2.0 users are highly vulnerable to cyberattacks because of the centralization of user information in platforms, resulting in data loss and leakage. Sometimes, this personal information can be exposed to the public during a data breach (Behnke 2022). Ownership is one of the factors limiting Web 2.0. The free will and speech of users are determined by administrators of Web 2.0

platforms. Governments can easily interfere with or shut down applications hosted on centralized servers when they suspect that users are expressing an opinion that contradicts their propaganda (Dabit 2021). With the severe downsides of Web 2.0, users are looking toward the next WWW generation and expecting it to be a game-changer.

3 THE THIRD GENERATION OF THE WWW

Web 3.0 is a term that is still evolving and has multiple interpretations. It is considered the next evolution of the Internet (Patel 2013). However, some experts have defined Web 3.0 as the "Semantic Web," which aims to improve how data is shared and combined from different sources (Choudhury 2014, 3). Additionally, Web3 is the term that refers to the next version of the WWW and the use of blockchain technology, smart contracts, and decentralized networks to provide a new way of interacting with the web (Stackpole 2022). It seems that the term Web3 is more about the technological aspect of the next web era, whereas Web 3.0 is more focused on the vision and goal of this new era.

3.1 Introduction of Web 3.0

The definition of Web 3.0 has been coined several times throughout the past (Farah 2012, 1). The phrase "Web 3.0" first appeared in early 2006 in a blog article "Critical of Web 2.0 and associated technologies such as Ajax" by Jeffrey Zeldman and then it was written in a New York Times article by John Markoff. This term created a debate within the web industry at the Technetium Summit in November 2006 (Chalopin & Trehan 2022). As Tim Berners-Lee described, Web 3.0 is also stated as the "read-write-execute (r-w-x)" web (Jacksi & M.Abass 2019, 3).

Web 3.0 represents a significant shift in focus from the front end of the web, as seen in Web 2.0, to the back end. It aims to transform the web into a vast database that can be applied in various fields through the Internet. The data structure is defined and linked, providing a higher level of discovery, automation, integration, and reuse for different applications (Choudhury 2014, 3). In comparison to its predecessors, Web 3.0 has considerable differences. Four of the most prominent features that establish its significance are the semantic web, artificial intelligence (AI), 3D graphics, and ubiquity. The semantic web assists in teaching the computer the meaning of data, allowing AI to formulate real-world use cases which are more promising for the data utilization (Cointelegraph 2022a).

The term "Web 3.0" is often misunderstood as a synonym for "semantic web," although Tim Berners-Lee, one of the proponents of the semantic web, described the semantic web as a component of Web 3.0 (Farah 2012, 2). The semantic web is an evolving extension of the existing

WWW set standards of the W3C (Takyar 2022a). As mentioned earlier, it aims to find, share, and combine data from distinct sources more profoundly. Web 3.0 will promote greater data communication using semantic metadata, leading to an enhanced user experience that takes advantage of all available information (Cointelegraph 2022a). In accordance with the Linked Data principle introduced by Berners-Lee in 2007, data can be created on the web by adding it to a single global data space, where data is freely accessible and interconnected. The Resource Description Framework (RDF), RDF Schema (RDFS), Querying RDF data (SPARQL), and Web Ontology Language (OWL) are among the significant semantic web technologies that are currently used on the web to enable machines to understand and assist users with various tasks (Choudhury 2014, 3).

Thanks to AI, Web 3.0 can filter and suggest the most suitable data for users. While in Web 2.0, customer feedback is collected to increase the understanding of the user experience, Web 3.0 leverages user feedback as an essential resource for supporting the web to offer reliable information to the community. Rotten Tomatoes, https://www.rottentomatoes.com/, are a popular website example of the rate and review of movies. Good films receive a huge number of positive reviews. When a user searches for a good film list, good data, such as resources from Rotten Tomatoes, has a priority to display. Nevertheless, users can negatively affect AI by corrupting practices such as manipulating data or biased product reviews. Hence, AI must learn to distinguish between fake and genuine data to provide users with trustworthy information (Cointelegraph 2022a).

Web 3.0 has been complimented as the Spatial Web since it blurs the line between the physical and digital worlds by upgrading from a simple two-dimensional (2D) web to a more realistic three-dimensional (3D) virtual world. Its revolution supports reimagining graphics technologies alongside providing easier interaction in the 3D cyber world. This application offers a high user experience in numerous sectors, such as games, health, and e-commerce (Cointelegraph 2022a).

The ubiquity refers to the ability for data and services to be accessed from any device, anywhere, at any time. In that sense, Web 2.0 is already ubiquitous because, for instance, a user posts a status on a social media platform, and after being published, the status becomes omnipresent. Web 3.0 takes this a step further to allow for greater control and ownership of data by individuals and a more secure and efficient way for data and services to be shared among multiple parties (Cointelegraph 2022a).

3.2 The background of Web3

Web3 is not simply an evolution of the WWW but rather a concept that pertains to the application of blockchain technology, cryptocurrencies, and non-fungible tokens (NFTs) in the Web 3.0 era. A blockchain is a decentralized, secure, and shared system of record keeping where each participant holds a copy of the records. Updates can only be made if all parties involved in a transaction agree. On the other hand, cryptocurrency or crypto refers to a digital currency secured using cryptography. NFTs are a type of digital asset that represents ownership of a unique item or a piece of content, such as artwork and virtual real estate (Bashir 2022). The origins of Web3 can be traced back to 1991, when blockchain technology was first described by research scientists W. Scott Stornetta and Stuart Haber. However, the concept largely remained dormant until the launch of Bitcoin in 2009, a digital currency that relied on blockchain technology and was created under the pseudonym of Satoshi Nakamoto (Stackpole 2022). In 2014, Dr. Gavin Wood, Ethereum co-founder, outlined a definition for Web3 during Ethereum's formation, and he refers to it as "a decentralized online ecosystem based on blockchain" in a blog post. The goal of Web3 is to return data ownership to users and decentralize the Internet by blockchain. In 2017, Dr. Wood founded Web3 Foundation, an organization to support decentralized web applications and protocols (Edelman 2021).

While Bitcoin is designed as a digital currency and a store of value, Ethereum, launched in 2015 on Bitcoin's innovation, is a payment network and a platform that allows developers to build and deploy decentralized applications (dApps, DApps, or dapps) (Ethereum 2022b). These dApps can take various forms, such as websites, mobile apps, and games, and their content is often controlled by a blockchain network (Voshmgir 2020, 33). According to ethereum.org, a leading online resource for the Ethereum community, Web3 is currently under development and does not yet have a clear definition. However, the main guiding principles for its creation include decentralization, permissionless, native payments, and trustless (Ethereum 2022a).

Decentralization is a fundamental principle of Web3 provided by blockchain technology. The decentralized model aims to present a more flexible, more inclusive, and less vulnerable digital experience while prioritizing peer-to-peer (P2P) connectivity over the support of third parties. In a P2P network, there is no central controller, and all nodes can communicate with each other directly, which lets transactions be completed instantly among participants without intermediary interference (Bashir 2020).

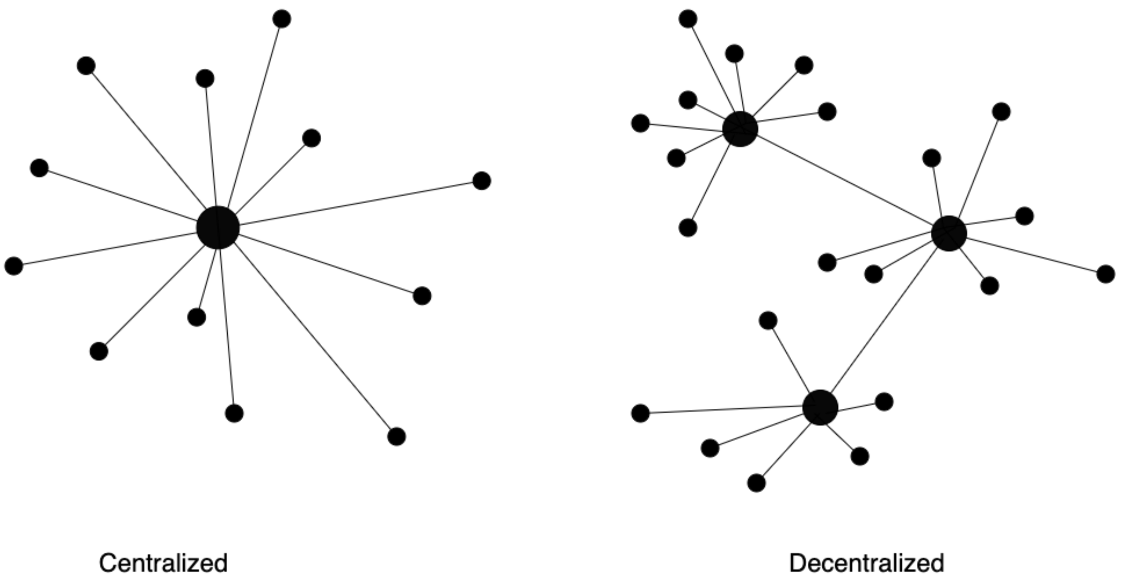

Figure 2: The difference between centralized and decentralized networks (adapted from Jain 2022).

Both terms “centralization” and “decentralization” mentions in the ranks of control (Jain 2022). In figure 2, all small dots are connected to a big central dot in a centralized system. The central dot presents a server that stores data and is responsible for all system operations, while the small dots are users (nodes) in the real world. If the server crashes, the website is down, and users cannot access data until the server is fixed or switched to a backup server. As seen in figure 2, decentralized networks offer a better approach than centralized systems. All dots are directly or indirectly linked, meaning that the system has multiple central owners instead of having a central owner (Hooda 2022). These dots (nodes) exchange messages to create a consensus or agreement as needed (Jain 2022). However, a decentralized network also comes with certain turn-offs. Building and maintaining a decentralized system face high costs, which is not ideal for small companies (Hooda 2022). Decentralization makes technology more complex and, further, out of reach for basic users rather than more straightforward and convenient (Stackpole, 2022).

Web3 operates on “permissionless” blockchains, which have no centralized control and do not require parties in a transaction or interaction to seek permission from a mediator before proceeding (Stackpole, 2022). This character contributes to Internet equality and reduces the control of large corporations in the virtual world. Additionally, the native payments feature allows using crypto for payments and money transfers, as opposed to depending on traditional payment processors. This makes it significantly more secure against cyberattacks on organizations. The term “trustless” refers to the ability for interactions and transactions to occur between parties without the involvement of a trusted intermediary. For example, individuals can send tokens such as Ether

(ETH), the currency of Ethereum apps, directly to another person without the need for trusted third parties. Thanks to blockchain algorithms and encryption, the transaction process cannot be interfered with and disrupted (Ethereum 2022a).

4 WEB3 MICROSERVICES

The architecture of Web3 comprises the backend, front end, and data. In comparison to figures 1 and 2, Web3 platforms redefine the backend of the web, and the front end of Web3 platforms shares some similarities with Web 2.0 platforms. Even so, some other aspects differ when it comes to functionality. As seen in figure 3, Web3 operates without the requirement of a middleman. There is no web server for the backend logic and centralized database in the process of Web3 (Kasireddy 2021).

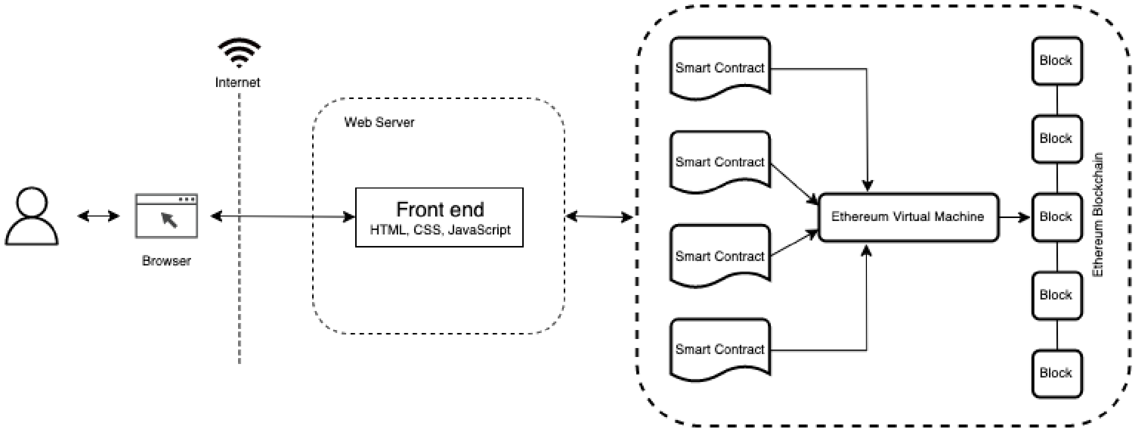

Figure 3: The basic architecture of Web3 (adapted from Kasireddy 2021).

To understand how a dApp functions, a backend developer must first create a smart contract and deploy it on the chain. As an example, in figure 3, the Ethereum blockchain and Ethereum Virtual Machines (EVM) are used. When a user interacts with the dApp via the browser, the front end directly communicates with the smart contract and automatically adds this interaction. This action is packaged into a block, along with other data, and stored on the chain. And finally, the front end receives the data that has been successfully uploaded on the chain, and the user interface updates. It is important to note that figure 3 only displays the basic architecture of Web3. Additional components are added to the Web3 application throughout this thesis to enhance its data storage capabilities, security, and more.

In the backend, Web3 utilizes blockchain technology rather than a centralized database or web server to create decentralized applications on a virtual state machine maintained by anonymous internet nodes. This shared state machine, defined as a blockchain, supports the program states and stability by enforcing predefined rules. The virtual state machine in figure 4 is the Ethereum Virtual Machine, which is cooperatively maintained and not under the control of any blockchain network participants. As illustrated in figure 4, the traditional backend server in Web 2.0 is replaced by smart contracts that define the backend logic and are deployed on the virtual state machines. This backend code runs on the P2P network, enabling anyone to contribute to the development of blockchain applications by meeting certain requirements, such as owning and locking crypto (Kasireddy 2021; Schevchuk 2022).

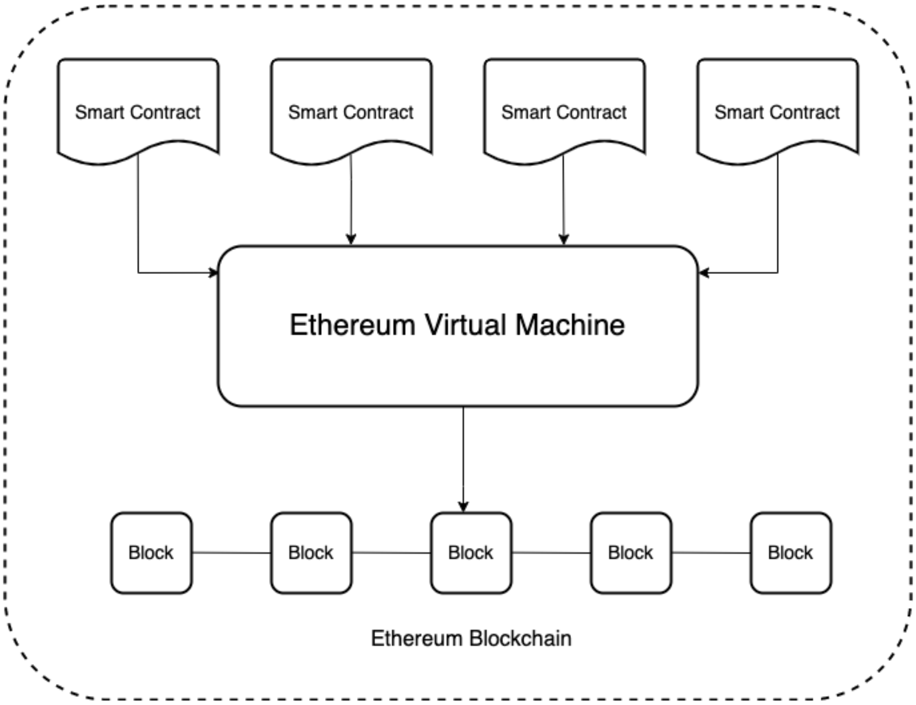

Figure 4: The backend architecture of Web3 (adapted from Kasireddy 2021).

To gain a comprehensive understanding of Web3, a thorough examination of the underlying technologies that support it is imperative. As Web3 is still in its early stages, its architecture and technologies are subject to constant change and development. Therefore, the three primary components of Web3, with an emphasis on the backend component consisting of smart contracts, virtual machines, and blockchain, which represent the most significant departure from previous generations of the WWW, will be discussed.

4.1 Blockchain

In 2008, the “chain of blocks” concept was first introduced in the paper named Bitcoin “A Peer-to-Peer Electronic Cash System.” Over time, this term has evolved into the commonly used term “blockchain.” As depicted in figure 4, blockchain technology serves as the foundational layer of the Web3 stack. While there are various definitions of blockchain, a technical definition is that a blockchain is “a peer-to-peer distributed ledger that is cryptographically secure, append-only, immutable (extremely hard to change), and updateable only via consensus or agreement among peers” (Bashir 2020).

A distributed ledger is a database that is spread across a network of computers rather than being stored in a single location. Each computer in the network has a copy of the ledger, and all the copies are constantly being updated and synced to ensure they are identical. The ledger is “cryptographically secure,” meaning that cryptography is used to provide security services that secure this ledger against tampering and misuse. The “append-only” storage model of blockchain technology refers to the ability to add new data to the blockchain in a time-sequential order while existing data cannot be modified or deleted. This feature ensures consistency and order of events in distributed systems. The key attribute of a blockchain is the update ability via consensus. This refers to the ability to add new blocks of information to the blockchain only after consensus has been achieved among the participants in the network or nodes on the network. Consensus algorithms ensure that all nodes in the network have the same view of the database and that any new information added to the database is valid. This feature guarantees the integrity and security of the data stored on the distributed ledger, as any changes to the database must be made simultaneously across all nodes and easily detected (Bashir 2020).

Blockchains can be classified into three broad types: public, private, and permissioned. Public blockchains such as Bitcoin and Ethereum are networks where individuals can participate in the network as a node. Public blockchains are open source so that individuals can access the code and participate in the development of the blockchain. In contrast, private blockchains are networks typically used in business and enterprise settings, where access to the network is restricted to a select group of participants. Private blockchains are not open source and are typically controlled by a central authority. Examples of private blockchains include Kadena and Quorum. Permissioned blockchains are a hybrid of public and private blockchains, where access to the network is restricted but not limited to a specific group of participants. Public blockchains are considered more transparent and secure than private blockchains due to the large number of nodes in the network, making it difficult to control the network. However, they are considered less private because of the visibility of transactions on the blockchain (Jain 2022; Bashir 2020).

Figure 5 displays how the blockchain collects information in groups called blocks. Each block contains sets of information, such as a list of transactions and a cryptographic hash of the previous block. A transaction, which is the record of the exchange of value, such as the transfer of money or the transfer of ownership of an asset, is added to a block and becomes a permanent and unchangeable part of the blockchain. The transaction will be linked to the address of the sender and to the address of the recipient, allowing individuals to see the transaction on the blockchain and trace the movement of the funds from one address to another. The address serves as an identifier for the sender and recipient of a transaction. If a block does not reference a previous block, it is the genesis block, the first block in the blockchain. The genesis block is created manually by the creator of the blockchain. It is the foundation of the entire blockchain and is hard-coded into the blockchain protocol (Bashir 2020).

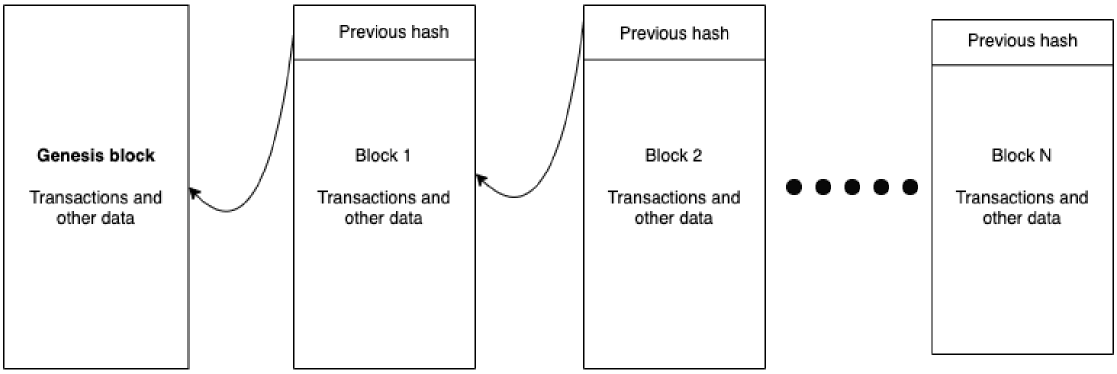
Genesis block
Transactions and other data
Previous hash
Block 1
Transactions and other data
Previous hash
Block 2
Transactions and other data
Previous hash
Block N
Transactions and other data

Figure 5: The generic structure of a blockchain (adapted from Bashir 2020).

As displayed in figure 6, the block body consists of a set of transactions, while the block header includes the previous block's hash, nonce, timestamp, and Merkle root. The first element of a block is the previous block hash, which refers to the cryptographic hash of the preceding block and links each block to the previous one in the blockchain. The nonce, a random number, is a part of the consensus mechanism in a proof-of-work blockchain. The timestamp is a record of the exact time at which the block was added to the blockchain. The last element of a block is Merkle root, a hash value derived from all the transactions in a block on the blockchain, which ensures the integrity of the data stored on the blockchain and allows for efficient verification of a single transaction within a block (Bashir 2020).

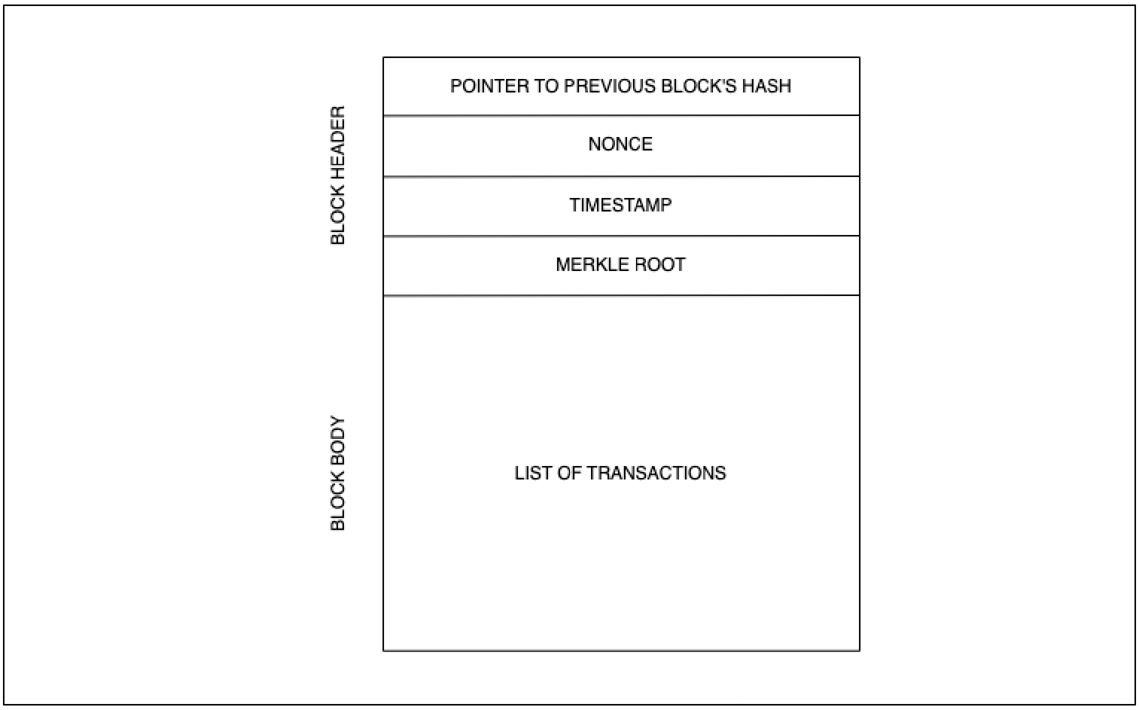

Figure 6: The generic structure of a block (adapted from Bashir 2020).

The consensus mechanism is a fundamental component of a blockchain, serving as the backbone that decentralizes control through the process of mining. Through consensus, all the participants in a blockchain network agree on the state of the blockchain and the validity of new transactions. It ensures that all nodes in the network possess the same copy of the blockchain and that no single entity can control or manipulate the network. Several consensus mechanisms can be implemented in a blockchain, including Proof of Work (PoW)- utilized by the Bitcoin blockchain- and Proof of Stake (PoS)- used by the Ethereum blockchain (Bashir 2020).

In the PoW consensus mechanism, miners who create new blocks and mint cryptocurrency (coins) compete to solve a complex mathematical problem. The first miner to solve the problem is rewarded with the right to add the next block to the blockchain. This process, referred to as mining, requires significant computational power and energy. Conversely, PoS is more energy efficient. In the PoS consensus mechanism, instead of mining, the blockchain is secured by validators, who are chosen to create the next block based on the amount of cryptocurrency they hold and are willing to “stake” or lock up as collateral (Bashir 2020; Jain 2022).

The selection of a consensus mechanism can greatly impact the security, scalability, and decentralization of a blockchain. For example, PoW is utilized in public permissionless blockchains, while other mechanisms are more suitable for permissioned blockchains. Each mechanism has its own advantages and disadvantages, and the appropriate mechanism will depend on the specific use case and requirements of the blockchain (Bashir 2020). The fundamental aspect of the concept of consensus is to impose a severe penalty for cheating the system. In PoW, this penalty is in the form of energy consumption, whereas in PoS, it is the currency staked (Jain 2022).

On public blockchain networks, where there is no centralized authority, a mechanism is needed to authenticate users. This is achieved by private and public key pairs. Each participant on the network is given a unique pair of keys, with the private key remaining under the user's control and kept highly secure. The private key is used to sign the user's transactions, while the public key, visible to all other participants, can validate the signature. In this way, the private and public key infrastructure ensures security on the decentralized blockchain network, even without a central authority (Jain 2022).

The process of generating a block on a blockchain involves several steps. As illustrated in figure 7, the first step is creating a block. The initiation of a transaction is carried out by a node, which first establishes the transaction and subsequently digitally signs it using its private key. Second, the transaction is validated and broadcast throughout the network using data-dissemination protocols like the Gossip protocol, which is validated by peers based on pre-established validity criteria. Verification is carried out to ensure the validity of the transaction before it is propagated. Next, upon receipt and validation of the transaction by miners within the blockchain network, the transaction is included in a block, and the process of mining commences. Then upon the successful resolution of a mathematical puzzle or fulfillment of the requirements of the consensus mechanism implemented within the blockchain, the block is considered "found" and finalized. At this stage, the transaction is considered confirmed. The newly created block is then validated, transactions or smart contracts are executed, and it is broadcast to other peers for validation and execution. Once validated, the block is added to the chain, and the next block cryptographically links itself to this block through a hash pointer (Bashir 2020).

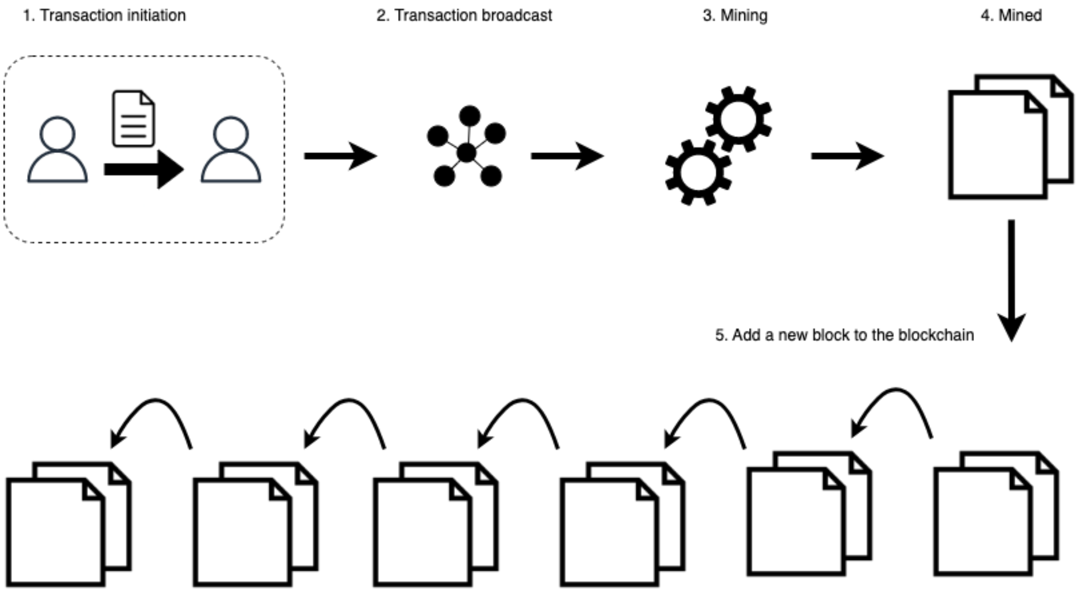
1. Transaction initiation
2. Transaction broadcast
3. Mining
4. Mined
5. Add a new block to the blockchain

Figure 7: The block generation process (adapted from Bashir 2020).

4.2 Smart contracts

The concept of smart contracts was first proposed in the 1990s by Nick Szabo in the article " Formalizing and Securing Relationships on Public Networks. Until 2009, its functionality was utilized in a limited fashion in Bitcoin. There are various definitions of smart contracts, but most of them are not specific enough. According to Bashir, a comprehensive definition of smart contracts is that it is a computer program that automatically and securely executes and enforces the terms of an agreement. At its core, a smart contract is a computer program written in a language that a computer or target machine can understand. It represents an agreement between parties in the form of business logic. One key feature of smart contracts is that they are automatically executed based on the instructions coded into them, triggered when certain conditions are met. They are also enforceable, meaning that all contractual terms are carried out as specified and expected, even in the presence of adversaries (Bashir 2020).

In figure 4, a smart contract is above the blockchains in the structure of the Web3 stack. In the context of Web3, smart contracts play a role as the application's backend. It defines the application logic and controls the functionality of the application. The smart contract allows developers to create decentralized apps and tokens with high level-languages such as Solidity and Vyper (Kasireddy 2021). The smart contract is a self-executing agreement formalized as computer software. The code contains a set of conditions under which the parties involved in the contract have agreed to interact with each other. Upon the satisfaction of the predefined conditions, the agreement is automatically enforced through a consensus mechanism on the blockchain network (Voshmgir 2020, 176). When a smart contract function is called, there is a change in the state of the blockchain network. Later, the changed state is accepted and transmitted throughout the network of nodes (Awosika 2022a).

The term “smart contract” is derived from the self-enforcing nature of these digital agreements. These contracts are an autonomous code that operates without administrators or controllers needing human intervention or management (Awosika 2022a). However, the term “smart” may be misleading, as these contracts execute the instructions they have been programmed with. This property ensures consistency and repeatability in producing the same output every time they are executed. The deterministic nature of smart contracts is highly desirable in blockchain platforms, where consistency and repeatability are essential for maintaining the integrity of the network (Bashir 2020). Smart contracts can potentially reduce the transaction costs associated with agreements by streamlining the process of reaching, formalizing, and enforcing the agreement, thanks to its self-executing nature. If implemented correctly, smart contracts can provide transaction security that exceeds traditional contract law, thus reducing the coordination costs associated with auditing and enforcing agreements (Voshmgir 2020, 177).

4.3 Virtual state machine

A virtual state machine is a computational model that is used to simulate the behavior of a system in different states. In a blockchain, a VTM is used to keep track of the current state of a smart contract, including the state of the contract storage and account balances. This allows the execution of smart contract code to be deterministic, meaning it will always produce the same result for a specific input (Awosika 2022b).

As mentioned earlier, this thesis will use Ethereum Virtual Machine (EVM). To understand the capabilities of the EVM, it is important first to understand the concept of Turing completeness. A Turing-complete machine is capable of processing any computation, regardless of complexity, given sufficient time and resources (Awosika 2022b).

The EVM is a software environment that runs on the Ethereum blockchain to build dApps and other applications. It is a virtual machine that can execute smart contracts written in programming languages like Solidity by compiling high-level language into a machine-readable format known as bytecode (Jain 2022; Kasireddy 2021). The EVM is a Turing-complete machine, meaning it can process any computationally feasible program, but is constrained by the amount of gas required to execute operations. These gas requirements act as a safeguard against infinite loops that can result in denial-of-service attacks (Bashir 2020). The EVM is responsible for smart contracts deployments and handles the state of the network after a new block is added to the chain and can be accessed worldwide through participating nodes on the Ethereum network. With the EVM, deploying a smart contract would be feasible as it provides a secure, sandboxed environment for the execution of smart contract code (Kasireddy 2021; Awosika 2022b).

4.4 Frontend

In Web3, because the client side of dApp can use standard web technologies such as HTML and JavaScript, developers can use familiar tools, libraries, and frameworks with Web 2.0. The front-end architecture focuses on communicating with smart contracts, which differs from the communication between the front and back end in Web 2.0. Each node in the network contains a copy of all states, including the code on the blockchain and the data linked with every smart contract, and it can promote a request for a transaction to be conducted on the EVM. Thus, if the front end wants to communicate with the smart contract, it must interact with one of these nodes. There are two methods to propagate a new transaction: utilize a third-party node provider and set up a node. Each technique has trade-offs. Due to the launching of its blockchain infrastructure, users can verify their data and decrease their dependence on mediators. Still, it is a challenging, time-consuming, and expensive process, especially because the blockchain continues to grow. Using third-party node providers is better, although it generates a centralized dependency component (Kasireddy 2021).

Regardless of which option the developers choose, the providers are the nodes that associate with the blockchain. Every provider executes a JavaScript Object Notation Remote Procedure Call (JSON-RPC) specification to guarantee a consistent set of methods for front-end applications to interact with the blockchain. JSON-RPC is a lightweight remote procedure call (RPC) protocol that encodes its requests and responses using JSON format. A remote procedure call, in general, is a method of requesting a service from a program located on another device. It creates an illusion that a local procedure call is being made even though the procedure may be executed on a different device. Because it is transport-agnostic, as meaning that the ideas can be applied within the same process through sockets, HTTP, or different message-passing environments, it interacts with

Ethereum nodes over communication protocols. Once the blockchain is connected through a provider, such as in figure 8, the users can read the information about the state of the blockchain (Kasireddy 2021; Bashir 2020).

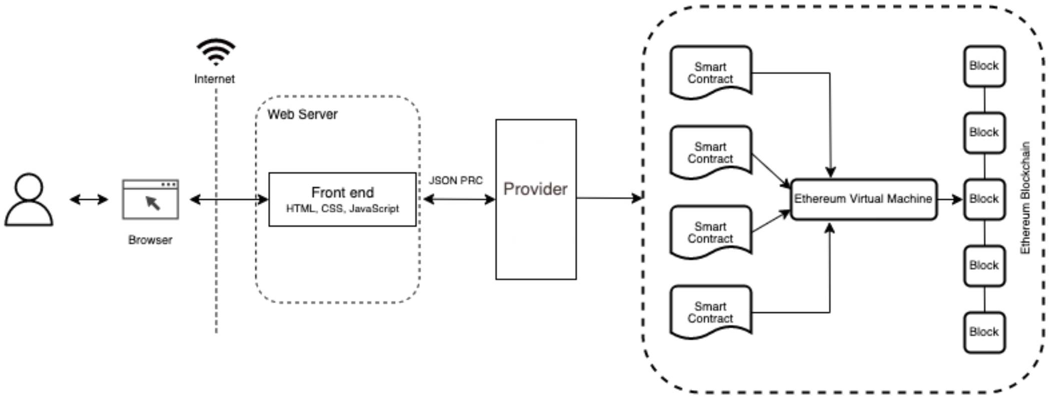

Figure 8: Front end connects with a smart contract provider (adapted from Kasireddy 2021).

In traditional web applications, users are prompted to login in with an email address (or username) and a password for identification and authentication with a certain level of insecurity because of personalized data leakage. In decentralized applications, dApps need permission to access the user's wallet to enable certain functionality. A blockchain wallet refers to a digital wallet that allows individuals to securely store, send, and receive cryptocurrency and other digital assets built on blockchain technology. The essential elements of a wallet are a public key, a private key, and a blockchain address which serves a similar purpose to bank account numbers in traditional financial transactions. Digital signature verification is performed utilizing wallet software. Analogous to traditional handwritten signatures, digital signatures serve to confirm the identity of the signatory. When implemented correctly, digital signatures are more resilient to forgery than traditional handwritten signatures. In the context of blockchain networks, digital signatures are employed for both the authentication, which verifies the identity of the sender of tokens and the integrity of the transaction, which ensures that the specified number of tokens has been sent. The private key is utilized to sign token transactions while validating nodes in the network use the public key to verify the signature. (Voshmgir 2020).

To write to the state, users must use their private key to sign a transaction digitally before initiating the transaction to the blockchain. The users must spend an amount of cryptocurrency as a gas or miner fee to verify the transactions. Metamask is the most popular wallet solution that acts as a transaction signer and key management. A user's private keys are stored in the browser by Metamask, and Metamask is called when the user makes a transaction request (Schevchuk 2022).

Then dApp relays the transaction to the blockchain. Otherwise, the transaction is not accepted. Metamask is both provider and a signer, which is the best solution for reading data from a smart contract and writing data (Kasireddy 2021).

Let's take the social media web as an example (see figure 9). When a user likes content in a browser, this action needs to be recorded on the chain after interacting with the front end. The application must activate the wallet Metamask, which will ask the user to sign in for additional information. The transaction is only initiated after the wallet is signed.

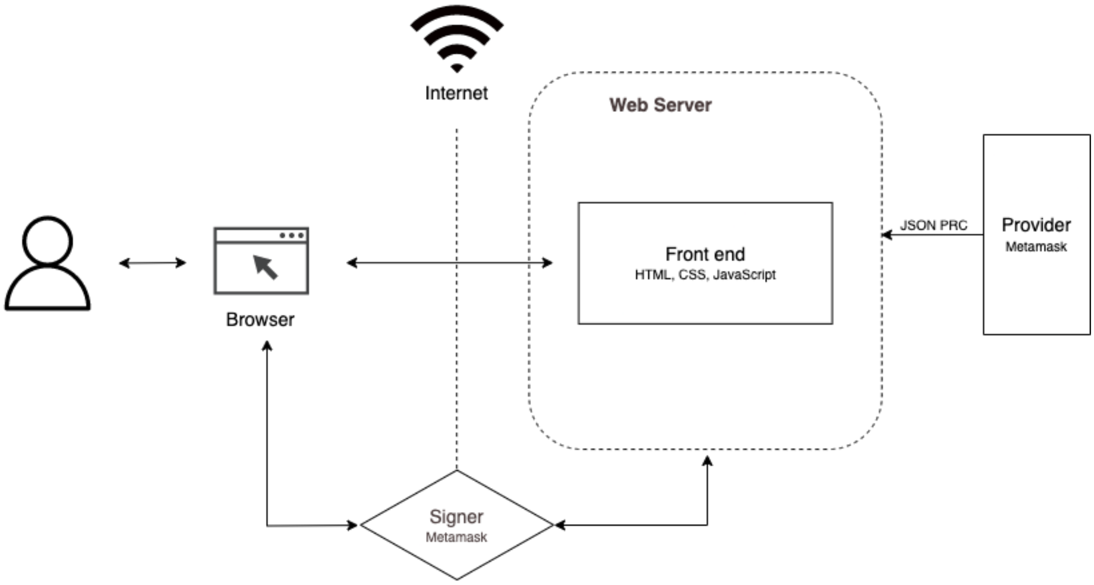

Figure 9: Verifying user process with wallet Metamask (adapted from Kasireddy 2021).

4.5 Data storage

Blockchain is the ideal information storage thanks to its security, trustlessness, and transparency. However, blockchains are unsuitable for storing or processing large amounts of data. Keeping and distributing large static assets such as images and videos on the blockchain has expensive transaction gas fees and low speed, so there are better solutions than a blockchain. Hence, dApps utilize off-chain data storage services on a data storage platform. Decentralized storage services such as Interplanetary File System (IPFS) and Swarm are needed. In certain, several dApps even store the resources of the application's frontend web interface on IPFS/ Swarm to ensure the highest decentralization, allowing for a more decentralized and resilient way of delivering the frontend to the user (Kasireddy 2021; Awosika 2022b).

The IPFS is a decentralized file system protocol that allows storing and accessing data in a P2P network. Each user has its node in the blockchain. These nodes can communicate with each other and share files. Every single bit of data is cryptographically hashed, and the hash function identifies that file. Instead of storing the data on a single server, the files are stored on the IPFS system and can be retrieved from any IPFS node by using its unique hash. The purpose of IPFS is to replace HTTP as a protocol of choice for the delivery of web applications (IPFS 2022). Swarm is identical to IPFS in the decentralized storage network, but its system is implemented through smart contracts in the Ethereum blockchain network. Like IPFS, it allows storing files to be published and replicated by Swarm nodes (Kasireddy 2021). Although the data is off-chain, the P2P distributed file system helps avoid the monopoly of centralized databases so third parties cannot tamper with data.

As shown in figure 10, the front end of a dApp is hosted on a decentralized storage solution, such as IPFS or Swarm, rather than a central server. The smart contract provider acts as a bridge between the front end and the decentralized data storage. For example, when a user wants to make a transaction in the dApp, the front end will gather the necessary information from the user and use the smart contract provider to broadcast the transaction to the blockchain network. Once the network confirms the transaction, the smart contract provider will update the state of the data storage accordingly, and the front end will then reflect the updated state to the user.

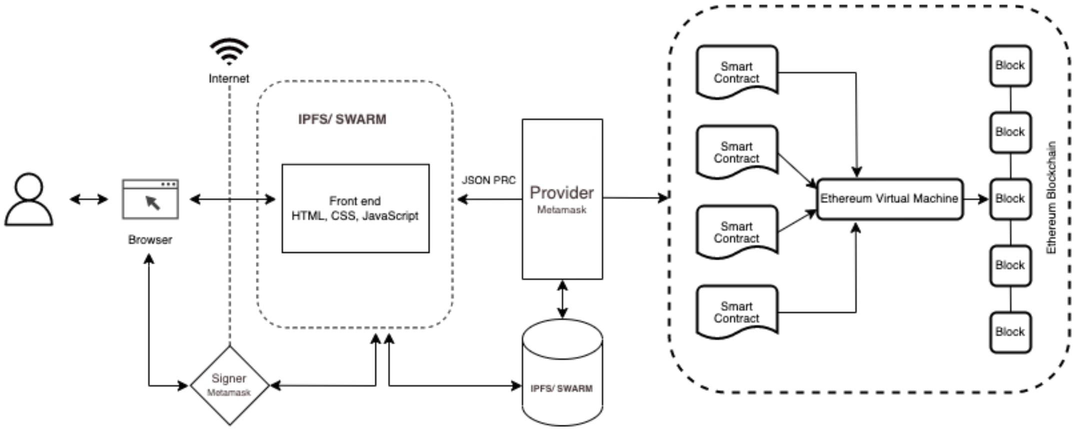

Figure 10: The web3 architecture with decentralized storage services (adapted from Kasireddy 2021).

Although blockchain technology is an ideal solution for decentralized and transparent data storage, data access in the blockchain is a challenging endeavor that developers must spend a notable amount of time finding methods to approach. There are two ways to read data from smart contracts on the blockchain: smart contract events and The Graph service. The choice of method to query a blockchain will depend on the blockchain platform, the type of data needed, and the intended use case (Kasireddy 2021).

When a user accesses the web using a traditional web application (Web 2.0), the user uses a client, such as a web browser, to request information from a web server using HTTP. This allows the client to retrieve and display the information on the device of the user. In contrast, dApps are built on top of blockchain technology and do not rely on central servers or traditional HTTP communication protocols. Instead, they use smart contract events to communicate with the blockchain. To communicate with the blockchain, dApps use libraries such as ether.js or web3.js. These libraries provide a set of methods that can be used to initialize JSON-RPC requests and trigger smart contract functions. These libraries provide an interface for developers to interact with the blockchain and for users to trigger smart contract functions through the user interface of the dApps. It is worth noting that dApps can use web3.js only for Ethereum (Awosika 2022a).

In Web3, dApps can query blockchain data for the use of application logic by Application Programming Interfaces (APIs). An API is a defined rule describing how a disparate computer or application interacts with others. The Graph is an example of an API blockchain to make a query on data from multiple blockchains easier by using GraphQL as a query language. It specifies and converts smart contract events and function calls into entities that frontend logic can use. The Graph protocol provides a high-performance solution that eliminates unnecessary event querying from nodes and decreases the latency when querying on-chain data in application logic thanks to indexing blockchain data (Kasireddy 2021; Awosika 2022b). As displayed in figure 11, the Graph protocol can be used to connect the front end with the back end by indexing the data stored on the blockchain. It also enables the connection of the front end with a decentralized storage solution like IPFS or Swarm. Both allow the front end to retrieve data directly from the P2P network without having to go through a smart contract provider.

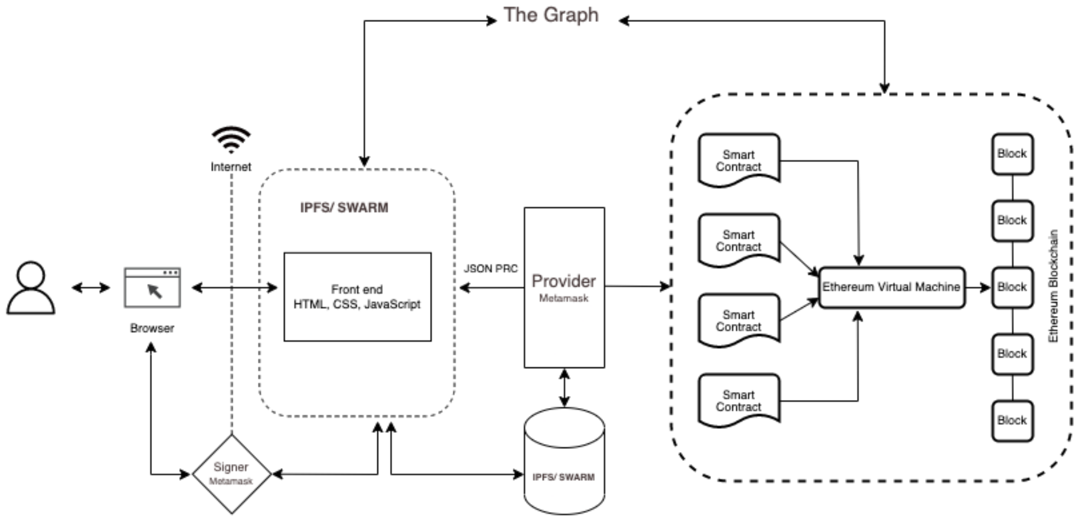

Figure 11: Connecting the Graph with the front end (adapted from Kasireddy 2021).

5 WEB3 APPLICATIONS

Web3 applications are still relatively new and evolving technology that represents the next step in the evolution of the Internet. These applications are built on decentralized platforms. And they aim to provide a more transparent and decentralized online experience. Some of the popular use cases for dApps include non-fungible tokens (NFTs), decentralized finance (DeFi), decentralized autonomous organizations (DAOs), and the Metaverse. NFTs are unique digital assets representing ownership, DeFi offers decentralized financial services, DAOs are decentralized organizations governed by smart contracts, and the Metaverse is a virtual world where users can interact with each other and digital assets. As the technology matures, it is expected that more and more use cases for dApps will emerge, potentially revolutionizing how we interact with the Internet.

5.1 Non-fungible tokens

With the rapid growth of blockchain technology and its applications, various tokens and token ecosystems have emerged. A coin is a cryptocurrency that runs natively on its blockchain. For example, Bitcoin and Ether are coins with native blockchains. On the other hand, a token is an asset representation built on top of a blockchain. Ethereum, for instance, has not only its own Ether coin but also hosts thousands of other tokens created for different purposes. Thanks to its smart contract support, Ethereum has become a platform for various tokens, such as utility tokens, game tokens, and specialized tokens with high value. Tokens can be grouped into two categories based on their usage: fungible and non-fungible tokens (Bashir 2020).

NFTs are digital assets with unique identification codes and metadata that distinguish them from other tokens. They can be traded and exchanged for various forms of value, including tradable currencies, other NFTs, and more, dependent upon the perceived value placed on them by the market and their respective owners. For example, the creation of a token for a digital image of a banana could be facilitated with a decentralized exchange (Sharma 2023).

The creation of NFTs is accomplished through a procedure referred to as mining. This process records the information of the NFT on a blockchain. It entails validating information by a validator, followed by creating a new block and its closure. The minting process involves the integration of smart contracts that manage the ownership and transferability of NFT. As NFTs are minted, they receive a unique identifier linked to a specific blockchain address, granting ownership to the address of the owner. The ownership information of each NFT, as indicated by its blockchain address, is publicly accessible. Although multiple NFTs of the same item may be minted, each token is distinguishable from the others due to its unique identifier (Sharma 2023).

One of the most well-known cases of NFTs is Cryptokitties. Launched in November of 2017, Crytokitties are digital cats with different identification codes recorded on the Ethereum blockchain. Each Cryptokitty holds a unique value and is considered a separate entity from its counterparts. The process of "reproduction" within the Cryptokitties ecosystem results in the creation of new descendants with differing attributes and market values compared to their ancestors. Within a brief time after their launch, Crytokitties fans invested over $20 million worth of Ether in purchasing, maintaining, and raising them (Sharma 2023).

5.2 Decentralized Finance

DeFi, a technology-driven financial system built on secure and decentralized ledger systems like those used by cryptocurrencies, may prove to be the transformative decentralized application that the industry has been anticipating. The traditional financial sector requires the involvement of a trusted third party, such as a bank or a financial institution, to conduct business. These intermediaries are often relied upon to provide necessary services and to ensure trust in financial transactions. However, DeFi seeks to disrupt this centralized financial paradigm by enabling P2P exchanges and granting individuals greater control over their financial assets. By eliminating the fees associated with intermediaries, DeFi offers individuals the ability to securely manage their assets through digital wallets, quickly transfer funds, and access financial services with an Internet connection (Bashir 2020; Sharma 2022).

Stable coins or stable tokens are a type of cryptocurrency that is designed to maintain a stable value compared to a specific asset such as fiat currencies or precious metals. It aims to minimize the volatility often associated with other cryptocurrencies (Bashir 2020). For example, one USDC token is equivalent to one US dollar (@gillesdc 2022). The growth of DeFi has resulted in the emergence of decentralized exchanges, referred to as DEXs. These exchanges operate without a central authority or intermediaries and facilitate direct P2P trading among traders. Popular DEXs include Uniswap, Bancor, WavesDEX, and IDEX. The DEX ecosystem is rapidly expanding and is projected to continue its growth (Bashir 2020).

While DeFi offers numerous benefits, such as increased accessibility and lower costs, it also faces significant challenges that must be addressed to drive wider adoption. The DeFi ecosystem is still in its early stages of development and requires further usability and improvements in user experience. Furthermore, the absence of a regulatory framework raises concerns about the potential for illegal activities within the DeFi space. Additionally, relying solely on code instead of traditional paper contracts with established financial institutions may be a hurdle for many consumers accustomed to traditional economic systems. A human error on a blockchain can have severe consequences, particularly in the context of DeFi or cryptocurrency blockchains, where any mistake can result in significant financial losses (Bashir 2020).

5.3 Decentralized autonomous organization

DAO represents a novel form of legal arrangement that lacks a centralized governing authority and operates through the collaboration of its members toward a common objective for the best interest of the entity. DAOs have been popularized by integrating blockchain technology and cryptocurrency. They are designed to enhance the conventional organizational structure prevalent in numerous companies through a bottom-up management style that empowers every member with a voice, a vote, and the ability to propose initiatives instead of relying on a single individual or a limited group of individuals to steer the organization. It is noteworthy that digital currencies are inherently decentralized, and DAOs embody this characteristic by being unaffiliated with any nation-state or regulatory authority. Instead, they are disseminated across a diverse network, ensuring complete decentralization (Takyar 2022c; Reiff 2022).

The foundation of DAOs is rooted in the utilization of smart contracts. These logically coded agreements serve as the cornerstone of DAOs, defining rules and executing actions collectively agreed upon by their members. For instance, certain codes may be implemented in response to the outcome of a decision, leading to an increase in the circulating supply, burning of reserved tokens, or the issuance of rewards to existing token holders. In contrast to traditional centralized power structures, DAOs rely on the proposals of their members. Each node can voluntarily cast a vote for a given proposal, which will be adopted and implemented through the rules encoded in the smart contract if it gains the support of most nodes. The voting process is recorded on the blockchain and usually requires users to make mutually exclusive choices. The voting power is often determined by the number of tokens held by each user, with those possessing more tokens having a proportionately greater influence on the outcome of the vote. As blockchain operates transparently and publicly, it is impossible to unilaterally modify a DAO's code or rules without it being noticed (Takyar 2022c; Reiff 2022).

The DAO was a groundbreaking and complex smart contract launched on the Ethereum network in 2016. The DAO aimed to provide a decentralized platform for fund management, eliminating the need for traditional fund managers. This organization conducted a month-long token crowd sale that amassed more than $150 million in funds, making it the largest crowdfunding campaign in history. The DAO token holders were intended to become co-owners of the decentralized investment fund, proportional to their token holdings, with proportional voting rights for investment decisions. The DAO token holders could hire subcontractors to provide specialized services, with decisions made through majority consensus. However, a programming error in the software resulted in the theft of a third of The DAO's funds before it became operational, leading to a controversial hard fork of the Ethereum network (Voshmgir 2020). Although the DAO hack initially posed a significant threat to the fledgling Ethereum protocol, it ultimately proved to be a catalyst for its growth and reinforcement (@gillesdc 2022).

5.4 Metaverse

The concept of the Metaverse was first introduced by novelist Neal Stephenson in his novel, "Snow Crash," published in 1992. It refers to a virtual reality-based digital world where individuals can interact with each other through virtual reality headsets. Recently advancements in technology, such as the development of virtual reality (VR) and augmented reality (VR), and the growth of blockchain, have made it a reality. Users can access the Metaverse through virtual reality VR headsets, AR glasses, or smartphone apps and interact with the virtual environment and other users in real-time (Rijmenam 2022).

The Metaverse can be broadly categorized into two types of platforms. The first involves using NFTs and cryptocurrencies to establish blockchain-based Metaverse startups. This allows individuals to purchase virtual land and design their environments on platforms such as Decentraland and The Sandbox. The second category encompasses virtual worlds, where individuals can gather for both professional and leisure purposes. While free accounts may be available on some Metaverse services, those buying or trading virtual assets on blockchain-based platforms must utilize cryptocurrencies. For instance, individuals can participate in trading NFT art pieces or charge an entrance fee for virtual concerts or shows on Decentraland (Cointelegraph 2022b).

The Metaverse has numerous potential uses that could impact various industries. Beyond gaming and entertainment, it promises to transform education, commerce, and social connections. The Metaverse will eventually blend with reality, enabling individuals to switch between virtual and real-life experiences fluidly. Although the Metaverse is still in its early stages of development, it has the potential to revolutionize the way we interact with technology and with each other. As technology continues to evolve, the Metaverse will become an increasingly sophisticated and immersive platform for a wide range of activities and experiences (Rijmenam 2022).

6 UNPACKING THE OPPORTUNITIES AND CHALLENGES OF WEB3

6.1 The importance

Web3 represents a major step forward in the evolution of the Internet, as it allows for decentralized ownership, censorship resistance, digital identity, and native payment capabilities. These enable the creation of dApps that be used for a wide range of purposes, from finance, gaming, and social media, which has the potential to disrupt and transform traditional industries.

In the decentralized web, owners of data and interactions are distributed among the users, which means that individuals have more control over their data and can choose to share or keep it private. This is achieved through blockchain technology and smart contracts, which allow for creating and transferring unique digital assets and decentralized decision-making. Examples of Web3 ownership include using NFTs to represent ownership of digital art and collectibles and using DAOs to allow for decentralized ownership and decision-making. Additionally, users have more control over how their data is used and can choose to participate in decentralized applications and services that align with their values and interests (Dock Blog 2022).

Censorship resistance is a concept that refers to the ability of a system or network to withstand attempts to control or restrict access to information or communication. In the context of Web3, censorship resistance is the ability to prevent centralized authorities, such as governments or social media platforms, from controlling or manipulating the information or communication its users share (CoinMarketCap 2022). An example of censorship resistance is using a decentralized social media platform like Steemit. Steemit is built on the Steem blockchain and allows users to create and share content and earn rewards for their contributions. Because it is built on a decentralized blockchain, no central authority can censor or control the content shared on the platform (Voshmgir 2020).

Digital identity refers to how an individual or organization can establish and verify their online presence and collect information that represents them on the Internet (Dock Blog 2022). In traditional Web 2.0 systems, individuals are required to create a separate account for each platform they use. For instance, an individual may have a different account for Twitter and YouTube. This process not only requires a significant amount of time and effort but also poses a problem when an individual wishes to modify their display name or profile picture, as these changes must be made across all accounts. While social sign-ins may be used as an alternative in certain cases, they are not a foolproof solution as they still present the issue of censorship. With a single click, these platforms can restrict access to an entire online presence of an individual. Furthermore, many platforms necessitate sharing personally identifiable information to create an account, which raises concerns about trust and privacy. Web3 addresses the issues associated with traditional digital identity management by providing a decentralized solution based on an Ethereum address and ENS profile. With this approach, individuals can control their digital identity through a single login across multiple platforms, which is not only secure but also resistant to censorship and guarantee anonymity (Ethereum 2022a).

Native payment in Web3 refers to using cryptocurrencies and decentralized platforms for financial transactions on the Internet. This contrasts with traditional Web 2.0 payments, typically processed through centralized systems such as banks or payment processors. Web3 payments enable the transfer of money to be made directly of money on the platform using various cryptocurrencies, such as Bitcoin or Ethereum, without needing third-party payment processors, which can reduce costs and increase efficiency. These payments include faster, cheaper, and more secure transactions (Takyar 2022b)

6.2 The limitations

Web3 is still a relatively new concept and technology. Despite its potential benefits, it still faces several significant limitations for users, including technological and financial problems, usability, high entrance costs, and the prevalence of crypto, NFTs, and DeFi scams (Supra Oracles 2022). This is a major obstacle to the widespread adoption of Web3 and its potential to bring about a new era of decentralized and secure online interactions.

Entry to Web3 is currently hindered by high technical barriers. Users must have a clear understanding of security considerations, be able to interpret complex technical documentation, and navigate user interfaces that could be more intuitive (Ethereum 2022a). These difficulties arise from the complex processes and poor user interface design, making it challenging for people unfamiliar with the crypto world to access dApps. For example, obtaining a crypto wallet, a necessary first step for accessing Web3 can prove challenging even for tech-savvy individuals unfamiliar with the crypto space, particularly among older people. Furthermore, even for those willing to learn, the terms and mechanics of how many dApps and DeFi application functions can be confusing and difficult to understand. Simple financial activities, such as staking on PoS networks and staking LP tokens on exchanges for yield farming, need to be better explained by the platforms as they can also be a challenge for those not crypto-savvy (Supra Oracles 2022).

Transactions on dApps tend to be expensive, ranging from $35 to $100 or even more, resulting in gas fees that consume a significant portion of the investment for users who wish to invest a small amount in DeFi protocols or hold their assets. For instance, a user who wants to transfer $350 of crypto from their Coinbase account to a non-custodial wallet would likely need to pay a fee of $35-55, which constitutes 10-15% or more of their total transfer amount. These high fees undermine the notion that crypto transactions reduce costs, as they surpass most fees in traditional finance (Supra Oracles 2022).

Cryptocurrencies and DeFi present opportunities for criminal activity and exploitation by individuals and governments for personal gain. Such illicit activities include people utilizing these systems for traditional money laundering and hacking that take advantage of vulnerabilities in exchanges and DeFi protocols. According to blockchain data services firm Chainalysis, a total of $8.6 billion was laundered through cryptocurrencies in 2021 alone, with projections suggesting that this number will continue to rise in the years to come. Although blockchain-based transactions can be traced and important information is publicly accessible, the use of cryptocurrencies for money laundering is likely to increase shortly, especially with the growing popularity of privacy-focused cryptocurrencies such as ZCash (Supra Oracles 2022).

The instability of crypto assets and the occurrence of “pump and dump” or “rug pull” schemes pose a challenge to the growing crypto economy. Many individuals, drawn by the prospect of rapid wealth, have suffered substantial losses by investing in small-cap cryptos that were overhyped by influencers and failed to deliver on their promises. Although regulation may address some of these challenges, it could also limit the scope of innovations that have the potential to address real-world problems through crypto and DeFi. Additionally, NFTs, including virtual land, have experienced “pump and dump” scams. The practice of “wash trading,” in which an NFT creator purchases their NFT and resells it to inflate the price artificially, is also prevalent in the NFT market (Supra Oracles 2022).

7 DISCUSSION

As a web development major, my prior knowledge of the growth of the WWW, particularly Web3, was limited. This thesis presented an opportunity for me to gain a deeper understanding of the basics and applications of Web3. Initially, I was unaware of the discussions surrounding Web3 technology and its applications. However, through this thesis project, I was able to gain a general understanding of the architecture and technologies behind Web3. Despite facing challenges along the way, I was able to overcome them and achieve a sense of satisfaction with my work. Now I see Web3 as a new and important technology that will likely play a vital role in the future of the Internet. This thesis has also allowed me to improve my technical documentation skills and broaden my perspective on the evolution of the WWW and its impact on our lives. To conclude this thesis, I will provide a brief consideration of my research findings based on the content of this thesis.

The evolution of the WWW from Web 1.0 to Web 2.0 and now to Web 3.0 highlights a continuous journey towards a more connected, participatory, and secure online environment. Web 1.0 marks the beginning of the Internet as a tool for information sharing and communication. This was followed by the arrival of Web 2.0. Today, Web 2.0 continues to evolve and is prevalent through the widespread use of social media platforms such as Facebook and Instagram for connecting, sharing information, and creating content. Online communities, podcasts, and blogs allow for the collaborative exchange of ideas. Businesses and organizations use Web 2.0 technologies to engage with their customers and stakeholders, providing interactive experiences. The rise of mobile devices and the Internet of Things has further expanded the reach and capabilities of Web 2.0. However, in this era, tech giants such as Facebook and Google hold control over the utilization of personal data, using algorithms to influence the information that individuals consume. The third generation of WWW presents a significant shift in how the Internet operates and users interact with it, affecting not just Web 2.0 but other industries like finance, education, and entertainment. These changes aim to create a more intelligent, accessible, and secure web for all users.

The defining difference between Web 2.0 and Web 3.0 is the use of artificial intelligence. Web 2.0 is focused on user-generated content and collaboration. In contrast, Web 3.0 is designed to be more intelligent, using linked data and semantic technologies to create machine-readable data that can easily be processed and analyzed by AI systems.

The key between Web 2.0 and Web3 is how information is processed and stored. In Web 2.0, data is controlled by centralized intermediaries, such as social media platforms, whereas in Web3, the data is controlled by the users. This eliminates the need for intermediaries and gives users greater autonomy and control over their data. Additionally, the usage of smart contracts, decentralized networks, and blockchain technology in Web3 allows for more efficient and transparent transactions and interactions.

Developers face various constraints while constructing on the Web3 platform, including the complexity of the technology and limited document resources. These difficulties can impede the development process and make it challenging to create dApps of high quality. However, as the Web3 community grows and evolves, these limitations will probably be overcome, enabling developers to make even more innovative and impactful dApp.

It is important to note that Web3 is not meant to replace Web 2.0 but rather to evolve and complement it. While Web3 represents a major step forward in the evolution of the Internet, Web 2.0 is still a crucial part of the online landscape and will continue to be so in the foreseeable future. The integration of the best features from both Web 2.0 and Web3 will result in a more user-centric and decentralized Internet infrastructure.

REFERENCES

@gillesdc 2022. Web3 tour. Search date 2.2.2023. https://www.gillesdc.com/web3/tour

Aced, Cristina 2013. Web 2.0: The origin of the word that has changed the way we understand public relations. Search date 21.10.2022. https://www.researchgate.net/publication/266672416_Web_20_the_origin_of_the_word_that_has_changed_the_way_we_understand_public_relations

Akinola, Ayomide 2022. A brief history of Web3. Search date 3.12.2022. https://web3.hashnode.com/a-brief-history-of-web-3

Anderson, Paul 2007. What is Web 2.0? Ideas, technologies, and implications for education. Search date 28.10.2022. http://www.dator8.info/pdf/WEB2.0/0.pdf

Awosika, Emmanuel 2022a. What Is The Web3 Stack? Search date 15.12.2022. https://businesstechguides.co/what-is-the-web3-stack

Awosika, Emmanuel 2022b. Understanding The Ethereum Virtual Machine (EVM). Search date 16.12.2022. https://businesstechguides.co/what-is-the-ethereum-virtual-machine

Bashir, Imran 2022. Mastering Blockchain. Third Edition. Packt Publishing. Search date 04.01.2023. https://learning.oreilly.com/library/view/mastering-blockchain/9781839213199/ . Access required.

Behnke, Rob 2022. What is Web3? The ultimate guide. Search date 3.12.2022. https://halborn.com/what-is-web3-the-ultimate-guide/

Berners-Lee, Tim & Cailliau, Robert 12 November 1990. WorldWideWeb: Proposal for a HyperText Project. Search date 19.10.2022. https://www.w3.org/Proposal.html

Chalopin, Jean & Trehan, Robin 2022. A Brief History of Web 3.0. Search date 7.11.2022. https://www.deltecbank.com/2022/08/18/a-brief-history-of-web-3-0/?locale=en

Choudhury, Nupur 2014. World Wide Web and Its Journey from Web 1.0 to Web 4.0. International Journal of Computer Science and Information Technologies Volume 5 (6). Search date 19.10.2022. http://ijcsit.com/docs/Volume%205/vol5issue06/ijcsit20140506265.pdf

CoinMarketCap 2023. Censorship Resistance. Search date 28.1.2023. https://coinmarketcap.com/alexandria/glossary/censorship-resistance

Cointelegraph 2022a. What is Web 3.0: A beginner's guide to the decentralized internet of the future. Search date 12.1.2023. https://cointelegraph.com/blockchain-for-beginners/what-is-web-3-0-a-beginners-guide-to-the-decentralized-internet-of-the-future

Cointelegraph 2022b. What is Metaverse in blockchain? A beginner's guide on an Internet-enabled virtual world. Search date 4.3.2023. https://cointelegraph.com/metaverse-for-beginners/what-is-metaverse-in-blockchain

Dabit, Nader 2021. What is Web 3? The Decentralized Internet of the Future Explained. Search date 3.12.2022. https://www.freecodecamp.org/news/what-is-web3/

Dock Blog 2022. The Complete History of the WWW (From Web1 to Web3). Search date 28.1.2023. https://blog.dock.io/the-complete-history-of-the-world-wide-web/

Edelman, Gilad 2021. The Father of Web3 Wants You to Trust Less. Search date 8.11.2022. https://www.wired.com/story/web3-gavin-wood-interview/

Ethereum 2022a. Introduction to Web3. Search date 18.11.2022. https://ethereum.org/en/web3/

Ethereum 2022b. What is Ethereum?. Search date 9.12.2022. https://ethereum.org/en/what-is-ethereum/

Farah, Josiane 2012. Predicting the Intelligence of Web 3.0 Search Engines. International Journal of Computer Theory and Engineering, Volume 4 No. 3. Search date 9.11.2022. http://www.ijcte.org/papers/503-G1326.pdf

Governor, James, Hinchcliffe, Dion & Nickull, Duane 2009. Web 2.0 architectures. Beijing: Farnham: O'Reilly. Search date 19.10.2022. https://learning.oreilly.com/library/view/web-2-0-architectures/9780596514433/ . Access required.

Hooda, Parikshit 2022. Comparison – Centralized, Decentralized, and Distributed Systems. Search date 11.1.2023. https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/

IPFS 2022. What is IPFS? Search date 6.1.2023. https://docs.ipfs.tech/concepts/what-is-ipfs/#decentralization

Jacksi, Karwan & Abass, Shakir M. September 2019. Development History Of The World Wide Web. International Journal of Scientific & Technology Research Volume 8, Issue 09. Search date 19.10.2022. https://www.researchgate.net/profile/Karwan-Jacksi/publication/336073851_Development_History_Of_The_World_Wide_Web/links/5d8d1f8f92851c33e94064cb/Development-History-Of-The-World-Wide-Web.pdf

Jain, Shashank Mohan 2022. A Brief Introduction to Web3: Decentralized Web Fundamentals for App Development. Apress. Search date 10.1.2023. https://learning.oreilly.com/library/view/a-brief-introduction/9781484289754/ . Access required.

Kasireddy, Preethi 2021. The Architecture of Web 3.0 Application. Search date 2.11.2022. https://www.preethikasireddy.com/post/the-architecture-of-a-web-3-0-application

M. Rajendra Prasad, Dr. B. Manjula & V. Bapuji 2013. A Novel Overview and Evolution of World Wide Web: Comparison from Web 1.0 to Web 3.0. Search date 21.10.2022. http://www.ijcst.com/vol41/3/mrajendra.pdf

O'Reilly, Tim 30 September 2005. What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software. Search date 26.10.2022. https://www.oreilly.com/pub/a//web2/archive/what-is-web-20.html. Access required.

Patel, Karan 2013. Incremental Journey for World Wide Web: Introduced with Web 1.0 to Recent Web 5.0- A survey Paper. International Journal of Advanced Research in Computer Science and Software Engineering Volume 3 Issue 10. Search date 5.11.2022. https://www.researchgate.net/publication/262562142_Incremental_Journey_for_World_Wide_Web_Introduced_with_Web_10_to_Recent_Web_50_-_A_Survey_Paper

Reiff, Nathan 2022. Decentralized Autonomous Organization (DAO): Definition, Purpose, and Example. Search date 31.1.2023. https://www.investopedia.com/tech/what-dao/

Rijmenam, Mark Van 2022. Step into the Metaverse. Wiley. Search date 4.2.2023. https://learning.oreilly.com/library/view/step-into-the/9781119887577/ . Access required.

Schevchuk, Vitalii 2022. Top Web3 Architecture Layers Explained: Frontend, Backend, and Data. Search date 12.12.2022. https://itnext.io/top-3-web-3-0-architecture-layers-explained-frontend-backend-and-data-e10200f7fc76

Sharma, Rakesh 2022. What is Decentralized Finance (DeFi) and How does it work? Search date 2.2.2023. https://www.investopedia.com/decentralized-finance-defi-5113835

Sharma, Rakesh 2023. Non-Fungible Token (NFT): What it means and How it works. Search date 3.2.2023. https://www.investopedia.com/non-fungible-tokens-nft-5115211

Stackpole, Thomas 2022. What is Web3?. Search date 9.12.2022. https://hbr.org/2022/05/what-is-web3?ab=seriesnav-bigidea

Statista Research Department, Sep 20, 2022. Worldwide digital population July 2022. Search date 16.10.2022. https://www.statista.com/statistics/617136/digital-population-worldwide/

Supra Oracles 2022. The Pros and Cons of Web3. Search date 4.2.2023. https://supraoracles.com/academy/the-pros-and-cons-of-web3/

Takyar, Akash 2022a. Web3 vs Web 3.0: How are they different? Search date 9.11.2022. https://www.leewayhertz.com/web3-vs-web3-0/

Takyar, Akash 2022b. How Web3 is changing payments? Search date 29.1.2023. https://www.leewayhertz.com/how-does-payment-work-in-web3/

Takyar, Akash 2022c. DAO: The Future of Work. Search date 31.1.2023. https://www.leewayhertz.com/decentralized-autonomous-organization/

Voshmgir, Shermin 2020. Token Economy. Search date 21.11.2022. https://blockchainhub.net/web3-decentralized-web/

W3C 2022a. Facts about W3C. Search date 1.12.2022. https://www.w3.org/Consortium/facts

W3C 2022b. W3C Mission. Search date 1.12.2022. https://www.w3.org/Consortium/mission

W3C Technical Architecture Group, December 15, 2004. Architecture of the World Wide Web, Volume One. Search date 17.10.2022. https://www.w3.org/TR/webarch/

Wikipedia 2022. Facebook–Cambridge Analytica data scandal. Search date 7.12.2022. https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal