CommIT Journal 19(1), 29–43, 2025

Architecture for the Academic Certificate System on the Ethereum Layer 2 Solution

Sukosol Wanotayapitak*
Department of Information Technology, Faculty of Digital Technology and Innovation,
Southeast Bangkok University
Bangkok, Thailand 10260
Email: sukosol@southeast.ac.th

***Abstract*—The Ethereum blockchain, plagued by network congestion and exorbitant transaction fees, faces significant scalability challenges. While Layer 2 solutions offer a promising avenue to address these concerns, their potential remains largely unexplored on blockchain applications. The research proposes a novel Layer 2 architecture specifically designed for the academic certificate system on the Ethereum network. The method commences with a comprehensive survey of existing literature, followed by an analysis of solutions within the business domain. Subsequently, the most suitable and comprehensive solutions are identified for integration into the proposed academic certificate system architecture. In the selection process, the research analyzes 20 studies to determine the frequency of solutions employed in each investigation. The results indicate the InterPlanetary File System (IPFS) exhibiting the highest frequency, while Oracle, Decentralized Identifiers (DIDs), and Application Programming Interfaces (APIs) have comparable frequencies. Furthermore, an analysis of rankings from 10 websites evaluating Layer 2 Ethereum solutions and their performance across various aspects reveals Arbitrum as the top-ranked solution, followed by Polygon and Optimism, respectively. The research demonstrates the implementation of this system architecture within the proposed system's process. The culmination of this effort is a valuable blueprint for developers seeking to build and deploy similar systems efficiently. Notably, the inherent adaptability of the architecture extends beyond the educational domain, paving the way for its application across diverse contexts. The system architecture presented constitutes an initial exploration into developing Decentralized Applications (DApps) on the Ethereum Layer 2 network because prior research has not specifically focused on its application.**

***Index Terms*—Ethereum Layer 2 Solution, Blockchain, Academic Certificate**

I. Introduction

CERTIFICATES serve as official documentation, attesting to an individual's successful completion of studies and verifying their acquired knowledge and skills. Historically, they have served as crucial evidence in securing employment and pursuing further education. However, the critical role of certificates as proof of qualifications renders them vulnerable to counterfeiting, with the intent to deceive individuals into accepting forged documents as genuine. Before the widespread adoption of computerized systems, paper certificates necessitated extensive verification procedures by educational institutions to identify potential forgeries.

While traditional paper certificates remain commonplace, the digital age has ushered in online digital certificates. However, these digitized credentials are not immune to the threat of counterfeiting. Despite the ease of access that the online display affords, digital information's inherent excitability, reproducibility, and rapid dissemination make it more susceptible to forgery than its paper counterpart. Consequently, digital documents lack admissibility without verification through reliable mechanisms, such as electronic signature verification by a trusted institution. Despite their long-standing existence, this vulnerability has hindered the widespread adoption of digital certificates.

The advent of blockchain technology has fundamentally reshaped digital information management, enabling its secure and reliable utilization. This transformative technology traces its origins to Bitcoin, the first cryptocurrency introduced by Satoshi Nakamoto [1]. The Ethereum blockchain further propels this technological advancement by pioneering smart contracts, which facilitate the automation of digital transactions [2]. Blockchain technology has evolved beyond its initial application in cryptocurrencies, emerging as a versatile tool for decentralized applications, finance, and governance. Significant advancements include Layer 1 solutions, exemplified by Ethereum 2.0's transition to a proof of stake consensus mechanism, and Layer 2 scalability technologies, such as rollups. Interoperability protocols, including Polka-

Received: April 23, 2024; received in revised form: Oct. 09, 2024; accepted: Oct. 09, 2024; available online: April 17, 2025.
*Corresponding Author

dot and Cosmos, facilitate communication between disparate blockchain networks. Decentralized finance platforms offer an array of financial services, encompassing lending, trading, and yield optimization strategies. The proliferation of Non-Fungible Tokens (NFTs) and asset tokenization creates novel digital asset classes, particularly within gaming ecosystems and virtual environments [3]. Concurrent developments in privacy-enhancing technologies, enterprise-focused blockchain solutions, and regulatory frameworks, such as the European Union's Markets in crypto-assets regulation, shape the broader ecosystem [4] while the field faces persistent challenges related to scalability, security, and environmental sustainability, innovation continues to progress rapidly across various domains within the blockchain space.

Ethereum's applications permeate various industries, including the domain of education. It extends beyond the realm of finance. Researchers within the educational field have acknowledged the potential of blockchain technology to revolutionize existing systems, particularly in the context of certificate management. However, Ethereum, a publicly accessible global blockchain, faces significant challenges stemming from high transaction congestion and exorbitant fees. As of 2023, it processed a mere 20–30 Transactions per Second (TPS) with average fees of $7, reaching a peak of $40 in 2021 [5]. These unsustainable costs, projected to escalate with an increasing user base, pose a substantial obstacle to widespread adoption.

In response to scaling concerns, Layer 2 solutions have emerged within the Ethereum ecosystem, enabling high-throughput transactions at substantially reduced costs [6]. Despite their inherent promise, a comprehensive analysis of extant literature across diverse domains unveils a paucity of research specifically dedicated to exploring Layer 2 solutions and their integration with the Web3 infrastructure. This dearth of focused research impedes the full realization of this transformative technology's potential.

The research aims to develop a system architecture for an academic certificate platform addressing the following objectives:

1) Identify and integrate appropriate and efficient Web3 solutions as components within the system architecture.
2) Evaluate and select optimal Ethereum Layer 2 solutions for seamless integration with Web3 components within the architecture.
3) Demonstrate the practical implementation of the proposed system architecture through the development of real-world applications.

II. Research Method

The process of designing an academic certificate system architecture to achieve the research objectives comprises the following steps:

1) Explore the literature related to blockchain application research in four main domains: health care, education, Internet of Things (IoT), and security.
2) Analyze and classify Web3 solutions used in research across all four domains.
3) Summarize the analysis results and classify the solutions based on their frequency of application to identify the most popular Web3 solutions for integration into the system architecture.
4) Survey articles from ten technology websites regarding the popularity ranking of Ethereum Layer 2 solutions.
5) Analyze and score Ethereum Layer 2 solutions according to various performance aspects to select high-scoring solutions.
6) Utilize the selected Web3 and Ethereum Layer 2 solutions to design an academic certificate system architecture.
7) Implement the designed architecture of academic certificate system to develop a real-world academic certificate system.

Then, the research data collection procedure comprises the following steps. First, the researcher delineates the scope of blockchain capabilities examined. The researcher investigates the design of system architectures for blockchain technology, focusing on four key areas: 1) scalability and efficiency, aiming to address limitations in transaction throughput and processing speed; 2) security and privacy, encompassing research on designing architectures that enhance the security posture of blockchain systems; 3) interoperability and integration, exploring architectures that enable communication and interaction between different blockchains; and 4) domain-specific system architecture, exemplified by the design of a customized architecture for an educational certificate system leveraging blockchain technology. Second, the researcher specifies the domain of focus for the investigation. The researcher undertakes a systematic literature review to explore the diverse applications of blockchain technology comprehensively across four distinct domains: security, education, health care, and IoT. Third, the researcher establishes the criteria for selecting relevant research articles. The primary objective of this review is to analyze and synthesize existing data on Web3 infrastructure and services within these domains, thereby establishing a foundational framework for the subsequent research phase. To ensure the relevance and contemporary nature of the reviewed research, the

researcher implements two inclusion criteria: 1) the research must leverage Web3 infrastructure or services that demonstrably enhance the targeted system, and 2) the research must have been published within the past five years.

When all three steps of the data collection process are carried out, the result is research data that meets all the conditions and criteria. It results in 20 previous studies. The first research proposes a novel system for document sharing and version control that leverages blockchain technology to eliminate the need for a central authority. The system utilizes smart contracts to manage the process, enabling secure and decentralized document storage on a distributed file system. The authors implement and test this system, making the smart contract code publicly available [7].

The second research suggests a fully decentralized solution for multiparty authorization that leverages Ethereum smart contracts, InterPlanetary File System (IPFS) storage, and Oracle for computationally expensive tasks. The system incorporates reputation mechanisms to ensure trust. It is also secure, cost-effective, and generalizable. With its source code publicly available, this novel approach effectively addresses the limitations of existing centralized systems and offers a more trustworthy and efficient way to manage access to shared data [8].

The third research proposes a platform for secure and privacy-preserving decentralized data sharing among untrusted participants in off-grid networks. The platform integrates with existing blockchain frameworks (Hyperledger Fabric, Indy, Aries), leverages off-grid network devices, and distributes file systems. Its performance, evaluated through experiments, demonstrates promising throughput and latency characteristics, making it suitable for supporting off-grid decentralized applications. This innovative approach addresses the limitations of centralized systems and empowers previously unconnected communities through secure and transparent communication within off-grid networks [9].

The fourth research provides the initial design of a decentralized and peer-to-peer service discovery system. This system empowers peers to both offer and request services, creating a novel "market of services" where providers and brokers can compete based on factors such as price and uptime. Notably, it leverages Decentralized Identifiers (DIDs) as a critical mechanism for service discovery [10].

The fifth research proposes a privacy-preserving data marketplace for generating statistics. It allows data providers to sell information while protecting their privacy using differential privacy and blockchain. The system targets scenarios with numerous data providers. A proof of concept for smart grids demonstrates its feasibility [11].

The sixth research uses MedSecureChain, a novel blockchain-based identity and access management system designed for the medical ecosystem. It leverages OAuth for delegated access control and the IPFS for decentralized data storage, guaranteeing user data privacy and security. Furthermore, smart contracts enhance the system's security by eliminating dependence on a single authority, leading to improved data control and decentralization [12].

The seventh research examines a novel approach leveraging blockchain technology and NFTs for time-bound access and monetization of private data. Users upload encrypted content and mint it into NFTs, which are accessible to others via purchase or licensing. Purchasing transfers ownership, while licensing grants limited access, with automatic data deletion afterward. This decentralized and robust system utilizes Decentralized Applications (DApps), proxy re-encryption, IPFS, and a trusted execution environment. A proof of concept implemented on an Ethereum environment demonstrates functionality and security, with cost and generalization analysis provided. The project's source code is publicly available under an open-source license [13].

The eighth research proposes a secure communication framework for the future, leveraging blockchain technology and signcryption for robust data confidentiality and authentication. This framework facilitates noninteractive message verification and audit trails, harnessing blockchain's tamper-proof nature to ensure non-repudiation, availability, and public verification. It seamlessly integrates with both large data (e.g., files) and small data (e.g., cryptographic hashes) transfer scenarios, utilizing the IPFS as a decentralized storage platform for large data sets [14].

The ninth research suggests a blockchain-based architecture for e-learning solutions. It highlights the advantages of immutability, security, transparency, and a simplified global ecosystem. The aim is to create a universally trusted system for managing and verifying educational credentials [15].

The tenth research tackles the issues of fraud and data breaches in educational institutions by proposing a secure and transparent blockchain-based identity management system. Leveraging Hyperledger Indy and the Plenum-based Redundant Byzantine Fault Tolerance (RBFT) protocol, the previous authors use this framework to bolster trust and security within the education system. The RBFT algorithm guarantees data integrity while preventing human intervention and manipulation, fostering a more reliable environment for educational data management [16].

The eleventh research employs EduChain, a novel heterogeneous blockchain system utilizing both private and consortium blockchains to improve data security and transparency. EduChain also introduces a novel mechanism for database consistency checks and error tracking, ensuring data integrity and enabling efficient error identification. The system demonstrates strong performance in information verification, error traceback, and data security, offering a promising solution for educational data management [17].

The twelfth research explores the potential of Distributed Ledger Technology (DLT) to address financial challenges within higher education. It proposes the ASTER open-source system as a hybrid DLT architecture for student assignment submission and grading, mitigating concerns inherent in traditional systems such as centralization and downtime. However, it also discusses the potential security implications of utilizing a public ledger for student work alongside this novel approach's broader advantages and disadvantages [18].

The thirteenth tackles the limited adoption of blockchain technology in education by proposing DApps for managing and verifying educational credentials. It integrates a codesign methodology rooted in blockchain-oriented software engineering to prioritize users' needs and address real-world industry challenges. The DApps foster social awareness and knowledge of this emerging technology while simultaneously offering a modular architecture, interoperability-supported tools, and a carefully selected blockchain platform. These advancements are anticipated to enhance adoption potential significantly, particularly within the education and recruitment sectors [19].

The fourteenth research proposes a patient-centric system built on the Ethereum blockchain, granting patients secure, verifiable, and tamper-proof control over their medical data. The system ensures data security and privacy while enabling controlled sharing by leveraging decentralized storage and trusted re-encryption methods. This comprehensive work details the system's design, implementation, performance evaluations, security analysis, and limitations, aiming to empower patients with data ownership and revolutionize the healthcare landscape [20].

The fifteenth research explores a secure and privacy-preserving consortium blockchain-based scheme for managing and sharing personal health records. The scheme leverages the IPFS for secure storage and zero-knowledge proofs for verifying keyword index authenticity on the blockchain. It further utilizes customized attribute-based encryption and smart contracts for secure search, preserving privacy and enabling personalized access control. Extensive security analysis and real-world data evaluations demonstrate the scheme's effectiveness and superiority compared to existing solutions [21].

The sixteenth research proposes a novel solution for exchanging electronic health records that prioritizes security, privacy, and user control. The solution combines blockchain technology, self-sovereign identity (SSI), and decentralized storage to achieve these goals [22].

The seventeenth research suggests a novel middleware for seamless IoT-Ethereum integration. This addresses the critical need for tamper-proof and traceable data distribution in the IoT domain. Their solution guarantees data integrity and facilitates real-time data distribution through a secondary IPFS channel, bridging a crucial gap in blockchain-IoT integration and paving the way for secure and efficient data distribution within the ever-evolving world of interconnected devices [23].

The eighteenth research examines a service model for IoTs that combines blockchain and the IPFS for efficient, secure data and service sharing. Hashed credentials and data reside on the IPFS for fast access, while encrypted hash values secure them on the blockchain. Service discovery is achieved through consumer requests on the blockchain. Utilizing proof of authority and a service verification scheme reduces computational costs. Smart contracts facilitate dispute resolution between consumers and providers. Then, simulations demonstrate the model's superior efficiency and effectiveness compared to existing solutions [24].

The nineteenth research utilizes a novel decentralized identity framework for Industrial IoTs based on the SSI model. This framework is implemented and evaluated on two blockchain platforms, Ethereum and Hyperledger Indy, to analyze the underlying performance overhead [25].

The twentieth research proposes a novel decentralized architecture for the IoT that leverages blockchain and a distributed Oracle layer to unlock the potential of a global IoT market. This solution offers data independence, automatic discovery, and robust data quality, addressing the limitations of centralized systems and paving the way for a new era in IoT data exchange [26].

III. Results and Discussion

A. Previous Research Analysis

The literature review identifies several Web3 infrastructures and services, including the IPFS, Oracle, DIDs, and APIs, summarized in Table I. Then, the frequency distribution of Web3 solution adoption across four domains is visually represented in Fig. 1. From the analysis results in Table I and Fig. 1, the IPFS is the most popular Web3 infrastructure component across

TABLE I
WEB3 INFRASTRUCTURES AND SERVICES.

Articles	Domains	IPFS	Oracle	DIDs	APIs
[5]	Security	✓	✓	X	X
[6]	Security	✓	✓	X	X
[7]	Security	✓	X	✓	X
[8]	Security	✓	X	✓	✓
[9]	Security	✓	X	✓	X
[10]	Security	✓	X	X	X
[11]	Security	✓	✓	X	X
[12]	Security	✓	✓	X	X
[13]	Education	✓	X	X	✓
[14]	Education	X	X	✓	✓
[15]	Education	✓	X	X	✓
[16]	Education	✓	X	X	✓
[17]	Education	✓	X	✓	✓
[18]	Healthcare	✓	✓	X	X
[19]	Healthcare	✓	✓	X	X
[20]	Healthcare	✓	X	✓	X
[21]	IoT	✓	X	X	X
[22]	IoT	✓	X	X	X
[23]	IoT	✓	X	✓	X
[24]	IoT	✓	✓	X	X
		19	7	7	6

Note: InterPlanetary File System (IPFS), Decentralized Identifiers (DIDs), Application Programming Interfaces (APIs), and Internet of Things (IoT).

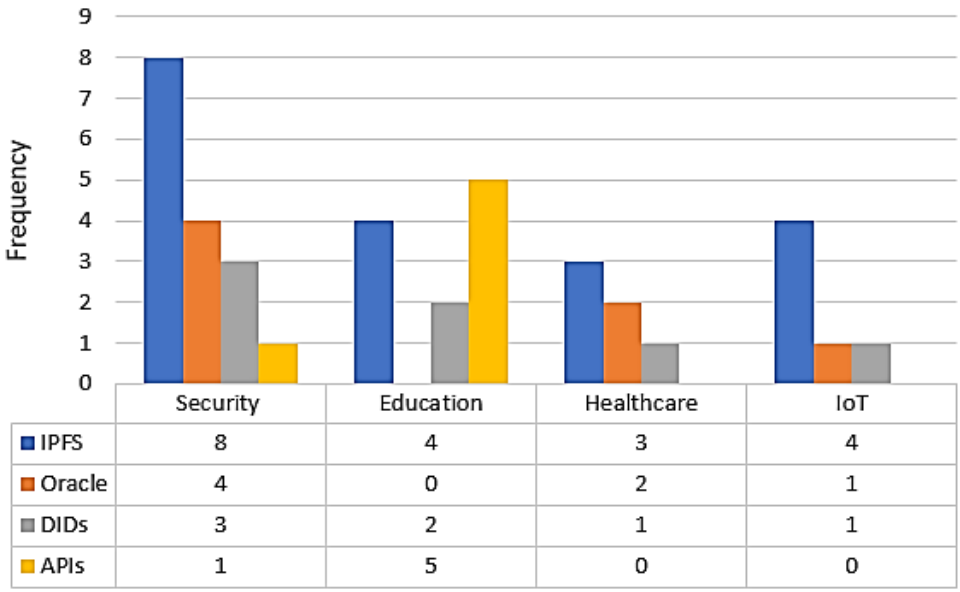

Fig. 1. The frequency distribution of Web3 solution adoption across four domains. InterPlanetary File System (IPFS), Decentralized Identifiers (DIDs), Application Programming Interfaces (APIs), and Internet of Things (IoT).

all domains. This finding highlights the widespread recognition of on-chain storage limitations and the consequent emphasis on off-chain solutions. Oracle and DIDs receive comparable research attention, while APIs, though not categorized as Web3 infrastructure, also attract considerable interest. However, all three components remain less popular than the IPFS, as evidenced by the significantly lower number of associated studies.

Moreover, Oracle appears in all research domains except education, with the security domain boasting the highest prevalence, followed by healthcare and IoT, respectively. The result reflects these domains’ openness and Oracle technology’s critical role. Conversely, the education system’s focus on academic institutions likely explains the limited research attention it receives. APIs are most commonly encountered in education, whereas their presence is rare or nonexistent in other

TABLE II
DISTRIBUTION OF WEB3 SOLUTION ADOPTION ACROSS DOMAINS (IN PERCENTAGE).

Domains	IPFS	Oracle	DIDs	APIs
Security	100	50	38	13
Education	80	0	40	100
Healthcare	100	67	33	0
IoT	100	25	25	0

Note: InterPlanetary File System (IPFS), Decentralized Identifiers (DIDs), Application Programming Interfaces (APIs), and Internet of Things (IoT).

domains. It suggests that educational applications often involve multiple stakeholders, necessitating an interface for easy data access. APIs effectively fulfill this need, whereas domains with fewer stakeholders may not require separate APIs as the system can provide access.

A detailed analysis of Web3 solution adoption across domains reveals the relative significance of each solution within specific sectors, as illustrated in Table II. The findings indicate several notable trends. First, the IPFS demonstrates high importance across all four domains, with adoption rates ranging from 80% to 100%. Second, the education sector shows no adoption of Oracle (0%) but full utilization of APIs (100%). Conversely, the healthcare sector exhibits the highest Oracle adoption (67%), followed by the security (50%) and IoT (25%) domains, respectively. Third, healthcare and IoT domains show no adoption of APIs (0%). Last, DIDs exhibit low to moderate adoption across all domains (25–40%), with the highest rate in education (40%), followed by security (38%), health care (33%), and IoT (25%).

B. Selection of Ethereum Layer 2 Solutions

Due to the proliferation of Ethereum Layer 2 solutions on the market, careful selection is crucial for architectural implementation. It necessitates a multistage evaluation process. The stage involves a comprehensive survey of Layer 2, gathering ranking data from ten established websites. The data are then converted into a numerical score based on the following criteria: 3 for first place, 2 for second place, and 1 for third place. The solution with the highest cumulative score is ranked first, followed by second and third, respectively. The results of this survey and scoring are presented in Table III.

Based on the rankings of Layer 2 solutions in 10 technology websites, six solutions are identified as top contenders: Arbitrum, Polygon, and Optimism, respectively. Solutions ranked fourth to sixth are excluded from further consideration. However, it is important to

TABLE III
WEBSITE RANKINGS OF LAYER 2 SOLUTION.

Sources	AR	PO	OP	LR	IX	OM
[27]	3	2	0	0	1	0
[28]	2	3	1	0	0	0
[29]	3	1	2	0	0	0
[30]	3	2	1	0	0	0
[31]	3	3	2	0	0	0
[32]	2	3	0	1	0	0
[33]	0	3	0	2	0	1
[34]	3	0	2	0	1	0
[35]	2	3	0	1	0	0
[36]	3	1	2	0	0	0
Sum	24	21	10	4	2	1
Rank	1	2	3	4	5	6

Note: AR = Arbitrum, PO = Polygon, OP = Optimism, LR = Loopring, IX = Immutable X, and OM = OmiseGo.

acknowledge that the website rankings primarily reflect the individual opinion of the researcher and may not provide a definitive evaluation of the solutions' true potential. Therefore, a more comprehensive assessment focuses on in-depth feature analysis across six key areas: throughput, decentralization, security, scalability, transaction fees, and Ethereum Virtual Machine (EVM) compatibility. A three-tier scoring system is employed, with "Highest" scoring 3, "Medium" scoring 2, and "Lowest" scoring 1. Each feature is evaluated by comparing reference data from various sources and assigning a score based on the relative strengths of the three shortlisted solutions. The results are presented in Tables IV–VI.

As indicated by the analysis in Table IV, Polygon demonstrates strengths in throughput, scalability, and transaction fees. However, it exhibits weaknesses in terms of decentralization and security. Meanwhile, in Table V, Arbitrum demonstrates strong performance in decentralization, security, and EVM compatibility. Furthermore, it exhibits notably positive results in terms of throughput, scalability, and transaction fees. Next, in Table VI, Optimism demonstrates strengths in decentralization and security but exhibits weaknesses across the remaining attributes.

Significant differences exist in transaction processing speed (throughput) among the three solutions. Polygon boasts 65,000 TPS, followed by Arbitrum at 40,000 TPS and Optimism at 2,000 TPS [37]. Consequently, Polygon, Arbitrum, and Optimism receive scores of 3, 2, and 1 respectively, for this feature. These variations in throughput arise from the distinct technologies employed by each solution. Optimism and Arbitrum utilize the Optimistic rollup technique, while Polygon leverages a sidechain approach, resulting in differing characteristics [38]. Rollup solutions retain transaction data on the main Ethereum network

TABLE IV
IN-DEPTH FEATURE RATINGS ACROSS THE LAYER 2 SOLUTIONS (POLYGON).

Attributes	Values	Score
Throughput	65,000 Transactions per Second (TPS)	3
Decentralization	Sidechain	1
Security	Sidechain	1
Scalability	Sidechain	3
Transaction fee	$<$ \$0.01	3
Ethereum Virtual Machine (EVM)-compatible	Solidity, Vyper	2
Sum		13
Rank		2

TABLE V
IN-DEPTH FEATURE RATINGS ACROSS THE LAYER 2 SOLUTIONS (ARBITRUM).

Attributes	Values	Score
Throughput	40,000 Transactions per Second (TPS)	2
Decentralization	Rollups	3
Security	Rollups	3
Scalability	Rollups	2
Transaction fee	\$0.27	2
Ethereum Virtual Machine (EVM)-compatible	All EVM languages	3
Sum		15
Rank		1

TABLE VI
IN-DEPTH FEATURE RATINGS ACROSS THE LAYER 2 SOLUTIONS (OPTIMISM).

Attributes	Values	Score
Throughput	2,000 Transactions per Second (TPS)	1
Decentralization	Rollups	3
Security	Rollups	3
Scalability	Rollups	1
Transaction fee	\$0.44	1
Ethereum Virtual Machine (EVM)-compatible	Solidity	1
Sum		10
Rank		3

TABLE VII
SUMMARY OF OVERALL SCORES AND RANKINGS OF THE LAYER 2 SOLUTIONS.

Attributes	Score		
	AR	PO	OP
Throughput	2	3	1
Decentralization	3	1	3
Security	3	1	3
Scalability	2	3	1
Transaction fee	2	3	1
Ethereum Virtual Machine (EVM)-compatible	3	2	1
Sum	15	13	10
Rank	1	2	3

Note: AR = Arbitrum, PO = Polygon, and OP = Optimism.

(Layer 1 solution), thereby maintaining high levels of decentralization and security [39]. It contrasts with sidechains, which operate as independent blockchains detached from the main Ethereum network [40]. While sidechains offer lower levels of decentralization and security, they compensate by providing faster transaction processing speeds and lower fees due to their independent operation and the absence of time-consuming fraud-proof challenges inherent in rollup solutions [41]. Therefore, Optimism and Arbitrum, which use the Optimistic rollup technique, receive a score of 3 for decentralization and security features, while Polygon, utilizing the sidechain approach, has a score of 1.

Polygon, on the other hand, obtains a score of 3 for scalability, while both Optimism and Arbitrum share the same fraud-proofing challenges. Arbitrum demonstrates superior performance in this area, earning a score of 2, compared to Optimism with a score of 1. Similarly, due to its scalability advantage, Polygon offers the most affordable transaction fees, followed by Arbitrum and Optimism. It translates to transaction fee scores of 3 for Polygon, 2 for Arbitrum, and 1 for Optimism.

Regarding EVM compatibility, the supported programming languages differ among the solutions. Optimism supports only Solidity. Then, Polygon supports both Solidity and Vyper, and Arbitrum supports Solidity, Vyper, Flint, and Yul+ [42]. Consequently, the EVM compatibility scores are 1 for Optimism, 2 for Polygon, and 3 for Arbitrum.

In summary, the overall score ranking for the three solutions remains unchanged, with Arbitrum leading the way, followed by Polygon and Optimism. Therefore, the researcher concludes that the Arbitrum solution is the most suitable choice for integration with the Web3 infrastructure components and services within the architectural design and implementation of the educational certificate system. The summary can be seen in Table VII.

C. System Architecture

Based on research analysis and proposed solutions to support Ethereum Layer 2 DApps, the resulting system architecture is depicted in Fig. 2. The proposed architecture comprises four primary components: Web3 infrastructure, DApps, APIs, and Ethereum Layer 2. The functionalities of each component are detailed as follows.

The aspiration for a decentralized and user-controlled Internet, as envisioned by Web3 infrastructures, harbors immense potential to transform the interaction with information and technology fundamen-

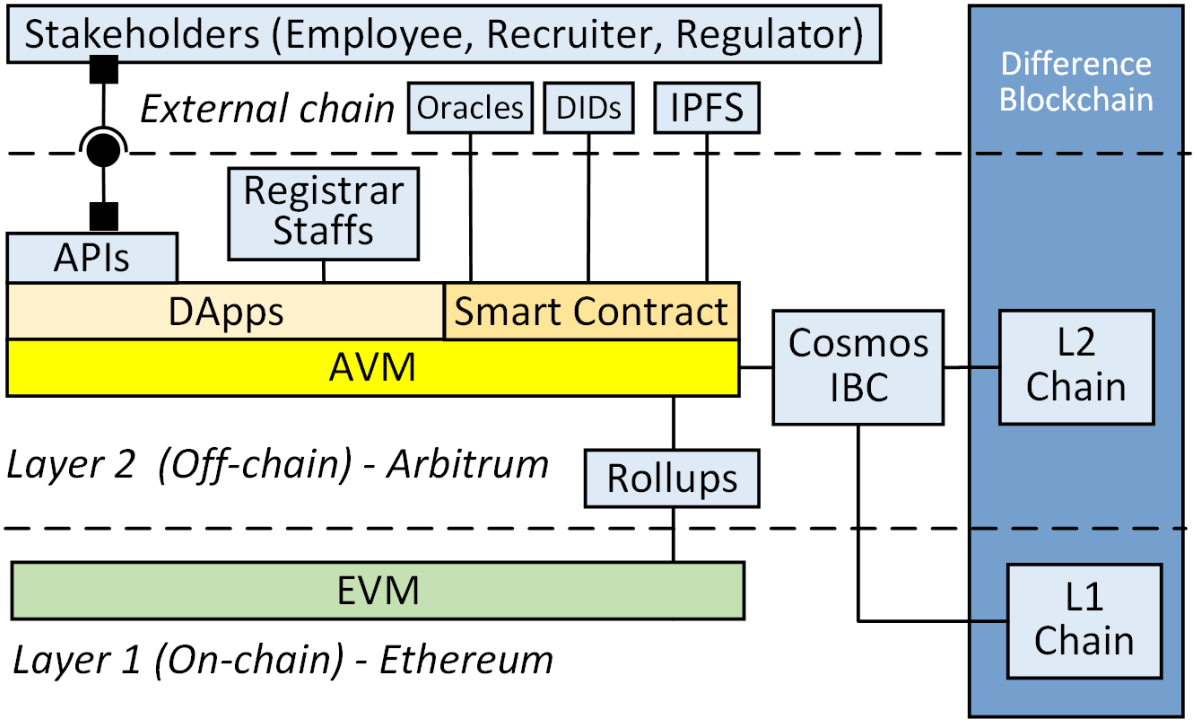

Fig. 2. Academic certificate system architecture on Ethereum Layer 2. It has Decentralized Identifiers (DIDs), InterPlanetary File System (IPFS), Application Programming Interfaces (APIs), Decentralized Applications (DApps), Arbitrum Virtual Machine (AVM), Inter-Blockchain Communication protocol (IBC), Ethereum Virtual Machine (EVM), Layer 2 (L2), and Layer 1 (L1).

tally [43]. However, the realization of this vision hinges on the development of a robust and adaptable infrastructure capable of sustaining its growth and functionality. In this context, Web3 infrastructure emerges as the bedrock upon which the decentralized applications and services of the future will be built [44]. The Web3 infrastructure comprises blockchain networks, distributed Oracle, distributed data stores, identity management systems, and interoperability protocols. The proposed architecture mandates smart contract control over all web3 components.

Blockchain networks are distributed ledgers, serving as the bedrock upon which the Web3 ecosystem rests. It functions as a secure and tamper-proof platform for recording and verifying transactions [45]. Prominent examples include Ethereum, Solana, Avalanche, and Cosmos, each contributing to the flourishing of Web3 development.

Decentralized Oracle acts as a bridge between the real world and the realm of blockchain. These services empower smart contracts to access and utilize external data and events [46]. Chainlink and Band Protocol stand as exemplary decentralized Oracle networks [47], facilitating this crucial interaction and enabling smart contracts to operate within the broader context of the real world. Harnessing pre-built functionalities via APIs presents numerous advantages for both developers and users. Developers experience significant efficiency gains, reductions in development time and costs, and the opening of doors to innovation. Furthermore, APIs enhance the scalability of applications, facilitating effortless accommodation of expanding user bases and the seamless integration of new features [48].

Decentralized storage offers secure and tamper-proof alternatives to centralized storage servers. These platforms empower users with greater control and autonomy over their data [49]. Leading examples include the IPFS [50], Arweave [51], and Filecoin [52], each providing a decentralized and verifiable platform for data storage.

The identity management system can empower users to own and manage their online identities. These solutions promote a more autonomous and privacy-centric Web3 experience. SelfKey and the Decentralized Identity Foundation (DIF) actively engage in developing decentralized identity standards and protocols, laying the groundwork for a user-centric approach to identity management within the Web3 ecosystem [53].

The interoperability protocols enable seamless communication and data exchange between diverse blockchain networks [54]. These bridges foster a more interconnected and interoperable Web3 ecosystem.

Cosmos IBC and Chainlink Cross-Chain Interoperability Protocol (CCIP) serve as key examples of such interoperability protocols, paving the way for enhanced collaboration [55], innovation, and the potential for a more unified Web3 experience.

The second architectural component is DApps, which constitutes the Web3 infrastructure's landscape. DApps comprise a diverse tapestry of technologies, tools, and services that form the foundation for the development and operation of Web3 applications and services [56]. The proposed architecture incorporates two roles of DApps: DApps on Layer 2 and DApps within Arbitrum Virtual Machine (AVM) [57]. In the role of DApps on Layer 2, the academic certificate system resides between Layer 1 and the external chain. The stakeholders outside the blockchain, such as employers, recruiting agencies, and regulators, can interface with the DApps through APIs, facilitating a quick and efficient user experience. Access of registrar staff within Layer 2 bypasses APIs but necessitates authentication via DIDs stored on the IPFS. Meanwhile, Oracle provides smart contract conditions within the Web3 infrastructure. All three components collaborate with smart contracts to execute certificate transactions.

In the role of DApps within AVM, Arbitrum utilizes optimistic rollups to interact seamlessly with EVM Ethereum [58]. Users submit transactions to the sequencer, which aggregates them into batches, updates the AVM Arbitrum state, and generates proofs for validation on Ethereum. After a designated challenge period, state updates are finalized on Ethereum, guaranteeing the integrity of the system. Users can readily withdraw funds back to Ethereum through the bridge, completing the cross-chain interaction [59]. DApps of the certificate system on Arbitrum can interact with various blockchains through Cosmos IBC, enabling efficient cross-chain access to assets and functionalities. A bridge contract acts as a communication bridge between the chains, ensuring the reliable transfer of information and assets. Transactions are finalized on both chains, providing enhanced security and guaranteeing the integrity of the system.

APIs are the third component of the proposed architecture. They serve as the crux of communication between software programs, analogous to a restaurant menu. They provide a transparent and concise catalog of available functionalities and access protocols, facilitating seamless communication and data exchange [60]. In essence, APIs function as digital messengers, conveying user requests to service providers and delivering the corresponding responses. This crucial functionality dramatically simplifies software development and fosters seamless integration with diverse services.

The final component of the proposed architecture is the Ethereum Layer 2 solution. The exponential growth of Ethereum has introduced a critical challenge–scalability [61]. Fortunately, innovative Layer 2 scaling solutions have emerged as a promising countermeasure, paving the way for Ethereum's continued viability and sustained future success. L2 solutions are currently in various stages of development and implementation, each offering a unique approach and distinct advantages.

D. System Architecture Implementation

To offer a deeper understanding of the proposed system architecture, the researcher details its implementation within the certification system process. It is divided into two key phases: certificate issuance and certificate viewing. These phases are represented in two activity diagrams. The certificate issuance system and viewing system process appear in Figs. 3 and 4, respectively.

In Fig. 3, the system initiates with the registrar logging in through an authentication mechanism. This mechanism leverages DIDs to search for personal identity information stored on the IPFS. In the absence of such information, the registrar is redirected to a new login screen for completion. Once the information is verified as correct, the process proceeds to the next step. It involves executing a smart contract that triggers the issuance of the student's certificate and subsequent updates that are reflected across the system.

In Fig. 4, multiple stakeholders require access to student certificates, each with their motivations. For example, employers seek to verify credentials for job applications, recruitment agencies aim to evaluate potential candidates, and regulators strive to ensure educational quality assurance. Despite stakeholders' diversity, they all utilize standardized APIs to interact with the system, facilitating accessibility for users within the blockchain network. Once API access is granted, a smart contract triggers a request for the student's certificate. This request prompts a data retrieval process via Oracle to ascertain the student's graduation status. If the student has not yet graduated, stakeholders are notified accordingly. However, upon graduation, the certificate information is retrieved from the IPFS and subsequently relayed to stakeholders.

It is noteworthy that the certificate viewing system does not necessitate interaction with Arbitrum or Ethereum because no data updates are required. Furthermore, its implementation can be achieved more efficiently than the certificate issuance process, which is attributable to the reduced number of steps and the absence of Layer 1 and Layer 2 interaction.

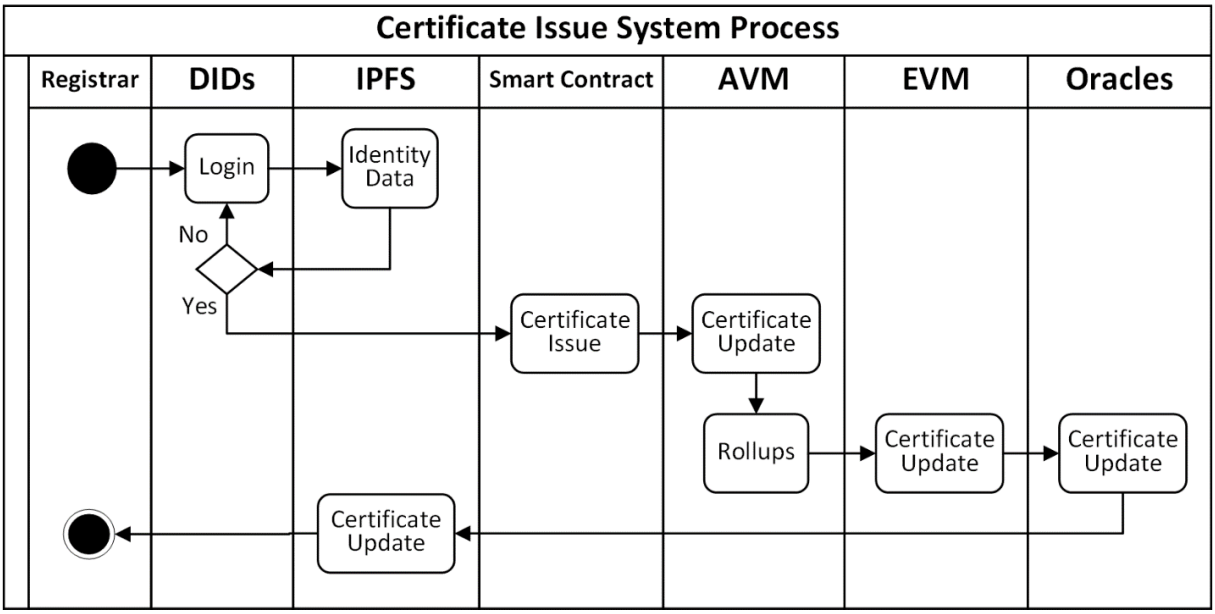

Fig. 3. Implementation of the academic certificate system architecture in the certificate issuance process. It has Decentralized Identifiers (DIDs), InterPlanetary File System (IPFS), Arbitrum Virtual Machine (AVM), and Ethereum Virtual Machine (EVM).

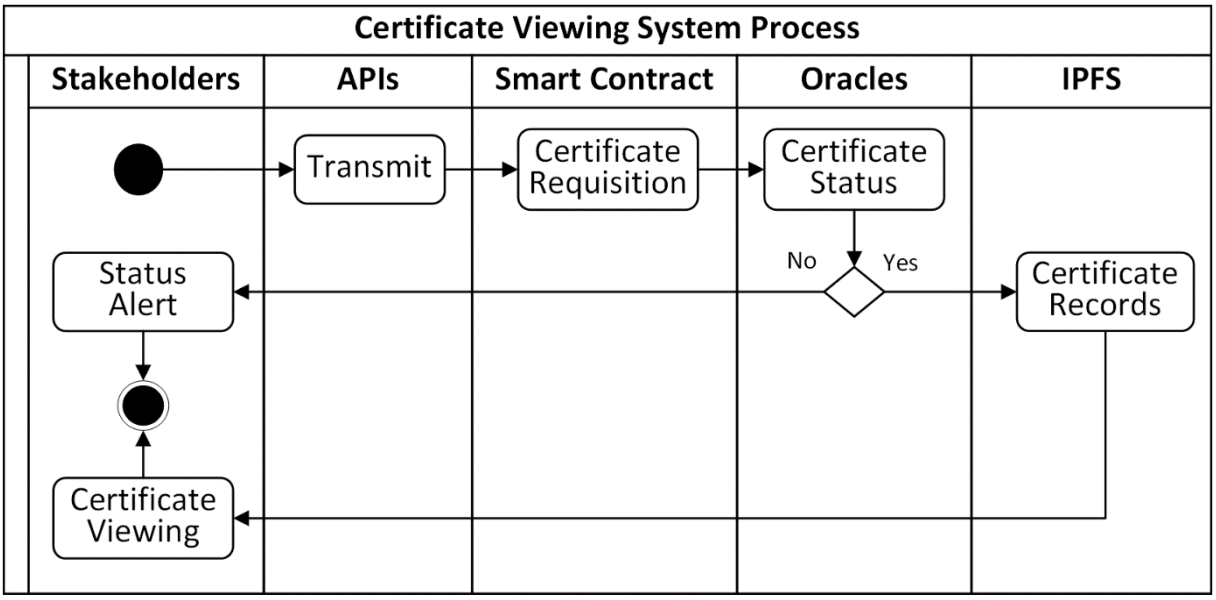

Fig. 4. Implementation of the academic certificate system architecture in the certificate viewing process. It has InterPlanetary File System (IPFS) and Application Programming Interfaces (APIs).

E. Interpretation of Results

Regarding system architecture flexibility, the proposed system architecture provides a comprehensive overview of the key components that facilitate Layer 2 optimization. While the research focuses on the educational domain, architecture possesses inherent adaptability and can be readily applied to other domains by simply modifying DApps according to the desired domain. The core system components remain unchanged, ensuring efficient implementation across diverse contexts.

Then, Web3 infrastructure components are strategically positioned externally to the blockchain to facilitate future expansion and mitigate transaction congestion on the main chain. This strategic design facilitates

fast transaction processing and minimizes gas costs. However, selecting the most suitable service provider for each Web3 infrastructure component, including DIDs, Oracle, and IPFS, is crucial for optimal system performance. With the current market offering a diverse range of service providers, conducting thorough research and comparing features are essential to identify the best fit for the specific needs of the system implemented.

In Ethereum Layer 2, the selection of Arbitrum as a component of the system architecture in the research reflects a design decision based on available solutions within the current market landscape (2025). However, the technological landscape is constantly evolving, potentially leading to the emergence of newer and more efficient solutions or even advancements within Arbitrum itself. While the system architecture remains adaptable to accommodate the integration of new solutions, its fundamental design principles remain unchanged.

F. Limitations and Strengths

While Oracle has the potential to enhance smart contract efficiency [62], a critical gap exists in the Oracle landscape, with a dearth of providers specifically catering to the education sector. Currently, Oracle solutions primarily serve business domains such as decentralized finance, supply chain management, and healthcare. Consequently, the development of a dedicated educational oracle provider emerges as a crucial requirement for fully realizing smart contract applications within the educational context. Moreover, oracles have reliability issues due to their centralized nature and reliance on potentially uncertain data [63].

The design of the system architecture incorporates Cosmos IBC to facilitate interfacing between different blockchains. As blockchain applications gain increasing traction within the education sector, the potential emergence of multiple blockchains developed by different institutions becomes a distinct possibility. In such scenarios, interfacing between these diverse blockchains becomes crucial, particularly when students transfer between institutions and seek to transfer previously earned credits. Cosmos IBC significantly simplifies and streamlines credit transfer compared to manual entry, which is not only time-consuming but also prone to errors. Cosmos IBC's interoperability with Layer 1 and Layer 2 environments allows developers to adapt code readily to accommodate new interfaces [64]. While Cosmos IBC represents a significant advancement in interoperability, it has limitations. Technical challenges, such as complexity, security vulnerabilities, and performance overhead impede its adoption [65], particularly among smaller development teams. Moreover, IBC's scope is constrained because it is incompatible with non-Cosmos blockchains, reliant on light clients, and restricted in data transfer capacity. Finally, its widespread implementation and efficacy are contingent upon network effects and the establishment of standardized protocols.

DIDs constitute vital components of the Web3 infrastructure. Despite their significant potential to enhance system functionality, DIDs remain underinvestigated within blockchain application research across diverse domains, especially in education. DIDs are more secure than traditional authentication methods because they offer user ownership and control, stronger cryptography, data minimization, improved privacy, and interoperability [66]. It means users can control their identity data, use strong cryptographic methods to protect their identity, share only the information required for a specific transaction, control how much personal information they reveal online, and use their DIDs across different platforms and services [67] Integrating DIDs into the system architecture in the research serves as a timely reminder of their critical role in enhancing system performance and functionality.

IV. Conclusion

The research proposes the academic certificate system architecture leveraging the Ethereum Layer 2 solution. This architecture is a blueprint for developing DApps that seamlessly integrate Web3 infrastructure. Addressing the scalability limitations of Ethereum Layer 1, which has largely remained unexplored by researchers within the educational domain, constitutes the primary objective of this system architecture.

In the research, the researcher employs a comprehensive literature review methodology to meticulously investigate blockchain applications across diverse domains. The researcher aims to identify elements of Web3 infrastructure that possess the potential to enhance system efficiency. Subsequently, the researcher conducts a rigorous evaluation of various Layer 2 solutions based on predefined criteria, ultimately culminating in selecting Arbitrum as the optimal solution. Armed with the chosen Web3 infrastructure components and the Arbitrum solution, the researcher then proceeds to design the architecture of the academic certificate system. After selecting the optimal Web3 infrastructure and Ethereum Layer 2 solutions, the researcher commences with the system architecture design process. The design accounts for the interconnections between the blockchain's Layer 1, Layer 2, and off-chain components. Additionally, the researcher implements cross-network communication between different blockchain networks using

the IBC Cosmos solution. Last, to facilitate a deeper understanding of the proposed system architecture, the research incorporates an illustrative example of its implementation within system processes. The example utilizes activity diagrams to depict two key processes: certificate issuance and certificate viewing.

While Oracle technology can enhance smart contract performance in architecture, a lack of education-focused providers limits its application. Most solutions serve business sectors, highlighting the need for a specialized educational oracle. Additionally, oracles face reliability challenges due to centralization and uncertain data sources. Then, although the Cosmos IBC integrated into architecture supports adaptability across Layer 1 and Layer 2 networks, its practical implementation is constrained by challenges such as complexity, security vulnerabilities, and limited compatibility with non-Cosmos blockchains. The effectiveness of IBC is contingent upon network adoption and the establishment of standardized protocols. The final limitation of the architecture is the DID, a key component of the Web3 infrastructure. Although DID has significant potential to enhance system performance, it remains insufficiently explored in blockchain research, particularly in education.

Based on the system architecture proposed in the research, several avenues for future exploration emerge. First, expanding the APIs for interfacing with external stakeholders to encompass the online labor market, particularly social media platforms such as Facebook and LinkedIn, warrants further investigation. Second, the design of a specialized oracle architecture tailored to the unique attributes and formats of the education sector constitutes a promising area for future research.

Acknowledgement

A grant from Southeast Bangkok University in 2023–2024 supported the research. The author is indebted to the Faculty of Digital Technology and Innovation at Southeast Bangkok University for providing a grant to assist with the research.

Author Contribution

Conceived and designed the analysis; Collected the data; Contributed data or analysis tools; Performed the analysis; and Wrote the paper, S. W.

Data Availability

The author confirms that the data supporting the findings of the research are available within the references.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," 2014. [Online]. Available: https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf

[3] A. F. Aysan, G. Gozgor, and Z. Nanaeva, "Technological perspectives of Metaverse for financial service providers," *Technological Forecasting and Social Change*, vol. 202, pp. 1–13, 2024.

[4] A. Ferreira and P. Sandner, "EU search for regulatory answers to crypto assets and their place in the financial markets' infrastructure," *Computer Law & Security Review*, vol. 43, pp. 1–15, 2021.

[5] J. Ronis, "Understanding Ethereum's Layer 1 and Layer 2: Differences, adoption, and drawbacks," 2023. [Online]. Available: https://shorturl.at/ycfw1

[6] M. B. Saif, S. Migliorini, and F. Spoto, "A survey on data availability in Layer 2 Blockchain rollups: Open challenges and future improvements," *Future Internet*, vol. 16, no. 9, pp. 1–17, 2024.

[7] N. Nizamuddin, K. Salah, M. A. Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using Ethereum blockchain and IPFS," *Computers & Electrical Engineering*, vol. 76, pp. 183–197, 2019.

[8] A. A. Battah, M. M. Madine, H. Alzaabi, I. Yaqoob, K. Salah, and R. Jayaraman, "Blockchain-based multi-party authorization for accessing IPFS encrypted data," *IEEE Access*, vol. 8, pp. 196 813–196 825, 2020.

[9] H. Niavis, N. Papadis, V. Reddy, H. Rao, and L. Tassiulas, "A blockchain-based decentralized data sharing infrastructure for off-grid networking," in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. Toronto, Canada: IEEE, May 2–6, 2020, pp. 1–5.

[10] C. Farmer, S. Pick, and A. Hill, "Decentralized identifiers for peer-to-peer service discovery," in *2021 IFIP Networking Conference (IFIP Networking)*. Espoo and Helsinki, Finland: IEEE, June 21–24, 2021, pp. 1–6.

[11] N. Fotiou, V. A. Siris, and G. C. Polyzos, "Enabling self-verifiable mutable content items in IPFS using decentralized identifiers," in *2021 IFIP Networking Conference (IFIP Networking)*.

Espoo and Helsinki, Finland: IEEE, June 21–24, 2021, pp. 1–6.

[12] T. Rathee and P. Singh, "A secure identity and access management system for decentralising user data using blockchain," *International Journal of Computational Vision and Robotics*, vol. 12, no. 4, pp. 343–359, 2022.

[13] M. Madine, K. Salah, R. Jayaraman, A. Battah, H. Hasan, and I. Yaqoob, "Blockchain and NFTs for time-bound access and monetization of private data," *IEEE Access*, vol. 10, pp. 94 186–94 202, 2022.

[14] L. Zhang, H. Kan, Y. Li, and J. Huang, "Poster: Blockchain-envisioned secure generic communication framework using Signcryption," in *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*. New York, United States: Association for Computing Machinery, June 8–10, 2022, pp. 251–253.

[15] K. Palanivel, "Blockchain architecture to higher education systems," *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS)*, vol. 8, no. 2, pp. 124–138, 2019.

[16] N. Priya, M. Ponnavaikko, and R. Aantonny, "An efficient system framework for managing identity in educational system based on blockchain technology," in *2020 International Conference on Emerging Trends in Information Technology and Engineering (IC-ETITE)*. Vellore, India: IEEE, Feb. 24–25, 2020, pp. 1–5.

[17] Y. Liu, K. Li, Z. Huang, B. Li, G. Wang, and W. Cai, "EduChain: A blockchain-based education data management system," in *Blockchain Technology and Application: Third CCF China Blockchain Conference, CBCC 2020*. Jinan, China: Springer, Dec. 18–20, 2021, pp. 66–81.

[18] F. Miah, S. Onalo, and E. Pfluegel, "Transforming higher education systems architectures through adoption of secure overlay blockchain technologies," in *Cybersecurity, Privacy and Freedom Protection in the Connected World: Proceedings of the 13th International Conference on Global Security, Safety and Sustainability*. London: Springer, 2021, pp. 343–355.

[19] Z. Z. Li, J. K. Liu, J. Yu, D. Gasevic, and W. Yang, "CVallet: A blockchain-oriented application development for education and recruitment," in *International Conference on Network and System Security*. Denarau Island, Fiji: Springer, Dec. 9–12, 2022, pp. 580–597.

[20] M. M. Madine, A. A. Battah, I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, S. Pesic, and S. Ellahham, "Blockchain for giving patients control over their medical records," *IEEE Access*, vol. 8, pp. 193 102–193 115, 2020.

[21] Y. Wang, A. Zhang, P. Zhang, Y. Qu, and S. Yu, "Security-aware and privacy-preserving personal health record sharing using consortium blockchain," *IEEE Internet of Things Journal*, vol. 9, no. 14, pp. 12 014–12 028, 2021.

[22] M. Tcholakian, K. Gorna, M. Laurent, H. Kafel Ben Ayed, and M. Naghmouchi, "Self-sovereign identity for consented andcontent-based access to medical records using blockchain," *Security and Communication Networks*, vol. 2023, 2023.

[23] S. Krejci, M. Sigwart, and S. Schulte, "Blockchain-and IPFS-based data distribution for the Internet of Things," in *Service-Oriented and Cloud Computing: 8th IFIP WG 2.14 European Conference, ESOCC 2020*. Heraklion, Greece: Springer, Sep. 28–30, 2020, pp. 177–191.

[24] H. Zareen, S. Awan, M. B. E. Sajid, S. M. Baig, M. Faisal, and N. Javaid, "Blockchain and IPFS based service model for the Internet of Things," in *Complex, Intelligent and Software Intensive Systems: Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2021)*. Asan, Korea: Springer, July 1–3, 2021, pp. 259–270.

[25] A. Dixit, M. Smith-Creasey, and M. Rajarajan, "A decentralized IIoT identity framework based on self-sovereign identity using blockchain," in *2022 IEEE 47th Conference on Local Computer Networks (LCN)*. Edmonton, Canada: IEEE, Sep. 26–29, 2022, pp. 335–338.

[26] L. Gigli, I. Zyrianoff, F. Montori, C. Aguzzi, L. Roffia, and M. Di Felice, "A decentralized oracle architecture for a blockchain-based IoT global market," *IEEE Communications Magazine*, vol. 61, no. 8, pp. 86–92, 2023.

[27] Binance Square, "Top 8 best Layer 2 blockchain tokens to invest in 2023," 2023. [Online]. Available: https://www.binance.com/en/square/post/1147461

[28] G. Hristov and S. Ullman, "5 Best Ethereum (ETH) Layer 2 (L2) solutions," 2023. [Online]. Available: https://milkroad.com/layer-2/

[29] E. Shin, "Best Layer 2 Crypto networks in 2025," 2025. [Online]. Available: https://www.datawallet.com/crypto/best-layer-2-cryptos

[30] N. Valshonok, "Best Layer-2 Crypto projects for 2025: The top picks," 2023. [Online]. Available: https://beincrypto.com/learn/layer-2-crypto-projects/

[31] C. Caringal, "Top 15 Layer 2 (L2)

Crypto list to consider in 2023," 2023. [Online]. Available: https://helalabs.com/blog/top-15-layer-2-l2-crypto-list-to-consider-in-2023/

[32] R. Nambiampurath, "The 5 best Ethereum Layer 2 solutions," 2022. [Online]. Available: https://www.makeuseof.com/best-ethereum-layer-2-solutions/

[33] D. Weidner, "Top 5 Ethereum Layer 2 projects for lucrative investments in 2024," 2024. [Online]. Available: https://cryptoticker.io/en/top-5-ethereum-layer-2/

[34] P. Jovanovic, "Best Layer 2 chains: A comprehensive guide to Ethereum's top 11 layer 2 projects," 2025. [Online]. Available: https://captainaltcoin.com/best-layer-2-chains/#google_vignette

[35] A. Robertson, "What are the best Ethereum Layer 2 solutions?" 2022. [Online]. Available: https://www.cryptoknowmics.com/news/best-ethereum-layer-2-solutions

[36] Victor, "The best 6 Ethereum Layer 2 solutions," 2021. [Online]. Available: https://www.altcoinbuzz.io/reviews/altcoin-projects/the-best-6-ethereum-layer-2-solutions/

[37] B. Chaseling, "Arbitrum (ARB) deep dive: Infrastructure, ARB ecosystem and competitors," 2023. [Online]. Available: https://zerocap.com/insights/research-lab/arbitrum-arb-deep-dive/

[38] Y. Yi, "The investigation of Layer 2 blockchain technologies for decentralized applications," in *Proceedings of the 1st International Conference on Data Science and Engineering (ICDSE 2024)*. SCITEPRESS – Science and Technology Publications, Lda., 2024, pp. 326–333.

[39] H. Song, Z. Qu, and Y. Wei, "Advancing blockchain scalability: An introduction to Layer 1 and Layer 2 solutions," in *2024 IEEE 2nd International Conference on Sensors, Electronics and Computer Engineering (ICSECE)*. Jinzhou, China: IEEE, Aug. 29–31, 2024, pp. 71–76.

[40] A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, and K. K. R. Choo, "Sidechain technologies in blockchain networks: An examination and state-of-the-art review," *Journal of Network and Computer Applications*, vol. 149, 2020.

[41] S. R. Heinrich and A. Antonovici, "Arbitrum (ARB) vs Optimism (OP) vs Polygon (MATIC): Which is best?" 2024. [Online]. Available: https://www.tastycrypto.com/blog/layer-2-networks/

[42] J. P. Njui, "Comparing Ethereum's Layer-2 solutions: Polygon vs. Arbitrum vs. Optimism," 2022. [Online]. Available: https://shorturl.at/cSUuH

[43] K. Nabben, "Web3 as 'self-infrastructuring': The challenge is how," *Big Data & Society*, vol. 10, no. 1, pp. 1–6, 2023.

[44] R. Huang, J. Chen, Y. Wang, T. Bi, L. Nie, and Z. Zheng, "An overview of Web3 technology: Infrastructure, applications, and popularity," *Blockchain: Research and Applications*, vol. 5, no. 1, pp. 1–10, 2024.

[45] C. Guan, D. Ding, J. Guo, and Y. Teng, "An ecosystem approach to web3. 0: a systematic review and research agenda," *Journal of Electronic Business & Digital Economics*, vol. 2, no. 1, pp. 139–156, 2023.

[46] Y. Cai, N. Irtija, E. E. Tsiropoulou, and A. Veneris, "Truthful decentralized blockchain oracles," *International Journal of Network Management*, vol. 32, no. 2, pp. 1–20, 2022.

[47] V. Chaurasia and M. Kamber, "Unleashing blockchain magic: A comparative journey through developer ecosystems and tools in ethereum polygon and polkadot," *Dogo Rangsang Research Journal*, vol. 13, no. 6, pp. 34–39, 2023.

[48] B. R. Cherukuri, "Building scalable web applications: Best practices for backend architecture," *International Journal of Science and Research (IJSR)*, vol. 13, no. 10, pp. 126–139, 2024.

[49] M. I. Khalid, I. Ehsan, A. K. Al-Ani, J. Iqbal, S. Hussain, S. S. Ullah *et al.*, "A comprehensive survey on blockchain-based decentralized storage networks," *IEEE Access*, vol. 11, pp. 10 995–11 015, 2023.

[50] S. Kumar, A. K. Bharti, and R. Amin, "Decentralized secure storage of medical records using blockchain and IPFS: A comparative analysis with future directions," *Security and Privacy*, vol. 4, no. 5, 2021.

[51] L. He, "A comparative examination of network and contract-based blockchain storage solutions for decentralized applications," in *Proceedings of the 3rd International Conference on Digital Economy and Computer Application (DECA 2023)*. IEEE, 2023, pp. 133–145.

[52] I. Giacomelli, "Filecoin: From proof-of-space blockchain to decentralized storage," in *CryptOrino 2021*, 2024, pp. 27–31.

[53] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, "Decentralized identity: Where did it come from and where is it going?" *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 10–13, 2019.

[54] A. Lohachab, S. Garg, B. Kang, M. B. Amin, J. Lee, S. Chen, and X. Xu, "Towards inter-

connected blockchains: A comprehensive review of the role of interoperability among disparate blockchains," *ACM Computing Surveys (CSUR)*, vol. 54, no. 7, pp. 1–39, 2021.

[55] M. Sober, G. Scaffino, and S. Schulte, "Cross-blockchain communication using oracles with an off-chain aggregation mechanism based on zk-SNARKs," *Distributed Ledger Technologies: Research and Practice*, vol. 3, no. 4, pp. 1–24, 2024.

[56] S. Wan, H. Lin, W. Gan, J. Chen, and P. S. Yu, "Web3: The next Internet revolution," *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34 811–34 825, 2024.

[57] X. Tang and L. Shi, "Security analysis of smart contract migration from Ethereum to Arbitrum," *Blockchains*, vol. 2, no. 4, pp. 424–444, 2024.

[58] O. Patel, "Blockchain Layer 2 Rollups, Optimistic vs Zero Knowledge," *International Journal of Advanced Research in Engineering and Technology (IJARET)*, vol. 14, no. 2, pp. 13–29, 2023.

[59] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng, and W. Han, "An overview on cross-chain: Mechanism, platforms, challenges and advances," *Computer Networks*, vol. 218, pp. 1–21, 2022.

[60] A. Amjad, F. Azam, M. W. Anwar, and W. H. Butt, "A systematic review on the data interoperability of application layer protocols in industrial IoT," *IEEE Access*, vol. 9, pp. 96 528–96 545, 2021.

[61] A. Gangwal, H. R. Gangavalli, and A. Thirupathi, "A survey of Layer-two blockchain protocols," *Journal of Network and Computer Applications*, vol. 209, 2023.

[62] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, "Trustworthy blockchain oracles: Review, comparison, and open research challenges," *IEEE Access*, vol. 8, pp. 85 675–85 685, 2020.

[63] G. Caldarelli, "Understanding the blockchain oracle problem: A call for action," *Information*, vol. 11, no. 11, pp. 1–19, 2020.

[64] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[65] M. S. Peelam, B. K. Chaurasia, A. K. Sharma, V. Chamola, and B. Sikdar, "Unlocking the potential of interconnected blockchains: A comprehensive study of cosmos blockchain interoperability," *IEEE Access*, vol. 12, pp. 171 753–171 776, 2024.

[66] Y. Kortesniemi, D. Lagutin, T. Elo, and N. Fotiou, "Improving the privacy of IoT with Decentralised Identifiers (DIDs)," *Journal of Computer Networks and Communications*, vol. 2019, pp. 1–10, 2019.

[67] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "DNS-IdM: A blockchain identity management system to secure personal data sharing in a network," *Applied Sciences*, vol. 9, no. 15, pp. 1–19, 2019.