IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 30 April 2024, accepted 20 May 2024, date of publication 24 May 2024, date of current version 3 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3405409

METHODS

Leveraging Blockchain to Enhance Digital Transformation in Small and Medium Enterprises: Challenges and a Proposed Framework

HOAI-NAM NGUYEN[1,2], HOANG-ANH PHAM[1,2], (Member, IEEE), NGUYEN HUYNH-TUONG[3], AND DUC-HIEP NGUYEN[4]

[1]Faculty of Computer Science and Enginering, Ho Chi Minh City University of Technology (HCMUT), Ho Chi Minh City 72506, Vietnam
[2]Vietnam National University Ho Chi Minh City (VNU-HCM), Ho Chi Minh City 71308, Vietnam
[3]Faculty of Information Technology, Industrial University of Ho Chi Minh City (IUH), Ho Chi Minh City 71408, Vietnam
[4]Vietnam Blockchain Corporation (VBC), Ho Chi Minh City 72600, Vietnam

Corresponding author: Hoang-Anh Pham (anhpham@hcmut.edu.vn)

This study is funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number DS2022-20-07.

ABSTRACT This paper presents a Blockchain-based framework for providing Blockchain services for purposes of stability in terms of consensus protocol infrastructure and governance mechanisms and accessible auxiliary services suitable for the vast majority of current business needs, including fundamental factors such as digital identity with autonomous identity, building solutions to ensure transaction privacy with zero-knowledge proofs, and other services related to digital assets. The proposed framework helps promote digital transformation for businesses, especially small and medium enterprises with limited resources and costs, to apply Blockchain technology to their business models, increasing competitive advantages and assisting the companies in focusing on business logic while still using Blockchain technology in their functions.

INDEX TERMS Blockchain-as-a-services, enterprise blockchain, digital transformation, self sovereign identity, zero-knowledge proofs, digital assets.

I. INTRODUCTION

Modern businesses, especially small and medium enterprises (SMEs), seek solutions to increase their competitiveness in the global market through the digital transformation and digitization of business processes [1], [2]. In addition, many countries apply various policies to encourage businesses to apply leading technologies to their businesses for economic and social development [3]. Innovation through technology allows enterprises to quickly adapt to new challenges and realities by supporting old business models and new ways of operating. Businesses can better understand market preferences by collecting and analyzing large amounts of customer data. Automating operations will make it easier to homogenize a company's behavior. Therefore, it is possible to scale, improve productivity, and limit errors and risks during lower human operation. Through technology, business operations are easily coordinated, service quality is enhanced, and market reach is globally expanded. This is why companies choose a digital transformation solution and tailor it to their unique operational needs. Blockchain is a potential technology that can be applied to many fields [4].

Blockchain promotes the value chain business model of enterprise groups. Businesses can leverage Blockchain to digitize and share data, interact with each other, and prevent fraud. Moreover, data security mechanisms and digital assets are strengths of this technology in digital transformation. Businesses can create new services based on digital transformation data and value chains, thereby expanding their revenue. Additionally, digital transformation activities based

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

on Blockchain technology have been developed in recent years to find ways to exploit it in different fields, such as supply chains, healthcare, government and public services, and agriculture [5], [6], [7], [8], [9], [10], [11], [12], [13]. Blockchain solutions have helped businesses transform processes in their operations to be more efficient, increasing trust in profile data and connecting those services back to the core digital transformation processes of the business. Blockchain can also create data consistency within an ecosystem of organizations and agents beyond the boundaries of a traditional centralized organization. Despite its potential, building a software solution that applies Blockchain remains a massive challenge for businesses, especially small- and medium-sized enterprises (SMEs). Owing to the complexity of Blockchain technology, it often requires excessive resources and expenses to build, maintain, and monitor the operation of a Blockchain system. Therefore, many providers have been born to provide Blockchain-as-a-Service (BaaS) tailored to different business needs. Popular Blockchain services are now operated by centralized corporations, such as Microsoft, Amazon, Oracle, and IBM.

BaaS is an effective solution that solves the various business needs of companies that want to adopt Blockchain technology without paying much attention to its technical details. BaaS embeds Blockchain into cloud computing systems and provides cloud infrastructure services. However, the aforementioned BaaS services still lack ancillary services, or their services are just a fundamental part of how other businesses access the Blockchain. Therefore, BaaS services should provide more details about common ancillary services for companies that need to use Blockchain in digital transformation in terms of digital identity and digital assets, which are the strengths of Blockchain technology. This paper presents a study focusing on the aspect of Blockchain services from consensus protocol infrastructure and governance mechanisms to maintain the stability of the Blockchain service platform and ancillary services regarding entity identification in the network and digital assets. Then, we present the design of a BaaS framework for enterprises to expand on ancillary services to be applied to different areas of life and market needs. The proposed framework aims to provide a stable and accessible platform for developing an effective enterprise Blockchain ecosystem that strengthens network governance policies, improves data security and privacy, and provides services related to identity and digital assets based on private Blockchain infrastructure. The main contributions of our study are summarized as follows:

- Investigate the impacts of Blockchain and issues of concern for small and medium enterprises when using this technology.
- Propose a Blockchain-as-a-Service (BaaS) framework that focuses on expanding several ancillary services to help accelerate the digital transformation process.

The remainder of this article is organized as follows. Section II summarizes the related works. Section III describes the proposed framework. Section IV presents the experimental results for the performance evaluation and discussion. Finally, conclusions are presented in Section V.

II. RELATED WORKS

A. THE IMPACT OF BLOCKCHAIN ON ECONOMICS

Blockchain has recently attracted growing interest from governments, businesses, and research communities, with applications in key industries such as agriculture [14], finance [15], insurance [16], education [17], logistics [18], energy [19], transportation [20], and other domains [21]. Blockchain is a promising general infrastructure technology that provides security, safety, and new services based on smart contracts that meet strict requirements for protecting data privacy in the Internet environment [22]. An increasing of companies, including large corporations such as IBM, Microsoft, Cisco, Intel, JP Morgan, and Toyota, are forming alliances and investing in the research and development of Blockchain and its applications,

Blockchain technology can potentially change current business models and thus has a transformative impact on industries, governments, and society [23]. Bitcoin was the first Blockchain-based payment application. Soon after, as the adoption of Blockchain-based electronic payment methods increased, the dynamics of international trade, foreign relations, and diplomacy changed significantly. However, its impact may not be limited to how monetary value is transferred on a global scale. For example, the World Economic Forum (September 2015) expected at least 10% of global GDP to be stored on Blockchain platforms by 2025. According to an analysis from PwC in 2020 [24], Blockchain technologies have the potential to increase the global economy by US$1.76 trillion by 2030 by enhancing levels of tracking, traceability, and confidence.

Blockchain is also a technology that paves the way for the creation of other services that enable peer-to-peer value transfer and increase levels of security and privacy for users, making platforms more efficient and independent. For example, value creators such as artists, composers, and designers can transfer work directly to customers or consumers. Blockchain allows tracking of the transfer of assets and ownership, thus protecting producers and consumers on digital platforms. Through Blockchain-based platforms, users not only consume services but also gain additional benefits from participating in maintaining and monitoring networks [25].

Privacy and security are central issues in Blockchain solutions [26]. Many Blockchain applications inevitably require linking transactions to known identities, thereby increasing data privacy requirements. As Blockchain applications deploy new decentralized value creation models, decentralized governance rules must be implemented to manage risk and create a compliance framework for participating parties.

B. STRATEGIC CAPABILITIES AND KEY VALUES OF ENTERPRISE BLOCKCHAINS

As seen in the maturation of Blockchain technology in recent years, although the technology is still young, many agree that Blockchain can impact economic, social, and political contexts as the Internet has. A survey based on more than 30 Blockchain application developers from many different industries, sectors, and types of businesses aims to determine Blockchain's true business value and how to build Blockchain-based business applications at various stages of development in many real business projects [27]. The above results show optimistic signs about the current state of enterprise Blockchains and the benefits of blockchain technology that help solve many problems.

Blockchain effectively addresses the lack of trust by providing the ability to trace the origins of transactions and digital assets and ensure the immutability of records. In addition, Blockchain has the potential to create a strategic alliance between two or more organizations to exchange and share resources or to co-develop products, services, or technologies, leading to an enhanced competitive position and operational efficiency [28]. In addition, Blockchain will help businesses in an alliance improve their value, specificity, and inimitability. For example, companies can enhance high-quality services and the value of their products by providing the ability to verify claims made to their products through Blockchain platforms, helping consumers understand the company's products via verifiable information. Blockchain also helps to automate the process via smart contracts to achieve cost efficiency and eliminate intermediaries.

In summary, businesses can approach Blockchain technology to build alliances that increase their competitive advantage in several ways.

- First, join Blockchain alliances, build relationships within alliances, and contribute existing capabilities.
- Second, share and build capabilities into shared resources, data, and risk management.
- Third, develop the ability to use smart contracts and build expertise in deploying Blockchain solutions.

The effective implementation of enterprise Blockchain solutions can facilitate the development of trust, collaboration, and risk sharing between companies or companies and their customers. As such, Blockchain technology allows a business to think beyond the barriers of a traditional centralized information technology system. No party can control or manipulate an entire network. Neither party can change its records after they are validated and recorded on a shared distributed ledger. Neither party can change or control the agreed-upon process through a smart contract. Therefore, an enterprise blockchain can help create a reliable network that overcomes the challenges of cultural, economic, and institutional differences between businesses. An enterprise Blockchain [29] can offer incredible value compared to a traditional centralized system, as follows:

- Replace three intermediaries with complex, secure encryption, and consensus algorithms that allow parties to transact directly with each other;
- Maintain a version of the truth without disputes, transactions in the Blockchain are fully validated before being added to the ledger;
- Provide an entire public, transparent transaction for all nodes that helps track and trace all transactions and instant status updates of the network;
- Allow traceability of existing assets;
- Execute smart contract logic automatically when pre-programmed conditions are met;
- Provide a fault-tolerant system with high availability.

These capabilities and values differentiate enterprise Blockchain technology from other technologies or software systems. However, for a business to achieve high efficiency, these values depend on the level of expertise, internal management ability, software features, and ''plug-and-play'' capabilities of enterprise Blockchain solutions.

C. WHY ENTERPRISE BLOCKCHAIN MUST BE BASE ON PERMISSIONED BLOCKCHAIN

The following are reasons to clarify why an Enterprise Blockchain should be built on top of a Private Blockchain network rather than a Public Blockchain (see **Table 1**) [30].

- **Improve Data Privacy**: Businesses do not want their confidential information to be public because they may contain secrets that can give competitors an advantage. They want to limit access to the network to identify individuals, and data privacy needs to be guaranteed. A private Blockchain framework accommodates this by exposing only the content of individual transactions to a subset of the network [31].
- **Provide Better Scalability and Performance**: The main component that maintains the security of a Blockchain is its consensus protocol. Some public Blockchains maintain a consensus protocol with a high number of consensus nodes; expanding more nodes, in this case, increases security but limits network throughput, making the time it takes for a transaction to be completed longer. While private Blockchains use identity mechanisms, controlling user identities by accessing the network and through digital signatures to maintain trust, the risk of illegal transactions is still present in the network. Therefore, private Blockchains allow inferior security (fewer nodes) to obtain better scalability and performance [32].
- **Reduce and Eliminate the Possibility of Forks**: Private Blockchains can overcome fork limitations using proof-of-authority (PoA) consensus protocols. By reducing the probability of forks, transactions are validated faster [33], [34].
- **Easy to Make Updates**:General update agreements are easy to achieve in a private Blockchain installation, as participants can get to know each other better and discuss changes together. Permissions are sometimes

TABLE 1. Comparison of Public Blockchain and Private Blockchain [30].

Features	Public Blockchain	Private Blockchain
Access	Anyone	Selected Organizations
Participants	Permissionless & Anonymous	Permissioned & Known Identities
Security	Consensus machanism & PoW or PoS	Pre-approved participants & PoA consensus & Voting
Transaction Speed	Slow	Lighter and Faster
Fork Ability	Yes	No
Easy to Make Updates	No	Yes

granted to allow an organization to perform new software updates.

D. CHALLENGES OF ENTERPRISE BLOCKCHAIN

As clarified in the previous section, enterprise Blockchains are built on top of private Blockchains, which have overcome some limitations. However, some challenges still exist when applied to business problems, especially for SMEs with a limited resources. This section will cover some of these technical and non-technical challenges.

1) TECHNICAL PROFICIENCY REQUIRED

To develop Blockchain solutions for businesses, technical expertise in Blockchain technology is required for exploiting Blockchain networks. It will be more difficult for small companies because of the limited knowledge and number of personnel. Furthermore, using private Blockchain frameworks requires technical skills in configuring, programming, using, and operating Blockchain nodes [35].

2) COMPLIANCE WITH REGULATIONS

Blockchain is an emerging technology, and the legal frameworks surrounding it are still being perfected in many countries and regions worldwide. For example, a Blockchain data ledger will encounter several concerns surrounding regulations such as the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley Act of 2002 (SOX), Know Your Customer (KYC), and anti-money laundering (AML) rules. The lack of regulations, policies, and technical frameworks that generally apply to the development of this technology is also a major challenge. Therefore, an enterprise Blockchain platform and its ecosystem must comply with local laws and regulations [36].

3) DATA PRIVACY

Data privacy is an essential attribute of enterprise Blockchains, which means that the content of a transaction is only visible to a small group of authorized participants. The level of privacy is flexible and varied per protocol and according to the use case [37]. Ideally, there should be governance rules that require Blockchain users to respect privacy laws when uploading or controlling personal data on the Blockchain. For private blockchains, it is easy to apply rules, such as prohibiting users from uploading specific types of data to the Blockchain or limiting the access of specific groups of users.

4) SECURITY AND RISKS OF MALICIOUS ACTIONS FROM INSIDE

Typically, a Blockchain system has deal with a trade-off between privacy and security. As the number of nodes that confirm transactions decreases, data tampering becomes easier. However, the more participants receive, read, and validate transactions, the more difficult it becomes to mine the consensus protocol. This leads to a direct trade-off: the more secure the blockchain, the more nodes that verify transactions, and the less privacy it leads, which is in contrast to private blockchains. Some private Blockchain implementations can only verify transactions by using a subset of validators. While this ensures that the transaction content does not have to be verified by the rest of the network, it is highly private and can lead to centralization [38].

5) PERFORMANCE AND SCALABILITY

As above-mentioned, a private Blockchain works by a single group or organization, where multiple licensed entities participate in establishing a decentralized community, sharing the same interests in this system. Write's permissions are granted only to trusted entities. Read's permissions may be public or restricted to other participants. Private Blockchains can achieve higher performance than public blockchains. However, this depends on the consensus protocol used. In fact, adding more verifier nodes to the network can reduce performance. Currently, scalability remains a [35] challenge that different private Blockchains try to solve in various ways.

6) APPLY TO EXISTING BUSINESS MODELS

In reality, business processes can be large, rigid, and difficult to repair. This makes it difficult to adapt or digitally transform pre-existing business processes to adopt the Blockchain technology [39]. This is especially true for most larger, older businesses as individuals become accustomed to their traditional business processes. Changing an established business model to incorporate a new technology fundamentally requires a paradigm shift and digital transformation courage

from leaders and managers. Although this challenge applies to all new and disruptive technologies, it can severely hinder Blockchain adoption.

7) INTEROPERABILITY WITH OTHER SYSTEMS

Interoperability is an important factor that enables collaboration possible. Interoperability refers to the capacity of several systems or applications to share and utilize the exchanged information. Several Blockchain platforms allow the operation of a prominent enterprise blockchain network, such as Hyperledger Fabric, Hyperledger Besu, OpenEthereum, and EOS. These different frameworks, in turn, will perform different functions across various protocols. For example, some frameworks can expose Application Programming Interface (API) functionality on the Hypertext Transfer Protocol (HTTP). In contrast, others can communicate using a Remote Procedure Call (RPC) in a format specific to a certain programming language (e.g., JavaScript, C#, Python, etc). Another form of challenge in interoperability is communication and coordination between the various Blockchain networks and frameworks under study [40].

8) ECOSYSTEM GOVERNANCE

The governance of an enterprise Blockchain ecosystem is essential because it is a difficult task with many challenges. However, enterprise Blockchain has many positive impacts that promote the production and business activities of a business or an alliance to create more value. If users or developers are unhappy with how the network is governed, they can decide to leave the chain, develop themselves based on a fork, or terminate using the Blockchain platform [41]. In addition, governance affects the scalability of the number of transactions, the mechanism through the law of consensus, and the ability to expand the number of participants, which also poses challenges that a Blockchain platform must solve.

- How to decide the consensus protocol;
- How to decide which new features are added and which are not;
- How to determine if a new participant is allowed into the network;
- Who will oversee operations, server costs, and maintenance?

A well-governed Blockchain creates a highly resilient enterprise Blockchain ecosystem. This element is essential for the successful deployment of software solutions and applications and their adaptability and interoperability with each other. Because of the large scale of Blockchain projects, governance manages and coordinates the entire community towards the same goal. Businesses are increasingly interested in a blockchain that can govern well and achieve regulatory compliance to safely and efficiently deploy their applications. As many public blockchains now face many problems related to privacy and digital currencies, Blockchain governance requires even more special attention.

The assessment and analysis of challenges for enterprise blockchain have implications for selecting and implementing solutions based on this technology. Blockchain solutions must be relevant to business cases and provide a competitive advantage over other alternatives. The chosen balance between the desired elements of Blockchain for enterprise applications is both possible and necessary, resulting in different Blockchain solutions and services optimized for the needs and purposes of different organizations.

III. THE PROPOSED FRAMEWORK

Based on the investigation of related issues, such as the impact of Blockchain and the special values that Blockchain brings to the economy in general, and businesses in particular, we can see the necessity of this technology for life and the digital transformation revolution in businesses. Since then, BaaS platforms have been developed to provide Blockchain services, accelerating the process of building and converting business logic in the Blockchain network. However, it can be seen that current BaaS platforms, such as IBM, Microsoft, and AWS have quite monotonous support for all types of Blockchain needs. The proposed BaaS framework supports platforms and consensus protocols that fit the needs and budgets of businesses, particularly SMEs. Furthermore, we propose a solution and governance model for the participating parties and support scalable governance using smart contracts. In addition to supporting the platform infrastructure and governance capabilities, we offer ancillary services, such as services that improve individuals' data privacy and identity services that carry self-sovereign identity and other digital asset services to drive effective digital transformation for enterprises.

A. SELECTION OF BLOCKCHAIN PLATFORM AND CONSENSUS PROTOCOL

To date, there have been two most commonly used open-source Blockchain platforms for enterprise blockchain: Ethereum and Hyperledger Fabric. Ethereum and Hyperledger Fabric are both very flexible overall but in different aspects. Ethereum's powerful smart contract engine makes it a universal platform for literally all types of applications. Ethereum focuses on automated digital asset management; to do so, it supports smart contracts or assets, making it easy to create asset management programs. Ethereum can also be applied in distributed business environments. Thanks to EVM, custom business logic (i.e., smart contracts) can be used for new applications. However, Ethereum's public modus operandi and its complete transparency are at the cost of performance scalability and limited privacy.

Hyperledger Fabric solves the performance, scalability, and privacy issues with permissioned operations and fine-grained access control. Fabric enables privacy controls and limits access to the transaction ledger to out-of-channel actors, which is a competitive advantage of an enterprise Blockchain platform. Fabric also offers smart contracts for application development called Chaincode. Chaincode can be developed in many languages, such as NodeJS, Go, Java, and Typescript.

Ethereum previously used the PoW consensus and performed worse than Hyperledger Fabric using Raft. With PoW, transactions are propagated to all nodes in the network and processed during the creation of new blocks. Meanwhile, Raft performs transaction processing before committing its results to a new block and propagating it. Specifically, Hyperledger Fabric achieves a higher throughput and lower latency than Ethereum when the transaction volume varies up to 10,000 transactions [42]. Additionally, the differences between these two platforms in terms of transaction execution time and average latency become more significant as the number of transactions increases. Hyperledger Fabric's average throughput also changes much faster than that of Ethereum. However, Ethereum can simultaneously process more concurrent transactions using similar computational resources. Hyperledger Fabric's success rate decreases faster as the transaction sending rate increases compared to Ethereum [43].

Overall, Ethereum has a powerful smart contract engine that can design logic for any type of decentralized application. Fabric has mechanisms for controlling permissions, restricting access, and improving ledger data privacy. Furthermore, its custom module architecture features are quite nice. Developed in 2019, Hyperledger Besu is an Ethereum client that extends the Ethereum protocol, but adds functionality related to private transactions and privacy, such as Hyperledger Fabric (see **Table 2**). Therefore, Hyperledger Besu enables the deployment of both public and private Blockchain networks for businesses or joint ventures. Due to the extension of the Ethereum protocol, most of the core components and concepts in Hyperledger Besu's architecture will follow Ethereum while emphasizing technical innovations related to the following features:

- **Finality** guarantees that transactions cannot be altered, reversed, or canceled after their completion. The latency of the Blockchain network will affect this chain property. Finality is a metric used to quantify the duration required to provide reliable assurance that transactions executed on a Blockchain will not be reversed or modified. Hyperledger Besu can offer finality because it adopts the IBFT 2.0 (Proof of Authority) consensus protocol. In addition, several other consensus protocols can be customized, such as Ethash (Proof of Work), Clique (Proof of Authority), and QBFT (Proof of Authority).
- **Permissioning** in Hyperledger Besu increases network security by defining access rights at the Node Permissioning or Account Permissioning level. Assigning permissions can be performed locally on each node or by smart contracts on the network that license the nodes and their locations.
- **Privacy** is ensured because Hyperledger Besu's nodes maintain public world states for the Blockchain and private states for each Privacy Group. However, private states contain data that is not shared with the world state.

Blockchain networks can operate in different geographical environments and industry sectors with diverse businesses participating in the venture. All Blockchain use cases have a heterogeneous group of network members: entrepreneurs (business representatives, agencies, organizations), consumers, transaction customers, developers, investors, etc. This social diversity can lead to conflicts, pushing the network to be reputable, maintaining data integrity, and resisting malicious actors and behaviors. Blockchain must be transparent and provide attestations to clarify the parties' responsibilities through consensus rules. Besu supports four different consensus rules, divided into two main groups: Proof of Work (Ethash) and Proof of Authority (Clique, QBFT, IBFT 2.0). Where Ethash consensus rules are used to run an Ethereum node compatible with the Ethereum mainnet, we suggest focusing on PoA consensus rules that fit the context of private Blockchains for businesses.

In summary, the Hyperledger Besu platform was designed for multiple purposes. This is suitable for developing Blockchain platforms for businesses, including establishing a private network with private and consistent transactions via private contracts. Hyperledger Besu also supports robust smart contracts such as Ethereum to develop diverse business logic. Besides, Hyperledger Besu and the IBFT 2.0 consensus protocol are suitable for building more Blockchain services that target business needs.

B. SELECTION OF THE GOVERNANCE MODEL IN ENTERPRISE BLOCKCHAIN ECOSYSTEMS

The governance of a Blockchain ecosystem is essential because the governance factor will be decisive for the sustainability of Blockchain as it allows stakeholders to discuss and make decisions and policies that the Blockchain will develop. Effective governance will increase the likelihood of success and adaptation of Blockchain to specific sectors and markets. As Blockchain is a vast network, governance depends on the relevant community's management and coordination with common goals. Driven by concerns about the success of the enterprise Blockchain ecosystem, we designed a conceptual framework for Blockchain governance to establish a shared understanding of the topic of governance and to guide businesses, regulators, and users of the system.

Blockchain governance is different from governance by Blockchain [44], which refers to the use of Blockchain technology to manage and coordinate existing actions and behaviors more effectively. In this concept, technology itself plays a supporting role in improving the existing governance process. Meanwhile, Blockchain governance aims to develop, adapt, and maintain technology itself. In other words, Blockchain governance is how the Blockchain community and stakeholders come together, demonstrating a degree of centralization in decision-making power, providing incentive mechanisms, defining access, exercising accountability, and resolving conflicts that can be technical or non-technical. Blockchain governance creates processes,

TABLE 2. Comparison of Ethereum, Hyperledger Besu and Hyperledger Fabric [18].

Characteristics	Ethereum	Hyperledger Fabric	Hyperledger Besu
Governance	Ethereum developers	Linux Foundation	Linux Foundation
Ledger Type	Permissionless/Permissioned	Permissioned	Permissionless & Permissioned
Platform	Generic BC platform	Modular BC platform	Generic BC platform
Transactions per second	15 - 20 TPS	Approx 3500 TPS	350 – 400 TPS
Consensus Algorithm	Nakamoto based PoW/PoS	Pluggable PBFT/various	PoW, PoS, PoA
Forks	Yes	No	No
State	Account based model	Key-value database	Account based model
Confidentiality	No (Transparent)	Yes	Hybrid
Vulnerability of attacks	51%	grater than one-third faulty nodes	DoS, Brute-force
Tamper proof	Difficult	Easy	Difficult
Data Storage	Swarm	CouchDB, LevelDB	CouchDB, LevelDB
Currency/Token	Ether	FabToken System	Ether
Smart contract Type	ETH smart contracts	Chain-code in fabric	ETH smart contracts
Smart contract language	Solidity, Vyper, LLL	Python, Golang, Java	Solidity, Vyper, LLL
Tokenization support	Yes	No	Yes
Key management	No	Yes (through CA)	No
Scalability	Difficult	Easy	Easy
Suited for	B2C DApps	B2B DApps	B2C & B2B DApps

rules, and procedures to direct, control, and collaborate among other stakeholders in the network to ensure the sustainability and sustainable development of the Blockchain ecosystem.

In the context of our enterprise blockchain ecosystem, we define Blockchain governance as consisting of two main governance activities: internal and external. External governance pertains to the impact exerted by external stakeholders, such as the community, media, and public, on companies within the Blockchain network. Meanwhile, internal governance defines the technical and non-technical governance rules of self-governance.

In practice, internal governance strategies can be implemented by adopting voting decisions based on the smart contracts of the board participants. As for external governance, we encourage all parties to participate in building a sustainable ecosystem that reflects the value of Blockchain for life. Blockchain governance is also an efficient method of limiting risks and ensuring specific local compliance and policies.

Initially, we retained the right to initiate and control the evolution of the ecosystem as an enterprise Blockchain service provider. We then delegate the rights and support the participation of investors and potential partners involved in harnessing the value of the shared Blockchain network. This decision-making process by the internal board is called on-chain governance and will become a central part of the protocol. Promote various equal decisions, such as architecture upgrades, smart contract upgrades, service upgrades, integration of other protocols, funding, and fund management. This governance process is carried out through two layers: (1) discussion, collecting suggestions from the off-chain community, and (2) conducting on-chain smart contract voting for proposals from selected voters. Tokens in the smart contract represent voting rights based on these votes.

- How voting rights are determined;
- How many votes are needed for quorum;
- What choices and votes people have when voting;
- What kind of tokens should be used for voting;
- Time for voting and governance decisions;
- Roles of stakeholders (such as proponents, executors responsible for implementing decisions, and administrators of voting system's activities).

These aspects are modularized by other smart contracts that are interactively integrated with the governor. One or more of these proposals will be implemented by the governor's contract after a discussion and consultation with the off-chain community. Data on the proposal are encrypted and go through the governor's voting process afterward. This process consists of the following: (1) creating a proposal in the form of tokens, (2) when a proposal takes effect, the selected delegates vote, and (3) after the voting process is complete, a proposal will be passed if the number of votes in favor of qualified delegates is over 50%. The proposal was deemed successful and continued to be implemented soon thereafter. This is a way to pass internal management decisions that affect the development of the enterprise Blockchain ecosystem in the future.

C. SELF-SOVEREIGN IDENTITY SERVICE AND DATA PRIVACY IMPROVEMENT

1) HOW TO MANAGE IDENTITY BY BLOCKCHAIN

Identity management is an administrative process that creates and maintains user accounts for authentication and identity in online services. It is necessary to simplify the process of providing the required rights to users and ensure that legitimate users can access services. The life cycle of an identity management system (IDM), or Identity and Access Management (IAM), consists of four stages: *registration, authentication, issuance, and verification*. Enrollment and agents involved in this lifecycle are authentication, attribute, service, and identity providers. We have designed solutions around digital identity and its services to provide a better solution that ensures privacy, security, and anti-repudiation, as well as increases interoperability between entities in the enterprise Blockchain ecosystem.

Cryptography is an essential factor in ensuring a private and secure identity. In Blockchain, we know the transaction owner through the widely publicized key, and the ownership of the private key is known only by the owner. Private and public keys are also cryptography and are used to identify a natural person in the Blockchain environment as a whole. However, the validator's result only results in information about ownership through the identity key, without additional attribute information. The logic behind this is that the stored data are anonymous, not personal information. Therefore, a practical approach to building a digital identity on the Blockchain for natural persons who participate in the network and still maintain privacy, allowing accountability while preserving anonymity in the transaction, is to deploy smart contracts for identity and cryptographic techniques on its properties. These contracts are determined by the ownership and control of the subject's private key.

Identities are created and maintained through the logic of an identity contract, which interacts with mechanisms that authenticate the attribute information associated with the identity.

- First, the identity must be authenticated by an identity issuer (a trusted entity). Each identity comprises a decentralized digital identifier (DID) and its associated attributes. An entity declares an identity with verifiable credentials (VC) that are attested after verifying specific user identification attributes (e.g., phone number, email, government identification (ID), and biometrics). A DID is a unique anonymous identifier of a person, company, or object. Each DID is secured using a private key. Only the private key owner can prove that they own or control their identity [45]. Identity owners manage their DIDs and VCs stored in user-controlled off-chain storage. They can be presented to any trusted party as needed [46].
- After creating its DID and VC, the identity must be associated with one or several separate pseudonyms (Blockchain identity keys) for different service providers. This process is known as *concatenation*. Upon successful pairing, the identity/identity owner can present a verified valid identifier (in the form of a QR code) to prove their valid identity and use certain services. The service provider verifies identity by verifying the proof of control and ownership attestation associated with a DID, proof of identity (attributes), and owner's private key (pseudonym). Thus, identity owners can associate identities with authorized pseudonyms with third-party applications and service providers.

Decentralized storage is one of the core components of secure identity data management. In a Blockchain-based identity management framework, determining the form of storage and limiting the data required for decentralized storage are primary concerns. Because the stored data will be copied and transparent to all participating nodes, instead of storing copies of relevant data directly onto the Blockchain, the subject should maintain the pointer to the data origin. This reliable repository will always provide the latest information updates, which is also a premise for Blockchain to meet compliance with secure storage of personal data, such as GDPR [47], as the data stored on the Blockchain is technically immutable.

2) SELF-SOVEREIGN IDENTITY (SSI) MODEL

In the enterprise Blockchain ecosystem relying on SSI to manage the identities of entities (e.g., individuals, organizations, and applications), users who are subjects of identities [48], [49] have control and are assured of security and information privacy, as well as mitigating the risks of data leakage or identity theft [50].

SSI is a decentralized identity management model approach that allows entities to fully control their identities and information flows in their digital interactions without depending on any authority, eliminating a single point of failure. This creates interoperability of user identities across multiple locations, with user control and oversight over that digital identity, creating user autonomy. As such, SSI is a model that changes power from a centralized identity provider to the owner of that identity. Users then manage unique DID codes and grant access to third-party applications to use certain services. Furthermore, DID, VC, and related personal data need to be presented only when proof of identity is required. This starkly contrasts with the current identity management, which relies on several well-known centralized identity service providers, such as Facebook Connect and Google Sign-In, or users having to create their own digital identities at different service providers [51].

SSI allows users to make a request (registration) that may include personally identifiable information and the corroborating data given to them by other persons or entities. Through efficient smart contracts, Blockchain-based SSI can enhance rights control, access control, and on-chain proof-of-ownership authentication. Blockchain is an immutable identity registry allowing users to present their identities and claims others can verify with cryptographic certainty

when needed. However, an identity standing alone on the Blockchain will not make sense, nor will self-made claims by the subject without the endorsement of trusted authorities. Identities need to be strengthened with appropriate attestation claims or extensive attributes, which can be achieved through different services and applications by different service providers, whether on- or off-chain. SSI guarantees that users are independent of the service provider. However, for each service provider, users should register their public key to prove ownership of their identity to that service provider.

A typical SSI on the Blockchain consists of keys, a decentralized identifier (DID), a verifiable credential (VC), and information authentication methods (e.g., encryption, hashing, digital signature recovery, and zero-knowledge proof).

- Initially, each user must own a pair of identification keys on the Blockchain (private and public keys). When a DID is generated, it maps to Blockchain's public key to ensure ownership and control over the DID token and SSI identity.
- Each DID is a code that exists only on the Blockchain in Identity contracts. In addition, each DID is associated with a DDO (DID's Document) that specifies the public key, protocol for authentication, authentication credentials, and service endpoint information (authentication certificate issuer) [45]. Later, the relevant details in the DDO of a DID can be updated, and the evidence of this information change will be stored in the Blockchain for the authentication process. A DID will persist until the owner no longer wants to use this identity and revokes it.
- After receiving a user request or statement of attestation, the issuer creates and digitally signs an authentication certificate. The authentication certificate bears the issuer's mark and validity period, so the issuer can issue a revocation statement or mark it as expired later. Authentication is an essential part of verifying identity information. Verifiers can rely on the identity owner's evidence and the issuer's signature when performing identity verification.
- Authentication methods are used to determine the association of an identifier with an identity controlled by a private key or other data regarding the identity. The verifier then reuses the original authentication method to check the identity, its attributes or statements provided by the identity owner, and the validity of authentication attestations.

In many cases, users do not want to disclose data about themselves, which means data privacy protection (including transaction data); for this purpose, in addition to the fact that the user's data will mainly be stored off-chain and secured by one or more basic layers of security, such as symmetric encryption, asymmetric encryption in a storage situation, and sharing of decryption keys when sharing. Information about certain attributes, integrity, and authentication mechanisms will be implemented using data hashes and digital signatures. The essential signature confirms that the owner (private key) has signed a statement to generate authentic certificates. Privacy requirements in more complex cases, including privacy for on-chain transactions, for example, proving a statement made, "Alice is +18 years old!" (see Figure 1) using Zero-Knowledge Proof (ZKP) tool to ensure data privacy and provide the ability to validate the correctness of that statement on the Blockchain without initially disclosing the complete information.

We recommend that identity-tied transactions be made private by default. However, our design also allows service users to flexibly choose when making transactions. Affiliates in a transaction can choose to trade public identities, meaning that each party knows the attributes of the shared identity when executing the other party's transaction. This allows each person to control and track their disclosure and the information disclosed in return. Properties and identities will be publicly disclosed in a fully public transaction. In a semi-public transaction, the attributes are encrypted, the identities are public, or the attributes are public, but the identifying information is anonymous. The attributes are encrypted in a private transaction, and all identifying information is anonymized.

In summary, ZKP can effectively protect data privacy and transactions, which is the basis for SSI services to satisfy the GDPR compliance requirements outlined in the previous section. This technique is also crucial for the future scalability of the platform. Therefore, we covered the SSI model, its core components, and the role of the ZKP technique in the system. In the next section, we propose designing an identity-as-a-service system called the **SSID Service**.

3) THE PROPOSED SSID SERVICE

The proposed SSID serves participants in the platform's enterprise Blockchain ecosystem. In the service template, we package and wrap the corresponding child services as APIs to make the design pattern easy to integrate and distribute the development across participants. The SSID service design pattern architecture is divided into Service, Off-chain Data, and On-chain Data layers in a technical stack.

- **Service Layer** is divided into subservices: Registry Services, Certificate Management, Verification Services, Authorization Services, Recovery Services, and Extension Services. These services are wrapped in APIs and delivered to facilitate system development. Each participating partner in the system can integrate and authenticate another user's identity. It is also possible for each user to create a private key management wallet, register the SSID identity, and use it with integrated service providers in the ecosystem.
- **Off-chain Data Layer** is where people and businesses can store their own personal data and authentication certificates (on private storage or devices). They use encryption and hashing protocols and generate cryptographic signatures and ZKP proofs for attribute data, depending on the purpose of use in each specific

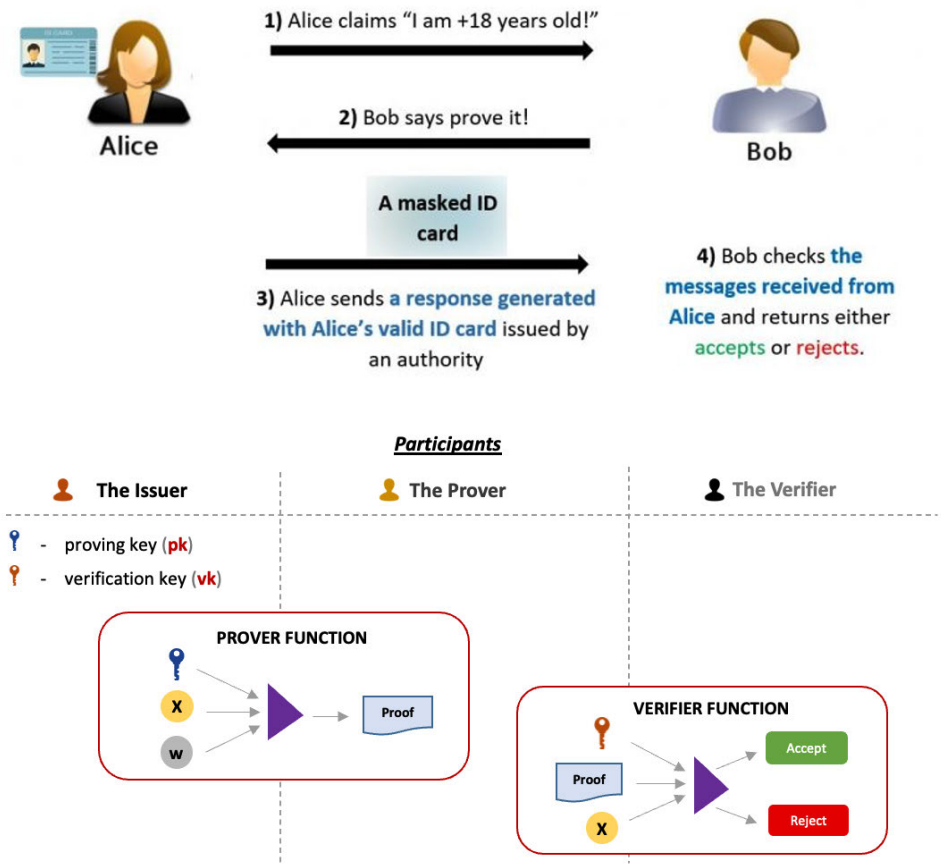

FIGURE 1. Zero-Knowledge Proof.

case. Each set of data attributes is created in a DDO document to be registered and associated with its own DID. They are stored in an off-chain distributed data repository integrated with each issuer or service provider.

- **On-chain Data Layer** is to store the owner's proof of the authenticity data. A user SSI is a smart contract on the Blockchain that registers a unique DID number and links it to the owner's key. The identity contract will also maintain the DID's mappings to DDOs stored off-chains.

When a service provider integrates the SSID platform, it can be the owner of their own identity for their organization; the issuer, who authenticates the identity of their users; or the verifier of the identity information provided by another owner (another third party may issue the identity). The role varies according to the context of each system's application, but there are three entities in a general system [52].

- **Issuers** provide verifiable claims (attestations) to people and other organizations.
- **Owners** possess digital identities and authentication certificates for their identities issued by issuers, storing them in vaults they trust or on their own devices. Besides, owners can exercise ownership and control, grant access permissions, and track access to other verifiers who interact with them.
- **Verifiers** require identity and authentication certificates from other owners and organizations to check the validity of the information provided, grant access to their protected resources and services, or accept transactions with them.

When creating an SSI system, each identity is independent of any one application, which creates a paradigm change and enhances the mobility and flexibility of the user identification process between applications and parties (e.g., education, logistics, health, and public services) interacting with each other in a common ecosystem. Figure 2 describes an overview of the proposed SSID model, which helps to realize the above description.

- **Registry Services.** Each user registers a DID using a Blockchain account via this service. An identity contract with a DID identifier is then generated in the Blockchain. It should be noted that the user's primary key is automatically registered to control ownership and access. The user can then register additional subkeys to use across different applications and recover the identity management key if the primary key is stolen. Each DID identifier can be associated with multiple subkeys

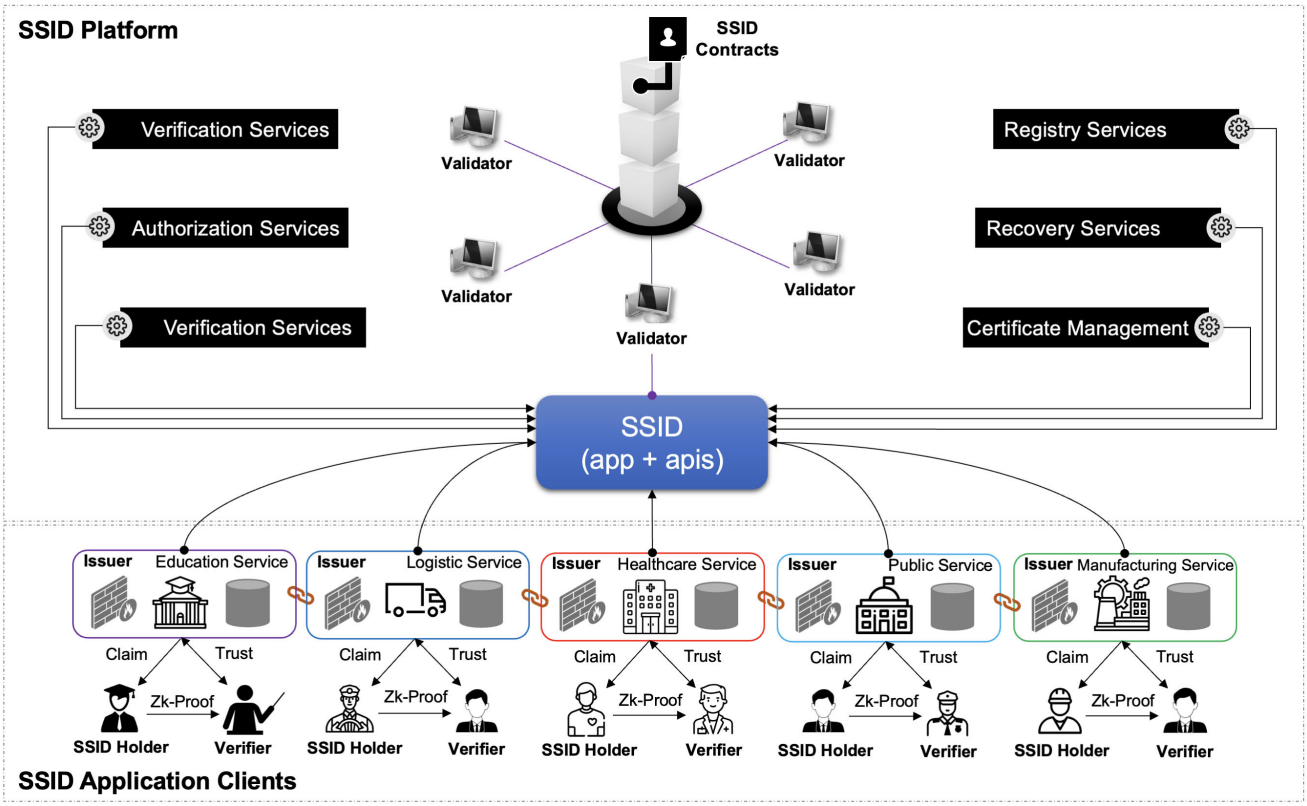

FIGURE 2. The proposed SSID Framework.

(aliases) for use across various apps, depending on the owner's intended use.

- **Certificate Management.** This service helps publishers allocate, manage, verify, and store their authentication certificates for publishers who issue and generate cryptographic signatures on each user authentication certificate. Users must register and query authentication certificates generated by issuers they trust through this service.
- **Verification Services.** They maintain the mapping of credentials and on-chain identity information to authenticate attestations stored off-chain. Through various authentication methods, they can check the integrity and correctness of the information provided and answer the verifier of the result based on the authentic question they want to know.
- **Authorization Services.** Owners must grant or revoke access to certain service providers while using their identities. They then use this service to perform transactions with the identity contract to adjust access restrictions.
- **Recovery Services.** Key recovery and data recovery are the primary concerns in our system design. An SSI system may encounter risks or problems during operation. The recovery service will help users, organizations, and businesses limit risks, such as key theft and issues with stored data.
- **Extension Services.** They include a group of support services during use related to cryptographic techniques, key sharing, information sharing, and transaction lookup and can extend other APIs to suit new needs.

The proposed SSID itself does not act as an issuer or an identity validator. It provides a GDPR-compliant infrastructure and services to meet the needs of participating businesses and improve the privacy and security of personal data, especially their identification data, in the digital environment.

D. BLOCKCHAIN-BASED DIGITAL ASSET SERVICE

The proposed platform will provide full-service support for tokens representing any asset; they can be digital or physical. A digital asset management system on Blockchain has outstanding features such as distributed storage (preventing loss of marks), high security, data privacy protection, strengthening trust, protecting real property rights, combining data fingerprinting, anti-tampering, and providing data traceability. With the rapid development of information technology and the continuous development of digital transformation processes for enterprises, content, data, and digital information of certain values accumulate during enterprises' production and management, forming many digital assets [53].

Effective management and use of digital assets by enterprises is an important measure for improving the efficiency

of digital transformation and automating production and business processes to bring economic benefits to enterprises. However, the traditional digital asset management model has a high level of data concentration, data security risks, high centralized data storage costs, inadequate efficiency of use and exploitation of digital asset value, copyright disputes, leakage of private information, data tampering, and single-point failure. Therefore, a strategy to build an enterprise digital asset management system based on Blockchain technology is an urgent solution that can overcome the above disadvantages.

Blockchain technology can ensure reliability, safety, and security, along with the ability to verify on-chain data through cryptographic algorithms and consensus mechanisms, thus minimizing the risks brought by the centralized management model. Digital asset management solutions using blockchain technology are applicable to various needs in various fields. Digital assets on Blockchain mean tokenizing related assets, such as physical (physical) assets, or digital assets, such as data, images, and sound, using Blockchain technology and issuing these types of assets as tokens. This tokenization uses smart contracts to promote processes that take place automatically and transparently, improve security, protect ownership, and exchange processes (buying, selling, and owning assets) that take place securely. These processes can use Fungible Tokens (FT), Non-Fungible Tokens (NFT), and Fractional Non-Fungible Tokens (F-NFT) [54], depending on the characteristics of the assets and the business model of the enterprise.

NFTs are a popular way of digitizing assets, helping to solve difficulties, and creating innovative business models. One of these everyday use cases is that many creators worldwide mint their artworks as NFTs (digital art). An artist creates a work of art and then establishes an NFT that represents that work and sells it to another individual [55]. Another idea is to register NFTs as trademarks, the benefit of which is the disclosure of trademark ownership in the decentralized database of the Blockchain, with the definite nature of NFT ownership. Afterward, it will be used to record legal trademark ownership with a government organization to protect ownership from infringements because the NFT specification only allows the actual owner to use his property. Thus, NFTs can become independent brand assets. Brands can leverage the flexible structure of NFTs to create ownership and engagement with the brand [56]. These business models have grown enormously over the past few years, especially as the world faces the COVID-19 pandemic, making purchasing and selling digital assets more popular and helping art creators find income in challenging circumstances.

Blockchain is an effective support technology for building and strengthening a brand's consumer trust. Trust between consumers and emotions is an essential factor that positively affects brand loyalty [57]. Loyalty programs are an important tool to improve brand loyalty by creating stronger economic relationships and habits [58], [59]. These programs are used in a wide range of industries, particularly in retail, airlines, travel, e-commerce, and finance, as the most critical and widespread marketing tool for brands looking to build customer loyalty and manage relationships [59], [60], [61], [62]. A Blockchain-based loyalty program system that tokenizes assets in tokens offers more benefits to both brands and consumers. Such a system would help consumers manage brands' reward points in a single wallet, and they could use or exchange tokens in multiple ways and across various platforms, crossing geographical boundaries. These are prominent cases in many other applications that utilize Blockchain to create and trade digital assets in many fields.

In our framework, we propose a digital asset service (DAS) to provide an asset-as-a-service that generates assets in the form of FT tokens, NFTs, and F-NFTs. Based on the fully decentralized infrastructure available, businesses can use DAS to operate their digital assets and control their identity and data. The proposed DAS allows enterprises to create and manage Blockchain assets without building and maintaining infrastructure related to token operations. It is a powerful and flexible suite of services for tokenizing assets, verifying ownership data, and tracing origin data.

In the design pattern of the proposed DAS, we package and wrap the corresponding sub-services as APIs to make the design pattern easy to integrate and distribute across different systems in the DAS ecosystem. As shown in Figure 3, the DAS design pattern architecture is divided into three layers on a technical stack.

- **Blockchain Service layer** includes distributed functions around interacting systems, including the FT/NFT/F-NFT Factory, ownership certificate management, asset management wallets, traceability inspections, and the digital asset marketplace. Companies of all sizes and industries can use the proposed DAS tools and services to create Blockchain products or use digital assets as part of their strategy. With the proposed DAS, enterprises and developers can quickly integrate some or all services with flexible APIs, such as token activation, event logging, enabling in-app asset transactions, linking asset management wallets, verifying on-chain certificate data, and peer-to-peer exchanges in decentralized markets.
- **Security and Privacy layer** allows using cryptographic techniques to protect data and ensure data privacy. Property and event data on assets often require privacy and security to protect against data copying, breach, or tampering. Similar to digital identity, the ZKP is implemented as a core component in this layer to protect data privacy and on-chain verification capabilities. In addition, other data hashing and encryption techniques have been used for various enterprise security goals.
- **Storage layer** provides various options for storing the described content of a given asset, including on-chain, centralized, decentralized, and physical storage. In most cases, the cost of storage directly on the Blockchain is high, coupled with the limited capacity and data

format in a transaction. Hence, tokens represent an asset stored in the Blockchain. This token contains a pointer (URI/URL) to the digital asset, descriptive data, and sometimes the data hash value itself.

Together with SSID, the service layer of DAS includes FT/NFT/F-NFT Factory, Ownership Certificate, Wallet, Traceability Inspections, and Marketplace services in a mutually integrated enterprise Blockchain ecosystem provide the tools and solutions for developers and enterprises to tokenize assets and incorporate them into software.

- **FT/NFT/F-NFT Factory** allows the creation of Blockchain tokens and token contracts based on appropriate smart contract standards supported by well-known standards such as ERC20, ERC721, and ERC1155 [54].
- **Ownership Certificate** creates and manages digital certificates that record the ownership of assets created through the platform. The development of this digital certificate system aims to complement and maintain the linkage between a token and a given asset. In addition, it seeks to limit partner enterprises' counterfeiting of registered assets. The digital ownership certificate system also provides authentication capability for auditability and accountability to ensure the reliability of assets on the Blockchain.
- **Wallet** primarily manages, stores, trades, and transfers token assets as an easy-to-use and secure e-wallet. This e-wallet also adds convenient features like tracing origin data and verifying relevant digital certificates to extend user experience and interoperability with other applications.
- **Traceability Inspections** are components of recording and retrieving origin data, such as reports and checks related to digital assets (e.g., NFTs) during their lifecycle. Reality shows that the traceability of products, goods in the supply chain, or other areas that require digitization of assets and historical records is essential. For each NFT asset, recording historical information from the moment it was created to the stories the NFT went through would help with the buying and selling processes and make the NFT more believable.
- **Marketplace** is a peer-to-peer marketplace for purchases, auctions, and reservations of digital assets. The marketplace helps attract investors and customers to own digital assets and encourages businesses and developers to build Blockchain assets. In addition, the marketplace allows buyers and sellers to trade and exchange Blockchain assets safely and quickly. Users can choose to conduct public or private transactions for their assets in the market.

The variety of research and solutions around token assets on Blockchain (especially for NFTs) is enormous. They have been developed extensively across sectors and overlap in terms of creative endeavors. To provide a deep and clear insight into the technology and components created in our systems, each of the following sections describes the orientation and creates a standard framework for the proposed DAS's asset digitization service solution.

1) DATA RETENTION

There are many asset data storage layouts that are allowed to choose such as:

- **On-chain Storage.** Descriptive metadata about the asset is stored directly in a smart contract on the Blockchain, implying that the data remains immutable. However, it must be noted that storing a large amount of data is expensive.
- **Centralized Storage.** Metadata is stored in addition to the smart contract, which is stored on the enterprise server, and the data pointer is maintained to make the connection.
- **Decentralized Storage.** Metadata is stored in a decentralized system, similar to on-chain storage but less expensive. The decentralized system distributes data across many nodes and is accessible via content-identification addresses. One of the typical systems for this is the InterPlanetary File System (IPFS), a globally distributed file system built on a peer-to-peer network. Files stored in IPFS are broken down into smaller, cryptographically hashed parts, each with a content identifier based on the contents of the stored file [63], [64], [65].
- **Physical Storage.** Metadata is the key's hash value that owns the physical asset (e.g., the radio frequency data hash value is used to unlock the car) and can be stored on a smart contract.

2) TOKEN STANDARDS

The token standards for FT, NFTS, and any other asset are ERC-20, ERC-721, and ERC-1155.

- **ERC-20** is a popular token standard used on the Ethereum platform to create fungible tokens. It includes a token rule describing buying, selling, or trading to which tokens are subject [54].
- **ERC-721** is the most commonly used standard for NFTs. This standard allows for the production of separate tokens with different values and represents different assets
- **ERC-1155** is a scalable token standard that represents fungible and non-fungible tokens. A single ERC1155 contract can generate an unlimited number of tokens. This standard's outstanding advantage is its ability to transfer multiple tokens in a single transaction, resulting in lower costs and shorter waiting times.

3) ASSET TYPE

NFTs can represent many different classes of assets. In our design, NFTs represent several asset classes defined by the following groups.

- **Marketplace** includes featured assets minted into NFTs, auctioned, and traded on the marketplace from multiple sources.

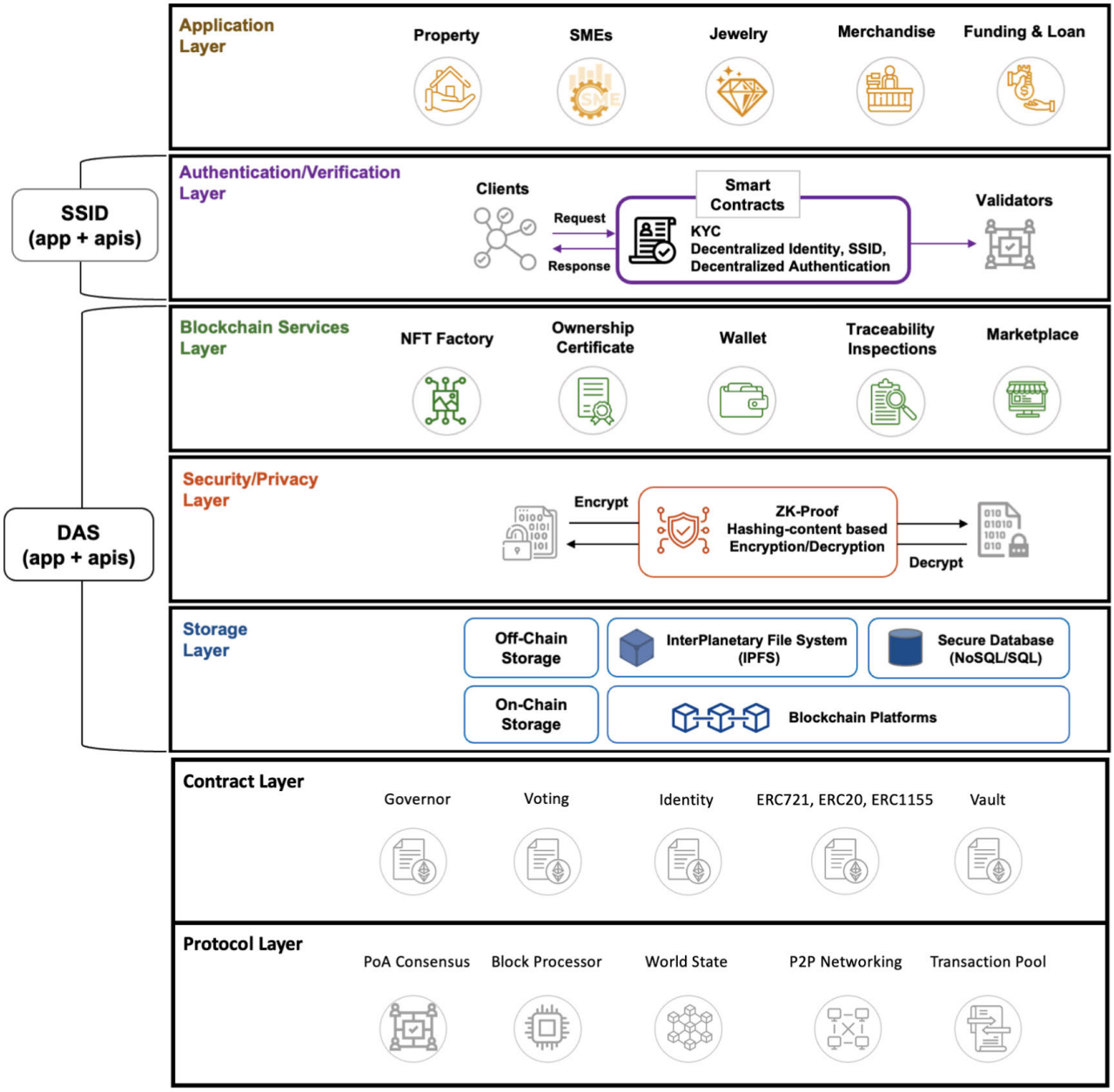

FIGURE 3. The architecture of the proposed framework.

- **Event** includes assets that represent the brand are of high value and limited quantity. These assets created on special occasions can be minted into NFTs and made available for reservation to promote the brand.
- **Magic bag** includes randomly appearing digital or physical assets minted into NFTs that match randomly occurring artistic creations or reward business models.
- **Limited** includes premium and exclusive assets that are created in limited quantities and distributed by listing them as NFTs on the Blockchain.
- **Fractionalized** includes high-value assets that can be minted into F-NFTs, and smaller segments that share ownership among multiple users.

4) SIZE PER NFT VERSION

Each NFT is unique through its smart contract ID and address when verified on a Blockchain. However, multiple versions of NFTs with the same content (metadata) can coexist if their mint is decided. Three instance sizes can be determined as follows:

- **Unique** means that an NFT represents a single item with only one existing copy of that item.
- **Collection** means that an NFT is part of an NFT collection in which multiple copies of the same nature and characteristics are created. This is similar to a set of identical tickets created with limited copies.

TABLE 3. Performance comparison between Blockchain platforms.

Characteristics	VBchain	Ethereum	Binance Smart Chain	Polygon
Gas Limit	30,000,000	30,000,000	140,000,000	30,000,000
Average Block Time (second)	2	10 - 14	3	2
Transactions per Second (TPS)	$\sim$ 68.3	$\sim$ 12.5	$\sim$ 40.9	$\sim$ 32.7

- **Open Version** means that these NFTs have no limit or a fixed number of reservations and have become popular recently, meaning that NFT copies can be created over time depending on market demand.

In summary, the proposed DAS provides services and tools for businesses and developers to digitize any asset (pictures, music, collectibles, real estate, jewelry, etc.) into tokens on the Blockchain and manage and exploit their potential and value. Owners of these assets gain new experiences of actual ownership and tap into the value chain from each asset's ownership and data.

IV. IMPLEMENTATION AND EVALUATION

A. IMPLEMENTATION

The proposed BaaS framework was implemented and deployed under the VBchain of Vietnam Blockchain Corporation (VBC), which has supported several digital transformation solutions in Vietnam. To date, more than eight million transactions have been processed in VBchain.[1] Depending on the usage needs, the above applications integrate services such as installing a private blockchain node or participating in VBchain's blockchain network, digital asset services, and self-sovereign identification services.

For example, Agridential[2] was the first solution to apply Blockchain technology for traceability and supply chain management in the agricultural sector in Vietnam. Currently, Agridential has helped many farmers and Vietnamese farms meet standards for the safety and origin of products to enhance the trust of domestic and foreign consumers and promote brand image in the eyes of consumers. More than eight million traceability stamps are available for over 800 activated products. Agridential has been developed in VBchain to utilize SSID, DAS, and traceability services.

B. EVALUATION

1) PERFORMANCE

When comparing the performance of the Blockchain network, we usually pay attention to the number of transactions that the network can process per second (TPS), calculated by the number of transactions in a block divided by the time it takes to process a block.

Figure 4 depicts the evaluation results performed using the Blockchain network performance measurement tool to simultaneously send a series of transactions to the network to test its processing performance. The horizontal column represents the number of transactions performed simultaneously in each turn, and the vertical column represents the number of transactions per second the node processes and creates blocks. It can be seen that our VBchain can reach the highest performance at 94 TPS and an average of 68.3 TPS.

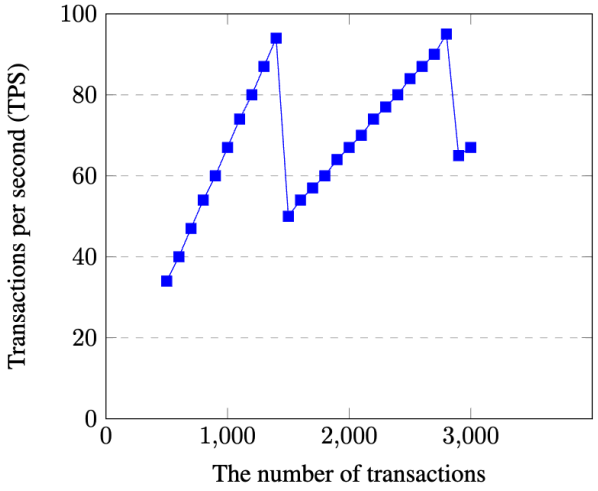

FIGURE 4. Evaluation results in term of transaction per second (TPS).

In addition, Table 3 summarizes the performance calculation results for the currently popular EVM-compatible Blockchain networks. The results show that VBchain's Blockchain network currently performs well compared to other platforms.

2) SECURITY ANALYSIS

While developing the proposed BaaS framework, security and privacy are always considered the solution's foundation. Regarding security in Blockchain network infrastructure design, the Hyperledger Besu protocol itself provides many important security mechanisms of a Blockchain network, such as a decentralized network, PoA consensus rule, and an anti-DDoS attack on a Blockchain node. In addition, the security design of the underlying component layers in the overall architecture of the proposed framework is divided into the following types:

- **Cryptographic security** includes authentication, encryption/decryption, and digital signatures.
- **Data storage security** uses data encryption techniques, access control, and decentralized data storage.

[1] https://vbchain.vn/en/home
[2] https://agridential.vn/

- **Zero-knowledge proof security** is guaranteed by DDoS attack protection, access control, and decentralized off-chain data storage.
- **Smart contracts' security** is developed based on widely recognized standards, such as OpenZeppelin, and they undergo auditing and bug fixing before being used.

V. CONCLUSION

Blockchain-as-a-Service framework for digital transformation solutions makes Blockchain and its underlying technology more accessible to businesses, especially SMEs with limited resources. The proposed framework was developed based on the Hyperledger Besu platform; therefore, installing and maintaining Blockchain nodes requires a cheaper system cost than public platforms such as Ethereum. Moreover, the enterprise Blockchain environment is high-performance and supports convenient tools for developers. The highlight of this development framework lies in its focus on the need to digitize the essential digital identities and assets of life sectors packaged as easy-to-use and customizable services based on needs. Besides, the proposed framework allows users to customize public or private transactions based on network infrastructure protocols and ZK-Proofs technology to improve personal data privacy.

In addition to the growing interest in Blockchain and its widespread adoption in various fields, many problems have been faced and solved to meet evolving needs. This study also contributes to the development trend of current BaaS systems and makes Blockchain a helpful technology in the digital transformation process of current and future businesses. The effective implementation of enterprise Blockchain solutions also facilitates the development of trust, cooperation, and risk-sharing between alliance members, creating a value chain.

ACKNOWLEDGMENT

The authors would like to acknowledge Ho Chi Minh City University of Technology (HCMUT), VNU-HCM supporting for this study.

REFERENCES

[1] P. Parviainen, M. Tihinen, J. Kääriäinen, and S. Teppola, "Tackling the digitalization challenge: How to benefit from digitalization in practice," *Int. J. Inf. Syst. Project Manage.*, vol. 5, no. 1, pp. 63–77, Feb. 2022.

[2] I. Antoniadis, S. Kontsas, and K. Spinthiropoulos, "Blockchain and brand loyalty programs: A short review of applications and challenges," *Proc. Econ. Bus. Administraion*, vol. 5, no. 1, pp. 8–16, Dec. 2019.

[3] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital transformation: An overview of the current state of the art of research," *SAGE Open*, vol. 11, no. 3, Jul. 2021, Art. no. 215824402110475.

[4] M. Friedlmaier, A. Tumasjan, and I. M. Welpe, "Disrupting industries with blockchain: The industry, venture capital funding, and regional distribution of blockchain ventures," in *Proc. 51st Hawaii Int. Conf. Syst. Sci.*, 2018, pp. 3517–3526.

[5] D. Agrawal, N. Jureczek, G. Gopalakrishnan, M. N. Guzman, M. McDonald, and H. Kim, "Loyalty points on the blockchain," *Bus. Manage. Stud.*, vol. 4, no. 3, p. 80, Aug. 2018.

[6] V. Varriale, A. Cammarano, F. Michelino, and M. Caputo, "New organizational changes with blockchain: A focus on the supply chain," *J. Organizational Change Manage.*, vol. 34, no. 2, pp. 420–438, Mar. 2021.

[7] R. W. Ahmad, H. Hasan, R. Jayaraman, K. Salah, and M. Omar, "Blockchain applications and architectures for port operations and logistics management," *Res. Transp. Bus. Manage.*, vol. 41, Dec. 2021, Art. no. 100620.

[8] J.-S. Lee, C.-J. Chew, J.-Y. Liu, Y.-C. Chen, and K.-Y. Tsai, "Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract," *J. Inf. Secur. Appl.*, vol. 65, Mar. 2022, Art. no. 103117.

[9] A. Tandon, A. Dhir, A. K. M. N. Islam, and M. Mäntymäki, "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda," *Comput. Ind.*, vol. 122, Nov. 2020, Art. no. 103290.

[10] C. Pauletto, "Blockchain in international e-government processes: Opportunities for recognition of foreign qualifications," *Res. Globalization*, vol. 3, Dec. 2021, Art. no. 100034.

[11] Á. F. Alcaide, C. Núñez-Gómez, F. M. Delicado, C. Carrión, and M. B. Caminero, "A blockchain-based e-Government service for quantity surveyors," *IT Prof.*, vol. 25, no. 4, pp. 61–66, Jul. 2023.

[12] O. Bermeo-Almeida, M. Cardenas-Rodriguez, T. Samaniego-Cobo, E. Ferruzola-Gómez, R. Cabezas-Cabezas, and W. Bazán-Vera, "Blockchain in agriculture: A systematic literature review," in *Proc. Int. Conf. Technol. Innov.* Cham, Switzerland: Springer, 2018, pp. 44–56.

[13] A. F. Aysan, B. Sadriu, and H. Topuz, "Blockchain futures in cryptocurrencies, trade and finance: A preliminary assessment," *Buletin Ekonomi Moneter dan Perbankan*, vol. 23, no. 4, pp. 525–542, Dec. 2020.

[14] J. Ordóñez, A. Alexopoulos, K. Koutras, A. Kalogeras, K. Stefanidis, and V. Martos, "Blockchain in agriculture: A PESTELS analysis," *IEEE Access*, vol. 11, pp. 73647–73679, 2023.

[15] L. Xue, "The application of blockchain technology in the financial field," in *Proc. Int. Conf. Forthcoming Netw. Sustainability AIoT Era (FoNeS-AIoT)*, Dec. 2021, pp. 130–134.

[16] A. Shetty, A. D. Shetty, R. Y. Pai, R. R. Rao, R. Bhandary, J. Shetty, S. Nayak, T. K. Dinesh, and K. J. Dsouza, "Block chain application in insurance services: A systematic review of the evidence," *SAGE Open*, vol. 12, no. 1, Jan. 2022, Art. no. 215824402210798.

[17] P. Ocheja, F. J. Agbo, S. S. Oyelere, B. Flanagan, and H. Ogata, "Blockchain in education: A systematic review and practical case studies," *IEEE Access*, vol. 10, pp. 99525–99540, 2022.

[18] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain technology for secure supply chain management: A comprehensive review," *IEEE Access*, vol. 10, pp. 85493–85517, 2022.

[19] M. Sivianes, J. M. Maestre, A. Zafra-Cabeza, and C. Bordons, "Blockchain for energy trading in energy communities using stochastic and distributed model predictive control," *IEEE Trans. Control Syst. Technol.*, vol. 31, no. 5, pp. 2132–2145, Sep. 2023.

[20] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain for intelligent transportation systems: Applications, challenges, and opportunities," *IEEE Internet Things J.*, vol. 10, no. 21, pp. 18961–18970, Jun. 2023.

[21] F. A. Sunny, P. Hajek, M. Munk, M. Z. Abedin, Md. S. Satu, M. I. A. Efat, and Md. J. Islam, "A systematic review of blockchain applications," *IEEE Access*, vol. 10, pp. 59155–59177, 2022.

[22] M. Ebrahim, A. Hafid, and E. Elie, "Blockchain as privacy and security solution for smart environments: A survey," 2022, *arXiv:2203.08901*.

[23] G. O. Alandjani, "Blockchain technology and impacts on potential industries," in *Proc. IEEE 2nd Int. Conf. AI Cybersecurity (ICAIC)*, Feb. 2023, pp. 1–4.

[24] PwC. (2020). *Time for Trust: The Trillion-Dollar Reason to Rethink Blockchain*. [Online]. Available: https://www.pwc.com.cy/en/issues/assets/blockchain-time-for-trust.pdf

[25] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, "Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing," *Future Internet*, vol. 14, no. 11, p. 341, Nov. 2022. [Online]. Available: https://www.mdpi.com/1999-5903/14/11/341

[26] N. Gupta, "A deep dive into security and privacy issues of blockchain technologies," in *Handbook of Research on Blockchain Technology*, S. Krishnan, V. E. Balas, E. G. Julie, Y. H. Robinson, S. Balaji, and R. Kumar, Eds. New York, NY, USA: Academic, 2020, pp. 95–112.
[27] M. C. Lacity, *A Manager's Guide to Blockchains for Business: From Knowing What to Knowing How*. U.K.: SB Publising, 2018.
[28] J. Barney, "Firm resources and sustained competitive advantage," *J. Manage.*, vol. 17, no. 1, pp. 99–120, Mar. 1991.
[29] J. Holbrook, "Enterprise blockchains," in *Architecting Enterprise Blockchain Solutions*. NJ, USA: Wiley, 2020, ch. 2, pp. 29–68.
[30] M. Soelman. (2021). *Permissioned Blockchains: A Comparative Study*. [Online]. Available: https://fse.studenttheses.ub.rug.nl/id/eprint/25270
[31] L. D. Nguyen, J. Hoang, Q. Wang, Q. Lu, S. Xu, and S. Chen, "BDSP: A fair blockchain-enabled framework for privacy-enhanced enterprise data sharing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2023, pp. 1–9.
[32] Y. Ucbas, A. Eleyan, M. Hammoudeh, and M. Alohaly, "Performance and scalability analysis of ethereum and hyperledger fabric," *IEEE Access*, vol. 11, pp. 67156–67167, 2023.
[33] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.
[34] Md. M. Islam, M. M. Merlec, and H. P. In, "A comparative analysis of proof-of-authority consensus algorithms: Aura vs clique," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, Jul. 2022, pp. 327–332.
[35] C. V. Helliar, L. Crawford, L. Rocca, C. Teodori, and M. Veneziani, "Permissionless and permissioned blockchain diffusion," *Int. J. Inf. Manage.*, vol. 54, Oct. 2020, Art. no. 102136. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0268401219314586
[36] E. Tan, S. Mahula, and J. Crompvoets, "Blockchain governance in the public sector: A conceptual framework for public management," *Government Inf. Quart.*, vol. 39, no. 1, Jan. 2022, Art. no. 101625.
[37] E. Ben Hamida, K. L. Brousmiche, H. Levard, and E. Thea, "Blockchain for enterprise: Overview, opportunities and challenges," in *Proc. 13th Int. Conf. Wireless Mobile Commun. (ICWMC)*, Nice, France, Jul. 2017, pp. 1–7. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01591859
[38] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, and M. Omar, "Blockchain architectures for physical Internet: A vision, features, requirements, and applications," *IEEE Netw.*, vol. 35, no. 2, pp. 174–181, Mar. 2021.
[39] V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," *Bus. Horizons*, vol. 62, no. 3, pp. 295–306, May 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0007681319300096
[40] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," 2020, *arXiv:2005.14282*.
[41] M. Risius and K. Spohrer, "A blockchain research framework," *Bus. Inf. Syst. Eng., Int. J. Wirtschaftsinformatik*, vol. 59, no. 6, pp. 385–409, 2017.
[42] M. Soelman, "Permissioned blockchains: A comparative study," M.S. thesis, Faculty Sci. Eng., Univ. Groningen, Groningen, The Netherlands, 2021. [Online]. Available: https://fse.studenttheses.ub.rug.nl/id/eprint/25270
[43] S. Pongnumkul, C. Siripanpornchana, and S. Thajchayapong, "Performance analysis of private blockchain platforms in varying workloads," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2017, pp. 1–6.
[44] S. M. Alshurafa, D. Eleyan, and A. Eleyan, "A survey paper on blockchain as a service platforms," *Int. J. High Perform. Comput. Netw.*, vol. 17, no. 1, p. 8, 2021.
[45] Y. Liu, Q. Lu, H.-Y. Paik, X. Xu, S. Chen, and L. Zhu, "Design pattern as a service for blockchain-based self-sovereign identity," *IEEE Softw.*, vol. 37, no. 5, pp. 30–36, Sep. 2020.
[46] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018.
[47] N. Al-Zaben, M. M. H. Onik, J. Yang, N.-Y. Lee, and C.-S. Kim, "General data protection regulation complied blockchain architecture for personally identifiable information management," in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCECE)*, Aug. 2018, pp. 77–82.
[48] M. de Vasconcelos Barros, F. Schardong, and R. F. Custódio, "Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass," 2022, *arXiv:2202.09207*.
[49] Š. Cucko and M. Turkanovic, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021.
[50] A.-E. Panait, R. F. Olimid, and A. Stefanescu, "Identity management on blockchain—Privacy and security aspects," 2020, *arXiv:2004.13107*.
[51] S. M. Smith and D. Khovratovich, "Identity system essentials," *Evernym, Mar*, vol. 29, p. 16, Mar. 2016.
[52] P. Bai, S. Kumar, G. Aggarwal, M. Mahmud, O. Kaiwartya, and J. Lloret, "Self-sovereignty identity management model for smart healthcare system," *Sensors*, vol. 22, no. 13, p. 4714, Jun. 2022.
[53] Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu, and W. C. Chu, "Digital asset management with distributed permission over blockchain and attribute-based access control," in *Proc. IEEE Int. Conf. Services Comput. (SCC)*, Jul. 2018, pp. 193–200.
[54] B. Sakız and A. H. Gencer, "Blockchain beyond cryptocurrency: Non-fungible tokens," in *Proc. Int. Conf. Eurasian Economies*, Aug. 2021, pp. 144–151. [Online]. Available: https://www.avekon.org/papers/2527.pdf
[55] T. Sharma, Z. Zhou, Y. Huang, and Y. Wang, "'It's a blessing and a curse': Unpacking creators' practices with non-fungible tokens (NFTs) and their communities," 2022, *arXiv:2201.13233*.
[56] A. Colicev, "How can non-fungible tokens bring value to brands," *Int. J. Res. Marketing*, vol. 40, no. 1, pp. 30–37, Mar. 2023.
[57] M. Laroche, M. R. Habibi, and M.-O. Richard, "To be or not to be in social media: How brand loyalty is affected by social media?" *Int. J. Inf. Manage.*, vol. 33, no. 1, pp. 76–82, Feb. 2013.
[58] M. Epstein, *The Zen Therapy Zen Therapy*. New York, NY, USA: Penguin, Jan. 2023.
[59] A. Boukis, "Exploring the implications of blockchain technology for brand–consumer relationships: A future research agenda," *J. Product Brand Manage.*, vol. 29, no. 3, pp. 307–320, Jul. 2019.
[60] J. Choi, "Modeling the intergrated customer loyalty program on blockchain technology by using credit card," *Int. J. Future Revolution Comput. Sci. Commun. Eng.*, vol. 4, no. 2, pp. 388–391, 2018.
[61] L. Wang, R. Luo, and B. Xue, "Too good to be true? Understanding how blockchain revolutionizes loyalty programs," in *Proc. Amer. Conf. Inf. Syst.*, 2018, pp. 1–10. [Online]. Available: https://api.semanticscholar.org/CorpusID:53046545
[62] V. Stallone, M. Wetzels, and M. Klaas, "Applications of blockchain technology in marketing—A systematic review of marketing technology companies," *Blockchain, Res. Appl.*, vol. 2, no. 3, Sep. 2021, Art. no. 100023.
[63] O. Olsson, "A taxonomy of non-fungible tokens: Overview, evaluation and explanation," M.S. thesis, Dept. Inform. Media, Uppsala Universitet, Uppsala, Sweden, 2022. [Online]. Available: https://uu.diva-portal.org/smash/get/diva2:1672740/FULLTEXT01.pdf
[64] S. M. H. Bamakan, N. Nezhadsistani, O. Bodaghi, and Q. Qu, "A decentralized framework for patents and intellectual property as NFT in blockchain networks," 2021, doi: 10.21203/rs.3.rs-951089/v1.
[65] Q. Xu, Z. Song, R. S. Mong Goh, and Y. Li, "Building an Ethereum and IPFS-based decentralized social network system," in *Proc. IEEE 24th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, Dec. 2018, pp. 1–6.

HOAI-NAM NGUYEN received the B.Eng. and M.Sc. degrees in computer science from the Faculty of Computer Science and Engineering, Ho Chi Minh City University of Technology (HCMUT), VNU-HCM, Vietnam, in 2019 and 2024, respectively.

In 2019, he was a Blockchain Expert and a System Architect for several blockchain systems with Vietnam Blockchain Corporation (VBC). His research interests include agriculture management, track-and-trace applications, and blockchain technology.

HOANG-ANH PHAM (Member, IEEE) received the B.Eng. degree in computer science and engineering from Ho Chi Minh City University of Technology (HCMUT), VNU-HCM, Vietnam, in 2005, and the M.Sc. and Ph.D. degrees in information and communications engineering from MYONGJI University, South Korea, in 2010 and 2014, respectively.

From 2005 to 2008, he was a Faculty Member with the Faculty of Computer Science and Engineering. He has been the Director of the Internet of Things Laboratory and the HCMUT-Renesas SuperH Laboratory (specializing in embedded systems and robotics) since 2016 and 2018, respectively. Additionally, he is currently an Executive Member with the UTS-HCMUT Joint Technology and Innovation Research Center (JTIRC) towards smart city applications. He is the Vice Dean of the Faculty of Computer Science and Engineering, HCMUT. His research interests include computer networking, computer vision, cyber-physical systems, autonomous robots, the IoT, and blockchain.

NGUYEN HUYNH-TUONG received the B.Eng. degree in information technology from Ho Chi Minh City University of Technology (HCMUT), VNU-HCM, Vietnam, in 2001, and the M.Sc. and Ph.D. degrees in information technology from François Rabelais University, Tours, France, in 2006 and 2009, respectively.

From 2009 to 2022, he was a Faculty Member with the Faculty of Computer Science and Engineering, HCMUT. Since 2023, he has been an Associate Professor with the Faculty of Information Technology, Industrial University of Ho Chi Minh City. His current research interests include manufacturing scheduling, transportation problems, education assessment, and blockchain applications.

DUC-HIEP NGUYEN received the B.Eng. and M.Sc. degrees in computer science from the Faculty of Computer Science and Engineering, Ho Chi Minh City University of Technology, VNU-HCM, Vietnam, in 2018 and 2022, respectively.

Since 2018, he has been a Blockchain Expert and a Business Analyst for several blockchain systems with Vietnam Blockchain Corporation. His research interests include transportation applications, game programming, agriculture, and blockchain applications.