Exploring the Intersection of Cloud Computing and Blockchain Technologies: Use Cases in Decentralized Applications, Supply Chain Tracking, and Digital Identity

Ahmed Nafea Ayesh

Al-Iraqia University (Baghdad, Iraq)

ahmed.n.ayesh@aliraqia.edu.iq

Exploring the Intersection of Cloud Computing and Blockchain Technologies: Use Cases in Decentralized Applications, Supply Chain Tracking, and Digital Identity

Ahmed Nafea Ayesh

Al-Iraqia University (Baghdad, Iraq)

ahmed.n.ayesh@aliraqia.edu.iq

Abstract

The current buzz in blockchain technology has largely highlighted its use in cryptocurrencies. Blockchain can offer many advantages, such as immutable data recording, transparency via the sharing of an encrypted ledger, and decentralized and tamper-resistant mechanisms. The availability of this infrastructure can potentially change computing paradigms and yield services for cloud resources in a more secure, private, decentralized, and performant environment.

Our exploration of blockchain use cases in current cloud computing settings spans a wide range of applications, such as the decentralized applications domain, which includes de-duplication, cloud storage, data security, property rights certification for digital content, cloud storage auditing, real-time services monitoring, Several of these use cases have been explored more broadly, not just in the blockchain context but from a technology-driven standpoint. We turn our attention to the combination of blockchain in a circular relationship with cloud computing technologies.

Keywords: cloud computing, blockchain technologies, decentralized applications, supply chain tracking, and digital identity .

1.2. Introduction to Cloud Computing and Blockchain Technologies

Cloud computing is the concept of remotely hosted and scalable services that provide a service that is needed on demand. These services include compute power, memory storage, database support, and instructional standby. Cloud computing originated when computer devices or other drivers put information as a way to leverage inexpensive computing functionality. Consequently, it was observed that there was a possible structure of functionality. There were some observed knowledge characteristics about cloud computing. It is necessary that cloud computing is based on the principles of server farms, which are part of the internet. By using the internet with various web and server

technologies, a detailed setup has been established, including a set of policies and a range of services. This expanding policy shows that there must be consequences of computing visions. The main idea is to move away from having to interact on a one-to-one basis with a host machine to execute specific tasks. Cloud computing systems might not direct customers to a specified server or even a host machine for that matter. They could merely be linked to the massive resources that the system offers to implement large-scale duties with unique access. This attracts interested users who need to rent out the resources on a transactional basis. (GEORGE and GEORGE2022)

1.3. Definition and Overview of Cloud Computing

Cloud computing is the emergent paradigm for providing computing as a utility. In essence, the cloud is a resource pool that can be easily accessed and quickly provisioned with minimal management effort in terms of configuration or interaction with the provider. The task of managing services and infrastructure in a domain-agnostic manner while maintaining service level agreements can be quite challenging and is the primary objective in the design of large-scale data centers, which are characteristic of cloud architectures. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. In other words, cloud computing promises simplified access to costly infrastructure that is managed elsewhere, thus offloading the user from expensive and complicated asset procurement and management.

1.4. Definition and Overview of Blockchain Technologies

Blockchain is a decentralized, digitally distributed ledger that can store multiple types of assets. It uses participants' processing power from their computing resources. In addition to public cryptographic keys, individuals have access to a private key that is held securely and gives access to blockchain cryptography. It is the key to signing blocks of an aspiring transaction. Although the information is shown to everyone, identification is registered first. Transactions are further linked to a user by the user's digital signature. All users' peers see that the transaction has the correct signature, authorizing the transaction itself. The system is driven by a kind of intelligent authority, a consensus, unlike traditional banking. More than half the users need to accept the blockchain, which normally takes place within the first hundred blocks in the ledger to keep changing the master fork logs. This is accomplished by every work participant solving a puzzle of CPU comfort problems as directed by the network. The service is provided with a monetary reward for keeping a stable, secure network, and the transaction is authenticated. This has a 'proof-of-work' incentive referred to as the system, named after its misleading

underlying digitization as an aspect of physical difficulty. It operates in a fundamentally stable environment because the cost of controlling 51% of miners to gain control over and stage or reject transactions depends on the number of open transactions. (Gietzmann & Grossetti, 2021)

1.5. Importance of Exploring the Intersection

While we have identified various intersections of cloud computing and blockchain technologies, the development of use cases that employ blockchain technology with cloud components has not been sufficiently discussed. As cloud computing can provide enhanced capabilities to blockchain technology and a large pool of data could further enhance the learnings from the blockchain, this paper provides an exploration of the various cloud-based components that can augment blockchain technology. It is well understood that blockchain first came into existence as the technology underlying Bitcoin. Subsequently, many applications are envisioned using blockchain technology, where Bitcoin is just one of the several applications that can be built using blockchain. One of the best-known properties of blockchain is that of recording a distributed ledger. Each block in a blockchain ledger contains a list of standard transactions, a list of all new users who have submitted a transaction, and a hash of the preceding block in the blockchain. (Miyachi & Mackey, 2021)

Such a hash chain strengthens the security and helps maintain the integrity and uniqueness of the blockchain. The distributed nature of storing data eliminates a single point of control or failure. While current designs for storing massive datasets, distributed computing, and peer-to-peer edge computing may be problematic, there are few designs at present that are capable of handling small datasets, which can also interact with a blockchain. This paper begins with a review and explanation of blockchain and introduces the concept of several cloud elements or cloud computing concepts that can improve a blockchain's capabilities. With the readiness of the technology industry to adopt cloud-based systems and solutions, the intersection discussed in the paper describes how the intersection of cloud computing and blockchain portfolio characteristics can create a competitive advantage for business organizations and public administrations.

2. Fundamental Concepts in Cloud Computing and Blockchain

Cloud computing has become an expected part of everyday life yet remains a challenge to define. The definition of cloud computing uses five characteristics, as well as three service models and four deployment models. Those concepts have been supplemented over time by others. Cloud computing service models dictate the level of control the cloud user has over the cloud infrastructure. Infrastructure as a Service, the lowest level of control, is simply management of what is on the cloud.

In Platform as a Service, users can build applications with the help of tools provided by cloud providers. Software as a Service is the highest level of control, and users rent computing-based services. With respect to the deployment services, cloud computing services may be public clouds, hybrid clouds, private clouds, or community clouds based on the type of users using the service.

Blockchain technology represents a shared consensus engine or ledger for processing transactions with digital properties, such as cryptocurrencies. It is characterized by the fact that it is immutable and hence tamper-evident. It affords users an immutable history of all transactions. Blockchain is a shared, distributed ledger technology that simplifies various business processes. A blockchain is like an append-only distributed ledger wherein a group of transactions is asynchronously replicated across the ledger. Furthermore, it supports custom smart contracts for processing these transactions in addition to facilitating privacy with transaction privacy. Blockchain utilizes cryptographic techniques to verify all transactions for integrity. The blockchain architecture creates security-based consensus as part of its prescribed trust model. The blockchain can be easily maintained at low cost and results in increased efficiencies for enterprises and a single version of the truth for all participants. This makes blockchain technology like a financial institution without intermediation that supports enormous financing and integration capabilities. (Dong et al., 2023)

2.1. Cloud Computing Models: IaaS, PaaS, SaaS

Cloud computing offers a way to store information and allow access at any time via the internet. When information is stored on the cloud, data is not saved on a specific computer. Users do not have to worry about losing their data due to device breakdown. Data saved in the cloud is easily accessible via various web-based devices such as smartphones, computers, or tablets. In addition, people have the ability to share information with colleagues or friends, so they can exchange information more efficiently. Organizations can also move applications from the desktop to the cloud in order to perform office activities such as word processing, accounting software, emails, and spreadsheets that perform organizational tasks as well as other activities that are critical to ensuring the growth of their companies. Cloud computing serves as a backbone to the commercial sphere by offering access to a robust technical infrastructure. This infrastructure provides scalability, resilience, availability, and a pay-as-you-consume cost model that allows firms to focus on growing the business collection rather than solving complex technological difficulties. Cloud computing supplies three types of services: infrastructure software, computing platform, and program software. The features of cloud computing may vary depending on the type of service provided.

2.2. Blockchain Consensus Mechanisms: PoW, PoS, DPoS

A core part of a blockchain's operations is determining who has the right to append a new block of transactions. Public blockchains use an algorithm to form consensus about this right, ensuring that appenders are rewarded within the blockchain system. Different trade-offs between security, efficiency, and resource use can be achieved by tweaking the parameters of these consensus mechanisms. They fall into two categories: Proof of Work and permissionless, and have a pivotal role in ensuring the security and relevance of a blockchain. In a permissioned setup for a private blockchain, other consensus mechanisms can be employed that are more efficient than Proof of Work. This is also essential as Proof of Work requires a large amount of computational resources to mine a block.

The idea behind Proof of Work is to require some work to be performed in creating a new block. In detail, the content of the new block and a nonce must be hashed, and the result compared to a known value or set of values. This is a simple set of operations a computer can execute. It cannot be completed exhaustively as a fixed-point finding problem, and this cannot be solved better than ineffectively attempting it about once every ten minutes. When the correct nonce is found, this constitutes proof, and the block is appended to the blockchain. The node accomplishing this gets to include the set of transactions that will go into the newly mined block in their preferred form and is rewarded with some amount of cryptocurrency. The set of content validators must consider must not be predictable. This is achieved by including the hash of the previous block. This ties new blocks to the history that precedes them. If a Proof of Work blockchain grows long, it is unlikely users will be interested in changing a piece deep inside the block. The benefit of this is that a large fraction of the nodes will continue to build on the longest branch, creating a self-reinforcing commitment effect. The cost is the requirement for proofs to be included in the block's header to be statistically verifiable. The cost for miners today is the energy it takes to operate their mining machines. A side effect is that the incentive to maintain the network is derived from having a market value for the coins supported on the platform. Consequently, the large chunk of data warehouses dedicated to mining run only because the corresponding value, if monetized as a traditional storage or distribution service, would make it relevant. However, the benefit for the network is null, since a significant fraction of the invested money in mining is dedicated to the mining itself. It is substantial that mining farms are hosted for most of their energy consumption in places where energy is cheap and stable, hence where mining is more profitable, often fed by renewable and oversupplied power. (Sovacool et al., 2022)

3. Use Cases of Cloud Computing and Blockchain Integration

In this section, we present three use cases that describe how emerging instances of pairing blockchain technologies with cloud computing are providing novel solutions to technical challenges and business problems in applications such as decentralized applications, track and trace blockchain supply chain tracking, and digital identity. These are among the applications that are highlighted as prime capabilities in the intersection of both technologies. We present a detailed characterization of these use cases through a thorough survey. We then describe how these use cases can benefit from the integration of those two technologies and contribute emerging key problem statements.

Cloud environments allow customers to use resources, such as virtual servers, storage, web hosting, and email, without incurring the corresponding overhead of the hardware, software, high-bandwidth internet connection, or security experts necessary to maintain a data center. Although cloud adoption is increasingly recognized as a business enabler, there are several scenarios, such as secure application execution and provenance verification, which are increasingly ubiquitous in both the consumer and business sectors, where the cloud model may present major technical challenges. To answer these challenges, blockchain technology can enable transformational capabilities across various trust-based IT use cases. It overcomes the need for a trusted third-party intermediary, thereby enabling transactional trust. Hence, combined, these two emerging technologies, cloud computing and blockchain technology, have the potential to make a significant impact on today's infrastructure for trusted computing and towards enabling groundbreaking trust-based services. (Qian and Papadonikolaki2021)

3.1. Decentralized Applications (DApps)

Decentralized Applications (DApps) - Perhaps the most popular use case for exploring the intersection of cloud computing and blockchain technologies concerns the creation of decentralized applications (DApps). Just as with traditional web-based applications, software developers use specialized tools and create applications that typically provide some type of interface to users over the Internet. While common, traditional web-based applications rely heavily on cloud-based servers and data storage architectures to work. The servers and storage are typically controlled by the organization associated with the web application, with data shared between the cloud service and associated databases, web servers, and even business logic hosted on the servers. With only a few exceptions, centralized control and service are the defining characteristics of traditional web applications. When the idea for a DApp is

conceived, however, the centralized control model is often rejected in favor of a more controlled and transparent approach to both client data and Application Programming Interface execution.

DApps are a form of software or interface that allows the contents of a smart contract written to a blockchain to be manipulated. The contract dictates how data should be viewed, by whom, and gives a set of rules for how data should be modified. Unfortunately, using a blockchain as a cloud and application host is extremely limiting by design. The virtual machine, for example, takes a significant amount of computation to perform even a simple operation like storing data on a blockchain. In order to perform this operation, a user must supply gas, or a unit of computational power, in the form of cryptocurrency. At the time of writing this chapter, the cost to perform even a very simple operation would be prohibitively expensive. Furthermore, organizations associated with many of the most successful DApps now face, or will face in the near future, significant scalability issues related to their application's blockchain and cloud architectures. (Murthy et al., 2020)

3.2. Supply Chain Tracking and Management

Supply chain management (SCM) includes a set of approaches utilized to effectively integrate partners and achieve efficient production and distribution methods. SCM has gained increasing interest and become an important part of every business. In recent years, companies have begun to pay more attention to transparency and traceability in their supply chains. Improved supply chain transparency not only reduces risks and meets safety and quality requirements but also allows companies to assert better whether the partner's or supplier's practices and products are ethical or sustainable. However, these benefits could be destroyed by creating a good but false impression. One approach to deal with this is to demand increased transparency on data from the partner or supplier, which will increase the respectability of your claims with third parties. To meet these requirements, blockchain technology appears as a possible solution, as it enables individual parties to obtain trusted information about products. Supply chain blockchain applications could enable increased traceability, visibility, and oversight in the supply chain, making it easier to make fair quality and ethical claims.

Many industries seek to adopt supply chain blockchain solutions for one or more of these reasons. The most obvious use case for supply chain blockchain is the ability to track products from origin to end consumer's hand. This is important in many scenarios such as food safety, product recall, luxury product anti-counterfeiting, and so on. Manufacturers or the supply chain could use this capability in these scenarios to support, verify, or deny insurance claims, import tariffs, etc. As global trade increases, increasing transparency becomes more important because there can be six to eight

intermediate suppliers between raw material production and finished products, resulting in increased opportunities for counterfeiting before arrival on the shop floor. Because supply chain blockchain applications make tracking transparent and available in near real-time, the obstruction and data falsification of the existing supply chain management system that trade participants can view will be reduced. As a result, rapid, accurate responses to product counterfeiting, distribution disruptions, and other situations for related supply chain participants will be possible. (Gonczol et al., 2020)

3.3. Digital Identity Verification

There have always been the twin challenges of verifying who someone is and what they are saying. In the online world, the task of authenticating identity is most often solved with a combination of usernames, passwords, and confirmation codes sent via email or SMS. In the past, it has been the case that only in-depth checks provide a higher level of trust. However, while these verification processes provide a high level of confidence, they cannot be used all the time. For one, they are time-consuming, which adds friction to a customer/business interaction. Secondly, they are also expensive because trained staff need to be involved in the process. The significant issue with this system is that once a user's private data has been compromised, they are at a much higher risk of fraud and identity theft.

Blockchain technology is interesting in this context due to the combination of immutability, encryption, and pseudonymity that it makes possible. The immutability of blockchain's record means that you build a chain of trust that can be trusted by anyone. There are no access controls, no license agreements, and no terms of service that you have to accept. You can call on its unmatched ability to ensure that no record has been changed or altered going forward. By encrypting sensitive data and using the address of the encryption signature as a pseudonym, private user data is kept secure. Finally, the immutable nature of the data in a blockchain prevents users from denying their actions when using a system. All of these characteristics combine to form a powerful protection program that allows personal information to be protected while still allowing data to be used as the link between physical and digital. (Dong et al., 2023)

4. Challenges and Opportunities in Integrating Cloud Computing and Blockchain

Cloud computing and blockchain technologies are both slow to change but become more robust over time. They are mutually complementary and could work together to promote the development of the Internet. This, in turn, develops both cloud providers and users. Given the ever-growing interest in blockchain technology, it is likely that we will continue to see an increasing number of use cases and

platforms that leverage both cloud computing and blockchain. The combination can be used to address problems that arise in the cloud in a scalable, distributed, and secure way.

Despite the potential of blockchain and cloud computing presented as a potent deployment nexus, several challenges require attention. Research is needed to understand and address these challenges, while cloud service providers are integrating these technologies into their offerings. The challenges include trusted non-profit participants, inter- or intra-organizational business processes development using both technologies, contracts running on cloud platforms, multi-fold business contracts, SLA enforcement, developing consensus mechanisms, and developing financial cloud computing business metaphysics. (Habib et al.2022)

4.1. Scalability Issues

Scalability is a well-known Achilles' heel of blockchain systems. Bitcoin and Ethereum can only process a handful of transactions per second, resulting in long wait times and high fees during times of heavy load. On the other hand, cloud computing data centers can execute billions of instructions per second, but their current storage and CPU levels to handle all blockchain transactions would result in excessively high costs both to store the data and to transact. Transaction costs should remain quite modest—or ideally free—in order to see some solutions become viable with large numbers of microtransactions. A limited capacity to store data, especially during periods of rapid growth, is also a known issue. The dataset price must remain such that the classical data center keeps a copy of the blockchain. In the absence of large companies able to act as trusted nodes for other blockchains, data has to be easily accessible. In Ethereum, it is easy to catch up with the latest blocks with a fraction of a device as long as that device has sufficient storage space to retrieve all the data. Finally, all miners and validators have to be able to verify transactions quickly and for a very low cost. Such conditions are necessary for blockchains to be viable for large-scale use cases.

4.2. Interoperability Challenges

Interoperability is the capability of different information and communications technology (ICT) systems, software applications, and services to communicate, read, manipulate, and exchange data with a high degree of meaningful understanding in order to facilitate their accessibility, sharing, use, and reuse. Interoperability is a present and future challenge due to the existence of multiple blockchain technologies embodying diverse technological and architectural features. Different consensus mechanisms, cryptographic algorithms, network topologies, gas price allocation models, transaction throughput rates, and consequently, economies reinforce the difficulty of developing a component able

to efficiently and reliably communicate, read, and write data across several heterogeneous blockchains with minimum loss of data consistency and reliability. Although several techniques and protocols address the interoperability challenge, enhancing the connectivity and interaction between blockchains, full interoperability among blockchains remains an unsolved issue.

A literature survey covering metadata and identity management, peer-to-peer networks, cross-chain protocols, cross-chain atomic swaps, oracle services, and prediction markets, as well as the interoperability model and the connection model distinguishes projects centered on limited blockchain networks having a finite and select number of pre-registered member blockchains and machine-to-machine communication requirements from those supporting unbounded networks. The connectivity problem is divided into two sub-problems. Firstly, some systems allow pre-registration of blockchain URLs for future communication. Secondly, other systems focus on transaction lifetimes, cross-chain transactional state, and data processing requirements to derive a shared public key preventing exfiltration of bitcoins from one side of the channel to the other side. Each project is evaluated in terms of its capabilities, restrictions, needs, limitations, communication requirements, scalability, and trustworthiness. The evaluation criteria refer to aspects such as restoration and maintenance responsibilities, size of the trusted base, connectivity range, network topology, some choice restrictions, flows, degrees of privacy, blockchain state, data interchange, and cost. (Teymourifar et al.2021)

4.3. Security and Privacy Concerns

While the technical aspects of a solution vary greatly within the cloud, security and privacy are and always have been a major concern. Multiple cloud solutions exist to provide secure storage and computation, but each brings an increase in difficulty for the developer using that service and increased lifetime costs. To bring these concerns to a solution built on blockchain technology, we consider a solution's trust model. If usable software is a primary concern, then we believe the solution must require minimal additional effort from existing software vendors. This gives us three high-level threat models to consider: service provider, malicious miner, and users of the service. The service provider threat model considers the types of threats that can be posed by the cloud service provider. The malicious miner considers the types of threats that can be posed by those running the public blockchain infrastructure. The users of the service model consider the types that should be provided additional capabilities to further control access to their data. We can classify these solutions into three categories: utilize a private blockchain, utilize a public blockchain, or utilize a centralized trust party. (Habib et al.2022)

5. Research Methodologies in Studying Cloud Computing and Blockchain Integration

Exploring the intersection of cloud computing and blockchain allows firms to understand how the integrated system can benefit blockchain systems during the development and implementation phase. This chapter subjects itself to the task of understanding this intersection from the perspective of cloud customers in terms of value delivery. Using a use case-based approach, this chapter establishes the customer-focused understanding of cloud computing and blockchain systems through data and resonates with findings from the cloud computing and blockchain systems literature to build propositions and develop future research directions. With the findings from the use case analysis, the implications of the integrated cloud computing and blockchain technologies in order to reduce the present gap in the understanding of and adoption of cloud-blockchain systems.

This research adopts the methodology of a review of literature to establish a theoretical base for customer-driven creation of value at the intersection of cloud computing and blockchain systems. Following this, the chapter uses a use case-based approach to bolster this theoretical base and corroborate the contribution of applied work from the cloud computing, blockchain, and the Information Systems literature. We believe that this approach of developing integrated cloud computing-blockchain models through a use case-based approach not only fills several gaps in this domain but also enriches this multidisciplinary tapestry of cloud and blockchain systems. (Mio et al.2020)

5.1. Literature Review

The idea of locating both blockchain oracles and decentralized application backend servers in the same environment, particularly one that leverages a more dynamic infrastructure, offers a lot of promise going forward. We first draw a high-level comparison between multiple popular cloud computing options. We then discuss the use of cloud-init and other patterns for booting nodes, and then apply these concepts to the question of how a chain coordinator can use ephemeral cloud infrastructure to propagate state changes from multisignature wallets to smart contracts. Finally, we offer a concrete breakdown, in terms of costs and latencies, of our test implementation. It also supports more straightforward escrow transactions in which the funds held by the contract are released by multiple keys held by independent signatories. It allows for the execution of a Turing-complete script, allowing something like a traditional program to run on many nodes. Such programs return deterministic results when run with a common runtime context, including the contents of a contract’s state. The community

has developed a number of useful dapps like decentralized exchanges, without setting up off-chain trust-minimized oracles to provide their data.

5.2. Case Studies

5.2.1. Real Estate Transactions Buying or selling a home or residential property can be a long and cumbersome process, requiring the coordination of multiple parties including property inspectors, banks, mortgage and title companies, and lawyers in order to finalize the transaction. By leveraging blockchain and cloud technologies, several initiatives have piloted to streamline transactions. The key elements include the use of a blockchain architecture hosted on a digital cloud platform that non-trusted parties can access. Performance, data security, and immutability of a distributed ledger core are the main characteristics of blockchain technology, and thanks to the cloud platform, those benefits can be easily accessed by any peer connected to the internet regardless of their technical skills. The cloud platform is utilized to store the encrypted digital signature to allow access to the parties involved, but also to store the original documents such as architectural drawings, mortgage information, and lien research. Outcomes demonstrated how a cloud-based blockchain architecture can integrate tools to provide seamless verification of immutable transactions without the interference of a middleman. The results illustrate the potential of this architecture to extend beyond real estate into other industries like healthcare, e-voting, intellectual property, and so on.

5.3. Experimental Research

We started, as we said, by performing some proof-of-concept experiments that are meant to provide a practical preliminary evaluation of the performance of blockchain systems implemented on the cloud. The blockchain and the Byzantine Fault-Tolerant system are two of the most used systems today for implementing blockchain systems and have many implementations that are used to test the performance of the applications utilizing these implementations. However, as shown by the experiments we carried out, the first is much more scalable with the increase of the load than the second. The same is true for identifying specific transactions used in the process of the experiment, and the proof-of-concept program we first implemented could be essential in scaling the applications implemented on the cloud that uses the system. These solutions were ranked among the best alternatives, where the second system was found to be not very scalable, and the first was proven to be scalable on the FIFO of the Second Test Plan, where it worked on all FIFOs but also failed when the experiment on the same FIFO was repeated seven times. Due to our priorities, we intend to improve our study in the future with final

experiments to conduct a complete analysis and discuss the other security requirements of the implemented systems, their costs, and make a significant effort to replicate our work.

6. Decentralized Applications (DApps) in Depth

Defining Decentralized Applications (DApps)

DApps, also known as smart contracts, set the stage for the rest of the book by directly implementing blockchain and cloud computing technologies together. When a blockchain supports at least one smart contract in its ecosystem, it is referred to as a second-generation blockchain (as opposed to first-generation blockchains, like Bitcoin, which use blockchains to simply store and transmit information). Conversely, it can be said that the purpose of a smart contract is to implement a DApp on a blockchain. The first truly complete configuration of a DApp on a blockchain was Ethereum.

Decentralized applications can be understood directly from the name of the concept. Nowadays, web applications like Facebook and SimpleNote do not run in a single infrastructural location; rather, they are distributed throughout servers all over the world. Netizens connect to these applications via the cloud. But why are these types of web applications being called centralized? Because any server hosting the application may suffer from failures or attacks, as we well know from traditional cloud computing. Also, the publishers of these web applications contain (and may even manipulate) the user data that passes through the applications. However, DApp architectures significantly alleviate these two problems by running the code and data locally on the web's cloud-based users, who only need to interact with consensus algorithms to maintain these applications as a group of peers. (Popchev & Radeva, 2024)

6.1. Definition and Characteristics

To help the reader fully appreciate how to explore the intersection of cloud computing and blockchain technologies in decentralized applications, and how to perform use cases in supply chain tracking and digital identity use cases, this last part of this chapter aims to detail some background knowledge. We first provide subsections describing what blockchain and cloud computing are, as well as presenting some common characteristics of each, and then dive into existing works that explore the integration of cloud computing and blockchain technologies.

Blockchain has created a ripple effect in the technological world by accomplishing distributed, peer-to-peer consensus without the help of a central trusted authority. Now advocates of the technology feel that a myriad of transactions in various domains such as finance, insurance, logistics, and education

could become more trustworthy if they adopted blockchain constructs. A blockchain can be defined as a decentralized, distributed, and also autonomous data management protocol designed for robustness, security, and anonymization. Each blockchain node implements a peer-to-peer network, protocols for secure transaction verification, methods for accessing the blockchain, and enables redundancy, transparency of operations, and immutability of the stored ledgers. Blockchain maintenance, the key to its operation, could be either permissionless and public, permissioned and private, partly private and partly public, or generic, i.e., tailored to the specific echelons of commerce and business to which respective user communities belong. (Santana & Albareda, 2022)

6.2. Architecture of DApps

The drive to discover new ways to extend the use of cloud computing technologies is a constant theme in the computer science fields within academia, in the research and development endeavors of information technology companies, and in the marketplace in general. The growing use of cloud technologies, and the demand for new and innovative applications, have led to significant efforts to research ways that applications running in the cloud can interact with innovative technologies such as blockchain. The goal of this paper is to provide new insights into the intersection of these two important technologies, not just what they are, but how they work together. Cloud service models, types, and popular providers will first be introduced, before considering what blockchain technology is and the basics of how it works. After considering these two sections, a detailed exploration of the potential intersection of these technologies will provide new insights for researchers, industrial technologists, and curricular developers in computer science, information technology, and related areas. (Zhaobin et al.2024)

6.3. Popular DApp Platforms

Ethereum has emerged as the most popular platform for DApps thanks to its programming model and in-built support for smart contracts. Smart contracts propose generic, programmable, trusted, and transparent mechanisms for providing or consuming decentralized services. The applications of smart contracts are plenty; a well-known example is the exploitation of smart contracts in the case of a decentralized organization, which exclusively runs on Ethereum. Currently, there are numerous successful DApps present on the Ethereum blockchain. Smart contracts are written by developers in a Turing-complete language called Solidity, which is then compiled into Ethereum Virtual Machine bytecode, the executable format for Ethereum contracts. Ethereum has a short block time and allows for

the validation of smart contracts in a Turing-complete language, which contributes to its popularity. (Jamil et al., 2021)

7. Supply Chain Tracking with Blockchain Technology

Supply chain management (SCM) deals with the efficient and effective design of a networked relationship among numerous companies integrated into a business process that transforms raw materials into final products and ultimately provides them to customers. These companies generally include producers, suppliers, distributors, and customers that modify and transfer the products. The decentralized nature of blockchain and smart contract applications can facilitate transparency, traceability, and immutability features critical to all supply chain management processes. By utilizing the procurement process, a supply chain can be tracked through the combined use of smart contracts and blockchain. It is quite valuable in locating points of failure and contamination before and after the successful delivery of goods. Moreover, progress in the supply chain with the help of blockchain can decrease delays, cut down expenses, and restrict fraud. By structuring the processes in the form of smart contracts in supply chain applications, operations that are currently being conducted by intermediaries can be automated.

Blockchain can be successfully applied to SCM processes due to the significant number of related examples for retailers and suppliers. The potential of utilizing blockchain technologies for SCM is already a major focus in the industry and academia. The real-world SCM use cases that are currently in the proof-of-concept or pilot testing phase are based on various blockchain platforms. For example, a novel technique has been proposed to identify vulnerabilities in global supply chains. This work uses cryptocurrency to follow and verify the flow of goods and handle the recall and reputation of counterfeit product manufacturers to ensure the supply chain is entirely protected against counterfeiting. (Dutta et al.2020)

7.1. Importance of Supply Chain Transparency

In this chapter, the intersection of cloud computing and blockchain technologies from a use case perspective is researched. The open-source technology stack is explored as an enabler for the next generation of decentralized applications. Examples of three such supply chain use cases are provided. The importance of true transparency in the supply chain is introduced.

In all businesses, various aspects like the cost of operations, energy, and other inputs required for operation have become increasingly important topics on the agenda. Ideas like corporate social

responsibility are gaining importance. The need to deliver on the promises made to customers means that today companies not only need to think in terms of near real-time changes to the supply chain but also need to be able to communicate these changes and adjustments with customers. They need to have the capability to share the truth of what is happening from the raw material processor to the retailer. Customers should not only be able to verify the authenticity of the various products irrespective of their location but also be able to access all the facets of the journey of that product. Providing proof of being counterfeit-free and conveying all the information, irrespective of the number of nodes or processors involved in the lifecycle of the product, is essential. Cloud and edge computing solutions become enablers in the journey of this information and transparency, along with the combination of blockchain technology.

7.2. Benefits of Blockchain in Supply Chain Tracking

The supply chain is an obvious and early target for blockchain. This is due to a reality that knits modern global commerce together, one that aspiring disruptors need to appreciate: few, if any, single companies still truly control an entire supply chain. Even large corporations enroll third parties, a mix of suppliers, manufacturers, transportation and logistics firms, and others to move component parts and products from origin to destination. Blockchain can enable a level of decentralized trust and coordination needed for optimizing the supply chain. By democratizing access to historical trade and logistics recordings across companies and regions, enterprises can integrate the logistics processes of all the parties involved on a single platform and still manage assured access control over who can interact and access data.

Additionally, with immutability in trade and logistics record keeping powered by decentralized trust, both the enterprises and the individual parties can secure greater transparency in real time, resulting in reduced fraudulent activities through sharing of consignment tracking and monitoring, and in improved customer satisfaction through trusted verified delivery estimations. Finally, with automatic verification at every stage enabled by integrating smart contracts into the supply chain process flow ledgers, enterprises can increase the speed of goods transit, reduce discrepancies, and enforce contractual compliance, resulting in reduced structural delays and human errors. (Udeh et al., 2024)

7.3. Real-world Examples

The concept of a decentralized application (dApp) is a primary blockchain use case. Instead of running on a single computer, a decentralized application operates on a P2P network of computers. These types of dApps enable developers to leverage features of blockchain ledgers to create consumer and/or

enterprise applications, where users maintain full control over their data and where they are incentivized and rewarded for their contribution to and use of the network.

Examples of dApps can be found in different fields, such as in the area of finance: a prediction market platform; a decentralized autonomous organization; and a money market protocol. In the area of social networks, there are various platforms. A secure multi-blockchain and multi-currency wallet for users is also available. The Ethereum network has the most dApps. There are a decentralized network of nodes that are able to communicate with one another; a blockchain game where players can buy, breed, and sell digital cats; and a cryptocurrency wallet. It is often used to store Ethereum and ERC20 tokens. There are many dApp marketplaces, from various app stores to others that list hundreds of applications grouped by the network they operate on.

8. Digital Identity Verification using Blockchain

The importance of digital identity verification has grown in recent years as online and e-commerce activities continue to proliferate. More and more services take advantage of digital apps to enable various activities and transactions, creating new digital personas users identify with. Secure digital identity verification becomes significant to control the digital crime issue. Blockchain technology becomes a major facilitator for protecting digital identities from being stolen.

The idea of implementing a blockchain-based identity verification system has been proposed. The approach of injecting digital identity data into blockchain nodes is needed. The strong linkage between digital tokens and human process entities has been established. Then digital identity verification can be performed by retrieving missing information. The idea of merging miners who are working both in blockchain mining and in the exchange of private information check processes has been proposed. This approach helps to verify the identity of the information receiver and prevents data leakage. In addition, attempts to index the user's private data still allow quick searches but do not access the data to be obtained, even removing the storage facility. Several companies have already used blockchain technology to protect digital identities. A software company has developed a blockchain-based digital identity verification application for establishing secure transactions. The company provides a blockchain-based platform for a variety of applications in multiple industries. The security and convenience of the program have been enhanced to protect the identity and data of both legal entities and individual customers. At the same time, a product is created that allows users to record their marriages, diplomas, and birth certificates using the blockchain platform. This effort is aimed at solving

the problem of legal identity in the world. Once the identity of a person is misused in these countries, it is impossible to register and verify through all centralized systems. (Zwitter et al., 2020)

8.1. Challenges in Traditional Identity Verification

Identity theft, as well as data breaches from service-providing organizations, has led to a loss of trust in online transactions. Malicious users with fake identities take advantage of the fact that governments have not been able to provide efficient online identity solutions for the majority of their citizens. In some countries, the only online government service that uses a person's real identity is electronically filed tax returns. Critics argue that later down the line, hidden costs can be reflected in a trade-off between identity confirmation assurance levels and the strength of the protections developed to secure identified transactions. Service providers following the principle of risk-based authentication assign different risks to different types of transactions. For organizations, these assignments are based on considering integrity and confidentiality measures along with continually ensuring the security of their applications.

The problem with risk-based user authentication is that the privacy of the user is not fully guaranteed. Privacy and identity management issues have been defined as the root of online insecurity. In Europe, the General Data Protection Regulation clarifies that any processing of personal data has to be justified under one of six lawful conditions, determined by the Data Protection Act. The ePrivacy regulation made it impossible to delegate authentication services to companies not registered inside European borders. However, two years later, the European Commission included an article on eID to be one of the priorities of the eEurope action plan. Since then, the European Commission has spent millions in order to support the mutual recognition by Member States of eIDs. Evidently, more efforts are necessary in order to establish an effective eID solution supporting an internal European digital single market, compatible with international regulations, and at the same time, acceptable to citizens. (Yeung & Bygrave, 2022)

8.2. Advantages of Blockchain-based Identity Verification

Decentralized identity verification systems offer substantial potential advantages over their centralized counterparts. It is worth noting that the capacity to assure that an individual is who he or she claims to be is foundational for many real-world interactions. Some examples include proof of age and proof of citizenship, as well as essential financial services such as obtaining a loan, receiving unemployment or other benefits to which an individual may be entitled, or even downloading free digital content. Despite

this need, on a global basis, there are believed to be over one billion people who lack the conventional forms of official ID which are often required for these sorts of transactions. (Glöckler et al.2024)

8.3. Case Studies

Embarking on the journey of bridging two major distinct technologies: cloud computing and blockchain, we develop several case studies or use cases for exploring our propositions. Some of the use cases are realistic where blockchain can be replaced by cloud and still work, but blockchain offers different advantages than cloud does at a significantly low cost. Some use case scenarios are hypothetical, but may serve to enable new applications or technologies when cloud meets blockchain. In our use cases, we take examples from decentralized applications, supply chain tracking, counterfeit warranties app, digital identity and access management, decentralized VPN, and decentralized AI marketplaces.

For the use case of decentralized applications, we consider the realistic scenario of cloud and blockchain acting as generalized backend services. The use case assumes that the public blockchain platforms over the cloud host smart contract software comprising data and logic for an application service. In this model, the overall client payment and computation retrieval architecture are such that when trusted code is uploaded, it can be programmed to enable the retrieval requests. These requests can return the response required by a phase two operation on the relied cloud resource. For decentralized cloud services, we consider the hypothetical scenario where a cost-effective architecture is built using both cloud and blockchain that can support storage and computation, enabling the deployment of cloud services to end users. The decentralized cloud services employ an off-chain cloud database managed by cloud service providers operating in a decentralized setup on a large scale. These service providers may offer cost-effective, untrusted resources.

10. Conclusion

Blockchain and cloud computing are technologies which by their very nature are designed to enable collaboration and cryptocurrency paradigm. However, as we have explored the various use cases, it has become clear how cloud computing can address some of the inherent challenges with blockchain implementation, making it more viable for a range of different applications. We have seen that blockchain is a fit for a range of applications given its key attributes of being trust, transparency, and auditability with its goal to enable decentralization. However, it is also clear at the same time that cloud computing is also a good for a wide range of applications, because of the need for centralized management and control for enabling business logic that blockchain doesn’t necessarily provide. It is

important to stress that cloud computing partnering with Blockchain technology can enhance the key attributes of blockchain, and bring decentralization to a wide range of different applications. Blockchain teamed up with cloud computing is a secure, flexible, and cost-efficient solution. Given the rapid grow of IoT devices and platforms, and the growth of decentralized and centralized business applications, the work put forth in this chapter will be useful for developers, researchers, and decision makers on the relationship and trade-offs between cloud and blockchain technologies, and in assisting in trying to decide which technologies may suit an application best. In particular, the analysis framework, and the case studies, user can see that many centralized enterprise applications can be replaced by decentralized ones.

References

GEORGE, D. A. S., & GEORGE, A. H. (2022). Potential risk: Hosting cloud services outside the country. International Journal of Advanced Research in Computer and Communication Engineering, 11(4), 5-11. researchgate.net

Gietzmann, M. & Grossetti, F. (2021). Blockchain and other distributed ledger technologies: where is the accounting?. Journal of Accounting and Public Policy. ssrn.com

Miyachi, K. & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information processing & management. cafetarjome.com

Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. PeerJ Computer Science. peerj.com

Sovacool, B. K., Upham, P., & Monyei, C. G. (2022). The “whole systems” energy sustainability of digitalization: Humanizing the community risks and benefits of Nordic datacenter development. Energy Research & Social Science. sciencedirect.com

Qian, X., & Papadonikolaki, E. (2021). Shifting trust in construction supply chains through blockchain technology. Engineering, Construction and Architectural Management, 28(2), 584-602. ucl.ac.uk

Murthy, C. V. N. U. B., Shri, M. L., Kadry, S., & Lim, S. (2020). Blockchain based cloud computing: Architecture and research challenges. IEEE access. ieee.org

Gonczol, P., Katsikouli, P., Herskind, L., & Dragoni, N. (2020). Blockchain implementations and use cases for supply chains-a survey. Ieee Access. ieee.org

Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: benefits, challenges, applications, and integration of blockchain technology with cloud computing. Future Internet, 14(11), 341. mdpi.com

Teymourifar, A., Rodrigues, A. M., & Ferreira, J. S. (2021). A comparison between simultaneous and hierarchical approaches to solve a multi-objective location-routing problem. Graphs and Combinatorial Optimization: from Theory to Applications: CTW2020 Proceedings, 251-263. [HTML]

Mio, C., Panfilo, S., & Blundo, B. (2020). Sustainable development goals and the strategic role of business: A systematic literature review. Business strategy and the environment, 29(8), 3220-3245. unive.it

Popchev, I. & Radeva, I. (2024). Decentralized Application (dApp) Development and Implementation. Cybernetics and Information Technologies. sciendo.com

Santana, C. & Albareda, L. (2022). Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda. Technological Forecasting and Social Change. sciencedirect.com

Zhaobin, C., Jingrong, H., Chenyang, F., & Xinyi, J. (2024). Research on smart contract and front-end technology integration in Dapp development. Academic Journal of Computing & Information Science, 7(3), 55-62. francis-press.com

Jamil, F., Iqbal, N., Ahmad, S., & Kim, D. (2021). Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. Ieee Access. ieee.org

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and transportation review, 142, 102067. nih.gov

Udeh, E. O., Amajuoyi, P., Adeusi, K. B., & Scott, A. O. (2024). The role of IoT in boosting supply chain transparency and efficiency. tgdaddy.com

Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: universal identity management and the concept of the “Self-Sovereign” individual. Frontiers in Blockchain. frontiersin.org

Yeung, K. & Bygrave, L. A. (2022). Demystifying the modernized European data protection regime: Cross-disciplinary insights from legal and regulatory governance scholarship. Regulation & Governance. wiley.com

Glöckler, J., Sedlmeir, J., Frank, M., & Fridgen, G. (2024). A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Business & Information Systems Engineering, 66(4), 421-440. springer.com