JOURNAL OF INTERNATIONAL CRISIS AND RISK COMMUNICATION RESEARCH
ISSN: 2576-0017
2021, VOL 4, No S4

From Legacy to Innovation: Architecting CloudBased AI and Blockchain Solutions for Secure and Intelligent Financial Transactions

[1]Abhishek Dodda,

Principal Product Manager,abhishek.dodda1@gmail.com, ORCID: 0009-0000-6728-945X

Abstract

Research and development (R&D) progress and thinking in interweaving cloud-centric AI and blockchain technology have been ongoing and growing over the last three years. In the shadow of the global pandemic, we see their realization in actual solutions in the financial services industry. The joint solution—AI and Blockchain Powered by Data Engineering for Business—addresses a historical operational issue, improves inter-organization relationships, safeguards transactions, introduces machine operational intelligence for blockchain nodes, introduces off-ledger intelligent online diagnosis possibilities, and can help three frontline professionals in financial services. Such AI-driven blockchain solutions can be considered a case in a class of their own. They are in marked contrast with another cloud-centric characteristic—blockchain-first AI provisioned by Cloud AI services for blockchain-aware deep learning.

We begin by giving arguments for the significance and timeliness of our position by reviewing the large implications of the realized and not-yet-realized facets of blockchain- and AI-centric financial transaction systems, before proceeding with the current state of the art of unifying cloud, blockchain, and AI. We discuss the general authenticity of transactions, followed by a specific case study articulating how secure and intelligent financial systems are being architected for today's stakeholders. A matching blockchain architecture hierarchy is then presented. Such a hierarchy cannot ignore the necessity of business process innovation with relevance and authenticity secured by AI. We conclude this exposition with a call for the de-autonomization of the current cloud blockchain generation.

Keywords: AI-driven blockchain, Cloud-Centric AI, Blockchain in Financial Services, AI-powered financial Transactions, Secure Intelligent Systems, Data Engineering for Business, Blockchain Node Intelligence, AI for Transaction Security, Cloud AI for Blockchain, Blockchain-Aware Deep Learning, Financial Systems Innovation, AI and Blockchain Integration, Machine Learning for Blockchain, Off-Ledger Diagnosis, Smart Contracts and AI, Business Process Innovation, Blockchain Architecture Hierarchy, AI for Fraud Detection, Autonomous Cloud Blockchain, Future of Financial Technology.

1. Introduction

Today, financial services are performed in a large regulated, and, in many aspects, centralized ecosystem. Financial services are accessible only to a restricted set of consumers and providers due to regulations, technological impediments, security, privacy, and user experience issues, among others. At the same time, domain-specific mammoth expenses endure for both financial services industry players and consumers, which are associated with non-zero operations latency. Very often, financial services transparency, auditability, and trust reliability face challenges from all stakeholders. Financial services revolve around transactions between stakeholders and business

or market entities or instruments at different granularities, and a set of prices characterizes each set of transactions based on the market's claims and available evidence or history. Market infrastructures, as some of the most utilized institutional bets, play a key role in regulation, solvency, and financial stability. These financial milestones have triggered innovation, with different learning curves; this equally applies to the transactions' network of digital data and information, including AI and blockchain technologies.

In search of sustainability, resilience, and intelligence, a new digital framework tailored to financial market transactions needs to be envisioned. This digital infrastructure should deploy secure systems to guarantee that all transactions happening on the backbone are frequently and immutably protected. Providing issuance, transfer, and sharing interoperability standards, a set of APIs should be key for innovation, making value exchange between transactions available for other FinTechs easier from the marketplace. Consequently, this signifies a call for financial market transactions, which are at the core of the financial segment, to lead in terms of digital transformation design. With this in mind, this paper proposes to architect cloud-based AI and blockchain secure and intelligent transaction solutions that contribute to the framework for transactions of the future and enable the digital transformation of the financial industry in a broad sense.

1.1. Purpose and Scope of the Study

Since security has proven an obstacle to smooth and cost-effective transactions in digital finance, healthcare, and insurance sectors, the study aims to develop financial delivery solutions that address security concerns for businesses where data privacy and security are the greatest concerns. The study combines the use of AI with the trustworthiness of modern cryptographic blockchain to provide solutions that enable users to expand the range of financial services from a regulated territory to a flexible hybrid of permissioned and permissionless environments in insecure, threat-ridden jurisdictions. The smart contract provides the ability to mix the payment rails of two countries and the ability to conclude cross-jurisdictional financial agreements that are not onlyecure but also private using computation-driven technology.

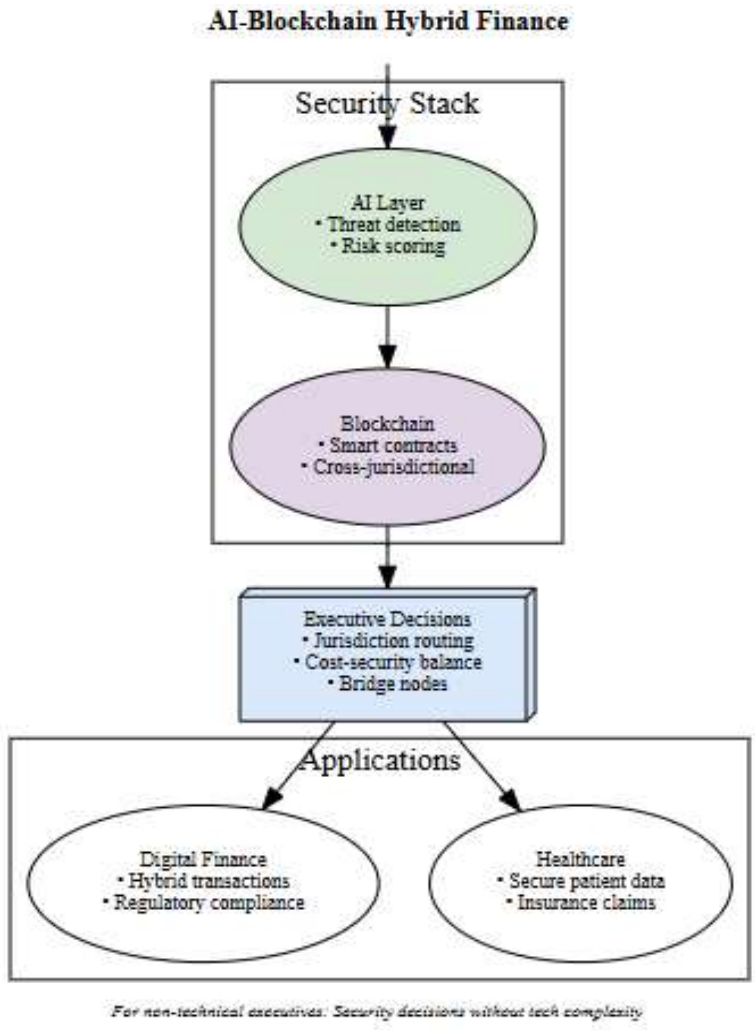

Fig 1 : AI-Blockchain Hybrid Finance

Non-technical executives and senior managers are the main target of the study, as financial decision-makers for the services designed to benefit from the results.

The location-based permissionless and trusted permissioned financial agreements are included in the study based on threat levels. Leaders can use the study as a map of opportunities and dangers to make strategic business delivery decisions. For example, decision-makers can use this information to determine where the security weaknesses are to delegate to a public bridge node on a particular international transaction to save transaction costs. If a promise exceeds a certain percentage, its fiat leg may be over a foreign blockchain built in a threat-poor territory with little public information in the country. The business person can decide to send a trusted country bridge node's payment command or gateway to a country with better regulation and more secure legal recourse to send a traditionally regulated communicable fiat payment to avoid failures and complications. Respondents can thus process many decisions on the security of the executed system and can be left independent by the smart contracts over dissimilar financial agreements as

a reflection of the surrounding sense of security. Executives can study their requirements without diverting into technical specifications.

1.2. Significance and Objectives of the Research

Let's start with the backdrop: As the global business moves towards a digital economy, businesses increasingly rely on breakthrough technologies to support secure, transparent, and intelligent financial transactions. Of the many technologies that address the challenge, two stand out and dominate the discourse: artificial intelligence and blockchain. In contrast to their diversified impacts on other industrial sectors, their applications remain rare to be incepted and developed into a complete form in the financial and banking sectors. However, studies and enterprises strongly support the relations that can be harnessed by exploiting artificial intelligence and blockchain within the context of financial transactions.

The specific objectives of reported architecture research are twofold: On the one hand, the paper seeks synergies to uncover unappreciated and unattributed potential relations of two leading and independent technologies in general, particularly within the financial transaction domain. In demonstrating the potentialities within the digital supply chain finance domain, the research looks into streamlining transaction processes, adding complex capabilities to enhance security and intelligent capabilities, and encompassing partner-specific transactional conditions. Furthermore, the research will divide the architectural components into specialized models to design the artificial intelligence and blockchain-assisted digital supply chain finance process.

The research will reveal the unique 'journey' by adopting six research models and utilizing them to uncover functional building blocks to enhance specific focus functional frameworks. Subsequently, it will allow discussions to identify contemporary and future development scope. Furthermore, it will touch on pattern mechanisms to create blueprints to replicate similar future solutions. More importantly, each of the six research models will uncover alternative approaches, which provide value points to engage with stakeholders. Some of the architecture design use case examples will be based on field data, knowledge, and the combined global experience.

2. Contextual Framework

The infiltration of artificial intelligence, machine learning, and blockchain into core computer science, IT consulting, financial, and regulatory architectures effectively abstracts but presents viable intelligent engines for the following computer science challenges: cloud-based intelligence, cloud-based business process innovation, and cloud security. These significant constructs are appropriately contextualized on the well-documented extensive, diverse, scalable, and successful international experience in cloud computing: cloud stakeholder-driven and operational constructs are well documented. Cloud economics among customers, cloud service consumers, and cloud service providers are all well in place. The recent security and business service descriptions, taxonomies, and cloud business models are essential ingredients for a better understanding of the invasive nature of the above-mentioned intelligent solutions for financial transactions.

The extraction of AI and blockchain-connected architectural solutions for financial transactions deserves critical attention for the following reasons. On the computational front, both of these pioneering technologies are based on the state of the art in computing infrastructure and mathematical/regulatory innovations. In distinct ways, they: a) provide financial transaction solutions at the ends of the financial transaction spectrum (near-immediate all-on-all and all-to-all financial proximity and non-privacy demanded target trading), b) demand distinctive data, process

control, and performance requirements. AI and blockchain-connected proposed solutions also confront other challenges in making verifiable actions secure in computer science domains. Since the mid-1980s, distributed computing scientists have defined intrusion-tolerant actions as verifiable actions such that a misbehaving process cannot present credible proof of action compliance in a published message without actually performing the actions demanded of the service.

Equation 1 : Blockchain-Based Transaction Verification

$$H_{\text{block}} = H_{\text{prev}} + \text{Hash}(T_1, T_2, ..., T_n)$$

H_{block} = Current block hash,
H_{prev} = Previous block hash,
T_i = Transactions in the block.

2.1. Examination of Traditional Financial Systems

Traditional banking finance systems and banks have existed for decades. Banks connect people by accepting deposits from customers and issuing loans to other parties. These depositors and borrowers would likely never meet, but the banks create working capital for businesses and provide houses for homebuyers. As important as it was during the institution's beginnings, the banking industry is still an essential part of the economy through extended services such as safeguarding, lending, and clearing checks and wire transfers. However, financial intermediaries present high expenses and security problems, including a complex redemption process from different parties for products with a significant percentage of fees and intermediaries.

The banking industry continues to face numerous significant problems that challenge the status quo. These problems include high costs, especially for remittance where fees range around 10%; overregulation with a substantial increase in complexity, recordkeeping, and reporting for banks by respective governmental institutions enforcing their powers through loosely tailored commandments; and limited accessibility as thousands of communities across the globe remain unbanked. Banking systems require investment in physical infrastructure and are relatively robust. Banks are fixed points with high operating costs but can shift millions of transactions, making this model suitable for densely populated urban areas. However, the fixed model is less well suited for under-resourced rural areas where the general public is structured in decentralized networks known as communities. Banks typically avoid these less economically prosperous parts of the world.

2.2. Foundations of Cloud Computing

Cloud computing represents a new deployment and delivery paradigm for IT-based capabilities that dynamically change the nature, cost, and diversity of how technology and business workloads are fulfilled. The workloads range from simple web applications to complex business processes and increasingly rely on combinations of services offered by multiple providers. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provided and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three deployment models, and four service models.

The definition of cloud computing characterizes a service as providing on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. On-demand self-service implies that consumers can unilaterally provision computing capabilities, such as server time and network storage, as needed, without requiring human interaction with each service provider. Broad network access means that capabilities are available over the network and can be

accessed using diverse platforms. The service automates the necessary resources. There are no directly allocated resources to a single user. Rapid elasticity implies that capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly and flexibly. Finally, it is very straightforward to pay only for actual use, enabling capabilities to be monitored, controlled and reported.

2.3. Fundamentals of Artificial Intelligence

Artificial Intelligence (AI) has been researched and developed for more than half a century. Emerging new technologies have brought AI to the brink of revolution for broad industrial applications, scientific research, and social life. To capture the value of AI, access to a fraction of the outer boundary results in cutting-edge research or products, and investment in a deep, rigorous, and state-of-the-art knowledge ensemble of basic ideas is essential. This requires a clear conceptual model that is widely accepted by the public, as this facilitates third-party services, reduces entry barriers, and allows for an efficient distributed workforce in knowledge computing. This chapter focuses on delivering fundamental concepts for AI, rational motivational analysis, category wikis, and strategic and immediate business intelligence for commercialization, as a means to prepare our readers interested in financial technologies to take advantage of the following chapters.

AI aims to create computers or machines that can accomplish and solve typically cognitive tasks that require various types of intelligence when operating with humans. Intelligence perceives its environment and takes action to accomplish its goals. Machine intelligence is based on intelligent agents that receive input from the environment, process the input using reasoning, learning, and acting under uncertainty, and then output external actions as the result of their dynamic models and interactions with the environment. By slightly modifying the exploited methodologies and frameworks, AI research and technology focus on different perspectives of the solutions, including simulating mental processes, developing human intelligence, rational thinking, or rational agents, and automating the performance of intricate physical tasks.

2.4. An Overview of Blockchain Technology

A blockchain consists of a ledger that provides a verifiable and immutable history of transactions. It is based on a sequence of records, known as blocks, that are simultaneously linked and secured using the hash of the previous block and are extended by the next block. Today, a diverse range of blockchain platforms has been developed since the original concept of distributed ledger technology was proposed. However, similar design approaches are implemented in the majority of these types of blockchains. In the design of such platforms, blockchain builders apply two architectural patterns frequently used in distributed systems. One is distributed systems themselves, and another is cryptographic algorithms used to implement simplified security solutions. Hence, a blockchain is a chain of blocks of transactions distributed globally to a large group of computers, maintaining a consensus record of transactions accepted globally.

A blockchain is a chain of blocks of transactions with security mechanisms, making it tamper-evident and almost tamper-proof. In particular, a blockchain is a type of distributed ledger containing transactions, with the append-only property and immutability enforced. The key property of a blockchain is that it embodies a system where multiple parties who do not trust each other agree on the information without the need for a central administrator. In addition, participants can replicate the consensus-verified information with ease. The validation and verification across all the parties in the system, therefore, maintain the integrity of the data. Consequently, a

blockchain is public and accessible to all individuals who participate within the system. However, to enforce meaningful consensus, information maintained in a blockchain is secure unless a consensus is reached. Hence, a blockchain can be controlled by the entire community of relevant users and stakeholders who work together to maintain the accuracy and trustworthiness of information and transactions contained within the blockchain.

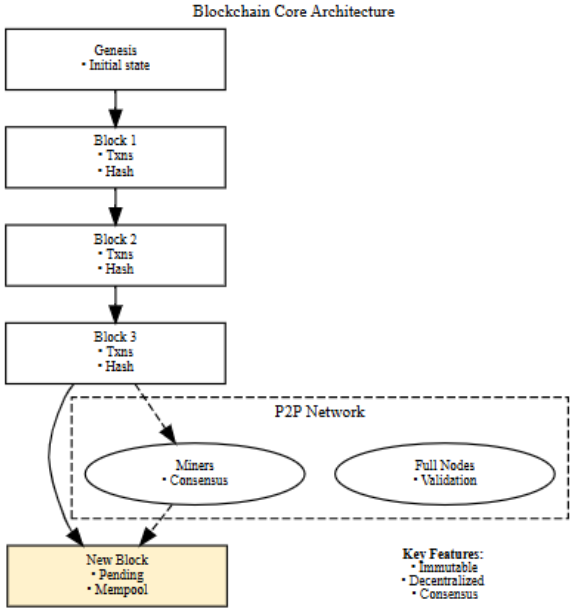

Fig 2 : Blockchain Core Architecture

3. Challenges in Current Financial Transactions

The rapidly changing digital commerce and user experience present a significant challenge to data security. Large-scale adoption of AI has proven to be increasingly beneficial for companies and consumers that leverage financial and commercial blockchain transactions, especially when deployed on top of modern distributed cloud-based systems. This paper devised an innovative cloud-based AI and blockchain solution to enhance blockchain security and financial transaction intelligence through a novel multi-layered framework merging architecture properties and deduplication with machine learning.

The recent wave of AI techniques, particularly with deep learning, has proven to be increasingly beneficial for companies and consumers. When deployed on top of the financial and blockchain transaction system, these AI algorithms perform critical tasks. With the advent of distributed cloud solutions, we argue that it is necessary to create a multi-layer AI architecture blockchain model to effectively co-innovate and co-engineer on top of flexible and scalable financial transaction systems that minimize harmful economic gap situations by increasing investment and insurance.

3.1. Security Vulnerabilities

In blockchain and DLT, multiple critical vulnerabilities exist. The likelihood of occurrence and consequences of such vulnerabilities can be catastrophic. In general, security vulnerabilities can be classified into four categories. Innovations in technology, products, and services often miss addressing some of these distributions in cybersecurity. Scarcity or misdistribution of specific training of the existing labor force and the absence of skilled cyber investigators often expose such vulnerable advancements. Cyber forensics and incident response require rapid reactions performed

by skilled cyber professionals with prevention, protection, detection, and response capabilities in a cybersecurity framework.

Another critical vulnerability is the human factor that can activate a chain reaction among the currently vulnerable utilities by failing to adhere to defined operating protocols and cybersecurity standards. Computers should record every action and keystroke and are thus subject to management policies and procedures. Risk management of cybersecurity cryptocurrency transactions and their legality of use should incorporate risk maturity and business requirements within the business organization, security architecture, and user-level investment. Regulators should work closely with businesses on a more comprehensive regulatory framework to address current vulnerabilities such as gaps in the standard regulation of DLT money transfers in various jurisdictions.

3.2. Inefficiencies in Transaction Processing

Firms and individual end-users regularly execute financial transactions with financial institutions. These transactions are rapidly processed at various stages and by a multitude of intermediary software applications from the initiation of the transactions through the execution of the transactions, the settlement of the transactions, and the final confirmations of the completed transactions. This transaction processing, involving so many intermediaries, has generally been inefficient, with the operational need for data transfer between these parties acting as a bottleneck on system processing efficiency.

Efficiencies in data processing rates can thus matter for many of these transactions, with potential financial implications for entities with a processing involvement in transactions and/or with legal ownership or stewardship of financially significant transaction-related data, who might then seek system transactions in which they can lead, guarantee, or otherwise determine transaction processing throughput and data security. In response to some of these challenges, including an inconsistent record of transaction-related data consent, we generally propose a policy solution based on historical precedents. First, transaction participants can choose a higher-priority or a zero-priority blockchain infrastructure for their transactions, achieving the greatest possible data processing rate and response time, even if their processing request is for a transaction phenotype that is not a preexisting blockchain or is removed from the relevant ledger or blockchain.

We named our mediation processing improvement "off-chain mediation." Second, and in line with the timeless legal suggestion, the efficient throughput and data handling that mediation provides for traditional sensitive financial transactions will also apply to the exclusion of blockchain-preserving classic financial transactions executed in parallel on the relevant systems. We have denominated this "off-ledger mediation." Through this priority facilitation mechanism, mediated or higher priority transaction partners with larger margins for getting there first will be able to have in the future not only their traditional business operations but also their financial throughput smoothed or straightened by defining the quid pro quo data processing transactions that they will be able to perform in the overall system or prevailing infrastructures, as well as in parallel, and conveying the information in a business sign language already familiar to most of them. Data submitters will thus have the material ability and the actual means to commit their data processing requests in direct proportion to their elapsed time urgency without legal constraint, even if the data that needs to be ordered marks a unique message versus timestamped inventory net inventory loss treatment similar to the data organization of most traditional financial transactions. Data stair-step conveyance will also enable market forces to respond to other data-related and system-related forces of constraint.

3.3. Regulatory Compliance Issues

Regulatory compliance is treated differently from security. While various statutes and regulations are, to varying degrees, taken into account in the security section, regulatory compliance, particularly in the context of legally binding principles to support high-value financial transactions, is now addressed.

To be a leader in the provision of secure and intelligent support for high-value, low-volume financial transactions, cloud-based AI and blockchain solutions must comply with multiple laws and guidelines, always bearing in mind local financial services jurisdiction-sensitive enactment. The key areas are the use of private, rather than public blockchains, strong control for the right to view, validate, anchor, and persuade others of the record, judgment execution facilitation stimulating the prevention and mitigation of disputes, and development of common elements to codify financial legal practice and, perhaps, inspire law reform. These areas are elaborated in the following seven sub-clauses.

Strict privacy legislation, when applied to personal information, overlaps with regulatory compliance. It is very significant that, in study after study, it has been reported that privacy is the number one obstacle to accepting blockchain technology in applications touching on individuals. Previously touched-on subjects may be regulatory compliance; enforcement of judgments as to what records fulfill the role of credible evidence and authentic evidence or are registered documents and who, if anyone, may view those records; and innovation of the financial sector to codify and automate law and to promote legal reform. The emphasis is on blockchain's development and deployment in practice, with a strong focus on regulatory compliance in the high-value, low-volume financial services context.

4. The Role of AI in Financial Transactions

The recent progress in artificial intelligence has created a fresh opportunity to tackle the difficult problem of how to ensure that a customer is who he or she claims to be in online or real-world transactions. For decades, the finance community has implemented various types of information-based solutions to address the need for strong authentication. None of these offered a convenient, uncompromising, and trusted method of ensuring that bonds were enforceable. One of the reasons for the lack of popularity of these information-based solutions was that they attempted to define who a person is, not to measure who a person is. By definition, names, personal identification numbers, and addresses can be shared with others. As a result, they can be lost, stolen, or fraudulently obtained.

Neural networks are useful not only for account opening but for many applications where the user is not willing to reveal the pattern required for classification. In all such cases, we can outsource the pattern search to a trained neural network. Blockchain can then be used to create an immutable ledger that captures evidence of the neural network's process. The platform introduced in this paper is such a holistic product that uses neural networks for pattern recognition and blockchain for evidence preservation. We show with a case study that this platform can be productively harnessed to significantly reduce the cost of bank account opening while ensuring adequate levels of security.

4.1. Fraud Detection and Prevention

It is challenging for financial institutions to comply with anti-financial crimes (AFC) regulations that require them to detect and prevent fraud-related activities. To ease this process, we have implemented a basic hybrid blockchain with the following qualities: - A self-distributed property that enhances access to files and variations based on hash values - A Proof-of-Work algorithm to enhance data transfer rates and log management - Scalability and efficiency in terms of managing numerous transaction operations while handling heavy loads of transactional data. In this paper, we introduce a layered blockchain model that focuses on the consensus algorithm, ledger, and smart contracts that are needed to build big system solutions. A novel Proof-of-Work algorithm is evaluated as a part of the paper's contribution. It generates and proposes a commercial blockchain model through the implementation of intelligent APIs. Our implementations significantly outperform other existing blockchain testing scenarios.

Digital transformation of the financial industry is a complex task as it requires a shift from legacy systems to more modern, fully functional, and secure systems. The introduction of new key technologies, i.e., cloud, big data, AI, or blockchain, is key to helping with this transition and transformation. In this paper, we present blockchain solutions that are specifically designed for securing cross-border or domestic financial transactions. Furthermore, to avoid criminal activities, which have grown since the COVID-19 pandemic, we create and integrate AI-building groups. We have experimentally proven that the foundations we propose and the customization of our blockchain for cross-border financial transactions are all robust, efficient, and secure. Our blockchain-based AI and smart processes enhance the security mechanisms and reduce the computational power, costs, and time required for financial organizations to conduct their identity checks for real-time financial clearance.

4.2. Predictive Analytics for Risk Management

Predictive analytics and risk modeling can be applied as pragmatic tools for uncovering risk factors in investment decision-making processes, identifying future investment prospects, and monitoring risk exposure levels. With these tools, companies and organizations can predict, plan for, collaborate on, and assess potential profitability and loss, and develop risk strategies to mitigate possible severe outcomes. In finance, predictive models demonstrate improved robustness in incorporating new information and handling cases with different nonlinear patterns or extreme value distributions and variations. The deep learning of big financial data, combined with a natural language processing model, can promote sentiment analysis for measuring and understanding the mood of investors and the possible impacts of different investor perceptions on investment decision-making. Visualization, representation, and classification analysis of keyword changes reveal the relationship between news sentiment and arbitrage behavior. Technical trading and news data patterns are effectively discovered, and estimated models are established for making a profitable strategy. The news content evolution is visualized, providing real-time updates of live news reports. To escape from the curse of longer-term event-driven predictions, smoothing mechanisms are effectively applied, leveraging smoothed signals, adjusting coverage, or merging probability distribution information for arbitrage decision-making. Text mining of detailed structured reports is performed to facilitate knowledgeable decisions such as companies' earnings and credit evaluation, with multiple learning-based feature selection methods being deployed and a visualized survey identification enhancing cross-sector business applications.

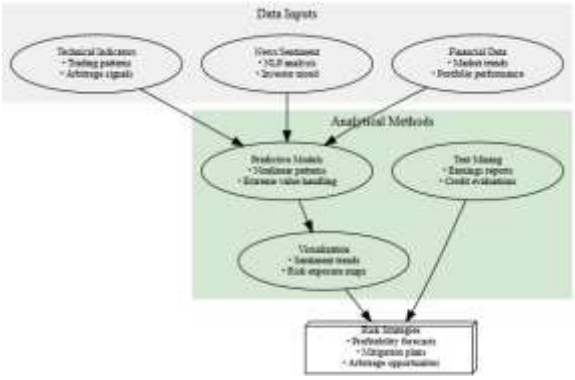

Fig 3 : Predictive Risk Analytics Framework

Equation 2 : AI-Driven Fraud Detection in Financial Transactions

$$F_{\text{risk}} = P(T_{\text{flagged}}|X) = \frac{P(X|T_{\text{flagged}})P(T_{\text{flagged}})}{P(X)}$$

F_{risk} = Fraud probability score,
X = Transaction data features,
$P(T_{\text{flagged}})$ = Prior probability of fraudulent transactions,
$P(X|T_{\text{flagged}})$ = Likelihood of observed features given fraud,
$P(X)$ = Total probability of transaction features.

4.3. Customer Service Automation

AI and blockchain applications for financial institutions extend beyond back-office operations, with customer service automation being some of the most innovative. Utilizing AI, organizations can benefit from recommendations, automatic ticket classification, and customer interaction analytics to improve engagement, action, query management, and operational monitoring. Our assistant solution offers a virtual agent who uses natural language to interact via chat with users, thereby understanding the user's intent and offering the most relevant responses, reducing customer support hotlines, more effectively managing employee resources, and improving patient satisfaction. Enhanced with AI, virtual agents not only offer exact answers, but they can also identify and resolve problems through conversation with users.

Coincidentally, virtual agents developed with AI can also handle over 30,000 requests daily, as well as 1.5 million customer talk-time minutes per month, to alleviate maintenance and operations pressure. Additionally, virtual agents can aid with multi-purpose business performance and automated services, information distribution, and consulting business. As AI technology makes checking account information, fund remittances, and credit card cash services automatic, the next step for customer service operations in banking is to build more complicated networks and layers of services, functions, and processes that are increasingly automated and intelligent. Technologies like Dialogflow are examples of infrastructure that would support this next step.

5. The Role of Blockchain in Financial Transactions

Blockchain and associated technologies, such as distributed consensus protocols, smart contracts, and decentralized domain name services, are poised to help meet these challenges. Although the blockchain revolution began with the introduction of a cryptocurrency that removed the need for a financial intermediary and thus allows peer-to-peer transactions, many industries are exploring how the underlying blockchain technology could help enable business transactions without the need for intermediaries. In this work, we will explore the utility of blockchain to support financial

transactions in banking. There are two dimensions to banking activities: firstly, traditional services that process transactions such as deposits, withdrawals, and fund transfers; and secondly, maintaining personal and account balance information that is relevant for taxation and financial reporting purposes.

Typically, in traditional banking, financial institutions like credit unions or commercial banks operate as intermediaries, allowing financial transactions to occur between individuals. This eliminates the need for two parties to directly trust each other and lowers fraud. However, banks that provide these services charge a fee for infrastructure as well as the risk that services may go unmet, and they often achieve significant financial gains from providing these services. Blockchain has the potential to radically transform the financial industry, enabling financial transactions to become peer-to-peer. We aim to discuss the role of blockchain in supporting secure and intelligent financial transactions.

5.1. Decentralization and Transparency

Are decentralized solutions the Holy Grail that will allow each user to check the process from end to end and verify its integrity, or are they just utopic attempts with little impact on the real world? Decentralization benefits mainly from having no central authority as well as trusted third parties in the process. Authentic users do not want to see decisions made on their behalf; they want to be part of the decision-making process. If such decentralization is converted into governance using well-known consensus algorithms, often inherent in blockchain, a large part of the work of court experts, notaries, valuators, loan signature panels, and so on must be conducted differently. These professionals are replaced by specialized open algorithms or similar technologies, making processing decisions far easier for all participants. Innovative decentralized cloud-based AI and blockchain solutions, in combination with LAN and WAN state proxy processing, result in a large part of the existing work being done differently.

The benefit of presenting the decentralized network of voters systematically undermines the cost and added value of trustworthy third-party services at the same time. Decentralized securing of public and private data, cryptography standards, and algorithms have become the norm in a hyper-connected modern foundational layer for machine-to-machine communication both inside and outside the data center. The latter algorithm dramatically improves this foundation by transforming much of the work of the public register in the company's network. This hands-on practice, built from a pilot and now in production, reveals that even when this degree of trust is guaranteed using a transparent and decentralized governance model, the other inherently subjective value of organizational stability and cooperation between the involved parties remains.

5.2. Smart Contracts in Finance

Smart contracts are computer programs that can automatically execute the terms of a contract. They run upon the occurrence of an event, and once certain conditions have been fulfilled, it is guaranteed that the results of such execution cannot be repudiated without the signature of relevant parties. We show how complex financial contracts can be implemented as a set of confirmations. We provide a framework in which to assess whether a contract should use smart contract technology. To illustrate how our framework can be applied, we present several examples in the financial markets, including a streaming quote system, debt contracts with covenants, and chatroom systems. Our analysis of complexity reveals the practical limits of current smart contract technology.

A smart contract integrates a protocol with user interfaces such that rules and restrictions on transaction acceptance are recognized, understood, and enforced. Smart contracts aim to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting. They can be executed in internationally dispersed locations at a low cost. Current smart contract technologies have limited potential to replace or enhance the execution of contracts involving a high degree of discretion on the part of human agents. This encompasses many of the contracts in complex financial transactions, such as complex structured products, financial institutions, and large corporations.

5.3. Cross-Border Transactions

Cross-Border Transactions. To carry out transactions across countries, a business entity in one country typically establishes a branch, subsidiary, or bank account in the other country and executes business transactions between the two entities. Transaction settlement includes the exchange of the transaction amount and the remittance of service fees. The transaction is reflected, monitored, and audited through the financial statements of the two entities. Foreign exchange risk arises when the transaction is executed with a unit of measurement different from the transacting currency. The transaction amount has the possibility of appreciation or depreciation during the period between the time at which the exchange rate is determined and the time when the amount is paid or received. Management faces the risk of the financial statements transaction amount being misread by the stakeholders who use a functional currency different from the transaction's measurement unit. Transfer pricing helps to set the intracompany transfer price and the intercompany transaction amount.

The legal and regulatory environment, blanked for anti-money laundering, intensifies the management's duty towards protecting financial stability, pursuing the transaction's beneficial ownership, avoiding and investigating balance sheet types of exposure, and creating asset loss provisions. The corporate tax rate difference between the business entity's country and the country where the transaction is carried out should be integrated into the firm's tax planning model for decision-making. These costs, along with the benefits, result in the net benefit/cost value of establishing and maintaining the branch or subsidiary. In addition to a forward exchange contract and the use of the money market hedge, recent advancements in cryptocurrency and blockchain technology open the door for a more secure and efficient fund transfer and exchange. The transaction amount and the party's knowing your customer limit the amount. Mime as a service uses blockchain technology to economize the compliance cost that the business entity would have incurred to verify the AML and KYC information. MaaS can give other financial institutions temporary access to the financial institution's verified account user information. The terms and conditions for using the information, the limits of the authorization, and the revenue-sharing system are subject to the cleared cryptocurrency token contract.

6. Architecting Cloud-Based Solutions

Now, let's initiate enterprise implementation by architecting a financial transaction industry-ready solution prototype. In this solution, we focus on securing financial transactions first and give the same focus, whenever possible, to other enterprises in the financial transaction lifecycle when presenting the solution. In the following chapters, we provide a detailed reference solution. The solution is designed for selected functional requirements in either financial transactions or the operation of execution use cases. Part of this cloud-based solution makes the selected domain

techniques and tools that we use in constructing the solution serve a large scale, and as a result, users, even personal users.

For financial transactions, a variety of industries, including banks, asset managers, hedge funds, electronic payment systems operators, retail brokers, equity exchanges, and regulatory surveillance exchanges, serving financial intermediaries depend on the financial transaction lifecycle to generate their sales. Whenever financial intermediaries and their customers execute the business use cases to perform financial transactions, they go through the financial transaction lifecycle. These businesses operating the financial transaction lifecycle sub-processes personally need to either construct themselves, follow the Common Object Model that the standard creates and adopts, or both strategies.

6.1. Design Principles for Cloud Architecture

This section introduces the design principles for developing a cloud-based AI solution, aiming to ensure secure and intelligent financial transactions. The guiding principles described here offer a general framework and a unique design strategy for overcoming implementation challenges in the context of AI. Safety is especially important in the applications of financial technologies, and to overcome inherent duplication risks, the principles offer unique techniques. Security is made implicit by the Safe AI principles. With the main focus on achieving safe AI, the other safe infrastructure principles also help build the necessary environment. In adverse times, security is necessary to ensure that the infrastructure enabling AI work remains efficient to use, and thus efficient to build. The safe AI design principles guide the development and implementation used to build a usable and useful AI infrastructure, enhanced with security concerns.

Overall, the design principles can be expected to apply to systems and infrastructure used universally, across a wide range of applications and domains. Ensuring organizations fulfill mission responsibilities represents an important challenge that the principles focus on. The most critical decision in developing a system, technology investment, or organizational approach involves ensuring safe, secure AI and mission performance support. The failure to account in procurement for the possibility of challenges that may arise in actual operations may underperform mission responsibilities. The safe AI design principles apply universally to ensure automated systems using AI are responsive and flexible in addressing the full range of mission responsibilities. The safe AI design principles espouse a broad range of management practices in mechanical, electrical, and software engineering.

6.2. Scalability and Flexibility

Scalability and flexibility are key considerations in financial systems due to the unpredictable nature of financial markets. The financial markets have various peak periods and low periods. Hence, the financial system must be able to scale on demand whenever it reaches peak periods but also scale down to cater to low-traffic periods. To achieve scalability and flexibility, cloud storage migration and cloud bursting are two practical solutions provided by cloud computing. In cloud storage migration, data is moved from self-owned hardware to the cloud storage provided by cloud computing. This reduces the number of hardware systems, and it is easier to manage data in cloud storage than in several disparate storage systems in a self-owned data center.

Cloud bursting means a company’s applications run in a private cloud or data center, but extra capacity is accessed from a public cloud when the need occurs. Although it is difficult to implement cloud bursting, it is beneficial for companies that do not want to move all their applications to a public cloud. The financial system must be able to operate efficiently during crash

periods; the capability to scale down these applications can take advantage of the financial system. The cloud scaling model developed in the software engineering field is evolving toward a more precise scaling method tailored to various types of software systems. The cloud burst model complements the infrastructure software in effecting scaling capability to realize liberal resource allocation according to the software sensitivity setting. The financial application software's characteristics, such as hardware device sensitivity or object dependency, could be essential to paving the way for effective cloud scaling.

6.3. Integration of AI and Blockchain

In many ways, the DNA of AI and blockchain applications are very different. On the one hand, AI lends itself to open, complete, and collaborative data sharing and use. Blockchain, on the other hand, has a distributed, collaborative, and secure nature. This nature contrasts and leads to the protection of operational and functional information. Despite their differences, the integration of AI and blockchain is advantageous. Blockchain guarantees that the AI-generated output has not been tampered with. Other advantages include privacy preservation, preserving IP rights of AI models, and ensuring transactivity about data. The combination of secure data transactions made possible via blockchain and data processing and AI model execution allows the generation of AI model outputs securely.

Multiple blockchain-based AI model evaluation and execution solutions are currently being proposed. The AI-blockchain consortium relies on BaaS as the infrastructure for enterprise-scale AI applications that can be leveraged. Some AI models need to interact with outside information through real-time spatial information, making these models primarily developed in the form of smart contracts intelligent. Although blockchain-based model execution and real-time interaction have trouble due to scale constraints and the blockchain consensus protocol's limitations, EVM can also compromise incentives to execute AI model providers when using gas. Diffusion is a hybrid of AI off-chain in combination with on-chain public state transfers and coordinated agreement developed. A more scalable and robust off-chain solution through a combination of state channels and supervised learning has been developed. The number of transactions that arise within Ethereum's primary network can be decreased by off-chain interaction within P2P communication. Small amounts of models constructed for individual purposes capturing a single feature within a convolutional neural network have also been seen. This leans towards the cooperation of the consortium. Small-scale collaborative ones lend themselves well to the combination category, where real-time information transaction speed is also crucial for the consortium.

7. Case Studies

Not all blockchain use cases are the same. It is important to start with "why?" In difficult times like these, people want to save and protect their money. It is no surprise that many efforts and companies have entered the space, from traditional large players to small innovative startups, to harness blockchain capabilities and meet the needs of the financial industry. In this chapter, we will focus on two promising blockchain and AI use cases that are controlling financial fraud in the future with our real production capability, respectively.

AI for Blockchain World Wire is an advanced blockchain technology developed, which uses the distributed ledger to create an optimized, faster, lower cost, and more transparent way to clear and settle cross-border payment transactions. Blockchain, together with AI and other cutting-edge big

data technologies, can create massive economic benefits for the whole society. However, blockchain is not a perfect silver bullet that can solve every cybersecurity and privacy problem. Blockchain also has many characteristics that make it an ideal place to host cybersecurity and privacy models, both traditional and contextual. Blockchains store tamper-proof transaction records in chains. On the blockchain, the power consumption and CPU or GPU used are transformed into a reliable method in the presence of the necessity to trust a third party to algebraically prove the consistency of the blockchain's transaction record.

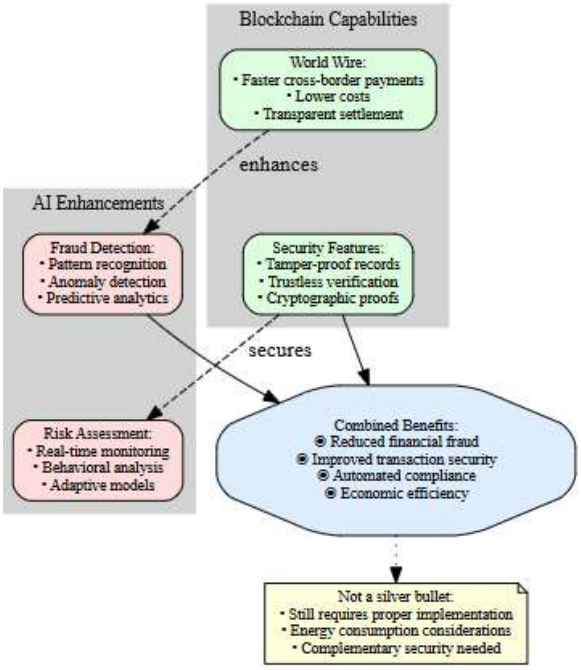

Fig 4 : Blockchain & AI for Financial Fraud Control
Start with "Why?": Protecting Money in Difficult Times

7.1. Successful Implementations of AI in Finance

Only a few truly successful implementations of AI come from financial application areas. Almost all of these applications rely on the power of neural networks to uncover relationships in large amounts of financial data. Artificial neural network techniques have been used to help predict the stock market's short-term movements by using the past values of the stock, trading volume, the risk-free interest rate, and the exchange rate between the local currency and the US dollar as input variables. Neural networks, genetic algorithms, and technical trading were also combined successfully in forecasting the stock market prices of US stand-alone computers. A heteroskedastic two-step probit TARCH model outperforms various other prediction methods, including neural networks, in predicting stock market direction, without regard to financial crises. It has also been shown that artificial neural networks are powerful tools to detect patterns, thereby improving the performance of the tests.

In addition to predicting stock prices, neural networks have been found useful in predicting the creditworthiness ratings of companies. The predictions are based on a logistic regression model, a neural network, and a non-linear discriminant analysis model. Overall, their results suggest that discarding linear assumptions common in traditional models results in better performance. Recent studies encompass methods of reducing the computational demand of trading-oriented neural networks, analysis of technical trading rule profitability with MLPs, comparison of GARCH and

static price volatility forecasting models, and combination of nearest neighbor analysis and cascading MLPs to predict real interest rate changes.

7.2. Blockchain Use Cases in Banking

The backbone of open banking is the use of APIs that help banks easily share financial information with third-party service providers. These service providers then analyze the data and offer enhanced or personalized financial products to consumers. However, the security and privacy of their financial data is a big concern for consumers in this new banking model. Banks need to ensure the privacy and security of consumer banking data and also manage the privacy and security implications that third-party service providers have on the banks and their customers. Blockchain provides the inherent security properties required to meet this need. The decentralized, immutable, time-stamped, and encrypted data capabilities of blockchain can be used to secure: (a) an audit trail of who accessed what data and when; (b) co-mingled financial data that will encrypt the data and user transactions; and (c) a secure method for data analysis while the data remains private and encrypted.

One of the core aspects and promises of open banking is the ability to allow banks to share customer data via application programming interfaces with other third-party companies. These non-bank-regulated third parties aim to deliver financial services to bank customers. Bank customers desire that these third parties will deliver compliant, innovative products and services that simplify and improve consumer experience and that these third parties are managed safely and securely. Banks could explore the prospects of data collaboration to build robust customer data security solutions that are more accurate, efficient, and timely by leveraging customer security attributes and context provided by the collective wisdom of a consortium of users within relevant external ecosystems. Such collaboration would benefit banks by allowing them to contribute meaningfully to, and take advantage of, the collective wisdom of the external ecosystem in combating financial crime with efficient and effective fraud monitoring capabilities.

7.3. Hybrid Models of AI and Blockchain

Hybrid models combine supervised and reinforcement machine learning techniques with blockchain to mitigate consumer vulnerability. While discussing the linkage of AI and blockchain through modeling, there are no particular details on hybrid blockchain models. We propose that a combination of AI in both supervised and reinforcement learning models could have significant structural implications and could potentially offer unintended and illicit assistance to financial services customers. The practical utility of hybrid models is contrasted with general AI, conditional specialization, and local intelligence perspectives, by creating the strongest possible and most specific assistants, who are unlikely to share knowledge regarding how their capabilities operate or can be duplicated, yet are used most effectively from an intelligence augmentation perspective, e.g., proactive business process automation assistance or remediation/incident response to business disruptions.

To assist codependent consumers in the context of secondary markets with more transactional data and unique competitive strategies, hybrid deep learning models such as Stack RNN, in which the top RNN models depend on the output of the stack, are likely to provide greater predictive and explanatory decision support. Other hybrid deep learning models leverage RNN to evaluate individual data elements and apply reinforcement learning strategies such as policy gradients to the output RNN probability predictions. Meta-reinforcement deep learning models could leverage an ensemble of Q-functions to evaluate predictions from any given action, whereas another RNN

represents the output from multiple Q-value combinations. Alternatively, federated learning can leverage blockchain to optimize multiple deep learning models among different organizations without aggregating datasets, thereby minimizing privacy and confidentiality concerns.

8. Security Considerations

An evolving secure and resilient measures framework was created to facilitate the improvement and integration of important security features that IoT and blockchain have in common. In telemetry systems with IoT, it is neither always possible to use timeout nor to authenticate potentially faulty data. Through a combination of secure hardware and state-of-the-art prediction methods, such systems will be guaranteed to generate warnings within a certain amount of time and with provably high reliability. For this purpose, a hybrid approach with limited data usage and blockchain integration has been proposed. To separate data streams into secure/timed and untrustworthy/unspecified data streams, a multi-modal model for driving events and an additional semi-offline learning phase are proposed.

The IoT has recently acquired more and more space, and it is an undisputed part of the future. It has a lot of potential in health, precision agriculture, and many more sectors. The blockchain offers hidden layers of cryptographic security protocols to implement contracts and manage data securely without intermediaries. Both innovative technologies have unusual difficulties, but they can be combined to meet them in the best way and at low costs. However, while most data streams provided by next-generation IoT sensors are secure and might be checked and used by autonomous services for contract execution on a blockchain, such services need external guarantees of secure data streams for proper operation.

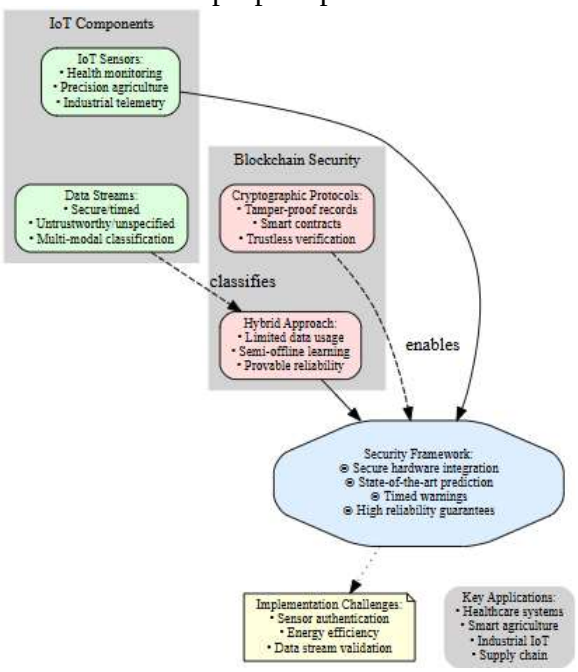

Fig 5 : Secure & Resilient IoT-Blockchain Framework
Hybrid Approach for Trusted Data Streams

8.1. Data Privacy and Protection

Today's regulatory landscape for data privacy and protection is constantly changing and becoming increasingly complex. Virtually all companies operating on a global scale need to deal with such regulations as the General Data Protection Regulation issued by the European Union. This poses significant compliance challenges because AI systems function optimally when they can utilize as much data as possible. Accordingly, this chapter has reviewed several areas in which cloud architectures can be adapted to facilitate more privacy-preserving AI systems. The chapter has addressed such areas as tokenization of private data, which is directly applicable to increasing AI model privacy. In addition, there is individual privacy concerning AI solution predictions, which can be handled through a well-defined API. In all of the explored scenarios, it has become evident that truly private scenario implementations require transaction logs and blockchain to match AI models to actual cloud usage.

8.2. Cybersecurity Threats and Mitigation

Data privacy and security of blockchain, AI, and financial transactions are top concerns of users today. Missteps in the adoption of these disruptive technologies are easily avoidable by architecting security instead of bolting it on. With the adoption of secure engineering principles and practices, the top cybersecurity threats can be mitigated when architecting blockchain systems and cloud-based AI services. In this body of research, it is shown how emerging technologies are providing opportunities to secure and defend financial data using AI, blockchain, and edge computing in a cloud, fog, and mist continuum. The unique features are presented as a compelling guide to those architecting blockchains and cloud-based AI services to securely and intelligently manage financial transactions.

The top cybersecurity threats present before the adoption of a blockchain system continue to be of concern after adoption. Protecting the wallet, establishing secure channels to the blockchain, protecting the smart contract, and protecting the operating environment are an extension of conventional secure operations. The remaining top threats on a blockchain system, those related to cryptography and noneconomic consensus, are not addressed here since proper blockchain design and operation management mitigate threats. Whether the system is operated privately or publicly, both warrant thorough security design in the first place.

8.3. Regulatory Compliance Strategies

This paper extracts and analyzes the regulation models for traditional e-commerce established by various entities and advises based on blockchain technology for the establishment of a new e-commerce regulation model capable of meeting the requirements of the new situation. From the perspectives of the transaction entity, transaction object, transaction content, and transaction characteristics at cryptocurrency trade e-commerce, and on the nature of the decentralization of blockchain technology, it is proposed to establish a transaction service model that combines information exchange with government services closely, to establish an industry self-regulation mode, transaction technology mode, and transaction method mode, and create a diversified transaction policy model to deal with the new situation.

Drawing on the transaction entity, basic transaction module, specific service module, and basic architecture of the financial services transaction system, specific application models for exchange trade, over-the-counter trade, cryptocurrency 2.0, and payment methods are devoted. The system has a decoupling characteristic and possesses the potential for significant practicality. The ultimate goal of the system established is to drive the development of blockchain technology and provide

service for the safe and effective transaction of e-commerce, with the implementation of the new model, along with the completion and improvement of the transaction service ecosystem brought about by the spread of the transaction policy and the introduction of specific regulations.

9. Future Trends in Financial Technology

In conclusion, cloud-based economic models and micro-tasks not only provide real business case studies but also mirror AI and blockchain promises based on decentralized and distributed solutions in a volatile world with minimal long-term contractual obligations. The security of challenge questions for the single-factor-based authentication process in these models demonstrates not only the attack resiliency of our AI and blockchain service but also the resistibility of the global arbitrator chain. Using another successful real-world development, we propose an important research direction for designing the next generation of concept infrastructure solutions. In our future work, we will extend and apply blockchain-based data sharing for various types of systems that will break down the geographical borders of large data governance and enable systems to achieve better intelligence.

This paper addresses the future trends and challenges of financial technology, which benefits consumers and businesses. Here, innovation is based on AI and blockchain solutions and the application of these frontier technologies to financial transactions. AI innovations are driven by predicting user behaviors. To provide forward-looking insights using these financial data innovations, peripheral predictive tasks use a combination of AI and blockchain, sharing data between AI and other AI using blockchain and also between AI and blockchain based on the AI and blockchain cloud architecture. Optimizing and solving challenges involves addressing a growing number of business cases that promote forward data and regulation sharing while charging equations and other blockchain costs to increase simplicity and improve the relevance of the gained knowledge. Optimizing financial flows requires AI-supported automatic actions based on blockchain chain solutions. A key challenge is to prepare AI-based transformed business models for full use of the proposed process changes that take time to explore.

9.1. Emerging Technologies and Innovations

Emerging technologies play significant roles in business digital transformation. They have been increasingly becoming popular within businesses to solve more problems. In the last two decades, artificial intelligence, IoT, and blockchain technologies have been impacting the global economy and business world. Cloud technology has become a powerful tool providing computing resources at a lower cost, with advantages in security, scalability, and elasticity. To develop applications with intelligence, privacy, and security on the cloud, these base technologies contain many challenges. Applications may encounter performance and cost issues in the meantime. In the combination of involved technologies, there are many aspects to consider within the applications. The design strategies of architectures and technologies must evolve through a continuous process. Such applications in the business world need a high level of automation to allow users to run all their AI workloads easily and flexibly. Business financial management is a common function; we will explore how to develop blockchain with cloud in those applications.

Emerging technologies not only play a strategic role in creating businesses' competitive power but also create firms' new business models and value quickly. Small and medium-sized financial firms face a significant challenge in building innovative cloud-based financial technologies, especially merging artificial intelligence, secured blockchain, and analytic workload capabilities. Two case

studies are chosen for analysis and discussion. The examination will focus on how SMEs built cloud-based modern financial workflows, solutions, and services. It then evaluates how the cloud-enabled seamless big data transaction analytics provides the best tool support for those workloads needed. To help ensure good management or governance, the solution must provide strong security. Finally, the quantitative review is used to demonstrate that the solutions have competitive performance compared to previous solutions.

9.2. The Impact of Quantum Computing

Some of the general-purpose quantum computing applications include solving problems in quantum physics, simulating complex molecules, performing complex mathematical calculations, and simulating multifactor optimization. If a fast, general-purpose quantum computer were to be developed, some of the most common classical cryptographic functions would be vulnerable, making the Internet insecure regardless of the classical encryption lengths in use: all encrypted web traffic, online encrypted communication, encrypted systems, encrypted backups, encrypted documents, encrypted smart appliances and vehicles, and a safe workplace environment.

With quantum computing, adversarial cryptanalysis becomes a real-time intrusion of encryption systems. Whether hack, cipher, or snoop, the process of adversarial analysis remains costly and requires a huge power consumption; that is, adversary interference on surfaces may require substantial capital investment. An adversary attack could be detected by monitoring intrusion sites' use of power or through wireless interception. Once intrusion sites are detected, the adversary power can be removed to restore security. As such, it would become impossible to ensure any kind of online cybersecurity during a value network communication with financial flow between different parties generating electronic data finds, and when sending and receiving financial data outside of a protected environment, real-time data integrity and confidentiality are required for secure financial transactions.

Equation 3 : AI-Optimized Payment Settlement Time $T_{\text{settle}} = \frac{S}{R + C}$

T_{settle} = Estimated settlement time,

S = Transaction size,

R = Network processing rate,

C = Blockchain consensus delay.

9.3. Sustainability in Financial Technology

Financial enterprises seeking to be more sustainable often consider the lifecycle of their own and their customers' financial products, or how their actions have an impact on the environment as well as the balance sheet and bottom line. We also focus on sustainable technology, recognizing the need to develop scalable, reusable, and secure technology solutions. However, when financial technology providers exclusively concentrate on delivering efficient computational speed, scalability, stability, and security through centralized activities, they inadvertently provide only temporary solutions to complex problems. Many enterprises see these massive costs as energy inefficiencies. Users of public blockchain technology also have growing concerns about exorbitant electricity usage, the need for both water- and air-cooling buildings that are popping up in various locations, and the growing demand for importing impoverished, disenfranchised communities of skilled workers globally.

A key requirement for sustainability is to define adequate infrastructure and flexible governance models for decentralized solutions rather than centralized systems to serve as the backbone of sustainable fintech solutions. Indeed, the successful deployment of decentralized blockchain protocols combined with the responsible propagation of modern software, cloud, machine learning, and AI methods, make financial systems secure from security risks, easily explainable, more efficient to operate, and truly intelligent to match demands across the dynamic social and economic scale of the world's universal super-interest rate, is a grand sustainability challenge that transcends traditional data center and financial technology industry silo solutions.

10. Conclusion

This chapter is intended to provide an overview of the potential areas where the application of both artificial intelligence and blockchain as emerging technologies can address the challenges of the current financial industry and pave the way for a more secure and intelligent financial future. We also suggested and briefly portrayed future cloud-based scenarios that include cloud storage services, cloud cognitive analytics services, and cloud blockchain services. Then we discussed the current best practices of these cloud services and illustrated some criticisms for improvements. Of the four scenarios, innovation represents new ways of securing and automating finance and is expected to be the next singular period. These scenarios resonate with the actual growth in demand for cloud and with the increased demand for AI and blockchain, reinforcing the trust in the VSM as a prediction for future technology development. Moreover, as case companies in financial industries intend to migrate legacy applications to the cloud and are moving into iterative creative functional solutions, we are confident that the path illustrated in this chapter will lead to successful, increased business value while demonstrating the key role of research activities in bringing new cloud-based innovative solutions.

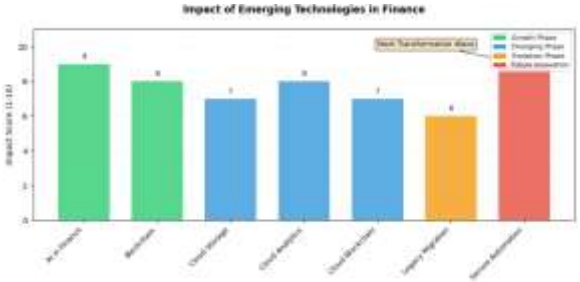

Fig 6 : Impact of Emerging Technologies in Finance

10.1. Summary and Key Takeaways

This chapter provided a comprehensive review of a series of open issues and challenges in architecting financial systems leveraging AI and blockchain technologies, as well as the design of a process orchestrator based on stateflow patterns to enforce the main design issues. Following the pattern proposed above, two innovative architectural patterns were introduced, addressing the design of a cloud-based solution for secure and efficient transactional financial services based on AI and blockchain. Furthermore, the power of stateflow patterns to orchestrate the proposed architectural patterns successfully was demonstrated. This state-of-the-practice chapter encourages rapid innovation in cloud-based secure and efficient management of financial products and services based on AI and blockchain. The open issues and proposed architectural solutions are intended to support a financial organization that aims to move from legacy to the innovative offerings necessary to assure the success and sustainable outcome of advanced digital financial

services. In conclusion, we have successfully applied two CAD standards to financial transactional cloud-based services leveraging AI and blockchain technologies, as well as the design of a process orchestrator based on stateflow patterns in agreement with the patterns proposed.

11. References

[1] Kalisetty, S., & Ganti, V. K. A. T. (2019). Transforming the Retail Landscape: Srinivas's Vision for Integrating Advanced Technologies in Supply Chain Efficiency and Customer Experience. Online Journal of Materials Science, 1, 1254.

[2] Sikha, V. K. (2020). Ease of Building Omni-Channel Customer Care Services with Cloud-Based Telephony Services & AI. Zenodo. https://doi.org/10.5281/ZENODO.14662553

[3] Siramgari, D., & Korada, L. (2019). Privacy and Anonymity. Zenodo. https://doi.org/10.5281/ZENODO.14567952

[4] Maguluri, K. K., & Ganti, V. K. A. T. (2019). Predictive Analytics in Biologics: Improving Production Outcomes Using Big Data.

[5] Ganesan, P. (2020). PUBLIC CLOUD IN MULTI-CLOUD STRATEGIES INTEGRATION AND MANAGEMENT.

[6] Siramgari, D., & Korada, L. (2019). Privacy and Anonymity. Zenodo. https://doi.org/10.5281/ZENODO.14567952

[7] Polineni, T. N. S., & Ganti, V. K. A. T. (2019). Revolutionizing Patient Care and Digital Infrastructure: Integrating Cloud Computing and Advanced Data Engineering for Industry Innovation. World, 1, 1252.

[8] Somepalli, S. (2019). Navigating the Cloudscape: Tailoring SaaS, IaaS, and PaaS Solutions to Optimize Water, Electricity, and Gas Utility Operations. Zenodo. https://doi.org/10.5281/ZENODO.14933534

[9] Ganesan, P. (2020). Balancing Ethics in AI: Overcoming Bias, Enhancing Transparency, and Ensuring Accountability. North American Journal of Engineering Research, 1(1).

[10] Somepalli, S., & Siramgari, D. (2020). Unveiling the Power of Granular Data: Enhancing Holistic Analysis in Utility Management. Zenodo. https://doi.org/10.5281/ZENODO.14436211

[12] Ganesan, P. (2020). DevOps Automation for Cloud Native Distributed Applications. Journal of Scientific and Engineering Research, 7(2), 342-347.

[13] Vankayalapati, R. K. (2020). AI-Driven Decision Support Systems: The Role Of High-Speed Storage And Cloud Integration In Business Insights. Available at SSRN 5103815.

[14] Ganti, V. K. A. T. (2019). Data Engineering Frameworks for Optimizing Community Health Surveillance Systems. Global Journal of Medical Case Reports, 1, 1255.

[15] Sondinti, K., & Reddy, L. (2019). Data-Driven Innovation in Finance: Crafting Intelligent Solutions for Customer-Centric Service Delivery and Competitive Advantage. Available at SSRN 5111781.

[16] Pandugula, C., & Yasmeen, Z. (2019). A Comprehensive Study of Proactive Cybersecurity Models in Cloud-Driven Retail Technology Architectures. Universal Journal of Computer Sciences and Communications, 1(1), 1253. Retrieved from https://www.scipublications.com/journal/index.php/ujcsc/article/view/1253