Integrating AI with Blockchain for Secure Financial Transactions

By Dr. Felipe Bustamante

Associate Professor of Industrial Engineering, University of Santiago de Chile

1. Introduction

Over the last two years, AI and blockchain have attracted widespread attention, and there is evidence of their being adopted in a wide range of applications. Opposite though they are in terms of centralization, using AI in blockchain technology has emerged as an inevitable trend. As a key piece of the financial services infrastructure, blockchain has the potential to play a key role in supporting the development of AI, and, more importantly, AI can help blockchain become more flexible and expand its functionalities. There are opportunities for utilizing blockchain technology in AI ecosystems, in a drive for openness and fairness, which would be attractive to the full community and reduce the concentration of AI industries in a monopolistic way. Wouldn't it be wonderful if AI could help us secure the key components of a bank-controlled account, and meet the requirements for both privacy and security, while providing convenience just as today's e-wallet and credit card environments do? Since ancient times, the ability to hold one's own money and not have it handled by others is the irreproachable cornerstone for using financial transactions securely. But as time goes by, the emergence of three indisputable requirements: the need to do business, the requirement for anonymity, and the need for a central governing organization for legal supervision and control of currencies has become the driving force for enhancing the convenience of the traditional model.

1.1. Background and Significance

The use of artificial intelligence or AI has grown at an unprecedented speed in recent years. AI is now assisting humans in a great many applications such as medical diagnostics, targeted advertising, and even autonomous control of self-driving cars or unmanned aerial vehicles. However, AI is also being employed for more nefarious purposes, such as malware detection and design, and destabilization of markets through high-frequency trading of securities. Automated trading has emerged as a common use case for AI in the finance sector and combines both legitimate and malicious uses—identifying and exploiting arbitrage

This work is licensed under CC BY-NC-SA 4.0.

opportunities to generate profits. Unfortunately, the secure use of AI to aid in financial trading is hampered by its susceptibility to adversarial attacks.

A potential new way forward to conceive and design secure AI systems is to combine aspects of AI with the principles of a secure cryptographic protocol. Consequently, a secure and decentralized blockchain has emerged as a data-sharing platform for secure financial transactions with small transaction costs. At its heart, a blockchain is a secure, distributed transaction ledger. As a secure and transparent financial infrastructure, blockchain is considered a possible solution for securing future AI-based trading systems. Secure and tamper-proof AIs running over a secure blockchain could establish decentralized and trustless financial exchanges and share trading strategies while ensuring the identities of traders remain anonymous. The goal of this chapter is to envision a secure and private integration of AIs with a blockchain for financial transactions within a secure environment.

1.2. Research Objectives

It is the first research to propose a system that integrates AI with blockchain for secure financial transactions. All the work and challenges need to be discussed in detail before implementing such a system. The blockchain and AI integration process has components such as AI-as-a-Service and blockchain-as-a-Service that need to be designed and integrated. We also estimate the quantum time required as all financial transaction systems are at risk of exposure due to quantum computing. We also propose an integrated BCI based on the needs for currency and security.

Due to the replacement of humans by artificial intelligences and the revolution in blockchain, the security of the whole ecosystem is necessary. A decentralized and secure financial transaction, which is less time-consuming, is required for the latest revolution in Industry 4.0. The existing ecological approach between AI and blockchain, due to the operation of the blockchain service, is centralized and hence prone to modification, tampering, or data loss, which is in turn a point of exposure due to denial-of-service attacks. In addition, Artificial Intelligence-as-a-Service, which will utilize the sufficient resources required to operate the model and encryption key in a secure manner, is absent in advanced intelligent technological devices. Hence, in this thesis work, we propose to integrate AI with blockchain as a foundation for secure financial transactions.

This work is licensed under CC BY-NC-SA 4.0.

2. Foundations of AI and Blockchain

The focus of this chapter is to present a concise survey of the concepts underlying AI and blockchain technologies. Our intention in presenting the foundations is to introduce readers to the fundamental concepts that underlie the technologies. In so doing, we hope to provide a deeper understanding of both AI and blockchain technologies and how they could be used in combination for cloud applications. Furthermore, we want to emphasize the fact that AI is never really combined with blockchain. Rather, the workings of an AI system may be embedded into a blockchain system just as they may be embedded in non-blockchain systems. The foundation of AI should always be seen as an underlying element of all uses of new technologies, and in the case of AI, it has the dramatic capability to disrupt traditional systems of governance and responsibility behind new technologies.

Artificial intelligence (AI) is conceptually old, yet actually fairly new. The idea of a machine that could undertake simple operations had been imagined and, in large part, built by the mid-20th century. Of course, back then, the machines were primarily made of gears and lever arms. The term artificial intelligence was first used in a proposal for a conference at which the field would emerge in 1956. Yet even as the field emerged, it was named and viewed as much as an analogy to human intelligence as it was a definition of machine intelligence. For example, very few machine-based successes of the mid-20th century are considered intelligent today. In fact, when covered in undergraduate AI classes, the 'search dog' is often used to demonstrate that search capability does not necessitate intelligence of any type, much less the artificial kind. Over time, AI practitioners moved away from the idea of human imitation and towards separate concepts or theories of intelligence. Today, AI is often covered as an umbrella term covering computer vision, natural language processing, and machine learning, which ultimately represents a single subfield.

2.1. Understanding AI and Machine Learning

The first computer program built to perform a human function was created by Ada Lovelace, considered the world's first computer programmer, and was designed as a substitution for weaving machines, using Charles Babbage's analytical engine. Artificial Intelligence (AI) and its primarily related field, Machine Learning (ML), are two of the most challenging but rewarding areas of computer science. These fields involve the design and development of

This work is licensed under CC BY-NC-SA 4.0.

algorithms that allow computational systems to perform symbol processing, complex reasoning, and learning tasks that were once considered to be strictly within the domain of those acting under the "natural" intelligence umbrella. AI refers to the science of developing computers to perform tasks that require human intelligence. AI is an attempt to make machines perform better the tasks that humans do. It is an interdisciplinary field, a convergence of computer science, philosophy, psychology, linguistics, operations research, economics, and other disciplines. Machine Learning (ML) is a subfield within the broader field of AI and focuses on the development of algorithms that can learn from and make predictions or decisions based on data. One way to think about ML is to consider it as the process of getting machines to generalize from a large set of examples. There are different ways that ML can occur, including supervised learning, unsupervised learning, and reinforcement learning, among others. Researchers in ML attempt to ensure that ML algorithms learn in an unbiased way that allows systems to make generalizations from new examples that are not just direct copies of examples the systems have learned from. Also, some of the consequences of learning from data towards human biases and prejudices can be curbed using developments in this field.

2.2. Key Concepts of Blockchain Technology

All the transactions in the Bitcoin network are recorded in a public ledger called a blockchain. A blockchain is a distributed ledger that records transactions in an immutable sense; once recorded, it cannot be changed or deleted. In cryptocurrency networks, such as Bitcoin, all transactions are included in the blockchain in a sequential order. A complete and full copy of the blockchain is stored in all of its network nodes. Every new transaction is distributed across the network and, after verification, the transaction is included in a set of several transactions that are then called the block. Once the block is composed, it is broadcast to all network nodes, and each node will add this block to its own blockchain. In summary, a blockchain consists of blocks that contain a set of transactions placed within the block in chronological order. Each block is recognized through a cryptographic hash value of the previous block header. It is determined through a consensus algorithm. Data added to a block is identified through a unique digital signature. Any further modifications to the blockchain are not permitted, as they would require a huge amount of computational resources to restart the consensus process from the start. Each transaction of a blockchain network depends on a cryptocurrency

This work is licensed under CC BY-NC-SA 4.0.

system that serves as a means for value transfer between its peers. These digital currencies rely on a cryptographic system that ensures that the transactions are made with a high level of security and privacy. In the Bitcoin network, for example, users are assigned digital wallets based on the assumption that a specific address can hold users' funds. The privacy and security of this address are ensured through public and private key pairs that form Elliptic Curve Cryptography.

3. Integration of AI and Blockchain in Finance

Integrating AI with Blockchain for Secure Financial Transactions

The concept of state channels has introduced the possibility of integrating AI with a Blockchain to secure transactions. The state channels can potentially facilitate off-chain computations with trust by bringing AI capabilities outside the Blockchain. The potential use of AI in Blockchain finance includes AI-driven smart contracts, bringing off-chain data on-chain securely, AI orchestrated market making, multimodal learning on images and voice data, data generation for machine learning training, technical analysis on price/volume movements, and complex modeling of financial data. This can lead to AI-driven trading, investment, and insurance strategies.

Blockchain can be integrated with Artificial Intelligence (AI) to offer decentralized, secure, transparent, and tamper-evident data-driven predictive modeling services. The combination of AI with a tamper-evident Blockchain can provide a multitude of decentralized services such as financial transactions, equity on-demand, share issuance, employment verification, secure and accountable identity assertion, SSL certificate issuance, notary, certification, and proof of creation/termination. These services can potentially reduce the role of trusted parties in providing, maintaining, and validating these services and make the process more decentralized and efficient. With predictable computational confirmation time and guarantee on tamper-evident data storage, the outcome of the delivered data-driven predictive performance/behavior model can be independently verified by customers for handling misuse, security, privacy, and regulatory concerns.

3.1. Benefits and Challenges

This work is licensed under CC BY-NC-SA 4.0.

There are several reasons why financial transactions are the primary use cases of blockchain. First, the requirement of real-time transactions combined with the location of the middleman results in high financial costs. Second, financial transactions must meet several security and privacy requirements, which are difficult to achieve without mechanisms based on public key cryptography and timestamps. Third, if financial transactions do not solve the so-called double-spending problem, they are not useful. Double-spending occurs regardless of whether it is a physical problem or a digital one. In contrast to regular energy costs that increase the disadvantages of using classic proof-of-work blockchains for these use cases, several artifacts are marginalized by use cases focused mainly on the integration with currently widely used financial systems.

The major benefit of integrating AI and blockchain lies in the fact that the combination of these technologies enables advances in each field. Together, they can form collaborative socio-technical systems that are capable of performing high-level functions that neither could perform alone. In financial transactions, in which we are highly vigilant to attackers, autonomous intelligent decision-makers suitable for premature advanced threats can benefit us now. It can also help us integrate well-documented AI difficulties such as contaminating machine learning.

4. Developing Smart Contracts for Financial Transactions

Contacting smart contracts execution Considering the inconsistent existing guarantees from data suppliers which are responsible for providing data to blockchains, as well as the concern for providing guarantees and especially making the result of smart contracts' computer code protected by the verification of reliable data even from the monetary point of view, there are some characteristics of smart contract code execution that should be analyzed. The smart contract code must be executed. The execution must not be avoided whether it is not an exclusive prerogative of the platform. When it is exclusive, it is distinct from other characteristics because in such a situation a more secondary function of creating or updating smart contract code should not be available since these actions should be accomplished off the platform. For example, because simple code is executing rather than another, even if another code analyzes the situation and decides about the execution next steps. The contract to be executed must be decided by the parties who authored the smart contract code. Determination

This work is licensed under CC BY-NC-SA 4.0.

by parties rather than by secondary consent by producers is essential because there may be blocking, permanent denial, or forgery by producers. If updating is allowed, the date and time locking of the parity of smart contract code to be executed consensus should happen when an instance is initiated as per the smart contract's written conditions. This locking prevents forgery and blocking from creating a favorable condition for arbitration which can occur if, for example, the locking is exclusive to the beneficiary of the code result, which will be managed directly by producers or indirectly by corrupting producers and should benefit from locking at another time. If there are conditions obstructing the execution of all code functions, only the functions incompatible with these conditions should not have their results played back. These are the requirements for the electoral arbitration of Enforce Protocols.

4.1. Definition and Functionality

Integrating AI with Blockchain for Secure Financial Transactions

Widely associated with the rise of digital cryptocurrency, the blockchain is a technology that promises radical change to business models and analytical reasoning and applications. It achieves this through creating a single and widely distributed digital ledger that records and enables the transfer of complex assets. The blockchain enables its users to immutably record, update, and manage the existence and transfer of complex assets online in a rapid and open environment. This has enabled it to become the enabling technology for decentralized digital currencies and alternative digital coins. Initially developed to empower digital currencies, today's blockchain technology has matured significantly over the years, reaching the quality of being a globally universal, immutable, decentralized, transparent, public ledger. It has the capability of storing information about different, complex and interrelated assets in a unique and digitally distributed way.

The blockchain is a technology that is capable of revolutionizing the foundations of transactional activity. By this, it has the potential of shaping not only the future of finance but corporate structures as well. Since its inception and network growth, the blockchain has always been another term for cryptocurrencies that are Bitcoin. It is a well-known and established fact that blockchain accomplishes its single, distributed, immutable, and secure nature through a combination of different and complex technical features that are related to software engineering, cryptography, game theory, economy, and especially to decentralized

This work is licensed under CC BY-NC-SA 4.0.

and distributed computing principles. Addresses on the blockchain network are important, defining transaction sources or transaction recipients.

4.2. Use Cases in Banking

The banking, financial services, and insurance industries have been the forerunners in utilizing technology to streamline business processes. A few specific instances of where they are leveraging blockchain technology and the reasons why they are doing so are explained below.

Cross Border Payments Making payments across the world can involve a number of intermediary banks. The funds may need to be held in trust until the last mile is confirmed to have been delivered. This is the standard operating procedure followed in the widely accepted payment transfer mechanism. The problem with that is that small intermediary banks may not be able to provide such a transaction owing to a lack of funds or feel the need to add an additional security charge on account of the transactional risk. It is not unheard of for transactions to take several days to weeks to be cleared. It is even not unknown to have transactions canceled after the funds have been held in trust that long. Using blockchain to manage this process would automate and simplify the process, reduce costs, and speed up the time taken for the transaction to be completed.

Customer Onboarding and Authorized Agents Currently, the process for a customer to be onboarded is to fill out several application forms with supporting documentation, like passports, etc. These documents are then checked by the bank. In order to speed up the process of the bank being able to check the customer, the bank relies on authorized agents to do this on its behalf, e.g., lawyers who set up trusts or companies. However, the bank is still responsible for these checks, so the bank must continuously educate the authorized agents as to not being lax in their checks or simply take the authorized agents' word for it. This status, if performed using blockchain, would result in an immutable ledger, i.e., that it cannot be altered, thus allowing audits to be performed on the process, replicating events and identifying potential risk.

5. Decentralized Applications (DApps) in Banking

This work is licensed under CC BY-NC-SA 4.0.

Decentralized applications describe the next generation of banking, capital markets, and insurance. Blockchain will revolutionize various markets with its unique features of data integrity, data dependence, and an open and transparent platform. Banks can definitely use DApps to analyze the credit affordability of individuals and grant loans by reaping the benefits of multiple, invariable bank customer source documentation. They can help with international fund transfers. Money is transferred to the blockchain network from one DApp, exchanged through the network, and finally converted to money via another application. In addition, DApps help in micro-financing, supply chain trade financing, and online trading. The penetration of universal banking through small-scale, tailor-made blockchain applications is possible even in rural areas.

The capital market is another area that will be positively affected by blockchain technology through the development and utilization of DApps. Stock trading may be easier and cheaper with fewer intermediary infrastructures; in addition, there would be a reduction in time by connecting the two receiving and sending exchanges in real time. Applications in the capital market include reduced clearance and placement of payment times, automated reporting, increased transaction accuracy, enhanced transparency, and substitution of traditional clearing houses. Such market applications can enforce real-time repos or pre- and post-trade data analysis. A blockchain system allows the completion of a transaction settlement over the weekend. The system is used to process and distribute payments by completing the necessary submissions to the network and accessing the network for transmission on days and during periods when the network is otherwise closed. When an application results in buying and selling transactions over a network interface in real time, hence immediate settlement of transactions affecting liquidity management on an exchange and user level, such settlement is performed.

5.1. Overview and Advantages

AI has potential for predicting future outcomes, understanding images, understanding the stories in a given text, analyzing complex high-dimensional data, and many more. However, the effect of AI has not been evidently seen in blockchain architecture, which is considered secure. We integrate AI into the model to improve its security. The need is also justified by considering the millions of attack surfaces of the state-of-the-art AI models. The model using

This work is licensed under CC BY-NC-SA 4.0.

AI prediction of partial chains and attributes in a block is shown to have better security relative to other models and efforts in this work. The model has been validated using a benchmark dataset. The integration of AI with blockchain has two major advantages. First, a very large number of attribute-sensitive operations of the blockchain will receive extra strong authentication from AI. It is practically very difficult to ensure the data in the block is of the required quality since the data placed in a block can be smart contracts, fintech transactions, or reliable source data for many financial and logistic transactions. The model shows that a large number of such requirements of AI can be clubbed together and represented as a list of items with AI ratings. This rating results in proper cleaning of the data in the attributes, leading to proper quality in the attributes. The AI should be properly trained in the chain to ensure the quality of the transaction attributes. The AI should continue to assess the quality of the attributes of the blockchain to improve security. The second advantage is to use the AI facility for defining the consensus among the smart contracts. The description of the smart contract is an NP-Hard problem. The secure use has added complexity. The AI has to be trained to generate advanced sequential attributes in the chain of a block. It is also an iterative process until all the milestones of the smart contract are identified. The normal sequential stack algorithms can be run in parallel with the execution of the smart contracts. Security is often considered, and an extra token is allocated to those who help in building the consensus towards the smart contract. The AI-based rating correlates the extra security on the consensus to be obtained. Assuming samples are provided for training the AI model, the stability of the consensus obtained from the smart contract results in significant AI confidence.

5.2. Examples of DApps in the Finance Sector

After the crash of the housing market in 2008, the world lost trust in the traditional banking system. Cryptocurrencies captured some hearts as they provided an alternative. However, the increase in cybercrime and cryptocurrency fraud is a growing concern. So, in today's world, stringent controls are necessary. The technology that provided cryptocurrency comes with extra baggage like high storage and computational requirements, and time. DApps are the solution. DApps have brought a revolutionary transition into the tech world. Now, not only can you transfer money instantly, but you can also buy a green card, a plot of land, or sign a legal contract and get it notarized without logging into your bank account. Banking and

This work is licensed under CC BY-NC-SA 4.0.

financial services have come a long way. A few examples that are used in financial services are:

Banking: Loans, payment of mortgages, insurance, fund transfer, etc., without physical supervision.

Private Blockchains: Banks are increasingly resorting to private blockchains to enable faster and cheaper transactions between banks by hosting interbanks on the same network. Banks are also implementing forensics to investigate criminal activities during block generation. Managing customer and company accounts has also become hassle-free.

Storage and Digital Asset Management: DApps can be used to store and transfer money. They can also be used for secure and hassle-free trade in stocks, bonds, derivatives, etc., like the exchanges do.

Cross-Border Payments: Transferring money from one foreign account to another takes a long time and would also be charged a hefty fee using traditional methods. With DApps, this action is completed almost instantly and at lower rates. This can lead to immense global growth of GDP.

Compliance: Legal work, court, and notary services can be done using DApps. Government contracts, legal agreements, real estate transactions, etc., are registered in the blockchain in a secure manner for others to look into. This makes all contractual work public. Abuse of work is minimized, legal bureaucracy is reduced, and unused permissions are set to expire.

6. Future Direction

The secure payments using blockchain with the intervention of AI, decentralized credit manager for crypto loan lending platform, and cryptocurrency traders and trade decisions will be the future extension of our work. The advanced features including face recognition using AI with blockchain on Android mobile payment application will also be suggested. The online merchandiser refund management using longer transaction time of bitcoin as a payment confirmation will be proposed. The collaboration of private sector and government body for sending cryptocurrency allowances in the form equivalent to vouchers which can be

This work is licensed under CC BY-NC-SA 4.0.

paid using bitcoin will also be designed. Integrating secure AI predictive models with the blockchain frameworks is the challenge to be considered in the future work.

7. Conclusion

This paper discusses how blockchain technology could be used to integrate with a series of popularly used machine learning algorithms to build a secure AI prediction or decision-making model for financial services. We propose secure AI-on-blockchain protocols and a prototypical proof of concept. Our proposed protocols not only protect the prediction models but also protect the training data and the model training process. The concept of federated learning is introduced to protect the training data, so that individual user data is never transferred to any party. The model itself is protected by both BE-OPE and the concept of secure enclaves. By directly running the training process on the blockchain, we eliminate the possibility of using timestamp differences for zero-day attacks. As a case study, we focus on the complex decision-making with artificial intelligence and address the critical issue of security. The proposed methods solve the problem with an innovative design and high efficiency. In summary, building a secure AI prediction model requires the privacy of the input data to be protected, the privacy of the model to be protected, and the training process and the model to be performed in an effective way. All our proposed secure AI protocols solve the problems effectively and efficiently. We show the proposed approach can be applied to solve real-world financial service problems. Besides just security, we also consider the efficiency of the system. Therefore, it is one of the next generations of servers to serve the needs of the modern AI-based economy.

Reference:

1. Tamanampudi, Venkata Mohit. "Automating CI/CD Pipelines with Machine Learning Algorithms: Optimizing Build and Deployment Processes in DevOps Ecosystems." *Distributed Learning and Broad Applications in Scientific Research* 5 (2019): 810-849.

This work is licensed under CC BY-NC-SA 4.0.

2. Pasupuleti, Vikram, et al. "Enhancing supply chain agility and sustainability through machine learning: Optimization techniques for logistics and inventory management." Logistics 8.3 (2024): 73.
3. Thota, Shashi, et al. "Federated Learning: Privacy-Preserving Collaborative Machine Learning." Distributed Learning and Broad Applications in Scientific Research 5 (2019): 168-190.
4. J. Singh, “Advancements in AI-Driven Autonomous Robotics: Leveraging Deep Learning for Real-Time Decision Making and Object Recognition”, J. of Artificial Int. Research and App., vol. 3, no. 1, pp. 657–697, Apr. 2023
5. Alluri, Venkat Rama Raju, et al. "Serverless Computing for DevOps: Practical Use Cases and Performance Analysis." Distributed Learning and Broad Applications in Scientific Research 4 (2018): 158-180.
6. Machireddy, Jeshwanth Reddy. "Assessing the Impact of Medicare Broker Commissions on Enrollment Trends and Consumer Costs: A Data-Driven Analysis." *Journal of AI in Healthcare and Medicine* 2.1 (2022): 501-518.
7. S. Chitta, S. Thota, S. Manoj Yellepeddi, A. Kumar Reddy, and A. K. P. Venkata, “Multimodal Deep Learning: Integrating Vision and Language for Real-World Applications”, Asian J. Multi. Res. Rev., vol. 1, no. 2, pp. 262–282, Nov. 2020
8. Ahmad, Tanzeem, et al. "Hybrid Project Management: Combining Agile and Traditional Approaches." Distributed Learning and Broad Applications in Scientific Research 4 (2018): 122-145.
9. Tamanampudi, Venkata Mohit. "CoWPE: Adaptive Context Window Adjustment in LLMs for Complex Input Queries." Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023 5.1 (2024): 438-450.
10. Thota, Shashi, et al. "Few-Shot Learning in Computer Vision: Practical Applications and Techniques." Human-Computer Interaction Perspectives 3.1 (2023): 29-59.

This work is licensed under CC BY-NC-SA 4.0.

11. Tamanampudi, Venkata Mohit. "Leveraging Machine Learning for Dynamic Resource Allocation in DevOps: A Scalable Approach to Managing Microservices Architectures." Journal of Science & Technology 1.1 (2020): 709-748.

12. J. Singh, "Autonomous Vehicle Swarm Robotics: Real-Time Coordination Using AI for Urban Traffic and Fleet Management", Journal of AI-Assisted Scientific Discovery, vol. 3, no. 2, pp. 1–44, Aug. 2023

13. S. Kumari, "Cloud Transformation for Mobile Products: Leveraging AI to Automate Infrastructure Management, Scalability, and Cost Efficiency", J. Computational Intel. & Robotics, vol. 4, no. 1, pp. 130–151, Jan. 2024.

This work is licensed under CC BY-NC-SA 4.0.