2021

Converging artificial intelligence and blockchain technologies for security and risk management in banking

Van Binh Hai Tran
University of Northern Iowa

CONVERGING ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN TECHNOLOGIES FOR SECURITY AND RISK MANAGEMENT IN BANKING

A Thesis Submitted
in Partial Fulfillment
of the Requirements for the Designation
University Honors

Van Binh Hai Tran
University of Northern Iowa

May 2021

This Study by: Van Binh Hai Tran

Entitled: Converging Artificial Intelligence and Blockchain Technologies for Security and Risk Management in Banking

has been approved as meeting the thesis or project requirement for the Designation

University Honors with Distinction or University Honors (select appropriate designation)

________ ____

Date Dr. Arti Mann, Honors Thesis Advisor

________ ____

Date Dr. Jessica Moon, Director, University Honors Program

1. INTRODUCTION

The COVID-19 crisis created a perfect storm for hackers around the world as companies struggle to prepare for their remote workforce and adapt to the new "norms." The finance sector was one of the main targets. In March, financial-related attacks accounted for 52% of all attacks seen across the VMware Carbon Black dataset, which was 'an unprecedented anomaly in [their] data tracking' (Upatham & Treinen, 2020). COVID-19 related attacks grew from fewer than 5,000 cases per week in the beginning of February to more than 200,000 in late April 2020 (Aldasoro et al., 2021, p. 6). Hackers also played on people's fear of the novel coronavirus, resulting in 18 million daily malware and phishing emails related to COVID-19 in April 2020 (Crisanto & Prenio, 2020, p. 2). As companies shifted towards a virtual working environment, hackers tried to take advantage of the expanding technology footprints and attack surface. The remote work environment created other concerns, such as money laundering, new account fraud, identity thief or data leakage. Employees accessed highly sensitive data using less secure home networks, and reduced oversight of the remote workforce creates opportunities for internal fraud.

Furthermore, bad actors exploited the weakened anti-money laundering (AML) process as some financial institutions shifted their focus to other disruptions caused by the pandemic while others are simply just not equipped to verify customers' identities remotely (Crisanto & Prenio, 2020, p. 3). Banks faced numerous ransomware[1] and distributed-denial-of-services attacks (DdoS)[2], both of which were getting increasingly sophisticated and targeted (Imeson, 2020). With the dramatic increase in financial crimes, financial institutions need to catch up with changing technology and deploy new, proactive security measures that can detect and control threats on-demand to protect them against attacks from both external and internal malicious activities.

To combat the increasingly sophisticated frauds and cyberattacks, many companies in the financial sector are looking into integrating blockchain and artificial intelligence (AI) into their security systems. AI and blockchain are gaining more and more interest as their implementation can fundamentally change the structures of businesses and even the governments.

The focus of this thesis is on understanding the potential applications of blockchain and AI technologies in the banking and finance sector for better risk management and cybersecurity. In this thesis, I will do an extensive literature review of research on AI and Blockchain in the top eight information systems journals and some top-rated computer science journals. The intention is to examine the use of blockchain and AI to enhance remote work security and fraud detection in the Banking and Finance sector.

The thesis is organized as follows: the next section will focus on the applications of blockchain, AI, and the integration of the two in the field of banking cybersecurity and risk management. The following sections of the research will examine two of the most popular blockchain frameworks, Hyperledger Fabric and R3 Corda, as well as the use case of Digital Identity Management in banking. The last section concludes the paper with a discussion of limitations and future work.

2. APPLICATIONS OF BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE IN BANKING SECURITY AND RISK MANAGEMENT

1. Artificial Intelligence

While many people think of AI in the context of robots or smartphones' virtual assistants, the applications of this technology go well beyond that. AI is a branch of computer science that studies and develops smart technologies and machines that can think and act like humans. In the beginning, the limited computing resources resulted in high rates of false positives, which leads to hours of labor work wasted on investigating authentic transactions. As computers are a lot faster, cheaper, and stronger today, advanced AI technology made it possible for companies to implement more sophisticated algorithms and make full use of the vast amounts of data they collect. The 1980s saw the emergence of machine learning (ML) technologies, which was a major improvement in the field of AI (Zeadally et al., 2020, p. 23817). ML allows computers to learn and adapt to various conditions using their past experiences, patterns, and knowledge without having pre-defined coding. About a decade ago, deep learning (DL), which uses multiple layers of neural networks to study data was introduced as a method that can discover hidden relationships and therefore generate more accurate results for prediction (Zeadally et al., 2020, p. 23817). DL quickly improves automation, data analytics and becomes the driving force behind products like self-driving cars and digital assistants.

While AI itself is not entirely a new concept, it is becoming more and more prominent in the financial services sector. Nearly 60% of financial services sector respondents in McKinsey's Global AI Survey report that their companies have embedded at least one AI capability (Cam et al., 2019). A PricewaterhouseCooper study shows that around 25% of financial institutions are utilizing machine learning (ML) techniques for fraud detection, AML, and risk management (Biswas, et al., 2020). In their article, Zeadally et al. note that recently there has been an increase in the use of AI in cybersecurity, partly fueled by the large amount of data generated today which requires significant time and resources to analyze (2020, p. 23818). There has been a strong focus on intrusion detection and phishing detection methods in prior research from 2008 to 2018 (Wiafe et al., 2020, p. 146603). Specifically, in the case of network intrusion, ML provides the ability to detect new traffic patterns and anomalies using ensembles, resulting in a much higher rate of accuracies and a lower rate of false positives as well as energy consumptions (Wiafe et al., 2020, p. 146604). Patterns of frauds and cyber-attacks learned from historical data are used to flag suspicious activities and predict future behaviors. AI is also used to automatically test software for known security vulnerabilities, as well as producing malicious inputs to help improve test models (Horowitz, et al., 2018, p. 4). In a case study by Teradata, the fraud detection system of Danske Bank, the largest bank in Denmark, saw a 60% reduction in false positives (innocent transactions are mistakenly flagged as suspicious) and a 50% increase in fraud detection capabilities after implementing deep learning tools (Knowles-Marchione & Kolpek, 2017). At JPMorgan Chase, DL, and other AI techniques are utilized to develop an “early warning” system that detects malware, Trojans, and phishing campaigns (Shroff, 2020). The system claims to be able to identify suspicious behaviors even before phishing emails are sent to employees. JPMorgan Chase also uses DL to compare malicious URLs with known suspicious patterns, looking for jumbled URLs or spelling mistakes (Shroff, 2020).

Furthermore, AI is also extensively applied to fraud detection and AML activities. The current AML system is a combination of human expertise and machine automation. Despite the advancement of AI, these systems are still heavily dependent on human auditors. Han et al. in their paper on AI for AML note that the AI systems in financial systems tend to be simplistic and rule-based, which requires auditors to review all flagged transactions to determine their authenticity (2020, p. 213). The authors propose a complementary framework that utilizes Natural Language Processing (NLP) and DL for entity recognition, entity resolution, relation extraction and sentiment analysis (Han et al., 2020, p. 226-229). This framework introduced social media and other news sources into the AML process to help find evidence and improve the investigation stage that is usually carried out by auditors, both in terms of efficiency and accuracy. In addition to identity verification, AI and automation can help banks keep a close watch on illicit financial threats even when they are not prioritized. This has proven to be crucial for banks especially in crisis situations such as the COVID-19 pandemic where most attention is shifted to transitioning to remote work.

Lastly, AI biometric technology gained a lot of attention from both public and private sectors, especially for security purposes. Biometrics is the process of detecting and recording a person's unique physical and personal traits to verify his or her identity. Facial recognition, voice recognition iris, fingerprint scan, etc. are much more reliable than the normal password security system as distinctive identifiers are used (Bush, 2018). This area of AI is becoming more and more familiar with the public as many technology companies implement facial recognition or fingerprint to their products. Banking mobile applications are also using biometrics to authenticate customers. AI biometrics technology not only enhances security but also provides more convenience to customers as they no longer have to remember or type in their log in credentials as often.

Nevertheless, the Financial Stability Institute warns that the effectiveness of AI techniques, especially those that train on past patterns of behaviors, might be reduced. The disruption brought by COVID-19 has altered the definition of “normal behaviors” of retail and corporate clients **(**Crisanto & Prenio, 2020, p. 7). Also, banks are facing huge monitoring challenges as they have little information on employees’ whereabouts (Caplain & Jacco, 2020). Remote employees’ working schedules also have become much more flexible, and some might be accessing companies’ systems from their own devices at home (Caplain & Jacco, 2020). This makes it more difficult for the AI algorithm to accurately recognize risks as employees can be constantly on the move and check on their everyday tasks while working.

2. Blockchain

In addition to AI, blockchain is another emerging technology that is believed to fundamentally transform the financial industry. While many people think of blockchain as the technology behind Bitcoin, the applications of blockchain are well beyond just cryptocurrency. Blockchain can be understood as a distributed, decentralized, public ledger where the “history of any digital asset is unalterable and transparent through the use of decentralization and cryptographic hashing” (“Blockchain,” n.d.). Every node on the network has a copy of the ledger. The peers validate and group transactions into blocks. Each new block includes a hash (a cryptographic signature) of the previous one, chaining them together, hence the name “blockchain” (Androulaki, et al., 2018, p.1). Blockchain is based on five main categories: Distributed database; Peer-to-peer transmissions; Transparency with Pseudonymity; Irreversible of Records; and Computational Logic **(**Tapscott & Tapscott, 2017**).** The computational logic of blockchain allows users to implement algorithms that automatically trigger the transaction between nodes (users within a blockchain network). This last principle is also the principle of smart contract, which is another element of blockchain that has attracted a lot of research interest.

To better understand the concept of blockchain, Builtin.com compares the technology to Google Doc. A Google Doc is distributed among, instead of copied or transferred to, those who have access to it. Because of this centralized distribution chain, all users can access the document at the same time, and all changes are recorded in real-time, making all modifications completely transparent ("Blockchain," n.d.). While blockchain is much more complicated than Google Doc, the analogy illustrates the critical ideas behind this technology: Digital assets are distributed amongst all users directly without any intermediary; the assets are decentralized, allowing full real-time access, and the transparency of blockchain preserves the integrity of the document and creates the trust ("Blockchain," n.d.).

There are two main types of blockchain: public and permissioned. A public blockchain is open to everyone, and an example of a public blockchain is the platform that runs Bitcoin. Permissioned blockchain is only accessible to a certain number of nodes who have the permission to enter. As a result, this type of blockchain undermines the "decentralization" aspect of the technology. This thesis will focus on analyzing the application of permissioned blockchain as the banking industry handles a lot of sensitive data, such as personal information and account balance, that should not be made public.

Despite blockchain being a fairly new technology, the benefits that it brings are being widely recognized by business leaders around the world. According to a survey conducted by Cognizant - a technology company that specializes in business consulting, information technology and outsourcing services - firms in the financial sector believe improved data management, improved risk management, heightened security, reduced fraud, and improved auditing are among the top benefits of blockchain (Varghese et al., 2017, p. 8). In addition, a study by Taylor et al. shows that the majority of blockchain research on cybersecurity focuses on the Internet of things (IoT) (45%) and Data storage and Sharing (16%) (2020, p. 150). Leaders in the industry are starting to look into blockchain to create a secured environment that can protect them against cyber-attacks and frauds.

Firstly, the implementation of blockchain can help banks control risks much more effectively. All transactions being encrypted, untamperable, time-stamped, and tracked in real-time discourage fraudulent activities. As a result, communications among peers are protected, and the integrity of data is ensured. In addition, audits can be conducted more effectively. Blockchain technology and its transparency element also allow banks to verify the identity of their customers, which saves banks time and money on their Know Your Customer (KYC) process. The fourth part of this paper further examines the identity management framework of blockchain to understand how it can enable a new generation of KYC policies.

Secondly, blockchain can enhance data privacy and security as all data is encrypted and stored across all nodes in the network instead of just one centralized server, which eliminates a single point of failure. An article by Deloitte discusses the applications of blockchain on IoT security and DDoS prevention. A DDoS attack occurs when many computers connected to the Internet are recruited (as botnets) to simultaneously and repeatedly send traffic to the targeted server to overload it. Hackers either remotely access devices using easily guessable login credentials to install malware, or they launch DDoS attacks with a Command and Control server, which is a master server that gives instructions for the bots to read and act on (Sallaba et al., 2017, p. 2). Instead of the default login credential, blockchain requires devices to use a public key and private key cryptography that would only be known to the user, making the system more difficult to hack (Sallaba et al., 2017, p. 2). As a decentralized, peer-to-peer network, the attacker's Command and Control server will not be able to gain access to control other nodes to launch a DDoS attack. Sallaba et al. also notes that blockchain can eliminate the use of Domain Name System (DNS) server, which is a centralized server that maps IP addresses to domain names (2017, p. 2-3). As the name and address pair will be stored on blockchain and copied across all nodes, there is no longer a need for a DNS server and therefore, no one single point of failure. Multiple companies such as Blockstack, Namecoin and Nebulis are working towards a decentralized DNS system using blockchain (Sallaba et al., 2017, p. 3). Lastly, the distributed and shared nature of the blockchain could facilitate the recovery of both data and processes in the case of an attack (assuming that not all the nodes are corrupted simultaneously). This could reduce the need for costly recovery plans (Dzhaparov, 2020, p. 47).

Lastly, as smart contracts are unbiased, digitized agreements that only execute when all requirements are met, less trust is needed between partners. This, along with other benefits of blockchain discussed above, provides a safe environment that encourages the sharing of information between partners, with or without trust being established in advance.

Despite the many promising benefits, blockchain is an emerging technology that is still in its infancy. Even though blockchain is commonly believed to be “unhackable,” there are still many loopholes in the system. Blockchain’s decentralization, despite being one of the main security strong points, introduces a different set of weaknesses. For example, as data is being shared with all users on a network, private data can be monitored or pieced together to become a serious data privacy breach (Fitzpatrick, 2019). Blockchain technology also faces problems of vulnerabilities in smart contracts’ code, identification of malicious behaviors in historical data, and difficulties in operational maintenance (Zheng et al., 2020, p. 1). Furthermore, it is worth noting that blockchain technology has only been around for ten years. Smart contracts, though more reliable, are expensive and difficult to program. Several studies selected analyzed proposals or concepts and have little quantitative data or practical applications. Some practical solutions to problems concerning data security, mutability, and authentication of users are present, however, those usually require a significant change to the current infrastructure of the companies. Blockchain is also proved to have issues with scalability. In his paper “The Quest of Scalable Blockchain Fabric,” Marko Vukolic brings forth the tradeoff between scalability and performance amongst the two types of blockchain - Proof-of-Work (PoW) based and Byzantine fault-tolerant (BFT) based (2015, p. 4). PoW blockchain is the technology behind Bitcoin which requires nodes to “mine,” or to add another block to the chain. A block is usually added every ten minutes, and mining takes up a lot of computing power (Vukolic, 2015, p. 2). However, PoW blockchain is a public blockchain and offers good scalability. On the other hand, BFT-based blockchain offers good performance for a small number of replicas or nodes (Vukolic, 2015, p. 3). This brings up the discussion of the Scalability Trilemma, a term coined by the founder of the public blockchain Ethereum, Vitalik Buterin (Viswanathan & Shah, 2018). The trilemma refers to the tradeoffs between security, scalability, and decentralization. Currently, there are no blockchain platforms that can optimize all three of these factors, and it is up to the business to decide which factors are best suited for their needs.

2. The integration of blockchain and AI

Even though both blockchain and AI have been receiving a lot of attention recently due to their functionality, both technologies have certain weaknesses. Some research has been done on the integration of blockchain and AI as one has the potential to overcome the limitations of the other. In their article "Blockchain Intelligence: When Blockchain Meets Artificial Intelligence," Zheng, Dai, and Wu (2020) suggest that AI techniques such as ML, data mining, and data visualization can help identify risks in blockchain transactions, identify vulnerable programming codes in smart contracts, etc. (p. 1). In return, blockchain can help enhance data integrity to improve the results of AI techniques. AI diagnostic analytics can monitor the performance of blockchain systems and identify faults or bottlenecks to optimize the system and improve reliability.

The integration of blockchain and AI can also promote secure data sharing over the web. Wang et al. propose SecNet, an architecture that enables secure data storing, computing, and sharing in the Internet environment. The architecture integrates three components: blockchain-based data sharing, AI-based secure computing platform and trusted value-exchange mechanism for purchasing security service (Wang et al., 2019, p. 77981). In addition, there has been some research focused on business process automation and risk management. Dhieb et al. propose a Smart Insurance System based on Blockchain and Artificial Intelligence (SISBAR) to codify business rules, automate claims processing, estimate clients risk levels, and detect fraudulent claims (2020, p. 58546-58547). AI data analysis methods such as XGBoost and VFDT to study the data stored on blockchain and propose a fraud detecting and risk estimating model. The Hyperledger Fabric is used for the blockchain component of this framework, and a representational state transfer (REST) server is also developed to insure communication between blockchain, AI and other applications via REST application programming interfaces.

Loan services is another area that can benefit from the integration of AI and blockchain. Customers can send in their request through an application, and their inputs will be hashed and sent to the blockchain (Horbonos & Sotnichek, 2019). The hash creates a connection between client's identity and information, but the information itself is not stored in the blockchain and therefore remains private. On the backend, data is run through pre-trained AI models to determine the validity of the request, and return a response, which is also stored in the blockchain (Horbonos & Sotnichek, 2019). With the request, customer's ID and response, banks' employees can easily process the loans.

Lastly, some research projects have been focused on the combination of AI and Blockchain to improve the security of the Internet of Things. As mentioned above, blockchain eliminates the single point of failure from the IoT, and AI machine learning methods can be utilized to analyze the huge amount of data collected from the IoT and detect abnormal activities to prevent cyberattacks.

III. Hyperledger Fabric and Corda

In their article on Medium.com, Swish lists Hyperledger Fabric and Corda as two of the most popular permissioned blockchain platforms for enterprises (2019). These two platforms also stand out because of their scalability and confidentiality features that make them suitable for the financial industry. The final decision on which platform to implement should be based on how blockchain aligns with the firm's business strategies and infrastructure.

	Fabric	**Corda**
Governance	Linux	R3
Industry	Cross-industry	Financial
Smart contracts	Standard, general-purpose programming language	Smart legal contract (legal prose)
Consensus	Modular/Pluggable Not all nodes in a network must take part in the consensus process	Only parties involved take part in decision making
Privacy	'Channel' as a data partitioning mechanism	Consensus only on individual agreements - not on whole ledger
Interoperability	No	Yes – A Global Logical Ledger

1. Governance and Industry

R3 Corda is a distributed ledger technology (DLT) developed by R3, an enterprise software firm that specializes in enterprise blockchain technology for the financial services industry and beyond. Initially built for the highly-regulated financial service industry, the Corda platform consists of an open source software project, Corda, and a set of standards, network parameters and associated governance processes.

Is Corda a Blockchain?

Corda is both a blockchain and not a blockchain. It is a DLT, which is defined as a decentralized database managed by multiple participants across multiple nodes (“Blockchain 101,” n.d.). Blockchain is a specific type of DLT where sequences of blocks are chained together using cryptographic hashes and distributed among users. Corda is a blockchain because transactions on the platform are cryptographically chained to other transactions that it depends on. The major difference between Corda and other blockchain platforms is that Corda does not periodically group transactions needing confirmation into a block to confirm them in one go (“Blockchain 101,” n.d.). Instead, transactions are confirmed in real-time. As a result, the confirmation of one transaction does not depend on any others, increasing both performance and security.

Hyperledger Fabric is an open-source, permissioned blockchain project from Linux Foundation. Fabric is a modular framework that uses plug-and-play components to accommodate for a wide range of use cases (“Hyperledger Fabric,” n.d.).

2. **Smart Contract**

Corda is designed to model and automate real world transactions in a legally enforceable manner. Corda’s smart contracts (known as CorDapps) are expressed in legal prose and are legally binding. Corda’s flow framework enables coordination between multiple mutually distrusting parties across the internet without a central controller by simplifying the process of writing complex multi-step protocols (Brown, 2018, p. 6).

Hyperledger Fabric claims to be the first blockchain system to run distributed applications written in standard, general purpose programming language without systemic dependency on a native cryptocurrency (Androulaki et al., 2018, p. 1). This results in many benefits such as flexibility, easier deployment and widespread adoption. Fabric also develops its own smart contract called "Chaincode."

3. Consensus

With Corda, only parities who are involved in the transaction take part in the decision-making process, and this plays a vital role in the privacy feature of this framework.

Fabric supports modular consensus protocols and membership services, allowing companies to tailor the framework to fit their needs. Fabric's consensus architecture deviates from the common *execute-order* model in which all peers need to execute every transaction, and every transaction must be deterministic (Androulaki et al., 2018, p. 2). This model requires the sequential execution of transactions, limiting performance and manageability. Fabric uses the *execute-order-validate* paradigm that lets transactions execute before consensus is reached on their place in the chain (Androulaki et al., 2018, p. 2). Transactions can also be executed in parallel which improves performance. Once enough peers agree on the results, transactions are added to the ledger and are ordered. Now that they are in sequence, peers can check whether a later transaction was invalidated by an earlier transaction. This step prevents the exact same transaction from happening twice (called *double-spending*) (Rilee, 2018). With Fabric's pluggable consensus policy that defines which peers need to execute which transactions, a given chaincode can be kept private from nodes that are not a part of the policy.

4. Privacy

One key feature that makes Corda stand out from its competitors is its privacy. A major issue with the adoption of blockchain in the banking industry is data stored on a distributed ledger can be seen by anyone on the network. This is not ideal in an industry that collects and stores a huge amount of highly sensitive data like financial services. As mentioned above in the Consensus section, Corda solves this problem by only broadcasting data to those who are involved in the transaction (Brown, 2018, p. 6).

Similar to Corda, Fabric’s privacy feature is also what makes it unique. The blockchain platform supports data “channels” where private data can be shared among a specific group, and each channel maintains its own separate ledger (“Hyperledger Fabric,” n.d.). This feature is different from that of Corda because it provides less privacy. Fabric’s channel works similarly to an online group chat, meaning that the messages are only visible to participants of the group. However, once new users are added, they gain access to the entire history of the channel and therefore are able to see details of transactions that do not involve them. On the other hand, Corda, by broadcasting each transaction on a peer-to-peer basis, provides more privacy but a much higher management overhead. The channel architecture also focuses more on the why rather than the who which makes it easier to reason about all a peer’s relationship from a business perspective (Shin, 2020).

5. Interoperability

Another important feature of Corda is its interoperability. The platform allows multiple applications to coexist and interoperate on the same network. The Corda software is implemented on industry standard tools to maximize deplorability and integration with existing enterprise infrastructures (Brown, 2018, p. 7). R3 envisions Corda to be a "global logical ledger," a reliable single source, "with which all economic actors will interact and which will allow any parties to record and manage agreements amongst themselves in a secure, consistent, reliable, private, auditable, and authoritative manner" (Brown, 2018, p.5).

In their introduction paper, Corda points out that interoperability is one of the key differences between Corda and other platforms such as Fabric (Brown, 2018, p. 19). With Fabric, each business solution is an independent, standalone network that is not compatible with others. Each requires its own identity, consensus, and governance process.

IV. Digital Identity Management

Since the COVID-19 pandemic moved many different financial services online, banks need to rethink their identity verification and credential sharing processes as physical contacts need to be kept to a minimum. As mentioned at the beginning of the paper, the financial services industry has witnessed a significant increase in the number of identity thefts and frauds. Sensitive data being stored in centralized databases by third parties opens up many vulnerabilities for hackers to exploit. Furthermore, customers having to manage multiple accounts and passwords over many different websites also puts their personal data at risk. They can forget their log-in credentials, which in return might force them to provide the third party with even more personal data to regain their passwords. Similar, easier-to-remember passwords can also be used over multiple websites as a result, leaving many of their online accounts vulnerable. Lastly, the KYC policies have always been considered overly costly and complex.

AI can help improve the security of digital identity through biometrics-based verification systems. ML algorithms can also quickly recognize forgery attempts on identity documents and flag any suspicious log-in behaviors. With automation, AI verification process is much faster than the traditional manual process, allowing a much higher number of requests to be processed at a lower price.

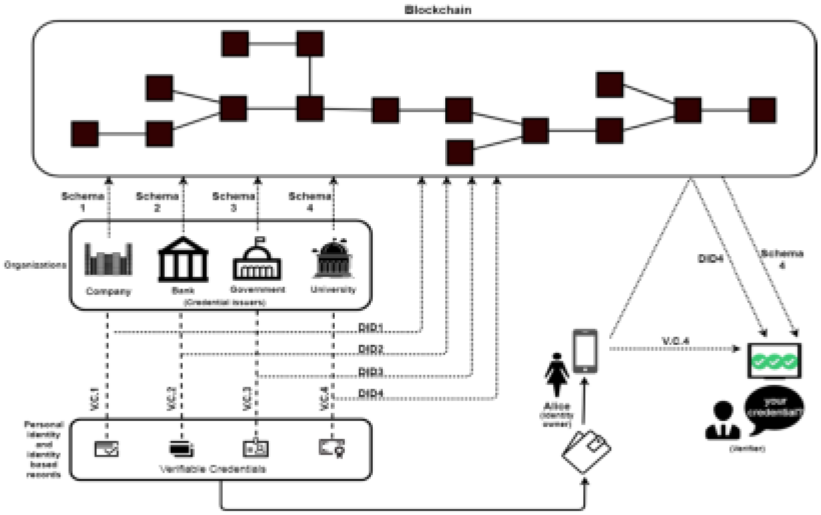
Blockchain introduces a new identity management system with the concept of self-sovereign identity, which allows an individual (a person or an organization) to be in full control and ownership of their own data.

Framework

Figure 1 is a blockchain's identity management framework proposed by Aydar, Ayvaz and Cetin (2020, p. 7-17).

Figure 1

Overall workflow of the proposed identity system



Note. From “Towards a Blockchain based digital identity verification, record attestation and record sharing system,” by M. Aydar, S. Ayvaz and S. Cemil, 2020, p. 8 (https://arxiv.org/abs/1906.09791). arXiv.org perpetual, non-exclusive license.

In the system above, a digital identity is assigned to each individual through blockchain. The blockchain itself does not store any actual private personal data, but rather the proof of verification (Aydar et al., 2020, p. 8). For example, if someone’s driving license is being used to verify their identity, the actual license is not stored on the blockchain. What will be on the blockchain is just the fact that their document has been verified by, in this case, the local government and therefore is good to use (Aydar et al., 2020, p. 8). Users can store all of their verifiable credentials, which are machine readable, cryptographically secure digital credentials, in an identity wallet. Once again, identity owners fully control their data and can divide whom to share their data. In this system, AI can be used to add another layer of security with biometrics and ML.

Benefits

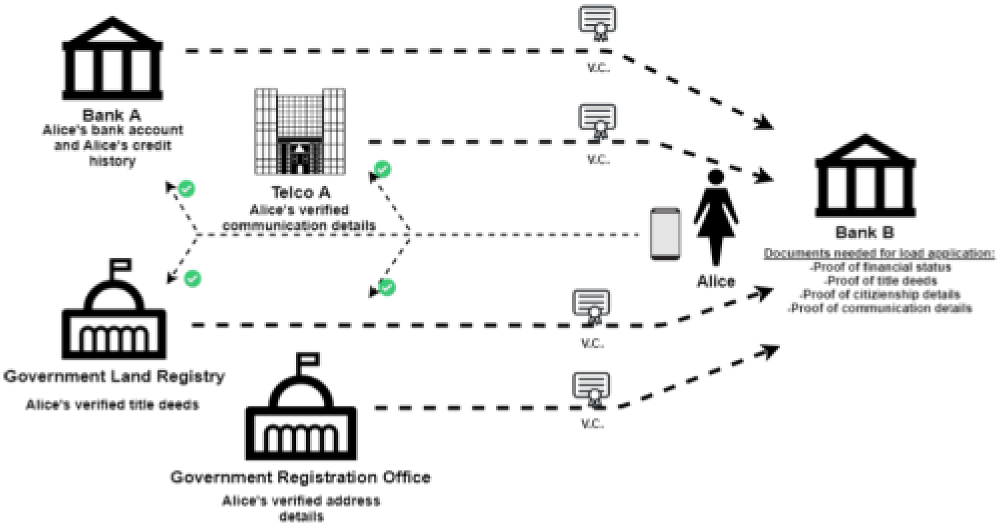
This identity management system allows banks to streamline their customer on-boarding processes. Banks no longer have to spend as much time, money and labor on verifying customers’ information. Transparency as well as information accuracy and reliability are also significantly increased. Due to the secure nature of blockchain, the risk of ID theft and fraud is also reduced.

For customers, blockchain’s identity management system provides a much more convenient user experience as all verifiable credentials are stored in one place, users no longer need to memorize multiple log-in credentials or reach out to third parties whenever they need to verify their identities. Customers are once again in full control of their own data, which provides full transparency between customers and financial institutions.

Limitations

Blockchain technology is not without flaws. Since all identities are essentially created and only existed in the digital world, banks still need to figure out who is responsible to provide the trust mapping between real life physical identity and the digital identity (“Practical thoughts,” n.d., p. 9). It will be crucial to ensure that a vulnerable identity provider doesn’t open up opportunities for an identity takeover on the network. Furthermore, with blockchain still being a very new technology, businesses may face resistance from both partners and their own employees. In order to retain their customers, verifying organizations may refuse to share data or collaborate (“Practical thoughts,” n.d., p. 10). Lastly, there has not been many clear regulations on the use of blockchain in the financial sector. As a result, all entities involved have to accept risk and uncertainty by agreeing to participate in an identity network.

Figure 2


Bank A
Alice's bank account and Alice's credit history
Telco A
Alice's verified communication details
Government Land Registry
Alice's verified title deeds
Government Registration Office
Alice's verified address details
V.C.
V.C.
V.C.
V.C.
Alice
Bank B
Documents needed for load application:
-Proof of financial status
-Proof of title deeds
-Proof of citizienship details
-Proof of communication details

Use Case: Loan Application

Note. From "Towards a Blockchain based digital identity verification, record attestation and record sharing system," by M. Aydar, S. Ayvaz and S. Cemil, 2020, p. 11 (https://arxiv.org/abs/1906.09791). arXiv.org perpetual, non-exclusive license.

Figure 2 shows an example use case of a loan application (Aydar et al., 2020, p. 11). In this use case, the customer Alice, who is a current customer of Bank A, wants to apply for a loan with Bank B. Bank A and Bank B are trusted partners. Alice also owns land, and that information is kept by the local government. Because Bank B has never worked with Alice before, they are required by KYC regulations to know her before accepting her application. Using the proposed framework, Allice authenticates herself with Bank B, who then reaches out to related organizations to collect the information needed for the loan application. Alice will need to give her consent to these organizations before they can share her information in the form of verifiable credentials. The whole process happens within minutes without physical interaction between any parties involved. Similar to the loan case mentioned in section 2, AI can be used to track and monitor behaviors in real time and to enhance mobile security using biometric authentication.

V. Conclusion

The banking and finance industry has always been a target for hackers, but the COVID-19 pandemic, along with the rising number of sophisticated frauds and cyberattacks, further emphasizes the importance of a more advanced and proactive security system. This thesis discusses how AI and blockchain can be used to enhance cybersecurity and risk management in the financial services industry. While AI can be used to detect malicious activities and help verify the authenticity of customers, blockchain technology provides a decentralized, trust-less and transparent platform that also significantly improves security, data management and risk management. The integration of blockchain and AI has been gaining a lot of attention recently as these two technologies can overcome the limitations of each other. Both technologies not only help banks quickly react to changes but also prevents potential threats even in times of disruptions. However, as discussed in the thesis, blockchain is a relatively new technology that is fairly expensive and cumbersome to implement. The lack of regulations makes this a risky investment, even though blockchain is being experimented and implemented by more and more businesses as well as governments around the world. The last two sections introduce two prominent permissioned blockchain frameworks, Hyperledger Fabric and R3 Corda, and examine the application of AI and blockchain in identity management. This digital identity framework fosters the collaboration between banks and their customers even in the age of remote work as it removes the need for physical interaction between parties involved.

This thesis mostly discusses blockchain and AI from a business perspective and therefore does not go into details about the technical aspects of either technology. The use of cryptocurrency as well as its impact on the banking industry is also not mentioned despite it being an evolving development in the fintech industry. I briefly discussed some limitations of blockchain and did not review the challenges of blockchain implementations and developments. The ethics of AI and concerns surrounding issues such as job loss, trust, misuse of technology, privacy and surveillance are also not examined.

The topic of AI, Blockchain and banking security is vital in the field of Business Analytics, or specifically Security Analytics, as these two technologies are expected to create fundamental changes to this industry. Furthermore, Blockchain and AI can assist analysts in making data-driven decisions using high quality data in a secure network. Lastly, since blockchain is still in its infancy, it is important for analysts to understand the foundation and the implications of this technology early on to effectively make decisions and implement blockchain for their businesses.

For future work, researchers can look more closely into the long-term impacts of AI and blockchain, both economically and socially. It could also be interesting to further investigate the integration of blockchain and AI in digital identity management and edge computing to provide a more secured working environment as we head into the age of connectivity, digitalization, and remote work.

References

Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021, January 14). Covid-19 and cyber risk in the financial sector. Retrieved May 02, 2021, from https://www.bis.org/publ/bisbull37.pdf

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15).

Aydar, M., Ayvaz, S., & Cemil Cetin, S. (2020, June 23). Towards a blockchain based digital identity verification, record attestation and record sharing system. *arXiv e-prints, arXiv-1906.*

Biswas, S., Carson, B., Chung, V., Singh, S., & Thomas, R. (2020, September 19). *AI-bank of the future: can banks meet the AI challenge?* McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge.

Blockchain. Builtin. (n.d.). https://builtin.com/blockchain.

Blockchain 101 - blockchain technology & DLT explained. R3. (n.d.). https://www.r3.com/blockchain-101/.

Brown, R. G. (2018, May). *The corda platform: an introduction white paper.* R3. https://www.r3.com/white-papers/the-corda-platform-an-introduction-whitepaper/.

Bush, H. (2018, October 9). *Driving identity security in banking using biometric identification*. Microsoft Azure. https://azure.microsoft.com/en-us/blog/driving-identity-security-in-banking-using-biometric-identification/.

Cam, A., Chui, M., Hall, B., & DeLallo, D. (2019, November 22). *Global AI survey: AI proves its worth, but few scale impact*. McKinsey & Company. https://www.mckinsey.com/featured-insights/artificial-intelligence/global-ai-survey-ai-proves-its-worth-but-few-scale-impact.

Caplain, J., & Jacco, C. (2020, May 12). *Key cyber risks for banks during COVID-19*. Retrieved October 28, 2020, from https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html.

Crisanto, J. C., & Prenio, J. (2020, May). *Financial crime in times of Covid-19 – AML and cyber resilience measures.* Bank for International Settlements. https://www.bis.org/fsi/fsibriefs7.pdf.

Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A secure AI-driven architecture for automated insurance systems: Fraud Detection and Risk Measurement. *IEEE Access, 8*, 58546-58558.

Dzhaparov, P. (2020). Application of blockchain and artificial intelligence in bank risk management. Икономика и управление, 17(1), 43-57.

Fitzpatrick, L. (2019, February 2). *A hacker's take on blockchain security.* Forbes. https://www.forbes.com/sites/lukefitzpatrick/2019/02/04/a-hackers-take-on-blockchain-security/

Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: a review and extension. *Digital Finance*, 1-29.

Horbonos, P., & Sotnichek, M. (2019, October 31). *The convergence of blockchain and AI: Applications in finance*. Apriorit. https://www.apriorit.com/dev-blog/643-ai-blockchain-convergence.

Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018, July). *Artificial intelligence and international security*. Center for a New American Security. https://csdsafrica.org/wp-content/uploads/2020/06/CNAS_AI-and-International-Security.pdf.

Hyperledger Fabric. Hyperledger. (n.d.). https://www.hyperledger.org/use/fabric.

Imeson, M. (2020, September 2). *Ransomware threat tests banks' resilience to cyber crime.* The Banker. https://www.thebanker.com/Transactions-Technology/Ransomware-threat-tests-banks-resilience-to-cyber-crime

Knowles-Marchione , K., & Kolpek, M. (2017, July 25). *Danske bank: Innovating in artificial intelligence and deep learning to detect sophisticated fraud*. Teradata. https://www.teradata.com/Blogs/Danske-Bank-Innovating-in-Artificial-Intelligence.

Ostroverkh, Y. (2020, January 30). *Ways the blockchain will augment banking security*. Diceus. https://diceus.com/ways-the-blockchain-will-augment-banking-security/

Practical thoughts on blockchain and identity. Okta. (n.d.). https://www.okta.com/resources/whitepaper/practical-thoughts-on-blockchain-and-identity/.

Rilee, K. (2018, February 9). *Understanding hyperledger fabric - endorsing transactions*. Medium. https://medium.com/kokster/hyperledger-fabric-endorsing-transactions-3c1b7251a709.

Sallaba, M., Kumar, S., & Paulsen, J. H. (2018, December 03). *Prevention of DDoS attacks with blockchain technology.* Deloitte. https://www2.deloitte.com/de/de/pages/technology-media-and-telecommunications/articles/cyber-security-prevention-of-ddos-attacks-with-blockchain-technology.html

Shroff, R. (2020, January 16). *Artificial intelligence for risk reduction in banking: current uses.* Towards Data Science. https://towardsdatascience.com/artificial-intelligence-for-risk-reduction-in-banking-current-uses-799445a4a152

Swish Team. (2019, January 4). *The 5 best blockchain platforms for enterprises and what makes them a good fit.* Medium. https://medium.com/swishlabs/the-5-best-blockchain-platforms-for-enterprises-and-what-makes-them-a-good-fit-1b44a9be59d4.

Tapscott, A., & Tapscott, D. (2017, March 1). How blockchain Is changing finance. Harvard Business Review. https://hbr.org/2017/03/how-blockchain-is-changing-finance.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2), 147-156.

Upatham, P., & Treinen, J. (2020, April 15). Amid COVID-19, global orgs see a 148% spike in ransomware attacks; finance industry heavily targeted. Carbon Black. https://www.carbonblack.com/blog/amid-covid-19-global-orgs-see-a-148-spike-in-ransomware-attacks-finance-industry-heavily-targeted/

Varghese, L., Tomer, M., & McCraw, F. (2017, June). Financial services: Building blockchain one block at a time. Cognizant. https://www.cognizant.com/whitepapers/financial-services-building-blockchain-one-block-at-a-time-codex2742.pdf

Viswanathan, S., & Shah, A. (2018, October 19). The scalability trilemma in blockchain. Medium. https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df.

Vukolić, M. (2015, October). The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International workshop on open problems in network security (pp. 112-125). Springer, Cham.

Wang, K., Dong, J., Wang, Y., & Yin, H. (2019). Securing data with blockchain and AI. IEEE Access, 7, 77981-77989.

Wiafe, I., Koranteng, F. N., Obeng, E. N., Assyne, N., Wiafe, A., & Gulliver, S. R. (2020). Artificial intelligence for cybersecurity: a systematic mapping of literature. IEEE Access, 8, 146598-146612.

Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. IEEE Access, 8, 23817-23837.

Zheng, Z., & Dai, H. N. (2020, April 3). Blockchain intelligence: When blockchain meets artificial intelligence. arXiv preprint arXiv:1912.06485.

[1] **Ransomware** is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.

[2] A **denial-of-service (DoS)** attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. A **distributed denial-of-service (DDoS)** attack occurs when multiple machines are operating together to attack one target.