International Journal of Finance, Economics and Business
Vol. 4, No. 2, June 2025, pp.78-92.
e-ISSN: 2948-3883
DOI: 10.56225/ijfeb.v4i2.422

Review Article

Blockchain Approaches for Secure Financial Transactions in Defi and Auditing

Dennis Deladem Kwadzode [1,*]

[1] Department of Applied Financial Economics, Richard A. Chaifetz School of Business, Saint Louis University, 221 N Grand Blvd MO63103, Missouri, USA.
* Correspondence: edemkoby@gmail.com (D.D.K.)

Citations: Kwadzode, D.D. (2025). Blockchain Approaches for Secure Financial Transactions in Defi and Auditing. *International Journal of Finance, Economics and Business*, *4*(2), 78-92.

Received: 16 April 2025 Revised: 18 May 2025 Accepted: 22 June 2025 Published: 30 June 2025

Abstract: Blockchain technology is becoming an important tool for secure financial transactions. It supports decentralized finance (DeFi) services and innovative auditing methods. This paper provides an overview of how blockchain is utilized in financial modeling, with a focus on decentralized finance (DeFi) and auditing. This study explains the basic technology behind popular blockchain systems, like public platforms such as Ethereum (with smart contracts and oracle networks), and private systems like Hyperledger Fabric. This study also examines advanced methods, such as zero-knowledge proofs. This study demonstrates how these tools facilitate the development of financial models in DeFi by enabling peer-to-peer services without requiring trust, and in auditing by enhancing data transparency and security. This study compares different blockchains in terms of speed, cost, and scalability. Security issues (like smart contract bugs or attacks on consensus) and practical problems (like trusting oracles and following laws) are also discussed. The review article examines the challenges of using blockchain and explores some of the latest solutions, including Ethereum's transition to proof-of-stake, sharding for improved scalability, and the application of zero-knowledge proof for enhanced privacy. This study also suggests future research topics, including connecting different blockchains, verifying smart contracts with formal methods, developing more effective rules and regulations, and training skilled workers. The goal is to help researchers and professionals understand the current situation and future of blockchain in finance and auditing.

Keywords: Blockchain Technology, Financial Modeling, Transaction Security, Distributed Ledger Technology, Smart Contracts, Consensus Mechanisms, Cybersecurity, Fintech, Regulatory Technology

1. Introduction

Financial markets and institutions are beginning to utilize blockchain for secure and transparent transaction processing (Segun Adanigbo et al., 2024). The primary features of blockchain decentralization, immutable records, and robust cryptographic security provide a novel approach to financial modeling. Instead of using central systems, transaction rules and asset behavior are stored on shared digital ledgers (Schär, 2021). One popular example is Decentralized Finance (DeFi). This is a group of financial apps built on public blockchains, such as Ethereum. DeFi tries to copy traditional financial services (like trading, lending, and issuing assets), but in an open and permissionless way (Schär, 2021). At its peak in late 2021,

the total value locked (TVL) in DeFi exceeded $250 billion, demonstrating rapid growth and substantial amounts of capital being managed on blockchain systems (Bhambhwani & Huang, 2024).

At the same time, the auditing and accounting field is exploring blockchain to improve the accuracy of financial records. Because blockchain maintains a record that cannot be altered, it enables auditors to verify data in real-time and create more robust audit trails. However, blockchain in finance also faces big challenges. In DeFi, smart contracts sometimes contain bugs or weaknesses that result in significant losses, highlighting the need for robust audits and formal code reviews (Y. Zhang et al., 2025). Traditional auditors also face problems: for example, a transaction on the blockchain may not prove that something real happened outside the system. This means we need clear regulations and ways to connect digital records to real-world events. Another issue is performance. Current blockchains, particularly Ethereum, can be slow and costly, with limitations on the number of transactions they can handle. There are also open questions about how to integrate blockchain systems with today's financial systems and regulations, without compromising the benefits of decentralization and transparency (Zhang et al., 2025).

This paper reviews the latest blockchain methods for secure financial transactions, with a focus on DeFi and auditing use cases. First, this study explains the technology behind popular platforms like Ethereum and Hyperledger, as well as tools such as smart contracts, oracles, and zero-knowledge proofs. Next, this study compares how these tools are utilized in DeFi versus auditing, examining performance (including speed, cost, and scalability) and security concerns. This study also examines key challenges, including technical issues (such as consensus limits and privacy concerns), as well as legal and governance concerns. Finally, this study lists future research topics. These include better scaling methods (like Layer-2, sharding, and faster consensus), stronger ways to audit security, and creating common standards for compatibility and legal compliance. Our goal is to give a useful overview for researchers and professionals working with blockchain in finance and accounting, using recent studies to support real-world research and projects.

2. Literature Review

In this section, this study reviews the fundamental blockchain technology that enables secure financial transactions, particularly for applications such as decentralized finance (DeFi) and auditing. This study examines the distinctions between public and private blockchains, the operation of smart contracts, the integration of external data into blockchains via oracles, and the enhancement of privacy and security through advanced tools, such as zero-knowledge proofs. These are the primary components that people use to construct financial systems on blockchain.

2.1 Public Blockchain Platforms (Ethereum and DeFi)

Ethereum is a good example of a public (or permissionless) blockchain, and it's widely used in decentralized finance (DeFi). It was proposed by Vitalik Buterin in 2013 as a kind of "world computer" and introduced smart contracts that can run on a shared, global ledger (Zheng et al., 2020). On Ethereum, anyone can create and run smart contracts or join the network as a user or validator without needing permission. The system is designed to prioritize security and decentralization over speed and efficiency. Every transaction and contract is verified and validated across all the network's nodes to ensure accuracy and correctness. This means contracts always run exactly as written, and all changes (like value transfers) are permanent and visible to everyone (Scherer, 2017). But this design comes with limits. The older version of Ethereum used Proof-of-Work, which could only handle about 15 transactions per second (Bez et al., 2019; Kaur & Gandhi, 2020). This often caused slowdowns and high transaction fees, especially when the network was busy. In 2021, for example, fees sometimes reached tens or even hundreds of dollars for a single transaction, making it difficult for many people to use (Zheng et al., 2020).

To fix these problems, Ethereum started its upgrade plan (called Ethereum 2.0). In 2022, it transitioned to Proof-of-Stake (referred to as "the Merge"), which eliminated the need for energy-intensive mining and prepared the system for future updates, such as sharding (Rashid et al., 2025). Sharding will divide the network into smaller parts to handle more transactions simultaneously. Additionally, Layer-2 solutions, such as rollups and state channels, assist by performing most of the work off the main chain, then sending only the final results back to Ethereum (Bez et al., 2019). These changes are expected to increase Ethereum's speed from just a few transactions per second to thousands, a necessary step if global financial systems are to run on blockchain.

Ethereum is crucial in DeFi because it was the first to utilize smart contracts, which enable complex financial rules to execute directly on the blockchain. Most DeFi applications, such as decentralized exchanges, lending platforms, stablecoins, and derivatives, are built as smart contracts on the Ethereum

blockchain. These apps benefit from Ethereum's strong security and ability to connect with each other. Because Ethereum is open and permissionless, anyone can build a new financial product that works with existing ones. This has created a lively "money Lego" system, where many parts fit and work together (Schär, 2021). Another big advantage is transparency. Since everything on Ethereum is public, DeFi brings a new level of openness to finance. All actions, including trades, loans, and collateral deposits, are recorded on a permanent ledger that is accessible to anyone for review (Schär, 2021). This can help keep markets honest, but it also creates privacy problems, because people's account balances and transactions are visible. Some privacy methods, such as zero-knowledge proofs, can help with this. A key challenge in Ethereum-based DeFi is the need for external data, including asset prices and interest rates. This data comes through oracles. However, if an oracle provides incorrect data, it can cause significant problems, such as accidental liquidations on lending platforms (Kadeba, 2024). Thus, Ethereum provides a strong foundation for secure financial systems within an open network. It still has its limitations, such as high costs and low speed, but ongoing updates are working to address these issues.

2.2. Permissioned Blockchain Platforms (Hyperledger and Enterprise)

Unlike public blockchains, permitted blockchains like Hyperledger Fabric are made for private groups or businesses, where all participants and validators are known. Hyperledger Fabric is an open-source project under the Linux Foundation. It doesn't use proof-of-work. Instead, it uses a flexible consensus method and a network with access control. Only approved nodes can approve transactions and assist in ordering them. This eliminates the need for heavy mining, allowing for significantly improved performance. In Fabric, transactions undergo two steps: first, they are endorsed, and then they are ordered and confirmed (Y. Zhang et al., 2025). This setup separates the transaction logic from the agreement on the order. Thanks to this design and the smaller, trusted network, Fabric can handle hundreds to thousands of transactions per second, significantly more than Ethereum can currently handle. In normal setups, Fabric has achieved approximately 2000 TPS, and in research tests with special modifications, it has reached up to 20,000 TPS (Vera-Rivera, 2022). The transaction is also much faster. Fabric utilizes consensus methods such as Crash Fault Tolerance (CFT) or Byzantine Fault Tolerance (BFT) in small networks, which can confirm blocks in just a few seconds. In contrast, Ethereum (especially during the PoW period) required minutes to confirm a transaction was final. Due to their high speed and low latency, permissioned blockchains like Fabric are well-suited for use cases that require the rapid processing of large amounts of data, such as bank payments, supply chain finance, or real-time audits within companies.

Hyperledger Fabric is designed to meet business needs, featuring robust privacy and security controls. It allows data on the ledger to be separated into channels, so only the people involved in a transaction can see it. This helps protect confidential information, which is challenging to do on public blockchains. Smart contracts in Fabric are called "chaincode", and they can be written in common programming languages like Go or Java. These contracts run on specific approved nodes, called endorsing peers (Vera-Rivera, 2022). This makes it easier to connect blockchain systems with existing company software and comply with legal regulations. For example, in auditing, a Fabric network could include a company, its auditors, and regulators. The ledger would store financial records that only those groups can see. Chaincode could help by automatically checking for compliance or warning about unusual activity. Because the network is permissioned, private data stays protected. In fact, big accounting firms have already tested this. PwC, for example, developed a blockchain audit tool utilizing a permissioned ledger, which reportedly reduced reconciliation time by 90% by automatically matching transactions (Y. Zhang et al., 2025). This demonstrates how permissioned blockchains, such as Fabric, can enhance audits by automating tasks and sharing data in real-time.

Hyperledger Fabric is designed for business use, with strong privacy and security features. It allows to split data into channels, so only the individuals involved in a transaction can view it. This helps keep private information safe, which is difficult to do on public blockchains. Smart contracts in Fabric are called "chaincode", and they can be written in common languages like Go or Java. These contracts run on special approved nodes called endorsing peers (Vera-Rivera, 2022). This setup facilitates easier integration of blockchain with existing company systems and adherence to legal regulations. For example, in an auditing case, a Fabric network could include a company, its auditors, and regulators. The ledger would store financial data that only these groups can see. Chaincode can automatically check for compliance or alert when something appears to be incorrect. Since the network is permissioned and private, data remains secure. Big accounting firms have already tried this. PwC, for instance, built a blockchain audit system with a permissioned ledger. It reportedly reduced reconciliation time by 90% by matching transactions

automatically (Zhang et al., 2025). This demonstrates that permissioned blockchains, such as Fabric, can facilitate faster and easier audits by leveraging automation and real-time data sharing.

2.3. Smart Contracts and Financial Automation

Smart contracts are a crucial component of financial systems built on blockchain. The idea originated in the 1990s with Nick Szabo, but it gained significant traction with the launch of Ethereum (Szabo, 2017). A smart contract is essentially a program on the blockchain that executes automatically when specific conditions are met. In DeFi, smart contracts handle the rules of financial services. For example, a lending contract can calculate interest, manage collateral, and initiate liquidation without requiring any human intervention. One significant benefit of smart contracts is the enhanced trust they provide, and they don't need to rely on a bank or middleman; the contract's code is open for anyone to check and will always do exactly what it's written to do (Savelyev, 2017). This makes it hard for anyone to break the agreement or change the rules. That's why smart contracts are seen as helpful in solving trust issues in finance; they ensure both sides keep their promises (John et al., 2023). DeFi platforms utilize smart contracts to develop services similar to those of banks, exchanges, and asset managers, all without the need for a central company. Things like stablecoins and automated trading run 24/7 using just code.

But even though smart contracts are powerful, they also come with serious risks. Since they control real money, any bugs or mistakes in the code can result in substantial losses. Unlike regular software, smart contracts are hard, or sometimes impossible, to fix once they're on the blockchain, because the code becomes permanent. A notable case occurred in 2017 when a bug in an Ethereum multisignature wallet locked approximately $150 million worth of Ether, and the funds couldn't be recovered (Buhler, 2025). Many studies have identified common problems in smart contracts, such as reentrancy bugs or integer overflows, and have documented real-world attacks (Schär, 2021). One notable example is the DAO attack in 2016, where a hacker exploited a reentrancy bug to steal approximately $50 million from a decentralized fund (Bagirovs, 2025). Since then, numerous similar hacks have occurred in DeFi, highlighting that security remains a significant issue in blockchain finance (Li et al., 2022; Wang et al., 2022; Liyi Zhou et al., 2023).

To reduce these risks, a new industry of smart contract auditing has grown. Security companies review the code and sometimes conduct formal testing to ensure it's safe. Research shows that DeFi projects with more audits, especially those conducted by well-known firms, tend to attract more investment and earn users' trust (Bhambhwani & Huang, 2024). One study examined 316 DeFi projects and found that those reviewed by multiple independent auditors had a higher total value locked (TVL) and better market value. Obtaining even one audit provided a clear boost in confidence and attracted more users and funding (Kadeba, 2024; Vera-Rivera, 2022). These results demonstrate that robust audits and thorough quality checks are crucial in DeFi. In many ways, they serve as a substitute for traditional banks or regulators, helping to ensure the safety and integrity of the system.

Another problem with smart contracts today is that they can't directly access information from outside the blockchain. Blockchains operate in closed systems, so a smart contract cannot simply check the price of a stock from a website or confirm if an event occurred in the real world. This issue is often referred to as the "oracle problem." John et al. (2023) highlight a key limitation: smart contracts struggle to work with off-chain data and cannot easily integrate with traditional legal systems in the event of an error. Because there's no built-in trusted middleman, linking blockchain programs with the real world needs special tools called oracles (discussed next). Additionally, if there's disagreement or confusion, there's no court or third party to intervene, unlike in regular systems.

Another challenge is cost. Without intermediaries like banks or clearinghouses, every part of a financial process must be built into the smart contract. This results in more code, increased redundancy, and additional cryptographic checks for enhanced security. Ironically, removing middlemen can make the system more expensive, in terms of computing power, storage, and time needed for development (John et al., 2023). This cost is reflected in blockchain fees and the work each node must perform to maintain system security. Researchers in finance and computer science are developing solutions, such as enhanced virtual machines, faster bytecode, and methods to more easily connect smart contracts with real-world data and legal systems (John et al., 2023).

2.4. Oracles: Bridging Blockchain with Real-World Data

Oracles play a crucial role in blockchain-based financial systems, as they integrate real-world data into smart contracts. Many financial contracts require information from outside the blockchain, such as asset prices, exchange rates, interest rates, or real-world events (for example, if an insurance event occurs). An

oracle is a service or tool that collects data from off-chain sources and stores it on the blockchain, allowing smart contracts to utilize it. For example, a DeFi contract for derivatives might require the price of gold in USD, or an audit system on the blockchain might utilize an oracle to verify an inventory check or a reading from an IoT sensor. Oracles can be software (extracting data from APIs) or hardware (such as devices tracking physical events), and they can be simple single feeds or large, decentralized networks where multiple sources are combined to provide a single value (John et al., 2023).

Even though oracles seem simple, they bring trust and security problems. That's because they break the blockchain's closed and predictable environment. If an oracle provides false data, whether intentionally or by accident, the consequences can be severe, particularly in finance. In fact, there have been real cases where DeFi systems were attacked through oracles. One example is from November 2020, when an oracle exploit on the Compound lending platform resulted in approximately $89 million in unexpected liquidations (John et al., 2023). Attackers tricked the oracle by using thin markets to display a fake price, causing the contract to incorrectly believe the collateral had lost value and initiate loan liquidation. This demonstrates that a smart contract's security is only as strong as the data it receives. If the oracle is wrong or dishonest, the contract can fail. As a result, the blockchain community is working diligently to develop trustworthy oracles (Gueye & Chaifetz, 2025). One method is the use of decentralized oracle networks (DONs), such as Chainlink, where multiple sources provide data, and the result is determined by consensus or averaging. This makes it difficult for a single bad actor to influence the outcome. Chainlink is also working on version 2.0, which plans to add enhanced security and even allow oracles to run some computations off-chain (Breidenbach et al., 2021). Another method is to use incentives, where oracle providers are required to post collateral and forfeit it if they send incorrect data. This gives them a strong reason to be honest.

In auditing, oracles can be used to bring data from company systems or sensors into the blockchain. For example, in a supply chain audit, temperature readings or GPS locations from sensors can be recorded on the blockchain using oracles. This provides auditors with a permanent record of conditions during shipping that cannot be altered. A review from Zhang et al. (2025) on blockchain auditing explains that while blockchain can protect the data once it is recorded, it cannot prove that the event happened in the real world. This is the core problem with oracles. Because of this, audit and legal rules must be in place to verify and confirm that what is recorded on the blockchain accurately reflects the actual events. In practice, this may involve combining blockchain records with traditional audit evidence or utilizing verified oracle providers. Looking ahead, some experts believe that oracles themselves could undergo decentralized checks or audits. New technologies, such as multi-party computation or trusted hardware, could help make data feeds more reliable. For now, oracles are a key component of financial systems on blockchain, but they remain a weak point. They enable smart contracts to respond to real-world events, but they also reintroduce the need to trust someone. This trust must be managed carefully, utilizing both technology and effective governance.

2.5. Zero-Knowledge Proofs and Privacy-Preserving Models

Zero-knowledge proofs, or ZKPs, are a powerful type of cryptography that is gaining importance in blockchain finance. They help solve problems related to privacy and scalability (Sun et al., 2021). A ZKP enables one person (the prover) to demonstrate to another person (the verifier) that something is true, without sharing any additional information. In blockchain and finance, this means it can prove a transaction is valid without revealing details such as who was involved or the amount of money sent (Lei Zhou et al., 2024). For example, a ZKP can confirm that the sender has sufficient funds and that the transaction adheres to the rules, while keeping the actual amount and identities private. This idea is already used in privacy-focused cryptocurrencies like Zcash. Zcash uses a special type of ZKP called zk-SNARKs to make transactions that are hidden but still verified by the network. This way, the system stays secure and transparent, while keeping sensitive data private (Chen et al., 2022).

In decentralized finance, ZKPs are mainly used for two things: privacy and scalability. For privacy, ZKPs can hide personal or financial details during trading or lending. For example, a DeFi exchange could use a ZK rollup (explained later) to match buy and sell orders and complete trades without showing every user's order in public. This would provide users with privacy, similar to traditional dark pools, while maintaining a fair and decentralized system. ZKPs are also very useful in auditing . Instead of giving auditors access to all sensitive transaction data, a financial institution could provide them with cryptographic proof showing that certain rules are followed, for example, that the company's liabilities are not greater than its assets, without sharing the actual numbers or client information. This idea is still new, but it fits well with privacy laws and the idea that auditors only need to see what's necessary. In the future, this type of zero-

knowledge auditing could enable auditors to verify whether a company is adhering to the rules by utilizing proofs, rather than requiring full access to all the data (Ajayi et al., 2024).

On the scalability side, zero-knowledge proofs are a key component of Layer 2 solutions, known as zk-rollups. A zk-rollup processes many transactions off the main blockchain and then creates a small cryptographic proof that confirms all those transactions were valid. This proof is then sent to the main chain, which only needs to verify the proof, rather than checking each transaction individually. This makes the system much faster and lighter, since one proof can confirm hundreds or even thousands of transactions. zk-rollups are already operational on Ethereum through projects like zkSync, StarkNet, and Polygon's zkEVM, demonstrating that these systems can handle high transaction volumes while maintaining the full security of the Ethereum network. This proof also ensures that, even though the actual work is done off-chain, the result remains correct and trusted. Some zk-rollups, such as Aztec Network, also incorporate encryption to maintain the privacy of transaction details while still benefiting from the speed and efficiency of rollups (Sun et al., 2021).

The potential of zero-knowledge proofs in blockchain is also gaining attention in academic research. A recent 2024 study in Security and Privacy noted that ZKPs can ease the computational load of verifying transactions, helping blockchains support more users and transactions while maintaining privacy and security. This means ZKPs can help blockchains grow without compromising decentralization, by performing the heavy work off-chain and simply proving it on-chain in a concise and reliable manner. From a privacy perspective, ZKPs enable blockchains to conceal certain data while still proving its validity, thereby avoiding the typical trade-off between openness and confidentiality. For example, a user could prove they are over 18 or have a sufficiently high credit score to access a financial service without sharing their actual age or credit report. This type of proof can help meet regulations such as KYC or AML in DeFi without compromising full control of personal information (Lei Zhou et al., 2024).

3. Results

3.1. Blockchain in DeFi vs. Auditing

This section compares how blockchain is utilized in decentralized finance and auditing, examining how each setting addresses performance, security, and practical applications. It focuses on key areas, including the number of transactions the system can handle, associated costs, trust and security management, data privacy levels, and the system's compliance with relevant rules and regulations. The aim is to highlight both the differences and similarities between what DeFi platforms require, such as open access and the ability to integrate multiple services, and what audit systems necessitate, including robust evidence that records are accurate and cannot be altered. Different blockchain technologies offer different strengths in meeting these needs.

3.2. Performance and Scalability

Throughput and latency are key performance measures for financial platforms, indicating the number of transactions a system can handle per second and the speed at which they are confirmed. Public DeFi platforms, such as those on Ethereum, have long struggled with low throughput. The Ethereum mainnet, operating under Proof-of-Work, could process only around 10 to 20 transactions per second, with 15 TPS often considered the real-world limit. This is far below centralized systems like Visa, which handles about 2000 TPS. When DeFi became popular, the Ethereum network often became crowded, causing delays and high transaction fees, making it hard for users with small transactions to participate. Ethereum's shift to Proof-of-Stake and the growth of Layer-2 solutions are helping to improve this. Rollups, both optimistic and zero-knowledge types, can increase throughput into the hundreds or more (Hu et al., 2019). However, optimistic rollups can add delay due to challenge periods lasting up to a week, while ZK-rollups confirm faster because their proofs are verified upfront. Regarding latency, Ethereum's block time is approximately 12 seconds, meaning a basic transaction can be confirmed in under a minute. However, in DeFi, actions often involve several on-chain steps, which adds to the total time (Hu et al., 2019).

Permissioned blockchains used in enterprise or audit settings typically offer significantly higher throughput and faster confirmation times compared to public chains. Hyperledger Fabric, for example, is built to run in controlled environments and can handle thousands of transactions per second. Tests and real-world deployments show that Fabric can reach over 2,000 TPS, with final confirmation times often under a second or within just a few seconds. Since there is no open mining process or need to broadcast to thousands of unknown nodes, these networks can utilize fast and efficient consensus methods, such as variations of Byzantine Fault Tolerance, among a small group of trusted participants. In an audit network with only about

10 nodes, such as a company, its auditors, and regulators, consensus can be reached almost instantly. Once the required number of nodes sign a block, the data is final (Hu et al., 2019). This setup works well for real-time auditing, where systems constantly feed data and auditors require immediate alerts if an issue arises.

Still, the performance gap between public and private blockchains is getting smaller as new technologies are developed. Public chains are improving their speed through techniques like sharding, which is planned for Ethereum and already used in networks like Polkadot and other modern Layer-1 blockchains. Layer-2 solutions that handle processing off the main chain are also helping public networks reach higher transaction speeds (Mohan, 2019). On the other hand, systems like Hyperledger Fabric can also face limitations, particularly as the number of participants increases or when the network spans different regions. Delays between nodes and the cost of maintaining full data consistency can slow down the process. A recent study has shown that, although Fabric performs significantly better than Ethereum in small setups, it may still be insufficient for very large-scale systems, such as national-level retail payments, without significant changes. For example, researchers developed a new version called Fabric-X, which achieved approximately 20,000 TPS by modifying certain aspects of the system, including how it verifies transactions and handles disk operations (Mohan, 2019). This indicates that while both public and private chains are improving, each still faces its own unique scalability challenges. Public chains handle the weight of decentralized consensus, while private chains must manage technical limitations in infrastructure and coordination as more members join.

In decentralized finance, transaction fees are a fundamental component of how the system operates. On Ethereum, every action in a smart contract consumes a resource called gas, and users must pay gas fees to have their transactions confirmed by the network. These fees can be very expensive, especially for complex operations such as adding liquidity or executing multi-step trades. In busy times, fees can rise to tens of dollars or more, making it difficult for smaller users or for use cases that require fast and frequent transactions. A change in 2021, known as EIP-1559, helped make fees more predictable; however, it didn't prevent them from spiking when the network was crowded (Zhang & Zhang, 2023). Due to this, cost efficiency is one of the primary reasons people utilize Layer-2 networks in DeFi. These systems handle most of the work off the main chain and only settle final results on-chain, which significantly reduces fees. Still, users do have to pay some cost to use Layer-2s, including a share of the final proof that gets posted to the main chain. Other blockchains, such as Solana or Binance Smart Chain, offer lower fees and higher speeds, but often with trade-offs in decentralization or security (Oh & Sukmana, 2025). Therefore, DeFi users and developers must decide what matters most when selecting a platform: low cost, strong security, or full decentralization.

In private or permissioned blockchain systems, transaction fees are typically absent, unlike those found in public blockchains. The network is run by known and trusted participants, and the cost of maintaining the system, including running servers and handling data, is covered internally by these members. This means users who are allowed to use the network can submit transactions for free, as long as they follow the rules and the system's capacity isn't exceeded. This setup feels more like using regular business software, where actions don't come with extra costs. It works well in situations with extremely high transaction volumes, such as tracking millions of events from sensors in a supply chain or an audit system. Since there are no miners, there's no need for financial incentives to keep the network running. Some networks may use collateral from members to ensure honesty, but this differs from the fee-based model on public chains like Ethereum. However, having no fees means there is a risk that people will overload the system with unnecessary activity. To prevent this, permissioned systems rely on access controls and agreed-upon rules to manage who can do what, instead of using fees to limit usage.

Efficiency in resource utilization also differs between public and private blockchains. Public chains, such as Ethereum, are built for trust without requiring central control, so every node executes every smart contract, even if it's redundant. This adds overhead but ensures no single party controls the outcome. In private blockchains, such as Hyperledger Fabric, roles are divided; for example, one set of nodes verifies transactions, while another simply records them, so not every node has to perform the same work. According to a review by John et al., removing a central authority in blockchain systems often increases setup and operation costs because more steps and checks are needed across multiple nodes. In DeFi, for instance, a trade that a central exchange could finish in seconds may take much longer on Ethereum due to multiple contract calls and confirmations across the network. In auditing, a simple database lookup might return results immediately, but checking the same data through a blockchain trail could involve generating cryptographic proof and multiple layers of verification, which slows down the process. So, in terms of raw performance, blockchains are generally less efficient than centralized systems. The trade-off is that blockchains offer better transparency, stronger data integrity, and less reliance on any single party. If those

benefits aren't critical, centralized systems are often faster and cheaper. That's why many DeFi and auditing solutions today are moving toward hybrid models, utilizing blockchain where it adds the most value, such as for trust and tamper-proof records, and combining it with off-chain or centralized tools for speed and usability.

3.3. Security and Trust Considerations

In public blockchains like Ethereum, which now uses proof-of-stake, security is based on economic incentives. To attack the network and alter the ledger, someone would need to control more than half of the total staking power, which is an extremely costly and difficult endeavor. This makes large networks like Ethereum very secure against tampering with transaction history. However, smaller or newer blockchains, especially those using proof-of-work, have been targeted in the past when an attacker was able to rent sufficient mining power or accumulate enough stake to control the network. In decentralized finance, if the base blockchain is attacked, everything built on top of it is also at risk. For example, an attacker could double-spend collateral or reorder transactions, causing significant damage. Ethereum's proof-of-stake system has different risks, like long-range or "nothing at stake" attacks, but these are managed through rules like slashing and finality checkpoints. In general, DeFi platforms need to build on a secure base layer to stay safe, which is why most major DeFi projects still use Ethereum. It has a strong record of security, while some smaller chains have seen hacks or system failures (Stephen & Alex, 2018).

Permissioned blockchains do not face mining-based attacks as public chains do; however, their security relies on a different model known as Byzantine fault tolerance. This means the system can continue to function correctly as long as no more than a certain number of participants, often up to one-third, act maliciously. In a typical audit network comprising a regulator and several firms, the assumption is that most of these parties are honest and will not collude to cheat the system (Leng et al., 2020). This is similar to how traditional audits operate, where a certain level of trust is expected and is backed by legal consequences for fraud. Blockchain can enhance this setup by ensuring that no single participant can alter records alone; others would detect and reject any tampering. Still, the system does require that a majority of members act in good faith. If most or all participants attempt to rewrite the ledger together, they may succeed, although this is less likely if the participants are competitors or subject to strict regulation. In contrast, public blockchains used in DeFi do not trust anyone by default, relying instead on the idea that attackers would need to spend a huge amount of money to take control (Chen et al., 2022).

Smart contract bugs are one of the biggest security risks in decentralized finance. Because DeFi systems are open to the public, attacks can come from anyone around the world, and they often do. In 2022 alone, reports estimate that around $3.8 billion was stolen from cryptocurrency and DeFi projects, primarily through bugs in smart contracts or weaknesses in their interaction with external data. Every new DeFi project introduces new risks, as its code may contain unique issues. To manage this, the DeFi community has established a robust culture of code reviews, audits, and reward programs for identifying bugs. Still, security breaches continue to happen regularly. One way to reduce risk is by limiting the capabilities of smart contracts. Some projects utilize features such as time delays or multisignature approval, allowing developers to halt the contract or transfer the funds if a problem is identified. However, this adds a layer of central control. There is always a balance between security and decentralization; contracts with no admin control are more independent but can be dangerous if they contain bugs, while contracts with admin access may be safer but require users to trust the people in charge (Stephen & Alex, 2018).

In blockchains used for auditing, smart contracts are often simpler and serve different purposes compared to those in decentralized finance (DeFi). They may be used to enforce business rules or automate checks, and are usually created by enterprises with standard software testing methods. The risk of outside attacks is lower since the network consists of known, trusted participants, rather than anonymous users. However, if there's a bug, it could still be misused, either by someone inside the network or by an outsider if the system is not properly secured. Zhang et al. (2025) highlight that once a flawed smart contract is running, it can be challenging to stop, as contracts are self-executing and often can't be easily modified. In a corporate audit setting, this could mean a contract that contains incorrect calculations might continue to yield inaccurate results until someone notices and the group agrees to correct them. On permissioned blockchains, updates are easier to coordinate because participants can work together to approve changes. Still, blockchain does not inherently make code secure. Careful development, testing, and growing use of tools that mathematically verify smart contracts for errors are all necessary, especially in high-stakes situations such as financial systems (Leng et al., 2020).

Oracle and external data risks affect both DeFi and auditing blockchains, but in different ways. In DeFi, these risks are more severe because public data feeds, often sourced from centralized exchanges or price sites, directly influence smart contract actions, such as loan liquidations. Attackers have taken advantage of this by manipulating low-volume markets or feeding fake prices to trick oracles. In auditing systems, oracles may be connected to a company's IT systems or IoT devices. These can still be hacked or misused, but the risks typically arise from insiders or compromised hardware, and such issues may be easier to detect using cross-checks from multiple data sources. In permissioned audit blockchains, the data providers are known and legally responsible, such as a shipping company sending GPS data. If they send false data, they could face legal or contractual penalties. In contrast, DeFi is an oracle operator that could act dishonestly and simply disappear with the money. So, while both areas face oracle risks, the response is different. DeFi is working on decentralized oracle networks and reward systems to make data more trustworthy, while enterprise systems focus on connecting reliable sources and sometimes utilize trusted hardware to ensure the accuracy of the data. (Leng et al., 2020).

Privacy works very differently in DeFi compared to enterprise or audit systems. In DeFi, everything is public by default; users are only identified by wallet addresses, but all trades, balances, and actions are visible on the blockchain. While this openness allows anyone to monitor risk and spot problems early, it also means users have very little privacy. Sensitive strategies or holdings can be exposed, and most DeFi apps don't include privacy tools unless added separately. Some newer projects are attempting to address this issue by utilizing technologies like zkSNARKs to develop private trading or lending systems (Chen et al., 2022). In these cases, only the people involved see the details, but others can still verify that the system is functioning correctly. These solutions are still being tested, but they demonstrate a growing interest in introducing more privacy to DeFi without compromising trust and transparency.

In auditing, privacy is a key requirement because financial records and personal data are highly sensitive. A blockchain used for audits must ensure that only authorized users, such as specific auditors, can access certain information. Permissioned blockchains help by limiting who can access the network, but even within that group, not everyone should have access to everything. For example, one company should not be able to view a competitor's data, even if both are part of the same system. Tools like Fabric's channels or data encryption on-chain help manage this. Zero-knowledge proofs can also be used, allowing an auditor to confirm that data meets certain rules without needing to view the raw data. This means that blockchain solutions for auditing are typically designed with robust privacy features from the outset. In contrast, DeFi has focused more on transparency and open access, where user activity is publicly visible. As privacy laws like GDPR or banking regulations grow stricter, enterprise blockchains may need to store private data off-chain and only put secure references (like hashes) on-chain. Overall, public DeFi tends toward openness and flexibility, while audit-focused systems prioritize confidentiality and controlled access, even if it means sacrificing some decentralization (Xu et al., 2019).

Resilience and system continuity are crucial in both DeFi and auditing blockchains, but the approaches each takes to address them differ. Public blockchains, such as those used in DeFi, rely on extensive global networks of nodes. This makes them highly resistant to failure; there is no single point that can bring the entire system down, and as long as most nodes are honest, the network remains operational. DeFi protocols often enhance decentralization by utilizing governance tokens, which enable users to vote on changes and rules (Makarov & Schoar, 2022). On the other hand, audit blockchains are run by a smaller group of known participants, so they don't need thousands of nodes. Instead, they often follow standard business practices for backup and recovery. If a node fails or a key is lost, network members can coordinate to restore service, rotate keys, or recover data from backups. In DeFi, unique risks can arise from the governance system itself, such as an individual acquiring enough tokens to influence decisions, potentially allowing them to alter the rules in harmful ways. Therefore, DeFi must consider not only technical security but also protection against economic attacks. In contrast, audit systems focus more on traditional IT concerns, such as access control, identity management, and system recovery, all of which are key components of running a secure blockchain within a business setting (Carter & Jeng, 2021).

4. Discussion

4.1. Implementation Challenges

While blockchain technologies offer compelling advantages for secure financial transactions, numerous implementation challenges must be addressed to fully realize their potential in both DeFi and auditing domains. Some challenges are technical, including scalability limitations, interoperability issues, and ensuring security in complex smart contract systems. Others are organizational and human-centric, such as

the need for skilled personnel, changes to business processes, and regulatory acceptance. In this section, we discuss the key challenges that practitioners and researchers face when deploying blockchain-based financial solutions, drawing on insights from current literature.

4.2. Scalability and Throughput Limits

Even with new technologies, making blockchains faster and more scalable remains a significant challenge, particularly for public blockchains like Ethereum. These systems can only handle a small number of transactions per second and require a significant amount of computer power (Xie et al., 2019). This makes them difficult to use for applications such as high-speed trading or large-scale payment systems. Layer-2 solutions and newer blockchains attempt to address this by handling more work off the main chain; however, using them can be confusing and adds extra steps, such as moving tokens between networks. In private blockchains used by businesses or auditors, it's also tricky to grow the network without slowing it down. When more participants are added, it can take longer for everyone to agree on transactions. Another problem is that blockchains store every transaction permanently, which means the data grows rapidly and can be difficult to manage. Some projects are testing ways to store only important data on-chain and keep the rest off-chain, but this approach makes the system more complex (Paik et al., 2019). Researchers are working on innovative methods to break down the data (such as sharding) and reduce the size of proofs (utilizing zero-knowledge proofs), but these approaches are still in development. For now, many projects focus on using blockchain for just the most critical steps, such as final settlement, while handling other parts off-chain to stay fast and efficient.

4.3. Smart Contract Complexity and Security

As financial logic moves on-chain, ensuring the correctness and security of that logic is challenging. Smart contracts often handle large amounts of value, making them attractive targets for hackers. The variety of potential bugs is wide (reentrancy, arithmetic overflow, logic errors, front-running issues, etc.), and tooling for secure smart contract development is still developing. While there are static analyzers and formal verification tools, they require specialized expertise to be used effectively. Additionally, contracts in DeFi are often composed together (one protocol uses another's contracts), creating interdependent systems where a bug in one can cascade into others. The "composability" that is a strength of DeFi is also a risk – it's akin to the interconnectedness of financial institutions that can lead to systemic risk. Recent incidents, such as the cascade of liquidations triggered by a platform's failure, affecting others, illustrate this. A challenge is how to implement effective risk controls in a decentralized context. Traditional finance has circuit breakers and oversight bodies; DeFi may need algorithmic versions of these (for example, contracts that halt trading if abnormal conditions are detected). For enterprise use, while contracts might be simpler, the challenge lies in integrating them with legacy systems without introducing vulnerabilities. Smart contracts must be fed correct input data and their outputs correctly interpreted by off-chain systems; any gap can be exploited (for example, an attacker might focus on the interface between a corporate database and the blockchain itself) (Li et al., 2022; Wang et al., 2022; Liyi Zhou et al., 2023).

4.4. Integration and Interoperability

Most financial organizations have complex legacy systems. Replacing or interfacing these with blockchain platforms is a major challenge. On a technical level, interoperability is necessary between different blockchains (such as a company's private ledger and a public chain for specific transactions) and between blockchains and traditional systems (e.g., ERP, databases). Standards for data formats, APIs, and identity are crucial but still in flux. Projects like Hyperledger Cactus are attempting to provide interoperability frameworks. In auditing, one challenge is integrating blockchain-based records with existing audit software and workflows. Auditors might need dashboards that combine on-chain verification results with off-chain evidence management. Without seamless integration, blockchain could add, rather than remove, friction in audit processes. Interoperability between blockchains is also crucial in DeFi – many DeFi platforms utilize cross-chain bridges to transfer assets between networks. These bridges have proven to be points of vulnerability (numerous bridge hacks have occurred). A challenge is designing secure, ideally trust-minimized, interoperability protocols that allow a financial model to span multiple platforms. This is important because different blockchains offer distinct advantages (one might be faster, another more liquid, etc.), and a holistic financial system may want to leverage all of them.

4.5. Regulatory Uncertainty and Legal Challenges

Laws governing blockchain and smart contracts are still unclear in many jurisdictions. For DeFi, this is a big problem. Projects often span multiple countries, with no clear rules on who is responsible or what is legally permissible. Big financial companies want to know how to follow the rules, such as verifying who their users are or protecting consumers, but DeFi doesn't always make that easy. If a government decides that a certain DeFi service is illegal, individuals using it could face legal trouble, even if the code itself is open-source and no one controls it. In auditing, regulators might ask: "Is a blockchain record enough proof?" or "Does it meet our standards?" There's also the question of which country's law applies when a smart contract is used globally. What happens if there's a disagreement? Right now, there are no clear answers. Some people are working on ways to link legal contracts with code, for example, Ricardian contracts, but the law and blockchain still don't fit together well. Until legal rules catch up, many businesses may hesitate to use blockchain for their most critical financial tasks.

4.6. Human Capital and Expertise

To build blockchain systems for finance or auditing, it needs individuals who understand both the technical and financial aspects. Currently, there aren't enough experts who possess both knowledge. Many blockchain developers lack a comprehensive understanding of finance and auditing, while finance professionals often have limited knowledge of cryptography and blockchain technology. A study by Zhang et al. (2025) highlighted that this lack of knowledge, particularly in cryptography, poses a significant challenge in audit work. Auditors and accountants may require new training to effectively utilize blockchain tools. At the same time, blockchain engineers need to understand how finance works to design effective systems. To address this, companies and schools are launching programs to educate individuals on all three aspects – technology, finance, and law. However, until more people are trained, blockchain projects can be slowed down or cause serious mistakes if the wrong individuals design them. That's why it's essential to have mixed teams, comprising tech professionals, finance experts, and legal professionals working together from the outset.

4.7. User Experience and Adoption

In DeFi, using blockchain applications remains challenging for many people (Tharani & Zelenyanszki, 2022). It needs to manage private keys, understand how wallet apps work, and pay gas fees to make transactions. Many users lose money because they forget their login credentials or fall victim to scams. Even if the smart contract is safe, if the wallet is hacked, the money is gone. In business, the way people use blockchain matters. If accountants must use complex tools or learn coding just to check records, they probably won't use it. Blockchain needs to work with the tools people already know. Additionally, businesses will only adopt blockchain if it clearly helps them save money or work more efficiently. For DeFi, people will use it more if it gives better results than normal finance and becomes easier to use. Making the user experience simpler, such as through easier apps, better designs, and teaching people how to use them, is just as important as building the technology..

4.8. Security of Infrastructure

Beyond smart contracts, the surrounding infrastructure (nodes, wallets, exchanges, oracles) must be secure. Many attacks target not the blockchain itself but the endpoints – e.g., hacking an exchange or a wallet to get private keys. In enterprise blockchains, if an adversary compromises one organization's node, they might tamper with data that that node is responsible for submitting (Gupta et al., 2023). Ensuring robust cybersecurity practices around blockchain deployments is critical. This includes key management (use of HSMs or multi-signature schemes), network security (preventing DDoS attacks on nodes), and continuous monitoring. The nice property is that blockchains usually make data tampering evident (due to consensus rules), but an attacker could still disrupt availability or attempt to insert fraudulent transactions if they gain control of a participant's credentials. As blockchain use grows, it becomes part of the larger attack surface of financial systems; thus, it must adhere to the same, if not higher, security standards as other mission-critical systems (Li et al., 2022; Wang et al., 2022; Liyi Zhou et al., 2023).

5. Conclusions and Future Research

5.1. Conclusions

Blockchain has introduced a new way to manage and record financial transactions. This review examined the application of blockchain in decentralized finance (DeFi) and financial auditing. It focused on performance, security, and real-world challenges. In DeFi, platforms like Ethereum have demonstrated that complex financial services can be executed without the need for banks or intermediaries. Smart contracts enable the trading, lending, and issuance of assets using only code. These systems offer transparency and global access, but they also face challenges such as high fees, slow speeds, and security risks. Ethereum's upgrades, such as Proof-of-Stake and Layer 2 networks, aim to address these issues. Security audits are also crucial for establishing trust in decentralized finance (DeFi) systems. For auditing and enterprise finance, blockchain's features, such as tamper-proof records and shared ledgers, can enhance trust and efficiency. Some companies have achieved significant time savings by using blockchain for auditing tasks. However, there are still problems: blockchains don't easily connect to real-world events (oracle problem), traditional systems are difficult to integrate, and rules for using blockchain in audits are still in development.

This paper compares public blockchains, such as Ethereum, to private ones, like Hyperledger Fabric. Public chains offer openness but are slower and less private. Private chains are faster and more secure but require trust in known participants. Each has different use cases. A mix of both, a hybrid model, may be the future, where public chains handle settlement, and private ones manage transactions. Key challenges remain scaling, security, regulation, and connecting different systems. But progress is happening. New tools, such as zero-knowledge proofs and improved scaling methods, are becoming a reality. These can help blockchains offer both privacy and performance. Regulators are also starting to respond and create new rules for blockchain use. Looking forward, a team effort is needed. Developers, finance experts, auditors, and regulators must collaborate to create secure, compliant, and practical systems. Some experts suggest establishing shared standards and training individuals in both technology and finance. This could lead to a more trusted and efficient financial system. In short, blockchain already shows strong potential in both DeFi and auditing. With continued progress and collaboration, it could become a key part of everyday finance and trust-building in the financial world. A future where both decentralized and traditional systems work together is not only possible but also already starting to take shape.

5.2. Future Research

Blockchain is rapidly transforming the way financial systems are perceived. As seen in earlier sections, there are significant opportunities, as well as substantial challenges. This section examines the next steps for research and development to address current issues and unlock new applications in both decentralized finance (DeFi) and blockchain-based auditing. These ideas include technical upgrades, enhanced teamwork across various fields, and refined rules and standards.

1. Scaling Solutions and Performance Enhancements: One of the biggest goals is making blockchains faster and able to handle more transactions without losing security or decentralization. A lot of attention is on "Layer-2" solutions, which help move most activities off the main blockchain to reduce traffic. New rollup systems, especially those utilizing zero-knowledge proofs, are becoming more advanced and can support more complex applications. Ethereum, for example, is working on a feature called "sharding" to divide the network into smaller parts that operate in parallel; however, further work is needed to ensure these parts communicate effectively with each other. For private blockchains, researchers are exploring methods to accelerate transactions using advanced hardware, such as GPUs. Some are even exploring new types of blockchain systems, such as DAGs or other non-linear methods, which may offer significantly higher speeds. Additionally, it's essential to have fair ways to measure performance, so new tools are being developed to test how fast and efficient these systems truly are.
2. Smart Contract Security and Verification: Smart contracts are powerful but risky. Bugs in the code can lead to big losses. Future research focuses on making contracts safer by utilizing tools that can verify the logic before the contract is deployed. Some languages are being built to help developers write contracts that can be mathematically checked to avoid errors. Others are working on tools that utilize AI to identify bugs in code by recognizing patterns observed in previous hacks. There is also interest in creating contracts that can monitor themselves and shut down or alert someone if something appears to be wrong. Insurance for smart contracts is growing too. Some DeFi projects already offer coverage in case of hacks. In the future, smart contract audits may become more similar to traditional IT audits, with standardized methods and clear reporting.

3. Interoperability and Cross-Chain Finance: In the future, we'll likely have many blockchains working together. This means that assets and data should be able to move easily between different networks, including public, private, and enterprise networks. Research is ongoing to develop bridges and standards that enable this and ensure security. Projects like Cosmos and Polkadot are already working on these ideas. One exciting path is to use zero-knowledge proofs to enable one blockchain to prove to another that something has happened, without sharing all the details. This could help link private audit systems with public financial apps. It also means connecting with existing company systems using middleware and APIs. But to make all this work, we'll also need shared rules about how data should be formatted and how digital assets should be identified.
4. Privacy-Enhancing Technologies: Keeping a balance between privacy and transparency is another big topic. Zero-knowledge proofs are likely to play a bigger role, not just in scaling, but also in hiding sensitive information while still proving that a rule was followed. Some DeFi apps are already working on this, such as exchanges where trades are hidden but still transparent and fair. In auditing, we may encounter systems where a company can verify the accuracy of its financial data without providing every detail. This could enable a new type of audit that respects privacy while ensuring accuracy. Confidential computing, which lets encrypted data be processed in secure hardware, may also be combined with blockchain in the future.
5. Regulatory Technology (RegTech) and Governance: It's not just about technology. We also need better rules and systems to manage the operation of blockchain networks. In DeFi, an increasing number of projects are being managed by DAOs (decentralized autonomous organizations). However, we still need to study how these groups operate, how to prevent attacks on their governance, and how to grant them legal status. In enterprise systems, governance is about sharing control fairly across different companies and maintaining the system's integrity. Research is needed on how groups, such as audit firms, could share a blockchain and establish trust in it. We also need to establish guidelines for handling blockchain data in reports and audits. Governments and regulators are testing blockchain, for example, by using it for tax purposes or digital currencies. In the future, we may see smart contracts that follow rules by design, automatically blocking illegal actions.
6. Cross-Disciplinary Collaboration: Many of these problems need people from different backgrounds to work together. For example, building a legal and functional smart contract for a complex financial product requires expertise from finance, legal, and development professionals. More universities are creating programs that mix blockchain with business, law, and tech. Research papers on blockchain are now appearing in top finance and accounting journals. This mix of knowledge can lead to better designs, such as incorporating economic ideas into fair governance models or utilizing risk models to design safer blockchains.

Thus, blockchain has a bright future in finance and auditing. Areas such as speed, security, privacy, and regulation are improving rapidly. Over the next few years, many of the current problems could be addressed. We may see central banks utilizing blockchain for digital currencies or large firms employing it regularly for audits. If all parts come together, technology, law, policy, and education, blockchain could become a strong base for a more open, safe, and efficient financial system. The future will likely combine decentralized tools with traditional systems, working together to enhance the way finance works for everyone.

Author Contributions: Conceptualization, D.D.K.; methodology, D.D.K.; software, D.D.K.; validation, D.D.K.; formal analysis, D.D.K.; investigation, D.D.K.; resources, D.D.K.; data curation, D.D.K.; writing—original draft preparation, D.D.K.; writing—review and editing, D.D.K.; visualization, D.D.K.; project administration, D.D.K.; funding acquisition, D.D.K. Author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to thank Saint Louis University, USA, for supporting this research and publication. We also thank the reviewers for their constructive comments and suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

References

Ajayi, A. A., Emmanuel, I., Soyele, A. D., & Enyejo, J. (2024). Enhancing digital identity and financial security in decentralized finance (DeFi) through zero-knowledge proofs (ZKPs) and blockchain solutions for regulatory compliance and privacy. *Iconic Res. Eng. J*, *8*(4), 373–394.

Bagirovs, E. (2025). *Blockchain Security in Decentralized Finance (DeFi)*. JAMK University of Applied Sciences.

Bez, M., Fornari, G., & Vardanega, T. (2019). The scalability challenge of ethereum: An initial quantitative analysis. *2019 Ieee International Conference on Service-Oriented System Engineering (Sose)*, 167–176.

Bhambhwani, S. M., & Huang, A. H. (2024). Auditing decentralized finance. *The British Accounting Review*, *56*(2), 101270.

Breidenbach, L., Cachin, C., Chan, B., Coventry, A., Ellis, S., Juels, A., Koushanfar, F., Miller, A., Magauran, B., Moroz, D., Nazarov, S., Topliceanu, A., Tramer, F., & Zhang, F. (2021). *Chainlink 2.0: Next steps in the evolution of decentralized oracle networks* (Vol. 1). Chainlink Labs. https://research.chain.link/whitepaper-v2.pdf

Buhler, M. (2025). *Enhancing multi-signature cryptocurrency wallets with risk-based authentication* [University of Calgary]. https://hdl.handle.net/1880/120367

Carter, N., & Jeng, L. (2021). DeFi protocol risks: The paradox of DeFi. *Regtech, Suptech and beyond: Innovation and Technology in Financial Services" Riskbooks–Forthcoming Q*, *3*.

Chen, T., Lu, H., Kunpittaya, T., & Luo, A. (2022). A review of zk-snarks. *ArXiv Preprint ArXiv:2202.06877*.

Gueye, N. S., & Chaifetz, R. (2025). Multi-Criteria Optimization of Financial Management in Digital Marketing for Large Enterprises using Fuzzy Decision-Making Systems. *International Journal of Advance Research and Innovation*, *10*(5). https://www.researchgate.net/profile/Ndeye-Siga-Gueye/publication/392982111_Multi-Criteria_Optimization_of_Financial_Management_in_Digital_Marketing_for_Large_Enterprises_using_Fuzzy_Decision-Making_Systems/links/685b8900e8fa0f5c282684f1/Multi-Criteria-Optimization-of-Financial-Management-in-Digital-Marketing-for-Large-Enterprises-using-Fuzzy-Decision-Making-Systems.pdf

Gupta, A., Gupta, R., Jadav, D., Tanwar, S., Kumar, N., & Shabaz, M. (2023). Proxy smart contracts for zero trust architecture implementation in Decentralised Oracle Networks based applications. *Computer Communications*, *206*, 10–21.

Hu, Y., Manzoor, A., Ekparinya, P., Liyanage, M., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2019). A delay-tolerant payment scheme based on the ethereum blockchain. *Ieee Access*, *7*, 33159–33172.

John, K., Kogan, L., & Saleh, F. (2023). Smart contracts and decentralized finance. *Annual Review of Financial Economics*, *15*(1), 523–542. https://doi.org/10.1146/annurev-financial-110422-102455

Kadeba, O. (2024). How open data is reshaping supply chains for social equity. *International Journal of Advance Research, Ideas and Innovations in Technology*, *10*(1), 147–155. https://www.ijariit.com/manuscripts/v10i1/V10I1-1200.pdf

Kaur, G., & Gandhi, C. (2020). Scalability in blockchain: Challenges and solutions. In *Handbook of Research on Blockchain Technology* (pp. 373–406). Elsevier.

Leng, J., Zhou, M., Zhao, J. L., Huang, Y., & Bian, Y. (2020). Blockchain security: A survey of techniques and research directions. *IEEE Transactions on Services Computing*, *15*(4), 2490–2510.

Li, W., Bu, J., Li, X., & Chen, X. (2022). Security analysis of DeFi: Vulnerabilities, attacks and advances BT. *2022 IEEE International Conference on Blockchain (Blockchain)*, 488–493.

Makarov, I., & Schoar, A. (2022). Cryptocurrencies and decentralized finance (DeFi). *Brookings Papers on Economic Activity*, *2022*(1), 141–215.

Mohan, C. (2019). State of public and private blockchains: Myths and reality. *Proceedings of the 2019 International Conference on Management of Data*, 404–411.

Oh, L. K., & Sukmana, H. T. (2025). A Comprehensive Study on Public and Private Blockchain Performance. *Journal of Current Research in Blockchain*, *2*(1), 13–27.

Paik, H.-Y., Xu, X., Bandara, H. M. N. D., Lee, S. U., & Lo, S. K. (2019). Analysis of data management in blockchain-based systems: From architecture to governance. *Ieee Access*, *7*, 186091–186107.

Rashid, M., Rasool, I., Afzaal, H., & Zafar, N. A. (2025). Formal verification of safety properties of epoch processing in Beacon Chain. *Scientific Reports*, *15*(1), 43522. https://doi.org/10.1038/s41598-025-27396-w

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review*, *103*(2), 153–174. https://doi.org/10.20955/r.103.153-74

Scherer, M. (2017). *Performance and scalability of blockchain networks and smart contracts*. Umea University.

Segun Adanigbo, O., Sophia Ezeh, F., Success Ugbaja, U., Iyabode Lawal, C., & Christopher Friday, S. (2024). Advances in Blockchain and IoT Applications for Secure, Transparent, and Scalable Digital Financial Transactions. *International Journal of Advanced Multidisciplinary Research and Studies*, *4*(6), 1863–1869. https://doi.org/10.62225/2583049X.2024.4.6.4158

Stephen, R., & Alex, A. (2018). A review on blockchain security. *IOP Conference Series: Materials Science and Engineering*, *396*(1), 12030.

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network*, *35*(4), 198–205. https://doi.org/10.1109/MNET.011.2000452

Szabo, N. (2017). *Winning Strategies for Smart Contracts*. Blockchain Research Institute. https://grazielabrandao.wordpress.com/wp-content/uploads/2019/06/g86cmijoeemm8wp4g3tktg_1c16c8a028ce11e999f58be72bb04114_szabo-smart-contracts-v6d_1_.pdf

Tharani, J. S., & Zelenyanszki, D. (2022). A UI/UX Evaluation Framework. *Blockchain–ICBC 2022: 5th International Conference, Held as Part of the Services Conference Federation, SCF 2022, Honolulu, HI, USA, December 10–14, 2022, Proceedings*, *13733*, 48.

Vera-Rivera, A. (2022). *Design and implementation of a blockchain-based task sharing service for edge computing servers using the Hyperledger Fabric platform* [University of Manitoba]. https://mspace.lib.umanitoba.ca/server/api/core/bitstreams/601d645c-1049-4e65-b258-2334ca403878/content

Wang, Y., Zuest, P., Yao, Y., Lu, Z., & Wattenhofer, R. (2022). Impact and user perception of sandwich attacks in the DeFi ecosystem BT -. *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–15.

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A survey on the scalability of blockchain systems. *IEEE Network*, *33*(5), 166–173.

Xu, Y., Ren, J., Zhang, Y., Zhang, C., Shen, B., & Zhang, Y. (2019). Blockchain empowered arbitrable data auditing scheme for network storage as a service. *IEEE Transactions on Services Computing*, *13*(2), 289–300.

Zhang, L., & Zhang, F. (2023). Understand waiting time in transaction fee mechanism: An interdisciplinary perspective. *ArXiv Preprint ArXiv:2305.02552*.

Zhang, Y., Ma, Z., & Meng, J. (2025). Auditing in the blockchain: a literature review. *Frontiers in Blockchain*, *8*, 1549729. https://doi.org/10.3389/fbloc.2025.1549729

Zheng, P., Zheng, Z., Wu, J., & Dai, H.-N. (2020). XBlock-ETH: Extracting and Exploring Blockchain Data From Ethereum. *IEEE Open Journal of the Computer Society*, *1*, 95–106. https://doi.org/10.1109/OJCS.2020.2990458

Zhou, Lei, Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, *80*, 103678. https://doi.org/10.1016/j.jisa.2024.103678

Zhou, Liyi, Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., & Gervais, A. (2023). SoK: Decentralized finance (DeFi) attacks BT - 2023 IEEE Symposium on Security and Privacy (SP). *2023 IEEE Symposium on Security and Privacy (SP)*, 2444–2461.