



Blockchain-Based Smart Contracts and Their Potential to Develop Some Financial and Banking Operations in Iraq

Laith Haleem Al-Hchemi^{1,*}

¹ University of Al-Qadisiyah, Diwaniyah City, Iraq

Email: laith.haleem@qu.edu.iq

Received: November 20, 2024 Revised: December 28, 2024 Accepted: January 23, 2025 ★ Corresponding author

ABSTRACT

This research explores the great potential of blockchain-based smart contracts in Iraq's financial and banking sector. It looks into how this technology can improve financial operations by automating transactions, reducing operational cost, increasing transparency, and reducing intermediaries. The research also tackles the challenges of adoption, such as the lack of digital infrastructure and legal frameworks and the presence of cybersecurity risks. The findings show that smart contracts can lead to higher operational efficiency and more strategic flexibility for financial institutions in Iraq. Therefore, the research recommends developing digital infrastructure and establishing comprehensive regulatory frameworks to support smart contracts and digital transformation in the financial and banking sector according to international standards.

Keywords: Blockchain ▪ Digital infrastructure ▪ Cybersecurity risks

1. INTRODUCTION

In the last few decades, the world has witnessed rapid technological advancements that have changed many sectors, with the financial and banking industry leading the pack. Financial institutions are adopting innovative technologies to improve their performance and efficiency and meet the demands of customers in a digital world. Among these technologies, blockchain has emerged as a game changer that has redefined data storage and verification through its decentralized architecture, robust security, and transparency in transactions. Blockchain operates on an immutable and shared digital ledger, providing a transparent environment for storing and sharing information without a central authority, as well as advanced encryption and protection.

With the rise of blockchain, many applications have surfaced, most notably "smart contracts." These contracts are seen as a solution with vast potential to develop and automate financial processes. Smart contracts, with their ability to execute

operations independently without human intervention, open up new avenues to create new financial models, reduce costs, and speed up transactions. The focus on these technologies highlights their potential to support digital transformation in the financial sector and make processes more efficient and adaptable, especially in countries that want to sustain their financial institutions.

In Iraq, the need to adopt modern technologies has become crucial to drive progress in the financial sector and keep up with global market changes. Adopting smart contracts is a strategic step toward improving the performance of financial and banking institutions in the country. This technology offers opportunities to enhance transparency and security, improve operational efficiency, and reduce dependence on traditional methods that hinder sector growth. As awareness of digital transformation rises, adopting such tools is imperative for Iraqi institutions to build advanced infrastructure that can meet the aspirations of the digital economy. This adoption will position Iraq to strengthen its financial competitiveness

and leverage technology for sustainable economic growth according to global standards and trends.

Against this backdrop, this research aims to provide a comprehensive understanding of the role of smart contracts in reshaping the financial and banking infrastructure in Iraq. It explores the capabilities of smart contracts and evaluates the benefits they can bring to financial performance while addressing the technical, legal, and economic challenges that may hinder their application. Moreover, the study examines the impact of this technology on Iraq's digital economy and proposes a forward-looking vision to enable the Iraqi financial sector to fully harness the potential of smart contracts amid the existing challenges. Through this analysis, the research seeks to provide practical insights that can guide financial institutions and policymakers in adopting effective strategies to support Iraq's digital transformation, align with global economic demands, and enhance the country's regional and international competitiveness.

2. BLOCKCHAIN

2.1 An Overview of Blockchain

Blockchain technology represents a groundbreaking and remarkable shift in how data are stored and information is exchanged in a decentralized way. This concept goes back to the early 1990s, when researchers Stuart Haber and W. Scott Stornetta developed a system in 1991 to protect digital records using what are called digital timestamps. This system ensured that digital documents could not be altered or forged; it was a powerful tool for digital data integrity (Haber & Stornetta, 1991). While this laid the foundation for advanced protection mechanisms in digital record keeping, the practical and widespread application of the concept was realized only with the birth of the cryptocurrency Bitcoin in 2008.

Introduced by an individual or group under the pseudonym "Satoshi Nakamoto," Bitcoin was the first real-world implementation of blockchain technology (Nakamoto, 2008). This was not only a breakthrough in digital currency, but also the foundation of a reliable way to record transactions in a decentralized, transparent, and secure manner. It has since become the backbone of many advanced digital applications.

Blockchain technology works through a sequential structure of units called "blocks." Each block contains a collection of transaction data, such as sender and receiver identifiers and the timestamp of the operation. These blocks are linked through a unique identifier called a "hash," which is an encrypted code linking one block to the previous one. This sequential linkage ensures data integrity and prevents attempts to alter or manipulate records without alerting the rest of the network participants. If any modification occurs in one block, the entire hash chain is affected, so the network can detect changes easily. This interconnectivity makes the system trustworthy and resistant to tampering, as all nodes in the network maintain a copy of the distributed ledger. Nodes—all the computing devices participating in data verification and recording in the blockchain network—play a crucial role in decentralization and system robustness (Zheng et al., 2017).

Transaction validation in blockchain networks relies on what is called the "consensus mechanism," the core process of

the network. This mechanism uses complex mathematical models and software to verify every transaction added to the network and requires approval from the majority of nodes. One of the most popular consensus mechanisms is Proof of Work (PoW), which requires participating nodes to perform complex mathematical computations for every transaction on the network. This ensures transaction security and completion, making it extremely difficult to alter any information in the blocks without controlling more than half of the network's active nodes—a process that is technically difficult and very costly (Vukolić, 2015).

2.2 Types of Blockchain

The development of blockchain and its increasing use across many industries have led to different types of blockchain, each with its own structure and technical features suited to modern applications.

2.2.1 Public Blockchain

This is the most widely used type of blockchain and is employed in cryptocurrencies such as Bitcoin, Ethereum, and Litecoin (Swan, 2015). Public blockchains are open-source and transparent; all network users can view and verify transactions. They are fully decentralized, with no single entity controlling or monopolizing the network. However, public blockchains face challenges such as slow data processing and high operational cost due to their large network size (Nofer et al., 2017).

2.2.2 Private Blockchain

Private blockchains are not public and are governed by a central entity, such as an organization or company. Access is restricted to authorized individuals (Pilkington, 2016). They are faster and cheaper in transaction processing because they do not require approval from many nodes. Private blockchains are easier to manage and control, but they can be manipulated if they are not managed transparently (Drescher, 2017).

2.2.3 Consortium Blockchain

Also known as federated blockchain, this type is a middle ground between public and private blockchains and is managed by a consortium of participating organizations or entities. It is used in industrial alliances, banking systems, and inter-company networks. Consortium blockchains offer fast transaction processing and operational efficiency while maintaining internal transparency among members. However, they can face challenges in scalability and trust management among diverse participants (Zyskind et al., 2015).

2.2.4 Hybrid Blockchain

Hybrid blockchains combine features of public and private blockchains, allowing controlled access to some data while keeping other data transparent. This makes them suitable for applications that require flexibility in data management (Xu et al., 2019). They are used in scenarios that require a balance between transparency and privacy, such as government data and healthcare systems. Hybrid blockchains are effective at dynamically customizing data according to need, but require technically complex designs to harmonize their public and private components (Khan et al., 2021).

3. SMART CONTRACTS

3.1 The Concept of Smart Contracts

Smart contracts represent one of the most sophisticated applications of blockchain technology. They have the potential to transform conventional contracts from an analog to a digital format because their conditions are executed automatically without intervention by a third party or central authority, leading to a substantial reduction in the time and cost associated with intermediaries.

The conceptualization of smart contracts can be traced back to the early 1990s and the writings of computer scientist Nick Szabo, who defined smart contracts as digital protocols intended to ensure the automatic execution of agreements among different parties. Once participants have a sufficiently transparent and trustworthy mechanism with which to interact, there is no need for intermediaries (Szabo, 1997). Several years of theoretical development underscored the need for a decentralized environment capable of supporting the practical implementation of these concepts.

Smart contracts could only be implemented in practice using blockchain technology, which changed the way digital transactions are documented in a decentralized manner. Early blockchain networks such as Bitcoin were conceived to facilitate financial transactions. The system initially focused on recording and securing financial transactions in an intermediary-free environment, but its limited series of Boolean commands was insufficient for business applications. Consequently, smart contracts could not function fully during the initial stages of their development.

Vitalik Buterin addressed this limitation in 2015 through the establishment of the Ethereum network, which was specifically designed to support smart contracting and overcome drawbacks in traditional blockchain architecture. The development of the Solidity programming language gave developers the ability to build smart contracts capable of running complex, self-executing instructions within the system (Jaganathan et al., 2023). This flexible platform enabled developers to create decentralized applications (DApps), which rely heavily on smart contracts. These applications now extend beyond cryptocurrencies to decentralized finance (DeFi), insurance contract management, supply chain management, and other fields. Ethereum therefore became more than a cryptocurrency platform; it grew into a complete ecosystem with smart-contract capabilities and support for innovative applications requiring secure and reliable execution. With these advances in place, smart contracts gained a firm footing in various sectors by offering decentralized technological solutions that improve efficiency and transparency. Their widespread acceptance indicates their future role in emerging technologies.

3.2 Characteristics of Smart Contracts

3.2.1 Decentralization and Elimination of Intermediaries

Decentralization is a crucial feature of smart contracts because there is no centralized authority performing tasks such as validating or executing transactions. Allowing all participants to access contract information removes intermediaries and their associated transaction costs, making business operations more efficient. This decentralized capability inherently

limits opportunities for fraud or mismanagement by intermediaries. According to Teng (2022), decentralization makes smart contracts reliable and fast, thereby increasing transaction efficiency.

3.2.2 Automatic Execution of Transactions

One of the biggest advantages of smart contracts is their ability to execute transactions automatically. These contracts are built on programmed rules that ensure the conditions of an agreement are met without human intervention. As Hillbom and Tillström (2016) explain, this reduces the chance of errors or delays, making transactions faster and more streamlined.

3.2.3 Encryption and Security

Encryption is a foundational element of smart contracts and uses robust cryptographic methods to secure data and transactions. Built on blockchain technology, smart contracts are resistant to tampering or unauthorized alterations. As noted by Mohanta et al. (2018), encryption safeguards sensitive information related to the contract, ensuring the confidentiality and security of the data.

3.2.4 Speed

Transaction speed is a key feature that differentiates smart contracts from traditional systems. Once the conditions are met, a contract is executed within minutes, depending on the size of the transaction and the network's capacity. As Bhat et al. (2021) state, speed of execution is important for blockchain-based systems, especially in financial and banking applications.

3.2.5 Transparency

Smart contracts are designed to be transparent, allowing all parties involved to see the data and agreements. This transparency enables stakeholders to monitor contract execution and verify the terms, building trust and reducing potential disputes (Taherdoost, 2023).

3.2.6 Immutability

Once deployed on a blockchain, smart contracts are unchangeable, so the agreed terms cannot be altered or modified. As Vasiļevska (2022) explains, this prevents contract manipulation and makes the contracts more credible.

4. APPLICATIONS OF SMART CONTRACTS IN FINANCIAL AND BANKING SECTORS

4.1 Decentralized Finance (DeFi)

Decentralized Finance (DeFi) is a modern means of financial intermediation that dispenses with traditional intermediaries such as banks or financial institutions and therefore opens new opportunities for individuals to connect with a wide range of financial services. It is founded primarily on smart-contract technology, which ensures the safe and efficient management of financial activities involving lending, trading, and crypto-asset management. Smart contracts enforce financial agreements automatically without third parties, making the process transparent and cost-effective.

Examples of DeFi applications include Aave, Compound, and Uniswap, which use smart contracts to facilitate decentralized trading, lending, borrowing, and asset custody (Schär, 2021).

Despite the growth of this field, it faces many technical and regulatory challenges. DeFi has liquidity constraints compared with traditional financial systems and struggles to build user trust because of regulatory and legislative ambiguity. Security and asset protection are also major concerns. Nevertheless, DeFi is a promising field that can change the financial landscape and offer new opportunities for investment and financial services, especially in areas without access to traditional financial systems. Its growth and adoption, however, depend on addressing liquidity, trust, security, and regulatory clarity (Metelski & Sobieraj, 2022).

4.2 Trade Finance

Smart contracts enhance trade-finance operations such as letters of credit and guarantees by integrating with technologies such as the Internet of Things (IoT) and sensors, enabling seamless automation of information. For instance, in letters of credit, combining smart contracts with smart sensors automates payment verification when shipment conditions are met. Sensors relay real-time data to the smart contract, which processes payments without human intervention, reducing settlement delays (Tian, 2016).

In guarantees, smart contracts combined with IoT ensure compliance. For example, in asset-backed loans, sensors monitor equipment status on the blockchain. If equipment is moved to unauthorized locations or damaged, updates alert the relevant parties. This synergy between smart contracts and IoT fosters transparency and reduces fraud risks, making financial systems more secure and efficient (Tapscott & Tapscott, 2017). Platforms such as TradeLens, Marco Polo, and WeTrade are notable for automating trade-finance operations alongside various banks and institutions.

4.3 Insurance Services

The insurance sector increasingly leverages smart contracts for the secure and efficient automation of insurance operations, minimizing human involvement. These contracts improve operational efficiency by expediting claims processing. For example, insurers can automate payments when predefined conditions are met, such as the submission of a car-accident report. Upon data entry, the smart contract verifies its accuracy and processes payment, reducing errors and enhancing customer satisfaction (Christidis & Devetsikiotis, 2016).

Companies such as Etherisc demonstrate how smart contracts can revolutionize insurance services. Etherisc's flight-delay insurance automates compensation based on external data sources when delays occur, streamlining the customer experience (Sedkaoui & Chicha, 2021).

4.4 Know Your Customer (KYC) System

Know Your Customer (KYC) processes, which are essential for verifying client identities and preventing illicit activities such as money laundering, benefit significantly from smart contracts. Automating KYC through smart contracts can reduce identity-management costs by up to 30% (Ya, 2020). By sharing verified and standardized data among network participants, redundant processes are minimized and operations are accelerated. Additionally, embedding compliance requirements into smart contracts ensures adherence to local

and international regulations, reducing the risk of penalties (Martens et al., 2017).

4.5 Securities Settlement Systems

Smart contracts have changed securities settlement and clearing in financial markets by using blockchain for faster and more secure settlements. This reduces operational costs and human effort. For example, the Australian Securities Exchange (ASX) conducted the CHES Replacement Project, which used blockchain and smart contracts to reduce settlement time from two days to minutes (Agarwal et al., 2023).

The Depository Trust & Clearing Corporation (DTCC) launched Project Ion, a distributed-ledger system for large-scale financial trades with speed and security. Other initiatives include Synapse, launched by the Hong Kong Stock Exchange, which reduces operational risks and settlement delays through real-time data synchronization across time zones and integration with DTCC's Institutional Trade Processing (ITP) service (Colle, 2021).

5. SMART CONTRACTS IN THE FINANCIAL AND BANKING SECTOR: CHALLENGES

Despite the numerous advantages offered by smart contracts, including process automation, faster transactions, enhanced security, and reduced operational costs, their adoption in financial and banking institutions is hindered by several challenges and risks.

5.1 Cybersecurity Risks and Challenges

Cyber threats are among the most significant challenges facing the application of blockchain and smart-contract technologies in the financial sector. Although these technologies are designed to provide high levels of security through encryption and data decentralization, vulnerabilities can still be exploited by hackers and criminal organizations. For instance, Distributed Denial of Service (DDoS) attacks can disrupt networks, affecting or halting banking operations. Moreover, the lack of integration between traditional systems and smart contracts often creates security gaps, further complicating the cybersecurity landscape. Financial institutions must adopt multilayered strategies to bolster cybersecurity and mitigate these risks (Weerawarna et al., 2023).

5.2 Legal and Regulatory Challenges

Smart contracts face many legal and regulatory challenges that hinder their implementation in various sectors, including finance and banking. One of the biggest challenges is the lack of a clear legal framework governing their use. Most existing regulations are not designed to address the unique characteristics of this technology, such as decentralization and immutable data records, making it difficult to assign legal responsibilities. This raises the question of how current laws can be applied to transactions conducted through smart contracts (Zohar et al., 2022).

Moreover, data-protection laws such as the European Union's General Data Protection Regulation (GDPR) add further challenges, requiring careful handling of personal data within blockchain networks. The lack of international and local standardization also acts as a barrier to adoption. Global regu-

Table 1. Forms of Decentralized Finance (DeFi)

Form of Financing	Description
Lending and Borrowing	Platforms enabling users to lend and borrow digital assets via smart contracts without traditional intermediaries, such as Aave and Compound.
Decentralized Trading (DEX)	Allows users to trade cryptocurrencies without relying on centralized platforms, leveraging protocols such as Uniswap and SushiSwap.
Digital Savings	Enables users to deposit their savings (e.g., cryptocurrencies) into specific protocols in exchange for fixed or variable returns, such as BlockFi and Binance.
DeFi Crowdfunding	Facilitates investment in projects or startups through decentralized crowdfunding platforms, such as Gitcoin and DAOs.
DeFi Staking	Users can lock or stake their digital assets to support certain decentralized-finance networks in exchange for rewards, such as Yearn and Polkadot.

latory standards must be developed to enable interoperability and compliance across jurisdictions (Gilcrest & Carvalho, 2018).

5.3 Economic and Financial Challenges

Economic and financial barriers prevent smart contracts from being widely adopted. Implementing this technology requires substantial upfront investment in infrastructure, including hardware and software, and can involve high energy consumption. These costs are a burden, especially for smaller institutions. Ongoing operational costs, such as system maintenance and software updates, further constrain profitability and viability. In addition, ensuring security and regulatory compliance adds financial pressure and requires investment in measures that protect sensitive information and satisfy applicable laws. These challenges require a carefully considered plan to ease the financial burden of smart-contract implementation (Ahl et al., 2022).

5.4 Scalability and Integration Challenges with Traditional Systems

Another challenge facing blockchain and smart contracts is scalability and integration with existing financial systems. Verifying transactions through consensus mechanisms requires substantial computational resources and slows down as the number of users increases. Research has shown that this is a significant challenge for systems that need to process high volumes of transactions in real time, such as banking and electronic-payment systems (Croman et al., 2016). Unlike centralized infrastructures, blockchain networks may not process transactions rapidly.

Integration with existing banking systems also poses challenges and often requires extensive overhauls of current infrastructure to accommodate smart contracts, including changes to data processing, security frameworks, and regulatory policies (Peters & Panayi, 2016). Although these technical hurdles are real barriers to adoption, emerging solutions such as sharding and layer-two scaling technologies can improve smart-contract efficiency and integration without compromising decentralization and security (Zamyatin et al., 2020).

5.5 Key Statistics on Smart Contracts

Table 2 shows the growth of the blockchain-based smart-contract market from 2019 to 2023. The market size grew from \$0.65 billion in 2019 to \$2.1 billion in 2023, with an annual growth rate of approximately 20–25%. The market

shares of Europe and the Asia-Pacific region increased, while that of North America decreased. This indicates that smart-contract adoption is growing in these regions as investment increases and use cases broaden across industries.

Table 3 shows that the finance and banking sector maintained the largest share of smart-contract applications, with a significant increase from 35% in 2019 to 45% in 2023. There is growing reliance on smart contracts to improve efficiency while reducing costs. However, the share of supply chains and retail declined, indicating regulatory and technical issues that inhibit adoption. Moderate growth occurred in the healthcare and real-estate sectors as interest in data security and smart contracts increased. The government sector experienced a significant reduction in its share, moving from 22% to 9%, which may imply slower adoption of this technology.

6. THE POTENTIAL FOR ADOPTING SMART-CONTRACT TECHNOLOGY IN THE FINANCIAL AND BANKING SECTOR IN IRAQ

Adopting blockchain-based smart-contract technology in Iraq's financial and banking sector is a major strategic step toward full digital transformation. However, many challenges may hinder this process and prevent the country from keeping pace with the global financial system. One of the main challenges is the lack of technological awareness among many financial and banking institutions in Iraq. A survey of private banks in Baghdad regarding blockchain found that these institutions lack skilled professionals capable of handling modern technologies. This shortage will limit their ability to adopt such systems in the short term. However, the study showed that some private banks in Baghdad are ready to adopt and implement decentralized-finance technologies, although this readiness is limited by a lack of expertise and training (Al-Khayyat & Saharwardi, 2023).

With respect to infrastructure, Iraqi banks face a major challenge in upgrading their systems to keep pace with developments in blockchain-based smart contracts. These systems require advanced infrastructure to automate and accelerate digital transactions and secure data, which demands substantial investment in modern technology. One study found that many Iraqi banks still use old systems and therefore cannot handle the volume of data and transactions that blockchain technology will require (Jaber, 2022).

Another major challenge in adopting smart contracts in Iraq

Table 2. Market Size and Annual Growth Rate of Smart Contracts. Source: Market Research Future, Valuates Reports, and Global Market Estimates

Indicator	2019	2020	2021	2022	2023
Global Market Size (Billion USD)	0.65	0.78	1.40	1.75	2.10
Annual Growth Rate (CAGR)	0.20	0.22	0.24	0.23	0.25
North America	0.35	0.34	0.33	0.32	0.30
Europe	0.25	0.26	0.27	0.28	0.29
Asia-Pacific	0.20	0.22	0.23	0.24	0.25
Other	0.20	0.18	0.17	0.16	0.16

Table 3. Estimated Sector Shares of Smart-Contract Applications. Source: Zion Market Research, The Insight Partners, and Cognitive Market Research

Sector	2019	2020	2021	2022	2023
Finance & Banking	35%	38%	40%	42%	45%
Supply Chains & Retail	18%	16%	15%	14%	13%
Real Estate	10%	12%	13%	12%	11%
Health Services	8%	9%	10%	11%	12%
Gaming & Entertainment	7%	8%	9%	10%	10%
Public Sector & Government	22%	17%	13%	11%	9%

is the absence of suitable legal and regulatory frameworks to support these technologies. This is one of the main factors that may hinder implementation of smart-contract technology in financial and banking systems, as there is no clear legal framework permitting the use of digital currencies or smart contracts. Moreover, the Central Bank of Iraq has criminalized the use of digital currencies and decentralized-finance tools that are not under its control, citing regulatory oversight, legal issues, money laundering, and terrorism-financing concerns (Central Bank of Iraq, 2022).

Financial and banking experts in Iraq state that attention should be given to keeping pace with modern technologies, especially decentralized-finance technologies such as blockchain, to enhance transparency and operational efficiency in the Iraqi financial system. This will be particularly useful in areas such as auditing, financial reporting, and the automation of banking operations to reduce financial risks and comply with regulations and laws (Zubair & Dhnoon, 2023).

7. CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

- A) Smart contracts are a game changer for financial and banking institutions. They automate processes, increase transparency, and reduce human intervention, resulting in lower costs and more reliable financial systems.
- B) The current regulatory and legal framework in Iraq does not support decentralized digital systems in the financial and banking sector. Existing laws do not meet the requirements of blockchain and smart contracts.
- C) Iraq needs an advanced technological environment to support the infrastructure of decentralized digital systems. Financial and banking institutions do not have sophisticated information systems compatible with blockchain technology, so they cannot fully benefit from smart con-

tracts in financial automation and data-management applications.

- D) Iraq faces challenges in technological awareness and workforce skills in the financial and banking sector. The lack of qualified personnel to manage and operate smart-contract systems is a major obstacle to adopting this technology.
- E) Weak security and cyber threats are major challenges for smart contracts, creating a need for national cybersecurity strategies to protect digital data and secure financial and banking operations.

7.2 Recommendations

- A) Financial and banking institutions should use smart-contract technology to improve performance, transparency, and operational efficiency. They should focus on automation and reduced human intervention to increase the reliability and accuracy of financial systems.
- B) The legal and regulatory framework in Iraq should be updated to accommodate decentralized digital technologies such as smart contracts. This will protect financial institutions and citizens and create a legislative environment for these technologies.
- C) Iraq should develop its technological and digital infrastructure and upgrade the information systems of financial institutions to make them compatible with blockchain technology. This will support smart contracts and enable them to automate operations and manage data.
- D) Intensive training and capacity-building programs should be conducted to improve the skills of the workforce in Iraq's financial and banking sector, especially in managing and operating decentralized digital systems. This will accelerate adoption of these technologies in the financial sector.
- E) National cybersecurity strategies should be established

to address cyber threats, with a focus on developing a strong security system to protect digital data and secure financial operations.

REFERENCES

- [1] A. R. Jaber, "The impact of blockchain technology on the efficiency of internal control systems in iraqi commercial banks," *Tikrit Journal of Administrative and Economic Sciences*, vol. 18, no. 59, 2022.
- [2] R. G. M. Al-Khayat and H. M. S. Al-Sahrawardi, "The availability of infrastructure for blockchain technology and its impact on electronic banking services: A survey study in a group of private banks in baghdad," *Journal of Sustainable Studies*, vol. 5, no. 2, 2023.
- [3] R. H. M. A. Zubair and A. A. Dhnoon, "The impact of adopting blockchain technology on the stages of external auditing: A survey study," *Journal of Business Economics and Applied Research*, vol. 4, no. 4, 2023.
- [4] N. Agarwal, P. Wongthongtham, N. Khairwal, and K. Coutinho, "Blockchain application to financial market clearing and settlement systems," *Journal of Risk and Financial Management*, vol. 16, no. 10, p. 452, 2023.
- [5] A. Ahl, M. Goto, M. Yarime, K. Tanaka, and D. Sagawa, "Challenges and opportunities of blockchain energy applications: Interrelatedness among technological, economic, social, environmental, and institutional dimensions," *Renewable and Sustainable Energy Reviews*, vol. 166, p. 112623, 2022.
- [6] A. Bhat, R. M. Nor, M. Amiruzzaman, and M. R. Islam, "Methodology and analysis of smart contracts in blockchain-based international trade application," arXiv preprint arXiv:2107.14140, 2021.
- [7] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.
- [8] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [9] Cognitive Market Research, "Smart contracts market size, share & growth report, 2019–2023," Cognitive Market Research, 2023.
- [10] L. Colle, "Reaching for the moon: An analysis of real-time securities clearing and settlement in light of emerging blockchain technologies," *Virginia Law and Business Review*, vol. 16, p. 601, 2021.
- [11] K. Croman *et al.*, "On scaling decentralized blockchains: A position paper," in *International Conference on Financial Cryptography and Data Security*. Berlin, Heidelberg: Springer, 2016, pp. 106–125.
- [12] D. Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress, 2017.
- [13] J. Gilcrest and A. Carvalho, "Smart contracts: Legal considerations," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 3277–3281.
- [14] Global Market Estimates, "Smart contracts market analysis: Size & forecasts," Global Market Estimates, 2023.
- [15] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1991.
- [16] R. Weerawarna, S. J. Miah, and X. Shao, "Emerging advances of blockchain technology in finance: A content analysis," *Personal and Ubiquitous Computing*, vol. 27, pp. 1495–1508, 2023.
- [17] E. Hillbom and T. Tillström, "Applications of smart contracts and smart property utilizing blockchains," 2016.
- [18] S. C. B. Jaganathan *et al.*, "The future of web crowdfunding: An ethereum blockchain approach," in *Intelligent Technologies for Sensors*. Apple Academic Press, 2023, pp. 337–372.
- [19] S. N. Khan *et al.*, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 2901–2925, 2021.
- [20] A. Lafarre and C. V. der Elst, "The viability of blockchain in corporate governance," SSRN, 2023.
- [21] Market Research Future, "Smart contracts market: Information by blockchain platform, technology, and end users—forecast till 2030," Market Research Future, 2023.
- [22] D. Martens, A. T. V. Serooskerken, and M. Steenhagen, "Exploring the potential of blockchain for kyc," *Journal of Digital Banking*, vol. 2, no. 2, pp. 123–131, 2017.
- [23] D. Metelski and J. Sobieraj, "Decentralized finance (defi) projects: A study of key performance indicators in terms of defi protocols' valuations," *International Journal of Financial Studies*, vol. 10, no. 4, p. 108, 2022.
- [24] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2018, pp. 1–4.
- [25] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
- [26] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," *Business & Information Systems Engineering*, vol. 59, no. 3, pp. 183–187, 2017.
- [27] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in *Blockchain and Modern Banking Systems*. Springer, 2016, pp. 239–278.

-
- [28] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. Edward Elgar Publishing, 2016.
 - [29] H. Taherdoost, "Smart contracts in blockchain technology: A critical review," *Information*, vol. 14, no. 2, p. 117, 2023.
 - [30] F. Schär, "Decentralized finance: On blockchain- and smart contract-based financial markets," *Federal Reserve Bank of St. Louis Review*, 2021.
 - [31] S. Sedkaoui and N. Chicha, "Blockchain-based smart contract technology application in the insurance industry: The case of "fizzy"," *MJBS*, vol. 2, 2021.
 - [32] M. Swan, *Blockchain: Blueprint for a New Economy*. O'Reilly Media, 2015.
 - [33] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, 1997.
 - [34] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Penguin, 2017.
 - [35] H. Teng, W. Tian, H. Wang, and Z. Yang, "Applications of the decentralized finance (defi) on the ethereum," in *2022 IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC)*, 2022, pp. 573–578.
 - [36] The Insight Partners, "Smart contracts market analysis and industry forecast, 2019–2023," The Insight Partners, 2023.
 - [37] F. Tian, "An agri-food supply chain traceability system for china based on rfid & blockchain technology," in *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, 2016.
 - [38] Valuates Reports, "Smart contracts market research report, size, industry forecast analysis," Valuates Reports, 2023.
 - [39] A. Vasilevska, "Regulating smart contracts: The future of contract law or simply technical innovation," 2022.
 - [40] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. bft replication," in *International Workshop on Open Problems in Network Security*. Cham: Springer, 2015, pp. 112–125.
 - [41] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*. Springer, 2019.
 - [42] J. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain technology overview," National Institute of Standards and Technology, Tech. Rep. NISTIR 8202, 2018.
 - [43] S. Yakovenko, "Proof of history: A clock for blockchain," Solana White Paper, 2018.
 - [44] J. Yli-Huumo *et al.*, "Where is current research on blockchain technology? a systematic review," *PLoS ONE*, vol. 11, no. 10, p. e0163477, 2016.
 - [45] X. Zeng and J. Zhang, "Blockchain technology: Challenges and opportunities," *IEEE Internet Computing*, vol. 21, no. 4, pp. 35–41, 2017.
 - [46] W. Zheng *et al.*, *Blockchain Basics: Accelerating Adoption*. Springer, 2018.
-