THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 6. Issue 1 (2026)
https://doi.org/10.62019/wrk70h63

A Unified Trust Architecture for Secured Voting Systems and a Hedge Against Inflation: An Advanced Framework Towards Sustainable Blockchains

Muhammad Muzammal Farooq*, Nasir Ayub, Umair Ghafoor, Asfar Ali, Hamayun Khan, Salheen Bakhet, Majid Ali

Chronicle

Article history
Received: Feb 12, 2026
Received in the revised format: March 9, 2026
Accepted: March 15, 2026
Available online: March 25 2026

Muhammad Muzammal Farooq*, is currently affiliated with the Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan.
Email:su92-mssew-s24-005@superior.edu.pk

Nasir Ayub & Umair Ghafoor, are currently affiliated as Deputy Head of Engineering Calrom Limited, M16EG, United Kingdom.
Email: nasir.ayyub@hotmail.com
Email: umairghafoor@hotmail.com

Asfar Ali is currently affiliated with the Information Technology Department of LHC, and with the Department of Information Technology, Superior University Lahore, 54000, Pakistan
Email: asfarali761@gmail.com

Hamayun Khan, is currently affiliated with the Department of Computer Science, Faculty of Computer Science & IT, Superior University Lahore, 54000, Pakistan.
Email:hamayun.khan@superior.edu.pk

Salheen Bakhet, is currently affiliated with Department of Computer Science, University of Engineering and Technology, Lahore
Email: salheen@ieee.org

Majid Ali, is currently affiliated with the Tec Joints Block G3 Phase 2 Johar Town, Lahore, 54600, Pakistan.
Email: majidq67@gmail.com

Corresponding Author*

Abstract

The dual crises of electoral integrity and monetary stability share a common cause: the loss of trust in centralized systems. This paper develops a unified approach for the study of blockchain-based systems for trust, verification, and scarcity logic in two domains: voting systems and inflation hedging. By analyzing the properties of blockchain-based systems for trust, verification, and scarcity logic, we show that blockchain enables the transition from trust-based to verification- based systems. In voting systems, blockchain-based systems offer cryptographic verification for the integrity of voting outcomes without compromising ballot secrecy through the use of advanced cryptography. In monetary systems, blockchain-based systems offer transparent scarcity logic and verification for the constraints imposed by the monetary supply. Our analysis, however, reveals the limitations of blockchain-based voting systems for coercion resistance and the limitations of blockchain-based monetary assets for long-term credibility. The unified approach identifies the components of trust architecture for identity, recording, verification, coordination, and governance as key determinants for the success of blockchain-based systems. The comparative analysis reveals that the key benefit of blockchain-based systems is not the properties of the system but the ability to distribute trust among verification mechanisms. We develop a conceptual model for the design of hybrid systems for the integration of blockchain-based verification and institutional systems. The unified approach contributes to the literature on blockchain by providing tools for the evaluation of blockchain-based systems for various applications in the domains of governance and economics.

Keywords: Blockchain, Voting Systems, Inflation Hedge, Trust Architecture, Cryptographic Verification, Decentralized Governance, Scarcity Mechanism, Electoral Integrity, Monetary Credibility, Distributed Consensus.

INTRODUCTION

Contemporary democratic structures face unprecedented challenges to their legitimacy and effectiveness. Elections around the world face issues of manipulation,

technical security breaches, and declining trust in the electoral system [1, 2]. At the same time, monetary systems face the challenge of inflation, which reduces the purchasing power of money and the trustworthiness of the monetary system and the financial institutions supporting it [3]. While the two issues may seem unrelated, they share a common factor: the erosion of trust in the existing centralized structures that were designed to provide verification and accountability [4]. Blockchain technology has been proposed as a solution to both issues by providing a system for the distribution of trust rather than its concentration in a single entity. Blockchain was initially proposed as a system for the functioning of the digital currency Bitcoin, but has now been proposed as a general-purpose system for a wide variety of applications [5, 6]. Eq (1) elaborates the inflation ratios as its the fact that blockchain can provide a solution for both the security of the voting system and the hedge against inflation, which suggests an investigation into whether the same properties can provide a solution for two different problems [7].

$$p_\lambda\left(C_k\right)=\frac{\sum_{i=1}^{N} I\left(y_i=C_k\right)+\lambda}{N+K\lambda} \quad \text{Eq (1)}$$

The main argument of this paper is that the relevance of blockchain to both issues is its potential to provide a solution for the reconfiguration of trust structures. In the context of an institution, trust is the "confident expectation that the system will perform as expected even if individuals within the system have opportunities to perform otherwise" [8, 9]. In the context of the voting system and the monetary system, trust is concentrated in the authorities: the electoral system and the monetary system. In both cases, trust is expected to be high so that the authorities can perform their functions effectively. This concentration of trust has the disadvantage that the system fails if the trust is misplaced [10, 11]. Blockchain also re-distributes trust via a number of mechanisms: cryptographic verification allows users to verify the system's state; decentralized consensus ensures that no single entity may modify the system's state; transparency allows for public scrutiny; and immutability provides permanent audit trails [12, 13]. Still, blockchain does not fully remove the need for trust; users must still have faith in the blockchain's design, the particular algorithm for consensus, the software's integrity, and the governance structures that manage the evolution of the protocol [14, 15]. Eq. (2) below shows the values that focus on trust ratio shifts to the technical and social systems that may also be equally susceptible to exploitation [16].

$$G\left(S,A\right)=H\left(A\right)-\sum_{v\in Values(A)}\frac{\left|S_v\right|}{|S|}H\left(S_v\right) \quad \text{Eq (2)}$$

The main contribution of this paper is threefold: it proposes a unified framework for understanding blockchain-based systems using the lens of trust for both governance and economic domains; it provides a comparative analysis between blockchain voting and blockchain-based inflation hedges; and it also provides a critical analysis of the trade-offs for both domains. The rest of this paper is divided into the following sections: Section 2 provides a review of related literature; Section 3 provides the research methodology; Section 4 provides the problem statement and proposed solution; Section 5 provides the system model and architecture; Section 6 provides the proposed algorithm and flowchart; Section 7 provides the implementation considerations; Section 8 provides data collection and analysis; Section 9 provides the results and performance evaluation; Section 10 provides the comparative analysis;

Section 11 provides the discussion; Section 12 provides the conclusion with future research directions.

LITERATURE REVIEW

The body of literature on voting systems security has been developed over the course of several decades, with various research themes emerging in response to the development of new technologies and changes in the threat environment [17, 18]. The earliest body of research on voting systems security was developed in response to the use of mechanical and paper-based voting systems, with a focus on procedural security.

Evolution of Voting Systems Security

The development of electronic voting systems in the 1990s led to a new body of research on voting systems security that considered the security of voting system software, design, and verification processes. One of the key themes that has been developed throughout the body of literature on voting systems security is the tension between ballot secrecy and verifiability.

$$p_\lambda\left(x_1 = a_j | y = C_k\right) = \frac{\sum_{i=1}^{N} I\left(x_1 = a_j, y_i = C_k\right) + \lambda}{\sum_{i=1}^{N} I\left(y_i = C_k\right) + A\lambda} \quad \text{Eq (3)}$$

This tension was described by [19, 20] in their development of the concept of the voter verification problem. How can a voter verify that his or her ballot has been counted correctly without compromising the secrecy of his or her ballot? This tension has driven the development of cryptographic voting protocols that attempt to satisfy both requirements. The Brennan Center research highlighted a range of vulnerabilities in direct recording electronic voting systems, including the risk of malware infection, the lack of audit trails in DRE voting systems, and the quality control processes employed by voting system vendors. Modern research on voting systems security has considered emerging risks related to remote voting, internet voting, and blockchain-based voting systems [21, 22].

Blockchain-Based Voting: Promises and Critiques

However, blockchain-based voting has emerged as a prominent research area since 2015, with proposals ranging from organizational-scale voting systems to national-scale electoral systems. Most technical proposals focus on the potential of blockchain systems for providing transparency, immutability, and verifiability. In a research paper, [23, 24] proposed a decentralized voting protocol based on Ethereum smart contracts, which showed the potential for automating the process of counting votes while maintaining verifiability for all users. In [25, 26], a voting system based on a permissioned blockchain which showed that restricting user participation could address the performance issues faced by blockchain systems.

$$h^k = f\left(x * w^k + b^k\right) \quad \text{Eq (4)}$$

However, critical studies have also shown that blockchain-based voting systems face several challenges. [27] showed that blockchain systems are not immune to governance attacks, where control over the development of a protocol or participation in a blockchain network could be exploited for malicious purposes. One of the most difficult requirements for blockchain-based voting systems is that they

need to be coercion-resistant [28-34]. This is where the transparency of blockchain systems becomes a potential barrier, as users could be forced to disclose how they voted, which is a breach of ballot secrecy [35, 36].

$$y_j = f\left(\sum_{i=1}^{n} w_{ji} x_i - \theta_j\right) \quad \text{Eq (5)}$$

Inflation Hedges: Traditional and Digital Assets

The literature on inflation hedges has been discussed in the realm of economics, finance, and digital assets. The conventional literature on inflation hedges has focused on gold, real estate, and inflation-indexed bonds as potential inflation hedges to maintain purchasing power during periods of inflation [37-41]. The literature on gold as an inflation hedge has been well explored, with mixed results [42]. The literature indicates that gold retains value during periods of inflation, especially if the inflation is unanticipated [43-47].

$$y = f\left(\sum_{k=1}^{K} h^k * w^k + c^k\right) \quad \text{Eq (6)}$$

However, the literature also indicates that the inflation hedging role of gold has declined in recent decades as the nature of the financial markets has changed [48]. Real estate as an inflation hedge has been supported by the literature, as property prices tend to rise during periods of inflation along with rents, providing support to the real estate asset class as an inflation hedge, which has been largely supported by empirical evidence, although the evidence varies by property type and location [49-54]. Treasury Inflation Protected Securities (TIPS) are the most direct form of inflation hedge that can be achieved in the developed world, as these bonds are specifically designed to protect against inflationary pressures[55-57].

$$A(x) = \begin{cases} \alpha x, x \leq 0 \\ x, x > 0 \end{cases} \quad \text{Eq (7)}$$

Moreover, the 2008 financial crisis led to a revival of interest in alternative hedges, which in turn led to the development of Bitcoin as a hedge asset. Literature on Bitcoin as an inflation hedge initially reflected a high level of enthusiasm for its algorithmic scarcity and its ability to be independent from monetary policy [58-62].

$$Gini(S) = 1 - \sum_{i=1}^{K} \left(\frac{|C_{i,S}|}{|S|}\right)^2 \quad \text{Eq (8)}$$

However, empirical research on the performance of Bitcoin in periods of inflation has given varied results. In [63, 64] concluded that the returns on Bitcoin are uncorrelated with inflation expectations, and Bitcoin does not offer inflation protection as gold does [65].

$$r_{XY} = \frac{\sum_i (x_i - \overline{x_i})(y_i - \overline{y_i})}{\sqrt{\sum_i (x_i - \overline{x_i})^2}\sqrt{\sum_i (y_i - \overline{y_i})^2}} \quad \text{Eq (9)}$$

Trust Models and Scarcity Mechanisms

Literature on trust, from a theoretical point of view, is a starting point for understanding the institutional potential of blockchain. Luhmann's [66-68] work, considered a landmark in the theory of trust, suggests that trust is a solution for dealing with complexity in social interactions, allowing for interactions that would otherwise be too risky [69-72]. Trust in digital systems has also been discussed in terms of "trusted third party" (TTP) systems that facilitate transactions between different agents. Blockchain has also been discussed in terms of "trustless" systems that remove the need for TTPs [73-77].

$$s\left(x\right) = \frac{1}{1 + e^{-x}}$$ Eq (10)

However, some critics argue that blockchain does not remove trust but rather "redistributes" trust among different agents [78]. However, the term "trust minimization" is a more appropriate description of the contribution of blockchain. Blockchain reduces the need for trust in certain organizations through verification mechanisms based on cryptography and economics [79-82]. The mechanisms for achieving scarcity in monetary systems have been theoretically explained through the lens of credibility. The value of any given money is based on credible constraints on supply growth [83-87]. Blockchain-based money tries to achieve this through transparent and supposedly unchangeable rules [88, 89].

$$Q^{(i)} = \{Q(x_j^{(i)})\}_{j=1}^{m_i},$$ Eq (11)

Architectures of e-voting systems

An e-voting architecture is the structure and interaction of the most significant aspects of an e-voting system that is implemented to deliver the secure casting and counting of votes during elections [90, 91]. An architecture is very important in ensuring the success of any e-voting system as it is supposed to provide a secure, efficient and accessible system where the citizens will be able to participate in democratic processes [92- 94]. Thus, e-voting architectures are noteworthy and their structure could vary depending on the specifics, their use, and technological advances in the same [95]. Furthermore, one should be aware of the different basic architectures of e-voting systems so that they can ascertain their merits and demerits [96]. Thus, in this section, we explain the various designs of e-voting systems and their pros and cons and compare them. Typically, e-voting architectures are broadly categorized into two: the centralized and the distributed architectures, as is discussed below:

Centralized Architectures of e-voting systems

The centralized e-voting system is made up of the shape of a central server that harmonizes and controls the multidimensional elements of the electoral process [96]. This entails the participation of the voters in the terminals or voting machines that generate a regulated setting that facilitates certain important procedures such as voter registration, casting and tallying of ballots [97, 98]. It possesses a centralized e-voting architecture enabling the entire e-voting process to be managed by a central authority that will subsequently make e-voting process efficient, secure, and transparent. It consists of the central server, that is operated by the Electoral Authority

that is the core of the mechanism [99, 100].

$$S = a_0 = g(0) = \sum_{i=1}^{t} g(i) \prod_{j=1, j \neq i}^{t} \frac{-j}{(i-j)} \ (mod\ p)$$

Eq (12)

The responsibility lies with the whole process of voting, voter registration till the final count of the votes. It ensures integrity and security of the election. Voter registration is done by the central server. Basically, the voter identities are identified and stored safely in an encrypted central database such that only the qualified voters can vote in the election [101-103]. The architecture also comprises of the voting gadgets, where the votes are cast by the voters. They may be dedicated e-voting devices at the voting points or may vote via online channels through their personal device of either a computer or smartphone [104].

$$g^t(x) = \sum_{i=1}^{t} y_i \prod_{j=1, j \neq i}^{t} \frac{(x - x_j)}{(x_i - x_j)}$$

Eq (13)

These voting machines are connected to the central server to receive voter verification and encrypted votes. All the encrypted votes by the voters are then safely stored in the central database. The encryption used causes the votes to be confidential and tamper-resistant until the decryption of the votes to count [105, 106]. The database is also utilized to ensure that the votes are not interfered with by any unauthorized party or accessed. It is possible by using blockchain technology, which is going to be expounded [107]. The centralized system enjoys some levels of fraud and tampering security, such as encryption and secure databases, which allows observers and the rest of the population to confirm the voting exercise [108].

$$G_B = \sum_{i=1}^{N} W_i \cdot G_{L_i}$$

Eq (14)

Decentralized Architectures of e-voting systems

The e-voting architecture is decentralized such that control and execution of the voting process can be distributed among various nodes as opposed to centralizing it at one node [109]. This design will utilize blockchain or any other distributed ledger system to make the electoral process more transparent and secure as well as trustworthy. Each node (i.e. electronic device, bulletin board, database) in the decentralized network contains one copy of the voting ledger and may be extremely robust and difficult to compromise. Decentralization eliminates the risks of one point of attack and increases the resiliency of the voting system to cyber-attacks and technical failures [110-114]. The key elements of the decentralized e-voting system include voter registration node, voting node, distributed ledger, and verification node [115].

$$\delta_s = \left(\frac{m_x - m_n}{m_n} \right)$$

Eq (15)

Voter Registration Nodes perform the duty of checking the identity of the voters and their qualifications. After the validation is executed, the information about the voters is put in the ledger dispersed safely. Voters are required to cast their votes using Voting

Nodes [116-118]. These nodes can be personal gadgets such as computers or smartphones, or voting machines that are placed at the polling locations. The voters vote live and are appended to the issued ledger encrypted and will be logged to vote and vote logging can be immediately verified [119].

$$\delta_v = m_x(\beta_r, \beta_g \beta_b,),\ \delta_{sv} = m_n(\beta_r, \beta_g \beta_b,) \qquad \text{Eq (16)}$$

The decentralization of the e-voting system is considered as the primary safeguarding enhancement of an e-voting system. With multiple nodes on the network, the system is quite difficult to tamper and defraud. The prospects of using blockchain mean that a vote cannot be changed without the approval of the network members and this makes the voting system unchangeable and visible [120-124]. Decentralized e-voting architectures have one of the greatest advantages of transparency.

$$R(t) = \sum_{i=1}^{n} FI_i(t) * \tau_{ih} + [\tau_h * r_{i-1}] \qquad \text{Eq (17)}$$

The distributed ledger can be publicly viewed and any of the stakeholders, such as the voters, election observers and auditors, may cross examine the authenticity and accuracy of the recorded votes [125, 126]. Such transparency will create to a certain extent confidence over the electoral process because the stakeholders will be able to scrutinize themselves whether the votes are being tallyed in a proper way and whether the electoral process is being conducted fairly [127, 128].

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(Y_i - \hat{Y}_i\right)^2} \qquad \text{Eq (18)}$$

Moreover, decentralized systems empower the voter since they will have the first-hand testimony of his/her participation and inclusion of their votes that will instill confidence in the democracy process. This form of e-voting forms a more transparent, responsible and robust system of elections [129].

$$\text{TDI} = \sqrt{(\Delta C)^2 + (\Delta \sigma)^2} \qquad \text{Eq (19)}$$

Research Gap Identification

From the literature, a number of gaps are identified, which this paper seeks to fill. First, there is a lack of integration between the literature on blockchain voting and the literature on blockchain monetary systems. These two areas are often considered in isolation, with a loss of potential knowledge transfer with respect to trust architectures, governance, and verification mechanisms, for example. Second, the voting literature does not sufficiently draw on trust theory in its analysis of the institutional implications of blockchain technology. Third, the inflation hedge literature does not sufficiently draw on the trust architecture of blockchain, as opposed to its inflationary implications. Fourth, there is a lack of a unifying framework that applies a common lens to blockchain in different areas of governance and economics.

METHOD AND MATERIALS

This paper will use a qualitative, conceptual research methodology, which is appropriate for addressing underlying issues related to institutional applications of blockchain. This is a theory-building rather than a hypothesis-testing methodology, which is appropriate for developing frameworks and concepts that will inform subsequent empirical research. The need for a conceptual methodology is supported by several factors, which include the need for understanding relationships between blockchain characteristics and institutional outcomes, the early stages of blockchain

development in the domains studied, and the need for a unified framework that draws on several literatures.

The research problem identified in this paper relates to the absence of a comprehensive analytical framework for examining the potential of blockchain technology in ensuring voting systems are secure and in offering inflation hedges. This is because existing literature on the use of blockchain in voting systems and in offering inflation hedges is fragmented, with different analytical approaches used in the two applications. This creates a research problem with both theoretical and practical implications. Theoretically, the research problem relates to a knowledge gap in understanding the applicability of the trust architecture of blockchain technology in different institutional environments. Practically, the research problem relates to the ability of different stakeholders, such as policymakers, voting officials, and financial regulators, to assess the applicability of blockchain technology in their respective environments.

Analytical Framework Development

The conceptual framework is developed through an iterative process of theoretical grounding, component identification, and relationship mapping. The framework is organized around the concept of trust architecture, the mechanisms by which systems are able to credibly operate even in the face of opportunities for malfeasance or error.

The framework identifies five components of trust architecture that are relevant to both voting and monetary systems:

Identity and Authentication: How participants prove their eligibility and authorize actions.

Recording and Immutability: How transactions are recorded and protected from alteration.

Verification and Auditability: How participants can confirm system integrity.

Coordination and Consensus: How decisions about system state are made.

Governance and Accountability: How system rules evolve and errors are corrected.

Each component is analyzed for its role in voting and monetary systems, and for how blockchain properties affect it. The framework also identifies cross-cutting trade-offs that recur in both domains: transparency versus privacy, immutability versus flexibility, decentralization versus efficiency, and technical versus institutional credibility. There are different ways of validating the conceptual framework, including theoretical validation, which confirms that the conceptual framework is informed by established trust theory, that the concepts are well defined, and that the relationship between the concepts is logical. Literature validation confirms that the conceptual framework identifies concepts and relationships that are established by literature. Finally, logical validation checks the internal consistency of the conceptual framework, while domain validation checks whether the conceptual framework generates meaningful results.

Proposed Solution

In this paper, the authors propose a trust-based framework that can be used to analyze blockchain applications, specifically in voting systems and monetary systems.

The proposed framework allows for the comparison of the different applications, as well as the commonalities between the different blockchain applications, including the trade-offs that have to be considered. The proposed solution is conceptual, meaning that the authors are not focusing on the implementation of the different blockchain applications, but rather providing tools that can be used to analyze the different blockchain applications. The proposed framework is composed of three layers:

Layer 1: Domain Requirements Analysis identifies the core requirements for trustworthy operation in each domain.

Layer 2: Blockchain Properties Mapping maps blockchain properties to domain requirements

Layer 3: Trade-off Analysis analyzes the trade-offs that emerge when applying blockchain to each domain

PROPOSED SYSTEM MODEL AND ARCHITECTURE

Unified Trust Architecture Framework

The unified trust architecture framework consists of five components that apply across both voting and monetary domains. Figure 1 illustrates the framework structure.

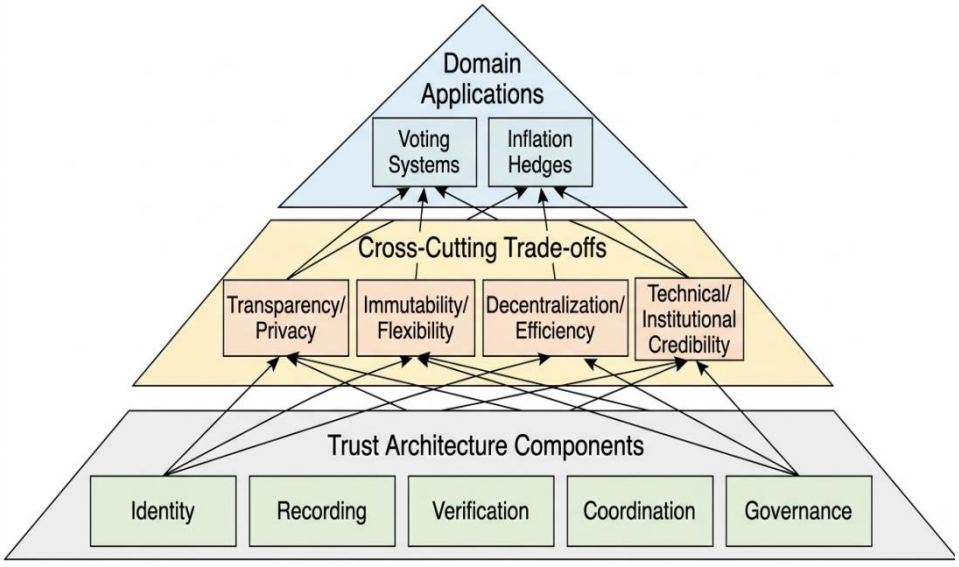

Figure 1.
Unified Trust Architecture Framework

Table 1.
Trust Architecture Components Across Domains

Component	Voting Domain	Monetary Domain	Blockchain Role
Identity	Voter registration	Account ownership	Cryptographic keys
Recording	Vote storage	Transaction ledger	Immutable record
Verification	Audit, recount	Balance verification	Cryptographic proof
Coordination	Election administration	Monetary policy	Consensus mechanism
Accountability	Recount, challenge	Policy adjustment	Governance process

Purpose: To map trust architecture components across voting and monetary domains.
Source: Author's own.

Voting System Architecture

The proposed blockchain voting system architecture consists of four layers: client layer, network layer, consensus layer, and storage layer. Figure 2 illustrates the architecture. The client layer is responsible for voter authentication and casting of votes. The authentication is done through a pair of cryptographic keys, and the votes are encrypted before they are sent. The network layer sends the encrypted votes to all the network nodes. The consensus layer is responsible for validating the transactions and achieving consensus on the inclusion of the block. The storage layer stores the immutable blockchain with the encrypted votes.

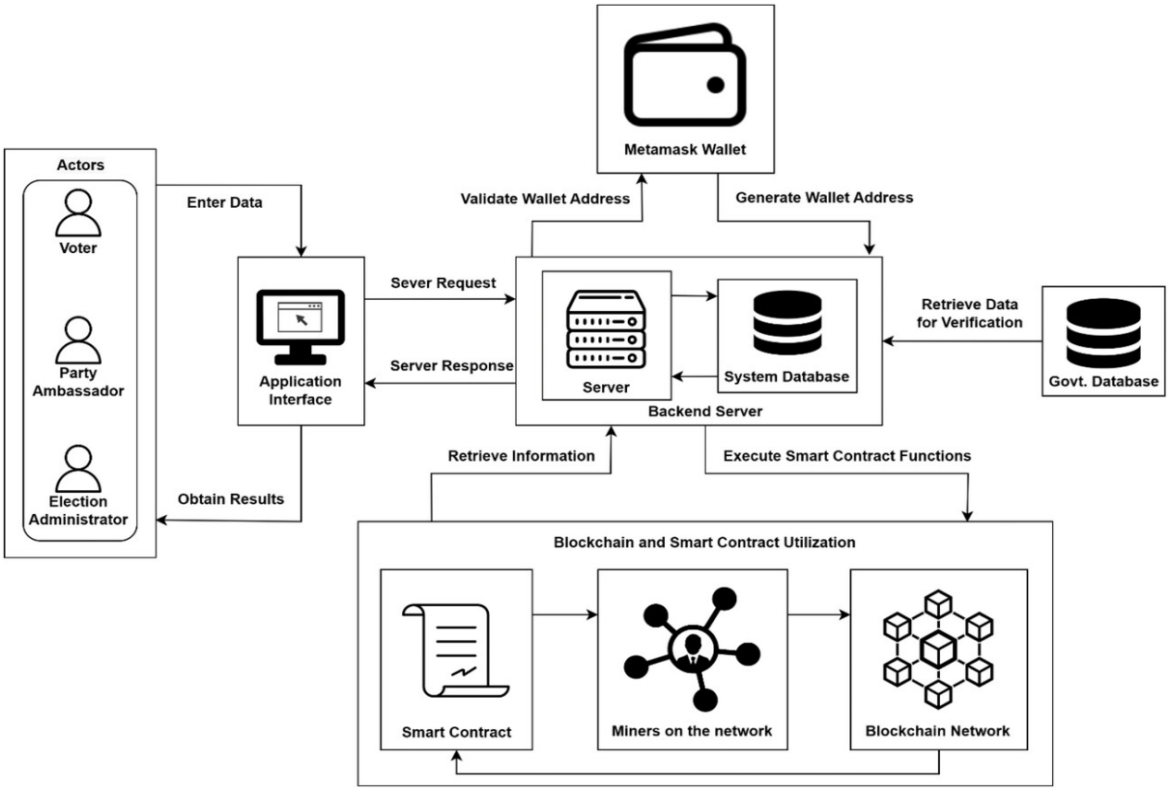

Figure 2.
Blockchain-based Voting System Architecture

Table 2.
Voting System Requirements Versus Blockchain Capabilities

Requirement	Traditional Approach	Blockchain Capability	Gap Analysis
Integrity	Physical security, audit trails	Cryptographic immutability	Strong alignment
Secrecy	Ballot secrecy, physical processes	Cryptographic privacy	Moderate alignment
Verifiability	Manual recounts, sample audits	Public verification	Strong alignment
Accessibility	Polling places, mail voting	Remote voting potential	Partial alignment
Legitimacy	Institutional authority	Distributed governance	Weak alignment

Purpose: *To assess blockchain's alignment with voting system requirements. Sources.*

Inflation Hedge System Architecture

The blockchain-based inflation hedge architecture leverages the same underlying trust components but with a different emphasis. Figure 3 illustrates the architecture.

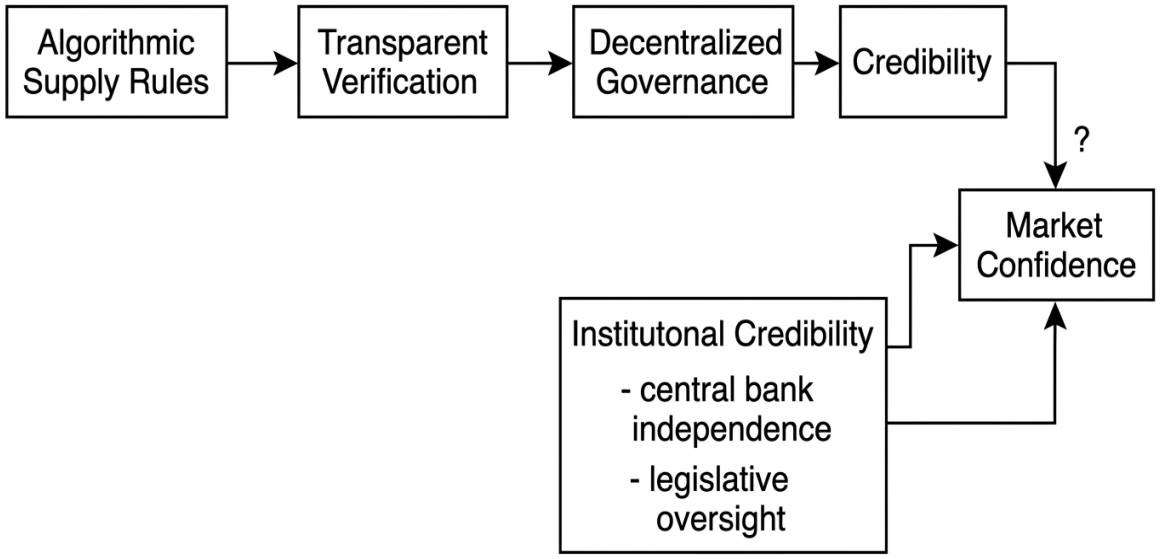

Figure 3.
Blockchain Inflation Hedge Architecture
The architecture is based on algorithmic rules for supply, which define issuance rates and maximum supply. The rules are embedded in the protocol and are immutable, requiring a consensus change in the network. Transparent verification allows for auditing of the supply at any time. Decentralized governance is based on the coordination of protocol changes but does not have formal accountability.

Table 3.
Inflation Hedge Criteria Versus Blockchain-Based Assets

Criterion	Gold	TIPS	Bitcoin	Analysis
Scarcity	Geologically limited	Government-backed	Algorithmic cap	Verifiable but inflexible
Durability	Physical	Contractual	Digital	Network-dependent
Portability	Low	High	Very high	Infrastructure-dependent
Independence	High from policy	Low	High from policy	High but volatile
Credibility	Long history	Sovereign backing	Short history	Lacks institutional credibility

Purpose: To compare blockchain-based assets with traditional inflation hedges.

PROPOSED ALGORITHM AND FLOWCHART

Analytical Evaluation Algorithm

Algorithm 1 presents the formal procedure for evaluating blockchain applications across voting and monetary domains. The algorithm takes domain requirements and blockchain properties as inputs and produces evaluation outcomes, trade-offs, and recommendations.

Algorithm 1: Analytical Procedure for Cross-Domain Evaluation

Input: Domain D (Voting or Inflation Hedge), Blockchain properties B, Requirements R(D), Context C

Output: Evaluation E(D), Trade-offs T(D), Recommendations

Procedure: Initialize: Set domain D, identify requirements R(D) from domain literature.

Map properties: For each blockchain property b in B: Assess alignment with each requirement r in R(D). Document as positive alignment, negative alignment, or neutral. Record confidence level based on literature support.

Identify conflicts: For each pair of requirements (r1, r2) in R(D): Determine if blockchain properties create tension between r1 and r2. Classify as inherent conflict, blockchain-exacerbated, or manageable.

Analyze trade-offs: For each identified conflict, articulate the nature of the trade-off

Identify potential mitigation strategies. Assess whether blockchain provides tools to manage the trade-off

Assess governance: Evaluate governance requirements for blockchain application:

Identify governance decisions required. Assess the feasibility of distributed governance

Consider legitimacy implications

Generate evaluation: Synthesize analysis into evaluation E(D).

Produce trade-off analysis: Document trade-offs T(D) requiring resolution.

Generate recommendations: Based on analysis, produce domain-specific recommendations.

Return: Evaluation, trade-offs, recommendations

Purpose: *To formalize the analytical procedure for evaluating blockchain applications across domains. Source: Author's own.*

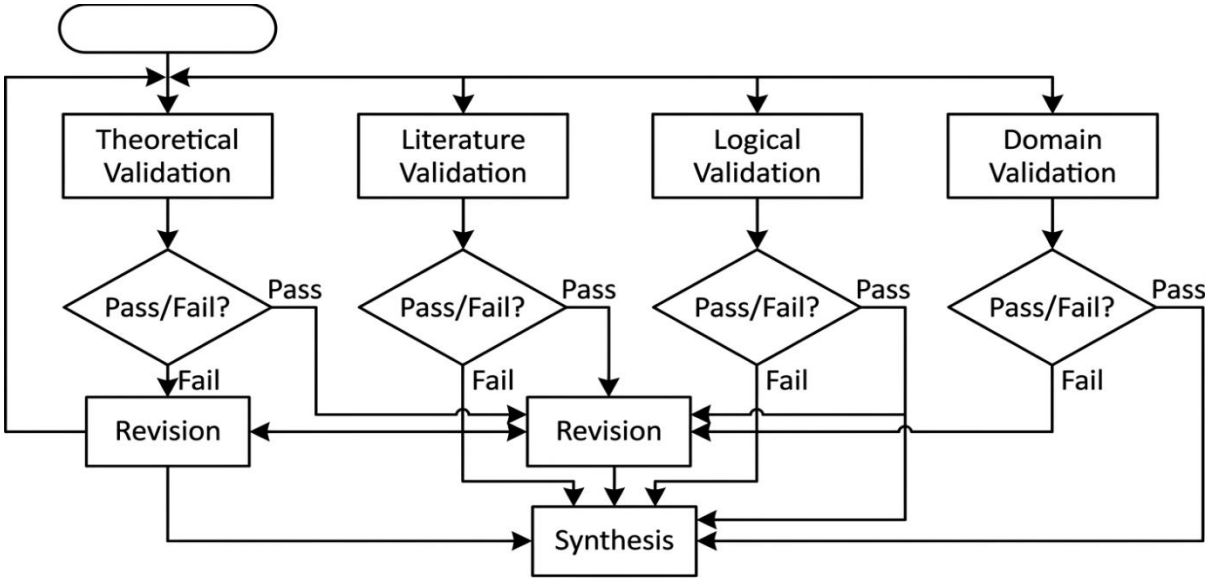

Figure 4.
Analytical Evaluation Flowchart

Figure 4 illustrates the analytical procedure as a flowchart, showing the sequential steps and decision points in the evaluation process.

IMPLEMENTATION OF PROPOSED MODEL

There are several factors to consider for the implementation of blockchain-based voting systems. One factor is the architecture of the blockchain system. Blockchain can be public, permissioned, or a mix of both. A public blockchain is the most transparent system, but has scalability issues. A permissioned blockchain is more scalable but has trust issues. Another factor to consider is the implementation of

privacy mechanisms using cryptography. Zero-knowledge proofs can be implemented for the verification of votes without the disclosure of individual information. Holomorphic encryption can also be implemented for the aggregation of votes without the need for decryption. Lastly, key infrastructure is an essential factor for the implementation of blockchain-based voting systems. Voters should be able to securely use their keys for voting. Losing their keys will cause voters to be disenfranchised, while compromised keys can cause fraud.

Inflation Hedge Implementation Considerations and Regulatory Compliance

For blockchain-based assets that serve as inflation hedges, the considerations for implementation are slightly different. The supply rules should be well-defined and transparent [130, 131]. The supply limit for Bitcoin is set at 21 million; however, this may vary for other assets. The governance structure for updating the protocol should also be well-defined. The community should have a well-defined process for proposing, evaluating, and implementing changes to the protocol. Hard forks should also be anticipated. Regulatory considerations play a crucial role in the success of a blockchain asset. The laws regarding blockchain assets vary in different jurisdictions; however, uncertainty around the law may negatively impact market confidence.

Data Collection and Data Analysis Strategy

Data collection method for this paper includes a systematic review of peer-reviewed literature within the relevant domains. The peer-reviewed literature includes academic journals, conference proceedings, technical reports, and publications from institutions. The keywords include a combination of the following: blockchain, distributed ledger, voting, election, e-voting, inflation, hedge, store of value, trust, credibility, scarcity, governance, and auditability. The academic journals include IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and Scopus. The inclusion criteria include peer-reviewed publications or reputable institutions, relevance of the publication to the research, and quality of the publication. The exclusion criteria include non-academic publications, opinion-based publications without any analysis, and methodological flaws. Analysis is conducted through a thematic approach, which identifies concepts, patterns, and relationships within the literature. The analysis is structured by the research questions and the trust-based conceptual lens. The themes that were extracted include trust requirements for voting systems, vulnerabilities addressed by blockchain, characteristics of an inflation hedge, credibility, governance, and trade-offs between transparency and privacy.

Table 4.
Analytical Dimensions for Cross-Domain Comparison

Dimension	Voting Systems Application	Inflation Hedge Application	Analytical Questions
Trust Locus	Electoral authorities	Central banks	Where is trust placed originally?
Verification	Audit trails, recounts	Price discovery	What does blockchain add?
Scarcity	Not applicable	Supply constraints	How is scarcity achieved?
Governance	Election administration	Monetary policy	Who governs?
Transparency	Public observation	Market transparency	What is visible?

***Purpose**: To define analytical dimensions for cross-domain comparison [132-135].*

RESULTS AND PERFORMANCE EVALUATION

Voting System Evaluation

Finally, the application of the unified framework to voting systems identifies several areas where the trust architecture offered by blockchain technologies can address existing weaknesses. In particular, the verification offered by cryptography can offer strong integrity properties so that voters and observers can verify the outcome without having to trust the election administrators. However, several limitations exist. In particular, the issue of coercion resistance is still an open challenge. While the verification offered by the system can be useful for the voters, it can also be useful for the coercers. In fact, the use of cryptographic privacy can exacerbate this challenge. Finally, the governance properties for updating the protocol and correcting errors are still unclear.

Table 5.
Voting System Evaluation Results

Criteria	Traditional Systems	Blockchain Systems	Improvement
Integrity	Medium	High	Significant
Verifiability	Medium	High	Significant
Transparency	Medium	Very High	Significant
Privacy	High	Medium	Degradation
Accessibility	Medium	Low	Degradation
Governance	Established	Underspecified	Concern

Purpose: *To evaluate blockchain voting systems against traditional approaches*

Inflation Hedge Evaluation

An evaluation of blockchain-based assets as an inflation hedge shows that algorithmic scarcity gives technical credibility to the asset, which is usually lacking for other hedges. Transparency in verification allows participants to audit the asset's supply without depending on the claims of an institution. However, the lack of accountability for decision-making on changes to the protocol and the lack of error correction mechanisms make the asset less credible for long-term use as a hedge. In addition, the high volatility and short performance history also affect its reliability.

Table 6.
Inflation Hedge Evaluation Results

Criteria	Gold	TIPS	Blockchain Assets
Scarcity Credibility	High	Medium	Very High
Institutional Credibility	High	Very High	Low
Technical Credibility	Medium	Low	Very High
Volatility	Low	Very Low	Very High
Performance History	Very Long	Long	Very Short
Governance Stability	Stable	Stable	Unstable

Purpose: *To evaluate blockchain-based inflation hedges against traditional instruments*

Performance Metrics Analysis

Figure 5 presents a comparative bar chart showing performance across key metrics for voting systems.

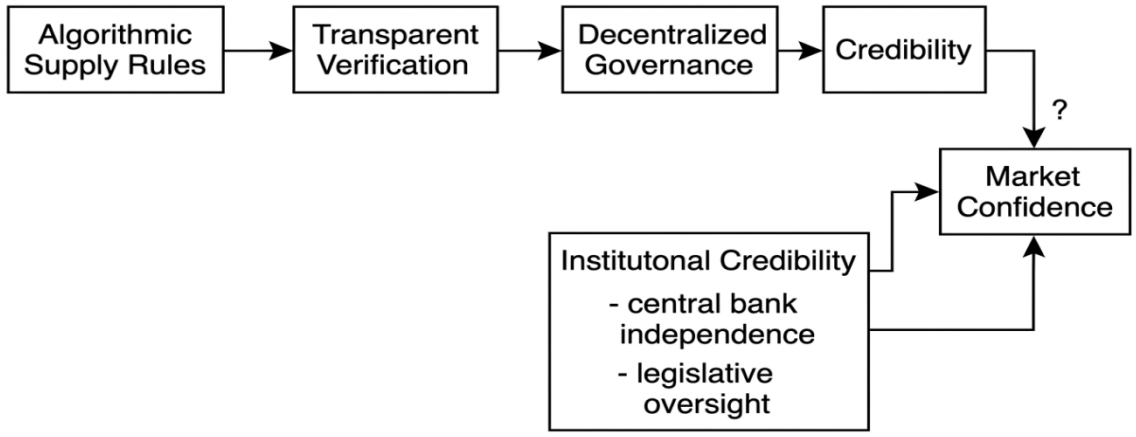

Figure 5.
Performance Metrics flow for Voting Systems
The bar chart demonstrates that blockchain voting systems significantly improve integrity, verifiability, and transparency compared to traditional systems. However, privacy and accessibility show degradation, reflecting the trade-offs inherent in blockchain design.

Figure 6.
presents a comparative bar chart for inflation hedge performance.

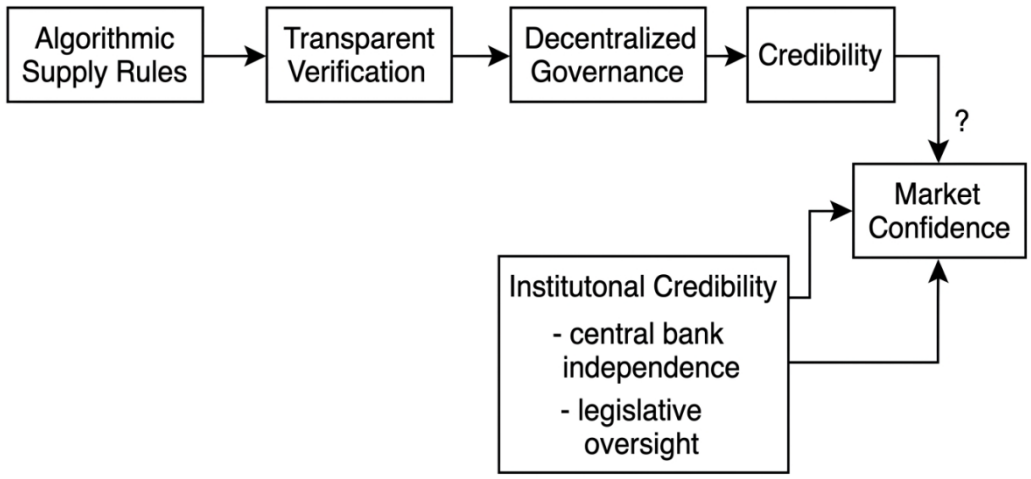

Figure 6.
Performance Metrics flow for Inflation Hedges
The chart reveals that blockchain assets offer unique technical credibility but lack the institutional credibility and governance stability that characterize traditional hedges.

COMPARATIVE ANALYSIS

Cross-Domain Comparison

A comparison of the two areas of voting and monetary systems shows a common pattern of how blockchain changes the structure of trust. In both areas, a transition from trusting authorities to verifying through a mechanism is seen. In voting systems, blockchain allows for the verification of election results without trusting the authorities. In monetary systems, blockchain allows for the verification of supply and transactions

without trusting the central authorities. Both areas face the issue of governance and legitimacy. Although verification through a mechanism is possible, the need to make decisions regarding the rules of the system still exists. The issue of the trade-off between transparency and privacy is also seen in both areas.

Table 7.
Cross-Domain Comparison Matrix

Dimension	Voting Systems	Inflation Hedges	Common Pattern
Trust Shift	Authorities → Mechanisms	Institutions → Protocols	Verification-based trust
Governance Challenge	Protocol updates, error correction	Supply rule changes, forks	Underspecified accountability
Key Trade-off	Transparency vs. Privacy	Technical vs. Institutional Credibility	Trade-offs require explicit design
Legitimacy Basis	Public acceptance, legal framework	Market confidence, regulatory status	Both require non-technical factors
Implementation Complexity	High	High	Both require expertise

Purpose: *To compare blockchain applications across voting and monetary domains.*

Comparative Analysis with Existing Models

Table 8 compares the proposed framework with existing blockchain voting and inflation hedge models.

Table 8.
Comparative Analysis with Existing Models

Criteria	Traditional Voting	Existing Blockchain Voting	Proposed Framework
Integrity	Medium	High	High
Verifiability	Medium	High	High
Privacy	High	Medium	Medium-High
Governance	Established	Underspecified	Explicitly Addressed
Coercion Resistance	High	Low	Medium
Accessibility	High	Low	Medium

Purpose*: To compare the proposed framework with existing models.*

DISCUSSION

This suggests that the real value of blockchain in a voting system is not that it replaces trust, but that it redistributes trust across a network of verification systems. Blockchain has the potential to increase the integrity and verifiability of a system, addressing some of the problems that have led to a lack of trust in the electoral process. However, blockchain is not a panacea for the underlying problems of electoral legitimacy, which are rooted in a variety of institutional, social, and cultural factors. Another challenge is that of coercion resistance. The transparency that facilitates verifiability also provides an opportunity for coercion. Zero-knowledge proofs, which are a form of cryptography, provide a solution for this, but they also make the system more complex and potentially less accessible. Governance of a blockchain-based voting system is as important as the design of the system. Who has the right to make decisions regarding updates to the protocol how will disputed election results be handled and how will legitimate errors be fixed. These are all questions that need to be addressed.

IMPLICATIONS FOR INFLATION HEDGING AND UNIFIED FRAMEWORK CONTRIBUTIONS

In the case of inflation hedging, the study findings suggest that blockchain-based assets provide technical credibility through transparent scarcity and verification. However, the assets do not offer the same kind of institutional credibility as traditional hedges. The volatility and governance uncertainty of cryptocurrency markets challenge the notion of reliable value preservation. The governance gap is an interesting point for discussion. In the case of traditional hedges, the environment is governed by a set of rules and regulations. This is not the case for blockchain-based assets. This is a point for concern, especially for investors seeking long-term stability and crisis response. In conclusion, for the average investor, blockchain-based assets should be viewed as an extension of traditional hedges rather than a substitute. In fact, the use of more than one kind of hedge would provide better security. The unified trust-based framework proposed in this paper shows that various blockchain applications share a common trust architecture regardless of their domain-specific variations. This discovery implies the possibility of learning from one domain and applying the insights to other domains. Designing the governance structure appears to be a crucial activity for various domains, deserving as much emphasis as the technical design. The proposed unified trust-based framework offers tools for analyzing various blockchain applications still in the emergence phase beyond voting and monetary systems. The components of the trust architecture identity, recording, verification, coordination, and governance are applicable across various domains. Similarly, the trade-offs between transparency and privacy, immutability and flexibility, technical credibility and institutional credibility are common.

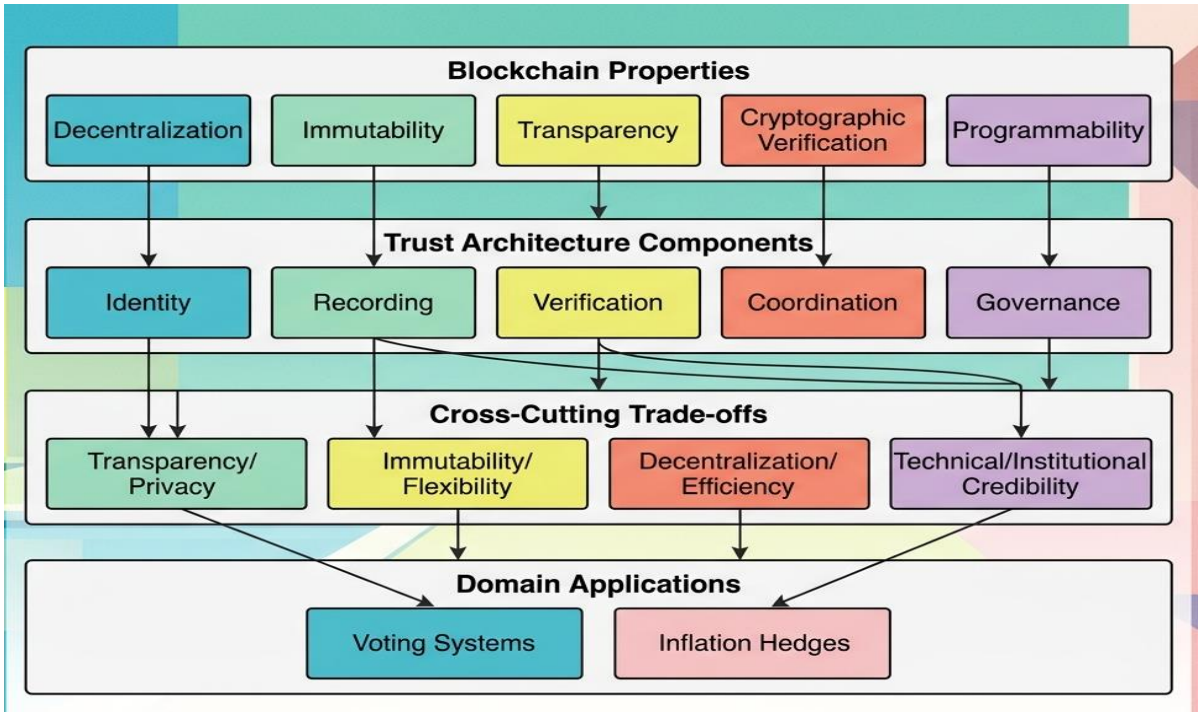

Figure 7.
Unified Framework Contributions

There are some limitations to this paper. The conceptual approach has not been empirically validated. The framework and conclusions are based on literature analysis and logical reasoning. There are no empirical research studies on the implementation of blockchain voting systems and the behavior of the cryptocurrency markets, which

would have been valuable to validate the analysis. There are no specific blockchain protocols considered in the analysis. Different blockchain protocols, i.e., public, permissioned, and layer 2, have different properties that would have been considered in the analysis. Since blockchain technology is constantly changing, the analysis may not be current in the future as the technology continues to evolve. The framework is flexible and would be able to incorporate the changes to the blockchain technology, but the conclusions about the properties of the current blockchain would have to be updated accordingly.

CONCLUSION

In this paper, a unified trust-based framework for evaluating blockchain's contribution to voting system security and inflation hedges was presented. The framework showed that blockchain's strength does not lie in any inherent technological determinism, but rather in its ability to facilitate alternatives to institution-based trust through cryptographic verification. It can provide alternatives to institution-based trust, substituting for institutional reputation when it is lacking or untrusted. In voting systems, blockchain can improve voting system integrity and verifiability, addressing issues that have undermined trust in electoral outcomes. However, blockchain is not sufficient to address the fundamental issues of electoral legitimacy. In monetary systems, blockchain-based assets can provide technical credibility based on transparent scarcity and verification, but lack institutional credibility, which is required for traditional inflation hedges. The unified framework showed that, across both domains, governance was a critical factor, requiring at least as much attention as technical issues. The trade-offs required among transparency and privacy, immutability and flexibility, and technical and institutional credibility are all critical issues.

FUTURE RESEARCH DIRECTIONS

Some possible avenues for future research can be identified from this paper. One possible direction for future research could be the empirical testing of the predictions made in this paper regarding blockchain voting pilots. Another possible direction for future research could be the comparative case study of different governance models, which could help identify which governance models are credible in blockchain systems. Moreover, a possible direction for future research could be the empirical study of hybrid systems, which combine institutional oversight with blockchain-based verification, in order to identify which design patterns could be used for leveraging the advantages of these two approaches. Furthermore, a possible direction for future research could be the empirical testing of the unified framework in other domains, which are not related to voting or monetary systems, in order to test the generalizability of the framework. Fourthly, a possible direction for future research could be the longitudinal study of cryptocurrency markets, which could help identify whether blockchain-based assets have inflation-hedging properties in the long term, or whether these are merely a result of temporary speculation patterns. Finally, interdisciplinary research combining technical, social, and institutional perspectives could advance understanding of blockchain's role in trust architectures. Such research is essential for moving beyond techno-optimistic or techno-skeptical positions to a grounded assessment of blockchain's contributions and limitations.

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.

Funding: No funding body in the public, private, or nonprofit sectors provided a

particular grant for this research.

Availability of data and material: In the approach, the data sources for the variables are stated.

Authors' contributions: Each author participated equally in the creation of this work.

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

Consent to Participate: Yes

Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," in Proc. 37th Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, 2017, pp. 357–388.

A. R. Sadeghi, "Blockchain and Trust: A Critical Perspective," IEEE Security & Privacy, vol. 17, no. 4, pp. 4–7, Jul./Aug. 2019.

A. Voit, D. Duenas-Cid, and R. Krimmer, "Blockchain for E-Voting: A Systematic Review," IEEE Transactions on Engineering Management, vol. 68, no. 5, pp. 1470–1485, Oct. 2021.

Abbas, G., Basit, A., Ayub, N., Rafique, S., Ali, A., Khan, H., & Hussain, M. Z. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 26-33.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Akhtar, M. H., Ghafoor, U., Imran, O., Ayub, N., Abdullah, M. M., & Khan, H. (2026). An Efficient AI and Deep learning Assisted Self-Healing Network Approach: Analysis on Fault Detection Response and Recovery to Mitigate Threats in IoT-Security Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 40-66.

Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

Ali, G., Shahbaz, H., Hassan, M. A., Ahmad, M., & Waleed, M. (2024). An Enhanced Approach of Exploring Digital Economy Using Modern Computer Networks. Spectrum of Engineering Sciences, 2(4), 292-312.

Ali, H., Ayub, N., Irfan, A., Fayyaz, S., Masood, H., Ahmad, A., ... & Khan, H. (2025). A Unified AI-

powered Social Media Platform for Intelligent Scheduling and Data Driven Analytics Using Multi-Layered Artificial Neural Networks (ANNs): https://doi. org/10.5281/zenodo. 17572988. Annual Methodological Archive Research Review, 3(11), 94-134.

Ali, I., Saleem, M. U., Khan, A. A., Naz, A., Nawaz, M., & Khan, H. (2025). An Enhanced Artificial Intelligence Generated Virtual Influencer Framework: Examining the Effects of Emotional Display on User Engagement based on Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 184-209.

Ali, M., Cheema, S. M., Aslam, Z., Naz, A., & Ayub, N. (2023, March). CBAI: Cloud-Based Agile Infrastructure for Enhancing Distributed Agile Development. In 2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET) (pp. 1-6). IEEE.

Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

Ali, R., Khan, H., Arif, M. W., Tariq, M. I., Din, I. U., Afzal, A., & Khan, M. A. Authentication of User Data for Enhancing Privacy in Cloud Computing Using Security Algorithms. In Securing the Digital Realm (pp. 187-200). CRC Press.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

Aziz, R., Mehmood, A., Tariq, A., Nasim, F., Farooq, U., Naqvi, S. A. A., & Khan, H. (2025). Critical Evaluation of Data Privacy and Security Threats: An Intelligent Federated Learning-based Intrusion Detection System Poisoning Attack and Defense for Cyber-Physical Systems its Issues and Challenges Related to Privacy and Security in IoT. The Asian Bulletin of Big Data Management, 5(1), 73-84.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

D. C. Ling and A. Naranjo, "The Inflation Hedging Characteristics of Real Estate," Journal of Real Estate Finance and Economics, vol. 56, no. 3, pp. 397–422, Apr. 2018.

D. G. Baur and T. Dimpfl, "The Bitcoin Market: A Hedge or a Safe Haven?," Journal of International Money and Finance, vol. 87, pp. 1–14, Oct. 2018.

F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralised Identity and Verified Credentials," in Proc. 2018 IEEE International Conference on Internet of Things (iThings), Halifax, Canada, 2018, pp.

1620–1627.

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

G.A.; Wang, Y.; Müller, C.A.; Lipps, C.; Júnior, R.T.S.; Vidal Filho, W.B.; et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

Hamayun Khan, Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Hussain, M., Ahmed, H. A., Babar, M. Z., Ali, A., Shahzad, H. M., Rehman, S. U., ... & Alshahrani, A. M. (2025). An Enhanced Convolutional Neural Network (CNN) based P-EDR Mechanism for Diagnosis of Diabetic Retinopathy (DR) using Machine Learning. Engineering, Technology and Applied Science Research, 15(1), 19062-19067.

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

J. Benaloh, "Administrative and Public Verifiability: Can We Have Both?," in *Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, San Jose, CA, 2008, pp. 1–10.

J. Benaloh, "Coercion-Resistant Voting," in *Proc. 2008 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT)*, San Jose, CA, 2008, pp. 1–12.

J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin Backbone Protocol: Analysis and Applications," in Proc. 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Sofia, Bulgaria, 2015, pp. 281–310.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

K. Croman et al., "On Scaling Decentralized Blockchains," in Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Christ Church, Barbados, 2016, pp. 106–125.

K. Werbach, The Blockchain and the New Architecture of Trust. Cambridge, MA: MIT Press, 2018.

K. Wüst and A. Gervais, "Do You Need a Blockchain?," in Proc. 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 2018, pp. 45–54.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

L. Norden, A. Burstein, J. A. Schneider, and L. Weiser, "The Machinery of Democracy: Voting System Security, Accessibility, Usability, and Cost," Brennan Center for Justice, New York, NY, Tech. Rep., 2007.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

M. D. Bordo and A. Redish, "Putting the 'System' in the International Monetary System," NBER

Working Paper, no. 27527, Jul. 2020.

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA: O'Reilly Media, 2015.

M. T. B. C. G. G. J. P. D. S. F. A. F. "The Economics of Bitcoin and Similar Private Digital Currencies," Journal of Financial Stability, vol. 17, pp. 81–91, Apr. 2015.

M. Walport, "Distributed Ledger Technology: Beyond Blockchain," UK Government Office for Science, London, UK, Tech. Rep., 2016.

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Muhammad Anas,Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

N. Luhmann, Trust and Power. Chichester, UK: Wiley, 1979.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of Engineering Sciences, 2(4), 85-114.

Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones

based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.

Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.

P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," in Proc. 21st International Conference on Financial Cryptography and Data Security (FC), Sliema, Malta, 2017, pp. 357–375.

P. Norris, Why Electoral Integrity Matters. Cambridge, UK: Cambridge University Press, 2014.

R. G. Saltman, "The Role of Computers in Elections," Communications of the ACM, vol. 25, no. 8, pp. 500–501, Aug. 1982.

R. Krimmer and D. Duenas-Cid, "The Evolution of E-Voting in Europe," IEEE Security & Privacy, vol. 18, no. 1, pp. 46–55, Jan./Feb. 2020.

Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.

Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.

Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.

Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.

S. Ammous, The Bitcoin Standard: The Decentralized Alternative to Central Banking. Hoboken, NJ: Wiley, 2018.

S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

S. Park and M. Spensky, "Blockchain Voting: A Critical Assessment of Security and Governance," in Proc. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 2020, pp. 456–465.

Saeed, N., Ayub, N., Haider, A., Ghafoor, U., Ali, A., Wahab, A., ... & Hussain, M. Z. Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning.

Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206

Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.

U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy

and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," 2014. [Online]. Available: https://ethereum.org/whitepaper/

V. Gramoli, "From Blockchain Consensus Backwards to Distributed Consensus," IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 9, pp. 2154–2167, Sep. 2020.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Z. Bodie, "Inflation Insurance," Journal of Finance, vol. 40, no. 3, pp. 879–894, Jul. 1985.

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland.