UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Computer Science Curriculum

Xinyue Zhang

Towards Developing a Blockchain Selection Toolkit for Smart Cities

Master's Thesis (30 ECTS)

Supervisor(s): Mubashar Iqbal, PhD

Tartu 2025

Towards Developing a Blockchain Selection Toolkit for Smart Cities

Abstract:
In recent years, the rapid development of smart cities has driven the integration with innovative technologies such as blockchain to enhance urban systems' efficiency, transparency, and credibility. This thesis presents a comprehensive and systematic survey of blockchain applications in smart cities and proposes a toolkit of blockchain options for the diverse needs of smart cities. The study firstly reviews the background of blockchain technology and smart city framework, followed by a systematic literature review of public, private, and federated chains, and analyzes the challenges faced during their integration. Based on this, a blockchain selection toolkit is designed and implemented to provide city planners with references on selecting appropriate blockchain technologies in different smart city scenarios through existing cases. The toolkit is evaluated through three case studies: a small-scale energy grid, a large-scale supply chain system, and a secure healthcare system. Finally, the thesis discusses the practical implications of the research, answers the research questions, and identifies the limitations and future directions of the research. The study results show that the proposed toolkit supports adoption decisions for smart city blockchain technology.

Keywords:
Blockchain, Smart Cities, Toolkit, Blockchain Selection Toolkit, Systematic Literature Review

CERCS: P170, Computer Science, Numerical Analysis, Systems, Control

Plokiahela valikutööriista väljatöötamise suunas nutikatele linnadele

Lühikokkuvõte:
Viimastel aastatel on nutikate linnade kiire areng soodustanud innovaatiliste tehnoloogiate, nagu plokiahel, integreerimist, et suurendada linnasüsteemide tõhusust, läbipaistvust ja usaldusväärsust. Käesolev magistritöö esitab põhjaliku ja süstemaatilise ülevaate plokiahela rakendustest nutikates linnades ning pakub välja tööriistakasti, mis sisaldab plokiahela valikuid nutikate linnade erinevate vajaduste jaoks. Uuring annab esmalt ülevaate plokiahela tehnoloogia ja nutika linna raamistikust, millele järgneb süstemaatiline kirjanduse ülevaade avalikest, privaatsetest ja föderaalsetest plokiahelatest ning nende integreerimise käigus esinevatest väljakutsetest. Selle põhjal kavandatakse ja rakendatakse plokiahela valikutööriist, mis annab linnaplaneerijatele juhiseid sobiva plokiahela tehnoloogia valimiseks erinevates nutika linna stsenaariumides olemasolevate juhtumite kaudu. Tööriistakasti hinnatakse kolme juhtumiuuringu kaudu: väikesemahuline energiasüsteem, suuremahuline tarneahela süsteem ja turvaline tervishoiusüsteem. Lõpuks arutletakse uurimistöö praktilise tähtsuse üle, vastatakse uurimisküsimustele ning tuuakse välja uuringu piirangud ja tuleviku suunad. Uuringu tulemused näitavad, et välja pakutud

tööriistakast toetab nutikate linnade plokiahelatehnoloogia kasutuselevõtu otsuseid.

Võtmesõnad:
Plokiahel, Nutikad linnad, Tööriistakast, Plokiahela valikutööriistakast, Süstemaatiline kirjanduse ülevaade

CERCS: P170 Arvutiteadus, arvanalüüs, süsteemid, kontroll

Acknowledgment

Supervisor
I would like to express my deepest gratitude to my supervisor, Dr. Mubashar Iqbal, for his invaluable guidance and expert advice throughout the entire process of this thesis. His provision of essential learning materials and well-structured recommendations were instrumental in shaping the direction and quality of this work. Beyond his academic mentorship, his encouragement and patience greatly motivated me to overcome challenges and refine my research. This thesis would not have reached its current form without his dedication and insightful contributions.

ChatGPT
During the process of writing this thesis, the AI chatbot tool ChatGPT[1] version 3.5 and 4 was used. ChatGPT is a natural language processing chatbot that allows having human-like conversations using a text prompt. The tool was used as a knowledge-broadening and brainstorming tool to learn about subjects related to the thesis. Additionally, ChatGPT was used to find synonyms of different words and as an assistant to find different structures of sentences to broaden the vocabulary for expressing ideas.

Grammarly
Grammarly[2] is a writing assistance tool that uses artificial intelligence and natural language processing to check and improve the quality of written text. Grammarly was used to find issues in grammar, spelling, and punctuation in the near final draft of this thesis.

Cyber-security Excellence Hub in Estonia and South Moravia

This work is part of the Cyber-security Excellence Hub in Estonia and South Moravia (CHESS: https://chess-eu.cs.ut.ee) project funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[1] https://chat.openai.com/
[2] https://www.grammarly.com/

Contents

1 Introduction

With the rapid development of information technology, cities worldwide are undergoing a digital transformation. This transformation has given rise to the concept of smart cities, which enable the intelligent management of urban systems through advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and big data. However, the rapid development of smart cities also brings many challenges, including data security, privacy protection, the complexity of system interconnections, and the need for transparency and trust [29]. In this context, blockchain technology is gradually becoming a key technology in the smart city field due to its decentralized, immutable, tamper-proof, and transparency features. Blockchain can improve the security of data sharing, automate smart cities management, and improve the efficiency of city services through smart contracts and decentralized consensus mechanisms [11].

In recent years, several fields have begun to explore the application of blockchain in smart cities, such as smart transport, energy management, healthcare, and digital finance. However, despite the widely recognized potential of blockchain technology in smart cities, there are still some limitations in existing research, such as insufficient analysis of the trade-offs between different types of blockchain in terms of energy consumption and security and limited integration of cross-disciplinary knowledge, which has resulted in synergies between blockchain and urban planning that have not yet been fully exploited. In addition, most studies focus on specific application areas and lack a comprehensive analysis of the entire smart city ecosystem. Therefore, this study aims to systematically investigate the current status of the application of blockchain technology in smart cities, fill the gaps in existing research, and provide decision support for policymakers, urban planners, and technicians.

1.1 Problem Statement

Given the accelerated progress in smart city development, urban management and infrastructure are facing unprecedented challenges. These challenges include efficient management of urban resources, data privacy and security, and data sharing between different departments. Blockchain, as a decentralized, secure, and tamper-proof technology, has been proposed as a potential solution to these problems due to its transparency and efficiency. In particular, in many fields of smart cities (e.g., transportation, energy, healthcare, and finance), blockchain technology helps to achieve data sharing, automatic execution of smart contracts, and improve transparency and trust. Smart cities are growing fast to tackle urban problems using IoT, AI, and big data. By 2050, over 68% of the world's population will live in cities [34]. As cities use more digital tools, they may face cybersecurity risks and trust issues that need new solutions. Smart city systems combine different technologies, like smart transport, energy grids, and e-governance. This mix creates many weak points for attacks. For example, the 2021 Colonial Pipeline ransomware attack [3] and the 2023 Lisbon smart meter data breach [15] show how centralized systems and poor data management can harm important city services.

Blockchain's decentralized approach could help, but current uses still have critical limitations, such as: Insufficient analysis of energy consumption vs. security tradeoffs in public vs. private chains, Minimal cross-domain knowledge transfer between blockchain R&D and urban planning. Existing studies mainly focus on specific domains, such as smart grids or healthcare, rather than providing a comprehensive analysis of blockchain's potential to revolutionize the entire smart city ecosystem. This limited scope creates challenges for policymakers and urban planners in making well-informed, evidence-based decisions regarding the adoption of emerging technologies.

This systematic survey therefore aims to address these gaps by providing a comprehensive analysis of blockchain's role in smart cities, focusing on three key dimensions:

- Holistic Implementation Landscape: Mapping existing blockchain applications across the smart city ecosystem to reveal patterns, trends, and gaps in current deployments.
- Energy-Security Tradeoffs: Systematically reviewing and comparing the performance of public and private chains across different urban domains to identify best practices and limitations.
- Cross-Domain Knowledge Integration: Synthesizing insights from blockchain research and urban planning studies to highlight opportunities for multifaceted collaboration.

By offering a comprehensive understanding of blockchain applications, this study aims to empower policy makers, urban planners, and technologists to make informed decisions, fostering resilient, efficient, and citizen-centric smart cities.

1.2 Research Method

This thesis uses the methodology of design science research. In the design-science paradigm, knowledge and understanding of a problem domain and its solution are achieved in the building and application of the designed artifact [13]. It is fundamentally a problem solving paradigm [13]. The guidelines presented in Table 1 illustrate the standardized design science research methodology employed in this study. The artifact DG.1 in this thesis is the proposed solution in Section 4. This thesis finds DG.2 by reviewing the context of blockchain and smart city in Section 2. The proposed solution is evaluated (DG.3) based on selected criteria in Section 5 and further discussion in Section 6. The research contribution (DG.4) and research rigor (DG.5) is based on providing Section 4 to produce a proposed solution and the foundation in Section 3. The design guidelines DG.6 and DG.7 are achieved by finding the requirements for the proposed solution as well as the descriptive diagrams and high-level architectural overviews and descriptions of the proposed solutions and technologies used.

Table 1. Design Science Research Guidelines

Guideline	Description
DG.1 Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
DG.2 Problem relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.
DG.3 Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
DG.4 Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
DG.5 Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
DG.6 Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
DG.7 Communication of research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

1.3 Research Questions

To address the issues discussed in Section 1.1, we set our main research question: *What is the current role of blockchain technology in enhancing smart city ecosystems?* To answer our main research question, we formulated five sub-research questions:

RQ1: What are the existing blockchain-based applications in smart city domains?

RQ2: How are different blockchain solutions being compared in smart city infrastructure?

RQ3: How can we build a tool to optimize the selection of blockchain technology for smart cities?

RQ4: What are the challenges and future directions associated with integrating blockchain into smart city systems?

1.4 Contributions

This thesis aims to advance theoretical understanding and deliver practical solutions. The contributions are structured to answer the sub-research questions by systematically exploring blockchain applications:

- A comprehensive and up-to-date systematic survey of blockchain applications in smart cities has been conducted. This survey not only consolidates fragmented knowledge across domains but also identifies underexplored areas and emerging trends, offering a structured foundation for future research.
- A comparative framework for evaluating blockchain types (public, private, and consortium) has been developed. This framework introduces new insights into the trade-offs between energy efficiency, security, scalability, and governance models, thus aiding scholars and practitioners in selecting appropriate blockchain architectures for specific urban use cases.
- A blockchain selection toolkit tailored for smart city contexts has been designed and implemented. This practical tool, based on multi-criteria decision analysis, enables policymakers and system designers to match blockchain solutions with project-specific requirements, bridging the gap between theory and practice.
- Based on the synthesis of research findings, this thesis presents a set of identified challenges and future research directions for blockchain adoption in smart cities.

1.5 Thesis Outline

The thesis is structured as follows. Section 2 describes the leading technologies and concepts employed in this study. It provides a comprehensive explanation of blockchain, including its workflow, different types of blockchain, and their consensus algorithms. It also identifies the characteristics, key components, and current pioneers of smart cities. Section 3 performs a systematic review of the literature, focusing on existing research related to blockchain applications in smart cities. Also, a comparative analysis of different blockchains used in different scenarios and the rationale behind their selection. Section 4 proposes a solution to address cognitive barriers between urban planners and technical experts. Section 5 evaluates the toolkit designed based on 3 scenarios. Sections 6 and 7 discuss and conclude the thesis with a summary of the key findings.

2 Background

This section introduce blockchain technology's characteristics, workflow, types, and consensus mechanisms. Followed by an introduction to the concept of smart cities and what constitutes a smart city. Finally, the section explores the potential of blockchain technology in smart cities, along with its applications across different domains, lays the foundation for the subsequent detailed introduction of blockchain technology in different domains of a smart city.

2.1 Blockchain

Blockchain technology became widely known in 2009 with the launch of the Bitcoin network, the first of many modern cryptocurrencies. Because of this, blockchain technology is often viewed as bound to Bitcoin or possibly cryptocurrency solutions in general. However, the technology is available for various applications and is being investigated for various sectors. Blockchains can be defined as distributed digital ledgers of cryptographically signed transactions grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper-evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules [44]. At its core, blockchain transactions are conducted in a decentralized manner in a peer-to-peer network. In other words, transactions are verified and stored through a distributed consensus mechanism without the need for verification by a central entity.

The key characteristics of the blockchain technology are as follows: **Data immutability**: One of the most critical features of blockchain technology is its ability to prevent data corruption. This is achieved through a decentralized ledger system, where each node in the network maintains an identical copy of the ledger. Any modification to the data requires unanimous consensus from all nodes, ensuring security and transparency. **Decentralized**: Transaction management is distributed across a network of nodes. These nodes collectively validate and record transactions, ensuring that no central entity has the power to alter or manipulate the data. This decentralization enhances security, reduces the risk of fraud, and promotes transparency, as all participants in the network have access to the same information and can independently verify the validity of transactions.

Anonymity: All transactions and validations across the blockchain are done by maintaining anonymity for the stakeholders, employing hash addresses to safeguard user information confidentiality [20]. For instance, in the case of Bitcoin, when a person transfers funds, the recipient can observe that the sender is associated with a Bitcoin address, but the sender's actual identity remains undisclosed. **Transparency**: Blockchain enables tracing every transaction, whether tangible or intangible, from its initiation to completion. As each block in the chain contains references to the preceding block, enabling sequential storage of transactions and facilitating the traceability of tampering or malicious activity within the blockchain [21].

The workflow of blockchain technology can be summarized in the following key steps: First, a transaction is initiated by a computing node (i.e., a user device) and broadcast to a peer-to-peer network consisting of multiple computing nodes. These nodes receive the transaction request and validate both the transaction and the status of the requesting user using validation algorithms, such as public key cryptography, to ensure legitimacy and authenticity. Once the transaction is successfully validated, it is considered a verified transaction (e.g., cryptocurrency transactions, smart contracts, or data records). The verified transaction is combined with other validated transactions to form a new data block. Before being added to the blockchain, this block must undergo validation through a consensus algorithm, such as Proof of Work. Once validated, the block is permanently and immutably added to the existing blockchain ledger. This ensures the integrity and security of the blockchain. Finally, once the new block is successfully integrated into the blockchain, the transaction is complete, and the updated ledger is accessible to all network participants. This decentralized process ensures transparency, security, and trustworthiness in digital transactions.

Based on the characteristics and policies, blockchain technology is broadly classified into three types: public, private, and consortium blockchain. A public blockchain provides an open platform for people from various organizations and backgrounds to join, transact, and mine [35]. There are no restrictions; anyone can join the network, access blockchain data, and validate and record transactions. Therefore, these are also called permissionless blockchains. Every participant is given full authority to read and write transactions, perform auditing in the blockchain, or review any part of the blockchain at any time. Bitcoin is one of the most well-known examples of a public blockchain. Every participant can join the Bitcoin network by downloading the software and contributing computing power. Transactions are validated and recorded by nodes on the network, and the data is publicly accessible to anyone with an internet connection. Another example is Ethereum, a public blockchain platform with smart contract functionality.

By contrast, in a private blockchain network, a central entity decides and attributes the right to individual peers to participate in the write or read operations of the blockchain [41]. This means they are only partially decentralized; only approved participants can join the network and access the data. Thus, permissioned blockchain networks may also be used by organizations that need to control and protect their blockchain more tightly. The most widely known instances of permissioned blockchains are Hyperledger Fabric and R3 Corda [5]. Consortium or hybrid blockchains combine features from public and private blockchains. Instead of being controlled by a single entity, consortium blockchain networks are partially private, operated by a group of organizations, and governed collectively. This means they have privileged permissioned nodes across the network to operate it. This type of blockchain can be helpful for large organizations with multiple stakeholders, all sharing specific control and privacy levels. Representative examples of hybrid blockchains include Dragonchain and IBM Blockchain.

Being a decentralized system, blockchain systems do not need a third-party trusted authority. Instead, blockchain adopts the decentralized consensus mechanism to guarantee the reliability and consistency of the data and transactions. In the existing blockchain systems, there are five major consensus mechanisms: PoW (Proof of Work), PoS (Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), PoA (Proof of Authority), and DPoS (Delegated Proof of Stake). PoW is the consensus algorithm used in Bitcoin. Its core idea is to allocate the accounting rights and rewards through the hashing power competition among the nodes [27]. The PoW mechanism uses the solution of puzzles to prove the reliability of the data. The puzzle is usually a computationally complex but easily verifiable problem. When a node creates a block, it must resolve a PoW puzzle. After the PoW puzzle is resolved, it will be broadcast to other nodes to achieve the purpose of consensus. PoW takes the workload as a safeguard to effectively guarantee the blockchain's safety. However, at the same time, its limitations are high energy consumption and poor scalability. Instead of investing in powerful hardware to perform intensive computations for hash calculations in a proof-of-work system, proof of stake suggests purchasing cryptocurrency and using it as a stake within the network. A cryptographic random algorithm selects leaders to generate new blocks rather than solve puzzles. The probability of being selected depends on how many stakes the node has [43]. People with more currencies are believed to be less likely to attack the network. As a result, the attackers need to accumulate many coins and hold them long enough to attack the blockchain. This also greatly increases the difficulty of attack [27].

PBFT is a replication algorithm to tolerate byzantine faults [8]. Hyperledger Fabric utilizes the PBFT as its consensus algorithm since PBFT can handle up to 1/3 malicious byzantine replicas. As a permissioned and network-intensive consensus mechanism, PBFT ensures the security of the ongoing transactions among acknowledged participants, but it cannot scale to large networks. This makes it a perfect fit for private blockchains [22]. Proof of Authority has been proposed as an underlying consensus algorithm for permissioned blockchains. Ethereum Proof-of-Authority is designed for enterprise-ready permissioned blockchain and was released on Azure. The system is not anonymous. Each participating node has one and only one known and reputable identity [43]. The major difference between PoS and DPOS is that PoS is directly democratic while DPOS is representative democratic [48]. All stakeholders can vote to determine who is trusted to generate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions. The blockchain using DPoS is more efficient and power-saving than PoW and PoS.

2.2 Smart Cities

A formal definition of smart cities is given in [11]: "A smart city is a system that enhances human and social capital wisely using and interacting with natural and economic resources via technology-based solutions and innovations to address public issues and efficiently achieve sustainable development and high quality of life". Based on the definition, smart cities bring together human, organizational, and technological elements to drive sustainable growth and enhance residents' quality of life. A conceptual framework of smart cities is charted in Figure 1.

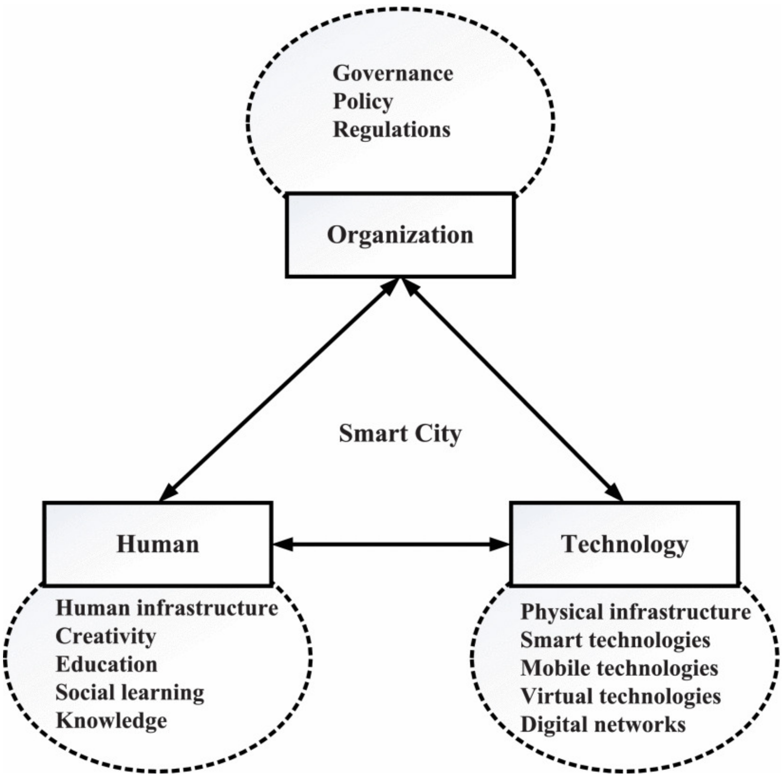


Figure 1. A conceptual framework of smart cities [42].

Nam and Pardo explain why the term smart city is becoming more widespread and accepted in solving new urbanization challenges [29]. 'Smartness' is centered on a user perspective and is better than the more elitist term 'intelligent.' 'Smart' means to be able to self-adapt and provide customized interfaces and services to user needs, which is more user-friendly than 'intelligent,' which implies having a quick mind and being responsive to feedback [45]. Institutional infrastructure, physical infrastructure, social infrastructure, and economic infrastructure are considered the four pillars of a smart city [28]. The governance of smart cities comes under the institutional infrastructure. It focuses on clear decision-making, citizen involvement, and cooperation between agencies. Technocratic governance uses data and technology to improve urban services and policies [19]. Physical infrastructure includes natural resources and built environments like ICT networks, transportation, and energy systems. Urban development now focuses on sustainability. This means saving resources, planning cities in eco-friendly ways, and using smart utility systems [39]. Social infrastructure is about intellectual capital, human capital, and QoL. Citizen awareness, responsibility, and commitment play a key role in popularizing the smart city concept. Hence, social infrastructure becomes crucial for the evolution and sustainability of a smart city. And this will help with innovation, education, and community growth [30]. The economic infrastructure supports economic and job growth in smart cities. It involves digital changes in industries, smart manufacturing, and e-commerce. The success of a smart economy can be measured by key indicators like public expenditure on research and development, GDP per head of city population, and employment rate in various industries [33].

Table 2 presents examples of smart cities worldwide that have integrated blockchain into their urban development initiatives. It highlights various efforts by smart cities to leverage blockchain to enhance governance, connectivity, and data security.

Table 2. Examples of Smart Cities Worldwide and Their Blockchain Initiatives

City	Blockchain Initiatives and Smart City Efforts
Dubai	Dubai aims to create and share intellectual capital related to its Blockchain adoption by developing case studies for each city pilot. In April 2018, Smart Dubai launched the Smart Cities Global Network, the largest international network of smart-city stakeholders. The network includes members from government, private industry, academia, and media. Dubai is a pioneer in Blockchain technology, with a clear vision to become a global leader in this domain.
Singapore	Singapore is a prime example of a smart city, with efforts centralized under the Smart Nation initiative launched in 2014. The initiative aims to create a technical architecture for the world's first Smart Nation, including IoT standardization and the development of the Smart Nation Platform. This platform provides enhanced connectivity, nationwide IoT sensor networks, and data analytics capabilities.
Barcelona	Barcelona ranks highly in smart city comparisons. The Decode project, an EU-funded initiative, develops a blockchain-based architecture for data sovereignty. It aims to create a framework for secure and traceable data sharing across the internet, using decentralized technologies like Bitcoin, Blockstack, and Sovrin.

2.3 Technology Selection Toolkit and its Purpose

Technology selection is concerned with choosing the best technology from several available options. Technology selection involves choosing a technology that a firm views as most suitable based on considering its technological, organizational, and business environments [37]. A Technology Selection Toolkit is a structured collection of assessment tools or methods designed to help decision makers systematically compare and select multiple technology options. Such tools typically combine qualitative and quantitative methods and are based on various metrics such as cost, performance, scalability, interoperability, compliance, and fit with organizational goals. From a scientific perspective, selection toolkits are grounded in multi-criteria decision-making (MCDM) theories such as the Analytic Hierarchy Process (AHP), the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), or fuzzy logic. These techniques help transform complex decision-making scenarios into rational, traceable, and repeatable processes, reducing cognitive biases and ad hoc reasoning.

The dispersion of technology sources across organizations, geographical locations, and countries, and the resulting obscurity, makes accessing suitable technologies and selecting the most suitable option more difficult [7]. Generic tools exist to help with technology selection decisions, e.g., decision support tools. However, the abundance of technological options, organizational complexity of the receiving company, and dynamism of the business environment necessitate a specific method for selecting technology that can be applied in practice [37]. Consequently, developing customized technology selection toolkits tailored to specific contexts or domains becomes essential. These specialized toolkits can provide more accurate, relevant, and actionable insights by considering the target environment's unique requirements, constraints, and strategic objectives. In contrast to generic decision-support tools, domain-specific toolkits are better equipped to incorporate domain knowledge, stakeholder preferences, regulatory constraints, and contextual performance indicators. For example, in the context of smart cities, a blockchain selection toolkit must consider factors such as transaction latency, data privacy, scalability under high user load, and compatibility with existing digital infrastructure. A customized toolkit improves the robustness and transparency of the decision-making process and facilitates alignment between technological capabilities and the practical needs of end-users and institutions. Therefore, such toolkits are critical in reducing decision uncertainty, ensuring technology adoption success, and enhancing the overall strategic fit between selected technologies and organizational or urban goals.

3 Systematic Literature Review

This section presents a Systematic Literature Review (SLR) to demonstrate existing blockchain-based applications in smart city domains and justify why different types of blockchain are selected for various applications within smart cities. The SLR methods and structure were guided by the Kitchenham review guidelines [17]. Different global use cases are reviewed and summarized from the perspective of using blockchain for smart cities to compare different technology selections based on different scenario requirements. The results from the SLR are presented in Section 3.6. Furthermore, this provides literature support for the design and development of the toolkit in Section 4. The review focuses on answering the research question **RQ1: What are the existing blockchain-based applications in smart city domains?** The results are systematically analyzed, classified, and compared. To answer **RQ2: How are different blockchain solutions being compared in smart city infrastructure regarding energy efficiency, security, and scalability?** Section 3.1 provides the review questions developed for the research questions above. The search queries used to find the related research are in Section 3.2. The selection criteria used to filter the relevant papers are given in Section 3.3. Literature selection in Section 3.4 describes the selection process of the papers. The strategy for extracting relevant data is described in Section 3.5. The outcomes of the SLR, derived from the data extraction strategy, are provided in Section 3.6.

3.1 Review Questions

We develop the four review questions corresponding to RQ1 and RQ2 to perform the SLR, which are defined as follows:

RQ1.1: What are the motivations for adopting blockchain in smart city domains?
RQ1.2: In which areas are various types of blockchains utilized in smart cities?
RQ2.1: Are there trade-offs between the choice of blockchain technology?
RQ2.2: What criteria determine the choice of blockchain type for a specific scenario?

3.2 Search Queries

The preparative data sources for the literature review are IEEE digital library, ScienceDirect, Scopus and ACM digital library. The primary reason for choosing these databases lies in their reputation as leading sources for up-to-date technological research papers. The search strategy employed a structured query using Boolean operators to ensure comprehensive retrieval of relevant studies. The search terms were formulated as:"("smart cities" OR "intelligent cities") AND ("blockchain technology" OR "distributed ledger") AND ("application domains" OR "use cases") AND ("energy efficiency" OR "power consumption" OR "energy metrics") AND ("security" OR "scalability" OR "trade-offs") ". This query was designed to capture the intersection between blockchain technologies and various aspects of smart city development. The initial selection criterion required that these search terms appear in either the title or abstract of the papers, ensuring that the papers are directly relevant to the research focus.

3.3 Selection Criteria

The systematic literature review ensures a complete and focused collection of relevant studies. The chosen Exclusion Criteria (EC) are meant to refine the search results by narrowing the scope to recent, high-quality, and directly relevant literature. The exclusion criteria focus on removing non-English publications, old studies (published before 2015), and literature that does not clearly mention blockchain technology or its relevance to smart cities. The Inclusion Criteria (IC) are made to find literature that gives useful insights into the use, impact, and future potential of blockchain technology in smart cities. This includes studies that focus on specific smart city areas, provide empirical data or theoretical frameworks, and discuss challenges and future directions. The inclusion and exclusion criteria are shown below:

Inclusion criteria

- IC1: Literature focusing on the implementation of blockchain technology in specific smart city domains.
- IC2: Literature that provides empirical data, case studies, or theoretical frameworks on blockchain integration in urban infrastructure, governance, or services.
- IC3: Literature that discusses metrics used to evaluate the cost-effectiveness of blockchain solutions in smart cities.

Exclusion criteria

- EC1: Exclude literature not in the English language.
- EC2: Literature that is not journals, magazines, or conference papers.
- EC3: Literature without explicit mention of specific use cases.

3.4 Literature Selection

The literature search was conducted across IEEE Xplore, ACM Digital Library, and Web of Science, resulting in 1,689 records. After removing duplicates, 933 records remained for screening. During the title screening phase, 878 records were excluded as irrelevant, leaving 55 records for abstract screening. After evaluating the abstracts, 30 records were excluded, and 25 full-text articles were assessed for eligibility. Among those, nine articles were excluded for specific reasons (e.g., off-topic or insufficient data), resulting in 16 articles ultimately included for in-depth study(see Figure 2).

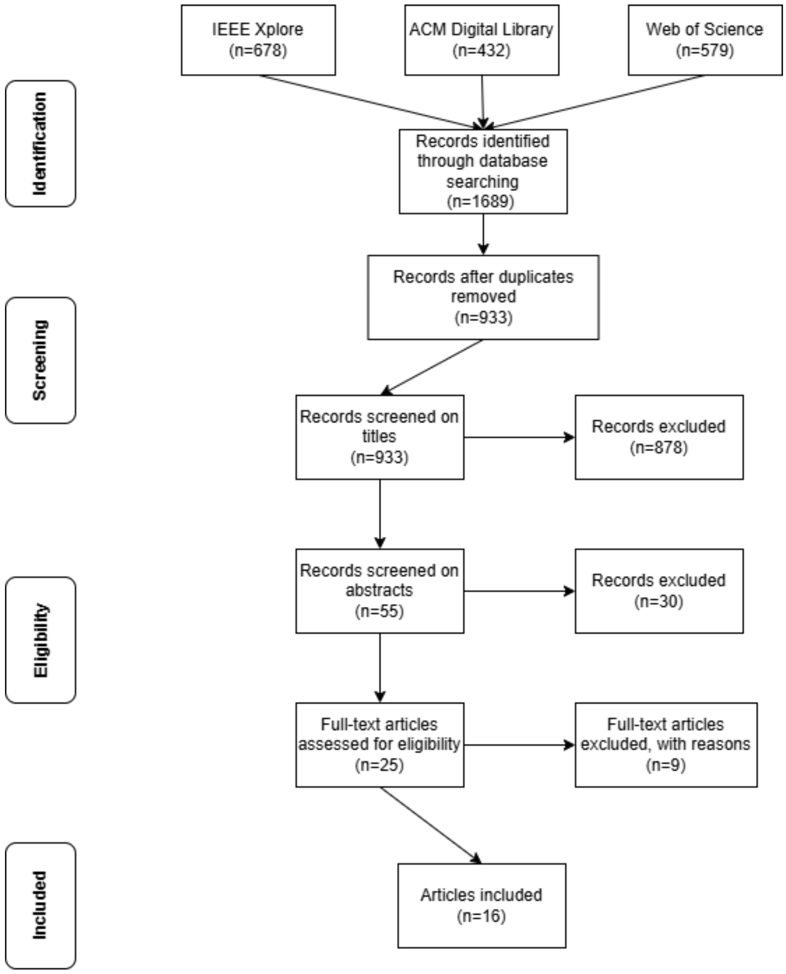


Figure 2. Review process of systematic literature review

3.5 Data Extraction

Sixteen papers were read through to gather data for the review questions. The data found in the research papers, which could answer the research questions, are noted in a table for further analysis. The data extraction table (as Table 3 shows) consists of the data items as research work, application, blockchain technology, consensus algorithm, cost, smart contract, and data storage. These data items were chosen in accordance with the RQs.

Table 3. Data Extraction Form

Data Item	Value
Research Work, Year	Citations and Year of publication
Application	Area of blockchain usage
Blockchain Technology	Specific blockchain type
Consensus Algorithm	Consensus mechanism adopted in the project
Cost Efficiency	Cost analysis
Smart Contract	Use of self-executing smart contracts
Data Storage	Architecture for storing the data

3.6 SLR Results

In this section, the review outcomes are summarized in Table 4, which presents the application areas of the selected studies in alignment with the research questions outlined in Section 3.1. The studies are categorized based on their blockchain application domains. As shown in Table 4, among the 16 reviewed papers, three studies focus on the smart grid sector, three are related to smart transportation, two address supply chain management, two explore healthcare applications, one is concerned with education, one focuses on EV charging, one is related to land registration, one addresses e-voting, one explores local energy trade, one focuses on agriculture, and one targets food trading.

Table 4. SLR Results Categorized Based on the Blockchain Applications, Types, and Consensus Algorithms

Study	Application	Blockchain Technology	Consensus Algorithm	Details
[14]	Educational Data Management	Ethereum Stellar	Proof of Work Federated Byzantine Fault Tolerance	A management system that provides a secure and publicly verifiable system for educational data. Student data is recorded through smart contracts and blockchain, initially in a case pilot in the Cambridge Public School District in the United States.

Continued on next page

Table 4 – continued from previous page

Study	Application	Blockchain Type	Consensus Algorithm	Details
[10]	Electric Vehicle Charging Management	Ethereum	Proof of Work	An Ethereum-based EV charging management framework for decentralized and management of the charging process through smart contracts, validated at a real demonstration site in Switzerland.
[2]	Land title registration	Bitcoin Exonum	PBFT PoW	Georgia's National Agency of Public Registry (NAPR) has partnered with Biffury to manage the registration of land titles through the private Exonum blockchain and anchor transaction

Continued on next page

Table 4 – continued from previous page

Study	Application	Blockchain Type	Consensus Algorithm	Details
[9]	E-voting system	Ethereum MetaMask	Casper Proof-of-Stake	An Ethernet blockchain-based e-voting system that ensures security, transparency and privacy concerns in elections. The system automates voter registration, voting, and counting through smart contracts, and uses encryption technologies such as SHA-256 hashing, ECDSA signatures, and Zero Knowledge Proof (ZKP) to ensure data security.VoteChain also supports offline voting functionality for areas with limited infrastructure, and has been validated for scalability through performance testing (supporting 100,000 concurrent users with a TPS of 1200).
[31]	Mobile Healthcare	Consortium Blockchain	Proof of Work	A decentralized data management system based on a federation chain for securely managing health data in mHealth. The system implements data collection, etc. through a layered architecture, uses IPFS as an off-chain storage solution, and ensures data security and privacy through encryption and digital signatures.

Continued on next page

Table 4 – continued from previous page

Study	Application	Blockchain Type	Consensus Algorithm	Details
[26]	Microgrid Energy Markets	Private Blockchain	Tendermint Protocol	A blockchain-based local energy trading platform that allows consumers and producers to trade renewable energy via P2P. The system uses private blockchain technology to enable decentralised transactions and supports smart contracts and real-time energy pricing.
[47]	Secure PHI sharing in e-Health systems	JUICE	Proof of Conformance	The BSPP protocol enables privacy-preserving PHI sharing among hospitals using private blockchains and a consortium blockchain. It includes encrypted keyword search, identity protection via pseudo-identities, and time-controlled access.
[12]	Food traceability	Hyperledger Fabric	PBFT	A blockchain- and IoT-based traceability system for agricultural products. By using IoT devices for real-time data collection, and stores data on a permissioned blockchain network built with Hyperledger Fabric. The architecture includes clients (sensors), a business logic server, and a smart contract-enabled blockchain backend to ensure reliable, tamper-proof tracking throughout the food supply chain.

Continued on next page

Table 4 – continued from previous page

Study	Application	Blockchain Type	Consensus Algorithm	Details
[25]	Food trading platform	Ethereum	Improved Practical Byzantine Fault Tolerance	An automatic food trading platform built on a consortium blockchain using Ethereum. It includes smart contract lifecycle management, optimized transaction matching, and a double auction mechanism to facilitate fair and efficient trading between stakeholders. Smart contracts are used for negotiation, execution, and rollback management in the event of product quality issues.
[1]	Smart grid	Ethereum	Proof of Work	A blockchain-based system for managing electricity transactions in smart grids. It utilizes Ethereum's smart contracts to automate and secure transactions between producers and consumers. The system ensures immutability of transaction records, enabling traceability and dispute resolution.

Continued on next page

Table 4 – continued from previous page

Study	Application	Blockchain Type	Consensus Algorithm	Details
[4]	Vehicular Communications	IBM Blockchain	-	The paper surveys security and privacy challenges in modern cars, covering intra-vehicle networks, gateways, and inter-vehicle communications. It references Blockchain as a potential solution for tracking part provenance in the automotive supply chain.
[36]	Automotive industry in smart cities	Private Ethereum blockchain	Fruit Fly Optimization Algorithm	A blockchain-based distributed framework to manage the entire lifecycle of vehicles in a smart city, from manufacturing and sales to leasing, maintenance, and recycling. Smart contracts are used at each phase to ensure trust and traceability. A novel miner selection algorithm based on FOA enhances mining efficiency.

Continued on next page

Table 4 – continued from previous page

Study	Application	Blockchain Type	Consensus Algorithm	Details
[16]	P2P electricity trading among hybrid EVs	Consortium blockchain (custom-built)	Proof of Work	A secure and decentralized electricity trading system enabling PHEVs to trade surplus energy locally at hotspots. The system employs consortium blockchain maintained by authorized local aggregators, who act as brokers and auditors. Privacy is preserved using pseudonyms, and rewards (energy coins) incentivize energy contributions.
[38]	Smart energy trading	Custom blockchain framework	Byzantine Fault Tolerant Consensus	A blockchain-secured energy trading model where parked EVs act as distributed energy storage, supplying power to the grid during peak demand. Communication is facilitated by SCADA, with bidirectional information and power flows. The blockchain ledger, protected by SHA-256 hashing and Byzantine consensus, secures transactional and energy data, ensuring system resilience against cyberattacks.

Continued on next page

Table 4 – continued from previous page

Study	Application	Blockchain Type	Consensus Algorithm	Details
[23]	Supply chain management	UnicalCoin	Proof of Work	A blockchain-enabled supply chain framework using a software connector that integrates enterprise information systems with an Ethereum-like blockchain. Results show blockchain improves data trust, discourages information falsification, and reduces negative effects of data asymmetry across supply chain echelons.
[40]	Supply chain management	Custom Ethereum	Not explicitly specified(similar to PBFT)	A framework to solve fragmentation, poor traceability, and lack of real-time information in the precast supply chain. Four participants (owner, contractor, precast plant, and logistics company) who share a distributed ledger of operations related to precast components. Each operation is recorded as a transaction validated by all endorsing peers via smart contracts.

3.7 Comparative Analysis of Blockchains in Smart Cities

This section analyzes, compares, and summarizes the usage scenarios of different blockchains in the smart cities domain (Table 5). For example, in smart cities, the choice and selection of blockchain type, e.g., public, private, or consortium, can affect the urban solutions' efficiency, security, and scalability. Public blockchains are suitable for applications that need high security and resistance to censorship, like education, because of their decentralization and transparency. On the other hand, private blockchains provide controlled environments with strong privacy and faster transaction speeds, making them suitable for e-voting and land registration, though they lose decentralization. Consortium blockchains offer efficiency and transparency, helping organizations work together in local energy trade and healthcare. Still, they need a complex governance structure and trust between participants.

Table 5. Comparative Analysis of Blockchains in Smart Cities

Feature	**Public Blockchain**	**Private Blockchain**	**Consortium Blockchain**
Access Control	Open to everyone	Restricted to specific participants	Combination of public and private
Efficiency	Low	High	High
Privacy	Low	High	High
Governance	Decentralized	Centralized	Mixed governance structure
Transparency	High	Low	Variable transparency
Scalability	Limited scalability	High scalability	High scalability potential
Security	High	Low	Variable security
Transaction Speed	Slower	Faster	Variable speed
Examples	Bitcoin, Ethereum	Hyperledger	Quorum, Hyperledger, Corda

3.7.1 Public Blockchains in Smart Cities

Kratos is a secure, authenticated, and publicly verifiable educational data management system developed using blockchain to address current issues of privacy protection, data ownership, data access control, and data interoperability in educational data management [14]. The system employs smart contracts to define data access rules between schools and educational technology (edutech) providers and uses blockchain deposits to provide a tamper-proof data access record. Kratos guarantees data transparency through a decentralized architecture, making educational data management more secure and efficient and empowering students to take control of their own data. Kratos uses different blockchain platforms to optimize the system's performance and cost, primarily considering Ethereum and Stellar. Ethereum initially used PoW and later moved to PoS, which supports complex smart contract execution but has high transaction costs. In contrast, Stellar uses the PBFT, which provides low-latency, low-cost transaction validation. Kratos adopted Stellar for data timestamping depositories in an early release to ensure low cost and high throughput, and is planning to deploy smart contracts on Ethereum to improve data transparency and auditability.

Kratos digitizes education data access protocols through smart contracts and stores them on the blockchain to ensure transparency and compliance with data access. On Ethereum, smart contracts can directly execute and store access logs, making data access and usage rules auditable and tamper-proof. On Stellar, as it does not support complex smart contracts, Kratos employs an indirect deposit method, whereby hashes of contract execution are submitted to the blockchain regularly, ensuring that data access behavior can be verified.

As for blockchain transaction costs, Ether has higher transaction fees (gas fees) and is subject to volatility, while Stellar has lower transaction costs and is better suited for frequent data depository and access log storage. As a result, Kratos chose Stellar as its primary depository platform and plans to execute more complex smart contracts on Ether to balance cost and auditability. Kratos uses a two-tier architecture combining blockchain, decentralized storage (IPFS), and the traditional database PostgreSQL to optimize data management. Blockchain is mainly used to store data access logs and timestamps, while IPFS is used to store encrypted educational data to ensure data integrity and security. Meanwhile, PostgreSQL, an efficient relational database, is responsible for storing and managing data indexes to improve query efficiency.

With the popularity of electric vehicles and the growing demand for charging infrastructure, the traditional centralized energy management model shows some limitations when facing high-frequency user demand. In order to enhance the transparency, security, and efficiency of EV charging, a charging management framework based on the Ethereum public blockchain has been introduced, deployed, and tested in a real-world scenario in Switzerland [10]. The framework is based on Ethereum and initially used PoW as the consensus mechanism but gradually transitioned to PoS with the advancement of Ether 2.0. PoW adds new blocks by solving complex mathematical problems with high computational costs and energy consumption. PoS, on the other hand, selects block validators based on the number of coins held and the length of locking, thus significantly reducing energy consumption while improving transaction processing efficiency.

Smart contracts are the core component of this charging management framework. Each charging station and EV is identified by a unique Ethereum address and registered in the smart contract. When an EV finishes charging, the charging station sends information such as charge volume and time stamp to the smart contract, which automatically settles and updates the ledger. Each participant (charging station, EV user) has an energy account that records its energy supply and consumption, ensuring the accuracy of the transaction. Written in the Solidity language and rigorously tested, the smart contract code automatically executes charging transactions using smart contracts, ensuring that exchanging energy between charging stations and EV users is open, trustworthy, and requires no intermediaries. When using a public blockchain, the cost is mainly the transaction fee (gas fee) and smart contract deployment cost. Gas Fee: Transaction fees on the Ethernet network are calculated by gas and are affected by network congestion. Experiments on a test network (Ropsten) have shown that the average gas fee for a single charge transaction is about 0.00074103 ETH (about 1 CHF). Smart Contract Deployment Costs: Deploying smart contracts consumes a large amount of gas, the cost of which depends on the complexity of the contract.

Regarding data storage, the framework adopts on-chain and off-chain storage schemes. For on-chain storage, the smart contract will record the core data of the transaction, such as the amount of charge, the addresses of both parties to the transaction, and the transaction timestamp. The data stored on-chain is highly reliable due to the non-tampering nature of blockchain. For off-chain storage, in order to reduce gas cost, a large amount of non-critical data (e.g., real-time status of charging station, EV charging history, etc.) is stored in InfluxDB and MySQL database and interacted with blockchain through API. This data storage method takes into account security, cost control, and data query efficiency, which not only ensures the tamperability of critical data but also reduces the cost of blockchain storage.

The viability of blockchain in EV charging management depends mainly on its transaction throughput, latency, and scalability. Currently, the transaction throughput of the Ethereum mainnet is about 15 TPS. However, with Ethereum 2.0 and Layer 2 solutions (e.g., Optimistic Rollup), it is expected to be increased to more than 1,000 TPS, which can support high-frequency EV charging transactions. Experimental results show that this framework's average transaction confirmation time is about 13.7 seconds, which can meet the real-time demand of EV charging settlement. In addition, by adopting the Layer 2 scheme, the system can support more extensive EV charging networks while maintaining decentralization to ensure the security and trustworthiness of the transactions.

3.7.2 Private Blockchains in Smart Cities

The National Agency of Public Registry of Georgia (NAPR) has introduced blockchain technology in the field of land registration to provide secure and transparent digital land certificates [2]. The system uses the Exonum framework to build a private blockchain and data integrity checks with the help of the Bitcoin blockchain. NAPR, in partnership with the Bitfury Group, launched the project in April 2016 to increase public trust in the land registry system, as well as reduce corruption and disputes over property rights. The system's private blockchain uses a consensus mechanism similar to PBFT. This mechanism comprises known and authorized nodes (NAPRs and Notaries) responsible for transaction validation and block generation. Consensus of transactions requires the agreement of most nodes, thus guaranteeing data immutability and high availability. Only one full node is required to recover the entire blockchain data, ensuring regular operation in case of individual node failure. The consensus mechanism improves the security and efficiency of the system and is suitable for NAPR's permission-based environment.

Currently, the system is mainly used for land registration and verification, and smart contracts have not yet been fully implemented. However, in the future, smart contracts will be added to support leasing and mortgages so that leasing and mortgage agreements can be automatically executed through blockchain, automatically transfer ownership, reduce manual approval, and improve transaction efficiency. To meet the high throughput demands of land registration, the Exonum blockchain has a transaction processing capacity of up to 5,000 TPS, which is much higher than public chains such as Bitcoin and Ether. The key performance of this system is that it can support massively concurrent transactions, ensuring no delays in land registration, as well as fast validation, reducing the time for searching and validating land certificates from 1-3 days to a few minutes, significantly improving efficiency. As transactions are mainly executed on the private chain, the system is not affected by the congestion and high costs of the public chain. This performance enables NAPR to manage land registry transactions nationwide efficiently.

VoteChain is an e-voting system developed based on blockchain and designed specifically for the Palestinian electoral environment [9], aiming to solve the problems of security, transparency, and efficiency in traditional elections. The system adopts a private chain architecture and ensures that only authorized users can participate in voting through strict permission management, thus effectively preventing unauthorized access and data tampering. VoteChain introduces the CasperPoS mechanism regarding the consensus algorithm. Compared with the traditional PoW, Casper PoS can punish malicious nodes through the pledge mechanism, which reduces energy consumption and improves the system's security and efficiency. The system uses smart contracts written in Solidity to manage voter registration automatically, candidate information entry, voting transaction processing, and result counting, ensuring that the entire election process is carried out in strict accordance with the pre-set rules, minimizing human intervention, and guaranteeing the transparency and non-tamperability of all operations. In order to reduce the high storage and transaction costs on the blockchain, VoteChain adopts an off-chain data storage solution, storing ballots and transaction records on the Ethereum blockchain.

In contrast, sensitive data such as voter identity information is stored in offline databases such as MongoDB, which not only optimizes data querying performance but also effectively controls the overall cost of the system. To ensure voter privacy and security, the system introduces several advanced encryption technologies, such as SHA-256 hash, elliptic curve digital signature, zero-knowledge proof, and homomorphic encryption, which not only ensure data integrity and tampering but also make the voter's specific voting content always encrypted and not leaked during the verification process. Meanwhile, VoteChain focuses on high throughput and low latency in its system design to meet large-scale election performance requirements. As proven by large-scale concurrency tests, the system is able to maintain an average transaction completion time of less than 2 seconds in the face of up to 100,000 concurrent users, with a system availability of more than 99.98%, a transaction processing capacity of 1,200 TPS and network latency within a reasonable range. Network latency is kept within reasonable limits. In summary, VoteChain provides a practical solution for secure, transparent, and efficient e-voting by adopting an advanced consensus algorithm, smart contract mechanism, cost-optimized data storage solution, and comprehensive privacy protection technology, which fully demonstrates the great potential of blockchain technology in modern election systems.

3.7.3 Consortium Blockchains in Smart Cities

With the rapid development of mobile health, medical devices and applications are constantly collecting a large amount of health data. The traditional centralized data management model faces serious security challenges, such as a single point of failure and distributed denial of service attacks. To solve these problems, HealChain [31] is proposed as a decentralized data management system based on a federated blockchain in order to ensure secure storage, reliable transmission, and verifiability of medical data. HealChain uses Proof-of-Work as a consensus mechanism to ensure the authenticity and non-tampering of data. Under this mechanism, Consortium Blockchain Nodes compete for bookkeeping rights by solving PoW algorithmic puzzles, and successful miners are rewarded with blocks. The consensus mechanism can withstand a Sybil Attack, but the computational cost is high. HealChain adopts an optimized computational resource allocation strategy through the Genetic Algorithm to enable miners to balance computational costs and economic benefits. PoW has better security and decentralization characteristics in large-scale medical data management compared to the traditional PBFT. However, due to the high computational overhead of PoW, HealChain adopts a computational power optimization model to reduce the energy consumption of miners.

In terms of smart contracts, HealChain includes data validation, whereby when a user uploads medical data, the smart contract automatically verifies the authenticity of the data, including digital signatures and digital certificates. There is also an incentive mechanism whereby miners can automatically receive block rewards through smart contracts after performing data verification tasks. The smart contract is maintained by the medical institutions (e.g., hospitals, clinics, etc.) in the alliance blockchain network, ensuring the legitimacy and fairness of the transaction while avoiding the trust issues that may be faced by traditional centralized systems. HealChain has conducted an in-depth study on cost optimization. For storage cost, it adopts Off-chain Storage, storing large-scale medical data in IPFS and storing the data hash index only on the blockchain, thus significantly reducing the storage burden of the blockchain. This approach combines the security of the blockchain with the scalability of IPFS to reduce data redundancy and improve storage efficiency. HealChain adopts a three-layer architecture to ensure efficient data storage and security, which consists of the user, blockchain, and storage layers. In the Blockchain Layer, a federated blockchain consisting of multiple CBNs is responsible for data auditing and authentication, and the blocks contain medical data hashes, digital signatures, and user identity information to ensure data integrity and traceability. The block contains medical data hash value, digital signature, and user identity information to ensure data integrity and traceability.

Brooklyn Microgrid [26] is a Consortium Blockchain-based local energy trading platform that aims to enable peer-to-peer energy transactions between consumers and producers through a decentralized approach. The project uses the Tendermint protocol as its blockchain infrastructure, demonstrating the potential of Consortium Blockchain for real-world applications in the energy market. BMG's blockchain network uses the Tendermint consensus algorithm, a consensus mechanism based on Byzantine Fault Tolerance, where Tendermint validates transactions through pre-selected trusted nodes, ensuring efficient and secure transaction confirmation. This consensus mechanism is particularly suitable for federation chain scenarios as it can provide high transaction throughput and low latency while maintaining decentralization.

BMG's energy trading platform relies on smart contracts to automate the trading process. Smart contracts are executed on the blockchain to ensure transparency and tamperability of transactions. For example, when a consumer and a producer enter into a transaction agreement, the smart contract automatically allocates and makes payments without needing a third-party intermediary. This automated mechanism improves transaction efficiency and reduces the risk of human error and fraud. Compared with public chains, federated blockchains have lower operating costs. BMG's blockchain network adopts a Proof-of-Identity (PoW) mechanism instead of the computationally intensive PoW mechanism, significantly reducing energy consumption and computational resource waste. In addition, since transactions are only conducted between authorized community members, the network's computation and storage requirements are relatively small, reducing operational costs.

BMG's blockchain network employs distributed ledger technology, storing all transaction data on multiple nodes, ensuring data redundancy and reliability. Due to the limited number of participants in the alliance chain, the scale of data storage is relatively controllable, avoiding the problem of data inflation common in public chains. In addition, BMG's blockchain platform integrates the TransActive Grid meter, which can record energy production and consumption data in real time and write this data directly to the blockchain, ensuring real-time data availability and accuracy. In terms of privacy protection, BMG's blockchain network ensures the privacy of transaction data through authentication mechanisms and encryption. Only authorized participants can access transaction information; all transaction data is encrypted to prevent unauthorized access and tampering. In addition, BMG's blockchain platform supports anonymous transactions, further protecting user privacy. BMG's blockchain network is designed with performance requirements in mind. The Tendermint consensus algorithm can support high-throughput transaction processing, ensuring that confirmation of a large number of transactions can be completed in a short period. In addition, due to the limited number of participants in the alliance chain, the network has low latency and can meet the demand for real-time energy transactions. BMG's blockchain platform also has good scalability and can be flexibly scaled up with the increase in the number of users, ensuring the system's long-term stable operation.

3.8 Challenges of Blockchain Integration in Smart Cities

During the implementation of blockchain technology into a smart city, there are always indispensable open research challenges. In this section, we discuss some challenges and issues in current studies.

Security and privacy are two major challenges in blockchain-based smart city systems. Citizens cannot use a system that does not guarantee the privacy of citizens' data and is not resistant against cyber-attacks [24]. For example, public blockchain networks are fully transparent and any participant can audit the entire transaction record. Although devices interact with each other via pseudo-anonymised public addresses, these identifiers are still a privacy risk - a malicious act with external contextual information can correlate the address with the transaction pattern, allowing for user de-anonymisation. In cryptocurrency-based smart city applications, the use of safeguards such as disposable temporary addresses can effectively reduce this risk of privacy exposure. In addition to this, as the public properties of blockchain make user data and pseudonymous identities publicly accessible, some advanced privacy-preserving techniques, such as distributed consent management based on zero-knowledge proofs and double-blind data sharing, can enable selective anonymised data exchange in multi-party transactions in smart city ecosystems [46]. While on-chain encryption methods can protect transactional data, their implementation tends to introduce additional latency, resulting in a trade-off between privacy and system performance.

Latency, the time required for transaction processing, and throughput, which represents the maximum number of transactions that can be processed by the system in a given time period, together determine the scalability of a blockchain application. In blockchain-enabled smart cities, latency mainly stems from the computational time consumed by nodes and is further exacerbated by communication between nodes, and these two types of latency together determine the final performance of the network. Therefore, a low-latency, high-throughput blockchain smart city system must be achieved through multiple technical solutions. Forking effects triggered by propagation delays can significantly affect the performance of the system. For example, when a miner who successfully generates a block broadcasts it to the whole network, other miners may preemptively broadcast their own blocks before receiving the block, resulting in multiple competing blocks in the network. To eliminate forking, [6] uses a nearest neighbour selection scheme (CNS) to reduce the network propagation delay; another scheme [18] identifies forking through an acknowledgement mechanism when receiving a new block. Once a fork occurs, the block generation process is restarted until the update of the forkless block is completed. However, this fork effect leads to probabilistic transaction confirmations.

Energy efficiency has always been one of the core objectives of smart cities [32]. With increasingly stringent environmental standards and rapidly escalating energy costs, energy efficiency has been given high priority. However, certain consensus mechanisms (e.g., PoW) have extremely high computational costs. In PoW, all blockchain nodes need to perform complex computations to mine new blocks, and this redundant computation makes PoW a non-energy-efficient solution that consumes a large amount of electrical energy. Researchers are developing new consensus mechanisms for blockchain systems with lower computational costs. Schemes such as Delegated PoS (DPoS) and Byzantine fault-tolerant class algorithms have been proposed. However, the security of PoS and DPoS has not been rigorously verified, while Byzantine fault-tolerant algorithms usually suffer from a lack of scalability, making them difficult to apply to systems involving thousands of participants. Some researchers have proposed a new type of consensus protocol called ‘proof of trust’, which solves the problems of high energy consumption and security flaws of existing protocols through a trust model. These consensus mechanisms are promising, but are still in the early stages of development. Therefore, it is valuable to study energy-efficient consensus mechanisms for blockchain systems.

3.9 Summary

This chapter conducted a systematic literature review to methodologically analyze the current applications and rationale for the technological selection of blockchain in smart city domains. Guided by the Kitchenham framework, we ultimately synthesized 16 pivotal works through multi-stage screening. The research addressed two primary objectives: RQ1 identified blockchain implementations across 12 smart city sectors including smart grid, transportation management, and healthcare; RQ2 revealed technical trade-offs among public, private, and consortium blockchains through comparative analysis of energy efficiency (e.g., PoW energy consumption), security (e.g., Byzantine fault tolerance mechanisms), and scalability (e.g., TPS performance). These findings provided critical theoretical foundations for the toolkit design in Chapter 4, while uncovering significant challenges in privacy preservation and energy efficiency within existing research.

4 Blockchain Selection Toolkit

In the process of smart city construction, blockchain technology has gradually gained attention due to its features such as trustworthy data and transparent processes. However, urban planners are usually not technological experts, and when faced with a wide variety of blockchain platforms with different technological characteristics, they often lack sufficient information and professional judgment to make a suitable technological choice. This gap between technology perception and practical application greatly limits the promotion and implementation of blockchain in urban governance. To address this problem, this study proposes a set of blockchain selection tools for urban planners. The core concept of the tool is not to start from abstract technical parameters, but to provide planners with references for blockchain applications that can be learned from and landed by analysing existing successful cases and combining the current business scenarios and development goals of cities. Through the case-driven approach, it reduces the technical threshold of planners and improves the science and operability of selection. This section focuses on the introduction of the tool, firstly clarifying the core needs of urban planners in technology selection, then designing a set of system framework based on case recommendation, and explaining its implementation mechanism and key algorithms, and finally verifying the effectiveness and practical value of the system through specific application scenarios.

4.1 Requirements Analysis

According to the results of the SLR, there are numerous aspects of smart cities, such as smart healthcare, smart education, EV charging, smart estate, E-Voting, and energy trade networks. In fact, there are broader applications for blockchain in smart cities, as blockchain technology needs to be widely used in scenarios such as cross-departmental collaboration (e.g., traffic data sharing) and public service optimization (e.g., digital identity authentication), as the demand for trusted data interactions in smart cities is currently growing. However, urban planners also face multiple challenges in technology selection: the complexity of the blockchain technology stack (e.g., the trade-off between public and federated chains), the lack of localized cases to refer to, and the difficulty in quantifying the benefits of the technology. To find a solution to this issue, this project proposes to develop a decision support tool based on case matching, which assists planners in quickly locating suitable technology solutions through a structured case base and an intelligent recommendation mechanism. Therefore, the core users of this tool are decision-makers in urban planning departments, whose roles usually cover the development of urban digital strategies, the coordination of cross-sectoral resources, and the final review of technical solutions.

Most of the decision-makers in this user group have policy and management backgrounds. However, their understanding of blockchain technology remains at the conceptual level (e.g., ‘tamper-proof,’ ‘decentralized’), and they lack in-depth knowledge of technical details, such as the differences in consensus algorithms and the cost of developing smart contracts. When selecting technology, they are more concerned about compliance, whether it can bring significant social benefits, and the feasibility of cross-departmental collaboration, for example, whether it can open up the data barriers of the transport and environmental protection departments, rather than pure technological advancement. As a consequence, the system must meet the following requirements to be a useful decision-making tool for urban planners: simplify blockchain technology selection, reduce technical complexity and provide clear recommendations for non-technical users; provide localized case support, improve decision-making reliability based on successful cases in similar cities; help assess the social impact of the technology, to enable users to understand the potential impact of blockchain solutions on public services; support cross-sectoral collaborative assessments, facilitate data sharing.

In order to help urban planners systematically evaluate the advantages and applicability scenarios of different platforms when facing diverse blockchain technology selections, we summarize and collate the key elements affecting blockchain selection in this section. Table 5 details the classification of these elements and their specific indicators of concern, covering multiple dimensions including security, performance, costs, ecosystem, regulatory, sustainability, customization, and confidentiality to provide an intuitive and structured reference for practical decision-making.

Table 6. Key Factors for Blockchain Selection in Smart Cities

Category	**Factor**	**Description**	**Example Considerations**
Security	Consensus Mechanism	Determines how transactions are validated and secured.	PoW (secure but energy-intensive), PoS (efficient but centralization risk)
	Security Audits	Regular audits help identify and fix vulnerabilities.	Third-party audits, penetration testing
	Developer Community	A strong community ensures quick bug fixes and improvements.	Active GitHub repositories, large contributors' base
Performance	Transaction Speed (TPS)	Higher TPS ensures better performance and user experience.	Bitcoin (7 TPS) vs. Solana (65,000 TPS)

Continued on next page...

Table 6 (Continued)

Category	**Factor**	**Description**	**Example Considerations**
	Scaling Solutions	Methods to improve performance and reduce congestion.	Layer 2 (Optimistic Rollups, ZK-Rollups), Sharding
	Finality	Time required for transactions to become irreversible.	Bitcoin (10 min), Solana (400 ms)
Costs	Gas Fees	Costs associated with executing transactions.	Ethereum (high fees) vs. Flow (low fees)
	Costs	Some blockchains have predictable or dynamic fees.	Fixed vs. fluctuating fees based on demand
Ecosystem	Developer Tools	Availability of SDKs, APIs, and documentation.	Ethereum (Web3.js), Polkadot (Substrate)
	DApp Ecosystem	A rich ecosystem supports interoperability and innovation.	DeFi, NFTs, DAOs
	Interoperability	Ability to interact with other chains.	Polkadot, Cosmos (IBC protocol)
Regulatory	Jurisdictional Restrictions	Some regions have strict blockchain regulations.	GDPR (EU), SEC (USA)
	KYC & AML Requirements	Mandatory identity verification for financial security.	Required in regulated DeFi platforms
Sustainability	Power Consumption	Energy-efficient blockchains are more sustainable.	Bitcoin (high energy) vs. Algorand (low energy)
Customization	Governance & Upgradability	Ability to modify and upgrade blockchain features.	Ethereum (smart contracts), TON (custom modules)
Confidentiality	Privacy Technologies	Protects sensitive data on the blockchain.	Zero-Knowledge Proofs, Homomorphic Encryption

4.2 System Design

Building upon the requirements analysis presented in Section 5.1, this section introduces the overall design of the proposed decision-support system. The primary objective of this system is to assist urban planners in efficiently and systematically selecting appropriate blockchain technologies based on specific application scenarios and technical requirements. To achieve this, the system adopts a modular and structured design approach, consisting of four core components: user input interface, back-end processing logic, case database, and recommendation engine. First, the system requires users to provide essential information to precisely identify their technological needs. These inputs primarily include the intended application domain (such as intelligent transportation, energy management, government services, public safety, etc.), key technology requirements (e.g., privacy protection, decentralization, high throughput, low latency), preferred governance models (e.g., public blockchain, consortium blockchain, private blockchain), and integration preferences with existing infrastructures. In the back-end processing stage, after receiving the front-end request, the system calls the matching algorithm, query the case database, screen the most matching blockchain application cases based on the input requirements, and ultimately return the recommended results to the user.

The core matching mechanism relies on the case database, which collects and organizes real application cases of blockchain in smart cities and stores them in a structured way. The case database is a structured collection of real-world blockchain application cases in smart cities. Each case is annotated with detailed metadata, including application scenarios, technical features, governance models, performance indicators, and implementation outcomes. This structured information enables the system to conduct efficient and reliable case matching. At the same time, the matching mechanism is proposed as a Multi-Dimensional Semantic Weighted Matching Mechanism to recommend blockchain solutions for smart city applications, the overall algorithm embodies the combination of natural language processing and multidimensional weight modeling. The system takes the information submitted by the user and semantically vectorizes the unstructured textual information through a semantic coding model while parsing the technical indicators and other structured fields in a standardized way. Subsequently, the system compares the blockchain cases in the database. It generates an overall matching score by calculating the similarity scores on each dimension and combining them with a set of adjustable weighting strategies.

After sorting the match scores, the system selects several cases with the highest similarity as the recommendation results, which are merged and returned to the user with the reasons for recommending the case. In addition, the system also recommends the type of blockchain, blockchain platform, and consensus algorithm, along with other variables, based on the user's input. It will automatically generate a report for the user to download as a PDF file. Through this matching mechanism, the system can provide urban planners with scientific and feasible references for blockchain technology selection, thus contributing to the efficient construction of smart cities.

This use case diagram (Figure 3) shows the interaction between two main types of participants in the system - User and Administrator. The core use cases that Users can execute include submitting technical requirements, adjusting weighting strategies, viewing recommended solutions, and receiving system-generated PDF files. The Administrator is mainly responsible for the maintenance and quality monitoring of the system database. Its core use cases include maintaining the case database, updating the semantic model, and monitoring the matching quality. Through these use cases, the system realises the complete process from user input to system recommendation and background quality control.

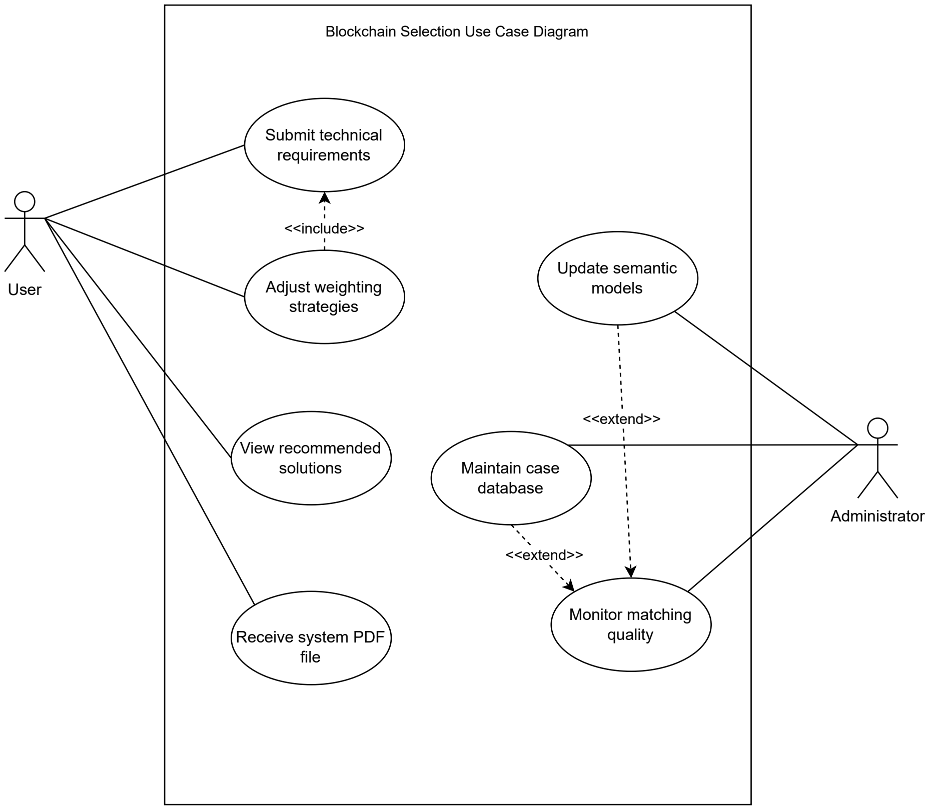


Figure 3. System Use Case Diagram

4.3 Implementation

Figure 4 demonstrates the architecture of the system. The front-end of the system is designed to provide urban planners and decision makers with an intuitive and easy-to-use interactive interface, which is designed to facilitate the input of key parameters about the smart city blockchain application (as Figure 9 shows). As the first interaction portal of the system, the core task is to guide users to fill in the standardized demand information so that the subsequent matching and recommendation process based on the cases can be carried out smoothly. The front end of this system is developed using the React.js framework, and the overall interface style is modern and straightforward, emphasizing usability and responsiveness. The core page is designed around the three main processes of the user inputting demand parameters, adjusting weight configuration, and viewing matching results, providing users with a completely interactive experience.

Regarding functional implementation, the front end supports users in inputting or selecting demand information for city blockchain applications from multiple dimensions, including application scenarios, TPS, latency, security level, technology stack, city size, and budget range. Meanwhile, through the introduction of WeightSliders, users can independently adjust the weight ratio of each matching dimension according to their specific preferences, thus enhancing the personalized degree of the matching mechanism. Regarding application scenario input, the system introduces a hybrid interaction mode of label-based selection and free input. Predefined typical scenario labels such as 'energy grid,' "logistics," and 'real estate' can be added quickly by clicking on them, and users can also add customized descriptions in the text field, which enhances the input flexibility and semantic expressiveness. The user can also add customized descriptions in the text field, enhancing input flexibility.

In terms of displaying matching results, the system uses dynamic components to present details of the recommended cases, covering the reasons for the recommendation, core parameters, and technical features. At the same time, MatchRadar is embedded to graphically display the matching scores of each recommended case in each dimension so that users can intuitively understand the composition and advantages and disadvantages of the matching results. Finally, the system automatically downloads the analysis report in PDF format after the matching is completed, which is convenient for archiving the results and subsequent reporting. Overall, the front-end implementation focuses on user experience in the interaction design and strengthens the interpretability and visualization of the results in order to support the overall goal of the urban blockchain application recommendation system.

The system's back end is built based on the FastAPI framework, which provides a high-performance RESTful API interface for receiving and parsing user input data, executing matching logic, and generating and outputting recommendation results. The design concept of the back-end module emphasizes scalability and interpretability, and its core task is to comprehensively evaluate the similarity between user demand information

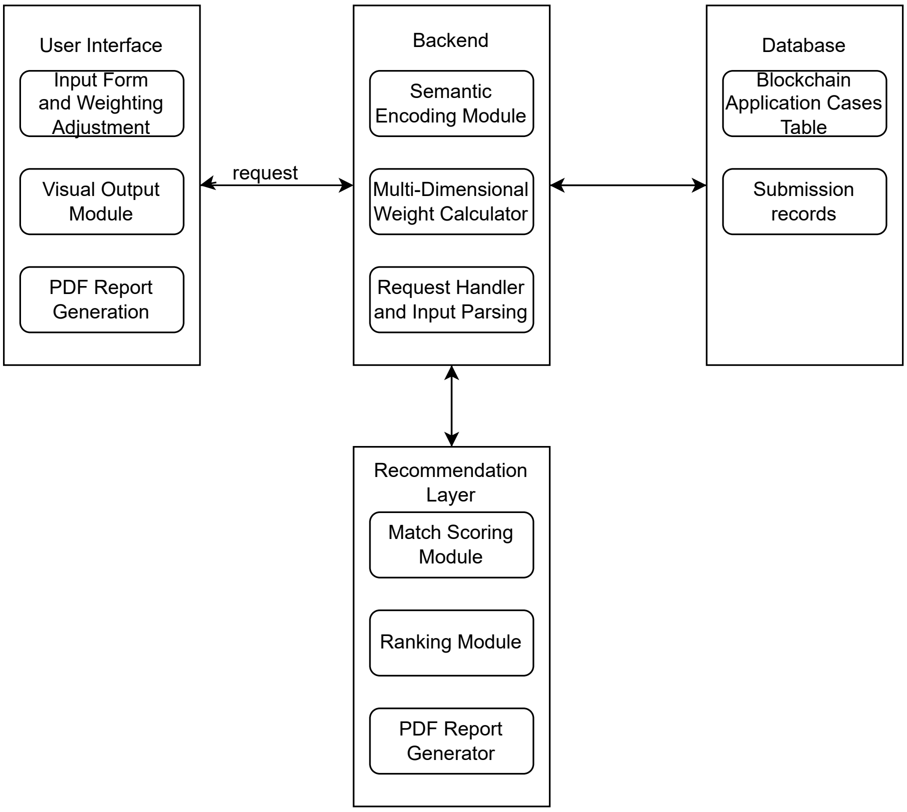


Figure 4. The System Architecture

and historically successful cases. Hence, the system builds a set of multi-dimensional comprehensive matching mechanisms, integrating natural language processing, structured feature matching, and a weighted scoring strategy to generate matching recommendation results. The whole matching process mainly includes the following dimensions:

- Application Scenario Matching: For the application scenario, the system uses the SentenceTransformer model for semantic similarity calculation (Listing 1). Based on the semantic encoding method of the pre-trained language model Sentence-BERT (all-MiniLM-L6-v2), the user input and the case description are vectorized, and the semantic proximity between the two is calculated using Cosine Similarity to achieve in-depth comprehension of the scene semantics and comparison. The keyword extraction and fuzzy similarity comparison mechanisms filter the input and case scenes to ensure that the recommendations are only made within the scope of the relevant scenes, which fundamentally improves the contextual relevance of the recommendations.

```
def _text_match(self, text1: str, text2: str) -> float:
    """text similarity"""
    try:
        embeddings = self.model.encode([text1, text2])
        sim = cosine_similarity([embeddings[0]], [embeddings
    [1]])[0][0]
        return float(sim)
    except Exception as e:
        print(f"Text match error: {str(e)}")
        return 0.0
```

Listing 1. Text similarity calculation using cosine similarity

- Technical Requirements Matching: The system employs a Gaussian similarity function to evaluate numerical technical requirements such as TPS and latency (Listing 2). This function assigns higher scores to values that are numerically closer, with the score decreasing exponentially as the difference increases. This ensures sensitivity to performance proximity between user input and case data. For security level matching, a fuzzy logic approach is used. Security levels ("low", "medium", "high") are mapped to numerical values (0, 1, 2), and similarity is calculated based on their difference. A perfect match scores 1.0, a one-level difference scores 0.5, and a two-level difference scores 0. This balances strict matching with a degree of flexibility.

```
def _tech_requirement_match(self, user: dict, case: dict) ->
    float:
    tps_score = self.gaussian_similarity(user['tps'], case['tps'
    ], sigma=500)
    latency_score = self.gaussian_similarity(user['latency'],
    case['latency'], sigma=100)

    sec_levels = {'low': 0, 'medium': 1, 'high': 2}
    sec_diff = abs(sec_levels[user['security_level']] -
    sec_levels[case['security_level']])
    sec_score = 1 - sec_diff / 2

    return 0.4 * tps_score + 0.3 * latency_score + 0.3 *
    sec_score
```

Listing 2. Gaussian similarity and security level scoring

- Technology Stack Overlap: The technology stack fields are treated as unordered sets and compared using Jaccard similarity (Listing 3), which computes the ratio of the intersection to the union of the user and case technology sets, thereby quantifying their overlap.

```python
def _tech_stack_match(self, user_stack: list, case_stack: list)
    -> float:
    set_user = set(user_stack)
    set_case = set(case_stack)
    intersection = set_user & set_case
    union = set_user | set_case
    return len(intersection) / len(union) if union else 0
```

Listing 3. Jaccard similarity

- City Size & Budget Matching: City size is achieved by exact matching of categories, and budget intervals are combined with upper and lower bound distance calculations to ensure that the recommendations are realistic and feasible. The city size field is used as a discrete categorical variable with an exact matching strategy, giving full scores if the city sizes are the same and punitively low scores (0.3) if they are not, in order to simplify the modeling complexity and to ensure basic consistency in the geographic dimensions.

The back-end matching mechanism can be formalized as a multi-dimensional feature-based weighted scoring function. Let the user demand be represented as an input feature vector $\mathbf{U}$, and the historical case base be denoted as $\mathcal{C} = \{\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_n\}$. The matching goal is to identify the case(s) $\mathbf{C}_i$ that are most similar to $\mathbf{U}$ in terms of multi-dimensional criteria.

The overall matching score S_i between the user demand $\mathbf{U}$ and a candidate case $\mathbf{C}_i$ is computed as:

$$S_i = \sum_{k=1}^{m} w_k \cdot \mathrm{sim}_k(U_k, C_{ik})$$

where:

- m is the number of matching dimensions (e.g., application scenario, technical requirements, technology stack, city size, and budget);
- w_k is the weight assigned to the k-th dimension, with the constraint $\sum_{k=1}^{m} w_k = 1$;
- sim_k is the similarity function defined for the k-th dimension;
- U_k and C_{ik} denote the feature values of the user input and the i-th case in the k-th dimension, respectively.

The system ultimately weighs and sums up the matching scores of the above five dimensions. The weights can be set by the system's default or user-defined settings to meet the needs of recommendation strategies in different usage scenarios. Cases with higher scores will be considered more compatible with the user's needs and prioritized for a recommendation. The scores of the above dimensions are weighted and fused according to the user-defined weights to form the final matching score. In addition, the system also generates a match explanation item for each recommendation result, pointing out which dimensions of performance the match is excellent or high to enhance the recommendation's interpretability. After the recommendation is completed, the back-end support automatically downloads the results of the analysis report in PDF format to meet the subsequent archiving, project discussion, or preparation of materials.

In addition to the case-based matching mechanism, the system also builds a set of independent rule-based auto-recommendation modules to directly generate feasible blockchain technology architecture recommendations in the absence of reference cases or when users want to obtain customized solutions quickly. The module integrates domain knowledge, and through a series of conditional judgments and logic rules, it automatically maps from user inputs to complete blockchain solution configurations, which can assist users in forming preliminary architectural blueprints in the early design stage. Specifically, the module generates customized recommendations based on user-input requirements in the following dimensions:

- **Blockchain Type Determination:** Analysing data makes intelligent inference sensitive, collaboration scope, and deployment conditions. If the scenario involves multi-party collaboration or high-security level requirements, *Consortium Chain* is recommended if the budget is sufficient and the deployment environment is a large city, a *Public Chain* is recommended; in the rest of the cases, a *Private Chain* is preferred to reduce the cost and complexity.

- **Platform Selection Strategy:** The recommended platforms are further refined based on the selected chain type. For example, *Hyperledger Fabric* is preferred in high-security federation chain scenarios, while *Quorum* is recommended in cases where compliance requirements are not too high; if the demand is for a high TPS or low-latency public chain application, then *Solana* or *Polygon* , otherwise use *Ethereum* and other mainstream platforms; for private chain scenarios, choose *Hyperledger Besu* or a custom private chain solution depending on whether or not the technology stack includes Java.

- **Consensus Mechanism Matching:** is auto-configured by combining platform characteristics and security levels, such as *PBFT* for Fabric, *RAFT* and *IBFT2* for Quorum, and *PoS* for Solana, Polygon, and Ethereum as the default choice.

- **Data Storage Model Recommendation:** combines business throughput and data types to make fitness recommendations. For big data or high concurrency applications, it is recommended to use *IPFS and other off-chain storage* or *hybrid* *storage* solutions; if the business involves auditing, document retention, or compliance needs, it is preferred to *on-chain storage* combined with the Merkle tree mechanism for data integrity assurance.

- **Network Topology Design:** Recommended configuration of node size and deployment method based on chain type. For example, alliance chains recommend 4-10 nodes for cross-organizational deployment and are equipped with endorsement strategies; public chains can participate in verifying node sets or introduce Layer 2 technology to improve performance; and private chains are recommended to use 1-3 trusted nodes to build a simplified network.

- **Security Enhancement Strategy:**Additional suggestions are given based on user scenarios and security requirements, including enabling *identity management mechanism (e.g., CA/MSP)*, *introducing confidential transaction or zero-knowledge module*, *audit log*, and *multi-signature mechanism*, etc., to strengthen the system reliability and Traceability.

This Docker Compose configuration (Listing 4) builds a blockchain application development environment that includes a front-end, back-end, and database. The front-end is built locally and exposes port 3000, relying on the back-end service to provide the data interface; the back-end is also built locally, connects to the PostgreSQL database and configures the database connectivity information through environment variables, and maps port 8000 for external access; and the database service is initialised with the official PostgreSQL 13 image, loads local SQL scripts, and exposes standard port 5432. The database service is initialised using the official PostgreSQL 13 image, which loads local SQL scripts and exposes standard port 5432. The overall structure is clear and easy to develop and test.

```yaml
version: "3.8"
services:
  frontend:
    build: ./frontend
    ports:
      - "3000:3000"
    depends_on:
      - backend
  backend:
    build: ./backend
    ports:
      - "8000:8000"
    depends_on:
      - db
    environment:
      - DATABASE_URL=postgresql://postgres:postgres@db:5432/
   blockchain
```

```
    volumes:
      - ./backend:/app
  db:
    image: postgres:13
    restart: always
    environment:
      POSTGRES_USER: postgres
      POSTGRES_PASSWORD: postgres
      POSTGRES_DB: blockchain
    ports:
      - "5432:5432"
    volumes:
      - ./database/init.sql:/docker-entrypoint-initdb.d/init.sql
```

Listing 4. Docker Compose File

In order to ensure the efficient operation of the system and data manageability, the back-end module is built on top of a relational database, adopting a structured table design and field specification, which is used to store the recommended demand information submitted by users and the typical blockchain cases predefined in the system, respectively. The database is managed by the PostgreSQL system, which has good scalability, transaction support, and JSON field compatibility, and can meet the coexistence of multi-source data structure and query performance requirements. The system is designed with two main tables:

```sql
CREATE TABLE IF NOT EXISTS case_submissions (
    id SERIAL PRIMARY KEY,
    application_scenarios TEXT,
    technical_requirements TEXT,
    technology_stack TEXT,
    city_size VARCHAR(100),
    budget_range VARCHAR(100),
    created_at TIMESTAMP DEFAULT CURRENT_TIMESTAMP
);
```

Listing 5. User Submission Table

```sql
CREATE TABLE IF NOT EXISTS blockchain_cases (
    id SERIAL PRIMARY KEY,
    case_name TEXT NOT NULL,
    application_scenarios TEXT NOT NULL,
    technical_requirements JSON NOT NULL,
    technology_stack JSON NOT NULL,
    city_size TEXT CHECK(city_size IN ('small', 'medium', 'large')),
    budget_range JSON NOT NULL
);
```

Listing 6. Blockchain Cases Table

4.4 Summary

This chapter presents a comprehensive blockchain selection toolkit tailored to the needs of urban planners in the context of smart city development. It identifies non-technical decision-makers' challenges when choosing appropriate blockchain technologies and proposes a case-driven decision support system to bridge the knowledge gap. The toolkit simplifies the selection process by integrating a structured case database, a semantic-weighted matching algorithm, and an intuitive user interface, enabling users to match their unique requirements with real-world blockchain applications. This chapter demonstrates how the toolkit can facilitate informed, context-aware, and socially beneficial technology adoption in urban governance through detailed system architecture, algorithm design, and implementation.

5 Evaluation

The development of smart cities involves a complex decision-making process that requires careful evaluation of various technologies, resources, and frameworks. To demonstrate the effectiveness of this tool, this section explores three different smart city use cases: energy grid, supply chain management, and healthcare. We outline the key requirements for each scenario and apply the tool to evaluate suitable solutions and select appropriate technologies.

5.1 Blockchain Selection for a Small-Scale Energy Grid

This case simulates the scenario of a small city planning to introduce blockchain technology to optimize the management of its energy system. The decision maker wants to achieve system performance with high transaction throughput (1000 TPS) and low latency (200ms) with high security standards. At the same time, the decision makers preferred an Ethereum-based technology architecture and kept the project budget between $500,000 and $1 million. Choosing the right blockchain solution became especially critical due to the small size of the city and the limited resources and technical support associated with it. Users assign equal weights to each matching dimension (application scenario, technology requirements, technology stack, city size, budget) in the tool to reflect neutral and comprehensive considerations. In blockchain applications for energy infrastructure, small cities often face several challenges: limited resources, relatively insufficient budgets and staffing, and security-sensitive, as energy systems are critical infrastructures with extremely high security requirements. The core motivation of this case is to find a blockchain solution that meets the performance and security requirements and is feasible under the budget and resource constraints. CityChain Advisor tool helps city managers to quickly filter the suitable blockchain system, reduce the cost of trial and error, and improve the efficiency of the selection process by matching the technical parameters with the application requirements in a structured and visual way.

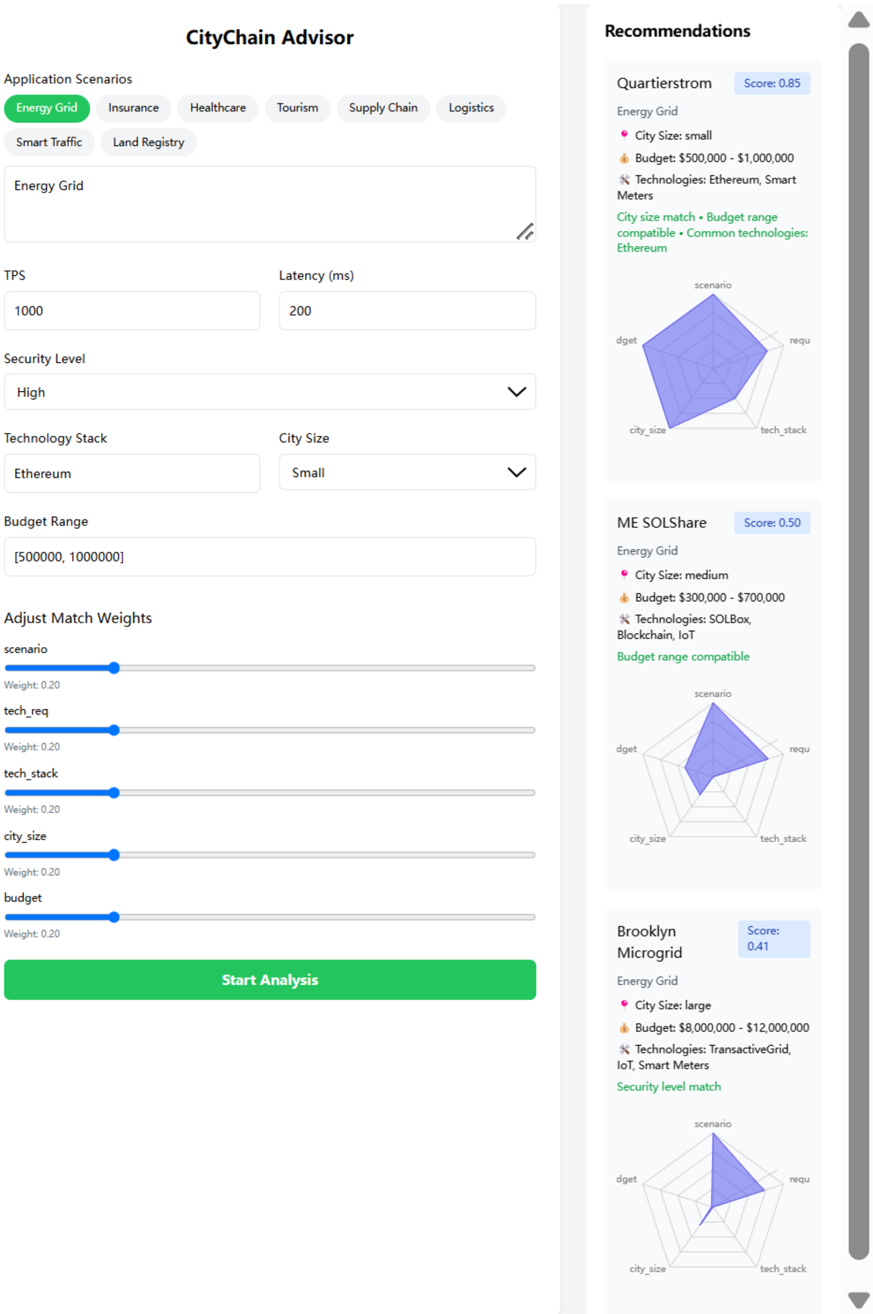
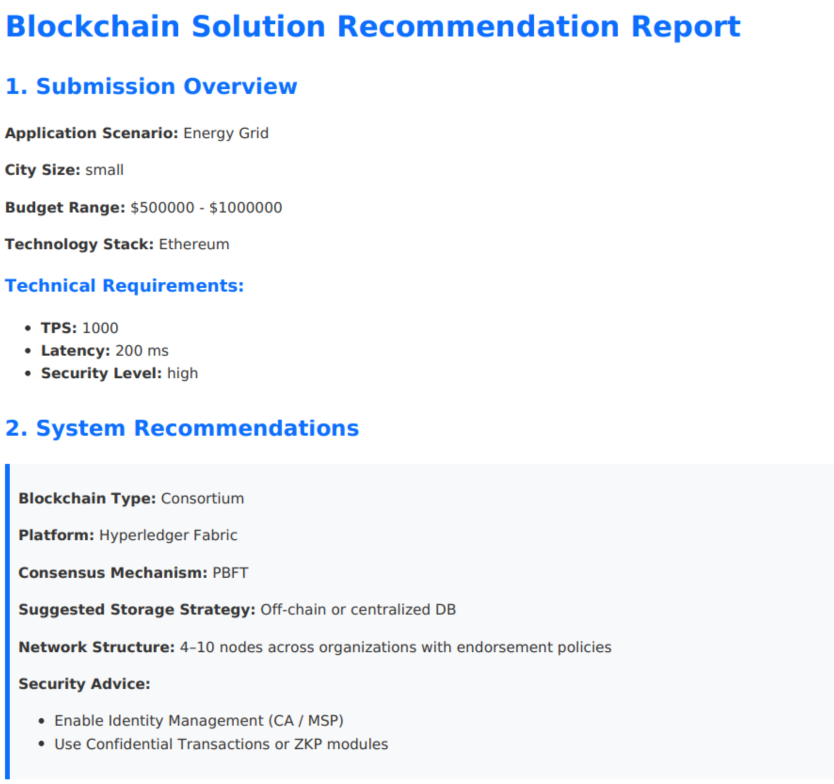


Figure 5. Energy Grid Case Evaluation

In the first case, the top recommended solution, Quartierstrom, achieved a high matching score of 0.85, reflecting strong alignment across city size, budget, and selected technology stack (Ethereum). The second and third ranked options (ME SOLShare and

Brooklyn Microgrid) scored significantly lower (0.50 and 0.41), primarily due to city size or security level mismatches. This outcome suggests that the tool places appropriate emphasis on critical parameters such as city scale and stack compatibility, and can effectively filter out irrelevant or loosely matched options. The radar charts on the right offer additional interpretability by visually highlighting where mismatches occur, which helps users understand the reasoning behind rankings (see Figure 5).



Blockchain Solution Recommendation Report

1. Submission Overview

Application Scenario: Energy Grid

City Size: small

Budget Range: $500000 - $1000000

Technology Stack: Ethereum

Technical Requirements:

- **TPS:** 1000
- **Latency:** 200 ms
- **Security Level:** high

2. System Recommendations

Blockchain Type: Consortium

Platform: Hyperledger Fabric

Consensus Mechanism: PBFT

Suggested Storage Strategy: Off-chain or centralized DB

Network Structure: 4–10 nodes across organizations with endorsement policies

Security Advice:

- Enable Identity Management (CA / MSP)
- Use Confidential Transactions or ZKP modules

Figure 6. System recommendations

5.2 Blockchain Selection for Large-Scale Supply Chain Systems

This case simulates the scenario of a large city seeking to implement blockchain technology in the supply chain area. The decision maker aims to achieve high system performance with a transaction throughput of 1000 TPS and low latency, while maintaining high security standards. The preferred technology stack includes IoT devices with a project budget of $ 1 million to $ 6 million. Given the large size of the city, the project requires scalable solutions capable of handling complex infrastructure needs. Challenges in blockchain applications for large-scale urban infrastructure include managing high transaction volumes, ensuring interoperability across diverse systems, and maintaining robust security protocols. The core motivation of this case is to identify blockchain solutions that meet stringent performance and security criteria while aligning with the city's substantial budget and technical capabilities.

The top recommended solution, BMW VerifyCar, achieved a high matching score of 0.78, reflecting excellent alignment across the city's large-scale infrastructure, budget constraints, and preferred technology stack (VeChainThor with IoT devices). This highlights the tool's ability to identify solutions that meet critical requirements. The alternative options, Port of Los Angeles Blockchain Cargo Tracking and Port of Valencia Smart Port Project, scored lower due to significant budget mismatches and over-specialization in logistics, despite their strong security and scalability (see Figure 7).

5.3 Blockchain Selection for Secure Healthcare Systems

This case tests the tool's recommendation accuracy and professional adaptation in the healthcare domain. The parameters entered by the user are: the application scenario is Healthcare, the performance requirement is 500 TPS and 200 ms latency, the security level is high, the chosen technology stack is Hyperledger Fabric, the city size is medium, and the budget range is $1M to $4M. Blockchain deployments in healthcare scenarios require high stability, privacy protection, and compliance with the technology platform. Core challenges compared to general scenarios include high data sensitivity. Due to the highly private nature of medical data, recommender systems need to prioritise projects with rights management, data encryption, and federation chain features. In addition, the healthcare sector differs from general business systems, requiring blockchain projects to be more auditable, traceable, and transparent in their operations. Therefore, the recommended system's results will also help test its intelligence and reliability in dealing with scenarios with high specialisation and explicit constraints.

As a result of this evaluation, the system recommended three blockchain projects: Guardtime, Singapore Medical Records, and MedRec. Regarding the match score, Guardtime, the highest, reached 0.70, with the main advantages being the high fit between city size, budget scope, and security level. However, its technology stack does not match the Hyperledger Fabric that the user sets. In contrast, Singapore Medical Records matches the user's needs in terms of technology stack, but has a slightly lower match (0.68) due to its upper budget range being slightly higher than the value set by the user. This result suggests a trade-off between technology matching and budget feasibility for different projects in the healthcare scenario, and the recommender system can synthesise multiple dimensions to achieve a more reasonable ranking and improve the decision-making efficiency of urban planners (see Figure 8).

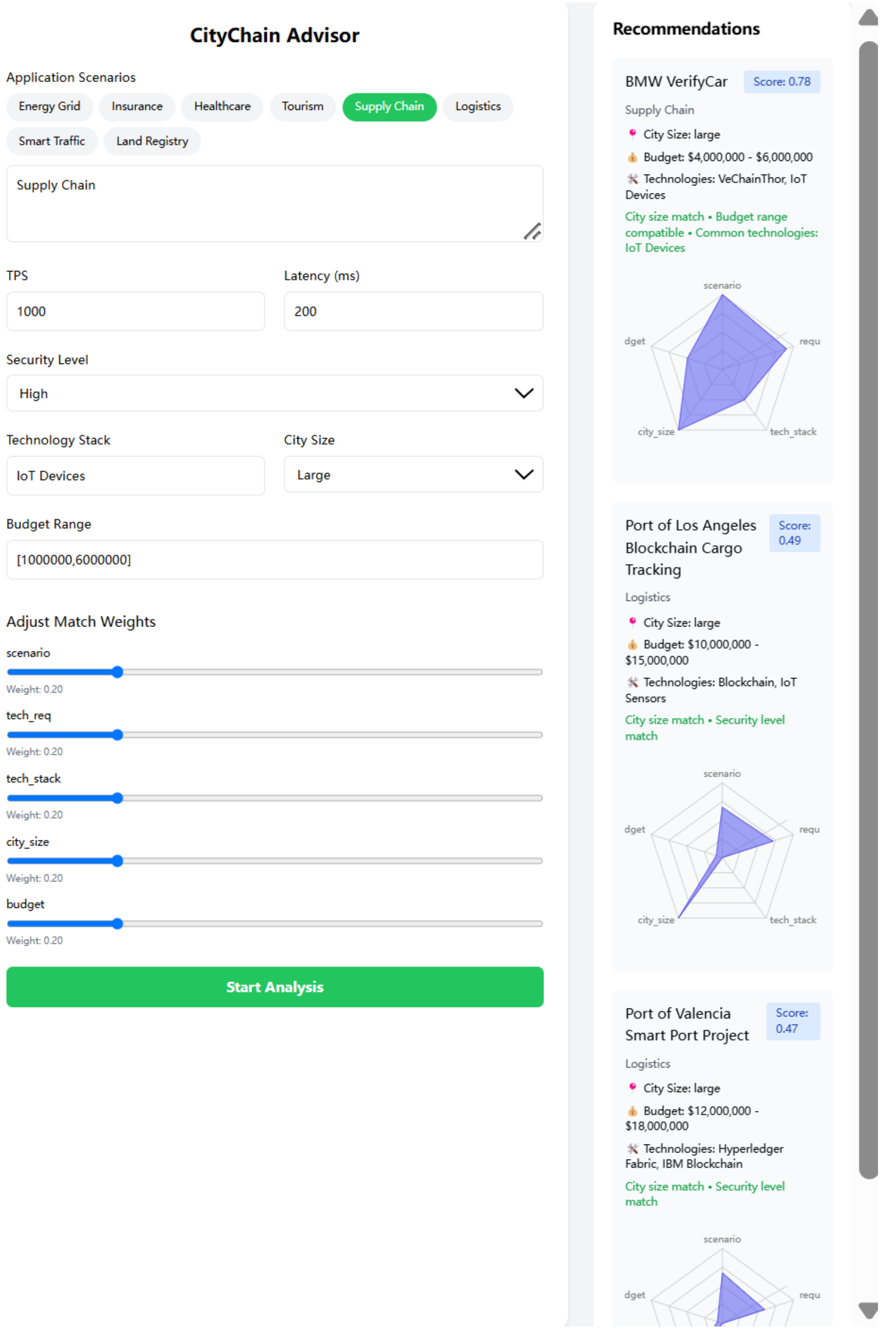


Figure 7. Supply Chain Case Evaluation

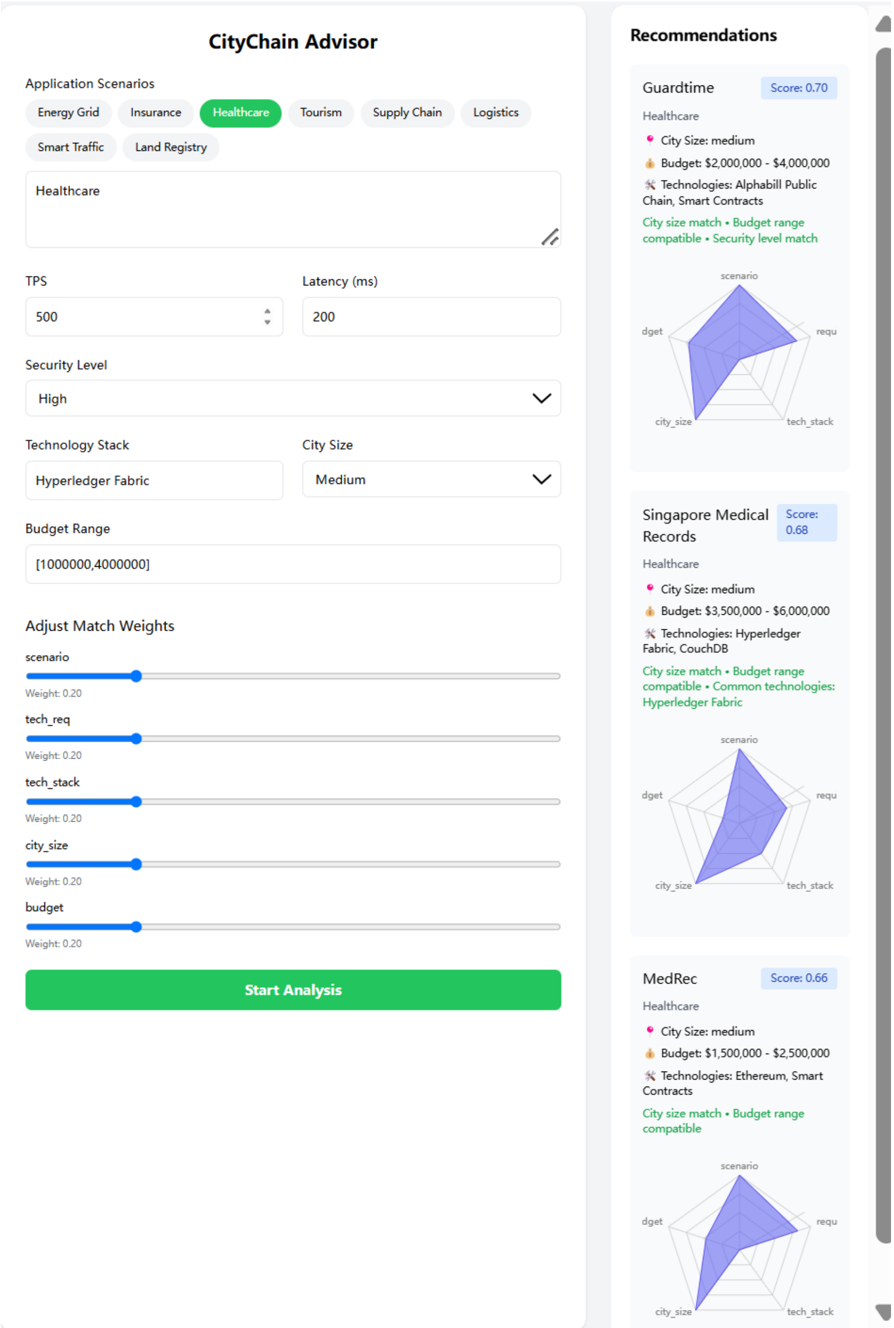


Figure 8. Healthcare Case Evaluation

5.4 Summary

This chapter evaluates the real-world performance of the CityChain Advisor toolkit through three representative case studies: a small energy infrastructure, a large supply chain system, and a secure healthcare network. Each case demonstrates the tool's ability to integrate blockchain solutions with specific technical, financial, and environmental needs. The evaluation showed that the system provides reliable and interpretable recommendations, with radar chart visualisations to help understand trade-offs. The results confirm that CityChain Advisor can be a valuable decision support tool for city planners and technology managers by streamlining the blockchain selection process and improving decision-making accuracy in smart city development.

6 Discussion

In this section, we review the study's main findings, starting by answering the initial research questions. We then critically review the limitations of the developed blockchain choice recommendation tool and suggest directions for future work. Through this discussion, we aim to provide a comprehensive understanding of the contributions, shortcomings, and potential for further development of the current system.

6.1 Practical Significance

This study is significant at the practical application level, especially for urban policy makers, planners, and stakeholders who wish to apply blockchain technology in smart city projects but lack the technical background. In addition, by providing a systematic overview of current blockchain applications in smart cities, this study reveals blockchain technology's application patterns and development trends in actual urban environments. The blockchain selection tool developed in this study provides a non-technical, instance-based decision support system for non-technical people, enabling city managers to make informed choices based on specific needs. In addition, this study provides a firm reference for practical decision-making by comparing blockchains and their applicability and trade-offs in areas such as energy management, data sharing, identity verification, and urban governance. As more and more cities push for digital transformation, this study provides timely insights. It builds practical tools to help achieve better synergy and realization between blockchain technology and urban development goals, and promote the transformation of theoretical innovation into real-world applications.

6.2 Answers to Research Questions

The work aimed to address the main research question "What is the current role of blockchain technology in enhancing smart city ecosystems?" by investigating four specific sub-research questions. In this section, we discuss the outcomes and results of the work in the context of these research questions. The mapping of research questions to their corresponding study sections is summarized in Table 7.

Table 7. Research Questions and Corresponding Sections

RQs	Description	Section addressing RQ
RQ1	What are the existing blockchain-based applications in smart city domains?	Section 3.6
RQ2	How are different blockchain solutions being compared in smart city infrastructure?	Section 3.7
RQ3	How can we build a tool to optimize the selection of blockchain technology for smart cities?	Section 4
RQ4	What are the challenges and future directions associated with integrating blockchain into smart city systems?	Section 3.8

This study systematically explored the role of blockchain in smart cities through four key research questions. For RQ1, it identified existing applications across areas such as education, governance, and healthcare, revealing both usage trends and gaps in adoption. In response to RQ2, the study compared public, private, and consortium blockchain models, outlining their respective trade-offs in scalability, security, and energy consumption, and offering a practical framework for decision-making. To address RQ3, a user-friendly blockchain selection toolkit was developed, specifically designed for city planners without technical backgrounds, to support more accessible and context-appropriate adoption. Finally, RQ4 highlighted critical challenges, including security risks, latency, and energy inefficiency, that should be addressed to enable broader implementation. Together, these contributions provide both theoretical insights and practical guidance for integrating blockchain into smart city development.

6.3 Limitations

Although the blockchain selection recommendation tool developed in this study has some reference value in smart city planning, it still has the following limitations:

First, there are limitations in the coverage of the case database. The cases included in the current system are mainly derived from open literature and white papers of mainstream blockchain platforms, resulting in the database presenting limitations in two dimensions: one is the order of magnitude limitation, which currently only covers common application scenarios in the field of smart cities (e.g., energy transactions, digital identity management, etc.), and lacks representativeness for emerging scenarios or composite demand scenarios; the second is the geographic bias, where the majority of the existing cases are focused on large-scale implementation experiences in developed cities, with insufficient analysis of the adaptability of infrastructure conditions and policy environments specific to cities in developing countries. Second, the core recommendation algorithm uses an experience-based weighted similarity matching model, which, although it has advantages in terms of interpretability, has functional limitations compared to machine-learning-based recommendation systems. The current weight assignment scheme relies on the subjective judgment of domain experts, making it challenging to capture non-linear associations between multi-dimensional features. For example, complex associations between technical indicators (e.g., the balance between high throughput and low latency) are simplified, and linear weighting algorithms find it challenging to model such complex interactions accurately. Finally, the current system focuses on explicit parameters such as technical indicators and economic costs. However, the quantitative assessment of soft factors such as policy compliance risks, e.g., data localization requirements in different jurisdictions, has not yet been incorporated into the recommendation model, which may affect the actual implementation of the program.

6.4 Future Work

Given the limitations of the existing system in terms of the coverage of the case database, future work should be devoted to expanding the diversity and representativeness of the case sources. On the one hand, non-public cases from actual project implementation can be supplemented through cooperation with industry organizations to cover more emerging application scenarios, such as urban carbon emission management and smart healthcare. On the other hand, research on blockchain applications in cities in developing countries can be strengthened to analyze the particularities of the infrastructure conditions and policy environment in the place to enhance the system's adaptability in different geographical cities.

In addition, the existing recommendation algorithms are mainly based on the similarity matching model with empirical weights, which is insufficient in mining the complex associations among features. However, it has a certain degree of interpretability. In the future, machine learning algorithms, especially deep learning and graph neural network technology, can be introduced to improve the modeling ability of non-linear relationships between multi-dimensional features. Finally, the existing system does not fully consider the impact of practical conditions on the scheme's feasibility, especially regarding policy compliance, such as data localization and privacy protection. A set of indicator systems for quantifying policy risk can be constructed in the future, with compliance requirements as one of the model input parameters. Introducing these social variables will help improve the system's feasibility in deployment.

7 Conclusion

This thesis proposes and implements a set of Blockchain Selection Toolkit for the growing demand for blockchain technology selection in smart cities to assist relevant stakeholders in making scientific and reasonable technology selection decisions in diverse urban application scenarios. Through an in-depth analysis of the key features of blockchain technology and smart cities, and combined with a Systematic Literature Review, this study identifies the key factors affecting the integration of blockchain in smart cities, covering the comparison of the applicability of public, private, and federated chains as well as the challenges faced.

The toolkit was developed through three main phases: requirements analysis, system design and implementation, and evaluation through three typical scenarios: a small-scale energy network, a large-scale supply chain system, and a secure healthcare system. The evaluation results show that the toolkit has good adaptability and practical value, and can effectively support users in screening and matching blockchain technologies under different requirements and resource constraints. Theoretically, this study elucidates the fit between different types of blockchain technologies and smart cities; on the practical side, it constructs a set of reusable decision-support frameworks that guide policymakers.

Despite the results achieved in this study, there are still some limitations. For example, the scope of the case validation is relatively limited, and the applicability of the toolkit needs to be further tested in a wider, dynamic technological environment. Future research could focus on deployment practices in real projects, cross-chain interoperability, and other emerging blockchain technology trends.

In conclusion, this thesis provides the theoretical foundation and tool support to promote the orderly and efficient application and selection of blockchain technology in smart cities, which is a key step towards realizing more innovative, safer, and more sustainable urban development.

References

[1] Anak Agung Gde Agung and Rini Handayani. Blockchain for smart grid. *Journal of King Saud University-Computer and Information Sciences*, 34(3):666–675, 2022.

[2] David Allessie, Maciej Sobolewski, Lorenzino Vaccari, and Francesco Pignatelli. Blockchain for digital government. *Luxembourg: Publications Office of the European Union*, pages 8–10, 2019.

[3] Jack Beerman, David Berent, Zach Falter, and Suman Bhunia. A review of colonial pipeline ransomware attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, pages 8–15. IEEE, 2023.

[4] Cesar Bernardini, Muhammad Rizwan Asghar, and Bruno Crispo. Security and privacy in vehicular communications: Challenges and opportunities. *Vehicular Communications*, 10:13–28, 2017.

[5] Richard Gendal Brown, James Carlyle, Ian Grigg, and Mike Hearn. Corda: an introduction. *R3 CEV, August*, 1(15):14, 2016.

[6] Talal Ashraf Butt, Razi Iqbal, Khaled Salah, Moayad Aloqaily, and Yaser Jararweh. Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions. *IEEE Access*, 7:79694–79713, 2019.

[7] John Cantwell. A survey of theories of international production. *The nature of the transnational firm*, 2, 2000.

[8] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In *OsDI*, volume 99, pages 173–186, 1999.

[9] Eman Daraghmi, Ahmed Hamoudi, and Mamoun Abu Helou. Decentralizing democracy: Secure and transparent e-voting systems with blockchain technology in the context of palestine. *Future Internet*, 16(11):388, 2024.

[10] Marina Dorokhova, Jeremie Vianin, Jean-Marie Alder, Christophe Ballif, Nicolas Wyrsch, and David Wannier. A blockchain-supported framework for charging management of electric vehicles. *Energies*, 14(21):7144, 2021.

[11] Victoria Fernandez-Anez. Stakeholders approach to smart cities: A survey on smart city definitions. In *Smart Cities: First International Conference, Smart-CT 2016, Málaga, Spain, June 15-17, 2016, Proceedings 1*, pages 157–167. Springer, 2016.

[12] Jianli Guo, Korhan Cengiz, and Ravi Tomar. An iot and blockchain approach for food traceability system in agriculture. *Scalable Computing: Practice and Experience*, 22(2):127–137, 2021.

[13] Alan R Hevner, Salvatore T March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS quarterly*, pages 75–105, 2004.

[14] Velislava Hillman and Varunram Ganesh. Kratos: A secure, authenticated and publicly verifiable system for educational data using the blockchain. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 5754–5762. IEEE, 2019.

[15] industrialcyber. Port of lisbon targeted by lockbit ransomware hackers, website still down, 2023. Accessed: 2023-1-02.

[16] Jiawen Kang, Rong Yu, Xumin Huang, Sabita Maharjan, Yan Zhang, and Ekram Hossain. Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains. *IEEE Transactions on Industrial Informatics*, 13(6):3154–3164, 2017.

[17] Staffs Keele et al. Guidelines for performing systematic literature reviews in software engineering. Technical report, Technical report, ver. 2.3 ebse technical report. ebse, 2007.

[18] Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. Blockchained on-device federated learning. *IEEE Communications Letters*, 24(6):1279–1283, 2020.

[19] Rob Kitchin. The real-time city? big data and smart urbanism. *GeoJournal*, 79:1–14, 2014.

[20] Nir Kshetri. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10):1027–1038, 2017. Celebrating 40 Years of Telecommunications Policy – A Retrospective and Prospective View.

[21] Nir Kshetri. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*, 41(10):1027–1038, 2017.

[22] Bahareh Lashkari and Petr Musilek. A comprehensive review of blockchain consensus mechanisms. *IEEE Access*, 9:43620–43652, 2021.

[23] Francesco Longo, Letizia Nicoletti, Antonio Padovano, Gianfranco d'Atri, and Marco Forte. Blockchain-enabled supply chain: An experimental study. *Computers Industrial Engineering*, 136:57–69, 2019.

[24] Umer Majeed, Latif U. Khan, Ibrar Yaqoob, S.M. Ahsan Kazmi, Khaled Salah, and Choong Seon Hong. Blockchain for iot-based smart cities: Recent advances, requirements, and future challenges. *Journal of Network and Computer Applications*, 181:103007, 2021.

[25] Dianhui Mao, Zhihao Hao, Fan Wang, and Haisheng Li. Novel automatic food trading system using consortium blockchain. *Arabian Journal for Science and Engineering*, 44:3439–3455, 2019.

[26] Esther Mengelkamp, Johannes Gärttner, Kerstin Rock, Scott Kessler, Lawrence Orsini, and Christof Weinhardt. Designing microgrid energy markets: A case study: The brooklyn microgrid. *Applied energy*, 210:870–880, 2018.

[27] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. A review on consensus algorithm of blockchain. In *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 2567–2572, 2017.

[28] Saraju P. Mohanty, Uma Choppali, and Elias Kougianos. Everything you wanted to know about smart cities. *IEEE Consumer Electronics Magazine*, 5(3):60 – 70, 2016. Cited by: 820.

[29] Taewoo Nam and Theresa A Pardo. Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th annual international digital government research conference: digital government innovation in challenging times*, pages 282–291, 2011.

[30] Taewoo Nam and Theresa A. Pardo. Conceptualizing smart city with dimensions of technology, people, and institutions. In *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times*, dg.o '11, page 282–291, New York, NY, USA, 2011. Association for Computing Machinery.

[31] Weiquan Ni, Xumin Huang, Junxing Zhang, and Rong Yu. Healchain: A decentralized data management system for mobile healthcare using consortium blockchain. In *2019 Chinese Control Conference (CCC)*, pages 6333–6338. IEEE, 2019.

[32] Thays A Oliveira, Miquel Oliver, and Helena Ramalhinho. Challenges for connecting citizens and smart cities: Ict, e-governance and blockchain. *Sustainability*, 12(7):2926, 2020.

[33] Hend Farouh Patrizia Lombardi, Silvia Giordano and Wael Yousef. Modelling the smart city performance. *Innovation: The European Journal of Social Science Research*, 25(2):137–149, 2012.

[34] United Nations United Nations Human Settlements Programme. *World Cities Report 2022: Envisaging the future of cities*. United Nations Research Institute for Social Development, 2022.

[35] Deepak Puthal, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, and Gautam Das. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, 7(4):6–14, 2018.

[36] Pradip Kumar Sharma, Neeraj Kumar, and Jong Hyuk Park. Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Transactions on Industrial Informatics*, 15(7):4197–4205, 2019.

[37] Noordin Shehabuddeen, David Probert, and Robert Phaal. From theory to practice: challenges in operationalising a technology selection framework. *Technovation*, 26(3):324–335, 2006.

[38] A. Sheikh, V. Kamuni, A. Urooj, S. Wagh, N. Singh, and Dhiren Patel. Secured energy trading using byzantine-based blockchain consensus. *IEEE Access*, 8:8554–8571, 2020.

[39] G Summit. Smart cities: Regional perspective. *The Government Summit-Arab Region Dubai: UAE*, 2015.

[40] Zhaojing Wang, Tengyu Wang, Hao Hu, Jie Gong, Xu Ren, and Qiying Xiao. Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Automation in construction*, 111:103063, 2020.

[41] Karl Wüst and Arthur Gervais. Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 45–54, 2018.

[42] Junfeng Xie, Helen Tang, Tao Huang, F. Richard Yu, Renchao Xie, Jiang Liu, and Yunjie Liu. A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys Tutorials*, 21(3):2794–2830, 2019.

[43] Jie Xu, Cong Wang, and Xiaohua Jia. A survey of blockchain consensus protocols. *ACM Comput. Surv.*, 55(13s), July 2023.

[44] Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. Blockchain technology overview. *arXiv preprint arXiv:1906.11078*, 2019.

[45] ChuanTao Yin, Zhang Xiong, Hui Chen, JingYuan Wang, Daven Cooper, and Bertrand David. A literature survey on smart cities. *Science China. Information Sciences*, 58(10):1–18, 2015.

[46] Zhihao Yu, Liang Song, Linhua Jiang, and Omid Khold Sharafi. Systematic literature review on the security challenges of blockchain in iot-based smart cities. *Kybernetes*, 51(1):323–347, 2022.

[47] Aiqing Zhang and Xiaodong Lin. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *Journal of medical systems*, 42(8):140, 2018.

[48] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress)*, pages 557–564, 2017.

Appendix

Code Repository `https://github.com/zxy1a/smartcitytoolkit`
The repository contains the complete source code of the toolkit. The codebase is well-organized, with a clear directory structure where each component is placed appropriately. Users can easily locate specific files by referring to the folder names.

Demo Video `https://www.youtube.com/watch?v=zcLwtV2UrSw&ab_channel=Xinyue`
The video introduces the toolkit from four aspects: Docker environment configuration, backend workflow, database setup, and demonstration of test cases. It provides a comprehensive overview of how to use the toolkit effectively.

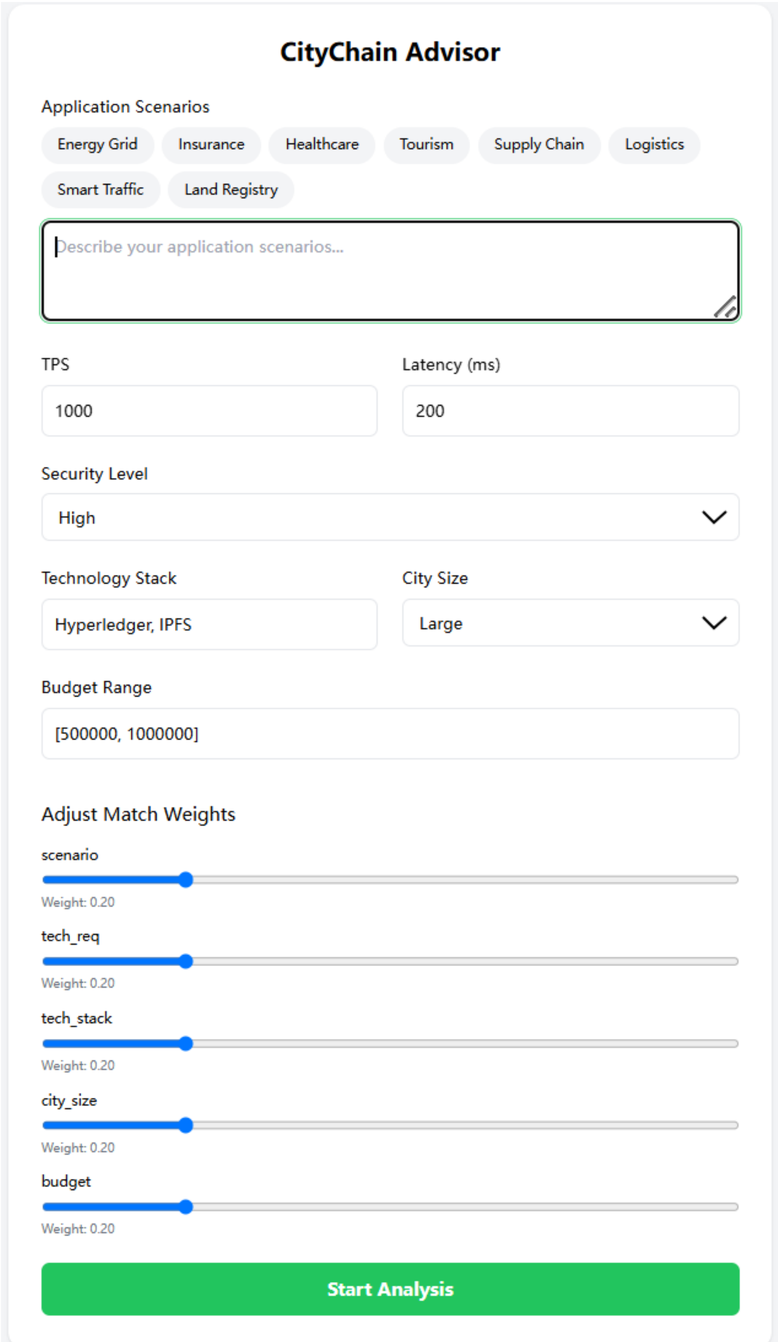


Figure 9. Toolkit Front-end Page

Non-exclusive licence to reproduce thesis and make thesis public

I, **Xinyue Zhang**,

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Towards Developing a Blockchain Selection Toolkit for Smart Cities,

   supervised by Dr. Mubashar Iqbal.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Xinyue Zhang
14/05/2025