Securi-Chain: Enhancing Smart Contract Security in Blockchain Systems Through Optimized Access Control

Keanu Swart, Stacey Omeleze Baror and Hein Venter
University of Pretoria, South Africa

keanu.swart@tuks.co.za
stacey.baror@cs.up.ac.za
hventer@cs.up.ac.za

Abstract: With the increase in usage of blockchain technology across domains, there is a high demand for the need of secure access control and a high level of security for smart contracts within blockchain to accommodate the domains that already implement blockchain and become accessible to other domains that require a high level of security in its transactions. This paper aims to evaluate the relationship between the best practices of access control and security of smart contracts in blockchain to optimise the usage of both technologies for blockchain usage across domains into a generalized blockchain model named the *Securi-Chain* Model. A literature review compares the relationship between access control and the security of smart contracts across three domains: Healthcare, IoT, and e-voting. Based on the findings of the literature review, *Securi-Chain* is proposed to implement the best practices displayed in these three domains and combine them in a way that ensures secure transactions across blockchain as a generalized approach that can be used throughout various domains. This model will also implement methods that enhance the security of transaction processes within the system. A Case Scenario is used to implement the *Securi-Chain* Model for the Healthcare and e-voting domains to display how this proposed model is used for domains that have been researched. The research that is conducted found that blockchain networks can support not only high-level access control across transactions in a network but also the security of smart contracts that comply to safeguard confidentiality, integrity, and data accessibility. *Secrui-Chain*, as well as the findings of the literature review, seem to benefit the domains that have been researched, as well as domains that require a high level of security regarding transactions across a network. These domains can benefit from using blockchain technology as well as the level of security that comes with the access control and security of smart contracts that have been implemented in *Securi-Chain*.

Keywords: Access-Control, Security-Requirements, Blockchain, Smart Contracts, Transactions

1. Introduction

Blockchain has emerged as a revolutionary technology, transforming numerous sectors by enabling secure and transparent transactions. A crucial element within blockchain is smart contracts, which are notable for automating agreements and initiating operations. However, the adoption of blockchain has faced challenges, primarily related to access control and privacy protection concerns in smart contracts. With blockchain systems storing sensitive data and managing intricate transactions, the establishment of robust access control mechanisms becomes critical. Current access control strategies in industry-oriented blockchain systems often need to fully meet the privacy demands tied to smart contracts (Pradnya, et al., 2021). Unauthorized access, coupled with the struggle to revoke such access effectively, poses risks to the system's data confidentiality and integrity (Khan, et al., 2018). This research plans to examine the relationship between access control methods and the privacy attributes of smart contracts within a blockchain framework. It aims to assess the efficiency of various access control strategies employed in industry-standard blockchain setups, including Role-Based Access Control (Pradnya, et al., 2021) and Token-Based Access Control (Ouaddah, et al., 2017) (Neloy, et al., 2023) among others discussed later. The goal is to discern their strengths, weaknesses, and adaptability for diverse sectors, pinpointing an access control strategy that is universally applicable and ensures privacy across these sectors. The methodology encompasses a Literature Review, Model, and Case Scenario. The Literature Review dives into studies examining access control methods in domains such as IoT, Healthcare, and e-Voting. This review aims to assess the applicability and efficiency of different access control methodologies, especially the preservation of privacy within smart contracts. The model, termed *Securi-Chain*, offers a conceptual depiction of a blockchain system's access control, which is aimed at robust access control and privacy preservation within smart contracts. This model will incorporate the most promising access control techniques. Designed to be domain-agnostic, *Securi-Chain* will strive for heightened privacy measures, considering the unique demands and challenges of the domains assessed in the review. The Case Scenario validates *Securi-Chain's* accuracy concerning its implementation domain, validating its real-world applicability and effectiveness. Current access control models in many blockchain systems need to be revised to address complex privacy needs (Pradnya, et al., 2021). This study aims to analyse and compare prevalent access control methods by identifying their benefits and disadvantages to establish a versatile access control model suitable

for diverse privacy requirements in different blockchain applications. With the prevalence of unauthorized access and potential data breaches in industrial smart contracts, there is a need to find solutions that mitigate these risks, ensuring secure and restricted access to sensitive data. Current systems often grant all-or-nothing access (Khan, et al., 2018), needing more nuanced access policies. In addition to analysing access control methods, this research seeks to explore access control mechanisms offering finer granularity, promoting dynamic and adaptive access policies within smart contracts. Addressing these challenges, *Securi-Chain* will be developed, offering an optimal access control solution enhancing privacy in blockchain-based smart contracts across various sectors. This paper is structured as follows: Section 3 introduces *Securi-Chain*, detailing its layers and importance. Section 4 elaborates on *Securi-Chain's* transaction processes with detailed diagrams and descriptions. Section 5 presents a case scenario illustrating *Securi-Chain's* adaptability, focusing on Client EMR transfers in healthcare. Section 6 reviews the literature that informed *Securi-Chain's* development, focusing on access control methods and smart contract security. Section 7 evaluates *Securi-Chain*, assessing features enhancing smart contract security. Section 8 concludes, summarizing the paper and discussing future opportunities concerning *Securi-Chain* and smart contract access control methods. Beginning with Section 2 which provides the necessary background knowledge.

2. Background

This section will introduce essential components and features that will assist in providing a solid foundational knowledge to understand the remainder of this paper. The foundation of this paper is built upon *Blockchain technology*. *Blockchain technology* is a transformative innovation that has gained significant attention in recent years. "A blockchain consists of a chain of blocks that contains information about transactions," (Dias, et al., 2019) and each of these transactions is digitally signed by the entity emitting them. "Transactions are combined into a block, that is committed to the chain, establishing the blockchain." (Dias, et al., 2019). Blockchain is characterized by its openness, transparency, and distributed nature, "record[ing] transactions between two parties efficiently in a verifiable and permanent way." (Ding, et al., 2019) Blockchain's applications offer a broad range of possibilities for industries seeking secure and transparent record-keeping solutions (Yli-Huummo, et al., 2016). The implementation of blockchain technology also introduces innovative *Access Control* mechanisms, ensuring secure transactions. "Attributed based access control (ABAC) is a logical access control model, which controls the access between subjects and objects, according to the attributes of entries, operations and related environments" (Liu, et al., 2020). ABAC "firstly extracts the attributes of user (subject), resource (object), permission and environment respectively, then combines the relationship of these attributes flexibly, and finally transforms the management of permission into the management of attribute, providing a fine-grained and dynamic access management method" (Liu, et al., 2020). ABAC offers "an attribute-based access control policy" which "combines a set of rules expressing conditions over a set of attributes paired to the subject, to the resource or to the environment" (Maesa, et al., 2017) and in turn "eliminates the stress of allocating roles or making access control list for all devices in the system" (Pradnya, et al., 2021) essentially enabling entities to define access policies based on attributes, highlighting ABAC's adaptable access management solutions. Effective access control within blockchain networks is closely linked to *Consensus Mechanisms*, as they collectively shape the security and integrity of the entire system. Blockchain *consensus mechanisms* are seen to serve as "a fault-tolerant mechanism for transaction verification". "Proof of Stake (PoS)," has been introduced as an energy-efficient option that incorporates the stake size to address fairness concerns, making it a sustainable consensus approach. As "several blockchain solutions initially employ PoW and gradually transform to PoS," the evolution of consensus mechanisms is evident (Lashkari & Musilek, 2021). *Smart contracts*, pivotal to blockchain technology, are "self-executing programs based on agreements between two or more different parties." (Neloy, et al., 2023) They represent a "series of symbolic protocols" that are automatically executed within the blockchain environment (Liu & Liu, 2019). Essentially, these contracts require a trigger, sourced either from the "frontend or backend program of the main application." (Neloy, et al., 2023) Without smart contracts, a blockchain would simply be a "normal database that cannot be changed or manipulated." (Liu & Liu, 2019) Thanks to the advent of decentralized blockchain technology, a trusted environment has been established in recent years, further amplifying the role and relevance of smart contracts.

3. High-Level Model of Securi-Chain

The *Securi-Chain* model is a conceptual blockchain model that has been developed for the purpose of offering optimal access control methods in relation to efficient security for smart contracts in addition to being a

generalized model that offers adaptability across domains. The following sub-sections details the respective layers that form *Securi-Chain*.

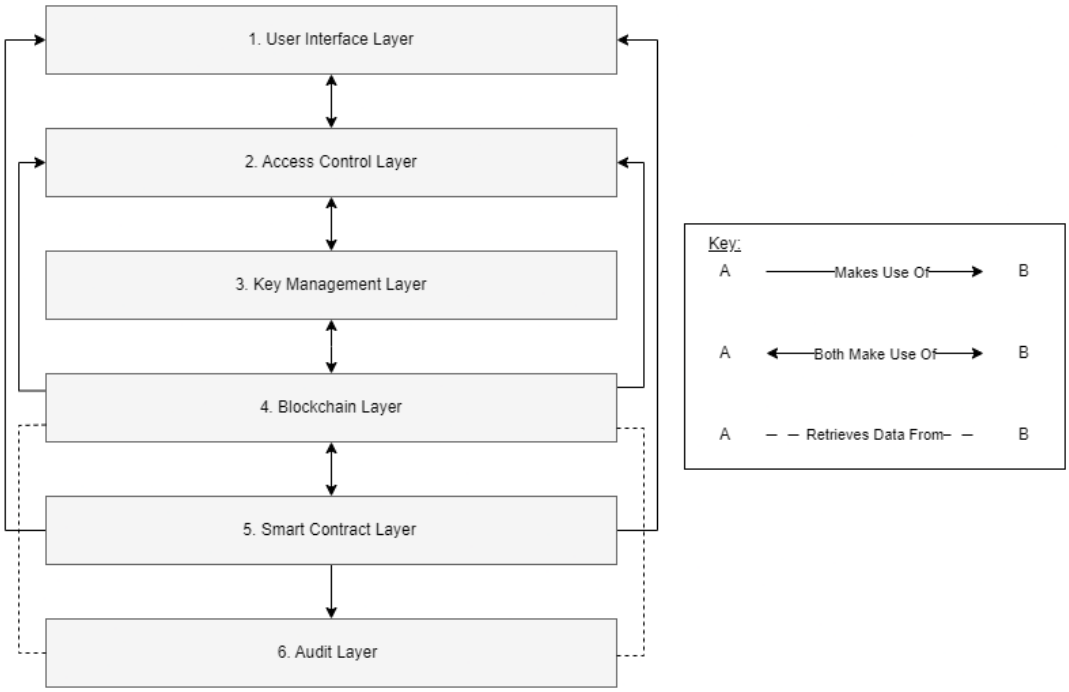

Figure 1: High-Level model of Securi-Chain

3.1 User-Interface Layer

The User-Interface Layer comprises three primary components: an *Authentication Module* for secure user logins, a *Smart Contract Interface* to manage transaction inputs and displays, and a *Notification System* that updates the user on transaction statuses. Users interact directly with the system through this layer, which communicates directly with the Blockchain Layer to initiate transactions.

3.2 Access Control Layer

The Access Control Layer has an *Attribute Checker* that is used to validate user permissions based on the attributes a user possesses. The *Multi-Signature Validator* functionality is used to check for necessary approvals for a transaction. This layer interfaces with the User-Interface Layer for access decisions and engages with the Blockchain Layer to enforce transactional access rules.

3.3 Key Management Layer

Key Management focuses mainly on cryptographic functionalities, including the *Generation*, *Storage*, *Rotation*, and *Distribution* of cryptographic keys. It ensures *Encryption* of user credentials via interaction with the User-Interface Layer and liaises with the Access Control Layer for cryptographic identity verifications.

3.4 Blockchain Layer

At the Blockchain Layer, user inputs are processed through components such as the *Transaction Constructor and Signer*. The *Broadcast Module* distributes transactions across the network, the *State Database* holds the current blockchain status, and the *Consensus Mechanism* sets validation rules by implementing PoS. With a comprehensive *Node Network* and a *Homomorphic Encryption Module*, this layer interacts with the User-Interface Layer for inputs and the *Smart Contract Executor* for private transactions, requiring cryptographic services from the Key Management Layer.

3.5 Smart Contract Layer

The Smart Contract Layer provides tools for contract creation and houses a library of deployed contracts. With *Oracles* and a *Smart Contract Executor*, this layer facilitates smart contract interactions and decisions. It predominantly interfaces with the Blockchain Layer for state modifications and transaction handling.

3.6 Audit Layer

Ensuring transparency and compliance, the Audit Layer logs transactions through the *Transaction Logger* and monitors them with the *Regulatory Checker* for adherence to set regulations. This layer closely observes the Blockchain Layer's activities and generates necessary audit reports and alerts. Based off the understanding of the layers that offer a foundation for *Securi-Chain*, a detailed walkthrough of the transaction process for the model will be presented.

4. Detail of the Transaction Process for the Securi-Chain Model

A secure transaction platform forms a strong foundation for a blockchain network. The following subsections are with respect to the secure transaction process offered by *Securi-Chain*. Each written section below corresponds to its respectively numbered section in *Figure 2*.

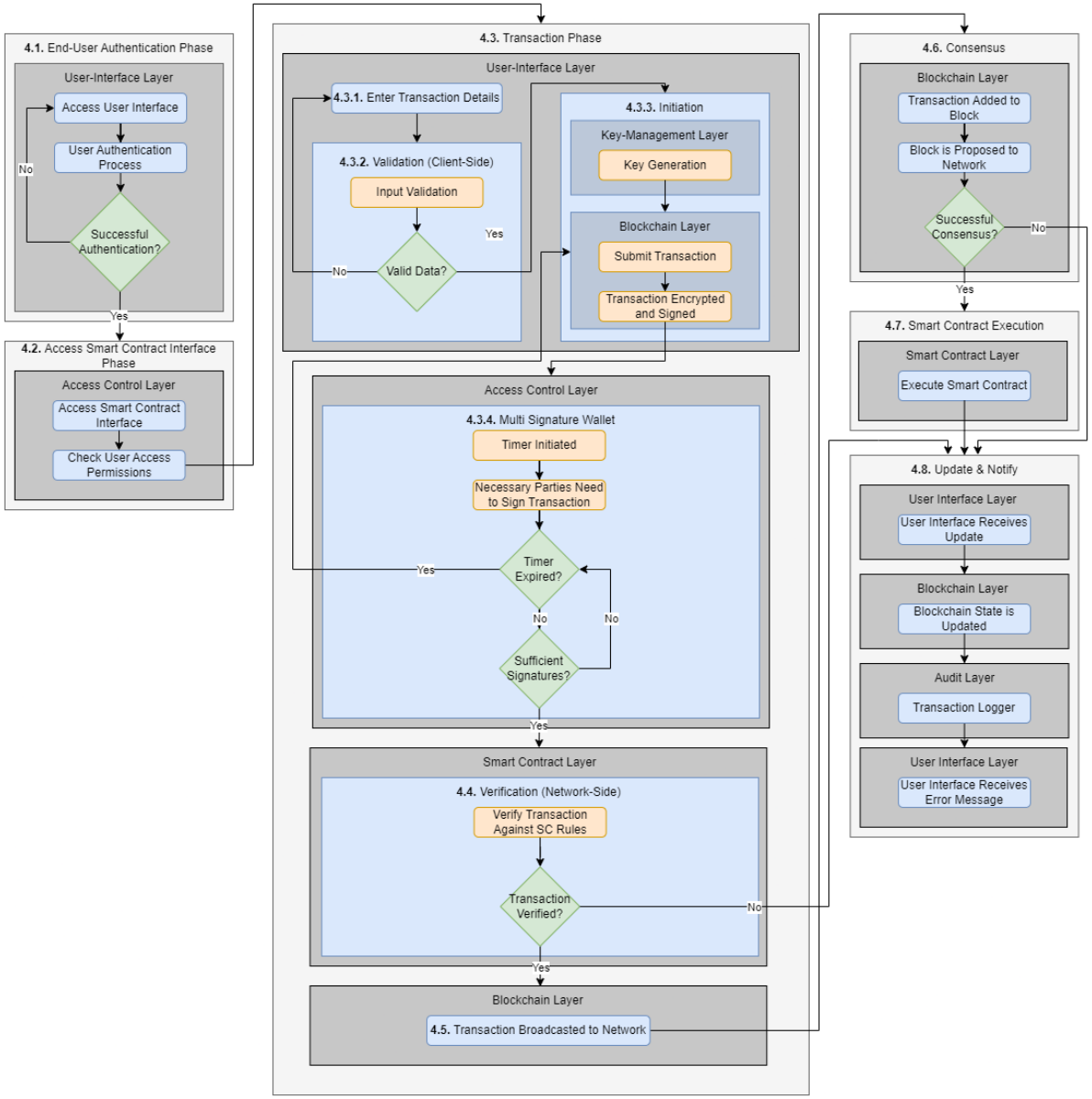

Figure 2: Detail of the Transaction Process for the Securi-Chain Model

4.1 End-User Authentication

To initiate the transaction, the user accesses the web-based user interface. Next, they are prompted to provide authentication to verify their identity. Depending on the domain in which this model is applied, authentication methods may include biometrics, passphrases, or multi-factor authentication. For enhanced security, the user's credentials are encrypted and matched with encrypted credentials in the network's

database to ensure validity. If the user fails the authentication multiple times, they are temporarily locked out of the system.

4.2 Access Smart Contract Interface

Once authenticated, the user accesses the smart contract interface to create and submit their transaction. Before proceeding, the system applies access control using the *Attribute Checker*, determining the user's functionality during the transaction creation and submission phase. Only administrators can create or edit the access control settings in the *Attribute Checker* which is part of the Access Control Layer.

4.3 Transaction Phase

4.3.1 Enter transaction details

In the smart contract interface, users enter the necessary information into the transaction fields, tailored to the specific industry where the model applies. These fields typically include the recipient's address within the network and any intended message. These fields are determined but the administrative party.

4.3.2 Transaction validation (client-side)

After inputting the necessary transaction details, the client-side interface validates the data to ensure it aligns with the domain-specific formats and criteria. Should the validation fail, users receive a prompt to correct the discrepancies. These domain-specific formats and criteria are set by the administrative party of the blockchain network.

4.3.3 Initiation

Should the transaction clear validation, it undergoes Homomorphic encryption, using a key accessed from the *Key Management Layer* (*Figure 1, 3*). Additionally, the user's private key signs the transaction, generating a Digital Signature that's appended to the transmitted data. The process then moves to the *Multi-Signature Wallet* phase.

4.3.4 Multi-Signature wallet

User permissions are verified against specified fields, triggering a time lock. This time lock is initiated when the digital signature has successfully been generated and appended to the transmitted data. Within this timeframe, necessary administrative parties must sign the transaction, ensuring swift processing and avoiding potential bottlenecks or prolonged vulnerability to attacks. Given the Multi-Signature Wallet's nature, only a predetermined number of authorized users are needed to sign for transaction acceptance. If signatures aren't secured in time, the transaction cycles back to the submission phase, slotting into the end of the current transaction queue to prevent further bottlenecks.

4.4 Verification (Network-Side)

Validator nodes within the network validate the digital signature using the sender's public key. Once verified, these nodes compare the transaction to the smart contract's stipulations. Initially, they authenticate the digital signature to confirm the transaction's integrity. For further verification against the smart contract rules — via the *Smart Contract Layer* (*Figure 1, 5*) — these nodes process the contract logic on the encrypted data. Since this data remains encrypted homomorphically, the smart contract interacts without needing decryption. The essential key for digital signature verification comes from the *Key Management Layer* (*Figure 1, 3*). With the data encrypted in this manner, it ensures confidentiality, integrity, and authenticity during processing, eliminating potential overheads.

4.5 Transaction Broadcast to Network

Now that the transaction has been signed-off by an authorized party, the transaction is safe to be broadcasted to the Blockchain network where this model resides in. This is where all nodes in the network with sufficient access control will be able to receive the transaction request. At this stage, the transaction isn't yet considered confirmed or finalized. Broadcasting simply means making the network aware of a new transaction.

4.6 Consensus

After verification, the transaction is added to a block. All nodes in the blockchain network participate in a consensus, PoS. If the transaction can reach a consensus, the transaction is firstly added to the memory pool,

to wait for the Smart Contract Execution phase (*Figure 2, 7.7*) and is then added to the blockchain. If a consensus cannot be reached, the transaction as whole is rejected.

4.7 Smart Contract Execution

Now that the transaction is ready to be executed, a validator node fetches the transaction from the memory pool and includes it in a new block in the blockchain network, this is where the network of nodes will validate the block. If the conditions in the smart contract are met, the transaction is finally executed. If the execution is successful, the results of that execution are recorded in its respective block.

4.8 Update & Notify

Now that the transaction has been completed, the user's interface will receive a notification about the status of the transaction – whether it failed or whether it succeeded. If the transaction was successful, the blockchain state in the Blockchain Layer is updated, however, if the transaction failed, an error message is displayed to the end user. To showcase the adaptability of this model as well as the transaction process that has been detailed, the model has been seen to be conceptualized in a suitable scenario that is made use of in the healthcare domain (Dias, et al., 2019).

5. Case Scenario: EMR Sharing

The following scenario intends to showcase the adaptability and secure nature of *Securi-Chain* by implementing it within a scenario that is prevalent in the healthcare domain, namely the Electronic Medical Record (EMR) transfer within a blockchain network (Dias, et al., 2019). In the city of 'Medville', Bob is advised to visit a new heart specialist, Alice. Alice needs his medical history to provide an accurate diagnosis, so she turns to *Securi-Chain*. Alice logs into the *Securi-Chain* User Interface. She enters her credentials for the network, which are encrypted and verified against the encrypted credentials stored in the network's database. Alice authenticates successfully, allowing her to access the smart contract interface (Figure 2, 4.1). In the smart contract interface, the system's access control checks Alice's permissions based on her assigned attributes via the Attribute Checker. This ensures she has sufficient access rights to proceed with creating and submitting a transaction request to access Bob's EMR data (Figure 2, 4.2). Alice is verified through access control and enters the transaction details in the smart contract interface. She inputs the required transaction details, including Bob's network address and a message indicating her intention to access his EMR (Figure 2, 4.3.1). After Alice submits her transaction details, the client-side interface validates them, ensuring they meet the required format and criteria for this adaptation of *Securi-Chain* (Figure 2, 4.3.2). Alice's transaction request, now validated, undergoes Homomorphic encryption, and is signed with her private key, generating a Digital Signature (Figure 2, 4.3.3). The transaction then enters the Multi-Signature Wallet phase (Figure 2, 4.3.4). Here, the necessary administrative parties, in this case, the manager and the referring doctor's account are notified through the application that they must sign the transaction within a set timeframe. Once the required number of authorized parties sign, the transaction is pushed into the network. Validator nodes in the network check the digital signature using Alice's public key, verifying the transaction against the smart contract rules, and executing the contract's logic on the encrypted transaction data (Figure 2, 4.4). After verification by the validator nodes, the transaction broadcasts into the blockchain network, waiting for consensus (Figure 2, 4.5). Picked up for consensus, the transaction adds to a block and enters a consensus stage using PoS. Reaching consensus, it moves to the memory pool, awaiting smart contract execution (Figure 2, 4.6). A validator node retrieves the transaction from the memory pool, includes it in a new block, and, upon successful validation and meeting smart contract conditions, records the results in the new block (Figure 2, 4.7). Alice receives a notification that the transaction is successful. The blockchain state updates and Alice accesses Bob's EMR. Prepared for medical consultation, Bob also gets a notification that Alice views his EMR, enhancing transparency in the EMR sharing process (Figure 2, 4.8). The *Securi-Chain* model facilitates a seamless, secure, and transparent interaction between Alice and Bob's EMRs, enabling Alice to provide Bob with accurate medical consultation. Concluding the details of *Securi-Chain*, it is worth noting the related literature that assists the development and evaluation of it.

6. Related Work

Reference	Summary	Related Contribution	Conclusion
(Salonikias, et al., 2022)	The proposed model focuses on data privacy and accessibility by removing centralized vulnerabilities. NGAC	*Securi-Chain* prioritizes Fine-Grained Access Control (FGAC) and access precision, with the	There is a shared focus on security in both models, with *Securi-*

Reference	Summary	Related Contribution	Conclusion
	provides enhanced access precision by enforcing admin efficiency. However, there are scalability concerns that arise from NGAC deployments in addition to complexities mentioned due to healthcare provisioning.	Access Control Layer (*Figure 1, 2*). Both models emphasize cryptographic security, with *Securi-Chain* having a dedicated Key Management Layer (*Figure 1,* 3).	*Chain* employing cryptographic methods in conjunction with FGAC that complement the practicality of the methods used in this paper.
(Dias, et al., 2019)	This paper focuses on achieving FGAC through ABAC and RBAC. It emphasizes the importance of authenticity, immutability, and auditability in the context of access control mechanisms. The study emphasizes the significance of maintaining consensus among distributed nodes while maintaining robust access control measures.	*Securi-Chain* aims to ensure secure and controlled access to sensitive data. Moreover, the attention given to administrative efficiency and consensus in proposed framework is mirrored in *Securi-Chain*.	*Securi-Chain* has utilized FGAC with decentralisation, ensuring secure access management, privacy preservation and effective administrative operations features proposed by this paper.
(Ouaddah, et al., 2017)	This paper introduces the *FairAccess* framework which employs Token-Based Access Control (TBAC) methods, addressing IoT access control challenges, promoting decentralized decisions, and ensuring transparent and traceable access records, thus allowing fine-grained policy definitions. Integrating these systems poses complexities, and transaction validations can strain system efficiency, with the consensus algorithm being a pivotal factor.	Once again, *Securi-Chain* values FGAC, due to the Access Control Layer *(Figure 1, 2)* facilitating access decisions similarly to the *FairAccess* framework. The Audit Layer (*Figure 1, 6*) aligns with discussed emphasis on transparency, traceability, and auditable records. Both frameworks also promote decentralized decision-making, enhancing the system's reliability and integrity.	The Securi-Chain model has made use of components mentioned in this paper's model, such auditable access management - by implementing the Audit Layer (*Figure 1, 6*).
(Pradnya, et al., 2021)	This paper displays the integration for blockchain with IoT in addition to how encryption techniques offer enhanced security. The combination of blockchain with encryption for IoT provides improved data integrity, minimizes transaction interference as well as enhancing reliability and eliminating single-points-of-failure. Future works should emphasize scalability issues, protocol standardization between IoT devices and blockchain technology in addition to computation overhead.	Both models provide the capability of integration between blockchain and IoT devices. Both highlight the importance of decentralization, with *Securi-Chain* using various layers to enhance reliability. Data integrity is a shared concern, with *Securi-Chain* employing cryptographic functions, digital signing, and consensus mechanisms to align with discussed emphasis on integrity and automation in supply chain management.	There is mutual emphasis in both models regarding supply chain management due to the decentralized nature of blockchain.
(Khan, et al., 2018)	This paper presents an Access Control layer that offers a range of authentication methods that include biometrics as well as username/password input. Through validation of these methods, authorized users are allowed to cast their votes, while denying further access to those who fail to authenticate. The focus of this paper lies in ensuring a robust access control mechanism that bolsters privacy and security in the voting blockchain system.	Both models underscore the importance of robust access control and authentication methods. The web-based application feature highlighted in this paper is relevant to *Securi-*Chain's user interface, providing a platform for user interaction and transaction initiation.	*Securi-Chain* has employed a web-based application interface that is discussed in this paper's model, as well as the implementation of transaction initiation.
(Neloy, et al., 2023)	This paper introduces an access control model centred around unique identifiers: voter's State ID, Wallet Address, and Email. This model leverages government databases to validate the identity of voters. Moreover, the access control model ensures that each voter can only cast a single vote. By employing these measures, the paper aims to establish a secure and privacy-enhancing access control mechanism within the voting blockchain system.	Both models mentioned deploy robust access control mechanisms for authentication and access decisions. *Securi-Chain*'s multi-layered model mirrors the reliability and real-time confirmation shown in the paper, allowing for real-time updates to be displayed to the user. Both models can also be adapted for different sectors.	*Securi-Chain* is seen to adopt a multi-layered model that allows for real-time updates to the user interface as well as the ability to be adapted to various domains, such as the model mentioned in the paper.

7. Evaluation

The *Securi-Chain* model, demonstrated through the EMR transfer scenario, exemplifies secure and transparent data exchange in healthcare. Its adaptability and efficiency underline its significance. Central to *Securi-Chain* is its layered architecture, offering a dynamic user interface adaptable across domains for the quick, secure, and ethical transfer of sensitive information. This dynamic adaptability, coupled with an intuitive interface, underscores the model's user-focused approach. The model benefits from the integration of optimal features derived from academic research. This encompasses a robust access control layer (Khan, et al., 2018), a focus on unique identifiers (Neloy, et al., 2023), and an emphasis on granular data privacy (Salonikias, et al., 2022). *Securi-Chain* seamlessly combines these best practices to meet current needs and sets a standard for future initiatives. A deeper examination, comparing *Securi-Chain* to related works, provides valuable perspectives. Khan et al. (2018) highlights the importance of a comprehensive access control layer, advocating for diverse authentication methods, a sentiment echoed in *Securi-Chain*. Neloy et al. (2023) stress the need for unique identifiers to ascertain identity, aligning with *Securi-Chain's* robust access controls. However, the model has its constraints. Its dependence on a layered, real-time framework could lead to delays in larger networks, affecting immediate data access. Its universal suitability might be questionable in areas with infrastructural issues or strict data laws. These challenges indicate areas for future improvement, such as scalability and further adaptability. Salonikias et al. (2022) and Dias et al. (2019) resonate with *Securi-Chain's* focus on data privacy and balancing security and transparency. While Ouaddah et al. (2017) stress transparent access controls in their *FairAccess* framework, *Securi-Chain's* decentralized decision-making enhances its trustworthiness and highlights areas for investigation. Its alignment with key principles from notable research solidifies its credibility. The incorporation of ABAC signifies its versatility. Such mechanisms guarantee data safety and rightful access, mirroring Dias et al. (2019). The layers discussed in *Figure 1* can be seen to prevent potential security issues, such as user misbehaviour. The Audit Layer provides an oversight into user activity that can be viewed by administration. If anything is deemed as misbehaviour, the team will be able to identify where this misbehaviour originated from and from who and will be able to handle this as expected. As blockchain and access control evolve, *Securi-Chain* must adapt to remain scalable. The system's commitment to user-awareness, exemplified by notifying Bob when Alice accesses his EMR, ensures transparency and accountability. With decentralized management, it melds security and responsibility. As *Securi-Chain* evolves, it leads in secure, decentralized systems, but it also acknowledges the need for continuous adaptation in a dynamic cybersecurity environment.

8. Conclusion

In conclusion, the *Securi-Chain* model stands as a paradigm for enhancing the security and privacy of transactions within the realm of blockchain. Its distinct layered architecture, combined with its user-centric design, establishes it as a desirable adaptable solution for access control in blockchain-powered smart contracts. While it has competently integrated features from academic research, the challenges it faces, especially in scalability and adaptability, emphasize the model's potential for future enhancement. By addressing these challenges, *Securi-Chain* not only supports the safe and efficient adoption of blockchain technology across multiple sectors but also emphasizes the crucial balance between confidentiality, integrity, and data accessibility. Moving forward, practical implementations and consistent refinement of the model are essential. Future work in this area should focus on real-world implementation and further refinement of the *Securi-Chain* model, as well as exploring additional use cases and domains for its application in addition to further optimising the scalability and adaptability of *Securi-Chain* in order to test these characteristics for the given architecture of the model.

References

Dias, J. P., Ferreira, H. S. & Martins, A., 2019. A Blockchain-Based Scheme for Access Control in e-Health Scenarios. *Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018),* pp. 238-247.

Ding, S. et al., 2019. A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT. *IEEEAccess,* 7(SPECIAL SECTION ON SECURITY AND PRIVACY FOR CLOUD AND IOT), pp. 38431-38432.

Khan, K. M., Arshad, J. & Khan, M. M., 2018. Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research (IJEGR),* 14(1), pp. 53-62.

Lashkari, B. & Musilek, P., 2021. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEEAccess,* Volume 9, pp. 43620-43630.

Liu, H., Deshi, H. & Li, H., 2020. Fabric-iot: A Blockchain-Based Access Control System in IoT. *IEEEAccess,* 8(SPECIAL SECTION ON BLOCKCHAIN-ENABLED TRUSTWORTHY SYSTEMS), pp. 18207-18209.

Liu, J. & Liu, Z., 2019. A Survey on Security Verification of Blockchain Smart Contracts. *IEEEAccess,* Volume 7, pp. 77894-77895.

Maesa, D. D. F., Mori, P. & Ricci, L., 2017. Blockchain Based Access Control. *17th IFIP International Conference on Distributed Applications and Interoperable Systems (DAIS),* pp. 206-220.

Neloy, M. N. et al., 2023. A remote and cost-optimized voting system using blockchain and smart contract. *IET Blockchain.*

Ouaddah, A., Elkalam, A. A. & Ouahman, A. A., 2017. Towards a novel privacy-preserving access control model based on blockchain technology in IoT. *Europe and MENA cooperation advances in information and communication technologies,* pp. 523-533.

Pradnya, P., M, S. & Vidhyacharan, B., 2021. Blockchain for IoT access control, security and privacy: a review. *Wireless Personal Communications,* Volume 117, pp. 1815-1834.

Salonikias, S., Khair, M., Mastoras, T. & Mavridis, I., 2022. Blockchain-based access control in a globalized healthcare provisioning ecosystem. *Electronics,* 11(17), p. 2652.

Yli-Huummo, J. et al., 2016. Where is Current Research on Blockchain Technology? - A Systematic Review. *PLoS ONE,* 11(10), pp. 1-4.