https://dx.doi.org/10.4314/dujopas.v9i4b.30
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 9 No. 4b December 2023*

A Car Insurance Claim Processing Prototype Using Smart Contracts and Zero-Knowledge Proofs

[1]Mamudu Francis Itanyi, [1]Modi B., [1]Mamudu Friday

[1]Department of Computer Science,
Gombe State University
Gombe,
Nigeria

Email: mamudufrancis2014@gmail.com

Abstract

Ensuring the confidentiality and accuracy of owner information is critical in car insurance claims. However, the current traditional auto insurance claims system is inefficient and prone to data leaks, leading to service confusion and inaccurate data. The primary focus is on enhancing the privacy and security of insurance information and car owner data. This paper employs blockchain, smart contracts, and zero-knowledge proof technologies to address privacy concerns and introduces an innovative car insurance claim system. The system transforms authorization and claims processes, incorporating private and public smart contracts for issuing and canceling auto insurance, as well as authorizing and validating claims. Using ZoKrates optimizes data storage and computation on the blockchain while preserving maximum privacy for sensitive information. Experimental results affirm the effectiveness of the scheme in terms of security and performance.

Keywords: Insurance; Blockchain; Smart Contract; Zero-Knowledge Proof; Prototype

INTRODUCTION

The insurance industry is currently undergoing a digital transformation to align with the evolving needs of modern society (Satuluri, 2021). In the realm of car insurance, the collaboration of various entities from different fields, such as the police, county administrators, insurance agents, and healthcare professionals, is vital for effective car insurance claims management (Catlin et al., 2018). This collaborative sharing of multi-source information is essential for insurance companies to make accurate decisions regarding policyholders' claims.

While insurance plans are widespread, settling and processing insurance claims can be challenging and prone to errors (Huang et al., 2022). Issues such as manipulation of terms and conditions by insurance companies to avoid payouts and the presence of fraudulent claims pose challenges for insurers (Derrig, 2002). Block chain and smart contracts present advantages that can enhance transparency, efficiency, and resistance to fraud in insurance contracts (Gatteschi et al., 2018). Various block chain-based solutions have been proposed, with the core idea of establishing a trust mechanism between customers and insurance companies, confirming the content of car insurance payouts. Automated smart contracts can expedite claims processing and reduce insurers' operating costs (Qi et al., 2020).

**Author for Correspondence*

However, the use of block chain-based car insurance plans introduces two significant challenges. Firstly, the public exposure of users' identities and insurance details may lead to privacy breaches and information misuse (Qi et al., 2020). Attackers could access transaction data, analyze it, and trace relationships between transactions and accounts. Secondly, the reliance on the automatic execution of smart contracts in the car insurance claims process may expose sensitive information on the block chain, such as the vehicle owner's identity, compromising privacy (Khan et al., 2021). To address these challenges, further advancements in privacy-preserving techniques and data encryption on the block chain are necessary.

A number of studies have been conducted to demonstrate the applications of blockchain in the insurance industry. In recent years, groundbreaking contributions have propelled the integration of smart contracts into the realm of car insurance policies. Bader et al. (2018) spearheaded this shift, introducing a smart contract-based framework during the 2018 IEEE Globecom Workshops in Abu Dhabi. Departing from traditional models, their approach revolutionized the landscape of car insurance policies. Simultaneously, Baghery et al. (2020) focused on enhancing the security of car insurance claim processing. Presented at the International Conference on Cryptology and Network Security in Vienna, their research delved into utilizing zero-knowledge proofs, specifically Groth’s zk-SNARK, to fortify the confidentiality of claims-related information.

In line with these advancements, Bhamidipati et al. (2021) unveiled the Claim chain platform at the 2021 IEEE International Conference on Blockchain in Melbourne. This innovative blockchain system is meticulously designed to secure and transparently manage the entire lifecycle of insurance claims. Meanwhile, Chiu and Meng (2021) explored decentralized possibilities in insurance, as exemplified in their study presented at the 36th Annual ACM Symposium on Applied Computing. Focusing on bicycle insurance, their research showcased the potential of blockchain to establish efficient and decentralized systems for managing insurance policies.

The utilization of blockchain in various sectors, including insurance services, has garnered considerable interest in recent times. This paper provides a hybrid smart contract proxy model, utilizing a private smart contract for creating car insurance to protect insurance data from third-party access. A public smart contract is then employed for insurance verification, achieving identity authentication without revealing sensitive user information. The use of ZoKrates enables zero-knowledge authorization and verification for car insurance, avoiding the exposure of privacy attributes' ownership in a publicly transparent distributed ledger and ensuring non-linkability between vehicle owners and their insurance details.

Smart contracts

A smart contract is a computerized script anchored on a blockchain that executes predefined actions when triggered by a validated transaction. Despite its name, a smart contract is essentially 'dumb' computer code and may not always represent a legally binding construct. The concept predates blockchain. According to Swan (2015), a smart contract is a self-executing computer program that runs on a blockchain, containing code that directly implements, verifies, or enforces the terms of an agreement or contract. It automatically executes predefined actions when certain conditions specified in the code are met, facilitating trustless and transparent transactions. They range from simple logic execution to more complex processes resembling legal contracts. An example is an automated hotel room management system, where leaving the room triggers predefined actions like billing or cleaning. While initially seeming unnecessary for centralized processes, smart contracts on a blockchain become valuable when involving multiple entities, reducing trust issues and

improving process efficiency through transparent and forgery-proof information logging. Smart contracts function on blockchain networks like Ethereum or Hyperledger Fabric. Figure 1 illustrates the operational process of smart contracts on the blockchain, aided by a practical example.

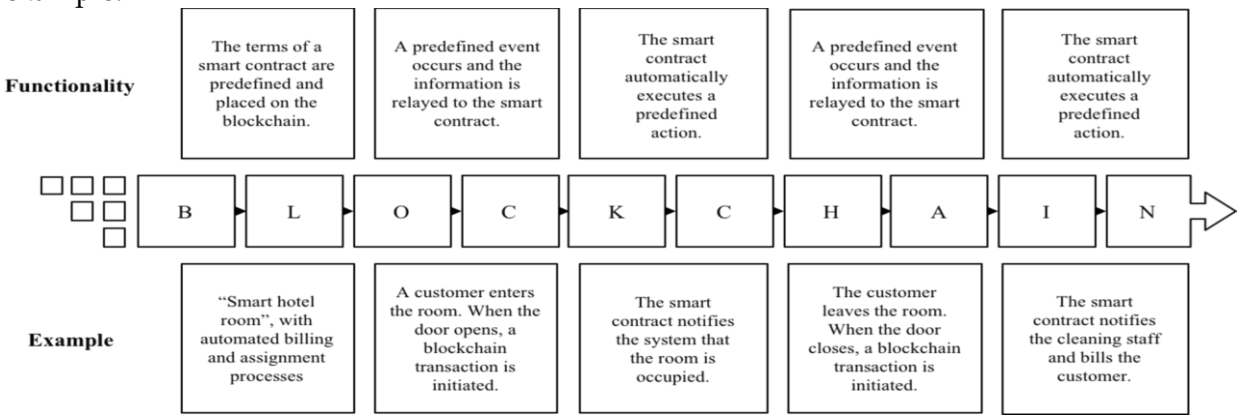


Figure 1. Smart contract on the block chain. *Source*: Ante, L. (2020)

Zero-Knowledge Proofs

Zero-Knowledge Proofs (ZKPs) are cryptographic protocols that allow one party, the prover, to demonstrate the truth of a statement to another party, the verifier, without revealing any additional information beyond the statement's validity (Anthony et al, 2021). These proofs come in interactive and non-interactive forms, enabling secure and private transactions. ZKPs find applications in diverse fields, including blockchain technology, where they enhance privacy by allowing users to prove ownership or knowledge of specific data without disclosing the data itself (Bader et al., 2018). This cryptographic concept plays a crucial role in ensuring confidentiality and security in digital interactions, contributing to advancements in authentication protocols and confidential transactions.

Car Insurance Claim Processing

Car insurance claim processing involves the assessment and settlement of claims made by policyholders following incidents like accidents, theft, or damage to their vehicles. This crucial aspect of the insurance industry faces challenges such as inefficiencies, data reliability issues, and security concerns (Huang et al., 2022). Traditional processes often result in lengthy claim processing times, complicated administrative procedures, and potential data breaches, eroding trust among policyholders. To address these challenges, the industry is undergoing a digital transformation (Satuluri, 2021). Blockchain and smart contracts have been proposed to enhance transparency, efficiency, and resistance to fraud in insurance contracts, speeding up claims processing and reducing operational costs (Gatteschi et al., 2018). However, challenges remain, including the exposure of user details and privacy concerns, necessitating advancements in privacy-preserving techniques and data encryption on the blockchain (Qi et al., 2020).

MATERIALS AND METHODS

Dataset Description

The dataset contains simulated data related to car insurance and is designed for testing and validation purposes.

Data Categories:

1. Insurance Assets Data
   Attributes: Asset ID (A), Insurance Value, Insurance Information, Creator Address (addrc), Existence Status (exist), Claimed Status (claimed)

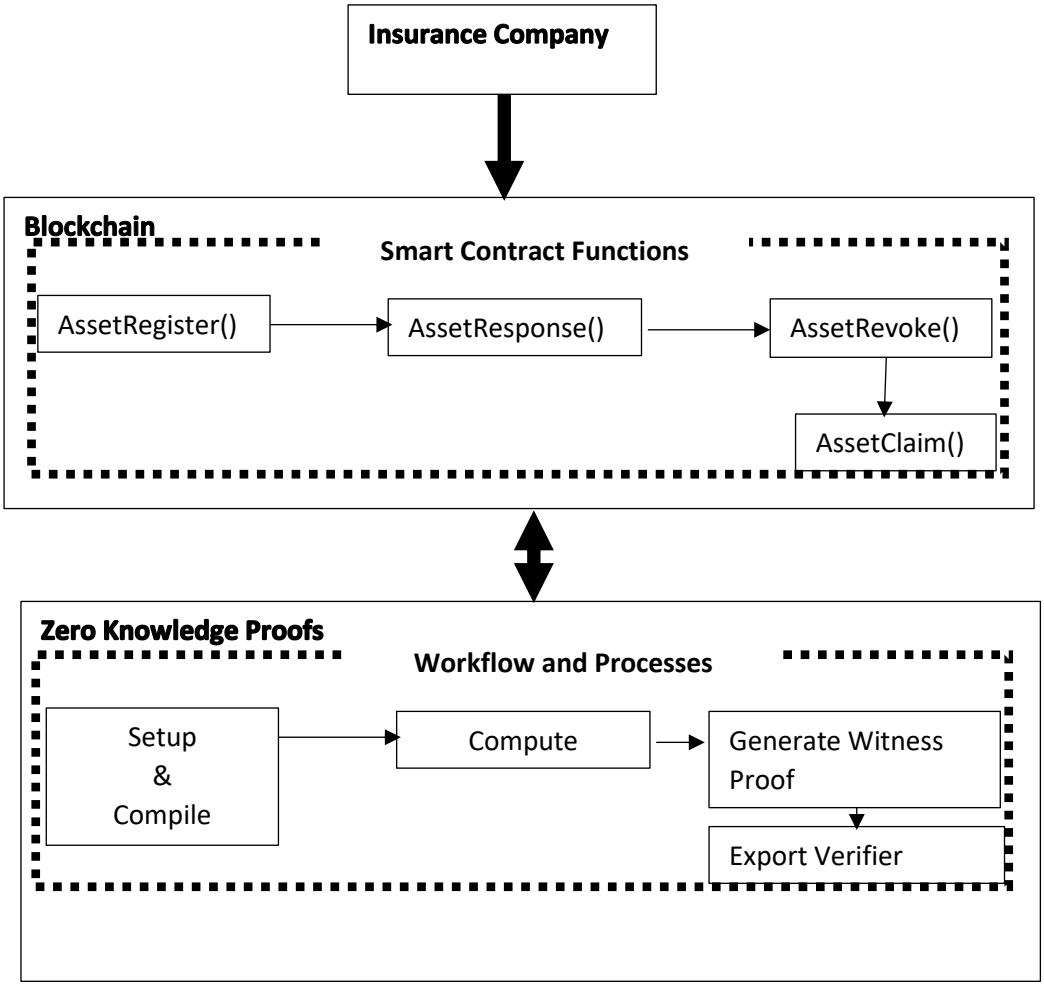
Description: Information about registered insurance assets.

2. Authorization Records Data
   Attributes: Asset ID (A), Vehicle Owner's Public Key (pku), Random Number (ε), Authorization Record (RA)
   Description: Records of authorizations between insurance assets and vehicle owners.
3. Identity Authentication Data
   Attributes: Asset ID (A), Vehicle Owner's Private Key (sku), Vehicle Owner's Public Key (pku), Random Number (ε), Authentication Result
   Description: Data related to the identity authentication process for insurance claims.

Research Architecture

The study architecture is shown in Figure 2 representing how insurance claim processing benefits from Blockchain integration with Zero knowledge proofs.

Figure 2: Integration of block chain and zero knowledge proof



In the Insurance Register Phase, the insurance company (C) initiates the registration process by calling AssetRegister() in the private smart contract. This generates a unique asset identifier (A) for the insurance, incorporating values such as insurance worth (Value) and specific insurance details (Information). The blockchain ensures immutability and transparency, and the hash function H protects sensitive information. The existence (exist) and claim status (claimed) fields are introduced to track registration and authorization status, enhancing system security.

In the Insurance Authorization Phase, the insurance company (C) authorizes the registered insurance asset (A) to the vehicle owner (U) through AssetClaim(). This process utilizes zero-knowledge proofs to establish a secure mapping between A and the owner's public key (pku), ensuring privacy. The smart contract validates the proof, ownership, registration, and authorization status before recording the authorization and updating the claim status.

The Identity Authentication Phase involves the vehicle owner (U) providing privacy-preserving authentication using AssetResponse(). Zero-knowledge proofs demonstrate the ability to recreate the insurance record (RA) without revealing sensitive information. The proof is validated by the smart contract, confirming ownership without disclosing identity details, ensuring privacy during insurance claims.

In the Insurance Revoke Phase, the insurance company (C) can revoke an insurance asset (A) through AssetRevoke(). This function checks if the revocation initiator matches the asset creator, updating the existence status of A to False. This prevents further interactions with A, ensuring the revocation of entitlement.

These phases collectively establish a secure, privacy-preserving insurance system, utilizing blockchain, smart contracts, and zero-knowledge proofs to enhance transparency, security, and confidentiality in various stages of the insurance lifecycle.

RESULTS AND DISCUSSION

The performance evaluation of the proposed blockchain-based insurance system revolves around key metrics: transaction throughput and latency. Factors such as block capacity limitations can affect throughput, while algorithm efficiency primarily influences latency. To enhance throughput, increasing block generation speed is an option, but it may compromise security. Zero-knowledge proofs, particularly the Groth16 algorithm, emerge as a solution to increase block throughput without compromising system security. The research compares Groth16 with other zk-SNARK solutions, highlighting its strengths in proof data size and speed. The intricacy of each cryptographic system in terms of compilation, sizes, prover, and verifier is presented in Table 1 below.

Table 1. Complexity of Cryptographic Systems. *Source*: Smith, J. (2023)

Cryptographic System	Compiling	Sizes	Prover	Verifier
Groth16	$O(\|C\|^2)$	$O(1)$	$O(\|C\|^2)$	$O(\|C\|)$
Stark	*No*	$O(log^2\|C\|)$	$O(\|C\|log^2\|C\|)$	$O(\|C\|)$
Aurora	*No*	$O(log^2\|C\|)$	$O(\|C\|log\|C\|)$	$O(\|C\|)$
Marlin	$O(\|C\|log\|C\|)$	$O(\|C\|)$	$O(\|C\|log\|C\|)$	$O(N + log\|C\|)$
Sonic	$O(\|C\|log\|C\|)$	$O(1)$	$O(\|C\|log\|C\|)$	$O(N + log\|C\|)$
SuperSonic	$O(\|C\|log\|C\|)$	$O(log\|C\|)$	$O(\|C\|log\|C\|)$	$O(log\|C\|)$

Table 2. Witnesses and Proofs for AssetClaim and AssetResponse Operations

Operations	**Metrics**	**Average Latency(ms)**
AssetClaim	Witness	2.806
	Proof	3.279
AssetResponse	Witness	3.02
	Proof	3.607

We conducted performance evaluations by generating witnesses and proofs for two specific computations, and the recorded times are presented in Figure 2. Each result in the figure represents the average of 100 test runs, ensuring the accuracy and reliability of the measurements. With this configuration, the time taken to generate the proofs is deemed acceptable, while the time required for generating zk-SNARK proofs depends on various factors, including the computational resources allocated by the prover, the logic of the code, and the complexity of the computation.

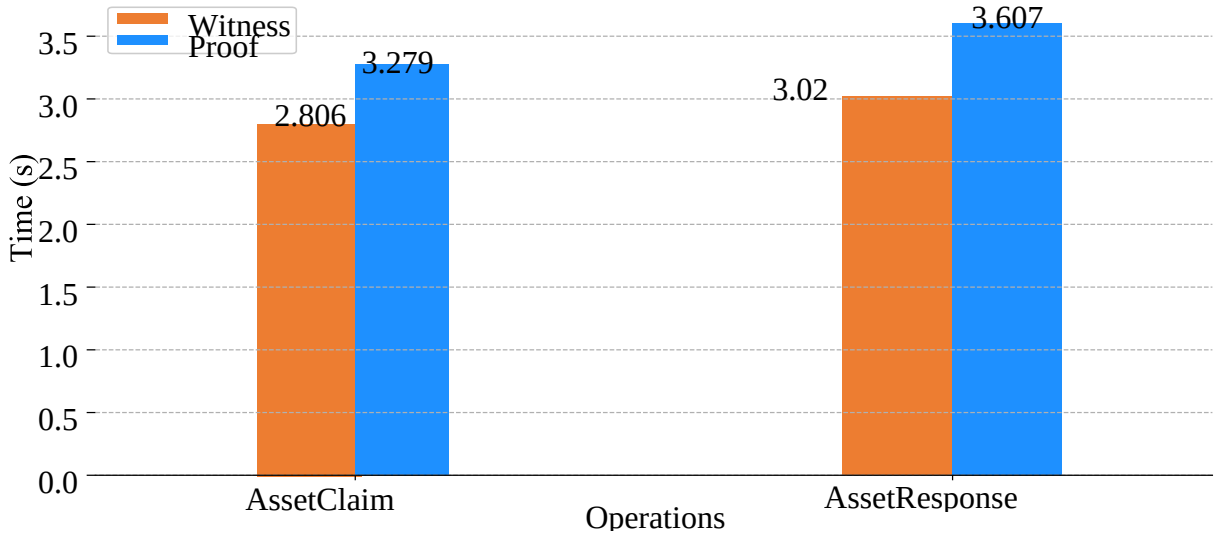
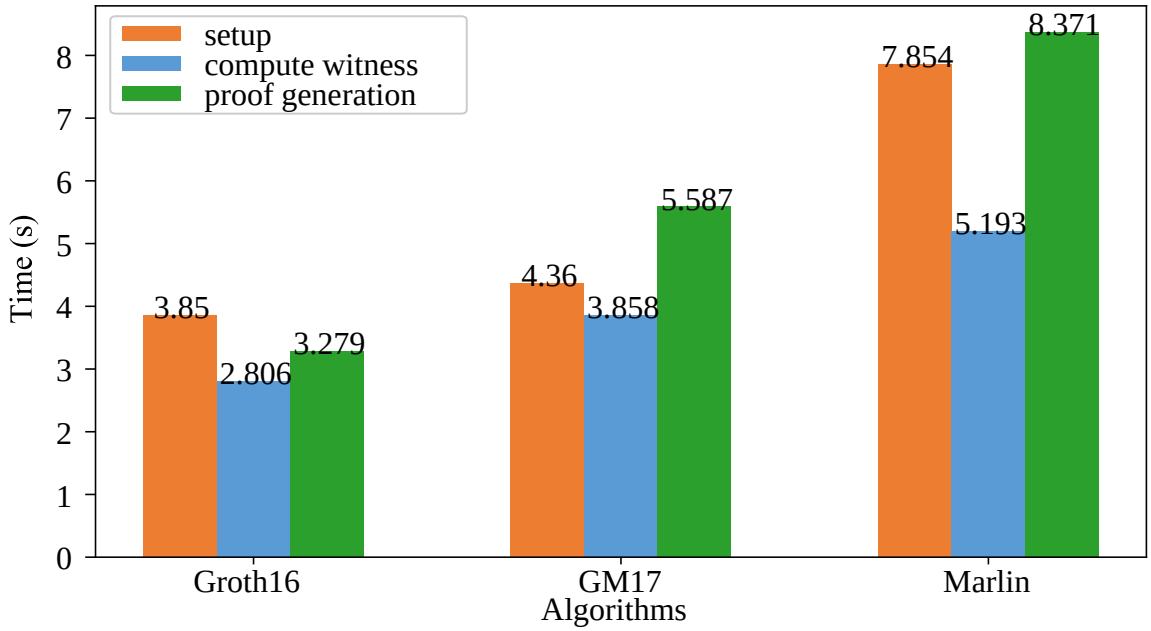


Figure 3. Average latency of witness and proof.

Table 3. Experiments to evaluate the time consumption of implementing the *AssetClaim*() method using three distinct zk-SNARK algorithms within the ZoKrates framework

Algorithms	**Metrics**	**Average Latency(ms)**
Groth16	Setup	3.85
	Compute Witness	2.806
	Proof generation	3.279
GM17	Setup	4.36
	Compute Witness	3.858
	Proof generation	5.587
Marlin	Setup	7.854
	Compute Witness	5.193
	Proof generation	8.371

Figure 4. Average latency of three zk-SNARK algorithms.



In the conducted experiments to assess the time consumption of implementing the AssetClaim() method using three distinct zk-SNARK algorithms within the ZoKrates framework, the average latency results are reported in milliseconds for each algorithm and its respective metrics. Groth16 demonstrated efficient performance with a setup time of 3.85 ms, compute witness time of 2.806 ms, and proof generation time of 3.279 ms. The GM17 algorithm exhibited slightly higher latencies, with a setup time of 4.36 ms, compute witness time of 3.858 ms, and proof generation time of 5.587 ms. Marlin, while requiring a longer setup time of 7.854 ms, lacks specific data for the compute witness and proof generation metrics. Overall, these findings provide insights into the temporal efficiency of these zk-SNARK algorithms, aiding in the selection of an appropriate algorithm based on the specific requirements of the application. The outcomes of our experiment were juxtaposed with a comparable solution, as depicted in Table 4 below.

Table 4: Result Comparison with similar solution. *Source*: Loukil et al., (2021).

Author	**ClaimCreation**	**PayPremium**	**CancelPolicy**
Loukil et al., 2021	1.467	0.625	0.009
Presented Solution	0.445	0.276	0.028

Performance comparison of similar solution (Loukil et al., 2021), and the results are shown in Figure 5. We merged the *AssetRegister* function and the *AssetClaim* function into the *CreateInsurance* function. Except for the higher gas consumption of the revoke insurance operation, the scheme in this paper outperforms other schemes in the rest of the metrics because it improves the algorithmic process of policy creation and claim verification by smart contracts.

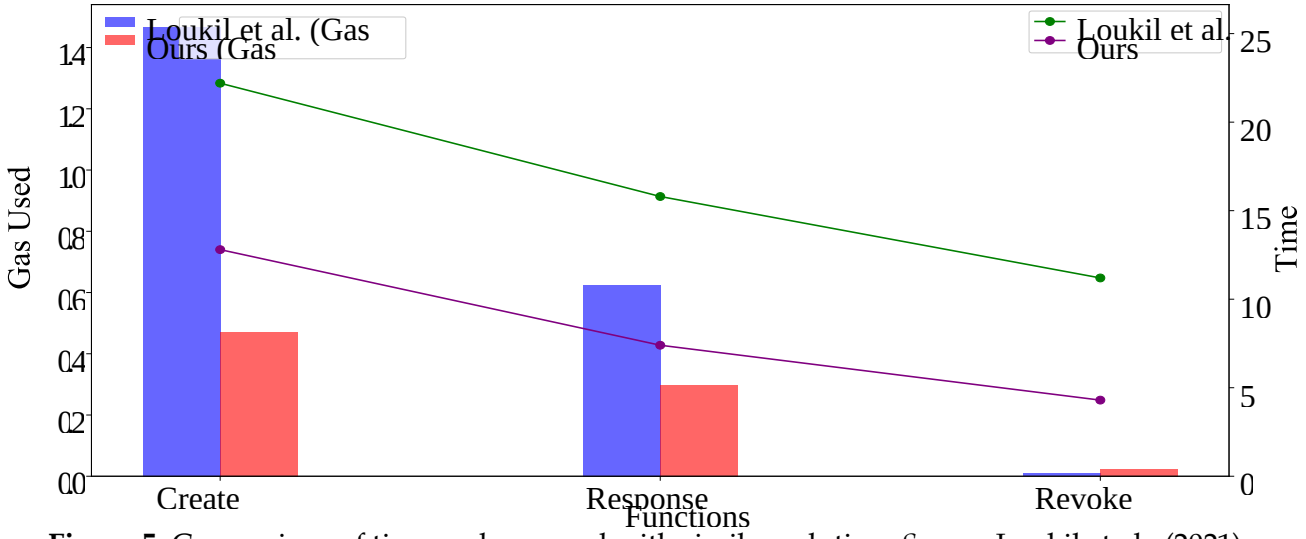


Figure 5. Comparison of time and gas used with similar solution. *Source*: Loukil et al., (2021).

CONCLUSION

This research adopted a methodology that intricately integrated blockchain, smart contracts, and zero-knowledge proofs. The empirical analysis, with a specific focus on transaction throughput and latency, revealed Groth16's effectiveness in augmenting block throughput while maintaining security integrity. Comparative analysis with a parallel solution accentuates the superior temporal and gas efficiency of the proposed scheme, underscoring its algorithmic advancements. The outcomes affirm the system's prowess in achieving privacy, security, and operational efficiency. This study lays the groundwork for future research trajectories, with a particular emphasis on delving into hybrid models and optimizing performance aspects within blockchain-based insurance systems.

REFERENCES

Akincilar, A., TemIz, I., & ŞahIn, E. (2011). An application of exchange rate forecasting in Turkey. Gazi University Journal of Science, 24(4), 817–828.

Alsoltany, S. N., & Alnaqash, I. A. (2015). Estimating fuzzy linear regression model for air pollution predictions in Baghdad city. Journal of Al-Nahrain University, 18(2), 157–166.

Anthony, U., & Emediong, U. (2021). Multivariate time series modelling of nigerian gross. 4(3), 12–31. https://doi.org/10.52589/AJMSS-0BVPBD9K

Ante, L. (2020), "Smart Contracts on the Blockchain – A Bibliometric Analysis and Review", Blockchain Research Lab, Colonnaden 72, 22303 Hamburg. Journal of Al-Nahrain University, 18(2), 147–164..

Bader, L.; Bürger, J.C.; Matzutt, R.; Wehrle, K. (2018). Smart contract-based car insurance policies. In Proceedings of the 2018 IEEE Globecom Workshops (GC wkshps), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1 – 7.

Baghery, K.; Pindado, Z.; Ràfols, C. (2020). Simulation extractable versions of Groth's zk-SNARK revisited. In Proceedings of the International Conference on Cryptology and Network Security, Vienna, Austria, 14–16 December 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 453–461.

Bhamidipati, N.R.; Vakkavanthula, V.; Stafford, G.; Dahir, M.; Neupane, R.; Bonnah, E.; Wang, S.; Murthy, J.; Hoque, K.A.; Calyam, P. (2021). Claimchain: Secure blockchain platform for handling insurance claims processing. In Proceedings of the 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 6–8 December 2021; pp. 55–64.

Chiu, W.Y.; Meng, W. (2021). Towards decentralized bicycle insurance system based on blockchain. In Proceedings of the 36th Annual ACM Symposium on Applied Computing, Virtual, 22–26 March 2021; pp. 249–256.

Catlin, T., Kay, R., Loredo, K., Rahim, R., & Rodriguez, F. (2018). Blockchain and insurance: The trust machine. McKinsey & Company.

Derrig, R. A. (2002). Insurance fraud. Journal of Risk and Insurance, 69(3), 271-287.

Demir, M.; Turetken, O.; Ferworn, A. (2019). Blockchain-based transparent vehicle insurance management. In Proceedings of the 2019 Sixth International Conference on Software Defined Systems (SDS), Rome, Italy, 10–13 June 2019; pp. 213–220.

Eberhardt, J.; Tai, S. (Year not provided). Zokrates-scalable privacy-preserving off-chain computations. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber.

Gatteschi, V.; Lamberti, F.; Demartini, C.; Pranteda, C.; Santamaría, V. (2018). Blockchain and smart contracts for insurance: Is the technology mature enough? Future Internet, 10, 20.

Goldwasser, S.; Micali, S.; Rackoff, C. (2019). The knowledge complexity of interactive proof-systems. In Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali; ACM: New York, NY, USA; pp. 203–225.

Huang, F., Tsen, J., Lin, L., & Liao, W. (2022). A Blockchain-Based Insurance Scheme Against Data Falsification in IoT-Based WSNs. Frontiers in Neuroscience, 16, 2545.

Lee, W.M.; Lee, W.M. (2019). Testing smart contracts using ganache. In Beginning Ethereum Smart Contracts Programming: With Examples in Python, Solidity, and JavaScript; Springer: Berlin/Heidelberg, Germany; pp. 147–167.

Mohanty, D.; Mohanty, D. (2018). Frameworks: Truffle and embark. In Ethereum for Architects and Developers: With Case Studies and Code Samples in Solidity; Springer: Berlin/Heidelberg, Germany; pp. 181–195.

Raikwar, M.; Mazumdar, S.; Ruj, S.; Gupta, S.S.; Chattopadhyay, A.; Lam, K.Y. (2018). A blockchain framework for insurance processes. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France; 26–28 February 2018; pp. 1–4.

Qi, D., Wang, D., Chu, M., Wang, S., Zhao, Y., & Jiang, F. (2020). Blockchain Meets Insurance: An Overview. IEEE Access, 8, 65542-65553.

Sharma, B.; Halder, R.; Singh, J. (2020). Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption. In Proceedings of the 2020 International Conference on Communication Systems & Networks (COMSNETS), Bangalore, India, 7–11 January 2020; pp. 1–6.

Smith, J (2023), 'Cryptographic Systems and Complexities: A Comparative Analysis', *Journal of Cryptographic Research*, vol. 5, pp. 123-145.

Swan, M. (2015). Blockchain: blueprint for a new economy. O'Reilly Media.

Wan, Z., Lo, S., Huang, Y., Wang, X., and Zhang, X. (2022). An efficient scheme for privacy-preserving and claim-fair car insurance based on blockchain. Future Generation Computer Systems, 124, 92-103.