International Journal of Artificial Intelegence Research
Vol 6, No 2, December 2022
ISSN: 2579-7298

Framework Authentication e-document using Blockchain Technology on the Government system

Isyak Meirobie[a,1], Agustinus Purna Irawan[b,2], Husni Teja Sukmana[c,3], Diana Putri Lazirkha[d,4*], Nuke Puji Lestari Santoso[e,5]

[a] *Tarumanagara University, Letjen S. Parman Street No. 1, Jakarta 11440, Indonesia*
[b] *Tarumanagara University, Letjen S. Parman Street No. 1, Jakarta 11440, Indonesia*
[c] *Syarif Hidayatullah State Islamic University Jakarta, Ir H. Juanda Street No.95, Cemp. Putih, Kec. Ciputat Tim., Jakrta 15412, Indonesia*
[d] *University of Raharja, Jenderal Sudirman Street No.40, RT.002 / RW.006, Cikokol, Tangerang 15117, Indonesia*
[e] *University of Raharja, Jenderal Sudirman Street No.40, RT.002 / RW.006, Cikokol, Tangerang 15117, Indonesia*
[1] *isyak.11821004@stu.untar.ac.id;* [2] *agustinus01@yahoo.com;* [3] *husniteja@uinjkt.ac.id*; [4] *diana.putri@raharja.info*;* [5]*nuke@raharja.info*

ARTICLE INFO

Article history:
Received 24 April 2022
Revised 25 May 2022
Accepted 12 June 2022

Keywords:
Blockchain
Smart Contracts
e-Document
Governance
Authentication

ABSTRACT

As a sophisticated platform, namely Blockchain, which has 3 (three) potentials to change the governance system which is still considered traditional, solve the problem of principal agents, and minimize the crime of document falsification. However, in the government sector, the documents used can be insecure and lead to document falsification. Blockchain is becoming increasingly significant in document services and beyond until questions arise about the authenticity and security of manuscripts and documents in the government sector. So, Go-Chain (Government Blockchain) it is necessary to authenticate documents using Blockchain to minimize document forgery. By utilizing the potential of Blockchain technology, this research aims to maximize government e-documents in a modern and secure manner. Propose a Blockchain-based document framework method that is applied with a literature review study—in addition to ensuring the speed of system execution by utilizing DAO (Decentralized Autonomous Organization) and Smart Contracts. The result is that modern and safe government e-documents in document verification can significantly maintain transparency and increase trust in public services.

I. Introduction

Following the development of technology and the industrial era 4.0, using Blockchain has become increasingly widespread [1]. The growing concern is especially in data security, where any threat to stability and trust is critical. This research **aims** to show how Blockchain and smart contracts can help document security in the government sector in Indonesia. **Existing problems** include a lack of security in storing all document data, a centralized system so that data does not spread in a distributed manner, deep redundancy concerns, and the presence of third parties that can interfere. Blockchain for data security, which is then synchronized with Smart Contracts and DAO, then produces an authenticated document [2].

Blockchain currently has a powerful influence in various sectors, such as the academic and government sectors [3]. This study proposes applying Blockchain technology as an e-document authentication system to record the authenticity of a data/asset [4]. Now Blockchain is overgrowing, where every activity in it is protected by cryptographic procedures that do not require the involvement of third parties in the work process [5]. Blockchain is a distributed database of consistent, node-based, and distributed transactions from a technology perspective [6]. When a new transaction is validated, it is cryptographically protected from manipulation and uses consensus techniques to promote database integrity. The existence of a Block is used to store all transactions on the Blockchain.

Transaction data is encrypted and stored in data structure blocks. Legality which states that the validity of documents is to get a signature, where documents and certificates can be obtained by someone after going through authentication [7].

Decentralized Autonomous Organization (DAO) is the most complicated type of smart contract because it can control a collection of individuals with the same interests and goals [8]. DAOs are run by governance rules with tokens defined in the application layer code. These token governance rules, both at the Blockchain and application layers, can disrupt governance by eliminating the need for human management participation [9]. Blockchains like Ethereum seek to provide a more flexible development environment than the Bitcoin Blockchain, which separates the smart contracts layer from the Blockchain layer [10]. Instead of setting all governance rules directly in the Blockchain layer, Individuals in smart contracts can now flexibly define governance rules [11] [12]. Smart Contracts only verify whether the individuals in the transactions follow the predefined rules of smart contracts. If yes, the transaction is confirmed; if not, it is rejected [13]. Only intelligent individuals create and audit and rely on the knowledge available to them at the time of coding. They lack the flexibility and access that existing institutional infrastructure can provide to deal with unforeseen events. The DAO points to the lack of dispute resolution and governance procedures for edge situations that divide communities, both at the smart contract and Ethereum blockchain levels. The inability to anticipate going from "unknown" to "known." The DAO points out that smart contracts can only be a default state that must be overturned by the majority in the relevant community if deemed necessary [14]. This research **aims** to focus on the use of blockchain against the government, which provides a way to use modern or up-to-date systems called Go-Chain (Government Blockchain) for document verification called and authentication so that the level of security is higher.

II. Research Method

The literature review research method from previous research can support creating a blockchain application framework in a government system that provides durable records protected from manipulation or loss of personal information, enabling direct provision and validation of transcripts by trusted experts and professors [15]. This provides a standardized representation of assets as a step towards a secure and decentralized method of ensuring the widespread use of this technology [16] [17].

By using Blockchain as a reliable source of truth for government data, the entire process can be automated and accelerated. Governments can upload a collection of data and documents to the Blockchain and use signatures to sign transactions [18] [19]. Signatures are freely accessible via the institute's website. Any government that wants to verify the document that the Blockchain wants to authenticate can do so by taking advantage of their digital transcript and confirming that the transaction that uploads the document to the Blockchain is signed by the government itself [20].

Instead of storing all the complete data on the Blockchain, only the SHA256 signature hash of the data is stored. This eliminates the need for massive storage while ensuring the integrity and verification of any data. The data can be downloaded so that it can be used offline. Data validity can also be validated by using Blockchain as a trusted third party [21].

Each batch of transcripts stored on the Blockchain requires one transaction. Transactions on Blockchain have a typical structure that includes the sender's public key, the recipient's public key, the amount to be sent, and the message. The sender can digitally sign the entire transaction and verify that the data was added from a valid source and time [22].

While it is feasible to issue a single transcript with a single transaction, giving a batch of transcripts with a single transaction is significantly more economical. The government can upload a pdf or word file containing government documents or certificates. The program creates a digital transcript in the form of a json file for the public. These digital transcripts can be distributed to the public via email or other means.

The public can show the hashed document to any company or institution as valid proof. The framework recalculates the Merkle root to use the Merkle route stored in the digital transcript when verifying uploading the digital transcript. Root recalculation requires a recursive sequence of operations that systematically keep nodes from leaf to root. The framework compares the computed

root with the Merkle root on the Blockchain and determines whether it is signed by a legitimate institution [23] [24].

The need for contributions is significant in building a system to run well. This research **contributes** by leveraging smart contracts and decentralized storage to authenticate document verification issues on the Blockchain after prepared documents. This results in an **impact** that will address uncontrollable risks, slow-moving systems, human intervention, and fraud. Access to transactions is required to read Blockchain data and send new transactions. All nodes on the public Blockchain can read Blockchain data and propose recent transactions. Still, only nodes registered by the central authority can read Blockchain data and offer new trades on the private Blockchain (See Table 1). The public Blockchain allows access to validation of permitted or unauthorized transactions [25]. Only pre-registered nodes can verify transactions on the official Blockchain [26].

Table 1. Blockchain Topologists

Access to Transactions	**Access to Validation Transactions**	
	Without Permission	***With Permission***
Privacy	Irrelevant	Transactions can only be viewed, delivered, and authorized by authorized nodes.
Audience	Transactions can be viewed, transmitted, and validated by any node.	Transactions can be viewed and transmitted by any node. Transactions can only be validated by authorized nodes.

Here are some basic terminology for building a system:

I. Distributed Ledger Technology

A distributed ledger is a geographically dispersed digital data set with no centralized administrator. It can also be duplicated, shared, and synced [27]. This distributed ledger securely enables data and information storage and generates decentralized digital data security.

II. Proof of Authority (PoA)

Proof of authority is a process used in Blockchain that enables fast transactions by using identification as collateral. Validators on PoA-based networks can store and validate transactions in blocks [28]. Users can gain the privilege of becoming a validator by attaching a reputation to their identity.

III. Secure Hash Algorithm-256 (SHA-256)

SHA-256 is a series of cryptographic hash algorithms developed using Merkle Damgard's structure of customized block ciphers. The SHA-256 algorithm, which is part of the SHA-2 family, is a cryptographic one-way function that converts arbitrary long inputs into a 256-bit essence. SHA-256 serves as a requirement for document authentication such as user authorization, e.g. login system security.

IV. Merkle Trees

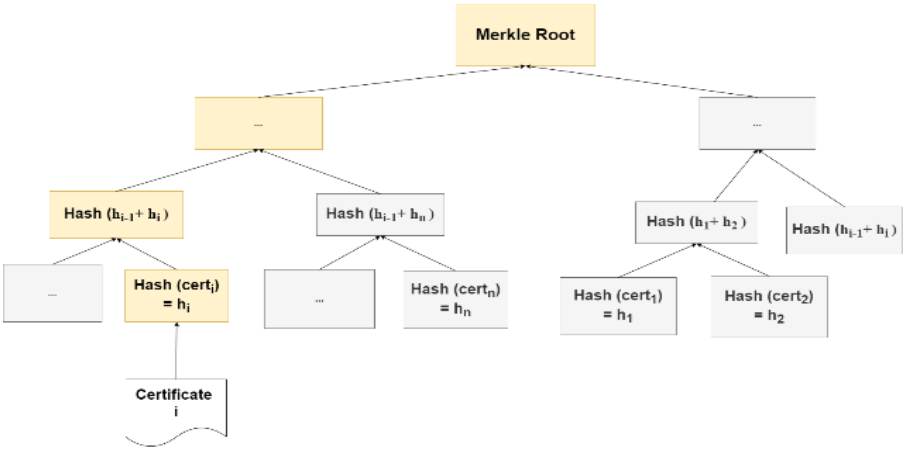

Fig. 1. Markle Trees Generation

Merkle Trees, trees in which each leaf node counts a number of hashes proportional to the logarithm of the number of leaf nodes using the hash of the node label child, provides secure verification of the contents of large data structures [29]. Merkle Tress is considered very useful because it makes savings on verification requests from many data and documents and compiling data to be easily processed [24].

V. Digital Signature Algorithm (DSA)

The equivalent elliptic curve to the Digital Signature Algorithm is the Digital Signature Algorithm (DSA). DSA generates keys and signs and validates Blockchain transactions and guarantees that only the rightful owner can control the documents [11].

III. Results and Discussion

A. Verification Layer Framework

The application layer is built with a simple and easy-to-understand user interface to avoid users being overwhelmed by the complex underlying technology.

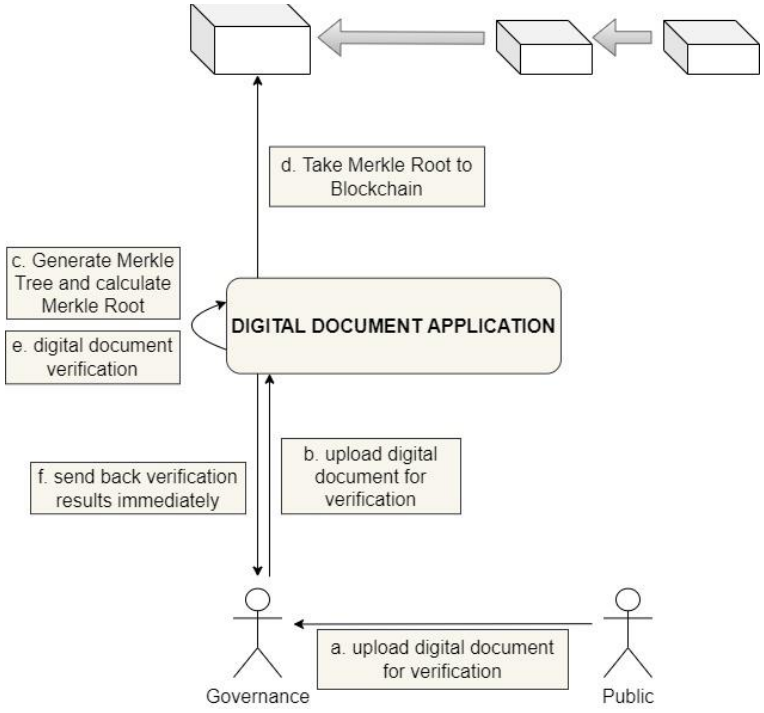

Fig. 2. Go-Chain document Verification Framework

Table 2. Algorithm Upload Data Into Blockchain

```
public function uploadfile() {
    header('Content-type: application/json');
    $user = Auth::user();
    $actionTakenBy = escape($user->fname.' '.$user->lname);
    $random = Str::random(61);
    /*
     * Check, whether IP address register is allowed in .env
     * If yes, then capture the user's IP address
     */
    if (env('REGISTER_IP_ADDRESS_IN_HISTORY') == 'Enabled') {
       $actionTakenBy .= ' ['.getUserIpAddr().']';
    }
    $data = array(
                "company" => $user->company,
                "uploaded_by" => $user->id,
                "name" => input("name"),
                "folder" => input("folder"),
                "file" => $_FILES['file'],
                "is_template" => "No",
                "source" => "form",
                "document_key" => "ABC".$random,
                "activity" => 'File uploaded by <span class="text-
primary">'.$actionTakenBy.'</span>.'
            );
    $upload = Signer::upload($data);
    if ($upload['status'] == "success") {
       exit(json_encode(responder("success", "", "","documentsCallback()", false)));
    }else{
       exit(json_encode(responder("error", "Oops!", $upload['message'])));
    }
  }
```

Table 3. Algorithm Generates Hash

```
public function save() {
    header('Content-type: application/json');
   $user = Auth::user();
    $signature = File::upload(
```

```
            input("signature"),
            "signatures",
            array(
                "source" => "base64",
                "extension" => "png"
            )
        );

        if ($signature['status'] == "success") {
            if (!empty($user->signature)) {
                File::delete($user->signature, "signatures");
            }
            Database::table(config('auth.table'))->where("id"   ,   $user->id)->update(array("signature" => $signature['info']['name']));
            exit(json_encode($response = array(
                    "status" => "success",
                    "callback"                                                                  => "signatureCallback('".url("")."uploads/signatures/".$signature['info']['name']."')",
                    "notify" => false,
                    "callbackTime" => "instant"
                )));
        }else{
            exit(json_encode(responder("error", "Oops!", "Failed to save signature please try again.")));
        }
    }


}
```

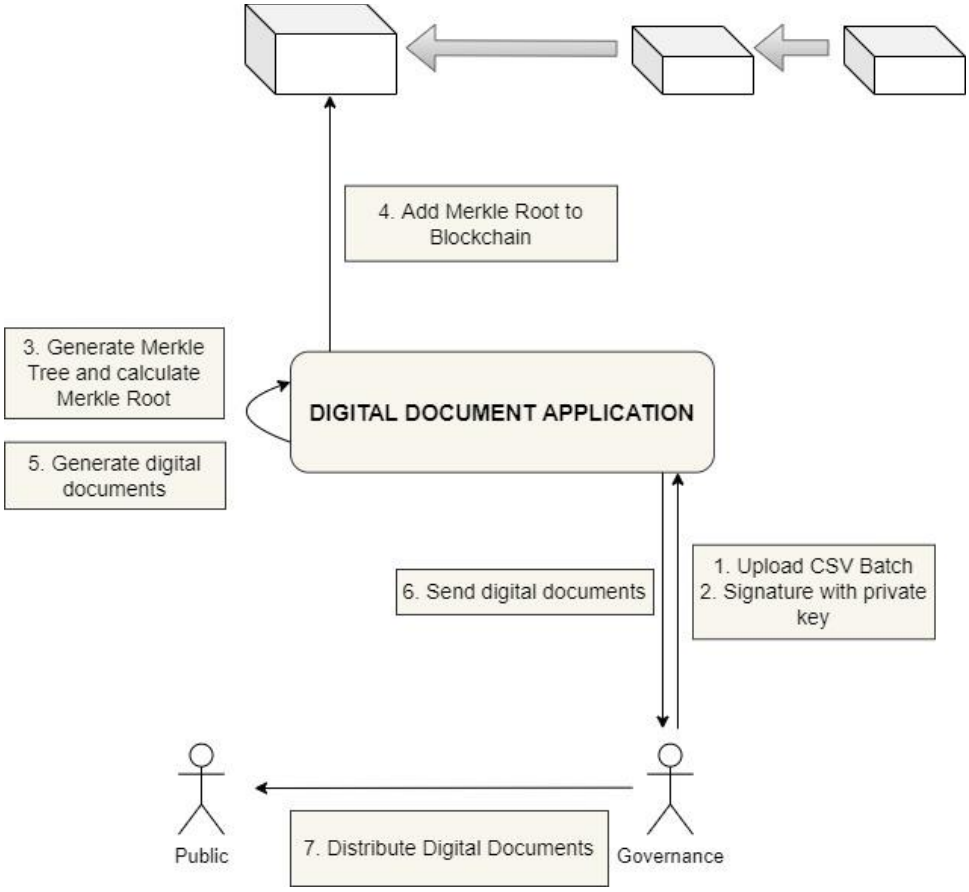

Fig. 3.Go-Chain Issuance Proposal Framework

Figure 2 (two) is presented the framework of verification of digital government documents where the public or the public will upload their digital documents to governance that will be verified through blockchain and calculated with Merkle Root. At the same time, figure 3 (three) discusses the proposed issuance of digital documents. In figure 3 (three), documents that have been calculated with Merkle Root and signed will be distributed to the public.

Application clients for all services provided are Web Applications built with HTML5, CSS3, and JavaScript (ES6). Due to its spread and ease of use, the Author chose the browser to connect with applications and Blockchain [30]. It has a smooth design. The Author also created a wallet in JavaScript to sign transactions to be uploaded to the Blockchain and validate current transactions taken from the Blockchain. JavaScript is used because signing can be done on a client without sending a private key over the network. The authors use a DSA with a P-256 curve, compatible with Go-Chain (Government Blockchain).

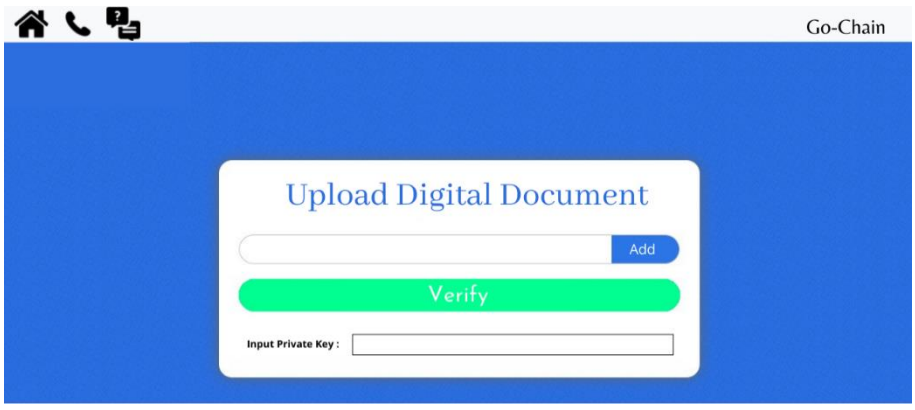

Fig. 4. *User Interface* for uploading *Batch Records* documents

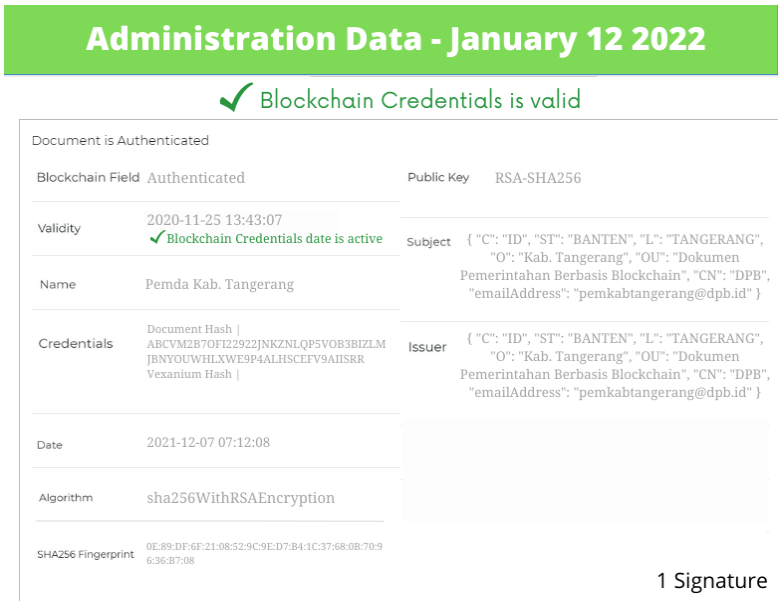

Fig. 5. Valid Document Verification View

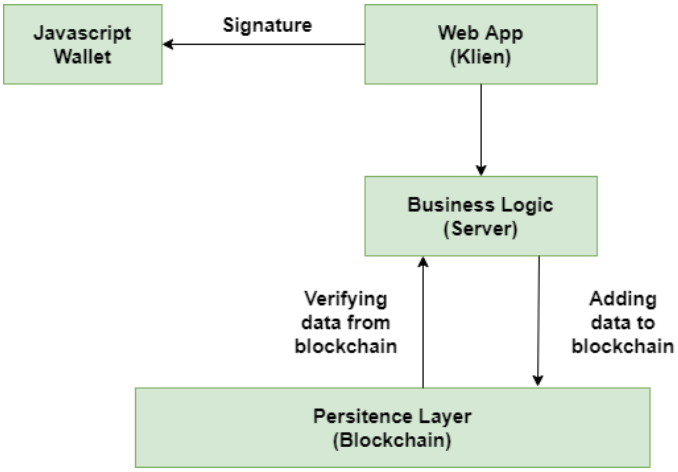

Fig. 6. Block Diagram for Go-Chain Implementation Proposal Framework

Digital documents can be verified on the Go-Chain website. Figure 4 displays the User Interface page to upload batch records documents. Data or documents can be uploaded by entering a private key. Figure 5 shows the verification view of documents that have been through the blockchain and are validly signed. Public Key, SHA265 fingerprint, and other data appear when the document is valid.

Figure 6 describes the framework of the proposed implementation of government. Data from the blockchain will go to the server and then be signed with Javascript Wallet. The server layer or Business Logic can also add data to the blockchain layer.

B. Service Layer

The author uses HTTP servers to make static files available on the internet. Python 3 (three) and the Flask framework are used to create servers, which contain business logic for data conversion and interface with Blockchain and are responsible for business logic as follows:

1. Building the Merkle Tree
2. Document process
3. Interacting with blockchain
4. Run the front end using static HTML, CSS, and JS files
5. Make REST services available for web applications for publishing and retrieving data.

C. Data Persistence Layer

Authors use a public Blockchain that without requiring permission to store transactions as an irreversible transparent notebook of records and HTTP REST to interact with the Blockchain directly from the Author's web application. The chain used one of the first Blockchains designed from the ground up for governance. An unlicensed public blockchain that uses the PoA consensus process. This is distinguished by the high transaction rate, the predictability of the time intervals at which new blocks are created, and the absence of requirements for high-performance hardware. Serialization is done in JSON, and Blockchain is possible through the HTTP REST API.

Novelty in this study is to combine blockchain technology, authentication table storage mechanisms on e-documents, and smart contracts to build a decentralized storage system called Go-Chain (Government Blockchain) in higher government systems. The study gained considerable advantages over the centralized storage systems standard regarding data storage and accessibility in the government sector.

IV. Conclusion

The problem of assets that exist today is still traditional in the government sector. One of which is in the document section that currently still does not implement good enough security. So that the government document verification system does not have security and transparency of data. Nowadays, innovation is increasingly advanced, implementing sophisticated digital so that the problem of counterfeiting can be eliminated. This research solution is to ease the burden of government performance in data verification so that data security increases and prevent state losses. Focuses on specific challenges in government areas such as security and trust in legitimately published documents. The study also discussed potential use cases for Blockchain technology in transcript verification and provided implementation for governments and many institutions. Digital platforms show a level of security that is arguably quite significant and surprising. This prompts Authors to investigate the nature of Blockchain further. After recognizing the DAO, Smart contracts and some essential technologies to build the system framework finally became a meaningful discussion of new trust and governance with the typical application of Blockchain technology in government services. **Findings** of this study are a Go-chain framework that focuses on the field of government in today's digital era. The government can safely store all document data, there will be no point of failure, redundancy concerns are deep, and no third party can interfere and profit from the author's framework.

Compared to the old methods used in Government, the newly built framework has been shown to reduce human efforts to provide lightning-fast verification results regardless of geographic location. As a result, only one system can be used by the government in document verification. The authors believe that Blockchain can be used to make systems easier for the government sector by encouraging openness, accountability, and security. Furthermore, Blockchain solutions with proof of stake and proof of work consensus algorithm approaches can outperform in the field of governance as the authors present a comprehensive Blockchain-based document verification method that allows faster insertion of blocks into the chain and also includes the capacity to cover additional use cases to develop a fully functional governance system. Finally, further research can be developed on blockchain research in other sectors.

Acknowledgment

The author would like to thank University of Raharja and Alphabet Incubator for developing research programs making this article more relevant to practice.

References

[1] U. Bodkhe *et al.*, "Blockchain for industry 4.0: A comprehensive review," *IEEE Access*, vol. 8, pp. 79764–79800, 2020.

[2] N. P. L. Santoso, Y. Durachman, S. Watini, and S. Millah, "Manajemen Kontrol Akses Berbasis Blockchain untuk Pendidikan Online Terdesentralisasi," *Technomedia Journal*, vol. 6, no. 1, pp. 111–123, 2021.

[3] A. S. Anwar, U. Rahardja, A. G. Prawiyogi, and N. P. L. Santoso, "iLearning Model Approach in Creating Blockchain Based Higher Education Trust," *International Journal of Artificial Intelligence Research*, vol. 6, no. 1, 2022.

[4] R. F. Nevizond, U. Rahardja, N. P. L. Santoso, S. Purnama, and W. Y. Prihastiwi, "Collaboration Blockchain Technology and Gamification in iLearning systems," *Scientific Journal of Informatics*, vol. 8, no. 2, pp. 213–221, 2021.

[5] M. Hardini, Q. Aini, U. Rahardja, R. D. Izzaty, and A. Faturahman, "Ontology of Education Using Blockchain: Time Based Protocol," 2020. doi: 10.1109/ICORIS50180.2020.9320807.

[6] A. K. Sharma, D. M. Sharma, N. Purohit, S. A. Sharma, and A. Khan, "Blockchain Technology," *Blockchain Technology*, pp. 163–180, Feb. 2022, doi: 10.1201/9781003138082-10.

[7] A. Pambudi, S. Purnama, T. Ayuninggati, N. P. L. Santoso, and A. Oktariyani, "Legality On Digital Document Using Blockchain Technology: An Exhaustive Study," in *2021 Sixth International Conference on Informatics and Computing (ICIC)*, 2021, pp. 1–6.

[8] U. Rahardja, S. Kosasi, E. P. Harahap, and Q. Aini, "Authenticity of a Diploma Using the Blockchain Approach," *International Journal*, vol. 9, no. 1.2, 2020.

[9] U. Rahardja, A. N. Hidayanto, T. Hariguna, and Q. Aini, "Design Framework on Tertiary Education System in Indonesia Using Blockchain Technology," *2019 7th International Conference on Cyber and IT Service Management, CITSM 2019*, pp. 5–8, 2019, doi: 10.1109/CITSM47753.2019.8965380.

[10] U. Rahardja, Q. Aini, M. D. A. Ngadi, M. Hardini, and F. P. Oganda, "The Blockchain Manifesto," 2020. doi: 10.1109/ICORIS50180.2020.9320798.

[11] M. Rakhmansyah, U. Rahardja, N. P. L. Santoso, A. Khoirunisa, and A. Faturahman, "Smart Digital Signature berbasis Blockchain pada Pendidikan Tinggi menggunakan Metode SWOT," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 2, no. 1, pp. 39–47, 2021.

[12] R. Ekawati, Y. Arkeman, S. Suprihatinr, and S. Suprihatinr, "Smart Contract Blockchain Application Design Based on The Distribution of Product Return Transaction Data," *International Journal of Artificial Intelligence Research*, vol. 6, no. 2, Dec. 2021, doi: 10.29099/IJAIR.V6I1.263.

[13] L. Honesti, Q. Aini, M. I. Setiawan, N. P. L. Santoso, and W. Y. Prihastiwi, "Smart Contract-based Gamification Scheme for College in Higher Education," *APTISI Transactions on Management (ATM)*, vol. 6, no. 2, pp. 102–111, 2022.

[14] I. K. Gunawan, N. Lutfiani, Q. Aini, F. M. Suryaman, and A. Sunarya, "Smart Contract Innovation and Blockchain-Based Tokenization in Higher Education," *Journal of Education Technology*, vol. 5, no. 4, pp. 636–644, 2021.

[15] J. C. Farah, A. Vozniuk, M. J. Rodríguez-Triana, and D. Gillet, "A blueprint for a blockchain-based architecture to power a distributed network of tamper-evident learning trace repositories," in *2018 IEEE 18th International Conference on Advanced Learning Technologies (ICALT)*, 2018, pp. 218–222.

[16] E. E. Bessa and J. S. B. Martins, "A blockchain-based educational record repository," *arXiv preprint arXiv:1904.00315*, 2019.

[17] L. Meria, Q. Aini, N. P. L. Santoso, U. Raharja, and S. Millah, "Management of Access Control for Decentralized Online Educations using Blockchain Technology," in *2021 Sixth International Conference on Informatics and Computing (ICIC)*, 2021, pp. 1–6.

[18] U. Rahardja, M. Hardini, A. L. al Nasir, and Q. Aini, "Taekwondo Sports Test and Training Data Management Using Blockchain," in *2020 Fifth International Conference on Informatics and Computing (ICIC)*, 2020, pp. 1–6.

[19] I. Sudirman, I. Sunaryo, A. Aisha, J. Monang, and I. R. Prasetyo, "A Website-based Information System Design of SME Development Facilitation Registration," *INTENSIF: Jurnal Ilmiah Penelitian dan Penerapan Teknologi Sistem Informasi*, vol. 5, no. 2, pp. 218–233, 2021.

[20] H. Nusantoro, R. Supriati, N. Azizah, N. P. L. Santoso, and S. Maulana, "Blockchain Based Authentication for Identity Management," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–8.

[21] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain as a notarization service for data sharing with personal data store," in *2018 17th ieee international conference on trust, security and privacy in computing and communications/12th ieee international conference on big data science and engineering (TrustCom/BigDataSE)*, 2018, pp. 1330–1335.

[22] M. Wang, M. Duan, and J. Zhu, "Research on the security criteria of hash functions in the blockchain," in *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, 2018, pp. 47–55.

[23] D. Ahmad, N. Lutfiani, A. D. A. R. Ahmad, U. Rahardja, and Q. Aini, "Blockchain Technology Immutability Framework Design in E-Government," *Jurnal Administrasi Publik: Public Administration Journal*, vol. 11, no. 1, pp. 32–41, 2021.

[24] A. G. Prawiyogi, R. Rahman, A. Sastromiharjo, S. Sulistiawati, and Q. Aini, "Ontologi Blockchain Pada Karya Tulis Puisi Di Pendidikan Sekolah Dasar: Metode Merkle Root," *CSRID (Computer Science Research and Its Development Journal)*, vol. 13, no. 1, pp. 23–33, 2021.

[25] U. Rahardja, Q. Aini, A. Khairunisa, and S. Millah, "Implementation of Blockchain Technology in Learning Management System (LMS)," *APTISI Transactions on Management (ATM)*, vol. 6, no. 2, pp. 112–120, 2022.

[26] R. Yuan, X. Yu-Bin, H.-B. Chen, Z. Bin-Yu, and J. Xie, "Shadoweth: Private smart contract on public blockchain," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 542–556, 2018.

[27] U. Rahardja, Q. Aini, F. P. Oganda, and V. T. Devana, "Secure Framework Based on Blockchain for E-Learning During COVID-19," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*, 2021, pp. 1–7.

[28] P. K. Singh, R. Singh, S. K. Nandi, and S. Nandi, "Managing smart home appliances with proof of authority and blockchain," in *International Conference on Innovations for Community Services*, 2019, pp. 221–232.

[29] D. Lee and N. Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree," *Multimedia Tools and Applications*, vol. 80, no. 26, pp. 34517–34534, 2021.

[30] W. Setyowati, U. Rahardja, Q. Aini, N. P. L. Santoso, and W. Y. Prihastiwi, "DESIGN FINANCIAL ACCOUNTING USING BLOCKCHAIN APPROACH IN EDUCATION," *Media Riset Akuntansi, Auditing & Informasi*, vol. 21, no. 2, pp. 161–174, 2021.