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

**RESUME**

En tant que plateforme sophistiquée, à savoir Blockchain, qui a 3 (trois) potentiels pour changer le système de gouvernance qui est toujours considéré comme traditionnel, résoudre le problème des agents principaux, et minimiser le crime de falsification de documents. Cependant, dans le secteur gouvernemental, les documents utilisés peuvent être peu sûrs et conduire à la falsification de documents. La blockchain prend de plus en plus d'importance dans les services documentaires et au-delà, jusqu'à ce que des questions se posent sur l'authenticité et la sécurité des manuscrits et des documents dans le secteur gouvernemental. Il est donc nécessaire d'authentifier les documents à l'aide de la Blockchain afin de minimiser la falsification des documents. En utilisant le potentiel de la technologie Blockchain, cette recherche vise à maximiser les documents électroniques du gouvernement d'une manière moderne et sécurisée. Proposer une méthode d'encadrement des documents basée sur la blockchain qui est appliquée avec une étude de la littérature - en plus de garantir la vitesse d'exécution du système en utilisant DAO (Decentralized Autonomous Organization) et des contrats intelligents (Smart Contracts). Le résultat est que les documents électroniques modernes et sûrs du gouvernement dans la vérification des documents peuvent considérablement maintenir la transparence et augmenter la confiance dans les services publics.

1. **Introduction**

Suite au développement de la technologie et de l'ère industrielle 4.0, l'utilisation de la blockchain est de plus en plus répandue [1]. L'inquiétude croissante concerne surtout la sécurité des données, où toute menace pour la stabilité et la confiance est critique. Cette recherche vise à montrer comment la blockchain et les contrats intelligents peuvent contribuer à la sécurité des documents dans le secteur gouvernemental en Indonésie. Les problèmes existants comprennent un manque de sécurité dans le stockage de toutes les données des documents, un système centralisé afin que les données ne se propagent pas de manière distribuée, des problèmes de redondance profonde et la présence de tierces parties qui peuvent interférer. La blockchain pour la sécurité des données, qui est ensuite synchronisée avec les Smart Contracts et les DAO, produit alors un document authentifié [2]. La blockchain exerce actuellement une forte influence dans divers secteurs, tels que les secteurs universitaire et gouvernemental [3]. Cette étude propose d'appliquer la technologie Blockchain en tant que système d'authentification de documents électroniques pour enregistrer l'authenticité d'une donnée ou d'un bien [4]. Aujourd'hui, la blockchain est en pleine expansion, chaque activité y étant protégée par des procédures cryptographiques qui ne nécessitent pas l'implication de tiers dans le processus de travail [5]. Du point de vue technologique, la blockchain est une base de données distribuée de transactions cohérentes, basées sur des nœuds et distribuées [6]. Lorsqu'une nouvelle transaction est validée, elle est protégée par cryptographie contre toute manipulation et utilise des techniques de consensus pour promouvoir l'intégrité de la base de données. L'existence d'un bloc est utilisée pour stocker toutes les transactions sur la blockchain.

Les données de transaction sont cryptées et stockées dans des blocs de structure de données. La légalité qui stipule que la validité des documents est d'obtenir une signature, où les documents et les certificats peuvent être obtenus par quelqu'un après avoir passé par l'authentification [7]. L'organisation autonome décentralisée (DAO) est le type de contrat intelligent le plus complexe, car elle peut contrôler un ensemble d'individus ayant les mêmes intérêts et les mêmes objectifs [8]. Les DAO sont gérées par des règles de gouvernance avec des jetons définis dans le code de la couche d'application. Ces règles de gouvernance par jetons, tant au niveau de la Blockchain que des couches applicatives, peuvent perturber la gouvernance en éliminant la nécessité d'une participation humaine à la gestion [9]. Les blockchains comme Ethereum cherchent à fournir un environnement de développement plus flexible que la blockchain Bitcoin, qui sépare la couche des contrats intelligents de la couche de la blockchain [10]. Au lieu de définir toutes les règles de gouvernance directement dans la couche Blockchain, les individus dans les contrats intelligents peuvent maintenant définir les règles de gouvernance de manière flexible [11] [12]. Les contrats intelligents vérifient uniquement si les individus participant aux transactions suivent les règles prédéfinies des contrats intelligents. Dans l'affirmative, la transaction est confirmée ; dans le cas contraire, elle est rejetée [13]. Seuls les individus intelligents créent et vérifient et s'appuient sur les connaissances dont ils disposent au moment du codage. Ils n'ont pas la flexibilité et l'accès que l'infrastructure institutionnelle existante peut fournir pour faire face aux événements imprévus. La DAO souligne l'absence de procédures de résolution des litiges et de gouvernance pour les situations délicates qui divisent les communautés, tant au niveau du contrat intelligent que de la blockchain Ethereum. L'incapacité à anticiper le passage de « l'inconnu » au « connu ». La DAO souligne que les contrats intelligents ne peuvent être qu'un état par défaut qui doit être renversé par la majorité de la communauté concernée si cela est jugé nécessaire [14]. Cette recherche vise à se concentrer sur l'utilisation de la blockchain contre le gouvernement, qui fournit un moyen d'utiliser des systèmes modernes ou à jour appelés Go-Chain (Blockchain du gouvernement) pour la vérification des documents appelés et l'authentification, de sorte que le niveau de sécurité est plus élevé.

1. **Méthode de recherche**

La méthode de recherche de l'analyse documentaire des recherches précédentes peut soutenir la création d'un cadre d'application de la blockchain dans un système gouvernemental qui fournit des enregistrements durables protégés contre la manipulation ou la perte d'informations personnelles, permettant la fourniture directe et la validation des transcriptions par des experts et des professeurs de confiance [15]. Cela fournit une représentation normalisée des actifs comme une étape vers une méthode sécurisée et décentralisée pour assurer l'utilisation généralisée de cette technologie [16] [17]. En utilisant la blockchain comme source de vérité fiable pour les données gouvernementales, l'ensemble du processus peut être automatisé et accéléré. Les gouvernements peuvent télécharger une collection de données et de documents sur la Blockchain et utiliser des signatures pour signer les transactions [18] [19]. Les signatures sont librement accessibles via le site web de l'institut. Tout gouvernement qui souhaite vérifier le document que la blockchain veut authentifier peut le faire en profitant de sa transcription numérique et en confirmant que la transaction qui télécharge le document dans la blockchain est signée par le gouvernement lui-même [20]. Au lieu de stocker toutes les données complètes sur la blockchain, seul le hachage de la signature SHA256 des données est stocké. Cela élimine la nécessité d'un stockage massif tout en garantissant l'intégrité et la vérification de toutes les données. Les données peuvent être téléchargées afin d'être utilisées hors ligne. La validité des données peut également être validée en utilisant la blockchain comme tiers de confiance [21]. Chaque lot de transcriptions stocké sur la Blockchain nécessite une transaction. Les transactions sur la Blockchain ont une structure typique qui comprend la clé publique de l'expéditeur, la clé publique du destinataire, le montant à envoyer et le message. L'expéditeur peut signer numériquement l'ensemble de la transaction et vérifier que les données ont été ajoutées à partir d'une source et d'une date valides [22].

S'il est possible de délivrer une seule transcription en une seule opération, il est nettement plus économique de délivrer un lot de transcriptions en une seule opération.

Le gouvernement peut télécharger un fichier pdf ou word contenant des documents ou des certificats gouvernementaux. Le programme crée une transcription numérique sous la forme d'un fichier sous la forme d'un fichier json pour le public. Ces transcriptions numériques peuvent être distribuées au public par courrier électronique ou par d'autres moyens.

Le public peut présenter le document haché à toute entreprise ou institution comme preuve valable.

Le cadre recalcule la racine de Merkle pour utiliser la route de Merkle stockée dans la transcription numérique lors de la vérification du téléchargement de la transcription numérique.

Le recalcul de la racine nécessite une séquence récursive d'opérations qui conservent systématiquement les nœuds de la feuille à la racine. Le cadre compare la racine calculée avec la racine de Merkle sur la Blockchain et détermine si elle est signée par une institution légitime [23] [24].

Le besoin de contributions est important dans la construction d'un système qui fonctionne bien. Cette recherche contribue

en tirant parti des contrats intelligents et du stockage décentralisé pour authentifier les problèmes de vérification des documents sur la Blockchain après les documents préparés.

sur la Blockchain après la préparation des documents. Il en résulte un impact qui traitera les risques incontrôlables, les systèmes lents, les problèmes humains et les problèmes de sécurité.

les risques incontrôlables, les systèmes lents, l'intervention humaine et la fraude. L'accès aux transactions est nécessaire pour lire les données de la blockchain et envoyer de nouvelles transactions.

L'accès aux transactions est nécessaire pour lire les données de la blockchain et envoyer de nouvelles transactions. Tous les nœuds de la blockchain publique peuvent lire les données de la blockchain et proposer des transactions récentes. Cependant, seuls les nœuds enregistrés dans la Blockchain publique peuvent lire les données de la Blockchain et proposer des transactions récentes.

Voici quelques termes de base pour la construction d'un système :

**I. Technologie du grand livre distribué**

Un grand livre distribué est un ensemble de données numériques géographiquement dispersées sans administrateur centralisé.

Il peut également être dupliqué, partagé et synchronisé [27]. Ce grand livre distribué

permet de stocker des données et des informations en toute sécurité et de générer des données numériques décentralisées.

**II. Preuve d'autorité (PoA)**

La preuve d'autorité est un processus utilisé dans la blockchain qui permet des transactions rapides en utilisant l'identification comme garantie.

Les validateurs des réseaux basés sur la preuve d'autorité peuvent stocker et valider les transactions dans les blocs [28].

Les utilisateurs peuvent obtenir le privilège de devenir un validateur en attachant une réputation à leur identité.

**III. Algorithme de hachage sécurisé-256 (SHA-256)**

SHA-256 est une série d'algorithmes de hachage cryptographique développés à partir de la structure de Merkle Damgard de chiffrement par bloc personnalisé. L'algorithme SHA-256, qui fait partie de la famille SHA-2 est une fonction cryptographique à sens unique qui convertit des entrées longues arbitraires en une essence de 256 bits.

SHA-256 est nécessaire pour l'authentification de documents tels que l'autorisation de l'utilisateur, par exemple le système de connexion.

**IV. Arbres de Merkle**

Les arbres de Merkle, arbres dans lesquels chaque nœud feuille compte un nombre de hachages proportionnel au logarithme du nombre de nœuds feuilles en utilisant le hachage de l'enfant de l'étiquette du nœud.

L'étiquette du nœud enfant permet de vérifier en toute sécurité le contenu de grandes structures de données [29]. Merkle Tress est considéré comme très utile car elle permet de réaliser des économies sur les demandes de vérification à partir de nombreux documents et données et de compiler les données pour les traiter facilement [29].

**V. Algorithme de signature numérique (ASN)**

La courbe elliptique équivalente à l'algorithme de signature numérique est l'algorithme de signature numérique (DSA).

Algorithme de signature numérique (DSA). L'ASN génère des clés, signe et valide les transactions de la blockchain et garantit que seul le propriétaire légitime peut accéder à la blockchain.

garantit que seul le propriétaire légitime peut contrôler les documents [11].

**III. Results and Discussion**

1. **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

La figure 2 (deux) présente le cadre de vérification des documents numériques du gouvernement où

le public télécharge ses documents numériques à la gouvernance qui seront vérifiés par la blockchain et calculés avec la racine de Merkle.

blockchain et calculés avec la racine Merkle. Dans le même temps, la figure 3 (trois) traite de la proposition de délivrance de documents numériques.

de la délivrance de documents numériques. Dans la figure 3 (trois), les documents qui ont été calculés avec la racine

Merkle Root et signés seront distribués au public.

Les clients d'application pour tous les services fournis sont des applications web construites avec HTML5, CSS3 et JavaScript (ES6).

JavaScript (ES6). En raison de sa diffusion et de sa facilité d'utilisation, l'auteur a choisi le navigateur pour se connecter aux applications et à la blockchain [30].

Il a un design fluide. L'auteur a également créé un portefeuille en JavaScript pour signer les transactions à télécharger sur la Blockchain et valider les transactions actuelles extraites de la Blockchain.

extraites de la blockchain. JavaScript est utilisé parce que la signature peut être effectuée sur un client sans envoyer de clé privée sur le réseau.

sans envoyer de clé privée sur le réseau. Les auteurs utilisent un DSA avec une courbe P-256, compatible avec

Go-Chain (Blockchain gouvernementale).

Les documents numériques peuvent être vérifiés sur le site web de Go-Chain. La figure 4 présente la page de l'interface utilisateur

pour télécharger des documents d'enregistrement de lots. Les données ou les documents peuvent être téléchargés en saisissant une clé privée.

privée. La figure 5 montre la vue de vérification des documents qui sont passés par la blockchain et sont

sont valablement signés. La clé publique, l'empreinte SHA265 et d'autres données apparaissent lorsque le document est valide.

valide.

La figure 6 décrit le cadre de la mise en œuvre proposée pour le gouvernement. Les données de la

blockchain seront envoyées au serveur, puis signées avec Javascript Wallet. La couche serveur ou

Business Logic peut également ajouter des données à la couche blockchain.

**B. Couche service**

L'auteur utilise des serveurs HTTP pour mettre des fichiers statiques à disposition sur l'internet. Python 3 (trois) et

le framework Flask sont utilisés pour créer des serveurs, qui contiennent la logique commerciale pour la conversion des données et l'interface avec la blockchain.

L'interface avec la blockchain est responsable de la logique commerciale comme suit :

1. Construction de l'arbre de Merkle

2. Processus de document

3. Interaction avec la blockchain

4. Exécuter le front-end en utilisant des fichiers HTML, CSS et JS statiques

5. Mettre les services REST à la disposition des applications web pour la publication et la récupération de données.

**C. Couche de persistance des données**

Les auteurs utilisent une blockchain publique qui, sans nécessiter d'autorisation, stocke les transactions sous la forme d'un carnet transparent irréversible d'enregistrements et de services REST HTTP.

comme un carnet de notes transparent irréversible et HTTP REST pour interagir avec la blockchain directement depuis l'application web de l'auteur.

directement à partir de l'application web de l'auteur. La chaîne a utilisé l'une des premières Blockchains conçues dès le départ pour la gouvernance.

conçue dès le départ pour la gouvernance. Il s'agit d'une blockchain publique sans licence qui utilise le processus de consensus PoA. Cette blockchain

se distingue par un taux de transaction élevé, la prévisibilité des intervalles de temps au cours desquels de nouveaux blocs sont créés, et l'absence d'exigences en matière de transparence.

sont créés, et l'absence d'exigences en matière de matériel de haute performance. La sérialisation se fait en

JSON, et la blockchain est possible via l'API HTTP REST.

La nouveauté de cette étude est de combiner la technologie blockchain, les mécanismes de stockage de table d'authentification

d'authentification sur les documents électroniques et les contrats intelligents pour construire un système de stockage décentralisé appelé GoChain (Government Blockchain) dans les systèmes gouvernementaux supérieurs. L'étude a permis d'obtenir des avantages considérables

avantages considérables par rapport à la norme des systèmes de stockage centralisés en ce qui concerne le stockage et l'accessibilité des données dans le secteur gouvernemental.

dans le secteur gouvernemental.

**IV. Conclusion**

Le problème des actifs qui existent aujourd'hui est toujours traditionnel dans le secteur gouvernemental. L'un d'entre eux est

dans la section des documents qui, à l'heure actuelle, ne met toujours pas en œuvre une sécurité suffisante. Ainsi, le système de vérification des documents du gouvernement ne dispose pas de la sécurité et de la transparence des données.

système de vérification des documents gouvernementaux ne dispose pas de la sécurité et de la transparence des données. Aujourd'hui, l'innovation est de plus en plus avancée,

l'innovation est de plus en plus avancée, mettant en œuvre des systèmes numériques sophistiqués afin que le problème de la

de la contrefaçon. Cette solution de recherche vise à alléger le fardeau de l'administration

Cette solution de recherche consiste à alléger le fardeau de la performance du gouvernement en matière de vérification des données afin d'accroître la sécurité des données et d'éviter les pertes pour l'État. Elle se concentre sur

des défis spécifiques dans les domaines gouvernementaux tels que la sécurité et la confiance dans les documents légitimement publiés.

légitimement publiés. L'étude a également examiné les cas d'utilisation potentiels de la technologie Blockchain dans la transcription.

et a fourni une mise en œuvre pour les gouvernements et de nombreuses institutions. Les plateformes numériques

présentent un niveau de sécurité qui est sans doute assez important et surprenant. Cela incite les auteurs à

à approfondir la nature de la blockchain. Après avoir reconnu la DAO, les contrats intelligents et certaines technologies essentielles, les auteurs ont décidé de se pencher sur la nature de la blockchain.

techniques essentielles

Par rapport aux anciennes méthodes utilisées dans l'administration, il a été démontré que le nouveau cadre permettait de

réduire les efforts humains et fournir des résultats de vérification rapides comme l'éclair, quelle que soit la situation géographique.

Par conséquent, un seul système peut être utilisé par le gouvernement pour la vérification des documents. Les auteurs

Les auteurs pensent que la blockchain peut être utilisée pour faciliter les systèmes pour le secteur gouvernemental en encourageant l'ouverture, la responsabilité et la sécurité.

en encourageant l'ouverture, la responsabilité et la sécurité. En outre, les solutions Blockchain avec les approches d'algorithmes de consensus proof of stake et proof of work peuvent être utilisées pour faciliter le processus de vérification des documents.

de la preuve de l'enjeu et de la preuve du travail peuvent être plus performantes dans le domaine de la gouvernance.

les auteurs présentent une méthode complète de vérification des documents basée sur la blockchain qui permet d'accélérer l'insertion des blocs dans la chaîne et d'améliorer la sécurité.

l'insertion plus rapide de blocs dans la chaîne et qui inclut également la capacité de couvrir des cas d'utilisation supplémentaires pour développer un système de gouvernance entièrement fonctionnel.

pour développer un système de gouvernance pleinement fonctionnel. Enfin, d'autres recherches peuvent être menées sur la blockchain

dans d'autres secteurs.

Resume technique :

1. **Verification Layer Framework**

La couche applicative est construite avec une interface utilisateur simple et facile à comprendre pour éviter que les utilisateurs ne soient submergés par la technologie sous-jacente complexe.

La figure 2 (deux) présente le cadre de vérification des documents gouvernementaux numériques où le public ou le public téléchargera ses documents numériques sur la gouvernance qui seront vérifiés via la blockchain et calculés avec Merkle Root. En même temps, la figure 3 (trois) discute de la délivrance proposée de documents numériques. Dans la figure 3 (trois), les documents qui ont été calculés avec Merkle Root et signés seront distribués au public.

Les clients d'application pour tous les services fournis sont des applications Web construites avec HTML5, CSS3 et JavaScript (ES6). En raison de sa diffusion et de sa facilité d'utilisation, l'auteur a choisi le navigateur pour se connecter aux applications et à la Blockchain [30]. Il a une conception fluide. L'auteur a également créé un portefeuille en JavaScript pour signer les transactions à télécharger sur la Blockchain et valider les transactions en cours extraites de la Blockchain. JavaScript est utilisé car la signature peut être effectuée sur un client sans envoyer de clé privée sur le réseau. Les auteurs utilisent un DSA avec une courbe P-256, compatible avec Go-Chain (Government Blockchain).

Les documents numériques peuvent être vérifiés sur le site Web de Go-Chain. La figure 4 affiche la page d'interface utilisateur pour télécharger des documents d'enregistrement par lots. Les données ou les documents peuvent être téléchargés en saisissant une clé privée. La figure 5 montre la vue de vérification des documents qui ont traversé la blockchain et sont validement signés. La clé publique, l'empreinte digitale SHA265 et d'autres données apparaissent lorsque le document est valide.

La figure 6 décrit le cadre de la mise en œuvre proposée du gouvernement. Les données de la blockchain seront envoyées au serveur puis signées avec JavaScript Wallet. La couche serveur ou Business Logic peut également ajouter des données à la couche blockchain.

1. **Service Layer**

L'auteur utilise des serveurs HTTP pour rendre les fichiers statiques disponibles sur Internet. Python 3 (trois) et le framework Flask sont utilisés pour créer des serveurs, qui contiennent la logique métier pour la conversion des données et l'interface avec la Blockchain et sont responsables de la logique métier comme suit :

1. construction de l'arbre de Merkle
2. processus de documentation
3. interaction avec la blockchain
4. exécution du front-end à l'aide de fichiers HTML, CSS et JS statiques
5. rendre les services REST disponibles pour les applications Web pour la publication et la récupération de données.
6. **Data Persistence Layer**

Les auteurs utilisent une blockchain publique qui, sans nécessiter d'autorisation, stocke les transactions sous forme de carnet d'enregistrements transparent et irréversible et HTTP REST pour interagir avec la blockchain directement depuis l'application Web de l'auteur. La chaîne utilise l'une des premières blockchains conçues dès le départ pour la gouvernance. Une blockchain publique sans licence qui utilise le processus de consensus PoA. Cela se distingue par le taux de transaction élevé, la prévisibilité des intervalles de temps auxquels de nouveaux blocs sont créés et l'absence d'exigences en matière de matériel hautes performances. La sérialisation est effectuée en JSON et la blockchain est possible via l'API HTTP REST.

La nouveauté de cette étude est de combiner la technologie blockchain, les mécanismes de stockage de tables d'authentification sur les documents électroniques et les contrats intelligents pour créer un système de stockage décentralisé appelé Go-Chain (Government Blockchain) dans les systèmes gouvernementaux supérieurs. L'étude a obtenu des avantages considérables par rapport à la norme des systèmes de stockage centralisés en ce qui concerne le stockage et l'accessibilité des données dans le secteur gouvernemental.