Revue Internationale du Chercheur
ISSN: 2726-5889
Volume 7 : Numéro 1

Gouvernance numérique et financement territorial : Vers un modèle multi-agents sécurisé des CTDs au Cameroun.

Digital governance and territorial financing: Towards a secure multi-agent model for DTL in Cameroon.

NGODO ESSONO Emmanuel Francois Xavier
Doctorant
Université Internationale Ibéro Américaine
Département de projet
Mexique

Julio Cesar Martinez ESPINOZA
Enseignant chercheur
Université Internationale Ibéro Américaine
Département de projet
Mexique

MEZAMA MINKA Pierre
Doctorant
Université Internationale Ibéro Américaine
Département de projet
Mexique

Date de soumission : 29/01/2026

Date d'acceptation : 20/02/2026

Pour citer cet article :

NGODO ESSONO. E & al. (2026) «Gouvernance numérique et financement territorial : Vers un modèle multi-agents sécurisé des CTDs au Cameroun.», Revue Internationale du chercheur « Volume 7 : Numéro 1 » pp : 553-575

Résumé

Le mécanisme de dotation financière des projets portés par les Collectivités Territoriales Décentralisées (CTD) souffre d'un déficit de coordination entre les acteurs institutionnels, marqué par un fonctionnement en silos et une faible synchronisation entre les phases de planification, d'exécution et de contrôle. Cette fragmentation accroît les risques d'opacité, d'inefficacité et de non-exécution des projets. Face à ces constats, cet article propose la conception d'un modèle d'e-gouvernement sécurisé visant à harmoniser les interactions entre les entités impliquées dans la chaîne de financement des projets des CTD. L'objectif est d'instaurer un climat de confiance institutionnelle et d'assurer une traçabilité complète des flux financiers, depuis leur allocation jusqu'à leur utilisation finale. La recherche s'appuie sur le potentiel de la blockchain comme technologie de gouvernance décentralisée garantissant sécurité, transparence et intégrité des transactions. Elle propose l'implémentation d'une architecture hybride combinant VPN et blockchain, reliant les quatre entités clés du processus d'octroi et de gestion des financements des projets des CTD.

Mots clés : Financement CTD ; blockchain ; VPN ; e-gov ; CMMI.

Abstract

The financial allocation mechanism for projects implemented by Decentralized Territorial Authorities (DTAs) suffers from a lack of coordination among institutional stakeholders, characterized by silo-based operations and poor synchronization between planning, implementation, and control phases. This fragmentation increases the risks of opacity, inefficiency, and partial or non-execution of projects. In response, this article proposes the design of a secure e-government model aimed at harmonizing interactions among entities involved in the DTA project financing chain. The objective is twofold: to establish institutional trust through robust technological protocols and to ensure full traceability of financial flows, from allocation to final use. The study highlights blockchain technology as a decentralized governance tool capable of enhancing security, transparency, and trust. It ultimately proposes the implementation of a hybrid architecture combining VPN and blockchain, connecting the four key entities involved in the allocation and management of DTA project funding.

Keywords: DTA financing; blockchain; VPN; e-gov; CMMI.

Introduction

L'essor du numérique a profondément transformé les modes de gouvernance publique, incitant les administrations à recourir à l'e-gouvernement pour améliorer la transparence, l'efficacité et la redevabilité de l'action publique (Petrič & Orehek, 2024). Dans les États à gouvernance décentralisée comme le Cameroun, la digitalisation des mécanismes de financement des projets des Collectivités Territoriales Décentralisées (CTDs) constitue un levier stratégique pour renforcer la coordination interinstitutionnelle et assurer la traçabilité des flux financiers.

Cependant, les dispositifs existants demeurent marqués par un fonctionnement en silos, une faible articulation entre les phases de planification, d'exécution et de contrôle, ainsi qu'un déficit de traçabilité décisionnelle. Cette fragmentation institutionnelle accroît les risques d'opacité, d'inefficacité et de non-exécution des projets, compromettant les objectifs mêmes de la décentralisation. Par ailleurs, la mise en œuvre de systèmes numériques de gouvernance financière soulève des enjeux critiques de sécurité et de confiance. Les vulnérabilités technologiques, l'absence d'interopérabilité des systèmes d'information et la persistance de pratiques administratives peu formalisées exposent les institutions publiques à des risques accrus de manipulation ou d'altération des données (Owen et al., 2024).

Dans ce contexte, la présente recherche s'inscrit dans une démarche de réflexion sur la conception de dispositifs numériques de gouvernance adaptés aux réalités institutionnelles des États en développement. Elle interroge plus spécifiquement les conditions dans lesquelles un système d'e-gouvernement peut contribuer à améliorer la gouvernance du financement des projets des Collectivités Territoriales Décentralisées, sans se limiter à une approche strictement techniciste. La question centrale qui guide cette recherche est la suivante : **Comment concevoir, dans le contexte institutionnel camerounais, un modèle conceptuel d'e-gouvernement sécurisé permettant d'améliorer la coordination interinstitutionnelle, la traçabilité et la gouvernance du financement des projets des Collectivités Territoriales Décentralisées ?**

Afin de répondre à cette question, l'étude poursuit les objectifs spécifiques suivants :

- OS1 : analyser structurellement le processus actuel de financement des projets des CTDs et identifier les principales discontinuités informationnelles et organisationnelles ;
- OS2 : évaluer de manière exploratoire la maturité des processus de gouvernance financière à l'aide d'un cadre analytique hybride combinant CMMI et analyse SWOT ;

- OS3 : concevoir un modèle conceptuel d'e-gouvernement sécurisé fondé sur une architecture multi-agents, intégrant des mécanismes de traçabilité et de sécurisation adaptés au contexte camerounais.

La contribution de cette recherche est principalement conceptuelle et méthodologique. Elle vise la production d'un artefact théorique testable, inscrit dans une démarche de Design Science Research, sans prétendre à une validation empirique exhaustive à ce stade.

Le présent article est structuré en quatre sections. La première section propose une revue de la littérature et présente le cadre conceptuel mobilisé pour l'analyse de la conception et de la sécurisation des systèmes d'e-gouvernement. La deuxième section décrit la méthodologie retenue pour la conception du modèle proposé. La troisième section est dédiée à la présentation des résultats. Enfin, la quatrième section discute ces résultats, avant de conclure et de formuler des recommandations.

1. Revue de la Littérature

1.1 Décentralisation

La littérature sur la décentralisation dans les pays en développement souligne un écart récurrent entre ses objectifs théoriques et ses résultats empiriques. L'analyse de Rondinelli (1981) sur le Soudan montre que, malgré des ambitions de renforcement de la planification locale et de participation citoyenne, l'absence de capacités institutionnelles, de ressources adéquates et de cadres juridiques clairs a limité la portée des réformes engagées. Les ambiguïtés de rôles et la persistance de résistances administratives ont contribué à en réduire les effets attendus.

Ces observations trouvent un prolongement dans l'étude de Lameck (2023) sur la Tanzanie, qui met en évidence une décentralisation formelle largement contrainte par un contrôle central persistant, notamment sur les ressources fiscales et les processus décisionnels. Les tensions entre acteurs locaux et administrateurs déconcentrés illustrent les difficultés d'opérationnalisation d'une gouvernance territoriale réellement autonome.

Dans une perspective complémentaire, Jonathan et al. (2024) montrent que la transformation numérique peut soutenir différentes formes de décentralisation en améliorant la circulation de l'information et la coordination interinstitutionnelle. Toutefois, les bénéfices observés restent conditionnés par le niveau de maturité numérique, la qualité de la gouvernance IT et l'appropriation organisationnelle des outils déployés.

Ces travaux suggèrent que ni la décentralisation institutionnelle, ni la digitalisation prise isolément, ne suffisent à garantir une gouvernance locale efficace et durable, en particulier dans des contextes à capacités institutionnelles contraintes.

1.2 Les modèles de maturité et la structuration de la gouvernance numérique

Les modèles de maturité constituent des cadres pertinents pour accompagner la transformation de systèmes socio-techniques complexes. Le CMMI-ACQ V1.3 (SEI, 2010) fournit un référentiel structuré visant à réduire les risques liés aux processus d'acquisition et à renforcer leur alignement stratégique. Sa capacité d'adaptation est illustrée par les travaux de Patón-Romero et al. (2019) sur le Green IT et d'Omol et al. (2025) sur la maturité numérique des PME, montrant que le CMMI peut être mobilisé comme un cadre générique d'amélioration progressive des processus.

Toutefois, ces adaptations ne traitent que partiellement des spécificités de la gouvernance publique décentralisée, notamment les enjeux de coordination interinstitutionnelle, de redevabilité financière et de cybersécurité. Dans cette recherche, le CMMI est ainsi mobilisé comme un socle méthodologique flexible, destiné à structurer la montée en maturité d'un système d'e-gouvernement appliqué au financement des CTDs.

1.3 Outils stratégiques et technologiques

L'analyse SWOT constitue un outil de diagnostic utile pour identifier les capacités internes et les contraintes externes des systèmes publics, mais demeure limitée sur le plan opérationnel, même dans ses extensions adaptées aux écosystèmes numériques complexes (Namugenyi et al., (2019) ; Sammut-Bonnici et Galea (2015). De même, les modèles d'e-gouvernement offrent un cadre fonctionnel prometteur, mais leur efficacité reste conditionnée par les contextes institutionnels, les capacités humaines et la gouvernance des accès (Alshehri & Drew, 2010 ; Schuppan, 2009). L'analyse interne identifie les ressources tangibles (matérielles, financières) et intangibles (brevets, réputation), les capacités (utilisation des ressources) et les compétences clés (avantages durables).

Dans ce cadre, la blockchain apparaît comme un mécanisme pertinent de renforcement de la traçabilité et de la confiance (Paul et al., 2021 ; Kassen, 2022), tandis que les VPN constituent une infrastructure éprouvée pour la sécurisation des échanges interinstitutionnels (Ferguson & Huston, 1998). Ghouly et Faslyh, (2019) dans le même sens mettent en exergue la confiance électronique, la pratique de la signature électronique, la certification électronique renforçant la

sécurité des échanges des informations entre les entités, procurant une valeur juridique et administrative appropriée au domaine numérique renforçant la gouvernance électronique par la mise en œuvre d'une politique de sécurité solide et rigoureuse. ` Kaizar et al. (2025) analysent l'usage combinatoire des ERP et des outils avances tels que l'intelligence artificielle et le big data dans l'optique de l'optimisation des capacités analytiques et prédictives des ERP par rapport aux limites des approches traditionnelles, mettant en relief la centralisation des données la traçabilité garantissant la sécurité du système. Néanmoins, ces technologies ne prennent pleinement sens que lorsqu'elles sont intégrées dans une architecture organisationnelle et procédurale cohérente.

Mkude (2023) explore les pratiques d'innovation ouverte (IO) dans l'e-gouvernement en Tanzanie via une méthodologie qualitative (15 entretiens avec des responsables ICT d'institutions publiques). L'étude révèle que l'IO reste peu comprise (33,3% des répondants seulement en maîtrisent le concept) et rarement mise en œuvre (5 institutions sur 15), avec des pratiques émergentes comme les *living labs*, le *crowdsourcing* et les séminaires.

Manoharan et al. (2017) examine l'adoption de l'e-gouvernement par les gouvernements locaux en intégrant le modèle par étapes (information, transaction, participation) et une perspective institutionnelle. Ils identifient des facteurs clés de succès : les facilitateurs externes (compétition politique, adoption citoyenne) et internes (compétences techniques, leadership managérial), ainsi que des barrières (manque de ressources, contraintes juridiques).

Schuppan (2009) analyse les défis et opportunités de l'e-gouvernement en Afrique subsaharienne, soulignant que le transfert direct de modèles des pays développés est inadapté. L'auteur identifie des problèmes structurels (faible capacité administrative, népotisme, corruption) et des facteurs contextuels (déficits infrastructurels, diversité linguistique, fracture numérique) qui exigent une approche adaptée. Bien que l'e-gouvernement offre des potentiels significatifs (amélioration des services publics, gestion fiscale, participation citoyenne), il comporte des risques de centralisation accrue, de corruption électronique ou d'exclusion sociale si les spécificités locales sont ignorées.

Synthèse

La littérature examinée met en évidence la complémentarité potentielle, mais aussi les limites, des approches stratégiques, organisationnelles et technologiques mobilisées isolément. C'est sur cette base que la présente recherche propose un modèle hybride d'e-gouvernement, articulant diagnostic stratégique, structuration des processus, sécurisation des échanges et

mécanismes de confiance numérique, afin de répondre de manière contextualisée aux enjeux du financement des CTDs au Cameroun.

1.4 Cadre conceptuel intégré à la recherche

Dans cette recherche, la gouvernance numérique est entendue comme l'ensemble des mécanismes institutionnels, organisationnels et technologiques encadrant l'usage des technologies numériques dans l'action publique (Schuppan, 2009). La traçabilité renvoie à la capacité d'un système à enregistrer, conserver et restituer de manière fiable et vérifiable l'ensemble des décisions et des flux financiers associés à un processus public. La confiance institutionnelle repose sur la fiabilité des systèmes, la sécurité des données, la responsabilité des acteurs et la transparence des procédures (Kassen, 2022). Le CMMI est mobilisé comme un cadre d'évaluation de la maturité des processus, tandis que l'analyse SWOT permet une lecture stratégique des forces, faiblesses, opportunités et menaces. Leur hybridation s'inscrit dans une démarche de Design Science Research, visant non pas la mesure de performance, mais la structuration d'un artefact conceptuel adapté à un problème socio-technique complexe.

2. Méthodologie de la Recherche

2.1 Positionnement méthodologique

Cette recherche s'inscrit dans une démarche de Design Science Research (DSR), particulièrement adaptée à l'étude de problèmes socio-techniques complexes impliquant à la fois des processus organisationnels, des acteurs institutionnels multiples et des dispositifs technologiques. L'objectif n'est pas d'évaluer ex post la performance d'un système existant, mais de concevoir un artefact, en l'occurrence un modèle hybride d'e-gouvernement sécurisé, fondé sur un diagnostic rigoureux des dysfonctionnements actuels du circuit de financement des Collectivités Territoriales Décentralisées (CTDs).

La présente recherche adopte une démarche de Design Science Research exploratoire. Les données empiriques collectées ne visent pas une validation statistique du modèle proposé, mais un diagnostic illustratif destiné à éclairer la conception de l'artefact. Le choix de questionnaires à réponses binaires (Oui/Non) se justifie par les contraintes d'accès aux acteurs institutionnels, la nécessité de comparabilité interinstitutionnelle et l'objectif d'identifier l'existence ou l'absence de pratiques formalisées.

Les auteurs reconnaissent que ce choix limite la richesse qualitative et la capacité explicative des données. En conséquence, les résultats doivent être interprétés comme indicatifs et

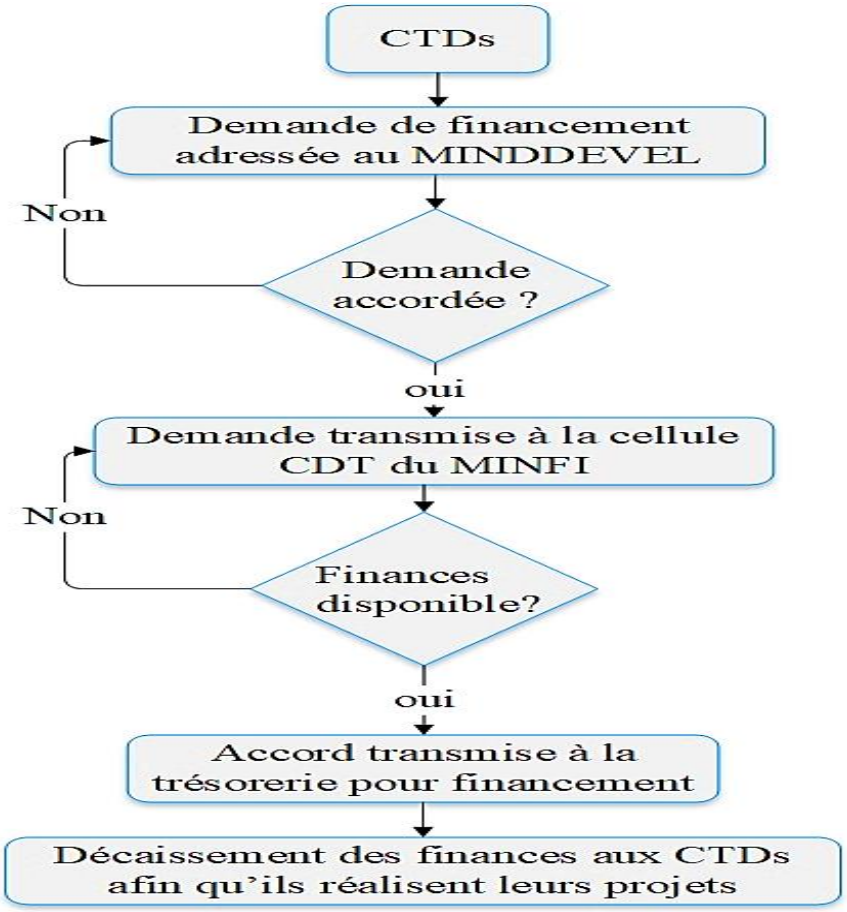
exploratoires, et non comme des preuves empiriques généralisables. L'usage du CMMI dans cette étude ne constitue pas une évaluation normative conforme aux standards du SEI, mais une adaptation heuristique visant à structurer la réflexion sur la maturité des processus.

Conformément aux principes établis par Hevner et al. (2004) et Peffers et al. (2007), la recherche se concentre sur l'identification de domaines critiques à améliorer, la structuration d'un cadre d'analyse pertinent et la proposition d'une solution conceptuellement fondée, ouvrant la voie à des expérimentations futures.

Ces objectifs structurent l'ensemble de la démarche de Design Science Research adoptée et orientent successivement le diagnostic du système existant, la formalisation analytique du processus de financement et la conception de l'artefact d'e-gouvernement proposé.

2.2. Analyse du processus actuel de dotation des CTDs et identification de la faille centrale

Figure1 : Processus d'octroi du financement des projets CTDs



Source : Auteurs

Le processus de dotation financière des CTDs au Cameroun suit un schéma séquentiel impliquant plusieurs acteurs institutionnels. Les besoins exprimés par les populations sont consolidés au niveau des conseils municipaux, qui sélectionnent les projets à financer. Les demandes sont ensuite transmises au Ministère de la Décentralisation et du Développement Local (MINDDEVEL), chargé d'en apprécier la pertinence, avant d'être soumises à la cellule des CTDs du Ministère des Finances (celL CTD-Budget/MINFI) pour validation financière. Une fois approuvée, la dotation est matérialisée par un « carton de financement » papier, permettant aux responsables des CTDs de procéder au retrait des fonds auprès du Trésor public.

L'analyse de ce processus met en évidence une faille centrale, à savoir un déficit de coordination interinstitutionnelle, générateur d'opacité, de lenteurs administratives et de vulnérabilités en matière de traçabilité et de contrôle des risques. Cette fragmentation informationnelle constitue le point de départ du dispositif méthodologique adopté.

2.3. Définition des domaines d'analyse

À partir de la faille centrale identifiée, quatre domaines d'analyse ont été définis, chacun correspondant à un pilier structurant du processus de financement :

- **Coordination**, relative à la synchronisation des acteurs et des décisions entre MINDDEVEL, MINFI et CTDs ;
- **Traçabilité**, concernant la capacité à suivre de manière fiable et continue les flux financiers et décisionnels ;
- **Contrôle des risques**, incluant les mécanismes de prévention des fraudes, de l'arbitraire et des abus ;
- **Gestion financière**, portant sur la planification budgétaire, l'anticipation des ressources et l'alignement des calendriers financiers.

Ces domaines constituent le cadre analytique à partir duquel sont collectées et analysées les données empiriques.

2.4. Stratégie de collecte des données

La collecte des données repose sur des entretiens semi-directifs structurés, administrés sous forme de questionnaires distincts pour chacun des acteurs clés du circuit de financement : les CTDs, le MINDDEVEL, la cell CTD/MINFI et le Trésor public représentant la population. L'échantillonnage est une sélection précise de personnes ciblées par autorisation hiérarchique formalisée en vue de réaliser un entretien, un sondage ou un questionnaire, Dans notre cas nous

avons les receveurs des finances des mairies ou secrétaires généraux , le chef de service dotation CTD du Ministère de la décentralisation et du développement local (MINDDEVEL), le chef de cellule à la cellule CTD-budget du ministère des finances, le Chef de service CTD-Trésorerie via fondé de pouvoir no 2 Trésorerie /Ministère des Finances.

Les questionnaires sont composés exclusivement de questions binaires (Oui/Non)**,** un choix méthodologique motivé par :

- la simplicité d'administration dans des contextes institutionnels hétérogènes ;
- la facilité de quantification des réponses ;
- la capacité à identifier rapidement les ruptures de processus et les dysfonctionnements critiques.

Cette approche vise à garantir la comparabilité des réponses tout en limitant les biais d'interprétation.

2.5. Modèle d'analyse des données

L'analyse des données repose sur une combinaison de trois niveaux complémentaires, permettant une lecture à la fois opérationnelle, stratégique et comparative.

2.5.1. Évaluation de la maturité des processus par le CMMI

Pour chaque domaine d'analyse, un taux de maturité est calculé à partir du ratio entre le nombre de réponses positives et le nombre total de questions associées au domaine, selon la formule suivante :

Taux CMMI=Nombre de reponses "Oui"Nombre total de questions×100Taux\ CMMI = \frac {Nombre\ de\ réponses\ "Oui"} {Nombre\ total\ de\ questions} \times 100Taux CMMI=Nombre total de questionsNombre de re´ponses "Oui"×100

Ce taux permet de positionner chaque domaine sur une échelle de maturité allant du niveau initial (0), caractérisé par l'absence de processus structurés, au niveau d'optimisation (4)**,** marqué par une amélioration continue fondée sur des indicateurs quantitatifs.

2.5.2. Lecture stratégique par l'analyse SWOT

Parallèlement, chaque réponse est interprétée selon une grille SWOT :

- les réponses révélant des pratiques existantes sont codées comme forces ou opportunités ;
- les absences de pratiques ou les dysfonctionnements sont codés comme faiblesses ou menaces, selon leur origine interne ou externe.

Cette lecture stratégique permet de hiérarchiser les enjeux et d'identifier les leviers d'action prioritaires.

2.5.3. Triangulation interinstitutionnelle

Une triangulation croisée des réponses des différents acteurs est ensuite réalisée afin d'identifier :

- les incohérences de perception entre institutions ;
- les points de convergence critiques signalant des dysfonctionnements systémiques.

Cette étape renforce la validité de l'analyse en dépassant les discours institutionnels isolés.

2.6. Intégration CMMI–SWOT et conception du modèle proposé

L'originalité de la méthodologie réside dans **l'**intégration conjointe des lectures CMMI et SWOT, permettant d'associer le niveau de maturité opérationnelle d'un processus à sa valeur stratégique. Une réponse positive indique l'existence d'un processus, interprété comme une force ou une opportunité, tandis qu'une réponse négative signale une défaillance, analysée comme une faiblesse ou une menace.

Cette double lecture constitue le socle analytique à partir duquel est conçu le modèle hybride d'e-gouvernement sécurisé. Les résultats obtenus orientent le choix des composantes technologiques (traçabilité par blockchain, sécurisation des accès par VPN, gouvernance des processus) et la structuration d'une architecture multi-agents adaptée au contexte institutionnel camerounais.

Tableau 1 : Logique d'Alignement CMMI-SWOT

Réponse	Interprétation CMMI	Interprétation SWOT
Oui	Processus existant (niveau ≥1)	Force (Pratique actuelle efficace) ou Opportunité (Potentiel futur d'amélioration)
Non	Défaillance (niveau 0)	Faiblesse (Lacune *interne* avérée) ou Menace (Risque externe objectif)

Source : notre enquête

- Réponse "Oui"

Tableau 2 : Logique d'alignement CMMI-SWOT

Interprétation	Explication
CMMI : Processus existant (≥ niveau 1)	Indique une pratique formalisée, même minimale. Le niveau exact dépend du % de "Oui" dans le domaine.
SWOT : Force OU Opportunité	- Force : Si la question porte sur un *atout actuel* (ex : procédure existante). - Opportunité : Si la question révèle un *potentiel d'amélioration* (ex : adhésion à une innovation).

Source : notre enquête

- Réponse "Non"

Tableau 3 : Logique d'alignement CMMI-SWOT

Interprétation	Explication
CMMI : Défaillance (niveau 0)	Signale l'absence totale de processus structuré. Cible prioritaire pour la modélisation.
SWOT : Faiblesse ou Menace	- Faiblesse : Si le problème est *interne* au système (ex : délais excessifs). - Menace : Si le risque est *externe* (ex : fraude documentée).

Source : notre enquête

2.7. Portée et limites de la démarche

La méthodologie adoptée vise la conception d'un modèle alternatif robuste, fondé sur une analyse rigoureuse des limites du système existant. Elle ne prétend pas évaluer empiriquement la performance du système proposé, mais en démontrer la cohérence conceptuelle, la pertinence contextuelle et la testabilité future. Cette posture ouvre la voie à des travaux ultérieurs d'expérimentation, de simulation ou de déploiement pilote.

3. Résultats

La section suivante présente les résultats obtenus en réponse aux objectifs de recherche définis, en particulier l'analyse structurelle du circuit de financement (OS1), la formalisation analytique du système (OS2) et la conception de l'architecture e-gouvernement sécurisée (OS3). Le modèle mathématique et l'architecture e-gouvernement présentés dans cette section doivent

être interprétés comme des constructions conceptuelles exploratoires. Les coefficients α ne sont pas estimés empiriquement et n'ont pas de valeur prédictive. L'objectif de la modélisation est de formaliser les relations systémiques entre acteurs institutionnels et d'illustrer les effets de la coordination et de la traçabilité sur le processus de financement, et non de produire un modèle opérationnel immédiatement déployable.

3.1 Résultats de la modélisation du processus de financement des projets CTD

Les résultats issus de cette recherche reposent sur la conception d'un modèle mathématique compartimental représentant le circuit réel de financement des projets des Collectivités Territoriales Décentralisées (CTD). Quatre variables principales (X1 à X4), associées à des coefficients de validation (α1 à α4), modélisent les différentes étapes de validation administrative et financière, depuis l'expression du besoin local jusqu'au décaissement effectif par le Trésor.

Les variables identifiées toutes indépendantes traduisent :

- le devis initial proposé par la CTD,
- sa validation successive par le MINDDEVEL,
- son approbation budgétaire par la Cellule CTD–Budget du MINFI,
- et sa disponibilité finale pour décaissement au Tresor.

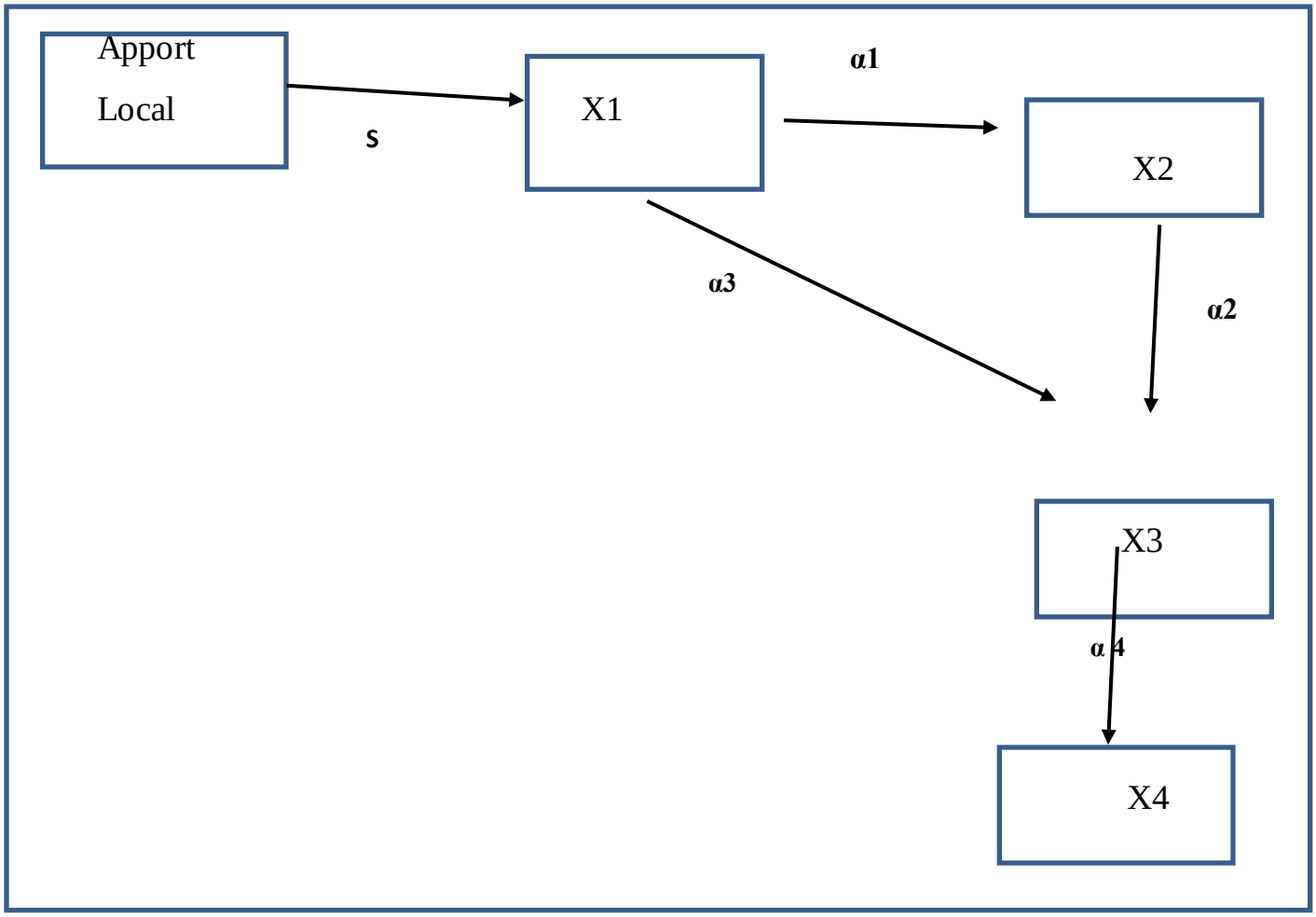
Les paramètres αi, compris entre 0 et 1, représentent les règles institutionnelles, administratives et budgétaires qui conditionnent chaque transition. Cette formalisation met en évidence les points de friction, les pertes de valeur et les délais induits par l'absence de coordination et de traçabilité.

Tableau 4: Paramètres

Désignation	**Significations**	**Unité**
α1	**Taux de validation de X1 à X2**	**Million**
α 2	**Taux de validation de X2 à X3**	**Million**
α 3	**Taux de validation de X1 à X3**	**Million**
α 4	**Taux de validation de X3 à X4**	**Million**

Source : notre enquête

Figure 2 : Diagramme d'interaction



Source : notre enquête

Dans le diagramme d'interaction ci-dessus, l'apport local S est la contribution locale que fournit la CTD au devis établi dans les CTDs. Cet apport peut être le fruit des efforts de collecte des populations locales, la production des CTDs dans ses prélèvements communaux.

Le devis de financement établi au niveau des CTDs au bénéfice d'un projet des localités et l'apport local constituent la demande de financement qui sera adresseé au MINDDEVEL X1X2 ajusté du coefficient **α1**.

Le devis de financement en provenance des CTDs multiplié par α1 le taux de validation de X1 à X2 est appelé α1X1X2 au niveau du MINDDEVEL. Le MINDDEVEL vérifie toutes les conditions requises établies à la validation d'un devis de financement. Si ces conditions sont remplies, alors X1X2 devient X2X3 et multiplié par le taux α2 de validation de X2 a X3 et l'ensemble est acquitté par MINDDEVEL. α2.X2X3 acquitté est donc transmis du MINDDEVEL à la Cell CTD-Budget/Minfi.

La Cell CTD-Budget/Minfi compare le contenu α2X2X3 acquitté par MINDDEVEL au contenu α3X1X3 issu des CTDs. Si les éléments du contenu α3X1X3 sont conformes à ceux validés α2X2X3 par MINDDEVE, alors vérification de la disponibilité du financement dans les caisses. Si financement disponible, alors X3X4 est multiplié par le taux α4 de validation de X3 A X4 et approuvé par Cell CTD-Budget/Minfi, puis transmis au Tresor en α4X3X4 pour décaissement et autorisation aux CTDs pour réception de financement au Trésor.

Système d'équations Mathématiques

$$\begin{cases} X_1' = S - \propto_1 X_1X_2 - \propto_3 X_1X_3 \\ X_2' = \propto_1 X_1X_2 - \propto_2 X_2X_3 \\ X_3' = \propto_2 X_2X_3 + \propto_3 X_1X_3 - \propto_4 X_3X_4 \\ X_4' = \propto_4 X_3X_4 \end{cases}$$

3.2 Dynamique du système et interprétation des équations

L'analyse dynamique du système montre que chaque acteur institutionnel exerce une influence mesurable sur la trajectoire du financement :

- Le MINDDEVEL agit comme un filtre normatif, réduisant ou ajustant le devis initial selon α1 et α2.
- La Cellule CTD–Budget/MINFI joue un rôle central de régulation, combinant contrôle de conformité et contrainte de disponibilité financière (α3 et α4).
- Le Trésor intervient exclusivement en aval, conditionné par les décisions précédentes.

Ce modèle met en évidence une dépendance systémique forte entre les acteurs, où toute opacité ou rupture d'information à un niveau se répercute sur l'ensemble de la chaîne.

3.3 Résultat principal : conception d'une architecture e-gouvernement sécurisée

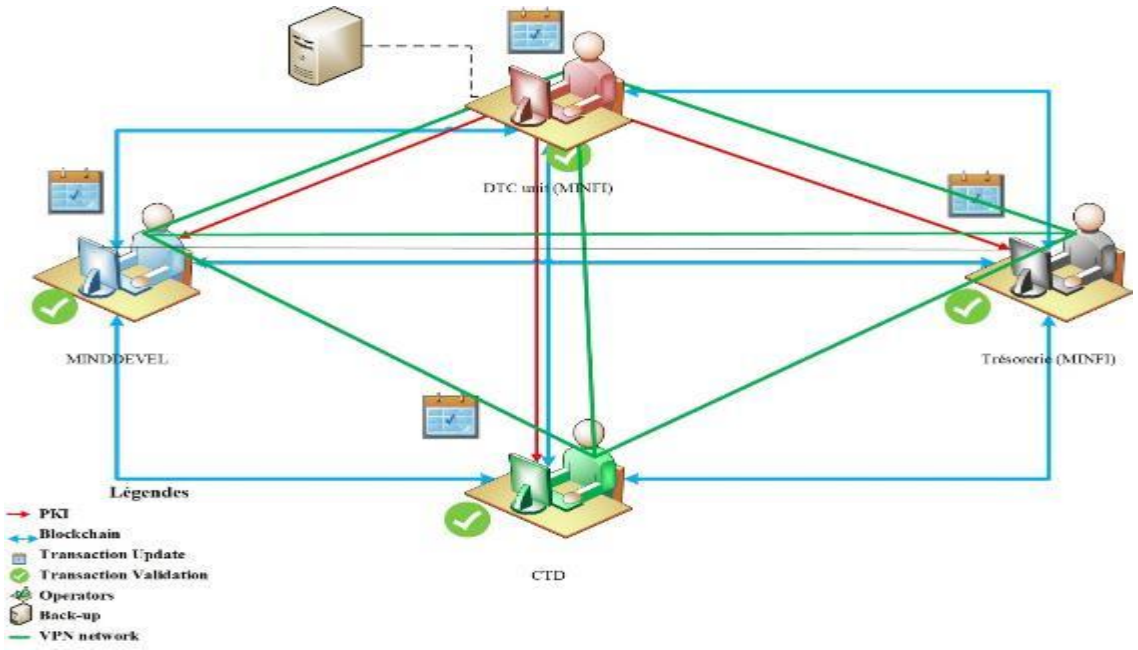
À partir du modèle mathématique, la recherche aboutit à la conception d'une architecture e-gouvernement hybride sécurisée, structurée autour de quatre piliers technologiques :

1. **Sécurisation des communications** par un VPN gouvernemental IPSec/IKEv2 superposé à TLS 1.3.
2. **Traçabilité inviolable** assurée par une blockchain permissionnée, où chaque transaction est horodatée et signée.

3. **Gouvernance des accès** fondée sur une approche Zero Trust, un contrôle RBAC dynamique et une authentification multi-facteurs.
4. **Souveraineté et résilience numérique**, avec un hébergement local, une réplication géographique et un système de supervision SIEM du flux financier transitant entre les nœuds via VPN.

La Cellule CTD–Budget/MINFI émerge comme nœud de confiance central, jouant le rôle d'autorité de certification, garantissant l'intégrité, la cohérence et l'auditabilité du système. Néanmoins ce positionnement de la Cellule CTD-Budget/MINFI comme nœud de confiance central soulève un risque potentiel de centralisation excessive. Ce choix est envisagé ici comme une solution transitoire, nécessitant des mécanismes de contrôle institutionnel renforcés et une gouvernance partagée.

Figure 3: Architecture e-gov hybride sécurisée



Source : Auteur

3.4 Résultats organisationnels : modélisation multi-agents

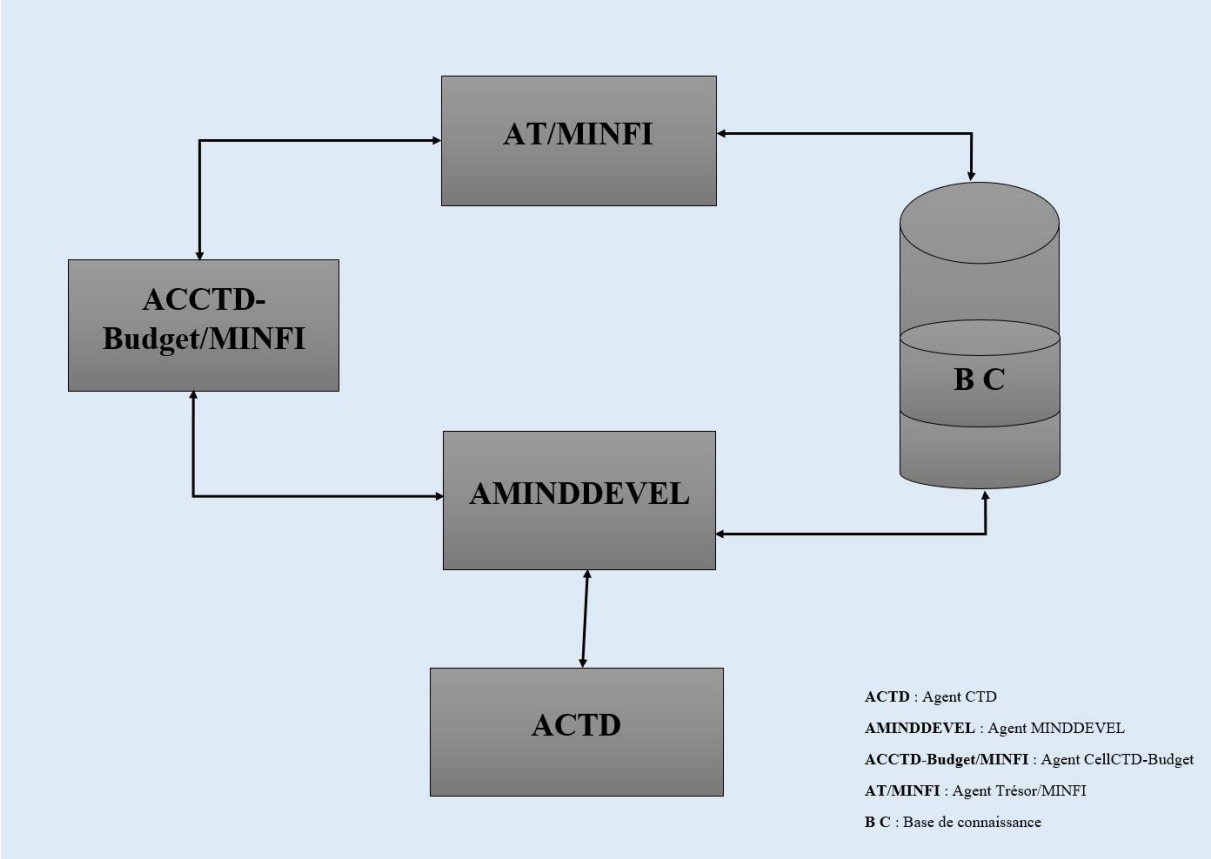
Le système est décliné en un Système Multi-Agents (SMA) où chaque institution est représentée par un agent autonome :

- Agent CTD,
- Agent MINDDEVEL,
- Agent Cell CTD–Budget/MINFI,

- Agent Trésor.

Les interactions sont automatisées, traçables et synchronisées via la blockchain, le VPN, et d'une base de connaissance dotée de modules d'intelligence artificielle éliminant les échanges papier et réduisant significativement les délais administratifs. Ce qui explique le dynamisme du système.

Figure 4: Architecture Système Multi-Agents (SMA) de l'application E-Gov



Source : notre enquête

4. Discussion des résultats, Conclusion et Recommandations

Les résultats obtenus permettent de discuter la pertinence du modèle proposé au regard des objectifs de recherche initiaux, tant sur le plan théorique que sur le plan institutionnel.

4.1 Apports théoriques et méthodologiques

Les résultats confirment qu'une approche combinant CMMI, SWOT et Design Science Research permet de concevoir un modèle d'e-gouvernement adapté aux contextes de décentralisation à faible maturité numérique. Contrairement aux modèles généralistes (GOV.BR, IndiaStack), l'approche proposée privilégie une sécurisation ciblée de la chaîne de

financement, répondant directement aux risques systémiques identifiés. (cf. Tableau rendant compte de l'analyse comparative des solutions e-gouvernementales dans le monde en annexe).

4.2 Apports pratiques et institutionnels

Le modèle proposé :

- renforce la coordination interinstitutionnelle,
- assure une traçabilité complète des flux financiers,
- réduit les délais administratifs,
- limite les risques de fraude documentaire,
- et améliore la confiance entre acteurs publics.

L'intégration de solutions hybrides (VPN, blockchain, modes hors-ligne) garantit une inclusion des CTDs rurales, réduisant la fracture territoriale.

4.3 Positionnement international et originalité (cfère annexe)

En s'inspirant :

- de la résilience estonienne,
- de l'inclusion financière kényane,
- et de l'adaptation rwandaise aux zones faiblement connectées,

le modèle camerounais se distingue par une centralisation sécurisée contextualisée, transformant les contraintes institutionnelles en leviers d'innovation.

4.4 Limites et perspectives

La présente recherche demeure de nature conceptuelle et se heurte à plusieurs limites structurelles, notamment :

- (i) la résistance organisationnelle de certains acteurs institutionnels,
- (ii) les contraintes juridiques et budgétaires encadrant la transformation numérique de l'action publique, et
- (iii) la nécessité d'une volonté politique forte pour soutenir un processus de réforme systémique.

Au-delà des considérations strictement techniques et institutionnelles, l'acceptabilité sociale du dispositif proposé constitue un facteur déterminant de sa soutenabilité. L'appropriation du

modèle par les élus locaux, les agents administratifs et les acteurs financiers conditionne directement l'effectivité des mécanismes de coordination interinstitutionnelle et de traçabilité financière envisagés. Dans des contextes caractérisés par des pratiques administratives historiquement peu numérisées, l'introduction d'un système d'e-gouvernement sécurisé est susceptible de générer des résistances organisationnelles, voire des stratégies d'évitement. Ces enjeux plaident en faveur d'un déploiement progressif du dispositif, adossé à des actions ciblées de formation, de sensibilisation et de co-construction avec les parties prenantes locales.

Dans cette perspective, les recommandations issues de la recherche peuvent être hiérarchisées comme suit :

- la mise en œuvre d'une expérimentation pilote sur un nombre limité de Collectivités Territoriales Décentralisées (CTDs) ;
- la conduite d'une analyse juridique et institutionnelle préalable du cadre de gouvernance proposé ;
- le renforcement des capacités humaines en matière de cybersécurité et de gouvernance numérique ;
- la réalisation d'une évaluation coût-bénéfice avant tout déploiement à grande échelle.

BIBLIOGRAPHIE

Alshehri, M. & Drew, S. (2010). E-government fundamentals. In Proceedings of the LADIS International Conference: ICT, Society and Human Beings 2010 (pp. 35–40). International Association for the Development of the Information Society (IADIS).

Ferguson, P. & Huston, G. (1998). What is a VPN? Revision I. Cisco Systems Technical Documentation.

Ghouly M & Fasly H. (2019) « La sécurité des échanges électroniques : Cas du gouvernement électronique », Revue Internationale des Sciences de Gestion « Numéro 6 / Volume 3 : numéro 1 » pp : 869 – 889 Digital Object Identifier https://doi.org/10.5281/zenodo.3664949

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105. https://doi.org/10.2307/25148625

Jonathan et al. (2024). Digital transformation-driven Decentralisation of public Governance. Procedia computer science,239,1220-1229. https://doi.org/10.1016/j-procs.2024.06.290.

Kaizar C. & al. (2025). ERP Et gestion des risques en contrôle de gestion : vers une meilleure anticipation des aléas financiers Revue Belge ISSN : 2593-9920 Volume 12 : Numéro 134. www.doi.org/10.5281/zenodo. 18436244

Kassen, M. (2022). Blockchain and e-government innovation: Automation of public information processes. Information Systems, 103, 101862. https://doi.org/10.1016/j.is.2021.101862

Kärestad, J., Johnson, L. & Peters, R. (2023). A taxonomy of factors that contribute to organizational cybersecurity awareness (CSA). Information & Computer Security, 33(3), 141–160. https://doi.org/10.1108/ICS-03-2023-0072

Lameck, G. (2023). Political decentralisation and administrative relations in local councils in Tanzania. Public Administration and Policy, 26(3), 335–343

Manoharan, A. P., Melitski, J., & Bromberg, D. (2017). Conceptualizing e-government from local government perspectives. Public Administration Quarterly, 41(4), 764–789.

Mkude, C. (2023). Open innovation in e-government: Exploring its practices in Tanzania. Digital Government Research and practice,4(1), Article I. https://doi.org/10.1145/3571822

Namugenyi & al. (2019). Design of a SWOT analysis model and its evaluation in diverse digital business ecosystem contexts. Procedia Computer Science, 159,1145-1154.https://doi.org/10.1016/i.procs.2019.09.283

Omol & al. (2025. Digital maturity Assesment model (DMAM): Assimilation of design science research (DSR) and capability Maturity Model Integration (CMMI). Digital transformation and society, 10(2) ,128-152.https://doi.org/10.1168/DTS.04.2024.0049.

Owen et al., 2024. Optimism bias in susceptibility to phishing attacks: An empirical study information et computer security,32(5),656-674, doi:10.1108/ICS-02-2023-0027.

Paul, P. K., Aithal, P. S., Saavedra, R., & Ghosh, S. (2021). Blockchain technology and its types: A short review. International Journal of Research in Engineering, Science and Management, 4(3), 18–27.

Patón-Romero et al. (2019). Maturity model based on CMMI for governance of green IT. IET software,13(6),555-563, https://doi.org/10.1049/iet-sen.2018.5351

Peffers, K., Tuunanen, T., Rothenberger.,. & Catterjee,S.(2007). A design science research methodology for information systems research. Journal of management Information Systems,24(3),45-77. https://doi.org/10.2753/MIS0742-1222240302

Petrič & Orehek, 2024. Expressing opiniohs about information security in an organization: The spiral of silence theory perspective. Information et computer security,33(2),223-241.

Rondinelli,1981. Administrative decentralisation and economic development: the Sudan's experiment with devolution. The journal of modern African Studies,19(4),595-624. https: //doi.org/10.1017/S0022278X00020188.

Sammut-Bonnici et Galea (2015). SWOT analysis. In C.I. cooper (ED), Wiley Encyclopedia of management (vol 3). john Wiley et Sons, Ltd. https://doi.org/10.1002/9781118785317.weom320103.

Schuppan, T. (2009). E-government in developing countries. Experiences from sub-Saharan Africa. Government Information Quaterly,26(2), 118-127. https://doi.org/10.1016/j-giq.2008.01.006

Software Engineering Institute, 2010. CMMI for acquisition, version 1.3(Technical Report CMU/SEI-2010-TR-032), Carnegie Mellon University.

ANNEXE

Tableau Annexe 1: Analyse Comparative des solutions e-gouvernementales dans le monde

Critères	Cameroun (Modèle Proposé)	Rwanda (Irembo Platform) Nyirishema & Ntawanga (2020)	Kenya (eCitizen) Gichoya, D. (2018)	Brésil (GOV.BR) Pires, R. R. C., & Garcia, A. C. B. (2022)	Estonie (X-Road) Kalvet, T. (2020)	Inde (IndiaStack) Sharma, S. K. (2021).
Domaine Cible	Financement des CTDs (Collectivités Territoriales Décentralisées)	Services publics unifiés (permis, impôts, état civil)	Services administratifs (passeports, licences)	Portail citoyen intégré	Interconnexion sécurisée des registres publics	Identité numérique et paiements (Aadhaar/UPI)
Technologies Clés	- Blockchain privée - Chiffrement homomorphe - HSM souverain - VPN national	- Cloud souverain - SMS Gateway - Paiements mobiles	- Intégration M-Pesa - Biométrie	- Certificats numériques ICP-Brasil - API Gateway	- Blockchain KSI - Signature électronique	- Aadhaar (biométrie) - UPI (paiements)
Sécurité	- Architecture zero-trust - Journalisation blockchain - RBAC dynamique	- Authentification 2FA - Chiffrement SSL	- Vérification OTP - Contrôles d'accès basiques	- PKI nationale - Audit cryptographique	- Chiffrement quantique-résistant	- Authentification biométrique - Tokenisation
Gouvernance	Autorité de Certification centrale (celCTD-MINFI)	Agence de Transformation Digitale (RTDA)	Direction e-Gouvernement	Comité Directeur Digital (DGD)	Fondation X-Road	India Stack Governance Committee

	avec déploiement décentralisé					
Innovation Principale	NFT institutionnel pour le suivi des projets + Smart contracts de décaissement automatisé	Première plateforme unifiée d'Afrique subsaharienne	Intégration bancaire mobile (leader mondial)	Notifications proactives via "Meu GOV.BR"	Data Embassy (serveurs extraterritoriaux)	Stack ouverte avec 1,3 milliard d'utilisateurs Aadhaar
Traçabilité	Traçage intégral des fonds (allocation → décaissement) sur blockchain avec preuve tokenisée	Suivi des demandes par SMS	Historique des transactions dans le portail	Suivi des démarches en temps réel	Journal des accès cryptographiquement vérifiable	Registre public des transactions UPI
Résultats	Objectifs : - Réduction de 70% des délais - Suppression des fraudes documentaires	Réalisé : 90% des services accessibles en ligne (2023)	Réalisé : 6 000 services digitalisés	Réalisé : 100M d'utilisateurs (2023)	Réalisé : 99% des services en ligne	Réalisé : 40M transactions UPI/jour
Défis	Fracture numérique rurale Résistances bureaucratiques	Couverture internet limitée (60%)	Cyberattaques fréquentes	Inégalités d'accès régionaux	Dépendance énergétique	Exclusion des non-biométrisés