

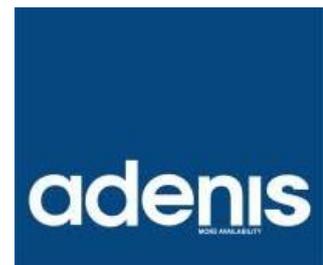
Mémoire de recherche pour l'obtention d'un master MIAGE

Parcours Système d'Information et Innovation (S2I)



**Les patterns logiciels architecturaux de la blockchain
utilisés pour la gestion des dossiers de santé
électronique : Une revue systématique de littérature.**

Réalisé par : **Alliel Steeven**
Tuteur enseignant : **Herbaut Nicolas**
Maître d'apprentissage : **Marciano David**
Année : **2021/2022**



ATTESTATION SUR L'HONNEUR DE NON-PLAGIAT

Je soussigné(e) ALLIEL Steeven déclare sur l'honneur que ce mémoire est le fruit d'un travail personnel et que je n'ai ni contrefait, ni falsifié, ni copié tout ou partie de l'œuvre d'autrui afin de la faire passer pour mienne.

Toutes les sources d'information utilisées (supports papiers, audiovisuels et numériques) et les citations d'auteur ont été mentionnées conformément aux usages en vigueur. Je suis conscient(e) que le fait de ne pas citer une source ou de ne pas la citer clairement et complètement est constitutif de plagiat, que le plagiat est considéré comme une faute grave au sein de l'Université et qu'il peut être sévèrement sanctionné.

Date et signature :

22/09/2022

A handwritten signature in black ink, appearing to read 'Alliel', with a long horizontal line extending to the right and a large loop underneath.

Remerciements

Je souhaite avant tout remercier monsieur Edgar Faure, ministre de l'Éducation de 1969, pour avoir mis en place le cursus MIAGE ainsi que les fondateurs et membres actuels du CFA AFIA. Ils ont permis à des étudiants comme moi d'effectuer une formation en apprentissage en parallèle du cursus universitaire, et ce, depuis 1992.

Ensuite, je souhaite remercier l'ensemble des enseignants de la MIAGE et plus particulièrement mon tuteur enseignant, M. Nicolas Herbaut. Je souhaite lui exprimer toute ma reconnaissance pour m'avoir suivi, encadré, aidé et conseillé tout au long de l'élaboration de ce mémoire. Je le remercie notamment pour son soutien et son implication qui m'ont été d'une aide précieuse.

Je terminerai par remercier mon maître d'apprentissage M. David Marciano pour sa confiance au quotidien et ses précieux conseils.

Abstract

In a world where digitization is taking over all areas, medicine is no exception, quite the contrary. Electronic health record is becoming more and more important, and it is becoming vital to digitize this data in order to facilitate its use and sharing. However, many problems, particularly in terms of security, are to be considered and to which the blockchain could respond. The integration of blockchain into the architecture of electronic health records is a solution proposed by many people. The blockchain being a recent and complex technology, standards or accepted and recognized patterns of the community could greatly facilitate this integration.

In this systematic literature review, we will attempt to analyze, in the literature, the various articles dealing with this subject in order to identify which are the blockchain-based architectural software patterns that are used in current electronic health record systems (EHR).

Dans un monde où la digitalisation s'empare de tous les domaines, la médecine ne fait pas exception, bien au contraire. Le dossier de santé électronique (DSE) prend de plus en plus d'importance et il devient indispensable de numériser ces données afin d'en faciliter l'utilisation et le partage. Cependant, de nombreux problèmes, notamment en termes de sécurité, sont à prendre en compte et auxquels la blockchain pourrait répondre. L'intégration de la blockchain dans l'architecture des dossiers de santé électronique est une solution proposée par de nombreuses personnes. La blockchain étant une technologie récente et complexe, des standards ou patterns acceptés et reconnus par la communauté pourraient grandement faciliter cette intégration.

Dans cette revue systématique de la littérature, nous tenterons d'analyser, dans la littérature, les différents articles traitant de ce sujet afin d'identifier quels sont les patterns logiciels architecturaux basés sur la blockchain qui sont utilisés dans les systèmes de dossiers de santé électronique (DSE) actuels.

Mots clefs

Blockchain – Dossier de santé électronique (DSE) – Dossier médical électronique (DME) – patterns logiciel architecturaux - revue systématique de littérature (SLR)

Table des matières

Remerciements.....	3
Abstract.....	4
Mots clefs.....	4
Table des matières	5
Introduction	7
I. Contexte.....	7
II. Définition de la problématique	8
III. Structure de l'article	8
Définition des termes clés	9
I. Les patterns logiciels architecturaux de la blockchain.....	9
A. La blockchain.....	9
B. Les patterns logiciels architecturaux	10
II. Les Dossiers de santé électronique.....	11
Protocole de recherche	12
I. La revue systématique de littérature : SLR	12
II. Les Questions et hypothèses de recherches	13
III. La Conduite de la recherche	14
A. La requête de recherche	14
B. Liste de contrôle d'évaluation de la qualité	15
C. Les critères de sélection.....	16
D. Exécution de la requête.....	17
Extraction et analyse des données.....	19
I. Analyse quantitative	19
A. Peut-on identifier des patterns architecturaux ?	19
B. Est-ce que les patterns architecturaux sont bien définis ?.....	20
C. Peut-on identifier le(s) système(s) blockchain utilisé(s) ?	21
D. Est-ce que le papier fait partie d'une bonne conférence ?	22
II. Analyse Qualitative.....	24
A. Classification de l'approche de l'article.....	24
B. Les patterns existant dans les dossiers de santé électronique	25
C. Les patterns les plus utilisés.....	33
D. L'utilisation de la blockchain dans les dossiers de santé électronique	36
E. L'utilisation des patterns logiciels architecturaux.....	41
Discussion	43

Conclusion	45
Déclaration d'intérêts concurrents	46
Références	46
Tables des illustrations.....	50
Tables des tableaux.....	50
Glossaires.....	51
Annexes.....	53

Introduction

I. Contexte

Au cours des dernières décennies, notre savoir médical s'est accru. Il existe plus d'options d'investigations et de traitements à notre disposition, par conséquent, nos patients vivent plus longtemps et nous transigeons avec plus de problèmes chroniques. Les médecins de famille ne peuvent pas « tout savoir » ni « tout faire pour tous les patients ».

Du point de vue actuel du diagnostic médical et du traitement au niveau national, la prescription papier est toujours le seul bordereau délivré par le médecin pour permettre au patient de prendre le médicament prescrit à la pharmacie ou à la clinique.

Cependant, pour bien répondre aux besoins complexes de nos patients, il nous faut de bonnes sources de renseignements et de bonnes relations, y compris l'accès à une équipe multidisciplinaire de professionnels et d'autres spécialistes. Nous avons besoin d'outils qui améliorent l'accès à l'information et aux relations.

Pour cela, l'adoption de systèmes technologiques de soins de santé par les prestataires de soins a augmenté au fil des ans. C'est pourquoi, dans le monde entier, la plupart des médecins numérisent les processus de prestation de soins de santé dans les hôpitaux et les cliniques. Les dossiers médicaux électronique (DME) sont l'un des systèmes médicaux numériques les plus courants que les hôpitaux ont inclus dans leur système de soins de santé. Dans la cyber-santé, les données pour les dossiers de santé électronique (DSE) des patients peuvent être recueillies à partir de plusieurs sources, telles que des dispositifs portables, capteurs intelligents et équipements d'imagerie médicale, ce qui rend leurs utilités encore plus intéressantes. Ce qui explique que le marché mondial des dossiers de santé électroniques (DSE) connaît une croissance spectaculaire et devrait atteindre 39,7 milliards de dollars d'ici à fin 2022 [1].

Cependant, la numérisation de ces données n'a pas que des avantages, en effet les systèmes informatiques des hôpitaux sont souvent vieux et peu sécurisés et les données médicales des patients sont pourtant très prisées. Depuis 2016, on observe une explosion des logiciels malveillants rançongiciels, qui ont causé la perte ou la corruption de nombreuses données et tout particulièrement dans les hôpitaux. Pour protéger la sécurité et la confidentialité des dossiers électroniques des patients, il a fallu trouver des solutions capables de parer à ce genre de logiciel.

Sur la blockchain, ce risque est théoriquement nul car c'est l'ensemble de la puissance de calcul du réseau qui garantit que ce qui s'y trouve est inaltérable. En effet, la blockchain accroît la confiance, la sécurité, la transparence, l'immutabilité et la traçabilité des données dans un réseau d'entreprises grâce à ses nombreuses propriétés [2]. La blockchain est devenue un domaine de recherche populaire depuis son introduction, car les avantages ont été constatés dans diverses industries [3]. Cela pourrait également grandement profiter au secteur de la santé et notamment au niveau des DSE ou DME en palliant différentes menaces de sécurité qui planent sur ces derniers.

Ainsi, l'intégration de différents systèmes blockchain dans la numérisation des données médicales permettrait de favoriser et d'accélérer le développement des dossiers médicaux électroniques.

II. Définition de la problématique

Nombreux sont ceux qui ont déjà mis en place des systèmes de dématérialisation des données médicales à l'aide de dossiers électroniques de santé. Mais si tout le monde ne franchit pas le cap, c'est parce que la plupart sont conscients des dangers potentiels et des failles que peut causer cette évolution. Cependant, quelques chercheurs, persuadés que les dossiers médicaux de santé peuvent avoir un grand impact positif dans le domaine de la santé, ont vu le potentiel dans la blockchain et dans ses caractéristiques. Ils ont donc décidé de proposer et/ou de mettre en place des architectures l'intégrant. L'objectif de la plupart d'entre eux étant de garantir la fiabilité, la sécurité et la confidentialité des données patients grâce à la blockchain.

Toutefois, nous avons remarqué qu'il n'y a pratiquement pas d'étude dans la littérature qui explique et/ou qui standardise la mise en place d'une architecture qui intègre la technologie blockchain.

Ainsi, l'objectif de cette revue littéraire systématique est d'analyser les solutions et approches évoquées par la communauté scientifique afin d'identifier :

De quelle manière les patterns logiciels architecturaux basés sur la blockchain sont utilisés dans les systèmes actuels de dossier de santé électronique (DSE).

III. Structure de l'article

L'article est organisé de la manière suivante. Nous allons dans un premier temps donner une définition des éléments-clés de cette revue : La blockchain, les patterns logiciels, les dossiers de santé électronique (DSE). Puis nous détaillerons le protocole de recherche pour effectuer cette étude littéraire systématique. Ensuite nous présenterons l'extraction et l'analyse des données de cette recherche. Enfin, nous discuterons des résultats obtenus et de ce que ça apporte à la communauté scientifique avant de conclure dans la dernière section.

Définition des termes clés

Le présent travail est une revue systématique de littérature permettant de recenser les résultats concernant les patterns logiciels architecturaux de la blockchain qui sont utilisés dans les systèmes actuels de dossier électronique de santé (DSE). Nous allons donc définir ces termes clés.

I. Les patterns logiciels architecturaux de la blockchain

A. La blockchain

Le concept de la technologie blockchain a été introduit pour la première fois par Satoshi Nakamoto dans l'article bien connu sur le Bitcoin [4]. Depuis, La blockchain est devenue l'une des technologies les plus populaires du moment. Dans son livre *Blockchain, la révolution de la confiance*, Leloup donne plusieurs définitions de la blockchain adaptées à différents niveaux de compréhension. Nous avons choisi de citer celle-ci :

Définition 1 : Une Blockchain est une nouvelle technologie de base de données s'appuyant et tirant pleinement profit d'internet, du protocole libre, de la puissance de calcul et de la cryptographie. Cette base de données transactionnelle distribuée est comparable à un grand livre de compte (registre) dans lequel chaque nouvelle transaction est écrite à la suite des autres, sans avoir la possibilité de modifier ou d'effacer les précédentes. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds).

Concrètement, cela revient à dire qu'une Blockchain est une base de données transactionnelle distribuée. Elle est comparable à un grand livre comptable décentralisé et partagé, qui stocke et transfère de la valeur des données via internet, de façon transparente, sécurisée et autonome, car sans organe central de contrôle. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie appelé : *Consensus entre les membres ou participants* : *Nœuds*. Chaque membre du réseau possède une copie à jour du grand livre et le contenu est toujours en phase avec l'ensemble des participants.

L'architecture de la Blockchain peut être principalement divisée en trois couches : ***Application, Decentralized Ledger*** et ***Peer-to-Peer Network*** [5].

1. ***La couche Applications*** : (couche supérieure du réseau) contient le logiciel de l'application.
2. ***La couche Decentralized Ledger*** : (couche intermédiaire) est une base de données partagée, répliquées et synchronisée entre les membres du réseau. Elle tient les registres des transactions et échanges entre les participants. Chaque fois que de nouvelles transactions sont effectuées, des mineurs les collectent pour miner ce qu'on appelle un nouveau « bloc ». Chaque bloc est constitué d'un en-tête contenant

fondamentalement un horodatage, le hash du bloc précédent, le hash du *Merkle root*, du nonce. L'ensemble des blocs forment la Blockchain.

3. **La couche Peer-to-Peer Network** : (couche inférieure) est la couche qui permet concrètement de se séparer des différents tiers lors des transactions.

B. Les patterns logiciels architecturaux

Dans le domaine du génie civil, les patterns sont de solides atouts pour les ingénieurs et les architectes pour concevoir des applications robustes et bien conçues. Dans son livre *A pattern Language* [6], C. Alexander propose une définition des patterns :

Définition 2 : *Chaque modèle décrit un problème qui se produit à plusieurs reprises dans notre environnement, puis décrit le cœur de la solution à ce problème, de telle sorte que vous puissiez utiliser cette solution des millions de fois, sans jamais avoir à le faire deux fois de la même manière.*

Concrètement, c'est un arrangement caractéristique de module reconnu comme bonne pratique pour résoudre un problème de conception.

Cette définition peut également être étendue à la conception de logiciel et d'architecture informatique. En effet, il existe toute une collection de patterns logiciels qui décrit des solutions standards, reconnues et admises par la communauté, qui répondent à des problèmes courants, utilisables dans la conception de différents logiciels, et ce, dans de nombreux domaines [7, 8].

Les différents patterns existants peuvent être regroupés en trois catégories [9] :

1. Les **patterns architecturaux** : qui définissent, au plus haut niveau d'abstraction, la structure générale de l'application (éléments, connexions).
2. Les **design patterns** : (ou patterns de conception) qui définissent une façon d'organiser des modules, des classes ou des composants pour résoudre un problème.
3. Les **idiomes** : sont des solutions à un problème lié au langage au niveau du code.

Il existe également un catalogue **d'anti-patterns**. Comme son nom l'indique, un anti-pattern est un exemple de mauvaise pratique à ne surtout pas suivre.

L'utilisation de patterns dans une application est grandement bénéfique. En effet, accélérer le processus de développement en fournissant des paradigmes de développement qui sont le fruit de nombreuses années de travail, de nombreux débats et tests ont été réalisés sur des applications réelles.

Par association de ces deux concepts, les patterns logiciels architecturaux de la blockchain sont des structures générales d'application dans lesquelles des technologies, développées à l'aide de la blockchain, sont intégrées pour répondre à des problèmes ou des besoins connus.

II. Les Dossiers de santé électronique

Les dossiers de santé électronique (DSE) ou Dossier médical électronique (DME) regroupent l'ensemble des données relatives à la santé provenant de sources multiples sous un format numérique. Les prestataires de soins de santé génèrent une multiplicité de données sous différents formats qui sont saisies dans les référentiels de données des patients et sont accessibles aux personnels de santé par le biais des dossiers médicaux électroniques. À leur tour, ces professionnels produisent des documents qui résument ces données, les analysent, les interprètent et définissent des actions [10].

L'image ci-dessus représente l'ensemble des informations de santé d'un patient qui peuvent être enregistré dans un DME/DSE.

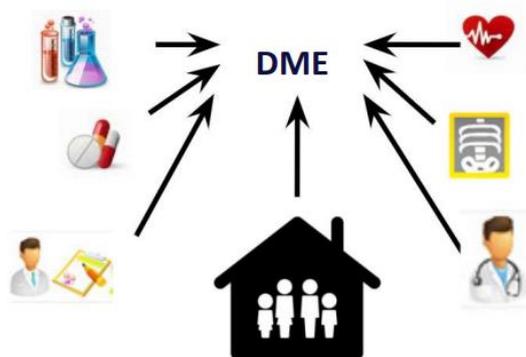


Figure 1: Origine des informations de santé d'un patient dans un DME [10].

Le dossier de santé électronique (DSE) est une information critique et très sensible liée à la santé pour le diagnostic et le traitement des patients sous soins.

Le volume de données sur les patients dans plusieurs DSE continue de croître de façon spectaculaire. En effet, les DSE existants appartiennent à des patients et des hôpitaux spécifiques, de sorte que les données sont dispersées, ce qui limite la portée et l'accès.

L'accès, le partage et la distribution des DSE à d'innombrables acteurs de la santé, y compris les hôpitaux, les médecins, les pharmacies, les laboratoires, les compagnies d'assurance, les chercheurs et les familles des patients, sont des défis auxquels le secteur de la santé est confronté aujourd'hui. Par exemple, les patients atteints du VIH ou du cancer doivent maintenir un long historique de plans de traitement, de tests, de rapports de diagnostic médical, de processus de réadaptation post-traitement et de soins de suivi. L'accès, le stockage, le partage et la distribution de ces informations à plusieurs professionnels de la santé sont essentiels pour maintenir à jour les antécédents médicaux des patients, les tests de laboratoire appropriés, ainsi que les diagnostics, les traitements et l'état de santé des patients [22].

Protocole de recherche

I. La revue systématique de littérature : SLR

Une revue systématique consiste à collecter le maximum de connaissances, en réponse à une question structurée. Puis à en réaliser une évaluation critique et une synthèse afin que son utilisateur puisse se faire une idée de l'état des savoirs actuel et de mettre en évidence les domaines à approfondir. Il existe deux types de revue systématique :

- **La revue systématique de cartographie (SMS)**, qui est conçue pour donner une vue d'ensemble d'un vaste domaine de recherche par le biais d'une classification et d'un comptage des contributions par rapport aux catégories de cette classification [11]. Cela consiste à effectuer une analyse « en largeur » de la littérature afin de par exemple établir des statistiques pour structurer un domaine de recherche.
- **La revue systématique de littérature (SLR)**, quant à elle, identifie, sélectionne et évalue de manière critique la recherche dans le but de répondre à une question clairement formulée [12]. Cela consiste à effectuer une analyse « en profondeur » de la littérature afin de dresser un résultat qui permet de synthétiser toutes les connaissances existant sur notre question de recherche.

Ainsi, dans notre cas, le choix de réaliser une SLR est plus pertinent puisque nous souhaitons répondre à une question clairement définie :

De quelle manière les patterns logiciels architecturaux basés sur la blockchain sont utilisés dans les systèmes actuels de dossier de santé électronique (DSE).

Pour cela, nous devons effectuer une collecte et une analyse qualitative et quantitative des différents articles de la littérature traitant de ce sujet afin de réaliser la synthèse des résultats obtenus. En effet, il est intéressant de connaître comment la recherche évolue pour ce sujet, les normes et patterns admis, validés ou proposés par la communauté scientifique.

Pour réaliser au mieux cette revue systématique de littérature, nous avons choisi de suivre la ligne directrice proposée par Kitchenham [13].

Elle se décompose en quatre grandes étapes :

1. **Planification** : durant laquelle nous avons défini le contexte et les objectifs de notre étude, établi la question de recherche principale et ses sous-questions, choisi les stratégies de recherche des articles à sélectionner et déterminer des critères d'inclusion/exclusion.
2. **Conduite de la recherche** : c'est-à-dire la mise en place des stratégies précédemment définies afin d'extraire et de filtrer les articles les plus pertinents pour notre revue. Ces études sont ensuite lues dans le but d'en retirer les données nécessaires pour répondre aux questions de recherche.
3. **Rapports des résultats** : où nous avons étudié et analysé les données extraites, établi des résultats et répondu à nos questions de recherches.

II. Les Questions et hypothèses de recherches

Le but de cette étude est d'extraire de la littérature, les différentes architectures, mise en place autour de la blockchain, relatives aux dossiers de santé électronique (DSE) afin de connaître les différents patterns utilisés. Pour atteindre cet objectif, nous avons établi quatre questions de recherche, à savoir :

- *QR1 : Quels sont différents patterns logiciels de la blockchain existant dans les architectures des dossiers de santé électronique ?*
- *QR2 : Quels sont les patterns les plus utilisés dans ces architectures ?*
- *QR3 : En quoi l'utilisation de patterns logiciels architecturaux peut être bénéfique ?*
- *QR4 : Quels sont les systèmes blockchain utilisés dans ces architectures ?*

Nous avons également émis des hypothèses de recherche par rapport à nos connaissances et nos opinions qui seront par la suite vérifiées ou infirmées en fonction de nos résultats.

- *H1 : Toutes les architectures des dossiers de santé électronique basées sur la blockchain utilisent au moins un pattern logiciel de blockchain.*
- *H2 : Les patterns utilisés ne sont pas définis de manière explicite.*
- *H3 : Les patterns logiciels de la blockchain qui sont utilisés dans les différentes architectures sont toujours les mêmes. Il n'y a pas de consensus clairement défini et adopté.*
- *H4 : La blockchain est parfaitement adaptée dans les architectures des dossiers médicaux électroniques.*

III. La Conduite de la recherche

A. La requête de recherche

Notre objectif étant d'extraire un panel d'articles traitant de notre sujet, nous avons dû concevoir une requête de recherche permettant de filtrer les différentes bases de données d'article. Par la suite, nous avons aussi utilisé l'effet boule de neige (*snowballing*) sur les articles préalablement sélectionnés.

En parallèle de cette étude, une autre revue systématique de littérature est réalisée sur un sujet similaire : ***Les aspects de vie privée dans l'échange de données médicales avec la blockchain.***

En effet, dans le domaine de la santé, la confidentialité des données est primordiale. Comme dit précédemment, il existe certains dangers et failles potentiels dans le développement des dossiers de santé électronique et notamment en matière de vie privée et de confidentialité des données. Il est donc intéressant de voir comment dans la littérature ce problème est traité.

Par conséquent, nous avons fait le choix d'appliquer une méthode de recherche commune à nos deux sujets et de partir sur un même corpus d'articles pour ensuite les traiter sous des axes différents chacun de notre côté.

Au cours du projet, nous avons également travaillé en collaboration sur l'analyse de la vie privée de certains articles à l'aide de l'outil [linddun Go](#) au cours duquel j'ai contribué à la validation de ses propositions architecturales.

Pour réaliser la requête de recherche, nous avons défini les termes clés « patterns », « architecture », « blockchain », « healthcare » et « electronic records ».

Pour relier les deux revues, nous avons également ajouté le terme « privacy ».

Afin d'augmenter nos résultats de recherches, nous avons déterminé des synonymes de ces termes clés, à savoir « design », « model », « health », « health-care », « medical », « electronic files », « confidentiality », « private », « protection » et « security ».

Nous avons utilisé les opérateurs booléens AND (pour connecter les termes de recherches définis) et le mot clé OR (pour intégrer les termes et/ou expressions alternatifs aux termes clés principaux).

Ainsi, nous avons pu obtenir la requête suivante :

```
("Electronic Records" OR "Electronic Files") AND ("blockchain") AND ("healthcare" OR "health" OR "health-care" OR "medical") AND ("pattern" OR "architecture" OR "design" OR "model") OR ("privacy" OR "confidentiality" OR "private" OR "protection" OR "security")
```

Une fois la requête déterminée, nous avons choisi d'utiliser **MIAGE Scholar** [14] comme source principale de recherche des études existantes.

B. Liste de contrôle d'évaluation de la qualité

Pour préparer la phase n°2 de conduite de la recherche, nous avons listé une série de questions permettant d'évaluer la qualité des articles obtenue à l'aide la requête :

- *QQ1 : Peut-on identifier des patterns architecturaux ?*

Tout l'objectif de ce mémoire est de savoir si la communauté scientifique connaît les principaux patterns existants et les utilise dans leurs architectures ou s'ils les construisent sans même s'en servir.

- *QQ2 : Si des patterns architecturaux sont utilisés, sont-ils clairement définis ?*

Le fait de se servir de certain pattern est une bonne chose mais nous avons besoin de savoir si les auteurs justifient correctement leurs utilisations.

- *QQ3 : Peut-on identifier le(s) système(s) blockchain utilisé(s) ?*

Si des patterns sont utilisés, il est intéressant de connaître les systèmes blockchain utilisés pour permettre à d'autres de les réutiliser par la suite dans un même domaine d'application.

- *QQ4 : Est-ce que le papier fait partie d'une bonne conférence ?*

Un papier faisant partie d'une bonne conférence permet d'appuyer nos arguments et nos conclusions et ainsi d'avoir un impact beaucoup plus important ensuite.

Pour chacune des questions, nous avons déterminé trois propositions de réponse, à savoir : « oui » qui a un poids de 1, « partiellement » qui a un poids de 0.5 et « non » qui a un poids de 0.

Pour chacune des études recensées depuis **MIAGE Scholar**, nous avons répondu à toutes ces questions.

C. Les critères de sélection

Enfin, nous avons établi des critères d'inclusion et d'exclusion qui nous ont permis par la suite de filtrer les articles issus de la requête. Ils fournissent des directives systématiques pour inclure ou exclure des articles pendant la phase de filtrage. Les études qui sont ainsi incluses sont sélectionnées pour une lecture plus approfondie.

Ces critères sont contenus dans le tableau ci-dessous :

Critères d'inclusion	Critères d'exclusion
1. Présente un ou plusieurs modèles basés sur la blockchain.	1. Ce document est un double d'une autre étude. 2. Ne contient pas d'architecture incluant la blockchain 3. L'article est une revue/SLR 4. L'article n'est pas écrit en anglais. 5. L'article est trop ancien.

Tableau 1: Liste des critères d'inclusion et d'exclusion.

- Critère d'inclusion

Nous avons décidé d'inclure la quasi-totalité des articles qui présentent une architecture de dossier électronique de santé basée sur la blockchain. Notre objectif principal étant d'analyser les solutions et approches évoquées par la communauté scientifique afin d'identifier quels sont les patterns logiciels architecturaux qui sont utilisés dans le but de savoir si les patterns sont connus et appliqués ou non.

- Critère d'exclusion

2. Un article ne présentant pas d'architecture incluant la blockchain n'a aucun intérêt particulier dans notre revue systématique.

3. Nous ne traitons pas les revues systématiques.

4. Nous avons décidé de ne traiter que des articles rédigés en anglais.

5. La blockchain étant une technologie assez récente, nous avons jugé qu'il ne serait pas pertinent de traiter des articles trop anciens. De plus, si des informations assez intéressantes auraient été publiées dans de bonnes conférences, nous sommes partis du principe qu'elles sont forcément reprises et citées dans les articles les plus récents.

D. Exécution de la requête

Une fois toutes les étapes précédentes déterminées, nous avons transformé et exécuté notre requête de recherche sur **MIAGE Scholar** :

```
(TITLE (healthcare) OR TITLE(health) OR TITLE(health-care) OR TITLE(medical)) AND  
(TITLE(blockchain)) AND (TITLE(electronic files) OR TITLE(electronic records)) AND  
(TITLE-ABS-KEY("pattern") OR TITLE-ABS-KEY("architecture") OR TITLE-ABS-  
KEY("design") OR TITLE-ABS-KEY("model")) AND (TITLE-ABS-KEY("privacy") OR TITLE-  
ABS-KEY("confidentiality") OR TITLE-ABS-KEY("private") OR TITLE-ABS-KEY("protection")  
OR TITLE-ABS-KEY("security")) AND PUBYEAR < 2022
```

Nous avons ajouté entre temps le critère « PUBYEAR < 2022 » parce que nous n'aurions pas pu ajouter et traiter tous les nouveaux articles qui seraient apparus tout au long de la réalisation de cette revue systématique de littérature.

À l'aide de cette requête, nous avons pu obtenir 59 résultats. Un seul doublon a été identifié et sept articles n'ont pas pu être traités puisqu'ils étaient inaccessibles ou pas en anglais. Ensuite, nous avons réalisé une première phase d'analyse uniquement en lisant le titre de l'article, son résumé et son schéma d'architecture lorsqu'il y en avait un. Cette étape a fait retirer cinq autres articles de notre liste de résultats. À ce stade, il nous restait 48 articles que nous avons lus et sur lesquels nous avons appliqué principalement nos critères d'exclusion 2 et 4. Nous avons ainsi dû retirer dix autres articles. Au cours de la phase de lecture, beaucoup d'articles mentionnés par d'autres comme source ou citation ont été identifiés (*forward* et *backward snowballing*). Treize d'entre eux ont été sélectionnés, mais aucun n'a été retenu puisque nous avons remarqué que les articles récupérés ainsi n'apportent aucune information supplémentaire pertinente par rapport à ce que nous avons déjà dans les autres articles.

La figure ci-dessous représente les différentes étapes de filtrage réalisées pour obtenir un corpus de 36 articles.

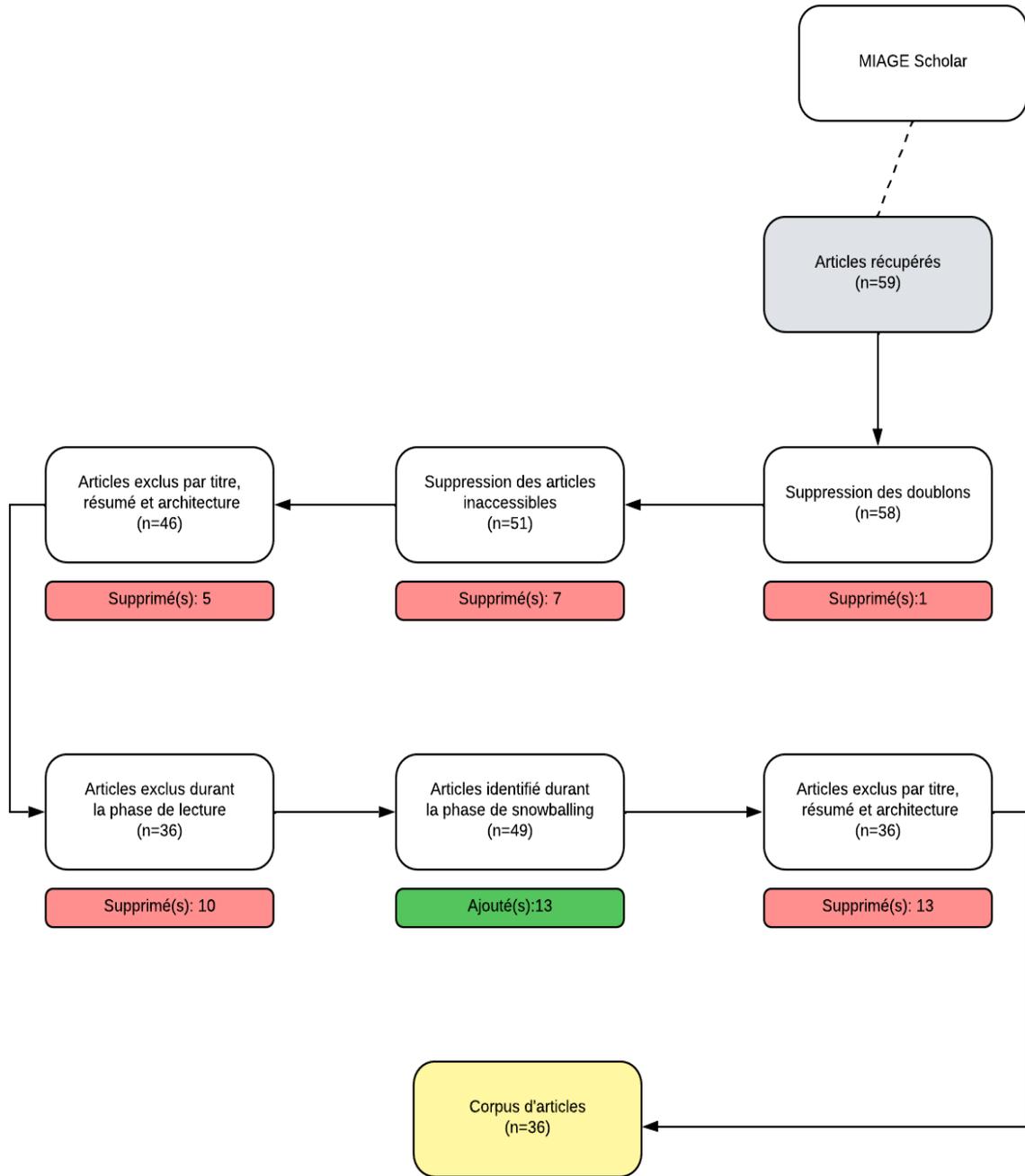


Figure 2: Liste des étapes de sélection appliqué à notre corpus d'article.

Extraction et analyse des données

Après avoir obtenu notre corpus d'articles, nous avons réalisé la synthèse des données qui consiste à rassembler et à résumer les résultats de ces études primaires. Pour cela, nous avons effectué une analyse quantitative et qualitative afin d'en extraire les données qui nous permettront de répondre aux questions posées et d'approuver ou réfuter nos hypothèses de recherche.

Nous allons effectuer une étape de classification des données qui consiste à effectuer une analyse statistique sur l'ensemble des publications de notre revue de manière cohérente avec nos questions de recherche.

Pour ce faire, nous avons utilisé le site parsif.ai [15]. Il nous a permis de récupérer l'ensemble de nos articles, de saisir nos différentes questions et d'y répondre articles par articles afin de pouvoir par la suite extraire les résultats.

I. Analyse quantitative

Lors de la phase précédente, nous avons élaboré une série de questions permettant d'évaluer la qualité des articles obtenus.

Contrairement à l'objectif principal de ces questions, qui est d'évaluer si un article obtient un score suffisant pour être sélectionné, nous avons décidé d'opter pour une autre approche.

Nous avons répondu à ces questions dans le but de révéler si la présence des patterns dans les différentes architectures identifiées est explicite et clairement définie ou non et de manière quantifiable. Nous avons ainsi concrètement voulu analyser la qualité de nos articles afin de valider ou non nos hypothèses de recherche.

A. Peut-on identifier des patterns architecturaux ?

Pour la question **QQ1**, la réponse « oui » nous permet d'identifier quels articles utilisent de manière explicite des patterns architecturaux de la blockchain. Par exemple, dans l'article [17], fait clairement mention du pattern **Off-chain data storage** dans les étapes de son architecture.

Un autre [18] utilise un dérivé de ce pattern de manière explicite aussi, un mécanisme de stockage hybride, le **On-chain-off-chain**. Il consiste à stocker une partie des données sur la blockchain et le reste est cryptées dans une base de données locale. Pour la suite de cette SLR, nous allons inclure cette proposition en tant qu'**Off-chain data storage**.

La réponse « partiellement » quant à elle fait plutôt référence au fait que l'article ne mentionne aucun nom de pattern, néanmoins dans son architecture ou dans le texte, nous arrivons clairement à identifier certains patterns. Par exemple, dans [19]. L'auteur nous explique que chaque hôpital dispose d'un serveur et de plusieurs ordinateurs clients. Chaque client informatique enregistre les informations de santé du patient. L'administrateur du serveur diffuse ensuite les mots-clés du dossier de santé électronique vers la blockchain autorisée. Ce qui correspond exactement à la définition du pattern **off-chain data storage** de l'article [20]. Pourtant, à aucun moment, il n'est fait mention de ce pattern dans l'article. Dans [1] et

[16] les auteurs expriment également clairement que les données des dossiers de santé électronique seront stockées hors chaîne, sur des nœuds périphériques ou sur une base de données externe. C'est toujours l'application du pattern **Off-chain data storage**.

Le fait que l'on n'obtienne aucun article avec la réponse « non » valide notre première hypothèse :

H1 : Toutes les architectures des dossiers de santé électronique basées sur la blockchain utilisent au moins un pattern logiciel de blockchain.

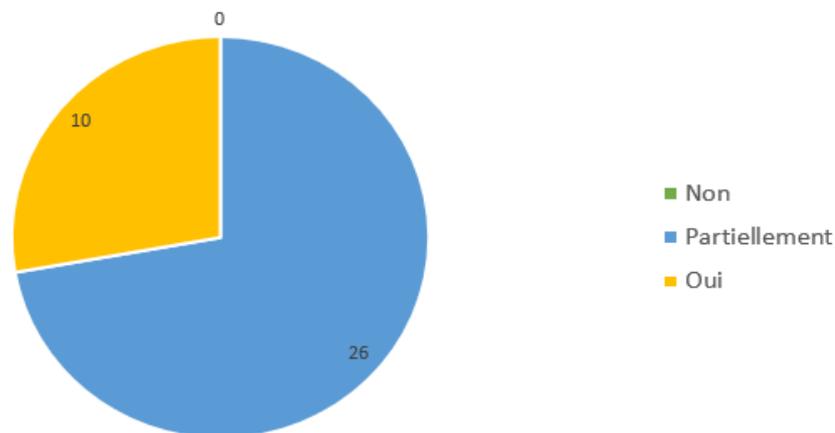


Figure 3: Répartition des articles en fonction des patterns identifiables.

B. Est-ce que les patterns architecturaux sont bien définis ?

Les réponses à la question **QQ2** nous révèlent un nombre majoritaire de « non » ce qui est parfaitement cohérent avec les réponses à la question **QQ1**. La grande majorité des articles sélectionnés pour ce corpus ne parle de patterns que de manière partielle et indirecte. Par conséquent, si déjà les patterns eux-mêmes ne sont pas explicites, il y avait donc peu de chances qu'ils soient clairement définis.

La réponse « partiellement » a été utilisée lorsqu'un article propose un modèle qui semble utiliser un pattern dans son architecture et le justifie de manière générale sans pour autant rentrer dans les détails. Dans [21], les auteurs font une proposition d'architecture pour mettre en place un système de dossier patient électronique. Dans ce système, il suggère de classifier les données patients en trois catégories en fonction de leurs degrés de confidentialité avec un barème prédéfini. Dans cette architecture, nous arrivons à identifier plusieurs patterns s'exprimant de manière implicite. Un de ces patterns est le **Minimize on-chain data**, en-effet, lorsque les auteurs décrivent le système d'enregistrement des données patient, il explique que si les informations du dossier médical du patient contiennent une grande quantité d'informations et que le degré de confidentialité n'est pas élevé, un index peut être établi sur la blockchain sans stocker les informations sur la blockchain. Ils expliquent concrètement que si les informations ne sont pas jugées suffisamment importantes (selon leur système de gradation) elles doivent être stockées en dehors de la blockchain. Ce qui est en soit un des problèmes auxquels tente de répondre ce pattern. Ils ne précisent pas de raison particulière

à cette règle, mais nous pouvons supposer que l'une de ses raisons serait de limiter les coûts d'enregistrement.

Nous avons répondu « oui » à cette question uniquement pour deux articles, comme le [17], qui utilise le pattern **Off-chain data storage**, en stockant les données sur le cloud. L'auteur cite trois autres articles pour justifier le choix d'utiliser le cloud comme moyen de stockage de la donnée et donc indirectement pour justifier le choix d'utiliser ce pattern. Ce qui lui permet de définir comme domaine d'application de ce pattern le fait de garantir la confidentialité et la sécurité des données de santé des patients, de réduire les coûts et temps de transaction.

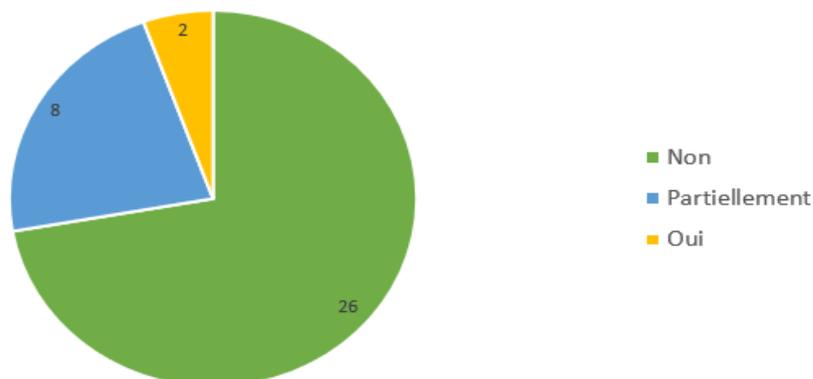


Figure 4: Répartition des articles en fonction des patterns qui sont définis.

C. Peut-on identifier le(s) système(s) blockchain utilisé(s) ?

Pour la question **QQ3**, nous avons identifié les systèmes blockchain pour seulement moins de la moitié des articles, par exemple [16, 22] qui utilisent la blockchain **Hyperledger**. Nous avons répondu « partiellement » lorsque la blockchain utilisée n'était pas explicite, mais que son type l'était comme [23, 24] ou que les auteurs ont utilisé leurs propres implémentations de blockchain [25, 26]. Et enfin « non » quand vraiment rien n'était exprimé à ce sujet ou beaucoup trop implicite [27].

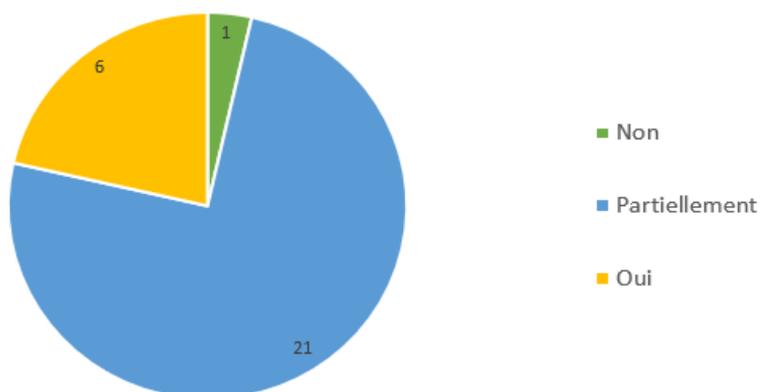


Figure 5: Répartition des articles en fonction des blockchains utilisés

D. Est-ce que le papier fait partie d'une bonne conférence ?

Enfin, la dernière question d'évaluation de la qualité des articles QQ4, était de savoir si l'article fait partie d'une bonne conférence. Pour cela, nous nous sommes servi essentiellement des sites [CORE conférence portal](#) [28], [CORE journal portal](#) [29] et [MIAGE Scholar](#) [14] qui attribue un rang (A+/Q1+, A/Q1, B/Q2, C/Q3 ou autres) et définit un classement à la conférence dans lequel sont publiés les différents articles et journaux.

Nous avons répondu à cette question par « oui » si les articles font partie d'une conférence avec un rang A+ ou A, « partiellement » si les articles font partie d'une conférence notée B et « non » pour les autres.

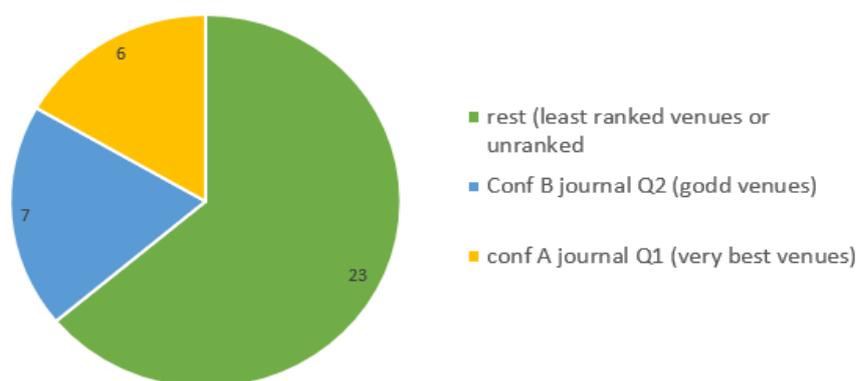


Figure 6: Répartition des articles en fonction de leurs conférences.

On constate que seulement trois des 10 articles, [21, 22, 27] qui parlent de manière explicite d'au moins un pattern font partie d'une bonne conférence.

Nous avons donc répondu aux trois premières questions d'évaluation de la qualité et établi le tableau suivant :

Questions	Non	Partiellement	Oui
QQ1 : Peut-on identifier des patterns architecturaux ?	0	26	10
QQ2 : Est-ce que les patterns architecturaux sont bien définis ?	26	8	2
QQ3 : Peut-on identifier le(s) système(s) blockchain utilisé(s) ?	1	21	14
QQ4 : L'article fait-il partie d'une bonne conférence ?	20	8	8

Tableau 2: Résultats des réponses aux questions d'évaluation de la qualité des articles.

Les résultats obtenus correspondent au nombre d'articles ayant obtenu telle ou telle réponse par question. Chaque réponse obtient un score de 0, 0.5 ou 1.

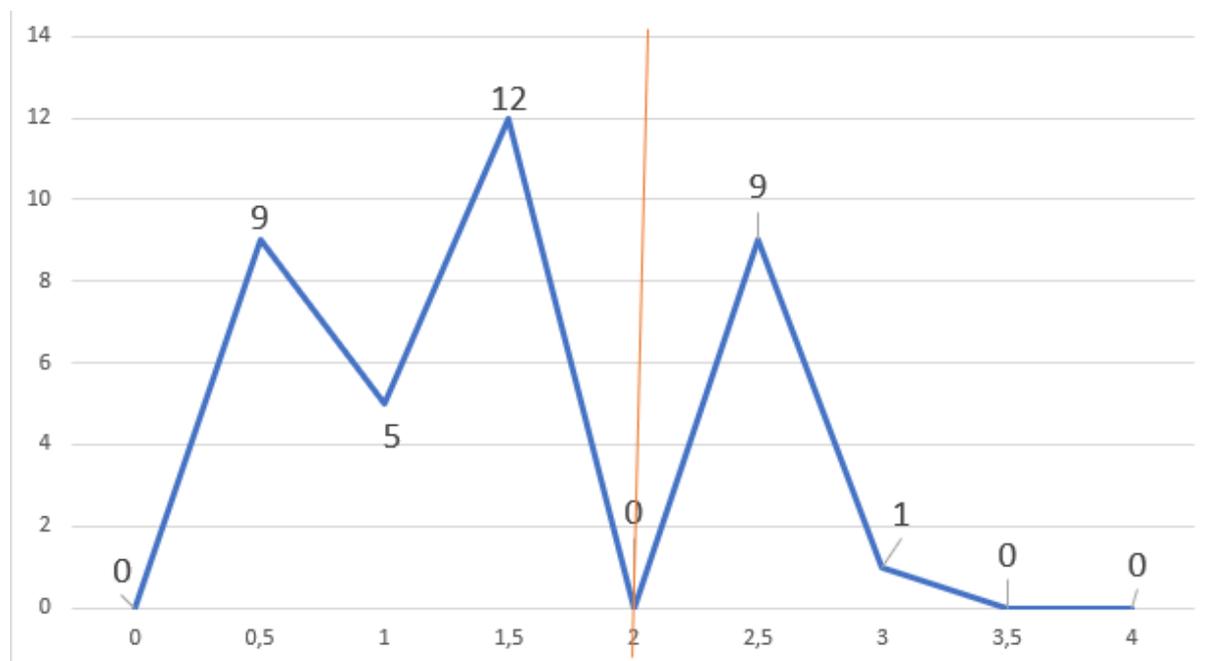


Figure 7: Score des différents articles.

En faisant la moyenne des scores pour chacun des articles en fonction des réponses obtenues aux questions, nous pouvons dès à présent remarquer qu'en grande majorité nos articles ne répondent pas à nos questions de qualité.

II. Analyse Qualitative

Nous avons étudié plus en profondeur les articles afin d'en extraire les données nécessaires pour répondre à nos questions de recherche.

A. Classification de l'approche de l'article

Nous avons jugé pertinent de classer les différentes approches des articles de ce corpus dans le but de comprendre les objectifs de leurs auteurs. Pour cela, nous nous sommes basés sur [30]. Dans cet article, les auteurs veulent nous apprendre à classer différents papiers de recherches en fonction de différents critères. Il en ressort six grandes catégories :

- **Evaluation research**: il s'agit de l'investigation d'un problème dans la pratique de l'ingénierie des exigences ou de la mise en œuvre d'une technique d'ingénierie des exigences dans la pratique. En général, la recherche aboutit à une nouvelle connaissance des relations causales entre les phénomènes ou à une nouvelle connaissance des relations logiques entre les propositions.
- **Proposal of solution** : l'article propose une technique de solution et plaide pour sa pertinence, sans une validation complète. Une preuve de concept peut être offerte au moyen d'un petit exemple, d'un argument solide ou par tout autre moyen.
- **Validation research** : étude des propriétés d'une proposition de solution qui n'a pas encore été mise en œuvre dans la pratique de l'ingénierie des exigences. L'enquête utilise une configuration de recherche approfondie et méthodologiquement solide. Les méthodes de recherche possibles sont les expériences, la simulation, le prototypage, l'analyse mathématique, la preuve mathématique des propriétés, etc.
- **Philosophical papers**: ces articles esquissent une nouvelle façon de voir les choses, un nouveau cadre conceptuel, etc.
- **Opinion papers**: ces articles contiennent l'opinion de l'auteur sur ce qui est mal ou bien à propos de quelque chose, comment nous devrions faire quelque chose, etc.
- **Personal experience papers**: dans ces articles, l'accent est mis sur quoi et non sur pourquoi. Le document doit contenir une liste des leçons tirées par l'auteur de son expérience. Les articles de cette catégorie proviendront souvent de praticiens de l'industrie ou de chercheurs qui ont utilisé leurs outils dans la pratique, et l'expérience sera rapportée sans discussion des méthodes de recherche.

Ainsi, nous avons pu obtenir l'histogramme suivant :

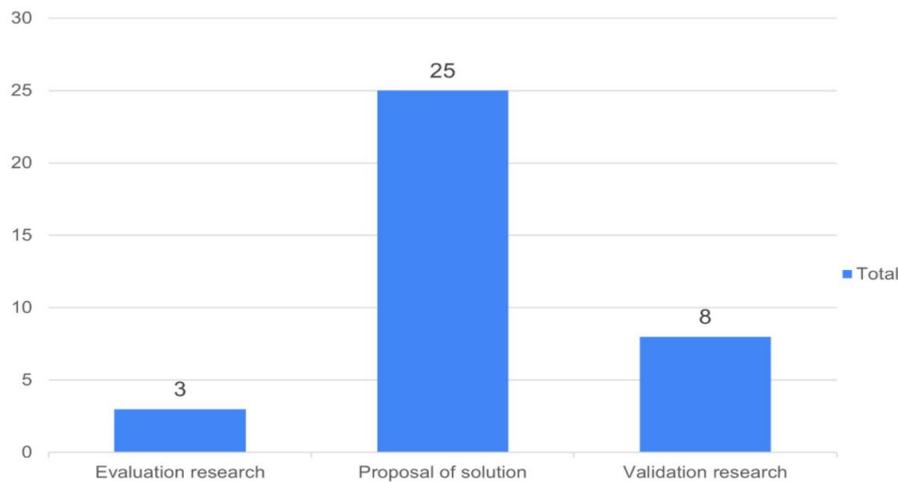


Figure 8: Répartition des articles en fonction de leurs approches.

Nous constatons alors que la grande majorité des articles que nous avons sélectionnés sont des **propositions de solutions**. Cela est parfaitement cohérent puisque la blockchain est une technologie très récente et pas encore adoptée de tous. L'objectif étant de prouver que cette technologie peut parfaitement s'adapter dans l'architecture des dossiers de santé électronique, de nombreux chercheurs ont tenté de proposer une solution pour mettre en place cette intégration.

Nous avons également 8 articles que nous avons classés comme **Validation de recherche** lorsqu'il proposait une solution, qu'elle a été mise en place, testée et validée et qu'elle respecte les critères énoncés dans [30].

Enfin, nous avons identifié trois articles en tant qu'**Évaluation de recherche**, puisque leurs objectifs étaient de prouver comment la technologie blockchain pourrait être exploitée pour améliorer et enrichir les systèmes de dossier de santé électronique existant dans les soins de santé.

B. Les patterns existant dans les dossiers de santé électronique

Dans cette partie, nous souhaitons répondre à cette question :

QR1 : Quels sont différents patterns logiciels de la blockchain existant dans les architectures des dossiers de santé électronique ?

Pour réussir à identifier les patterns architecturaux de la blockchain qui sont présents dans les différentes propositions d'architectures des dossiers médicaux électroniques de notre corpus, nous avons réutilisé la liste des 120 patterns architecturaux extraite de la revue systématique de littérature [9].

Liste de 120 patterns logiciel de la blockchain

- | | |
|---|--|
| 1. AccessRestriction | 61. Math |
| 2. AddressMapping | 62. Migration |
| 3. Announcement | 63. MinimizeOnChainData |
| 4. AutomaticDeprecation | 64. Mortal |
| 5. AvoidRedundantOperations | 65. MultipleAuthorization |
| 6. BlockchainBasedReputationSystem | 66. MultipleRegistration |
| 7. BlockchainBpEngine | 67. Mutex |
| 8. BlockchainSecurityPatternForBigDataEcosystems | 68. NodeSync |
| 9. Blocklist | 69. OffChainContractRegistry |
| 10. BoundWithSocialMedia | 70. OffChainDataStorage |
| 11. BulletinBoard | 71. OffChainSecretEnabledDynamicAuthentication |
| 12. ChallengeResponse | 72. OffChainSignatures |
| 13. ChecksEffectInteractions | 73. OneOffAccess |
| 14. CommitAndReveal | 74. Optimizer |
| 15. ConfidentialAndPseudoAnonymousContractEnforcement | 75. Oracle |
| 16. ContractBalanceLimit | 76. Ownership |
| 17. ContractComposer | 77. PackingBooleans |
| 18. ContractDecorator | 78. PackingVariables |
| 19. ContractMediator | 79. Poll |
| 20. ContractObserver | 80. ProxyContract |
| 21. ContractRegistry | 81. PublisherSubscriber |
| 22. DataContract | 82. PullBasedInboundOracle |
| 23. DecentralizeBusinessProcess | 83. PullBasedOutboundOracle |
| 24. DefaultValue | 84. PullPayment |
| 25. DelegateList | 85. PushBasedInboundOracle |
| 26. DelegatedComputation | 86. PushBasedOutboundOracle |
| 27. DelegatedTransactions | 87. Randomness |
| 28. DigitalRecord | 88. RateLimit |
| 29. DualResolution | 89. ReverseOracle |
| 30. DynamicBinding | 90. Satellite |
| 31. EmbeddedPermission | 91. SecureEtherTransfer |
| 32. EmergencyStop | 92. SelectiveContentGeneration |
| 33. EncryptingOnChainData | 93. SelfConfirmedTransactions |
| 34. EstablishGenesis | 94. SelfGeneratedTransactions |
| 35. EventLog | 95. ShortCircuit |
| 36. ExchangeTransfer | 96. ShortConstantStrings |
| 37. ExplicitelyMarkExternalFunction | 97. SingleLineSwap |
| 38. FactoryContract | 98. SmartContractActivities |
| 39. FewerFunctions | 99. SmartContractTranslation |
| 40. FixedSize | 100. Snapshotting |
| 41. Flyweight | 101. SpeedBump |
| 42. ForkCheck | 102. StateAggregation |
| 43. FreeingStorage | 103. StateChannel |
| 44. HardFork | 104. StateInitialization |
| 45. HashSecret | 105. StateMachine |
| 46. HotColdWalletStorage | 106. Termination |
| 47. IdentifierRegistry | 107. TickerTape |
| 48. IncentiveExecution | 108. TightVariablePacking |
| 49. InterFamilyCommunication | 109. TimeConstrainedAccess |
| | 110. TimeConstraint |

50. InternalFunctionCalls	111. TokenBurning
51. Judge	112. Tokenisation
52. KeySharding	113. TransactionReplay
53. KeyValueStore	114. TransparentEventLog
54. LegalAndSmartContractPair	115. UintVsUint256
55. LimitExternalCalls	116. UseLibraries
56. LimitModifiers	117. VirtualMachineEmulation
57. LimitStorage	118. Vote
58. LowContractFootprint	119. WriteValues
59. MappingVsArray	120. XConfirmation
60. MasterSubKey	

Tableau 3: Liste des patterns de la blockchain [9].

À partir de cette liste, nous avons parcouru une à une les différentes architectures afin d'identifier le plus de patterns possibles.

Ainsi, nous avons réussi à relever neuf patterns différents qui sont utilisés dans notre corpus et que nous allons définir ci-dessous à l'aide de [9, 20] :

1. **Decentralize Business Process** : Ce pattern a pour but d'apporter une solution dans les processus collaboratifs. Les activités exécutées par une organisation sont généralement en dehors du domaine d'influence des autres organisations. Si une organisation est en charge d'un nombre particulièrement élevé de tâches dans un processus, cela peut entraîner une dépendance importante vis-à-vis de l'organisation. Ainsi, la blockchain peut être utilisée comme un outil pour connecter des sous-processus dans un processus décentralisé et comme un outil pour inciter à un comportement correct. En tant que connecteur logiciel, la technologie blockchain peut être utilisée comme interface pour les flux de messages entre différentes organisations [22, 23, 31, 34, 52].
2. **Encrypting on-chain Data** : est utilisé pour préserver la confidentialité des participants impliquée à l'aide d'un chiffrement symétrique ou asymétrique pour chiffrer les données avant de les insérer dans la blockchain. L'une des manières de procéder est de créer une clé privée pour chiffrer et distribuer les données lors d'un échange de clés initiales. Lorsque l'un des participants a besoin d'ajouter une nouvelle donnée à la blockchain, il la chiffre d'abord symétriquement à l'aide de la clé privée. Seuls les participants autorisés à accéder à la transaction disposent de la clé secrète et peuvent déchiffrer les informations [16, 18, 21, 22, 23, 24, 26, 27, 31, 32, 33, 37, 38, 40, 43, 49, 50, 52, 53, 54, 55]
3. **Identifier Registry** : dans les systèmes logiciels centralisés traditionnels, les mappages entre un identifiant et l'emplacement de stockage des données d'identité sont maintenus par une autorité unique centralisée qui peut devenir un point de défaillance unique potentiel. Ce pattern consiste à implémenter un registre d'identifiants conçu comme un contrat intelligent pour maintenir les liaisons entre un identifiant et l'emplacement des attributs de données d'identité hors chaîne associés. Ce contrat intelligent de registre d'identifiants est le principal point d'entrée pour

accéder aux attributs d'une identité, qui peut mapper chaque identifiant à un emplacement de stockage (par exemple, IPFS, Dropbox, etc.). Seul le propriétaire de l'identifiant est autorisé à mettre à jour l'emplacement de stockage des attributs d'identité. Chaque identifiant pointe vers un document d'identifiant qui décrit comment utiliser cet identifiant spécifique, par exemple les clés publiques utilisées pour les signatures numériques, les points de terminaison de service pour l'interaction, etc. [3, 16, 18, 21, 22, 24, 32, 33, 35, 37, 51, 54].

4. **Inter-family communication** : Dans un environnement de contrat intelligent, une propriété souhaitable est d'avoir la capacité pour les contrats intelligents d'appeler d'autres contrats intelligents. Ce pattern fournit une solution de conception permettant aux contrats intelligents de communiquer entre eux, même dans le cas où les contrats intelligents sont écrits dans différents langages de programmation [41].
5. **Minimize on-chain data** : Les coûts en gaz d'une transaction sont très élevés et bien supérieurs au coût de la mémoire. Ainsi, il faut minimiser les données en chaîne. Moins vous mettez de données en chaîne dans les variables de stockage, moins vos coûts de gaz sont importants. Stockez uniquement les données critiques en chaîne pour le SC et conservez toutes les données possibles hors chaîne [33].
6. **Off-chain data storage** : La blockchain a une capacité de stockage limitée. Cependant, les données ne peuvent pas profiter de l'immutabilité ou de garanties d'intégrité sans être stockées sur la blockchain. Ainsi, à l'aide de ce pattern, pour les données de grande taille, plutôt que de stocker les données brutes directement sur la blockchain, la solution est de stocker une valeur de hachage (également appelée condensée) des données brutes sur la chaîne. La valeur est générée par une fonction de hachage, par ex. une de SHA-2 qui mappe des données de taille arbitraire à des données de taille fixe. La valeur de hachage est utilisée pour assurer l'intégrité des données brutes stockées hors chaîne, et la transaction sur blockchain qui comprend la valeur de hachage garantit l'intégrité de la valeur de hachage ainsi que les données brutes d'origine à partir desquelles le hachage a été [1, 3, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 33, 34, 35, 37, 38, 40, 42, 44, 49, 51, 52, 53, 54, 55, 56].
7. **Oracle** : L'environnement d'exécution d'une blockchain est autonome. Il ne peut accéder qu'aux informations présentes dans les données et les transactions sur la blockchain. Les contrats intelligents exécutés sur la blockchain sont de pures fonctions par conception. L'état des systèmes externes n'est pas directement accessible aux contrats intelligents. Donc, pour connecter l'environnement d'exécution fermée de la blockchain au monde extérieur, un oracle est introduit pour évaluer les conditions qui ne peuvent pas être exprimées dans un contrat intelligent exécuté dans l'environnement de la blockchain. Un oracle est un tiers de confiance qui fournit aux contrats intelligents des informations sur le monde extérieur [1, 16, 17, 18, 19, 21, 22, 24, 25, 31, 32, 33, 34, 35, 38, 40, 41, 44, 46, 48, 51, 52, 53].
8. **Reverse Oracle** : Dans un système logiciel, où la blockchain est l'un des composants, les composants hors chaîne peuvent avoir besoin d'utiliser les données stockées sur la blockchain et les contrats intelligents exécutés sur la blockchain pour vérifier certaines conditions. Certains domaines utilisent des systèmes matures et très

volumineux, conformes aux normes existantes. Pour de tels domaines, une approche non intrusive est souhaitée pour tirer parti des systèmes complexes existant avec la blockchain sans changer le cœur des systèmes existant. Solution proposée L'identifiant unique des transactions ou des blocs sur la blockchain est une donnée facilement intégrable dans les systèmes existants. La validation des données peut être mise en œuvre par des contrats intelligents fonctionnant sur blockchain. Un composant hors chaîne est nécessaire pour interroger la blockchain en utilisant l'ID des données [1, 16, 17, 19, 21, 22, 24, 25, 31, 32, 33, 35, 38, 40, 41, 44, 46, 48, 51, 52, 53].

9. **Smart Contract Activities** : Dans un processus inter-organisationnel, différents collaborateurs sont responsables de certaines activités. L'exécution d'activités menées par une organisation peut être considérée comme une « boîte noire » pour d'autres organisations. Sans aucune modification, les collaborateurs ne peuvent pas vérifier la bonne exécution des activités des autres collaborateurs. De plus, il n'est pas non plus traçable jusqu'à eux si même les ressources nécessaires pour exécuter l'activité à un certain moment sont disponibles. Ce pattern propose d'encoder la logique métier d'une activité dans un contrat intelligent et de le déployer sur la blockchain. L'exécution du contrat intelligent est soit déclenchée par le collaborateur responsable, soit par un autre contrat intelligent, tel qu'un moteur de processus métier décentralisé [32, 41].

Dans toutes les architectures de notre corpus, aucun pattern n'est mis en avant ni explicité alors qu'ils sont pourtant bien utilisés.

Prenons comme exemple ces 3 architectures :

Dans cette étude [33], les auteurs proposent un modèle d'architecture de dossier de santé électronique basé sur la blockchain pour répondre aux problèmes du manque de confidentialité et de sécurité des données. Ils prennent comme exemple les données liées à la maladie de la COVID-19, contenant le diagnostic du patient et le certificat de vaccination en Indonésie.

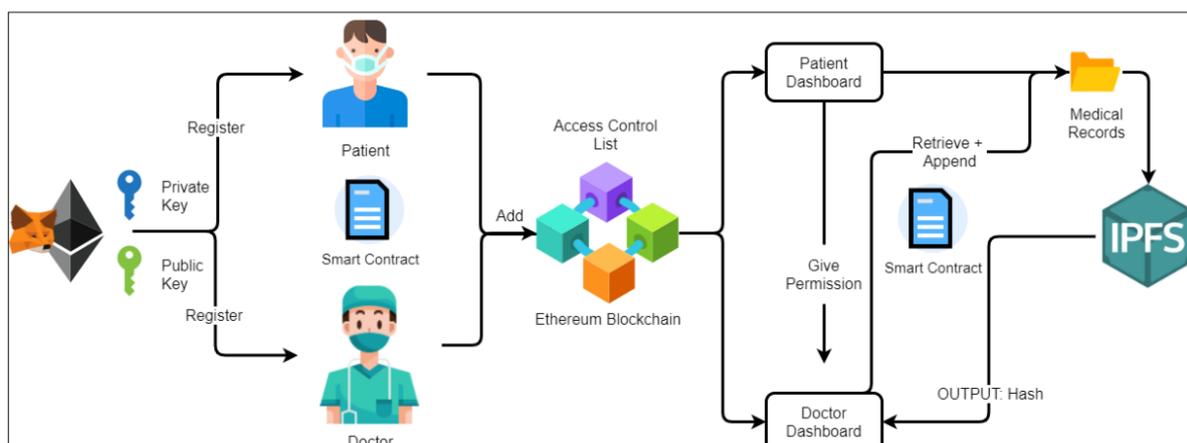


Figure 9: Proposition de modèle de [33].

À l'aide du texte et des différents schémas présents dans cette proposition de modèle, nous arrivons à relever 6 patterns différents. Ces patterns ne sont pas définis explicitement dans le texte, mais nous avons pu les identifier grâce à nos connaissances et aux différentes informations relevées dans cet article :

1. **Un Oracle** : dans cette architecture, nous pensons donc que les oracles font référence aux patients et au docteur qui, tous deux, vont transmettre des informations personnelles, des droits d'accès, et des directives, ... au contrat intelligent qui lui va agir en fonction sur la blockchain. Au vu du niveau de détail donné dans cet article, nous l'avons jugé utile, pour ce scénario.
2. **Encrypting on-chain data** : les données sont préalablement chiffrées avant d'être enregistrées. Ici, les candidats au test COVID-19 utilisent une clé symétrique afin de chiffrer les dossiers médicaux et leurs données personnelles. Après cela, les données chiffrées et la clé symétrique sont stockées sur l'*IPFS*. En ne stockant que le hachage des informations chiffrées sur la chaîne dans le contrat intelligent, seuls les propriétaires des données sont en mesure d'identifier la clé symétrique telle qu'elle est sans chiffrement. L'auteur ne fait pas mention de ce pattern, mais il est clairement identifiable.
3. **Minimize on-chain data** : Ne sont stockées sur la blockchain que les données essentielles et chiffrées pour réduire au minimum les coûts de gaz. La consommation de gaz la plus élevée dans la conception de ce système est de 164 391 Wei, de sorte que s'il est converti en éther, il est d'environ 0,0000000000164391 ETH. La conversion en USD est de 0,0000000006 USD, soit, selon leurs recherches, nettement inférieure au résultat moyen de l'utilisation des transactions dans la blockchain qui est de 0,01 à 1 USD.
4. **Reverse oracle** : ce composant exécute le processus inverse d'un oracle, c'est-à-dire qu'il transmet les données de la blockchain à des applications externes. Dans ce système, cela correspond au fait de donner l'accès aux données chiffrées dans la blockchain, depuis les tableaux de bord des patients et des docteurs qui vont permettre à l'aide du smart contrat de récupérer les données stockées hors chaîne.
5. **Off-chain data storage** : Qui consiste à stocker les données en dehors de la blockchain. C'est le seul pattern qui est explicite dans cette étude. Actuellement, la taille des données stockées dans un bloc sur la blockchain n'est que d'environ 1 Mo [33], il n'est donc pas facile de stocker de grandes quantités de données. Comme les documents liés aux tests COVID-19, à l'identification et aux déplacements seront trop coûteux pour être stockés en chaîne, ces documents doivent être stockés de manière décentralisée et sécurisée. Le stockage *IPFS* est diffusé et publié pour tout le monde ; par conséquent, les informations sont enregistrées sur l'*IPFS* de manière cryptée et seules les entités autorisées ont la permission de lire le contenu en clair.
6. **Identifier registry** : Implémentation d'un registre d'identifiants pour maintenir les liaisons entre un identifiant et l'emplacement des attributs de données d'identité hors

chaîne associés. Les candidats au test COVID-19 utilisent une clé symétrique pour chiffrer les dossiers médicaux et les PII (Personal Identifiable Information). Après cela, les données chiffrées et la clé symétrique sont stockées sur l'IPFS. En ne stockant que le hachage des informations chiffrées sur la chaîne dans le contrat intelligent, seuls les propriétaires des données sont en mesure d'identifier la clé symétrique telle qu'elle est sans chiffrement.

Dans cette étude [34], les auteurs proposent une nouvelle architecture de système de gestion de dossier de santé électronique (DSE) inviolable basée sur la blockchain.

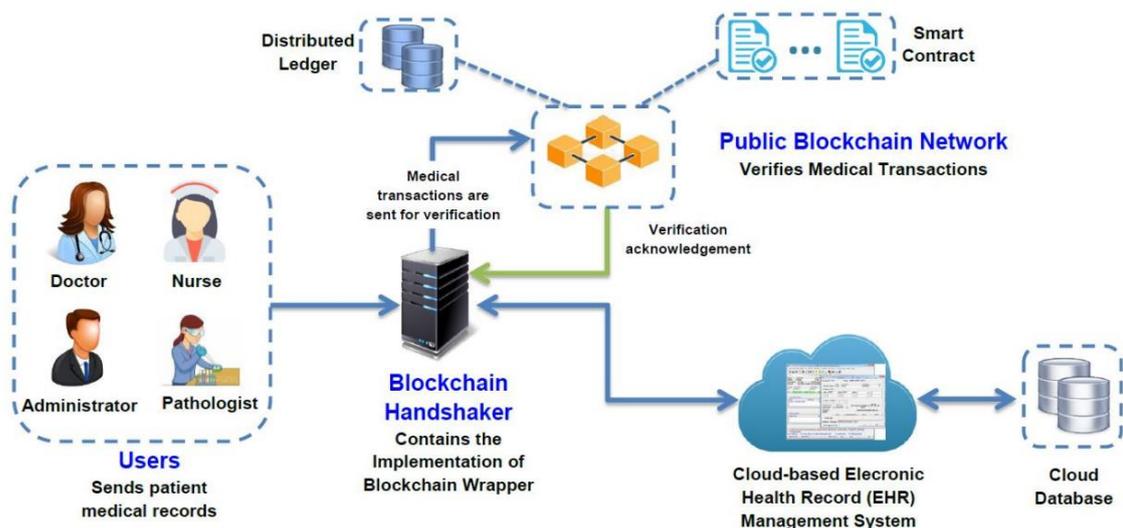


Figure 10 : Proposition de model de [34].

Nous arrivons à identifier 4 patterns en fonction de la description du fonctionnement de l'architecture proposée :

2. les auteurs utilisent un « *blockchain Handshaker* ». Ce composant agit comme un connecteur qui lie l'application utilisateur, le système DSE basé sur le cloud et le réseau de blockchain public dans notre architecture proposée. Ainsi ce composant joue un rôle **d'Oracle** (ce n'est pas précisé dans l'article, mais cela nous semble évident que les données peuvent effectuer le chemin inverse pour être lu et ainsi ce composant jouera également un rôle de **Reverse oracle** à la fois).
3. **Off-chain data storage** : un *cloud* est utilisé ici pour fournir deux services. Le premier service comprend l'hébergement du système de gestion du DSE. Le deuxième service est le service de stockage. Le *cloud* fournit une base de données pour stocker tous les dossiers de santé.
4. **Decentralize business process** : les nœuds de la blockchain reçoivent les transactions et les valident sur la base de contrats intelligents. Si une transaction est validée, les données sont converties en blocs et ajoutées au registre distribué. Le réseau blockchain public envoie un accusé de réception comme vrai ou faux au validateur de transaction de l'*handshaker blockchain*.

Dans [35], les auteurs proposent un partage de données préservant la confidentialité basée sur la blockchain pour les DME, appelé BPDS. Dans BPDS, les DME originaux sont stockés en toute sécurité dans le cloud et les index sont réservés dans une blockchain de consortium inviolable.

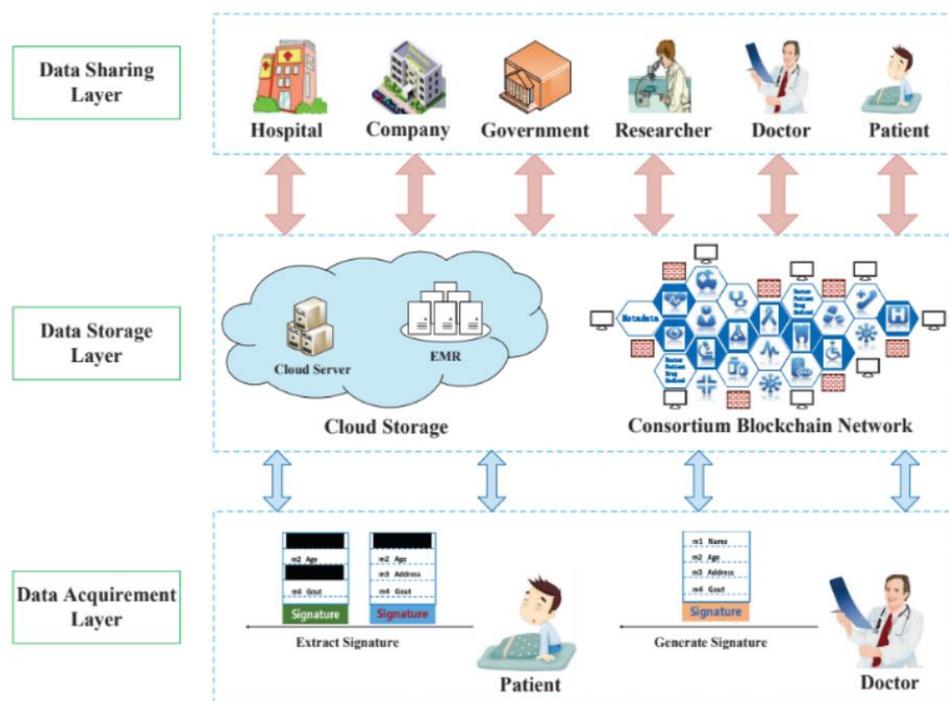


Figure 11; Proposition de modèle de [35].

Nous avons réussi à identifier 4 patterns dans ce modèle :

1. **Off-chain data storage** : les patients enregistrent leurs données et informations sur le cloud de manière encryté.
2. **Oracle** : L'oracle ici n'est clairement pas précisé, mais au vu du niveau de détail donné dans l'article, les docteurs doivent enregistrer les signatures dans la blockchain, nous avons considéré que ce pattern serait donc très utile pour leur permettre d'écrire sur la blockchain.
3. **Reverse oracle** : de même que pour l'oracle, nous avons considéré que ce pattern serait ainsi très utile pour récupérer les index stockés dans la blockchain afin de retrouver les données correspondantes dans le cloud.
4. **Identifiant registry** : un patient se rend chez son médecin qui intègre ses données médicales associées en tant que DME. Dès réception des DME, le patient le stocke dans le cloud et soumet les index des DME au docteur qui les enregistre sur la blockchain avec la liste des utilisateurs de données autorisés à les traiter.

Nous avons fourni, en **annexe 1, 2 et 3**, des architectures orientées patterns de ces modèles dans lequel nous faisons clairement apparaître la présence des patterns utilisés. Cela permet de mieux comprendre l'objectif de chaque partie de ces systèmes et de plus standardiser les solutions.

Ainsi, nous avons pu répondre à notre première question de recherche :

RR1 : *comme vu à la section précédente dans notre analyse quantitative, seuls deux articles parlent explicitement de pattern, tous les autres articles n'en font pas mention.*

Pour mettre en évidence le manque de présence explicite des patterns et pour montrer qu'ils sont pourtant bien utilisés, nous avons donc reproduit quelques architectures afin de les mettre en évidence.

Nous en concluons alors qu'une liste de patterns est bien présente dans les architectures des DSE et qu'ils peuvent être identifiés comme nous l'avons fait ici, mais uniquement, en ayant des connaissances préalables dessus.

*Ainsi, en nous basant sur la liste des 120 patterns issue de [9] et sur leurs définitions, nous avons réussi à identifier neuf patterns différents dans l'ensemble des architectures proposées dans ce corpus : **Decentralize Business Process, Encrypting on-chain Data, Identifier Registry, Inter-family communication, Minimize on-chain data, Off-chain data storage, Oracle, Reverse Oracle, Smart Contract Activities.***

Cela valide également notre deuxième hypothèse :

H2 : *Les patterns utilisés ne sont pas définis de manière explicite.*

C. Les patterns les plus utilisés

Après avoir recensé la liste des patterns utilisée dans les différentes architectures de ce corpus, nous les avons comptabilisés afin de connaître la réponse à notre seconde question de recherche :

QR2 : *Quels sont les patterns les plus utilisés dans ces architectures ?*

L'objectif étant de savoir s'il y a ou non un accord « implicite » dans la communauté pour réaliser des architectures de dossier de santé électronique basé sur la blockchain.

Étant donné que nous nous intéressons qu'à un cas d'étude précis, à savoir l'architecture des dossiers médicaux électronique, nous avons émis l'hypothèse suivante :

H3 : *Les patterns logiciels de la blockchain qui sont utilisés dans les différentes architectures sont toujours les mêmes. Il n'y a pas de consensus clairement défini et adopté.*

Pour répondre à cette question, nous avons comptabilisé l'ensemble des patterns identifiés par articles. Nous obtenons ainsi le graphique suivant :

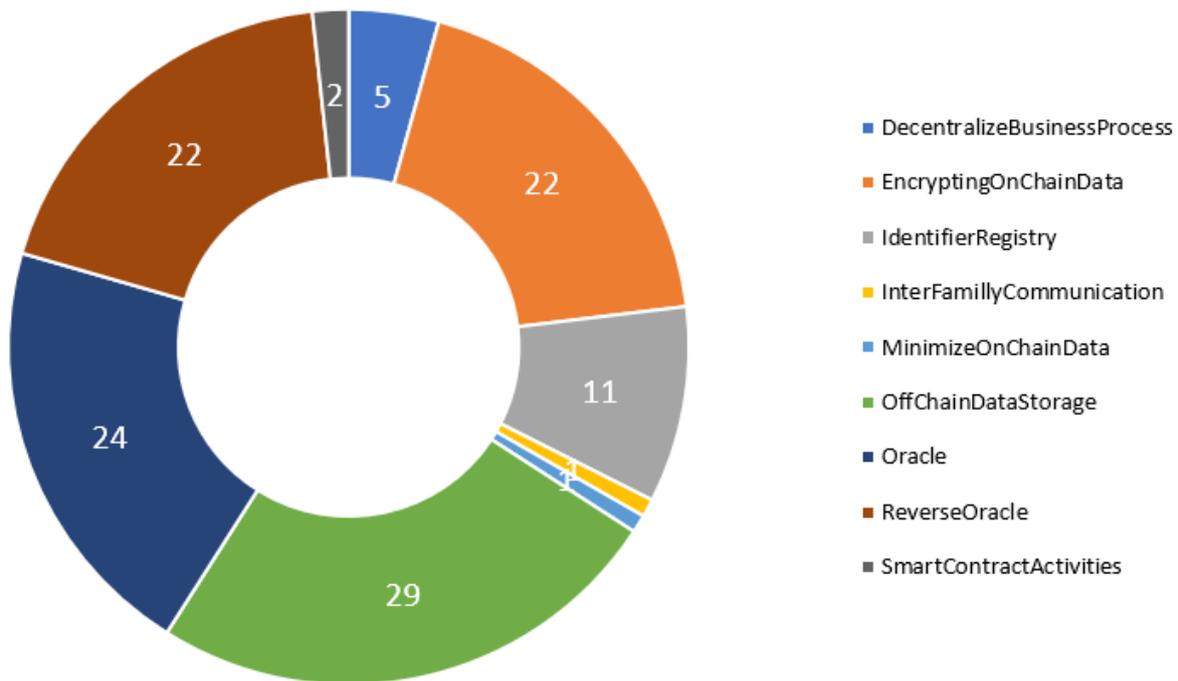


Figure 12: Répartition des patterns les plus utilisés.

Nous constatons que quasiment à l'unanimité, les chercheurs intègrent le pattern **Off-chain data storage** dans leur architecture. Pourtant, nous avons vu précédemment que seuls deux articles en font mention explicitement et parmi tous les articles.

Nous avons relevé trois moyens de stockage des données en dehors de la blockchain :

1. **IPFS** : *Inter Planetary File System (IPFS)* est un système de fichiers pair à pair qui peut non seulement stocker des fichiers dans divers formats, mais renvoie également la valeur de hachage du fichier actuel lorsque le fichier est téléchargé sur le système IPFS. Il suffit ensuite d'utiliser le code de hachage comme un index lors de l'accès au même fichier pour la prochaine fois. [37]. Cet index est par la suite stocké dans la blockchain.
2. **Cloud** : les environnements de *cloud computing* offrent une excellente opportunité d'adapter efficacement les services de santé en ligne dans différents scénarios. Il est considéré comme une plate-forme de stockage distribué et flexible accessible à tout moment et n'importe où sur demande [38].
3. **Une base de données en local** : pour sa simplicité et pour avoir un total contrôle sur les données stockées. Ce qui implique de devoir gérer l'hébergement, la maintenance et la sécurité de ces données.

Les données étant stockées hors chaîne, un processus de hachage est souvent utilisé avant leur enregistrement afin de préserver leur confidentialité.

Les principales raisons à l'utilisation de tels systèmes de stockage dans les différentes architectures sont [33] :

- Pouvoir surmonter les limitations d'espace de stockage et les performances
- Permettre une évolutivité et surtout pour réduire les coûts de transaction et le temps de réponse

qui sont les principales contraintes d'utilisation de la blockchain.

Ces moyens de stockage peuvent également être utilisés sans la blockchain, mais les systèmes de gestion peuvent être exposés à des abus, des fuites, des pertes ou des vols. [39]. Par exemple, les DSE peuvent être supprimés ou falsifiés par des intrus.

Ils peuvent aussi être trafiqués donnant des avantages aux compagnies d'assurance ou subir des dissimulations de fautes professionnelles médicales (par exemple, diagnostic erroné et diagnostic tardif).

Ainsi l'association de la blockchain et de ces moyens de stockage peut parer aux inconvénients de chacun.

Nous remarquons par ailleurs que le pattern **Encrypting on-chain data** est aussi largement utilisé, dans 22 architectures.

Un des points majeurs à respecter lors de l'utilisation des dossiers de santé électronique est de garantir la confidentialité et l'intégrité des données patient. Pour cela nous venons de voir qu'il existe deux moyens de stockage des données : *on-chain* (dans la blockchain) et *off-chain* (en dehors de la blockchain). Que ce soit avec l'un ou avec l'autre, l'ensemble des articles recommande de crypter les données avant leur enregistrement avec différents types d'algorithmes comme le SHA-256 [40]. Ainsi seul le hash est stocké sur la blockchain ou simplement un index (lui-même haché ou non).

Dans le même ordre d'idées, nous avons le **Minimize on-chain data** qui consiste à réduire les coûts de gaz en stockant les données essentiellement hors chaîne. Nous l'avons relevé seulement lorsque l'auteur stipule clairement cette intention comme [33]. Il est fortement lié avec le pattern **Off-chain data storage** puisque toutes les données qui ne sont pas stockées sur la blockchain seront stocké en dehors.

Les patterns **Oracle** et **Reverse Oracle** ne sont absolument pas cités dans les articles, mais nous les jugeons très utiles dans plus de 20 articles de notre corpus. En effet ces architectures communiquent avec la blockchain pour y insérer des données ou en lire. Pour ce faire, des contrats intelligents sont généralement utilisés et ils ont besoin d'information extérieure pour exécuter leurs instructions.

Environ un tiers des articles ont intégré le pattern **Identifier Registry**. Ils ont fait le choix de stocker les données en dehors de la blockchain, souvent en utilisant le système **IPFS** ou le **Cloud** et en les indexant à l'aide d'un identifiant ou d'un mot clés sur la blockchain.

Le **Smart contract activities** se retrouvait principalement dans les architectures nécessitant un tiers pour valider certaines transactions.

Enfin, **Inter-family communication** tout de même présent une fois afin de faire communiquer plusieurs contrats intelligents ensemble [41].

Ainsi, nous pouvons valider notre hypothèse **H3**, car nous avons identifié neuf patterns présents dans ce corpus et parmi ces patterns la plupart des articles utilisent les mêmes, comme notamment le **Off-chain data storage**.

De plus, nous n'avons identifié aucun consensus au sujet des patterns utilisés dans les architectures des dossiers médicaux électronique et que plusieurs papiers cherchent à répondre à une même problématique sans se rendre compte que certains patterns ont déjà été étudiés et réalisés pour cela.

Nous répondons alors à notre deuxième question de recherche de la manière suivante :

RR2 : *Nous avons constaté que le pattern **Off-chain data storage** est le plus utilisé et le seul qui est explicitement mentionné. Il permet de réduire les coûts de stockage de la blockchain tout en maintenant l'intégrité des données. Ensuite, nous avons le **Encrypting on-chain data** puisqu'une partie des données est tout de même stockée sur la blockchain et toujours de manière encryptée.*

*Enfin, nous avons jugé fortement utile d'intégrer l'**Oracle** et le **Reverse oracle** même s'ils ne sont pas identifiables afin de faciliter les échanges d'information entre la blockchain et le monde extérieur.*

Ainsi, nous remarquons les patterns les plus utilisés sont ceux concernant le stockage et la manipulation des données tout en garantissant leurs sécurités et leurs confidentialités.

D. L'utilisation de la blockchain dans les dossiers de santé électronique

Le nombre de dossiers sur la santé personnelle croît de façon exponentielle avec l'essor de l'informatique mobile et omniprésente. Cette tendance se caractérise par la technologie informatique portable et divers types de capteurs liés au domaine de la santé [42]. Ainsi, l'ensemble des articles de notre corpus ont été rédigés avec un objectif commun : proposer un modèle qui permet de répondre aux problèmes actuels des dossiers de santé électronique.

Nous avons relevé les problèmes les plus importants et qui revenaient le plus souvent dans les différents articles :

- Garantir l'intégrité des enregistrements de données et améliorer l'interopérabilité des systèmes de santé électroniques en suivant tous les événements qui surviennent dans les bases de données. Les systèmes d'enregistrements des données électroniques nécessitent une protection contre l'utilisation abusive des données [25].
- Les systèmes de dossiers médicaux électroniques (DME) sont confrontés à des problèmes cruciaux concernant la sécurité, l'accessibilité et la gestion des données. Un grand nombre de menaces de sécurité liées à la vie privée des patients impliquent un accès non autorisé aux dossiers médicaux, une mauvaise utilisation des rapports de maladie des patients [3, 24].
- Il n'existe actuellement aucun système fiable de partage et de stockage des données médicales dans la chaîne de valeur de la santé. Par conséquent, aucune plateforme

n'est utilisée pour suivre la traçabilité des patients sur l'ensemble de la chaîne de soins [42].

- Les DSE basés sur le *cloud* résolvent le problème du partage d'informations dans les DSE traditionnels. Cependant, les DSE basés sur le *cloud* souffrent d'un problème centralisé, c'est-à-dire un centre de services *cloud* et un centre de génération de clés [43].
- Les DME sont fragmentés dans les hôpitaux décentralisés, ce qui entrave le partage des données et met en danger la vie privée des patients [35].
- Problème du partage des données, de l'interopérabilité et de la sécurité des données [44].
- Les systèmes de DSE existants manquent le plus souvent d'une sécurité appropriée, d'un contrôle d'accès confié et de la gestion des problèmes de confidentialité et de secret et des défis dans les infrastructures hospitalières actuelles [22].
- Les systèmes de dossiers médicaux électroniques (DME) sont confrontés à des problèmes cruciaux concernant la sécurité, l'accessibilité et la gestion des données. Un grand nombre de menaces de sécurité liées à la vie privée des patients impliquent un accès non autorisé aux dossiers médicaux, une mauvaise utilisation des rapports de maladie des patients, etc. [3].

De plus, tous ces articles ont en commun le fait de vouloir utiliser la blockchain pour résoudre ces problèmes.

La blockchain est devenue un domaine de recherche populaire depuis son introduction, car ses avantages ont été constatés dans diverses industries. Cela pourrait grandement profiter au secteur de la santé parce qu'elle offre l'anonymat, l'immutabilité, la décentralisation des données et pourrait être utilisée pour améliorer les niveaux de sécurité.

Les données de santé en ligne peuvent être stockées dans des blocs médicaux sécurisés pour affirmer la confidentialité et l'intégrité des données.

En raison de sa nature décentralisée, la blockchain pourrait être utilisée pour atteindre un certain niveau de sécurité sans compter sur un autre intermédiaire.

Dans [24], l'auteur rapporte les derniers travaux de recherche basés sur la blockchain dans le domaine médical et notamment dans l'échange de données médicales.

Cela confirme donc notre quatrième hypothèse, à savoir :

H4 : La blockchain est parfaitement adaptée dans les architectures des dossiers médicaux électroniques.

Nous devons noter cependant qu'il existe quand même quelques contraintes à son utilisation comme les coûts des transactions qui peuvent devenir très importants en fonction de la quantité de données à traiter. Mais comme expliqué précédemment, ce problème peut être

évité grâce à certains patterns comme le **Off-chain data storage** ou le **Minimize on-chain data**, etc.

Nous souhaitons maintenant savoir de quelle manière la blockchain était utilisée et si certains systèmes blockchain sont plus recommandés que d'autres dans ce type d'architecture afin de répondre à notre question de recherche :

QR4 : Quels sont les systèmes blockchain utilisés dans les architectures des dossiers de santé électronique ?

Lors de notre phase d'analyse, nous nous sommes rendu compte que les systèmes blockchain ne sont pas forcément définis dans les différents papiers de ce corpus. En effet plus de la moitié des articles ne précisent pas clairement le système blockchain utilisé, mais simplement son type.

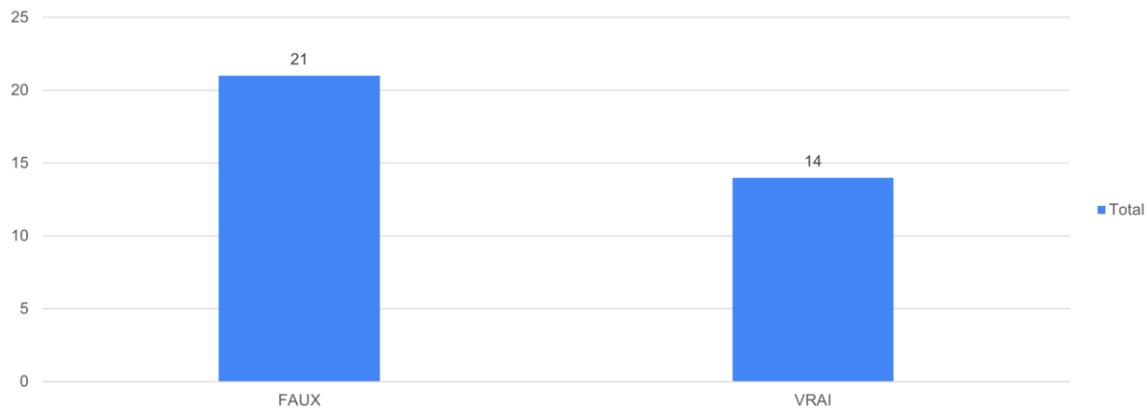


Figure 13: Répartition des articles qui définissent les systèmes blockchain utilisés.

Nous avons alors subdivisé notre question de recherche en deux :

QR4.1 : Quels sont les systèmes blockchain utilisés dans les architectures des dossiers de santé électronique ?

QR4.2 : Quels sont les types blockchain utilisés dans les architectures des dossiers de santé électronique ?

1) Les systèmes blockchain utilisés

Pour pouvoir identifier les systèmes blockchain utilisés, nous avons préalablement listé les systèmes blockchain existant les plus couramment utilisés :

- **Bitcoin** : c'est la Blockchain originelle dont le consensus repose sur la preuve de travail (PoW : proof of work) des mineurs [4].
- **Ethereum** : permet, au-delà des fonctions de Bitcoin, de créer des contrats intelligents (*smart-contract*), c'est-à-dire des comptes pouvant transporter des *ethers* (*crypto-monnaie*) pilotés par du code informatique. Il existe deux consensus dans cette blockchain *proof of work* (PoW) et *proof of stake* (PoS) ce qui divise cette blockchain en deux grandes catégories *Ethereum PoW* et *Ethereum PoS* [57].
- **Corda** : C'est un protocole d'échange d'informations spécialement conçu pour répondre aux besoins des sociétés financières. Le *framework* de Corda rend tout à fait possible la création d'une DLT (*Distributed Ledger Technologies*) pour n'importe quel cas d'usage, y compris extérieur à la finance. Son utilisation sera néanmoins peut-être moins adaptée que d'autres *frameworks* DLT plus complets.
- **Hyperledger** : est une plateforme open source de développement de Blockchain. Son algorithme de consensus est le Raft. Les projets *Hyperledger* se font sur un réseau privé sur ce que l'on appelle vulgairement des « *permissioned blockchains* ».

Pour identifier les systèmes blockchains utilisés, nous avons classé les articles par système lorsqu'ils sont cités explicitement et dans 'autres' pour le reste.

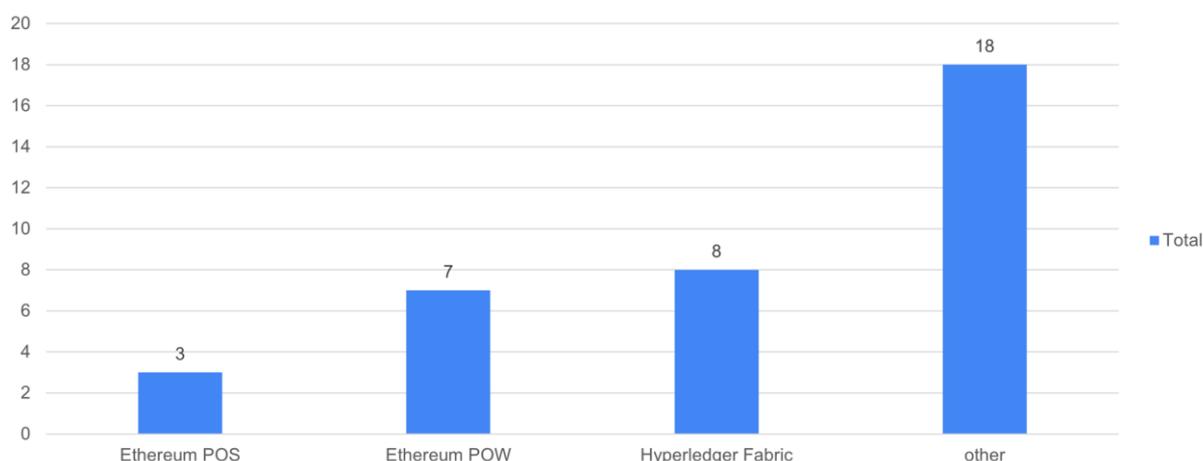


Figure 14: Répartition des systèmes blockchain utilisés.

Nous constatons que la majorité des systèmes blockchains se trouvent dans la catégorie autre. Cela est dû au fait que soit les chercheurs ont créé leurs propres blockchains, soit ils ne donnaient pas suffisamment d'information dans leurs papiers pour en déduire quel système ils utilisent.

On remarque tout de même que 8 études ont réalisé leur architecture en se basant sur la blockchain **Hyperledger**. Enfin, le reste est basé sur **Ethereum** en fonction du type de consensus adopté. Les autres systèmes ne sont pas évoqués.

RR4.1 : Nous avons remarqué que plus de la moitié des articles ne présentent pas les systèmes blockchain qu'ils utilisent. Les systèmes définis connus que nous avons pu relever sont **Hyperledger fabric** et **Ethereum**.

2) Les types de blockchain utilisés

À défaut de pouvoir identifier totalement les systèmes blockchain utilisés, nous avons remarqué que pratiquement à l'unanimité, les chercheurs précisent de manière explicite le type de blockchain utilisé. Nous avons donc voulu savoir lesquels sont les plus utilisés et si l'utilisation de certains types de blockchain ont une quelconque influence sur l'utilisation de tel ou tel pattern.

Il existe trois principaux types de blockchain [52] :

- **Public ou permissionless** : Les blockchains publiques ou sans permission sont décentralisées et ne nécessitent aucun tiers de confiance. Leur principale caractéristique est qu'elles sont accessibles à tous. La plus connue est celle du Bitcoin, mais il en existe une multitude. Bien que sécurisées, les blockchains publiques n'offrent pas la même flexibilité qu'une blockchain privée.
- **Private ou permissioned** : Les réseaux de blockchain privés sont ceux où le contrôle est réduit à une seule entité, responsable de la maintenance de la chaîne. Il octroie des autorisations aux utilisateurs qui souhaitent participer à la proposition de transactions et de l'acceptation des blocs. Certains ne les classent pas dans la même catégorie et les considèrent comme deux types de blockchain distinct [42].
- **Hybrid ou consortium** : les blockchains hybrides ne sont pas ouvertes à la participation du public, mais un certain nombre d'organisations, d'entités ou d'entreprises. Ils sont responsables de la gestion du réseau dans son ensemble et de la conservation de copies synchronisées du registre.

Ainsi, nous obtenons le diagramme suivant :

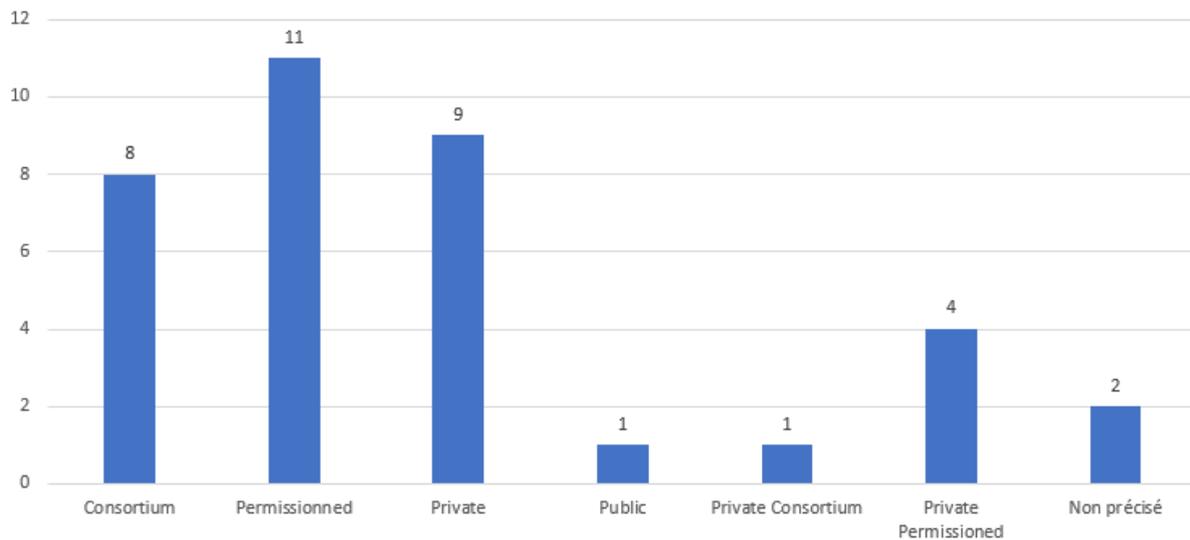


Figure 15: Répartition des types de blockchain utilisés.

Nous constatons que type **public** n'est présent qu'une seule fois [34] parmi toutes les propositions de ce corpus et ils justifient leur choix en disant qu'une blockchain **public** comme **3thereum** utilise un mécanisme de consensus *Proof-of-Work* qui est le mécanisme de consensus le plus largement déployé dans les technologies de blockchain existantes. En revanche, nous avons une grande majorité de blockchain de type **private** et **permissionned** et parfois même les deux en même temps. Les auteurs justifient leurs choix par le fait que tout le monde ne doit pas avoir accès aux traitements des données patients et que parmi les personnes qui y ont accès, il peut y avoir des restrictions. Nous pouvons en déduire que cette catégorie de blockchain est plus adaptée pour les architectures des dossiers de santé électronique. Cependant, nos recherches sur cette partie ne nous permettent pas de conclure si un type de blockchain est privilégié par rapport à un autre pour l'utilisation de certains patterns.

RR4.2 : Les auteurs se sont plus attardés sur le type de blockchain choisit et mettent avant les types **Private**, **Permissionned** et **Consortium** qui favorisent davantage la sécurité et la confidentialité des données.

E. L'utilisation des patterns logiciels architecturaux

QR3 : En quoi l'utilisation de patterns logiciels architecturaux peut être bénéfique ?

Nous aurions tendance à penser que l'utilisation des patterns n'est pas forcément bénéfique ou utile, car au vu de nos résultats, très peu d'articles en parlent de manière explicite.

Nos articles sont axés sur un cas d'étude précis, à savoir l'utilisation de la blockchain dans les architectures des dossiers médicaux électroniques. Et, étant donné que les technologies de la blockchain en sont à un stade précoce, il manque une vision systématique et holistique de la conception de systèmes logiciels utilisant la blockchain [20].

En revanche, de manière générale, l'utilisation de pattern, dans beaucoup d'autres domaines comme les programmations et les langages orientés objet [58], les systèmes de micro-

services [59], etc., est totalement admis et fortement recommandé. Elle permet par-exemple de résoudre de nombreux problèmes quotidiens auxquels sont confrontés les concepteurs orientés objet [45].

Étant donné que nombreux chercheurs considèrent la blockchain comme faisant partie d'un système plus vaste qui nécessite des modèles d'utilisation de la blockchain dans la conception de leur architecture logicielle. Ils se lancent dans la réalisation d'une collection de pattern comme [20] ou encore d'une taxonomie de patterns comme [9] relatif à la blockchain et qui permettront par la suite de les utiliser.

La blockchain est une solution prometteuse, mais son appréhension et son intégration peuvent parfois être fastidieuses. Ainsi, l'utilisation de patterns logiciels est une solution intéressante pour assurer la haute qualité et l'efficacité des applications décentralisées nouvellement (et prochainement) construites à l'aide de la blockchain. Ils garantissent que les problèmes courants dans un contexte donné sont résolus avec des solutions largement testées. Cela permettra également aux architectes logiciels de bénéficier d'un cadre pour la conception et la mise en œuvre d'applications basées sur la blockchain.

RR3 : *de manière générale, l'utilisation de pattern, dans n'importe quel domaine, est vivement recommandé. Elle permet d'accélérer les processus de développement et de réalisation en se basant sur des concepts et des systèmes déjà validés et admis par la communauté. Ils permettent de répondre à des problèmes connus, ils sont plus facilement reconnaissables et déjà documentés. Néanmoins, nous pouvons supposer qu'il existe quelques raisons de ne pas les utiliser qui justifie leur absence dans la majorité des articles de ce corpus. Comme le fait que cela demande des connaissances et une certaine compréhension de ces patterns avant leurs intégrations. De plus, une utilisation abusive de patterns peut également nuire à une application, car ça pourrait trop la complexifier et l'alourdir.*

Discussion

L'utilité d'un pattern logiciel est évidente. Les patterns logiciels permettent notamment d'accélérer le processus de développement. Ils fournissent des paradigmes de développement qui ont fait leurs preuves, ce qui aide à gagner du temps sans avoir à réinventer des modèles chaque fois qu'un problème apparaît.

Comme les patterns logiciels sont créés dans le but de régler des problèmes connus, ceux-ci peuvent être prédits avant même de devenir visibles pendant le processus de mise en œuvre. N'ayant aucune obligation en place, les organisations et les entreprises réalisent leurs architectures sans forcément adopter l'intégration de pattern logiciel. La plupart se contentent simplement d'identifier les problèmes qu'ils ont à résoudre et de trouver leurs propres solutions à cela, sans chercher à savoir si ces solutions n'ont pas déjà été trouvées, ni de tenter de les standardiser pour d'autres.

Ainsi, dans cette section, nous allons tenter de répondre de manière générale à notre question de recherche centrale pour donner suite à notre SLR :

De quelle manière les patterns logiciels architecturaux basés sur la blockchain sont utilisés dans les systèmes actuels de dossier de santé électronique ?

La blockchain, une technologie prometteuse pour les DSE

Notre SLR nous permet de proposer que l'intégration de la blockchain dans l'architecture des dossiers de santé électronique soit une solution très prometteuse. Différentes propositions sont faites pour savoir quel système blockchain est utilisé (***Ethereum, Hyperledger, ...***) mais de manière générale les blockchains de type ***private*** et ***permissioned*** sont privilégiés. L'ensemble des articles de notre corpus s'accorde pour prouver que la blockchain peut parer aux différents problèmes qui ralentissent l'évolution des dossiers de santé électronique. Les nombreuses études et analyses qui ont été faites dans ce corpus et les résultats obtenus nous permettent de valider cette proposition.

La présence de patterns de manière implicite

À la suite de notre analyse de la qualité des études sélectionnées, nous avons constaté que toutes les architectures présentes dans ce corpus utilisent des patterns sans en faire mention explicitement ou sans même le savoir, à l'exception de 2 articles. Nous remarquons donc, que les chercheurs, ne font pas de l'utilisation des patterns leurs priorités et négligent leurs usages en second plan.

Des patterns communs à l'ensemble des architectures proposées.

Nous avons également remarqué que parmi l'ensemble des architectures proposées une poignée de pattern est utilisé et identifiable : ***Decentralize Business Process, Encrypting on-chain Data, Identifier Registry, Inter-family communication, Minimize on-chain data, Off-chain data storage, Oracle, Reverse Oracle, Smart Contract Activities***. Au minimum 22 études sur les 36 sélectionnées utilisent les mêmes patterns et ce chiffre peut aller jusqu'à 28 sans pour autant qu'il y ait de consensus clairement défini et adopté. On constate alors de nombreuses répétitions dans les articles de recherche qui pourraient être évité si la communauté se met d'accord pour l'acceptation d'un ou plusieurs patterns dans ce type d'architecture pour ce domaine d'application.

Le pattern **Off-chain data storage**, une solution qui fait quasiment l'unanimité.

Un des exemples les plus parlants à ces répétitions est le pattern **Off-chain data storage**. Comme nous l'avons expliqué précédemment, ce pattern est énormément utilisé (souvent associé au **Minimize on-chain data** ou à l'**Identifiant Registry**) et c'est le seul pattern qui est cité explicitement. Les raisons qui justifient son utilisation sont, elles aussi, clairement définies et identiques à chaque fois : la préservation de la confidentialité et de l'intégrité des données même en dehors de la blockchain, l'anonymat des patients, l'amélioration de l'évolutivité et de la vitesse de la Blockchain, les gains de coût...

De nombreux moyens de stockage externes peuvent être envisageables (**cloud, IPFS, base de données, local**) et les chercheurs peuvent rester libres sur ce choix.

Nous pourrions le proposer comme étant une bonne pratique à adopter dans les prochaines architectures des dossiers de santé électronique au vu des résultats obtenus préalablement, même s'il y a quelques risques à prendre en compte.

Les avantages d'utiliser des patterns logiciels dans les architectures DSE.

Nous avons vu auparavant que même si la présence des patterns se fait de manière implicite, ils sont bien présents. Il existe plusieurs avantages à cela, qui sont pour la plupart des avantages communs à l'utilisation des patterns en général :

- L'intégration de la blockchain peut paraître assez vaste et complexe, ainsi l'utilisation de patterns logiciels peut grandement la faciliter.
- Les patterns logiciels sont des solutions standard qui ont fait leurs preuves qui permettent une économie de temps et d'argent.
- Un vocabulaire de conception commun qui facilite la discussion et la communication entre les différentes parties impliquées dans la réalisation de ces architectures.
- Une compréhension simplifiée et déjà documentée de l'architecture.

Les limites à l'utilisation des patterns.

Bien sûr, l'utilisation de patterns logiciels a également quelques limites :

- L'utilisation de pattern logiciel nécessite de solides connaissances et compréhension de ces derniers avant de les intégrer. Un pattern a généralement pour but de répondre à un ou plusieurs problèmes, mais ne résout pas tous les problèmes
- L'abus de patterns dans une même architecture peut également être une mauvaise pratique qui risque de complexifier l'architecture et sa compréhension.
- Individuellement, chaque pattern a ses avantages et inconvénients.

Conclusion

La numérisation des données de santé patient et le développement des dossiers de santé électronique (DES) sont en plein essor. Cependant, quelques obstacles freinent encore leur mise en place complète. Beaucoup de chercheurs ont donc envisagé d'utiliser la blockchain pour parer à ses différents problèmes. Il existe néanmoins différents moyens d'intégrer cette nouvelle technologie dans les architectures des DSE en fonction des objectifs à atteindre.

C'est pourquoi, comme dans beaucoup d'autres domaines, des patterns logiciels architecturaux de la blockchain ont été mis en place et admis par la communauté scientifique. Ainsi, notre revue systématique de littérature a pour objectif d'analyser de quelle manière les patterns logiciels architecturaux basés sur la blockchain sont utilisés dans les systèmes actuels de dossier de santé électronique (DSE). À ce jour, aucune autre étude connue ayant déjà effectué ce travail de recherche n'est connue pour ce domaine d'application.

Pour mener à bien ce travail, nous avons sélectionné un corpus de 36 études proposant des modèles d'architecture basé sur la blockchain pour les dossiers de santé électronique.

Nous avons réalisé une analyse quantitative et qualitative de l'ensemble de ces articles. Ce qui nous a permis de comprendre dans un premier temps que les patterns logiciels architecturaux de la blockchain ne sont pratiquement pas présents dans ce corpus. À l'exception de deux études, aucun article ne cite ni ne définit les patterns utilisés pour leur modèle.

Pourtant, nous avons tout de même réussi à identifier neuf patterns parmi l'ensemble des architectures proposées. Un de ces patterns, est utilisé quasiment à l'unanimité dans ce corpus, le **Off-chain data storage** sans pour autant être mis en avant ni clairement défini.

Nous avons également constaté que beaucoup d'articles réutilisent les mêmes patterns : quatre patterns ont été relevés au minimum 22 fois sur 36 articles.

Les types de blockchains privilégiés sont les **Private** et **Permissioned** et systèmes blockchain connus les plus utilisés sont **Ethereum** et **Hyperledger**.

Ainsi, nous en concluons qu'il n'y a pas de consensus clairement défini sur l'utilisation de ces patterns. La plupart des études se servent des patterns sans forcément le savoir ou sans les mettre en avant. Ce qui est dommage puisque leurs travaux ne permettent pas de faciliter leur mise en place aux d'autres chercheurs en standardisant ces solutions et imposent ainsi une répétition des informations dans les différents articles.

Cette SLR aura donc permis de faire prendre conscience à la communauté scientifique actuelle, que la présence des patterns utilisés n'est absolument pas mise en avant. Par conséquent, dans les travaux futurs, l'objectif d'un grand nombre de chercheurs sera de mettre en œuvre les solutions proposées de ce corpus (ou d'en proposer d'autre) mais en faisant cette fois clairement apparaître les patterns utilisés et en le justifiant. Pour ce faire, une taxonomie [9] relevant l'ensemble des patterns admis de la blockchain a été publié cette année afin de permettre à tous de connaître les patterns existants et les problème auxquels ils tentent de répondre.

Déclaration d'intérêts concurrents

Les auteurs déclarent ne pas avoir d'intérêts financiers concurrents ou de relations personnelles connus qui auraient pu sembler influencer les travaux rapportés dans cet article.

Références

- [1] Guo, H., Li, W., Nejad, M., & Shen, C.-C. (2019). Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture. 2019 IEEE International Conference on Blockchain (Blockchain).
- [2] <https://www.ibm.com/fr-fr/topics/benefits-of-blockchain>
- [3] Al Mamun, A., Faruk Jahangir, Md. U., Azam, S., Kaiser, M. S., & Karim, A. (2020). A Combined Framework of InterPlanetary File System and Blockchain to Securely Manage Electronic Medical Records. Proceedings of International Conference on Trends in Computational and Cognitive Engineering, 501–511.
- [4] S.Nakamoto, Bitcoin: a peer-to-peer electronic cash system, Decentralized Bus. Rev. (2008), 21260
- [5] Sarmah, s. (2018). Understanding Blockchain Technology. 8. 23-29.
- [6] C. Alexander, S. Ishikawa, M. Silverstein, et al.. A Pattern Language: Towns, Buildings, Construction, Oxford university press, New York, NY, USA, 1997.
- [7] D Taibi, V Lenarduzzi, Claus Pahl, Architectural Patterns for Microservices: A Systematic Mapping Study. CLOSER 2018: Proceedings of the 8th International Conference on Cloud Computing and Services Science; Funchal, Madeira, Portugal, 19-21 March 2018; Funchal, Madeira, Portugal., SCITEPRESS, Setúbal, Portugal, 2018, pp. 221-232.
- [8] S. Qanbari et al., "IoT Design Patterns: Computational Constructs to Design, Build and Engineer Edge Applications," 2016 IEEE First International Conference on Internet-of-Things Design and Implementation (IoTDI), 2016, pp. 277-282.
- [9] N. Six, N. Herbaut, C. Salinesi
Blockchain software patterns for the design of decentralized applications: a systematic literature review
Blockchain: Res. Appl., 3 (2) (2022), Article 100061
- [10] Les dossiers médicaux électroniques et l'importance de la manière de les documenter
Organisation panaméricaine de la Santé.
Boîte à outils de transformation numérique OPS/EIH/IS/21-022.
Monography Fr | PAHOIRIS | ID: phr-55411
- [11] Kai Petersen, Sairam Vakkalanka, Ludwik Kuzniarz,
Guidelines for conducting systematic mapping studies in software engineering: An update, Information and Software Technology, Volume 64, 2015, Pages 1-18, ISSN 0950-5849,
- [12] Mackenzie, Heather & Dewey, Ann & Drahot, Amy & Kilburn, Sally & Kalra, Paul & Fogg, Carole & Zachariah, D.. (2012). Systematic reviews: what they are, why they are important, and how to get involved. Journal of Clinical and Preventive Cardiology. 1.
- [13] Kitchenham, Barbara & Charters, Stuart. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. 2.

- [14] <https://scholar.miage.dev/>
- [15] <https://parsif.al/>
- [16] Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z (2020) Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLOS ONE 15(12): e0243043.
- [17] Martinez, A., Molina, C., & Subauste, D. (2020). Electronic Medical Records Management in Health Organizations using a Technology Architecture based on Blockchain. 2020 IEEE ANDESCON.
- [18] Zhang, J., Li, Z., Tan, R., & Liu, C. (2021). Design and Application of Electronic Rehabilitation Medical Record (ERMR) Sharing Scheme Based on Blockchain Technology. BioMed Research International, 2021, 1–12.
- [19] Niu, S., Chen, L., Wang, J., & Yu, F. (2020). Electronic Health Record Sharing Scheme With Searchable Attribute-Based Encryption on Blockchain. IEEE Access, 8, 7195–7204.
- [20] Xiwei Xu, Cesare Pautasso, Liming Zhu, Qinghua Lu, and Ingo Weber. 2018. A Pattern Collection for Blockchain-based Applications. In Proceedings of the 23rd European Conference on Pattern Languages of Programs (EuroPLoP '18). Association for Computing Machinery, New York, NY, USA, Article 3, 1–20.
- [21] Zhao, Y., Cui, M., Zheng, L., Zhang, R., Meng, L., Gao, D., & Zhang, Y. (2019). Research on electronic medical record access control based on blockchain. International Journal of Distributed Sensor Networks, 15(11), 155014771988933.
- [22] Uddin, M., S. Memon, M., Memon, I., Ali, I., Memon, J., Abdelhaq, M., & Alsaqour, R. (2021). Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. Computers, Materials & Continua, 68(2), 2377–2397.
- [23] Xia, Q., Sifah, E., Smahi, A., Amofa, S., & Zhang, X. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information, 8(2), 44.
- [24] Ray, P. P., Chowhan, B., Kumar, N., & Almogren, A. (2021). BioTHR: Electronic Health Record Servicing Scheme in IoT-Blockchain Ecosystem. IEEE Internet of Things Journal, 8(13), 10857–10872.
- [25] Yang, G., Li, C., & Marstein, K. E. (2019). A blockchain-based architecture for securing electronic health record systems. Concurrency and Computation: Practice and Experience, 33(14). Portico.
- [26] Wang, Y., & He, M. (2021). CPDS: A Cross-Blockchain Based Privacy-Preserving Data Sharing for Electronic Health Records. 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA).
- [27] Kiran Dash, K., Nayak, B., & Kumar Mohanta, B. (2021). An Approach to Securely Store Electronic Health Record(EHR) Using Blockchain with Proxy Re-Encryption and Behavioral Analysis. Advances in Intelligent Systems and Computing, 415–423.
- [28] <http://portal.core.edu.au/conf-ranks/>
- [29] <http://portal.core.edu.au/jnl-ranks/>
- [30] Wieringa, R., Maiden, N., Mead, N. et al. Requirements engineering paper classification and evaluation criteria: a proposal and a discussion. Requirements Eng 11, 102–107 (2006).

- [31] Li, J. (2020). A New Blockchain-based Electronic Medical Record Transferring System with Data Privacy. 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT).
- [32] Alexaki, S., Alexandris, G., Katos, V., & Petroulakis, N. E. (2018). Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions. 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD).
- [33] Riadi, I., Ahmad, T., Sarno, R., Purwono, P., & Ma'arif, A. (2022). Developing Data Integrity in an Electronic Health Record System using Blockchain and InterPlanetary File System (Case Study: COVID-19 Data). *Emerging Science Journal*, 4, 190–206.
- [34] Rahman, M. S., Khalil, I., Mahawaga Arachchige, P. C., Bouras, A., & Yi, X. (2019). A Novel Architecture for Tamper Proof Electronic Health Record Management System using Blockchain Wrapper. Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure - BSCI '19.
- [35] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., & Guizani, M. (2018). BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. 2018 IEEE Global Communications Conference (GLOBECOM).
- [37] Wu, S., & Du, J. (2019). Electronic medical record security sharing model based on blockchain. Proceedings of the 3rd International Conference on Cryptography, Security and Privacy - ICCSP '19.
- [38] Ali, A., Rahim, H. A., Ali, J., Pasha, M. F., Masud, M., Rehman, A. U., Chen, C., & Baz, M. (2021). A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority. *Applied Sciences*, 11(21), 9999.
- [39] Zhang A, Lin X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J Med Syst*. 2018 Jun 28;42(8):140.
- [40] Hashim, F., Shuaib, K., & Sallabi, F. (2021). MedShard: Electronic Health Record Sharing Using Blockchain Sharding. *Sustainability*, 13(11), 5889.
- [41] Ajayi, O., Abouali, M., & Saadawi, T. (2020). Blockchain Architecture for Secured Inter-healthcare Electronic Health Records Exchange. *Advances in Intelligent Systems and Computing*, 161–172.
- [42] Centobelli, P., Cerchione, R., & Riccio, E. (2021). A novel architecture for enhancing Electronic Health Record interoperability: A Blockchain-based approach. 2021 IEEE Technology & Engineering Management Conference - Europe (TEMSCON-EUR).
- [43] Tang, F., Ma, S., Xiang, Y., & Lin, C. (2019). An Efficient Authentication Scheme for Blockchain-Based Electronic Health Records. *IEEE Access*, 7, 41678–41689.
- [44] Sari, P. K., & Yazid, S. (2020). Design of Blockchain-based Electronic Health Records for Indonesian Context: Narrative Review. 2020 International Workshop on Big Data and Information Security (IW BIS).
- [45] Gamma, E., Helm, R., Johnson, R., Vlissides, J. M. (1994). *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley Professional. ISBN: 0201633612
- [46] Adlam, R., & Haskins, B. (2019). A Permissioned Blockchain Approach to the Authorization Process in Electronic Health Records. 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC).
- [47]

- [48] KalaiPriya, R., Devadharshini, S., Rajmohan, R., Pavithra, M., & Ananthkumar, T. (2020). Certain Investigations on Leveraging Blockchain Technology for Developing Electronic Health Records. 2020 International Conference on System, Computation, Automation and Networking (ICSCAN).
- [49] Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain. *Sensors*, 20(10), 2913.
- [50] Niu, S., Li, W., & Liu, W. (2020). Electronic Health Record Data Sharing Cryptographic Algorithm Based on Blockchain. *Artificial Intelligence and Security*, 363–375.
- [51] Alfaidi, A., & Chow, E. (2020). Health Record Chain (HRC): Implementation of Mobile Healthcare system using Blockchain to enhance Privacy of Electronic Health Record EHR. 2020 International Conference on Computational Science and Computational Intelligence (CSCI).
- [52] Gutiérrez, O., Romero, G., Pérez, L., Salazar, A., Charris, M., & Wightman, P. (2020). HealthyBlock: Blockchain-Based IT Architecture for Electronic Medical Records Resilient to Connectivity Failures. *International Journal of Environmental Research and Public Health*, 17(19), 7132.
- [53] Arul, P., & Renuka, S. (2021). Hyperledger blockchain based secure storage of electronic health record system in edge nodes. *Journal of Physics: Conference Series*, 2115(1), 012034.
- [54] Mahore, V., Aggarwal, P., Andola, N., Raghav, & Venkatesan, S. (2019). Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain. 2019 IEEE Conference on Information and Communication Technology.
- [55] Guo, R., Shi, H., Zhao, Q., & Zheng, D. (2018). Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems. *IEEE Access*, 6, 11676–11686.
- [56] Beinke, J. H., Fitte, C., & Teuteberg, F. (2019). Towards a Stakeholder-Oriented Blockchain-Based Architecture for Electronic Health Records: Design Science Research Study. *Journal of Medical Internet Research*, 21(10), e13585.
- [57] V. Buterin, Ethereum white paper, 2013. Available online: <https://github.com/ethereum/wiki/wiki/White-Paper>
- [58] Kent Beck and Ward Cunningham. 1987. Using Pattern Languages for Object Oriented Programs. In Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA). ACM, Orlando, FL, USA.
- [59] Taibi, D.; Lenarduzzi, V. and Pahl, C. (2018). Architectural Patterns for Microservices: A Systematic Mapping Study. In Proceedings of the 8th International Conference on Cloud Computing and Services Science - CLOSER, ISBN 978-989-758-295-0; ISSN 2184-5042, pages 221-232.

Tables des illustrations

Figure 1: Origine des informations de santé d'un patient dans un DME [10].	11
Figure 2: Liste des étapes de sélection appliqué à notre corpus d'article.	18
Figure 3: Répartition des articles en fonction des patterns identifiables.	20
Figure 4: Répartition des articles en fonction des patterns qui sont définis.	21
Figure 5: Répartition des articles en fonction des blockchains utilisés.	21
Figure 6: Répartition des articles en fonction de leurs conférences.	22
Figure 7: Score des différents articles.	23
Figure 8: Répartition des articles en fonction de leurs approches.	25
Figure 9: Proposition de modèle de [33].	29
Figure 10 : Proposition de modèle de [34].	31
Figure 11; Proposition de modèle de [35].	32
Figure 12: Répartition des patterns les plus utilisés.	34
Figure 13: Répartition des articles qui définissent les systèmes blockchain utilisés.	38
Figure 14: Répartition des systèmes blockchain utilisés.	39
Figure 15: Répartition des types de blockchain utilisés.	41

Tables des tableaux

Tableau 1: Liste des critères d'inclusion et d'exclusion.	16
Tableau 2: Résultats des réponses aux questions d'évaluation de la qualité des articles.	22
Tableau 3: Liste des patterns de la blockchain [9].	27

Glossaires

SLR : Une revue systématique de littérature ou SLR est un travail de collecte, d'évaluation critique et de synthèse des connaissances existantes dans la littérature scientifique actuelle dans l'objectif de répondre sur une question spécifique.

Consensus : Un mécanisme de consensus permet d'arriver à un accord commun entre différents participants. Concrètement, sur la blockchain, un algorithme de consensus est une mise en conformité de chaque acteur du réseau blockchain afin de se mettre d'accord sur la création et l'enchaînement de chaque bloc.

Proof of Work : La preuve de travail (PoW) décrit un système qui nécessite un effort non négligeable mais réalisable afin de dissuader les utilisations frivoles ou malveillantes de la puissance de calcul, telles que l'envoi de spams ou le lancement d'attaques par déni de service. Le PoW est utilisé comme mécanisme de consensus dans la blockchain, comme Bitcoin par exemple, qui consiste à résoudre une énigme cryptographique, en utilisant la puissance de calcul de leur matériel informatique.

Proof of Stake : preuve d'enjeu, ou encore preuve de participation, a été conçue pour combler les problèmes causés par le PoW qui consomme trop d'énergie inutilement. C'est également un mécanisme de consensus dans lequel, l'utilisateur d'une blockchain souhaitant participer à la création de nouveaux blocs doit posséder et mettre en jeu une certaine quantité de jetons, dans la crypto-monnaie utilisée sur le réseau.

Proof of Authority : est une méthode de consensus qui donne à un nombre restreint et désigné d'acteurs d'une blockchain le pouvoir de valider des transactions ou des interactions avec le réseau et de mettre à jour son registre plus ou moins distribué.

Distributed Ledger Technologies : La technologie de grand livre distribué (DLT) fait référence à l'infrastructure et aux protocoles technologiques qui permettent un accès, une validation et une mise à jour simultanés des enregistrements de manière immuable sur un réseau réparti sur plusieurs entités ou emplacements. Le DLT, plus communément connu sous le nom de technologie blockchain, a été introduit par Bitcoin. En termes simples, le DLT porte sur l'idée d'un réseau « décentralisé » par rapport au mécanisme « centralisé » conventionnel, et il est réputé avoir des implications profondes sur les secteurs et les entités qui s'appuient depuis longtemps sur un tiers de confiance.

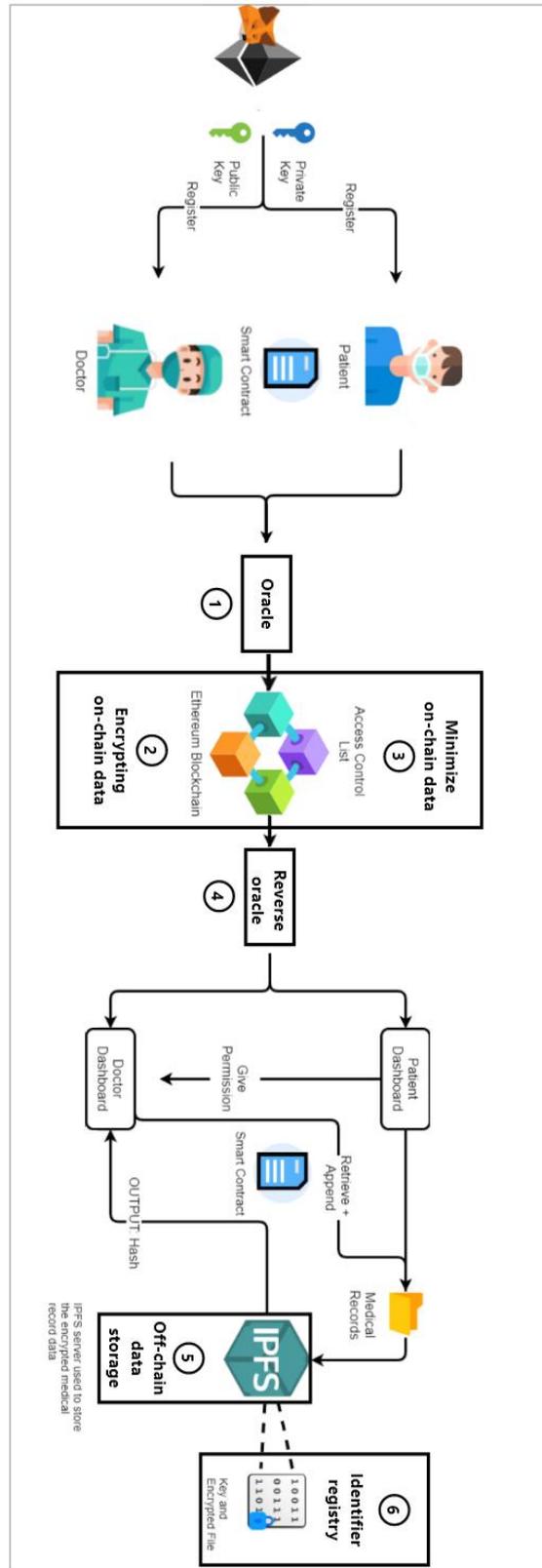
Smart Contract : Les contrats intelligents sont des contrats numériques stockés dans une blockchain qui sont automatiquement exécutés lorsque des conditions générales prédéterminées sont remplies. Ils sont généralement utilisés pour automatiser l'exécution d'un accord de sorte que tous les participants puissent être immédiatement certains du résultat, sans intervention d'un intermédiaire ni perte de temps. Ils peuvent également automatiser un flux de travail, déclenchant l'action suivante lorsque les conditions sont remplies.

Coût de gaz : Ce sont les commissions que l'on verse au mineur qui effectue la validation d'une transaction donnée. Par défaut, ce prix du gaz est exprimé en GWei ou giga-wei, le wei étant la plus petite unité d'ETH (Ethereum).

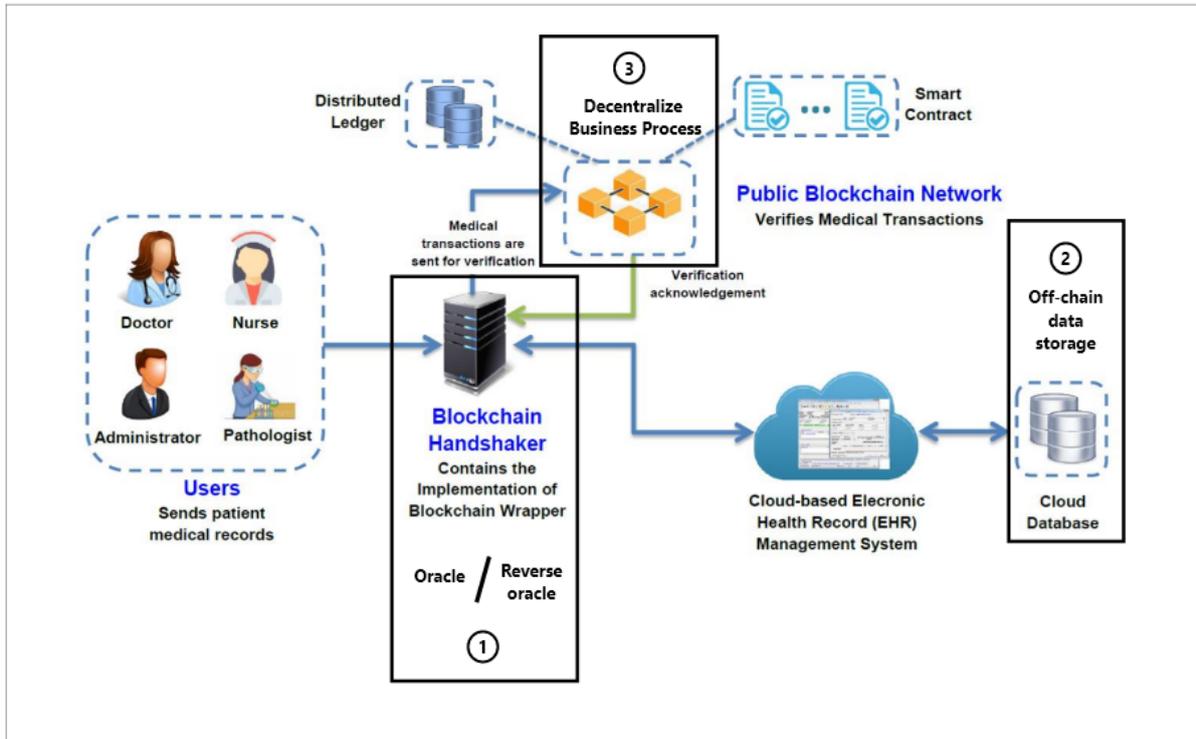
IPFS : est un protocole pair à pair décentralisé dont le but est de rendre le Web plus rapide, plus sûr, plus ouvert et moins cher pour le stockage.

Annexes

Annexe 1 : Architecture orientée pattern de [33]



Annexe 2 : Architecture orientée pattern de [34]



Annexe 3 : Architecture orientée pattern de [35]

