

Towards practical digital health designs: A single electronic health record for South Africa

Wesley Moonsamy 

University of Pretoria, Hatfield Campus, Lynnwood Road, Pretoria, South Africa

ABSTRACT

Since announcing the implementation of a single electronic health record for all South Africans, the government has not yet informed healthcare facilities of how this would be accomplished. The siloed South African healthcare system would have to be redesigned to accommodate a single electronic health record. A systematic literature review conducted across three databases returned 9 790 results. By applying ten filters, 22 documents were eventually retrieved for analysis. The analysis showed that existing research focuses on healthcare architectures from a theoretical perspective. Therefore, the literature review revealed a practically based research deficiency and a lack of theoretical studies merged with practical cases. Seeking to enhance the understanding of designing a single electronic health record, the documents were analysed using a qualitative inductive content analysis technique, revealing that a single electronic health record cannot be formulated using a fully centralised architecture as this is not practical. A fully decentralised architecture, such as blockchain, is equally infeasible because this requires significant changes to the existing systems and infrastructure and would require re-skilling system builders. Since the South African healthcare architecture is already decentralised, hybrid architecture incorporating edge computing with clusters of systems and information that connect using middleware should be considered.

Keywords single electronic health record, centralised architecture, decentralised architecture, healthcare systems, blockchain, edge computing, hybrid architecture

Categories

- Applied Computing → Life and Medical Sciences → Healthcare information systems
- Computer Systems Organization → Architectures → Distributed architectures

Email

Wesley Moonsamy – wesley.moonsamy@up.ac.za (CORRESPONDING)

Article history

Received: 26 May 2025
Accepted: 4 Jun 2026
Online: 31 July 2026

1 INTRODUCTION

South Africa has proposed implementing a single electronic health record (EHR) for all citizens (Moonsamy, 2025; Ramaphosa, 2025). Such an implementation would require changes to the existing healthcare technology architecture to combine the relevant data from various

Moonsamy, W. (2026). Towards practical digital health designs: A single electronic health record for South Africa. *South African Computer Journal* 38(1), 79–108. <https://doi.org/10.18489/sacjv38i1/22366>

Copyright © the author(s); published under a [Creative Commons NonCommercial 4.0 License](#) 
SACJ is a publication of *SAICSIT*. ISSN 1015-7999 (print) ISSN 2313-7835 (online)

sources to form an accurate and comprehensive view of a patient. Apart from major changes to the South African healthcare landscape, such as the implementation of SAP Health Information System (HIS) (Sobuwa, 2023), recent cybersecurity incidents (ITWEB, 2023, 2024; Kahn, 2024) necessitate safer and more future-proofed healthcare systems designs.

The two principal architectural design options are centralised and decentralised design. Much of the examined literature highlights the deficiencies of centralised designs, noting that they are single points of failure (Hussien et al., 2021; Miyachi & Mackey, 2021; X. Wang, 2022) and pose a security risk (Jayabalan & Jeyanthi, 2022). In contrast, decentralised architectures do not share the same security challenges as they offer several benefits, such as advanced security (Miyachi & Mackey, 2021; Zhu et al., 2024) and data-sharing capabilities (Guo et al., 2024). Existing research particularly focuses on the theoretical aspects of architectural designs. Nevertheless, practically speaking, existing technology landscapes must be considered along with the skill sets of the individuals involved.

This research paper is structured as follows: Section 2 provides the identification, filtering and results of the systematic literature review (SLR); this is followed by the research method in Section 3, which explains the application of the qualitative inductive content analysis; Section 4 presents the results of the data analysis and explains how the results relate to the single EHR; Section 5 proposes recommendations for designing the single EHR, followed by the conclusion.

2 LITERATURE REVIEW

Balsam and Mishra (2025) note the benefits of SLRs as being repeatable and conducive to identifying research deficits and identifying relevant literature based on inclusion and exclusion criteria. Phillips and Barker (2021) note that SLRs are transparent and provide a synthesis of existing relevant literature. Hence, this research followed the SLR methodology, supplemented by an adaptation of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Rethlefsen & Page, 2021) to report the search results graphically.

2.1 A SINGLE ELECTRONIC HEALTH RECORD

South Africa intends to introduce a single EHR for all South Africans (Moonsamy, 2025; Ramaphosa, 2025). A single EHR would provide accurate and real-time healthcare data to medical professionals, which, in turn, supports healthcare service delivery (Moonsamy, 2025). However, the highly fragmented South African healthcare landscape causes several challenges to implementing a single EHR:

1. The private and public healthcare sectors store their data separately (Moonsamy & Singh, 2024);
2. Systems struggle to share information due to interoperability issues (Tsegaye & Flowerday, 2021);

3. Data privacy must be considered (Tsegaye & Flowerday, 2021); and
4. Information security is a concern (Tsegaye & Flowerday, 2021).

Apart from the challenges to implementing a single EHR, the term “single electronic health record” has not yet been clearly defined within the South African healthcare context – to this author’s knowledge. A single EHR might suggest a centralised system whereby all healthcare records are housed in a single physical location. Conversely, a single EHR could be implemented by logically grouping healthcare records through a decentralised mechanism. In the absence of a suitable definition, the author assumes that a single EHR refers to *a logical grouping of healthcare records from several repositories forming a dynamic and comprehensive view of a patient*.

Several authors have discussed centralised and decentralised designs from a theoretical perspective, meaning that existing systems and their associated challenges are not directly considered in the existing literature. Shamshad et al. (2020) suggest using blockchain technology to share healthcare information. C. Wang et al. (2024) discuss authorisation and access control through decentralisation for enhancing information security. However, South Africa and other developing countries have ageing Health Information Systems (HISs) that cannot be easily decentralised or migrated. Through a synthesis of existing literature, the author noted a deficiency of practically based research and an absence of theoretical studies merged with practical cases. This practicality insufficiency led to further investigation of existing ideas through the SLR discussed in Section 2.2.

2.2 LITERATURE SEARCH AND RESULTS

The study utilised three databases (*EBSCO*, *ScienceDirect* and *Wiley*) to search for existing literature on healthcare systems designs, as the author has institutional access to these resources. The following search string was used in the *EBSCO* and *Wiley* databases:

```
("Central electronic health record" OR "Central record"  
OR "Central storage" OR "Centralised electronic health record"  
OR "Centralised record" OR "Centralised storage"  
OR "Centralized electronic health record" OR "Centralized storage"  
OR "Centralized record" OR "Decentralised electronic health record"  
OR "Decentralised record" OR "Decentralised storage"  
OR "Decentralized electronic health record" OR "Decentralized record"  
OR "Decentralized storage" OR "Single view of patient"  
OR "Single view of patient record" OR "Single view of patient records")
```

Since the *ScienceDirect* database allows search strings with a maximum of eight Boolean operators, the author divided the search string into two strings and merged the results. Below are the separate search strings:

```
("Central electronic health record" OR "Central record"  
OR "Central storage" OR "Centralised electronic health record"
```

OR "Centralised record" OR "Centralised storage"
 OR "Centralized electronic health record" OR "Centralized storage"
 OR "Centralized record")
 ("Decentralised electronic health record" OR "Decentralised record"
 OR "Decentralised storage" OR "Decentralized electronic health record"
 OR "Decentralized record" OR "Decentralized storage"
 OR "Single view of patient" OR "Single view of patient record"
 OR "Single view of patient records")

Figure 1 presents the results of the literature search.

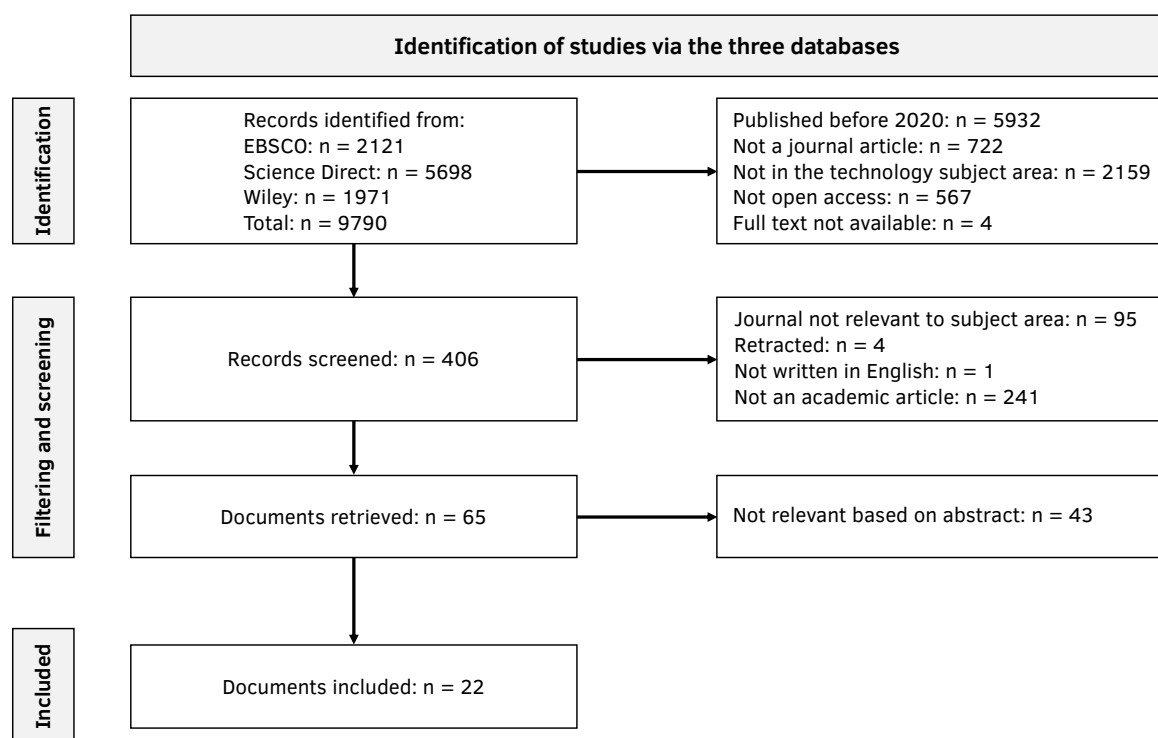


Figure 1: Adapted PRISMA layout of search results

The searches yielded 9 790 records at the identification stage. The author applied ten filters to the search results (published since 2020, journals only, appropriate subject area, open access, full text, relevant journals, not retracted, English only, academic article only and relevant abstract), thereby excluding 99.77% of the records and retaining 22 documents for further investigation. Table 1 summarises the 22 studies identified for further review.

Table 1: Summary of the documents included and their relevance

Document
D01: Zhu et al. (2024) <i>A survey of blockchain, artificial intelligence, and edge computing for Web 3.0</i> Discusses four key technologies: blockchain, artificial intelligence, edge computing and Web 3.0. These technologies are key to a decentralised architecture, which could benefit healthcare systems, especially from a security perspective.
D02: Jayabalan and Jeyanthi (2022) <i>Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy</i> Introduces the idea that blockchain alone cannot scale to the levels some systems, such as healthcare systems, require. Discusses off-chain models and connecting them to the blockchain (on-chain).
D03: Sonbol et al. (2020) <i>EdgeKV: Decentralized, scalable, and consistent storage for the edge</i> Edge computing can benefit a decentralised healthcare system; one example discussed is EdgeKV.
D04: Gao et al. (2022) <i>Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing</i> Discusses blockchain and off-chain models from a security perspective, a key requirement in healthcare systems.
D05: Miyachi and Mackey (2021) <i>hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design</i> Similar to D04. Discusses security options available to blockchain systems.
D06: Hussien et al. (2021) <i>Blockchain technology in the healthcare industry: Trends and opportunities</i> Discusses the gap between existing healthcare systems, which might be either centralised or decentralised options such as blockchain technologies.
D07: Shamshad et al. (2020) <i>A secure blockchain-based e-health records storage and sharing scheme</i> Introduces the notion of a private blockchain and a consortium blockchain of indexes. The research also considers sharing EHRs between different healthcare organisations.
D08: Sumana and Hareesha (2020) <i>Grouping of distributed data at multiple sites by sustaining the privacy of data</i> Refers to clusters of data and acknowledges that data are stored in multiple locations.
D09: Naz et al. (2024) <i>Cloud-based framework for data exchange to enhance global healthcare</i> Refers to data sharing between EHRs within a cloud-based environment.

Continued...

Table 1: Summary of the documents included and their relevance (continued)

Document
D10: Thantilage et al. (2023) <i>Healthcare data security and privacy in data warehouse architectures</i> Considers the vast amount of healthcare data possibly existing within a system and how information can be accessed from data warehouses.
D11: M. Wang et al. (2022) <i>Big data healthcare platform with multisource heterogeneous data integration and massive high-dimensional data governance for large hospitals: design, development, and application</i> Healthcare data stored on different systems can be considered heterogeneous, which complicates data sharing and data governance.
D12: Manyane et al. (2025) <i>Affordances and constraints of the open medical record system (OpenMRS) for public health services delivery in Lesotho</i> Focuses on open-source healthcare technologies used in resource-constrained developing countries.
D13: Li et al. (2022) <i>Information sharing and privacy protection of electronic nursing record management system</i> Discusses the disadvantages of centralised healthcare data storage and introduces blockchain as a decentralised storage option.
D14: X. Wang (2022) <i>Design and implementation of a data sharing model for improving blockchain technology</i> Debates data sharing in the context of centralised and decentralised architectures.
D15: Guo et al. (2024) <i>Secure data sharing technology of medical privacy data in the Web 3.0</i> Examines information security within the healthcare context through Web 3.0 technologies.
D16: Monniot et al. (2023) <i>Supporting dynamic allocation of heterogeneous storage resources on HPC systems</i> Discusses the storage and retrieval of large heterogeneous datasets, which applies to the healthcare context.
D17: de Oliveira et al. (2023) <i>Storage standards and solutions, data storage, sharing, and structuring in digital health: a Brazilian case study</i> Introduces the concept of medical silos within a developing country context which is also relevant to the South African healthcare context.
D18: Valeonti et al. (2024) <i>Decentralising digital humanities: exploring blockchain technology and “web3” for the Sloane Lab and Towards a National Collection (TaNC)</i> Focuses on deficiencies related to Web 3.0 research.

Continued...

Table 1: Summary of the documents included and their relevance (continued)

Document
D19: Grover and Kushwaha (2022) <i>Authorization and privacy preservation in cloud-based distributed EHR system using blockchain technology and anonymous digital ring signature</i> Discusses centralised and decentralised options for EHRs by examining cloud-based and blockchain-based designs.
D20: Gao et al. (2023) <i>Similarity-based deduplication and secure auditing in IoT decentralized storage</i> Similar to D13 and D14. Supplements the discussion by including data deduplication and IoT.
D21: Wu et al. (2022) <i>DSPR: Secure decentralized storage with proof-of-replication for edge devices</i> Discusses edge computing, one of the key technologies related to a decentralised healthcare system architecture.
D22: Mohsan et al. (2022) <i>Decentralized patient-centric report and medical image management system based on blockchain technology and the inter-planetary file system</i> Similar to D02, D13, D14 and D20. Introduces discussions on datasets constituting large media files.

2.3 CENTRALISED VERSUS DECENTRALISED ARCHITECTURES

Healthcare data are sensitive and private and thus must be secure, especially when shared with other systems (de Oliveira et al., 2023; Gao et al., 2022). Notwithstanding this requirement, typical centralised healthcare architectures do not offer adequately secured mechanisms for sharing healthcare data with other systems (Shamshad et al., 2020). Moonsamy and Singh (2024) argue that the South African healthcare ecosystem comprising private and public healthcare sectors is more complicated when considering the components of each system. The private sector alone constitutes more than five main hospital groups, each centralising their data. In addition to these hospital groups, thousands of private healthcare providers store their patient data. The public sector has recently implemented SAP HIS for Gauteng (Sobuwa, 2023) but not yet in other provinces. This situation poses a practical challenge by creating medical silos, as mentioned by de Oliveira et al. (2023). Figure 2 depicts the existing healthcare ecosystem in South Africa. The healthcare ecosystems of other developing countries are expected to be similar.

Data islands are included in Figure 2 due to the persistence of paper-based systems and digitised systems that do not share their data with other systems. Some studies (Gao et al., 2022; Jayabalan & Jeyanthi, 2022; Li et al., 2022; Zhu et al., 2024) highlight the benefits of decentralised systems within a healthcare context, whereas Monniot et al. (2023) discuss heterogeneous datasets and, Grover and Kushwaha (2022) consider centralised and decentralised systems. None of the authors suggested a fully centralised design – mostly due to security concerns. From a practical perspective, neither a fully centralised nor a fully decentralised

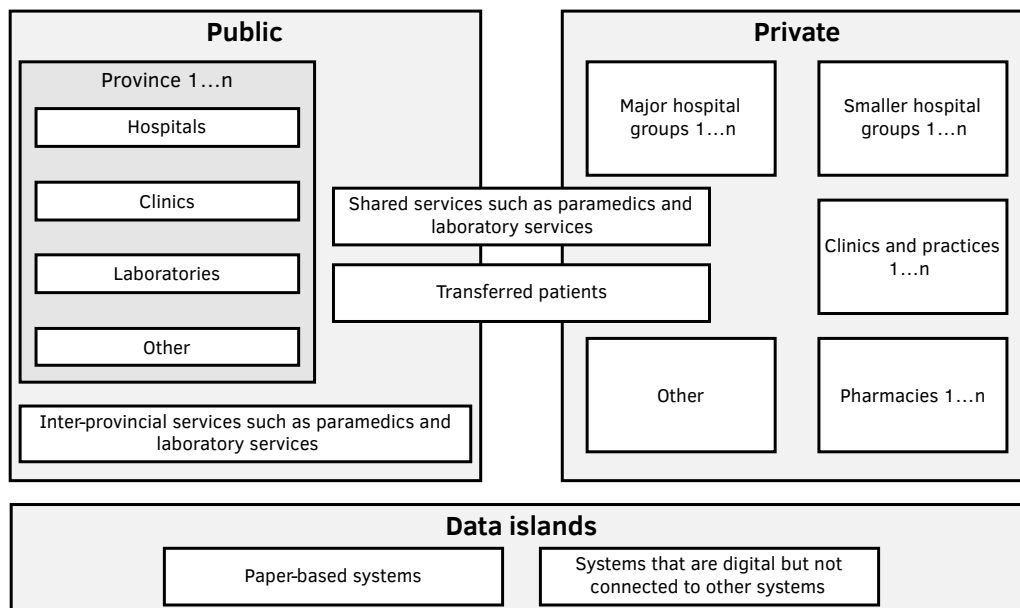


Figure 2: South African healthcare ecosystem

system might be feasible designs due to the security risks of a fully centralised design and the large amount of work required to decentralise the healthcare system comprehensively.

2.4 LITERATURE REVIEW SUMMARY

The healthcare ecosystem in South Africa is not only fragmented insofar as service delivery, but also the systems and data are siloed, albeit with touchpoints in some areas, such as emergency patient transport and laboratory services. Even though previous authors have discussed the merits of a decentralised system, this author is not convinced that a fully decentralised system – even with off-chain functionality – would be practical. After examining the existing literature, the practicality gaps in the literature relating to designing a single EHR became more pronounced. This outcome called for a deeper analysis of the 22 included documents via an inductive content analysis. The analysis would promote a deeper understanding of the associations between the merits and shortcomings of centralised designs, decentralised designs, edge computing, Web 3.0 and other related technologies when designing a single EHR.

3 METHODOLOGY

Vears et al. (2022) describe inductive content analysis as a qualitative data analysis method suitable for the analysis of healthcare-related textual information such as research reports (journal articles) or non-research-related reports (doctors' notes). Since the methodology for this study was inherently inductive, the researcher needed to read through the texts to deduce

meaning, thus negating the need for existing theories. This approach differs from a deductive content analysis, which uses existing theories on well-established literature. For this research, the author considered a well-established body of literature but did not consider existing theories related to the main concept of centralised and decentralised systems. The author opted for the inductive approach to establish new ideas or theories from the existing literature within a practical context.

Table 2: Inductive content analysis steps

Step#	Name	Description and adaptation to this study
1	Read and familiarise	Since a researcher might not be familiar with all the data, they should first read through the documents to gain understanding before coding the text. In this study, the researcher first read through documents and then initiated the coding phase. Notably, some documents contained technical formulae and algorithms not easily coded; however, the study interpreted the summaries and descriptions provided in the documents.
2	First-round coding: identifying the big-picture meaning units	Coding chunks of text while considering the overall perspective the text relates to. The author followed this step as explained.
3	Second-round coding: developing subcategories and fine-grained codes	Consider each broad view category and link this to the text. For this step, the author grouped all the codes into broad view categories using subnetworks in ATLAS.ti.
4	Refining the fine-grained subcategories	Compare and relate the fine-grained subcategories. The author grouped the subnetworks into networks.
5	Synthesis and interpretation	Rather than creating a general theory, as in thematic analysis, this step requires the researcher to remain close to the research question and problem statement. The author used the relationships between the networks (which included the subnetworks and codes) to answer the research question.

Table 2 describes the five steps followed in analysing the 22 documents, and Section 4 discusses the analysis results.

4 ANALYSIS AND RESULTS

The analysis of the 22 documents, together with the results of the analysis, are presented based on the five steps, as explained in Table 2. The documents were analysed using *ATLAS.ti* version 25.0.1.32924. Even though this version of *ATLAS.ti* integrates with *OpenAI* and is capable of performing coding using artificial intelligence, the author decided not to use this functionality and opted to code each document manually.

4.1 READ AND FAMILIARISE

During this step, the author read a document, coded the document and then moved on to the next document. Reading each document prior to coding gave the author a more detailed

understanding of the core concepts of each document and how they related to centralised and decentralised healthcare system designs. Table 1 provides a summary of the concepts learnt from each document. As mentioned in Table 2, the very technical parts of some documents, such as the formulae and algorithms, were not examined in detail; however, the summaries and diagrams were synthesised, which led to the formulation of related codes. Section 4.2 contains a discussion of the first round of coding.

4.2 FIRST-ROUND CODING

The 22 documents were qualitatively analysed using inductive coding. During this step, 160 codes were formulated, presented in Appendix A. The coding depth or the number of codes identified per document has not been presented because some documents were very technical and focused on formulae and algorithms that did not directly impact this study. Furthermore, Vears et al. (2022) argue that qualitative content analysis is not concerned with counting frequencies of codes even though this notion contradicts Vaismoradi et al. (2013), who argue that content analysis – a branch of qualitative analysis – is concerned with interpreting the counts of codes.

The output of the SLR (22 documents) was the input for the data analysis; hence, the 22 documents informed the sample size of the study. Braun and Clarke (2019) argue that thematic analysis and, by extension, content analysis do not always need to be examined for data saturation. Furthermore, Ahmed (2025) argues that the sample size for a content analysis depends on the amount of available text. Figure 3 presents the number of emerging codes per document.

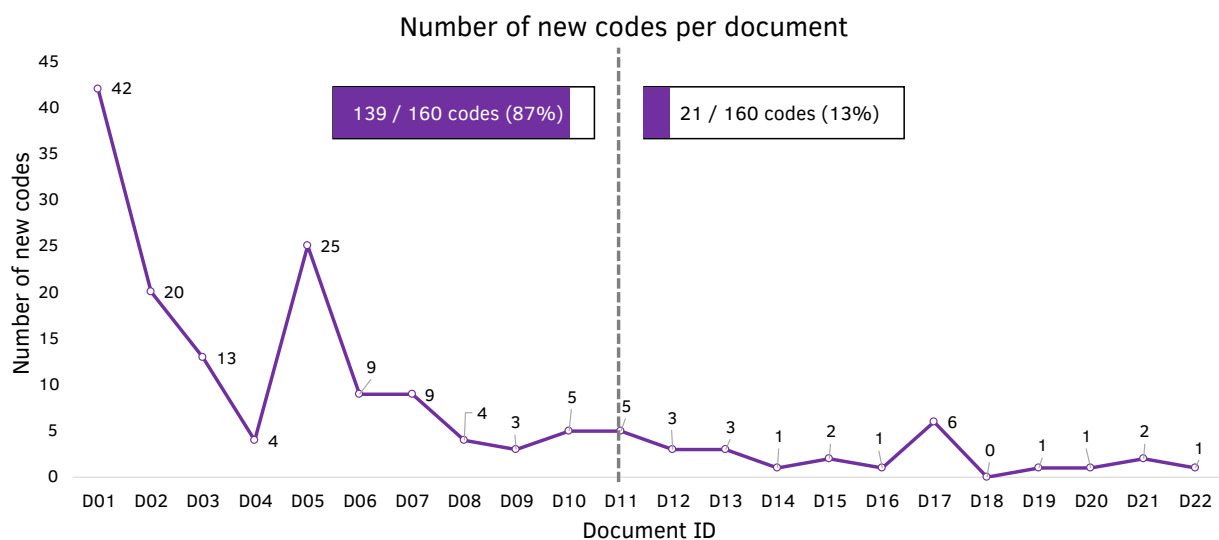


Figure 3: Emerging codes per document

The 160 codes formulated during the first round of coding were used as input for the second round of coding, as discussed in [Section 4.3](#).

4.3 SECOND-ROUND CODING

During the second round of coding, the 160 codes were grouped into 28 subnetworks, presented in [Appendix A](#). The 28 subnetworks can be grouped into two main system design architectures: centralised and decentralised. Centralised data can support artificial intelligence and other forms of decision-making; however, healthcare systems (South Africa is no exception) store data fragmentedly or in medical silos. Decentralised systems are supported by technologies such as blockchain, Web 3.0 and edge computing. Blockchain has the potential to store indexes on-chain and can link to larger datasets stored off-chain. Even though edge computing and blockchain support decentralised designs, they are complicated to implement and require specialist skills and appropriate infrastructure. Once the subnetworks had been formulated, they were grouped into networks, which are discussed in [Section 4.4](#).

4.4 REFINING THE FINE-GRAINED SUBCATEGORIES

During this step, the 28 subnetworks were grouped into 14 networks, presented in [Appendix A](#) and explained in detail in [Table 3](#).

Table 3: Description of networks

Network	Description
Artificial intelligence	Centralised information supports decision-making systems that use artificial intelligence.
Big data	Big data require high-performance computing and benefit from centralised data.
Blockchain challenges	Blockchain requires specialist skills and systems, is susceptible to performance congestions, struggles to store large files, and requires off-chain systems to store related data.
Blockchain opportunities	Blockchain is secure and robust, supports decentralisation and can benefit from off-chain storage mechanisms.
Centralised healthcare designs	Centralised designs are still in use even though they pose a single point of failure risk. There are opposing views regarding whether centralisation supports or hinders patient-centredness.
Edge computing challenges	Heterogeneous systems hinder interoperability and complicate data sharing.
Edge computing opportunities	Edge computing reduces single-point-of-failure risks, supports healthcare systems; grouping of nodes can assist with interoperability challenges and promote security through the decentralisation of systems.
Healthcare architecture	Healthcare architectures are usually made up of centralised pockets of data (silos) and are hindered by data islands that do not connect to other systems or share data.
Healthcare data	Data must be protected by adequate governance measures and are at risk of being duplicated in decentralised systems.

Continued...

Table 3: Description of networks (continued)

Network	Description
Middleware systems	Connect heterogeneous systems for data sharing.
Patient-centredness	Patients should have access to and a degree of control over their data.
Web 3.0 challenges	Web 3.0 is difficult to implement and can result in a complex landscape.
Web 3.0 opportunities	Web 3.0 supports healthcare through decentralising and sharing data. Web 3.0 also promotes trust and can be implemented with other decentralised technologies such as blockchain.
Web technologies	Have evolved since Web 1.0 and now support trust and data sharing through decentralisation.

Following the formulation of the codes, subnetworks and networks, the networks were used to answer the research questions, discussed in Section 4.5.

4.5 SYNTHESIS AND INTERPRETATION

Thus far, the literature review and data analysis have provided insights into healthcare system designs. A fully centralised system would easily support a single EHR as all records would be housed in a single location. Nonetheless, a fully centralised system is unquestionably impossible for South Africa to implement since there are potentially thousands of existing systems and data islands to consolidate. In addition, a fully centralised architecture is a security risk. Figure 2 illustrates siloed systems across the public and private sectors and the data islands created by unintegrated or paper-based systems. A closer inspection of Figure 2 reveals that the South African healthcare architecture is already decentralised even though Web 3.0, edge computing, and blockchain technologies are not directly referenced within this context.

RQ1: Is a single electronic health record better supported by a centralised or decentralised architecture in South Africa?

The question might be answered as follows: Since South Africa does not have a centralised healthcare architecture but is, instead, already decentralised, a single EHR would need to be designed based on this decentralised architecture, notwithstanding its siloed nature.

RQ2: Does the current South African healthcare architecture support a single electronic health record?

The question might be answered as follows: In its current state, the South African healthcare architecture does not support a single EHR. Even though decentralised systems can nevertheless connect, share information and create a single view of a patient, the primary requirement for system connectivity is absent or, at the very least, oversimplified.

Section 5 provides recommendations for the design of a single EHR.

5 DISCUSSION AND RECOMMENDATIONS

Several authors have criticised centralised architectures for being at risk of cyberattacks and subsequently becoming single points of failure (Hussien et al., 2021; Miyachi & Mackey, 2021; X. Wang, 2022). Therefore, decentralised architectures can benefit the healthcare system as they can be more secure since the South African healthcare architecture is already decentralised. However, creating a single EHR requires that the edge nodes (private and public hospital databases, private and public clinics, pharmacies and other facilities) should be connected. Even though middleware systems connect disparate systems (Sonbol et al., 2020), it might not be practical to link thousands of systems via a single middleware system since this would shift the single point of failure to the middleware system itself. Table 4 presents a list of recommendations for designing a single EHR.

Table 4: Recommendations for the design of a single EHR

Recommendation	Rationale
Utilise the benefits of edge computing	Node groups sharing information can connect to other groups to form clusters. Clusters can then share information through middleware systems, potentially creating a grid-like design, thus removing single points of failure.
Utilise blockchain with caution	Although blockchain can benefit the healthcare system from a security perspective, South Africa must first re-skill healthcare software programmers on blockchain technologies. Off-chain storage must be carefully considered as a supporting data storage mechanism.
Use Web 3.0 concepts	Although Web 3.0 primarily refers to the web, related concepts, such as governance in a decentralised architecture, can be used within the healthcare system.
Ensure effort estimations are accurate	Connecting thousands of healthcare systems to form a single EHR is a complex task; the effort involved in connecting systems should not be underestimated.
Consider bridging data islands	Many practices are paper-based or do not connect to other systems, which could result in incomplete and inaccurate single EHRs. System owners should be educated on the risks and benefits of connecting their systems to other nodes to make informed decisions on whether they want to contribute to a single EHR.

The recommendations presented in Table 4 and the existing landscape illustrated in Figure 2 could result in a hybrid design, whereby clusters of centralised systems can share information with a decentralised middleware architecture. All systems in the landscape can share information to form a single EHR. This concept is illustrated in Figure 4.

Creating a single EHR based on the architecture presented in Figure 4 requires further investigation to optimise searching for a patient and collecting all relevant data to form a single view of the patient. In addition, the hybrid architecture could be designed in detail by including blockchain and Web 3.0 principles. Failover scenarios should be investigated in future research.

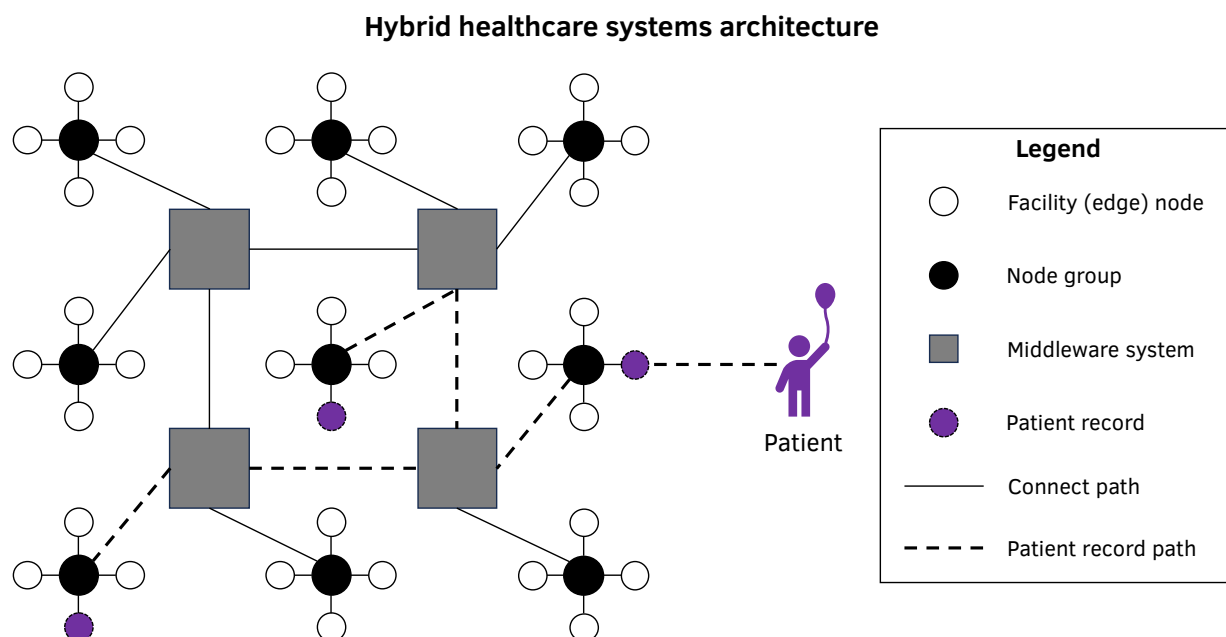


Figure 4: Hybrid healthcare systems architecture

6 CONCLUSION

South Africa seeks to benefit from a single EHR for all citizens, even though a single EHR has not been adequately defined. Therefore, the author proposes the following definition: “A single electronic health record is a logical grouping of healthcare records from several repositories forming a dynamic and comprehensive view of a patient”. The author conducted an SLR to identify relevant studies related to the formulation of a single EHR focusing on centralised and decentralised technologies. This review led to the analysis of 22 documents using qualitative inductive content analysis. The first round of coding identified 160 codes, later grouped into 28 subnetworks and then further refined into 14 networks.

The author suggests a more practical approach to decision-making around healthcare architectures relating to centralisation versus decentralisation. Since it is impractical and unsafe to centralise the entire healthcare system, and fully decentralising the system requires significant skills development and changes to existing infrastructure, the author suggests a hybrid approach. In such an approach, a patient’s entire record can be obtained from the relevant edges (facilities), which link up as edge groups. These edge groups are connected using middleware systems to form clusters. A single EHR can then be formulated based on following the correct path.

The proposed hybrid design considers decentralisation and edge computing because the South African healthcare architecture already resembles this layout. Future research should consider incorporating the benefits of blockchain, Web 3.0 and artificial intelligence technologies while considering the limitations of these technologies and the skill sets of existing resources.

References

- Ahmed, S. K. (2025). Sample size for saturation in qualitative research: Debates, definitions, and strategies. *Journal of Medicine, Surgery, and Public Health*, 5, 100171. <https://doi.org/10.1016/j.glmedi.2024.100171>
- Balsam, S., & Mishra, D. (2025). Web application testing – Challenges and opportunities. *Journal of Systems and Software*, 219, 112186. <https://doi.org/10.1016/j.jss.2024.112186>
- Braun, V., & Clarke, V. (2019). To saturate or not to saturate? Questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, 13(2), 201–216. <https://doi.org/10.1080/2159676x.2019.1704846>
- de Oliveira, N. R., dos Santos, Y., Mendes, A. C. R., Barbosa, G. N. N., de Oliveira, M. T., Valle, R., Medeiros, D. S. V., & Mattos, D. M. F. (2023). Storage standards and solutions, data storage, sharing, and structuring in digital health: A Brazilian case study. *Information*, 15(1), 20. <https://doi.org/10.3390/info15010020>
- Gao, Y., Zhang, A., Wu, S., & Chen, J. (2022). Blockchain-based multi-hop permission delegation scheme with controllable delegation depth for electronic health record sharing. *High-Confidence Computing*, 2(4), 100084. <https://doi.org/10.1016/j.hcc.2022.100084>
- Gao, Y., Chen, L., Han, J., Wu, G., & Liu, S. (2023). Similarity-based deduplication and secure auditing in IoT decentralized storage. *Journal of Systems Architecture*, 142, 102961. <https://doi.org/10.1016/j.sysarc.2023.102961>
- Grover, B., & Kushwaha, D. K. (2022). Authorization and privacy preservation in cloud-based distributed EHR system using blockchain technology and anonymous digital ring signature. *Health Services and Outcomes Research Methodology*, 23(2), 227–240. <https://doi.org/10.1007/s10742-022-00281-z>
- Guo, S., Chen, C., & Tong, Q. (2024). Secure data sharing technology of medical privacy data in the Web 3.0. *IET Blockchain*, 4(4), 335–343. <https://doi.org/10.1049/blc2.12086>
- Hussien, H. M., Yasin, S. M., Udzir, N. I., Ninggal, M. I. H., & Salman, S. (2021). Blockchain technology in the healthcare industry: Trends and opportunities. *Journal of Industrial Information Integration*, 22, 100217. <https://doi.org/10.1016/j.jii.2021.100217>
- ITWEB. (2023). *South Africa ranked 5th on global cyber crime density list* [Accessed: 12 July 2023]. <https://www.itweb.co.za/article/south-africa-ranked-5th-on-global-cyber-crime-density-list/KA3WwMdz1nBvrydZ>

- ITWEB. (2024). *SA's cyber security vulnerability exposed* [Accessed: 28 January 2025]. <https://www.itweb.co.za/article/sas-cyber-security-vulnerability-exposed/KWEBb7yL1XavmRjO>
- Jayabalan, J., & Jeyanthi, N. (2022). Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *Journal of Parallel and Distributed Computing*, 164, 152–167. <https://doi.org/10.1016/J.JPDC.2022.03.009>
- Kahn, T. (2024). *NHLS still not fully operational after cyberattack* [Accessed: 23 July 2025]. <https://www.businessday.co.za/bd/national/health/2024-07-16-nhls-still-not-fully-operational-after-cyberattack/>
- Li, Q., Yu, H., & Li, W. (2022). Information sharing and privacy protection of electronic nursing record management system (A. Farouk, Ed.). *Scientific Programming*, 2022, 1–12. <https://doi.org/10.1155/2022/4169340>
- Manyanye, S., Kapepo, M., Belle, J. P. V., & Mthwasi, G. (2025). Affordances and constraints of the Open Medical Record System (OpenMRS) for public health services delivery in Lesotho. *Procedia Computer Science*, 256, 816–824. <https://doi.org/10.1016/J.PROCS.2025.02.183>
- Miyachi, K., & Mackey, T. K. (2021). hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information Processing & Management*, 58(3), 102535. <https://doi.org/10.1016/J.IPM.2021.102535>
- Mohsan, S. A. H., Razzaq, A., Ghayyur, S. A. K., Alkahtani, H. K., Al-Kahtani, N., & Mostafa, S. M. (2022). Decentralized patient-centric report and medical image management system based on blockchain technology and the inter-planetary file system. *International Journal of Environmental Research and Public Health*, 19(22), 14641. <https://doi.org/10.3390/ijerph192214641>
- Monniot, J., Tessier, F., Robert, M., & Antoniu, G. (2023). Supporting dynamic allocation of heterogeneous storage resources on HPC systems. *Concurrency and Computation: Practice and Experience*, 35(28). <https://doi.org/10.1002/cpe.7890>
- Moonsamy, W. (2025). *Working towards a single electronic health record for SA* [Accessed: 29 April 2025]. <https://www.itweb.co.za/article/working-towards-a-single-electronic-health-record-for-sa/Pero37Z38KyMQb6m>
- Moonsamy, W., & Singh, S. (2024). Digital health model for South Africa's national health insurance: Addressing hospital occupancy and emergency care. *Journal of Health Informatics in Africa*, 10(2), 10–14. <https://doi.org/10.12856/JHIA-2023-v10-i2-395>
- Naz, A., Ali, M., Cheema, S. M., & Pires, I. M. (2024). Cloud-based framework for data exchange to enhance global healthcare. *Procedia Computer Science*, 241, 570–575. <https://doi.org/10.1016/j.procs.2024.08.082>
- Phillips, V., & Barker, E. (2021). Systematic reviews: Structure, form and content. *Journal of Perioperative Practice*, 31(9), 349–353. <https://doi.org/10.1177/1750458921994693>
- Ramaphosa, C. (2025). *State of the nation address by President Cyril Ramaphosa* [Accessed: 10 February 2025]. https://www.stateofthenation.gov.za/assets/downloads/SONA_2025_Speech.pdf

- Rethlefsen, M. L., & Page, M. J. (2021). PRISMA 2020 and PRISMA-S: Common questions on tracking records and the flow diagram. *Journal of the Medical Library Association*, 110(2). <https://doi.org/10.5195/jmla.2022.1449>
- Shamshad, S., Minahil, Mahmood, K., Kumari, S., & Chen, C.-M. (2020). A secure blockchain-based e-health records storage and sharing scheme. *Journal of Information Security and Applications*, 55, 102590. <https://doi.org/10.1016/j.jisa.2020.102590>
- Sobuwa, Y. (2023). *How Gauteng's new information system will improve the quality of healthcare accreditation* [Accessed: 24 August 2023]. <https://www.news24.com/news24/southafrica/news/how-gautengs-new-information-system-will-improve-the-quality-of-healthcare-20230822>
- Sonbol, K., Özkasap, Ö., Al-Oqily, I., & Aloqaily, M. (2020). EdgeKV: Decentralized, scalable, and consistent storage for the edge. *Journal of Parallel and Distributed Computing*, 144, 28–40. <https://doi.org/10.1016/j.jpdc.2020.05.009>
- Sumana, M., & Hareesha, K. S. (2020). Grouping of distributed data at multiple sites by sustaining the privacy of data. *Procedia Computer Science*, 171, 1688–1697. <https://doi.org/10.1016/j.procs.2020.04.181>
- Thantilage, R. D., Le-Khac, N., & Kechadi, M. (2023). Healthcare data security and privacy in data warehouse architectures. *Informatics in Medicine Unlocked*, 39, 101270. <https://doi.org/10.1016/j.imu.2023.101270>
- Tsegaye, T., & Flowerday, S. (2021). A system architecture for ensuring interoperability in a South African national electronic health record system. *South African Computer Journal*, 33(1). <https://doi.org/10.18489/sacj.v33i1.838>
- Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences*, 15(3), 398–405. <https://doi.org/10.1111/nhs.12048>
- Valeonti, F., Vlachidis, A., Nyhan, J., Bikakis, A., Kotarski, R., & Jovanovic, P. (2024). Decentralising digital humanities: Exploring blockchain technology and “web3” for the Sloane Lab and towards a national collection (TaNC). *Journal of Documentation*, 81(1), 211–235. <https://doi.org/10.1108/jd-04-2024-0093>
- Vears, D. F., Gillam, L., & Vears, D. (2022). Inductive content analysis: A guide for beginning qualitative researchers. *Focus on Health Professional Education*, 23(1), 111–127. <https://doi.org/10.11157/FOHPE.V23I1.544>
- Wang, C., Xu, J., Tan, S., & Yin, L. (2024). Secure decision tree classification with decentralized authorization and access control. *Computer Standards & Interfaces*, 89, 103818. <https://doi.org/10.1016/j.csi.2023.103818>
- Wang, M., Li, S., Zheng, T., Li, N., Shi, Q., Zhuo, X., Ding, R., & Huang, Y. (2022). Big data health care platform with multisource heterogeneous data integration and massive high-dimensional data governance for large hospitals: Design, development, and application. *JMIR Medical Informatics*, 10(4), e36481. <https://doi.org/10.2196/36481>

- Wang, X. (2022). Design and implementation of a data sharing model for improving blockchain technology (Q. Li, Ed.). *Advances in Multimedia*, 2022, 1–8. <https://doi.org/10.1155/2022/4578525>
- Wu, C., Chen, Y., Qi, Z., & Guan, H. (2022). DSPR: Secure decentralized storage with proof-of-replication for edge devices. *Journal of Systems Architecture*, 125, 102441. <https://doi.org/10.1016/j.sysarc.2022.102441>
- Zhu, J., Li, F., & Chen, J. (2024). A survey of blockchain, artificial intelligence, and edge computing for Web 3.0. *Computer Science Review*, 54, 100667. <https://doi.org/10.1016/J.COSREV.2024.100667>

A SUPPLEMENTARY MATERIAL

Table A.1: Networks, subnetworks and codes

Network	Subnetwork	Code
Artificial Intelligence	Centralised information supports artificial intelligence	- Artificial intelligence uses centralised information for processing - Artificial intelligence supports problem-solving and decision-making
Big data	Big data are usually stored and processed centrally	- Big data collected from users are generally stored centrally - Big data mistrust among central authorities - High-performance computers usually follow a very centralised approach to data storage
Blockchain challenges	Blockchain requires specialist skills and standardisation	- Blockchain requires specialised technical skills - Blockchain requires specialist skills and systems - Blockchain still requires more standardisation to support the healthcare industry
	Access rights must be granted between blockchain and other systems to share data	- Blockchain systems cannot directly access outside resources - Hybrid on-chain and off-chain requires authentication between systems
	Blockchains are at risk of bottlenecks and exposing off-chain records	- Blockchains can be susceptible to storage bottlenecks - Placing data off-chain to reduce the load on the blockchain can place off-chain records at risk
	Blockchains that are too large and store large files are susceptible to performance bottlenecks	- Blockchain does not handle the large amount of data generated through IoMT or IoT devices - Large files such as scans can lead to scalability issues if stored on-chain - Blockchains are susceptible to computational issues - Large files such as X-rays can increase the load on a blockchain - Off-chain systems can reduce the performance of the blockchain if data are unavailable
Centralised healthcare designs	Centralised architectures benefit patients and doctors despite some limitations	- Centralised systems can have performance issues when all systems are trying to access the data - Centralised designs are still popular - Cloud computing generally uses a centralised design - Centralised records can provide adequate data for doctors - Data islands make it difficult to check for consistency
	Centralised designs pose a risk to healthcare systems	- Centralised systems complicate information sharing - Centralised designs limit data sharing - Centralised systems are susceptible to cyberattacks such as ransomware - Centralised systems offer a patient-centric approach - Centralised designs limit patient-centredness - Centralised systems face issues such as data leakage, data loss and misplacement - Centralised designs pose a risk - Centralised designs are not known for providing a secure mechanism for sharing information - Centralised systems managed by third-party companies may compromise the data - Centralised systems represent a single point of failure

Continued...

Table A.1: Networks, subnetworks and codes (continued)

Network	Subnetwork	Code
Edge computing challenges	Edge computing systems are complicated to design and implement	- Designing edge computing systems is complex due to storage and processing requirements - Edge devices can be vulnerable and unreliable - Heterogeneous systems make integration difficult
Edge computing opportunities	Edge computing supports healthcare data storage and sharing	- Edge computing is suitable for healthcare systems - Edge computing supports security through decentralisation - Edge computing provides opportunities for healthcare - Edge computing supports data availability - Edge computing supports decentralising data - Edge computing supports decision-making - Edge computing negates the need for centralised storage - Edge computing supports the caching of data to void latency - Edge computing reduces single-point-of-failure risks
	EdgeKV is an edge computing product that can support healthcare systems	- EdgeKV works with other heterogeneous nodes - EdgeKV is an edge-computing product - EdgeKV can support real-time scenarios such as autonomous driving
	Edge computing can form a tree-like structure	- Edge computing consists of a local layer and a global layer - Edge computing can consist of edge groups - Separate nodes can support heterogeneity - Edge computing supports real-time data processing - Edge computing supports load-balancing resources - Edge computing supports faster processing - Edge computing places processing and storage closer to the end-user
Healthcare architecture	Healthcare data are fragmented and stored in a decentralised manner	- Healthcare systems have digitised many processes and associated data - Private medical databases may store other information which may not be suitable for sharing with third parties - Most healthcare data are unstructured - Isolated data islands cannot be connected to other systems - Fragmented information makes it difficult to create a consolidated EHR
	Healthcare systems require strict governance to limit the probability of cybersecurity incidents	- WHO recommends that resource-constrained countries use open-source software to reduce costs - Increased adoption of blockchain in healthcare - eHealth systems differ in their approaches to privacy and governance - EHR security is a concern due to the sharing of the data with multiple systems - Several cyberattacks have been noted in healthcare systems - EHRs are private and should be secured - Permission structures related to healthcare data must be set up in the early stages - Two-factor authentication can be compromised - Three-factor authentication has been introduced to support two-factor authentication

Continued...

Table A.1: Networks, subnetworks and codes (continued)

Network	Subnetwork	Code
	Decentralised systems are complicated to design but benefit from technologies that connect systems and share data	- Distributed systems such as P2P offer flexibility but can be susceptible to security risks - Distributed systems can store data in different geographical locations - Distributed systems have advantages - If a decentralised system is compromised, only a subset of the data is breached, not the person's entire record - The increased volume of healthcare data has revealed the limitations of centralised systems - Modularity supports healthcare systems design - Web services can be used as a means to allow other systems to access data - It is possible to introduce new technology without replacing entire systems - Healthcare systems generally use a centralised design - Siloed systems limit information sharing - Institution-centric designs are not patient-centred and limit patients' access to their data - Sharing data between different cloud platforms is not easy due to interoperability restrictions - Interoperability can be a challenge - Middleware systems struggle with interoperability, which hampers data exchange
Healthcare data	Healthcare data can be combined with other forms of data	- Britain combines data from other domains with healthcare to support decision-making - High-income countries led the big data movement within healthcare
	Real-time data can be useful provided they are of a high quality	- Data can be repeated or lost making them difficult to use - Accurate and up-to-date medical history supports patient care - Healthcare systems contain duplicates, which increases complexity - Real-time and accurate data can assist in outbreaks and pandemics - Health information systems might not be delivering the intended benefits
	Healthcare data require a high degree of governance to protect the anonymity of the patient	- Big data can result in data governance and credibility issues - When grouping data, privacy still needs to be maintained - Patient anonymity should be a priority - Some eHealth systems have privacy preserving data sharing schemes - Data governance needs to be agreed upon prior to data mining
	Healthcare data exist in silos, but large data warehouses exist, suggesting an unbalanced amount of data stored across a decentralised system	- Decentralised systems can result in duplicated records - Data access in healthcare is usually distributed - Telecare Medicine Information Systems generate large amounts of data - Cloud-based platforms support healthcare data sharing - Hospitals are resource constrained making sharing information difficult - Distributed data need to be grouped and contextualised to make inferences - Healthcare data exist in silos - Browser/server architecture can be applied to EHR - Distributed data warehouses partition data in parallel across various nodes - Data can be mined across a distributed network instead of centralising the data - Data warehouses store large amounts of data for mining and analysis - Data generated through IoT further exposes the limitations of centralised designs

Continued...

Table A.1: Networks, subnetworks and codes (continued)

Network	Subnetwork	Code
Blockchain opportunities	Blockchain supports privacy and security	- Some blockchain technologies support permission delegation - Blockchain Merkle Tree structure assists with timestamp issues - Blockchain is robust - Smart contracts can be used for EHR access - Blockchain supports privacy - Blockchain supports trust
	Blockchain can be supported by off-chain and the use of lightweight nodes	- Off-chain data and resources can be linked to on-chain - Off-chain blockchain systems can store information in external devices, cloud storage or distributed systems - Blockchain supports decentralisation - Off-chain blockchain systems can perform computation thereby reducing the load on the on-chain system - Off-chain blockchain systems are more scalable and reduce storage requirements on on-chain - Blockchain can be energy-efficient - Blockchain lightweight nodes store a subset of information
	Blockchain can be used in a healthcare environment if the data storage is optimised	- Blockchain full nodes store the entire transaction history - Blockchain presents opportunities for healthcare - Blockchain designs can place the patient as the data owner - Blockchain can be more patient-centred - Blockchain can enhance transparency between patients and healthcare providers - Blockchain supports healthcare systems - Blockchain could enhance patient interactions with real-time data - Off-chain blockchain systems support healthcare systems by reducing on-chain storage - Each hospital could have a private blockchain linked to a consortium blockchain
Middleware systems	Middleware systems connect disparate healthcare systems	- Middleware systems connect disparate systems - Universal health coverage cannot be achieved without an EHR - Middleware systems can aid in edge computing
Patient-centredness	Patients should have access to and control over their master EHR	- Sharing EHRs helps doctors provide high-quality patient care - Patients should have control over their data - Successfully sharing healthcare data can support positive patient outcomes - Patients should also have access to their records - There needs to be consistency with Master Patient records
Web 3.0 challenges	Web 3.0 can be difficult to implement	- Web 3.0 can contradict cloud computing architecture - Web 3.0 is difficult to understand and implement - The decentralised nature of Web 3.0 can cause issues with artificial intelligence which usually requires centralised information - Web 3.0 can be challenging to implement

Continued...

Table A.1: Networks, subnetworks and codes (continued)

Network	Subnetwork	Code
Web 3.0 oppor- tunities	Web 3.0 supports trust and data ownership through decentralisation	- Web 3.0 resolves certain centralisation issues - Web 3.0 has been accepted across various industries - Web 3.0 enables trust - Web 3.0 presents opportunities for healthcare - Web 3.0 supports decentralisation - Web 3.0 solves problems related to data ownership - Web 3.0 supports interconnected networks - Web 3.0 supports security - Web 3.0 consists of decentralised nodes
Web technologies	Web technologies support the creation, storage, retrieval and privacy of data, including healthcare data	- Data can be stored on the IPFS using private data keywords, trapdoors and ciphertext data - IPFS (Interplanetary File System) provides decentralised storage opportunities - Cloud services are susceptible to latency issues - Web 3.0 supports co-management, co-construction, sharing access and private data sharing - Web technologies Web 2.0 allowed users to create and share content - The web is a hypertext document management system - Web 1.0 was static or read-only for one-way communication - Web 1.0 had compatibility issues - Web 3.0 and blockchain can work together - Web 2.0 is referred to as the Social Web - Web 2.0 is more dynamic and interactive

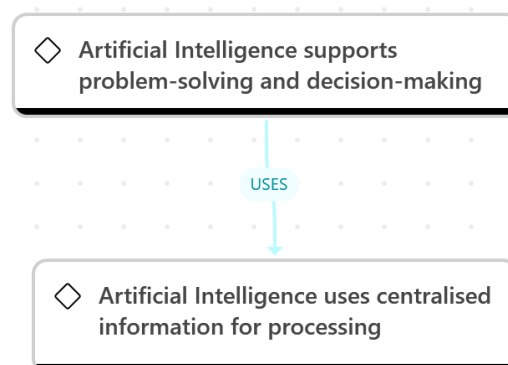


Figure A.1: Network - Artificial intelligence

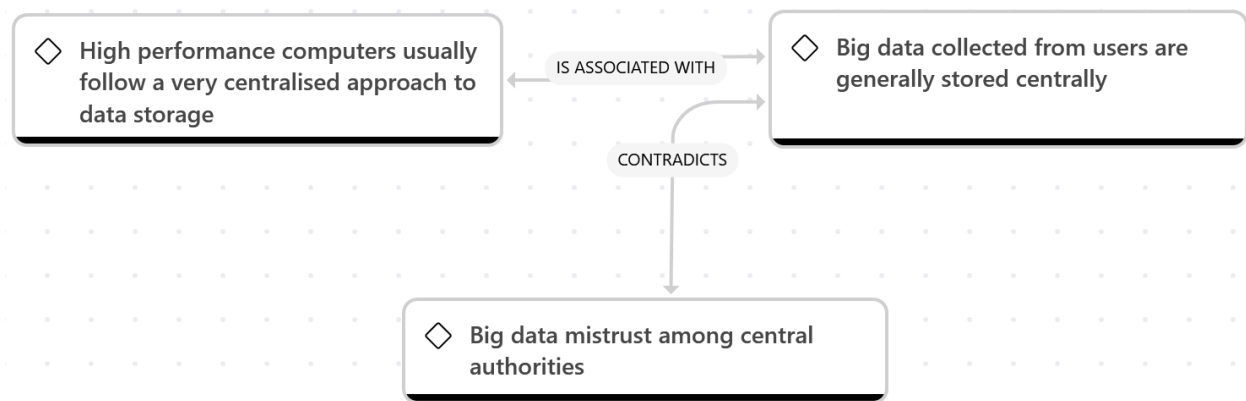


Figure A.2: Network - Big data

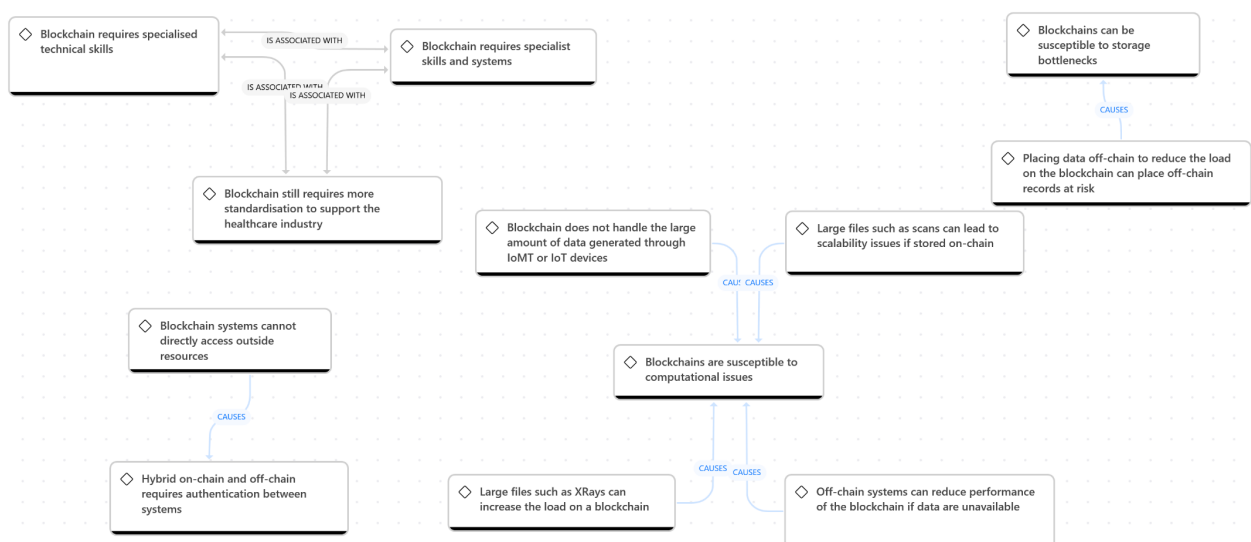


Figure A.3: Network - Blockchain challenges



Figure A.4: Network - Blockchain opportunities

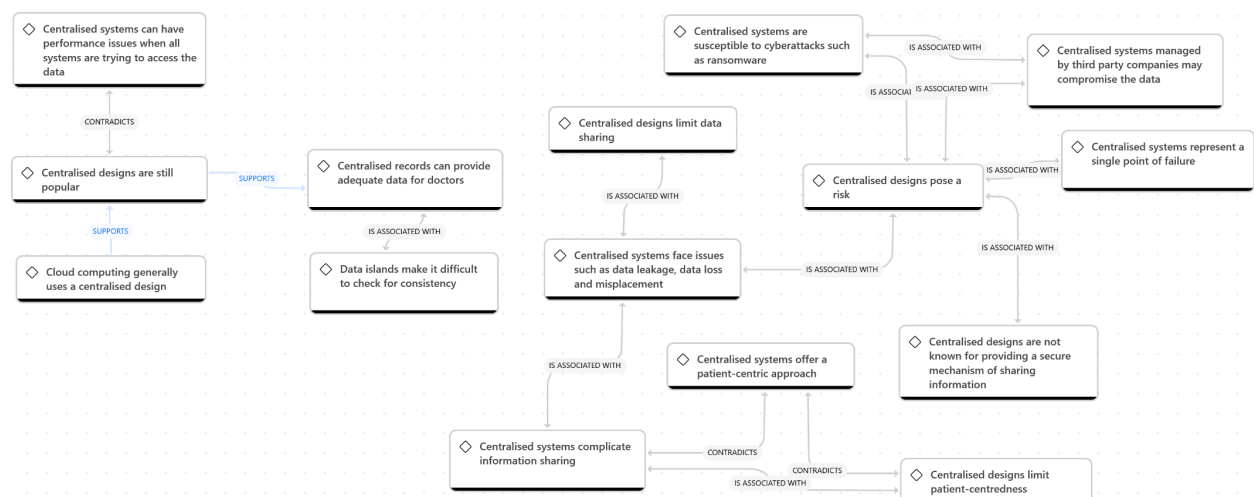


Figure A.5: Network - Centralised healthcare designs

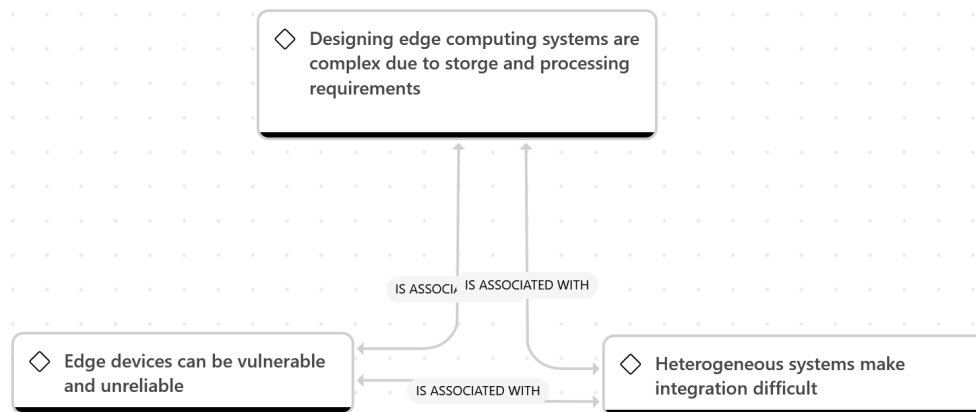


Figure A.6: Network - Edge computing challenges



Figure A.7: Network - Edge computing opportunities

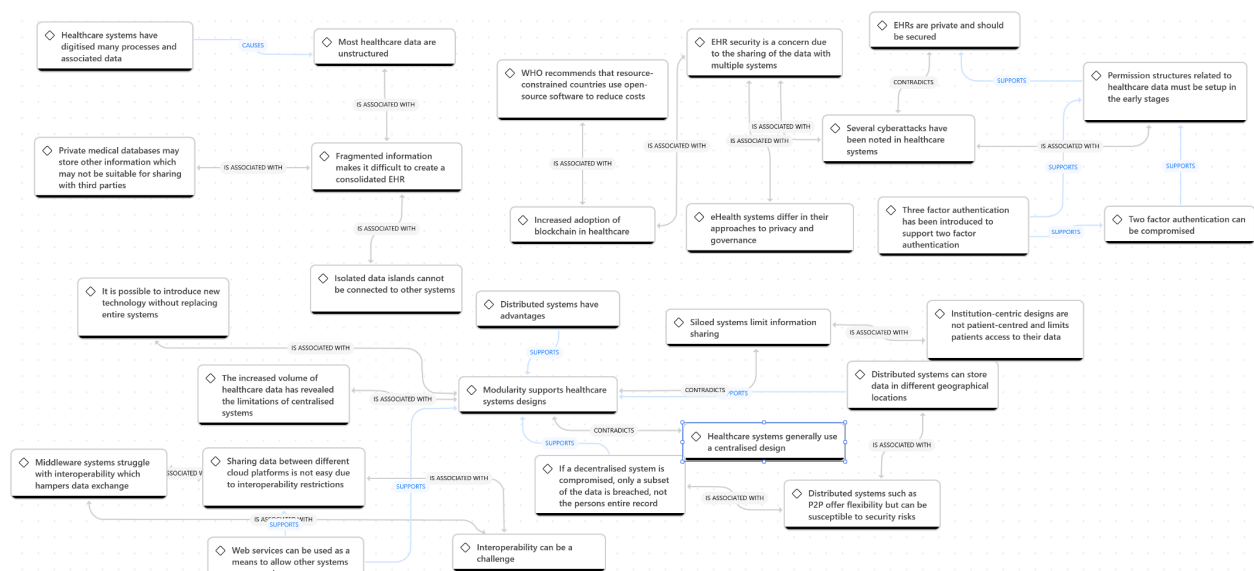


Figure A.8: Network - Healthcare architecture

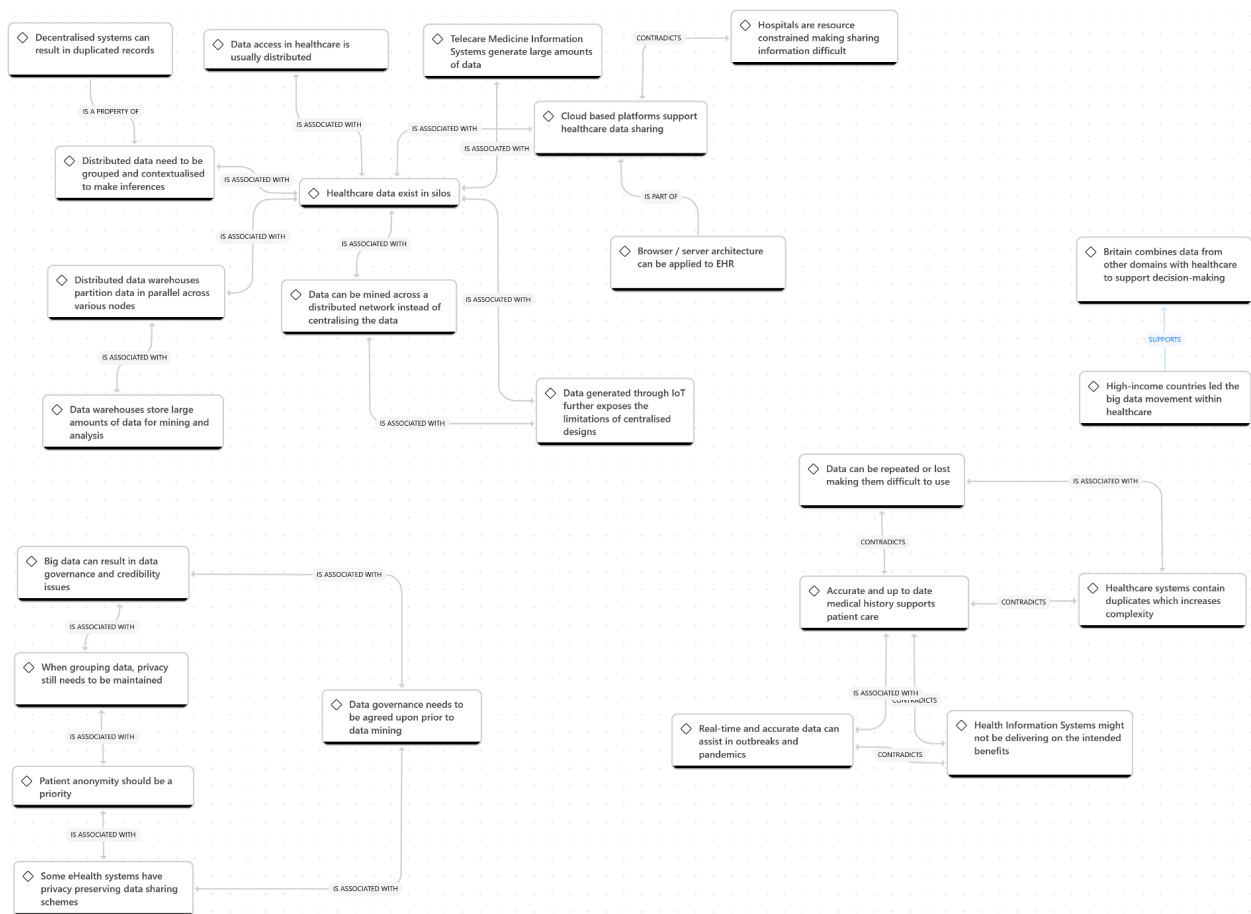


Figure A.9: Network - Healthcare data

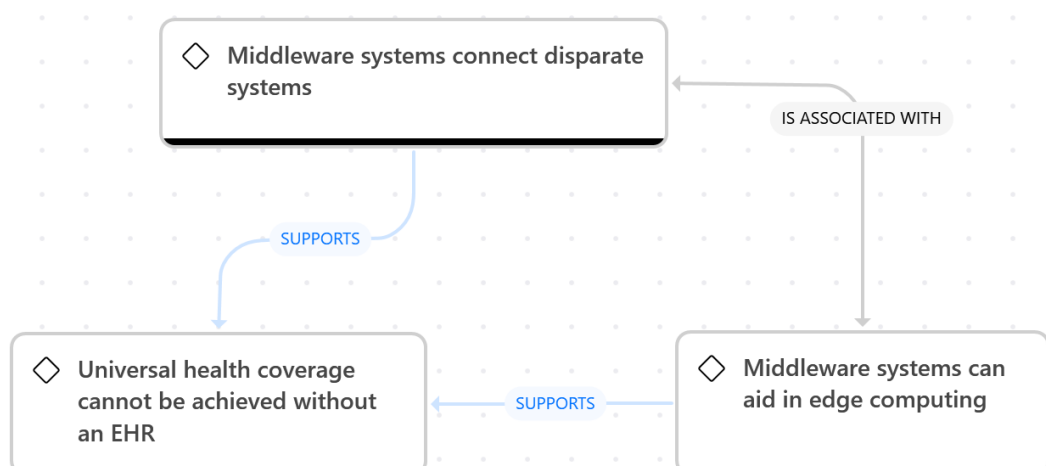


Figure A.10: Network - Middleware systems

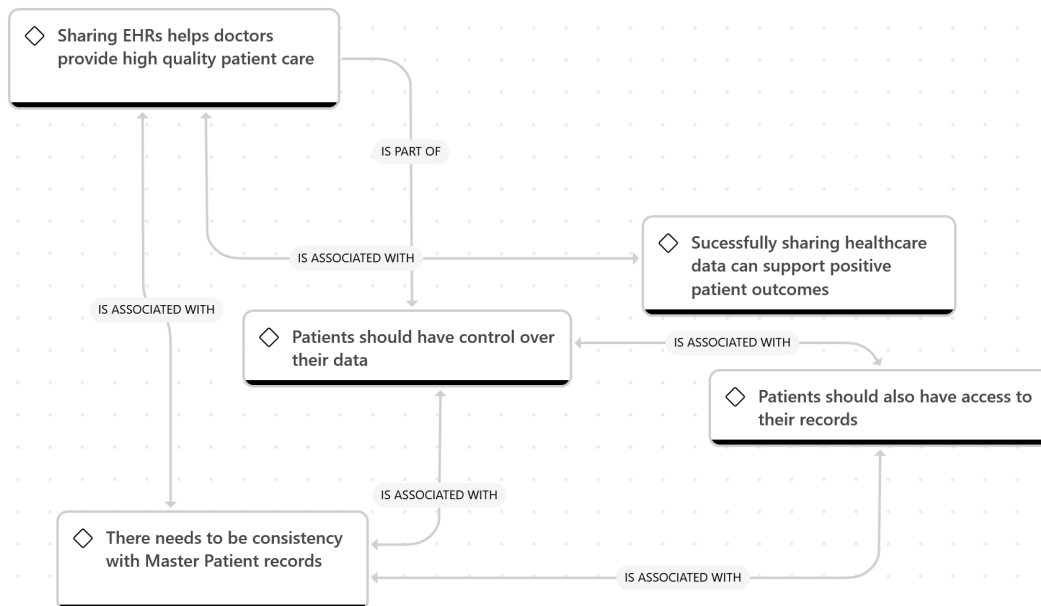


Figure A.11: Network - Patient centredness

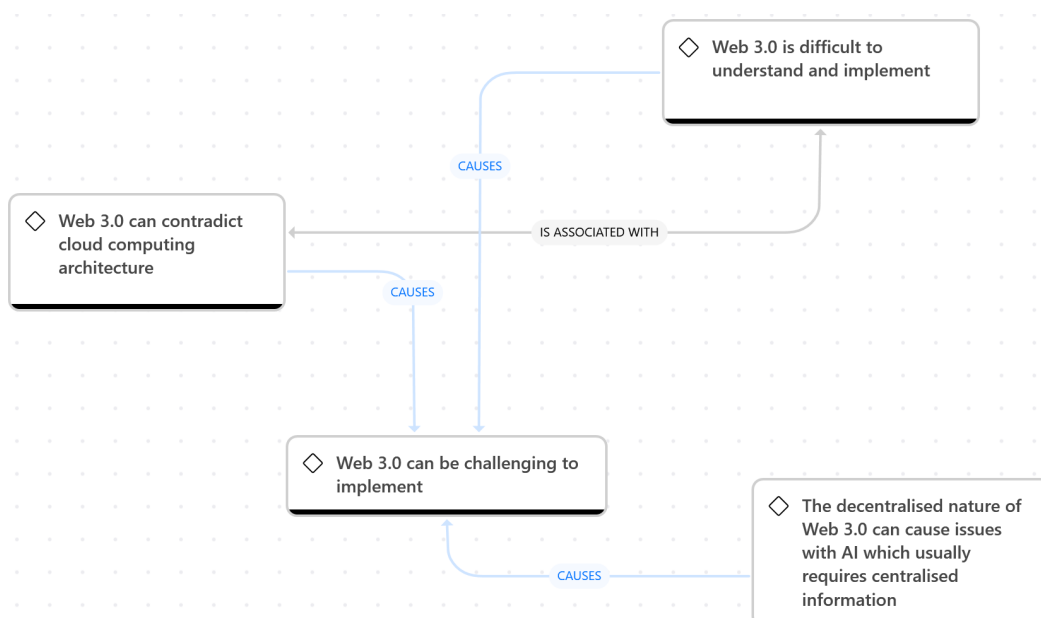


Figure A.12: Network - Web 3.0 challenges

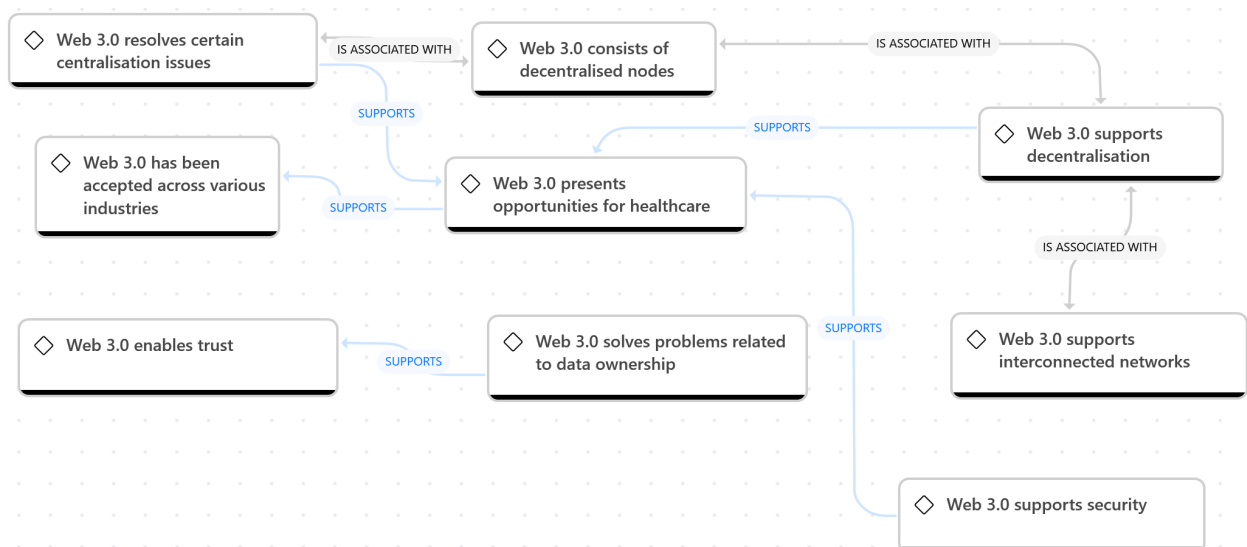


Figure A.13: Network - Web 3.0 opportunities

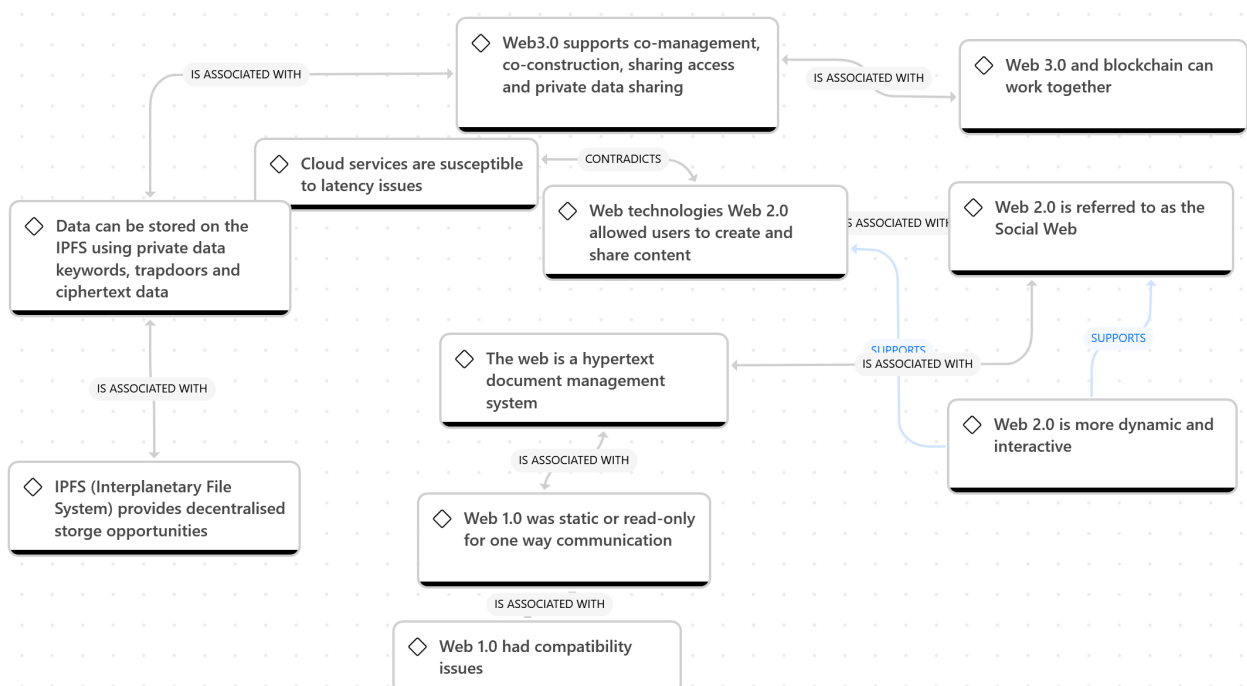


Figure A.14: Network - Web technologies