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…

https://doi.org/10.18489/sacjv38i1/22366

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…

https://doi.org/10.18489/sacjv38i1/22366

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…

https://doi.org/10.18489/sacjv38i1/22366

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…

https://doi.org/10.18489/sacjv38i1/22366

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

Network	Subnetwork	Code
Web 3.0 opportunities	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

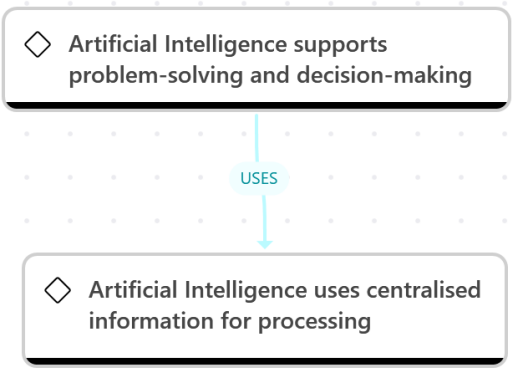


Figure A.1: Network - Artificial intelligence

https://doi.org/10.18489/sacjv38i1/22366

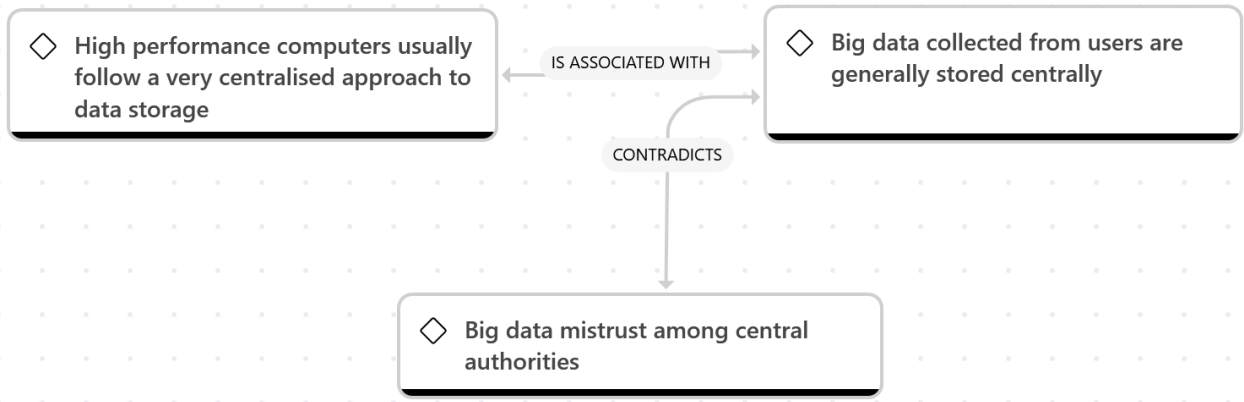


Figure A.2: Network - Big data

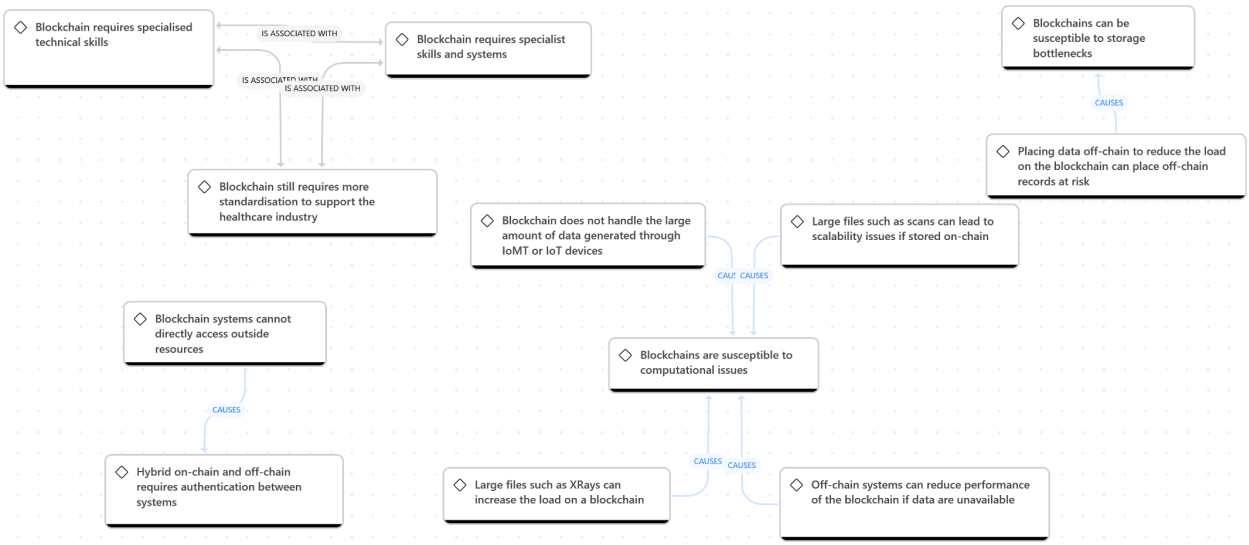


Figure A.3: Network - Blockchain challenges

https://doi.org/10.18489/sacjv38i1/22366



Figure A.4: Network - Blockchain opportunities

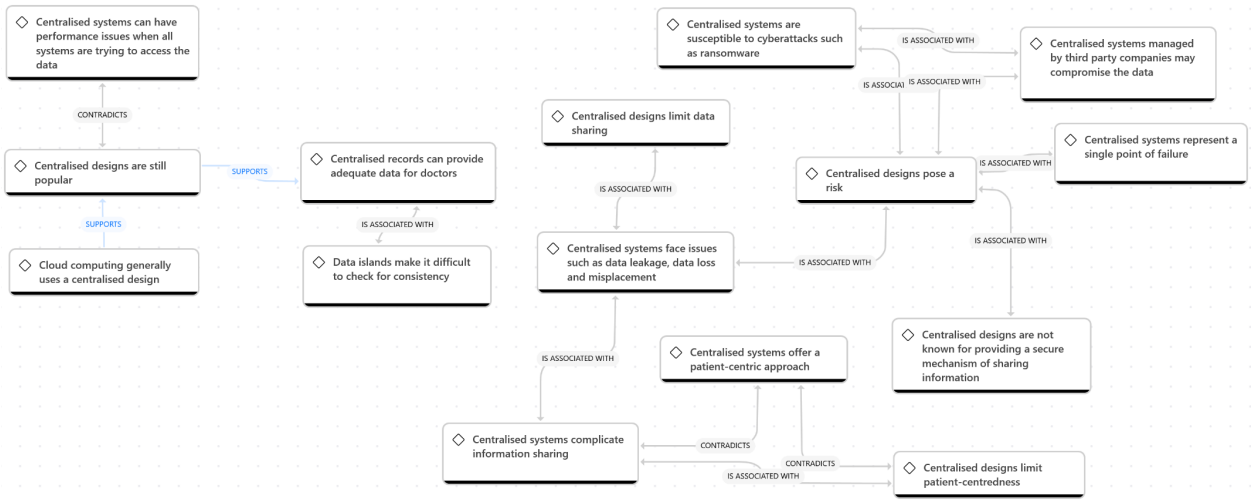


Figure A.5: Network - Centralised healthcare designs

https://doi.org/10.18489/sacjv38i1/22366

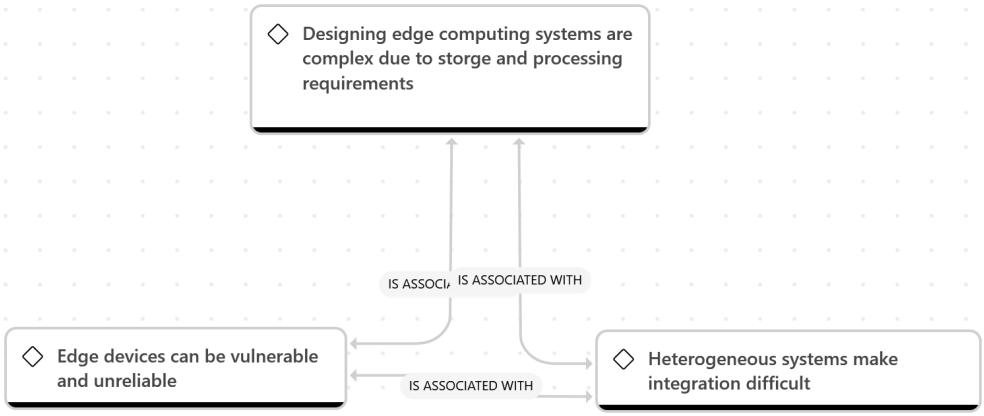


Figure A.6: Network - Edge computing challenges



Figure A.7: Network - Edge computing opportunities

https://doi.org/10.18489/sacjv38i1/22366



Figure A.8: Network - Healthcare architecture

https://doi.org/10.18489/sacjv38i1/22366

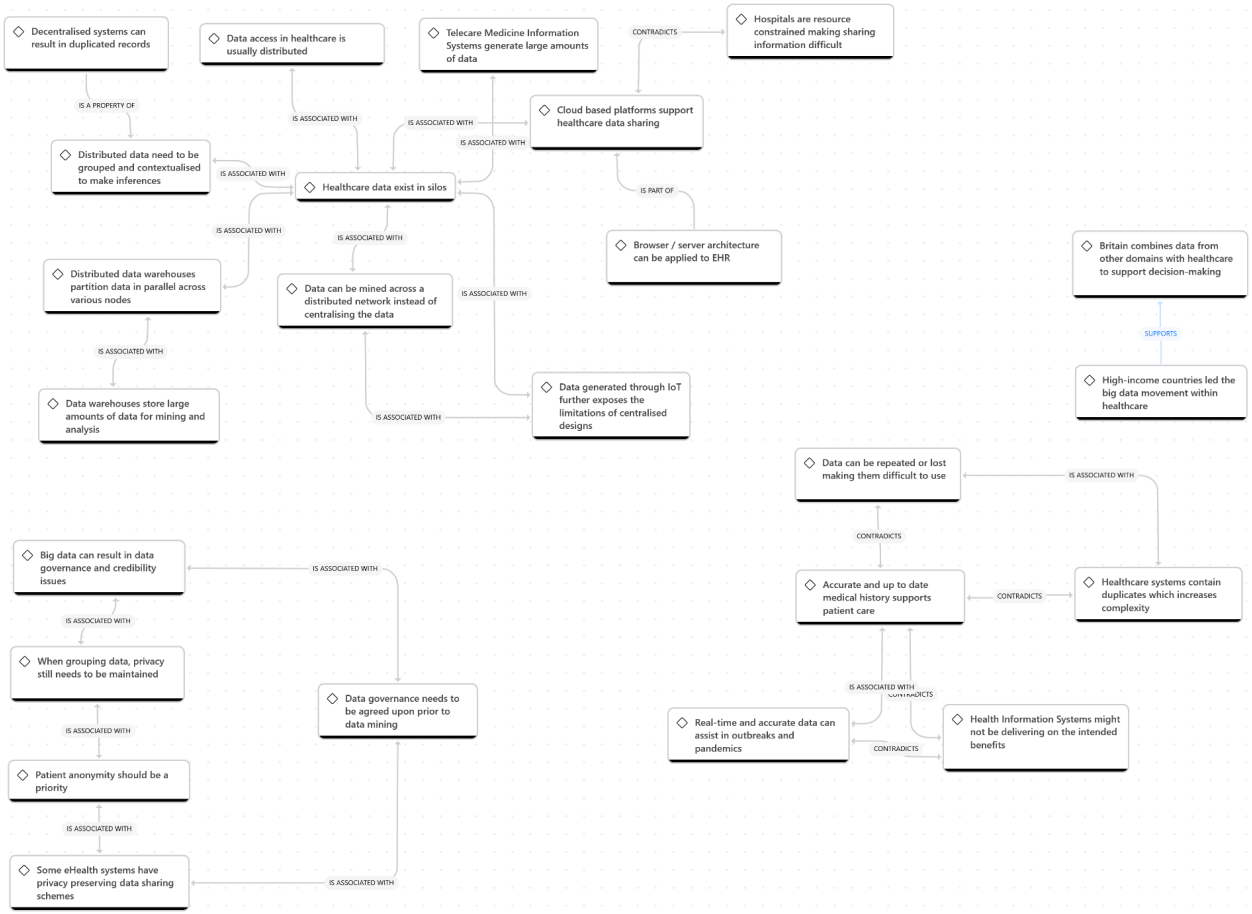


Figure A.9: Network - Healthcare data

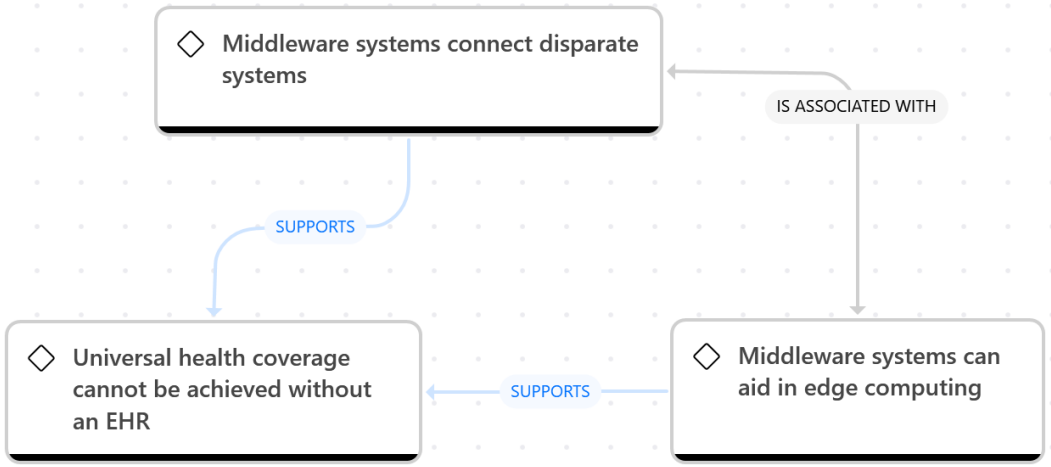


Figure A.10: Network - Middleware systems

https://doi.org/10.18489/sacjv38i1/22366

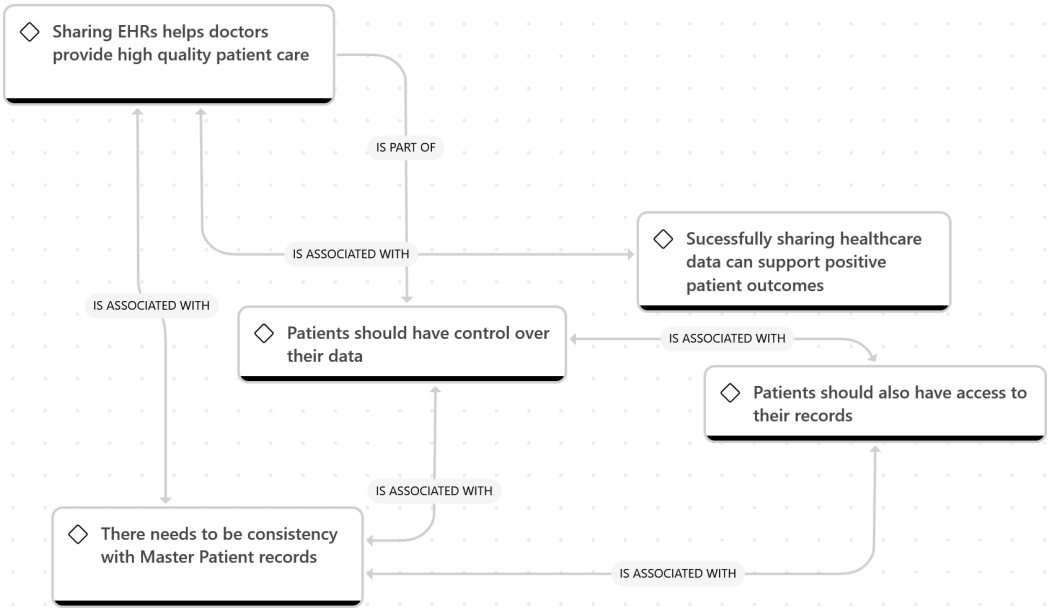


Figure A.11: Network - Patient centredness

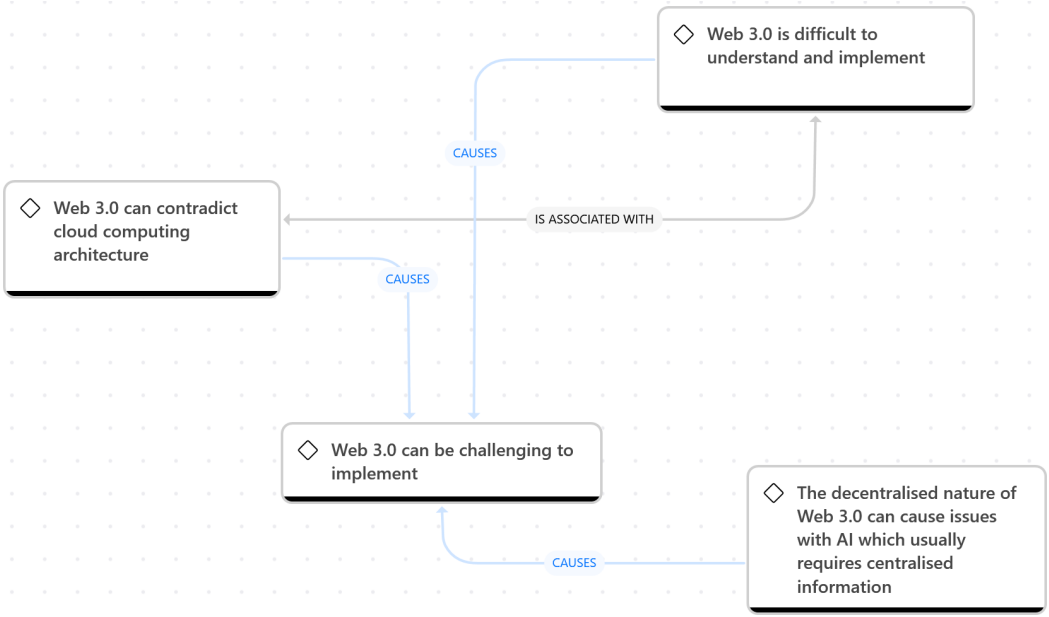


Figure A.12: Network - Web 3.0 challenges

https://doi.org/10.18489/sacjv38i1/22366

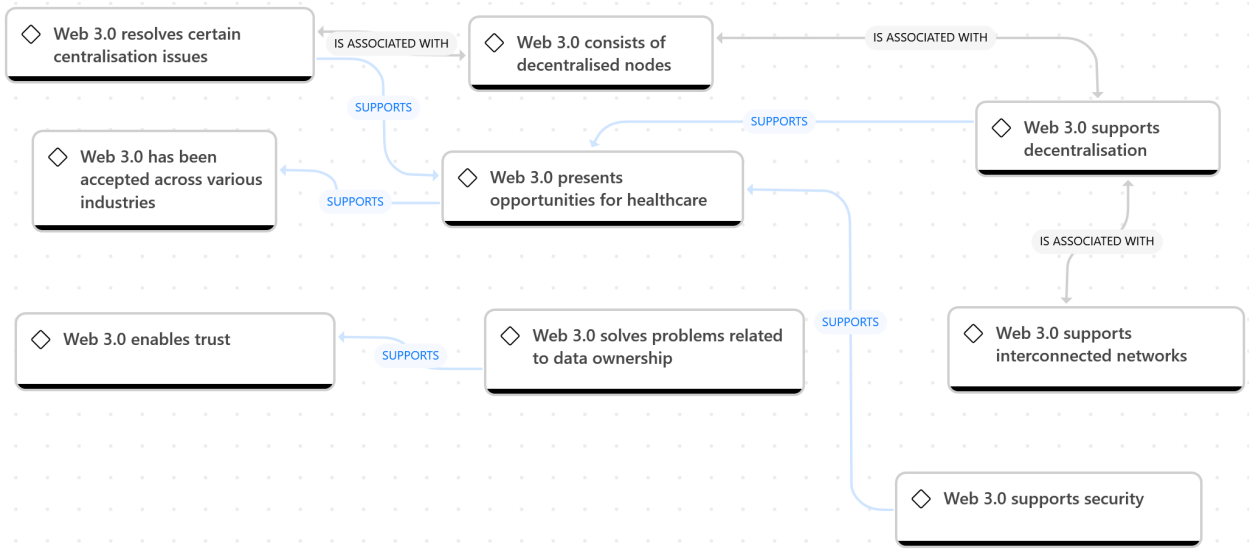


Figure A.13: Network - Web 3.0 opportunities

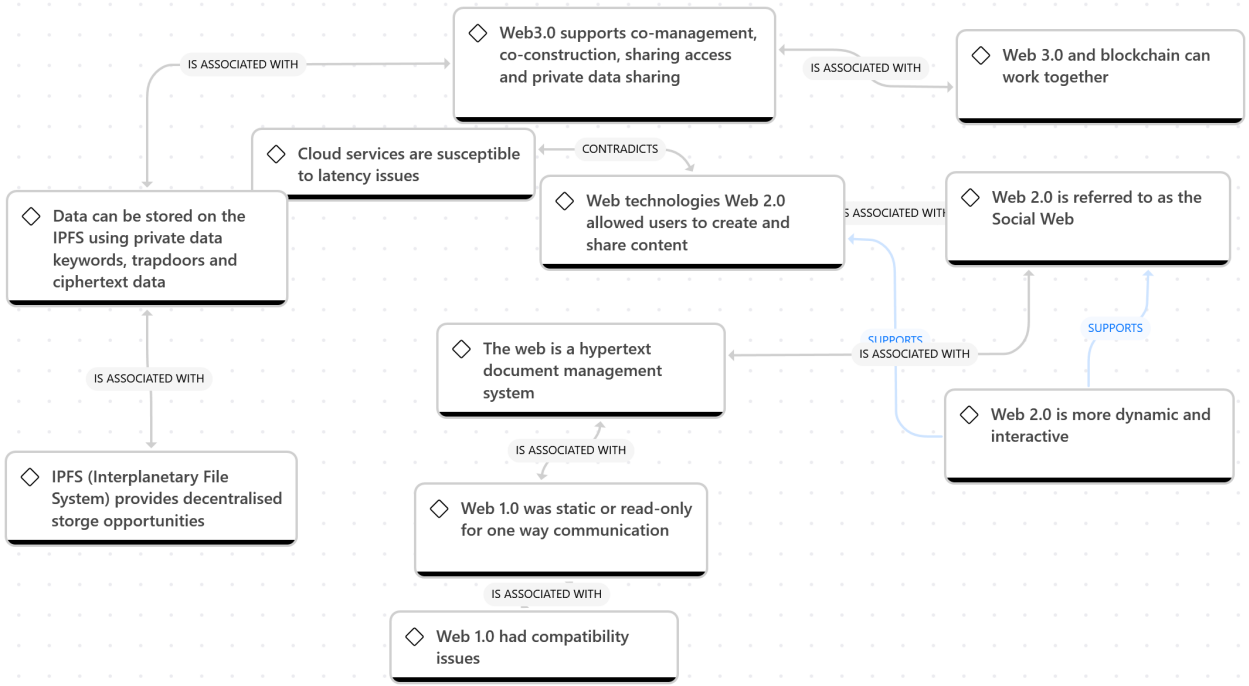


Figure A.14: Network - Web technologies

https://doi.org/10.18489/sacjv38i1/22366